SOME NEW DIFFERENCE SETS

BASIL GORDON, W. H. MILLS, AND L. R. WELCH

1. A difference set is a set $D = \{d_1, d_2, \ldots, d_k\}$ of k distinct residues modulo v such that each non-zero residue occurs the same number of times among the $k(k-1)$ differences $d_i - d_j$, $i \neq j$. If λ is the number of times each difference occurs, then

$$\lambda(v-1) = k(k-1). \tag{1}$$

When we wish to emphasize the particular values of v, k, and λ involved we will call such a set a (v, k, λ) difference set. Another (v, k, λ) difference set $E = \{e_1, e_2, \ldots, e_k\}$ is said to be equivalent to the original one if there exist a and t such that $(t, v) = 1$ and $E = \{a + td_1, \ldots, a + td_k\}$. If $t = 1$ we will call the set E a slide of the set D. If $D = E$, then t is called a multiplier of D.

Difference sets have been studied extensively, partly for their own sake, and partly because of their close connection with symmetric block designs.

A number of cases are known of inequivalent difference sets with the same values of v, k, and λ. For example, Hall **(2)** has shown that for every prime p of the form $4x^2 + 27$ there are at least two inequivalent difference sets with $v = p$, $k = \frac{1}{2}(p-1)$, $\lambda = (p-3)/4$. He also found four inequivalent difference sets with $v = 121$, $k = 40$, $\lambda = 13$ and two such sets with $v = 63$, $k = 31$, $\lambda = 15$.

We have found a close connection between the two inequivalent (63, 31, 15) difference sets and have succeeded in generalizing this situation. We will prove:

THEOREM 1. *Let q be any prime power, say $q = p^e$. Let n and m be positive integers, $n \geqslant 3$. Let m be the product of r prime numbers, not necessarily distinct, and let $N = nm$. Then there are at least 2^r inequivalent difference sets with*

$$v = \frac{q^N - 1}{q - 1}, k = \frac{q^{N-1} - 1}{q - 1}, \lambda = \frac{q^{N-2} - 1}{q - 1}. \tag{2}$$

Our methods not only prove the existence of these sets, but provide the means for actually constructing them. Theorem 1 has the following consequence:

COROLLARY. *Given any positive integer s, there exist v, k, λ for which there are at least s inequivalent (v, k, λ) difference sets.*

In particular this answers the question of whether or not there is an infinite number of (v, k, λ) for which inequivalent difference sets exist (cf. **(2**, p. 980**)**).

Received August 7, 1961. This research was supported, in part, by the Institute for Defense Analyses.

https://doi.org/10.4153/CJM-1962-052-2 Published online by Cambridge University Press

We also prove that the only multipliers of the difference sets that we construct are powers of p. The difference sets arising from geometries over finite fields are included in our class. Thus we are able to determine completely the multipliers of these particular sets—in fact these multipliers are precisely the powers of the characteristic of the coefficient field.

With the exception of the finite geometries and the case $v = 63$, all of the difference sets that we construct are new.

2. By a linear functional from a field E to a subfield F we will mean a mapping from E to F which is linear over F.

We begin with a well-known lemma:

LEMMA 1. *Let F be a finite field, E a finite extension field of F, and L a non-zero linear functional from E to F. Then every linear functional from E to F is of the form L_μ, $\mu \in E$, where $L_\mu(\omega) = L(\mu\omega)$ for all $\omega \in E$. Moreover if $\mu \neq \nu$, then $L_\mu \neq L_\nu$.*

This lemma is a consequence of the fact that if s is the number of elements of E, then there are exactly s distinct linear functionals from E to F and exactly s distinct linear functionals of the form L_μ, $\mu \in E$.

3. For each prime power $q = p^e$ and each integer $N \geqslant 2$, there is a well-known difference set, with v, k, λ given by (2), that is obtained from an appropriate finite geometry over the field $GF(q)$. We now give an algebraic description of this difference set.

Let α be a primitive element of $GF(q^N)$, that is, an element of order $q^N - 1$. Let L be a non-zero linear functional from $GF(q^N)$ to $GF(q)$. Let v, k, λ be given by (2). We will show that the set of all j such that

$$L(\alpha^j) = 0 \tag{3}$$

is a (v, k, λ) difference set.

Since $v = (q^N - 1)/(q - 1)$, it follows that $\alpha^v \in GF(q)$, and hence (3) determines a set of residues modulo v. Moreover α^i runs through all non-zero elements of $GF(q^N)$. Hence $L(\alpha^i) = 0$ for exactly $q^{N-1} - 1$ values of i modulo $q^N - 1$. Thus (3) gives us a set of exactly k residues modulo v. Finally let b be a non-zero residue modulo v. We seek the number of solutions modulo v of $L(\alpha^i) = L(\alpha^{i+b}) = 0$; that is, the number of values of i modulo v such that

$$L_{\alpha^i}(1) = L_{\alpha^i}(\alpha^b) = 0. \tag{4}$$

Since $\alpha^b \notin GF(q)$ and since L_{α^i} runs through all non-zero linear functionals from $GF(q^N)$ to $GF(q)$, it follows that (4) is satisfied by exactly $q^{N-2} - 1$ values of i modulo $q^N - 1$, and hence by exactly λ values of i modulo v. Since λ is independent of b it follows that (3) defines a (v, k, λ) difference set. We denote this set by $\mathfrak{D}_0$.

