L'Enseignement Mathématique, t. 40 (1994), p. 187-192

CYCLIC DIFFERENCE SETS WITH PARAMETERS (511, 255, 127)

by Roland BACHER

This note describes the (equivalence classes of) cyclic difference sets with parameters (511, 255, 127). There are five non-isomorphic such classes which are listed at the end of this note. We give also a version of their triple intersection polynomial (our version differs by a numerical factor from the polynomial used in [EK]). The first and second belong to known families and are obtained by a geometric construction and by the GMW-construction described (for example) in [EK]. The last three appear to be exotic.

The technique used to produce all cyclic difference set with the above parameters is the same as in [C]. It uses heavy computer calculations and we will only sketch it.

Let v, k, λ be positive integers. Denote by C_v the cyclic group of order v which we identify with the additive group of the ring $\mathbf{Z}/v\mathbf{Z}$. A *cyclic difference set with parameters* (v, k, λ) is a subset D of cardinality k in C_v such that every element $c \neq 0$ in C_v can be written in exactly λ different ways as

$$c = d_1 - d_2$$

with d_1, d_2 in D. We identify D with its characteristic function. Hence D can be considered as an element of the group ring $\mathbf{Z}C_v$. Denote by $\sigma : C_v \to C_v$ the automorphism of C_v which sends $c \in C_v$ to its inverse $-c$. For an element X of $\mathbf{Z}C_v$ set $\overline{X} = \sigma(X)$. An element $X \in \mathbf{Z}C_v$ is a cyclic difference set if and only if all coefficients of X belong to the set $\{0, 1\}$ and X satisfies the equation

$$X\overline{X} = \lambda C_v + (k - \lambda)\{0\}$$

for appropriate λ and k. Difference sets are preserved under translation in C_v and under automorphisms of C_v. Two difference sets related by a translation and an automorphism are considered equivalent.

For l prime to v we define an *l-orbit* X in C_v as an orbit of the automorphism $\varphi_l : C_v \to C_v$ which sends $c \in C_v$ to lc. The multiplier theorem (see e.g. section 1 in [EK]) shows that each cyclic difference set D' with parameters (511, 255, 127) is equivalent to a difference set D fixed under φ_2, i.e. D is a union of 2-orbits in C_{511}. We can hence restrict the search to such difference sets.

Reduction modulo 73 shows that all 2-orbits of C_{511} have 9 elements, with 3 exceptions:

$$\{0\}, \quad A = \{219, 365, 438\}, \quad B = \{73, 146, 292\} .$$

Since we are searching for a difference set D of cardinality 255, we see that $\{0\}$ cannot be in D and that exactly one of A, B is in D. The automorphism φ_3 of C_{511} exchanges the sets A and B, hence we may suppose that $A \subset D$ and $B \not\subset D$.

In order to reduce the search further we use the fact that $511 = 7 \cdot 73$ is not a prime. Let us introduce the obvious surjective group homomorphisms $\pi_7 : C_{511} \to C_7$ and $\pi_{73} : C_{511} \to C_{73}$. For $M \in \mathbf{Z}C_{511}$ we set $M_7 = \pi_7(M)$, $\overline{M_7} = \pi_7(\overline{M})$, $M_{73} = \pi_{73}(M)$ and $\overline{M_{73}} = \pi_{73}(\overline{M})$. If the coefficients of $M \in \mathbf{Z}C_v$ are constant on 2-orbits then so are the coefficients of M_l, $\overline{M_l}$ for $l = 7$, 73. We take now for M a cyclic difference set D preserved by φ_2 and satisfying $A \subset D$. Clearly $D \in \mathbf{Z}C_{511}$ is an element with all coefficients constant on 2-orbits and in the set $\{0, 1\}$.

By considering the 2-orbits of C_7 we have $C_7 = X_0 \cup X_1 \cup X_2$ where $X_0 = \{0\}$, $X_1 = \{1, 2, 4\}$, $X_2 = \{3, 5, 6\}$. Hence we can write $D_7 = \sum x_i X_i$. All 2-orbits of D except A contain 9 elements. Since 2 is a square (mod 7), any 2-orbit of D distinct from A contributes 9 to x_0 if its elements are in the kernel of the projection π_7 or 3 to x_1 or x_2 according to whether it consists of squares or non-squares (mod 7). Moreover $A \in D$ contributes 1 to x_1. All coefficients of D are either 0 or 1 and their sum is equal to 255, hence x_0, x_1, x_2 are positive integers not greater than 73 such that $x_0 \equiv 0 \pmod 9$, $x_1 \equiv 1 \pmod 3$, $x_2 \equiv 0 \pmod 3$ and $x_0 + 3x_1 + 3x_2 = 255$. Since the difference set D satisfies the equation

$$D\overline{D} = 127 C_v + 128\{0\}$$

in $\mathbf{Z}C_{511}$ the projection D_7 satisfies

$$D_7\overline{D_7} = 128\{0\} + 127 \cdot 73 C_7 = 9399\{0\} + 9271(X_1 \cup X_2) .$$

