The Neighbor Graph of Linear Complementary Dual Codes

Carlos Vela

5th Pythagorean Conference
Kalamata, 5th June

Joint work with Javier de la Cruz, Anna-Lena Horlemann
Marc Newman and Wolfgang Willems.

supported by the Leading House Latin America Research Partnership Grant no. RPG2352.

Linear codes

Definition

- A q-ary linear code C is a k-dimensional subspace of $\mathbb{F}_q^n$.
- The dual code $C^\perp$ is defined as:

$$C^\perp = \{y \in \mathbb{F}_q^n \mid \langle x, y \rangle = 0 \text{ for all } x \in C\}.$$

It is itself a linear code of dimension $n - k$.

- The Hamming distance between two codewords $c, c' \in \mathbb{F}_q^n$ is the number of positions where they differ:

$$d_H(c, c') = |\{i : c_i \neq c'_i\}|.$$

- The minimum Hamming distance of a code C is:

$$d = \operatorname{mín}_{c \neq c' \in C} d_H(c, c').$$

Linear Complementary Dual (LCD) Codes

Definition

A linear code $C \subset \mathbb{F}_q^n$ is an <u>LCD code</u> if its dual code $C^\perp$ satisfies:

$$C \cap C^\perp = \{0\}.$$

Equivalently, there exists a generator matrix G such that $GG^\top$ is nonsingular.

Lemma

C is LCD $\iff$ $C^\perp$ is LCD

Some cool application for LCD codes.

- Entanglement Assisted Quantum Error Correcting Codes (EAQECC) from LCD Codes.
- Decoding with LCD codes.
- LCD codes against Side channel and Fault injection attacks

Known Results and Open Questions on LCD Codes

- Every $[n,k]_q$ code has an equivalent LCD code (reached through monomial operations on the columns of G), as long as $q \geq 4$.
  $\Longrightarrow$ via basis transformation, known constructions and decoding algorithms can be adapted to LCD
- Every $[n,k]_{2^m}$ LCD code has an equivalent $[nm,km]_2$ LCD code.
- For $q = 2, 3$ the question of how to construct (and decode) good LCD codes is open.
- Also open: the number of equivalence classes, the maximal achievable distance, subcode behavior etc.

Neighbors of Linear Codes

Definition

Two $[n, k]_q$ codes are *neighbors* if they intersect in dimension $k - 1$.

Notation:

$$C_0(v) := \{c \in C \mid \langle c, v \rangle = 0\}.$$

Definition

Let $C \subseteq \mathbb{F}_q^n$ be a linear code and let $v \notin C \cup C^\perp$. The *associated neighbor* of C *with respect to* v is defined as:

$$N(C, v) := \langle C_0(v), v \rangle.$$

Associated Neighbors are Neighbors

Lemma

If C' is an associated neighbor of C w.r.t. v, then

$$C \cap N(C, v) = C_0(v)$$

and hence

$$\dim(C \cap N(C, v)) = \dim C - 1.$$

... but not the other way around ...

Associated Neighborship is not Symmetric

- Consider the neighboring $[4,2]_2$ codes C and C' generated by:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad G' = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

$$\implies C \cap C' = \langle (1,1,0,0) \rangle$$

-

$$C_0((1,1,1,0)) = \langle (1,1,0,0) \rangle$$

$$\implies N(C, v) = C'$$

- However: for all $v' \notin C' \cup C' \perp$, $C_0'(v') \neq C \cap C'$.

$$\implies N(C', v') \neq C$$

Number of Neighbors

Proposition

Let $C \subseteq \mathbb{F}_q^n$ be a k-dimensional code. Then:

- *C has $\frac{(q^k-1)(q^{n-k+1}-q)}{(q-1)^2}$ neighbors.*
- *C has at most*

$$\frac{q^n - |C \cup C^{\perp}|}{q-1} \leq \frac{q^n - q^{\text{máx}(k,n-k)}}{q-1}$$

  associated neighbors with respect to some $v \in \mathbb{F}_q^n \setminus (C \cup C^{\perp})$.

