TWO-STEP MAJORITY-LOGIC DECODING

Roman Shor, Eitan Yaakobi

I. Introduction

In this work we describe decoding of Two-Step Majority-Logic codes as defined in [1] and provide a lower bound on redundancy of such codes.

II. Defenitions

Definition 1: Let $E = \{e_{i_1}, e_{i_2}, \ldots, e_{i_M}\}$ be a set of M error digits, where $0 \leq i_1 < i_2 < \cdots < i_M < n$.

A set of J parity-check sums $A_1, A_2, \ldots, A_J$ is said to be orthogonal on the set $E \iff$

1) Every error digit e_{i_ℓ}in E is checked by every check-sum A_j for $1 \leq j \leq J$.
2) No other error digit is checked by more than one check-sum.

For example, the following four parity-check sums are orthogonal on the set $E = \{e_6, e_8\}$:

$$\begin{aligned} A_1 &= e_0 + e_2 + e_6 + e_8, \\ A_2 &= e_3 + e_4 + e_6 + e_8, \\ A_3 &= e_1 + e_6 + e_7 + e_8, \\ A_4 &= e_5 + e_6 + e_8. \end{aligned}$$

By same argument as in one-step majority-logic in case of $\lfloor \frac{J}{2} \rfloor$ or fewer errors, we can correctly determine the sum of error digits in E.

General

Consider an (n, k) cyclic code C that is used for error control in a communication (or storage) system. Let $\mathbf{e} = (e_0, e_1, \ldots, e_{n-1})$ denote the error vector that occurs during the transmission of a codeword $\mathbf{v} \in C$. Let $E_1^1, E_2^1, \ldots, E_j^1, \ldots$ be some properly selected sets of error digits of size 2, each containing e_{n-1}.

Let $S\left(E_j^1\right)$ denote the modulo-2 sum of the error digits in E_j^1. Suppose that for each set E_j^i it is possible to form at least J parity-check sums orthogonal on it. Then , the sum $S\left(E_j^1\right)$ can be estimated from these J orthogonal check-sums. The estimated value of $S\left(E_j^1\right)$ is 1 if more than half of the parity-check sums are 1 and 0 otherwise. The estimation is correct provided there are no more than $\lfloor \frac{J}{2} \rfloor$ errors in $\mathbf{e}$. From the sums $S\left(E_1^1\right), S\left(E_2^1\right), \ldots, S\left(E_j^1\right), \ldots$ (possibly together with other check-sums) we get J or more check-sums orthogonal on e_{n-1}.

Decoding

Suppose that $\mathcal{C}$ is a two-step majority-logic linear cyclic code correcting $\lfloor \frac{J}{2} \rfloor$ errors. $\mathcal{C}$ is of length n, over a field F , and say $\mathcal{C}$ has dimension $n - d$.

Let $E_1, E_2, \ldots, E_M$ be some properly selected sets of error digits of size 2, each containing e_{n-1}, $M < J$. For each set E_j it is possible to form at least J parity-check sums orthogonal on it.

Also there are $J - M$ parity-check sums orthogonal e_{n-1}(also orthogonal to the sets $E_1, E_2, \ldots, E_M$).

Let $r = (r_0, r_1, \ldots, r_{n-1})$ be the received vector.

