Can. J. Math., Vol. XXVI, No. 6, 1974, pp. 1466-1474

AN ARITHMETICAL DIFFERENCE SYSTEM WITH APPLICATION TO B.I.B. DESIGNS

KULENDRA N. MAJINDAR

1. Introduction. In this paper we have established the existence of an arithmetical difference system by a constructive method. Our arithmetical difference systems are a generalization of cyclic difference sets.

Let v, k, h, n, λ be positive integers, $1 < k < v$. By an h-block arithmetical difference system (mod v), with block size k and residue frequency λ, we mean h blocks (i.e. sets) of integers $d_{1t}, d_{2t}, \ldots, d_{kt}$, $t = 1, 2, \ldots h$ such that among the $hk(k-1)$ differences of the form $d_{it} - d_{i't}$ (mod v), $i \neq i'$, $i, i' = 1, 2, \ldots k$, $t = 1, 2 \ldots h$, each non-zero residue class mod v appears λ times (necessarily $\lambda(v-1) = hk(k-1)$). An arithmetical difference set is merely a 1-block arithmetical difference system (equivalently called a cyclic difference set).

These arithmetical difference systems may be called supplementary cyclic difference sets $h - (v, k, \lambda)$ in the terminology of J. Wallis [**4**]. These are also related to the sets of differences discussed by Stanton and Sprott [**5**] and difference families in elementary abelian groups of Wilson [**6**].

If two different blocks $d_{1t}, d_{2t}, \ldots d_{kt}$ and $d_{1t'}, d_{2t'}, \ldots d_{kt'}$ are such that there is an integer i for which the residues $d_{1t'}, d_{2t'}, \ldots d_{kt'}$ (mod v) equal $d_{1t} + i$, $d_{2t} + i$, $\ldots d_{kt} + i$ (mod v) in a certain order, we say that one of the two blocks is a translate of the other and in this case the set of residues $d_{it} - d_{i't}$ (mod v) are the same as the set of residues $d_{it'} - d_{i't'}$ (mod v), $i, i' = 1, 2 \ldots k$ in a certain order. A difference system in which no block is a translate of another is called translate-free.

The main result of this paper is stated in the following theorem.

THEOREM. *If $q = p^m$ is a prime power and n is any even integer $\geqq 4$, then there exists a translate-free h-block arithmetical difference system* (mod v) *with block size k and residue frequency λ where $v = (q^{n+1} - 1)/(q - 1)$, $k = (q^{n-1} - 1)/(q - 1)$, $h = (q^n - 1)/(q^2 - 1)$, $\lambda = (q^{n-2} - 1)(q^{n-1} - 1)/(q^2 - 1)(q - 1)$.*

As an example, taking $q = 2$, $n = 4$, we have a 5-block arithmetical difference system (mod 31) given by

$$[1, 2, 3, 5, 12, 19, 20], [2, 3, 5, 8, 20, 29, 31], [2, 3, 11, 18, 20, 23, 27],$$
$$[1, 8, 12, 18, 20, 23, 31], [1, 2, 8, 19, 23, 27, 29] \text{ with } k = 7, \lambda = 7.$$

The theorem has been applied to construct a series of balanced incomplete

Received May 30, 1973.

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

block designs in the last section. An alternative proof of Singer's Theorem on difference sets has also been given in section 4.

2. Singer's difference set.

In the paper [1] (which inaugurated the interesting topic of difference sets in number and group theories), James Singer proved the following:

SINGER'S THEOREM. *For $q = p^m$ a prime power and any n, there is an arithmetic difference set* (mod v) *with block size k and residue frequency λ where* $v = (q^{n+1} - 1)/(q - 1)$, $k = (q^n - 1)/(q - 1)$, $\lambda = (q^{n-1} - 1)/(q - 1)$.

So far, no purely arithmetical proof of this theorem has been discovered. In this paper we prove Singer's theorem anew by simple arithmetical and algebraical arguments. This new proof led the author to the theorem of section 1.

