CHAPTER 2: Linear codes

ABSTRACT

Most of the important codes are special types of so-called linear codes.

Linear codes are of importance because they have

very concise description,

very nice properties,

very easy encoding

And,

in principle, quite easy decoding.

Linear codes

Linear codes are special sets of words of the length n over an alphabet $\{0,..,q-1\}$, where q is a power of prime.

Since now on sets of words F_q^n will be considered as vector spaces $V(n,q)$ of vectors of length n with elements from the set $\{0,..,q-1\}$ and arithmetical operations will be taken modulo q.

The set $\{0,..,q-1\}$ with operations + and $\bullet$ modulo q is called also the Galois field $GF(q)$.

Definition A subset $C \subseteq V(n,q)$ is a linear code if

(1) $u + v \in C$ for all $u, v \in C$

(2) $au \in C$ for all $u \in C$, $a \in GF(q)$

Example Codes C_1, C_2, C_3 introduced in Lecture 1 are linear codes.

Lemma A subset $C \subseteq V(n,q)$ is a linear code if one of the following conditions is satisfied

(1) C is a subspace of $V(n,q)$

(2) sum of any two codewords from C is in C (for the case $q = 2$)

If C is a k-dimensional subspace of $V(n,q)$, then C is called [n,k] -code. It has q^k codewords. If minimal distance of C is d, then it is called [n,k,d] code.

Linear codes are also called "group codes".

Exercise

Which of the following binary codes are linear?

$C_1 = \{00, 01, 10, 11\}$
$C_2 = \{000, 011, 101, 110\}$
$C_3 = \{00000, 01101, 10110, 11011\}$
$C_5 = \{101, 111, 011\}$
$C_6 = \{000, 001, 010, 011\}$
$C_7 = \{0000, 1001, 0110, 1110\}$

How to create a linear code

Notation If S is a set of vectors of a vector space, then let $\langle S \rangle$ be the set of all linear combinations of vectors from S.

Theorem For any subset S of a linear space, $\langle S \rangle$ is a linear space that consists of the following words:

- the zero word,
- all words in S,
- all sums of two or more words in S.

Example $S = \{0100, 0011, 1100\}$

$$\langle S \rangle = \{0000, 0100, 0011, 1100, 0111, 1011, 1000, 1111\}.$$

Basic properties of linear codes

Notation: $w(x)$ (weight of x) is the number of non-zero entries of x.

Lemma If $x, y \in V(n,q)$, then $h(x,y) = w(x - y)$.

Proof $x - y$ has non-zero entries in exactly those positions where x and y differ.

Theorem Let C be a linear code and let weight of C, notation $w(C)$, be the smallest of the weights of non-zero codewords of C. Then $h(C) = w(C)$.

Proof There are $x, y \in C$ such that $h(C) = h(x,y)$. Hence $h(C) = w(x - y) \geq w(C)$.

On the other hand for some $x \in C$

$$w(C) = w(x) = h(x,0) \geq h(C).$$

Consequence

- If C is a code with m codewords, then in order to determine $h(C)$ one has to make $\binom{m}{2} = \theta(m^2)$ comparisons.
- If C is a linear code, then in order to compute $h(C)$, $m - 1$ comparisons are enough.

Basic properties of linear codes

If C is a linear $[n,k]$ -code, then it has a basis consisting of k codewords.

Example

Code

$$C_4 = \{0000000, 1111111, 1000101, 1100010, 0110001, 1011000, 0101100, 0010110, 0001011, 0111010, 0011101, 1001110, 0100111, 1010011, 1101001, 1110100\}$$

has the basis

$$\{1111111, 1000101, 1100010, 0110001\}.$$

How many different bases has a linear code?

Theorem A binary linear code of dimension k has

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$$

bases.

Advantages and disadvantages of linear codes I.

Advantages - big.

1. Minimal distance $h(C)$ is easy to compute if C is a linear code.
2. Linear codes have simple specifications.

- To specify a non-linear code usually all codewords have to be listed.
- To specify a linear $[n,k]$ -code it is enough to list k codewords.

