CODING THEORY

ELISA LORENZO GARCÍA

Contents

1. Lecture 4

1.1. Cyclic codes.

Definition 1.1. the cyclic shift of a word $(c_0, c_1, .., c_{n-1}) \in \mathbb{F}_q^n$ is defined by $\sigma(c) = (c_{n-1}, c_0, c_1, .., c_{n-2})$.

Definition 1.2. C an $\mathbb{F}_q$-linear code is cyclic if $\sigma(c) \in C$ for all $c \in C$.

Example 1.3. The $\mathbb{F}_7$-code given by the generator matrix $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix}$ is cyclic since $\sigma(g_1) = g_1$, $\sigma(g_2) = 5g_2$ and $\sigma(g_3) = 4g_3$.

Proposition 1.4. *The dual of a cyclic code is again cyclic.*

Proof. $\sigma(x)c = x\sigma^{n-1}(c) = 0$ for all $c \in C$ then $\sigma(x) \in C^{\perp}$. □

Definition 1.5. $\mathbb{C}_{q,n} = \mathbb{F}_q[x]/(x^n - 1)$

Let us consider $\phi : \mathbb{F}_q^n \to \mathbb{C}_{q,n} : c \mapsto c_0 + c_1x + ... + c_{n-1}x^{n-1}$. We also denote $\phi(c)$ by $c(x)$.

Proposition 1.6. *ϕ is an isomorphism of vector spaces. It defines a one-to-one correspondence between ideals of $\mathbb{C}_{q,n}$ and cyclic codes in $\mathbb{F}_q^n$.*

Proof. $\phi(e_i) = x^i$, ϕ is given by the identity in the basis $\{e_i\}$ and $\{x_i\}$. Let I be an ideal in $\mathbb{C}_{q,n}$. Let $C = \phi^{-1}(I)$. Then C is a linear code. Let $c \in C$, then $c(x) = \phi(c) \in I$ and $x \cdot c(x) \in I$ and $xc(x) = x(c_0 + c_1x + ... + c_{n-1}x^{n-1}) = c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}$. So $\sigma(c) = \phi^{-1}(xc(x)) \in C$ and C is cyclic.

Conversely, $I = \phi(C)$ with C cyclic. then I is closed under addition, and for all $i \in \{0, ...n-1\}$, if $\phi(c) \in I$ then $x^i\phi(c) = \phi(\sigma^i(c)) \in I$. □

$\mathbb{F}_q[x]$ is a principal ideal domain, hence all ideals are generated by one element. It's unique if monic. And for $\mathbb{C}_{q,n}$ if we take it of minimal degree. Such polynomial it's called the generator polynomial of C.

Example 1.7. The generator polynomial of $\mathbb{F}_q^n$ is 1 and of $\{0\}$ is $x^n - 1$. The repetition code and its dual have as generators polynomials $x^{n-1} + ... + x + 1$ and $x - 1$ respectively. Recall that for the repetition code we have

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

Proposition 1.8. *$g(x) \in \mathbb{F}_q^n$ monic is a generator polynomial iff $g \mid x^n - 1$*

Proof. the ideal also contain $x^n - 1$, so the generator divides the gcd of the other polynomial and $x^n - 1$. □

Example 1.9. $(x^3+x+1)(x^5-x^3-x^2+x-1) = x^8-1 \in \mathbb{F}_3[x]$ So the first one generates a ternary cyclic code of length 8.

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

the other shifted vectors are linear combination of this ones. Hence, $k = 5$. We compute

$$red(G) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

and the parity check one

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

and we find $d = 3$.

Proposition 1.10. *For a cyclic code* $\deg(g) = n - k$.

Proof. Generated by $< g, xg, ..., x^{k-1}g >$ and the matrix generated by

$$\begin{pmatrix} g_0 & g_1 & g_2 & ... & ... & ... & 0 \\ 0 & g_0 & g_1 & ... & ... & ... & 0 \\ ... & ... & ... & ... & ... & ... & 0 \\ 0 & 0 & 0 & ... & g_0 & ... & g_l \end{pmatrix}$$

has rank at least l. □

Definition 1.11. $h(x) = \frac{x^n-1}{g(x)}$ is called the parity check polynomial of C.

