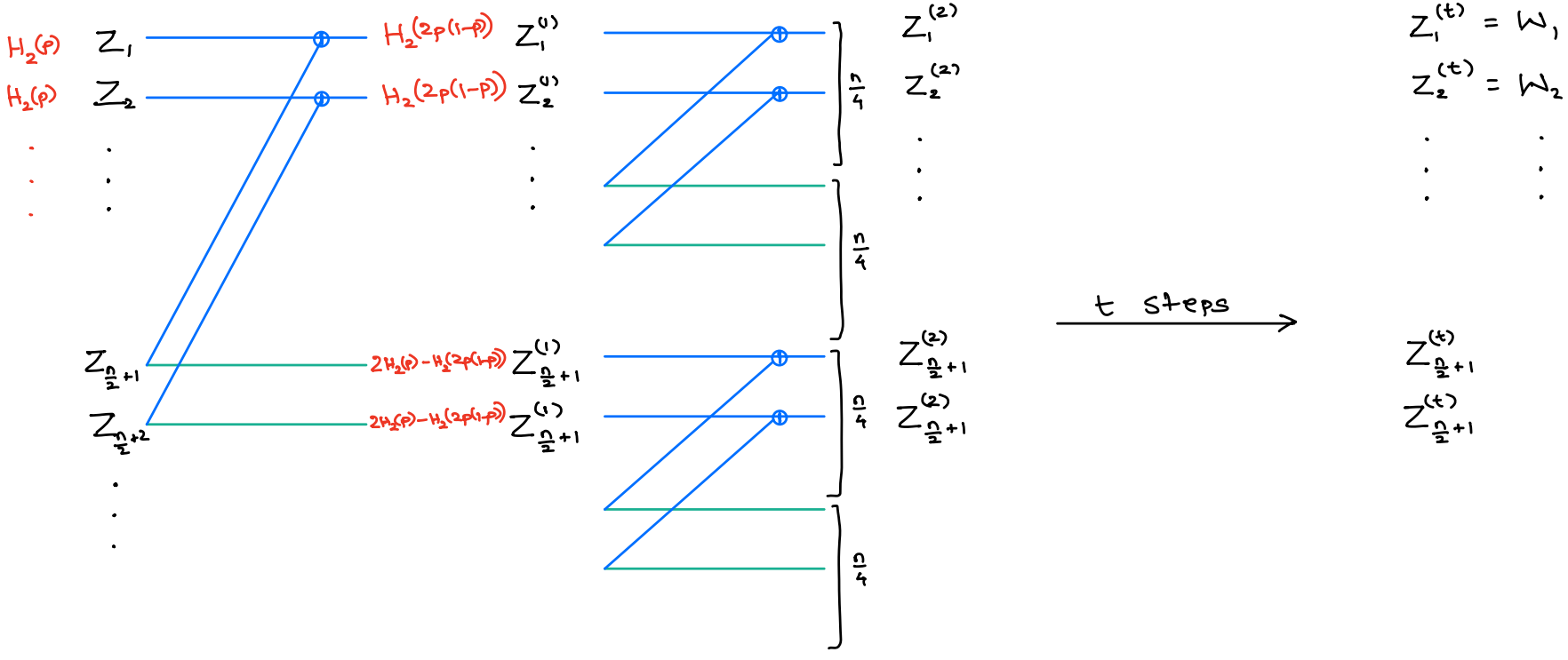
Recap (Polar Codes) : Capacity for Binary Symmetric Channel

$R \to 1 - H_2(p)$

$$P_n = \begin{pmatrix} P_{n/2} & P_{n/2} \\ 0 & P_{n/2} \end{pmatrix} \qquad n = 2^t$$

