JOURNAL OF COMBINATORIAL THEORY (A) 19, 177–191 (1975)

A Generalization of Cyclic Difference Sets II*

CLEMENT W. H. LAM†

Department of Mathematics, Statistics, and Computing Science,
University of Calgary, Calgary, Alberta, Canada

Communicated by H. J. Ryser

Received October 30, 1974

This is the second paper on addition sets. A generalization of Hall's Multiplier Theorem for difference sets is given. Some nonexistence theorems are also given. These methods are used to compile a table of addition sets with parameter $k \leqslant 10$. One unsolved case still remains.

1. INTRODUCTION

This is the second paper on addition sets. The first paper [5] introduced some basic properties of addition sets and gave some examples. In this paper, we are mainly concerned with a search of addition sets with parameter $k \leqslant 10$. Some nonexistence theorems and some construction methods are developed to aid the search.

A (v, k, λ, g)*-addition set* $A = \{a_1, ..., a_k\}$, or simply an *addition set*, is a collection of k distinct residues modulo v, such that for any residue $\gamma \not\equiv 0 \pmod v$ the congruence

$$a_i + ga_j \equiv \gamma \qquad (\text{mod } v) \tag{1.1}$$

has exactly λ solution pairs (a_i, a_j) with a_i and a_j in A.

It is clear that the well-known difference sets are addition sets with $g = -1$. Other examples are given in [5].

To avoid degeneracy, we further require a nontrivial addition set to satisfy

$$1 < k < v - 1. \tag{1.2}$$

A parameter d is also defined by letting $d + \lambda$ be the number of ways that 0 can be represented as $(a_i + ga_j)$ modulo v with a_i and a_j in the addition set A.

* This research was supported in part by the Army Research Office—Durham.

† Present address: Computer Science Department, Concordia University, 1455 de Maisonneuve Blvd. West, Montreal, Quebec H3G 1M8, Canada.

Some of the results in [5] are needed in this paper. We will just state them without proof.

THEOREM 1.1. *The parameters of a nontrivial addition set satisfy*

(i) $k^2 = d + \lambda v$,
(ii) $0 \leqslant d + \lambda \leqslant k$,
(iii) $0 < \lambda < k$, *and*
(iv) $-k < d < k$.

Instead of the addition set itself, it is often convenient to deal with its *Hall-polynomial*. Here, a Hall-polynomial of a set A is the polynomial

$$\theta(x) = x^{a_1} + \cdots + x^{a_k},$$

where $a_i \in A$. The importance of the Hall-polynomial is due to the following result.

THEOREM 1.2. *A set A of k distinct residues modulo v is a (v, k, λ, g)-addition set if and only if its Hall-polynomial satisfies*

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\text{mod } x^v - 1).$$

Furthermore, we have the following two results.

THEOREM 1.3. *If A is a nontrivial (v, k, λ, g)-addition set with $d \neq 0$, then* GCD $(g, v) = 1$.

THEOREM 1.4. *If A is a nontrivial addition set with v even, then d is a square.*

2. MULTIPLIER THEOREMS

The multiplier theorems have been very useful in the study of difference sets. Some of them can be generalized for addition sets. Let us first give some definitions.

Given a set $A = \{a_1, ..., a_k\}$ modulo v, then for any integer s the set $\{a_1 + s, ..., a_k + s\} \equiv A + s$ taken modulo v is a *shift* of A by s. If t is relatively prime to v and if the set $\{ta_1, ..., ta_k\} \equiv tA$ taken modulo v is some shift $A + s$ of the original addition set A, then t is called a *multiplier* of A. If $t \not\equiv 1 \pmod{v}$, then t is a nontrivial multiplier. If $tA \equiv A$ when taken modulo v, then t is a multiplier *fixing* the addition set A.

The following two results from [5] established the existence of multipliers for many addition sets.

THEOREM 2.1. *Let A be a nontrivial (v, k, λ, g)-addition set with $d \neq 0$. Given any integer h prime to v, A is also a (v, k, λ, h)-addition set if and only if gh is a multiplier fixing A.*

COROLLARY 2.2. *Let A be a nontrivial (v, k, λ, g)-addition set with $d \neq 0$. Then g^2 is a multiplier fixing A.*

If $g^2 \not\equiv 1 \pmod{v}$, then Corollary 2.2 gives us a nontrivial multiplier for the addition set.

