Atlantic Electronic
Journal of Mathematics
Volume **6**, Number **1**, Summer **2014**

http://aejm.ca
http://aejm.ca/rema
pp. **1-10**

THE PARTITION WEIGHT ENUMERATOR AND BOUNDS ON MDS CODES

T.L. Alderson
Svenja Huntemann

Department of Mathematical Sciences
University of New Brunswick Saint John
Saint John, NB E2L 4L5

Abstract. Maximum Distance Separable (MDS) codes are those error - correction codes that meet the singleton bound, thus they have the largest minimum distance possible. The main research problem is to find an upper bound on the length of the codewords when the alphabet size and dimension of the code are fixed.

This paper will present a new technique using the Partition Weight Enumerator for solving this problem in some cases.

1. **Introduction.** A q-ary code C of length n and dimension k is a collection of q^k n-tuples, called *codewords*, with entries from a set (or alphabet) A of size q. In other words, C is a subset of A^n with $|C| = q^k$.

A code is *linear* if its codewords form a k-dimensional subspace of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ denotes the field of order q. Unless otherwise stated, the codes discussed in the sequel shall not be assumed to be linear.

The (Hamming) *distance* between two elements of A^n is the number of coordinate positions in which they differ. Hamming distance d_H serves as a metric on A^n. In particular the triangle inequality holds:

$$d_H(c_1, c_2) + d_H(c_2, c_3) \geq d_H(c_1, c_3) \quad \text{for all } c_1, c_2, c_3 \in A^n.$$

The *minimum distance* d of C is the minimum over all distances between distinct pairs of codewords. It follows that any two codewords agree in at most $n - d$ common coordinates. The information rate of C is k/n, and essentially measures the proportion of a code that is useful (non-redundant).

Error detection is the ability to decide whether the received data is correct or not without having a copy of the original message. Hence, a code C is t error detecting if changing up to t digits in a codeword never produces another codeword.

We say that an $(n, k, d)_q$ code C is e error correcting if from any n-tuple differing from some codeword in at most e places allows the codeword to be deduced.

Error correcting codes enable the provision of reliable digital data transmission and storage when the communication medium (channel) used is subject to bit errors, or “noise”. Through the use of an error correcting code, the receiver is able to

2000 *Mathematics Subject Classification.* Primary: 94B65; Secondary: 94B60, 94B05.

Key words and phrases. MDS code, Weight enumerator, Nonlinear codes, code equivalence.

The first author acknowledges support through the N.S.E.R.C. of Canada. The second author thanks the N.S.E.R.C. of Canada for support through a U.S.R.A. grant.

automatically correct certain errors. The key to error correction is redundancy, adding extra bits to a data string (at a cost to the information rate).

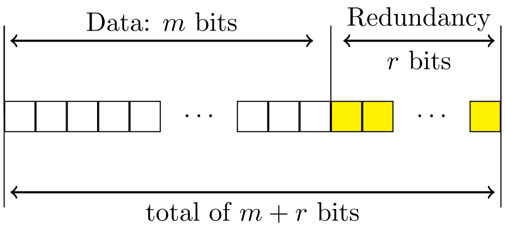

FIGURE 1. Key to error correction: Add redundancy.

For example, instead of sending 1023, the word 10231023 is sent. Such a method is able to detect a single error, but cannot correct any errors. Now for each $\alpha \in A$ use "$\alpha\alpha\alpha$" to represent α. Any single error can be now be corrected (by majority rules). More errors can be corrected by making more repetitions, but this rapidly reduces the information rate of the code, yielding it inefficient. One of the main objectives in information theory is to produce efficient codes with high error correcting ability.

The set of all n-tuples within a distance of t from a given word c is often called a Hamming ball of radius t. If C is a code of minimum distance d, then (by the triangle inequality) any two Hamming balls of radius $\lfloor\frac{d-1}{2}\rfloor$ must be disjoint. Hence, through nearest neighbour decoding, an $(n,k,d)_q$ code C can correct e errors, where $e=\lfloor\frac{d-1}{2}\rfloor$. It is therefore desirable to construct codes with large minimum distance.