3. Preliminaries.

Let $F = GF(q)$ be a Galois field where $q = p^m$ is a prime power, $F^* =$ the nonzero elements of F. We extend F to a Galois field $GF(q^{n+1})$ by means of a polynomial of degree $n + 1$ with coefficients in F and irreducible in F in the usual manner. If w is a generator of the multiplicative group of the nonzero elements of $GF(q^{n+1})$, then w satisfies an equation of the form $a_0 + a_1w + a_2w^2 \ldots + a_{n+1}w^{n+1} = 0$, $a_{n+1} \neq 0$, $a_i \in F$ and $w, w^2, w^3, \ldots w^{v(q-1)}$, where

(3.1) $\quad v = (q^{n+1} -1)/(q - 1),$

are all distinct and give the nonzero elements of $GF(q^{n+1})$. If $a_1, a_2, \ldots a_{n+1} \in F$ and not all of them are 0, then there is a unique integer i, $1 \leqq i \leqq v(q - 1)$, such that $a_1 + a_2w + \ldots + a_nw^{n-1} = w^i$. If $c \in F^*$, and $c(a_1 + a_2w \ldots + a_{n-1}w^{n-1}) = w^{i'}$, then $i \equiv i'$ (mod v). Also $w^i \in F^*$ if and only if i is a multiple of v.

Vectors everywhere below have their components in F. The coefficients of any polynomial in w belong to F.

A ν-vector $(a_1, a_2, \ldots a_\nu)$ is said to be equivalent to the vector $(a'_1, a'_2, \ldots a_\nu')$ if and only if $(a_1, a_2 \ldots a_\nu) = c(a'_1, a'_2 \ldots a_\nu')$ for some c in F^*. Clearly this is an equivalence relation.

If S is any vector space of n-vectors and is of rank α, then the $(q^\alpha - 1)$ nonnull vectors of S can be classified by means of the above equivalence relation into $(q^\alpha - 1)/(q - 1)$ equivalence classes C_i. Each class C_i determines uniquely a residue class d_i (mod v), $1 \leqq d_i \leqq v$ by

(3.2) $\quad w^di = a_1 + a_2w + \ldots + a_nw^{n-1}$ with $(a_1, a_2 \ldots a_n) \in C_i$

These $(q^\alpha - 1)/(q - 1)$ distinct integers d_i make up a set to be denoted by $[S]$. Let

(3.3) $\quad U =$ the vector space of all n-vectors,

(3.4) $\quad [U] = [d_1, d_2, \ldots d_k]$ with $k = (q^n - 1)/(q - 1)$.

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

Amongst the $k(k-1)$ differences $d_{i'} - d_i \pmod v$ $d_i, d_{i'} \in [U]$, $d_i \neq d_{i'}$, let there be e distinct residue classes $(\text{mod } v)$ and j, $1 \leqq j \leqq v-1$, be one of the residue classes. So $j = d_{i'} - d_i \pmod v$, $d_{i'} \neq d_i$, and there exist at least one pair of nontrivial polynomials $a_1 + a_2w + \ldots + a_nw^{n-1}$, $b_1 + b_2w + \ldots + b_nw^{n-1}$ connected by $w^j(a_1 + a_2w + \ldots + a_nw^{n-1}) = b_1 + b_2w + \ldots + b_nw^{n-1}$. Till the end of this section, j is fixed.

We now define an important subspace V of U. $(a_1, a_2, \ldots, a_n) \in V$ if and only if there exists a polynomial $b_1 + b_2w + \ldots + b_nw^{n-1}$ such that

$$(3.5) \qquad w^j(a_1 + a_2w + \ldots + a_nw^{n-1}) = b_1 + b_2w + \ldots + b_nw^{n-1}.$$

By the definition of j, V contains non-null vectors. Also if $d \in [V]$ then $j + d \equiv$ some d' of $[U] \pmod v$.

Let W be the collection of n-vectors not belongong to V. Thus $(c_1, c_2, \ldots c_n) \in W$ if and only if

$$(3.6) \qquad w^j(c_1 + c_2w + \ldots + c_nw^{n-1}) = \text{a polynomial in } w \text{ with degree } n.$$

This implies that if $d \in [U]$ but not to $[V]$, then $j + d \not\equiv$ any integer of $[U] \pmod v$.

