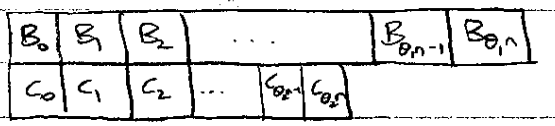
$\begin{matrix} a & b \\ c & d \end{matrix}$ $\quad ac+bd \quad (a+b)(c+d)$

Let B_w and C_w denote the # of codewords of weight w, in the first $\theta_1 n$ code-bits & the l $\theta_2 n$ code-bits. Let D_w denote the resultant wei distrib.

$$D_w = \sum_{i=0}^{w} B_i C_{w-i}$$

$$S = \sum_{w=0}^{n} D_w \rho^w = \sum_{w=0}^{n} \rho^w \sum_{i=0}^{w} B_i C_{w-i}$$



C.S. inequality:

$$S \leq \sum_{w=0}^{n} \rho^w \sqrt{\sum_{i=0}^{w} B_i^2} \sqrt{\sum_{i=0}^{w} C_i^2}$$

$$S = \sum_{w=0}^{n} \sum_{i=0}^{w} \left[(B_i \rho^i)(C_{w-i} \rho^{w-i}) \right]$$

$$\leq \sum_{w=0}^{n} \left[\sum_{i=0}^{w} B_i \rho^i \right] \left[\sum_{i=0}^{w} C_{w-i} \rho^{w-i} \right] \quad \text{, since } B_i, C_i$$

$$= \sum_{w=0}^{n} \left[\sum_{i=0}^{w} B_i \rho^i \right] \left[\sum_{i=0}^{w} C_i \rho^i \right]$$

JUNE '10

DIMAKIS ET. AL. - RD FN. FOR LDGM CODE

Sequence $S \sim$ iid Bernoulli $p = 1/2$. $\quad S \in \{0,1\}^n$

↓ quantize

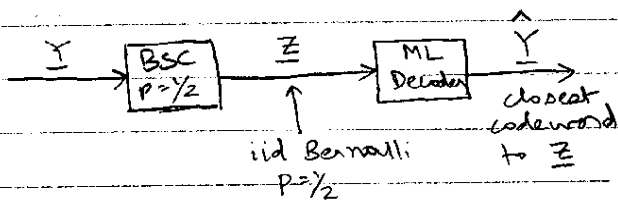
$\hat{Z} \in \{0,1\}^m$

↓ Reconstruct

$\hat{S} = G\hat{Z}$, $\quad \hat{S} \in \{0,1\}^n$

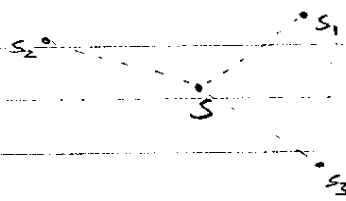
$G \in \{0,1\}^{n \times m}$

Connection with BSC - decoding:



ML - decoding:

Given S, can identify a set $\{\hat{S}_i\}$ of codewords that are closest (at same distance) to S.



If the codeword is unique, can then relate the entropy $H(\hat{Z}|S)$ to the rank of G. Difficulty is in dealing with the case that there are multiple codewords at the nearest neighbour distance.

1|06|10 ANALYZING COMPONENT DUAL CODES SEPARATELY:

$$G = \underbrace{[G_1}_{k\times\theta_1 n} \underbrace{: G_2]}_{k\times\theta_2 n}{}_{k\times n} \qquad \theta_1 + \theta_2 = 1$$

$$q_v = \sum_{u,\ \langle v|u\rangle = 1} p_u \qquad v = [\underbrace{v_1}_{1\times\theta_1 n} : \underbrace{v_2}_{1\times\theta_2 n}] \qquad \mathbb{F}_2^n \ni u = [u_1 : u$$

