CLASSICAL GEOMETRIES

10. Orthogonal Latin squares and finite projective planes

10.1 Latin squares

Suppose that you wish to make a quilt with 9 patches in a 3 by 3 square but there are only 3 different colors available for each patch. In order to avoid monotony, suppose that you decide that each row and each column have one patch of each color. If the three colors are A, B, and C, it is clear that the following is "essentially" the only way to construct the quilt:

$$\begin{matrix} A & B & C \\ B & C & A \\ C & A & B \end{matrix}$$

Figure 10.1.1

This is called a 3 by 3 *Latin square.*

Suppose that you wish to make another Latin square so that when they overlap, all possible pairs of colors occur. We say that the 2 Latin squares are *orthogonal* in this case. The following is an example:

$$\begin{matrix} AA & BB & CC \\ BC & CA & AB \\ CB & AC & BA \end{matrix}$$

Figure 10.1.2

It is clear how to generalize this. An n by n Latin square is a square array (or matrix) of n symbols A, B, C,... such that no 2 symbols appear twice in any row or column and each symbol appears once and only once in each row and column. We say that 2 Latin squares are *orthogonal* if all n^2 possible ordered pairs of symbols occur (once and only once). It is clear that there cannot be another Latin square orthogonal to

$$\begin{matrix} A & B \\ B & A \end{matrix}$$

Euler conjectured that there was not even one pair of orthogonal 6 by 6 Latin squares. In 1900 Tarry proved that Euler was right. There are not any pair of orthogonal 6 by 6 Latin squares. However, Euler even went so far as to conjecture that there was no pair of orthogonal n by n Latin squares for any $n \equiv 2 \pmod 4$, $n \geq 6$. In other words, in addition to the case $n = 6$, Euler conjectured that there were no such orthogonal Latin squares for $n = 10, 14, 18, 22, 26, \ldots$. However, in 1959 R. C. Bose and S. S. Shrikhande as well as E. T. Parker proved that for any $n \equiv 2 \pmod 4$, $n \geq 10$, there are always at least 2 orthogonal Latin squares of order n, disproving Euler's conjecture completely. See the copy of two orthogonal 10 by 10 Latin squares at the end of this Chapter. See also Martin Gardner's Chapter, which is a reprint of an earlier column of his in the Scientific American.

10.2 Experimental design

Suppose that you have three varieties of wheat, A, B, C, and you wish to test the effects of a fertilizer in three different concentrations. However, there may be some unpredictable effects due to differences in the soil. You arrange an experiment to grow the wheat in a 3 by 3 grid. In each grid cell you grow one of the varieties of wheat, and treat it with one of the concentrations of fertilizer. You naturally want to arrange the experiment so that you see all 9 possible combinations of fertilizer and wheat. But you also want to arrange each row and column so that all three varieties of wheat and three concentrations of fertilizer occur, in order to minimize any bias due to variation in the soil. The design in Figure 10.1.2 does the job. The left symbol represents the variety of wheat, and the right symbol represents the concentration of fertilizer.

Clearly you can do the same sort of thing for any number of varieties that are one of the possibilities for orthogonal Latin squares. See the books by Cox and Finney.

10.3 Planes and squares

What does Section 10.1 got to do with finite projective planes?

Theorem 10.3.1. *There are $n-1$ mutually orthogonal n by n Latin squares if and only if there is a finite projective plane of order n.*

For instance, since there are finite projective planes of order $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, \ldots$ the theorem says that there are at least 2 orthogonal Latin squares of those orders except for order 2 (corresponding to the Fano plane).

Proof of Theorem 10.3.1. We will describe a correspondence from finite projective planes of order n to a set of $n-1$ mutually orthogonal n by n Latin squares. Fix any two distinct points X_∞ and V_∞. Let l_∞ be the line incident to them. Since each line has $n+1$ ppoints on it let Q_1, Q_2, … ,Q_{n-1} be the remaining points on l_∞. The i-th Latin square will correspond to Q_i.

