Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes
B. Preneel et al. (Eds.)
IOS Press, 2009

doi:10.3233/978-1-60750-002-5-260

Classification of Doubly Resolvable Designs and Orthogonal Resolutions

Svetlana TOPALOVA and Stela ZHELEZOVA
Institute of Mathematics and Informatics, BAS,Bulgaria
svetlana@math.bas.bg, stela@math.bas.bg

Abstract. We classify doubly resolvable designs with small parameters by a modification of a known algorithm for classification of the binary equidistant constant weight codes which correspond to resolvable designs with these parameters. For each of these designs we next construct all the sets of mutually orthogonal resolutions. We also derive lower bounds for some parameters beyond the application range of this general approach and check the correctness of the computational results in several ways.

Keywords. classification, orthogonal resolution, doubly resolvable design

Introduction

Let $Z_q = \{0, 1, ..., q-1\}$. A word of length r over Z_q is an r-tuple $x = (x_1, x_2, ..., x_r) \in Z_q^r$. The Hamming distance $d(x, y)$ between two words $x, y \in Z_q^r$ is the number of coordinates in which the words differ. An equidistant $(r, v, d)_q$ code is a set of v words of length r over Z_q, with the property that the distance between any two distinct words is d.

For the basic concepts and notations concerning combinatorial designs and their resolvability refer, for instance, to [1], [2], [3], [4], [5].

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ – a finite collection of k-element subsets of V, called *blocks*. If any 2-subset of V is contained in exactly λ blocks of $\mathcal{B}$, then $D = (V, \mathcal{B})$ is a 2-(v,k,λ) *design*, or *balanced incomplete block design (BIBD)*.

A 2-(v,k,$m\lambda$) design is called an *m-fold multiple* of 2-(v,k,λ) designs if there is a partition of its blocks into m subcollections, which form 2-(v,k,λ) designs.

A *resolution* of the design is a partition of the collection of blocks into *parallel classes*, such that each point is in exactly one block of each parallel class. A design is resolvable if it has at least one resolution. There is a one-to-one correspondence [6] between the resolutions of $2-(qk, k, \lambda)$ designs and the $(r, qk, r-\lambda)_q$ equidistant codes, $q > 1$.

Some of the known applications of design resolutions in cryptography concern anonymous (2,k)-threshold schemes from resolvable 2-(v,k,1) designs [7], [8], synchronous multiple access to channels by resolvable 2-(v,3,1) designs [9], and unconditionally secure commitment schemes [10].

Existence and classification of resolvable 2-(v,k,λ) designs with definite parameters has been extensively studied, see for instance [11], [12], [13], [14], [4], [15], [16], [17]. A very good recent survey of the different approaches for constructing and classifying design resolutions is contained in [18].

Two resolutions of one and the same design are *orthogonal* if each pair of parallel classes, one from the first, and one from the second resolution, have at most one common block. A *doubly resolvable design (DRD)* is a design which has at least two orthogonal resolutions. We denote by ROR a resolution which is orthogonal to at least one other resolution, and by m-MOR a set of m mutually orthogonal resolutions. The m-MOR is maximal if no more resolutions can be added to it.

Sets of mutually orthogonal resolutions can be used for the construction of perfect secret sharing schemes [19], [20]. They also appear in product association schemes [21].

Cryptographic applications of resolutions often use the fact that each resolution class is uniquely defined by any of its blocks, and that for some designs the block itself is uniquely defined by a proper subset of its points. Consider as an example a resolution of a 2-$(v,3,1)$ design. In this case a block is defined by any 2 of its points. And if you construct a threshold scheme, for instance, you can have r secrets corresponding to the r parallel classes, each of them uniquely determined by two of the 3 shares corresponding to one of its blocks.

While a resolution parallel class is uniquely determined by any of its blocks, a parallel class of the m-MOR is uniquely determined by any pair of its blocks, and that is why m-MORs can be used for cryptographic applications in ways similar to those in which resolutions are used. If the resolution has r classes, the m-MOR has $m.r$ parallel classes. But, of course, this can work well, only if the underlying design has some additional nice properties considering the point sets that uniquely define a block. In some cases their size is known from the design parameters, but in others some of the designs might be useful for such purposes, some may not. In a similar way, the constructions from [19] and [20] depend on properties of the 2-MOR which do not follow from its parameters (i.e. on the critical sets of the Room squares used). Therefore classification results for doubly resolvable designs and orthogonal resolutions might be of major interest for any possible further cryptographic applications.

