GT 8

11,8 , 11,10

Date / /

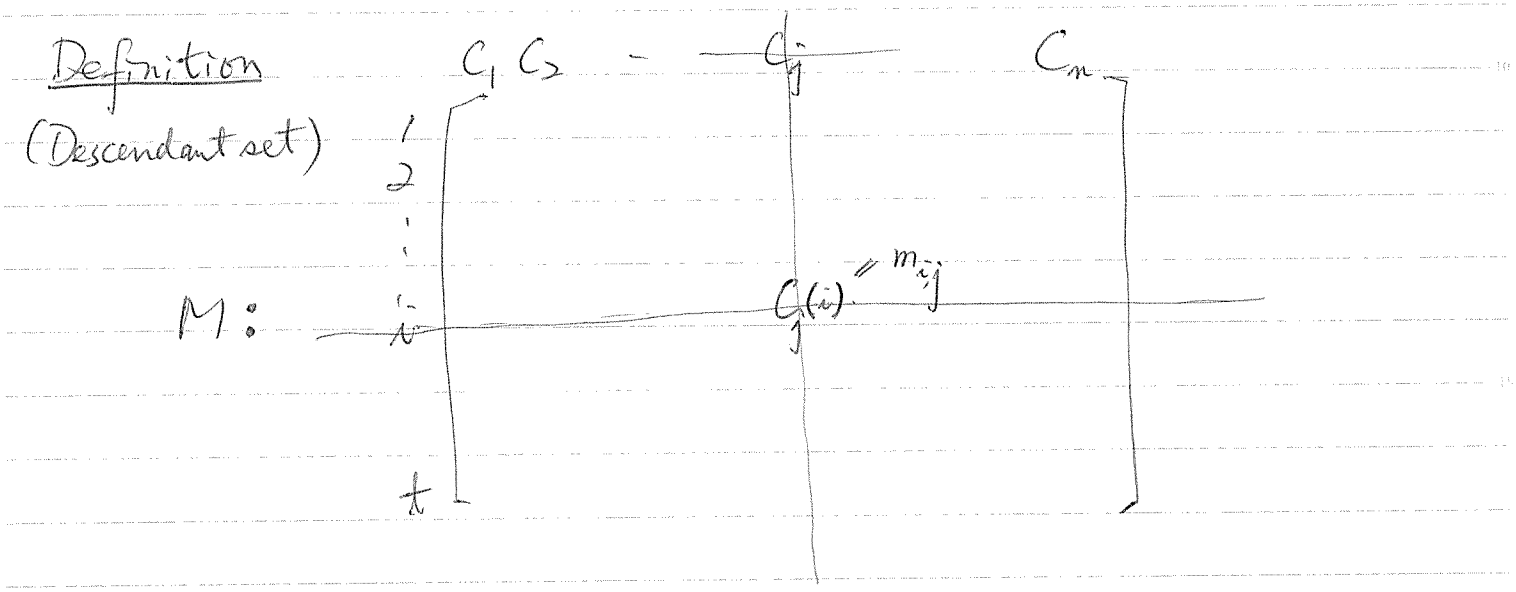
No. 1

We can extend the idea of d-separability (or $\bar{d}$-separability) to a $[0, q-1]$-matrix where $q \geq 2$. Regularly, q is taken as a prime power for the sake of computation. We start with an example.

Let M': $\begin{matrix} c_1 & c_2 & c_3 & c_4 & c_5 \end{matrix}$

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 2 \\ 1 & 2 & 3 & 1 & 3 \end{bmatrix}$$

. Is M' 2-separable or $\bar{2}$-separable?



The matrix we consider is of the above form. We shall treat each column as a column vector (or a codeword) and thus $C_j(i)$ will be the ith coordinate of the vector C_j. Now, let $\mathbb{C}$ be a set of column vectors say $\{C_1, C_2, \cdots, C_d\}$. Then, we use $\mathbb{C}(i)$ to denote the set of ith coordinates of C_i's where $i = 1, 2, \cdots, d$, i.e., $\mathbb{C}(i) = \{C_1(i), C_2(i), \cdots, C_d(i)\}$. The descendant set (code) of $\mathbb{C}$ is

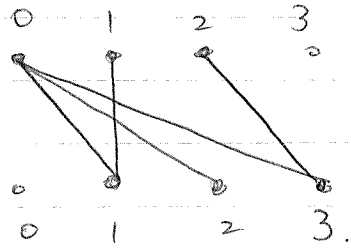
For example, in M' mentioned above, the descendant set of $\{C_1, C_2, C_4\} = \{0,1\} \times \{1,2\}$. (Note that C_1, C_2, C_4 are possible vectors of the form $(0,1)^t, (0,2)^t, (1,1)^t, (1,2)^t$ then.)

