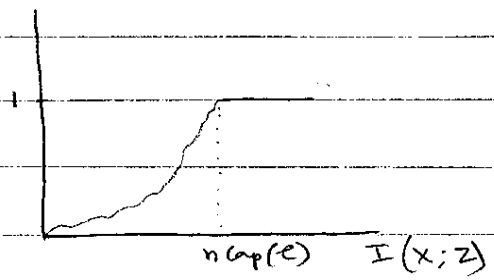
9/10/09

CAPACITY ACHIEVING CODES - RANDOM THOUGHTS

$P_{\mathcal{C}}\{ I(X;Z) \leq n\,cap(\epsilon) \} = CDF(MI)$



$I(X;Z) \rightarrow$ R.V., one value for each code with parameters (k,n,d)

$CDF(MI) \rightarrow$ in the ensemble (k,n,d)

To show that the ensemble is capacity achieving need to show that $CDF(MI-\epsilon) < 1 \quad \forall \epsilon > 0$.

$$\Phi_n(w) = E\left[e^{jwI_n}\right] = \int_{-\infty}^{\infty} e^{jwx} f_{I_n}(x)\,dx$$

$$f_{I_n}(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \Phi_n(w)\, e^{-jwx}\,dw$$

SUMMARY OF KOLCHIN'S RESULTS:

SEC 3.2: Matrices with independent elements.

- $A = \| \alpha_{ij} \| \in \mathbb{F}_2^{T \times n}$

$\alpha_{ij} \sim$ iid Bernoulli - $\frac{1}{2}$

If $n \to \infty$ and $T = n+m$, (m is a fixed integer)

prob $P(rk(A) = r)$ known in closed form (Thm 3.

(this ensemble is not good for channel coding because we always have asymptotic rate = 1)

- Generalization of above result for iid Bernoulli-p.
- Expected value of the number of non-trivial solutions of $A\underline{x} = \underline{0}$, for A of the above type. (Thm 3.2.4)

SEC 3.3: Rank of sparse matrices

$A = \| \alpha_{ij} \| \in \mathbb{F}_2^{T \times n}$

$P\{\alpha_{ij} = 1\} = \frac{\log n + x}{n}$, $P\{\alpha_{ij} = 0\} = 1 - \frac{\log n + x}{n}$

(x is a constant)

$\lim_{n \to \infty} P\{\alpha_{ij} = 1\} = 0$ (sparsity increases with n)

- Limit distribution of $T - \text{rank}(A)$ (Thm 3.3.1)
- System $A\underline{x} = \underline{b}$, $b_i \sim$ iid Bernoulli-$\frac{1}{2}$

Prob. of above system being consistent (Thm 3.3.3)

SEC 3.4: Cycles and consistency of systems of random equations.

$x_{i(t)} + x_{j(t)} = \beta_t$, $t = 1, \ldots, T$

$i(t), j(t) \sim$ iid unif$(1, 2, \ldots, n)$

$\beta_t \sim$ unif$(\mathbb{F}_2)$

- prob of consistency of above system (th. 3.4.2)
- Generalizations to non-equiprobable $i(t), j(t)$ (thm 3.4.3)

SEC 3.5 : Hypercycles and consistency of systems of random equations

$x_{i_1(t)} + \cdots + x_{i_r(t)} = b_t \quad t = 1, \ldots, T$

$i_j(t) \to$ iid, unif$(\{1, 2, \ldots, n\})$

$b_i \to$ iid, unif$(\mathbb{F}_2)$

$A = \|\alpha_{tj}\|_{T \times n}$, No more than r ones on each row

$T, n \to \infty$, $T/n = \alpha$

- Threshold result for the $\mathbb{E}$ # of critical sets (analogous result for $\mathbb{E}$ rank) (th. 3.5.1)

SEC 3.6 : Reconstructing the true solution

$x_{i(t)} + x_{j(t)} = b_t \quad t = 1, \ldots, T$

$i(t) < j(t)$, $(i(t), j(t)) \sim$ iid unif with prob $\binom{n}{2}^{-1}$

true values X^*, $AX^* = B^*$

Corrupted B : $b_t = b_t^* + \varepsilon_t$, $t = 1, \ldots, T$

Given A, B, find X^*

$P(\varepsilon_1 = 1) = p = \frac{1-\Delta}{2}$, $P(\varepsilon_1 = 0) = q = \frac{1+\Delta}{2}$