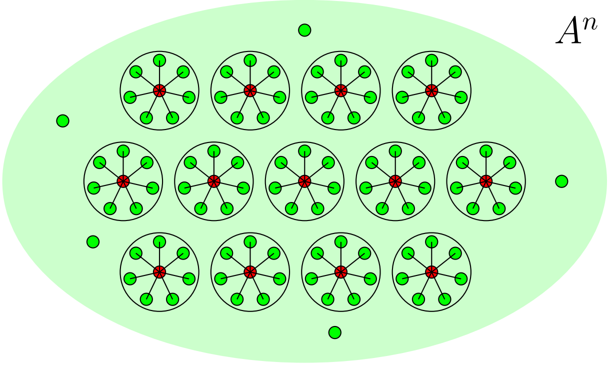

FIGURE 2. Any two hamming balls of radius $\lfloor\frac{d-1}{2}\rfloor$ are disjoint.

To obtain a bound on how large d can be, we observe that in an $(n,k,d)_q$ code C, no two words agree in as many as $n-d+1$ coordinates. There are q^{n-d+1} possible $(n-d+1)$-tuples over A, and each of these may occur at most once as the first $n-d+1$ coordinates of a codeword. Consequently we have $|C|=q^k \leq q^{n-d+1}$, hence $k \leq n-d+1$. This is the Singleton bound, most often expressed as follows:

$$d \leq n-k+1.$$

If C meets the Singleton bound, it is said to be *Maximum Distance Separable* (MDS), denoted $(n,k)_q$-MDS (or $[n,k]_q$-MDS in the linear case). Thus, MDS codes satisfy $d = n - k + 1$ and are in this sense optimal.

Since MDS codes have the largest minimum distance possible, they can detect and correct more errors than any other type of code, a desirable property in the industry. Indeed, over 10,000 U.S. patent applications in the past decade involved MDS codes. A certain type of linear MDS codes, called Reed-Solomon codes, are among the most ubiquitous of error correcting codes, having applications that vary from digital audio, data transfer over mobile radio, satellite communications, and spread spectrum systems. We refer to [24] for detailed discussions regarding both historic and neoteric applications of MDS codes. In addition, MDS codes are equivalent to many constructs in finite geometry, combinatorics, and statistics.

For fixed q and k, a much-studied problem is that of finding the longest code length (n) possible, denoted $M(k,q)$. This fundamental problem has its roots in a statistical question discussed in 1952 by K.A. Bush [6] in a part of combinatorics connected with the orthogonal arrays discussed by R.C. Bose and others. MDS codes were also studied in [19] by R.C. Singleton. F.J. MacWilliams and N.J.A. Sloane [12] introduce their chapter on MDS codes as "one of the most fascinating [. . .] in all of coding theory". There is indeed voluminous literature on the subject.

For example, let $k = 2$. Then C is a set of q^2 codewords of length n, no two of which agree in as many as 2 positions. This is equivalent to the existence of a (Bruck) net of order q and degree n [5], or equivalently a set of $n-2$ mutually orthogonal Latin squares (MOLS) of order q. Thus, determining $M(2,q)$ is equivalent to finding the maximum number MOLS of order q. This problem attracted the attention of L. Euler in the 18th century by way of the 36 officer problem. Tarry [21, 22] showed at the beginning of the last century that the problem had no solution (and hence $M(2,6) = 3$).

It follows that $M(2,q) \leq q+1$, the case of equality corresponding to an affine plane (and hence a projective plane) of order q.

For q a prime power, the existence of affine planes has been known since 1896 [15], but otherwise the problem is almost completely open. The long-standing prime power conjecture states that the order of a finite projective plane must be the power of a prime. At the moment an exact answer to the question of the existence and structure of a finite plane of general order q seems well beyond known techniques. The best result we have so far is the Bruck-Ryser-Chowla Theorem (1949-1950): If a finite projective plane of order q exists and q is congruent to 1 or 2 (mod 4), then q must be the sum of two squares. Accordingly, it seems that one cannot expect much progress with determining $M(2,q)$ in full generality.

The higher dimensional cases, in which MDS codes are equivalent to certain sets of mutually orthogonal latin hypercubes, are even more resistant towards a solution. Similarly to the 2-dimensional case, the problem of determining $M(k,q)$ in the linear case has been met with more success than the general case.

