Can. J. Math., Vol. XXXI, No. 3, 1979, pp. 637–654

ON THE NUMBER OF CONJUGATES OF N-ARY QUASIGROUPS

MARY McLEISH

1. Introduction. Higher dimensional quasigroups (a set Q with a cancellative, n-ary operation $\langle\quad\rangle$, ([**2**]) have been studied by T. Evans ([**3**], [**4**]), A. Cruse [**1**], C. C. Lindner ([**10**], [**11**]) and also by many others under the guise of magic cubes, Graeco-latin cubes, etc. Conjugates or parastrophes have been discussed by S. K. Stein [**18**], A. Sade [**17**] and more recently by C. C. Lindner and D. Steedley in [**14**], where it is shown that ordinary quasigroups exist of every order $\geqq 4$ with a prescribed number of distinct conjugates. It is suggested that the problem be extended to n-ary quasigroups.

This paper is primarily concerned with ternary quasigroups (§ 3) and the problem is completely solved for 1, 3, 4, 6, 12 and 24 distinct conjugates as summarized in Theorem 3.6.1. The missing cases of 2 and 8 distinct conjugates are discussed in [**15**]. A partial explanation for the separation of these two cases is given in Conclusion 2.10. Although the methods used in this paper provide simple alternate constructions to those given in [**14**] for 3 and 6 distinct conjugates (see the remarks following Theorems 2.8 and 3.1.6), they do not apply to the case of 2 conjugacy classes for ordinary quasigroups or 2 and 8 conjugacy classes in the ternary case. For ordinary quasigroups, C. C. Lindner has successfully used a special variation of the singular direct product of quasigroups [**16**]. Unfortunately, it has been found by the author and further substantiated by B. Ganter [**5**] that this product does not extend naturally to three dimensions. In [**15**], several infinite classes of orders of 3-quasigroups with 2 or 8 distinct conjugates have been found, however, using block designs.

In § 2, some results for general n-ary quasigroups are given. The examples chosen are those which also apply to the case $n = 3$, although a couple of additional examples are given to indicate further possibilities. The main results are given in Conclusion 2.10.

As additional results that arose as a result of the conjugacy problem, the generalized idempotent law and generalized idempotent, commutative, non-Steiner 3-quasigroups are discussed in Lemma 3.2.3 and Theorem 3.4.4 respectively. It should be noted that, in fact, the whole problem of conjugates is equivalent to finding the spectrum of certain sets of n-quasigroup identities.

Received December 15, 1977 and in revised form June 5, 1978. This paper consists of a part of the author's Ph.D. thesis, McMaster University, 1977, written under the supervision of Professor Alexander Rosa. The preparation of the paper while at the University of Alberta was supported by the NRC Grant of Professor A. Meir.

2. N-ary quasigroups.

Definition 2.1. Let $(Q, \langle\ \rangle)$ be an n-ary quasigroup where $\langle a_1, a_2, \ldots, a_n\rangle = a_{n+1}$ (or d), $a_i, d \in Q$, $i = 1, 2, \ldots, n + 1$. Let π be any member of S_{n+1}. Then the *conjugate* n-ary quasigroup $(Q, \langle\ \rangle_\pi)$ is defined by $\langle a_1, a_2, \ldots, a_n\rangle = a_{n+1}$ if and only if $\langle a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle_\pi = a_{\pi(n+1)}$.

$|C(Q, \langle\ \rangle)|$ is called the *conjugacy class number of* $(Q, \langle\ \rangle)$.

THEOREM 2.2. $|C(Q, \langle\ \rangle)|$ *divides* $(n + 1)!$

Proof. Let $S = \{\pi(\langle\ \rangle) = \langle\ \rangle_\pi | \pi \in S_{n+1}\}$ where $\langle\ \rangle$ is a fixed member of the set E of all n-ary quasigroup operations on Q. Then $|S| = |C(Q, \langle\ \rangle)|$ and S forms a set of transitivity of E. The permutations of S_{n+1} which fix $\langle\ \rangle$ form a subgroup of S_{n+1} of index $|S|$ in S_{n+1}. (cf. [**6**]).

THEOREM 2.3. *There exists an* n-ary *quasigroup with exactly one conjugacy class for all orders* $m \geqq 1$.

Proof. Let $Q = \{0, \ldots, m - 1\}$ and define an n-ary operation $\langle\ \rangle$ on Q by $\langle a_1, \ldots, a_n\rangle = -(a_1 + a_2 + \ldots + a_n) \equiv d = a_{n+1} \pmod m$ where a_i, $i = 1, \ldots, n + 1 \in Q$ and $d \in Q$. Then $(Q, \langle\ \rangle)$ is an n-ary quasigroup. Clearly $\langle\ \rangle_\pi = \langle\ \rangle$, if $\pi(n + 1) = n + 1$, where $\pi \in S_{n+1}$. However if we consider some permutation π where $\pi(n + 1) \neq n + 1$ and π acts on $\{1, \ldots, n + 1\}$, then $\langle a_{\pi(1)}, \ldots, a_{\pi(j-1)}, d, a_{\pi(j+1)}, \ldots, a_{\pi(n)}\rangle = -(a_{\pi(1)} + a_{\pi(2)} + \ldots + a_{\pi(j-1)} - (a_1 + a_2 + \ldots + a_n) + a_{\pi(j+1)} + \ldots + \pi(a_n)) = a_{\pi(j)}$.

LEMMA 2.4. *If* $\phi(n)$ *is the Euler function, then* $\phi(n) \geqq \sqrt{n}$, *except when* $n = 2$ *or* 6.

Proof. This follows from $\phi(n) = \prod_{p^\alpha/n} p^{\alpha-1}(p - 1)$. [**7**].

THEOREM 2.5. *If* $m > 4(n - 1)^2$ *then there exists an* n-ary *quasigroup of order* m *with* $(n + 1)!$ *conjugacy classes.*

Proof. Let $(Q, \langle\ ,\ ,\ \rangle)$ be an n-ary quasigroup of order m with $Q = \{0, 1, \ldots, m - 1\}$; where $\langle a_1, a_2, \ldots, a_n\rangle = d \equiv a_1 + a_2p_2 + \ldots + a_np_n \pmod m$; where all the p_i are relatively prime to m; and where $p_i + p_j \not\equiv 0 \pmod m$, $(i \neq j)$, $p_i \neq p_j$, and $p_i \neq n - 1$, $\forall\ i$. Then $(Q, \langle\ \rangle)$ has $(n + 1)!$ conjugacy classes.

To show this consider the following cases:

(1) Clearly any single transposition π among the integers 1 to n will result, in some instance, in $\langle a_1, \ldots, a_n\rangle \neq \langle a_{\pi(1)}, \ldots, a_{\pi(n)}\rangle$.

(2) Consider any permutation of $\{1, 2, \ldots, n + 1\}$, which leaves $n + 1$ fixed. Then suppose $\pi = (i_1, j_1)\ (i_2, j_2) \ldots (i_{n-1}, j_{n-1})$, when written as a product of transpositions. Suppose that $i_1 \neq j_1$. Let $a_{i_1} \neq a_{j_1} \neq 0$ and the remaining a_{i_k}, a_{j_k} all be 0. Then we have a contradiction from case 1 again.

(3) Suppose $\pi(n + 1) = s$, $s \neq 1$ and $\pi(s) = n + 1$, where every other

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

element is left unchanged by π. Then we have $\langle a_1, \ldots, a_n\rangle = d$ and suppose

$$\langle a_1, \ldots, a_{s-1}, d, a_{s+1}, \ldots, a_n\rangle \equiv a_1 + \sum_{\substack{i\neq s\\ i\geq 2}}^{n} p_i a_i + p_s\left(a_1 + \sum_{2}^{n} a_i p_i\right) = a_s.$$

If $a_i = 0, \forall\, i, i \neq s$, then $p_s^2 a_s \equiv a_s$ implies $p_s^2 \equiv 1 \pmod m$. But then

$$a_1(1 + p_s) + \textstyle\sum_{i=2}^n a_i(1 + p_s) \equiv 0 \pmod m.$$

If $a_i = 0\ \forall\, i \geqq 2$, then $1 + p_s$ must be $0 \pmod m$, which is false.

