Medial groupoids and Mersenne numbers

by

J. Dudek (Wrocław)

Abstract. Let $(G, +)$ be a groupoid and let $\mathfrak{M}_n$ $(n \geqslant 1)$ denote the variety of all idempotent commutative medial (i.e., $(x+y)+(u+v) = (x+u)+(y+v)$) groupoids satisfying $x+ny = x$ (where $x+ny = (\ldots(x+y)+y)+\ldots+y)+y$, x occurs once and y occurs n times). The main purpose of the note is to prove the following theorem: The variety $\mathfrak{M}_n$ is equationally complete iff the Mersenne number $M_n = 2^n-1$ is prime.

0. For a natural number n the number $M_n = 2^n-1$ will be called the *n-th Mersenne number* (see [4]). It is an open problem how many prime Mersenne numbers exist (the same applies to nonprime Mersenne numbers).

In this note we exhibit a connection between prime Mersenne numbers M_n and some equationally complete varieties $\mathfrak{M}_n$ of indempotent groupoids (see below).

In Section 1, a characterization theorem for groupoids from $\mathfrak{M}_n$ is given which is needed to prove our main result.

The terminology and the notations are adopted from [2], [3] and [4].

By an algebra $\mathfrak{A} = (A; F)$ we shall understand an ordered pair $(A; F)$, where A is a nonempty set and F is a set of operations on A. For a given algebra $\mathfrak{A}$ by $A(F)$ we denote the set of all algebraic operations over $\mathfrak{A}$ (see [3]).

Two algebras $\mathfrak{A}_1 = (A; F_1)$ and $\mathfrak{A}_2 = (A; F_2)$ are considered equal (polynomially equivalent in [1]) if $A(F_1) = A(F_2)$.

A groupoid is an algebra $(G; \cdot)$ with a binary fundamental operation $x \cdot y$. We write xy instead of $x \cdot y$ and xy^n stands for $(\ldots(xy)\ldots)y$, where x occurs once and y occurs n times. We shall also omit the brackets in an expression $(\ldots(x_1x_2)\ldots)x_n$. So, e.g., we write $x_1x_2x_3$ instead of $(x_1x_2)x_3$.

A groupoid $(G; \cdot)$ is said to be *idempotent* if $xx = x$ for every $x \in G$.

In general, an algebra $(A; F)$ is *idempotent* if every fundamental operation of it is idempotent, i.e., if $f \in F$, then $f(x, \ldots, x) = x$ for all $x \in A$. For a given algebra $\mathfrak{A} = (A; F)$ by $I(\mathfrak{A})$ we denote the algebra $(A; I(F))$, where $I(F)$ is the set of all idempotent algebraic operations of $\mathfrak{A}$. This algebra is called the *idempotent reduct of* $\mathfrak{A}$.

A groupoid $(G; \cdot)$ is *commutative* if $xy = yx$ for all $x, y \in G$ and it is called *medial* if $(xy)(uv) = (xu)(yv)$ holds for all $x, y, u, v \in G$.

For any natural number n, the class of all idempotent commutative medial groupoids $(G;\cdot)$ which satisfy the identity $xy^n = x$ is denoted by $\mathfrak{M}_n$.

A variety of algebras is called the *zero-variety* if it consists only of one-element algebras. It will be denoted by O. A variety V of algebras is said to be *equationally complete* if the only proper subvariety of V is O.

In this note we are going to prove the following theorem.

THEOREM. *The Mersenne number M_n is prime if and only if the variety $\mathfrak{M}_n$ is equationally complete.*

Before proving this theorem (Section 2) we need some information on groupoids from $\mathfrak{M}_n$.

1. Characterization theorem for groupoids from $\mathfrak{M}_n$. Let $n\geqslant 2$ be a fixed natural number and let $d>1$ be a divisor of 2^n-1. Now let $(G;+)$ be an abelian group of exponent d. Denote by $G(d,n)$ the groupoid $(G;c(x+y))$ where $c=(d+1)/2$.