The main results in the linear case have been obtained building on the geometrical methods used by B. Segre [17]. Segre asked a question that eventually became known as the Main Conjecture for Linear MDS Codes: $M(k,q) = k+1$ if $k \geq q$ and $M(k,q) = q+1$ if $k \leq q$, except for $M(k,q) = q+2$ if $k = 3$ or $k = q-1$ and q even.

In the decades since the question has been posed, a lot of work has been done towards proving the Main Conjecture for linear MDS codes; [9] contains a comprehensive list of cases in which the conjecture is known to be true. The recent work of Ball [2], and Ball and DeBeule [3] show the Main Conjecture for linear MDS codes to hold for the majority of cases. Thus the problem of finding $M(k, q)$ is close to being solved for linear MDS codes.

For general, not necessarily linear, MDS codes on the other hand very little is known. Counting arguments show that $M(k, q) \leq q + k - 1$ (see for example [18]), but as the dimension increases, the gap between this bound and the Main Conjecture increases.

Many of the results obtained in the sequel may be found in [25]. Our results were arrived at independently, however for the sake of consistency we have endeavoured where possible to adopt the notation of [25].

2. **Preliminaries.** Two MDS codes are called *equivalent* if one can be obtained from the other through the application of a series of the following operations:

(a) Symbol permutations: fix a coordinate position and apply a permutation over the alphabet to all entries in that position;

(b) Positional permutations: choose two coordinate positions and exchange their entries in every codeword.

Given an arbitrary MDS code C and any codeword $c \in C$ one may clearly apply operations of type (a) to transform c to the zero codeword. This proves the following, which we shall make use of in the sequel.

Lemma 1. *Any $(n, k)_q$-MDS code is equivalent to an $(n, k)_q$-MDS code which contains the all zero codeword.*

An $(n, k)_q$-MDS code holds q^k codewords, no two having as many as k $(= n-d+1)$ common coordinates. Consequently if k (ordered) coordinate positions are fixed, then every possible k-tuple over A arises precisely once in these positions as one ranges over all codewords. Similar observations give the following.

Lemma 2. [18] *Let C be an $(n, k)_q$ MDS code over the alphabet A. Fix a set of $r \leq k$ coordinate positions $\{i_1, \ldots, i_r\}$, and let $\alpha_1, \ldots, \alpha_r$ be (not necessarily distinct) elements of A. There are exactly q^{k-r} codewords with α_j in position i_j.*

The *support* of a codeword c, denoted by $supp(c)$, is the set of coordinate positions in which c has non-zero entries. The *weight* of a codeword, denoted by $wt(c)$, is the size of the support or equivalently, if the code contains the zero codeword, the distance to the zero codeword.

The *weight enumerator* $E(w)$ for a code C counts the codewords of a given weight w. That is $E(w) = |\{c \in C : wt(c) = w\}|$.

Theorem 1. [23] *The weight distribution for $(n, k)_q$ MDS codes which contain the zero codeword is completely determined: $E(0) = 1$; for $0 < w < d$ $E(w) = 0$; and for $d \leq w$*

$$E(w) = (q-1)\binom{n}{w}\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j} \tag{1}$$

As observed by El-Khamy and McEliece [8], the weight enumerator can be generalized as follows. Let $T = \{T_1, T_2, \ldots, T_s\}$ be a partition on the set of coordinate positions $\{1, \ldots, n\}$, where $|T_i| = n_i$ for $i = 1, \ldots, s$. For each $c \in C$ let

$w_i = |supp(c) \cap T_i|$, then c is said to have *T-weight profile*

$$W_T(c) = (w_1, \ldots, w_s).$$

The *partition weight enumerator* for a code C with partition T and associated weight profile $(w_1, \ldots, w_s)$ is given by

$$A^T(w_1, w_2, \ldots, w_s) = |\{c \in C \mid W_T(c) = (w_1, \ldots, w_s)\}|\,.$$

The following Theorem is established by El-Khamy and McEliece in [8] for linear MDS codes. Though their proof can be suitably modified to hold for arbitrary MDS codes containing the zero codeword, we provide an alternate proof.