We show that W is not empty. If W is empty, then all n-vectors belong to V. Using (3.5), we get

$$\prod w^j(a_1 + a_2w + \ldots + a_nw^{n-1}) = \prod (b_1 + b_2w \ldots + b_nw^{n-1})$$

where $(a_1, a_2, \ldots a_n)$, $(b_1, b_2 \ldots b_n)$ run through all non-null n-vectors. By cancellation, we infer that $\Pi w^j = 1$, i.e., $w^{j(q^n-1)} = 1$ which implies $j(q^n - 1)$ is divisible by $q^{n+1} - 1$. But $q^{n+1} - 1 = (q^n - 1)q + q - 1$ so that the greatest common divisor of $q^{n+1} - 1$ and $q^n - 1$ is $q - 1$. So j is divisible by $(q^{n+1} - 1)/(q - 1) = v$ of (3.1), a contradiction.

If $\delta_1, \delta_2 \in W$, then, because of (3.6), a linear combination $c_1\delta_1 + c_2\delta_2$ with $c_1, c_2 \in F^*$, is in V. From this,

$$(3.7) \qquad \text{rank } V = n - 1.$$

Thus $[V]$ consists of a subset of $(q^{n-1} - 1)/(q - 1)$ integers of $[U]$. Moreover $j + d \equiv d' \pmod v$ with $d, d' \in [U]$ holds if and only if $d \in [V]$. So among all the differences $d_i - d_{i'} \pmod v$ $d_i \neq d_{i'}$, $d_i, d_{i'} \in [U]$ the residue class $j \pmod v$ appears $\lambda = (q^{n-1} - 1)/(q - 1)$ times, a number independent of j.

4. Proof of Singer's Theorem. $[U]$ of (3.4) is a difference set $(\text{mod } v)$. For, each of e possible residue sets $(\text{mod } v)$ can be represented as $d - d'$ $(\text{mod } v)$ with $d \neq d'$, $d, d' \in [U]$ in λ possible ways. So $e\lambda = k(k - 1)$ whence $e = v - 1$. In other words, each non-zero residue $(\text{mod } v)$ can be represented as $d - d' \pmod v$ with $d, d' \in [U]$ in λ possible ways. This completes the proof.

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

5. Some vector spaces associated with subspaces of V. U, V, W are as in (3.4), (3.5), (3.6). If S is a collection of ν-vectors and γ is a ν-vector then let $\gamma + S = \{\gamma + s : s \in S\}$. Associated with each nontrivial subspace T (i.e., rank $T > 1$) of V, we define two useful vector spaces T, T'. Let j, $1 \leqq j \leqq v - 1$ be an integer. There exist polynomials $a_1 + a_2w + \ldots + a_nw^{n-1}$ and $b_1 + b_2w + \ldots b_nw^{n-1}$ connected by $w^j(a_1 + a_2w + \ldots + a_nw^{n-1}) = b_1 + b_2w + \ldots + b_nw^{n-1}$ as seen in the proof of Singer's Theorem. Fix j in this section. η everywhere is a non-null n-vector. Let

$$(5.1) \qquad \tilde{T} = \{(b_1, b_2 \ldots b_n) : w^j(a_1 + a_2w + \ldots a_nw^{n-1}) = b_1 + b_2w + \ldots b_nw^{n-1} \text{ with } (a_1, a_2 \ldots a_n) \in T\}.$$

Since T is a subspace of V, $\tilde{T}$ is well defined. Note that $(a_1, a_2 \ldots a_n)$ and the corresponding $(b_1, b_2 \ldots b_n)$ are inequivalent. $\tilde{T}$ is a vector space and

$$(5.2) \qquad \text{rank } \tilde{T} = \text{rank } T.$$

Let

$$(5.3) \qquad T' = \{(a_1, a_2 \ldots a_n, b_1, b_2 \ldots b_n) : w^j(a_1 + a_2w + \ldots a_nw^{n-1}) = b_1 + b_2w + \ldots b_nw^{n-1} \text{ with } (a_1, a_2 \ldots a_n) \in T\}.$$

Note that if $(a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n) \in T'$ then $(a_1, a_2 \ldots a_n)$ is not equivalent to $(b_1, b_2, \ldots b_n)$. Clearly T' is a vector space and

$$(5.4) \qquad \text{rank } T' = \text{rank } T.$$

We establish now a few lemmas relating to $\tilde{T}$ and T'.

