Coding Theory[*]

Mihai Prunescu[†]

[*] This is more or less a translation in English of some sections of the book *Codierungstheorie* from Wolfgang Willems, published by de Gruyter, Berlin, New York, 1999.

[†] University of Bucharest, Faculty of Mathematics and Informatics; and Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania.
mihai.prunescu@imar.ro, mihai.prunescu@gmail.com

Contents

Part I

Introduction

1 What is a code

Definition 1.1 Let F be a finite set with $q = |F|$ elements. We call the set:

$$C \subseteq F^n = \{(u_1, \dots, u_n) \,|\, u_i \in F\}, C \neq \emptyset,$$

a block code over the alphabet F.

A code consists of code-words. The number n is called length of C.

If $q = 2$ we speak about a binary code, and we take $F = \mathbb{F}_2$. Also if $q = 3$ we have a ternary code, and we take $F = \mathbb{F}_3$. If $|C| = 1$ the code is called trivial. In general $F = \{0, 1, \dots, q-1\}$ is identified with $\mathbb{Z}_q$. If q is a prime-power, $q = p^m$ with $m \geq 1$, it is better to identify F with the finite field $\mathbb{F}_q$, which has a completely different structure than the ring $\mathbb{Z}_q$.

Definition 1.2 (R. W. Hamming, 1950) For $u, v \in F^n$, we define the function:

$$d(u, v) = |\{i \,|\, u_i \neq v_i\}|,$$

called Hamming distance between u and v.

Theorem 1.3 *The Hamming distance induces a structure of metric space over the set F^n or over the code C. With other words, the distance fulfills the following metric properties:*

1. *$d(u, v) \geq 0$ and $d(u, v) = 0 \leftrightarrow u = v$.*
2. *$d(u, v) = d(v, u)$.*
3. *Triangle inequality: $d(u, v) \leq d(u, w) + d(w, v)$.*

Moreover, if F is an abelian group, then d is invariant under translations:

$$d(u + w, v + w) = d(u, v).$$

Proof: (1) and (2) are immediate. Proof of (3): If we transform u in w and then w in v, we do more modifications as when we transform u in v, because some coordinates must be modified two times. Proof of the invariance under translations:

$$u_i \neq v_i \leftrightarrow u_i + w_i \neq v_i + w_i.$$

□

Definition 1.4 *The set:*

$$B_r(u) = \{v \,|\, v \in F^n, d(u, v) \leq r\}$$

is called ball of center u and radius r.

Lemma 1.5 *If $|F| = q$ and $r \geq 0$ then for all $u \in F^n$, one has:*

$$|B_r(u)| = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j.$$

Proof: It follows directly from the following remark:

$$|\{v \,|\, v \in F^n, d(u, v) = j\}| = \binom{n}{j} (q-1)^j.$$

□

Definition 1.6 The code C is t-error recognizing if for all $c \in C$,

$$B_t(c) \cap C = \{c\}.$$

Definition 1.7 The code C is e-error correcting if for all $c, c' \in C$ with $c \neq c'$,

$$B_e(c) \cap B_e(c') = \emptyset.$$

Definition 1.8 The code C has the minimal distance:

$$d(C) = \min\{d(c, c') \mid c \neq c'; c, c' \in C\}.$$

Definition 1.9 If the code $C \subset F^n$ has the minimal distance $d = d(C)$ and has $M = |C|$ elements, we say that C is a (n, M, d)-code over F.

Theorem 1.10 *If C is a code and $d = d(C)$ its minimal distance, then:*

1. *If $d \geq t + 1$ then C is t-error recognizing.*
2. *If $d \geq 2e + 1$ then C is e-error correcting.*

□

Here are some examples of codes used in the every-day life.

Example 1.11 Repetition code of length n:

$$C = \{(c, \dots, c) \mid c \in F\}.$$

As $d(C) = n$, C is $\leq \frac{n-1}{2}$-error correcting.

Example 1.12 Bank-account code. Take $F = \{0, 1, 2, \dots, 9\}$. Let $Q(z)$ be the digit-sum of z. We observe that $z \rightsquigarrow Q(2z)$ is a permutation of F. The code consists of all $(c_1, \dots, c_n)$ such that:

$$c_n + Q(2c_{n-1}) + c_{n-2} + Q(2c_{n-3}) + \cdots = 0 \bmod 10.$$

The code is 1-error recognizing, but it recognizes also accidental transpositions of neighbor digits.

Example 1.13 ISBN-10 Code. $F = \{0, 1, 2, \dots, 9, X\}$. The code is a succession of blocks, representing the language, the editor house, the book, and a final check digit. Example:

$$0 - 387 - 96617 - X.$$

The rule is that $10z_1 + 9z_2 + \cdots + 2z_9 + z_{10} = 0 \bmod 11$. Observe that as $\mathbb{Z}_{11}$ is a field, $i \rightsquigarrow iz$ is a permutation for all $z \neq 0$. This code recognizes one false digit, but recognizes as well an accidental transposition.

Example 1.14 EAN-13 Code. $F = \{0, 1, 2, \dots, 9\}$. The code-words have length 13, and the condition is that:

$$c_1 + 3c_2 + c_3 + 3c_4 + \cdots + c_{11} + 3c_{12} + c_{13} = 0 \bmod 10.$$

Again $z \rightsquigarrow 3z \bmod 10$ is a permutation of F.

2 Perfect codes

Definition 2.1 A code C is called *perfect* if and only if there is an $e \in \mathbb{N}$ such that:

$$F^n = \bigsqcup_{c \in C} B_e(c)$$

is a *disjoint* union of balls.

Theorem 2.2 *If $|F| = q$, C is a code of length n and $d(C) \geq 2e+1$ then the following inequality holds. This is called Hamming bound.*

$$q^n \geq |C| \sum_{j=0}^{e} \binom{n}{j} (q-1)^j.$$

Moreover, the code C is perfect if and only if we have equality.

Proof: Let $|F| = q$, C is a code of length n and $d(C) \geq 2e+1$. We know that for $c \neq c'$, $B_e(c) \cap B_e(c') = \emptyset$. Then:

$$q^n = |F|^n \geq \big| \bigcup_{c \in C} B_e(c) \big| = \sum_{c \in C} |B_e(c)| = |C||B_e(c)| = |C| \sum_{j=0}^{e} \binom{n}{j} (q-1)^j.$$

□

We observe that trivial codes, F^n and repetition codes of length $n = 2e+1$ are perfect.

Example 2.3 The $(n, |C|, d) = (7, 2^4, 3)$ Hamming Code. The code consists of all the tuples $(c_1, \ldots, c_7) \in \mathbb{F}_2^7$ such that following equalities are fulfilled:

$$\begin{aligned} c_1 + c_4 + c_6 + c_7 &= 0, \\ c_2 + c_4 + c_5 + c_7 &= 0, \\ c_3 + c_5 + c_6 + c_7 &= 0. \end{aligned}$$

The code is a linear variety of dimension 4, so it contains $|C| = 2^4$ elements. We observe that $\mathbb{F}_2^7$ is an abelian group, so the Hamming distance is invariant under translations. It follows that:

$$d(C) = \min\{d(c, 0) \mid c \neq 0\}.$$

We show now that $d(C) \geq 3$. It is to show that every code word contains at least three digits different from 0. Let $c_1 = 1$. From the first equation, it follows that one of c_4, c_6 or c_7 is 1. From the other two equations it follows now that one of c_2, c_5 or c_7 must be 1. The same happens also if we start with another $c_i \neq 0$.

Now we show that $d(C) \leq 3$. Indeed the point $c = (0,0,0,1,1,1,0) \in C$, and it has $d(c, 0) = 3$.

So $d(C) = 3$. If we take $e = 1$ then $d(C) \geq 2 \cdot 1 + 1$ so C is 1-error correcting and 2-error recognizing.

Moreover, C **is perfect**:

$$2^7 \geq |C|(1+n) = 2^4(1+7) = 2^7,$$

so the Hamming bound condition is fulfilled.

Remark 2.4 Zinov'ev and Leont'ev, *The nonexistence of perfect codes over Galois fields.* Problems of control and information theory 2, 123 - 132, 1973, proved the following: If q is a prime power, the only perfect codes are:

- The $(\frac{q^k-1}{q-1}, q^{n-k}, 3)$ Hamming codes,

- The $(23, 2^{12}, 7)$ binary Golay code,

- The $(11, 3^6, 5)$ ternary Golay code.

If q is not a prime power, there are not known perfect codes and the problem is open.

The following result is called Singleton Bound Theorem.

Theorem 2.5 *C code of length n over F with $|F| = q$. If $d = d(C)$, then:*

$$d \leq n - \log_q |C| + 1.$$

Proof: Consider some projection $\alpha : F^n \to F^{n-d+1}$, for example $\alpha(u_1, \dots, u_n) = (u_1, \dots, u_{n-d+1})$. Because the minimal distance $d(C) = d$, $\alpha|C$ is an injection, so:

$$|C| = |\alpha(C)| \leq |F^{n-d+1}| = q^{n-d+1}.$$

This means that $\log_q |C| \leq n - d + 1$, so $d \leq n - \log_q |C| + 1$. □

Definition 2.6 Codes C which satisfy:

$$d = n - \log_q |C| + 1$$

are called Maximum Distance Separable codes, shortly MDS-codes.

3 Linear codes

Definition 3.1 Let K be a finite field and $C \leq K^n$ be a vector subspace. We call C linear code over K. We speak about an:

$$[n, k, d]$$

code if $k = \dim_K C$ and $d = d(C)$.

Definition 3.2 The weight function wt $: K^n \to \mathbb{N}$ is defined as:

$$\mathrm{wt}\,(u) = |\{i \,|\, u_i \neq 0\}|.$$

For a linear code C we define:

$$\mathrm{wt}\,(C) = \min\{\mathrm{wt}\,(c) \,|\, 0 \neq c \in C\}.$$

The set $\{i \,|\, u_i \neq 0\}$ is called support of u and denoted supp (u). Shortly, wt $(u) = |$supp $(u)|$. For a subset $U \subseteq K^n$,

$$\mathrm{supp}\,(U) = \bigcup_{u \in U} \mathrm{supp}\,(u).$$

We consider in general codes with supp $(C) = \{1, 2, \dots, n\}$.

Lemma 3.3 *If C is a linear code,* wt $(C) = d(C)$.

Proof: If $|C| = 1$, there is nothing to prove. Else:

$$d(C) = \min\{d(c, c') \,|\, c \neq c'; c, c' \in C\} = \min\{d(c - c', 0) \,|\, c \neq c'; c, c' \in C\} =$$

$$= \min\{\mathrm{wt}\,(c) \,|\, c \neq 0, c \in C\} = \mathrm{wt}\,(C).$$

□

Remark 3.4 To save a linear code, it is enough to keep a basis instead of the whole code.

Definition 3.5 Let $\mathcal{M}_{k\times n}(K)$ the set of matrices with k rows and n columns with elements in K. If $A \in \mathcal{M}_{k\times n}(K)$ then the transposed matrix $A^T \in \mathcal{M}_{n\times k}(K)$. We denote by $\mathrm{rk}\, A$ the rank of A, which is the number of linear independent columns or the number of linear independent rows.

Definition 3.6 Let C be an $[n, k]$-code over K. A matrix $G \in \mathcal{M}_{k\times n}(K)$ is a generating matrix of C if we consider $G : K^k \to K^n$ by:

$$G(u) = uG = (u_1, \dots, u_k)G,$$

and $C = G(K^k) = Im(G)$ is the image of G. The rows of G form a basis for C. Then:

$$\mathrm{rk}\,(G) = k = \dim_K(C).$$

Definition 3.7 Let C be an $[n, k]$-code over K. A matrix $H \in \mathcal{M}_{(n-k)\times n}(K)$ is a check matrix for C if :

$$C = \{u \,|\, u \in K^n, Hu^T = 0\} = Ker(H),$$

the code is the kernel of H. In this case:

$$\mathrm{rk}\,(H) = n - \dim Ker(H) = n - \dim C = n - k.$$

Every subspace of dimension k is an intersection of $n - k$ many hyperplanes, so there is always a check matrix.

Maximum Likelihood and Syndrome Decoding. Let $\tilde{c} \in K^n$ a received word, possibly containing errors. We look for a $c \in C$ such that $f = \tilde{c} - c \in \tilde{c} + C$ has minimal weight. But:

$$H\tilde{c}^T = H(f + c)^T = Hf^T + Hc^T = Hf^T.$$

Definition 3.8 $Hv^T = s_v \in K^{n-k}$ is called the syndrome of $v \in K^n$.

We observe that $\tilde{c}$ and f have the same syndrome.

For some equivalence class $v + C \subset K^n$ we find a representative $f_v \in v + C$ such that:

$$\mathrm{wt}\,(f_v) = \min\{\mathrm{wt}\,(v + c) \,|\, c \in C\}.$$

So decoding works with $\tilde{c} \rightsquigarrow c = \tilde{c} - f_{\tilde{c}}$. □

Theorem 3.9 *Let C be a nontrivial $[n, k]$-code over K and H its check matrix. Then:*

$$d(C) = \mathrm{wt}\,(C) = \min\{w \,|\, \text{there are } w \text{ many linear dependent columns in } H\} =$$

$$= \max\{w \,|\, \text{any } w - 1 \text{ many columns of } H \text{ are linear independent}\}.$$

Proof: Let $h_1, \dots, h_n$ be the columns of H. As $C \neq \{0\}$, this family of vectors is linear dependent. Let $w \in \mathbb{N}$ minimal such that there are w many linear dependent columns $h_{i_1}, \dots, h_{i_w}$. So there is a relation:

$$\sum_{j=1}^{n} c_j h_j = 0,$$

with $c_j \in K$ and all $c_k \neq 0$ if and only if $k \in \{i_1, \dots, i_w\}$.

Choose $c = (c_1, \dots, c_n)$. Then $Hc^T = 0$ so $c \in C$. But $\mathrm{wt}\,(c) = w$ so $\mathrm{wt}\,(C) \leq w$. Suppose there is some $0 \neq \tilde{c} \in C$ with $\mathrm{wt}\,(\tilde{c}) < w$. But $H\tilde{c}^T = 0$, so there are $< w$ many linear dependent columns in H. Contradiction. □

Part II

Code constructions

4 Hamming and Simplex codes

Let K be a finite field with q elements and $k \geq 2$ a natural number.

The projective space of dimension $k-1$ is the set:

$$\mathbb{P}^{k-1}(q) = \{\langle u\rangle \,|\, 0 \neq u = (u_1, \ldots, u_k)^T, u_i \in K\}.$$

Here $\langle u\rangle$ is the equivalence class of u for the equivalence relation defined as $\langle u\rangle = \langle v\rangle$ if and only if $\exists\, \lambda \in K^\times, u = \lambda v$. The projective space has n elements, where:

$$n = |\mathbb{P}^{k-1}(q)| = \frac{q^k - 1}{q-1}.$$

If $\mathbb{P}^{k-1}(q) = \{\langle h_1\rangle, \ldots, \langle h_n\rangle\}$, we define:

$$H = (h_1, \ldots, h_n) \in \mathcal{M}_{k\times n}(K).$$

Definition 4.1 We define a Hamming Code as the code C over K with check matrix H:

$$C = \{c \,|\, c \in K^n, Hc^T = 0\} \leq K^n.$$

As $\mathrm{rk}\,(H) = k$, $\dim C = n - k$.

Every two columns of H are linear independent, but $\langle h_1\rangle$, $\langle h_2\rangle$ and $\langle h_1 + h_2\rangle$ are linear dependent. So $\mathrm{wt}\,(C) = d(C) = 3$.

So C has the parameters $[n, n-k, 3]$, where $n = (q^k - 1)/(q-1)$. As $3 \geq 2 \cdot 1 + 1$, C is 1-error correcting.

The fact that C is perfect follows from the sphere-packing equation:

$$\big|\bigcup_{c\in C} B_1(c)\big| = |C|\; |B_1(0)| = q^{n-k}(1 + n(q-1)) = q^{n-k}\big(1 + \frac{q^k-1}{q-1}(q-1)\big) = q^n.$$

For the Hamming code there is a special notation: $Ham_q(k)$.

Definition 4.2 We define a Simplex Code as the code C over K with generating matrix H:

$$C = \{aH \,|\, a \in K^k\} \leq K^n.$$

Theorem 4.3 *Let C be a Simplex code and $c \in C \setminus \{0\}$. Then* $\mathrm{wt}\,(c) = q^{k-1}$.

Proof: Let z_i be the rows of H.

$$0 \neq c = (c_1, \ldots, c_n) = \sum_{i=1}^{k} a_i z_i = \sum_{i=1}^{k} a_i (z_{i1}, \ldots, z_{in}) \in C.$$

$$U = \{(b_1, \ldots, b_k)^T \,|\, b_i \in K, \sum_{i=1}^{k} a_i b_i = 0\}$$

is a $(k-1)$-dimensional vector space and contains q^{k-1} elements. A number of $(q^{k-1}-1)/(q-1)$ of the columns h_j of H are equivalent with elements of U. In fact:

$$c_j = 0 \longleftrightarrow \exists\, b \in U\; \exists j\; \langle h_j\rangle = \langle b\rangle.$$

In conclusion:

$$\mathrm{wt}\,(c) = n - \frac{q^{k-1}-1}{q-1} = \frac{q^k-1}{q-1} - \frac{q^{k-1}-1}{q-1} = q^{k-1}.$$

□

So the Hamming distance between two code-words is q^{k-1}, and the minimal distance is q^{k-1} as well. So the Simplex Code is a

$$\Big[\frac{q^k-1}{q-1}, k, q^{k-1}\Big]$$

code. For the Simplex Code one has the special notation $Sim_q(k)$.

5 Classic evaluation codes

Let K be a field with q elements and $1 \leq k \leq n \leq q$. Recall that $K[x]$ is the ring of polynomials in variable x over K. Consider a set $M \subseteq K$ with $M = \{a_1 \ldots, a_n\}$ with $a_i \neq a_j$ for $i \neq j$. We consider the following linear subspace of K^n:

$$C = \{(f(a_1), \ldots, f(a_n)) \,|\, f \in K[x], \deg f < k\}.$$

C is called classic Reed-Solomon code or RS-code, and is an evaluation code.

Because $n \geq k$ we can get back the coefficients of f from the code-word. So C has length n and dimension k. Moreover, every code-word different from 0 has at least $n-(k-1)$ many coordinates $\neq 0$, so $\mathrm{wt}\, c \geq n-k+1$. For the polynomial $f(x) = (x-a_1)\ldots(x-a_{k-1})$ we have $\mathrm{wt}\, c_f = n-k+1$. So $d(C) = n-k+1$ and the code is a $[n, k, n-k+1]$-code.

For the classic Reed-Müller code (Reed, Müller, 1950, introduced independently in different articles), we present only the situation with $K = \mathbb{F}_2$. Let $K[x_1, \ldots, x_m]$ be the polynomial ring in variables $x_1, \ldots, x_m$ over K. For a polynomial:

$$0 \neq f = \sum k_{(e_1,\ldots,e_m)} x_1^{e_1} \ldots x_m^{e_m} \in K[x_1, \ldots, x_m],$$

we define $\deg f = \max\{e_1 + \cdots + e_n \,|\, k_{(e_1,\ldots,e_m)} \neq 0\}$, and define $\deg 0 = -\infty$. If $K^m = \{P_1, \ldots, P_n\}$ - so $n = 2^m$ - we consider the evaluation:

$$f \rightsquigarrow c_f = (f(P_1), \ldots, f(P_n)) \in K^n,$$

where $f(P) = f(a_1, \ldots, a_n)$ for $P = (a_1, \ldots, a_n)$. As the polynomials x and x^2 define the same function in K, we evaluate only polynomials like:

$$f = \sum_{0 \leq e_i \leq 1} k_{(e_1,\ldots,e_m)} x_1^{e_1} \ldots x_m^{e_m}.$$

We stress the fact that the evaluation is done with the convention $0^0 = 1$.

Let V be the vector space of these polynomials and for $r \leq m$:

$$V_r = \{f \in V \mid \deg f \leq r\}.$$

Then $\dim V = 2^m$ and $\dim V_r = \sum_{i=0}^{r} \binom{m}{i}$.

Definition 5.1 *Let $K = \mathbb{F}_2$ and $0 \leq r \leq m$. We define the Reed-Müller code of order r:*

$$RM(r, m) = \{(f(P_1), \ldots, f(P_n)) \,|\, f \in V_r\}.$$

Theorem 5.2 *The Reed-Müller code $RM(r, m)$ is a linear code with parameters:*

$$\Big[2^m, \sum_{j=0}^{r} \binom{m}{j}, 2^{m-r}\Big].$$

Proof: The linearity and the length are trivial. The dimension of the code comes from the fact that the evaluation is an injective morphism, like for the Reed-Solomon codes. So in the rest of the proof we will compute the minimal distance.

