BULL. AUSTRAL. MATH. SOC. 15A33, 12C15
VOL. 37 (1988) [333–335]

SINGLETON ARRAYS IN CODING THEORY

TATSUYA MARUTA, ISAO KIKUMASA AND HITOSHI KANETA

We construct all Singleton arrays for the field $GF(q)$ when q is odd. There exist $\varphi(q-1)$ arrays in this case.

INTRODUCTION

Let $GF(q)$ be the finite field of q elements, and let $S_q (q \geqslant 3)$ denote the triangular array

$$\begin{array}{cccccccc}
1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\
1 & a_1 & a_2 & a_3 & \dots & a_{q-3} & a_{q-2} & \\
1 & a_2 & a_3 & \cdot & \dots & a_{q-2} & & \\
1 & a_3 & \cdot & \cdot & \dots & & & \\
\cdot & \cdot & \cdot & \cdot & \dots & & & \\
1 & a_{q-3} & a_{q-2} & & & & & \\
1 & a_{q-2} & & & & & & \\
1 & & & & & & &
\end{array}$$

where $a_i \in GF(q)$. We call S_q a Singleton array if every square submatrix is nonsingular. See [**2**, p.322] for the relation between Singleton arrays and MDS codes. Singleton arrays exist:

THEOREM 1. [**3**]. *Let ξ be a primitive element of $GF(q)$. Then the above S_q with $a_i = 1/(1-\xi^i)$ $(1 \leqslant i \leqslant q-2)$ is a Singleton array.*

We note that Theorem 1 is an easy consequence of Lemma 4 in the next section. In this paper we shall prove the converse:

THEOREM 2. *If the above S_q is a Singleton array, then $a_i = 1/(1-\xi^i)$ for some primitive element ξ of $GF(q)$, provided q is odd.*

To our regret, the case $q = 2^h$ is still open.

Received 14 July 1987

PROOF OF THEOREM 2

A set K of k points of the projective plane $PG(2,GF(q))$ (or $PG(2,q)$ for simplicity) is called a k-arc if no three points of K are collinear. It is well-known that $\max\{k;\ \text{a } k\text{-arc exists}\}$ is equal to $q+1$ or $q+2$ according as q is odd or even [**1**, p.164]. A k-arc with maximal k is called an oval. We refer to [**1**, p.168] for the proof of the following celebrated theorem.

THEOREM 3 (SEGRE). *Let q be odd. Then an oval K of $PG(2,q)$ admits a projective transformation T such that $T(K) = \{{}^t(x_0,x_1,x_2);\ x_0x_1+x_1x_2+x_2x_0 = 0\}$ and that $TP_1 = {}^t(1,0,0)$, $TP_2 = {}^t(0,1,0)$ and $TP_3 = {}^t(0,0,1)$ for three prescribed points of K.*

Denote by $S_{m,n}(q)$ the set of (m,n)-matrices with $GF(q)$ entries such that every square submatrix is nonsingular. An (m,n)-matrix (a_{ij}) is called a Cauchy matrix if $a_{ij} = 1/(1-x_iy_j)$ for some x_i, y_j in $GF(q)$ (for $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$) with $x_iy_j \neq 1$. As to the determinant of a Cauchy matrix we have [**4**, p.202]

LEMMA 4. (Cauchy). *The determinant of a square Cauchy matrix is given by the formula*

$$\deg\left(1/(1-x_iy_j)\right) = D(x_1,\dots,x_n)D(y_1,\dots,y_n)/\prod_{i=1}^{n}\prod_{j=1}^{n}(1-x_iy_j),$$

where $D(x_1,\dots,x_n) = \prod_{1\leqslant i<j\leqslant n}(x_i-x_j)$.

COROLLARY TO THEOREM 3. *Assume that q is odd. If the matrix*

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & a_1 & a_2 & \dots & a_{q-3} \\ 1 & b_1 & b_2 & \dots & b_{q-3} \end{pmatrix}$$

belongs to $S_{3,q-2}(q)$, then A is a Cauchy matrix with $a_i, b_i \in GF(q)-\{0,1\}$ ($1 \leqslant i \leqslant q-3$).