$$\{u \mid \langle v|u\rangle = 0\} = \left\{u \;\middle|\; \begin{array}{l} \langle v_1|u_1\rangle = 0 \ \&\ \langle v_2|u_2\rangle = 0 \\ \text{OR} \quad \langle v_1|u_1\rangle = 1 \ \&\ \langle v_2|u_2\rangle = 1 \end{array}\right\}$$

$$1 - q_v = \underbrace{\sum_{\substack{u:\ \langle v_1|u_1\rangle = 0 \\ \langle v_2|u_2\rangle = 0}} p_u}_{\triangleq\, q_v^1} + \underbrace{\sum_{\substack{u:\ \langle v_1|u_1\rangle = 1 \\ \langle v_2|u_2\rangle = 1}} p_u}_{\triangleq\, q_v^2}$$

$$Y = XG$$
$$= X[G_1\ G_2]$$

$$[Y_1\ Y_2] = [XG_1\ XG_2]$$

$$\overset{\tau}{\downarrow}\quad\overset{\tau = BSC(p)}{\downarrow}$$

$$Z_1\quad Z_2$$

$$z_i = Y_i + \xi_i$$

$$q_v^2 = P_r\{ v_1 z_1^T = 1\ ,\ v_2 z_2^T = 1 \}$$

Suppose that v is such that $v_1 \notin C_1^\perp$, $v_2 \notin C_2^\perp$

$$q_v^2 = P_r\{ v_1(Y_1 + \xi_1) = 1\ ,\ v_2(Y_2 + \xi_2) = 1 \}$$

CHECK!

$$= P_r\{ \beta_1 = 1\ ,\ \beta_2 = 1 \}, \qquad \beta_1, \beta_2 \sim \text{iid Bernoulli}$$

$$= 1/4 = q_v^1$$

$v_1 \in C_1^\perp$, $v_2 \in C_2^\perp$:

$$q_v^2 = P_r\left\{ \sum_{i:(v_1)_i=1} \xi_i = 1\ ,\ \sum_{i:(v_2)_i=1} \xi_i = 1 \right\}$$

$$= P_r\left\{ \sum_{i:(v_1)_i=1} \xi_i = 1 \right\} \cdot P_r\left\{ \sum_{i:(v_2)_i=1} \xi_i = 1 \right\}$$

$$= \frac{1 - \prod_{i,(v_1)_i=1}(1-2p_i)}{2} \cdot \frac{1 - \prod_{i,(v_2)_i=1}(1-2p_i)}{2}$$

$v_1 \in C_1^\perp$, $v_2 \notin C_2^\perp$:

$$q_v^2 = P_r\left\{ \sum_{i:(v_1)_i=1} \xi_i = 1\ ,\ \beta_2 = 1 \right\}$$

$$= \frac{1}{2} \cdot \left[\frac{1 - \prod_{i,(v_1)_i=1}(1-2p_i)}{2} \right]$$

$v_1 \notin C_1^\perp$, $v_2 \in C_2^\perp$ $\quad q_v^2 = \frac{1}{2}\left[\frac{1 - \prod_{i,(v_2)_i=1}(1-2p_i)}{2} \right]$

$v_1 \in C_1^\perp$, $v_2 \in C_2^\perp$: $\quad \overbrace{\prod_{i,(v_1)_i=1}(1-2p_i)}^{\triangleq a}$ $\quad \overbrace{\prod_{i,(v_2)_i=1}(1-2p_i)}^{\triangleq b}$

$$q_v' = \left(\frac{1+\prod_{i,(v_1)_i=1}(1-2p_i)}{2}\right)\left(\frac{1+\prod_{i,(v_2)_i=1}(1-2p_i)}{2}\right)$$

$v_1 \in C_1^\perp$, $v_2 \notin C_2^\perp$:

$$q_v' = \frac{1}{2}\left[\frac{1+\prod_{i,(v_1)_i=1}(1-2p_i)}{2}\right]$$

$v_1 \notin C_1^\perp$, $v_2 \in C_2^\perp$:

$$q_v' = \frac{1}{2}\left[\frac{1+\prod_{i,(v_2)_i=1}(1-2p_i)}{2}\right]$$

$v_1 \notin C_1^\perp$, $v_2 \notin C_2^\perp$: $1-q_v = 1/2$

$v_1 \in C_1^\perp$, $v_2 \notin C_2^\perp$: $1-q_v = \frac{1}{2}\left[\frac{1}{2}+\frac{1}{2}\right] = \frac{1}{2}$