The evaluation of the polynomial $f(x_1, \dots, x_m) = x_1 \dots x_r$ has the weight 2^{m-r} because this is the number of vectors $(x_1, \dots, x_m)$ that evaluate 1. Now we show that every polynomial $f \in V_r$ generates a code-word of weight $\geq 2^{m-r}$. This is done by induction. For $m = 0$, this is true. Suppose that this is already true for $RM(r, m-1)$ for $m \geq 1$ and all $0 \leq r \leq m-1$. We can write $f \in V_r$ as:

$$f = f(x_1, \dots, x_m) = g(x_1, \dots, x_{m-1}) + h(x_1, \dots, x_{m-1})x_m.$$

Consider the cardinalities:

$$\begin{array}{rcl} a & = & |\{P = (*, \dots, *, 0) \,|\, P \in K^m, f(P) \neq 0\}|, \\ b & = & |\{P = (*, \dots, *, 1) \,|\, P \in K^m, f(P) \neq 0\}|. \end{array}$$

If $h = 0$, we get by induction $a, b \geq 2^{m-1-r}$ so $a + b \geq 2^{m-r}$. If $h \neq 0$, we get by induction $a \geq 2^{m-1-r}$ if $g \neq 0$ and $b \geq 2^{m-1-r}$ if $g + h \neq 0$. Finally if $g = 0$ or if $g = -h$ then $\deg h \leq r - 1$ and by induction $b \geq 2^{(m-1)-(r-1)} = 2^{m-r}$. □

6 Generalized Reed-Solomon codes

Let K be a field with q elements, and $2 \leq d \leq n \leq q$. We fix values $a = (a_1, \dots, a_n) \in K^n$ with $i \neq j \to a_i \neq a_j$ and $v = (v_1, \dots, v_n) \in K^n$ such that all $v_i \neq 0$.

One constructs the following matrix $H \in \mathcal{M}_{(d-1)\times n}(K)$:

$$H = \begin{pmatrix} v_1 & \dots & \dots & \dots & v_n \\ a_1 v_1 & \dots & \dots & \dots & a_n v_n \\ a_1^2 v_1 & \dots & \dots & \dots & a_n^2 v_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1^{d-2} v_1 & \dots & \dots & \dots & a_n^{d-2} v_n \end{pmatrix}.$$

Every $(d-1)\times(d-1)$ submatrix of H is regular, as it has the determinant $v_{i_1} \dots v_{i_{d-1}} \prod_{i<j}(a_j - a_i)$. We define the Generalized Reed-Solomon Code $GRS_d(a, v)$ as:

$$GRS_d(a, v) = \{c \,|\, c \in K^n, Hc^T = 0\}.$$

As all $(d-1) \times (d-1)$ minors are regular, $d(GRS_d(a, v)) = d$. Also, this code has dimension $n - \mathrm{rk}\,(H) = n - d + 1$. So $GRS_d(a, v)$ is a code:

$$[n, n - d + 1, d].$$

Now recall that for finite fields K, the multiplicative group $K^\times$ is cyclic. Let α be a generator of this group. If $v = a = (1, \alpha, \dots, \alpha^{q-2})$ we are dealing with a Reed-Solomon Code of dimension $q - d$.

Definition 6.1 A code C is cyclic if for every $c = (c_1, \dots, c_n) \in C$, one has $(c_n, c_1, \dots, c_{n-1}) \in C$.

Theorem 6.2 *A Reed-Solomon code is cyclic.*

Proof: Let $c = (c_0, \dots, c_{q-2}) \in RS_d$. We see that:

$$\sum_{i=0}^{q-2} c_i \alpha^{ij} = 0$$

for all $j = 1, \dots, d-1$. So:

$$0 = \alpha^j \sum_{i=0}^{q-2} c_i \alpha^{ij} = \sum_{i=0}^{q-2} c_i \alpha^{(i+1)j} = c_{q-2} + c_0\alpha^j + \cdots + c_{q-3}\alpha^{(q-2)j}$$

for $j = 1, \dots, d-1$. So $c' = (c_{q-2}, c_0, \dots, c_{q-3}) \in C$.

7 Binary Reed-Müller codes by Plotkin construction

Put again $K = \mathbb{F}_2$. We start with a method called Plotkin construction:

Lemma 7.1 *For $i = 1, 2$ let C_i be $[n, k_i, d_i]$ codes over K. Then:*

$$C = C_1 \ \& \ C_2 = \{(c_1, c_1 + c_2) \,|\, c_1 \in C_1, c_2 \in C_2\} \leq K^{2n}$$

is a $[2n, k_1 + k_2, \min(2d_1, d_2)]$-code.

Proof: Consider $\alpha : C_1 \oplus C_2 \to C$ given by $\alpha(c_1, c_2) = (c_1, c_1 + c_2)$. As this mapping is injective, $\dim C = k_1 + k_2$. Now $\mathrm{wt}\,(c_1) \geq |\mathrm{supp}\,(c_1) \cap \mathrm{supp}\,(c_2)|$ so:

$$\mathrm{wt}\,(c) = \mathrm{wt}\,(c_1) + \mathrm{wt}\,(c_1 + c_2) \geq \mathrm{wt}\,(c_1) + \mathrm{wt}\,(c_1) + \mathrm{wt}\,(c_2)$$

$$-2\,|\mathrm{supp}\,(c_1) \cap \mathrm{supp}\,(c_2)| \geq \mathrm{wt}\,(c_2) \geq d_2,$$

if $c_2 \neq 0$. For $c_2 = 0$, $\mathrm{wt}\,(c) = 2\mathrm{wt}\,(c_1) \geq 2d_1$. If one of c_1 and c_2 is 0 and the other one has minimal weight, the minimum is also taken. □

Let $K = \mathbb{F}_2 = \{0, 1\}$ and $r, m \in \mathbb{N}$, $0 \leq r \leq m$.

The binary Reed-Müller codes $RM(r, m)$ are $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$ inductively defined as follows:

$RM(0, m)$ is the $[2^m, 1, 2^m]$ repetition code of length 2^m.

$RM(m, m) = \{0, 1\}^{2^m}$.

$RM(r, m) = RM(r, m-1) \ \& \ RM(r-1, m-1)$ for $1 \leq r \leq m-1$.

So $RM(r, m)$ has length 2^m and minimal distance:

$$d = \min(2 \cdot 2^{m-1-r}, 2^{m-1-(r-1)}) = 2^{m-r}.$$

Its dimension can be inductively computed as well:

$$\dim RM(r, m) = \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} = 1 + \sum_{i=0}^{r-1} \left[\binom{m-1}{i+1} + \binom{m-1}{i}\right] =$$

$$= 1 + \sum_{i=0}^{r-1} \binom{m}{i+1} = \sum_{i=0}^{r} \binom{m}{i}.$$

We observe also that always $RM(r-1, m) \subset RM(r, m)$ and that $(1, 1, \dots, 1) \in RM(r, m)$.

$RM(1, 5)$ is a $[32, 6, 16]$-code and was used by the Mariner Mars Mission 1969 - 1976. As $7 \leq (d-1)/2 = 15/2$, so 7 errors per code-word could be corrected. The code-words encoded $2^6 = 64$ different tones of grey for black and white pictures of high resolution.

8 Linear code mappings

Recall that $GL(n, K)$ is the group of invertible square matrices with coefficients in K.

Definition 8.1 A matrix $A \in GL(n, K)$ is an isometry according to the Hamming metric if for all $u, v \in K^n$, $d(uA, vA) = d(u, v)$.

Let $Iso(n, K)$ mean the set of these matrices, which are Hamming isometries. $Iso(n, K) \leq GL(n, K)$ is a subgroup. We observe that the group of permutations S_n can be also embedded in $GL(n, K)$, as follows. An element $\pi \in S_n$ corresponds to the permutation matrix $P(\pi)$, where:

$$P(\pi) = (p_{ij}) = \begin{cases} 1, & i = \pi j, \\ 0, & \text{else}. \end{cases}$$

Definition 8.2 A matrix M is called monomial if it has the form:

$$M = Diag(a_1, \dots, a_n)P(\pi),$$

for some $a_i \neq 0$ and some $\pi \in S_n$. The monomial matrices build the monomial group $M(n, K)$.

Theorem 8.3 $Iso(n, K) = M(n, K)$.

Proof: It is clear that $M(n, K) \subseteq Iso(n, K)$. For the converse, consider an $A \in Iso(n, K)$. When acting on a standard basis vector $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, $1 = \text{wt}\,(e_i) = \text{wt}\,(e_i A)$, so $e_i A = a_i e_{i'}$ with $a_i \neq 0$ and such that $(i \rightsquigarrow i')$ is a permutation π of $\{1, \dots, n\}$.
So $A = Diag(a_1, \dots, a_n)P(\pi^{-1})$. □

Definition 8.4 Consider the linear codes $C, C' \leq K^n$.

1. C and C' are equivalent codes, denoted $C \simeq C'$, if there is $A \in M(n, K)$, $CA = C'$.
2. The automorphism group of C is the set:
$$Aut(C) = \{A \,|\, A \in M(n, K), CA = C\}.$$
3. Consider the mapping $\alpha : Aut(C) \to S_n$ given by $\alpha(Diag(a_1, \dots, a_n)P(\pi)) = \pi$. The group of permutations of a code C is $Per(C) = Im(\alpha)$.

If we permute columns or rows of the check matrix H or of the generating matrix G, or if we multiply them with scalars, we obtain equivalent codes.

Definition 8.5 Let C be an $[n, k]$-code over K.

1. The following code is called the extension of C:
$$\hat{C} = \Big\{(c_1, \dots, c_{n+1}) \,|\, c_i \in K, (c_1, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\Big\}.$$
$\hat{C}$ is an $[n+1, k]$-code and $d(C) \leq d(\hat{C}) \leq d(C) + 1$. $\hat{C}$ is recognised by the matrix:
$$\hat{H} = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ & & & & 0 \\ & & H & & 0 \\ & & & & 0 \end{pmatrix}.$$

2. Let $n \geq 2$ and $1 \leq i \leq n$. The code:

$$\check{C} = \check{C}_i = \{(c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n) \,|\, (c_1, \dots, c_{i-1}, 0, c_{i+1}, \dots, c_n) \in C\}$$

is called truncation of C. If C has length n, $\check{C}_i$ is a $[n-1, k-1]$-code. Also, $d(\check{C}) \geq d(C)$. The check matrix $\check{H}$ is the check matrix H without the column corresponding to the coordinate which is truncated.

3. Let $n \geq 2$ and $1 \leq i \leq n$. The code:

$$\mathring{C} = \mathring{C}_i = \{(c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n) \,|\, (c_1, \dots, c_{i-1}, c_i, c_{i+1}, \dots, c_n) \in C\}$$

is called punctuation of C.

Examples: If C is a binary code with odd $d(C)$, then $d(\hat{C}) = d(C) + 1$ because we have an even number of ones in every code-word. In particular the extended binary Hamming code has minimal distance 4.

If $C = GRS_d(a, v)$ then $\hat{C} = GRS_{d+1}(\hat{a}, \hat{v})$ where $\hat{a} = (a, 0)$ and $\hat{v} = (v, 1)$.

If C is an MDS-code, then a truncation of C is an MDS-code again. □

Observation 8.6 A finite field K with q^m elements is a vector space of dimension m over a field K_0 with q elements. So every n-code C over K is an mn-code C_0 over K_0. If C is e-error correcting, C_0 can correct e groups of m many consecutive errors, which in a transmision are very usual.

Observation 8.7 Given a $[n, k, d]$-code, by simple concatenation of t code-words in all possible ways, one constructs a $[tn, tk, d]$-code named interleaving of the original code.

Definition 8.8 Let E be a set and $U \leq S(E)$ be a subgroup of its permutation group.

1. For some $i \in E$, $U_i = \{\pi \,|\, \pi \in U, \pi i = i\}$ is the stabilizer of i in U.
2. U is called k-transitive on E if for every pair of ordered subsets $(i_1, \dots, i_k)$ and $(j_1, \dots, j_k)$ of E, there is a $\pi \in U$ such that $\pi i_t = j_t$ for all t. For 1-transitive, we say just transitive.

If U is k-transitive, then:

(U is transitive over E) and (every stabilizer U_i is $(k-1)$-transitive over $E \setminus \{i\}$).

Theorem 8.9 *C is a code of length n over K.*

1. *If $Per(C)$ is transitive, then all punctuated codes of C are equivalent.*
2. *If $0 \neq C < K^n$ and $Per(C)$ is 2-transitive, then every diagonal automorphism of C has the shape $Diag(a, a, \dots, a)$.*

Proof: (1) Take $i \in \{1, \dots, n-1\}$. As $Per(C)$ is transitive, there is a monomial matrix $M = P(\pi)Diag(a_1, \dots, a_n) \in Aut(C)$ with $\pi n = i$. For every $(c_1, \dots, c_n) \in C$ there is a $(\tilde{c}_1, \dots, \tilde{c}_n) \in C$ such that:

$$(c_1, \dots, c_n) = (\tilde{c}_1, \dots, \tilde{c}_n)M = (a_1 \tilde{c}_{\pi 1}, \dots, a_n \tilde{c}_{\pi n}).$$

$$(c_1, \dots, c_{n-1}) = (a_1 \tilde{c}_{\pi 1}, \dots, a_{n-1} \tilde{c}_{\pi(n-1)}) =$$

$$= (\tilde{c}_1, \dots, \tilde{c}_{i-1}, \tilde{c}_{i+1}, \tilde{c}_n) P(\sigma) Diag(a_1, \dots, a_{n-1}),$$

where $\sigma \in S_{n-1}$ is some permutation. So $\mathring{C}_n = \mathring{C}_i P(\sigma) Diag(a_1, \dots, a_{n-1})$.

(2) Take $0 \neq c = (c_1, \dots, c_n) \in C$ with $\mathrm{wt}\,(c)$ minimal. If $\mathrm{wt}\,(c) = 1$ then c is some e_i and with $Per(C)$ transitive, all $e_i \in C$ and $C = K^n$, which is a contradiction. So $\mathrm{wt}\,(c) \geq 2$. Suppose that $D = Diag(a_1, \dots, a_n) \in Aut(C)$ with $a_n \neq a_i$ for some i. As $Per(C)$ is 2-transitive, one can suppose that $c_i \neq 0$ and $c_n \neq 0$. So:

$$a_n c - cD = ((a_n - a_1)c_1, \dots, (a_n - a_{n-1})c_{n-1}, 0) \in C.$$

But $(a_n - a_i) \neq 0$ and $\mathrm{wt}\,(ca_n - cD) < \mathrm{wt}\,(c)$, which is a contradiction to the minimality of $\mathrm{wt}\,(c)$. So $Diag(a, a, \dots, a)$ with $a \in K^\times$ are the unique diagonal automorphisms of C. □

Theorem 8.10 *Up to a permutation of coordinates, every k-dimensional code C has a generating matrix in systematic form:*

$$G = (E_k \,|\, *).$$

Proof: Let G be the generating matrix of some $[n, k]$-code over K. As G has rank k, there are k many columns of G, say $s_{i-1}, \dots, s_{i-k} \in (K^k)^T$ such that $X = (s_{i-1}, \dots, s_{i-k})$ is a regular matrix. Choose $\pi \in S_n$ such that $GP(\pi) = (X \,|\, Y)$. It follows that $X^{-1}GP(\pi) = (E_k \,|\, Z)$. Because $K^k X^{-1} G = K^k G = C$, the matrix $X^{-1}G$ is a generating matrix for C. Also, $K^k X^{-1} GP(\pi) = CP(\pi) = C'$, a code obtained from C by permuting some coordinates, and the matrix $X^{-1}GP(\pi) = (E_k \,|\, Z)$ is the generating matrix for C'. □

9 Griesmer bound

Theorem 9.1 *Let K be a field with q elements and let C be a $[n, k, d]$-code over K. Then:*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Proof: Induction over k. The statement is correct for $k = 0, 1$. Let be $k \geq 2$ and G be a generating matrix for C. We can suppose that the first row of G is a code-word of minimal weight. Moreover, by applying an equivalence of codes, we can suppose that:

$$G = \begin{pmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ & G_1 & & & G_2 & \end{pmatrix} = \begin{pmatrix} & z & \\ G_1 & & G_2 \end{pmatrix}.$$

Here is G_1 a $(k-1) \times d$ matrix and G_2 a $(k-1) \times (n-d)$ matrix. We show first that the rank of G_2 is $k - 1$. $(G_1 \,|\, G_2)$ can be taken in the following form:

$$\begin{pmatrix} a_1 & \dots & a_d & 0 & \dots & 0 \\ & * & & & * & \end{pmatrix}$$

using some elementary transformations. If $a_1 = a_2 = \dots = a_d$, we get a contradiction with the fact that G has rank k. So:

$$0 \neq c = a_1 z - (a_1, \dots, a_d, 0, \dots, 0) \in C,$$

but this is a contradiction because $\mathrm{wt}\,(c) < d$. So G_2 is a generating matrix for a $[n-d, k-1, d_2]$-code, that we call C_2. Consider now $(u \,|\, v)$ some row of the matrix $(G_1 \,|\, G_2)$ with $u = (u_1, \dots, u_d)$. For $b \in K$ let $n_b = |\{i \,|\, u_i = b\}|$. For some $a \in K$ is $n_a = \max(n_b \,|\, b \in K)$. Clearly,

$$n_a \geq \left\lceil \frac{d}{q} \right\rceil.$$

But $0 \neq (u \,|\, v) - az \in C$ and $\mathrm{wt}\,((u \,|\, v) - az) \geq d$, and so:

$$\mathrm{wt}\,(v) \geq \left\lceil \frac{d}{q} \right\rceil.$$

Over elementary transformations of $(G_1 \,|\, G_2)$ we can reach every $0 \neq v \in C_2$. The induction hypothesis reads now:

$$n - d \geq \sum_{i=0}^{k-2} \left\lceil \frac{d_2}{q^i} \right\rceil \geq \sum_{i=0}^{k-2} \left\lceil \frac{d}{q^{i+1}} \right\rceil = \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

$$n \geq \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil + \left\lceil \frac{d}{q^0} \right\rceil = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Corollary 9.2 *If there is a $[n, k, d]$-code over some field, then there is also a $[n-d, k-1, d']$-code with $d' \geq \left\lceil \frac{d}{q} \right\rceil$.*

Theorem 9.3 *The binary Reed-Muller-codes $RM(1, m)$ reach the Griesmer bound. Moreover, they are uniquely determined by their parameters $[2^m, m+1, 2^{m-1}]$ up to code equivalence.*

Proof: The Griesmer bound reads:

$$2^m \geq \sum_{i=0}^{m} \left\lceil \frac{2^{m-1}}{2^i} \right\rceil = 2^{m-1} + \cdots + 2 + 1 + 1 = 2^m.$$

Second part remains as an exercise. □

10 Gilbert-Varshamov bound

Theorem 10.1 *Let K be a field with q elements and let $n, k, d \in \mathbb{N}$ with $k \leq n$ and*

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i.$$

Then there exists a $[n, k, d']$-code with $d' \geq d$.

Proof: If $k = n$ then $d = 1$ and the statement is true. So let $k < n$, $V = K^{n-k}$, $v_1, \ldots v_{n-k}$ be a basis of V and suppose that we already found vectors $v_{n-k+1}, \ldots, v_{n-k+s} \in V$ such that every $d-1$ elements in $V_s = \{v_1, \ldots, v_{n-k+s}\}$ are linear independent. The number of vectors which can be represented as linear combination of at most $d-2$ many elements of V_s, is $\leq$

$$\sum_{i=0}^{d-2} \binom{n-k+s}{i} (q-1)^i.$$

If this sum is strictly smaller then q^{n-k}, we can find $v_{n-k+s+1} \in V \setminus \langle V_s \rangle$ such that every $d-1$ vectors in:

$$V_{s+1} = V_s \cup \{v_{n-k+s+1}\}$$

are linear independent. Finally we get $V_k = \{v_1, \ldots, v_n\}$. We write those vectors as the columns of a matrix $H \in \mathcal{M}_{(n-k)\times n}(K)$, so is H the check matrix of a $[n, k, d']$-code with $d' \geq d$. □

Part III
Duality

11 The dual code

Definition 11.1 Let K be some field and $n \in \mathbb{N}$. The function $\langle\, , \rangle : K^n \times K^n \to K$ given by:

$$\langle u, v\rangle = \sum_{i=1}^{n} u_i v_i$$

defines a symmetric non-degenerated K-bilinear form over K^n. For $C \subseteq K^n$ (code or just subset),

$$C^\perp = \{u \in K^n \,|\, \forall\, c \in C \ \langle u, c\rangle = 0\}$$

is the dual code to C. A code is called self-dual if $C = C^\perp$ and is called self-orthogonal if $C \subseteq C^\perp$.

