Channel Coding as part of MOBCOM

Topics Covered:

- Basic of coding
- Linear Block coding
- Some algebraic error correcting codes
- Convolutional codes for error correction
  - Representation, properties
  - Soft Decoding
- Polar …. Turbo and LDPC codes
-
-

Outlines

I. Groups, Finite Fields, and Vector Spaces
II. Linear Block Codes
III. Error Detecting and Error Correcting Capabilities
IV. Error Correcting Decoders
V. Single Parity Check Codes
VI. Hamming Codes
VII. Hadamart Codes

NOTE: Many slides are generously provided by Professor Cottatellucci.

Group: Definition

Definition: A group is an algebraic system $\langle G, * \rangle$, where G is a nonempty set and $*$ is an operation on pairs of elements of G such that

(A1) *(axiom of closure)* for every a and b in G, $a * b$ is also in G;

(A2) *(associative law)* for every a, b and c in G, $a * (b * c) = (a * b) * c$;

(A3) *(existence of a neutral element)* there is an element e of G such that $a * e = e * a = a$;

(A4) *(existence of inverses)* for every a in G there is b in G such that $a * b = b * a = e$. The element b is called the inverse of a and it is denoted by a^{-1}.

Group: Examples

Let $G = \mathbb{Z}_m = \{0, 1, \ldots m-1\}$

$\langle \mathbb{Z}_m, \oplus \rangle$ **where** $\oplus$ **is addition modulo** m.

$\langle \mathbb{Z}_p \backslash \{0\}, \odot \rangle$ **where** $\odot$ **is multiplication modulo a prime** p.

$\langle \mathbb{Z}_m^N, \oplus \rangle$ **where** $\mathbb{Z}_m^N$ **is the set of** N**-tuples whose components are in** $\mathbb{Z}_m$ **and** $\oplus$ **is component-by-component addition modulo** m.

Group: Exercises

Verify that the following algebraic systems are groups, i.e. verify closure and additivity, determine neutral element, inverse elements.

Case 1

Let $G = \{0, 1\}$ and

$\boxdot$	0	1
0	0	1
1	1	0

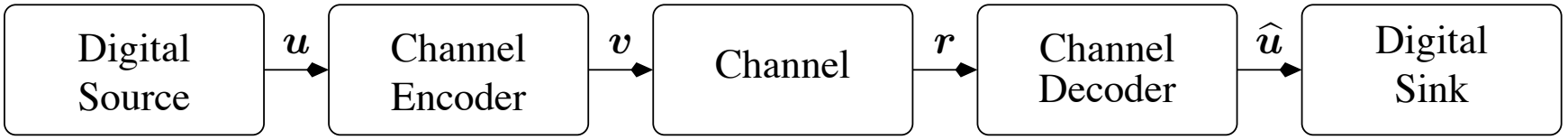
Case 2

Let $G = \{0, 1, 2, 3, 4, 5\}$ and addition modulo 6

$\boxplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Block Codes: System Model and Definitions

Communication Model



A message is segmented in blocks of k bits, $\boldsymbol{u}$.

The encoder transforms $\boldsymbol{u}$ in a block of n bits $\boldsymbol{v}$ called codeword.

Definition: A binary block code of length n is a non-empty set $\mathcal{B}$ of binary vectors of length n. Equivalently, $\mathcal{B}$ a non-empty subset of $GF(2^n)$. It is denoted by $\mathcal{C}(n,k)$. The rate of the code is $\frac{\log_2|\mathcal{B}|}{n}$.

The theory for binary ($GF(2)$) block codes can be generalized to codes on any finite field $GF(q)$.

If $q=2^r$, a block code $\mathcal{C}(n,k)$ is equivalent to a block code $\mathcal{C}(nr,kr)$ in $GF(2)$.

Linear Block Code

Definition: An (n,k) binary linear block code is a k dimensional subspace V of $GF(2^n)$. The rate is thus $R = \frac{k}{n}$.

We restrict to binary linear block codes.

