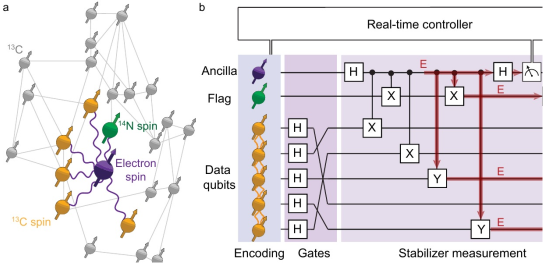
arXiv:2408.10323
arXiv:2603.19901

Felix Huber, U. Gdańsk

SDP bounds on quantum codes

joint works with:
Gerard Munné, Jagiellonian U. Gdaśnk
Andrew Nemec, Texas A & M

Quantum computing



Blatt laboratory, Abobeih et al. 2022

- Information is physical (atoms, photons, electric charges . . .)
- Quantum physics is noisy / quantum information is fragile
- Quantum information cannot be treated classically
  (state collapse, no-cloning, continuity of states & errors)

. . . we need a way to protect quantum states from noise

Quantum error-correcting codes

- A quantum code encodes quantum information (e.g. a qubit) redundantly. The encoded state can be recovered after being affected by noise.
- Quantum codes form the backbone of quantum computers: allow for fault-tolerant processing of quantum information.

Example

$$\alpha |0\rangle + \beta |1\rangle \quad \mapsto \quad \alpha |000\rangle + \beta |111\rangle$$

- circumvents no-cloning.
- discretization of errors.
  (detect single flip by measurement of ZZI, ZIZ, IZZ)
- syndrome measurement collapses state onto code subspace.

Conditions for quantum error correction

- Code is a subspace $(\mathbb{C}^2)^{\otimes n}$, represented by a projector Π.
- Noise acts as a quantum channel on a state ϱ

$$\mathcal{N}(\varrho) = \sum_{E_\mu \in N} E_\mu(\varrho)E_\mu^\dagger$$

where $\sum_\mu E_\mu^\dagger E_\mu = \mathbb{1}$.

Conditions for quantum error correction

- Code is a subspace $(\mathbb{C}^2)^{\otimes n}$, represented by a projector Π.
- Noise acts as a quantum channel on a state ϱ

$$\mathcal{N}(\varrho) = \sum_{E_\mu \in N} E_\mu(\varrho) E_\mu^\dagger$$

  where $\sum_\mu E_\mu^\dagger E_\mu = \mathbb{1}$.
- Knill-Laflamme conditions: $\mathcal{N}$ can be corrected on Π, iff

$$\Pi E_\mu^\dagger E_\nu \Pi = c_{\mu\nu} \Pi$$

  for all $E_\mu, E_\nu \in N$.

Conditions for quantum error correction

- Code is a subspace $(\mathbb{C}^2)^{\otimes n}$, represented by a projector Π.
- Noise acts as a quantum channel on a state ϱ

$$\mathcal{N}(\varrho) = \sum_{E_\mu \in N} E_\mu(\varrho) E_\mu^\dagger$$

  where $\sum_\mu E_\mu^\dagger E_\mu = \mathbb{1}$.
- Knill-Laflamme conditions: $\mathcal{N}$ can be corrected on Π, iff

$$\Pi E_\mu^\dagger E_\nu \Pi = c_{\mu\nu} \Pi$$

  for all $E_\mu, E_\nu \in N$.
- Think of this as a type of sphere packing: equivalent to

$$\langle\phi| E_\mu E_\nu |\psi\rangle = c_{\mu\nu} \langle\phi|\psi\rangle$$

  for all $E_\mu, E_\nu \in N$. and $|\phi\rangle, |\psi\rangle \in \mathrm{ran}(\Pi)$.

Error basis

Our goal: correct all tensor-product errors of at most weight δ.

The *Pauli matrices* form a basis for complex 2×2 matrices.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Tensor-product basis
  $\mathcal{E}_n = \left\{ E_\alpha = e_{\alpha_1} \otimes \ldots \otimes e_n \,|\, e_i \in \{I, X, Y, Z\} \right\}$
- Weight $\mathrm{wt}(E_\alpha)$ is the number of coordinates where E_α acts non-trivially. E.g. $\mathrm{wt}(IXIZZ) = 3$

Fundamental question in (quantum) coding theory

A $(\!(n, K, \delta)\!)$ quantum code is then a projector Π on $(\mathbb{C}^2)^{\otimes n}$ of rank K, such that

$$\Pi E_a^\dagger E_b \Pi = c_{ab} \Pi$$

for all $E_a, E_b \in \mathcal{E}_n$ with $\mathrm{wt}(E_a^\dagger E_b) < \delta$.