Theorem 11.2 *Let C be a $[n, k]$-code over K. Then:*

1. *H is the check matrix for C if and only if H is the generating matrix for $C^\perp$.*
2. *$(E_k \,|\, A)$ is generating matrix for C if and only if $(-A^T \,|\, E_{n-k})$ is generating matrix for $C^\perp$.*

Proof: Let G be a generating matrix for C. Some $(n-k) \times n$ matrix H over K is a check matrix for C if $HG^T = 0$ and the rank of H is $n - k$. For the second statement, observe that:

$$(-A^T \,|\, E_{n-k})(E_k \,|\, A)^T = (-A^T \,|\, E_{n-k})\begin{pmatrix} E_k \\ A^T \end{pmatrix} = -A^T + A^T = 0.$$

□

Theorem 11.3 *Let $GRS_d(a, v)$ be a generalized Reed-Solomon code over the field K with $2 \le d \le n \le q$. Then there is a vector v' such that:*

$$GRS_d(a, v)^\perp = GRS_{n-d+2}(a, v').$$

This v' is determined up to a scalar multiple by the condition $\langle v'\rangle = GRS_n(a, v)$.

If K has characteristic 2, and $d \ge (n + 2)/2$ then there is v such that the code $GRS_d(a, v)$ is self-orthogonal. If moreover n is even and $d = (n + 2)/2$, the code is self-dual.

Proof: Observe first that $\dim GRS_n(a, v) = 1$, because $GRS_d(a, v)$ is a $[n, n-d+1, d]$-code. Take a $0 \ne v' = (v'_1, \dots, v'_n)$ such that:

$$\begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ \vdots & & \vdots \\ a_1^{n-2} & \dots & a_n^{n-2} \end{pmatrix}\begin{pmatrix} v_1 v'_1 \\ \vdots \\ v_n v'_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Suppose that $v'_i = 0$ for some i. We exclude the column i from the matrix and the component i in both vectors. We get a square system of equations with non-singular matrix, so then all $v_j v'_j = 0$, so $v' = 0$, contradiction. It follows that all components of v' are different from 0. For $0 \le r \le d-2$ and $0 \le s \le n - d$ we observe:

$$\sum_{i=1}^{n} a_i^r v_i a_i^s v'_i = \sum_{i=1}^{n} a_i^{r+s} v_i v'_i = 0.$$

This means that $GRS_d(a, v)^\perp \subseteq (GRS_{n-d+2}(a, v')^\perp)^\perp \subseteq GRS_{n-d+2}(a, v')$. But they have both dimension $d - 1$, so the sets are equal.

In order to determine v', we consider the system:

$$\begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ \vdots & & \vdots \\ a_1^{n-2} & \dots & a_n^{n-2} \\ a_1^{n-1} & \dots & a_n^{n-1} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

By Cramer's Rule we get:

$$u_k = (-1)^{n+k} \frac{\prod_{i<j}^{i,j \neq k}(a_j - a_i)}{\prod_{i<j}(a_j - a_i)} = \prod_{i \neq k}(a_k - a_i)^{-1}.$$

We can take $v'_k = u_k / v_k$.

Now, if K has characteristic 2, the Frobenius map $x \rightsquigarrow x^2$ is an automorphism of K so every element in K is a square. So we can choose v_k such that $v_k^2 = u_k$ for all k, and so $v' = v$. Then for $d \geq (n+2)/2$:

$$GRS_d(a,v) \subseteq GRS_{n-d+2}(a,v) = GRS_d(a,v)^\perp,$$

This means that $GRS_d(a,v)$ is self-orthogonal. If n is even and $d = (n+2)/2$, $GRS_d(a,v)$ is self-dual. □

Theorem 11.4 *Let C be a code of dimension ≥ 1.*

C is an MDS-code if and only if $C^\perp$ is an MDS-code.

Proof: As $(C^\perp)^\perp = C$, it is enough to prove only one direction. Suppose that n is the length of C. Suppose there is an element $0 \neq c^\perp \in C^\perp$ with $\mathrm{wt}\,(c^\perp) \leq k$. We can choose $c^\perp$ as row in a generating matrix $G^\perp$ of $C^\perp$. So there are $n-k$ columns in $G^\perp$, which are linear dependent. But $d(C) = n-k+1$, so every $n-k$ columns must be linear independent. This contradiction shows that $d(C^\perp) \geq k+1$. By the singleton bound, we see that:

$$k+1 \leq d(C^\perp) \leq n-(n-k)+1 = k+1,$$

so is $C^\perp$ an MDS-code. □

Definition 11.5 Let $r \in \mathbb{N}$, $r > 1$. A code C is r-divisible if for all $c \in C$, $r \,|\, \mathrm{wt}\,(c)$.

Lemma 11.6 *If C is a self-orthogonal code over $\mathbb{F}_2$ or $\mathbb{F}_3$, then C is 2-divisible, respectively 3-divisible. Moreover, in the first case $(1, \dots, 1) \in C^\perp$.*

Proof: Take some $c = (c_1, \dots, c_n) \in C$. Every $c_i \in \{0,1\}$ for $p = 2$ or in $\{0,-1,1\}$ for $p = 3$. So $c_i^2 = 1$ if $c_i \neq 0$ and

$$0 = \langle c, c \rangle = \mathrm{wt}\,(c) \bmod p.$$

Moreover for $p = 2$ and $v = (1, \dots, 1)$,

$$\langle c, v \rangle = \mathrm{wt}\,(c) = 0,$$

so $v \in C^\perp$. □

Lemma 11.7 *Let C be some binary code.*

1. *If $C \subseteq C^\perp$ and if C has a basis consisting of vectors, whose weights are all divisible by 4, then C is 4-divisible.*

2. If C is 4-divisible, then $C \subseteq C^\perp$.

Proof: Both follow from the remarks that:

$$\langle c, c' \rangle = |\mathrm{supp}\,(c) \cap \mathrm{supp}\,(c')| \bmod 2,$$

$$\mathrm{wt}\,(c + c') = \mathrm{wt}\,(c) + \mathrm{wt}\,(c') - 2|\mathrm{supp}\,(c) \cap \mathrm{supp}\,(c')|.$$

□

12 The Golay codes

The following codes have been defined by Golay in 1949.

Definition 12.1 *Gol*(11) is the ternary code generated by the matrix $G_{11} = (E_6 \,|\, G)$ where:

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

For $C = \mathit{Gol}(11)$ call $\mathit{Gol}(12) = \hat{C}$ its extension.

Theorem 12.2 *$\mathit{Gol}(12)$ is a self-dual $[12, 6, 6]$-code.*

Proof: $\mathit{Gol}(12)$ has length 12 and dimension 6. If we add to G_{11} the column:

$$\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ 0 \end{pmatrix},$$

we get G_{12}, the generating matrix for $\mathit{Gol}(12)$. Let $z_1, \ldots, z_6$ the rows of G_{12}. One verifies that $\langle z_i, z_j \rangle = 0$ for all pairs (i, j), including the cases $i = j$. So $\mathit{Gol}(12) \subseteq \mathit{Gol}(12)^\perp$. But $\dim \mathit{Gol}(12)^\perp = 12 - \dim \mathit{Gol}(12) = 12 - 6 = 6$, $\mathit{Gol}(12) = \mathit{Gol}(12)^\perp$, so the code is self-dual.

We must show now that $d(\mathit{Gol}(12)) = 6$. We observe that $G_{12} = (E_6 \,|\, A_6)$ and that $\tilde{G}_{12} = (-A_6^T \,|\, E_6)$ is also a generating matrix for $\mathit{Gol}(12)$. Being self-orthogonal over $\mathbb{F}_3$, $\mathit{Gol}(12)$ is 3-divisible. Suppose now that there is some $c \in \mathit{Gol}(12)$ with $\mathrm{wt}\,(c) = 3$.

We know that $\mathrm{wt}\,(z_i) = 6$ for all i, so $c \neq z_i$. So is c a linear combination of 2 or 3 different z_i. If it is a linear combination of 2 different z_i, in the last 6 coordinates has c exactly one which is different from 0. If we now look to $\tilde{G}_{12}$, c has to be ± a row of this matrix. But all such rows have weight 6. If it is a linear combination of 3 different z_i, it must have 0 on all last 6 coordinates, and this contradicts again $\tilde{G}_{12}$. As $\mathit{Gol}(12)$ is 3-divisible and all z_i have weight 6, it follows that $d(\mathit{Gol}(12)) = 6$. □

Theorem 12.3 *$\mathit{Gol}(11)$ is a perfect $[11, 6, 5]$-code.*

Proof: It is immediate that the parameter are 11, 6 and 5. To show that it is perfect, compute:

$$3^{11} \geq |\bigcup_{c \in Gol(11)} B_2(c)| = |Gol(11)|\ |B_2(0)| = 3^6 \Big(1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 4\Big) =$$

$$= 3^6(1 + 22 + 220) = 3^6 \cdot 3^5 = 3^{11}.$$

□

Definition 12.4 *Gol*(23) is the binary code generated by the matrix $G_{23} = (E_{12} \,|\, G)$, where the rows of G are all the 11 rotations of the vector:

$$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$$

completed with a last row of ones. The code *Gol*(24) is the corresponding extension. They are the binary Golay code and the extended binary Golay code.

It is a similar job to show that *Gol*(24) is a $[24, 12, 8]$-code self-dual and that *Gol*(23) is a $[23, 12, 7]$ perfect code.

13 Trace and characters

Let $K \leq E$ be an extension of finite fields. Let G be the Galois group of this extension. This is the set of all automorphisms of E that fix K pointwise. We define the mapping Trace $Tr_{E/K} : E \to K$ given as:

$$Tr_{E/K}(a) = \sum_{\gamma \in G} \gamma(a).$$

As the value $Tr_{E/K}(a)$ remains fixed by all the automorphisms $\gamma \in G$, this value belongs to K.

If K has q elements and $[E : K] = n$, it is known that the automorphisms are generated by the Frobenius automorphism $x \rightsquigarrow x^q$ and consequently the trace can be defined by:

$$Tr_{E/K}(a) = a + a^q + a^{q^2} + \dots + a^{q^{n-1}}.$$

Let A be an a finite abelian group. A homomorphism $\chi : A \to \mathbb{C}^\times$ is called character of A. It fulfills the rule $\chi(a + b) = \chi(a)\chi(b)$. If it is constant equal 1, χ is the trivial character. If χ is a character, its complex conjugated values $\bar{\chi}$ define a character as well. As every value of a character is a root of 1, we observe that $\bar{\chi}(a) = \chi(-a)$. With the complex multiplication, the characters build a group $Ch(A)$ which is isomorphic with A.

The connection between trace and characters is the following: Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_p$ the prime field of K. Let $\varepsilon \in \mathbb{C}$ be a complex p-root of 1. V is a finitely dimensional vector space over K and its dual space is $V^* = Hom_K(V, K)$. Then:

$$Ch(V) = \{\chi_f \,|\, f \in V^*\},$$

where we define $\chi_f(v) = \varepsilon^{Tr_{K/F}(f(v))}$ for $v \in V$. Here we identify F with $\{0, 1, \dots, p-1\}$.

Denote with $\mathbb{C}^A$ the set of all functions $f : A \to \mathbb{C}$. On this set we define the Hermitian product:

$$\langle f, g \rangle = \frac{1}{|A|} \sum_{x \in A} f(x)\overline{g(x)}.$$

If A is a finite abelian group, and $\chi, \psi \in Ch(A)$, then:

$$\langle \chi, \psi \rangle = \begin{cases} 1, & \chi = \psi, \\ 0, & \chi \neq \psi. \end{cases}$$

In particular, the set $Ch(A)$ is an orthonormal basis of $\mathbb{C}^A$ for the Hermitian product.

14 Weight polynomial

Definition 14.1 Let C be a code of length n. Let A_i be the number of code-words of weight i in C. The polynomial:

$$A_C(z) = \sum_{i=0}^{n} A_i z^i \in \mathbb{Z}[z]$$

the weight polynomial of C.

The following duality theorem belongs to MacWilliams:

Theorem 14.2 *Let C be an $[n,k]$-code over $K = \mathbb{F}_q$ with the weight polynomial $A(z)$, and let $A^{\perp}(z)$ be the weight polynomial of $C^{\perp}$, then:*

$$A^{\perp}(z) = q^{-k}(1+(q-1)z)^n A\Big(\frac{1-z}{1+(q-1)z}\Big).$$

Proof: Let χ be a non-trivial character of the additive group of K, this means a non-constant homomorphism $\chi : (K,+,0) \to (\mathbb{C}^{\times}, \cdot, 1)$. For $u \in K^n$ we define:

$$g_u(z) = \sum_{v \in K^n} \chi(\langle u, v\rangle) z^{\mathrm{wt}\,(v)} \in \mathbb{C}[z].$$

We observe that:

$$\sum_{c \in C} g_c(z) = \sum_{c\in C}\sum_{v \in K^n} \chi(\langle c, v\rangle) z^{\mathrm{wt}\,(v)} = \sum_{v \in K^n} f(v) z^{\mathrm{wt}\,(v)},$$

where $f(v) = \sum_{c \in C} \chi(\langle c, v\rangle)$. The mapping $c \rightsquigarrow \chi(\langle c, v\rangle)$ is a character χ_v of C which is trivial 1_C for $v \in C^{\perp}$. The orthogonality relations for characters implies now:

$$f(v) = \sum_{c \in C} \chi(\langle c, v\rangle) = |C|\langle \chi_v, 1_C\rangle = \begin{cases} |C|, & v \in C^{\perp}, \\ 0, & v \notin C^{\perp}. \end{cases}$$

So:

$$\sum_{c \in C} g_c(z) = \sum_{c^{\perp} \in C^{\perp}} |C| z^{\mathrm{wt}\,(c^{\perp})} = |C| A^{\perp}(z).$$

Now we compute the left side in a different way. For $c = (c_1, \dots, c_n) \in C$ one has:

$$\begin{aligned} g_c(z) &= \sum_{v \in K^n} z^{\mathrm{wt}\,(v)} \chi(\langle c, v\rangle) \\ &= \sum_{(a_1,\dots,a_n)\in K^n} z^{\sum_{i=1}^n \mathrm{wt}\,(a_i)} \chi\Big(\sum_{i=1}^n c_i a_i\Big) \\ &= \sum_{(a_1,\dots,a_n)\in K^n} \prod_{i=1}^n z^{\mathrm{wt}\,(a_i)} \chi(c_i a_i) \\ &= \prod_{i=1}^n \sum_{a_i \in K} z^{\mathrm{wt}\,(a_i)} \chi(c_i a_i). \end{aligned}$$

But as $\chi \neq 1$ is $\sum_{a \in K^{\times}} \chi(a) = -1$, so:

$$\sum_{a_i \in K} z^{\mathrm{wt}\,(a_i)} \chi(c_i a_i) = \begin{cases} \sum_{a_i \in K} z^{\mathrm{wt}\,(a_i)} = 1 + (q-1)z & c_i = 0, \\ 1 + z\sum_{a \in K^{\times}} \chi(a) = 1 - z & c_i \neq 0. \end{cases}$$

This means that:

$$g_c(z) = (1-z)^{\mathrm{wt}\,(c)}(1+(q-1)z)^{n-\mathrm{wt}\,(c)}.$$

We can finally conclude:

$$\begin{aligned} A^{\perp}(z) &= |C|^{-1}\sum_{c\in C} g_c(z) \\ &= q^{-k}(1+(q-1)z)^n \sum_{c\in C}\Big(\frac{1-z}{1+(q-1)z}\Big)^{\mathrm{wt}\,(c)} \\ &= q^{-k}(1+(q-1)z)^n A\Big(\frac{1-z}{1+(q-1)z}\Big). \end{aligned}$$

□

In this context we recall that $Sim_q(k) = Ham_q(k)^{\perp}$ and that we already implicitly shown that the Simplex code has the following weight polynomial:

$$A(z) = 1 + (q^k - 1)z^{q^{k-1}}.$$

So using the theorem, one can compute the weight polynomial of the Hammimg code as well.

15 Theorem of Prange

Theorem 15.1 *A binary code C has the weight polynomial $A(z) = \sum_{i=0}^{n} A_i z^i$ and its extension $\hat{C}$ has the weight polynomial $\hat{A} = \sum_{i=0}^{n} \hat{A}_i z^i$. Suppose that $Per(\hat{C})$ is transitive. Then:*

$$A_{2i-1} = \frac{2iA_{2i}}{n+1-2i} = \frac{2i\hat{A}_{2i}}{n+1}$$

for $1 \le i \le \frac{n+1}{2}$. In particular, the minimal weight of C is odd.

Proof: It is easy to see that $\hat{A}_{2i} = A_{2i} + A_{2i-1}$ and $\hat{A}_{2i-1} = 0$. In $\hat{C}$ exactly A_{2i-1} many codewords of weight A_{2i} have the digit 1 in the last coordinate. This is true for all other coordinates, because $Per(\hat{C})$ is transitive over the set $\{1, \dots, n+1\}$.

$$\sum_{\mathrm{wt}\,(\hat{c})=2i} \mathrm{wt}\,(\hat{c}) = 2i\hat{A}_{2i}.$$

This implies:

$$A_{2i-1} = \frac{2i\hat{A}_{2i}}{n+1},$$

and because $\hat{A}_{2i} = A_{2i} + A_{2i-1}$,

$$A_{2i-1} = \frac{2iA_{2i}}{n+1-2i}.$$

16 Equivalence of codes

Let K be a finite field and $V \le K^n$. The projection $f_i(v) = v_i$ is a linear function over V, so $f_i \in V^*$. The prime field of K is $F = \mathbb{F}_p = \{0, 1, \dots, p-1\}$ and $\varepsilon \ne 1$ a complex p-root of 1. We recall that every $f \in V^*$ determines a character χ_f of V over:

$$\chi_f(v) = \varepsilon^{Tr_{K/F} f(v)}$$

Lemma 16.1 *For all $v \in V$,*

$$(n - \mathrm{wt}\,(v))|K| = \sum_{i=1}^{n} \sum_{a \in K} \chi_{af_i}(v).$$

Proof: If $f_i(v) = 0$ then $\chi_{af_i}(v) = 1$ and $\sum_{a\in K} \chi_{af_i}(v) = |K|$.
If $f_i(v) \neq 0$, recall that $Tr : K \to F$ is surjective, so there is a decomposition:

$$K = \bigcup_{i=0}^{p-1} (a_i + Kern\ Tr),$$

with $Tr(a_i) = i$.

$$\sum_{a\in K} \chi_{af_i}(v) = \sum_{a\in K} \varepsilon^{Tr(af_i(v))} = \sum_{a\in K} \varepsilon^{Tr(a)} = |Kern\ Tr| \sum_{i=0}^{p-1} \varepsilon^i = 0.$$

□

The following theorem was discovered by MacWilliams. The proof is from Ward and Wood.

