A CONSTRUCTION FOR ROOM'S SQUARES AND AN APPLICATION IN EXPERIMENTAL DESIGN

By J. W. Archbold and N. L. Johnson

University College, London

1. T. G. Room [1] recently proposed the following problem: To arrange the $n(2n-1)$ symbols rs (which is the same as sr) formed from all pairs of $2n$ different digits in a square of $2n-1$ rows and columns such that in each row and column there appear n symbols (and $n-1$ blanks) which among them contain all $2n$ digits.

He remarked that the problem is soluble when $n = 1$ (trivially) and $n = 4$ but not when $n = 2$ or 3; and he gave one solution for $n = 4$.

Squares of such a type have uses in experimental designs. We explain below a simple construction for squares where n has the form 2^{2m-1}. Each square constructed in this way is represented in a canonical form by applying a well-known theorem of J. Singer [2]. In this form as soon as the top row of entries in a square is known, all the other entries may be written down immediately by means of a straight-forward cyclic process. Thus an index of first rows is all that is necessary to catalogue squares in their canonical forms.

It may be permissible to give here a slight modification of the proof of Singer's theorem in order to show a natural application of the regular representation of linear algebras.

2. Let $\mathfrak{A}$ be a linear associative algebra, of order m and with modulus, over a commutative field K. It is well known that $\mathfrak{A}$ is isomorphic with an algebra of $m \times m$ matrices whose elements belong to K (c.f. Macduffee [3], Section 123).

A Galois field $GF(p^{mn})$ is such a linear algebra over a $GF(p^n)$. If the elements of the $GF(p^{mn})$ are $0, \alpha, \alpha^2, \cdots, \alpha^{p^{mn}-1} = 1$ the irreducible equation, of degree m and with coefficients in $GF(p^n)$,

$$f(x) \equiv x^m - a_1 x^{m-1} - \cdots - a_m = 0$$

which is satisfied by α is called primitive (Dickson [4], Section 35). A basis for the algebra consists of $1, \alpha, \alpha^2, \cdots, \alpha^{m-1}$ and the modulus is 1.

The primitive equation is both the minimum and characteristic equation of the companion matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \\ a_m & a_{m-1} & a_{m-2} & \cdots & a_1 \end{pmatrix}$$

Received December 20, 1956; revised October 16, 1957.

The correspondence $\alpha^r \leftrightarrow \mathbf{A}^r$ determines an isomorphy, or regular representation, of the $GF(p^{mn})$ on the algebra or Galois field whose elements are the $m \times m$ matrices 0, $\mathbf{A}$, $\mathbf{A}^2$, $\cdots$, $\mathbf{A}^{p^{mn}-1} = \mathbf{I}$, where $\mathbf{I}$ is the unit matrix (c.f. Macduffee [3], Section 109). If $N = 1 + p^n + \cdots + p^{(m-1)n}$ then the matrices $\mathbf{A}^{jN}$, for $j = 1, \cdots, p^n - 1$, are the multiples of $\mathbf{I}$ by the elements of $GF(p^n)$ and form a sub-algebra, of matrices, isomorphic with $GF(p^n)$.

In a finite projective space $PG(m-1, p^n)$ over the $GF(p^n)$, let $\mathbf{x}$ and $\mathbf{y}$ denote column coordinate vectors. Then *the equation* $k\mathbf{y} = \mathbf{Ax}$, *where* k *is any non-zero element of* $GF(p^n)$, *determines a homography in the space of period* N. This is Singer's theorem; and the proof differs from his more in form than substance. It is significant for us that N is also the number of points in the space.

3. Confine attention now to the case where $p = 2$ and $n = 1$. The space, a $PG(m-1, 2)$, contains μ, $= 2^m - 1$, points, with three on every line.

