Quantum error-correcting codes from generalized Toeplitz graphs

Andreas Garcia, Layla Jarrahy, & Elisaveta (Lisa) Samoylov (Mentor: Dr. Padmapani Seneviratne)

Theoretical and Application Driven Mathematics REU

Abstract

In a groundbreaking paper, Calderbank et al. established that quantum stabilizer (qubit) codes can be represented by self-orthogonal additive codes over $GF(4)^n$. In this presentation, we specifically look at the representation of 0-dimensional qubit codes by self-dual additive codes. Self-dual additive codes are additive subgroups of $GF(4)^n$ and are classified by their length and their minimum distance (a quantity proportional to the number of errors the code can correct). Additionally, self-dual additive codes can be generated by graphs, though many such current codes in literature are constructed from circulant graphs and their variations.

We present a new code-construction from generalized Toeplitz graphs to generate new zero-dimensional qubit codes. Let G be a finite group. A generalized Toeplitz graph $\Gamma = T_G(S)$ has the vertex set $V(\Gamma) = G$ and the edge set $E(\Gamma) = \{(v, sv) : s \in S, sv \in G\}$. Using the given generalized Toeplitz construction and randomized computer search, we obtained 66- and 93-length qubit codes that improve the minimum distance of the current codes by one.

Key words: Generalized toeplitz graph, qubit codes

Self-Dual Additive Codes

Let $GF(q)$ be an alphabet, $q \in \mathbb{N}$. An additive code of length n over $GF(q)$ is any additive subgroup of $GF(q)^n$. They are often represented as a *generator matrix*, whose rows additively span the subgroup. Under the Hermitian trace inner product $*$,

$$C^* := \{\vec{x} \in GF(q)^n : \forall \vec{c} \in C, \vec{c} * \vec{x} = 0\}.$$

C is called *self-orthogonal* if $C \subseteq C^*$ and *self-dual* if $C = C^*$. Codes whose codewords all have even weight are called Type II; else, they are Type I.

From graphs to QECCs

Danielson and Parker An $n \times n$ graph adjacency matrix A generates a self-dual additive code over $GF(4)$ defined by $A + \omega I$ with parameters $[[n, 0, d]]_2$ [3] They detect $d-1$ errors and correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Calderbank et al. A self-orthogonal additive $(n, 2^{n-k})$ $\mathbb{F}_4$ code C, where all elements of $C^* \setminus C$ have minimum weight greater than or equal to d, corresponds to a quantum error correction code with length n, dimension k, and minimum distance d[2].

0-dimensional QECCs are important for testing the accuracy of quantum computers. Using these theorems lets us efficiently construct 0-dimensional QECCs.

Generalized Toeplitz Graphs

Circulant Graphs are commonly used to generate QECCs[4] and have a circulant adjacency matrix:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}$$

Toeplitz graphs generalize circulant graphs and have a Toeplitz adjacency matrix:

$$\begin{bmatrix} 2 & 3 & 1 & 0 & -1 \\ 1 & 2 & 3 & 1 & 0 \\ 9 & 1 & 2 & 3 & 1 \\ 0 & 9 & 1 & 2 & 3 \\ 2 & 0 & 9 & 1 & 2 \end{bmatrix}$$

Definition

Let G be a semigroup, $S \subset V \subseteq G$, with $|V|$ finite.

The **generalized Toeplitz graph** [1] $\Gamma = T_V(S)$ has

$$V(\Gamma) = V$$

$$E(\Gamma) = \{(v, sv) : s \in S, sv \in V\}$$

To ensure that the graph is simple and undirected, $S = -S$ and $\mathbf{1} \notin S$.
We consider graphs with $V = G$ and G a group.