Definition A $k \times n$ matrix whose rows form a basis of a linear $[n,k]$ -code (subspace) C is said to be the generator matrix of C.

Example The generator matrix of the code

$$C_2 = \begin{Bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{Bmatrix} \quad \text{is} \quad \begin{Bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{Bmatrix}$$

and of the code

$$C_4 \quad \text{is} \quad \begin{Bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{Bmatrix}$$

3. There are simple encoding/decoding procedures for linear codes.

Advantages and disadvantages of linear codes II.

Disadvantages of linear codes are small:

1. Linear q -codes are not defined unless q is a prime power.

2. The restriction to linear codes might be a restriction to weaker codes than sometimes desired.

Equivalence of linear codes

Definition Two linear codes $GF(q)$ are called equivalent if one can be obtained from another by the following operations:

(a) permutation of the positions of the code;

(b) multiplication of symbols appearing in a fixed position by a non-zero scalar.

Theorem Two $k \times n$ matrices generate equivalent linear $[n,k]$ -codes over $GF(q)$ if one matrix can be obtained from the other by a sequence of the following operations:

(a) permutation of the rows

(b) multiplication of a row by a non-zero scalar

(c) addition of one row to another

(d) permutation of columns

(e) multiplication of a column by a non-zero scalar

Proof Operations (a) - (c) just replace one basis by another. Last two operations convert a generator matrix to one of an equivalent code.

Equivalence of linear codes

Theorem Let G be a generator matrix of an $[n,k]$ -code. Rows of G are then linearly independent .By operations (a) - (e) the matrix G can be transformed into the form: $[\ I_k \mid A\ ]$ where I_k is the $k \times k$ identity matrix, and A is a $k \times (n - k)$ matrix.

Example

$$\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{matrix} \rightarrow \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{matrix} \rightarrow$$

$$\begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{matrix} \rightarrow \begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{matrix} \rightarrow ?$$

Encoding with a linear code

is a vector $\times$ matrix multiplication

Let C be a linear $[n,k]$ -code over $GF(q)$ with a generator matrix G.

Theorem C has q^k codewords.

Proof Theorem follows from the fact that each codeword of C can be expressed uniquely as a linear combination of the basis vectors.

Corollary The code C can be used to encode uniquely q^k messages.
Let us identify messages with elements $V(k,q)$.

Encoding of a message $u = (u_1, \dots ,u_k)$ with the code C:

$$u \cdot G = \sum_{i=1}^{k} u_i r_i \text{ where } r_1,\dots,r_k \text{ are rows of } G.$$

Example Let C be a [7,4] -code with the generator matrix

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

A message (u_1, u_2, u_3, u_4) is encoded as:???

For example:

0 0 0 0 is encoded as .... ?

1 0 0 0 is encoded as .... ?

1 1 1 0 is encoded as .... ?

Uniqueness of encodings

with linear codes

Theorem If $G=\{w_i\}_{i=1}^{k}$ is a generator matrix of a binary linear code C of length n and dimension k, then

$$v = uG$$

ranges over all 2^k codewords of C as u ranges over all 2^k words of length k.

Therefore

$$C = \{\, uG \mid u \in \{0,1\}^k \,\}$$

Moreover

$$u_1 G = u_2 G$$

if and only if

$$u_1 = u_2.$$

Proof If

$$0 = \sum_{i=1}^{k} u_{1,i} w_i - \sum_{i=1}^{k} u_{2,i} w_i = \sum_{i=1}^{k} (u_{1,i} - u_{2,i}) w_i$$

then, since w_i are linearly independent, $u_1 = u_2$.

Decoding of linear codes

Decoding problem: If a codeword: $x = x_1 \dots x_n$ is sent and the word $y = y_1 \dots y_n$ is received, then $e = y - x = e_1 \dots e_n$ is said to be the error vector. The decoder must decide, from y, which x was sent, or, equivalently, which error e occurred.

To describe main Decoding method some technicalities have to be introduced

Definition Suppose C is an $[n,q]$ -code over $GF(q)$ and $a \in V(n,q)$. Then the set

$$a + C = \{ a + x \mid x \in C \}$$

is called a coset of C in V(n,q).