Proposition 1.12. *$c(x) \in C$ iff $c(x)h(x) = 0$*

Proof. $c(x) \in C$ iff $c(x) \in (g(x))$ iff $c(x)h(x) = 0$. □

Proposition 1.13. *$\tilde{h}$, the monic reciprocal of h, is the generator polynomial of $C^\perp$*

Proof. If $k = 0$ or n, then $g = x^n - 1$ or 1 and it is true. Otherwise, $g = g_0 + g_1 x + ... + g_{n-k}x^{n-k}$, $h = h_0 + ... + h_k x^k$ and for $t \neq 0, n$ we have $\sum_i g_i h_{t-i} = 0$. In particular $g_0 h_k + g_1 h_{k-1} + ... = 0$ and $\tilde{h} \in C^\perp$, by a dimension argument we have the equality. □

Example 1.14. [6, 3] cyclic code over $\mathbb{F}_7$ with $g(x) = x^3 + 3x^2 + x + 6$. Then $h(x) = x^3 + 4x^2 + x + 1$. Then $g^\perp(x) = x^3 + x^2 + 4x + 1$ and

$$G^\perp = H = \begin{pmatrix} 1 & 4 & 1 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 1 & 0 \\ 0 & 0 & 1 & 4 & 1 & 1 \end{pmatrix},$$

and $d = 4$.

Definition 1.15. Let α a primitive root of $x^n - 1$ over an extension $\mathbb{F}_q^m$ of $\mathbb{F}_q$ (we assume $p \not| n$), then $Z(C) := \{i \in \mathbb{Z}_n \mid c(\alpha^i) = 0 \, \forall c \in C\}$.

Proposition 1.16. $g(x) = \prod_{i \in Z(C)}(x - \alpha^i)$

Proof. Write $g(x) = \prod_{i \in Z_g}(x - \alpha^i)$ $c(x) = a(x)g(x)$ then $c(\alpha^i) = 0$ for all $in \in Z(C)$ then $Z_g \subseteq Z(C)$.

We have $g(x) \in C$, then $g(\alpha^i) = 0$ for all $i \in Z(C)$ then $Z(C) \subseteq Z_g$. □

Proposition 1.17. $Z(C^\perp) = \mathbb{Z}_n / \{-i \mid i \in Z(C)\}$

Proof. $h(x) = \frac{x^n - 1}{g(x)}$ and $g^\perp(x) = \tilde{h}(x)$ □

1.2. **BCH Bound: Bose-Chaudhuri-Hocquenghem.**

Proposition 1.18. *Let C be a cyclic code that has at least $\delta - 1$ consecutive elements in $Z(C)$ modulo n, then $d \geq \delta$.*

Proof. Let I be the defining set for a cyclic code C, then $c(\alpha^i) = 0$ for all $i \in I$. Let $\tilde{H}$ be the $\#I \times n$ matrix α^{ij}. Let $\tilde{C}$ be the $\mathbb{F}_q^m$-linear code with parity check matrix $\tilde{H}$. Then C is the restriction of $\tilde{C}$ and any bound of the minimum distance for $\tilde{C}$ holds for C.

For our case: $(\alpha^{ij} \mid b \leq i \leq b + \delta - 2, 0 \leq j \leq n)$ is a parity check matrix of a code $\tilde{C}$ that has C as a subfield code. $\tilde{C}$ is equivalent to the one with parity check matrix $(\alpha^{ij} \mid 0 \leq i \leq \delta - 2, 0 \leq j \leq n)$. As a generator matrix of the dual we get an MDS code as in example **??**. So with parameters $[n, \delta - 1, n - \delta - 2]$, so for the dual $[n, n - \delta + 1, \delta]$. □

Definition 1.19. a cyclic code with defining set $\{b, b + 1, ..., b + \delta - 2\}$ is called a BCH code with designed minimum distance δ. It's called narrow sense if $b = 1$ and primitive if $n = q^m - 1$.

Definition 1.20. δ_{BCH} = largest integer $\delta \leq n + 1$ such that there is a subset of $Z(C)$ consisting on $\delta - 1$ elements that are consecutive of some period modulo n.

Example 1.21. $n = 17$, $q = 2$. $Z_\alpha = \{1, 2, 4, 8, 9, 13, 15, 16\}$ has $\delta = 3$ because at most 2 consecutive ones, but $Z_{\alpha^6} = \{3, 5, 6, 7, 10, 11, 12, 14\}$ (we multiply by 3) has $\delta = 4$. Actually, $\delta_{BCH} = 4$.

Theorem 1.22. $d \geq \delta_{BCH}$

The APGZ (Arimoto-Peterson-Gorenstein-Zierler) decoding algorithm for cyclic codes. It efficiently corrects errors of weight at most $w \leq (\delta - 1)/2$, even if the minimum distance bigger than δ. You use the information you are sure you have to give a linear system $w \times w$ that describe the errors.