To take care of some of the remaining cases, we will give a generalization of the Multiplier Theorem due to Hall [2]. In some cases, the multipliers constructed by this generalization are more suitable for a computer search than the ones constructed by Corollary 2.2. A discussion of how multipliers are used will be given in Section 4.

The following facts of algebraic number theory are needed in the remainder of this section and part of the next. They are quoted from [1, pp. 52–53]. Here, we let Q denote the rational field and we let ξ_d denote a primitive dth root of unity. $\varphi(d)$ will be the Euler φ-function.

THEOREM 2.3. *The prime ideal decomposition of the rational prime p [that is of the principal ideal (p)] in $Q(\xi_d)$ is given by*

$$(p) = (1 - \xi_d)^{\varphi(d)} \qquad \textit{when} \quad d = p^i, \tag{2.1}$$

$$(p) = P_1 \cdots P_g \qquad \textit{when} \quad (d, p) = 1, \tag{2.2}$$

where the distinct prime ideals P_i are conjugates. Further, g is $\varphi(d)/f$, where f is the order of p modulo d. The field automorphism determined by the mapping $\xi_d \to \xi_d{}^p$ fixes each of these prime ideals P_i.

$$(p) = (P_1 \cdots P_g)^{\varphi(p^a)} \qquad \textit{when} \quad d = p^a w, \quad (p, w) = 1, \tag{2.3}$$

where g is $\varphi(w)/f$ and f is the order of p modulo w. The ideals $P_1, \ldots, P_g$ of (2.2), (2.3) can be determined explicitly. For, if $f(x)$ denotes the irreducible equation satisfied by ξ_d over the rationals, then, with the $f_i(x)$ irreducible modulo p,

$$f(x) \equiv (f_1(x) \cdots f_g(x))^{\varphi(p^a)} \pmod{p}$$

and

$$P_i = (p, f_i(\xi_d)).$$

As the polynomial $1 + x + \cdots + x^{v-1}$ appears quite often in this paper it is sometimes denoted by $T(x)$.

The next lemma is needed to generalize Hall's Multiplier Theorem. A proof of the lemma can be found in [1, pp. 55–57].

LEMMA 2.4. *Let $g(x)$ be a polynomial with integral coefficients and let $f_i(x)$, $i = 1, 2, \dots, m$ be the irreducible factors of $T(x) = 1 + x + \cdots + x^{v-1}$. Furthermore, let* GCD $(n, v) = 1$. *Assume that for each $f_i(x)$, there exists a polynomial $S_i(x)$ with integral coefficients, such that*

$$g(x) \equiv nS_i(x) \qquad (\bmod f_i(x)).$$

Then there exist polynomials $R(x)$ and $A(x)$, both with integral coefficients, such that

$$g(x) = nR(x) + A(x)\,T(x).$$

Now, we are ready to prove the next theorem.

THEOREM 2.5 (Multiplier Theorem). *Let A be a nontrivial (v, k, λ, g)-addition set and let n_0 be a divisor of d, where $(n_0, v) = 1$, and $n_0 > \lambda$. If, for every prime p dividing n_0, there is an integer j_p such that*

$$p^{j_p} \equiv t \qquad (\bmod v),$$

then t is a multiplier for A.

Proof. First of all, let us note that when the assumption of the theorem is satisfied, d is nonnegative. If d is negative, then we have

$$n_0 > \lambda \geqslant |\, d \,|,$$

which is impossible.

From

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\bmod x^v - 1)$$

comes the factorization

$$\theta(x)\,\theta(x^g) \equiv d = n_0 n_1 \qquad (\bmod f_i(x)), \tag{2.4}$$

where $f_i(x)$ is any one of the distinct irreducible factors of $T(x) = 1 + x + \cdots + x^{v-1}$ over the rational field Q. Let $\xi = e^{2\pi ij/v}$ be that root of $f_i(x)$ for which j is least positive. Congruence (2.4) gives the factorization

$$\theta(\xi)\,\theta(\xi^g) = n_0 n_1 . \tag{2.5}$$

Let us take a rational prime p which divides n_0. Then p divides $\theta(\xi)\,\theta(\xi^g)$. Now if P is any prime ideal divisor of p, then we also have P dividing the ideal generated by $\theta(\xi)\,\theta(\xi^g)$. However, P is fixed by the automorphism α of the field $Q(\xi)$ determined by $\xi \to \xi^p$. Hence P divides $\theta(\xi)\,\theta(\xi^{gp})$. Since $p^{j_p} \equiv t\ (\bmod v)$ by assumption, we have that P divides $\theta(\xi)\,\theta(\xi^{gt})$.