$\Delta \to 0$ with n

$$\frac{\Delta^2 T}{n \log n} \to \infty$$

$$T = \alpha n \qquad \frac{\Delta^2 \alpha \kappa}{\kappa \log n} \to \infty$$

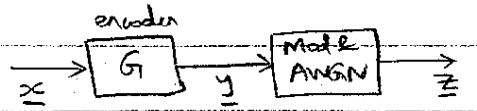
- P_e result for voting algorithm (th. 3.6.1)
- P_e result for coordinate testing (th. 3.6.2)
- P_e result for hybrid algos (th. 3.6.3 & th 3.6.4)

109

LINEAR CODES OVER AWGN :

$$z_i = y_i + w_i \quad , \quad w_i \sim \text{iid } CN(0,1)$$

$$\underset{1\times n}{\underline{y}} = \underset{1\times k}{\underline{x}} \; \underset{k\times n}{G}$$



We use a binary linear code with BPSK signalling $\{-\sqrt{P}, \sqrt{P}\}$

$$I(\underline{z}; \underline{x}) = I(\underline{z}, \underline{y})$$
$$= H(\underline{z}) - \underbrace{H(\underline{z}|\underline{y})}_{= H(\underline{w}) = \log(\pi e)^n}$$

What is $H(\underline{z})$?

pdf of $\underline{z}$:

$$p(\underline{z}) = \sum_{\underline{c} \in \mathcal{C}} \frac{1}{|\mathcal{C}|} \mathcal{N}(\underline{z} - \underline{y}_i) \quad , \mathcal{C} = \{\underline{y}_1, \ldots, \underline{y}_{2^k}\}$$

Need distances to all codewords

codeword $\underline{c} \equiv \left((-1)^{c_1}\sqrt{P}, (-1)^{c_2}\sqrt{P}, \ldots, (-1)^{c_n}\sqrt{P}\right)$

21/10/09

$\underline{z} = \underline{y} + \underline{w}$, $\underline{w} \sim N(0, \frac{1}{\rho} I)$

$$I(\underline{x};\underline{z}) = H(\underline{z}) - H(\underline{z}|\underline{x})$$
$$= H(\underline{z}) - H(\underline{z}|\underline{x},\underline{y})$$
$$\leq H(\underline{z}|\underline{y}) \quad (\text{deterministic fn. of } \underline{x})$$
$$\geq I(\underline{y};\underline{z})$$

$$H(\underline{z}|\underline{y}) = H(\underline{w}) = \frac{1}{2}\log[(2\pi e)^n/\rho^n]$$

Need lower bounds on $H(\underline{z})$

① Entropy-power inequality

$$2^{\frac{2}{n}h(\underline{x}+\underline{y})} \geq 2^{\frac{2}{n}h(\underline{x})} + 2^{\frac{2}{n}h(\underline{y})}$$

$$2^{\frac{2}{n}h(\underline{z})} \geq 2^{\frac{2}{n}h(\underline{y})} + 2^{\frac{2}{n}h(\underline{w})}$$
$$= 2^{\frac{2}{n}\text{rank}(G)} + 2^{\frac{2}{n}\cdot\frac{1}{2}\log\left(\frac{2\pi e}{\rho}\right)^n}$$
$$= 2^{\frac{2}{n}\text{rank}(G)} + 2\pi e/\rho$$

$$\frac{2}{n}h(\underline{z}) \geq \log_2\left[2^{\frac{2}{n}\text{rank}(G)} + 2\pi e/\rho\right]$$

$$h(\underline{z}) \geq \frac{n}{2}\log_2\left[2^{\frac{2}{n}\text{rank}(G)} + 2\pi e/\rho\right]$$

$$I(\underline{x};\underline{z}) \geq \frac{n}{2}\log_2\left[2^{\frac{2}{n}\text{rank}(G)} + 2\pi e/\rho\right] - \frac{n}{2}\log\left(\frac{2\pi}{\rho}\right.$$

$$= \frac{n}{2}\log\left[1 + \frac{2^{\frac{2}{n}\text{rank}(G)}}{2\pi e/\rho}\right]$$

$6 \times 3.14 \times 2.7$

$$= -\frac{n}{2} \log \left[\frac{1}{1 + \frac{2^{3/n \, \text{rank}(G)}}{2\pi e/\rho}} \right]$$

$$-\mathbb{E}[I(\underline{x};\underline{z})] \leq \mathbb{E}\left[\frac{n}{2} \log [\,\cdot\,]\right] \leq \frac{n}{2} \log [\mathbb{E}(\,)]$$

$$\mathbb{E}\, I(\underline{x};\underline{z}) \geq -\frac{n}{2} \log \left[\mathbb{E}\left(\frac{1}{\cdot}\right)\right.$$

