Θεωρία Πληροφορίας και Κωδίκων

Δρ. Νικόλαος Κολοκοτρώνης
Λέκτορας

Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Υπολογιστών
Τέρμα Οδού Καραϊσκάκη, 22100 Τρίπολη

E–mail: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

Ενότητα 2^{η} : *εισαγωγή στη θεωρία κωδίκων*

http://eclass.uop.gr/courses/CST273/

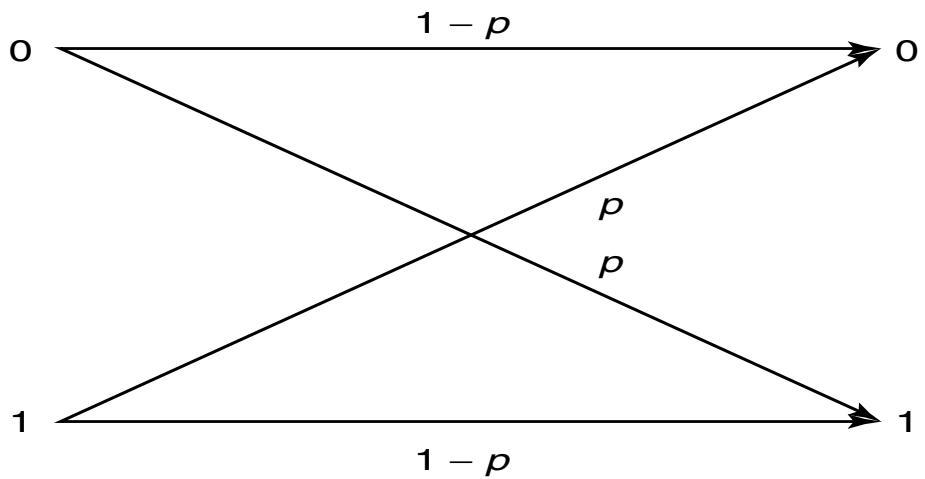
Περιεχόμενα Ομιλίας

Πρόβλημα Αξιόπιστης Επικοινωνίας

Example (Binary Symmetric Channel – BSC)

Given input $\boldsymbol{v} = (v_0 \ \cdots \ v_{n-1})$, the output $\boldsymbol{r} = (r_0 \ \cdots \ r_{n-1})$ satisfies

- $r_i \neq v_i$ with probability p
- $r_i = v_i$ with probability $1 - p$



$\forall\, i = 0, \ldots, n-1$ and $0 \leq p \leq 1$; *what happens if* $p = \frac{1}{2}$*?*

Τμηματικοί Κώδικες

Let the output of the source be a sequence over $\mathbb{F}_2 = \{0, 1\}$. In block coding:

- a sequence is segmented into blocks $\boldsymbol{u}$ of fixed length k
- the encoder transforms each $\boldsymbol{u}$ into an n-tuple $\boldsymbol{v}$ with $n > k$
- there should be $1 - 1$ correspondence between $\boldsymbol{u}$ and $\boldsymbol{v}$

Important things to remember:

- the set $\mathscr{C} = \{\boldsymbol{v} \in \mathbb{F}_2^n : \boldsymbol{v} = f(\boldsymbol{u}), \boldsymbol{u} \in \mathbb{F}_2^k\}$ is a (n, k) *block code*
- $\exists\, 2^k$ different *codewords* $\boldsymbol{v}$ of length n
- $\exists\, 2^k$ different *message blocks* $\boldsymbol{u}$ of length k

Unless $f : \mathbb{F}_2^k \to \mathbb{F}_2^n$ has a certain special structure, encoding/decoding will be prohibitively complex for large k, n.

Ορισμός Γρ. Τμηματικών Κωδίκων

We restrict our attention to *linear block codes* that can be mechanized in a practical manner

Definition

A block code $\mathscr{C}$ of length n and 2^k codewords is a *linear* (n, k) *code* if and only if its codewords form a k–dimensional subspace of $\mathbb{F}_2^n$.

Q: What does this imply?

- the modulo–2 sum of two codewords is also a codeword
- it is possible to find k LI codewords $\boldsymbol{g}_0, \ldots, \boldsymbol{g}_{k-1}$ of $\mathscr{C}$ such that

$$\boldsymbol{v} = u_0\boldsymbol{g}_0 + \cdots + u_{k-1}\boldsymbol{g}_{k-1}, \qquad \forall\, \boldsymbol{v} \in \mathscr{C} \tag{1}$$

where $u_i \in \mathbb{F}_2$

Ορισμός Γρ. Τμηματικών Κωδίκων (*συν.*)

- if we write (1) in matrix formulation, we get that

$$\boldsymbol{v} = \boldsymbol{u} \cdot \begin{pmatrix} \boldsymbol{g}_0 \\ \vdots \\ \boldsymbol{g}_{k-1} \end{pmatrix} \quad \Leftrightarrow \quad \boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{G}, \quad \forall\, \boldsymbol{v} \in \mathscr{C} \tag{2}$$

  where $\boldsymbol{u} = (u_0 \ \cdots \ u_{k-1})$ and $\boldsymbol{G}$ is the $k \times n$ matrix

$$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{g}_0 \\ \vdots \\ \boldsymbol{g}_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

- the rows of $\boldsymbol{G}$ generate or span the entire (n, k) linear code $\mathscr{C}$
  - $\boldsymbol{G}$ is called a *generator matrix* for $\mathscr{C}$
- the encoder only stores the rows of $\boldsymbol{G}$ to process the input $\boldsymbol{u}$

Παράδειγμα $(7, 4)$ Κώδικα

An $(7, 4)$ linear code $\mathscr{C}$ is given by

message $\boldsymbol{u}$	codeword $\boldsymbol{v}$	–
(0000)	(0000000)	
(1000)	(1101000)	$\star$
(0100)	(0110100)	$\star$
(1100)	(1011100)	
(0010)	(1110010)	$\star$
(1010)	(0011010)	
(0110)	(1000110)	
(1110)	(0101110)	
(0001)	(1010001)	$\star$
(1001)	(0111001)	
(0101)	(1100101)	
(1101)	(0001101)	
(0011)	(0100011)	
(1011)	(1001011)	
(0111)	(0010111)	
(1111)	(1111111)	

The codewords marked with $\star$ are LI; so the matrix

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

is a generator matrix for the $(7, 4)$ linear code $\mathscr{C}$

Q: Did you notice any structure in $\mathscr{C}$ and $\boldsymbol{G}$?