Fundamental question in (quantum) coding theory

A $((n, K, \delta))$ quantum code is then a projector Π on $(\mathbb{C}^2)^{\otimes n}$ of rank K, such that

$$\Pi E_a^\dagger E_b \Pi = c_{ab} \Pi$$

for all $E_a, E_b \in \mathcal{E}_n$ with $\mathrm{wt}(E_a^\dagger E_b) < \delta$.

- A code is *pure*, if $c_{ab} \propto \mathrm{tr}(E_a E_b)$ for $1 < \mathrm{wt}(E_a^\dagger E_b) < \delta$. (maximally mixed marginals)
- A code is *self-dual* if $K = 1$ and the code is pure.

Fundamental question in (quantum) coding theory

A $(\!(n, K, \delta)\!)$ quantum code is then a projector Π on $(\mathbb{C}^2)^{\otimes n}$ of rank K, such that

$$\Pi E_a^\dagger E_b \Pi = c_{ab} \Pi$$

for all $E_a, E_b \in \mathcal{E}_n$ with $\mathrm{wt}(E_a^\dagger E_b) < \delta$.

- A code is *pure*, if $c_{ab} \propto \mathrm{tr}(E_a E_b)$ for $1 < \mathrm{wt}(E_a^\dagger E_b) < \delta$. (maximally mixed marginals)
- A code is *self-dual* if $K = 1$ and the code is pure.

Question

For a given block length n and distance d, what is the maximal size K for quantum codes $(\!(n, K, d)\!)_D$ on n quDits?

- Linear programming bounds
- Analytical bounds (q. Singleton)
- SDP bounds. . . ?

Contributions

Result (A)

A quantum code with parameters $(\!(n, K, \delta)\!)_2$ *exists if and only if a certain SDP hierarchy is feasible at every level.*

Result (B)

The Lovász number bounds the existence of self-dual quantum codes. A symmetrization recovers the quantum Delsarte bound.

Result (C)

There a symmetry-reduced SDP of size $O(n^4)$ *based on the Terwilliger algebra. Codes with parameters* $(\!(7, 1, 4)\!)_2$, $(\!(8, 9, 3)\!)_2$, $(\!(10, 5, 4)\!)_2$,... *do not exist.*

An attempt: Stabilizer codes

- Stabilizer group $S = \langle g_1, \ldots, g_{n-k} \rangle$, $-\mathbb{1} \notin S$, g_i generators.
- Projector onto the code subspace

$$\Pi = \frac{1}{2^{n-k}} \sum_{i=1}^{n-k} (\mathbb{1} + g_i) = \frac{1}{2^{n-k}} \sum_{s \in S} s$$

- Simplest case: graph states $g_i = X_i \bigotimes_{j \in N(i)} Z_j$
- Commutative group: $[g_i, g_j] = 0$ for all g_i, g_j.

An attempt: Stabilizer codes

- Stabilizer group $S = \langle g_1, \ldots, g_{n-k} \rangle$, $-\mathbb{1} \notin S$, g_i generators.
- Projector onto the code subspace

$$\Pi = \frac{1}{2^{n-k}} \sum_{i=1}^{n-k} (\mathbb{1} + g_i) = \frac{1}{2^{n-k}} \sum_{s \in S} s$$

- Simplest case: graph states $g_i = X_i \bigotimes_{j \in N(i)} Z_j$
- Commutative group: $[g_i, g_j] = 0$ for all g_i, g_j.

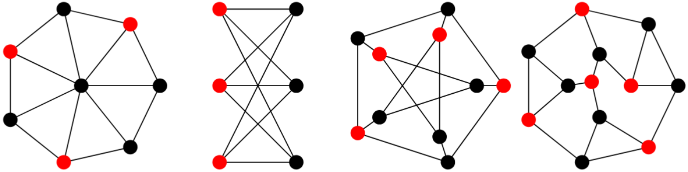
Is there a stabilizer code with $K = 1$ with distance δ (i.e. a $\delta - 1$-uniform graph state)?