The only solutions in $\mathbf{Z}C_7$ satisfying all the above requirements are

$$x_0 = 27, \; x_1 = 37, \; x_2 = 39$$

$$x_0 = 45, \; x_1 = 37, \; x_2 = 33 .$$

For C_{73} we have $C_{73} = \cup_{j=0}^{8} Y_j$ where $Y_0 = \{0\}$ and

$$
\begin{aligned}
Y_1 &= \{1, 2, 4, 8, 16, 32, 64, 55, 37\}\,, \\
Y_2 &= \{3, 6, 12, 24, 48, 23, 46, 19, 38\}\,, \\
Y_3 &= \{5, 10, 20, 40, 7, 14, 28, 56, 39\}\,, \\
Y_4 &= \{9, 18, 36, 72, 71, 69, 65, 57, 41\}\,, \\
Y_5 &= \{11, 22, 44, 15, 30, 60, 47, 21, 42\}\,, \\
Y_6 &= \{13, 26, 52, 31, 62, 51, 29, 58, 43\}\,, \\
Y_7 &= \{17, 34, 68, 63, 53, 33, 66, 59, 45\}\,, \\
Y_8 &= \{25, 50, 27, 54, 35, 70, 67, 61, 49\}\,,
\end{aligned}
$$

is the decomposition of C_{73} into 2-orbits. We are searching for positive integers $y_0, \ldots, y_8$ not greater than 7 such that $D_{73} = \sum_{j=0}^{8} y_j Y_j$. We already know that D contains a unique 2-orbit of cardinality 3 and that D does not contain 0. This implies that $y_0 = 3$. Moreover we have $y_0 + 9\sum_{j=1}^{8} y_j = 255$ and $D_{73} = \sum y_i Y_i$ satisfies

$$D_{73}\overline{D_{73}} = 128\{0\} + 127 \cdot 7C_{73} = 1017\{0\} + 889(\cup_{i=1}^{8} Y_i)\,.$$

A small computer program gives (up to multiplication by an invertible element in C_{73}) the following four solutions $(S1), .., (S4)$ with $y_0 = 3$, and $(y_1, .., y_8) =$

$(S1)$	$(7, 3, 3, 3, 3, 3, 3, 3)\,,$
$(S2)$	$(1, 5, 3, 3, 3, 3, 5, 5)\,,$
$(S3)$	$(1, 2, 4, 4, 5, 3, 4, 5)\,,$
$(S4)$	$(6, 3, 4, 3, 2, 2, 3, 5)\,.$

Hence every cyclic difference set with parameters $(511, 255, 127)$ is equivalent to a difference set D which projects onto one of the above 2 solutions in C_7 and onto one of the above 4 solutions in C_{73}. One can reduce the number of cases somewhat more by considering the orbit of a difference set D under multiplication by 74 which is an invertible square (mod 7) (and hence keeps A fixed) and the identity (mod 73). There remain more than 10^{10} unions of 2-orbits which have these projections. A computer program written in FORTRAN running about 50 hours on a SUN-workstation found (up to isomorphism) exactly five difference sets denoted by $D_1, .., D_5$. The notation $D_i = (a_1, .., a_l)$ means that the difference set D_i is the union of the 2-orbits generated by $a_1, .., a_l$. The polynomial $P_i(x)$ associated to D_i is defined by

$$P_i(x) = \sum_{a,b \in C_{511},\ 1 \leqslant a < b < 511} x^{\#\{D_i \cap (D_i + a) \cap (D_i + b)\}}$$

where $D_i + a$ denotes the translate of D_i by a.

One easily checks that the usual triple intersection polynomial is just a scalar multiple of the one above.

Remark: For a difference set this polynomial does not depend on the choice of the fixed first block. For a symmetric design whose automorphism group is not transitive on the blocks it does in general. So this gives a condition fulfilled by a symmetric design coming from a difference set.

Two difference sets project onto $(S1)$: These two correspond to known constructions and give factorizations of the elements $D_i'(y)$ in the ring $\mathbf{Z}[y]/(y^{511} - 1)$ where

$$D_i'(y) = \sum_{k \notin D_i} y^k .$$

We also give a factorization of $D_i'(y)$ in $\mathbf{Z}[y]/(y^{511} - 1)$ (the factorization is not unique).

The first such difference set is

$$D_1 = (1, 7, 13, 17, 21, 23, 31, 35, 37, 39, 51, 53, 55, 59, 61, 75, 77, 79, 83, 85, 91, 95, 103, 109, 123, 183, 187, 219, 223) ,$$