We now consider the effect of replacing L by another non-zero linear functional L' from $GF(q^N)$ to $GF(q)$. By Lemma 1 we have $L' = L_\mu$ for some $\mu \in GF(q^N)$, $\mu \neq 0$. Clearly $\mu = \alpha^c$ for some integer c. Now $L'(\alpha^i) = L(\mu\alpha^i) = L(\alpha^{i+c})$. Hence $L'(\alpha^i) = 0$ if and only if $i + c$ is in the original difference set $\mathfrak{D}_0$. Thus the effect of replacing L by L' is to replace the difference set $\mathfrak{D}_0 = \{d_1, d_2, \ldots, d_k\}$ by its slide $\{d_1 - c, d_2 - c, \ldots, d_k - c\}$. Therefore, without loss of generality, we can assume that $L(1) = 1$.

The effect of replacing α by another primitive element is to replace $\mathfrak{D}_0$ by an equivalent difference set.

4. The complement of a difference set is a difference set with the same v, with k replaced by $v - k$, and with λ replaced by $v - 2k + \lambda$. For our purpose it is desirable to make this change. Then (2) becomes

$$v = \frac{q^N - 1}{q - 1}, \; k = q^{N-1}, \; \lambda = q^{N-2}(q - 1). \tag{5}$$

The difference set described in § 3 now becomes the set of all j such that $L(\alpha^j) \neq 0$, $0 \leqslant j < v$. We denote this difference set by $\mathfrak{D}(L, \alpha)$.

For an arbitrary difference set $\{d_1, \ldots, d_k\}$ Hall **(3)** has introduced the polynomial

$$\Theta(x) = \sum_{i=1}^{k} x^{d_i}.$$

Since the d_i are defined modulo v, it follows that $\Theta(x)$ is determined modulo $x^v - 1$ by the difference set. We call $\Theta(x)$ the Hall polynomial of the set $\{d_1, \ldots, d_k\}$, whether or not this set is a difference set. Let $d_1, d_2, \ldots, d_k$ be distinct modulo v. They form a (v, k, λ) difference set if and only if

$$\Theta(x)\Theta(x^{-1}) \equiv k - \lambda + \lambda T_v(x) \pmod{x^v - 1}, \tag{6}$$

where $T_v(x) = (x^v - 1)/(x - 1) = 1 + x + \ldots + x^{v-1}$.

Let $\{e_1, \ldots, e_k\}$ be a second (v, k, λ) difference set, and let

$$\Theta_0(x) = \sum_{i=1}^{k} x^{e_i}.$$

These two difference sets are equivalent if and only if there exist integers a and t such that $(t, v) = 1$ and

$$\Theta_0(x) \equiv x^a\Theta(x^t) \pmod{x^v - 1},$$

while they are slides of each other if and only if there is an integer a such that

$$\Theta_0(x) \equiv x^a\Theta(x) \pmod{x^v - 1}.$$

Furthermore t is a multiplier of $\{d_1, \ldots, d_k\}$ if and only if $(t, v) = 1$ and there exists an integer a such that

$$\Theta(x) \equiv x^a\Theta(x^t) \pmod{x^v - 1}.$$

5. Now let $\Theta(x)$ be the Hall polynomial of the particular difference set $\mathfrak{D}(L, \alpha)$. We have

$$\Theta(x) = \sum_{i=0}^{v-1} \epsilon_i x^i,$$

where

$$\epsilon_i = \begin{cases} 0 & \text{if} \quad L(\alpha^i) = 0, \\ 1 & \text{if} \quad L(\alpha^i) \neq 0. \end{cases}$$

Now let $n|N$. Let L_0 be the restriction of L to $GF(q^n)$. We know that L_0 is not identically zero because of the normalization $L(1) = 1$. Furthermore if $n = 1$, then L_0 is the identity mapping.

Let ζ be an element of $GF(q^N)$. Then $\delta \to L(\zeta\delta)$ is a linear functional from $GF(q^n)$ to $GF(q)$. Hence, by Lemma 1, there is a unique element $\tilde{L}(\zeta) \in GF(q^n)$ such that

$$L_0(\tilde{L}(\zeta)\delta) = L(\zeta\delta)$$

for all $\delta \in GF(q^n)$. The mapping $\tilde{L}$ is a linear functional from $GF(q^N)$ to $GF(q^n)$. We have $\tilde{L}(1) = 1$. If $n = 1$, then $\tilde{L} = L$.

