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 3^{η} : *σχεδιασμός απλών τμηματικών κωδίκων*

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

Περιεχόμενα Ομιλίας

1. Περιεχόμενα της ομιλίας
2. Οικογένειες γραμμικών τμηματικών κωδίκων
   - Κώδικες Hamming
   - Κώδικες LDPC
3. Σύνοψη & βιβλιογραφία

Ορισμός Κωδίκων Hamming

Definition (Hamming Codes)

For any positive integer $m \geq 3$ there exists an (n, k) code $\mathscr{C}$ with the following parameters

- code length $n = 2^m - 1$;
- number of information symbols $k = 2^m - m - 1$;
- number of parity–check symbols $m = n - k$; and
- error correcting capability $t = 1$ $(d_{\min} = 3)$.

Such a code is called a *Hamming code*

Ορισμός Κωδίκων Hamming (*συν.*)

Property

Hamming codes have the following properties:

- the parity–check matrix $\boldsymbol{H}$ consists of all the nonzero m–tuples as its columns
- in systematic form $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{I}_m & \boldsymbol{P}^t \end{pmatrix}$ and the rows of $\boldsymbol{P}$ are the nonzero m–tuples of weight ≥ 2
- in systematic form $\boldsymbol{G} = \begin{pmatrix} \boldsymbol{P} & \boldsymbol{I}_{2^m-m-1} \end{pmatrix}$

The minimum distance of $\mathscr{C}$ equals 3 since, for any columns $\boldsymbol{h}_i, \boldsymbol{h}_j$ of $\boldsymbol{H}$, we have

$$\exists\, \boldsymbol{h}_k : \ \boldsymbol{h}_k = \boldsymbol{h}_i + \boldsymbol{h}_j \quad \Rightarrow \quad \boldsymbol{h}_i + \boldsymbol{h}_j + \boldsymbol{h}_k = 0$$

(hint: $\boldsymbol{v} \cdot \boldsymbol{H}^t = 0$)

Παράδειγμα $(7,4)$ Κώδικα (συν.)

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

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

This is a Hamming code with parameters

- code length $n = 7$ $(2^3 - 1)$
- number of information symbols $k = 4$ $(2^3 - 3 - 1)$
- number of parity–check symbols $m = 3$ $(7 - 4)$

Ιδιότητες Κωδίκων Hamming

Definition (Perfect Codes)

An (n, k) t–error–correcting code $\mathscr{C}$ is called a *perfect code* if its standard array has all error patterns of weight $\leq t$ as coset leaders, and no others

Proposition

Hamming codes are perfect single–error–correcting codes

Proof

There exist 2^{2^m-1} possible words, 2^{2^m-m-1} codewords, and 2^m error patterns of weight ≤ 1 (and length $2^m - 1$) ∎

Ιδιότητες Κωδίκων Hamming (*συν.*)

Definition (Shortened Hamming Codes)

Any code obtained from an $(2^m - 1, 2^m - m - 1)$ Hamming code $\mathscr{C}$ by deleting l columns from $\boldsymbol{H}$ is called a *shortened Hamming code*

Such codes have the following parameters

- code length $n = 2^m - l - 1$;
- number of information symbols $k = 2^m - m - l - 1$;
- number of parity–check symbols $m = n - k$; and
- error correcting capability $d_{\min} \geq 3$.

Note: rate is decreased

Ιδιότητες Κωδίκων Hamming (*συν.*)

Example

Suppose we delete from $\boldsymbol{P}^t$ in $\boldsymbol{H}$ all even–weight columns; then we obtain a code of length 2^{m-1}, and

- all columns in $\boldsymbol{H}$ have odd weight;
- no three columns add to zero; and
- minimum distance equals $d_{\min} = 4$.

Definition (Dual Hamming Codes)

The dual of an $(2^m - 1, 2^m - m - 1)$ Hamming code $\mathscr{C}$ is an $(2^m - 1, m)$ linear block code

- its codewords are the $2^m - 1$ vectors of weight 2^{m-1}, plus the all–zero vector

Ιδιότητες Κωδίκων Hamming (*συν.*)

The weight enumerators $A(z), B(z)$ of a Hamming code and its dual are given by

$$A(z) = 2^{-m}(1+z)^{-1}\left[(1+z)^{2^m} + (2^m - 1)(1-z^2)^{2^{m-1}}\right] \qquad (1)$$

$$B(z) = 1 + (2^m - 1)z^{2^{m-1}} \qquad (2)$$

So, it is easier to compute the probability $\Pr_u(E)$ using (2)

