Des. Codes Cryptogr. (2012) 65:107–113
DOI 10.1007/s10623-012-9667-5

The generating rank of the space of short vectors in the Leech lattice mod 2

Andries Brouwer · Çiçek Güven

Received: 6 July 2011 / Revised: 19 March 2012 / Accepted: 22 March 2012 /
Published online: 10 April 2012

Abstract Consider the partial linear space on the images in $\Lambda/2\Lambda$ of the shortest nonzero vectors in the Leech lattice Λ, where the lines are the triples of vectors adding up to zero. We determine the universal embedding dimension and the generating rank of this space (both are 24) and classify its hyperplanes.

Keywords Leech lattice · Universal embedding dimension · Generating rank · Golay code

Mathematics Subject Classification 05B25 · 11H31 · 51E26

1 Introduction

Let Λ denote the Leech lattice, the unique even unimodular lattice without roots in $\mathbb{R}^{24}$. There are 196,560 shortest nonzero vectors in Λ, and they map into 98,280 points in $\Lambda/2\Lambda$, where each point $\bar{x}$ has preimage $\{x, -x\}$. The aim of this note is to prove the following.

Theorem 1 *Let (X, L) be the partial linear space where the set of points is the set of* 98,280 *images in $\Lambda/2\Lambda$ of the shortest nonzero vectors in Λ, and the set of lines is the collection of triples of points adding up to zero (in $\Lambda/2\Lambda$). Then (X, L) has universal embedding dimension and generating rank* 24*, and three types of hyperplanes, as described in Sect.* 5.6 *below.*

We also give details on the related partial linear space on the octads.

The Leech lattice and extended binary Golay code are very well-known objects. A standard reference is Conway and Sloane [3].

This is one of several papers published together in *Designs, Codes and Cryptography* on the special topic: "Geometric and Algebraic Combinatorics".

A. Brouwer (✉) · Ç. Güven
Department of Mathematics, Technical University Eindhoven, P.O. Box 513,
5600 MB Eindhoven, The Netherlands
e-mail: aeb@cwi.nl

Ç. Güven
e-mail: cicekguven@gmail.com

2 Partial linear spaces and generating rank

A *partial linear space* (X, L) is a geometry with set of points X, and set of lines L, where L is a collection of subsets of X, with the property that two distinct points are joined by at most one line. Points are called *collinear* when they are joined by a line.

A *subspace* of a partial linear space (X, L) is a subset Y of X with the property that any line that meets Y in at least two points is contained in Y. A (geometric) *hyperplane* of (X, L) is a proper subspace H with the property that it meets each line.

An arbitrary intersection of subspaces is again a subspace. If S is a set of points of a partial linear space (X, L), then $\langle S\rangle$, the *span* of S, is the smallest subspace of (X, L) that contains S. The *generating rank* of (X, L) is the size of the smallest set S with $\langle S\rangle = X$.

3 Universal $\mathbb{F}_2$-embeddings

Let (X, L) be a partial linear space with lines of length 3, and V a vector space over $\mathbb{F}_2$. We call a map $\phi : X \to V$ an *embedding* when $\phi(x) + \phi(y) + \phi(z) = 0$ for each line $\{x, y, z\}$ in L. (Note that we do not require ϕ to be injective.)

The *universal embedding space* (over $\mathbb{F}_2$) of (X, L) is the quotient U of the binary vector space with basis X by the subspace $Z = \langle x + y + z \mid \{x, y, z\} \in L\rangle$. The *universal embedding* is the map $x \mapsto x + Z$ from X into U. The *universal embedding dimension* is $\dim U$.

The universal embedding is universal in the sense that every other embedding is a quotient. It follows that $\dim U \geq \dim V$ for any V in which we have an embedding.

On the other hand, $\dim U \leq |S|$ for any subset S of X for which $\langle S\rangle = X$. (That is: the universal embedding dimension is not larger than the generating rank.)

Given an embedding $\phi : X \to V$, the inverse image $\phi^{-1}(H)$ of a hyperplane H in V is a (geometric) hyperplane in (X, L) if it is not all of X.

Given a geometric hyperplane H of (X, L), the map that sends the points of H to 0 and those outside H to 1 is an embedding into the 1-dimensional vector space $\mathbb{F}_2$. It follows that each geometric hyperplane is the inverse image of a hyperplane of U, and the number of geometric hyperplanes equals $2^d - 1$ if $d = \dim U$.

