LCD codes over $\mathbb{F}_q$ are as good as linear codes for q at least four

Ruud Pellikaan
g.r.pellikaan@tue.nl

International Conference on Graph Theory and Information Security
ICGTIS, August 7, 2017
Universitas Indonesia, Depok, Indonesia

Content

1. Error-correcting codes
   - Parameters of a code
   - Generator and parity check matrix of a linear code
2. LCD codes
   - Inner product and dual code
   - Hull of a code and linear codes with complementary dual (LCD)
   - Permutational, scalar and monomial equivalence
3. Applications
   - Two-user binary adder channel (2-BAC)
   - Side channel attack (SCA) and Fault Injection Attack (FIA)
4. Proof Main Theorem
   - Theory of Gröbner bases
   - Proof
5. Conclusion

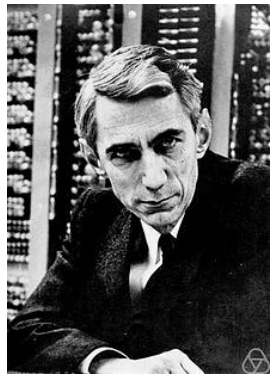
Error-correcting codes

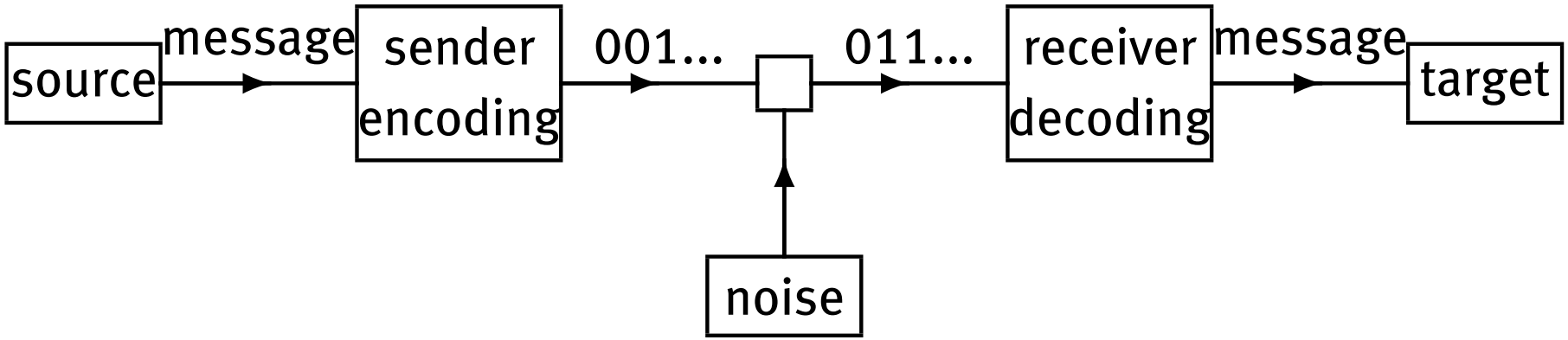
Error-correcting codes

TYPE OF CODE	REED-SOLOMON	LOW-DENSITY PARITY-CHECK (LDPC)	TURBO
APPLICA-TIONS	 DATA STORAGE (CD/DVD)	 WIFI, BROADCASTING	 CELLULAR (3G, 4G), SATELLITE COMMUNICATIONS

Communication: internet, telephone, WiFi, computer
Memory: computer, compact disc, DVD, USB stick
Barcodes, ISBN, product codes, QR codes ...