Theorem 16.2 *Let C and C' two linear codes of dimension k in K^n. Then $C \simeq C'$ if and only if there is weight preserving K-linear isomorphism of vector spaces $\varphi : C \to C'$.*

Proof: If $C \simeq C'$ then every isometry is in particular a weight preserving isomorphism from C to C'. Now consider a linear isomorphism $\varphi : C \to C'$ with $\mathrm{wt}\,\varphi(c) = \mathrm{wt}\,c$ for all $c \in C$. We consider the projections $f_i(c) = c_i$ and $f_i'(c) = (\varphi(c))_i$. Both $f_i, f_i' \in C^*$. We apply the Lemma and we find out that for all $c \in C$ one has:

$$\sum_{i=1}^{n} \sum_{a\in K} \chi_{af_i}(c) = (n - \mathrm{wt}\,(c))|K| =$$

$$= (n - \mathrm{wt}\,(\varphi(c)))|K| = \sum_{j=1}^{n} \sum_{b\in K} \chi_{bf_j'}(c).$$

In conclusion the following functions are identic:

$$\sum_{i=1}^{n} \sum_{a\in K} \chi_{af_i} = \sum_{j=1}^{n} \sum_{b\in K} \chi_{bf_j'} \in \mathbb{C}^C.$$

As $\chi_0 = 1$ we can reduce this to:

$$\sum_{i=1}^{n} \sum_{a\in K^\times} \chi_{af_i} = \sum_{j=1}^{n} \sum_{b\in K^\times} \chi_{bf_j'}.$$

Recall now that the characters of C build a basis of $\mathbb{C}^C$, there is a $\sigma(1) \in \{1, \dots .n\}$ and a $a_1 \in K^\times$ such that $\chi_{a_1 f_{\sigma(1)}} = \chi_{f_1'}$. This implies $a_1 f_{\sigma(1)} = f_1'$. Then one has that:

$$\sum_{a\in K^\times} \chi_{af_{\sigma(1)}} = \sum_{b\in K^\times} \chi_{bf_1'},$$

$$\sum_{i\neq\sigma(1)} \sum_{a\in K^\times} \chi_{af_i} = \sum_{j=2}^{n} \sum_{b\in K^\times} \chi_{bf_j'}.$$

Inductively we find a permutation $\sigma \in S_n$ and elements $a_i \in K^*$ such that $a_i f_{\sigma(i)} = f'_i$ for $i = 1, \dots, n$.

$$(f_1(c), \dots, f_n(c)) Diag(a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)}) P(\sigma) = (a_1 f_{\sigma(1)}(c), \dots, a_n f_{\sigma(n)}(c))$$
$$= (f'_1(c), \dots, f'_n(c)).$$

Theorem 16.3 *Both the Hamming code $Ham_q(k)$ and the simplex code $Sim_q(k)$ have the group of automorphisms isomorphic with $GL(k, q)$.*

Proof: It is clear that $Aut\ Ham_q(k) \simeq Aut\ Sim_q(k)$ because the codes are dual. Let $C = Sim_q(k) \leq K^n$ with $|K| = q$ and $n = (q^k - 1)/(q - 1)$. Every $\varphi \in GL(C)$ is weight preserving because all $0 \neq c \in C$ have the same weight. MacWilliams' Theorem shows that φ can be extended to a monomial application of K^n. So $GL(C)$ is a subgroup of $Aut(C)$. We need to show that the homomorphism of natural restriction $Aut(C) \to GL(C)$ corresponding to the restriction of some C-preserving automorphism of K^n to C, is injective. Let $M = Diag(a_1, \dots, a_n)P(\pi)$ a monomial isometry of K^n, such that $M|C$ is the identity. Suppose that for some i, $\pi(i) \neq i$. But the columns of the generating matrix of C are linear independent over K, so there exists $c \in C$ with $c_i \neq a_{\pi(i)} c_{\pi(i)}$. But:

$$c = (c_1, c_2, \dots, c_n) = (c_1, c_2, \dots, c_n)M = (a_{\pi(1)} c_{\pi(1)}, \dots, a_{\pi(n)} c_{\pi(n)}),$$

so $c_i = a_{\pi(i)} c_{\pi(i)}$, which is a contradiction. So M was a diagonal matrix, and this has to be the identity. □

The linearity is an important hypothesis in the Theorem of Ward and Wood. One knows examples of codes with the same cardinality and the same distribution of weights, which are not equivalent.

17 Subfield codes

In this section $K = \mathbb{F}_q \leq E = \mathbb{F}_{q^m}$, so $m = [E : K]$. The Galois group G of E over K is generated by the Frobenius automorphism $x \rightsquigarrow x^q$. The action of G on E can be extended over E^n by:

$$\tau(x_1, \dots, x_n) = (\tau x_1, \dots, \tau x_n).$$

Similarly one can extend the action of the trace function $Tr = Tr_{E/K}$ to tuples, as:

$$Tr(x_1, \dots, x_n) = (Tr(x_1), \dots, Tr(x_n)).$$

Definition 17.1 Let C be a linear E-vector subspace of E^n. The code $C|K = C \cap K^n$ is called subfield code of C. The set $Tr(C) \leq K^n$ is the trace code of C.

It is clear that $C|K$ consists of all elements in C which are let invariant by the Frobenius automorphism of E^n.

Theorem 17.2 *Hamming codes are subfield codes of GRS codes. If $\gcd(m, q-1) = 1$, the Hamming code $Ham_q(m)$ is equivalent to a cyclic code. In particular, every binary Hamming code is equivalent to a cyclic code.*

Proof: Let $n = (q^m - 1)/(q - 1)$. Let $h_j = (h_{1j}, \dots, h_{mj})^T$ the column j of a check matrix of $Ham_q(m)$. Consider a K-basis $u_1, \dots, u_m$ of E over K and $v_j = \sum_{i=1}^m h_{ij} u_i \in E$. Let $v = (v_1, \dots, v_n) \in E^m$. Then $Ham_q(m) = v^\perp | K$. But as $v^\perp = GRS_2(*, v)$, Hamming codes are subfield codes of generalized Reed-Solomon codes.

Now consider the case $\gcd(m, q-1) = 1$. But then:

$$n = \frac{q^m - 1}{q - 1} = q^{m-1} + \cdots + q + 1 =$$

$$= (q-1)[q^{m-2} + 2q^{m-3} + \cdots + (m-2)q + (m-1)] + m,$$

so it follows $\gcd(n, q-1) = 1$. Let α be a primitive n-root of 1 in E. We can choose $v = (1, \alpha, \dots, \alpha^{n-1})$ because $\alpha^i \notin K$ for $i = 1, \dots, n-1$. Indeed, if $\alpha^i = a \in K$, then $\alpha^{i(q-1)} = 1$, which is in contradiction with $\mathrm{ord}(\alpha^{q-1}) = \mathrm{ord}(\alpha)/\gcd(n, q-1) = \mathrm{ord}(\alpha) = n$. So $\langle v \rangle$ is cyclic, and $\langle v \rangle^{\perp} | K$ is cyclic. □

The following theorem was discovered by Delsarte:

Theorem 17.3 *If C is a code of length n over E, then:*

$$(C|K)^{\perp} = Tr(C^{\perp}).$$

Proof: We show first that $(C|K)^{\perp} \subseteq Tr(C^{\perp})$, or equivalent that $(Tr(C^{\perp}))^{\perp} \subseteq C|K$. Take $x = (x_1, \dots, x_n) \in (Tr(C^{\perp}))^{\perp}$ and $y = (y_1, \dots, y_n) \in C^{\perp}$. For every $a \in E$, because $x \in K^n$, one has:

$$0 = \langle x, Tr(ay) \rangle = \sum_{i=1}^{n} x_i Tr(ay_i) = Tr(a\langle x, y \rangle).$$

So $\langle x, y \rangle = 0$ and $x \in C^{\perp\perp} = C$, but also $x \in K^n$, so $x \in C|K$.

For the other inclusion, we must show that if $y \in C^{\perp}$ and $c \in C|K$, then $\langle c, Tr(y) \rangle = 0$. Recall that Tr is K-linear.

$$\langle c, Tr(y) \rangle = \sum_{i=1}^{n} c_i Tr(y_i) = \sum_{i=1}^{n} Tr(c_i y_i) =$$

$$= Tr\Big(\sum_{i=1}^{n} c_i y_i \Big) = Tr(\langle c, y \rangle) = Tr(0) = 0.$$

□

Part IV

Cyclic codes

18 Codes as ideals

Instead of subset of K^n, we can see a code also as subset of $R = \{f \mid f \in K[x], \deg f < n\}$. The advantage is that now we have a new operation defined by:

$$f \circ g = (fg) \bmod (x^n - 1).$$

We see that $(R, +, \circ, 0, 1)$ is a ring.

Theorem 18.1 *A code $C \leq R$ is cyclic if and only if C is an ideal in the ring R.*

Proof: This follows immediately from the observation that if $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in C$ then:

$$c(x) \circ x = c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1}.$$

□

Theorem 18.2 *If $C \leq R$ is a cyclic $[n, k]$-code, then:*

1. *There is a uniquely determined monic polynomial $g \in K[x]$ with $\deg g = n - k$ such that $g \mid x^n - 1$ and $C = g \circ R$.*
2. *$\{gx^j \mid j = 0, 1, \dots, k-1\}$ is a K-basis of C.*

Proof: Every ideal in $K[x]$ is a principal ideal and is generated by a polynomial of lest degree, contained inside. This property is heired by the factor algebra $K[x]/(x^n - 1)K[x]$. So $C = g \circ R$. If we choose g monic, then is g uniquely determined. But $x^n - 1 = gh + r$ with $\deg r < \deg g$ and because $-r = g \circ h \in C$ it follows that $r = 0$, so $g \mid x^n - 1$. Also:

$$\deg g = \dim K[x]/gK[x] = \dim R/C = \dim R - \dim C = n - k.$$

□

Definition 18.3 If $C \leq R$ is a cyclic code, the polynomial g given by the theorem above is called generating polynomial of C. The polynomial

$$h = \frac{x^n - 1}{g}$$

is called check polynomial of C.

Lemma 18.4 *Let $C \leq R$ be a cyclic $[n, k]$-code. Further let $g = g_0 + \cdots + g_{n-k} x^{n-k}$ its generating polynomial and $h = h_0 + \cdots + h_k x^k$ the check polynomial of C. Then is:*

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & \dots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ 0 & 0 & \dots & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix} \in \mathcal{M}_{k \times n}(K)$$

a generating matrix of C, and

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & h_0 \end{pmatrix} \in \mathcal{M}_{(n-k) \times n}(K)$$

a check matrix of C.

Proof: G is of course a generating matrix for C. The equality:

$$x^n - 1 = gh = \sum_{i=0}^{n} \Big(\sum_{j=0}^{n-k} g_j h_{i-j} \Big) x^i,$$

implies that:

$$\sum_{j=0}^{n-k} g_j h_{i-j} = 0$$

for all $i = 1, \dots, n-1$, which is equivalent with $GH^T = 0$. Also, from $gh = x^n - 1$ follows $g_0 h_0 = -1$, so $h_0 \neq 0$. So H has rank equal $n-k$ and is check matrix for C. □

Definition 18.5 For $f \in K[x]$ of degree n we define its dual polynomial:

$$f^*(x) = x^n f\Big(\frac{1}{x}\Big).$$

Corollary 18.6 *Let C be a cyclic code of dimension k with generating polynomial g and check polynomial h. Then is $g^\perp = h(0)^{-1}h^*$ the generating polynomial of $C^\perp$. Moreover, $C^\perp$ is equivalent to the code generated by h.*

Using the Theorem of Delsarte, if the caracteristic of $K = \mathbb{F}_q$ does not divide the length of the code, cyclic codes are trace codes. In this case there is an extension of K such that $x^n - 1 = \prod(x - \alpha^i)$ where α is a primitive n-root of 1. The polynomials $g \in K[x]$ such that $g \,|\, (x^n - 1)$ correspond uniquely to sets:

$$\mathcal{R}(g) = \{i \,|\, i \in \mathbb{Z}_n, g(\alpha^i) = 0\}.$$

where $\mathcal{R}(g)$ is closed under the mapping $i \rightsquigarrow iq \bmod n$. If g is the generating polynomial of a cyclic code C of length n over K,

$$C = \{(c_0, \dots, c_{n-1}) \,|\, c_i \in K, \forall\, j \in \mathcal{R}(g) \ \sum_{i=0}^{n-1} c_i \alpha^{ij} = 0\}.$$

Theorem 18.7 *If K is a finite field, its characteristic does not divide n, α is a primitive n-root of 1 in some extension $E \geq K$ and $h \in K[x]$ with $h \,|\, (x^n - 1)$, the following statements are equivalent:*

1. *$C \leq K^n$ is cyclic with check polynomial h.*
2. *$C = Tr_{E/K}(D)$ where D is the vector space generated by the vectors $v_j = (1, \alpha^j, \dots, \alpha^{j(n-1)})$ over E and $j \in \mathcal{R}(h^*)$.*

Proof: h is the check polynomial of C if and only if h^* is the generating polynomial of $C^\perp$, so

$$C^\perp = \{(c_0, \dots, c_{n-1}) \,|\, c_i \in K, \forall\, j \in \mathcal{R}(h^*) \ \sum_{i=0}^{n-1} c_i \alpha^{ij} = 0\}.$$

With the definition of D, $C^\perp = D^\perp \,|\, K$, and the Theorem of Delsarte implies:

$$C = (D^\perp \,|\, K)^\perp = Tr_{E/K}(D).$$

□

Application: Let C be a cyclic $[n, k]$-code with generating polynomial g. Consider a message $m \in R_{k,K}$. To encode this message, one builds the code-word:

$$c(x) = x^{n-k} m(x) - [x^{n-k} m(x) \bmod g] \in C \leq R_{n,K}.$$

For error detection, one checks if the received message $v(x)$ is divisible by g. If yes, we can read directly $x^{n-k}m(x)$ in $v(x)$, because $v(x) = x^{n-k}m(x) + b(x)$ where $\deg b(x) < n - k$. If there is an error, one ask for the repetition of the message. This is the principle of the CRC-codes, cyclic redundancy check codes. □

This error recognition is even faster if the code is generated by an idempotent element e, that is an element such that $e^2 = e$. Such elements decompose the ring as:

$$R = eR \oplus (1 - e)R.$$

Indeed, from $r = er + (1 - e)r$ one has $R = eR + (1 - e)R$. But multiplication with e produces the identity on eR and the zero function on $(1 - e)R$, so $eR \cap (1 - e)R = 0$ and the sum is direct.

If a code is generated by an idempotent element e, then $v \neq ev$ means that an error occurred during the transmission.

Theorem 18.8 *Suppose that K is a field of characteristic p and that $p \not| n$. Let $C \leq R = R_{n,K}$ be a cyclic code. Then there is a uniquely determined $e \in K[x]$ with $\deg e < n$ such that $C = e \circ R$ and $e \circ e = e$. We call e the idempotent of C.*

Proof: Let g be the generating polynomial of C and h the check polynomial of C. One can prove that $\gcd(p, n) = 1$ implies that $\gcd(g, h) = 1$. So there are $a, b \in K[x]$ such that $ga + hb = 1$. Define $e = g \circ a = 1 - h \circ b \in C$. For $c = g \circ f \in C$ one has:

$$e \circ c = (1 - h \circ b) \circ (g \circ f) = g \circ f - h \circ b \circ g \circ f = g \circ f = c.$$

This shows also that $e \circ e = e$ and that $C = e \circ R$. If also $C = e' \circ R$ with $e' \circ e' = e'$ then $e' = e' \circ e = e$ because both multiplications with e and with e' are identities. □

We can take:

$$e = \frac{x \circ g \circ h'}{n},$$

where h' is the differentiation of h. This can be seen by derivating the identity $x^n - 1 = gh$.

Theorem 18.9 *Let the characteristic of K does not divide n and let $C \leq R = R_{n,K}$ be a cyclic code with generating polynomial g. Further α is a primitive n-root of 1 over K and $e \in K[x]$ with $\deg e < n$ and $e = e \circ e$.*

The element e is the idempotent of C if and only if e and g have the same roots in the multiplicative group generated by α.

Proof: As the characteristic of K does not divide n, all roots of g have multiplicity 1 and are contained in $\langle\alpha\rangle$. Now $e \circ R = g \circ R$ if and only if $e = g \circ a$ and $g = e \circ b$ for $a, b \in K[x]$. So g and e have the same roots in $\langle\alpha\rangle$. On the other side, if g and e have the same roots in $\langle\alpha\rangle$, then $\gcd(e, x^n - 1) = g$. This implies $eK[x] + (x^n - 1)K[x] = gK[x]$, so $e \circ R = g \circ R$. □

19 BCH codes

The following result was discovered by Hocquenghem in 1959 and independently by Bose and Ray-Chaudhuri in 1960 in the binary case. It is called BCH-bound.

Theorem 19.1 *Let K be a finite field and let α be a primitive n-root of 1 over K. Further $l \in \mathbb{N} \setminus \{0\}$, $2 \leq d \leq n$ and $r \in \mathbb{N}$ with $\gcd(n, r) = 1$. If the elements:*

$$\alpha^l, \alpha^{l+r}, \ldots, \alpha^{l+(d-2)r}$$

are roots for the generating polynomial of a cyclic code C of length n over K, then C has the minimal weight $d(C) \geq d$.

Proof: We define $a = (1, \alpha^r, \dots, \alpha^{(n-1)r})$ and $v = (1, \alpha^l, \dots, \alpha^{l(n-1)})$. As $\gcd(n, r) = 1$, α^r is itself a primitive n-root of 1. We observe that $C \leq GRS_d(a, v)|K$. The bound is true because $d(GRS_d(a, v)) = d$. □

Definition 19.2 Let $GRS_d(a, v)$ be the generalized Reed-Solomon code with $a = (1, \alpha, \dots, \alpha^{n-1})$ and $v = (1, \alpha^l, \dots, \alpha^{l(n-1)})$, where α is a primitive n-root of 1 over $K = \mathbb{F}_q$ and $l \geq 1$. The existence of α is equivalent with $\gcd(q, n) = 1$. The subfield code $C = GRS_d(a, v)|K$ is called BCH-code of designed distance d. A BCH-code C with $n = q^m - 1$ is called primitive. If moreover $l = 1$, C is a classic BCH-code (in narrow sense). All BCH-codes are cyclic.

Theorem 19.3 *The generating polynomial of a BCH-code with designated distance d is:*

$$g = \operatorname{lcm}(m_{\alpha^i} \,|\, i = l, \dots, l + d - 2)$$

where m_a is the minimal polynomial of a over K, and its minimal distance is ≥ 2.

Proof: This polynomial is the polynomial of smallest degree with the given roots. The statement about the minimal distance is just the BCH bound. □

Example 19.4 A Reed-Solomon code C over $K = \mathbb{F}_q$ with minimal distance d has the generating polynomial

$$g = \prod_{i=1}^{d-1} (x - \alpha^i),$$

where α generates the multiplicative group of K. So the check polynomial of C is:

$$h = \prod_{j=d}^{q-1} (x - \alpha^i).$$

The dual check polynomial h^* has the roots:

$$\{\alpha^{-d}, \alpha^{-(d+1)}, \dots, \alpha^{-(q-1)}\} = \{\alpha^{q-1-d}, \alpha^{q-2-d}, \dots, 1\}.$$

Using the Theorem of Delsarte applied for cyclic codes, we get:

$$C = \{(f(1), f(\alpha), \dots, f(\alpha^{q-2})) \,|\, f \in K[x], \deg(f) = q - 1 - d\}.$$

Example 19.5 $K = \mathbb{F}_q$ and $\gcd(k, q - 1) = 1$. The Hamming code $Ham_q(k) \simeq GRS_2(*, v)|K = v^\perp|K$ with $v = (1, \alpha, \dots, \alpha^{n-1})$. So in this case the Hamming code is a BCH-code. The generating polynomial is the minimal polynomial m_α of α. The minimal distance is ≥ 3 because for each root α of m_α, α^q is a root as well. Also, n and $q - 1$ are relatively prime.

Definition 19.6 For $A \in GL(V)$ and $w \in V$ we define the mapping $(A, w) : V \to V$ as:

$$(A, w)(v) = Av + w.$$

The affine linear group of V is:

$$AGL(V) = \{(A, w) \,|\, A \in GL(V), w \in V\}.$$

Theorem 19.7 *Let $\hat{C}$ be the extension of a primitive classical BCH-code C of length $n = q^m - 1$ over $K = \mathbb{F}_q$. Then $AGL(1, E) \leq Per(\hat{C})$. In particular, $Per(\hat{C})$ is 2-transitive.*

Proof: Let α be a primitive n-root of 1 in $E = \mathbb{F}_{q^m} \geq K$. We identify the indexes $0, 1, \dots n$ used to denote positions in a vector $v \in K^{n+1}$ with elements of E, as we identify i with α^i for $i \neq n$ and we identify n with $0 \in E$. If $AGL(1, E) = \{(a, b) \mid a \in E^{\times}, b \in E\}$, this group operates over K^{n+1} as follows:

$$(c_0, \dots, c_n)(a, b) = (c_{(a,b)^{-1}(0)}, \dots, c_{(a,b)^{-1}(n)}).$$

For $(c_0, \dots, c_n) \in \hat{C}$, $(c_0, \dots, c_n)(\alpha, 0) = (c_{n-1}, c_0, \dots, c_{n-3}, c_{n-2}, c_n) \in \hat{C}$, as C is cyclic. So $\hat{C}$ is invariant for the group $\{(a, 0) \mid a \in E^{\times}\}$. But $(a, b) = (a, 0)(1, a^{-1}b)$ and $(1, u) = (u, 0)(1, 1)(u^{-1}, 0)$, we must show only that $(1, 1) \in Per(\hat{C})$. If d is the designed distance of the BCH-code C, for $1 \leq j \leq d - 1$ we have:

$$\sum_{i=0}^{n-1} c_{(1,1)^{-1}(i)}\alpha^{ij} = \sum_{i=0}^{n-1} c_{(1,-1)(i)}\alpha^{ij} = \sum_{i=0,\, \alpha^i \neq -1}^{n-1} c_i(\alpha^i + 1)^j + c_n =$$

$$= \sum_{i=0}^{n-1} c_i(\alpha^i + 1)^j + c_n = \sum_{i=0}^{n-1} c_i \sum_{r=0}^{j} \binom{j}{r} \alpha^{ir} + c_n =$$

$$= \sum_{r=0}^{j} \binom{j}{r} \sum_{i=0}^{n-1} c_i\alpha^{ir} + c_n = \sum_{i=0}^{n} c_i = 0,$$

where we use the fact that $(c_0, \dots, c_{n-1}) \in C$, so for $1 \leq r \leq j \leq d - 1$,

$$\sum_{i=0}^{n-1} c_i\alpha^{ir} = 0.$$

So $\hat{C}$ is invariant for $(1, 1)$. It follows that $ACL(1, q^m) \leq Per(\hat{C})$. But it is known that $ACL(1, E)$ operates 2-transitively on E (exercise!), so $Per(\hat{C})$ operates 2-transitively on $\{0, \dots, n\}$. □

Corollary 19.8 *Using the Theorem of Prange, it follows that the minimal distance of binary primitive classic BCH-codes is always an odd number.*

In the following examples, $K = \mathbb{F}_2$ and C is a primitive classic BCH-code of designed distance d.

