Error Correcting Codes: Combinatorics, Algorithms and Applications (Spring 2010)

Lecture 29: Construction of Disjunct Matrices

March 31, 2010

Lecturer: Atri Rudra *Scribe: Sarah Karpie*

Some sort of introduction to construction of disjunct matrices.

1 D-Disjunction Matrix

Definition 1 *A d-disjunct matrix is a matrix for which* $\forall S \subseteq [n]$, $|S| \leq d$, $\forall j \in S$, $\exists i$ *s.t.* $M_{i,j}$=1 *and* $\bigcup_{k \in S} M_{ik}$= 0.

Please note that all matrices noted in this lecture are binary.

$\Omega(d\ log\ n) \leq t(d,n) \leq n$

(i) Strongly explicit: $t(d,n) \leq O(d_2\ log_2\ n)$, (ii) Randomized: $t(d,n) \leq O(d_2\ log\ n)$

Lemma 1 *Where* $d \leq d \leq n$, *let M be a txn matrix, (i)* $\forall j \in [n]$, $|M_j| \geq w_{min}$ *and (ii)* $\forall i \neq j \in [n]$ $|M_i \cap M_j \leq$? *for some integers* $a_{max} \leq w_{min} \leq t$, *where a stands for agreement and w stands for weight. Then M is* $\left\lfloor \dfrac{w_{min}-1}{a_{max}} \right\rfloor$*-disjunct.*

This is stronger than simply having a subset of size B, this is saying for apair of columns. Therefore no matter what column i you choose in the matrix, that column will contain atleast w_{min} 1s, and the total number of 1s shared by two columns is at most a_{max}.

Example 1 *Fix an arbitrary* $S \subseteq [n]$, $|S| \leq d$, $j \notin S$, *and each column has a different arrangement of 1s in each column. For a value in column i that is equal to 1, there is a match if there exists a 1 in another column j. In this case the total number of matches* $\leq a_{max} \cdot\ d \leq a_{max} \left(\dfrac{w_{min}}{a_{max}}\right) = w_{min} - 1 < w_{min}$. *Therefore there must be an all 0 row in S.*

Step 1: $|C| = n$, $C \subseteq \{0,1\}_t$, *and* $C = \{\bar{c}_1, \cdots, \bar{c}_n\}$

$$M_C = \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ \bar{c}_1 & \bar{c}_2 & \cdots & \bar{c}_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix}$$

We need to find a C* s.t. (i) $\forall \bar{c} \in$ C*, $|c| \geq w_{min}$ and (ii) $\forall \bar{c}_1 \neq \bar{c}_2 \in$ c*, $|\{i \mid \bar{c}_1^2 = \bar{c}_2^2 = 1\}|$ $\leq a_{max}$ Need to show M_{C^*} is $\left\lfloor \dfrac{w_{min}-1}{a_{max}} \right\rfloor$-disjunct.

Note that the lower bound of the hamming weight for this matrix is greater than w_{min}

2 Kautz-Singleton Code Concatenation

Pick an Reed-Sullivan code with a block length q, c* $= c_{out} \cdot c_{in}$, c_{out}: $[q,k]_q$–RS code, c_{in}: $[q] \rightarrow \{0,1\}^q$, j $\in [q]$, $c_{in}(j) = (00\cdots010\cdots00)$, where 1 is in the i^{th} position.

Example 2 *Let k=1, q=3,* $c_{out} = (0,0,0),(1,1,1),(2,2,2), n = q^k, t = qxq = q^2$, *so* w_{min}=*q*

$$M_{C^*} = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \qquad \rightarrow \qquad M_{C^*} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Divide the rows into q sized chunks, and number these rows as [q] x [q]. Each column then corresponds to a codeword, M defined as M_{C^*}. Where $\bar{c}_{k_1}$,$\bar{c}_{k_2} \in c_{out}$, if $M_{(i,j),k_1} = M_{(i,j),k_2} = \bar{c}_{k_1}$(i) $= \bar{c}_{k_2}$(i) = j. So the corresponding codeword **agreed** in postion i.

This implies that $|M_{k_1} \cap M_{k_2}|$ = q - $\triangle(\bar{c}_{k_1}, \bar{c}_{k_2}) \rightarrow \leq$ k - 1 defined as a_{max}. Note that $\triangle(\bar{c}_{k_1}, \bar{c}_{k_2}) \geq$ q - k + 1 (MDS) and that $\left\lfloor \dfrac{w_{min} - 1}{a_{max}} \right\rfloor$ is defined as d.

Now pick q and k so the ratio equals d exactly. (s.t. $\left\lfloor \dfrac{q-1}{k-1} \right\rfloor$ = d) Now $\dfrac{q}{k} \simeq$ d $\Rightarrow$ q $\simeq$ kd, and therefore q_k = n $\Rightarrow$ k = $\dfrac{logn}{logq} \leq$ log n. So one can imply that t = $q^2 \cong (kd)^2 \leq$ (d log n)^2 $\surd$

Now pick d = d^2 log n with a large constant...txn every entry...$\dfrac{t}{d}$ expected weight for...and somehow missed the last statment of the lecture...