Now put $\xi = (q^N - 1)/(q^n - 1)$ and $\beta = \alpha^\xi$. Then β is a primitive element of $GF(q^n)$. Put

$$w = \frac{q^n - 1}{q - 1}, l = q^{n-1}, \mu = q^{n-2}(q - 1). \tag{7}$$

Let $\theta(y)$ be the Hall polynomial of $\mathfrak{D}(L_0, \beta)$. Thus

$$\theta(y) = \sum_{j=0}^{w-1} \delta_j y^j,$$

where

$$\delta_j = \begin{cases} 0 & \text{if} \quad L_0(\beta^j) = 0, \\ 1 & \text{if} \quad L_0(\beta^j) \neq 0. \end{cases}$$

It is understood that $\theta(y) = 1$ if $n = 1$.

We put $y = x^\xi$. Then $\theta(y)$ becomes a polynomial in x, and since $y^w - 1 = x^v - 1$ we have

$$\theta(y)\theta(y^{-1}) \equiv l - \mu + \mu T_w(y) \qquad (\text{mod } x^v - 1). \tag{8}$$

We will now establish a connection between $\theta(y)$ and $\Theta(x)$. The polynomial $\Theta(x)$ can be written in the form

$$\Theta(x) = \sum_{i=0}^{\xi-1} x^i \omega_i(y),$$

where

$$\omega_i(y) = \sum_{j=0}^{w-1} \epsilon_{i+\xi j} y^j.$$

For every value of i, $\tilde{L}(\alpha^i)$ is either 0 or a power of β. If $\tilde{L}(\alpha^i) \neq 0$ we put $\tilde{L}(\alpha^i) = \beta^{-m_i}$. Now $\epsilon_{i+\xi j} = 0$ if and only if $L(\alpha^{i+\xi j}) = 0$. We have

$$\begin{aligned} L(\alpha^{i+\xi j}) &= L(\alpha^i\beta^j) \\ &= L_0(\tilde{L}(\alpha^i)\beta^j) \\ &= \begin{cases} 0 & \text{if} \quad \tilde{L}(\alpha^i) = 0, \\ L_0(\beta^{j-m_i}) & \text{if} \quad \tilde{L}(\alpha^i) \neq 0. \end{cases} \end{aligned}$$

Hence

$$\epsilon_{i+\xi j} = \begin{cases} 0 & \text{if} \quad \tilde{L}(\alpha^i) = 0, \\ \delta_{j-m_i} & \text{if} \quad \tilde{L}(\alpha^i) \neq 0. \end{cases}$$

Therefore $\omega_i(y) = 0$ if $\tilde{L}(\alpha^i) = 0$, while if $\tilde{L}(\alpha^i) \neq 0$ we have

$$\begin{aligned} \omega_i(y) &= \sum_{j=0}^{w-1} \epsilon_{i+\xi j} y^j = \sum_{j=0}^{w-1} \delta_{j-m_i} y^j \\ &\equiv \sum_{j=0}^{w-1} \delta_j y^{j+m_i} = y^{m_i}\theta(y) \qquad \pmod{x^v - 1}. \end{aligned}$$

Thus we have proved:

THEOREM 2. *Let q be a power of the prime p and let N be an integer, $N \geqslant 2$. Let L be a linear functional from the finite field $GF(q^N)$ to the subfield $GF(q)$, such that $L(1) = 1$. Let L_0 be the restriction of L to an intermediate field $GF(q^n)$, where $n|N$. Let $\tilde{L}$ be the linear functional from $GF(q^N)$ to $GF(q^n)$ such that $L_0(\tilde{L}(\zeta)\delta) = L(\zeta\delta)$ for all $\zeta \in GF(q^N)$ and $\delta \in GF(q^n)$. Set $v = (q^N - 1)/(q - 1)$, $w = (q^n - 1)/(q - 1)$, and $\xi = v/w$. Let α be a primitive element of $GF(q^N)$, and set $\beta = \alpha^\xi$. Let $\Theta(x)$ and $\theta(y)$ be the Hall polynomials of $\mathfrak{D}(L, \alpha)$ and $\mathfrak{D}(L_0, \beta)$ respectively. If $n = 1$ it is understood that $\theta(y) = 1$. Let $y = x^\xi$. Then $\theta(y)$ divides $\Theta(x)$ in the sense that there exists a polynomial $\Omega(x)$ such that*

$$\Theta(x) \equiv \Omega(x)\theta(y) \qquad \pmod{x^v - 1}.$$

The polynomial $\Omega(x)$ is given by

$$\Omega(x) = \Sigma x^i y^{m_i}, \tag{9}$$

where the summation is over those values of i for which

$$\tilde{L}(\alpha^i) \neq 0, \; 0 \leqslant i < \xi, \quad \textit{and} \quad \tilde{L}(\alpha^i) = \beta^{-m_i}.$$

