Czechoslovak Mathematical Journal

Philip Holgate

Logarithmetics and quasigroup structure

Czechoslovak Mathematical Journal, Vol. 44 (1994), No. 2, 293–304

Persistent URL: http://dml.cz/dmlcz/128462

Czechoslovak Mathematical Journal, 44 (119) 1994, Praha

LOGARITHMETICS AND QUASIGROUP STRUCTURE

P. HOLGATE, London

(Received June 5, 1992)

Some properties of the logarithmetic of a finite quasigroup are studied in relation to the structure of the quasigroup

1. INTRODUCTION

Etherington [6] introduced the term 'logarithmetic' for the arithmetic of the indices of powers of elements in a nonassociative algebra. Logarithmetics of finite quasigroups were discussed extensively by Popova ([10–17], Bruck [2; 4, pp. 82–86] and Evans [7, 8]. In this paper the ideals and quotients of logarithmetics are examined in §§ 2 and 3, the relations between quasigroups and their logarithmetics is developed in § 4, and the study of the classification of the quasigroups that have a given logarithmetic is begun in § 5. All quasigroups studied in this paper are finite.

The free nonassociative integers N are the elements generated by 1, without using the associative or commutative laws. For a finite quasigroup Q, the quasi-integers are the equivalence classes of the congruence relationship on the free nonassociative integers: $r \equiv s \pmod{\log Q}$ if $a_i^r = a_i^s$ for all $a_i \in Q$. The notation Q_a will be used for the subquasigroup generated by an element a, but Q_{a_i} will shortened to Q_i. Consider the equivalence relation defined by $r \equiv s$ (mod log a_i) if $a_i^r = a_i^s$. It commutes with addition and multiplication since $a_i^r = a_i^s$ and $a_i^u = a_i^v$ imply $a_i^{r+u} = a_i^{s+v}$ and $(a_i^r)^u = (a_i^s)^v$. Clearly $b^r = b^s$ for every $b \in Q_i$. The quotient set $N/(\equiv$ mod log $a_i)$ with nonassociative integer addition and multiplication is called the logarithmetic of a_i, and denoted by $L(a_i)$. The quotient

$$N/(\equiv \bmod \log a_1) \cap \ldots \cap (\equiv \bmod \log a_n)$$

with the same operations is the logarithmetic of Q. The quasi-integer r has a natural representation by the row vector $(a_1^r, \ldots, a_n^r)$. Addition of quasi-integers corresponds to componentwise multiplication of the vectors. Since rs is represented by the vector $(a_1^{rs}, \dots, a_n^{rs})$, it follows that if r is represented by $(b_1, \dots, b_n)$, then rs is represented by $(b_1^s, \dots, b_n^s)$. Hence, multiplication of quasi-integers corresponds to componentwise exponentiation of the vector representing the left hand factor by any nonassociative integer representing the right hand factor. The logarithmetic of Q, denoted by $L(Q)$, is a quasigroup $L_+(Q)$ with respect to addition, and a semigroup $L_\times(Q)$ with respect to multiplication. The operations are linked by a left (but not a right) distributive law since $a^{r(s+t)} = a^{rs} \cdot a^{rt}$. It can be called a left quasiring. The multiplicative semigroup has a matrix representation $r \to M_r$, where M_r has a 1 in the j *th* column of row i if $a_i^r = a_j$, $i = 1, \dots, n$; and 0 elsewhere. Popova gives a number of examples of logarithmetics in her papers, particularly [16].

2. Invertible and uniform elements

The invertible elements of $L_\times(Q)$ are the quasi-integers r for which $a_i^r \neq a_j^r$ if $i \neq j$. In [11] Popova obtains some corollaries to the condition that $L_\times(Q)$ is a group. At the other extreme, if $a_i^r = b$ for some $b \in Q$, all i, r will be called a uniform quasi-integer. In this case M_r has 1's in every position in column j, where $a_j = b$, and zeros elsewhere. The plenary powers of an element a in a nonassociative system are defined by $a^{[1]} = a$, $a^{[n+1]} = (a^{[n]})^2$. The plenary nonassociative integers $[n]$ are given by $[1] = 1$, $[n+1] = [n] + [n]$. The plenary quasi-integers, generated in the same way from 1 (mod log Q) are those for which at least one of the nonassociative integers that represent it is plenary. The ideas of invertibility and uniformity of quasi-integers have the following elementary consequences.