(4) Suppose $\pi(n + 1) = 1$ and $\pi(1) = n + 1$, and every other element is left fixed by π. Suppose $\langle a_1, \ldots, a_n\rangle = d$, $\langle d, a_2, \ldots, a_n\rangle = a_1$. Then $(a_1 + \sum_2^n p_i a_i) + \sum_2^n p_i a_i = a_1$ and $2\sum_2^n a_i p_i \equiv 0 \pmod m$. Letting $a_2 = 1$ and all other $a_i = 0$, one obtains $2p_2 \equiv 0 \pmod m$, a contradiction.

(5) Suppose $n + 1$ and 1 are interchanged under π and the remaining a_i are permuted by at least one transposition. Then $\langle a_1, \ldots, a_n\rangle = d$ and $\langle d, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle = a_1$. Thus $a_1 + \sum_2^n p_i a_i + \sum_2^n p_i a_{\pi(i)} \equiv a_1 \pmod m$, where at least one $a_{\pi(i)} \neq a_i$. Suppose in fact $\pi(i) \neq i$ for some fixed i. Then there exists a j such that $\pi(j) = i$. Let $a_k = 0$ for all $k \neq 1$ or i. We have $(p_i + p_j) \equiv 0 \pmod m$, a contradiction.

(6) Suppose $n + 1$ and 2 (or any $i, i \neq 1$) are interchanged under π and the remaining elements are permuted by at least one transposition. Then $\langle a_1, \ldots, a_n\rangle = d$ and, say, $\langle a_{\pi(1)}, d, \ldots, a_{\pi(n)}\rangle = a_2$. Thus $a_{\pi(1)} + p_2(a_1 + \sum_2^n a_i p_i) + \sum_3^n a_{\pi(i)} p_i \equiv a_2 \pmod m$. From this, we may conclude that $p_2^2 \equiv 1 \pmod m$, and $a_1(p_2 + p_s) + a_{\pi(1)}(1 + p_2 p_{\pi(1)}) + \sum_3^n a_{\pi(i)}(p_2 p_{\pi(i)} + p_i) \equiv 0 \pmod m$, where $\pi(s) = 1$ for some $s \neq 1$. Choose $a_i = 0$, $\forall\, a_i$ except a_1 and a_2; let $a_1 = 1$. Then $p_2 + p_s \equiv 0 \pmod m$, a contradiction. If, however, $\pi(1) = 1$, $a_1(1 + p_2) + \sum_3^n a_{\pi(i)}(p_2 p_{\pi(i)} + p_i) \equiv 0 \pmod m$. If all $a_i \equiv 0$, $i \geqq 3$, then $1 + p_2 \equiv 0$, a contradiction.

(7) Suppose $a_{\pi(1)} = d$, but $\pi(n + 1) \neq 1$. Say $\langle a_1, \ldots, a_n\rangle = d$, but $\langle d, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle = a_{\pi(n+1)}$, where $a_{\pi(n+1)} \neq a_1$. Then $a_1 + \sum_2^n a_i p_i + \sum_2^n a_{\pi(i)} p_i = a_{\pi(n+1)}$. If $a_1 = 1$ and all the other $a_i = 0$, then $a_1(1 + p_{\pi(j)}) \equiv 0 \pmod m$, where $\pi(j) = 1$, and this is impossible.

(8) Finally, suppose $\pi(i) = n + 1$ for some $i \neq 1$ (without loss of generality, we may take $i = 2$) and $\pi(n + 1) \neq 2$. Then we make the following three considerations:

Suppose $\pi(n + 1) = 1$. Then $\langle a_1 \ldots a_n\rangle = d$ and $\langle a_{\pi(1)}, d, \ldots, a_{\pi(n)}\rangle = a_1$ or $a_{\pi(1)} + p_2 a_1 + p_2 \sum_2^n a_i p_i + \sum_3^n a_{\pi(i)} p_i \equiv a_1 \pmod m$. But this implies $p_2 = 1$, a contradiction.

Suppose $\pi(1) = 1$. Then

$$a_1 + (a_1 + \textstyle\sum_2^n a_i p_i) p_2 + \sum_3^n a_{\pi(i)} p_i) \equiv a_{\pi(n+1)} \pmod m,$$

which implies $1 + p_2 \equiv 0 \pmod m$, a contradiction.

Suppose $\pi(j) = 1$, $j \neq 1$. Then

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

$$a_{\pi(1)} + p_2\left(a_1 + \sum^n a_i p_i\right) + p_j a_i + \sum_{\substack{i=3\\ i\neq j}}^{n} a_{\pi(i)} p_i \equiv a_{\pi(n+1)}.$$

But this leads to $p_2 + p_j \equiv 0 \pmod{m}$, a contradiction.

(9) To complete the proof of the theorem, we need only show that one can choose $n - 1$ numbers p_i, which are relatively prime to m and not pairwise summable to m or equal to $m - 1$. Now if each p_i is less than $m/2$ and is relatively prime to m, this will be the case. Thus if we can make $\phi(m)/2 > n - 1$, $n - 1$ such numbers can be found. By Lemma 2.4, this will be the case if $\sqrt{m}/2 > n - 1$, which is true if $m > 4(n - 1)^2$.

THEOREM 2.6. *There exists an integer $m_j(n)$ such that for every order $m \geqq m_j(n)$ there exists an n-ary quasigroup of order m with $(n + 1)!/j!$ conjugacy classes, $j = 1, \ldots, n$.*

Proof. (1) We have just seen the case $j = 1$. Consider every case other than $j = 1$ or n. Define $(Q, \langle\ \ \rangle)$, where $Q = \{0, 1, \ldots, m - 1\}$ by $\langle a_1, \ldots, a_n\rangle = a_1 + a_2 + \ldots + a_j + p_{j+1}a_{j+1} + \ldots + p_n a_n$ where addition is taken $\pmod{m}$. Here $p_{j+1}, \ldots, p_n$ are integers relatively prime to m, are not pairwise summable to m, and are all different from $m - 1$ or 1. Then every permutation π on $\{1, \ldots, n + 1\}$, which fixes the elements $1, \ldots, j$, $j < n$, will leave the product $\langle a_{\pi(1)}, \ldots, a_{\pi(n)}\rangle$ unchanged and thus not introduce a new conjugacy class. We must show that any other type of permutation π on $\{1, \ldots, n + 1\}$ results in $\langle a_{\pi(1)}, \ldots, a_{\pi(n)}\rangle \neq a_{\pi(n+1)}$.

Consider the case where π fixes $n + 1$ and $a_{\pi(i)} = a_l$ for some $i > j$ and $l \leqq j$. Then we have $\sum_1^j a_{\pi(i)} + \sum_{j+1}^n p_i a_{\pi(i)} = \sum_{j+1}^n p_i a_i + \sum_1^j a_i$. Let $a_l = 1$ and the rest of the a_i be $= 0$. Then $p_i = 1$. Suppose $\pi(i) = \pi(l)$, where $i, l > j$. Let $a_l = 1$ and the remaining a_i's all be zero. Then $p_i a_l \equiv p_l a_l$ implies $p_i = p_l$, a contradiction.

If $a_{\pi(i)} = d$ and $a_{\pi(n+1)} = a_i$ for any $i \leqq j$, and π fixes all the other i, we have:

$$a_1 + a_2 + \ldots + a_{i-1} + \left(\textstyle\sum_1^j a_i + \sum_{j+1}^n p_i a_i\right) + a_{i+1} + \ldots + a_j + \textstyle\sum_{j+1}^n p_i a_i \equiv a_i.$$

If all $a_k = 0$ except $a_{j+1} = 1$, we have $2p_{j+2} \equiv 0 \pmod{m}$ a contradiction.

If $a_{\pi(n+1)} = a_i$ and $a_{\pi(i)} = d$, where $i > j$, and π fixes every other element, we obtain a contradiction similar to that in (3) of Theorem 2.5.

If $a_{\pi(n+1)} = a_i$, $i \leqq j$, $a_{\pi(i)} = d$, we obtain a contradiction similar to Theorem 2.5(5).

If $a_{\pi(n+1)} = a_j$ and $a_{\pi(j)} = d$, where $i > j$, we obtain a contradiction similar to Theorem 2.5(6).

Now if $a_{\pi(i)} = d$, where $i \leqq j$, but $a_{\pi(n+1)} \neq a_i$, we obtain: $\langle a_{\pi(1)}, \ldots, d, \ldots, a_{\pi(n)}\rangle = a_{\pi(n+1)}$, and so $a_{\pi(1)} + \ldots + a_{\pi(i-1)} + \left(\sum_1^j a_i + \sum_{j+1}^n p_i a_i\right) + a_{\pi(i+1)} + \ldots + a_{\pi(j)} + \sum_{j+1}^n p_i a_{\pi(i)} = a_{\pi(n+1)}$. If $a_{\pi(n+1)} = a_k$, where $k \leqq j$, let all the a_i's be zero except one a_t and possibly a_k, where $t \leqq j$, $t \neq i$. Then either

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

$a_t(l + p_s) \equiv 0 \pmod{m}$ for some s or $2a_t \equiv 0 \pmod{m}$; in either case we get a contradiction for $m > 2$.

