Upper Bounds on the Minimum Distance of Abelian Two-Block Group Algebra Quantum Codes

F. Arnault, P. Gaborit, **W. Rozendaal**, N. Saussay, G. Zémor

Journées C2, Pornichet - 31 March 2025

Abelian Two-Block Group Algebra codes

Two-Block quantum codes:

- $\mathbf{A}$ and $\mathbf{B}$ a pair of square commuting matrices
- CSS stabiliser code: $\mathbf{H}_X = [\mathbf{A}|\mathbf{B}]$, $\mathbf{H}_Z = [\mathbf{B}^\top| - \mathbf{A}^\top]$
- Orthogonality: $\mathbf{H}_X\mathbf{H}_Z^\top = \mathbf{AB} - \mathbf{BA} = \mathbf{0}$

Group algebra:

- Finite field F, finite abelian group G of order ℓ
- Group algebra $F[G]$: F-linear space of all formal sums $\sum_{g\in G} x_g g$ with $x_g \in F$
- Product formula: $xy = \sum_{g\in G} \left(\sum_{h\in G} x_h y_{h^{-1}g}\right) g$
- Permutation matrix $\mathbb{B}(g)$: $\mathbb{B}(g)_{i,j} = 1 \Leftrightarrow g_i = gg_j$

Abelian Two-Block Group Algebra codes

Abelian 2BGA codes: (Pryadko, Lin - 2023)

- $a = \sum_{g \in G} a_g g$ and $b = \sum_{g \in G} b_g g \in \mathbb{F}_2[G]$
- $\mathbf{A} = \sum_{g \in G} a_g \mathbb{B}(g)$ and $\mathbf{B} = \sum_{g \in G} b_g \mathbb{B}(g) \in \mathcal{M}_\ell(\mathbb{F}_2)$
- Commutativity: $\mathbf{AB} = \mathbf{BA}$ since $\mathbb{B}(g)\mathbb{B}(h) = \mathbb{B}(gh) = \mathbb{B}(hg) = \mathbb{B}(h)\mathbb{B}(g)$
- CSS stabiliser code: $\mathbf{H}_X = [\mathbf{A}|\mathbf{B}]$, $\mathbf{H}_Z = [\mathbf{B}^\top|\mathbf{A}^\top]$

Parameters of Abelian 2BGA codes:

- Length $n = 2\ell$
- Dimension $k = 2\ell - \operatorname{rank}\mathbf{H}_X - \operatorname{rank}\mathbf{H}_Z$, with $\operatorname{rank}\mathbf{H}_X = \operatorname{rank}\mathbf{H}_Z$
- Minimum distance $d = d_X = d_Z$

Generalised Bicycle codes

$G = C_\ell$ cyclic group of order ℓ

- $a, b \in \mathbb{F}_2[C_\ell] \simeq \mathbb{F}_2[x] \,/ < x^\ell - 1 >$
- $\mathbf{P}$ the cyclic permutation matrix describing the action of x

$$\mathbf{P} = \begin{pmatrix} 0 & \dots & 0 & 1 \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix}$$

- Circulant matrices $\mathbf{A} = a(\mathbf{P})$, $\mathbf{B} = b(\mathbf{P}) \in \mathcal{M}_\ell(\mathbb{F}_2)$
- Commutativity: $\mathbf{AB} = ab(\mathbf{P}) = ba(\mathbf{P}) = \mathbf{BA}$

Generalised Bicycle codes: (Kovalev, Pryadko - 2013)

- CSS stabiliser code: $\mathbf{H}_X = [\mathbf{A}|\mathbf{B}]$, $\mathbf{H}_Z = [\mathbf{B}^\top|\mathbf{A}^\top]$

Bivariate Bicycle codes

$G = C_r \times C_s$ **product of two cyclic groups, with** $\ell = rs$

- $a, b \in \mathbb{F}_2[C_r \times C_s] \simeq \mathbb{F}_2[x, y] \, / < x^r - 1, y^s - 1, xy - yx >$
- $\mathbf{X} = \mathbf{P}_r \otimes \mathbf{I}_s$ describes the action of x
- $\mathbf{Y} = \mathbf{I}_r \otimes \mathbf{P}_s$ describes the action of y
- $\mathbf{A} = a(\mathbf{X}, \mathbf{Y})$, $\mathbf{B} = b(\mathbf{X}, \mathbf{Y}) \in \mathcal{M}_\ell(\mathbb{F}_2)$
- Commutativity: $\mathbf{AB} = \mathbf{BA}$ since $\mathbf{XY} = \mathbf{YX}$