Advantages of linear block codes over general block codes:

- **Easier to analyze and understand (e.g. code distance property);**
- **Easier to implement encoder and, sometimes, decoder;**
- **Excellent performance of hard, soft, and iterative decoding.**

Generator Matrix

Let $g_1, g_2, \ldots g_k$ be a basis for V, the k dimensional subspace of the codewords. Then, every codeword can be written as

$$\boldsymbol{v} = u_1\boldsymbol{g}_1 + u_2\boldsymbol{g}_2 + \ldots u_k\boldsymbol{g}_k$$

Equivalently

$$\boldsymbol{v} = (u_1, u_2, \ldots, u_k) \begin{pmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_k \end{pmatrix} = \boldsymbol{uG}.$$

Any matrix G whose rows are a basis for the linear code V is a generator matrix for V.

Some properties

The encoder needs to memorize only the k row vectors $\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots \boldsymbol{g}_k$.

The properties of a vector space/subspace and the definition of linear block codes yield

Property 1: A linear block code consists of all possible sums of the rows of a generator matrix.

Property 2: The sum of two codewords is still a codeword.

Property 3: The n-tuple of all zeros is always a codeword.

Exercise

- Consider the following codebooks

$$\mathcal{C}_1 = \{(00000), (11001), (01100), (11111)\}$$
$$\mathcal{C}_2 = \{(00000), (11001), (00110), (11111)\}$$
$$\mathcal{C}_3 = \{(00000), (10101), (01010), (11111)\}$$

  which of them is a linear block code? Explain why, eventually, they are not linear block codes.

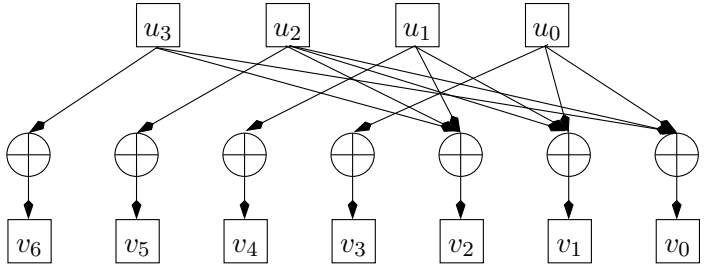
- Provide the generator matrices of the linear block codes in the previous item.
- Given the codebook $\mathcal{C}^* = \{101101, 111111\}$ add one or more codewords such that the resulting codebook is linear.

Examples and Implementation

A parity check code $(7, 4)$

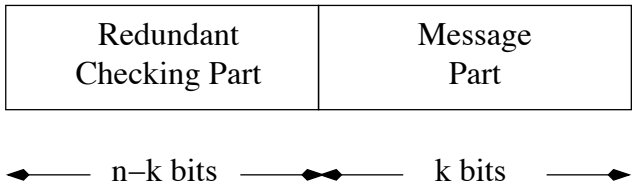
$$
\begin{aligned}
v_6 &= u_3 \\
v_5 &= u_2 \\
v_4 &= u_1 \\
v_3 &= u_0 \\
v_2 &= u_1 + u_2 + u_3 \\
v_1 &= u_0 + u_1 + u_2 \\
v_0 &= u_0 + u_2 + u_3
\end{aligned}
$$

$$
\boldsymbol{v} = (u_0, u_1, u_2, u_3) \underbrace{\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}}_{\text{Generator matrix}}
$$



Systematic Codes

Systematic Structure of a Codeword



Definition: An (n, k) block code is called systematic if it has a generator matrix of the form

$$\boldsymbol{G} = (\boldsymbol{P}, \boldsymbol{I}_k)$$

where $\boldsymbol{P}$ is a $k \times (n-k)$ matrix.

Any generator matrix can be reduced to a systematic generator matrix by linear combination of rows and/or column permutations.

Parity Check Coding Matrix

Definition: The equations uP are called the parity check equations of the code.

Equivalent representation of a code $\mathcal{C}(n,k)$ generated by $\boldsymbol{G}$:

An n-tuple v is a codeword of the code $\mathcal{C}(n,k)$ generated by $\boldsymbol{G} = (\boldsymbol{P}, \boldsymbol{I}_k)$ if and only if $v\boldsymbol{H}^T = 0$ with

$$\boldsymbol{H} = (\boldsymbol{I}_{n-k}, \boldsymbol{P}^T).$$

Definition: The matrix H is called the parity check matrix.

