Sieve of Eratosthenes and Bose’s Packing Problem

Peide CHEN\textsuperscript{a} and Percy Brill\textsuperscript{b}

\textsuperscript{a}Dept. of Statistics, Colorado State University, U. S. A.
\textsuperscript{b}Dept. of Management Sci. & Dept. of Mathematics & Statistics, University of Windsor, Canada.

May 13, 1997

Abstract

In this paper we discuss Bose’s Packing Problem on $PG(k-1, s)$, where $PG(k-1, s)$ denotes the $(k - 1)$ dimensional projective space on the Galois field $GF(s)$. The problem is to determine the largest possible $N \times k$ matrix having property $P_t$. An $N \times k$ matrix on $GF(s)$ has property $P_t$, $t \leq k$, if any of its $t \times k$ submatrices is of full rank. The maximum value of $N$ will be denoted by $N(s, t, k)$. When $s = 2$, $t = 3$, the problem has already been solved. In section 2, we describe a general method called the removing procedure, which is similar to the classical sieve of Eratosthenes, to solve the problem for any parameter set. In section 3, we give an example with $(s, t, k) = (5, 3, 4)$ to show the method in detail, and also give results for some other parameter values. In section 4, we propose another method, the search procedure, which is more effective than the removing procedure after the latter performs to a certain step, especially when it is near the end. In section 5, we give a complete solution for $s = t = 3$: $N(3, 3, k) = 2^{k-1}$, and the matrix consists of all row vectors in $\{0,1\}^k$ with odd weight.
1. Preliminary

Sieve of Eratosthenes is a general method to find all prime numbers not greater than a given integer \( n \). We do not consider 1 as a prime, so the first prime is 2. We remove all the multiples of 2 from the list \{2, 3, \ldots, n\}, and the first unremoved number 3 is the second prime. Next we remove all the multiples of 3 from the remaining list \{3, 5, \ldots, n\} to get a new prime — the first unremoved number 5. Inductively, after getting a new prime, remove all its multiples from the remaining list, and then the first unremoved number is the next new prime. Continue this procedure until the remaining list becomes empty, to get all the primes not greater than \( n \).

An \( N \times k \) matrix on \( GF(s) \) has property \( P_t, \ t \leq k \), if any of its \( t \times k \) sub-matrices is of full rank, i.e., any \( t \) row vectors are linearly independent. To determine the largest possible \( N \times k \) matrix on \( GF(s) \) with property \( P_t \), is a famous open problem known as “Bose’s Packing Problem”. The maximum value of \( N \) which depends on \( s, \ t, \ k \), will be denoted by \( N(s, t, k) \). The motivation came from the area of factorial design where we regard a \( k \)-dimensional non-zero vector as a point in the \((k-1)\)-dimensional projective space \( PG(k-1, s) \), so the problem is commonly known as Bose’s Packing Problem on \( PG(k-1, s) \). The solutions are known for only a few cases with very small parameter values. For \( t = 1, 2 \) the problem becomes trivial: \( N(s, 1, k) = \infty \), \( N(s, 2, k) \) = the number of distinct
points in $PG(k - 1, s) = \frac{s^k - 1}{s - 1}$. The first non-trivial $t$ is $t = 3$.

The main idea in Sieve of Eratosthenes can be used to solve Bose’s Packing Problem for any specific parameter group $(s, t, k)$, by listing all non-zero row vectors of $PG(k - 1, s)$ in some order and giving a reasonable removing procedure.

For a Galois field $GF(s)$, when $s$ is a prime, we use $\{0, 1, \ldots, s - 1\}$ to represent its elements, so it has a natural order. If $s = p^l$ is a power of prime $p$, we wish to give $GF(s)$ an ordering and list its elements as $\{\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{s-1}\}$. To do so, we consider $\sum_{i=0}^{l-1} a_i x^i \in GF(s)$ as a vector $(a_{l-1}, \ldots, a_1, a_0) \in [GF(p)]^l$, and use the lexicographic order of $[GF(p)]^l$ to order them. Thus for $p = l = 2$,

$$GF(4) = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = x, \alpha_3 = x + 1\},$$

and for $p = 3, l = 2$,

$$GF(9) = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = 2, \alpha_3 = x, \ldots, \alpha_7 = 2x + 1, \alpha_8 = 2x + 2\}$$

e etc.

For the projective space $PG(k - 1, s)$, we always assume that its elements have their normalized form, i.e., the first non-zero components are always equal to 1.