Example Let C = {0000, 1011, 0101, 1110}

Cosets:

$$0000 + C = C,$$
$$1000 + C = \{1000, 0011, 1101, 0110\},$$
$$0100 + C = \{0100, 1111, 0001, 1010\},$$
$$0010 + C = \{0010, 1001, 0111, 1100\}.$$

Are there some other cosets in this case?

Theorem Suppose C is a linear $[n,k]$ -code over $GF(q)$. Then

(a) every vector of $V(n,k)$ is in some coset of C,

(b) every coset contains exactly q^k elements,

(c) two cosets are either disjoint or identical.

Nearest neighbour decoding scheme:

Each vector having minimum weight in a coset is called a coset leader.

1. Design a (Slepian) standard array for an [n,k] -code C - that is a $q^{n-k} \times q^k$ array of the form:

codewords	coset leader	codeword 2	…	codeword 2^k
	coset leader	+	…	+
	..	+	+	+
	coset leader	+	…	+
	coset leader			

Example

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

A word y is decoded as codeword of the first row of the column in which y occurs.

Error vectors which will be corrected are precisely coset leaders!

In practice, this decoding method is too slow and requires too much memory.

Probability of good error correction

What is the probability that a received word will be decoded as the codeword sent (for binary linear codes and binary symmetric channel)?

Probability of an error in the case of a given error vector of weight i is

$$p^{i}(1-p)^{n-i}.$$

Therefore, it holds.

Theorem Let C be a binary $[n,k]$ -code, and for $i = 0,1, \ldots, n$ let α_i be the number of coset leaders of weight i. The probability $P_{corr}(C)$ that a received vector when decoded by means of a standard array is the codeword which was sent is given by

$$P_{corr}(C) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}.$$

Example For the [4,2] -code of the last example

$$\alpha_0 = 1,\ \alpha_1 = 3,\ \alpha_2 = \alpha_3 = \alpha_4 = 0.$$

Hence

$$P_{corr}(C) = (1-p)^4 + 3p(1-p)^3 = (1-p)^3(1+2p).$$

If $p = 0.01$, then $P_{corr} = 0.9897$

Probability of good error detection

Suppose a binary linear code is used only for error detection.

The decoder will fail to detect errors which have occurred if the received word *y* is a codeword different from the codeword *x* which was sent, i. e. if the error vector $e = y - x$ is itself a non-zero codeword.

The probability $P_{undetect}(C)$ that an incorrect codeword is received is given by the following result.

Theorem Let *C* be a binary [*n*,*k*] -code and let A_i denote the number of codewords of *C* of weight *i*. Then, if *C* is used for error detection, the probability of an incorrect message being received is

$$P_{undetect}(C) = \sum_{i=0}^{n} A_i p^i (1-p)^{n-i}.$$

Example In the case of the [4,2] code from the last example

$$A_2 = 1 \quad A_3 = 2$$

$$P_{undetect}(C) = p^2(1-p)^2 + 2p^3(1-p) = p^2 - p^4.$$

For $p = 0.01$

$$P_{undetect}(C) = 0.000099.$$

Dual codes

Inner product of two vectors (words)

$$u = u_1 \ldots u_n, \quad v = v_1 \ldots v_n$$

in $V(n,q)$ is an element of $GF(q)$ defined by

$$u \cdot v = u_1 v_1 + \ldots + u_n v_n.$$

Example In $V(4,2)$: $1001 \cdot 1001 = 0$

In $V(4,3)$: $2001 \cdot 1210 = 2$

$1212 \cdot 2121 = 2$

If $u \cdot v = 0$ then words (vectors) u and v are called orthogonal.

Properties If $u, v, w \in V(n,q)$, $\lambda, \mu \in GF(q)$, then

$$u \cdot v = v \cdot u, \quad (\lambda u + \mu v) \cdot w = \lambda (u \cdot w) + \mu (v \cdot w).$$

Given a linear $[n,k]$ -code C, then dual code of C, denoted by $C^\perp$, is defined by

$$C^\perp = \{v \in V(n,q) \mid v \cdot u = 0 \text{ if } u \in C\}.$$

Lemma Suppose C is an $[n,k]$ -code having a generator matrix G. Then for $v \in V(n,q)$

$$v \in C^\perp \iff vG^T = 0,$$

where G^T denotes the transpose of the matrix G.