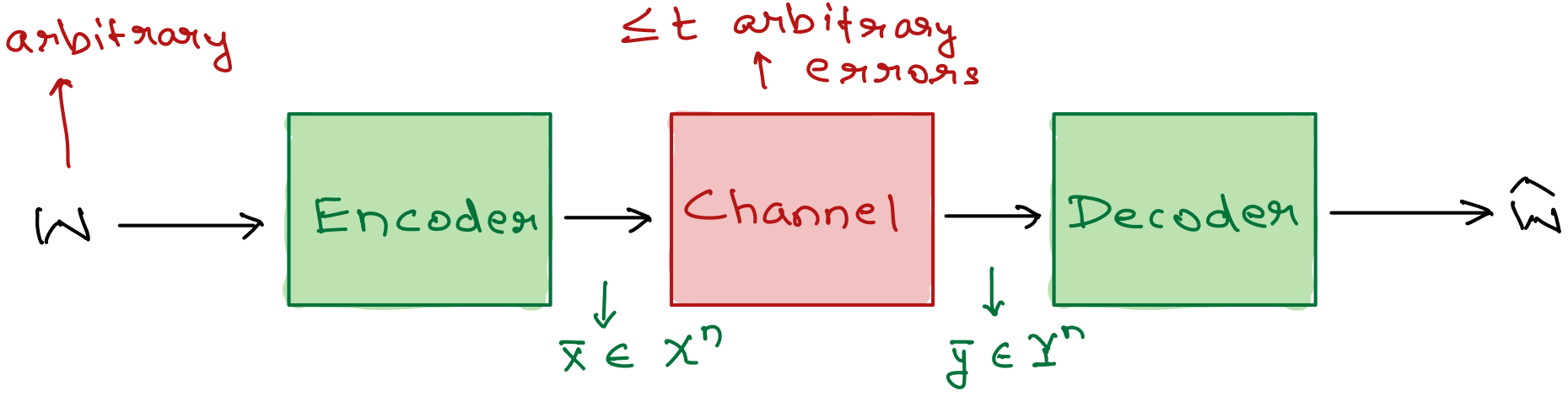
$X_j = H(Z_i^{(j)} \mid Z_{<i}^{(j)})$ for random $i \in [n]$



- (Speed of polarization) $\forall \gamma > 0 \quad \exists \alpha \in (0,1), \beta > 0$ s.t. $\forall t$

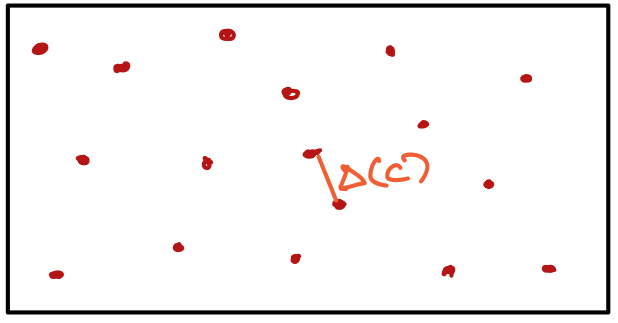
$$P[X_t \in (\gamma^t, 1-\gamma^t)] \leq \beta \cdot \alpha^t$$

Hamming model



- $X = Y = F_q$, $C = \text{im}(\text{Encoder}) \subseteq F_q^n$

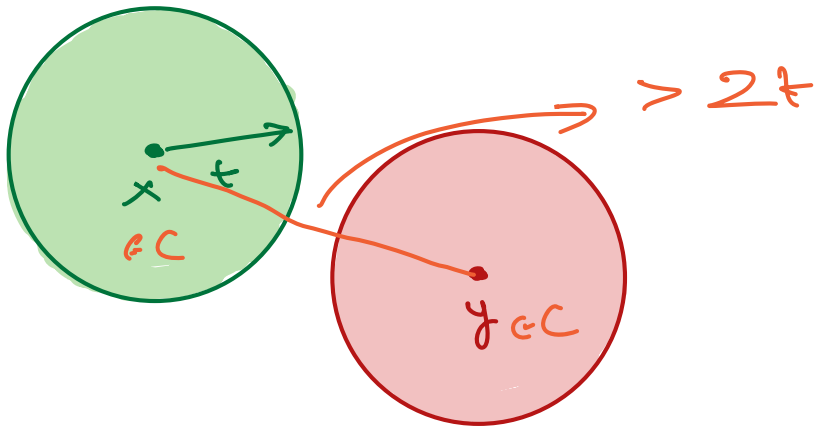
Distance: $\Delta(C) = \min_{\substack{x,y \in C \\ x \neq y}} \Delta(x,y)$



Ex: $\Delta(x,y) + \Delta(y,z) \geq \Delta(x,z)$ for $\Delta \equiv$ Hamming distance (is a metric)

- $C \subseteq F_q^n$ can correct t errors iff $\Delta(C) \geq 2t+1$

Proof:



Must have $B(x,t) \cap B(y,t) = \emptyset \quad \forall x, y \in C, x \neq y$

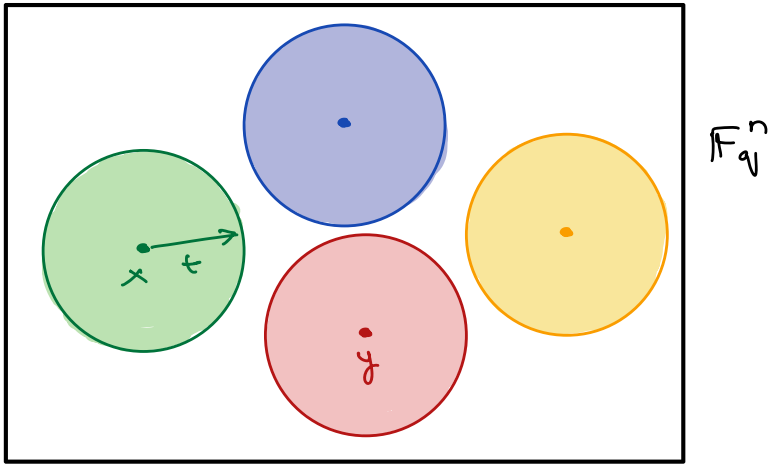
Rate-distance tradeoffs

- (Hamming bound) For $C \subseteq \mathbb{F}_q^n$, $t = \left\lfloor \frac{\Delta(C)-1}{2} \right\rfloor$