If $a_{\pi(n+1)} \neq a_i$, $i > j$, but $a_{\pi(i)} = d$, then

$$\sum_1^j a_{\pi(i)} + p_i\left(\sum_1^j a_i + \sum_{j+1}^n p_i a_i\right) + \sum_{\substack{s=j+1\\ s\neq i}} p_s a_{\pi(s)} \equiv a_{\pi(n+1)},$$

if $\langle\ \ \rangle_\pi = \langle\ \ \rangle$. Then if $a_l \neq 0$, $\forall\, l$ except k, where $a_k = a_{\pi(n+1)}$, we obtain either $p_k{}^2 a_k \equiv a_k \pmod{m}$ or $p_i a_k \equiv a_k \pmod{m}$. The latter case is impossible and in the former, we cancel $p_k{}^2 a_k$ and a_k from the equation. In the resulting equation, let $a_1 = 1$ and the remaining a_l's be all zero. Then if $1 = \pi(k)$, where $k \leqq j$, $a_1 + p_i a_1 \equiv 0$ or $(1 + p_i) \equiv 0 \pmod{m}$. If $\pi(k) > j$, $p_i a_1 + p_k a_1 \equiv 0 \pmod{m}$ implies $(p_i + p_k) \equiv 0 \pmod{m}$. Both these are impossible, and so the theorem is proven for $j < n$.

(2) If $j = n$, we define $\langle a_1, \ldots, a_n\rangle = a_1 + a_2 + \ldots + a_n$. Clearly there are $n!$ members of one class. Consider the two following possibilities: $\langle d, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle = a_1$ or $\langle d, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle = a_{\pi(n+1)} \neq a_1$, say $a_{\pi(n+1)} = a_k$. In the first case $\sum_1^n a_i + \sum_2^n a_{\pi(i)} \equiv a_1$ and so $2(\sum_2^n a_i) \equiv 0$, a contradiction. In the second case, $\sum_1^n a_i + \sum_2^n a_{\pi(i)} \equiv a_k$, or

$$\left(\sum_{\substack{i=1\\ i\neq k}}^n a_i + \sum_{i=2}^n a_{\pi(i)}\right) \equiv 0$$

and hence

$$2\left(\sum_{\substack{i=1\\ i\neq k}}^n a_i\right) \equiv 0,$$

a contradiction. Therefore, there are exactly $n + 1$ classes.

(3) As in Theorem 2.5, Lemma 2.4 may be used to determine $m_{j(n)}$, depending on the number of relatively prime numbers required.

THEOREM 2.7. *If $m \geqq 3$, there exists an* n-ary *quasigroup* $(n > 3)$ *of order m with exactly $n(n + 1)/2$ conjugacy classes.*

Proof. Define $(Q, \langle\ \ \rangle)$, where $Q = \{0, 1, \ldots, m - 1\}$, by $\langle a_1, \ldots, a_n\rangle = d = -a_1 + a_2 + \ldots + a_n$ and addition is taken $(\text{mod}\, m)$, a_i, $i = 1, \ldots, n$, $d \in Q$. If π is any permutation on $\{1, 2, \ldots, n + 1\}$ which fixes 1 and $n + 1$, then $\langle a_{\pi(1)}, \ldots, a_{\pi(n)}\rangle = a_{\pi(n+1)}$. Therefore, the conjugate 3-quasigroup $(Q, \langle\ \ \rangle_\pi)$ defined by $\langle a_{\pi(1)}, \ldots, a_{\pi(n)}\rangle_\pi = a_{\pi(n+1)}$ if and only if $\langle a_1, \ldots, a_n\rangle = d = a_{n+1}$ is identical with $(Q, \langle\ \ \rangle)$. There are $(n + 1)!$ such permutations and therefore at least $(n - 1)!$ members of one conjugacy class.

Suppose π is a permutation on $\{1, 2, \ldots, n + 1\}$ such that $a_{\pi(1)} = d$ and $a_{\pi(n+1)} = a_1$. Then $\langle d, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle = a_1$ only if $-(-a_1 + \sum_2^n a_i) + \sum_2^n a_{\pi(i)} \equiv a_i \pmod{m}$. Therefore $(Q, \langle\ \ \rangle_\pi) = (Q, \langle\ \ \rangle)$. As there are another $(n - 1)!$ permutations of this type, there are at least $2(n - 1)!$ members of the conjugacy class identical with Q.

However, if $\langle a_1, d, a_{\pi(3)}, \ldots, a_{\pi(n)}\rangle = a_2$, that is $\pi(2) = n + 1, \pi(n + 1) = 2$, $\pi(1) = 1$, then $-a_1 - a_1 + \sum_2^n a_i + \sum_3^n a_{\pi(i)} \equiv a_2 \pmod m$. This becomes $-2a_i + 2\sum_3^n a_i \equiv 0 \pmod m$, a contradiction if $m \geqq 3$.

Consider the case where $\langle d, a_{\pi(2)}, \ldots, a_{\pi(n)}\rangle = a_{\pi(n+1)} = a_k$, $k \neq 1$. Then $a_1 - \sum_2^n a_i + \sum_2^n a_{\pi(i)} \equiv a_k \pmod m$ and $2(a_1 - a_k) \equiv 0 \pmod m$, again a contradiction.

If $\langle a_{\pi(1)}, d, a_{\pi(3)}, \ldots, a_{\pi(n)}\rangle = a_{\pi(n+1)} = a_k$, $k \neq 2$, then $-a_{\pi(1)} - a_1 + \sum_2^n a_i + \sum_3^n a_{\pi(i)} \equiv a_k \pmod m$. If $n = 3$, there is one case in which this is indeed true. Namely, if $\langle a_2, d, a_1\rangle = a_3$, $-a_2 - a_1 + a_2 + a_3 + a_1$ equals a_3. However, if $n > 3$ and $m(n) > 3$, then $-\pi(a_1) - a_1 + \sum_2^n a_i + \sum_3^n a_{\pi(i)} \equiv 0 \pmod m$, and there remains at least one variable, with a coefficient $\leqq 2$, that will not cancel out on the left hand side. Hence the congruence will not always be identically zero. Thus $(Q, \langle\ \rangle)$ has $(n + 1)!/2(n - 1)! = n(n + 1)/2$ conjugacy classes.

THEOREM 2.8. *If $m \geqq 3$ and $n \geqq 3$ is odd, there exists an n-ary quasigroup of order m with $(n + 1)!/2[(n + 1/2)!]^2$ conjugacy classes.*

(Letting $n = 2r - 1$, this becomes $(2r)!/2(r!)^2 = 1/2\,{}_rC_{2r}$.)

Proof. Define $\langle a_1, a_2, \ldots, a_n\rangle = a_{n+1} \equiv (a_1 - a_2 + a_3 + \ldots + a_n) \pmod m$ on $Q = \{0, 1, \ldots, m - 1\}$. Briefly, permutations of the following types only will result in $\langle\ \rangle_\pi = \langle\ \rangle$.

(1) Any permutation π of $\{1, 2, \ldots, n + 1\}$ such that $\pi(2t) = 2s$ and $\pi(2t' - 1) = 2s' - 1$ for any integers s, t, s', t'. That is, the even numbers are permuted among themselves only and similarly for the odd numbers. There are clearly $[(n + 1/2)!]^2$ such permutations.

(2) Any permutation π in which $\pi(n + 1) = t$, where t is odd and $\pi(2s - 1) = 2l$, $\pi(2s') = 2l' - 1$ for any integers s, l, s', l'. That is, π takes even numbers into odd ones and vice versa. There are another $[(n + 1/2)!]^2$ permutations of this type.

We note one last result which provides an alternate construction, in the case $n = 2$, for 3 conjugacy classes, to that given in [**14**], where embedding theorems are needed.

THEOREM 2.9. *If $m \geqq 3$ and n is even, there exists an n-ary quasigroup of order m with $(n + 1)!/((n + 2)/2)!(n/2)!$ conjugacy classes.*

(Letting $n = 2r$, this becomes $(2r + 1)!/(r + 1)!r! = {}_rC_{2r+1}$.)

