Recap

Linear Codes: $C \leq \mathbb{F}_2^n$ (subspace)

$$C = \{ GW \mid W \in \mathbb{F}_2^k \} = \text{im}(G) = \ker(H) = \{ x \in \mathbb{F}_2^n \mid Hx = 0 \}$$

$\text{im}(G)$: Generator

$\ker(H)$: Parity check

Hamming Code:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \in \mathbb{F}_2^{3 \times 7}$$

$x \longrightarrow y = x + e_i$

e_i: bit flip, unknown i

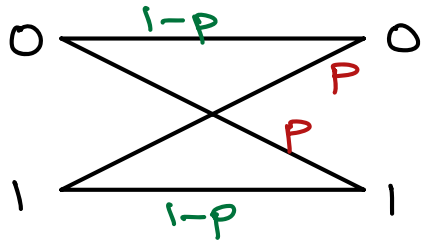
$$Hy = Hx + He_i$$

$$= 0 + (i^{th} \text{ col of } H)$$

$$= (i \text{ in binary})$$

Explicit Codes achieving Capacity (for BSC) [Arikan 09]

Linear $C \leq \mathbb{F}_2^n$



$$\dim(C) \geq n \cdot (1 - H_2(p) - \epsilon)$$

$$\forall x \in C \quad \mathbb{P}_{z \sim Q^n} [\, \mathrm{Dec}(x+z) \neq x \,] \to 0$$

$\hookrightarrow$ $\mathrm{Bern}(p)$

$O(n \log n)$ time encoding and decoding

Linear Compression

Goal: Compress $Z \in \mathbb{F}_2^n$, $Z \sim (\text{Bern}(p))^n$

$\text{Com}: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$

$\text{Decom}: \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$

$m \geq ?$

$$\mathbb{P}_{Z \sim (\text{Bern}(p))^n}[\text{Decom}(\text{Com}(Z)) \neq Z] \to 0$$

Ex: Easy as above via prefix-free codes

Linear Compression: Must have

$$\text{Com}(Z) = HZ \quad \text{for } H \in \mathbb{F}_2^{m \times n}$$

From linear compression to codes

$$\underset{Z \sim (\mathrm{Bern}(p))^n}{P}\left[\mathrm{Decom}(HZ) \neq Z\right] \longrightarrow 0 \quad , \quad H \in \mathbb{F}_2^{m \times n}$$
$$m \leq n \cdot (H_2(p) + \epsilon)$$

- Given linear compression, $C = \ker(H) = \{x \mid Hx = 0\}$ is a good code

Proof:

$$x \longrightarrow x + Z = y$$

$$Hy = Hx + HZ$$

$$y + \mathrm{Decom}(Hy) \overset{\text{whp.}}{=} x + Z + Z = x$$

$$\text{rate} = \frac{\dim(C)}{n} \geq \frac{n-m}{n} \geq 1 - H_2(p) - \epsilon$$

From linear compression to entropy polarization

$$H : \mathbb{F}_2^m \to \mathbb{F}_2^n \quad , \quad m \le (H_2(p) + \epsilon) \cdot n \quad , \quad P(\text{Decom}(HZ) \neq Z) \le \delta$$

$$P = \begin{pmatrix} H \\ \hline H' \end{pmatrix} \in \mathbb{F}_2^{n \times n} \quad \text{invertible}$$

$$Z \sim \text{Bern}(p) \quad , \quad W = PZ \qquad H(W) =$$

$$H(W) = \underbrace{H(W_1) + \cdots + H(W_m \mid W_{<m})}_{\approx (H_2(p) - \delta) \cdot n} + H(W_{m+1} \cdots W_n \mid W_1 \cdots W_m)$$

Ex: $H(W_{m+1} \cdots W_n \mid W_{\le m}) \le H_2(\delta) + \delta \cdot n$

Entropy Polarization

An invertible $P \in \mathbb{F}_2^{n \times n}$ is (ϵ, τ)-polarizing

for $Z \sim (\text{Bern}(p))^n$ if for $W = PZ$ and

$S_\tau = \{ i \in [n] \mid H(W_i | W_{<i}) \geq \tau \}$, $|S_\tau| \leq (H_2(p) + \epsilon) \cdot n$

Ex: Must have $|S_\tau| \geq (H_2(p) - \tau) \cdot n$

Natural compression scheme: $\text{Com}(Z) = P_{S_\tau} Z$

$\text{Decom}(Z) =$

Linear Compression from Polarization

Invertible $P \in \mathbb{F}_2^{n \times n}$, $S_\tau = \{ i \in [n] \mid H(W_i | W_{<i}) \geq \tau \}$

$|S_\tau| \leq (H_2(p) + \epsilon) \cdot n$

$\text{Com}(Z) = Y = P_{S_\tau} Z$

$\text{Decom}(Y) = P^{-1} \hat{W}$

For $i = 1$ to n

if $i \in S_\tau$, $\hat{W}_i = Y_i$

else $\hat{W}_i = \underset{b \in \{0,1\}}{\text{argmax}} \, \mathbb{P}[\hat{W}_i = b | \hat{W}_{<i}]$