Bivariate Bicycle codes: (Bravyi, Cross, Gambetta, Maslov, Rall, Yoder - 2024)

- $\mathbf{A} = \mathbf{A}_1 + \mathbf{A}_2 + \mathbf{A}_3$, $\mathbf{B} = \mathbf{B}_1 + \mathbf{B}_2 + \mathbf{B}_3 \in \mathcal{M}_\ell(\mathbb{F}_2)$, with each $\mathbf{A}_i$ and $\mathbf{B}_j$ a power of $\mathbf{X}$ or $\mathbf{Y}$
- CSS stabiliser code: $\mathbf{H}_X = [\mathbf{A}|\mathbf{B}]$, $\mathbf{H}_Z = [\mathbf{B}^\top|\mathbf{A}^\top]$
- Gross code $[[144, 12, 12]]$

Toric codes (Kitaev - 1997)

- $G = C_m \times C_m$ product of two cyclic groups
- $a = 1 + x, b = 1 + y \in \mathbb{F}_2[x, y] \,/ < x^m - 1, y^m - 1, xy - yx >$

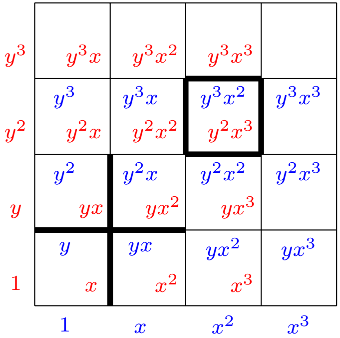

Figure: The toric code as an Abelian Two-Block Group Algebra code

Upper bounds on the minimum distance of GB codes

Bravyi-Terhal bound: (Bravyi, Terhal - 2009)

Let $\mathcal{C}$ be a stabiliser code of length n such that

- qubits are indexed by the vertices of $\{1, \dots, L\}^D$ or $(\mathbb{Z}/L\mathbb{Z})^D$
- the support of any generator is included in a hypercube with r^D vertices
- $L \geq 2(r-1)^2$

Then the minimum distance satifies $d \leq rL^{D-1} = r\,n^{(D-1)/D}$.

Upper bounds on the minimum distance of GB codes: (Pryadko, Wang - 2022)

Let $\mathcal{C}$ be a non-trivial GB code of length n and with stabiliser generators of weight w.
Then the minimum distance d of the code is in $O(n^{(D-1)/D})$, with $D \leq w - 1$.

Upper bounds on the minimum distance of Abelian 2BGA codes

Distance bound for geometrically-local codes:

Let $\mathcal{C}$ be a stabiliser code of length $n = m\ell$ such that

- qubits are indexed by the vertices of $\mathbb{Z}^D/\Lambda$, where Λ is a D-dimensional sublattice of $\mathbb{Z}^D$ such that $|\mathbb{Z}^D/\Lambda| = \ell$, and each vertex indexes m qubits
- the support of any generator is included in a Euclidean ball of $\mathbb{Z}^D/\Lambda$ of radius r
- $\ell^{1/D} \geq 8r\sqrt{\gamma_D}$, where γ_D is D-dimensional Hermite's constant ($\gamma_D \leq 1 + D/4$)

Then the minimum distance satifies $d \leq m(4r + \sqrt{D})\sqrt{\gamma_D}\,\ell^{(D-1)/D}$.

Upper bounds on the minimum distance of Abelian 2BGA codes:

Let $\mathcal{C}$ be a non-trivial Abelian 2BGA code of length 2ℓ and with stabiliser generators of weight w. Then the minimum distance d of the code satisfies $d \leq 2(4 + \sqrt{D})\sqrt{\gamma_D}\,\ell^{(D-1)/D}$, with $D = w - 2$, whenever $\ell^{1/D} \geq 8\sqrt{\gamma_D}$.