- Need maximal commuting subgroup of Pauli group.
- If $E_a E_b = -E_b E_a$, then not both can be in S.
- If $1 < \mathrm{wt}(E_a) < \delta$, then E_a is not in S.

Independence number

Independence number (maximum size of disconnected set)

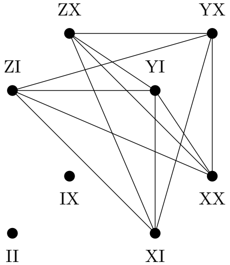
$$\alpha \quad = \quad \max_{W \subset V} \quad |W| \quad \text{s.t.} \quad (i,j) \notin E \quad \text{for all} \quad i,j \in W$$



- It is known that $\alpha(G) \leq \vartheta(G)$
- ϑ is efficiently computable via SDP, α is not.

Lovász bound for stabilizer codes

- Index by "Pauli cube":
  $\mathcal{E}_{n,\delta} = \{E_a \in \mathcal{E}_n \mid \mathrm{wt}(E_a) \geq \delta\}$
- Confusability graph:
  $a \sim b$ if $E_a E_b = -E_b E_a$.
- If a self-dual stabilizer code with distance δ exists, then there is an independent set of size $\alpha = 2^n$
- As a consequence: $2^n \leq 1 + \vartheta(G)$.



Lovász bound for all quantum codes

Key idea (c.f. uncertainty relations)

- Write $\langle E_a \rangle$ for $\mathrm{tr}(E_a \varrho)$ with $\varrho = \Pi/K$.
- Construct moment matrix $\Gamma_{ab} = \langle E_a^\dagger \rangle \langle E_b \rangle \langle E_a E_b^\dagger \rangle$ for $E_\alpha \in \mathcal{E}_n$,

$$\Gamma = \begin{array}{c c} & \begin{array}{cccc} \mathbb{1} & \langle E_1 \rangle E_1^\dagger & \cdots & \langle E_N \rangle E_N^\dagger \end{array} \\ \begin{array}{c} \mathbb{1} \\ \langle E_1 \rangle E_1^\dagger \\ \vdots \\ \langle E_N \rangle E_N^\dagger \end{array} & \begin{bmatrix} 1 & \Gamma_{01} & \cdots & \Gamma_{0N} \\ & \Gamma_{11} & \dots & \Gamma_{1N} \\ & & \ddots & \vdots \\ & & & \Gamma_{NN} \end{bmatrix} \end{array} \succeq 0\,,$$

- For two qubits, one would index with $\langle II \rangle II, \langle IX \rangle IX, \dots, \langle YZ \rangle YZ, \langle ZZ \rangle ZZ$.

Lovász bound for all quantum codes (II)

$$\Gamma \quad = \quad \begin{array}{c c} & \begin{array}{cccc} \mathbb{1} & \langle E_1\rangle E_1^\dagger & \cdots & \langle E_N\rangle E_N^\dagger \end{array} \\ \begin{array}{c} \mathbb{1} \\ \langle E_1^\dagger\rangle E_1 \\ \vdots \\ \langle E_N^\dagger\rangle E_N \end{array} & \begin{bmatrix} 1 & \Gamma_{01} & \cdots & \Gamma_{0N} \\ & \Gamma_{11} & \dots & \Gamma_{1N} \\ & & \ddots & \vdots \\ & & & \Gamma_{NN} \end{bmatrix} \end{array} \succeq 0\,,$$

$$N = 4^n - 1$$

Consider $K = 1$. Then:

- $\Gamma_{00} = \langle \mathbb{1} \rangle = 1$
- $\Gamma_{ab} = \Gamma_{a0} = \langle E_a \rangle^2$
- $\sum_{a=0}^N \Gamma_{aa} = 2^n$, corresponding to $\operatorname{tr}(\varrho^2) = 1$.

Note: If Γ is a valid moment matrix, then so is $(\Gamma + \Gamma^T)/2$.
Impose extra condition:

- $\Gamma_{ab} = 0 \quad$ if $\quad E_a E_b = -E_b E_a$.