Theorem 2. *([8]-for linear codes)*
Let C be an $(n,k)_q$ MDS code containing the zero codeword and let $T = \{T_1, \ldots, T_s\}$ be a partition with associated weight profile $(w_1, \ldots, w_s)$. Then the partition weight enumerator is given by

$$A^T(w_1, \ldots, w_s) = (q-1)\binom{n_1}{w_1}\binom{n_2}{w_2}\cdots\binom{n_s}{w_s}\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j} \qquad (2)$$

where $d \leq w = \sum_{i=1}^{s} w_i$.

Proof. Fix $w \geq d$ coordinate positions, say $W = \{i_1, \ldots, i_w\}$, and let N be the number of codewords with support W, i.e. $N = |\{c \in C \mid supp(c) = W\}|$. For $S \subseteq W$, let $A_S = \{c \in C \mid c \neq 0, supp(c) \subseteq W \setminus S\}$. Observe that if $|S| \geq k - (n-w) = w - d + 1$, then $|A_S| = 0$. Second, if $|S| = t \leq w - d$, then $n - w + t$ positions have fixed zero entries, moreover, $0 \notin A_S$, so we have (Lemma 2):

$$|A_S| = q^{k-(n-w+t)} - 1 \quad \left(= q^{w-d-t+1} - 1\right).$$

For each i, $0 \leq i \leq w$, let $\mathcal{A}_i$ be the number of ordered pairs (S, c) where $S \subseteq W, |S| = i, c \in C, supp(c) \subseteq W \setminus S$. It follows by the principle of inclusion-exclusion that

$$\begin{aligned}
N &= \sum_{j=0}^{w}(-1)^j\mathcal{A}_j\\
&= \sum_{j=0}^{w-d}(-1)^j\mathcal{A}_j\\
&= \sum_{j=0}^{w-d}(-1)^j\binom{w}{j}(q^{w-d-j+1}-1)\\
&= \sum_{j=1}^{w-d}(-1)^j\binom{w-1}{j-1}(q^{w-d+1-j}-1)+\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}(q^{w-d+1-j}-1)\\
&= \sum_{j=0}^{w-d-1}(-1)^{j+1}\binom{w-1}{j}(q^{w-d-j}-1)+\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}(q^{w-d+1-j}-1)\\
&= -\sum_{j=0}^{w-d-1}(-1)^j\binom{w-1}{j}q^{w-d-j}+\sum_{j=0}^{w-d-1}(-1)^j\binom{w-1}{j}\\
&\quad+\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d+1-j}-\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}\\
&= q\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}-\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}\\
&\quad+(-1)^{w-d}\binom{w-1}{w-d}q^{w-d-(w-d)}-(-1)^{w-d}\binom{w-1}{w-d}\\
&= (q-1)\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}.
\end{aligned}$$

Therefore

$$A^T(w_1,\ldots,w_s)=(q-1)\binom{n_1}{w_1}\binom{n_2}{w_2}\ldots\binom{n_s}{w_s}\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}. \qquad \square$$

Taking any $(n,k)_q$ MDS code C and deleting a fixed coordinate from each codeword, the resulting code C' is an $(n-1,k)_q$ MDS code. Taking as a subset of C those codewords that have a fixed entry in a fixed position and deleting that coordinate from each codeword, the resulting code C'' is an $(n-1,k-1)_q$ MDS code. These observations result in the following lemmata, whose contrapositive forms shall prove useful in what follows.

Lemma 3. [18] *If an $(n,k)_q$ MDS code exists, then an $(n-1,k)_q$ MDS code exists.*

Lemma 4. [13] *If an $(n,k)_q$ MDS code exists, then an $(n-1,k-1)_q$ MDS code exists.*

3. **A summary of some known results.** The following is a selection of some long established bounds on the length of MDS codes:

Proposition 1. *For an $(n,k)_q$ MDS code the following holds:*

1. *$k+1 \leq M(k,q) \leq q+k-1$;*
2. *$M(k,q) = k+1$ if $k \geq q$;*
3. *$M(k,q) \leq q+k-2$ if q is odd, $k \geq 3$;*
4. *$M(k,q) \leq q+k-3$ if $q \equiv 2 \pmod 4$, $k \geq 3$;*
5. *$M(k,q) \leq q+k-3$ if q is even, $36 \nmid q$, $k \geq 4$;*
6. *$M(k,q) \leq q+k-3$ if $q \equiv 1, 2 \pmod 4$ and the square-free part of q is divisible by a prime of the form $4t+3$.*

Proof. For the first three items see [18]. Items 4 and 5 are found in [1], and for 6 see [13, Theorem 1 (8)]. □

For some codes of restrictive dimension or alphabet size it is sometimes possible to improve upon the bounds stated above.