Proof. Define $\langle a_1, a_2, \ldots, a_n\rangle = a_{n+1} \equiv (a_1 - a_2 + a_3 \ldots - a_n) \pmod m$ on $Q = \{0, 1, \ldots, m - 1\}$.

2.10. Conclusion to the n-ary case. We have found that for sufficiently large $m(n)$, there exists an n-ary quasigroup of order $m \geqq m(n)$ having each of the following number of conjugacy classes:

(1) $(n + 1)!/q!$, $q = 1, 2, \ldots, n + 1$,

(2) $n(n + 1)/2$,

(3) $(1/2)_r C_{2r}$ where $n = 2r - 1,\ r \geqq 2$ or
(4) $_r C_{2r+1}$ where $n = 2r$.

Clearly examples of n-ary quasigroups with other conjugacy class numbers can be found by variations of the techniques used here. However, if a permutation π containing a cycle $(a\ b\ c)$ must satisfy $\langle\ \ \rangle_\pi = \langle\ \ \rangle$ for some $(Q, \langle\ \ \rangle)$ and at the same time one requires $\langle\ \ \rangle_\alpha$, $\langle\ \ \rangle_\beta$ and $\langle\ \ \rangle_\gamma$ all to be different from $\langle\ \ \rangle$, where $\alpha = (a\ b)$, $\beta = (b\ c)$ and $\gamma = (a\ c)$, these algebraic methods are of no use. In the case of $n = 3$, some results were found using "weakened" Steiner quadruple systems [**15**]. However, the general question "Given integers m, n and c, where c divides $(n + 1)!$, does there exist a n-ary quasigroup of order m with c conjugacy classes", has still to be answered.

3. Ternary Quasigroups. The case of 1 conjugacy class is covered in Theorem 2.3 and 2 and 8 conjugacy classes are discussed in [**15**]. There remains then the cases of 3, 4, 6, 12 or 24 conjugacy classes.

As shown in [**14**] for ordinary quasigroups, each conjugate quasigroup is identical to the original quasigroup if and only if a certain identity is satisfied by the original quasigroup. The following list is given for future reference. Here $\langle , , \rangle = \langle , , \rangle_{\pi_i}$, $\pi_i \in S_4$, if and only if L_i holds in $(Q, \langle , , \rangle)$.

TABLE I

	Permutation π_i	Type	Corresponding Identity L_i
1.	1243	$(\cdot)(\cdot)(\cdot\cdot)$	$\langle a, b, \langle a, b, d\rangle\rangle = d$
2.	2134	$(\cdot\cdot)(\cdot)(\cdot)$	$\langle a, b, c\rangle = \langle b, a, c\rangle$
3.	2143	$(\cdot\cdot)(\cdot\cdot)$	$\langle a, b, \langle b, a, d\rangle\rangle = d$
4.	1324	$(\cdot)(\cdot\cdot)(\cdot)$	$\langle a, b, c\rangle = \langle a, c, b\rangle$
5.	4231	$(\cdot)(\cdot)(\cdot\cdot)$	$\langle\langle d, b, c\rangle, b, c\rangle = d$
6.	4321	$(\cdot\cdot)(\cdot\cdot)$	$\langle\langle d, c, b\rangle, b, c\rangle = d$
7.	3214	$(\cdot\cdot)(\cdot)(\cdot)$	$\langle c, b, a\rangle = \langle a, b, c\rangle$
8.	3412	$(\cdot\cdot)(\cdot\cdot)$	$\langle a, \langle c, d, a\rangle, c\rangle = d$
9.	1432	$(\cdot)(\cdot)(\cdot\cdot)$	$\langle a, \langle a, d, c\rangle, c\rangle = d$
10.	2314	$(\cdot)(\cdot\cdot\cdot)$	$\langle c, a, b\rangle = \langle a, b, c\rangle$
11.	3124	$(\cdot\cdot\cdot)(\cdot)$	$\langle b, c, a\rangle = \langle a, b, c\rangle$
12.	2431	$(\cdot)(\cdot\cdot\cdot)$	$\langle a, \langle d, a, c\rangle, c\rangle = d$
13.	4132	$(\cdot)(\cdot\cdot\cdot)$	$\langle\langle b, d, c\rangle, b, c\rangle = d$
14.	3241	$(\cdot)(\cdot\cdot\cdot)$	$\langle a, b, \langle d, b, a\rangle\rangle = d$
15.	4213	$(\cdot)(\cdot\cdot\cdot)$	$\langle c, b, \langle d, b, c\rangle\rangle = d$
16.	1423	$(\cdot)(\cdot\cdot\cdot)$	$\langle a, \langle a, c, d\rangle, c\rangle = d$
17.	1342	$(\cdot)(\cdot\cdot\cdot)$	$\langle a, b, \langle a, d, b\rangle\rangle = d$
18.	4123	$(\cdot\cdot\cdot\cdot)$	$\langle\langle b, c, d\rangle, b, c\rangle = d$
19.	4312	$(\cdot\cdot\cdot\cdot)$	$\langle\langle c, d, b\rangle, b, c\rangle = d$
20.	2341	$(\cdot\cdot\cdot\cdot)$	$\langle a, b, \langle d, a, b\rangle\rangle = d$
21.	2413	$(\cdot\cdot\cdot\cdot)$	$\langle a, \langle c, a, d\rangle, c\rangle = d$
22.	3142	$(\cdot\cdot\cdot\cdot)$	$\langle a, b, \langle b, d, a\rangle\rangle = d$
23.	3421	$(\cdot\cdot\cdot\cdot)$	$\langle a, \langle d, c, a\rangle, c\rangle = d$
24.	1234	the identity permutation	$\langle a, b, c\rangle = d$

We also give all the subgroups of S_4, considered as sets of identities (cf. [**6**], [**9**]).

Order 2. The nine subgroups are generated by L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8 and L_9.

Order 3. The 4 subgroups are generated by L_{10}, L_{12}, L_{14} and L_{16}.

Order 4. The 6 subgroups are: $\{L_3, L_6, L_8, L_{24}\}$, $\{L_{18}, L_{20}, L_8, L_{24}\}$, $\{L_{19}, L_{23}, L_3, L_{24}\}$, $\{L_{21}, L_{22}, L_6, L_{24}\}$, $\{L_1, L_2, L_3, L_{24}\}$, $\{L_4, L_5, L_6, L_{24}\}$ and $\{L_7, L_8, L_9, L_{24}\}$.

Order 6. The 4 subgroups are: $\{L_2, L_4, L_7, L_{10}, L_{11}, L_{24}\}$, $\{L_2, L_5, L_9, L_{12}, L_{13}, L_{24}\}$, $\{L_1, L_5, L_7, L_{14}, L_{15}, L_{24}\}$, and $\{L_1, L_4, L_9, L_{16}, L_{17}, L_{24}\}$.

Order 8. These 3 subgroups are all isomorphic to the dihedral group of order 8. $\{L_1, L_2, L_3, L_6, L_8, L_{19}, L_{23}, L_{24}\}$ has $A = \pi_{19}$ and $B = \pi_2$ as generators, where $A^4 = 1$, $B^2 = 1$ and $BA = A^3B$. $\{L_3, L_4, L_5, L_6, L_8, L_{21}, L_{22}, L_{24}\}$ corresponds to $A = \pi_{21}$, $B = \pi_4$; $\{L_3, L_6, L_8, L_9, L_{18}, L_{20}, L_{24}\}$ corresponds to $A = \pi_{18}$, $B = \pi_7$.

Order 12. There is only the alternating group A_4: $\{L_3, L_6, L_8, L_{10}, L_{11}, L_{12}, L_{13}, L_{14}, L_{15}, L_{16}, L_{17}, L_{24}\}$. We also note that π_{18} and π_{10} generate S_4. In fact, any pair where the first is an even permutation of order 3 and the second is odd of order 4 will be generators.

3.1. 24 Conjugacy classes. From Theorem 2.5, if $m > 16$, there exists a ternary quasigroup of order m with 24 conjugacy classes. We will now consider the lower orders.

LEMMA 3.1.1. *If* (*i*) $m \geqq 7$, *m odd, or if*
(*ii*) $m \geqq 14$, *m even*,
then there exists a ternary quasigroup of order m with 24 *conjugacy classes.*

Proof. By Theorem 2.5, we need only show there exist integers $q, r \in \{0, 1, 2, \ldots, m-1\}$ such that $q \neq r$, q, r are relatively prime to m, $q + r \not\equiv 0 \pmod{m}$ and $q, r \neq m-1$ or 1. If m is odd, $m \geqq 7$, then $q = 2$, $r = [m/2]$ may be chosen. If $m = 2^s t \geqq 14$ where $s \geqq 1$, t is odd, then we may take $q = t + 2$ and $r = t + 4$.

