MEDIAL IDEMPOTENT GROUPOIDS III

JUNG R. CHO and JÓZEF DUDEK

(Received 7 October 1998; revised 6 September 1999)

Communicated by B. A. Davey

Abstract

As a sequel to the previous two papers of the second author, we investigate the structure of medial idempotent groupoids by p_n -sequences. To complete the series of research, this paper has three purposes. First, we summarize some results in the previous papers so that this paper can cover the materials presented there. Secondly, using earlier results, we prove a few theorems which show the importance of the medial law in controlling the growth of p_n -sequences of groupoids. Finally, we state some problems and conjectures raised during the series of research.

2000 Mathematics subject classification: primary 08A40, 20N02.

1. Introduction

In the class of groupoids, the idempotent law and the medial law have received a special attention because they appear very naturally in most branches of mathematics, and many authors have studied medial idempotent groupoids with many different approaches, sometimes under different names [26]. Especially, the medial law has received about ten different names in many different areas [1], and much research has been done on this identity by Ježek and Kepka in their monograph [19].

In this paper, as in the earlier papers of this series [10, 12], we approach medial idempotent groupoids by means of the number of essential term functions. Characterizing the structure of a groupoid or any algebra in general by its p_n -sequence has been an active research problem for many years, and it turned out that the p_n -sequence gives much information about an algebra, especially when the algebra is idempotent.

The first author was supported by the academic research fund of Ministry of Education, Republic of Korea, Project No. BSRI-97-1433.

^{© 2000} Australian Mathematical Society 0263-6115/2000 \$A2.00 + 0.00

It is also true that the p_n -sequence is very hard to determine without the idempotent law. Many results on p_n -sequences of algebras are collected in the valuable survey article of Grätzer and Kisielewicz [17] with a detailed history, references and open problems. It is shown in [1] that the variety of medial idempotent groupoids and the variety of commutative idempotent groupoids are generated by affine spaces over prime fields, and so it is not surprising that affine spaces play a very important role in characterizing those groupoids in this way.

For an algebra **A**, we denote by $p_n(\mathbf{A})$ the number of essentially n-ary term functions (or simply 'terms') of **A** for all $n \ge 1$. Note that $p_0(\mathbf{A})$ is the number of all constant unary terms of **A**. The sequence $(p_0(\mathbf{A}), p_1(\mathbf{A}), p_2(\mathbf{A}), \dots)$ is called the p_n -sequence of the algebra **A**. Two algebras with the same set of term functions are said to be *term* equivalent and it is clear that term equivalent algebras have the same p_n -sequence. In this paper, we will treat term equivalent algebras as the same algebras.

A groupoid is called *proper* if the fundamental operation is essentially binary. A groupoid is called an *n*-polynomial groupoid if $p_n(G, \cdot) = n$ for all n, and these groupoids are completely characterized in [24].

For further concepts and terminology not defined in this paper, we refer the readers to [10, 16], especially for the definition of a Płonka sum of algebras. We will say a Płonka sum of algebras is *proper* if the semilattice ordered system for the sum is not trivial and the algebras involved in the sum are not all trivial.

For simplicity, we use xy^n for the term $(\cdots((xy)y)\cdots)y$ with y repeated n times, and use $x_1x_2\cdots x_n$ for $(\cdots((x_1x_2)x_3)\cdots)x_n$. We also use the following notations.

 V_i : the variety of all idempotent groupoids,

 V_{ci} : the variety of all commutative idempotent groupoids,

 $V_{\rm mi}$: the variety of all medial idempotent groupoids,

 $V_{
m mci}$: the variety of all medial commutative idempotent groupoids,

SL: the variety of all semilattices,

DSQ: the variety of all distributive Steiner quasigroups,

NG: the class of all n-polynomial groupoids,

RB: the class of all proper rectangular bands,

Aff(q): the class of all nontrivial affine spaces over GF(q),

PA(q): the class of all proper Płonka sums of affine spaces over GF(q),

where GF(q) is the Galois field with q elements.