Property The matrix H is the null space of G, i.e. G and H are orthogonal

$$\boldsymbol{G}\boldsymbol{H}^T = 0$$

Exercise

Consider a linear block code defined by the parity check equations below and determine the parity check coding matrix and the generator matrix

Parity Check Equations

$$
\begin{aligned}
x_1 + x_3 + x_4 &= 0 \\
x_3 + x_5 &= 0 \\
x_1 + x_3 + x_6 &= 0 \\
x_2 + x_3 + x_7 &= 0 \\
x_1 + x_2 + x_8 &= 0 \\
x_2 + x_9 &= 0 \\
x_1 + x_2 + x_{10} &= 0
\end{aligned}
$$

Parity Check and Generator Matrices

$$
\boldsymbol{H} = \begin{pmatrix}
101 & 1000000 \\
001 & 0100000 \\
101 & 0010000 \\
011 & 0001000 \\
110 & 0000100 \\
010 & 0000010 \\
110 & 0000001
\end{pmatrix}
$$

$$
\boldsymbol{G} = \begin{pmatrix}
100 & 1010101 \\
010 & 0001111 \\
001 & 1111000
\end{pmatrix}
$$

2 Maximum likelihood detection

- Probabilistic criterion for decoding is equivalent to finding the closest codeword.
- Given a received vector $\mathbf{r}$
- Minimize the probability of error
- Find codeword $\mathbf{c}_i$ which maximizes $P(\mathbf{c} = \mathbf{c}_i|\mathbf{r})$. This is called the *maximum a posteriori* decision rule.
- We note by Bayes rule that

$$P(\mathbf{c}|\mathbf{r}) = \frac{P(\mathbf{c})P(\mathbf{r}|\mathbf{c})}{P(\mathbf{r})},$$

where $P(\mathbf{r})$ is the probability of observing the vector $\mathbf{r}$.

- $P(\mathbf{r})$ is independent of $\mathbf{c}$, so max $P(\mathbf{c}|\mathbf{r})$ is equivalent to maximizing

$$P(\mathbf{c})P(\mathbf{r}|\mathbf{c}).$$

Assume equiprobable *codeword*s, so maximize $P(\mathbf{r}|\mathbf{c})$.

- M*aximum likelihood* criterion.

Let us see what this means for us.

$$P(\mathbf{r}|\mathbf{c}) = \prod_{i=1}^{n} P(r_i|c_i)$$

Assuming a BSC channel with crossover probability p, we have

$$P(r_i|c_i) = \begin{cases} 1-p & \text{if} c_i = r_i \\ p & \text{if} c_i \neq r_i \end{cases}$$

Then

$$\begin{aligned} P(\mathbf{r}|\mathbf{c}) &= \prod_{i=1}^{n} P(r_i|c_i) = (1-p)^{\#(p_i=c_i)} p^{\#(p_i \neq c_i)} \\ &= (1-p)^{n-\#(p_i \neq c_i)} p^{\#(p_i \neq c_i)} = (1-p)^n \left(\frac{p}{1-p}\right)^{d(\mathbf{c},\mathbf{r})}. \end{aligned}$$

Then if we want to maximize $P(\mathbf{r}|\mathbf{c})$, we should choose that $\mathbf{c}$ which is **closest** to $\mathbf{r}$, since $0 \leq (p/(1-p)) \leq 1$. Thus, under our assumptions, the ML criterion is the minimum distance criterion. In every case, we should choose the error vector of lowest weight.