6. If $n > 1$, then the set $\mathfrak{D}(L_0, \beta)$ is a (w, l, μ) difference set, where w, l, μ are given by (7). Let $\{b_1, b_2, \ldots, b_l\}$ be an arbitrary difference set with the same parameters w, l, μ. Let $\theta_0(y)$ be the associated Hall polynomial

$$\theta_0(y) = \sum_{i=1}^{l} y^{b_i}, \tag{10}$$

and put

$$\Theta_0(x) = \Omega(x)\theta_0(y), \tag{11}$$

where $y = x^\xi$ as before and $\Omega(x)$ is given by (9). It follows from (9), (10), and (11) that

$$\Theta_0(x) = \sum_{i=1}^{k} x^{e_i},$$

where the e_i are distinct modulo v. Furthermore, from (8) and the analogous congruence for $\theta_0(y)$, we have

$$\theta_0(y)\theta_0(y^{-1}) \equiv l - \mu + \mu T_w(y) \equiv \theta(y)\theta(y^{-1}) \qquad (\text{mod } x^v - 1).$$

Hence, using (11) and (6),

$$\begin{aligned}\Theta_0(x)\Theta_0(x^{-1}) &= \Omega(x)\Omega(x^{-1})\theta_0(y)\theta_0(y^{-1})\\ &\equiv \Omega(x)\Omega(x^{-1})\theta(y)\theta(y^{-1})\\ &= \Theta(x)\Theta(x^{-1})\\ &\equiv k - \lambda + \lambda T_v(x) \qquad (\text{mod } x^v - 1).\end{aligned}$$

Therefore $\{e_1, e_2, \ldots, e_k\}$ is a (v, k, λ) difference set with the same values of v, k, λ, that is, those given by (5).

7. We now determine the conditions under which two difference sets obtained in this way are equivalent to each other. Let $B = \{b_1, b_2, \ldots, b_l\}$ and $C = \{c_1, c_2, \ldots, c_l\}$ be two (w, l, μ) difference sets, and let $\theta_b(y) = \sum y^{b_i}$ and $\theta_c(y) = \sum y^{c_i}$ be their Hall polynomials. If $n = 1$ it is understood that $\theta_b(y) = \theta_c(y) = 1$. Put

$$\Theta_b(x) = \Omega(x)\theta_b(y), \qquad \Theta_c(x) = \Omega(x)\theta_c(y).$$

Then $\Theta_b(x)$ and $\Theta_c(x)$ are the Hall polynomials of (v, k, λ) difference sets, say $\bar{B}$ and $\bar{C}$ respectively. Suppose $\bar{B}$ and $\bar{C}$ are equivalent. Then there exist integers a and t such that $(t, v) = 1$ and

$$\Theta_b(x) \equiv x^a\Theta_c(x^t) \qquad (\text{mod } x^v - 1). \tag{12}$$

Our analysis of (12) will not only give us necessary and sufficient conditions that $\bar{B}$ and $\bar{C}$ be equivalent, but by putting $B = C$ it will give us the multipliers of $\bar{B}$.

LEMMA 2. *If* (12) *holds, then there exist integers r and s such that*

$$\Omega(x) \equiv x^r\Omega(x^t) \qquad (\text{mod } x^v - 1) \tag{13}$$

and

$$\theta_b(y) \equiv y^s\theta_c(y^t) \qquad (\text{mod } y^w - 1).$$

In particular if B and C are inequivalent, then so are $\bar{B}$ and $\bar{C}$.

Proof. By construction $\Theta_b(x) = \sum x^i y^{m_i}\theta_b(y)$, where the summation is over those values of i for which $\tilde{L}(\alpha^i) \neq 0$, $0 \leqslant i < \xi$. Similarly

$$x^a\Theta_c(x^t) = \sum x^{a+ti} y^{tm_i}\theta_c(y^t),$$

https://doi.org/10.4153/CJM-1962-052-2 Published online by Cambridge University Press

where the summation is over the same values of i. Choose an h such that $\tilde{L}(\alpha^h) \neq 0$. Then, by comparing terms in (12), we obtain

$$x^h y^{m_h} \theta_b(y) \equiv x^{a+tj} y^{tm_j} \theta_c(y^t) \pmod{x^v - 1},$$

where $a + tj \equiv h \pmod{\xi}$. Since $x^v - 1 = y^w - 1$, this gives us

$$\theta_b(y) \equiv y^s \theta_c(y^t) \pmod{y^w - 1},$$

where $s = tm_j - m_h + \xi^{-1}(a + tj - h)$. Now

$$\Omega(x)\theta_b(y) \equiv x^a \Omega(x^t)\theta_c(y^t) \pmod{x^v - 1}$$

by (12). Since

$$\theta_b(y)\theta_b(y^{-1}) \equiv l - \mu + \mu T_w(y) \pmod{y^w - 1},$$

it follows that $\theta_b(y)$ is relatively prime to $y^w - 1$. Hence

$$\Omega(x) \equiv x^a y^{-s} \Omega(x^t) \pmod{x^v - 1},$$

which proves the lemma.

Now let $Q = GF(q)$, and let Q^* be the set of all non-zero elements of Q.

LEMMA 3. *Suppose* (13) *holds with* $(t, v) = 1$. *Put* $\eta = \alpha^r$, *and let* $\omega \in GF(q^N)$. *Then* $\tilde{L}(\omega) \in Q^*$ *if and only if* $\tilde{L}(\eta\omega^t) \in Q^*$.