Proof Easy.

IV054 PARITE CHECKS versus ORTHOGONALITY

For understanding of the role the parity checks play for linear codes, it is important to understand relation between orthogonality and parity checks.

If words *x* and *y* are orthogonal, then the word y has even number of ones in the positions determined by ones in the word *x*.

This implies that if words *x* and *y* are orthogonal, then *x* is a parity check word for *y* and *y* is a parity check word for *x*.

Exercise: Let the word

100001

be orthogonal to a set *S* of binary words of length *6*. What can we say about words in *S*?

EXAMPLE

For the $[n,1]$ -repetition code C, with the generator matrix

$$G = (1,1, \dots ,1)$$

the dual code $C^{\perp}$ is $[n,n - 1]$ -code with the generator matrix $G^{\perp}$, described by

$$G^{\perp} = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ & .. & & & & \\ 1 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Parity check matrices

Example If

$$C_5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \text{ then } C_5^{\perp} = C_5.$$

If

$$C_6 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \text{ then } C_6^{\perp} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Theorem Suppose C is a linear $[n,k]$ -code over $GF(q)$, then the dual code $C^{\perp}$ is a linear $[n,n-k]$ -code.

Definition A parity-check matrix H for an $[n,k]$ -code C is a generator matrix of $C^{\perp}$.

Parity check matrices

Definition A parity-check matrix H for an [n,k] -code C is a generator matrix of $C^{\perp}$.

Theorem If H is parity-check matrix of C, then

$$C = \{x \in V(n,q) \mid xH^{T} = 0\},$$

and therefore any linear code is completely specified by a parity-check matrix.

Example Parity-check matrix for

$$C_5 \text{ is } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

and for

$$C_6 \text{ is } \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

The rows of a parity check matrix are parity checks on codewords. They say that certain linear combinations of the coordinates of every codeword are zeros.

Syndrome decoding

Theorem If $G = [I_k \mid A]$ is the standard form generator matrix of an $[n,k]$ -code C, then a parity check matrix for C is $H = [-A^T \mid I_{n-k}]$.

Example

$$\text{Generator matrix } G = \left|\, I_4 \left| \begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix} \right| \right. \Rightarrow \text{parity check m. } H = \left| \begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{matrix} \right| I_3 \,\Big|$$

Definition Suppose H is a parity-check matrix of an $[n,k]$ -code C. Then for any $y \in V(n,q)$ the following word is called the syndrome of y:

$$S(y) = yH^T.$$

Lemma Two words have the same syndrom iff they are in the same coset.

Syndrom decoding Assume that a standard array of a code C is given and, in addition, let in the last two columns the syndrom for each coset be given.

$$\begin{array}{cccc|cccc|cccc|cccc|cc}
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0
\end{array}$$

When a word y is received, compute $S(y) = yH^T$, locate $S(y)$ in the “syndrom column”, and then locate y in the same row and decode y as the codeword in the same column and in the first row.

KEY OBSERVATION for SYNDROM COMPUTATION

When preparing a "syndrome decoding" it is sufficient to store only two columns: one for coset leaders and one for syndromes.

Example

coset leaders	syndromes
l(z)	z
0000	00
1000	11
0100	01
0010	10

Decoding procedure

- **Step 1** Given y compute $S(y)$.
- **Step 2** Locate $z = S(y)$ in the syndrome column.
- **Step 3** Decode y as y - l(z).

Example If $y = 1111$, then $S(y) = 01$ and the above decoding procedure produces

$$1111 - 0100 = 1011.$$

Syndrom decoding is much fatser than searching for a nearest codeword to a received word. However, for large codes it is still too inefficient to be practical.

In general, the problem of finding the nearest neighbour in a linear code is NP-complete. Fortunately, there are important linear codes with really efficient decoding.

Hamming codes

An important family of simple linear codes that are easy to encode and decode, are so-called Hamming codes.