1) First step of the decoding will be to estimate $S(E_j)$ for each $j \in [0, M]$.
   a) Let $h_0^j, h_1^j, \ldots, h_{J-1}^j \in \mathcal{C}^\perp$ be the dual code code words representing the J parity-check sums for E_j.
   b) We compute the parity-check sums as follows
   $$A_0^j = r \cdot h_0^j$$
   $$A_1^j = r \cdot h_1^j$$
   $$\vdots$$
   $$A_{J-1}^j = r \cdot h_{J-1}^j$$
   c) If more then half of the parity-check sums result in 1, than if $|e| \leq \lfloor \frac{J}{2} \rfloor$ (e being the error vector) there is an error in one of the two symbols of the set E_j.
   d) $S(E_j)$ gets the value of 1 if more then half of the parity-check sums result in 1.
2) Second step will be to compute the $J - M$ parity-check sums orthogonal on e_{n-1}.
   a) Let $h_0, h_1, \ldots, h_{J-M-1} \in \mathcal{C}^\perp$ be the dual code code words representing the $J - M$ parity-check sums orthogonal on e_{n-1}.
   b) As before, we compute the parity-check sums as follows
   $$A_0 = r \cdot h_0$$
   $$\vdots$$
   $$A_{J-M-1} = r \cdot h_{J-M-1}$$
   c) Now if more then half of the parity-check sums and the orthogonal sets estimates $S(E_j)$ result in 1, than if $|e| \leq \lfloor \frac{J}{2} \rfloor$ there is an error in e_{n-1}.
   d) e_{n-1}gets the value of 1 if more then half of the parity-check sums and the orthogonal sets estimates $S(E_j)$ result in 1.

3) After that we can cyclically shift r and compute the value of e_{n-2} using $r' = (r_{n-1}, r_0, r_1, \ldots, r_{n-2})$ in same fashion as before.
4) We continue doing that until we complete full cycle of r, and get the value of the error vector e.

Example 1

Consider the $(7,4)$ cyclic code generated by $g(X) = 1 + X + X^3$. This is a Hamming code. The parity-check matrix (in systematic form) is found as follows:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h_0} \\ \mathbf{h_1} \\ \mathbf{h_2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

We see that the vectors $\mathbf{h_0}$ and $\mathbf{h_2}$ are orthogonal on digit position 5 and 6 (or $X^5$and X^6). We also see that the vectors $\mathbf{h_0} + \mathbf{h_1}$ and $\mathbf{h_2}$ are orthogonal on positions 4 and 6. Let $E_1^1 = \{e_5, e_6\}$ and $E_1^1 = \{e_4, e_6\}$ be two selected sets. Let $r = (r_0, r_1, r_2, r_3, r_4, r_5, r_6)$ be the received vector. Then, the parity-check sums formed from $\mathbf{h_0}$ and $\mathbf{h_2}$ are

$$A_1 = r \cdot \mathbf{h_0} = e_0 + e_3 + e_5 + e_6$$

$$A_2 = r \cdot \mathbf{h_2} = e_2 + e_4 + e_5 + e_6$$

and the parity-check sums formed from $\mathbf{h_0} + \mathbf{h_1}$ and $\mathbf{h_2}$ are

$$B_1 = r \cdot (\mathbf{h_0} + \mathbf{h_1}) = e_0 + e_1 + e_4 + e_6$$

$$B_2 = r \cdot \mathbf{h_2} = e_2 + e_4 + e_5 + e_6$$

The parity-check sums A_1 and A_2 are orthogonal on the set $E_1^1 = \{e_5, e_6\}$, and the parity-check sums B_1 and B_2 are orthogonal on the set $E_2^1 = \{e_4, e_6\}$. Therefore, the sum $S\left(E_1^1\right) = e_5 + e_6$ can be estimated from A_1 and A_2, and the sum $S\left(E_2^1\right) = e_4 + e_6$ can be estimated from $B_1$and B_2. The sums $S\left(E_1^1\right)$ and $S\left(E_2^1\right)$ will be correctly estimated provided there is no more than one error in the error vector $\mathbf{e}$. Now, let $E_1^2 = \{e_6\}$. We see that $S\left(E_1^1\right)$ and $S\left(E_2^1\right)$ are orthogonal on e_6. Hence, e_6 can be estimated from $S\left(E_1^1\right)$ and $S\left(E_2^1\right)$. The value of e_6 will be estimated correctly provided that there is no more than one error in $\mathbf{e}$. Therefore, the $(7,4)$ Hamming code can be decoded with two steps of orthogonalization, and it is two-step majority-logic decodable. Because its minimum distance is 3 and $J = 2$, it is two-step completely orthogonalizable.