Affine spaces are introduced in [22], and it is proved in [25] that, for a prime number p, if $(A, F) \in Aff(p)$ then (A, F) is term equivalent to the algebra (A, f) for any essentially n-ary operation f in F with $n \ge 2$. Thus, we regard Aff(p) as the class of groupoids (G, ((p+1)/2)(x+y)), where (G, +) is an Abelian group of exponent p (see also [10]). Then it is clear to see that $Aff(p) \subseteq V_{mci}$. By [23], it also follows that $PA(p) \subseteq V_{mci}$.

2. Some characterization of affine spaces

In this section, we summarize the main results of the previous two papers of this series of research and some other results related to them so that this paper can be used as a reference in the future.

The following are the main results of the previous two papers of this series of research.

THEOREM 2.1 ([10, 12]). Let (G, \cdot) be a nontrivial groupoid in V_{mi} . Then,

- (i) $p_2(G, \cdot) = 0$ if and only if (G, \cdot) satisfies xy = x or xy = y;
- (ii) $p_2(G, \cdot) = 1$ if and only if $(G, \cdot) \in SL \cup Aff(3)$;
- (iii) $p_2(G, \cdot) = 2$ if and only if $(G, \cdot) \in NG \cup RB \cup Aff(4)$;
- (iv) $p_2(G, \cdot) = 3$ if and only if $(G, \cdot) \in Aff(5) \cup PA(3)$;
- (v) $p_2(G, \cdot) = 5$ if and only if $(G, \cdot) \in Aff(7) \cup PA(5)$.

In the proof of the Theorem 2.1, the following result was critical.

THEOREM 2.2 ([10]). If $(G, \cdot) \in V_{\text{mi}}$ and $p_3(G, \cdot) = 3$ then (G, \cdot) is term equivalent to a groupoid in V_{mci} .

The next two theorems give more results related to Theorem 2.1 and explain some results of the theorem in more detail.

THEOREM 2.3. Let (G, \cdot) be a nontrivial groupoid in V_{mci} . Then,

- (i) $(G, \cdot) \in SL$ if and only if either $xy^2 \in \{xy, yx^2, xy^3\}$ or $xy^2x \in \{yx^2y, yx^2, xy^3, yx^3\}$ ([6, 12]);
 - (ii) $(G, \cdot) \in Aff(3)$ if and only if $xy^2x = x$ (equivalently $xy^2 = x$) ([10, 18]);
 - (iii) $(G, \cdot) \in Aff(5)$ if and only if $xy^2x = y$ ([10, 18]);
 - (iv) $(G, \cdot) \in Aff(5)$ if and only if $xy^3 = yx^2$ and $p_2(G, \cdot) = 3$ ([10]);
 - (v) $(G, \cdot) \in Aff(7)$ if and only if it $xy^3 = x$ ([12]);
- (vi) $(G, \cdot) \in PA(3)$ if and only if $(G, \cdot) \notin SL$ and either $xy^2x = xy^2$, $xy^3 = yx^3$ or $xy^3 = xy$ ([12]);
 - (vii) (G, \cdot) is an affine module over \mathbb{Z}_d with $d \mid 2^n 1$ if and only if $xy^n = x$ ([4]);
- (viii) (G, \cdot) is a Plonka sum of affine modules over \mathbb{Z}_d with $d \mid 2^n 1$ if and only if $xy^{n+1} = xy$ ([6]).

THEOREM 2.4 ([10, 12]). Let (G, \cdot) be a nontrivial groupoid in V_{mi} . Then,

- (i) if $xy^3 = yx^2$, then $(G, \cdot) \in Aff(5)$ if and only if $p_2(G, \cdot) = 3$;
- (ii) if $xy^2 = x$ or $xy^2 = yx^2$, then $(G, \cdot) \in Aff(7)$ if and only if $p_2(G, \cdot) = 5$;
- (iii) if $xy^3 = xy$, then $(G, \cdot) \in PA(3)$ if and only if $p_2(G, \cdot) = 3$;
- (iv) if $xy^2 = yx$, then $(G, \cdot) \in PA(5)$ if and only if $p_2(G, \cdot) = 5$.

3. p_n -sequences and the medial law

In this section, we present a few theorems which show how easily the medial law is implied even by a relatively loose restriction on the growth of p_n -sequences. First, we recall some known results for the later use.