1.3. **Polynomial Codes.**

Definition 1.23. (Reed-Solomon Codes) $\alpha \in \mathbb{F}_q$, primitive, $n = q-1$. $0 \leq b, k, \leq n$. $g_{b,k}(x) = (x-\alpha^b)...(x-\alpha^{b+n-k-1})$.

$RS_k(n,b)$ is the q-ary cyclic code with generator $g_{b,k}$.

Proposition 1.24. *$RS_k(n,b)$ has length $n = q-1$, is cyclic, linear and MDS of dim. k. Moreover, $(RS_k(n,b))^\perp = RS_{n-k}(n, n-b+1)$.*

Proof. $n = q-1$, cyclic and linear by definition. $\deg g_{b-k}(x) = n-k$, then dimension k.

$U + \{b, b+1, .., b+n-k-1\}$ def. set, then by BCH bound $d \geq n-k+1$ and by the Singleton bound equal. Then MDS.

For the dual we get the def. set $\mathbb{Z}_n/U = \{n-b-1, ..., n-b+k\}$ then $RS_{n-k}(n, n-b+1)$. □

Applications: for CD's, it was the first use of strong error correction coding in a mass-produced consumer product. Also for two-dimensional bar codes.

Definition 1.25. $f(x) \in \mathbb{F}_q[x]$, $ev(f(x)) = (f(1), f(\alpha), ..., f(\alpha^{n-1}))$

Proposition 1.26. $RS_k(n,b) = \{ev(x^{n-b+1}f(x)) \mid f(x) \in \mathbb{F}_q[x], \deg(f) < k\}$

Proof. $ev(x^{n-b+1}x^i) = (1, \alpha^{n-b+1+i}, ..., \alpha^{(n-1)(n-b+1-i)})$

The parity check matrix is $H = (\alpha^{ij} \mid b \leq i \leq b-n+k-1, 0 \leq j \leq n-1)$ that is the generator matrix of the dual $RS_{n-k}(n, n-b+1)$. □

Example 1.27. Consider $R_3(7,1)$. It is a cyclic code over $\mathbb{F}_8$ with generator polynomial $g_{1,3}(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$ where $\alpha^3 = \alpha + 1$. So it is the code in exercise 3.6 with

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{pmatrix}.$$

In the second description we have: $RS_3(7,1) = \{ev(f(x)) \mid f(x) \in \mathbb{F}_8[x], \deg(f) < 3\}$ and we find the 3 rows of G by taking the basis of $\mathbb{F}_8[x]_{<3}$ given by $1, x, x^2$.

1.4. **Reed-Solomon decoder.** Let $c = (f(x_1), ..., f(x_n))$ with $\deg f < k$. Let $r \in \mathbb{F}_q^n$ with $d(r,c) \leq t$. x and r are known. We want to compute c (or f).

(1) Let $P = P_0(x) + P_1(x)y \in \mathbb{F}_q[x,y]$ such that $\deg P_0 < n-t$, $\deg P_1 < n-k-t$ and for all $i \in \{1, ..., n\}$, $P(x_i, r_i) = 0$.
(2) If $t \leq \frac{n-k}{2}$, then $f = -\frac{P_0}{P_1}$.

Proof. $\deg(P(x, f(x))) < n-t$ but it has at least $n-t$ roots, so it is zero. □

Definition 1.28. (Generalized Reed-Solomon codes)

$$GRS_k(a,b) = \{ev_{k-r,a}(f(x)) * b \mid f(x) \in \mathbb{F}_q[x], \deg(f) < k\}$$

There is also a generalization for the decoding algorithm.

Definition 1.29. (Alternant codes)

$$ALT_r(a,b) = \mathbb{F}_q - \text{linear restriction of } (GRS_r(a,b))^\perp$$

Proposition 1.30. *Every linear code with $d \geq 2$ is an alternant code.*

Proof. See Proposition 5.3.4 in Pellikaan, Wu, Bulygin, Jurrius book "Codes, Cryptology and Curves with Computer Algebra". □

RS $\subseteq$ BCH $\subseteq$ cyclic $\subseteq$ poly. $\subseteq$ linear
Goppa $\subseteq$ alternant $\subseteq$ linear
RS $\subseteq$ RM
RS $\subseteq$ GRS