Computational Methods

Algorithm 1 Pseudocode to Generate GT Graph

```
Require: A ⊆ V \ {1}, A = A^{-1}
for v ∈ V do
  for a ∈ A do
    if av ∈ V then
      Add edge (v, av) to graph Γ
    end if
  end for
end for
```

Algorithm 2 Pseudocode to Generate GT Codes

```
G is a group of order n
d_max is minimum distance
for i = 1 → 10^9 do
  A := RandomSubset(G) \ {1}
  Γ := ToeplitzGraph(A, G)
  AdjMat := AdjacencyMatrix(Γ)
  C := AdditiveCode(AdjMat + ωI)
  if VerifyMinDistance(C, d_max) = true then
    You have a code, minimum distance at least d!
  end if
end for
```

Coding Theory Results

From the adjacency matrices of generalized Toeplitz graphs, we discovered two new QECCs of lengths $n = 66$ and $n = 93$ with respective minimum distances $d = 17$ and $d = 22$, improving upon previous best minimum distances of $d = 16$ and $d = 21$. The following codes were generated from a randomized search using the `MAGMA programming language`.

Codes of New Type

Table 1: Optimal Codes of a Type Unattainable via Circulant Graphs [4]

Γ_n	$d_{\min}(C(\Gamma_n))$	Type	Group ID	A	$k(\Gamma_n)$	$\lvert Aut(\Gamma_n)\rvert$
Γ_8	4	I	$G_{8,2}$	A_{18}	4	48
Γ_{12}	6	I	$G_{12,2}$	A_{12}	6	12
Γ_{20}	8	I	$G_{20,5}$	A_{20}	6	40
Γ_{22}	8	I	$G_{22,1}$	A_{22}	10	22
Γ_{28}	10	I	$G_{28,3}$	A_{28}	16	28
Γ_{36}	12	II	$G_{36,5}$	A_{36}	13	72

Directly Constructed Codes

Table 2: Optimal codes created using a direct construction

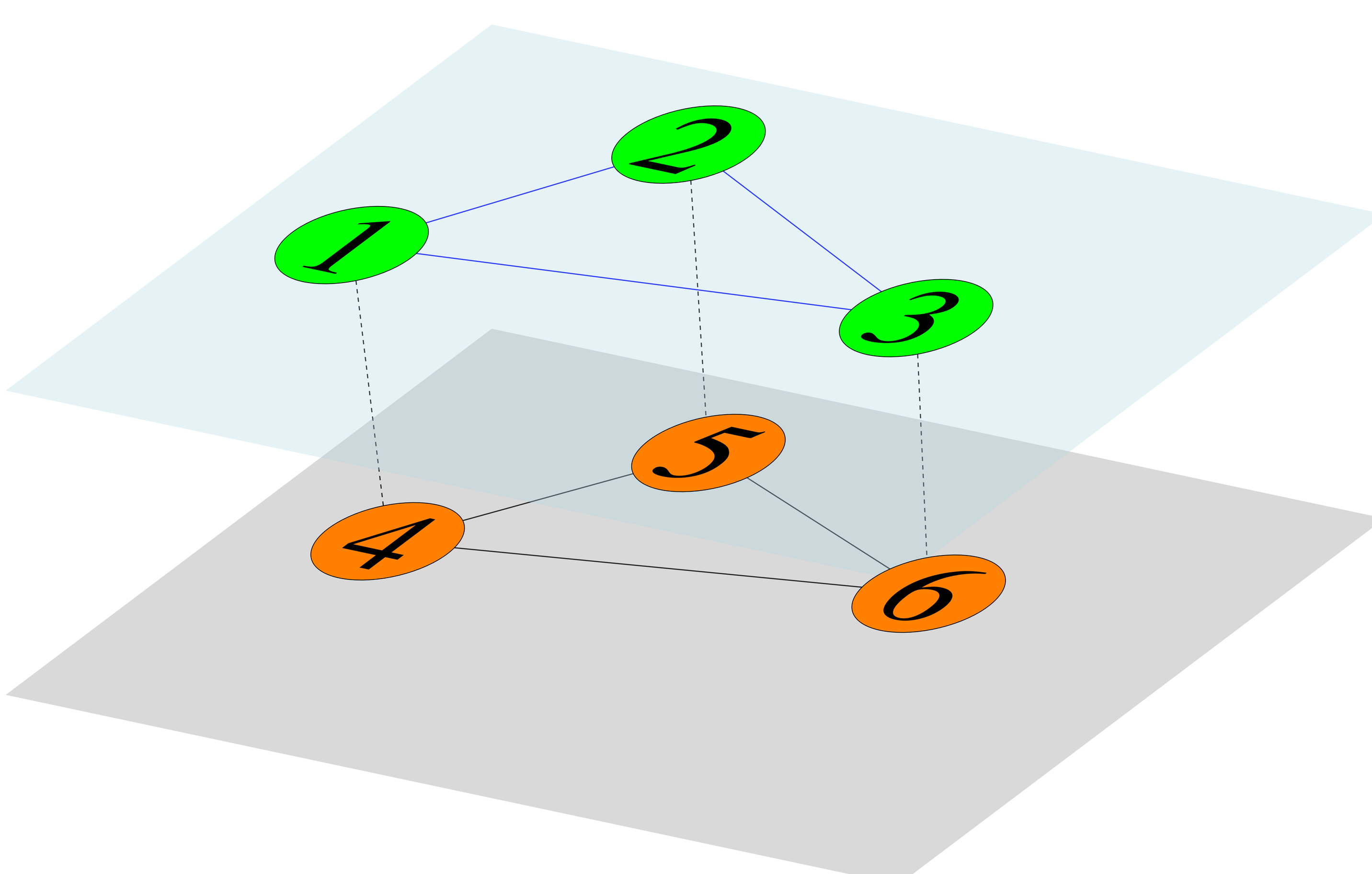
Code	Order	Group	Min Dist
$[[55,0,16]]$	55	$\mathbb{Z}_5 \ltimes \mathbb{Z}_{11}$	16
$[[81,0,20]]$	81	SmallGroup(81,8)	20