Information theory - Shannon

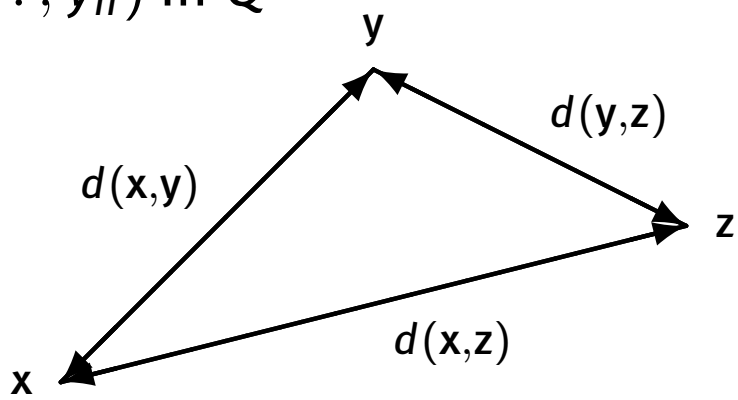




Hamming distance

Q alphabet of q elements

Hamming distance $d(\mathbf{x}, \mathbf{y}) = |\{i \mid x_i \neq y_i\}|$
between $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ in Q^n



Triangle inequality

Block codes

C is called (block) code if it is a subset of Q^n
The minimum distance of C is:

$$d(C) = \min \{ d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y} \}$$

parameters of C are $(n, M, d)_q$ or (n, M, d)

q	$=$	$\lvert Q \rvert$	$=$	size of alphabet Q
n	$=$			length of C
M	$=$	$\lvert C \rvert$	$=$	size of C
d	$=$	$d(C)$	$=$	minimum distance of C

Linear codes and their parameters

$\mathbb{F}_q$ the finite field with $q = p^e$ elements and p prime
$\mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear vector space of dimension n

A linear code is an $\mathbb{F}_q$-linear subspace C of $\mathbb{F}_q^n$
with parameters $[n, k, d]_q$ or $[n, k, d]$ or $[n, k]$

q = size finite field
n = length of C
k = dimension of C
d = minimum distance of C

r = redundancy of $C = n - k$

Generator matrix

Let C be an $[n, k]$ linear code over $\mathbb{F}_q$

Then G is a generator matrix of C if it is a $k \times n$ matrix with entries in $\mathbb{F}_q$ such that its rows are a basis of C

Let $\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$ be a message
Then $\mathbf{c} = \mathbf{m}G$ is a codeword

$$\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

Encoding

$$\mathbf{m} \mapsto \mathbf{m}G = \mathbf{c}$$

So C is the image of $\mathbb{F}_q^k$ under G

Parity check matrix

Let C be an $[n, k]$ linear code over $\mathbb{F}_q$

Then H is called a parity check matrix of C if it is a $(n-k) \times n$ matrix with entries in $\mathbb{F}_q$ such that $\mathbf{r} \in C$ if and only if $\mathbf{r}H^T = 0$

$$\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$$

$$\mathbf{r} \mapsto \mathbf{r}H^T$$

$\mathbf{r} \in C$ if and only if syndrome $\mathbf{c}H^T$ is zero
So C is left kernel (null space) of H^T

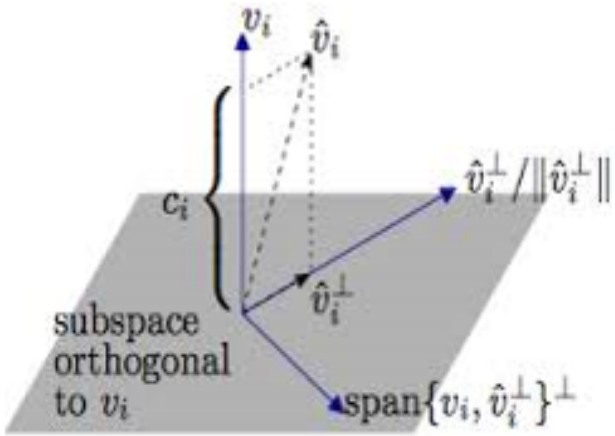
LCD codes

Inner product

The standard inner product is defined by

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \cdots + a_n b_n$$

Is bilinear and non-degenerate but positive definite makes no sense



not right picture

Vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ are perpendicular denoted by $\mathbf{a} \perp \mathbf{b}$ if and only if $\mathbf{a} \cdot \mathbf{b} = 0$

