The Discovery of Simple 7-Designs with Automorphism Group $P\Gamma L(2, 32)$

Anton Betten, Adalbert Kerber, Axel Kohnert, Reinhard Laue, Alfred Wassermann

Universität Bayreuth,
Lehrstuhl II für Mathematik
D-95440 Bayreuth

Abstract. A computer package is being developed at Bayreuth for the generation and investigation of discrete structures. The package is a C and C++ class library of powerful algorithms endowed with some graphical interface modules. Some standard applications can be run automatically whereas research projects mostly require small C or C++ programs. The basic philosophy behind the system is to transform problems into standard problems of e.g. group theory, graph theory, linear algebra, graphics, or databases and use highly specialized routines from that field to tackle the problems. The transformations required often follow the same principles especially in questions about generation and isomorphism testing. We therefore explain some of this background.
We relate orbit problems to double cosets and offer a way to solve double coset problems in many important cases. Since the graph isomorphism problem is equivalent to some double coset problem, no polynomial algorithm can be expected in general. But the reduction techniques used still allow to solve problems of an interesting size. As examples we explain how the 7-designs in the title were found and how representatives for all isomorphism types of codes or graphs of a certain size can be obtained.
The two simple 7-designs with parameters 7-(33,8,10) and 7-(33,8,16) are presented in this paper for the first time, to the best of our knowledge they are the first 7-designs with small λ and small number of blocks ever found. Teirlinck [19] had shown previously that non trivial t-designs without repeated blocks exist for all t. The smallest parameters for the case $t = 7$ are 7-$(40320^{15} + 7, 8, 40320^{15})$.
The designs have $P\Gamma L(2, 32)$ as automorphism group, and they are constructed by the Kramer-Mesner method [7]. This group had previously been used by [13] to find simple 6-designs. The presentation of our results is compatible with that earlier publication.
The Kramer-Mesner method requires to solve a system of linear diophantine equations by a $\{0, 1\}$-vector. We used the recent improvements by Schnorr of the LLL-algorithm for finding the two solutions to the 32×97 system.

References

1. E. Arnold: Äquivalenzklassen linearer Codes, Zulassungsarbeit Bayreuth 1993.

2. E. F. Brickell: Solving low density knapsacks. *Advances in Cryptology, Proceedings of Crypto '83*, Plenum Press, New York (1984), 25–37.
3. M. J. Coster, B. A. LaMacchia, A. M. Odlyzko, C. P. Schnorr: An improved low-density subset sum algorithm. *Proceedings EUROCRYPT '91, Brighton, May 1991* in *Springer Lecture Notes in Computer Science* **547** (1991), 54–67.
4. M. R. Garey, D. S. Johnson: *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman and Company (1979).
5. C. F. Gauss: *Disquisitiones Arithmeticae*, German edition by H. Maser, Chelsea Pub., New York (1965).
6. A. Korkine, G. Zolotareff, Sur les forms quadratiques. *Math. Ann.* **6** (1873), 366–389.
7. E. S. Kramer, D. M. Mesner: t-designs on hypergraphs. *Discrete Math.* **15** (1976), 263–296.
8. D. L. Kreher, S. P. Radziszowski: Finding Simple t-Designs by Using Basis Reduction. *Congressus Numerantium* **55** (1986), 235–244.
9. J. C. Lagarias, A. M. Odlyzko: Solving low-density subset sum problems. *J. Assoc. Comp. Mach.* **32** (1985), 229–246.
10. R. Laue: Construction of combinatorial objects – A tutorial. *Bayreuther Math. Schr.* **43** (1993), 53–96.
11. A. K. Lenstra, H. W. Lenstra Jr., L. Lovász: Factoring Polynomials with Rational Coefficients, *Math. Ann.* **261** (1982), 515–534.
12. M. W. Liebeck, C. E. Praeger, J. Saxl: The maximal factorizations of the finite simple groups and their automorphism groups, *Memoirs of the Amer. Math. Soc.* **432**(1990), Chapter 9.
13. S. Magliveras, D. W. Leavitt: Simple 6-$(33, 8, 36)$ designs from $P\Gamma L_2(32)$. *Computational Group Theory*, M. D. Atkinson ed., Academic Press 1984, 337–352.
14. B. Schmalz: The t-designs with prescribed automorphism group, new simple 6-designs. *J. Combinatorial Designs* **1** (1993), 125–170.
15. C. P. Schnorr: A hierachy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science* **53** (1987), 201–224.
16. C. P. Schnorr: A More Efficient Algorithm for Lattice Basis Reduction. *J. Algorithms* **9** (1988), 47–62.
17. C. P. Schnorr, M. Euchner: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Proceedings of Fundamentals of Computation Theory 91* in *Lecture Notes in Computer Science* **529** (1991), 68–85.
18. D. Slepian: Some further theory of group codes. In I. F. Blake: *Algebraic Coding Theory: History and Development (Benchmark papers in electrical engineering and computer science)*, Stroudsburg, Dowden, Hutchinson & Ross Inc. (1973), 118–151.
19. L. Teirlinck: Non trivial t-designs without repeated blocks exist for all t. *Discrete Mathematics* **65** (1987), 301–311.
20. S. Weinrich: Konstruktionsalgorithmen für diskrete Strukturen und ihre Implementierung, Diplomarbeit Bayreuth (1993), 274 pp.

This article was processed using the LaTeX macro package with LLNCS style