Varieties of idempotent medial quasigroups

By B. CSÁKÁNY and L. MEGYESI in Szeged

Quasigroups are algebras with three binary operations $\cdot$, $/$, and $\backslash$, called multiplication, right, and left division, respectively, which are connected by the identities

$$xy/y = y\backslash yx = (x/y)y = y(y\backslash x) = x. \tag{1}$$

A quasigroup $\mathbf{Q}$ is *idempotent* if its multiplication is idempotent. $\mathbf{Q}$ is called *medial* if, for the multiplication, the identity

$$(xy)(uv) = (xu)(yv) \tag{2}$$

holds. These two conditions — separately as well as jointly — were studied by several authors; see, e.g., STEIN [11] and BELOUSOV [2], [3].

In what follows we apply the results of the preceding paper [7] to characterize varieties of idempotent medial quasigroups, especially the variety of all such quasigroups and equationally complete varieties of them as well. The considerations we made are closely related with the recent investigations of MITSCHKE and WERNER [10]; as a matter of fact, the groupoids involved in [10] are equivalent to special idempotent medial quasigroups.

We will use the conventions of [7] without further references. We write abc instead of $(ab)c$; more generally, the absence of parentheses in any product indicates that multiplication must be performed from left to right even in the case when exponents occur; e.g., $a(bc^2)d$ denotes $\big(a((bc)c)\big)d$. Let $\mathbf{P}$ denote the ring of all rational functions of form $\dfrac{f(x)}{x^k(1-x)^l}$, where $f(x)\in\mathbf{Z}[x]$ and k, l are non-negative integers.

Theorem 1. *The variety $\mathscr{P}$ of all idempotent medial quasigroups is equivalent to the variety of all affine modules over $\mathbf{P}$. Any variety $\mathscr{R}$ of idempotent medial quasigroups is equivalent to the variety of all affine modules over some homomorphic image of $\mathbf{P}$.*

Proof. To prove that $\mathscr{R}$ is equivalent to $\mathscr{A}(\mathbf{R})$ for *some* commutative ring $\mathbf{R}$, it is enough to show that $\mathscr{R}$ is regular, idempotent, Abelian and Hamiltonian. Indeed, in this case $\mathscr{R}$ satisfies the conditions of Theorem 2 in [7].

Any variety of quasigroups is regular [6]. As Stein observed [11], in any quasigroup the idempotency of multiplication implies the idempotency of both divisions; hence $\mathscr{R}$ is idempotent. Again by [11], from mediality of multiplication follows the mediality of divisions, and so each fundamental operation in $\mathscr{R}$ commutes with itself; in order to prove that $\mathscr{R}$ is Abelian it remains to show that they commute with each other. Using (1) and (2) we obtain

$$x/y \cdot u/v = (x/y \cdot u/v)(yv)/yv = xu/yv,$$

and similarly we get the other two desired identities.

Let $\mathbf{Q} \in \mathscr{R}$ and consider an arbitrary subquasigroup $\mathbf{A}$ of $\mathbf{Q}$. Then the distinct sets of form $Aq = \{aq \mid a \in A\}$, where q is a fixed element of Q, furnish a partition of Q. Indeed, suppose $Ab \cap Ac \neq \emptyset$ $(b, c \in Q)$. We have to prove $Ab \subseteq Ac$. There exist a_1, a_2 A such that $a_1 b = a_2 c$. Take an a_3 from A; then

$$a_3 b = (a_3/a_1)b = \big((a_3/a_1)b\big)(a_1 b) = \big((a_3/a_1)b\big)(a_1 b \backslash a_2 c) = \big((a_3/a_1)(a_1 \backslash a_2)\big)c;$$

i.e., $Ab \subseteq Ac$. Now the mediality implies that this partition is compatible with the quasigroup operations, showing that A is a congruence class in $\mathbf{Q}$. Thus, the Hamiltonian property of $\mathscr{R}$ is established.

