MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 223–241

The Structure of Certain Triple Systems

By Raphael M. Robinson

To Derrick H. Lehmer on his 70th birthday, February 23, 1975

Abstract. For each prime power $q \equiv 7 \pmod{12}$, there is a triple system of order q whose automorphism group is transitive on unordered pairs. The object of this paper is to study these systems. This is done by analyzing how pairs of elements are linked. The linkage of a and b consists of a triple (a, b, c) and of some cycles in which adjacent pairs of elements form triples alternately with a and with b. Because of the transitivity, the lengths of the cycles will be independent of the choice of a and b.

Using a computer, the linkage between two elements was determined for each $q < 1000$. Some curious facts concerning the lengths of the cycles were uncovered; for example, the number of cycles of length greater than 4 is even. The systems of prime order $p < 1000$ were found to have no proper subsystems of order greater than 3. In the remaining case, $q = 343$, there are subsystems of orders 7 and 49, and all subsystems of the same order are isomorphic. For no q with $7 < q < 1000$ is the automorphism group doubly transitive.

Finally, some general results are proved. The cycles of lengths 4 and 6 are determined. Using this result, it is shown that there can be no subsystem of order 7 or 9, except for the subsystems of order 7 when q is a power of 7. Hence, by a theorem of Marshall Hall, the automorphism group cannot be doubly transitive, except possibly when q is a power of 7. (Added August 1974. In a postscript, it is shown that the automorphism group is not doubly transitive in this case either.)

0. Doubly Transitive Triple Systems. A (Steiner) triple system on a given set of elements is a set of triples of these elements such that each pair of elements is included in one and only one triple. Triple systems are discussed, for example, in Hall [5]. If n is a positive integer, then there is a triple system on n elements if and only if $n \equiv 1, 3 \pmod{6}$. The system is unique for $n \leqslant 9$, but for larger n, this is no longer the case.

Of especial interest are triple systems with a high degree of symmetry. The only systems which are known to have a doubly transitive automorphism group are the projective spaces over the 2-element field and the affine spaces over the 3-element field, where the triples in each case are the lines of the geometry. These yield triple systems with $2^r - 1$ and 3^r elements. Another description of these systems is obtained by starting with the field of 2^r elements with 0 deleted, or with the field of 3^r elements, and letting (x, y, z) form a triple whenever $x + y + z = 0$. A paper by Hall

Received July 8, 1974.
AMS (MOS) subject classifications (1970). Primary 05B05.

[4] raises the question whether there are any other triple systems with doubly transitive automorphism groups, and makes a contribution to the solution by showing that these are the only systems satisfying a stronger condition.

The automorphisms of the system with 3^r elements clearly include the linear transformations $x^\sigma = ax + b$ with $a \neq 0$. These transformations are sufficient to guarantee the double transitivity. In this section, we shall show that there is no other triple system based on a field and having all these automorphisms. Indeed, we find that there is no other system having even the automorphisms $x^\sigma = \pm x + b$.

It will be convenient to discuss first cyclic triple systems, that is, triple systems having an automorphism which permutes the elements cyclically. We may use as elements the residue classes mod n, and assume that $x^\sigma = x + 1$ is an automorphism. Associated with a triple (x, y, z) is the difference triangle (u, v, w) with $u = y - x$, $v = z - y$, $w = x - z$. Here $u + v + w = 0$, but $u \neq 0$, $v \neq 0$, $w \neq 0$. Only the cyclic order of u, v, w is important.

We may represent the system geometrically by placing the element h at $e^{2\pi ih/n}$ A difference triangle can be visualized as a triangle inscribed in the unit circle, its vertices being elements of the triple. However, the lengths of the sides are measured by the arcs cut off. Rotating the triangle through the angle $2\pi/n$ corresponds to the automorphism $x^\sigma = x + 1$. If the triangle is scalene, it will produce n different triples by rotation. It is not permissible for the triangle to be isosceles, since it would produce two different triples with a pair in common. However, if n is a multiple of 3, we could use an equilateral triangle with side $n/3$. It will produce only $n/3$ triples by rotation.

The various difference triangles used must be such that the sides and their negatives exhaust the nonzero residue classes mod n. If $n = 6k + 1$, there must be k scalene triangles, whereas if $n = 6k + 3$, there must be k scalene triangles and an equilateral triangle.

The difference triangle $(-w, -v, -u)$ is equivalent to (u, v, w). But the reversed triangle (w, v, u) or $(-u, -v, -w)$ is not equivalent to this, and is indeed inconsistent with it, unless the triangle is equilateral.

More generally, consider triple systems on an Abelian group of order n which are invariant under addition of constants. These reduce to cyclic triple systems if the group is cyclic. Similar considerations hold in general, except that there may be more than one equilateral triangle. The side of such a triangle will satisfy the equation $3u = 0$, that is, must be a group element of order 3. If a triple system associated with an Abelian group also has the automorphism $x^\sigma = -x$, then with every difference triangle we also have the reversed triangle, hence all difference triangles are equilateral.

We now apply this conclusion to triple systems on a field having the automorphisms $x^\sigma = \pm x + b$. The argument will be based solely on the fact that all difference triangles are equilateral. If u is the side of such a triangle, then $3u = 0$ but $u \neq 0$. It follows that $3 = 0$. Thus $p = 3$ and so $q = 3^r$. Also, in any triple (x, y, z), we would have

$$x + y + z = x + (x + u) + (x + 2u) = 0,$$

which leads back to the triple system of order 3^r already discussed.

1. Systems Transitive on Unordered Pairs. The group of automorphisms $x^\sigma = ax + b$ with $a \neq 0$ discussed in Section 0 has a subgroup of index 2, where a is restricted to be a square. The subgroup takes 0 and 1 into any two elements differing by a nonzero square. Now if -1 is not a square, then these squares and their negatives exhaust the field, except for 0. Hence the subgroup will be transitive on unordered pairs.

In this section, we shall determine the triple systems on a field which admit this group. Since -1 is not a square, we have $p \equiv 3 \pmod 4$ and r odd, or, what is equivalent, $q \equiv 3 \pmod 4$. For a triple system, we must have $q \equiv 1, 3 \pmod 6$. The case $q \equiv 3 \pmod 6$ arises only when $q = 3^r$. In this case, there must be at least one equilateral difference triangle. Multiplication by all nonzero squares then yields $(q - 1)/2$ equilateral difference triangles, so all difference triangles are equilateral. As shown at the end of Section 0, this leads to the doubly transitive system of order 3^r discussed there. Thus we need consider only the case $q \equiv 1 \pmod 6$. Then we must have $q \equiv 7 \pmod{12}$, which is equivalent to $p \equiv 7 \pmod{12}$ and r odd.