Not every partial linear space with lines of length 3 has an injective embedding. For example, the affine plane of order 3 has generating rank 3 and universal embedding dimension 0 (since there are no hyperplanes).

Let us write $\mathrm{udim}(X, L)$ for the universal embedding dimension of (X, L). If (X, L) is finite, with point-line incidence matrix N, then $\mathrm{udim}(X, L) = |X| - \mathrm{rk}_2(N)$.

4 Octads

Consider the extended binary Golay code C, the unique binary code of word length 24, dimension 12 and minimum distance 8. It has weight enumerator $1 + 759X^8 + 2576X^{12} + 759X^{16} + X^{24}$, so that there are 759 words of weight 8, known as *octads*. If Ω is the 24-set of coordinate positions, then the octads can be regarded as subsets of Ω of size 8.

This set of octads is made into a distance-regular graph Γ of diameter 3 if we call two octads adjacent when they are disjoint. Two octads have distance 0,1,2,3 in the graph Γ when they have 8,0,4,2 elements in common, respectively.

This graph is the collinearity graph of a partial linear space (X, K) with lines of size 3. Indeed, any two disjoint octads determine uniquely a third disjoint from both. One has $\mathrm{udim}(X, K) = 23$, see [2].

Now consider a different way of making the set of octads into a partial linear space. Take as lines the triples of vectors $\{b, c, d\}$ of weight 8 in C with $b + c + d = 0$. (If we view the octads as sets of size 8, then these lines are triples of octads that pairwise meet in four points but have no common point.) Let (X, L) be this partial linear space.

Lemma 1 $\mathrm{udim}(X, L) = 12$.

Since (X, L) is very small, this can easily be checked by computer. But doing it by hand is not difficult either.

Proof Let U be the universal embedding of (X, L), and let $+_U$ be the addition in U. We have the embedding C of dimension 12, so $\dim U \geq 12$.

Let us first identify the all-1 vector $\mathbf{1}$ in U. Define $\mathbf{1} = x +_U y +_U z$ for some line $\{x, y, z\} \in K$ (that is, for some triple x, y, z of pairwise disjoint octads). If $\{x, y', z'\}$ is another triple of pairwise disjoint octads, then y, z meet each of y', z' in four points, so $y +_U y'$ and $z +_U z'$ are both octads, in fact the same octad, and $\mathbf{1} = x +_U y +_U z = x +_U y' +_U z'$. Since (X, K) is a connected partial linear space the sum of the three octads in a line of (X, K) does not depend on the line chosen.

Now let $\sum c_i = 0$ in C, where each c_i is either an octad or $\mathbf{1}$. We want to show that this sum is 0 in U. (Once shown, this implies that U can be identified with C.) Argue by induction on the number of octad summands. If the sum is chosen minimal with nonzero sum in U, then no two summands are equal, and no two summands sum to an octad. If two summands x, y are disjoint octads, and $z = \mathbf{1} - x - y$, then $x +_U y = \mathbf{1} +_U z$ with fewer octads. So, any two octads in the sum meet in two points. Now if x, y, z are three octad summands, find an octad a such that $x + a$ and $x + a + y$ and $z + a$ are octads. Then $x +_U y +_U z = (x +_U a) +_U y +_U (z +_U a) = ((x + a) + y) +_U (z + a)$ is a sum of two octads and we are done. Is there such an a? Yes: we want an octad a that has 1 point in $x \cap y$ and 3 points in each of $x \setminus y$ and $y \setminus x$ (where we identified binary vectors with their supports), and there are 40 of those. And a must have precisely 4 points in z, and that is easily arranged. □

A stronger result is the fact that also the generating rank of (X, L) is 12. One checks by computer that the lexicographically minimal basis

000000000000000011111111
000000000000111100001111
000000000011001100110011
000000000101010101010101
000000001001011001101001
000000110000001101010110
000001010000010101100011
000010010000011000111010
000100010001000101111000
001000010001001000011101
010000010001010001001110
100000010001011100100100

is a generating set. The corresponding sequence of subspace sizes is 1, 3, 7, 15, 30, 46, 78, 130, 210, 330, 506, 759.

The largest singular subspaces have size 15. They are found by taking all octads disjoint from a given octad a and not containing some symbol γ not in a.

The largest sets of pairwise collinear octads have size 21. There are two types: (i) the 21 octads on three given symbols, (ii) for three given symbols α, β, γ 1 octad a containing α, β, γ, and the 20 octads meeting a in four symbols but not containing α, β, γ.