Existence of DRDs and bounds on m for their m-MORS have been intensively studied in the last two decades [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]. When classifying resolutions with certain parameters some authors have also searched for orthogonal ones among them, see for instance [33], [34], [35], [36]. A Room square of side n, $RS(n)$, is equivalent to a 2-MOR of a 2-$(n+1,2,1)$ BIBD. Full classification of Room squares with small parameters is known [37], [38], [39].

We present here recent classification results for 2-(v,k,λ) DRDs and their RORs and m-MORs [40], [41].

1. Construction Method, Classification Results, Parameter Range

We first construct RORs [40], and then classify the DRDs and construct m-MORs [41]. Most people who have constructed resolutions, actually construct their corresponding equidistant codes. So do we. We use the word by word orderly generation, but from some word on, we start applying an orthogonal resolution existence (ORE) test. For de-

signs with $v = 2k$ we also use parameter specific double resolvability restrictions [42]. Having constructed all non isomorphic RORs, we apply a standard design isomorphism test to obtain the non isomorphic DRDs. For each DRD we next find all its maximal m-MORs. We use two different algorithms for the ORE test [43], and partially check the correctness of the results in several ways.

The m-MOR classification results are summarized in Table 1, where the number of maximal (left value) and all (right value) m-MORs is presented in the columns m-MORs for $m = 2, 3, 4$. In the column "No" the number of the design in the tables of [44] is given, RS(7) means that the 2-MORs correspond to Room squares of side 7.

Table 1. Classification results for m-MORs by computer search [41]

q	v	k	λ	RORs	DRDs	2-MORs		3-MORs		4-MORs		No
2	6	3	8	1	1	1	1	-	-	-	-	236
2	6	3	12	1	1	0	1	1	1	-	-	596
2	6	3	16	1	1	0	$\geq$15	0	$\geq$485	$\geq$485	$\geq$485	1078
2	8	4	6	1	1	1	1	-	-	-	-	101
2	8	4	9	1	1	0	1	1	1	-	-	278
2	8	4	12	4	4	7	17	0	60	60	60	524
2	10	5	16	5	5	5	5	-	-	-	-	891
2	10	5	24	6	6	2	7	5	5	-	-	-
2	12	6	10	1	1	1	1	-	-	-	-	319
2	12	6	15	1	1	0	1	1	1	-	-	743
2	12	6	20	546	546	691	$\geq$ 701	0	$\geq$ 223	$\geq$ 223	$\geq$ 223	-
2	16	8	14	5	5	5	5	-	-	-	-	618
2	16	8	21	5	5	0	5	5	5	-	-	-
2	20	10	18	3	3	3	3	-	-	-	-	1007
3	9	3	3	5	3	2	7	5	5	-	-	66
3	9	3	4	83	38	351	449	284	285	1	1	145
4	8	2	1	4	1	4	6	1	1	-	-	RS(7)
4	12	3	2	70	20	252	254	1	2	1	1	55
4	16	4	2	1	1	0	1	1	1	-	-	44

The RORs construction programme covers most parameters for which all the resolutions have been classified. Exceptions are the RORs of 2-(9,3,5), 2-(12,2,1) and 2-(14,2,1) designs, for which full classification or enumeration (for $v = 14$) of the resolutions is known ([45], [46]), but the expected number of RORs is very big. By applying ORE test to the recently classified resolutions of 2-(28,4,1) designs [18], we find that there is no ROR among them, but we cannot obtain the result by our RORs classification programme. For $q = 2$ with additional double resolvability restrictions we cover RORs with parameters for which all the resolutions have not been classified yet, namely 2-(10,5,24), 2-(12,6,15), 2-(12,6,20), 2-(16,8,14), 2-(16,8,21), 2-(20,10,18). Classification of the m-MORs in the way we do it, is not possible for some of the parameters, for which we have classified the RORs. One of the reasons is the fast growth of the number of RORs and m-MORs of designs with some of the next parameters due to multiple designs. A relation between the number of m-MORs of multiple designs and the number of inequivalent sets of $v/k - 1$ mutually orthogonal latin squares of size m is obtained in [41]. Using it lower bounds on the number of RORs and m-MORs are computed

for some small parameters. The growth of their number is well illustrated by the lower bounds presented in Table 2.