Dual code

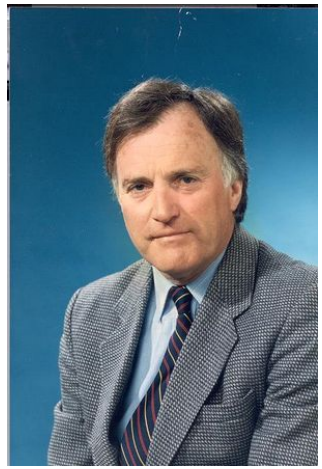
Let C be a linear code in $\mathbb{F}_q^n$
The dual code is defined by

$$C^{\perp} = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C \}$$

PROPOSITION

Let C be an $[n, k]$ code with generator matrix G
Then $C^{\perp}$ is an $[n, n-k]$ code with G as parity check matrix

LCD codes - Massey 1992



The code C is called linear with complementary dual (LCD) if

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

PROPOSITION
(1992 Massey) LCD codes are asymptotically good
(2004 Sendrier) LCD codes meet the Gilbert-Varshamov bound

Hull of a code

The hull of an $\mathbb{F}_q$-linear code C is defined by

$$H(C) = C \cap C^{\perp}$$

Hence
C is LCD if and only if $H(C) = \{0\}$

Dimension of the hull

PROPOSITION

Let C be an $\mathbb{F}_q$-linear $[n, k]$ code
Let h be the dimension of $H(C)$ and $r = k - h$
Then C has a generator matrix G_0 such that

$$G_0 G_0^T = \left(\begin{array}{c|c} O_{h\times h} & O_{h\times r} \\ \hline O_{r\times h} & P \end{array} \right),$$

where $O_{l\times m}$ is the all zeros $l \times m$ matrix and
P is an invertible $r \times r$ matrix

Furthermore the rank of $G_1 G_1^T$ is r for every generator matrix G_1 of C

COROLLARY

Let C be an $\mathbb{F}_q$-linear $[n, k]$ code with generator matrix G
Then the following statements are equivalent:

- C is LCD
- $C \cap C^{\perp} = \{0\}$
- GG^T has rank k
- GG^T is invertible

Example - Hamming code

Let C be the binary $[7, 4, 3]$ Hamming code with generator matrix

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Then

$$G_1 G_1^T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$ has rank 1

Hence $H(C)$ has dimension 3

Example - Hamming code

Now C has another generator matrix

$$G_0 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

with

$$G_0 G_0^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Permutational, diagonal and monomial matrices

- A permutation matrix is a square matrix with zeros and ones such that in every row (and in every column) there is exactly one element equal to one
- A diagonal matrix is a square matrix with zeros outside its diagonal
- A monomial matrix is a square matrix such that in every row (and in every column) there is exactly one nonzero element

A permutation matrix and an invertible diagonal matrix are special monomial matrices

Permutational, scalar and monomial equivalent

Let C_1 and C_2 be $\mathbb{F}_q$-linear codes of length n
Then C_1 and C_2 are called

- permutational equivalent
  if there exists a permutation matrix P such that $C_1 P = C_2$
- diagonal equivalent
  if there exists an invertible diagonal matrix D such that $C_1 D = C_2$
- linear equivalent or monomial equivalent
  if there exists a monomial matrix M such that $C_1 M = C_2$

Dimension of the hull under equivalence

The dimension of the hull of a code is

- invariant under permutational equivalence
- also invariant under monomial equivalence if $q = 2, 3$
- can be computed with the (extended) weight enumerator
- is used to find the permutation in case C_1 and C_2 are permutational equivalent
- is not a monomial equivalence invariant if $q \geq 4$

Applications

Two-user binary adder channel (2-BAC)

Let $x, y \in \mathbb{F}_2$
Define $x \oplus y \in \mathbb{Z}$ by

x	y	$x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	2

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$
Define

$$\mathbf{x} \oplus \mathbf{y} = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)$$

