Proof of Uniform Partitioning Theorem for LBC

T. Ganesan

gana@ieee.org

SPC Lab, Dept. of ECE

Mar 12th, 2011

Outline

1. Introduction
   - Preliminaries

2. Properties of Uniform codes
   - Uniform Distance

3. Uniform Partitioning Theorem
   - Proof

Linear Block Codes

- A Linear Block Code (LBC) is a collection of n-tuples from a finite or infinite alphabet from a field such that they form a group as per the *addition* defined in the field.
- The smallest Hamming weight of non-zero codeword is the *minimum distance* of the code.
- LBC can be partitioned into uniform sub-sets called *cosets*.
    - The 0^{th} coset is a sub-code by itself.

Definitions

- **Uniform set:** A set is said to be **uniform** if the distance between any pair of elements is a constant.
- **Maximal uniform set:** A uniform set U is said to be **maximal**, if it is the largest possible set in terms of cardinality, for the given length and uniform distance.
- **Non-trivial uniform set:** A uniform set U is said to be **non-trivial** if it contains atleast 3 non-zero elements.

Pair-wise Partitioning Lemma(1)

Lemma I.1

For any LBC, there exists a disjoint code-word pair set (partitioning) such that distance between the code-word pairs is constant. In fact, there exists at least one code-word pair partition for every Hamming weight in the code's distance spectrum.

Pair-wise Partitioning Lemma(2)-Proof

- **Proof:** Consider $d in D(\mathcal{C})$, $\mathbf{c}_1 \in \mathcal{C}$, $D(\mathcal{C})$ be the distance spectrum of $\mathcal{C}$.
  - $\mathcal{D}_H(\mathbf{0}, \mathbf{c}_1) = d$.
- Add any code-word $\mathbf{c}_2 \neq \mathbf{0}$, $\mathbf{c}_2 \neq \mathbf{c}_1$, to both.
  - $\mathcal{D}_H(\mathbf{c}_2, \mathbf{c}_1 + \mathbf{c}_2) = d$.
- We can create disjoint code pairs with distance d for every Hamming weight in the distance spectrum of $\mathcal{C}$.

Uniform Partitioning of LBC

- We seek to partition an LBC such that

$$\mathcal{C} = \bigcup_{i=1}^{L} \mathbf{C}_i, \tag{1}$$

such that $\mathbf{C}_i \cap \mathbf{C}_j = \{\phi\}$, $1 \leq i, j \leq L$, $i \neq j$, where L is the number of constituent uniform sub-sets and $\mathbf{C}_i$, $i = 1, 2, \ldots, L$ are non-trivial uniform sub-codes.

  - We focus on binary LBCs only.

Even Uniform Distance(1)

Lemma II.1

The distance d_u for any non-trivial uniform linear code $\mathbf{C}_0$ is even.

Moreover, the uniform code is linear if and only if $d_u = 2\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1)$ for any two non-zero $\mathbf{c}_0, \mathbf{c}_1 \in \mathbf{C}_0$.

Even Uniform Distance(2)-Proof

Proof: Let $\mathbf{C}_0$ be a linear uniform code with distance d_u. There exists

- $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2 \in \mathbf{C}_0$ such that $\mathbf{c}_2 = \mathbf{c}_0 + \mathbf{c}_1$ and $\mathbf{c}_i \neq \mathbf{0}$ for $i = 0, 1, 2$.
- Consider the Hamming weight of $\mathbf{c}_2$:

$$\mathcal{W}_H(\mathbf{c}_2) = \mathcal{W}_H(\mathbf{c}_0) + \mathcal{W}_H(\mathbf{c}_1) - 2\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1) \tag{2}$$

$$d_u = 2[d_u - \mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1)] \tag{3}$$

- To prove the converse, let $\mathbf{C}_0$ be a uniform code with $d_u = 2\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1)$. Then,

$$\mathcal{W}_H(\mathbf{c}_0 + \mathbf{c}_1) = 2[d_u - \mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1)] = d_u, \tag{4}$$

and hence $\mathbf{c}_2 \in \mathbf{C}_0$.

Even Uniform Distance(3)

Lemma II.2

The uniform distance of a non-trivial linear uniform code and its even parity extension code are the same.

