Local Banach space theory and resource quantification in Quantum Information Processing

Aleksander M. Kubicki

Supervised by

Manuel Maestre, Carlos Palazuelos and David Pérez-Garcia

Facultat de Ciències Matemàtiques
Universitat de València

This dissertation is submitted for the degree of
Doctor at the University of Valencia (Doctorate degree programme in Mathematics)

April 2021

I declare that this dissertation titled *Local Banach space theory and resource quantification in Quantum Information Processing* and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a degree of Doctor in Mathematics at Valencia University.
- Where I have consulted the published works of others, this is always clearly attributed.
- Where I have quoted from the works of others, the source is always given. With the exception of such quotations, this dissertation is entirely my own work.
- I have acknowledged all main sources of help.

Valencia, April 7th, 2021

Aleksander M. Kubicki

We declare that this dissertation presented by Aleksander Marcin Kubicki titled *Local Banach space theory and resource quantification in Quantum Information Processing* has been done under our supervision at Valencia University. We also state that this work corresponds to the thesis project approved by this institution and it satisfies all the requisites to obtain the degree of Doctor in Mathematics.

Valencia, April 7th, 2021

Manuel Maestre **Carlos Palazuelos** **David Pérez-García**

Agradecimientos

El trabajo de años condensado en este documento dista mucho de ser una creación puramente individual. Es mucho el tiempo vertido en llevar a término el proyecto que aquí culmina, y en consecuencia, hay en él parte de quienes han compartido ese tiempo conmigo.

Esta tesis no sería sin la ayuda de mis directores. Agradezco profundamente a David su entusiasmo y ensoñador empuje; a Carlos, su natural predisposición al trabajo sucio (de polvo de tiza), al cual debo buena parte del aprendizaje acumulado durante el camino hasta aquí; y a Manolo, haber sido el artífice de la oportunidad para que echara a andar este camino.

Esta tesis tampoco sería sin ella, Laura. Tu apoyo y compañía han hecho posible que superara los días más duros y han hecho dichosos todos los demás. Es justo decir que estas páginas son también en parte tuyas.

A mi familia también debo la existencia de esta tesis. Especialmente a mi madre. Sin ella, ni yo mismo sería. No hay forma suficientemente justa de darte las gracias.

Doy las gracias también a los *bra-kets* del despacho 251 de la Facultad de Matemáticas de la UCM. Sois en buena parte responsables de estos años que me han llevado a concluir esta etapa. Ana, Pepe, Ángela, Abderramán, Patricia y Alberto; sin vuestra conversación y opinión probablemente podría haber acabado esta tesis mucho antes. No obstante, vuestra falta también me habría privado de mucho del enriquecimiento personal que os debo. Gracias por estar en esta tesis. A Abderramán agradezco también su ayuda con la versión en valenciano del resumen de este documento.

A Jaime, Raúl, Sergio y Lydia; gracias por hacerme sentir como en casa desde el primer día que llegué a Valencia. Sois parte también de esta tesis.

En el ámbito más privado, he tenido la inmensa suerte de compartir gran parte del tiempo que he pasado elaborando este trabajo con personas extraordinarias. Sergio y Carol; sin la fortuna de haberos conocido habría naufragado ya hace tiempo en mis proyectos y ambiciones. PepIsa, Vicente y Pablo; habéis formado parte irremplazable de esta etapa crucial de mi vida. Gracias a los seis por ser mi familia estos años. Jesús, Álvaro y Cosme; una parte inestimable de mi pensamiento y mi carácter está forjada en base a vuestra amistad. Gracias a los tres por ser mi familia siempre.

Concluyendo, agradezco al Ministerio de Ciencia e Innovación de España por apoyar económicamente el contrato FPI que ha posibilitado la realización de este trabajo.

I would like to thank Prof. Marius Junge for his immense generosity sharing his time with me whenever we managed to make our spatio-temporal coordinates coincident. Our discussions have been an invaluable source of inspiration for this thesis. I sincerely thank Prof. Jop Briët for kindly hosting me at CWI, an experience that has enriched myself as a researcher. I also thank Prof. Michael Wolf and Prof. Michal Sedlák for hosting me in my short stays at TUM and RCQI, respectively. These visits have been also important for the development of my thesis.

Resumen

Esta tesis se desarrolla en el terreno común entre el ámbito del análisis funcional y el estudio de la información cuántica. El principal objetivo que ha servido de guía para este trabajo es el estudio de la *Criptografía Cuántica Basada en la Posición* desde el punto de vista de la teoría local de espacios de Banach. Tal programa se ha llevado a cabo en dos fases. En primer lugar, se han contruido conexiones entre los problemas abordados en el ámbito de la información cuántica y ciertas ramas del análisis funcional. Esto nos ha permitido desarrollar herramientas de naturaleza analítica con las cuales avanzar en la comprensión del escenario criptográfico. Es más, de la conexión anterior surgen nuevas técnicas e ideas cuyo impacto no se restringe al estudio de la criptografía cuántica. Una muestra de ello es el estudio de los *Procesadores Cuánticos Programables.* Las técnicas aquí desarrolladas nos han permitido un mejor entendimiento de estos objetos fundamentales en la teoría cuántica de la computación. Esta es otra de las principales aportaciones de esta tesis.

Comenzaremos con un breve resumen de la estructura del trabajo. Los Capítulos 1 y 2 son de naturaleza introductoria. El objetivo del Capítulo 1 es introducir los elementos necesarios relativos al estudio cuántico de la información mientras que el Capítulo 2 está dedicado a las herramientas de análisis funcional necesarias para el desarrollo de los capítulos subsiguientes. En dichos capítulos, Capítulos 3 y 4, se presentan los principales resultados obtenidos. En el Capítulo 3 se estudian los Procesadores Cuánticos Universalmente Programables, considerados por vez primera por Nielsen y Chuang en [72]. Los Procesadores Cuánticos Programables se caracterizan por incluir una memoria cuya programación permite modificar la operación implementada por el procesador. La dimensión de memoria requerida para elevar a universal el

conjunto de operaciones *programables* es la principal cantidad estudiada, para la cual se han obtenido nuevas cotas que mejoran exponencialmente las conocidas con anterioridad. En el Capítulo 4 se presenta nuestro estudio sobre Criptografía Basada en la Posición. Es sabido que en este escenario criptográfico no es posible establecer seguridad frente a adversarios arbitrariamente poderosos. La principal pregunta abierta en este campo es hasta qué punto deben restringirse los recursos de los que pueden disponer los adversarios para evitar que puedan romper la seguridad del protocolo. Más en concreto, y ya en el ámbito de la criptografía cuántica, para comprometer la seguridad de la Criptografía Basada en la Posición, un equipo de adversarios necesita en general compartir *entrelazamiento cuántico*. Aquí abordamos el estudio de la dimensión necesaria de dicho recurso para comprometer la seguridad de cualquier protocolo en este escenario. Nuestra contribución a dicha pregunta se basa en la construcción de un determinado protocolo para la *Verificación de Posición* y la obtención de cotas al entrelazamiento necesario para atacarlo. Esto nos ha permitido desentrañar una profunda conexión entre el problema fundamental presentado y una serie de preguntas circunscritas naturalmente a la teoría local de espacios de Banach. Finalmente, en el Capítulo 5 se han recopilado algunas preguntas abiertas surgidas del trabajo antes presentado.

A continuación se hacen algunos apuntes históricos que servirán para contextualizar mejor el trabajo aquí expuesto. Más adelante en esta introducción retomaremos la descripción de los contenidos de la tesis para dar al lector una visión algo más detallada de los mismos antes de sumergirse en el texto principal.

Tan pronto como la teoría cuántica fue formalizada por J. Von Neumann en su tratado *Mathematische Grundlagen der Quantenmechanik*, publicado en 1932 aunque prácticamente completo ya en 1927 [120], emergieron fuertes lazos con el análisis funcional. Aunque tras casi un siglo ambos campos han experimentado un espectacular desarrollo de forma independiente, la relación entre ellos no ha hecho más que consolidarse por medio de un creciente número de sorprendentes conexiones. Una de estas conexiones es la que aquí nos trae: el entendimiento de ciertas construcciones en información cuántica a través de la teoría local de espacios de Banach y los espacios de operadores.

Respecto a la teoría local de espacios de Banach, el primero en reconocer el papel fundamental de los subespacios *finito* dimensionales fue A. Grothendieck. Su seminal *Résumé* [40] fue popularizado toda una década después de su publicación en 1953, cuando Lindenstrauss y Pełczyński reinterpretaron el "teorema fundamental de la teoría métrica de los productos tensoriales topológicos" de Grothendieck como una sencilla desigualdad de normas sobre matrices finito dimensionales [61]. Esta es la que hoy en día se conoce en este contexto como *desigualdad de Grothendieck*. Nacía así la teoría local de espacios de Banach que enriquecería notablemente el entendimiento de estos espacios. Algunos de los creadores de esta hermosa rama del análisis funcional son A. Pietsch, R. Schatten, G. Pisier, N. Tomczak-Jaeggermann, B. Maurey, J. L. Krivine, S. Kwapień y muchos otros que no nombramos aquí atendiendo a criterios puramente personales, y por tanto, arbitrarios.

Cambiando de tercio, el estudio de la información cuántica se comienza a erigir como un cuerpo de estudio independiente dentro de la teoría cuántica a partir de la invención del "Código Conjugado" de Wiesner. Este avance data de finales de la década de los 60, aunque tuvieron que pasar quince años para que la publicación de este trabajo fuera aceptada [127]. La idea de Wiesner supuso el nacimiento de la criptografía cuántica y, más ampliamente, el campo de la información cuántica. Esta rama de estudio acabaría conformándose como un cuerpo heterogéneo y extenso que actualmente abarca la computación cuántica, la cuantización de la teoría de Shannon de la información y otros campos como el estudio de los juegos no locales. En la última dirección señalada, es pertinente citar también el trabajo de Bell [6] como el origen de muchas de las ideas que han acabado siendo fundamentales. Una primera conexión entre el estudio de los juegos no locales y la teoría local de espacios de Banach se remonta a los trabajos de Tsirelson, que en [117] probó que la máxima violación de desigualdades de Bell bipartitas por medio de correlaciones cuánticas está acotada precisamente por la desigualdad de Grothendieck. El posterior desarrollo de esta conexión descubierta por Tsirelson ha resultado en una profunda interacción entre el estudio de juegos no locales y el estudio de normas tensoriales (en el sentido en el que las concibió Grothendieck) y espacios de operadores. La combinación de las ideas anteriores ha desembocado en fascinantes descubrimientos que han impactado de forma notable tanto el campo de la información cuántica como ciertas ramas del análisis funcional. Dos ejemplos destacados son el descubrimiento de violaciones no acotadas de desigualdades de Bell [81], que refuta la posibilidad de cierta extensión trilinear de la desigualdad de Grothendieck, y la incomputabilidad del valor entrelazado de juegos no locales [48], que implica la resolución del famoso problema de inmersión de Connes. El trabajo recogido en esta tesis continúa la tradición esbozada por las interconexiones entre los párrafos anteriores.

En el resto de esta introducción recogemos un resumen de los contenidos de este documento. El objetivo del Capítulo 1 es introducir algunas nociones de información cuántica al mismo tiempo que fijar cierta notación. Para ello, es necesario que dicho capítulo comience con una exposición muy elemental sobre espacios vectoriales y C*-álgebras. No se persigue aquí ninguna clase de completitud, los contenidos se han seleccionado por su utilidad más adelante en esta tesis y con la idea de establecer cierto convenio notacional. Tras esto, en la Sección 1.2 se presenta el formalismo de la mecánica cuántica siguiendo un enfoque abstracto que facilita la introducción de las nociones de estado, canal e instrumento cuánticos de manera más afín a la forma en la que estos elementos aparecerán más adelante. Los resultados de esta sección son plenamente autocontenidos, habiéndose adaptado ciertas pruebas clásicas a la presentación más bien peculiar que se ha escogido de esta materia. Además de aportar cierto grado de originalidad en la exposición de contenidos de sobra conocidos entre los practicantes del campo, esta forma de exposición ayuda a entroncar de forma mucho más natural la tradición recogida en este primer capítulo con los desarrollos posteriores realizados en este trabajo. Este primer capítulo finaliza introduciendo cierto tipo de juegos cuánticos que constituirán el marco adecuado para formalizar la conexión entre el estudio de la Criptografía Basada en la Posición y los espacios de Banach construida en el Capítulo 4. El Capítulo 2 es también de naturaleza introductoria. En él se introducen las herramientas de análisis funcional necesarias para el desarrollo de los Capítulos 3 y 4. La Sección 2.1 está dedicada a introducir algunas definiciones básicas relativas a los espacios de Banach y los espacios de operadores. Estas construcciones son las bases de naturaleza analítica sobre las que descansan los resultados alcanzados más adelante. En la

Sección 2.2 se discute la teoría de tipo y cotipo en espacios de Banach, nociones de importancia capital en esta tesis que aparecerán en los principales resultados presentados en los Capítulos 3 y 4. En el Capítulo 4 harán falta algunas herramientas técnicas adicionales, parte de las cuales se introducen en las Secciones 2.3 y 2.4. Más concretamente, en la Sección 2.3 se discute brevemente la interpolación compleja de espacios de Banach y en la Sección 2.4, con algo más de profundidad, los ideales de operadores entre espacios de Banach. Estos últimos están estrechamente relacionados con el estudio de normas tensoriales, iniciado por Grothendieck en su *Résumé*. En la última parte de esta última sección podemos encontrar la primera contribución original de esta tesis. Allí se introduce una clase de operadores que surge de manera natural de nuestro estudio en el Capítulo 4. La definición de esta clase de operadores puede entenderse como una generalización de los operadores de clase débil Schatten-von Neummann cuando se tienen en cuenta ciertos elementos nativos de la teoría de espacios de operadores. Hasta donde llega nuestro conocimiento, esta clase es nueva en la literatura. Concluyendo este capítulo, se prueban algunas propiedades básicas de estos operadores posponiendo para el futuro un estudio más profundo de ellos.

En el Capítulo 3 iniciamos el estudio de los Procesadores Cuánticos Universalmente Programables. Estos son un modelo de computador cuántico que trata de *cuantizar* la arquitectura de programa-en-memoria en la cual están basados los computadores clásicos más usuales. En [72], donde estos objetos son definidos por vez primera, M. A. Nielsen e I. L. Chuang prueban el conocido como *teorema de no programabilidad*[1]. Este resultado establece que un Procesador Cuántico Universalmente Programable capaz de implementar cualquier unitaria sobre un registro de dimensión dada, necesita una memoria de dimensión infinita para su funcionamiento. Es decir, el modelo exacto introducido por Nielsen y Chuang no es realizable en la práctica. Esto nos motiva a considerar modelos aproximados en los que la computación se lleva a cabo de forma imperfecta. De hecho, en [72] se muestra también que el modelo aproximado si que es factible cuando únicamente se dispone de recursos finito dimensionales. Un ejemplo sencillo de esto puede obtenerse a partir del protocolo de teleportación cuántica [7]. Dado esto, surge de manera

[1] Esto es una traducción libre del término *no-programming theorem.*

natural la pregunta acerca de la optimalidad de estos objetos. Más concretamente, nos preguntamos por la dimensión de memoria óptima para alcanzar cierto grado de precisión sobre un registro de entrada de dimensión dada. El trabajo presentado en este capítulo se orienta a acotar esta cantidad.

Nuestro principal resultado es una cota inferior a la memoria requerida por un Procesador Cuántico Universalmente Programable, la cual es exponencialmente más fuerte que los resultados conocidos en relación a la dependencia de esta con la dimensión del registro de entrada. En cierto sentido, esta cota es cercana a ser óptima. No obstante, la optimización de la dimensión de memoria en este contexto es un problema multiparamétrico que hace difícil obtener resultados que sean óptimos en todos los rangos de valores que uno pueda considerar. Para obtener esta cota hemos conseguido *caracterizar* los Procesadores Cuánticos Universalmente Programables como inclusiones isométricas de espacios de operadores de clase traza, $\mathcal{S}_1^d$ para cierto número natural d, en espacios de operadores acotados (equipado con la norma de operadores), $\mathcal{S}_\infty^m$ para cierto número natural m. La mera existencia de estas isometrías impone restricciones sobre los espacios implicados, las cuales pueden traducirse a fortiori en restricciones sobre los recursos requeridos por Procesadores Cuánticos Universalmente Programables. La herramienta clave para el estudio de las isometrías antes referidas resulta ser la constante de tipo-2 de los espacios de Banach involucrados. Como consecuencia de este análisis se obtiene la cota inferior anunciada. Por otra parte, complementamos el resultado anterior con una construcción de Procesador Cuántico Universalmente Programable basada en ϵ-recubrimientos del grupo unitario. Dicha construcción puede entenderse como una adaptación de trabajos anteriores en el contexto de las Medidas Cuánticas Programables [29]. De lo anterior se deducen nuevas cotas, ahora superiores, para la dimensión de memoria de dichos procesadores. Estas cotas, pese a la sencillez de la construcción propuesta, son esencialmente óptimas en cierto rango de dependencia. En particular, la dependencia del tamaño del Procesador Cuántico Universalmente Programable considerado con el parámetro de error coincide con otras cotas inferiores previamente. La combinación de los resultados obtenidos aclara significativamente la fenomenología que puede darse en estos objetos teóricos.

Tal y como se comentó al principio del párrafo anterior, el entendimiento último de la relación entre los parámetros de este tipo de procesadores es complejo y deja aún varias preguntas abiertas. En primer lugar, nuestras cotas inferiores son sólo *esencialmente* óptimas, en el sentido de que predicen una dependencia exponencial con la dimensión del registro de entrada mientras que las construcciones de Procesadores Cuánticos Universalmente Programables más eficientes conocidas hacen uso de una memoria exponencial en una cantidad cuadrática en la dimensión del registro de entrada. Esto deja algo de espacio para la mejora, ya sea encontrando nuevas cotas inferiores más fuertes o nuevas construcciones más eficientes. De momento no sabemos cuál de las dos posibilidades tiene mayor verosimilitud. Es interesante notar que la anterior pregunta abierta puede traducirse al ámbito del estudio de los subespacios del espacio normado de operadores acotados en dimensión finita por medio de la caracterización obtenida de los Programadores Cuánticos Universalmente Programables como inclusiones isométricas. La respuesta a la pregunta resultante, puramente matemática, parece ser desconocida pese a resultar ser una pregunta muy natural en este contexto. Acotando un poco el problema en cuestión conseguimos obtener algunos resultados parciales, aunque, como se ha dicho, el anterior sigue siendo un problema abierto. Por otro lado, probar nuevas cotas que recojan satisfactoriamente la dependencia de la dimensión de memoria con la dimensión del registro de entrada y el parámetro de error en todos los posibles rangos de valores parece estar fuera del alcance de las técnicas manejadas aquí. Tal mejora podría aportar nueva información relevante sobre la construcción conceptual estudiada en este capítulo. Los contenidos del Capítulo 3 están basados en la publicación:

- A. M. Kubicki, C. Palazuelos and D. Pérez-García. Resource quantification for the no-programming theorem. *Physical Review Letters, 122(8), 2019.*

En el Capítulo 4 presentamos nuestro estudio sobre Criptografía Basada en la Posición. La Criptografía Basada en la Posición se basa en la idea de desarrollar tareas criptográficas usando la posición geográfica como el único credencial que identifica a una parte. Así, la principal tarea a llevar a cabo es la Verificación de Posición, en la cual un agente ha de probar su posición a un grupo de verificadores a su alrededor. En escenarios puramente clásicos, esta propuesta es inherentemente insegura frente a ataques coordinados. Un grupo de adversarios sin acceso a la localización geográfica a verificar puede interceptar la comunicación procedente de los verificadores y simular cualquier acción que pudiera realizar un agente honesto ubicado en la posición que se pretende verificar. Esto motiva el estudio de protocolos para la Verificación de Posición considerando el uso de canales cuánticos para la comunicación entre las partes implicadas. Esta idea fue explorada originalmente por A. Kent [53] y formalizada más tarde en [15] por H. Buhrman y coautores. Pese a que los ataques coordinados que son capaces de burlar la seguridad de protocolos clásicos no pueden extenderse a este caso, en [15] los autores construyen un ataque genérico a cualquier protocolo de Verificación de Posición incluso cuando la comunicación entre verificadores y agentes es cuántica. No obstante, dicho ataque tiene la interesante característica de requerir la delicada manipulación de entrelazamiento cuántico. De hecho, en [15] se muestra también que esto es una característica indispensable para comprometer la seguridad de ciertos protocolos cuánticos de Verificación de Posición. De nuevo, esto plantea una pregunta sobre la optimalidad de los recursos necesarios para dicha tarea: ¿cuánto entrelazamiento es necesario y suficiente para atacar cualquier protocolo de Verificación de Posición?

Esta pregunta ha resultado ser inesperadamente dura y, de hecho, su entendimiento sigue siendo relativamente pobre. Los avances alcanzados en esta tesis sólo pueden calificarse de parciales en este sentido. En primer lugar, porque hemos estudiado aquí un escenario particular en el que nos hemos centrado en cuantificar los recursos cuánticos requeridos por la acción deshonesta de los adversarios despreciando los recursos clásicos puestos en juego, los cuales han sido considerados como recursos libres. La motivación para tal simplificación es que en el futuro cercano el coste del uso de recursos cuánticos será previsiblemente mucho mayor que el coste de usar recursos clásicos. No obstante, en un futuro más lejano en el que la computación cuántica universal con tolerancia a errores sea una realidad, la consideración del escenario especificado aquí puede dejar de ser adecuada. Aún así, el entendimiento de escenarios intermedios como este nos permite ahondar en la comprensión de la Criptografía Basada en la Posición y desarrollar técnicas que contribuyan a tal fin último. En segundo lugar, el entendimiento que aportan los resultados obtenidos en esta tesis de este escenario intermedio es también parcial, quedando importantes preguntas abiertas aún por contestar incluso en este caso. Sin embargo, pese a no haber alcanzado aún un conocimiento respecto a este escenario criptográfico tal que nos permita extraer consecuencias de relevancia práctica, el avance obtenido en esta tesis forma una sólida base sobre la que seguir desarrollando ideas y técnicas que permitan la resolución del puzle criptográfico planteado por la Criptografía Basada en la Posición.

En un nivel de concreción mayor, nuestra contribución en este contexto consiste en la construcción de cierto protocolo cuántico de Verificación de Posición y el desarrollo de técnicas para el estudio de la cantidad de entrelazamiento necesaria para atacarlo. Por un lado, se han obtenido cotas inferiores totalmente explícitas para esta cantidad pero que dependen de ciertas propiedades analíticas de las estrategias de los adversarios que tratan de corromper la seguridad del protocolo. Estas propiedades cuantifican en un sentido concreto la regularidad de dichas estrategias. Para estrategias *suficientemente regulares*, nuestros resultados implican fuertes cotas que muestran la seguridad de nuestro protocolo a *todos los efectos prácticos* en este caso restringido. El caso general queda aún abierto. El estudio de las constantes de tipo de ciertos espacios normados juega de nuevo un papel crucial en estos resultados. De hecho, también se presentan cotas alternativas que son válidas con total generalidad pero que vienen dadas en términos de ciertas constantes de tipo-2 que no hemos logrado estimar. No obstante, proponemos una conjetura en relación a dicha constante de tipo y obtenemos algunos resultados parciales que apoyan una posible resolución positiva de la conjetura. En particular, se muestran estimaciones para las constantes de tipo de diversos subespacios y para la *razón de volumen* de ciertos espacios normados que son compatibles con la validez de la conjetura. La verificación de esta supondría un avance muy destacado en la comprensión de este escenario criptográfico. Por otro lado, su revocación podría tener consecuencias inesperadas sobre la relación entre la razón de volumen y las constantes de cotipo en espacios de Banach.

Para completar esta perspectiva sobre el Capítulo 4 de este documento, daremos algunas pinceladas sobre su contenido a un nivel más técnico. Los resultados anteriores se han obtenido reinterpretando la acción de los adversarios como la estrategia para jugar cierto juego cuántico cooperativo en el que la comunicación entre los jugadores está restringida de forma muy particular. Esto aparece en la Sección 4.3. Una característica importante de estos juegos es que permiten una satisfactoria y elegante caracterización matemática. Adicionalmente, el protocolo de Verificación de Posición que proponemos ha sido construido de manera que su estructura nos ha permitido relacionar las estrategias deshonestas con funciones sobre el hipercubo Booleano que toman valores sobre determinados espacios normados. La probabilidad de éxito en el juego alcanzada por una estrategia viene controlada precisamente por el valor esperado de la norma de la imagen de la función asociada. Nuestros resultados principales se obtienen del estudio de esta cantidad. Para ello, recurrimos a una desigualdad de tipo Sobolev debida a Pisier que nos permite obtener cotas en función de cierto parámetro de regularidad asociado a la función y las constantes de tipo de cierto espacio normado sobre el que toma valores la función, cf. Sección 4.4. Estudiando estas constantes de tipo es como se deducen las cotas obtenidas. En la Sección 4.6 se prueban los resultados para estrategias *suficientemente regulares* mientras que la Sección 4.7 se dedica a enunciar formalmente nuestra conjetura relativa al caso general y la prueba de cierta evidencia que la respalda (constantes de tipo de subespacios y estimaciones para la razón de volumen). Las herramientas empleadas en esta última sección pertenecen al repertorio clásico de la teoría local de espacios de Banach, como, por ejemplo, la desigualdad de Balschke-Santaló, la desigualdad de Chevet o ciertas propiedades de operadores 2-sumantes y espacios con suficientes simetrías.

Este capítulo está basado en el trabajo:

- M. Junge, A.M. Kubicki, C. Palazuelos and D. Pérez-García. Applications of geometric Banach space theory to Position Based Cryptography. *Preprint, 2021.*

En el Capítulo 5 se recogen algunos comentarios finales y se proponen ciertas preguntas abiertas motivadas por este trabajo. Las principales líneas de continuación de esta tesis se circunscriben al estudio de los problemas que quedan abiertos en los Capítulos 3 y 4. Respecto al estudio de Procesadores Cuánticos Programables (Capítulo 3), aunque las nuevas cotas obtenidas en esta tesis para los recursos requeridos por dichos objetos mejoran sustancialmente el conocimiento preexistente de estos, aún queda cierto margen de mejora. Por un lado, aún queda por resolver la dependencia correcta del tamaño óptimo de memoria de un Procesadores Cuántico Universalmente Programable con el tamaño del registro de entrada. Este problema tiene una interesante contrapartida a nivel puramente matemático: decidir cual es la dimensión d del mayor subespacio del espacio de operadores $\mathcal{S}_\infty^m$ que es aproximadamente isométrico a $\mathcal{S}_1^d$. Pese a ser una pregunta muy natural en este contexto, aún no es conocida una respuesta definitiva a ella. Volviendo al estudio de Procesadores Cuánticos Programables, dejamos abierto también la deducción de cotas al tamaño de memoria que sean óptimas tanto en la dependencia con el parámetro de error del procesador como con el tamaño del registro de entrada. Resulta curioso observar que las cotas existentes (tanto superiores como inferiores) parecen capturar de forma adecuada el comportamiento de la cantidad en estudio solamente con respecto a uno de los parámetros. Esto parece indicar que la obtención de cotas que vayan más allá de este rango de parámetros puede ser un problema ciertamente desafiante.

En cuanto al estudio de la Criptografía Basada en la Posición (Capítulo 4), son más las preguntas que quedan abiertas que las respuestas alcanzadas en esta tesis. El trabajo mostrado aquí abre una vía nueva para explorar tales cuestiones. La principal pregunta en este contexto, la cantidad de entrelazamiento frente a la que se puede garantizar la seguridad criptográfica en este escenario, queda aún ampliamente abierta. Nuestros avances se centran en un escenario más concreto en el que comparamos los recursos cuánticos necesarios para comprometer la seguridad de este tipo de protocolos criptográficos con la cantidad de recursos cuánticos requeridos en la ejecución honesta de estos, dejando de lado el uso de recursos clásicos los cuales hemos considerado como recursos libres. Una primera cuestión a explorar sobre la base de este trabajo es qué parte de los resultados obtenidos pueden extenderse al escenario original en el que recursos cuánticos y clásicos son medidos de igual manera. Este es el escenario criptográfico estándar. Aunque ciertos resultados en esta dirección pueden obtenerse como continuación directa del trabajo aquí presentado, el estudio en profundidad de esta cuestión se deja para el futuro. Otra importante pregunta abierta en este punto es la validez de la conjetura hecha en el Capítulo 4. Su resolución podría aclarar el escenario analizado aquí así como producir nuevas herramientas técnicas con las que seguir avanzando en la comprensión de este campo de la criptografía cuántica.

Dejando de lado las preguntas más directamente relacionadas con los principales resultados de la tesis, las profundas conexiones establecidas en ella motivan además la exploración de otras cuestiones en el ámbito del análisis funcional. Del estudio llevado a cabo en el Capítulo 4 se pueden extraer diversas líneas de investigación interesantes por sí mismas, como es el estudio de la clase de operadores que introducimos al final del Capítulo 2, del parámetro de regularidad introducido en el estudio analítico de estrategias deshonestas en el contexto de la Criptografía Basada en la Posición o el desarrollo de nuevas técnicas que permitan profundizar en el estudio de las propiedades de tipo y cotipo de los espacios tratados en el Capítulo 4.

Summary

The present thesis develops at the intersection of functional analysis and quantum information science. In this vein, this work is mainly concerned with the study of *Position Based Quantum Cryptography* from the perspective of local Banach space theory. This programme is conducted first by building a connection between both fields and then by developing tools in the context of the latter to tackle open questions in the cryptographic setting. Additionally, some of the techniques that we build along the way are of independent interest to other problems within quantum information. In particular, here we also make notorious progress in the understanding of *Programmable Quantum Processors*.

First, we succinctly explain the structure of this work. We begin by setting out some preliminary notions in Chapter 1 – mainly devoted to a presentation of some relevant elements of quantum information – and Chapter 2 – devoted to providing the necessary functional analytic background. The main results are presented in subsequent chapters. In Chapter 3 we discuss Universal Programmable Quantum Processors, introduced by Nielsen and Chuang in [72], and obtain bounds for the optimal dimension of the memory used by these objects. In Chapter 4 we study the setting of Position Based Cryptography. The main open problem in this field consist on studying the amount of resources required by a team of attackers to defeat the security of any protocol in this setting. We contribute to the understanding of this question by constructing a *Position Verification* protocol and obtaining new lower bounds for the entanglement dimension necessary to compromise its security. Interestingly, while doing so, we uncover a deep relation between the above fundamental problem and natural questions in the context of local Banach space theory. Finally, in Chapter 5 we summarize a collection of open questions that arise from the work presented in this

thesis. A more thorough overview of the contents of this manuscript will be provided later in this introductory text. But before that, we make some remarks that help to contextualize better the work presented here.

Quantum theory and functional analysis were intimately tied up as early as the formalization of the former was initiated by J. Von Neumman in his famous treatise *Mathematische Grundlagen der Quantenmechanik*, originally published in 1932 although almost completed in 1927 [120]. Since then, both fields have independently undergone an extraordinary growth remaining, however, tightly intertwined by a growing number of connections between them. Here, we will be mainly concerned with one of these connections: the understanding of some constructions in quantum information in terms of the local theory of Banach spaces and operators spaces.

In what concerns local Banach space theory, the first one in recognizing the importance of finite dimensional subspaces in the theory of Banach spaces was A. Grothendieck. His celebrated *Résumé* [40] was only popularized a decade after its publication in 1953, when Lindestrauss and Pełczyński reinterpreted Grothendieck's "fundamental theorem of the metric theory of topological tensor products" as an inequality between norms on finite dimensional matrices [61] – this is nowadays known as *Grothendieck's inequality* –. This nascent local Banach space theory was fully established in subsequent decades, deeply enriching the understanding of Banach spaces. Some of the authors we are indebted to for this beautiful field of functional analysis are A. Pietsch, R. Schatten, G. Pisier, N. Tomczak-Jaeggermann, B. Maurey, J. L. Krivine, S. Kwapień and many others that we do not include here attending uniquely to personal and, therefore, arbitrary reasons.

On the other hand, the origins of quantum information can be traced back to Wiesner's *Conjugate Coding*, discovered in the late 1960s and only published fifteen years later in [127]. This resulted in the birth of quantum cryptography and, more broadly, the study of quantum information that would end up encompassing the theory of quantum computation, Shannon's quantum information theory and other fields such as the study on non-local games. In this broad sense, it is fair to also point out to Bell's work in 1964 [6] as the source of some of the ideas that have become seminal in the field.

A first connection between the study of non-local games and local Banach space theory appears in the work of Tsirelson, who showed in [117] that the maximal violation of Bell inequalities by quantum correlation matrices is upper bounded precisely by Grothendieck's inequality. Further exploration of the connection uncovered by Tsirelson had led to deep interactions between the seemingly innocent setting of non-local games and tensor norms of Banach spaces (as conceived by Grothendieck) and operator spaces. The combination of these ideas has resulted in exciting discoveries that have had a major impact in the field of quantum information as well as in functional analysis. Two culminating instances of that are the discovery of unbounded violations of tripartite Bell inequalities [81] – that refutes a natural trilinear extension of Grothendieck's inequality – and the uncomputability of the entangled value of non-local games [48] – that solves in the negative the long-standing Connes' embedding problem –. Moreover, the study of non-local games has had a great repercussion also in more practical contexts, leading to the creation of the field of device-independent cryptography [67, 4], among other applications such as randomness generation [84] or verification of quantum computations [99, 100]. We contribute to this circle of ideas by building new connections between quantum games – a generalization of non-local games –, Position Based Cryptography and local Banach space theory. As we have already mentioned, these connections also spread over other subfields of quantum information. In fact, another relevant contribution of this thesis is a better understanding of Programmable Quantum Processors.

To conclude, we summarize is some detail what can be found in this document. The aim of Chapter 1 is to introduce some notions of quantum information relevant to us at the same time as setting some notation. This chapter begins with an elementary exposition on finite dimensional linear spaces and C*-algebras. This exposition does not intend any sort of completeness, it is tailored to serve for our latter purposes. With that, we present the formalism of quantum mechanics in Section 1.2 following a rather abstract approach that facilitates the introduction of the basic constructions of states, channels and instruments in the precise form used later on. After proving some standard results of importance for the present work, this chapter concludes with the notion of quantum games. This kind of games provides the right framework to formalize the connection between Position Based Cryptography and Banach spaces developed in Chapter 4.

Chapter 2 is also introductory in nature. There, we provide the functional analytic tools necessary to develop forthcoming chapters. In Section 2.1, basic definitions concerning Banach spaces and operator spaces are presented. In Section 2.2, the notions of type and cotype of a Banach space are discussed stating some key results that will be needed in the remaining chapters. Type and cotype turn out to be fundamental notions in this thesis, appearing at the heart of the results presented in Chapter 3 and Chapter 4. Chapter 4 will require some additional artillery, part of which is introduced in Sections 2.3 and 2.4. There, we briefly discuss the method of complex interpolation and, more thoroughly, the essential construction of operator ideals between Banach spaces, intimately related with the subject of tensor norms initiated by Grothendieck. In Section 2.4 we find the first original contribution of this thesis. At the end of the cited section, we define some spaces of operators that have appeared naturally in our investigations of Chapter 4. These can be seen as a generalization of the class of weak Schatten-von Neummann operators enriched with ingredients coming from operator space theory. To the best of our knowledge, this is new in the literature. The chapter concludes with the proof of some very basic properties of this new class of operators. A deeper understanding of them is left for future work.

In Chapter 3 we present results in the subject of Universal Programmable Quantum Processors. These conform a conceptual model for a quantum computer that mimics the stored-program architecture of daily used classical computers. In [72], where the definition of these objects was introduced, M. A. Nielsen and I. L. Chuang showed their *no-programming theorem.* This result states that a Universal Programmable Quantum Processor able to perfectly implement any unitary operation in an arbitrary input state of given dimension requires an infinite dimensional system as memory. Therefore, the exact model is not implementable in practice and we are invited to explore approximate models in which the computation is performed imperfectly. The authors of [72] also showed that the approximate model is in fact implementable with a finite amount of resources. A simple example is given by the protocol of quantum teleportation [7]. However, the question about the optimality of Universal Programmable Quantum Processors naturally arises here. In particular, we ask for the optimal memory dimension for a given input dimension and a given error threshold. Our work in this chapter is devoted to obtaining bounds for this quantity. Our main result is a lower bound that exponentially outperforms any previous bounds in terms of the dependence with the input dimension of the processor. This is achieved by means of a *characterization* of Universal Programmable Quantum Processors as nearly isometric embeddings of the finite dimensional first Schatten class into a finite dimensional space of bounded operators (endowed with the operator norm). Given that, we use the type constants of the spaces involved to obtain bounds on the distortion of the isometric embedding in terms of the dimension of the spaces. Additionally, we also show that in terms of the error parameter – considering a fixed input dimension – previously known lower bounds are nearly optimal by providing a simple construction of an approximate Universal Programmable Quantum Processor based on ϵ-nets for the unitary group. This construction can be understood as an adaptation of previous work in the related field of Programmable Quantum Measurements [29]. The content of this chapter is based on the work:

- A. M. Kubicki, C. Palazuelos and D. Pérez-García. Resource quantification for the no-programming theorem. *Physical Review Letters, 122(8), 2019.*

In Chapter 4 we present our study of Position Based Cryptography. This consists on the development of cryptographic tasks using the geographical position of an agent as its only credential. Therefore, the central task in this context is Position Verification, in which the agent, who communicates with a team of verifiers surrounding it, has to convince them of its location. When the verification protocol is purely classical it is easy to show that Position Based Cryptography is inherently insecure against colluding attacks. This motivates the investigation of protocols for Position Verification that incorporate the use of quantum messages. This idea was first explored by A. Kent [53] and formalized later on in [15] by H. Burhman and coauthors. In [15], the authors presented a generic attack that allows colluding cheaters to break the security of Position Verification even when quantum communication is considered. An intriguing feature of this attack is that the cheaters have to engage in a convoluted manipulation of the delicate resource of quantum *entanglement*. In fact, it was already shown in [15] that this resource is in general imperative to break Position Verification protocols. Again a question about optimality arises: how much entanglement is necessary and sufficient in order to break the security of any Position Verification protocol?

This has proven to be a difficult question and, intriguingly, the answer is still very poorly understood. We contribute to its understanding by presenting a protocol for Position Verification and providing lower bounds on the entanglement necessary to break it. Our contributions here can be separated into two blocks. First, we obtain explicit lower bounds depending on some analytic properties of the cheating strategies that quantify their regularity (in some specific sense). When only strategies that are *regular enough* are considered, our results imply strong lower bounds that turn our protocol secure *for all practical purposes* against this kind of attacks. Nonetheless, the general case remains open. Secondly, we contribute to this broader context providing alternative lower bounds that apply in full generality (independently of the regularity properties of the strategies). The drawback of these unconditional bounds is that they are given in terms of the type-2 constant of a Banach space that we have not been able to estimate. Still, we conjecture a particular behaviour for this type constant and provide some computations that support a possible positive solution to our conjecture. The verification of the conjecture would remarkably improve our understanding of this cryptographic scenario. On the contrary, its refutation might also have some new implications in the relation between volume ratio and cotype constants of Banach spaces.

To obtain these results, we first assimilate the cheating action in the studied setting to the strategy to win a cooperative quantum game when the communication between the players is restricted in a concrete manner. This is explained in Section 4.3. Given that, the definition of the Position Verification protocol that we present allows us to understand cheating strategies as vector valued functions on the Boolean hypercube. The *score* attained by a considered strategy is given by the expected value of the norm of the image of the previous function. Our results follow from bounding this quantity. For that, we appeal to a Sobolev-type inequality due to Pisier that provides us with a bound in terms of some smoothness parameter depending on the function and the type constants of appropriate Banach spaces, see Section 4.4. The announced bounds are obtained from the study of these type constants. In Section 4.6 we prove the results for *regular enough* strategies while Section 4.7 is devoted to formally stating the conjecture for the unconditional case and proving some results supporting the conjecture. This chapter is based on:

- M. Junge, A.M. Kubicki, C. Palazuelos and D. Pérez-García. Applications of geometric Banach space theory to Position Based Cryptography. *Preprint, 2021.*

Finally, in Chapter 5 we make some concluding remarks and collect some interesting open questions emerging from our work.

Resum

Aquesta tesi es desenvolupa en el terreny comú entre l'àmbit de l'anàlisi funcional i l'estudi de la informació quàntica. El principal objectiu que ha servit de guia per fer aquest treball és l'estudi de la *Criptografia Quàntica Basada en la Posició* des del punt de vista de la teoria local d'espais de Banach. Això s'ha dut a terme construint primer connexions entre els dos camps que ens han permet desenvolupar eines de naturalesa analítica amb les quals abordar qüestions relatives a l'escenari criptogràfic. Les tècniques així desenvolupades resulten d'interès al marge del context criptogràfic anterior, siguent potencialment útils en altres problemes d'informació quàntica. Una mostra d'això és l'estudi dels *Processadors Quàntics Programables*, el millor enteniment del qual és una altra de les principals aportacions d'aquesta tesi.

Començarem amb un breu resum de l'estructura del treball. Els Capítols 1 i 2 són de naturalesa introductòria. L'objectiu del Capítol 1 és introduir els elements necessaris relatius a l'estudi de la informació quàntica mentre que el Capítol 2 està dedicat a les eines d'anàlisi funcional necessàries per al desenvolupament dels capítols subsegüents. En aquests capítols, Capítols 3 i 4, es presenten els principals resultats. En el Capítol 3 s'estudien els Processadors Quàntics Universalment Programables, considerats per primera vegada per Nielsen i Chuang a [72], obtenint-se cotes òptimes per a la dimensió de memòria utilitzada per aquests objectes. En el Capítol 4 es presenta el nostre estudi sobre Criptografia Basada en la Posició. El problema obert més important en aquest camp és la pregunta sobre la dimensió d'entrellaçament que un equip d'adversaris necessiten compartir per comprometre la seguretat de qualsevol protocol en aquest escenari. La nostra contribució a aquesta pregunta es basa en la construcció d'un determinat protocol per a la Verificació de Posició i l'obtenció de cotes a l'entrellaçament necessari per atacar-lo. Això ens ha

permès descobrir una profunda connexió entre el problema fonamental presentat i una sèrie de preguntes circumscrites naturalment a la teoria local d'espais de Banach. Finalment, en el Capítol 5 s'han recopilat algunes preguntes obertes sorgides de la feina abans presentada.

A continuació, es mostraran alguns apunts històrics que serviran per contextualitzar millor el treball aquí exposat. Més endavant en aquesta introducció reprendrem la descripció dels continguts de la tesi per donar al lector una visió un poc més detallada dels mateixos abans de submergir-se en el text principal.

Tan prompte com la teoria quàntica va ser formalitzada per J. Von Neumann en el seu tractat *Mathematische Grundlagen der Quantenmechanik*, publicat el 1932 tot i que estava pràcticament complet ja en 1927 [120], van emergir forts llaços amb l'anàlisi funcional. Encara que després de gairebé un segle els dos camps han experimentat un espectacular desenvolupament de forma independent, la relació entre ells no ha fet més que consolidar-se per mitjà d'un creixent nombre de sorprenents connexions. Una d'aquestes connexions és la que aquí ens porta: l'enteniment de certes construccions en informació quàntica a través de la teoria local d'espais de Banach i els espais d'operadors.

Respecte a la teoria local d'espais de Banach, el primer a reconèixer el paper fonamental dels subespais *finit* dimensionals va ser A. Grothendieck. El seu seminal *Résumé* [40] va ser popularitzat tota una dècada després de ser publicat en 1953, quan Lindenstrauss i Pełczyński van reinterpretar el"teorema fonamental de la teoria mètrica dels productes tensorials topològics" de Grothendieck com una senzilla desigualtat de normes sobre matrius finit dimensionals [61]. Aquesta és la que avui dia es coneix en aquest context com a *desigualtat de Grothendieck.* Naixia així la teoria local d'espais de Banach que enriquiria notablement l'enteniment d'aquests espais. Alguns dels creadors d'aquesta bella branca de l'anàlisi funcional són A. Pietsch, R. Schatten, G. Pisier, N. Tomczak-Jaeggermann, B. Maurey, J. L. Krivine, S. Kwapień i molts altres que no anomenem aquí atenent a criteris purament personals, i per tant, arbitraris.

Canviant de tema, l'estudi de la informació quàntica es comença a erigir com un cos d'estudi independent dins de la teoria quàntica a partir de la invenció de el "Codi Conjugat" de Wiesner. Aquest avanç data de finals de la dècada dels 60, tot i que van haver de passar quinze anys perquè la publicació d'aquest treball fos acceptada [127]. La idea de Wiesner va suposar el naixement de la criptografia quàntica i, més àmpliament, el camp de la informació quàntica. Aquesta branca d'estudi acabaria conformant-se com un cos heterogeni i extens que actualment abasta la computació quàntica, la quantització de la teoria de Shannon de la informació i altres camps com l'estudi dels jocs no locals. En l'última adreça assenyalada, és pertinent citar també el treball de Bell [6] com l'origen de moltes de les idees que han acabat sent fonamentals.

Una primera connexió entre l'estudi dels jocs no locals i la teoria local d'espais de Banach es remunta als treballs de Tsirelson, que en [117] va provar que la màxima violació de desigualtats de Bell bipartites per mitjà de correlacions quàntiques està fitada precisament per la desigualtat de Grothendieck. El posterior desenvolupament d'aquesta connexió descoberta per Tsirelson ha resultat en una profunda interacció entre l'estudi de jocs no locals i l'estudi de normes tensorials (en el sentit en què les va concebre Grothendieck) i espais d'operadors. La combinació de les idees anteriors ha desembocat en fascinants descobriments que han impactat de manera notable tant en el camp de la informació quàntica com en certes branques de l'anàlisi funcional. Dos exemples destacats són el descobriment de violacions no acotades de desigualtats de Bell [81], que refuta la possibilitat de certa extensió trilinear de la desigualtat de Grothendieck, i la incomputabilitat del valor entrellaçat de jocs no locals [48], que implica la resolució del famós problema d'immersió de Connes.

A la resta d'aquesta introducció recollim un resum dels continguts d'aquesta tesi. L'objectiu de l'Capítol 1 és introduir algunes nocions d'informació quàntica al mateix temps que fixar certa notació. Per a això, és necessari que aquest capítol comenci amb una exposició molt elemental sobre espais vectorials i C*-àlgebres. No es persegueix aquí cap classe de completesa, els continguts s'han seleccionat per la seva utilitat en aquesta tesi i amb la idea d'establir cert conveni notacional. Després d'això, en la Secció 1.2 es presenta el formalisme de la mecànica quàntica seguint un punt de vista abstracte que facilita la introducció de les nocions d'estat, canal i instrument quàntics de manera més afí a la forma en què aquests elements de sortir a més endavant. Després de presentar les proves d'alguns resultats importants, aquest primer capítol finalitza introduint cert tipus de jocs quàntics, que constituiran el marc adequat per a formalitzar la connexió entre l'estudi de la Criptografia Basada en la Posició i els espais de Banach construïda al Capítol 4.

El capítol 2 és també de naturalesa introductòria. En ell s'introdueixen les eines d'anàlisi funcional necessàries per al desenvolupament dels Capítols 3 i 4. La Secció 2.1 està dedicada a introduir algunes definicions bàsiques relatives als espais de Banach i els espais d'operadors. A la Secció 2.2 es discuteix la teoria de tipus i cotipus en espais de Banach. Aquestes són nocions de cabdal importància en aquesta tesi que apareixeran en els principals resultats presentats en els capítols 3 i 4. En el Capítol 4 caldran algunes eines tècniques addicionals, part de les quals s'introdueixen en les seccions 2.3 i 2.4. Més concretament, en la Secció 2.3 es discuteix breument la interpolació complexa d'espais de Banach i en la Secció 2.4, amb un poc més de profunditat, els ideals d'operadors entre espais de Banach. Aquests últims estan estretament relacionats amb l'estudi de normes tensorials, iniciat per Grothendieck en el seu Résumé. En l'última part d'aquesta última secció podem trobar la primera contribució original d'aquesta tesi. Allà s'introdueix una classe d'operadors que sorgeix de manera natural del nostre estudi en el Capítol 4. La definició d'aquesta classe d'operadors es pot entendre com una generalització dels operadors de classe feble Schatten-von Neummann quan es tenen en compte certs elements natius de la teoria d'espais d'operadors. Fins on arriba el nostre coneixement, aquesta classe és nova en la literatura. En conclusió aquest capítol, es proven algunes propietats bàsiques d'aquests operadors posposant per al futur un estudi més profund d'ells.

En el capítol 3 es presenten els resultats relatius a Processadors Quàntics Universalment Programables. Aquests són un model de computador quàntic que tracta de quantitzar l'arquitectura de programa-en-memòria en la qual estan basats els computadors clàssics més usuals. En [72], on aquests objectes són definits per primera vegada, M. A. Nielsen i I. L. Chuang proven el conegut com a *teorema de no programabilitat*[2]. Aquest resultat estableix que un Processador Quàntic Universalment Programable capaç d'implementar qualsevol unitària sobre un registre de dimensió donada necessita una memòria de dimensió infinita per al seu

[2] Això és una traducció lliure de el terme *no-programming theorem*

funcionament. És a dir, el model exacte introduït per Nielsen i Chuang no és realitzable en la pràctica. Això ens motiva a considerar models aproximats en què la computació es porta a terme de forma imperfecta. De fet, en [72] es mostra també que el model aproximat si que és factible quan únicament es disposa de recursos finit dimensionals. Un exemple senzill d'això pot obtenir a partir de l'protocol de teleportació quàntica [7]. Atès això, sorgeix de manera natural la pregunta sobre l'optimalitat d'aquests objectes. Més concretament, ens preguntem per la dimensió de memòria òptima per aconseguir cert grau de precisió sobre un registre d'entrada de dimensió donada. El treball presentat en aquest capítol s'orienta a delimitar aquesta quantitat. El nostre principal resultat és una fita inferior exponencialment més fort que els resultats coneguts en relació a la dependència amb la dimensió del registre d'entrada. Aquesta cota s'obté *caracteritzant* els processadors Quàntics Universalment Programables com inclusions isomètriques d'espais d'operadors de classe traça en espais d'operadors acotats (equipat amb la norma d'operadors). Addicionalment, en termes ara del paràmetre d'error, vam mostrar que altres cotes inferiors prèviament conegudes són òptimes en cert sentit donant una construcció de Processador Quàntic Universalment Programable basada en ϵ-recobriments de el grup unitari. Aquesta construcció es pot entendre com una adaptació de treballs anteriors en el context de les Mesures Quàntiques Programables [29]. Els continguts d'aquest capítol estan basats en la publicació:

- A. M. Kubicki, C. Palazuelos and D. Pérez-García. Resource quantification for the no-programming theorem. *Physical Review Letters, 122(8), 2019.*

En el capítol 4 presentem el nostre estudi sobre Criptografia Basada en la Posició. En aquest àmbit, l'objectiu és el desenvolupament de tasques criptogràfiques usant la posició geogràfica com l'únic credencial que identifica una de les parts. Així, la principal tasca a dur a terme és la Verificació de Posició, en la qual un agent ha de provar la seva posició a un grup de verificadors al seu voltant. En escenaris purament clàssics, aquesta proposta és inherentment insegura davant d'atacs coordinats. Això motiva l'estudi de protocols per a la Verificació de Posició considerant l'ús de canals quàntics per a la comunicació. Aquesta idea va ser explorada originalment per A. Kent [53] i formalitzada més tard a [15] per H. Buhrman i coautors. En [15], els autors construeixen un atac genèric a qualsevol protocol de Verificació de Posició fins i tot quan la comunicació entre verificadors i agents és quàntica. No obstant això, aquest atac té la interessant característica de requerir la delicada manipulació d'entrellaçament quàntic. De fet, en [15] es mostra també que això és una característica indispensable per a comprometre la seguretat de certs protocols quàntics de Verificació de Posició. De nou, això planteja una pregunta d'optimalitat dels recursos necessaris per a aquesta tasca: quant entrellaçament és necessari i suficient per a atacar qualsevol protocol de Verificació de Posició?

Aquesta pregunta ha resultat ser inesperadament dura i, de fet, el seu enteniment segueix sent relativament pobre. La nostra contribució al respecte consisteix en la construcció de cert protocol de Verificació de Posició i la prova de cotes inferiors a l'entrellaçament necessari per atacar-lo. En primer lloc, s'han obtingut cotes inferiors totalment explícites però que depenen de certes propietats analítiques de les estratègies dels adversaris que intenten corrompre la seguretat el protocol. Aquestes propietats quantifiquen en un sentit concret la regularitat d'aquestes estratègies. Per estratègies *prou regulars*, els nostres resultats impliquen fortes cotes que mostren la seguretat del nostre protocol a *tots els efectes pràctics* en aquest cas restringit. El cas general queda encara obert. Per a aquest cas genèric presentem cotes alternatives que són vàlides amb total generalitat però que vénen donades en termes de certes constants de tipus-2 que no hem aconseguit estimar. No obstant això, proposem una conjectura en relació a aquesta constant de tipus i obtenim alguns resultats parcials que donen suport a una possible resolució positiva de la conjectura. La verificació d'aquesta suposaria un avanç molt destacat en la comprensió d'aquest escenari criptogràfic. D'altra banda, la seva revocació podria tenir conseqüències inesperades sobre la relació entre la raó de volum i les constants de cotipo en espais de Banach.

Els resultats anteriors s'han obtingut reinterpretant l'acció dels adversaris com l'estratègia per jugar cert joc quàntic cooperatiu en què la comunicació entre els jugadors està restringida de forma molt particular. Això apareix en la Secció 4.3. Amb això, l'estructura de l'protocol de verificació de Posició proposat ens ha permès relacionar aquestes estratègies amb certes funcions vectorials sobre el hipercub Booleà. La probabilitat d'èxit en el joc aconseguida per una estratègia ve controlada precisament pel valor esperat de la norma de la imatge de la funció associada. Els nostres resultats principals s'obtenen de l'estudi d'aquesta quantitat. Per a això, vam recórrer a una desigualtat de tipus Sobolev deguda a Pisier que ens permet obtenir cotes en funció de cert paràmetre de regularitat associat a la funció i les constants de tipus de cert espai de Banach, cf. Secció 4.4. Estudiant aquestes constants de tipus és com es dedueixen les cotes obtingudes. A la secció 4.6 es proven els resultats per estratègies *prou regulars* mentre que la Secció 4.7 es dedica a enunciar formalment la nostra conjectura relativa a el cas general i la prova de certa evidència que dóna suport. Aquest capítol està basat en el treball:

- M. Junge, A.M. Kubicki, C. Palazuelos and D. Pérez-García. Applications of geometric Banach space theory to Position Based Cryptography. *Preprint, 2021.*

En el Capítol 5 es recullen alguns comentaris finals i es proposen certes preguntes obertes motivades per aquest treball.

Contents

Chapter 1

Preliminaries I: Some notions on quantum information

The aim of this first chapter is to introduce the formalism of the quantum theory of finite dimension systems. This is the natural framework in the study of quantum information, at least for what this thesis is concerned, and it is the basic framework to state the questions we address later on. Once we establish the fundamental elements of quantum theory needed for the development of our work – in Section 1.2 – we present an application of this formalism that will become particularly relevant in Chapter 4: the notion of *quantum games* – cf. Section 1.3. Before that, we review some elementary facts about linear spaces and C*-algebras in Section 1.1.

1.1 Basic mathematical constructions

1.1.1 Vector spaces and linear operators

In this section we are mainly concerned with finite dimensional vector spaces. Later on we will be interested in some normed structures on these objects, but for the moment, we start recalling some basic facts relying only on their linear structure. The main goal of this section is fixing some notation and nomenclature.

Vector spaces. Given a natural number d, we consider the complex d-dimensional vector space $\mathbb{C}^d$. In the case of real vector spaces we simply specify it as $\mathbb{R}^d$, although we will usually consider the underlying field to be $\mathbb{C}$. We understand $\mathbb{C}^d$ (or $\mathbb{R}^d$) simply as the linear span of the elements of a standard basis denoted by $\{|i\rangle\}_{i=1}^d$. This follows standard notation used in quantum mechanics. Sometimes, the considered vector space will be defined by a given alphabet – a non-empty, finite set –, $\mathcal{X}$, as the linear span of a basis indexed by elements of $\mathcal{X}$, $\{|x\rangle\}_{x\in\mathcal{X}}$. In this case, the corresponding $|\mathcal{X}|$-dimensional complex vector space will be denoted by $\mathbb{C}^{\mathcal{X}}$ (alternatively $\mathbb{R}^{\mathcal{X}}$). We will usually use this latter notation reserving calligraphic $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}, \dots$ to denote alphabets.

The algebraic dual of a vector space $\mathbb{C}^{\mathcal{X}}$, denoted $(\mathbb{C}^{\mathcal{X}})^\sharp$, is the space of linear forms acting on it. Given a basis of $\mathbb{C}^{\mathcal{X}}$, $\{|x\rangle\}_{x\in\mathcal{X}}$, the dual $(\mathbb{C}^{\mathcal{X}})^\sharp$ can be constructed as the linear span of the basis *dual* to $\{|x\rangle\}_{x\in\mathcal{X}}$. The latter is defined by a sequence of forms, denoted by $\{\langle x|\}_{x\in\mathcal{X}}$, verifying $\langle x|(|x'\rangle) =: \langle x|x'\rangle = \delta_{xx'}$ for any x, $x' \in \mathcal{X}$. This in fact defines the *pairing*:

$$\langle u|v\rangle := u(v) = \sum_{x\in\mathcal{X}} u_x\, v_x, \tag{1.1}$$

for any $u = \sum_{x\in\mathcal{X}} u_x \langle x| \in (\mathbb{C}^{\mathcal{X}})^\sharp$, $v = \sum_{x\in\mathcal{X}} v_x |x\rangle \in \mathbb{C}^{\mathcal{X}}$. We also fix the following convention. Given an element $u = \sum_{x\in\mathcal{X}} u_x |x\rangle \in \mathbb{C}^{\mathcal{X}}$, we associate to it a unique element $u^* = \sum_{x\in\mathcal{X}} \overline{u}_x \langle x| \in (\mathbb{C}^{\mathcal{X}})^\sharp$, where $\overline{u}_x$ is the complex conjugate of the complex number u_x. Notice that this fixes a bijection $\mathbb{C}^{\mathcal{X}} \simeq (\mathbb{C}^{\mathcal{X}})^\sharp$. When there is no risk of confusion, we denote such elements also in *bra-ket* notation: $u \equiv |u\rangle \in \mathbb{C}^{\mathcal{X}}$, $u^* \equiv \langle u| \in (\mathbb{C}^{\mathcal{X}})^\sharp$. Given two vector spaces $\mathbb{C}^{\mathcal{X}}$, $\mathbb{C}^{\mathcal{Y}}$ we can construct another vector space of dimension $|\mathcal{X}|\,|\mathcal{Y}|$ as the linear span of the set $\{|x, y\rangle\}_{x\in\mathcal{X},\, y\in\mathcal{Y}}$. This is the *tensor product* of these vector spaces, denoted by $\mathbb{C}^{\mathcal{X}} \otimes \mathbb{C}^{\mathcal{Y}}$. Accordingly, we also use the notation $|x, y\rangle \equiv |x\rangle \otimes |y\rangle$ for any $x \in \mathcal{X}$, $y \in \mathcal{Y}$.

Euclidean spaces. We can understand the pairing (1.1) as an *inner product* on $\mathbb{C}^{\mathcal{X}}$. This inner product turns $\mathbb{C}^{\mathcal{X}}$ into an *Euclidean* space, also refereed later on as *Hilbert* space[1] and denoted $\mathcal{H}_{\mathcal{X}}$. With that definition at hand, two non-zero vectors u, $v \in \mathcal{H}_{\mathcal{X}}$ are *orthogonal* if

[1] Recall that in the infinite dimensional case, to call a space Hilbert we also require completeness w.r.t. the norm induced by the scalar product. Here, we will use the

$\langle u, v\rangle = 0$. Therefore, the standard basis $\{|x\rangle\}_{x\in\mathcal{X}}$ considered before turns out to be an *orthonormal basis* – recall the definition of the dual basis $\{\langle x|\}_{x\in\mathcal{X}}$. The pairing (1.1) also induces a norm on $\mathcal{H}_{\mathcal{X}}$: for any $|u\rangle \in \mathcal{H}_{\mathcal{X}}$,

$$\||u\rangle\|_{\mathcal{H}_{\mathcal{X}}} := \Big(\langle u|u\rangle\Big)^{1/2}. \tag{1.2}$$

This norm is sometimes called *Euclidean* norm and provides the natural normed structure in a Hilbert space.

Linear operators. Consider again two vector spaces $\mathbb{C}^{\mathcal{X}}$, $\mathbb{C}^{\mathcal{Y}}$. The set of *linear operators* (or simply *operators*) from $\mathbb{C}^{\mathcal{X}}$ into $\mathbb{C}^{\mathcal{Y}}$ is denoted $\mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$. Any operator $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ can be characterized by $|\mathcal{X}|\,|\mathcal{Y}|$ scalars $(f_{xy})_{x\in\mathcal{X},y\in\mathcal{Y}}$ such that $|f(x)\rangle = \sum_{y\in\mathcal{Y}} f_{xy}|y\rangle$ for each $x \in \mathcal{X}$. Furthermore, this allows us to identify f with an element $\hat{f}$ in $\mathbb{C}^{\mathcal{Y}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$: $\hat{f} = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} f_{xy}|y\rangle \otimes \langle x|$. From now on, we simplify a bit the presentation denoting elements in this tensor product as $\hat{f} = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} f_{xy}|y\rangle\langle x|$. In the opposite direction, given an element $\sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} \lambda_{xy}|y\rangle\langle x| \in \mathbb{C}^{\mathcal{Y}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$ we can associate an operator $\lambda \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ such that $|\lambda(x)\rangle := \sum_{y\in\mathcal{Y}} \lambda_{xy}|y\rangle$. That is, in the finite dimensional case, we have the equivalence $\mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}}) \simeq \mathbb{C}^{\mathcal{Y}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$.