Given a $(t - 1) \times k$ matrix with row vectors $\xi_1, \xi_2, \ldots, \xi_{t-1}$ in $PG(k - 1, s)$, suppose they are linearly independent and in lexicographic order. By doing elementary row transformations, we can obtain its canonical form with row vectors
\( \eta_1, \eta_2, \ldots, \eta_{t-1} \) where \( \eta_i = (0, \ldots, 0, 1, b_{i, r_i+1}, \ldots, b_{i, k}) \) for \( 1 \leq i \leq t - 1 \), i.e. \( r_i \) is the position of the first non-zero component of the vector \( \eta_i \), and is such that

(i) \( 1 \leq r_{t-1} < \cdots < r_2 < r_1 \leq k \),

(ii) \( b_{i, r_j} = 0 \) for all \( 1 \leq i < j \leq t - 1 \).

Such row vectors \( \eta_1, \eta_2, \ldots, \eta_{t-1} \) form the smallest basis of the row space generated by \( \xi_1, \xi_2, \ldots, \xi_{t-1} \) in the following sense: If \( \xi_1, \xi_2, \ldots, \xi_{t-1} \) is any other basis of the row space in lexicographic order, then \( \eta_i \leq \xi_i \) for all \( 1 \leq i \leq t - 1 \), and the sub-matrix \( (b_{t-i, r_j})_{1 \leq i, j \leq t-1} \) is the identity matrix of size \( (t - 1) \times (t - 1) \).

Notice that in the above procedure for obtaining the canonical form of the matrix, the linear independence of \( \xi_1, \xi_2, \ldots, \xi_{t-1} \) is not essential. However without such linear independence, the first few \( \eta \) may be zero row vectors, and the properties (i) and (ii) would hold only for subscripts corresponding to non-zero \( \eta \). The removing procedure given in next section uses only the case of linear independence.

2. The Removing Procedure

Section 1 describes how to give any Galois field \( GF(s) \) a reasonable order, and therefore it is possible to list all vectors of \( PG(k-1, s) \) in lexicographical ordering. Now we describe a removing procedure to solve Bose's Packing Problem on \( PG(k-1, s) \) for any given parameter set \( (s, t, k) \). In the following discussion, \( (s, t) \) is given and fixed.
Obviously, if an $N_k \times k$ matrix on $GF(s)$ is a solution for parameter set $(s, t, k)$, then adding a zero column on the left, the $N_k \times (k+1)$ matrix is that part of a solution for parameter set $(s, t, k+1)$ which consists of all row vectors before $e_1$, where $e_i$ denotes the unit vector with the $i$-th component 1 and elsewhere 0. So to get a solution for parameter set $(s, t, k)$ with $k > t$, we use induction and assume that a solution for parameter set $(s, t, k-1)$ is available. Denote the row vectors of the $(s, t, k-1)$-solution (after adding a 0 as their first component) by \{\xi_1, \cdots, \xi_{N_{k-1}}\}. Then any $t$ vectors of \{\xi_1, \cdots, \xi_{N_{k-1}}\} are linearly independent, while any other vector having first component 0 must be a linear combination of some $t-1$ vectors of \{\xi_1, \cdots, \xi_{N_{k-1}}\}, which we want to remove. After we remove all of them, the remaining list of all non-zero vectors in $PG(k-1, s)$ consists of all vectors with first component 1. The first one $e_1$ will be a new row vector of the solution. Denote it as $\xi_{N_{k-1}+1}$, and add it to the list of $\xi$.

In general, when we get a new vector of the solution $\xi_j = (a_{j1}, \cdots, a_{jk})$ such that any $t$ vectors of \{\xi_1, \cdots, \xi_j\} are linearly independent, while any other vector before $\xi_j$ must be a linear combination of some $t-1$ vectors of \{\xi_1, \cdots, \xi_{j-1}\}, and has been removed (\xi_1, \cdots, \xi_j themselves are also removed) we add it to the list of $\xi$, and do the following removing procedure.

For any $1 \leq i_1 < \cdots < i_{t-2} \leq j-1 < i_{t-1} = j$, $\xi_{i_1}, \cdots, \xi_{i_{t-1}}$ are linearly independent and in lexicographical order. Regard them as the row vectors of a $(t-1) \times k$ matrix, get its canonical form described in section 1 with row vectors
\( \eta_1, \eta_2, \ldots, \eta_{t-1}, \) remove all vectors of the form \( \xi_j + \sum_{u=1}^{t-2} c_u \eta_u, \) \( 0 \leq c_u \leq s - 1 - a_j r_u, \) \( 1 \leq u \leq t - 2 \) from the remaining list. Then denote the first unremoved row vector by \( \xi_{j+1}, \) which is the next new vector of the solution, add it to the list \( \xi, \) and redo the removal until the list becomes empty.