Proof: The even parity extension of a code results in code-words with even Hamming weight. From Lemma II.1, code-words in the linear uniform code all have an even weight. Hence, parity extension simply results in appending a 0 to the code-words, which does not change the distance property of the code.

Existence Condition(1)

Lemma II.3

Let $\mathbf{c_0}, \mathbf{c}_1, \mathbf{c}_2$ *belong to a uniform linear code with distance* d_u *and* $\mathbf{c}_i \neq \mathbf{0}$, *for* $i = 0, 1, 2$. *Then,* $\mathbf{c_0} = \mathbf{c}_1 + \mathbf{c}_2$ *if and only if* $\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \mathbf{c}_2) = 0$.

Existence Condition(1)-Proof

Proof: Consider the sum $\mathbf{c_0} + \mathbf{c}_1 + \mathbf{c}_2$. Using Lemma II.1, one can write

$$\mathcal{W}_H(\mathbf{c}_0 + \mathbf{c}_1 + \mathbf{c}_2) = d_u + d_u - 2\mathcal{W}_H(\mathbf{c}_0 * (\mathbf{c}_1 + \mathbf{c}_2))$$
$$= 2d_u - 2\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 + \mathbf{c}_0 * \mathbf{c}_2) = 2[d_u - d_u + 2\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \mathbf{c}_2)]$$
$$= 4\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \mathbf{c}_2) \tag{5}$$

which shows that if $\mathcal{W}_H(\mathbf{c}_1 * \mathbf{c}_2 * \mathbf{c}_3) = 0$, then $\mathbf{c_0} + \mathbf{c}_1 + \mathbf{c}_2 = \mathbf{0}$. To prove the converse, let $\mathbf{c}_2 = \mathbf{c}_0 + \mathbf{c}_1$. Then,

$$\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \mathbf{c}_2) = \mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 + \mathbf{c}_0 * \mathbf{c}_1) = \mathcal{W}_H(\mathbf{0}).$$

Existence Condition(2)

Corollary 1

If $\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \mathbf{c}_2) = d_u/4$, *then* $\mathcal{W}_H(\mathbf{c}_0 + \mathbf{c}_1 + \mathbf{c}_2) = d_u$, *where* $\mathbf{c}_0$, $\mathbf{c}_1$ *and* $\mathbf{c}_2$ *belong to a uniform linear code* $\mathbf{C}_0$ *with atleast 8 code-words.*

Follows directly from (5) and Lemma II.1.

Rate-1 Code Paritioning(1)

Lemma II.4

There exists a non-trivial uniform sub-code $\mathbf{C}_u \subset \mathbb{F}_2^n \ni$

$$d_u = \begin{cases} \frac{n}{2} & \text{if} \quad n = 4k \\ \frac{n-1}{2} & \text{if} \quad n = 4k+1 \\ \frac{n+2}{2} & \text{if} \quad n = 4k+2 \\ \frac{n+1}{2} & \text{if} \quad n = 4k+3, \end{cases} \tag{6}$$

where $k \in \mathbb{N}, k \geq 1$*. Moreover, subset* $\mathbf{C}_0^F \in \mathbf{C}_u$ *exists which spans a vector space with dimension at least 2.*

Rate-1 Code Paritioning(2)-Proof

Proof: Consider the cardinality for $n = 4k$,

- First, we show that a non-trivial uniform sub-code $\mathbf{C}_u \subset \mathbb{F}_2^n$ exists with distance d_u given in (6) and then show that a linear subset $\mathbf{C}_0^F$ can be obtained from this sub-code.
  - Let $M_{n=4k+i}$ denote the cardinality of the uniform set with code-words of length $n = 4k + i$ for $k \geq 1$, and $i = 0, 1, 2, 3$.
- Hadamard matrices exist for $n = 1, 2$ and $4k$ [1].
  - $\Rightarrow$ there exist uniform codes with distance $d_u = n/2$. i.e., $M_{4k} \geq n$ and $d_u = n/2$.

