The Ternary Golay Code, the Integers Mod 9 and the Coxeter-Todd Lattice*

A. R. Calderbank and *N. J. A. Sloane*
Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

October 30, 1995

ABSTRACT

The 12-dimensional Coxeter-Todd lattice can be obtained by lifting the ternary Golay code to a code over the integers mod 9 and applying Construction A.

* *IEEE Trans. Inform. Theory*, submitted.

Several recent papers have pointed out connections between codes over $\mathbb{Z}_4$ and lattices [1], [3]. It is the aim of this note to show that the Coxeter-Todd lattice K_{12} ([4], [5], Chap 4., Section 9) can be obtained in a similar way from a code over $\mathbb{Z}_9$.

Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ denote the ring of integers mod m. Let C be a cyclic code of length n over $\mathbb{Z}_p$, where p is a prime such that $(n, p) = 1$, with generator polynomial $g(x)$. If α is a primitive element of $\mathbb{Z}_p$, let S denote the set of s such that α^s is a root of $g(x)$. It is pointed out in [2] that C is self-orthogonal if and only if $S \cup (-S)$ contains representatives from every residue class mod n. Furthermore, for $a = 2, 3, \ldots$, exactly the same condition is also necessary and sufficient for the Hensel lift (cf. [6]) of C to a cyclic code over $\mathbb{Z}_{p^a}$ to be self-orthogonal mod p^a. Self-orthogonality of the lifted code is a purely combinatorial property of the roots of the original code.

Consider now the $[11, 5, 6]$ self-orthogonal ternary Golay code, with generator polynomial

$$g(x) = x^6 - x^5 - x^4 - x^3 + x^2 + 1$$

([7], p. 482). This lifts to

$$G(x) = x^6 + 2x^5 - 4x^4 + 2x^3 + x^2 - 3x + 1 \ ,$$

a divisor of $x^{11} - 1 \bmod 9$, which by the previous remark generates a self-orthogonal code over $\mathbb{Z}_9$. Appending a 0 to these words and adjoining the all-1's vector as an additional generator, we obtain a self-dual code $\mathcal{G}$ of length 12 over $\mathbb{Z}_9$.

By applying Construction A (cf. [5], Chaps. 5, 7), that is, taking all vectors in $\mathbb{Z}^{12}$ that are congruent to any codeword of $\mathcal{G}$ mod 9, and rescaling by dividing by $\sqrt{3}$, we obtain the Coxeter-Todd lattice: a 12-dimensional lattice of determinant 729, minimal squared length 4 and 756 minimal vectors. We omit the straightforward proof that this is isomorphic to the standard construction from a code (the "hexacode") of length 6 over $GF(4)$ ([4], [5, p. 128], [8]).

References

[1] A. Bonnecaze, A. R. Calderbank and P. Solé, Quaternary quadratic residue codes and unimodular lattices, *IEEE Trans. Inform. Theory*, **41** (1995), 366–377 and 1536.

[2] A. R. Calderbank, W.-C. W. Li and B. Poonen, A 2-adic approach to the analysis of cyclic codes, preprint.

[3] A. R. Calderbank and N. J. A. Sloane, Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices, *J. Algebraic Combinatorics*, submitted.

[4] J. H. Conway and N. J. A. Sloane, The Coxeter-Todd lattice, the Mitchell group and related sphere packings, *Math. Proc. Comb. Phil. Soc.*, **93** (1983), 421–440.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups (Second Edition)*, Springer-Verlag, NY, 1993.

[6] F. Q. Gouvêa, *P-adic Numbers*, Springer-Verlag, NY, 1993, esp. §3.4.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[8] N. J. A. Sloane, Self-dual codes and lattices, in *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math., Vol. 34, American Mathematical Society, Providence, RI, 1979, pp. 273–308.