We notice that, in the previous representation of operators $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ as vectors in $\mathbb{C}^{\mathcal{Y}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$, the array of scalars $(f_{xy})_{x\in\mathcal{X},y\in\mathcal{Y}}$ is just the matrix representation of f in the bases $\{|x\rangle\}_{x\in\mathcal{X}}$, $\{|y\rangle\}_{y\in\mathcal{Y}}$. In view of this observation, the bra-ket convention chosen to denote elements of a vector space and its dual matches the standard convention on regarding *kets* $|x\rangle$ as column vectors and *bras* $\langle x|$ as row vectors. When $|\mathcal{X}| = |\mathcal{Y}|$, the matrix representing an operator in some bases is a square matrix and we can consider the trace as the linear functional that outputs the sum of its diagonal terms. Coming back again to the representation of operators as vectors in the tensor product $\mathbb{C}^{\mathcal{X}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$, we have the following representation for the trace map:

$$\begin{array}{rccc} \mathrm{Tr}: & \mathbb{C}^{\mathcal{X}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp & \longrightarrow & \mathbb{C} \\ & \hat{f} = \sum_{x,x'\in\mathcal{X}} f_{xx'}|x'\rangle\langle x| & \mapsto & \mathrm{Tr}(\hat{f}) := \sum_{x\in\mathcal{X}} f_{xx}. \end{array}$$

nomenclature of Hilbert rather than Euclidean spaces, even though for us there will be usually no difference between these two notions.

It is an elementary fact that this definition is independent of the choice of bases.

For the sake of completeness we also introduce the space of bilinear forms on $\mathbb{C}^{\mathcal{X}} \times \mathbb{C}^{\mathcal{Y}}$, denoted by $\mathscr{B}i\ell(\mathbb{C}^{\mathcal{X}} \times \mathbb{C}^{\mathcal{Y}})$. An element in $\mathscr{B}i\ell(\mathbb{C}^{\mathcal{X}} \times \mathbb{C}^{\mathcal{Y}})$ is a function

$$\begin{array}{rccc} f: & \mathbb{C}^{\mathcal{X}} \times \mathbb{C}^{\mathcal{Y}} & \longrightarrow & \mathbb{C} \\ & (|x\rangle, |y\rangle) & \mapsto & f(x,y) \end{array}$$

that is linear in each one of its components. In a similar vein as before, we can also identify the tensor product $(\mathbb{C}^{\mathcal{X}})^\sharp \otimes (\mathbb{C}^{\mathcal{Y}})^\sharp$ with $\mathscr{B}i\ell(\mathbb{C}^{\mathcal{X}} \times \mathbb{C}^{\mathcal{Y}})$: the map f above defines a tensor $\hat{f} = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} f(x,y)\langle x| \otimes \langle y|$ and any tensor $\hat{t} = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} t_{xy}\langle x| \otimes \langle y|$ defines a bilinear form by $t(x,y) = \langle\, \hat{t}, (|x\rangle \otimes |y\rangle)\,\rangle = t_{xy}$ for any $x \in \mathcal{X}$, $y \in \mathcal{Y}$.

In Chapter 2, we will revisit the previous identifications, $\mathbb{C}^{\mathcal{X}} \otimes \mathbb{C}^{\mathcal{Y}} \simeq \mathscr{L}((\mathbb{C}^{\mathcal{Y}})^\sharp, \mathbb{C}^{\mathcal{X}}) \simeq \mathscr{B}i\ell((\mathbb{C}^{\mathcal{X}})^\sharp \times (\mathbb{C}^{\mathcal{Y}})^\sharp)$, in the more subtle infinite dimensional case. These identifications play an important role in the fundamental notion of tensor norms on the tensor product of Banach spaces.

Moving to the following notion we need to introduce, one can notice that the tensor representation $\sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} f_{xy}|y\rangle\langle x|$ is not unique (one might consider a different basis on $\mathbb{C}^{\mathcal{Y}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$). The singular value decomposition provides us with a canonical representation:

Theorem 1.1 (Singular value decomposition)**.** *Let $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ be an operator with rank r. Then, there exist orthonormal systems $\{|u_1\rangle, \dots, |u_r\rangle\} \subset \mathbb{C}^{\mathcal{Y}}$, $\{|v_1\rangle, \dots, |v_r\rangle\} \subset \mathbb{C}^{\mathcal{X}}$, and unique (up to reordering) complex numbers $0 < s_1(f) \leq \dots \leq s_r(f)$ such that*

$$\hat{f} = \sum_{i=1}^{r} s_i(f)\, |u_i\rangle\langle v_i|.$$

The numbers $s_1(f) \leq \dots \leq s_r(f) < 0$ are the *singular values* of the operator f. The definition of singular values allows us to introduce the second family of normed spaces appearing in this thesis: the finite dimensional *Schatten* classes $\mathcal{S}_p(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$, for $1 \leq p \leq \infty$.

Given $1 \leq p \leq \infty$, the space $\mathcal{S}_p(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ is the vector space $\mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ endowed with the norm

$$\|f\|_{\mathcal{S}_p(\mathbb{C}^{\mathcal{X}},\mathbb{C}^{\mathcal{Y}})} := \Big(\sum_{i=1}^{r} |s_i(f)|^p\Big)^{\frac{1}{p}},$$

for any $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$.

In order to extend these notions to the infinite dimensional case, we have to take into account some further subtleties. In first place, we upgrade the linear spaces $\mathbb{C}^{\mathcal{X}}$, $\mathbb{C}^{\mathcal{Y}}$ to Hilbert spaces (taking into account completion in the Euclidean norm). Next, in order to make sense of the definitions above – that involve the singular value decomposition of the operator under consideration – we have to restrict to compact operators[2]. Therefore, being $\mathcal{H}$ and $\mathcal{K}$ arbitrary Hilbert spaces, $\mathcal{S}_p(\mathcal{H}, \mathcal{K})$ denotes de Banach space consisting of the closed subspace of *compact* operators in $\mathscr{L}(\mathcal{H}, \mathcal{K})$ with finite $\| \cdot \|_{\mathcal{S}_p}$ norm.

For $p = \infty$, the norm $\| \cdot \|_{\mathcal{S}_\infty}$ coincides with the *operator norm*:

$$\|f\| := \sup_{|u\rangle \in \mathsf{ball}(\mathcal{H})} \|f(|u\rangle)\|_{\mathcal{K}},$$

that no longer relies on the singular value decomposition of $f \in \mathscr{L}(\mathcal{H}, \mathcal{K})$. In fact, we can define the Banach space of linear operators in $\mathscr{L}(\mathcal{H}, \mathcal{K})$ with finite operator norm, denoted as $\mathscr{B}(\mathcal{H}, \mathcal{K})$. Notice that $\mathcal{S}_\infty(\mathcal{H}, \mathcal{K}) \subsetneq \mathscr{B}(\mathcal{H}, \mathcal{K})$. Of course, when $\mathcal{H}$ or $\mathcal{K}$ is finite dimensional every operator $f \in \mathscr{L}(\mathcal{H}, \mathcal{K})$ is automatically compact and both spaces coincide, $\mathcal{S}_\infty(\mathcal{H}, \mathcal{K}) = \mathscr{B}(\mathcal{H}, \mathcal{K})$.

A consequence of the singular value decomposition, together with the bijection $\mathbb{C}^{\mathcal{X}} \simeq (\mathbb{C}^{\mathcal{X}})^\sharp$, is a canonical representation of elements in $\mathbb{C}^{\mathcal{X}} \otimes \mathbb{C}^{\mathcal{Y}}$ known as Schmidt decomposition:

Corollary 1.2 (Schmidt decomposition)**.** *Given* $|u\rangle \in \mathbb{C}^{\mathcal{X}} \otimes \mathbb{C}^{\mathcal{Y}}$*, there exists a natural number* $r \leq \min(|\mathcal{X}|, |\mathcal{Y}|)$*, orthonormal systems* $\{|u_1\rangle, \ldots, |u_r\rangle\} \subset \mathbb{C}^{\mathcal{X}}$*,* $\{|v_1\rangle, \ldots, |v_r\rangle\} \subset \mathbb{C}^{\mathcal{Y}}$ *and complex numbers* $\lambda_1, \ldots, \lambda_r$

[2] The singular value decomposition stated in Theorem 1.1 can be extended to the infinite dimensional case when the operator is restricted to be compact, see e. g. [97, Section VI.5].

such that:

$$|u\rangle = \sum_{i=1}^{r} \lambda_i |u_i\rangle \otimes |v_i\rangle.$$

Next, we define the adjoint operator associated to $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$. Given a tensor $\hat{f} \in \mathbb{C}^{\mathcal{Y}} \otimes (\mathbb{C}^{\mathcal{X}})^\sharp$, we have already seen how we can associate an operator $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}}, \mathbb{C}^{\mathcal{Y}})$ to it. However, given $\hat{f} = \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} f_{xy} |y\rangle\langle x|$ we can also construct an operator $f^* : (\mathbb{C}^{\mathcal{Y}})^\sharp \to (\mathbb{C}^{\mathcal{X}})^\sharp$ defined by $\langle f^*(y)| = \sum_{x\in\mathcal{X}} f_{xy} \langle x| \in (\mathbb{C}^{\mathcal{X}})^\sharp$. This is the adjoint operator of f, that is, the operator fulfilling $\langle f^*(u)|v\rangle = \langle u|f(v)\rangle$ for any $u \in (\mathbb{C}^{\mathcal{Y}})^\sharp$, $v \in \mathbb{C}^{\mathcal{Y}}$. When understood as a matrix, the tensor associated to f^* is the conjugate transpose of $(f_{xy})_{x\in\mathcal{X}, y\in\mathcal{Y}}$, traditionally denoted by a dagger. This motivates the notation $\hat{f}^\dagger$ for the tensor associated to the adjoint operator f^*. Throughout this thesis, this choice will result much more natural than it seems now.

There are several classifications of operators attending to different properties of them. Here, we briefly recall some of them that are relevant for us.

- We say that an operator $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}})$ is *normal* if $f \circ f^* = f^* \circ f$. Furthermore, f is *hermitian* if[3] $f^* = f$. Another example of normal operators is the case of *unitary* operators, that are those $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}})$ such that $f \circ f^* = \mathrm{Id}_{\mathbb{C}^{\mathcal{X}}} = f^* \circ f$. This set will appear very often later on so we choose a specific notation for it, $\mathscr{U}(\mathbb{C}^{\mathcal{X}})$. For normal operators, the singular value decomposition of Theorem 1.1 can be strengthened as follows:

  Theorem 1.3 (Spectral decomposition). *Let $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}})$ be a normal operator. There exist an orthonormal basis of $\mathbb{C}^{\mathcal{X}}$, $\{|u_x\rangle\}_{x\in\mathcal{X}}$, and unique (up to reordering) complex numbers $\{\lambda_x(f)\}_{x\in\mathcal{X}}$ such that*

  $$\hat{f} = \sum_{x\in\mathcal{X}} \lambda_x(f)\, |u_x\rangle\langle u_x|.$$

  Furthermore, if f is hermitian, $\{\lambda_x(f)\}_{x\in\mathcal{X}}$ are real numbers.

[3] To make sense of this last definition, one has to identify $\mathbb{C}^{\mathcal{X}} \simeq (\mathbb{C}^{\mathcal{X}})^\sharp$. When $\hat{f}$ is regarded as a matrix, $f = f^*$ simply means that $\hat{f}$ is invariant under conjugate transposition.

This representation of normal operators will be referred as the *spectral decomposition* of f and $\{\lambda_x(f)\}_{x\in\mathcal{X}}$ as the *eigenvalues* of f.

- An hermitian operator $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}})$ is *positive semi-definite* if all its eigenvalues are in $\mathbb{R}^+$. This is equivalent to the condition $\langle u|f\,(u)\rangle \geq 0$ for all $|u\rangle \in \mathbb{C}^{\mathcal{X}}$ and also to the existence of a decomposition $f = g^* \circ g$ for some operator $g \in \mathscr{L}(\mathbb{C}^{\mathcal{X}})$. The set of positive semi-definite operators on a vector space $\mathbb{C}^{\mathcal{X}}$ is denoted $\mathrm{Pos}(\mathbb{C}^{\mathcal{X}})$. A particular case of positive semi-definite operators is the set of *density operators*, that are elements $\rho \in \mathrm{Pos}(\mathbb{C}^{\mathcal{X}})$ such that $\mathrm{Tr}\rho = 1$.

- Finally, projectors are idempotent operators, i.e., $f \in \mathscr{L}(\mathbb{C}^{\mathcal{X}})$ such that $f^2 = f$. When a projection is also hermitian, it is said to be orthogonal.

1.1.2 Basics on C*-algebras

A C*-algebra, $\mathscr{A}$, is a Banach algebra such that:

- there is an antilinear involution *, such that $(f\,g)^* = g^*\,f^*$ for all elements in the algebra;

- and this involution is compatible with the norm in the sense that $\|f\,f^*\| = \|f\|^2 = \|f^*f\|$ for any f in the algebra.

Example 1.4. The C*-algebra of bounded operators on a Hilbert space, $\mathscr{B}(\mathcal{H})$.

- The group operation on $\mathscr{B}(\mathcal{H})$ is given by the operator composition;

- the involution of an element $f \in \mathscr{B}(\mathcal{H})$ is provided by the adjoint operator f^*;

- the norm is given by the *operator norm*:

$$\text{for any } f \in \mathscr{B}(\mathcal{H}), \qquad \|f\|_{\mathscr{B}(\mathcal{H})} = \sup_{|u\rangle\in\mathcal{H}\,:\,\||u\rangle\|_{\mathcal{H}}\leq 1} \Big\||f(u)\rangle\Big\|_{\mathcal{H}}.$$

The GNS representation places the previous example in a central position, since it allows us to understand C*-algebras as C*-subalgebras of the canonical space $\mathscr{B}(\mathcal{H})$. We will always consider unital C*-algebras in which there exists an identity.

When restricted to finite dimensional algebras, the underlying Hilbert space $\mathcal{H}$ can be always taken to be finite dimensional. Therefore, finite dimensional C*-algebras are simply matrix algebras where the involution is given by the conjugate transpose operation and the C*-norm, by the operator norm defined in the preceding example. When the relevant dimension is signified, $\mathcal{H} = \mathbb{C}^d$, we use the more compact notation $\mathcal{S}_\infty^d$ to denote the C*-algebra $\mathscr{B}(\mathbb{C}^d)$. The abelian C*-(sub)algebra of diagonal d-dimensional complex matrices is correspondingly denoted by ℓ_∞^d or $\ell_\infty^{\mathcal{X}}$ when it is the alphabet $\mathcal{X}$ what is specified.

The * operation endows any C*-algebra $\mathscr{A}$ with a natural order. In terms of *, an element $f \in \mathscr{A}$ is positive if $f = g^* g$ for some $g \in \mathscr{A}$. It is a standard result that this set is a closed convex cone. Given elements $f, g \in \mathscr{A}$, we say that $f \geq g$ if $f - g$ is positive.

Remark 1.5. Notice that in the case $\mathscr{A} = \mathcal{S}_\infty^d$, the definition of positivity coincides with the definition of positive semi-definite operators, introduced in the previous section.

Furthermore, being $\mathscr{A}$ a C*-algebra and d a natural number, there is a natural way to regard the tensor product $\mathcal{S}_\infty^d \otimes \mathscr{A}$ also as a C*-algebra. In fact, this C* structure is unique (the C*-norm is determined in a unique way by the algebraic structure) and the resulting C*-algebra is denoted by $\mathcal{S}_\infty^d(\mathscr{A})$ from now on. A concrete way to understand this construction is identifying $\mathscr{A}$ as a subspace of $\mathscr{B}(\mathcal{H})$, for some Hilbert space $\mathcal{H}$, and then understanding $\mathcal{S}_\infty^d(\mathscr{B}(\mathcal{H})) \simeq \mathscr{B}(\mathcal{H}^{\otimes d})$ as the space of bounded operators on the Hilbert space $\mathcal{H} \otimes \overset{d)}{\dots} \otimes \mathcal{H}$. Clearly, we have again a notion of positivity in this C*-algebra and a related order. This observation will be important for the next paragraph.

Given two C*-algebras, $\mathscr{A}$, $\mathscr{B}$, we say that a linear map $f : \mathscr{A} \to \mathscr{B}$ is *positive* if it maps positive elements of $\mathscr{A}$ into positive elements of $\mathscr{B}$. Furthermore, f is *completely positive* if the maps $\mathrm{Id}_{\mathcal{S}_\infty^d} \otimes f : \mathcal{S}_\infty^d(\mathscr{A}) \to \mathcal{S}_\infty^d(\mathscr{B})$ are positive for any $d \in \mathbb{N}$. The set of completely positive maps between $\mathscr{A}$ and $\mathscr{B}$ is denoted $\mathrm{CP}(\mathscr{A}, \mathscr{B})$. In the concrete case that $\mathscr{A} \simeq \mathscr{B}(\mathcal{H})$, $\mathscr{B} \simeq \mathscr{B}(\mathcal{K})$, we simplify the notation to $\mathrm{CP}(\mathcal{H}, \mathcal{K})$.

Remark 1.6. When the range or the domain C*-algebra is commutative, positive maps are automatically completely positive, see for example [76, Chapter 3] for this well known result.

Another important property of maps between unital C*-algebras is *unitality*: $f : \mathscr{A} \to \mathscr{B}$ is *unital* if it maps the identity in $\mathscr{A}$ to the identity in $\mathscr{B}$.

The last notion we introduce is a combination of the previous two. A *state* in a C*-algebra is a unital and positive functional $\rho : \mathscr{A} \to \mathbb{C}$. In the case $\mathscr{A} = \mathscr{S}_\infty^d$, $\rho : \mathscr{S}_\infty^d \to \mathbb{C}$ can be understood as an operator $\mathbb{C}^d \to \mathbb{C}^d$. Under this identification, ρ is a state when it is a density operator, in the sense of our previous discussion of linear operators.

1.2 Quantum theory of finite dimensional systems

1.2.1 Registers, states and evolution

Our main focus is on the description of systems whose observation leads only to finitely many different possible outcomes. For reasons that will become clear later, we refer to such systems as *finite dimensional.* Following [124], we identify those systems with *registers*, as defined next. Therefore, we use both words – *system* and *register* – interchangeably, although system evokes a more concrete nuance while register emphasizes the abstract description deprived of the details of any physical realization.

Definition 1.7. *A register* X *is either one of the following objects:*

1. *a finite, non-empty, set (that is, an alphabet)* $\mathcal{X}$*;*
2. *an* n*-tuple* $\mathsf{X} = (\mathsf{X}_1, \dots, \mathsf{X}_n)$ *being* n *a positive integer and* $\mathsf{X}_1, \dots, \mathsf{X}_n$*, registers. For a composed register as* X*, we refer to* $\mathsf{X}_1, \dots, \mathsf{X}_n$ *as subregisters.*

According to the previous definition, any register can be identified with an alphabet. We denote the corresponding alphabet with the same letter as the register but in calligraphic style.

The second item in the definition emphasizes the composability nature of the alluded notion, that reflects the idea that we can regard multiple systems as a unique, composed, one. For the sake of concreteness, we specify the alphabet of a composite register in terms of its components:

The alphabet associated to register $\mathsf{X} = (\mathsf{X}_1, \dots, \mathsf{X}_n)$ is the Cartesian product of the alphabets of *subregisters* $\mathsf{X}_1, \dots, \mathsf{X}_n$,

$$\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_n.$$

Classical states. Once we have fixed this basic convention, we briefly describe *classical finite dimensional* systems. The following discussion can be seen as a reformulation of basic probability theory over finite sample spaces.

In consonance to previous paragraphs, we identify a classical finite dimensional system with a register X. The elements of the corresponding alphabet $\mathcal{X}$ represent the possible outcomes of an observation of the system. The result of an observation is described by a probability distribution describing the probability of obtaining each of the elements in $\mathcal{X}$ as result. We refer to this probability distribution as a *classical state* of the register X. More concretely,

Definition 1.8. *The classical state space associated to a register* X *is the set of probability measures over register's alphabet* $\mathcal{X}$*. We denote that set as* $\mathcal{P}(\mathcal{X})$*.*

Remark 1.9. Elements of $\mathcal{P}(\mathcal{X})$ are indeed positive functions

$$\begin{array}{cccc} p: & \mathcal{X} & \longrightarrow & [0,1] \\ & x & \mapsto & p(x) \end{array},$$

normalized such that $\sum_{x \in \mathcal{X}} p(x) = 1$. When linearly extended to a linear form

$$\begin{array}{cccc} p: & \mathbb{C}^{\mathcal{X}} & \longrightarrow & \mathbb{C} \\ & \sum_{x\in\mathcal{X}} \lambda_x |x\rangle & \mapsto & \sum_{x\in\mathcal{X}} \lambda_x \, p(x) \end{array},$$

it is positive and unital. That is, p can be understood as a *state* on the commutative C*-algebra $\ell_\infty^{\mathcal{X}}$.

Classical evolutions. The most general evolution that a (classical) state of a given register X can undergo is a map between probability vectors

$$\begin{array}{rccc} \mathcal{E}: & \mathbb{R}^{\mathcal{X}} & \longrightarrow & \mathbb{R}^{\mathcal{Y}} \\ & p & \mapsto & \mathcal{E}(p) \end{array},$$

satisfying the following consistency conditions:

i. Linearity. A convex combination of probability vectors $\lambda\, p+(1-\lambda)p'$, $\lambda \in [0,1]$ is another probability vector whose interpretation is as follows: with probability λ, the register is in the state p while, with probability $(1-\lambda)$, it is in the state p'. Therefore, after evolution $\mathcal{E}$, the state of the register is $\mathcal{E}(p)$ with probability λ and $\mathcal{E}(p')$ with probability $(1-\lambda)$. That is, the interpretation of classical states as probability distribution enforces that $\mathcal{E}(\lambda p + (1\lambda)p') = \lambda\mathcal{E}(p) + (1-\lambda)p'$ for any p, $p' \in \mathscr{P}(\mathcal{X})$, $\lambda \in [0,1]$.

ii. Positivity. For any $p \in \mathscr{P}(\mathcal{X})$, $\mathcal{E}(p)$ must be also positive.

iii. Measure preserving. For any $p \in \mathscr{P}(\mathcal{X})$, $\mathcal{E}(p)$ must be also well normalized.

Observations and post-selection. As noted at the beginning of this section, the description of classical systems that we have presented above is just a convenient reformulation of probability theory over discrete, finite probability spaces. Given a register X, the role of the sample space is played here by the alphabet $\mathcal{X}$: events related to the observation of X are just subsets of this alphabet. Finally, the probability measure in each case is determined by the state $p \in \mathscr{P}(\mathcal{X})$ of the register. We specify now the customary interpretation of such a probability measure.

Given an event $\mathcal{S} \subseteq \mathcal{X}$, the probability that $\mathcal{S}$ happens on an observation of the register $\mathcal{X}$ is given by $\sum_{x\in\mathcal{S}} p(x)$. Understanding p as a vector $(p(x))_{x\in\mathcal{X}} \in \mathbb{R}^{\mathcal{X}}$, we can express the previous probability in the following way:

$$\langle \chi_{\mathcal{S}}, p\rangle := \sum_{x\in\mathcal{X}} \chi_{\mathcal{S}}(x)\, p(x),$$

where

$$\chi_{\mathcal{S}}(x) = \begin{cases} 1 & \text{if } x \in \mathcal{S}, \\ 0 & \text{o.w.} \end{cases}$$

is the characteristic function associated to the event $\mathcal{S}$.

The last concept we discuss before passing to the quantum setting is the notion of *post-selection*. After an observation, the provided information update produces a change in the state describing X. The classical state describing the system is updated to the conditional probability distribution

$$p' \ : \ p'(x) := p(x|\mathcal{S}) = \chi_{\mathcal{S}}(x) \frac{p(x)}{\langle \chi_{\mathcal{S}}, p \rangle}.$$

As a final comment, we remark the prominent role played by $\chi_{\mathcal{S}}$ in the observation process. We further stress that we can associate to $\chi_{\mathcal{S}}$ the linear operator

$$\begin{array}{ccc} \ell_\infty^{\mathcal{X}} & \longrightarrow & \ell_\infty^{\mathcal{X}} \\ |x\rangle & \mapsto & \chi_{\mathcal{S}}(x)|x\rangle, \end{array} \tag{1.3}$$

that can be represented by the tensor $\hat{\chi}_{\mathcal{S}} = \sum_{x\in\mathcal{S}} |x\rangle\langle x| \in (\mathbb{C}^{\mathcal{X}})^\sharp \otimes \mathbb{C}^{\mathcal{X}}$. Notice that the previous operator is in fact an orthogonal projection. As commented in Remark 1.9, a classical state $p \in \mathscr{P}(\mathcal{X})$ can be regarded as a state in the C*-algebra $\ell_\infty^{\mathcal{X}}$, while $\ell_\infty^{\mathcal{X}}$ can be also understood as the subalgebra of diagonal matrices of $\mathcal{S}_\infty^{\mathcal{X}}$. By these means, p can be identified with a diagonal matrix $\hat{p} \in \mathcal{S}_\infty^d$. With this, we can rewrite the probability that $\mathcal{S}$ happens as:

$$\langle \hat{\chi}_{\mathcal{S}}, \hat{p} \rangle = \mathrm{Tr} \hat{\chi}_{\mathcal{S}}\, \hat{p}.$$

This remark puts the process of observing a classical system and its quantum analogue, that we describe later on, in similar grounds.

These notions complete the abstract description of a classical *finite dimensional* system: states, evolutions and observations. We stress that there is one more ingredient that was provided implicitly in the previous discussion, that is the way different systems are combined into a global one. This step, that might seem rather trivial in the classical case, is one of the crucial differences with the quantum description that we present next.

Quantum states. The quantum description of a system can be understood as a non-commutative extension of the classical case.

Definition 1.10. *The quantum state space, simply state space from now on, associated to a register* X *is the set of density operators on a complex* $|\mathcal{X}|$*-dimensional Hilbert space* $\mathcal{H}_{\mathcal{X}}$*. We denote that set as* $\mathscr{D}(\mathcal{H}_{\mathcal{X}})$*.*

Remark 1.11. In order to spot the parallelism with Definition 1.8, we note that elements in $\mathscr{D}(\mathcal{H}_{\mathcal{X}})$ are unital positive *operators*

$$\begin{array}{rccc} \rho: & \mathscr{L}(\mathcal{H}_{\mathcal{X}}) & \longrightarrow & \mathbb{C} \\ & A & \mapsto & \rho(A) := \mathrm{Tr}(A\,\rho) \end{array} .$$

That is, ρ is a state in the C*-algebra $\mathscr{B}(\mathcal{H}_{\mathcal{X}})$. Unitality is imposed by the proper normalization of ρ. One just has to notice that $\rho(\mathrm{Id}_{\mathcal{H}_{\mathcal{X}}}) = \mathrm{Tr}\rho$.

From this point of view, it is clear that the classical state space of a register X is included in its (quantum) state space. $\mathscr{P}(\mathcal{X})$ can be identified with the subset of *diagonal* operators of $\mathscr{D}(\mathcal{H}_{\mathcal{X}})$. From now on, we understand $\mathscr{P}(\mathcal{X})$ as this subset. In this sense, $\mathscr{D}(\mathcal{H}_{\mathcal{X}})$ is a more general description of X.

Concluding with the introduction of quantum states of X, we review the state space of composite systems. Recall that the alphabet of a composite register $(\mathsf{X}_1, \ldots, \mathsf{X}_n)$ is given by the Cartesian product $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$. Accordingly, the state space of such a composite system is the set of density operators on the *tensor product* of the individual Hilbert spaces, $\mathcal{H}_{\mathcal{X}_1} \otimes \cdots \otimes \mathcal{H}_{\mathcal{X}_n}$.

Quantum evolutions. The evolution of states is given again by a linear map between state spaces fulfilling some positivity and normalization conditions. More specifically,

Definition 1.12. *A quantum channel (or simply channel) is a completely positive and trace preserving linear map*

$$\mathcal{E} : \mathscr{L}(\mathcal{H}_{\mathcal{X}}) \to \mathscr{L}(\mathcal{H}_{\mathcal{Y}})$$

where $\mathcal{H}_{\mathcal{X}}$*,* $\mathcal{H}_{\mathcal{Y}}$ *are complex Hilbert spaces. We denote* $\mathrm{CPTP}(\mathcal{H}_{\mathcal{X}}, \mathcal{H}_{\mathcal{Y}})$ *the set of such channels, using the shortcut* $\mathrm{CPTP}(\mathcal{H}_{\mathcal{X}})$ *when input and output spaces are the same.*

Linearity can be again motivated by the fact that the convex combination of density matrices $\lambda\rho + (1-\lambda)\rho'$, $\lambda \in [0,1]$, is interpreted as the state in which we associate probability λ to the system being described by ρ and probability $1-\lambda$ to being described by ρ'. Complete positivity is enforced by the requirement that the image of a density operator must be again a density operator. But this has to happen not only under the action of $\mathcal{E}$, but also when $\mathcal{E}$ acts on a subregister (then the total evolution would be described by the tensor product of evolutions, $\mathcal{E}' \otimes \mathcal{E}$). Finally, trace preservation is the natural replacement to measure preservation in the classical case. It guarantees that the state after the evolution is still well normalized.

Example 1.13. The trace as a channel. The mapping

$$\begin{array}{rccc} \operatorname{Tr}: & \mathscr{L}(\mathcal{H}_{\mathcal{X}}) & \longrightarrow & \mathbb{C} \\ & T & \mapsto & \operatorname{Tr} T, \end{array}$$

as well as the partial trace $\operatorname{Tr}_{\mathcal{H}_{\mathcal{X}}} := \operatorname{Tr} \otimes \operatorname{Id}_{\mathcal{H}_{\mathcal{Y}}} : \mathscr{L}(\mathcal{H}_{\mathcal{X}} \otimes \mathcal{H}_{\mathcal{Y}}) \to \mathscr{L}(\mathcal{H}_{\mathcal{Y}})$ are channels. Tr is clearly positive and trace preserving (interpreting the trace on $\mathbb{C}$ simply as the trivial function $1 : \mathbb{C} \ni \lambda \mapsto \lambda \in \mathbb{C}$). Furthermore, positive maps with values in a commutative C*-algebra are also completely positive – recall Remark 1.6 –, hence $\operatorname{Tr} \in \operatorname{CPTP}(\mathcal{H}_{\mathcal{X}}, \mathbb{C})$. In addition, notice that the partial trace is nothing else than a matricial extension of Tr and therefore it is also completely positive. Trace preservation can be checked again by direct computation.

Example 1.14. The *completely dephasing* channel. Another map that naturally appears in the present context is:

$$\begin{array}{rccc} \Delta: & \mathscr{L}(\mathcal{H}_{\mathcal{X}}) & \longrightarrow & \mathscr{L}(\mathcal{H}_{\mathcal{X}}) \\ & T & \mapsto & \sum_k \langle k|T|k\rangle \, |k\rangle\langle k|, \end{array}$$

known as the completely dephasing channel. Notice that this map is the orthogonal projection on the subalgebra of $\mathscr{L}(\mathcal{H}_{\mathcal{X}})$ of diagonal matrices. This allows us to see Δ as a map taking values on the commutative C*-algebra $\ell_\infty^{\mathcal{X}}$, and therefore, again Δ is completely positive iff it is just positive – cf. Remark 1.6. But Δ is clearly positive, hence it is also completely positive. Trace preservation also follows straightforwardly, so Δ is a channel, $\Delta \in \operatorname{CPTP}(\mathcal{H}_{\mathcal{X}})$.

The completely dephasing channel Δ plays an important role in our presentation of quantum observations. This is the next topic we introduce.

Quantum observations. Analogously to the situation depicted in the classical description of X, the state of the register represents the information about X that is available to the observer. Now, the acquisition of that information from the system is more subtle. For us, the measurement process merely consists on the extraction of *classical* information about the system, formalizing this process as follows.

The idea is reducing this process to the observation of classical systems, that was already introduced before. First, we introduce the notion of *quantum-to-classical* channels. These are particular channels, $\mathcal{E} \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{X}}, \mathcal{H}_{\mathcal{Y}})$, verifying that $\mathcal{E}(\mathscr{D}(\mathcal{H}_{\mathcal{X}})) \subseteq \mathscr{P}(\mathcal{Y})$, where $\mathscr{P}(\mathcal{Y})$ is regarded as a subalgebra of $\mathcal{S}_{\infty}^{\mathcal{Y}}$. That is, quantum channels whose output is a classical state. Δ is a prominent example of such a channel. More explicitly, we can define quantum-to-classical channels as CPTP maps with the following structure:

$$\begin{array}{rccc} \mathcal{E}: & \mathscr{L}(\mathcal{H}_{\mathcal{X}}) & \longrightarrow & \mathscr{L}(\mathcal{H}_{\mathcal{Y}}) \\ & \rho & \mapsto & \mathcal{E}(\rho) = \sum_{i \in \mathcal{Y}} \mathcal{E}_i(\rho) \, |i\rangle\langle i| \end{array},$$

where $\mathcal{E}_i \in \mathscr{L}(\mathcal{X}, \mathbb{C})$ for any $i \in \mathcal{I}$. The subset of such channels is denoted here by $\mathrm{CPTP}_{qc}(\mathcal{H}_{\mathcal{X}}, \mathcal{H}_{\mathcal{Y}})$.

We again distinguish between observations and post-selection.

Observation: it consists of a quantum-to-classical evolution followed by an observation of the resulting classical state.

First, we can think of the system evolving according to a quantum-to-classical channel

$$\mathcal{E} : \mathscr{L}(\mathcal{H}_{\mathcal{X}}) \longrightarrow \mathscr{L}(\mathcal{Y}).$$

After that, the observation of register Y follows in the same way as in the classical case. The probability of obtaining a result associated to an event $\mathcal{S} \subseteq \mathcal{Y}$ is:

$$\langle \hat{\chi}_{\mathcal{S}}, \mathcal{E}(\rho) \rangle = \mathrm{Tr}(\hat{\chi}_{\mathcal{S}} \, \mathcal{E}(\rho)) = \langle \mathcal{E}^*(\hat{\chi}_{\mathcal{S}}), \rho \rangle,$$

where $\hat{\chi}_{\mathcal{S}}$ was defined in Equation (1.3).

Furthermore, given a partition of $\mathcal{Y}$, $\{\mathcal{S}_i\}_{i\in\mathcal{I}} \subseteq \mathcal{Y}$, and a quantum-to-classical channel as above, $\mathcal{E} \in \mathrm{CPTP}_{qc}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y})$, $\mathcal{E}^*(\hat{\chi}_{\mathcal{S}_i})$ is a positive operator on $\mathcal{H}_\mathcal{X}$ for each $i \in \mathcal{I}$ and $\sum_{i\in\mathcal{I}} \mathcal{E}^*(\hat{\chi}_{\mathcal{S}_i}) = \mathcal{E}^*\Big(\sum_{i\in\mathcal{I}} \hat{\chi}_{\mathcal{S}_i}\Big) = \mathcal{E}^*(\mathrm{Id}_{\mathcal{H}_\mathcal{Y}}) = \mathrm{Id}_{\mathcal{H}_\mathcal{X}}$. A family of positive operators with this property is called a positive operator-valued measure (POVM).

Definition 1.15. *A POVM on a register* X *is a family of positive operators* $\{E_i\}_{i\in\mathcal{I}} \subseteq \mathscr{L}(\mathcal{H}_\mathcal{X})$ *summing to the identity on* $\mathcal{H}_\mathcal{X}$*, i.e.,* $\sum_{i\in\mathcal{I}} E_i = \mathrm{Id}_{\mathcal{H}_\mathcal{X}}$. *We denote* $\mathrm{POVM}(\mathcal{H}_\mathcal{X})$ *the set of POVMs on* X.

Remark 1.16. Any POVM can be understood as in the discussion above.

Proof. We have already proven one direction: a quantum-to-classical channel $\mathcal{E} \in \mathrm{CPTP}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y})$ together with a partition of $\mathcal{Y}$, $\{\mathcal{S}_i\}_{i\in\mathcal{I}}$, define a POVM $\{\mathcal{E}^*(\hat{\chi}_{\mathcal{S}_i})\}_{i\in\mathcal{I}}$.

For the other direction we start with a family of positive operators on $\mathcal{H}_\mathcal{X}$, $\{E_i\}_{i\in\mathcal{I}}$, summing up to the identity, $\sum_{i\in\mathcal{I}} E_i = \mathrm{Id}_{\mathcal{H}_\mathcal{X}}$. Now we show the existence of a quantum-to-classical channel $\mathcal{E} \in \mathrm{CPTP}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{I})$ and a partition $\{\mathcal{S}_i\}_{i\in\mathcal{I}}$ of $\mathcal{H}_\mathcal{I}$ such that $E_i = \mathcal{E}^*(\chi_{\mathcal{S}_i})$.

We first fix the partition with the naïve choice $\mathcal{S}_i = \{i\}$. Therefore, $\chi_{\mathcal{S}_i} = |i\rangle\langle i|$. Next, we construct $\mathcal{E}^* \in \mathrm{CPTP}(\mathcal{H}_\mathcal{I}, \mathcal{H}_\mathcal{X})$ according to the prescription $\mathcal{E}^*(|i\rangle\langle j|) = \delta_{i,j} E_i$ for any $i, j \in \mathcal{I}$. Next we show that $\mathcal{E}^*$ is completely positive and unital, hence $\mathcal{E}$ is in fact a channel. The fact that $\mathcal{E}^*$ is positive follows directly from the fact that the operators E_i are positive by construction. Furthermore, to see that $\mathcal{E}^*$ is completely positive we realize that it is the composition of two completely positive operators:

$$\begin{tikzcd}
\mathscr{L}(\mathcal{H}_\mathcal{Y}) \arrow[r, "\mathcal{E}^*"] \arrow[d, "\Delta"'] & \mathscr{L}(\mathcal{H}_\mathcal{X}) \\
\mathscr{P}(\mathcal{Y}) \arrow[ur, "\tilde{\mathcal{E}}^*"'] &
\end{tikzcd},$$

where Δ is the completely dephasing channel introduced previously, and $\tilde{\mathcal{E}}^*$ is defined by $\tilde{\mathcal{E}}^*(|i\rangle\langle i|) = E_i$. Δ is completely positive (it is indeed a channel) and $\tilde{\mathcal{E}}^*$ is also completely positive since it is a positive operator acting on the commutative C*-algebra $\ell_\infty^\mathcal{I}$. Finally, since $\sum_{i\in\mathcal{I}} E_i = \mathrm{Id}_{\mathcal{H}_\mathcal{X}}$, $\mathcal{E}^*$ it is clearly unital. □

Post-selection: the state after an observation must be again updated according to the revealed information. In the case described before, in which the system undergoes a quantum-to-classical evolution $\mathcal{E}$ prior to the observation, the classical state resulting from this evolution is updated as described in previous sections: the updated state is the corresponding conditional probability distribution. In order to describe the most general situation, we complement the process depicted before with the possibility that the channel $\mathcal{E}$ additionally outputs a register in a general quantum state. We define *quantum-to-classical-quantum* channels as CPTP maps with a bipartite output register (Y, Z) such that:

$$\begin{array}{rccc} \mathcal{E}: & \mathscr{L}(\mathcal{H}_{\mathcal{X}}) & \longrightarrow & \mathscr{L}(\mathcal{H}_{\mathcal{Y}} \otimes \mathcal{H}_{\mathcal{Z}}) \\ & \rho & \mapsto & \mathcal{E}(\rho) = \sum_{i \in \mathcal{Y}} |i\rangle\langle i| \otimes \mathcal{E}_i(\rho) \end{array},$$

where now $\mathcal{E}_i \in \mathrm{CP}(\mathcal{H}_{\mathcal{X}}, \mathcal{H}_{\mathcal{Z}})$ for each $i \in \mathcal{I}$. We denote the set of this channels as $\mathrm{CPTP}_{qcq}(\mathcal{H}_{\mathcal{X}}, \mathcal{H}_{\mathcal{Y}} \otimes \mathcal{H}_{\mathcal{Z}})$.

According to our previous discussion, a measurement consists on the observation of the *classical* register Y. The probability of occurrence of an event $\mathcal{S} \subseteq \mathcal{Y}$ is given by:

$$\langle \hat{\chi}_{\mathcal{S}}, \mathrm{Tr}_{\mathcal{H}_{\mathcal{Z}}} \circ \mathcal{E}(\rho) \rangle = \langle (\mathrm{Tr}_{\mathcal{Z}} \circ \mathcal{E})^*(\hat{\chi}_{\mathcal{S}}), \rho \rangle,$$

where $(\mathrm{Tr}_{\mathcal{Z}} \circ \mathcal{E})^*(\hat{\chi}_{\mathcal{S}}) = \mathcal{E}^*(\hat{\chi}_{\mathcal{S}} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}})$.

Provided that the event $\mathcal{S} \subseteq \mathcal{Y}$ have occurred, the state of the system is updated taking into account this information. Denoting here $\chi_{\mathcal{S}_i} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}}(\,\cdot\,) = (\hat{\chi}_{\mathcal{S}_i} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}})\,(\,\cdot\,)\,(\hat{\chi}_{\mathcal{S}_i} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}})$, where the action in the RHS is given simply by matrix multiplication, the updated state is described by:

$$\rho' = \frac{\chi_{\mathcal{S}} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}}(\mathcal{E}(\rho))}{\langle \mathcal{E}^*(\hat{\chi}_{\mathcal{S}} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}}), \rho \rangle}.$$

Given a partition of $\mathcal{Y}$, $\{\mathcal{S}_i\}_{i \in \mathcal{I}}$, we have a family of completely positive maps $\{\mathcal{E}_i := \mathrm{Tr}_{\mathcal{H}_{\mathcal{Y}}} \circ \chi_{\mathcal{S}_i} \otimes \mathrm{Id}_{\mathcal{H}_{\mathcal{Z}}} \circ \mathcal{E}\}_{i \in \mathcal{I}}$ whose sum is a trace preserving map, i.e., a channel. Any family of completely positive maps with this property is called an *instrument*.

Definition 1.17. *An instrument on a register* X *is a family of completely positive maps* $\{\mathcal{E}_i\}_{i \in \mathcal{I}} \subseteq \mathrm{CP}(\mathcal{H}_{\mathcal{X}}, \mathcal{H}_{\mathcal{Z}})$ *summing to a channel* $\sum_{i \in \mathcal{I}} \mathcal{E}_i \in$

$\mathrm{CPTP}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Z})$. *We denote the set of instruments on a register* X *with output register* Z *by* $\mathrm{Ins}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Z})$.

Remark 1.18. Any instrument can be understood as in the discussion above.

Proof. As in the case of Remark 1.16, we have already proven one direction: any $\mathcal{E} \in \mathrm{CPTP}_{qcq}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z})$ together with a partition of $\mathcal{Y}$, $\{\mathcal{S}_i\}_{i\in\mathcal{I}}$, defines an instrument $\{\mathcal{E}_i = \mathrm{Tr}_{\mathcal{H}_\mathcal{Y}} \circ \chi_{\mathcal{S}_i} \otimes \mathrm{Id}_{\mathcal{H}_\mathcal{Z}} \circ \mathcal{E}\}_{i\in\mathcal{I}} \in \mathrm{Ins}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Z})$.

Conversely, given an instrument $\{\mathcal{E}_i\}_{i\in\mathcal{I}} \in \mathrm{Ins}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Z})$, consider:

- the quantum-to-classical-quantum channel $\mathcal{E} \in \mathrm{CPTP}_{qcq}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{I} \otimes \mathcal{H}_\mathcal{Z})$ defined by:
$$\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{I}} |i\rangle\langle i| \otimes \mathcal{E}_i(\,\cdot\,).$$
$\mathcal{E}$ is completely positive since it is a the sum of the completely positive maps: $\cdot \mapsto |i\rangle\langle i| \otimes \mathcal{E}_i(\,\cdot\,)$. Furthermore, it is trace preserving since $\sum_{i\in\mathcal{I}} \mathcal{E}_i(\,\cdot\,)$ is trace preserving by hypothesis.

- The partition $\{i\}_{i\in\mathcal{I}}$ of the alphabet $\mathcal{I}$.

Then, it is easy to check that $\mathrm{Tr}_{\mathcal{H}_\mathcal{I}} \circ \chi_{\{i\}} \otimes \mathrm{Id}_{\mathcal{H}_\mathcal{Z}} \circ \mathcal{E} = \mathcal{E}_i$. □

1.2.2 Some results about quantum states, channels and measurements

Most proofs appearing in this section are adaptations of the ideas presented in [124].

Distinguishability. In quantum information theory, one usually encounters some notions of closeness between states and channels. In the case of states, a natural distance is based on the trace norm on $\mathscr{L}(\mathcal{H})$:

Definition 1.19. *The trace distance between two states* ρ, $\sigma \in \mathscr{D}(\mathcal{H})$ *is defined by* $D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_{\mathcal{S}_1(\mathcal{H})}$.

The trace distance is intimately related with the task of state discrimination. In the latter, a register X is randomly prepared in one out of two possible states, ρ, $\sigma \in \mathscr{D}(\mathcal{H}_{\mathcal{X}})$, each with probability $\frac{1}{2}$. Based on an observation of that register, we want to determine in which state X was actually prepared. The optimal success probability on this task is elegantly determined by the trace distance $D(\rho, \sigma)$. This is the content of the Holevo-Helstrom theorem we state next:

Theorem 1.20 (Holevo-Helstrom)**.** *Let ρ, $\sigma \in \mathscr{D}(\mathcal{H})$. Then,*

$$p^*_{dis}(\rho, \sigma) = \frac{1}{2} + \frac{1}{2} D(\rho, \sigma)$$

is the optimal probability of distinguishing between states ρ and σ when a single instance of one of them is provided with probability $\frac{1}{2}$ each.

Proof. We make first some initial remarks:

- The most general action to discriminate between ρ and σ is characterized by a POVM on $\mathcal{H}$, $\mathbf{E} = \{E_\rho, E_\sigma\}$. When the outcome of the measurement is the one associated to E_ρ, we guess that the actual state of the system was ρ. Similarly for E_σ and the state σ.

- Given $\mathbf{E} = \{E_\rho, E_\sigma\} \in \mathrm{POVM}(\mathcal{H})$, the probability of successfully discriminate between ρ and σ when the system is prepared in each one of these states with probability 1/2 is:

  $$p^{\mathbf{E}}_{dist}(\rho, \sigma) = \frac{1}{2} \mathrm{Tr} E_\rho \, \rho + \frac{1}{2} \mathrm{Tr} E_\sigma \, \sigma.$$

  The corresponding error probability is:

  $$p^{\mathbf{E}}_{err}(\rho, \sigma) = \frac{1}{2} \mathrm{Tr} E_\rho \, \sigma + \frac{1}{2} \mathrm{Tr} E_\sigma \, \rho.$$

- Since $p^{\mathbf{E}}_{err}(\rho,\sigma) = 1 - p^{\mathbf{E}}_{dist}(\rho,\sigma)$ we can write:

$$\begin{aligned} p^{\mathbf{E}}_{dist}(\rho,\sigma) &= \frac{1}{2} + \frac{1}{2}(p^{\mathbf{E}}_{dist}(\rho,\sigma) - p^{\mathbf{E}}_{err}(\rho,\sigma)) \\ &= \frac{1}{2} + \frac{1}{2}\Big(\operatorname{Tr}\left(E_\rho - E_\sigma\right)\frac{1}{2}(\rho-\sigma)\Big) \\ &= \frac{1}{2} + \frac{1}{2}\Big\langle E_\rho - E_\sigma,\, \frac{\rho-\sigma}{2}\Big\rangle. \end{aligned}$$

Therefore, we have the following expression for the optimal probability of distinguishing ρ and σ:

$$p^{*}_{dist}(\rho,\sigma) = \frac{1}{2} + \frac{1}{2}\sup_{\mathbf{E}=\{E_\rho,E_\sigma\}\in \mathrm{POVM}(\mathcal{H})} \Big\langle E_\rho - E_\sigma,\, \frac{\rho-\sigma}{2}\Big\rangle.$$

We note that for any POVM $\mathbf{E}=\{E_\rho,E_\sigma\}$, $E_\rho - E_\sigma = 2E_\rho - \mathrm{Id}_{\mathcal{H}}$. In particular, $\|E_\rho - E_\sigma\|_{\mathscr{B}(\mathcal{H})} \leq 1$. That is,

$$p^{*}_{dist}(\rho,\sigma) \leq \frac{1}{2} + \frac{1}{2}\sup_{E\in \mathsf{ball}(\mathscr{B}(\mathcal{H}))} \Big\langle E,\, \frac{\rho-\sigma}{2}\Big\rangle = \frac{1}{2} + \frac{1}{2}\Big\|\frac{\rho-\sigma}{2}\Big\|_{\mathcal{S}_1(\mathcal{H})}.$$

Furthermore, taking into account the spectral decomposition $\frac{\rho-\sigma}{2} = \sum_k \lambda_k \left|\psi_k\right\rangle\!\left\langle\psi_k\right|$, where the singular values λ_k are real, we can write the trace norm of this operator as follows:

$$\Big\|\frac{\rho-\sigma}{2}\Big\|_{\mathcal{S}_1(\mathcal{H})} = \sum_k |\lambda_k| = \Big\langle \mathrm{P}_+ - \mathrm{P}_-,\, \frac{\rho-\sigma}{2}\Big\rangle.$$

Here, P_+, P_- are the orthogonal projections on the eigenspaces associated to positive and negative singular values, respectively. Notice that these projections indeed define a projective measurement $\{\mathrm{P}_+,\mathrm{P}_-\}$. Hence:

$$\frac{1}{2} + \frac{1}{2}\Big\|\frac{\rho-\sigma}{2}\Big\|_{\mathcal{S}_1(\mathcal{H})} \leq p^{*}_{dist}(\rho,\sigma).$$

According to the definition of $D(\rho,\sigma)$, this concludes the proof. □

We can extend the previous discussion to the case of channels instead of states. In this case, the natural notion for distance is provided by the *diamond distance*. We first define the *diamond norm* of an operator $\mathcal{E} : \mathscr{L}(\mathcal{H}) \to \mathscr{L}(\mathcal{K})$ as:

$$\|\mathcal{E}\|_\diamond = \sup_{\substack{\mathcal{K}', \\ T \in \mathsf{ball}(\mathcal{S}_1(\mathcal{H}\otimes\mathcal{K}'))}} \|\mathcal{E} \otimes \mathrm{Id}_{\mathcal{K}'}(T)\|_{\mathcal{S}_1(\mathcal{K}\otimes\mathcal{K}')},$$

where $\mathcal{K}'$ is an arbitrary finite dimensional Hilbert space.

Definition 1.21. *The diamond distance between two channels $\mathcal{E}$, $\mathcal{R} \in$ CPTP$(\mathcal{H},\mathcal{K})$ is defined by $D_\diamond(\mathcal{E},\mathcal{R}) := \frac{1}{2}\|\mathcal{E}-\mathcal{R}\|_\diamond$.*

This distance is again perfectly motivated by a discrimination task. In the task of channel discrimination, we are provided with a black box that implements channels $\mathcal{E}$, $\mathcal{R}$, each with probability 1/2. After a single application of the black box, we are required to determine which channel was actually implemented. The optimal probability of succeeding at this task is characterized by the diamond distance $D_\diamond(\mathcal{E},\mathcal{R})$:

Theorem 1.22. *Let $\mathcal{E}$, $\mathcal{R} \in$ CPTP$(\mathcal{H},\mathcal{K})$. Then,*

$$p^*_{dist}(\mathcal{E},\mathcal{R}) = \frac{1}{2} + \frac{1}{2} D_\diamond(\mathcal{E},\mathcal{R}),$$

is the optimal probability of distinguishing between channels $\mathcal{E}$ and $\mathcal{R}$ when a single instance of one of them is provided with probability 1/2 each.

In the proof of this theorem we will make use of the following lemma:

Lemma 1.23. *For Hermitian preserving linear maps $\mathcal{E} : \mathscr{L}(\mathcal{H}) \to \mathscr{L}(\mathcal{K})$,*

$$\|\mathcal{E}\|_\diamond = \sup_{\substack{\mathcal{K}', \\ \rho \in \mathscr{D}(\mathcal{H}\otimes\mathcal{K}')}} \|\mathcal{E} \otimes \mathrm{Id}_{\mathcal{K}'}(\rho)\|_{\mathcal{S}_1(\mathcal{K}\otimes\mathcal{K}')}.$$

Furthermore, the state ρ in the supremum can be restricted to be pure.

Proof. It is clear that

$$\|\mathcal{E}\|_\diamond \geq \sup_{\substack{\mathcal{K}', \\ \rho \in \mathscr{D}(\mathcal{H}\otimes\mathcal{K}')}} \|\mathcal{E} \otimes \mathrm{Id}_{\mathcal{K}'}(\rho)\|_{\mathcal{S}_1(\mathcal{K}\otimes\mathcal{K}')},$$

so we focus on the converse inequality. For any $\mathcal{K}'$ and T in the unit ball of $\mathcal{S}_1(\mathcal{H}\otimes\mathcal{K}')$, we consider the hermitian element

$$\tilde{T} := T\otimes|0\rangle\langle 1| + T^{\dagger}\otimes|1\rangle\langle 0| \in \mathcal{S}_1(\mathcal{H}\otimes\tilde{\mathcal{K}}').$$

where $\tilde{\mathcal{K}}' = \mathcal{K}'\otimes\ell_2^2$. The norm of this element is bounded by the norm of T: $\|\tilde{T}\|_{\mathcal{S}_1(\mathcal{H}\otimes\tilde{\mathcal{K}}')} = \|T\|_{\mathcal{S}_1(\mathcal{H}\otimes\mathcal{K}')} \leq 1$.

With the previous definition, and taking into account that $\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}$ is Hermitian preserving,

$$\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(\tilde{T}) = \mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}}(T)\otimes|0\rangle\langle 1| + (\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}}(T))^{\dagger}\otimes|1\rangle\langle 0|,$$

from where it is easy to deduce that

$$\|\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(\tilde{T})\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')} = \|\mathcal{E}\otimes\mathrm{Id}_{\mathcal{K}'}(T)\|_{\mathcal{S}_1(\mathcal{K}\otimes\mathcal{K}')}.$$

Now, since $\tilde{T}$ is hermitian, we can consider its spectral decomposition $\tilde{T} = \sum_k \lambda_k|\xi_k\rangle\langle\xi_k|$, that allows us to bound the previous norm as:

$$\|\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(\tilde{T})\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')} \leq \sum_k |\lambda_k| \|\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(|\xi_k\rangle\langle\xi_k|)\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')}.$$

Furthermore, since $\|\tilde{T}\|_{\mathscr{B}(\mathcal{H}\otimes\tilde{\mathcal{K}}')} = \sum_k|\lambda_k| \leq 1$, it must hold that

$$\begin{aligned}\|\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(\tilde{T})\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')} &= \|\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(\tilde{T})\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')}\\ &\leq \|\mathcal{E}\otimes\mathrm{Id}_{\tilde{\mathcal{K}}'}(|\xi\rangle\langle\xi|)\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')}.\end{aligned}$$

for some $|\xi\rangle \in \{|\xi_k\rangle\}_k$. Therefore, we finally obtain that:

$$\begin{aligned}\|\mathcal{E}\|_{\diamond} &= \sup_{\substack{\mathcal{K}',\\ T\in\mathsf{ball}(\mathcal{S}_1(\mathcal{H}\otimes\mathcal{K}'))}} \|\mathcal{E}\otimes\mathrm{Id}_{\mathcal{K}'}(T)\|_{\mathcal{S}_1(\mathcal{K}\otimes\mathcal{K}')}\\ &\leq \sup_{\substack{\mathcal{K}',\\ |\xi\rangle\in\mathcal{H}\otimes\tilde{\mathcal{K}}'}} \|\mathcal{E}\otimes\mathrm{Id}_{\mathcal{K}'}(|\xi\rangle\langle\xi|)\|_{\mathcal{S}_1(\mathcal{K}\otimes\tilde{\mathcal{K}}')}\\ &= \sup_{\substack{\mathcal{K}',\\ |\xi\rangle\in\mathcal{H}\otimes\mathcal{K}'}} \|\mathcal{E}\otimes\mathrm{Id}_{\mathcal{K}'}(|\xi\rangle\langle\xi|)\|_{\mathcal{S}_1(\mathcal{K}\otimes\mathcal{K}')},\end{aligned}$$

that is the desired inequality.

□

Proof of Theorem 1.22. The theorem can be understood as a consequence of the Holevo-Helstrom theorem, Theorem 1.20. For that, we have to note that the most general way to discriminate between channels $\mathcal{E}$ and $\mathcal{R}$ –recall the previous discussion for the specification of the discrimination task– is acting with the black box in part of a bigger system with underlying Hilbert space $\mathcal{H} \otimes \mathcal{K}'$ when the system is prepared in a state $\rho \in \mathscr{D}(\mathcal{H} \otimes \mathcal{K}')$ of our choice. That is, $p^*_{dist}(\mathcal{E}, \mathcal{R})$ is the supremum over finite dimensional Hilbert spaces $\mathcal{K}'$ and states $\rho \in \mathscr{D}(\mathcal{H} \otimes \mathcal{K}')$ of the optimal probability of distinguishing the states $\mathcal{E} \otimes \mathrm{Id}_{\mathcal{K}'}(\rho)$ and $\mathcal{R} \otimes \mathrm{Id}_{\mathcal{K}'}(\rho)$. Therefore, according to the previous Holevo-Helstrom theorem:

$$p^*_{dist}(\mathcal{E}, \mathcal{R}) = \frac{1}{2} + \frac{1}{2} \sup_{\substack{\mathcal{K}',\\ \rho \in \mathscr{D}(\mathcal{H} \otimes \mathcal{K}')}} \left\| \frac{1}{2} (\mathcal{E} - \mathcal{R}) \otimes \mathrm{Id}_{\mathcal{K}'}(\rho) \right\|_{\mathcal{S}_1(\mathcal{K} \otimes \mathcal{K}')}.$$

Finally, since the operator $\mathcal{E} - \mathcal{R}$ is Hermitian preserving, the statement in the theorem is obtained thanks to Lemma 1.23. □

Dilation theorems. The main contents of this section are the standard purification results of quantum states and channels, that allow us to understand any quantum state (channel) as part of a *pure* state (unitary channel) in a bigger system. We start with the simpler case of states.

Definition 1.24. *A state $\rho \in \mathscr{D}(\mathcal{H})$ is pure if it is a rank-one projection. Therefore, pure states are of the form $\rho = |\psi\rangle\langle\psi|$ for a unit vector $|\psi\rangle \in \mathcal{H}$.*

Theorem 1.25. *For any positive semi-definite operator $\rho \in \mathscr{L}(\mathcal{H})$ there exist a Hilbert space $\mathcal{K}$ and a vector $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ with norm $\||\psi\rangle\|_{\mathcal{H}\otimes\mathcal{K}} = \mathrm{Tr}\rho$ such that*

$$\rho = \mathrm{Tr}_{\mathcal{K}} |\psi\rangle\langle\psi|.$$

Furthermore, the dimension of $\mathcal{K}$ can be taken equal to $\mathrm{rank}(\rho)$.

Proof. We just have to consider the spectral decomposition of ρ. Since it is a positive semi-definite operator, its spectral decomposition can be written as

$$\rho = \sum_{i=1}^{\mathrm{rank}(\rho)} \lambda_i |\psi_i\rangle\langle\psi_i|,$$

where $\lambda_i \geq 0$ for any i and $\{|\psi_i\rangle\}_i$ is an orthonormal system in $\mathcal{H}$. To finish, consider a Hilbert space $\mathcal{K}$ of dimension rank(ρ) and construct the unit vector:

$$|\psi\rangle = \sum_{i=1}^{\mathrm{rank}(\rho)} \sqrt{\lambda_i}|\psi_i\rangle_{\mathcal{H}} \otimes |i\rangle_{\mathcal{K}}.$$

It is now a straightforward calculation to check that

$$\rho = \mathrm{Tr}_{\mathcal{K}}|\psi\rangle\langle\psi|.$$

□

The previous purification is not unique, there exist different vectors $|\psi\rangle$ purifying a given density operator ρ. However, all these purifications are related:

Theorem 1.26. *Given two vectors $|\psi\rangle, |\psi'\rangle$ in a composite Hilbert space $\mathcal{H} \otimes \mathcal{K}$, they verify*

$$\mathrm{Tr}_{\mathcal{K}}|\psi\rangle\langle\psi| = \rho = \mathrm{Tr}_{\mathcal{K}}|\psi'\rangle\langle\psi'|,$$

if and only if there exist a unitary operator $U \in \mathcal{U}(\mathcal{K})$ such that $|\psi'\rangle = \mathrm{Id}_{\mathcal{H}} \otimes U|\psi\rangle$.