We only use the first \( t - 2 \) row vectors of the canonical form, and replace the last one by \( \xi_j \) itself, because we need only to remove vectors after \( \xi_j. \) In performing the removing procedure, we suggest to keep all the \((t - 2) \times k\) matrices formed by the first \( t - 2 \) row vectors of the canonical form as important information for each \( \xi_j, \) since in addition to their essential role in further removing, they also help to check if \( \xi_j \) is correctly unremoved. A routine argument shows that \( \xi_j \) is correctly unremoved if and only if all such \((t - 2) \times k\) matrices for \( \xi_j \) are distinct.

There remains the question of getting a solution for the smallest possible \( k = t \) as the starting point. We have two cases, one trivial, and the other not difficult, as follows.

(i) When \( t \geq s, \) \( N(s, t, t) = t + 1 \) is trivial, \( \xi_i = e_i \) for \( 1 \leq i \leq t \) and \( \xi_{t+1} = (1, 1, \ldots, 1) \) gives a solution. This is because a vector with some zero components is a linear combination of at most \( t - 1 \) vectors from \( \{\xi_1, \ldots, \xi_t\}, \) while a vector without zero component must have at least two components taking the same value in \( GF(s), \) so it is a linear combination of \( \xi_{t+1} \) and at most \( t - 2 \) vectors from \( \{\xi_1, \ldots, \xi_t\}. \)

(ii) When \( t \leq s - 1, \) \( N(s, t, t) \geq t + 2 \) is easy, \( \xi_i = e_i \) for \( 1 \leq i \leq t \)
and \( \xi_{t+1} = (1, 1, \ldots, 1) \), \( \xi_{t+2} = (1, 2, \ldots, s-1) \) gives the first \( t + 2 \) row vectors of a solution as our starting point, and the following revised removing procedure will find the rest of the solution vectors. Since we have not removed any vector before, the removing procedure needs to be revised for the first step: for any \( 1 \leq i_1 < i_2 < \cdots < i_{t-1} \leq t + 2 \), vectors \( \xi_{i_1}, \ldots, \xi_{i_{t-1}} \) are linearly independent and in lexicographic order. Regard them as the row vectors of a \((t-1) \times t\) matrix, get its canonical form described in section 1 with row vectors \( \eta_{i_1}, \eta_{i_2}, \ldots, \eta_{i_{t-1}} \), remove all vectors of the form \( \xi_{i_{t-1}} + \sum_{u=1}^{t-2} c_u \eta_u \), \( 0 \leq c_u \leq s - 1 - a_j r_u \), \( 1 \leq u \leq t - 2 \) and \( \xi_{i_1}, \ldots, \xi_{i_{t-1}} \) from the list. The only procedural difference is that here we allow \( \xi_{i_{t-1}} \neq \xi_{t+2} \). The first unremoved row vector becomes a new member of the solution. Then use the original removing procedure to obtain the remaining vectors of a solution.

3. Examples

Example 1. Solution for parameter set \((s, t, k) = (7, 6, 6)\)

We have

\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 & 5 & 6 \\
\end{pmatrix}
\]

as our starting point. Obviously, all row vectors with some zero components will
be removed because they are linear combinations of at most five unit vectors \( e \). Furthermore all row vectors with at least two components taking the same value will be removed because they are linear combinations of \( \xi_7 \) and at most four unit vectors \( e \). The first seven row vectors have already reduced a list of 19608 vectors to a list of 120 vectors, the rest are vectors with the last five components being permutations of \( (2, 3, 4, 5, 6) \). If the permutation contains at least one fixed point, then the vector is a linear combination of \( \xi_8 \) and at most four unit vectors \( e \), and hence is removed. Now there remains a list of 44 vectors, 24 being permutations which are 5-cycles, and 20 being permutations, each of which is a product of a 3-cycle and a transposition. The row space generated by \( \xi_8 \), \( \xi_8 \) removes 33 of them (any row vector differing from vectors of that row space at most in three components, will be removed). The rest, eleven row vectors are