Table 2. Lower bounds on the number of m-MORs

v	k	λ	DRDs	m	lower bound on m-MORs
8	4	15	82	5	8
8	4	18	240	6	31824
8	4	21	650	7	33.10^{10}
8	4	24	1803	8	29.10^{33}
8	4	27	4763	9	19.10^{67}

References

[1] E.F.Jr. Assmus, J.D. Key, Designs and their Codes, Cambridge Tracts in Mathematics, Vol. 103, Cambridge University Press, 1992.

[2] Th.Beth, D.Jungnickel, H.Lenz, *Design Theory*, Cambridge University Press, 1993.

[3] C.J.Colbourn and J.H.Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL., 2007.

[4] P.Kaski and P.Östergård, *Classification algorithms for codes and designs*, Springer, Berlin, 2006.

[5] V.D.Tonchev, *Combinatorial configurations*, Longman Scientific and Technical, New York, 1988.

[6] N.V.Semakov, V.A.Zinoviev, Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs, *Problems Inform. Transmission* 4 (1968) no. 2, 1-7.

[7] W. Kishimotoa, K. Okadab, K. Kurosawa, W. Ogata, On the bound for anonymous secret sharing schemes, *Discrete Applied Mathematics* Vol. 121, Issues 1-3 (2002), 193-202.

[8] D.R. Stinson, S.A. Vanstone, A combinatorial approach to threshold schemes, *SIAM Journal on Discrete Mathematics* Vol. 1 , Issue 2 (1988), 230 - 236, DOI 10.1137/0401024.

[9] C.J. Colbourn, J.H. Dinitz, D.R. Stinson, Applications of Combinatorial Designs to Communications, Cryptography, and Networking, 1999, preprint.

[10] C. Blundo, B. Masucci, D. R. Stinson and R. Wei. Constructions and bounds for unconditionally secure non-interactive commitment schemes. Designs, Codes and Cryptography 26 (2002), 97-110.

[11] D.J.Curran, S.A.Vanstone, Resolvable designs from generalized Bhaskar Rao designs, *Discrete Mathematics* 73 (1988/89), 49-63.

[12] P.Kaski, Isomoprph-free exhaustive generation of combinatorial designs, Helsinki University of Technology Laboratory for Theoretical Computer Science, Research Reports 70, 2002.

[13] P.Kaski, L.Morales,P.Östergård, D.Rosenblueth, C.Velarde, Classification of resolvable 2-(14,7,12) and 3-(14,7,5) designs, *Journal of Combinatorial Mathematics and Combinatorial Computing* 47 (2003), 65-74.

[14] P.Kaski, P.Östergård, Enumeration of 2-(9,3,λ) designs and their resolutions, *Designs, Codes and Cryptography* 27 (2002), 131-137.

[15] L.Morales, C.Velarde, A complete classification of (12,4,3)-RBIBDs, *Journal of Combinatorial Designs* vol.9,issue 6 (2001), 385-400.

[16] L.Morales, C.Velarde, Enumeration of resolvable 2-(10,5,16) and 3-(10,5,6) designs, *Journal of Combinatorial Designs* vol.13, issue 2 (2005), 108-119.

[17] P.Östergård, Enumeration of 2-(12,3,2) designs, *Australasian Journal of Combinatorics* 22 (2000), 227-231.

[18] P.Kaski and P.Östergård, Classification of resolvable balanced incomplete block designs - the unitals on 28 points, *Mathematica Slovaca*, to appear.

[19] G.R. Chaudhry, J. Seberry, Secret sharing schemes based on Room squares, *Combinatorics, Complexity and Logic, Proceedings of DMTCS'96*, Springer-Verlag Singapore (1996), pp. 158-167.

[20] G.R. Chaudhry, H. Ghodosi, J. Seberry, Perfect secret sharing schemes from Room squares, *J. Combin. Math. and Combin. Computing (JCMCC), Canada* 28 (1998), pp.55-61.

[21] W.J. Martin, Designs in product association schemes,*Designs, Codes and Cryptography* Vol. 16, Number 3 (1999), 271-289, DOI 10.1023/A:1008340128973.

[22] R.J.R.Abel, E.R.Lamken, J.Wang, A few more Kirkman squares and doubly near resolvable BIBDS with block size 3, *Discrete Mathematics* 308 (2008), 1102-1123.

[23] C.J.Colbourn, E.Lamken, A.Ling, W.Mills, The existence of Kirkman squares - doubly resolvable (v,3,1)-BIBDs, *Designs, Codes and Cryptography* 26 (2002), 169-196.