Lovász bound for all quantum codes (III)

This corresponds to a point in the theta body

$$\mathrm{TH}(G) = \left\{ \mathrm{diag}(M) \,\middle|\, \begin{pmatrix} 1 & x^T \\ x & M \end{pmatrix} \succeq 0 \,, x_a = M_{aa} \; \forall a \,, M_{ab} = 0 \text{ if } a \sim b \right\}.$$

where the *quantum confusability graph* has $\mathcal{E}_n \backslash \mathbb{1}$ as vertices and

$$\begin{aligned} a \sim b \quad \text{if} \quad & \begin{cases} 0 < \mathrm{wt}(E_a E_b) < \delta \quad \text{or} \\ E_a E_b = -E_b E_a \end{cases} \\ a \sim a \quad \text{if} \quad & \quad\; 0 < \mathrm{wt}(E_a) < \delta \end{aligned}$$

Lovász bound for all quantum codes (III)

This corresponds to a point in the theta body

$$\mathrm{TH}(G) = \left\{ \mathrm{diag}(M) \,\middle|\, \begin{pmatrix} 1 & x^T \\ x & M \end{pmatrix} \succeq 0\,, x_a = M_{aa}\ \forall a\,, M_{ab} = 0 \text{ if } a \sim b \right\}.$$

where the *quantum confusability graph* has $\mathcal{E}_n \backslash \mathbb{1}$ as vertices and

$$\begin{array}{lll} a \sim b & \text{if} & \begin{cases} 0 < \mathrm{wt}(E_a E_b) < \delta & \text{or} \\ E_a E_b = -E_b E_a \end{cases} \\ a \sim a & \text{if} & \quad 0 < \mathrm{wt}(E_a) < \delta \end{array}$$

Lovász bound on self-dual quantum codes

If a $((n, 1, \delta))$ code exists, then
b) $\mathrm{TH}(G)$ contains an element with $2^n = 1 + \sum_{a=1}^{N} M_{aa}$ and
a) $2^n \leq \vartheta(G) + 1$

Symmetry-reduction

This scales badly: Pauli cube has 4^n elements!

- Average Γ over all row and column permutations which keep triples of weights $i = \mathrm{wt}(E_a)$, $j = \mathrm{wt}(E_b)$, and $k = \mathrm{wt}(E_a^\dagger E_b)$ invariant.
- The resulting matrix

$$\tilde{\Gamma} = \sum_{\pi \in \mathrm{Aut}_0} \pi \Gamma \pi^{-1}$$

  can be block-diagonalized with the Terwilliger algebra.
- This results in an SDP of size $O(n^4)$.

Gijswijt, Schrijver, Tanaka, J. Comb. Theory, A 113, 8, 2006, 1719-1731

$\longrightarrow$ Efficiently computable Lovasz bounds!

Complete SDP hierarchy for code existence

1. Formulate the Knill-Laflamme conditions $\Pi E_a E_b \Pi = c_{ab} \Pi$ as

$$K \sum_{\substack{E \in \mathcal{E}_n \\ \mathrm{wt}(E)=j}} \mathrm{tr}(E \varrho E^\dagger \varrho) = \sum_{\substack{E \in \mathcal{E}_n \\ \mathrm{wt}(E)=j}} \mathrm{tr}(E \varrho) \, \mathrm{tr}(E^\dagger \varrho)$$

   for $j < \delta$. (In short: $KB_j = A_j$ for $j < \delta$)

Complete SDP hierarchy for code existence

1. Formulate the Knill-Laflamme conditions $\Pi E_a E_b \Pi = c_{ab}\Pi$ as

$$K \sum_{\substack{E\in\mathcal{E}_n\\ \mathrm{wt}(E)=j}} \mathrm{tr}(E\varrho E^\dagger \varrho) = \sum_{\substack{E\in\mathcal{E}_n\\ \mathrm{wt}(E)=j}} \mathrm{tr}(E\varrho)\,\mathrm{tr}(E^\dagger \varrho)$$

   for $j < \delta$. (In short: $KB_j = A_j$ for $j < \delta$)

2. State polynomial optimization: Consider non-commutative letters $\{x_i\}$. Form words $w = x_{j_1} \dots x_{j_k}$. Associate expectations $\langle w \rangle$ behaving as $v\langle w\rangle = \langle w\rangle v$ and $\langle v\langle w\rangle\rangle = \langle v\rangle\langle w\rangle$. State monomials have the form $w_{i_1}\langle w_{i_2}\rangle \dots \langle w_{i_m}\rangle$. Use Positivstellensatz for positive state polynomials / corresponding moment hierarchy. (Note: Γ from above is an intermediate level!) Klep et al. 2023

- This recovers RHS in above condition. LHS. . . ?

