Additive twisted codes: new distance bounds and infinite families of quantum codes

Reza Dastbasteh[1] and Petr Lisoněk[2]
[1]University of Navarra, Spain
[2]Simon Fraser University, Burnaby, BC, Canada

WCC 2024: The Thirteenth International Workshop on Coding and Cryptography
Perugia, Italy

17 June 2024

Overview

We provide a new construction of quantum codes that enables integration of a broader class of classical codes into the mathematical framework of quantum stabilizer codes.

Next, we present new connections between twisted codes and linear cyclic codes and we provide novel bounds for the minimum distance of twisted codes. We show that classical tools such as the Hartmann-Tzeng minimum distance bound are applicable to twisted codes.

This enabled us to discover five new infinite families and many other examples of record-breaking, and sometimes optimal, binary quantum codes.

Additive twisted codes

An $\mathbb{F}_2$-linear subspace of $\mathbb{F}_4^n$ is called an additive code over $\mathbb{F}_4$. Additive codes are especially important due to their application in the construction of binary quantum codes. Additive twisted codes are possibly the most structured family of additive codes. They were introduced Bierbrauer and Edel (1997). Twisted codes, like linear cyclic codes, are defined and constructed using a (unique) defining set, and the BCH minimum distance bound holds for them. Bierbrauer and Edel (2000) constructed several families and examples of good quantum codes using dual-containing twisted codes.

While the original work on the additive twisted codes has been widely referenced in literature, twisted codes have not been developed much since their invention. This is likely due to their study being technically much more difficult than the study of many other common families of codes.

Quantum codes

The parameters of a binary quantum error-correcting code that encodes k logical qubits into n physical qubits and has minimum distance d are denoted by $[\![n, k, d]\!]$. The most common approach to construction of quantum codes is by using the stabilizer formalism which builds a bridge between certain dual-containing additive codes and quantum (stabilizer) codes.

One of the main challenges of quantum stabilizer codes is the dual-containment condition, which only allows a small number of classical codes to be used to construct good quantum codes.

Outline

In this talk, we first give a novel construction of binary stabilizer quantum codes that makes it possible to also use additive codes that are not dual-containing.

Next, we introduce a new perspective on twisted codes by viewing each code as an additive subcode of a particular linear cyclic code. This new approach enables us to give novel minimum distance lower and upper bounds for twisted codes and show new similarities between twisted codes and linear cyclic codes. In particular, we prove that the Hartmann-Tzeng bound holds for twisted codes.

We demonstrate that five infinite families of record-breaking, and sometimes optimal, quantum codes can be constructed from twisted codes using these bounds.

Background

Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$. An additive code $C \subseteq \mathbb{F}_4^n$ with $\mathbb{F}_2$-dimension k will be denoted by $(n, 2^k)$, with minimum non-zero weight $d(C)$.

Let $\mathrm{Tr} : \mathbb{F}_4 \to \mathbb{F}_2$ be defined by $\mathrm{Tr}(x) = x + \overline{x}$, where $\overline{x} = x^2$. The trace inner product of $u, v \in \mathbb{F}_4^n$ is

$$u * v = \mathrm{Tr}(u \cdot \overline{v}) = (u \cdot \overline{v}) + \overline{(u \cdot \overline{v})} = \sum_{i=1}^{n} (u_i \overline{v_i} + \overline{u_i} v_i).$$

The trace dual of C with respect to the trace inner product is defined by

$$C^{\perp_t} = \{u \in \mathbb{F}_4^n : u * v = 0 \text{ for all } v \in C\}.$$

Note $C^{\perp_t}$ is an $(n, 2^{2n-k})$ additive code.

Quantum codes from additive codes

We say that C is dual-containing (respectively self-dual) code with respect to the trace inner product if $C^{\perp_t} \subseteq C$ (respectively $C^{\perp_t} = C$).

Theorem (Calderbank, Rains, Shor, Sloane 1998)

Let $C \subseteq \mathbb{F}_4^n$ be an $(n, 2^{n+k}, d)$ additive code such that $C^{\perp_t} \subseteq C$. Then an $[\![n, k, d']\!]$ binary quantum stabilizer code can be constructed, where d' is the minimum weight in $C \setminus C^{\perp_t}$ if $k > 0$ and $d' = d$ if $k = 0$.

If $d = d'$ the above quantum code is called pure, and otherwise ($d < d'$) impure.