Proposition 2. *(Bounds for codes of small dimension)*

1. *$M(2,6) = 3$;*
2. *$4 \leq M(2,q) \leq q+1$ if $q \neq 2, 6$;*
3. *$M(2,10) \leq 8$;*
4. *If $q \equiv 1, 2 \pmod 4$ and q is not the sum of two squares, then*
   - *(a) Let t be the largest positive integer for which $\frac{1}{2}t^4 - t^3 + t^2 + \frac{1}{2}t - 1 < q$. Then $M(2,q) \leq q-t$.*
   - *(b) Let t be the largest positive integer for which $8t^3 + 18t^2 + 8t + 4 - 2\rho(t^2 - t - 1) + \frac{9}{2}\rho(\rho-1)(t-1) < 3q$, where $\rho \in \{0,1,2\}$ and $\rho \equiv t+1 \pmod 3$. Then $M(2,q) \leq q-t$.*
5. *$M(3,q) \leq q$ if $q \equiv 2 \pmod 4$.*

Proof. The first item is from Tarry [21, 22]. For the second point see [4] and Proposition 1. Lam et al. [10] showed that $M(2,10) \leq 10$, which results in the third item when combined with the main result in [20] (as mentioned in [16]). Part 1 of item 4 can be found in [5] and part 2 in [14]. The last result is from [1]. □

Proposition 2 (4) together with Lemma 4 give the following result which does not seem to appear in the literature.

Corollary 1. *If $q \equiv 1, 2 \pmod 4$ and q is not the sum of two squares, and t is the largest positive integer for which either*

$$\frac{1}{2}t^4 - t^3 + t^2 + \frac{1}{2}t - 1 < q,$$

or

$$8t^3 + 18t^2 + 8t + 4 - 2\rho(t^2 - t - 1) + \frac{9}{2}\rho(\rho-1)(t-1) < 3q$$

where $\rho \in \{0,1,2\}$ and $\rho \equiv t+1 \pmod 3$, then $M(k,q) \leq q+k-2-t$.

Quite recently, Yang, Zhang, and Wang [25] established new bounds on MDS codes using the generalized weight enumerator.

Proposition 3. *(See [25])*

1. *If q is odd, then $M(q-1,q) \leq q+1$.*
2. *If q is even, $t \geq 4$, and $(t-1)!$ does not divide $(q-t+4)(q-t+3)\cdots(q+1)(q)(q-2)$, then $M(t,q) \leq q+t-3$, and $M(q-2,q) \leq q+t-3$.*

As we see, the main conjecture for linear MDS codes does not hold for general MDS. Relaxing the conditions to inequalities gives the general conjecture.

Conjecture 1 (**The Main Conjecture for General MDS Codes**).

$$M(k,q) = k+1 \textit{ if } \; q \leq k.$$

Taking $q > k$ we have

$$M(k,q) \leq \begin{cases} q+2 & \textit{if } q = 2^t, t \geq 2 \textit{ and } k = 3 \textit{ or } k = q-1, \\ q+1 & \textit{otherwise.} \end{cases}$$

4. **Some new proofs.** The following has been shown in many different ways. To our knowledge, the alternative proof given here is new.

Theorem 3. *If q is odd and $k \geq 3$, then $M(k,q) \leq q+k-2$.*

Proof. Let C be a $(q+k-1,k)_q$-MDS code, thus $d = q$. Assume without loss of generality that the zero codeword is contained in C.