Syndrome and Error Detection

Error Vector $\boldsymbol{e} = \boldsymbol{r} + \boldsymbol{v}$ with

$$e_j = \begin{cases} 0 & \text{for } r_j = v_j, \\ 1 & \text{for } r_j \neq v_j. \end{cases}$$

Definition: A syndrome is the $(n-k)$-dimensional vector $\boldsymbol{s} = \boldsymbol{r}\boldsymbol{H}^T$

$$\boldsymbol{s} \neq 0 \quad \Rightarrow \boldsymbol{r},\, \boldsymbol{e} \notin \mathcal{C}(n,k) \qquad \text{Detected Error}$$

$$(\boldsymbol{s} = 0) \wedge (\boldsymbol{e} \neq \boldsymbol{0}) \quad \Rightarrow \quad \boldsymbol{r},\, \boldsymbol{e} \in \mathcal{C}(n,k) \qquad \text{Undetectable Error}$$

($2^k - 1$ undetectable errors)

Exercise

- Consider the encoder proposed at page 21 and determine its codewords.
- Determine the number of undetectable error patterns of weight 1, 2, 3, 4, 5, 6, 7, 8, 9.
- Determine the percentage of error pattern of weight 1,2,...9 that can be detected by the code.
- Given a BSC with error probability ϵ, determine the probability that an error pattern of weight 5 occurs.

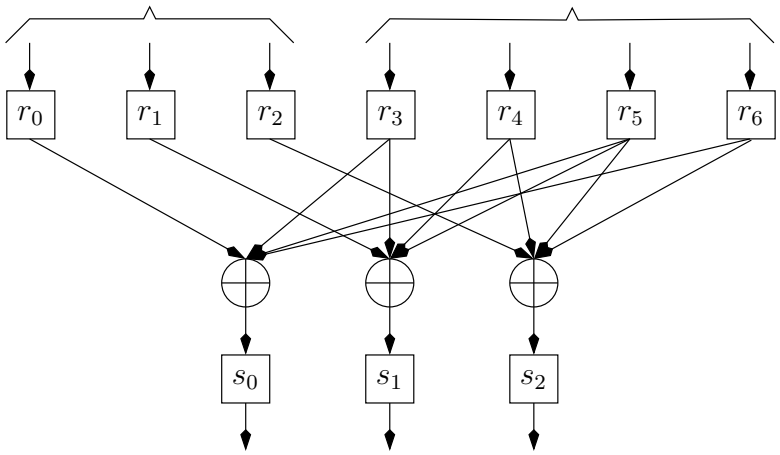
Syndrome Circuit: An Example

Parity Check Equations

$$\boldsymbol{v}_0 = \boldsymbol{u}_0 + \boldsymbol{u}_2 + \boldsymbol{u}_3$$

$$\boldsymbol{v}_1 = \boldsymbol{u}_0 + \boldsymbol{u}_1 + \boldsymbol{u}_2$$

$$\boldsymbol{v}_2 = \boldsymbol{u}_1 + \boldsymbol{u}_2 + \boldsymbol{u}_3$$



$$\boldsymbol{s} = \boldsymbol{r}\boldsymbol{H}^T = (\boldsymbol{v} + \boldsymbol{e})\boldsymbol{H}^T = \boldsymbol{e}\boldsymbol{H}^T$$

Linear system of $n - k$ equations in n unknowns. $\Rightarrow$ There are 2^k possible solutions. $\Rightarrow$ Among all possible solutions we choose the one that minimize the error codeword probability.

An Example

Let us transmit a codeword $\boldsymbol{v} = (1001011)$ of the $(7, 4)$ code proposed in slide 18 and let us receive $\boldsymbol{r} = (1001001)$

```
H = [ 1 0 0  1 0 1 1 ;
      0 1 0 1 1 1 0 ;
      0 0 1 0 1 1 1 ]
e = r-v = [0 0 0 0 0 1 0]
s = r * H^T = [1 1 1]
```

$$\boldsymbol{s} = \boldsymbol{r}\boldsymbol{H}^T = \boldsymbol{e}\boldsymbol{H}^T = (1, 1, 1)$$

System of linear equations for the error

$$\begin{aligned} 1 &= e_0 + e_3 + e_5 + e_6 \\ 1 &= e_1 + e_3 + e_4 + e_5 \\ 1 &= e_2 + e_4 + e_5 + e_6 \end{aligned}$$

Solutions

$$\begin{array}{cccc} (0000010) & (1110000) & (1010011) & (0100001) \\ (1101010) & (0011000) & (0111011) & (1001001) \\ (0110110) & (1000100) & (1100111) & (0010101) \\ (1011110) & (0101100) & (0001111) & (1111101) \end{array}$$