Proof. From (9) we have

$$\Omega(x) = \sum x^i y^{m_i} = \sum x^{i+\xi m_i} = \sum_{j \in S} x^j, \tag{14}$$

where S is the set of all j such that $L(\alpha^j) = 1$, $0 \leqslant j < q^N - 1$. Since α^v is a primitive element of Q^*, the effect of adding v to j is to multiply $\tilde{L}(\alpha^j)$ by a primitive element of Q^*. Therefore (14) can be written in the form

$$\Omega(x) \equiv \sum_{j \in S'} x^j \pmod{x^v - 1},$$

where S' is the set of all j such that $\tilde{L}(\alpha^j) \in Q^*$, $0 \leqslant j < v$. The assumption (13) implies that $\tilde{L}(\alpha^j) \in Q^*$ if and only if $\tilde{L}(\alpha^{r+jt}) \in Q^*$. If $\omega = 0$ the lemma is immediate. If $\omega \neq 0$, we obtain the desired result by putting $\omega = \alpha^j$.

LEMMA 4. *Suppose* (13) *holds with* $(t, v) = 1$. *Let* $\eta = \alpha^r$, $\zeta \in GF(q^n)$, *and* $\omega \in GF(q^N)$. *Then* $\tilde{L}(\omega) \in \zeta Q^*$ *if and only if* $\tilde{L}(\eta\omega^t) \in \zeta^t Q^*$.

Proof. Suppose first that $\zeta \neq 0$. Then $\tilde{L}(\omega) \in \zeta Q^*$ is equivalent to $\tilde{L}(\omega\zeta^{-1}) \in Q^*$. By Lemma 3 this is true if and only if $\tilde{L}(\eta\omega^t\zeta^{-t}) \in Q^*$, which in turn is equivalent to $\tilde{L}(\eta\omega^t) \in \zeta^t Q^*$. Next suppose $\tilde{L}(\omega) = 0$. We have $\tilde{L}(\eta\omega^t) \in \nu^t Q^*$ for some $\nu \in GF(q^n)$. If $\nu \neq 0$, then by the first part of the proof we have $\tilde{L}(\omega) \in \nu Q^*$, a contradiction. Hence $\nu = 0$ and $\tilde{L}(\eta\omega^t) = 0$, which completes the proof of the lemma.

LEMMA 5. *Suppose that* (13) *holds with* $(t, v) = 1$. *Let* $\zeta_1, \zeta_2, \ldots, \zeta_m$ *be*

https://doi.org/10.4153/CJM-1962-052-2 Published online by Cambridge University Press

elements of $GF(q^N)$ that are linearly independent over $GF(q^n)$. Let c_i, a_i, $1 \leqslant i \leqslant m$ be elements of $GF(q^n)$ such that

$$\left(\sum_{i=1}^{m} c_i\zeta_i\right)^t = \sum_{i=1}^{m} a_i\zeta_i^t.$$

Then $a_i \in c_i^t Q^*$, $1 \leqslant i \leqslant m$.

Proof. By Lemma 1 there exist elements μ_j of $GF(q^N)$ such that $\tilde{L}(\mu_j\zeta_i) = \delta_{ij}$, $1 \leqslant i, j \leqslant m$, where as usual,

$$\delta_{ij} = \begin{cases} 0 & \text{if} \quad i \neq j, \\ 1 & \text{if} \quad i = j. \end{cases}$$

Then, by Lemma 4, $\tilde{L}(\eta\mu_j^t\zeta_i^t) = 0$ if $i \neq j$, and $\tilde{L}(\eta\mu_j^t\zeta_j^t) \in Q^*$. Now $\tilde{L}(\mu_j\sum c_i\zeta_i) = c_j$, so that

$$\tilde{L}(\eta\mu_j^t(\sum c_i\zeta_i)^t) \in c_j^t Q^*.$$

On the other hand,

$$\tilde{L}(\eta\mu_j^t(\sum c_i\zeta_i)^t) = \sum_i a_i\tilde{L}(\eta\mu_j^t\zeta_i^t) \in a_j Q^*.$$

Hence $a_j \in c_j^t Q^*$.

LEMMA 6. *Suppose* (13) *holds with* $(t, v) = 1$. *Let $\zeta_1, \zeta_2, \ldots, \zeta_m$ be a basis for $GF(q^N)$ over $GF(q^n)$. Then $\zeta_1^t, \zeta_2^t, \ldots, \zeta_m^t$ is also a basis for $GF(q^N)$ over $GF(q^n)$.*

Proof. Suppose $\sum a_i\zeta_i^t = 0$ with $a_i \in GF(q^n)$, $1 \leqslant i \leqslant m$. We apply Lemma 5 with $c_1 = c_2 = \ldots = c_m = 0$ and obtain $a_1 = a_2 = \ldots = a_m = 0$. Hence $\zeta_1^t, \zeta_2^t, \ldots, \zeta_m^t$ are linearly independent over $GF(q^n)$. It follows that they form a basis for $GF(q^N)$ over $GF(q^n)$.

