A Generalization of Sree's Result

Ziquan Yang

June 26, 2015

Theorem 0.1. *Consider a linear code $\mathcal{C}$ over $\mathbb{F}_5$ of length $n = 5^m - 1$, distance $d \geq 6$, and locality $r = 2$. Let m be an even number greater than 2. Suppose the set of coordinates $[n]$ can be divided into $n/3$ groups, $\{g_i\}_{i=1}^{n/3}$, such that the repair of a given coordinate only requires the bits stored in the coordinates in its corresponding group. This implies that the dual code has a codeword (parity-check) of Hamming weight $r + 1 = 3$ supported by the coordinates in each group g_i. Then,*

$$k \leq \frac{2}{3}(5^m - 1) - m - 1$$

where $k = \dim \mathcal{C}$.

Proof. Let $\mathbf{x} = (x_1, \cdots, x_n)$ be a codeword and $g_i = \{i, i+1, i+2\}$. For each g_i, we may find a vector $\mathbf{q}_i \in \mathcal{C}^\perp$, such that $\mathrm{wt}(\mathbf{q}_i) = 3$ and $\mathrm{supp}(\mathbf{q}_i) = g_i$. These $\mathbf{q}_i$'s are clearly linear independent. Let $Q = \{\mathbf{q}_i\}_{i=1}^{n/3}$. Let L_q be the linear transformation corresponding to the matrix $M_q = [\mathbf{q}_1; \mathbf{q}_2; \cdots; \mathbf{q}_{n/3}]$ (Matlab notation: $\mathbf{q}_i$'s are row vectors of the matrix). In other words, L_q records the images of $\mathbb{F}_5^n$ under the projection to each of the g_i's. We have that $\mathcal{C} \subseteq M_q^\perp$.

Our plan is to add more parity checks to push up the minimum distance. We want to give a lower bound on the codimension for a subspace of $M_q^\perp$ that has $d \geq 6$. If such a $\mathcal{C}$ is found, then we notice that its translates at $v_1, v_2 \in M_q^\perp, \mathrm{wt}(v_1), \mathrm{wt}(v_2) \leq 2$ are disjoint, i.e. $(v_1 + \mathcal{C}) \cap (v_2 + \mathcal{C}) = \emptyset$ since otherwise $v_1 - v_2 \in \mathcal{C}$ despite $\mathrm{wt}(v_1 - v_2) \leq 4$. A vector in $M_q^\perp$ must be supported in some g_i, and conversely each g_i produces exactly 12 vectors of weight 2. Therefore

$$(12 \times \frac{1}{3}(5^m - 1) + 1) \cdot |C| \leq |M_q|$$

and hence

$$\mathrm{codim}_{M_q^\perp} \mathcal{C} \geq \lceil \log_5(4(5^m - 1) + 1) \rceil = m + 1$$

□

The wonderful thing is, we may prove that the bound can almost be met by showing there exists such a subspace $\mathcal{C} \subseteq M_q^\perp$ of codimension $m + 2$. In fact, the $\mathcal{C}$ whose existence we show satisfies a stronger condition: it does not contain codewords of weight 6 that can be written as the sums of two vectors in $M_q^\perp$ of weight 3. To find such a subspace $\mathcal{C}$ is the same as to find a linear transformation $L : M_q^\perp \to \mathbb{F}_5^{m+2}$ such that L is injective on $S := \{v \in M_q^\perp : \mathrm{wt}(v) \leq 3\}$. The correspondence is $\mathcal{C} = \ker L$, of course. Clearly S generates $M_q^\perp$ as a vector space. We may first define L on S and then extend by linearity, so long as our L is compatible with the linear dependence relations inside S. To be precise, if for each $s_j \in S$, we can choose $w_j \in \mathbb{F}_5^{2m+2}$ such that whenever $\sum a_j s_j = 0$, $\sum a_j w_j = 0$, then we may define L by setting $L(s_j) = w_j$. Let $S_i = \{v \in S : \mathrm{supp}(v) \subseteq g_i\}$. We see that to respect the linear dependence relations in S is the same as to respect those in each