It is not difficult to see the following.

LEMMA 3.1.2. *There do not exist any* 3-*quasigroups with* 24 *conjugacy classes of orders* 1, 2 *or* 3.

Consider the following definition, which also provides a representation of a ternary quasigroup as a latin cube.

Definition 3.1.3. Define the *front vertical faces* of a ternary quasigroup $(Q, \langle\, , ,\rangle)$ to be the Cayley tables of the quasigroups $(Q, \circ_{F_i})$ derived from $(Q, \langle\, , ,\rangle)$ by setting $a \circ_{F_i} b = c$ if and only if $\langle a, b, i\rangle = c \quad \forall\ a, b, c, \in Q$, where $Q = \{1, 2, \ldots, n\}$. Similarly the *side vertical faces* are the Cayley tables of the quasigroups $(Q, \circ_{s_i})$ where $a \circ_{s_i} b = c$ if and only if $\langle a, i, b\rangle = c$. Finally, the *horizontal faces* are the Cayley tables of $\{(Q, \circ_{H_i})\}$ where $a \circ_{H_i} b = c$ if and only if $\langle i, a, b\rangle = c$.

LEMMA 3.1.4. *There exists a 3-quasigroup of order 4 with 24 conjugacy classes.*

Proof. Consider the 3-quasigroup defined by the following front vertical faces.

	1	2	3	4
1	1	2	3	4
2	3	4	1	2
3	4	3	2	1
4	2	1	4	3

FACE 1

	1	2	3	4
1	4	3	1	2
2	1	2	4	3
3	2	1	3	4
4	3	4	2	1

FACE 2

	1	2	3	4
1	3	4	2	1
2	2	1	3	4
3	1	2	4	3
4	4	3	1	2

FACE 3

	2	1	3	4
1	2	1	4	3
2	4	3	2	1
3	3	4	1	2
4	1	2	3	4

FACE 4

Law 2 is clearly not satisfied. L_1 is contradicted by $\langle 2, 2, 3\rangle = 1$, and $\langle 2, 2, 1\rangle = 4$. If L_1 is not satisfied with the first two positions equal (2), then L_3 is not satisfied. L_6 is contradicted by $\langle 3, 2, 1\rangle = 3$, $\langle 1, 2, 3\rangle = 4$. This also means L_4 does not hold. L_9 is contradicted by $\langle 1, 3, 2\rangle = 1$, $\langle 1, 1, 2\rangle = 4$. L_8 is contradicted by $\langle 2, 3, 1\rangle = 1$, $\langle 1, 1, 2\rangle = 4$, while for L_7, consider $\langle 3, 2, 1\rangle = 3$, $\langle 1, 2, 3\rangle = 4$. Now L_{10} does not hold because $\langle 1, 2, 3\rangle = 4$, $\langle 2, 3, 1\rangle = 1$ and therefore L_{11} does not hold either. For L_{12} to L_{17}, we need only consider L_{12}, L_{14} and L_{16}. L_{12} is violated by $\langle 2, 1, 3\rangle = 2$, $\langle 1, 2, 3\rangle = 4$; L_{14} by $\langle 3, 2, 1\rangle = 3$, $\langle 1, 2, 3\rangle = 4$; and L_{16} by $\langle 2, 1, 3\rangle = 2$, $\langle 2, 2, 1\rangle = 4$.

In fact L_{18} to L_{23} cannot hold as π_{18} generates a subgroup of order 4 containing π_8, π_3 is in the subgroup $\{\pi_3, \pi_{19}, \pi_{23}, \pi_{24}\}$ and $\pi_6 \in \{\pi_6, \pi_{21}, \pi_{22}, \pi_{24}\}$. Therefore $|C(Q, \langle\ ,\ ,\ \rangle)| = 24$.

The example for $n = 5$ was found to generalize to produce an alternate method for constructing 3-quasigroups of higher orders with 24 conjugacy classes.

LEMMA 3.1.5. *There exists a ternary quasigroup of order m with 24 conjugacy classes for all $m \geqq 5$.*

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

Proof. Consider the following construction. Let $(Q, \circ_{F_1})$ be defined by $a \circ_{F_1} b \equiv (a + b - 1) \pmod m \quad \forall\, a, b \in Q$, $Q = \{1, 2, \ldots, m\}$, $m \geqq 5$. Interchange the first 2 rows of the Cayley table of $(Q, \circ_{F_1})$. Construct the remaining front vertical faces $2, \ldots, m$ by adding 1 (mod m) successively to each of the corresponding elements of face 1. Clearly the resulting cube will be latin.

Now interchange the first and second front vertical faces. Also interchange the second and third side vertical faces (the first and second cannot be chosen as commutativity is then restored to the original faces). Call the corresponding 3-quasigroup $(Q, \langle\, ,\, ,\rangle$.

These manipulations result in the following entries in the first, second and third front vertical faces:

$$
\begin{array}{cccc}
2 & 4 & 3 & \ldots \\
1 & 3 & 2 & \ldots \\
3 & 5 & 4 & \ldots \\
4 & . & . & . \\
. & . & . & . \\
. & . & . & .
\end{array}
\qquad
\begin{array}{cccc}
3 & 5 & 4 & \ldots \\
2 & 4 & 3 & \ldots \\
4 & 0 & 5 & \ldots \\
. & . & . & . \\
. & . & . & . \\
. & . & . & .
\end{array}
\qquad
\begin{array}{cccc}
4 & 0 & 5 & \ldots \\
3 & 5 & 4 & \ldots \\
5 & 0 & 0 & \ldots \\
. & . & . & . \\
. & . & . & . \\
. & . & . & .
\end{array}
$$

FACE 1 FACE 2 FACE 3

The zeroed entries have values greater than 5 if $m > 6$, 1 or 2 if $m = 5$, and 1 and 6 if $m = 6$.

Now face 1 is non-commutative, so $(Q, \langle\, ,\, ,\rangle)$ does not satisfy L_2. Further, L_1 is violated by $\langle 2, 2, 1\rangle = 3$, and $\langle 2, 2, 3\rangle = 5$. This also violates L_3. L_4 is violated by $\langle 2, 3, 1\rangle = 2$, $\langle 2, 1, 3\rangle = 3$. L_5 doesn't hold because $\langle 2, 1, 3\rangle = 3$, while $\langle 3, 1, 3\rangle = 5$. L_6 is contradicted by the example for L_4. L_7 does not hold because $\langle 2, 1, 3\rangle = 3$, but $\langle 3, 1, 2\rangle = 4$. L_8 is contradicted by $\langle 1, 1, 1\rangle = 2$ and $\langle 1, 2, 1\rangle = 4$, which also contradicts L_9. It remains only to discuss L_{10}, L_{12}, L_{14} and L_{16}. The fact that $\langle 1, 2, 1\rangle = 4$, $\langle 2, 1, 1\rangle = 1$ contradicts L_{10}. For L_{12}, $\langle 1, 1, 1\rangle = 2$ should imply $\langle 1, 2, 1\rangle = 1$, but $\langle 1, 2, 1\rangle = 4$. For L_{14}, $\langle 1, 1, 1\rangle = 2$ implies $\langle 1, 1, 2\rangle = 1$, while we have $\langle 1, 1, 2\rangle = 3$. Finally $\langle 1, 1, 1\rangle = 2$ and $\langle 1, 2, 1\rangle = 4$, violating L_{16}. Theorem $|C(Q, \langle\, ,\, ,\rangle)| = 24$.

Lemmas 3.1.1-3.1.5 result in:

THEOREM 3.1.6. *Ternary quasigroups with* 24 *conjugacy classes exist for all orders* $m \geqq 4$ *and do not exist for any* $m < 4$.

We remark that if $x \circ y$ on $Q = \{0, 1, 2, \ldots, m - 1\}$ is defined to be $x + py \pmod m$, where $p \neq 1$ or $m - 1$ and p is relatively prime to m, then $|C(Q, \circ)| = 6$. If $m \geqq 5$ and odd, take $p = (m + 1)/2$. If $m \geqq 8$ and even, $m = 2^s t$, t odd, take $p = t + 2$. This provides a simple alternate construction to that given in [**14**] for ordinary quasigroups, where again embedding theorems are needed.

