Introduction to Linear Codes over Finite Fields

By: M'hammed BOULAGOUAZ

5th Days of
Algebra, Number Theory and
Applcations
November 26-27,2021
OUJDA MOROCCO

Linear Codes over Finite Fields

- $A = \mathbb{F}_q$ a finite field with q elements.

Definition

*A $\mathbb{F}_q$- sub-vector space of $\mathbb{F}_q^n$ is called a **linear** code of length n over $\mathbb{F}_q$.*

Definition

The weight of $(x_1, ..., x_n) \in F_q^n := |\{x_i \neq 0\}|$ is denoted $wt(x)$ and we have also $wt(x) = d_H(0_{F_q}, (x_1, ..., x_n))$.

Remarks

For a linear code C we have :

1. *If $dim_{\mathbb{F}_q}(C) = k$ then $\sharp(C) = M = q^k$.*
2. *$d_{min}(C) := min\{wt(x)/x \in C \backslash \{0\}\}$.*

A linear code of **length** n, **dimension** k and **minimal distance** d is called a $[n, k, d]$-linear code.

Linear Codes over Finite Fields

◇ $A = \mathbb{F}_q$ a finite field with q elements.

Definition

*A $\mathbb{F}_q$- sub-vector space of $\mathbb{F}_q^n$ is called a **linear** code of length n over $\mathbb{F}_q$.*

Definition

The weight of $(x_1, ..., x_n) \in F_q^n :=\mid \{x_i \neq 0\} \mid$ is denoted $wt(x)$ and we have also $wt(x) = d_H(0_{F_q}, (x_1, ..., x_n))$.

Remarks

For a linear code C we have :

1. *If $dim_{\mathbb{F}_q}(C) = k$ then $\sharp(C) = M = q^k$.*
2. *$d_{min}(C) := min\{wt(x)/x \in C\backslash\{0\}\}$.*

A linear code of **length** n, **dimension** k and **minimal distance** d is called a $[n, k, d]$-linear code.

Example

- $A = \mathbb{F}_2$
- $C = \{(\lambda(1,1,0) + \beta(0,1,1) | \lambda, \beta \in \mathbb{F}_2\}$,

$$C = \{(\lambda, \lambda + \beta, \beta) | \lambda, \beta \in \mathbb{F}_2\}.$$

$$C = \{000, 011, 110, 101\},$$

$$dim(C) = 2, \quad \sharp(C) = 4 \text{ and } \quad d_{min}(C) = 2.$$

Proposition-Definition

(The inequality of the Singleton bound).
The minimal distance of a linear code satisfies

$$d \leq n - k + 1.$$

Example

- $A = \mathbb{F}_2$
- $C = \{(\lambda(1,1,0) + \beta(0,1,1) | \lambda, \beta \in \mathbb{F}_2\}$,

$$C = \{(\lambda, \lambda + \beta, \beta) | \lambda, \beta \in \mathbb{F}_2\}.$$

$$C = \{000, 011, 110, 101\},$$

$$dim(C) = 2, \quad \sharp(C) = 4 \text{ and } \quad d_{min}(C) = 2.$$

Proposition-Definition

(The inequality of the Singleton bound).
The minimal distance of a linear code satisfies

$$\boldsymbol{d} \leq n - k + 1.$$

Generator matrix

◇ If C is a (n, k, d)-linear code over $\mathbb{F}_q$.

Definition

A generator matrix G of the code C is a matrix $G \in M_{(k,n)}(\mathbb{F}_q)$ whose vectors rows form a basis of C.

Examples:

1. Let be

$$C = \{(x, y, x + y)/(x, y) \in \mathbb{F}_2^2\}.$$

Then

$$C = \{x(1, 0, 1) + y(0, 1, 1)/(x, y) \in \mathbb{F}_2^2\}$$

$k = 2$, $d = 2$ and C is a $[3, 2, 2]$-code.
In addition
$G_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ are two generator matrices.