Definition M is d-separable if for any two distinct d-subsets (at most for $\bar{d}$) of $\{C_1, C_2, \cdots, C_n\}$, their corresponding descendant sets are distinct. $\mathbb{C}_1, \mathbb{C}_2$, $des(\mathbb{C}_1) \neq des(\mathbb{C}_2)$

Again, in M', all descendant sets of two column vectors are $\{0\} \times \{1,2\}, \{0\} \times \{1,3\}, \{0,1\} \times \{1\}, \{0,2\} \times \{1,3\}, \{0\} \times \{2,3\}, \{0,1\} \times \{1,2\}, \{0,2\} \times \{2,3\}$, $\{0,1\} \times \{1,3\}, \{0,2\} \times \{3\}, \{1,2\} \times \{1,3\}$. Since they are distinct, M' is 2-separable. Furthermore, M' is $\bar{2}$-separable. But, let $\mathbb{C}_1 = \{C_1, C_4, C_5\}$ and $\mathbb{C}_2 = \{C_3, C_4, C_5\}$. Then, $des(\mathbb{C}_1) = \{0,1,2\} \times \{1,3\}$ and $des(\mathbb{C}_2) = \{0,1,2\} \times \{1,3\}$. This implies that M' is not 3-separable.

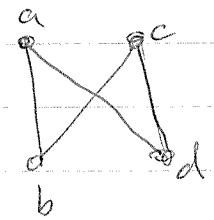
Observation Let M' be a $2 \times n$ $[0, q-1]$-matrix. Then we can view each vector as an edge of a bipartite graph defined on (A, B) where $A = B = \mathbb{Z}_q$.

e.g. $M' \approx$



Fact 1. Let G be the graph induced by the columns of a $2 \times q$ $[0, q-1]$-matrix A. Then A is 2-separable if and only if G does not contain a 4-cycle.

Proof. ($\Rightarrow$) If G contains a 4-cycle (a,b,c,d), then $\mathrm{des}(\{(a,b)^t, (c,d)^t\}) = \mathrm{des}(\{(a,d)^t, (c,b)^t\})$. Hence A is not 2-separable. Since the reverse statement is also true, we have ($\Leftarrow$). ∎



Fact 2. Let $\mathbb{C}$ denote the set of column vectors. Then,

$\max. |\mathbb{C}| = \mathrm{ext.}(n, n; C_4\text{-free})$.

Definition Let $z(m,n;h,k)$ denote the maximum number of edges in a bipartite graph defined on (A,B) where $|A| = m$ and $|B| = n$ which forbids $K_{h,k}$.

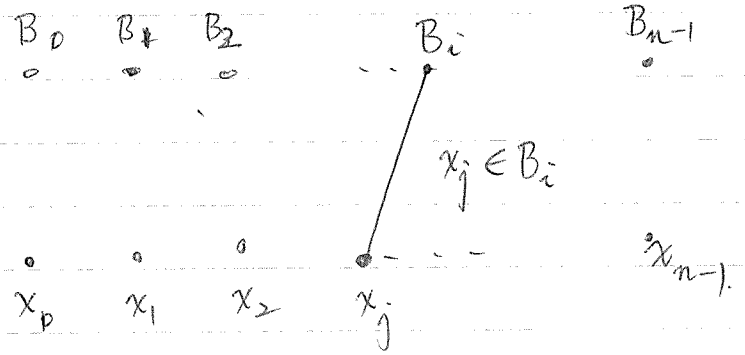
Open problem (Zarankiwicz's problem)

Fact 3. If $m = n = q^2+q+1$ where q is a prime power, then $z(n,n;2,2) = (q^2+q+1)\cdot(q+1)$.

Proof. This result can be obtained from the existence of a Projective plane.

(Review: If $(X,\mathcal{B})$ is a projective plane of order q, then $|X| = q^2+q+1$, $|\mathcal{B}| = q^2+q+1$ and for each $B \in \mathcal{B}$, $|B| = q+1$.)

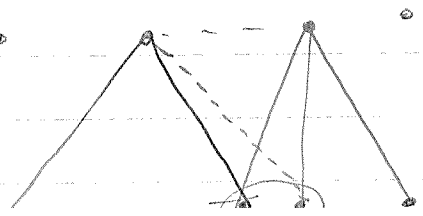
Now, let $n = q^2+q+1$, $X = \{x_i \mid i \in \mathbb{Z}_n\}$ and $\mathcal{B} = \{B_i \mid i \in \mathbb{Z}_n\}$.