LEMMA 1. *If $T = \tilde{T}$ and* rank $T = \alpha \neq 1$ *then* $(\alpha, n + 1)$, *i.e. the greatest common division of α and $n + 1$ is greater than* 1.

Proof. Any vector $(a_1, a_2, \ldots a_n)$ of T uniquely determines a vector $(b_1, b_2, \ldots b_n)$ of $\tilde{T}$ by the relation $w^j(a_1 + a_2w + \ldots + a_nw^{n-1}) = b_1 + b_2w + \ldots + b_nw^{n-1}$. Since $T = \tilde{T}$, as in section 3 we infer that $w^{j(q^\alpha - 1)} = 1$ whence the divisibility of $j(q^\alpha - 1)$ by $q^{n+1} - 1$.

If α divides $n + 1$ the lemma holds. So suppose α does not divide $n + 1$. We now show by the familiar Euclid's algorithm for finding the greatest common divisor that $(q^\alpha - 1, q^{n+1} - 1) = q^h - 1$ where $h = (\alpha, n + 1)$. This result is known. For the sake of completeness, we give the proof.

Let $n + 1 = \alpha t_1 + m_1$, $1 \leqq m_1 < \alpha$. If a, b are integers we know $(a, b) = (a, b - a)$ and $(a, cb) = (a, b)$ if c is relatively prime to a. Thus

$$(q^\alpha - 1, q^{n+1} - 1) = (q^\alpha - 1, q^{n+1} - q^\alpha) = (q^\alpha - 1, q^{n-\alpha+1} - 1) = (q^\alpha - 1, q^{n-\alpha+1} - q^\alpha) = (q^\alpha - 1, q^{n-2\alpha+1} - 1) = \ldots = (q^\alpha - 1, q^{m_1} - 1)$$

If m_1 divides α, then $(\alpha, n + 1) = m_1$ and $(q^\alpha - 1, q^{m_1} - 1) = q^{m_1} - 1$, and the result holds.

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

Suppose m_1 does not divide α, and $\alpha = m_1 t_2 + m_2$, $1 \leqq m_2 < m_1$, then, as before $(q^\alpha - 1, q^{m_1} - 1) = (q^{m_2} - 1, q^{m_1} - 1)$. Proceeding thus, we see that $(q^\alpha - 1, q^{n+1} - 1) = q^h - 1$.

As $q^{n+1} - 1$ divides $j(q^\alpha - 1)$, it follows that j is divisible by $(q^{n+1} - 1)/(q^h - 1)$. If $h = 1$, j would be divisible by $(q^{n+1} - 1)/(q - 1)$, a contradiction. This completes the proof.

COROLLARY 1. *If* rank $T = \alpha$ and $(\alpha, n + 1) = 1$, *then* $\tilde{T}$ *contains at least one vector not belonging to* T.

COROLLARY 2. *If n is even, then $\tilde{V}$ contains at least one vector not belonging to V.* This is because rank $V = n - 1$ and $(n - 1, n + 1) = (n - 1, 2) = 1$.

If $\eta = (c_1, c_2 \ldots c_n)$ and $\xi = (a_1, a_2 \ldots a_n, b_1, b_2, \ldots b_n)$, we say that one of them is totally or partially orthogonal to the other according as

$$(5.5)\qquad \begin{array}{l} \sum_{i=1}^{n} a_i c_i = 0 = \sum_{i=1}^{n} b_i c_i \quad \text{or} \\ \sum_{i=1}^{n} a_i c_i = 0 \neq \sum_{i=1}^{n} b_i c_i \end{array}$$

For a given n-vector η, let
$U(\eta)$ = the vector space of all n-vectors orthogonal to η,
$V(\eta)$ = the vector space of all vectors in V orthogonal to η,

(5.6) $V^*(\eta)$ = the vector space of all $2n$-vectors in V' totally orthogonal to η(where V' is defined by (5.3) with T replaced by V).