- LEMMA 3.1. (i) Let $(G, \cdot) \in V_i$. Then $p_2(G, \cdot) < 6$ if and only if $(G, \cdot) \in SL \cup DSQ \cup RB \cup NG$ ([7]).
- (ii) If $(G, \cdot) \in V_{ci}$ and $(G, \cdot) \notin Aff(3) \cup SL$, then $p_n(G, \cdot) \geq 3^{n-1}$ for all $n \geq 4$ ([8]).
 - (iii) $NG \subseteq V_{mi}$ ([13]).
- (iv) If $(G, \cdot) \in V_i$ and $(G, \cdot) \notin Aff(2) \cup SL \cup RB$, then $p_{n+1}(G, \cdot) \geq p_n(G, \cdot) + 1$ for all $n \geq 2$ ([20]).

THEOREM 3.1. If (G, \cdot) is a nontrivial groupoid in V_i such that $p_n(G, \cdot) \leq n$ for some $n \geq 4$, then (G, \cdot) is medial.

PROOF. Suppose that $p_n(G, \cdot) \leq n$ for some $n \geq 4$. We claim that $p_3(G, \cdot) < 6$. Assume $p_3(G, \cdot) \geq 6$. Then $(G, \cdot) \notin SL \cup RB \cup Aff(2)$, since $p_3(G, \cdot) \leq 2$ otherwise. Thus, by Lemma 3.1(iv), we have that $p_{n+1}(G, \cdot) \geq p_n(G, \cdot) + 1$ for all $n \geq 2$. Then, for all $n \geq 3$, we have that $p_n(G, \cdot) \geq p_{n-1}(G, \cdot) + 1 \geq p_{n-2}(G, \cdot) + 2 \geq \cdots \geq p_3(G, \cdot) + (n-3) \geq 6 + (n-3) = n+3$, which is a contradiction to our hypothesis. Thus, $p_3(G, \cdot) < 6$ as we claimed. Now, by Lemma 3.1(i), $(G, \cdot) \notin SL \cup RB \cup NG \cup DSQ$. Obviously, (G, \cdot) is medial if $(G, \cdot) \in SL \cup RB$. By Lemma 3.1(iii), (G, \cdot) is medial if $(G, \cdot) \in SL \cup RB$. By Lemma 3.1(iii), $(G, \cdot) \in Aff(3)$ by Lemma 3.1(ii) and so (G, \cdot) is medial.

REMARK 3.1. We note that the bound $n \ge 4$ in the above theorem is the best possible. In fact, a distributive Steiner quasigroup has only three ternary terms, namely (xy)z, (yz)x and (zx)y, but there exist nonmedial distributive Steiner quasigroups [27].

Following [15], we say that a sequence $\mathbf{a} = (a_0, a_1, a_2, \dots)$ has a subexponential growth if there exists a positive constant c such that $a_n \le c^n$ for all n, and that \mathbf{a} has a subpolynomial growth if there exists a polynomial $\varphi(x)$ in $\mathbb{Z}[x]$ such that $a_n \le \varphi(n)$ for all n.

An identity is called regular if both sides of the identity involve the same variables.

THEOREM 3.2. If $(G, \cdot) \in V_{ci}$ and the p_n -sequence of (G, \cdot) has a subexponential growth, then (G, \cdot) is medial.

PROOF. Assume that $(G, \cdot) \in V_{ci}$ and there is a constant c such that $p_n(G, \cdot) \le c^n$ for all n. Using [15, Theorem 3], we can deduce that (G, \cdot) is a semilattice, an affine space over \mathbb{Z}_d or a Płonka sum of affine spaces over \mathbb{Z}_d for some odd integer d. A semilattice is obviously medial. An affine space over \mathbb{Z}_d is term equivalent to a groupoid (G, ((d+1)/2)(x+y)) for some Abelian group (G, +) of exponent d (see [6]), which is certainly medial. Note that a Płonka sum of groupoids preserves regular identities common to all groupoids involved in the sum (see [23]). Since affine spaces are medial and the medial law is a regular identity, Płonka sums of affine modules are also medial.

THEOREM 3.3. If $(G, \cdot) \in V_{ci}$ and the p_n -sequence of (G, \cdot) has a subpolynomial growth, then (G, \cdot) is a semilattice (and hence medial).