$\boldsymbol{e}^* = (0000010)$ is the most probable error vector for memoryless BSC.
We assume $\boldsymbol{e}^*$ to be actual error and reconstruct the transmitted vector

$$\begin{aligned} \widehat{\boldsymbol{v}} &= \boldsymbol{r} + \boldsymbol{e}^* \\ &= (1001001) + (0000010) \\ &= (1001011) \end{aligned}$$

Hamming Distance

Definition: $w(\boldsymbol{v})$, **Hamming weight of** $\boldsymbol{v}$ **is the number of nonzero components of** $\boldsymbol{v}$.

Definition: The minimum weight $w_{\min}$ **of a linear code** $\mathcal{C}(n,k)$ **is the minimum weight of its nonzero codewords, i.e.** $w_{\min} = \min_{\boldsymbol{x}\in\{\boldsymbol{x}\in\mathcal{C},\boldsymbol{x}\neq\mathbf{0}\}} w(\boldsymbol{x})$.

Definition: $d(\boldsymbol{v},\boldsymbol{w})$, **the Hamming distance between the vectors** $\boldsymbol{v}$ **and** $\boldsymbol{w}$ **is the number of elements where** $\boldsymbol{v}$ **and** $\boldsymbol{w}$ **differ, or equivalently,** $d(\boldsymbol{v},\boldsymbol{w}) = w(\boldsymbol{v}+\boldsymbol{w})$.

Definition: The minimum distance of a linear code $\mathcal{C}(n,k)$, **denoted by** $d_{\min}$ **is defined as**

$$d_{\min} = \min\{d(\boldsymbol{v},\boldsymbol{w}) : \boldsymbol{v},\boldsymbol{w} \in \mathcal{C}(n,k), \boldsymbol{v} \neq \boldsymbol{w}\}$$

Theorem: The minimum distance of a linear block code is equal to the minimum weight of its nonzero codewords and viceversa.

$$\begin{aligned} d_{\min} &= \min\{d(\boldsymbol{v},\boldsymbol{w}) : \boldsymbol{v},\boldsymbol{w} \in \mathcal{C}(n,k), \boldsymbol{v} \neq \boldsymbol{w}\} \\ &= \min\{w(\boldsymbol{x}) : \boldsymbol{x} \in \mathcal{C}(n,k), \boldsymbol{x} \neq \mathbf{0}\} \\ &= w_{min} \end{aligned}$$

Minimum Distance

Theorem: Let $\mathcal{C}(n,k)$ be a linear code with parity check matrix H. For each codeword of Hamming weight ℓ, there exist ℓ columns of H such that the vector sum of these columns is equal to the zero vector. Conversely, if there exist ℓ columns of H whose vector sum is the zero vector, there exists a codeword of Hamming weight ℓ.

Corollary: Let $\mathcal{C}(n,k)$ be a linear block code with parity check matrix H. If no $d-1$ columns of H add to zero, the code has minimum distance at least d.

Corollary: Let $\mathcal{C}(n,k)$ be a linear block code with parity check matrix H. The minimum distance of the code is equal to the smallest number of columns of H that sum to 0.

Error Detection Capabilities

- Recall: any error pattern that is not a codeword, is detectable. Hence-->
- If a code has minimum distance $d_{\min}$ it can detect any error pattern of weight not greater than $d_{\min} - 1$.
- There are $2^n - 2^k$ detectable error patterns even with $d_{\min}$ or more errors .
- There are $2^k - 1$ undetectable error patterns.

Definition: Let A_i be the number of codewords of weight i in the linear block code $\mathcal{C}(n, k)$. The numbers $A_1, A_2, \ldots A_n$ are called the weight distribution of $\mathcal{C}(n, k)$.

Probability of Undetected Error

$$P_u(E) = \sum_{i=1}^{n} A_i \varepsilon^i (1-\varepsilon)^{n-i}$$

** Compute the probability of undetected error for the code at page 21. Make use of the intermediate results obtained for the exercise at page 23.

