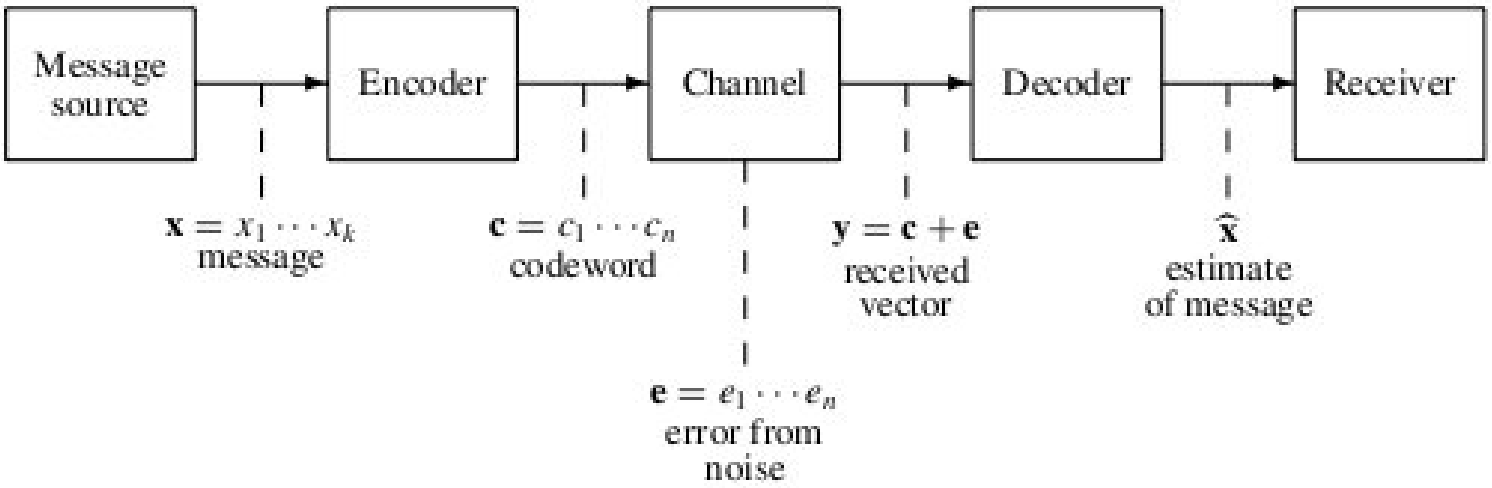
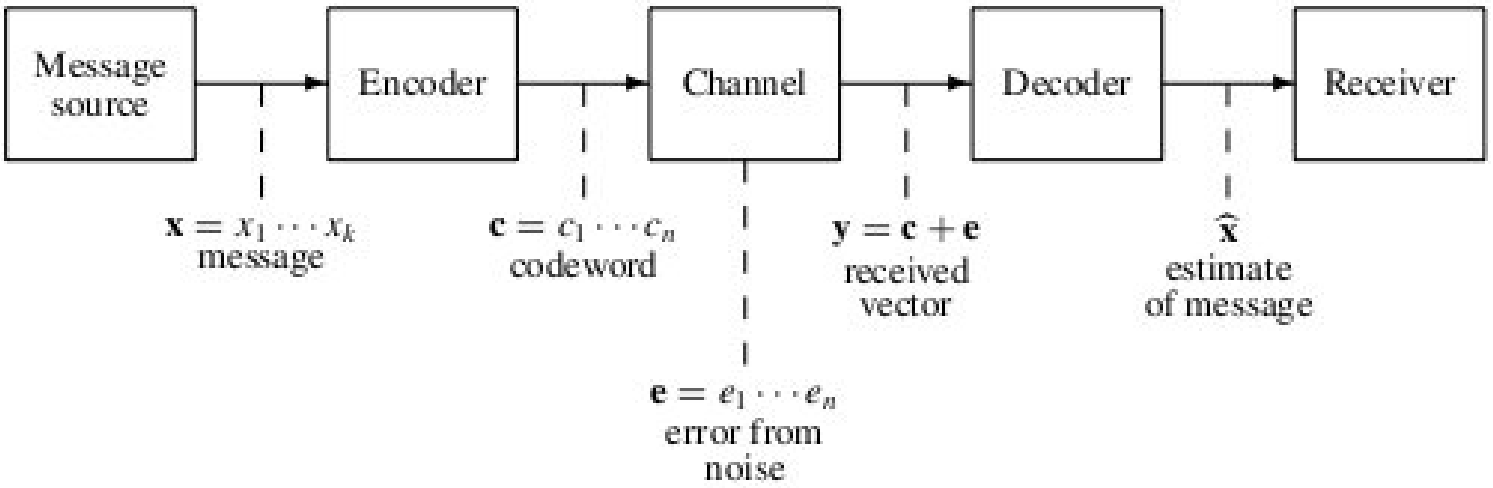
Decoding linear codes