Definition Let r be an integer and H be an $r \times (2^r - 1)$ matrix columns of which are non-zero distinct words from $V(r,2)$. The code having H as its parity-check matrix is called binary Hamming code and denoted by $Ham(r,2)$.

Example

$$Ham(2,2) = H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

$$Ham(3,2) = H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \Rightarrow G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Theorem Hamming code $Ham(r,2)$

- is $[2^r - 1, 2^r – 1 - r]$ -code,
- has minimum distance 3,
- is a perfect code.

Properties of binary Hamming coes Coset leaders are precisely words of weight ≤ 1. The syndrome of the word 0…010…0 with 1 in j -th position and 0 otherwise is the transpose of the j -th column of H.

Hamming codes - decoding

Decoding algorithm for the case the columns of H are arranged in the order of increasing binary numbers the columns represent.

- **Step 1** Given y compute syndrome $S(y) = yH^T$.
- **Step 2** If $S(y) = 0$, then y is assumed to be the codeword sent.
- **Step 3** If $S(y) \neq 0$, then assuming a single error, $S(y)$ gives the binary position of the error.

Example

For the Hamming code given by the parity-check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

and the received word

$$y = 110\ 1011,$$

we get syndrome

$$S(y) = 110$$

and therefore the error is in the sixth position.

Hamming code was discovered by Hamming (1950), Golay (1950).

1

It was conjectured for some time that Hamming codes and two so called Golay codes are the only non-trivial perfect codes.

Comment

Hamming codes were originally used to deal with errors in long-distance telephon calls.

ADVANTAGES of HAMMING CODES

Let a binary symmetric channel is used which with probability q correctly transfers a binary symbol.

If a *4*-bit message is transmitted through such a channel, then correct transmission of the message occurs with probability q^4.

If Hamming (7,4,3) code is used to transmit a *4*-bit message, then probability of correct decoding is

$$q^7 + 7(1 - q)q^6.$$

In case $q = 0.9$ the probability of correct transmission is 0.651 in the case no error correction is used and 0.8503 in the case Hamming code is used - an essential improvement.

IMPORTANT CODES

- Hamming (7,4,3) -code. It has 16 codewords of length 7. It can be used to send $2^7 = 128$ messages and can be used to correct 1 error.

- Golay (23,12,7) -code. It has 4 096 codewords. It can be used to transmit 8 3888 608 messages and can correct 3 errors.

- Quadratic residue (47,24,11) -code. It has

16 777 216 codewords

and can be used to transmit

140 737 488 355 238 messages

and correct 5 errors.

- Hamming and Golay codes are the only non-trivial perfect codes.

GOLAY CODES - DESCRIPTION

Golay codes G_{24} and G_{23} were used by *Voyager I* and *Voyager II* to transmit color pictures of Jupiter and Saturn. Generation matrix for G_{24} has the form

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

G_{24} is (24,12,8) –code and the weights of all codewords are multiples of 4. G_{23} is obtained from G_{24} by deleting last symbols of each codeword of G_{24}. G_{23} is (23,12,7) –code.

GOLAY CODES - CONSTRUCTION

Matrix G for Golay code G_{24} has actually a simple and regular construction.

The first 12 columns are formed by a unitary matrix I_{12}, next column has all 1's.

Rows of the last 11 columns are cyclic permutations of the first row which has 1 at those positions that are squares modulo 11, that is

0, 1, 3, 4, 5, 9.

SINGLETON BOUND

If C is a linear (n,k,d) -code, then $n - k \geq d - 1$ (Singleton bound).

To show the above bound we can use the following lemma.

Lemma If u is a codeword of a linear code C of weight s,then there is a dependence relation among s columns of any parity check matrix of C, and conversely, any dependence relation among s columns of a parity check matrix of C yields a codeword of weight s in C.

Proof Let H be a parity check matrix of C. Since u is orthogonal to each row of H, the s components in u that are nonzero are the coefficients of the dependence relation of the s columns of H corresponding to the s nonzero components. The converse holds by the same reasoning.

