

Quasirandom Quantum Channels

Tom Bannink

CWI, 1098 XG Amsterdam, Netherlands
QuSoft, Science Park 123, 1098 XG Amsterdam, Netherlands
tombannink@gmail.com

Jop Briët

CWI, 1098 XG Amsterdam, Netherlands
QuSoft, Science Park 123, 1098 XG Amsterdam, Netherlands
j.briet@cw.nl

Farrokh Labib

CWI, 1098 XG Amsterdam, Netherlands
QuSoft, Science Park 123, 1098 XG Amsterdam, Netherlands
labib@cw.nl

Hans Maassen

QuSoft, Science Park 123, 1098 XG Amsterdam, Netherlands
Korteweg-de Vries Institute for Mathematics, Radboud University, Nijmegen, Netherlands
H.Maassen@math.ru.nl

Abstract

Mixing (or quasirandom) properties of the natural transition matrix associated to a graph can be quantified by its distance to the complete graph. Different mixing properties correspond to different norms to measure this distance. For dense graphs, two such properties known as spectral expansion and uniformity were shown to be equivalent in seminal 1989 work of Chung, Graham and Wilson. Recently, Conlon and Zhao extended this equivalence to the case of sparse vertex transitive graphs using the famous Grothendieck inequality.

Here we generalize these results to the non-commutative, or “quantum”, case, where a transition matrix becomes a quantum channel. In particular, we show that for irreducibly covariant quantum channels, expansion is equivalent to a natural analog of uniformity for graphs, generalizing the result of Conlon and Zhao. Moreover, we show that in these results, the non-commutative and commutative (resp.) Grothendieck inequalities yield the best-possible constants.

2012 ACM Subject Classification Theory of computation → Quantum information theory

Keywords and phrases Quantum channels, quantum expanders, quasirandomness

Digital Object Identifier 10.4230/LIPIcs.TQC.2020.5

Funding *Tom Bannink*: Supported by the Gravitation-grant NETWORKS-024.002.003 from the Dutch Research Council (NWO).

Jop Briët: Supported by the Gravitation-grant NETWORKS-024.002.003 from the Dutch Research Council (NWO). Additionally supported by an NWO VENI grant.

Farrokh Labib: Supported by the Gravitation-grant NETWORKS-024.002.003 from the Dutch Research Council (NWO).

Acknowledgements We would like to thank Māris Ozols, Michael Walter and Freek Witteveen for fruitful discussions.

1 Introduction

In a seminal work [8], Chung, Graham and Wilson – building on work of Thomason [33, 34] – proved that several seemingly distinct notions of quasirandomness for graphs are equivalent. In particular, they identified seven properties found in random graphs with high probability, that always coexist simultaneously in any large dense graph. Two of these properties are



© Tom Bannink, Jop Briët, Farrokh Labib, and Hans Maassen;
licensed under Creative Commons License CC-BY

15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020).

Editor: Steven T. Flammia; Article No. 5; pp. 5:1–5:20



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

spectral expansion and *uniformity* (defined below). A question of Chung and Graham [7] on the equivalence of these two properties in *sparse* graphs resulted in a line of research culminating in recent work of Conlon and Zhao [9], which introduced a surprising new item to the armory of combinatorics: the famous Grothendieck inequality [13]. In this paper, we draw a parallel line in the context of quantum information theory, where quantum channels take the place of graphs. In addition, we give a streamlined proof of the main result of [9] and show that the use of Grothendieck's inequality yields an optimal constant. Similarly, we show that the non-commutative Grothendieck inequality gives an optimal constant in the quantum setting.

Spectral expansion and uniformity

Spectral expansion is a linear-algebraic property given in terms of the transition matrix of a graph. This transition matrix is the normalized adjacency matrix, which for a d -regular graph $G = (V, E)$ is given by $A_{uv} = e(\{u\}, \{v\})/d$, where $e(S, T)$ denotes the number of edges connecting subsets $S, T \subseteq V$. We say that the graph G is an (n, d, λ) graph if $|V| = n$, it is d -regular and all but the largest eigenvalue of A , which is always 1, have modulus at most λ . The smallest value of λ for which this holds is denoted by $\lambda(G)$. Spectral expansion then refers to the property that $\lambda(G)$ is much smaller than 1, in which case G is referred to as a (spectral) expander. Expanders have many important applications in mathematics and computer science (we refer to [23] for an extensive survey). One such application is in randomized algorithms, which can exploit the fact that a random walk on an expander rapidly mixes (i.e. quickly converges to its limit distribution) to significantly reduce the amount of randomness needed.

Uniformity is a combinatorial property of the configuration of the edges. An n -vertex d -regular graph $G = (V, E)$ is ϵ -uniform if for all $S, T \subseteq V$,

$$\left| e(S, T) - \frac{d}{n}|S||T| \right| \leq \epsilon dn \quad (1)$$

and $\epsilon(G)$ denotes the smallest value of ϵ for which this holds. Uniformity then refers to the property that this parameter is much smaller than 1; trivially any graph is 1-uniform. Intuitively, this says that for any two vertex subsets, the number of edges between those sets is close to the expected number of edges in a random graph with the same edge density.

A basic result known as the Expander Mixing Lemma [23] shows that for any regular graph G we have $\epsilon(G) \leq \lambda(G)$, which is to say that spectral expansion implies uniformity. A sequence G_n of d_n -regular graphs is called *dense* if $d_n \geq \Omega(n)$, and *sparse* if $d_n/n \rightarrow 0$. It was shown in [8] that in the dense case, a converse to the Expander Mixing Lemma $\epsilon(G_n) \leq o(1) \Rightarrow \lambda(G_n) \leq o(1)$ also holds. In contrast, Krivelevich and Sudakov [25] showed that this is false for sparse graphs, thereby answering the question posed in [7]. Their counterexample is not regular, however (and a later one from [4] is not connected). But in [9] it was shown that even regular sparse graphs (where $d_n \leq o(n)$) can simultaneously satisfy $\epsilon(G_n) \leq o(1)$ and $\lambda(G_n) \geq \Omega(1)$. Surprisingly, Kohayakawa, Rödl, and Schacht [24] showed that Cayley graphs over abelian groups, including sparse ones, do again admit such a converse. Cayley graphs are an important class of regular graphs that include for instance the famous Ramanujan graphs of Margulis [27] and Lubotzky, Phillips and Sarnak [26]. Conlon and Zhao [9] generalized this to all Cayley graphs and showed that this implies the same for all vertex-transitive graphs in general, for which they showed that $\lambda(G) \leq 4K_G\epsilon(G)$, where $1.6769\dots \leq K_G < 1.7822\dots$ is the famous *Grothendieck constant*, whose exact value is currently unknown; the bounds shown here are the best known and were shown by Davie

and Reeds (independently) in [11, 30] and Braverman et al. in [5], respectively. Spectral expansion and uniformity are thus equivalent notions of quasirandomness for dense graphs and vertex-transitive graphs.

Quasirandomness in quantum information theory

A transition matrix, such as the normalized adjacency matrix of a graph, maps probability vectors¹ to probability vectors. A natural non-commutative generalization of a transition matrix is a *quantum channel*, a completely positive trace preserving linear map $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$; see Section 2 for formal definitions. Quantum channels are the most general operations on quantum systems that are physically realizable. They encapsulate the “classical” transition matrices by restricting them to diagonal matrices whose diagonals form probability vectors; we discuss this in more detail in Section 3. In quantum information theory, general linear maps from $M_n(\mathbb{C})$ to itself are referred to as *superoperators*. Since superoperators are in one-to-one correspondence with bilinear forms on $M_n(\mathbb{C}) \times M_n(\mathbb{C})$, they also appear in the context of (generalizations of) Bell inequalities from physics in the form of quantum XOR games [31, 10], as well as in combinatorial optimization [28].

The graph-theoretic concepts mentioned above have natural analogues for superoperators, which we discuss next.

In independent work, Hastings [18] and Ben-Aroya, Schwartz and Ta-Schma [3] introduced *quantum expanders* as a special class of quantum channels defined analogously to spectral expanders. For a unital² quantum channel Φ , the expansion parameter is given by

$$\lambda(\Phi) = \|\Phi - \Pi\|_{S_2 \rightarrow S_2} = \sup \{ \|(\Phi - \Pi)(X)\|_{S_2} : \|X\|_{S_2} \leq 1 \}, \quad (2)$$

where $\Pi : X \mapsto \frac{1}{n} \text{Tr}(X) \text{Id}$ is the projection onto the identity, $\|X\|_{S_2} = \sqrt{\langle X, X \rangle}$ is the Frobenius (or Schatten-2) norm and $\langle X, Y \rangle = \frac{1}{n} \text{Tr}(Y^* X)$ is the normalized trace inner product. A quantum channel is an expander if $\lambda(\Phi)$ is much smaller than 1. Also quantum expanders found many applications, one of which is again randomness reduction, where randomness takes on the form of random unitary matrices. Since a k -qubit unitary requires 4^k real parameters, sampling one from the uniform distribution (Haar probability measure) is very expensive. A 1-design is a fixed collection of unitaries U_1, \dots, U_m such that the superoperator $\Phi(X) = \frac{1}{m} \sum_{i=1}^m U_i X U_i^*$ exactly effects the projection Π , thus mimicking in a finite way the Haar measure on $U(n)$. Quantum expanders can be used to construct *approximate* 1-designs, meaning that $\Phi(X)$ and $\Pi(X)$ are close in trace distance³ instead of precisely equal. Another application is in cryptography where Ambainis and Smith [1] used quantum expanders to construct short quantum one-time pads. It was shown in [18] that truly random quantum channels (given by independent Haar-uniform U_i as described above) are quantum expanders with high probability, supporting the idea that this is a notion of quasirandomness.

In this work we introduce a natural notion of uniformity for superoperators, informally given by how well they mimic the action of Π on projectors on subspaces, which may be thought of as generalizations of vertex subsets in graphs. This is similar to Hasting’s notion of edge expansion for quantum channels [18]. In particular, we say that Φ is ϵ -uniform if for any two subspaces $V, W \subseteq \mathbb{C}^n$ with associated projections P_V, P_W , it holds that

$$|\langle P_V, (\Phi - \Pi)(P_W) \rangle| \leq \epsilon. \quad (3)$$

¹ We use the convention of writing probability vectors as *column* vectors instead of row vectors.

² This is the superoperator analogue of regularity for graphs, defined in Section 2.

³ The trace distance is the distance induced by the Schatten-1 norm, defined in Section 2.

