A list of representative simple difference sets of the Singer type for small orders m.

Wolfdieter Lang [1]
Karlsruhe
Germany
July 2020
wolfdieter.lang@partner.kit.edu

Abstract

The representative difference sets of order m, of special *Singer* type $(m^2+m+1, m+1, 1)$, for m a power of a prime number are listed for $m = 1, 2, 3, 4, 5, 7, 8, 9, 11, 13$ and 16.

1 Introduction

Difference sets [4], [5], [6], related to the additive group $(\mathbb{Z}_v, +)$ (integers modulo v, using the $+$ part of the ring $\mathbb{Z}/v\mathbb{Z}$) are denoted by (v, k, λ), with $2 \leq k < v$, with $k \in \mathbb{N}$ and $\lambda \in \mathbb{N}$. The smallest nonnegative complete residue system of $(\mathbb{Z}_v, +)$ is $RS(v) = \{0, 1, 2, ..., v-1\}$. A difference set (v, k, λ) in $RS(v)$ is a subset $D \subseteq RS(v)$ satisfying (i) $|D| = k$, (ii) the multiset $[x - y \,|\, x, y \in D, x \neq y]$, with $k\,(k-1)$ elements, contains each element of $RS(v) \setminus (0)$ exactly λ times. (With [4] we use the notation $[MS]$ for multisets and $\{S\}$ for sets, and order the elements from $RS(v)$ increasingly.). Obviously $r := \lambda\dfrac{v-1}{k-1} = k$. In the following only simple difference sets with $\lambda = 1$ are considered, and the multiset in (ii) becomes a set.

The interest is in the development $Dev(D)$ of a given difference set D in the additive Abelian group $RS(v)$ (this is in fact a ring, even a field for prime v) by adding element-wise all $v-1$ positive elements of $RS(v)$, computing modulo v. This produces translates of D, named D_j if j is added, and the set $Dev(D) = \{D = D_0, D_1, , ..., D_{v-1}\}$ of v difference sets, each of size k. This defines an equivalence relation $D_1 \sim D_2$ if $D_1 \in Dev(D_2)$. Thus $Dev(D)$ defines a class. The number of equivalence classes is denoted here by $c = c(v, k, \lambda)$.

A counting argument shows that the replication number r, the number of D_js of $Dev(D)$ in which each chosen element of $RS(v)$ appears, is the $r = r(v, k, \lambda)$ as given above.

Example 1: A $(7, 3, 1)$ difference set in $RS(7)$ is D$=\{1, 2, 4\}$, with $r = 3$. The 6 translates are $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 0\}$, $\{5, 6, 1\}$, $\{6, 0, 2\}$ and $\{0, 1, 3\}$. $Dev(D)$ becomes, independent of the D_j one starts with, after reordering the D_js, a set of $v = 7$ difference sets in lexicographical order called here $DS_1(7, 3, 1)$.

[1] http://www.itp.kit.edu/~wl

$DS_1(7,3,1) = \{\{0,\ 1,\ 3\},\ \{0,\ 2,\ 6\},\ \{0,\ 4,\ 5\},\ \{1,\ 2,\ 4\},\ \{1,\ 5,\ 6\},\ \{2,\ 3,\ 5\},\ \{3,\ 4,\ 6\}\}$.

$|DS_1(7,3,1)| = v = 7$, $|D_j| = k = 3$, and *e.g.*, 0 appears exactly in $r = 3$ difference sets D_0, D_1, D_3, similar for other numbers from $RS(7)$.

The class number is $c = 2$ because the difference set $\widehat{D} = \{0,\ 1,\ 5\}$, with $Dev(\widehat{D}) = \{\{0,\ 1,\ 5\},\ \{0,\ 2,\ 3\},\ \{0,\ 4,\ 6\},\ \{1,\ 2,\ 6\},\ \{1,\ 3,\ 4\},\ \{2,\ 4,\ 5\},\ \{3,\ 5,\ 6\}\}$, named $DS_2(7,3,1)$. The representatives of the two classes will later be taken as the difference sets with elements 0 and 1, *i.e.*, $\{0,\ 1,\ 3\}$ and $\{0,\ 1,\ 5\}$. There are no other classes, assuming the later formula for the classes.

The two classes are isomorphic, *e.g.*, the permutation $\pi = (0)\,(1,5,3)\,(2,4)\,(6)$ of order 6 maps $DS_1(7,3,1) \to DS_2(7,3,1)$, and vice versa with $\pi^{-1} = (0)\,(1,3.5)\,(2,4)\,(6)$.