LEMMA 1. *The groupoids $G(d,n)$ belong to the variety $\mathfrak{M}_n$.*

Proof. We have $xx=(d+1)x=x$. The commutativity of xy follows from the fact that $(G;+)$ is an abelian group. To prove the medial law, let us observe that the binary operation $\alpha x+\beta y$ is medial in every module over a commutative ring. Since any abelian group of exponent d can be regarded as a $\mathfrak{Q}_d$-module, where

$$\mathfrak{Q}_d = (\{o,\dots,d-1\};\ +(\operatorname{mod} d);(\operatorname{mod} d)),$$

we infer that $G(d,n)$ is medial.

Now let us check the identity $xy^n=x$. We have $x_1x_2x_3=c^2(x_1+x_2)+cx_3$ and in general

$$x_1\dots x_k = c^{k-1}x_1+c^{k-1}x_2+c^{k-2}x_3+\dots+cx_k.$$

Hence we have

$$xy^n = c^nx+(c+\dots+c^n)y = c^nx+\frac{c(c^n-1)}{c-1}y.$$

Since $(c-1,c)=1$ and $(c-1,d)=1$ and $d|2^n-1$, we infer that $c^n\equiv 1(\operatorname{mod} d)$ and $\dfrac{c^{n+1}-c}{c-1}\equiv o(\operatorname{mod} d)$. Thus we conclude that $G(d,n)\in\mathfrak{M}_n$.

LEMMA 2. *If $(G;\cdot)\in\mathfrak{M}_n$ then there exists an abelian group $(G;+)$ of exponent d, $d|2^n-1$, such that $xy=c(x+y)$ for all $x,y\in G$ with $c=(d+1)/2$.*

Proof. If $\operatorname{card}G=1$ then $d=1$ and $xy=x+y$. Now let $\operatorname{card}G\geqslant 2$ and $x+y=xyo^{n-1}$ for some $o\in G$. We prove that $(G;+)$ is the required group. Indeed, observe that $x+y=y+x$ and $x+o=xoo^{n-1}=xo^n=x$. Using the mediality and distributivity (which follows from the mediality and idempotency of xy), we have

$$\begin{aligned}(x+y)+z &= xyo^{n-1}zo^{n-1} = xyo^{n-1}zoo^{n-2} = ((xyo^{n-1}o)(zo))o^{n-2}\\ &= ((xyo^n)(zo))o^{n-2} = ((xy)(zo))o^{n-2}\\ &= (y+z)+x = x+(y+z).\end{aligned}$$

We have thus proved that $(G;+)$ is a commutative semigroup with the zero-element o.

Observe that any equation $x+a=b$ has a solution in G for $a,b\in G$. Indeed, $x+a=xao^{n-1}=b$ and hence $xa=xao^{n-1}o=bo$ and $x=oba^{n-1}$ is the required solution. One can easily check that the solution is unique, and so $(G;+)$ is a group.

Observe that $2x=xo^{n-1}$ and $2^2x=xo^{n-2}$. By induction it follows that $2^kx=xo^{n-k}$. Putting $k=n-1$ we get $2^{n-1}x=xo$ and hence $2^nx=((xo)(xo))o^{n-1}=xo^n=x$. Since we are in the group $(G;+)$, therefore $(2^n-1)x=o$ for all $x\in G$. Thus the exponent d of G divides 2^n-1 and $d>1$.

Further, observe that

$$xy = \frac{d+1}{2}(x+y).$$

Indeed, $2^{n-1}x+2^{n-1}y = xo+yo = ((xo)(yo))o^{n-1} = xyoo^{n-1} = xyo^n = xy$. To complete the proof of our lemma it is enough to prove that

$$2^{n-1}-\frac{d+1}{2}\equiv(\operatorname{mod} d).$$

We have

$$\frac{(2^n-1)-d}{2}\equiv o(\operatorname{mod} d),$$

which is a simple consequence of $d|2^n-1$ and $(2,d)=1$.

The proof is completed.

The following theorem results from Lemmas 1 and 2.