$v_1 \notin C_1^\perp$, $v_2 \in C_2^\perp$: $1-q_v = \frac{1}{2}$

$v_1 \in C_1^\perp$, $v_2 \in C_2^\perp$:

$$1-q_v = \frac{1}{4}\left[(1+a)(1+b) + (1-a)(1-b)\right]$$

$$= \frac{1}{4}\left[1+a+b+ab+1-a-b+ab\right]$$

$$= \frac{1}{2}\left[1+ab\right]$$

$$= \frac{1}{2}\left[1+\prod_{i,(v_1)_i=1}(1-2p_i)\cdot\prod_{i,(v_2)_i=1}(1-2p_i)\right]$$

$$= \frac{1}{2}\left[1+\prod_{i,v_i=1}(1-2p_i)\right]$$

$$\Rightarrow q_v = \frac{1}{2}\left[1-\prod_{i,v_i=1}(1-2p_i)\right]$$

$$\sum_{v \in \mathbb{F}_2^n} (1-2q_v)^2 = \sum_{v_1 \in \mathbb{F}_2^{\theta_1 n}} \sum_{v_2 \in \mathbb{F}_2^{\theta_2 n}} (1-2q_{v_1 v_2})^2$$

$$= \sum_{\substack{v_1 \in C_1^\perp \\ v_2 \in C_2^\perp}} \left[\prod_{i,\, v_i = 1} (1-2p_i)^2 \right]$$

Suppose that all the $p_i = p$

$$\sum_{v \in \mathbb{F}_2^n} (1-2q_v)^2 = \sum_{w_1=0}^{\theta_1 n} \sum_{w_2=0}^{\theta_2 n} B_{w_1} B_{w_2} (1-2p)^{2(w_1+w_2)}$$

$$= \sum_{w_1=0}^{\theta_1 n} \sum_{w_2=0}^{\theta_2 n} B_{w_1} (1-2p)^{2w_1} \cdot B_{w_2} (1-2p)^{2w_2}$$

$$= \left[\sum_{w_1=0}^{\theta_1 n} B_{w_1} (1-2p)^{2w_1} \right] \cdot \left[\sum_{w_2=0}^{\theta_2 n} B_{w_2} (1-2p)^{2w_2} \right]$$

$$\log_2 \left[\sum_{v \in \mathbb{F}_2^n} (1-2q_v)^2 \right] = \log_2 \left[\sum_{w_1=0}^{\theta_1 n} B_{w_1} (1-2p)^{2w_1} \right] + \log_2 \left[\sum_{w_2=0}^{\theta_2 n} B_{w_2} (1-2p)^{2w_2} \right]$$

14/06/10

EXTENSION TO MORE THAN 2 DEGREES:

$$G = [G_1\ G_2 \ \dots\ G_N]_{k \times n} \qquad G_i = k \times \theta_i N$$

$$v = [v_1\ v_2 \ \dots\ v_N]_{k \times n}$$

$$\{u \mid \langle v|u \rangle = 0\} = \{u \mid \text{even number of } \langle v_i|u_i \rangle = 1\}$$