The following are primitive irreducible polynomials over $GF(2)$:

$$x^2 - (x+1), \quad x^3 - (x+1), \quad x^4 - (x+1),$$
$$x^5 - (x^2+1), \quad x^6 - (x+1), \quad x^7 - (x+1)$$
$$x^8 - (x^4 + x^3 + x^2 + 1), \quad x^9 - (x^8 + x^4 + x^3 + x^2 + 1).$$

This list is taken from Dickson ([4], p. 44); it is not exhaustive for the degrees mentioned but for each degree the second largest exponent of x is as small as possible.

For a given m, choose any appropriate primitive polynomial and consider the associated homography of $PG(m-1, 2)$ of period μ. If P_1 is any point of the space, let its successive transforms under the homography be $P_2, P_3, \cdots, P_\mu$ $(P_{\mu+1} = P_1)$.

Now consider the space $PG(m-1, 2)$ as being a prime in a $PG(m, 2)$. To achieve this, suppose $\mathbf{x}_1, \cdots, \mathbf{x}_\mu$ are coordinate vectors for $P_1, \cdots, P_\mu$. Then coordinate vectors for all but one of the points in $PG(m, 2)$ are obtained by adding a further zero or unit coordinate at the end of each $\mathbf{x}_i$; and the last point by taking coordinates consisting of m zeros followed by 1. Denote this last point by Q_0 and let Q_i be the third point on the line Q_0P_i; Q_i and P_i have the same first m coordinates.

To fix ideas, take $m = 3$ and $f(x) = x^3 - x - 1$. Then $\mu = 7$ and the corresponding homography is

$$k\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

or

$$y_0 : y_1 : y_2 = x_1 : x_2 : x_0 + x_1 .$$

Starting with $x_0 = 1, x_1 = x_2 = 0$, we obtain for $PG(3, 2)$ the following points:

$$P_1\ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}\quad P_2\ \begin{pmatrix}0\\0\\1\\0\end{pmatrix}\quad P_3\ \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\quad P_4\ \begin{pmatrix}1\\0\\1\\0\end{pmatrix}\quad P_5\ \begin{pmatrix}0\\1\\1\\0\end{pmatrix}\quad P_6\ \begin{pmatrix}1\\1\\1\\0\end{pmatrix}\quad P_7\ \begin{pmatrix}1\\1\\0\\0\end{pmatrix}$$

$$Q_0\ \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\quad Q_1\ \begin{pmatrix}1\\0\\0\\1\end{pmatrix}\quad Q_2\ \begin{pmatrix}0\\0\\1\\1\end{pmatrix}\quad Q_3\ \begin{pmatrix}0\\1\\0\\1\end{pmatrix}\quad Q_4\ \begin{pmatrix}1\\0\\1\\1\end{pmatrix}\quad Q_5\ \begin{pmatrix}0\\1\\1\\1\end{pmatrix}\quad Q_6\ \begin{pmatrix}1\\1\\1\\1\end{pmatrix}\quad Q_7\ \begin{pmatrix}1\\1\\0\\1\end{pmatrix}$$

4. The idea is now to rename the points $Q_1, \cdots, Q_\mu$ as $R_1, \cdots, R_\mu$ in some order to be determined with the object, when possible, of ensuring that whenever the line Q_iQ_j passes through a point P_r then the line R_iR_j passes through a different point P_s.

The various incidences are then registered in a table of μ rows and μ columns as follows: if the line Q_iQ_j passes through P_r and R_iR_j passes through P_s make the entry

$$i, j \qquad (\text{or } j, i)$$

in the place belonging to the rth row and sth column of the table.

The number of entries in each row and column is the number of lines through a point of $PG(m, 2)$ which do not lie in a prime through the point. This number is $(2^m - 1) - (2^{m-1} - 1) = 2^{m-1}$. And the entries in every row and column are all the integers $0, 1, 2, 3, \cdots, 2^m - 1$ taken in pairs. No two pairs are the same and there are $2^{m-1}(2^m - 1)$ entries altogether.

