On binary polynomials in idempotent commutative groupoids

by

J. Dudek (Wrocław)

Abstract. In this paper one estimates the number of essentially binary polynomials in idempotent and commutative groupoids (Theorem 3, 4 and 5).

1. Introduction. Let $\mathfrak{A} = (A, F)$ be an algebra. We denote by $A^{(n)}(\mathfrak{A}) = \bigcup_{k=0}^{\infty} A_k^{(n)}(\mathfrak{A})$ the set of all n-ary polynomials in $\mathfrak{A}$, where $A_0^{(n)} = A_0^{(n)}(\mathfrak{A}) = \{e_1^{(n)}, \ldots, e_n^{(n)}\}$, and $A_{k+1}^{(n)} = A_{k+1}^{(n)}(\mathfrak{A}) = A_k^{(n)}(\mathfrak{A}) \cup \{f(f_1, \ldots, f_m): f \in \boldsymbol{F}, f_1, \ldots, f_m \in A_k^{(n)}(\mathfrak{A})\}$ (see [3]). By $p_n(\mathfrak{A})$ we denote the number of all essentially n-ary polynomials in $\mathfrak{A}$ ([2]).

If $(G, \cdot)$ is a groupoid, then, xy^n stands for the expression $(\ldots(xy)\cdot \ldots \cdot y)y$ where x occurs once and y occurs n times.

The class of all idempotent and commutative groupoids $(G, \cdot)$ is denoted by $V(\cdot)$. For a fixed $n \geqslant 1$ we denote by $V_n(\cdot)$ the subvariety of $V(\cdot)$ of all groupoids $(G, \cdot)$ which satisfy $xy^n = x$.

A groupoid $(G, \cdot)$ is called *medial* if it satisfies the medial law, i.e., $(xy)(uv) = (xu)(yv)$ for all $x, y, u, v \in G$.

In this paper we prove the following theorems.

THEOREM 1. *If $(G, \cdot) \in V(\cdot)$ and $\operatorname{card} G \geqslant 2$, then $xy^n \neq y$ for all n.*

THEOREM 2. *If $(G, \cdot) \in V(\cdot)$ and $\operatorname{card} G \geqslant 2$ and xy^s is not essentially binary for a certain $s \geqslant 1$, then there exists an n such that* (1) $(G, \cdot) \in V_n(\cdot)$, (2) $(G, \cdot) \notin V_k(\cdot)$ *for all* $1 \leqslant k \leqslant n-1$ *and* (3) $(G, \cdot)$ *is a quasigroup.*

THEOREM 3. *Suppose $(G, \cdot) \in V_n(\cdot)$ for a certain $n \geqslant 2$ and $(G, \cdot) \notin V_k(\cdot)$ for all $k < n$. Then $(G, \cdot)$ contains at least $2n-1$ essentially binary polynomials if n is odd and at least $n-1$ essentially binary polynomials if n is even.*

THEOREM 4. *If $(G, \cdot) \in V(\cdot)$ and $xy^2 = yx^2$, then every essentially binary polynomial f over $(G, \cdot)$ is symmetric (i.e., $f(x, y) = f(y, x)$), and it is of the form: $f(x, y) = xy^n$ for some $n \geqslant 1$.*

THEOREM 5. *If $(G, \cdot) \in V(\cdot)$, $\operatorname{card} G \geqslant 2$ and $(G, \cdot)$ is medial, then the number of all essentially binary polynomials over $(G, \cdot)$ is odd or infinite.*

2. Lemmas and proofs of theorems. The proof of Theorem 1 can be found in an earlier published paper [1]. Here we give the same proof for the sake of completeness.

Proof of Theorem 1. Assume that $xy^n = y$ for all $x, y \in G$ and that n is the smallest such number. Since xy is essentially binary, we have $n > 1$. Then we get

$$\begin{aligned} xy^{n-1} &= y(xy^{n-1})^n = \big(y(xy^{n-1})\big)(xy^{n-1})^{n-1} = \big((xy^{n-1})y\big)(xy^{n-1})^{n-1} \\ &= (xy^n)(xy^{n-1})^{n-1} = y(xy^{n-1})^{n-1} = \big(y(xy^{n-1})\big)(xy^{n-1})^{n-2} \\ &= \big((xy^{n-1})y\big)(xy^{n-1})^{n-2} = (xy^n)(xy^{n-1})^{n-2} = y(xy^{n-1})^{n-2} = \ldots \\ \ldots &= y(xy^{n-1}) = (xy^{n-1})y = xy^n = y. \end{aligned}$$

So, we have a contradiction $xy^{n-1} = y$.