Geometric hyperplanes correspond to cosets of C in $\mathbb{F}_2^{24}$, where $u + C$ determines the hyperplane $u^\perp \cap X$. There are 1771, 2024, 276, 24 geometric hyperplanes of size 375, 378, 407, 506, respectively. Each of these four types is a single orbit under M_{24}. Each has universal embedding dimension 11.

More generally, all big subspaces of (X, L) must be intersections with linear subspaces of C. But there are small subspaces that are closed for lines but not for linear combinations in C. For example, one can find five octads such that the ten pairwise intersections are ten pairwise disjoint pairs. Now these five will sum to zero in C, but the fifth is not in the geometric span of the first four.

5 Short vectors in the Leech lattice

Consider the universal embedding dimension of the partial linear space Σ on the images of the shortest nonzero vectors of the Leech lattice Λ in $\Lambda/2\Lambda$ where the lines are given by the triples x, y, z with $x + y + z = 0$ (in $\Lambda/2\Lambda$).

There are 196,560 shortest nonzero vectors in Λ, and they map into 98,280 points in $\Lambda/2\Lambda$, where each point x has preimage $\{x, -x\}$. We use Leech lattice vectors as names for the points, so that x and $-x$ are the same point.

The 196,560 shortest vectors can be described (up to a scaling factor $\frac{1}{\sqrt{8}}$) in $\mathbb{Z}^{24}$ as: (i) $4 \times \binom{24}{2} = 1{,}104$ vectors of shape $((\pm 4)^2, 0^{22})$; (ii) $2^7 \times 759 = 97{,}152$ vectors of shape $((\pm 2)^8, 0^{16})$ with the ± 2's on the positions of an octad, and an even number of minus signs; (iii) $2^{12} \times 24 = 98{,}304$ vectors of shape $((\mp 3), (\pm 1)^{23})$ with minus signs on the positions of a vector in C.

5.1 The subspace R

Let R be the set of 552 points of type (i). Then R is a subspace of Σ, and R is spanned by the 24 vectors r_i $(0 \le i \le 23)$ where $r_0 = (4^2, 0^{22})$ and $r_i = (-4, 0^{i-1}, 4, 0^{23-i})(i > 0)$.

(Indeed, let $p_{ab} := (0^a, -4, 0^b, 4, 0^{22-a-b})$ and $q_{ab} := (0^a, 4, 0^b, 4, 0^{22-a-b})$. Then $p_{0b} = r_{b+1}$ and p_{ab} with $a > 0$ is on the line $\{p_{ab}, r_a, r_{a+b+1}\}$ since $p_{ab} = r_{a+b+1} - r_a$. And $q_{00} = r_0$, and q_{0b} with $b > 0$ is on the line $\{q_{0b}, r_0, p_{1,b-1}\}$, and q_{ab} with $a > 0$ is on the line $\{q_{ab}, q_{0,a+b}, r_a\}$.)

5.2 The subspace $R \cup S$

Let S be the set of 48,576 points of type (ii). Then $R \cup S$ is a subspace of Σ, spanned by R together with 12 points of S.

(Indeed, let S_0 be a set of 12 points of type $(2^8, 0^{16})$ such that the corresponding octads span the partial linear space (X, L) on the octads as in Lemma 1. Since $\langle R \cup S_0 \rangle$ contains, together with each vector s of type (ii), also all vectors s' obtained by changing an even number of signs, and since any two octads meet in an even number of points, we see that $\langle R \cup S_0 \rangle = R \cup S$.)

5.3 The space $R \cup S \cup T$

Let T be the set of 49,152 points of type (iii). Then $R \cup S \cup T$ (the entire point set of Σ) is spanned by $R \cup S$ together with a single point of T.

(Indeed, since $x = -x$ we may pick coordinates of shape $(-3, (\pm 1)^{23})$ for any point in T. Adding a vector of shape $(4, -4, 0^{22})$ to $(-3, 1^{23})$ allows one to move the -3 to a different position. Adding vectors of type (ii) allows one to change signs on the positions of a vector in C.)