Suppose that all $v_i \in C_i^\perp$

$$\Pr\{vz^T = 0\} = \Pr\{\text{exactly an even no. of } v_i z_i^T = 1, \text{ rest } 0\}$$

$$= \Pr\{\text{Zero number of } v_i z_i^T = 1,\ N \text{ of them zero}\} +$$

$$\Pr\{\text{Two } \dots\ \dots\ \dots\ \dots,\ N-2\ \dots\ \dots\ \dots\} +$$

$$\dots + \Pr\{N \text{ of them } 1,\ 0 \text{ of them zero}\}$$

DEPENDENCE BETWEEN SUMS OF CODEWORDS

$$\Pr\left\{ v_1^T(Y_1 + \xi_1) = 1 \;,\; v_2^T(Y_2 + \xi_2) = 1 \right\}$$

$$v_1^T Y_1 \neq 0 \;, \quad v_2^T Y_2 \neq 0$$

Each component of $Y_1 (Y_2)$ is a sum of $d_1 (d_2)$ randomly chosen info. symbols.
Let w_1 & w_2 denote the weights of v_1 and v_2.

Have a total of k info symbols, iid Bernoulli($\frac{1}{2}$)
Sum 1: Pick $w_1 d_1$ from the info symbols (with replacement) and add w_1 iid Bernoulli(p) variables to it
Sum 2: $w_2 d_2$ from info symbols + w_2 iid Bernoulli(p)

$$\text{Need} \quad P(\text{sum 1} = 1, \ \text{sum 2} = 1)$$
$$\leq P(\text{sum 1} + \text{sum 2} = 0)$$

If there is one info symbol that appears solely in sum i and not sum j ($i \neq j$), then sum 1 and sum 2 are independent. What is this probability equal to?

One particular way in which atleast one symbol is distinct between the two sums: for sum 1, pick the first variable, and pick the remaining $(w_1 d_1 - 1)$ from the remaining $(k-1)$ variables. For sum 2, pick $w_2 d_2$ variables from the $(k-1)$ variables.
# of ways in which this can be done:

$$k \cdot (k-1)^{w_1 d_1 - 1} \cdot (k-1)^{w_2 d_2}$$

Total # of ways of picking the two sums: $k^{w_1 d_1} \cdot k^{w_2 d_2}$

$$\text{Prob(atleast one distinct)} \geq \frac{k \cdot (k-1)^{w_1 d_1 + w_2 d_2}}{(k-1) \; k^{w_1 d_1 + w_2 d_2}} = \left(\frac{k-1}{k}\right)^{w_1 d_1 + w_2 d_2 - 1}$$

At worst, w_i grows as $\alpha_i k$

$$Pr(\text{atleast one distinct}) \geq \left(\frac{k-1}{k}\right)^{k(d_1\alpha_1 + d_2\alpha_2) - 1}$$

$$= \left(\frac{k-1}{k}\right)^{\beta k - 1}, \text{ some const.}$$

$$= \left(1 - \frac{1}{k}\right)^{\beta k} \cdot \frac{1}{1 - \frac{1}{k}}$$

$$\left\{ e^x = \lim_{n \to \infty} \left(1 + \frac{x}{n}\right)^n \right\}$$

$$\lim_{k \to \infty} Pr\{\text{atleast one distinct}\} \geq e^{-\beta}$$

Suppose that we exclude one variable (into symbol) from the set of codewords with degree d_1 and only include it in the set with degree d_2.
What is the prob. that the $w_2 d_2$ variables picked for sum 2 contains this particular into symbol?

Prob. that it will appear:

$$\frac{1 \cdot (k-1)^{w_2 d_2 - 1} + 1 \cdot (k-1)^{w_2 d_2 - 3} + 1 \cdot (k-1)^{w_2 d_2 - 5} + \cdots + (k-1)^0}{k^{w_2 d_2}}$$

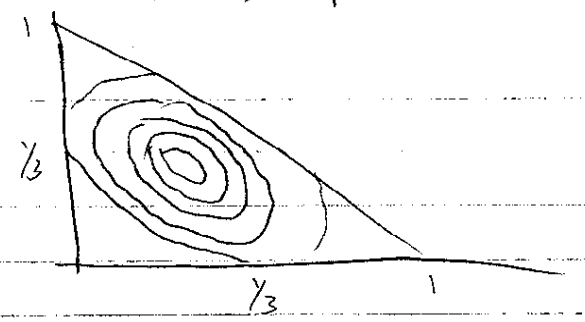
↑ if $w_2 d_2$ is odd

$$= 1 \cdot \left[(k-1)^2\right]$$

$1 \geq X, Y, Z \geq 0$, $X+Y+Z = 1$

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

$\tilde{H}(X, Y) = \mu$



$$P_u \xrightarrow{H} q_v$$

$$H(z)$$

$$\| P_u - H_\pi^{-1} \| = \| q_v - \pi \|$$

8/06/10

I.I.D RANDOM CASE :