Proof of Theorem 2. By Theorem 1 there exists a smallest $n \geqslant 1$ such that $xy^n = x$ in $(G, \cdot)$, because xy is idempotent. Now, xy^k is essentially binary for all $1 \leqslant k \leqslant n-1$. Hence $(G, \cdot) \notin V_k(\cdot)$. We prove that the groupoid is a quasigroup. Indeed, if $x_1 a = x_2 a$, then $x_1 = x_1 a^n = (x_1 a)a^{n-1} = (x_2 a)a^{n-1} = x_2 a^n = x_2$. It is clear that $x = ba^{n-1}$ is a solution of the equation $x \cdot a = b$. This completes the proof.

Proof of Theorem 3. Let $(G, \cdot) \in V_n(\cdot)$ for a certain $n \geqslant 2$ and let $(G, \cdot) \notin V_k(\cdot)$ for every $k < n$. Observe that if at least one of the polynomials $x(xy)^k$, where $k = 1, \ldots, n-1$, is not essentially binary, then n is even. Indeed, let $x(xy)^k = x$ for some k. Then, putting yx^{n-1} for y, we get $x = x\big(x(yx^{n-1})\big)^k = x\big((yx^{n-1})x\big)^k = x(yx^n)^k = xy^k$, which proves that $(G, \cdot) \in V_k(\cdot)$, which is impossible. Let $x(xy)^k = y$ for a certain $1 \leqslant k < n$. Then $x = x(xy)^n = \big(x(xy)^k\big)(xy)^{n-k} = y(xy)^{n-k}$ and $y = x(xy)^k = x(yx)^{n-k} = x(xy)^{n-k}$. If $n-k \neq k$, then from (3) of Theorem 2 we infer that $(G, \cdot)$ is cancellative, whence $x(xy)^s = x$ for some $1 \leqslant s \leqslant n-1$, which gives a contradiction with the case considered above. We have thus proved that if $x(xy)^k$, for a certain $1 \leqslant k < n$, is not essentially binary, then n is even. Moreover $k = n/2$.

Case 1. n is odd. From the above remark we see that the polynomials $x(xy)^k$ are essentially binary for all $k = 1, \ldots, n-1$.

By (3) of Theorem 2, $(G, \cdot)$ is a quasigroup. Hence the polynomials $xy, x(xy), y(yx), x(xy)^2, y(yx)^2, \ldots, x(xy)^{n-1}, y(yx)^{n-1}$ are different, and so $p_2(G, \cdot) \geqslant 2n-1$.

Case 2. n is even. If the polynomials $x(xy)^k$ are essentially binary for $k = 1, \ldots, n-1$, then, as in case 1, we have $p_2(G, \cdot) \geqslant 2n-1 > n-1$. Assume now that there exists a k such that $x(xy)^k$ is not essentially binary. Then, by the argument above, n is even, $k = n/2$ and $x(xy)^{n/2} = y$ holds in $(G, \cdot)$. Putting yx^{n-1} for y, we get $xy^{n/2} = yx^{n-1}$. It is clear that this identity is equivalent to the previous one. So, consider the polynomials $xy, x(xy), y(yx), x(xy)^2, y(yx)^2, \ldots, x(xy)^{n/2-1}, y(yx)^{n/2-1}$. From the minimality of n we infer that all these polynomials are different and essentially binary. Thus $p_2(G, \cdot) \geqslant 2(n/2-1)+1 = n-1$. The proof is completed.

Proof of Theorem 4. Let $(G, \cdot)$ be an idempotent commutative groupoid for which $xy^2 = yx^2$. Our aim is to prove that if $f(x, y)$ is a nontrivial binary polynomial over $(G, \cdot)$, then f is symmetric and there exists a positive integer k such that $f(x, y) = xy^k$. To prove this assertion we use Marczewski's formula of [3] for a description of the set $A^{(n)}(\mathfrak{A})$ of a given algebra $\mathfrak{A} = (A, F)$. In our case we have $A^{(2)}(G, \cdot) = \bigcup_{k=0}^{\infty} A_k^{(2)}(G, \cdot)$, where $A_0^{(2)} = \{x, y\}$ and $A_{k+1}^{(2)} = A_k^{(2)} \cup \{f_1 f_2 \colon f_1, f_2 \in A_k^{(2)}\}$.