Let $\epsilon(\Phi)$ denote the smallest ϵ for which this holds. As we show in Section 3.3, the parameters $\lambda(\Phi)$ and $\epsilon(\Phi)$ reduce to their graphical analogs under a suitable embedding of graphs into quantum channels.

Finally, also symmetry, which in the graph-theoretic context takes the form of vertex transitivity, is an important property of quantum channels. In particular, *irreducibly covariant* quantum channels, which turn out to generalize vertex-transitive graphs (see Section 3), play an important role in questions about the capacity of quantum channels as noisy transmitters of quantum information [22]. A now famous result of Hastings [19] shows that the minimum output capacity in general does not have the intuitively natural property of being sub-additive under tensor products. However, it was shown earlier by Holevo [21], that the capacity is additive for the subclass of irreducibly covariant quantum channels.

Summary of our results

In this work we make a first step in the study of the equivalence of quasirandom properties for quantum channels, or superoperators in general, and show optimality in the case of vertex-transitive graphs and covariant quantum channels.

- (Section 3.2) Our main result shows that under irreducible covariance, expansion and uniformity are equivalent for superoperators. In particular, while a simple analogue of the classical Expander Mixing Lemma implies that $\epsilon(\Phi) \leq \lambda(\Phi)$ in general, we show using a non-commutative version of Grothendieck's inequality due to Haagerup [14], that for this class of superoperators, also $\lambda(\Phi) \leq 2\pi^2\epsilon(\Phi)$ always holds. This implies the same result for vertex-transitive graphs with \mathbb{C} -weighted edges, essentially proved in [9] with the factor 2 replaced by the *complex* Grothendieck constant $1.3380\dots \leq K_G^{\mathbb{C}} \leq 1.4049\dots$
- (Section 3.3) We show that a construction of sparse regular graphs from [9] can be embedded to give a sequence of quantum channels Φ_n that are not irreducibly covariant and for which it holds that $\epsilon(\Phi_n) \leq o(1)$ and $\lambda(\Phi_n) \geq \Omega(1)$.
- (Section 3.4) We show that for *randomizing* channels, a notion introduced in [2], the two notions of quasirandomness are also equivalent. This can be interpreted as a generalization of the same statement for dense graphs proved in [8].
- (Section 4.1) We show that the result of [9] cannot be improved in the sense that the factors $4K_G$ and $\pi^2 K_G^{\mathbb{C}}$ are optimal in the case of vertex-transitive graphs with \mathbb{R} -weighted and \mathbb{C} -weighted edges, respectively.
- (Section 4.2) Our work leaves open whether the factor $2\pi^2$ in our main result is optimal. However, our proof consists of two steps, the first of which gives a factor 2 and the second a factor π^2 , and we show these steps are individually optimal. We prove that the first step is optimal by showing that an example of Haagerup and Ito [16] for the non-commutative Grothendieck inequality is irreducibly covariant, which uses some representation theory of $SO(n)$. The optimality of the second step follows directly from a result of [9].

2 Preliminaries

Write $[n] = \{1, \dots, n\}$. For a finite set S , write $\mathbb{E}_{s \in S}$ for $\frac{1}{|S|} \sum_{s \in S}$. For a compact set S , write $C(S)$ for the set of continuous functions from S to \mathbb{C} . For a compact group Γ , write $\mathbb{E}_{g \in \Gamma}$ for the integral with respect to the (unique) Haar probability measure on Γ .

Write $M_n(\mathbb{C})$ for the set of complex $n \times n$ matrices and let $U(n) = \{X \in M_n(\mathbb{C}) : X^*X = \text{Id}\}$ be the set of unitary matrices. Here, all maps of the form $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ are linear, and we refer to these as superoperators. A superoperator Φ is *unital* if $\Phi(\text{Id}) = \text{Id}$

and it is *completely positive* if for all $k \in \mathbb{N}$ the superoperator $\text{Id} \otimes \Phi : M_k \otimes M_n \rightarrow M_k \otimes M_n$ maps positive semidefinite matrices to positive semidefinite matrices. Completely positive superoperators that are trace preserving are called *quantum channels*.

We normalize inner products so that for $x, y \in \mathbb{C}^n$ we define $\langle y, x \rangle = \mathbb{E}_{i \in [n]} \bar{y}_i x_i$ and for matrices $X, Y \in M_n(\mathbb{C})$ we have $\langle Y, X \rangle = \frac{1}{n} \text{Tr}[Y^* X]$.

Norms

For $p \in [1, \infty)$, $x \in \mathbb{C}^n$ and $X \in M_n(\mathbb{C})$, the L_p norm and (normalized) Schatten- p norm are defined by

$$\|x\|_{L_p} = \left(\mathbb{E}_{i \in [n]} |x_i|^p \right)^{1/p} \quad \text{and} \quad \|X\|_{S_p} = \left(\frac{1}{n} \text{Tr}[(X^* X)^{p/2}] \right)^{1/p}$$

and $\|x\|_{L_\infty} = \max_i |x_i|$ and $\|X\|_{S_\infty} = \sup\{|\langle Xx, y \rangle| : \|x\|_{L_2}, \|y\|_{L_2} \leq 1\}$. Note that for the identity matrix $\text{Id} \in M_n$ we have $\|\text{Id}\|_{S_p} = 1$ for all $p \in [1, \infty)$.

► **Proposition 1.** *Let $p \geq 1$ and let $X \in M_n(\mathbb{C})$. Then $\|X\|_{S_p} \geq \|(X_{11}, \dots, X_{nn})\|_{L_p}$.*

Proof. For a vector $x \in \mathbb{C}^n$, denote by $\text{Diag}(x)$ the $n \times n$ matrix with x on the diagonal and for a matrix X denote by $\text{diag}(X)$ the matrix where we set the off-diagonal elements to 0. A small computation shows that

$$\mathbb{E}_{s \in \{\pm 1\}^n} \text{Diag}(s) X \text{Diag}(s) = \text{diag}(X).$$

Since the Schatten- p norms are invariant under conjugation with a unitary matrix, applying the above with the triangle inequality gives

$$\|(X_{11}, \dots, X_{nn})\|_{L_p} = \|\text{diag}(X)\|_{S_p} \leq \mathbb{E}_{s \in \{\pm 1\}^n} \|\text{Diag}(s) X \text{Diag}(s)\|_{S_p} = \|X\|_{S_p}. \quad \blacktriangleleft$$

For $q \in [1, \infty)$, define $q' \in [1, \infty)$ to be its dual given by $\frac{1}{q} + \frac{1}{q'} = 1$. For $p, q \in [1, \infty)$, a matrix $A \in M_n(\mathbb{C})$ and a superoperator $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$, define

$$\begin{aligned} \|A\|_{L_p \rightarrow L_q} &= \sup\{|\langle y, Ax \rangle| : \|x\|_{L_p} \leq 1, \|y\|_{L_{q'}} \leq 1\} \\ \|\Phi\|_{S_p \rightarrow S_q} &= \sup\{|\langle Y, \Phi(X) \rangle| : \|X\|_{S_p} \leq 1, \|Y\|_{S_{q'}} \leq 1\}. \end{aligned}$$

Also define the *cut norms* by

$$\begin{aligned} \|A\|_{\text{cut}} &= \max\{|\langle y, Ax \rangle| : x, y \in \{0, 1\}^n\} \\ \|\Phi\|_{\text{cut}} &= \sup\{|\langle Y, \Phi(X) \rangle| : X, Y \text{ projectors}\}. \end{aligned}$$

It is then not hard to see that if G is a d -regular graph with normalized adjacency matrix A , then $\epsilon(G) = \|A - \frac{1}{n} J\|_{\text{cut}}$, where J is the all-ones matrix. Similarly, we have $\epsilon(\Phi) = \|\Phi - \Pi\|_{\text{cut}}$.

We have the following relation between these norms, the proof of which is a simple generalization of the same result from [9] for matrices.

► **Lemma 2.** *For any superoperator Φ , we have $\|\Phi\|_{\text{cut}} \leq \|\Phi\|_{S_\infty \rightarrow S_1} \leq \pi^2 \|\Phi\|_{\text{cut}}$ and π^2 is the best possible constant.*

Proof. First note that the cut norm as defined above can also be written as

$$\|\Phi\|_{\text{cut}} = \sup\{|\langle Y, \Phi(X) \rangle| : X, Y \succeq 0, \|X\|_{S_\infty}, \|Y\|_{S_\infty} \leq 1\}, \quad (4)$$

because the set $\{X : X \succeq 0, \|X\|_{S_\infty} \leq 1\}$ is the convex hull of the set of projectors. Hence, by linearity the supremum in (4) will always be attained by projectors.

The first inequality of the lemma follows by dropping the positive semidefinite constraint. For the second inequality, let z be a complex number of norm 1, and w a uniform random complex number of norm 1. Then

$$z = \pi \mathbb{E}_w [w \mathbf{1}_{\{\Re(z\bar{w}) \geq 0\}}].$$

Note that $\mathbb{E}_w[f(w)] = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta})d\theta$, hence the equality follows by using $\int_{-\pi/2}^{\pi/2} \cos(\theta)d\theta = 2$. We have $\|\Phi\|_{S_\infty \rightarrow S_1} = \sup\{|\langle Y, \Phi(X) \rangle| : \|X\|_{S_\infty}, \|Y\|_{S_\infty} \leq 1\}$. The set of matrices X such that $\|X\|_{S_\infty} \leq 1$ is the convex hull of the set of unitary matrices, so by linearity we can assume that the supremum in $\|\Phi\|_{S_\infty \rightarrow S_1}$ is obtained by unitary X, Y . Unitary matrices are diagonalizable, so write $X = UAU^*$ and $Y = VB^*V$ with U, V unitary and A, B diagonal. Let $u, w \in \mathbb{C}$, $|u| = |w| = 1$ be uniform random complex numbers and define diagonal matrices A', B' as $A'_{ii}(w) = \mathbf{1}_{\{\Re(A_{ii}\bar{w}) \geq 0\}}$ and $B'_{ii}(u) = \mathbf{1}_{\{\Re(B_{ii}\bar{u}) \geq 0\}}$. By the above we have $A = \pi \mathbb{E}_w[wA'(w)]$ and similar for B , so we have $X = \pi \mathbb{E}_w[wUA'(w)U^*]$ and $Y = \pi \mathbb{E}_u[uVB'(u)V^*]$. Now, $UA'(w)U^*$ and $VB'(u)V^*$ are projections for all values of w and u , as required in the definition of the cut norm. Therefore

$$\begin{aligned} \|\Phi\|_{S_\infty \rightarrow S_1} &= |\langle Y, \Phi(X) \rangle| = \pi^2 |\mathbb{E}_{u,w} \bar{u}w \langle VB'(u)V^*, \Phi(UA'(w)U^*) \rangle| \\ &\leq \pi^2 \mathbb{E}_{u,w} |\langle VB'(u)V^*, \Phi(UA'(w)U^*) \rangle| \\ &\leq \pi^2 \mathbb{E}_{u,w} \|\Phi\|_{\text{cut}} \\ &= \pi^2 \|\Phi\|_{\text{cut}}, \end{aligned}$$

completing the first part of the proof. Conlon and Zhao show that π^2 is the best possible constant in the commutative case, using the matrix $A \in M_n(\mathbb{C})$ given by $A_{st} = e^{2\pi i(s-t)/n}$. This matrix satisfies $\|A\|_{L_\infty \rightarrow L_1} = n$ and one can show $\|A\|_{\text{cut}} = (\pi^{-2} + o(1))n$. By Proposition 10 in Section 3.3, their example can be embedded into a superoperator with the same norms so π^2 is also the best possible constant here. \blacktriangleleft