- the right part of $\boldsymbol{v} \in \mathscr{C}$ equals $\boldsymbol{u}$
- the right part of $\boldsymbol{G}$ equals $\boldsymbol{I}_4$

Συστηματικοί Κώδικες

The above structure, according to which a codeword is divided into two parts (the message part and the redundant checking part), is desirable

Definition

A linear block code is called a (n, k) *linear systematic block code* if

- the message part consists of the k information digits (unaltered)
- the redundant checking part consists of $n-k$ parity–check digits (linear sums of the information digits)

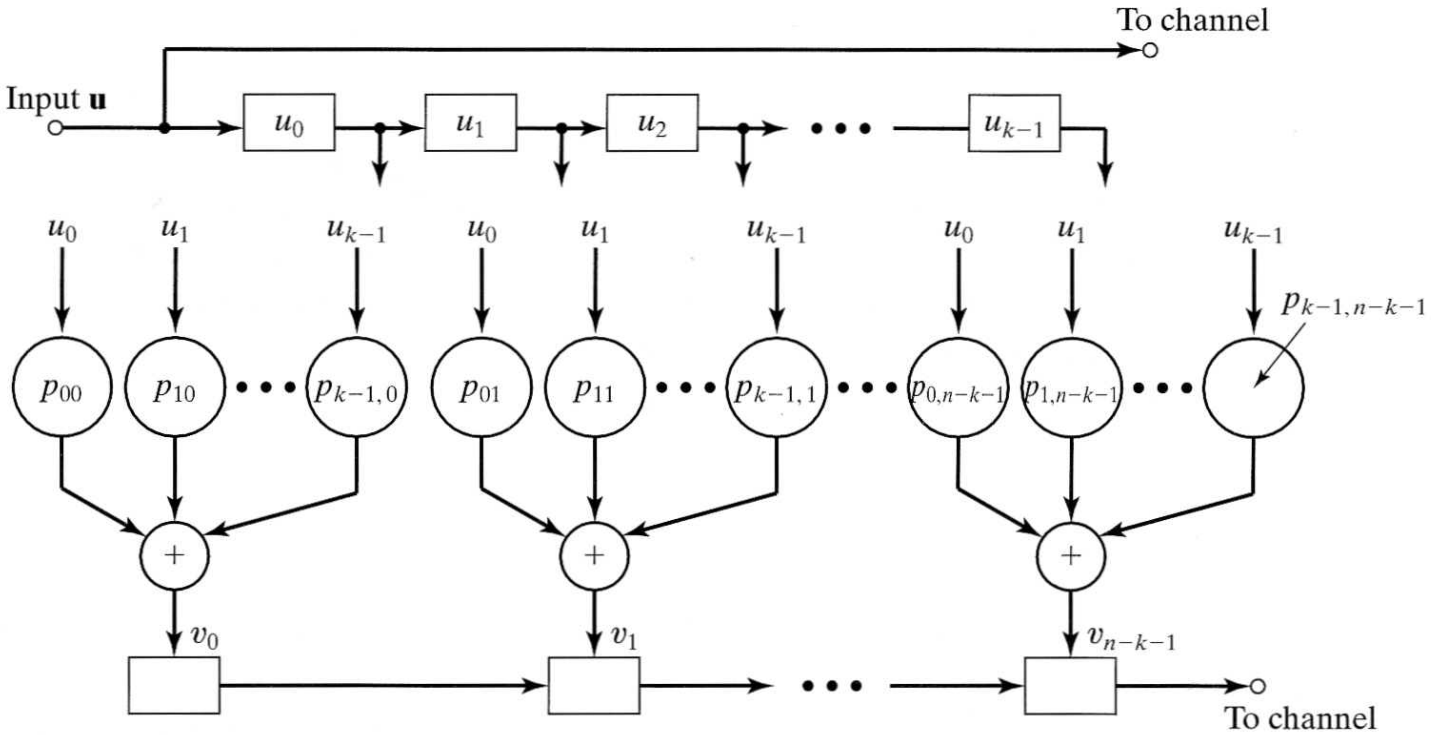
Then, we can write $\boldsymbol{G} = \begin{pmatrix} \boldsymbol{P} & \boldsymbol{I}_k \end{pmatrix}$ where $\boldsymbol{P}$ is an $k \times n-k$ matrix, and

$$\boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{G} = \boldsymbol{u} \cdot \begin{pmatrix} \boldsymbol{P} & \boldsymbol{I}_k \end{pmatrix} = \begin{pmatrix} \boldsymbol{u} \cdot \boldsymbol{P} & \boldsymbol{u} \cdot \boldsymbol{I}_k \end{pmatrix} = \begin{pmatrix} \boldsymbol{u} \cdot \boldsymbol{P} & \boldsymbol{u} \end{pmatrix}$$

The $n-k$ equations $\boldsymbol{u} \cdot \boldsymbol{P}$ are the *parity–check equations* of the code $\mathscr{C}$

Κύκλωμα Κωδικοποίησης (n, k) Κώδικα

Hence, we have $v_j = \boldsymbol{u} \cdot \boldsymbol{p}_j^t = \sum_{i=0}^{k-1} u_i p_{ij}$, for all $0 \leq j < n-k$, which leads to the encoding circuit



The encoding complexity is $\Theta(n)$, that is linearly proportional to n

Πίνακας Ισοτιμίας

Another useful matrix associated with the (n, k) code $\mathscr{C}$ is an $n-k \times n$ matrix $\boldsymbol{H}$ called *parity–check matrix*

Proposition

If $\mathscr{C}$ is the (n, k) code generated by $\boldsymbol{G}$, then $\boldsymbol{v} \in \mathscr{C}$ if and only if

$$\boldsymbol{v} \cdot \boldsymbol{H}^t = \mathbf{0}, \qquad \forall\, \boldsymbol{v} \in \mathscr{C}\,. \tag{3}$$

Due to the way $\boldsymbol{H}$ is constructed:

- the rows of $\boldsymbol{H}$ are LI, that is, $\text{rank}(\boldsymbol{H}) = n - k$
- every vector in the *row space* of $\boldsymbol{G}$ is orthogonal to the rows of $\boldsymbol{H}$
- the code $\mathscr{C}$ coincides with the *null space* of $\boldsymbol{H}$