CoCoNut, 2016

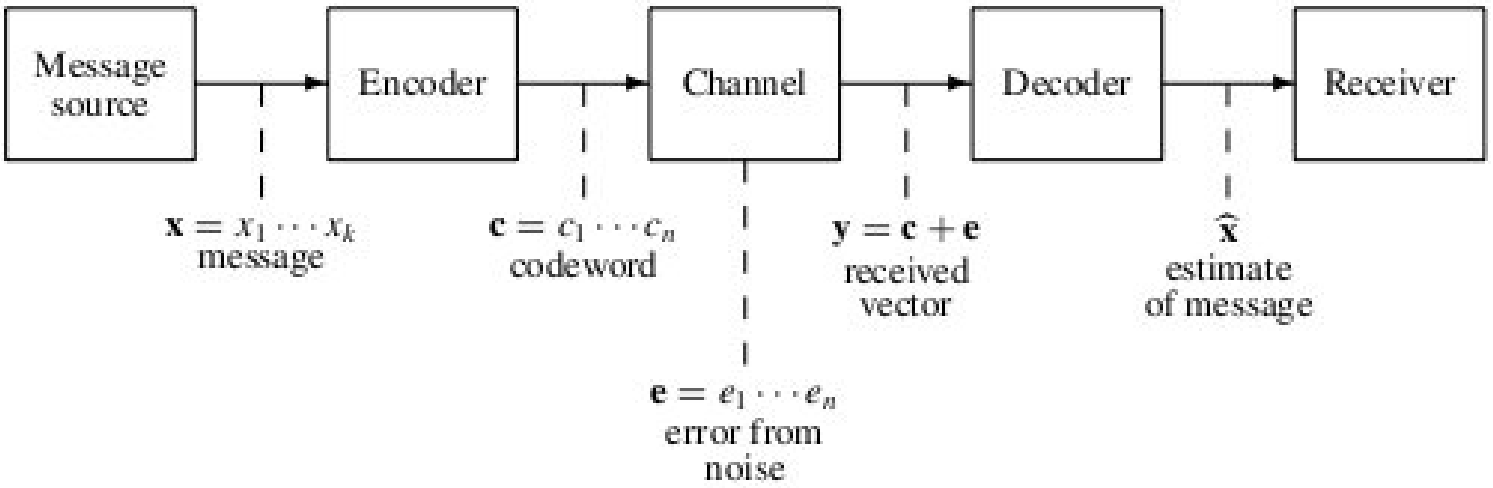
Emmanuela Orsini

Previously


Message source
Encoder
Channel
Decoder
Receiver
$\mathbf{x} = x_1 \cdots x_k$
message
$\mathbf{c} = c_1 \cdots c_n$
codeword
$\mathbf{e} = e_1 \cdots e_n$
error from noise
$\mathbf{y} = \mathbf{c} + \mathbf{e}$
received vector
$\hat{\mathbf{x}}$
estimate of message



- $C = \{00000, 01011, 10101, 11110\}$
- Let $\mathbf{r} = 00101$ be the received word