\[
\begin{align*}
1 & 3 & 2 & 5 & 6 & 4 \\
1 & 4 & 2 & 5 & 6 & 3 \\
1 & 5 & 2 & 6 & 3 & 4 \\
1 & 6 & 4 & 2 & 3 & 5
\end{align*}
\begin{align*}
1 & 3 & 6 & 4 & 2 & 5 \\
1 & 4 & 5 & 3 & 6 & 2 \\
1 & 5 & 2 & 6 & 4 & 3 \\
1 & 6 & 4 & 3 & 2 & 5
\end{align*}
\begin{align*}
1 & 3 & 6 & 5 & 2 & 4 \\
1 & 4 & 5 & 6 & 2 & 3 \\
1 & 5 & 6 & 2 & 3 & 4
\end{align*}

Since any of them differs from some vectors of the row space generated by \( \xi_7 \), \( \xi_8 \) at most in three components, so they are all removed. Therefore the starting \( 8 \times 6 \) matrix is in fact the whole solution.

It is somewhat surprising that the solutions for \((s, t, k) = (7, j, j), j =\)
3, 4, 5 are
\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} =
\begin{pmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
1 & 1 & 1 \\
1 & 2 & 3 \\
1 & 3 & 2 \\
1 & 5 & 6 \\
1 & 6 & 5 \\
\end{pmatrix},
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} =
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 \\
1 & 3 & 6 & 2 \\
1 & 6 & 5 & 3 \\
\end{pmatrix},
\]
and
\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} =
\begin{pmatrix}
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 & 5 \\
1 & 3 & 2 & 5 & 6 \\
\end{pmatrix},
\]
i.e., \( N(7, j, j) = 8 \) for \( j = 3, 4, 5, 6 \). And it is much easier to get the solutions
for \((s, t, k) = (5, j, j), \ j = 3, 4, \) which are
\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} =
\begin{pmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
1 & 1 & 1 \\
1 & 2 & 3 \\
1 & 3 & 4 \\
1 & 5 & 6 \\
1 & 6 & 5 \\
\end{pmatrix},
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} =
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 \\
1 & 3 & 6 & 2 \\
1 & 6 & 5 & 3 \\
\end{pmatrix},
\]
and the solution for \((s, t, k) = (4, 3, 3)\) which is
\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} =
\begin{pmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
1 & 1 & 1 \\
1 & \alpha_2 & \alpha_3 \\
\end{pmatrix}.
\]
We can unify all these results in a formula:

\[ N(s, t, t) = s \lor t + 1 = \begin{cases} 
  s + 1 & \text{for } t < s \\
  t + 1 & \text{for } t \geq s
\end{cases} \]

for \( s \leq 7 \). The question arises whether the above formula is true for other \( s \). As we have shown, the \( t \geq s \) part is true for any \( s \), but the answer for the other part is no in general. In fact, the next prime \( s = 11 \) gives a counter-example: \( N(11, 3, 3) = 8 \neq 12 \), a solution is given by

\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} = \begin{pmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
1 & 1 & 1 \\
1 & 2 & 3 \\
1 & 3 & 2 \\
1 & 4 & 5 \\
1 & 5 & 4 \\
\end{pmatrix}.
\]

In the above example and other results, all the solutions are the "starting point", i.e. in the case when \( k = t \). Now we discuss the case of \( k > t \) by giving an example to show the detail of the removing procedure and some further results.

**Example 2. Solution for the parameter set** \( (s, t, k) = (5, 3, 4) \)

We have already a starting point

\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\xi_7 \\
\xi_8 \\
\end{pmatrix} = \begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 \\
0 & 1 & 2 & 3 \\
0 & 1 & 3 & 4 \\
\end{pmatrix}
\]

10
After getting $\xi_7 = (1 \ 0 \ 0 \ 0)$, we use the notation $(i, j)$ at the end of a vector to indicate that the vector has been removed due to being a linear combination of $\xi_i$ and $\xi_j$, and use $(*)k$ to denote the vector is the $k$-th member of the required solution. We keep all $\eta_{1}^{(i, j)}$ ($1 \leq i < j$, for each $j$), the first row vector in the canonical form of the matrix $\begin{pmatrix} \xi_i \\ \xi_j \end{pmatrix}$ as important information for further use as previously mentioned.