Define the *Grothendieck norm* of a matrix $A \in M_n(\mathbb{C})$ by

$$\|A\|_G := \sup \left\{ \left| \frac{1}{n} \sum_{i,j=1}^n A_{ij} \langle x_i, y_j \rangle \right| : d \in \mathbb{N}, x_i, y_j \in \mathbb{C}^d, \|x_i\|_{L_2} \leq 1, \|y_j\|_{L_2} \leq 1 \right\}.$$

Then, the *complex Grothendieck constant* is given by

$$K_G^{\mathbb{C}} := \sup \left\{ \frac{\|A\|_G}{\|A\|_{L_\infty \rightarrow L_1}} : n \in \mathbb{N}, A \in M_n(\mathbb{C}) \right\}.$$

The current best upper and lower bounds on $K_G^{\mathbb{C}}$ are 1.4049 [15] and 1.338 [11], respectively. The real version of the Grothendieck constant, denoted by K_G and mentioned in the introduction, is obtained by replacing the underlying field in the above quantities by the reals.

Some basic group theory

Given a graph $G = (V, E)$, a permutation $\pi : V \rightarrow V$ is an *automorphism* of G if for all $u, v \in V$, we have $\{\pi(u), \pi(v)\} \in E \Leftrightarrow \{u, v\} \in E$. The automorphisms of G form a group under composition, which we call $\text{Aut}(G)$. Then, G is said to be *vertex transitive* if for every $u, v \in V$, there is a $\pi \in \text{Aut}(G)$ such that $\pi(u) = v$. For superoperators, we have the following

analogous definitions. A unitary representation of a group Γ on \mathbb{C}^n is a homomorphism from Γ to $U(n)$ and it is irreducible if the only subspaces of \mathbb{C}^n that are left invariant by the group action are the zero-dimensional subspace and \mathbb{C}^n itself.

► **Definition 3** (Irreducible covariance). *A superoperator $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ is irreducibly covariant if there exist a compact group Γ and continuous irreducible unitary representations $U, V : \Gamma \rightarrow U(n)$ such that for all $g \in \Gamma$ and $X \in M_n(\mathbb{C})$, we have*

$$\Phi(U(g)XU^*(g)) = V(g)\Phi(X)V^*(g).$$

3 Converse expander mixing lemmas

In this section, we prove the “converse expander mixing lemmas” announced in the first and third bullet in the introduction. As a warm-up, we start with a proof of the commutative case due to Conlon and Zhao, which we reprove in a slightly different manner analogous to how we will prove the non-commutative case.

3.1 Commutative case

In the following, let S be a compact set and Γ be a compact group acting continuously and transitively on S . The Haar probability measure on Γ induces a measure on S (by pullback) according to which the L_p -norm (for $p \in [1, \infty)$) and inner product of $f, g \in C(S)$ are given by

$$\|f\|_{L_p} = \left(\mathbb{E}_{\pi \in \Gamma} |f(\pi(s_0))|^p \right)^{\frac{1}{p}} \quad \text{and} \quad \langle f, g \rangle = \mathbb{E}_{\pi \in \Gamma} \overline{f(\pi(s_0))} g(\pi(s_0)), \quad (5)$$

where (by transitivity) s_0 can be taken to be some arbitrary but fixed element of S . We lift the action of Γ on S to an action on $C(S)$ by precomposition, that is, for any function $f \in C(S)$ and element $\pi \in \Gamma$, define the function f^π by $f^\pi(s) := f(\pi(s))$. Furthermore, for a linear map $A : C(S) \rightarrow C(S)$ define A^π by $A^\pi f := (Af^\pi)^{\pi^{-1}}$ and say that A is transitive covariant with respect to Γ if for any $\pi \in \Gamma$ we have $A^\pi = A$.⁴ We sometimes omit the group and simply say A is *transitive covariant* if such a group Γ exists.

In [9], the following result is proved (over the real numbers) for the case $S = [n]$, in which case transitive covariant linear maps A are simply $n \times n$ matrices which commute with the permutation matrices of a transitive subgroup Γ of S_n . However, their proof easily implies the more general version below.

► **Theorem 4** (Conlon–Zhao). *Let S be as above and let $A : C(S) \rightarrow C(S)$ be a linear map that is transitive covariant with respect to Γ . Then,*

$$\|A\|_{L_2 \rightarrow L_2} \leq K_G^{\mathbb{C}} \|A\|_{L_\infty \rightarrow L_1}.$$

Here we give a somewhat more streamlined proof of this result based on a well-known factorization version of Grothendieck’s inequality [13] (see also [29]), which will serve as a stepping stone to the proof of the non-commutative case.⁵ In our setting the inequality asserts the following

⁴ In general one says A is *covariant* with respect to Γ , but we say *transitive* to emphasize that we require Γ to act transitively on S .

⁵ The main difference is that in [9], the result is first proved for weighted Cayley graphs, after which it is shown that this implies the result for transitive covariant matrices.

► **Theorem 5** (Commutative Grothendieck inequality (factorization)). *Let S be as above and let $A : C(S) \rightarrow C(S)$ be a linear map. Then, there exist probability measures λ, ν on S such that for all $f, g \in C(S)$, we have*

$$|\langle g, Af \rangle| \leq K_G^{\mathbb{C}} \|A\|_{L_\infty \rightarrow L_1} \left(\int_S |f(s)|^2 d\lambda(s) \right)^{1/2} \left(\int_S |g(s)|^2 d\nu(s) \right)^{1/2}.$$

Proof of Theorem 4. It follows from the triangle inequality and transitivity that

$$|\langle g, Af \rangle| \leq \mathbb{E}_{\pi \in \Gamma} |\langle g, A^\pi f \rangle| = \mathbb{E}_{\pi \in \Gamma} |\langle g^\pi, Af^\pi \rangle|.$$

By Theorem 5 and the AM-GM inequality there are probability measures λ, ν on S such that the above right-hand side is at most

$$\frac{K_G^{\mathbb{C}} \|A\|_{L_\infty \rightarrow L_1}}{2} \mathbb{E}_{\pi \in \Gamma} \left(\int_S |f^\pi(s)|^2 d\lambda(s) + \int_S |g^\pi(s)|^2 d\nu(s) \right) = \frac{K_G^{\mathbb{C}} \|A\|_{L_\infty \rightarrow L_1}}{2} (\|f\|_{L_2}^2 + \|g\|_{L_2}^2),$$

where we switched the order of the integrals (using Tonelli's theorem) and the expression (5) for the L_2 norm. For $\|f\|_{L_2} = \|g\|_{L_2} = 1$ this shows $\|A\|_{L_2 \rightarrow L_2} \leq K_G^{\mathbb{C}} \|A\|_{L_\infty \rightarrow L_1}$. ◀

3.2 Non-commutative case

Our main technical result is as follows.

► **Theorem 6.** *Let $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ be an irreducibly covariant superoperator. Then, $\|\Phi\|_{S_\infty \rightarrow S_1} \leq \|\Phi\|_{S_2 \rightarrow S_2} \leq 2\|\Phi\|_{S_\infty \rightarrow S_1}$.*

Since the supremum in $\|\Phi\|_{S_\infty \rightarrow S_1}$ is taken over X, Y with S_∞ -norm equal to 1, the first inequality of the theorem follows from the fact that $\|X\|_{S_2} \leq \|X\|_{S_\infty}$. As projectors have Schatten- ∞ norm 1, the first inequality also easily implies the analogue of the Expander Mixing Lemma, that is, $\epsilon(\Phi) \leq \lambda(\Phi)$, where $\lambda(\Phi)$ and $\epsilon(\Phi)$ are as in (2) and (3), respectively; note that when Φ is irreducibly covariant, so is $\Phi - \Pi$. The second inequality is proved at the end of this section and in Section 4.2 we show that the factor 2 in the theorem is optimal. With Lemma 2, which relates the uniformity parameter $\epsilon(\Phi)$ to $\|\Phi - \Pi\|_{S_\infty \rightarrow S_1}$, Theorem 6 then immediately gives the following result stated in the introduction.

► **Corollary 7** (Converse Quantum Expander Mixing Lemma). *Let $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ be an irreducibly covariant superoperator. Then, $\lambda(\Phi) \leq 2\pi^2 \epsilon(\Phi)$.*

In this non-commutative setting we use the following analog of Theorem 5 (a factorization version of the non-commutative Grothendieck inequality), proved by Haagerup in [14]; see also [29]. A density matrix is a positive semidefinite matrix with trace equal to 1.

► **Theorem 8** (Haagerup). *Let $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ be a superoperator. Then, there exist density matrices $\rho_1, \rho_2, \sigma_1, \sigma_2$ such that for any $X, Y \in M_n(\mathbb{C})$, we have*

$$|\langle Y, \Phi(X) \rangle| \leq \|\Phi\|_{S_\infty \rightarrow S_1} (\text{Tr}[\rho_1 X^* X] + \text{Tr}[\rho_2 X X^*])^{1/2} (\text{Tr}[\sigma_1 Y^* Y] + \text{Tr}[\sigma_2 Y Y^*])^{1/2}. \quad (6)$$

We also use the following lemma.