Additive twisted codes

Let n, r be positive integers such that $n \mid 2^r - 1$. The map $\phi_\gamma : \mathbb{F}_{2^r} \to \mathbb{F}_2 \times \mathbb{F}_2$ is defined by

$$\phi_\gamma(x) = (\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)), \tag{1}$$

where $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ and Tr_1^r is the trace map from $\mathbb{F}_{2^r}$ to $\mathbb{F}_2$. Let $W = \{1, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\}$, where α is a primitive n-th root of unity in $\mathbb{F}_{2^r}^*$.

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. We define $B(A)$ to be the matrix over $\mathbb{F}_{2^r}$ whose rows and columns are labelled by elements of A and W, respectively, and the entry in row j and column α^i is α^{ij}. Let $C(A)$ be the length n linear cyclic code over $\mathbb{F}_{2^r}$ with the defining set A. Then $B(A)$ is a generator matrix for the code $C(A)^\perp$, the Euclidean dual of $C(A)$.

Additive twisted codes

Definition

Let $\langle , \rangle_s : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{F}_2$ be the symplectic $\mathbb{F}_2$-bilinear form defined by

$$\Big\langle \big((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2})\big), \big((b_{11}, b_{12}), \ldots, (b_{n1}, b_{n2})\big) \Big\rangle_s = \sum_{i=1}^{n} a_{i1} b_{i2} - a_{i2} b_{i1}.$$

Definition

Let $n \mid 2^r - 1$ for some integer r and A be a subset of $\mathbb{Z}/n\mathbb{Z}$. The dual of the code $\phi_\gamma(C(A)^\perp)$ with respect to the symplectic inner product $\langle , \rangle_s$ is called a twisted code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Such a twisted code will be denoted by $\mathcal{C}_\gamma(A)$. In other words,

$$\mathcal{C}_\gamma(A) = \big(\phi_\gamma(C(A)^\perp)\big)^{\perp_s}.$$

Additive twisted codes

The $\mathbb{F}_2$-linear isomorphism $\psi : \mathbb{F}_2^{2n} \to \mathbb{F}_4^n$ defined by

$$\psi\big((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2})\big) = (a_{11}\omega + a_{12}\omega^2, \ldots, a_{n1}\omega + a_{n2}\omega^2)$$

maps each twisted code into an additive code over $\mathbb{F}_4$. Moreover, we have

$$\langle u, v \rangle_s = \psi(u) * \psi(v)$$

for each $u, v \in \mathbb{F}_2^{2n}$.

In general, the set A in the above definition is not unique. We denote

$$\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2].$$

Let $Z(a)$ denote the 2-cyclotomic coset modulo n containing a.

Additive twisted codes

Definition (Bierbrauer and Edel 2000)

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $a \in A$. If κ divides $|Z(a)|$ and $\kappa \mid i-j$ for each $2^i a, 2^j a \in Z(a) \cap A$, then $Z(a) \cap A$ is called unsaturated. Otherwise, $Z(a) \cap A$ is called saturated.

Let $Z \cap A$ be unsaturated and $a \in Z \cap A$. We define

$$(Z \cap A)^H = \{a2^{\kappa i} : 0 \leq i \leq \frac{|Z(a)|}{\kappa} - 1\}.$$

Bierbrauer and Edel (2000) show that the set

$$\tilde{A} = \bigcup_{Z \cap A \ sat} Z \bigcup_{Z \cap A \ unsat} (Z \cap A)^H \tag{2}$$

is the largest defining set (called the complete defining set) that the twisted code $\mathcal{C}_\gamma(A)$ can have.

Additive twisted codes

Moreover $\mathcal{C}_\gamma(A)^{\perp_s} = \phi_\gamma(C(A)^\perp) = \mathcal{C}_\gamma(A_d)$, where

$$A_d = \bigcup_{Z \cap A = \emptyset} -Z \bigcup_{Z \cap A \ \textit{unsat}} -((Z \cap A)^H).$$

Hence a twisted code $\mathcal{C}_\gamma(A)$ is dual-containing if and only if $A \subseteq A_d$.

Theorem (Bierbrauer and Edel 2000)

Let $n \mid 2^r - 1$ be a positive integer and $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Then the $\mathbb{F}_2$-dimension of $\mathcal{C}_\gamma(A)$ is $\sum_Z c_Z(A)$, where the sum runs over all 2-cyclotomic cosets modulo n and

$$c_Z(A) = \begin{cases} 2|Z| & \text{if } Z \cap A = \emptyset \\ |Z| & \text{if } Z \cap A \text{ is unsaturated} \\ 0 & \text{if } Z \cap A \text{ is saturated.} \end{cases}$$

Nearly dual-containing additive codes

We present a new method of constructing quantum stabilizer codes from additive codes over $\mathbb{F}_4$ that are not dual containing with respect to the trace inner product.