LEMMA 7. *Suppose* (13) *holds with* $(t, v) = 1$. *Let ω be an element of $GF(q^N)$, and suppose that $N > n$. Then there exist a_1 and a_2 in Q^* such that $(1 + \omega)^t = a_1 + a_2\omega^t$.*

Proof. Suppose first that $\omega \notin GF(q^n)$. Then we can find a basis $\zeta_1, \zeta_2, \ldots, \zeta_m$ of $GF(q^N)$ over $GF(q^n)$ with $\zeta_1 = 1$ and $\zeta_2 = \omega$. Taking $c_1 = c_2 = 1$, $c_3 = \ldots = c_m = 0$, we have

$$1 + \omega = \sum_{i=1}^{m} c_i\zeta_i.$$

Moreover $\zeta_1^t, \zeta_2^t, \ldots, \zeta_m^t$ is also a basis by Lemma 6, so that we have

$$(1 + \omega)^t = \sum_{i=1}^{m} a_i\zeta_i^t$$

with $a_i \in GF(q^n)$. By Lemma 5 we have $a_3 = a_4 = \ldots = a_m = 0$, $a_1 \in Q^*$, $a_2 \in Q^*$, which settles the case $\omega \notin GF(q^n)$.

Now suppose $\omega \in GF(q^n)$. We recall that $\tilde{L}(1) = 1$. Let ζ be an element of $GF(q^N)$ such that $\zeta \notin GF(q^n)$ and $\tilde{L}(\zeta) = \omega$. Then $\tilde{L}(1 + \zeta) = 1 + \omega$ and $\tilde{L}(\eta(1 + \zeta)^t) \in (1 + \omega)^t Q^*$. By the first part of the proof $(1 + \zeta)^t = b + c\zeta^t$ with $b, c \in Q^*$. Therefore

$$\tilde{L}(\eta(1 + \zeta)^t) = \tilde{L}(\eta(b + c\zeta^t)) = b\tilde{L}(\eta) + c\tilde{L}(\eta\zeta^t).$$

Now $\tilde{L}(\eta) = \tilde{L}(\eta 1^t) \in Q^*$ and $\tilde{L}(\eta\zeta^t) \in \omega^t Q^*$. It follows that $(1 + \omega)^t = a_1 + a_2\omega^t$ with $a_1, a_2 \in Q^*$.

8. To complete our discussion we need a theorem about finite fields that is of interest for its own sake. Throughout this section we make the following assumptions: $N \geqslant 3$, q is a power of the prime p, $Q = GF(q)$, Q^* is the set of non-zero elements of Q, $v = (q^N - 1)/(q - 1)$, t is an integer relatively prime to v, and for every $\omega \in GF(q^N)$ there exist a_1, a_2, in Q^* such that

$$(1 + \omega)^t = a_1 + a_2\omega^t. \tag{15}$$

Since (15) holds for all $\omega \in GF(q^N)$ it follows that for every pair ψ_1, ψ_2 of elements of $GF(q^N)$ we have $(\psi_1 + \psi_2)^t = b_1\psi_1{}^t + b_2\psi_2{}^t$ for suitable b_1, b_2 in Q^*. By induction it follows that given any $\psi_1, \psi_2, \ldots, \psi_u$ in $GF(q^N)$ there exist $b_1, b_2, \ldots, b_u$ in Q^* such that

$$(\psi_1 + \psi_2 + \ldots + \psi_u)^t = b_1\psi_1^t + b_2\psi_2^t + \ldots + b_u\psi_u^t. \tag{16}$$

We write (15) in the form

$$(1 + \omega)^t = r_\omega(1 + s_\omega\omega^t),$$

where r_ω, s_ω are elements of Q^*. Since $(t, v) = 1$, it follows that if $\omega \notin Q$, then $\omega^t \notin Q$ and r_ω, s_ω are uniquely determined.

LEMMA 8. *If ω^t, τ^t, ζ^t are linearly independent over Q, then $s_{\zeta/\omega} = s_{\zeta/\tau}s_{\tau/\omega}$.*

Proof. For uniquely determined $b_1, b_2, b_3, c_1, c_2, c_3$ in Q^* we have

$$\begin{aligned} b_1\omega^t + b_2\tau^t + b_3\zeta^t &= (\omega + \tau + \zeta)^t \\ &= c_1(\omega + \tau)^t + c_2\zeta^t \\ &= c_1\omega^t(1 + \tau/\omega)^t + c_2\zeta^t \\ &= c_3(\omega^t + s_{\tau/\omega}\tau^t) + c_2\zeta^t. \end{aligned}$$

It follows that $s_{\tau/\omega} = b_2/b_1$. By symmetry $s_{\zeta/\tau} = b_3/b_2$ and $s_{\zeta/\omega} = b_3/b_1$. The lemma follows immediately.

Let α be a primitive element of $GF(q^N)$. We have $(1 + \alpha)^t = r_\alpha(1 + s_\alpha\alpha^t)$. Later we shall reduce the general case to the case $s_\alpha = 1$. We now derive a few consequences of this equality.