Let $q = 6k + 1$. There must be k scalene difference triangles. We may assume that at least two sides of each triangle are squares; otherwise, we reverse the cyclic order of the sides and change their signs. Multiplying the sides of any triangle by the $3k$ nonzero squares, we obtain each of the triangles three times, with their sides permuted cyclically. Hence all of the sides must be squares. Let the triangle containing 1 be $(1, u, v)$. Multiplying by u^{-1} gives the triangle $(u^{-1}, 1, vu^{-1}) = (1, vu^{-1}, u^{-1})$. Hence $vu^{-1} = u$ and $u^{-1} = v$, and so $v = u^2$ and $u = v^2$. It follows that $u^3 = v^3 = 1$.

Since $p \equiv 1 \pmod 6$, the equation $x^3 = 1$ has three integer solutions, that is, three solutions in the p-element subfield. If ω is either of the solutions other than 1, then we may take $u = \omega$ and $v = \omega^2$. All difference triangles are obtained from the basic triangle $(1, \omega, \omega^2)$ by multiplying by nonzero squares. This does yield a triple system with the prescribed automorphisms. The two choices for ω lead to two isomorphic copies of the triple system. One differs from the other by reversing the cyclic order of the differences, which corresponds to changing the signs of all the elements. Except for a few remarks about triple systems in general and about the systems considered in Section 0, the rest of this paper will be devoted to these triple systems.

It will be convenient to introduce the character $\chi(a)$, which has the value 1, 0, or -1 according as a is a nonzero square, 0, or a nonsquare. If $q = p$, then $\chi(a)$ is the Legendre symbol (a/p). More generally, if $q = p^r$ with r odd, and a is an integer, then $\chi(a) = (a/p)$. Since $p \equiv 1 \pmod 6$ in the cases considered, we have $\chi(-3) = 1$. Furthermore, we assumed that $\chi(-1) = -1$, hence also $\chi(3) = -1$.

The third element of a triple (x, y, z) is determined from x and y by the formula

$$z = y + (y - x)\omega \quad \text{if} \quad \chi(y - x) = 1.$$

In case $\chi(y - x) = -1$, then we have $\chi(x - y) = 1$, hence the same formula may be used with x and y interchanged.

When $r > 1$, we may also consider the field of $q = p^r$ elements as an r-dimensional affine space over the p-element field. Since ω is an integer, the preceding paragraph shows that the three elements of any triple are collinear. Every linear subspace will therefore define a subsystem of the given triple system.

In the computer programs discussed in Section 2, I chose the numerically smaller value of ω. For theoretical purposes, a different choice may be better. Since $\omega = (\omega^2)^2$ and $\omega + 1 = -\omega^2$, we have $\chi(\omega) = 1$ and $\chi(\omega + 1) = -1$. These do not furnish any distinction between the two choices for ω. But the latter shows that $\chi(\omega^2 - 1) = -\chi(\omega - 1)$. In other words, for one choice of ω we have $\chi(\omega - 1) = 1$, for the other we have $\chi(\omega - 1) = -1$. We may suppose that ω is chosen so that $\chi(\omega - 1) = 1$. This choice of ω may also be characterized by assuming that $(1, \omega, \omega^2)$ is a triple as well as a difference triangle. Indeed, the triple $(1, \omega, \omega^2)$ corresponds to the difference triangle $(\omega - 1, \omega^2 - \omega, 1 - \omega^2)$, which is obtained from the basic difference triangle $(1, \omega, \omega^2)$ by multiplying by $\omega - 1$. Furthermore, since $(\omega - 1)(\omega + 2) = \omega^2 + \omega - 2 = -3$, it follows that $\chi(\omega + 2) = 1$.

The prescribed linear automorphisms $x^\sigma = ax + b$ with $\chi(a) = 1$ form a group of order $q(q - 1)/2$. The r automorphisms of the field of $q = p^r$ elements are also automorphisms of the triple system which we constructed. We see that a field automorphism commutes with the group of linear automorphisms. Hence, together, the prescribed linear automorphisms and the field automorphisms generate a group of order $rq(q - 1)/2$. For $q = 7$, the automorphism group is in fact larger, and is doubly transitive.

Using a theorem of Marshall Hall, we show in Sections 7–9 that the automorphism group is not doubly transitive in any other case, except possibly when $q = 7^r$. (These sections are independent of Sections 3–6.) Using the results of a computer calculation, we show in Section 5 that it is also not doubly transitive when $q = 7^3$. (This section is independent of Sections 3–4.) Thus only the cases $q = 7^r$ $(r = 5, 7, 9, \cdots)$ remain open.

The triple systems of this section have been characterized by Lüneburg [8] and Kantor [7]. Their work is discussed by Dembowski [3, pp. 96–99]. The description which was given above is on a more elementary level, starting from somewhat special assumptions.

I have not been able to find who first studied the triple system of order $p \equiv 7 \pmod{12}$ considered here. Dembowski [3, p. 98], ascribes it to Netto [9], but this is incorrect, since the system discussed by Netto is different. Netto's system also appears in his book [10, pp. 220–221]; in a note to the second edition, pp. 329–331, Th. Skolem introduces a class of systems including both Netto's and the one discussed here. However, Skolem makes no mention of the special properties of the present system, so it hardly can be ascribed to him. The first appearance of the system in print may be in a problem in Carmichael [1, p. 436].

2. Linkages. A useful tool in studying isomorphisms and automorphisms of triple systems is the type of linkage between two elements. Let S be any triple system, and let a and b be two elements of S. They determine a triple (a, b, c), which we call the key triple of the linkage. All of the rest of the elements fall into cycles of the form $(c_1, c_2, \cdots, c_{2l})$, where $l \geqslant 2$ and (a, c_1, c_2), (b, c_2, c_3), $(a, c_3, c_4), \cdots, (a, c_{2l-1}, c_{2l})$, (b, c_{2l}, c_1) are all triples. Thus any cycle has an even length not less than 4.

Such linkages were used by Reiss [11] in the special case where all the elements not in the key triple form a single cycle. He constructed triple systems of all possible orders in which a suitable pair of elements are linked in this way. Linkages as a tool in studying isomorphisms seem to have been introduced by Cole, Cummings, and White [2]. Details are given in [12, Parts 3–5]. This method was used again by Hall and Swift [6].

If we want more information than is furnished by the cycles described above, we can compute the cross-links joining pairs of elements in the same or different cycles which form a triple with the third element c of the key triple. If S is mapped isomorphically onto another system S', then a and b must be mapped onto elements a' and b' such that the linkage between a' and b' has the same structure as the linkage between a and b.

In the linkage between a and b, the pairs of consecutive elements of a cycle form triples alternately with a and with b. The linkage between b and a is the same, except for the interchange of the first and second pairings. This difference may, however, be enough to make it possible to show that there can be no automorphism interchanging a and b.

