Introduction to Coding Theory

Post-Quantum Cryptography in Bilbao 23-27 June, 2025,
@BCAM, Basque Center for Applied Mathematics

imUVa Instituto de Investigación en Matemáticas
Universidad de Valladolid

Edgar Martínez-Moro

Institute of Mathematics, University of Valladolid

edgar.martinez@uva.es

Outline

This minicourse on coding theory serves as a preparatory session for the main lecture Code-Based Cryptography by Philippe Gaborit (Université de Limoges), scheduled for Wednesday. It is designed to provide some background in classical coding techniques relevant to cryptographic applications. We will review fundamental algebraic codes, with special attention to evaluation codes such as Reed-Solomon and also to cyclic codes. The session will also introduce Low-Density Parity-Check (LDPC) codes, emphasizing their structure. Key decoding strategies for both algebraic and LDPC codes will be discussed. This course aims to equip participants—especially those less familiar with coding theory—with some tools to better follow and engage with the material in the main course.

Introduction to error correcting codes

* Digital communications cannot avoid errors
* How can one store information so that a flip can be corrected?

THIS WAS THE ORIGINAL PROBLEM.

SIMPLE ANSWER: Repeate it three times. Efficiency $1/3$

MORE ELABORATE: $\boxed{\text{Hamming solution.}}$

Break bits in size $\underline{4}$ blocks and encode them as a $\underline{7}$ bit string

$$G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \qquad \overline{m} = (m_1, m_2\, m_3\, m_4) \longmapsto \overline{m} \cdot G$$

FACT 1 If $\bar{m} \neq \bar{m}'$, then $\bar{m}G$ and $\bar{m}'G$ differ in at least three coordinates

Proof will come later.

$\Downarrow$

$\boxed{\text{One can correct one error}}$ why?

This motivates the following defn's on distances / metric

BASIC DEFINITIONS Alphabet $\mathcal{A}$ of size q, ambient space $\underbrace{\mathcal{A}^n}_{\text{both codewords \& their corrupts.}}$

Hamming distance $\bar{x}, \bar{y} \in \mathcal{A}^n$

$$d_H(\bar{x}, \bar{y}) = \#\{ i \mid x_i \neq y_i \quad i = 1, \dots, n \}$$

Hamming weight $\bar{x} \in \mathcal{A}^n$ $\quad w_H(\bar{x}) = d_H(\bar{x}, \bar{0})$

A **code** $\mathcal{C}$ is just a subset $\mathcal{C} \subseteq A^n$ and its **minimum distance** is

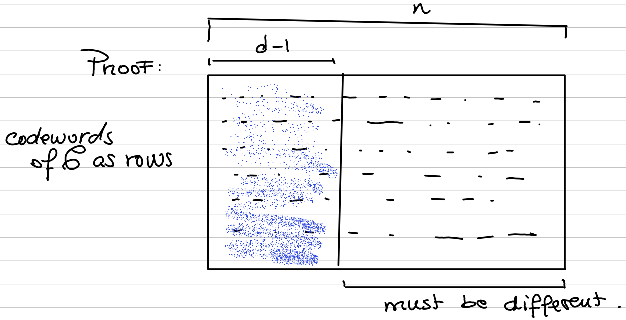
$$d(\mathcal{C}) = \min_{\substack{\bar{x}, \bar{y} \in \mathcal{C} \\ \bar{x} \neq \bar{y}}} \{ d_H(\bar{x}, \bar{y}) \}$$

FACT 2

$$|\mathcal{C}| \leq q^{n - d(\mathcal{C}) + 1}$$

$\boxed{\text{SINGLETON BOUND}}$

Proof:



Fact 3

$\mathcal{C}$ has minimum distance $d(\mathcal{C}) = 2t+1 \iff$

$\iff \mathcal{C}$ is $2t$ error detecting

$\iff \mathcal{C}$ is t error correcting.

NOTATION: q = size of A, n = block length, k : message length $\Downarrow$ $|\mathcal{C}| = q^k$

d = minimum distance of $\mathcal{C}$.

$(n,k,d)_q$ code or $[n,k,d]_q$ code if it is linear.

Rate: k/n Relative distance $\delta = d/n$

$$SB \Rightarrow q^k \le q^{n-d+1} \Longrightarrow \boxed{k \le n-d+1} \qquad \frac{k}{n} \le 1 - \delta + \frac{1}{n}$$

If $=$ is MDS code

PROOF FACT 1

DUAL CODE & PARITY CHECK MATRIX.