► **Lemma 9.** *Let Γ be a compact group. Then, a unitary representation $U : \Gamma \rightarrow U(n)$ is irreducible if and only if for any $X \in M_n(\mathbb{C})$, we have*

$$\mathbb{E}_{g \in \Gamma} U(g) X U(g)^* = \text{Tr}(X) \frac{1}{n} \text{Id}.$$

Proof. By Schur's lemma, if U is an irreducible representation, then for $T \in M_n(\mathbb{C})$

$$\left[\forall g \in \Gamma \quad U(g)TU(g)^* = T \right] \iff \left[\exists \lambda \in \mathbb{C} \quad T = \lambda \text{Id} \right].$$

Let $T_X = \mathbb{E}_{g \in \Gamma} U(g)XU(g)^*$, then by the group structure we have $U(g)T_XU(g)^* = T_X$ for all $g \in \Gamma$. Therefore, if U is irreducible then $T_X = \lambda_X \text{Id}$. By taking the trace, it follows that $\lambda_X = \text{Tr}(X)/n$. In the other direction, if U is reducible then there exists a projector P onto an irreducible subspace that is left invariant, i.e. $U(g)PU(g)^* = P$ for all $g \in \Gamma$, so $T_P \neq \lambda \text{Id}$. \blacktriangleleft

Proof of Theorem 6. Denote by Γ and $U, V: \Gamma \rightarrow U(n)$ the group and irreducible representations such that Φ is irreducibly covariant with respect to Γ (see Definition 3). For any $X, Y \in M_n(\mathbb{C})$ write $X_g = U(g)XU(g)^*$ and $Y_g = V(g)YV(g)^*$, then we have

$$|\langle Y, \Phi(X) \rangle| = \mathbb{E}_{g \in \Gamma} |\langle Y_g, \Phi(X_g) \rangle|.$$

By Theorem 8 and the AM-GM inequality, there exist density matrices $\rho_1, \rho_2, \sigma_1, \sigma_2$ such that the right hand side is bounded from above by

$$\frac{1}{2} \|\Phi\|_{S_\infty \rightarrow S_1} \mathbb{E}_{g \in \Gamma} \left(\text{Tr}[\rho_1 X_g^* X_g] + \text{Tr}[\rho_2 X_g X_g^*] + \text{Tr}[\sigma_1 Y_g^* Y_g] + \text{Tr}[\sigma_2 Y_g Y_g^*] \right).$$

By Lemma 9 we have $\mathbb{E}_{g \in \Gamma} X_g^* X_g = \mathbb{E}_{g \in \Gamma} U(g)X^* X U(g)^* = \frac{1}{n} \text{Tr}[X^* X] \text{Id} = \|X\|_{S_2}^2 \text{Id}$. Let ρ be a density matrix, then $\mathbb{E}_{g \in \Gamma} \text{Tr}[\rho X_g^* X_g] = \|X\|_{S_2}^2$. The same holds for $\mathbb{E}_{g \in \Gamma} \text{Tr}[\rho X_g X_g^*]$ but with U , and for Y with V , so we see that the above quantity is equal to

$$\|\Phi\|_{S_\infty \rightarrow S_1} \left(\|X\|_{S_2}^2 + \|Y\|_{S_2}^2 \right).$$

If $\|X\|_{S_2} = \|Y\|_{S_2} = 1$ we obtain $\|\Phi\|_{S_2 \rightarrow S_2} \leq 2\|\Phi\|_{S_\infty \rightarrow S_1}$. \blacktriangleleft

3.3 Embedding graphs into quantum channels

In this subsection, we elucidate the claim that quantum channels generalize graphs and prove the result stated in the second bullet in the introduction, namely that there are non-irreducible quantum channels for which a converse expander mixing lemma does not hold.

We consider the following embeddings. For $A \in M_n(\mathbb{C})$, define $\Phi_A: M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ as

$$\Phi_A(X) = \sum_{i,j} A_{ij} X_{jj} E_{ii}, \tag{7}$$

where E_{ij} is the matrix with a single 1 at position (i, j) . When A is a transition matrix, i.e., its column sums are 1, then it is not hard to see that Φ_A is completely positive and trace preserving and that $\Phi_{\frac{1}{n}J} = \Pi$. Several other ways exist to create quantum expanders from expander graphs, see for example [20] and [17], but as we show below, our embedding given above carries over all relevant properties of the graph we consider here.

Conlon and Zhao [9] give an infinite sequence of d -regular graphs G_n that are $o(1)$ -uniform but for which $\lambda(G_n) \geq 1/2$. Combined with the following proposition, this immediately gives the result stated in the second bullet in the introduction.

Proposition 10. *Let $A \in M_n(\mathbb{C})$ and $p, q \in [1, \infty]$. Then, for Φ_A as in (7), we have*

$$\|\Phi_A - \Pi\|_{S_p \rightarrow S_q} = \|A - \frac{1}{n}J\|_{L_p \rightarrow L_q} \quad \text{and} \quad \|\Phi_A - \Pi\|_{\text{cut}} = \|A - \frac{1}{n}J\|_{\text{cut}}.$$

5:10 Quasirandom Quantum Channels

Proof. Let $B = A - \frac{1}{n}J$, then $\Phi_A - \Pi = \Phi_B$. By compactness and definition of $\|\cdot\|_{S_p \rightarrow S_q}$ we can assume there is an $X \in M_n(\mathbb{C})$ such that $\|\Phi_B\|_{S_p \rightarrow S_q} = \|\Phi_B(X)\|_{S_q} / \|X\|_{S_p}$. Write $X = \text{diag}(x) + X_{\text{other}}$ where $x \in \mathbb{C}^n$ is the diagonal of X , and X_{other} are the off-diagonal entries. Note that by definition of Φ_B we have $\Phi_B(X) = \Phi_B(\text{diag}(x)) = \text{diag}(Bx)$. By definition of Schatten norms, $\|\text{diag}(x)\|_{S_p} = \|x\|_{L_p}$ and by Proposition 1 we have $\|X\|_{S_p} \geq \|x\|_{L_p}$. We have

$$\|B\|_{L_p \rightarrow L_q} \geq \frac{\|Bx\|_{L_q}}{\|x\|_{L_p}} \geq \frac{\|\text{diag}(Bx)\|_{S_q}}{\|X\|_{S_p}} = \frac{\|\Phi_B(X)\|_{S_q}}{\|X\|_{S_p}} = \|\Phi_B\|_{S_p \rightarrow S_q}$$

Now let $y \in \mathbb{C}^n$ be such that $\|B\|_{L_p \rightarrow L_q} = \|By\|_{L_q} / \|y\|_{L_p}$. Then

$$\|\Phi_B\|_{S_p \rightarrow S_q} \geq \frac{\|\Phi_B(\text{diag}(y))\|_{S_q}}{\|\text{diag}(y)\|_{S_p}} = \frac{\|\text{diag}(By)\|_{S_q}}{\|y\|_{L_p}} = \frac{\|By\|_{L_q}}{\|y\|_{L_p}} = \|B\|_{L_p \rightarrow L_q}.$$

This proves the first part.

The cut norm of a matrix takes the supremum over $x, y \in \{0, 1\}^n$. Instead we can relax this to $x, y \in [0, 1]^n$, since by linearity the supremum will always be attained by the extreme points. Similarly, for the superoperator case, we use Equation (4). Then, there exist $x, y \in [0, 1]^n$ such that $\|B\|_{\text{cut}} = |\langle Bx, y \rangle|$. We have $\text{diag}(x), \text{diag}(y) \succeq 0$ and $\|\text{diag}(x)\|_{S_\infty}, \|\text{diag}(y)\|_{S_\infty} \leq 1$. Therefore

$$\|\Phi_B\|_{\text{cut}} \geq |\langle \text{diag}(y), \Phi_B(\text{diag}(x)) \rangle| = |\langle \text{diag}(y), \text{diag}(Bx) \rangle| = |\langle y, Bx \rangle| = \|B\|_{\text{cut}}.$$

In the other direction, let $X, Y \in M_n(\mathbb{C})$ such that $X, Y \succeq 0$ and $\|X\|_{S_\infty}, \|Y\|_{S_\infty} \leq 1$. Define x, y to be the diagonals of X, Y , i.e. $x_i = X_{ii}$ and $y_i = Y_{ii}$. By Proposition 1 we have $\|x\|_{L_\infty}, \|y\|_{L_\infty} \leq 1$. Since $X, Y \succeq 0$ we know all diagonal entries of X and Y are real and non-negative, so we have $x, y \in [0, 1]^n$. We conclude

$$\|B\|_{\text{cut}} \geq |\langle y, Bx \rangle| = |\langle \text{diag}(y), \text{diag}(Bx) \rangle| = |\langle Y, \Phi_B(X) \rangle| = \|\Phi_B\|_{\text{cut}},$$

completing the proof. ◀

Note that $\|A - \frac{1}{n}J\|_{L_2 \rightarrow L_2}$ is the second largest eigenvalue in absolute value of the matrix A , so spectral expansion is preserved under the embedding of graphs into quantum channels. Also, uniformity is preserved since the cut-norm does not change.

The following proposition shows that the embedding (7) preserves transitivity. This shows that our Theorem 6 generalizes the main result of [9], albeit with a slightly worse constant.

► **Proposition 11.** *For any $A \in M_n(\mathbb{C})$, A is vertex transitive if and only if Φ_A is irreducibly covariant.*

Proof. Suppose A is vertex transitive. Let $\pi \in \text{Aut}(A)$ be a permutation and $P_\pi \in M_n(\mathbb{C})$ be the associated permutation matrix, so that $P_\pi A P_\pi^* = A$. Then,

$$\begin{aligned} \Phi_A(P_\pi X P_\pi^*) &= \sum_{i,j} A_{ij} (P_\pi X P_\pi^*)_{jj} E_{ii} \\ &= \sum_{i,j} A_{ij} X_{\pi^{-1}(j)\pi^{-1}(j)} E_{ii} \\ &= \sum_{i,j} A_{i\pi(j)} X_{jj} E_{ii} \\ &= \sum_{i,j} A_{\pi(i)\pi(j)} X_{jj} E_{\pi(i)\pi(i)} \\ &= \sum_{i,j} A_{\pi(i)\pi(j)} X_{jj} (P_\pi E_{ii} P_\pi^*) = P_\pi \Phi_A(X) P_\pi^*. \end{aligned}$$

This shows that for all $\pi \in \text{Aut}(A)$ we have $\Phi_A(P_\pi X P_\pi^*) = P_\pi \Phi_A(X) P_\pi^*$.