1. *The quasi-integer* 2, *and hence all plenary quasi-integers, are invertible if and only if Q is a diagonal quasigroup.*

2. *The quasi-integer* 2, *and hence all plenary quasi-integers, are uniform if and only if Q is a unipotent quasigroup.*

These classes of quasigroups are defined respectively in [5, p. 31] and in [1, § 7].

3. *If r is noninvertible, then rs is noninvertible, for every s.*

Proof. If two components a_i^r and a_j^r are equal, so are the corresponding components a_i^{rs} and a_j^{rs}. □

4. *If r is uniform, so are rs and sr for every s, and $sr = r$.*

Proof. If r has vector representation $(b, \dots, b)$, then rs is represented by $(b^s, \dots, b^s)$. The second assertion follows because an integer r is uniform precisely when all elements raised to the power r are equal, the common value defining the quasi-integer. Alternatively we can use the matrix representation. If r is uniform,

M_r has a column of 1's, and all the rest of its elements are 0. It follows that M_rM_s has a column of 1's and remaining elements zero, while M_sM_r has the same column of 1's as M_r. □

5. *If r is invertible and s is uniform, then $r+s$ and $s+r$ are invertible.*

Proof. Let $a_i^s = b$. Then the values $a_i^{r+s} = a_i^r b$ are all different, as are ba_i^r. □

6. *If r, s are both uniform, so are $r+s$ and $s+r$.*

7. *If Q contains 2 or more idempotents, $L_\times(Q)$ contains no uniform quasi-integers.*

Proof. If a_i, a_j, are two idempotents of Q, the i^{th} and j^{th} components of every quasi-integer of $L(Q)$ will have a_i, a_j, in the i, j^{th} components of its vector representation. □

8. *If Q contains exactly one idempotent, $L(Q)$ contains either exactly one uniform quasi-integer, or none.*

Proof. Let a_i ($= b$, say) be the unique idempotent. The i *th* component of every quasi-integer will have b in the i *th* component of its representative vector. If for all $j \neq i$, there exists a quasi-integer $r(j)$ such that $a_j^{r(j)} = b$, then $(b, b, \ldots, b)$ is the representative of the unique uniform quasi-integer. Otherwise the representative vectors of all quasi-integers contain as well as b, a component different from b. □

The situation considered here occurs whenever Q is a loop.

9. *The set $U(Q)$ of uniform quasi-integers is a sub-left quasiring of $L(Q)$. Its additive structure $U_+(Q)$ is isomorphic to a subquasigroup of Q. Its multiplicative semigroup $U_\times(Q)$ is a two-sided semigroup ideal of $L_\times(Q)$.*

Proof. Closure under addition follows from 6. The isomorphism arises from $(a, a, \ldots, a) \to a$, and the ideal property for multiplication from 4, above. □

10. *Let $S(Q)$ denote the set of quasi-integers that are invertible or uniform. Then $S_\times(Q)$ is a subsemigroup of $L_\times(Q)$.*

Proof. This follows from 4 and the group property of the invertible quasi-integers. □

Let $\sigma_1, \sigma_2, \ldots, \sigma_t$ be mutually exclusive subsets of the set of integers $1, \ldots, n$. A quasi-integer r such that $a_i^r = a_j^r$ if $i, j \in \sigma_k$ for some k will be said to have pattern $(\sigma_1, \ldots, \sigma_t)$. The uniform integers are the case $\sigma_1 = \{1, \ldots, n\}$. Since calculations with quasi-integers are carried out componentwise, the integers with fixed pattern are closed with respect to quasigroup operations. Hence:

11. *Results* 4 *and* 9 *are valid if "uniform integers" is replaced by "integers having a fixed pattern"*.

The following examples (1, 3, and 4 of [16]) illustrate invertibility and uniformity.