- $C = \{00000, 01011, 10101, 11110\}$
- Let $\mathbf{r} = 00101$ be the received word
- $E = \{00101, 01110, \mathbf{10000}, 11010\}$
  The most likely codeword is the one corresponding to the one of smallest weight

- An $[n, k, d]_q$ linear code is a k-dimensional subspace of $\mathbb{F}_q^n$.
- We have seen the following way of defining an $[n, k, d]_q$ linear code C:
  - ◇ Using a $k \times n$ generator matrix G, so that C is obtained multiplying all vectors $\mathbf{x} \in \mathbb{F}_q^k$ by G
  - ◇ Using an $(n-k) \times n$ parity-check matrix H such that

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

- *Maximum likelihood decoding*: decoding procedure in which a received word is decoded as one of the codewords which is most likely to have been sent.

Consider the $[6,3]_3$ linear code with generator matrix

```
> G;
[1 0 0 1 0 1]
[0 1 0 1 1 2]
[0 0 1 1 1 1]
```

```
> H;
[1 0 0 2 1 0]
[0 1 0 1 0 2]
[0 0 1 2 2 1]
```

1. How many codewords? Minimum Distance?
2. Is $\mathbf{y} = (1,0,0,0,0,0)$ in C?

Consider the $[6,3]_3$ linear code with generator matrix

```
> G;
[1 0 0 1 0 1]
[0 1 0 1 1 2]
[0 0 1 1 1 1]
```

```
> H;
[1 0 0 2 1 0]
[0 1 0 1 0 2]
[0 0 1 2 2 1]
```

1. How many codewords? Minimum Distance?
2. Is $\mathbf{y} = (1,0,0,0,0,0)$ in C?

```
>y*Transpose(H);
>(1 0 0)
```

List of all codewords:

```
<(0 0 0 0 0 0), (1 0 0 1 0 1), (2 0 0 2 0 2), (0 1 0 1 1 2),
 (1 1 0 2 1 0), (2 1 0 0 1 1), (0 2 0 2 2 1), (1 2 0 0 2 2),
 (2 2 0 1 2 0), (0 0 1 1 1 1), (1 0 1 2 1 2), (2 0 1 0 1 0),
 (0 1 1 2 2 0), (1 1 1 0 2 1), (2 1 1 1 2 2), (0 2 1 0 0 2),
 (1 2 1 1 0 0), (2 2 1 2 0 1), (0 0 2 2 2 2), (1 0 2 0 2 0),
 (2 0 2 1 2 1), (0 1 2 0 0 1), (1 1 2 1 0 2), (2 1 2 2 0 0),
 (0 2 2 1 1 0), (1 2 2 2 1 1), (2 2 2 0 1 2)>
```

Theorem (Singleton Bound)

If C is an $(n, M, d)_q$ code, then $A_q(n, d) \leq q^{n-d+1}$

$$q^k \leq q^{n-d+1} \longrightarrow k \leq n - d + 1$$

Codes that meet this bound, i.e. satisfy $d = n - k + 1$, are called **Maximum Distance Separable** (MDS) codes.

This lecture...

Fix $n, k \in \mathbb{N}$, such $k \leq n$ and q a prime power with $q \geq n$. Consider the finite field $\mathbb{F}_q$ and construct the code as follows:

Fix $n, k \in \mathbb{N}$, such $k \leq n$ and q a prime power with $q \geq n$. Consider the finite field $\mathbb{F}_q$ and construct the code as follows:

1. Choose n distinct points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$
2. Let $\mathbf{m} = (m_0, \ldots, m_{k-1})$ a message in $\mathbb{F}_q^k$, we can rewrite $\mathbf{m}$ as

$$m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1} \in \mathbb{F}_q[x]$$

3. Encode $m(x)$ evaluating it in α_i, $i = 1, \ldots, n$:

$$c(\alpha_1, \ldots, \alpha_n) = (m(\alpha_1), \ldots, m(\alpha_n)).$$

Definition (Reed-Solomon codes)

Take n distinct points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, with n such that $q \geq n$, and let k be an integer such that $1 \leq k \leq n$. We define the Reed-Solomon code as

$$RS_q(n,k) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_q^n \mid f \in \mathbb{F}_q[x] s.t. \deg(f) \leq k-1 \cup \{0\}$$

Remark: Usually the set of points $S = \{\alpha_1, \ldots, \alpha_n\}$ is $\mathbb{F}_q^*$.