First of all let us prove that $f(x, y) = xy^k$ is commutative for every $k \geqslant 1$. For $k = 1, 2$ this follows immediately from the assumption of the theorem. Supposing that $xy^k = yx^k$ for $k \leqslant n$, we have

$$\begin{aligned} xy^{n+1} &= (xy^{n-1})y^2 = y(xy^{n-1})^2 = \big(y(xy^{n-1})\big)(xy^{n-1}) \\ &= (xy)^n(xy^{n-1}) = (yx^n)(yx^{n-1}) = \big((yx^{n-1})x\big)(yx^{n-1}) \\ &= \big(x(yx^{n-1})\big)(yx^{n-1}) = x(yx^{n-1})^2 = (yx^{n-1})x^2 = yx^{n+1}. \end{aligned}$$

Let us find the elements of the set $A_k^{(2)}$. We have

$$A_1^{(2)} = \{x, y, xy\} \quad \text{and} \quad A_2^{(2)} = \{x, y, xy, xy^2\}.$$

Assume that $A_k^{(2)} = \{x, y, xy, xy^2, \ldots, xy^k\}$ and consider $A_{k+1}^{(2)}$. Using Marczewski's formula, we have

$$A_{k+1}^{(2)} = A_k^{(2)} \cup \{f_1 f_2 \colon f_i \in A_k^{(2)},\ i = 1, 2\}.$$

If at least one of the polynomials f_1, f_2 is trivial, then $f_1 f_2 \in \{x, y, xy, \ldots, xy^{k+1}\}$. Indeed, if $f_1 = xy^r$ where $1 \leqslant r \leqslant k$ and $f_2 = x$ (the case $f_2 = y$ is obvious), then by the commutativity of xy^m for all $m \geqslant 1$ we have $f_1 f_2 = (xy^r)x = (yx^r)x = yx^{r+1} = xy^{r+1}$. Let $f_1 = xy^r$ and $f_2 = xy^p$, where $1 \leqslant r, p \leqslant k$. Let $p = r+q$. Without loss of generality we can assume that $q \geqslant 1$. Then, using again the commutativity of xy^m, we get

$$\begin{aligned} f_1 f_2 &= (xy^r)(xy^p) = (xy^r)\big((xy^r)y^q\big) = (xy^r)\big(y(xy^r)^q\big) = \big(y(xy^r)^q\big)(xy^r) \\ &= y(xy^r)^{q+1} = (xy^r)y^{q+1} = xy^{r+q+1} = xy^{p+1}, \end{aligned}$$

where $p+1 \leqslant k+1$, and thus $f_1 f_2$ is either trivial or of the form xy^s, where $s \leqslant k+1$. Hence

$$A_{k+1}^{(2)} = A_k^{(2)} \cup \{xy^s \colon s \leqslant k+1\} = \{x, y, xy, \ldots, xy^{k+1}\},$$

which completes the proof.

Before proving Theorem 5 we need some lemmas.

Lemma 1. *If $(G, \cdot)$ is medial and $(G, \cdot) \in V(\cdot)$, then*

$$A_k^{(2)}(G, \cdot) = A_{k-1}^{(2)}(G, \cdot) \cdot x \cup A_{k-1}^{(2)}(G, \cdot) \cdot y \quad \textit{for all } k,$$

where $A_0^{(2)}(G, \cdot) = \{x, y\}$ and $A_j^{(2)}(G, \cdot) \cdot u = \{fu \colon f \in A_j^{(2)}(G, \cdot),\ u \in \{x, y\}\}$, $j = 1, 2, \ldots$

Proof. We proceed by induction on k. For $k=1$ we have

$$A_1^{(2)} = A_0^{(2)} \cup \{f_1 f_2 : f_i \in A_0^{(2)},\ i=1,2\} = \{x, y\} \cup \{xy\}$$
$$= \{x, y, xy\} = \{x, xy\} \cup \{y, xy\} = \{xx, yx\} \cup \{xy, yy\}$$
$$= \{x, y\}\cdot x \cup \{x, y\}\cdot y = A_0^{(2)}\cdot x \cup A_0^{(2)}\cdot y.$$