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

a) $\{ \bar{x} G \mid \bar{x} \in \mathbb{F}_2^4 \} = \{ \bar{y} \mid \bar{y} H = \bar{0} \}$

b) If $H_{i\bullet}$ is the ith row of H

$$y H = \sum_{i / y_i \neq 0} H_{i\bullet}$$

If $\left\{ \begin{array}{l} w_H(\bar{y}) = 2 \\ \bar{y} \in \mathcal{C} \end{array} \right.$ $\iff$ $H_{i_1\bullet} = H_{i_2\bullet}$ $\exists\, i_1 \neq i_2$

which is not the case $\blacksquare$

Decoding (1 error) $\bar{e} = (0, \ldots, \overset{i}{1}, \ldots 0)$

$\bar{c} \in \mathcal{C}$ $\quad \bar{c} + \bar{e} \rightsquigarrow (\bar{c} + \bar{e}) H = \bar{c} H + e H = H_{i\bullet}$

If $\mathcal{C}$ is a linear code (linear subespace of $\mathbb{F}_q^n$) of dimension k then a $n \times (n-k)$ matrix H of rank $(n-k)$ such that $\bar{y} H = 0 \;\forall \bar{y} \in \mathcal{C}$ is called a PARITY CHECK MATRIX. The $[n, n-k, \cdot]_q$ code generated by the colums of H is THE DUAL CODE of $\mathcal{C}$, $\mathcal{C}^{\perp}$.

Note that it is possible that $\mathcal{C} \cap \mathcal{C}^{\perp} \neq \{0\}$ and $\mathcal{C} = \mathcal{C}^{\perp}$.
(selfdual code)

EXAMPLE: $\mathcal{C} = \{(0,1,1,0),(0,0,0,0)\}$ is a $[4,1,2]_2$ code.

$\mathcal{C}^{\perp} = \{(0,1,1,0)\ (1,1,1,0),\ (0,1,1,1)\ (1,0,0,1),\ (1,0,0,0)$
$(0,0,0,1),\ (1,1,1,1)\ (0,0,0,0)\}$ is a $[4,3,1]_2$ code

GENERALIZED HAMMING CODES

$\ell \in \mathbb{Z}_{>0}$

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

$2^{\ell-1} \times \ell$ matrix.

Parity check of the ℓ-th Hamming code.

$$R \longrightarrow 1 \quad \text{as} \quad n \to \infty$$

BUT WE WANT LARGER d!

ALGEBRAIC CODES

REED-SOLOMON CODES (1960)

Specifications

- $A = \mathbb{F}_q$
- n, k with $n < q$
- $\bar{a} = (\alpha_1, \dots, \alpha_n)$ distinct elements in $\mathbb{F}_q$

A message $(m_0, \dots, m_{k-1}) = \bar{m}$ is associated with polynomial

$$p(x) = \sum_{i=0}^{k-1} m_i x^i \in \mathbb{F}_q[x]$$

Encoding (evaluation map)

$$\mathbb{F}_q[x]_{<k} \longrightarrow \mathbb{F}_q^n$$

$$p(x) \longmapsto (p(\alpha_1), \dots, p(\alpha_n))$$

(∗)

Δ RS-code is an $[n, k, n-k+1]_q$ code

MDS

Why? Non-zero degree $k-1$ polynomial has at most $k-1$ roots.

Why large alphabets?

- Usually a single byte is taken as a single symbol.
- Error is sometimes bursty!

Note that if $q=n$ and we write the elements of $\mathbb{F}_q$ as $\log n$ bit strings then (∗) becomes

$$[n \log n, k \log n, n-k+1]_2$$

Example: $k = n-4$ $\sim$ $[N, N-4\log N, 5]_2$

$$\downarrow$$

$K \leq N - 2\log N$ (a factor of two worse than the best possible).

BIVARIATE POLINOMIALS

- Think the message as a matrix $\overline{m} = (a_{ij})_{i,j<\sqrt{k}}$
- Associate to $\overline{m}$ a bivariate polynomial of degree at most $\sqrt{k}$.
- Evaluate at distint points in $S \times S \subseteq \mathbb{F}_q^2$
- What is the distance?

Theorem $\boxed{\text{[SCHWARTZ - ZIPPEL LEMMA]}}$

A m-variate polynomial $f(x_1 \dots x_n) \in \mathbb{F}[x_1 \dots x_n]$ of degree d
$\not\equiv 0$
is zero on at most $\frac{d}{|S|}$ fraction of the entries of S^m.

The proof follows from choosing $\overline{x_1} \dots \overline{x_m}$ randomly from S^m and argue that random choice gives zero evaluation with probability at most $d/|S|$. The procedure is by induction and case $m=1$ is clear.