Thus, $\mathscr{R}$ is equivalent to $\mathscr{A}(\mathbf{R})$ for some $\mathbf{R}$. We have to prove that $\mathbf{R}$ is a homomorphic image of $\mathbf{P}$. The set R equipped with the ring addition and right multiplications is a free $\mathbf{R}$-module with the free generator 1. By Lemma 2 in [7], the associated affine module $\mathbf{R}^*$ is free in $\mathscr{A}(\mathbf{R})$ with the free generating set $\{0, 1\}$. Let $\mathbf{F}_2$ denote the free idempotent medial quasigroup with the same free generating set. Then there exists a weak isomorphism $\varphi: \mathbf{F}_2 \to \mathbf{R}^*$ such that $0\varphi = 0$, $1\varphi = 1$. Denote by ζ the one-to-one correspondence of the polynomials of $\mathbf{F}_2$ and $\mathbf{R}^*$ under this weak isomorphism.

Take $(\cdot)\zeta = (x, x')$. Then $1 = 1 \cdot 1 = (x, x')(1, 1) = x + x'$, whence $x' = 1 - x$. If $(/)\zeta = (u, u')$ then $1 = (1/0)0 = (1u + 0u')x + 0(1-x) = ux$, and, by idempotency of the right division, $u' = 1 - u$. If $(\backslash)\zeta = (v, v')$, then we get $v(1-x) = 1$, $v' = 1 - v$ analogously. Observe that for any $f(x) \in \mathbf{Z}[x]$, and non-negative integers k, l, the ring $\mathbf{R}$ contains the product $f(x)u^k v^l$. On the other hand, using the commutativity of $\mathbf{R}$ and the equations $ux = v(1-x) = 1$, an induction (on the number of fundamental operations occuring in the expression of elements of $\mathbf{F}_2$ over $\{0, 1\}$) shows that every element of $(\mathbf{F}_2\varphi =)\mathbf{R}$ may be written in the form $f(x)u^k v^l$. Hence there exists a homomorphism of $\mathbf{P}$ onto $\mathbf{R}$ (namely, $\dfrac{f(x)}{x^k(1-x)^l} \to f(x)u^k v^l$), proving the second part of the theorem.

Now we can assume that $\mathscr{P}$ is equivalent to $\mathscr{A}(\mathbf{R}_0)$ for some homomorphic image $\mathbf{R}_0$ of $\mathbf{P}$. It is clear from the proof of Theorem 3 in [7] that $\mathscr{A}(\mathbf{R}_0)$ is equivalent to some subvariety of $\mathscr{A}(\mathbf{P})$. But $\mathscr{A}(\mathbf{P})$ itself is equivalent to some variety of idempotent medial quasigroups. Indeed, the polynomials

$$(3) \qquad (x, 1-x), \quad \left(\frac{1}{x}, 1-\frac{1}{x}\right), \quad \left(\frac{1}{1-x}, 1-\frac{1}{1-x}\right),$$

considered as multiplication and divisions, satisfy (1); further, an induction (on the arity) shows that all polynomials of any affine module over $\mathbf{P}$ may be expressed as polynomials over (3). Thus, $\mathbf{P}$ is also a homomorphic image of $\mathbf{R}_0$, whence, using the fact that $\mathbf{P}$ is Noetherian, it follows $\mathbf{R}_0 \cong \mathbf{P}$, qu.e.d.

Corollary 1. *There exist countably many varieties of idempotent medial quasigroups.*

Theorem 2. *The equationally complete varieties of idempotent medial quasigroups coincide up to equivalence with the varieties of affine modules over finite fields except GF(2).*

Proof. In virtue of the remark at the end of [7], the varieties of quasigroups in question are equivalent to varieties of affine modules over simple quotient rings of $\mathbf{P}$. Such quotient rings are fields; we prove that they are finite. Observe that $\mathbf{P}$ is a homomorphic image of the polynomial ring $\mathbf{Z}[x_1, x_2, x_3]$, because the last one is free with the free generating set $\{x_1, x_2, x_3\}$ in the variety of commutative rings with unit element. It is known, that any maximal ideal in $\mathbf{Z}[x_1, x_2, x_3]$ has a finite index there (see [4], p. 68.). Hence the same holds for $\mathbf{P}$. Thus, the quotient fields of $\mathbf{P}$ are finite, indeed.

On the other hand, any finite field $\mathbf{K}$ consisting of at least three elements, is a homomorphic image of $\mathbf{P}$, because the correspondence $0 \to 0$, $1 \to 1$, $x \to \alpha$ (where α is a multiplicative generator of $\mathbf{K}$) may be extended to a homomorphism of $\mathbf{P}$ onto $\mathbf{K}$. The trivial fact that no polynomials of affine modules over GF(2) may be essentially binary, completes the proof.