The above observation is true for any rational prime p which divides n_0. Hence we have n_0 divides $\theta(\xi)\,\theta(\xi^{gt})$. That is,

$$\theta(x)\,\theta(x^{gt}) \equiv n_0 S_i(x) \qquad (\operatorname{mod} f_i(x)),$$

where $S_i(x)$ has rational integral coefficients. There is such a congruence for each irreducible factor $f_i(x)$ of $T(x)$. By Lemma 2.4, there exist polynomials $R(x)$ and $A(x)$, both with integral coefficients, such that

$$\theta(x)\,\theta(x^{gt}) = n_0 R(x) + A(x)\,T(x). \tag{2.6}$$

Equation (2.6) when taken modulo $x^v - 1$ becomes

$$\theta(x)\,\theta(x^{gt}) \equiv n_0 R(x) + A(1)\,T(x) \qquad (\operatorname{mod} x^v - 1). \tag{2.7}$$

Let $x = 1$ in the congruence (2.7); then we have

$$k^2 = n_0 R(1) + A(1)\,v.$$

Since $k^2 = d + \lambda v$ and GCD $(n_0, v) = 1$, we have

$$A(1) \equiv \lambda \qquad (\operatorname{mod} n_0).$$

Thus, by altering $R(x)$ if necessary, we have

$$\theta(x)\,\theta(x^{gt}) \equiv n_0 R(x) + \lambda T(x) \qquad (\operatorname{mod} x^v - 1). \tag{2.8}$$

Now every coefficient on the left side of this congruence is nonnegative and since $n_0 > \lambda$ all the coefficients of $R(x)$ are nonnegative also. Further, with $x = 1$, this congruence gives $k^2 = n_0 R(1) + \lambda v$; thus $R(1) = n_1$. Substituting x^g for x in (2.8), we have

$$\theta(x^g)\,\theta(x^{g^2t}) \equiv n_0 R(x^g) + \lambda T(x^g) \qquad (\operatorname{mod} x^{vg} - 1). \tag{2.9}$$

Congruence (2.9) when taken modulo $x^v - 1$ becomes

$$\theta(x^g)\,\theta(x^{g^2t}) \equiv n_0 R(x^g) + \lambda T(x) \qquad (\operatorname{mod} x^v - 1). \tag{2.10}$$

We still have the relationship

$$\theta(x)\,\theta(x^g) \equiv d + \lambda T(x) \qquad (\operatorname{mod} x^v - 1). \tag{2.11}$$

Substituting x^{gt} for x in (2.11) and reducing modulo $x^v - 1$ we obtain

$$\theta(x^{gt})\,\theta(x^{g^2t}) \equiv d + \lambda T(x) \qquad (\operatorname{mod} x^v - 1). \tag{2.12}$$

From (2.8) and (2.10), we obtain

$$\theta(x)\,\theta(x^{g})\,\theta(x^{gt})\,\theta(x^{g^2t})$$

$$\equiv [n_0R(x) + \lambda T(x)][n_0R(x^g) + \lambda T(x)] \qquad (\text{mod } x^v - 1),$$

while (2.11) and (2.12) give

$$\theta(x)\,\theta(x^{g})\,\theta(x^{gt})\,\theta(x^{g^2t}) \equiv [d + \lambda T(x)]^2 \qquad (\text{mod } x^v - 1).$$

Hence

$$n_0^2R(x)\,R(x^g) + 2d\lambda T(x) + \lambda^2 vT(x) \equiv d^2 + 2dT(x) + \lambda^2 vT(x) \qquad (\text{mod } x^v - 1),$$

which implies that

$$R(x)\,R(x^g) \equiv n_1^2 \qquad (\text{mod } x^v - 1).$$

This implies [since $R(x)$ has nonnegative coefficients] that $R(x)$ has only a single nonzero term. Hence $R(x) = n_1x^s$ and

$$x^{s(g+1)} \equiv 1 \qquad (\text{mod } x^v - 1). \tag{2.13}$$

Putting $R(x) = n_1x^s$ in (2.8), we have

$$\theta(x)\,\theta(x^{gt}) \equiv dx^s + \lambda T(x) \qquad (\text{mod } x^v - 1).$$

Multiplying this last congruence by $\theta(x^t)$ and simplifying yields

$$\theta(x) \equiv x^s\theta(x^t) \qquad (\text{mod } x^v - 1),$$

which implies that t is a multiplier of the addition set and that $tA = A - s$. Hence the proof is completed.

