Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 18–23*

New perfect difference families [1]

Tsonka Baicheva and Svetlana Topalova tsonka,svetlana@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
5000 Veliko Tarnovo, 78 N. Gabrovski street
Bulgaria

Abstract. We construct all $(v, k, 1)$ perfect difference families with $k = 3$ and $v \leq 55$, with $k = 4$ and $v \leq 85$, and with $k = 5$ and $v = 121$.

1 Introduction

1.1 Motivation

The motivation of this work is the recent paper of Park, Hong, No and Shin [1] where a construction of high-rate regular quasi-cyclic low-density parity-check (QC LDPC) codes based on cyclic difference families is presented. QC LDPC codes are suitable for hardware implementation using simple shift registers due to the regularity in their parity-check matrices and that is why they have been adopted in many practical applications. It is known that QC LDPC codes having a parity-check matrix consisting of a single row of circulants is adequate for generating high-rate QC LDPC codes of short and moderate lengths. In [2]–[5], QC LDPC codes constructed from cyclic difference families (CDFs) are proposed but they have restricted lengths. In [1] new high-rate regular QC LDPC codes having parity-check matrices consisting of a single row of circulants are proposed based on special classes of CDFs, namely perfect difference families (PDFs). The code rate and length of the proposed codes can be flexibly chosen from a set of values including the minimum achievable code length for the given column-weight and design rate under girth 6. It is shown that the error correcting performance of the proposed QC LDPC codes is almost the same as that of the existing high-rate QC LDPC codes.

CDFs and PDFs have many other relations and practical applications. They are related to one-factorizations of complete graphs and to cyclically resolvable cyclic Steiner triple systems [6]. Very efficient constructions of new optimal perfect secrecy systems that are one-fold secure against spoofing are obtained via CDF [7]. Optimal frequency-hopping sequences can be constructed from $(v, k, 1)$ CDFs. They can also be used for a construction of other types of

[1]This research is partially supported by the Bulgarian National Science Fund under Contract No. I01/0003.

combinatorial structures like regular perfect systems of difference sets, difference triangle sets, perfect optimal optical orthogonal codes, cyclic 2-(v,k,1) designs, etc.

1.2 Definitions and notations

For a general background on difference families we refer to [8].

Definition 1. *Let B be a subset of an additive group G. We denote by ΔB the list of all possible differences $b-b'$ with (b, b') an ordered pair of distinct elements of B. More generally, if $F = \{B_1, B_2, \ldots, B_n\}$ is a collection of subsets of G, then the list of differences from F, denoted by ΔF, is the multiset obtained by joining $\Delta B_1, \ldots, \Delta B_n$. F is said to be a $(v, k, 1)$* **difference family** *(DF) if G has order v, every B_i is of size $k \geq 3$, and ΔF covers every non-zero element of G exactly once. If further, $G = Z_v$, then this difference family is said to be* **cyclic** *(CDF).*

Definition 2. *Let F be a CDF. Denote by $\bar{\Delta} B$ the list of all possible differences $b - b'$ with $b > b'$, where b and b' are distinct elements of B. If $\bar{\Delta} F = \{1, 2, \ldots, (v-1)/2\}$, then F is called a* **perfect difference family**, *or briefly, a $(v, k, 1)$ PDF.*

Therefore $(v, k, 1)$ PDFs are a subclass of $(v, k, 1)$ CDFs. In this work we will focus on PDFs because as it is shown in [1], (Corollary 1), QC LDPC codes based on them do not have any cycle of length 4 for a large range of code lengths.

For a k-element set $B = \{b_0, b_1, ...b_{k-1}\}$ it is convenient to present the differences from $\bar{\Delta} B$ by a difference triangle D with elements $D_i^j = b_{i+j} - b_i$. A difference triangle for $k = 5$ can be illustrated as follows:

$$\begin{array}{ccccccccc} & & & & d_1^4 & & & & \\ & & & d_1^3 & & & d_2^3 & & \\ & & d_1^2 & & & d_2^2 & & & d_3^2 \\ & d_1^1 & & & d_2^1 & & & d_3^1 & & & d_4^1 \end{array}$$

The most important property of a difference triangle is that the sum of the elements in the upper half of the triangle is equal to the sum of the elements in the lower half.