Πίνακας Ισοτιμίας (*συν.*)

From (2) and (3) we have $(\boldsymbol{u} \cdot \boldsymbol{G}) \cdot \boldsymbol{H}^t = \boldsymbol{0}$ for all $\boldsymbol{u} \in \mathbb{F}_2^k$, which leads to

$$\boldsymbol{G} \cdot \boldsymbol{H}^t = \boldsymbol{0}. \tag{4}$$

If $\boldsymbol{G} = \begin{pmatrix} \boldsymbol{P} & \boldsymbol{I}_k \end{pmatrix}$, then $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{P}^t \end{pmatrix}$

Definition (dual code)

The $(n, n-k)$ linear block code generated by (the rows of) $\boldsymbol{H}$ is called the *dual code* of $\mathscr{C}$ and is denoted by $\mathscr{C}^\perp$

From (4) we obtain $(\boldsymbol{u} \cdot \boldsymbol{G}) \cdot (\widetilde{\boldsymbol{u}} \cdot \boldsymbol{H})^t = 0$ for all $\boldsymbol{u} \in \mathbb{F}_2^k$, $\widetilde{\boldsymbol{u}} \in \mathbb{F}_2^{n-k}$; hence:

Proposition

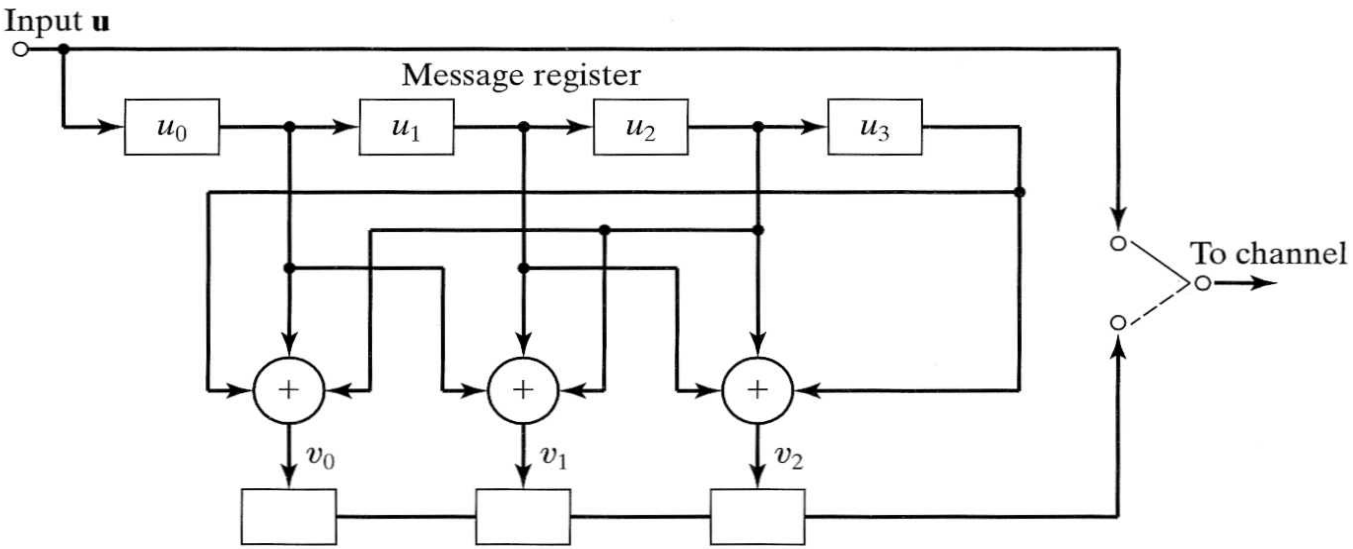
Let $\mathscr{C}$ and $\mathscr{C}'$ be (n, k) and $(n, n-k)$ linear block codes respectively; then $\mathscr{C}' = \mathscr{C}^\perp$ if and only if $\boldsymbol{v} \cdot \widetilde{\boldsymbol{v}}^t = 0, \forall\, \boldsymbol{v} \in \mathscr{C}$ and $\widetilde{\boldsymbol{v}} \in \mathscr{C}'$.

Παράδειγμα $(7, 4)$ Κώδικα (*συν.*)

The parity–check matrix (generator matrix of $\mathscr{C}^{\perp}$) of the $(7, 4)$ linear block code $\mathscr{C}$ is given by

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

The encoding circuit is shown below



Τρόπος Υπολογισμού Συνδρόμου

- because of the channel noise $\boldsymbol{r} \neq \boldsymbol{v}$; the vector $\boldsymbol{e} = \boldsymbol{r} + \boldsymbol{v}$ is called *error vector*
  - the 1's in $\boldsymbol{e}$ correspond to transmission errors
- to detect the presence of errors the decoder computes

$$\boldsymbol{s} = \boldsymbol{r} \cdot \boldsymbol{H}^t \tag{5}$$

  which is called the *syndrome* of $\boldsymbol{r}$
  - $\boldsymbol{s} = \boldsymbol{0}$ if and only if $\boldsymbol{r} \in \mathscr{C}$ (and $\boldsymbol{s} \neq \boldsymbol{0}$ if and only if $\boldsymbol{r} \notin \mathscr{C}$)
- if $\boldsymbol{r} \neq \boldsymbol{v}$ and $\boldsymbol{e} \in \mathscr{C}$, then the error cannot be detected!
  - these error patterns are called *undetectable* error patterns
  - $\exists\, 2^k - 1$ undetectable error patterns
  - in this case, the decoder performs a *decoding error*

Τρόπος Υπολογισμού Συνδρόμου (*συν.*)

Proposition

The syndrome $\boldsymbol{s}$ *computed via* (5) *depends only on* $\boldsymbol{e}$*, that is* $\boldsymbol{s} = \boldsymbol{e} \cdot \boldsymbol{H}^t$