In using a multiplier t in the construction of an addition set, we cannot assume that the set is fixed by the multiplier. For example, $t = -1$ is the only nontrivial multiplier for the (8, 3, 1, 3)-addition set {0, 1, 2}. However, $t = -1$ fixes no addition set with the same parameters. Hence, (2.13) is of some interest. It states that the shift s must satisfy

$$s(g + 1) \equiv 0 \qquad (\text{mod } v).$$

In particular, when GCD $(g + 1, v) = 1$, $s \equiv 0$ (mod v).

If GCD $(t - 1, v) = 1$, then the multiplier t fixes a shift of the addition set A. If $tA \equiv A + s$ (mod v), then the shift of A by $-s(t - 1)^{-1}$ is fixed by the multiplier.

In the next section we will develop some nonexistence theorems.

3. Nonexistence Theorems

One of the difficulties with any computer search is the number of cases one has to consider. In this section, we will try to reduce the number of possible parameter sets that we have to consider in a search for addition sets.

Most of the results in this section are on the parameter g. So far, we know that if the addition set is nontrivial and $d \neq 0$, then GCD $(g, v) = 1$. In [5], we have also seen that we only need to consider those g's in the range $0 \leqslant g \leqslant v - 1$, and that there is no nontrivial solution for $g = 1$. To further reduce the possible values of g, we need the following lemma.

Lemma 3.1. *Let A be a nontrivial (v, k, λ, g)-addition set. Then it is also a (v, k, λ, g^{-1})-addition set.*

Proof. Since A is nontrivial, GCD $(g, v) = 1$ and we can talk about the inverse of g. Let f be the order of g modulo v [f is the smallest integer such that $g^f \equiv 1 \pmod{v}$]. Then g^{-1} is $g^{f-1} \pmod{v}$. The Hall-polynomial of A satisfies

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^v - 1). \quad (3.1)$$

Substituting $x^{g^{f-1}}$ for x in (3.1) gives

$$\theta(x^{g^{f-1}})\,\theta(x) \equiv d + \lambda(1 + x^{g^{f-1}} + \cdots + x^{g^{f-1}(v-1)}) \qquad (\operatorname{mod} x^{vg^{f-1}} - 1),$$

which when reduced modulo $x^v - 1$ gives

$$\theta(x^{g^{f-1}})\,\theta(x) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^v - 1).$$

Hence A is also a (v, k, λ, g^{-1})-addition set.

Theorem 3.2. *Let A be a nontrivial (v, k, λ, g)-addition set with $d \neq 0$ and let the order of g modulo v be f. Then f is even and A is also a $(v, k, \lambda, g^{2i+1})$-addition set for $i = 0, 1,..., (f/2) - 1$.*

Proof. We will prove that A is a $(v, k, \lambda, g^{2i+1})$-addition set by induction on i. It is clearly true when $i = 0$. Suppose that A is a $(v, k, \lambda, g^{2i+1})$-addition set. Since A is still a (v, k, λ, g)-addition set, Theorem 2.1 implies that $g^{2(i+1)}$ fixes A. Lemma 3.1 implies that A is also a (v, k, λ, g^{-1})-addition set. Applying Theorem 2.1 again we have that A is a $(v, k, \lambda, g^{2i+3})$-addition set.

If f is odd, then there exist i such that $2i + 1 = f$. In this case, A will also be an addition set with $g = 1$. However in [3], it was proved that there is no nontrivial addition set with $g = 1$. Hence f is even, and the theorem is proved.

COROLLARY 3.3. *Let A be a nontrivial (v, k, λ, g)-addition set and let the order of g modulo v be f where $f = 2^r s$ and s is odd. Then A is also a (v, k, λ, g^s)-addition set. Moreover, the order of g^s modulo v is 2^r.*

Proof. Since f is even, $r > 0$. Hence $s < f$, and there exist i such that $2i + 1 = s$. Thus the corollary follows from the theorem.

Corollary 3.3 means that in deciding whether an addition set exists for some given parameters v, k and λ we only need to consider those g's whose orders modulo v are powers of 2.

Corollary 3.3 also implies the following result. Here $\varphi(v)$ stands for the Euler φ-function.