PROOF. Assume that $(G, \cdot) \in V_{ci}$ and $p_n(G, \cdot) \leq \varphi(n)$ for some polynomial $\varphi(x)$ in $\mathbb{Z}[x]$ and for all n. Then there exist a positive integer k and a constant c such that $p_n(G, \cdot) < cn^k$ for all n. Then, by [15, Theorem 2], (G, \cdot) is a semilattice and hence medial.

REMARK 3.2. Theorem 3.3 is not true in general if the groupoid is not commutative. In fact, we find in [3] noncommutative idempotent nonmedial groupoids (G, \cdot) with $p_n(G, \cdot) = n^2$ for all n.

Now we introduce some earlier results which are useful to prove the next theorem.

LEMMA 3.2. (i) If $(G, \cdot) \in V_{ci}$ then $xy^n \neq y$ in (G, \cdot) for all n ([5]).

- (ii) If $(G, \cdot) \in V_i$, then $(G, \cdot) \in SL$ if and only if (G, \cdot) is a distributive commutative groupoid satisfying $xy^2 = yx^2$ ([6]).
- (iii) If $(G, \cdot) \in V_{mci}$, xy^2 is essentially binary and $xy^2 \neq yx^2$, then $p_n(G, \cdot) \geq 3^{n-1}$ for all $n \geq 1$ ([8]).

THEOREM 3.4. If $(G, \cdot) \in V_{ci}$ and $p_2(G, \cdot) > 1$, then xy^2 is essentially binary and $p_n(G, \cdot) \geq 3^{n-1}$ for all $n \geq 4$. If, in addition, (G, \cdot) is medial, then $xy^2 \neq yx^2$ and $p_n(G, \cdot) \geq 3^{n-1}$ for all $n \geq 1$.

PROOF. Suppose $(G, \cdot) \in V_{ci}$ and $p_2(G, \cdot) > 1$. Since $p_2(G, \cdot) > 1$, we infer that (G, \cdot) is not a semilattice and $(G, \cdot) \notin Aff(3)$ by Theorem 2.1. Then, by Lemma 3.1(iii), we obtain that $p_n(G, \cdot) \geq 3^{n-1}$ for all $n \geq 4$. If $xy^2 = x$ then (G, \cdot) is a Steiner quasigroup and so $p_2(G, \cdot) \leq 1$, a contradiction. By Lemma 3.2(i), we have $xy^k \neq y$ for all k, and hence $xy^2 \neq y$. Thus xy^2 is essentially binary. Suppose, furthermore, that (G, \cdot) is medial. Then (G, \cdot) is distributive by the medial law and the idempotent law. If $xy^2 = yx^2$ then $(G, \cdot) \in SL$ by Lemma 3.2(ii) and so

 $p_2(G, \cdot) = 1$, a contradiction. Hence $xy^2 \neq yx^2$. Then, by Lemma 3.2(iii), we obtain that $p_n(G, \cdot) \geq 3^{n-1}$ for all $n \geq 1$, which completes the proof.

4. The medial law and minimal clones

A set of term functions of an algebra is called a *clone* of the algebra if it contains all projections and is closed under taking compositions. A clone is called *minimal* if it properly contains only the trivial clone, that is, the clone consisting of projections only.

LEMMA 4.1. Let $(G, \cdot) \in V_{ci}$ satisfy $xy^n = x$ for some $n \ge 2$. Then the clone of (G, \cdot) is minimal if and only if $(G, \cdot) \in Aff(p)$ for some prime p dividing $2^n - 1$ (compare with Theorem 2.3(vii)).

THEOREM 4.1. Let $(G, \cdot) \in V_{ci}$.

- (i) If (G, \cdot) satisfies $xy^n = x$ for some $n \ge 1$ and the clone of (G, \cdot) is minimal then (G, \cdot) is medial.
- (ii) If (G, \cdot) is a cancellative groupoid and $p_2(G, \cdot)$ is finite, then the clone of (G, \cdot) is minimal if and only if $(G, \cdot) \in Aff(p)$ for some prime $p \ge 3$.
- PROOF. (i) follows from the Lemma 4.1, since any affine space over GF(p) with $p \ge 3$ is term equivalent to the medial groupoid (G, ((p+1)/2)(x+y)) by Lemma 3.1, where (G, +) is an Abelian group of exponent p. (ii) Since $p_2(G, \cdot)$ is finite, we see that the mapping $k \mapsto xy^k$ is not injective. Thus $xy^i = xy^j$ for some distinct integers i and j, say $j \ge i$. Then, by the cancellativity, we have that $xy^{j-i} = x$ and the conclusion follows by Lemma 4.1.

