Notes on Sree's paper

Ziquan Yang

May 30, 2014

Theorem 0.1. *Consider a binary linear code C of length $n = 2^m - 1$, distance $d = 6$, and locality $r = 2$. Suppose $m \geq 2$ is even. Suppose $[n]$ can be divided into $n/3$ groups $\{g_i\}$ and the dual code has a codeword of Hamming weight 3 supported by the coordinates in each g_i. Then we have*

$$k \leq \frac{2}{3}(2^m - 1) - m$$

Proof. Suppose $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in C$. Let $\mathbf{c}_i$ denote the parity check supported by g_i. Then since $\mathbf{x} \cdot \mathbf{c}_i = 0$, we see that the projection of $\mathbf{x}$ onto g_i could only be one of $\{000, 011, 101, 110\}$. Call this projection map p_i and identify the set $\{000, 011, 101, 110\}$ with the $\mathbb{F}_4$ we can identify $\mathbf{x}$ with $\mathbb{F}_4^{(2^m-1)/3}$ by:

$$\varphi : x \mapsto (p_1(\mathbf{x}), p_2(\mathbf{x}), \cdots, p_{(2^m-1)/3}(\mathbf{x}))$$

. Denote the weight of $\mathbf{x}$ by $wt(\mathbf{x})$. Since we see that $\mathbf{x}$ intersects with g_i at at most two points, exactly $\frac{wt(\mathbf{x})}{2}$ $p_i(\mathbf{x}) \neq 0$. This shows that

$$wt(\varphi(\mathbf{x})) = \frac{wt(\mathbf{x})}{2}$$

. Thus we see that the image of C in $\mathbb{F}_4^{(2^m-1)/3}$ has minimum distance 3. We only need to show that the dimension for its image k' is bounded by

$$k' \leq \frac{2^m - 1}{3} - \frac{m}{2}$$

To prove the above inequality, we show that there exists a set of coordinates T, $|T| = m/2$, such that $\dim C = \dim C^T$, where C^T denotes the punctured code. Thus by singleton bound, we see that

$$\dim C = \dim C^T \leq \frac{2^m - 1}{3} - \frac{m}{2}$$

It suffices to find a set T such that the canonical projection map $\pi : C \mapsto C^T$ has trivial kernel. We can construct this set inductively. Since $d' \geq 3$, we can take any set T_2, where $|T_2| = 2$, and we see that the corresponding $\ker \pi_2 = 0$. Now we show that given a set T_u, $|T_u| = u, \ker \pi_u = 0$, where $4^u < n' - u$, there exists coordinate i_{u+1} such that the union $T_{u+1} = T_u \cup \{i_{u+1}\}$ satisfies $\ker \pi_{u+1} = 0$.
Consider the collection of all possible $T = T_u \cup \{j\}$, where $j \in [n'] - T_u$. Suppose for each T, we have the coresponding $\ker \pi_T \neq 0$, then for each T we can pick a non-zero vector $\mathbf{x}_T \in \ker \pi_T$. Note that by assumption we have

$$\#\{\pi_u(\mathbf{x}_T)\} = n' - u > 4^u \geq |\mathrm{Im}\pi_u|$$

there exists T and T' such that $\pi_u(\mathbf{x}_T) = \pi_u(\mathbf{x}_{T'})$. Note that we have $wt(\mathbf{x}_T - \mathbf{x}_{T'}) \leq 2$, contradicting with $d' = 3$. Thus there must exist a T, such that $\ker T = 0$. Then we can let the corresponding $j = i_{u+1}$ and $T = T_{u+1}$. The maximum possible u is $m/2 - 1$, so we can construct T_{u+1} up to $u = m/2 - 1$ and the required T is found. $\square$

Theorem 0.2. *Consider a binary linear code C of length $n = 2^m - 1$, distance $d \geq 10$, and locality $r = 2$. Suppose $m \geq 2$ is even. Suppose $[n]$ can be divided into $n/3$ groups $\{g_i\}$ and the dual code has a codeword of Hamming weight 3 supported by the coordinates in each g_i. Then we have*

$$k \leq \frac{2}{3}(2^m - 1) - 2m + 1$$

, and if k is even, then

$$k \leq \frac{2}{3}(2^m - 1) - 2m$$

.

Proof. This is easily done by sphere packing. Again we map C to $\mathbb{F}_2^{n'}$, where $n' = n/3$. $d' \geq 5$ this time, so balls centered at codewords of radius 2 do not intersect with each other, thus we have

$$4^{n'} \geq |C|(1 + 3n' + \frac{9n'(n'-1)}{2})$$

Take $\log_2$ on both sides, we have

$$k \leq \frac{2n}{3} + 1 - 2m$$

for any even $m > 2$. $\square$

Theorem 0.3. *Consider a binary linear code C of length $n = 2^m - 1$, distance $d = 6$, and locality $r = 2$. If $2 \mid m$ and $m > 8$, then the upper bound on the dimenstion of C:*

$$k \leq \frac{2}{3}(2^m - 1) - m$$

continues to hold.