Proof. Consider a Schmidt decomposition for $|\psi\rangle = \sum_i \lambda_i \, |\xi_i\rangle_{\mathcal{H}} \otimes |\phi_i\rangle_{\mathcal{K}}$ where $\{|\xi\rangle\}_i$, $\{|\phi_i\rangle\}_i$ are orthonormal systems in $\mathcal{H}$, $\mathcal{K}$, respectively, and every λ_i is different from zero. Let us expand the previous systems to orthonormal bases in $\mathcal{H}$, $\mathcal{K}$ that we denote again $\{|\xi\rangle\}_i$, $\{|\phi_i\rangle\}_i$ in the rest of the proof. We rewrite $|\psi\rangle = \sum_{i,j} \lambda_{i,j} \, |\xi_i\rangle_{\mathcal{H}} \otimes |\phi_j\rangle_{\mathcal{K}}$ where $\lambda_{ij} = 0$ whenever $j \neq i$. Consider next the expression of $|\psi'\rangle$ in the basis $\{|\xi_i\rangle \otimes |\phi_j\rangle\}_{i,j}$:

$$|\psi'\rangle = \sum_{i,j} \lambda'_{ij} \, |\xi_i\rangle_{\mathcal{H}} \otimes |\phi_j\rangle_{\mathcal{K}}.$$

Defining $|\phi_i'\rangle := \sum_j \frac{\lambda_{ij}'}{\lambda_{ii}}|\phi_j\rangle$ for $i = 1, \dots, \dim(\mathcal{H})$ we can rewrite:

$$|\psi'\rangle = \sum_i \lambda_{ii}|\xi_i\rangle_{\mathcal{H}} \otimes |\phi_i'\rangle_{\mathcal{K}}.$$

The condition $\mathrm{Tr}_{\mathcal{K}}|\psi\rangle\langle\psi| = \mathrm{Tr}_{\mathcal{K}}|\psi'\rangle\langle\psi'|$ now implies that:

$$\sum_i |\lambda_i|^2 |\xi_i\rangle\langle\xi_i| = \sum_{i,k} \lambda_{ii}\overline{\lambda_{kk}}\langle\phi_k'|\phi_i'\rangle\, |\xi_i\rangle\langle\xi_k|.$$

But from this condition follows that $\{|\phi_i'\rangle\}_i$ is in fact an orthonormal system in $\mathcal{K}$. Expand again this orthonormal system to a basis of $\mathcal{K}$ referred also as $\{|\phi_i'\rangle\}_i$ (where now there are more elements in this set than before). Now, notice that there exists a unique unitary $U \in \mathcal{U}(\mathcal{K})$ such that $|\phi_i'\rangle = U|\phi_i\rangle$ for all $i = 1, \dots, \dim(\mathcal{H})$. This is enough to conclude one direction of the statement of the theorem. The other direction follows from a straightforward calculation. □

Next, we move to the description of channels presenting three standard representations of these objects. First we introduce an identification of channels with states that is known as the Choi-Jamiołkowski isomorphism, denoted here as $J(\,\cdot\,)$.

Definition 1.27. *Given finite dimensional Hilbert spaces $\mathcal{H}$, $\mathcal{K}$, for any map $\mathcal{E} : \mathscr{L}(\mathcal{H}) \to \mathscr{L}(\mathcal{K})$*

$$J(\mathcal{E}) := \sum_{i,j=1}^{\dim(\mathcal{H})} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j| \in \mathscr{L}(\mathcal{K} \otimes \mathcal{H}),$$

is the Choi representation of $\mathcal{E}$.

Remark 1.28. J is a linear and invertible mapping. The inverse map J^{-1} is determined by the following relation

$$\mathcal{E}(\,\cdot\,) = \mathrm{Tr}_{\mathcal{H}}\, J(\mathcal{E})\,(\mathrm{Id}_{\mathcal{K}} \otimes \,\cdot\,^t),$$

where ^{t} denotes the transpose.

With that we can state the following theorem that subsumes the most standard representations of a quantum channel.

Theorem 1.29. *Given finite dimensional Hilbert spaces $\mathcal{H}$, $\mathcal{K}$ and an arbitrary linear map $\mathcal{E} : \mathscr{L}(\mathcal{H}) \to \mathscr{L}(\mathcal{K})$, the following statements are equivalent:*

1. $\mathcal{E} \in \mathrm{CPTP}(\mathcal{H}, \mathcal{K})$;
2. *(Choi's representation) $J(\mathcal{E})$ is a positive operator in $\mathscr{L}(\mathcal{H} \otimes \mathcal{K})$ and $\mathrm{Tr}_{\mathcal{K}} J(\mathcal{E}) = \mathrm{Id}_{\mathcal{H}}$.*
3. *(Kraus' representation) there exists an alphabet $\mathcal{A}$ and a collection of operators $\{A_a\}_{a\in\mathcal{A}} \subset \mathscr{L}(\mathcal{H}, \mathcal{K})$ such that*
$$\mathcal{E}(\,\cdot\,) = \sum_{a\in\mathcal{A}} A_a(\,\cdot\,)A_a^\dagger$$
and $\sum_{a\in\mathcal{A}} A_a^\dagger A_a = \mathrm{Id}_{\mathcal{H}}$. Furthermore, $\mathcal{A}$ can be taken with cardinal $\mathrm{rank}(J(\mathcal{E}))$;
4. *(Stinespring's representation) there exist a Hilbert space $\mathcal{K}'$ and an isometry $A \in \mathscr{L}(\mathcal{H}, \mathcal{K} \otimes \mathcal{K}')$ such that*
$$\mathcal{E}(\,\cdot\,) = \mathrm{Tr}_{\mathcal{K}'} A(\,\cdot\,)A^\dagger.$$
Furthermore, $\mathcal{K}'$ can be taken $\mathrm{rank}(J(\mathcal{E}))$–dimensional.

Proof. We follow the natural order (1.) ⇒ (2.) ⇒ (3.) ⇒ (4.) ⇒ (1.) in the following proof.

- *(1.) ⇒ (2.) :*

The complete positivity of $\mathcal{E}$ straightforwardly implies the positivity of $J(\mathcal{E})$. One only needs to realize that $J(\mathcal{E})$ is the image of the positive element $\sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j|$ by the positive map $\mathcal{E} \otimes \mathrm{Id}_{\mathcal{H}}$. Furthermore, since $\mathcal{E}$ is trace preserving, $\mathrm{Tr}\,\mathcal{E}(|i\rangle\langle j|) = \delta_{ij}$ and therefore:

$$\mathrm{Tr}_{\mathcal{K}} J(\mathcal{E}) = \sum_{i,j=1}^{\dim(\mathcal{H})} \mathrm{Tr}\Big(\mathcal{E}(|i\rangle\langle j|)\Big)\, |i\rangle\langle j| = \sum_{i=1}^{\dim(\mathcal{H})} |i\rangle\langle i| = \mathrm{Id}_{\mathcal{H}}.$$

- *(2.) ⇒ (3.) :*

The spectral decomposition of the positive semi-definite operator $J(\mathcal{E}) \in \mathscr{L}(\mathcal{H} \otimes \mathcal{K})$ can be written:

$$J(\mathcal{E}) = \sum_{a \in \mathcal{A}} |\alpha_a\rangle\langle\alpha_a|,$$

for an alphabet $\mathcal{A}$ with cardinal $\operatorname{rank}(J(\mathcal{E}))$ and vectors $|\alpha_a\rangle \in \mathcal{H} \otimes \mathcal{K}$ for any $a \in \mathcal{A}$. In the following we consider the expansion on coefficients of those vectors. For each $a \in \mathcal{A}$:

$$|\alpha_a\rangle = \sum_{i=1}^{\dim(\mathcal{K})} \sum_{j=1}^{\dim(\mathcal{H})} \alpha_{a,ij}\, |i\rangle|j\rangle.$$

In the following lines we no longer specify the ranges of the sums appearing, so that we can obtain cleaner expressions.

Now, according to Remark 1.28, for any $\rho = \sum_{i,j} \rho_{ij} |i\rangle\langle j| \in \mathscr{L}(\mathcal{H})$ we can write:

$$\begin{aligned}\mathcal{E}(\rho) &= \operatorname{Tr}_{\mathcal{H}} J(\mathcal{E})\,(\mathrm{Id}_{\mathcal{K}} \otimes \rho^t) = \sum_a \operatorname{Tr}_{\mathcal{H}} |\alpha_a\rangle\langle\alpha_a|\,(\mathrm{Id}_{\mathcal{K}} \otimes \rho^t)\\ &= \sum_a \sum_{i,j,k,l} \alpha_{a,ij}\, \rho_{jl}\, \overline{\alpha}_{a,kl}\, |i\rangle\langle j|\\ &= \sum_a A_a\, \rho\, A_a^\dagger,\end{aligned}$$

where we have defined the operators $A_a = \sum_{i,j} \alpha_{a,ij}\, |i\rangle\langle j| \in \mathscr{L}(\mathcal{H}, \mathcal{K})$. Additionally, we also have that

$$\begin{aligned}\mathrm{Id}_{\mathcal{H}} = \operatorname{Tr}_{\mathcal{K}} J(\mathcal{E}) &= \sum_a \operatorname{Tr}_{\mathcal{K}} |\alpha_a\rangle\langle\alpha_a| = \sum_a \sum_{i,j,l} \alpha_{a,ij}\, \overline{\alpha}_{a,il}\, |j\rangle\langle l|\\ &= \sum_a A_a^\dagger\, A_a.\end{aligned}$$

In the last equality we simply have taken into account the definition of the operators $\{A_a\}_a$.

• *(3.)* $\Rightarrow$ *(4.)*:

Identify $\mathcal{K}' = \mathcal{H}_{\mathcal{A}}$. Then, the operator $A = \sum_a |a\rangle \otimes A_a \in \mathscr{L}(\mathcal{H}, \mathcal{K} \otimes \mathcal{H}_{\mathcal{A}})$ fulfils conditions in the statement.

• *(4.)* $\Rightarrow$ *(1.)*:

Finally, it is clear that for any finite dimensional Hilbert space $\mathcal{H}'$, the map $\mathrm{Tr}_{\mathcal{K}'}(\mathrm{Id}_{\mathcal{H}'} \otimes A)\,(\,\cdot\,)\,(\mathrm{Id}_{\mathcal{H}'} \otimes A^\dagger)$ is positive. Furthermore, since A is an isometry, $A^\dagger A = \mathrm{Id}_{\mathcal{H}}$ and

$$\mathrm{Tr}\mathcal{E}(\rho) = \mathrm{Tr}\, A\, \rho\, A^\dagger = \mathrm{Tr}\, \rho\, A^\dagger A = \mathrm{Tr}\rho,$$

for any $\rho \in \mathscr{L}(\mathcal{H})$. That is, we have concluded that $\mathcal{E} \in \mathrm{CPTP}(\mathcal{H}, \mathcal{K})$. □

Remark 1.30. We further note that, given $\mathcal{E} \in \mathscr{L}(\mathcal{H}\otimes\mathcal{K})$, $\mathrm{rank}(J(\mathcal{E})) \leq \dim(\mathcal{H})\, \dim(\mathcal{K})$.

We will usually refer to the representation in the last item of the previous theorem as a *purification* of the channel $\mathcal{E}$. This convention is motivated by the fact that the Stinespring's representation allows us to understand the channel as a unitary operation in a bigger system followed by a partial transpose.

Extremality. Now we turn our attention to the convex structure that naturally appears underlying the objects we have introduced before. For convenience, we state the results in this section for the case of quantum-to-classical-quantum channels. Specific results for states, general channels, POVMs and instruments can be obtained as particular cases from the former.

We start settling the convex structure we analyse later on.

Proposition 1.31. *Given registers* X, Y, Z *where* Y *is considered classical, the set of quantum-to-classical-quantum channels* $\mathrm{CPTP}_{qcq}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z})$ *is compact and convex.*

Proof. According to Theorem 1.29, 2., the set $\mathrm{CPTP}_{qcq}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z})$ can be identified with the image via J^{-1} of the set

$$S = \left\{ \sum_{y\in\mathcal{Y}} |y\rangle\langle y| \otimes \rho_y \quad : \quad \begin{array}{c} \rho_y \in \mathsf{Pos}(\mathcal{H}_\mathcal{Z}) \quad \forall y \in \mathcal{Y}, \\ \sum_{y\in\mathcal{Y}} \mathrm{Tr}_{\mathcal{H}_\mathcal{Z}}\rho_y = \mathrm{Id}_{\mathcal{H}_\mathcal{X}} \end{array} \right\}.$$

The claim in the proposition follows now from proving that S is a compact and convex set. That is the case because S can be understood as the intersection of the cone of positive semidefinite operators on the

C*-algebra $\ell_\infty^{\mathcal{Y}}(\mathscr{B}(\mathcal{H}_Z))$ and the affine subspace $\{\sum_{y\in\mathcal{Y}} |y\rangle\langle y| \otimes \rho_y \quad : \sum_{y\in\mathcal{Y}} \mathrm{Tr}_{\mathcal{H}_\mathcal{Z}}\rho_y = \mathrm{Id}_{\mathcal{H}_\mathcal{X}}\}$. Both sets are closed and convex, so the same holds for S.

Finally, any element in S has bounded trace norm, so this set is also bounded and, hence, compact. □

Remark 1.32. The set of states is the particular case in which X and Y are trivial[4] while general quantum-to-quantum channels are recovered setting only Y to be trivial. The case in which Z is trivial is intimately related with the definition of POVMs – recall Remark 1.16 – while the original case considered in the statement of Proposition 1.31 is concerned with quantum instruments – recall Remark 1.18.

The previous proposition motivates the description of sets of states, channels and instruments as convex hulls of their respective extreme points. These extreme points can be characterized by the following theorem, originally discovered by Man-Duen Choi, [26][5].

Theorem 1.33. *Given registers* X, Y, Z *where* Y *is considered classical, a quantum-to-classical-quantum channel* $\mathcal{E} \in \mathrm{CPTP}_{qcq}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z})$ *is an extreme point of the set* $\mathrm{CPTP}_{qcq}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z})$ *if and only if*

$$\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{a\in\mathcal{A}^i} A_a^i\,(\,\cdot\,)\,A_a^{i\,\dagger}$$

for alphabets $\mathcal{A}^i$ *and operators* $A_a^i \in \mathscr{L}(\mathcal{H}_\mathcal{X}, \mathcal{H}_\mathcal{Z})$ *such that* $\{A_b^{i\,\dagger} A_a^i\}_{i\in\mathcal{Y},\,a,b\in\mathcal{A}^i}$ *is a linearly independent set.*

For the proof we need the following lemma:

Lemma 1.34. *Let* $\mathcal{A}$, $\mathcal{B}$ *be alphabets such that* $|\mathcal{A}| \le |\mathcal{B}|$. *For any two collections of operators* $\{A_a\}_{a\in\mathcal{A}}$, $\{B_b\}_{b\in\mathcal{B}} \subset \mathscr{L}(\mathcal{H}, \mathcal{K})$:

$$\sum_{a\in\mathcal{A}} A_a(\,\cdot\,)A_a^\dagger = \sum_{b\in\mathcal{B}} B_b(\,\cdot\,)B_b^\dagger,$$

[4] Given a state $\rho \in \mathscr{D}(\mathcal{H}_\mathcal{Z})$, it can be seen as an operator $\rho : \mathscr{L}(\mathcal{H}_\mathcal{Z}) \to \mathbb{C}$. The dual map, $\rho^*(\lambda) = \lambda\rho$ for any $\lambda \in \mathbb{C}$, is completely positive and trace preserving, $\rho^* \in \mathrm{CPTP}(\mathbb{C}, \mathcal{H}_\mathcal{Z})$.

[5] Choi originally stated these results for CPTP maps and that is as it usually appears in the literature. However, the statement we prove is more convenient for our purposes and follows essentially from the same techniques used in [26]

if and only if there exists an isometry $\lambda = \sum_{a\in\mathcal{A},\, b\in\mathcal{B}} \lambda_{ab} |a\rangle\langle b|$ *satisfying* $B_b = \sum_{a\in\mathcal{A}} \lambda_{ab}\, A_a$ *for all* $b \in \mathcal{B}$*. Moreover,* λ *is unitary when* $|\mathcal{A}| = |\mathcal{B}|$*.*

Proof. The operators $\{A_a\}_{a\in\mathcal{A}}$, $\{B_b\}_{b\in\mathcal{B}} \subset \mathscr{L}(\mathcal{H},\mathcal{K})$ define completely positive maps A, $B : \mathscr{B}(\mathcal{H}) \to \mathscr{B}(\mathcal{K})$ with

$$A = \sum_{a\in\mathcal{A}} A_a(\,\cdot\,)A_a^\dagger,\ B = \sum_{b\in\mathcal{B}} B_b(\,\cdot\,)B_b^\dagger.$$

Therefore, $\sum_{a\in\mathcal{A}} A_a(\,\cdot\,)A_a^\dagger = \sum_{b\in\mathcal{B}} B_b(\,\cdot\,)B_b^\dagger$ holds iff their corresponding Choi's representations also coincides, $J(A) = J(B)$. These Choi's representations can be written in this case as:

$$J(A) = \sum_{a,i,j} A_a|i\rangle\langle j|A_a^\dagger \otimes |i\rangle\langle j|, \quad J(B) = \sum_{b,i,j} B_b|i\rangle\langle j|B_b^\dagger \otimes |i\rangle\langle j|,$$

where $J(A)$, $J(B) \in \mathscr{L}(\mathcal{K}\otimes\mathcal{H})$. Consider now a third Hilbert space $\mathcal{H}'$ of dimension $\max(|\mathcal{A}|,|\mathcal{B}|)$. Using this space we can consider the purifications

$$J(A) = \mathrm{Tr}_{\mathcal{H}'}|\alpha\rangle\langle\alpha|,\ J(B) = \mathrm{Tr}_{\mathcal{H}'}|\beta\rangle\langle\beta|,$$

where we have defined vectors

$$|\alpha\rangle = \sum_{a,i} A_a|i\rangle \otimes |i\rangle \otimes |a\rangle_{\mathcal{H}'},\ |\beta\rangle = \sum_{b,i} B_b|i\rangle \otimes |i\rangle \otimes |b\rangle_{\mathcal{H}'}.$$

Now, recalling Theorem 1.26, $J(A) = J(B)$ iff $|\beta\rangle = (\mathrm{Id}_{\mathcal{K}\otimes\mathcal{H}} \otimes \lambda)|\alpha\rangle$ for a unitary operator $\lambda \in \mathscr{U}(\mathcal{H}')$. Writing down this operator in coordinates, $\lambda = \sum_{a,b} \lambda_{ab}|b\rangle\langle a|$, we can equivalently state that:

$$J(A) = J(B) \quad \text{iff} \quad B_b = \sum_a \lambda_{ab} A_a \text{ for all } b \in \mathcal{B}.$$

This is equivalent to the claim in the statement. □

Proof of Theorem 1.33. • *Only if part*:

Consider an extreme quantum-to-classical-quantum channel

$$\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \mathcal{E}_i(\,\cdot\,) : \mathscr{L}(\mathcal{H}_\mathcal{X}) \to \mathscr{L}(\mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z}).$$

Fix a Kraus representation $\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{a\in\mathcal{A}^i} A^i_a\,(\,\cdot\,)\,{A^i_a}^\dagger$, such that for each $i \in \mathcal{Y}$, $\{A^i_a\}_{a\in\mathcal{A}^i}$ is a linearly independent set. Consider now a collection of complex numbers $\{\lambda^i_{ab}\}_{i,a,b}$ such that

$$\sum_{i,a,b} \lambda^i_{ab}\, {A^i_b}^\dagger A^i_a = 0. \tag{1.4}$$

We will see that the extremality of $\mathcal{E}$ implies that $\lambda^i_{ab} = 0$ for all $i \in \mathcal{Y}$, a, $b \in \mathcal{A}$.

Firstly, we notice that we can assume $\lambda^i = (\lambda^i_{ab})_{a,b}$ to be an hermitian matrix for each $i \in \mathcal{Y}$. This follows from the fact that $\lambda^i_{ab} = 0$ for all $i \in \mathcal{Y}$, a, $b \in \mathcal{A}^i$ iff $\lambda^i_{ab} \pm \overline{\lambda^i_{ab}} = 0$ for all $i \in \mathcal{Y}$, a, $b \in \mathcal{A}^i$ and the observation that condition (1.4) also implies $\sum_{i,a,b}(\lambda^i_{ab}+\overline{\lambda^i_{ab}})\, {A^i_b}^\dagger A^i_a = 0 = \sum_{i,a,b} i\,(\lambda^i_{ab} - \overline{\lambda^i_{ab}})\, {A^i_b}^\dagger A^i_a$. Furthermore, we can also assume λ^i such that $-\mathrm{Id}_{\mathcal{H}_{\mathcal{A}^i}} \le \lambda^i \le \mathrm{Id}_{\mathcal{H}_{\mathcal{A}^i}}$ simply dividing (1.4) by the scalar $\max_{i\in\mathcal{Y}} \|\lambda^i\|$.

Next, we construct the channels

$$\mathcal{R}_\pm(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \Big(A^i_a\,(\,\cdot\,)\,{A^i_a}^\dagger \pm \sum_{a,b\in\mathcal{A}^i} \lambda^i_{ab}\, A^i_a\,(\,\cdot\,)\,{A^i_b}^\dagger\Big),$$

that trivially decompose $\mathcal{E}$ as the convex combination $\mathcal{E} = \frac{1}{2}(\mathcal{R}_+ + \mathcal{R}_-)$. The fact that $\mathcal{R}_\pm$ are channels follows from the positivity of the operators $\mathrm{Id}_{\mathcal{H}_{\mathcal{A}^i}} \pm \lambda^i$ and the hypothesis (1.4): the positivity of $\mathrm{Id}_{\mathcal{H}_{\mathcal{A}^i}} \pm \lambda^i$ allows us to factorize $\mathrm{Id}_{\mathcal{H}_{\mathcal{A}^i}} + \lambda^i = {\alpha^i}^\dagger \alpha^i$ for some operators $(\alpha^i_{ab})_{a,b}$, one for each $i \in \mathcal{Y}$. Defining $B^i_a := \sum_{a\in\mathcal{A}^i} \alpha^i_{ab} A^i_b$, we can rewrite $\mathcal{R}_+(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{a\in\mathcal{A}^i} B^i_a\,(\,\cdot\,)\,{B^i_a}^\dagger$. Moreover, (1.4) implies that $\sum_{i\in\mathcal{Y}} \sum_{a\in\mathcal{A}^i} {B^i_a}^\dagger B^i_a = \sum_{i\in\mathcal{Y}} \sum_{a\in\mathcal{A}^i} {A^i_a}^\dagger A^i_a$, and, according to Theorem 1.29,3., this equals $\mathrm{Id}_{\mathcal{H}_\mathcal{X}}$. Therefore $\mathcal{R}_+$ is indeed a channel. Similarly for $\mathcal{R}_-$.

Finally, the extremality of $\mathcal{E}$ implies that $\mathcal{R}_+ = \mathcal{E}$. Hence, in virtue of Lemma 1.34, the matrices $(\alpha^i_{ab})_{a,b}$ are unitary[6]. Nonetheless, recalling their definition we have $\mathrm{Id}_{\mathcal{H}_\mathcal{A}} + \lambda^i = {\alpha^i}^\dagger \alpha^i = \mathrm{Id}_{\mathcal{H}_\mathcal{A}}$, that is, $\lambda^i = 0$ for any $i \in \mathcal{Y}$.

- *If part*:

[6] Notice that the linear independence of $\{A^i_a\}_{a\in\mathcal{A}^i}$ determines uniquely the coefficients α^i_{ab}.

Consider a channel

$$\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{a\in\mathcal{A}^i} A_a^i\,(\,\cdot\,)\,A_a^{i\,\dagger},$$

where $\{A_b^{i\,\dagger} A_a^i\}_{i\in\mathcal{Y},\,a,b\in\mathcal{A}^i}$ are linearly independent. Now, suppose that $\mathcal{E}$ is the convex combination of two other channels:

$$\mathcal{E} = \lambda\,\mathcal{R}_1 + (1-\lambda)\mathcal{R}_2, \quad \lambda\in(0,1),$$

with $\mathcal{R}_k(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{a\in\mathcal{B}^i} B_a^{k,i}\,(\,\cdot\,)\,B_a^{k,i\dagger}$ such that $\sum_{i\in\mathcal{Y}}\sum_{a\in\mathcal{B}^i} B_a^{k,i\dagger}\, B_a^{k,i} = \mathrm{Id}_{\mathcal{H}_\mathcal{X}}$, for $k=1,\,2$.

Accordingly, denoting $\lambda_1=\lambda$, $\lambda_2 = 1-\lambda$, we rewrite

$$\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{k=1,2}\sum_{b\in\mathcal{B}^i} \lambda_k\, B_b^{k,i}\,(\,\cdot\,)\,B_b^{k,i\dagger}.$$

Recalling again Lemma 1.34, the last line implies that

$$B_b^{k,i} = \sum_{a\in\mathcal{A}^i} \alpha_{ba}^{k,i}\, A_a^i,$$

for scalars $\alpha_{ba}^{k,i}$, where $k=1,\,2$, $i\in\mathcal{Y}$, $a\in\mathcal{A}^i$, $b\in\mathcal{B}^i$. Moreover, since

$$\begin{aligned}\mathrm{Id}_{\mathcal{H}_\mathcal{X}} &= \sum_{i\in\mathcal{Y}}\sum_{a\in\mathcal{A}^i} A_a^{i\,\dagger} A_a^i = \sum_{i\in\mathcal{Y}}\sum_{b\in\mathcal{B}^{k,i}} B_b^{k,i\dagger} B_b^{k,i}\\ &= \sum_{i\in\mathcal{Y}}\sum_{a,c\in\mathcal{A}^i}\sum_{b\in\mathcal{B}^{k,i}} \overline{\alpha}_{ba}^{k,i}\,\alpha_{bc}^{k,i}\, A_a^{i\,\dagger} A_c^i,\end{aligned}$$

and $\{A_a^{i\,\dagger}\, A_c^i\}_{i,a,c}$ are linearly independent, it must hold that $\sum_{b\in\mathcal{B}^{k,i}} \overline{\alpha}_{ba}^{k,i}\ \alpha_{bc}^{k,i} = \delta_{ac}$. That is, $\sum_{i\in\mathcal{Y}} |i\rangle\langle i| \otimes \sum_{a\in\mathcal{A}^i,\,b\in\mathcal{B}^{k,i}} \alpha_{ba}^{k,i} |b\rangle\langle a|$ is an isometry, and therefore, again by Lemma 1.34, $\mathcal{R}_k = \mathcal{E}$. □

Corollary 1.35. *The extreme points of the set of quantum states of a given register* Z *are the pure states in* $\mathscr{D}(\mathcal{H}_\mathcal{Z})$.

Proof. As pointed out before, the set of states $\mathscr{D}(\mathcal{H}_\mathcal{Z})$ can be identified as the set of channels $\mathrm{CPTP}(\mathbb{C},\mathcal{H}_\mathcal{Z})$. Given $\rho\in\mathscr{D}(\mathcal{H}_\mathcal{Z})$, the corresponding map $\rho^* : \mathbb{C}\ni\lambda\mapsto\lambda\rho\in\mathscr{L}(\mathcal{H}_\mathcal{Z})$ is an element in

$\mathrm{CPTP}(\mathbb{C},\mathcal{H}_{\mathcal{Z}})$. Conversely, any element $\sigma \in \mathrm{CPTP}(\mathbb{C},\mathcal{H}_{\mathcal{Z}})$ defines a state $\sigma^* \in \mathscr{D}(\mathcal{H}_Z) \subseteq \mathscr{L}(\mathscr{L}(\mathcal{H}_Z),\mathbb{C})$. According to the previous theorem, $\sigma \in \mathrm{CPTP}(\mathbb{C},\mathcal{H}_{\mathcal{Z}})$ is an extreme point of the set $\mathrm{CPTP}(\mathbb{C},\mathcal{H}_{\mathcal{Z}})$ iff

$$\sigma(\lambda) = \sum_{a\in\mathcal{A}} \lambda\,|\alpha_a\rangle\langle\alpha_a| \quad \text{for any } \lambda \in \mathbb{C},$$

where $\{|\alpha_a\rangle\}_{a\in\mathcal{A}} \subset \mathscr{L}(\mathbb{C},\mathcal{H}_{\mathcal{Z}}) \simeq \mathcal{H}_{\mathcal{Z}}$ are such that $\{\langle\alpha_b|\alpha_a\rangle\}_{a,b\in\mathcal{A}} \subset \mathbb{C}$ is a linearly independent set. The last condition clearly implies that $|\alpha_a\rangle = 0$ for any $a \in \mathcal{A}$ except one. Call $|\alpha\rangle$ the unique non-null element of $\{|\alpha_a\rangle\}_a$. Then,

$$\sigma(\lambda) = \lambda\,|\alpha\rangle\langle\alpha|.$$

Since σ is a channel, $|\alpha\rangle$ must be a unit vector in $\mathcal{H}_{\mathcal{Z}}$. This implies that the corresponding state $\sigma^* \in \mathscr{D}(\mathcal{H}_{\mathcal{Z}})$ is the rank-one operator $|\alpha\rangle\langle\alpha|$ where $|\alpha\rangle$ is a unit vector in $\mathcal{H}_Z$. □

Corollary 1.36. *The extreme points of the set of instruments* $\mathrm{Ins}(\mathcal{H}_{\mathcal{X}},\mathcal{H}_{\mathcal{Z}})$ *have at most* $|\mathcal{X}|^2$ *possible different outcomes.*

Proof. An instrument in $\mathrm{Ins}(\mathcal{H}_{\mathcal{X}},\mathcal{H}_{\mathcal{Z}})$ is a sequence of completely positive maps $\{\mathcal{E}_i\}_{i\in\mathcal{I}} \subset \mathrm{CP}(\mathcal{H}_{\mathcal{X}},\mathcal{H}_{\mathcal{Z}})$, for some alphabet $\mathcal{I}$, such that $\sum_{i\in\mathcal{I}}\mathcal{E}_i \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{X}},\mathcal{H}_{\mathcal{Z}})$. In consonance with Remark 1.18, the former instrument can be characterized by the quantum-to-classical-quantum channel:

$$\mathcal{E}(\,\cdot\,) = \sum_{i\in\mathcal{I}} |i\rangle\langle i| \otimes \mathcal{E}_i(\,\cdot\,).$$

Taking into account Theorem 1.33, if this channel is an extreme point, $\mathcal{E}_i \neq 0$ for at most $(\dim\mathcal{H}_{\mathcal{X}})^2$ different indices $i \in \mathcal{Y}$. This implies the claim in the statement. □

1.3 Quantum games

We finish this first chapter with an application of some of the previous notions to a particular setting: *cooperative quantum games* or, simply, *quantum games*.

In the last sixty years, multiplayer cooperative games have proven to be a perfect representative of a field in which the irruption of quantum mechanics leads to far-reaching implications. Starting with Bell's work in the sixties, the study of quantum agents interacting in cooperative games is nowadays the cornerstone of a continuously increasing amount of lines of work. Substantive examples can be found in quantum cryptography [35, 4, 2, 52, 21], complexity theory [96, 14, 16, 47] and even the recent resolution of Connes' embedding problem [48].

The cited groundbreaking developments can be classified in the study of *non-local* games, that are cooperative games in which the interaction between players and referee is mediated by *classical* messages. However, the players are usually considered to use quantum resources in their strategy.

Here, we are interested in a generalization of such games in which also the communication between players and referee can be quantum. These are what we call *quantum games.* In particular, we restrict ourselves to the case of two-player quantum games. In this setting, two players, Alice and Bob, interact with a referee receiving from him a bipartite quantum state. Acting on the received system, Alice and Bob obtain another bipartite state which is communicated back to the referee who checks the validity of players' answer performing a measurement.

Quantum games have appeared naturally in quantum information theory in several places, see [78, 112, 55, 60, 25] for some examples, and some specific classes of quantum games were rigorously defined and studied in [28, 98, 20, 51]. Indeed, our starting point is one of these latest notions. In the rest of this section we introduce *rank-one quantum games*, originally defined in [28], and present a slight generalization that we call *mixed* rank-one quantum games. This setting will be central for Chapter 4. Rank-one quantum games also underlie some of the key ideas in Chapter 3, even though we will not make any explicit reference to this fact anymore.

A (two-player one-round) rank-one quantum game, ROQG, is specified by:

1. a tripartite Hilbert space $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$;

2. and unit vectors $|\psi\rangle$, $|\gamma\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$.

The game then proceeds as follows:

- the referee starts preparing the state $|\psi\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$ and sends registers $\mathcal{H}_\mathcal{A}$, $\mathcal{H}_\mathcal{B}$ to Alice and Bob, respectively;
- the players apply an allowed quantum operation[7] on the received registers, $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, sending them back to the referee;
- finally, in order to decide whether the players win or lose the game, the referee performs the projective measurement given by elements $\{|\gamma\rangle\langle\gamma|, \mathrm{Id} - |\gamma\rangle\langle\gamma|\}$. When the outcome of this measurement is the one associated to $|\gamma\rangle\langle\gamma|$, the referee declares Alice and Bob winning. Otherwise they lose.

We give now a formal definition for this type of games (see [28] for further details):

Definition 1.37. *We identify a rank-one quantum game (ROQG), G, with a tensor $\hat{G}$ in the unit ball of $\mathcal{S}_1(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$. Such a tensor can be always written in the form $\hat{G} = \mathrm{Tr}_{\mathcal{H}_\mathcal{C}} |\psi\rangle\langle\gamma|$ for some ancillary Hilbert space $\mathcal{H}_\mathcal{C}$ and vectors $|\psi\rangle$, $|\gamma\rangle$ in the unit ball of $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$ (see [28, Prop. 3.1] for an explicit proof of this easy fact) .*

A strategy for G is a quantum channel $\mathcal{S}$ acting on the system $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. That is, $\mathcal{S} \in \mathrm{CPTP}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$. The value achieved by this strategy is defined by:

$$\omega(G;\mathcal{S}) := \mathrm{Tr}\Big[\, |\gamma\rangle\langle\gamma| \ \ (\mathrm{Id}_C \otimes \mathcal{S}) \Big(|\psi\rangle\langle\psi|\Big) \,\Big], \tag{1.5}$$

and corresponds to the winning probability achieved in the game described above when the players use strategy $\mathcal{S}$ to play.

In general, not any quantum operation will be considered to be an allowed strategy, since the actions of Alice and Bob might be restricted in a given situation. For example, one can consider situations in which Alice and Bob are spatially isolated so they cannot communicate between them. In other situations, even when the players have the capability to share messages, the communication might be constrained in their structure, as it will be the case in Chapter 4. We refer to sets of allowed strategies as

[7] The action of the players might be constrained for physical or other reasons forbidding Alice and Bob to apply a completely general quantum channel. Below we state these limitations in more detail.

scenarios, which are usually motivated by physical constraints on the players.

Definition 1.38. *In a particular scenario $\mathfrak{S} \subseteq \mathrm{CPTP}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$, the value of the game G is:*

$$\omega_{\mathfrak{S}}(G) := \sup_{\mathcal{S} \in \mathfrak{S}} \omega_{\mathfrak{S}}\left(G; \mathcal{S}\right). \tag{1.6}$$

Example 1.39. The honest scenario. In this preliminary chapter we only introduce the simplest scenario, the one in which we allow any quantum channel on $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ to be a valid strategy. That is, in this scenario, the set of allowed strategies is $\mathfrak{S} = \mathrm{CPTP}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$. This corresponds to the case in which Alice and Bob are allowed to apply any global operation, so they perform as if they were a single agent with access to the full question in the game. We refer to this situation as the *honest scenario.*

Definition 1.40. *The Honest value of G is given by:*

$$\omega_H(G) = \sup_{\mathcal{S} \in \mathrm{CPTP}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})} \omega(G; \mathcal{S}). \tag{1.7}$$

The nomenclature for this scenario was borrowed from the interpretation we give to such games in Chapter 4 and it is not in any sense standard. In fact, in [28] the previous value was called *maximal.* More importantly, this scenario serves as a natural normalization for the game, it is the largest value achievable under the unique assumption that quantum mechanics is the underlying model explaining players' behaviour.

Remark 1.41. It turns out that the supremum in (1.7) can be restricted to unitary channels without altering its value. In this case, we can work out (1.7) to obtain the following equivalent expression:

$$\begin{aligned} \omega_H(G) &= \sup_{U \in \mathfrak{U}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})} \omega(G; U(\,\cdot\,)U^\dagger) = \sup_{U \in \mathfrak{U}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})} \Big(\mathrm{Tr}(\hat{G}\,U)\Big)^2 \\ &\equiv \sup_{U \in \mathfrak{U}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})} \langle U, \hat{G} \rangle^2 = \|\hat{G}\|^2_{\mathcal{S}_1(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})}. \end{aligned} \tag{1.8}$$

Indeed, by compactness, this supremum is achieved by some unitary U_G, that can be interpreted as the ideal action the players have to perform to maximize their chances to win the game. This gives us a useful interpretation of rank-one quantum games: Alice and Bob have to simulate the application of a given unitary, U_G, on registers $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ of the system $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$ prepared on the initial state $|\psi\rangle$.

Proof of (1.8). According to Definitions 1.40 and 1.37,

$$\omega_H(G) = \sup_{\mathcal{S} \in \mathrm{CPTP}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})} \mathrm{Tr}\Big[\, |\gamma\rangle\langle\gamma| \;\; (\mathrm{Id}_C \otimes \mathcal{S}) \Big(|\psi\rangle\langle\psi|\Big) \,\Big]. \tag{1.9}$$

Considering a purification of $\mathcal{S}$, cf. Theorem 1.29, 4, we can write $\mathcal{S}$ in terms of an isometry $A \in \mathscr{B}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}, \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{K}')$ to obtain:

$$\begin{aligned}
&\mathrm{Tr}\Big[\, |\gamma\rangle\langle\gamma| \;\; (\mathrm{Id}_C \otimes \mathcal{S}) \Big(|\psi\rangle\langle\psi|\Big) \,\Big] \\
&\quad = \mathrm{Tr}\Big[\, (|\gamma\rangle\langle\gamma| \otimes \mathrm{Id}_{\mathcal{K}'})\, (\mathrm{Id}_C \otimes A)\, |\psi\rangle\langle\psi|\, (\mathrm{Id}_C \otimes A^\dagger)\Big] \\
&\quad = \Big\| (\langle\gamma| \otimes \mathrm{Id}_{\mathcal{K}'})\, (\mathrm{Id}_C \otimes A)\, |\psi\rangle \Big\|_{\mathcal{K}'}^2 \\
&\quad = \sup_{\langle\xi| \in \mathsf{ball}(\mathcal{K}')} \Big((\langle\gamma| \otimes \langle\xi|)\, (\mathrm{Id}_C \otimes A)\, |\psi\rangle \Big)^2 \\
&\quad = \sup_{\langle\xi| \in \mathsf{ball}(\mathcal{K}')} \Big(\mathrm{Tr}\,[\, \langle\xi| A\, \mathrm{Tr}_\mathcal{C} |\psi\rangle\langle\gamma|\,] \Big)^2 \\
&\quad = \sup_{\langle\xi| \in \mathsf{ball}(\mathcal{K}')} \Big\langle \langle\xi| A, \hat{G} \Big\rangle^2.
\end{aligned}$$

Taking this manipulation into account, we can rewrite (1.9) as:

$$\omega_H(G) = \sup_{\substack{\mathcal{K}', \\ A \in \mathscr{B}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}, \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{K}'), \\ \langle\xi| \in \mathsf{ball}(\mathcal{K}')}} \Big\langle \langle\xi| A, \hat{G} \Big\rangle^2,$$

where A in the supremum is an isometry. Therefore, the supremum is actually taken over bounded operators of the form $\langle\xi| A \in \mathscr{B}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$. This translates into the fact:

$$\omega_H(G) \leq \sup_{A \in \mathscr{B}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})} \langle A, \hat{G} \rangle^2,$$

but the former supremum can be restricted to unitary operators $U \in \mathcal{U}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$, which turns out that can be always written in the form $\langle \xi | A$ (consider $A = |\xi\rangle \otimes U$, for instance) and hence we have an equality in the previous expression. Concluding, we have shown that

$$\omega_H(G) = \sup_{U \in \mathcal{U}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}),} \langle U, \hat{G} \rangle^2.$$

□

To complete this section, we introduce the notion of *mixed rank-one quantum games.* These games are constructed from a family of ROQGs, say $\{G_{t_a,t_b}\}_{t_a,t_b}$, indexed by $t_a \in \mathcal{T}_A$, $t_b \in \mathcal{T}_B$, together with a probability distribution $\{p_{t_a,t_b}\}_{t_a,t_b}$[8]. For the sake of readability, we refer to pairs (t_a, t_b) by $\mathbf{t}$, so that $\mathbf{t} \in \mathcal{T}_A \times \mathcal{T}_B$. The game proceeds as follows:

- The referee chooses randomly one of the ROQG, $G_\mathbf{t}$, according to the probability distribution $p_\mathbf{t}$.
- The referee prepares the state corresponding to the game $G_\mathbf{t}$. He sends a quantum system to Alice and Bob, as specified by the ROQG $G_\mathbf{t}$, together with the classical information $\mathbf{t}$. Alice receives t_a and Bob t_b – recall that $\mathbf{t} = (t_a, t_b)$;
- Alice and Bob, with the information they received, prepare a state to answer the referee;
- finally, with the state communicated by Alice and Bob, the referee performs the final measurement defined in $G_\mathbf{t}$. This decides whether the players win or lose.

Once we introduced this family of games, we now give a formal definition:

Definition 1.42. *We identify a mixed rank-one quantum game (MROQG), G, with a sequence of tensors* $\left\{ \hat{G}_\mathbf{t} = \mathrm{Tr}_C |\psi_\mathbf{t}\rangle\langle\gamma_\mathbf{t}| \right\}_\mathbf{t}$, *where each* $\hat{G}_\mathbf{t}$ *is in the unit ball of* $\mathcal{S}_1(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B})$, *together with a probability distribution* $\{p_\mathbf{t}\}_\mathbf{t}$.

[8] For each t_a t_b, $p_{t_a,t_b} \geq 0$ and $\sum_{t_a,t_b} p_{t_a,t_b} = 1$. We restrict ourselves to finite index sets $\mathcal{T}_A$, $\mathcal{T}_B$.

A strategy for G is a sequence of quantum channels $\{\mathcal{S}_{\mathbf{t}}\}_{\mathbf{t}}$ acting on the system $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. The value achieved by this strategy is defined by:

$$\omega(G;\{\mathcal{S}_{\mathbf{t}}\}_{\mathbf{t}}) := \mathbb{E}_{\mathbf{t}} \ \mathrm{Tr}\left[\, |\gamma_{\mathbf{t}}\rangle\langle\gamma_{\mathbf{t}}| \ \ (\mathrm{Id}_C \otimes \mathcal{S}_{\mathbf{t}}) \left(|\psi_{\mathbf{t}}\rangle\langle\psi_{\mathbf{t}}|\right) \right], \qquad (1.10)$$

where $\mathbb{E}_{\mathbf{t}}$ denotes the expectation over the random variable $\mathbf{t}$ distributed according to $\{p_{\mathbf{t}}\}_{\mathbf{t}}$.

As in the previous discussion, we also consider restricted families of allowed strategies for MROQGs, that is, subsets $\mathfrak{S} \subseteq \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}})^{\times|\mathrm{T}_{\mathcal{A}}\times\mathrm{T}_{B}|}$. This leads to the value of a MROQG in a given scenario:

Definition 1.43. *In a particular scenario $\mathfrak{S} \subseteq \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}})^{\times|\mathrm{T}_{\mathcal{A}}\times\mathrm{T}_{B}|}$, the value of the game is:*

$$\omega_{\mathfrak{S}}(G) := \sup_{\mathcal{S}\in\mathfrak{S}} \omega_{\mathfrak{S}}\left(G;\mathcal{S}\right). \qquad (1.11)$$

Matching our earlier discussion on ROQGs, we also comment that the *honest* scenario is defined considering any strategy as valid; that is, setting $\mathfrak{S} = \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}})^{\times|\mathrm{T}_{\mathcal{A}}\times\mathrm{T}_{B}|}$. This leads to define $\omega_H(G)$ for a MROQG in analogy with (1.7). With similar computations as in Remark 1.41 we can obtain:

$$\omega_H(G) = \mathbb{E}_{\mathbf{t}} \, \|G_{\mathbf{t}}\|^2_{\mathcal{S}_1^{AB}}.$$

Formally, this equation perfectly matches the idea of MROQGs as distributions of ROQGs.

As said before, we will come back to MROQGs in Chapter 4, where this notion of quantum games will be the key to formalize our constructions in the study of Position Based Quantum Cryptography.

Chapter 2

Preliminaries II: Banach spaces and operator space theory

In this chapter we develop some basic notions mainly concerned with Banach spaces, although we make a brief introduction to operator spaces in Section 2.1.2. The selection of the contents of this chapter, as well as its presentation, is strongly biased towards the tools that we will use in next chapters. After providing basic some definitions about Banach and operator spaces in Section 2.1, we introduce in Section 2.2 one of the main notions that we study in this thesis: the type and cotype of a Banach space. We introduce in Section 2.3 some technical tools from interpolation theory and we finish this chapter devoting Section 2.4 to the important notion of operator ideals in Banach spaces.

2.1 Some basics on Banach spaces and operator spaces

2.1.1 Banach spaces

A finite dimensional Banach space is simply a vector space endowed with a *norm*. According to that, a Banach space is identified with a couple $(X, \| \cdot \|_X)$ being X a vector space while $\| \cdot \|_X$ denotes the norm. However, we will usually refer to such a space simply by X, referring to the norm only implicitly. In general, X is also required to be complete with respect to $\| \cdot \|_X$. When completeness is not guaranteed, it is customary to refer to X as a *normed space*. In the finite dimensional case, completeness is always granted and both notions refer to the same thing, being this the reason why we sometimes use both nomenclatures interchangeably. The underlying field for us will be always the set of complex numbers, unless the contrary is specified. Given a *Banach* space X, we fix the notation $\mathsf{ball}(X)$ for the closed unit ball of X.

Some particular Banach spaces. As we said repeatedly before, this thesis is mainly concerned with the study of finite dimensional Banach spaces. We introduce next some of the spaces that appear frequently in next chapters. Our first example was already introduced in Chapter 1. That is the case of the Hilbert space $\mathcal{H}_\mathcal{X}$ in which the norm was defined by:

$$\text{for any } |u\rangle = \sum_{x\in\mathcal{X}} u_x |x\rangle \in \mathbb{C}^\mathcal{X}, \quad \|u\|_{\mathcal{H}_\mathcal{X}} = \langle u|u\rangle^{\frac{1}{2}}.$$

To refer to arbitrary – finite or infinite dimensional – Hilbert spaces we use $\mathcal{H}$, $\mathcal{K}$, ...

The previous norm can be generalized as follows. For $1 \leq p < \infty$ and any $|u\rangle = \sum_{x\in\mathcal{X}} u_x|x\rangle \in \mathbb{C}^\mathcal{X}$:

$$\|u\|_{\ell_p^\mathcal{X}} = \Big(\sum_{x\in\mathcal{X}} |u_x|^p \Big)^{1/p}.$$

For $p = \infty$ is customary to fix:

$$\|u\|_{\ell_\infty^\mathcal{X}} = sup_{x\in\mathcal{X}} |u_x|.$$

This gives rise to the classical $\ell_p^\mathcal{X}$ spaces, that motivates the alternative notation $\ell_2^\mathcal{X}$ for the Hilbert space $\mathcal{H}_\mathcal{X}$. We usually use this alternative notation when the dimension of the space is explicitly known: we refer to a d-dimensional Hilbert space as ℓ_2^d. The previous definition extends in an obvious way to the infinite dimensional case of sequences $(u_i)_{i\in\mathbb{N}}$ instead of finite dimensional vectors $(u_x)_{x\in\mathcal{X}}$. We denote the Banach space obtained (after completion) simply by ℓ_p. In particular, ℓ_2 denotes a separable Hilbert space.

Another natural Banach space that we consider is the space of bounded operators between two Banach spaces X, Y. We define $\mathcal{B}(X,Y)$ as the Banach space of linear operators $f : X \to Y$ such that

$$\|f\| := \sup_{x \in \mathsf{ball}(X)} \|f(x)\|_Y < \infty.$$

Bounded operators, as defined above, are the natural morphisms between Banach spaces. In fact, they give us the right abstraction to define the *dual* of a Banach space X: X^* is simply identified with the space of bounded linear forms acting on X,

$$X^* \simeq \mathcal{B}(X, \mathbb{C}).$$

It is easy to check that, according to the previous definition, the following isometric relations between ℓ_p spaces hold:

$$(\ell_p)^* \simeq \ell_q \quad \text{for } 1 \leq p < \infty \text{ and } q \ : \ \frac{1}{p} + \frac{1}{q} = 1.$$

In the finite dimensional case, the above isometric identification is also true in the case $p = \infty$ ($q = 1$).

The previous example allows us to reintroduce Schatten classes, cf. Section 1.1.1. In the present context, these can be understood as a non-commutative generalization of ℓ_p spaces. From this perspective, given Hilbert spaces $\mathcal{H}$, $\mathcal{K}$, $\mathcal{S}_p(\mathcal{H},\mathcal{K})$ is the Banach space of compact operators from $\mathcal{H}$ into $\mathcal{K}$ whose sequence of singular values is in ℓ_p. When the underlying Hilbert spaces are separable, $\mathcal{H} = \ell_2 = \mathcal{K}$, we use the simpler notation $\mathcal{S}_p = \mathcal{S}_p(\ell_2, \ell_2)$. In the finite dimensional case, we use the notation $\mathcal{S}_p^{d,d'}$ to refer to $\mathcal{S}_p(\ell_2^{d'}, \ell_2^d)$.

Inherited from the duality between ℓ_p spaces, Schatten classes also display a similar relation:

$$(\mathcal{S}_p(\mathcal{H},\mathcal{K}))^* \simeq \mathcal{S}_q(\mathcal{H},\mathcal{K}) \quad \text{for } 1 \leq p < \infty \text{ and } q \ : \ \frac{1}{p} + \frac{1}{q} = 1,$$

where the case $p = \infty$ is also included when $\mathcal{H}$ or $\mathcal{K}$ are finite dimensional. The case $p = 2$ is a notable one. According to the previous relation, $\mathcal{S}_2(\mathcal{H}, \mathcal{K})$ is self-dual. In fact, $\mathcal{S}_2(\mathcal{H}, \mathcal{K})$ can be identified with the Hilbert space $\mathcal{H} \otimes \mathcal{K}$.

Concluding the basic set of examples presented here, we consider now the vector valued version of the former ℓ_p spaces. Concretely, given a Banach space X and $1 \leq p \leq \infty$, $\ell_p(X)$ is the Banach space of sequences $(x_i)_{i\in\mathbb{N}}$ of elements in X such that

$$\left\|(x_i)_{i\in\mathbb{N}}\right\|_{\ell_p(X)} := \Big(\sum_{i\in\mathbb{N}} \|x_i\|_X^p\Big)^{1/p} < \infty.$$

Some other classical Banach spaces include the space of p-integrable functions, L_p, as well as its vector valued generalization, $L_p(X)$, being X a Banach space. For our purposes, it is enough to define the latter as the Banach space of measurable functions on a measure space M, $f : M \to X$, such that

$$\|f\|_{L_p(X)} := \left(\int_M \|f(t)\|_X^p \, \mathrm{d}\mu(t)\right)^{\frac{1}{p}},$$

for an (implicitly) given measure μ. Notice that fixing M to be the set of natural numbers endowed with the discrete measure with unit weights, we recover the definition of $\ell_p(X)$ spaces.

2.1.2 Operator spaces

From the perspective of pure maths, the technical contributions appearing in this thesis can be mainly circumscribed to the local theory of *Banach* spaces. Nonetheless, some of the constructions appearing later are properly understood only within the context of operator spaces. This explains the need to provide a brief introduction to that matter. We redirect the interested reader to the standard references [34, 88] for an in-depth exposition on operator spaces.

An operator space is a complex Banach space X together with a sequence of *reasonable* norms on the spaces $\mathbb{M}_n \otimes X = \mathbb{M}_n(X)$ for any $n \in \mathbb{N}$, where $\mathbb{M}_n(X)$ is the space of $n \times n$ matrices with entries in X.

Reasonable here means that these matrix norms satisfy the following properties for any n, $m \in \mathbb{N}$ and any $x \in \mathbb{M}_n(X)$, $y \in \mathbb{M}_m(X)$:

- $\|x \oplus y\|_{\mathbb{M}_{n+m}(X)} \leq \max(\|x\|_{\mathbb{M}_n(X)}, \|y\|_{\mathbb{M}_m(X)})$;
- for any $\alpha \in \mathbb{M}_{m,n}$, $\beta \in \mathbb{M}_{n,m}$,
$$\|\alpha\, x\, \beta\|_{\mathbb{M}_m(X)} \leq \|\alpha\|_{\mathbb{M}_{m,n}} \|x\|_{\mathbb{M}_n(X)} \|\beta\|_{\mathbb{M}_{n,m}}.$$

Setting up this sequence of norms turns out to be equivalent to consider X as a closed subspace of some $\mathcal{B}(\mathcal{H})$ via a chosen isometric embedding (this equivalence was originally proven in [129]). This embedding fixes the matrix norm $\mathbb{M}_n(X)$ as the norm inherited from the embedding $\mathbb{M}_n(X) \subset \mathbb{M}_n(\mathcal{B}(\mathcal{H})) \simeq \mathcal{B}(\ell_2^n(\mathcal{H}))$. The precise choice of a sequence of reasonable norms $(\mathbb{M}_n(X))_{n\in\mathbb{N}}$, – equivalently, the isometric identification of X as a subspace of $\mathcal{B}(\mathcal{H})$ – defines an *operator space structure* (o.s.s) on X.

The natural morphisms in the category of operator spaces that are compatible with this additional structure are the completely bounded (cb) maps. Given a linear map between operator spaces $\Phi : X \to Y$, we define its completely bounded norm as $\|f\|_{cb} := \sup_n \|\mathrm{Id}_{\mathbb{M}_n} \otimes f : \mathbb{M}_n(X) \to \mathbb{M}_n(Y)\|$. Thus, the cb maps are those for which $\|f\|_{cb} < \infty$, and we denote them by $\mathcal{CB}(X, Y)$. Additionally, we say that a map is completely contractive if $\|f\|_{cb} \leq 1$ and it is a complete isometry if $\mathrm{Id}_{\mathbb{M}_n} \otimes \Phi : \mathbb{M}_n(X) \to \mathbb{M}_n(Y)$ is an isometry for all $n \in \mathbb{N}$. Finally, cb maps provides us also with the notion of duality for an operator space X. The *operator space* X^* is determined such that $\mathbb{M}_n(X^*) = \mathcal{CB}(X, \mathcal{S}_\infty^n)$ for any $n \in \mathbb{N}$. It is a basic result that the completely bounded norm coincides with the usual operator norm when the range is a commutative C*-algebra – see, for instance, [34, Proposition 2.2.6]. In particular, $\mathcal{CB}(X, \mathbb{C}) \simeq \mathcal{B}(X, \mathbb{C})$ isometrically, showing that the duality between operator spaces restricted to the first matrix level ($n = 1$ above) coincides with the duality as Banach spaces.

Some particular operator spaces. Following a structure similar to the previous section, we now introduce some particular operator spaces that will appear in subsequent sections. In first place, we make the observation that the Banach space $\mathcal{B}(\mathcal{H})$ carries over a natural o.s.s., the one inherited from the identification $\mathbb{M}_n(\mathcal{B}(\mathcal{H})) \simeq \mathcal{B}(\ell_2^n(\mathcal{H}))$[1]. This trivial observation has the interesting consequence of providing us with a natural o.s.s. also in the spaces $\mathcal{S}_\infty(\mathcal{H})$ and $\mathcal{S}_1(\mathcal{H})$. In the first case, the o.s.s. can be fixed regarding $\mathcal{S}_\infty(\mathcal{H})$ as the closed subspace of $\mathcal{B}(\mathcal{H})$ of compact operators. Then, $\mathcal{S}_1(\mathcal{H})$ inherits a natural o.s.s. as the dual of $\mathcal{S}_\infty(\mathcal{H})$, where the dual action is given by $\langle A, B\rangle = \mathrm{Tr} A\, B^t$, denoting by B^t the transpose of B.

It is now crucial to remark that, in general, for an arbitrary Banach space X, there is no privileged way to endow X with an o.s.s. In fact, we encounter many different o.s.s. on the same Banach space[2]. Apart from the spaces $\mathcal{B}(\mathcal{H})$, $\mathcal{S}_\infty(\mathcal{H})$ and $\mathcal{S}_1(\mathcal{H})$, we briefly discuss the case of the Hilbert space $\mathcal{H}$. There are two o.s.s. on $\mathcal{H}$ that we use later on in Section 2.4. These are the *row* and *column* o.s.s., denoted $R(\mathcal{H})$ and $C(\mathcal{H})$, respectively. $R(\mathcal{H})$ is defined via the *row* embedding:

$$\mathcal{H} \simeq \mathcal{B}(\mathcal{H}, \mathbb{C}), \tag{2.1}$$

while $C(\mathcal{H})$ is defined by the *column* embedding:

$$\mathcal{H} \simeq \mathcal{B}(\mathbb{C}, \mathcal{H}). \tag{2.2}$$

We simplify the notation to R and C when the Hilbert space involved is separable and to R_n, C_n when it is the finite dimensional ℓ_2^n.

These last two operator spaces turn out to be non-isomorphic, on the contrary to what happens at the Banach level, where they are simply Hilbert spaces. Despite that, they are still dual between themselves, that is, $C^* \simeq R$ and $C \simeq R^*$ completely isometrically.

For the sake of completeness, we briefly comment on the possibility of endowing the spaces ℓ_p, $\ell_p(X)$ and $\mathcal{S}_p(\mathcal{H})$ with an o.s.s. via complex

[1] Furthermore, for any C*-algebra the GNS representation provides us with a canonical isometric embedding into $\mathcal{B}(\mathcal{H})$, and therefore, we can also endow the C*-algebra with a natural o.s.s.

[2] Interestingly, Paulsen showed that this is always the case for any operator space of dimension ≥ 5 [77], a result that was refined to any dimension ≥ 3 in [93]. There, Pisier also commented on the striking fact that the only known examples of Banach spaces with unique o.s.s. are ℓ_1^2 and ℓ_∞^2. According to the recent [95], this seems to be still the state of the art regarding this innocent-looking question.

interpolation starting with $\mathcal{S}_1(\mathcal{H})$ and $\mathcal{S}_\infty(\mathcal{H})$ as extreme cases. Once again, this was firstly realized by G. Pisier in [91].

2.2 Type and cotype of a Banach space

The notion of type and cotype becomes central in this thesis, appearing at the core of the results presented in upcoming chapters. This notion is probabilistic in nature and it is a way to study certain geometric properties of Banach spaces. The development of a systematic theory of type/cotype traces back to the work of J. Hoffmann-Jørggensen, S. Kwapień, B. Maurey and G. Pisier in the 1970's.

We are concerned here with Rademacher random variables that are random variables taking values -1 and 1 with probability $1/2$ each. We usually denote by $(\varepsilon_i)_{i=1}^n$ a family of i.i.d. such random variables. Typically we will be interested on the expected value of some real valued function of such random variables, $f : \{-1,1\}^{\times n} \to \mathbb{R}$, denoting it as $\mathbb{E} f\Big((\varepsilon)_{i=1}^n\Big)$ or $\mathbb{E}_\varepsilon\, f\Big((\varepsilon)_{i=1}^n\Big)$ when we want to make explicit reference to the random variables in which the expected value acts. More concretely, denoting $\varepsilon = (\varepsilon_i)_{i=1}^n$, $\mathbb{E}_\varepsilon f(\varepsilon) = \frac{1}{2^n}\sum_{\varepsilon\in\{\pm 1\}^n} f(\varepsilon)$.

Given that, we introduce now the notion of type and cotype of a Banach space.

Definition 2.1. *Let X be a Banach space and let $1 \le p \le 2$. We say X is of type p if there exists a positive constant* T *such that for every natural number n and every sequence $\{x_i\}_{i=1}^n \subset X$ we have*

$$\left(\mathbb{E}\Big[\Big\|\sum_{i=1}^n \varepsilon_i x_i\Big\|_X^2\Big]\right)^{1/2} \le \mathrm{T}\left(\sum_{i=1}^n \|x_i\|_X^p\right)^{1/p}.$$

The infimum of the constants T *fulfilling the previous inequality is the type-p constant of X, denoted as* $\mathrm{T}_p(X)$.

The notion of type of a normed space finds a dual notion in the one of cotype:

For $2 \leq q < \infty$*, X is of cotype q if there exists a positive constant* C *such that for every natural number n and every sequence $\{x_i\}_{i=1}^n \subset X$,*

$$\mathrm{C}^{-1}\Big(\sum_{i=1}^n \|x_i\|_X^q\Big)^{1/q} \leq \bigg(\mathbb{E}_\varepsilon\Big[\Big\|\sum_{i=1}^n \varepsilon_i x_i\Big\|_X^2\Big]\bigg)^{1/2}.$$

The infimum of the constants C *is the cotype-q constant of X, denoted as* $\mathrm{C}_q(X)$*.*

If the number of elements x_i in the definitions above is restricted to be lower than or equal to some natural number m, we obtain the related notion of *type/cotype constants of X with m vectors*, denoted here as $\mathrm{T}_p^{(m)}(X)$ and $\mathrm{C}_q^{(m)}(X)$. Although frequently is enough to work with the notion of type/cotype constants, sometimes we will need to make use of the more precise latter notion.

Remark 2.2. An alternative characterization of the type-p constant of a Banach space X is given by the norm of the linear map:

$$\begin{array}{rccc} \mathrm{Rad}: & \ell_p(X) & \longrightarrow & L_2(X) \\ & (x_i)_i & \mapsto & \sum_i \varepsilon_i\, x_i \end{array},$$

where $\{\varepsilon_i\}_i$ are i.i.d. Rademacher random variables and[3]

$$\Big\|\sum_i \varepsilon_i\, x_i\Big\|_{L_2(X)} := \bigg(\mathbb{E}_\varepsilon\Big\|\sum_i \varepsilon_i x_i\Big\|_X^2\bigg)^{\frac{1}{2}}.$$

With that, the following equivalence is clear:

$$\mathrm{T}_p(X) = \|\mathrm{Rad} : \ell_p(X) \longrightarrow L_2(X)\|.$$

We use this equivalent definition for $\mathrm{T}_p(X)$ in our discussion on the behaviour of type constants with respect to the method of complex interpolation, in Section 2.3.