Unique decodable

Let C and D be $\mathbb{F}_q$-linear codes of length n
Define

$$C \times D = \{ (\mathbf{c}, \mathbf{d}) \mid \mathbf{c} \in C, \mathbf{d} \in D \}$$

$$C \oplus D = \{ \mathbf{c} \oplus \mathbf{d} \mid \mathbf{c} \in C, \mathbf{d} \in D \}$$

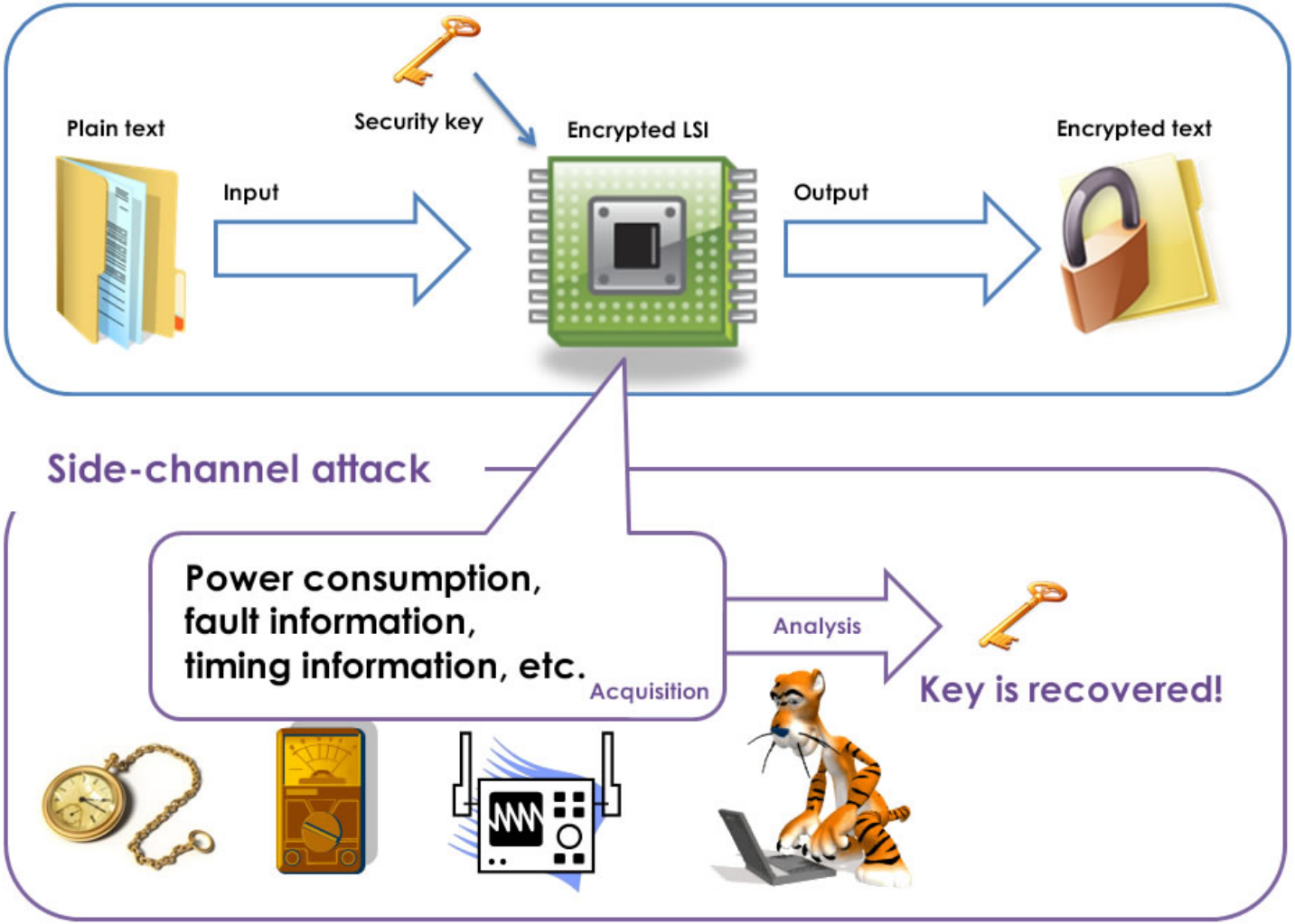
$C \oplus D$ is called unique decodable if the map