Proof. Let $Q = \{\mathbf{q}_1, \mathbf{q}_2, \cdots, \mathbf{q}_b\}$ be a set of linearly independent parity checks of weight 3 that cover $[n]$. Assume that Q is the minimal set that satifies the condition. Suppose

$$b = \frac{1}{3}(2^m - 1) + t$$

where $0 \leq t \leq m$. $t \geq 0$ since at least $(2^m - 1)/3$ parity checks of weight 3 are needed to cover $[n]$, and when $t \geq (m+1)$ the conclusion follows directly from

$$k \leq n - b \leq \frac{2}{3}(2^m - 1) - m - 1 < \frac{2}{3}(2^m - 1) - m$$

Let P_m be the maximal set of pairwise disjoint parity checks of weight 3 in Q. Let $|P_m| = N$. Reorder Q if needed, we suppose $P_m = \{\mathbf{q}_1, \mathbf{q}_2, \cdots, \mathbf{q}_N\}$. For each $\mathbf{q}_k \notin P_m$, if

$$\operatorname{supp}(\mathbf{q}_k) \cap \bigcup_{i=1}^{N} \operatorname{supp}(\mathbf{q}_i) = \varnothing$$

then $P_m \bigcup \{\mathbf{q}_k\}$ is also pairwise disjoint, contradicting with the maximality of P_m, i.e. each $\mathbf{q}_k \notin P_m$ covers at most 2 more coordinates not in $\bigcup_{i=1}^{N} \operatorname{supp}(\mathbf{q}_i)$. By inclusion-exclusion principle we have

$$3N - 2(b - N) \geq n$$

thus

$$N \geq \frac{2^m - 1}{3} - 2m$$

On the other hand, if

$$\text{supp}(\mathbf{q}_k) \subset \bigcup_{i=1}^{N} \text{supp}(\mathbf{q}_i)$$

then we can remove $\mathbf{q}_k$ from Q the the rest still covers $[n]$, contradicting with the minimality of Q. Thus each $\mathbf{q}_k \notin P_m$ intersects with at most 2 parity checks in P_m. Hence at most $6m$ parity checks in P_m have an non-empty intersection with some parity checks in $Q - P_m$, the remaining N^* parity checks in P_m intersect with neither other parity checks in P_m nor any parity checks in $Q - P_m$ and we have

$$N^* \geq \frac{2^m - 1}{3} - 8m$$

$N^* > 0$ when $m > 8$. Reorder P_m if needed, then we can assume $\text{supp}(\mathbf{q}_i) \cap \text{supp}(\mathbf{q}_j) = \varnothing$ for $1 \leq i \leq N^*, N^* + 1 \leq j \leq b$. Now let

$$C_N = \{\mathbf{x} \in \mathbb{F}_2^n \mid \text{supp}(\mathbf{x}) \subset \bigcup_{i=1}^{N^*} \text{supp}(\mathbf{q}_i), \mathbf{x} \cdot \mathbf{q}_i = 0, 1 \leq i \leq N^*\}$$

Cleary $\mathbf{x} \cdot \mathbf{q}_i = 0$ if and only if its $|\text{supp}(\mathbf{x}) \cap \text{supp}(\mathbf{q}_i)| = 2$ for $\mathbf{x} \neq 0$. Moreover, if $\mathbf{x} \in C_N$ and $wt(\mathbf{x}) = 2$, then $\mathbf{x} \cdot \mathbf{q}_i = 0$ for each $1 \leq i \leq b$ if and only if $\text{supp}(\mathbf{x}) \subset \text{supp}(\mathbf{q}_k)$ for some $1 \leq k \leq N^*$. Similarly if instead $wt(\mathbf{x}) = 4$, then it must be the sum of two codewords in C_N of weight 2. In order to exclude those $\mathbf{x}$ with weight 2 or 4, we need to add more parity checks. Let M be the minimal matrix formed by such parity checks. We need for $\mathbf{c}_1 \neq \mathbf{c}_2$ to have $\mathbf{c}_1 + \ker M \neq \mathbf{c}_2 + \ker M$. Thus we must have

$$2^{b'} = |\text{Im} M| = |M / \ker M| \geq 1 + 3N^* \geq 2^m - 24m$$

. This gives $b' \geq m$, thus we conclude that

$$n - k \geq b + b' \geq \frac{2^m - 1}{3} + m$$

□

My Improvement

The above theorem shows that the assumption on disjoint locality parity checks leads to no loss in optimality in Theorem 0.1. Actually, Theorem 0.2 can be generalized in a similar manner. In the above proof again we consider vectors of even weight in C_N. To enforce the minimum distance of 10, we need to impose parity checks to rule out vectors in C_N with weight 2, 4, 6, 8. We have seen that each vector in C_N with weight 4 is the sum of two vectors with weight 2. Furthermore, we observe that given two vectors $\mathbf{x}_1$, $\mathbf{x}_2$ of weight 4, we have

$$wt(\mathbf{x}_1 + \mathbf{x}_2) = |\text{supp}(\mathbf{x}_1 + \mathbf{x}_2)| = \begin{cases} 2, & \text{if } |\text{supp}(\mathbf{x}_1) \cap \text{supp}(\mathbf{x}_2)| = 3 \\ 4, & \text{if } |\text{supp}(\mathbf{x}_1) \cap \text{supp}(\mathbf{x}_2)| = 2 \\ 6, & \text{if } |\text{supp}(\mathbf{x}_1) \cap \text{supp}(\mathbf{x}_2)| = 1 \\ 8, & \text{if } |\text{supp}(\mathbf{x}_1) \cap \text{supp}(\mathbf{x}_2)| = 0 \end{cases}$$

The converse is also clearly true: each vector $\mathbf{x} \in C_N$ of weight 2, 4, 6, or 8 can be written as the sum of some $\mathbf{x}_1$ and $\mathbf{x}_2$, both of weight 4. Thus we have

$$M\mathbf{x} \neq 0 \Leftrightarrow \mathbf{x}_i + \ker M \neq \mathbf{x}_j + \ker M, \text{ for all } \mathbf{x}_i \text{ and } \mathbf{x}_j \text{ of weigth 4}$$

A unique vector of weight 4 is constructed by selecting two vectors of weight 2. Thus we have

$$2^{b'} \geq \binom{3N^*}{2}$$

which requires $b' \geq 2m - 1$ when $m \geq 10$.