May 9, 2019

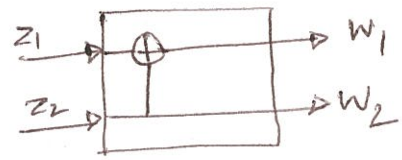
REMINDERS

(•) Please fill in course evals
(•) Proof reading due by noon next Th.
(•) Video grading delayed till end of next week.

RECAP:

Base case:

Polarizing matrix: $P_2(Z_1, Z_2) = (Z_1+Z_2, Z_2)$



$n = 2^t$ for $t > 1$

$$Z = (\underbrace{\overline{U}}_{(\cancel{Z_1}, \dots, \cancel{Z_{\frac{n}{2}}})}, \underbrace{\overline{V}}_{(Z_{\frac{n}{2}+1}, \dots, Z_n)})$$

$$P_n(\overline{Z}) = \left(P_{\frac{n}{2}}(\overline{U}+\overline{V}), P_{\frac{n}{2}}(\overline{V})\right)$$

Polynomially strong polarization: Fix $0 < p < \frac{1}{2}$ & const $c > 0$. Assume given to us.

$\forall \varepsilon > 0$, $\exists\ n = 2^t$ s.t $\frac{1}{\varepsilon} < n \le poly(\frac{1}{\varepsilon})$ s.t

P_n is $(\frac{1}{n^c}, \varepsilon)$ - ~~plo~~ polarizing with unpredictable columns $S \subseteq [n]$ s.t $|S| \le (H(p)+\varepsilon)n$

[Pf in Sec 11.5] [recall $S = \{i \mid H(W_i \mid \overline{W}_{<i}) \ge \frac{1}{n^c}\}$]

Compression: ① Compute $P_n(\overline{Z})$ recursively in $O(n\log n)$ time

② Output $(P_n(\overline{Z}))_S$

Decoder: Main insight; work with $Z \in Bern(p_1) \times Bern(p_2) \times \dots \times Bern(p_n)$