Corollary 2. *There exist countably many equationally complete varieties of idempotent medial quasigroups.*

Theorem 2 enables us to axiomatize equationally complete varieties of idempotent medial quasigroups. Let $\mathbf{K}$ be an arbitrary finite field consisting of $q(>2)$ elements. Take a generating element α of the multiplicative group of $\mathbf{K}$. Let k be the unique integer between 0 and $q-1$ for which $\alpha^k = (1-\alpha)^{-1}$ holds; let, furthermore, for $i = 1, \ldots, q-2$ the integer $i\sigma$ $(0 < i\sigma < q-1)$ defined by the equation $\alpha^{i\sigma} = \alpha^{i+1} - \alpha + 1$. This definition fails for $i \equiv -(k+1) \pmod{(q-1)}$ if $2 \mid q$ and for $i \equiv -\left(\dfrac{q-1}{2} + k + 1\right) \pmod{(q-1)}$ if $2 \nmid q$, and so the mapping σ has a domain con-

taining $q-3$ numbers; it is one-to-one and its range does not include $q-1-k$, but $(q-1-k)\sigma$ exists always unless the domain of σ is empty.

Theorem 3. *The variety $\mathscr{K}$ of idempotent medial quasigroups determined by the further identities*

(6) $x/y = xy^{q-2}$,

(7) $y\backslash x = xy^{k}$,

(8) $xy^{i}x = xy^{i\sigma}$ if $1 \leqq i \leqq q-2$ and $i\sigma$ is defined,

(9) $xy^{i}x = y$ if $1 \leqq i \leqq q-2$ and $i\sigma$ is undefined,

is equationally complete and equivalent to $\mathscr{A}(\mathbf{K})$.

Proof. Any affine module $\mathbf{A}$ over $\mathbf{K}$ considered as a quasigroup with multiplication and divisions

(10) $(\alpha, 1-\alpha)$, $(\alpha^{-1}, 1-\alpha^{-1})$, $((1-\alpha)^{-1}, 1-(1-\alpha)^{-1})$

belongs to $\mathscr{K}$. Indeed, a routine computation shows that $\mathbf{A}$ is idempotent, medial, and the identities (6)—(9) are satisfied in it; furthermore, the familiar induction used in this paper, gives that all polynomials of $\mathbf{A}$ may be expressed as polynomials over (10). It remains to prove that $\mathscr{K}$ is equationally complete.

Observe first that (6) and (7) implies the identities

(6′) $xy^{q-1} = x$,

(7′) $yxy^{k} = x$.

Only (7′) needs a verification. Using several times the identity

(11) $(yx)y = y(xy)$

(a consequence of the idempotency and mediality) we get $yxy^{k}=y(xy^{k})=y(y\backslash x)=x$.

We establish the equational completeness of $\mathscr{K}$ by proving that any algebra $\mathbf{A}_n$ in $\mathscr{K}$, with a minimal generating set of n elements, is determined uniquely up to isomorphism. $\mathbf{A}_1$ consists of a single element. Let $\mathbf{A}_2$ be generated by the set $\{x, y\}$. We show that A_2 consists exactly of the elements

(12) $y, x, xy, \ldots, xy^{q-2}$.

For this aim we show that the product of any two elements from (12) occurs in (12) (since, in virtue of (6)—(7), divisions in $\mathbf{A}_2$ can be expressed by multiplication). This requires some computations which may be surveyed on the following table:

	y	x	xy^{t_2}
y	*	(13)	(15)
x	*	*	(16)
xy^{t_1}	*	*	(17)

Here asterisk means that product of the leading members indicating the considered row and column obviously occurs in (12); the numbers in brackets refer to the computations what follow:

(13) $yx \overset{(6')}{=} yxy^{q-1} = yxy^{k}y^{q-1-k} \overset{(7')}{=} xy^{q-1-k}$.

Hence also

(14) $xy^{t}x^{2} = xy^{q-1-k}$

follows in the case when $t\sigma$ is undefined.

(15) $y(xy^{t}) \overset{(11)}{=} yxy^{t} \overset{(6')}{=} yxy^{k}y^{q-1-k+t} \overset{(7')}{=} xy^{q-1-k+t}$.