In general, the number and lengths of the cycles for the linkage between a and b in S will depend on a and b. However, this will not be the case if the automorphism group is doubly transitive, or even transitive on unordered pairs. Now in the two known kinds of triple systems with doubly transitive automorphism groups, the systems of orders $2^r - 1$ and 3^r, the cycles are all of the same length. Consider the systems as based on the field of 2^r elements with 0 deleted, or on the field of 3^r elements. For the system of order $2^r - 1$, the key triple is $(a, b, a + b)$, and every cycle has the form $(x, x + a, x + a + b, x + b)$. For the system of order 3^r, the key triple is $(a, b, -a - b)$, and every cycle has the form $(x, -x - a, x + a - b, -x + a + b, x - a + b, -x - b)$. Furthermore, in both cases, every element is cross-linked to the opposite element of the same cycle. The key triple with each cycle forms a subsystem of order 7 or 9, respectively.

For the triple systems of order $q \equiv 7 \pmod{12}$ discussed in Section 1, we have a new situation. The linkage structure for each q is unique, except for the possible interchange of the two pairings of consecutive elements of a cycle, but it varies with q in a manner which is not easily predictable. Thus the number and lengths of the cycles for each q seems an interesting object of study. They may be computed taking $a = 0$ and $b = 1$. This was done for $q < 1000$ during March and April 1974 using the CDC 6400 at the Computer Center of the University of California, Berkeley. The main program covered primes $p < 1000$. A special program was written for the only other case, $q = 343$.

In the computer programs, the numerically smaller value of ω was chosen. The key triple is $(0, 1, \omega + 1)$. The remaining elements fall into cycles, and these were computed. In addition, the computer printed out the number to which each element of a cycle was cross-linked, and the name of the cycle to which this number belonged. It is impossible to reproduce all this information here, although it is necessary to refer to it at times. The numbers of cycles of various lengths are given in Table 1. The arrangement is as follows: For each value of q, the total number of cycles is given, then the number of cycles of lengths 6, 12, 18, 24, 30, and then the lengths of all other cycles.

Here are some interesting facts about the lengths of the cycles for $q < 1000$ which may be read from Table 1. (1) There is a cycle of length 4 if and only if $q \equiv 7 \pmod{24}$. (2) The number of other cycles is even. (3) The average length of the cycles is less than 12, but seems to be approaching 12. (4) In the prime cases, the cycles all have lengths divisible by 6 except for one congruent to 4 mod 6 (40 cases) or two congruent to 2 mod 6 (4 cases). For $q = 343$, there is a cycle of length 4 and three of length 14 besides the cycles whose lengths are divisible by 6.

A general proof of (1) is given in Sections 7–8. The statements (2) and (3) lead to obvious conjectures. Finally, with regard to (4), it is clear that there is a strong preference for cycles whose lengths are divisible by 6, but it is not clear whether we should expect the number of exceptions to remain bounded.

We shall also be interested in determining the subsystems of the triple systems considered. In general, if a triple system has n elements and a proper subsystem has s elements, then $n \geqslant 2s + 1$. Otherwise, there would not be enough elements to complete the triples determined by elements of the subsystem and a fixed element not in the subsystem.

A subsystem of the given system of order q which contains 0 and 1 will consist of the key triple and a certain number of cycles. Furthermore, all cycles may be divided into equivalence classes of cycles which are connected by cross-links. There may be a number of minor classes, with fewer than $q/2$ elements each, and perhaps one major class, with more than $q/2$ elements. A proper subsystem containing 0 and 1 must consist of the key triple and some minor classes.

TABLE 1

q	Total Cycles		Cycles of Length				Lengths of Other Cycles
		6	12	18	24	30	
7	1	0	0	0	0	0	4
19	2	1	0	0	0	0	10
31	3	1	0	1	0	0	4
43	4	2	1	0	0	0	16
67	6	4	0	0	1	0	16
79	7	5	0	0	0	0	4, 42
103	9	5	1	1	0	0	4, 36
127	11	8	1	0	0	0	4, 60
139	14	9	2	0	1	0	14, 20
151	13	10	1	0	0	0	4, 72
163	14	9	3	0	0	1	40
199	17	11	2	2	0	0	4, 66
211	18	14	0	1	0	0	28, 36, 42
223	21	14	3	2	0	0	4, 60
271	23	16	1	2	0	2	4, 60
283	24	19	0	2	0	0	10, 42, 78
307	28	18	4	2	0	1	10, 36, 36
331	28	19	4	1	2	0	34, 66
343	33	21	2	3	0	3	4, 14, 14, 14
367	33	23	5	1	1	1	4, 90
379	34	22	6	0	3	1	16, 54
439	41	27	6	2	2	2	4, 54
463	41	28	5	0	1	3	4, 36, 36, 42
487	45	32	7	2	1	0	4, 42, 102
499	44	30	6	2	1	0	22, 36, 36, 42, 48
523	48	32	6	4	1	1	14, 14, 42, 60
547	50	31	9	3	2	3	16, 42
571	50	33	8	3	2	1	28, 36, 78
607	53	40	6	1	0	2	4, 36, 42, 132
619	56	41	4	2	2	1	20, 20, 36, 42, 42, 48
631	57	38	8	2	4	1	4, 36, 48, 54
643	58	39	7	6	0	2	10, 36, 42, 66
691	62	43	9	2	3	0	36, 42, 42, 46, 48
727	63	42	7	3	3	2	4, 36, 36, 36, 36, 54
739	64	46	4	5	3	2	16, 36, 66, 72
751	67	45	6	7	2	2	4, 36, 42, 42, 48
787	72	47	12	4	4	0	14, 20, 36, 54, 66
811	72	50	12	1	2	3	36, 54, 58, 60
823	73	52	9	4	0	3	4, 48, 48, 66, 72
859	74	54	9	1	2	2	10, 42, 42, 48, 72, 84
883	76	55	9	3	1	3	36, 42, 42, 46, 108
907	78	56	7	5	2	1	36, 36, 36, 40, 48, 54, 66
919	81	56	10	4	6	1	4, 42, 42, 126
967	85	61	12	3	3	0	4, 36, 42, 60, 66, 120
991	87	59	10	4	5	3	4, 36, 42, 42, 48, 60

The classes of cycles which are cross-linked to each other were computed. For each prime $p < 1000$, there is a major class, and it contains the longest cycle. On the other hand, for $q = 343$, all classes are minor. The lengths of the cycles in all of the minor classes are printed in Table 2. The notation $4 + 3 \cdot 6$ means that there is a class consisting of a cycle of length 4 and three cycles of length 6. The notation $2(3 \cdot 6)$ means that there are two different classes each consisting of three cycles of length 6. If the totality of minor classes has the form $j(3 \cdot 6)$, with $j = 0, 1, 2, 3$, then the corresponding value of q is listed in the appropriate line in Table 2a. The remaining values of q appear in Table 2b, with the minor classes listed.