Corollary If C is a linear code, then C has minimum weight d if d is the largest number so that every $d - 1$ columns of any parity check matrix of C are independent.

Corollary For a linear (n,k,d) it holds $n - k \geq d - 1$.

A linear (n,k,d) -code is called maximum distance separable (MDS code) if $d = n - k + 1$.

MDS codes are codes with maximal possible minimum weight.

REED-MULLER CODES

Reed-Muller codes form a family of codes defined recursively with interesting properties and easy decoding.

If D_1 is a binary $[n,k_1,d_1]$ -code and D_2 is a binary $[n,k_2,d_2]$ -code, a binary code C of length $2n$ is defined as follows $C = \{ | u | u + v |, \text{ where } u \in D_1, v \in D_2\}$.

Lemma C is $[2n,k_1 + k_2, \min\{2d_1,d_2\}]$ -code and if G_i is a generator matrix for D_i, $i = 1, 2$, then $\begin{pmatrix} G_1 & G_2 \\ 0 & G_2 \end{pmatrix}$ is a generator matrix for C.

Reed-Muller codes $R(r,m)$, with $0 \leq r \leq m$ are binary codes of length $n = 2^m$. $R(m,m)$ is the whole set of words of length n, $R(0,m)$ is the repetition code.

If $0 < r < m$, then $R(r + 1,m + 1)$ is obtained from codes $R(r + 1,m)$ and $R(r,m)$ by the above construction.

Theorem The dimension of $R(r,m)$ equals $1+\binom{m}{1}+\ldots+\binom{m}{r}$. The minimum weight of $R(r,m)$ equals 2^{m-r}. Codes $R(m - r - 1,m)$ and $R(r,m)$ are dual codes.

Singleton Bound

Singleton bound: Let C be a *q*-ary (*n, M, d*)-code.

Then

$$M \leq q^{n-d+1}.$$

Proof Take some $d - 1$ coordinates and project all codewords to the resulting coordinates.

The resulting codewords are all different and therefore *M* cannot be larger than the number of *q*-ary words of length $n-d-1$.

Codes for which $M = q^{n-d-1}$ are called MDS-codes (Maximum Distance Separable).

Corollary: If *C* is a *q*-ary linear [*n, k, d*]-code, then

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

Shortening and puncturing of linear codes

Let C be a q-ary linear $[n, k, d]$-code. Let

$$D = \{(x_1, \ldots, x_{n-1}) \mid (x_1, \ldots, x_{n-1}, 0) \in C\}.$$

Then D is a linear $[n-1, k-1, d]$-code – a shortening of the code C.

Corollary: If there is a q-ary $[n, k, d]$-code, then shortening yields a q-ary $[n-1, k-1, d]$-code.

Let C be a q-ary $[n, k, d]$-code. Let

$$E = \{(x_1, \ldots, x_{n-1}) \mid (x_1, \ldots, x_{n-1}, x) \in C, \text{ for some } x \leq q\},$$

then E is a linear $[n-1, k, d-1]$-code – a puncturing of the code C.

Corollary: If there is a q-ary $[n, k, d]$-code with $d > 1$, then there is a q-ary $[n-1, k, d-1]$-code.

Lengthening of Codes – Constructions X and XX

Construction X Let C □ D be q-nary linear codes with parameters $[n, K, d]$ and $[n, k, D]$, where $D > d$, and $K > k$. Assume also that there exists a q-nary code E with parameters $[l, K - k, \delta]$. Then there is a ”longer” q-nary code with parameters

$$[n + l, K, \min(d + \delta, D)].$$

The lengthening of C is constructed by appending $\varphi(x)$ to each word x □ C, where $\varphi : C/D \rightarrow E$ is a bijection – a well known application of this construction is the addition of the parity bit in binary codes.