Generator matrix

◇ If C is a (n, k, d)-linear code over $\mathbb{F}_q$.

Definition

A generator matrix G of the code C is a matrix $G \in M_{(k,n)}(\mathbb{F}_q)$ whose vectors rows form a basis of C.

Examples:

1. Let be

$$C = \{(x, y, x + y)/(x, y) \in \mathbb{F}_2^2\}.$$

Then

$$C = \{x(1, 0, 1) + y(0, 1, 1)/(x, y) \in \mathbb{F}_2^2\}$$

$k = 2$, $d = 2$ and C is a $[3, 2, 2]$-code.
In addition
$G_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ are two generator matrices.

More generally

2. Let be

$$C = \{(x_1, ..., x_{n-1}, x_1 + ... + x_{n-1})/(x_1, ..., x_{n-1}) \in \mathbb{F}_2^{n-1}\}.$$

Then,

$$C = \{x_1(1, 0, ..., 1) + ... + x_{n-1}(0, ..., 1, 1)/(x_1, ..., x_{n-1}) \in \mathbb{F}_2^{n-1}\}$$

So $k = n - 1$, $d = 2$ and C is a $[n, n-1, 2]$-code.
In addition

$$G = \begin{pmatrix} & & 1 \\ & I_{n-1} & \vdots \\ & & 1 \end{pmatrix}$$

is a generator matrix of C.

Encoding by linear codes

◇ Let be C a (n, k, d)-linear code over $\mathbb{F}_q$ with G as generator matrix.

◇ $g : \mathbb{F}_q^k \longrightarrow C$
$m \longrightarrow mG$, is an isomorphism, which can serve an **encoding mechanism of** C.

If $((g_{11}, ..., g_{1n}), ..., (g_{k1}, ..., g_{kn}))$ is a basis of C,
then for each $(m_1, ..., m_k) \in F_2^k$ we have:

$$\Sigma_{j=1}^{k} m_j(g_{j1}, ..., g_{jn}) = (\Sigma_{j=1}^{k} m_j g_{j1}, ..., \Sigma_{j=1}^{k} m_j g_{kn}) \in C.$$

Then we use the equality

$$(m_1 ... m_k) \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \vdots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} = \begin{pmatrix} \Sigma_{j=1}^{k} m_j g_{j1} \\ \vdots \\ \Sigma_{j=1}^{k} m_j g_{kn}) \end{pmatrix},$$

to encode $m_1 ... m_k \in F_2^K$ by $(\Sigma_{j=1}^{k} m_j g_{j1}) ... (\Sigma_{j=1}^{k} m_j g_{kn}) \in C$.

Encoding Examples

Let be
$C = \{(x, y, x+y)/(x, y) \in \mathbb{F}_2^2\} = \{x(1,0,1) + y(0,1,1)/(x, y) \in \mathbb{F}_2^2\}$.

1. by using the generator matrix $G_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ a message $(m_1, m_2) \in F_2^2$ is encoded by

$(m_1\ m_2)(\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (m_1\ m_2\ (m_1 + m_2))$.

So, the message : **11**0110
is encoded by :**110**011101

2. By using the generator matrix $G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ a message $(m_1, m_2) \in F_2^2$ is encoded by

$(m_1\ m_2)G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} = (m_2\ (m_1 + m_2)\ m_1)$.

So, the message : **11**0110
is encoded by :**101**110011.

Encoding Examples

Let be
$C = \{(x, y, x+y)/(x, y) \in \mathbb{F}_2^2\} = \{x(1,0,1) + y(0,1,1)/(x, y) \in \mathbb{F}_2^2\}$.

1. by using the generator matrix $G_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ a message $(m_1, m_2) \in F_2^2$ is encoded by

$(m_1\ m_2)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (m_1\ m_2\ (m_1 + m_2))$.

