The Neighbor Graph of Linear Complementary Dual Codes

Marc Newman and Anna-Lena Horlemann

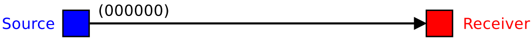
University of St.Gallen, Switzerland

Workshop on Coding Theory and Combinatorics
University of Queensland
April 3rd 2025

Joint work with Carlos Vela, Javier de la Cruz and Wolfgang Willems,
supported by the Leading House Latin America Research Partnership Grant no. RPG2352.

Idea of Error-Correcting Codes

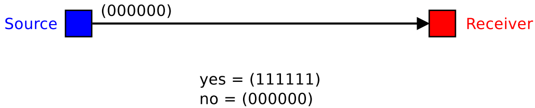
- Communication channels introduce errors due to noise.
- Question: How to encode/decode messages to recover from errors?



yes = (111111)
no = (000000)

Idea of Error-Correcting Codes

- Communication channels introduce errors due to noise.
- Question: How to encode/decode messages to recover from errors?

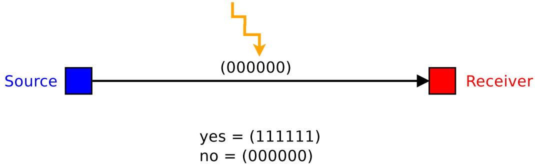


Idea: Add redundancy to protect against errors.

- Example: repetition code – encode information b as (b, b, b).
- If one coordinate is erroneous, majority decoding recovers the data.
- ”Smarter” approaches achieve better efficiency and error tolerance.

Idea of Error-Correcting Codes

- Communication channels introduce errors due to noise.
- Question: How to encode/decode messages to recover from errors?

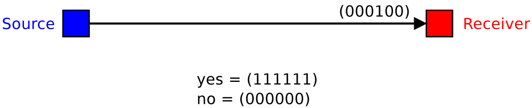


Idea: Add redundancy to protect against errors.

- Example: repetition code – encode information b as (b, b, b).
- If one coordinate is erroneous, majority decoding recovers the data.
- "Smarter" approaches achieve better efficiency and error tolerance.

Idea of Error-Correcting Codes

- Communication channels introduce errors due to noise.
- Question: How to encode/decode messages to recover from errors?

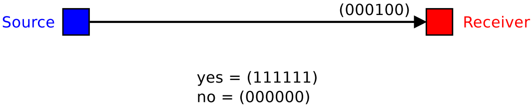


Idea: Add redundancy to protect against errors.

- Example: repetition code – encode information b as (b, b, b).
- If one coordinate is erroneous, majority decoding recovers the data.
- ”Smarter” approaches achieve better efficiency and error tolerance.

Idea of Error-Correcting Codes

- Communication channels introduce errors due to noise.
- Question: How to encode/decode messages to recover from errors?



Idea: Add redundancy to protect against errors.

- Example: repetition code – encode information b as (b, b, b).
- If one coordinate is erroneous, majority decoding recovers the data.
- ”Smarter” approaches achieve better efficiency and error tolerance.

$\boxed{\text{Coding theory} \cong \text{algorithmic approach to finite metric spaces}}$

Linear Codes

Definition

- A q-ary *linear code* 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 $n - k$.

Linear Codes

Definition

- A q-ary *linear code* 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 $n - k$.

- Such a code is denoted as an $[n, k]_q$ code.
- It can be represented by a *generator matrix* $G \in \mathbb{F}_q^{k \times n}$.
- $C = \{mG \mid m \in \mathbb{F}_q^k\}$, where m is a message vector.
- If H is generator matrix of $C^\perp$, then

$$C = \{y \in \mathbb{F}_q^n \mid Hy^\top = 0\}.$$

It is also called the *parity-check matrix* of C.

Hamming Distance

- 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:

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

- Determines error-detecting and error-correcting capability:
  - Detects up to $d - 1$ errors.
  - Corrects up to $\lfloor (d-1)/2 \rfloor$ errors.

Hamming Distance

- 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:

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

- Determines error-detecting and error-correcting capability:
  - Detects up to $d - 1$ errors.
  - Corrects up to $\lfloor (d-1)/2 \rfloor$ errors.

Other metrics

Depending on the application also other metrics, such as the *Lee* or *rank metric*, are used.

Linear Complementary Dual (LCD) Codes

Definition

A linear code $C \subset \mathbb{F}_q^n$ is an *LCD code* 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.