Complete SDP hierarchy (II)

3. Use the quantum MacWilliams identity

$$B(x,y) = A\Big(\frac{x+3y}{2}, \frac{x-y}{2}\Big)\,,$$

where $A(x,y) = \sum_{j=0}^{n} A_j(\Pi)x^{n-j}y^j$ and likewise for $B(x,y)$.

4. Hierarchy is dimension-free: restrict to qubits by characterization of quasi-Clifford algebras with generator relations $\alpha_i\alpha_j = (-1)^{\chi_{ij}}\alpha_j\alpha_i$, $\chi_{ij} \in \{0,1\}$ and $\alpha_i^2 = 1$.

Gastineau-Hills 1982

5. Impose that $\varrho = \Pi/K$: use swap-like constraints,

$$\mathrm{tr}(\varrho^m) = \mathrm{tr}\left((1,2,\dots,m)\varrho^{\otimes m}\right) = \frac{1}{K^{m-1}}$$

expanded in Pauli matrices.

Applications

- Averaging the Lovász bound over distance-preserving automorphism leads to the quantum Delsarte bound,

$$\begin{aligned} \eta = \max \quad & \sum_{j=0}^{n} A_j \,, \\ \text{subject to} \quad & A_0 = 1\,, \quad A_j \geq 0 \ \text{ with equality for } \ 1 < j < \delta\,, \\ & \sum_{i=0}^{n} K_j(i) A_i \geq 0 \quad \text{for } j = 0, \ldots, n\,. \end{aligned}$$

  If $\eta < 2^n$, then code does not exist.
- Hierarchy with $O(n^4)$ scaling: Average over distance and zero-preserving autormorphisms. Symmetry-reduce using the 4-ary Terwilliger algebra. Gijswijt, Schrijver, Tanaka 2006

Table

n \ δ	2	3	4	5	6	7	8
6	16	2^{α}	1	0	0	0	0
7	24 - 26	2 - 3	0	0	0	0	0
8	64	**8**(9)	1	0	0	0	0
9	100 - 112	12 - 13	1	0	0	0	0
10	256	24	**4**(5)	0	0	0	0
11	416 - 460	32 - $\mathbf{42}^{\alpha}$(53)	4 - 7	2	0	0	0
12	1024	64 - 89	16 - 20	2	1	0	0
13	1586 - 1877	128 - 204	20 - 40	2 - 3	**0**(1)	0	0
14	4096	256 - $\mathbf{295}^{\alpha}$(324)	64 - 102	4 - $\mathbf{9}^{\alpha}$(10)	1	0	0
15	6476 - 7606	512 - 580	64 - $\mathbf{138}^{\alpha}$(150)	8 - 18	1	0	0
16	16384	1024 - **1170**(1260)	128 - 256	32 - 42	4 - 6	0	0
17	26333 - 30720	2048 - 2145	512	32 - $\mathbf{59}^{\alpha}$(71)	4 - 8	2	0
18	65536	2048 - 4096	512 - **921**(986)	64 - 113	16 - 22	2	1
19	106762 - 123790	4096 - $\mathbf{7420}^{\alpha}$(8426)	1024 - 1804	128 - **249**(276)	32 - 47	2 - 3	**0**(1)

Figure: Lower - upper (old bound). α: code must be impure.

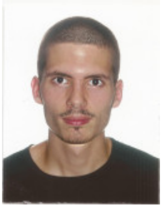
For pure codes the bounds strenghten to:

$$((6,1,3))_2, ((11,41,3))_2, ((14,290,3))_2, ((14,8,5))_2,$$
$$((15,135,4))_2, ((17,57,5))_2, ((19,7314,3))_2$$

Contributions

- Complete SDP hierarchies for bounds on quantum codes.
- Quantum analogues of the Lovász and Delsarte bounds.
- Numerically practical relaxations.
- Flexibility in applications, formally dimension-free: extensions to qudit codes & more general confusability graphs possible.

G. Munné, A. Nemec, FH, *SDP bounds on quantum codes*, `arXiv:2408.10323`
G. Munné, FH, *SDP bounds on quantum codes: rational certificates*, `arXiv:2603.19901`




Support: Foundation for Polish Science TEAM-NET POIR.04.04.00-00-17C1/18-00 (GM, FH) and QLCI (AN)