Note that there are $168 = 2^2 \cdot 3 \cdot 7$ automorphism of the projective *Fano* plane (the number of three from the seven points which cannot lie on one line using the projective plane requirements). But not all may be difference sets, see *e.g.*, [4] Fig. 1.1., p. 3 (with point labels -1 to be from $RS(7)$). This is a special block design (a $symsBIBD$, see later) but the block $\{0,\ 1,\ 2\}$ cannot be an element of a difference set $(7,3,1)$ in $RS(7)$ (because the difference 1 appears twice).

See also the isomorphism α between this $symsBIBD$ Figure and the present Figure 1 (the $DS_1(7,3,1)$) given as Example 1.20. in [4], p. 9, if the $\{a,b,c,d,e,f,g\}$ are renamed as $RS(7)$.

Each of the two examples gives the projective *Fano* plane. For $DS_1(7,3,1)$ see *Figure 1*, with $v = 7$ points and 7 lines, where each line has exactly 3 points (k = 3), and each point is intersected by exactly 3 lines (r = k). Here $v = m^2 + m + 1$, and $k = m + 1$, for $m = 2$. This is an example of a *Singer* [3] difference set $(m^2 + m + 1, m + 1, 1)$ where m is a power of a prime.

In *Figure 2* this *Fano* plane is drawn as a planar graph with nodes (vertices) 0, 1, 2, 3, 4, 5, 6 of order 3, 3, 3, 5, 5, 6, 5, respectively. See A335862 for the adjacency matrix of this graph, and its characteristic polynomial $\Phi(x) = x^7 - 15\,x^5 - 26\,x^4 + 3\,x^3 + 24\,x^2 + 2\,x - 6 = (x^3 - 2\,x^2 - 10\,x - 6)\,(x^2 + x - 1)^2$. The zeros of the cubic polynomial are given in $x1 =$ A335862, $x2 = -$A335863 and $x3 = -$A335864. The other zeros are twice $-1 + \varphi$, and twice $-\varphi$, with the golden section $\varphi =$ A001622.

Such difference sets in $RS(v)$ with their development $Dev(D)$, called here $DS(v,k,\lambda)$ (now for any $\lambda \in \mathbb{N}$), are symmetric balanced incomplete block designs ($symBIBD$s) $(RS(v), Dev(D))$.

A block design (BD) (see,e.g., [4]) denoted by (X, A) is (i) a set X of elements called points and (ii) a multiset A (with possibly repeated elements) of nonempty subset of X, called blocks. If the multiset is a set the BD is called simple, denoted by sBD.

A $BIBD$, a *balanced incomplete block design*, denoted by (v,k,λ), with $v > k \geq 2$, is a BD (X, A) with (a) $|X| = v$, (b) $|B_i| = k$, for each block $B_i \in A$, and (c) each pair of points (x, y), with $x \neq y$, is contained in exactly λ blocks. If $\lambda = 1$ the $BIBD$ is simple, denoted by $sBIBD$.