Thus bivariate codes give $[n,k,d]$ codes where

$$\boxed{d \geq n - k - \left(\sqrt{k}\,(2q - \sqrt{k})\right)}$$

<u>DEFECT.</u>

Can be improved to $\sqrt{k}\,(2q - 2\sqrt{k})$

$\boxed{\text{REED-MULLER CODES}}$ $RM_q(\ell, m)$

$n = q^m$, $k = \binom{m+\ell}{m}$ where one takes polynomials of degree ℓ in $\mathbb{F}_q[x_1, \dots x_m]$

and $d = \left(1 - \frac{\ell}{q}\right) q^m$

If $q = 2$ and $\ell = 1$ it is a $[2^\ell, \ell+1, 2^{\ell-1}]_2$ code called

HADDAMARD CODE

CYCLIC CODES

A linear code $\mathcal{C}$ of length n is cyclic if it is invariant under the cyclic shift

$$(c_0 \dots c_{n-1}) \xrightarrow{\tau} (c_0 \dots c_n)\cdot \underbrace{\begin{bmatrix} 0 & 1 & 0 & & 0 \\ \vdots & 0 & 1 & & \vdots \\ \vdots & \vdots & 0 & \dots & \vdots \\ 1 & 0 & 0 & & 1 \end{bmatrix}}_{T}$$

Suppose now that $\bar{u} \in \mathbb{F}_q^n \setminus \{\bar{0}\}$

and $k = \max\{ j > 0 \mid \bar{u}, \tau(\bar{u}), \tau^2(\bar{u}), \dots, \tau^{j-1}(\bar{u}) \text{ are l.i} \}$

Then
$$\begin{bmatrix} \bar{u} \\ \tau(\bar{u}) \\ \tau^2(\bar{u}) \\ \vdots \\ \tau^{j-1}(\bar{u}) \end{bmatrix}$$
is a generator matrix of a cyclic linear code of dimension k.

If $\tau^k(u) = \sum_{i=0}^{k-1} c_i \tau^i(\bar{u})$ and $\bar{x} = \bar{v}\cdot G$ $\exists \bar{v} \in \mathbb{F}_q^k$

$$\tau(\bar{x}) = \bar{x}T = \bar{v}GT = v \cdot MG$$

Where M is the <u>COMPANION MATRIX</u> of $f(z) = \sum_{i=0}^{k-1} c_i z^i$

Another way of thinking cyclic codes.

$$\rho : \mathbb{F}_q^{\,n} \longrightarrow \mathbb{F}_q[x] / \langle x^n - 1\rangle$$

$$(a_0, \dots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i \bar{x}^i \qquad \bar{x} = x + \langle x^n - 1\rangle$$

$\mathbb{F}$-algebra

and $\rho(\tau(\bar{a})) = \bar{x} \cdot \rho(\bar{a})$

A cyclic code under this representation is nothing more that an **IDEAL** in $\mathbb{F}_q[x] / \langle x^n - 1\rangle$. Note that all ideals are principal.

$\Downarrow$

$\exists$ a unique monic polynomial of minimal degree $g(x)$ s.t. $\langle g(\bar{x})\rangle = \mathcal{C}$

and $$G = \begin{bmatrix} g(\bar{x}) \\ \bar{x} g(\bar{x}) \\ \vdots \\ \bar{x}^{k-1} g(\bar{x}) \end{bmatrix} \qquad k = \dim(\mathcal{C}) = n - \partial^\circ(g)$$

What about the distance?

$\boxed{\text{BCH BOUND}}$ (Bose, Ray-Chauduri, Hocquenghem)

If α is a primitive n-th root of unity (eventually living in $\mathbb{F}_{q^m}$)

$\begin{cases} \langle g(\bar{x}) \rangle = \mathcal{C} \quad \text{and} \quad g(\alpha^i) = 0 \quad \text{for } i = m_0, m_0+1, \dots, m_0+d-2 \end{cases}$

Then $0 \neq c(\bar{x}) \in \mathcal{C}$ has weight at least d.

Suppose there is a codeword $v(\bar{x}) \in \mathcal{C}$ and $w_H(v) = d' < d$.

$$v(\alpha^j) = S_j = \sum_{i=1}^{d'} \underset{\text{value}}{Y_i} \, \underset{\text{location}}{X_i^j}$$

Thus $S_{m_0} = S_{m_0+1} = \dots = S_{m_0+d'-1} = 0 \qquad (*)$

$$\underset{\text{Location polynomial}}{\sigma(x)} = \prod_{i=1}^{d'} (x - X_i) = x^{d'} + \sum_{i=1}^{d'} \sigma_i x^{d'-i} \implies \sigma(X_i) = 0 \quad i = 1, 2, \dots, d'$$

$$\sum_{i=1}^{d'} Y_i X_i^{j-d'} \sigma(X_i) = S_j + \sum_{i=1}^{d'} \sigma_i S_{j-i} \qquad \forall j \qquad (**)$$

$\sum_{i=1}^{d'} Y_i X_i^{j-d'} \sigma(X_i) = 0$ by previous statement

$(*) + (**) \Rightarrow S_{m_0+d'} = 0 \Rightarrow S_{m_0+d'+1} = 0 \; \ldots$ and so on

Thus $v(\alpha^j) = 0 \;\forall j \Rightarrow v(\bar{x}) = \bar{x}^n - 1 = 0 \mod x^n - 1$ $\blacksquare$

R.T. Chien "A new proof of the BCH Bound" IEE Trans. Inf Th. 1972, (52-8)

Generalizations Hartmann - Tzeng BOUND

Information and control 20 489-498 (1972)

...

