

# The mass of extremal doubly-even self-dual codes of length 40

Oliver D. King \*

April 25, 2001

## Abstract

We determine the mass of extremal doubly-even self-dual binary codes of length 40. It follows that there are at least 12579 such codes.

*keywords: extremal Type II codes, unimodular lattices*

## I Introduction

We assume the reader is acquainted with codes and lattices; see [1] and [2] for background. A binary code is said to be of Type II if it is self-dual and it is doubly even (meaning the Hamming weight of each codeword is divisible by 4). Type II codes of length  $n$  exist only for  $n$  divisible by 8, and they have been completely enumerated (up to equivalence) for  $n = 0$  (1 code),  $n = 8$  (1 code),  $n = 16$  (2 codes),  $n = 24$  (9 codes), and  $n = 32$  (85 codes) (see [3, 4, 5]). The mass  $M_n$  of Type II codes of length  $n$  is defined to be

$$M_n = \sum_C \frac{1}{|\text{Aut}(C)|}$$

with the sum taken over a complete set of inequivalent Type II codes  $C$  of length  $n$ . MacWilliams, Sloane and Thompson [6] have shown that

$$M_n = \frac{2}{n!} \prod_{i=1}^{n/2-2} (2^i + 1)$$

for  $n$  divisible by 8. This formula provides a check for the enumerations of Type II codes of length  $n \leq 32$ , and according to Rains and Sloane in [1] it suggests that “length 32 is probably a good place to stop,” since

$$M_{40} = \frac{2377696177368502121671913075767}{135923795925811870040064000} = 17492.86$$

(which implies that there are at least 17493 Type II codes of length 40).

The minimal distance  $d$  of any Type II code of length  $n$  satisfies  $d \leq 4\lfloor n/24 \rfloor + 4$ , and a code for which equality holds is called extremal [7]. Notice that for  $n = 24, 32$ , and 40, a Type II code is extremal if its minimal distance is 8. The Golay code  $g_{24}$  is the unique extremal Type II code of length 24 [8], and there are five extremal Type II codes of length 32 [4]. By a computation involving Fourier coefficients of Siegel Eisenstein series we have shown:

**Theorem 1** *The mass of extremal Type II codes of length 40 is*

$$\frac{888096280193441}{70601932800} = 12578.92.$$

Thus there are at least 12579 inequivalent extremal Type II codes of length 40. We shall not conjecture on whether length 32 is a good place to stop with the enumeration of extremal Type II codes, but do note that 1000 such codes of length 40 have already been constructed by Harada in [9]. (See also [10, 11, 12, 13, 14, 15, 16], which collectively construct between 100 and 200 inequivalent extremal Type II codes of length 40, some of which may be equivalent to codes in [9].)

---

\*Dept. of Mathematics, University of California, Berkeley, CA 94720-3840 (e-mail: king@math.berkeley.edu)

**Remark 1** We could tighten the lower bound of 12579 a bit by accounting for the contribution that the known codes make to the mass, since many of them have nontrivial automorphism groups. For example, the 45 codes in [14] each have automorphisms of order 5, so their combined mass is at most 9, and we can add  $36 = 45 - 9$  to the lower bound of 12579.

## II Overview of computation

For a root system  $R$ , let  $w(R)$  denote the order of the Weyl group of  $R$ , and let  $m_n(R)$  denote the mass of the even unimodular  $n$ -dimensional lattices with root system  $R$ . There is a one-to-one correspondence between equivalence classes of even unimodular  $n$ -dimensional lattices  $\Lambda$  with root system  $A_1^n$  and equivalence classes of Type II codes  $C$  of length  $n$  with minimal distance  $d \geq 8$ . This correspondence is induced by the map  $\Lambda \mapsto \Lambda/Q \cong C$ , where  $Q$  is the sublattice of  $\Lambda$  generated by the root system  $A_1^n$ ; the inverse map, taking a code  $C$  of length  $n$  to the lattice  $\Lambda = \{x \in \mathbb{R}^n \mid \sqrt{2}x \pmod{2} \in C\}$ , is known as Construction A [17]. The correspondence has the property that  $|\text{Aut}(\Lambda)| = w(A_1^n) \cdot |\text{Aut}(C)|$ , where  $w(A_1^n) = 2^n$ . (This is the simplest case of a more general correspondence between lattices with root systems of full rank and self-dual codes, described by Venkov in [18].) Thus we have