THEOREM 4.2. Let **A** be an algebra with $p_2(\mathbf{A}) = 3$. Then the following statements are equivalent.

- (i) $\mathbf{A} \in \mathrm{Aff}(5)$.
- (ii) The clone of A is minimal.
- (iii) $A \in V_{mci}$ and A satisfies $xy^2x = y$.
- (iv) A is a groupoid with $p_n(A) = (4^n (-1)^n)/5$ for all n.
- (v) $A \in V_{mi}$ and A satisfies a nonregular identity.

PROOF. (i) is equivalent to (ii) by [9]. (i) is equivalent to (iii) by Theorem 2.3(iii). (i) is equivalent to (iv) by [2] and [11]. Clearly (iii) implies (v). It remains only to show (v) implies (i). By Theorem 2.1, $A \in PA(3)$ or $A \in Aff(5)$. Since a Płonka sum satisfies only regular identities (see [23]), we have the latter case.

THEOREM 4.3. Let A be an algebra with $p_2(A) = 5$. Then the following statements are equivalent.

- (i) $A \in Aff(7)$.
- (ii) The clone of A is minimal.
- (iii) $A \in V_{mci}$ and A satisfies $xy^3 = x$.
- (iv) $A \in V_{mi}$ and A satisfies a nonregular identity.

PROOF. (i) is equivalent to (ii) by [14] and (i) is equivalent to (iii) by Theorem 2.3(v). Clearly (iii) implies (iv). We prove (iv) implies (i). By Theorem 2.1, $A \in PA(5)$ or $A \in Aff(7)$. Since a Płonka sum satisfies only regular identities, $A \in Aff(7)$.

5. Problems and conjectures

We present here some problems and conjectures.

PROBLEM 5.1. Characterize all medial idempotent groupoids (G, \cdot) with $p_2(G, \cdot) = 2d - 1$ for some d > 1. Is it true that if $p_2(G, \cdot) = 2d - 1$, then (G, \cdot) is a medial idempotent groupoid if and only if (G, \cdot) is an affine module over \mathbb{Z}_{2d+1} or a proper Płonka sum of affine modules over \mathbb{Z}_{2d-1} (see Theorem 2.3 (vii) and (viii))? Note that the problem is solved in the positive for d = 2, 3 ([10, 12]). In these cases, the affine modules in question are simply affine spaces.

PROBLEM 5.2. Characterize medial idempotent groupoids (G, \cdot) with $p_2(G, \cdot) = 4$. Note that all medial idempotent groupoids with $p_2(G, \cdot) \in \{0, 1, 2, 3, 5\}$ were classified (Theorem 2.1).

PROBLEM 5.3. Characterize medial idempotent groupoids (G, \cdot) satisfying a non-regular identity and $p_2(G, \cdot) = p$ for a prime number p. Are these groupoids affine spaces over GF(p)? (See theorems in Section 4.)

CONJECTURE 5.4. For a prime number $p \ge 3$, the following statements are equivalent for a nontrivial groupoid (G, \cdot) .

- (i) (G, \cdot) is a nontrivial affine space over GF(p).
- (ii) $p_n(G, \cdot) = ((p-1)^n (-1)^n)/p$ for all n.
- (iii) The sequence $(0, 1, p-2, p^2-3p+3, (p-2)(p^2-2p+2))$ determines the p_n -sequence of (G, \cdot) in the class of all groupoids.

In [14], it was conjectured that the statement (i) of Conjecture 5.4 is equivalent to the following.

(iv) The clone of (G, \cdot) is minimal and $p_2(G, \cdot) = p - 2$ for all $p \ge 5$.

However, Lévai and Pálfy [21] showed that this conjecture is not true for prime numbers of the form 3k + 2 with $k \ge 2$. Note that the equivalence of (i) and (iv) is true for p = 5 and p = 7. For p = 3, the equivalence of all the above statements is true [12, 18].