DUALITY OF ALGEBRAIC CODES

R-S codes

Consider that we evaluate at all the points in $\mathbb{F}_q$ $\boxed{n=q}$

$$\boxed{RS_k^{\perp} = RS_{q-k-2}}$$

Proof: Checking dimensions $\dim RS_k = k+1$

$\dim RS_{q-k} = q-k-1$

Thus it is enough that both spaces are orthogonal.

RS_k is spanned by the evaluations of $\{x^i\}_{i=0}^{k}$, thus it suffices that for any $a \leq q-2$

$$\sum_{f\in\mathbb{F}_q} f^a = 0$$

Of course we can sum over all $\mathbb{F}_q^*$ (0 makes no difference)

If $\langle\xi\rangle = \mathbb{F}_q^*$

$$\sum_{\ell=1}^{q-1} (\xi^{\ell})^i = \frac{\xi^i - \xi^{iq}}{1-\xi} = 0$$

∎

R-M Codes

The history is pretty much as RS case.

$$\boxed{RM_q(\ell, m)^{\perp} = RM_q(m(q-1)-\ell-1, m)}$$

For a proof one just need to compute the equality of the dimensions and use the following lemma:

<u>Lemma</u>: ℓ and $\lambda \in \mathbb{N}$, If $\lambda < m(q-1)\ell$ then

$$RM_q(\ell, m)^{\perp} \supseteq RM_q(\lambda, m)$$

<u>Proof</u>. Check that if f is a $\underbrace{\text{reduced}}_{X_i^q \to X_i}$ polynomial $\Rightarrow \sum_{\bar{v} \in \mathbb{F}_q^m} f(\bar{v}) = 0$,

and use $\quad \bar{c}_f \cdot \bar{c}_g = \sum_{\vec{v} \in \mathbb{F}_q^m} (f \cdot g)(\vec{v}) = 0 \qquad$ ▨

Cyclic Codes

The dual code of $\mathcal{C} = \langle g(\bar{x}) \rangle \triangleleft \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$ is cyclic and has generator polinomial $g^{\perp}(x) = x^k h(x^{-1})$ where $h(x) = \frac{x^n - 1}{g(x)}$ and $k = \partial h$.

Note that $x^k h(x^{-1})$ "reverses" the coeff. in h.

How to prove it?

1. Check dimensions
2. Check that the matrix constructed from the "reverse" shifts is orthogonal to the generator matrix.

OTHER TYPES OF ALGEBRAIC CODES

Evaluation codes

RS, RM, GRS, GRM, algebraic geometric, hyperbolic, cartesian products, affine, toric, j-affine ...

Cyclic-like codes

Abelian, group codes, polycyclic, multicirculant...

WHAT ABOUT DECODING?

What is decoding?

a) Maximum Likelihood decoding (SHANNON) MLD

Given a channel and a distribution on the messages
↓
Compute the most likely message (codeword) given a received vector.

b) Nearest codeword problem NCP

Given a received vector $\bar{r}$, find $\bar{c} \in \mathcal{C}$ nearest to $\bar{r}$.

$\boxed{\text{NCP corresponds to MLD for the } q\text{-ary symmetric ch.}}$

What happens with ties?

c) Soft decision decoding

Given an $n \times q$ matrix M of non-negative reals

columns indexed by A.

compute a codeword $c \in \mathcal{C}$ that maximizes

$$\sum_{i=1}^{n} M_{i c_i} \qquad (*)$$

- If entries in M are $0/1$ with one "1" per column we get the NCP.

- For a iid channel, for each symbol compute $P_{i\alpha}$ the probability that we get what we got provided the transmitted symbol on i-th coordinate is α

  and $\quad M_{i\alpha} = -\log P_{i\alpha}$

  Then $* \Rightarrow$ MLD for the iid channel.

$\leftarrow$ Really hard problems

$\boxed{d = d(\mathcal{C})}$

What is reasonable?

a) Unique decoding — Given $\bar{r} \in A^n$ compute $\bar{c} \in \mathcal{C}$ such that $d(r,c) < d/2$ if it exist.

or

$\boxed{\text{BOUNDED DISTANCE DECODING.}}$

b) Relative near codeword (RNC) Parameter $\gamma > 0$

Given $\bar{r}$, $e < \gamma d$ find $\bar{c} \in \mathcal{C}$ with $d(\bar{r}, \bar{c}) \leq e$ if it exist.

c) LIST DECODING — Like in RNC but now we allow a list of codewords each one of them $d(\bar{r}, \bar{c}) \leq e$.