Error Correction Capabilities

Theorem: If a linear block code $\mathcal{C}(n,k)$ had minimum distance $d_{\min}$, it is capable to correct all error patterns of t or fewer errors with

$$2t+1 \leq d_{\min} \leq 2t+2.$$

Proof: Let transmit $\boldsymbol{v}$ and receive $\boldsymbol{r}$. For another codeword $\boldsymbol{w} \in \mathcal{C}(n,k)$

$$d(\boldsymbol{v},\boldsymbol{r}) + d(\boldsymbol{w},\boldsymbol{r}) \geq d(\boldsymbol{v},\boldsymbol{w})$$

then $d(\boldsymbol{w},\boldsymbol{v}) \geq d_{\min} \geq 2t+1$.

Let an error pattern with t' errors occur $\Rightarrow d(\boldsymbol{v},\boldsymbol{r}) = t'$. Then

$$\begin{aligned} d(\boldsymbol{w},\boldsymbol{r}) &\geq d(\boldsymbol{w},\boldsymbol{v}) - d(\boldsymbol{v},\boldsymbol{r}) \\ &\geq 2t+1-t' \end{aligned}$$

If $t' < t$ then $d(\boldsymbol{w},\boldsymbol{r}) > t$ and for a BSC channel $\boldsymbol{v}$ is the codeword closest to $\boldsymbol{r}$. Applying maximum likelihood decoding $P(\boldsymbol{r}|\boldsymbol{v})$ is greater than $P(\boldsymbol{r}|\boldsymbol{w})$ for $\boldsymbol{v} \neq \boldsymbol{w}$ and the decoder detects correctly $\boldsymbol{v}$.

In contrast, it can be shown that for $t' > t$ there exists at least an error pattern that can not be reconstructed correctly.

Error Correction Capabilities

Definition: The parameter $t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ is called the error correcting capability of the code.

Definition: The code is referred to as a t-error correcting code.

Upper bound on the Probability of Erroneous Decoding in BSC

$$P(E) \leq \sum_{i=t+1}^{n} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i}$$

Standard Array of a Linear Block Code

A standard array is a rule to partition the 2^n possible received signal into 2^k disjoint sets.

1. Place the 2^k codewords of C in a row with all-zero codeword $\boldsymbol{v}_1 = (00\ldots0)$ in the first (leftmost) position;
2. From the $2^n - 2^k$ remaining elements of $GF(2^n)$ choose an n-tuple $\boldsymbol{e}_2$ and place it under the vector $\boldsymbol{v}_1$;
3. Build the second row by adding $\boldsymbol{e}_2$ to each codeword $\boldsymbol{v}_i$ in the first row;
4. Build the third row by choosing a vector $\boldsymbol{e}_3$ that does not appears in the first two rows and add it to each $\boldsymbol{v}_i$, $1 \leq i \leq 2^k$;
5. Repeat the previous step until all elements of $GF(2^n)$ are in the table.

$\boldsymbol{v}_1 = \boldsymbol{0}$	$\boldsymbol{v}_2$	$\ldots$	$\boldsymbol{v}_j$	$\ldots$	$\boldsymbol{v}_{2^k}$
$\boldsymbol{e}_2$	$\boldsymbol{e}_2 + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_2 + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_2 + \boldsymbol{v}_{2^k}$
$\boldsymbol{e}_3$	$\boldsymbol{e}_3 + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_3 + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_3 + \boldsymbol{v}_{2^k}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\boldsymbol{e}_\ell$	$\boldsymbol{e}_\ell + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_\ell + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_\ell + \boldsymbol{v}_{2^k}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\boldsymbol{e}_{2^{n-k}}$	$\boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_{2^k}$

Example

Consider the $(6, 3)$ linear code with generator matrix

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

The standard array is

Coset Leader							
000000	011100	101010	110001	110110	101101	011011	000111
100000	111100	001010	010001	010110	001101	111011	100111
010000	001100	111010	100001	100110	111101	001011	010111
001000	010100	100010	111001	111110	100101	010011	001111
000100	011000	101110	110101	110010	101001	011111	000011
000010	011110	101000	110011	110100	101111	011001	000101
000001	011101	101011	110000	110111	101100	011010	000110
100100	111000	001110	010101	010010	001001	111111	100011