$\xi = (a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n) \in V^*(\eta)$ if and only if

$$(5.7)\qquad (a_1, a_2, \ldots a_n), (b_1, b_2, \ldots b_n) \in U(\eta) \text{ and } w^j(a_1 + a_2 w + \ldots + a_n w^{n-1}) = b_1 + b_2 w + \ldots + b_n w^{n-1}.$$

This implies that

$$(5.8)\qquad j + d_\imath \equiv d_{i'} \pmod{v} \text{ with } d_i, d_{i'} \in [U(\eta)]$$

where $[U(\eta)]$ contains $(q^{n-1} - 1)/(q - 1)$ integers.

Exactly as in the case of Singer's Theorem, we easily establish the following lemma.

LEMMA 2. *Amongst the residue classes* $d_i - d_{i'} \pmod{v}$, $i \neq i'$, $d_i, d_{i'} \in [U(\eta)]$ *the nonzero residue class* $j \pmod{v}$ *appears* $(q^\alpha - 1)/(q - 1)$ *times where* α = rank $V^*(\eta)$.

As rank $V = n - 1$ there is an n-vector, call it specially η_0, such that all vectors orthogonal to it make up V. Note that η_0 depends on j. Easily

$$(5.9)\qquad \begin{aligned} \text{rank } V(\eta) &= n - 1 \text{ if } \eta \text{ is equivalent to } \eta_0, \\ &= n - 2 \text{ if } \eta \text{ is inequivalent to } \eta_0. \end{aligned}$$

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

If ξ, ξ_1, are $2n$-vectors, each partially orthogonal to η, then a suitable combination $c\xi + \xi_1$, $c \in F^*$ is totally orthogonal to η. Consequently the collection $V'(\eta)$ of all partially orthogonal vectors can be expressed as $c\xi + V^*(\eta)$ where ξ is a particular vector, partially orthogonal to η and c varies over F^*. If all $2n$-vectors of V' are totally orthogonal to η, then rank $V^*(\eta) =$ rank $V(\eta)$; otherwise rank $V^*(\eta) =$ rank $V(\eta) - 1$. So

(5.10) rank $V^*(\eta) =$ rank $V(\eta)$ or rank $V(\eta) - 1$.

Thus $V^*(\eta_0) = n - 2$ or $n - 1$. We have the following lemma.

LEMMA 3. *If n is even*, rank $V^*(\eta_0) = n - 2$.

Proof. If possible, let rank $V^*(\eta_0) = n - 1$. As rank $V' = n - 1$ we have $V' = V^*(\eta_0)$. This means all vectors in V are orthogonal to η_0. As rank $\tilde{V} =$ rank $V = n - 1$, we must have $V = \tilde{V}$, contradicting Corollary 2 of Lemma 1, n being even. Hence the lemma.

By (5.10), rank $V^*(\eta)$ can be $n - 3$ or $n - 2$. Call a vector η (inequivalent to η_0) to be of type 1 or type 2 according as rank $V^*(\eta) = n - 3$ or $n - 2$. Thus η is of type 1 or type 2 according as V' has a vector partially orthogonal to η or not. Note that the type of a given η depends on j.

We shall now count the number of type 1 vectors. This number will be shown to be $q^2(q^{n-2} - 1)/(q - 1)$, as stated in the following lemma.

LEMMA 4. *If $V \neq \tilde{V}$, then the number of type* 1 *vectors* (no two equivalent) *is equal to $q^2(q^{n-2} - 1)/(q - 1)$ and the number of type* 2 *vectors* (no two equivalent) *is equal to q.*

Proof. As $V \neq \tilde{V}$, there is a vector in V not orthogonal to η_0 and so V' has a vector partially orthogonal to η_0.

Let $V'(\eta_0)$ be the collection of vectors in V', partially orthogonal to η_0. Then as rank $V' = n - 1$ and rank $V^*(\eta_0) = n - 2$, $V'(\eta_0)$ contains $((q^{n-1} - 1) - (q^{n-2} - 1))/(q - 1) = q^{n-2}$ vectors, no two equivalent. Let $\xi = (a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n)$.