$\gamma = 1/2$ BDD = RNC = List decoding.

- <u>For general linear codes</u>

  - Encoding is easy
  - Error detection is easy
  - Easure correction is easy

    $\bar{r} \in (A \cup \{?\})^n$ compute $\bar{c} \in \mathcal{C}$ s.t. $r_i \neq ? \Rightarrow r_i = c_i$

    Solving linear system.

Syndrome decoding

$$\bar{r} = \bar{c} + \bar{e}, \quad \bar{r}H = \bar{c}\underbrace{H}_{0} + \bar{e}H = \bar{e}H$$

Brute force table $\bar{e} \longmapsto \bar{e}H$.

↓ Any decoding algorithm $\Rightarrow$ SD.

↓ Exponential time.

Unique decoding RS codes

PROBLEM:

Given n distinct points $(\alpha_i, r_i) \in \mathbb{F}_q^2$

Compute $p(x) \in \mathbb{F}[x]$ $\partial p < k$ s.t.

$$p(\alpha_i) = r_i$$

for at least $\frac{n+k}{2}$ values of $i \in \{1 \ldots n\}$

ERROR LOCATOR POLYNOMIAL

In the previous conditions $E(x)$ is an error locator polinomial if

- $p(\alpha_i) \neq r_i \Rightarrow E(\alpha_i) = 0$
- $E(x)$ has at least $k+1$ non-zeros.

1) If we know $E(x)$ we can compute $p(x)$!

2) Such polynomial $E(x)$ exist (an its degree is the # of errors)

$$E(x) = \prod_{i \mid r_i \neq p(\alpha_i)} (x - \alpha_i)$$

$\boxed{\text{The KEY EQUATION}}$

Fix $E(x)$ of degree e and $N(x) = E(x)p(x)$

(KE) $\quad \forall i \quad N(\alpha_i) = p(\alpha_i)E(\alpha_i) = r_i E(\alpha_i)$

Algoritm :

1) Find a pair (N, E) with $N \neq 0 \neq E$ & $\begin{cases} \partial^\circ N \leq k+e \\ \partial^\circ E \leq e \end{cases}$ satisfying the (KE)

2) Output N/E . if it is a polinomial with the right conditions ELSE no exist.

Q1.- How can we deal with step1

Substitute unknowns for coeffs & solve a linear system.

Q2:- Is there a solution? We just showed one

Q3:- Is it unique? NO

Lemma:- $\boxed{\text{If } (N,E) \text{ and } (M,F) \text{ are solutions then } \frac{N}{E} \equiv \frac{M}{F}}$

PROOF. $\forall i \quad r_i N(\alpha_i) F(\alpha_i) = r_i M(\alpha_i) E(\alpha_i)$

Case i) $r_i \neq 0$ Cancel both sides and $N(\alpha_i)F(\alpha_i) = M(\alpha_i)E(\alpha_i)$

Case ii) $r_i = 0$ then $N(\alpha_i)F(\alpha_i) = M(\alpha_i)E(\alpha_i) = 0$

Thus, for n values $N \cdot F = ME$, if $n > k+2e$ then $\frac{N}{E} \equiv \frac{M}{F}$ ∎

ERROR CORRECTING PAIRS

Pellikaan, Kotter, Duursma. 1988

KE relies on linear algebra or on polynomial algebra?

$\mathcal{C}$ an $[n,k,d]_q$ code

Construct an error-locator code E such that $E*\mathcal{C} \subseteq \mathcal{N}$, a code with larger distance. More precisely

i) $\dim E > e$

ii) $E * \mathcal{C} \subseteq \mathcal{N}$

iii) $d(\mathcal{N}) > e$

(iv) $d(\mathcal{N}) > n - d(E)$

If there is an $(E, \mathcal{N})$ e-error correcting pair for $\mathcal{C}$ then there is an e-error correcting algorithm for $\mathcal{C}$

Algorithm

1) Given $\bar{r} = (r_1 \dots r_n)$

2) Find $\underset{\neq 0}{\bar{a}} \in \mathcal{E}$ and $\underset{\neq 0}{\bar{b}} \in \mathcal{N}$ such that $a * r = b$ and $a_i = 0$ if $r_i \neq c_i$

3) For any i with $a_i = 0$ set $r_i = ?$

4) Do erasure decoding on the resulting vector.

PROOF:

a) $\bar{a}$ and $\bar{b}$ exist.

Since $\leq e$ errors have occurred, then $a_i = 0$ for at most e values, that gives e linear coustrains on a, but $\dim(\bar{\mathcal{E}}) > e \Rightarrow \exists a$ ✓

Now define $\bar{b} = \bar{a} * \bar{c} \in \mathcal{N}$, and $b_i = a_i r_i$ because either $r_i = c_i$ or if $r_i \neq c_i$ $a_i = 0$

Thus $\exists b$ ✓

!! All the operations are efficient since they are linear algebra.