[3] Formally, to establish this identification we can consider a realization of the random variables ε_i as real valued functions on the interval $[0,1]$. A standard choice is setting $\varepsilon_i(t) = \mathrm{sign}\big(\sin(2^i\pi t)\big)$. In that way, for a function ϕ of the random variable ε, $\mathbb{E}_\varepsilon\phi(\varepsilon) = \int_0^1 \phi(\varepsilon(t))\mathrm{d}t$, which makes the connection with L_p spaces.

Basic properties regarding type and cotype. In latter chapters we will be very interested in the study of type constants of certain Banach spaces. In sight of that, we collect some properties of type constants that will be relevant for us.

The following proposition follows straightforwardly from Definition 2.1.

Proposition 2.3. *$\mathrm{T}_p(X)$ is preserved by subspaces. That is, if S is a subspace of X, then $\mathrm{T}_p(S) \leq \mathrm{T}_p(X)$.*

The following result also follows easily from the definition of type constant:

Proposition 2.4. *Given a linear isomorphism between two Banach spaces X and Y, $\Phi : X \to Y$, the following relation between type constants holds:*

$$\mathrm{T}_p(X) \leq \|\Phi\| \|\Phi^{-1}\| \, \mathrm{T}_p(Y). \tag{2.3}$$

Proof. Let us assume that Y has type p constant $\mathrm{T}_p(Y)$. Then, for any n and any family $\{x_i\}_{i=1}^n \subset X$ we note that, since Φ is an isomophism, for any i there exist an $y_i \in Y$ such that $x_i = \Phi^{-1}(y_i)$. Then,

$$\begin{aligned}
\left(\mathbb{E}\left[\Big\| \sum_{i=1}^n \varepsilon_i x_i \Big\|_X^2 \right] \right)^{1/2} &= \left(\mathbb{E}\left[\Big\| \sum_{i=1}^n \varepsilon_i \Phi^{-1}(y_i) \Big\|_X^2 \right] \right)^{1/2} \\
&\leq \|\Phi^{-1}\| \left(\mathbb{E}\left[\Big\| \sum_{i=1}^n \varepsilon_i y_i \Big\|_X^2 \right] \right)^{1/2} \\
&\leq \|\Phi^{-1}\| \mathrm{T}_p(Y) \Big(\sum_{i=1}^n \|y_i\|_Y^p \Big)^{1/p} \\
&= \|\Phi^{-1}\| \mathrm{T}_p(Y) \Big(\sum_{i=1}^n \|\Phi(x_i)\|_Y^p \Big)^{1/p} \\
&\leq \|\Phi\| \|\Phi^{-1}\| \mathrm{T}_p(Y) \Big(\sum_{i=1}^n \|x_i\|_X^p \Big)^{1/p}.
\end{aligned}$$

Since $\mathrm{T}_p(X)$ is by definition the smallest constant satisfying the inequality above, the stated inequality must hold and we conclude our proof. □

As we have already announced before, there exists some kind of duality between type and cotype. In particular, we can state the following:

Proposition 2.5. *Given a Banach space X and* $1 < p \leq 2,\ 2 \leq q < \infty\ :\ \frac{1}{p} + \frac{1}{q} = 1$,

$$\mathrm{C}_q(X^*) \leq \mathrm{T}_p(X).$$

On the contrary, the reverse inequality fails in general – a classical example is given by the spaces ℓ_1 and ℓ_∞. However, it turns out that such a relation can be made true *up to logarithmic* factors:

Proposition 2.6. *Given a finite dimensional Banach space X and* $1 < p \leq 2,\ 2 \leq q < \infty\ :\ \frac{1}{p} + \frac{1}{q} = 1$,

$$\mathrm{T}_p(X) \leq c \log(\dim(X))\, \mathrm{C}_q(X^*),$$

for some universal constant c.

See [64, Section 6] for a proof of the previous two results. In a historical note, we comment that the latest is a direct consequence of Pisier's studies on the notion of K-convexity and its relation with type and cotype, see [86].

Type constants of some specific Banach spaces. To finish the present section we state some well-known estimates of the type and cotype constants of some classical spaces. We begin with the case of Hilbert spaces. Any Hilbert space $\mathcal{H}$ satisfies that $\mathrm{C}_2(\mathcal{H}) = 1 = \mathrm{T}_2(\mathcal{H})$. Actually something deeper can be said in this case: Any Banach space of type 2 and cotype 2 is isomorphic to a Hilbert space, result that was proven by Kwapień in [58].

A situation in which type and cotype properties are also remarkably well understood is the case of ℓ_p spaces. The following bounds are well-known, see [115, Section 4]:

Considering $1 \leq p \leq 2$ and $2 \leq q \leq \infty$ such that $\frac{1}{p} + \frac{1}{q} = 1$,

$$n^{\frac{1}{r} - \frac{1}{p}} \leq \mathrm{T}_p(\ell_r^n) \leq c\, r^{\frac{1}{2}}\, n^{\frac{1}{r} - \frac{1}{p}} \qquad \text{when } r \in [1, 2], \tag{2.4}$$

$$\mathrm{C}_q(\ell_r^n) \leq c\, q \qquad \text{when } r \in [1, 2], \tag{2.5}$$

and

$$\begin{aligned} \mathrm{T}_p(\ell_r^n) &\leq r^{\frac{1}{2}} && \text{when } r \in [2,\infty), && (2.6)\\ n^{\frac{1}{r}-\frac{1}{p}} \leq \mathrm{C}_q(\ell_r^n) &\leq c\, q\, n^{\frac{1}{r}-\frac{1}{q}} && \text{when } r \in [2,\infty], && (2.7) \end{aligned}$$

being c an independent constant.

Considering the previous estimates, the following bound can be easily obtained for the type constants of ℓ_∞^n:

$$(\log n)^{1-\frac{1}{p}} \leq \mathrm{T}_p(\ell_\infty^n) \leq c\,(\log n)^{\frac{1}{2}}, \quad 1 \leq p \leq 2. \tag{2.8}$$

We provide next a short proof.

Proof. For simplicity, we consider in the proof the Banach space ℓ_∞^n to be real. The same argument applies for the complex case with minor adjustments.

The first inequality follows from identifying in ℓ_∞^n an isometric copy of $\ell_1^{\log(n)}$. The bound is obtained from the estimates (2.4) taking into account Proposition 2.3.

For the second inequality we use the fact that the Banach-Mazur distance between ℓ_r^n and ℓ_∞^n is $n^{\frac{1}{r}}$, for $r \geq 2$. With that, and Proposition 2.4, we can obtain:

$$\mathrm{T}_p(\ell_\infty^n) \leq n^{\frac{1}{r}} \mathrm{T}_p(\ell_r^n) \leq n^{\frac{1}{r}} r^{\frac{1}{2}}.$$

The claim follows considering $r = \log(n)$. □

N. Tomczak-Jaegermann proved in [114] that Schatten classes behave with respect to type and cotype in a similar way than their commutative analogues, the previously discussed ℓ_p spaces. In particular, the estimates in Equations (2.4)–(2.7) still apply for $\mathcal{S}_r^n$ spaces instead of ℓ_r^n. This is also true for the estimate (2.8)[4] . Of special relevance for upcoming chapters are the following two particular cases, that we explicitly state here for future reference:

$$\mathrm{T}_2(\mathcal{S}_1^n) = n^{\frac{1}{2}}, \qquad (\log(n))^{\frac{1}{2}} \leq \mathrm{T}_2(\mathcal{S}_\infty^n) \leq c\,(\log(n))^{\frac{1}{2}}, \tag{2.9}$$

[4] To adapt the proof above, notice that the Banach-Mazur distance between Schatten classes also behaves exactly in the same way as in the case of ℓ_p spaces.

where c is an independent constant. In the rectangular case $\mathcal{S}_r^{n,m}$, one realizes that the relevant dimension is given by the minimum between n and m. More precisely, the following bounds hold:

$$\mathrm{T}_2(\mathcal{S}_1^{n,m}) = \min(n,m)^{\frac{1}{2}},$$
$$(\log(\min(n,m)))^{\frac{1}{2}} \leq \mathrm{T}_2(\mathcal{S}_\infty^{n,m}) \leq c\,(\log(\min(n,m)))^{\frac{1}{2}}.$$

2.3 Interpolation of Banach spaces

The content of previous sections will be enough to develop Chapter 3, but later on, in Chapter 4, we will make use of some more involved constructions for which we give a basic introduction in the following two sections.

Interpolation methods have proven very useful in many areas of functional analysis and their appearance in this thesis is motivated by the good behaviour of type constants with respect to them. Here we restrict ourselves to the study of the *complex interpolation space* $(X_0, X_1)_\theta$ for $0 < \theta < 1$ and finite dimensional Banach spaces X_0, X_1. We decided to avoid a full treatment of the rather cumbersome definition of this space and focus on stating some natural properties it displays. That is enough for the scope of this work. We redirect the interested reader to the classical references [9, 116].

In our case, in which X_0, X_1 are finite dimensional, the space $(X_0, X_1)_\theta$ can always be constructed. In the general case, for arbitrary Banach spaces, if we still can define $(X_0, X_1)_\theta$ we say that the couple (X_0, X_1) is compatible[5], so we fix this terminology from now on. For the sake of concreteness, here we will consider the case in which X_0, X_1 and $(X_0, X_1)_\theta$ are algebraically the same space but endowed with different norms. The complex interpolation method, that assigns to any compatible couple (X_0, X_1) the space $(X_0, X_1)_\theta$, is an *exact interpolation functor of exponent θ.* This means that it satisfies the following:

[5] Technically, this condition is usually stated as the requirement that X_0 and X_1 embed continuously in a common Hausdorff topological vector space.

Theorem 2.7 ([9], Thm. 4.1.2.). *For any compatible couples* $(X_0,\, X_1)$, $(Y_0,\, Y_1)$, *and any linear map* $f : (X_0, X_1)_\theta \to (Y_0, Y_1)_\theta$*:*

$$\Big\| f : (X_0, X_1)_\theta \to (Y_0, Y_1)_\theta \Big\| \leq \Big\| f : X_0 \to Y_0 \Big\|^{1-\theta} \, \Big\| f : X_1 \to Y_1 \Big\|^{\theta}.$$

Now we turn our attention to the classical sequence ℓ_p spaces. Interpolation in this case becomes remarkably natural. We have the isometric identification $\ell_p = (\ell_\infty,\, \ell_1)_{1/p}$ for any $1 \leq p \leq \infty$. Indeed, such an identification follows in a much more general setting, as the following theorem states:

Theorem 2.8 ([9], Thm. 5.1.2.). *For any compatible couple* $(X_0,\, X_1)$, $p_0,\, p_1 \in [1, \infty]$ *and* $\theta \in (0, 1)$ *the following identification is isometric:*

$$\Big(L_{p_0}(X_0),\, L_{p_1}(X_1) \Big)_\theta = L_p\Big((X_0,\, X_1)_\theta \Big),$$

where $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$.

Identifying $\ell_p(X)$ spaces as particular vector valued Lebesgue spaces $L_p(X)$, we can translate the previous statement also to this case:

$$\Big(\ell_{p_0}(X_0),\, \ell_{p_1}(X_1) \Big)_\theta = \ell_p\Big((X_0,\, X_1)_\theta \Big), \tag{2.10}$$

where $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$.

Pleasantly, an analogue result for Schatten classes is also true.

Theorem 2.9 ([92], Cor. 1.4.). *For* $p_0,\, p_1 \in [1, \infty]$ *and* $\theta \in (0, 1)$ *the following identification is isometric:*

$$(\mathcal{S}_{p_0},\, \mathcal{S}_{p_1})_\theta = \mathcal{S}_p,$$

where $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$.

Our interest now turns into the interaction between type and interpolation. We state the following general known result:

Proposition 2.10. *Let* X_0, X_1 *be an interpolation couple, where* X_i *has type* p_i *for some* $1 \leq p_i \leq 2$, $i = 0,\, 1$. *Let* $0 < \theta < 1$ *and* $1 < p < 2$ *be* *such that* $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$. *Then,*

$$\mathrm{T}_p\left((X_0, X_1)_\theta\right) \leq \left(\mathrm{T}_{p_0}(X_0)\right)^{1-\theta} \left(\mathrm{T}_{p_1}(X_1)\right)^{\theta}.$$

The proof follows easily from the interpolation properties of vector valued ℓ_p and L_p spaces. We decided to include a simple proof next.

Proof. As said in Section 2.2, the type-p constant of a Banach space X can be understood as the norm of the mapping:

$$\begin{array}{rccc} \mathrm{Rad}: & \ell_p(X) & \longrightarrow & L_2(X) \\ & (x_i)_i & \mapsto & \sum_i \varepsilon_i\, x_i \end{array},$$

where $\{\varepsilon_i\}_i$ are i.i.d. Rademacher random variables and

$$\|\sum_i \varepsilon_i\, x_i\|_{L_2(X)} := \left(\mathbb{E}_\varepsilon \Big\| \sum_i \varepsilon_i x_i \Big\|_X^2\right)^{\frac{1}{2}}.$$

Then, we write

$$\mathrm{T}_p\left((X_0, X_1)_\theta\right) = \left\|\mathrm{Rad}: \ell_p\left((X_0, X_1)_\theta\right) \longrightarrow L_2\left((X_0, X_1)_\theta\right)\right\|.$$

Taking into account the equivalences (Theorem 2.8):

$$\ell_p\left((X_0, X_1)_\theta\right) = \left(\ell_{p_0}(X_0), \ell_{p_1}(X_1)\right)_\theta, \qquad L_2\left((X_0, X_1)_\theta\right) = \left(L_2(X_0), L_2(X_1)\right)_\theta,$$

we can bound:

$$\begin{aligned} &\left\|\mathrm{Rad}: \ell_p\left((X_0, X_1)_\theta\right) \longrightarrow L_2\left((X_0, X_1)_\theta\right)\right\| \\ &\quad \leq \left\|\mathrm{Rad}: \ell_{p_0}(X_0) \longrightarrow L_2(X_0)\right\|^{1-\theta} \left\|\mathrm{Rad}: \ell_{p_1}(X_1) \longrightarrow L_2(X_1)\right\|^{\theta} \\ &\quad = \left(\mathrm{T}_{p_0}(X_0)\right)^{1-\theta} \left(\mathrm{T}_{p_1}(X_1)\right)^{\theta}, \end{aligned}$$

where Theorem 2.7 was used in the first inequality. □

2.4 Operator ideals

In Chapter 4 we will make use of some constructions coming from the theory of ideals of operators between Banach spaces and tensor norms. These are nowadays fundamental structures in local Banach space theory whose origins are traced back to the work of Schatten [103] and, independently, to Grothendieck's *Résumé* [40] – from the point of view of tensor norms. Later, Pietsch further developed a systematic theory from the point of view of operator ideals [82]. In this section we introduce some basic definitions and particular examples that will be relevant to us. We mainly base the discussion below on references [83, 30], where the interested reader can find further details. What cannot be found there is the content of the end of this section, where we introduce what we have called *weak-cb Schatten-von Neumman operators*. That is a notion that arises naturally from the study in Chapter 4 and that, to the best of our knowledge, did not appear before in the literature. This class of operators is a natural extension of the classical weak Schatten-von Neumman operators when elements from operator space theory are incorporated. It turns out that precisely this new class describes the basic structures in our study of cheating strategies in Position Based Cryptography, cf. Chapter 4.

Recall that $\mathcal{B}(X, Y)$ denotes the Banach space of bounded operators between Banach spaces X and Y. An *operator ideal* can be thought of as an assignment α that associates to any pair of Banach spaces X, Y, a subspace of $\mathcal{B}(X, Y)$, $\alpha(X, Y)$, that has the *ideal* property of being closed under composition with bounded linear maps. This assignment is further called a *normed operator ideal* when it additionally endows $\alpha(X, Y)$ with a norm $\| \cdot \|_{\alpha(X,Y)}$ satisfying the property:

$$\|T \circ S \circ R\|_{\alpha(X_0,Y_0)} \leq \|T\| \|S\|_{\alpha(X,Y)} \|R\|, \tag{2.11}$$

for any $T \in \mathcal{B}(Y, Y_0)$, $S \in \mathcal{B}(X, Y)$, $R \in \mathcal{B}(X_0, X)$. Above $\| \cdot \|$ denotes the operator norm. When $\alpha(X, Y)$ is complete w.r.t. the ideal norm we refer to ir as a *Banach operator ideals*.

Changing the subject for a moment, we consider now the tensor product of Banach spaces and the fundamental notion of *tensor norm*. Later, we will see that there is an intimate relation between tensor norms and normed operator ideals, as introduced above. We start expanding on the discussion in Section 1.1.1 of tensor product of vector spaces in order to include the general infinite dimensional case. With a clear resemblance to the finite dimensional case, we can define $X \otimes Y$ as the vector space of finite linear combinations of elements of the type $x \otimes y$, where $x \in X$ and $y \in Y$, when the linear structure is determined by the identities:

$$\begin{aligned}(\lambda_1 x_1 + \lambda_2 x_2) \otimes y &= \lambda_1\, x_1 \otimes y + \lambda_2\, x_2 \otimes y,\\ x \otimes (\lambda_1 y_1 + \lambda_2 y_2) &= \lambda_1\, x \otimes y_1 + \lambda_2\, x \otimes y_2,\end{aligned}$$

for any scalars λ_1, λ_2 and vectors x, x_1, $x_2 \in X$, y, y_1, $y_2 \in Y$.

Now we summarize some customary ways to look at elements in $X \otimes Y$. Firstly, and very importantly for us, an arbitrary tensor $u = \sum_{i=1}^n x_i \otimes y_i \in X \otimes Y$ unequivocally defines a map[6]

$$\begin{array}{rccc} f_u: & X^\sharp & \longrightarrow & Y \\ & x & \mapsto & \sum_{i=1}^n \langle x | x_i \rangle\, y_i. \end{array}$$

Therefore, $X \otimes Y$ can be seen as a subspace of $\mathscr{L}(X^\sharp, Y)$ – it is in fact the subspace of finite rank operators in $\mathscr{L}(X^\sharp, Y)$. This observation can be subsumed in the inclusion

$$X \otimes Y \subseteq \mathscr{L}(X^\sharp, Y). \tag{2.12}$$

It is clear that, in a similar way, $X \otimes Y$ can be also identified with the space of finite rank operators in $\mathscr{L}(Y^\sharp, X)$.

Apart from that, we can also identify $u = \sum_{i=1}^n x_i \otimes y_i \in X \otimes Y$ with a bilinear form $b_u \in \mathscr{B}i\ell(X^\sharp \times Y^\sharp)$ defined by

$$\begin{array}{rccc} b_u: & X^\sharp \times Y^\sharp & \longrightarrow & \mathbb{C} \\ & (x, y) & \mapsto & \sum_{i=1}^n \langle x | x_i \rangle \langle y | y_i \rangle. \end{array}$$

That is, we also have the inclusion

$$X \otimes Y \subseteq \mathscr{B}i\ell(X^\sharp \times Y^\sharp). \tag{2.13}$$

[6] Recall that the symbol $\sharp$ denotes the algebraic dual of a vector space.

When X, Y are, in addition, Banach spaces, one is invited to think about $X \otimes Y$ also as a Banach space. However, the normed structure on the tensor product $X \otimes Y$ is far from being uniquely determined by those of X and Y separately, as we show next. A first natural way to set a norm on $X \otimes Y$ is endowing $\mathscr{L}(X^*, Y)$ with the operator norm and promoting the embedding

$$X \otimes Y \subseteq \mathscr{B}(X^*, Y),$$

to an isometry. By these means, $X \otimes Y$ inherites a norm. This norm is usually called the *injective tensor norm* and the resulting Banach space (after completion when necessary), denoted here as $X \otimes_\varepsilon Y$.

In contrast, we can also endow $X \otimes Y$ with a norm by imposing the natural condition: for any $x \in X$, $y \in Y$,

$$\|x \otimes y\| \leq \|x\|\,\|y\|.$$

The largest norm that still fulfils this property is given by the following definition: for any $u \in X \otimes Y$,

$$\|u\|_{X \otimes_\pi Y} := \inf \Big\{ \sum_i \|x_i\|_X \|y_i\|_Y \ : \ u = \sum_i x_i \otimes y_i \Big\}. \tag{2.14}$$

This is called the *projective tensor norm*, and the resulting Banach space will be denoted here by $X \otimes_\pi Y$.

It is easy to check that the previous norms satisfy also the *metric mapping property*: being $\alpha = \varepsilon$ or π, for any Banach spaces X_0, X_1, Y_0, Y_1, and any operators $f \in \mathscr{B}(X, X_0)$, $g \in \mathscr{B}(Y, Y_0)$,

$$\| f \otimes g : X \otimes_\alpha Y \to X_0 \otimes_\alpha Y_0 \| \leq \|f\|\,\|g\|. \tag{2.15}$$

More generally, there are several ways to endow $X \otimes Y$ with a norm compatible with the local norms on X and Y. We say that an assignment α that associates to $X \otimes Y$ a norm $\alpha(X, Y)$ for any pair of Banach spaces, is a *tensor norm* if it satisfies the following two properties:

- α is *in between* of the injective and projective tensor norms, that is,

$$\text{for any } x \in X \otimes_\alpha Y, \ \ \|x\|_{X\otimes_\varepsilon Y} \leq \|x\|_{X\otimes_\alpha Y} \leq \|x\|_{X\otimes_\pi Y};$$

- α satisfies the metric mapping property (2.15).

The resulting Banach space in each case is denoted $X \otimes_\alpha Y$. Later on, in Chapter 4, Section 4.7, we will more generally refer to tensor norms as norms defined *tensorizing* consecutively different tensor norms. For example, if α, α' are tensor norms, the assignment on any three Banach spaces X, Y, Z of the norm $(X \otimes_\alpha Y) \otimes_{\alpha'} Z$ will be called also tensor norm.

Tensor norms act as basic building blocks that allow us to understand Banach spaces from a different standpoint, emerging a deeper understanding from this shift of perspective. This point is cleanly illustrated by the following example.

Example 2.11. The tensor product structure of the spaces $\mathcal{S}_1$ and $\mathcal{S}_\infty$. Recall that $\mathcal{S}_1$ and $\mathcal{S}_\infty$ are subspaces of $\mathcal{B}(\ell_2, \ell_2)$. On one hand, $\mathcal{S}_\infty$ is the norm-closed subspace of bounded compact operators on ℓ_2. In this case, this subspace is the same as the norm closure of the space of finite rank operators[7], but this is nothing else than the definition of the injective tensor product of ℓ_2 with itself, i.e., $\mathcal{S}_\infty \simeq \ell_2 \otimes_\varepsilon \ell_2$.

On the other hand, $\mathcal{S}_1$ was defined as the norm-closed subspace of compact operators with finite $\|\cdot\|_{\mathcal{S}_1}$ norm. Remind that this norm was defined as the ℓ_1-sum of singular values. A careful look at (2.14) particularized to $X = \ell_2 = Y$ reveals that the infimum is attained at the value $\sum_{i\in\mathbb{N}} s_i(f) = \|f\|_{\mathcal{S}_1}$. This is easy to show for finite rank operators. For that, consider the singular value decomposition in the optimization present in (2.14). The case of arbitrary compact operators follows from considering a sequence of finite rank operators converging to the original compact operator.

In conclusion, we have the following very important isometric identifications:

$$\mathcal{S}_\infty \simeq \ell_2 \otimes_\varepsilon \ell_2, \quad \mathcal{S}_1 \simeq \ell_2 \otimes_\pi \ell_2.$$

[7] This can be seen as a consequence of ℓ_2 being a space with the approximation property, see, for instance, [102].

Now we revisit the relation (2.12) between tensor products and spaces of operators to remark that tensor norms and Banach operator ideals are in fact two sides of the same coin. Under the identification (2.12) the metric mapping property is precisely the ideal property (2.11) understood at the level of tensor products. In fact, in the category of finite dimensional Banach spaces, tensor norms and operator ideals are in one-to-one correspondence. As usual, things become subtler in the infinite dimensional case, although a tight relation between both notions still exists in this case, see [30, Section 17] for further information. Based on that, we will tend to present our results making explicit the underlying tensor product structure, although sometimes, especially in this preliminary chapter, it will be more natural to look at some Banach spaces as operator ideals.

Apart from the injective and projective norms introduced before, another classical tensor norm that will briefly appear in Chapter 4 is the *2-summing norm*: the space $\pi_2(X^*, Y)$ is the space of operators $f \in \mathscr{B}(X^*, Y)$ such that

$$\|f\|_{\pi_2(X^*,Y)} := \Big\|\mathrm{Id} \otimes f : \ell_2 \otimes_\varepsilon X^* \to \ell_2(Y)\Big\| < \infty. \tag{2.16}$$

According to the notation set before, we can also refer to this Banach space as $X \otimes_{\pi_2} Y$.

In the next few lines, we restrict ourselves to spaces of operators between Hilbert spaces. In this setting, let us recall the Schatten classes introduced in Section 2.1.1, denoted as $\mathcal{S}_p(\mathcal{H})$ for $1 \le p \le \infty$. These spaces satisfy the ideal property (2.11), although they are not Banach operator ideals in the sense above: Schatten classes endow with a norm any pair of Hilbert spaces but not arbitrary Banach spaces. A way to generalize Schatten classes to spaces of linear maps between arbitrary Banach spaces is provided by *weak Schatten-von Neumman* operators, as defined next:

Definition 2.12. *Given an operator $f : X \to Y$ and $1 \le p \le \infty$ we say that f is of weak Schatten-von Neumann type ℓ_p if*

$$\|f\|_{\mathfrak{S}_p^w(X,Y)} := \sup\left\{ \left\| \Big(s_i(g \circ f \circ h) \Big)_i \right\|_{\ell_p} \; : \; \begin{array}{c} \|g : Y \to \ell_2\| \le 1 \\ \|h : \ell_2 \to X\| \le 1 \end{array} \right\} < \infty,$$

where $\big(s_i(g\circ f\circ h)\big)_i$ *is the sequence of singular values of the operator* $g\circ f\circ h:\ell_2\longrightarrow\ell_2$.

We denote by $\mathfrak{S}_p^w(X,Y)$ *the space of operators* $f:X\longrightarrow Y$ *of weak Schatten-von Neumann type* ℓ_p. $\mathfrak{S}_p^w(X,Y)$*the space of operators of weak Schatten-von Neumann type* ℓ_p *from* X *into* Y

See e.g. [83] for a discussion on the properties of these spaces. Here, Definition 2.12 serves us to motivate the following class of operators that has appeared in the study of strategies for Position Based Cryptography – Chapter 4 – and that seems to be new in the literature. Its definition, while based on Definition 2.12, incorporates elements of the theory of operators spaces. Moreover, while this space of operators does not satisfy the ideal property (2.11) it does satisfy an equivalent ideal property in the category of operator spaces, underlining the fact that this construction belongs more naturally to this latter category. For the definition, recall that R and C denote the row and column operator spaces over the separable Hilbert space ℓ_2:

Definition 2.13. *Given an operator between operator spaces* $f:X\to Y$ *and* $1\le p\le\infty$ *we say that* f *is of weak-cb Schatten-von Neumann type* ℓ_p *if*

$$\|f\|_{\mathfrak{S}_p^{w-cb}(X,Y)}:=\sup\left\{\Big\|\left(s_i\left(g\circ f\circ h\right)\right)_i\Big\|_{\ell_p}\ :\ \begin{array}{c}\Big\|g:Y\longrightarrow C\Big\|_{cb}\le 1\\ \Big\|h:R\longrightarrow X\Big\|_{cb}\le 1\end{array}\right\}$$
$$<\infty,$$

where $\big(s_i(g\circ f\circ h)\big)_i$ *is the sequence of singular values of the operator* $g\circ f\circ h:\ell_2\longrightarrow\ell_2$.

We denote by $\mathfrak{S}_p^{w-cb}(X,Y)$ *the space of operators* $f:X\longrightarrow Y$ *of weak-cb Schatten-von Neumann type* ℓ_p.

It is straightforward to see that $\|\cdot\|_{\mathfrak{S}_p^{w-cb}(X,Y)}$ is in fact a norm. The following ideal property also follows easily from the previous definition:

Proposition 2.14. *Given operator spaces* X_0, Y_0, X, Y *and elements* $f\in\mathcal{CB}(Y,Y_0)$, $g\in\mathfrak{S}_p^{w-cb}(X,Y)$, $h\in\mathcal{CB}(X_0,X)$:

$$\|f\circ g\circ h\|_{\mathfrak{S}_p^{w-cb}(X_0,Y_0)}\le\|f\|_{cb}\,\|g\|_{\mathfrak{S}_p^{w-cb}(X,Y)}\,\|h\|_{cb}.$$

Notice the appearance of the completely bounded norm in contrast with (2.11).

Proof of Proposition 2.14. We only need to explicit Definition 2.13 for $f \circ g \circ h \in \mathscr{L}(X_0, Y_0)$ – for notational convenience, we restate the ℓ_p sum of the singular value of the operator involved as the $\mathcal{S}_p$ norm of that operator:

$$\begin{aligned}\|f \circ g \circ h\|_{\mathfrak{S}_p^{w-cb}(X_0,Y_0)} &= \sup \|r \circ f \circ g \circ h \circ s\|_{\mathcal{S}_p} \\ &= \|f\|_{cb}\|h\|_{cb} \sup \left\| \left(\frac{r \circ f}{\|f\|_{cb}}\right) \circ f \circ \left(\frac{h \circ s}{\|h\|_{cb}}\right) \right\|_{\mathcal{S}_p}.\end{aligned}$$

The supremum (in both lines) is taken over maps $r \in \mathsf{ball}(\mathscr{CB}(Y_0, C))$, $s \in \mathsf{ball}(\mathscr{CB}(R, X_0))$. Notice that, thanks to the normalization in the second line above, $\frac{r \circ f}{\|f\|_{cb}} \in \mathsf{ball}(\mathscr{CB}(Y, C))$ and $\frac{h \circ s}{\|h\|_{cb}} \in \mathsf{ball}(\mathscr{CB}(R, X))$. Therefore, the previous expression is upper bounded by

$$\|f\|_{cb}\|h\|_{cb} \sup \|r \circ g \circ s\|_{\mathcal{S}_p},$$

where now the supremum runs over maps $r \in \mathsf{ball}(\mathscr{CB}(Y, C))$, $s \in \mathsf{ball}(\mathscr{CB}(R, X))$. However, this is nothing but $\|f\|_{cb}\|h\|_{cb}\|g\|_{\mathfrak{S}_p^{w-cb}(X,Y)}$, which is the stated bound. □

Next, we look at the relation between $\mathfrak{S}_p^{w-cb}(X, Y)$ and some other more standard norms. In first place, we can readily notice that, since ball $(\mathscr{CB}(X, Y)) \subseteq \mathsf{ball}(\mathscr{B}(X, Y))$ for any operator spaces X, Y, the following inequality holds for any $1 \leq p \leq \infty$ and any $f \in \mathfrak{S}_p^{w-cb}(X, Y)$:

$$\|f\|_{\mathfrak{S}_p^{w-cb}(X,Y)} \leq \|f\|_{\mathfrak{S}_p^{w}(X,Y)}. \tag{2.17}$$

A bit less obvious is the following relation with the interpolation space $(X \otimes_\varepsilon Y, X \otimes_\pi Y)_{\frac{1}{p}}$.

Proposition 2.15. *Given finite dimensional operator spaces X, Y, for any $1 \leq p \leq \infty$ and any $f \in \mathscr{L}(X, Y)$,*

$$\|f\|_{\mathfrak{S}_p^{w-cb}(X,Y)} \leq \|f\|_{\mathfrak{S}_p^{w}(X,Y)} \leq \|f\|_{(X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{p}}}.$$

Proof. We have already established the first inequality in previous comments. Therefore we focus on the second inequality.

According to the definition of $\mathfrak{S}_p^w(X,Y)$, Definition 2.12, we can write:

$$\|f\|_{\mathfrak{S}_p^w(X,Y)} = \sup_{\substack{g\in \mathsf{ball}(\mathcal{B}(Y,\ell_2))\\ h\in \mathsf{ball}(\mathcal{B}(\ell_2,X))}} \|g\circ f\circ h\|_{\mathcal{S}_p} = \sup_{\substack{g\in \mathsf{ball}(\mathcal{B}(Y,\ell_2))\\ h\in \mathsf{ball}(\mathcal{B}(\ell_2,X))}} \|g\circ f\circ h\|_{(\mathcal{S}_\infty,\mathcal{S}_1)_{\frac{1}{p}}},$$

where we have used Theorem 2.9 to state the last equality.

The map $g\circ f\circ h : \ell_2 \to \ell_2$ can be interpreted, as a tensor, as the image of the mapping $h^*\otimes g : X^*\otimes Y \to \ell_2\otimes\ell_2$ acting on f. Then, the previous expression can be written as:

$$\begin{aligned}\|f\|_{\mathfrak{S}_p^w(X,Y)} &= \sup_{\substack{g\in \mathsf{ball}(\mathcal{B}(Y,\ell_2))\\ h\in \mathsf{ball}(\mathcal{B}(\ell_2,X))}} \|(h^*\otimes g)(f)\|_{(\mathcal{S}_\infty,\mathcal{S}_1)_{\frac{1}{p}}}\\ &\leq \|f\|_{(X^*\otimes_\varepsilon Y, X^*\otimes_\pi Y)_{\frac{1}{p}}}\\ &\quad \sup_{\substack{g\in \mathsf{ball}(\mathcal{B}(Y,\ell_2))\\ h\in \mathsf{ball}(\mathcal{B}(\ell_2,X))}} \|h^*\otimes g : (X^*\otimes_\varepsilon Y, X^*\otimes_\pi Y)_{\frac{1}{p}} \to (\mathcal{S}_\infty,\mathcal{S}_1)_{\frac{1}{p}}\|.\end{aligned}$$

Now, it only remains to show that for any contractions $h^* : X^*\to\ell_2$, $g : Y\to\ell_2$

$$\|h^*\otimes g : (X^*\otimes_\varepsilon Y, X^*\otimes_\pi Y)_{\frac{1}{p}} \to (\mathcal{S}_\infty,\mathcal{S}_1)_{\frac{1}{p}}\| \leq 1.$$

This follows from the interpolation property, Theorem 2.7:

$$\begin{aligned}&\|h^*\otimes g : (X^*\otimes_\varepsilon Y, X^*\otimes_\pi Y)_{\frac{1}{p}} \to (\mathcal{S}_\infty,\mathcal{S}_1)_{\frac{1}{p}}\|\\ &\quad\leq \|h^*\otimes g : X^*\otimes_\varepsilon Y \to \mathcal{S}_\infty\|^{\frac{p-1}{p}} \|h^*\otimes g : X^*\otimes_\pi Y \to \mathcal{S}_1\|^{\frac{1}{p}},\end{aligned}$$

together with the understanding of $\mathcal{S}_\infty$ and $\mathcal{S}_1$ as the tensor products $\ell_2\otimes_\varepsilon\ell_2$ and $\ell_2\otimes_\pi\ell_2$, respectively. This allows us to bound

$$\|h^*\otimes g : X^*\otimes_\varepsilon Y \to \mathcal{S}_\infty\| \leq \|h^* : X^*\to\ell_2\|\ \|g : Y\to\ell_2\| \leq 1,$$

thanks to the metric mapping property displayed by the injective tensor norm. Analogously

$$\|h^* \otimes g : X^* \otimes_\pi Y \to \mathcal{S}_1\| \leq \|h^* : X^* \to \ell_2\| \ \|g : Y \to \ell_2\| \leq 1.$$

Hence, the claim in the statement follows. □

The last remark we make here concerns with the more specific setting that appears in Chapter 4. There, we will be interested in the case in which $p = 2$ and $X^* = Y = \mathcal{S}_1^{n,m}$, that is, we study the space $\mathfrak{S}_2^{w-cb}(\mathcal{S}_\infty^{n,m}, \mathcal{S}_1^{n,m})$. Equivalently, we use next the notation $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{n,m}$. The lemma is a simple characterization of the norm in Definition 2.13 that brings it closer to the setting analysed later on:

Lemma 2.16. *Given a tensor $f \in \mathcal{S}_1^{n,m} \otimes \mathcal{S}_1^{n,m}$, where $\mathcal{S}_1^{n,m}$ is endowed with its natural o.s.s., we have that:*

$$\|f\|_{\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{n,m}} = \sup_{\substack{r \in \mathbb{N} \\ g,h \in \mathsf{ball}(\mathcal{S}_\infty^{nr,m})}} \Big\| (h \otimes g)(f) \Big\|_{\ell_2^{r^2}}.$$

Above, the action of $h = \sum_{i=1}^n \sum_{j=1}^r \sum_{l=1}^m h_{ijl} |ij\rangle\langle l| \in \mathcal{S}_\infty^{nr,m}$ on a tensor $t = \sum_{i=1}^n \sum_{j=1}^m t_{ij} |i\rangle\langle j| \in \mathcal{S}_1^{n,m}$ is defined by

$$h(t) := \sum_{j=1}^r \left(\sum_{i=1}^n \sum_{l=1}^m h_{ijl} t_{ijl} \right) |j\rangle \in \ell_2^r.$$

Proof. The claim follows from the following observations:

- a standard argument shows that the supremum in Definition 2.13 can be taken over finite dimensional C_r and R_r, where $r \in \mathbb{N}$ is arbitrarily large;
- for an operator between Hilbert spaces, as $g \circ f \circ h$ in Definition 2.13, the ℓ_2-sum of the singular values coincide with the Hilbert-Schmidt norm of the operator, which is the same as the Euclidean norm of the associated tensor. In our case, with a slight abuse of notation, the relevant tensor is $(h \otimes g)(f)$;
- finally, when we set $X = \mathcal{S}_\infty^{n,m}$, $Y = \mathcal{S}_1^{n,m}$ in Definition 2.13, the optimization is carried over elements $g \in \mathsf{ball}(\mathscr{CB}(\mathcal{S}_1^{n,m}, C_r))$

ans $h \in \mathsf{ball}(\mathscr{CB}(R_r, \mathcal{S}_\infty^{n,m}))$. But now, it is again a standard result that the following are complete isometries [34, Section 9.3]: $\mathscr{CB}(\mathcal{S}_1^{n,m}, C_r) \simeq \mathcal{S}_\infty^{nr,m} \simeq \mathscr{CB}(R_r, \mathcal{S}_\infty^{n,m})$. The claim of the lemma is obtained acting with g, h viewed as elements in $\mathsf{ball}(\mathcal{S}_\infty^{nr,m})$ as defined in the statement.

□

Chapter 3

Resource quantification for the no-programming theorem

This chapter reflects joint work with C. Palazuelos and D. Pérez-García. In particular, its content is mainly based on the publication [57].

The no-programming theorem prohibits the existence of a Universal Programmable Quantum Processor. This statement has several implications in relation to quantum computation, but also to other tasks of quantum information processing, making this construction a central notion in this context. Nonetheless, it is well known that even when the strict model is not implementable, it is possible to conceive of it in an approximate sense. Unfortunately, the minimal resources necessary for this aim are still not completely understood. In this chapter, we investigate quantitative statements of the theorem, improving exponentially previous bounds on the resources required by such a hypothetical machine. The results presented here are based on a new connection between quantum channels and embeddings between Banach spaces that allows us to use classical tools from geometric Banach space theory in a clean and simple way. More concretely, we characterize Universal Programmable Quantum Processors as approximate isometric embeddings of the Banach space $\mathcal{S}_1^d$ into subspaces of $\mathcal{S}_\infty^m$.

We summarise the contents of this chapter. After setting the problem we study and providing an overview of previous related work in Section

3.1, in Section 3.2 we outline the results that will be obtained here. Section 3.3 is devoted to introducing the necessary formal definitions. In Section 3.4 the characterization of Universal Programmable Quantum Processors as approximate isometric embeddings is obtained. With that, the main results of this chapter are obtained in Section 3.5. We finish with some final remarks in Section 3.6.

3.1 Background and previous work

Since the early days of Quantum Information Theory, no-go theorems have served as guideline in the search of a deeper understanding of quantum theory as well as for the development of applications of quantum mechanics to cryptography and computation. They shed light on those aspects of quantum information which make it so different from its classical counterpart. Some renowned examples are the no-cloning [41, 32, 70, 123, 63], no-deleting [75] and no-programming [72] theorems.

The no-programming theorem concerns with the so-called Universal Programmable Quantum Proccesor, UPQP[1]. A UPQP is a universal machine able to perform any quantum operation on an arbitrary input state of fixed size, programming the desired action in a quantum register inside the machine (a quantum memory). It can be understood as the quantum version of a stored-program computer. For the sake of simplicity, we will consider programmability of unitary operations, although this is not really a restrictive assumption[2]. With this figure of merit, the no-programming theorem is stated as the non-existence of a UPQP using finite dimensional resources. The key observation made in [72] is that in order to program two different unitaries we need two orthogonal program states. Then, the infinite cardinality of the set of unitary operators, even in the simplest case of a qubit, leads immediately to the requirement of an infinite dimensional memory. Similar consequences follow for the related concept of Universal Programmable Quantum Measurements [33, 36, 29], which are machines with the capability to be programmed to implement arbitrary quantum measurements.

[1] Originally called Programmable Quantum Gate Array [72].

[2] Even in this case we could program general quantum channels implementing a unitary first and tracing out a part of the output.

From a conceptual point of view, the no-programming theorem points out severe limitations in how universal quantum computation can be conceived. However, these limitations can be surpassed by relaxing the requirements on the model of UPQP. In particular, one can consider programmable devices working noisily or probabilistically. Indeed, in the last two decades, several proposals of such approximate UPQPs have appeared in the literature [72, 54, 42, 13, 8, 122, 45]. Thus, it is interesting to look for more quantitative statements about *quantum programmability*. To put it in explicit words, we worry here about the relation between the memory size of an approximate UPQP, m, and both, the accuracy of the scheme, ϵ, and the size of the input register in which we want to implement the program, d. Despite their relevance, these relations are still poorly understood. Existing results are summarized in Table 3.1.

3.2 Summary of results

In this chapter we provide new upper and lower bounds which substantially clarify the ultimate resources required by approximate UPQPs. See the second column in Table 3.1. Our results entail exponential improvements over previously known results, narrowing significantly the optimal dependence of m with parameters ϵ and d separately. In fact, the lower bound provided by Theorem 3.11 is nearly saturated for fixed ϵ by the performance of Port Based Teleportation, which was originally conceived as a UPQP [45]. On the other hand, in Proposition 3.9 we deduce an upper bound that saturated almost optimally the scaling with ϵ of the bound from [80].

Our proofs are based on a connection with geometric functional analysis that we uncover. The use of techniques from this branch of functional analysis, in particular, from Banach space theory and operator spaces - as it is the case here - have proven to be very fruitful in the study of different aspects of quantum information such as entanglement theory, quantum non-locality and quantum channel theory (see [3, 74] and references therein). We find the path to put forward this mathematical technology to the framework studied here. More precisely, we *characterize* UPQPs as isometric embeddings between concrete Banach spaces which

	Previous results		This thesis	
Lower bounds	$m \geq \mathsf{K}(\frac{1}{d})^{\frac{d+1}{2}} \left(\frac{1}{\epsilon}\right)^{\frac{d-1}{2}}$ $m \geq \mathsf{K}\left(\frac{d}{\epsilon}\right)^2$	[80] [62]	$m \geq 2^{\frac{(1-\epsilon)}{\mathsf{K}}d-\frac{2}{3}\log d}$	[Th.3.11]
Upper bounds	$m \leq 2^{\frac{4d^2 \log d}{\epsilon^2}}$	[45, 5, 27]	$m \leq \left(\frac{\mathsf{K}}{\epsilon}\right)^{d^2}$	[Prop.3.9]

Table 3.1 Best known bounds for the optimal memory size of UPQPs in comparison with the results presented here. Above, K denotes universal constants, not necessarily equal between them. Let us point out that the bound from [80] was deduced for programmable measurements instead of UPQPs. However, since a UPQP can always be turned into a Universal Programmable Quantum Measurement, this lower bound also applies for the case studied here. Notice that the alluded bound, although it enforces a strong scaling of m with ϵ, becomes trivial for large input dimension d. It is in this regime where the bound from [62] is more informative, but still exponentially weaker than the bound provided by Theorem 3.11.

are in addition complete contractions (considering some operator space structure). Once this characterization is established, the results about UPQPs are deduced comparing the type-2 constant of the spaces involved in the embeddings. We think that the general ideas presented here and potential generalizations of them can provide further insights in other contexts related with quantum computation and cryptography. A first step in this direction will be taken in Chapter 4, where some of the ideas and techniques of the present chapter are used in the study of Position Based Cryptography.

3.3 Universal Programmable Quantum Processors, UPQPs

We will consider repeatedly a d-dimensional complex Hilbert space ℓ_2^d as input state space, and an ancillary m-dimensional complex Hilbert space ℓ_2^m as the memory of the programmable device under consideration. We recall that logarithms are taken in base 2.

We start formally defining the objects we study later on. Firstly, we provide a rigorous definition for UPQPs:

Definition 3.1. *A quantum operation $\mathcal{P} \in \mathrm{CPTP}(\ell_2^d \otimes \ell_2^m)$ is a d-dimensional Universal Programmable Quantum Processor,* UPQP_d*, if for every $U \in \mathcal{U}(\ell_2^d)$ there exists a unit vector $|\phi_U\rangle \in \ell_2^m$ such that:*

$$\mathrm{Tr}_{\ell_2^m}\left[\mathcal{P}\left(\rho \otimes |\phi_U\rangle\langle\phi_U|\right)\right] = U\rho U^\dagger, \quad \textit{for every} \;\; \rho \in \mathcal{D}(\ell_2^d).$$

Essentially, this is the concept of Universal Quantum Gate Array introduced in [72], and whose impossibility is the content of the no-programming theorem discovered also there. As we said in the previous section, the no-programming theorem does not apply if one considers a relaxation of the previous definition; that is, in the case of approximate UPQPs. Two notions of approximate UPQPs have been considered in the literature: probabilistic settings [72, 43], which implement exactly the desired unitary with some probability of failure, obtaining information about the success or failure of the procedure; and deterministic UPQPs [121], which always implement an operation which is close to the desired one. Notice that both notions are related, since probabilistic UPQPs can be also understood as deterministic ones just ignoring the information about the success or failure of the computation. A natural way to express these notions of approximation is through the distance induced by the diamond norm, recall Definition 1.21:

Definition 3.2. *Given* $0 < \epsilon \leq 1$*, we say that* $\mathcal{P} \in \mathrm{CPTP}(\ell_2^d \otimes \ell_2^m)$ *is a* d*-dimensional* ϵ*–Universal Programmable Quantum processor,* $\epsilon - \mathrm{UPQP}_d$*, if for every* $U \in \mathcal{U}(\ell_2^d)$ *there exists a unit vector* $|\phi_U\rangle \in \ell_2^m$ *such that:*

$$\frac{1}{2}\left\|\mathrm{Tr}_{\ell_2^m}\left[\mathcal{P}\left(\,\cdot\,\otimes|\phi_U\rangle\langle\phi_U|\right)\right]\; - \; U(\,\cdot\,)U^\dagger\right\|_\diamond \leq \epsilon,$$

where $\|\,\cdot\,\|_\diamond$ *denotes the* diamond norm*.*

Two illustrative examples of approximate UPQPs are given next:

Example 3.3. Standard teleportation as a (probabilistic) $\epsilon - \mathrm{UPQP}_d$ [72]. It was observed by Nielsen and Chuang that the celebrated quantum teleportation protocol can be arranged in a probabilistic UPQP in the following way: we proceed to teleport a qudit state $|\psi\rangle \in \ell_2^d$ by means of a d^2 dimensional maximally entangled state $|\varphi\rangle = \sum_{i=1}^{d^2}|ii\rangle \in \ell_2^d \otimes \ell_2^d$. Now, instead of carrying the usual teleportation protocol we apply the desired unitary, $U \in \mathcal{U}(\ell_2^{d^2})$, to the part of the resource state receiving the teleported input, $|\varphi\rangle \to |\varphi_U\rangle = (id_d \otimes U)|\varphi\rangle$. Then, we continue with the teleportation protocol but without correcting the output, obtaining $U|\psi\rangle$ in the second part of the resource state with probability $\frac{1}{d^2}$. This is an ϵ–UPQP with $\epsilon = 1 - \frac{1}{d}$.

Example 3.4. Port Based Teleportation [45]. The interesting protocol of Port Based Teleportation was originally conceived as an approximate UPQP. Here, an input state $|\psi\rangle \in \ell_2^d$ is again teleportated by means of a resource state $|\varphi\rangle \in (\ell_2^d)^{\otimes N} \otimes (\ell_2^d)^{\otimes N}$, but now, the correcting operations after the teleportation consists simply on discarding any of the N d-dimensional systems of the second part of the resource state except one, determined by the outcome of a POVM measured at the other side of the protocol. Taking advantage of the commutativity of the partial trace applied in the correction step with $(id_{d^N} \otimes U^{\otimes N})$, we can encode the desired unitary $U \in \mathcal{U}(\ell_2^{d^2})$ – before the teleportation is performed – in the state $|\varphi_U\rangle = (id_{d^N} \otimes U^{\otimes N})|\varphi\rangle$. The result is a noisy version of $U|\psi\rangle$ that provides us with an $\epsilon -$ UPQP$_d$ where the relation between the error ϵ and the dimension of the resource space is $m = O\Big(\exp(d^2 \log d/\epsilon^2)\Big)$ [5, 27].

Notice that in the first case, the resources used are remarkably efficient. The counterpart is that the success probability (accuracy of the setting) is rather low. In contrast, in the second example the accuracy can be arbitrarily improved at the prize of increasing the dimension of the resource state. These examples show the rich landscape of behaviours displayed by UPQPs, which turns the understanding of these objects challenging. The results presented here shed new light on them.

3.4 UPQPs and ϵ-embeddings

In this section we establish the key connection between $\epsilon -$ UPQP$_d$ and isometric embeddings between Banach spaces, that is at the heart of the proofs of our main results.

The crucial ingredient is the characterization of UPQP$_d$ as isometric embeddings $\Phi : \mathcal{S}_1^d \hookrightarrow \mathcal{S}_\infty^m$ with completely bounded norm $\|\Phi\|_{cb} \leq 1$, i.e., complete contractions. For $\epsilon -$ UPQP$_d$, the characterization holds distorting the isometric property of the embedding with some disturbance $\delta(\epsilon)$. This characterization is obtained in Theorems 3.5 and 3.6 below.

The appearance of the completely bounded norm here is due to the *completely isometric* identification $\mathcal{S}_\infty(\ell_2^d \otimes \ell_2^m) \simeq \mathcal{CB}\left(\mathcal{S}_1^d, \mathcal{S}_\infty^m\right)$. This constitutes the starting point in establishing the characterization proved in this section. The identification is established putting any $V \in \mathcal{S}_\infty(\ell_2^d \otimes \ell_2^m)$ in one-to-one correspondence with the linear map[3]

$$\begin{array}{rccl} \Phi_V : & \mathcal{S}_1^d & \hookrightarrow & \mathcal{S}_\infty^m \\ & \sigma & \mapsto & \Phi_V(\sigma) := \mathrm{Tr}_{\ell_2^d} V(\sigma^{\mathrm{T}} \otimes \mathrm{Id}_{\ell_2^m}). \end{array} \tag{3.1}$$

Given this, the completely bounded norm of Φ_V can be simply regarded as $\|\Phi_V\|_{cb} = \|V\|_{\mathcal{S}_\infty(\ell_2^d \otimes \ell_2^m)}$, see [34, Proposition 8.1.2].

[3] Algebraically, this is precisely the identification between tensors and linear maps discussed in Chapter 2, (2.12) (applied twice). In this case we have an identification rather than an inclusion because we are dealing here with finite dimensional spaces.

The rest of this section is devoted to prove Theorems 3.5, 3.6. Firstly, in Theorem 3.5 we associate to any $\epsilon-\mathrm{UPQP}_d$ an approximate isometric embedding $\Phi : \mathcal{S}_1^d \to \mathcal{S}_\infty^m$.

Theorem 3.5. *Every unitary* $\epsilon - \mathrm{UPQP}_d$*, given by* $\mathcal{P}(\,\cdot\,) = V(\,\cdot\,)V^\dagger \in \mathrm{CPTP}(\ell_2^d \otimes \ell_2^m)$*, defines a completely contractive map* $\Phi_V : \mathcal{S}_1^d \longrightarrow \mathcal{S}_\infty^m$ *such that*

$$\|\sigma\|_{\mathcal{S}_1^d} \geq \|\Phi_V(\sigma)\|_{\mathcal{S}_\infty^m} \geq (1-\epsilon)^{1/2}\|\sigma\|_{\mathcal{S}_1^d}$$

for every $\sigma \in \mathcal{S}_1^d$*. Such a map is called a completely contractive* ϵ*-embedding.*

Proof. Given a unitary channel $\mathcal{P}(\,\cdot\,) = V(\,\cdot\,)V^\dagger$, we consider the map $\Phi_V :\ \mathcal{S}_1^d \longrightarrow \mathcal{S}_\infty^m$ defined by

$$\Phi_V(\,\cdot\,) := \mathrm{Tr}_{\ell_2^d} V(\,\cdot^{\mathrm{T}}\, \otimes \mathrm{Id}_{\ell_2^m}).$$

The completely bounded norm of $\Phi_V :\ \mathcal{S}_1^d \longrightarrow \mathcal{S}_\infty^m$ coincides with $\|V\|_{\mathcal{S}_\infty^{dm}} = 1$. Thus, Φ_V is completely contractive. In addition, since

$$\|\Phi_V :\ \mathcal{S}_1^d \to \mathcal{S}_\infty^m\| \leq \|\Phi_V :\ \mathcal{S}_1^d \to \mathcal{S}_\infty^m\|_{cb} = 1,$$

we immediately deduce that $\|\Phi_V(\sigma)\|_{\mathcal{S}_\infty^m} \leq \|\sigma\|_{\mathcal{S}_1^d}$ for every $\sigma \in \mathcal{S}_1^d$.

For the second inequality in the statement, we elaborate on the norm:

$$\left\|\Phi_V(\sigma)\right\|_{\mathcal{S}_\infty^m} = \sup \left\|\mathrm{Tr}_{\ell_2^d}\left[V\left(\sigma^{\mathrm{T}} \otimes \mathrm{Id}_{\ell_2^m}\right)\right]|\xi\rangle\right\|_{\ell_2^m},$$

where the supremum is taken over unit vectors $|\xi\rangle \in \ell_2^m$. Now, we consider the singular value decomposition of $\sigma^{\mathrm{T}} = \sum_i \mu_i |\psi_i\rangle\langle\gamma_i|$, being $(|\psi_i\rangle)_{i=1}^d$, $(|\gamma_i\rangle)_{i=1}^d$ orthonormal bases of ℓ_2^d. Therefore $|\gamma_i\rangle = U|\psi_i\rangle$ for some unitary U. Furthermore, we can take $\mu_i \geq 0$ and then $\sum_i \mu_i = \|\sigma^{\mathrm{T}}\|_{\mathcal{S}_1^d} = \|\sigma\|_{\mathcal{S}_1^d}$, which can be assumed to be, obtaining the general case by homogeneity. Besides, it is convenient to express σ^{T} as

$$\begin{aligned}\sigma^{\mathrm{T}} &= \sum_i \mu_i |\psi_i\rangle\langle\psi_i|U^\dagger \\ &= \mathrm{Tr}_{\mathcal{K}}\Big(\sum_i \sqrt{\mu_i}|i\rangle_{\mathcal{K}}|\psi_i\rangle\Big)\Big(\sum_j \sqrt{\mu_j}\langle j|_{\mathcal{K}}\langle\psi_j|U^\dagger\Big) = \mathrm{Tr}_{\mathcal{K}}|\psi\rangle\langle\gamma|, \quad (3.2)\end{aligned}$$

where we have considered a new auxiliary Hilbert space $\mathcal{K}$ and have defined $|\psi\rangle := \sum_i \sqrt{\mu_i}|i\rangle_{\mathcal{K}}|\psi_i\rangle$, $|\gamma\rangle := (\mathrm{Id}_{\mathcal{K}} \otimes U)|\psi\rangle$. Now, we are ready to rewrite

$$\begin{aligned}
&\left\|\Phi_V(\sigma)\right\|_{\mathcal{S}_\infty^m} \\
&= \sup_{|\xi\rangle\in\mathsf{ball}(\ell_2^m)} \left\|\mathrm{Tr}_{\mathcal{K}\otimes\ell_2^d}\left[(\mathrm{Id}_{\mathcal{K}}\otimes V)(|\psi\rangle\langle\gamma|\otimes \mathrm{Id}_{\ell_2^m})\right]|\xi\rangle\right\|_{\ell_2^m} \\
&= \sup_{|\xi\rangle\in\mathsf{ball}(\ell_2^m)} \left[\mathrm{Tr}\left[(|\gamma\rangle\langle\gamma|\otimes \mathrm{Id}_{\ell_2^m})(\mathrm{Id}_{\mathcal{K}}\otimes V)(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|)(\mathrm{Id}_{\mathcal{K}}\otimes V^\dagger)\right]\right]^{\frac{1}{2}} \\
&\geq \left[\mathrm{Tr}\left[(|\gamma\rangle\langle\gamma|\otimes \mathrm{Id}_{\ell_2^m})(\mathrm{Id}_{\mathcal{K}}\otimes V)(|\psi\rangle\langle\psi|\otimes|\xi_U\rangle\langle\xi_U|)(\mathrm{Id}_{\mathcal{K}}\otimes V^\dagger)\right]\right]^{\frac{1}{2}},
\end{aligned} \tag{3.3}$$

where $|\xi_U\rangle$ is the state associated to U in the definition of $\epsilon - \mathrm{UPQP}_d$, Definition 3.2.

At this point, we appeal to the operational interpretation of the distance induced by the diamond norm given by Theorem 1.22. In fact, it turns out that (3.3) can be understood in terms of the optimal probability p^*_{dist} of distinguishing the channel $\mathcal{P}_{|\xi_U\rangle}(\,\cdot\,) := \mathrm{Tr}_{\ell_2^m} V(\,\cdot\, \otimes |\xi_U\rangle\langle\xi_U|)V^\dagger$ from the ideal channel $U(\,\cdot\,)U^\dagger$. We claim that

$$\|\Phi_V(\sigma)\|_{\mathcal{S}_\infty^m} \geq \sqrt{2}(1-p^*_{dist})^{1/2}. \tag{3.4}$$

With this estimate at hand, we can easily finish our proof since, according to the operational characterization of the diamond distance, Theorem 1.22, we obtain

$$\left\|\Phi_V(\sigma)\right\|_{\mathcal{S}_\infty^m} \geq \left(1 - \frac{1}{2}\left\|\mathcal{P}_{|\xi_U\rangle}(\,\cdot\,) - U(\,\cdot\,)U^\dagger\right\|_\diamond\right)^{\frac{1}{2}} \geq (1-\epsilon)^{\frac{1}{2}}\,.$$

To finish our proof, let us show claim (3.4). To this end, we recall the operational meaning of p^*_{dist}. A strategy to distinguish between channels $\mathcal{P}_{|\xi_U\rangle}(\,\cdot\,)$ and $U(\,\cdot\,)U^\dagger$ consists on: first, applying the channel received to a larger system $\mathcal{K}\otimes\ell_2^d$ prepared in a state of our choice, ρ; and then, measuring a dichotomic POVM to try to distinguish between states $\mathrm{Id}_{\mathcal{K}}\otimes\mathcal{P}_{|\xi_U\rangle}(\rho)$ and $(\mathrm{Id}_{\mathcal{K}}\otimes U)\,\rho\,(\mathrm{Id}_{\mathcal{K}}\otimes U^\dagger)$. Using such a strategy, we succeed at correctly distinguishing between given channels with some probability. p^*_{dist} is the supremum of that probability when optimizing over auxiliary spaces $\mathcal{K}$, states ρ and distinguishing POVMs. Therefore, p^*_{dist} can be lower bounded by the success probability attained by the particular strategy specified by:

- the state $|\psi\rangle\langle\psi| \in \mathfrak{D}(\mathcal{K} \otimes \ell_2^d)$ defined in (3.2);
- the POVM $\{|\gamma\rangle\langle\gamma|, \mathrm{Id}_{\mathcal{K}\otimes\ell_2^d} - |\gamma\rangle\langle\gamma|\}$, where $|\gamma\rangle \in \mathcal{K} \otimes \ell_2^d$ was also defined in (3.2).