$$C \times D \to C \oplus D \text{ given by } (\mathbf{c}, \mathbf{d}) \mapsto \mathbf{c} \oplus \mathbf{d}$$

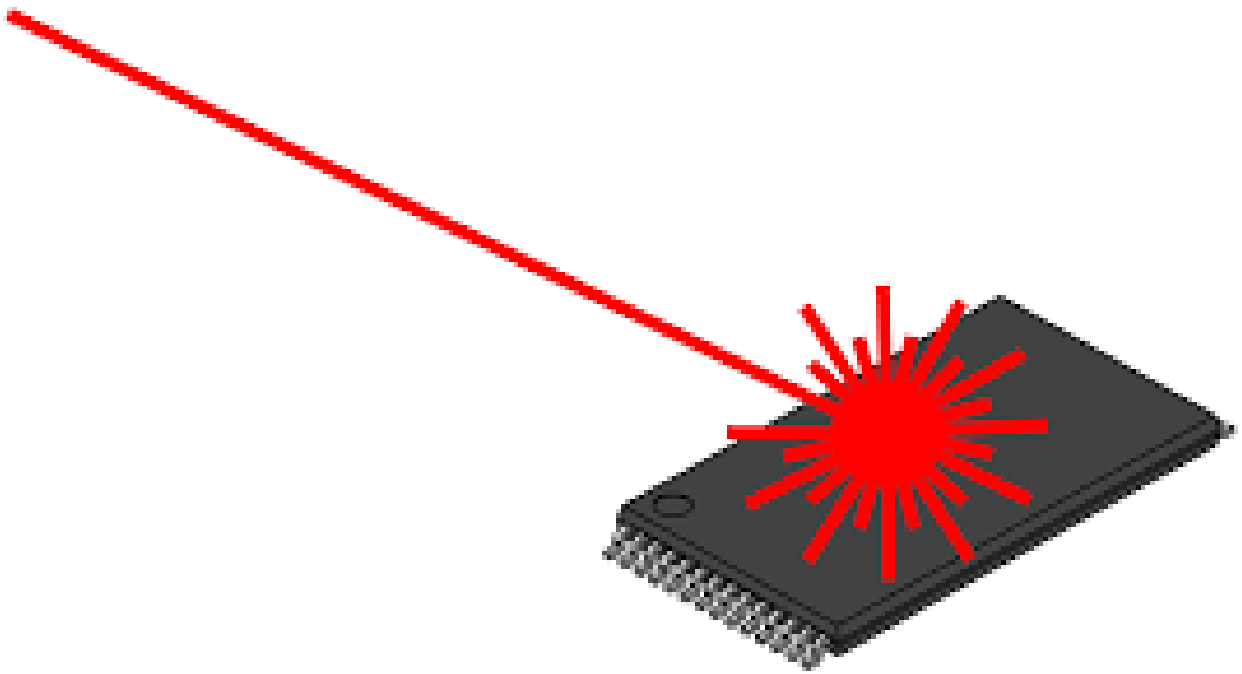
is injective

$C \oplus D$ is unique decodable if and only if $C \cap D = \{0\}$
Hence
$C \oplus C^{\perp}$ is unique decodable if and only if C is LCD

Side Channel Attack (SCA)



Fault Injection Attack (FIA)



Orthogonally Direct Sum Masking (ODSM)

Carlet and Guilley (2014)

Let C and D be $\mathbb{F}_q$-linear codes of length n
Define

$$C + D = \{ \mathbf{c} + \mathbf{d} \mid \mathbf{c} \in C, \mathbf{d} \in D \}$$

