On "On Self-Dual, Doubly Even Codes of Length 32"

Martin Leslie

Department of Mathematics
University of Arizona

April 30, 2009

Why we care

Theorem (Conway-Sloane)

An odd unimodular lattice Λ in $\mathbb{R}^{32}$ with $\min \Lambda = 4$ is uniquely determined by a code C, constructed from Λ, which is a self-dual, doubly even binary code of length 32 with minimum weight at least 8.

- The paper of Koch tells us that there are precisely five of these codes, which, with a little extra work, shows that there are precisely five such lattices.

History

- Conway and Pless in their 1980 paper "On the enumeration of self dual codes" found all 85 inequivalent binary self-dual doubly even codes of length 32 including 5 of minimal weight 8.
- Their method is very laborious and requires finding the automorphism groups of all these codes and using a counting formula to check that there are only 85 of them.
- Koch's 1989 paper "On self-dual, doubly even codes of length 32" gives a simpler proof that there are only 5 such codes of minimum weight 8.

Some coding theory

- An $[n, k, d]$ *binary linear code* is a k-dimensional subspace of $\mathbb{F}_2^n$ which has minimum weight of a codeword d.
- The dual of a code C is

$$C^\perp = \{x \in \mathbb{F}_2^n \mid \langle x, c \rangle = 0 \text{ for all } c \in C\}.$$

  A code is *self-dual* if $C = C^\perp$.
- A code is *doubly even* if the weight of every codeword is divisible by 4.
- Two codes are *equivalent* if one can be transformed into the other by a permutation of the columns.

CP codes

- Define a *CP code* to be a length 32, self-dual doubly even binary code of minimum weight 8.
- Note that this is a $[32, 16, 8]$ code so has $2^{16} = 65\,356$ codewords.
- The result of Koch's paper is that there are exactly 5 inequivalent CP codes, denoted by RM, QR, F, G and U.
- RM is the well known Reed–Muller code $\mathcal{R}(2, 5)$.
- QR is the extended quadratic reciprocity code corresponding to $p = 31$.

F

- Let H and H^* be extended quadratic reciprocity and quadratic non-reciprocity codes for $p = 7$ and define F to be the set of codewords of the form

$$(h_1 + h_2^*, h_1 + h_2 + h_2^*, h_2 + h_1^* + h_2^*, h_2 + h_1^*)$$

where $h_1, h_2 \in H$ and $h_1^*, h_2^* \in H^*$.

G

- This code is given by a nice geometrical description of a basis.
- Write the 32 positions of a codeword in two 4×4 matrices and then the sixteen basis vectors have one 1 in the left hand matrix and seven 1's in the corresponding row and column of the right hand matrix.
- For example, one basis vector is

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{matrix} \qquad \begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix}$$

U

- We specify codewords by giving their *support*: a subset of $\{1, 2, \ldots, 32\}$ which is the positions of the code that are 1.
- Let Γ be the group generated by the permutation

$$(5, 9, 13, 17, 21, 25, 29)(6, 10, 14, 18, 22, 26, 30) \times (7, 11, \ldots, 31)(8, 12, \ldots, 32).$$

- Then U is generated as a Γ-module by

$$\{1, 2, 3, 4, 5, 6, 7, 8\}, \{1, 5, 9, 13, 17, 21, 25, 29\},$$
$$\{10, 12, 15, 16, 23, 24, 26, 28\}, \{3, 4, 14, 16, 19, 20, 22, 24\},$$
$$\{6, 7, 10, 12, 26, 28, 30, 31\}, \{2, 4, 10, 11, 18, 20, 26, 27\},$$
$$\{6, 7, 15, 16, 23, 24, 30, 31\}, \{2, 3, 7, 8, 18, 19, 31, 32\}.$$

Some invariant theory

- A theorem of Gleason says that for a self-dual doubly even code, if A_w is the number of weight w codewords, the *weight enumerator*

$$W(x,y) = \sum A_w x^n y^{n-w}$$

is a polynomial in

$$\theta = x^8 + 14x^4y^4 + y^8 \text{ and } \phi = x^4y^4(x^4 - y^4)^4.$$

- So we must have $W(x,y) = a\theta^4 + b\theta\phi$ which yields $a = 1$ and $b = -56$. Thus

$$W(x,y) = y^{32} + 620x^8y^{24} + 13888x^{12}y^{20} + 36518x^{16}y^{16} + 13888x^{20}y^{12} + 620x^{24}y^8 + x^{32}.$$

Some design theory

- A t-design with parameters (v, k, λ) is a collection, $\mathcal{D}$, of subsets of a set S of v points such that every member of $\mathcal{D}$ contains k points and any set of t-points is contained in exactly λ members of $\mathcal{D}$.
- It can be proven (using the self-dual and doubly even hypotheses) that the subsets of $S = \{1, 2, \ldots, 32\}$ that support codewords of weight 8 in a CP code form a 3-design with parameters $(32, 8, 7)$.
- So if we fix three positions a, b, c of a CP code then there are exactly seven codewords of weight 8 containing those positions.

Configurations

- Call the equivalence class of such a set of 7 codewords a *configuration*.
- Each pair of words of a configuration must overlap in exactly one position that is not one of a, b, c.
- The words of a configuration are determined, up to equivalence, by positions which occur three or more times.
- Each word of a configuration must contain such a position, a pair of such positions can only occur in one word in the configuration and each word of the configuration can contain no more than three such positions.

Idea of the proof

- Write down all possible configurations from conditions above.
- Find all possible configurations of codes RM, QR, F, G using knowledge of their structure. Find three configurations of U.
- For each configuration scheme, show that it can come from only the codes listed.

Table of configuration schemes

TABLE I

1	*d*	*d*	*d*	*d*	*d*	*d*	*d*	RM, F, U
2	*de*	*d*	*d*	*d*	*d*	*e*	*e*	G, U
3	*de*	*d*	*d*	*d*	*e*	*e*	*e*	G
4	*d*	*d*	*d*	*d*	*e*	*e*	*e*	—
5	*de*	*df*	*d*	*d*	*ef*	*e*	*f*	—
6	*de*	*df*	*dg*	*d*	*ef*	*eg*	*fg*	QR, G
7	*de*	*df*	*d*	*e*	*e*	*f*	*f*	—
8	*def*	*d*	*d*	*e*	*e*	*f*	*f*	G
9	*df*	*dg*	*d*	*ef*	*eg*	*e*	*fg*	—
10	*def*	*dg*	*d*	*eg*	*e*	*fg*	*f*	—
11	*def*	*dg*	*dh*	*eg*	*eh*	*fg*	*fh*	—
12	*def*	*dgh*	*d*	*eg*	*eh*	*fg*	*fh*	—
13	*def*	*dgh*	*di*	*egi*	*eh*	*fg*	*fhi*	U
14	*def*	*dgh*	*dij*	*egi*	*ehj*	*fgj*	*fhi*	F, G

A useful fact

Theorem

A CP code which contains an $[n, k] = [15, 4]$ *code is equivalent to either RM, F or G.*

Proof.

Uses classification of self-dual doubly even codes of length 24. □