Definition 1.31. ((classical) Goppa codes, or polynomial ones) $L = (a_1, .., a_n)$, $a_i \in \mathbb{F}_q^m$. $g \in \mathbb{F}_q^m[x]$ such that $g(a_i) \neq 0$.

$$\Gamma(L, g) = \{c \in \mathbb{F}_q^m \mid \sum \frac{c_i}{x - a_j} \equiv 0 \bmod g(x)\}$$

Proposition 1.32. $\Gamma(L, g) = ALT_r(a, b)$ *with* $b_j = \frac{1}{g(a_j)}$

def2

Definition 1.33. (q-ary Reed-Muller code) Let $P = \{P_1, ..., P_n\}$ be an enumeration of the elements of $\mathbb{F}_q^m$ with $n = q^m$. Let $0 \leq r \leq m(q-1)$

$$RM_q(r, m) = \{ev_P(f) \mid d \in \mathbb{F}_q[x_1, .., x_m], \deg(f) \leq r\}$$

2. Lecture 5

2.1. **Algebraic Geometry Goppa codes.** Let X be an absolutely irreducible non-singular projective curve over $\mathbb{F}_q$. Let $P_1, .., P_n$ be rational points on X. Set $D = P_1 + ... + P_n$. Let G another rational divisor that has support disjoint with D and such that $2g - 2 < \deg G < n$ (this last condition is not really necessary).

Definition 2.1. (Algebraic-geometry code or geometric RS code)

$$C_L(D, G) = \{(f(P_1), ..., f(P_n)) | f \in \mathcal{L}(G)\}.$$

Theorem 2.2. *The code $C_L(D, G)$ has dimension $k = \deg(G) - g + 1$ and minimum distance $d \geq n - \deg(G)$.*

Theorem 2.3. *(Riemann-Roch) Let D be a divisor on a non-singular projective curve of genus g, then for any canonical divisor K we have*

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1$$

Corollary 2.4. *(1)* $\deg(K) = 2g - 2$
(2) If $\deg(D) > 2g - 2$ *then* $\ell(D) = \deg(D) - g + 1$

Proof. If $f(P) = 0$ then $f \in \mathcal{L}(G - D)$ but $\ell(G - D) = 0$ because $\deg(G - D) < 0$ and $\deg(G) > 2g - 2$ so $\ell G = \deg(G) - g + 1$.

If $f(P)$ has weight d then it is in $\mathcal{L}(G - E)$ where $E = P_{i_1} + ... + P_{i_{n-d}}$, so $\deg(G - E) \geq \mathrm{def}(f) = 0$, hence $\deg(G) - n + d \geq 0$ □

Definition 2.5. Let D be a divisor on a curve X. We define

$$\Omega(D) = \{\omega \in \Omega^1(X) \mid (\omega) - D \geq 0\},$$

and we denote its dimension by $\delta(D) = \ell(K - D)$ (there is an isomorphism between both vector spaces sending f to $f\omega$) called the index of speciality of D.

Definition 2.6. $(\omega) = \sum_{P \in X} v_P(\omega) P$. $\omega = f \, \mathrm{d}\, t$, $f = \sum a_i t^i$, then $\mathrm{Res}_P(\omega) = a_{-1}$ and we have that $\sum_{P \in X} \mathrm{Res}_P(\omega) = 0$.

Definition 2.7. The linear code $\mathcal{C}_\Omega(D, G)$ of length n over $\mathbb{F}_q$ is the image of $\Omega(G - D)$ by the linear map $\mathrm{Res}_P(\eta) = (\mathrm{Res}_{P_1}(\eta), ..., \mathrm{Res}_{P_n}(\eta))$.

Theorem 2.8. *The code $\mathcal{C}_\Omega(D, G)$ has dimension $k^* = n - \deg(G) + g - 1$ and minimum distance $d^* \geq \deg(G) - 2g + 2$.*

Proof. If $\mathrm{Res}_P(\eta) = 0$ then $\eta \in \Omega()$ and ... $\delta(G-D) = \ell(K-G+D) = 2g-2+n-\deg(G)-g+1$. □

Example 2.9. Let $L = (\alpha_1, ..., \alpha_n)$ be a set of n distinct elements of $\mathbb{F}_{q^m}$. Let $g \in \mathbb{F}_{q^m}[x]$ not zero at the α_i. The classical Goppa code $\Gamma(L, g)$ is defined as

$$\{c \in \mathbb{F}_q^n \mid \sum \frac{c_i}{x-\alpha_i} \equiv 0 \bmod g\}.$$

Let us take $X = \mathbb{P}^1$, $P_i = (\alpha_i : 1)$, $Q = (1:0)$, $D = P_1 + ... + P_n$ and E the divisor of zeros of g. Then $\Gamma(L, g) = C_\Omega(D, E-Q)$.