$$\sum_C \frac{1}{|\text{Aut}(C)|} = \sum_\Lambda \frac{2^n}{|\text{Aut}(\Lambda)|} = 2^n \cdot m_n(A_1^n)$$

with the first sum taken over a complete set of inequivalent Type II codes  $C$  of length  $n$  and minimal distance  $d \geq 8$ , and the second sum taken over a complete set of inequivalent even unimodular  $n$ -dimensional lattices  $\Lambda$  with root system  $A_1^n$ . Theorem 1 then follows from the computation of  $m_{40}(A_1^{40})$ , which we describe below.

In [19] we gave an algorithm (suggested by Borcherds) for computing the mass of even unimodular  $n$ -dimensional lattices having any given root system  $R$ , and for  $n = 32$  we computed this mass for each  $R$ . We were mainly interested in  $R = \emptyset$ , but to compute  $m_n(R)$  we first had to compute  $m_n(S)$  for all  $S$  into which  $R$  embeds. To speed up the computation here, only those root systems of rank  $n = 40$  into which  $A_1^{40}$  embeds need be considered, namely those whose components are all of the form  $A_1, E_7, E_8$ , or  $D_k$  for even  $k$ . (The computation in [19] took about two weeks; the computation here took under an hour.) Order all such root systems  $R_1, \dots, R_s$  so that  $\det(R_i) \geq \det(R_j)$  if  $i > j$ . Then the mass  $m_n(R_i)$  of lattices with root system  $R_i$  may be computed using the formula

$$m_n(R_i) = \frac{1}{r(R_i, R_i)} \left\{ m_n \cdot a_n(R_i) - \sum_{j=1}^{i-1} r(R_j, R_i) m_n(R_j) \right\}$$

where  $r(M, N)$  is the number of representations of  $N$  by  $M$ ,

$$m_n = \sum_\Lambda \frac{1}{|\text{Aut}(\Lambda)|}$$

is the mass of even unimodular  $n$ -dimensional lattices (with the sum taken over a complete set of inequivalent even unimodular  $n$ -dimensional lattices  $\Lambda$ ), and

$$a_n(N) = \frac{1}{m_n} \sum_\Lambda \frac{r(\Lambda, N)}{|\text{Aut}(\Lambda)|}$$

is the average number of representations of  $N$  by a complete set of inequivalent even unimodular  $n$ -dimensional lattices  $\Lambda$ . For root lattices  $R$  and  $S$ , calculating  $r(R, S)$  is basically combinatorial; the problem is NP-Hard, but is still manageable in dimension 40. By the Minkowski-Siegel mass formula (see [2]), for positive  $n$  divisible by 8 we have

$$m_n = \frac{|B_{n/2}|}{n} \prod_{i=1}^{n/2-1} \frac{|B_{2i}|}{4i}$$

Table 1: Masses of even unimodular 40-dimensional lattices with root system  $R$ , where  $A_1^{40}$  embeds into  $R$  and  $R$  has least 24 components  $A_1$ .