Proof

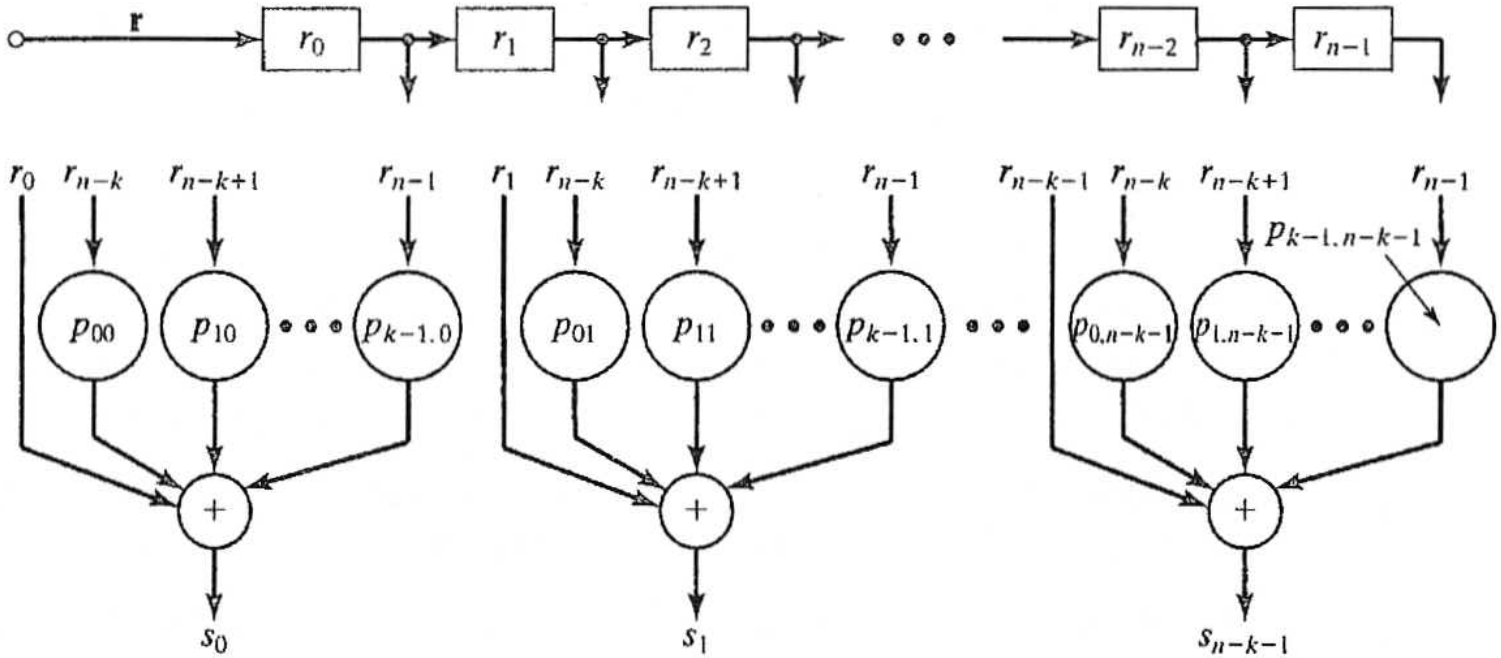
$$\boldsymbol{s} = \boldsymbol{r} \cdot \boldsymbol{H}^t = (\boldsymbol{v} + \boldsymbol{e}) \cdot \boldsymbol{H}^t = \boldsymbol{v} \cdot \boldsymbol{H}^t + \boldsymbol{e} \cdot \boldsymbol{H}^t = \boldsymbol{e} \cdot \boldsymbol{H}^t$$

Important things to remember:

- if $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{P}^t \end{pmatrix}$, then we just have $\boldsymbol{s} = \boldsymbol{r}_{\text{par}} + \boldsymbol{r}_{\text{inf}} \cdot \boldsymbol{P}$
- finding the error $\boldsymbol{e}$ from $\boldsymbol{s} = \boldsymbol{e} \cdot \boldsymbol{H}^t$ is not that simple
  - $\exists\, 2^k$ different solutions!
- the decoder tries to find the *most probable* error pattern in order to minimize the probability of decoding error
  - this usually leads to assuming a low–weight error pattern

Κύκλωμα Υπολογισμού Συνδρόμου (n, k) Κώδικα

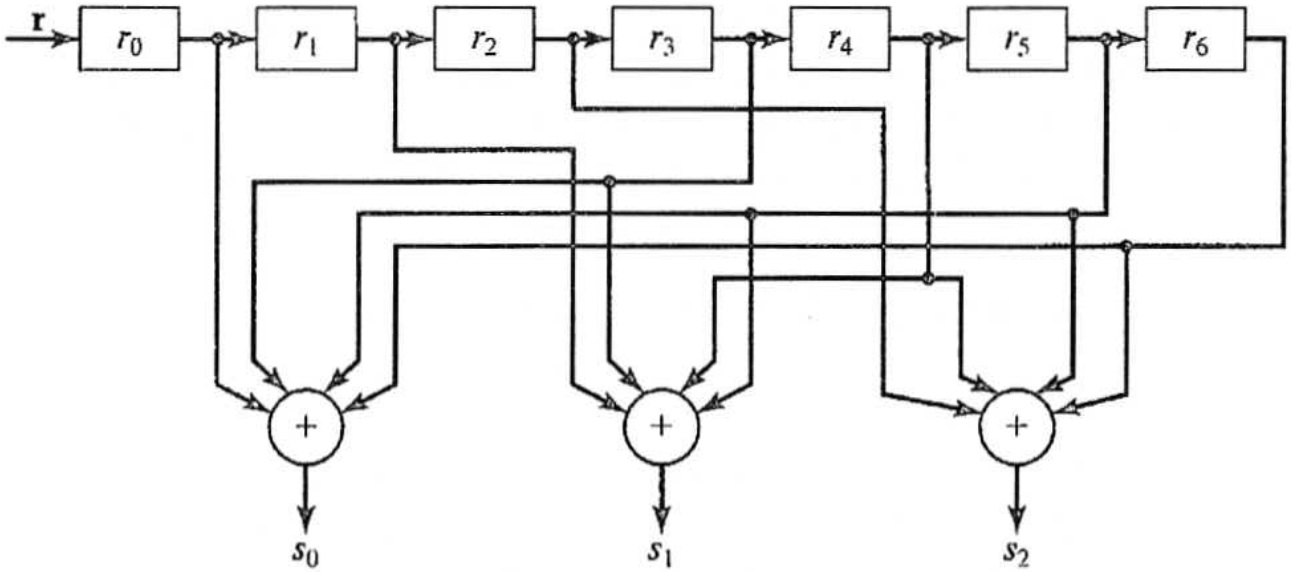
If $\mathscr{C}$ is a systematic (n, k) linear block code, then $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{P}^t \end{pmatrix}$ and its syndrome computation circuit is



due to the above analysis

Παράδειγμα $(7, 4)$ Κώδικα (*συν.*)

