Why is $72 = 24 \cdot 3$ so hard?

Jon-Lark Kim

Department of Mathematics
University of Louisville, KY, USA

Poster Session: Coding Theory
RICAM and RISC, Linz, Austria
May 1, 2006

Problem

Does there exist a Type II $[24k, 12k, 4k + 4]$ code $C(k)$ for $k \geq 3$?

- A binary self-dual code whose weights are divisible by 4 is called Type II. Otherwise, Type I.
- Binary self-dual codes with these parameters are called extremal.
- If $k = 1$, then $C(1)$ is the $[24, 12, 8]$ Golay code. This is unique (Pless, 1968).
- If $k = 2$, then $C(2)$ is the extended quadratic residue code. This is unique (Houghten, Lam, Thiel, and Parker, 2003).
- The existence of $C(k)$ for $k = 3$ (or $n = 72$) is one of the long-standing open problems in coding theory! It is unknown for higher k too.

Related Facts

- The weight enumerator of a putative Type II $[72, 36, 16]$ code $C(3)$:
  $W = 1 + 249,849y^{16} + 18,106,704y^{20} +$
  $462,962,955y^{24} + 4,397,342,400y^{28} +$
  $16,602,715,899y^{32} + 25,756,721,120y^{36} + \cdots$
- The only possible "prime" orders of an automorphism of $C(3)$ are 2,3,5, and 7.
- The existence of $C(3) \Longleftrightarrow$ the existence of a Type I $[70, 35, 14]$ code. (Rains, 1998)
- The weight enumerator of a Type I $[70, 35, 14]$ code:
  $W = 1 + 11,730y^{14} + 150,535y^{16} + 1,345,960y^{18} + \cdots$.
- The existence of $C(3) \Longrightarrow$ the existence of a Type I $[72, 36, 14]$ code. (Gulliver, Harada, Kim, 2003).

Remarks

- From Brouwer's Table, it is unknown whether there exist a binary linear $[72, 36, 16]$ code. There is a $[72, 36, 15]$ code from a $[73, 36, 16]$ cyclic code.
- Possible attempts to construction $C(3)$ by (Dougherty, Kim, and Sole, 2006)

  I. SRG (Strongly Regular Graphs) with parameters (36,15,6,6) produce a lot of Type II $[72, 36, 12]$ codes.

  II. DRT (Doubly Regular Tournaments) of order 36 produce Type II $[72, 36, 8 \text{ or } 12]$ codes.

  It is hoped that $d = 16$ is possible if there is enough data for SRG and DRT of the above parameters.

Monetary Prizes

This content is from
`http://academic.scranton.edu/faculty/doughertys1/`

- N.J.A. Sloane \$10 (1973)
- F.J. MacWilliams \$10 (1977) - invalid

  The following prizes were announced in the Yamagata conference, October, 2000 and at WCC2001 in Paris.
- S.T. Dougherty \$100 for the existence of $C(3)$
- M. Harada \$200 for the nonexistence of $C(3)$
- The prize is awarded only once and the result must be published in a refereed reputable mathematics journal. All decisions about the prize are decided by those offering the prize.