Note:

$$\frac{q^n - q^{\text{máx}(k,n-k)}}{q-1} < \frac{(q^k-1)(q^{n-k+1}-q)}{(q-1)^2}$$

Duality of Neighbors

Proposition

1. *C and C' are neighbors $\iff$ $C^\perp$ and $C'^\perp$ are neighbors.*
2. *C' is an associated neighbor of C $\iff$ $C^\perp$ is an associated neighbor of $C'^\perp$.*

If

$$C' = N(C, v)$$

then

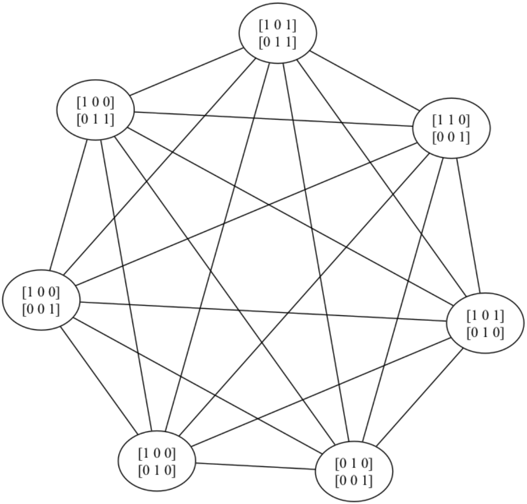
$$C^\perp = N(C'^\perp, u - v)$$

for some $u \in C \setminus C_0(v)$ with $u - v \in C^\perp \setminus C'^\perp$.

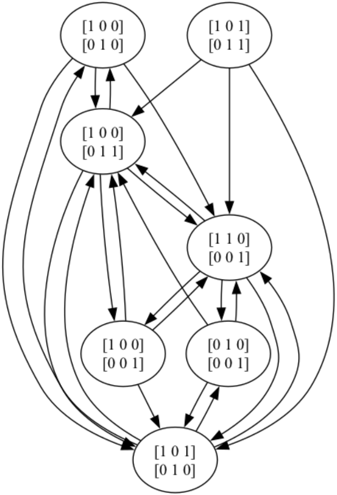
Neighborship as a Graph

- Neighborship relations between codes can be modeled as a graph.
- Each node in the graph represents a code (e.g., C, C').
- An edge between two nodes indicates that the corresponding codes are neighbors.
- Since general neighborship is symmetric, the corresponding graph is undirected. For associated neighborship we need a directed graph.
- This representation helps visualize relationships between codes, allowing for easier analysis and exploration of code properties.