Code Tables

Graph Theory Results

Generalized Toeplitz Graph Example

The GT graph $T_{\mathbb{Z}_2 \times \mathbb{Z}_3}(\{(0,1),(0,2),(1,2)\})$.



Generalized Toeplitz Properties

Let $S \subset G$ be the defining set, and $\Gamma = T_G(S)$ be the generalized toeplitz graph generated from S.

- If G is a group, then a unique S produces a unique edge set. (ie. $A \neq B \Rightarrow E(T_V(A)) \neq E(T_V(B))$.)
- The complement $\overline{\Gamma} := T_G((G \setminus S) \setminus \{1\})$.
- If G is a semigroup, then $T_G(S)$ is $|S|$-regular
- Let G be a finite group. Then the valence of $T_G(S)$ is even if S contains an even number of involutions.
- Let G be a finite group with $|G| = n$. Let $H \leq G$ be a subgroup such that $[G : H] = 2$. Let $K_{\frac{n}{2}}$ denote the complete graph on $n/2$ vertices. For $H^* = H \setminus \{1\}$,
$$T_G(H^*) \cong K_{\frac{n}{2}} \cup K_{\frac{n}{2}}$$
- Let G, H be finite groups. If $G \cong H$ with $\varphi : G \to H$, then
$$T_G(S) \cong T_H(\varphi(S))$$

References

[1] Sheng Bau.
A generalization of the concept of toeplitz graphs.
Mong. Math. J, 1:54–61, 2011.

[2] A Robert Calderbank, Eric M Rains, Peter M Shor, and Neil JA Sloane.
Quantum error correction via codes over gf (4).
IEEE Transactions on Information Theory, 44(4):1369–1387, 1998.

[3] Lars Eirik Danielsen and Matthew G Parker.
On the classification of all self-dual additive codes over gf (4) of length up to 12.
Journal of Combinatorial Theory, Series A, 113(6):1351–1367, 2006.

[4] Ken Saito.
Self-dual additive f4-codes of lengths up to 40 represented by circulant graphs.
Adv. Math. Commun, 13(3):213–220, 2019.

Acknowledgements

The content of this poster is based upon work from the TADM-REU, supported by the NSF under the grant DMS-2243991. Travel is supported by the NSF under Grant No. 2015553 and the Hamilton College Kirkland Endowment Funds.