If $C \cap D = \{0\}$ then $C + D$ is denoted by $C \uplus D$

Then
$C \uplus D = \mathbb{F}_q^n$ if and only if $C \cap D = \{0\}$ and $\dim C + \dim D = n$

Hence
$C \uplus C^\perp = \mathbb{F}_q^n$ if and only if C is LCD

Main Theorem

Star product

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$
Then the star product is defined by

$$\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n)$$

Let $\mathbf{x} \in \mathbb{F}_q^n$ have nonzero entries
Define

$$\mathbf{x}^{-1} = (x_1^{-1}, \ldots, x_n^{-1})$$

Let $C \subseteq \mathbb{F}_q^n$
Define

$$\mathbf{x} * C = \{ \mathbf{x} * \mathbf{c} \mid \mathbf{c} \in C \}$$

C_1 and C_2 are scalar equivalent if and only if
there exists an $\mathbf{x}$ with nonzero entries such that $C_2 = \mathbf{x} * C_1$

LCD codes are good

THEOREM (2017 Carlet-Mesnager-Tang-Qi-P)

If $q \geq 4$ and C is an $\mathbb{F}_q$-linear code
Then there exits an $\mathbf{x} \in \mathbb{F}_q^n$ with nonzero entries
such that $\mathbf{x} * C$ is an LCD code

Hence
LCD codes over $\mathbb{F}_q$ are as good as $\mathbb{F}_q$-linear codes if $q \geq 4$

LCD codes are good

THEOREM (2017 Carlet-Mesnager-Tang-Qi-P)

If $q \geq 4$ and C is an $\mathbb{F}_q$-linear code
Then there eixts an $\mathbf{x} \in \mathbb{F}_q^n$ with nonzero entries
such that $\mathbf{x} * C$ is an LCD code

Hence
LCD codes over $\mathbb{F}_q$ are as good as $\mathbb{F}_q$-linear codes if $q \geq 4$

PROPOSITION
Let $f(X)$ be a nonzero polynomial of $\mathbb{F}_q[X_1, \ldots, X_n]$
such that the degree of $f(X)$ with respect to X_j is at most $q-1$ for all j
Then there exists a $\mathbf{x} \in \mathbb{F}_q^n$ such that $f(\mathbf{x}) \neq 0$

PROPOSITION
Let $f(X)$ be a nonzero polynomial of $\mathbb{F}_q[X_1, \ldots, X_n]$
such that the degree of $f(X)$ with respect to X_j is at most $q-2$ for all j
Then there exists a $\mathbf{x} \in \mathbb{F}_q^n$ with nonzero entries such that $f(\mathbf{x}) \neq 0$

Proof

We may assume that C has a generator matrix of the form $G = (I_k | B)$
Let $\mathbf{x} = (x_1, \ldots, x_k)$ be an k-tuple of nonzero elements of $\mathbb{F}_q$
Let $D(\mathbf{x})$ be the diagonal matrix with $\mathbf{x}$ on its diagonal
Let $G_{\mathbf{x}} = (D(\mathbf{x})|B)$ be the generator matrix of the code $C_{\mathbf{x}}$
Then $C_{\mathbf{x}}$ is monomial equivalent with C
Now

$$\det(G_{\mathbf{x}} G_{\mathbf{x}}^T) = \det(D(x_1^2, \ldots, x_k^2) + BB^T)$$

is a polynomial in $x_1, \ldots, x_k$
Its degree with respect to x_i is 2 for all i
which is at most $q - 2$, since $q \geq 4$
Hence there exists a $\mathbf{x} \in \mathbb{F}_q^n$ with nonzero entries
such that $\det G_{\mathbf{x}} G_{\mathbf{x}}^T \neq 0$
So $G_{\mathbf{x}} G_{\mathbf{x}}^T$ is invertible
Therefore $C_{\mathbf{x}}$ is LCD

Thank you