[24] C.J.Colbourn, A. Rosa, Orthogonal resolutions of triple systems, *Australasian J. Combin.* 12 (1995) pp. 259Ű269.

[25] M.Deza, R.C.Mullin, S.A.Vanstone, Orthogonal systems, *Aequationes Math.* 17 (1978), 322-330.

[26] R.Fuji-Hara, S.A.Vanstone, On the spectrum of doubly resolvable designs, *Congressus Numerantium* 28 (1980), 399-407.

[27] E.R.Lamken, Coverings, orthogonally resolvable designs and related combinatorial configurations, Ph.D. Thesis, Univ. of Michigan (1983).

[28] E.R.Lamken, Constructions for resolvable and near resolvable (v,k,k-1)-BIBDs, *D.K. Ray-Chaudhuri (ed.), Coding Theory and Design Theory. Part II. Design Theory*, Springer (1990), 236Ű250.

[29] E.R.Lamken, S.A.Vanstone, Designs with mutually orthogonal resolutions, *Europ.J.Combinatorics* (1986) 7, 249-257.

[30] E.R.Lamken , S.A.Vanstone, The existence of a class of Kirkman squares of index 2, *J. Ausral. Math. Soc. (Series A)* 44 (1988), 33-41.

[31] A.Rosa, S.A.Vanstone, Starter-adder techniques for Kirkman squares and Kirkman cubes of small sides, *Ars Combin.* 14 (1982), 199-212.

[32] S.A.Vanstone, Doubly resolvable designs, *Discrete Math.* 29 (1980), 77-86.

[33] M.Cohen, C.J.Colbourn, Lee A.Ives, A.Ling, Kirkman triple systems of order 21 with nontrivial automorphism group., *Math. Comput.* 71(238): 873-881 (2002).

[34] P.Kaski, P.Östergård, S.Topalova, R.Zlatarski, Steiner Triple Systems of Order 19 and 21 with Subsystems of Order 7, *Discrete Mathematics*, Vol 308 (2008), 2732-2741, doi:10.1016/j.disc.2006.06.038.

[35] D. R. Stinson, S. A. Vanstone, Orthogonal packings in PG(5,2), *Aequationes Math.* 31 (1986), 159-168.

[36] V.D.Tonchev, Steiner triple systems of order 21 with automorphisms of order 7, *Ars Combinatoria* 23 (1987) 93-96.

[37] J.H.Dinitz, Room squares, *The CRC Handbook of Combinatorial Designs*, Boca Raton, FL., 2007, 584-590.

[38] J.H. Dinitz, D.R. Stinson, Room squares and related designs, J.H. Dinitz (ed.) D.R.Stinson (ed.), Contemporary Design Theory: A Collection of Surveys , Wiley (1992).

[39] R.C.Mullin, W.D. Wallis, The existence of Room squares, *Aequationes Math.* 13 (1975), 1-7.

[40] S. Topalova, S. Zhelezova, On the classification of doubly resolvable designs, Proceedings of the Fourth International Workshop on Optimal Codes and Related Topics, Pamporovo,Bulgaria, 2005, 265-268.

[41] S. Topalova, S. Zhelezova, Sets of mutually orthogonal resolutions of BIBDs, Proceedings of the Elevenh International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria (2008), 280-285.

[42] S.Zhelezova, PCIMs in constructing doubly resolvable designs, *Proc. V Intern. Workshop OCRT*, White Lagoon, Bulgaria, 2007, 260-266.

[43] S.Topalova, S.Zhelezova, On an algorithm for a double resolvability test, *Proc. Intern. Conference on Theory and Applications of Mathematics and Informatics*, Alba Iulia, Romania, 2007, 323-330.

[44] R.Mathon, A.Rosa, 2-(v,k,λ) designs of small order, *The CRC Handbook of Combinatorial Designs*, Boca Raton, FL., 2007, 25-57.

[45] J. H. Dinitz, D. K. Garnick, B.D.McKay, There are 526,915,620 nonisomorphic one-factorizations of K12, *J. Combin. Des.* 2 (1994), 273Ű285.

[46] P.Kaski and P.Östergård, There are 1,132,835,421,602,062,347 nonisomorphic one-factorizations of K14, *Journal of Combinatorial Designs*, DOI: 10.1002/jcd.20188, to appear.