We choose to partition the code the following way with associated weight profile:

$$T_1 = \{1,2\} \quad T_2 = \{3,4,\ldots,k-1\} \quad T_3 = \{k,k+1,\ldots,q+k-1\};$$

$$w_1 = 2 \quad w_2 = 0 \quad w_3 = q-2.$$

(Note that $T_2 = \emptyset$ is admissible.) Let $S \subseteq C$ be the collection of codewords satisfying this characteristic. From Equation 2 we know

$$|S| = A^T(2,0,q-2) = (q-1)\binom{q}{2} = \frac{q(q-1)^2}{2}.$$

Let $C_{a,b} = \{c \in S \mid c_1 = a, c_2 = b\}$ with $a,b \neq 0$. Then $S = \bigcup C_{a,b}$. From the $(q-1)^2$ choices for the pair a,b, there will be one such that

$$|C_{a,b}| \geq \left\lceil \frac{q}{2} \right\rceil. \tag{3}$$

Each codeword in $C_{a,b}$ has exactly two zeroes in the positions of T_3, moreover, no two words in $C_{a,b}$ have a zero entry in a common coordinate of T_3 (else $d = q$ is violated in C). It follows that

$$|C_{a,b}| \leq \left\lfloor \frac{q}{2} \right\rfloor. \tag{4}$$

From (3) and (4) we have $\frac{q}{2}$ an integer, so q is even. The result follows. □

Remark 1. Proposition 3-part 1 can be proven similarly by choosing $\{T_1 = \{1,2\}, T_2 = \{3,\ldots,q+2\}\}$ as a partition and $(2,2)$ as the weight profile. Observing that $(supp(\alpha) \cap T_2) \cap (supp(\beta) \cap T_2) = \emptyset$ for any two distinct $\alpha, \beta \in C_{a,b}$ (else $d < 4$) gives $|C_{a,b}| \leq \lfloor q/2 \rfloor$.

The next result follows from Proposition 3. However, the proof given here is new, and demonstrates the use of the partition weight enumerator as well as a link with triple systems.

Theorem 4. *If $q \equiv 4 \pmod 6$, then $M(q-2,q) \leq q+1$.*

Proof. Assume that a $(q+2,q-2)_q$ MDS code C with $q \equiv 4 \pmod 6$ exists, thus $d = 5$. Without loss of generality assume that the code contains the zero codeword.

We choose to partition the code and associate a weight profile in the following way:

$$T_1 = \{1,2\} \quad T_2 = \{3,4,\ldots,q+2\};$$

$$w_1 = 2 \quad w_2 = 3.$$

Let $S \subseteq C$ be the set of all codewords satisfying these criteria. From the partition weight enumerator (Equation 2) we know that

$$|S| = A^T(2,3) = (q-1)\binom{q}{3} = \frac{q(q-1)^2(q-2)}{6}.$$

Then there exist $a, b \neq 0$ from the alphabet, such that

$$|C_{a,b}| \geq \left\lceil \frac{q(q-2)}{6} \right\rceil, \tag{5}$$

where $C_{a,b} = \{c \in S \mid c_1 = a, c_2 = b\}$.

To achieve a minimum distance of $d = 5$, for any two codewords $\alpha, \beta \in C_{a,b}$ it has to hold that $supp(\alpha) \cap T_2$ and $supp(\beta) \cap T_2$ have at most one coordinate in common. Thus the collection $\{supp(\alpha) \cap T_2 \mid \alpha \in C_{a,b}\}$ forms a set of triples with no pair in common (a triple system).

Counting ordered pairs (α, t) where $\alpha \in C_{a,b}$ and $t \in supp(\alpha) \cap T_2$, we get

$$(|C_{a,b}|)(3) \leq (q) \left\lfloor \frac{q-1}{2} \right\rfloor. \tag{6}$$

Since q is even, combining (5) and (6) results in

$$|C_{a,b}| = \frac{q(q-2)}{6}.$$

Then, $\frac{q(q-2)}{6}$ has to be an integer, thus $q \equiv 0, 2 \pmod 6$ which is a contradiction to $q \equiv 4 \pmod 6$. Therefore if $q \equiv 4 \pmod 6$ no $(q+2, q-2)_q$ MDS code exists and by Lemma 3, $M(q-2, q) \leq q+1$. □

Combining the result of Theorem 4 with Lemma 4, we get the following.

Corollary 2. *If $q \equiv 4 \pmod 6$, then $M(q-1, q) \leq q+2$.*

5. Conclusion.

There are still many open questions concerning the upper bound of general MDS codes. Except for small or very large dimensions, little is known regarding truth of the main conjecture. Moreover a motivating question is that of when the conjectured bounds are met with equality. In short, even though the case for linear codes has been largely solved, there is still plenty of room for progress regarding general MDS codes.