$$|C| \leq \frac{q^n}{|B(0,t)|}$$

$$B(x,t) = \{z \mid \Delta(x,z) \leq t\}$$

Proof:



$$\sum_{x \in C} B(x,t) \leq q^n$$

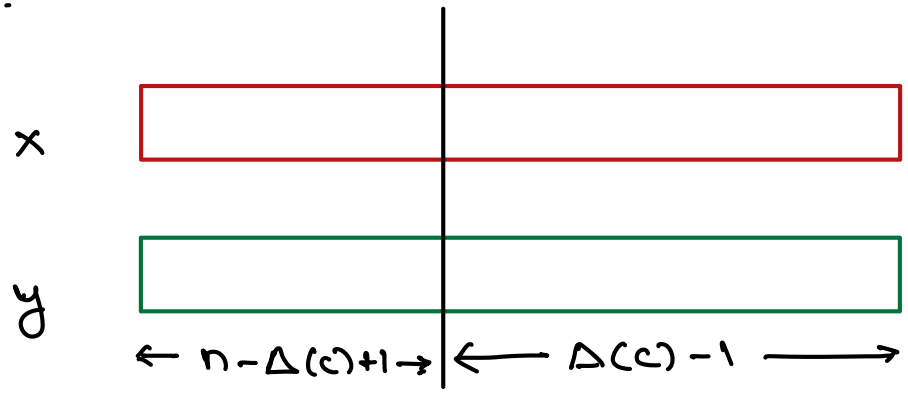
Ex: Is Hamming bound tight for Hamming code?

Ex: For $C : \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^n$ and $\Delta(C) = \delta n$, rate $= \frac{k}{n} \leq 1 - H_2(\delta) + o(1)$

Singleton bound

- For $C : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, $\Delta(C) \leq n - k + 1$

Proof:



$$q^k = |C| \leq q^{n-\Delta(C)+1}$$

$$\frac{\Delta(C)}{n} \leq 1 - \frac{k}{n} + \frac{1}{n}$$

Finite fields revisited

$\mathbb{F}_q = \{0, 1, \ldots, q-1\}$, q prime. $+, \cdot : \mathbb{F}_q \to \mathbb{F}_q \pmod q$

- Fermat's little theorem: $a^q \equiv a \pmod q$, $a \in \{0, 1, \ldots, q-1\}$

- Polynomials: $\mathbb{F}_q[x] = \{c_0 + c_1 \cdot x + \ldots + c_{q-1} x^{q-1} \mid c_0 \ldots c_{q-1} \in \mathbb{F}_q\}$

$$\mathbb{F}_q^{\leq d}[x] = \{c_0 + c_1 \cdot x + \ldots + c_d \cdot x^d \mid c_0 \ldots c_d \in \mathbb{F}_q\}$$

- Lagrange interpolation: Given distinct $a_1, \ldots, a_{d+1} \in \mathbb{F}_q$
arbitrary $b_1, \ldots, b_{d+1} \in \mathbb{F}_q$

There is a unique $f \in \mathbb{F}_q^{\leq d}[x]$ s.t. $f(a_i) = b_i \; \forall i \in [d+1]$

$$f(x) = \sum_{i=1}^{d+1} b_i \cdot \prod_{j \neq i} \left(\frac{x - a_i}{a_j - a_i}\right)$$

Ex: $f \in \mathbb{F}_q^{\leq d}[x]$, $f \neq 0$ has $\leq d$ roots.

Lagrange interpolation

Proof 1: Solve for coefficients $c_0, \dots, c_{d+1}$ $(f(x) = c_0 + c_1 \cdot x + \dots + c_d \cdot x^d)$

$$\begin{bmatrix} 1 & a_1 & \cdots & a_1^d \\ 1 & a_2 & \cdots & a_2^d \\ \vdots & & & \\ 1 & a_{d+1} & \cdots & a_{d+1}^d \end{bmatrix} \begin{bmatrix} c_0 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_{d+1} \end{bmatrix}$$

$c_0 + c_1 \cdot a_1 + c_2 \cdot a_1^2 + \dots + c_d \cdot a_1^d = b_1$

↪ $\det = \prod_{i<j} (a_i - a_j)$

Proof 2: Polynomials $g_i(x) = \prod_{j \neq i} \frac{(x - a_j)}{(a_j - a_i)}$ are a basis for $\mathbb{F}_q^{\leq d}[x]$