LEMMA 9. *If $s_\alpha = 1$ and if $\omega \notin Q$, then $s_\omega = 1$.*

Proof. Since $(t, v) = 1$ it follows that α^t is not contained in any proper subfield of $GF(q^N)$. Hence α^t has degree N over Q. Hence $1, \alpha^t$, and α^{2t} are linearly independent over Q. Put $\omega = \alpha^u$, $1 \leqslant u < q^N - 1$. We proceed by induction on u. By Lemma 8 we have $s_{\alpha^2} = s_\alpha s_\alpha = 1$. Thus the lemma holds for $u = 1$ and $u = 2$. Suppose that $u \geqslant 3$ and that the lemma holds for all positive integers less than u. Since $\omega \notin Q$ and $(t, v) = 1$ it follows that $\omega^t \notin Q$, so that 1 and ω^t are linearly independent over Q. Since $1, \alpha^t$, and α^{2t} are linearly independent over Q, it follows that $1, \alpha^{jt}, \alpha^{ut}$ are linearly independent over Q either for $j = 1$ or for $j = 2$.

Lemma 8 now gives us $s_\omega = s_{\alpha^u} = s_{\alpha^j} s_{\alpha^{u-j}} = 1$ which completes the proof by induction.

Lemma 10. *If* $s_\alpha = 1$ *then* $(1 + \omega)^t = 1 + \omega^t$ *for all* $\omega \notin Q$.

Proof. Since $N \geqslant 3$ there is a ζ such that $1, \omega^t, \zeta^t$ are linearly independent over Q. Then, for suitable c_1, c_2, c_3 in Q^*, we have $(1 + \omega + \zeta)^t = c_1 + c_2\omega^t + c_3\zeta^t$. Moreover, c_1, c_2, c_3 are uniquely determined. Now $(1 + \omega)^t = r_\omega(1+\omega^t)$ by Lemma 9. It follows that $(1 + \omega)^t/\zeta^t \notin Q$ and hence $(1 + \omega)/\zeta \notin Q$. Applying Lemma 9 again we have

$$\begin{aligned}(1 + \omega + \zeta)^t &= a(1 + \omega)^t + a\zeta^t\\ &= ar_\omega + ar_\omega\omega^t + a\zeta^t,\end{aligned}$$

where $a = r_{(1+\omega)/\zeta}$. Hence $c_1 = c_2$. Similarly $c_1 = c_3$. Therefore $r_\omega = 1$, and $(1 + \omega)^t = 1 + \omega^t$.

We now come to the main theorem of this section:

Theorem 3. *Let* $N \geqslant 3$, *q be a power of the prime p*, $v = (q^N - 1)/(q - 1)$, *and t an integer relatively prime to v. Suppose that for every $\omega \in GF(q^N)$ there exist non-zero elements a_1 and a_2 in $GF(q)$ such that* $(1 + \omega)^t = a_1 + a_2\omega^t$. *Then t is congruent to a power of p modulo v.*

Proof. Without loss of generality suppose $0 < t < v$. Using the notation already developed we have $(1 + \alpha)^t = r_\alpha(1 + s_\alpha\alpha^t)$, where α is a fixed primitive element of $GF(q^N)$. Since $s_\alpha \in Q^*$ we have $s_\alpha = \alpha^{vc}$ for some c such that $0 \leqslant c < q - 1$. Put $t' = t + vc$. Then $0 < t' < q^N - 1$, and $(t', v) = 1$. Furthermore for any ω in $GF(q^N)$ there exist r_ω' and s_ω' in Q^* such that

$$(1 + \omega)^{t'} = r'_\omega(1 + s'_\omega\omega^{t'}).$$

Moreover $s_\alpha' = 1$. Hence, by Lemma 10,

$$(1 + \omega)^{t'} = 1 + \omega^{t'} \tag{17}$$

for all $\omega \in GF(q^N)$, $\omega \notin Q$. Now suppose that t' is not a power of p. Then (17) becomes a polynomial equation of degree at most $t' - 1$, with at least $q^N - q$ roots. Therefore $t' > q^N - q$. Put $u = q^N - 1 - t'$. Multiplying (17) by $\omega^u(1 + \omega)^u$ we obtain

$$\omega^u = (1 + \omega)^u\omega^u + (1 + \omega)^u$$

for all $\omega \in GF(q^N)$, $\omega \notin Q$. Hence $2u \geqslant q^N - q$. Therefore

$$q^N - 1 = t' + u > \frac{3}{2}(q^N - q)$$

or $q^N < 3q - 2$ which is impossible since $N \geqslant 3$, $q \geqslant 2$. It follows that t' is a power of p, and hence t is congruent to a power of p modulo v, which completes the proof of the theorem.

Theorem 3 is false for $N = 2$; in fact the hypothesis is fulfilled for all t relatively prime to v.