References

- [1] J. R. Cho, Varieties of medial algebras (Ph. D. Thesis, Emory University, Atlanta, 1986).
- [2] B. Csákány, 'On affine spaces over prime fields', Acta Sci. Math. (Szeged) 37 (1975), 33-36.
- [3] S. Crvenković and J. Dudek, 'Rectangular groupoids', Czechoslovak Math. J. 35 (1985), 405-414.
- [4] J. Dudek, 'Medial groupoids and Mersenne's numbers', Fund. Math. 114 (1981), 109-112.
- [5] —, 'On binary polynomials in idempotent commutative groupoids', Fund. Math. 120 (1984), 187–191.
- [6] ——, 'Varieties of idempotent commutative groupoids', Fund. Math. 120 (1984), 193-204.
- [7] ——, 'Polynomial characterization of some idempotent algebras', Acta Sci. Math. (Szeged) 50 (1986), 39-49.
- [8] —, 'Polynomials in idempotent commutative groupoids', *Dissertationes Math.* **286** (1989), 1–55.
- [9] —, 'The unique minimal clone with three essentially binary operations', *Algebra Universalis* 27 (1990), 201–209.
- [10] ——, 'Medial idempotent groupoids I', Czechoslovak Math. J. 41 (1991), 249–259.
- [11] ——, 'On Csákány's problem concerning affine spaces', Acta Sci. Math. (Szeged) 46 (1992), 3-13.
- [12] ——, 'Medial idempotent groupoids II', in: *Proceeding of the workshop on general algebra*, Contribution to general algebras 9 (Linz, 1994), pp. 133–150.
- [13] —, 'On varieties of groupoid modes', Demonstratio Math. 27 (1994), 815–818.
- [14] —, 'Another unique minimal clone', preprint.
- [15] J. Dudek and A. Kisielewicz, 'Idempotent algebras with log-linear free spectra', Algebra Universalis 28 (1991), 119–127.
- [16] G. Grätzer, Universal algebra, 2nd edition, (Springer, New York, 1979).
- [17] G. Grätzer and A. Kisielewicz, 'A survey of some open problems on p_n -sequences and free spectra of algebras and varieties', in: *Universal algebra and quasigroup theory* (eds. A. Romanowska and J. D. H. Smith), (Helderman, Berlin, 1992), pp. 57–88.
- [18] G. Grätzer and R. Padmanabhan, 'On commutative, idempotent and nonassociative groupoids', Proc. Amer. Math. Soc. 28 (1971), 75-78.
- [19] J. Ježek and T. Kepka, 'Medial groupoids', Rozpravy ČSAV, Řada Mat. Přírod. Věd 93 (1983).
- [20] A. Kisielewicz, 'The p_n-sequences of idempotent algebras are strictly increasing II', Algebra Universalis 27 (1990), 261-269.
- [21] L. Lévai and P. Pálfy, 'On binary minimal clones', Acta Cybernet. 12/3 (1996), 279-294.
- [22] F. Ostermann and J. Schmidt, 'Der baryzentrische Kalkül als axiomatische Grundlage der affinen Geometrie', J. Reine Angew. Math. 224 (1966), 44-57.
- [23] J. Płonka, 'On equational classes of abstract algebras defined by regular equations', Fund. Math. 64 (1969), 241-247.
- [24] ——, 'On algebras with *n* distinct essentially *n*-ary operations', *Algebra Universalis* 1 (1971), 73–79.
- [25] ----, 'R-prime idempotent reduct of abelian groups', Archiv. Math. (Basel) 24 (1973), 129-132.

- [26] A. Romanowska and J. D. H. Smith, Modal theory, an algebraic approach to order, geometry and convexity (Helderman, Berlin, 1985).
- [27] J. Soublin, 'Étude algébrique de la notion de moyenne', J. Math. Pures Appl. 50 (1971), 53-264.

Department of Mathematics
Pusan National University
Pusan 609-735
Korea
e-mail: jungcho@hyowon.pusan.ac.kr

Mathematical Institute University of Wrocław pl. Grunwaldzki 2/4 50-384 Wrocław Poland

e-mail: dudek@math.uni.wroc.pl