So, the message : **11**0110
is encoded by :**110**011101

2. By using the generator matrix $G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ a message $(m_1, m_2) \in F_2^2$ is encoded by

$(m_1\ m_2)G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} = (m_2\ (m_1 + m_2)\ m_1)$.

So, the message : **11**0110
is encoded by :**101**110011.

Parity Check matrix

◇ Let be C a $[n, k, d]$-linear code over $\mathbb{F}_q$.

Definition

A Parity Check matrix of the code C is a matrix $H \in M_{(n-k,n)}(\mathbb{F}_q)$ such that

$$x \in C \Leftrightarrow xH^T = 0_{(1,n-k)}.$$

Example

$$C_{\sum} = \{(x_1 , ... , x_{n-1} , x_1 + ... + x_{n-1}) \, (x_1 , ... , x_{n-1}) \in \mathbb{F}_q^{n-1}\}.$$

◇ A parity Check matrix H of $C_{\sum}$ is

$$H = (-(1)...(-1)1).$$

Parity Check matrix

◇ Let be C a $[n, k, d]$-linear code over $\mathbb{F}_q$.

Definition

A Parity Check matrix of the code C is a matrix $H \in M_{(n-k,n)}(\mathbb{F}_q)$ such that

$$x \in C \Leftrightarrow xH^T = 0_{(1,n-k)}.$$

Example

$$C_{\sum} = \{(x_1 , \dots , x_{n-1} , x_1 + \dots + x_{n-1}) \ (x_1 , \dots , x_{n-1}) \in \mathbb{F}_q^{n-1}\}.$$

◇ A parity Check matrix H of $C_{\sum}$ is

$$H = (-(1)...(-1)1).$$

Dual Code

Let consider the scalar product on the vector space $\mathbb{F}_q^n$ defined by

$$< (x_1, ..., x_n), (y_1, ..., y_n) >= \sum_{i=1}^{n} x_i y_i.$$

Definition

The dual code of a linear code $C \subset \mathbb{F}_q^n$ is defined by:

$$C^{\perp} = \{y \in \mathbb{F}_q^n / (\forall x \in C)(< x , y >= 0)\}.$$

Note that:

1. $C^{\perp}$ is a linear code of dimension $n - dim(C)$.
2. $(C^{\perp})^{\perp} = C$.

Dual Code

Let consider the scalar product on the vector space $\mathbb{F}_q^n$ defined by

$$< (x_1, ..., x_n), (y_1, ..., y_n) >= \sum_{i=1}^{n} x_i y_i.$$

Definition

The dual code of a linear code $C \subset \mathbb{F}_q^n$ is defined by:

$$C^{\perp} = \{y \in \mathbb{F}_q^n / (\forall x \in C)(< x , y \ >= 0)\}.$$

Note that:

1. $C^{\perp}$ is a linear code of dimension $n - dim(C)$.
2. $(C^{\perp})^{\perp} = C$.

Dual Code

Let consider the scalar product on the vector space $\mathbb{F}_q^n$ defined by

$$< (x_1, ..., x_n), (y_1, ..., y_n) >= \sum_{i=1}^{n} x_i y_i.$$

Definition

The dual code of a linear code $C \subset \mathbb{F}_q^n$ is defined by:

$$C^{\perp} = \{y \in \mathbb{F}_q^n / (\forall x \in C)(< x , y \ >= 0)\}.$$

Note that:

1. $C^{\perp}$ is a linear code of dimension $n - dim(C)$.
2. $(C^{\perp})^{\perp} = C$.

Dual Code

Let consider the scalar product on the vector space $\mathbb{F}_q^n$ defined by

$$< (x_1, ..., x_n), (y_1, ..., y_n) >= \sum_{i=1}^{n} x_i y_i.$$

Definition

The dual code of a linear code $C \subset \mathbb{F}_q^n$ is defined by:

$$C^{\perp} = \{y \in \mathbb{F}_q^n / (\forall x \in C)(< x , y \ >= 0)\}.$$

Note that:

1. $C^{\perp}$ is a linear code of dimension $n - dim(C)$.