Example in $\mathbb{F}_2^3$

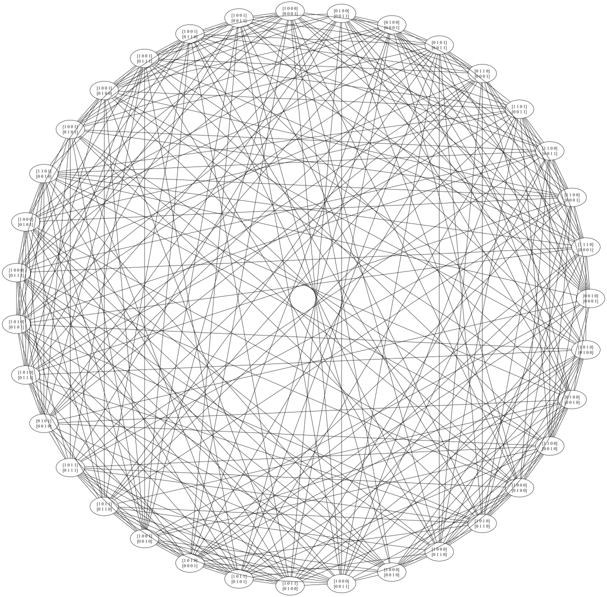


neighbors

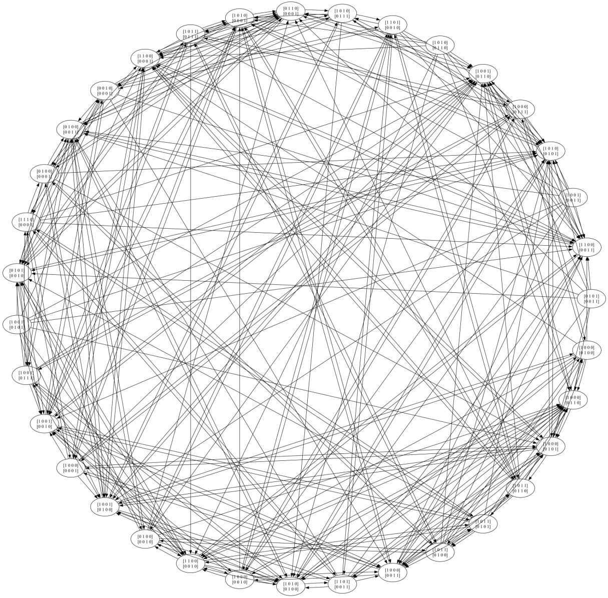


associated neighbors

Example: Neighbors in $\mathbb{F}_2^4$



Example: Associated Neighbors in $\mathbb{F}_2^4$



LCD Neighbors of LCD Codes

Theorem

Let $C \subseteq \mathbb{F}_q^n$ be a k-dimensional LCD code. Then C has

$$\begin{cases} \frac{q-1}{q}N - \left(\frac{-1}{q}\right)^{n/2} q^{n/2-1} & \text{if } q \text{ is odd, } n \text{ is even, and } k \text{ is odd,} \\ \frac{q-1}{q}N & \text{otherwise,} \end{cases}$$

neighbors that are LCD, where $N := \frac{(q^k-1)(q^{n-k+1}-q)}{(q-1)^2}$ is the overall number of neighbors.

Corollary

- *For $q = 2$, exactly half of the neighbors of any LCD code are LCD themselves.*
- *As q grows, the fraction of LCD neighbors approaches 1.*

Symmetry of Associated Neighborship for LCD Codes

Theorem

If C and C' are neighbors and LCD, then C is an associated neighbor to C' if and only if C' is associated to C.

$$- - -Or - - -$$

Let C be an $[n,k]_q$ LCD code, let $v \in \mathbb{F}_q^n \setminus (C \cup C^{\perp})$, and let $C' = N(C,v)$ also be an LCD code. Then $\exists v' \in \mathbb{F}_q^n \setminus (C' \cup C'^{\perp})$ such that $C = N(C',v')$.

The number of associated neighbors is not constant, it depends on the code.

The Neighbor Graph of LCD Codes

Theorem

The undirected graph of LCD neighbors of dimension k in $\mathbb{F}_q^n$:

- $|V| \approx q^{\lfloor \frac{k(n-k)}{2} \rfloor} \begin{bmatrix} \lfloor \frac{n}{2} \rfloor \\ \lfloor \frac{k}{2} \rfloor \end{bmatrix}_{q^2}$ [1]
- $|E| = \frac{1}{2}|V| \cdot \delta$
- *The graph is regular of degree*

$$\delta := \begin{cases} \frac{q-1}{q}N - \left(\frac{-1}{q}\right)^{n/2} q^{n/2-1} & \text{if } q \text{ is odd, } n \text{ is even, and } k \text{ is odd,} \\ \frac{q-1}{q}N & \text{otherwise.} \end{cases}$$

- *It is generally (for non-trivial $1 < k < n-1$)*
  - *not strongly nor distance-regular*
  - *not edge-transitive,*
  - *hence not symmetric.*

[1] The exact formula depends on the parities of q, k and n.

Vertex-Transitivity

Theorem

If $q = 2$, the LCD neighbor graph is vertex-transitive if and only if n is even and k is odd. If q is odd, the LCD neighbor graph is vertex-transitive only if n is even and k is odd.

Proof idea:

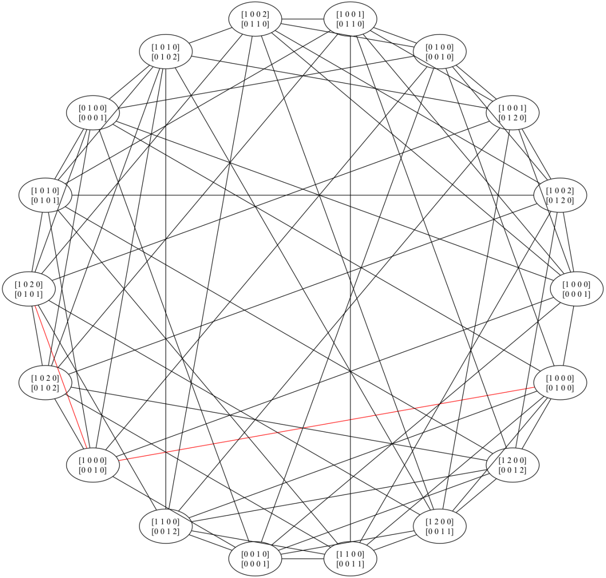
- For $q = 2, n$ is even and k is odd, $O(n, q)$ is transitive.
- In other cases, the orthogonal group splits $LCD[n, k]_q$ into several orbits of different cardinalities.