① $\|G\| = (q+1)(q^2+q+1)$.

② Since $|B_i \cap B_{i'}| \leq 1$, G contains no 4-cycle.

③ Adding one more edge not in G will produce a 4-cycle.



(•) Most of n, $\exists(n,n;2,2)$ is unknown.

Now, we consider $\bar{3}$-separable case.

Observation If $A_{2\times n}$ is $\bar{3}$-separable, then its corresponding graph defined on (A,B) where $A=B=\mathbb{Z}_n$ can not contain a 4-cycle and a 6-cycle. That is the girth of G is at least 8.

Proof If G contains a 6-cycle (a,b,c,d,e,f), then

$$des(\{a,b\},\{c,d\},\{e,f\}) = des(\{c,b\},\{e,d\},\{a,f\}).$$

Fact 4. Let $\mathbb{C}$ be the set of column vectors of a $\bar{3}$-separable $2\times n$ matrix $\underset{\wedge}{A}$. Then $\max|\mathbb{C}| = ext.(n,n;\underbrace{C_4,C_6\text{-free}}_{girth(G)\geq 8})$.

Open problem Let $G=(A,B)$ such that $|A|=|B|=n$ and G (G bipartite) is of girth 8. Find the maximum size of G.

(•) Not much is known so far.

Open problem How about girth $2t$ for $t\geq 5$?

Open problem How to deal with $3\times n$ $[0,g-1]$-matrices?

Basic Idea in Coding Theory

(To be used in GT with errors occurred in outcomes! (Non-adaptive algorithm))

Definition (q-ary codes)

A q-ary code of length n is a subset of $(\mathbb{Z}_q)^n$, i.e., $\mathbb{C}$ is a set of vectors (codewords) selected from $(\mathbb{Z}_q)^n$. Clearly, $(\mathbb{Z}_q)^n$ contains q^n codewords.

In general, $\mathbb{Z}_q$ is replaced by $GF(q)$ a finite field of order q and thus q is chosen to be a prime power.

Definition (Distance)

The distance between two codewords $\vec{x} = (x_0, x_1, \cdots, x_{n-1})$ and $\vec{y} = (y_0, y_1, \cdots, y_{n-1})$,

$d(\vec{x}, \vec{y}) = |\{ i \mid x_i \neq y_i,\ i = 0, 1, 2, \cdots, n-1 \}|$ i.e., the number of coordinates which are distinct following the order.

Definition (Distance of a code)

Let $\mathbb{C} = \{\vec{x}_1, \vec{x}_2, \cdots, \vec{x}_m\}$ be a code. Then the distance of $\mathbb{C}$,

$d(\mathbb{C}) = \min_{\text{def}} \{ d(\vec{x}_i, \vec{x}_j) \mid 1 \leq i < j \leq m \}$.

For example, $\mathbb{C} = \{(1,1,0,1,0,0,0), (0,1,1,0,1,0,0), (0,0,1,1,0,1,0),$

(•) Fact If $\mathcal{C}$ is code (binary) of distance d, then $\mathcal{C}$ can detect (up to) $d-1$ errors and correct (up to) $\lfloor \frac{d-1}{2} \rfloor$ errors.

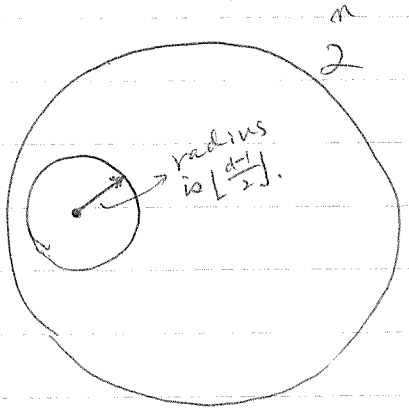
The fundamental problem of coding theory

Let $A_q(n,d)$ denote the maximum number of codewords in a q-ary code of length n with code distance d. (If $q=2$, we use $A(n,d)$ for convenience.)

Example $A(7,3) = 16$.

Fact (Sphere packing bound)

$$A_q(n,d) \leq q^n \Big/ \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} \cdot (q-1)^i .$$



$$A(n,d) \leq 2^n \Big/ \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{\lfloor \frac{d-1}{2} \rfloor} .$$

Example $A(7,3) \leq 2^7 \Big/ \binom{7}{0} + \binom{7}{1} = 2^4$.

$A(7,3) \geq 16$

16 codewords

0000000	1111111
1011000	0100111
0101100	1010011
0010110	1101001
0001011	1110100
1000101	0111010
1100010	0011101
0110001	1001110