PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 55, Number 1, February 1976

THE NUMBER OF SEMIGROUPS OF ORDER n

DANIEL J. KLEITMAN[1], BRUCE R. ROTHSCHILD AND JOEL H. SPENCER[1]

ABSTRACT. The number of semigroups on n elements is counted asymptotically for large n. It is shown that "almost all" semigroups on n elements have the following property: The n elements are split into sets A, B and there is an $e \in B$ so that whenever $x, y \in A$, $xy \in B$, but if x or y is in B, $xy = e$.

1. **The problem.** Fix a labelled n-element set $[n] = \{1, \ldots, n\}$. A *semigroup* SG on $[n]$ is an associative binary operation (denoted by concatenation). Let $S(n)$ denote the number of semigroups on $[n]$. We find an asymptotic approximation to $S(n)$. Let

$$f(t) = \binom{n}{t} t^{1+(n-t)^2}. \tag{1.1}$$

THEOREM 1.

$$S(n) = \left[\sum_{t=1}^{n} f(t)\right](1 + o(1)). \tag{1.2}$$

Define $t_0 = t_0(n)$ as that t which maximizes $f(t)$. One can show

$$t_0 \sim n/(2 \ln n) \tag{1.3}$$

and $f(t)$ has a sharp peak at t_0. Equation (1.2) simplifies to

$$S(n) = f(t_0)(1 + o(1)) \tag{1.4}$$

except in those "rare" instances when $f(t_0 + 1)$ or $f(t_0 - 1)$ are "near" $f(t_0)$.

For the remainder of the paper we adopt the convention that any inequality about functions of n is meant to be true only for all n sufficiently large, where how large depends on the statement.

2. **Construction of the semigroups.** Let $A \subseteq [n]$, $|A| = n - t$, $t \geqq 1$. Set $B = A^0$. We construct a family $\mathbb{S}(A)$ of semigroups on $[n]$ as follows:

(i) Select $e \in B$.

(ii) For $x, y \in A$ define xy to be an arbitrary member of B.

(iii) For $x \in B$ or $y \in B$ define $xy = e$.

Received by the editors May 11, 1973.

AMS (MOS) subject classifications (1970). Primary 05A15, 20M99.

Key words and phrases. Semigroup, asymptotic enumeration.

[1] Research supported by ONR N00014-67-A-0204-0063 and NSF GP-33580X.

Then for all $x, y, z \in [n]$, $xy \in B$ so $(xy)z = e$. Similarly, $x(yz) = e$. This yields

$$(2.1) \qquad |\mathfrak{S}(A)| = t^{1+(n-t)^2}$$

semigroups. Call a semigroup SG of type T (for trivial) if it is of the above form for some A, e.

Let $\mathfrak{S}_1(A)$ denote those semigroups $SG \in \mathfrak{S}(A)$ such that for no $a \in A$ is $ax = xa = e$ for all $x \in [n]$. Then

$$(2.2) \qquad |\mathfrak{S}_1(A)| = (1 + o(1))|\mathfrak{S}(A)|$$

and the $\mathfrak{S}_1(A)$ are disjoint. Hence, there are $(\sum_{t=0}^{n} f(t))(1 + o(1))$ semigroups of type T. This implies

$$(2.3) \qquad S(n) \geqq \left[\sum_{t=0}^{n} f(t)\right](1 + o(1)).$$

3. **An upper-bound.** Let $\mathfrak{T}(A)$ denote the family of semigroups for which A is a minimal (in cardinality) set of generators. (I.e. all $x \in [n]$ may be expressed as $x = a_1 \cdots a_k$ for some $k \geqq 1, a_1, \ldots, a_k \in A$.) Set $N(A) = |\mathfrak{T}(A)|$. Then

$$(3.1) \qquad S(n) \leqq \sum_{A \subseteq [n]} N(A).$$

If $a_1, a_2 \in A$ then

$$(3.2) \qquad a_1 a_2 \in \{a_1, a_2\} \cup B,$$

as otherwise $A - \{a_1 a_2\}$ would be a smaller set of generators. We bound $N(A)$ by constructing all $SG \in \mathfrak{T}(A)$ as follows:

(i) For $a_1, a_2 \in A$ choose $a_1 a_2 \in \{a_1, a_2\} \cup B$. (This may be done in $(t + 2)^{(n-t)^2}$ ways.)