| 1000 (* 7) | 1001 (1,7) | 1002 (1,7) | 1003 (1,7) | 1004 (1,7) |
| 1010 (2,7) | 1011 (* 8) | 1012 (1,8) | 1013 (1,8) | 1014 (1,8) |
| 1020 (2,7) | 1021 (2,8) | 1022 (7,8) | 1023 (* 9) | 1024 (1,9) |
| 1030 (2,7) | 1031 (2,8) | 1032 (7,9) | 1033 (7,8) | 1034 (* 10) |
| 1040 (2,7) | 1041 (2,8) | 1042 (8,9) | 1043 (2,9) | 1044 (7,8) |

1000: 0001, 0010, 0100, 0111, 0123, 0134
1011: 0001, 0010, 0100, 0111, 0123, 0134, 0011
1023: 0001, 0010, 0100, 0111, 0123, 0134, 0014, 0012
1034: 0001, 0010, 0100, 0111, 0123, 0134, 0013, 0014, 0011

| 1100 (3,7) | 1101 (* 11) | 1102 (6,9) | 1103 (1,11) | 1104 (1,11) |
| 1110 (* 12) | 1111 (4,7) | 1112 (1,12) | 1113 (6,10) | 1114 (1,12) |
| 1120 (2,12) | 1121 (2,11) | 1122 (4,8) | 1123 (5,7) | 1124 (11,12) |
| 1130 (2,12) | 1131 (2,11) | 1132 (* 13) | 1133 (11,12) | 1134 (6,7) |
| 1140 (6,8) | 1141 (5,9) | 1142 (11,12) | 1143 (12,13) | 1144 (11,13) |

1101: 0001, 0010, 0100, 0111, 0123, 0134, 0101, 0140, 0133, 0122
1110: 0001, 0010, 0100, 0111, 0123, 0134, 0110, 0104, 0142, 0131, 0014
1132: 0001, 0010, 0100, 0111, 0123, 0134, 0132, 0121, 0114, 0103, 0012,
0011
1200 (3, 7) 1201 (4, 10) 1202 (5, 8) 1203 (8, 13) 1204 (* 14)
1210 (3, 12) 1211 (3, 8) 1212 (4, 11) 1213 (6, 7) 1214 (5, 9)
1220 (5, 10) 1221 (4, 12) 1222 (4, 7) 1223 (3, 9) 1224 (6, 8)
1230 (6, 11) 1231 (6, 9) 1232 (3, 13) 1233 (4, 8) 1234 (3, 10)
1240 (4, 9) 1241 (5, 7) 1242 (6, 10) 1243 (4, 13) 1244 (6, 12)

1204 : 0001, 0010, 0100, 0111, 0123, 0134, 0102, 0124, 0143, 0110, 0103, 0144, 0122

1300 (3, 7) 1301 (4, 9) 1302 (11, 14) 1303 (6, 8) 1304 (4, 13)
1310 (6, 9) 1311 (3, 8) 1312 (4, 10) 1313 (8, 12) 1314 (5, 7)
1320 (5, 8) 1321 (6, 10) 1322 (10, 12) 1323 (3, 9) 1324 (8, 13)
1330 (7, 12) 1331 (8, 11) 1332 (5, 9) 1333 (4, 7) 1334 (3, 10)
1340 (10, 11) 1341 (7, 13) 1342 (6, 7) 1343 (5, 10) 1344 (4, 8)

1400 (3, 7) 1401 (3, 11) 1402 (6, 12) 1403 (10, 12) 1404 (7, 11)
1410 (5, 11) 1411 (3, 8) 1412 (4, 9) 1413 (* 15) 1414 (9, 13)
1420 (* 16) 1421 (6, 7) 1422 (1, 16) 1423 (3, 9) 1424 (5, 12)
1430 (9, 14) 1431 (9, 12) 1432 (5, 7) 1433 (2, 15) 1434 (3, 10)
1440 (9, 11) 1441 (5, 13) 1442 (8, 14) 1443 (5, 8) 1444 (4, 7)

1413 : 0001, 0010, 0100, 0111, 0123, 0134, 0142, 0103, 0110, 0121, 0124, 0101, 0112, 0132

1420 : 0001, 0010, 0100, 0111, 0123, 0134, 0130, 0141, 0103, 0114, 0143, 0120, 0131, 0113, 0012

We now have the solution for the parameter set (5, 3, 4) with $N(5, 3, 4) = 16$.

