

CHAPTER 3

## A Strongly Regular Graph Derived from the Perfect Ternary Golay Code

E. R. BERLEKAMP†

*Bell Telephone Laboratories, Inc., Murray Hill, N.J. 07974, U.S.A.*

and

J. H. VAN LINT and J. J. SEIDEL

*Technological University of Eindhoven, Eindhoven, The Netherlands*

By use of the perfect ternary Golay code, a strongly regular graph on 243 vertices is constructed, having the property that any adjacent pair of vertices is in one triangle and that any nonadjacent pair of vertices is in one quadrangle. The graph realizes one of the five possibilities for graphs with this property. It provides a (243, 22, 2)-system on 22 and 23 in the sense of Bridges and Ryser [1969].

### 1. Introduction

Strongly regular graphs have been introduced by Bose [1963], as an abstraction from 2-association schemes for partially balanced incomplete block designs. They satisfy the following, essentially characteristic, properties. For any pair of adjacent vertices  $x$  and  $y$ , the number  $p_{11}^1$  of vertices adjacent to  $x$  and to  $y$  is independent of the choice of  $x$  and  $y$ . For any pair of nonadjacent vertices  $u$  and  $v$ , the number  $p_{11}^2$  of vertices adjacent to  $u$  and to  $v$  is independent of the choice of  $u$  and  $v$ . We shall be interested in strongly regular graphs with the special property

$$p_{11}^2 - p_{11}^1 = 1.$$

For  $p_{11}^1 = 0$ , this amounts to the Moore graphs of diameter 2 and girth 5, which have been discussed by Hoffman and Singleton [1960]. For  $p_{11}^1 = 1$ , these graphs have the property that any adjacent pair of vertices is in one triangle, and that any nonadjacent pair is in one quadrangle. In Section 2 it is shown that such a graph can exist for at most 5 values of  $n$ . An example is provided by the lattice graph on 3 symbols. In Section 4 a further such graph, on 243 vertices, is constructed in three different ways.

As a starting point for the constructions of this graph, in Section 3 the perfect ternary 2-error-correcting code is explained. This code has been

† Current address: University of California, Berkeley, Calif. 94720, U.S.A.

discovered by Golay [1949]. It was discussed by Coxeter [1958] in a geometric context, and by Bose [1961], who indicated its connection to the theory of confounding and fractional replication.

Bridges and Ryser [1969] considered yet another generalization of block designs. Their  $(n, k, \lambda)$ -systems on  $r$  and  $s$  are defined in terms of binary square matrices  $X$  and  $Y$  of order  $n$  satisfying the real matrix equation†

$$XY = YX = (k - \lambda)I + \lambda J, \quad k \neq \lambda,$$

which, for  $\lambda \neq 0$ , implies

$$JX = XJ = rJ, \quad JY = YJ = sJ$$

for integer  $r$  and  $s$ . In particular,  $(n, k, \lambda)$ -systems on  $k$  and  $k + 1$  are characterized by symmetric matrices  $C$  with zero diagonal and elements  $+1$  and  $-1$  elsewhere, such that

$$C^2 = (1 + 4(k - \lambda))I + (n - 2 - 4(k - \lambda))J, \quad CJ = (2k - n + 1)J.$$

For special choices of the parameters, such as  $n - 1 = 2k$ , and  $n - 2 = 4(k - \lambda)$ , this leads to orthogonal matrices with zero diagonal, which have been discussed by Goethals and Seidel [1967]. However, there are other values of the parameters for which these systems exist. In fact,  $(n, k, \lambda)$ -systems on  $k$  and  $k + 1$  are the same objects as strongly regular graphs with  $p_{11}^2 - p_{11}^1 = 1$ .

## 2. Strongly regular graphs with $p_{11}^2 - p_{11}^1 = 1$

Strongly regular graphs on  $n$  vertices may be defined in terms of their  $(1, 0)$  adjacency matrix  $A$ , and its eigenvalues  $k, r, s$  as follows (cf. Hoffman [1963], Seidel [1968, 1969]):

$$(A - rI)(A - sI) = \frac{(k - r)(k - s)}{n}J, \quad AJ = kJ.$$

Excluding complete bipartite graphs and their complements, we take  $r \geq 0$  and  $s < 0$ . For the multiplicities  $1, \alpha, \beta$  of the eigenvalues  $k, r, s$  we have

$$n = 1 + \alpha + \beta, \quad \text{tr}A = 0 = k + \alpha r + \beta s, \quad \text{tr}A^2 = nk = k^2 + \alpha r^2 + \beta s^2,$$

whence, by elimination of  $\alpha$  and  $\beta$ ,

$$(k - r)(k - s) = n(k + rs).$$

By multiplying out the defining equation, we obtain

$$-r - s + p_{11}^1 = k + rs, \quad p_{11}^2 = k + rs.$$

From now on, we restrict ourselves to strongly regular graphs with the special property

$$p_{11}^2 - p_{11}^1 = 1,$$

† Here  $I$  denotes the  $n \times n$  identity matrix and  $J$  denotes the  $n \times n$  matrix all of whose entries are 1.