PROOF OF COROLLARY: It is evident that a_i and b_i are equal to neither 0 nor 1. Let a $(3,3)$-matrix E_3 be the unit matrix. Then $q+1$ columns of the $(3,q+1)$-matrix (E_3,A) make up an oval of $PG(2,q)$. In view of Theorem 3 there exists a diagonal $(3,3)$-matrix $[1,d_1,d_2]$ ($d_i \neq 0$) such that the set of columns of $[1,d_1,d_2](E_3,A)$ is equal to $\{{}^t(x_0,x_1,x_2);\ x_0x_1+x_1x_2+x_2x_0 = 0\}$ as a subset of $PG(2,q)$. Thus the set of columns of $[1,d_1,d_2]A$ coincides with the set of columns of the $(3,q-2)$-matrix

$$B = \begin{pmatrix} 1 & 1 & \dots & 1 \\ -\xi & -\xi^2 & \dots & -\xi^{q-2} \\ -1/(1-\xi^{-1}) & -1/(1-\xi^{-2}) & \dots & -1/(1-\xi^{-q+2}) \end{pmatrix}$$

as a subset of $PG(2,q)$, where ξ is a primitive element of $GF(q)$. Hence $d_1 = -\xi^k$ and $d_2 = -1(1-\xi^{-k})$ for some $1 \leqslant k \leqslant q-2$. We shall show that $B' = [1, d_1, d_2]^{-1} B$ is a Cauchy matrix. Then it follows that A is a Cauchy matrix, since B' is equal to A up to the order of columns. Let ${}^t(1, 1/(1-u_i), 1/(1-v_i))$ be the i-th column of the matrix B'. For $1 \leqslant i < j \leqslant q-2$ and $i, j \neq k$ we have $u_i v_i u_j v_j \neq 0$. Furthermore, $u_i v_j - u_j v_i$ vanishes, because it equals

$$(1-\eta^{i-k})(1-(1-\eta^j)/(1-\eta^k)) - (1-\eta^{j-k})(1-(1-\eta^i)/(1-\eta^k))$$

where $\eta = \xi^{-1}$. Thus B' is a Cauchy matrix, as desired.

PROOF OF THEOREM 2: Let

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & a_1 & a_2 & \dots & a_{q-3} \\ 1 & a_2 & a_3 & \dots & a_{q-2} \end{pmatrix}$$

be a submatrix of a Singleton array S_q. Then the matrix A belongs to $S_{3,q-2}(q)$. We can write $a_i = 1/(1-\xi^{n_i})$ ($1 \leqslant n_i \leqslant q-2, 1 \leqslant i \leqslant q-2$). Since A is a Cauchy matrix by the Corollary, so are the submatrices

$$\begin{pmatrix} a_{i-1} & a_i \\ a_i & a_{i+1} \end{pmatrix} \qquad (2 \leqslant i \leqslant q-3).$$

Consequently we get $n_{i-1} + n_{i+1} = 2n_i \bmod (q-1)$ ($2 \leqslant i \leqslant q-3$). In other words we have $n_{i+1} - n_i = n_i - n_{i-1} \bmod (q-1)$. Hence there exist integers $0 \leqslant n', d < q-1$ such that $n_i = n' + di \bmod (q-1)$ ($1 \leqslant i \leqslant q-2$). Since $\{n' + di;\ 1 \leqslant i \leqslant q-2\} = \{1, 2, \dots q-2\}$ in $\mathbb{Z}/(q-1)$, the set $\{di;\ 1 \leqslant i \leqslant q-2\}$ must contain $q-2$ elements. It now follows that $(d, q-1) = 1$ and $n' = 0$. Thus $a_i = 1/(1-\gamma^i)$, where $\gamma = \xi^d$ is a primitive element of $GF(q)$. This completes the proof of Theorem 2.

REFERENCES

[1] J.W.P. Hirschfeld, *Projective Geometry over Finite Fields* (Oxford University Press, 1979).

[2] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes* (North-Holland Amsterdam, 1977).

[3] R.M. Roth and G. Seroussi, 'On generator matrices of MDS codes', *IEEE Trans. Inform. Theor.* IT-31 (1985), 826–830.

[4] H. Weyl, *The Classical Groups* (Princeton University Press, 1946).

Department of Mathematics
Faculty of Science
Okayama University
Okayama 700
JAPAN

https://doi.org/10.1017/S0004972700026940 Published online by Cambridge University Press