J. Sci. Hiroshima Univ. Ser. A-I
31 (1967), 191-194

A Note on the Cyclical Generation of Disjoint Spreads

Noboru Hamada and Teijiro Fukuda

(Received September 20, 1967)

1. It is unknown whether the BIB design PG$(t=2n-1, 2)$: 1 obtained by choosing the points in PG$(t, 2)$ as treatments and all lines as blocks is resolvable or not for $t\geq 5$. C. R. Rao [1], [2] showed that the BIB design PG$(t=3, 2)$: 1 with parameters $v=15$, $b=35$, $k=3$, $r=7$, $\lambda=1$ was resolvable by decomposing all lines in PG(3, 2) into 7 disjoint 1-fold spreads*) S_0, S_1, $\cdots$, S_6. The procedure of constructing these spreads is as follows:

(1) A set S_0 consisting of 5 lines cyclically generated from the initial line $L(x^0, x^5, x^{10})$ of the minimum cycle $\theta=5$ is chosen as the initial 1-fold spread.

(2) Generate S_{j+1} cyclically by a transformation $\sigma(S_j)=S_{j+1}$ $(j=0, 1, \cdots, 5)$ where σ is a nonsingular linear transformation in PG(3, 2) such that

$$\sigma:\quad \begin{array}{lll} (x^{\alpha})=((\varepsilon, y^{p})) \longrightarrow (x^{\beta})=((\varepsilon, y^{p+1})) & & (p=0, 1, \cdots, 5) \\ (x^{3})=((1, 0, 0, 0)) \longrightarrow (x^{3})=((1, 0, 0, 0)) & & \text{(invariant)}. \end{array}$$

He conjectured that, in general, all lines in PG$(t, 2)$ would be decomposed into disjoint 1-fold spreads by the similar method. The purpose of this note is to show that it is impossible to decompose all lines in PG$(t, 2)$ into disjoint 1-fold spreads for all t greater than 3 by such a procedure.

2. Let x be a primitive element of GF(2^{t+1}), then every nonzero element of GF(2^{t+1}) can be represented either as a power of x or a polynomial of degree less than $t+1$ over GF(2) mod $f(x)$ where $f(x)$ is the minimum function of GF(2^{t+1}) which determines x. If

$$x^{\alpha}\equiv\varepsilon x^{t}+a_{t-1}x^{t-1}+\cdots+a_1x+a_0 \qquad (\bmod f(x)) \tag{2.1}$$

then, the correspondence x^{α} and an ordered set $(\varepsilon, a_{t-1}, \cdots, a_1, a_0)$ of elements of GF(2) is unique.

Let y be a primitive element of GF(2^t). When $(a_{t-1}, \cdots, a_1, a_0)\neq(0, \cdots, 0, 0)$ in (2.1), there exists an integer p such that the element of GF(2^t) corresponding to the ordered set $(a_{t-1}, \cdots, a_1, a_0)$ is represented as y^p, i.e.,

$$y^{p}\equiv a_{t-1}y^{t-1}+\cdots+a_1y+a_0 \qquad (\bmod g(y)) \tag{2.2}$$

---

*) A μ-fold spread S in a projective geometry $\sum$ is defined by Rao [2] as a set of linear subspaces (flats) of a given dimension such that each point of $\sum$ is contained in exactly μ members of S.

where $g(y)$ is the minimum function of $GF(2^t)$ which determines y.

We denote the element of $GF(2^{t+1})$ corresponding to the ordered set $(\varepsilon, a_{t-1}, \cdots, a_1, a_0)$ as x^α or (ε, y^p) and represent formally these correspondences as

$$x^\alpha = (\varepsilon, a_{t-1}, \cdots, a_1, a_0) = (\varepsilon, y^p). \tag{2.3}$$

It is known that the following linear transformation in $PG(t, 2)$ is non-singular [1], [2].

$$\sigma: \begin{array}{ll} (x^\alpha) = ((\varepsilon, y^p)) \longrightarrow (x^\beta) = ((\varepsilon, y^{p+1})) & (p=0, 1, \cdots, 2^t-3) \\ (x^t) = ((1, 0, \cdots, 0)) \longrightarrow (x^t) = ((1, 0, \cdots, 0)) & \text{(invariant)} \end{array} \tag{2.4}$$

where (x^α), $((\varepsilon, y^p))$ and $((\varepsilon, a_{t-1}, \cdots, a_1, a_0))$ are points in $PG(t, 2)$ corresponding to the elements x^α, (ε, y^p) and $(\varepsilon, a_{t-1}, \cdots, a_1, a_0)$ of $GF(2^{t+1})$, respectively.