that is,  $r+s = -1$ . Putting  $p_{11}^2 = \lambda$ , we have

$$\begin{aligned} A^2 + A &= (k-\lambda)I + \lambda J, & AJ &= kJ, \\ 2k - (n-1) + (\alpha-\beta)(2r+1) &= 0, \\ k^2 &= (n-1)\lambda, & k &= \lambda + r(r+1). \end{aligned}$$

The case  $\alpha = \beta$  reduces to

$$(J-I-2A)^2 = nI - J, \quad n = 2k+1 = 4\lambda+1 = (2r+1)^2,$$

$$C^2 = \begin{bmatrix} 0 & j^T \\ j & J-I-2A \end{bmatrix}^2 = nI,$$

where  $j$  is  $(n \times 1)$ . So  $C$ , of order  $n+1$ , is an orthogonal matrix with zero diagonal. Such matrices, for which  $n$  must be a sum of two squares of integers, have been constructed for

$$n = p^\alpha \equiv 1 \pmod{4}, \quad p \text{ prime,}$$

and for some additional orders, e.g., for  $n = 225$ . An easy example is  $C_6$ , with  $A = \text{circulant}(0, 1, 0, 0, 1)$ . The smallest order for which the existence is unknown is  $n = 45$ . For details the reader is referred to Van Lint and Seidel [1966], and Goethals and Seidel [1967].

In the case  $\alpha \neq \beta$ , the relations between the parameters imply that  $r$  is an integer. Elimination of  $n$  and  $k$  yields

$$(2r+1)^4 - 2(2r+1)^2 - 16(\alpha-\beta)\lambda(2r+1) - 16\lambda^2 + 1 = 0.$$

Therefore,  $2r+1$  must divide  $16\lambda^2 - 1$ . Thus, given  $\lambda$ , there are only finitely many possibilities for the parameters  $r, k, n$ .

Hoffman and Singleton [1960] considered  $\lambda = 1$ , which admits  $r = 1, 2, 7$ , with  $(n, k, \lambda) = (10, 3, 1), (50, 7, 1), (3250, 57, 1)$ , respectively.† The first case is realized by the Petersen graph. The second graph was constructed by Hoffman and Singleton [1960], drawn by N. Robertson [private comm.], and has an adjacency matrix which may be arranged as follows by use of the cyclic permutation matrix  $P$  of order 5:

$$\begin{bmatrix} P+P^{-1} & 0 & 0 & 0 & 0 & I & I & I & I & I \\ 0 & P+P^{-1} & 0 & 0 & 0 & I & P & P^2 & P^3 & P^4 \\ 0 & 0 & P+P^{-1} & 0 & 0 & I & P^2 & P^4 & P^6 & P^8 \\ 0 & 0 & 0 & P+P^{-1} & 0 & I & P^3 & P^6 & P^9 & P^{12} \\ 0 & 0 & 0 & 0 & P+P^{-1} & I & P^4 & P^8 & P^{12} & P^{16} \\ I & I & I & I & I & P^2+P^{-2} & 0 & 0 & 0 & 0 \\ I & P & P^2 & P^3 & P^4 & 0 & P^2+P^{-2} & 0 & 0 & 0 \\ I & P^2 & P^4 & P^6 & P^8 & 0 & 0 & P^2+P^{-2} & 0 & 0 \\ I & P^3 & P^6 & P^9 & P^{12} & 0 & 0 & 0 & P^2+P^{-2} & 0 \\ I & P^4 & P^8 & P^{12} & P^{16} & 0 & 0 & 0 & 0 & P^2+P^{-2} \end{bmatrix}$$

The existence of the last graph is still undecided.

We now turn to  $\lambda = 2$ , which admits  $r = 1, 3, 4, 10, 31$ , with  $(n, k, \lambda) = (9, 4, 2), (99, 14, 2), (243, 22, 2), (6273, 112, 2), (494019, 994, 2)$ , respectively.