COROLLARY 3.4. *There is no nontrivial (v, k, λ, g)-addition set with $d \neq 0$, $d + \lambda < k$ and 2 strictly dividing $\varphi(v)$.*

Proof. Since 2 strictly divides v, the only g's whose orders modulo v are powers of 2 are ± 1. But there is no nontrivial solution for $g = 1$, and $g = -1$ corresponds to a difference set which contradicts the condition $d + \lambda < k$.

If v is a prime of the form $4v + 3$, then 2 strictly divides $\varphi(v) = v - 1$. The above corollary eliminates cases like $v, k, \lambda, d = 23, 5, 1, 2$ and $v, k, \lambda, d = 47, 7, 1, 2$.

The next theorem is a generalization of a result by Mann [6]. Here, when w divides v, we define a *w-multiplier* of a (v, k, λ, g)-addition set to be any integer t, prime to w, for which there exists an integer s satisfying

$$\theta(x^t) \equiv x^s \theta(x) \qquad (\text{mod } x^w - 1),$$

where $\theta(x)$ is the Hall-polynomial for the addition set.

THEOREM 3.5. *Let $w > 1$ be a divisor of v and assume a nontrivial (v, k, λ, g)-addition set exists with w-multiplier $t \geqslant 1$. Let p be a prime divisor of d for which $(p, w) = 1$. If there exists an integer $f \geqslant 0$ such that $tp^f \equiv g$ modulo w, then d is strictly divisible by an even power of p.*

Proof. Let P be a prime ideal divisor of p in $K(\xi_w)$ and let P^i strictly divide $\theta(\xi_w)$. Since t is a w-multiplier, P^i strictly divides $\theta(\xi_w{}^t)$. By Theorem 2.3, P is fixed by the mapping $\xi_w \to \xi_w{}^p$. Hence P^i strictly divides $\theta(\xi_w^{tp})$. Since $tp^f \equiv g$ modulo w, we have P^i strictly dividing $\theta(\xi_w{}^g)$. Since $\theta(\xi_w)\, \theta(\xi_w{}^g) = d$, P^{2i} strictly divides d, and this implies by Theorem 2.3 that d is strictly divisible by an even power of p.

Theorem 3.5 is often used with $t = 1$, the trivial multiplier. For example, the case $v, k, \lambda, d = 33, 8, 2, -2$ is eliminated by this theorem.

The next nonexistence result is a generalization of a result by Turyn [7]. Let us first quote a part of his proof as a lemma.

LEMMA 3.6. *Let $\theta(x) = \sum_{i=0}^{w-1} a_i x^i$ be a polynomial with integral coefficients. Furthermore, let us assume that the a_i's satisfy $0 \leqslant a_i \leqslant A$ for some integer A, and that $\theta(\xi_w{}^j) \equiv 0$ modulo m for $1 \leqslant j \leqslant w - 1$. If* GCD $(m, w) = 1$, *then $m \leqslant A$. If* GCD $(m, w) > 1$, *then $m \leqslant 2^{r-1}A$, where r is the number of distinct prime factors of* GCD (m, w).

We still need the following definitions. Let p be a prime and let p^l strictly divide the integer w, that is, let $w = p^l w_1$ with GCD $(p, w_1) = 1$. If there exists an integer $f > 0$ such that $p^f \equiv g \pmod{w_1}$, then p is said to be *g-conjugate modulo w*. If all the prime divisors of an integer m are g-conjugate modulo w, then m is said to be *g-conjugate modulo w*. Note that if m is g-conjugate modulo w, then it is also g-conjugate modulo any divisor of w.

THEOREM 3.7. *Assume a nontrivial (v, k, λ, g)-addition set exists. Let m^2 divide d and suppose that $m > 1$ is g-conjugate modulo w for some divisor $w > 1$ of v. If* GCD $(m, w) = 1$ *then $m \leqslant (v/w)$. If* GCD $(m, w) > 1$ *then $m \leqslant 2^{r-1}(v/w)$ where r is the number of distinct prime factors of* GCD (m, w).

Proof. Since GCD $(g, v) = 1$ and m is g-conjugate modulo w, every prime ideal divisor of m is fixed in the field $Q(\xi_w)$ by the mapping $\xi_w \to \xi_w{}^g$. Let $\theta(x)$ be the Hall-polynomial of the addition set. Then $\theta(\xi_w)\,\theta(\xi_w{}^g) = d$. Hence every prime ideal divisor of m divides both $\theta(\xi_w)$ and $\theta(\xi_w{}^g)$, which implies that $\theta(\xi_w) \equiv 0$ modulo m. Similarly it follows that $\theta(\xi_w{}^j) \equiv 0$ modulo m for $1 \leqslant j \leqslant w - 1$. Further, if we let

$$\theta(x) \equiv \sum_{i=0}^{w-1} a_i x^i \qquad (\operatorname{mod} x^w - 1),$$

then $0 \leqslant a_i \leqslant v/w$. The theorem then follows from Lemma 3.6.