Let $\boldsymbol{v} = (1001011)$ and $\boldsymbol{r} = (1001001)$; then, the receiver computes $\boldsymbol{s} = \boldsymbol{r} \cdot \boldsymbol{H}^t = (111)$ via the circuit



If the channel is a BSC, $\boldsymbol{e} = (0000010)$ is the most probable error vector satisfying the preceding equations (has the smallest weight). So, we let $\boldsymbol{v}^\star = \boldsymbol{r} + \boldsymbol{e} = (1001011)$

Ελάχιστη Απόσταση Κώδικα

Notation

- the *Hamming weight* of vector $\boldsymbol{v} \in \mathbb{F}_2^n$ is defined as

$$\mathrm{wt}(\boldsymbol{v}) = \#\{0 \leq i < n : v_i \neq 0\}$$

- the *Hamming distance* of vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_2^n$ is

$$\begin{aligned} d(\boldsymbol{v}, \boldsymbol{w}) &= \#\{0 \leq i < n : v_i \neq w_i\} = \#\{0 \leq i < n : v_i + w_i \neq 0\} \\ &= \mathrm{wt}(\boldsymbol{v} + \boldsymbol{w}) \end{aligned}$$

Definition

The *minimum distance* of $\mathscr{C}$, denoted by $d_{\min}$, is defined as

$$d_{\min} = \min\{d(\boldsymbol{v}, \boldsymbol{w}) : \boldsymbol{v}, \boldsymbol{w} \in \mathscr{C} \text{ and } \boldsymbol{v} \neq \boldsymbol{w}\}$$

Ελάχιστη Απόσταση Κώδικα (*συν.*)

Theorem

If $\mathscr{C}$ is a linear block code, then $d_{min} = \min\{\mathrm{wt}(\boldsymbol{v}) : \boldsymbol{v} \in \mathscr{C} \text{ and } \boldsymbol{v} \neq \mathbf{0}\}$

Theorem

If $\mathscr{C}$ is a linear block code, and $\boldsymbol{v} \in \mathscr{C}$ is such that $\mathrm{wt}(\boldsymbol{v}) = l$, then there exist l columns of $\boldsymbol{H}$ the sum up to $\mathbf{0}$ (hint: $\boldsymbol{v} \cdot \boldsymbol{H}^t = \mathbf{0}\ \forall\ \boldsymbol{v} \in \mathscr{C}$)

Corollary

Let $\mathscr{C}$ be a linear block code with parity–check matrix $\boldsymbol{H}$

- *if no $d-1$ or fewer columns of $\boldsymbol{H}$ add to $\mathbf{0}$, the code has minimum weight at least d*
- *the minimum weight (or minimum distance) of $\mathscr{C}$ is equal to the smallest number of columns of $\mathscr{C}$ that sum to $\mathbf{0}$*

Κατανομή Βάρους Κωδικών Λέξεων

- Let $\mathscr{C}$ be an (n, k) linear code, and define the numbers

$$A_i = \#\{\boldsymbol{v} \in \mathscr{C} : \mathrm{wt}(\boldsymbol{v}) = i\}, \qquad 0 \leq i \leq n. \tag{6}$$

  Then $\{A_0, \ldots, A_n\}$ is called the *weight distribution* of $\mathscr{C}$.

- It may also be represented in polynomial form as follows

$$A(z) = A_0 + A_1 z + \cdots + A_n z^n = \sum_{i=0}^{n} A_i z^i.$$

  $A(z)$ is called the *weight enumerator* for the (n, k) linear code $\mathscr{C}$.

- The weight enumerator $B(z)$ of the dual $\mathscr{C}^{\perp}$ satisfies

$$A(z) = 2^{-(n-k)} (1+z)^n \, B\left(\frac{1-z}{1+z}\right) \tag{7}$$

  which is well–known as the *MacWilliams identity*.

Παράδειγμα $(7, 4)$ Κώδικα (*συν.*)

An $(7, 4)$ linear code $\mathscr{C}$ is given by

message $\boldsymbol{u}$	codeword $\boldsymbol{v}$	–
(0000)	(0000000)	
(1000)	(1101000)	$\star$
(0100)	(0110100)	$\star$
(1100)	(1011100)	
(0010)	(1110010)	$\star$
(1010)	(0011010)	
(0110)	(1000110)	
(1110)	(0101110)	
(0001)	(1010001)	$\star$
(1001)	(0111001)	
(0101)	(1100101)	
(1101)	(0001101)	
(0011)	(0100011)	
(1011)	(1001011)	
(0111)	(0010111)	
(1111)	(1111111)	

The weight distribution of $\mathscr{C}$ is

- $A_0 = 1$
- $A_1 = A_2 = 0$
- $A_3 = A_4 = 7$
- $A_5 = A_6 = 0$
- $A_7 = 1$

or equivalently

$$A(z) = 1 + 7z^3 + 7z^4 + z^7$$

as a polynomial

- $d_{\min} = 3$

Ανιχνευτική Ικανότητα Κώδικα

Any pair of codewords of an (n, k) block code $\mathscr{C}$ differs in *at least* $d_{\min}$ places. Therefore:

- error patterns $\boldsymbol{e}$ such that $\mathrm{wt}(\boldsymbol{e}) = l < d_{\min}$ cannot change $\boldsymbol{v}$ into another codeword $\boldsymbol{r}$
- these are called *detectable* error patterns ($\exists\ 2^n - 2^k$)

Property (error detection)

The *random–error detecting* capability of a block code with minimum distance $d_{\min}$ is $d_{\min} - 1$

Error patterns $\boldsymbol{e}$ that can be detected:

- all $\boldsymbol{e}$ with $\mathrm{wt}(\boldsymbol{e}) < d_{\min}$
- many $\boldsymbol{e}$ with $\mathrm{wt}(\boldsymbol{e}) \geq d_{\min}$