Definition (Reed-Solomon codes)

Take n distinct points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, with n such that $q \geq n$, and let k be an integer such that $1 \leq k \leq n$. We define the Reed-Solomon code as

$$RS_q(n,k) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \in \mathbb{F}_q^n \mid f \in \mathbb{F}_q[x] s.t. \deg(f) \leq k-1 \cup \{0\}$$

Remark: Usually the set of points $S = \{\alpha_1, \ldots, \alpha_n\}$ is $\mathbb{F}_q^*$.

- Let $\mathcal{P}_{k-1}$ be the vector space of all polynomials of degree at most $k-1$ over $\mathbb{F}_q$

  $$\{1, x, \ldots, x^{k-1}\}$$

  is a basis for it.

We can define a code $C = RS(n, k)$ as the image of

$$\begin{aligned} \text{Enc} : \mathcal{P}_{k-1} &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(\alpha_1), \ldots, f(\alpha_n)) \end{aligned}$$

In this way the Vandermonde matrix

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}$$

(obtained evaluating $\{1, x, \ldots, x^{k-1}\}$ in $\alpha_1, \ldots, \alpha_n$) is a generator matrix for C.

Example

Consider the RS codes over $\mathbb{F}_9$ with $k = 3$. Let $\{1, x, x^2\}$ a basis for $\mathcal{P}_2$. Then let S be the set of points $\mathbb{F}_9^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$, we obtain the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix}.$$

The corresponding Reed-Solomon code is a linear code with block length $n = q - 1 = 8$, and dimension $k = \dim \mathcal{P}_{k-1} = 3$.

Example

Consider the RS codes over $\mathbb{F}_9$ with $k = 3$. Let $\{1, x, x^2\}$ a basis for $\mathcal{P}_2$. Then let S be the set of points $\mathbb{F}_9^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$, we obtain the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix}.$$

The corresponding Reed-Solomon code is a linear code with block length $n = q - 1 = 8$, and dimension $k = \dim \mathcal{P}_{k-1} = 3$.

What about the distance?

Example

Consider the RS codes over $\mathbb{F}_9$ with $k = 3$. Let $\{1, x, x^2\}$ a basis for $\mathcal{P}_2$. Then let S be the set of points $\mathbb{F}_9^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$, we obtain the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix}.$$

The corresponding Reed-Solomon code is a linear code with block length $n = q - 1 = 8$, and dimension $k = \dim \mathcal{P}_{k-1} = 3$.

What about the distance?

The $RS_q(n, k)$ is MDS, i.e. it is an $[n, k, d = n - k + 1]_q$ code

Example

Consider the RS codes over $\mathbb{F}_9$ with $k = 3$. Let $\{1, x, x^2\}$ a basis for $\mathcal{P}_2$. Then let S be the set of points $\mathbb{F}_9^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$, we obtain the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{pmatrix}.$$

The corresponding Reed-Solomon code is a linear code with block length $n = q - 1 = 8$, and dimension $k = \dim \mathcal{P}_{k-1} = 3$.

What about the distance?

The $RS_q(n, k)$ is MDS, i.e. it is an $[n, k, d = n - k + 1]_q$ code

The code above is an $[8, 3, 6]$ Reed-Solomon code over $\mathbb{F}_9$

Decoding linear codes

It is important to know the type of channel used for transmission, as we need to know how the noise can modify the transmitted word.

It is important to know the type of channel used for transmission, as we need to know how the noise can modify the transmitted word.
A q-ary symmetric channel (**SC** for short) is a channel with the following properties:

a) the components of a transmitted word (an element of $\mathbb{F}_q$ that here we name generally "symbol") can be changed by the noise only to another element of $\mathbb{F}_q$;

b) the probability that a symbol becomes another one is the same for all pairs of symbols;

c) the probability that a symbol changes during the transmission does not depend on its position;

d) if the i-th component is changed, then this fact does not affect the probability of changing for the j-th components, even if j is close to i.