Let $\mathbb{T} = \{c \in \mathbb{C} : |c| = 1\}$ be the complex unit circle. For $\alpha \in \mathbb{T}^n$, define $U_\alpha := \text{diag}(\alpha)$. We have $U_\alpha E_{ii} U_\alpha^* = |\alpha_i|^2 E_{ii} = E_{ii}$ and $(U_\alpha X U_\alpha^*)_{ii} = |\alpha_i|^2 X_{ii} = X_{ii}$. Therefore

$$\Phi_A(U_\alpha X U_\alpha^*) = \sum_{i,j} A_{ij} (U_\alpha X U_\alpha^*)_{jj} E_{ii} = \sum_{i,j} A_{ij} X_{jj} U_\alpha E_{ii} U_\alpha^* = U_\alpha \Phi_A(X) U_\alpha^*.$$

We combine these two observations as follows. First we have that

$$\left(\mathbb{E}_{\alpha \in \mathbb{T}^n} U_\alpha X U_\alpha^* \right)_{ij} = \mathbb{E}_{\alpha \in \mathbb{T}^n} \alpha_i X_{ij} \bar{\alpha}_j = \int_0^{2\pi} \int_0^{2\pi} \alpha_i X_{ij} \bar{\alpha}_j d\alpha_i d\alpha_j = X_{ii} \delta_{ij}$$

If A is vertex transitive then for all $x \in \mathbb{C}^n$ we have $\mathbb{E}_{\pi \in \text{Aut}(A)} P_\pi \text{diag}(x) P_\pi^* = (\mathbb{E}_i x_i) \text{Id}$. Therefore

$$\mathbb{E}_{\substack{\pi \in \text{Aut}(A) \\ \alpha \in \mathbb{T}^n}} (P_\pi U_\alpha) X (P_\pi U_\alpha)^* = \mathbb{E}_{\pi \in \text{Aut}(A)} P_\pi \left(\mathbb{E}_{\alpha \in \mathbb{T}^n} U_\alpha X U_\alpha^* \right) P_\pi^* = \frac{\text{Tr}(X)}{n} \text{Id}.$$

Letting $G \subset M_n(\mathbb{C})$ be the subgroup generated by the U_α and P_π for $\pi \in \text{Aut}(A)$, we see that for any $g \in G$

$$\Phi_A(g X g^*) = g \Phi_A(X) g^*$$

and by the previous equation and Lemma 9, G acts irreducibly on \mathbb{C}^n (and it is unitary). This proves Φ is irreducibly covariant with respect to the group G with equal representations.

For the other direction, let $U : G \rightarrow U(n)$ be the irreducible representation such that Φ_A is irreducibly covariant, i.e. $\Phi_A(U(g) X U(g)^*) = U(g) \Phi_A(X) U(g)^*$ for all $g \in G$. Define $P_g \in M_n(\mathbb{C})$ as $(P_g)_{ij} = |U(g)_{ij}|^2$ so that $(U(g) E_{jj} U(g)^*)_{ii} = (P_g)_{ij}$. Then

$$\begin{aligned} A_{kl} &= \text{Tr}[E_{kk} \Phi_A(E_{ll})] = \text{Tr}[U(g) E_{kk} U(g)^* \Phi_A(U(g) E_{ll} U(g)^*)] \\ &= \sum_{ij} A_{ij} (P_g)_{jl} (P_g)_{ik} = (P_g^T A P_g)_{kl}, \end{aligned}$$

showing $P_g^T A P_g = A$. Since $U(g)$ is unitary, P_g is doubly stochastic so by Birkhoff's Theorem P_g is a convex combination of permutation matrices, i.e., $P_g = \mathbb{E}_i \Pi_i$ for some (not necessarily uniform) probability distribution and where Π_i is a permutation matrix. We have

$$A_{kl} = (P_g^T A P_g)_{kl} = \mathbb{E}_i \mathbb{E}_j (\Pi_i^T A \Pi_j)_{kl} = \mathbb{E}_i \mathbb{E}_j A_{\pi_i(k) \pi_j(l)}.$$

Since A is $\{0, 1\}$ -valued, it follows that if $A_{kl} = 1$ then all elements of the convex combination on the right-hand side must be 1, and if $A_{kl} = 0$ then all elements of the right hand side must be 0. Therefore, for all i we have $\Pi_i^T A \Pi_i = A$. By irreducibility, we have for all k, l that

$$\frac{1}{n} = \frac{\text{Tr}[E_{kk}]}{n} \text{Id}_{ll} = \left(\mathbb{E}_{g \in G} U(g) E_{kk} U^*(g) \right)_{ll} = \mathbb{E}_{g \in G} |U(g)_{lk}|^2,$$

showing $\mathbb{E}_{g \in G} (P_g)_{lk} = 1/n$. It follows that there is a $g \in G$ such that $(P_g)_{lk} > 0$. Decomposing P_g into permutation matrices shows there is a $\Pi \in \text{Aut}(A)$ such that $\Pi_{lk} = 1$. This holds for all k, l , proving the lemma. \blacktriangleleft

3.4 Randomizing superoperators

We prove the following analogue of one of the results from [8] showing that for any d -regular graph G , it holds that $\lambda(G) \leq (2\epsilon(G)/\delta^2)^{1/4}$, where $\delta = d/n$ is the edge density. This in particular establishes a tight relation between spectral expansion and uniformity for sequences of graphs with $\delta_n \geq \Omega(1)$. For $A \in M_n(\mathbb{C})$, we have $\|A\|_{L_1 \rightarrow L_\infty} = n \sup_{ij} |A_{ij}|$, and for an n -vertex d -regular graph with normalized adjacency matrix A we have $\sup_{ij} |A_{ij}| = \frac{1}{d}$ so $\|A\|_{L_1 \rightarrow L_\infty} = \frac{1}{\delta}$. Therefore, a sequence of graphs with normalized adjacency matrices A_n is dense exactly when $\|A_n\|_{L_1 \rightarrow L_\infty} \leq \mathcal{O}(1)$.

A superoperator Φ is said to be η -randomizing if $\|\Phi\|_{S_1 \rightarrow S_\infty} \leq \eta$, which when $\eta \leq \mathcal{O}(1)$, may thus be seen as an analogue of density. Note that by Proposition 10 the embedding of any dense graph is $\mathcal{O}(1)$ -randomizing.

► **Proposition 12.** *Let $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ be a unital superoperator that is $\mathcal{O}(1)$ -randomizing. Then, $\lambda(\Phi) \leq \mathcal{O}(\epsilon(\Phi)^{1/4})$.*

To prove Proposition 12, we require the following lemma.

► **Lemma 13.** *Let $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ be a superoperator and let $C = \|\Phi\|_{S_1 \rightarrow S_\infty}$. Then we have $\|\Phi\|_{S_2 \rightarrow S_2} \leq \left(C^3 \|\Phi\|_{S_\infty \rightarrow S_1} \right)^{1/4}$.*

Proof. Note that by definition of C we have $|\langle Q, \Phi(P) \rangle| \leq C \|Q\|_{S_1} \|P\|_{S_1}$. Let $X, Y \in M_n(\mathbb{C})$ be such that $\langle Y, \Phi(X) \rangle = \|\Phi\|_{S_2 \rightarrow S_2}$ with $\|X\|_{S_2} = \|Y\|_{S_2} = 1$. Write $X = \frac{1}{n} \sum_{i=1}^n \lambda_i P_i$ and $Y = \frac{1}{n} \sum_{i=1}^n \mu_i Q_i$ with P_i, Q_i rank-1 matrices with $\|Q_i\|_{S_1} = \|P_i\|_{S_1} = 1$. We have $\|\lambda\|_{L_2} = \|\mu\|_{L_2} = 1$ and by applying Cauchy-Schwarz twice,

$$\begin{aligned} |\langle Y, \Phi(X) \rangle|^4 &= \left| \mathbb{E}_{ij} \lambda_i \mu_j \langle Q_j, \Phi(P_i) \rangle \right|^4 \\ &\leq \left(\mathbb{E}_i \lambda_i^2 \right)^2 \left(\mathbb{E}_j \left| \mathbb{E}_i \mu_j \langle Q_j, \Phi(P_i) \rangle \right|^2 \right)^2 \\ &= \left(\mathbb{E}_{i,j,j'} \mu_j \mu_{j'} \langle Q_j, \Phi(P_i) \rangle \langle P_i, \Phi^*(Q_{j'}) \rangle \right)^2 \\ &\leq \left(\mathbb{E}_{j,j'} \mu_j^2 \mu_{j'}^2 \right) \left(\mathbb{E}_{j,j'} \left| \mathbb{E}_i \langle Q_j, \Phi(P_i) \rangle \langle P_i, \Phi^*(Q_{j'}) \rangle \right|^2 \right) \\ &= \mathbb{E}_{i,i',j,j'} \langle Q_j, \Phi(P_i) \rangle \langle P_i, \Phi^*(Q_{j'}) \rangle \langle Q_{j'}, \Phi(P_{i'}) \rangle \langle P_{i'}, \Phi^*(Q_j) \rangle, \end{aligned}$$

where all indices are averaged from 1 to n . Now we see

$$\begin{aligned}
|\langle Y, \Phi(X) \rangle|^4 &\leq \mathbb{E}_{i,j} \langle Q_j, \Phi(P_i) \rangle \left\langle \mathbb{E}_{j'} \langle Q_{j'}, \Phi(P_i) \rangle Q_{j'}, \Phi \left(\mathbb{E}_{i'} \langle P_{i'}, \Phi^*(Q_j) \rangle P_{i'} \right) \right\rangle \\
&\leq \mathbb{E}_{i,j} |\langle Q_j, \Phi(P_i) \rangle| \|\Phi\|_{S_\infty \rightarrow S_1} \|\mathbb{E}_{j'} \langle Q_{j'}, \Phi(P_i) \rangle Q_{j'}\|_{S_\infty} \|\mathbb{E}_{i'} \langle P_{i'}, \Phi^*(Q_j) \rangle P_{i'}\|_{S_\infty} \\
&\leq \mathbb{E}_{i,j} |\langle Q_j, \Phi(P_i) \rangle| \|\Phi\|_{S_\infty \rightarrow S_1} \max_{j'} |\langle Q_{j'}, \Phi(P_i) \rangle| \max_{i'} |\langle Q_j, \Phi(P_{i'}) \rangle| \\
&\leq C^3 \|\Phi\|_{S_\infty \rightarrow S_1}. \quad \blacktriangleleft
\end{aligned}$$

Proof of Proposition 12. Let $\Pi(X) = \frac{1}{n} \text{Tr}[X] \text{Id}$ and $\mathcal{E} = \Phi - \Pi$, then $\|\mathcal{E}\|_{\text{cut}} \leq \epsilon$ by assumption. Define $C = \|\Phi\|_{S_1 \rightarrow S_\infty}$. We have $\|\Pi\|_{S_1 \rightarrow S_\infty} = 1$ so by the triangle inequality, $\|\mathcal{E}\|_{S_1 \rightarrow S_\infty} \leq C + 1$. Using Lemma 2 and Lemma 13 applied to \mathcal{E} we find $\|\mathcal{E}\|_{S_2 \rightarrow S_2} \leq ((C + 1)^3 \pi^2 \epsilon)^{1/4}$. \blacktriangleleft

4 Optimality of constants

4.1 Commutative case

In this section we prove the fourth bullet point in our introduction. Theorem 4 shows that $K_G^{\mathbb{C}}$ bounds the ratio of the $L_2 \rightarrow L_2$ and $L_\infty \rightarrow L_1$ norms, and Lemma 2 (the matrix version) shows that π^2 bounds the ratio of the $L_\infty \rightarrow L_1$ norm and the cut norm. We now prove the optimality of the combined inequality.