Case I. $\xi \notin V'(\eta_0)$: We can find a non-null vector $\eta = (c_1, c_2, \ldots c_n)$ which is partially orthogonal to ξ, since we have merely to choose the c_i's so as to have $\sum a_i c_i = 0$, $\sum b_i c_i = 1$. This is possible, as $(a_1, a_2, \ldots a_n)$ and $(b_1, b_2, \ldots b_n)$ are inequivalent, ξ being in V'. There are q^{n-2} such vectors η, automatically no two equivalent. None of these is equivalent to η_0 as $\xi \notin V'(\eta_0)$

Case II. $\xi \in V'(\eta_0)$: As in case I, we get q^{n-2} vectors, no two equivalent and each partially orthogonal to ξ. But one of these vectors is equivalent to η_0.

To get the number of type 1 vectors we proceed as follows. Take a vector ξ of V'. Find all vectors η, no two equivalent and none equivalent to η_0 and each partially orthogonal to ξ. Letting ξ vary over the $(q^{n-1} - 1)/(q - 1)$ inequivalent vectors in V', we get in all $q^{n-2}((q^{n-1} - 1)/(q - 1) - q^{n-2}) + q^{n-2}(q^{n-2} - 1)$ vectors none equivalent to η_0, the first summand corresponds

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

to Case I and the second to Case II. These $q^{n-1}(q^{n-2}-1)/(q-1)$ vectors are not all distinct.

In the above procedure, each vector η of type 1 arises from q^{n-3} inequivalent vectors in V', namely from $\xi + V^*(\eta)$ where ξ is a particular vector in V', partially orthogonal to this η. Taking this into consideration, we get the number of type 1 vectors, no two equivalent.

The number of type 2 vectors, no two equivalent, is therefore $((q^n-1)-q^2(q^{n-2}-1))/(q-1)-1=q$. This completes the proof.

6. Proof of the theorem in section 1. We take n even, $n \geqq 4$. Corresponding to each of the $h'=(q^n-1)/(q-1)$ n-vectors (no two of which are equivalent), we have a vector space $U(\eta_t)$ of vectors orthogonal to η_t and so a block,

$$(5.11)\quad [U(\eta_t)] = [d_{1t}, d_{2t}, \ldots d_{kt}]$$

of $k=(q^{n-1}-1)/(q-1)$ distinct integers d_{it}, $1 \leqq d_{it} \leqq v$. We get h' such blocks in all.

Case I. η_t equivalent to η_0 or of type 2: Now rank $V^*(\eta_t)=n-2$. By Lemma 2, the residue class j (mod v) appears $(q^{n-2}-1)/(q-1)$ amongst the residue classes $d_{it}-d_{i't}(\text{mod } v)$, $i \neq i'$, $d_{it}, d_{it'} \in [U(\eta_t)]$.

Case II. η_t of type 1: Now rank $V^*(\eta_t)=n-3$. By Lemma 2, this residue class j (mod v) occurs $(q^{n-3}-1)/(q-1)$ times amongst the residue classes $d_{tt}-d_{i't}(\text{mod } v)$, $i \neq i'$, $d_{it}, d_{i't} \in [U(\eta_t)]$.

By Lemma 4, the number of type 1 vectors η_t is $q^2(q^{n-2}-1)/(q-1)$ and the number of type 2 vectors is q. So the $h'k(k-1)$ differences $d_{it}-d_{i't}(\text{mod } v)$, $i \neq i'$, $i, i' = 1, 2 \ldots k$, $t=1, 2, \ldots h'$ contain the residue class $j(\text{mod } v)$ λ' times, where

$$\lambda' = (q^{n-2}-1)/(q-1) + q(q^{n-2}-1)/(q-1) + q^2(q^{n-2}-1)(q^{n-3}-1)/(q-1)^2 = (q^{n-1}-1)(q^{n-2}-1)/(q-1)^2.$$

As j is arbitrary and λ' is free of j, we conclude that the above h' blocks form an h' — block difference system (mod v). As yet, the difference system is not translate-free.