Abelian 2BGA codes are geometrically-local

Lemma

Any non-trivial Abelian 2BGA code is equivalent to an Abelian 2BGA code given by $\mathbf{A} = \sum_{g \in G} a_g \mathbb{B}(g)$ *and* $\mathbf{B} = \sum_{g \in G} b_g \mathbb{B}(g)$ *with* $\operatorname{supp}(a) = \{e, g_{a_1}, \ldots, g_{a_r}\}$ *and* $\operatorname{supp}(b) = \{e, g_{b_1}, \ldots, g_{b_s}\}$.

Let $\{\epsilon_i\}_{1 \leq i \leq r+s}$ be the computational basis of $\mathbb{Z}^{r+s}$ and consider the $\mathbb{Z}$-linear map

$$\Psi : \mathbb{Z}^r \times \mathbb{Z}^s \to G, \ \epsilon_i \mapsto \begin{cases} g_{a_i} & \text{if } 1 \leq i \leq r, \\ g_{b_{i-r}} & \text{if } r+1 \leq i \leq r+s \end{cases}$$

Lemma

If Ψ *is not surjective, then the Abelian 2BGA code* C *can be decomposed into a direct sum of* $[G : \operatorname{im}\Psi]$ *equivalent non-trivial Abelian 2BGA codes. These subcodes have a smaller codelength, but the same minimum distance, and stabiliser generators of the same weight.*

Abelian 2BGA codes are geometrically-local

The isomorphism $\bar{\Psi} : \mathbb{Z}^{r+s}/\ker\Psi \to G$ allows one to identify each qubit by a vertex of $\mathbb{Z}^{r+s}/\ker\Psi$:

- Represent the j-th qubits by $\bar{\Psi}^{-1}(g_j)$ for $j \in [[0, n-1]]$
- Represent the $(n+j)$-th qubits by $\bar{\Psi}^{-1}(g_j)$ for $j \in [[0, n-1]]$

Sabiliser generators (rows of $\mathbf{H}_X$ and $\mathbf{H}_Z$) have supports represented respectively by

- $S_i^X = \{\bar{\Psi}^{-1}(g_i), \bar{\Psi}^{-1}(g_i) - \epsilon_1, \ldots, \bar{\Psi}^{-1}(g_i) - \epsilon_{r+s}\}) \subset B(\bar{\Psi}^{-1}(g_i), 1)$
- $S_i^Z = \{\bar{\Psi}^{-1}(g_i), \bar{\Psi}^{-1}(g_i) + \epsilon_1, \ldots, \bar{\Psi}^{-1}(g_i) + \epsilon_{r+s}\}) \subset B(\bar{\Psi}^{-1}(g_i), 1)$

Theorem

Let C be a non-trivial Abelian 2BGA code with stabiliser generators of weight w. There exists an undecomposable Abelian 2BGA subcode of C of length $n = 2\ell$, and a $D = w - 2$ dimensional sublattice $\Lambda \subset \mathbb{Z}^D$ of volume ℓ such that

- *the qubits are indexed by the vertices of $\mathbb{Z}^D/\Lambda$, where each vertex indexes 2 qubits*
- *the support of any generator is included in a Euclidean ball of $\mathbb{Z}^D/\Lambda$ of radius 1*

Hence, whenever $\ell^{1/D} \geq 8\sqrt{\gamma_D}$, then the minimum distance satisfies $d \leq 2(4 + \sqrt{D})\sqrt{\gamma_D}\,\ell^{(D-1)/D}$.

Take away

Abelian Two-Block Group Algebra codes

- Two-Block codes constructed from a group algebra over a finite abelian group
- Generalisation of toric codes, Generalised Bicycle codes and Bivariate Bicycle codes
- LDPC codes with regular structure (simplified implementation)

Distance bound for Abelian 2BGA codes

- Geometrically-local in D dimensions, with $D =$ (weight of stabliser generators) - 2
- The minimum distance of an Abelian 2BGA code of length $n = 2\ell$ satifies

$$d \leq 2(4+\sqrt{D})\sqrt{\gamma_D}\,\ell^{(D-1)/D} = O(D\,\ell^{(D-1)/D})$$

Thank you for your attention! Any questions?