Explicitly, we have that

$$\begin{aligned} p^*_{dist} &\geq \frac{1}{2}\mathrm{Tr}\Big[|\gamma\rangle\langle\gamma|\,(\mathrm{Id}_{\mathcal{K}} \otimes U)(|\psi\rangle\langle\psi|)(\mathrm{Id}_{\mathcal{K}} \otimes U^\dagger)\Big] \\ &+ \frac{1}{2}\mathrm{Tr}\Big[(\mathrm{Id} - |\gamma\rangle\langle\gamma|)\,(\mathrm{Id}_{\mathcal{K}} \otimes \mathcal{P}_{|\xi_U\rangle}(|\psi\rangle\langle\psi|))\Big] \\ &= 1 + \frac{1}{2}\mathrm{Tr}\Big[|\gamma\rangle\langle\gamma|\Big(\mathrm{Id}_{\mathcal{K}} \otimes \mathcal{P}_{|\xi_U\rangle}(|\psi\rangle\langle\psi|)\Big)\Big], \end{aligned}$$

where we can recognize the last expression in (3.3) recalling that $\mathcal{P}_{|\xi_U\rangle}(\,\cdot\,) = \mathrm{Tr}_{\ell_2^m}\Big[V(\,\cdot\,\otimes|\xi_U\rangle\langle\xi_U|)V^\dagger\Big]$. Claim (3.4) follows now straightforwardly. □

The previous theorem is the basis for our main results about the performance of UPQPs, that will be presented in Section 3.4. Before that, we find next a converse to Theorem 3.5 that promotes the relation between UPQPs and ϵ-embeddings (in the sense of Theorem 3.5) to a *characterization.*

Theorem 3.6. *Every completely contractive map $\Phi : \mathcal{S}_1^d \longrightarrow \mathcal{S}_\infty^m$ such that*

$$\|\sigma\|_{\mathcal{S}_1^d} \geq \|\Phi(\sigma)\|_{\mathcal{S}_\infty^m} \geq (1-\delta)\|\sigma\|_{\mathcal{S}_1^d}$$

for every $\sigma \in \mathcal{S}_1^d$, defines an $\epsilon - \mathrm{UPQP}_d$ with $\epsilon = \sqrt{2\delta}$ and memory dimension at most m^2.

The statement can be proved combining the two lemmas we state next, for which we fix two finite dimensional Hilbert spaces $\mathcal{H}$, $\mathcal{K}$.

To motivate the first one, we begin with an elementary observation. Let $\mathcal{H}$ be a finite dimensional Hilbert space. Given an arbitrary tensor $\sigma \in \mathcal{S}_1(\mathcal{H})$ and considering its polar decomposition $\sigma = \rho U^\dagger$, being $\rho \geq 0$

and U a unitary operator, we can find a norming element for σ that is independent of its positive part, ρ. In particular, the norming element is simply given by U. That is, the norm of σ in $\mathcal{S}_1(\mathcal{H})$ can be computed as $\|\sigma\|_{\mathcal{S}_1(\mathcal{H})} = \langle U, \sigma \rangle = \operatorname{Tr} \rho$. The next lemma shows that this property is approximately preserved by ϵ-embeddings $\Phi : \mathcal{S}_1(\mathcal{H}) \to \mathcal{S}_\infty(\mathcal{K})$.

Lemma 3.7. *Consider an injective linear map $\Phi : \mathcal{S}_1(\mathcal{H}) \to \mathcal{S}_\infty(\mathcal{K})$ with bounded inverse Φ^{-1} when restricted to its range . Then, for any unitary $U \in \mathcal{U}(\mathcal{H})$ there exists an element $\Theta_U \in \mathcal{S}_1(\mathcal{K})$ with norm one satisfying that*

$$\|\Phi\| \operatorname{Tr} \rho \geq \langle \Theta_U, \Phi(\rho U^\dagger) \rangle \geq \frac{1}{\|\Phi^{-1}\|} \operatorname{Tr} \rho,$$

for any positive element $\rho \in \mathcal{S}_1(\mathcal{H})$. Above, $\|\Phi^{-1}\| := \left\| \Phi^{-1}|_{\Phi(\mathcal{S}_1(\mathcal{H}))} : \Phi(\mathcal{S}_1(\mathcal{H})) \subseteq \mathcal{S}_\infty(\mathcal{K}) \to \mathcal{S}_1(\mathcal{H}) \right\|$.

Proof. Consider a unitary $U \in \mathcal{U}(\mathcal{H})$. In virtue of the duality relation $\mathcal{S}_1(\mathcal{H})^* = \mathcal{S}_\infty(\mathcal{H})$ we can identify U with a linear map,

$$\begin{array}{rccl} u : & \mathcal{S}_1(\mathcal{H}) & \longrightarrow & \mathbb{C} \\ & \sigma & \mapsto & u(\sigma) := \langle U^{\mathrm{T}}, \sigma \rangle = \operatorname{Tr}[U\sigma] \end{array}$$

with norm one.

Given that, consider the map $u \circ \Phi^{-1} : \Phi(\mathcal{S}_1(\mathcal{H})) \subseteq \mathcal{S}_\infty(\mathcal{K}) \to \mathbb{C}$, that already fulfils:

$$u \circ \Phi^{-1}(\Phi(\rho U^\dagger)) = \operatorname{Tr} \rho, \text{ for any } 0 \leq \rho \in \mathcal{S}_1(\mathcal{H}).$$

Moreover, the norm of this map is upper bounded by $\|u \circ \Phi^{-1}\| \leq \|u\| \, \|\Phi^{-1}\| = \|\Phi^{-1}\|$.

To finish the proof, we extend $u \circ \Phi^{-1}$ to a map acting on the full space $\mathcal{S}_\infty(\mathcal{K})$, $\widetilde{u \circ \Phi^{-1}} : \mathcal{S}_\infty(\mathcal{K}) \to \mathbb{C}$. Such an extension is guaranteed by the Hahn-Banach theorem, that also provides us with the norm of the extended map: $\|\widetilde{u \circ \Phi^{-1}} : \mathcal{S}_\infty(\mathcal{K}) \to \mathbb{C}\| = \|u \circ \Phi^{-1} : \Phi(\mathcal{S}_1(\mathcal{H})) \to \mathbb{C}\| \leq$

$\|\Phi^{-1}\|$. This construction can be summarized in the following diagram:

$$\begin{tikzcd}
\mathcal{S}_1(\mathcal{H}) \arrow[r, "\Phi"] \arrow[d, "u"'] & \Phi(\mathcal{S}_1(\mathcal{H})) \arrow[dl, "u\circ\Phi^{-1}"] & \subseteq \mathcal{S}_\infty(\mathcal{K}) \arrow[dll, "\widetilde{u\circ\Phi^{-1}}"] \\
\mathbb{C} & &
\end{tikzcd}$$

Again, due to the duality $\mathcal{S}_\infty(\mathcal{K})^* \simeq \mathcal{S}_1(\mathcal{K})$, $\widetilde{u\circ\Phi^{-1}}/\|\widetilde{u\circ\Phi^{-1}}\|$ can be identified with an element in the unit sphere of $\mathcal{S}_1(\mathcal{K})$. This is the norming element Θ_U that we wanted. □

The second lemma associates to any linear map $\Phi : \mathcal{S}_1(\mathcal{H}) \to \mathcal{S}_\infty(\mathcal{K})$ with completely bounded norm one a channel with some programmability properties. Concretely:

Lemma 3.8. *Given a linear map $\Phi : \mathcal{S}_1(\mathcal{H}) \to \mathcal{S}_\infty(\mathcal{K})$ such that $\|\Phi : \mathcal{S}_1(\mathcal{H}) \to \mathcal{S}_\infty(\mathcal{K})\|_{cb} = 1$, there exists an associated channel $\mathcal{P}_\Phi \in \mathrm{CPTP}(\mathcal{H}\otimes\mathcal{K})$ verifying*

$$\frac{1}{2}\Big\|\mathrm{Tr}_{\mathcal{K}}[\mathcal{P}_\Phi(\,\cdot\,\otimes|\xi\rangle\langle\xi|)] - U(\,\cdot\,)U^\dagger\Big\|_\diamond \le \sup_{\substack{\rho\in\mathsf{ball}(\mathcal{S}_1(\mathcal{H}))\\ :\ \rho\ge 0}} \left(1 - \Big\|\Phi(\rho\, U^\dagger)\,|\xi\rangle\Big\|_{\mathcal{K}}^2\right)^{\frac{1}{2}}$$

for any unitary $U \in \mathcal{U}(\mathcal{H})$ and any unit vector $|\xi\rangle \in \mathcal{K}$.

Proof. We start constructing a channel associated to Φ. In view of the completely isometric identification $\mathcal{CB}(\mathcal{S}_1(\mathcal{H}), \mathcal{S}_\infty(\mathcal{K})) \simeq \mathcal{S}_\infty(\mathcal{H}\otimes\mathcal{K})$, we can identify Φ with a norm one operator $\hat{\Phi} \in \mathcal{S}_\infty(\mathcal{H}\otimes\mathcal{K})$ in such a way that

$$\Phi(\,\cdot\,) = \mathrm{Tr}_{\mathcal{H}}\hat{\Phi}(\,\cdot\,\otimes \mathrm{Id}_{\mathcal{K}}).$$

Furthermore, the Russo-Dye Theorem provides us with a decomposition of $\hat{\Phi}$ as a convex combination of at most $\dim\mathcal{H}\,\dim\mathcal{K}$ unitaries:

$$\hat{\Phi} = \sum_{i\in\mathcal{I}} \lambda_i\, V_i, \text{ for some unitaries } V_i \in \mathcal{S}_\infty(\mathcal{H}\otimes\mathcal{K}),$$

where $\mathcal{I}$ is an alphabet whose cardinal is no greater than $\dim\mathcal{H}\,\dim\mathcal{K}$.

Given that, consider the following unitary operator

$$V := \sum_{i\in\mathcal{I}} V_i \otimes |i\rangle\langle i| \,\in\, \mathscr{U}(\mathcal{H}\otimes\mathcal{K}\otimes\mathcal{H}_{\mathcal{I}}).$$

Together with the state $|\lambda\rangle\langle\lambda| := \sum_{k,l\in\mathcal{I}} \sqrt{\lambda_k\lambda_l}\,|k\rangle\langle l| \in \mathscr{D}(\mathcal{H}_{\mathcal{I}})$, we can now define the channel:

$$\mathcal{P}_\Phi(\,\cdot\,) := \mathrm{Tr}_{\mathcal{H}_{\mathcal{I}}} V\,(\,\cdot\otimes|\lambda\rangle\langle\lambda|)\,V^\dagger.$$

We prove next that this channel has the property stated in the lemma. Consider a density matrix $\rho\in\mathcal{S}_1(\mathcal{H})$ with purification $|\psi\rangle\in\mathcal{H}\otimes\mathcal{H}'$ such that $\rho = \mathrm{Tr}_{\mathcal{H}'}|\psi\rangle\langle\psi|$. Consider also a unitary $U\in\mathscr{U}(\mathcal{H})$ and a unit vector $|\xi\rangle\in\mathcal{K}$. We denote $|\gamma\rangle := U\otimes\mathrm{Id}_{\mathcal{H}'}|\psi\rangle$. We are interested now on bounding the fidelity $\mathcal{F}\Big(|\gamma\rangle\langle\gamma|, \mathrm{Tr}_{\mathcal{K}}[\mathcal{P}_\Phi\otimes\mathrm{Id}_{\mathcal{H}'}(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|)]\Big)$, where $\mathcal{F}(|\gamma\rangle\langle\gamma|,\rho) := (\mathrm{Tr}|\gamma\rangle\langle\gamma|\,\rho)^{\frac{1}{2}}$ for any positive $\rho\in\mathcal{S}_1(\mathcal{H}\otimes\mathcal{H}')$. Expanding on $\mathcal{P}_\Phi$ we have

$$\begin{aligned}
&\mathcal{F}\Big(|\gamma\rangle\langle\gamma|, \mathcal{P}_\Phi\otimes\mathrm{Id}_{\mathcal{H}'}(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|)\Big)\\
&\quad=\Bigg(\mathrm{Tr}\Big[\Big(|\gamma\rangle\langle\gamma|\otimes\mathrm{Id}_{\mathcal{K}}\otimes\mathrm{Id}_{\mathcal{H}_{\mathcal{I}}}\Big)\\
&\qquad\qquad\Big(V\otimes\mathrm{Id}_{\mathcal{H}'}(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|\otimes|\lambda\rangle\langle\lambda|)V^\dagger\otimes\mathrm{Id}_{\mathcal{H}'}\Big)\Big]\Bigg)^{\frac{1}{2}},
\end{aligned}$$

that can be lower bounded by:

$$\begin{aligned}
&\geq\Bigg(\mathrm{Tr}\Big[\Big(|\gamma\rangle\langle\gamma|\otimes\mathrm{Id}_{\mathcal{K}}\otimes|\lambda\rangle\langle\lambda|\Big)\\
&\qquad\qquad\Big(V\otimes\mathrm{Id}_{\mathcal{H}'}(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|\otimes|\lambda\rangle\langle\lambda|)V^\dagger\otimes\mathrm{Id}_{\mathcal{H}'}\Big)\Big]\Bigg)^{\frac{1}{2}}\\
&=\Bigg(\sum_{i,j}\lambda_i\lambda_j\mathrm{Tr}\Big[\Big(|\gamma\rangle\langle\gamma|\otimes\mathrm{Id}_{\mathcal{K}}\Big)\,V_i\otimes\mathrm{Id}_{\mathcal{H}'}\Big(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|\Big)V_j^\dagger\otimes\mathrm{Id}_{\mathcal{H}'}\Big]\Bigg)^{\frac{1}{2}}\\
&=\Big\|\sum_i\lambda_i\langle\gamma|V_i\otimes\mathrm{Id}_{\mathcal{H}'}|\psi\rangle|\xi\rangle\Big\|_{\mathcal{K}}=\Big\|\sum_i\lambda_i\mathrm{Tr}_{\mathcal{H}}\Big[V_i(\rho U^\dagger\otimes\mathrm{Id}_{\mathcal{K}})\Big]|\xi\rangle\Big\|_{\mathcal{K}}\\
&=\Big\|\Phi(\rho U^\dagger)|\xi\rangle\Big\|_{\mathcal{K}}.
\end{aligned}$$

The proof concludes with the following application of the Fuchs-van de Graaf inequalities [37, Theorem 1]:

$$\begin{aligned}&\frac{1}{2}\Big\|\mathrm{Tr}_{\mathcal{K}}[\mathcal{P}_\Phi(\,\cdot\,\otimes|\xi\rangle\langle\xi|)]-U(\,\cdot\,)U^\dagger\Big\|_\diamond\\ &\leq \sup_{\substack{|\psi\rangle\in\mathsf{ball}(\mathcal{H}\otimes\mathcal{H}')\\ \mathcal{H}'}}\left(1-\mathcal{F}\Big(|\gamma\rangle\langle\gamma|,\mathcal{P}_\Phi\otimes\mathrm{Id}_{\mathcal{H}'}(|\psi\rangle\langle\psi|\otimes|\xi\rangle\langle\xi|)\Big)^2\right)^{\frac{1}{2}}.\end{aligned}$$

Together with the bound proved before, that is enough to obtain the claim in the lemma. □

Proof of Theorem 3.6. Consider the map $\Phi:\mathcal{S}_1^d\to\mathcal{S}_\infty^m$ in the statement having completely bounded norm one (otherwise we could simply divide Φ by its completely bounded norm). Notice that the hypothesis in the Theorem implies that $\|\Phi^{-1}\|\leq\frac{1}{1-\delta}$.

We will show that, given Φ, Lemma 3.7 allows us to promote the channel provided by Lemma 3.8 to an $\epsilon-\mathrm{UPQP}_d$.

Consider an element $\sigma\in\mathcal{S}_1^d$. Writing down the polar decomposition $\sigma=\rho U^\dagger$, where $\rho\geq 0$ and U is a unitary operator, we can apply Lemma 3.7 to obtain an element $\Theta_U\in\mathsf{ball}(\mathcal{S}_\infty^m)$ such that

$$\langle\Theta_U,\Phi(\sigma)\rangle\geq(1-\delta)\|\sigma\|_{\mathcal{S}_1(\mathcal{H})}. \tag{3.5}$$

Next, we carry out a sort of *purification* of Θ_U. Consider the singular value decomposition of this element, $\Theta_U=\sum_{i\in\mathcal{I}}\lambda_i|\alpha_i\rangle\langle\beta_i|$ with a suitable alphabet $\mathcal{I}$ of cardinal at most m. Now, we can rewrite $\Theta_U=\mathrm{Tr}_{\mathcal{H}_\mathcal{I}}|\xi_U\rangle\langle\chi_U|$, where $|\xi_U\rangle:=\sum_{i\in\mathcal{I}}\lambda_i^{1/2}|\alpha_i\rangle\otimes|i\rangle$, $|\chi_U\rangle:=\overline{\lambda}_i^{1/2}|\beta_i\rangle\otimes|i\rangle\in\mathsf{ball}(\ell_2^m\otimes\mathcal{H}_\mathcal{I})$. Accordingly, we modify the map Φ to

$$\begin{array}{rccc}\Phi': & \mathcal{S}_1^d & \longrightarrow & \mathcal{S}_\infty(\ell_2^m\otimes\mathcal{H}_\mathcal{I})\\ & \sigma & \mapsto & \Phi(\sigma)\otimes\mathrm{Id}_{\mathcal{H}_\mathcal{I}}.\end{array}$$

In terms of this new map, inequality (3.5) transforms into:

$$\langle\,|\xi_U\rangle\langle\chi_U|,\Phi'(\sigma)\,\rangle\geq(1-\delta)\|\sigma\|_{\mathcal{S}_1(\mathcal{H})}.$$

Furthermore, we notice that

$$\langle\, |\xi_U\rangle\langle\chi_U|, \Phi'(\sigma)\,\rangle = \langle\chi_U|\Phi'(\sigma)|\xi_U\rangle \leq \left\|\Phi'(\sigma)|\xi_U\rangle\right\|_{\ell_2^m\otimes\mathcal{H}_\mathcal{I}},$$

i.e.

$$\|\Phi'(\sigma)|\xi_U\rangle\|_{\ell_2^m\otimes\mathcal{H}_\mathcal{I}} \geq (1-\delta)\|\sigma\|_{\mathcal{S}_1(\mathcal{H})}. \tag{3.6}$$

Additionally, it is straightforward to check that $\|\Phi'\|_{cb} = \|\Phi\|_{cb} = 1$. Therefore, Lemma 3.8, applied to the unitary $U \in \mathcal{U}(\ell_2^d)$ and the vector $|\xi_U\rangle \in \mathsf{ball}(\ell_2^m \otimes \mathcal{H}_\mathcal{I})$, provides us with a channel $\mathcal{P}_{\Phi'} \in \mathrm{CPTP}(\ell_2^d \otimes \ell_2^m \otimes \mathcal{H}_\mathcal{I})$ such that

$$\begin{aligned}&\frac{1}{2}\left\|\mathrm{Tr}_{\ell_2^m\otimes\mathcal{H}_\mathcal{I}}[\mathcal{P}_{\Phi'}(\,\cdot\,\otimes|\xi_U\rangle\langle\xi_U|)] - U(\,\cdot\,)U^\dagger\right\|_\diamond \\ &\leq \sup_{\substack{\rho\in\mathsf{ball}(\mathcal{S}_1(\mathcal{H}))\\ :\ \rho\geq 0}} \left(1 - \left\|\Phi'(\rho\, U^\dagger)\,|\xi_U\rangle\right\|_{\mathcal{K}}^2\right)^{\frac{1}{2}}.\end{aligned}$$

Inequality (3.6) finishes the proof. For the quantification of the memory dimension of $\mathcal{P}_{\Phi'}$ we recall that $\dim\mathcal{H}_\mathcal{I}$ was upper bounded by m. □

3.5 Bounds on resources required by UPQPs

The characterization given in the preceding section leads to a better understanding of UPQPs. In this section we obtain lower and upper bounds for the optimal memory dimension of $\epsilon - \mathrm{UPQP}_d$. These are summarized in the last column of Table 3.1. Let us begin with the upper bound:

Proposition 3.9. *For any natural number d, and any $\epsilon > 0$, there exists an $\epsilon - \mathrm{UPQP}_d$ with memory dimension*

$$m \leq \left(\frac{\tilde{C}}{\epsilon}\right)^{d^2},$$

being $\tilde{C}$ an independent constant.

Proof. Although this bound follows easily from an ϵ-net argument, we find instructive to follow the lines of the proof of Theorem 3.6 in this simplified case.

We think at the level of embeddings between Banach spaces and consider the following mapping:

$$\begin{array}{cccc} \Phi : & \mathcal{S}_1^d & \longrightarrow & \ell_\infty^{\mathsf{ball}(\mathcal{S}_\infty^d)} \\ & \sigma & \mapsto & \Big(\mathrm{Tr}[A\sigma^{\mathrm{T}}]\Big)_{A\in\mathsf{ball}(\mathcal{S}_\infty^d)}. \end{array} \tag{3.7}$$

Recall that $\mathsf{ball}(X)$ denotes the unit ball of a Banach space X and, for a given set $\mathcal{X}$, $\ell_\infty^{\mathcal{X}}$ denotes the space of bounded functions from $\mathcal{X}$ to $\mathbb{C}$ endowed with the supremum norm. Then, it is straightforward to see that this embedding is isometric. Indeed, noting that $\mathcal{S}_\infty^d$ is the Banach dual of $\mathcal{S}_1^d$, the embedding considered is usually recognized as a standard consequence of the Hahn-Banach theorem [101].

In addition, the fact that $\ell_\infty^{\mathcal{X}}$ can be understood as a commutative C*-algebra guarantees that the bounded and completely bounded norms of $\Phi : \mathcal{S}_1^d \to \ell_\infty^{\mathcal{X}}$ coincide [34, Proposition 2.2.6]. This also allows us to drop out the awkward transposition in (3.7).

In order to obtain a finite dimensional version of the embedding (3.7), we discretize the image by means of an ϵ–net on $\mathcal{U}(\ell_2^d)$. That is, we consider a finite sequence $\{U_i\}_{i=1}^{|\mathcal{I}|} \subset \mathcal{U}(\ell_2^d)$ such that for every $U \in \mathcal{U}(\ell_2^d)$ there exists an index $i \in \mathcal{I}$ verifying $\|U - U_i\|_{\mathcal{S}_\infty^d} \leq \epsilon$. Then, we define the embedding

$$\begin{array}{cccccc} \tilde{\Phi} : & \mathcal{S}_1^d & \longrightarrow & \ell_\infty^{\mathcal{I}} & \hookrightarrow & \mathcal{S}_\infty(\mathcal{H}_{\mathcal{I}}) \\ & \sigma & \mapsto & \Big(\mathrm{Tr}[U_i\sigma]\Big)_{i\in\mathcal{I}} & \mapsto & \sum_{i\in\mathcal{I}} \mathrm{Tr}[U_i\sigma]\, |i\rangle\langle i|, \end{array}$$

being $\mathcal{H}_{\mathcal{I}}$ a complex Hilbert space of dimension $|\mathcal{I}|$.

Now, it is an easy exercise to see that

$$\|\sigma\|_{\mathcal{S}_1^d} \geq \|\tilde{\Phi}(\sigma)\|_{\mathcal{S}_\infty(\mathcal{H}_{\mathcal{I}})} \geq \left(1 - \frac{\epsilon^2}{2}\right) \|\sigma\|_{\mathcal{S}_1^d},$$

for every $\sigma \in \mathcal{S}_1^d$. Then, $\tilde{\Phi}$ is a particular instance of a map in the conditions of Theorem 3.6, but its very simple structure allows to get to the conclusion of the theorem very easily in this case, as we show now.

The embedding $\tilde{\Phi}$ suggests considering the channel $\mathcal{P}(\,\cdot\,) = V(\,\cdot\,)V^\dagger$, with $V \in \mathcal{U}(\ell_2^d \otimes \mathcal{H}_\mathcal{I})$ being the controlled unitary:

$$V = \sum_{i\in\mathcal{I}} U_i \otimes |i\rangle\langle i|,$$

where the register $\mathcal{H}_\mathcal{I}$ plays the role of a memory. Finally, with Definition 3.2 in mind, let us compute the diamond distance of this channel (with a suitable memory state) to any unitary $U \in \mathcal{U}(\ell_2^d)$. Since the action of the considered channel on the input state is unitary, the problem reduces in this case to compute the usual trace distance

$$\begin{aligned}
&\min_{i\in\mathcal{I}} \max_{|\psi\rangle\in\mathsf{ball}(\ell_2^d)} \frac{1}{2}\| U_i|\psi\rangle\langle\psi|U_i^\dagger - U|\psi\rangle\langle\psi|U^\dagger\|_1 \\
&= \min_{i\in\mathcal{I}} \max_{|\psi\rangle\in\mathsf{ball}(\ell_2^d)} \sqrt{1 - |\langle\psi|U_i^\dagger U|\psi\rangle|^2} \\
&\leq \max_{|\psi\rangle\in\mathsf{ball}(\ell_2^d)} \sqrt{1 - \left(1 - \frac{\epsilon^2}{2}\right)^2} \leq \epsilon.
\end{aligned}$$

Therefore, the considered channel, $\mathcal{P}$, is an $\epsilon - \mathrm{UPQP}_d$ with memory dimension $|\mathcal{I}|$, the cardinality of the ϵ-net considered. This cardinal can be taken lower than $(\tilde{C}/\epsilon)^{d^2}$ for some constant $\tilde{C}$ [3, Theorem 5.11], which is the announced bound. □

Observation 3.10. *Due to the particular structure of the $\epsilon - \mathrm{UPQP}_d$ constructed in Proposition 3.9, we notice that the program states encoding different unitaries of the ϵ–net $\{U_i\}_{i=1}^{|\mathcal{I}|}$ are indeed orthogonal. This is in consonance with the fact discovered by Nielsen and Chuang that, for a UPQP_d ($\epsilon = 0$), any two program states encoding different unitaries must be orthogonal [72]. Then, given an arbitrary $\epsilon - \mathrm{UPQP}_d$, it is tempting to try to reverse the previous ϵ–net argument to find $|\mathcal{I}|$ mutually orthogonal program states, lower bounding in this way the dimension m with the cardinality $|\mathcal{I}|$. However, in general ($\epsilon > 0$) the orthogonality between program states is no longer true (one can consider, for example, the case of Port Based Teleportation [45]). Moreover, previous lower bounds in [80] and [62] (see Table 3.1) were based precisely on this kind of ϵ–net arguments which, in the end, essentially reduce to rough volume estimations. It turns out that the type constants of the Banach spaces* *involved in Theorem 3.5 give a more refined information of their geometry, as we see next.*

The following is the main result of this chapter, the lower bound on m that appears on the upper-right corner of Table 3.1. It follows from the combination of Theorem 3.5 with the type properties of the spaces involved:

Theorem 3.11. *Let $\mathcal{P} \in \mathrm{CPTP}(\mathcal{H}_d \otimes \mathcal{H}_m)$ be an $\epsilon - \mathrm{UPQP}_d$. Then*

$$m \geq 2^{\frac{(1-\epsilon)}{3C} d - \frac{2}{3}\log d}$$

for some positive constant C. Furthermore, if $\mathcal{P}$ is a unitary channel one has $m \geq 2^{\frac{(1-\epsilon)}{C} d}$.

The basic idea to obtain the statement consists on studying ϵ-embeddings between $\mathcal{S}_1^d$ and $\mathcal{S}_\infty^m$. These two spaces are extremely different as Banach spaces and it is this intuition which leads us to Theorem 3.11. For simplicity, we restrict to the case where the considered UPQP is a unitary channel. The general case can be handled by means of a Stinesprings dilation of the channel under consideration. See Appendix A.1 for a detailed argument.

Proof (unitary case). A quick argument to study necessary conditions on the dimensions of the spaces involved is provided considering their type-2 constants. Since Φ_V in Theorem 3.5 maps $\mathcal{S}_1^d$ into a subspace of $\mathcal{S}_\infty^m$ –with distortion $(1-\epsilon)^{1/2}$– the following relation between type constants of these spaces is enforced:

$$\mathrm{T}_2(\mathcal{S}_1^d) \leq \frac{1}{(1-\epsilon)^{\frac{1}{2}}} \mathrm{T}_2(\Phi_V(\mathcal{S}_1^d)) \leq \frac{1}{(1-\epsilon)^{\frac{1}{2}}} \mathrm{T}_2(\mathcal{S}_\infty^m).$$

The first inequality follows from Φ_V being an ϵ-embedding (in the sense of Theorem 3.5), while the second inequality follows from the property of type constants being preserved by subspaces. Introducing in those inequalities the following known estimates for type constants of the spaces involved:

$$\sqrt{d} \leq \mathrm{T}_2(\mathcal{S}_1^d), \quad \mathrm{T}_2(\mathcal{S}_\infty^m) \leq \sqrt{C \log m},$$

we obtain the desired bound:

$$d \leq \frac{C}{(1-\epsilon)} \log m \quad \Rightarrow \quad m \geq 2^{\frac{(1-\epsilon)}{C} d}.$$

The constant here, as well as in the general case of nonunitary channels, can be taken equal to 4.

□

Observation 3.12. *The type-argument sketched above can be made more explicit, obtaining bounds for the memory size necessary to program specific families of unitaries. For instance, we notice that the proof remains unchanged if we restrict to the family of elements* $\Big\{diag(\varepsilon_1, \dots, \varepsilon_d)$ $: \varepsilon_i \in \{\pm 1\}\Big\} \subset \mathcal{S}_1^d$ *instead of considering the action of* $\Phi_{\mathcal{P}}$ *on the whole* $\mathcal{S}_1^d$*. That is true since these elements are enough to estimate* $\mathrm{T}_2(\ell_1^d) \geq \sqrt{d}$ *– this can be checked by direct calculation. More importantly, this means that a programmable processor implementing the family of unitaries* $\Big\{diag(\varepsilon_1, \dots, \varepsilon_d) : \varepsilon_i \in \{\pm 1\}\Big\}$ *up to accuracy* ϵ^{-1} *also has to satisfy the bound of Theorem 3.11. Explicitly, it means that to program the* 2^d *elements in* $\Big\{diag(\epsilon_1, \dots, \epsilon_d) : \epsilon_i \in \{\pm 1\}\Big\} \subset \mathcal{S}_1^d$ *a memory of dimension at least* $2^{\frac{(1-\epsilon)}{3C} d - \frac{2}{3}\log d}$ *is needed, while a classical memory of dimension* 2^d *is enough to store them with no error.*

When looking at m as a function of the input dimension d, fixing the error parameter ϵ, the previous observation shows that Theorem 3.11 is optimal in a sense. However, in the case of universal programmability – where one desires to program the full unitary group $\mathcal{U}(\ell_2^d)$ – we see that there is still a gap between the upper bound in Proposition 3.9 and the lower bound in Theorem 3.11. Summarizing both results, we have proven that the optimal memory dimension of an $\epsilon - \mathrm{UPQP}_d$, as a function of d, is restricted by:

$$\Omega(\exp(d)) = m = O(\exp(d^2)). \tag{3.8}$$

Therefore, a question that remains open is the correct exponent in the previous bounds.

According to the characterization built in Section 3.4, the previous question can be stated purely in the context of normed spaces. In particular, we remark the following open question in local Banach space theory:

Question 1. Given $\epsilon > 0$, what is the largest natural number d such that there exists a d–dimensional subspace of $\mathcal{S}_\infty^m$ that is ϵ–isomorphic to $\mathcal{S}_1^d$?

Coming back to the study of $\epsilon - \mathrm{UPQP}_d$, we recall that in Theorem 3.6 we had to enforce the additional condition that the ϵ–embedding $\Phi : \mathcal{S}_1^d \hookrightarrow \mathcal{S}_\infty^m$ must be completely contractive. Therefore, a hypothetical solution to question 1 with d such that $m = O(\exp(d))$ will not suffice to solve the problem for $\epsilon - \mathrm{UPQP}_d$. A particular case in which the condition about complete contractivity can be relaxed is the one in which $\mathcal{S}_\infty^m$ is replaced by its *commutative version*, ℓ_∞^m – the completely bounded norm of a map $\Phi : \mathcal{S}_1^d \to \ell_\infty^m$ coincides with its usual operator norm. This is precisely the case of the construction in Proposition 3.9. It turns out that, in this restricted case, a more satisfactory answer to Question 1 exists, showing that the upper bound $m = O(\exp(d^2))$ is almost optimal. In precise terms, we state:

Theorem 3.13. *Let Φ be a linear map $\Phi : \mathcal{S}_1^d \longrightarrow \ell_\infty^m$ such that*

$$\forall\, \sigma \in \mathcal{S}_1^d, \qquad \|\sigma\|_{\mathcal{S}_1^d} \geq \|\Phi(\sigma)\|_{\ell_\infty^m} \geq (1-\epsilon)\|\sigma\|_{\mathcal{S}_1^d}.$$

Then

$$m \geq 2^{\frac{d^2(1-\epsilon)^2}{C\log d}},$$

being C a constant.

The proof is based on more involved arguments regarding the type constant of $\mathcal{S}_\infty^d$ and its relation to ϵ–nets for certain spaces. The main argument can be seen as an adjustment of a result by B. Maurey, which appears in [85, Theorem 3]. For the convenience of the reader we provide a proof following the main ideas in [85]. The starting point is the following lemma:

Lemma 3.14 (Maurey, [85, Lemma 2])**.** *Let X be a Banach space of type p, and $\Psi : \ell_1^m \longrightarrow X$ a bounded linear map. Then, $\forall k \in \mathbb{N}$ there exists an ϵ_k–net covering $\Psi(\mathsf{ball}(l_1^m)) \subset X$ with $\epsilon_k = 2k^{-1/q}\mathrm{T}_p(X)\|\Psi\|$*

and cardinality $N_k \leq (2m)^k$. Here, $\mathrm{T}_p(X)$ is the type p constant of X and q is such that $\frac{1}{p} + \frac{1}{q} = 1$.

This lemma also allows to obtain an alternative proof of Theorem 3.11. This proof uses essentially the same ingredients as the one appearing above but we found it less transparent. Besides, it provides a bound that is weaker than the one we have already obtained. Therefore, we decided not to put more emphasis on that and relegate this alternative proof to Appendix A.2.

Let us come back to the proof of Theorem 3.13:

Proof of Theorem 3.13. We begin considering a naive modification of the embedding Φ, defined just by $\tilde{\Phi} := \frac{1}{1-\epsilon}\Phi$. Then,

$$\forall \sigma \in \mathcal{S}_1^d, \qquad \frac{1}{1-\epsilon}\|\sigma\|_{\mathcal{S}_1^d} \geq \|\tilde{\Phi}(\sigma)\|_{\ell_\infty^m} \geq \|\sigma\|_{\mathcal{S}_1^d}. \tag{3.9}$$

Now, we wonder about the adjoint map $\tilde{\Phi}^\dagger : \ell_1^m \longrightarrow \mathcal{S}_\infty^d$. Inherited from (3.9), $\tilde{\Phi}^\dagger$ verifies that $\mathsf{ball}(\mathcal{S}_\infty^d) \subset \tilde{\Phi}^\dagger(\mathsf{ball}(\ell_1^m))$[4] and $\|\tilde{\Phi}^\dagger\| = \|\tilde{\Phi}\| \leq \frac{1}{1-\epsilon}$.

Then, by Lemma 3.14 (choosing $p = 2$) applied to $\tilde{\Phi}^\dagger$, we obtain a δ–net of $\mathsf{ball}(\mathcal{S}_\infty^d)$ with cardinality $N \leq (2m)^k$ and $\delta = \frac{2}{1-\epsilon}(\frac{c}{k}\log d)^{1/2}$ (recall that $\mathrm{T}_2(\mathcal{S}_\infty^d) \leq (c \log d)^{1/2}$, cf. (2.9)) for $k \in \mathbb{N}$ chosen freely and c an independent constant. On the other hand, by standard volume considerations, for any d dimensional normed space the following lower bound for the cardinality of an δ–net covering the unit ball of the space must hold:

$$N \geq \left(\frac{1}{\delta}\right)^d.$$

In our case, this yields to the following condition:

$$\left(\frac{2}{1-\epsilon}\left(\frac{c}{k}\log d\right)^{1/2}\right)^{-d^2} \leq (2m)^k. \tag{3.10}$$

Finally, to conclude the proof it is enough to consider $k \in \mathbb{N}$ large enough in order to fulfil

$$\frac{2}{1-\epsilon}\left(\frac{c}{k}\log d\right)^{1/2} \leq \frac{1}{2}. \tag{3.11}$$

[4] To see why, it is enough to consider that, restricting to $\mathsf{ball}(\mathcal{S}_\infty^d)$, $(\tilde{\Phi}^\dagger)^{-1} = (\tilde{\Phi}^{-1})^\dagger$

Therefore, we get that

$$2^{d^2} \leq (2m)^k \quad \text{i.e.} \quad m \geq 2^{\frac{d^2}{k}-1}.$$

Analysing (3.11), we choose $k \geq \frac{8c \log d}{(1-\epsilon)^2}$, which implies the statement of the theorem.

□

Theorem 3.13 proves that the construction in Proposition 3.9 is optimal in the restricted sense of this theorem. However, we insist that the gap (3.8) remains open for the general case.

In fact, $\epsilon - \mathrm{UPQP}_d$ as the one in the proof of Proposition 3.9 – whose associated embedding Φ has commutative range – can be regarded as making use of a *classical memory.* Hence, the question about the optimality of Equation (3.8) can be interestingly understood as whether a *quantum memory* allows to improve over Proposition 3.9 or not. For a possible answer in the negative, we now comment on the obstructions for a generalization of Theorem 3.13. Firstly, the proof of the key Lemma 3.14 uses crucially the fact that $\mathsf{ball}(\ell_1^m)$ is a polytope with just $2m$ extremal points. In the general case of embeddings $\mathcal{S}_1^d \longrightarrow \mathcal{S}_\infty^m$, if we want to follow the line of the previous proof, the unit ball of ℓ_1^m is replaced by $\mathsf{ball}(\mathcal{S}_1^d)$. This unit ball has infinitely many extremal points, hence the proof cannot be adapted to this case. Furthermore, the original Theorem 3 in [85] is also valid (with modifications in the factors appearing in the bound) for embeddings $\Phi : X \longrightarrow \ell_\infty^m$, being X any finite dimensional normed space. In particular (choose $X = \ell_2^d$), the theorem implies the well known fact that ℓ_2^d cannot be embedded isomorphically in ℓ_∞^m when m is lower than $O(\exp d)$. Turning again to the possibility of replacing ℓ_∞^m by $\mathcal{S}_\infty^m$ in Theorem 3.13, such a generalization would imply similar bounds for embeddings $\ell_2^d \longrightarrow \mathcal{S}_\infty^m$. But this cannot be true since ℓ_2^d can embedded *isometrically* in $\mathcal{S}_\infty^d$ – recall, for instance, the row and column embeddings (2.1), (2.2). In conclusion, in case the right scaling in (3.8) is of order $\Theta(\exp d^2)$, it seems that the proof should come from different techniques that the ones used here or at least from a substantial refinement. In the opposite direction, proving that the optimal scaling for $m(d)$ is $\Theta(\exp d)$ would probably imply new constructions for ϵ-

embeddings $\mathcal{S}_1^d \to \mathcal{S}_\infty^m$ that exploits the non-commutative structure of $\mathcal{S}_\infty^m$ in a highly non-trivial way.

3.6 Discussion

In this chapter we have studied the minimal conditions, in terms of resources, that have to be satisfied by approximate UPQPs. The bounds presented here have clarified several questions about optimality of this conceptual construction. In fact, we have almost closed the gaps in the optimal scaling of the memory size of UPQPs with the accuracy ϵ and input dimension d, when considered separately.

Firstly, in Proposition 3.9 we have deduced an upper bound for m giving a construction based on an ϵ–net on $\mathcal{U}(\ell_2^d)$. In this sense, this construction can be seen as a generalization to the case of UPQPs of the programmable measurement introduced in [29]. As in that case, our proposal improves exponentially the memory resources consumed by other known constructions (see Table 3.1). In fact, this bound exponentially improves the scaling with the accuracy ϵ of Port Based Teleportation and nearly saturates the lower bound deduced in [80] in the context of Universal Programmable *Measurements*. This shows that, indeed, this is the optimal dependence on that parameter also in the case of UPQPs. More generally, it also outperforms Port Based Teleportation whenever $\tilde{C}/\epsilon \leq d^{4/\epsilon^2}$. Obviously, the drawback is that the optimal $\epsilon - \mathrm{UPQP}_d$ constructed here cannot be used to achieve any kind of teleportation.

On the other hand, the main result in this chapter is the lower bound in Theorem 3.11. The first and most obvious consequence of this result is that for any fixed value of ϵ, the dimension of the memory of $\epsilon - \mathrm{UPQP}_d$ must scale exponentially with the input dimension d. Indeed, in this case the dependence with d in the stated lower bound is exponentially stronger than all known previous results. Furthermore, this bound is nearly saturated in this sense by the performance of Port Based Teleportation, referred in table 3.1 as the best upper bound for m. However, as expressed in Question 1, there still remains a gap in this case that we were not able to close.

Furthermore, more difficult relations ϵ–d can be considered, being the general scaling in this case still another open question. However, we also contribute to this point giving an upper bound for the achievable accuracy by UPQPs with memory of size $\mathsf{poly}(d)$. As a straightforward consequence of Theorem 3.11 we obtain the next:

Corollary 3.15. *For any* $\epsilon - \mathrm{UPQP}_d$ *with memory size* $m \leq kd^s$ *for some constants* k, s, *the following inequality is satisfied:*

$$\epsilon \geq 1 - C'_{k,s} \frac{\log d}{d},$$

where $C'_{k,s} = 3C(s + \log k + 2/3)$.

This severely restricts the accuracy achievable by $\epsilon - \mathrm{UPQP}_d$ with polynomially sized memories. Moreover, up to a logarithmic factor, the scaling in the previous bound matches the performance of standard teleportation when understood as an $\epsilon - \mathrm{UPQP}_d$, cf. Example 3.3. Interestingly, this shows the optimality of the protocol of quantum teleportation from the perspective of its programmability properties.

Approaching the end of this chapter, we remark the relation between UPQPs and other tasks such as quantum teleportation [72, 45], state discrimination [33, 104, 105, 131, 130, 106], parameter estimation [49, 108], secret and blind computation [39, 79], homomorphic encryption [128], quantum learning of unitary transformations [10], etc. This spreads the potential implications of the knowledge about UPQP to a wide variety of topics. For example, as a direct application of the results presented here, we also obtain a lower bound for the dimension of the resource space necessary to implement deterministic Port Based Teleportation. There exist more accurate bounds for this particular case, see [27], but notice that we did not use in any way the many symmetries presented in that protocol, and our bound is generic for any protocol implementing, in some sense, a UPQP. Furthermore, it is deduced from our results that the unavoidable exponential scaling with ϵ^{-1} in the case of Port Based Teleportation, comes entirely from the signalling restrictions imposed in this protocol, and cannot be deduced from the programming properties of it.

Finally, we comment on some other interesting questions related with the work presented here. In first place we can ask whether it is possible to deduce a lower bound on m unifying the bound from [80] and the bound from Theorem 3.11. This could give more information about optimality of UPQPs in cases beyond the scope of this work. In relation with that, it would be desirable to improve the exponents in the bounds to match exactly lower and upper bounds, as we have already discussed. Further on, it would be also very interesting to look for relations between memory requirements on UPQPs and circuit complexity problems. A way to explore this line of research could consist on looking for correspondences between circuits and memory states in UPQPs.

Chapter 4

Lower bounds for entanglement consumption in attacks to Position Based Cryptography

This chapter is based on joint work with M. Junge, C. Palazuelos and D. Pérez-García. In this work we initiate the study of Position Based Quantum Cryptography (PBQC) from the perspective of geometric functional analysis and its connections with quantum games. The main question we are interested in asks for the optimal amount of entanglement that a coalition of attackers have to share in order to compromise the security of any PBQC protocol. Known upper bounds for that quantity are exponential in the size of the quantum systems manipulated in the honest implementation of the protocol. However, known lower bounds are only linear.

In order to deepen the understanding of this question, here we propose a Position Verification protocol and find lower bounds on the resources needed to break it. The main idea behind the proof of these bounds is the understanding of cheating strategies as vector valued assignments on the Boolean hypercube. Then, the bounds follow from the understanding of the type constants of particular Banach spaces. Under some regularity assumptions on the former assignment, our results lead to exponential lower bounds on the quantum resources employed, clarifying the question in this restricted case. Known attacks indeed satisfy the assumption we make, although we do not know how universal this feature is. Furthermore, we show that the understanding of the type properties of some more involved Banach spaces would allow to drop out the regularity assumption and lead to unconditional exponential lower bounds on the resources used to attack our protocol. Unfortunately, we were not able to estimate the relevant type constant. Despite that, we conjecture an upper bound for this quantity and show some evidence supporting that conjecture. A positive solution of the conjecture would lead to prove the Position Verification protocol we propose to be secure for all practical purposes and to a major progress towards the question asked above.

We sum up the structure of this chapter: in Section 4.1 we present and motivate the setting of Position Based Cryptography summarizing previous work that is relevant to us. In Section 4.2 we give an overview of the results that we obtain along the chapter. In Section 4.3 we discuss more formally the setting of Position Verification in one spatial dimension, that is the precise setting in which this work develops. In that section we also relate the adversarial action in 1-D Position Verification with mixed rank-one quantum games, introduced in Chapter 1, Section 1.3. Section 4.4 is technical in nature. There, we introduce an inequality of Pisier for vector valued functions on the hypercube and use it together with type constants to provide generic bounds that will be used later on. We also provide some estimates for type constants used in subsequent sections. In Section 4.5 we define the protocol analyzed in this work and deduce some necessary simplifications. In Section 4.6 our results for strategies fulfilling additional regularity assumptions are proven. In Section 4.7, this approach is abstracted in order to remove the extra assumptions. This leads us to the announced conjecture about the type constants of certain spaces. Computations supporting the conjecture are also presented in that section. Finally, in Section 4.8 we make some final remarks spotting at possible connections and future directions for this work. For the sake of readability, in this chapter we use symbols $\gtrsim$, $\lesssim$, $\gtrsim_{\log}$, $\lesssim_{\log}$ to denote inequalities up to multiplicative dimension independent constants or up to multiplicative factors that are logarithmic in the dimension, respectively.

4.1 Background and previous work

In the field of Position Based Cryptography (PBC) one aims to develop cryptographic tasks using the geographical position of an agent as its only credential. Once the agent proved to the verifier that he is in fact at the claimed position, they interact considering the identity of the agent as guaranteed. Basing cryptographic security on the position of the communicating parties could result very appealing in practical contexts such as the use of autonomous cars, or the secure communication between public services or banks. Besides that, at a more fundamental level, secure PBC could also serve as a way to circumvent insecurity under man-in-the middle attacks, a security leak suffered by standard cryptographic primitives. This vulnerability still prevails even in presence of information-theoretical security, as, for example, in the celebrated case of Quantum Key Distribution. In these settings, the security guarantees always come after the assumption that the identity of the trusted agents is granted. In PBC this assumption can be, at least, relaxed. Moreover, PBC proved to be a rich field of research emanating deep questions and connections from its study. To mention a few, attacks for PBC have been related with quantum teleportation [5], circuit complexity [107], classical complexity theory [17] and, very recently, with properties of the boundary description of some processes in the context of the holographic duality AdS/CFT [65, 66]. In this work, we add to this list a connection with deep questions on the geometry of Banach spaces.

The main task in PBC is the one of *Position Verification* (PV). In PV a prover has to convince a verifier (usually composed by several agents spatially distributed) that it is located at a claimed position. This setting has been studied since the 90's in the context of classical cryptography. Nonetheless, in purely classical scenarios, PV is easily proven to be insecure against a team of colluding adversaries surrounding the honest location [23]. This motivates the study of *quantum* PV schemes, in which the communication between prover and verifier is in general quantum. This idea was initially developed by A. Kent [53] and made rigorous only later on in [15]. In this last paper, the authors construct a generic attack for any quantum PV scheme. To this end, the general attack of [15], the authors built on works by L. Vaidman [119], realizing that the cheating action in the setting of PV consists on performing what they called *instantaneous non-local computation*. In this last task, two (or more) distant agents have to implement a quantum operation on a distributed input when subjected to non-signalling constraints – see [15] or Section 4.3 below for more details. At a first sight, the existence of general attacks to quantum PV renders the development of secure PBQC a hopeless program. However, their attack did not come for free for the adversaries, as in the case of classical PV. On the contrary, in order to cheat, the dishonest agents have to use a huge amount of entanglement – a delicate and expensive resource in quantum information processing. Even when in [5] another generic attack to PV was proposed exponentially reducing the entanglement consumption, the amount of entanglement required is still far from what is realizable in any practical situation. This leads naturally to the following question, which is the one motivating this work:

Question 2. How much entanglement is necessary to break *any* PV scheme?

Answering this question with a large enough lower bound would lead to the existence of PBC schemes which are *secure for all practical purposes*, term coined in [22]. The search of such an answer has been an active field of research in the last decades, specially in the years right after the publication of [15]. Therefore, some progress is already available. Indeed, [15] provides the first PV protocol secure against cheaters with *no* entanglement. This was improved in [5] and later in [113] providing PV protocols requiring a linear amount of entanglement (linear in the size of the quantum system used in the honest protocol). In terms of this figure of merit, the entanglement consumption in the generic attack of [5] is exponentially large, hence leaving an exponential gap between lower and upper bounds for the amount of entanglement necessary to break PV schemes. After almost ten years since [15] this is still essentially all it is known about Question 2 in its original formulation. Other works have studied attacks with some specific structure [17], have designed attacks that are efficient emulating the computation of unitaries with low complexity [107] or have studied security under additional cryptographic assumptions [118].

4.2 Summary of results

Here we aim to go back to Question 2 in its simplest form: the one-dimensional case without any further assumptions. Unfortunately, we were not able to find a definite answer to the question but we report here some progress that opens an avenue for a deeper understanding of the problem. From now on, we focus on the study of *quantum* resources required to attack PV, considering classical communication as a free resource and unlimited computational power for all the agents involved. In this work,

- we rephrase the setting of PV in the framework of quantum games,
- connecting that way Question 2 with powerful techniques coming from Banach space theory,
- and providing new lower bounds on the amount of entanglement necessary to break a specific PV protocol presented in Section 4.5. However, the bounds presented are not completely general and they depend on some properties of the strategies considered. Intuitively, *smooth* strategies, i.e., strategies with a smooth dependence in the unitary to be implemented, lead to exponential lower bounds providing evidence supporting the existence of PV schemes that are *secure for all practical purposes*;
- finally, we relate the possibility of turning the previous bounds unconditional with a collection of open problems in local Banach space theory. In particular, we relate the bounds on resources to break our PV protocol with estimates for type constants of tensor norms of ℓ_2 spaces. In this direction, we put forward a conjecture that would imply to the desired unconditional exponential lower bounds and then provide some evidence supporting it.

The protocol $\boldsymbol{G_{Rad}}$. To formalize this discussion, we propose a PV protocol that we denote G_{Rad}. This makes reference to a family $\{G^{(n)}_{Rad}\}_{n\in\mathbb{N}}$ rather than to a single task. The index n represents the security parameter and it determines the size of the quantum systems manipulated in the honest implementation of the protocol.

The general structure of a PV protocol in the studied setting – one-dimensional PV – proceeds in four basic steps:

1. The verifier prepares a bipartite system and distributes it to two verifying agents that surrounds the location to be verified, x. For the sake of concreteness, we locate these agents at points $x \pm \delta$ for some positive δ.

2. Agents at $x \pm \delta$, when synchronized, communicate the registers their hold to x.

3. an honest prover located at x, upon receiving both registers, immediately applies a required computation resulting in another bipartite system. The latter has to be returned to locations $x \pm \delta$. One register should be sent to the agent at the left of x $(x - \delta)$, and the other, to its right $(x + \delta)$.

4. Finally, the verifiers check whether prover's answer arrives on time and whether the computation was performed correctly. Based on this information they declare the verification successful or not.

In the dishonest scenario, two cheaters surrounding the location x, intercept the communication with the honest prover and try to emulate the ideal action in the honest protocol preventing any delay in their response. This restricts cheaters' action to consist of two rounds of local operations mediated by a step of *simulatenous two-way communication* – see Section 4.3 for a detailed discussion of this model.

Once we have fixed this basic setting, let us describe the protocol G_{Rad} involved in our main results. The honest implementation is as follows:

1. Given a natural number n, in $G^{(n)}_{Rad}$ the verifier starts uniformly sampling a vector of n^2 signs $\varepsilon = (\varepsilon_{ij})^n_{i,j=1}$, where each $\varepsilon_{ij} = \pm 1$, and preparing the state $|\psi\rangle := \frac{1}{n}\sum_{i,j} |i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$ in a

tripartite Hilbert space $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{C}}$. The agent at $x - \delta$ receives registers $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ while the one at $x + \delta$ is informed (classically) of the choice of ε. Register $\mathcal{H}_{\mathcal{C}}$ is kept as private for the verifier during the execution of the protocol.

2. Then, registers $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ are forwarded to the verifying location x from its left. From the right, the classical information about the choice of ε is communicated.

3. an honest prover located at x, upon receiving both pieces of information, has to apply the diagonal unitary determined by ε on $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. Immediately, registers $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ must be returned, but this time only $\mathcal{H}_{\mathcal{A}}$ should travel to the verifier at the left. $\mathcal{H}_{\mathcal{B}}$ should be sent to the verifier at the right.

4. After receiving those registers, the verifiers check answer's timing and, at some later time, they perform the measurement $\{|\psi_\varepsilon\rangle\langle\psi_\varepsilon|, \mathrm{Id} - |\psi_\varepsilon\rangle\langle\psi_\varepsilon|\}$ on system $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{C}}$, where $|\psi_\varepsilon\rangle := \frac{1}{n}\sum_{i,j} \varepsilon_{ij} |i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$. They accept the verification only if the arriving time was correct and the outcome of the measurement was the one associated to $|\psi_\varepsilon\rangle\langle\psi_\varepsilon|$.

Next, let us specify the implementation of $G_{Rad}^{(n)}$ in an adversarial scenario. In this situation, we consider that two cheaters located between the honest location x and the verifying agents at $x \pm \delta$, intercepts the communication in the honest protocol. In this work, we refer to these cheaters as Alice, at position $x - \delta'$, and Bob, at position $x + \delta'$, for some $0 < \delta' < \delta$. Their general action proceeds as follows[1]: in advance, the cheaters share a bipartite state $|\varphi\rangle$ in which Bob, after receiving the information about ε, applies an isometry W_ε and sends part of the resulting system to Alice together with the classical information determining ε. On her part, when Alice receives registers $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ of $|\psi\rangle$, she applies another isometry V (independent of ε) on these registers and her part of the shared state $|\varphi\rangle$. Part of her resulting system is communicated to Bob. After this step of simultaneous two-way

[1] For simplicity, we state here the case in which Alice and Bob use what we call *pure* strategies. The most general case can be reduced to this one by purification. See Section 4.5 for a detailed discussion.

communication Alice and Bob are allowed to apply another pair of local isometries $\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon$ on the systems they hold. Then, they have to forward an answer to agents at $x \pm \delta$.

Main results. The structure of G_{Rad} allows us to understand cheating strategies as vector valued assignments on the n^2-dimensional boolean hypercube, $\mathcal{Q}_{n^2} = \{\pm 1\}^{n^2}$. In our main result, we find lower bounds for the resources consumed in such an attack depending on the *regularity* of the former assignment. Very informally, we can state:

Cheating strategies depending on the value of $\varepsilon \in \{\pm 1\}^{n^2}$ *in a sufficiently regular way require an amount of entanglement exponential in n to pass* $G_{Rad}^{(n)}$ *.*

To quantify the regularity of a strategy we introduce a parameter σ that can be regarded as a measure of the *total influence* of the associated function on the Boolean hypercube. We give a precise definition for this parameter in Section 4.6. Here, we restrict ourselves to give an intuitive idea behind this definition presenting some approximations below. Based on two complementary ideas, given a strategy we construct two different assignments leading to two parameters $\sigma^i_{\mathcal{S}}$ and $\sigma^{ii}_{\mathcal{S}}$. The subscript $\mathcal{S}$ makes reference to the strategy we started with. According to the previous discussion, any such strategy can be characterized by a sequence of elements $\mathcal{S} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_{\varepsilon \in \mathcal{Q}_{n^2}}$. With that, we can bound, up to logarithmic factors:

$$\sigma^i_{\mathcal{S}} \lesssim_{\log} \ \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon - \tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} + O\left(\frac{1}{n}\right),$$

$$\sigma^{ii}_{\mathcal{S}} \lesssim_{\log} \ \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \left(V \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\right) |\varphi\rangle \right\|^2_{\ell_2} \right)^{1/2} + O\left(\frac{1}{n}\right).$$

Here, $\overline{\varepsilon}^{ij}$ denotes the sign vector $(\varepsilon_{11}, \ldots, -\varepsilon_{ij}, \ldots, \varepsilon_{nn})$. The first of these parameters is therefore related with how strongly the *second round of local operations* in the strategy depends on ε. On the other hand, $\sigma^{ii}_{\mathcal{S}}$ is similarly concerned with the dependence on ε of the *first round of* *local operations.* With this at hand, we can state – yet informally – our main result. Denoting $\omega(G^{(n)}_{Rad};\mathcal{S})$ the success probability attained by a strategy $\mathcal{S}$ in $G^{(n)}_{Rad}$:

Theorem 4.1 (Informal). *Given a cheating strategy for $G^{(n)}_{Rad}$, $\mathcal{S}$, using quantum resources of local dimension k,*

I.

$$\omega(G^{(n)}_{Rad};\mathcal{S}) \leq C_1 + C_2\ \sigma^{i}_{\mathcal{S}}\ \log^{1/2}(nk) + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\begin{aligned}&\omega(G^{(n)}_{Rad};\mathcal{S})\\ &\quad\leq \tilde{C}_1 + C_3\ \sigma^{ii}_{\mathcal{S}}\, n^{3/4}\log^{3/2}(nk) + O\left(\frac{1}{n^{1/2}} + \frac{\log^{3/2}(nk)}{n}\right);\end{aligned}$$

where C_1, $\tilde{C}_1 < 1$, C_2, C_3 are positive constants.

What this theorem tells us is that cheating strategies for G_{Rad} for which $\sigma^{i}_{\mathcal{S}}$ or $\sigma^{ii}_{\mathcal{S}}$ are small enough necessarily need to make use of quantum resources of size exponential in a power of n, (loosely) matching the exponential entanglement consumption of known attacks[2]. We give a more concrete statement in the form of a corollary:

Corollary 4.2 (Informal). *Consider a cheating strategy for $G^{(n)}_{Rad}$, $\mathcal{S}$, attaining value $\omega(G_{Rad};\mathcal{S}) \geq 1-\epsilon$ for some $0 \leq \epsilon \leq \frac{1}{8}$. Denote by k the local dimension of the quantum resources used in $\mathcal{S}$.*

If $\sigma^{i}_{\mathcal{S}} = O(\mathrm{polylog}(n)/n^{\alpha})$ or $\sigma^{ii}_{\mathcal{S}} = O(\mathrm{polylog}(n)/n^{3/4+\alpha})$ for some $\alpha > 0$, then:

$$k = \Omega\Big(\exp\left(n^{\alpha'}\right)\Big) \quad \textit{for some } \alpha' > 0.$$

As we see, the regularity parameters $\sigma^{i(ii)}_{\mathcal{S}}$ play a key role in these results. We notice that known attacks in [15, 5] in fact fulfil the hypothesis

[2] The attack from [5] requires an entangled system of dimension $O(\exp(n^4))$, that is still much larger than our bounds for smooth strategies. Nonetheless, we consider any strategy using quantum systems of dimension exponential in a power of n to be infeasible for *all practical purposes.* This is our main motivation in this work.

of the previous corollary: the second round of local operations in these attacks is ε-independent, hence $\sigma^{i}_{\mathcal{S}} \sim \log(n)/n$. However, we do not known how generic this behaviour is. More generally, it turns out that from any Programmable Quantum Processor [72] – as the already considered protocol of Port Based Teleportation, for example – with the capability of implementing the diagonal unitaries required in $G^{(n)}_{Rad}$, we can construct an assignment Φ fulfilling Theorem 4.1 with regularity parameter again of order $\sigma^{i}_{\Phi} \sim \log(n)/n$. Therefore, Corollary 4.2 also applies to this broader case allowing to recover some of the results obtained in Chapter 3. This is not a coincidence, our approach here builds on ideas introduced in this previous work.

Turning our attention towards $\sigma^{ii}_{\mathcal{S}}$, a trivial example of a family of *smooth* attacks for which $\sigma^{ii}_{\mathcal{S}} \sim \log(n)/n$ is given by cheaters sharing no entanglement in advance – even when entanglement can be created in the first round of local operations and distributed for the second round. On the contrary, we can also easily compute $\sigma^{ii}_{\mathcal{S}}$ for the attack in [5] obtaining $\sigma^{ii}_{\mathcal{S}} \geq O(1)$. Therefore, our second item in Theorem 4.1 is not able to predict good lower bounds for this case. Still, we think that this second item might be useful for restricting the structure of possible attacks to PV, especially in conjunction with the first part of the theorem.

More importantly, the second part of Theorem 4.1 leads us to put forward the possibility of an unconditional lower bound for k, i.e., a bound in the spirit of Corollary 4.2 but dropping out the assumptions regarding $\sigma^{i(ii)}_{\mathcal{S}}$. Even when we were not able to prove such a bound, we relate its validity with a conjecture about the geometry of some Banach spaces. The positive resolution of this conjecture would prove our scheme G_{Rad} *secure for all practical purposes*. More precisely, our conjecture has to do with estimates of type constants of tensor norms on finite dimensional Hilbert spaces. Even when these constructions are relatively simple and well known in the theory of Banach spaces, there are long-standing open questions about the type of this kind of spaces. E.g., the type-2 constant of the simple space $\ell_2^n \otimes_\varepsilon \ell_2^n \otimes_\varepsilon \ell_2^n$ is still poorly understood. In fact, the related cotype-2 constant of its dual is a famous open question asked by Pisier decades ago – see, for instance, [89].