S_i. There certainly exists a map $\varphi : S_i \hookrightarrow \mathbb{F}_5^2$ that can extend linearly to all $\mathbb{F}_5^3$. In fact, S_i is nothing but $\langle \mathbf{q}_i \rangle^\perp - \{0\} \subseteq \mathbb{F}_5^3$ (we are abusing notation a bit and looking at $\mathbf{q}_i$ in its support). If there exist $(5^m - 1)/3$ maps $L_i : \mathbb{F}_5^2 \hookrightarrow \mathbb{F}_5^{m+2}$ whose images are disjoint from each other except at the origin, then writing a vector in $M_q^\perp$ as $(\mathbf{v}_1, \cdots, \mathbf{v}_{n/3})$ we may define the map $L : M_q^\perp \to \mathbb{F}_5^{m+2}$ by

$$(\mathbf{v}_1, \cdots, \mathbf{v}_{n/3}) \mapsto \sum_{i=1}^{n/3} L_i(\varphi(\mathbf{v}_i))$$

We are left to show that $\mathbb{F}_5^{m+2}$ is large enough to accomodate that many L_i's. The proof is completed by the following lemma:

Lemma 0.2. *For each $\mathbb{F}_5^m$, $m \geq 2$ is even, there exists a collection $\mathcal{A}$ of injections $L_i : \mathbb{F}_5^2 \to \mathbb{F}_5^m$ such that $\mathrm{Im}L_i \cap \mathrm{Im}L_j = \{0\}$ for every $i \neq j$ and $|\mathcal{A}| \geq 5^{m-2}$.*

Proof. We proceed by induction. The conclusion is trivial for $m = 2$. Now suppose it has been shown for m. For each $L \in \mathcal{A}_m$ and define 25 maps $L_i : \mathbb{F}^2 \hookrightarrow \mathbb{F}^{m+2}$ such that we may take $\mathcal{A}_{m+2} = \{L_i : L \in \mathcal{A}_m, 1 \leq i \leq 25\}$. Label vector in $\mathbb{F}_5^2 - \{0\}$ by $v_1, \cdots, v_{24}$ and suppose $\{v_1, v_2\}$ is a basis. Let D be an automorphism of $\mathbb{F}_5^n$ that has no eigenvectors, e.g.

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

This matrix works since its characteristic polynomial $x^2 + 2 = 0$ has no roots over $\mathbb{F}_5$. Now for each v_i we define a linear map $A_i : \mathbb{F}_5^2 \to \mathbb{F}_5^2$ by sending $[1, 0] \mapsto v_i, [0, 1] \mapsto D(v_i)$. A_i is an automorphism since $D(v_i)$ and v_i are linearly independent. Now we may define $L_i = L \oplus A_i$ for $1 \leq i \leq 24$ and $L_{25} = L \oplus [0]_{2\times 2}$.

Now let us check that it works: Let $p_{\leq m} : \mathbb{F}_5^{m+2} \to \mathbb{F}_5^m$, $p_{>m} : \mathbb{F}_5^{m+2} \to \mathbb{F}_5^2$ be projections to the first $\leq m$ and last two coordinates respectively. Given a vector $w \neq 0 \in \mathbb{F}_5^{m+2}$, $p_{\leq m}(w)$ lies in the image of at most one $L \in \mathcal{A}_m$, by induction hypothesis. Now suppose w is indeed hit by some L and $p_{\leq m}(w) \neq 0$. We write $w = (L(v_\alpha), v_\beta)$ and $v_\alpha = (\alpha_1, \alpha_2) \in \mathbb{F}_5^2$. If $v_\beta = 0$, then $w \in L_{25}$. Otherwise, if $w \in \mathrm{Im}L_i$, then we must have $v_\beta = \alpha_1 v_i + \alpha_2 D(v_i)$ for some i. Such an i is unique: Suppose there is j, such that

$$v_\beta = \alpha_1 v_i + \alpha_2 D(v_i) = \alpha_1 v_j + \alpha_2 D(v_j)$$

i.e.

$$\alpha_1(v_i - v_j) + \alpha_2 D(v_i - v_j) = 0$$

. α_1, α_2 cannot both be zero. If $\alpha_2 = 0$ then $\alpha_1 \neq 0 \Rightarrow v_i = v_j$. The same applies to the $\alpha_1 = 0$ case. If $\alpha_1\alpha_2 \neq 0$, and $v_i \neq v_j$, then $v_i - v_j$ will be an eigenvector of D, a case which we have precluded. In any case $v_i = v_j$. □

Remark 0.3. The arguments should generalize to larger primes as well. Moreover, if we replace $\mathbb{F}_5$ by $\mathbb{F}_p$, $p \geq 7$, then numerically we can prove $\mathrm{codim}_{M_q^\perp} \mathcal{C} \geq m + 2$. Then lemma should still work and in fact we produce codes that meet the bound exactly.