Analyze the quantity $Pr\{ I(X, Z) < n\,Cap(\tau) \}$ for the iid random ensemble. This will allow us to see if our bounding techniques are responsible for the looseness in threshold, or if it is a limitation of the fact that we aren't choosing an appropriate backoff from capacity. See if the random coding case provides some hints on choosing good backoffs.

Look at the bounds of Macmullan & Collins. Try to use some facts that the coset of a random code is yet another random code, and see if this bound can be analysed.

28/06/10

WEIGHT DISTRIBUTION OF RANDOM LINEAR CODES

Random linear code $C(n, k)$ in $\mathbb{F}_q^n$

$G \in \mathbb{F}_q^{k \times n}$: entries chosen iid from $\mathbb{F}_q$ with prob.

A_i : # of codewords of Hamming weight i,

$i = 0, 1, \ldots, n$

$x \log\left(\frac{1}{x}\right)$ $\quad f(\mathbb{E}(x)) \geq \mathbb{E}[f(x)]$

$$W_C(x) = \sum_{i=0}^{n} A_i x^i$$

$$\mathbb{E}\left[W_C(x)\right] = 1 + \frac{q^k - 1}{q^n}\left(1 + (q-1)x\right)^n$$

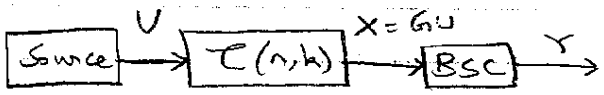
See Blinovsky, Erez & Litsyn, "Weight distribution moments of random linear coset codes" Des. Codes Cryptogr.

Random coset code:

$$\tilde{C}(n,k) = C(n,k) + \tilde{c}_0, \qquad \tilde{c}_0 \sim \text{unif}\left(\mathbb{F}_q^n\right)$$

$$\mathbb{E}\left[W_{\tilde{C}}(x)\right] = q^{k-n}\left[1 + (q-1)x\right]^n$$

MACMULLAN & COLLINS' RESULT:



It is assumed that X is an invertible funct of U, i.e., that G is of rank k.

$$C_{YX} = C_{YU} = k + H(R) - nH(p), \quad \text{where}$$

$$H(R) = \sum_{i=1}^{2^{n-k}} \sum_{j=0}^{n} w(i,j)\, p^j (1-p)^{n-j} \log\left[\frac{1}{\sum_{j=0}^{n} w(i,j)\, p^j (1-p$$

$w(i,j) \rightarrow$ # of n-tuples of Hamming weight j in i^{th} row of the standard array of $C(n,k$

In general, the rank is not always full when picking all entries of G iid uniformly at random from $\mathbb{F}_q$. Pdf of the rank known, see Levitskaya

Suppose that we have a many to one mapping:

$$U \xrightarrow{\text{many to one}} X \longrightarrow Y$$

Suppose that groups of n_u number of values of U get mapped to a particular X.

Claim: $H(Y/X) = H(Y/U)$ (see AWGN writeup for a proof)

Hence the invertability assumption for $U \to X$ is not needed in MacMillan-Collins.