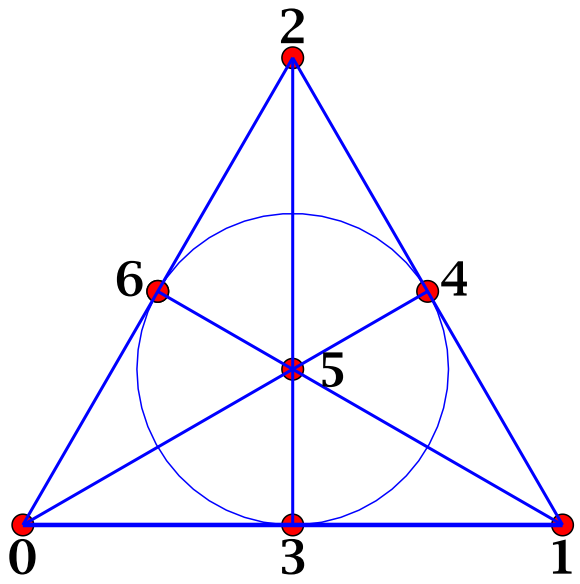

Figure 1

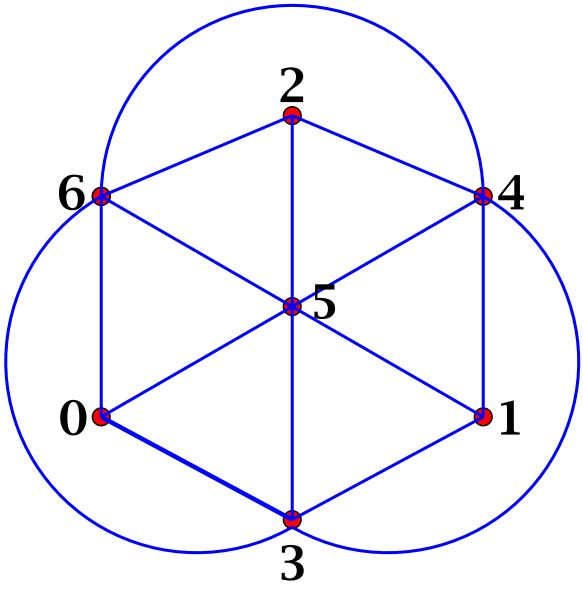

Figure 2

Figure 1: The projective plane $(7, 3, 1)$, the *Fano* plane.

Figure 2: The Fano plane shown as a planar graph.

The counting for a $BIBD$ shows that the replication number r (the number of blocks in which each point of X appears) is $r = \lambda\dfrac{v-1}{k-1} = k$, and the number of blocks $b = |A|$ is $b = \dfrac{v\,r}{k} = \lambda\,\dfrac{v\,(v-1)}{k\,(k-1)}$, (see *Theorems* 1.8. and 1.9. in [4], pp. 4 - 5). Sometimes $BIBD$s are denoted here by $(v, k, \lambda; b, r)$. *E.g.*, the *Fano* plane is then written as $(7, 3, 1; 7, 3)$. The requirement $k < v$ explains the name incomplete, and (c) is the balance property. The notation v originates from varieties ([4]. p. 2).

If $v = b$ the $BIBD$ is called symmetric, denoted by $symBIBD$. The *Fano* plane is then a $symsBIBD$ (symmetric and simple).

Due to this connection between a $Dev(D)$ with the group $(\mathbb{Z}_v.+)$ and a $symBIBD$ the property (ii) of the BD tells that each distinct pair of numbers from $RS(v)$ appears in precisely λ difference sets D_i. *E.g.*, in $DS_1(7, 3, 1)$ the pair $(4, 5)$ appears only in D_3 $(\lambda = 1)$.

The card game *Dobble* (or *Spot it!*) [2] (in German), [7] (in German), [1], uses 55 cards, each with 8 distinct symbols, and each pair of cards has precisely one symbol in common, which has to be detected (in various ways of playing the game). If one uses the simple difference sets of the *Singer* type from $DS(v, 8, 1)$ to represent the 8 symbols from the repertoire of v given symbols, one would use $v = 57$ cards, for the projective plane of order 7, that is $(57, 8, 1)$. Therefore in a Dobble game with only 55 (or in a junior version 30 instead of 31) two cards (or one card) could be added to complete a $symsBIDB$.

For difference sets in an Abelian group (here $(\mathbb{Z}_v, +)$) also element-wise multiplication with positive integers n are very useful: $n\,D := \{n\,x \,|\, x \in D\}$. This means the sum of n times x (taken always modulo v). If $n\,D \in Dev(D)$, *i.e.*, $n\,D = D + y$, for some $y \in RS(v)$, then n

is called a *multiplier*. If $n\,D = D$ then D is a fixed point under the map $\alpha : RS(v) \to RS(v)$, $x \mapsto n\,x$, or D is fixed by the multiplier n. See [4] sect. 3.4, pp. 54 - 58.

There are theorems on multipliers which allow one to find difference sets in $(\mathbb{Z}_v, +) = RS(v)$. First of all, if n is a multiplier of a difference set in $R(v)$ then $\gcd(n, v) = 1$ ([4], Lemma 3.31, p. 55), but the reverse is false. It is clear that if D is difference set in $RS(v)$ and n is a multiplier then the above defined map α is an automorphism of $Dev(D)$, or $\alpha \in Aut(R(v), Dev(D))$. [[4], Lemma 3.32., p. 55].
Important is the so-called

Multiplier Theorem, [[4], Theorem 3.33., pp. 55-56]

If four conditions are satisfied for $D = (v, k, \lambda)$ in $RS(v)$, namely, 1. p is a prime number, 2. $\gcd(p, v) = 1$, 3. $k - \lambda \equiv 0\,(mod\,p)$, and 4. $p > \lambda$, then p is a multiplier.

This will be used later for simple Difference sets of the special sl Singer type of order m ($\lambda = 1$), where point 3. becomes $m \equiv 0\,(mod\,p)$, *i.e.*, $p|m$, and point 4. is automatically satisfied.

