Commentationes Mathematicae Universitatis Carolinae

Václav Koubek; Vojtěch Rödl

Note on the number of monoids of order n

Commentationes Mathematicae Universitatis Carolinae, Vol. 26 (1985), No. 2, 309--314

Persistent URL: http://dml.cz/dmlcz/106370

COMMENTATIONES MATHEMATICAE UNVERSITATIS CAROLINAE

26,2 (1985)

NOTE ON THE NUMBER OF MONOIDS OF ORDER n

Václav KOUBEK, Vojtěch RÖDL

Abstract: We derive upper bounds for the number of monoids with n elements. As a consequence, we obtain that almost all n-element monoids are endomorphism monoids of graphs with cn $\log_2$ n vertices for some constant $c > 0$.

Key words: Monoid, endomorphism monoid of graphs.

Classification: 20M99, 05C99

We recall that a semigroup S with zero 0 is called three-nilpotent if for each triple x, y, z of elements of S, $x.y.z = 0$. Analogously, a monoid M (i.e. a semigroup with a unity 1) is three-nilpotent if for each triple x, y, z of elements of S different from 1 we have $x.y.z = 0$.

We set

S(n) is the number of all semigroups on an n-element set X,

$S_3(n)$ is the number of all three-nilpotent semigroups on an n-element set X,

M(n) is the number of all monoids on an n-element set X,

$M_3(n)$ is the number of all three-nilpotent monoids on an n-element set X,

G(n) is the number of all groups on an n-element set X.

It follows immediately from the result of [3] that

(1) $G(n) \leq n!\, n^{cn^{2/3}\log_2 n}$, where $c = 2/1-(\frac{1}{2})^{2/3}$

The asymptotic formulas for $S(n)$ and $S_3(n)$ were investigated by D.J. Kleitman, B.R. Rothschild and J.H. Spencer [5]. They proved

<u>Theorem 1:</u> $$S(n) = S_3(n)\ (1 + o(1)) = \left(\sum_{t=1}^{m} f_n(t)\right)(1 + o(1)) = (f_n(t_n-1) + f_n(t_n) + f_n(t_n+1))(1 + o(1)),$$

where $f_n(t) = \binom{n}{t} t^{1+(n-t)^2}$ and t_n is a natural number such that $f_n(t_n) \geq f_n(t)$ for every $t = 1,2,\dots,n$. Moreover, $t_n = \frac{n}{2 \ln n}(1 + o(1))$.

The aim of this note is to use the Theorem 1 to derive similar formula for monoids. We prove:

<u>Theorem 2:</u> $M(n+1) = M_3(n+1)\ (1+o(1)) = (n+1)S(n)(1+o(1))$.

Theorem 2 has applications in graph theory. It is well-known fact [4] that every monoid is isomorphic to the monoid of all endomorphisms of a graph. For a monoid M denote by $\Phi(M)$ the minimum size of a set V such that there is a graph (V,E) for which its endomorphism monoid is isomorphic to M. The following has been shown by L. Babai [1] and the present authors [6]:

<u>Proposition 3:</u> There is a constant c with
$$\Phi(M) \leq c\ n^{3/2}$$
for any monoid M with n elements.

On the other hand we showed (thereby disproving conjecture of L. Babai and J. Nešetřil - see [6]):

<u>Proposition 4:</u> There exists a constant $c > 0$ such that for every natural number n there exists a three-nilpotent monoid M with n elements such that

$$\Phi(M) \geq cn \sqrt{\log_2 n}$$

and there exists a constant d such that for every three-nilpotent monoid M with n elements

$$\Phi(M) \leq dn \log_2 n$$

Combining Theorem 2 and Proposition 4 we obtain

<u>Corollary 5</u>: For almost all monoids M with n elements

$$\Phi(M) \leq dn \log_2 n$$

It remains to prove Theorem 2. For a monoid M denote by Gr(M) the set of all elements x of M such that x.y = 1 for some element y of M. If M is finite, then clearly Gr(M) is a subgroup of M and M - Gr(M) is a subsemigroup of M. Since $1 \in Gr(M)$ we have $Gr(M) \neq \emptyset$. For every $x \in Gr(M)$, the mappings f(y) = x.y, g(y) = = y.x map the set M - Gr(M) bijectively on itself (see [2]). Hence we obtain:

<u>Proposition 6</u>: Let X be an n-element set and let k be a natural number with $0 < k \leq n$. Assume that the following are given

a) a subset Y of X of size k;

b) a group G on the set Y with a set A of generators;

c) a semigroup S on the set X - Y;

d) two mappings $\ell, r: A \times (X - Y) \longrightarrow X - Y$ such that for every $a \in A$, $\ell(a,-)$, r(a,-) are bijections of X - Y into itself.

Then there exists at most one monoid M on X such that

(i) Gr(M) = G and S is a subsemigroup of M;

(ii) for every $a \in A$, $x \in X - Y$ we have $a.x = \ell(a,x)$, x.a = = r(a,x).

On the other hand every monoid is determined by a),b),c) and d).