The aim of our work is classification of PDFs, which are a special kind of CDFs. That is why we have to know when two CDFs are equivalent.

Definition 3. *Two difference families $\mathbf{F} = \{B_1, B_2, \ldots, B_n\}$ and $\mathbf{F}' = \{B_1', B_2', \ldots, B_n'\}$ over Z_V are equivalent if there is an automorphism α of Z_V such that for each $i = 1, 2, \ldots, n$ there exists B_j' which is a translate of $\alpha(B_i)$.*

1.3 Some basic known results

The known existence results for PDFs can be summarized as follows:

Theorem 1. *1) If* $v \equiv 1$ *or* 7 $(mod\ 24)$*, then a* $(v, 3, 1)$ *PDF exists [8].*
2) A $(12t + 1, 4, 1)$ *PDF exists for* $t = 1$*,* $4 \leq t \leq 1000$ *[9].*
3) $(20t + 1, 5, 1)$ *PDFs are known for* $t = 6, 8, 10$ *but for no other values of* $1 \leq t \leq 50$ *[8].*
4) There are no $(v, k, 1)$ *PDF for the following values [8]:*
a) $k = 3$*,* $v \equiv 13$ *or* 19 $(mod\ 24)$*,*
b) $k = 4$*,* $m \in \{25, 37\}$*,*
c) $k = 5$*,* $v \equiv 21$ $(mod\ 40)$ *or* $m \in \{41, 81\}$*,*
d) $k \geq 6$*.*

We know computer-aided classification results only for $(121, 5, 1)$ PDFs which were classified in 1982 by Laufer [10]. PDFs with these parameters consist of six difference triangles. Laufer first constructs all the possible systems of six incomplete triangles (a brilliant idea), i.e. triangles for which only the upper two rows are determined. He next extends these partial solutions to PDFs and obtains 75 PDFs. For these parameters this is a very serious achievement for the computers of the early 80-ties. In the present work we establish that the $(121, 5, 1)$ PDFs are actually more than 75, but this error in Laufer's computations does not make his idea and result less attractive.

1.4 The present paper

The main aim of the present work is the computer-aided classification of PDFs. The availability of all PDFs with definite parameters might be of interest for future applications in Coding Theory and elsewhere. We present classification results for $(v, k, 1)$ PDFs with $k = 3$ and $v \leq 55$, with $k = 4$ and $v \leq 85$, and with $k = 5$ and $v = 121$.

2 Our classification algorithms

We use two different algorithms to construct PDFs.

2.1 Algorithm 1

For a $(v, k, 1)$ PDF it holds that $v = k(k-1)m+1$. We first construct a list of all possible k-element subsets of the set of the integers from 1 to v, such that their corresponding difference sets do not contain differences which are greater than $k(k-1)m/2$. For $k = 5$ we also compute the sum of the elements of the first (last) two rows of their difference triangles. We sort the list by the minimum (or maximum) differences of the sets and a lexicographic order defined on the triangles.

We choose the elements of the current PDF by back track search. When s sets have been chosen, we add a set containing the smallest (or biggest) difference which is not contained in the already chosen difference triangles. We also check the following:

- We calculate S_{max} - the sum of the biggest $m - s$ (or $3m - s$ for $k = 5$) differences which are not contained in the already chosen difference triangles
- We calculate S_{min} - the sum of the smallest $(k-1)(m-s)$ (or $(2k-3)(m-s)$ for $k = 5$) differences which are not contained in the already chosen difference triangles
- If $S_{max} \geq S_{min}$ we choose an $(s+1)$-st element. If $S_{max} < S_{min}$ we change the s-th element by the next possible one.

The sum of the elements of the m first rows of the difference triangles for $k = 3$ equals S - half of the sum of the first $k(k-1)m/2$ integers. So does the sum of the first two rows of the difference triangles for $k = 5$. So in these cases instead of $S_{max} \geq S_{min}$ we check if $S_{max} \geq S$ and $S \geq S_{min}$.