Let $S^{m-1} = \{x \in \mathbb{C}^m : \|x\|_{L_2} = 1\}$ denote the $(m-1)$ -dimensional unit sphere endowed with its Haar probability measure μ .

► **Theorem 14.** *For any $\epsilon > 0$ there exist positive integers m, k and a transitive covariant linear map $M : C(S^{m-1} \times [k]) \rightarrow C(S^{m-1} \times [k])$ such that $\|M\|_{L_2 \rightarrow L_2} \geq (\pi^2 K_G^{\mathbb{C}} - \epsilon) \|M\|_{\text{cut}}$.*

The optimality of π^2 between the $L_\infty \rightarrow L_1$ norm and the cut norm is already covered in Lemma 2. We show that $K_G^{\mathbb{C}}$ is optimal in the sense that Theorem 4 cannot be improved (despite the fact that the exact value of the Grothendieck constant $K_G^{\mathbb{C}}$ is unknown). We do this in Lemma 15 below. Then in Lemma 16 we show that any map can be lifted to one on a bigger space with appropriately bounded cut norm. The combination of these lemmas proves our theorem.

In the introduction we also mentioned the optimal constant $4K_G$ in the case where the field is \mathbb{R} instead of \mathbb{C} . The proofs below still apply in this case, with only small modifications.

► **Lemma 15.** *For any $\epsilon > 0$ there exists a positive integer m and a transitive covariant linear map $B : C(S^{m-1}) \rightarrow C(S^{m-1})$ such that $\|B\|_{L_2 \rightarrow L_2} \geq (K_G^{\mathbb{C}} - \epsilon) \|B\|_{L_\infty \rightarrow L_1}$.*

Proof. By definition of the Grothendieck constant, for any $\epsilon > 0$ there exists an $n \in \mathbb{N}$ and a linear map $A \in M_n(\mathbb{C})$ such that $\|A\|_G \geq (K_G^{\mathbb{C}} - \epsilon) \|A\|_{L_\infty \rightarrow L_1}$. This map A might not be transitive covariant, so from it we will now construct a transitive covariant linear map $B : C(S^{2n-1}) \rightarrow C(S^{2n-1})$ such that $\|B\|_{L_\infty \rightarrow L_1} \leq \|A\|_{L_\infty \rightarrow L_1}$ and $\|B\|_{L_2 \rightarrow L_2} \geq \|A\|_G$. This idea is based on a lemma found in [6].

Let $x^i, y^j \in S^{2n-1}$ be the vectors that attain the Grothendieck norm for A , which can always be assumed to be $2n$ -dimensional since there are only $2n$ of them, so

$$\|A\|_G = \left| \frac{1}{n} \sum_{i,j} A_{ij} \langle x^i, y^j \rangle \right|.$$

5:14 Quasirandom Quantum Channels

Define the map B by

$$\langle f, B(g) \rangle = \frac{1}{n} \sum_{i,j} A_{ij} \int_{U(2n)} f(Ux^i)g(Uy^j)dU.$$

To bound $\|B\|_{L_\infty \rightarrow L_1}$ we have to bound $|\langle f, B(g) \rangle|$ for $f, g : S^{2n-1} \rightarrow [-1, 1]$. By the triangle inequality,

$$|\langle f, B(g) \rangle| \leq \int_{U(2n)} \left| \frac{1}{n} \sum_{i,j} A_{ij} f(Ux^i)g(Uy^j) \right| dU \leq \int_{U(2n)} \|A\|_{L_\infty \rightarrow L_1} dU \leq \|A\|_{L_\infty \rightarrow L_1}.$$

Now for each $i \in [2n]$ let $f_i \in C(S^{2n-1})$ be given by $f_i(x) = x_i$ (i.e. the i -th coordinate). Then,

$$\begin{aligned} \frac{1}{2n} \sum_{i=1}^{2n} \langle f_i, B(f_i) \rangle &\leq \frac{1}{2n} \sum_{i=1}^{2n} \|B\|_{L_2 \rightarrow L_2} \|f_i\|_{L_2}^2 \\ &= \|B\|_{L_2 \rightarrow L_2} \int_{S^{2n-1}} \frac{1}{2n} \sum_{i=1}^{2n} x_i^2 d\mu(x) \\ &= \|B\|_{L_2 \rightarrow L_2}. \end{aligned}$$

On the other hand,

$$\frac{1}{2n} \sum_{i=1}^{2n} \langle f_i, B(f_i) \rangle = \frac{1}{n} \sum_{i,j} A_{ij} \int_{U(2n)} \langle Ux^i, Uy^j \rangle dU = \frac{1}{n} \sum_{i,j} A_{ij} \langle x^i, y^j \rangle = \|A\|_G,$$

so we conclude $\|B\|_{L_2 \rightarrow L_2} \geq \|A\|_G$. We will show B is transitive covariant with respect to $\Gamma = U(2n)$. To show B is invariant, we have to prove that for all $V \in U(2n)$ we have $\langle f^V, B(g^V) \rangle = \langle f, B(g) \rangle$. Indeed,

$$\begin{aligned} \langle f^V, B(g^V) \rangle &= \frac{1}{n} \sum_{i,j} A_{ij} \int_{U(2n)} f(VUx^i)g(VUy^j)dU \\ &= \frac{1}{n} \sum_{i,j} A_{ij} \int_{U(2n)} f(U'x^i)g(U'y^j)dU' = \langle f, B(g) \rangle, \end{aligned}$$

which completes the proof. ◀

► **Lemma 16.** *Let S be any compact set and let $B : C(S) \rightarrow C(S)$ be a linear map. For any $\epsilon > 0$ there exists a $k \in \mathbb{N}$ and a linear map $M : C(S \times [k]) \rightarrow C(S \times [k])$ such that*

$$\frac{\|M\|_{\text{cut}}}{\|M\|_{L_2 \rightarrow L_2}} \leq \left(\frac{1}{\pi^2} + \epsilon \right) \frac{\|B\|_{L_\infty \rightarrow L_1}}{\|B\|_{L_2 \rightarrow L_2}}$$

and if B is transitive covariant then so is M .

Proof. We will choose k large enough, to be determined later. For any $f, g \in C(S \times [k])$ define $f^i \in C(S)$ as $f^i(s) := f(s, i)$, and similar for g^i . Define $\omega = e^{2\pi i/k}$. Define a linear map $M : C(S \times [k]) \rightarrow C(S \times [k])$ as

$$(M(f))(t, j) := \frac{1}{k} \sum_{i=1}^k \omega^{i-j} B(f^i)(t), \quad \text{for } t \in S \text{ and } j \in [k].$$

We then have

$$\langle g, M(f) \rangle_{S \times [k]} = \frac{1}{k^2} \left\langle \sum_i \omega^i g^i, B \left(\sum_j \omega^j f^j \right) \right\rangle_S$$

where one factor of $\frac{1}{k}$ comes from our normalization of the inner product. This implies

$$|\langle g, M(f) \rangle_{S \times [k]}| \leq \|B\|_{L_\infty \rightarrow L_1} \left\| \frac{1}{k} \sum_{i=1}^k \omega^i g^i \right\|_{L_\infty} \left\| \frac{1}{k} \sum_{j=1}^k \omega^j f^j \right\|_{L_\infty}. \quad (8)$$

If $f, g \in C(S \times [k])$ are the $[0, 1]$ -valued functions that attain the cut norm of M , then by (8)

$$\|M\|_{\text{cut}} \leq \left(\frac{1}{\pi^2} + \epsilon \right) \|B\|_{L_\infty \rightarrow L_1},$$

where we used Lemma 17 to bound $\left\| \frac{1}{k} \sum_{i=1}^k \omega^i g^i \right\|_{L_\infty}$.

Let $u, v \in C(S)$ with $\|u\|_{L_2} = \|v\|_{L_2} = 1$ be such that $\|B\|_{L_2 \rightarrow L_2} = \langle v, B(u) \rangle_S$. Now define $f(u), g(v) \in C(S \times [k])$ as $f(u)(s, i) := \omega^{-i} u(s)$ and $g(v)(s, i) := \omega^{-i} v(s)$, which also have L_2 -norm equal to 1. We then see

$$\|M\|_{L_2 \rightarrow L_2} \geq \langle g(v), M(f(u)) \rangle_{S \times [k]} = \langle v, B(u) \rangle_S = \|B\|_{L_2 \rightarrow L_2}.$$

The combination of these observations completes the first part of the proof. Now assume B is transitive covariant with respect to Γ , so $B(f^\pi)(\pi^{-1}(s)) = B(f)(s)$ for all $s \in S$ and $\pi \in \Gamma$. Define a new group Γ' as the cartesian product $\Gamma' = \Gamma \times \mathbb{Z}_k$. For $(\pi, m) \in \Gamma'$ define the action $(\pi, m) : S \times [k] \rightarrow S \times [k]$ as $(\pi, m)(s, i) = (\pi(s), i + m)$. By entering $f^{(\pi, m)}$ into the definition of M it follows that $M^{(\pi, m)} = M$, so M is transitive covariant with respect to Γ' , completing the proof. \blacktriangleleft

► **Lemma 17.** *Let $\epsilon > 0$, then there exists a $k_0 \in \mathbb{N}$ such that for all $k \geq k_0$ and $x \in [0, 1]^k$ we have*

$$\left| \frac{1}{k} \sum_{j=1}^k e^{2\pi i j/k} x_j \right| \leq \frac{1}{\pi} + \epsilon.$$

Proof. First let k_0 be arbitrary, to be determined later and $k \geq k_0$. Define $y \in [-1, 1]^k$ as $y_i = 2x_i - 1$, then

$$\left| \frac{1}{k} \sum_{j=1}^k e^{2\pi i j/k} x_j \right| = \frac{1}{2} \left| \frac{1}{k} \sum_{j=1}^k e^{2\pi i j/k} y_j \right| = \frac{1}{2} e^{2\pi i \phi} \frac{1}{k} \sum_{j=1}^k e^{2\pi i j/k} y_j.$$

In the first equality we used that $\sum_{j=1}^k e^{2\pi i j/k} = 0$. In the second equality we used that there exists a ϕ such that the full expression becomes real and positive. Since $e^{i\theta} = \cos(\theta) + i \sin(\theta)$ and the full expression is real, we know the sin component vanishes and therefore

$$\frac{1}{2} \frac{1}{k} \sum_{j=1}^k e^{2\pi i(\phi + j/k)} y_j = \frac{1}{2} \frac{1}{k} \sum_{j=1}^k \cos(2\pi(\phi + j/k)) y_j.$$

Now note that $\cos(2\pi(\phi + j/k)) y_j \leq |\cos(2\pi(\phi + j/k))|$ and hence

$$\frac{1}{2} \frac{1}{k} \sum_{j=1}^k |\cos(2\pi(\phi + j/k))| \xrightarrow{k \rightarrow \infty} \frac{1}{2} \int_0^1 |\cos(2\pi(\phi + x))| dx = \frac{1}{\pi}.$$

This completes the proof. \blacktriangleleft

4.2 Non-commutative case

In the non-commutative case we show optimality of Theorem 6. By Lemma 2, the factor π^2 between the cut-norm and $S_\infty \rightarrow S_1$ -norm is also optimal. In contrast with the commutative case, our work leaves the optimality of the combined inequality in Corollary 7 as an open problem. Straightforward analogues of the techniques employed in Lemma 16 did not follow through in the non-commutative case.