† The case  $r = 0$  is excluded because it leads to  $n = 2$ .

The first case is realized by the lattice graph of order 3, that is, the graph whose 9 vertices are the ordered pairs out of 3 symbols, any two vertices being adjacent if the corresponding ordered pairs have one coordinate equal. In Section 4 the graph with parameters (243, 22, 2) will be constructed. The existence of the other graphs remains undecided.

### 3. The perfect ternary Golay code

Let  $C_6$  be the orthogonal matrix with zero diagonal of order 6 which was mentioned above. The rows of the  $6 \times 12$  matrices

$$G = [I_6 \ C_6], \quad H = [-C_6 \ I_6]$$

each generate a subspace of dimension 6 of the vector space  $V(12, 3)$  of dimension 12 over  $GF(3)$ . These subspaces are orthogonal, since  $GH^T = 0$ . By inspection it is observed that in  $H$  no 5 columns are linearly dependent. This implies that the subspace generated by the rows of  $G$  has the property that its vectors, apart from the zero vector, have at least 6 nonzero coordinates. By deleting any one column of  $G$  the  $6 \times 11$  matrix  $G^*$  is obtained. The rows of  $G^*$  generate a subspace of dimension 6 of  $V(11, 3)$ , whose nonzero vectors have at least 5 nonzero coordinates. By the count

$$3^6(1 + 2 \times 11 + 2^2 \binom{11}{2}) = 3^{11}$$

it follows that every 11-dimensional vector over  $GF(3)$  differs from a unique vector in the row space of  $G^*$  in at most two coordinates.

In terms of coding theory (Berlekamp [1968]), we call the vectors of  $V(11, 3)$  the *words*, the number of nonzero coordinates of a word its *weight*, the subspace generated by  $G^*$  a *code*, the vectors of a code its *codewords*,  $G^*$  a *generator matrix*, and a matrix  $H^*$  generating the orthogonal complement of the code a *parity check matrix* of the code. The fact that every 11-dimensional vector over  $GF(3)$  differs from a unique codeword in at most two coordinates makes the code a *perfect code*. The perfect ternary code introduced above is called the (11, 6) *ternary Golay code*, after its discoverer Golay [1949].

We remark that an alternative description for the (11, 6) ternary Golay code is given by

$$G^* = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix},$$

and  $H^*$  the matrix consisting of the last 5 rows of  $G^*$  (cf. Van Lint [1969]).

The subspace of  $V(12, 3)$  generated by the rows of the  $6 \times 12$  matrix  $G$

mentioned above is called the (12, 6) ternary Golay code. It is a special case of an extended quadratic residue code. Several general properties of such codes are summarized in Section 15.2 of Berlekamp [1968].

#### 4. Constitution of the 243-graph

The perfect ternary Golay code partitions the vector space  $V(11, 3)$  into  $3^5$  cosets obtained by adding a fixed word to all codewords. Each word of weight  $\leq 2$  must be in a coset containing no other word of weight  $\leq 2$ , since the minimum nonzero weight of the code equals 5. Therefore, the 243 cosets of the code are uniquely represented by the 220 words of weight 2, the 22 words of weight 1, and the word of weight 0. Furthermore, the cosets form a linear space of dimension 5 over  $\text{GF}(3)$ .

Now consider the 243 cosets as the vertices of a graph. Any two vertices are called adjacent iff the difference of the corresponding cosets is a coset of minimum weight 1. This graph possesses the triangle and the quadrangle property. Indeed, by linearity this only needs to be verified if one of the vertices is the code. Let  $a, b \in \text{GF}(3) - \{0\}$ . The vertices represented by  $(0, 0, 0, \dots, 0)$  and  $(a, 0, 0, \dots, 0)$  are both adjacent to  $(-a, 0, 0, \dots, 0)$  only. The nonadjacent vertices  $(0, 0, 0, \dots, 0)$  and  $(a, b, 0, \dots, 0)$  are adjacent to  $(a, 0, 0, \dots, 0)$  and  $(0, b, 0, \dots, 0)$  only.