2. $(C^{\perp})^{\perp} = C$.

Dual Code

Let consider the scalar product on the vector space $\mathbb{F}_q^n$ defined by

$$< (x_1, ..., x_n), (y_1, ..., y_n) >= \sum_{i=1}^{n} x_i y_i.$$

Definition

The dual code of a linear code $C \subset \mathbb{F}_q^n$ is defined by:

$$C^{\perp} = \{y \in \mathbb{F}_q^n / (\forall x \in C)(< x , y \ >= 0)\}.$$

Note that:

1. $C^{\perp}$ is a linear code of dimension $n - dim(C)$.

2. $(C^{\perp})^{\perp} = C$.

Dual Code

Hence we have the following results:

Proposition

1. G is a generator matrix of the code C if and only if G^T is a parity matrix of the dual code $C^\perp$.

2. H is a parity matrix of the code C if and only if H^T is a generator matrix of the dual code $C^\perp$.

Dual Code

Hence we have the following results:

Proposition

1. G is a generator matrix of the code C if and only if G^T is a parity matrix of the dual code $C^\perp$.

2. H is a parity matrix of the code C if and only if H^T is a generator matrix of the dual code $C^\perp$.

Syndromes decoding

Let be C a code with $H \in M_{n-k}(\mathbb{F}_q)$ as parity matrix.
If t is the transmitted and r is the received message.

rH^T is called the syndrome of r and it is denoted by $S(r)$.

We have $r \in C \Leftrightarrow S(r) = 0 \in M_{1,n-k}(\mathbb{F}_q)$**.**

1) If $S(r) = 0$, then **we conclude that most likely no errors occurred**.
(It is possible sufficiently many errors occurred, to change the transmitted codeword into a different codeword, but we cant detect or correct this.)

2) If $S(r) \neq 0$, then **we conclude that at least one error occurred**, and $r = t + e$, where e is an error vector and $S(r) = S(e)$.

Syndromes decoding

Let be C a code with $H \in M_{n-k}(\mathbb{F}_q)$ as parity matrix.
If t is the transmitted and r is the received message.

rH^T is called the syndrome of r and it is denoted by $S(r)$.

We have $r \in C \Leftrightarrow S(r) = 0 \in M_{1,n-k}(\mathbb{F}_q)$.

1) If $S(r) = 0$, then **we conclude that most likely no errors occurred**.
(It is possible sufficiently many errors occurred, to change the transmitted codeword into a different codeword, but we cant detect or correct this.)

2) If $S(r) \neq 0$, then **we conclude that at least one error occurred**, and $r = t + e$, where e is an error vector and $S(r) = S(e)$.

Syndromes decoding

Let be C a code with $H \in M_{n-k}(\mathbb{F}_q)$ as parity matrix.
If t is the transmitted and r is the received message.

rH^T is called the syndrome of r and it is denoted by $S(r)$.

We have $r \in C \Leftrightarrow S(r) = 0 \in M_{1,n-k}(\mathbb{F}_q)$**.**

1) If $S(r) = 0$, then **we conclude that most likely no errors occurred**.
(It is possible sufficiently many errors occurred, to change the transmitted codeword into a different codeword, but we cant detect or correct this.)

2) If $S(r) \neq 0$, then **we conclude that at least one error occurred**, and $r = t + e$, where e is an error vector and $S(r) = S(e)$.

Syndromes decoding

Let be C a code with $H \in M_{n-k}(\mathbb{F}_q)$ as parity matrix.
If t is the transmitted and r is the received message.

rH^T is called the syndrome of r and it is denoted by $S(r)$.