CHARACTERIZATION THEOREM. *For a fixed natural number n, a groupoid $(G;\cdot)$ belongs to $\mathfrak{M}_n$ if and only if there exists an abelian group $(G;+)$ of exponent d with $d|2^n-1$ and*

$$xy = \frac{d+1}{2}(x+y)\quad \textit{for all } x,y\in G.$$

2. Proof of Theorem. In this section we shall prove the theorem stated in Section 0.

Proof. Let p be a prime number greater than 2. Denote by S_p the variety

$$\operatorname{HSP}\left(\{o,\dots,p-1\};\ \frac{p+1}{2}(x+y)\right)$$

where $+=+(\operatorname{mod} p)$, $\cdot=\cdot(\operatorname{mod} p)$ are understood in the sense of the Galois field

$$\operatorname{GF}(p) = (\{o,\dots,p-1\};+(\operatorname{mod} p),\cdot(\operatorname{mod} p)).$$

Using the result of [5], we infer that the groupoid

$$G_p = \left(\{o,\dots,p-1\};\ \frac{p+1}{2}(x+y)\right)$$

is polynomially equivalent to the idempotent reduct of the additive group of the field $\operatorname{GF}(p)$. This group can be regarded as a vector space over $\operatorname{GF}(p)$ and the groupoid G_p can be treated as an affine space over $\operatorname{GF}(p)$. As is shown in [1], every affine space over $\mathrm{GF}(p)$ is polynomially equivalent to some medial idempotent quasigroup and the variety of all affine spaces over $\mathrm{GF}(p)$ is equationally complete. So, we infer that S_p is equationally complete because of the following fact: if $\mathfrak{A}$ is an algebra of a fixed type τ_1 and if the algebra $\mathfrak{A}$ can also be considered as an algebra of a type τ_2 (with same algebraic operations), then $\mathrm{HSP}(\mathfrak{A})$ is equationally complete with respect to τ_1 if and only if it is equationally complete with respect to τ_2.

It follows from [1] that for different primes p and q the varieties S_p and S_q are different atoms in the lattice of subvarieties of all idempotent medial quasigroups.

Now we are in a position to complete the proof of the theorem. Suppose $\mathfrak{M}_n$ is equationally complete and suppose that $M_n = 2^n-1$ is not prime. Then there exist two different primes p and q such that $p|2^n-1$ and $q|2^n-1$. By Lemma 1 we infer that $G(p,n)$ and $G(q,n)$ belong to the variety $\mathfrak{M}_n$. Therefore the varieties S_p and S_q are contained as non-zero subvarieties in $\mathfrak{M}_n$, which contradicts the fact that $\mathfrak{M}_n$ is equationally complete.

Assume now that M_n is prime. To prove that $\mathfrak{M}_n$ is equationally complete it is enough to show $\mathfrak{M}_n = \mathrm{HSP}((G;\cdot))$ for every nontrivial groupoid $(G;\cdot)$ from $\mathfrak{M}_n$.

Let $(G;\cdot)\in\mathfrak{M}_n$. Then by Lemma 2 there exists an abelian group $(G;+)$ of exponent $d|2^n-1$, where $d>1$ and

$$(G;xy) = \left(G;\ \frac{d+1}{2}(x+y)\right).$$

Since 2^n-1 is prime, we have $d = 2^n-1$ and hence

$$\mathrm{HSP}((G;\cdot)) = \mathrm{HSP}((G;2^{n-1}(x+y))).$$

The latter variety is equal to the variety S_{2^n-1} since the sets of identities of the groupoid $(G;2^{n-1}(x+y))$ and $(\{o,\ldots,2^n-2\};\ 2^{n-1}(x+y))$ are equal (the latter groupoid is polynomially equivalent to the affine space over $\mathrm{GF}(2^n-1)$). By Lemma 1 we find that $S_{2^n-1}\subset\mathfrak{M}_n$ and $S_{2^n-1} = \mathrm{HSP}((G;\cdot))$ for all $(G;\cdot)\in\mathfrak{M}_n$ with $\operatorname{card} G\geqslant 2$. Using the well-known Birkhoff theorem, we infer that $\mathfrak{M}_n = S_{2^n-1}$ and hence $\mathfrak{M}_n$ is equationally complete.

References

[1] B. Csákány and L. Megyesi, *Varieties of idempotent medial quasigroup*, Acta Sci. Math. 37 (1975), pp. 17–24.