Ex: $\mathbb{P}[\text{Decom}(\text{Com}(Z)) \neq Z] \leq n \cdot \tau$

P_e

- $P_e \leq \sum_i \mathbb{P}[\hat{W}_i \neq W_i | \hat{W}_{<i} = W_{<i}]$

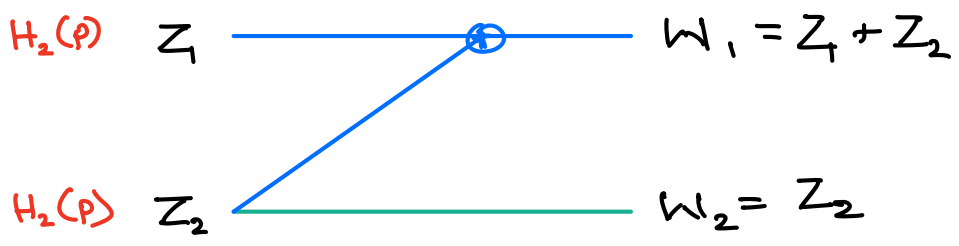
- For r.v. $X \in \{0,1\}$

$H(X) \leq \alpha$

$\Rightarrow \max\{\mathbb{P}(X=1), \mathbb{P}(X=0)\} \geq 1 - \alpha$

Slight polarization

$$P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad W = P \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = \begin{pmatrix} Z_1 + Z_2 \\ Z_2 \end{pmatrix}$$



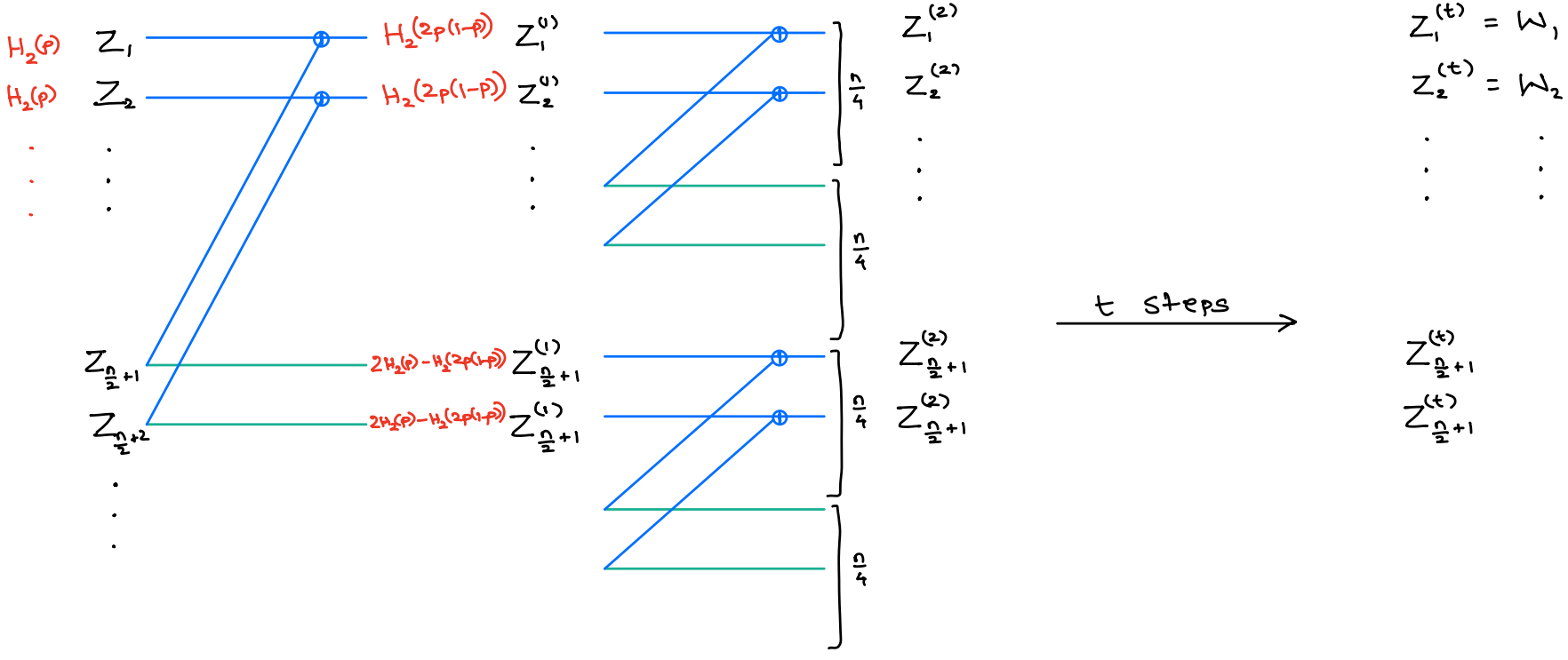
$$H(W_1) = H_2\left(2 \cdot p(1-p)\right) > H_2(p)$$

$$H(W_2 | W_1) = 2H_2(p) - H_2(2 \cdot p(1-p)) < H_2(p)$$

Recursion

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

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



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

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