From the difference set connection to a $symBIBD$, and property of the map α from above, which fixes always the point $0 \in RS(v)$, a whole block $\widehat{D} \in Dev(D)$ is fixed by a multiplier n [[4], Theorem 3.34., p. 56].

If in addition $\gcd(v, k) = 1$ holds, which for simple *Singer* difference sets of order m applies because $gcd(m^2 + m + 1, m + 1) = gcd(m + 1, 1 + m\,(m + 1)) = gcd(m + 1, 1) = 1$, then there exists in $Dev(RS(v)$ a difference set $\widehat{D}$ that is fixed by each multiplier ([4], *Theorem* 3.35., p. 5).

Example 2: A *Singer* difference set of order $m = 3$ is $D = \{0, 1, 5, 11\}$, the representative of a class Dev(D). Prime 2 does not satisfy the conditions because it does not divide m. But prime 3 satisfies all four conditions and also the additional $\gcd(v, k) = 1$ holds. Thus there must be a fixed $\widehat{D} \in Dev(D)$, in fact, this is $\widehat{D} = \{0, 4, 10, 12\}$. See the later *Example 3* for more details.
Are there other multipliers of D (not guaranteed from the lemmata and theorems above)? Such a multiplier would have also to fix $\widehat{D}$. *E.g.*, each positive integer power of 3 will also do it. One calculates modulo 13, so only 3 and 9 need to be checked as multipliers of D. But with multiplier 3 all expected classes are already found.
Note that multiplication of D with prime 2 (not a multiplier, dividing neither $v = 13$ nor $m = 3$) leads out of class $Dev(D)$ to another class with representative $\{0, 1, 4, 6\}$ (see the later list of representatives for $m = 3$).

The question is how to find any *Singer* difference set D of order m in $RS(v)$. The theorem of *Singer* guarantees the existence provides m is a power of a prime (including 1), *i.e.*, $m \in$ A000961. This can be achieved by assuming the existence of a D and using a multiplier for $DS(m^2+m+1, m+1, 1)$ in $RS(m^2+m+1)$ found from the above *Multiplier Theorem*. One searches for the $\widehat{D}$ in $RS(m^2+m+1)$ fixed by this prime multiplier p. For this one computes orbits of $RS(m^2+m+1)$ elements under repeated multiplication by p. These are disjoint cycles. Because $\widehat{D}$ is fixed it must be built from these cycles such that its length becomes $k = m+1$. There may be different possibilities to combine such cycles. Finally one has to find from these candidates those that are indeed difference sets.

For the *Singer* difference set of order $m = 4$ this is shown in [4], Example 3.36., p. 57. In this case the two candidates produce in fact elements from each of the two classes ($c(21, 5, 1) = 2$), namely {3, 6, 7, 12, 14} and {7, 9, 14, 15, 18}.

Example 3: *Singer* difference set of order 3. The five orbits of $RS(13)$ for multiplier 3 are {0}, {1, 3, 9}, {2, 6, 5}, {4, 12, 10}, and {7, 8, 11}. The length of a difference set is $m+1 = 4$. Therefor the candidates for a fixed $\widehat{D}$ by multiplier 3 need the {0}, and anticipating the class number $c(13, 3, 1) = 4$, one could hope that all 4 candidates are difference sets for these classes. This can be checked by subtracting after ordering increasingly the first member of a (modulo 13) neighboring pair (in general, not present in this example, (12, 0) would also be such a pair, but then 12 would be subtracted) in order to get a representative of a class. Here The first set {0, 1, 3, 9} is already a representative, the others are {0, 1, 8, 10}, {0, 1, 5, 11}, and {0, 1, 4, 6}. Hence all four classes have been reached. It is then trivial to get all members of these four classes (the $Dev(\widehat{D})$s) by adding the numbers 1 to 12 to each representative.

Note that in general not all candidates need to be difference sets, but it is expected that one finds all representatives of each class this way. See the later discussion for $m = 16 = 2^4$ with $v = 273 = 3 \cdot 7 \cdot 13$ with $c(273, 17, 1) = 12$.

2 Representative Singer type symsBIBD

Because every developed difference set $Dev(D) = DS(v, k, \lambda)$ in the additive Abelian group $(\mathbb{Z}_v, +) = RS(v)$ (integers modulo v) is a symmetric balanced incomplete block design $sBIBD$, the balance property (iii) of a simple ($\lambda = 1$) block design guarantees that there is always precisely one difference set $D = D_0$ which has elements 0 and 1 of $RS(v)$ (remember that $v > k \geq 2$). This D_0 of size k will be the taken as class representative from which all $Dev(D_0)$ elements are developed by element-wise addition.

