Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Ralph H. F. Denniston

Cyclic packings of the projective space of order 8

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **54** (1973), n.3, p. 373–377.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1973_8_54_3_373_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1973.

Geometria. — *Cyclic packings of the projective space of order 8.* Nota di RALPH H. F. DENNISTON, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Nello spazio proiettivo tridimensionale di Galois di ordine 8, si può costruire una collineazione T di periodo 73, ed un insieme $\mathcal{S}$ di rette (una cosiddetta *fibrazione*). Ogni punto dello spazio appartiene ad una ed una sola retta di $\mathcal{S}$: ogni retta appartiene ad uno ed uno solo degli insiemi $\mathcal{S}, T\mathcal{S}, T^2\mathcal{S}, \cdots, T^{72}\mathcal{S}$. Queste condizioni non bastano per caratterizzare la fibrazione $\mathcal{S}$; si costruiscono infatti parecchie fibrazioni, di tipi assai diversi, che le verificano.

In a recent Note [1] I gave the definition of a "packing", for a finite three-dimensional projective geometry, and mentioned the importance of finding various ways in which packings could be constructed. In the present Note I exhibit some packings of the space of order 8, which seem in two ways to be better than those given in [1]. Namely, each packing consists of spreads of a single projective type; and that type varies widely from one packing to another. So there is some hope that one of them might be used in the construction of a projective plane of order 72. This is an enterprise in which I have not succeeded: but I trust that the publication of these results may be a step towards its achievement by somebody.

Let the Galois field $GF(2^3)$ be constructed by adjoining to $GF(2)$ an element i such that $i^3 = i^2 + 1$. Let the three-dimensional projective space of order 8 be provided with non-homogeneous coordinates (x, y, z) over this field. A point which is neither the origin nor at infinity may be called "a general point", and a line which is neither at infinity nor through the origin, "a general line". Let us, by a well-known method (see for instance Snapper [4]), identify the finite points with the elements of $GF(2^9)$, in such a way that multiplication by a primitive element of $GF(2^9)$ gives a collineation that permutes the general points cyclically. The seventh and seventy-third powers of one such collineation may be specified by

$$T: \ (x, y, z) \to (i^3 x + i^6 y + iz , i^5 x + i^3 y + i^3 z , i^3 x + iy + i^5 z),$$

$$U: \ (x, y, z) \to (ix, iy, iz).$$

Then T^{73} and U^7 are the identity; and T and U commute, and generate a group that is sharply transitive on the general points (but fixes the origin). The plane at infinity has its points all permuted cyclically by T, and its lines likewise, whereas U fixes them all.

We may suppose that the point $P_0(0, 0, 1)$ was identified with the unit element of $GF(2^9)$; let us now use the symbol $[t, u]$ for the point $T^t U^u P_0$.

(*) Nella seduta del 10 marzo 1973.

Any given general point can be represented in this way by "coordinates" t and u, determined modulis 73 and 7 respectively.

Now it is known (from the theory of "multipliers") that another collineation will be obtained if we apply to each element of $GF(2^9)$ the automorphism $x \to x^2$. This collineation is

$$V: [t, u] \to [2t, 2u], \quad \text{or} \quad (x, y, z) \to (i^4 x^2 + i^6 y^2, x^2 + y^2, z^2),$$

and its period is 9. Let us take a line g_0—say $y = 0$, $z = 1$—and list the "coordinates" $[t, u]$ of the eight finite points of g_0:

$$[0, 0], \; [72, 0], \; [61, 1], \; [14, 3], \; [22, 4], \; [55, 4], \; [68, 4], \; [52, 5].$$

