An introduction to error correcting codes

Mathematics sin fronteras

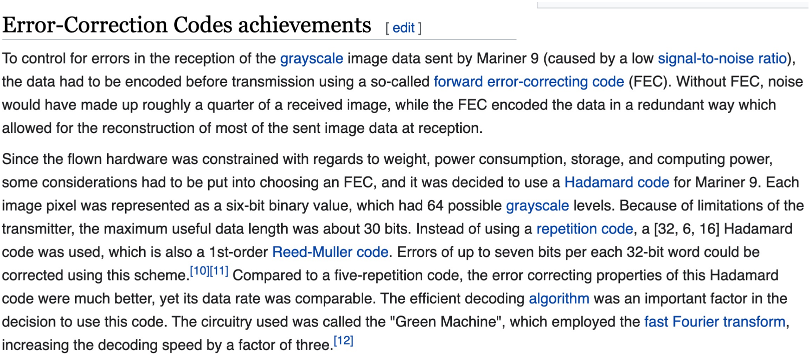
María Chara

Universidad Nacional del Litoral

May 19, 2021

FIQ UNL. FACULTAD DE INGENIERÍA QUÍMICA

Mariner 9, 1971



Error-Correction Codes achievements [edit]

To control for errors in the reception of the grayscale image data sent by Mariner 9 (caused by a low signal-to-noise ratio), the data had to be encoded before transmission using a so-called forward error-correcting code (FEC). Without FEC, noise would have made up roughly a quarter of a received image, while the FEC encoded the data in a redundant way which allowed for the reconstruction of most of the sent image data at reception.

Since the flown hardware was constrained with regards to weight, power consumption, storage, and computing power, some considerations had to be put into choosing an FEC, and it was decided to use a Hadamard code for Mariner 9. Each image pixel was represented as a six-bit binary value, which had 64 possible grayscale levels. Because of limitations of the transmitter, the maximum useful data length was about 30 bits. Instead of using a repetition code, a [32, 6, 16] Hadamard code was used, which is also a 1st-order Reed-Muller code. Errors of up to seven bits per each 32-bit word could be corrected using this scheme.[10][11] Compared to a five-repetition code, the error correcting properties of this Hadamard code were much better, yet its data rate was comparable. The efficient decoding algorithm was an important factor in the decision to use this code. The circuitry used was called the "Green Machine", which employed the fast Fourier transform, increasing the decoding speed by a factor of three.[12]

Figure: https://en.wikipedia.org/wiki/Mariner_9

Mariner 9, 1971

Coding and decoding with the generator matrix

- If $\mathcal{B} = \{v_1, \ldots, v_k\}$ is a basis of an $[n, k]$ code $\mathcal{C}$, we define the generator matrix G of the code as the matrix $G_{k\times n}$ for which the rows are the vectors v_i of the base.

- For an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ we can encode using the generator matrix G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Example: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

Coding and decoding with the generator matrix

- If $\mathcal{B} = \{v_1, \ldots, v_k\}$ is a basis of an $[n, k]$ code $\mathcal{C}$, we define the generator matrix G of the code as the matrix $G_{k\times n}$ for which the rows are the vectors v_i of the base.

- For an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ we can encode using the generator matrix G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Example: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

- Example: $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

Coding and decoding with the generator matrix

- If $\mathcal{B} = \{v_1, \ldots, v_k\}$ is a basis of an $[n, k]$ code $\mathcal{C}$, we define the generator matrix G of the code as the matrix $G_{k\times n}$ for which the rows are the vectors v_i of the base.

- For an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ we can encode using the generator matrix G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \rightarrow & c = uG \end{array}$$

- Example: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

- Example: $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

$$\begin{aligned} \mathcal{C} = \{&(000000), (100011), (010101), (001110), \\ &(110110), (011011), (101101), (111000)\}. \end{aligned}$$

Coding and decoding with the generator matrix

- If G is on standard form, i.e. $G = (I_k|A)$, then decoding is trivial since

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

Coding and decoding with the generator matrix

- If G is on standard form, i.e. $G = (I_k|A)$, then decoding is trivial since

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

- Example: $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), \\ (110110), (011011), (101101), (111000)\}.$$

Coding and decoding with the generator matrix

- If G is on standard form, i.e. $G = (I_k|A)$, then decoding is trivial since

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

- Example: $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

$$\begin{aligned}\mathcal{C} = \{&(000000), (100011), (010101), (001110),\\ &(110110), (011011), (101101), (111000)\}.\end{aligned}$$

How can we detect if a word has been transmitted with an error?

Parity check matrix and the dual code

The canonical inner product on $\mathbb{F}_q^n$ is defined by

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{F}_q^n$.