Label the lines, other than l_∞, incident to X_∞ by 1, 2, … ,n. Similarly, label the lines, other than l_∞, incident to V_∞ by 1, 2, … ,n. Each point not on l_∞ is incident to exactly one pair of these lines. We call P_{ij} the point which is incident to the line labeled

i through X_∞ and the line labeled j through V_∞. The point P_{ij} will correspond to the $4ij$-th position in any of the Latin squares.

Label the n lines, other than l_∞, that are incident to Q_i by the n symbols A, B, ... Each symbol for these lines corresponds to the same symbol in the Latin square associated to Q_i. In fact, the symbol X goes in the jk position of the i-th Latin square if X is the label of the line from P_{ij} to Q_i. See Figure 10.3.1.

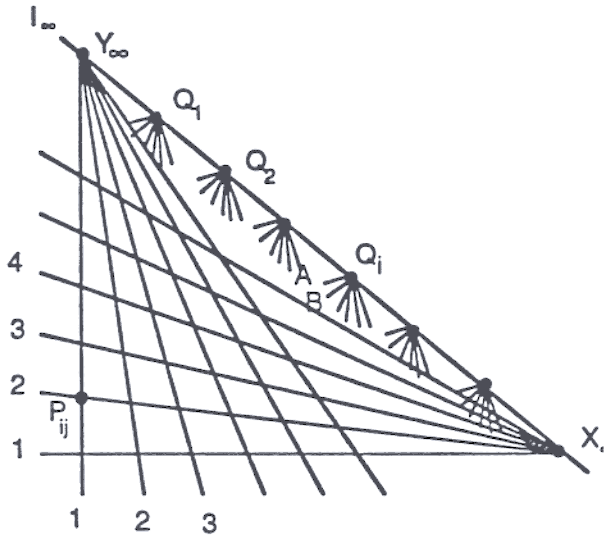


Figure 10.3.1

Note that this construction does produce a Latin square for each Q_i since the line labelled X incident to Q_i (which is not the line l_∞) will be incident to each of the lines from X_∞ as well as Y_∞ at exactly one point. Hence each row and each column will have one of each symbol.

Similarly, any two such Latin squares are orthogonal, since the line labelled X from Q_i meets the line labelled Y from Q_k in exactly one point. So all the pairs XY occur once and only once.

It is not hard to see that the correspondence works the other way as well. Namely, $n-1$ orthogonal n by n Latin squares can be used to create a projective plane of order n.

10.4 Impossible projective planes

Perhaps the moral of the story about orthogonal Latin squares for finite projective planes is that it is very difficult to construct finite projective planes, at least by using orthogonal Latin squares. Euler's conjecture, the correct part, eliminates there being any finite projective plane of order 6. But it seems that no other order for a projective plane can be eliminated so easily.

So the question arises: Are there any other orders for projective planes that can be eliminated? This is a very hard question and about the only result known, which we will not prove, is the following by R. H. Bruck and H. J. Ryser in 1949:

Theorem 10.4.1 (Bruck-Ryser). *Let $n \equiv 1$ or $2 \pmod 4$, and let the square-free part of n contain at least one prime $p \equiv 3 \pmod 4$. Then there does not exist a finite projective of order n.*

Write n as the product of distinct prime powers. Those primes with an odd power are primes in the statement of the Theorem.

For example, $6 = 2 \cdot 3 \equiv 2 \pmod 4$, and the primes in the square-free part are 2 and 3. We see that $3 \equiv 3 \pmod 4$, so the Bruck-Ryser Theorem eliminates 6 as a possible order for a projective plane. Similarly, $14, 21, 22, 30, 33, \ldots$ are also eliminated as orders.

Until recently, the orders in the Bruck-Ryser Theorem were the only orders that were known to be eliminated. In the last few years there has been a concerted effort, orchestrated by R. Graham at Bell Labs, to show that there is no finite projective plane of order 10, the first unsettled case, and a famous previously unsolved problem in combinatorics. (Recall that any prime power is the order of a finite projective plane.) This effort was successful, but only at the cost of a great deal of computer time. So as of now, 10 and the orders eliminated by the Bruck-Ryser Theorem are the only known orders eliminated for finite projective planes. The next unsettled case is order 12.

