On the Existence and Characterization of Binary Perfect Frequency Distance Codes

N.Suresh Babu, Ravivarma.B
Department of Mathematics
University College, Thiruvananthapuram
Kerala, India.
E-mail: suba_ja@yahoo.com, ravivarmarrr@gmail.com

Abstract

This paper deals with the study of Perfect Binary codes with Frequency distance. The study of Perfect codes is a classic problem in Algebraic Coding Theory.Perfect codes over finite fields with Hamming metric were studied extensively and a complete characterization was obtained for the class of these codes.The non-existence of Perfect codes in Rank metric also has been proved. In this work, the existence of Perfect Binary codes with Frequency distance is proved and a characterization of this class of codes is obtained.

Key words: Error correcting codes, Perfect codes, Hamming metric, Rank metric, Frequency metric.

1 Introduction

The search for the class of Perfect codes and its study is a classic research problem in Algebraic coding theory. An (n, M, d) - error correcting code over a Finite field F is perfect if spheres of radius $t = \lfloor (d-1)/2 \rfloor$ around the code words fill the entire space F^n. As a result of detailed investigations on Perfect codes with Hamming metric, it was proved that any non trivial perfect code over a finite field must have the same parameters as one of the Hamming or Golay codes [3,5,6,7], making it very rare and special.

Perfect Codes over the Binary field with Rank metric were studied in [8]. It was proved that there exists no non-trivial Perfect code of Block length $'n'$ over $GF(2^N)$ where $n \leq N$ [8].

The objective of this paper is to investigate whether Perfect codes exist on Binary spaces with a new metric named Frequency metric introduced in [9]

The main result of this paper is the characterization of Perfect codes in Frequency metric. In section 2, the basic definitions and results related to Perfect codes in Hamming metric are given. Section 3 gives a brief description of Frequency metric. In section 4, we get a relation between Frequency weight and Hamming weight through which the characterization of the class of Perfect codes in Frequency metric is obtained.

2 Perfect Codes with Hamming metric

Let F_2^n be the set of all binary sequences of length n. ie. $F_2^n = \{x = x_1x_2 \ldots x_n : x_i = 0 \ or \ 1\}$. Clearly F_2^n can be considered as an n- dimensional linear space over the binary field $F_2 = \{0, 1\}$ with respect to *modulo* 2 addition ($\oplus_2$) and *modulo* 2 multiplication ($._2$). We refer to [4] and [10] for the basic results in this section.

Definition 2.1. *For each $x = x_1x_2 \ldots x_n \in F_2^n$, the Hamming weight of x is defined as the number of non zero coordinates x_i of x and is denoted by $wt_H(x)$.*

Note that Hamming weight defines a 'norm' on the space F_2^n.

Definition 2.2. *Let $x, y \in F_2^n$. The Hamming distance $d_H(x, y)$ between x and y is the Hamming weight of $x - y$. ie. $d_H(x, y) = wt_H(x - y) = wt_H(x \oplus_2 y)$.*

Hamming distance d_H is a proper 'metric' on F_2^n [4].

Here after, by $F_2^n(H)$ we denote the n-dimensional linear space F_2^n over F_2 with the Hamming metric d_H. Clearly $F_2^n(H)$ is a Normed space with the 'norm' wt_H as well as a Metric space with the 'metric' d_H.

Definition 2.3. *A subset C of $F_2^n(H)$ is called a binary block code of length 'n'. If C has M elements, then C is called an (n, M) block code.*

Definition 2.4. *If C is a block code in $F_2^n(H)$, then the minimum distance of C is given by $d_H(C) = min\{d_H(c_i, c_j) : c_i, c_j \in C, c_i \neq c_j\}$.*

If $d_H(C) = d$, then we say that C is an (n, M, d) code.

Definition 2.5. *If C is a subspace of $F_2^n(H)$, then we call C as a binary linear code. In addition if $dim(C) = k$ and $d_H(C) = d$, then C is called a (n, k, d) linear code.*

Let C be an (n, M, d) code and let $\lfloor t = (d-1)/2 \rfloor$. Then the spheres of radius t around the code words are called Hamming spheres. It is clear that the Hamming spheres are disjoint and the code C is a t-error correcting code.

If C is a t -error correcting (n, M) binary code, then the number of words in a Hamming sphere around each code word is given by $\Sigma_{i=0}^{t} nC_i$.