P_1	a	b	c	d
a	c	a	d	b
b	d	b	a	c
c	a	c	b	d
d	b	d	c	a

P_3	a	b	c	d
a	b	d	c	a
b	c	a	b	d
c	a	c	d	b
d	d	b	a	c

P_4	a	b	c	d
a	b	c	d	a
b	d	a	b	c
c	c	b	a	d
d	a	d	c	b

In P_1 the logarithmetic consists of 64 quasi-integers, represented by the 4-vectors with b as second element, and the matrices with a 1 in the (2, 2) position and exactly one 1 in each other row. Only 6 of these are invertible, represented by vectors $(a\ b\ c\ d)$, $(a\ b\ d\ c)$, $(c\ b\ a\ d)$, $(c\ b\ d\ a)$, $(d\ b\ a\ c)$, $(d\ b\ c\ a)$, and the corresponding permutation matrices. A set of representatives of their equivalence classes is 1, $3+(2+4)$, $1+3$, $2+(4+4)$, $(4+3)+(3+3)$, $(1+2)+(2+2)$, and they form the symmetric group S_3. The quasigroup P_1 contains one idempotent. The first case of 8 above holds, and there is just one uniform quasi-integer, for which a class representative is 2^3. The logarithmetic of P_3 contains 4 quasi-integers, represented by the vectors $(a\ b\ c\ d)$, $(b\ a\ d\ c)$, $(c\ d\ a\ b)$, $(d\ c\ b\ a)$ and by representative nonassociative integers 1, 2, 3, $1+2$. These are all invertible, and under multiplication form the direct product $C_2 \times C_2$ of two cyclic groups of order 2. Finally, P_4 has a logarithmetic of 16 elements, listed in [16], of which 8 with vector representations $(a\ b\ c\ d)$, $(a\ b\ d\ c)$, $(b\ a\ c\ d)$, $(b\ a\ d\ c)$, $(c\ d\ a\ b)$, $(c\ d\ b\ a)$, $(d\ c\ a\ b)$, $(d\ c\ b\ a)$, are invertible, forming under multiplication the dihedral group D_8. The quasigroups P_3 and P_4 contain no idempotent, and their logarithmetics contain no uniform quasi-integers.

3. Ideals, differences and quotients

Results 9 and 10 suggest the possibility of quotient structures in logarithmetics. In general, a closed subset in a quasigroup needs some near-associativity before it can define a system of cosets with good combining properties, as in e.g. [3, pp. 60 ff.]. One way of achieving this different from those in the quoted reference is to require the entropic laws $(x+y)+(z+w) = (x+z)+(y+w)$, $(x\ y)(z\ w) = (x\ z)(y\ w)$ to hold for relevant quadruples of elements. We say that an additive quasigroup Q, containing a subquasigroup U, satisfies the U-entropic law if $(x+u)+(z+v) = (x+z)+(u+v)$ for all $x, z \in Q$, $u, v \in U$.

Lemma 3.1. *Suppose that the additively written quasigroup Q, and the subquasigroup $U \subset Q$, satisfy the U-entropic law. Let $r_i, t_i \in Q$, $r_i = t_i + u_i$, $u_i \in U$,*

$i = 1, \ldots, k$, and let $r_0 = \sum^s r_i$, $t_0 = \sum^s t_i$, $u_0 = \sum^s u_i$, where the superscript s is a nonassociative integer specifying the shape of the nonassociative sum $\sum^s$. Then $r_0 = t_0 + u_0$, $u_0 \in U$. In particular we have $(t + u)s = ts + us$.

P r o o f. This is obtained by repeated application of the U-entropic law, beginning with the innermost brackets of the nonassociative sum. The particular case occurs when all $t_i = t$, all $u_i = u$. □

The last result means that the U-entropic law implies a corresponding U-right distributive law. We now take Q to be L_+, the additive structure of the logarithmetic of a quasigroup, and U the set of uniform quasi-integers. We consider the equivalence relation generated by the relations $r \approx r$, all $r \in L_+$, and $r \approx s$ if $r = s + u$, $u \in U$.