(i) The case of $t=2n-1$ and $n \geq 3$

Let $L(x^\alpha, x^\beta, x^\gamma)$ be the line in $PG(t=2n-1, 2)$ passing through a pair of points (x^α) and (x^β) where $(x^\gamma)=(x^\alpha+x^\beta)$, and let S_0 be the initial 1-fold spread consisting of θ lines which are cyclically generated from the initial line $L(x^0, x^\theta, x^{2\theta})$ of the minimum cycle $\theta=(2^{2n}-1)/(2^2-1)$, i.e.,

$$S_0 = \{L(x^\lambda, x^{\theta+\lambda}, x^{2\theta+\lambda}) : \lambda=0, 1, \cdots, \theta-1\}. \tag{2.5}$$

The other spreads $S_1, S_2, \cdots$ are obtained by repeating the transformation σ to the initial spread S_0, i.e., $S_{j+1}=\sigma(S_j)$ $(j=0, 1, \cdots, 2^{2n-1}-3)$. The notation $P(\varepsilon_1, \varepsilon_2)$ is used as a set of points having the first component ε_1 and the second component ε_2, i.e.,

$$P(\varepsilon_1, \varepsilon_2) = \{(x^\alpha) : x^\alpha = (\varepsilon_1, \varepsilon_2, a_{2n-3}, \cdots, a_1, a_0)\}. \tag{2.6}$$

Lemma 1. *If there exists a line* $L(x^\alpha, x^{\theta+\alpha}, x^{2\theta+\alpha})$ *such that* 3 *points* (x^α), $(x^{\theta+\alpha})$ *and* $(x^{2\theta+\alpha})$ *on the line belong simultaneously to the set* $P(0, 0)$, *then the line* $L(x^{\alpha+1}, x^{\theta+\alpha+1}, x^{2\theta+\alpha+1})$ *is not only in the initial spread* S_0 *but also in the spread* $S_1=\sigma(S_0)$.

Proof. Since it is evident that the line $L(x^{(\alpha+1)}, x^{\theta+(\alpha+1)}, x^{2\theta+(\alpha+1)})$ belongs to S_0, we show that the line belongs also to S_1.

By the assumption, we can denote the point $(x^{j\theta+\alpha})$ as

$$(x^{j\theta+\alpha}) = ((0, 0, a_{2n-3}^{(j)}, \cdots, a_1^{(j)}, a_0^{(j)})) \qquad (j=0, 1, 2). \tag{2.7}$$

Let the element of $GF(2^{2n-1})$ corresponding to the ordered set $(0, a_{2n-3}^{(j)}, \cdots, a_1^{(j)}, a_0^{(j)})$ be y^{p_j}. Thus we have

$$(x^{j\theta+\alpha}) = ((0, 0, a_{2n-3}^{(j)}, \cdots, a_1^{(j)}, a_0^{(j)})) = ((0, y^{p_j})) \qquad (j=0, 1, 2). \tag{2.8}$$

The point $((0, y^{p_j})) = ((0, 0, a_{2n-3}^{(j)}, \cdots, a_1^{(j)}, a_0^{(j)}))$ is transformed to $((0, y^{p_j+1})) = ((0, a_{2n-3}^{(j)}, \cdots, a_1^{(j)}, a_0^{(j)}, 0))$ by the mapping σ and the line consisting of these three points $((0,\ y^{p_j+1}))$ $(j=0, 1, 2)$ belongs to S_1. On the other hand, the point in PG$(2n-1, 2)$ corresponding to the ordered set $(0, a^{(j)}_{2n-3}, \cdots, a^{(j)}_1, a^{(j)}_0, 0)$ is $(x^{(j\theta+\alpha)+1})$ for any primitive element x. These considerations show that the line $\mathrm{L}(x^{\alpha+1}, x^{\theta+\alpha+1}, x^{2\theta+\alpha+1})$ belongs also to S_1.