Result 1. *(***Hamming Bound): If C is a t- error correcting (n, M) code, then $M.\Sigma_{i=0}^{t} nC_i \leq 2^n$.**

Definition 2.6. *Any code satisfying the Hamming bound with equality is called a Perfect code.*

If C is a t-error correcting, binary Perfect code, then the Hamming spheres of radius t around the codewords completely fill the space $F_2^n(H)$. The set of Perfect codes is very limited.

Result 2. *The following are the only Binary Perfect Codes in Hamming metric [10].*

(1). The set of all n-tuples with minimum distance "1" and $t = 0$.

(2). Odd length Binary repetition code.

(3). Binary Hamming codes or other non-linear codes with equivalent parameters.

(4). The Binary $(23, 12, 7)$ *Golay code* G_{23}.

3 Frequency metric

We give a brief description of Frequency weight and Frequency metric on F_2^n introduced in [9] here.

Definition 3.1. *For each $x = x_1x_2 \ldots x_n \in F_2^n$, the 'frequency weight' or simply the 'frequency' of x is defined as $wt_f(x) = [\Sigma_{i=1}^{n-1}(x_i \oplus_2 x_{i+1})] + x_n$.*

Since $(x_i \ \oplus_2 \ x_{i+1}) = 0$ *or* 1 respectively as $x_i = x_{i+1}$ or $x_i \neq x_{i+1}$, the sum $[\Sigma_{i=1}^{n-1}(x_i \oplus_2 x_{i+1})]$ gives the number of of transitions between 0 and 1 (ie. transition number) in x.

Hence the *frequency* of x can be defined as:

$$wt_f(x) = \begin{cases} \text{transition number of x} & \text{if } x_n = 0 \\ \text{(transition number of x)} + 1 & \text{if } x_n = 1. \end{cases}$$

Result 3. *Frequency weight $wt_f(x)$ defines a norm on F_2^n.*

Definition 3.2. *Let $x, y \in F_2^n$. The frequency distance $d_f(x, y)$ between x and y is the frequency weight of $x - y$. ie. $d_f(x, y) = wt_f(x - y) = wt_f(x \oplus_2 y)$.*

By Result 3, the frequency distance d_f is a proper metric on F_2^n.

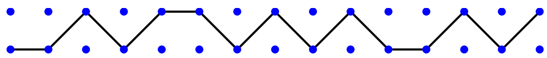
Here after, by $F_2^n(f)$ we denote the n-dimensional linear space F_2^n over F_2 with the Frequency metric d_f. Clearly $F_2^n(f)$ is a Normed space with the norm wt_f as well as a Metric space with the metric d_f.

Example

Space : ${F_2}^{15}$

1. Binary Sequence (x) : 001011010100101

   Binary Curve :

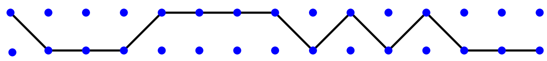
   

   Frequency Weight $(wt_f(x))$: 12

   Hamming Weight $(wt_f(x))$: 7

2. Binary Sequence (y) : 100011110101000

   Binary Curve :

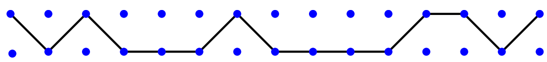
   

   Frequency Weight $(wt_f(y))$: 7

   Hamming Weight $(wt_f(x))$: 7

3. Binary Sequence (x-y) : 101000100001101

   Binary Curve :

   Frequency distance between x and $y = d_f(x, y) = (wt_f(x - y)) = 9$ Hamming distance between x and $y = d_H(x, y) = (wt_H(x - y)) = 6$

4 Relation between Frequency metric code and Hamming metric code

In this section we get a relation between a frequency metric code and a Hamming metric code through a bijective, linear, isometry between the spaces $F_2^n(H)$ and $F_2^n(f)$.

Define $g : F_2^n(H) \longrightarrow F_2^n(f)$ as g$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$, where $y_i = x_i \oplus_2 x_{i+1} \oplus_. .. \oplus_2 x_n$ for all $i = 1, 2, ..., n$.

It is obvious from the definition that g is a bijective, linear map. Also the inverse of g, $\quad g^{-1} : F_2^n(f) \longrightarrow F_2^n(H)$ can be defind as $g^{-1}(y) = x$ where $x_i = y_i \oplus_2 y_{i+1}$ for $i = 1$ to $n-1$ and $x_n = y_n$.