In the cases examined below, the desired objective is reached when m is odd by defining R_t to be Q_u, where $u = 2^m - t$; and then no position in the incidence table contains more than one entry of the form (i, j). When m is even, the same definition is used for R_t but this leads to two entries in each position in the south-

TABLE 1

	1	2	3	4	5	6	7
1			24		56	37	01
2		35		67	41	02	
3	46		71	52	03		
4		12	63	04			57
5	23	74	05			61	
6	15	06			72		34
7	07			13		45	26

TABLE 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1					3, 9		12, 13			2, 5	7, 14		4, 15	8, 10 0, 2	0, 1 6, 11
2				4, 10		13, 14			3, 6	8, 15		5, 1	9, 11 0, 3	7, 12	
3			5, 11		14, 15			4, 7	9, 1		6, 2	10, 12 0, 4	8, 13		
4		6, 12		15, 1			5, 8	10, 2		7, 3	11, 13 0, 5	9, 14			
5	7, 13		1, 2			6, 9	11, 3		8, 4	12, 14 0, 6	10, 15				
6		2, 3			7, 10	12, 4		9, 5	13, 15 0, 7	11, 1					8, 14
7	3, 4			8, 11	13, 5		10, 6	14, 1 0, 8	12, 2					9, 15	
8			9, 12	14, 6		11, 7	15, 2 0, 9	13, 3					10, 1		4, 5
9		10, 13	15, 7		12, 8	1, 3 0, 10	14, 4					11, 2		5, 6	
10	11, 14	1, 8		13, 9	2, 4 0, 11	15, 5					12, 3		6, 7		
11	2, 9		14, 10	3, 5 0, 12	1, 6					13, 4		7, 8			12, 15
12		15, 11	4, 6 0, 13	2, 7					14, 5		8, 9			13, 1	3, 10
13	1, 12	5, 7 0, 14	3, 8					15, 6		9, 10			14, 2	4, 11	
14	6, 8 0, 15	4, 9					1, 7		10, 11			15, 3	5, 12		2, 13
15	5, 10					2, 8		11, 12			1, 4	6, 13		3, 14	7, 9

west to north-east diagonal of the table: no better definition for R_i has been devised which will prevent two entries from occurring in the same position.

5. For the case $m = 3$, which we began to consider in Section 3, let us define R_i to be Q_{8-i} $(i = 1, \cdots, 7)$. We then obtain the incidences shown in Table 1.

It will be noticed that, beginning with the second, each row or column is obtained by a cyclic change in the positions, and values modulo 7, of the entries in the preceding row or column: that is, if X_{rs}, Y_{rs} are the entries in row r and column s and $X_{rs} \neq 0$, then, modulo 7,

$$X_{r,s} \equiv 1 + X_{r-1,s+1}, \qquad Y_{r,s} \equiv 1 + Y_{r-1,s+1}.$$

The whole table is therefore completely determined by the entries in any one row or column.

6. For $m = 4$, we have $\mu = 15$ and we take $f(x) = x^4 - x - 1$. R_i is now defined to be Q_{16-i} for $i = 1, \cdots, 15$. Table 2 is obtained.

Here the NE–SW diagonal is shared by two sets of entries. This is a characteristic feature arising when m is even but not when m is odd.

In fact, going now to the simplest case where $m = 2$ and $f(x) = x^2 - x - 1$, the table which arises is as follows:

	1	2	3
1			0 1 2 3
2		0 2 3 1	
3	0 3 1 2		

For $m = 5$, $\mu = 31$. Take $f(x) = x^5 - x^2 - 1$. Define R_i to be Q_{32-i}. Then we obtain Table 3 (only the first line of entries need be given).