Theorem 3.1. *If a logarithmetic $L(Q)$ of a quasigroup Q satisfies the U-entropic law in respect of the sub-left quasiring U of uniform quasi-integers, the equivalence classes of the relation $\approx$ corresponding to U form a left quasiring which is a homomorphic image of $L(Q)$.*

P r o o f. Suppose that $r = s+u$, $r' = s'+u'$ with $u, u' \in U$. Then $(r+r') \approx (s+s')$ by direct application of U-entropy. Moreover $r\ r' = (s + u)(s' + u') = s(s' + u') + u(s' + u')$ by U-right distributivity, $= s(s' + u') + u''$ by the first part of Result 4, $= (s\ s' + su') + u''$ by left distributivity. Hence $r\ r' \approx s\ s'$. Thus there are well defined multiplication and addition laws defined in the quotient $L(Q)/\approx$. □

Note (i). The quasi-integers of $L(Q)$ will satisfy the entropic law in respect of addition, without restriction, if the quasigroup Q itself satisfies the (multiplicative) entropic law. In general, let Q' denote also the subquasigroup of Q, isomorphic to $U_+(Q)$ by $(a_i, \ldots, a_i) \to a_i$, (§ 2, Result 9). Then $L(Q)$ is U-entropic if and only if $(a\ u_1)(b\ u_2) = (a\ b)(u_1 u_2)$ whenever $a, b \in Q_i$ for some i, $1 \leqslant i \leqslant n$; u_1, $u_2 \in Q'$.

Note (ii). By Result 11, the integers with a fixed pattern form an ideal and give rise to a (possibly trivial) quotient left quasiring.

The ideal U in $L_\times(Q)$ also gives rise to a quotient semigroup in the sense of [3, p. 60], if all the members of U are collapsed into a single element. If $L_+(Q)$ has the U-entropic property, this mapping commutes with the formation of the 'additive' quotient left quasiring defined above.

Since each distinct power of a_i must occur among the i^{th} components of the vector, the projection $(a_1^r, \ldots, a_n^r) \to a_i^r$ gives us

Lemma 4.1. *Each Q_i is a homomorphic image of $L_+(Q)$.*

If for $a \in Q$, $a^r \neq a^s$, let us say that a separates r and s. Let M be a minimal subset of Q such that for every pair r, s of quasi-integers in $L(Q)$, there is an $a_i \in M$ such that a_i separates r and s. Then M will be called a logarithmetic base for Q. Given any set $M = \{a_{i_1}, \ldots, a_{i_k}\}$ of elements of Q, we define the direct product quasigroup $V(M) = Q_{i_1} \times \ldots \times Q_{i_k}$. If for some subset M' of Q, $V(M)$ can be embedded in $V(M')$, or if $V(M)$ is a homomorphic image of $V(M')$, and if M is a logarithmetic base, then so is M'.

Examples. In P_1 considered above, the idempotent b is not a member of the logarithmetic base. Since $|L(Q)| = 2^3$, the logarithmetic base must be $\{a, c, d\}$. In P_3, each element is a logarithmetic base.

Theorem 4.1. *Let $M = \{a_1, \ldots, a_k\}$ be a logarithmetic base for Q. Then $L_+(Q)$ is isomorphic to the subquasigroup of $V(M)$ generated by $(a_1, \ldots, a_k)$. It is isomorphic to $V(M)$ if and only if $(a_1, a_2, \ldots, a_k)$ generates $V(Q)$.*

Proof. The quasi-integer r has the natural representation $(a_1^r, \ldots, a_n^r)$. The definitions of separability and logarithmetic base imply that if $r \neq s$, then $(a_1^r, \ldots, a_k^r) \neq (a_1^s, \ldots, a_k^s)$. Hence the projection $(r \leftrightarrow)(a_1^r, \ldots, a_n^r) \to (a_1^r, \ldots, a_k^r)$ is a bijection. □

Popova noted [10] that the logarithmetic is a subdirect product of the Q_i, and some of the above results are implicit in her work. The "only if" part of the last assertion in (i) is equivalent to Theorem 2, Corollary 2 of [10], which asserts that $L_+(Q) \cong Q_1 \times \ldots \times Q_n$ if $|L_+(Q)| = \Pi|Q_i|$. The reduced representation of the logarithmetic [15, Theorem 2] is embedded in the image of $Q_1 \times \ldots \times Q_n$ given by $(a_1, a_2, \ldots, a_k, a_{k+1}, \ldots, a_n) \to (a_1, a_2, \ldots, a_k)$.