Theorem 2.10. *The codes $C_L(D, G)$ and $C_\Omega(D, G)$ are dual codes.*

Proof. First notice that $k + k^* = n$. Now let $f \in \mathcal{L}(G)$ and $\eta \in \Omega(G-D)$. Let us check that the inner product of their images is 0. The differential $f\eta$ has no poles except maybe at the P_i and with residue $f(P_i)\,\mathrm{Res}_{P_i}(\eta)$. Then $\sum_{P_i} f(P_i)\,\mathrm{Res}_{P_i}(\eta) = \sum_{P \in X} f(P_i)\,\mathrm{Res}_{P_i}(\eta) = 0$ □

Theorem 2.11. *(Hasse-Weil-Serre bound) Let X be a curve of genus g over $\mathbb{F}_q$. Let $N_q(X)$ denote the number of $\mathbb{F}_q$-rational points on X. Then*

$$\mid N_q(X) - q - 1 \mid \leq g\lfloor 2\sqrt{q} \rfloor$$

Let X be a non-singular genus g curve over $\mathbb{F}_q$. Then an algebraic geometric code satisfy $k + d \geq n + 1 - g$. For the information rate $R = k/n$ and the relative minimum distance $\delta = d/n$ we have $R + \delta \geq 1 - \frac{g-1}{n}$. In order to construct asymptotically good codes we need curves with low genus and many $\mathbb{F}_q$-rational points.

Definition 2.12. A sequence of curve $\{X_m\}$ over $\mathbb{F}_q$ is called asymptotically good if $\lim_{m\to\infty} N_q(X_m) = \infty$, $\lim_{m\to\infty} g(X_m) = \infty$ and $\lim_{m\to\infty} \frac{N_q(X_m)}{g(X_m)}$ exists and is positive.

Theorem 2.13. *(Tsfasman-Vladut-Zink bound) Let q be a square. For every R, there exists an asymptotically good sequence of codes C such that $R(C) + \delta(C) \geq 1 - \frac{1}{\sqrt{q}-1}$*

Proof. (idea) Drinfeld-Vladut bound plus modular curves. □

García-Stichtenoth towers.
Serre book and https://manypoints.org/

Example 2.14. $X : y^2 + y = x^3$ over $\mathbb{F}_4$ is an elliptic curve with $g(C) = 1$. $\mathbb{F}_4 = \mathbb{F}_2[w]$ with $w^2 + w + 1 = 0$.

Let us take $Q = (0:1:0)$ and $P = \{P_1, .., P_8\}$ with $P_1 = (0:0:1)$, $P_2 = (0:1:1)$, $P_3 = (1:w:1)$, $P_4 = (1:w^2:1)$, $P_5 = (w:w:1)$, $P_6 = (w:w^2:1)$, $P_7 = (w^2:w:1)$ and $P_8 = (w^2:w^2:1)$. We take $G = 5Q$, then $\mathcal{L}(G) =< 1, x, y, x^2, xy >$. The code $C_L(D, G)$ is generated by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & w & w & w^2 & w^2 \\ 0 & 1 & w & w^2 & w & w^2 & w & w^2 \\ 0 & 0 & 1 & 1 & w^2 & w^2 & w & w \\ 0 & 0 & w & w^2 & w^2 & 1 & 1 & w \end{pmatrix}$$

we have $n = 8$, $k = 5$ and $d = 3 (\leq n - k = 3$ and $\geq n - \deg(G) = 3)$.

We have $\Omega^1(X) = \langle dx \rangle$, and then $\Omega(G-D) \simeq \mathcal{L}(D-G)$ and $\ell(D-G) = 3 - 1 + 1$ and actually $\mathcal{L}(D-G) = \langle \frac{1}{x(x-1)(x-\omega)}, \frac{1}{x(x-1)(x-\omega^2)}, \frac{1}{(x-1)(x-\omega)(x-\omega^2)} \rangle$ so we get the code

generated by (we take y/x^2 for the uniformizer of P_1 and P_2, $x-1$ for P_3 and P_4, $x-\omega$ for P_5 and P_6, etc.)

$$\begin{pmatrix} -\omega^2 & \omega^2 & \omega & \omega & 1 & 1 & 0 & 0 \\ -\omega & \omega & \omega^2 & \omega^2 & 1 & 1 & 0 & 0 \\ 0 & 0 & * & * & * & * & * & * \end{pmatrix}$$

with $n = 8$, $k = 3$ and $d = 5$.