The simple *Singer* type difference set in $(\mathbb{Z}_v, +)$ of order m is $(v(m), m+1, 1)$, with $v(m) = m^2+m+1$, for $m \geq 1$ a power of a prime number (including 1). Hence m is from A000961. If the trivial triangle for $m = 1$ is excluded these $symsBIDB$s $(v(m), m+1, 1; v(m), m+1)$ encode projective planes ([4], p. 27 and pp. 52 - 54). Note that this m restrictions on $(v(m), m+1, 1)$ is only sufficient to obtain difference sets. There may be other ones. But none have been found, as it seems.

For the number of classes of his simple difference sets of order m *Singer*[3] (he called it perfect

difference sets of order $m+1$) gave the conjectured formula $c(v,k,1) \stackrel{?}{=} \frac{\varphi(v)}{3\,n}$ if $m = p^n$, for a prime number p and $n \in \mathbb{N}$, where $\varphi =$ A000010 (*Euler*'s totient). He also conjectured that these are the only simple difference sets in the additive group $(\mathbb{Z}_v, +) = RS(v)$, with $v = m^2 + m + 1$.

We now list the representative simple difference sets $D(v(m), k(m), 1)$ in $RS(v)$ of order $m = m(n) =$ A000961(n), for $n = 1, 2, ..., 11$, with $v(m) = m^2 + m + 1$ and $k(m) = m + 1$. This expands *Singer*'s table.

$\mathbf{m = 1, v = 3, k = 2, c = 1}$. Not a projective plane, a triangle.

{0, 1}.

$\mathbf{m = 2, v = 7, k = 3, c = 2}$. The *Fano* plane.

{0, 1, 3}, {0, 1, 5}.

$\mathbf{m = 3, v = 13, k = 4, c = 4}$.

{0, 1, 3, 9}, {0, 1, 4, 6}, {0, 1, 5, 11}, {0, 1, 8, 10}.

$\mathbf{m = 4, v = 21 = 3 \cdot 7, k = 5, c = 2}$.

{0, 1, 4, 14, 16}, {0, 1, 6, 8, 18}.

$\mathbf{m = 5, v = 31, k = 6, c = 10}$.

{0, 1, 3, 8, 12, 18}, {0, 1, 3, 10, 14, 26}, {0, 1, 4, 6, 13, 21}, {0, 1, 4, 10, 12, 17},
{0, 1, 6, 18, 22, 29}, {0, 1, 8, 11, 13, 17}, {0, 1, 11, 19, 26, 28}, {0, 1, 14, 20, 24, 29},
{0, 1, 15, 19, 21, 24}, {0, 1, 15, 20, 22, 28}.

$\mathbf{m = 7, v = 57 = 3 \cdot 19, k = 8, c = 12}$.

{0, 1, 3, 13, 32, 36, 43, 52}, {0, 1, 4, 9, 20, 22, 34, 51} {0, 1, 4, 12, 14, 30, 37, 52}
0, 1, 5, 7, 17, 35, 38, 49, {0, 1, 5, 27, 34, 37, 43, 45}, {0, 1, 6, 15, 22, 26, 45, 55},
{0, 1, 6, 21, 28, 44, 46, 54}, {0, 1, 7, 19, 23, 44, 47, 49}, {0, 1, 7, 24, 36, 38, 49, 54},
{0, 1, 9, 11, 14, 35, 39, 51}, {0, 1, 9, 20, 23, 41, 51, 53}, {0, 1, 13, 15, 21, 24, 31, 53}.

$\mathbf{m = 8, v = 73, k = 9, c = 8}$.

{0, 1, 3, 7, 15, 31, 36, 54, 63}, {0, 1, 5, 12, 18, 21, 49, 51, 59}, {0, 1, 7, 11, 35, 48, 51, 53, 65},
{0, 1, 9, 21, 23, 26, 39, 63, 67}, {0, 1, 11, 20, 38, 43, 59, 67, 71}, {0, 1, 12, 20, 26, 30, 33, 35, 57},
{0, 1, 15, 23, 25, 53, 56, 62, 69}, {0, 1, 17, 39, 41, 44, 48, 54, 62}.

$\mathbf{m = 11, v = 133 = 7 \cdot 19, k = 12, c = 36}$.

