Codes, Lattices, and Steiner Systems

Patrick Solé[*]
CNRS, I3S,
ESSI, BP 145,
Route des Colles,
06 903 Sophia Antipolis,
France

Submitted: February 16 1996; Accepted: January 31, 1997

Abstract

Two classification schemes for Steiner triple systems on 15 points have been proposed recently: one based on the binary code spanned by the blocks, the other on the root system attached to the lattice affinely generated by the blocks. It is shown here that the two approaches are equivalent.

1991 AMS Classification: Primary: 05B07; Secondary: 11H06, 94B25.

1 Introduction

It has been known since 1919 [5] that there are 80 Steiner triple systems on 15 points. Recently, two algebraic invariants have been proposed to classify them. Let V denote the 35 block vectors v_i of length 15 and hamming weight 3 of such a system. One can attach to V either

- the binary linear code C spanned by the vectors of V [4]

[*] `sole@alto.unice.fr`

- the lattice $L := \{\sum_i z_i v_i : \sum_i z_i = 0 \ \& \ z_i \in \mathbf{Z}\}$ [3]

The lattice L has norm ≥ 2 and its norm 2 vectors afford a (possibly empty) root system R. It so happens that exactly 5 non-equivalent codes C and also 5 non-equivalent root systems R occur and that they induce the same partition of the 80 $S(2,3,15)$ in five parts. We shall provide a conceptual explanation of this experimental fact.

2 Notations and Definitions

A Steiner triple system $S(2,3,v)$ is a $2-(v,3,1)$ design.

A binary *code* of length n and dimension k is a $k-$dimensional vector subspace of $\mathbf{F}_2^n$. The (Hamming) weight of a vector of $\mathbf{F}_2^n$ is the number of non-zero coordinates it contains.

An $n-$dimensional *lattice* is a discrete $\mathbf{Z}-$module of $\mathbf{R}^n$ which may or may not be of maximal rank $(n.)$ The (squared euclidean) norm of a vector x of $\mathbf{R}^n$ is $x.x$. The *norm* of a lattice is the minimum nonzero norm of its elements. A lattice is *integral* if the dot product of any two of its vectors is an integer. An integral lattice is called *even* (or type II in[2]) if the norm of each its vectors is an even integer. A *root* in an even integral lattice is a vector of norm 2. A *root system* is the set of all such vectors in an even lattice.

3 Explanation

Let C_e denote the following subcode

$$C_e := \{\sum_i z_i v_i : \sum_i z_i = 0 \ \& \ z_i \in \mathbf{F}_2\}$$

of C. Recall that construction A of [2] (here with a different normalization) associates to a binary code D the lattice

$$A(D) := D + 2\mathbf{Z}^n.$$

Theorem 1 *The code C_e is the even weight subcode of C and*

$$L \subseteq A(C_e).$$

Proof: The second assertion is immediate from the definition of C_e. The first assertion comes from the fact that the sum of coordinates of a typical vector of L is

$$\sum_j(\sum_i z_i v_i)_j = \sum_i z_i(\sum_j (v_i)_j) \equiv 0\,(mod\,2).$$

This shows inclusion of C_e into the even weight subcode of C. Equality comes from the fact that C_e is generated by $v_1 + v_i,\ i = 2, \ldots, 15$, which yields the direct sum

$$C = \mathbf{F}_2 v_1 \oplus C_e.$$

$\square$

Remark: $L \neq A(C_e)$ for $2v_1 \in A(C_e)$ but $2v_1$ is not in L. While $A(C_e)$ is of maximal rank, L is not. To make this remark more precise, we introduce an auxilliary lattice. Let $e_i,\ i = 1, \ldots, 15$ denote the canonical basis (i.e. the 15 vectors of shape 10^{14}) and call k the dimension of C_e. Let L_k denote the $\mathbf{Z}$-span of the vectors $2e_i,\ i = k+1, \ldots, n$.

Theorem 2 *The lattice L is obtained from $A(C_e)$ by successive projections onto a vector space:*

$$A(C_e) = 2\mathbf{Z}v_1 \oplus L \oplus L_k.$$

Therefore the root system R depends solely on C.

Proof: Let

$$L' := \{\sum_i z_i v_i : \sum_i z_i = 0\,(mod 2)\ \&\ z_i \in \mathbf{Z}\}.$$

It is easy to see, using explicit projectors that

$$L' = 2\mathbf{Z}v_1 \oplus L.$$

Furthermore, from the generating matrix for construction A [2, p.183] we see that

$$A(C_e) = L' \oplus L_k.$$

Combining the last two equations we are done. $\square$

We can relate the root system R to the code C.

Theorem 3 *The root system R consists of vectors of the shape* $(\pm 1)^2 0^{13}$ *supported by weight 2 codewords in C.*

Proof: From Theorem 1 it follows that the vectors of norm 2 in L are in $A(C_e)$. It is known that the vectors of norm 2 of $A(C_e)$ comprise suitably signed versions of the vectors of weight 2 of C_e, i.e. of the vectors of weight 2 of C. □

4 Conclusion

From the preceding results it transpires that the lattice depends solely on the code and therefore, by combining with the results in [1, 4], since the code depends solely on its dimension, solely on the 2-rank of the considered STS. We leave to the interested reader the explicit determination of root systems and lattices involved.

5 Acknowledgements

We thank Ed Assmus, Michel Deza, and Vladimir Tonchev for sending us their preprints and Chris Charnes, Slava Grishukhin for helpful discussions. We thank the Mathematics Department of Macquarie University for its hospitality.

References

[1] E. F. Assmuss, jr. On 2-ranks of Steiner Triple Systems, Electronic Journal of Combinatorics, 2 (1995), paper R9.

[2] J.H. Conway, N.J.A. Sloane, *Sphere Packings Lattices and Groups*, second edition, Springer Verlag (1993).

[3] M. Deza,V. Grishukhin, Once More about 80 Steiner triple systems on 15 points, LIENS research report 95-8.

[4] V.D. Tonchev, R.S. Weishaar, Steiner Systems of order 15 and their codes, J. of Stat. Plann. and Inf. submitted (1995).

[5] H. S. White, F.N. Cole, L. D. Cummings, Complete Classification of the triad systems on fifteen elements, Mem. Nat. Acad. Sc. USA 14, second memoir (1919) 1-89.