Linear Complementary Dual (LCD) Codes

Definition

A linear code $C \subset \mathbb{F}_q^n$ is an *LCD code* 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

LCD as Regular Subspaces

- LCD codes are exactly the *regular* subspaces w.r.t. $\langle , \rangle$.
  $\implies$ can use Gram-Schmidt to get orthogonal bases

LCD as Regular Subspaces

- LCD codes are exactly the *regular* subspaces w.r.t. $\langle , \rangle$.
  $\implies$ can use Gram-Schmidt to get orthogonal bases
- Over $\mathbb{F}_2$ a linear code is LCD $\iff$ it has an orthonormal or symplectic basis.
- In odd characteristic a linear code is LCD $\iff$ it has an "almost" orthonormal basis, where one basis vector can also have norm a quadratic non-residue.

Orthogonal Group Action

The linear automorphism group of $LCD[n,k]_q$ is the full (general) orthogonal group.

$$LCD[n,k]_q \times O(n,q) \longrightarrow LCD[n,k]_q$$

For q **even:**

- The space $LCD[n,k]_q$ is split into one, two, or three orbits under $O(n,q)$ (depending on parities of k,n).

For q **odd:**

- The space $LCD[n,k]_q$ is split into two orbits under $O(n,q)$, corresponding to square and non-square determinants.

— Applications of LCD Codes —

Entanglement Assisted Quantum Error Correcting Codes (EAQECC) from LCD Codes

Theorem

Let H_1 and H_2 be parity check matrices of two linear codes $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively. Then an

$$[[n, k_1 + k_2 - n + c, \min\{d_1, d_2\}; c]]_q$$

EAQECC can be obtained where $c := \operatorname{rank}(H_1 H_2^\top)$ is the required number of maximally entangled states.

The information rate is maximized for $c = n - k$, which means that the codes are complementary duals. If you choose both codes to be the same code, then the quantum distance is equal to the classical distance, and maximal entanglement means that the code is LCD.

Decoding with LCD Codes

The nearest-codeword decoding problem for an LCD code reduces to the (apparently) simpler problem: given a word in the dual code, find the nearest codeword in the code.

Theorem

Let C be an $[n,k]_q$ LCD code and let Q be a mapping that maps each $u \in C^\perp$ to (one of) the closest codeword(s) v in C. Then there is an easily computable mapping that maps each $r \in \mathbb{F}_q^n$ to (one of) the closest codeword(s) v in C.

LCD Codes and Side Channel + Fault Injection Attacks

- **Orthogonal Direct Sum Masking (ODSM):**

$$\underbrace{\text{information}}_{\in U \leq \mathbb{F}_q^n} + \underbrace{\text{random mask}}_{\in \mathbb{F}_q^n \ominus U}$$

  - Use mask to hide data from eavesdroppers (on side channel).
  - For unique representation (decomposition): mask from "supplementary" subspace

- **Orthogonal Direct Sum Masking (ODSM):**

$$\underbrace{\text{information}}_{\in U \leq \mathbb{F}_q^n} + \underbrace{\text{random mask}}_{\in \mathbb{F}_q^n \ominus U}$$

  - Use mask to hide data from eavesdroppers (on side channel).
  - For unique representation (decomposition): mask from "supplementary" subspace
- To also have resistance against FIA, we need a large minimum Hamming distance of the code.

LCD Codes and Side Channel + Fault Injection Attacks

- **Orthogonal Direct Sum Masking (ODSM):**

$$\underbrace{\text{information}}_{\in C_{LCD}} + \underbrace{\text{random mask}}_{\in C_{LCD}^{\perp}}$$

  - Use mask to hide data from eavesdroppers (on side channel).
  - For unique representation (decomposition): mask from "supplementary" subspace
- To also have resistance against FIA, we need a large minimum Hamming distance of the code.
- $\implies C$ LCD with high minimum distance simultaneously improves the resistance against SCA and FIA.

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 $q \geq 4$.

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

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 $q \geq 4$.
  $\implies$ 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.

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.

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 $k-1$.

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

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

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:

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

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

Associated Neighborship is not Symmetric

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

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

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

-

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

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

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 $v' \in C'$, $C'_0(v') \neq C \cap C'$.