To these channel properties it is usually added a *source property*:

- *all words are equally likely to be transmitted.*

In case of q-ary SC, any codeword whose distance to the received word $\mathbf{r}$ is minimum (in the Hamming metric), is also the codeword which is most likely to have been sent
$\longrightarrow$ MLD is equivalent to the *nearest neighbour decoding*.

Fact

If the transmission uses a q-ary SC and the probability that a symbol changes into another one is less then the probability that a symbol is uncorrupted by noise, the word sent with the highest probability is the word "nearest" (in the sense of Hamming distance) to the received vector. If no more than t (the error correction capability) errors have occurred, this word is unique.

$$\mathbf{c} + \mathbf{e} = \mathbf{r}$$

$$\mathbf{c} + \mathbf{e} = \mathbf{r}$$

$$d(\mathbf{c}, \mathbf{r}) = \mathrm{wt}(\mathbf{c} - \mathbf{r}) = \mathrm{wt}(\mathbf{e})$$

$$\mathbf{c} + \mathbf{e} = \mathbf{r}$$

$$d(\mathbf{c}, \mathbf{r}) = \mathrm{wt}(\mathbf{c} - \mathbf{r}) = \mathrm{wt}(\mathbf{e})$$

- We want to find $\mathbf{e}$ of minimal weight such that $\mathbf{r} - \mathbf{e} \in C$.

$$\mathbf{c} + \mathbf{e} = \mathbf{r}$$

$$d(\mathbf{c}, \mathbf{r}) = \mathrm{wt}(\mathbf{c} - \mathbf{r}) = \mathrm{wt}(\mathbf{e})$$

- We want to find $\mathbf{e}$ of minimal weight such that $\mathbf{r} - \mathbf{e} \in C$.
- If the number of errors is less than t this vector is unique

Coset

Let C be an $[n, k, d]_q$ linear code and $\mathbf{u} \in \mathbb{F}_q^n$. A coset of C determined by $\mathbf{u}$ is the set

$$\mathbf{u} + C = \{\mathbf{u} + \mathbf{c} | \mathbf{c} \in C\}$$

1. If $\mathbf{u} \in \mathbf{v} + C$, then $\mathbf{v} + C = \mathbf{u} + C$, i.e. each word in the coset determines that coset;
2. $\mathbf{u} \in \mathbf{u} + C$
3. If $\mathbf{u} - \mathbf{v} \in C$, the $\mathbf{v}$ and $\mathbf{u}$ are in the same coset;
4. Every element of $\mathbb{F}_q^n$ is contained in one and only one coset, i.e. either $\mathbf{v} + C = \mathbf{u} + C$ or these cosets are disjoint,
5. $|\mathbf{v} + C| = |C| = q^k$,
6. There are q^{n-k} different cosets
7. C is a coset.

Decoding linear codes - Cosets

If $\mathbf{r} \in \mathbb{F}_q^n$ is the received word, we have to find $\mathbf{e} \in \mathbb{F}_q^n$ such that:

$$\mathbf{r} - \mathbf{e} \in C \rightarrow \exists\, \mathbf{c} \in C \quad s.t. \quad \mathbf{c} = \mathbf{r} - \mathbf{e} \text{ and then decode } \mathbf{r} \text{ with } \mathbf{c}$$
$$\rightarrow \mathbf{r} = \mathbf{e} + \mathbf{c} \rightarrow \mathbf{r} \in \mathbf{e} + C$$
$$\rightarrow \mathbf{r} \text{ and } \mathbf{e} \text{ are in the same coset!}$$

We have to find an element $\mathbf{e}$ in the same coset of $\mathbf{r}$, but

How can we choose $\mathbf{e}$?