The Hamming codes can be decoded by using the techniques mentioned so far

Γενικά Περί LDPC Κωδίκων

- Low–density parity–check (LDPC) codes are an important class of Shannon limit (or *channel capacity*)–approaching codes
- They were discovered by Gallager in the early 60's but ignored; it was Tanner's work that played a key role
  - graphical interpretation of LDPC codes
- Gallager did not provide a method to allow for algebraic and systematic construction of LDPC codes
  - they are specified in terms of their parity–check matrices
  - constructions based on finite geometries are now used
- Compared to turbo codes, LDPC codes
  - do not require a long interleaver to achieve good performance
  - have better *block error performance*
  - have a much simpler decoding (as it is not Trellis based)

Ορισμός LDPC Κωδίκων

Definition (LDPC Code)

An LDPC code $\mathscr{C}$ is defined as the null space of a parity–check matrix $\boldsymbol{H}$ that has the following structural properties:

1. each row and column of $\boldsymbol{H}$ consists of ρ and γ 1's respectively;
2. the number λ of 1's in common between two columns of $\boldsymbol{H}$, satisfies $\lambda \leq 1$; and
3. both ρ, γ are small compared to the length n of the code and the number of rows in $\boldsymbol{H}$

Such an LDPC code is called (γ, ρ)–*regular* LDPC code; otherwise, it is called *irregular*.

Ορισμός LDPC Κωδίκων (*συν.*)

Definition (Density of LDPC Code)

The density r of an LDPC code $\mathscr{C}$ is defined as the number of 1's in $\boldsymbol{H}$ over the total number of its entries:

$$r = \frac{\rho}{n} \qquad \Leftrightarrow \qquad r = \frac{\gamma}{J} \tag{3}$$

where J is the number of rows in $\boldsymbol{H}$ (hint: $\exists\ \rho J = \gamma n$ 1's in $\boldsymbol{H}$)

Note

- Property 2 also implies that no two rows of $\boldsymbol{H}$ have more than one 1 in common
- The rows of $\boldsymbol{H}$ need not be LI; if they are LI, then $J = n - k$
  - in general, we need to find rank$(\boldsymbol{H})$

Παράδειγμα LDPC Κώδικα

The parity–check matrix of an $(15, 7)$ LDPC code is shown next, with density 0.267

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

This is a $(4, 4)$–regular LDPC code

Κατασκευή LDPC Κώδικα

Construction (Gallager)

1. Choose positive integer $k > 1$, and parameters ρ, γ
2. Construct a $k\gamma \times k\rho$ parity–check matrix $\boldsymbol{H}$ as follows

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{H}_1 \\ \vdots \\ \boldsymbol{H}_\gamma \end{pmatrix} = \begin{pmatrix} \boldsymbol{H}_{11} & \cdots & \boldsymbol{H}_{1k} \\ \vdots & & \vdots \\ \boldsymbol{H}_{\gamma 1} & \cdots & \boldsymbol{H}_{\gamma k} \end{pmatrix} \tag{4}$$

   and each block $\boldsymbol{H}_i$, $i = 1, \ldots, \gamma$, has size $k \times k\rho$
   whereas block $\boldsymbol{H}_{ij}$, $j = 1, \ldots, k$, has size $k \times \rho$
3. Fix the ρ 1's of the jth row of $\boldsymbol{H}_1$ to be in the jth row of $\boldsymbol{H}_{1j}$

$$\boldsymbol{H}_{1j} = \begin{pmatrix} \cdots \\ \boldsymbol{1}_\rho \\ \cdots \end{pmatrix} \leftarrow j\text{th row} \tag{5}$$

Κατασκευή LDPC Κώδικα (συν.)

4. Obtain the other submatrices $\boldsymbol{H}_2, \ldots, \boldsymbol{H}_\gamma$ from $\boldsymbol{H}_i$ by appropriate column permutations
5. The parity–check matrix $\boldsymbol{H}$ has $k\rho\gamma$ 1's and a total of $k^2\rho\gamma$ entries; therefore its density is

$$r = \frac{1}{k}$$

Note

- We can make the density arbitrarily low by choosing large k
- The problem with this construction is that no systematic way is proposed for choosing the column permutations for $\boldsymbol{H}_2, \ldots, \boldsymbol{H}_\gamma$

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