With respect to the defined lexicographic order on the difference triangles, the currently obtained PDF is greater than the previous ones. We use this to check each PDF for equivalence to some of those which were constructed earlier. We achieve this by checking if the current solution can be mapped to a lexicographically smaller one by some of the automorphisms of Z_v. This way besides the set of all PDFs, we also obtain a set of inequivalent PDFs with the given parameters.

2.2 Algorithm 2

We use a modification of our algorithm for construction of optical orthogonal codes and CDFs [11]. By this algorithm we classify only the inequivalent PDFs with the given parameters. Algorithm 1 is much faster, but we use Algorithm 2 to compare part of the obtained results.

2.3 Implementation

Our computer implementations of both algorithms are written in C++. The programmes ran on a PC with an Intel Xeon 2.5 GHz 6 cores processor. With Algorithm 1 the classification of the (121,5,1) PDFs took 4 days (running in parallel on 12 threads).

3 Results

The results are presented in Table 1, where $PDFs$ is the number of the obtained PDFs, $ineq\ CDFs$ is the number of inequivalent CDFs if it is known from [11], and $ineq\ PDFs$ is the number of inequivalent PDFs.

Table 1: $(v, k, 1)$ perfect difference families, $v = k(k-1)m + 1$.

v	k	m	ineq. CDFs	PDFs	ineq. PDFs
25	3	4	12	168	12
31	3	5	80	672	68
49	3	8	157340	778240	150788
55	3	9	3027456	10498560	2520064
13	4	1	2	1	1
49	4	4	224	192	80
61	4	5	18132	5568	2544
73	4	6	1426986	200448	94368
85	4	7		9207040	4552504
121	5	6		7488	3744

References

[1] H. Park, S. Hong, J. No and D. Shin, Construction of high-rate regular quasi-cyclic LDPC codes based on cyclic difference families, *IEEE Trans. on Inform. Theory*, **50**, no 6, 1156–1176, 2004.

[2] B. Ammar, B. Honary, Y. Kou, J. Xu and S. Lin, Constructions of low-density parity-check codes based on balanced incomplete block designs, *IEEE Trans. on Inform. Theory*, **50**, no 5, 1257–1268, 2004.

[3] M. Fujisava and S. Sakata, A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8, *IEICE Trans. Fundamentals*, **E-90A**, no 5, 1055–1061, 2007.

[4] S. J. Johnson and S. R. Weller,A family of irregular LDPC codes with low encoding complexity, *IEEE Trans. on Inform. Theory*, **50**, no 6, 1156–1176, 2004.

[5] B. Vasik and O. Milenkovic, Combinatorial constructions of low-density parity-check codes for iterative decoding, *IEEE Trans. on Inform. Theory*, **50**, no 6, 1156–1176, 2004.

[6] R. Fuji-Hara, Y. Miao and S. Shinohara, Complete Sets of Disjoint Difference Families and their Applications, *Journal of Statistical Planning and Inference*, **106**, Issues 1–2, 87–103, 2002.

[7] M. Huber, Perfect Secrecy Systems Immune to Spoofing Attacks, *Int. J. Inf. Secur.*, **11**, Issue 4, 281-289, 2012.

[8] R. Julian R. Abel and M. Buratti *Difference families*, in: C.J. Colbourn, J.H. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL, 270–287, 1996.

[9] G. Ge, Y. Miao and X. Sun, Perfect difference families, perfect differnce matrices, and related combinatorial structures, *J. Combin. Des.*, **18**, no. 6, 415-449, 2010.

[10] Ph. Laufer, Regular perfect systems of difference sets of size 4 and extremal systems of size 3, , *Ann. Discrete Math.*, **12**, 193–201, 1982.

[11] T. Baicheva and S. Topalova, Classification results for (v, k, 1) cyclic difference families with small parameters, *Mathematics of Distances and Applications*, M. Deza, M. Petitjean, K. Markov eds., in International book series: *Information Science and Computing*, book 25, 24–30, 2012.