We show next that the above h' blocks can be broken up into $h=h'/(q+1)$ families, each consisting of $q+1$ blocks such that of any two blocks in it, one is a translate of the other.

Given $[U(\eta)]$, we now find its translates. With this end in view, we proceed as follows. For any given nonnull η and integer $i>0$, let $Q(\eta, i)$ = the vector space of all $(n+1)$ — vectors

$$(5.12)\quad (b_1, b_2, \ldots b_{n+1}) \text{ where } b_1 + b_2 w \ldots + b_{n+1}w^n = w^i(a_1 + a_2 w + \ldots + a_n w^{n-1}) \text{ with } (a_1, a_2, \ldots a_n) \in U(\eta).$$

$$Q_0(\eta, i) = \text{the subspace of } Q(\eta, i) \text{ consisting of all vectors of the form } (b_1, b_2, \ldots b_n, 0).$$

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

Note that rank $Q(\eta, i) = \text{rank } U(\eta) = n - 1$ and $Q(\eta, i) = Q(\eta, i')$ if $i \equiv i' \pmod{v}$. Moreover $Q(\eta, i) \neq Q(\eta, i')$ if $i \not\equiv i' \pmod{v}$; for $Q(\eta, i) = Q(\eta, i')$ implies (as seen by forming product as in section 3) that $(i - i')(q^{n-1} - 1)$ is divisible by $q^{n+1} - 1$ and as n is even this means $(i - i')$ is divisible by $(q^{n-1} - 1)/(q - 1)$, i.e., v.

If $Q(\eta, i)$ contains a vector $(b_1, b_2, \ldots b_{n+1})$ with $b_{n+1} \neq 0$, then as $Q(\eta, i) = c(b_1, b_2, \ldots b_{n+1}) + c'Q_0(\eta, i)$ c, c' varying over F, we see that

(5.13) the number of $(n + 1)$ — vectors in $Q(\eta, i)$ with last component nonzero $= q^{n-2}(q - 1)$,

and we have

(5.14) $b_{1\nu} + b_{2\nu}w + \ldots + b_{n+1,\nu}w^n = w^i(a_{1\nu} + a_{2\nu}w + \ldots + a_{n\nu}w^n)$,
$\nu = 1, 2, \ldots q^{n-2}(q - 1)$,
with $(a_{1\nu}, a_{2\nu}, \ldots a_{n\nu}) \in U(\eta)$ and $b_{n+1\nu} \neq 0$.

For some i's, $1 \leqq i \leqq v$, $Q(\eta, i) = Q_0(\eta, i)$. We need the number of such i. To get this number, we use the following procedure assuming that the non-null vectors of $U(\eta)$ have been arranged into $k = (q^{n-1} - 1)/(q - 1)$ equivalence classes.

Take a vector $(b_1, b_2, \ldots b_{n+1})$ with $b_{n+1} \neq 0$. Determine the unique integer i, $1 \leqq i < v$ such that $b_1 + b_2w + \ldots + b_{n+1}w^n = w^i(a_1 + a_2w + \ldots + a_nw^{n-1})$ for some vector $(a_1, a_2, \ldots a_n)$ in the first equivalence class of $U(\eta)$. Corresponding to this i, we get a vector space $Q(\eta, i)$ (containing by (5.13), q^{n-2} vectors with last component nonzero and no two equivalent).

Next determine the unique integer i', $1 \leqq i' < v$ such that $b_1 + b_2w + \ldots + b_{n+1}w^n = w^{i'}(a_1 + a_2w + \ldots + a_nw^{n-1})$ for some vector $(a_1, a_2, \ldots a_n)$ in the second equivalence class. Note that $i \neq i'$. Corresponding to i', we get $Q(\eta, i') \neq Q(\eta, i)$.

Proceeding thus with the same $(b_1, b_2, \ldots b_{n+1})$, we get $(q^{n-1} - 1)/(q - 1)$ distinct integers and that many distinct $Q(\eta, i)$'s.