Connectedness and Diameter

Theorem

The $[n, k]_q$ LCD neighbor graph is connected and for odd q has diameter $\text{mín}(k, n - k)$.

Example: Connectedness and Diameter



The Associated Neighbor Graph of LCD Codes

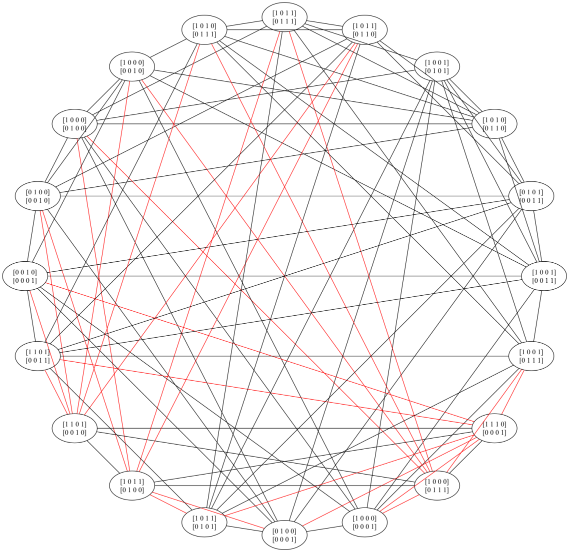
Remember: The graph can be represented as an undirected graph, by collapsing all pairs of directed edges with the same two vertices.

Theorem

The graph of LCD associated neighbors of dimension k in $\mathbb{F}_q^n$:

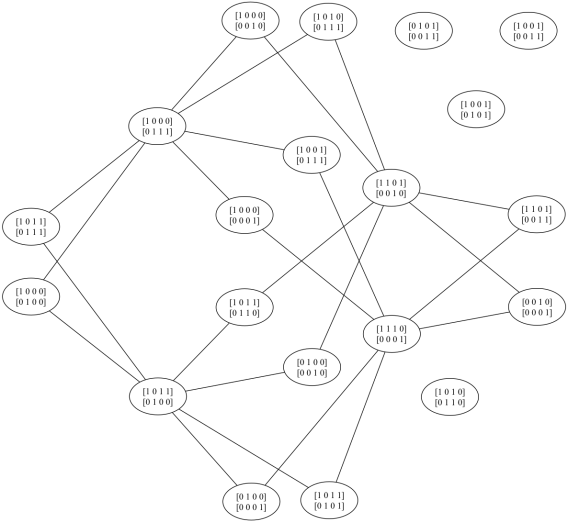
- $|V|$ *as before*
- *It is generally (for non-trivial* $1 < k < n-1$*)*
  - *not regular,*
  - *not vertex-transitive,*
  - *not edge-transitive,*

LCD Neighbor Graph in $\mathbb{F}_2^4$



— non-associated neighbors — associated neighbors

LCD Associated Neighbor Graph in $\mathbb{F}_2^4$



Summary and Outlook

- LCD codes have many applications in coding theory and cryptography.
- Open problems include finding good codes for $q = 2, 3$ and classifying them. $\Longrightarrow$ tackle with LCD neighbor graphs!
- Associated neighbors are easy to compute and define a subgraph of the neighbor graph.
- **Main results:** The $[n, k]_q$ LCD neighbor graph
  - is regular and connected
  - has diameter $\min\{k, n-k\}$ for odd q and girth 3.

  The associated neighbor graph is undirected (in the general case) and otherwise not very structured.
- **Ongoing work:** Count triangles, determine $|E|$ in associated neighbor graph, use cliques for classification, use Hermitian inner product, etc.

Thank you for your attention!

Questions? – Comments?