2.2. **Some crypto.** Nowadays mostly all ciphering schemes are based on difficult problems on Number Theory, like integers factorization (RSA) and the discrete logarithm problem (Diffie-Hellman, El Gammal).

(1) 1982: Feynman noticed that some quantum phenomenon can not be reproduce by a computer.
(2) 1994 Shor propose a quantum algorithm that factors an integer N in $log(N)$ operations.
(3) 1996: Grover gives a quantum algorithm for finding an element in an unsorted list of length N in $O(\sqrt{N})$ operations.

In 2007, the NIST call for post-quantum cipher schemes. Those ones are based on:

(1) Euclidean lattices
(2) Rank Metric Codes
(3) Hamming Metric Codes
(4) Elliptic curves isogenies
(5) Polynomial systems of equations

Advantages: ciphering and deciphering very fast, 5 and 150 times faster than RSA. Post-quantum.
Disadvantages: huge public keys.

2.3. **The McEliece Cryptosystem.**

(1) $\mathcal{F}$ is a set of codes of dimension k in $\mathbb{F}_q^n$
(2) $\mathcal{S}$ is a set of "secrets" with a sujertive map $\mathcal{C} : \mathcal{S} \to \mathcal{F}$
(3) We associate to each $s \in \mathcal{S}$ an algorithm $\mathcal{D}(s)$ that corrects t errors for $\mathcal{C}(s)$.

The scheme:

(1) Secret key: $s \in \mathcal{S}$ with generator matrix G
(2) Alice take a random invertible S and permutation matrix P
(3) Private key: (S, G, P)
(4) Public key: the basis $G' = SGP$ of $\mathcal{C}(s)$
(5) Encryption: Bob wants to send the message m to Alice, he takes $c = mG' \in \mathcal{C}(s)$ and a random e of weight t. He produces $y := c + e$.
(6) Alice receives y.
(7) Decryption: $c' = cP^{-1}$
(8) apply $\mathcal{D}(s)$ to c' ir order to find m'.
(9) she computes $m = m'S^{-1}$.

It has been used in the secure of an Instant Messenger, but the public key size is really a problem.

Example 2.15. Suppose $\int$ equals to the $[7,4,3]$ Hamming code, and the public key is the generator matrix

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

Alice want to send the message $m = (1,0,1,1)$ to Bob. Bob create an invertible matrix S and a random permutation matrix P that will keep secret.

$$S = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \; P = (1264753)$$

Bob gives the public key $G_1 = SGP$. Alice generates a random error vector $e = (0,1,0,0,0,0,0)$. Then $y = mG_1 + e = (0,0,0,1,1,0,0)$ is sent.

Bob needs to decrypt: $y_1 = yP^{-1} = (0,0,1,0,0,0,1)$. By applying the parity check matrix and changing the corresponding bit, it yields $x_1 = (0,0,1,0,0,1,1)$. Bob solves now $x_0 G = x_1$. $x_0 = (0,0,1,0)$. Bob finally gets $x = x_0 S^{-1} = (1,0,1,1)$ that was the original message.

3. Exercises

Exercise 3.1. The Hamming $[7,4,3]_2$-code is non-cyclic but equivalent to a cyclic one.

Exercise 3.2. Prove that the code over $\mathbb{F}_q$ generated by

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

is not cyclic.

Exercise 3.3. Let C be a cyclic code over $\mathbb{F}_q$ of length 7 such that $(1,1,1,0,0,0,0)$ is an element of C. Show that C is a trivial code if q is not a power of 3.

Exercise 3.4. Find the generator matrix of the binary cyclic code of length 7 generated by $1 + x + x^5$.

Exercise 3.5. Show that $2 + x^2 + x^3$ is the generator polynomial of a ternary cyclic code of length 13.

ex:RS

Exercise 3.6. Let $\alpha \in \mathbb{F}_8$ such that $\alpha^3 = \alpha + 1$. Let the generator matrix be

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{pmatrix}.$$

Show that this code is cyclic and compute the generator polynomial.

Exercise 3.7. Prove the equivalence of definitions 1.9 in Lecture 3 and 1.33.

Elisa Lorenzo García, Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.

Email address: elisa.lorenzogarcia@univ-rennes1.fr