We observe that 0 is the only value of u which appears just twice in this list, and that the corresponding residues t are 0 and -1. For integers t, u, v, the line $T^t U^u V^v g_0$ has on it the points $[t, u]$ and $[t - 2^v, u]$. Suppose, then, we are told that a given (general) line can be identified with some $T^t U^u V^v g_0$, but the exponents t, u, v are unknown: we may begin by looking, among the second "coordinates" of points on this line, for a residue u that occurs exactly twice. Then, since the 18 residues $\pm 2^v$ mod 73 ($v = 0, \cdots, 8$) are all different, we can find t and v by looking at the first "coordinates" of the same two points. So it is appropriate to use the symbol $[t, u, v]$ for $T^t U^u V^v g_0$, the "line-coordinates" t, u, v being determined modulis 73, 7, 9. But the number of general lines happens to be exactly 73.7.9; and it follows that every general line can be given "line-coordinates" in this way. (The space of order 2 is the only other one in which an arrangement like this could be made: the equation $p^k + 1 = 3k$ has just these two solutions.) The action on general lines of our three collineations is specified by

$$T[t, u, v] = [t+1, u, v] \quad , \quad U[t, u, v] = [t, u+1, v],$$
$$V[t, u, v] = [2t, 2u, v+1].$$

The collineation V fixes two lines, the z–axis and the line at infinity on $z = 0$ (say z and XY for short). It permutes all the other lines, and all the points not on z, in orbits of length nine. Now suppose we have managed to find integers $t_0, t_1, \cdots, t_6$, such that the lines $[t_0, 0, 0], [t_1, 1, 0], \cdots$ $\cdots, [t_6, 6, 0]$ are all skew to each other and to z and XY; and moreover that the set of 63 points on these seven lines has not more than one point in common with any point-orbit of V. Then we may transform each of the seven lines by V^v ($v = 0, \cdots, 8$), and so obtain 63 lines which again are all skew to each other, and to z and XY. The second and third "coordinates" of any such line are $2^v u$ and v ($u = 0, \cdots, 6$; $v = 0, \cdots, 8$), and are not both congruent (modd 7 and 9) to the respective "coordinates" of any other of the 63 lines.

There are nine points on a line and 9.65 points in the space; so a collection of 65 mutually skew lines must be a spread. Let $\mathcal{S}$ be the spread consisting of z, XY, and the 63 lines we have constructed: let us consider the images of $\mathcal{S}$ under collineations T^t, where $t = 0, 1, \cdots, 72$. We shall have z

transformed into each in turn of the 73 lines through the origin, and XY into each of the 73 lines at infinity. For each of the 63 lines, the " coordinate " t runs over the residues mod 73, while the other two " coordinates " remain fixed; we generate without any repetitions a set of 73.63 general lines—that is, the whole set of general lines. So each line of the projective space will belong to one and only one spread of the set $\{ T^t \mathcal{S} \}$: that is, this set of spreads will be a packing.

A complete search for sets $\{ t_u \}$, each of seven residues mod 73, was not impracticable, and in fact I carried it out by hand. A certain symmetry, which appeared when the solutions to the problem were tabulated, was a reassurance that no solution had been missed. There is in fact a polarity, W say, specified by

$$x_1 y_2 + y_1 x_2 + z_1 z_2 + 1 = 0 .$$

On the plane $z = 1$, any point is conjugate in W to itself and also to P_0; and so each line $[0, 0, v]$ $(v = 0, \cdots, 8)$ is self-polar in W. If points P and TQ are conjugate, then TP and Q are also conjugate in W: therefore, if g is the polar line of h, then Tg is the polar line of $T^{-1}h$. Similarly, if g is the polar line of h, then the polar line of $U^{-1}h$ is Ug; and we find, by repeated application of these results, that any general line $[t, u, v]$ has $[-t, -u, v]$ as its polar line in W. This means that, if the set $\{t_0, \cdots, t_6\}$ of residues mod 73 is a solution of our problem, a " dual " solution to it will be $\{-t_0, -t_6, \cdots, -t_1\}$. In fact, the former solution gives a packing, which is transformed (by the correlation W) into a set of sets of lines, with the self-dual property of being a packing.