We have $r \in C \Leftrightarrow S(r) = 0 \in M_{1,n-k}(\mathbb{F}_q)$**.**

1) If $S(r) = 0$, then **we conclude that most likely no errors occurred**.
(It is possible sufficiently many errors occurred, to change the transmitted codeword into a different codeword, but we cant detect or correct this.)

2) If $S(r) \neq 0$, then **we conclude that at least one error occurred**, and $r = t + e$, where e is an error vector and $S(r) = S(e)$.

Syndromes decoding

Let be C a code with $H \in M_{n-k}(\mathbb{F}_q)$ as parity matrix.
If t is the transmitted and r is the received message.

rH^T is called the syndrome of r and it is denoted by $S(r)$.

We have $r \in C \Leftrightarrow S(r) = 0 \in M_{1,n-k}(\mathbb{F}_q)$**.**

1) If $S(r) = 0$, then **we conclude that most likely no errors occurred**.
(It is possible sufficiently many errors occurred, to change the transmitted codeword into a different codeword, but we cant detect or correct this.)

2) If $S(r) \neq 0$, then **we conclude that at least one error occurred**, and $r = t + e$, where e is an error vector and $S(r) = S(e)$.

Syndromes decoding

1. $S(r) = S(e)$ if and only if r and e are in the same coset (in $\mathbb{F}_q^n/C$.)

2. There is one-to-one correspondance between **cosets** relatively to C and **syndromes**.

Conclusion: r is corrected by y such that:

$y = r - e$ with $wt(e)$ is minimal in $\{wt(x)/x \in r + C\ (= e + C)\}$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.
2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.
3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.
4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = \mathbf{1101}$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0101}$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error**$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.
2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.
3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.
4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error**$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.
2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.
3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.
4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq$ **t**

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq$ **t**.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq$ **t**.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq$ **t**.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{1}0\mathbf{1}$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{01}0\mathbf{1}$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error**$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = \mathbf{1101}$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0101}$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{1111}$ then $S(r) = 10$: **error**$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{01}01$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 1010$ then $S(r) = 10$: **error** and $y = 1110 \neq$ **t**

If $t = 1011$ and $r = 1101$ then $S(r) = 11$: **error** and $y = 0101 \neq$ **t**.

If $t = 1011$ and $r = 0101$ then $S(r) = 00$: No error and $y = 0101 \neq$ **t**.

If $t = 1011$ and $r = 0100$ then $S(r) = 10$: **error** $y = 0000 \neq$ **t**.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0101}$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error** $y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: error$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: error$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error** $y = 0000 \neq$ t.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error** $y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: error$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: error$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1111$ then $S(r) = 10$: **error**$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1\mathbf{111}$ then $S(r) = 10$: **error**$y = 1011 = t$.

Example

Let $C = \{0000, 1011, 0101, 1110\}$.

Then $G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

Since $d_{min}(C) = 2$, C **detect 1 error** and **correct zero error**.

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$.

More precisely if we receive a codeword r then we have:

1. $r \in 1000 + C$ then **S(r)=11**, we correct r by $y = r - 1000$.

2. $r \in 0100 + C$ then **S(r)=10**, we correct r by $y = r - 0100$.

3. $r \in 0010 + C$ then **S(r)=01**, we correct r by $y = r - 0010$.

4. $r \in C$, then **S(r)=00**, we correct r by $y = r$.

Application:

If $t = 1011$ and $r = 101\mathbf{0}$ then $S(r) = 10$: **error** and $y = 1110 \neq \mathbf{t}$

If $t = 1011$ and $r = 1\mathbf{10}1$ then $S(r) = 11$: **error** and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{010}1$ then $S(r) = 00$: No error and $y = 0101 \neq \mathbf{t}$.

If $t = 1011$ and $r = \mathbf{0100}$ then $S(r) = 10$: **error**$y = 0000 \neq \mathbf{t}$.

If $t = 1011$ and $r = 1\mathbf{111}$ then $S(r) = 10$: **error**$y = 1011 = t$.