Let $\mathbf{s} = (s_0, s_1, s_2) = \mathbf{r} \cdot \mathbf{H}^T$ be the syndrome of the received vector $\mathbf{r}$. Then, we can form the parity-check sums A_1, A_2, B_1, and B_2 from the syndrome digits as follows:

$$A_1 = s_0,\ A_2 = s_2,\ B_1 = s_0 + s_1,\ B_2 = s_2.$$

Example 2

Consider the triple-error-correcting $(15,5)$ BCH code whose generator polynomial is

$$g(X) = 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}$$

The parity-check matrix (in systematic form) is $\mathbf{H} =$

$$= \begin{bmatrix} \mathbf{h_0} \\ \mathbf{h_1} \\ \mathbf{h_2} \\ \mathbf{h_3} \\ \mathbf{h_4} \\ \mathbf{h_5} \\ \mathbf{h_6} \\ \mathbf{h_7} \\ \mathbf{h_8} \\ \mathbf{h_9} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Let

$$E_1^1 = \{e_{13}, e_{14}\},\ E_2^1 = \{e_{12}, e_{14}\},\ E_3^1 = \{e_{11}, e_{14}\},$$

$$E_4^1 = \{e_{10}, e_{14}\},\ E_5^1 = \{e_5, e_{14}\},\ E_6^1 = \{e_2, e_{14}\}$$

be six selected sets of error digits. For each of the preceding sets it is possible to find six parity-check sums orthogonal on it. Let $\mathbf{r} = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9, r_{10}, r_{11}, r_{12}, r_{13}, r_{14})$ be the received vector. By taking proper combinations of the rows $\mathbf{H}$, we find the following parity-check sums orthogonal on $E_1^1, E_2^1, E_3^1, E_4^1, E_5^1, E_6^1$:

1) Check-sums orthogonal on $E_1^1 = \{e_{13}, e_{14}\}$:

$$A_{11} = \mathbf{r} \cdot \mathbf{h_4} = e_4 + e_{10} + e_{13} + e_{14}$$

$$A_{12} = \mathbf{r} \cdot \mathbf{h_7} = e_7 + e_{12} + e_{13} + e_{14}$$

$$A_{13} = \mathbf{r} \cdot \mathbf{h_9} = e_9 + e_{11} + e_{13} + e_{14}$$

$$A_{14} = \mathbf{r} \cdot (\mathbf{h_0} + \mathbf{h_8}) = e_0 + e_8 + e_{13} + e_{14}$$

$$A_{15} = \mathbf{r} \cdot (\mathbf{h_1} + \mathbf{h_5}) = e_1 + e_5 + e_{13} + e_{14}$$

$$A_{16} = \mathbf{r} \cdot (\mathbf{h_3} + \mathbf{h_6}) = e_3 + e_6 + e_{13} + e_{14}$$

2) Check-sums orthogonal on $E_2^1 = \{e_{12}, e_{14}\}$:

$$A_{21} = \mathbf{r} \cdot \mathbf{h_0} = e_0 + e_{10} + e_{12} + e_{14}$$

$$A_{22} = \mathbf{r} \cdot \mathbf{h_3} = e_3 + e_{11} + e_{12} + e_{14}$$

$$A_{23} = \mathbf{r} \cdot \mathbf{h_7} = e_7 + e_{13} + e_{12} + e_{14}$$

$$A_{24} = \mathbf{r} \cdot (\mathbf{h_1} + \mathbf{h_2}) = e_1 + e_2 + e_{12} + e_{14}$$

$$A_{25} = \mathbf{r} \cdot (\mathbf{h_4} + \mathbf{h_8}) = e_4 + e_8 + e_{12} + e_{14}$$

$$A_{26} = \mathbf{r} \cdot (\mathbf{h_6} + \mathbf{h_9}) = e_6 + e_9 + e_{12} + e_{14}$$