TABLE 2a

Minor classes	Values of q
None	7, 19, 31, 43, 67, 103, 127, 151, 163, 199, 211, 271, 283, 331
$3 \cdot 6$	139, 223, 307, 379, 463, 499, 571, 739, 883
$2(3 \cdot 6)$	439, 487, 523, 547, 619, 631, 643, 751, 823, 859, 907, 991
$3(3 \cdot 6)$	691, 787, 811, 919, 967

TABLE 2b

q	List of Minor Classes
79	$4 + 3 \cdot 6$
343	$4, 3 \cdot 6 + 2 \cdot 12, 3 \cdot 14, 3(4 \cdot 6 + 18), 3(2 \cdot 6 + 30)$
367	$2(3 \cdot 6), 6 \cdot 6 + 12 + 18 + 24$
607	$2(3 \cdot 6), 11 \cdot 6 + 2 \cdot 12 + 30 + 42$
727	$3 \cdot 6, 3 \cdot 6 + 18$

3. **Automorphisms of Systems of Order** $p < 1000$. For primes p with $7 < p < 1000$, it was shown from the computer output that the system of order p has no automorphisms but the prescribed ones, so that the automorphism group has order $p(p - 1)/2$. Subsequently, a general proof was found, depending on some published results, and this is presented in Sections 7–9. The reader may proceed directly to this, if he wishes. However, it still seems worthwhile to describe how the result was obtained for $p < 1000$ by computation.

Consider an automorphism σ which takes 0 and 1 into 0 and 1 in either order. As described below, I checked that σ leaves the longest cycle fixed, that is, leaves each element of the cycle fixed. (For $p = 307$, there are two cycles of maximum length, and both were found to be fixed.) It then follows that σ leaves 0 and 1 fixed, so that the automorphism group is not doubly transitive. The set of fixed points of σ forms a subsystem including the key triple and a major class, the class of linked cycles containing the longest cycle. It follows that σ is the identity, hence the order of the automorphism group is $p(p - 1)/2$.

If σ takes $\{0, 1\}$ into $\{0, 1\}$, then it must take each cycle into some cycle of the same length. If there is no other cycle of the same length as a given cycle, then the given cycle must be mapped onto itself. This mapping, if not the identity, must be either a rotation or a reflection.

What I did was to mark the elements of the longest cycle which are cross-linked to other elements of the same cycle. In most cases, the pattern of marked elements was found not to have symmetry under either rotation or reflection. For example, when $p = 43$, the key triple is $(0, 1, 7)$, and the longest cycle is

$$(4, 28, 11, *34, 18, 21, 10, *27, *17, 33, 24, 39, 9, 20, *16, 26),$$

where the elements linked to others in the same cycle are starred. Indeed, $(7, 17, 34)$ and $(7, 16, 27)$ are triples. The pattern has no symmetry. Hence σ must keep the cycle fixed. In the case $p = 307$, both maximum cycles lack symmetry, and they also have different self-linkage patterns from each other, so both are fixed.

The only values of p with $7 < p < 1000$ for which there is any symmetry are 19, 31, 439, 463, 547, 907. The operation preserving the pattern is reflection for $p = 19, 31, 439, 547$, and a half-turn (rotation through half the length of the cycle) for $p = 463, 907$. However, except for $p = 19$, there are cases where pairs of symmetric elements are cross-linked to cycles of different lengths, so σ must keep the longest cycle fixed.

Only for $p = 19$ is a more elaborate argument needed. Here the key triple is $(0, 1, 8)$, and the linkage consists of the two cycles

$$(2, *5, 14, *16, 10, 6, *3, 17, 15, *9), \qquad (4, 13, 12, 11, 7, 18).$$

Here 3 and 5 are cross-linked, and 9 and 16 are cross-linked. The pattern is symmetric to the diameter joining 3 and 5. Multiplying the key triple $(0, 1, 8)$ by 16 yields $(0, 16, 14)$. Adding constants to both triples yields $(13, 14, 2)$ and $(15, 12, 10)$. But 2 and 14 are interchanged in the reflection, as are 10 and 15. Hence 12 and 13 must be fixed, so the short cycle is fixed. This holds the unstarred elements of the long cycle fixed, and prevents the reflection.

4. Subsystems of Systems of Order $p < 1000$. We shall show that none of the systems of prime order $p < 1000$ have any proper subsystems of order greater than 3. It is sufficient to consider subsystems containing 0 and 1. Such a subsystem will consist of the key triple and a certain number of minor classes, as given in Table 2. We might exclude the existence of subsystems by computing additional triples, but instead we shall attempt to do so using only the information in Table 2, which is based solely on triples containing $0, 1$, or $\omega + 1$.

Suppose that there are subsystems of order k, where $3 < k < p$. We will then have a design with these subsystems as blocks. Indeed, if there are λ such subsystems containing 0 and 1, then there will be λ subsystems containing any pair of elements. In other words, each pair of elements is contained in just λ blocks. In the usual notations for designs, we have a design with $v = p$ and the values of k and λ as above. If b is the total number of blocks, and r the number of blocks in which each element occurs, then simple counting gives

$$bk = pr, \qquad r(k - 1) = \lambda(p - 1).$$

Compare Hall [5, p. 101]. (The use of r here is different than elsewhere in this paper.) Since $p \equiv 3 \pmod 4$, the second equation shows that we cannot have $k \equiv 1$ (mod 4) and λ odd. Also, the first equation yields $k | r$, hence we have $k(k - 1) | \lambda(p - 1)$. If $p < 1000$, we cannot have $k \geqslant 33$ and $\lambda = 1$.

Let C_j denote the class of primes for which the only minor classes are j sets of three cross-linked cycles of length 6. These correspond to the various lines in Table 2a. For primes of class C_0, all cycles are linked, hence there is certainly no subsystem. For primes of class C_1, the only possibility is $k = 21$ and $\lambda = 1$, and this is excluded by the preceding paragraph. For the classes C_2 or C_3, we might have

$$k = 21, \quad \lambda = 1, 2, 3; \qquad k = 39, \quad \lambda = 1, 2, 3; \qquad k = 57, \quad \lambda = 1.$$

We cannot have $k = 39$ and $\lambda > 1$, since two subsystems of order 39 containing 0 and 1 would have to intersect in a system of order 21, which is impossible since $21 > 39/2$. The cases $k = 39, 57$ and $\lambda = 1$ are excluded since $k \geqslant 33$. Finally, the cases $k = 21$ and $\lambda = 1, 3$ are excluded since $k \equiv 1 \pmod 4$. So we are left with the case $k = 21, \lambda = 2$. Here we must have $21 \cdot 20 | 2(p - 1)$, hence $p \equiv 1$ (mod 210). With $p \equiv 7 \pmod{12}$, this yields $p \equiv 211 \pmod{420}$, hence $p = 211, 631$. But 211 is of class C_0, so only 631 remains. This will be reserved for later consideration.