3.2. Twelve conjugacy classes.

LEMMA 3.2.1. *There exists a ternary quasigroup of order m with 12 conjugacy classes whenever*

(*i*) $m \geqq 5$, *if m odd* or

(*ii*) $m \geqq 8$, *if m even.*

Proof. From Theorem 2.6 we may define $\langle a, b, c\rangle \equiv (a + b + pc) \pmod{m}$ on $Q = \{0, 1, 2, \ldots, m - 1\}$, where $p \in Q$, $p \neq m - 1$ or 1, and p is relatively prime to m. If $m \geqq 5$ and odd, let $p = 2$. If $m \geqq 8$, $m = 2^s t$, t odd, let $p = t + 2$.

Definition 3.2.2. A 3-quasigroup $(Q, \langle , ,\rangle)$ is said to satisfy the *generalized idempotent law* if $\langle x, x, y\rangle = \langle x, y, x\rangle = \langle y, x, x\rangle \quad \forall\, x, y \in Q$.

LEMMA 3.2.3. *There exists a 3-quasigroup of order 6 with 12 conjugacy classes which also satisfies the generalized idempotent law.*

Proof. Let $Q = \{1, 2, 3, 4, 5, 6\}$. Define $\langle a, b, c\rangle$ so that $\langle a, b, c\rangle \neq a, b$ or c, where a, b, c are distinct, by the table below. Then the remaining products may be defined by the generalized idempotent law. One may check that these products do indeed define a 3-quasigroup.

From the definition of $(Q, \langle , ,\rangle)$ one sees that L_7 is satisfied. Suppose $(Q, \langle , ,\rangle)$ had only 3 conjugacy classes. Then there would be a subgroup of order 8 of S_4 such that all the corresponding identities were satisfied. However, π_7 is in the subgroup $\{\pi_{18}, \pi_{20}, \pi_8, \pi_7, \pi_6, \pi_3, \pi_9, \pi_{24}\}$ and no other subgroup of order 8. We have $\langle 1, \langle 3, 6, 1\rangle, 3\rangle = \langle 1, 2, 3\rangle = 4 \neq 6$, contradicting L_8. Therefore $(Q, \langle , ,\rangle)$ cannot have only 3 conjugacy classes. π_7 is an odd permutation and thus cannot belong to the alternating subgroup A_4. But then $(Q, \langle , ,\rangle)$ cannot have 2 conjugacy classes.

The only subgroups of order 6 containing π_7 are $\{\pi_1, \pi_2, \pi_4, \pi_7, \pi_{10}, \pi_{11}, \pi_{24}\}$ and $\{\pi_5, \pi_1, \pi_7, \pi_{14}, \pi_{15}, \pi_{24}\}$. As $\langle , ,\rangle$ is clearly not commutative in the first 2 positions, L_2 is not satisfied. Also $\langle 2, 1, 3\rangle = 6$, but $\langle 2, 1, 6\rangle = 4 \neq 3$, contradicting L_1. Therefore we do not have a subgroup of order 6 of S_4 with all the corresponding identities satisfied.

Finally, the only subgroup of order 4 containing π_7 is $\{\pi_{24}, \pi_7, \pi_8, \pi_9\}$. But this is itself a subgroup of the subgroup of order 8 above. Therefore $|C, (Q, \langle , ,\rangle)| = 12$.

Remark 3.2.4. L. Humbolt in [**8**] constructs idempotent ($\langle x, x, x\rangle = x$) 3-quasigroups. However, the spectrum of 3-quasigroups satisfying the generalized idempotent law is not completely known. Any 3-quasigroup derived from a Steiner quadruple system (cf. [**12**], [**13**]) will satisfy this law providing orders congruent to 2 or 4(mod 6), and as the ordinary direct product of 3-quasigroups will clearly preserve it, there exist generalized idempotent quasigroups of orders 6^m, $6^m(2 + 6n)$, $6^m(4 + 6n)$. (cf. also [**10**], [**11**]).

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

Definition of triples with 3 distinct elements

$\langle 1, 2, 3\rangle = 4$	$\langle 1, 3, 4\rangle = 6$	$\langle 1, 4, 6\rangle = 2$
$\langle 2, 3, 1\rangle = 5$	$\langle 3, 4, 1\rangle = 5$	$\langle 4, 6, 1\rangle = 5$
$\langle 3, 1, 2\rangle = 6$	$\langle 4, 1, 3\rangle = 2$	$\langle 6, 1, 4\rangle = 3$
$\langle 2, 1, 3\rangle = 6$	$\langle 3, 1, 4\rangle = 2$	$\langle 4, 1, 6\rangle = 3$
$\langle 1, 3, 2\rangle = 5$	$\langle 1, 4, 3\rangle = 5$	$\langle 1, 6, 4\rangle = 5$
$\langle 3, 2, 1\rangle = 4$	$\langle 4, 3, 1\rangle = 6$	$\langle 6, 4, 1\rangle = 2$
$\langle 1, 2, 4\rangle = 3$	$\langle 1, 3, 5\rangle = 2$	$\langle 1, 5, 6\rangle = 3$
$\langle 2, 4, 1\rangle = 6$	$\langle 3, 5, 1\rangle = 6$	$\langle 5, 6, 1\rangle = 4$
$\langle 4, 1, 2\rangle = 5$	$\langle 5, 1, 3\rangle = 4$	$\langle 6, 1, 5\rangle = 2$
$\langle 2, 1, 4\rangle = 5$	$\langle 3, 1, 5\rangle = 4$	$\langle 5, 1, 6\rangle = 2$
$\langle 1, 4, 2\rangle = 6$	$\langle 1, 5, 3\rangle = 6$	$\langle 1, 6, 5\rangle = 4$
$\langle 4, 2, 1\rangle = 3$	$\langle 5, 3, 1\rangle = 2$	$\langle 6, 5, 1\rangle = 3$
$\langle 1, 2, 5\rangle = 6$	$\langle 1, 3, 6\rangle = 4$	$\langle 2, 3, 4\rangle = 1$
$\langle 2, 5, 1\rangle = 4$	$\langle 3, 6, 1\rangle = 2$	$\langle 3, 4, 2\rangle = 6$
$\langle 5, 1, 2\rangle = 3$	$\langle 6, 1, 3\rangle = 5$	$\langle 4, 2, 3\rangle = 5$
$\langle 2, 1, 5\rangle = 3$	$\langle 3, 1, 6\rangle = 5$	$\langle 3, 2, 4\rangle = 5$
$\langle 1, 5, 2\rangle = 4$	$\langle 1, 6, 3\rangle = 2$	$\langle 2, 4, 3\rangle = 6$
$\langle 5, 2, 1\rangle = 6$	$\langle 6, 3, 1\rangle = 4$	$\langle 4, 3, 2\rangle = 1$
$\langle 1, 2, 6\rangle = 5$	$\langle 1, 4, 5\rangle = 3$	$\langle 2, 3, 5\rangle = 6$
$\langle 2, 6, 1\rangle = 3$	$\langle 4, 5, 1\rangle = 2$	$\langle 3, 5, 2\rangle = 4$
$\langle 6, 1, 2\rangle = 4$	$\langle 5, 1, 4\rangle = 6$	$\langle 5, 2, 3\rangle = 1$
$\langle 2, 1, 6\rangle = 4$	$\langle 4, 1, 5\rangle = 6$	$\langle 3, 2, 5\rangle = 1$
$\langle 1, 6, 2\rangle = 3$	$\langle 1, 5, 4\rangle = 2$	$\langle 2, 5, 3\rangle = 4$
$\langle 6, 2, 1\rangle = 5$	$\langle 5, 4, 1\rangle = 3$	$\langle 5, 3, 2\rangle = 6$
$\langle 2, 3, 6\rangle = 5$	$\langle 2, 4, 5\rangle = 1$	$\langle 2, 4, 6\rangle = 3$
$\langle 3, 6, 2\rangle = 1$	$\langle 4, 5, 2\rangle = 6$	$\langle 4, 6, 2\rangle = 5$
$\langle 6, 2, 3\rangle = 4$	$\langle 5, 2, 4\rangle = 3$	$\langle 6, 2, 4\rangle = 1$
$\langle 3, 2, 6\rangle = 4$	$\langle 4, 2, 5\rangle = 3$	$\langle 4, 2, 6\rangle = 1$
$\langle 2, 6, 3\rangle = 1$	$\langle 2, 5, 4\rangle = 6$	$\langle 2, 6, 4\rangle = 5$
$\langle 6, 3, 2\rangle = 5$	$\langle 5, 4, 2\rangle = 1$	$\langle 6, 4, 2\rangle = 3$
$\langle 2, 5, 6\rangle = 1$	$\langle 3, 4, 5\rangle = 2$	$\langle 3, 4, 6\rangle = 1$
$\langle 5, 6, 2\rangle = 3$	$\langle 4, 5, 3\rangle = 1$	$\langle 4, 6, 3\rangle = 2$
$\langle 6, 2, 5\rangle = 4$	$\langle 5, 3, 4\rangle = 6$	$\langle 6, 3, 4\rangle = 5$
$\langle 5, 2, 6\rangle = 4$	$\langle 4, 3, 5\rangle = 6$	$\langle 4, 3, 6\rangle = 5$
$\langle 2, 6, 5\rangle = 3$	$\langle 3, 5, 4\rangle = 1$	$\langle 3, 6, 4\rangle = 2$
$\langle 6, 5, 2\rangle = 1$	$\langle 5, 4, 3\rangle = 2$	$\langle 6, 4, 3\rangle = 1$

