New Constructions of Constant-Weight Codes

Lei Li and Shoulun Long

Abstract. By generalizing a propagation rule for binary constant-weight codes, we present three constructions of binary constant-weight codes. It turns out that our constructions produce binary constant-weight codes with good parameters.

Mathematics Subject Classification (2000). Primary 94B60; Secondary 94B65.
Keywords. Constant-weight codes, sets, linear spaces, free modules.

1. Introduction

Constant-weight codes have a very long history because of both practical applications and theoretical interests. Various methods from algebra, finite geometry, combinatorics, etc., have been employed to construct good codes. The reader may refer to [6] and [2] for a good survey on this topic.

In this paper, we first give a simple propagation rule by identifying a binary constant-weight code with a family of subsets. This idea is further generalized to linear spaces and free modules to construct binary constant-weight codes with reasonable parameters.

2. Preliminaries

In this section, we introduce some concepts and definitions that will be used in the next sections.

2.1. Constant-Weight Codes

A binary constant-weight code \( C \subseteq \mathbb{F}_2^n \) is a set of codewords that have the same (Hamming) weight. \( C \) is called an \((n, M, d; w)\) constant-weight code if \( C \) is a set of cardinality \( M \), such that each codeword has the same weight \( w \), and the distance between any two codewords is at least \( d \). Given \( n, d \) and \( w \), to determine the maximum possible size \( A(n, d, w) \) of an \((n, M, d; w)\) binary constant-weight code is an important problem in coding theory.
In calculating the distance between two codewords we have a useful formula:

**Proposition 2.1** ([8], Lemma 4.3.4). For any two codewords \( x = (x_1, x_2, \ldots, x_n) \) and \( y = (y_1, y_2, \ldots, y_n) \) in \( \mathbb{F}_2^n \), put \( x \ast y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n) \), then

\[
d(x, y) = \text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2\text{wt}(x \ast y).
\]  

(2.1)

### 2.2. Gaussian Coefficients

Given a prime power \( q \) and two positive integers \( k, r \) with \( k \leq r \), the number

\[
\begin{align*}
\left[ \begin{array}{c}
\end{align*}
\end{align*}
\end{array}
\right]
\]

is called a Gaussian coefficient. For the convenience of later usage, we define \( \left[ \begin{array}{c}
\end{array}
\end{array}\right] = 0 \) if \( k > r \). The significance of Gaussian coefficients is described in the following proposition.

**Proposition 2.2** ([8], Theorem 5.1.12). Let \( \mathbb{F}_q \) be a finite field and \( V \) a linear space of dimension \( r \) over \( \mathbb{F}_q \). Then the number of dimension \( k (\leq r) \) subspaces of \( V \) is

\[
\left[ \begin{array}{c}
\end{array}
\end{array}
\right] = \frac{(q^r - 1)(q^r - q) \cdots (q^r - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}.
\]

### 2.3. Linearized Polynomials and Rank Distance Codes

We first review rank distance codes studied by Gabidulin in [3]. Let \( \Lambda = \{A_i\} \) be a set of \( t \times m \) matrices over a finite field \( \mathbb{F}_q \). The distance \( d(A, B) \) between two matrices \( A \) and \( B \) in \( \Lambda \) is defined by \( d(A, B) = \text{rank}(A - B) \) and the minimum distance of \( \Lambda \), denoted by \( d(\Lambda) \), is defined as \( d(\Lambda) = \min\{d(A, B) : A \neq B \in \Lambda\} \). Let \( d = d(\Lambda) \) and \( M = |\Lambda| \). We call \( \Lambda \) a \( (t \times m, M, d) \) rank distance code. For a \( (t \times m, M, d) \) rank distance code \( \Lambda \), the Singleton bound is valid, i.e.,

\[
d(\Lambda) \leq t - l + 1,
\]

(2.2)

where \( l = \log_{q^m} M \). Codes for which equality holds in (2.2) are referred to as MRD-codes (Maximum-Rank- Distance codes).

In [5], Johansson presents a method for constructing MRD-codes from linearized polynomials. Let \( 1 \leq l \leq t \leq m \) be positive integers. A polynomial of the form

\[
F(x) = \sum_{i=0}^{t} f_i x^{q^i},
\]

where \( f_i \in \mathbb{F}_{q^m} \) is called a linearized polynomial. Denote all linearized polynomials of degree not higher than \( q^{l-1} \) as

\[
P_{l,t,m} = \{ F(x) = \sum_{i=0}^{t} f_i x^{q^i} : f_i \in \mathbb{F}_{q^m}, \deg(F(x)) \leq q^{l-1} \}.
\]

Assume \( g_1, g_2, \ldots, g_t \) are specified elements in the field \( \mathbb{F}_{q^m} \) which are linearly independent over \( \mathbb{F}_q \), and for each \( F(x) \in P_{l,t,m} \), put

\[
A_F = (F(g_1), F(g_2), \ldots, F(g_t))^T.
\]