Code-Based Cryptography

Error-Correcting Codes and Cryptography

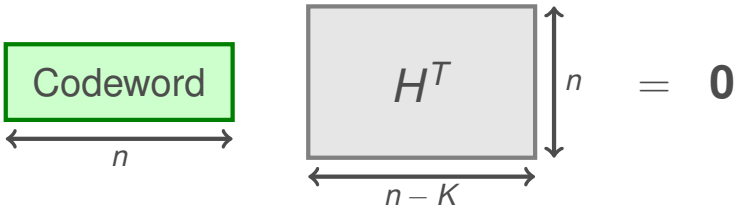
I. Márquez-Corbella

informatiques mathématiques

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. **Parity Checking**
5. Error Correcting Capacity
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. McEliece Cryptosystem

Parity Check Matrix



Parity check matrix

Let $\mathcal{C}$ be an $[n, k]_q$ code.

H is a **parity check matrix** of $\mathcal{C}$ $\iff$ $\mathcal{C}$ is the **null space** of H

That is:

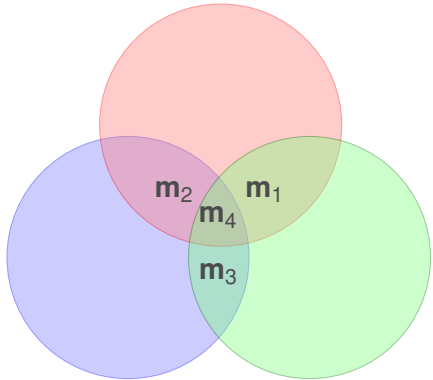
$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H^T = 0\}$$

[7,4]-Hamming code

$$\underbrace{(m_1, m_2, m_3, m_4)}_{\text{Information bits}}$$

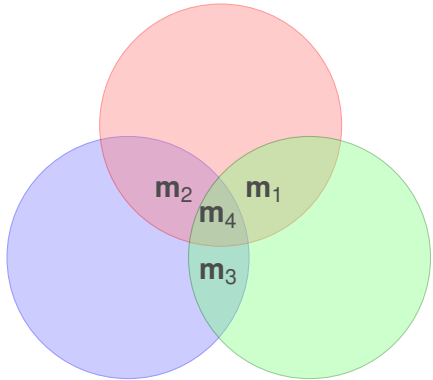
[7,4]-Hamming code

$$\underbrace{(m_1, m_2, m_3, m_4)}_{\text{Information bits}}$$



[7,4]-Hamming code

$$\underbrace{(m_1, m_2, m_3, m_4)}_{\text{Information bits}}$$

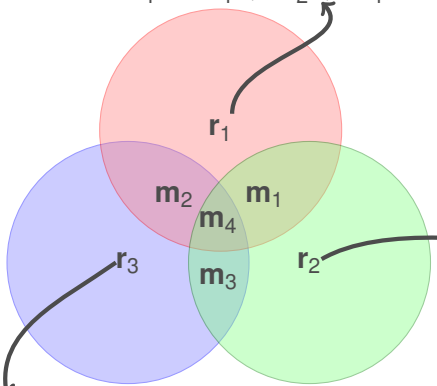


The number of ones
in every circle is even

[7,4]-Hamming code

$\underbrace{(m_1, m_2, m_3, m_4)}_{\text{Information bits}}$

$\mathbf{r}_1 = \mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_4 \mod 2$



The number of ones in every circle is even

$\mathbf{r}_2 = \mathbf{m}_1 + \mathbf{m}_3 + \mathbf{m}_4 \mod 2$

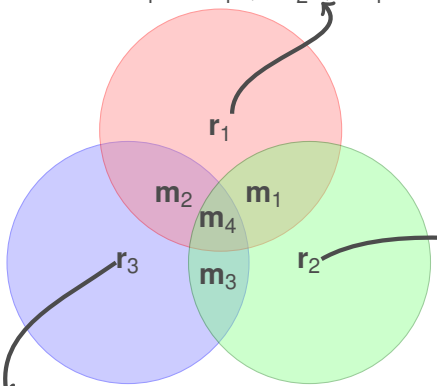
$\mathbf{r}_3 = \mathbf{m}_2 + \mathbf{m}_3 + \mathbf{m}_4 \mod 2$

[7,4]-Hamming code

$\underbrace{(m_1, m_2, m_3, m_4)}$ Information bits

$\underbrace{(r_1, r_2, r_3)}$ Redundant bits

$\mathbf{r}_1 = \mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_4 \mod 2$



The number of ones in every circle is even

$\mathbf{r}_2 = \mathbf{m}_1 + \mathbf{m}_3 + \mathbf{m}_4 \mod 2$

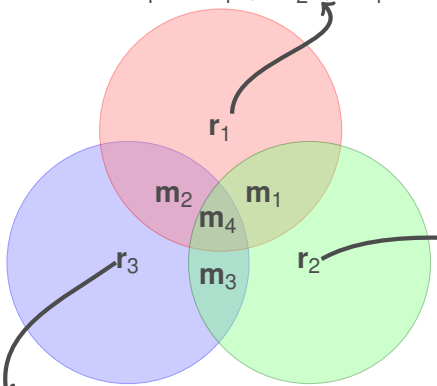
$\mathbf{r}_3 = \mathbf{m}_2 + \mathbf{m}_3 + \mathbf{m}_4 \mod 2$