$\langle 3, 5, 6\rangle = 2$	$\langle 5, 3, 6\rangle = 4$	$\langle 4, 5, 6\rangle = 3$	$\langle 5, 4, 6\rangle = 2$
$\langle 5, 6, 3\rangle = 1$	$\langle 3, 6, 5\rangle = 1$	$\langle 5, 6, 4\rangle = 1$	$\langle 4, 6, 5\rangle = 1$
$\langle 6, 3, 5\rangle = 4$	$\langle 6, 5, 3\rangle = 2$	$\langle 6, 4, 5\rangle = 2$	$\langle 6, 5, 4\rangle = 3$

THEOREM 3.2.5. *There exists a ternary quasigroup of order m with exactly* 12 *conjugacy classes if and only if* $m \geqq 4$.

Proof. One may show that no 3-quasigroup of order 2 or 3 exists with 12 conjugacy classes. If $m = 4$, consider the following example. (Here, the first fron vertical face is circled and the third front vertical face is squared.) The ternary quasigroup thus represented may be seen to have 12 conjugacy classes.

4 $\boxed{3}$ 2 1	1 $\boxed{4}$ 3 2	2 $\boxed{1}$ 4 3	3 $\boxed{2}$ 1 4
1 $\boxed{4}$ 3 2	3 $\boxed{2}$ 1 4	4 $\boxed{3}$ 2 1	2 $\boxed{1}$ 4 3
2 $\boxed{1}$ 4 3	4 $\boxed{3}$ 2 1	3 $\boxed{2}$ 1 4	1 $\boxed{4}$ 3 2
3 $\boxed{2}$ 1 4	2 $\boxed{1}$ 4 3	1 $\boxed{4}$ 3 2	4 $\boxed{3}$ 2 1

3.3. Six conjugacy classes. Although Theorem 2.7 does not apply, one may obtain the following results.

LEMMA 3.3.1. *If $m > 3$ and odd, there exists a ternary quasigroup of order m with* 6 *conjugacy classes.*

Proof. Let $Q = \{0, 1, \ldots, m - 1\}$. Define $\langle , , \rangle$ on Q by $\langle a, b, c\rangle \equiv (2a + 2b - c) \pmod m$ $\forall\, a, b, c \in Q$. It can be easily shown that L_1, L_2 and L_3 are satisfied.

Now the only subgroup larger than $\{\pi_1, \pi_2, \pi_3, \pi_{24}\}$ and containing it is the subgroup of order $8 = \{\pi_1, \pi_2, \pi_3, \pi_6, \pi_8, \pi_9, \pi_{23}, \pi_{24}\}$. However, consider L_6: $\langle\langle d, c, b\rangle, b, c\rangle = (2d + 2c - b)2 + 2b - c \equiv d$. If $b = 0$, $c = 1$, $d = 1$, $4 \equiv 1 \pmod m$, which is false.

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

LEMMA 3.3.2. *If* $m > 6$, *m is even and* $m \neq 8, 12$, *or* 24, *there exists a ternary quasigroup of order m with exactly* 6 *conjugacy classes.*

Proof. Let $Q = \{0, 1, \ldots, m - 1\}$. Define $\langle , , \rangle$ on Q by $\langle a, b, c\rangle \equiv (a(t + 2) + b(t + 2) - c \pmod m)$ where $m = 2^s t$, t odd. We need only show that L_6 does not hold. Now $\langle\langle d, c, b\rangle, b, c\rangle \equiv (d(t + 2) + c(t + 2) - b)(t + 2) + b(t + 2) - c \equiv c((t + 2)^2 - 1) + d(t + 2)^2 \equiv d(\bmod m)$. This implies $(t + 2)^2 \equiv 1(\bmod m)$, or $t^2 + 4t + 4 \equiv 1 \pmod m$, which gives $t^2 + 4t + 3 \equiv 0 \pmod m$. As $t|m$, $t|3$. Therefore $t = 1$ or 3. If $t = 1$, $9 \equiv 1(\bmod m)$ or $m = 2, 4$ or 8. If $t = 3$, $25 \equiv 1(\bmod m)$ and $m = 6, 12$ or 24. In every other case $(t + 2)^2 \not\equiv 1 \pmod m$.

It may be shown that no 3-quasigroups exist of orders $m < 3$ with 6 conjugacy classes. If $m = 3$, let $Q = \mathbf{Z}_3$ and define $\langle a, b, c\rangle = d$ if and only if $a + b - c - d = 1$. (This example is due to D. G. Hoffman.) If $m = 4$ or 6, constructions may be made however. We need the following definition.

Definition 3.3.2. Two quasigroups $(Q_1, \circ)$ and (Q_2, x) are *isotopic* [**2**] if there exists an ordered triple of one-to-one maps (θ, ϕ, ψ) of Q_1 onto Q_2 such that $\theta(a) \times \phi(b) = \psi(a \circ b) \quad \forall\ a, b \in Q_1$.

LEMMA 3.3.3. *There exists a ternary quasigroup of order* 4 *and of order* 6 *with* 6 *conjugacy classes and do not exist any of orders* $\leqq 3$ *with* 6 *classes.*

Proof. If $n = 4$, consider the following example, whose front vertical faces are:

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

FACE 1

4	1	2	3
1	3	4	2
2	4	3	1
3	2	1	4

FACE 2

3	4	1	2
4	2	3	1
1	3	2	4
2	1	4	3

FACE 3

2	3	4	1
3	1	2	4
4	2	1	3
1	4	3	2

FACE 4

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

If $n = 6$, the first vertical face is given below

1	2	3	4	5	6
2	3	1	6	4	5
3	1	2	5	6	4
4	6	5	1	2	3
5	4	6	2	3	1
6	5	4	3	1	2

The remaining faces are chosen all isotopic to Face 1 as follows: Let $\theta = \phi =$ dentity mapping. For each face let ψ be defined as below:

$\psi_2(1) = 2$	$\psi_3(1) = 3$	$\psi_4(1) = 4$
$\psi_2(2) = 1$	$\psi_3(2) = 5$	$\psi_4(2) = 6$
$\psi_2(3) = 4$	$\psi_3(3) = 1$	$\psi_4(3) = 2$
$\psi_2(4) = 5$	$\psi_3(4) = 6$	$\psi_4(4) = 1$
$\psi_2(5) = 6$	$\psi_3(5) = 4$	$\psi_4(5) = 3$
$\psi_2(6) = 3$	$\psi_3(6) = 2$	$\psi_4(6) = 5$
FACE 2	FACE 3	FACE 4

$\psi(1) = 5$	$\psi(1) = 6$
$\psi(2) = 3$	$\psi(2) = 4$
$\psi(3) = 6$	$\psi(3) = 5$
$\psi(4) = 2$	$\psi(4) = 3$
$\psi(5) = 1$	$\psi(4) = 2$
$\psi(6) = 4$	$\psi(4) = 1$
FACE 5	FACE 6

We give now a general theorem, which can be used to provide many alternate constructions to those given throughout this paper, and which here provides examples for the missing orders 8, 12 and 24.

LEMMA 3.3.4. *If q is any factor of m and if there exists a ternary quasigroup of order q with a specified number of conjugacy classes, then there exists a ternary quasigroup of order m with the same specified number of classes.*

For a proof see [**15**].

THEOREM 3.3.5. *There exists a 3-quasigroup of order m with 6 conjugacy classes if and only if $m \geqq 3$.*

3.4. Four conjugacy classes.

THEOREM 3.4.1. *There exists a ternary quasigroup of order m with 4 conjugacy classes if and only if* $m \geqq 3$.