The OUTPUT is unique since

a) The pair $(\bar{a}, \bar{b})$ satisfying the conditions

$$\Downarrow$$

$$\bar{a} * \bar{c} = \bar{b}$$

b) There is a unique $\bar{e}$ such that $\bar{a} * \bar{c} = \bar{b}$

PROOF

a) We know $\bar{a} * \bar{r} = \bar{b}$, suppose $\bar{a} * \bar{c} = \bar{b}'$.

Since $b_i' = a_i c_i$ and $b_i = a_i r_i$ we have $b_i' \neq b_i$ if $r_i \neq c_i$

but there are $\leq e$ errors, ie. at most e of those indices,

$d(\bar{b}, \bar{b}') \leq e$, but $\bar{b}, \bar{b}' \in \mathcal{N}$ and $d(\mathcal{N}) > e \Rightarrow \bar{b} = \bar{b}'$

b) Suppose $\bar{a} * \bar{c}' = \bar{b} = \bar{a} * \bar{c}$. Since $\bar{a} \in E$, $a_i \neq 0$ for at least $d(E)$ indices, ie $\bar{c}'$ and $\bar{c}$ agree on at least $d(E)$ coordinates $\Rightarrow d(\bar{c}', \bar{c}) < n - d(E)$, but $\bar{c}, \bar{c}' \in \mathcal{C}$ $(d(\mathcal{C}) > n - d(E))$ ↯

DECODING BCH CODES

Let $\alpha, \alpha^2, \dots, \alpha^{2t}$ the $2t$ consecutive roots of the generator poly.
Let $y(x)$ the received vector.

\# errors

$$S_j = y(\alpha^j) = c(\alpha^j) + e(\alpha^j) = e(\alpha^j) = \sum_{i=0}^{n-1} e_i (\alpha^j)^i = \sum_{k=1}^{v} e_{i_k} \alpha^{i_k j}$$

notation $Y_k = e_{i_k}$ $X_k = \alpha^{i_k}$ $\quad 1 \leq j \leq 2t$

$$S_j = \sum_{k=1}^{v} Y_k X_k^j \qquad 1 \leq j \leq 2t$$

We have a system of equations

$$\begin{cases} S_1 = Y_1 X_1 + Y_2 X_2 + \dots + Y_v X_v \\ S_2 = Y_1 X_1^2 + Y_2 X_2^2 + \dots + Y_v X_v^2 \\ \vdots \\ S_{2t} = Y_1 X_1^{2t} + Y_2 X_2^{2t} + \dots + Y_v X_v^{2t} \end{cases}$$

The error locator polynomial is

$$\Lambda(x) = (1 - xX_1)(1 - xX_2)\cdots(1 - xX_\nu) = \underset{\substack{\shortparallel \\ 1}}{\Lambda_0} + \sum_{i=1}^{\nu} \Lambda_i x^i$$

If we define

$$S(x) = \sum_{j=0}^{\infty} S_{j+1} x^j = \sum_{j=0}^{\infty} x^j \left(\sum_{k=1}^{\nu} Y_k X_k^{j+1} \right)$$

$$= \sum_{k=1}^{\nu} \frac{Y_k X_k}{(1 - x X_k)}$$

And define the error-evaluator poly as

$$\Omega(x) = \Lambda(x) S(x) = \sum_{k=1}^{\nu} Y_k X_k \prod_{\substack{j=1 \\ j \neq k}}^{\nu} (1 - xX_j)$$

$\partial^\circ \Omega(x) < \nu.$

Since we actually only know the first $2t$ terms of $S(x)$ we have

$$\boxed{\Lambda(x)\, S(x) \equiv \Omega(X) \mod x^{2t}}$$

The process of decoding is computing $\Lambda(x)$ [Once we know $\Lambda(x)$ and $S(x)$, then computing $\Omega(x)$ is immediate)

There are two main ways of solving it:

a) Euclidean method

b) Berlekamp-Massey.

LOW DENSITY PARITY CHECK CODES

Binary case : $q=2$

A parity check matrix of an $[n,k]_2$ code can be associated to a FACTOR GRAPH $\mathcal{G}$.

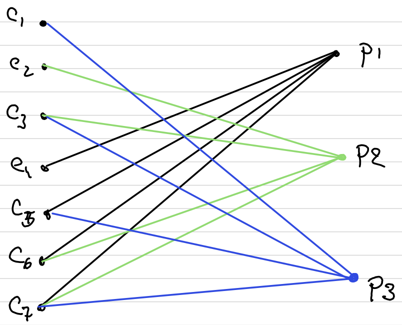
$\mathcal{G}$ is bipartite and has $n-k$ right vertices, called check nodes, and n left vertices called variable nodes.

A check node i is adjacent to all the variable nodes that appear in the i-th row of H.