$R$	$m_{40}(R) \cdot w(R)$	$R$	$m_{40}(R) \cdot w(R)$
$A_1^{40}$	$\frac{888096280193441}{70601932800}$	$A_1^{26} D_6 E_8$	$\frac{1}{11232}$
$A_1^{36} D_4$	$\frac{9170954969}{580608}$	$A_1^{26} D_6 D_8$	$\frac{3883}{2880}$
$A_1^{34} D_6$	$\frac{4756559}{13056}$	$A_1^{26} D_4^2 D_6$	$\frac{43841669}{34560}$
$A_1^{33} E_7$	$\frac{16867}{69120}$	$A_1^{26} D_4 D_{10}$	$\frac{187}{432}$
$A_1^{32} E_8$	$\frac{233}{1904640}$	$A_1^{26} D_{14}$	$\frac{1}{11232}$
$A_1^{32} D_8$	$\frac{1646341}{368640}$	$A_1^{25} D_8 E_7$	$\frac{193}{60480}$
$A_1^{32} D_4^2$	$\frac{55807181887}{4423680}$	$A_1^{25} D_4^2 E_7$	$\frac{7669}{3456}$
$A_1^{30} D_4 D_6$	$\frac{60964691}{69120}$	$A_1^{24} E_8^2$	$\frac{1}{489646080}$
$A_1^{30} D_{10}$	$\frac{7757}{92160}$	$A_1^{24} D_8^2$	$\frac{567733}{21288960}$
$A_1^{29} D_4 E_7$	$\frac{2209}{2304}$	$A_1^{24} D_8 E_8$	$\frac{1}{138240}$
$A_1^{28} D_6^2$	$\frac{13564391}{552960}$	$A_1^{24} D_6 D_{10}$	$\frac{799}{15120}$
$A_1^{28} D_4^3$	$\frac{564203333}{69120}$	$A_1^{24} D_4^4$	$\frac{52842490261}{11612160}$
$A_1^{28} D_4 E_8$	$\frac{1}{1344}$	$A_1^{24} D_4^2 E_8$	$\frac{49}{18432}$
$A_1^{28} D_4 D_8$	$\frac{55147}{3456}$	$A_1^{24} D_4^2 D_8$	$\frac{3057517}{92160}$
$A_1^{28} D_{12}$	$\frac{365}{157248}$	$A_1^{24} D_4 D_6^2$	$\frac{49858969}{483840}$
$A_1^{27} D_6 E_7$	$\frac{2257}{27648}$	$A_1^{24} D_4 D_{12}$	$\frac{1163}{69120}$
$A_1^{26} E_7^2$	$\frac{37}{399360}$	$A_1^{24} D_{16}$	$\frac{443}{61205760}$

where  $B_i$  is the  $i$ th Bernoulli number. Let  $B$  denote  $1/2$  times the Gram matrix of the lattice generated by  $R$ . Then by a theorem of Siegel's (see [20, Theorem 6.8.1]),  $a_n(R) = 1/2 \cdot c_{n,n/2}(B)$ , where  $c_{n,k}(B)$  is given by

$$(-1)^{nk/2} 2^{n(k-(n-1)/2)} (\det B)^{(2k-n-1)/2} b(B, k) \prod_{i=2k-n+1}^{2k} \frac{\pi^{i/2}}{\Gamma(i/2)}.$$

Here  $b(B, k)$  is the Siegel series, which can be calculated using the formula given by Katsurada in [21]. (For  $k > n$ ,  $c_{n,k}(B)$  is the Fourier coefficient of  $B$  in the Siegel Eisenstein series of degree  $n$  and weight  $k$ .) The key is that  $a_n(R)$  can be computed without knowing what all the even unimodular  $n$ -dimensional lattices  $\Lambda$  are, which is fortunate since there are at least  $2m_n$  of them, and  $m_{40} = 4.39 \times 10^{51}$ . Of the root systems  $R$  into which  $A_1^{40}$  embeds, there are 475 for which the mass  $m_{40}(R)$  is nonzero; Table 1 lists  $m_{40}(R) \cdot w(R)$  for those  $R$  which have at least 24 components  $A_1$ .

**Remark 2** From this table we can also recover the mass of extremal Type II codes of length 24 and 32, since  $m_{24}(A_1^{24}) \cdot w(A_1^{24}) = m_{40}(A_1^{24} E_8^2) \cdot 2w(A_1^{24} E_8^2)$  and  $m_{32}(A_1^{32}) \cdot w(A_1^{32}) = m_{40}(A_1^{32} E_8) \cdot w(A_1^{32} E_8)$ ; these values agree with the known enumerations by Pless and Conway.

## Acknowledgments

Thanks to Richard Borcherds for many helpful suggestions, and to Richard Fateman for advice on Lisp, which was used for all of the computations. This work was partially supported by grants from the National Science Foundation and the Royal Society.