(16) $x(xy^{t}) \overset{(6')}{=} x(xy^{t})x^{k}x^{q-1-k} \overset{(7')}{=}$

$$= xy^{t}x^{q-1-k} = \begin{cases} xy^{t\sigma}x^{q-1-k-1} & \text{by (8) for } t\sigma \text{ defined,} \\ y & \text{by (9) for } t\sigma \text{ undefined and } k = q-2, \\ xy^{q-1-k}x^{q-1-k-2} & \text{by (14) in the remainder case.} \end{cases}$$

We can iterate, if it is necessary, the last step of (16) until finally we get an expression of form y or $xy^{t'}$. The computation of $(xy^{t_1})(xy^{t_2})$ will be divided into three parts according to the cases $t_1>t_2$, $t_1=t_2(=t)$ and $t_1<t_2$.

(17_1) $(xy^{t_1})(xy^{t_2}) \overset{(2)}{=} xy^{t_1-t_2}xy^{t_2} = \begin{cases} xy^{(t_1-t_2)\sigma+t_2} & \text{by (8) for } (t_1-t_2)\sigma \text{ defined,} \\ y & \text{by (9) for } (t_1-t_2)\sigma \text{ undefined.} \end{cases}$

(17_2) $(xy^{t})(xy^{t}) = xy^{t}$.

(17_3) $(xy^{t_1})(xy^{t_2}) \overset{(2)}{=} x(xy^{t_2-t_1})y^{t_1} \overset{(16)}{=} \begin{cases} xy^{(t_2-t_1)'+t_1} & \text{or} \\ yy^{t_1} = y. \end{cases}$

Furthermore, the elements (12) are pairwise distinct. Indeed, $y=xy^{t}$ $(0<t<q-1)$ implies $y=yy^{q-1-t}=xy^{q-1}=x$ by (6′), in contrary to the assumption. From the regularity of $\mathscr{K}$, no other pairs of elements in (12) may equal. Thus we showed that $\mathbf{A}_2$ consists of the q distinct elements (12) and its multiplication table is uniquely defined.

Suppose, by induction, that $\mathbf{A}_n$ $(n\geqq 2)$ is unique, and let the minimal generating set of $\mathbf{A}_{n+1}$ be $\{x_0, x_1, \ldots, x_n\}$. Then $[x_0, x_1]$ and $[x_1, \ldots, x_n]$ are isomorphic to $\mathbf{A}_2$ and $\mathbf{A}_n$, respectively. Clearly, $[x_0, x_1]\cup[x_1, \ldots, x_n]$ generates $\mathbf{A}_{n+1}$. On the other hand, $[x_0, x_1]\cap[x_1, \ldots, x_n]=x_1$, since if $x\in[x_0, x_1]\cap[x_1, \ldots, x_n]$ holds for $x\neq x_1$, then $[x, x_1]\cong\mathbf{A}_2\cong[x_0, x_1]$, whence $[x, x_1]=[x_0, x_1]$, i.e., $[x_0, x_1]\subseteq[x_1, \ldots, x_n]$, denying the minimality of $\{x_0, x_1, \ldots, x_n\}$. Hence we can apply Lemma 1 from [7]: $\mathbf{A}_{n+1}\cong$ $\cong\{x_0, x_1]\times[x_1, \ldots, x_n]\cong\mathbf{A}_2\times\mathbf{A}_n$, and so $\mathbf{A}_{n+1}$ is unique up to isomorphism. Thus, $\mathscr{K}$ is equationally complete, ending the proof of the Theorem.

Corollary 3. *Equationally complete varieties of idempotent medial quasigroups are equivalent to varieties of groupoids.*

Remarks 1. The varieties $\mathscr{G}(n, k)$ of groupoids, discussed in [10], are also, in fact, equivalent to varieties of idempotent medial quasigroups. Indeed, as it is shown there, $\mathscr{G}(n, k)$ is equivalent to $\mathscr{A}(\mathbf{R}(n, k))$, where $\mathbf{R}(n, k)=\mathbf{Z}[x]/(x^n-1, x^k+x-1)$. Now, for any natural numbers $k<n$, $\mathbf{R}(n, k)$ is a homomorphic image of $\mathbf{P}$ under the homomorphism $\dfrac{f(x)}{x^u(1-x)^v}\to f(r)r^{(n-1)u+(n-k)v}$, where $r=x+(x^n-1, x^k+x-1)$ in $\mathbf{R}(n, k)$. Hence $\mathscr{G}(n, k)$ is equivalent to a subvariety of $\mathscr{P}$; i.e., it is equivalent to some variety $\mathscr{P}_{n,k}$ of idempotent medial quasigroups. Note that $\mathscr{P}_{n,k}$ may be axiomatized by the identities $x/y=xy^{n-1}$, $y\backslash x=xy^{n-k}$.