Parity check matrix and the dual code

The canonical inner product on $\mathbb{F}_q^n$ is defined by

$$\langle a, b\rangle = \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{F}_q^n$.

- If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a code then

  $$\mathcal{C}^\perp = \{u \in \mathbb{F}_q^n : \langle u, c\rangle = 0 \text{ for all } c \in \mathcal{C}\}$$

  is called the dual of $\mathcal{C}$.

Parity check matrix and the dual code

The canonical inner product on $\mathbb{F}_q^n$ is defined by

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{F}_q^n$.

- If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a code then

  $$\mathcal{C}^\perp = \{u \in \mathbb{F}_q^n : \langle u, c \rangle = 0 \text{ for all } c \in \mathcal{C}\}$$

  is called the dual of $\mathcal{C}$.

- The code $\mathcal{C}$ is called self-dual if $\mathcal{C}^\perp = \mathcal{C}$.

Parity check matrix and the dual code

The canonical inner product on $\mathbb{F}_q^n$ is defined by

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

for $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ in $\mathbb{F}_q^n$.

- If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a code then

  $$\mathcal{C}^\perp = \{u \in \mathbb{F}_q^n : \langle u, c \rangle = 0 \text{ for all } c \in \mathcal{C}\}$$

  is called the dual of $\mathcal{C}$.

- The code $\mathcal{C}$ is called self-dual if $\mathcal{C}^\perp = \mathcal{C}$.

Proposition

If $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_q$ then $\mathcal{C}^\perp$ is an $[n, n-k]$ code over $\mathbb{F}_q$.

Parity check matrix and the dual code

A generator matrix H of $\mathcal{C}^{\perp}$ is said to be a parity check matrix for C. Clearly H is an$(n-k) \times n$ matrix.

Parity check matrix and the dual code

A generator matrix H of $\mathcal{C}^{\perp}$ is said to be a parity check matrix for C. Clearly H is an$(n-k)\times n$ matrix.

- A parity check matrix H 'checks' whether a vector $u \in \mathbb{F}_q^n$ is a codeword or not since
$$x \in \mathcal{C} \iff Hx^T = 0.$$

Parity check matrix and the dual code

A generator matrix H of $\mathcal{C}^{\perp}$ is said to be a parity check matrix for C. Clearly H is an$(n-k) \times n$ matrix.

- A parity check matrix H 'checks' whether a vector $u \in \mathbb{F}_q^n$ is a codeword or not since
$$x \in \mathcal{C} \iff Hx^T = 0.$$
- If the generator matrix G of a code $\mathcal{C}$ is in standard form, i.e,
$$G = (I_k | A)$$
then a parity check matrix for $\mathcal{C}$ is
$$H = (-A^T | I_{n-k})$$
where I_{n-k} is the identity matrix of size $n-k$.

Parity check matrix and the dual code

A generator matrix H of $\mathcal{C}^{\perp}$ is said to be a parity check matrix for C. Clearly H is an$(n-k) \times n$ matrix.

- A parity check matrix H 'checks' whether a vector $u \in \mathbb{F}_q^n$ is a codeword or not since
$$x \in \mathcal{C} \iff Hx^T = 0.$$
- If the generator matrix G of a code $\mathcal{C}$ is in standard form, i.e,
$$G = (I_k|A)$$
then a parity check matrix for $\mathcal{C}$ is
$$H = (-A^T|I_{n-k})$$
where I_{n-k} is the identity matrix of size $n-k$.
- A matrix H of this form is said to be in standard form as a parity check matrix (although is not in standard form as a generator matrix of $\mathcal{C}^{\perp}$).

Example

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

$$\begin{aligned}\mathcal{C} = \{&(000000), (100011), (010101), (001110), \\ &(110110), (011011), (101101), (111000)\}.\end{aligned}$$

Error correction

Definition

If $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_q$ and H is a parity check matrix for $\mathcal{C}$, then for any word $y \in \mathbb{F}_q^n$ the *syndrome* of y is defined by $S(y) = yH^T$.

- $y \in \mathcal{C}$ if and only if $S(y) = 0$.
- If $y \notin \mathcal{C}$ then y is corrected as $y - e$ where $S(y) = S(e)$.

Definition

If $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_q$ and $a \in \mathbb{F}_q^n$, the *left coset* $a + \mathcal{C}$ is defined as $a + \mathcal{C} = \{a + x : x \in \mathcal{C}\}$.

Definition

If $\mathcal{C}$ is an $[n,k]$ code over $\mathbb{F}_q$ and $a \in \mathbb{F}_q^n$, the *left coset* $a+\mathcal{C}$ is defined as $a+\mathcal{C} = \{a+x : x \in \mathcal{C}\}$.