Coset leader

Definition

Let C be an $[n, k, d]_q$ code. For any coset $\mathbf{r} + C$, $\mathbf{r} \in \mathbb{F}_q^n$, and any vector $\mathbf{v} \in \mathbf{r} + C$, we say that $\mathbf{v}$ is a **coset leader** if it is an element of minimum weight in the coset.

1. Choose a word $\mathbf{e}$ of minimum weight in the coset $\mathbf{r} + C$,
2. Decode with $\mathbf{c} = \mathbf{r} - \mathbf{e}$

Coset leader

Definition

Let C be an $[n, k, d]_q$ code. For any coset $\mathbf{r} + C$, $\mathbf{r} \in \mathbb{F}_q^n$, and any vector $\mathbf{v} \in \mathbf{r} + C$, we say that $\mathbf{v}$ is a **coset leader** if it is an element of minimum weight in the coset.

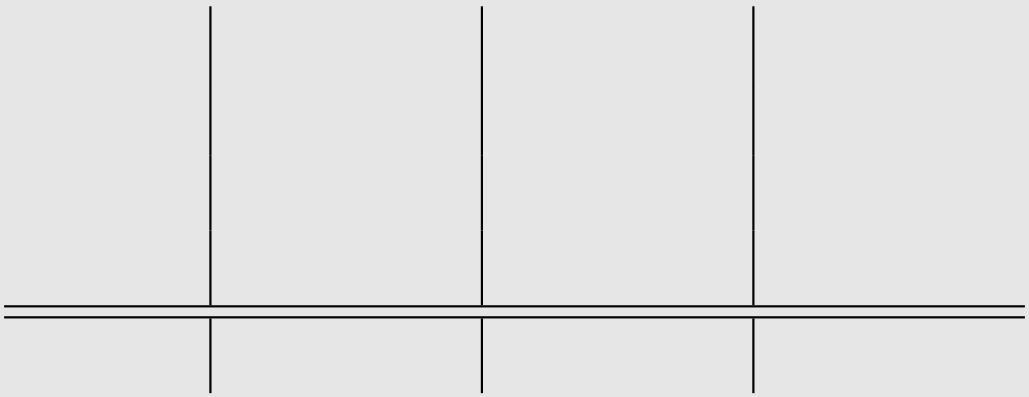
1. Choose a word $\mathbf{e}$ of minimum weight in the coset $\mathbf{r} + C$,
2. Decode with $\mathbf{c} = \mathbf{r} - \mathbf{e}$

Let C be a linear code with $d(C) = d$. If $\mathrm{wt}(\mathbf{x}) \leq \lfloor \frac{d-1}{2} \rfloor$, then $\mathbf{x}$ is the **unique** element of minimum weight in its coset of C and hence it is always a coset leader.

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$



Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000			
1011			
0101			
1110			
C			

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000		
1011	0011		
0101	1101		
1110	0110		
C	1000+C		

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000	0100	
1011	0011	1111	
0101	1101	0001	
1110	0110	1010	
C	1000+C	0100+C	