Despite the difficulty of constructing orthogonal Latin squares, it is possible to construct finite projective planes other than the ones coming from fields. However, all of these planes have prime power order. So we have the following basic conjecture, which seems to be one of the most difficult problems in combinatorial mathematics:

Conjecture 10.4.2. *Every finite projective plane has prime power order.*

Exercises:

1. A *magic square* (of a degenerate sort) is an n by n square array of the numbers $1, 2, 3, \ldots, n^2$, where the sum of each row and column is the same. (Usually the two main diagonals are required to have this "magic sum" as well, but we will not consider that extra property.) Show that this sum is $\frac{n(n^2+1)}{2}$.
2. Let (x_{ij}) and (y_{ij}) be orthogonal n by n Latin squares, where the symbols are the integers $0, 1, 2, \ldots, n-1$, and x_{ij} is the ij-th entry of the matrix (x_{ij}), and similarly for y_{ij}. Show that $(nx_{ij} + y_{ij} + 1)$ is an n by n square.

   For example, we can create a 3 by 3 Latin square this way as follows:

$$\begin{pmatrix} 3\cdot 0+0+1 & 3\cdot 1+1+1 & 3\cdot 2+2+1 \\ 3\cdot 2+1+1 & 3\cdot 0+2+1 & 3\cdot 1+0+1 \\ 3\cdot 1+2+1 & 3\cdot 2+0+1 & 3\cdot 0+1+1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 9 \\ 8 & 3 & 4 \\ 6 & 7 & 2 \end{pmatrix}$$

   Note that the diagonals do not add up to $15 = 3 \cdot (9+1)/2$, the magic sum.
3. Does the following 4 by 4 magic square arise from the method of exercise 2?

$$\begin{pmatrix} 1 & 15 & 14 & 4 \\ 12 & 6 & 7 & 9 \\ 8 & 10 & 11 & 5 \\ 13 & 3 & 2 & 16 \end{pmatrix}$$