We have $A_j^{(2)}\cdot x \cup A_j^{(2)}\cdot y \subset A_{j+1}^{(2)}$ for all j. Using Marczewski's formula of [3] for the description of $A^{(2)}(\mathfrak{A})$ and the inductive assumption, we get

$$A_{k+1}^{(2)} = A_{k-1}^{(2)}\cdot x \cup A_{k-1}^{(2)}\cdot y \cup U \subset A_k^{(2)}\cdot x \cup A_k^{(2)}\cdot y \cup U,$$

where $U = \{f_1 f_2 : f_1, f_2 \in A_k^{(2)}\}$. To finish the proof it is enough to show that $U \subset A_k^{(2)}\cdot x \cup A_k^{(2)}\cdot y$. Let $f \in U$. Then $f = f_1 f_2$ and $f_1, f_2 \in A_k^{(2)} = A_{k-1}^{(2)}\cdot x \cup A_{k-1}^{(2)}\cdot y$. If $f_1 = g_1 x$ and $f_2 = g_2 x$, then $f_1 f_2 = (g_1 x)(g_2 x) = (g_1 g_2)(xx) = (g_1 g_2)x = gx$, where $g = g_1 g_2 \in A_k^{(2)}$ since $g_i \in A_{k-1}^{(2)}$ $(i=1,2)$. Therefore, $f \in A_k^{(2)}\cdot x$. The case where $f_1, f_2 \in A_{k-1}^{(2)}\cdot y$ is proved analogously. Now let $f_1 = g_1 x$ and $f_2 = g_2 y$, where $g_1, g_2 \in A_{k-1}^{(2)}$. Then using the medial law, we have $f = f_1 f_2 = (g_1 x)(g_2 y) = (g_1 g_2)(xy) = g(xy)$, where $g = g_1 g_2 \in A_k^{(2)}$. If $g = hx$ and $h \in A_{k-1}^{(2)}$, then

$$f = (hx)(xy) = (hy)(xx) = (hy)x \in (A_{k-1}^{(2)}\cdot y)\cdot x \subset A_k^{(2)}\cdot x.$$

The case where $g = hy$ is proved analogously.

LEMMA 2. *If $(G, \cdot)$ is medial and $(G, \cdot) \in V(\cdot)$, then for every $f \in A^{(2)}(G, \cdot)$ there exist nonnegative integers α_i, β_j $(i, j = 1, 2, \ldots, n)$ such that $f(x, y) = x^{\alpha_1} y^{\beta_1} \ldots x^{\alpha_n} y^{\beta_n}$.* (In this lemma we adopt the convention $uv^0 = u$).

Proof. The assertion easily follows from Lemma 1 and Marczewski's formula for $A^{(2)} = \bigcup_{k=0}^{\infty} A_k^{(2)}$ (see the proof of the preceding lemma).

Proof of Theorem 5. Let $(G, \cdot)$ be medial, $(G, \cdot) \in V(\cdot)$, and $\operatorname{card} G \geqslant 2$, and let $f(x, y)$ be an essentially binary polynomial over $(G, \cdot)$. By Lemma 2, we have $f(x, y) = x^{\alpha_1} y^{\beta_1} \ldots x^{\alpha_n} y^{\beta_n}$. Observe that $f(x, y)f(y, x) = xy$, which easily follows from the identity $(g(x, y)y)(g(y, x)x) = (g(x, y)g(y, x))(xy)$ and inductive arguments with respect to the length of $f(x, y) = g(x, y)y$. Hence $f(x, y) = f(y, x)$ implies $f(x, y) = xy$.

Suppose $p_2 = p_2(G, \cdot)$ is finite. Since $\operatorname{card} G \geqslant 2$, we infer that $p_2 \geqslant 1$. We have to prove that p_2 is odd. Indeed, from the above consideration we conclude that the only commutative essentially binary polynomial over $(G, \cdot)$ is xy, whence p_2 is odd since $p_2 - 1$ must be even as the number of all different essentially binary noncommutative polynomials over $(G, \cdot)$. Further, observe that there exists a medial groupoid from $V(\cdot)$ for which p_2 is infinite, for instance $(R, (x+y)/2)$, where R is the set of all reals and $x+y$ the usual addition of real numbers. The proof is completed.

References

[1] J. Dudek, *Some remarks on distributive groupoids*, Czech. Math. J. 31 (1981), pp. 451–456.
[2] G. Gratzer, *Universal Algebra*, Springer-Verlag, 1979.
[3] E. Marczewski, *Independence and homomorphisms in abstract algebras*, Fund. Math. 50 (1961), pp. 45–61.

Accepté par la Rédaction le 18.5.1981