[7,4]-Hamming code

$\underbrace{(m_1, m_2, m_3, m_4)}_{\text{Information bits}}$ $\underbrace{(r_1, r_2, r_3)}_{\text{Redundant bits}}$

$\mathbf{r}_1 = \mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_4 \mod 2$

The number of ones in every circle is even



$\mathbf{r}_2 = \mathbf{m}_1 + \mathbf{m}_3 + \mathbf{m}_4 \mod 2$

$\mathbf{r}_3 = \mathbf{m}_2 + \mathbf{m}_3 + \mathbf{m}_4 \mod 2$

[7,4]-Hamming code

The **redundant information** can be obtained from the message by 3 **parity checks**:

$$\begin{cases} \mathbf{r}_1 &= \mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_4 \\ \mathbf{r}_2 &= \mathbf{m}_1 + \mathbf{m}_3 + \mathbf{m}_4 \\ \mathbf{r}_3 &= \mathbf{m}_2 + \mathbf{m}_3 + \mathbf{m}_4 \end{cases}$$

[7,4]-Hamming code

The **redundant information** can be obtained from the message by 3 **parity checks**:

$$\begin{cases} \mathbf{r}_1 &= \mathbf{m}_1 + \mathbf{m}_2 + \mathbf{m}_4 \\ \mathbf{r}_2 &= \mathbf{m}_1 + \mathbf{m}_3 + \mathbf{m}_4 \\ \mathbf{r}_3 &= \mathbf{m}_2 + \mathbf{m}_3 + \mathbf{m}_4 \end{cases}$$

$\mathbf{c} = (\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_4)$ is a codeword $\iff$ $H\mathbf{c}^T = 0$

with $H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 7}$

Binary Hamming Codes

Binary Hamming Codes

$H \in \mathbb{F}_2^{r \times 2^r - 1}$ such that H contains **all** nonzero binary r-tuples **exactly once** as a column

Binary Hamming Codes

Binary Hamming Codes

$H \in \mathbb{F}_2^{r \times 2^r - 1}$ such that H contains **all** nonzero binary r-tuples **exactly once** as a column

Any code with H as parity-check matrix is a **binary Hamming code** of redundancy r.

Binary Hamming Codes

Binary Hamming Codes

$H \in \mathbb{F}_2^{r \times 2^r - 1}$ such that H contains **all** nonzero binary r-tuples **exactly once** as a column

Any code with H as parity-check matrix is a **binary Hamming code** of redundancy r.

Binary Hamming codes correct up to 1 error.

Parity Check Matrix

A code can have more than one parity-check matrix!

Parity Check Matrix

A code can have more than one parity-check matrix!

Proposition: Characterization of a parity-check matrix

Let $\mathcal{C}$ be an $[n, k]_q$ code with generator matrix G

$$H \text{ is a parity check-matrix of } \mathcal{C} \iff GH^T = 0$$

Proof:

From the definition of parity check matrix: $\mathbf{c}H^T = \mathbf{0}$, for all $\mathbf{c} \in \mathcal{C}$

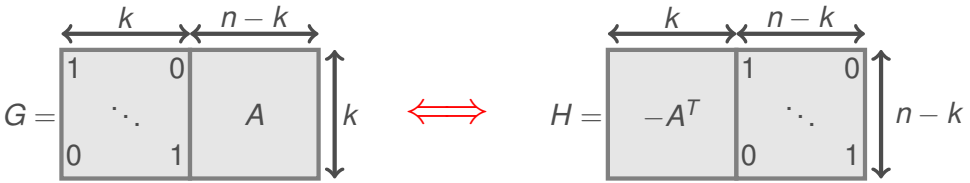
Recall that every codeword is of the form: $\mathbf{c} = \mathbf{m}G$ with $\mathbf{m} \in \mathbb{F}_q^k$

Thus, $(\mathbf{m}G)\, H^T = \mathbf{0}$, for all $\mathbf{m} \in \mathbb{F}_q^k$

And we conclude that $GH^T = 0$

Parity Check Matrix

Proposition: How to get a parity check-matrix?



is a generator matrix for $\mathcal{C}$ ⟺ is a parity-check matrix for $\mathcal{C}$

Proof:

"$\Longrightarrow$" We clearly have $HG^T = 0 = -A^T + A^T$
Thus, $\mathcal{C} \subseteq \ker(H)$
Since $\mathrm{rank}(H) = n - k \implies \dim(\ker(H)) = k = \dim(\mathcal{C})$
Hence, H is a parity check matrix for $\mathcal{C}$

"$\Longleftarrow$" The converse is proved similarly.