Examples. In an idempotent quasigroup, each Q_i is the single element a_i, and the logarithmetic is a single element 1, with $1 + 1 = 1$, $1^2 = 1$. The quasigroup P_3 has an automorphism group of order 4 consisting of the elements $1, (ab)(cd), (ac)(bd), (ad)(bc)$. The nonidentity elements map a into b, c, d, respectively so that a itself is a logarithmetic base. It therefore follows from the Theorem that $L_+(Q)$ is isomorphic to a subquasigroup of Q. The automorphism group of P_4 consists of $1, (ab)(cd)$. Hence a and c form a logarithmetic base, and $L_+(Q)$ must be isomorphic to a subquasigroup of $Q \times Q$. In both examples quoted, the isomorphisms are to the relevant quasigroup itself. In P_1 on the other hand, although each of the elements a, c, d is a single generator, their elementwise logarithmetics are different. We have Q_a: $a = a^1$, $c = a^2$, $b = (a^2)^2$, $d = a^{1+2}$; Q_c: $c = c^1$, $b = c^2$, $a = c^3$, $d = c^4$; Q_d: $d = d^1$, $a = d^2$, $b = d^3$, $c = d^4$. The partition of the nonassociative integers into equivalence classes modulo $\log a$ is different from that modulo $\log c$ or $\log d$. We have $a^3 = a$, or in terms of nonassociative integers, $3 \equiv 1$, while c, d give rise to equivalence classes that can be represented by the first four principal integers. Moreover, while the logarithmetics of c and d involve $\{1, 2, 3, 4\}$, and are isomorphic, the mapping that produces the isomorphism does not commute with the formation of nonassociative powers. The bijection on Q which makes correspond the elements that give rise to the same integer in $L(c)$ and $L(d)$, that is $(ab)(cd)$, is not an automorphism of P_1. The quasigroup P_1 also exemplifies the possibility $L(a) \neq L(Q_a) = L(Q)$. The phenomena arising here are a consequence of the fact that the multiplicative semigroup $L_\times(Q)$ of the logarithmetic is not cancellative.

We now determine which quasigroups can be additive structures of logarithmetics, and we characterize the logarithmetic.

Theorem 4.2. *Let Q be a quasigroup whose elements are equivalence classes of the nonassociative integers, defined by a relation T such that for any nonassociative integers r, s, u, v, $r\ T\ s$ and $u\ T\ v$ imply $(r+s)T(u+v)$. Then $L_+(Q)$ is isomorphic to Q.*

P r o o f. Let r, s be nonassociative integers with $r\ T\ s$. Then by the multiplication in Q, $x^r = x^s$ for all $x \in Q$, hence they belong to the same quasi-integer. The quasi-integer 1 consists of all those nonassociative integers s for which $x = x^s$, all $x \in Q$. Consider a mapping $M\colon L_+(Q) \to Q$, in which the quasi-integer 1 is mapped to the element $a \in Q$ containing the nonassociative integer 1. The logarithmetic is generated by 1, and it follows from the commutativity of T and addition that $1 \to a$ is extended to an isomorphism (in fact an identity) between $L_+(Q)$ and Q. □

In particular the conditions of Theorem 4.2 are satisfied if Q is a homomorphic image of N, or if Q is itself the additive structure of the logarithmetic of some quasigroup.

E x a m p l e. The quasigroup Q shown below has a logarithmetic of 4 quasi-integers that can be represented by 1, 2, $1+2$ and $2+2$, and whose addition table is also shown.

Q	a	b	c	d
a	b	a	c	d
b	a	b	d	c
c	d	c	a	b
d	c	d	b	a

$L_+(Q)$	1	2	$1+2$	$2+2$
1	2	$1+2$	$2+2$	1
2	1	$2+2$	$1+2$	2
$1+2$	$2+2$	1	2	$1+2$
$2+2$	2	$1+2$	1	$2+2$

Its subquasigroup $S \equiv \{a, b\}$ has a logarithmetic $L(S)$ containing the quasi-integers $\{1, 2\}$. The addition table of $L_+(S)$ is $1+1=2$, $1+2=1$, $2+1=1$, $2+2=2$. The relevant homomorphism maps 1 and $1+2$ onto 1, and 2 and $2+2$ onto 2.