Διορθωτική Ικανότητα Κώδικα

Any pair of codewords of an (n, k) block code $\mathscr{C}$ differs in *at least* $d_{\min}$ places. Therefore:

- a received word satisfies $d(\boldsymbol{r}, \boldsymbol{v}) + d(\boldsymbol{r}, \boldsymbol{w}) \geq d(\boldsymbol{v}, \boldsymbol{w}) \geq d_{\min}$
- correct decoding is performed if $d(\boldsymbol{r}, \boldsymbol{v}) < d(\boldsymbol{r}, \boldsymbol{w}),\ \forall\, \boldsymbol{w} \in \mathscr{C}$ with $\boldsymbol{w} \neq \boldsymbol{v}$ (assuming $\boldsymbol{v}$ was transmitted)

Property (error correction)

The *random–error correcting* capability of a block code with minimum distance $d_{\min}$ is $t = \lfloor (d_{\min} - 1)/2 \rfloor$

Error patterns $\boldsymbol{e}$ that can be corrected:

- all $\boldsymbol{e}$ with $\mathrm{wt}(\boldsymbol{e}) \leq t$
- many $\boldsymbol{e}$ with $\mathrm{wt}(\boldsymbol{e}) > t$ (a total of 2^{n-k})

Πιθανότητα Μη–Ανιχνεύσιμου Σφάλματος

The probability of an *undetected error* $\Pr_u(E)$ occurs only when the error pattern $\boldsymbol{e}$ is identical to a codeword of $\mathscr{C}^\star = \mathscr{C} \setminus \{\mathbf{0}\}$; hence

$$\begin{aligned}\Pr_u(E) &= \Pr\left(\boldsymbol{e} \in \mathscr{C}^\star\right) = \sum_{\boldsymbol{v} \in \mathscr{C}^\star} \Pr\left(\boldsymbol{e} = \boldsymbol{v}\right) \\ &= \sum_{i=1}^{n} A_i p^i \left(1-p\right)^{n-i} = \left(1-p\right)^n \sum_{i=1}^{n} A_i \left(\frac{p}{1-p}\right)^i\end{aligned}$$

from which we conclude that

$$\Pr_u(E) = \left(1-p\right)^n \left[A\left(\frac{p}{1-p}\right) - 1\right] \tag{8}$$

where p is the transition probability of the BSC

Πιθανότητα Μη–Ανιχνεύσιμου Σφάλματος (*συν.*)

Proposition

It holds $\mathbb{E}_{\mathscr{C}}\left[\Pr_u(E)\right] \leq 2^{-(n-k)}\left[1-(1-p)^n\right]$

Proof

Let $\boldsymbol{\mathscr{C}}$ be the ensemble of all systematic (n,k) linear block codes; if the code $\mathscr{C} \in \boldsymbol{\mathscr{C}}$ is chosen uniformly at random, then

$$\mathbb{E}_{\mathscr{C}}\left[\Pr_u(E)\right] = \sum_{\mathscr{C}\in\boldsymbol{\mathscr{C}}} \Pr(\mathscr{C})\Pr_u(E|\mathscr{C}) = \sum_{i=1}^{n} p^i(1-p)^{n-i} \cdot \frac{1}{|\boldsymbol{\mathscr{C}}|}\sum_{\mathscr{C}\in\boldsymbol{\mathscr{C}}} A_i^{\mathscr{C}}$$

$$\leq 2^{-(n-k)}\sum_{i=1}^{n}\binom{n}{i}p^i(1-p)^{n-i}$$

which concludes our proof ■

Since $\left[1-(1-p)^n\right] \leq 1$, we also have $\mathbb{E}_{\mathscr{C}}\left[\Pr_u(E)\right] \leq 2^{-(n-k)}$

Μέθοδος Αποκωδικοποίησης

Definition (decoding)

A *decoding scheme* is a rule to partition the 2^n possible received vectors $\boldsymbol{r}$ into 2^k disjoint subsets $D_1, \ldots, D_{2^k}$, so that

$$\text{if} \quad \boldsymbol{r} \in D_i \quad \Rightarrow \quad \boldsymbol{r} \mapsto \boldsymbol{v}_i$$

where $\boldsymbol{v}_i \in \mathscr{C}$ is the only one codeword contained in the subset D_i, for $1 \leq i \leq 2^k$

Solution (standard array: $D_i = \boldsymbol{v}_i + D_1$)

$$\begin{array}{cccc} \boldsymbol{e}_1 = \mathbf{0} = \boldsymbol{v}_1 & \boldsymbol{v}_2 & \cdots & \boldsymbol{v}_{2^k} \\ \boldsymbol{e}_2 & \boldsymbol{e}_2 + \boldsymbol{v}_2 & \cdots & \boldsymbol{e}_2 + \boldsymbol{v}_{2^k} \\ \vdots & \vdots & & \vdots \\ \boldsymbol{e}_{2^{n-k}} & \boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_2 & \cdots & \boldsymbol{e}_{2^{n-k}} + \boldsymbol{v}_{2^k} \end{array}$$

Μέθοδος Αποκωδικοποίησης (*συν.*)

The decoding based on the *standard array* is the minimum distance decoding (i.e., the maximum likelihood decoding)