Error Correcting Decoders

General Approach:

- The 2^n n-tuple over $GF(2)$ are partitioned into 2^k disjoint sets $D_1, D_2, \ldots D_{2^k}$ such that the codeword $\boldsymbol{v}_i$ is contained in D_i, for $1 \leq i \leq 2^k$.
- If the received vector $\boldsymbol{r}$ is found in the subset D_j, $\boldsymbol{r}$ is decoded into $\boldsymbol{v}_j$.
- The detection is correct if and only if $\boldsymbol{r}$ is in the set D_i that corresponds to the transmitted codeword.

Complexity: storage of 2^k sets consisting of a total of 2^n vectors of n bits ($n2^n$ bits) and repeated comparison of the received vector.

If n and k are large the complexity is unacceptable!

Some Definitions

- The 2^{n-k} rows of the standard array are called the cosets of the code C;
- The first n-tuple $\boldsymbol{e}_j$ of each coset is called a coset leader or coset representative;
- Any element of a coset can be used as its coset leader. This does not change the elements of the coset, it simply permutes them.
- The standard array induces a partition$^{(*)}$ of $GF(2^n)$ in 2^k sets

$$D_j = \{\boldsymbol{v}_j, \boldsymbol{e}_2 + \boldsymbol{v}_j, \boldsymbol{e}_3 + \boldsymbol{v}_j, \ldots \boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_j\}$$

Coset Leader			D_j		
$\boldsymbol{v}_1 = \boldsymbol{0}$	$\boldsymbol{v}_2$	$\ldots$	$\boldsymbol{v}_j$	$\ldots$	$\boldsymbol{v}_{2^k}$
$\boldsymbol{e}_2$	$\boldsymbol{e}_2 + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_2 + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_2 + \boldsymbol{v}_{2^k}$
$\boldsymbol{e}_3$	$\boldsymbol{e}_3 + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_3 + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_3 + \boldsymbol{v}_{2^k}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\boldsymbol{e}_\ell$	$\boldsymbol{e}_\ell + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_\ell + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_\ell + \boldsymbol{v}_{2^k}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\boldsymbol{e}_{2^{n-k}}$	$\boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_2$	$\ldots$	$\boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_j$	$\ldots$	$\boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_{2^k}$

$^{(*)}$ We will show later that a standard array induces a partition on $GF(2^n)$.

Some Properties of a Standard Array

Theorem: No two n-tuples in the same row of a standard array are identical. Every n-tuple is in one and only one row.

Proof: 1) Let us assume that two n-tuples on the same line are identical. Then,

$$\begin{aligned} & \boldsymbol{e}_\ell + \boldsymbol{v}_j = \boldsymbol{e}_\ell + \boldsymbol{v}_i, i \neq j \\ \Longrightarrow \quad & \boldsymbol{v}_j = \boldsymbol{v}_i \end{aligned}$$

which is impossible.

2) Assume two n-tuples in different rows are identical

$$\begin{aligned} \boldsymbol{e}_m + \boldsymbol{v}_i = \boldsymbol{e}_n + \boldsymbol{v}_j \qquad & \text{with } m < n \\ \boldsymbol{e}_n = \boldsymbol{e}_m + \boldsymbol{v}_i + \boldsymbol{v}_j = \boldsymbol{e}_m + \boldsymbol{v}_k \qquad & \text{with } \boldsymbol{v}_k = \boldsymbol{v}_i + \boldsymbol{v}_j \in C \end{aligned}$$

$\boldsymbol{e}_n$ should be in the coset having as coset leader $\boldsymbol{e}_m$ but this is impossible for the construction of the standard array.

A standard array induces a partition in $GF(2^n)$.

Some Properties of a Standard Array (cntd)

Theorem: All the 2^k n-tuples of a coset have the same syndrome. The syndromes for different cosets are different.