Secondly, we give the following alternative construction for the 243-graph. Let  $H^*$  be the  $5 \times 11$  parity check matrix of the perfect ternary Golay code. The columns of  $H^*$  are denoted by  $x_1, x_2, \dots, x_{11}$ , which are vectors of the vector space  $V(5, 3)$  of dimension 5 over  $\text{GF}(3)$ . There are 22 vectors of type  $\pm x_i$ , and 220 vectors of type  $\pm x_i \pm x_j$ ;  $i \neq j$ ;  $i, j = 1, 2, \dots, 11$ . These vectors are pairwise distinct, since by the minimum weight 5 of the code no 4 of the vectors  $x_1, x_2, \dots, x_{11}$  are dependent. Therefore, these vectors and the zero vector represent all vectors of  $V(5, 3)$ .

Now consider the  $3^5$  vectors of  $V(5, 3)$  as the vertices of a graph. Any two vertices are called adjacent if the difference of the corresponding vectors is one of  $\pm x_1, \pm x_2, \dots, \pm x_{11}$ . Again, the triangle and the quadrangle property are easily verified.

Finally, we indicate a third construction of the 243-graph, similar to the construction of the 2048-graph obtained from the (24, 12) binary Golay code in Goethals and Seidel [1970]. This construction depends on the compositions of the codewords of the (12, 6) ternary Golay code. The composition of a word is the unordered set of values of its coordinates (e.g., the composition of  $(0, 0, 1, 2, 1, 0, 2, 2, 1, 0, 1, 1)$  is  $0^4 1^5 2^3$ ).

**Lemma.** *Every word of composition  $0^9 1^3$  lies in some coset of the (12, 6) ternary Golay code which contains two words of composition  $0^9 1^3$ , two words of composition  $0^9 2^3$ , and no other words of weight  $\leq 3$ .*

This lemma may be proved by investigating the distribution of words of weight 3 in the cosets of the (12, 6) code; we shall not present the details here.

Now the construction runs as follows: It is wellknown that the (12, 6) ternary Golay code contains as a subcode the (12, 1) repetition code whose three vectors have compositions  $0^{12}$ ,  $1^{12}$ , and  $2^{12}$ . The 243 vertices of the graph are associated with the quotient of the (12, 6) ternary Golay code modulo its (12, 1) repetition subcode. Two vertices are adjacent iff the difference of the corresponding words contains only two elements of  $\text{GF}(3)$  in its composition. It is trivially verified that this definition of adjacency is reflective, and independent of the representative word of the vertex. The triangle and the quadrangle property are verified by use of the lemma.

### References

- E. R. Berlekamp, 1968, *Algebraic Coding Theory* (McGraw-Hill, New York).
- R. C. Bose, 1961, On some connections between the design of experiments and information theory, *Bull. Intern. Statist. Inst.* **38** (4), 257-271.
- R. C. Bose, 1963, Strongly regular graphs, partial geometries and partially balanced designs, *Pacif. J. Math.* **13**, 389-419.
- W. C. Bridges, and H. J. Ryser, 1969, Combinatorial designs and related systems, *J. Algebra* **13**, 432-446.
- H. S. M. Coxeter, 1958, Twelve points in  $PG(5, 3)$  with 95040 self-transformations, *Proc. Roy. Soc. London A* **247**, 151-165.
- J. M. Goethals, and J. J. Seidel, 1967, Orthogonal matrices with zero diagonal, *Canad. J. Math.* **19**, 1001-1010.
- J. M. Goethals, and J. J. Seidel, 1970, Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.* **22**, 597-614.
- M. Golay, 1949, Notes on digital coding, *Proc. I.R.E.* **37**, 637.
- A. J. Hoffman, and R. R. Singleton, 1960, On Moore graphs with diameters 2 and 3, *I.B.M. J. Res. Develop.* **4**, 497-504.
- A. J. Hoffman, 1963, On the polynomial of a graph, *Am. Math. Monthly* **70**, 30-36.
- N. Robertson, (private communication).
- J. J. Seidel, 1968, Strongly regular graphs with  $(-1, 1, 0)$  adjacency matrix having eigenvalue 3, *Linear Algebra Appl.* **1**, 281-298.
- J. J. Seidel, 1969, Strongly regular graphs, *Recent Progress in Combinatorics* (W. T. Tutte, ed.; Academic Press, New York), pp. 185-198.
- J. H. van Lint, 1969, 1967-1969 Rept. Discrete Mathematics Group, Technol. Univ. Eindhoven Rept. 69-WSK-04.
- J. H. van Lint, and J. J. Seidel, 1966, Equilateral point sets in elliptic geometry, *Koninkl. Ned. Akad. Wetensch. Proc. A*, **69** (= *Indag. Math.* **28**), 335-348.