4.3 Position Verification in 1-D

The major aim of this work is to make progress towards Question 2. For that, we restrict ourselves to the simplest scenario: position verification in 1-D. In this situation, we restrict the world to a line in which we consider a preferred location, x – the position to be verified. The verifier, composed by two agents, V_A and V_B, is located around the honest position x. Let us consider V_A at position $x-\delta$ and V_B at position $x+\delta$. Then, V_A and V_B perform an interactive protocol sending in the direction of x (possibly quantum) messages. These messages arrive to x at the same time, so that an honest prover located at x could receive them and generate answers for V_A and V_B. The verifier accepts the verification if and only if

- (correctness) the answers are correct with respect to verifier's messages (according to some public rule);
- (timeliness) the answers arrive on time to the locations of V_A and V_B. Assuming that the signals between verifier and prover travels at some known velocity c, the answers should arrive to V_A and V_B at time $2\delta c$ after the start of the protocol.

Before continuing, let us set a generic structure for such a protocol. To prepare the messages V_A and V_B must forward to the prover, the verifier prepares a (publicly known) state in a composite system with some underlying Hilbert space $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{C}}$. That is, he prepares a density matrix $\rho_0 \in \mathfrak{D}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{C}})$ and sends register $\mathcal{H}_{\mathcal{A}}$ to V_A and $\mathcal{H}_{\mathcal{B}}$ to V_B. $\mathcal{H}_{\mathcal{C}}$ is considered to take into account the possibility that the verifier keeps some part of the initial system as private during the protocol. Then, V_A and V_B send their systems in the direction of x. Now, the agent(s) interacting in the middle with V_A and V_B apply some quantum operation on the communicated system $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ obtaining as output another state $\rho_{ans} \in \mathfrak{D}(\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}})$. The subsystems $\mathcal{H}'_{\mathcal{A}}$, $\mathcal{H}'_{\mathcal{B}}$ are forwarded to V_A, V_B, respectively. To decide whether the verification is correct or not, the verifier first check the *timeliness* condition is fulfilled and then performs a (publicly known) dichotomic measurement on the system $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{C}}$.

Remark 4.3. Above, ρ_0 and ρ_{ans} are in general quantum states but they could perfectly describe also classical messages as well as quantum-classical messages. This will be indeed the case in the concrete scheme analysed in this work.

Remark 4.4. Note that an honest prover, that is, an agent at position x, should have no problem to pass the test: at time δc he would receive the whole system $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ from the verifiers, having the capability to perform any global operation on it to prepare the answer. This answer can still arrive on time to $V_{\mathcal{A}}$ and $V_{\mathcal{B}}$. The depicted prover's action is the most general operation that can be performed on verifier's messages, which are the only information transmitted in the protocol. Therefore, if the challenge is well designed (it can be passed), the honest prover must be able to succeed at it[3].

Next, let us focus on how the general protocol described above can be cheated. In order to impersonate the identity of an honest prover at position x, a couple of adversaries, Alice and Bob, at positions $x \pm \delta'$, $0 < \delta' < \delta$, can intercept the message systems $\mathcal{H}_{\mathcal{A}}$, $\mathcal{H}_{\mathcal{B}}$, interact between themselves to generate answers for the verifier and forward those answers in correct timing. In order to respect the timeliness of the protocol, the most general action of the cheaters proceeds as specified in Figure 4.1.

We call in this work *simultaneous two-way communication scenario*, *s*2*w*, the set of actions – strategies from now on – with this structure. This scenario is central for us and will appear repeatedly in the rest of this manuscript.

To finish this section, we relate the setting that we have just introduced with the setting of *quantum games*, that was introduced in Section 1.3. Conceptually, this is the link between PBC and the techniques we exploit later on.

[3] We don't take into account here the computational limitations at which the agents might be subjected.

[4] In general, we model in that way any kind of communication between Alice and Bob, classical or quantum. However, in the particular setting studied later on in Section 4.5, we will see that the dimension of $\mathcal{H}_{\mathcal{A}\to\mathcal{B}}$ and $\mathcal{H}_{\mathcal{B}\to\mathcal{B}}$ is essentially determined by the quantum resources the cheaters share, allowing us to disregard the classical communication that they might additionally use. See Section 4.5, Lemma 4.11, for a precise statement.

1. Before the start of the protocol, Alice and Bob prepare some shared entangled state in a private register $\mathcal{H}_{\mathcal{A}_E} \otimes \mathcal{H}_{\mathcal{B}_E}$;

2. Alice receives question register $\mathcal{H}_{\mathcal{A}}$ and applies a quantum channel $\mathcal{A} \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{A}_E}, \mathcal{H}_{\mathcal{A}\to\mathcal{B}} \otimes \mathcal{H}_{\mathcal{A}\to\mathcal{A}})$. Similarly, Bob receives $\mathcal{H}_{\mathcal{B}}$ and applies $\mathcal{B} \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{B}_E}, \mathcal{H}_{\mathcal{B}\to\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}\to\mathcal{B}})$;

3. the cheaters interchange registers $\mathcal{H}_{\mathcal{A}\to\mathcal{B}}$ and $\mathcal{H}_{\mathcal{B}\to\mathcal{B}}$, keeping $\mathcal{H}_{\mathcal{A}\to\mathcal{A}}$, $\mathcal{H}_{\mathcal{B}\to\mathcal{B}}$[4];

4. after this last step, Alice holds system $\mathcal{H}_{\mathcal{A}\to\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}\to\mathcal{A}}$, in which she applies another channel $\tilde{\mathcal{A}} \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}\to\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}\to\mathcal{A}}, \mathcal{H}'_{\mathcal{A}})$. Similarly, Bob applies $\tilde{\mathcal{B}} \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{B}\to\mathcal{B}} \otimes \mathcal{H}_{\mathcal{A}\to\mathcal{B}}, \mathcal{H}'_{\mathcal{B}})$;

5. finally, Alice sends $\mathcal{H}'_{\mathcal{A}}$ to V_A and Bob $\mathcal{H}'_{\mathcal{B}}$ to V_B.

Figure 4.1 Structure of adversarial action attacking 1-D PV schemes.

In particular, we will restrict to PV protocols that can be understood as mixed rank-one quantum games, MROQGs. Having in mind the setting explained above, we now think of two players, Alice and Bob – assimilated as cheaters in the PV protocol–, interacting with a referee – assimilated as the verifier.

On the side of PV, we first mildly restrict the protocol in order to make the connection with the later definition of G_{Rad} clearer. Let us assume that the state prepared by the verifier at the beginning, ρ_0, is a quantum-classical state of the form

$$\rho_0 = \sum_{t \in \mathcal{T}} p_t \, |\psi_t\rangle\langle\psi_t| \otimes |t\rangle\langle t|,$$

where $\mathcal{T}$ is an alphabet, $\{p_t\}_{t\in\mathcal{T}}$ is a probability distribution on this alphabet and $\{|\psi_t\rangle\}_{t\in\mathcal{T}}$ are unit vectors in a Hilbert space $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$. One can imagine that, in each execution of the protocol, the verifier picks at random a label t with probability p_t, causing the initial state to be $\rho_{0,t} = |\psi_t\rangle\langle\psi_t| \in \mathfrak{D}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C})$. Furthermore, assume the message that agent V_A communicates to the prover is composed by register $\mathcal{H}_\mathcal{A}$, while V_B communicates $\mathcal{H}_\mathcal{B}$ *together with the classical information about* t. On these messages, the prover applies a channel $\mathcal{S}_t \in \mathrm{CPTP}(\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}, \mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'})$ to generate an answer. To finish the protocol, after receiving this answer, the verifier measures the whole system $\mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'} \otimes \mathcal{H}_\mathcal{C}$ with a dichotomic POVM, that we also assume to be of a specific form:

$$\text{for each } t \in \mathcal{T}, \text{ the verifier measures } \{|\gamma_t\rangle\langle\gamma_t|, \mathrm{Id} - |\gamma_t\rangle\langle\gamma_t|\}$$

being $|\gamma_t\rangle$ a unit vector in $\mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'} \otimes \mathcal{H}_\mathcal{C}$. The PV is successful when the outcome of this measurement is the one associated to $|\gamma_t\rangle\langle\gamma_t|$.

Turning into quantum games, we notice that for each $t \in \mathcal{T}$, the above protocol can be readily understood as the implementation of a *rank-one quantum game* characterized by a tensor $G_t = \mathrm{Tr}_{\mathcal{H}_\mathcal{C}} |\psi_t\rangle\langle\gamma_t|$, recall Definition 1.37. The players in the game are identified with cheaters in the PV protocol and the referee of the game is identified with the verifier (together with agents V_A, V_B). The distribution of such games according to the probability distribution $\{p_t\}_{t\in\mathcal{T}}$ is in fact a *mixed rank-one quantum game*, recall Definition 1.42.

In particular, given a sequence of channels $\mathcal{S}_t \in \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}, \mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'})$, $t \in \mathcal{T}$, the probability of success of a prover applying these channels in the PV can be identified with the value achieved by the strategy $\mathcal{S} = \{\mathcal{S}_t\}_{t\in\mathcal{T}}$ in the MROQG. This value was defined as:

$$\omega(G; \{\mathcal{S}_t\}_t) := \mathbb{E}_t \operatorname{Tr}\left[\, |\gamma_t\rangle\langle\gamma_t|\, (\mathrm{Id}_C \otimes \mathcal{S}_t)(|\psi_t\rangle\langle\psi_t|)\,\right], \tag{4.1}$$

and will be the central quantity of interest in our study.

The understanding of MROQGs as PV protocols also affects in a crucial way the strategies that we consider to *play* such games. The *scenarios* – recall the terminology of Section 1.3 – that we consider now are two: the *honest* scenario and the *s2w* scenario.

The first one was already defined in Chapter 1, Section 1.3, and now it becomes clear the appearance of the qualifier *honest* for this scenario. In this case, any sequence of channels in $\mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}, \mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'})$ is considered as valid to play a MROQG. The set of allowed strategies in this scenario is therefore identified with $\mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}, \mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'})^{\times|\mathcal{T}|}$. As was stressed in Remark 4.4, this describes the set of possible actions for an honest prover in a PV protocol. The corresponding *honest value*, that was defined by

$$\omega_H(G) = \sup_{\mathcal{S}\in\mathrm{CPTP}(\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}, \mathcal{H}_{\mathcal{A}'}\otimes\mathcal{H}_{\mathcal{B}'})^{\times|\mathcal{T}|}} \omega(G; \mathcal{S}),$$

will be the reference value that the cheaters have to attain.

In the s2w scenario the set of allowed strategies is the subset of channels in $\mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}, \mathcal{H}_{\mathcal{A}'} \otimes \mathcal{H}_{\mathcal{B}'})^{\times|\mathcal{T}|}$ that are constructed according to Figure 4.1. That is, channels that are implementable by two cheaters in the PV protocol associated to the game under consideration. We can straightforwardly define a value $\omega_{s2w}(G)$ as the supremum of $\omega(G; \mathcal{S})$ over strategies allowed in the s2w scenario. Interestingly, the main result in [15], the existence of general attacks for PV, translates into the equivalence of the previous two scenarios in the context of MROQGs:

$$\text{for any MROQG } G, \qquad \omega_H(G) = \omega_{s2w}(G).$$

However, this equivalence holds as far as the resources in the s2w scenario are unbounded. In fact, it is not even known whether the precise value $\omega_H(G)$ can be still attained in the s2w scenario when the ancillary systems used – recall Figure 4.1 – are restricted to be finite dimensional. Moreover, it is known that the equivalence above does not hold when the use of any ancillary system is forbidden. The situation in between is precisely what Question 2 asks about. This motivates considering restricted versions of the s2w scenario in which the dimension of the ancillary, resourceful, systems is bounded. We postpone the precise definition of these models, as well as the discussion of them, to Section 4.5.

4.4 Type constants and functions on the boolean hypercube

The main idea underlying the results in this chapter consists on studying strategies to break a particular family of PV protocols – defined in Section 4.5 – as assignments on the boolean hypercube $\mathcal{Q}_m = \{-1,1\}^m$. We will associate to any cheating strategy a vector valued mapping $\Phi : \mathcal{Q}_m \to X$, being X some Banach space. In this section we introduce a key inequality of Pisier that allows us to control some properties of such maps. We will see that this inequality can be complemented with the information about the type properties of the involved Banach space, building a bridge for the second part of this section, where we present some estimates for the type-2 constant of some relevant spaces.

We start defining a measure of regularity for such functions – Definition 4.5 –, to introduce later on the alluded Pisier's inequality – Lemma 4.7 – and relate it with the type-2 constant of the Banach space involved – Corollary 4.8.

To quantify the regularity of maps $\Phi : \mathcal{Q}_m \to X$ we introduce the following parameter (depending also on the choice of X):

Definition 4.5. *To any Banach space valued map $\Phi : \mathcal{Q}_m \to X$ we associate the parameter:*

$$\sigma_\Phi := \log(m)\ \mathbb{E}_{\varepsilon\in\mathcal{Q}_m}\left(\sum_{i=1}^{m}\|\partial_i\Phi(\varepsilon)\|_X^2\right)^{1/2},$$

where

$$\partial_i \Phi(\varepsilon) := \frac{\Phi(\varepsilon_1, \ldots, \varepsilon_i, \ldots, \varepsilon_m) - \Phi(\varepsilon_1, \ldots, -\varepsilon_i, \ldots, \varepsilon_m)}{2}$$

is the discrete derivative on the boolean hypercube in the i-th direction.

Intuitively, σ_Φ is an average on both, the point $\varepsilon \in \mathcal{Q}_m$ and the direction (unnormalized in this last case), of the magnitude of the derivative of the map Φ. The prefactor $\log(m)$ is of minor importance for our purposes and we added it to the definition of σ_Φ with the only aim of obtaining more compact expressions later on.

Example 4.6. In order to gain some familiarity, let us compute the parameter σ of a linear map

$$\begin{array}{rccc} \Phi : & \mathcal{Q}_m & \longrightarrow & X \\ & \varepsilon & \mapsto & \Phi(\varepsilon) := \frac{1}{m}\sum_j \varepsilon_j x_j \end{array},$$

where $x_j \in \mathsf{ball}(X)$ for $j = 1, \ldots, m$.

First, for any point $\varepsilon \in \mathcal{Q}_m$, and any direction $i \in [m]$:

$$\partial_i \Phi(\varepsilon) = \frac{1}{2m}\left(\sum_j \varepsilon_j x_j - \varepsilon_j (-1)^{\delta_{i,j}} x_j\right) = \frac{1}{m}\varepsilon_i\, x_i.$$

Therefore,

$$\sigma_\Phi = \frac{\log(m)}{m}\left(\sum_i \|x_i\|_X^2\right)^{\frac{1}{2}} \leq \frac{\log(m)}{m^{\frac{1}{2}}}.$$

This example is the ideal representative of a *smooth* function for which our results lead to powerful lower bounds on the resources required to break PBC – recall Corollary 4.2.

Ultimately, the motivation for the definition of σ_Φ is the bound in Corollary 4.8 below. This is a consequence of the following Sobolev-type inequality due to Pisier for vector-valued functions on the hypercube:

Lemma 4.7 ([87], Lemma 7.3)**.** *In a Banach space X, let $p \geq 1$, $\Phi : \mathcal{Q}_m \to X$ and ε, $\tilde{\varepsilon}$ be independent random vectors uniformly distributed on $\mathcal{Q}_m$. Then,*

$$\mathbb{E}_\varepsilon \Big\| \Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon) \Big\|_X^p \leq (C \log m)^p \ \mathbb{E}_{\varepsilon, \tilde{\varepsilon}} \Big\| \sum_i \tilde{\varepsilon}_i \, \partial_i \Phi(\varepsilon) \Big\|_X^p ,$$

where C is an independent constant.

It is now very easy to combine this result with the type properties of X in order to obtain:

Corollary 4.8 (of Lemma 4.7)**.** *In a Banach space X, consider a function $\Phi : \mathcal{Q}_m \longrightarrow X$. Then*

$$\mathbb{E}_\varepsilon \Big\| \Phi(\varepsilon) \Big\|_X \leq \Big\| \mathbb{E}_\varepsilon \Phi(\varepsilon) \Big\|_X + C \ \sigma_\Phi \ \mathrm{T}_2^{(m)}(X),$$

where C is an independent constant.

This is the cornerstone of the building leading to Theorem 4.1.

Proof of Corollary 4.8. Fix $p = 1$ in Lemma 4.7. Therefore, we have that :

$$\mathbb{E}_\varepsilon \Big\| \Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon) \Big\|_X \leq (C \log m) \ \mathbb{E}_{\varepsilon, \tilde{\varepsilon}} \Big\| \sum_i \tilde{\varepsilon}_i \partial_i \Phi(\varepsilon) \Big\|_X .$$

Additionally, we can trivially bound:

$$\mathbb{E}_\varepsilon \Big\| \Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon) \Big\|_X \geq \mathbb{E}_\varepsilon \Big\| \Phi(\varepsilon) \Big\|_X - \Big\| \mathbb{E}_\varepsilon \Phi(\varepsilon) \Big\|_X .$$

On the other hand, according to the definition of the type-2 constant (with m vectors if one wants to be more precise) of X we can also can say:

$$\mathbb{E}_{\varepsilon, \tilde{\varepsilon}} \Big\| \sum_i \tilde{\varepsilon}_i \partial_i \Phi(\varepsilon) \Big\|_X \leq \mathrm{T}_2^{(m)}(X) \ \mathbb{E}_\varepsilon \left(\sum_i \| \partial_i \Phi_S(\varepsilon) \|_X^2 \right)^{1/2} .$$

That's enough to obtain the statement. □

Corollary 4.8 provides us with a tool to upper bound the expected norm of the image of Φ, provided that we have some control over the RHS of the inequality in the statement. The only piece there that is independent of the map Φ is the type-2 constant (with m vectors) $\mathrm{T}_2^{(m)}(X)$, to which the rest of this section is devoted.

In the precise maps that we will study in Sections 4.6 and 4.7, the spaces $\mathcal{S}_\infty^{n,m}$ and $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{n,m}$ appear in a natural way – recall that the second space was defined in Chapter 2, Section 2.4, Definition 2.13. The type and cotype properties of the first space are well known, in fact, we have already used them in Chapter 3. For future reference, we recall here that

$$\begin{aligned} \mathrm{C}_2(\mathcal{S}_\infty^{n,m}) &\lesssim \min(n^{1/2}, m^{1/2}), \\ \mathrm{T}_2(\mathcal{S}_\infty^{n,m}) &\lesssim \log^{1/2}(\min(n,m)). \end{aligned} \tag{4.2}$$

For $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{n,m}$ the situation is not that well understood at all. In fact, we were not able to obtain any non-trivial estimate for its type properties so far. Then, instead of dealing directly with this space, we will consider the interpolation space $(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}, \mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m})_{\frac{1}{2}}$, that turns out to be useful to upper bound the norm in $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{n,m}$. This was shown in Proposition 2.15 in a more general context. We recall the specific statement for the case we study now. Denoting $\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m} := (\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}, \mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m})_\theta$, for $0 < \theta < 1$, we have:

Proposition 4.9 (Particular case of Proposition 2.15)**.** *Given any $f \in \mathcal{S}_1^{n,m} \otimes \mathcal{S}_1^{n,m}$,*

$$\|f\|_{\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{n,m}} \le \|f\|_{\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w}} \mathcal{S}_1^{n,m}} \le \|f\|_{\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{n,m}}.$$

Thanks to the extra structure in $\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{n,m}$ provided by interpolation, we are able to obtain a bound for its type constants. To simplify the presentation, we consider in the following that $\min(n,m) = n$. Then, we can state:

Proposition 4.10. *Given $0 < \theta < 1$, and natural numbers $n \le m$:*

$$\mathrm{T}_{\frac{2}{1+\theta}} \left(\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m} \right) \lesssim_{\log} n^{\frac{1-\theta}{2}}.$$

An immediate consequence of the previous corollary is a bound for the type-2 constant with n^2 vectors:

$$\mathrm{T}_2^{(n^2)}\left(\mathcal{S}_1^{n,m}\otimes_{(\varepsilon,\pi)_\theta}\mathcal{S}_1^{n,m}\right)\leq n^\theta\ \mathrm{T}_{\frac{2}{1+\theta}}\left(\mathcal{S}_1^{n,m}\otimes_{(\varepsilon,\pi)_\theta}\mathcal{S}_1^{n,m}\right)\lesssim_{\log} n^{\frac{1+\theta}{2}}.$$

Particularizing for $\theta=\frac{1}{2}$:

$$\mathrm{T}_2^{(n^2)}\left(\mathcal{S}_1^{n,m}\otimes_{(\varepsilon,\pi)_{\frac{1}{2}}}\mathcal{S}_1^{n,m}\right)\lesssim_{\log} n^{\frac{3}{4}}. \tag{4.3}$$

This is the key type-estimate to obtain part II. of the main Theorem 4.1.

For the sake of concreteness, we explicit here the logarithmic corrections in (4.3):

$$\mathrm{T}_2^{(n^2)}\left(\mathcal{S}_1^{n,m}\otimes_{(\varepsilon,\pi)_{\frac{1}{2}}}\mathcal{S}_1^{n,m}\right)\lesssim n^{3/4}\log^{1/2}(nm)\log(n).$$

Proof of Proposition 4.10. The proof proceeds in two steps. First, using techniques from [89, 90], we obtain the estimate

$$\mathrm{T}_2(\mathcal{S}_1^{n,m}\otimes_\varepsilon\mathcal{S}_1^{n,m})\lesssim_{\log} n^{1/2}. \tag{4.4}$$

With this at hand, Proposition 4.10 follows from the behaviour of type constants with respect to the complex interpolation method, Proposition 2.10. In particular, it is enough to fix $p_0=2$, $p_1=1$ in that result and consider the trivial bound $\mathrm{T}_1(\mathcal{S}_1^{n,m}\otimes_\pi\mathcal{S}_1^{n,m})=1$.

Therefore, there remains to provide a proof for (4.4). To prove the stated estimate we bound the cotype-2 constant of the dual, $\mathcal{S}_\infty^{n,m}\otimes_\pi\mathcal{S}_\infty^{n,m}$. From the duality between type and cotype, Proposition 2.6, we obtain:

$$\mathrm{T}_2(\mathcal{S}_1^{n,m}\otimes_\varepsilon\mathcal{S}_1^{n,m})\lesssim\log(nm)\,\mathrm{C}_2(\mathcal{S}_\infty^{n,m}\otimes_\pi\mathcal{S}_\infty^{n,m}).$$

To estimate $\mathrm{C}_2(\mathcal{S}_\infty^{n,m} \otimes_\pi \mathcal{S}_\infty^{n,m})$, we use the following bound on the cotype of the projective tensor product, implicit in [89][5]:

$$\mathrm{C}_2(\mathcal{S}_\infty^{n,m} \otimes_\pi \mathcal{S}_\infty^{n,m}) \lesssim \mathrm{C}_2(\mathcal{S}_\infty^{n,m})\, \mathrm{UMD}(\mathcal{S}_\infty^{n,m})\, \mathrm{T}_2^2(\mathcal{S}_\infty^{n,m}),$$

where $\mathrm{UMD}(X)$ is the analytic UMD (unconditional martingale difference) parameter of the Banach space X. We now bound each of the quantities in the RHS of the last inequality:

- recalling (4.2) we have that $\mathrm{C}_2(\mathcal{S}_\infty^{n,m}) \lesssim n^{1/2}$ and $\mathrm{T}_2(\mathcal{S}_\infty^{n,m}) \lesssim \log^{1/2}(n)$;

- we estimate $\mathrm{UMD}(\mathcal{S}_\infty^{n,m})$ from known bounds for the UMD constant of the p-Schatten class $\mathcal{S}_p$, for $1 < p < \infty$. It is known that these spaces are UMD and the following estimate for $\mathrm{UMD}(\mathcal{S}_p)$ is available [94]:
$$\mathrm{UMD}(\mathcal{S}_p) \lesssim p.$$
This also translates on the same bound for the subspace $\mathcal{S}_p^{n,m}$. Now, we take into account the following relation between the UMD constants of arbitrary spaces X and Y at Banach-Mazur distance $d(X,Y)$. This is a direct consequence of the geometric characterization of the UMD property due to Burkholder [18] – see also [19]:
$$\mathrm{UMD}(X) \lesssim d(X,Y)\, \mathrm{UMD}(Y).$$
Finally, with this at hand, we obtain the bound
$$\mathrm{UMD}(\mathcal{S}_\infty^{n,m}) \lesssim d(\mathcal{S}_\infty^{n,m}, \mathcal{S}_p^{n,m})\, \mathrm{UMD}(\mathcal{S}_p^{n,m}) \lesssim n^{1/p}\, p.$$
Adjusting the parameter p as $p = \log(n)$ we obtain
$$\mathrm{UMD}(\mathcal{S}_\infty^{n,m}) \lesssim \log(n),$$

[5] The key result here is Theorem 5.1 in [89]. The bound we use is obtained keeping track of the constants appearing in the isomorphic statement of that theorem. We are indebted to Jop Briët for kindly sharing with us some very useful private notes on Pisier's method.

which is enough to conclude that

$$\mathrm{T}_2(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}) \lesssim \log(nm)\, \log^2(n)\, n^{1/2}.$$

□

4.5 The game G_{Rad}

In this section we describe the precise setting that we study, which we denote G_{Rad}. As explained in the second part of Section 4.3, our aim is to understand G_{Rad} as a MROQG. But first, we look at it from the point of view of protocols for PV – cf. first part of section 4.3. Actually, G_{Rad} will rather refer to a family of protocols indexed by a natural number, n, making reference to the *size* of the protocol. Nonetheless, we omit explicit reference to this index when there is no risk of confusion. G_{Rad} proceeds as follows:

1. The verifier prepares the state $|\psi\rangle = \frac{1}{n}\sum_{i,j=1}^n |ij\rangle_{AB} \otimes |ij\rangle_C \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$ and distributes registers $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ to V_A. He also chooses uniformly at random an n^2 dimensional sign vector $\varepsilon = (\varepsilon_{ij})_{i,j=1}^n \in \mathcal{Q}_{n^2}$ and informs V_B of that choice.

2. V_A forwards the quantum system $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ to the prover at x. From the other side, V_B communicates the classical information specifying the vector ε.

3. After receiving both messages, an honest prover located at x has to apply the unitary $U_\varepsilon = diag(\varepsilon_{11}, \dots, \varepsilon_{nn})$ on the received system $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ and forwards $\mathcal{H}_\mathcal{A}$ back to V_A and $\mathcal{H}_\mathcal{B}$ *to* V_B.

4. At some later time, V_A and V_B perform the joint measurement defined by elements $\{|\psi_\varepsilon\rangle\langle\psi_\varepsilon|, \mathrm{Id} - |\psi_\varepsilon\rangle\langle\psi_\varepsilon|\}$, where we have defined $|\psi_\varepsilon\rangle = U_\varepsilon \otimes \mathrm{Id}_C\, |\psi\rangle$. The verification is correct if the outcome of this final measurement is the one corresponding to $|\psi_\varepsilon\rangle\langle\psi_\varepsilon|$ and the registers $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ were received on time.

Consider now a coalition of attackers, Alice and Bob, trying to impersonate the honest prover intercepting the communication with V_A

and V_B at points $x-\delta'$, $x+\delta'$. As commented before, cheaters' action can be understood as Alice and Bob playing a collaborative quantum game with suitable restrictions in their resources – we consider the s2w scenario defined in Figure 4.1. The associated game is a MROQG. This game, which we also denote as G_{Rad}, is defined by tensors

$$\Big\{G_\varepsilon := \mathrm{Tr}_C|\psi_\varepsilon\rangle\langle\psi| = \frac{1}{n^2}\sum_{i,j=1}^{n}\varepsilon_{ij}|ij\rangle\langle ij|\Big\}_{\varepsilon\in\mathcal{Q}_{n^2}}$$

and the uniform probability distribution over $\mathcal{Q}_{n^2}$. The game proceeds as follows:

1. The referee prepares the state $|\psi\rangle = \frac{1}{n}\sum_{i,j}^{n}|ij\rangle_{AB}\otimes|ij\rangle_C \in \mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}\otimes\mathcal{H}_{\mathcal{C}}$ and samples uniformly at random an n^2 dimensional sign vector, $\varepsilon = (\varepsilon_{ij})_{ij=1}^{n}\in\mathcal{Q}_{n^2}$.

2. He sends registers $\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}$ to Alice and the classical description of ε to Bob.

3. Alice and Bob apply a quantum operation on the information received and send to the referee quantum messages resulting from that operation. Register $\mathcal{H}_{\mathcal{A}}$ has to be communicated from Alice and $\mathcal{H}_{\mathcal{B}}$ from Bob. Their action is restricted to be of the form of Figure 4.1. We study in detail this scenario below.

4. The referee performs the measurement $\{|\psi_\varepsilon\rangle\langle\psi_\varepsilon|, \mathrm{Id}-|\psi_\varepsilon\rangle\langle\psi_\varepsilon|\}$ on registers $\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}\otimes\mathcal{H}_{\mathcal{C}}$. He declares the players winning the game when the outcome of this last measurement is the one corresponding to $|\psi_\varepsilon\rangle\langle\psi_\varepsilon|$.

The main object of study in this work is the value of this game in the *s2w* scenario, denoted by $\omega_{s2w}(G_{Rad})$. A strategy in this scenario is determined by – cf. Figure 4.1:

- a shared entangled state $\varphi \in \mathfrak{D}(\mathcal{H}_{\mathcal{A}_E} \otimes \mathcal{H}_{\mathcal{B}_E})$ that we assume here to be pure[6]. From now on we use indistinguishably the notation φ or $|\varphi\rangle\langle\varphi|$ to refer to that state;
- a family – indexed by ε – of tuples of four "local" channels: for each $\varepsilon \in \mathcal{Q}_{n^2}$,

$$\begin{aligned} \mathcal{A} &\in \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{A}_E}, \mathcal{H}_{\mathcal{A}\to\mathcal{A}} \otimes \mathcal{H}_{\mathcal{A}\to\mathcal{B}}), \\ \mathcal{B}_\varepsilon &\in \mathrm{CPTP}(\mathcal{H}_{\mathcal{B}_E}, \mathcal{H}_{\mathcal{B}\to\mathcal{B}} \otimes \mathcal{H}_{\mathcal{B}\to\mathcal{A}}), \\ \tilde{\mathcal{A}}_\varepsilon &\in \mathrm{CPTP}(\mathcal{H}_{\mathcal{A}\to\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}\to\mathcal{A}}, \mathcal{H}'_A), \\ \tilde{\mathcal{B}}_\varepsilon &\in \mathrm{CPTP}(\mathcal{H}_{\mathcal{B}\to\mathcal{B}} \otimes \mathcal{H}_{\mathcal{A}\to\mathcal{B}}, \mathcal{H}'_B). \end{aligned}$$

  For verification, $\mathcal{H}'_A$, $\mathcal{H}'_B$ should be communicated to V_A and V_B respectively. Therefore, according to the definition of the game, these registers should be isomorphic to the originals $\mathcal{H}_{\mathcal{A}}$ and $\mathcal{H}_{\mathcal{B}}$.

Understood as a family of quantum channels, the strategy defined by these elements reads:

$$\begin{array}{rccc} \mathcal{S}_\varepsilon : & \mathfrak{D}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}) & \longrightarrow & \mathfrak{D}(\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}) \\ & \psi & \mapsto & \mathcal{S}_\varepsilon(\psi) = (\tilde{\mathcal{A}}_\varepsilon \otimes \tilde{\mathcal{B}}_\varepsilon) \circ (\mathcal{A} \otimes \mathcal{B}_\varepsilon)(\psi \otimes \varphi) \end{array}, \tag{4.5}$$

for each $\varepsilon \in \mathcal{Q}_{n^2}$. Recalling (4.1), we denote $\omega(G_{Rad}; \{\mathcal{S}_\varepsilon\}_\varepsilon)$ the value attained by such a strategy. Further denoting $\mathfrak{S}_{s2w}$ the set of strategies in the form (4.5), we define the value of G_{Rad} in the s2w scenario:

$$\begin{aligned} \omega_{s2w}(G_{Rad}) &= \sup_{\{\mathcal{S}_\varepsilon\}_\varepsilon \in \mathfrak{S}_{s2w}} \omega(G_{Rad}; \{\mathcal{S}_\varepsilon\}_\varepsilon) \qquad (4.6) \\ &= \sup \ \mathbb{E}_\varepsilon \ \omega\Big(G_\varepsilon; (\tilde{\mathcal{A}}_\varepsilon \otimes \tilde{\mathcal{B}}_\varepsilon) \circ (\mathcal{A} \otimes \mathcal{B}_\varepsilon)(\,\cdot\, \otimes \varphi)\Big), \end{aligned}$$

[6] It can be easily checked that, by convexity, the value achieved in G_{Rad} by strategies using mixed states is always upper bounded by the value when using pure states. Since the quantity we are interested in is the optimal value of the game, restricting ourselves to strategies using pure states would be enough.

where the supremum is over $\tilde{\mathcal{A}}_\varepsilon$, $\tilde{\mathcal{B}}_\varepsilon$, $\mathcal{A}$, $\mathcal{B}_\varepsilon$ and φ as indicated above and over any finite dimensional auxiliar Hilbert spaces appearing there – $\mathcal{H}_{\mathcal{A}_E(\mathcal{B}_E)}$, $\mathcal{H}_{\mathcal{A}(\mathcal{B})\to\mathcal{A}(\mathcal{B})}$, $\mathcal{H}_{\mathcal{A}(\mathcal{B})\to\mathcal{B}(\mathcal{A})}$. For future reference, we recall here the expression for the value of G_{Rad} in our particular case: consider the strategy defined by the family of channels (4.5), then

$$\omega(G_{Rad};\{\mathcal{S}_\varepsilon\}_\varepsilon) := \mathbb{E}_\varepsilon \operatorname{Tr}\left[\, |\psi_\varepsilon\rangle\langle\psi_\varepsilon| \;\; (\mathrm{Id}_C \otimes \mathcal{S}_\varepsilon)\left(|\psi\rangle\langle\psi|\right)\right], \qquad (4.7)$$

where $|\psi_\varepsilon\rangle = \frac{1}{n}\sum_{i,j}^n \varepsilon_{ij}\, |i\rangle \otimes |j\rangle \otimes |ij\rangle$, and $|\psi\rangle = \frac{1}{n}\sum_{i,j}^n |i\rangle \otimes |j\rangle \otimes |ij\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$.

Recall that, when rephrased in this language, the existence of general attacks for arbitrary PV schemes translates into the coincidence of the value in the $s2w$ scenario with the honest value. In our particular case:

$$\omega_{s2w}(G_{Rad}) = \omega_H(G_{Rad}) = 1. \qquad (4.8)$$

The main question we are interested in is the amount of entanglement necessary to establish this equality. It is natural then to define a restricted version of $\omega_{s2w}(G_{Rad})$ considering only strategies using a limited amount of resources. Here, we restrict the local dimension at any time during the protocol. Considering the definition of $\mathcal{A}$, $\mathcal{B}_\varepsilon$, $\tilde{\mathcal{A}}_\varepsilon$, $\tilde{\mathcal{B}}_\varepsilon$, $|\varphi\rangle$ and the corresponding auxiliar systems $\mathcal{H}_{\mathcal{A}_E(\mathcal{B}_E)}$, $\mathcal{H}_{\mathcal{A}(\mathcal{B})\to\mathcal{A}(\mathcal{B})}$, $\mathcal{H}_{\mathcal{A}(\mathcal{B})\to\mathcal{B}(\mathcal{A})}$ in the $\mathfrak{S}_{s2w}$ model established above, we now restrict their dimension:

Given k, $\tilde{k} \in \mathbb{N}$, we constrain:

$$\dim(\mathcal{H}_{\mathcal{A}_E(\mathcal{B}_E)}) \le k, \qquad \dim(\mathcal{H}_{\mathcal{A}(\mathcal{B})\to\mathcal{A}(\mathcal{B})})\, \dim(\mathcal{H}_{\mathcal{A}(\mathcal{B})\to\mathcal{B}(\mathcal{A})}) \le \tilde{k}.$$

I.e., we restrict the elements defining a strategy in our model to be as:

$$|\varphi\rangle \in \ell_2^{k^2},$$

$$\mathcal{A} \in \mathrm{CPTP}(\ell_2^{n^2 k}, \ell_2^{\tilde{k}}), \quad \mathcal{B}_\varepsilon \in \mathrm{CPTP}(\ell_2^{k}, \ell_2^{\tilde{k}}),$$
$$\tilde{\mathcal{A}}_\varepsilon \in \mathrm{CPTP}(\ell_2^{\tilde{k}}, \ell_2^{n}), \quad \tilde{\mathcal{B}}_\varepsilon \in \mathrm{CPTP}(\ell_2^{\tilde{k}}, \ell_2^{n}).$$

The model defined by the set of tuples $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\}_\varepsilon$ of such elements is denoted $\mathfrak{S}_{s2w;\tilde{k},k}$. The corresponding value of G_{Rad} in this model is denoted:

$$\omega_{s2w;\tilde{k},k}(G_{Rad}) = \sup_{\mathcal{S}\in\mathfrak{S}_{s2w;\tilde{k},k}} \omega(G_{Rad};\mathcal{S}). \tag{4.9}$$

Clearly,

$$\lim_{\tilde{k},k\to\infty} \omega_{s2w;\tilde{k},k}(G_{Rad}) = \omega_{s2w}(G_{Rad}) = \omega_H(G_{Rad}). \tag{4.10}$$

We want to study the rate of convergence of this limit. To the best of our knowledge, it is not even known whether the limit is in general attained for finite k, $\tilde{k}$. We worry about lower bounds in k, $\tilde{k}$ to achieve a given degree of approximation in (4.10). More precisely, we lower bound the difference $\omega_H(G_{Rad}) - \omega_{s2w;\tilde{k},k}(G_{Rad})$ in terms of k, $\tilde{k}$ and properties of the strategies considered. However, we postpone those results until Section 4.6. Before that, we need to provide here two reductions to the kind of strategies we consider in order to prepare the ground for next section.

Classical communication in the s2w scenario. First, we consider the role of classical communication between Alice and Bob. In our model, we regard this resource as free and, in fact, we have included in the structure of the considered strategies the free communication of the classical information about ε (in the second round of local operations this parameter was considered as public). This is justified by the fact that our interest is bounding the *quantum* resources used for attacking G_{Rad}, which are assumed to be much more expensive than classical communication. However, there is a potential problem with this approach. That is the possibility that the players use further classical communication apart from that of ε – *extra classical communication* from now on. In our model, this extra classical communication would be included in the definition of channels $\mathcal{A}$ and $\mathcal{B}_\varepsilon$. In the $\mathfrak{S}_{s2w,\tilde{k},k}$ scenario, this would affect the dimension $\tilde{k}$ being no longer a reliable witness for the quantum resources employed in a given strategy: $\tilde{k}$ would also include the dimension of the extra classical messages shared by Alice and Bob. Nonetheless, we show that the amount of *useful* extra classical communication in our setting is bounded by the initial dimension of the quantum system manipulated by the players, that is, by k and n. The following lemma allows us to control the contribution of the classical part of players' action to $\tilde{k}$.

Lemma 4.11. *The optimization over $\mathcal{S} \in \mathfrak{S}_{s2w,\tilde{k},k}$ in* (4.9) *can be restricted to strategies using extra classical communication of local dimension $\tilde{k}_{cl} \leq n^4 k^2$.*

Proof. The result follows from convexity taking into account the structure of extreme points in the set of instruments acting on a given Hilbert space, Chapter 1, Corollary 1.36.

Consider an arbitrary strategy $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\} \in \mathfrak{S}_{s2w;m,k}$ using extra classical communication of local dimension m_{cl}, where $m_{cl} \leq m$ are arbitrary natural numbers that will be conveniently fixed at the end of the proof. Therefore, we can further specify these classical messages in the structure of the channels $\mathcal{A}$ and $\mathcal{B}_\varepsilon$:

$$\mathcal{A}(\,\cdot\,) = \sum_{c_a=1}^{m_{cl}} \mathcal{A}^{c_a}(\,\cdot\,) \otimes |c_a\rangle\langle c_a| \quad : \quad \mathcal{A}^{c_a} \in \mathrm{CP}(\ell_2^{n^2 k}, \ell_2^{m/m_{cl}}) \text{ for any } c_a,$$

$$\mathcal{B}_\varepsilon(\,\cdot\,) = \sum_{c_b=1}^{m_{cl}} \mathcal{B}_\varepsilon^{c_b}(\,\cdot\,) \otimes |c_b\rangle\langle c_b| \quad : \quad \mathcal{B}_\varepsilon^{c_b} \in \mathrm{CP}(\ell_2^{k}, \ell_2^{m/m_{cl}}) \text{ for any } c_b.$$

These expressions are just the description of some instruments in $\mathrm{Ins}(\ell_2^k, \ell_2^{m/m_{cl}})$ ($\mathrm{Ins}(\ell_2^{n^2k}, \ell_2^{m/m_{cl}})$ in the first case) with m_{cl} outcomes each. The extreme points of $\mathrm{Ins}(\ell_2^k, \ell_2^{m/m_{cl}})$ consist of instruments with at most k^2 outcomes (n^4k^2 in the first case) – cf. Corollary 1.36. Therefore, we can rewrite the channels $\mathcal{A}$, $\mathcal{B}_\varepsilon$ as a convex combination of such extreme points:

$$\mathcal{A}(\,\cdot\,) = \sum_s \alpha_s \mathcal{A}_s(\,\cdot\,),$$

$$\mathcal{B}_\varepsilon(\,\cdot\,) = \sum_s \beta_{\varepsilon,s} \mathcal{B}_{\varepsilon,s}(\,\cdot\,),$$

where, for each s and each ε:

- $0 \leq \alpha_s,\ \beta_{\varepsilon,s} \leq 1 : \sum_s \alpha_s = 1 = \sum_s \beta_{\varepsilon,s}$;
- $\mathcal{A}_s \in \mathrm{Ins}(\ell_2^{n^4k^2}, \ell_2^{m/m_{cl}})$, $\mathcal{B}_{\varepsilon;s} \in \mathrm{Ins}(\ell_2^k, \ell_2^{m/m_{cl}})$ with at most n^4k^2 and k^2 outcomes, respectively. For simplicity we just fix $\tilde{k}_{cl}$ bounded by the largest of these bounds, $\tilde{k}_{cl} \leq n^4k^2$.

Denote $\mathcal{S}_{s,s'}$ the strategy specified by elements $\{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}_s, \mathcal{B}_{\varepsilon,s'}, \varphi\}_\varepsilon$ and $\mathcal{S}_{\varepsilon;s,s'}(\,\cdot\,)$ the corresponding channels, defined by the generic prescription (4.5). Notice that $\mathcal{S}_\varepsilon(\,\cdot\,) = \sum_{s,s'} \alpha_s \beta_{s'} \mathcal{S}_{\varepsilon;s,s'}(\,\cdot\,)$. Now, let us focus on the value achieved in G_{Rad}. We remark that $\omega(G_{Rad};\mathcal{S})$ is linear in $\mathcal{S}$, fact that allows us to write:

$$\begin{aligned}\omega(G_{Rad};\mathcal{S}) &= \sum_s \alpha_s \, \mathbb{E}_\varepsilon \sum_{s'} \beta_{\varepsilon,s} \, \omega(G_{Rad}; \{\mathcal{S}_{\varepsilon;s,s'}\}_\varepsilon) \\ &\le \max_s \left\{ \mathbb{E}_\varepsilon \max_{s'} \{\omega(G_{Rad}; \{\mathcal{S}_{\varepsilon;s,s'}\}_\varepsilon)\} \right\}.\end{aligned}$$

Denoting s^*, ${s'_\varepsilon}^*$ the indexes at which the maxima above are attained, the strategy $\{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}_{s^*}, \mathcal{B}_{\varepsilon,{s'_\varepsilon}^*}, \varphi\}_\varepsilon$, that uses extra classical communication of local dimension at most $\tilde{k}_{cl} \le n^4 k^2$, can be now regarded as an element in $\mathfrak{S}_{s2w;\tilde{k},k}$ with $\tilde{k} = m\tilde{k}_{cl}/m_{cl}$. This proves the claim.

□

Pure s2w strategies. The second reduction consists on purifying arbitrary strategies. We start fixing some notation. We say that a strategy $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\}_\varepsilon \in \mathfrak{S}_{s2w}$ is *pure* if the channels $\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon$ can be written as:

$$\mathcal{A}(\,\cdot\,) = V(\,\cdot\,)V^\dagger, \qquad \mathcal{B}_\varepsilon(\,\cdot\,) = W_\varepsilon(\,\cdot\,)W_\varepsilon^\dagger,$$

$$\tilde{\mathcal{A}}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{anc_a} \tilde{V}_\varepsilon(\,\cdot\,)\tilde{V}_\varepsilon^\dagger, \qquad \tilde{\mathcal{B}}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{anc_b} \tilde{W}_\varepsilon(\,\cdot\,)\tilde{W}_\varepsilon^\dagger,$$

for some contractive operators

$$\begin{gathered} V : \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{A}_E} \longrightarrow \mathcal{H}_{A\to A} \otimes \mathcal{H}_{A\to B}, \\ W_\varepsilon : \mathcal{H}_{\mathcal{B}_E} \longrightarrow \mathcal{H}_{B\to B} \otimes \mathcal{H}_{B\to A}, \\ \tilde{V}_\varepsilon : \mathcal{H}_{A\to A} \otimes \mathcal{H}_{B\to A} \longrightarrow \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{A}_{anc}}, \\ \tilde{W}_\varepsilon : \mathcal{H}_{B\to B} \otimes \mathcal{H}_{A\to B} \longrightarrow \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{B}_{anc}}, \end{gathered}$$

being $\mathcal{H}_{\mathcal{A}_{anc}}$, $\mathcal{H}_{\mathcal{B}_{anc}}$ arbitrary ancillary Hilbert spaces. In the restricted scenario s2w;$\tilde{k}, k$, these operators are of the form:

$$V : \ell_2^{n^2 k} \longrightarrow \ell_2^{\tilde{k}}, \qquad W_\varepsilon : \ell_2^{k} \longrightarrow \ell_2^{\tilde{k}}, \qquad \tilde{V}_\varepsilon, \tilde{W}_\varepsilon : \ell_2^{\tilde{k}} \longrightarrow \ell_2^{nr}, \qquad (4.11)$$

being r some natural number. For convenience, we identify pure strategies with families of such *pure* objects, setting the notation $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon$.

We further denote $\mathfrak{S}^{\mathcal{U}}_{s2w}$ the subset of pure strategies in the s2w scenario and $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k},k}$ the corresponding subset in the model with dimensional constraints. Due to Stinespring's dilation theorem, Chapter 1, Theorem 1.29, 4., it turns out that $\mathfrak{S}^{\mathcal{U}}_{s2w} = \mathfrak{S}_{s2w}$. However, when we restrict the dimension of the considered strategies, the situation is a bit subtler and the Stinespring's dilation of the channels involved affects the relevant dimensions defining the models $\mathfrak{S}_{s2w;\tilde{k},k}$ and $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k},k}$. This is taken care of by the following lemma:

Lemma 4.12. *Any strategy $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$ can be regarded as a pure strategy $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$ where $\tilde{k}' = n^2 k \tilde{k}^4$. That is, the chain of containments $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k},k} \subseteq \mathfrak{S}_{s2w;\tilde{k},k} \subseteq \mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$ holds.*

Proof. Set a strategy $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\}$ in $\mathfrak{S}_{s2w;\tilde{k},k}$.

We are going to consider Stinespring's dilations to purify the corresponding channels

$$\mathcal{S}_\varepsilon(\,\cdot\,) = (\tilde{\mathcal{A}}_\varepsilon \otimes \tilde{\mathcal{B}}_\varepsilon) \circ (\mathcal{A} \otimes \mathcal{B}_\varepsilon)(\,\cdot\, \otimes \varphi). \tag{4.12}$$

We start with

$$\tilde{\mathcal{A}}_\varepsilon,\, \tilde{\mathcal{B}}_\varepsilon \in \mathrm{CPTP}(\ell_2^{\tilde{k}},\, \ell_2^n).$$

These channels can be lifted (due to a Stinespring's dilation) to be of the form:

$$\tilde{\mathcal{A}}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{\widetilde{anc}} \tilde{V}_\varepsilon(\,\cdot\,)\tilde{V}_\varepsilon^\dagger, \qquad \tilde{\mathcal{B}}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{\widetilde{anc}} \tilde{W}_\varepsilon(\,\cdot\,)\tilde{W}_\varepsilon^\dagger,$$

where $\tilde{V}_\varepsilon, \tilde{W}_\varepsilon \,:\, \ell_2^{\tilde{k}} \longrightarrow \ell_2^n \otimes \mathcal{H}_{\widetilde{anc}}$ are Stinespring's isometries and $\dim(\mathcal{H}_{\widetilde{anc}})$ can be upper bounded by $n\tilde{k}$.

Proceeding similarly with $\mathcal{A} \in \mathrm{CPTP}(\ell_2^{n^2k}, \ell_2^{\tilde{k}})$ and $\mathcal{B}_\varepsilon \in \mathrm{CPTP}(\ell_2^k, \ell_2^{\tilde{k}})$ we obtain:

$$\mathcal{A}(\,\cdot\,) = \mathrm{Tr}_{anc_1} V(\,\cdot\,)V^\dagger, \qquad \mathcal{B}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{anc_2} W_\varepsilon(\,\cdot\,)W_\varepsilon^\dagger,$$

for Stinespring's dilations $V : \ell_2^{n^2k} \longrightarrow \ell_2^{\tilde{k}} \otimes \mathcal{H}_{anc_1}$, $W_\varepsilon : \ell_2^k \longrightarrow \ell_2^{\tilde{k}} \otimes \mathcal{H}_{anc_2}$ such that $\dim(\mathcal{H}_{anc_1}) \leq n^2 k\tilde{k}$, $\dim(\mathcal{H}_{anc_2}) \leq k\tilde{k}$.

With all that, and denoting $\mathcal{H}_{\mathcal{A}_{anc}} \equiv \mathcal{H}_{anc_1} \otimes \mathcal{H}_{\widetilde{anc}}$, $\mathcal{H}_{\mathcal{B}_{anc}} \equiv \mathcal{H}_{anc_2} \otimes \mathcal{H}_{\widetilde{anc}}$, we define the channels

$$\begin{aligned}
\tilde{\mathcal{A}}^{\mathcal{U}}_{\varepsilon}(\,\cdot\,) &:= \mathrm{Tr}_{\mathcal{A}_{anc}} \tilde{V}_{\varepsilon} \otimes \mathrm{Id}_{anc_1}(\,\cdot\,) \tilde{V}^{\dagger}_{\varepsilon} \otimes \mathrm{Id}_{anc_1},\\
\tilde{\mathcal{B}}^{\mathcal{U}}_{\varepsilon}(\,\cdot\,) &:= \mathrm{Tr}_{\mathcal{B}_{anc}} \tilde{W}_{\varepsilon} \otimes \mathrm{Id}_{anc_2}(\,\cdot\,) \tilde{W}^{\dagger}_{\varepsilon} \otimes \mathrm{Id}_{anc_2},\\
\mathcal{A}^{\mathcal{U}}(\,\cdot\,) &:= V(\,\cdot\,)V^{\dagger}, \qquad \mathcal{B}^{\mathcal{U}}_{\varepsilon}(\,\cdot\,) := W_{\varepsilon}(\,\cdot\,)W^{\dagger}_{\varepsilon}.
\end{aligned}$$

Then, we can rewrite (4.12) as:

$$\mathcal{S}_{\varepsilon}(\,\cdot\,) = (\tilde{\mathcal{A}}^{\mathcal{U}}_{\varepsilon} \otimes \tilde{\mathcal{B}}^{\mathcal{U}}_{\varepsilon}) \circ (\mathcal{A}^{\mathcal{U}} \otimes \mathcal{B}^{\mathcal{U}}_{\varepsilon})(\,\cdot\, \otimes |\varphi\rangle\langle\varphi|).$$

But clearly the strategy $\mathcal{S}^{\mathcal{U}} := \{\tilde{\mathcal{A}}^{\mathcal{U}}_{\varepsilon}, \tilde{\mathcal{B}}^{\mathcal{U}}_{\varepsilon}, \mathcal{A}^{\mathcal{U}}, \mathcal{B}^{\mathcal{U}}_{\varepsilon}, \varphi\}_{\varepsilon}$ is pure, finishing the proof of the lemma. A careful look at the definition of the channels defining $\mathcal{S}^{\mathcal{U}}$ reveals that $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$ for some $\tilde{k}' \leq n^2 k \tilde{k}^2$. For concreteness, we fix $\tilde{k}'$ to be $n^2 k \tilde{k}^2$ enlarging the underlying Hilbert space in the obvious way if necessary.

□

With Lemmas 4.11 and 4.12 at hand we can focus now in the study of strategies in $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$. Given a general strategy $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$, Lemma 4.11 guarantees that $\mathcal{S}$ can be taken such that the dimension of the classical resources used is upper bounded by

$$\tilde{k}_{cl} \leq n^4 k^2. \tag{4.13}$$

Then, Lemma 4.12 allows us to relate $\mathcal{S}$ with a pure strategy $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$ such that

$$\tilde{k}' \leq n^2 k \tilde{k}^2. \tag{4.14}$$

Accordingly, in the rest of this manuscript we will mainly work in the model $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$ redirecting the reader to (4.14) and (4.13) for the relation with the resources used by more general strategies. However, notice that these correspondences are at most polynomial in n, k and $\tilde{k}$ and, in fact, will only introduce corrections by constant factors in the bounds we state later on. In this sense, the precise exponents in (4.14), (4.13) are irrelevant. This will become clear in the next section.

For convenience, we finish the present section recalling the expression of $\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}})$, Equation (4.9), particularized for pure strategies $\mathcal{S}^{\mathcal{U}}=$

$\{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, \varphi\}$:

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \ \mathrm{Tr}\left[\, |\psi_\varepsilon\rangle\langle\psi_\varepsilon|\, (\mathrm{Id}_C \otimes \mathcal{S}^{\mathcal{U}}_\varepsilon)\, \Big(|\psi\rangle\langle\psi|\Big)\,\right], \qquad (4.15)$$

where now:

$$\begin{aligned} &\mathcal{S}^{\mathcal{U}}_\varepsilon(\,\cdot\,) \\ &\quad = \mathrm{Tr}_{\mathcal{H}_{\mathcal{AB}_{anc}}}\left[(\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon)\,(V \otimes W_\varepsilon)\,(\,\cdot\, \otimes |\varphi\rangle\langle\varphi|)\,(V^\dagger \otimes W^\dagger_\varepsilon)\,(\tilde{V}^\dagger_\varepsilon \otimes \tilde{W}^\dagger_\varepsilon)\right], \end{aligned}$$

with $\mathcal{H}_{\mathcal{AB}_{anc}} = \mathcal{H}_{\mathcal{A}_{anc}} \otimes \mathcal{H}_{\mathcal{B}_{anc}}$.

Notice that for strategies in the more specific model $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$, the operators $\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon$ are specified as in (4.11) and, therefore, $\mathcal{H}_{\mathcal{A}_{anc}}$ and $\mathcal{H}_{\mathcal{B}_{anc}}$ in this case are identified with ℓ_2^r for some $r \in \mathbb{N}$ that will be irrelevant for us.

Remark 4.13. Alternatively, (4.15) can be rewritten as:

$$\begin{aligned} &\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \\ &\quad = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon)\,(V|ij\rangle \otimes W_\varepsilon)\,|\varphi\rangle \right\|^2_{\mathcal{H}_{\mathcal{AB}_{anc}}}. \end{aligned} \qquad (4.16)$$

As commented before, in the $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$ scenario, $\mathcal{H}_{\mathcal{AB}_{anc}} = \ell_2^{r^2}$.

Before showing the easy proof of this claim, let us clarify the notation used above. By $V|ij\rangle$ we mean the operator $V \in \mathcal{S}_\infty^{\tilde{k}', n^2 k}$ with its indices corresponding to $\ell_2^{n^2}$ contracted with the vector $|ij\rangle$. That is, if we expand V on its coordinates, $V = \sum_{k,l=1}^n \sum_{m=1}^k \sum_p^{\tilde{k}'} V_{p,klm} |p\rangle\langle klm|$, and then $V|ij\rangle = \sum_{m=1}^k \sum_p^{\tilde{k}'} V_{p,ijm} |p\rangle\langle m| \in \mathcal{S}_\infty^{\tilde{k}',k}$. Similarly with $\langle i|\tilde{V}_\varepsilon$ and $\langle j|\tilde{W}_\varepsilon$.

Proof of (4.16). In first place, we notice that for finite dimensional Hilbert spaces $\mathcal{H}$, $\mathcal{H}'$, $\mathcal{K}$, any vectors $|\xi\rangle \in \mathcal{H}$, $|\eta\rangle \in \mathcal{H}'$ and any operator $U \in \mathcal{S}_\infty(\mathcal{H}', \mathcal{H} \otimes \mathcal{K})$

$$\begin{aligned} \mathrm{Tr}\left[|\xi\rangle\langle\xi|\, \mathrm{Tr}_{\mathcal{K}} U\, |\eta\rangle\langle\eta|\, U^\dagger\right] &= \mathrm{Tr}\left[(|\xi\rangle\langle\xi| \otimes \mathrm{Id}_{\mathcal{K}})\, U\, |\eta\rangle\langle\eta|\, U^\dagger\right] \\ &= \langle\eta|U^\dagger(|\xi\rangle \otimes \mathrm{Id}_{\mathcal{K}})\, (\langle\xi| \otimes \mathrm{Id}_{\mathcal{K}})\, U\, |\eta\rangle \\ &= \left\|(\langle\xi| \otimes \mathrm{Id}_{\mathcal{K}})\, U\, |\eta\rangle\right\|^2_{\mathcal{K}}. \end{aligned}$$

Applying this elementary identity to $|\psi_\varepsilon\rangle \in \mathcal{H}_\mathcal{A}\otimes\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_\mathcal{C}\equiv\mathcal{H}$, $|\psi\rangle\otimes|\varphi\rangle\in\mathcal{H}_\mathcal{A}\otimes\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_\mathcal{C}\otimes\mathcal{H}_{\mathcal{A}_E}\otimes\mathcal{H}_{\mathcal{B}_E}\equiv\mathcal{H}'$ and the operator $\mathrm{Id}_C\otimes(\tilde{V}_\varepsilon\otimes\tilde{W}_\varepsilon)\,(V\otimes W_\varepsilon)\in\mathcal{S}_\infty(\mathcal{H}',\mathcal{H}\otimes\mathcal{H}_{\mathcal{AB}_{anc}})$ we have that, for each $\varepsilon\in\mathcal{Q}_{n^2}$:

$$\begin{aligned}&\mathrm{Tr}\Big[\,|\psi_\varepsilon\rangle\langle\psi_\varepsilon|\,(\mathrm{Id}_C\otimes\mathcal{S}^{\mathcal{U}}_\varepsilon)\,\Big(|\psi\rangle\langle\psi|\Big)\,\Big]\\ &\quad=\mathbb{E}_\varepsilon\,\Big\|(\langle\psi_\varepsilon|\otimes\mathrm{Id}_{\mathcal{AB}_{anc}})\Big(\mathrm{Id}_C\otimes(\tilde{V}_\varepsilon\otimes\tilde{W}_\varepsilon)\,(V\otimes W_\varepsilon)\Big)\,(|\psi\rangle\otimes|\varphi\rangle)\Big\|^2_{\mathcal{H}_{\mathcal{AB}_{anc}}}.\end{aligned}$$

Equation (4.16) is obtained from the last line above just recalling the definitions $|\psi_\varepsilon\rangle=\frac{1}{n}\sum_{i,j=1}^n\varepsilon_{ij}|ij\rangle_{AB}\otimes|ij\rangle_C$, $|\psi\rangle=\frac{1}{n}\sum_{i,j=1}^n|ij\rangle_{AB}\otimes|ij\rangle_C$. □

4.6 Bounds for "smooth" strategies

This section is devoted to the proof of Theorem 4.1, which provides lower bounds on resources needed to break G_{Rad} by strategies characterized by regularity parameters based on Definition 4.5, Section 4.4. When we refer here to a cheating strategy for G_{Rad}, unless the opposite is explicitly specified, we mean a pure strategy $\mathcal{S}^{\mathcal{U}}=\{\tilde{V}_\varepsilon,\,\tilde{W}_\varepsilon,\,V,\,W_\varepsilon,\,|\varphi\rangle\}_\varepsilon\in\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$.

As we have explained before, the main idea leading to Theorem 4.1 is the understanding of cheating strategies for G_{Rad} as assignments on the hypercube $\mathcal{Q}_{n^2}$, i.e., vector-valued functions $\Phi:\mathcal{Q}_{n^2}\to X$ where X is a suitable Banach space. Given a strategy $\mathcal{S}^{\mathcal{U}}$, the corresponding assignment $\Phi_{\mathcal{S}^{\mathcal{U}}}$ must be related with the value attained by the strategy, $\omega(G_{Rad};\mathcal{S}^{\mathcal{U}})$. Ideally, we hope to bound $\omega(G_{Rad};\mathcal{S}^{\mathcal{U}})$ by the expected value of the norm of $\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)$, quantity for which we can use Corollary 4.8 to obtain upper bounds. Equation (4.16) gives us a first hint on how to construct $\Phi_{\mathcal{S}^{\mathcal{U}}}$. Given $\mathcal{S}^{\mathcal{U}}=\{\tilde{V}_\varepsilon,\,\tilde{W}_\varepsilon,\,V,\,W_\varepsilon,\,|\varphi\rangle\}_\varepsilon$, consider the map:

$$\begin{array}{rccc}\Phi_{\mathcal{S}^{\mathcal{U}}}: & \mathcal{Q}_{n^2} & \longrightarrow & \ell_2^{r^2}\\ & \varepsilon & \mapsto & \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\end{array},\qquad(4.17)$$

where

$$\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) := \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\left(\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon \right) \left(V|ij\rangle \otimes W_\varepsilon \right) |\varphi\rangle \right),$$

and r is determined by the strategy, recall (4.11).