5.4 Dimensions

So far we have spanned this partial linear space Σ on 98,280 points using $24 + 12 + 1 = 37$ points. But in U there are relations between the generators that we found. Since $s = -s$ for $s = (2^8, 0^{16})$, we can make a chain $s + ((-4)^2, 0^{22}) = s', s' + (0^2, (-4)^2, 0^{20}) = s'', s'' + (0^4, (-4)^2, 0^{18}) = s''', s''' + (0^6, (-4)^2, 0^{16}) = s$ and conclude that in U the four points $(4^2, 0^{22})$, $(0^2, 4^2, 0^{20})$, $(0^4, 4^2, 0^{18})$, $(0^6, 4^2, 0^{16})$ sum to zero. Using the expressions $q_{0b} = r_{b+1} + r_0 - r_1$ and $q_{ab} = r_{a+b+1} + r_a + r_0 - r_1$ $(a > 0)$ found earlier this means that each octad gives a relation involving the eight corresponding r_i (modulo $\langle r_0 \rangle$), and we only need a set of coset representatives of C, so that the linear span of $R \cup S$ in U has dimension at most $12 + 12 = 24$.

Similarly, since $t = -t$ for $t = (-3, 1^{23})$, we can make a chain $t + (0^{16}, (-2)^8) = t', t' + (0^8, (-2)^8, 0^8) = t'', t'' + (2^2, (-2)^6, 0^{16}) = t''', t''' + (4, -4, 0^{22}) = t$ and conclude that in U the four points $(0^{16}, (-2)^8)$, $(0^8, (-2)^8, 0^8)$, $(2^2, (-2)^6, 0^{16})$, $(4, -4, 0^{22})$ sum to zero. Modulo R this says that $\mathbf{1}$ in C equals 0 in U, which was not the case inside $R \cup S$, so this is a new relation and also U has dimension at most $(12 + 12) - 1 + 1 = 24$.

Since we have an embedding (namely $\Lambda/2\Lambda$) in which R, $R \cup S$ and $R \cup S \cup T$ all have dimension 24, it follows that the universal embedding dimensions of these spaces are at least 24.

Concluding: each of the subspaces R, $R \cup S$ and $R \cup S \cup T$ has universal embedding dimension 24.

5.5 Generating rank

We saw that R has generating rank 24. Also $R \cup S$ has generating rank 24. Indeed, if we write $\bar{4}$ instead of -4, then the 24 vectors

00000000000000000000044	00000000000000022222222
00000000000000000000044̄	00000000000022220000 2222
00000000000000000000440̄	00000000002200220022 0022
00000000000000000004400̄	00000000020202020202 0202
00000000000000000040040̄	00000000200220220020 2002
00000000000000000400040̄	00000022000000220202 0220
00000000000000004000040̄	00000202000002020220 0022
00000000000000400000040̄	00002002000002200022 2020
00000000000004000000040̄	00020002000200020222 2000
00000000000040000000040̄	00200002000200200002 2202
00000000004000000000040̄	02000002000202000200 2220
00000040000000000000040̄	20000002000202220020 0200

form a generating set of $R \cup S$. (Proof: First, these suffice to generate the generating set of R of size 24 given earlier. Next, the last 12 of these vectors were the generators of the octad space (X, L) (with 2's instead of 1's), but when $b + c = d$ for octads b, c, d written as 0-1 vectors, and with addition mod 2, then $2b + 2c'' = 2d$ with addition in $\mathbb{Z}$ if $2c''$ is obtained from $2c$ by changing 2 to -2 in the four positions where both $2b$ and $2c$ have 2. And $2c''$ is obtained via $2c - r = 2c'$, $2c' - r' = 2c''$ for two vectors r, r' in R. It follows that this set also generates all of S.)

The corresponding sequence of subspace sizes is 1, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 220, 374, 658, 1200, 2192, 3250, 5334, 8700, 13860, 21582, 32890, 49128.

Finally, the first 23 of the above vectors, together with the vector $t = (1^{23}, -3)$ form a generating set of $R \cup S \cup T = X$. (Proof: these first 23 vectors generate the hyperplane $x_1 = 0$. Now $t' = t + (0^{16}, (-2)^6, 2^2) = (1^{16}, (-1)^6, 3, -1)$, $t'' = t' + (0^{22}, -4, 4) = (1^{16}, (-1)^7, 3)$, $t''' = t'' + (0^8, (-2)^8, 0^8) = (1^8, (-1)^{15}, 3)$, $s = t + t''' = (2^8, 0^{16})$, so that these generate all of $R \cup S$.)

5.6 Hyperplanes

Every geometric hyperplane of Σ is the intersection with the point set of Σ of a hyperplane in its universal embedding $U = \Lambda/2\Lambda$.

