

Es gibt 7-Designs mit kleinen Parametern!

A. BETTEN, A. KERBER, R. LAUE, A. WASSERMANN

Mathematisches Institut, Univ. Bayreuth
D-95440 Bayreuth

Die ersten 7-Designs zu überschaubaren Parametern haben $P\Gamma L(2, 32)$ als Gruppe von Automorphismen. Ihre Parameter sind $7-(33, 8, 10)$ und $7-(33, 8, 16)$, und sie sind zueinander komplementär. Die $\{0, 1\}$ -Lösungsvektoren des Gleichungssystems der KRAMER / MESNER-Matrix aus [3] zu konstanter rechter Seite $\lambda = 10$ bzw. 16 sind:

```
0011100010100100110001101000010010000000101101100010111100000001001001010000110111011001010111000
11000111010110110011100101111011010010011101000011111110110110101111001000100110101000111
```

Jeder Eintrag 1 in einem dieser Vektoren entspricht einer der Bahnen von $P\Gamma L(2, 32)$ auf der Menge aller 8-Teilmengen aus 33 Punkten, die das 7-Design ausmachen. Anhand dieser Informationen kann nach [3] das vollständige Design konstruiert werden. Die Berechnung der 32×97 Matrix erfolgte nach [4]. Die Lösung konnte durch eine verbesserte Version des LLL-Algorithmus zum Auffinden kurzer Vektoren in Gittern ermittelt werden (siehe [2], [5]).

Literatur

- [1] E. S. KRAMER, D. M. MESNER: t -designs on hypergraphs. *Discrete Math.* **15** (1976), 263–296.
- [2] A. K. LENSTRA, H. W. LENSTRA JR., L. LOVÁSZ: Factoring Polynomials with Rational Coefficients, *Math. Ann.* **261** (1982), 515–534.
- [3] 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.
- [4] B. SCHMALZ: t -Designs zu vorgegebener Automorphismengruppe. *Bayreuther Mathematische Schriften* **41** (1992), 1–164.
- [5] C.P. SCHNORR, M. EUCHNER: Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. *Fundamentals of Computation Theory*, FCT '91, September 1991, Berlin, Germany.