The referred Equation (4.16) now reads:

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \|\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|^2_{\ell_2^{r^2}}, \tag{4.18}$$

so we are in good track. Since $\|\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\ell_2^{r^2}} \leq 1 \ \forall \varepsilon \in \mathcal{Q}_{n^2}$, we can use the trivial bound $\mathbb{E}_\varepsilon \|\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|^2_{\ell_2^{r^2}} \leq \mathbb{E}_\varepsilon \|\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\ell_2^{r^2}}$ and Corollary 4.8 to obtain – recall Definition 4.5 for $\sigma_{\Phi_{\mathcal{S}^{\mathcal{U}}}}$:

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\ell_2^{r^2}} + C \ \sigma_{\Phi_{\mathcal{S}^{\mathcal{U}}}} \mathrm{T}_2^{(n^2)}(\ell_2^{r^2}).$$

Furthermore, $\mathrm{T}_2^{(n^2)}(\ell_2^{r^2}) = 1$ since, more generally, $\mathrm{T}_2(\ell_2^{r^2}) = 1$.

The main problem with this approach is that the quantity $\left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\ell_2^{r^2}}$ might be of the same order as $\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}})$, making the previous bound trivial. The reason is that we can easily modify the map $\Phi_{\mathcal{S}^{\mathcal{U}}}$ *without increasing* any relevant dimension composing $\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)$ with an ε dependent unitary that “aligns” all vectors $\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)$ in the same direction. For this modified map, $\|\mathbb{E}_\varepsilon \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|^2_{\ell_2^{r^2}} = \mathbb{E}_\varepsilon \|\Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|^2_{\ell_2^{r^2}} = \omega(G_{Rad}; \mathcal{S}^{\mathcal{U}})$. The approach presented so far is unable to detect such an artefact, so we now look at alternative constructions for $\Phi_{\mathcal{S}^{\mathcal{U}}}$.

Next, we simplify the image of the map $\Phi_{\mathcal{S}^{\mathcal{U}}}$ at the expense of considering more involved choices for the output Banach space. This allows us to preserve an equivalence of the kind of (4.18) while obtaining good upper bounds for $\left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_X$.

Given a strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon$ we define the following two alternatives to $\Phi_{\mathcal{S}^{\mathcal{U}}}$:

$$\begin{array}{rccc} \Phi^i_{\mathcal{S}^{\mathcal{U}}} : & \mathcal{Q}_{n^2} & \longrightarrow & \mathcal{S}_\infty^{r^2, k\tilde{k}'} \\ & \varepsilon & \mapsto & \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \end{array},$$

with

$$\Phi^{i}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) := \frac{1}{n^2}\sum_{ij} \varepsilon_{ij}\left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon\right)\left(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}\right);$$

and

$$\begin{array}{rccc} \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}: & \mathcal{Q}_{n^2} & \longrightarrow & \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n} \\ & \varepsilon & \mapsto & \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \end{array},$$

with

$$\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) = \frac{1}{n^2}\sum_{ij} \varepsilon_{ij}\, \langle i| \otimes \langle j| \otimes \left(V|ij\rangle \otimes W_\varepsilon\right)|\varphi\rangle.$$

These are the central objects we study to obtain Theorem 4.1. Recall that the output space in $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$ was defined at the end of Section 4.4 as the interpolation space $(\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}, \mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n})_{1/2}$.

Now we comment on the idea behind the definition of these maps: recall that a strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon,\, \tilde{W}_\varepsilon,\, V,\, W_\varepsilon,\, |\varphi\rangle\}_\varepsilon$ consists of two rounds of local operations with a communication stage in between. Fixing the first round, that is related to V, W_ε and $|\varphi\rangle$, and understanding the optimization over any $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$ as computing a particular norm, leads to the definition of $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$. When the elements we fix are $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$ and V – this last one is ε-independent –, and the optimization is taken over $(\mathrm{Id}_{\ell_2^k} \otimes W_\varepsilon)|\varphi\rangle$, the map $\Phi^{i}_{\mathcal{S}^{\mathcal{U}}}$ is naturally obtained.

Next we describe how these maps are related to G_{Rad}, postponing the proofs to Section 4.6.1.

Lemma 4.14. *For any strategy $\mathcal{S}^{\mathcal{U}}$,*

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\| \Phi^{i(ii)}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{X^{i(ii)}},$$

where we have denoted $X^i = \mathcal{S}_\infty^{r^2, k\tilde{k}'}$ and $X^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$.

Remark 4.15. For $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$, the previous statement can be strengthen to

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\| \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}},$$

where $\tilde{X}^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}$. Recall Chapter 2, Definition 2.13 for this last norm.

The regularity of these maps can be characterized by parameters $\sigma^i_{\mathcal{S}^{\mathcal{U}}} := \sigma_{\Phi^i_{\mathcal{S}^{\mathcal{U}}}}$ and $\sigma^{ii}_{\mathcal{S}^{\mathcal{U}}} := \sigma_{\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}}$ – recall Definition 4.5. More explicitly:

$$\sigma^{i(ii)}_{\mathcal{S}^{\mathcal{U}}} = \log(n^2)\, \mathbb{E}_\varepsilon \left(\sum_{i,j} \| \partial_{ij} \Phi^{i(ii)}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \|^2_{X^{i(ii)}} \right)^{1/2} . \tag{4.19}$$

These quantities can be bounded by the easier expressions appearing in Section 4.2. See Appendix B.1 for details.

In the case of an arbitrary (possibly *non-pure*) strategy $\mathcal{S}$, we can assign parameters $\sigma^i_{\mathcal{S}}$, $\sigma^{ii}_{\mathcal{S}}$ to $\mathcal{S}$ with the simple prescription:

$$\sigma^{i(ii)}_{\mathcal{S}} := \inf_{\substack{\mathcal{S}^{\mathcal{U}} \\ \text{purifying } \mathcal{S}}} \sigma^{i(ii)}_{\mathcal{S}^{\mathcal{U}}} .$$

With definition (4.19) at hand and taking into account Corollary 4.8 and Lemma 4.14 (with the refinement in Remark 4.15), we can obtain:

Lemma 4.16. *For any strategy $\mathcal{S}^{\mathcal{U}}$,*

i.

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{X^i} + C\ \sigma^i_{\mathcal{S}^{\mathcal{U}}}\ \mathrm{T}_2^{(n^2)}\left(X^i \right),$$

ii.

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C\ \sigma^{ii}_{\mathcal{S}^{\mathcal{U}}}\ \mathrm{T}_2^{(n^2)}\left(X^{ii} \right),$$

where we have denoted $\tilde{X}^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}$.

Comment 4.6.1. Notice the change of norms in the second item of the lemma. This refinement is needed later on in order to obtain Proposition 4.17 below.

Lemma 4.16 allows us to somehow exchange the lack of control on the behaviour of a general strategy by the control of some properties of the Banach spaces involved. Bounding the quantities appearing there, we obtain our main result:

Theorem 4.1 (Formal statement)**.** *Given an arbitrary strategy $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$,* *I.*

$$\omega(G;\mathcal{S}) \leq C_1 + C_2\ \sigma^i_{\mathcal{S}}\ \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\omega(G;\mathcal{S}) \leq \tilde{C}_1 + C_3\ \tilde{\sigma}^{ii}_{\mathcal{S}}\ \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}} + \frac{\log(n)\log^{1/2}(k\tilde{k})}{n}\right),$$

where we have denoted $\tilde{\sigma}^{ii}_{\mathcal{S}} = n^{3/4}\log(n)\,\sigma^{ii}_{\mathcal{S}}$*.*

Above, C_1, $\tilde{C}_1$, C_2, C_3 *are positive constants such that* $C_1.\tilde{C}_1$ *are strictly lower than 1.*

Proof. To obtain the statement of the theorem, as we already said, we start considering Lemma 4.16. Then, we need to bound:

1. the type constants $\mathrm{T}_2^{(n^2)}(X^i)$ and $\mathrm{T}_2^{(n^2)}(X^{ii})$. These bounds are already provided in Equations (4.2) and (4.1), respectively. We recall these bounds here for reader's convenience:

$$\mathrm{T}_2^{(n^2)}(X^i) \leq \mathrm{T}_2(X^i) \lesssim \log^{1/2}(k\tilde{k}'),$$

$$\mathrm{T}_2^{(n^2)}(X^{ii}) \lesssim n^{3/4}\log(n)\log^{1/2}(n\tilde{k}');$$

2. the terms $\left\|\mathbb{E}_\varepsilon \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|_{X^i}$ and $\left\|\mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|_{\tilde{X}^{ii}}$. These quantities are handled by Proposition 4.17 below.

With this we obtain the stated bound in the case of pure strategies. Nonetheless, statements about pure strategies can be transformed into statements about general strategies taking into account the relation (4.14). As we said at the end of Section 4.5, this relation is polynomial in the parameters involved and therefore, the change from pure to general strategies only induces corrections by constant factors that can be absorbed in the constants C_2, C_3 present in the statement. Similar considerations deals with the amount of classical communication included in $\tilde{k}$, in this case one has to recall Equation (4.13). See Appendix B.2 for further details. □

In the rest of this section we first state the proposition alluded in the previous proof and then give the proofs, in this order, of Lemma 4.14, Lemma 4.16 and Proposition 4.17.

Proposition 4.17. *For any pure strategy $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k}',k}$:*

i.
$$\left\| \mathbb{E}_\varepsilon \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{X^i} \leq \frac{3}{4} + \frac{C}{\sqrt{n}}.$$

ii.
$$\left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} \leq \frac{\sqrt{3}}{2} + \frac{C'}{\sqrt{n}} + C'' \frac{\log(n)\log^{1/2}(k\tilde{k}')}{n}.$$

Here C, C', C'' are universal constants.

4.6.1 Proof of Lemmas 4.14 and 4.16

Proof of Lemma 4.14. The proof of both items in the lemma follows the same structure. We start with the bound regarding $\Phi^i_{\mathcal{S}^{\mathcal{U}}}$:

Recalling (4.16):

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon)\, (V|ij\rangle \otimes W_\varepsilon)\, |\varphi\rangle \right\|^2_{\ell_2^{r^2}}.$$

We bound this quantity as follows:

$$\begin{aligned}
&\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \\
&\quad = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon)\, (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}})\, (\mathrm{Id}_{\ell_2^k} \otimes W_\varepsilon)\, |\varphi\rangle \right\|^2_{\ell_2^{r^2}} \\
&\quad \leq \mathbb{E}_\varepsilon \sup_{|\varphi\rangle \in \mathsf{ball}(\ell_2^{k\tilde{k}'})} \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon)\, (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})\, |\varphi\rangle \right\|^2_{\ell_2^{r^2}} \\
&\quad = \mathbb{E}_\varepsilon \sup_{|\varphi\rangle \in \mathsf{ball}(\ell_2^{k\tilde{k}'})} \left\| \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)(|\varphi\rangle) \right\|^2_{\ell_2^{r^2}} = \mathbb{E}_\varepsilon \left\| \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|^2_{\mathcal{S}_\infty^{r^2, k\tilde{k}'}} \\
&\quad \leq \mathbb{E}_\varepsilon \left\| \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\mathcal{S}_\infty^{r^2, k\tilde{k}'}} \equiv \mathbb{E}_\varepsilon \left\| \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{X^i}.
\end{aligned}$$

For $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$, we prove a stronger result. That is, considering the map $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$ taking values on the space $\tilde{X}^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}$, we show that:

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\| \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}}. \tag{4.20}$$

Since the norm in $\tilde{X}^{ii}$ is smaller than in X^{ii}, cf. Proposition 4.9, the statement of the lemma is also true. Following the proof of the first item, we start bounding:

$$\begin{aligned}
&\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \\
&\quad = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i | \tilde{V}_\varepsilon \otimes \langle j | \tilde{W}_\varepsilon) \left(V |ij\rangle \otimes W_\varepsilon \right) |\varphi\rangle \right\|^2_{\ell_2^{r^2}} \\
&\quad \leq \mathbb{E}_\varepsilon \sup_{\tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr,\tilde{k}'})} \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i | \tilde{V} \otimes \langle j | \tilde{W}) \left(V |ij\rangle \otimes W_\varepsilon \right) |\varphi\rangle \right\|^2_{\ell_2^{r^2}} \\
&\quad = \mathbb{E}_\varepsilon \sup_{\tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr,\tilde{k}'})} \left\| (\tilde{V} \otimes \tilde{W}) \left(\frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left(\langle i | \otimes \langle j | \right) \left(V |ij\rangle \otimes W_\varepsilon \right) |\varphi\rangle \right) \right\|^2_{\ell_2^{r^2}} \\
&\quad = \mathbb{E}_\varepsilon \sup_{\tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr,\tilde{k}'})} \left\| (\tilde{V} \otimes \tilde{W}) \left(\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right) \right\|^2_{\ell_2^{r^2}} \\
&\quad \overset{\text{(Lemma 2.16)}}{\leq} \mathbb{E}_\varepsilon \left\| \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|^2_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}} \\
&\quad \leq \mathbb{E}_\varepsilon \left\| \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}} \equiv \mathbb{E}_\varepsilon \left\| \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}}.
\end{aligned}$$

□

Proof of Lemma 4.16. The first item is a direct consequence of Corollary 4.8 applied to the bound in Lemma 4.14, i.

The second item proceed similarly but with a small detour. Using now Pisier's inequality, Lemma 4.7 (with $p = 1$ and a trivial triangle inequality, as in the proof of Corollary 4.8), from inequality (4.20) we obtain

$$\mathbb{E}_\varepsilon \left\| \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} \le \left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C \, \log(n) \, \mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_{k,l=1}^{n} \tilde{\varepsilon}_{kl} \partial_{kl} \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} .$$

Now, according to Proposition 2.15, we can upper bound the last summand above changing the norm $\tilde{X}^{ii}$ by X^{ii}. Considering that

$$\mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_{k,l=1}^{n} \tilde{\varepsilon}_{kl} \partial_{kl} \Phi^{ii}(\varepsilon) \right\|_{X^{ii}} \lesssim \mathrm{T}_2^{(n^2)}(X^{ii}) \;\; \mathbb{E}_\varepsilon \left(\sum_{k,l=1}^{n} \left\| \partial_{kl} \Phi^{ii}(\varepsilon) \right\|^2_{X^{ii}} \right)^{1/2} ,$$

we have:

$$\begin{aligned} &\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \\ &\quad \le \left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C \, \log(n) \, \mathrm{T}_2^{(n^2)}(X^{ii}) \;\; \mathbb{E}_\varepsilon \left(\sum_{k,l=1}^{n} \left\| \partial_{kl} \Phi^{ii}(\varepsilon) \right\|^2_{X^{ii}} \right)^{1/2} . \end{aligned}$$

We obtain Lemma 4.16, ii., identifying $\sigma^{ii}_{\mathcal{S}^{\mathcal{U}}}$ above.

□

4.6.2 Proof of Proposition 4.17

Finally, as promised, we prove Proposition 4.17:

Proof of Proposition 4.17, i. The norm in the L.H.S. of Proposition 4.17, i., is attained at unit vectors $|\varphi\rangle \in \ell_2^{k\tilde{k}'}$, $|\xi\rangle \in \ell_2^{r^2}$ (independent of ε):

$$\left\| \mathbb{E}_\varepsilon \Phi^{i}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\mathcal{S}_\infty^{r^2, k\tilde{k}'}} = \left| \mathbb{E}_\varepsilon \, \langle \xi | \, \Phi^{i}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \, |\varphi\rangle \right| \le \mathbb{E}_\varepsilon \, \left| \langle \xi | \, \Phi^{i}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \, |\varphi\rangle \right| .$$

Expanding this expression, we have:

$$\begin{aligned} &\| \mathbb{E}_\varepsilon \; \Phi^{i}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \|_{\mathcal{S}_\infty^{r^2, k\tilde{k}'}} \\ &\quad \le \mathbb{E}_\varepsilon \, \Big| \, \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \langle \xi | \left(\langle i | \tilde{V}_\varepsilon \otimes \langle j | \tilde{W}_\varepsilon \right) \left(V \; |ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}} \right) |\varphi\rangle \, \Big| \\ &\quad = \mathbb{E}_\varepsilon \, \left| \langle \overline{\xi}_\varepsilon \, | \, \overline{\varphi} \rangle \right| , \end{aligned}$$

where we have defined the unit vectors:

$$\langle \overline{\xi}_\varepsilon| := \frac{1}{n}\sum_{i,j} \varepsilon_{ij} \langle ij|_C \otimes \langle \xi| \Big(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon \Big),$$

$$|\overline{\varphi}\rangle := \frac{1}{n}\sum_{i,j} |ij\rangle_C \otimes \Big(V\ |ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}} \Big) |\varphi\rangle.$$

Now, notice that there exists at least one ε^* such that $|\langle \overline{\xi}_{\varepsilon^*}\,| \overline{\varphi}\rangle| \geq \|\mathbb{E}_\varepsilon\ \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}}$. Moreover, $\langle \overline{\xi}_{\varepsilon^*}\,| \overline{\varphi}\rangle$ can be taken to be real w.l.o.g., since we can absorb any phase in $|\overline{\varphi}\rangle$ without changing our argument. This is taken into account in the rest of the proof. Next, consider ε^* to rewrite $|\overline{\varphi}\rangle = |\overline{\xi}_{\varepsilon^*}\rangle + (|\overline{\varphi}\rangle - |\overline{\xi}_{\varepsilon^*}\rangle)$. An application of Cauchy-Schwartz inequality gives us the following:

$$\begin{aligned}\|\mathbb{E}_\varepsilon\ \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}} &\leq \mathbb{E}_\varepsilon\ \Big|\langle \overline{\xi}_\varepsilon|\overline{\varphi}\rangle\Big| \\ &\leq \mathbb{E}_\varepsilon\ \Big|\langle \overline{\xi}_\varepsilon|\overline{\xi}_{\varepsilon^*}\rangle\Big| + \Big|\langle \overline{\varphi} - \overline{\xi}_{\varepsilon^*}|\overline{\varphi} - \overline{\xi}_{\varepsilon^*}\rangle\Big|^{1/2}. \qquad (4.21)\end{aligned}$$

Now we bound both summands in the R.H.S. of the previous expression separately:

- For the second:

$$\begin{aligned}&\Big|\langle \overline{\varphi} - \overline{\xi}_{\varepsilon^*}|\overline{\varphi} - \overline{\xi}_{\varepsilon^*}\rangle\Big|^{1/2} \\ &\quad\leq \Big(2(1 - \langle \overline{\xi}_{\varepsilon^*}|\overline{\varphi}\rangle)\Big)^{1/2} \leq \Big(2(1 - \|\mathbb{E}_\varepsilon\ \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}})\Big)^{1/2} \\ &\quad\leq \frac{7}{4} - \frac{4}{3}\|\mathbb{E}_\varepsilon\ \Phi^i_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}}.\end{aligned}$$

- For the first one, we have the following bound:

$$\begin{aligned}
\mathbb{E}_\varepsilon \left| \langle \bar{\xi}_\varepsilon | \bar{\xi}_{\varepsilon^*} \rangle \right| &= \mathbb{E}_\varepsilon \left| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon^*_{ij} \langle \xi | \left(\langle i | \tilde{V}_\varepsilon \tilde{V}^\dagger_{\varepsilon^*} | i \rangle \otimes \langle j | \tilde{W}_\varepsilon \tilde{W}^\dagger_{\varepsilon^*} | j \rangle \right) | \xi \rangle \right| \\
&\leq \mathbb{E}_\varepsilon \sup_{\substack{|\xi_i\rangle, |\varphi_j\rangle \in \mathsf{ball}(\ell_2^{r^2}) \\ \text{for } i,j=1,\dots,n}} \left| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon^*_{ij} \langle \xi_i | \varphi_j \rangle \right| \\
&\approx \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon^*_{ij} |i\rangle \otimes |j\rangle \right\|_{\ell_1^n \otimes_\varepsilon \ell_1^n} \\
&= \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} |i\rangle \otimes |j\rangle \right\|_{\ell_1^n \otimes_\varepsilon \ell_1^n}.
\end{aligned}$$

In the last two lines we have used, in this order, Grothendieck's inequality [40] and the fact that $\{\varepsilon_{ij}\varepsilon^*_{ij}\}_{i,j}$ are i.i.d. Rademacher random variables for any fixed signs $\varepsilon^*_{i,j}$. Finally, to conclude we can bound:

$$\mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} |i\rangle \otimes |j\rangle \right\|_{\ell_1^n \otimes_\varepsilon \ell_1^n} \lesssim \frac{1}{\sqrt{n}}.$$

One way to see this is considering the metric mapping property of the injective tensor norm and the estimate $\|\mathrm{Id} : \ell_2^n \to \ell_1^n\| = \sqrt{n}$. With this:

$$\begin{aligned}
\mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} |i\rangle \otimes |j\rangle \right\|_{\ell_1^n \otimes_\varepsilon \ell_1^n} &\leq n \, \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} |i\rangle \otimes |j\rangle \right\|_{\ell_2^n \otimes_\varepsilon \ell_2^n} \\
&= \frac{1}{n} \, \mathbb{E}_\varepsilon \left\| \sum_{ij} \varepsilon_{ij} |i\rangle\langle j| \right\|_{\mathcal{S}_\infty^n}.
\end{aligned}$$

The well-known estimate $\mathbb{E}_\varepsilon \left\| \sum_{ij} \varepsilon_{ij} |i\rangle\langle j| \right\|_{\mathcal{S}_\infty^n} \lesssim \sqrt{n}$ provides the desired bound.

Joining everything in (4.21) we obtain the bound in Proposition 4.17, i.

□

Proof of Proposition 4.17, ii. Notice first that, up to this point, we already have a full proof of Theorem 4.1, I. It turns out that Proposition 4.17, ii. is a consequence of this first part of our main theorem.

The key idea to see this is to understand the norm $\left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}} \right\|_{\tilde{X}^{ii}}$ as the optimization over a family of strategies with small enough parameter $\sigma^i_{\mathcal{S}^{\mathcal{U}}}$. Concretely, considering the characterization of the norm $\tilde{X}^{ii}$ given in Lemma 2.16, we can prove that

$$\left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} \leq \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr, \tilde{k}'})}} \omega^{1/2} \left(G_{Rad}; \{ \tilde{V},\, \tilde{W},\, V,\, W_\varepsilon,\, |\varphi\rangle \}_\varepsilon \right). \tag{4.22}$$

The desired bound follows now from realizing that in the strategies on which this optimization is performed, the second round of local operations, $\tilde{V} \otimes \tilde{W}$, is ε-independent. Therefore, for these strategies, according to Example 4.6, $\sigma^i \approx \frac{\log(n)}{n}$, which, in conjunction with Theorem 4.1, I., leads to the desired statement. To obtain the precise statement appearing there, we have considered the elementary inequality $\sqrt{1+x} \leq 1 + x/2$.

Then, to finish, let us prove claim (4.22).

Recall that, according to Lemma 2.16 in Chapter 2, we can write:

$$\begin{aligned} &\left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} \\ &\quad = \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr, \tilde{k}'})}} \left\| \mathbb{E}_\varepsilon \, (\tilde{V} \otimes \tilde{W}) \Big(\frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left((\langle i| \otimes \langle j|)\, (V |ij\rangle \otimes W_\varepsilon) \, |\varphi\rangle \right) \Big) \right\|_{\ell_2^{r^2}} \\ &\quad \leq \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr, \tilde{k}'})}} \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left((\langle i|\tilde{V} \otimes \langle j|\tilde{W})\, (V |ij\rangle \otimes W_\varepsilon) \, |\varphi\rangle \right) \right\|_{\ell_2^{r^2}}. \end{aligned}$$

Furthermore, considering the elementary bound $\mathbb{E}_\varepsilon\, \phi(\varepsilon) \leq \left(\mathbb{E}_\varepsilon\, \phi(\varepsilon)^2\right)^{\frac{1}{2}}$, valid for any function $\phi : \mathcal{Q}_{n^2} \to \mathbb{R}$, we can finally write:

$$\begin{aligned} &\left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} \\ &\quad \leq \sup_{\substack{r\in\mathbb{N} \\ \tilde{V},\, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr,\tilde{k}'})}} \left(\mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left(\langle i| \tilde{V} \otimes \langle j| \tilde{W} \right) \left(V|ij\rangle \otimes W_\varepsilon \right) |\varphi\rangle \right\|^2_{\ell_2^{r^2}} \right)^{\frac{1}{2}} \\ &\quad = \sup_{\substack{r\in\mathbb{N} \\ \tilde{V},\, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{nr,\tilde{k}'})}} \omega^{1/2} \left(G_{Rad}; \{ \tilde{V},\, \tilde{W},\, V,\, W_\varepsilon,\, |\varphi\rangle \}_\varepsilon \right), \end{aligned}$$

as claimed. □

We make a final comment that, in some sense, connects with the next section, where we discuss possible extensions of the approach presented up to this point.

Remark 4.18. The appearance of the norms $X^i = \mathcal{S}_\infty^{r^2, k\tilde{k}'}$, $X^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$ above might seem, at some point, arbitrary, in the sense that we have used these norms to *upper* bound the value $\omega(G_{Rad}, \mathcal{S}^{\mathcal{U}})$ being these upper bounds not tight in general. Part of the motivation to consider these spaces is the fact that we are able to properly understand their type properties. But we can wonder: is any norm upper bounding $\omega(G_{Rad}, \mathcal{S}^{\mathcal{U}})$ a reasonable choice provided that we can control the relevant type constants? This is not the case. Actually, in Section 4.7 we explore further this issue. For the moment, let us note that the chosen norms also satisfy some basic normalization conditions. In particular, it can be shown that the elements constituting $\Phi^i_{\mathcal{S}^{\mathcal{U}}}$, $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$ are well normalized when regarded as elements in X^i and X^{ii}, respectively. Concretely, for each $i,\, j \in [n]$

$$\left\| \left(\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon \right) \left(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}} \right) \right\|_{X^i} \leq 1$$

and

$$\| \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes W_\varepsilon)|\varphi\rangle \|_{X^{ii}} \ \leq 1,$$

no matters which are the operators $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$, V, W_ε as long as they are contractive or which is the vector $|\varphi\rangle$ as long as its Euclidean norm is upper bounded by one.

The first bound is straightforward. Since $\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon$ and $V \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}$ are contractive operators, $\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon$ and $V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}$ are also contractive and the same applies to their composition.

For the second bound, fixing i, j, we first notice that $|\tilde{\varphi}\rangle := (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})(\mathrm{Id}_{\ell_2^k} \otimes W_\varepsilon)|\varphi\rangle$ has norm $\||\tilde{\varphi}\rangle\|_{\ell_2^{\tilde{k}'2}} \leq 1$. Furthermore, considering the norm-one injections $\iota_i : \ell_2^{\tilde{k}'} \ni |\varphi\rangle \mapsto |i\rangle \otimes |\varphi\rangle \in \mathcal{S}_1^{\tilde{k}',n}$, we have that $|i\rangle \otimes |j\rangle \otimes |\tilde{\varphi}\rangle = \iota_i \otimes \iota_j\Big(|\tilde{\varphi}\rangle\Big)$. Therefore

$$\begin{aligned}
&\Big\||i\rangle \otimes |j\rangle \otimes |\tilde{\varphi}\rangle\Big\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}} \\
&\quad \leq \Big\||\tilde{\varphi}\rangle\Big\|_{\ell_2^{\tilde{k}'2}} \Big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}'2} \to \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}\Big\| \\
&\quad \leq 1.
\end{aligned}$$

It remains to justify that, in fact,

$$\Big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}'2} \to \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}\Big\| \leq 1.$$

This can be proved recalling that $\mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$ is the interpolation space $\Big(\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}, \mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n}\Big)_{\frac{1}{2}}$ and $\ell_2^{\tilde{k}'2}$ can be also regarded as the space $\Big(\ell_2^{\tilde{k}'} \otimes_\varepsilon \ell_2^{\tilde{k}'}, \ell_2^{\tilde{k}'} \otimes_\pi \ell_2^{\tilde{k}'}\Big)_{\frac{1}{2}}$. Then,

$$\begin{aligned}
&\Big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}'} \to \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}\Big\| \\
&\qquad \leq \Big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}'} \otimes_\varepsilon \ell_2^{\tilde{k}'2} \to \mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}\Big\|^{\frac{1}{2}} \\
&\qquad\quad \Big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}'} \otimes_\pi \ell_2^{\tilde{k}'} \to \mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n}\Big\|^{\frac{1}{2}} \\
&\qquad \leq \Big\|\iota_i : \ell_2^{\tilde{k}'} \to \mathcal{S}_1^{\tilde{k}',n}\Big\| \Big\|\iota_j : \ell_2^{\tilde{k}'} \to \mathcal{S}_1^{\tilde{k}',n}\Big\| \\
&\qquad \leq 1.
\end{aligned}$$

4.7 A conjecture towards unconditional lower bounds

In the previous section, we have modified the naïve choice (4.17) for $\Phi_{\mathcal{S}^{\mathcal{U}}}$ in order to circumvent the problem that $\left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\ell_2^{r^2}}$ can be in general too large, damning that way the bounds obtained through Corollary 4.8 to be trivial. The variations $\Phi^{i}_{\mathcal{S}^{\mathcal{U}}}$, $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$ allowed us to obtain the bounds in Theorem 4.1. An unsatisfactory feature of this result is that, in order to obtain concrete bounds on the quantum resources employed by a given strategy for G_{Rad}, we still need to make some additional assumption on that strategy. Recall that, in particular, the bounds in Theorem 4.1 depend on the regularity parameters $\sigma^{i}_{\mathcal{S}^{\mathcal{U}}}$, $\sigma^{ii}_{\mathcal{S}^{\mathcal{U}}}$. Ideally, we would like to obtain bounds only depending on the dimension of the quantum systems Alice and Bob manipulate.

Following this line of thought, one could ask whether given a strategy $\mathcal{S}^{\mathcal{U}}$ it is possible to construct a corresponding assignment $\Phi_{\mathcal{S}^{\mathcal{U}}}$ that additionally display the property of being regular enough, that is, with $\sigma_{\Phi_{\mathcal{S}^{\mathcal{U}}}} \lesssim_{\log} 1/n$. The answer is affirmative, but the cost of doing so is that the output Banach space of $\Phi_{\mathcal{S}^{\mathcal{U}}}$ becomes more involved and its type properties escape from the techniques used in this work. Given a strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon$, we define:

$$\begin{array}{rccc} \Phi^{iii}_{\mathcal{S}^{\mathcal{U}}} : & \mathcal{Q}_{n^2} & \longrightarrow & \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k}',n} \right) \otimes_\varepsilon \ell_2^{k\tilde{k}'} \\ & \varepsilon & \mapsto & \Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \end{array}, \qquad (4.23)$$

where

$$\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) := \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}).$$

This map relates with the value of the game G_{Rad} as stated in the following

Lemma 4.19. *For any pure strategy $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k}',k}$:*

$$\omega^{1/2}(G_{Rad}; \mathcal{S}^{\mathcal{U}}) \lesssim \mathbb{E}_\varepsilon \, \|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{X^{iii}},$$

where $X^{iii} := \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$.

Proof. For each $\varepsilon \in \mathcal{Q}_{n^2}$, we have to interpret the tensor $\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)$ as the mapping:

$$\begin{array}{rccc} \Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon): & \ell_2^{k\tilde{k}'} & \longrightarrow & \mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k}',n} \\ & |\varphi\rangle & \mapsto & \Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)(|\varphi\rangle) \end{array},$$

where

$$\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)(|\varphi\rangle) = \frac{1}{n^2}\sum_{ij} \varepsilon_{ij} \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}})\,|\varphi\rangle.$$

Then, the norm of this map is

$$\begin{aligned} &\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\| \\ &\quad = \sup_{|\varphi\rangle \in \mathsf{ball}(\ell_2^{k\tilde{k}'})} \left\| \frac{1}{n^2}\sum_{ij} \varepsilon_{ij} \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}})\,|\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k}',n}} \\ &\quad = \sup_{\substack{W \in \mathsf{ball}(\mathcal{S}_\infty^{\tilde{k}'}) \\ |\varphi\rangle \in \mathsf{ball}(\ell_2^{k\tilde{k}'})}} \left\| \frac{1}{n^2}\sum_{ij} \varepsilon_{ij} \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes W)\,|\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k}',n}}. \end{aligned}$$

Recalling again Chapter 2, Lemma 2.16, and proceeding similarly to the proof of Proposition 4.17, ii., we can write explicitly the norm above as:

$$\begin{aligned} &\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\| \\ &\quad = \sup_{\substack{m \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in \mathsf{ball}(\mathcal{S}_\infty^{\tilde{k}',nm}) \\ W \in \mathsf{ball}(\mathcal{S}_\infty^{\tilde{k}'}),\, |\varphi\rangle \in \mathsf{ball}(\ell_2^{k\tilde{k}'})}} \left\| \frac{1}{n^2}\sum_{ij} \varepsilon_{ij} \left(\langle i|\tilde{V} \otimes \langle j|\tilde{W}\right)(V|ij\rangle \otimes W)\,|\varphi\rangle \right\|_{\ell_2^{m^2}}. \end{aligned}$$

Finally, squaring this last expression and taking the expectation over ε we conclude that:

$$\begin{aligned}&\mathbb{E}_\varepsilon \left\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|^2 \\ &\quad = \mathbb{E}_\varepsilon \sup_{\substack{m\in\mathbb{N} \\ \tilde{V},\tilde{W}\in\mathsf{ball}(\mathcal{S}_\infty^{\tilde{k}',nm}) \\ W\in\mathsf{ball}(\mathcal{S}_\infty^{\tilde{k}'}),\,|\varphi\rangle\in\mathsf{ball}(\ell_2^{k\tilde{k}'})}} \left\| \frac{1}{n^2}\sum_{ij} \varepsilon_{ij}\left(\left(\langle i|\tilde{V}\otimes\langle j|\tilde{W}\right)\left(V|ij\rangle\otimes W\right)|\varphi\rangle\right\|^2_{\ell_2^{m^2}} \\ &\quad \geq \mathbb{E}_\varepsilon \left\| \frac{1}{n^2}\sum_{ij} \varepsilon_{ij}\left(\left(\langle i|\tilde{V}_\varepsilon\otimes\langle j|\tilde{W}_\varepsilon\right)\left(V|ij\rangle\otimes W_\varepsilon\right)|\varphi\rangle\right\|^2_{\ell_2^{m^2}} = \omega(G_{Rad};\mathcal{S}^{\mathcal{U}}),\end{aligned}$$

where we have considered that $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon$. With that we are almost done. This last expression is enough to obtain

$$\omega(G_{Rad};\mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|^2 \leq \mathbb{E}_\varepsilon \left\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|.$$

Furthermore, using Kahane's inequality [46], we can improve on that taking into account the equivalence $\mathbb{E}_\varepsilon \left\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|^2 \approx \left(\mathbb{E}_\varepsilon \left\|\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|\right)^2$. This allows us to obtain the statement of the lemma. □

Now, notice that $\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}$ is by construction a linear map of the kind of Example 4.6, and, consequently, $\sigma_{\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}} \lesssim \log(n)/n$. Furthermore, by symmetry, $\mathbb{E}_\varepsilon \Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) = 0$. Therefore, Corollary 4.8 applied to the statement of Lemma 4.19 directly implies the bound:

$$\omega(G_{Rad};\mathcal{S}^{\mathcal{U}}) \lesssim_{\log} \left(\frac{\mathrm{T}_2^{(n^2)}(X^{iii})}{n}\right)^2. \tag{4.24}$$

The problem now reduces to find a good estimate for the type-2 constant in the last expression.

We note that the norm X^{iii} is the smallest one for which we were able to prove an equivalent to Lemma 4.19. However, the whole argument from this lemma until here would be valid for any norm larger than X^{iii} fulfilling a normalization condition with respect to the elements that sum up to $\Phi^{iii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)$. We will be more explicit later on. An example of such a norm is $X^{ii}\otimes_\varepsilon \ell_2^{k\tilde{k}'}$ where $X^{ii} = \mathcal{S}_1^{\tilde{k}',n}\otimes_{(\varepsilon,\pi)_{1/2}}\mathcal{S}_1^{\tilde{k}',n}$. Motivated by the type properties of X^{ii}, cf. Proposition 4.10 and, more particularly, Equation (4.3), we are led to conjecture that:

$$\mathrm{T}_2^{(n^2)}\left(\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_{(\varepsilon,\pi)_{1/2}}\mathcal{S}_1^{\tilde{k}',n}\right)\otimes_\varepsilon \ell_2^{k\tilde{k}'}\right)\lesssim_{\log}\mathrm{T}_2^{(n^2)}\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_{(\varepsilon,\pi)_{1/2}}\mathcal{S}_1^{\tilde{k}',n}\right).$$

Recalling that $\mathrm{T}_2^{(n^2)}\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_{(\varepsilon,\pi)_{1/2}}\mathcal{S}_1^{\tilde{k}',n}\right)\lesssim_{\log} n^{3/4}$, we start stating our conjecture as follows:

Conjecture 1 (strongest form)**.**

$$\mathrm{T}_2^{(n^2)}\left(\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_{(\varepsilon,\pi)_{1/2}}\mathcal{S}_1^{\tilde{k}',n}\right)\otimes_\varepsilon \ell_2^{k\tilde{k}'}\right)\lesssim_{\log} n^{3/4}. \tag{4.25}$$

A weaker conjecture which would also imply the desired bounds in the setting of PBC is:

Conjecture 1 (weaker form)**.**

$$\mathrm{T}_2^{(n^2)}\left(\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_{(\varepsilon,\pi)_{1/2}}\mathcal{S}_1^{\tilde{k}',n}\right)\otimes_\varepsilon \ell_2^{k\tilde{k}'}\right)\lesssim_{\log} n^{\beta} \qquad \textit{for some } \beta<1. \tag{4.26}$$

According to what we explained above, there is a plethora of norms for which the positive resolution of the corresponding conjecture would imply unconditional exponential lower bounds for the resources in attacks to PBC. Next, we formalize this discussion characterizing those norms and rewriting Conjecture 4.25 in a unified form.

First, we characterize what we need from a norm X to follow the previous argument substituting X^{iii} by this X. As usually, we use the notation X to denote the norm as well as the corresponding Banach space itself. In this section we refer to X as a *valid norm* if it satisfies:

P.i. X is a norm on the algebraic tensor product $\mathcal{S}_1^{\tilde{k}',n}\otimes\mathcal{S}_1^{\tilde{k}',n}\otimes\ell_2^{k\tilde{k}'}$;

P.ii. $\|x\|_X\gtrsim\|x\|_{X^{iii}}$ for any $x\in X$;

P.iii. $\left\|\langle i|\otimes\langle j|\otimes(V|ij\rangle\otimes\mathrm{Id}_{\ell_2^{\tilde{k}'}})\right\|_X\leq 1$ for any $V\in\mathsf{ball}(\mathcal{S}_\infty^{n^2k,\tilde{k}'})$ and any i, $j=1,\ldots,n$.

Notice that P.ii. guarantees a relation with the value of G_{Rad} in analogy with Lemma 4.19 and P.iii. guarantees that $\Phi^{iii}_{\mathcal{S}\mathcal{U}}:\mathcal{Q}_{n^2}\to X$ still falls in the setting of Example 4.6, i.e., we still have $\sigma_{\Phi^{iii}_{\mathcal{S}\mathcal{U}}}\lesssim\log(n)/n$. These two properties therefore translates into the fact that the bound (4.24) is still true with the type-2 constant of any valid norm X instead of X^{iii}.

We can state

Conjecture 1 (even weaker form). *For some valid norm, i.e. a norm X satisfying properties* P.i., P.ii. *and* P.iii. *above, and some dimension independent constant $\beta < 1$:*

$$\mathrm{T}_2^{(n^2)}(X) \lesssim_{\log} n^{\beta}. \tag{4.27}$$

Now, to state our conjecture in its weakest form we need to introduce the notion of type constant of an operator $f : X \to Y$. The type-2 constant of a linear map $f : X \to Y$ is the infimum of the constants T such that

$$\left(\mathbb{E}_\varepsilon\left[\Big\| \sum_i \varepsilon_i f(x_i)\Big\|_Y^2\right]\right)^{1/2} \leq \mathrm{T}\left(\sum_i \|x_i\|_X^2\right)^{1/2},$$

for any finite sequence $\{x_i\}_i \subset X$. In analogy with the case of the type constant of a Banach space, when the cardinal of this sequence is restricted, we refer to the type-2 constant with m vectors of $f : X \to Y$ and denote $\mathrm{T}_2^{(m)}(f : X \to Y)$.

We are interested here in the type of the identity map $\mathrm{Id} : X \to X^{iii}$, being X a *valid norm.* In fact, the final statement of our conjecture is as follows:

Conjecture 1 (weakest form). *For some valid norm, i.e. a norm X satisfying properties* P.i., P.ii. *and* P.iii. *above, and some dimension independent constant $\beta < 1$:*

$$\mathrm{T}_2^{(n^2)}\left(\mathrm{Id} : X \to X^{iii}\right) \lesssim_{\log} n^{\beta}. \tag{4.28}$$

Remark 4.20. Notice that in particular, $\mathrm{T}_2^{(n^2)}(\mathrm{Id} : X \to X^{iii}) \lesssim \mathrm{T}_2^{(n^2)}(Y)$ for any *valid norm* Y such that $\|x\|_{X^{iii}} \lesssim \|x\|_Y \lesssim \|x\|_X$. Therefore, the last form of the conjecture, Equation (4.28), is indeed weaker than the previous ones.

Within the family of *valid* norms characterized by properties P.i., P.ii., P.iii. we obviously find the spaces X^{iii} and $\left(\mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$.

But also, spaces such as $\left(\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$ or $\left(\mathcal{S}_1^{\tilde{k}',n} \otimes_{\pi_2} \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$, see Chapter 2, Section 2.4 for the definition of $\mathfrak{S}_2^w$ and π_2. An obstruction for the techniques used in this work to obtain upper bounds for the type constants of these spaces is the pathological behaviour of the injective tensor product with respect to interpolation methods [59]. In order to support the validity of the stated conjecture, in the next subsections we explore the most direct approaches to disprove it, lower bounding the type-2 constant of the spaces involved. We find that these approaches do not lead to bounds stronger than $\mathrm{T}_2(X) \gtrsim_{\log} n^{3/4}$ for at least some *valid* norm X.

4.7.1 Type constant of subspaces

From the definition of the type constant of a normed space X, $\mathrm{T}_p(X)$, $1 \leq p \leq 2$, it follows that,

$$\text{for any subspace } S \subseteq X, \qquad \mathrm{T}_p(X) \geq \mathrm{T}_p(S).$$

This applies as well to $\mathrm{T}_p^{(m)}$ instead of T_p. Then, a way to disprove (4.27) is finding for any valid norm X, a subspace with type-2 constant of order n or greater.

For the sake of concreteness, we now restrict our attention to norms of the form $\left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$, being $\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$ a normed space *in between of* $\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}$ and $\mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$. That is, for any $x \in \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$:

$$\| x \|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k}',n}} \leq \| x \|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}} \leq \| x \|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}}.$$

All these norms clearly satisfy properties P.i., P.ii, P.iii.[7]

What we do here is looking at the most obvious subspaces of $\left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$ and study their type properties. Concretely, we study the following subspaces (in increasing order of complexity):

1. first, we find copies of $\ell_2^{k\tilde{k}'}$ and $\mathcal{S}_1^{\tilde{k}',n}$;

[7] For P.iii., recall Remark 4.18.

2. at the next level, we also find the subspaces $\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$ and $\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \ell_2^{k\tilde{k}'}$;

3. finally, we also study the subspaces $\left(\ell_2^{\tilde{k}'} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$ and $(\ell_1^n \otimes_\alpha \ell_1^n) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$. We were not able to obtain non-trivial estimates for $\left(\ell_1^n \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$.

Next, we provide upper estimates for the type-2 constants of these spaces for some choices of α, showing that at least these estimates are compatible with Conjecture (4.27). The limitation on the possible norms for which following bounds apply comes from the limited scope of the techniques available. Nonetheless, it might be the case that these bounds are more general than stated here. In fact, we did not find any choice of α for which we have results contradicting 4.27, so in principle any of these norms could be suitable for a positive solution of the conjecture.

The first item above is already well understood. The following estimates are very well known:

$$\mathrm{T}_2(\ell_2) = 1,\ \mathrm{T}_2(\mathcal{S}_1^{\tilde{k}',n}) = \sqrt{\min(n, \tilde{k}')}.$$

Continuing with the second item, in Section 4.4, Equation (4.3), we have already obtained a satisfactory bound for the type constant (with n^2 vectors in this case) of $\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$ with $\alpha = (\varepsilon, \pi)_{1/2}$. We don't rule out the possibility that a similar bound applies to other α's, but we were not able to find a proof for that. The reason why we managed to better understand the case $\alpha = (\varepsilon, \pi)_{1/2}$ is purely technical in origin, and it is due to the nice behaviour of type constants under interpolation methods.

A bound for the type-2 constant of $\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \ell_2^{k\tilde{k}'}$ is easier to obtain. Taking into account that $\|\mathrm{Id} : \mathcal{S}_2^{\tilde{k}',n} \to \mathcal{S}_1^{\tilde{k}',n}\| \, \|\mathrm{Id} : \mathcal{S}_1^{\tilde{k}',n} \to \mathcal{S}_2^{\tilde{k}',n}\| \leq \sqrt{n}$ and that $\ell_2^{n\tilde{k}'} \otimes_\varepsilon \ell_2^{k\tilde{k}'} = \mathcal{S}_\infty^{n\tilde{k}',k\tilde{k}'}$, we obtain

$$\mathrm{T}_2(\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \ell_2^{k\tilde{k}'}) \lesssim_{\log} \sqrt{n}.$$

Finally, we state our findings regarding the third item in the form of two propositions. For the first one, recall the Definitions 2.12 and (2.16) for the norms appearing next:

Proposition 4.21. *For $\alpha = \mathfrak{S}_2^w$ or $\alpha = \pi_2$,*

$$\mathrm{T}_2\left((\ell_2^{\tilde{k}'} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}) \otimes_\varepsilon \ell_2^{k\tilde{k}'} \right) \lesssim_{\log} \sqrt{n}.$$

Proof. The proof is as simple as noting that $\|\mathrm{Id} : \mathcal{S}_1^{\tilde{k}',n} \to \ell_2^{n\tilde{k}'}\| \, \|\mathrm{Id} : \ell_2^{n\tilde{k}'} \to \mathcal{S}_1^{\tilde{k}',n}\| \leq \sqrt{n}$ and, for the α's in the statement of the proposition, $\ell_2^{\tilde{k}'} \otimes_\alpha \ell_2^{n\tilde{k}'} = \ell_2^{n\tilde{k}'^2}$. This provides the following bound for the quantity of interest:

$$\mathrm{T}_2\left((\ell_2^{\tilde{k}'} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}) \otimes_\varepsilon \ell_2^{k\tilde{k}'} \right) \leq \sqrt{n}\ \mathrm{T}_2\left(\ell_2^{n\tilde{k}'^2} \otimes_\varepsilon \ell_2^{k\tilde{k}'} \right) \lesssim \sqrt{n \log(nk\tilde{k}'^2)}.$$

□

Proposition 4.22. *For any α in between of ε and π_2:*

$$\mathrm{T}_2\left((\ell_1^n \otimes_\alpha \ell_1^n) \otimes_\varepsilon \ell_2^{k\tilde{k}'} \right) \lesssim_{\log} \sqrt{n}.$$

Proof. The reason for which the claim turns out to be valid for α in a wide range of norms is due to Grothendieck's inequality, which makes all these norms collapse:

$$\ell_1^n \otimes_\alpha \ell_1^n \approx \ell_1^n \otimes_\varepsilon \ell_1^n.$$

Therefore, it is enough to study the type-2 constant of the space $\ell_1^n \otimes_\varepsilon \ell_1^n \otimes_\varepsilon \ell_2^{k\tilde{k}'}$. For this, we can isomorphically embed ℓ_1^n into $\ell_\infty^{c^n}$ for some constant $c > 2$. Therefore, we obtain $\ell_1^n \otimes_\varepsilon \ell_1^n \otimes_\varepsilon \ell_2^{k\tilde{k}'} \approx \ell_\infty^{c^n} \otimes_\varepsilon \ell_\infty^{c^n} \otimes_\varepsilon \ell_2^{k\tilde{k}'} = \ell_\infty^{c^{2n}}(\ell_2^{k\tilde{k}'})$. To conclude, we note that the type-2 constant of this last space is, up to logarithmic factors, of order $\sqrt{n}$. □

4.7.2 Volume ratio

Although the Banach spaces that appear in this thesis are prominently complex, for the sake of simplicity, we will restrict ourselves to real spaces in this section. There exist standard tools [68, 111, 125, 71] to transpose results in this case to the complex domain, albeit some technicalities might appear in that process [126]. Since our aim here is restricted to show some evidence in favour of our conjecture, we do not think that these intricacies add anything of essential importance to the following discussion.

A standard approach to understand the type/cotype properties of a space X consists on the computation of its volume ratio, $\mathrm{vr}(X)$, a notion originated in [109, 110]. The reason is that this parameter provides a lower bound for the cotype-2 constant. This is the content of the following result due to Milman and Bourgain:

Theorem 4.23 ([11]). *For a Banach space X,*

$$\mathrm{C}_2(X) \log\left(2\mathrm{C}_2(X)\right) \gtrsim \mathrm{vr}(X).$$

Taking into account the duality relation between type and cotype – cf. Chapter 2, Proposition 2.5 – the last result translates into a lower bound for the type-2 constant of the dual space:

$$\mathrm{T}_2(X) \geq \mathrm{C}_2(X^*) \gtrsim_{\log} \mathrm{vr}(X^*).$$

This provides us with another technique to try to disprove Conjecture 4.27. In this section we upper bound the volume ratio of various *valid* norms – in the sense of Conjecture 4.27 – obtaining results that are again compatible with a positive solution of the conjecture.

We make now a tiny digression about the relation between volume ratio and cotype. In few words, this relation is still far from being well understood. In fact, in [110] it was asked whether $\mathrm{vr}(X)$ can be estimated from the cotype-2 constant of the space and, in the more recent work [38], the authors of that paper commented on the question whether bounded volume ratio implies cotype q for every $q > 2$. Studying further these questions is an extremely interesting avenue to tackle the problems we are concerned with in this work, at the same time as clarifying the relation between two very fundamental notions in local Banach space theory.

Next we define the volume ratio of a normed space X, $\mathrm{vr}(X)$. Given a d-dimensional Banach space X,

$$\mathrm{vr}(X) = \left(\frac{\mathrm{vol}_d(\mathsf{ball}(X))}{\mathrm{vol}_d(\mathcal{E}_X)}\right)^{1/d}, \tag{4.29}$$

where $\mathcal{E}_X$ is the ellipsoid of maximal volume contained in $\mathsf{ball}(X)$ and $\mathrm{vol}_d(\,\cdot\,)$ denotes the d-dimensional Lebesgue measure.

We focus again on spaces of the form $\left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$, as in the previous section. We prove:

Theorem 4.24. *Let α be a* tensor norm *such that, for any $x \in \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$:*

1. $\|x\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}} \leq \|x\|^{1/2}_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n}} \|x\|^{1/2}_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}}$;
2. $\|x\|_{\ell_2^{n^2\tilde{k}'^2}} \leq \|x\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}}$.

Then, for $X = \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'}$, we have

$$\mathrm{vr}(X^*) \lesssim n^{3/4}.$$

The proof uses several standard tools from geometric Banach space theory, mainly following the approach of [38]. But before going into the proof, we note that some of our *valid* norms indeed fulfil the conditions of the theorem. Some examples are $\mathcal{S}_1^{\tilde{k}',n} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{\tilde{k}',n}$ or $\mathcal{S}_1^{\tilde{k}',n} \otimes_{\pi_2} \mathcal{S}_1^{\tilde{k}',n}$. An important feature of these spaces is the fact that, by construction, they *have enough symmetries*. This will be exploited in the following proof with no further mention. The reader can find some additional information in Appendix B.3.

Proof. We start noticing that α being a tensor norm translates into the fact that X *has enough symmetries*. This means that the only operator on that space that commutes with every isometry is the identity (or a multiple of it). The same happens with the dual X^*. Next, we provide an alternative way to compute the volume ratio using this property. To simplify notation, denote $d = \dim(X) = n^2 k\tilde{k}'^3$. Then, we can bound

(4.29) as follows:

$$\begin{aligned}
\mathrm{vr}(X^*) &\overset{(i.)}{=} \left(\frac{\mathrm{vol}_d(\mathsf{ball}(X^*))}{\mathrm{vol}_d(\mathsf{ball}(\ell_2^d))}\right)^{1/d} \left\|\mathrm{Id}:\ell_2^d \to X^*\right\| \\
&\overset{(ii.)}{\leq} \left(\frac{\mathrm{vol}_d(\mathsf{ball}(\ell_2^d))}{\mathrm{vol}_d(\mathsf{ball}(X))}\right)^{1/d} \left\|\mathrm{Id}:\ell_2^d \to X^*\right\| \\
&\overset{(iii.)}{\lesssim} \frac{\left\|\mathrm{Id}:\ell_2^d \to X^*\right\|}{\sqrt{d}} \left(\frac{1}{\mathrm{vol}_d(\mathsf{ball}(X))}\right)^{1/d} \\
&\overset{(iv.)}{\lesssim} \frac{\left\|\mathrm{Id}:\ell_2^d \to X^*\right\|}{\sqrt{d}}\, \mathbb{E}\left\|G\right\|_X, \qquad (4.30)
\end{aligned}$$

where $G = \sum_{i,j,k,l,m} g_{ijklm} |i\rangle\langle j| \otimes |k\rangle\langle l| \otimes \langle m|$ is a tensor in X with i.i.d. gaussian entries g_{ijklm}. The expectation is over these random variables. With respect to the chain of claims implicit in the previous manipulation: (i.) follows from the fact that the maximal volume ellipsoid $\mathcal{E}_{X^*}$ coincides with $\left\|\mathrm{Id}:\ell_2^d \to X^*\right\|^{-1} \mathsf{ball}(\ell_2^d)$ when X^* has enough symmetries [115, Section 16], in (ii.) we have used the famous Blaschke-Santaló inequality [88, Section 7], in (iii.), the standard volume estimation for the Euclidean ball, $\mathrm{vol}_d(\mathsf{ball}(\ell_2^d)) \approx d^{-d/2}$ and (iv.) follows from Lemma 3.4. in [38].

As a consequence, to obtain the stated bound we have to estimate the quantities $\left\|\mathrm{Id}:\ell_2^d \to X^*\right\|$ and $\mathbb{E}\left\|G\right\|_X$.

- Upper bounding $\left\|\mathrm{Id}:\ell_2^d \to X^*\right\|$:

  We show two complementary bounds for this quantity. The first one uses the second condition in the statement of the theorem, that can be equivalently stated as: $\left\|\mathrm{Id}:\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n} \longrightarrow \ell_2^{n^2\tilde{k}'^2}\right\| \leq 1$. This allows us to bound:

$$\begin{aligned}
\left\|\mathrm{Id}:\ell_2^d \to X^*\right\| &= \left\|\mathrm{Id}: X \to \ell_2^d\right\| \\
&= \left\|\mathrm{Id}: \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}'} \longrightarrow \ell_2^{n^2\tilde{k}'^2 k\tilde{k}'}\right\| \\
&\leq \left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \otimes_\varepsilon \ell_2^{k\tilde{k}'} \longrightarrow \ell_2^{n^2\tilde{k}'^2 k\tilde{k}'}\right\| \\
&\leq \sqrt{k\tilde{k}'}.
\end{aligned}$$

The assumption $\left\|\mathrm{Id}: \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n} \longrightarrow \ell_2^{n^2\tilde{k}'^2}\right\| \leq 1$ was used in the first inequality above.

Our second bound comes from the observation that the operator norm we want to bound is indeed upper bounded by the 2-summing norm of the identity between $\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$ and $\ell_2^{n^2\tilde{k}'^2}$. We can alternatively understand the studied norm as:

$$\begin{aligned}\left\|\mathrm{Id}: \ell_2^d \to X^*\right\| &= \left\|\mathrm{Id}: X \to \ell_2^d\right\| \\ &= \left\|\mathrm{Id}: \ell_2^{k\tilde{k}'} \otimes_\varepsilon \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \longrightarrow \ell_2^{k\tilde{k}'}(\ell_2^{n^2\tilde{k}'^2})\right\| \\ &\leq \sup_{k\in\mathbb{N}} \left\|\mathrm{Id}: \ell_2^{k} \otimes_\varepsilon \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right) \longrightarrow \ell_2^{k}(\ell_2^{n^2\tilde{k}'^2})\right\| \\ &= \pi_2\left(\mathrm{Id}: \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n} \longrightarrow \ell_2^{n^2\tilde{k}'^2}\right),\end{aligned}$$

where the last equality is simply the definition of the 2-summing norm of the indicated map – recall Chapter 2, Equation (2.16). While now we don't need the hypothesis used before, we need to invoke the tensor norm properties of α. Hopefully, thanks to this property[8], Lemma 5.2. of [31] provides us a satisfactory way to compute the above norm. Under the consideration that $\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}$ as well as $\ell_2^{n^2\tilde{k}'^2}$ have *enough symmetries in the orthogonal group* – see Appendix B.3 –, the cited lemma allows us to write the following identity:

$$\pi_2\left(\mathrm{Id}: \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n} \longrightarrow \ell_2^{n^2\tilde{k}'^2}\right) = \frac{n\tilde{k}'}{\left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\|}.$$

Taking into account the two bounds above, we can state that, under the conditions in the theorem:

$$\begin{aligned}&\left\|\mathrm{Id}: \ell_2^d \to X^*\right\| \\ &\qquad \leq \min\left(\sqrt{k\tilde{k}'},\ \frac{n\tilde{k}'}{\left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\|}\right). \qquad (4.31)\end{aligned}$$

[8] See again Appendix B.3 for clarification.

- Upper bounding $\mathbb{E}\,\|G\|_X$:

The upper estimate of this quantity follows from Chevet's inequality [24], see also [115, Section 43]. According to that:

$$\begin{aligned}
\mathbb{E}\,\|G\|_X &= \|G\|_{\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right)\otimes_\varepsilon \ell_2^{k\tilde{k}'}} \\
&\leq \sup_{\varphi\in \mathsf{ball}\left(\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right)^*\right)} \left(\sum_{i,j,k,l}\Big|\varphi\left(|i\rangle\langle j|\otimes|k\rangle\langle l|\right)\Big|^2\right)^{1/2} \\
&\quad\times \mathbb{E}\left\|\sum_m g_m\langle m|\right\|_{\ell_2^{k\tilde{k}'}} \\
&\quad+ \sup_{\varphi\in \mathsf{ball}\left(\left(\ell_2^{k\tilde{k}'}\right)^*\right)} \left(\sum_m |\varphi\left(\langle m|\right)|^2\right)^{1/2} \\
&\quad\times \mathbb{E}\left\|\sum_{i,j,k,l} g_{ijkl}|i\rangle\langle j|\otimes|k\rangle\langle l|\right\|_{\mathcal{S}_1^{\tilde{k}',n}\otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}}.
\end{aligned}$$

Here we note the coincidence of the 2-sums above with the norm of the following identity maps:

- $$\begin{aligned}
&\sup_{\varphi\in \mathsf{ball}\left(\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right)^*\right)} \left(\sum_{i,j,k,l}|\varphi\left(|i\rangle\langle j|\otimes|k\rangle\langle l|\right)|^2\right)^{1/2} \\
&\qquad= \left\|\mathrm{Id}:\left(\mathcal{S}_1^{\tilde{k}',n}\otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right)^* \longrightarrow \ell_2^{n^2\tilde{k}'^2}\right\|,
\end{aligned}$$

- $$\sup_{\varphi\in \mathsf{ball}\left(\ell_2^{k\tilde{k}'}\right)} \left(\sum_m |\varphi\left(\langle m|\right)|^2\right)^{1/2} = \left\|\mathrm{Id}:\ell_2^{k\tilde{k}'}\longrightarrow \ell_2^{k\tilde{k}'}\right\| = 1.$$

Furthermore, to simplify the presentation we also introduce the notation $\boldsymbol{g} = \sum_{i,j,k,l} g_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|$. With these comments, we can write

$$\begin{aligned}
\mathbb{E}\, \|G\|_X \leq{}& \left\| \mathrm{Id} : \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n} \right)^* \longrightarrow \ell_2^{n^2 \tilde{k}'^2} \right\| \, \mathbb{E} \left\| \sum_m g_m \langle m| \right\|_{\ell_2^{k\tilde{k}'}} \\
&+ \left\| \mathrm{Id} : \ell_2^{k\tilde{k}'} \longrightarrow \ell_2^{k\tilde{k}'} \right\| \, \mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}} \\
&\approx \left\| \mathrm{Id} : \left(\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n} \right)^* \longrightarrow \ell_2^{n^2 \tilde{k}'^2} \right\| \sqrt{k\tilde{k}'} \\
&+ \mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}}.
\end{aligned}$$

Now, it is just left to bound $\mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}}$. For that, we make use of condition 1. in the statement of the theorem, that is:

$$\begin{aligned}
\mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}} &\leq \mathbb{E} \left(\|\boldsymbol{g}\|^{1/2}_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n}} \|\boldsymbol{g}\|^{1/2}_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}} \right) \\
&\leq \left(\mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n}} \right)^{1/2} \left(\mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}} \right)^{1/2}.
\end{aligned}$$

The first term can be bounded as follows:

$$\begin{aligned}
\mathbb{E}\, \|\boldsymbol{g}\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\pi \mathcal{S}_1^{\tilde{k}',n}} &= \mathbb{E}\, \|\boldsymbol{g}\|_{\ell_2^n \otimes_\pi \ell_2^n \otimes_\pi \mathcal{S}_1^{\tilde{k}'}} \leq \sqrt{\tilde{k}'}\, \mathbb{E}\, \|\boldsymbol{g}\|_{\ell_1^{n^2}(\mathcal{S}_2^{\tilde{k}'})} \\
&\leq n\sqrt{\tilde{k}'}\, \mathbb{E}\, \|\boldsymbol{g}\|_{\ell_2^{n^2}(\mathcal{S}_2^{\tilde{k}'})} = n\sqrt{\tilde{k}'}\, \mathbb{E}\, \|\boldsymbol{g}\|_{\ell_2^{n^2 \tilde{k}'^2}} \\
&\lesssim n\sqrt{\tilde{k}'} n\tilde{k}' = n^2 \tilde{k}'^{3/2}.
\end{aligned}$$

For the other term, we use again Chevet's inequality:

$$\begin{aligned}
&\mathbb{E} \left\| \sum_{i,j,k,l} g_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l| \right\|_{\mathcal{S}_1^{\tilde{k}',n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}} \\
&\leq 2 \left\| \mathrm{Id} : \mathcal{S}_\infty^{\tilde{k}',n} \longrightarrow \ell_2^{n\tilde{k}'} \right\| \, \mathbb{E} \left\| \sum_{i,j} g_{ij} |i\rangle\langle j| \right\|_{\mathcal{S}_1^{\tilde{k}',n}} \\
&\leq 2\sqrt{n}\, \mathbb{E} \left\| \sum_{i,j} g_{ij} |i\rangle\langle j| \right\|_{\mathcal{S}_1^{\tilde{k}',n}} \\
&\lesssim \sqrt{n}\, n\sqrt{\tilde{k}'} = n^{3/2} \tilde{k}'^{1/2}.
\end{aligned}$$

With the previous bounds, we obtain:

$$\mathbb{E}\left\|G\right\|_X \lesssim \left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\| \sqrt{k\tilde{k}'} + n^{7/4}\tilde{k}'. \tag{4.32}$$

To finish, we introduce in (4.30) the information given by (4.31) and (4.32):

$$\begin{aligned}
\mathrm{vr}(X^*) \leq & \frac{\left\|\mathrm{Id}: \ell_2^d \to X^*\right\|}{\sqrt{d}}\, \mathbb{E}\left\|G\right\|_X \\
\leq & \frac{\min\left(\sqrt{k\tilde{k}'},\ \frac{n\tilde{k}'}{\left\|\mathrm{Id}:\ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n}\otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\|}\right)}{n\tilde{k}'\sqrt{k\tilde{k}'}} \\
& \times \left(\left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\| \sqrt{k\tilde{k}'} \ + \ n^{7/4}\tilde{k}'\right) \\
\leq & \frac{n\tilde{k}'}{n\tilde{k}'\sqrt{k\tilde{k}'}\left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\|} \\
& \times \left\|\mathrm{Id}: \ell_2^{n^2\tilde{k}'^2} \longrightarrow \mathcal{S}_1^{\tilde{k}',n} \otimes_\alpha \mathcal{S}_1^{\tilde{k}',n}\right\| \sqrt{k\tilde{k}'} + \frac{\sqrt{k\tilde{k}'}}{n\tilde{k}'\sqrt{k\tilde{k}'}} n^{7/4}\tilde{k}' \\
= & 1 + n^{3/4}.
\end{aligned}$$

That is enough to conclude the proof of the theorem.