Let C be an additive code over $\mathbb{F}_4$. The dual-containment deficiency of C is defined by

$$\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}).$$

New quantum code construction

Theorem

Let C be an $(n, 2^{n+k})$ additive code over $\mathbb{F}_4$ and $\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = 2e$. Then we can construct an $[\![n+e, k+e, d]\!]$ binary quantum code, where

$$d \geq \min\{d(C), d(C + C^{\perp_t}) + 1\}.$$

This is proved by explicitly constructing a generator matrix for a dual-containing code of length $n + e$, by first finding a basis for $C^{\perp_t}$ in a certain special form.

Minimum distance bounds for twisted codes

Similar to linear cyclic codes, the minimum distance of twisted codes can be bounded using the BCH bound. Currently, this is the only known minimum distance bound for the twisted codes.

Recall that $L \subseteq \mathbb{Z}/n\mathbb{Z}$ is called a consecutive set of length s if there exists an integer c with $\gcd(c, n) = 1$ such that

$$\{(cl) \bmod n : l \in L\} = \{(j + t) \bmod n : 0 \leq j \leq s - 1\}$$

for some $t \in \mathbb{Z}/n\mathbb{Z}$. The next proposition gives the BCH minimum distance bound for twisted codes.

Proposition (Bierbrauer and Edel 2000)

Let A be a defining set of a twisted code $\mathcal{C}_\gamma(A)$ such that A contains a consecutive set of size $t-1$. Then $d(\mathcal{C}_\gamma(A)) \geq t$.

Minimum distance bounds for twisted codes

The following theorem establishes a more powerful connection between twisted codes and linear cyclic codes.

Theorem

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a defining set of a twisted code $\mathcal{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Then the following statements are equivalent.

1. *The vector $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathcal{C}_\gamma(A)$.*
2. *The vector*
   $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2}) \in C(A)$.

Corollary

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a defining set of a twisted code $\mathcal{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. If $\mathcal{C}_\gamma(A)$ contains a weight t vector, then $C(A)$ also contains a weight t vector. In particular, $d(\mathcal{C}_\gamma(A)) \geq d(C(A))$.

Minimum distance bounds for twisted codes

The Hartmann-Tzeng bound (HT bound) is one of classical bounds on the minimum distance of linear cyclic codes. We generalize it for twisted codes.

Corollary

Let A be a defining set of a twisted code $\mathcal{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ such that A contains a subset in the form

$$B = \{(l + i_1 c_1 + i_2 c_2 + \cdots + i_k c_k) \bmod n : \ 0 \leq i_j \leq s_j, \ \gcd(c_j, n) = 1\},$$

where $l, c_j \in \mathbb{Z}/n\mathbb{Z}$ and s_j is a non-negative integer for $1 \leq j \leq k$.

Then $d(\mathcal{C}_\gamma(A)) \geq \left(\sum_{j=1}^{k} s_j \right) + 2.$

Minimum distance bounds for twisted codes

Theorem

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a symmetric ($A = -A$) defining set of a twisted code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ such that $0 \notin A$. If $d\big(\mathcal{C}_\gamma(A \cup \{0\})\big) \geq 5$, then $\mathcal{C}_\gamma(A)$ has no codeword of weight 4. If in addition $\gcd(n, 3) = 1$, then $d\big(\mathcal{C}_\gamma(A)\big) \geq 5$.

We also observed that the choice of γ has a (sometimes serious) impact on the minimum distance of twisted codes. Interestingly, this seems to have been ignored so far. Examples can be found in our WCC 2024 extended abstract.

Infinite classes of binary quantum codes

In this section we give five infinite families of binary quantum codes that produce good (record-breaking or optimal) binary quantum codes. First, the next theorem gives a secondary construction of binary quantum codes that are constructed from twisted codes.

Theorem

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $\mathcal{C}_\gamma(A)$ be a pure binary quantum code with parameters $[\![n, k, t]\!]$. Then the following results hold.

(i) *If $d(\mathcal{C}_\gamma(\bar{A})) \geq t+1$, where $\bar{A} = A \cup \{0\}$, then there exists an $[\![n+1, k-1, t+1]\!]$ quantum code.*

(ii) *If $\kappa = 2$ and $\{a, n-a\}$ is a 2-cyclotomic coset such that $d(\mathcal{C}_\gamma(\bar{A})) \geq t+1$ for $\bar{A} = A \cup \{a\}$, then there exists an $[\![n+1, k-1, t+1]\!]$ quantum code.*

Infinite classes of binary quantum codes

The minimum distance bounds for the constructions presented in this section employ our new results presented earlier in this talk.