$$P_n\{ I(\underline{x};\underline{z}) < n\, \text{Cap}(\mathcal{C}) \}$$

$$\leq P_n\left\{ \frac{n}{2} \log \left[1 + \frac{2^{3/n \, \text{rank}(G)}}{2\pi e/\rho} \right] < n \right\}$$

$$= P_n\left\{ 1 + \frac{2^{3/n \, \text{rank}(G)}}{2\pi e/\rho} < 4 \right\}$$

$$= P_n\left\{ 2^{3/n \, \text{rank}(G)} < 6\pi e \right\}$$

$$= P_n\left\{ \frac{3}{n} \text{rank}(G) < \log_2 6\pi e \right\}$$

$$= P_n\left\{ \text{rank}(G) < \frac{n}{2} \log_2 6\pi e \right\}$$

$\approx 2.8\, n$

Need a closed form expression (or upper bound) on the unconstrained capacity for the BPSK-AWGN channel.

$$I(x;y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)\,p(y)}$$

$$= \sum_{x,y} p(x)\, p(y|x) \log \frac{p(x)\, p(y|x)}{p(x) \sum_{x'} p(x')\, p(y|x')}$$

$$= \int_y \left[\frac{1}{2} p(y|0) \log \frac{p(y|0)}{\frac{1}{2}p(y|0) + \frac{1}{2}p(y|1)} + \frac{1}{2} p(y|1) \log \frac{p(y|1)}{\frac{1}{2}p(y|0) + \frac{1}{2}p(y|1)} \right] dy$$

Can evaluate numerically, using standard techniques (see Chugg notes)

② $h(\underline{z}) = -\int_{\underline{z}} p(\underline{z}) \log p(\underline{z}) \, d\underline{z}$

Using Jensen's inequality,

$\log\left(\mathbb{E}_f(g(x))\right) \geq \mathbb{E}_f[\log g(x)]$

Set $f = g$:

$\log\left(\int f^2(x)\,dx\right) \geq \underbrace{\int f(x) \log f(x)\, dx}_{= -H(x)}$

$h(\underline{z}) \geq -\log\left[\int_{\underline{z}} f^2(\underline{z})\, d\underline{z}\right]$

$f(\underline{z}) = \frac{1}{|C|} \sum_{i=1}^{|C|} N(\underline{z}; \underline{c}_i, \frac{1}{\rho} I)$

$= \frac{1}{|C|} \sum_{i=1}^{|C|} \frac{1}{(\sqrt{2\pi})^n \left(\frac{1}{\rho^n}\right)^{1/2}} e^{-\frac{1}{2}(\underline{z}-\underline{c}_i)^T \rho I (\underline{z}-\underline{c}_i)}$

$= \frac{1}{|C|} \sum_{i=1}^{|C|} \frac{\rho^{n/2}}{(\sqrt{2\pi})^n} e^{-\frac{\rho}{2}|\underline{z}-\underline{c}_i|^2}$

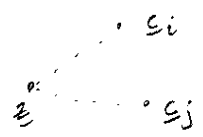
$f(\underline{z})^2 = \frac{\rho^n}{|C|^2 (2\pi)^n} \sum_{i,j=1}^{|C|} e^{-\rho/2\left[|\underline{z}-\underline{c}_i|^2 + |\underline{z}-\underline{c}_j|^2\right]}$

$= \frac{\rho^{2n}}{|C|^2 (2\pi)^n} \sum_{i,j=1}^{|C|} e^{-\rho/2 \left|\begin{bmatrix}\underline{z}\\ \underline{z}\end{bmatrix} - \begin{bmatrix}\underline{c}_i\\ \underline{c}_j\end{bmatrix}\right|^2}$

Define $\underline{z}' = \begin{bmatrix}\underline{z}\\ \underline{z}\end{bmatrix} - \begin{bmatrix}\underline{c}_i\\ \underline{c}_j\end{bmatrix}$ $\quad \underline{z}' \sim N($

$\underline{z}' = \underline{z} - \underline{c}_i \Rightarrow \underline{z} - \underline{c}_j = \underline{z}' + \underline{c}_i - \underline{c}_j$

$\int_{\underline{z}} f(\underline{z})^2 \, d\underline{z} = \int_{\underline{z}'} \frac{\rho^n}{|C|^2 (2\pi)^n} \sum_{i,j=1}^{|C|} e^{-\rho/2\left[|\underline{z}'|^2 + |\underline{z}' + \underline{c}_i - \underline{c}_j|^2\right]} \, d\underline{z}'$