Clearly,

1) there are $\binom{n}{k}$ subsets Y of X of size k;

2) there are G(k) groups G, and we can assume that $|A| \leq \log_2 k$;

3) there are S(n - k) semigroups S;

4) there are at most $(n-k)!^{2\log_2 k}$ mappings ℓ and r, thus

$M(n) \leq \sum_{k=1}^{m} \binom{n}{k} G(k)\, S(n-k)\, (n-k)!^{2\log_2 k}$.

First observe that the following holds:

<u>Lemma 8</u>: There exists n_o such that for every $n \geq n_o$ and every natural number k with

$$\left\lfloor \frac{n}{2} \right\rfloor \geq k > 1 \quad \text{we have}$$

$$\frac{S(n-k)}{S(n-1)} \leq \frac{1}{n^{(k-1)(2n-k)(1+o(1))}}$$

Proof: By Theorem 1 we get that there exists n_o such that for $n \geq n_o$

$$\frac{S(n-k)}{S(n-1)} = \frac{\sum_{t=1}^{n-k} \binom{n-k}{t} t^{1+(n-k-t)^2}}{\sum_{t=1}^{n-1} \binom{n-1}{t} t^{1+(n-1-t)^2}} (1+o(1)) \leq$$

$$\leq \sum t^{-(2n-k-1-2t)(k-1)} \; (1+o(1)) \leq \frac{1}{n^{(k-1)(2n-k)(1+o(1))}}$$

where the second sum is taken over all t with

$$\left\lceil 0.9 \frac{(n-k)}{2\ell(n-k)} \right\rceil \leq t \leq \left\lfloor 1.1 \frac{n-k}{2\ell n(n-k)} \right\rfloor . \qquad \Box$$

Now we shall finish the proof of Theorem 2. We shall use the following easy consequence of (1):

For a sufficiently large

(2) $$G(n) \leq n!\, 2^n$$

and hence for any $k \leq n$

(3) $$G(k) \leq k!\, n^k$$

Using (2),(3) and Lemma 8 we get the existence of n_1 such that for $n \geq n_1$

$$\frac{M(n)}{S(n-1)} \leq \sum_{k=1}^{m} \binom{n}{k} G(k) \left[(n-k)!\right]^{2\log_2 k} \frac{S(n-k)}{S(n-1)} \leq \binom{n}{1} + \binom{n}{2} 2(n!)^2 \cdot$$

$$\cdot \frac{S(n-2)}{S(n-1)} + \sum_{k=3}^{\lfloor m/2 \rfloor} \binom{n}{k} k!\, n^k \left[(n-k)!\right]^{2\log_2 k} \frac{S(n-k)}{S(n-1)}$$

$$+ \sum_{k=\lfloor m/2 \rfloor+1}^{m} \binom{n}{k} k!\, n^k \left[(n-k)!\right]^{2\log_2 k} \frac{S(n/2)}{S(n)} \leq$$

$$\leq n + \binom{n}{2} 2\, (n!)^2 \frac{1}{n^{(2n-2)(1+o(1))}} +$$

$$+ \sum_{k=3}^{\lfloor m/2 \rfloor} \binom{n}{k} k!\, n^k \left[(n-k)!\right]^{2\log_2 k} \frac{S(n-k)}{S(n-1)} +$$

$$+ \sum_{k=\lfloor m/2 \rfloor+1}^{m} \binom{n}{k} k!\, n^k \left[(n-k)!\right]^{2\log_2 k} \frac{S(n/2)}{S(n)} \leq n + o(1),$$

Thus $M(n) \leq nS(n-1)\ (1+o(1))$. Obviously, if we add the new unity to a three-nilpotent semigroup we obtain a three-nilpotent monoid and hence $M_3(n) \geq nS_3(n-1)$.

Thus we can summarize

$$nS(n-1)\ (1+o(1)) \geq M(n) \geq M_3(n) \geq nS_3(n-1)) = nS(n-1)\ (1+o(1))$$

and Theorem 2 is proved.

References

[1] L. BABAI: On the abstract group of automorphisms "Combinatorics" Proc. 8th British Comb. Conf. Swansea 1981, London Math. Soc. Lecture Note 52, 1-40.

[2] A.H. CLIFFORD, G.B. PRESTON: The algebraic theory of semigroups, Amer. Math. Soc. Providence, Rhode Island 1967.

[3] P.X. GALLAGHER: Counting finite groups of given order, Math. Z. 102(1967), 236-237.

[4] Z. HEDRLÍN, A. PULTR: Symmetric relations (undirected graphs) with given semigroups, Monatsh. Math. 69 (1965), 318-322.

[5] D.J. KLEITMAN, B.P. ROTHSCHILD, J.H. SPENCER: The number of semigroups of order n, Proc. Amer. Math. Soc. 55 (1976), 227-232.

[6] V. KOUBEK, V. RÖDL: On the minimum order of graphs with given semigroup, J.of Comb.Theory B,36(1984),135-155.

Matematicko-fyzikální fakulta, Univerzita Karlova, Malostranské nám. 25, Praha 1, Czechoslovakia

Math. Dept. Technical University, Husova 5, 115 19 Praha 1, Czechoslovakia

(Oblatum 4.12. 1984)