Varying $(b_1, b_2, \ldots b_{n+1})$ over the q^n $(n + 1)$ — vectors, no two equivalent and having their last components nonzero, we get $q^n(q^{n-1} - 1)/(q - 1)$ integers i, $1 \leqq i < v$ but not all of them distinct.

Each such i arises q^{n-2} times in the above procedure as seen from (5.14). Consequently we get $q^n(q^{n-1} - 1)/((q - 1)q^{n-2}) = q^2(q^{n-1} - 1)/(q - 1)$ distinct i's and that many distinct vector spaces $Q(\eta, i)$ each containing vectors with last components nonzero.

Hence there are precisely $v - q^2(q^{n-1} - 1)/(q - 1)$, i.e., $q + 1$ integers i, $1 \leqq i < v$ such that all vectors in $Q(\eta, i)$ have their last components zero. Let these be $Q(\eta, i_1), Q(\eta, i_2), \ldots Q(\eta, i_{q+1})$.

Omitting the last zero in each vector in $Q(\eta, i_\nu)$ we get a vector space T_{i_ν} of rank $n - 1$ and containing n-vectors and so $T_{i_\nu} = U(\eta_{i_\nu})$ for some n-vector

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press

η_{i_ν}. The vectors $(b_1, b_2, \ldots b_n)$ in $U(\eta_{i_\nu})$ are connected with the vectors $(a_1, a_2, \ldots a_n)$ in $U(\eta)$ by $b_1 + b_2 w + \ldots + b_n w^{n-1} =$

$$w^{i_\nu}(a_1 + a_2 w + \ldots + a_n w^{n-1}).$$

This immediately implies that $[U(\eta_{i_\nu})]$ is a translate of $[U(\eta)]$, obtained by adding i_ν to the integers in $[U(\eta)]$ then reducing (mod v).

We have thus shown that given a block $[U(\eta)]$, there are q other blocks $[U(\eta, i_\nu)]$ forming a family such that all these are translates of $[U(\eta)]$ and hence of one another. $[U(\eta)]$ has no other translate.

If we take one block from each such family, we get $h = h'/(q + 1)$ blocks $[d_{1t}, d_{2t}, \ldots d_{kt}]$, $t = 1, 2, \ldots h$. Any nonzero residue class (mod v) appears $\lambda = \lambda'/(q + 1)$ times amongst the differences $d_{it} - d_{i't}$(mod v). The number of blocks now is $h'/(q + 1)$, i.e., $(q^n - 1)/(q^2 - 1)$. This completes the proof.

7. Construction of a series of balanced incomplete block designs. Given a difference system, it is well-known [**2**; **3**] how to construct a balanced incomplete block design by "developing" the initial blocks of the difference system. So from our translate-free difference system, we get a balanced incomplete block design (with no two blocks identical) with parameters.

$$v = (q^{2n+1} - 1)/(q - 1),\ b = v(q^{2n} - 1)/(q^2 - 1)$$
$$r = k(q^{2n} - 1)/(q^2 - 1),\ k = (q^{2n-1} - 1)/(q - 1)$$
$$\lambda = (q^{2n-2} - 1)(q^{2n-1} - 1)/((q^2 - 1)(q - 1))$$

where q is any prime lower and $n \geqq 2$.

References

1. J. Singer, *A theorem in finite projective geometry and some applications to number theory,* Trans. Amer. Math. Soc. *43* (1938), 377–385.

2. K. N. Majindar, *On some methods of construction of b.i.b. designs,* Can. J. Math. *20* (1968), 929–938.

3. M. Hall, *Combinational theory* (Blaisdell Publishing Co., Waltham, Massachusetts, 1967).

4. J. Wallis, *On supplementary difference sets,* Aequationes Math. *8* (1972), 242–257.

5. R. C. Mullin and R. G. Stranton, *Ring generated difference blocks,* Sankhyā Ser. A, 30, *1* (1968), 101–106.

6. R. Wilson, *Cyclotomy and difference families in elementary Abelian groups,* J. Number Theory *4* (1972), 17–47.

Concordia University, Loyola Campus,
Montreal, Quebec

https://doi.org/10.4153/CJM-1974-141-5 Published online by Cambridge University Press