Char. fn of HQF-GRV:

$$\mathbb{E}\left[\exp\left(-s\underbrace{z^+ F z}_{CN(z,R)}\right)\right] = \int_z e^{-s z^+ F z} \frac{1}{\det(\pi R)} e^{-(z-\bar{z})R^{-1}(z-\bar{z})}\, dz$$

$$= \frac{\exp\left(-s z^+ F (I + sRF)^{-1} z\right)}{\det(I + sRF)}$$

Set: $F = I$, $s = \rho/2$, $R = \frac{2}{\rho} I$, $z = \varsigma_j - \varsigma_i$

$$\frac{1}{\det\left(\frac{2\pi}{\rho} I\right)} \int_z e^{-\frac{\rho}{2}|z|^2} e^{-\frac{\rho}{2}|z - (\varsigma_j - \varsigma_i)|^2} dz$$

$$= \frac{\exp\left[-\rho/2\,(\varsigma_j - \varsigma_i)^+ \left(I + \rho/2 \cdot \frac{2}{\rho} I\right)^{-1} (\varsigma_j - \varsigma_i)\right]}{\det\left(I + \rho/2 \cdot \frac{2}{\rho} I\right)}$$

$$\left(\frac{\pi}{\rho}\right)^n \int_z \text{"} \; dz = \frac{\exp\left[-\frac{\rho}{4}|\varsigma_j - \varsigma_i|^2\right]}{2^n}$$

$$\Rightarrow \int_z \text{"} \; dz = \left(\frac{\pi}{\rho}\right)^n \exp\left[-\frac{\rho}{4}|\varsigma_j - \varsigma_i|^2\right]$$

$$\therefore \int_z f(z)^2 dz = \frac{\cancel{\rho^n}}{e^{-i\pi/2}\cancel{\pi^n}} \sum_{i,j=1}^{|C|} \left(\frac{\pi}{\rho}\right)^n \exp\left[-\frac{\rho}{4}|\varsigma_j - \varsigma_i|^2\right]$$

$$= \left(\frac{1}{2}\right)^n \frac{1}{|C|^2} \sum_{i,j=1}^{|C|} \exp\left[-\frac{\rho}{4}|\varsigma_j - \varsigma_i|^2\right]$$

$$h(z) \geq -\log\left[\left(\frac{1}{2}\right)^n \frac{1}{|C|^2} \sum_{i,j=1}^{|C|} \exp\left(-\frac{\rho}{4}|\varsigma_j - \varsigma_i|^2\right)\right]$$

$$I(x, z) \geq -\log[\quad \text{"} \quad]$$

$$- \frac{1}{2}\log\left[(2\pi e)^n/\rho^n\right]$$

$R > 1 \Rightarrow n < k$

$$I(\underline{x};\underline{z}) \geq -\log\left[\left(\frac{1}{2}\right)^n \frac{1}{|\mathcal{C}|^2}\frac{(2\pi e)^{n/2}}{(\rho)^{n/2}}\sum_{i,j=1}^{|\mathcal{C}|}\exp\left(-\frac{\rho}{4}|\underline{c}_j-\underline{c}_i|^2\right)\right]$$

$$= -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2}\cdot\frac{1}{|\mathcal{C}|^2}\sum_{i,j=1}^{|\mathcal{C}|}\exp\left(-\frac{\rho}{4}\underbrace{|\underline{c}_j-\underline{c}_i|^2}_{=4\,d_H(\underline{b}_j,\underline{b}_i)}\right)\right]$$

$$|\underline{c}_j-\underline{c}_i|^2 = \sum_{k=1}^{n}(c_{j,k}-c_{i,k})^2$$

(binary encoded codeword symbols)

$$= \sum_{k=1}^{n}\left[(-1)^{b_{j,k}} - (-1)^{b_{i,k}}\right]^2$$

$$= 4\,d_H(\underline{b}_j,\underline{b}_i)$$

$$I(\underline{x};\underline{z}) \geq -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2}\frac{1}{|\mathcal{C}|^2}\sum_{i,j=1}^{|\mathcal{C}|}\exp\left(-\rho\,d_H(\underline{b}_j,\underline{b}_i)\right)\right]$$

CHECK!

$$= -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2}\frac{|\mathcal{C}|}{|\mathcal{C}|^2}\sum_{i=1}^{|\mathcal{C}|}\exp\left(-\rho\underbrace{d_H(\underline{0},\underline{b}_i)}_{=w_h(\underline{b}_i)}\right)\right]$$

Consider the null-space of the parity check matrix H used to generate the code.