Example 19.9 Take $n = 2^5 - 1 = 31$ and $d = 7$. C has the generating polynomial:

$$g = \text{lcm}\{m_{\alpha^i} \mid i = 1, \dots, 6\} = m_{\alpha} m_{\alpha^3} m_{\alpha^5},$$

where $i \not|\, 31$ implies $\text{ord}(\alpha^i) = 31$. So $\deg m_{\alpha^i} = 5$ for $i = 1, 3, 5$ and C is a $[31, 16]$-code with minimal distance $d(C) \geq d = 7$. If we suppose that $d(C) \geq 8$, it follows by the previous corollary that $d(C) \geq 9$, because it has to be an odd number. By the Hamming bound,

$$32768 = 2^{31-16} \geq \sum_{i=0}^{4} \binom{31}{i} = 36457,$$

which is a contradiction. So C is a $[31, 16, 7]$-code. □

Example 19.10 Take $n = 2^5 - 1 = 31$ and $d = 8$. Now the generating polynomial g has degree 20 because also m_{α^7} divides g. So C is a $[31, 11]$-code with $d(C) \geq d = 8$. Because $g(\alpha^j) = 0$ for $j = 1, 2, \dots, 10$, we get with the BCH-bound $d(C) \geq 11$. If $d(C) \geq 12$, as $d(C)$ must be odd, we get $d(C) \geq 13$. Using the Griesmer bound,

$$31 = n \geq \sum_{i=0}^{10} \left\lceil \frac{d}{2^i} \right\rceil = 33,$$

contradiction. So C is a $[31, 11, 11]$-code. □

20 Newton's Equations

For a very special kind of primitive classic BCH-codes, the minimal distance proves to be the same as the designed distance. But in order to prove this, we must shortly develop some theory about symmetric polynomials. Recall that the elementary symmetric functions $s_j = s_j(x_1, \dots, x_m)$ for $j = 0, \dots, m$ are defined as follows:

$$\begin{aligned} s_0 &= 1, \\ s_1 &= x_1 + \dots + x_m, \\ s_2 &= \sum_{i<j} x_i x_j, \\ \vdots & \quad \vdots \\ s_m &= x_1 \dots x_m. \end{aligned}$$

We define also another family of symmetric polynomials:

$$p_r = p_r(x_1, \dots, x_m) = \sum_{i=1}^{m} x_i^r.$$

The next result goes back to Isaac Newton:

Theorem 20.1 *The following identities hold for* $1 \leq r \leq m-2$*:*

$$\sum_{j=0}^{r-1} (-1)^j s_j p_{r-j} + (-1)^r r s_r = 0.$$

The following identities hold for $r \geq m-1$*:*

$$\sum_{j=0}^{m} (-1)^j s_j p_{r-j} = 0.$$

Proof: We consider the following polynomial:

$$\sigma(x) = \prod_{i=1}^{m} (1 - x_i x) = \sum_{j=0}^{m} (-1)^j s_j x^j \in K[x_1, \dots, x_m][x].$$

We apply the differentiation $\partial/\partial x$ and we develop the result as a sum of power series:

$$\sum_{j=0}^{m} (-1)^j j s_j x^{j-1} = \sigma'(x) = -\sum_{j=1}^{m} x_j \prod_{i \neq j} (1 - x_i x) =$$

$$= -\sum_{j=1}^{m} x_j \frac{\sigma(x)}{1 - x_j x} = -\sigma(x) \sum_{j=1}^{m} x_j \sum_{k=0}^{\infty} (x_j x)^k = -\sigma(x) \sum_{k=0}^{\infty} p_{k+1} x^k.$$

If one compares the coefficients of x in the first and in the last expression, one finds Newton's identities. □

Lemma 20.2 *If* $K = \mathbb{F}_q \leq E = \mathbb{F}_{q^n}$ *and* $u_0, \dots, u_h \in E$ *linear independent over* K*, the matrix:*

$$A = \begin{pmatrix} u_0 & \dots & u_h \\ u_0^q & \dots & u_h^q \\ \vdots & & \vdots \\ u_0^{q^h} & \dots & u_h^{q^h} \end{pmatrix}$$

is regular.

Proof: Of course $h+1 \leq n$. Is $E = \langle a \rangle$, then $1 = a^0, a, \dots, a^h$ are linear independent over K. So there is a regular matrix $B \in \mathcal{M}_{(h+1)\times(h+1)}(K)$ such that:

$$(u_0, \dots, u_h)B = (1, a, \dots, a^h).$$

If we apply different powers of the Frobenius automorphism, we find that for all $i \in \mathbb{N}$, $(u_0^{q^i}, \dots, u_h^{q^i})B = (1, a^{q^i}, \dots, a^{hq^i})$. All together:

$$AB = \begin{pmatrix} 1 & a & a^2 & \dots & a^h \\ 1 & a^q & a^{2q} & \dots & a^{hq} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a^{q^h} & a^{2q^h} & \dots & a^{hq^h} \end{pmatrix}.$$

This matrix is regular, being a Vandermonde matrix, so A is regular as well. □

Theorem 20.3 *Let $K = \mathbb{F}_q \leq E = \mathbb{F}_{q^n}$ and U a K-linear subspace of E, of dimension h. Then:*

$$\prod_{u \in U} (x-u) = x^{q^h} + a_{h-1}x^{q^{h-1}} + \dots + a_0 x \in E[x].$$

Proof: Fix a K-basis of U: $u_0, u_1, \dots, u_{h-1}$. The following system of linear equations:

$$(x_0, x_1, \dots, x_{h-1}) \begin{pmatrix} u_0 & \dots & u_h \\ u_0^q & \dots & u_h^q \\ \vdots & & \vdots \\ u_0^{q^h} & \dots & u_h^{q^h} \end{pmatrix} = -(u_0^{q^h}, u_1^{q^h}, \dots, u_{h-1}^{q^h})$$

has a unique solution $(a_0, \dots, a_{h-1}) \in E^h$. Consequently for $i = 0, \dots, h-1$ one has:

$$u_i^{q^h} + \sum_{j=0}^{h-1} a_j u_i^{q^j} = 0.$$

But the elements u_i build a basis of U and raising to the power q is the identity on $K = \mathbb{F}_q$, so it follows:

$$u^{q^h} + \sum_{j=0}^{h-1} a_j u^{q^j} = 0$$

for all $u \in U$. On the other hand, all elements $u \in U$ solve this equation and the equation $\prod_{u \in U}(x-u)$. As they have the same degree, are both monic and have the same solution, both polynomials must be equal. □

Theorem 20.4 *Let $K = \mathbb{F}_q$ and let C be a primitive classical BCH-code over K with designed distance $d = q^h - 1$. Then $d(C) = d$.*

Proof: Let $n = q^m - 1$ be the length of C and $E = \mathbb{F}_{q^m} \geq K = \mathbb{F}_q$. Further let U be a K-linear subspace of E of dimension h. As the minimal distance is always $\geq d$, it is enough to find an element of weight $d = q^h - 1$. In order to show this, we use the following identities:

$$\sum_{u \in U} u^r \quad = \quad 0 \qquad (1)$$

for $r = 1, 2, \dots, d-1$, that will be proven afterwards.

The code-words from C are indexed again with the elements from $E^\times$ using $i \rightsquigarrow \alpha^i$ for $i = 0, \dots, n-1$, where α is a primitive root of 1 in E. We choose c as the vector which has 1 exactly on the positions $u \in U \setminus \{0\}$. Then $\mathrm{wt}\,(c) = |U \setminus \{0\}| = q^h - 1 = d$, and the formula (1) shows that $c \in C$.

In order to prove (1) we observe that:

$$\prod_{u \in U} (x - u) = \sum_{j=0}^{q^h} (-1)^j s_j x^j =$$

$$= x^{q^h} + a_{h-1} x^{q^{h-1}} + \cdots + a_0 x \in E[x].$$

So if the characteristic of K does not divide j is $s_j = 0$, so $rs_r = 0$ for all $r = 0, \dots, q^h$. If we compute the power functions p_r in the elements of u, $p_r = \sum_{u \in U} u^r$. According with Newton's equations,

$$p_r = -\Big(\sum_{j=1}^{r-1} s_j p_{r-j} + (-1)^r r s_r \Big) = -\sum_{j=1}^{r-1} s_j p_{r-j}$$

for $r = 1, \dots, q^h - 2$. We apply now induction over r and find that $p_r = 0$ for all $r = 1, \dots, q^h - 2 = d - 1$. So the relations (1) are proven. □

21 Quadratic Rest codes

Let $p \in \mathbb{N}$ be a prime number. The function:

$$\Big(\frac{x}{p}\Big) : \mathbb{F}_p^\times \to \mathbb{F}_p^\times,$$

$$\Big(\frac{x}{p}\Big) = x^{\frac{p-1}{2}}.$$

is called symbol of Legendre. Its value is 1 if x is a square modulo p and is -1 if this is not the case. For odd prime numbers p and q one knows the Reciprocity rule of Gauss:

$$\Big(\frac{q}{p}\Big) = (-1)^{\frac{(p-1)(q-1)}{4}} \Big(\frac{p}{q}\Big),$$

$$\Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}},$$

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}}.$$

It is also known that given p prime, there exists an infinity of prime numbers r which are squares (quadratic residuals) modulo p. In fact there are infinitely many primes $r = kp + 1$ with $k \in \mathbb{N}$.

We denote with $\mathcal{Q}_p$ the nonzero quadratic residues modulo p and with $\mathcal{N}_p$ the non-quadratic residues modulo p. Both sets have $(p-1)/2$ elements. Let $r \neq p$ another prime, such that $r \bmod p \in \mathcal{Q}_p$. Let $K = \mathbb{F}_r$. Let α be some p-root of 1, that is a root of $x^p - 1$, and $E = K[\alpha]$. We consider the polynomials:

$$q(x) = \prod_{i \in \mathcal{Q}_p} (x - \alpha^i) \in E[x],$$

$$n(x) = \prod_{i \in \mathcal{N}_p} (x - \alpha^i) \in E[x].$$

As r is a quadratic residue modulo p, the Frobenius homomorphism $x \rightsquigarrow x^r$ acting on these polynomials permutes the roots. If α^i is a root of $q(x)$ then α^{ri} is a root of $q(x)$, and the same for $n(x)$. So the coefficients are preserved by all the powers of Frobenius, and that means that $q(x), n(x) \in K[x]$.

Definition 21.1 If $p \neq r$ are odd primes and $r \bmod p$ is a quadratic residue, we denote by Q, N, $\bar{Q}$, $\bar{N}$ codes over $K = \mathbb{F}_r$ of length p generated by $q(x)$, $n(x)$, $(x-1)q(x)$ and $(x-1)n(x)$. They are quadratic rest codes, or QR-codes.

Lemma 21.2 *The following statements are true:*

1. $\dim Q = \dim N = (p+1)/2$ *and* $\dim \bar{Q} = \dim \bar{N} = (p-1)/2$.
2. $Q \simeq N$ *and* $\bar{Q} \simeq \bar{N}$.

Proof: The first statement follows from the fact that a cyclic code has dimension $n - \deg g$, where g is the generating polynomial. For the second one, observe that if $l \in \mathcal{N}_p$, then the mapping $i \rightsquigarrow li \bmod p$ is a bijection between $\mathcal{Q}_p$ and $\mathcal{N}_p$. The corresponding permutation matrix produces both equivalences because:

$$\sum_{i=0}^{p-1} c_i (\alpha^j)^i = \sum_{i=0}^{p-1} c_i (\alpha^{\pi(j)})^{\pi^{-1}(i)} = \sum_{i=0}^{p-1} c_{\pi(i)} (\alpha^{\pi(j)})^i.$$

□

Example 21.3 Take $p = 7$ and $r = 2 = 3^2 \bmod 7$ is a quadratic residuum. Let $\alpha \neq 1$ be a 7-root of 1 in $\mathbb{F}_8$ with the minimal polynomial:

$$m_\alpha = x^3 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = q(x)$$

over $K = \mathbb{F}_2$. The QR-code corresponding to $q(x)$ is a BCH-code. We have already seen that it is the binary $[7, 4, 3]$ Hamming code.

Example 21.4 Take $p = 23$ and $r = 2$. We compute:

$$\left(\frac{2}{23}\right) = (-1)^{\frac{22 \cdot 24}{8}} = 1.$$

In $\mathbb{F}_2[x]$ one has the following decomposition:

$$x^{23} - 1 = (x-1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$$

Both polynomials of degree 11 are irreducible, because if they were reducible, there was a primitive 23-root of 1 in $\mathbb{F}_{2^t}$ for $t \leq 10$. But this is not the case because 23 does not divide any $2^t - 1$ for $t \leq 10$. For a good choice of a 23-root of 1, we may choose

$$q(x) = (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) = \prod_{i \in \mathcal{Q}_{23}} (x - \alpha^i).$$

so the QR-code is a BCH-code with parameters $[23, 12, d]$. But the set of squares

$$\mathcal{Q}_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

The squares contain the arithmetic progression $1, 2, 3, 4$ so the minimal distance is $d \geq 5$. We will show later that $d = 7$ and that this QR-code is the Golay code $Gol(23)$.

Example 21.5 Take $p = 11$ and $r = 3$.

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

In $\mathbb{F}_{11}[x]$ one has the following decomposition:

$$(x^{11}-1) = (x-1)(x^5+x^4-x^3+x^2-1)(x^5-x^3+x^2-x-1)$$

and both polynomials of degree 5 are irreducible because 11 does not divide any number 2^t-1 for $t \leq 4$. Any one of the two polynomials can be chosen to be $q(x)$, and we get a QR-code with parameters $[11, 6, d]$. With $l = 1$ and $r = 2$ in the definition of the BCH-bound, as $\mathcal{Q}_{11} = \{1, 3, 4, 5, 9\}$ we get the minimal distance $d \geq 4$. We will show that $d = 5$. The code is equivalent with Golay code $Gol(11)$.

Let $\alpha \neq 1$ a p-root of 1 over $K = \mathbb{F}_r$, where p is an odd prime and $r \neq p$ is a prime such that $r = x^2 \bmod p$. We define:

$$\gamma = \sum_{i=1}^{p-1} \Big(\frac{i}{p}\Big)\alpha^i.$$

As $\Big(\frac{r}{p}\Big) = 1$ and $-1 = 1$ in characteristic 2, we get the equation:

$$\gamma^r = \sum_{i=1}^{p-1} \Big(\frac{i}{p}\Big)^r \alpha^{ir} = \sum_{i=1}^{p-1} \Big(\frac{i}{p}\Big)\alpha^{ir} = \sum_{i=1}^{p-1} \Big(\frac{ir}{p}\Big)\alpha^{ir} = \gamma,$$

hence $\gamma \in \mathbb{F}_r$. It is known that $\gamma^2 = \Big(\frac{-1}{p}\Big)p \neq 0$, so $\gamma \neq 0$. (exercize, this is the so called Gauss sum.)

Now we define the following notion of extension of a QR-code. In the case $r = 2$ one has $\frac{\gamma}{p} = 1$ in $\mathbb{F}_2$, this notion coincides with the general extension of codes.

Definition 21.6 The extension $\tilde{Q}$ of a QR-code Q is defined as:

$$\tilde{Q} = \Big\{\Big(c_0, \dots, c_{p-1}, -\frac{\gamma}{p}\sum_{i=0}^{p-1} c_i\Big) \,|\, (c_0, \dots, c_{p-1}) \in Q\Big\}.$$

Theorem 21.7 *Let $p = 4k+3$ be a prime number and Q be a QR-code of length p over $K = \mathbb{F}_r$. In this case:*

1. $Q^\perp = \bar{Q}$.
2. $\tilde{Q}^\perp = \tilde{Q}$.

Proof: In the following we use the fact that -1 is not a square modulo p, so the application $x \rightsquigarrow -x$ maps $\mathcal{Q}_p$ one in one onto $\mathcal{N}_p$.

Let $q(x) = \prod_{i \in \mathcal{Q}_p}(x - \alpha^i)$ be the generating polynomial of Q. As always in cyclic codes, $Q^\perp$ has as generating polynomial:

$$q^\perp(x) = -n(0)^{-1}x^{\frac{p+1}{2}}n\Big(\frac{1}{x}\Big)\Big(\frac{1}{x}-1\Big) = -n(0)^{-1}\prod_{j\in\mathcal{N}_p}(1-\alpha^j x)(1-x) =$$

$$= \prod_{j\in\mathcal{N}_p}(\alpha^{-j}-x)(1-x) = \prod_{i\in\mathcal{Q}_p}(\alpha^i - x)(1-x) = \prod_{i\in\mathcal{Q}_p}(x-\alpha^i)(x-1) = q(x)(x-1).$$

So $Q^\perp = \bar{Q}$.

In order to prove that $\tilde{Q}$ is self-dual, we consider a generating matrix $\bar{G}$ of $\bar{Q}$ and the extended matrix:

$$G = \begin{pmatrix} & \bar{G} & \\ 1 & \dots & 1 \end{pmatrix} \in \mathcal{M}_{\frac{p+1}{2}\times p}(K).$$

We know that:

$$\sum_{i=0}^{p-1} x^i = \frac{x^p - 1}{x-1} = q(x)n(x)$$

and that $p \neq 0 \bmod r$. Consequently $(1,1,\dots,1) \in Q \setminus \bar{Q}$. So G is a generating matrix for Q. Now we consider the matrix:

$$\tilde{G} = \begin{pmatrix} & & & 0 \\ & \bar{G} & & \vdots \\ & & & 0 \\ 1 & \dots & 1 & -\gamma \end{pmatrix} \in \mathcal{M}_{\frac{p+1}{2} \times (p+1)}(K).$$

Because of $Q^\perp = \bar{Q}$ and because of $(1,1,\dots,1) \in Q$ we get $\sum_{i=0}^{p-1} c_i = 0$ for $(c_0, \dots, c_{p-1}) \in \bar{Q}$. Hence $\tilde{G}$ is generating matrix of $\tilde{Q}$. Call z the last row of $\tilde{G}$. It follows:

$$\langle z, z \rangle = p + \gamma^2 = p + \Big(\frac{-1}{p}\Big)p = p - p = 0.$$

So $\tilde{Q} \subseteq \tilde{Q}^\perp$ but as they have equal dimension $(p+1)/2$, they are equal sets. □

Now we finally can compute the minimal distance of the Golay code as QR-codes.

Example 21.8 *The QR-code Q with parameters $[23, 12]$ is equivalent with the Golay code $Gol(23)$.*

$\bar{Q}$ has the generating polynomial $(x+1)q(x) = x^{12}+x^{10}+x^7+x^4+x^3+x^2+x+1$. In particular, $\bar{Q}$ has a basis consisting of vectors of weight 8. Now we look to the generating matrix of the extended QR-code $\tilde{G}$ and we observe, that $\tilde{Q}$ has a basis consisting of vectors whose weights are divisible with 8. But $\tilde{Q}$ is a self-dual binary code, so it is 4-divisible. We know already that $d(Q) \geq 5$. So it is $d(\tilde{Q}) \geq 8$ and $d(Q) \geq 7$. On the other hand, by the Hamming bound $d(Q) \leq 7$, so $d(Q) = 7$.

Example 21.9 *The ternary $[11, 6]$-code Q is equivalent with the Golay code $Gol(11)$.*

Because $\tilde{Q}$ is self-dual, it is 3-divisible. We already know $d(Q) \geq 4$, so $d(\tilde{Q}) \geq 6$, which implies $d(Q) \geq 5$. Using again the Hamming bound, we get $d(Q) = 5$.

The proof that a code with parameters $[23, 12, 7]$ or $[11, 6, 5]$ that contains 0 is always a linear code, and is isomorphic with $Gol(23)$ or with $Gol(11)$ is more complicated, but the statement is true.