3) Check-sums orthogonal on $E_3^1 = \{e_{11}, e_{14}\}$:

$$A_{31} = \mathbf{r} \cdot \mathbf{h_3} = e_3 + e_{12} + e_{11} + e_{14}$$

$$A_{32} = \mathbf{r} \cdot \mathbf{h_9} = e_9 + e_{13} + e_{11} + e_{14}$$

$$A_{33} = \mathbf{r} \cdot (\mathbf{h_0} + \mathbf{h_5}) = e_0 + e_5 + e_{11} + e_{14}$$

$$A_{34} = \mathbf{r} \cdot (\mathbf{h_1} + \mathbf{h_8}) = e_1 + e_8 + e_{11} + e_{14}$$

$$A_{35} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_4}) = e_2 + e_4 + e_{11} + e_{14}$$

$$A_{36} = \mathbf{r} \cdot (\mathbf{h_6} + \mathbf{h_7}) = e_6 + e_7 + e_{11} + e_{14}$$

4) Check-sums orthogonal on $E_4^1 = \{e_{10}, e_{14}\}$:

$$A_{41} = \mathbf{r} \cdot \mathbf{h_0} = e_0 + e_{12} + e_{10} + e_{14}$$

$$A_{42} = \mathbf{r} \cdot \mathbf{h_4} = e_4 + e_{13} + e_{10} + e_{14}$$

$$A_{43} = \mathbf{r} \cdot (\mathbf{h_1} + \mathbf{h_6}) = e_1 + e_6 + e_{10} + e_{14}$$

$$A_{44} = \mathbf{r} \cdot (\mathbf{h_3} + \mathbf{h_5}) = e_3 + e_5 + e_{10} + e_{14}$$

$$A_{45} = \mathbf{r} \cdot (\mathbf{h_7} + \mathbf{h_8}) = e_7 + e_8 + e_{10} + e_{14}$$

$$A_{46} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_9}) = e_2 + e_9 + e_{10} + e_{14}$$

5) Check-sums orthogonal on $E_5^1 = \{e_5, e_{14}\}$:

$$A_{51} = \mathbf{r} \cdot (\mathbf{h_0} + \mathbf{h_5}) = e_0 + e_{11} + e_5 + e_{14}$$

$$A_{52} = \mathbf{r} \cdot (\mathbf{h_1} + \mathbf{h_5}) = e_1 + e_{13} + e_5 + e_{14}$$

$$A_{53} = \mathbf{r} \cdot (\mathbf{h_3} + \mathbf{h_5}) = e_3 + e_{10} + e_5 + e_{14}$$

$$A_{54} = \mathbf{r} \cdot (\mathbf{h_4} + \mathbf{h_5} + \mathbf{h_6}) = e_4 + e_6 + e_5 + e_{14}$$

$$A_{55} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_5} + \mathbf{h_7}) = e_2 + e_7 + e_5 + e_{14}$$

$$A_{56} = \mathbf{r} \cdot (\mathbf{h_5} + \mathbf{h_8} + \mathbf{h_9}) = e_8 + e_9 + e_5 + e_{14}$$

6) Check-sums orthogonal on $E_6^1 = \{e_2, e_{14}\}$:

$$A_{61} = \mathbf{r} \cdot (\mathbf{h_1} + \mathbf{h_2}) = e_1 + e_{12} + e_2 + e_{14}$$

$$A_{62} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_4}) = e_4 + e_{11} + e_2 + e_{14}$$

$$A_{63} = \mathbf{r} \cdot (\mathbf{h_0} + \mathbf{h_2} + \mathbf{h_6}) = e_0 + e_2 + e_2 + e_{14}$$

$$A_{64} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_3} + \mathbf{h_8}) = e_3 + e_8 + e_2 + e_{14}$$

$$A_{65} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_5} + \mathbf{h_7}) = e_5 + e_7 + e_2 + e_{14}$$

$$A_{66} = \mathbf{r} \cdot (\mathbf{h_2} + \mathbf{h_9}) = e_9 + e_{10} + e_2 + e_{14}$$