For example, Theorem 3.7 implies that the case $v, k, \lambda, d = 32, 6, 1, 4$ does not exist. Here, we let $w = 32$ and $m = 2$. It is clear that 2 is g-conjugate modulo 32 for any g relatively prime to 32. Since the parameters correspond to a nontrivial case, those g's are all that need to be considered. Theorem 3.7 implies that $2 \leqslant 1$, a contradiction.

The next result is quoted from [4]. Here, the Legendre symbol $(-1/p)$ stands for $(-1)^{(p-1)/2}$, and $\tau(v)$ is the number of divisors of v.

THEOREM 3.8. *The rational polynomial congruence relation*

$$\theta(x)^2 \equiv d + \lambda(1 + x + \cdots + x^v) \qquad (\text{mod } x^v - 1) \tag{3.2}$$

has a solution if and only if

(i) *$d + \lambda v$ is a rational square, and*

(ii) *d is a rational square unless v is a power of an odd prime p, in which case it can also be the product of a rational square with $(-1/p)\,p$. Moreover, if a solution exists, then the number of different $\theta(x)$'s modulo $x^v - 1$ which satisfy (3.2) is 2^f, where f is given by*

$$f = \begin{cases} 0 & \text{for } d = 0 \text{ and } d + \lambda v = 0, \\ 1 & \text{for } d = 0 \text{ and } d + \lambda v \neq 0, \\ \tau(v) - 1 & \text{for } d \neq 0 \text{ and } d + \lambda v = 0, \\ \tau(v) & \text{for } d \neq 0 \text{ and } d + \lambda v \neq 0. \end{cases}$$

It should be noted that all the 2^f solutions can be constructed (see [4]). In the case of a (v, k, λ, g)-addition set, its Hall-polynomial satisfies

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\text{mod } x^v - 1). \tag{3.3}$$

If for some divisor w of v, $g \equiv 1 \pmod{w}$, then (3.3) when reduced modulo $x^w - 1$ becomes

$$\theta(x)^2 \equiv d + (\lambda v/w)(1 + x + \cdots + x^{w-1}) \qquad (\text{mod } x^w - 1). \tag{3.4}$$

Hence Theorem 3.8 implies the following result.

COROLLARY 3.9. *Let A be a (v, k, λ, g)-addition set where $g \equiv 1 \pmod{w}$ and w is a divisor of v. If d is not a square, then w is a power of an odd prime p, and the square free part of d is $(-1/p)\,p$, where $(-1/p)$ is the Legendre symbol.*

For example, Corollary 3.9 can be used to eliminate the case $v, k, \lambda, d, g = 33, 6, 1, 3, 10$.

4. A LIST WITH $k \leqslant 10$

In this section, we shall discuss briefly the methods used to obtain a list of addition sets with $k \leqslant 10$. There remains one unsolved case with parameters $v, k, \lambda, d = 95, 10, 1, 5$. The various tests imply that to solve this case we only have to consider $g = 18$ and $g = 56$, both of which are computationally too expensive to do by methods discussed in this section.

Our aim is to determine the parameter sets v, k and λ that correspond to nontrivial addition sets. The parameter d is known once v, k and λ are given (Theorem 1.1). It is easy to see that if A is nontrivial addition set, its complement consisting of all the residues modulo v that are not in A is again an addition set. Hence we can restrict ourselves to $k \leqslant v/2$.

We first generate all the parameter sets that satisfy the conditions in Theorems 1.1 and 1.4. Those parameter sets with $d = 0, 1$ and -1 correspond to the Natural Central Groupoid type, the Reyser type and the Shifted Ryser type, respectively [5]. The parameter sets with $d = k - \lambda$ are parameters for difference sets and we can refer to the table in [1] to determine whether they exist. It is the ramaining parameter sets that we will consider from here on.

For those parameter sets, we generate a set of g's that need to be considered. Corollary 3.3 says that we need only those g's whose orders modulo v are powers of 2. Besides, we need not consider g's that are ± 1, Some cases are eliminated in this step.