In the rest of this section we show some interesting properties of the case $p = 8k + 7$, $r = 2$. We define the following polynomials:

$$e_q = \sum_{i \in \mathcal{Q}_p} x^i \in \mathbb{F}_2[x],$$

$$e_n = \sum_{i \in \mathcal{N}_p} x^i \in \mathbb{F}_2[x].$$

Theorem 21.10 *Let $p = 8k - 1$ and $r = 2$. For an adequate choice of α, e_q is the idempotent of Q and $1 + e_n$ is the idempotent of $\bar{Q}$.*

Proof: We observe that:

$$\Big(\frac{2}{p}\Big) = (-1)^{\frac{8k(8k-2)}{8}} = 1.$$

Hence:

$$e_q \circ e_q = \sum_{i \in \mathcal{Q}_p} x^{2i} = \sum_{i \in \mathcal{Q}_p} x^i = e_q.$$

Also $e_n \circ e_n = e_n$. So $e_q(\alpha), e_n(\alpha) \in \{0, 1\}$. But:

$$e_q(\alpha) + e_n(\alpha) = \alpha + \cdots + \alpha^{p-1} = -1 = 1.$$

It might be necessary to replace α with α^j with $j \in \mathcal{N}_p$, but up to this substitution we may suppose $e_q(\alpha) = 0$ and $e_n(\alpha) = 1$. Then $e_q(\alpha^i) = 0$ and $e_n(\alpha^i) = 1$ for all $i \in \mathcal{Q}_p$. Further is $e_q(1) = e_n(1) = (p-1)/2 = 1$. So e_q is idempotent and has the same roots in $\langle \alpha \rangle$ like the generating polynomial of Q, and $1 + e_n$ has the same roots in $\langle \alpha \rangle$ like the generating polynomial of $\bar{Q}$. The conclusion follows from the unicity of the idempotent of a cyclic code. □

Theorem 21.11 *For $p = 8k - 1$ and $r = 2$ is the extended QR-code $\tilde{Q}$ self-dual and 4-divisible.*

Proof: We already know that the code is self-dual. We also know that the elements $(1 + e_n) \circ x^i$ $(i = 0, \ldots, p-1)$ generate $\bar{Q}$. All those elements have weight $(p+1)/2$, which is divisible with 4. So $\tilde{Q}$ has a basis of elements, which have all weights divisible with 4. □

Part V

Error correction and other topics

22 Classic Goppa codes

Let K be a field. With $K(x)$ we denote the field of rational functions over K. This is the field of fractions of the ring of polynomials over K, which is a domain of integrity. If $f, h \in K(x)$ and $g \in K[x]$ we write $f \equiv h \bmod g$ if

$$f - h = \frac{u}{v}$$

with $u, v \in K[x]$, $\gcd(u, v) = 1$ and $g \mid u$. This congruence is a relation of equivalence over $K(x)$.

Definition 22.1 Consider the fields $K = \mathbb{F}_q \leq E = \mathbb{F}_{q^m}$. Let $\mathcal{P} = \{a_1, \dots, a_n\}$ a finite subset of E and g a monic polynomial in $E[x]$ with $g(a_i) \neq 0$ for all i. The linear code:

$$\Gamma(\mathcal{P}, g) = \Big\{ c = (c_1, \dots, c_n) \mid c_i \in K, \sum_{i=1}^{n} \frac{c_i}{x - a_i} \equiv 0 \bmod g \Big\}$$

is a classic Goppa code. The polynomial g is the Goppa polynomial. If g is irreducible, we say that the code is irreducible as well.

The classic Goppa codes are subfield codes for some generalized Reed-Solomon codes.

Theorem 22.2 *Let $\Gamma(\mathcal{P}, g)$ be a classic Goppa code with $\mathcal{P} = \{a_1, \dots, a_n\}$ and $\deg g = t$. Then:*

1. *If $t \geq n$ then $\Gamma(\mathcal{P}, g) = 0$.*
2. *If $t < n$ then $\Gamma(\mathcal{P}, g) = GRS_{t+1}(a, v)|K$, if $a = (a_1, \dots, a_n)$ and $v = (g(a_1)^{-1}, \dots, g(a_n)^{-1})$.*

Proof: Denote $\Gamma(\mathcal{P}, g)$ with C and write $g = g_t x^t + \cdots + g_0$ where $g_t \neq 0$. Define:

$$f_i(x) = -\frac{g(x) - g(a_i)}{x - a_i} g(a_i)^{-1},$$

such that:

$$(x - a_i) f_i(x) = 1 - g(a_i)^{-1} g(x) \equiv 1 \bmod g,$$

$$f_i(x) \equiv \frac{1}{x - a_i} \bmod g.$$

The polynomial $h(x) = g(x) - g(a_i)$ has $h(a_i) = 0$ so is divisible by the polynomial $x - a_i$. It follows that $f_i \in E[x]$ and that $\deg f_i = t - 1$. It follows that $c = (c_1, \dots, c_n) \in C$ if and only if $c_1 f_1(x) + \cdots + c_n f_n(x) \equiv 0 \bmod g$. But the left-hand side has degree $< t$, so the condition is $c_1 f_1(x) + \cdots + c_n f_n(x) = 0$.

We observe the identity:

$$\frac{g(x) - g(y)}{x - y} = g_t(x^{t-1} + x^{t-2}y + \cdots + y^{t-1}) + g_{t-1}(x^{t-2} + x^{t-3}y + \cdots + y^{t-2}) + \cdots +$$

$$+ g_2(x + y) + g_1.$$

Put $y = a_i$ and $v_i = g(a_i)^{-1}$. Then the condition $c_1 f_1(x) + \cdots + c_n f_n(x) = 0$ can be written down in the form of a check matrix:

$$\begin{pmatrix} g_t v_1 & \dots & g_t v_n \\ (g_{t-1} + a_1 g_t) v_1 & \dots & (g_{t-1} + a_n g_t) v_n \\ \vdots & & \vdots \\ (g_1 + a_1 g_2 + \cdots + a_1^{t-1} g_t) v_1 & \dots & (g_1 + a_n g_2 + \cdots + a_n^{t-1} g_t) v_n \end{pmatrix} =$$

$$= \begin{pmatrix} g_t & 0 & 0 & \dots & 0 \\ g_{t-1} & g_t & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ g_1 & g_2 & g_3 & \dots & g_t \end{pmatrix} \begin{pmatrix} v_1 & \dots & v_n \\ a_1 v_1 & \dots & a_n v_n \\ \vdots & & \vdots \\ a_1^{t-1} v_1 & \dots & a_n^{t-1} v_n \end{pmatrix}.$$

As $g_t \neq 0$, the right matrix is itself a check matrix for C. In the case $t \geq n$, the kernel of the right matrix consists of 0 only. □

It follows that $d(\Gamma(\mathcal{P}, g)) \geq 1 + t$, for $t < n$.

Example 22.3 Let C be a classic BCH-code over K of length n and of designed distance d. Let α be the corresponding primitive n-root of 1 over K. If we define $\mathcal{P} = \{\alpha^i \,|\, i = 0, 1, \dots, n-1\}$ and $g = x^{d-1}$, then $C \simeq \Gamma(\mathcal{P}, g)$.

23 The Berlekamp-Welch algorithm

The Berlecamp-Welch algorithm is a fast error correction procedure for a version of the classic Reed-Solomon code.

Definition 23.1 *Let K be a commutative field, not necessarily finite. Let $t \geq 1$ and $n = 3t + 1$. We consider the following linear code C of length n over K. Let $x_1, \dots, x_n \in K$ be fixed pairwise different elements.*

$$C = \{(f(x_1), \dots, f(x_n)) \,|\, f \in K[x], \deg f \leq t\}.$$

Theorem 23.2 *There is a procedure to fast correct $e < t$ many errors in C.*

Proof: Consider the polynomial:

$$Q(x, y) = f_0(x) - f_1(x)y,$$

where $f_0, f_1 \in K[x]$, $\deg f_0 \leq 2t$, $\deg f_1 \leq t$ and $f_1(0) = 1$. Suppose that the received code-word is $(y_1, \dots, y_n)$ and that there are at most e transmission errors. This means that there is a code-word $c = (c_1, \dots, c_n) \in C$ and there is a set of indexes $i_1, \dots, i_e$ such that $c_{i_j} \neq y_{i_j}$ but $c_k = y_k$ for $k \neq i_j$.

We write down the conditions $Q(x_k, y_k) = 0$. This means that we have got a system of $n = 3t + 1$ equations with $(2t+1)+t = 3t+1$ unknowns, which are the unknown coefficients of f_0 and f_1. We solve the system and we find out the polynomial f which has produced the code-word by division with remainder in the ring $K[x]$:

$$f(x) = \frac{f_0(x)}{f_1(x)}.$$

Now we must prove that $f_1 \,|\, f_0$ and the result of the polynomial division is really f, the polynomial corresponding to c. Indeed, consider the polynomial $P(x) = Q(x, f(x))$, where f is the polynomial we are trying to determine. The polynomial has degree $\leq 2t$ but at least $n - e$ roots - the valid points. But:

$$n - e > n - t > 3t - t = 2t,$$

so the polynomial has a number of roots which is bigger that its degree. As being defined over a commutative field, $P(x)$ must be 0, so the equality:

$$f_0(x) = f(x) f_1(x)$$

is a polynomial identity.

Now we can generate the original code-word:

$$(c_1, \dots, c_n) = (f(x_1), \dots, f(x_n)).$$

□

24 The Peterson-Gorenstein-Zierler algorithm

Let $GRS_d(a, v)$ be a generalized Reed-Solomon code of length n over $E = \mathbb{F}_{q^m}$. Recall that $2 \leq d \leq n \leq q^m$ and the components v_i of the vector v are all different from 0. The components a_i are pairwise different. In this section we suppose also that $a_i \neq 0$. $GRS_d(a, v)$ has the check matrix:

$$H = \begin{pmatrix} v_1 & \dots & v_n \\ a_1 v_1 & \dots & a_n v_n \\ \vdots & & \vdots \\ a_1^{d-2} v_1 & \dots & a_n^{d-2} v_n \end{pmatrix}.$$

Further let $K = \mathbb{F}_q \leq E$ and $C = GRS_d(a, v)|K$. The following algorithm decodes consequently Reed-Solomon codes, classic Goppa codes and BCH-codes.

Definition 24.1 Let $c = (c_1, \dots, c_n) \in C$. Let $\tilde{c} = c+f$ the received word. $f = (f_1, \dots, f_n) \in K^n$ is the error vector, with $\mathrm{wt}\,(f) = t \leq (d-1)/2$. Let $s = (s_1, \dots, s_{d-1})$ be the syndrome of $\tilde{c}$. This means:

$$(s_1, \dots, s_{d-1})^T = H\tilde{c}^T = H(c+f)^T = Hf^T.$$

The set $F = \mathrm{supp}\, f = \{i_1, \dots, i_t\}$ is the set of mistaken positions. The polynomial:

$$\sigma(x) = \prod_{l \in F} (1 - a_l x) = \sigma_0 + \sigma_1 x + \dots + \sigma_t x^t \in E[x],$$

with $\sigma_0 = 1$ is the error localisation polynomial. We observe $l \in F$ if and only if $\sigma(a_l^{-1}) = 0$.

Lemma 24.2 *1. For $i = 1, \dots, d-1$,*

$$s_i = \sum_{l \in F} a_l^{i-1} v_l f_l.$$

2. For $i = t+1, \dots, d-1$,

$$s_i = -\sum_{j=1}^{t} \sigma_j s_{i-j}.$$

Proof: (1) follows directly from the definition of the syndrom. In order to prove (2) compute for $i = t+1, \dots, d-1$:

$$\sum_{j=0}^{t} \sigma_j s_{i-j} = \sum_{j=0}^{t} \sigma_j \sum_{l \in F} a_l^{i-j-1} v_l f_l =$$

$$= \sum_{l \in F} a_l^{i-1} v_l f_l \Big(\sum_{j=0}^{t} \sigma_j a_l^{-j} \Big) =$$

$$= \sum_{l \in F} a_l^{i-1} v_l f_l \sigma(a_l^{-1}) = 0.$$

□

The first part of the Lemma says that if we have the error positions, then we can use the syndrome in order to compute c. The second part is useful to compute the error location polynomial.

Lemma 24.3 *Consider* $\eta(x) = 1 + \eta_1 x + \cdots + \eta_t x^t \in E[x]$*. If for* $j = t+1, \ldots, d-1$*,*

$$s_i = -\sum_{j=1}^{t} \eta_j s_{i-j},$$

then $\eta(x) = \sigma(x)$*.*

Proof: With $\eta_0 = 1$ we get following equations:

$$0 = \sum_{j=0}^{t} \eta_j s_{i-j} = \sum_{l \in F} a_l^{i-1} v_l f_l \eta(a_l^{-1})$$

with $i = t+1, \ldots, d-1$. There are $d - 1 - t \geq 2t - t = t$ equations. The following matrix is regular:

$$\left(a_l^{i-1} v_l f_l\right)_{l \in F}^{i=t+1,\ldots,2t}.$$

So $\eta(a_l^{-1}) = 0$ for $l \in F$, and $\eta(x) = \sigma(x)$. □

With other words, the error location polynomial is the polynomial of least degree, whose coefficients satisfy the given linear constraints.

Definition 24.4 For every $1 \leq r \leq [(d-1)/2]$, we consider the matrix:

$$S_r = \begin{pmatrix} s_1 & s_2 & \ldots & s_r \\ s_2 & s_3 & \ldots & s_{r+1} \\ \vdots & \vdots & & \vdots \\ s_r & s_{r+1} & \ldots & s_{2r-1} \end{pmatrix}.$$

The term s_{hk} is nothing else as $s_{hk} = s_{h+k-1}$.

Remark 24.5 The first t equations in Lemma 24.2 say that the coefficients σ_i of the error localization polynomial are solutions of the system:

$$S_t \begin{pmatrix} \sigma_t \\ \vdots \\ \sigma_1 \end{pmatrix} = - \begin{pmatrix} s_{t+1} \\ \vdots \\ s_{2t} \end{pmatrix}.$$

If we know the number of mistaken coordinates t, then we can compute the error localization polynomial, and this results from the following Lemma.

Lemma 24.6 *The matrix* S_t *is regular.*

Proof: We define following $t \times t$-matrices:
$A = (a_{hk})$ with $a_{hk} = a_{i_k}^{h-1} v_{i_k}$,
$B = (b_{hk})$ with $b_{hk} = \delta_{hk} f_{i_k}$,
$C = (c_{hk})$ with $c_{hk} = a_{i_k}^{h-1}$.

$$(ABC^T)_{hk} = \sum_{j=1}^{t} \sum_{m=1}^{t} a_{hj} b_{jm} c_{km} =$$

$$= \sum_{j=1}^{t} \sum_{m=1}^{t} a_{i_j}^{h-1} v_{i_j} \delta_{jm} f_{i_m} a_{i_m}^{k-1} =$$

$$= \sum_{j=1}^{t} a_{i_j}^{h-1} v_{i_j} f_{i_j} a_{i_j}^{k-1} =$$

$$= \sum_{j=1}^{t} a_{i_j}^{h+k-2} v_{i_j} f_{i_j} = s_{h+k-1} = s_{hk} = (S_t)_{hk}$$

All three matrices are regular and $S_t = ABC^T$. □

Now the only thing that remained to determine is the number of errors $t = |F|$. This is done with the following theorem:

Theorem 24.7 *Let $e = [(d-1)/2]$. Then $t = |F| = \operatorname{rk} S_e$ and S_r is singular for $t < r \le e$.*

Proof: Consider the matrix:

$$S_e = \begin{pmatrix} s_1 & s_2 & \dots & s_e \\ s_2 & s_3 & \dots & s_{e+1} \\ \vdots & \vdots & & \vdots \\ s_e & s_{e+1} & \dots & s_{2e-1} \end{pmatrix}.$$

As $t \le e$, we already know that the first t columns of S_e are linear independent, so $\operatorname{rk} S_e \ge t$. Take $t < r \le e$. The equalities from Lemma 24.2 mean that the column r of S_e is linear dependent on the t columns preceding it. So $\operatorname{rk} S_e = t$. □

To sum up, the Peterson, Gorenstein and Zierler algorithm works as follows:

1. Compute the syndrome $(s_1, \dots, s_{d-1})^T = H\tilde{c}^T$. If all $s_i = 0$, then $c = \tilde{c}$ and STOP.
2. Determine $t = \max\{r \mid 1 \le r \le [(d-1)/2], \det S_r \ne 0\}$. If all $\det S_r = 0$ there are too many mistakes, return FALSE.
3. Determine the error localization polynomial $\sigma(x)$ solving the system:

$$S_t \begin{pmatrix} \sigma_t \\ \vdots \\ \sigma_1 \end{pmatrix} = - \begin{pmatrix} s_{t+1} \\ \vdots \\ s_{2t} \end{pmatrix}.$$

4. Find out the set $F = \{i_1, \dots, i_t\}$ by the equivalence $i \in F \longleftrightarrow \sigma(a_i^{-1}) = 0$.
5. Compute the error $f = (f_1, \dots, f_n)$ solving the system of equations:

$$\begin{pmatrix} v_{i_1} & \dots & v_{i_t} \\ a_{i_1} v_{i_1} & \dots & a_{i_t} v_{i_t} \\ \vdots & & \vdots \\ a_{i_1}^{d-2} v_{i_1} & \dots & a_{i_t}^{d-2} v_{i_t} \end{pmatrix} \begin{pmatrix} f_{i_1} \\ \vdots \\ f_{i_t} \end{pmatrix} = - \begin{pmatrix} s_1 \\ \vdots \\ s_t \end{pmatrix}.$$

6. Return $c = \tilde{c} - f$.

Steps 2, 3 and 5 are computationally intensive. So new algorithms are done in order to optimize them.

25 Error correction using Euclid's algorithm

This section is a completion to Section 24. We keep all definitions and notations of this section. The algorithm was discovered by Sugiama, Kasahara, Hirasawa and Namekawa.

Definition 25.1 We call error evaluation polynomial:

$$\omega(x) = \sum_{l \in F} f_l v_l \prod_{l' \in F \setminus \{l\}} (1 - a_{l'} x).$$

The syndrome polynomial is:

$$S(x) = \sum_{i=0}^{d-2} s_{i+1} x^i.$$

Lemma 25.2 *Let $\sigma'(x)$ be the derivative of $\sigma(x)$. Then we can compute the errors using:*

$$f_l = -\frac{\omega(a_l^{-1})}{\sigma'(a_l^{-1})} \cdot \frac{a_l}{v_l}$$

for $l \in F$.

Proof: We observe that:

$$\sigma'(x) = -\sum_{l \in F} a_l \prod_{l' \in F \setminus \{l\}} (1 - a_{l'} x).$$

□

We can find out the error evaluation polynomial using the error location polynomial, according to the following Lemma:

Lemma 25.3 $S(x)\sigma(x) \equiv \omega(x) \bmod x^{d-1}$.

Proof: By direct computation, we get:

$$S(x)\sigma(x) = \Big(\sum_{i=0}^{d-2} \sum_{l \in F} a_l^i v_l f_l x^i\Big)\Big(\prod_{l \in F}(1 - a_l x)\Big) =$$

$$= \sum_{l \in F} v_l f_l \Big[(1 - a_l x) \sum_{i=0}^{d-2} (a_l x)^i\Big] \prod_{l' \in F \setminus \{l\}} (1 - a_{l'} x) =$$

$$= \sum_{l \in F} v_l f_l \Big[1 - (a_l x)^{d-1}\Big] \prod_{l' \in F \setminus \{l\}} (1 - a_{l'} x) =$$

$$= \sum_{l \in F} v_l f_l \prod_{l' \in F \setminus \{l\}} (1 - a_{l'} x) \mod x^{d-1} = \omega(x) \mod x^{d-1}.$$

□

We show now an algorithm that computes in the same time $\sigma(x)$ and $\omega(x)$. The algorithm works in the following way. Because $S(x)\sigma(x) \equiv \omega(x) \bmod x^{d-1}$, there is a true polynomial identity:

$$S(x)\sigma(x) + u(x)x^{d-1} = \omega(x).$$

We set $r_{-1}(x) = x^{d-1}$ and $r_0(x) = S(x)$, and we compute recursively:

$$r_{k-2}(x) = q_k(x) r_{k-1}(x) + r_k(x),$$

where $\deg r_k(x) < \deg r_{k-1}(x)$. This works since finally $r_m(x) = \gcd(x^{d-1}, S(x))$ and $r_{m+1}(x) = 0$. On the way backwards, we find relations for $k = -1, 0, 1, \dots, m$:

$$r_k(x) = a_k(x)x^{d-1} + b_k(x)S(x).$$

Here we put $a_{-1}(x) = 1$, $b_{-1}(x) = 0$, $a_0(x) = 0$, $b_0(x) = 1$.

Lemma 25.4 *The following statements are true:*

1. $\gcd(a_k(x), b_k(x)) = 1$ *for all* $k = -1, 0, \dots, m$.
2. $\deg b_k(x) = d - 1 - \deg r_{k-1}(x)$ *for* $k = 0, 1, \dots, m$.