2. The solution of Płonka's problem (Corollary 7 in [10]) can be derived from the above considerations as well. Let $\mathscr{G}$ be the variety of groupoids satisfying the identities $x^2=x$, $x(yx)=y$ and $xyz=zyx$. The last identity implies the mediality; defining x/y by yx and $y\backslash x$ by xy, $\mathscr{G}$ becomes a variety of quasigroups, which is clearly equivalent to $\mathscr{G}$. By Theorem 1, $\mathscr{G}$ is equivalent to $\mathscr{A}(\mathbf{R})$ for some ring $\mathbf{R}$, generated by an element α, such that the operation $(\alpha, 1-\alpha)$ of $\mathscr{A}(\mathbf{R})$ corresponds to the multiplication of $\mathscr{G}$. Then Płonka's second and third identities, rewritten with the aid of α, give $\alpha^2=1-\alpha$ and $\alpha(1-\alpha)=1$, and this implies that $\mathbf{R}\cong GF(4)$; i.e., $\mathscr{G}$ is equivalent to $\mathscr{A}(GF(4))$.

3. The characterization of medial Steiner triple systems (Corollary 8 in [10]) as affine modules over $GF(3)$ is even the special case $\mathbf{K}=GF(3)$ of Theorem 3. For related results, see [1] and [9].

4. Algebras with one ternary operation τ which commutes with itself and satisfies the identity

$$\tau(x, x, y)=\tau(x, y, x)=\tau(y, x, x)=y \tag{18}$$

were discussed by Aliev [1], who called them S^*-algebras. Aliev's results jointly with Givant's characterization of varieties in which all members are free [8] imply that the variety $\mathscr{S}^*$ of all S^*-algebras is equivalent to $\mathscr{A}(GF(2))$. This fact can be deduced also from our considerations as follows. Obviously, $\mathscr{S}^*$ is idempotent and Abelian; further the defining identities involve that the S^*-algebras are essentially flocks with commutative covering groups ([5], p. 40), whence $\mathscr{S}^*$ is regular and Hamiltonian. Then Theorem 2 in [7] shows that $\mathscr{S}^*$ is equivalent to $\mathscr{A}(\mathbf{R})$ for some commutative ring $\mathbf{R}$. Now the routine discussion of the identities (18) furnishes that $\mathbf{R}$ is generated by its unit element, and $1=-1$ in $\mathbf{R}$. Hence $\mathbf{R}\cong GF(2)$.

References

[1] I. S. o. Aliev, On the minimal variety of symmetric algebras, *Algebra i Logika*, **5**: 6 (1966), 5—14. (Russian)

[2] V. D. Belousov, *Foundations of the theory of quasigroups and loops*, Nauka (1967). (Russian)

[3] V. D. Belousov, Transitive distributive quasigroups, *Ukr. Mat. Ž.*, **10** (1958), 13—22. (Russian)

[4] N. Bourbaki, *Éléments de Mathématique XXX, Algèbre commutative*, Hermann, Paris 1964.

[5] R. H. Bruck, *A survey of binary systems*, Springer (1958).

[6] B. Csákány, Characterizations of regular varieties, *Acta Sci. Math.*, **31** (1970), 187—189.

[7] B. Csákány, Varieties of affine modules, *Acta Sci. Math.*, **37** (1975), 3—10.

[8] S. R. Givant, A representation theorem for universal classes of algebras in which all members are free, *Notices AMS*, **19**: 7 (1972), p. A—767.

[9] G. Grätzer, P. Padmanabhan, On idempotent, commutative and nonassociative groupoids, *Proc. Amer. Math. Soc.*, **28**: 1 (1971), 75—80.

[10] A. Mitschke, H. Werner, On groupoids representable by vector spaces over finite fields, *Archiv der Math.*, **24** (1973), 14—20.

[11] S. K. Stein, On the foundations of quasigroups, *Trans, Amer. Math. Soc.*, **85** (1957), 228—256.

(Received June 5, 1973)