- $\mathcal{C} \subset \mathbb{F}_q^n$ is a vector space
- The quotient

$$\mathbb{F}_q^n/\mathcal{C} = \{a+\mathcal{C} : a \in \mathbb{F}_q^n\}$$

is a vector space

$$\alpha(a+\mathcal{C}) = \alpha a + \mathcal{C} \qquad (a+\mathcal{C})+(b+\mathcal{C}) = (a+b)+\mathcal{C}$$

where $\alpha \in \mathbb{F}_q$ and $a, b \in \mathbb{F}_q^n$,

Definition

If $\mathcal{C}$ is an $[n,k]$ code over $\mathbb{F}_q$ and $a \in \mathbb{F}_q^n$, the *left coset* $a + \mathcal{C}$ is defined as $a + \mathcal{C} = \{a + x : x \in \mathcal{C}\}$.

- $\mathcal{C} \subset \mathbb{F}_q^n$ is a vector space
- The quotient
$$\mathbb{F}_q^n/\mathcal{C} = \{a + \mathcal{C} : a \in \mathbb{F}_q^n\}$$
is a vector space
$$\alpha(a+\mathcal{C}) = \alpha a + \mathcal{C} \qquad (a+\mathcal{C}) + (b+\mathcal{C}) = (a+b) + \mathcal{C}$$
where $\alpha \in \mathbb{F}_q$ and $a, b \in \mathbb{F}_q^n$,
- $|\mathbb{F}_q^n/\mathcal{C}| = |\mathbb{F}_q^n|/|\mathcal{C}| = q^n/q^k = q^{n-k}$.

Theorem

Every word of $\mathbb{F}_q^n$ belongs to exactly one left coset of $\mathcal{C}$. Two cosets are either disjoint or identical.

- There are q^{n-k} disjoint cosets (with q^k words).
- The *coset leader* is any word in the coset of minimum weight.
- To perform error correction we can construct a table with all the coset leaders and their syndromes.

Example

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathcal{C} = \{&(000000), (100011), (010101), (001110), \\ &(110110), (011011), (101101), (111000)\}. \end{aligned}$$

Example

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), (110110), (011011), (101101), (111000)\}.$$

$e_0 = (000000)\ S(e_0) = (000)$	$e_4 = (000100)\ S(e_4) = (100)$
$e_1 = (100000)\ S(e_1) = (011)$	$e_5 = (000010)\ S(e_5) = (010)$
$e_2 = (010000)\ S(e_2) = (101)$	$e_6 = (000001)\ S(e_6) = (001)$
$e_3 = (001000)\ S(e_3) = (110)$	$e_7 = (100100)\ S(e_7) = (111)$

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

- $x = (010101) \to y = (010001)$
- $x = (010101) \to y = (011101)$
- $x = (011011) \to y = (011111)$
- $x = (110110) \to y = (110010)$
- 2 errores: $x = (110110) \to y = (110101)$

Theorem

Let $\mathcal{C}$ be an $[n, k, d]$ code and let H be a parity check matrix for $\mathcal{C}$. Then

$$d = \min\{r : \textit{there are } r \textit{ linearly dependent columns in } H\}.$$

In other words, H has d linearly dependent columns but any set of $d - 1$ columns are linearly independents.

Theorem

Let $\mathcal{C}$ be an $[n, k, d]$ code and let H be a parity check matrix for $\mathcal{C}$. Then

$$d = \min\{r : \textit{there are } r \textit{ linearly dependent columns in } H\}.$$

In other words, H has d linearly dependent columns but any set of $d-1$ columns are linearly independents.

Proof

Theorem

Let $\mathcal{C}$ be an $[n, k, d]$ code and let H be a parity check matrix for $\mathcal{C}$. Then

$$d = \min\{r : \text{there are } r \text{ linearly dependent columns in } H\}.$$

In other words, H has d linearly dependent columns but any set of $d-1$ columns are linearly independents.

Proof Let H^1, H^2, ..., H^n the columns of H. Then

$$c = (c_1, \ldots, c_n) \in \mathcal{C} \Longleftrightarrow Hc^T = 0 \Longleftrightarrow cH^T = 0 \Longleftrightarrow c_1H^1 + \cdots + c_nH^n = 0.$$

Theorem

Let $\mathcal{C}$ be an $[n, k, d]$ code and let H be a parity check matrix for $\mathcal{C}$. Then

$$d = \min\{r : \textit{there are } r \textit{ linearly dependent columns in } H\}.$$

In other words, H has d linearly dependent columns but any set of $d - 1$ columns are linearly independents.