Reed-Solomon Codes

Fix $S = \{a_1, \ldots, a_n\} \subseteq \mathbb{F}_q$

$$C = \{(f(a_1), \ldots, f(a_n)) \mid f \in \mathbb{F}_q^{\leq (k-1)}[x]\}$$

linear code

Encoding maps

- $(m_0, \ldots, m_{k-1}) \longmapsto f_m(x) \equiv m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$

  $C(m_0, \ldots, m_{k-1}) = (f_m(a_1), \ldots, f_m(a_n))$

- $(b_1, \ldots, b_k) \longmapsto f_b \equiv$ unique f s.t. $f(a_i) = b_i \ \forall i \in [k]$

  $C(b_1, \ldots, b_k) = (f_b(a_1), \ldots, f_b(a_n))$

Ex: Find generator and parity-check matrices

Rate and distance

$$\text{Rate} = \frac{\log|C|}{(\log q)\cdot n} = \frac{\log q^k}{n \log q} = \frac{k}{n}$$

# of non-zero coordinates

- For any linear code, $\Delta(C) = \min_{\substack{x \in C \\ x \neq 0}} \Delta(x, 0) = \min_{\substack{x \in C \\ x \neq 0}} \text{wt}(x)$

Proof:

$$\Delta(x, y) = (x - y, 0)$$

$$\forall x, y \quad x \neq y \qquad \Delta(x, y) = \Delta(x - y, 0) \geq \min_{z \in C} \Delta(z, 0)$$

- For Reed-Solomon codes, $\Delta(C) = \min_{f \neq 0} \{ i \mid f(a_i) \neq 0 \}$

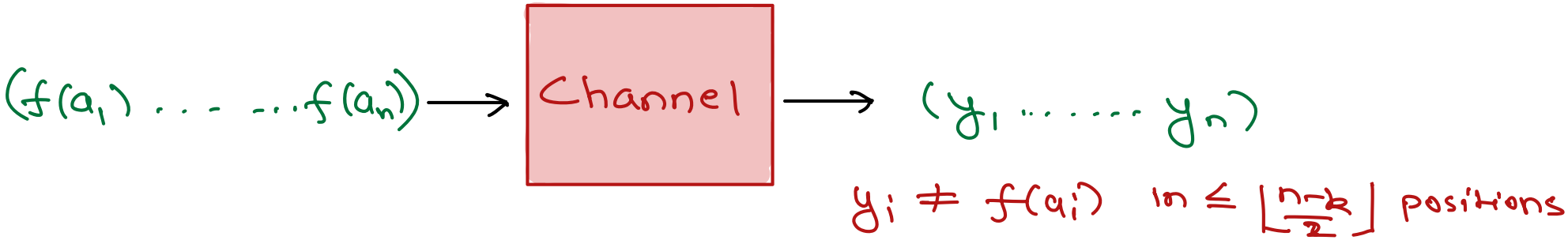
$$= n - \max_{f \neq 0} \{ i \mid f(a_i) = 0 \}$$

$$\geq n - (k - 1) = n - k + 1$$

(Unique) Decoding

[Welch, Berlekamp '86]

- Can correct any $t = \left\lfloor \frac{\Delta(C)-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$ errors



Ex: Can fix even $t' = n-k$ errors if locations known.

Idea: Locate errors via another polynomial!

$$f(a_i) \neq y_i \Rightarrow e(a_i) = 0$$

$$f(a_i) \cdot e(a_i) = y_i \cdot e(a_i) \quad \forall i$$

$\deg(g) \leq k-1+t$

Decoding via "error locator polynomials"

- Find $g, e \in \mathbb{F}_q[x]$ s.t.
  - $\deg(e) \leq t$
  - $\deg(g) \leq k-1+t$

  $\forall i \quad g(a_i) = e(a_i) \cdot y_i$

- Output $\frac{g}{e}$

And why does that work?

- For intended f, $\exists\, e_0$ s.t. $(g_0 = f \cdot e_0,\ e_0)$ is a solution.

Proof: $T = \{i \mid y_i \neq f(a_i)\}$ $\qquad e_0(a_i) = 0 \Leftarrow i \in T$

- For any two solutions (g_1, e_1) and (g_2, e_2)

$$\frac{g_1}{e_1} = \frac{g_2}{e_2}$$

Proof: $\deg \leq t + t + k - 1 \leq n$

$$g_1 e_2 \equiv g_2 e_1$$

$$\forall i \quad g_1(a_i) \cdot e_2(a_i) = y_i \cdot e_1(a_i) \cdot e_2(a_i)$$

$$= e_1(a_i) \cdot g_2(a_i)$$