Rate-1 Code Paritioning(2)-Proof Continued

Consider the cardinality for $n = 4k + 3$,

- Hadamard code has the all zero vector as one of its columns.
- Hadamard code can be shortened by 1 bit without loss of the properties of the code.
  - $M_{4k+3} \geq n$ and $d_u = \frac{n+1}{2}$.
  - Moreover, for $d_u = \frac{n+1}{2}$ the Plotkin boundis known to achieve the equality for uniform codes.

$$M_{Plotkin} \leq \frac{2d_u}{n - 2d_u},$$

- $M_{4k+3} = n + 1$.

Rate-1 Code Paritioning(2)-Proof Continued

To compute a bound of the cardinality for $n = 4k + 1$,

- Consider appending any non-zero column of Hadamard code for $n = 4k$ to the same code as $[\mathbf{H}_n | \mathbf{h}_i]$
- Each column of Hadamard code has $n/2$ non-zero values, half of the extended code has the same Hamming weight and the other half of the extended code-words have their Hamming weight increased by 1.
  - $n/2$ code-words of the extended code with $n = 4k + 1$ have $d_u = \frac{n-1}{2}$.
- $M_{4k+1} \geq \frac{n}{2}$.

Rate-1 Code Paritioning(2)-Proof Continued

To compute the cardinality for $n = 4k + 2$,

- Consider the 1 bit shortened code from $n = 4k + 3$. From Thm. 2 in [2], it follows that $M_{4k+2} \geq \left\lceil \frac{d_u M_{4k+3}}{n} \right\rceil = \left\lceil \frac{n+1}{2} \right\rceil$ and $d_u = \frac{n+2}{2}$. For $n \geq 4$, this lower bound is greater than or equal to 2.
- Thus, we have shown that a uniform sub-code of $\mathbf{C}_u$ exists with even-valued d_u given by (6) and that the cardinality of the sub-code is at least 2 for $k \geq 1$.
- Now, consider any two non-zero code-words and their sum. This creates a non-trivial uniform code.

Rate-1 Code Paritioning(2)-Proof Continued

- $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_0 + \mathbf{c}_1$ and $\mathbf{0}$ can be used to form $\mathbf{C}_0^F$, which is now a non-trivial linear uniform sub-code of $\mathbb{F}_2^n$ with uniform distance d_u given by (6).
- $\mathbf{C}_0^F$ has a cardinality of atleast 4 including the all zero code-word $\mathbf{0}$. Hence, the dimension of the vector space spanned by $\mathbf{C}_0^F$ is at least 2.

1 Introduction

- Preliminaries

2 Properties of Uniform codes

- Uniform Distance

3 Uniform Partitioning Theorem

- Proof

Uniform Partitioning Theorem

Theorem III.1

For a binary LBC $\mathcal{C}$, if $\mathbf{C}_0 \triangleq \mathbf{C}_0^F \cap \mathcal{C}$ is non-trivial for some $\mathbf{C}_0^F$ satisfying the properties in Lemma II.4, the following hold:

(i) *$\mathbf{C}_0$ and its cosets tile $\mathcal{C}$ and one can build a linear maximal uniform partitioning of $\mathcal{C}$ from the cosets of $\mathbf{C}_0$,*

(ii) *The cardinality of $\mathbf{C}_0$ is bounded as $2^2 \leq |\mathbf{C}_0| \leq 2^{\lfloor \log_2 n+1 \rfloor}$, and*

Uniform Partitioning Theorem - Continued

Theorem III.1 -Continued

(iii) $|\mathbf{C}_0| = 2^{j^*+1}$ if $j^* \geq 1$ is the largest integer such that *(a)* $\mathbf{C}_0$ has a subset $\mathbf{C}_{j^*}$ with cardinality j^*+1 and non-zero entries such that

$$\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \ldots * \mathbf{c}_{j^*}) = \frac{d_u}{2^{j^*}}, \tag{7}$$

where $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{j^*} \in \mathbf{C}_{j^*}$, and *(b)* For $l = 1, 2, \ldots, j^* - 1$, for all subsets $\mathbf{C}_l$ of $\mathbf{C}_{j^*}$ with cardinality $l+1$,

$$\mathcal{W}_H(\mathbf{c}_0 * \mathbf{c}_1 * \ldots * \mathbf{c}_l) = \frac{d_u}{2^l}, \tag{8}$$

where, with a slight abuse of notation, $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_l \in \mathbf{C}_l$.