{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109}, {0, 1, 3, 15, 46, 71, 75, 84, 94, 101, 112, 128},
{0, 1, 3, 17, 21, 58, 65, 73, 100, 105, 111, 124}, {0, 1, 3, 17, 29, 61, 80, 86, 91, 95, 113, 126},
{0, 1, 4, 12, 21, 26, 45, 68, 84, 97, 99, 127}, {0, 1, 4, 16, 50, 71, 73, 81, 90, 95, 101, 108},
{0, 1, 4, 27, 51, 57, 79, 89, 100, 118, 120, 125}, {0, 1, 5, 12, 15, 31, 33, 39, 56, 76, 85, 98},
{0, 1, 5, 21, 24, 39, 49, 61, 75, 92, 125, 127}, {0, 1, 5, 24, 44, 71, 74, 80, 105, 112, 120, 122},
{0, 1, 5, 25, 28, 68, 78, 87, 89, 104, 120, 126}, {0, 1, 6, 18, 39, 68, 79, 82, 98, 102, 124, 126},
{0, 1, 6, 22, 33, 40, 50, 59, 63, 88, 119, 131}, {0, 1, 7, 9, 42, 59, 73, 85, 95, 110, 113, 129},
{0, 1, 7, 35, 37, 50, 66, 89, 108, 113, 122, 130}, {0, 1, 8, 10, 32, 36, 52, 55, 66, 95, 116, 128},
{0, 1, 8, 14, 30, 45, 47, 56, 66, 106, 109, 129}, {0, 1, 8, 21, 33, 36, 47, 52, 70, 74, 76, 124},
{0, 1, 8, 21, 39, 43, 48, 54, 73, 105, 117, 131}, {0, 1, 9, 14, 16, 34, 45, 55, 77, 83, 107, 130},
{0, 1, 9, 19, 24, 31, 52, 56, 58, 69, 72, 98}, {0, 1, 10, 23, 29, 34, 61, 69, 76, 113, 117, 131},

{0, 1, 10, 58, 60, 64, 82, 87, 98, 101, 113, 126}, {0, 1, 12, 14, 22, 29, 54, 60, 63, 90, 110, 129},
{0, 1, 15, 18, 20, 24, 31, 52, 60, 85, 95, 107}, {0, 1, 15, 25, 45, 52, 58, 61, 63, 80, 84, 92},
{0, 1, 16, 21, 24, 49, 51, 58, 62, 68, 80, 94}, {0, 1, 23, 37, 57, 62, 75, 83, 86, 90, 92, 102},
{0, 1, 25, 30, 40, 46, 53, 96, 100, 114, 122, 131}, {0, 1, 26, 33, 39, 44, 53, 61, 63, 84, 118, 130},
{0, 1, 27, 39, 49, 74, 82, 103, 110, 114, 116, 119}, {0, 1, 32, 42, 44, 48, 51, 59, 72, 77, 97, 111},
{0, 1, 36, 49, 58, 78, 95, 101, 103, 119, 122, 129}, {0, 1, 36, 62, 65, 76, 78, 82, 103, 110, 115, 125},
{0, 1, 40, 54, 66, 72, 76, 83, 85, 110, 113, 118}, {0, 1, 42, 50, 54, 71, 73, 76, 82, 89, 109, 119}.

$\mathbf{m = 13, v = 183 = 3 \cdot 61, k = 14, c = 40}$.