A hyperplane of $\Lambda/2\Lambda$ corresponds to a sublattice of Λ of index 2. Such a sublattice is given by $\{x \in \Lambda \mid (x, w) \in 2\mathbb{Z}\}$ for a vector $w \in \Lambda \backslash 2\Lambda$. For $u \in \Lambda$, the sublattices defined by w and $w' = w + 2u$ coincide, and modulo 2Λ any vector in Λ is congruent to one of squared norm 0, 4, 6, or 8, where these cases occur with frequencies 1, 98280, 8386560, 8292375 (summing to 2^{24}). Thus, $\Lambda/2\Lambda$ has three types of hyperplane [1, Theorem 3.2].

The hyperplanes of Σ therefore fall into three orbits of sizes 98280, 8386560, 8292375, and these hyperplanes have size 51176, 49128 and 49128, respectively. For example, the choice $w = c(0, \ldots, 0, 8)$ (where $c = \frac{1}{\sqrt{8}}$) gives the hyperplane $R \cup S$ of size 49128. The choices $w = c(0, \ldots, 0, 4, 4)$ and $w = c(1, \ldots, 1, -3, -3, -3)$ give representatives of the other two orbits (of sizes 51,176 and 49,128, respectively).

5.7 Group and association scheme

The partial linear space Σ has full group of automorphisms Co_1, with point stabilizer Co_2 acting rank 4. The subdegrees are $1 + 4{,}600 + 46{,}575 + 47{,}104$. The suborbit of size 4,600 consists of the points collinear with the fixed point, and the induced subgraph has group $Co_2 \times 2$, where the additional two interchanges the two remaining points on each line through the fixed point.

Let Γ be the collinearity graph of Σ (Fig. 1).

The local graph (graph induced on the neighbourhood of a point) has a distinguished matching corresponding to the lines on that point. The quotient graph obtained by contracting the edges in this matching (that is, the graph on the lines on that point) is strongly regular with parameters $(v, k, \lambda, \mu) = (2300, 891, 378, 324)$ (Fig. 2).

The rank 4 action leads to a three-class association scheme with eigenmatrices

$$P = \begin{pmatrix} 1 & 4600 & 47104 & 46575 \\ 1 & 1000 & 1024 & -2025 \\ 1 & 76 & -320 & 243 \\ 1 & -20 & 64 & -45 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 299 & 17250 & 80730 \\ 1 & 65 & 285 & -351 \\ 1 & \frac{13}{2} & -\frac{1875}{16} & \frac{1755}{16} \\ 1 & -13 & 90 & -78 \end{pmatrix}.$$

Bill Martin remarks that this association scheme is cometric (cf. [4]).

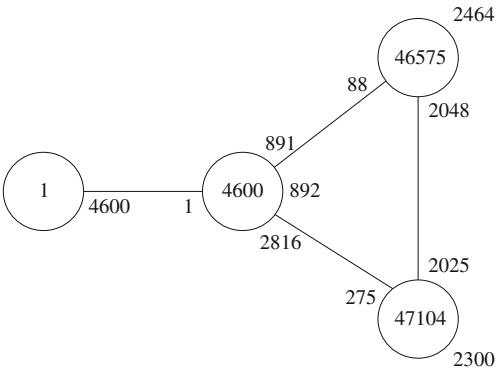

Fig. 1 Distance distribution diagram of Γ

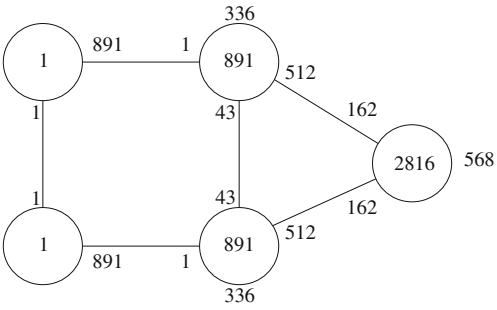

Fig. 2 Distance distribution diagram of the local graph

References

1. Bachoc C., Batut C.: Etude algorithmique de réseaux construits avec la forme trace. Exp. Math. **1**, 183–190 (1992).
2. Brouwer A.E., Cuypers H., Lambeck E.W.: The hyperplanes of the M_{24} near polygon. Graphs Comb. **18**, 415–420 (2002).
3. Conway J.H., Sloane N.J.A.: Sphere Packings, Lattices and Groups. Springer, New York (1988).
4. Martin W.J.: http://users.wpi.edu/~martin/RESEARCH/QPOL/. Accessed 19 March 2012.