Now look at the four primes in Table 2b. For $p = 79$, we would have $k = 25$ and $\lambda = 1$, which is excluded since $k \equiv 1 \pmod 4$. In the cases $p = 367, 607, 727$, no subsystem can be formed using only the sets of three linked cycles of length 6, for the same reasons as above. A subsystem formed using the remaining class of linked cycles, with or without some of these sets, is impossible since $k \geqslant 33$ and $\lambda = 1$.

Thus on the basis of Table 2, we were able to show that there could be no subsystems, except possibly for $p = 631$. A design with $k = 21$ and $\lambda = 2$ is not excluded by the basic equations used. We would have $r = 63$ and $b = 1893$. I do not know whether such a design exists or not. In any case, we can exclude the existence of a subsystem for $p = 631$ by computing an additional triple. The key triple is $(0, 1, 44)$, and three of the linked cycles of length 6 are given by the computer output as

$$(7, 330, 367, 625, 324, 374), \quad (8, 352, 301, 308, 51, 331),$$

$$(37, 302, 309, 345, 624, 323).$$

These do not form a subsystem of order 21, since, for example, (323, 330, 22) is a triple determined by two of its elements and containing a new element. Thus we cannot have $\lambda = 2$, and hence there is no subsystem.

5. The System of Order 343.

There is only one admissible value of $q < 1000$ which is not prime, namely $q = 343$. The required field is obtained by adjoining to the 7-element field a root θ of an irreducible cubic. We may assume that $\theta^3 = 2$. The field elements then have the form $a\theta^2 + b\theta + c$, with the coefficients taken mod 7. If we identify this element with the point having coordinates $x = a$, $y = b$, $z = c$, then the field is a 3-dimensional affine space over the 7-element field. As noted in Section 1, the elements of a triple are collinear. Thus each of the $(343 \cdot 342)/(7 \cdot 6) = 2793$ lines of the space is a triple system of order 7, and each of the $(343 \cdot 342 \cdot 336)/(49 \cdot 48 \cdot 42) = 399$ planes of the space is a triple system of order 49.

In the computer program, we took $\omega = 2$. The key triple is (0, 1, 3), and there is a cycle of length 4, namely (2, 6, 5, 4). Together, these form a triple system of order 7 consisting of the seven integers, which form the line $x = 0, y = 0$. From Table 2b, we see that all of the other cycles fall into eight classes each having 42 elements. With the key triple and the cycle of length 4, these will form the eight planes through the line $x = 0, y = 0$. Any subsystem containing 0 and 1 includes the key triple. If there are more than 3 elements, then it must also include the cycle of length 4, since otherwise its intersection with a suitable plane would consist of 45 points in the plane. Since any subsystem with more than 3 elements containing 0 and 1 includes the complete line through 0 and 1, it follows that any subsystem with more than 3 elements contains the complete line through any two of its points, and is therefore a linear subspace, with 7 or 49 elements, unless it is the whole space. These subsystems will be studied in Section 6.

There is a field automorphism which takes θ into 2θ. Using it permutes the elements $a\theta^2 + b\theta + c$, $4a\theta^2 + 2b\theta + c$, $2a\theta^2 + 4b\theta + c$ cyclically. The key triple and the 4-term cycle are fixed. Examination of the computer output shows that, except for the two 12-term cycles, all cycles are permuted cyclically in sets of three. The automorphism moves each of the 12-term cycles 4 spaces, that is, one-third of a turn.

If we mark the elements of the longest cycles, the three cycles of length 30, which are cross-linked to other elements of the same cycle, we must obtain the same pattern in all three cases. Examination of the computer output shows that this pattern has no symmetry under rotation or reflection. Hence any automorphism which takes {0, 1} into itself and takes one of these cycles into itself must leave the cycle fixed and hence also leave 0 and 1 fixed. But every automorphism which takes {0, 1} into itself is the product of a field automorphism and one of these automorphisms, and hence leaves 0 and 1 fixed. Thus we cannot interchange 0 and 1, and hence can never interchange a pair of elements. The automorphism group is not doubly transitive.

Now consider an automorphsim σ which leaves 0, 1, and a cycle of length 30 fixed. Then σ^2 must leave all three cycles of length 30 fixed. Since there is no proper subsystem of order greater than 49, every point must be fixed, and σ^2 is the identity. But σ cannot interchange two elements, hence σ is also the identity. Thus the only automorphisms which take $\{0, 1\}$ into itself are the field automorphisms. Together with the linear automorphisms prescribed in Section 1, they generate the entire automorphism group, which therefore has order $rq(q - 1)/2 = 3 \cdot 343 \cdot 171 = 175959$.

6. Subsystems of the System of Order 343. It was shown in Section 5 that the only proper subsystems of order greater than 3 are the linear subspaces, which form systems of orders 7 and 49. We want to study the properties of these subsystems.

We have already noted that the line $x = 0$, $y = 0$ is made up of the key triple and a cycle of length 4, and that the rest of each of the planes through this line is made up of a class of linked cycles. Examination of the computer output shows that the type is $3 \cdot 6 + 2 \cdot 12$ for the plane $x = 0$, $3 \cdot 14$ for the plane $y = 0$, $4 \cdot 6 + 18$ for the planes $y = 3x$, $y = 5x$, $y = 6x$, and $2 \cdot 6 + 30$ for the planes $y = x$, $y = 2x$, $y = 4x$. The field automorphisms take the first two planes into themselves, and permute each of the sets of three planes cyclically.

Putting $P = (x, y, z) = x\theta^2 + y\theta + z$, we see that the automorphisms $P^\sigma = \alpha P + \beta$ with $\alpha = 1, 2, 4$ and $\beta = 0, 1, 2, 3, 4, 5, 6$ take the line $x = 0, y = 0$ into itself, and also take each plane through this line into itself. We can take $\{0, 1\}$ into any pair of integers, that is, into any pair of points on the line $x = 0, y = 0$. These automorphisms will convert the linkage between 0 and 1 into the linkage of an arbitrary pair of integers. The cycles in each plane through $x = 0, y = 0$ will be converted into cycles in the same plane. Thus the cycle structure of each plane through the line $x = 0, y = 0$ will be the same, no matter what pair of integers are linked.

Since any line can be taken into any other line, we see that the eight planes through any line will also have these four types of cycle structure with frequencies 1, 1, 3, 3. The linkage type of each plane will be the same, no matter what pair of points on the line are linked.

Any two subsystems of order 7 are of course isomorphic, and indeed, we can take any one into any other by means of an automorphism of the system of order 343. We shall now prove a similar result for the subsystems of order 49. In the first place, we can take two points in any given plane into 0 and 1, and hence take the plane into a plane through the line $x = 0, y = 0$. It will be sufficient to show that each of these planes can be taken into the plane $x = 0$. The seven other planes have the form $y = tx$ $(t = 0, 1, 2, 3, 4, 5, 6)$.