TABLE 3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
12,20	8,23	9,21	14,15		10,17		27,29				2,19			18,31

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
22,26	5,11						16,25	3,6			13,24		7,28	4,30	0,1

7. If the columns of the first design of Section 5 be regarded as blocks, the rows as a set of treatments $a_1, \cdots, a_7$, and the numbers in the squares as a second set of treatments $b_0, \cdots b_7$, then the design is an incomplete block with respect to the first set of treatments and a complete randomized block with respect to the second set of treatments. The design is also balanced with respect to combinations of different levels of treatment a, with different levels of treatment b. The usual parametric model (Model I) would be

$$x_{ti;j} = A + B_t + \alpha_i + \beta_j + z_{ti;j}$$

(where $x_{ti;j}$ denotes the observation on treatment combination a_ib_j in the tth block, $\sum B_t = \sum \alpha_i = \sum \beta_j = 0$ and the $z_{ti;j}$'s are mutually independent random variables with common variance and mean zero). The analysis of variance appropriate to this model is obtained as follows:

(i) Carry out the standard incomplete block analysis on the means $\bar{x}_{ti}$ of pairs of observations for treatments a_i in the same (tth) block. Multiply the resultant sums of squares by two. This will give the Between Blocks and Adjusted Between Treatments a sums of squares in the final table.

(ii) Compute the Between Treatments b sum of squares in the usual way (that is, $7 \sum_{j=0}^{7} (\bar{x}_{\cdot\cdot j} - \bar{x}_{\cdot\cdot\cdot})^2$).

(iii) Compute the Residual sum of squares as Residual in (i) + $\sum_t \sum_i \sum_j (x_{ti;j} - \bar{x}_{ti\cdot})^2$ − Between Treatment sum of squares in (ii).

The degrees of freedom appropriate to these sums of squares are then

Blocks	6
Adjusted Treatments a	6
Treatments b	7
Residual	36

One advantage of this design lies in the fact that the treatment b sum of squares is orthogonal to the treatment a sum of squares. It is, unfortunately, not possible to test for interaction between the two sets of treatments. Certain specific interactions may, however, be isolated from the Residual sum of squares. For example the contrast b_2 vs. b_4 in the presence of a_1 can be compared with the average effect of the same contrast in the presence of $a_2a_3 \cdots a_7$, provided it is assumed that other interactions between a and b are negligible. The calculation of the sum of squares for such a contrast could be based on a two-way table with entries

$$b_2a_1, \quad b_4a_1 \qquad b_2 \sum_{i=2}^{7} a_i, \qquad b_4 \sum_{i=2}^{7} a_i$$

in the usual way.

Alternatively, the design may be regarded as an incomplete block design for treatments a, with main plots split for treatment b. In this case the design should be regarded as an incomplete block design also with respect to treatments b. The

model becomes

$$x_{tij} = A + B_t + \alpha_i + \beta_j + u_{ti} + z_{tij}$$

where the u_{ti}'s are independent random variables, with zero mean and common variance, which are also independent of the z_{tij}'s. The two incomplete block analyses may be carried out separately (except that the Blocks sum of squares in the Treatments b analysis is the Total sum of squares in the Treatments a analysis). The sums of squares in the complete analysis, and their associated degrees of freedom, are

Blocks	6	
Adjusted Treatments a	6	As in the original
Error (i)	15	analysis (i)
Adjusted Treatments b	7	
Error (ii)	21	

As in the earlier analysis it is not possible, in general, to test for interaction between a and b, but certain specific interactions can be isolated from Error (ii).

Similar considerations apply to the second design of Section 7.

The design shown in paragraph 8 is a supplemented incomplete block design (in the sense of [5]) with respect to treatment a. The analysis of the design will, however, be similar to that described above for the designs of Section 7, and in particular the Treatment b sum of squares will again be orthogonal to the adjusted Treatment a sum of squares.

REFERENCES

[1] T. G. Room, "A new type of magic square," *Math. Gazette*, Vol. 39 (1955), p. 307.

[2] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, Vol. 43, (1938), pp. 377–385.

[3] C. C. MacDuffee, *Introduction to Abstract Algebra*, John Wiley & Sons.

[4] L. E. Dickson, *Linear Groups*, Teubner, Leipzig (1901).

[5] T. N. Hoblyn, S. C. Pearce and G. H. Freeman, "Some considerations in the design of successive experiments in fruit plantations," *Biometrics*, Vol. 10, (1954), pp. 503–515.