Let $W_{c,i} \longrightarrow$ weight enumerating fn. for the i^{th} row of the std. array

$$H(R) = \sum_{i=1}^{2^{n-k}} \sum_{j=0}^{n} w(i,j)\, p^j (1-p)^{n-j} \log\left[\frac{1}{(1-p)^n\, W_{c,i}\left(\frac{p}{1-p}\right)}\right]$$

$$= \sum_{i=1}^{2^{n-k}} \log\left[\frac{1}{(1-p)^n\, W_{c,i}\left(\frac{p}{1-p}\right)}\right] (1-p)^n\, W_{c,i}\left(\frac{p}{1-p}\right)$$

EVALUATING OUR BOUNDS FOR THE RANDOM ENSEMBLE

$$P_n\left\{ I(X,Z) < n\, Cap(C)\right\} \le \log_2\left(\sum_{w=0}^{n} E[B_w]\,(1-2p)^{2w}\right)$$

$$= \log_2\left(E\left\{W_C\left((1-2p)^2\right)\right\}\right)$$

Incorrect, need to evaluate for weight enumerator for the dual code (this is what B_w stands for)

$$= \log_2\left[1 + \frac{2^k - 1}{2^n}\left(1 + (1-2p)^2\right)^n\right]$$

$$\left(2^k - 1\right)\left(\frac{1+(1-2p)^2}{2}\right)^n \le \left(2^R\,\frac{\left(1+(1-2p)^2\right)}{2}\right)^n \longrightarrow 0$$

$2^{R-1}\left[1+(1-2\right.$

< 1

$$2^R < \frac{2}{1+(1-2p)^2}$$

$$R < \log_2\left[\frac{2}{1+(1-2p)^2}\right]$$ ← Does not make sense. Looks like the condition to be

Wadayama's paper (Arxiv, Mar. 2008):

Random LDPC ensemble has weight distribution

$$\mathbb{E}[B_w] = \binom{n}{w} 2^{-(n-k)} \quad \text{for } n \geq 1,\ w \geq 1$$

$$\sum_{w=0}^{n} \mathbb{E}[B_w](1-2p)^{2w} = 1 + 2^{-(n-k)}\left[\sum_{w=1}^{n}\binom{n}{w}\left[(1-2p)^2\right]^w (1\right.$$

$$= 1 + 2^{-(n-k)}\left\{\left[1+(1-2p)^2\right]^n - 1\right\}$$

$$2^{-(n-k)}\left\{\left[1+(1-2p)^2\right]^n - 1\right\} \leq 2^{-(n-k)}\left[1+(1-2p)^2\right.$$

CHECK:

$\mathbb{E}[W_c(1)]$ should be equal to q^k

Blinovsky: $\mathbb{E}[W_c(1)] = 1 + \frac{q^k - 1}{q^n}\left(1+(q-1)(1)\right)^n$

$= q^k$ ✓

Wadayama $1 + \sum_{w=1}^{n}\binom{n}{w} 2^{-(n-k)}$

$= 1 + 2^{-(n-k)} \cdot (2^n - 1)$

$= 1 + 2^k - 2^{n-k} \neq 2^k$ (??)

30/06/10

CALCULATING THE WEIGHT ENUMERATOR FOR THE RANDOM ENSEMBLE :

Along the lines of Blinovsky et al.,

$$W_c(x,y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$$

$$= \sum_{m=0}^{n} \left(\sum_{i=0}^{q^k-1} \xi_{im} \right) x^m y^{n-m}$$

$$\mathbb{E}(\xi_{im}) = \begin{cases} 1, & i=0, m=0 \\ 0, & i=0, m\neq 0 \\ \frac{1}{q^n}\binom{n}{m}(q-1)^m, & \text{otherwise} \end{cases}$$

$$W_c(x,y) = y^n + \sum_{m=0}^{n} \sum_{i=1}^{q^k-1} \frac{1}{q^n}\binom{n}{m}(q-1)^m x^m y^{n-m}$$

$$= y^n + \frac{q^k-1}{q^n} \sum_{m=0}^{n} \binom{n}{m} [x(q-1)]^m y^{n-m}$$

$$= y^n + \frac{q^k-1}{q^n} \left[y + x(q-1) \right]^n$$

MacWilliams identity :

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(y-x, y+x)$$

The problem in using MacWilliams identity for the ensemble is that the code size is random as well