④ $Z_1 \sim Bern(p_1)$; $Z_2 \sim Bern(p_2)$

$\Rightarrow$ ① $Z_1 + Z_2 \sim Bern(b^+(p_1, p_2))$

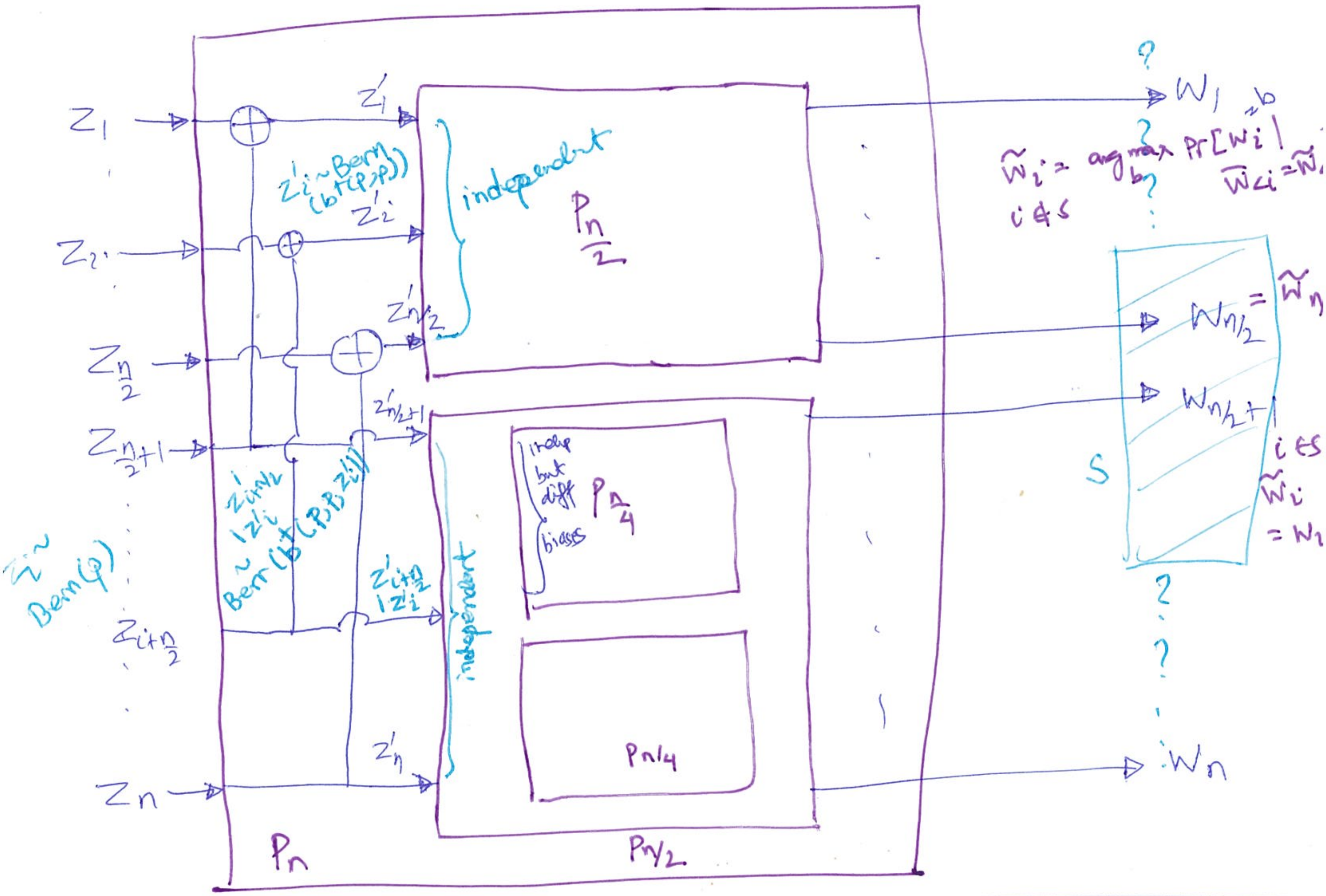
② $Z_2 \mid Z_1 + Z_2 = a \sim Bern(b^1(p_1, p_2, a))$.

TODAY: [Proofreaders: Dennis, Yunus, Yash, Vihari]

(•) Decoder for P_n
(+) Pf of correctness
(•) Quick overview of topics not covered (if time permits)

Decoder: i/p: $\bar{w} \in (\mathbb{F}_2 \cup \{?\})^n$ s.t $\forall i \in S$ $w_i \in \mathbb{F}_2$
o/w $w_i = ?$

$(\text{s.t } \bar{w} = (P_n(Z))_S)$



In general: $(Z_1, \dots, Z_n) \in \text{Bern}(p_1) \times \text{Bern}(p_2) \times \cdots \times \text{Bern}(p_n)$

$1 \le i \le \frac{n}{2}$ $\quad Z_i' \in \text{Bern}(b^+(p_i, p_{i+\frac{n}{2}})) = \text{Bern}(q_i')$

$Z'_{i+\frac{n}{2}} \mid Z_i' \in \text{Bern}(b'(p_i, p_{i+\frac{n}{2}}, z_i')) = \text{Bern}(r_i)$

PHASE 1: Keep doing the recursively ... $W_i \mid \bar{W}_{<i} = \tilde{w}_{<i} \sim \text{Bern}(p_i')$

PHASE 2: (A) $i \in S \Rightarrow \tilde{w}_i = w_i$

$i \notin S \Rightarrow \tilde{w}_i = \arg\max_b \Pr[W_i = b \mid \bar{W}_{<i} = \tilde{w}_{<i}] = \begin{cases} 1 & \text{if } p_i' \ge \frac{1}{2} \\ 0 & \text{o/w} \end{cases}$