Continuing this procedure, we get a solution for $(s, t, k) = (5, 3, 5)$ with $N(5, 3, 5) = 44$ by adding the following 28 row vectors to the solution for $(s, t, k) = (5, 3, 4)$:
and a solution for \((s, t, k) = (5, 3, 6)\) with \(N(5, 3, 6) = 112\) by adding the following 68 row vectors to the solution for \((s, t, k) = (5, 3, 5)\):

\[
\begin{align*}
10000 & 10011 10023 10034 10101 10110 10132 10204 10413 10420 \\
11001 & 11010 11032 11102 11113 11120 11131 11200 11212 11221 \\
12121 & 12224 12333 12434 13313 13444 14234 14321 \\
\end{align*}
\]

The calculations which give the above results are long and tedious, so we omit the details.

Solving the case \(t = 4\) is similar. Based on the starting point

\[
\begin{pmatrix}
\xi_1 \\
\xi_2 \\
\xi_3 \\
\xi_4 \\
\xi_5 \\
\xi_6 \\
\end{pmatrix} = \begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 \\
\end{pmatrix},
\]

we get a solution for \((s, t, k) = (5,4,5)\) with \(N(5,4,5) = 11\), by adding the following five vectors to the solution for \((s, t, k) = (5, 4, 4)\):

\[
\begin{align*}
10000 & 10112 10233 11013 11130 \\
\end{align*}
\]
and a solution for \((s, t, k) = (5, 4, 6)\) with \(N(5, 4, 6) = 21\), by adding the following 10 vectors to the solution for \((s, t, k) = (5, 4, 5)\):

\[
\begin{align*}
100000 & \\
100113 & \\
100232 & \\
101022 & \\
101304 & \\
110043 & \\
110124 & \\
111420 & \\
113223 & \\
124322 & 
\end{align*}
\]

4. The Search Procedure

Working on parameter set \((s, t, t)\), as we saw in the example \((7, 6, 6)\) the removing procedure is very effective at first, but near the end it becomes time consuming. The number of vectors which should be removed (those in the row spaces generated by \((t - 1)\) vectors in the solution list) increases very rapidly, but the remaining list becomes smaller and smaller, so the rate of true removing decreases significantly.

In this section we propose another method called Search Procedure, to replace the removing procedure after the latter performs to a certain step. The idea is very simple. When the remaining list becomes small in number, we do not generate all vectors to be removed (because most of them have already been removed). Instead we just check vectors in the remaining list as to whether they should be removed or not, one by one (in lexicographic order). Let us try to get a solution for the parameter set \((11, 10, 10)\). Similar to solving the case \((7, 6, 6)\), we need not list all related row vectors (about \(1.1 \times 10^{10}\) in number). Instead, remove all vectors with 0 components, with two components having the same value, and the remaining list has only \(9! = 362880\) vectors. We go even one step further: remove vectors
which differ from \((1,2,3,4,5,6,7,8,9,10)\) only in one component, and then the
number reduces to 93816, still quite large. We start to use the Search Procedure
at this stage. Instead of generating all 9-dimensional row spaces from \(\xi\), we only
generate two 2-dimensional row spaces from \((\xi_{10}, \xi_{12})\) and \((\xi_{11}, \xi_{12})\) and list the
essential vectors in lexicographical order as follows.

\[
\begin{array}{cccccccccc}
1 & 0 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 \\
1 & 1 & 7 & 2 & 8 & 3 & 9 & 4 & 10 & 5 \\
1 & 3 & 5 & 7 & 9 & 0 & 2 & 4 & 6 & 8 \\
1 & 3 & 10 & 6 & 2 & 9 & 5 & 1 & 8 & 4 \\
1 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & 9 \\
1 & 4 & 7 & 10 & 2 & 5 & 8 & 0 & 3 & 6 \\
1 & 5 & 2 & 10 & 7 & 4 & 1 & 9 & 6 & 3 \\
1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 & 0 & 4 \\
1 & 6 & 0 & 5 & 10 & 4 & 9 & 3 & 8 & 2 \\
1 & 6 & 9 & 1 & 4 & 7 & 10 & 2 & 5 & 8 \\
1 & 7 & 2 & 8 & 3 & 9 & 4 & 10 & 5 & 0 \\
1 & 7 & 5 & 3 & 1 & 10 & 8 & 6 & 4 & 2 \\
1 & 8 & 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 \\
1 & 8 & 4 & 0 & 7 & 3 & 10 & 6 & 2 & 9 \\
1 & 9 & 6 & 3 & 0 & 8 & 5 & 2 & 10 & 7 \\
1 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
1 & 10 & 4 & 9 & 3 & 8 & 2 & 7 & 1 & 6 \\
1 & 10 & 8 & 6 & 4 & 2 & 0 & 9 & 7 & 5 \\
\end{array}
\]