9. We now apply Theorem 3 to the situation of § 7. We recall that we started with two (w, l, μ) difference sets $B = \{b_1, \ldots, b_l\}$ and $C = \{c_1, \ldots, c_l\}$. We used these to construct two (v, k, λ) difference sets with associated polynomials $\Theta_b(x)$, $\Theta_c(x)$ respectively. We now suppose, as before, that there exist a and t with $(t, v) = 1$ and

$$\Theta_b(x) \equiv x^a \Theta_c(x^t) \pmod{x^v - 1}.$$

From Lemma 2, Lemma 7, and Theorem 3 we deduce that if $N \geqslant 3$ and $N > n$, then t is congruent to a power of p modulo v. Suppose first that $n > 1$. Since $w|v$ it follows that t is also congruent to a power of p modulo w. Now $l - \mu = q^{n-2}$, which is a power of p, and $p \nmid w$. A theorem of Hall (**2**, p. 976) states that in this situation every power of p is a multiplier of each (w, l, μ) difference set. (Hall's theorem applies directly to the complement of our difference set.) In particular, t is a multiplier of C. Hence

$$\theta_c(y^t) \equiv y^u \theta_c(y) \pmod{y^w - 1}$$

for some integer u. It follows from Lemma 2 that

$$\theta_b(y) \equiv y^{s+u} \theta_c(y) \pmod{y^w - 1}.$$

Therefore B is a slide of C. Thus we have proved:

THEOREM 4. *Let q be a power of the prime p and let N be a positive integer. Let $n|N$, $N > n \geqslant 2$. Let v, k, λ, w, l, μ be given by* (5) *and* (7), *let $\xi = v/w$, and let $\Omega(x)$ be the polynomial given by* (9). *To any (w, l, μ) difference set B with Hall polynomial $\theta(y)$, there corresponds a (v, k, λ) difference set $\bar{B}$ with Hall polynomial $\Theta(x) = \Omega(x)\theta(x^\xi)$. If B and C are (w, l, μ) difference sets then $\bar{B}$ and $\bar{C}$ are equivalent if and only if B is a slide of C.*

Theorem 4 is uninteresting if $n = 2$—in this case no new difference sets can be obtained by our methods. The smallest interesting case is $q = p = 2$, $n = 3$, $N = 6$. Here $w = 7$, $l = 4$, $\mu = 2$. The two $(7, 4, 2)$ difference sets $\{0, 1, 2, 4\}$ and $\{0, -1, -2, -4\}$ are not slides of each other, but every $(7, 4, 2)$ difference set is a slide of one of them. They lead to two inequivalent $(63, 32, 16)$ difference sets. One of the latter corresponds to a finite geometry and the other does not. See Hall (**2**, p. 985). We note that the two $(7, 4, 2)$ difference sets are equivalent. Similarly if we take $q = p = 2$, $n = 3$, $N = 9$ we obtain two inequivalent $(511, 256, 128)$ difference sets, one of which corresponds to a finite geometry. The other one is a new difference set.

In the above agument it was concluded that

$$\Theta_b(x) \equiv x^a \Theta_c(x^t) \pmod{x^v - 1}$$

implies that t is congruent to a power of p modulo v. Applying this to the case $B = C$ we conclude that every multiplier of B is a power of p modulo v. Since $k - \lambda = q^{N-2}$, which is a power of p, and $p \nmid v$, Hall's theorem asserts that every power of p is a multiplier of B. Thus the multipliers of the difference set B are precisely the powers of p. Setting $n = 1$, this gives us the result that if $N \geqslant 3$, then the multipliers of the set $\mathfrak{D}(L, \alpha)$ are precisely the powers of p. Dismissing the difference sets corresponding to $N = 2$ as trivial we have the following result:

THEOREM 5. *Let D be either one of the (v, k, λ) difference sets B of Theorem 4 or a non-trivial (v, k, λ) difference set that corresponds to a finite geometry over a finite field. Then the multipliers of D are precisely the powers of p modulo v.*

10. Let $n \geqslant 3$, and let M denote the number of inequivalent (w, l, μ) difference sets where w, l, μ are given by (7). It is known that -1 is not a multiplier of a non-trivial difference set, that is, a difference set with $1 < k < v - 1$. Hence there are at least $2M$ possible (w, l, μ) difference sets, none of which is a slide of any other. Hence there are at least $2M$ inequivalent (v, k, λ) difference sets with v, k, λ given by (5) or by (2). It follows by induction that if $N = nm$ where $n \geqslant 3$ and m is the product of r primes, not necessarily distinct, then there are at least 2^r inequivalent (v, k, λ) difference sets with v, k, λ given by (5), or equivalently by (2). This establishes Theorem 1 stated in § 1.

Actually the number of inequivalent difference sets is usually much greater than 2^r, as there will normally exist non-multipliers other than -1. For example in the case $q = 2$, $n = 5$, $N = 10$, there are two known difference sets with parameters (31, 16, 8). One of these leads to two inequivalent sets with parameters (1023, 512, 256) and the other leads to six more inequivalent sets with the same parameters.

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. M. Hall, *A survey of difference sets*, Proc. Amer. Math. Soc., *7* (1956), 975–986.
3. ——— *Cyclic projective planes*, Duke Math. J., *14* (1947), 1079–1090.
4. M. Hall and H. J. Ryser, *Cyclic incidence matrices*, Can. J. Math., *3* (1951), 495–502.

University of California
Yale University
Institute for Defense Analyses, Princeton