Now multiplication by $\pm(\theta - t)$ will be an automorphism, where the sign is chosen to make the factor a square. Since $\theta^3 = 2$, we have

$$(\theta - t)\,(a\theta^2 + b\theta + c) = (b - ta)\theta^2 + (c - tb)\theta + (2a - tc).$$

Thus the point $x = a, y = b, z = c$ goes into the point

$$x = \pm(b - ta), \qquad y = \pm(c - tb), \qquad z = \pm(2a - tc).$$

Hence the plane $y = tx$ is mapped onto the plane $x = 0$. In particular, the point $x = 0, y = 0, z = c$ is mapped onto the point $x = 0, y = \pm c, z = \mp tc$. Thus the line $x = 0, y = 0$ is mapped onto the line $x = 0, z = -ty$. As the various planes through the line $x = 0, y = 0$ go into the plane $x = 0$, the line goes into the various lines through the origin in the plane $x = 0$.

It follows that the cycle structure of the plane $x = 0$ with respect to the eight lines through the origin, and more generally the cycle structure of any plane with respect to the eight lines in the plane through any point, are of the four types with frequencies 1, 1, 3, 3. The cycle structure of the plane depends only on the line in which the linked points are chosen, and not on the choice of points within the line. Indeed, we see that this structure depends only on the direction of the line.

The 21 automorphisms $P^\sigma = \alpha P + \beta$ mentioned above take the line $x = 0$, $y = 0$ into itself. The three field automorphisms leave every point on the line fixed. Altogether, there are exactly 63 automorphisms of the space which take a line into itself, but they induce only 21 automorphisms of the line. This is a proper subgroup of the whole group of 168 automorphisms for a system of order 7.

In contrast to this, it will turn out that there are 441 automorphisms of the space which take a plane into itself, that they furnish 441 different automorphisms of the plane, and that these constitute the full automorphism group for the system of order 49 in the plane.

It will be convenient to consider the plane $y = 0$. All of the 63 automorphisms of the space which take the line $x = 0, y = 0$ into itself also take the plane $y = 0$ into itself. Any other automorphism of the space which takes the plane $y = 0$ into itself must take the line $x = 0, y = 0$ into another line with respect to which the plane is of type $3 \cdot 14$, that is, into a parallel line. Thus there are just $63 \cdot 7 = 441$ automorphisms of the space which are also automorphisms of the plane $y = 0$.

Are there any additional automorphisms of the plane? It is still true that the line $x = 0, y = 0$ must go into a parallel line. The 441 automorphisms above produce each possible image of $\{0, 1\}$ three times. The question whether there are any additional automorphisms reduces to whether there are any automorphisms other than the field automorphisms which take $\{0, 1\}$ into itself.

The part of the plane $y = 0$ not on the line $x = 0, y = 0$ consists of three cycles of length 14, which are permuted by the field automorphisms. It will be sufficient to show that no automorphism but the identity can take $\{0, 1\}$ into itself and one of these cycles into itself. The computer output shows that the linkage pattern of each cycle is

$$ABA * A * AA * B * BBB,$$

where the asterisk denotes an element cross-linked to another element of the same cycle, and the letters denote links to the other two cycles. The self-linkage alone would permit a reflection, but the linkage to the other two cycles shows that this is impossible. Thus if an automorphism takes a cycle into itself, the cycle must be fixed. The automorphism then has more than 7 fixed points, and is therefore the identity.

7. The Lengths of Cycles. The remaining sections are independent of Sections 3–6. In this section, we shall give some general results about the lengths of cycles. These will be used in Section 8 to determine the cycles of lengths 4 and 6.

Starting from the key triple $(0, 1, \omega + 1) = (0, 1, -\omega^2)$, we obtain the triple $(0, a, -\omega^2 a)$ when $\chi(a) = 1$. Subtracting 1 from each element of the key triple yields $(0, -1, \omega)$, hence $(0, a, -\omega a)$ is a triple when $\chi(a) = -1$.

Now suppose that $(a_0, b_0, a_1, b_1, \cdots, a_{l-1}, b_{l-1})$ is a cycle in the linkage of 0 and 1. Then

$$b_k = \begin{cases} -\omega^2 a_k & \text{if } \chi(a_k) = 1, \\ -\omega a_k & \text{if } \chi(a_k) = -1, \end{cases}$$

and

$$a_{k+1} - 1 = \begin{cases} -\omega^2(b_k - 1) & \text{if } \chi(b_k - 1) = 1, \\ -\omega(b_k - 1) & \text{if } \chi(b_k - 1) = -1. \end{cases}$$

It follows that

$$\chi(b_k) = -\chi(a_k), \qquad \chi(a_{k+1} - 1) = -\chi(b_k - 1).$$

Combining the functions expressing a_{k+1} in terms of b_k and b_k in terms of a_k, we find that the functions expressing a_{k+1} in terms of a_k are

$$(++)\ \ \omega x - \omega, \quad (+-)\ \ x - \omega^2, \quad (-+)\ \ x - \omega, \quad (--)\ \ \omega^2 x - \omega^2,$$

when the characters $\chi(a_k)$ and $\chi(b_k - 1)$ have the indicated signs.

Suppose that the character sequence

$$\chi(a_0),\ \chi(b_0 - 1),\ \chi(a_1),\ \chi(b_1 - 1), \cdots, \chi(a_{l-1}),\ \chi(b_{l-1} - 1)$$

is given. We see by induction that $a_k = \omega^{\lambda_k} a_0 + \mu_k \omega + \nu_k$, where λ_k, μ_k, ν_k are certain integers depending on the first $2k$ characters. In order to make $a_l = a_0$, we must choose a_0 so that

$$a_0 = \omega^{\lambda_l} a_0 + \mu_l \omega + \nu_l.$$

We shall call this the closing equation. If $\lambda_l \equiv 0 \pmod 3$, then the closing equation will hold for all values of a_0 or for no values of a_0. For other values of λ_l, the closing equation will hold for a unique value of a_0. Since $(1 - \omega)(1 - \omega^2) = 3$, we see that a_0 will have the form $(x\omega + y)/3$, where x and y are integers.

For a given character sequence, the closing equation is satisfied by no, one, or all values of a_0. In the first case, we say that the cycle is unclosable. In the remaining cases, we may speak of a special cycle or a general cycle belonging to the character sequence. In these cases, the cycle computed from the special a_0 or from a general a_0 using the given characters will close after $2l$ steps. However, there is no guarantee that the cycle thus computed will lead to the prescribed values of $\chi(a_k)$ and $\chi(b_k - 1)$.