If a vector differs from any row vector of the above list at most in seven com-
ponents, or in other words, has at least three components coinciding with some
vectors from the above list, it should be removed. But vectors in the remaining
list must have the first two components coinciding with some vector of the above
list, so the search procedure checks vectors in the remaining list to see if a third
coinciding component exists. Let us see a few examples, first a vector starting
with \(1 6 2 9\cdots\). If such a vector is a new member of the \(\xi\) list, its last six components should completely differ from those in the following six vectors:

\[
\begin{align*}
1 & 6 0 5 10 4 9 3 8 2 \\
1 & 6 9 1 4 7 10 2 5 8 \\
1 & 5 2 10 7 4 1 9 6 3 \\
1 & 7 2 8 3 9 4 10 5 0 \\
1 & 0 10 9 8 7 6 5 4 3 \\
1 & 10 4 9 3 8 2 7 1 6 \\
\end{align*}
\]

But we know, the last nine components of such a vector is a permutation of 2 to 10 and each value is different from its position (differ from 1 2 3 4 5 6 7 8 9 10 exactly in nine components), so no value is available for the component 5: it cannot be the position number 5, cannot be 6 2 9 which are located in position 234, and cannot be 3 4 7 8 10 which are values of the position 5 of the above six vectors. So we conclude that all vectors starting with 1 6 2 9\cdots in the remaining list must be removed. Similarly, a vector staring with 1 6 4 3\cdots or 1 6 7 9\cdots must be removed because their last six components cannot completely differ from one the following six vectors respectively (no value is available for the component 7 or 5).

\[
\begin{align*}
1 & 6 0 5 10 4 9 3 8 2 \\
1 & 6 9 1 4 7 10 2 5 8 \\
1 & 8 4 0 7 3 10 6 2 9 \\
1 & 10 4 9 3 8 2 7 1 6 \\
1 & 9 6 3 0 8 5 2 10 7 \\
1 & 7 5 3 1 10 8 6 4 2 \\
\end{align*}
\]

In fact any vector in the remaining list will be removed in this way, though sometimes we need to check more than 4 components to reach the same conclusion.

The advantage of the search procedure at this step is clear: using the removing
procedure, we need to generate 72 9-dimensional subspaces (about \(72 \times 11^7\) row vectors) to remove the remaining 93816 vectors; while using the search procedure, a few lines of argument may remove hundreds of vectors from the remaining list. The idea applies in solving general parameter sets \((s, t, k)\) as well, and for the special case of \(k = t\), it suggests the following conjecture.

**Conjecture** \(N(s, s - 1, s - 1) = s + 1\) for all prime \(s \geq 5, \xi_j = e_j\) for \(1 \leq j \leq s - 1\), and \(\xi_s = (1, 1, \ldots, 1), \xi_{s+1} = (1, 2, \ldots, s - 1)\) give a solution.

5. The Solution for \(s = t = 3\)

**Theorem 5.1** \(N(3, 3, k) = 2^{k-1}\). A solution consists of all row vectors in \(\{0, 1\}^k\) with odd weight.

**Proof** There are \(2^k\) row vectors in \(\{0, 1\}^k\), and half of them with odd weight (due to the combinatorial equality: \(\binom{k}{2i-1} = \binom{k-1}{2i-2} + \binom{k-1}{2i-1}\), we have \(\sum_{i=1}^{\lfloor \frac{k+1}{2} \rfloor} \binom{k}{2i-1} = \sum_{j=0}^{k-1} \binom{k-1}{j} = 2^{k-1}\)). We need to prove: (i) The \(2^{k-1} \times k\) matrix consisting of all row vectors in \(\{0, 1\}^k\) with odd weight has property \(P_3\) regarded as a matrix on \(GF(3)\); (ii) Any other row vector in \(\{0, 1, 2\}^k\) is a linear combination of two row vectors from the matrix.