From the foregoing orthogonal check-sums, the sums $S\left(E_1^1\right) = e_{13} + e_{14}$, $S\left(E_2^1\right) = e_{12} + e_{14}$, $S\left(E_3^1\right) = e_{11} + e_{14}$, $S\left(E_4^1\right) = e_{10} + e_{14}$, $S\left(E_5^1\right) = e_5 + e_{14}$, $S\left(E_6^1\right) = e_2 + e_{14}$ can be estimated provided that there are no more than three errors in the error vector $\mathbf{e}$. Let $E_1^2 = \{e_{14}\}$. We see that the error sums $S\left(E_1^1\right), S\left(E_2^1\right), S\left(E_3^1\right), S\left(E_4^1\right), S\left(E_5^1\right), S\left(E_6^1\right)$ are orthogonal on e_{14}. Hence, e_{14}can be estimated from these sums. Therefore, the $(15, 5)$ BCH code is two-step orthogonalizable. Because $J = 6$, it is capable of correcting three or fewer errors with two-step majority-logic decoding. It is known that the code has a minimum distance of exactly 7. Hence, it is two-step completely orthogonalizable.

III. Redundancy of two-step majority-logic codes correcting one error

Suppose that $\mathcal{C}$ is a two-step majority-logic linear cyclic code, correcting one error. C is of length n, over a field F , and say $\mathcal{C}$ has dimension $n - d$. Thus there are two options available:

1) The symbol e_{n-1} there exist two groups $E_1 = \{e_i, e_{n-1}\}$, $E_2 = \{e_j, e_{n-1}\}$, $i \neq j$, $0 \leq j, k < n-1$ and each group has two parity-check sums orthogonal on it.
Consider the parity checks $a_1, b_1, a_2, b_2 \in F^n$, so that a_1 and b_1 are nonzero vectors orthogonal on the E_1 , and that a_2 and b_2 are nonzero vectors orthogonal on E_2.
Now, these vectors are code words of the $\mathcal{C}^\perp$ and let $w_1, \ldots, w_n \in F^d$ be the columns of the generator matrix of $\mathcal{C}^\perp$.
Thus we can write $a_1 = (\langle v, w_1\rangle, \langle v, w_2\rangle, ..., \langle v, w_n\rangle)$,$b_1 = (\langle u, w_1\rangle, \langle u, w_2\rangle, ..., \langle u, w_n\rangle)$ and similarly $a_2 = (\langle s, w_1\rangle, \langle s, w_2\rangle, ..., \langle s, w_n\rangle)$, $b_2 = (\langle t, w_1\rangle, \langle t, w_2\rangle, ..., \langle t, w_n\rangle)$ for $v, u, s, t \in F^d$, and where $\langle, \rangle$ means inner product.
Now consider the polynomials $p_{n-1}(X) = \langle v, X\rangle \times \langle u, X\rangle \times \langle s, X\rangle \times \langle t, X\rangle$, where X is the vector $(X_1, ..., X_d)$, $p_{n-1}(w_j) = \begin{cases} 1 & \text{if } j = n-1 \\ 0 & \text{otherwise} \end{cases}$.
Since $\mathcal{C}$ is cyclically shift groups E_1, E_2 and get $E_1' = \left\{e_{(i-1) \mod n}, e_{n-2}\right\}$, $E_2' = \left\{e_{(j-1) \mod n}, e_{n-1}\right\}$.
By the same shift on a_1, b_1, a_2, b_2, we get $a_1', b_1', a_2', b_2' \in \mathcal{C}^\perp$ so that a_1' and b_1' are nonzero vectors orthogonal on the E_1' , and that a_2' and b_2' are nonzero vectors orthogonal on E_2'.
Similarly we can write $a_1' = (\langle v', w_1\rangle, \langle v', w_2\rangle, ..., \langle v', w_n\rangle)$,$b_1' = (\langle u', w_1\rangle, \langle u', w_2\rangle, ..., \langle u', w_n\rangle)$ and similarly $a_2' = (\langle s', w_1\rangle, \langle s', w_2\rangle, ..., \langle s', w_n\rangle)$, $b_2' = (\langle t', w_1\rangle, \langle t', w_2\rangle, ..., \langle t', w_n\rangle)$ for $v', u', s', t' \in F^d$.
Now consider the polynomials $p_{n-2}(X) = \langle v', X\rangle \times \langle u', X\rangle \times \langle s', X\rangle \times \langle t', X\rangle$, $p_{n-2}(w_j) = \begin{cases} 1 & \text{if } j = n-2 \\ 0 & \text{otherwise} \end{cases}$.
We can do same for $n-2$ more shifts and get a polynomial $p_i(w_j)$ for each symbol $0 \leq i \leq n-1$.
These n polynomials are orthogonal, since $p_i(w_j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{otherwise} \end{cases}$, but they also live in a $O\left(d^4\right)$-dimensional space, since they are degree-4 polynomials in d variables. So $d \geq n^{\frac{1}{4}}$.