Example: $[7,4,3]_2$

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

variable nodes check nodes



So, the number of edges is the number of 1's in H.

A special class of LDPC codes are regular LDPC codes, where left vertex has degree d_v and every right one has degree d_c.

In that case $\boxed{R = 1 - \frac{d_v}{d_c}}$

since $d_v n = d_c (n-k)$. Hence, implies $d_c > d_v$ for R being positive.

GILBER - VARSHAMOV BOUND

$A_q(n,d)$ = maximum size of a q-ary code of length n. and distance d.

$$A_q(n,d) \geq \frac{q^n}{\sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j}$$

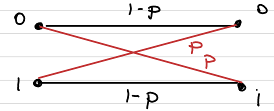
The GIRTH of a graph is the size of its smaller cycle.

Result $\boxed{\text{Gallager } 1963}$

i) With high probability, for large enough d_v and d_c, a random (d_v, d_c)-regular LDPC code achieves the GV. Bound.

ii) Random (d_v, d_c)-regular LDPC codes (with MLD) get close to the capacity of the BSC_p.

BSC_p



Capacity $1 - H_b(p)$

$$H_b(p) = -p \log p - (1-p) \log(1-p)$$

MLD is exponential, so Gallager developed and iterative decoder.

Received word $\bar{y} = (y_1 \dots y_n) \in \{0,1,?\}^n$

- Round of messages:

  i) <u>Variable to check</u>

  If (c_i, p_j) is an edge then c_i sends p_j a message.
  If $y_i \neq ?$, it passes its info to all its neighboring check nodes.

  ii) <u>Check to variable</u>

  If (p_j, c_i) is an edge then p_j sends a message.
  If p_j knows the correct value for c_i, it passes the value to c_i

More precisely:

1) If variable c_i knows its correct value then sends it, else sends $?$

2) If the check node p_j knows the value of c_i pases the value, else $?$.

At the end, every c_i knows its value with high probability.

MESSAGE MAPS

$c_i \longrightarrow p_j$ in round t

$$\Psi_{c_i}^{t,p_j}(y_i, \underbrace{m_1^{t-1}, \dots, m_{d_v-1}^{t-1}}) \longrightarrow \{0,1,?\}$$

messages received in c_i from its neighb. other than p_j in round $t-1$

$p_j \longrightarrow c_i$ in round t

$$\Psi_{p_j}^{t,c_i}(\underbrace{m_1^{t}, \dots, m_{d_c-1}^{t}}) \longrightarrow \{0,1,?\}$$

d_c-1 messages received in p_j from the variable nodes in round t

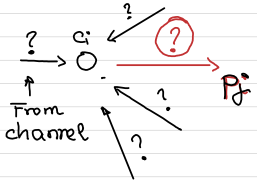
$c_i \longrightarrow P_j$

Round 1 $\quad \psi_{c_i}^{1,P_j}(y_i, m_1^0 \dots m_{d_v-1}^0) = y_i$

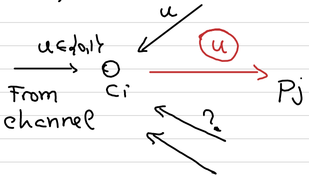
$t \geq 2$ $\quad \psi_{c_i}^{t,P_j}(y_i, m_1^{t-1}, \dots, m_{d_v-1}^{t-1}) = \begin{cases} \text{If any other incomming message is } \{0,1\} \text{ send it} \\ ? \text{ if all of them are } ? \end{cases}$

$$\psi_{P_j}^{t c_i}(m_1^t, \dots, m_{d_v-1}^t) = \begin{cases} ? & \text{if any of them is } ? \\ m_1^t \oplus \dots \oplus m_{d_v-1}^t & \text{otherwise} \end{cases}$$

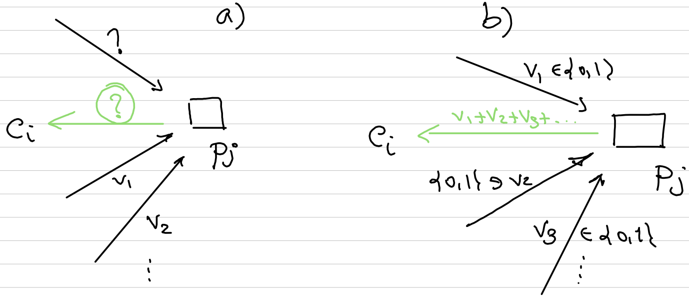
(a)



(b)