[2] G. Grätzer, *Universal Algebra*, Van Nostrand 1968.

[3] E. Marczewski, *Independence and homomorphism in abstract algebras*, Fund. Math. 50 (1961), pp. 45–61.

[4] W. Narkiewicz, *Teoria Liczb*, Warszawa 1977.

[5] J. Płonka, *On the arity of idempotent reducts*, Colloq. Math. 21 (1970), pp. 35–37.

Accepté par la Rédaction le 12. 11. 1979

Solution of a problem of Ulam on countable sequences of sets

by

Andrzej Pelc (Warszawa)

Abstract. Let E be a set of cardinality 2^ω and $\{A_n\colon n\in\omega\}$ an arbitrary sequence of subsets of E. Let $\mathscr{B}$ denote the σ-algebra of subsets of E generated by the family $\{A_n\colon n\in\omega\}$ and $\mathscr{B}^*$ the σ-algebra of subsets of E^2 generated by the family $\{A_n\times A_m\colon n,m\in\omega\}$. S. M. Ulam stated a problem (see [3]), whether there exists an injection $\Phi\colon E\to E^2$ transforming $\mathscr{B}$ into $\mathscr{B}^*$ and conversely.

We give a negative answer to this question and formulate a condition on $\{A_n\colon n\in\omega\}$ under which the answer is positive.

§ 0. We use standard set theoretical notation and terminology.

By E we always denote a set of cardinality 2^ω. If $A\subset E$ then we put $A^1 = A$, $A^0 = E\setminus A$. If $\mathscr{A} = \{A_n\colon n\in\omega\}$ is a sequence of subsets of E then the function $\varphi_{\mathscr{A}}\colon E\to 2^\omega$ such that $\varphi_{\mathscr{A}}(x)(n) = 1 \equiv x\in A_n$ is called the *characteristic function of* $\mathscr{A}$. For every $f\in 2^\omega$ the set $\mathscr{A}(f) = \varphi_{\mathscr{A}}^{-1} * \{f\} = \bigcap_n A_n^{f(n)}$ is called a *component of* $\mathscr{A}$ and f the *index of* $\mathscr{A}(f_i)$. If $e\in E$ then $S(e)$ denotes the component containing e. Clearly the components are pairwise disjoint and their union is E. Conversely, every pairwise disjoint family of cardinality 2^ω with union E is the set of components of some sequence $\mathscr{A}$.

We define generalized Borel classes over $\mathscr{A}$:

$$\Sigma_1^0(\mathscr{A}) = \{\textstyle\bigcup X\colon X\subset\mathscr{A}\},$$

$$\Sigma_\xi^0(\mathscr{A}) = \{\textstyle\bigcup X\colon |X|\leqslant\omega,\ X\subset \bigcup_{\eta<\xi}(\Sigma_\eta^0(\mathscr{A})\cup\Pi_\eta^0(\mathscr{A}))\},$$

$$\Pi_\xi^0(\mathscr{A}) = \{E\setminus X\colon X\in\Sigma_\xi^0(\mathscr{A})\},$$

$$\mathscr{B}(\mathscr{A}) = \bigcup_{\xi<\omega_1}(\Sigma_\xi^0(\mathscr{A})\cup\Pi_\xi^0(\mathscr{A})).$$

$\mathscr{B}(\mathscr{A})$ is the σ-algebra generated by $\mathscr{A}$. If $\mathscr{B}_1$ is a σ-algebra of subsets of E_1 and $\mathscr{B}_2$ a σ-algebra of subsets of E_2 then a function $\Phi\colon E_1\to E_2$ is called $(\mathscr{B}_1,\mathscr{B}_2)$-*preserving* iff $B\in\mathscr{B}_1 \Rightarrow \Phi*(B)\in\mathscr{B}_2$ and $B\in\mathscr{B}_2 \Rightarrow \Phi^{-1}*(B)\in\mathscr{B}_1$. In case when E_1 and E_2 are subsets of 2^ω and $\mathscr{B}_i$ is the family of Borel subsets of E_i ($i = 1,2$), we say that Φ is Borel preserving instead of saying $(\mathscr{B}_1,\mathscr{B}_2)$-preserving.