Theorem

Let $r > 5$ be an even integer. Then there exists a binary quantum code with parameters $[\![2^r, 2^r - \frac{3}{2}r - 2, d \geq 4]\!]$.

Proof idea: Use $n = 2^r - 1$, $\kappa = \frac{r}{2}$, and $A = \{1, a, b\}$, where $a = 2^{\frac{r}{2}} + 1$ and $b = 2^{\frac{r}{2}}$.

For instance, if $r = 6$, this construction gives a *record-breaking* $[\![64, 53, 4]\!]$ quantum code Q. Applying secondary constructions (shortening etc.) to Q produces many new record-breaking codes.

Infinite classes of binary quantum codes

Theorem

(i) Let $t = 2^{2k+1}$ for some integer $k \geq 1$ and $n = t^2 + t + 1$. Then there exists an $[\![n, n - 12k - 6, d \geq 5]\!]$ binary quantum code.
(ii) Let $t = 2^{2k}$ for some integer $k \geq 1$ and $n = t^2 - t + 1$. Then there exists an $[\![n, n - 12k, d \geq 5]\!]$ binary quantum code.

Proof ideas:
For part (i) use $\kappa = 2k + 1$ and $A = \{\pm 1, \pm t, \pm(t + 1)\}$.
For part (ii) use $\kappa = 2k$ and $A = \{\pm 1, \pm t, \pm(t - 1)\}$.

We construct one optimal as well as two new record-breaking quantum codes with minimum distance of five using the above results. Applying the secondary constructions gives 27 other record-breaking binary quantum codes. Moreover, this code can be used to construct 58 other binary quantum codes with missing constructions (red coloured entries in Markus Grassl's tables).

Infinite classes of binary quantum codes

Theorem

(i) Let $t \geq 4$ be an even integer and $n = 2^t + 1$. Then there exists a pure quantum code with parameters $[\![2^t + 1, 2^t - 2t + 1, d \geq 4]\!]$.
(ii) Let $t \geq 3$ be an odd integer and $n = 2^t + 1$. Then there exists a pure quantum code with parameters $[\![2^t + 2, 2^t - 2t, d \geq 4]\!]$.

Proof ideas:
For part (i) use $A = \{1, 2^{\frac{t}{2}}, -1, -2^{\frac{t}{2}}\}$ and $\kappa = \frac{t}{2}$ (note that $\kappa \mid r = 2t$).
For part (ii) use $A = \{-1, 1\}$ and $\kappa = t$.

Also this construction produces several optimal quantum codes.

Other recent work

In their recent preprint "Characterization of Nearly Self-Orthogonal Quasi-Twisted Codes and Related Quantum Codes" (arXiv:2405.15057), Ezerman, Grassl, Ling, Özbudak and Özkaya used the same technique as our construction to characterize nearly dual-containing quasi-twisted codes with respect to the Euclidean, Hermitian, and (trace) symplectic inner products.

Their construction provides an improved lower bound on the minimum distance. If C is an $(n, 2^{n+k})$ additive code over $\mathbb{F}_4$ and $\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = 2e$, then their construction gives an $[\![n+e, k+e, d]\!]$ binary quantum code, where

$$\begin{aligned} d &\geq \min\{\mathrm{wt}\big(C \setminus (C \cap C^{\perp_t})\big), \mathrm{wt}\big((C + C^{\perp_t}) \setminus C^{\perp_t}\big) + 1\} \\ &\geq \min\{d(C), d(C + C^{\perp_t}) + 1\} \quad \text{(our bound)}. \end{aligned}$$

They discovered numerous record-breaking quantum codes, both binary and non-binary, through an exhaustive search using nearly dual-containing quasi-twisted codes.

References

R. Dastbasteh, New quantum codes, minimum distance bounds, and equivalence of codes. PhD Thesis, Simon Fraser University, 2023.

Y. Edel and J. Bierbrauer, Twisted BCH-codes. J. Combin. Des. 5 (1997), 377–389.

J. Bierbrauer and Y. Edel, Quantum twisted codes. J. Combin. Des. 8 (2000), 174–188.

J. Bierbrauer, Introduction to coding theory. Chapman & Hall/CRC, Boca Raton, 2005.