Proof

- **Proof:** Note that, $\mathbf{C}_0$ is linear and its cosets tile $\mathcal{C}$ as it is an intersection of $\mathcal{C}$ and a linear set.
- Let $\mathbf{C}_0^{\max}$ represent a maximal linear uniform sub-code of $\mathcal{C}$ with the same uniform distance as $\mathbf{C}_0$.
- There exists a unitary transform between the basis vectors of $\mathbf{C}_0^{\max}$ and $\mathbf{C}_0$. Therefore, without loss of generality, we can transform the code words in $\mathbf{C}_0^{\max}$ such that it forms a superset of $\mathbf{C}_0$ and preserves the uniform distance property.
    - That is, we have $\mathbf{C}_0 \subseteq \mathbf{C}_0^{\max}$.

Proof-Continued

- Consider any code word $\mathbf{c} \in \mathbf{C}_0^{\max}$, $\mathbf{c} \notin \mathbf{C}_0$. Now, $\mathbf{c} + \mathbf{C}_0$ forms a coset of $\mathbf{C}_0$ and the coset belongs to $\mathbf{C}_0^{\max}$ since it is linear.
- Thus, $\mathbf{C}_0 \cup (\mathbf{C}_0 + \mathbf{c})$ is still a linear uniform set.
  - One can now repeat this procedure of combining the cosets of $\mathbf{C}_0$ to obtain $\mathbf{C}_0^{\max}$.
- Thus, there exists $\mathbf{C}_0^{\max} \supset \mathbf{C}_0$ with the same uniform distance.

Proof-Continued

- The bounds on the cardinality of $\mathbf{C}_0$ follow from the arguments presented in Lemma II.4.
  - The lower bound follows from the fact that when $\mathbf{C}_0$ is a non-trivial set.
  - The upper found follows from the fact that the number of elements is a power of 2 and using the Plotkin bound of $n+1$.
- To find $|\mathbf{C}_0|$, it can be shown from (2) that

$$\mathcal{W}_H\left(\mathbf{c}_0+\mathbf{c}_1+\ldots+\mathbf{c}_{j^*}\right)=\sum_{k=1}^{j^*} 2^k(-1)^{k+1}\binom{j^*}{k}\frac{d_u}{2^k}, \qquad (9)$$

Proof-Continued

- Since $\sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k} = 1$, the summation in (9) equals d_u.
  - This shows that the Hamming weight of the sum $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{j^*}$ is d_u (Due to Lemma II.3).
- Using a similar procedure, we can show the uniform distance property of any linear combination of the code-words $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{j^*}$.
  - The cardinality of the set comprising all linear combinations of these $j^* + 1$ vectors is 2^{j^*+1}.

Uniform Partitioning - Examples

- Hamming (7,4) code : $\mathbf{C}_0 = \{0, 1, 6, 7, 10, 11, 12, 13\}$ and $\mathbf{C}_1 = \{2, 3, 4, 5, 8, 9, 14, 15\}$.
  - $d_u = \frac{n+1}{2} = 4$
- MLSR $(6, 3, 3)_2$ code: $\mathbf{C}_0 = \{1, 2, 5, 6\}$ and $\mathbf{C}_1 = \{0, 3, 4, 7\}$.
  - $d_u = \frac{n+2}{2} = 4.$
- Hadamard codes are themselves maximal uniform codes.
  - $d_u = \frac{n}{2}.$
- MLSR $(9, 4, 3)_2$ code : $\mathbf{C}_0 = \{0, 2, 9, 11\}$
  - $d_u = \frac{n-1}{2} = 4$

Code Partitioning Procedure

1. Find code-words in $\mathcal{C}$ with Hamming weight d_u according to the code length n. Denote this sub-set as $\mathbf{C}_u$.
2. Find a sub-set of $\mathbf{C}_u$ that is closed by using the linearity conditions given in Theorem. Call this sub-set as $\mathbf{C}_0$.
3. Now, $\mathbf{C}_0$ and its cosets form a uniform partitioning of $\mathcal{C}$.

References

J. H. Van Lint and R. M. Wilson,
A Course in Combinatorics,
Cambridge University Press, second edition, 2001.

A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith,
"A new table of constant-weight codes,"
IEEE Transactions on Information Theory, vol. 36, pp. 1344–1380, 1990.