If this is the case, then we will have $\chi(b_k) = -\chi(a_k)$, $\chi(a_{k+1} - 1) = -\chi(b_k - 1)$, and $\chi(a_0 - 1) = -\chi(b_{l-1} - 1)$. Hence all elements of the character matrix

$$\begin{pmatrix} \chi(a_0) & \chi(b_0) & \cdots & \chi(a_{l-1}) & \chi(b_{l-1}) \\ \chi(a_0 - 1) & \chi(b_0 - 1) & \cdots & \chi(a_{l-1} - 1) & \chi(b_{l-1} - 1) \end{pmatrix}$$

will have known values. Conversely, from the character matrix, we can write the character sequence for the cycle starting at any point. If we start from some b_k, then the cycle must be written in reverse order, so that the first two elements will occur in a triple with 0. For example, if we start at the last term, b_{l-1}, then the character sequence will be

$$\chi(b_{l-1}),\ \chi(a_{l-1} - 1), \cdots, \chi(b_1),\ \chi(a_1 - 1),\ \chi(b_0),\ \chi(a_0 - 1).$$

Every character sequence formed from the character matrix by starting at any point in the cycle will be obtained from the original sequence or from this sequence by rotating an even number of places. All of these will be considered equivalent. Thus all character sequences will fall into equivalence classes, which usually will have $2l$ elements. It will be sufficient to examine one character sequence in each equivalence class.

A general restriction on possible character sequences may be noted. From the formulas for a_{k+1} in terms of a_k, we see that

$$\chi(a_{k+1}) = \chi(a_k - 1) \quad \text{if} \quad \chi(a_k) = \chi(b_k - 1).$$

Applying this equation to the character sequence for the cycle taken in reverse order, we find that

$$\chi(b_{k-1}) = \chi(b_k - 1) \quad \text{if} \quad \chi(b_k) = \chi(a_k - 1).$$

Using the fact that $\chi(a_k - 1) = -\chi(b_{k-1} - 1)$, $\chi(b_{k-1}) = -\chi(a_{k-1})$, and $\chi(b_k) = -\chi(a_k)$, these two equations yield

$$\chi(a_{k+1}) = -\chi(b_{k-1} - 1) \quad \text{if} \quad \chi(a_k) = \chi(b_k - 1),$$

$$\chi(a_{k-1}) = -\chi(b_k - 1) \quad \text{if} \quad \chi(a_k) = \chi(b_{k-1} - 1).$$

Thus if any two terms of the character sequence are equal, then the terms on either side of them are not equal to each other.

8. **Cycles of Lengths 4 and 6.** We shall now apply the method of Section 7 for small values of l. The case $l = 1$ (cycles of length 2) is of course impossible, but it is instructive to examine what the general method leads to in this case. The closing equation cannot be satisfied in the cases of the character sequences $(+-)$ and $(-+)$. The remaining cases, $(++)$ and $(--)$, are equivalent. In the case $(++)$, we find $a_0 = (-\omega + 1)/3$ and $b_0 = (\omega + 2)/3$. Hence $b_0 - 1 = -a_0$, so $\chi(b_0 - 1) = -\chi(a_0)$, contrary to hypothesis.

Now look at the case $l = 2$ (cycles of length 4). The 16 possible functions expressing a_2 in terms of a_0 are given in the following table.

		$(++)$	$(+-)$	$(-+)$	$(--)$
		$\omega x - \omega$	$x - \omega^2$	$x - \omega$	$\omega^2 x - \omega^2$
$(++)$	$\omega x - \omega$	$\omega^2 x + 1$	$\omega x + 1$	$\omega x - 2\omega$	$x + \omega$
$(+-)$	$x - \omega^2$	$\omega x + \omega^2$	$x - 2\omega^2$	$x + 1$	$\omega^2 x + 1$
$(-+)$	$x - \omega$	$\omega x + 1$	$x + 1$	$x - 2\omega$	$\omega^2 x + \omega$
$(--)$	$\omega^2 x - \omega^2$	$x + \omega^2$	$\omega^2 x - 2\omega^2$	$\omega^2 x + 1$	$\omega x + 1$

The functions at the left express a_1 in terms of a_0, while those at the top express a_2 in terms of a_1. The corresponding characters are given in each case. Each composite function, obtained by first applying the function at the left and then the one at the top, expresses a_2 in terms of a_0.

We see that in 6 of the 16 cases, the closing equation is impossible, and that in each of the other 10 cases, it has a unique solution. Thus we have 6 unclosable cycles and 10 special cycles. However, the two special cycles corresponding to entries on the main diagonal are in fact impossible, because the first and last halves of the character sequence are alike, so we would have $a_1 = a_0$. We are left with the 8 entries on neither diagonal, which give rise to special cycles. These cases fall into two equivalence classes, which may be computed using character matrices. Representative character sequences for the two classes are $(+++-)$ and $(-+++)$. In both cases, the starting value a_0 must be a solution of the equation $x = \omega x + 1$, hence $a_0 = (\omega + 2)/3$.

As noted in Section 1, we may assume that ω was chosen so that $\chi(\omega - 1) = 1$, hence also $\chi(\omega + 2) = 1$. With this choice of ω, we see that $\chi(a_0) = -1$, so that only the sequence $(-+++)$ can be used. For this sequence, we find that

$$a_0 = \frac{\omega + 2}{3}, \quad b_0 = \frac{-\omega + 1}{3}, \quad a_1 = \frac{-2\omega + 2}{3}, \quad b_1 = \frac{2\omega + 4}{3}.$$

Hence $\chi(b_0 - 1) = 1$ and $\chi(b_1 - 1) = 1$, where in the latter case we use the fact that $(\omega - 1)(2\omega + 1) = 3\omega^2$. Finally, $\chi(a_1) = \chi(2)$, so that all the conditions will be satisfied if $\chi(2) = 1$. Thus there is a unique cycle of length 4 when $\chi(2) = 1$, that is, when $q \equiv 7 \pmod{24}$, but there is no such cycle when $\chi(2) = -1$, that is, when $q \equiv 19 \pmod{24}$. Thus the behaviour observed in the computer output for $q < 1000$ has been verified in general.

We now turn to the case $l = 3$ (cycles of length 6). Here we must leave most of the computation to the reader. The first step is to form a table similar to that used for $l = 2$, but now having 16 rows and 4 columns. The arguments at the left are the entries in the body of the previous table, with the appropriate character sequences, and the arguments at the top are as before. When the table is filled in, we find 8 positions with the entry x, which lead to general cycles, 14 positions with entries of the form $x + c$, where $c \neq 0$, which yield unclosable cycles, and 42 other cases, which give special cycles. The last 42 positions fall into 7 equivalence classes, which may be found using character matrices. When the special cycles are computed in 7 representative cases, all are found to contain elements of the key triple. Thus none of the special cycles are in fact possible.