4. Use the finite field of order 5 as discussed in the text to write down a pair of 5 by 5 orthogonal Latin squares.

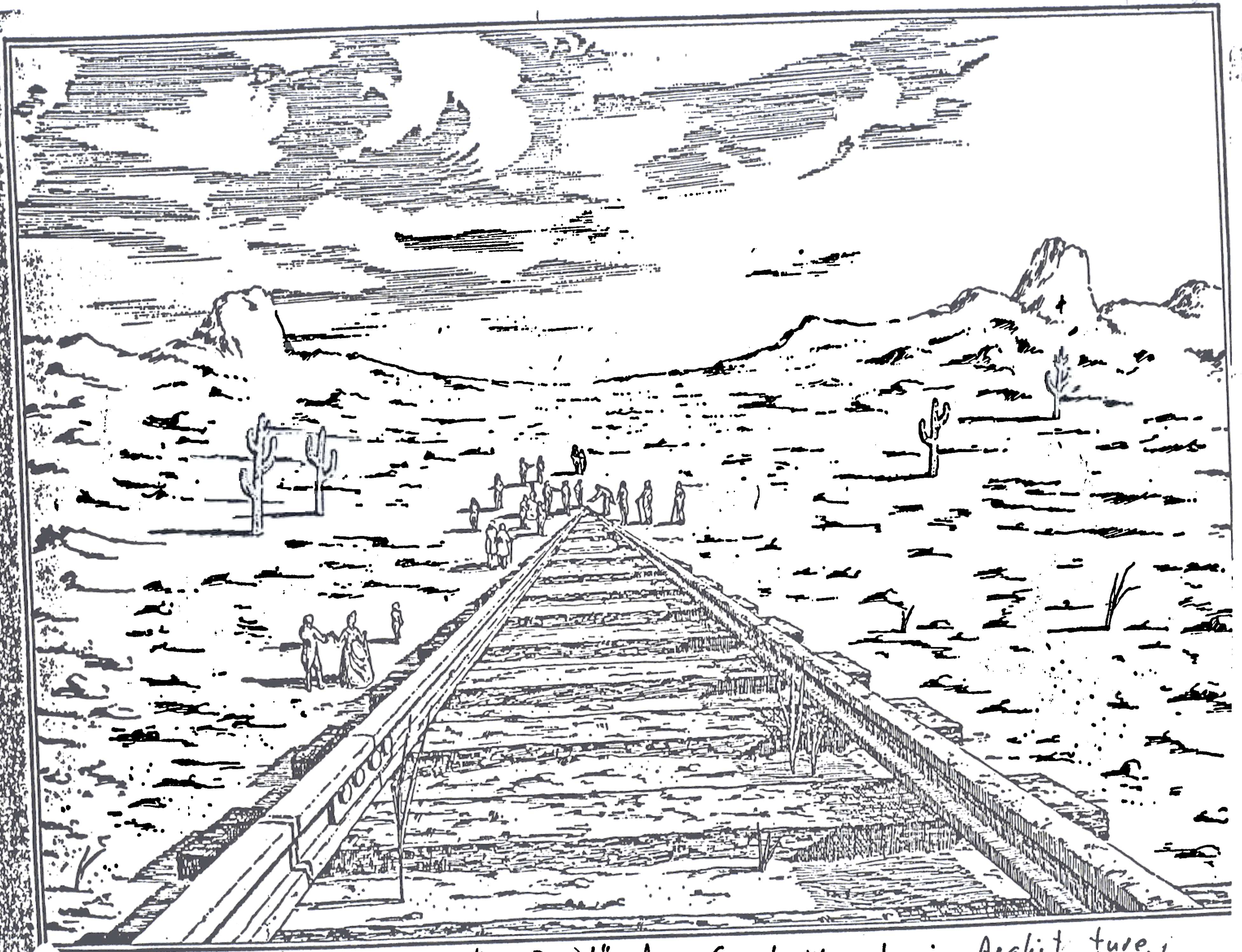
   It may be helpful to think in the following terms: The points Q_i on l_∞ can be regarded as slopes in an Affine plane, and the lines incident to Q_i as a set of parallel lines of fixed slope. Build the orthogonal Latin squares using the slopes 1/2 and 2/1 say, but in the field $\mathbf{Z}/5$, the integers modulo 5. For example, if A is one of the symbols, in the first Latin square corresponding to 1/2, at the position (i,j), then the other A's appear at $(i+1, j+2)$, $(i+2, j+4)$, etc., modulo 5, as below for the slope 1/2.

$$\begin{pmatrix} & & A & B & \\ B & & & & A \\ & A & B & & \\ & & & A & B \\ A & B & & & \end{pmatrix}$$

   What goes wrong with this method when $n = 6$?
5. Construct a pair of 9 by 9 orthogonal Latin squares.
6. It is a result in number theory that there are infinitely many primes $p \equiv 1 \pmod 4$, and there are infinitely many primes $p \equiv 3 \pmod 4$. Use this result to show that there are infinitely many orders for projective planes that are eliminated by the Bruck-Ryser Theorem.

00	47	18	76	29	93	85	34	61	52
86	11	57	28	70	39	94	45	02	63
95	80	22	67	38	71	49	56	13	04
59	96	81	33	07	48	72	60	24	15
73	69	90	82	44	17	58	01	35	26
68	74	09	91	83	55	27	12	46	30
37	08	75	19	92	84	66	23	50	41
14	25	36	40	51	62	03	77	88	99
21	32	43	54	65	06	10	89	97	78
42	53	64	05	16	20	31	98	79	87

FIG. 85
E. T. Parker's Graeco-Latin square of order 10, a counter-example to Euler's conjecture.



"Locating the Vanishing Point", from Great Moments in Architecture.