{0, 1, 3, 16, 23, 28, 42, 76, 82, 86, 119, 137, 154, 175},

{0, 1, 3, 24, 41, 52, 57, 66, 70, 96, 102, 149, 164, 176},

{0, 1, 3, 31, 45, 50, 56, 65, 77, 125, 143, 147, 160, 176},

{0, 1, 4, 9, 15, 40, 72, 95, 105, 123, 125, 142, 149, 171},

{0, 1, 4, 16, 23, 43, 57, 101, 107, 112, 136, 138, 166, 174},

{0, 1, 4, 28, 34, 46, 60, 71, 126, 133, 135, 143, 148, 164},

{0, 1, 5, 11, 42, 45, 58, 60, 67, 81, 93, 110, 156, 164},

{0, 1, 5, 13, 65, 68, 93, 111, 113, 122, 146, 152, 162, 169},

{0, 1, 5, 25, 27, 39, 42, 48, 55, 88, 99, 107, 117, 152},

{0, 1, 6, 8, 32, 47, 76, 90, 111, 124, 128, 161, 164, 173},

{0, 1, 6, 29, 56, 98, 101, 105, 116, 118, 137, 149, 159, 175},

{0, 1, 7, 15, 37, 41, 46, 79, 100, 103, 123, 155, 171, 173},

{0, 1, 8, 20, 35, 82, 88, 114, 118, 127, 132, 143, 160, 181},

{0, 1, 8, 24, 37, 41, 59, 107, 119, 128, 134, 139, 153, 181},

{0, 1, 9, 12, 22, 45, 50, 106, 110, 112, 126, 141, 158, 165},

{0, 1, 9, 25, 35, 47, 66, 68, 79, 83, 86, 128, 155, 178},

{0, 1, 9, 30, 47, 65, 98, 102, 108, 142, 156, 161, 168, 181},

{0, 1, 9, 30, 75, 81, 88, 99, 116, 119, 121, 131, 135, 158},

{0, 1, 10, 15, 55, 58, 62, 83, 118, 134, 152, 154, 160, 171},

{0, 1, 10, 18, 46, 48, 72, 77, 83, 127, 141, 161, 168, 180},

{0, 1, 10, 24, 50, 54, 56, 67, 72, 75, 87, 114, 148, 155},

{0, 1, 10, 31, 56, 59, 63, 71, 76, 82, 98, 100, 136, 150},

{0, 1, 11, 13, 29, 61, 81, 84, 105, 138, 143, 147, 169, 177},

{0, 1, 11, 20, 23, 56, 60, 73, 94, 108, 137, 152, 176, 178},

{0, 1, 11, 33, 67, 94, 106, 109, 113, 115, 129, 153, 158, 166},

{0, 1, 11, 59, 68, 87, 91, 99, 105, 112, 129, 132, 134, 168},

{0, 1, 13, 24, 30, 32, 50, 66, 101, 122, 126, 129, 169, 174},

{0, 1, 13, 35, 42, 59, 61, 79, 89, 112, 144, 169, 175, 180},

{0, 1, 13, 61, 67, 69, 107, 110, 132, 139, 149, 160, 165, 169},

{0, 1, 15, 19, 24, 35, 45, 52, 74, 77, 115, 117, 123, 171},
{0, 1, 15, 22, 32, 38, 62, 71, 73, 91, 116, 119, 171, 179},
{0, 1, 16, 50, 52, 55, 72, 79, 85, 93, 97, 116, 125, 173},
{0, 1, 18, 26, 31, 55, 69, 71, 75, 78, 90, 117, 151, 173},
{0, 1, 19, 26, 43, 58, 72, 74, 78, 134, 139, 162, 172, 175},
{0, 1, 20, 28, 74, 91, 103, 117, 124, 126, 139, 142, 173, 179},
{0, 1, 20, 36, 41, 49, 51, 58, 113, 124, 138, 150, 156, 180},
{0, 1, 26, 49, 53, 63, 65, 68, 85, 96, 103, 109, 154, 175},
{0, 1, 29, 36, 70, 97, 109, 112, 117, 128, 130, 134, 160, 174},
{0, 1, 32, 67, 77, 85, 96, 129, 136, 142, 145, 157, 159, 179},
{0, 1, 34, 48, 84, 86, 102, 108, 113, 121, 125, 128, 153, 174}.

$\mathbf{m = 16, v = 273 = 3 \cdot 7 \cdot 13, k = 17, c = 12}$.

Here a multiplier, satisfying the requirements of the *Multiplier Theorem* is the even prime $p = 2$. The orbits (cycles) $r\,2^l (\mathrm{mod}\, 273)$, with $r \in RS(v)$, $l = 1, 2, ..., L(r)$, with the primitive length of the period $L(r)$, come in five types 12_{26}, 6_2, 3_2, $2_1\,1_1$, where the indices give the multiplicity. *I.e.*, twenty-six 12-cycles from $r = 1, 3, 5, 7, 9, 11, 17, 19, 21, 23, 25, 27, 29, 33, 41, 49, 51\,57, 59, 67, 97$, two 6-cycles with $r = 13$ and 65, two $3-$cycle from $r = 39$ and 117, one 2-cycle from $r = 91$ and one 1-cycle from $r = 0$.

Any assumed existing difference set with $k = 17$ members which is fixed by this multiplier $p = 2$ has then to be built from these cycles. However, not all such constructed sets are difference sets. One has to check this for each candidate.

To obtain sets of length 17 the only possibilities to combine cycles are:

(i) $6 + 6 + (3, I) + 2$,

(ii) $6 + 6 + (3, II) + 2$,

with the two 3-cycles $(3, I) = \{39, 78, 156\}$ and $(3, II) = \{117, 234, 195\}$, and the one $2-$cycle is $\{91, 182\}$.