Next, we apply the tests of Theorems 3.5 and 3.7 to the remaining cases. After these two tests, there are still 13 parameter sets of v, k and λ left. Two of the parameters sets correspond to the Negative Quadratic Residue type (see [5]).

A constructive approach is used in the remaining cases. In many case, a nontrivial multiplier exists as a result of either Corollary 2.2 or Theorem 2.5, or both. We use the multipliers from Theorem 2.5 if possible. Multipliers are used to partition the residues modulo v into cycles. Then some combinations of these cycles are tested to determine whether they are addition sets. The longer the length of the cycles, the fewer combinations there are. Multipliers from Theorem 2.5 usually give longer cylces, and are better suited for computation. However, in all cases where the multiplier method applies, it is found that there are no possible addition sets. After this step, there are five cases left.

Next, we use Corollary 3.9 to eliminate two of the cases. The remaining three cases are

v	k	λ	d	g
30	8	2	4	7, 11
60	8	1	4	7, 11, 13, 29, 41
95	10	1	5	18, 56

We now use the construction in Theorem 3.8. If a (v, k, λ, g)-addition set exists where $g \equiv 1 \pmod{w}$ for a divisor w of v, then its Hall-polynomial $\theta(x)$ satisfies (3.2). Besides, $\theta(x)$ when reduced modulo $x^w - 1$

TABLE I

Addition Sets

v	k	λ	d	g		Class
4	2	1	0	2		NCG
	*0	1				
5	2	1	−1	2		SR = NQ
	*2	3				
7	3	1	2	−1		DS
	*1	2	4			
8	3	1	1	3		R
	*0	1	2			
9	3	1	0	3		NCG
	*0	1	2			
8	4	2	0	4		NCG
	*0	1	2	3		
13	4	1	3	−1		DS
	*0	1	3	9		
15	4	1	1	4		R
	*0	1	2	3		
16	4	1	0	4		NCG
	*0	1	2	3		
17	4	1	−1	4		SR
	*7	8	9	10		
17	4	1	−1	2		NB
	*1	4	13	16		
11	5	2	3	−1		DS
	*1	3	4	5	9	
12	5	2	1	5		R
	*0	1	2	3	4	
13	5	2	−1	−5		SR
	*0	1	2	11	12	
21	5	1	4	−1		DS
	*3	6	7	12	14	
24	5	1	1	5		R
	*0	1	2	3	4	

Key. NCG = National Central Groupoid [5, Theorem 3.1], R = Ryser [5, Theorem 3.2], SR = Shifted Ryser [5, Theorem 3.3], NQ = Negative Quadratic Residue [5, Theorem 3.5], NB = Negative Biquadratic Residue [5, Theorem 3.5], DS = Difference set.

Table continued

TABLE I (*continued*)

v	k	λ	d	g		Class		
25	5	1	0	5		NCG		
	*0	1	2	3	4			
12	6	3	0	6		NCG		
	*0	1	2	3	4	5		
13	6	3	−3	2		NQ		
	*1	3	4	9	10	12		
18	6	2	0	6		NCG		
	*0	1	2	3	4	5		
31	6	1	5	−1		DS		
	*1	5	11	24	25	27		
35	6	1	1	6		R		
	*0	1	2	3	4	5		
36	6	1	0	6		NCG		
	*0	1	2	3	4	5		
37	6	1	−1	6		SR		
	*16	17	18	19	20	21		
15	7	3	4	−1		DS		
	*0	1	2	4	5	8	10	
16	7	3	1	7		R		
	*0	1	2	3	4	5	6	
24	7	2	1	7		R		
	*0	1	2	3	4	5	6	
25	7	2	−1	7		SR		
	*0	1	2	3	22	23	24	
48	7	1	1	7		R		
	*0	1	2	3	4	5	6	
49	7	1	0	7		NCG		
	*0	1	2	3	4	5	6	
16	8	4	0	8		NCG		
	*0	1	2	3	4	5	6	7
17	8	4	−4	3		NQ		
	*1	2	4	8	9	13	15	16
21	8	3	1	8		R		
	*0	1	2	3	4	5	6	7
32	8	2	0	8		NCG		
	*0	1	2	3	4	5	6	7
57	8	1	7	−1		DS		
	*1	6	7	9	19	38	42	49