Lemma 4.2. (i) *If Q' is a subquasigroup of Q, $L(Q')$ is a homomorphic image of $L(Q)$.*

(ii) *If QH is a homomorphic image of Q under the mapping H, $L(QH)$ is a sub-left quasiring of $L(Q)$. $L(Q')$, $L(QH)$ may be $L(Q)$ itself, or a single idempotent.*

Proof. (i) Suppose the subquasigroup consists of the elements $(a_1, a_2, , a_k)$. Consider the representation of the logarithmetic by means of the embedding $r \to (a_1^r, \ldots, a_n^r)$. The projection $(a_1^r, \ldots, a_n^r) \to (a_1^r, \ldots, a_k^r)$ induces a homomorphism from $L(Q)$ to $L(Q')$. (ii) Suppose that in the above representation $a_1H = a_2H = \ldots = a_kH$, $a_{k+1}H = a_{k+2}H = a_{k+\ell}H$, etc. The sub-left quasiring of $L(Q)$ consisting of those elements with $a_1 = a_2 = \ldots = a_k$, $a_{k+1} = a_{k+2} = \ldots = a_{k+\ell}$, etc. is the logarithmetic of QH. □

Theorem 4.3. *Let Q be a quasigroup of order n, and let $\{a_1, \ldots, a_k\}$ be a logarithmetic base. Let S be a subquasigroup of $Q_1 \times \ldots \times Q_k$. Then S is isomorphic to $L_+(Q)$ if and only if* (i) *there is an $e \in S$, and for every i, $1 \leqslant i \leqslant k$ there is a homomorphism $H_i\colon S \to Q_i$ such that $eH = a_i$, and (ii) no proper subquasigroup of S has this property.*

Proof. Suppose that S has the specified properties. We construct a mapping $H\colon S \to Q_1 \times \ldots \times Q_k$ by defining $eH = (a_1, \ldots, a_k)$. Condition (i) ensures that H can be extended to a homomorphism of the subquasigroup S' of S that is generated by e, onto $Q_1 \times \ldots \times Q_k$. Since S' can be mapped homomorphically to each Q_i by the projection on the i *th* component, condition (ii) secures that $S' = S$. Conversely, $L(Q)$ can be mapped homomorphically to each Q_i by lemma 4.1, and we can take $e = (a_1, \ldots, a_k)$. If some $S' \subsetneq L(Q)$ satisfied the conditions we could construct an $S'' \subseteq S'$ isomorphic to $L(Q)$, which is a contradiction. □

The requirement $eH_i = a_i$ is essential. In Example P_1, $L(Q)$ can be represented by the 64 elements (a^r, c^r, d^r). The set (a, a, a), (b, b, b), (c, c, c) and (d, d, d) form a subquasigroup of $L(Q)$ that can be mapped homomorphically onto each of Q_a, Q_b, Q_c and Q_d, but not in the way specified by Theorem 4.3.

5. Quasigroups with a given logarithmetic

Different quasigroups may have isomorphic logarithmetics. We call Q an antilogarithmetic of $L(Q)$. We call the class of those quasigroups Q such that $L(Q) = S$, the antilogarithmetic class $A(S)$ of S, and we call the class of those quasigroups whose logarithmetics are S or a homomorphic image of S the cumulative antilogarithmetic $C(S)$ of S.

Theorem 5.1. *Let S be a leftquasiring and let $Q^{(1)}, Q^{(2)}, \ldots, \ldots, Q^{(t)} \in C(S)$. Then $\Pi^{\times} Q^{(i)} \in C(S)$. If at least one of the $Q^{(i)} \in A(S)$, then $\Pi^{\times} Q^{(i)} \in A(S)$. If $Q^{(1)} \times Q^{(2)} \in A(S)$, then $Q^{(i)} \in A(S)$, $i = 1, 2$.*

P r o o f. Let $a^{(i)} \in Q^{(i)}$, $i = 1, \ldots, t$. If m, n, are nonassociative integers, $\Pi^{\times}(a^{(i)})^m = \Pi^{\times}(a^{(i)})^n$ if and only if $(a^{(i)})^m = (a^{(i)})^n$ for every i. If $L(Q^{(i)})$ contained quasi integers not contained in an element of S (i.e. in an equivalence class contained in S), then so would $Q^{(1)} \times Q^{(2)}$. Let $Q^{(1)} \in C(S) \setminus A(S)$ and $Q^{(2)} \in A(S)$. Then $Q^{(1)} \times Q^{(2)} \in A(S)$ and so $Q^{(1)} \in A(S)$, a contradiction. □

Corollary. *If the category of quasigroups is regarded as a semigroup with respect to formation of direct products, $C(S)$ is a subsemigroup for any S, and $A(S)$ is a semigroup ideal.*

E x a m p l e (i). The trivial quasiring consisting of one element is the logarithmetic of every idempotent quasigroup and of no others.