Dual Code

G is a generator matrix for $\mathcal{C}$ $\iff$ H is a generator matrix for $\mathcal{C}^{\perp}$

The dual code

Let $\mathcal{C}$ be an $[n, k]_q$ code. We define the **dual code** $\mathcal{C}^{\perp}$ as

$$\mathcal{C}^{\perp} = \{\mathbf{x} \in \mathbf{F}_q^n \mid \mathbf{x} \cdot \quad \mathbf{c} = 0\ ,\ \forall \mathbf{c} \in \mathcal{C}\}$$

Dual Code

G is a generator matrix for $\mathcal{C}$ $\iff$ H is a generator matrix for $\mathcal{C}^{\perp}$

The dual code

Let $\mathcal{C}$ be an $[n,k]_q$ code. We define the **dual code** $\mathcal{C}^{\perp}$ as

$$\mathcal{C}^{\perp} = \{\mathbf{x} \in \mathbf{F}_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0\,,\ \forall \mathbf{c} \in \mathcal{C}\}$$

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ the **inner product** is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n = \sum_{i=1}^{n} x_i y_i$$

Dual Code

Proposition:

Let $\mathcal{C}$ be an $[n, k]_q$ code. Then,

the **dual code** $\mathcal{C}^\perp$ is an $[n, n-k]_q$ **code**.

Proof:

From the definition of dual code, the following statements are equivalents:

$$\begin{aligned} \mathbf{x} \in \mathcal{C}^\perp &\iff \mathbf{c} \cdot \mathbf{x} = \mathbf{0} \text{ , for all } \mathbf{c} \in \mathcal{C} \\ &\iff \mathbf{m}G\mathbf{x}^T = \mathbf{0} \text{ , for all } \mathbf{m} \in \mathbb{F}_q^k \\ &\iff G\mathbf{x}^T = 0 \end{aligned}$$

Thus, $\mathcal{C}^\perp = \ker(G)$

Moreover, since $\operatorname{rank}(G) = k \implies \dim(\mathcal{C}^\perp) = n - k$

We can also deduce that G is a parity check matrix for $\mathcal{C}^\perp$.

Dual Code

Proposition:

Let $\mathcal{C}$ be an $[n, k]_q$ code with generator matrix G. Then,

$$(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$$

Trapdoor one-way functions - Decoder

Encoder = Matrix Multiplication

EASY

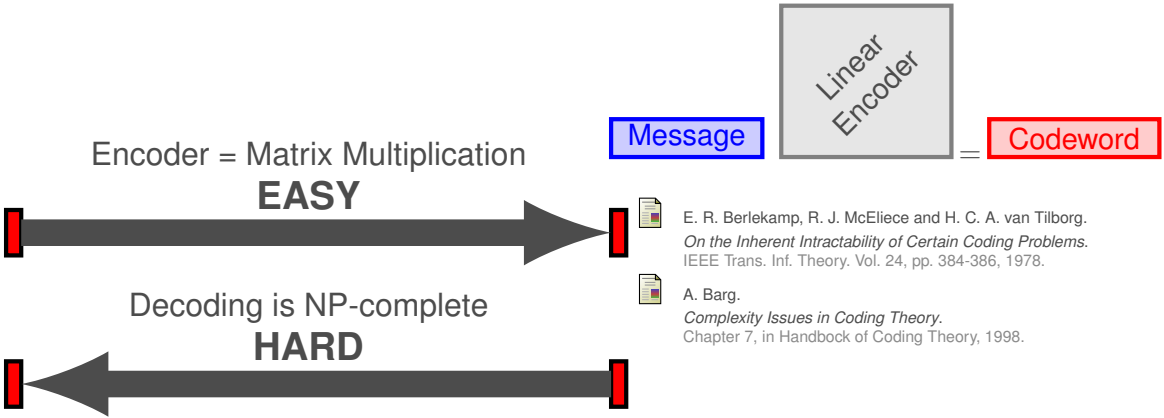
Message

Linear Encoder

$=$

Codeword

Trapdoor one-way functions - Decoder



E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg.
On the Inherent Intractability of Certain Coding Problems.
IEEE Trans. Inf. Theory. Vol. 24, pp. 384-386, 1978.

A. Barg.
Complexity Issues in Coding Theory.
Chapter 7, in Handbock of Coding Theory, 1998.

Trapdoor one-way functions - Decoder

Encoder = Matrix Multiplication

EASY

Decoding is NP-complete

HARD

Efficient decoder for certain families of codes

EASY(with TRAPDOOR information)

E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg.
On the Inherent Intractability of Certain Coding Problems.
IEEE Trans. Inf. Theory. Vol. 24, pp. 384-386, 1978.

A. Barg.
Complexity Issues in Coding Theory.
Chapter 7, in Handbock of Coding Theory, 1998.

1. Error-Correcting Codes and Cryptography

1. Introduction I - Cryptography
2. Introduction II - Coding Theory
3. Encoding (Linear Transformation)
4. Parity Checking
5. **Error Correcting Capacity**
6. Decoding (A Difficult Problem)
7. Reed-Solomon Codes
8. Goppa Codes
9. McEliece Cryptosystem