Construction XX Let the following q-ary codes be given: a code C with parameters $[n, k, d]$; its sub-codes C_i, $i = 1,2$ with parameters $[n, k - k_i, d_i]$ and with $C_1 \cap C_2$ of minimum distance $\geq D$; auxiliary q-nary codes E_i, $i = 1,2$ with parameters $[l_i, k_i, \delta_i]$. Then there is a q-ary code with parameters

$$[n + l_1 + l_2, \mathrm{k}, \min\{D, d_2 + \delta_1, d_1 + \delta_2, d + \delta_1 + \delta_2\}].$$

Strength of Codes

- **Strength of codes** is another important parameter of codes. It is defined through the concept of the strength of so-called **orthogonal arrays** - an important concepts of combinatorics.
- An orthogonal array $QA_{\lambda}(t, n, q)$ is an array of n columns, λq^{t} rows with elements from $\mathbf{F}_q$ and the property that in the projection onto any set of t columns each possible t-tuple occurs the same number λ of times. t is called **strength** of such an orthogonal array.
- For a code C, let $t(C)$ be the strength of C - if C is taken as an orthogonal array.
- Importance of the concept of strength follows also from the following **Principle of duality**: For any code C its minimum distance and the strength of $C^{\perp}$ are closely related. Namely

$$d(C) = t(C^{\perp}) + 1.$$

Dimension of Dual Linear Codes

If C is an $[n, k]$-code, then its dual code $C^{\perp}$ is $[n, n - k]$ code.

A binary linear $[n, 1]$ repetition code with codewords of length n has two codewords: all-0 codeword and all-1 codeword.

Dual code to $[n, 1]$ repetition code is so-called **sum zero code** of all binary n-bit words whose entries sum to zero (modulo 2). It is a code of dimension $n - 1$ and it is a linear $[n, n - 1, 2]$ code

Reed-Solomon Codes

An important example of MDS-codes are q-ary Reed-Solomon codes RSC(k, q), for $k \leq q$.

They are codes generator matrix of which has rows labeled by polynomials X^i, $0 \leq i \leq k-1$, columns by elements $0, 1, \ldots, q-1$ and the element in a row labeled by a polynomial p and in a column labeled by an element u is $p(u)$.

RSC(k, q) code is $[q, k, q-k+1]$ code.

Example Generator matrix for RSC(3, 5) code is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{pmatrix}$$

Interesting property of Reed-Solomon codes:

$$RSC(k, q)^{\perp} = RSC(q-k, q).$$

Reed-Solomon codes are used in digital television, satellite communication, wireless communication, barcodes, compact discs, DVD,... They are very good to correct burst errors - such as ones caused by solar energy.

Trace and Subfield Codes

- Let p be a prime and r an integer. A trace tr is mapping from $\mathbf{F}_{p^r}$ into $\mathbf{F}_p$ defined by

$$tr(x) = \sum_{i=0}^{r-i} x^{p^i}.$$

- Trace is additive ($tr(x_1 + x_2) = tr(x_1) + tr(x_2)$) and $\mathbf{F}_p$-linear ($tr(\lambda x) = \lambda tr(x)$).
- If C is a linear code over $\mathbf{F}_{p^r}$ and tr is a trace mapping from $\mathbf{F}_{p^r}$ to $\mathbf{F}_p$, then **trace code** $tr(C)$ is a code over $\mathbf{F}_p$ defined by

$$(tr(x_1), tr(x_2), \ldots, tr(x_n))$$

where $(x_1, x_2, \ldots, x_n)$ □ C.

- If C □ $\mathbf{F}^n_{p^r}$ is a linear code of strength t, then strength of $tr(C)$ is at least t.
- Let C □ $\mathbf{F}^n_{p^r}$ be a linear code. The **subfield code** $C_{\mathbf{F}p}$ consists of those codewords of C all of whose entries are in $\mathbf{F}_p$.
- **Delsarte theorem** If C □ $\mathbf{F}^n_{p^r}$ is a linear code. Then

$$tr(C)^{□} = (C^{□})_{\mathbf{F}p}.$$

Soccer Games Betting System

Ternary Golay code with parameters (11, 729, 5) can be used to bet for results of 11 soccer games with potential outcomes 1 (if home team wins), 2 (if guests win) and 3 (in case of a draw).

If 729 bets are made, then at least one bet has at least 9 results correctly guessed.

In case one has to bet for 13 games, then one can usually have two games with pretty sure outcomes and for the rest one can use the above ternary Golay code.