## References

- [1] E. M. Rains and N. J. A. Sloane, “Self-dual codes,” in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. New York: Elsevier, 1998.
- [2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd Ed. New York: Springer-Verlag, 1998.
- [3] V. S. Pless, “A classification of self-orthogonal codes over  $GF(2)$ ,” *Discrete Math.*, vol. 3, pp. 209–246, 1972.
- [4] J. H. Conway and V. S. Pless, “On the enumeration of self-dual codes,” *J. Combin. Theory Ser. A*, vol. 28, pp. 26–53, 1980.
- [5] J. H. Conway, V. S. Pless, and N. J. A. Sloane, “The binary self-dual codes of length up to 32: A revised enumeration,” *J. Combin. Theory Ser. A*, vol. 60, pp. 183–195, 1992.
- [6] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson, “Good self-dual codes exist,” *Discrete Math.*, vol. 3, pp. 153–162, 1972.
- [7] C. L. Mallows and N. J. A. Sloane, “An upper bound for self-dual codes,” *Information and Control*, vol. 22, pp. 188–200, 1973.
- [8] V. S. Pless, “On the uniqueness of the Golay codes,” *J. Combin. Theory Ser. A*, vol. 5, pp. 215–228, 1968.
- [9] M. Harada, “Existence of new extremal doubly-even codes and extremal singly-even codes,” *Des. Codes Cryptog.*, vol. 8, pp. 273–283, 1996.
- [10] V. D. Tonchev, “Block designs of Hadamard type and self-dual codes,” *Prob. Pered. Inform.*, vol. 19, pp. 25–30, 1983. English translation in *Probl. Inf. Transm.*, vol. 19, pp. 270–274, 1983.
- [11] V. D. Tonchev, “Self-orthogonal designs and extremal doubly-even codes,” *J. Combin. Theory Ser. A*, vol. 52, pp. 197–205, 1989.
- [12] F. C. Bussemaker and V. D. Tonchev, “Extremal doubly-even codes of length 40 derived from Hadamard matrices or order 20,” *Discrete Math.*, vol. 80, pp. 317–321, 1990.
- [13] V. Y. Yorgov, “Binary self-dual codes with an automorphism of odd order,” *Prob. Pered. Inform.*, vol. 19, pp. 11–24, 1983. English translation in *Probl. Inf. Transm.*, vol. 19, pp. 260–270, 1983.
- [14] V. Y. Yorgov and N. P. Ziapkov, “Doubly-even self-dual  $[40,20,8]$  codes with an automorphism of odd order,” *Prob. Pered. Inform.*, vol. 32, 1996. English translation in *Probl. Inf. Transm.*, vol. 32, pp. 253–257, 1996.
- [15] M. Ozeki, “Hadamard matrices and doubly-even self-dual error-correcting codes,” *J. Combin. Theory Ser. A*, vol. 44, pp. 274–287, 1987.
- [16] M. Harada, T. A. Gulliver and H. Kaneta, “Classification of extremal double circulant self-dual codes of length up to 62,” *Discrete Math.*, vol. 188, pp. 127–136, 1998.
- [17] J. Leech and N. J. A. Sloane, “Sphere packing and error-correcting codes,” *Canad. J. Math.*, vol. 23, pp. 718–745, 1971. Also Chapter 5 in [2].
- [18] B. B. Venkov, “The classification of integral even unimodular 24-dimensional quadratic forms,” *Trudy Mat. Inst. imeni V. A. Steklova*, vol. 148, pp. 65–76, 1978. Also Chapter 16 in [2].
- [19] O. D. King, “A mass formula for unimodular lattices with no roots,” preprint. Available at [arXiv:math.NT/0012231](https://arxiv.org/abs/math.NT/0012231)
- [20] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge Tracts in Math., vol. 106. Cambridge: Cambridge Univ. Press, 1993.
- [21] H. Katsurada, “An explicit formula for Siegel series,” *Amer. J. Math.*, vol. 121, pp. 415–452, 1999