B_w : number of vectors of weight w in the null-space of H

$$I(\underline{x};\underline{z}) \geq -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2}\cdot\frac{1}{|\mathcal{C}|}\sum_{w=0}^{n}B_w\,e^{-w\rho}\right]$$

If $B_w \to 0 \;\forall\; w \geq 1$ (full-rank)

$$I(\underline{x};\underline{z}) \geq -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2}\cdot\frac{1}{|\mathcal{C}|}\right]$$

$|\mathcal{C}| = 2^k$. Let $k = \alpha n$, $0 < \alpha \leq 1$

$$I(\underline{x};\underline{z}) \geq -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2}\cdot\frac{1}{2^{\alpha n}}\right]$$

$H: (n-k) \times n$

$H \underline{c} = \underline{0}$

$(n-k) \times n \quad n \times 1$

$\underline{c}^T H^T = \underline{0}$

$1 \times n \quad n \times (n-k)$ ← More rows than cols.

$-E(I) \leq E(\log(\ ))$

$\leq \log(E(\ ))$

$\left(\sqrt{\frac{\pi e \rho}{2}}\right)^n \cdot \frac{1}{2^{\alpha n}}$

$$= \log\left[\frac{2^{n/2} \rho^{n/2} 2^{\alpha n}}{(\pi e)^{n/2}}\right]$$

$$= \frac{n}{2} + \alpha n - \frac{n}{2}\log_2\left(\frac{\pi e}{\rho}\right)$$

$$P_n\{I(\underline{x};\underline{z}) < n\,Cap(\epsilon)\}$$

$$\leq P_n\left\{-\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2} \cdot \frac{1}{|C|} \sum_{w=0}^{n} B_w e^{-w\rho}\right] < n\,Cap(\epsilon)\right\}$$

$$= P_n\left\{\sum_{w=0}^{n} B_w e^{-w\rho} > 2^{-n\,Cap(\epsilon)} \cdot \left(\frac{2\rho}{\pi e}\right)^{n/2} |C|\right\}$$

$$-I(\underline{x};\underline{z}) \leq \log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2} \frac{1}{|C|} \sum_{w=0}^{n} B_w e^{-w\rho}\right]$$

$$\Rightarrow -E\{I(\underline{x};\underline{z})\} \leq E\left\{\log\left[\quad''\quad\right]\right\}$$

over the code ensemble

$$\leq \log\left\{E\left[\quad''\quad\right]\right\}$$

$$E\{I(\underline{x};\underline{z})\} \geq -\log\left[\left(\frac{\pi e}{2\rho}\right)^{n/2} \frac{1}{|C|} \sum_{w=0}^{n} E\{B_w\} e^{-w\rho}\right]$$

KOLCHIN'S RESULT ON HYPERCYCLES:

$T \times n$ matrix $\underline{A} = [\ \cdots\ ]$ ← max n ones in every row, uniformly distributed (mod 2 addition) (recall Kolchin model)

Hyperedges: $e_t = \{j : a_{tj} = 1\}$, $t = 1, \ldots, T$

Hypercycle: set of edges $C = \{e_{t_1}, \ldots, e_{t_m}\}$ such that the coordinatewise sum of rows $a_{t_1} + \cdots + a_{t_m} = \underline{0}$

(rows $t_1, \ldots, t_m$ sum to zero)

Let $\xi_{t_1, \ldots, t_m} = 1$ if hypercycle C occurs.

Let $\eta_1(s,n), \ldots, \eta_n(s,n)$ denote the contents of the n cells in the equiprobable scheme of allocating s particles into n cells.

$P(\xi_{t_1,\ldots,t_m} = 1) = P\{\eta_{t_1}(rm,n) \in E, \ldots, \eta_{t_m}(rm,n) \in E\}$

$E \rightarrow$ set of even numbers.

Let $P_E(rm,n) \triangleq P(\xi_{t_1,\ldots,t_m} = 1)$ — trivial

Average # of hypercycles ($=$ Avg. # of non-trivial vectors in the left null space of A)

$$\sum_{m=1}^{T} \binom{T}{m} P_E(rm,n)$$

$$P_E(s,n) \leq (\cosh\lambda)^n \frac{s!}{\lambda^s n^s} \qquad \lambda > 0 \text{ can be chosen arbitrarily}$$

$$P_E(rm,n) \leq (\cosh\lambda)^n \frac{(rn)!}{\lambda^{rm} n^{rm}}$$

CODEWORD STATISTICS:

LDPC ensemble, with max d constraints per codeword

$$\underset{n-k \times n}{H} \underline{c} = \underline{0}$$

H has in each row a maximum of d ones (d ones uniformly distributed in n bins)

Hypercycle involving w columns should have even no. of ones in all $(n-k)$ coordinate sums