Two equivalent general cycles correspond to character sequences $(++++++)$ and $(------)$. They are impossible, since they contradict the restriction found at the end of Section 7. The remaining six general cycles are equivalent to each other. We select the character sequence $(+++---)$ to use. Starting with an arbitrary element a, we obtain the cycle

$$a_0 = a, \quad b_0 = -\omega^2 a, \quad a_1 = \omega a - \omega, \quad b_1 = -a + 1,$$

$$a_2 = \omega a + 1, \quad b_2 = -\omega^2 a - \omega.$$

It is easily seen that all of the characters will have the prescribed values if and only if

$$\chi(a) = 1, \quad \chi(a - 1) = 1, \quad \chi(a + \omega) = -1, \quad \chi(a + \omega^2) = -1.$$

Thus all cycles of length 6 are obtained by starting with values of a satisfying these conditions. The chance that an arbitrary value of a will satisfy the conditions appears to be nearly $1/16$, which gives an estimate $q/16$ for the number of cycles of length 6. This is in good agreement with the actual number as given in Table 1.

9. Subsystems of Orders 7 and 9. A subsystem of order 7 containing 0 and 1 must consist of the key triple and a cycle of length 4. Furthermore, the opposite elements of the cycle must clearly be cross-linked. There is no cycle of length 4 unless $p \equiv 7 \pmod{24}$, and in that case there is a unique cycle, which was determined in Section 8. For this cycle, $b_0 = (-\omega + 1)/3$ and $b_1 = b_0 + \omega + 1$. Hence adding b_0 to the key triple $(0, 1, \omega + 1)$ yields the triple $(b_0, b_0 + 1, b_1)$. Thus b_0 and b_1 are cross-linked only if $b_0 + 1 = \omega + 1$, or $b_0 = \omega$. Using the value of b_0, the last equation reduces to $4\omega = 1$. Cubing yields $64 = 1$ and hence $p = 7$. Hence there can be no subsystem of order 7 unless $q = 7^r$.

A subsystem of order 9 containing 0 and 1 must consist of the key triple and a cycle of length 6. The only triple system of order 9 is the affine plane over the 3-element field. Hence, as noted in Section 2, each element of the cycle must be cross-linked to the opposite element. We determined the most general cycle of length 6 in Section 8. It will be sufficient to recall two things: The element opposite to the starting element a is $-a+1$, and a was subject to various conditions, including $\chi(a+\omega^2)=-1$. Subtracting 1 from the key triple gives $(-1,0,\omega)$, multiplying by $-a-\omega^2$ yields $(a+\omega^2,0,-\omega a-1)$, and adding $\omega+1$ gives the triple $(a,\omega+1,-\omega a+\omega)$. Thus a is cross-linked to $-\omega a+\omega=\omega(-a+1)\neq -a+1$, and so the opposite elements, a and $-a+1$, are not cross-linked. Hence there can be no subsystem of order 9.

Now by Hall [4, Theorem 4.1], a triple system whose automorphism group is doubly transitive must have a subsystem of order 7 or 9. It follows that, for the systems considered here, the automorphism group cannot be doubly transitive, except possibly for $q=7^r$. (This use of Hall's theorem was suggested to me by William M. Kantor in a letter written in 1971.) For $q=7$, the group is in fact doubly transitive. On the other hand, we showed in Section 5 that the group is not doubly transitive for $q=7^3$. It seems unlikely that it is doubly transitive for any $q>7$.

Whenever the automorphism group is not doubly transitive, it follows from Kantor [7, Proposition 6.1], that is must be generated by the linear automorphisms prescribed in Section 1 and the field automorphisms, and hence has order $rq(q-1)/2$ if $q=p^r$. This result is thus proved for $q\neq 7^r$ and also for $q=7^3$.

Postscript (added August 1974). It can also be shown that the automorphism group is not doubly transitive when $q=7^r$ with $r>1$. The following proof is a simplified version of one suggested to me by Kantor after seeing the above manuscript. The system of order 7^r is based on an r-dimensional affine space over the 7-element field, and the only subsystems of order 7 are the lines. Hence any automorphism of the triple system takes lines into lines, and is also an automorphism of the affine geometry. But in an automorphism of the affine geometry, the mapping of a line is determined as soon as the images of two points are known. Hence any automorphism of the triple system which interchanges 0 and 1 must take each integer z into $1-z$. This leads to a contradiction, since the key triple (0, 1, 3) is not preserved.

One additional result particularly deserves mention. Using the computer, it was found that the plane sections of the system of order 7^5 furnish two types of subsystems of order 49. Of the 400 planes through a line, 360 are isomorphic to the plane sections of the system of order 343, which were studied in Section 6, and 40 are of a new type. The new type of plane contains a subsystem of order 21. This is the first example of a subsystem other than the obvious ones in any of our systems. It still seems likely that none of the systems of prime order p have any subsystems of order k with $3<k<p$. This was verified in Section 4 for $p<1000$, and the general proof for the crucial cases $k = 7$ and $k = 9$ given in Section 9 has now been extended to $k = 13$ and $k = 15$.

Department of Mathematics
University of California
Berkeley, California 94720

1. ROBERT D. CARMICHAEL, *Introduction to the Theory of Groups of Finite Order*, Ginn, Boston, 1937; reprinted, Dover, New York, 1956. MR 17, 823.

→ F. N. COLE, LOUISE D. CUMMINGS & H. S. WHITE, "The complete enumeration of triad systems in 15 elements," *Proc. Nat. Acad. Sci. U. S. A.*, v. 3, 1917, pp. 197–199.

3. P. DEMBOWSKI, *Finite Geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, Berlin and New York, 1968. MR 38 #1597.

4. MARSHALL HALL, JR., "Automorphisms of Steiner triple systems," *IBM J. Res. Develop.*, v. 4, 1960, pp. 460–472. MR 23 #A1282.

5. MARSHALL HALL, JR., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967. MR 37 #80.

→ MARSHALL HALL, JR. & J. D. SWIFT, "Determination of Steiner triple systems of order 15," *Math. Tables Aids Comput.*, v. 9, 1955, pp. 146–152. MR 18, 192.

7. WILLIAM M. KANTOR, "Automorphism groups of designs," *Math. Z.*, v. 109, 1969, pp. 246–252. MR 43 #71.

8. HEINZ LÜNEBURG, "Steinersche Tripelsysteme mit fahnentransitiver Kollineationsgruppe," *Math. Ann.*, v. 149, 1962/63, pp. 261–270. MR 26 #2933.

9. EUGEN NETTO, "Zur Theorie der Tripelsysteme," *Math. Ann.*, v. 42, 1893, pp. 143–152.

10. EUGEN NETTO, *Lehrbuch der Combinatorik*, 2nd ed., Teubner, Leipzig, 1927; reprinted, Chelsea, New York, 1958. MR 20 #1632.

11. M. REISS, "Ueber eine Steinersche combinatorische Aufgabe," *J. Reine Angew. Math.*, v. 56, 1859, pp. 326–344.

12. H. S. WHITE, F. N. COLE & LOUISE D. CUMMINGS, "Complete classification of the triad systems on fifteen elements," *Mem. Nat. Acad. Sci. U. S. A.*, v. 14, no. 2, 1919, 89 pp.