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100
C	1000+C	0100+C	0010+C

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100
C	1000+C	0100+C	0010+C

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100
C	1000+C	0100+C	0010+C

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100
C	1000+C	0100+C	0010+C

Then we obtain $\mathbf{c} = 1101 + 1000 = 0101$

Decoding linear code - Standard array

Example

$$C = \{0000, 1011, 0101, 1110\} \text{ and } \mathbf{r} = 1101$$

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100
C	1000+C	0100+C	0010+C

Then we obtain $\mathbf{c} = 1101 + 1000 = 0101$

The table having the cosets of C as columns is called **standard array**

We construct the standard array of the $[7, 3, 4]_2$ code with generator matrix

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

0000000	0111100	1011010	1100110	1101001	1010101	0110011	0001111
1000000	1111100	0011010	0100110	0101001	0010101	1110011	1001111
0100000	0011100	1111010	1000110	1001001	1110101	0010011	0101111
0010000	0101100	1001010	1110110	1111001	1000101	0100011	0011111
0001000	0110100	1010010	1101110	1100001	1011101	0111011	0000111
0000100	0111000	1011110	1100010	1101101	1010001	0110111	0001011
0000010	0111110	1011000	1100100	1101011	1010111	0110001	0001101
0000001	0111101	1011011	1100111	1101000	1010100	0110010	0001110
1100000	1011100	0111010	0000110	0001001	0110101	1010011	1101111
1010000	1101100	0001010	0110110	0111001	0000101	1100011	1011111
0110000	0001100	1101010	1010110	1011001	1100101	0000011	0111111
1001000	1110100	0010010	0101110	0100001	0011101	1111011	1000111
0101000	0010100	1110010	1001110	1000001	1111101	0011011	0100111
0011000	0100100	1000010	1111110	1110001	1001101	0101011	0010111
1000100	1111000	0011110	0100010	0101101	0010001	**1110111**	1001011
1110000	1001100	0101010	0010110	0011001	0100101	1000011	1111111

$$H\mathbf{r} = H(\mathbf{c} + \mathbf{e}) = H\mathbf{c} + H\mathbf{e} = H\mathbf{e} = \mathbf{s}.$$

The vector $\mathbf{s} \in \mathbb{F}_q^{n-k}$ is called the **syndrome** associated to $\mathbf{r}$ (or to $\mathbf{e}$).

Definition

If $\mathbf{s}$ is a syndrome corresponding to an error of weight $\mathrm{wt}(\mathbf{e}) \leq t = \lfloor \frac{d-1}{2} \rfloor$, then we say that $\mathbf{s}$ is a **correctable syndrome**.

Let C be an $[n, k, d]_q$ code and $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$.

- $\mathbf{x}$ and $\mathbf{y}$ are in the same coset if and only if they have the same syndrome.
- $\mathbf{c} \in C$ if and only if the syndrome associated to $\mathbf{c}$ is the zero vector.

$[7, 3, 4]_2$ code with generator matrix

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

coset leader	syndrome
0000000	0000
1000000	1000
0100000	0100
0010000	0010
0001000	0001
0000100	0111
0000010	1011
0000001	0101
1100000	1100
1010000	1010
0110000	0110
1001000	1001
0101000	0101
0011000	0011
1000100	1111
1110000	1110

$[7, 3, 4]_2$ code with generator matrix

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

coset leader	syndrome
0000000	0000
1000000	1000
0100000	0100
0010000	0010
0001000	0001
0000100	0111
0000010	1011
0000001	0101

Given a table containing all the pairs $(\mathbf{e}, \mathbf{s_e})$, where $\mathbf{e}$ is the coset leader of its coset and $\mathbf{s_e}$ is the associated syndrome, the decoding algorithm proceeds as follows:

- given $\mathbf{r}$, compute the syndrome $\mathbf{s} = H\mathbf{r}$
- find the corresponding coset leaders $\mathbf{e}$ in the standard array table
- output $\mathbf{r} - \mathbf{e}$.

Definition

Let $n = \frac{q^r-1}{q-1}$ and let $H_r(q) \in \mathbb{F}_q^{r \times n}$ be a matrix with nonzero columns and such that each pair of columns are linearly independent. Then $H_r(q)$ is a parity-check matrix of the q-**ary Hamming code** (with parameter r) ($\mathcal{H}_r(q)$).

Let $r \geq 2$. Then the q-ary Hamming code $\mathcal{H}_r(q)$ has parameters:

- $n = \frac{q^r-1}{q-1}$
- $k = \frac{q^r-1}{q-1} - r$
- $d = 3$

Consider the usual $[7,4]_2$ Hamming code with parity-check matrix H, and suppose $\mathbf{r} = 1011000$ is the received word. Then the associated syndrome is

$$\mathbf{s} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

The decoding procedure for binary Hamming code is as follows:
Suppose a single error occurred in the ith component, then $\mathbf{s} = H\mathbf{e}_i = \mathbf{d}_i$, where $\mathbf{d}_i$ is the ith column of H.

- Compute the syndrome $\mathbf{s} = H\mathbf{r}$;
- Find the column $\mathbf{d}_i$ of H that matches the syndrome;
- Complement the ith bit of the received word.