(iii) $12 + (3, I) + 2$,

(iv) $12 + (3, II) + 2$, for the 26 12-cycles and the one $2-$cycle.

The $1-$ cycle $\{0\}$ cannot be used.

Now the two 6-cycles $(6, I) = \{13, 26, 52, 104, 208, 143\}$ and
$(6, II) = \{65, 130, 260, 247, 221, 169\}$ in version (i), as well as (ii), do not lead to invariant difference sets, because they have no two consecutive numbers as elements (modulo 273, where 0 and 272 are neighbors).

For example (i) produces the length $k = 17$ set after ordering $\{13, 26, 39, 52, 65, 78, 91, 104, 130, 143, 156, 169, 182, 208, 221, 247, 260\}$. Similarly for (ii) one gets $\{13, 26, 52, 65, 91, 104, 117, 130, 143, 169, 182, 195, 208, 221, 234, 247, 260\}$,

One is left with the two versions for the twenty-six $12-$cycles. It turns out that from (iii), as well as from (iv), one obtains precisely six difference sets. They come for version (iii) from $r = 7, 17, 18, 41, 59, 97$ and for version (iv) from $r = 1, 11, 23, 25, 29, 67$. Thus from the $2 \cdot 26 = 52$ invariant sets only 12 survive as invariant difference sets.

In order to obtain from these 12 difference sets the representative ones with neighboring elements 0 and 1 one subtracts the smaller number of a consecutive pair (for 0 and 272 one subtracts however 272) from each set element (always modulo 273). This produces the following $c = 12$ class representatives. They are ordered increasingly, and the original number r from the 12−cycle is given, as well as the value needed for subtraction, *e.g.*, as $[r = 7, -39]$.

$[1, -1]$: {0, 1, 3, 7, 15, 31, 63, 90, 116, 127, 136, 181, 194, 204, 233, 238, 255},

$[23, -91]$: {0, 1, 4, 16, 26, 57, 64, 91, 93, 99, 104, 123, 143, 205, 219, 228, 256},

$[41, -156]$: {0, 1, 8, 11, 26, 59, 64, 88, 156, 158, 172, 178, 195, 199, 208, 227, 239},

$[25, -234]$: {0, 1, 8, 20, 64, 89, 130, 139, 156, 160, 166, 188, 221, 234, 236, 239, 250},

$[7, -39]$: {0, 1, 8, 39, 41, 52, 55, 64, 100, 117, 121, 143, 149, 167, 239, 244, 254},

$[59, -181]$: {0, 1, 18, 46, 55, 69, 131, 151, 170, 175, 181, 183, 210, 217, 248, 258, 270},

$[17, -271]$: {0, 1, 19, 36, 41, 70, 80, 93, 138, 147, 158, 184, 211, 243, 259, 267, 271},

$[67, -233]$: {0, 1, 20, 30, 35, 107, 125, 131, 153, 157, 174, 210, 219, 222, 233, 235, 266},

$[97, -229]$: {0, 1, 22, 33, 83, 122, 135, 141, 145, 159, 175, 200, 226, 229, 231, 238, 246},

$[19, -38]$: {0, 1, 24, 35, 38, 40, 53, 86, 108, 114, 118, 135, 144, 185, 210, 254, 266},

$[11, -43]$: {0, 1, 28, 36, 43, 45, 48, 74, 99, 115, 129, 133, 139, 152, 191, 241, 252},

$[29, -116]$: {0, 1, 35, 47, 66, 75, 79, 96, 102, 116, 118, 186, 210, 215, 248, 263, 266}.

References

[1] Dobble, a card game, urlhttps://www.dobblegame.com/en/homepage/

[2] Ralf Goertz, Differenzmengen, Kartenspiel-Algebra, Spectrum Spezial Physik Mathematik Technik 4.18, pp. 24-29,

https://www.spektrum.de/pdf/72-77-sdw-06-2018-pdf/1563112

[3] H M.James Singer, A Theorem in Finite Projective Geometry and some Applications to Number Theory, Trans. AMS, 43 (1938) 377 - 385.

[4] Douglas R. Stinson, *Combinatorial Design*, Springer, 2004.

[5] Eric Weisstein's Math World, Difference Set, https://mathworld.wolframcom/DifferenceSet.htm

[6] Wikipedia, Difference Set, https://en.wikipedia.org/wiki/Difference_set

[7] Wikipedia, Dobble (in German), https://de.wikipedia.org/wiki/Dobble

---

Concerned with OEIS sequences: A000010, A000961, A001622, A335862, A335863, A335864.