□

4.8 Discussion

In this chapter we have proposed a protocol for PV, referred as G_{Rad} throughout the text, and proved lower bounds on the quantum resources necessary to break it. Our bounds, appearing in Theorem 4.1, do not answer in a definite way Question 2 and, in particular, are not enough for proving G_{Rad} *secure for all practical purposes.* The reason is that the bounds presented in Theorem 4.1 depend on some additional properties of the strategy under consideration: the parameters $\sigma_{\mathcal{S}}^{i}$, $\sigma_{\mathcal{S}}^{ii}$, related with the regularity of the strategy when regarded as a vector-valued assignment on the Boolean hypercube, cf. Section 4.6. However, our Theorem 4.1 is strong enough to encapsulate some previous results. As mentioned in Section 4.1, the hypotheses of Corollary 4.2 are satisfied by the teleportation based attacks of [15] and [5] and also by Universal Programmable Quantum Processors, rederiving in that way some results in [15, 5, 57]. In particular, Theorem 3.11 in Chapter 3 can be obtained from Corollary 4.2. Furthermore, we have related the final solution of Question 1 with the type/cotype properties of specific Banach spaces and, in fact, the results we obtained led us to put forward a conjecture about these mathematical objects. The positive solution of this conjecture would imply the *security for all practical purposes* of G_{Rad}. This would represent a major progress toward Question 2 – See Section 4.7 for a formal statement of the conjecture and details about the connection with the security of G_{Rad}. In this last section we have also provided some estimates supporting the conjecture. Concretely, we have obtained bounds for the type-2 constants of some subspaces involved in the conjecture as well as bounds for the volume ratio of the duals of the spaces appearing there. This last estimate relates our conjecture, and therefore, the problem about the security of G_{Rad}, with open problems in Banach space theory concerning the relation between cotype and volume ratio.

The future direction for this work is clear: trying to resolve the status of the security of G_{Rad}. Starting with the setting we introduced in Section 4.7, the most direct approach consists on developing new techniques to estimate type/cotype constants of tensor norm spaces. This is in fact an interesting avenue also in the context of local Banach space theory and we hope that this work could serve as motivation to pursue it. Extending the family of spaces whose type/cotype constants can be accurately estimated might shed new light on several poorly understood questions in this context, as it is the relation between volume ratio and cotype or the prevalence of type/cotype in tensor norms.

Coming back to our σ–dependent bounds, Theorem 4.1, it would be also a desirable development to achieve a better understanding of the regularity parameters introduced there, $\sigma_{\mathcal{S}}^{i}$ and $\sigma_{\mathcal{S}}^{ii}$. For example, it would be very clarifying to understand how the structure of strategies is restricted under the assumption of these parameters being small (in the sense of Corollary 4.2) or whether general strategies can be *made more regular* in order to have a better behaviour in terms of these parameters. Another interesting question in this direction is understanding whether $\sigma^i_{\mathcal{S}}$, $\sigma^{ii}_{\mathcal{S}}$ can be related with some physical properties of the strategies involved, such as their robustness against noise or the complexity of the operations performed.

Beyond the specific setting studied here, we have introduced a whole toolbox of constructions and connections that can be of interest in other related contexts. Firstly, most of the ideas we have used to study G_{Rad} can be explored in other MROQGs or even in more general games. Being more speculative, the recent connection between PBC and AdS/CFT [65, 66] seems to indicate that the tools we use here might have potential application to the understanding of holographic duality. Along this line, we can ask, for example, whether the notions of regularity studied here can be related with properties of the mapping between bulk and boundary theories in this context. In [66] it was claimed that properties of the AdS/CFT holographic correspondence allow to find cheating strategies that break PBC with polynomial resources. According to that, the exponential lower bounds in Corollary 4.2 opens the possibility to impose restrictions on the regularity of such holographic correspondence. This would be in consonance with a recent result of Kliesch and Koenig [56], based on previous work of Jones [50]. In [56], the continuum limit of discrete tensor-network toy models for holography was studied finding that, generically, this limit is extremely discontinuous.

Chapter 5

Concluding remarks and open questions

In this thesis we have established new connections between problems arising in the study of quantum information and local Banach space theory. In particular, type constants appear as the central quantity of interest. We have shown how the understanding of this parameter for some particular Banach spaces can be translated into bounds for the resources necessary to achieve some quantum information processing tasks. Here we have analysed the case of Universal Programmable Quantum Processors – cf. Chapter 3 – and attacks to Position Based Quantum Cryptography – cf. Chapter 4 –. However, there is no reason to think that the ideas we have introduced must only apply to these specific situations and further applications to other contexts within the study of quantum information remains as a promising future avenue to be explored. In fact, type constants had appeared before a related context in the work [12].

Focusing in the work filling these pages, we find some questions that remain open and that we think are worth of further exploration. We summarize next the ones that we consider most relevant.

Question 1. Given $\epsilon > 0$, what is the biggest natural number d such that there exists a d–dimensional subspace of $\mathcal{S}_\infty^m$ that is ϵ–isomorphic to $\mathcal{S}_1^d$?

In Chapter 3 we have shown that $\epsilon-\mathrm{UPQP}_d$ correspond to completely contractive ϵ–embeddings of $\mathcal{S}_1^d$ into a subspace of $\mathcal{S}_\infty^m$. When fixing an arbitrary $\epsilon > 0$ as constant, the bounds we have obtained still leaves open the gap:

$$\Omega(\exp(d)) \leq m \leq O(\exp(d^2)), \tag{5.1}$$

for the optimal memory dimension m. We have already mentioned that the previous gap is still open when we forget about the condition about the completely bounded norm of the embedding, resulting in Question 1 asked above. This question is remarkably natural in the context of the local theory of Banach spaces. Closing (5.1) by its upper edge, providing a stronger lower bound $m \geq \Omega(\exp(d^2))$, would also resolve the more stringent question about Universal Programmable Quantum Processors. On the contrary, the existence of ϵ–embeddings for which $m \leq O(\exp(d))$ might provide some insights on the geometry of $\mathcal{S}_1^d$.

Question 2. How much entanglement is necessary to break *any* PV scheme?

This is the main question that we tried to answer in Chapter 4. Despite the progress presented there, a satisfactory answer is still missing. However, our results establish some connections that naturally raise further questions of potential interest also beyond the setting of Position Based Cryptography. In first place, in Chapter 4, Section 4.6, we have related an analytical property – denoted as σ – of some vector-valued functions on the hypercube with the resources consumed to attack the Position Verification protocol G_{Rad}. This parameter σ, defined in Definition 4.5, can be understood as a non-commutative analogue of the *total influence*, a basic notion in the analysis of Boolean functions. In view of the relevant role played by the total influence in the study of real valued Boolean functions, we can wonder:

Question 3. Which properties of a vector valued function on the hypercube, $f : \mathcal{Q}_n \to X$, can be related with its regularity parameter σ_f? Are there any other applications in which this parameter plays a relevant role?

It is tempting to explore an extension of the classical theory of Boolean functions to the vector valued case in which the natural parameter σ_f, or some close variant, plays the role of the influence in the commutative theory. From our innocent ignorance about the feasibility of such a program, we can ask, for instance, whether non-commutative versions of the celebrated KKL theorem can be obtained in terms of the *non-commutative* influence σ_f or whether an analogous non-commutative extension of the recently proven [44] sensitivity conjecture holds. Furthermore, influence and related notions appear as key quantities in many practical application such as social choice, learning theory [73] or computational complexity [44, 1]. This partially explains the rich development of real valued Boolean analysis in stark contrast with the vector-valued extension discussed above. The work presented in this thesis opens the door for the exploration of further applications in the realm of quantum cryptography and, more generally, quantum computation.

In Chapter 4, Section 4.7, we have alternatively obtained unconditional bounds that only depend on the type constant of certain spaces. In this direction, the most obvious question that we leave open is the validity of Conjecture 1. Besides that, we can ask some other independent questions that are naturally related with that conjecture.

Question 4. For which spaces X the type-2 constant of $X \otimes_\varepsilon \ell_2^k$ is determined, up to logarithmic factors, by the type-2 constant of X?

First, we note that the logarithmic corrections are, in general, unavoidable. This is shown by the simple example of $\ell_2^k \otimes_\varepsilon \ell_2^k$. In the positive side, we can understand the previous question as motivated by the bounds $\mathrm{T}_2(\ell_\infty^k \otimes_\varepsilon X) \lesssim_{\log} \mathrm{T}_2(X)$ and $\mathrm{T}_2(\ell_2^k(X)) \lesssim \mathrm{T}_2(X)$. The space considered in Question 4 is a sort of hybrid between the previous two, which prompts us to ask whether the previous inequalities extend in some sense to that case. In the negative, we mention that the previous question is significantly challenging. Following the example considered earlier in this paragraph, the type constants of $\ell_2^k \otimes_\varepsilon \ell_2^k \otimes_\varepsilon \ell_2^k$ are widely unknown.

In relation with our estimates for the volume ratio of some tensor norms of ℓ_2 spaces – cf. Theorem 4.24 – we can ask:

Question 5. Is it possible to establish any non-trivial relation between the volume ratio of tensor norms of ℓ_2 spaces and its cotype constants?

Volume ratio and cotype are strongly interrelated notions, as shown by Milman-Bourgain's Theorem 4.23 or the characterization of weak cotype in terms of the volume ratio of subspaces, studied by Milman and Pisier [69]. However, there are features of this relation that are not understood yet. In particular, we do not known whether an inequality

$$\mathrm{C}_2(X) \lesssim_{\log} \mathrm{vr}(X) \tag{5.2}$$

can be established for some family of well-behaved spaces, for example, spaces with enough symmetries or tensor norms of ℓ_2 spaces, as in Question 5. A negative solution to Conjecture 1, in view of the estimates shown in Theorem 4.24, might show a counterexample to (5.2) in the last situation. In the opposite direction, an inequality as (5.2), even in the restricted case of tensor norms of ℓ_2 spaces, would prove the conjecture true.

Bibliography

[1] Aaronson, S., and Ambainis, A. The need for structure in quantum speedups. *Theory of Computing 10*, 6 (2014), 133–166.

[2] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., and Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett. 98* (2007), 230501.

[3] Aubrun, G., and Szarek, S. J. *Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory.* American Mathematical Society, 2017.

[4] Barrett, J., Hardy, L., and Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett. 95* (2005), 010503.

[5] Beigi, S., and König, R. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics 13*, 9 (2011), 093036.

[6] Bell, J. S. On the einstein podolsky rosen paradox. *Physics Physique Fizika 1*, 3 (1964), 195.

[7] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett. 70* (1993), 1895–1899.

[8] Bera, D., Fenner, S., Green, F., and Homer, S. Efficient universal quantum circuits. In *Computing and Combinatorics* (Berlin, Heidelberg, 2009), H. Q. Ngo, Ed., Springer Berlin Heidelberg, pp. 418–428.

[9] Bergh, J., and Löfström, J. *Interpolation Spaces.* Springer Berlin Heidelberg, 1976.

[10] Bisio, A., Chiribella, G., D'Ariano, G. M., Facchini, S., and Perinotti, P. Optimal quantum learning of a unitary transformation. *Phys. Rev. A 81* (2010), 032324.

[11] Bourgain, J., and Milman, V. D. New volume ratio properties for convex symmetric bodies in $\mathbb{R}^n$. *Inventiones mathematicae 88*, 2 (1987), 319–340.

[12] Brandao, F. G. S. L., and Harrow, A. W. Estimating operator norms using covering nets. *arXiv:1509.05065* (2015).

[13] Brazier, A., Bužek, V., and Knight, P. L. Probabilistic programmable quantum processors with multiple copies of program states. *Phys. Rev. A 71* (2005), 032306.

[14] Briët, J., Buhrman, H., Lee, T., and Vidick, T. Multipartite entanglement in xor games. *Quantum Info. Comput. 13*, 3–4 (2013), 334–360.

[15] Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., and Schaffner, C. Position-based quantum cryptography: Impossibility and constructions. In *Advances in Cryptology – CRYPTO 2011* (Berlin, Heidelberg, 2011), P. Rogaway, Ed., Springer Berlin Heidelberg, pp. 429–446.

[16] Buhrman, H., Cleve, R., Massar, S., and de Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys. 82* (2010), 665–698.

[17] Buhrman, H., Fehr, S., Schaffner, C., and Speelman, F. The garden-hose model. *Proceedings of the 4th conference on Innovations in Theoretical Computer Science - ITCS '13* (2013).

[18] Burkholder, D. L. A geometrical characterization of banach spaces in which martingale difference sequences are unconditional. *The Annals of Probability 9*, 6 (1981), 997–1011.

[19] Burkholder, D. L. Martingales and fourier analysis in banach spaces. In *Probability and Analysis* (Berlin, Heidelberg, 1986), G. Letta and M. Pratelli, Eds., Springer Berlin Heidelberg, pp. 61–108.

[20] Buscemi, F. All entangled quantum states are nonlocal. *Physical Review Letters 108*, 20 (2012).

[21] Chakraborty, K., Chailloux, A., and Leverrier, A. Robust relativistic bit commitment. *Physical Review A 94*, 6 (2016).

[22] Chakraborty, K., and Leverrier, A. Practical position-based quantum cryptography. *Physical Review A 92*, 5 (2015).

[23] Chandran, N., Goyal, V., Moriarty, R., and Ostrovsky, R. Position based cryptography. *CRYPTO2009* (2009), 391–407.

[24] Chevet, S. Séries de variables aléatoires gaussiennes à valeurs dans $E\hat{\otimes}_\varepsilon F$. application aux produits d'espaces de wiener abstraits. *Séminaire Analyse fonctionnelle (dit" Maurey-Schwartz")* (1978), 1–15.

[25] Childs, A. M., Leung, D., Mančinska, L., and Ozols, M. A framework for bounding nonlocality of state discrimination. *Communications in Mathematical Physics 323*, 3 (2013), 1121–1153.

[26] Choi, M.-D. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications 10*, 3 (1975), 285 – 290.

[27] Christandl, M., Leditzky, F., Majenz, C., Smith, G., Speelman, F., and Walter, M. Aymptotic performance of port-based teleportation. *Communications in Mathematical Physics* (2020).

[28] Cooney, T., Junge, M., Palazuelos, C., and Pérez-García, D. Rank-one quantum games. *computational complexity 24*, 1 (2015), 133–196.

[29] D'Ariano, G. M., and Perinotti, P. Efficient universal programmable quantum measurements. *Phys. Rev. Lett. 94* (2005), 090401.

[30] Defant, A., and Floret, K. *Tensor Norms and Operator Ideals.* North-Holland, Amsterdam, The Netherlands, 1993.

[31] Defant, A., Mastyło, M., and Michels, C. Summing norms of identities between unitary ideals. *Mathematische Zeitschrift 252* (2006), 863–882.

[32] Dieks, D. Communication by EPR devices. *Physics Letters A 92*, 6 (1982), 271 – 272.

[33] Dušek, M., and Bužek, V. Quantum-controlled measurement device for quantum-state discrimination. *Phys. Rev. A 66* (2002), 022112.

[34] Effros, E. G., and Ruan, Z.-J. *Operator Spaces.* Oxford University Press, 2000.

[35] Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett. 67* (1991), 661–663.

[36] Fiurášek, J., Dušek, M., and Filip, R. Universal measurement apparatus controlled by quantum software. *Phys. Rev. Lett. 89* (2002), 190401.

[37] Fuchs, C. A., and van de Graaf, J. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theor. 45*, 4 (2006), 1216–1227.

[38] Giladi, O., Prochno, J., Schütt, C., Tomczak-Jaegermann, N., and Werner, E. On the geometry of projective tensor products. *Journal of Functional Analysis 273*, 2 (2017), 471 – 495.

[39] Giovannetti, V., Maccone, L., Morimae, T., and Rudolph, T. G. Efficient universal blind quantum computation. *Phys. Rev. Lett. 111* (2013), 230501.

[40] Grothendieck, A. Résumé de la théorie métrique des produits tensoriels topologiques. *Boletim Da Sociedades de Matemática de São Paulo 8:1* (1953).

[41] Herbert, N. Flash—a superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics 12*, 12 (1982), 1171–1179.

[42] Hillery, M., Bužek, V., and Ziman, M. Programmable quantum gate arrays. *Fortschritte der Physik 49*, 10-11 (2001), 987–992.

[43] Hillery, M., Bužek, V., and Ziman, M. Probabilistic implementation of universal quantum processors. *Phys. Rev. A 65* (2002), 022301.

[44] Huang, H. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics 190*, 3 (2019), 949–955.

[45] Ishizaka, S., and Hiroshima, T. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett. 101* (2008), 240501.

[46] Jean-Pierre, K. *Some Random Series of Functions.* Cambridge University Press, 1993.

[47] Ji, Z. Classical verification of quantum proofs. *Theory of Computing 25* (2019), 1–42.

[48] Ji, Z., Natarajan, A., Vidick, T., Wright, J., and Yuen, H. MIP*=RE. *arXiv:2001.04383v2* (2020).

[49] Ji, Z., Wang, G., Duan, R., Feng, Y., and Ying, M. Parameter estimation of quantum channels. *IEEE Transactions on Information Theory 54*, 11 (2008), 5172–5185.

[50] Jones, V. F. A no-go theorem for the continuum limit of a periodic quantum spin chain. *Communications in Mathematical Physics 357*, 1 (2018), 295–317.

[51] Kempe, J., Kobayashi, H., Matsumoto, K., Toner, B., and Vidick, T. Entangled games are hard to approximate.

[52] Kent, A. Unconditionally secure bit commitment. *Physical Review Letters 83*, 7 (1999), 1447–1450.

[53] Kent, A., Munro, W. J., and Spiller, T. P. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A 84*, 1 (2011).

[54] Kim, J., Cheong, Y., Lee, J.-S., and Lee, S. Storing unitary operators in quantum states. *Phys. Rev. A 65* (2001), 012302.

[55] Kleinmann, M., Kampermann, H., and Bruss, D. Asymptotically perfect discrimination in the local-operation-and-classical-communication paradigm. *Physical Review A 84*, 4 (2011).

[56] Kliesch, A., and König, R. Continuum limits of homogeneous binary trees and the thompson group. *Physical Review Letters 124* (2020), 010601.

[57] Kubicki, A. M., Palazuelos, C., and Pérez-García, D. Resource quantification for the no-programing theorem. *Physical Review Letters 122*, 8 (2019).

[58] Kwapień, S. Isomorphic characterizations of inner product spaces by orthogonal series with vector valued coefficients. *Studia Mathematica 44*, 6 (1972), 583–595.

[59] Le Merdy, C. The schatten space S_4 is a $Q-$algebra. *Proceedings of the American Mathematical Society 126*, 3 (1998), 715–719.

[60] Leung, D., Toner, B., and Watrous, J. Coherent state exchange in multi-prover quantum interactive proof systems, 2011.

[61] Lindenstrauss, J., and Pełczyński, A. Absolutely summing operators in $l_{\{p\}}$-spaces and their applications. *Studia Mathematica 29*, 3 (1968), 275–326.

[62] Majenz, C. *Entropy in quantum information theory - Communication and cryptography.* PhD thesis, 2017.

[63] Mandel, L. Is a photon amplifier always polarization dependent? *Nature 304* (1983), 188.

[64] Maurey, B. Type, cotype and k-convexity. In *Handbook of the Geometry of Banach Spaces. Vol. 2* (2003), North-Holland, pp. 1299–1332.

[65] May, A. Quantum tasks in holography. *Journal of High Energy Physics 2019*, 10 (2019), 1–39.

[66] May, A., Penington, G., and Sorce, J. Holographic scattering requires a connected entanglement wedge. *Journal of High Energy Physics 2020*, 8 (2020).

[67] Mayers, D., and Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (1998), IEEE, pp. 503–509.

[68] Michal, A. D., and Wyman, M. Characterization of complex couple spaces. *Ann. Math. (2) 42* (1941), 247–250.

[69] Milman, V. D., and Pisier, G. Banach spaces with a weak citype 2 property. *Israel J. Math.*, 54 (1986), 139–158.

[70] Milonni, P., and Hardies, M. Photons cannot always be replicated. *Physics Letters A 92*, 7 (1982), 321 – 322.

[71] Muñoz, G., Sarantopoulos, Y., and Tonge, A. Complexifications of real banach spaces, polynomials and multilinear maps. *Studia Mathematica 134*, 1 (1999), 1–33.

[72] Nielsen, M. A., and Chuang, I. L. Programmable quantum gate arrays. *Phys. Rev. Lett. 79* (1997), 321–324.

[73] O'Donnell, R. *Analysis of Boolean Functions.* Cambridge University Press, 2014.

[74] Palazuelos, C., and Vidick, T. Survey on nonlocal games and operator space theory. *Journal of Mathematical Physics 57*, 1 (2016), 015220.

[75] Pati, A. K., and Braunstein, S. L. Impossibility of deleting an unknown quantum state. *Nature 404* (2000), 164 – 165.

[76] Paulsen, V. *Completely Bounded Maps and Operator Algebras.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2003.

[77] Paulsen, V. I. Representations of function algebras, abstract operator spaces, and banach space geometry. *Journal of Functional Analysis 109*, 1 (1992), 113 – 129.

[78] Peres, A., and Wootters, W. K. Optimal detection of quantum information. *Phys. Rev. Lett. 66* (1991), 1119–1122.

[79] Pérez-Delgado, C. A., and Fitzsimons, J. F. Iterated gate teleportation and blind quantum computation. *Phys. Rev. Lett. 114* (2015), 220502.

[80] Pérez-García, D. Optimality of programmable quantum measurements. *Phys. Rev. A 73* (2006), 052315.

[81] Pérez-García, D., Wolf, M. M., Palazuelos, C., Villanueva, I., and Junge, M. Unbounded violation of tripartite bell inequalities. *Communications in Mathematical Physics 279*, 2 (2008), 455–486.

[82] Pietsch, A. *Operator Ideals.* Mathematical Studies. North-Holland Publishing Company, 1980.

[83] Pietsch, A. *Eigenvalues and S-Numbers.* Cambridge University Press, USA, 1986.

[84] Pironio, S., Acín, A., Massar, Boyer de la Giroday, A., Matsukevich, D. N., Maunz, P., Olmschenk, S., D., H., Luo, L., Manning, T. A., and C., M. Random numbers certified by bell's theorem. *Nature 464*, 7291 (2010), 1021–1024.

[85] Pisier, G. *Remarques sur un résultat non publié de B. Maurey. Seminar on Functional Analysis, 1980-1981, Exp. No. V.* École Polytech., Palaiseau, 1981.

[86] Pisier, G. On the duality between type and cotype. In *Martingale Theory in Harmonic Analysis and Banach Spaces* (Berlin, Heidelberg, 1982), J.-A. Chao and W. A. Woyczyński, Eds., Springer Berlin Heidelberg, pp. 131–144.

[87] Pisier, G. Probabilistic methods in the geometry of banach spaces. In *Probability and Analysis* (Berlin, Heidelberg, 1986), G. Letta and M. Pratelli, Eds., Springer Berlin Heidelberg, pp. 167–241.

[88] Pisier, G. *The Volume of Convex Bodies and Banach Space Geometry.* Cambridge Tracts in Mathematics. Cambridge University Press, 1989.

[89] Pisier, G. Random series of trace class operators. *In Proceedings Cuarto CLAPEM Mexico 1990. Contribuciones en probabilidad y estadistica matematica* (1990), 29–42.

[90] Pisier, G. Factorization of operator valued analytic functions. *Advances in Mathematics 93*, 1 (1992), 61 – 125.

[91] Pisier, G. *The operator Hilbert space OH, complex interpolation, and tensor norms.* Memoirs of the American Mathematical Society. American mathematical society, Providence (R.I.), 1996.

[92] Pisier, G. Non-commutative vector valued l_p-spaces and completely p-summing maps. *Asterique 247* (1998).

[93] Pisier, G. *Introduction to Operator Space Theory.* London Mathematical Society Lecture Note Series. Cambridge University Press, 2003.

[94] Randrianantoanina, N. Non-commutative martingale transforms. *Journal of Functional Analysis 194*, 1 (2002), 181 – 212.

[95] Ray, S. K. On isometric embedding $\ell_p^m \to s_\infty$ and unique operator space structure. *Bulletin of the London Mathematical Society 52*, 3 (2020), 437–447.

[96] Raz, R. Exponential separation of quantum and classical communication complexity. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1999), STOC '99, Association for Computing Machinery, p. 358–367.

[97] Reed, M., and Simon, B. *Methods of modern mathematical physics: Functional analysis.* Academic Press, Inc., 1980.

[98] Regev, O., and Vidick, T. Quantum xor games. *ACM Transactions on Computation Theory 7*, 4 (2015), 1–43.

[99] Reichardt, B. W., Unger, F., and Vazirani, U. A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games, 2012.

[100] Reichardt, B. W., Unger, F., and Vazirani, U. A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science* (New York, NY, USA, 2013), ITCS '13, Association for Computing Machinery, p. 321–322.

[101] Rudin, W. *Functional Analysis.* McGraw-Hill, 1991.

[102] Ryan A., R. *Introduction to Tensor Products of banach Spaces.* Springer, London, 2002.

[103] SCHATTEN, R. *A Theory of Cross-Spaces. (AM-26).* Princeton University Press, 1950.

[104] Sedlák, M., Ziman, M., Přibyla, O. c. v., Bužek, V., and Hillery, M. Unambiguous identification of coherent states: Searching a quantum database. *Phys. Rev. A 76* (2007), 022326.

[105] Sentís, G., Bagan, E., Calsamiglia, J., and Muñoz Tapia, R. Multicopy programmable discrimination of general qubit states. *Phys. Rev. A 82* (2010), 042312.

[106] Sentís, G., Bagan, E., Calsamiglia, J., and Muñoz Tapia, R. Programmable discrimination with an error margin. *Phys. Rev. A 88* (2013), 052304.

[107] Speelman, F. Instantaneous non-local computation of low t-depth quantum circuits, 2015.

[108] Suzuki, J. Entanglement detection and parameter estimation of quantum channels. *Phys. Rev. A 94* (2016), 042306.

[109] Szarek, S. J. Kashin's almost euclidean orthogonal decomposition of L1_n. *Bulletin de L'Academie Polonaise des Sciences - Series des Sciencies Mathematiques, Astronomiques et Physiques 26*, 8 (1978), 691–694.

[110] Szarek, S. l., and Tomczak-Jaegermann, N. On nearly euclidean decomposition for some classes of banach spaces. *Compositio Mathematica 40*, 3 (1980), 367–385.

[111] Taylor, A. E. Analysis in complex Banach spaces. *Bull. Am. Math. Soc. 49* (1943), 652–669.

[112] Terhal, B. M., DiVincenzo, D. P., and Leung, D. W. Hiding bits in bell states. *Phys. Rev. Lett. 86* (2001), 5807–5810.

[113] Tomamichel, M., Fehr, S., Kaniewski, J., and Wehner, S. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics 15*, 10 (2013), 103002.

[114] Tomczak-Jaegermann, N. The moduli of smoothness and convexity and the rademacher averages of the trace classes S_p $(1 \leq p < \infty)$. *Studia Mathematica 50*, 2 (1974), 163–182.

[115] Tomczak-Jaegermann, N. *Banach-Mazur distances and finite-dimensional operator ideals*, vol. 38. Longman Sc. & Tech., 1989.

[116] Triebel, H. *Interpolation Theory, Function Spaces, Differential Operators.* North-Holland Publishing Company, 1978.

[117] Tsirel'son, B. S. Quantum analogues of the bell inequalities. The case of two spatially separated domains. *Journal of Soviet Mathematics 36*, 4 (1987), 557–570.

[118] Unruh, D. Quantum position verification in the random oracle model. In *Advances in Cryptology – CRYPTO 2014* (Berlin, Heidelberg, 2014), J. A. Garay and R. Gennaro, Eds., Springer Berlin Heidelberg, pp. 1–18.

[119] Vaidman, L. Instantaneous measurement of nonlocal variables. *Phys. Rev. Lett. 90* (2003), 010402.

[120] Van Hove, L. Von neumann's contributions to quantum theory. *Bulletin of the American Mathematical Society 64*, 3 (1958), 95–99.

[121] Vidal, G., and Cirac, J. I. Storage of quantum dynamics on quantum states: a quasi-perfect programmable quantum gate. *arXiv:quant-ph/0012067* (2000).

[122] Vidal, G., Masanes, L., and Cirac, J. I. Storing quantum dynamics in quantum states: A stochastic programmable gate. *Phys. Rev. Lett. 88* (2002), 047905.

[123] W. K. Wooters, W. H. Z. A single quantum cannot be cloned. *Nature 299* (1982), 802 –803.

[124] Watrous, J. *The Theory of Quantum Information.* Cambridge University Press, 2018.

[125] Wenzel, J. Real and complex operator ideals. *Quaestiones Mathematicae 18*, 1-3 (1995), 271–285.

[126] Wenzel, J. A supplement to my paper on real and complex operator ideals. *Quaestiones Mathematicae 20*, 4 (1997), 663–665.

[127] Wiesner, S. Conjugate coding. *SIGACT News 15*, 1 (1983), 78–88.

[128] Yu, L., Pérez-Delgado, C. A., and Fitzsimons, J. F. Limitations on information-theoretically-secure quantum homomorphic encryption. *Phys. Rev. A 90* (2014), 050303.

[129] Zhong-jin, R. Subspaces of c*-algebras. *Journal of Functional Analysis 76*, 1 (1988), 217 – 230.

[130] Zhou, T. Unambiguous discrimination between two unknown qudit states. *Quantum Information Processing 11*, 6 (2012), 1669–1684.

[131] Zhou, T., Cui, J. X., Wu, X., and Lon, G. L. Multicopy programmable discriminators between two unknown qubit states with group-theoretic approach. *Quantum Info. Comput. 12*, 11-12 (2012), 1017–1033.

Appendix A

A.1 Theorem 3.11. General case.

In this section, we prove that any $\epsilon - \mathrm{UPQP}_d$, $\mathcal{P}$, not necessarily unitary, satisfies the restrictions given by Theorem 3.11.

Proof. First, we consider a Stinespring's dilation for $\mathcal{P}$:

$$V \in \mathcal{U}(\ell_2^d \otimes \ell_2^{m'}), \;\text{ such that }\; \mathcal{P}(\,\cdot\,) = \mathrm{Tr}_{\mathcal{K}} V(\,\cdot\,)V^\dagger,$$

where $\ell_2^{m'} = \ell_2^m \otimes \mathcal{K}$ and $\mathcal{K}$ is an ancillary Hilbert space of dimension equal to the Krauss rank of $\mathcal{P}$, $rank(\mathcal{P}) \leq (\dim(\ell_2^d \otimes \ell_2^m))^2 \equiv (dm)^2$. Fixing the dimension of $\mathcal{K}$, V is uniquely determined up to unitaries on $\mathcal{K}$.

Now, we construct $\Phi_{\mathcal{P}}$ as in the unitary case:

$$\begin{array}{rccl} \Phi_{\mathcal{P}}: & \mathcal{S}_1^d & \hookrightarrow & \mathcal{S}_\infty^{m'} \\ & \sigma & \mapsto & \Phi_{\mathcal{P}}(\sigma) := \mathrm{Tr}_{\ell_2^d} V(\sigma^{\mathrm{T}} \otimes \mathrm{Id}_{\ell_2^{m'}}), \end{array} \tag{A.1}$$

and from Theorem 3.5 we obtain that:

$$\|\sigma\|_{\mathcal{S}_1^d} \geq \|\Phi_{\mathcal{P}}(\sigma)\|_{\mathcal{S}_\infty^{m'}} \geq (1-\varepsilon)^{1/2} \|\sigma\|_{\mathcal{S}_1^d}, \;\text{ for every }\; \sigma \in \mathcal{S}_1^d.$$

Using in the first place Proposition 2.4 and then Proposition 2.3, the last inequalities imply that:

$$\mathrm{T}_2(\mathcal{S}_1^d) \leq \frac{1}{(1-\varepsilon)^{\frac{1}{2}}} \mathrm{T}_2\Big(\Phi_V(\mathcal{S}_1^d)\Big) \leq \frac{1}{(1-\varepsilon)^{\frac{1}{2}}} \mathrm{T}_2\Big(\mathcal{S}_\infty^{m'}\Big). \tag{A.2}$$

Taking into account the estimates (2.9) we finally arrive to:

$$d \leq \frac{C}{(1-\varepsilon)} \log(\dim \ell_2^{m'}) \quad \Rightarrow \quad \dim \ell_2^{m'} \geq 2^{\frac{(1-\varepsilon)}{C} d},$$

where C can be taken equal to 4 or maybe better. Recalling that $\ell_2^{m'} = \ell_2^m \otimes \mathcal{K}$ with $\dim \mathcal{K} \leq (dm)^2$ we get the stated bound:

$$m \geq \frac{1}{d^{2/3}} 2^{\frac{(1-\varepsilon)d}{3C}} = 2^{\frac{(1-\varepsilon)d}{3C} - \frac{2}{3}\log d}.$$

□

A.2 Alternative proof of Theorem 3.11

As we have commented in Chapter 3, Section 3.5, Maurey's Lemma 3.14 allows us to give an alternative proof of Theorem 3.11 involving counting of cardinals of ε–nets. What we obtain following this route is[1]:

Claim A.2.1. *Let $\mathcal{P} \in \mathrm{CPTP}(\mathcal{H} \otimes \mathcal{H}_M)$ be a unitary $\epsilon - \mathrm{UPQP}_d$, then*

$$\dim \mathcal{H}_M \equiv m \geq 2^{\frac{(1-\varepsilon)}{64} \frac{d}{\log 2d}}.$$

Proof. By Theorem 3.5, the considered $\epsilon - \mathrm{UPQP}_d$ defines a linear map $\Phi : \mathcal{S}_1^d \hookrightarrow \mathcal{M}_m$ such that:

$$\|\sigma\|_{S_1^d} \geq \|\Phi_{\mathcal{V}}(\sigma)\|_{\mathcal{M}_m} \geq (1-\varepsilon)^{1/2} \|\sigma\|_{S_1^d} \qquad \forall \sigma \in S_1^d, \tag{A.3}$$

where m was the dimension of the memory register of the $\epsilon - \mathrm{UPQP}_d$. Now, we focus on the restriction of Φ to the subspace $\ell_1^d \subset \mathcal{S}_1^d$. Then, using Lemma 3.14, we construct a δ_k–net for $\Phi(ball(\ell_1^d))$, $\{\Phi(\sigma_i)\}_{i=1}^{|\mathcal{I}|}$,

[1] For simplicity, we restrict to the case of unitary UPQPs

where $\delta_k = 2k^{-1/q}\mathrm{T}_p(\mathcal{M}_m)$ for $k \in \mathbb{N}$. According to the Lemma, the cardinal of this δ_k–net is bounded by $|\mathcal{I}| \leq (2d)^k$. Furthermore, taking into account (A.3), we notice that $\{\sigma_i\}_{i=1}^{|\mathcal{I}|}$ is a $\delta_k/(1-\varepsilon)^{1/2}$–net of $ball(\ell_1^d)$. Then, the following bound for the cardinal $|\mathcal{I}|$ must be satisfied

$$\left(\frac{1-\varepsilon}{\delta_k}\right)^d \leq |\mathcal{I}| \leq (2d)^k. \tag{A.4}$$

Particularizing to $p = 2$, we have that $q = 2$ and $\mathrm{T}_2(\mathcal{M}_m) \leq (4\log m)^{1/2}$, as in the original proof in the submission. Choosing now $k \geq \frac{64\log m}{(1-\varepsilon)}$, we have that $\delta_k/(1-\varepsilon)^{1/2} \leq 1/2$. Then (A.4) reads as

$$2^d \leq (2d)^{\frac{64\log m}{(1-\varepsilon)}}.$$

From here, we finally obtain that

$$m \geq 2^{\frac{(1-\varepsilon)}{64}\frac{d}{\log 2d}}.$$

□

Appendix B

B.1 Handier expressions for $\sigma^{i}_{\mathcal{S}^{\mathcal{U}}}$, $\sigma^{ii}_{\mathcal{S}^{\mathcal{U}}}$

In this appendix we provide some expressions upper bounding $\sigma^{i}_{\mathcal{S}^{\mathcal{U}}}$ and $\sigma^{ii}_{\mathcal{S}^{\mathcal{U}}}$. The advantage of these expressions is that they are easier to compute and can be expressed directly in terms of the elements of a given strategy. However, we stress that in general these bounds might be inaccurate.

Proposition B.1. *Given a pure strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon \in \mathfrak{S}_{s2w}$,*

i.

$$\sigma^{i}_{\mathcal{S}^{\mathcal{U}}} \lesssim_{\log} \ \mathbb{E}_\varepsilon \ \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon - \tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}} \right\|^2_{M_{r^2},k\tilde{k}'} \right)^{1/2} + O\left(\frac{1}{n}\right);$$

ii.

$$\sigma^{ii}_{\mathcal{S}^{\mathcal{U}}} \lesssim_{\log} \ \mathbb{E}_\varepsilon \ \left(\sum_{i,j} \frac{1}{2} \left\| \left(\mathrm{Id}_{\ell_2^{k'}} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}) \right) |\varphi\rangle \right\|^2_{\ell_2^{k\tilde{k}'}} \right)^{1/2} + O\left(\frac{1}{n}\right).$$

Proof. We provide simple, likely far from tight, bounds for the quantity

$$\left(\sum_{i,j}\left\|\partial_{ij}\Phi^{i(ii)}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\right\|^2_{X^{i(ii)}}\right)^{1/2}$$

appearing in (4.19) (recall that $X^i = M_{\tilde{k}'^2,k\tilde{k}'}$, $X^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$). Recall also that $\partial_{ij}\Phi(\varepsilon) = \frac{\Phi(\varepsilon_{11},\dots,\varepsilon_{ij},\dots,\varepsilon_{nn})-\Phi(\varepsilon_{11},\dots,-\varepsilon_{ij},\dots,\varepsilon_{nn})}{2}$. In the rest of the proof we shorten notation denoting $(\varepsilon_{11},\dots,-\varepsilon_{ij},\dots,\varepsilon_{nn})$ as $\overline{\varepsilon}^{ij}$.

In the case of $\Phi^i_{\mathcal{S}^{\mathcal{U}}}$,

$$\begin{aligned}
&\|\partial_{ij}\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon)\|_{\mathcal{S}_\infty^{\tilde{k}'^2,k\tilde{k}'}}\\
&= \frac{1}{2}\left\|\frac{1}{n^2}\sum_{k,l\neq i,j}\varepsilon_{kl}\,\Big((\langle k|\tilde{V}_\varepsilon\otimes\langle l|\tilde{W}_\varepsilon)-(\langle k|\tilde{V}_{\overline{\varepsilon}^{ij}}\otimes\langle l|\tilde{W}_{\overline{\varepsilon}^{ij}})\Big)\,(V|kl\rangle\otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}})\right.\\
&\left.+\frac{1}{n^2}\,\varepsilon_{ij}\,\Big((\langle i|\tilde{V}_\varepsilon\otimes\langle j|\tilde{W}_\varepsilon)+(\langle i|\tilde{V}_{\overline{\varepsilon}^{ij}}\otimes\langle j|\tilde{W}_{\overline{\varepsilon}^{ij}})\Big)\,(V|ij\rangle\otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}})\right\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}}\\
&\leq \frac{1}{2}\left\|\frac{1}{n^2}\sum_{k,l}\varepsilon_{kl}\,\Big((\langle k|\tilde{V}_\varepsilon\otimes\langle l|\tilde{W}_\varepsilon)-(\langle k|\tilde{V}_{\overline{\varepsilon}^{ij}}\otimes\langle l|\tilde{W}_{\overline{\varepsilon}^{ij}})\Big)\,(V|kl\rangle\otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})\right\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}}\\
&+\frac{2}{n^2}\\
&= \frac{1}{2}\left\|\langle\psi_\varepsilon|\,\Big[\Big((\tilde{V}_\varepsilon\otimes\tilde{W}_\varepsilon)-(\tilde{V}_{\overline{\varepsilon}^{ij}}\otimes\tilde{W}_{\overline{\varepsilon}^{ij}})\Big)\,(V\otimes\mathrm{Id}_{\ell_2^{\tilde{k}'}})\otimes\mathrm{Id}_{\mathcal{H}_C}\Big]\,|\psi\rangle\right\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}}\\
&+O\left(\frac{1}{n^2}\right)\\
&\leq \frac{1}{2}\left\|(\tilde{V}_\varepsilon\otimes\tilde{W}_\varepsilon)-(\tilde{V}_{\overline{\varepsilon}^{ij}}\otimes\tilde{W}_{\overline{\varepsilon}^{ij}})\right\|_{\mathcal{S}_\infty^{r^2,k\tilde{k}'}}+O\left(\frac{1}{n^2}\right).
\end{aligned}$$

For $\Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}$, recalling the shortcut $X^{ii} = \mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$:

$$
\begin{aligned}
&\|\partial_{ij}\Phi^{ii}_{\mathcal{S}\mathcal{U}}(\varepsilon)\|_{X^{ii}} \\
&= \frac{1}{2}\left\| \frac{1}{n^2} \sum_{k,l\neq i,j} \varepsilon_{kl}\, |k\rangle \otimes |l\rangle \otimes \Big(V|kl\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}}\Big)\Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right. \\
&\left. + \frac{1}{n^2}\, \varepsilon_{ij}\, |i\rangle \otimes |j\rangle \otimes \Big(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}\Big)\Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right\|_{X^{ii}} \\
&\overset{(*)}{\leq} \frac{1}{2}\left\| \frac{1}{n^2} \sum_{k,l} \varepsilon_{kl}\, |k\rangle \otimes |l\rangle \otimes \Big(V|kl\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}}\Big)\Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right\|_{X^{ii}} \\
&+ \frac{2}{n^2} \\
&\leq \frac{1}{2n^2} \sum_{k,l} \left\| |k\rangle \otimes |l\rangle \otimes \Big(V|kl\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}}\Big)\Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right\|_{X^{ii}} \\
&+ O\left(\frac{1}{n^2}\right) \\
&\overset{(**)}{\leq} \frac{1}{2n^2} \sum_{k,l} \left\| \Big(V|kl\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}}\Big)\Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right\|_{\ell_2^{\tilde{k}'2}} + O\left(\frac{1}{n^2}\right) \\
&\leq \frac{1}{2n^2} \sum_{k,l} \left\| \Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right\|_{\ell_2^{k\tilde{k}'2}} + O\left(\frac{1}{n^2}\right) \\
&\leq \frac{1}{2} \left\| \Big(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle \right\|_{\ell_2^{k\tilde{k}'2}} + O\left(\frac{1}{n^2}\right).
\end{aligned}
$$

The previous two bounds lead automatically to the claimed statement.

In (*) we have applied a simple triangle inequality and used the fact that the elements in the sum are well normalized in the considered norm, recall Remark 4.18. For (**), if we denote $|\tilde{\varphi}_{kl}\rangle := \Big(V|kl\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}}\Big)\Big(\mathrm{Id}_{\ell_2^{k'}} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}})\Big)|\varphi\rangle$, we have to notice that, for each k, l, $|k\rangle \otimes |l\rangle \otimes |\tilde{\varphi}_{kl}\rangle = \iota_k \otimes \iota_l(|\tilde{\varphi}_{kl}\rangle)$ where ι_k, ι_l are the injections considered in Remark 4.18. There, we have proven that $\iota_k \otimes \iota_l$ is a contractive map from $\mathcal{S}_1^{\tilde{k}',n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}',n}$ into $\ell_2^{\tilde{k}'^2}$. Inequality (**) follows from this observation.

□

B.2 Non-pure strategies in Theorem 4.1

We give here some further details towards the proof of Theorem 4.1. We first explicit the statement we obtain in the case of *pure* strategies and then, how to obtain the general statement appearing in 4.1.

Claim B.2.1. *For $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$:*

I.

$$\omega(G;\mathcal{S}^{\mathcal{U}}) \leq C_1 + C_2' \; \sigma^{i}_{\mathcal{S}^{\mathcal{U}}} \; \log^{1/2}(k\tilde{k}') + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\omega(G;\mathcal{S}^{\mathcal{U}}) \leq \tilde{C}_1 + C_3' \; \tilde{\sigma}^{ii}_{\mathcal{S}^{\mathcal{U}}} \; \log^{1/2}(n\tilde{k}') + O\left(\frac{1}{n^{1/2}} + \frac{\log(n)\log^{1/2}(k\tilde{k})}{n}\right),$$

where we have denoted $\tilde{\sigma}^{ii}_{\mathcal{S}} = n^{3/4}\log(n)\,\sigma^{ii}_{\mathcal{S}}$.

Above, C_1, $\tilde{C}_1 < 1$, C_2', C_3' are positive constants.

Proof. Lemma 4.16 provides the following bounds:

$$\omega(G_{Rad};\mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^{i}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{X^i} + C \; \sigma^{i}_{\mathcal{S}^{\mathcal{U}}} \; \mathrm{T}_2^{(n^2)}\Big(X^i\Big), \tag{B.1}$$

$$\omega(G_{Rad};\mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^{ii}_{\mathcal{S}^{\mathcal{U}}}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C \; \sigma^{ii}_{\mathcal{S}^{\mathcal{U}}} \; \mathrm{T}_2^{(n^2)}\Big(X^{ii}\Big). \tag{B.2}$$

Taking into account the estimates

$$\mathrm{T}_2^{(n^2)}(X^i) \leq \mathrm{T}_2(X^i) \lesssim \log^{1/2}(k\tilde{k}'), \qquad \mathrm{T}_2^{(n^2)}(X^{ii}) \lesssim n^{3/4}\log(n)\log^{1/2}(n\tilde{k}'),$$

and Proposition 4.17, Equations (B.1), (B.2) transform in:

$$\omega(G_{Rad};\mathcal{S}^{\mathcal{U}}) \lesssim \frac{3}{4} + O\left(\frac{1}{n^{1/2}}\right) + C \; \sigma^{i}_{\mathcal{S}^{\mathcal{U}}} \; \log^{1/2}(k\tilde{k}'),$$

$$\omega(G_{Rad}; \mathcal{S}^{\mathcal{U}})$$
$$\lesssim \frac{\sqrt{3}}{2} + O\left(\frac{1}{\sqrt{n}} + \frac{\log(n)\log^{1/2}(k\tilde{k}')}{n}\right) + C\ \sigma^{ii}_{\mathcal{S}^{\mathcal{U}}}\ n^{3/4}\log(n)\log^{1/2}(n\tilde{k}').$$

□

Now, we use Lemma 4.12 to translate the previous bound to the case of a general strategy $\mathcal{S}$, obtaining that way the statement appearing in the main text.

Claim B.2.2. *The previous claim implies, for any* $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$*, the bounds:*

I.

$$\omega(G; \mathcal{S}) \leq C_1 + C_2\ \sigma^{i}_{\mathcal{S}}\ \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\omega(G; \mathcal{S}) \leq \tilde{C}_1 + C_3\ \tilde{\sigma}^{ii}_{\mathcal{S}}\ \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}} + \frac{\log(n)\log^{1/2}(nk\tilde{k})}{n}\right),$$

where we have denoted $\tilde{\sigma}^{ii}_{\mathcal{S}} = n^{3/4}\log(n)\,\sigma^{ii}_{\mathcal{S}}$*.*

Above, C_1, $\tilde{C}_1 < 1$, C_2, C_3 *are positive constants.*

Proof. Lemma 4.12 allows us to consider $\mathcal{S}$ as a pure strategy in $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$. The relevant estimate, also provided in that lemma, is that $\tilde{k}'$ can be taken to be lower or equal than $n^2k\tilde{k}^4$. I.e., $\mathcal{S}$ satisfies Claim B.2.1 with $\tilde{k}' \leq n^2k\tilde{k}^4$. Furthermore, we can roughly bound

$$k\tilde{k}' \leq (nk\tilde{k})^{\alpha},$$

for some positive constant α (take $\alpha = 4$, for instance). Since those factors appear in Claim B.2.1 only inside a logarithm, the exponent α only changes the constants C_2', C_3' appearing there. □

If one wants to state Theorem 4.1 in terms of the raw quantum dimension $\tilde{k}_q := \frac{\tilde{k}}{\tilde{k}_{cl}}$, where $\tilde{k}_{cl}$ was the dimension of the classical messages used in the strategy, it is possible to argue similarly as above using this time Lemma 4.11. The result is exactly the same, only the constants C_2, C_3 are affected.

B.3 Tensor norms and enough symmetries

In this appendix we give some additional information about spaces *with enough symmetries* and spaces *with enough symmetries in the orthogonal group*, properties used in our Theorem 4.24. Given a Banach space X, we refer to the group of isometries on that space as the *symmetry group* of X.

Definition B.2. *A Banach space X has enough symmetries if the only operators on X that commutes with the symmetry group of the space are $\lambda \operatorname{Id}_X$, being λ a scalar.*

It easy to see that if X has enough symmetries the same happens with X^*. Furthermore, it is a piece of folklore that tensor norms respect this property. That is, for any tensor norm α, $X \otimes_\alpha Y$ has enough symmetries when X and Y have enough symmetries. This fact follows from noticing that for any isometries f, g in X and Y, respectively, $f \otimes g$ is also an isometry in $X \otimes_\alpha Y$. This is guaranteed by the metric mapping property (2.15).

Finally, in [31] the notion of enough symmetries in the orthogonal group appears in the statement of [31, Lemma 5.2], result used in our proof of Theorem 4.24.

Definition B.3. *An n-dimensional Banach space X has enough symmetries in the orthogonal group if the symmetry group of X includes a subgroup of $GL(n)$ verifying the property that the only operators on X that commutes with that subgroup are $\lambda \operatorname{Id}_X$ for some scalar λ.*

We finally comment that tensor norms also preserve the property of having enough symmetries in the orthogonal group. The reason is the same as in the previous case of simply having enough symmetries. Furthermore, it is obvious from the definition that ℓ_2^n has enough symmetries in the orthogonal group and, therefore, $\ell_2^n \otimes_\alpha \ell_2^{n'}$, $(\ell_2^n \otimes_\alpha \ell_2^{n'}) \otimes_{\alpha'} \ell_2^{n''}$, $\ldots$ are also spaces with enough symmetries in the orthogonal group when α, α', $\ldots$ are tensor norms. In particular, the spaces considered in Theorem 4.24 have this property.

List of Symbols

Throughout this monograph we use the standard symbols $\mathbb{N}$, $\mathbb{R}$, $\mathbb{C}$ to denote the sets of natural, real and complex numbers, respectively. The set of complex matrices with n rows and m columns is denoted by $\mathbb{M}_{n,m}$ – $\mathbb{M}_n$ is the set of n-dimensional complex square matrices. When vector spaces are considered, the underlying field is always taken to be $\mathbb{C}$ unless the contrary is specified.

Symbols $\gtrsim$, $\lesssim$, $\gtrsim_{\log}$, $\lesssim_{\log}$ denote inequalities up to multiplicative dimension independent constants or up to multiplicative factors that are logarithmic in the dimension, respectively. Given real functions f, g, we say that $f(x) = O(g(x))$ ($f(x) = \Omega(g(x))$) if f is asymptotically bounded above (below) by g.

Logarithms are always taken in base 2, although the change of base is usually of minor importance in the context of this text.

Acronyms

MROQG	mixed rank-one quantum game, page 38
PBC	Position Based Cryptography, page 93
PBQC	Position Based Quantum Cryptography, page 91
POVM	positive operator-valued measure, page 16
PV	Position Verification, page 93
ROQG	rank-one quantum game, page 34
UPQP	Universal Programmable Quantum Processor, page 66

Linear spaces

$\langle\psi\ \vert, \langle\gamma\vert, \ldots$	linear forms in a vector space, page 2
$\lambda_i(f)$	i-th eigenvalue of f, page 6
$\mathbb{C}^{\mathcal{X}}$ $(\mathbb{R}^{\mathcal{X}})$	$\vert\mathcal{X}\vert$-dimensional complex (real) vector space, page 2
$\mathbb{C}^d$ $(\mathbb{R}^d)$	d-dimensional complex (real) vector space, page 2
Tr	trace map, page 4
†	conjugate transpose of a matrix, page 6
$^\sharp$	algebraic dual, page 2
f^*	adjoint operator associated to f, page 6
$s_i(f)$	i-th singular value of an operator f, page 4
$\vert\psi\rangle,\ \vert\gamma\rangle, \ldots$	vectors in a vector space, page 2

Banach spaces

ℓ_p	Banach space of p-summing sequences, page 43
$\ell_p^{\mathcal{X}}$ $(\ell_p^d$	Banach space of p-summing sequences with $\vert\mathcal{X}\vert(d)$ terms, page 43
ℓ_p^d	Banach space of p-summing sequences with d terms, page 43
*	dual space of a Banach space(or operator space, page 45), page 43
$(X_0, X_1)_\theta$	complex interpolation space between X_0 and X_1, page 52
$\mathcal{H}_{\mathcal{X}}$	$\vert\mathcal{X}\vert$-dimensional Hilbert space, page 2
$\mathfrak{S}_p^{w-cb}(X,Y)$	the space of operators of weak-cb Schatten-von Neumann type ℓ_p from X into Y, page 60

$\mathrm{C}_q(X)$	cotype-q constant of a Banach space X, page 48
$\mathrm{C}_q^{(m)}(X)$	cotype-q constant with m vectors of a Banach space X, page 48
$\mathrm{vr}(X)$	volume ratio of X, page 144
$\mathsf{ball}(X)$	closed unit ball of a Banach space X, page 42
$\pi_2(X, Y)$	space of 2-summing operators from X into Y, page 59
$\mathrm{T}_p(X)$	type-p constant of a Banach space X, page 47
$\mathrm{T}_p^{(m)}(X)$	type-p constant with m vectors of a Banach space X, page 48
$\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m}$	short-cut for the interpolation space $(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}, \mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m})_\theta$, page 109
σ_Φ	regularity parameter associated to Φ, page 107
$\mathcal{S}_p(\mathcal{H}, \mathcal{K})$	p-th Schatten of compact operators Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, page 43
$\mathcal{S}_p$	p-th Schatten of compact operators on the separable Hilbert spaces ℓ_2, page 43
$\mathcal{S}_p^{d,d'}$	p-th Schatten of operators from $\ell_2^{d'}$ into ℓ_2^d, page 43
$L_p(X)$	space of p-integrable functions with values in a Banach space X, page 44
$X \otimes_\pi Y$	the projective tensor product of X and Y, page 57
$X \otimes_\varepsilon Y$	the injective tensor product of X and Y, page 57
$\\|\cdot\\|$	operator norm, page 5

Spaces of operators

$\mathscr{B}(X, Y)$	space of bounded operators from X into Y, page 43

$\mathscr{L}(X,Y)$	space of linear operator from X into Y, page 3
$\mathscr{D}(\mathcal{H})$	set of density operators on $\mathcal{H}$, page 13
$\mathscr{P}(\mathcal{X})$	set of probability measures on $\mathcal{X}$, page 10
$\mathscr{C}\mathscr{B}(X,Y)$	space of completely bounded operators from X into Y, page 45
$\mathrm{CP}(\mathcal{H},\mathcal{K})$	set of completely positive maps from $\mathscr{B}(\mathcal{H})$ to $\mathscr{B}(\mathcal{K})$, page 8
$\mathrm{CPTP}(\mathcal{H},\mathcal{K})$	set of completely positive and trace preserving operators from $\mathscr{B}(\mathcal{H})$ into $\mathscr{B}(\mathcal{K})$, page 14
$\hat{f}$	tensor associated to the operator (or bilinear form) f, page 3
$\mathscr{B}i\ell(X\times Y)$	space of bilinear forms on X and Y, page 4
$\mathrm{Pos}(\mathcal{H})$	set of positive operators on $\mathcal{H}$, page 7
$\mathscr{U}(\mathcal{H})$	set of unitary operators in $\mathcal{H}$, page 6

Quantum Information

$\mathrm{CPTP}(\mathcal{H},\mathcal{K}\otimes\mathcal{K}')$	set of quantum-to-classical-quantum channels from $\mathscr{B}(\mathcal{H})$ into $\mathscr{B}(\mathcal{K}\otimes\mathcal{K}')$, page 17
$\mathrm{CPTP}_{qc}(\mathcal{H},\mathcal{K})$	set of quantum-to-classical channels from $\mathscr{B}(\mathcal{H})$ into $\mathscr{B}(\mathcal{K})$, page 15
Δ	completely dephasing channel, page 14
$\epsilon-\mathrm{UPQP}_d$	approximate Universal Programmable Quantum Processor of input dimension d and error threshold ϵ, page 70
$\mathfrak{S}^{\mathscr{U}}_{s2w;\tilde{k},k}$	set of pure strategies in the s2w;$\tilde{k}k$ scenario, page 119
$\mathfrak{S}^{\mathscr{U}}_{s2w}$	set of pure strategies in the s2w scenario, page 119

$\mathfrak{S}_{s2w;\tilde{k},k}$	set of strategies in the s2w;$\tilde{k}, k$ scenario, page 115
$\mathfrak{S}_{s2w}$	set of strategies in the s2w scenario, page 114
$\mathrm{Ins}(\mathcal{H}, \mathcal{K})$	set of instruments from $\mathscr{B}(\mathcal{H})$ into $\mathscr{B}(\mathcal{K})$, page 18
$\mathrm{POVM}(\mathcal{H})$	set of POVMs on $\mathscr{B}(\mathcal{H})$, page 16
$\omega(G; \mathcal{S})$	value achieved by a strategy $\mathcal{S}$ in a game G, Section 1.3
$\omega_{\mathfrak{S}}(G)$	value of a game G in a given scenario $\mathfrak{S}$, Section 1.3
$\omega_H(G)$	honest value of a game G , Section 1.3
$\omega_{s2w;\tilde{k},k}(G_{Rad})$	value of a game G in the s2w;$\tilde{k}, k$ scenario, page 116
$\omega_{s2w}(G)$	value of a game G in the s2w scenario, page 105
$\mathrm{Tr}_{\mathcal{H}}$	partial trace over $\mathcal{H}$, page 14
UPQP_d	Universal Programmable Quantum Processor of input dimension d, page 69
$J(\,\cdot\,)$	Choi-Jamiołokowski isomorphism, page 25
$\\|\cdot\\|_\diamond$	diamond norm, page 21

Other Symbols

$\mathbb{E}$	expected value, page 47
$(\varepsilon_i)_{i=1}^n$	n i.i.d. Rademacher random variables, page 47
$\mathbb{R}^+$	set of non-negative real numbers
$\mathcal{Q}_m$	m-dimensional Boolean cube, page 106