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

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*

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

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

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*

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

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

Note:

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

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

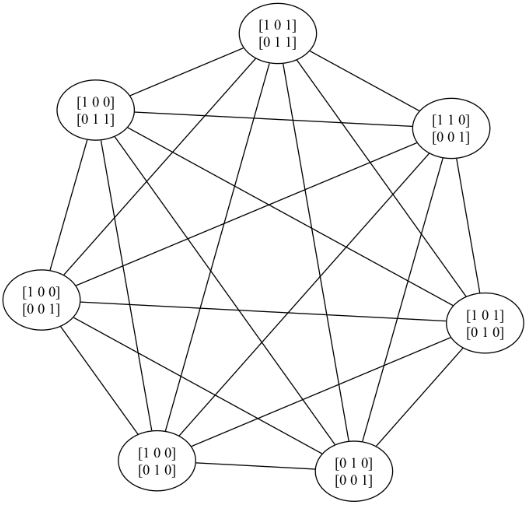
$$C^\perp = N(C'^\perp, u - v)$$

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

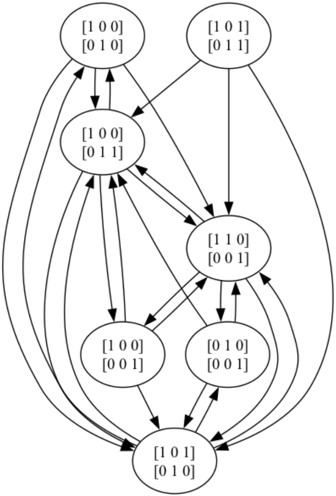
Neighborship as a Graph

- 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 $\mathbb{F}_2^3$

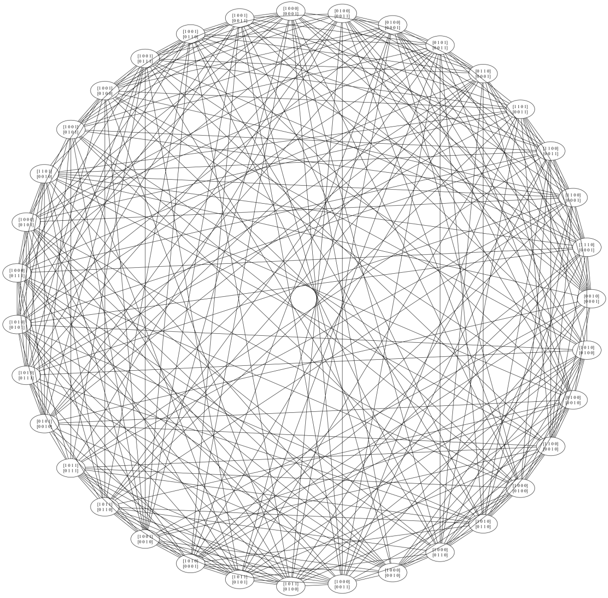


neighbors

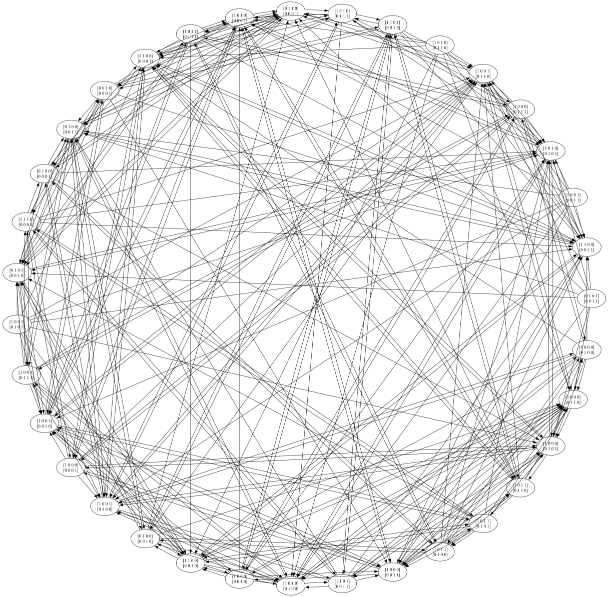


associated neighbors

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.

Lemmas for the Proof

Lemma

Let $U \subseteq \mathbb{F}_q^n$ be a k-dimensional subspace.

1. *If q is even, then either U contains only self-orthogonal vectors, or it contains q^{k-1} many self-orthogonal vectors (including zero).*
2. *If q is odd, then U contains*

$$\begin{cases} q^{k-1} & \text{if } k \text{ is odd,} \\ q^{k-1} + \frac{q-1}{q}\left(\frac{\det Q}{q}\right)\left(\frac{-1}{q}\right)^{k/2} q^{k/2} & \text{if } k \text{ is even,} \end{cases}$$

   many self-orthogonal vectors, including the zero vector, where Q denotes the quadratic form in k variables describing the subset of self-orthogonal vectors in U.