Proof: (1) For $k \geq 1$ we have $r_k(x) = r_{k-2}(x) - q_k(x)r_{k-1}(x)$ and so

$$\begin{aligned} a_k(x) &= a_{k-2}(x) - q_k(x)a_{k-1}(x), \\ b_k(x) &= b_{k-2}(x) - q_k(x)b_{k-1}(x). \end{aligned}$$

It follows:

$$\det\begin{pmatrix} a_k(x) & b_k(x) \\ a_{k-1}(x) & b_{k-1}(x) \end{pmatrix} = \det\begin{pmatrix} a_{k-2}(x) & b_{k-2}(x) \\ a_{k-1}(x) & b_{k-1}(x) \end{pmatrix} = \dots$$

$$\dots = \pm\det\begin{pmatrix} a_{-1}(x) & b_{-1}(x) \\ a_0(x) & b_0(x) \end{pmatrix} = \pm\det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pm 1,$$

and it follows also that $\gcd(a_k(x), b_k(x)) = 1$ for $k \geq 1$.

(2) For $k = 0$ the statement is correct, so take $k \geq 1$. We have $b_k(x) = b_{k-2}(x) - q_k(x)b_{k-1}(x)$ and $\deg q_k \geq 1$, so we get by induction $\deg b_k(x) > \deg b_{k-1}(x)$. Now we make a new induction and get:

$$\deg b_k(x) = \deg q_k(x)b_{k-1}(x) = \deg q_k(x) + \deg b_{k-1}(x) =$$

$$= \deg q_k(x) + (d - 1 - \deg r_{k-2}(x)) = \deg q_k(x) + d - 1 - \deg q_k(x)r_{k-1}(x) =$$

$$= d - 1 - \deg r_{k-1}(x).$$

□

Theorem 25.5 *The following statements are true:*

1. *There is a* $k \in \{0, 1, \dots, m\}$ *such that* $r_k(x) \neq 0$, $\deg r_k(x) < \frac{d-1}{2}$ *and* $\deg r_{k-1}(x) \geq \frac{d-1}{2}$.
2. *For this* k, $\sigma(x) = \mu b_k(x)$ *and* $\omega(x) = \mu r_k(x)$, *where* $\mu = b_k(0)^{-1}$.

Proof: Because of $r_m(x) = \gcd(x^{d-1}, S(x))$ and $S(x)\sigma(x) + u(x)x^{d-1} = \omega(x)$, $r_m(x) \,|\, \omega(x)$ and :

$$\deg r_m(x) \leq \deg \omega(x) \leq t - 1 < \frac{d-1}{2}.$$

So there is a k as in the statement.

The following relations are true:

$$\begin{aligned} \sigma(x)r_k(x) &= \sigma(x)[a_k(x)x^{d-1} + b_k(x)S(x)], \\ \omega(x)b_k(x) &= [S(x)\sigma(x) + u(x)x^{d-1}]b_k(x). \end{aligned}$$

By subtracting them, we get:

$$\sigma(x)r_k(x) - \omega(x)b_k(x) = [\sigma(x)a_k(x) - u(x)b_k(x)]x^{d-1}.$$

Because of $\deg \sigma(x) = t \leq (d-1)/2$ and $\deg r_k(x) < (d-1)/2$, $\deg \sigma(x) r_k(x) < d-1$. Further:

$$\deg b_k(x) = d - 1 - \deg r_{k-1}(x) \leq d - 1 - \frac{d-1}{2} = \frac{d-1}{2}.$$

$$\deg \omega(x) \leq t - 1 < \frac{d-1}{2} \longrightarrow \deg \omega(x) b_k(x) < d - 1.$$

Sot the congruence says in fact that:

$$\sigma(x) r_k(x) = \omega(x) b_k(x),$$

$$\sigma(x) a_k(x) = u(x) b_k(x).$$

But by definition, $\sigma(x)$ and $\omega(x)$ have no common root. So is $\gcd(\sigma(x), \omega(x)) = 1$. So $\sigma(x) \,|\, b_k(x)$ and as $\gcd(a_k(x), b_k(x)) = 1$, $b_k(x) \,|\, \sigma(x)$. So $\sigma(x) = \mu b_k(x)$, $\sigma(0) = 1$, so $\mu = b_k(0)^{-1}$. □

26 The Berlekamp-Masey algorithm

Let K be an arbitrary field and $L > 1$ a natural number. A sequence $(s_k) \subset K$ is a linear homogeneous recursion sequence over K if there are $\sigma_1, \dots, \sigma_L \in K$ such that for all $k \geq L+1$ one has:

$$s_k = -\sum_{i=1}^{L} \sigma_i s_{k-i}.$$

The polynomial $\sigma(x) = 1 + \sigma_1 x + \dots + \sigma_l x^l \in K[x]$, with $\sigma_0 = 1$, is called feedback polynomial. The pair $(L, \sigma(x))$ is a linear recursion of length L. The pair $(0, 1)$ is the trivial recursion.

Theorem 26.1 *For $r = 1, \dots, N$ let $(L_r, \sigma^{(r)})$ be a recursion of minimal length, which generates the sequence (s_k) with $k = 1, \dots, r$. Let $(L_0, \sigma^{(0)}(x))$ the trivial recursion. We define:*

$$\delta_r = \sum_{j=0}^{L_{r-1}} \sigma_j^{(r-1)} s_{r-j}.$$

It follows:

$$L_r = \begin{cases} L_{r-1}, & \delta_r = 0, \\ \max(L_{r-1}, r - L_{r-1}), & \delta_r \neq 0, \end{cases}$$

for all $1 \leq r \leq N$.

Proof: Because of the minimality of the length, $L_r \geq L_{r-1}$.

Now we show that if $\delta_r \neq 0$ then $L_r \geq \max(L_{r-1}, r - L_{r-1})$. In order to reach a contradiction, suppose that $L_r < r - L_{r-1}$. It is sure that $L_{r-1} \leq r - 1$. Now for $j \in \{1, \dots, L_{r-1}\}$ we get:

$$(1) \qquad L_r + 1 \leq r - L_{r-1} \leq r - j \leq r - 1,$$

and for $i \in \{1, \dots, L_r\}$

$$(2) \qquad L_{r-1} + 1 \leq r - L_r \leq r - i \leq r - 1.$$

The contradiction follows:

$$s_r \neq -\sum_{j=1}^{L_{r-1}} \sigma_j^{(r-1)} s_{r-j} \qquad \text{because } \delta_r \neq 0$$

$$= \sum_{j=1}^{L_{r-1}} \sigma_j^{(r-1)} \sum_{i=1}^{L_r} \sigma_i^{(r)} s_{r-j-i} \qquad \text{because (1)}$$

$$= \sum_{i=1}^{L_r} \sigma_i^{(r)} \sum_{j=1}^{L_{r-1}} \sigma_j^{(r-1)} s_{r-j-i}$$

$$= \sum_{i=1}^{L_r} \sigma_i^{(r)} s_{r-i} \qquad \text{because (2)}$$

$$= s_r.$$

Now we show the Theorem by induction over r. Put $r = 1$. If $\delta_1 = 0$, then $0 = \delta_1 = s_1$ is generated by the trivial recursion $(0, 1)$. So $L_0 = L_1$. If $\delta_1 \neq 0$, then $0 \neq \delta_1 = s_1$ is generated by the minimal recursion $(1, 1)$. So we got $1 = L_1 = \max\{L_0, 1 - L_0\}$ and the start of the induction is verified. Now suppose that the statement has been proven for $k = 1, \dots, r-1$ with $2 \leq r \leq N$. We can suppose that $\delta_t \neq 0$ for at least one $1 \leq t \leq r-1$ because if not, then the recursion of minimal length that generates $s_1, \dots, s_r$ would be $(0, 1)$ in the case that $\delta_r = s_r = 0$ and $(r, 1)$ in the case that $\delta_r = s_r \neq 0$.

Let $m \in \mathbb{N}$ be determined by the condition:

$$L_{r-1} = L_{r-2} = \cdots = L_m > L_{m-1}.$$

If $\delta_r = 0$ then $L_r = L_{r-1}$ because of $L_r \geq L_{r-1}$. So $\delta_r \neq 0$. We define a recursion $(L_r, \sigma^{(r)}(x))$ of minimal length, which generates the sequence $s_1, \dots, s_r$ and which verifies $L_r = \max(L_{r-1}, r - L_{r-1})$. We set:

$$\sigma^{(r)}(x) = \sigma^{(r-1)}(x) - \frac{\delta_r}{\delta_m} x^{r-m} \sigma^{(m-1)}(x).$$

We see that $L_m > L_{m-1}$ implies $\delta_m \neq 0$. Also $\deg \sigma^{(r)}(x) \leq \max(L_{r-1}, r - m + L_{m-1})$. The choice of m and the induction hypothesis imply:

$$L_{m-1} < L_{r-1} = L_m = \max(L_{m-1}, m - L_{m-1}) = m - L_{m-1}.$$

So $\deg \sigma^{(r)}(x) \leq \max(L_{r-1}, r - L_{r-1})$. Set now:

$$L = \max(L_{r-1}, r - L_{r-1}).$$

Now we see that $(L, \sigma^{(r)}(x))$ is a recursion that generates the sequence $s_1, \dots, s_r$, because:

$$s_k + \sum_{j=1}^{L} \sigma_j^{(r)} s_{k-j} = s_k + \sum_{j=1}^{L_{r-1}} \sigma_j^{(r-1)} s_{k-j} - \frac{\delta_r}{\delta_m} \left(s_{k+m-r} + \sigma_{j=1}^{L_{m-1}} \sigma_j^{(m-1)} s_{k+m-r-j} \right) =$$

$$= \begin{cases} \delta_r - \frac{\delta_r}{\delta_m} \delta_m = 0 & k = r, \\ 0 & k = L+1, \dots, r-1. \end{cases}$$

In order to apply this for $k = L+1, \dots, r-1$, we observe that $(L+1) + m - r > (r - L_{r-1}) + m - r = r - (m - L_{m-1}) + m - r = L_{m-1}$, hence $k + m - r \geq L_{m-1} + 1$ for $k = L+1, \dots, r-1$. In conclusion the recursion $(L, \sigma^{(r)}(x))$ the sequence $s_1, \dots, s_r$. Also, $L_r \geq L$, and by minimality $L_r = L$. □

The **Berlekamp - Masey Algorithm** works as follows:

1. Set $(L_0, \sigma^{(0)}) = (0, 1)$ and $L_{-1} = 0$.
2. For $r = 1, \dots, N$ execute the following steps:
   (a) Compute $\delta_r = \sum_{j=0}^{L_{r-1}} \sigma_j^{(r-1)} s_{r-j}$.

(b) If $\delta_r = 0$ set $(L_r, \sigma^{(r)}(x)) = (L_{r-1}, \sigma^{(r-1)}(x))$.

(c) If $\delta_r \neq 0$ set:

$$L_r = \max(L_{r-1}, r - L_{r-1}),$$

$$\sigma^{(r)}(x) = \sigma^{(r-1)}(x) - \frac{\delta_r}{\delta_m} x^{r-m} \sigma^{(m-1)}(x),$$

where $m = \max\{i \,|\, 0 \leq i \leq r-1, L_i > L_{i-1}\}$. If this maximum is 0, set $\sigma^{(r)}(x) = 1$.

3. $(L_N, \sigma^{(N)}(x))$ is a recursion of minimal length that generates $s_1, \dots, s_N$.

In order to find the error localisation polynomial, one constructs the recursion of minimal length that generates the syndrome sequence. If $L > \frac{d-1}{2}$ then send an error message. Else, we have got $\sigma(x)$ and we compute $\omega(x)$ with $S(x)\sigma(x) \equiv \omega(x) \bmod x^{d-1}$.

27 Unicity of the binary Golay code

We show in this section that the binary Golay code is unique, in the sense that:

Theorem 27.1 *Every $(23, 2^{12}, 7)$ binary code C that contains $(0, 0, \dots, 0)$ is a linear code and is equivalent with the binary Golay code $Gol(23)$.*

We first observe that:

Lemma 27.2 *Every $(23, 2^{12}, 7)$ binary code C is perfect.*

Proof: The Hamming bound theorem is a result about codes in general, not only about linear codes. We compute that:

$$2^{23} \geq |\bigcup_{c \in C} B_3(c)| = 2^{12}\,|B_3(0)| = 2^{12}\left(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}\right) = 2^{12}2^{11}.$$

The code is perfect as it satisfies the equality in the Hamming bound theorem. □

Proof of the theorem: We will show here that the code is linear and is formal equivalent with $Gol(23)$: has the same weight polynomial, and some other common properties. A complete proof of the equivalence is too long and not appropriate for this lecture series.

Denote $\mathbb{F}_2$ with K. We choose a $c_0 \in C$. Let $A_i = |\{c \,|\, c \in C, d(c, c_0) = i\}|$. Moreover, for $0 \leq j \leq 23$ we define the set:

$$X_j = \{(x, c) \,|\, x \in K^{23}, c \in C, d(x, c_0) = j, d(x, c) \leq 3\}.$$

We will count X_j in two different ways. As C is perfect, for every $x \in K^{23}$ there is exactly one $c \in C$ such that $d(x, c) \leq 3$. So one has:

$$|X_j| = |\{x \,|\, x \in K^{23}, d(x, c_0) = j\}| = |\{x \,|\, x \in K^{23}, d(x, 0) = j\}| = \binom{23}{j}.$$

On the other hand:

$$|X_j| = \sum_{c \in C} |\{x \,|\, x \in K^{23}, d(x, c_0) = j, d(x, c) \leq 3\}|.$$

If we write now $c = c_0 + f_i$ with $f_i \in K^{23}$ and $d(f_i, 0) = i$, it follows:

$$|\{x \,|\, x \in K^{23}, d(x, c_0) = j, d(x, c) \leq 3\}| =$$

$$= |\{y \mid y \in K^{23}, d(y + c_0, c_0) = j, d(y + c_0, c_0 + f_i) \leq 3\}| =$$
$$= |\{y \mid y \in K^{23}, d(y, 0) = j, d(y, f_i) \leq 3\}|.$$

This quantity depends now only of j and $i = d(f_i, 0)$. So we conclude:

$$\binom{23}{j} = |X_j| = \sum_{i=0}^{23} A_i \cdot |\{y \mid y \in K^{23}, d(y, 0) = j, d(y, f_i) \leq 3\}|.$$

However $|\{y \mid y \in K^{23}, d(y, 0) = j, d(y, f_i) \leq 3\}| \neq 0$ at most for $j - 3 \leq i \leq j + 3$. For $3 \leq j \leq 20$ we get:

$$\binom{23}{j} = \begin{cases} A_{j+3}\binom{j+3}{3} + A_{j+2}\binom{j+2}{2} + \\ +A_{j+1}\left[\binom{j+1}{1} + \binom{j+1}{2}\binom{23-(j+1)}{1}\right] + \\ +A_j\left[1 + \binom{j}{1}\binom{23-j}{1}\right] + \\ +A_{j-1}\left[\binom{23-(j-1)}{1} + \binom{j-1}{1}\binom{23-(j-1)}{2}\right] + \\ +A_{j-2}\binom{23-(j-2)}{2} + A_{j-3}\binom{23-(j-3)}{3}. \end{cases}$$

For $j = 4, 5, \ldots, 20$ we can compute the weight polynomial coefficients A_7, A_8, ... We get:

$$A(z) = 1 + 253z^7 + 506z^8 + 1288z^{11} + 1288z^{12} + 506z^{15} + 253z^{16} + z^{23}.$$

In particular $A_i \neq 0$ implies $i = 0, 3 \bmod 4$.

Now we show that the extension $\hat{C}$ is a linear, self-dual and 4-divisible code. This implies that C is also a linear code. Suppose that there are $\hat{c}_1, \hat{c}_2 \in \hat{C}$ such that $d(\hat{c}_1, \hat{c}_2) \neq 0 \bmod 4$. Then we can choose a component that we exclude, and we can find two elements in a $(23, 2^{12}, 7)$ code, whose distance is $= 1, 2 \bmod 4$, and this contradicts what we have proven before. So every Hamming distance in $\hat{C}$ is divisible with 4. As proven in the section dedicated to the self-dual codes, $\hat{C} \subset \hat{C}^\perp$, where we recall the fact that $A^\perp$ can be defined also for subsets, not only for subspaces. But $|\hat{C}| = 2^{12}$ and

$$\dim \hat{C}^\perp = \dim \langle \hat{C} \rangle^\perp \leq 24 - \dim \langle \hat{C} \rangle \leq 12,$$

we get $\hat{C}^\perp = \hat{C}$, so $\hat{C}$ is linear and C is linear. □

A similar proof works also for the $(11, 3^6, 5)$ ternary Golay code $Gol(11)$.

28 Low density parity check codes

This section deals with a family of binary codes. Consider a 2-party graph with vertex sets $V = \{x_1, \ldots, x_n\}$ and $W = \{y_1, \ldots, y_k\}$. The edges build a relation $E \subset V \times W$ because they connect vertexes from V with vertexes from W. One gets a binary check matrix $H = (h_{ij})$ by setting:

$$h_{ij} = 1 \longleftrightarrow (x_i, y_j) \in E.$$

This corresponds to a conjunction of linear conditions of the shape:

$$y_j = \sum_{(x_i, y_j) \in E} x_i = 0,$$

for $j = 1, \ldots, k$.

Definition 28.1 The 2-party graph is called (l, r) regular if every vertex $x \in V$ has degree l and every vertex $y \in W$ has degree r.

In this case the check matrix has k lines and n columns and one has the equality:

$$rk = nl.$$

Definition 28.2 For a subset $U \subseteq V$ we denote with ∂U the set:

$$\partial U = \{w \in W \,|\, w \text{ connected with } U\}.$$

Definition 28.3 A (l, r)-regular graph with $|V| = n$ is a $(n, l, r, \alpha, \delta)$-expander if:

$$\forall\, U \subseteq V \quad |U| \leq \alpha |V| \longrightarrow |\partial U| > \delta |U|.$$

Theorem 28.4 *Let E be a $(n, l, r, \alpha, \delta)$-expander such that $\delta \geq \frac{l}{2}$. Then the corresponding code $C(E)$ has minimal distance $d > \alpha n$ and consequently can correct $< \frac{\alpha n}{2}$ many errors.*

Proof: Recall that $nl = rk$. As $C(E)$ is determined by $k = \frac{nl}{r}$ equations, its dimension is:

$$\dim C(E) \geq n - \frac{nl}{r}.$$

Let $0 \neq v \in C(E)$. Consider the set $U = \{i \,|\, v_i = 1\}$. A number of $l|U|$ edges start in U. They end in $\geq \frac{l}{2}|U|$ many conditions. If $\text{wt}\,(v) \leq \alpha n$, there must be a condition that contains only one edge, because if not there would be less then $|U|/2$ conditions, and this contradicts with the property of being an expander. So a condition reads $y = v_j = 1$ and $v \notin C(E)$. Contradiction. □

Definition 28.5 For Low Density Parity Check Codes (LDPCC) one considers the following correction algorithm:

1. Compute all conditions for v.

2. Find x_i present in strictly more *false* conditions as in *correct* conditions. If there is no false condition, then stop.

3. Flip x_i in v. This means $v_i := 1 - v_i$.

4. Go to 1.

Theorem 28.6 *If $\delta = \frac{3}{4}l$ then the algorithm corrects $< \frac{\alpha n}{2}$ errors.*

Proof: Consider $v = (v_1, \dots, v_n)$ containing $< \frac{\alpha n}{2}$ errors. We say that the algorithm is in state (t, s) if there are t many errors and s many conditions are not verified. Supposed that we are in the state (t, s) with $t < \alpha n = \alpha |V|$. Let k be the number of correct conditions that contain corrupted values. As $\delta = \frac{3}{4}l$, one has:

$$s + k > \frac{3}{4}l,$$

because t corrupted values have edges to $s + k$ conditions.

In a correct condition with corrupted values, one has at least another corrupted value. In an incorrect condition, one has at least one corrupted value. So the number of conditions with corrupted variables fulfills:

$$lt \geq s + 2k.$$

All together:

$$tl \geq s + k + k > \frac{3}{4}lt + k,$$

and this yields:

$$k < \frac{1}{4}lt.$$

But as $s+k > \frac{3}{4}lt$, we get:

$$s > \frac{lt}{2}.$$

So there is a value such that more than half of its edges end in incorrect conditions. This value will be flipped. The value was not necessarily a corrupted one, but the number s becomes smaller by every flip, and that is what matters. □

29 Exercises

Exercise 1: *A* $[7,4,3]$ *Hamming code* C *has the following check-matrix:*

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

Find a generating matrix for this code.