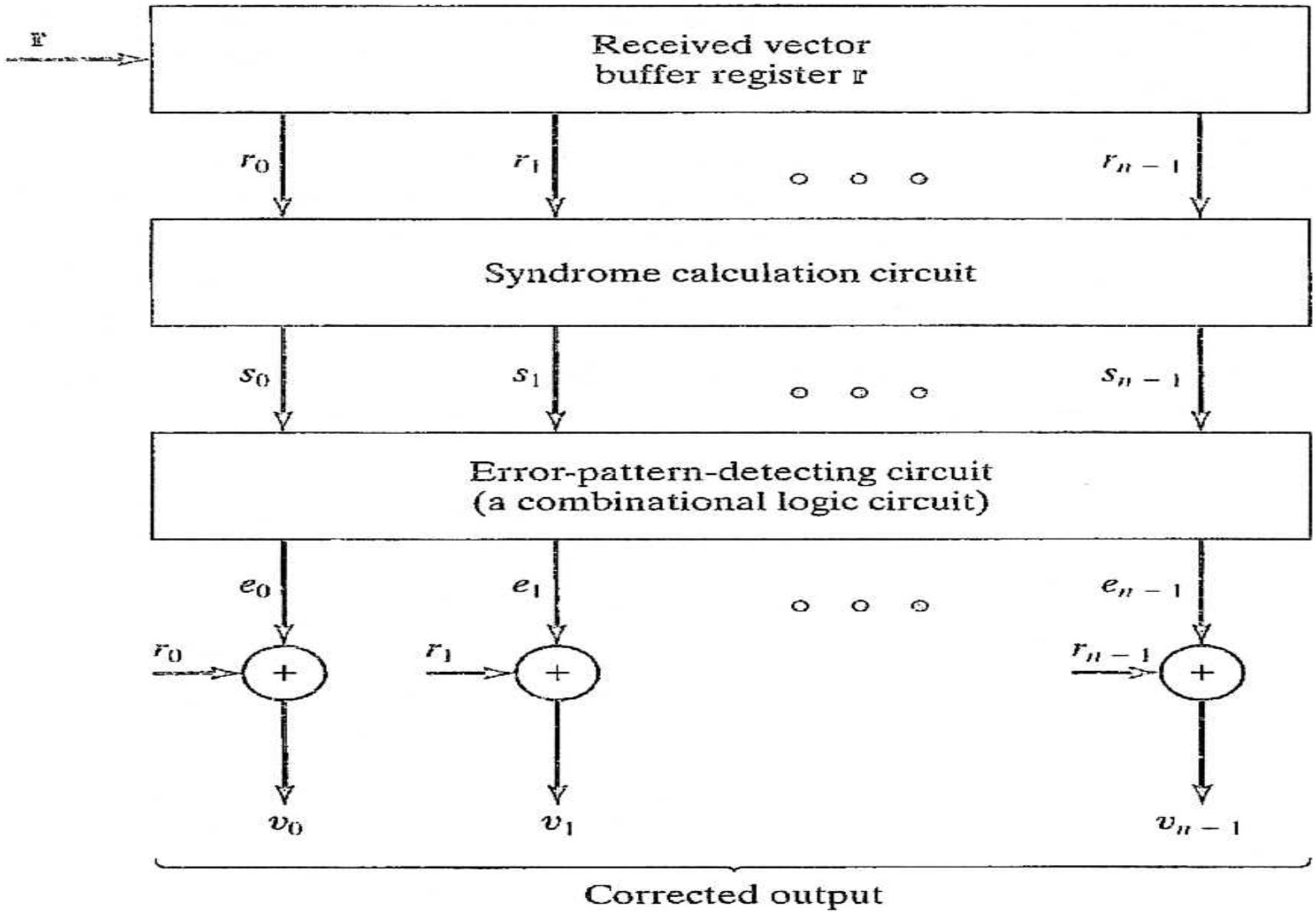
Theorem

All the 2^k n–tuples of a coset have the same syndrome; the syndromes for different cosets are different

Algorithm (syndrome decoding or table lookup decoding)

- compute the syndrome $\boldsymbol{r} \cdot \boldsymbol{H}^t$ of $\boldsymbol{r}$
- locate the coset leader $\boldsymbol{e}_l$ whose syndrome is equal to $\boldsymbol{r} \cdot \boldsymbol{H}^t$
  - then $\boldsymbol{e}_l$ is assumed to be the error pattern caused by the channel
- decode the received vector $\boldsymbol{r}$ into the codeword $\boldsymbol{v}^\star = \boldsymbol{r} + \boldsymbol{e}_l$

Κύκλωμα Αποκωδικοποίησης (n, k) Κώδικα



Παράδειγμα $(7, 4)$ Κώδικα (*συν.*)

The systematic $(7, 4)$ linear block code $\mathscr{C}$ of our example has the following standard array ($2^3 \times 2^4$):

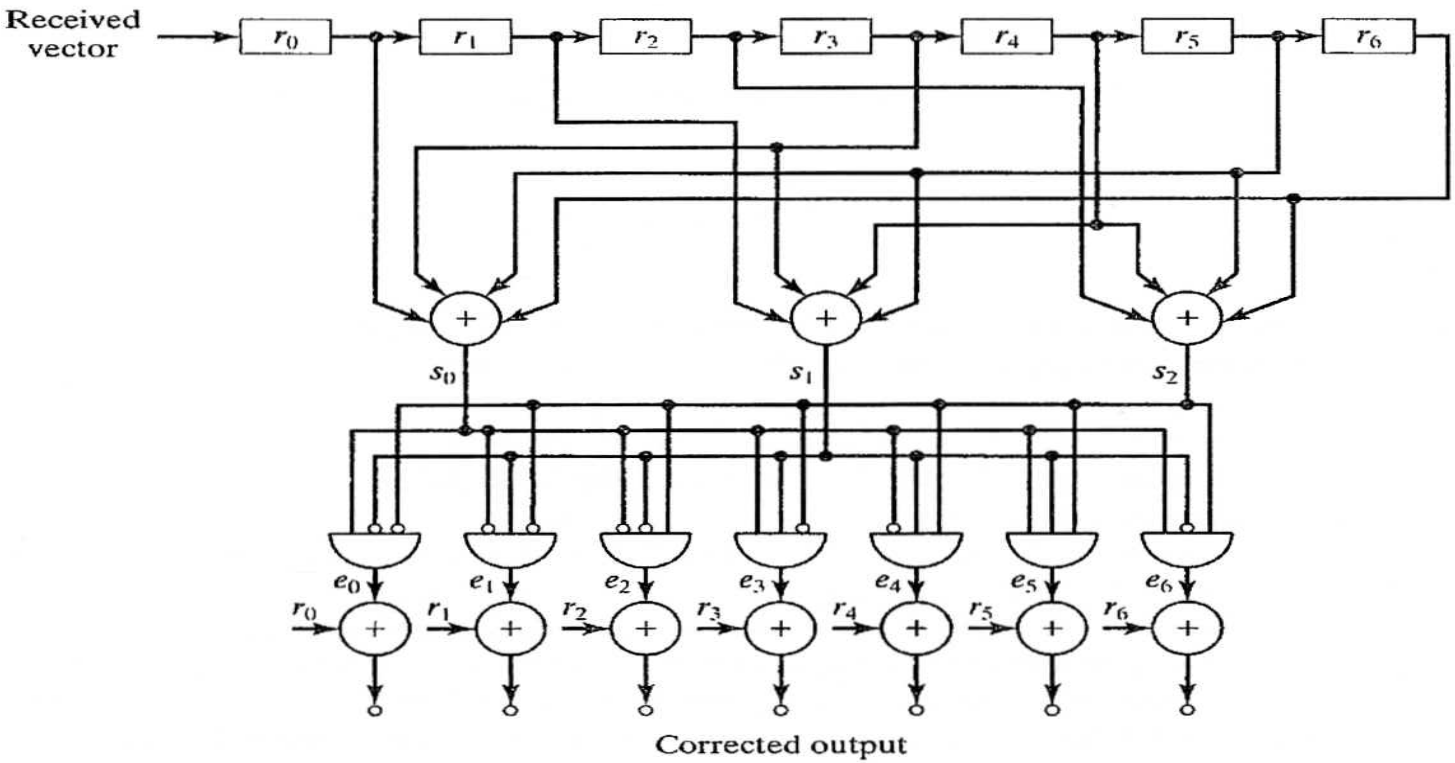
$\boldsymbol{e}$	$\boldsymbol{v}_0$	$\boldsymbol{v}_1$	$\cdots$	$\boldsymbol{v}_{14}$	$\boldsymbol{v}_{15}$	$\boldsymbol{s}$
(0000000)	(0000000)	(1101000)	$\cdots$	(0010111)	(1111111)	(000)
(1000000)	(1000000)	(0101000)	$\cdots$	(1010111)	(0111111)	(100)
(0100000)	(0100000)	(1001000)	$\cdots$	(0110111)	(1011111)	(010)
(0010000)	(0010000)	(1111000)	$\cdots$	(0000111)	(1101111)	(001)
(0001000)	(0001000)	(1100000)	$\cdots$	(0011111)	(1110111)	(110)
(0000100)	(0000100)	(1101100)	$\cdots$	(0010011)	(1111011)	(011)
(0000010)	(0000010)	(1101010)	$\cdots$	(0010101)	(1111101)	(111)
(0000001)	(0000001)	(1101001)	$\cdots$	(0010110)	(1111110)	(101)

