We end this paper with the following.

Question. Is the lattice $A_{2^k}(G_{2^k})$ D_{24}, A_1^{24} and Λ_{24} if $k \equiv 0, 1$ and $2 \pmod 3$, for all k?

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 1194–1205.

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

[3] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes and Cryptogr.* **6** (1995), 21–35.

where v is listed in Table 1 for $3 \leq k \leq 20$. Note that $X^{23} - 1 = (X-1)gf$ where f is the reciprocal polynomial of g.

Table 1: The value v in the generator polynomials

k	3	4	5	6	7	8	9	10	11
v	2	10	10	42	106	234	490	490	490
k	12	13	14	15	16	17	18	19	20
v	2538	2538	2538	18922	18922	84458	215530	215530	215530

The lifted Golay code G_{2^k} over $\mathbb{Z}_{2^k}$ is self-dual [3]. Moreover it is easy to see that G_{2^k} is Type II by checking the Euclidean weight of the rows of the generator matrix. Thus $A_{2^k}(G_{2^k})$ is an even unimodular lattice, that is, one of the Niemeier lattices. Since G_{2^k} is type 1^{24}, that is, a free module, it is easy to obtain a generator matrix of the lattice $A_{2^k}(G_{2^k})$. Using Magma, we obtained the minimum norm μ and the kissing number N of the lattices $A_{2^k}(G_{2^k})$ for $3 \leq k \leq 20$. These values are listed in Table 2. Niemeier lattices D_{24} and A_1^{24} are uniquely determined by the kissing numbers 1104 and 48, respectively. Thus the lattices $A_{2^k}(G_{2^k}), 3 \leq k \leq 20$, are determined by their kissing numbers and minimum norms. Therefore we have the following characterization of these lattices.

Proposition 2 *For $k \leq 20$, $A_{2^k}(G_{2^k}) = D_{24}, A_1^{24}$ and Λ_{24} if $k \equiv 0, 1$ and $2 \pmod 3$, respectively.*

Table 2: The lattices $A_{2^k}(G_{2^k})$

k	μ	N	k	μ	N
3	2	1104	12	2	1104
4	2	48	13	2	48
5	4	196560	14	4	196560
6	2	1104	15	2	1104
7	2	48	16	2	48
8	4	196560	17	4	196560
9	2	1104	18	2	1104
10	2	48	19	2	48
11	4	196560	20	4	196560

The minimum Euclidean weight $d_E(G_{2^k})$ of the lifted Golay code G_{2^k} is determined by the minimum norm μ_{2^k} of $A_{2^k}(G_{2^k})$, that is, $d_E(G_{2^k}) = 2^{k+1}, 2^{k+1}$ and 2^{k+2} if $k \equiv 0, 1$ and $2 \pmod 3$, respectively.

unimodular lattice Λ is *even* if the norm of every vector x of Λ is even. The minimum norm of Λ is the smallest norm among all nonzero vectors of Λ. The number of vectors of minimum norm is called the kissing number. There are exactly 24 distinct even unimodular lattices in dimension 24, one of which has minimum norm 4. These even unimodular lattices are called *Niemeier lattices*, and the unique even unimodular lattice with minimum norm 4 is called the *Leech lattice* Λ_{24}. The Niemeier lattices are characterized by their root systems. For example, D_{24} and A_1^{24} denote the Niemeier lattices with root systems D_{24} and A_1^{24}, respectively. Their kissing numbers are 1104 and 48, respectively.