► **Proposition 18.** *For any $\epsilon > 0$, there exists a positive integer n and an irreducibly covariant superoperator $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ such that $\|\Phi\|_{S_2 \rightarrow S_2} \geq (2 - \epsilon)\|\Phi\|_{S_\infty \rightarrow S_1}$.*

One of the forms of the non-commutative Grothendieck inequality, equivalent to Theorem 8, is the following [29]. Let $\Phi : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ be a linear map and $x_i, y_j \in M_n(\mathbb{C})$ finite sets of matrices. Then,

$$\left| \sum_i \langle x_i, \Phi(y_i) \rangle \right| \leq K'_G \|\Phi\|_{S_\infty \rightarrow S_1} \left(\frac{\|\sum_i x_i^* x_i\| + \|\sum_i x_i x_i^*\|}{2} \cdot \frac{\|\sum_i y_i^* y_i\| + \|\sum_i y_i y_i^*\|}{2} \right)^{1/2} \quad (9)$$

where $K'_G \leq 2$ and the norms on the right hand side are operator norms $\|\cdot\|_{S_\infty}$. To show tightness, i.e. $K'_G \geq 2$, Haagerup and Itoh [16] (see [29] for a survey) gave an explicit family of operators for which (9) gives a lower bound of K'_G approaching 2. We will show that slight modifications of these operators are irreducibly covariant, which proves Proposition 18. It is instructive to repeat their construction. The proof uses techniques familiar in the context of the antisymmetric Fock space, but our proof is self contained.

► **Lemma 19** ([16]). *For each $n \in \mathbb{N}$ there exists a $d \in \mathbb{N}$ and a linear map $\Phi : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$ with sets of matrices $\{x_i\}, \{y_i\}$ such that (9) yields $K'_G \geq (2n + 1)/(n + 1)$.*

Proof. Let $H = \mathbb{C}^{2n+1}$ and consider the antisymmetric k -fold tensor product $H^{\wedge k}$ which is a linear subspace of the k -fold tensor product $H^{\otimes k}$. A basis of $H^{\wedge k}$ is formed by vectors $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$ with $i_1 < \cdots < i_k$ where the e_i are standard basis vectors of H . Here \wedge is the wedge product or exterior product, which has the property $x \wedge y = -y \wedge x$ and is given by $x \wedge y = x \otimes y - y \otimes x$, for $x, y \in H$. We will consider $k = n$ and $k = n + 1$ so that the dimension of $H^{\wedge k}$ is $d = \binom{2n+1}{k}$ for both $k = n$ and $k = n + 1$.

For $1 \leq i \leq (2n + 1)$, define $c_i : H^{\wedge n} \rightarrow H^{\wedge(n+1)}$ as $c_i(x) := e_i \wedge x$, which physicists call the fermionic creation operator. Its adjoint $c_i^* : H^{\wedge(n+1)} \rightarrow H^{\wedge n}$ is known as the annihilation operator. By the antisymmetric property, $c_i(x) = 0$ whenever e_i was present in x , i.e., when $x = e_i \wedge x'$. The operator $c_i c_i^*$, also known as the number operator, is a projector onto the space spanned by basis vectors in which e_i is present. The operator $c_i^* c_i$ is a projector onto the space where e_i is *not* present. Since there are always $(n + 1)$ vectors present in $H^{\wedge(n+1)}$ and $(n + 1)$ vectors *not* present in $H^{\wedge n}$, we have

$$\sum_{i=1}^{2n+1} c_i c_i^* = (n + 1) \text{Id}_{H^{\wedge(n+1)}} \quad \text{and} \quad \sum_{i=1}^{2n+1} c_i^* c_i = (n + 1) \text{Id}_{H^{\wedge n}}.$$

We will now argue that

$$\langle c_i, c_j \rangle := \frac{1}{d} \text{Tr}(c_i^* c_j) = \delta_{i,j} \frac{n + 1}{2n + 1}, \quad (10)$$

$$\left\| \sum_{i=1}^{2n+1} \alpha_i c_i \right\|_{S_1} = \|\alpha\|_{L_2} \frac{n + 1}{\sqrt{2n + 1}} \quad \text{for } \alpha \in \mathbb{C}^{2n+1}. \quad (11)$$

The $\delta_{i,j}$ in (10) follows because $\langle x, c_i^* c_j x \rangle = 0$ for any $x = e_{k_1} \wedge \dots \wedge e_{k_n}$ when $i \neq j$. The factor $\frac{n+1}{2n+1}$ follows by taking the trace of one of the sums above and noting that by symmetry in i , every term of the sum must have the same trace. To prove (11), first note that for any unitary $U \in U(2n+1)$ we have

$$U^{\otimes(n+1)} \cdot c_i \cdot (U^{\otimes n})^{-1} = \sum_j U_{ji} c_j, \quad (12)$$

which can be shown by proving it for all basis states:

$$\begin{aligned} U^{\otimes(n+1)} c_i (U^{\otimes n})^{-1} (e_{k_1} \wedge \dots \wedge e_{k_n}) &= U^{\otimes(n+1)} c_i (U^{-1} e_{k_1} \wedge \dots \wedge U^{-1} e_{k_n}) \\ &= U^{\otimes(n+1)} (e_i \wedge U^{-1} e_{k_1} \wedge \dots \wedge U^{-1} e_{k_n}) \\ &= (U e_i \wedge e_{k_1} \wedge \dots \wedge e_{k_n}) \\ &= \left(\sum_j U_{ji} e_j \wedge e_{k_1} \wedge \dots \wedge e_{k_n} \right) \\ &= \sum_j U_{ji} c_j (e_{k_1} \wedge \dots \wedge e_{k_n}). \end{aligned}$$

The trace-norm is unitarily invariant, so (12) implies $\|c_i\|_{S_1} = \|\sum_j U_{ji} c_j\|_{S_1}$. Since $c_i^* c_i$ is a projector, we have $\sqrt{c_i^* c_i} = c_i^* c_i$ and hence $\|c_i\|_{S_1} = \frac{1}{d} \text{Tr}(c_i^* c_i)$. Now let $\alpha \in \mathbb{C}^{2n+1}$ with $\sum_i |\alpha_i|^2 = 1$, then there is a unitary $U \in U(2n+1)$ such that the i -th row of U is α . Note that $\|\alpha\|_{L_2} = 1/\sqrt{2n+1}$ since we use normalized L_2 -norms, which implies (11).

Since the dimensions of $H^{\wedge n}$ and $H^{\wedge(n+1)}$ are equal, we can identify the space of linear maps $L(H^{\wedge n}, H^{\wedge(n+1)})$ with $M_d(\mathbb{C})$ (by choosing bases for $H^{\wedge n}$ and $H^{\wedge(n+1)}$), and define the following operator $\Phi : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$,

$$\Phi(x) = \sum_{i=1}^{2n+1} \langle c_i, x \rangle c_i.$$

Consider (9) for Φ with $x_i = y_i = c_i$. For the left hand side, note that by (10) we have

$$\left| \sum_{j=1}^{2n+1} \langle c_j, \Phi(c_j) \rangle \right| = \left| \sum_{i,j=1}^{2n+1} \langle c_i, c_j \rangle \langle c_j, c_i \rangle \right| = \frac{(n+1)^2}{2n+1}.$$

For the right-hand side of (9), we require $\|\Phi\|_{S_\infty \rightarrow S_1} = \sup_{\|x\|_{S_\infty}=1} \|\Phi(x)\|_{S_1}$. For any $x \in M_d(\mathbb{C})$, define $v^{(x)} \in \mathbb{C}^{2n+1}$ as $v_i^{(x)} = \langle c_i, x \rangle$. Note that $\|v\|_{L_2} = \sup_{\|\alpha\|_{L_2}=1} |\langle v, \alpha \rangle|$. First apply (11) to obtain

$$\|\Phi(x)\|_{S_1} = \left\| \sum_{i=1}^{2n+1} \langle c_i, x \rangle c_i \right\|_{S_1} = \|v^{(x)}\|_{L_2} \frac{n+1}{\sqrt{2n+1}} = \sup_{\|\alpha\|_{L_2}=1} |\langle v^{(x)}, \alpha \rangle| \frac{n+1}{\sqrt{2n+1}}.$$

Using (11) again, we compute $\sup_{\|x\|_{S_\infty}=1} |\langle v^{(x)}, \alpha \rangle|$ for arbitrary α with $\|\alpha\|_{L_2} = 1$,

$$\sup_{\|x\|_{S_\infty}=1} |\langle v^{(x)}, \alpha \rangle| = \sup_{\|x\|_{S_\infty}=1} \frac{1}{2n+1} \left| \langle x, \sum_i \alpha_i c_i \rangle \right| = \frac{1}{2n+1} \left\| \sum_i \alpha_i c_i \right\|_{S_1} = \frac{n+1}{(2n+1)\sqrt{2n+1}}.$$

We obtain $\|\Phi\|_{S_\infty \rightarrow S_1} = (n+1)^2 / (2n+1)^2$. Now (9) yields $\frac{(n+1)^2}{2n+1} \leq K'_G \frac{(n+1)^2}{(2n+1)^2} \cdot (n+1)$ and therefore $\frac{2n+1}{n+1} \leq K'_G$. \blacktriangleleft

We use the following fact from [12, Theorem 19.14], about the representations of the odd dimensional complex special orthogonal groups on wedge products of *complex* vector spaces.