The system $H\vec{x} = \vec{0}$ reads:

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

We define the parameters $(x_4, x_5, x_6, x_7) = (a, b, c, d) \in \mathbb{F}_2^4$. It follows:

$$\begin{aligned} x_1 &= a + b + d \\ x_2 &= a + c + d \\ x_3 &= b + c + d \end{aligned}$$

The general solution decomposes as follows:

$$\begin{pmatrix} a+b+d \\ a+c+d \\ b+c+d \\ a \\ b \\ c \\ d \end{pmatrix} = a \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + d \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

We have found a basis of the code C. The rows of the generating matrix are the basis vectors. So:

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

□

Exercise 2: *A* $[7,4,3]$ *Hamming code* C *has the following generating matrix:*

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

Find a check-matrix for this code.

A check-matrix H has 3 rows and 7 columns, such that $HG^T = 0$. Let a arbitrary row of H be:

$$(a, b, c, d, e, f, g).$$

We observe that the right-most 4×4 minor of G is the unit matrix, we can choose the parameters $(a, b, c) \in \mathbb{F}_2^3$. The general solution decomposes as follows:

$$\begin{pmatrix} a \\ b \\ c \\ a+b \\ a+c \\ b+c \\ a+b+c \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Taking for (a, b, c) the standard basis vectors, one finds three linear independent possible rows of the check-matrix. So we found:

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

Observe that neither the generating matrix, nor the check-matrix, are unique. □

Exercise 3: *Compute the error syndromes for one error in the* $[7, 4, 3]$ *Hamming code* C *of the last exercises.*

Consider the vectors $e_i \in \mathbb{F}_2^7$ given by:

$$e_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}.$$

containing only one 1 at position i. Using the known check-matrix H we get:

$$He_1 = (1, 0, 0) \quad He_2 = (0, 1, 0) \quad He_3 = (0, 0, 1)$$

$$He_4 = (1, 1, 0) \quad He_5 = (1, 0, 1) \quad He_6 = (0, 1, 1)$$

$$He_7 = (1, 1, 1)$$

□

Exercise 4: *Using the syndromes from the previous exercise, correct the word:*

$$\tilde{c} = (1, 1, 0, 0, 1, 1, 1).$$

We compute immediately:

$$H\tilde{c} = (1, 1, 1),$$

so the corrected word will be:

$$c = \tilde{c} + e_7 = (1, 1, 0, 0, 1, 1, 0).$$

□

Exercise 5: *A code C consists of* 4 *binary words of length* 4*. Show that this code can NOT be* 1*-error correcting.*

If it was 1-error correcting, the code would have $d \geq 3$. But $d = 4$ is impossible for length 4, because C would have at most 2 elements. So $d = 3$. However, any $(4, 4, 3)$ code contradicts the Hamming bound, because one has:

$$16 = 2^4 \leq |C|\big(1 \cdot (2-1)^0 + \binom{4}{1}(2-1)^1\big) = 4(1+4) = 20,$$

while the Hamming bound reads $16 \geq 20$ in this situation. □

Exercise 6: *Show that* ISBN10 *recognises any letter transposition.*

Let $(c_1, \dots, c_{10}) \in$ ISBN10. Let c'_k be the letters composing the word after a transposition (i, j). Suppose that both code words fulfill the conditions:

$$\begin{aligned} \sum_{k=1}^{10} kc_k &= 0 \mod 11 \\ \sum_{i=k}^{10} kc'_k &= 0 \mod 11 \end{aligned}$$

By subtracting the relations, we get: $(j-i)(c_i - c_j) = 0 \bmod 11$. But $\mathbb{Z}_{11}$ is a field and we get $c_i = c_j$ unless $i = j$. □

Exercise 7: *Show that there is no binary code with parameters* $(7, 8, 5)$*.*

If $d = 5$ then $e = 2$. By Hamming Bound:

$$2^7 \geq 2^3\big(1 + \binom{7}{1} + \binom{7}{2}\big) = 2^3\big(1 + 7 + \frac{7!}{2!5!}\big) = 2^3(1 + 7 + 21) = 2^3 \cdot 29,$$

so $16 \geq 29$, which is false. □

Exercise 8: *Show that there is no binary code with parameters* $(90, 2^{78}, 5)$*.*

If $d = 5$ then $e = 2$. By Hamming Bound:

$$2^{90} \geq 2^{78}\big(1 + \binom{90}{1} + \binom{90}{2}\big)$$

is equivalent with $4096 \geq 4096$. As it transform the Hamming Bound in equality, this code, if it exist, should be perfect. But this code is neither the binary Golay code because $23 \neq 90$, nor a Hamming code, because $d = 5$. So this code cannot exist. □

Exercise 9: *Show that there is no binary code P with parameters* $(90, 2^{78}, 5)$*, but without using the characterisation of the perfect codes.*

We may suppose that $0 \in P$. We consider the sets:

$$V = \{v = (v_1, \dots, v_{90}) \,|\, v_i \in \{0, 1\}, v_1 = v_2 = 1, d(v, 0) = 3\},$$
$$C = \{c = (c_1, \dots, c_{90}) \in P \,|\, c_1 = c_2 = 1, d(c, 0) = 5\},$$
$$A = \{(v, c) \,|\, v \in V, c \in C, \langle v, c\rangle = 1\}.$$

We compute in two different ways the cardinality of A.

$$\sum_{c \in C} |\, \{v \in V \,|\, \langle c, v\rangle = 1\} \,| = \sum_{c \in C} 3 = 3|\, C \,|$$

On the other hand, for some $v \in V$, at most one $c \in C$ has the property that $\langle c, v\rangle = 1$. Of course, if $c_1 \neq c_2$ would fulfill this condition, then $d(c_1, c_2) < 5$. But there must be at least one c, because else there would be less then 2^{78} codewords, so there is exactly one.

It follows $88 = 3|\,C\,|$, contradiction.

Exercise 10: *Let p be a prime number, $q = p^t$ and $n = (q^k - 1)/(q - 1)$ with $k \geq 2$. Let C be a linear code with parameters $[n, n-k, 3]$. Show that C is a Hamming code.*

Let $K = \mathbb{F}_q$, $C \leq K^n$, $\dim C = n - k$. C is the intersection of k many independent hyperplanes. If the hyperplane H_i has the equation:

$$a_{i1}v_1 + \cdots + a_{in}v_n = 0,$$

let $H = (a_{ij}) \in M_{k\times n}$ the matrix built by those coefficients. Of course,

$$c \in C \leftrightarrow Hc^T = 0.$$

C has $d = 3$ so every two columns of H are linear independent. So every two columns generate different lines in K^k. But there are n many columns, so for every line going through 0 in K^k, one has a column generating this line. So H is the check-matrix for the Hamming code. □

Exercise 11: *Let $n \geq 1$ and let C be the set of binary words of length n containing an even number of ones. Show that C is a linear code and analyze this code.*

The word 0^n belongs to C. Let $c_1, c_2 \in C$. If c_i contains an even number k_i of ones, and s is the number of positions at which both words contain ones, then $c_1 + c_2$ contains $(k_1 - s) + (k_2 - s) = k_1 + k_2 - 2s$ many ones, which is an even number. So C is a vector space.

The condition that determines the code words is:

$$c_1 + c_2 + \cdots + c_n = 0.$$

This means that the check matrix is the matrix $H = (1, 1, \ldots, 1)$ because:

$$(1, 1, \ldots, 1)\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

The minimal distance is $d(C) = \min \mathrm{wt}\,(c) = 2$ and the parameters of the code are $[n, n-1, 2]$. The code is 1-recognising and 0-correcting.

C is the image of the mapping $G : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$ given by:

$$G(x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, x_1 + x_2 + \cdots + x_{n-1}).$$

This can be written as $G(x) = \vec{x}G$ where G is the generating matrix:

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

with $n - 1$ rows and n columns.

□

Exercise 12: *Find parameters, check-matrix and generating matrix for the repetition code:*

$$C = \{(0, \ldots, 0), (1, \ldots, 1)\}.$$

The parameters are $[n, 1, n]$. The generating matrix is $G = (1, 1, \dots, 1) \in \mathbb{F}_2^n$, because the code words are xG with $x \in \{0, 1\}$. For a check-matrix, observe that the condition met by the code words is to satisfy the following system of $n - 1$ equations:

$$\begin{aligned} x_1 &= x_n, \\ x_2 &= x_n, \\ \dots &= \dots \\ x_{n-1} &= x_n, \end{aligned}$$

The corresponding check-matrix H has $n - 1$ rows and n columns:

$$H = \begin{pmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1 \end{pmatrix}$$

Exercise 13: *Over the field $K = \mathbb{F}_q$ let C be the code implicitly given by the condition $c_1 + c_2 + \dots + c_n = 0$. Study this code.*

The check-matrix is the vector $(1, 1, \dots, 1)$. We observe that the minimal distance is 2 because the words containing one 1 and one -1 have minimal weight. Also, 2 is the minimal number d such that every family of $d - 1$ columns of H is linear independent. The dimension of C is $n - 1$. All the following $n - 1$ vectors belong to C:

$$\begin{aligned} v_1 &= (1, -1, 0, \dots, 0, 0) \\ v_2 &= (0, 1, -1, \dots, 0, 0) \\ \vdots &= \qquad \vdots \\ v_{n-1} &= (0, 0, 0, \dots, 1, -1) \end{aligned}$$

From:

$$\alpha_1 v_1 + \dots + \alpha_{n-1} v_{n-1} = (\alpha_1, \alpha_2 - \alpha_1, \dots, \alpha_{n-1} - \alpha_{n-2}, -\alpha_{n-1}),$$

we deduce that those vectors are linear independent, so they build a basis. So they are the rows of a generating matrix G. The parameters of the code are $[n, n - 1, 2]$ as in the case of the binary codes. □

Exercise 14: *Show that the Reed-Solomon code is a maximum distance separable code. (MDS code)*

Recall the Singleton Bound:

$$d \le n - \log_q |C| + 1.$$

The Reed-Solomon Code with polynomials with degree $< k$ has parameters $[n, k, d]$ with $d = n - k + 1$. So:

$$n - k + 1 \le n - \log_q(q^k) + 1 = n - k + 1,$$

realizes the equality, so the code is MDS. □

Exercise 15: *Show that the Reed-Solomon code has the generating matrix:*

$$G_k = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \dots & a_n^{k-1} \end{pmatrix}.$$

For $k \leq n-1$ the application given by $x \rightsquigarrow xG$ from K^k to K^n generates the code. This matrix can be imbedded in the $n \times n$ matrix G_n which has determinant $\neq 0$ as a Vandermonde determinant. So G_k has maximal rank. (Also, G_k contains a Vandermonde minor, which is invertible.) □

Exercise 16: *Show that $RM(m-1, m)$ consists of all words with $\sum c_i = 0$.*

The parameters of the code are $[2^m, 2^m - 1, 2^{[m-(m-1)]}] = [2^m, 2^m - 1, 2]$. It follows that the code is a hyperplane, and the minimal distance is 2. For every monomial $x_{i_1} \dots x_{i_k}$, if we evaluate it in every point $(x_1, \dots, x_m) \in \{0, 1\}^m$, one gets an even mumber of values 1. It follows that only even code-words are present in $RM(m-1, m)$. Because of the dimension and of the minimal distance, there must be all of them and exactly them. □

Exercise 17: *Show that $RM(r, m)^\perp = RM(m - r - 1, m)$.*

We observe that:

$$n - \sum_{l=0}^{r} \binom{m}{l} = \sum_{l=0}^{m} \binom{m}{l} - \sum_{l=0}^{r} \binom{m}{l} = \sum_{l=r+1}^{m} \binom{m}{l} = \sum_{l=0}^{m-r-1} \binom{m}{l},$$

because $\binom{m}{l} = \binom{m}{m-l}$. It follows that those spaces have the same dimension.

Now take $x \in RM(r, m)$ and $y \in RM(m - r - 1, m)$. We consider the scalar product:

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

The code-word $xy = (x_1 y_1, \dots, x_n y_n)$ is the result of the evaluation in all points of a polynomial of degree less or equal $r + (m - r - 1) = m - 1$. So this code-word is an even weight word, so $\sum x_i y_i = 0$. □

Exercise 18: *Let m be odd and $r = (m-1)/2$. Show that $RM(r, m)$ is self-dual.*

It follows that $r = m - r - 1$ and we apply the previous exercise. □

Exercise 19: *Consider the following sequence of Hadamard matrices over the field $\mathbb{F}_2$, defined as follows: $H_0 = (0)$,*

$$H_{n+1} = \begin{pmatrix} H_n & H_n \\ H_n & H_n + U_n \end{pmatrix}$$

where the matrix $U_n \in M_{2^n \times 2^n}(\mathbb{F}_2)$ contains only the digit 1. Show that the rows of the matrix H_n build together the code $RM(1, n)$.

Exampes:

$$H_0 = (0), \qquad H_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad H_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

We show that the rows of H_n build a vector space of dimension n over $\mathbb{F}_2$. This is true for $n = 0$ and $n = 1$.

Suppose the claim true for n. Consider H_{n+1}. Let $u, v \in H_{n+1}$ be two rows.

Case 1: If u, v belong to the first half of H_{n+1}, there exist $u', v' \in H_n$ such that $u = (u', u')$ and $v = (v', v')$. By the hypothesis of induction, $u' + v' \in H_n$ so $u + v \in H_{n+1}$. Moreover, $u + v$ lies in the first half of the matrix.

Case 2: If u, v belong to the second half of H_{n+1}, there exist $u', v' \in H_n$ such that $u = (u', \vec{1} + u')$ and $v = (v', \vec{1} + v')$. By the hypothesis of induction, $u' + v' \in H_n$ so $u + v = (u' + v', u' + v') \in H_{n+1}$. Moreover, $u + v$ lies in the first half of the matrix.

Case 3: If $u = (u', u')$ comes from the first half of the matrix and $v = (v', \vec{1} + v')$ from the second hald, then the sum $u + v = (u' + v', \vec{1} + u' + v')$ is in H_{n+1} in the second half of the matrix.

It is immediate that all rows of H_n are pair-wise different, so the dimension is n.

If $B_n = \{x_1, \ldots, x_n\}$ is a basis of H_n, then $B_{n+1} = \{y_1, \ldots. y_n, y_{n+1}\}$ is a basis of H_{n+1}, where $y_i = (x_i, x_i)$ for $i = 1, \ldots, n$ and $y_{n+1} = (\vec{0}, \vec{1})$. We observe that for all n, if $u \in H_n \setminus \{0\}$, u contains an equal number of 0 and 1. So $\vec{1} \notin H_n$. We observe that H_n is the simpex code of length 2^n and minimal distance 2^{n-1}, which is also known as $RM(1, n)$. □

Exercise 20: *Let C be the Simplex Code with parameters $[2^k - 1, k, 2^{k-1}]$ over $\mathbb{F}_2$. Compute its weight-polynomial $A_C(x)$.*

Every $c \in C \setminus \{0\}$ has weight 2^{k-1}. So the polynomial is:

$$A_C(x) = 1 + (2^k - 1)x^{2^{k-1}}.$$

□

Exercise 21: *Find out the weight-polynomial of the $[n = 2^k - 1, n - k, 3]$ Hamming Code.*

We apply MacWilliams for the polynomial corresponding to the Simplex Code:

$$\begin{aligned} A_{C^\perp}(x) &= \frac{1}{2^k}\Big[(1+x)^n + n(1-x)^{2^{k-1}}(1+x)^{2^{k-1}-1}\Big] \\ &= \frac{1}{n+1}\Big[(1+x)^n + n(1-x)(1-x^2)^{\frac{n-1}{2}}\Big] \\ &= \frac{1}{n+1}\Big[\sum_{j=0}^{n}\binom{n}{j}x^j + n(1-x)\sum_{j=0}^{\frac{n-1}{2}}\binom{\frac{n-1}{2}}{j}(-1)^j x^{2j}\Big] \end{aligned}$$

We keep the coefficients $A_i^\perp$ and we get:

$$A_i^\perp = \begin{cases} \frac{1}{n+1}\Big[\binom{n}{i} + n(-1)^{\frac{i}{2}}\binom{\frac{n-1}{2}}{\frac{i}{2}}\Big] & i = 2s \\ \frac{1}{n+1}\Big[\binom{n}{i} + n(-1)^{\frac{i+1}{2}}\binom{\frac{n-1}{2}}{\frac{i-1}{2}}\Big] & i = 2s+1 \end{cases}$$

□

Exercise 22: *A code of length $n = 2k$ over $\mathbb{F}_q$ is self-dual. What can we say about the coefficients A_0, A_1 and A_2?*

$$A(x) = A^\perp(x) = q^{-k}\sum_{j=0}^{n} A_j(1-x)^j(1+(q-1)x)^{n-j} =$$

$$= q^{-k}\sum_{j=0}^{n} A_j[1 - jx + \binom{j}{2}x^2 + \ldots][1 + (n-j)(q-1)x + \binom{n-j}{2}(q-1)^2x^2 + \ldots]$$

The following was already known:

$$1 = A_0 = q^{-k}\sum_{j=0}^{n} A_j.$$

But the following are new:

$$\begin{aligned} A_1 &= q^{-k}\sum_{j=0}^{n} A_j((n-j)(q-1)-j) = \\ &= q^{-k}\sum_{j=0}^{n} A_j(n(q-1)-jq) = \\ &= n(q-1) - q^{-k+1}\sum_{j=0}^{n} jA_j. \end{aligned}$$

$$A_2 = q^{-k}\sum_{j=0}^{n} A_j(-j(n-j)(q-1) + \binom{j}{2} + \binom{n-j}{2}(q-1)^2).$$

□

Exercise 23: *Show that the weight polynomial of the* $[24,12,8]$ *extended Golay code is:*

$$A(x) = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}.$$

We know that C is 4-divisible. We also know that $A_{24-i} = A_i$. Indeed, because $C \subseteq C^{\perp}$, $0 = \langle c, c\rangle = \sum c_i^2 = \langle c, \vec{1}\rangle$. But n is even and C is self-dual, so $c \rightsquigarrow c + \vec{1}$ is a bijection. On the other hand $\mathrm{wt}\,(c) = n - \mathrm{wt}\,(c+\vec{1})$. So:

$$A(x) = 1 + Ax^8 + Bx^{12} + Ax^{16} + x^{24}.$$

We put $x = 1$ and find out that $2 + 2A + B = |C| = 2^{12} = 4096$.

On the other hand, the code is self-dual and we apply:

$$A_2 = 2^{-12}\sum_{j=0}^{n} A_j(-j(n-j)(2-1) + \binom{j}{2} + \binom{n-j}{2}(2-1)^2).$$

So $0 = A_2 = 2^{-12}[552 + 40A - 12B]$. This system of equations has the solution: $A = 759$, $B = 2576$. □

Exercise 24: *Show that the weight polynomial of the extended ternary* $[12,6,6]$ *Golay code is:*

$$A(x) = 1 + 264x^6 + 440x^9 + 24x^{12}.$$

The code is self-dual and 3-divisible, so $A(x) = 1 + Ax^6 + Bx^9 + Cx^{12}$. We apply the relations for self-dual codes and we deduce the following equations:

$$\begin{aligned} A + B + C &= 3^6 - 1 = 728 \\ 6A + 9B + 12C &= 5832 \\ 3A - 6B + 66C &= -264 \end{aligned}$$

By solving the system, we deduce the coefficients above. □

Exercise 25: *Consider the following check matrix:*

$$\begin{aligned} y_1 &= x_1 + x_2 + x_3 \\ y_2 &= x_4 + x_5 + x_6 \\ y_3 &= x_7 + x_8 + x_9 \\ y_4 &= x_1 + x_4 + x_7 \\ y_5 &= x_2 + x_5 + x_8 \\ y_6 &= x_3 + x_6 + x_9 \end{aligned}$$

(a) Show that this check matrix corresponds to a $(9, 2, 3, \frac{2}{9}, \delta)$*-expander for* $\delta < \frac{2}{3}$.

(b) Deduce that the code C *has minimal distance* $d \geq 3$.

(c) Correct the word $v = (0, 0, 1, 1, 1, 0, 0, 1, 1)$.

(a) $n = 9$, $(l, r) = (2, 3)$, $\alpha = \frac{2}{9}$.

(b) $\delta < \frac{3}{2} = \frac{3}{4}l$. We apply the Theorem. It follows that $\dim C \geq 3$ and $d > \alpha n = 2$ so $d \geq 3$.

(c) We observe that $y_1 = 1$ and $y_4 = 1$. Also $\{1, 2, 3\} \cap \{1, 4, 7\} = \{1\}$. So x_1 occurs in two incorrect conditions and in none correct condition. We flip x_1. The vector $(1, 0, 1, 1, 1, 0, 0, 1, 1)$ verifies all conditions. □