We now give definitions for self-dual codes over $\mathbb{Z}_{2k}$ (see [1] for a complete description). A code C of length n over $\mathbb{Z}_{2k}$ (or a $\mathbb{Z}_{2k}$-code of length n) is a $\mathbb{Z}_{2k}$-submodule of $\mathbb{Z}_{2k}^n$ where $\mathbb{Z}_{2k}$ is the ring of integers modulo $2k$. An element of C is called a codeword of C. A *generator* matrix of C is a matrix whose rows generate C. The *Hamming weight* $wt_H(x)$ of a vector x in $\mathbb{Z}_{2k}^n$ is the number of non-zero components. The *Euclidean weight* $wt_E(x)$ of a vector $x = (x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^n \min\{x_i^2, (2k - x_i)^2\}$. The minimum Hamming and Euclidean weights, d_H and d_E, of C are the smallest Hamming and Euclidean weights among all non-zero codewords of C, respectively. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, we define the inner product of x and y in $\mathbb{Z}_{2k}^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_{2k}^n |\ x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^\perp$. Self-dual codes with the property that all Euclidean weights are divisible by $4k$ are called *Type II* [1].

By applying Construction A to self-dual $\mathbb{Z}_{2k}$-codes, we have the following construction of lattices. Define the reduction modulo $2k$

$$\rho : \mathbb{Z}^n \to \mathbb{Z}_{2k}^n$$

by $\rho(x_1, \ldots, x_n) = (x_1 \pmod{2k}, \ldots, x_n \pmod{2k})$.

Proposition 1 (Bannai et al. [1]) *If C is a self-dual code of length n over $\mathbb{Z}_{2k}$, then the lattice*

$$A_{2k}(C) = \frac{1}{\sqrt{2k}}\{x \in \mathbb{Z}^n \mid \rho(x) \in C\}$$

is an n-dimensional unimodular lattice. The minimum norm is $\min\{2k, d_E/2k\}$ where d_E is the minimum Euclidean weight of C. Moreover if C is Type II then the lattice $A_{2k}(C)$ is even.

3 The Lattices from the Lifted Golay Codes

The lifted Golay code G_{2^k} over $\mathbb{Z}_{2^k}$ Calderbank and Sloane [3] is the extended code obtained by appending **1** to the generator matrix of the cyclic code with generator polynomial g, and is obtained from the binary extended cyclic Golay code by lifting the generator polynomial. The generator polynomial g is defined as

$$X^{11} + vX^{10} + (v-3)X^9 - 4X^8 - (v+3)X^7 - (2v+1)X^6 \\ -(2v-3)X^5 - (v-4)X^4 + 4X^3 + (v+2)X^2 + (v-1)X - 1,$$

The Lifted Golay Codes and Their Lattice*

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560

October 26, 1999

Abstract

The lifted Golay code over $\mathbb{Z}_4$ gives a very simple construction of the Leech lattice via Construction A. Recently, the lifted Golay code over $\mathbb{Z}_{2^k}$ was introduced by Calderbank and Sloane. This raises the question, do other lifted Golay codes give the Leech lattice? In this note, we determine if the Leech lattice is constructed from the lifted Golay code over $\mathbb{Z}_{2^k}$ for $3 \leq k \leq 20$.

1 Introduction

Recently there has been interest in the relationships between self-dual codes over the ring $\mathbb{Z}_{2k}$ of integers modulo $2k$ and unimodular lattices. In particular, the lifted Golay code over $\mathbb{Z}_4$ was defined in [2], and this code gives a very simple construction of the Leech lattice by Construction A [2]. The lifted Golay code of length 24 over $\mathbb{Z}_{2^k}$ was introduced by Calderbank and Sloane [3], and is constructed from the binary extended cyclic Golay code by Hensel lifting. By Construction A, a Niemeier lattice (that is, a 24-dimensional even unimodular lattice) can be obtained from the lifted Golay code. This leads to the question, do other lifted Golay codes give the Leech lattice by Construction A? In this note, we determine which Niemeier lattices are constructed from the lifted Golay codes over $\mathbb{Z}_{2^k}$ for $3 \leq k \leq 20$.

2 Construction A and Self-Dual Codes

A (Euclidean) lattice Λ in $\mathbb{R}^n$ is integral if $\Lambda \subseteq \Lambda^*$ where Λ^* denotes the dual lattice of Λ defined in the standard way. An integral lattice with $\Lambda = \Lambda^*$ is called *unimodular*. A

*This manuscript is based on a joint work with T.A. Gulliver.