5:18 Quasirandom Quantum Channels

► **Lemma 20.** *Let $n, k \in \mathbb{N}$, $N := 2n + 1$ and let $R_k : \text{SO}(N, \mathbb{C}) \rightarrow \text{GL}((\mathbb{C}^N)^{\wedge k})$ be given by $A \mapsto A^{\otimes k}$. This representation is irreducible.*

Below, we actually need that the *real* special orthogonal group $\text{SO}(N, \mathbb{R})$ acts irreducibly on the same anti-symmetric space. Fortunately, this is implied by Lemma 20; see [12, pp. 439]. We will also use the fact that R_k and R_{N-k} are *unitarily* equivalent to each other. This is the content of the following proposition [32, Proposition IX.10.4].

► **Proposition 21.** *For positive integer n and $N = 2n + 1$ and $k \in \{1, \dots, N\}$, let R_k be the representation as in lemma 20. Then, there exists an isometry $V_k : (\mathbb{C}^N)^{\wedge k} \rightarrow (\mathbb{C}^N)^{\wedge(N-k)}$ such that*

$$V_k R_k(A) = R_{N-k}(A) V_k, \quad \forall A \in \text{SO}(N, \mathbb{R}).$$

of Proposition 18. Let d be the dimension of $(\mathbb{C}^N)^{\wedge n}$ and let $\Phi : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$ be as in the proof of Lemma 19. For each $k \in \mathbb{N}$, let $R_k : \text{SO}(N, \mathbb{R}) \rightarrow \text{GL}(H^{\wedge k})$ be the representation $A \mapsto A^{\otimes k}$, which is irreducible by Lemma 20. Define, for notational convenience, $\pi := R_{n+1}$ and $\rho := R_n$. We first show that for all $A \in \text{SO}(N, \mathbb{R})$, we have

$$\Phi(\pi(A)x\rho^*(A)) = \pi(A) \Phi(x) \rho^*(A). \quad (13)$$

For the left-hand side, note that

$$\begin{aligned} \Phi(\pi(A)x\rho^*(A)) &= \sum_i \langle c_i, \pi(A)x\rho^*(A) \rangle c_i \\ &= \sum_i \langle \pi(A)^* c_i \rho(A), x \rangle c_i \\ &= \sum_i \left\langle \sum_j A_{ij} c_j, x \right\rangle c_i \\ &= \sum_{ij} A_{ij} \langle c_j, x \rangle c_i, \end{aligned}$$

where we used (12) from the proof of Lemma 19 and noting that $\text{SO}(N, \mathbb{R}) \subset \text{U}(N)$ is a subgroup. Using (12) again for the right-hand side, we have

$$\begin{aligned} \pi(A) \Phi(x) \rho^*(A) &= \sum_i \langle c_i, x \rangle \pi(A) c_i \rho^*(A) \\ &= \sum_i \langle c_i, x \rangle \sum_j A_{ji} c_j \\ &= \sum_{ij} A_{ij} \langle c_j, x \rangle c_i. \end{aligned}$$

which proves (13).

Define a new superoperator $\Phi' : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$ by

$$\Phi'(x) = \Phi(xV^*)V,$$

where $V := V_{n+1}$ is the isometry as in Lemma 21 (we view V as a matrix in $M_d(\mathbb{C})$ by choosing basis). We first note that this Φ' might also be used in Lemma 19 to show that the non-commutative Grothendieck constant is 2, since Schatten-norms are unitarily invariant.

Hence, if we show that Φ' is irreducibly covariant, we are done. This follows from the following computation, where we use (13) and the fact that $V\pi(A) = \rho(A)V$ for all $A \in \text{SO}(N, \mathbb{R})$:

$$\begin{aligned} \Phi'(\pi(A)x\pi(A)^*) &= \Phi(\pi(A)x\pi(A)^*V^*)V \\ &= \Phi(\pi(A)xV^*\rho(A)^*)V \\ &\stackrel{(13)}{=} \pi(A)\Phi(xV^*)\rho(A)^*V \\ &= \pi(A)\Phi(xV^*)V\pi(A)^* \\ &= \pi(A)\Phi'(x)\pi^*(A), \end{aligned}$$

where the second-last line follows since $\rho(A)^* = V\pi(A)^*V^*$. Hence, Φ' is irreducibly covariant with respect to the irreducible representation π of $\text{SO}(N, \mathbb{R})$. ◀

References

- 1 Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In Klaus Jansen, Sanjeev Khanna, José D. P. Rolim, and Dana Ron, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 249–260, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.
- 2 Guillaume Aubrun. On almost randomizing channels with a short Kraus decomposition. *Comm. Math. Phys.*, 288(3):1103–1116, 2009. doi:10.1007/s00220-008-0695-y.
- 3 Avraham Ben-Aroya, Oded Schwartz, and Amnon Ta-Shma. Quantum expanders: Motivation and construction. *Theory of Computing*, 6(1):47–79, 2010. doi:10.4086/toc.2010.v006a003.
- 4 Béla Bollobás and Vladimir Nikiforov. Hermitian matrices and graphs: singular values and discrepancy. *Discrete Math.*, 285(1-3):17–32, 2004. doi:10.1016/j.disc.2004.05.006.
- 5 M. Braverman, K. Makarychev, Y. Makarychev, and A. Naor. The Grothendieck constant is strictly smaller than Krivine’s bound. *Forum Math. Pi*, 1:453–462, 2013. Preliminary version in FOCS’11. <https://arxiv.org/abs/1103.6161>.
- 6 Jop Briët. *Grothendieck inequalities, nonlocal games and optimization*. PhD thesis, Institute for Logic, Language and Computation, 2011.
- 7 Fan Chung and Ronald Graham. Sparse quasi-random graphs. *Combinatorica*, 22(2):217–244, 2002. Special issue: Paul Erdős and his mathematics. doi:10.1007/s004930200010.
- 8 Fan R. K. Chung, Ronald L. Graham, and Richard M. Wilson. Quasi-random graphs. *Combinatorica*, 9(4):345–362, 1989. doi:10.1007/BF02125347.
- 9 David Conlon and Yufei Zhao. Quasirandom Cayley graphs. *Discrete Anal.*, pages Paper No. 6, 14, 2017.
- 10 Tom Cooney, Marius Junge, Carlos Palazuelos, and David Pérez-García. Rank-one quantum games. *computational complexity*, 24(1):133–196, 2015.
- 11 A. Davie. Lower bound for K_G . Unpublished, 1984.
- 12 William Fulton and Joe Harris. *Representation theory: a first course*, volume 129. Springer Science & Business Media, 2013.
- 13 A. Grothendieck. Résumé de la théorie métrique des produits tensoriels topologiques. *Bol. Soc. Mat. São Paulo*, 8:1–79, 1953.
- 14 Uffe Haagerup. The Grothendieck inequality for bilinear forms on C^* -algebras. *Adv. in Math.*, 56(2):93–116, 1985. doi:10.1016/0001-8708(85)90026-X.
- 15 Uffe Haagerup. A new upper bound for the complex Grothendieck constant. *Israel J. Math.*, 60(2):199–224, 1987. doi:10.1007/BF02790792.
- 16 Uffe Haagerup and Takashi Itoh. Grothendieck type norms for bilinear forms on C^* -algebras. *J. Operator Theory*, 34(2):263–283, 1995.
- 17 Aram Wettroth Harrow. Quantum expanders from any classical cayley graph expander. *Quantum Information & Computation*, 8(8):715–721, 2008. URL: <http://www.rintonpress.com/xxqic8/qic-8-89/0715-0721.pdf>.

- 18 M. B. Hastings. Random unitaries give quantum expanders. *Phys. Rev. A* (3), 76(3):032315, 11, 2007. doi:10.1103/PhysRevA.76.032315.
- 19 Matthew B Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255, 2009.
- 20 Matthew B. Hastings and Aram Wettroth Harrow. Classical and quantum tensor product expanders. *Quantum Information & Computation*, 9(3):336–360, 2009. URL: <http://www.rintonpress.com/xxqic9/qic-9-34/0336-0360.pdf>.
- 21 Alexander S Holevo. Remarks on the classical capacity of quantum channel. *arXiv preprint quant-ph/0212025*, 2002.
- 22 Alexander S. Holevo. The additivity problem in quantum information theory. In *International Congress of Mathematicians. Vol. III*, pages 999–1018. Eur. Math. Soc., Zürich, 2006.
- 23 Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43:439–561, 2006.
- 24 Yoshiharu Kohayakawa, Vojtěch Rödl, and Mathias Schacht. Discrepancy and eigenvalues of Cayley graphs. *Czechoslovak Math. J.*, 66(141)(3):941–954, 2016. doi:10.1007/s10587-016-0302-x.
- 25 M. Krivelevich and B. Sudakov. Pseudo-random graphs. In *More sets, graphs and numbers*, volume 15 of *Bolyai Soc. Math. Stud.*, pages 199–262. Springer, Berlin, 2006. doi:10.1007/978-3-540-32439-3_10.
- 26 Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
- 27 Grigorii Aleksandrovich Margulis. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problems of Information Transmission*, 24(1):39–46, 1988.
- 28 Assaf Naor, Oded Regev, and Thomas Vidick. Efficient rounding for the noncommutative Grothendieck inequality. *Theory Comput.*, 10(11):257–295, 2014. Earlier version in STOC’13.
- 29 Gilles Pisier. Grothendieck’s theorem, past and present. *Bull. Amer. Math. Soc. (N.S.)*, 49(2):237–323, 2012. doi:10.1090/S0273-0979-2011-01348-9.
- 30 J. Reeds. A new lower bound on the real Grothendieck constant. Manuscript (<http://www.dtc.umn.edu/~reedsj/bound2.dvi>), 1991.
- 31 Oded Regev and Thomas Vidick. Quantum XOR games. *ACM Trans. Comput. Theory*, 7(4):Art. 15, 43, 2015. doi:10.1145/2799560.
- 32 Barry Simon. *Representations of finite and compact groups*. Number 10. American Mathematical Soc., 1996.
- 33 Andrew Thomason. Pseudorandom graphs. In *Random graphs ’85 (Poznań, 1985)*, volume 144 of *North-Holland Math. Stud.*, pages 307–331. North-Holland, Amsterdam, 1987.
- 34 Andrew Thomason. Random graphs, strongly regular graphs and pseudorandom graphs. In *Surveys in combinatorics 1987 (New Cross, 1987)*, volume 123 of *London Math. Soc. Lecture Note Ser.*, pages 173–195. Cambridge Univ. Press, Cambridge, 1987.