$$P_1(x) = 129540x^{63} + 255x^{127} ,$$

$D_1'(y)$ factorizes in $\mathbf{Z}[y]/(y^{511} - 1)$ as

$$\begin{aligned} D_1'(y) = {} & (1 + y^{73} + y^{146} + y^{292}) \\ & (1 + y^{27} + y^{43} + y^{47} + y^{54} + y^{86} + y^{87} + y^{94} + y^{107} + y^{108} + y^{119} \\ & + y^{172} + y^{174} + y^{177} + y^{179} + y^{185} + y^{188} + y^{195} + y^{197} + y^{205} \\ & + y^{214} + y^{216} + y^{229} + y^{231} + y^{238} + y^{241} + y^{255} + y^{269} + y^{277} \\ & + y^{279} + y^{299} + y^{309} + y^{315} + y^{344} + y^{345} + y^{348} + y^{353} + y^{354} \\ & + y^{358} + y^{370} + y^{371} + y^{376} + y^{383} + y^{390} + y^{394} + y^{395} + y^{405} \\ & + y^{410} + y^{413} + y^{428} + y^{432} + y^{441} + y^{447} + y^{453} + y^{458} + y^{462} \\ & + y^{476} + y^{479} + y^{482} + y^{495} + y^{503} + y^{507} + y^{509} + y^{510}) . \end{aligned}$$

The second such difference set is

$$D_2 = (1, 15, 23, 27, 37, 45, 47, 51, 53, 55, 57, 61, 63, 75, 77, 79, 83, 85, 87, 93, 103, 125, 127, 175, 183, 187, 219, 223, 255) ,$$

$$P_2(x) = 4536x^{55} + 121224x^{63} + 1512x^{71} + 2520x^{79} + 3x^{127} ,$$

$D'_2(y)$ factorizes in $\mathbf{Z}[y]/(y^{511}-1)$ as

$$D'_2(y) = (1 + y^{73} + y^{146} + y^{292})$$
$$(1 + y^9 + y^{11} + y^{18} + y^{22} + y^{25} + y^{31} + y^{36} + y^{44} + y^{50} + y^{59} + y^{62} + y^{65} + y^{67} + y^{72} + y^{88} + y^{100} + y^{118} + y^{119} + y^{124} + y^{130} + y^{134} + y^{144} + y^{176} + y^{193} + y^{199} + y^{200} + y^{231} + y^{236} + y^{238} + y^{239} + y^{247} + y^{248} + y^{260} + y^{261} + y^{268} + y^{271} + y^{285} + y^{288} + y^{289} + y^{315} + y^{352} + y^{355} + y^{371} + y^{375} + y^{379} + y^{386} + y^{391} + y^{398} + y^{400} + y^{413} + y^{433} + y^{441} + y^{443} + y^{445} + y^{451} + y^{462} + y^{472} + y^{476} + y^{477} + y^{478} + y^{481} + y^{494} + y^{496}) .$$

Two difference sets project onto $(S2)$:

$$D_3 = (3, 5, 7, 11, 13, 25, 27, 31, 35, 39, 47, 51, 53, 59, 61, 63, 79, 85, 91, 95, 107, 109, 111, 119, 127, 187, 191, 219, 223) ,$$

$$P_3(x) = 90x^{54} + 216x^{55} + 783x^{56} + 1746x^{57} + 3546x^{58} + 6912x^{59} + 10692x^{60} + 12906x^{61} + 16461x^{62} + 17703x^{63} + 17334x^{64} + 15615x^{65} + 10773x^{66} + 7236x^{67} + 4320x^{68} + 1971x^{69} + 1026x^{70} + 270x^{71} + 57x^{72} + 84x^{73} + 54x^{74}$$

and

$$D_4 = (9, 17, 21, 23, 25, 27, 35, 39, 43, 53, 59, 63, 75, 79, 85, 87, 93, 95, 107, 111, 117, 119, 125, 127, 171, 175, 187, 219, 255) ,$$

$$P_4(x) = 1353x^{55} + 25128x^{59} + 72813x^{63} + 29088x^{67} + 1413x^{71} .$$

No difference set projects onto $(S3)$.

One difference set projects onto $(S4)$:

$$D_5 = (1, 7, 9, 11, 25, 27, 31, 35, 37, 39, 47, 53, 55, 61, 77, 83, 85, 87, 107, 109, 111, 119, 171, 175, 183, 187, 191, 219, 223) ,$$

$$P_5(x) = 27x^{53} + 246x^{54} + 135x^{55} + 900x^{56} + 1863x^{57} + 3276x^{58} + 6237x^{59} + 9648x^{60} + 13851x^{61} + 17865x^{62} + 18486x^{63} + 16713x^{64} + 14364x^{65} + 10458x^{66} + 8262x^{67} + 3834x^{68} + 2007x^{69} + 1134x^{70} + 270x^{71} + 162x^{72} + 57x^{73} .$$

Acknowledgements. This note owes more to S. Eliahou and M. Kervaire than this short sentence can suggest. I also thank the Fonds National suisse pour la Recherche Scientifique for a grant during this work.

REFERENCES

[C] CHENG, U. Exhaustive Construction of (255, 127, 63)-Cyclic Difference Sets. *J. Combin. Theory Ser. A 35* (1982), 115-125.

[EK] ELIAHOU, S. and M. KERVAIRE. Barker Sequences and Difference Sets. *L'Enseignement Mathématique 38* (1992), 345-382.

(Reçu le 21 mars 1994)

Roland Bacher

Section de Mathématiques
Université de Genève
C.P. 240
1211 Genève 24 (Switzerland)