2) The symbol e_{n-1} there exist group $E_1 = \{e_i, e_{n-1}\}$ $0 \leq j < n-1$ witch has two parity-check sums orthogonal on it and there exists another parity-check that is orthogonal to $S(E_1)$ on e_{n-1}.
Consider the parity checks $a, b \in F^n$, so that a and b are nonzero vectors orthogonal on the E_1 , and $c \in F^n$ is a codeword that corresponds to the parity-check orthogonal to $S(E_1)$ on e_{n-1}.
Now, these vectors are code words of the $\mathcal{C}^\perp$ and let $w_1, \ldots, w_n \in F^d$ be the columns of the generator matrix of $\mathcal{C}^\perp$.
Thus we can write $a = (\langle v, w_1\rangle, \langle v, w_2\rangle, ..., \langle v, w_n\rangle)$,$b = (\langle u, w_1\rangle, \langle u, w_2\rangle, ..., \langle u, w_n\rangle)$ and similarly $c = (\langle s, w_1\rangle, \langle s, w_2\rangle, ..., \langle s, w_n\rangle)$ for $v, u, s \in F^d$, and where $\langle, \rangle$ means inner product.
Now consider the polynomials $p_{n-1}(X) = \langle v, X\rangle \times \langle u, X\rangle \times \langle s, X\rangle$, where X is the vector $(X_1, ..., X_d)$, $p_{n-1}(w_j) = \begin{cases} 1 & \text{if } j = n-1 \\ 0 & \text{otherwise} \end{cases}$.
Since $\mathcal{C}$ is cyclically shift E_1 and get $E_1' = \left\{e_{(i-1) \mod n}, e_{n-2}\right\}$.
By the same shift on a, b, c, we get $a', b', c' \in \mathcal{C}^\perp$ so that a' and b' are nonzero vectors orthogonal on the E_1' , and c' corresponds to the parity-check orthogonal to $S(E_1')$ on e_{n-2}.
Similarly we can write $a' =$

$(\langle v', w_1\rangle, \langle v', w_2\rangle, ..., \langle v', w_n\rangle)$,b' = $(\langle u', w_1\rangle, \langle u', w_2\rangle, ..., \langle u', w_n\rangle)$ and similarly $c' = (\langle s', w_1\rangle, \langle s', w_2\rangle, ..., \langle s', w_n\rangle)$ for $v', u', s' \in F^d$.

Now consider the polynomials $p_{n-2}(X) = \langle v', X\rangle \times \langle u', X\rangle \times \langle s', X\rangle$, $p_{n-2}(w_j) = \begin{cases} 1 & \text{if } j = n-2 \\ 0 & \text{otherwise} \end{cases}$.

We can do same for $n-2$ more shifts and get a polynomial $p_i(w_j)$ for each symbol $0 \leq i \leq n-1$.

These n polynomials are orthogonal, since $p_i(w_j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{otherwise} \end{cases}$, but they also live in a $O(d^3)$-dimensional space, since they are degree-3 polynomials in d variables. So $d \geq n^{\frac{1}{3}}$.

In general we get that $d \geq n^{\frac{1}{4}}$.

References

[1] S. Lin and D. J. Costello, *Error Control Coding (2nd Edition)*. Prentice Hall, 2004.