Proof Let H^1, H^2, ..., H^n the columns of H. Then

$$c = (c_1, \dots, c_n) \in \mathcal{C} \iff Hc^T = 0 \iff cH^T = 0 \iff c_1H^1 + \cdots + c_nH^n = 0.$$

If $c \in \mathcal{C}$ is a word of minimum weight d we have that H has d linearly dependent columns, but any set of $d - 1$ or less columns are linearly independent, because in that case we would have non-zero words in $\mathcal{C}$ with weight less than d.

Theorem

Let $\mathcal{C}$ be an $[n, k, d]$ code and let H be a parity check matrix for $\mathcal{C}$. Then

$$d = \min\{r : \textit{there are } r \textit{ linearly dependent columns in } H\}.$$

In other words, H has d linearly dependent columns but any set of $d - 1$ columns are linearly independents.

Proof Let H^1, H^2, ..., H^n the columns of H. Then

$$c = (c_1, \ldots, c_n) \in \mathcal{C} \iff Hc^T = 0 \iff cH^T = 0 \iff c_1H^1 + \cdots + c_nH^n = 0.$$

If $c \in \mathcal{C}$ is a word of minimum weight d we have that H has d linearly dependent columns, but any set of $d - 1$ or less columns are linearly independent, because in that case we would have non-zero words in $\mathcal{C}$ with weight less than d. Reciprocally, if there are r columns linearly dependent then there are words of weight r but the minimum distance is the smallest of these weights.

Hadamard Code

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \dots, 2^r - 1$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = 23 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = (11 \cdot 2 + 1) \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = 11 \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = (5 \cdot 2 + 1) \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = 5 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = (2 \cdot 2 + 1) \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = 2 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = (1 \cdot 2 + 0)2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Hadamard Code

A Hadamard code is an $[2^r, r, 2^{r-1}]$ linear code over a binary alphabet which can correct many errors. The generator matrix G can be constructed in the following way: the i^{th} column of G is the binary representation of i for $i = 0, \ldots, 2^r - 1$

$$23 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

- Example: the $[8, 3, 4]$ Hadamard code has generator matrix:

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

Punctured Hadamard code

UNL . FACULTAD DE
INGENIERÍA QUÍMICA

Punctured Hadamard code

The punctured Hadamard code is a $[2^{r-1}, r, 2^{r-2}]$ linear code over the binary alphabet. The generator matrix for this code is obtained from the generator matrix of a Hadamard code without the columns starting with 0.

Punctured Hadamard code

The punctured Hadamard code is a $[2^{r-1}, r, 2^{r-2}]$ linear code over the binary alphabet. The generator matrix for this code is obtained from the generator matrix of a Hadamard code without the columns starting with 0.

- Example: $r = 3$:

$$G_{[8,3,4]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \rightarrow \quad G_{[4,3,2]} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Punctured Hadamard code

The punctured Hadamard code is a $[2^{r-1}, r, 2^{r-2}]$ linear code over the binary alphabet. The generator matrix for this code is obtained from the generator matrix of a Hadamard code without the columns starting with 0.

- Example: $r = 3$:

$$G_{[8,3,4]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \to \quad G_{[4,3,2]} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\mathcal{C} = \{(0000), (0101), (0011), (1111), (0110), (1010), (1100), (1001)\}$$

Reed-Muller code

- For $0 \leq r \leq m$ the Reed-Muller denoted by $\mathcal{R}(r,m)$ is an $[n,k,d]$ binary code with

$$n = 2^m, \qquad k = \sum_{i=0}^{r} \binom{m}{i}, \qquad d = 2^{m-r}.$$

- The generator matrix for $\mathcal{R}(r,m)$ is

$$G_{r,m} = \begin{pmatrix} G_{r,m-1} & G_{r,m-1} \\ 0 & G_{r-1,m-1} \end{pmatrix} \qquad \text{si } 0 < r < m$$

$$G_{0,m} = \underbrace{(1\ 1\ \cdots 1)}_{m+1} \qquad\qquad G_{m,m} = \begin{pmatrix} G_{m-1,m} \\ 0 \cdots 0\ 1 \end{pmatrix}$$

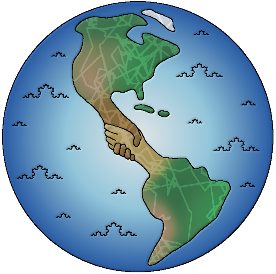
Challenge

Write the generator matrix of the

$$[32, 6, 16]$$

punctured Hadamard code used by Mariner 9.

¿Preguntas?



María Chara
charamaria@gmail.com

Saraí Hernández-Torres
sarai.h@campus.technion.ac.il