Six of the solutions included in $\mathcal{S}$ the line $[30, 0, 0]$ and its successive images under V; these nine lines in fact make up a regulus, and the complementary regulus consists of $[43, 0, 0]$ and its successive images. This means that, for each solution where $t_0 = 30$, there is another solution for which $t_0 = 43$, the other numbers t_u being unchanged. I found 20 solutions altogether; but, if I specify seven of them, the reader can complete the list by adding three for which $t_0 = 43$, and ten " dual " solutions.

	t_0	t_1	t_2	t_3	t_4	t_5	t_6
A	30	66	17	15	20	38	50
B	30	15	38	17	50	20	66
C	30	54	9	41	60	34	40
D	4	13	7	47	25	20	39
E	41	15	65	37	35	34	70
F	44	11	60	50	32	41	62
G	8	9	32	43	45	19	64

In case A, the spread $\mathcal{S}$ is regular, as I have verified by writing out Plücker line-coordinates for all its lines, and finding two equations that they satisfy. Accordingly, when we "switch" a regulus (by changing t_0 to 43, as above), we obtain another solution, with $\mathcal{S}$ as a subregular spread of index 1. Case B is more surprising: $\mathcal{S}$ here is made up of seven disjoint reguli (not all, as might be supposed, line-orbits of V), together with the lines z and XY. It happens that, if we switch all seven reguli at once, we arrive at a spread which is the dual solution to our problem; of course, these are only two out of 2^7 spreads which could be found by switching various subsets of the set of reguli, and which contain seven reguli each (taken from a set of 14). But I have verified that no fifteenth regulus is contained in any of these 2^7 spreads: so we have examples of a possibility hitherto unknown—a spread containing reguli without being subregular. These examples are not all projectively equivalent; if we search for nine lines that have just two common transversals, we never find them except in two of the 2^7 spreads, and these are in this case the two that are solutions to our problem. In case C, the spread $\mathcal{S}$ belongs to a similar collection of 2^7 spreads, but this time $\mathcal{S}$ is not one of the two with the property of including nine lines with just two common transversals.

In cases D and E, the spread $\mathcal{S}$ is of a type which I have described in another note [2]. Briefly, if we choose two planes which correspond in a suitable (non-projective) collineation of the space, and join corresponding points of those planes, we construct such a spread. In all spaces of order p^k (p prime, $k > 1$), spreads of this type exist, and they seem to be self-dual when p is odd or k even: but self-duality does not hold for the spreads we have here, and so cases D and E are slightly different from their own duals.

The spread $\mathcal{S}$ in case F contains no regulus; in fact, I have carried out a complete and unsuccessful search for nine lines of this spread with two common transversals. I have not made a detailed study of case G, but presume that results in that case would likewise be negative. (The reader may be inclined to wonder whether, among the spreads involved here, there might not be a spread of special tangents to a Segre ovoid [3]. But, in fact, the collineations fixing such a spread make up the Suzuki group of order $8^2.65.7$, and could not include our collineation V of period 9.)

We have seen that, by using a very special method, we can construct at least six packings of the projective space of order 8, none of which can be transformed into another by a collineation or a correlation. It would seem, not merely that packings exist in all the finite three-dimensional spaces (as established in [1]), but that the number of distinct types, in a given space, may be larger for packings than for spreads. The space of order 3, for instance, has no spreads other than the regular and the subregular of index 1: for we know that the only translation planes of order 9 are the Desarguesian and the Hall plane. But, since the presentation of [1], I have found three different packings of that space that consist entirely of subregular spreads; two (not covered by [1]) that each use one regular spread and twelve subregular; and three, each comprising eleven regular and two subregular spreads. In this enumeration, I am not counting a packing as different from its own image under a collineation, or even a correlation. On the other hand, as I have found by searching, the space of order 3 has no packing that consists entirely of regular spreads.

REFERENCES

[1] R. H. F. DENNISTON, *Some packings of projective spaces*, « Rend. Acc. Naz. Lincei », (8) *52*, 36–40 (1972).

[2] R. H. F. DENNISTON, *Spreads which are not subregular*, « Glasnik Mat. » *8*, 3–5 (1973).

[3] B. SEGRE, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, « Acta Arithm. », *5*, 315–332 (1959).

[4] E. SNAPPER, *Periodic linear transformations of affine and projective geometries*, « Can. J. Math. » *2*, 149–151 (1950).