Proof:

1) Let us consider a coset with coset leader $\boldsymbol{e}_i$. Any vector $\boldsymbol{v}_j + \boldsymbol{e}_i$ belonging to such a coset has syndrome

$$(\boldsymbol{v}_j + \boldsymbol{e}_i)\boldsymbol{H}^T = \boldsymbol{e}_i\boldsymbol{H}^T.$$

Then, all n-tuples belonging to a coset have the same syndrome as the coset leader.

2) Let us consider two different cosets with coset leaders $\boldsymbol{e}_m$ and $\boldsymbol{e}_n$ with $m < n$. If they had the same syndrome then

$$\begin{aligned} \boldsymbol{e}_m\boldsymbol{H}^T &= \boldsymbol{e}_n\boldsymbol{H}^T \\ (\boldsymbol{e}_m + \boldsymbol{e}_n)\boldsymbol{H}^T &= \boldsymbol{0} \\ \boldsymbol{v}_\ell\boldsymbol{H}^T &= \boldsymbol{0} \qquad \boldsymbol{v}_\ell = \boldsymbol{e}_m + \boldsymbol{e}_n \in C. \end{aligned}$$

Then, $\boldsymbol{e}_n = \boldsymbol{e}_m + \boldsymbol{v}_\ell$ which is impossible because of the construction of the standard array.

Some Properties of a Standard Array (cntd)

Theorem: Every (n, k) linear block code is capable of correcting 2^{n-k} error patterns.

Proof: It follows from the fact that errors can be corrected only if the error pattern is a coset leader.

In fact, if the error is a coset leader $\boldsymbol{e}_\ell$ and $\boldsymbol{v}_j$ is transmitted $\boldsymbol{r} = \boldsymbol{e}_\ell + \boldsymbol{v}_j$ is in D_j and $\boldsymbol{v}_j$ is detected properly.

If the error $\boldsymbol{x}$ is not a coset leader, then $\boldsymbol{x}$ is in the standard array as $\boldsymbol{x} = \boldsymbol{v}_m + \boldsymbol{e}_\ell$. The received vector is

$$\boldsymbol{r} = \boldsymbol{v}_j + \boldsymbol{x} = \boldsymbol{v}_j + \boldsymbol{v}_m + \boldsymbol{e}_\ell = \boldsymbol{v}_s + \boldsymbol{e}_\ell \text{ with } \boldsymbol{v}_j + \boldsymbol{v}_m = \boldsymbol{v}_s \in C.$$

Then, $\boldsymbol{r} \in D_s$ and erroneously we detect $\boldsymbol{v}_s$ instead of $\boldsymbol{v}_j$.

tx = vj
if x was coset leader, then OK
x not coset leader
x = el + vm (el coset leader)
r = vj +x (reality)
==> r = vj+vm+ el = vs +el
so you will decode vs (instead of vj)
because el is coset leader

Standard Array and Maximum Likelihood Detection

- The probability of a decoding error is minimized if the most frequent error patterns are coset leaders;
- In a BSC an error pattern of smaller weight is more probable than an error pattern of larger weight;
- In a BSC, a standard array should be built choosing as coset leader the n-tuple with least weight among the remaining n-tuples.
- The partition induced by such a standard array yields the maximum likelihood decoder.

Definition: Let α_i denote the number of coset leaders with weight i. The numbers $\alpha_0, \alpha_1, \ldots \alpha_n$ are called the weight distribution of the coset leaders.

Error Probability for a BSC

$$P(E) = 1 - \sum_{i=0}^{n} \alpha_i \varepsilon^i (1-\varepsilon)^{n-i}.$$

Syndrome Decoding or Table Look-up Decoding

1. Compute the syndrome of $\boldsymbol{r}$, $\boldsymbol{r}\boldsymbol{H}^T$;
2. Locate the coset leader $\boldsymbol{e}_\ell$ whose syndrome is equal to $\boldsymbol{r}\boldsymbol{H}^T$.
3. Assume $\boldsymbol{e}_\ell$ to be the actual error pattern;
4. Decode $\boldsymbol{r}$ into the codeword $\boldsymbol{v}^* = \boldsymbol{r} + \boldsymbol{e}_\ell$.