(B) $\tilde{Z} = \tilde{W} \cdot P_n^{-1} = (P_{\frac{n}{2}}(\bar{u} + \bar{v}), P_{\frac{n}{2}}(\bar{v}))$ $\quad P_n^{-1} = P_n$ $\quad P_2(P_2(z_1, z_2)) = P_2(z_1 + z_2, z_2) = (z_1, z_2)$

$\bar{W} = P_{\frac{n}{2}}(\bar{u} + \bar{v}) = (P_{\frac{n}{2}}(\tilde{x}), P_{\frac{n}{2}}(\tilde{y})) \Rightarrow \bar{u} = \tilde{x} + \tilde{y}, v = \tilde{y}$

BASIC POLAR DECODER $(\overline{W}; n, p)$

$(\tilde{Z}, \tilde{W}, \bar{p}) \leftarrow \text{RPD}(\overline{W}; n, (p, \ldots, p))$

return $\tilde{Z}$

$\tilde{Z} = P_n^{-1}(\tilde{W})$

function RPD $(\overline{W}; n, (p_1, \ldots, p_n))$

If $n = 1$ // Compute $\tilde{W}$ RPD $((\tilde{W}_1), 1, p_1)$

If $W_1 \in \mathbb{F}_2 \Rightarrow$ return (W_1, W, p_1)

else

if $p_1 \geq \frac{1}{2}$ return $(1, 1, p_1)$

else return $(0, 0, p_1)$

else // phase 1

$\overline{W} = (\overline{W}^{(1)}, \overline{W}^{(2)})$

recurse on 1st half

for $i = 1 \ldots n/2$ $\quad q_i = b^+(p_i, p_{\frac{n}{2}+i})$

$(\tilde{X}, \tilde{W}^1, \bar{p}^{(1)}) \leftarrow \text{RPD}(\overline{W}^{(1)}; \frac{n}{2}, (q_1, \ldots, q_{\frac{n}{2}}))$

for $i = 1 \ldots n/2$ $\quad r_i = b^1(p_i, p_{\frac{n}{2}+i}, \tilde{X}_i)$

$(\tilde{Y}, \tilde{W}^2, \bar{p}^{(2)}) \leftarrow \text{RPD}(\overline{W}^{(2)}; \frac{n}{2}, (r_1, \ldots, r_{\frac{n}{2}}))$

$\tilde{Z} = (\tilde{X} + \tilde{Y}, \tilde{Y})$

$\tilde{W} = (\tilde{W}^1, \tilde{W}^2)$

$\bar{p} = (\bar{p}^{(1)}, \bar{p}^{(2)})$

return $(\tilde{Z}, \tilde{W}, \bar{p})$.

$O(n \log n)$ time.

Correctness lemma: $\bar{Z} \in \text{Bern}(p_1) \times \ldots \times \text{Bern}(p_n)$, $\overline{W} = P_n(\bar{Z})$

$\overline{W}' = (W'_1, \ldots, W'_n)$ s.t. $\forall i \in S$ $W'_i = W_i$ & $W'_i = ?$ o/w

$(\tilde{Z}, \tilde{W}, \bar{p}) \leftarrow \text{RPD}(\overline{W}'; n, (p_1, \ldots, p_n))$

① $\forall i \quad \Pr_Z [W_i = 1 \mid \overline{W}_{<i} = \tilde{W}_{<i}] = p_i$

② $\Pr_Z (\tilde{W} \neq \overline{W}) \leq \tau n$

③ $\Pr_Z (\tilde{Z} \neq \bar{Z}) \leq \tau n$

(Pf in book)

Topics not covered

Combinatorics:

- MRRW bound
- Algebraic Geometric Codes (beat GV for $q \geq 49$) Ex 5.21

Codes:

- Reed-Muller codes (Chap 9)
- Expander codes (Forthcoming)

Algos:

- Decoding RM (Chap 14)
- Sub-linear decoding.