E x a m p l e (ii). If Q is any quasigroup and I is an idempotent quasigroup, we have $L(Q \times I) = L(Q)$. If L is of order 2 with elements $\{1, 2\}$, L_+ must be $1+1 = 2+2 = 2$, $1+2 = 2+1 = 1$ which is Z_2 (see example following Theorem 4.5). The other quasigroup of order 2 is not a logarithmetic since $1 + 1 = 1$ means that 1 does not generate it. Hence in Q, a_i^2 is an idempotent for every a_i. Thus $A(L)$ is the class of plenary stable quasigroups of index 2 studied in [9].

A quasigroup that has no nontrivial homomorphic images is said to be simple, and a simple quasigroup with no subquasigroups other than itself is said to be plain. Thus a quasigroup containing an idempotent, hence in particular a group, cannot be plain. (In [10] a simple quasigroup is called *plein* if it has no subquasigroups of order k, $1 < k < n$. In [12], one with no subquasigroups other than itself, even of order 1, is called uni. In [17], *plain* is used for what had been called *uni.*

The assertion below the statement of lemma 2 in [10] needs correction to "chaque élément *nonidempotent* d'un quasigroupe plein est son générateur". However since the presence of idempotents does not change the logarithmetic, the results of [10] are not affected.) In [11] Popova obtained results for logarithmetics of plain quasigroups. Some results for quasigroups whose logarithmetics are plain are given below. The requirement that plain quasigroups have no subquasigroups of order 1 is essential.

Lemma 5.1. *If $L_+(Q)$ is plain, then every nonidempotent element $a \in Q$, generates a subquasigroup isomorphic to $L(Q)$.*

Proof. Consider the subquasigroup Q_a. By Theorem 4.4 (i) its logarithmetic $L(Q_a)$ is a homomorphic image of $L(Q)$, and since $L_+(Q)$ is plain, $L(Q_a)$ must be trivial, or $L(Q)$ itself. Thus either a is idempotent or $Q_a \cong L(Q_a) = L(Q)$. □

Theorem 5.2. *Let S be a plain quasigroup containing no idempotents, and let Q be a quasigroup such that $L_+(Q) = S$. Then the set of elements of Q can be partitioned into disjoint subsets, each of which is a quasigroup isomorphic to S.*

Proof. The subquasigroup Q_1 is a homomorphic image of S by the property of a logarithmetic, and it is an isomorphism by the plainness of S. Now take an element $a_2 \notin Q_1$. If $Q_1 \cap Q_2 \neq \emptyset$, it contains a subquasigroup Q' generated by a single element, with $1 < |Q_1 \cap Q_2| < |S|$. The inverse image of Q' under the isomorphism $S \to Q_1$ is a subquasigroup of S, thus contradicting its plainness. Hence $Q_1 \cap Q_2 = \emptyset$. We proceed in this way until Q is exhausted. □

In studying logarithmetics, a way of constructing 'products' of given quasigroups, weaker than the direct product, is useful. Let P be a quasigroup of order k, with elements $A_1, A_2, \dots, A_k$. Let $Q_1, Q_2, \dots, Q_k$ be k quasigroups of order ℓ, each isomorphic to a quasigroup Q. Let the elements of Q_i be denoted by $a_{i1}, a_{i2}, \dots, a_{i\ell}$ and those of Q by $a_1, a_2, \dots, a_\ell$, labelling them so that each a_{is} is the image of a_s in some isomorphism $Q_i \to Q$. In the array formed by the multiplication table of P we now replace each symbol A_i occuring on the diagonal of the table by the multiplication table of Q_i, and each A_i occuring in an off diagonal position by the multiplication table of any quasigroup with elements $a_{i1}, a_{i2}, \dots, a_{i\ell}$, the implied head and sidelines being in the lexicographical orders given above. Any quasigroup obtained in this way is called a diagonal product of P by Q and will be denoted by $P \setminus Q$, the '$\setminus$' standing for 'diagonal'. The direct product $P \times Q$ is a special case of a diagonal product.