(i) Obviously any two rows are linearly independent, so if \(\xi_{i_1}, \xi_{i_2}, \xi_{i_3}\) are distinct row vectors from the matrix, then \(\alpha \xi_{i_1} + \beta \xi_{i_2} + \gamma \xi_{i_3} = 0\) implies \((\alpha, \beta, \gamma) \in \{1, 2\}^3\). But \(\alpha = \beta = \gamma = 1\) or \(\alpha = \beta = \gamma = 2\) are impossible since both imply \(\xi_{i_1} = \xi_{i_2} = \xi_{i_3}\). Consider \((\alpha, \beta, \gamma) = (1, 1, 2), \xi_{i_1} + \xi_{i_2}\) is a vector
in \( \{0, 1, 2\}^k \) such that the number of component 1 is even, but the number of component 2 in \( 2\xi_{i_3} \) is odd, so some component of \( \xi_{i_1} + \xi_{i_2} + 2\xi_{i_3} \) is 1, and hence \( \xi_{i_1} + \xi_{i_2} + 2\xi_{i_3} = 0 \) is impossible. This argument works for \( (\alpha, \beta, \gamma) = (1, 2, 1) \) and \( (\alpha, \beta, \gamma) = (2, 1, 1) \), and also for \( (\alpha, \beta, \gamma) = (2, 2, 1) \), \( (\alpha, \beta, \gamma) = (2, 1, 2) \), and \( (\alpha, \beta, \gamma) = (1, 2, 2) \) because

\[
\alpha\xi_{i_1} + \beta\xi_{i_2} + \gamma\xi_{i_3} = 0 \iff (3-\alpha)\xi_{i_1} + (3-\beta)\xi_{i_2} + (3-\gamma)\xi_{i_3} = 0.
\]

Therefore \( \xi_{i_1}, \xi_{i_2}, \xi_{i_3} \) are linear independent, and property \( P_3 \) holds.

(ii) If \( \xi \in \{0, 1\}^k \) is not a row vector in the matrix, then the number of component 1 must be even. In the following argument, we use \( e_j \) to denote the row vector in \( \{0, 1\}^k \) whose only component 1 is located at the position \( j \).

Suppose \( j \) is the position of the first component 1 of \( \xi \), let \( \xi_{i_1} = e_j, \xi_{i_2} = \xi - e_j \), then both \( \xi_{i_1} \) and \( \xi_{i_2} \) are row vectors of the matrix, and

\[
\xi = \xi_{i_1} + \xi_{i_2}.
\]

Otherwise, \( \xi \) contains some component 2, and we may normalize the row vector so that the first non-zero component is equal to 1, so the number of component 1 is not zero. Now let \( \alpha > 0, \beta > 0 \) be the number of component 1 and the number of component 2 respectively, and suppose that \( k_1, k_2, \ldots, k_\alpha \) are the positions of component 1; \( l_1, l_2, \ldots, l_\beta \) are the positions of component 2. We have the following 4 different cases.
Case 1. Both $\alpha$ and $\beta$ are odd. Let $\xi_{i_1} = \sum_{q=1}^{\alpha} e_{k_q}$, $\xi_{i_2} = \sum_{r=1}^{\beta} e_{i_r}$, then both $\xi_{i_1}$ and $\xi_{i_2}$ are row vectors of the matrix, and $\xi = \xi_{i_1} + 2\xi_{i_2}$.

Case 2. $\alpha$ is odd but $\beta$ is even. Let $\xi_{i_1} = \sum_{q=1}^{\alpha} e_{k_q} + \sum_{r=1}^{\beta} e_{i_r}$, $\xi_{i_2} = \sum_{q=1}^{\alpha} e_{k_q}$, then both $\xi_{i_1}$ and $\xi_{i_2}$ are row vectors of the matrix, and $\xi = 2\xi_{i_1} + 2\xi_{i_2}$.

Case 3. $\alpha$ is even but $\beta$ is odd. Let $\xi_{i_1} = \sum_{q=1}^{\alpha} e_{k_q} + \sum_{r=1}^{\beta} e_{i_r}$, $\xi_{i_2} = \sum_{r=1}^{\beta} e_{i_r}$, then both $\xi_{i_1}$ and $\xi_{i_2}$ are row vectors of the matrix, and $\xi = \xi_{i_1} + \xi_{i_2}$.

Case 4. Both $\alpha$ and $\beta$ are even. Let $\xi_{i_1} = \sum_{q=1}^{\alpha} e_{k_q} + \sum_{r=1}^{\beta} e_{i_r}$, $\xi_{i_2} = \sum_{q=2}^{\alpha} e_{k_q} + \sum_{r=1}^{\beta} e_{i_r}$, then both $\xi_{i_1}$ and $\xi_{i_2}$ are row vectors of the matrix, and $\xi = \xi_{i_1} + \xi_{i_2}$.$\square$

Acknowledgement.

This research was supported by NSF (U.S.A.) Grant DMS 9504561 and NSERC (Canada) Grant OGP 0006051.

References