Table continued

TABLE I (*continued*)

v	k	λ	d	g		Class				
63	8	1	1	8		R				
	*0	1	2	3	4	5	6	7		
64	8	1	0	8		NCG				
	*0	1	2	3	4	5	6	7		
65	8	1	−1	8		SR				
	*29	30	31	32	33	34	35	36		
19	9	4	5	−1		DS				
	*1	4	5	6	7	9	11	16	17	
20	9	4	1	9		R				
	*0	1	2	3	4	5	6	7	8	
27	9	3	0	9		NCG				
	*0	1	2	3	4	5	6	7	8	
37	9	2	7	−1		DS				
	*1	7	9	10	12	16	26	33	34	
40	9	2	1	9		R				
	*0	1	2	3	4	5	6	7	8	
41	9	2	−1	9		SR				
	*0	1	2	3	4	37	38	39	40	
73	9	1	8	−1		DS				
	*1	2	4	8	16	32	37	55	64	
80	9	1	1	9		R				
	*0	1	2	3	4	5	6	7	8	
81	9	1	0	9		NCG				
	*0	1	2	3	4	5	6	7	8	
20	10	5	0	10		NCG				
	*0	1	2	3	4	5	6	7	8	9
25	10	4	0	10		NCG				
	*0	1	2	3	4	5	6	7	8	9
33	10	3	1	10		R				
	*0	1	2	3	4	5	6	7	8	9
50	10	2	0	10		NCG				
	*0	1	2	3	4	5	6	7	8	9
91	10	1	9	−1		DS				
	*0	1	3	9	27	49	56	61	77	81
99	10	1	1	10		R				
	*0	1	2	3	4	5	6	7	8	9
100	10	1	0	10		NCG				
	*0	1	2	3	4	5	6	7	8	9
101	10	1	−1	10		SR				
	*46	47	48	49	50	51	52	53	54	55

still has nonnegative integral coefficients. So we construct all the possible solutions to

$$\theta(x)^2 \equiv d + \lambda(1 + x + \cdots + x^{w-1}) \qquad (\mathrm{mod}\, x^w - 1)$$

for an appropriate w. In some cases like $v, k, \lambda, g = 30, 8, 1, 11$, none of the solutions have nonnegative coefficients. The cases now remaining are

v	k	λ	d	g
30	8	2	4	7
60	8	1	4	7
95	10	1	5	18, 56

The last step also shows that the two possible Hall-polynomials reduced modulo $x^6 - 1$ for both $(v, k, \lambda, g) = (30, 8, 2, 7)$ and $(60, 8, 1, 7)$ are $3 + x + x^2 + x^3 + x^4 + x^5$ and $1 + x + x^2 + 3x^3 + x^4 + x^5$. Next, we use the fact that 7^2 is a multiplier fixing both addition sets. Cycles are generated. For the case (30, 8, 2, 7) there are four possible sets whose Hall-polynomials when reduced modulo $x^6 - 1$ give the above polynomials. For the case (60, 8, 1, 7) there are more possibilities. Then it is a simple matter of testing whether these sets satisfy the definitions of an addition sets. None of them do.

The constructive method of Theorem 3.8 does not apply to the case (95, 10, 1, 18). For the case (95, 10, 1, 56), the two possible Hall-polynomials reduced modulo $x^5 - 1$ are $2 + x + 3x^2 + 3x^3 + x^4$ and $2 + 3x + x^2 + x^3 + 3x^4$.

Table I is a list of all known addition sets for which $k \leqslant 10$. The question of the existence of multiple inequivalent addition sets has not been considered. Each addition set is identified by v, k, λ, d, g and by a class indicator which indicates its type. The addition set itself is given in the following line with an "*."

References

1. L. D. Baumert, "Cyclic Difference Sets," Lecture Notes in Mathematics, Vol. 182, Springer–Verlag, Berlin, 1971.
2. M. Hall, Jr., A survey of difference sets, *Proc. Amer. Math. Soc.* 7 (1956), 975–986.
3. W. H. Lam, Rational g-circulants satisfying the matrix equation $A^2 = dI + \lambda J$, Ph.D. Thesis, California Institute of Technology, 1974.
4. W. H. Lam, On rational circulants satisfying $A_a = dI + \lambda J$, *Linear Algebra and Appl.* to appear.
5. C. W. H. Lam, A generalization of cyclic difference sets I, *J. Combinatorial Theory*, **19** (1975), 51–65.
6. H. B. Mann, Balanced incomplete block designs and Abelian difference sets, *Illinois J. Math.* **8** (1964), 252–261.
7. R. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.