Lemma 5.2. (i) *If $L(P)$ and $L(Q)$ are of orders m_1, m_2 respectively, the order of $L(P \setminus Q)$ is at most $m_1 m_2$.*

(ii) *If $L(P)$, $L(Q)$ are identical, then $L(P \setminus Q)$ is identical to each of them.*

Proof. (i) The nonassociative integers are partitioned into m_1, m_2, classes by the relationships arising from the respective quasigroups. Hence there are at most $m_1 m_2$ classes such that for any pair r, s of nonassociative integers in a given class, $a_i^r = a_i^s$, $b_j^r = b_j^s$ for all $a_i \in P$, $b_j \in Q$. (ii) We have $(a_i, b_j)^r = (a_i^r, b_j^r) = (a_i^s, b_j^s) = (a_i, b_j)^s$ if and only if $r \equiv s \pmod P$, and $r \equiv s \pmod Q$. In this case the relationships are the same. □

Theorem 5.3. *Let S be a plain quasigroup. The class of quasigroups Q for which $L_+(Q) = S$ includes the diagonal products $I \setminus S$, for every idempotent quasigroup I, and the direct products of a finite number of such quasigroups.*

Proof. The first statement is an example of the situation described in Lemma 5.1. and the second statement an example of that described in Lemma 5.2 (ii). □

Corollory. *If S is plain, $L_+(Q) = S$, and $|Q| = 3|S|$, then Q is a diagonal product $I \setminus S$, with I idempotent.*

Proof. We must have $a_{1i}a_{2j} = a_{3k}$ for some k depending on i, j, for all i, j.

The product $a_{1i}a_{2j}$ cannot lie in Q_1, because the unique solution in Q of $a_{1i}x = a_{1s}$ lies in Q_1. Similarly it cannot lie in Q_2. There is thus a multiplicative quotient structure of Q on its subsets Q_1, Q_2, Q_3 which is a quasigroup. □

References

[1] *R.H. Bruck*: Some results in the theory of quasigroups. Trans. American Math. Soc. *5* (1944), 19–52.

[2] *R.H. Bruck*: Analogues of the ring of rational integers. Proc. American Math. Soc. *6* (1955), 50–57.

[3] *R.H. Bruck*: A Survey of Binary Systems. Springer Verlag, 1958.

[4] *R.H. Bruck*: What is a loop?. Studies in Modern Algebra (A.A. Albert, ed.). Math. Assn. of America, 1963, pp. 59–99.

[5] *J. Denes & A. D. Keedwell*: Latin Squares and their Applications. English Universities Press, 1974.

[6] *I. M. H. Etherington*: Nonassociative arithmetics. Proc. Royal Soc. Edinburgh *62* (1939), 442–453.

[7] *T. Evans*: Some remarks on a paper of R.H. Bruck. Proc. American Math. Soc. *7* (1956), 211–220.

[8] *T. Evans*: Non-associative number theory. American Math. Monthly *64* (1957), 299–309.

[9] *P. Holgate*: Plenary stable quasigroups. Comment. Math. Univ. Carolinæ *32* (1991), 1–8.

[10] *H. Popova*: Logarithmétiques des quasigroupes finis. Comptes Rendus Acad. Sci. Paris *234* (1953), 1936–1937.

[11] *H. Popova*: Sur les quasigroupes dont les logarithmétiques sont groupes. ibid. 2582–2583.
[12] *H. Popova*: Sur les vecteurs dérivés des quasigroupes unis. ibid. *235* (1953), 1360–1362.
[13] *H. Popova*: Logarithmétiques réductibles de quasigroupes. ibid. 1589–1591.
[14] *H. Popova*: L'isotopie des logarithmétiques des quasigroupes finis. ibid. *236* (1953), 769–771.
[15] *H. Popova*: Sur la logarithmétique d'une boucle. ibid. 1220–1222.
[16] *H. Popova*: Logarithmetics of finite quasigroups. I. Proc. Edinburgh Math. Soc. (2) *9* (1954), 74–81.
[17] *H. Popova*: Logarithmetics of finite quasigroups. II. ibid. (1956), 109–115.

Author's address: Department of Mathematics and Statistics, Birkbeck College, Malet Street, London WC1E 7HX, United Kingdom.