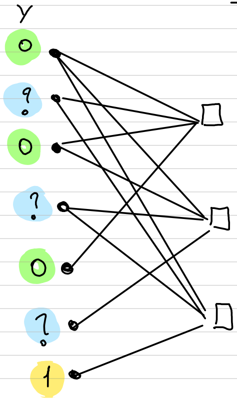


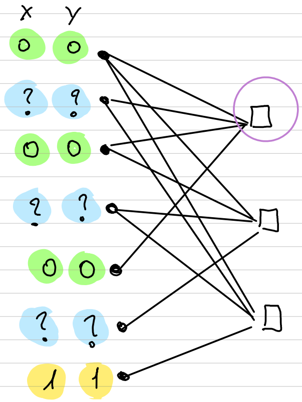
NEXT SLIDE


a)
?
?
C_i
P_j
v_1
v_2
b)
$v_1 \in \{0,1\}$
$v_1+v_2+v_3+\dots$
C_i
P_j
$\{0,1\} \ni v_2$
$v_3 \in \{0,1\}$

EXAMPLE

Initialization

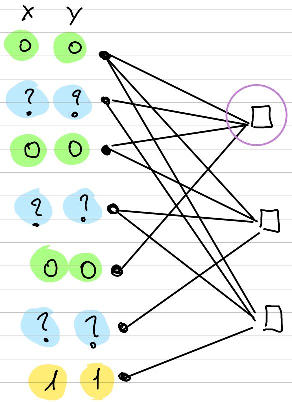




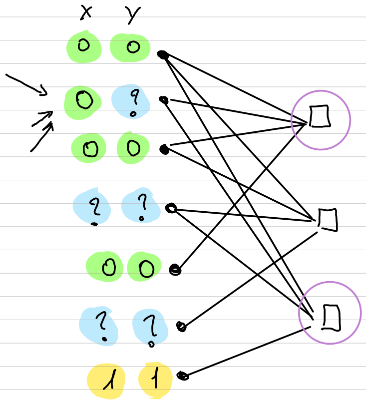
$\longrightarrow$

$v \to$ check

Round 1

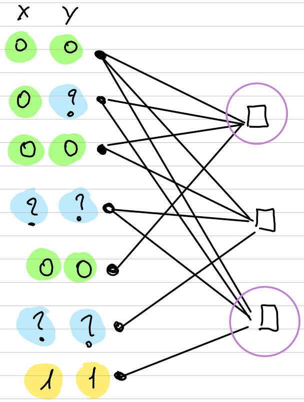


Check → variable

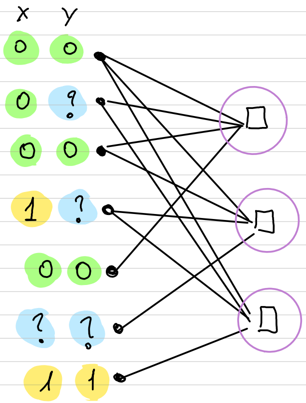


Variable → check

Round 2

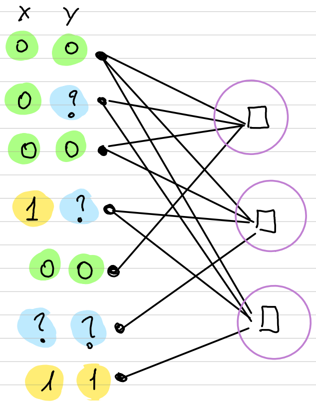


Check → variable

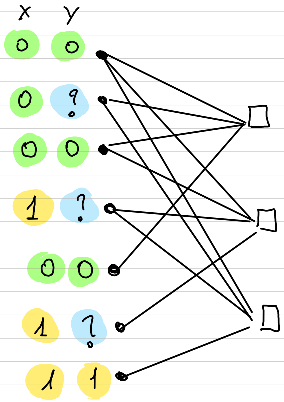


Variable → check.

Round 3



Check → variable

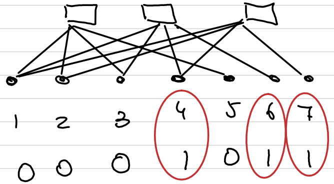


Variable → check

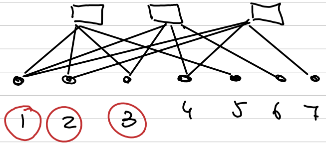
Decoding completed

A **STOPPING SET** is a subset S of the variable nodes such that every check node connected with S is connected with it <u>twice</u>.

- The empty set is a stopping set.
- The support set of any codeword is a stopping set.
- But a stopping set need not to be the support of a codeword.



$S = \{4, 6, 7\}$



$S = \{1, 2, 3\}$

There is no codeword with support $\{1, 2, 3\}$

- Every set of variables contains a largest stopping set.

  [Note that the union of stopping sets is also a stopping set]

- Message-passing decoding needs a node with at most one edge connected to an erasure to proceed.

- If the remaining erasures form a stopping set → STOP!

- Let E the initial set of ?. When the M-P stops, the remainder ? forms the largest stopping set $S \subset E$
  - If S empty → Codeword recovered.
  - If not → Fail!

Instituto de Matemáticas

Thanks for your attention!