The number of correctable errors (due to $d_{\min} = 3$) equals the total number of correctable errors (given by 2^{n-k}):

- $\binom{7}{0} + \binom{7}{1} = 8$
- $2^{7-4} = 8$

Παράδειγμα $(7, 4)$ Κώδικα (*συν.*)

The decoding circuit for the systematic $(7, 4)$ linear block code $\mathscr{C}$ will be



$e_0 = s_0\bar{s}_1\bar{s}_2, e_1 = \bar{s}_0 s_1\bar{s}_2, e_2 = \bar{s}_0\bar{s}_1 s_2, e_3 = s_0 s_1\bar{s}_2, e_4 = \bar{s}_0 s_1 s_2, e_5 = s_0 s_1 s_2,$
$e_6 = s_0\bar{s}_1 s_2.$

Πιθανότητα Λανθασμένης Αποκωδικοποίησης

For any t–error–correcting block code $\mathscr{C}$, the probability $\Pr(E)$ that the decoder commits an *erroneous decoding* is upper bounded by

$$\Pr(E) \leq \Pr\big(\mathrm{wt}(\boldsymbol{e}) > t\big) = \sum_{i=t+1}^{n} \Pr\big(\mathrm{wt}(\boldsymbol{e}) = i\big)$$

$$= \sum_{i=t+1}^{n} \binom{n}{i} p^i \big(1-p\big)^{n-i}. \tag{9}$$

An alternative formula is derived if the weights of the coset leaders are known; indeed, if $\{a_0, \ldots, a_n\}$ is the weight distribution, then

$$\Pr(E) = 1 - \sum_{i=0}^{n} a_i p^i \big(1-p\big)^{n-i} \tag{10}$$

where p is the transition probability of the BSC

Κώδικες Απλής Ισοτιμίας

Definition

A *single–parity–check* (SPC) code $\mathscr{C}$ is an $(n, n-1)$ linear block code with one parity–check digit

Property

- generator matrix $\boldsymbol{G} = \begin{pmatrix} \mathbf{1}_{n-1}^t & \boldsymbol{I}_{n-1} \end{pmatrix}$
- parity–check matrix $\boldsymbol{H} = \begin{pmatrix} 1 & \mathbf{1}_{n-1} \end{pmatrix}$
- minimum distance $d_{\min} = 2$ (all codewords have even weight)
- rate $R = 1 - 1/n$

Can only be used for simple error detection; errors of even weight are not detectable

Κώδικες Επανάληψης

Definition

A *repetition* code $\mathscr{C}$ of length n is an $(n, 1)$ linear block code with two codewords: $\mathbf{0}_n$ and $\mathbf{1}_n$

Property

- generator matrix $\boldsymbol{G} = \begin{pmatrix} \mathbf{1}_{n-1} & 1 \end{pmatrix}$
- parity–check matrix $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{n-1} & \mathbf{1}_{n-1}^t \end{pmatrix}$
- minimum distance $d_{\min} = n$ (usually choose n odd)
- rate $R = 1/n$

It is the dual of the $(n, n-1)$ SPC code

Αυτο–Δυϊκοί Κώδικες

Definition

An (n, k) linear block code $\mathscr{C}$ is *self–dual* if and only if $\mathscr{C}^{\perp} = \mathscr{C}$

Property

- generator matrix $\boldsymbol{G} = \begin{pmatrix} \boldsymbol{P} & \boldsymbol{I}_{n/2} \end{pmatrix}$
- parity–check matrix $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_{n/2} & \boldsymbol{P}^t \end{pmatrix}$
- we have $\boldsymbol{G} \cdot \boldsymbol{G}^t = 0$, and for systematic codes $\boldsymbol{P} \cdot \boldsymbol{P}^t = \boldsymbol{I}_{n/2}$
- rate $R = 1/2$

n must be even, since $k = n - k \Rightarrow k = n/2$

Προτεινόμενη Βιβλιογραφία

T. M. Cover and J. A. Thomas
Elements of Information Theory
John Wiley & Sons, 2006

R. Gallager
Information Theory and Reliable Communication
John Wiley & Sons, 1968

S. Lin and D. Costello
Error Control Coding, 2nd ed.
Prentice–Hall, 2004