Lemma 2. *If $n\geq 3$, there exists at least one line $\mathrm{L}(x^{\alpha}, x^{\theta+\alpha}, x^{2\theta+\alpha})$ in S_0 such that 3 points (x^{α}), $(x^{\theta+\alpha})$ and $(x^{2\theta+\alpha})$ on the line belong simultaneously to the set* P(0, 0).

Proof. If (x^{α}) and $(x^{\theta+\alpha})$ belong to P(0, 0), then $(x^{2\theta+\alpha})=(x^{\alpha}+x^{\theta+\alpha})$ also belongs to P(0, 0). It is, therefore, sufficient to show that if $n\geq 3$, then there exists at least one pair of points (x^{α}) and $(x^{\theta+\alpha})$ such that these two points belong simultaneously to the set P(0, 0).

Since for all i such that $0\leq i\leq 2n-3$, the point (x^{i}) belongs to P(0, 0), the following two cases can occur.

(1) The case where there exists at least one point (x^{i}) such that $(x^{\theta+i})$ belongs also to P(0, 0).

In this case, our lemma holds.

(2) The case where the point $(x^{i+\theta})$ does not belong to P(0, 0) for all i $(0\leq i\leq 2n-3)$.

In this case, any point of $2n-2$ points $(x^{i+\theta})$ $(0\leq i\leq 2n-3)$ must belong to any one of 3 sets P(0, 1), P(1, 0) and P(1, 1). Since inequality $2n-2\geq 4$ is valid by the assumption $n\geq 3$, there exist at least two points (x^{i_1}) and (x^{i_2}) $(0\leq i_1, i_2\leq 2n-3)$ such that two points $(x^{i_1+\theta})$ and $(x^{i_2+\theta})$ belong simultaneously to a set $\mathrm{P}(\varepsilon_1, \varepsilon_2)$ of these 3 sets, i.e.,

$$(x^{i_j+\theta})=((\varepsilon_1, \varepsilon_2, b^{(j)}_{2n-3}, \cdots, b^{(j)}_1, b^{(j)}_0)) \qquad (j=1, 2) \tag{2.9}$$

Let $(x^{\alpha})=(x^{i_1}+x^{i_2})$, then (x^{α}) belongs to P(0,0) and $(x^{\alpha+\theta})=(x^{i_1+\theta}+x^{i_2+\theta})$ also belongs to P(0, 0) from (2. 9). This completes the proof.

Lemma 1 and lemma 2 show that two spreads S_0 and S_1 are not disjoint for any $t=2n-1$ $(n\geq 3)$. Hence it is impossible to decompose all lines in PG$(2n-1, 2)$ into disjoint 1-fold spreads except for $n=2$ by the Rao's method. Our results, however, do not necessarily imply that the design PG$(2n-1, 2)$: 1 is not resolvable.

(ii) The case of $t=2n$

Since $v/k=(2^{2n+1}-1)/(2^2-1)$ is not integral in this case, the design PG$(2n, 2)$: 1 is not resolvable. It is, however, known that all lines in PG$(2n, 2)$ have the minimum cycle $v=2^{2n+1}-1$ and are decomposed into η disjoint 3-fold spreads where $\eta=(2^{2n}-1)/(2^2-1)$ is the number of initial lines in PG$(2n, 2)$ [3].

References

[1] Rao, C. R. (1946). Difference sets and combinatorial arrangements derivable from finite geometries. *Proc. Nat. Inst. Sci. India* **12** 123–135.

[2] Rao, C. R. (1966). Cyclical generation of linear subspaces in finite geometries. *Tech. Report* No. 31/66, *Research and Training School*, *Indian Statist. Inst.* (Presented at Chapel Hill Symposium on Combinatorial Mathematics, April, 1967.)

[3] Yamamoto, S., Fukuda, T. and Hamada, N. (1966). On finite geometries and cyclically generated incomplete block designs. *J. Sci. Hiroshima Univ. Ser.* A-1 **30** 137–149.

Department of Mathematics,
Faculty of Science,
Hiroshima University
and
Maritime Safety Academy, Kure