Lemmas for the Proof

Lemma

Let q be odd. Then

$$\sum_{x \in \mathbb{P}(\mathbb{F}_q^k)} \left(\frac{\langle x, x \rangle)}{q} \right) = \begin{cases} q^{\frac{k-1}{2}} & \textit{if } k \textit{ is odd,} \\ 0 & \textit{if } k \textit{ is even.} \end{cases}$$

Proof idea:

- $\left(\frac{\langle \lambda x, \lambda x \rangle)}{q} \right) = \left(\frac{\langle x, x \rangle)}{q} \right)$, because of bilinearity.
- $\langle x, x \rangle$ as quadratic form has known number of $x \in \mathbb{F}_q^k$ that results in a fixed $c \in \mathbb{F}_q$.
- Half of these $c \neq 0$ are quadratic residues, the other half are not.
- Summing up gives result.

Proof of Theorem

We distinguish two cases:

- <u>U is LCD:</u> In this case, $U^\perp = \mathbb{F}_q^n/U$, and only a self-orthogonal one-dimensional subspace will lead to a non-LCD neighbor. Applying the first lemma, there are that many choices for LCD:

$$\begin{cases} q^{n-k} - 1 & q \text{ even or } n-k \text{ even} \\ q^{n-k} - 1 - \left(\frac{\det Q}{q}\right)\left(\frac{-1}{q}\right)^{(n-k+1)/2} q^{(n-k-1)/2} & \text{else} \end{cases}$$

- <u>U is not LCD:</u> In this case all cosets corresponding to an element in $U^\perp \cap (\mathbb{F}_q^n/U)$ (dimension $n-k$) lead to a non-LCD neighbor. Hence we have

$$\frac{q^{n-k+1}-1}{q-1} - \frac{q^{n-k}-1}{q-1} - 1 = q^{n-k} - 1$$

many cosets that give rise to an LCD neighbor.

Proof of Theorem

Summing up over all possible U:

- If q even or $n-k$ even:

$$\frac{(q^k-1)(q^{n-k}-1)}{q-1} = \frac{q-1}{q}N$$

- Else:

$$\frac{(q^k-1)(q^{n-k}-1)}{q-1} - \sum_{U\leq C, \dim U = k-1} \left(\frac{\det Q_U}{q}\right)\left(\frac{-1}{q}\right)^{\frac{n-k+1}{2}} q^{\frac{n-k-1}{2}}$$

$$= \tfrac{q-1}{q}N - \left(\frac{-1}{q}\right)^{\frac{n-k+1}{2}} q^{\frac{n-k-1}{2}} \sum_{U^\perp \geq C^\perp, \dim U^\perp = n-k+1} \left(\frac{\det Q_U}{q}\right)$$

$$= \tfrac{q-1}{q}N - \left(\frac{-1}{q}\right)^{\frac{n-k+1}{2}} q^{\frac{n-k-1}{2}} \sum_{x\in\mathbb{P}(\mathbb{F}_q^k)} \left(\frac{\langle x, x\rangle}{q}\right),$$

to which we can apply the second lemma.

Recap

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 $\min(k, n-k)$.

Connectedness and Diameter

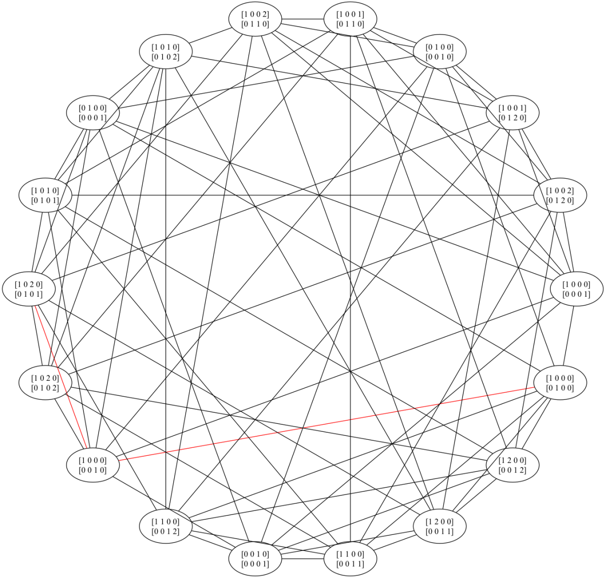
Theorem

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

Proof idea:

- If $k \leq \frac{n}{2}$, two non-intersecting codes must have distance $\geq k$.
- Use Householder reflections as generators of $O(n, q)$ to get from any node to another in $\leq k$ neighbor steps.