The Partition Weight Enumerator seems to provide some useful techniques for tackling the problem of determining $M(k, q)$, and we hope that further work will confirm this.

REFERENCES

[1] T. Alderson, *Extending MDS codes*, Ann. Comb., **9** (2005), no. 2, 125–135

[2] S. Ball, *On sets of vectors of a finite vector space in which every subset of basis size is a basis*, J. Eur. Math. Soc., **14** (2012), no. 3, 733–748

[3] S. Ball and J. DeBeule, *On sets of vectors of a finite vector space in which every subset of basis size is a basis II*, Des. Codes Cryptogr., **65** (2012), no. 1-2, 5–14

[4] R.C. Bose, S.S. Shrikhande, and E.T. Parker, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Canad. J. Math., **12** (1960), 189–203

[5] R.H. Bruck, *Finite nets. II. Uniqueness and imbedding*, Pacific J. Math., **2** (1963), 421–457

[6] K.A. Bush, *Orthogonal arrays of index unity*, Ann. Math. Statistics, **23** (1952), 426–434

[7] C.J. Colbourn and J.H. Dinitz (editors), *Handbook of combinatorial designs*, second ed., Chapman & Hall/CRC, Boca Raton, FL (2007)

[8] M. El-Khamy and R.J. McEliece, *The partition weight enumerator of MDS codes and its applications*, Proc. Int. Symp. Inf. Theory ISIT (2005), 926–930

[9] J.W.P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, Finite geometries, 201–246, Dev. Math., **3**, Kluwer Acad. Publ., Dordrecht, 2001

[10] C.W.H. Lam, L. Thiel, and S. Swiercz, *The non-existence of finite projective planes of order* 10, Canad. J. Math., **41** (1989), no. 6, 1117–1123

[11] T.P. Kirkman, *On a Problem in Combinations*, The Cambridge and Dublin Math. J., **2** (1847), 191–204

[12] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Co., Amsterdam, 1977

[13] C. Maneri and R. Silverman, *A vector-space packing problem*, J. Algebra, **4** (1966), 321–330

[14] K. Metsch, *Improvement of Bruck's completition theorem*, Des. Codes Cryptogr., **1** (1991), no. 2, 99–116

[15] E.H. Moore, *Tactical Memoranda I-III*, Amer. J. Math., **18** (1896), 264–303

[16] G.L. Mullen, *A candidate for the "next Fermat problem"*, Math. Intelligencer, **17** (1995), no. 3, 18–22

[17] B. Segre, *Curve razionali normali e k-archi negli spazi finiti*, Ann. Mat. Pura Appl. (4), **39** (1955), 357–379

[18] R. Silverman, *A metrization for power-sets with applications to combinatorial analysis*, Canad. J. Math., **12** (1960), 158–176

[19] R.C. Singleton, *Maximum distance q-nary codes*, IEEE Trans. Information Theory, **IT-10** (1964), 116–118

[20] S.S. Shrikhande, *A note on mutually orthogonal Latin squares*, Sankhā Ser. A, **23** (1961), 115–116

[21] G. Tarry, *Le problème de 36 officiers*, Compte Rendu de l'Assoc. Français Adv. Sci. Naturel, **1** (1900), 122–123

[22] G. Tarry, *Le problème de 36 officiers*, Compte Rendu de l'Assoc. Français Adv. Sci. Naturel, **2** (1901), 170–203

[23] L.M.G.M. Tolhuizen, *On Maximum Distance Separable codes over alphabets of arbitrary size*, Proc. Int. Symp. Inf. Theory ISIT (1994), 431

[24] S.B. Wicker and V.K. Bhargava (editors), *Reed-Solomon Codes and their Applications*, IEEE Press, New York, 1994

[25] J. Yang, Y. Zhang, and D. Wang, *Upper bounds of Maximum Distance Separable codes*, J. Shanghai Univ., **17** (2011), no. 3, 289–292

Received September 15, 2004; revised February 2005.

E-mail address: tim@unb.ca, svenja.huntemann@unb.ca