Proof. From Theorem 2.6, if $j = 3$, we have $\langle a_1, a_2, a_3\rangle \equiv (a_1 + a_2 + a_3) \pmod m$ and so $m_3(3) = 3$ as no primes are needed.

Remark 3.4.2. The 3-quasigroups in Theorem 3.4.1 satisfy identities L_2, L_4, L_7, L_{10} and L_{11}. It is easy, in this case, to provide constructions of 3-quasigroups satisfying sets of identities corresponding to the other subgroups of order 6. For the subgroup $\{\pi_2, \pi_5, \pi_9, \pi_{12}, \pi_{13}, \pi_{24}\}$, define $\langle a, b, c\rangle \equiv (-a - b + c) \pmod m$. Similarly the subgroup $\{\pi_1, \pi_5, \pi_7, \pi_{14}, \pi_{15}, \pi_{24}\}$ is obtained by defining $\langle a, b, c\rangle \equiv (-a + b - c) \pmod m$ and the subgroup $\{\pi_1, \pi_4, \pi_9, \pi_{16}, \pi_{17}, \pi_{24}\}$ be defining $\langle a, b, c\rangle \equiv (a - b - c) \pmod m$.

The following discussion provides a non-algebraic alternate construction to Theorem 3.4.1.

Definition 3.4.3. Let $(Q, \langle , ,\rangle)$ be a 3-quasigroup which satisfies the generalized idempotent and commutative laws, but does not satisfy Steiner's law: $\langle x, y, \langle x, y, z\rangle\rangle = z, \quad \forall\, x, y, z \in Q$. Such a 3-quasigroup is called a *generalized idempotent and commutative non-Steiner ternary quasigroup.*

Such 3-quasigroups have 4 conjugacy classes and satisfy the identities L_2, L_4, L_7, L_{10} and L_{11}. They have also been considered by C .C. Lindner (private communication), who observed that they will exist only if the order $m \equiv 2$ or $4 \pmod 6$. The next theorem shows the sufficiency of this condition.

THEOREM 3.4.4. *A generalized idempotent and commutative non-Steiner ternary quasigroup of order m exists if and only if* $m \equiv 2$ *or* $4 \pmod 6$, $m > 2$.

Proof. (1) Suppose $(Q, \langle , ,\rangle)$ is a ternary quasigroup derived from a Steiner quadruple system of order m. (cf. [**12**], [**13**]). $(Q, \langle , ,\rangle)$ is constructed to satisfy the generalized idempotent and commutative laws. On the sets $\{2, 3, \ldots, m\}$, $\{1, 3, 4, \ldots, m\}, \ldots, \{1, 2, \ldots, m - 1\}$ respectively define a set of quasigroups $\{(Q_i, \circ_i) \mid \ i = 1, \ldots, m\}$ by $a \circ_i b = c$ if $\langle a, b, c\rangle = i$, when $a \neq b$. The quasigroups are all required to be idempotent. Now perform the following interchange between $(Q_1, \circ_1)$ and $(Q_2, \circ_2)$. Whenever $a \circ_1 b = c, \quad a, b, c \neq 2$, $a' \circ_2 b' = c', \quad a', b', c' \neq 1$, define $a' \times_1 b' = c'$ on Q_1. Otherwise $\times_1 = \circ_1$ and $\times_2 = \circ_2$.

Now $(Q_1, \times_1)$ and $(Q_2, \times_2)$ will still be quasigroups and we may form (as in [**15**]) a new ternary quasigroup $(Q_1 \langle , ,\rangle')$ from $\{(Q_1, \times_1), (Q_2, \times_2), (Q_3, \circ_3), \ldots, (Q_m, \circ_m)\}$ according to $\langle a, b, c\rangle = d$ if $a \circ_d b = c$ or $a \times_d b = c$ when a, b and c are distinct. Otherwise the generalized idempotent law holds.

(2) Suppose $\langle a, b, c\rangle' = 2$ where $a \times_2 b = c$ in $(Q_2, \times_2)$ and none of a, b, c are equal to 1. Now $\langle\langle a, b, c\rangle', b, c\rangle' = \langle 2, b, c\rangle' = \langle 2, b, c\rangle$. But $\langle\langle a, b, c\rangle, b, c\rangle = \langle 1, b, c\rangle = a$. Therefore $\langle 2, b, c\rangle \neq a$ and $(Q, \langle , ,\rangle')$ is non-Steiner.

https://doi.org/10.4153/CJM-1979-064-6 Published online by Cambridge University Press

3.5. Three conjugacy classes.

THEOREM 3.5.1. *A ternary quasigroup of order m with exactly* 3 *conjugacy classes exists if and only if* $m \geqq 3$.

Proof. On $Q = \{0, 1, 2, \ldots, m-1\}$, define $\langle a, b, c\rangle = a - b + c$ with addition (mod m). One may check that all the identities corresponding to the elements of the subgroup $\{\pi_3, \pi_6, \pi_7, \pi_8, \pi_9, \pi_{18}, \pi_{20}, \pi_{24}\}$ are satisfied and no others. Again one may construct examples for the other subgroups of order 8. For the subgroup generated by π_2 and π_{19}, define $\langle a, b, c\rangle \equiv (a + b - c) \pmod m$ and for the subgroup generated by π_7 and π_{18}, take $\langle a, b, c\rangle \equiv (-a + b + c) \pmod m$.

3.6. Conclusion to ternary case.

THEOREM 3.6.1. (1) *There exist* 3-*quasigroups of order n with* 6, 12, *or* 24 *conjugacy classes if and only if* $m \geqq 3$.

(2) *There exist* 3-*quasigroups of order m with* 3 *or* 4 *conjugacy classes if and only if* $m \geqq 3$.

(3) *There exists a ternary quasigroup with one conjugacy class for all orders* $\geqq 1$.

Throughout Section 3, the emphasis has been on the existence of some 3-quasigroup with a specified number of conjugates. Occasionally additional examples are given, but the broader question of finding the spectrum of ternary quasigroups satisfying exactly the identities corresponding to each of the subgroups of S_4 remains unanswered.

REFERENCES

1. A. Cruse, *On the finite completion of partial latin cubes*, J. Combinatorial Theory (A) *17* (1974), 112–119.

2. J. Dénes and A. D. Keedwell, *Latin squares and their applications* (Academic Press, New York, 1974).

3. T. Evans, *The construction of orthogonal κ-skeins and latin k-cubes*, Aequationes Math. *14* (1976), 485–491.

4. ——— *Latin cubes orthogonal to their transposes—a ternary analogue of Stein quasigroups*, Aequationes Math. *9* (1973), 296–297.

5. B. Ganter, *Combinatorial designs and algebras*, Preprint No. *270*, Mai 1976, Technische Hochshule, Darmstadt.

6. M. Hall, Jr., *The theory of groups* (MacMillan, New York, 1959).

7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford University Press, 1968).

8. L. Humbolt, *Sur une extension de la notion de carrés latins*, C. R. Acad. Sc. Paris, Sér. A. *273* (1971), 795–798.

9. W. Lederman, *Introduction to the theory of finite groups* (Oliver and Boyd, Edinburgh, 1967).

10. C. C. Lindner, *Two finite embedding theorems for partial 3-quasigroups*, to appear.

11. ——— *A finite partial idempotent latin cube can be embedded in a finite idempotent latin cube*, J. Combinatorial Theory (A), *21* (1976), 104–109.

12. ——— *Some remarks on the Steiner triple systems associated with Steiner quadruple systems*, Colloquium Math. *32* (1975), 301–306.

13. C. C. Linder and A. Rosa, *A survey of Steiner quadruple systems*, Discrete Math., to appear.

14. C. C. Linder and D. Steedley, *On the number of conjugates of a quasigroup*, Alg. Universalis *5* (1975), 191–196.

15. M. McLeish, *On the existence of ternary quasigroups with* 2 *or* 8 *conjugacy classes*, J. Comb. Theory, Seria A, submitted.

16. A. Sade, *Produit direct—singulier de quasigroups, orthogonaux et anti-abéliens*, Ann. Soc. Sci. Bruxelles, Sér. I, *74* (1960), 91–99.

17. ——— *Quasigroupes parastrophiques. Expressions et identités*, Math. Nachr. *20* (1959), 73–106.

18. S. K. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. *85* (1957), 228–256.

University of Alberta,
Edmonton, Alberta