Result 4. *For any $x \in F_2^n(H), wt_H(x) = wt_f(g(x))$.*

Proof: Let $x = (x_1, x_2, ..., x_n)$. Then g$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) =$ y (say) where $y_i = x_i \oplus_2 x_{i+1} \oplus_. .. \oplus_2 x_n$.

$$\begin{aligned} wt_f(g(x)) = wt_f(y) &= \Sigma_{i=1}^{n-1}(y_i \oplus_2 y_{i+1}) + y_n \\ &= (y_1 \oplus y_2) + (y_2 \oplus y_3) + ... + (y_{n-1} \oplus y_n) + y_n \\ &= x_1 + x_2 + ... + x_n \\ &= wt_H(x) \end{aligned}$$

Result 5. *g is an isometry on $F_2^n(H)$*

Proof: Let $x, y \in F_2^n(H)$

$$\begin{aligned} d_H(x,y) &= wt_H(x-y) \\ &= wt_f(g(x-y)) \\ &= wt_f(g(x) - g(y)) \\ &= d_f(g(x), g(y)) \end{aligned}$$

Hence g is a bijective, linear, isometry between $F_2^n(H)$ and $F_2^n(f)$. Thus the '*minimum distance*' of any code C in $F_2^n(H)$ is equal to that of $g(C)$ in $F_2^n(f)$. Hence we have the following result.

Result 6. *If C is an $[n.M, t]$ code in $F_2^n(H)$, then $g(C)$ is an $[n, M, t]$ code in $F_2^n(f)$. Conversely, if C is an $[n.M, t]$ code in $F_2^n(f)$, then $g^{-1}(C)$ is an $[n, M, t]$ code in $F_2^n(H)$.*

This result implies the following result.

Result 7. *If C is a Perfect code in $F_2^n(H)$, then $g(C)$ is a Perfect code in $F_2^n(f)$. Conversely, if C is a Perfect code in $F_2^n(f)$, then $g^{-1}(C)$ is a Perfect code in $F_2^n(H)$*

As the only non trivial Binary perfect codes in $F_2^n(H)$ are the Hamming and Golay codes, by the above result we have the following main result.

Theorem 4.1. *Binary Perfect codes with frequency metric exist. The only binary perfect codes with frequency metric are the g-images of those binary perfect codes with Hamming metric.*

Thus we have the following characterization.

Theorem 4.2. *The only Binary Perfect codes with frequency metric are,*
(1). The set of all n-tuples with minimum frequency distance "1" and " $t = 0$ ".
(2). The code $\{000...0, 1010...01\}$ *which is the g-image of the "Repetition Code" of odd length.*
(3). g-images of binary Hamming codes and other non-linear codes with equivalent parameters.
(4). g-image of the binary $(23, 12, 7)$ *Golay code* G_{23}.

5 Conclusion

In this work we studied the Perfect binary codes with Frequency metric. We proved that Perfect binary codes with frequency metric exist and a complete characterization of this class of codes is given as Theorem 4.2.

References

[1] **M.Bodner, Y.D.Zhou, J.M.Fuster**, "High-Frequency Transitions in Cortical Spike Trains Related to Short-term memory ", Neuroscience, vol.86, no.4, pp.1083 - 1087, 1998.

[2] **Ernst M.Gabidulin, Jurian Simonis**, "Metrics Generated by Families of Subspaces " IEEE Trans.on Information theory, vol.44, no.3, May 1998.

[3] **M.R.Best**, "Perfect Codes hardly exist,IEEE Trans. Inform. Theory ", Vol.IT-29,pp.349-351,1983.

[4] **F.J. Mac Williams and N.J.A.Sloane**, "The Theory of Error Correcting Codes", North Holland 1981.

[5] **A.Tietavainen**, “On the non existence of perfect codes over finite fields”,Siam.Journal of Applied Math.,Vol.24, 1973.

[6] **J.H.Van Lint** , ”A survey of perfect codes”, Rocky mountain J.of math., Vol.5,pp. 199-224, 1975.

[7] **V.A.Zinovev and V.K.Leontev**, ”The non-existence of perfect codes over Galois fields ”, Problems of Control and Inf.theory, Vol.2,pp. 123-132,1973.

[8] **N.Suresh Babu**, ”On Perfect Codes in Rank distance”, Journal of Discrete Mathematical Sciences and Cryptography, vol.11, pp.1-11, Feb 2008.

[9] **N.Suresh Babu**, ”Frequency Metric in Binary Spaces”, International Journal of Mathematics Trends and Technology, vol.52, No.9, Dec 2017.

[10] **Todd K.Moon**, ”Error Correction Coding - Mathematical Methods and Algorithms”, Wiley India (P) Ltd., 2011.