Example: Connectedness and Diameter



Example: Connectedness and Diameter

$$C_0 : \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad C_1 : \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad C_2 : \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 \\ 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

The Associated Neighbor Graph of LCD Codes

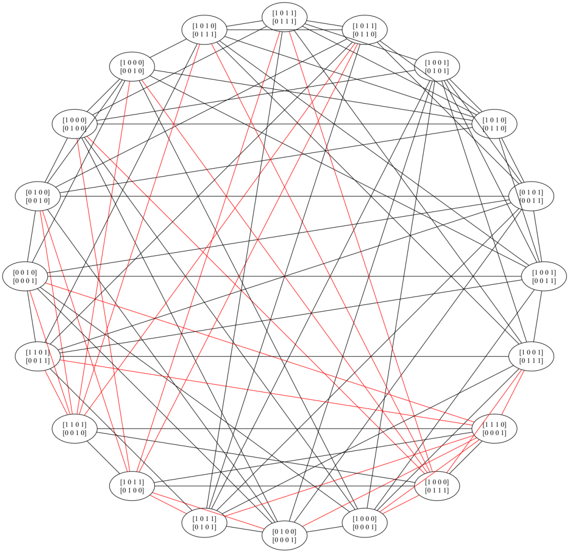
Remember: The graph can be represented as an undirected graph, by collapsing all pairs of directed edges with the same two vertices.

Theorem

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

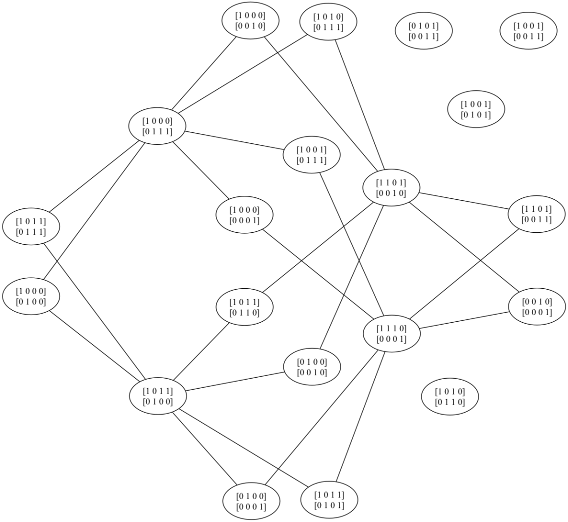
- $|V|$ *as before*
- *It is generally (for non-trivial* $1 < k < n-1$*)*
  - *not regular,*
  - *not vertex-transitive,*
  - *not edge-transitive,*
  - *and hence not symmetric.*

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

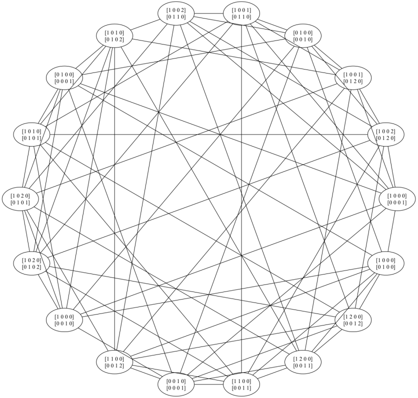


— non-associated neighbors — associated neighbors

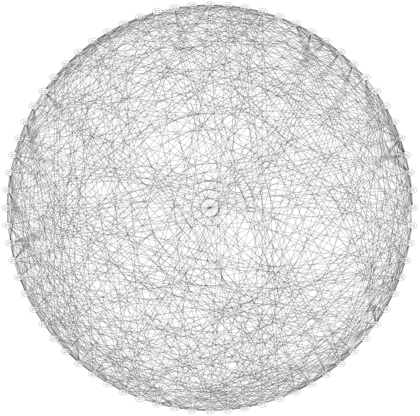
LCD Associated Neighbor Graph in $\mathbb{F}_2^4$



LCD Householder Neighbor Graph in $\mathbb{F}_3^4$



18 vertices, 8-regular



72 vertices, 26-regular

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!

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. $\implies$ tackle with LCD neighbor graphs!
- Associated neighbors are easy to compute and define a subgraph of the neighbor graph.

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. $\implies$ 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.

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.

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. $\implies$ 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?