(ii) Let A' be a minimal (in cardinality) subset of A so that $A'A \supseteq AA \cap B$. For each $b \in AA \cap B$ there exist a_b', a_b so that $b = a_b' a_b$. The set $X = \{a_b' : b \in B\}$ satisfies $XA \supseteq AA \cap B$, so that

$$(3.3) \qquad |A'| \leqq |X| \leqq |B| = t.$$

Since $A' \subseteq A$, $|A'| \leqq \min(t, n - t)$.

Now for all $a \in A'$, $b \in B$ choose ab arbitrarily. (This may be done in at most $n^{|A'||B|} \leqq n^{t \min(t,n-t)}$ ways.)

Claim 1. SG is determined by $AA \cup A'B$.

PROOF. As all $x, y \in [n]$ are finite products of A's, it suffices to show that all $a_1 a_2 \cdots a_k$ are determined. We show this by induction, it being trivial for $k \leqq 2$. For $k > 2$ set $a_1 a_2 = b$. If $b \in A$, $a_1 a_2 \cdots a_k = b a_3 \cdots a_k$ is determined by induction. If $b \notin A$, $b \in B \cap AA$ so $b = cd$ for some $c \in A'$, $d \in A$. Then $a_1 \cdots a_k = c(d a_3 \cdots a_k)$. Now $x = d a_3 \cdots a_k$ is determined by induction and cx is determined since $A'[n]$ is determined.

We have shown

$$N(A) \leqq (t+2)^{(n-t)^2} n^{t\min(t,n-t)}. \tag{3.4}$$

Thus there are at most $\binom{n}{t}(t+2)^{(n-t)^2} n^{t\min(t,n-t)}$ semigroups having a minimal set of generators of cardinality t.

From (3.1), (3.4),

$$S(n) \leqq \sum_{t=1}^{n} \binom{n}{t}(t+2)^{(n-t)^2} n^{t\min(t,n-t)} \tag{3.5}$$

so that

$$S(n) = [n/(2e+o(1))\ln n]^{n^2}. \tag{3.6}$$

Let $\varepsilon > 0$ be fixed and small ($\varepsilon = 10^{-6}$ will do). By elementary calculations and (2.3),

$$\sum{}' \binom{n}{t}(t+2)^{(n-t)^2} n^{t\min(t,n-t)} = o(S(n))$$

where $\sum'$ runs over t, $|t-t_0| > \varepsilon n/\ln n$. Thus: *Almost all semigroups are in* $\mathfrak{T}(A)$ *for some* A, $|A| = n-t$, $|t-t_0| \leqq \varepsilon n/\ln n$. *We restrict our attention to* t *in this range for the duration of this paper.*

4. **The easy case.** Our ultimate objective is to show

$$N(A) = t^{1+(n-t)^2}(1+o(1)) \tag{4.1}$$

for $|A| = n-t$, $|t-t_0| < \varepsilon n/\ln n$. In this section we show the corresponding result for a restricted class of semigroups.

We say that a semigroup in $\mathfrak{T}(A)$ has property E (for easy) if $a_1, a_2 \in A$ imply $a_1 a_2 \neq a_1$ and $a_1 a_2 \neq a_2$. Let $\mathfrak{T}^*(A)$ denote the subclass of $\mathfrak{T}(A)$ satisfying property E and $N^*(A) = |\mathfrak{T}^*(A)|$. We shall show

$$N^*(A) = t^{1+(n-t)^2}(1+o(1)) \tag{4.2}$$

for $|A| = n-t$, $|t-t_0| < \varepsilon n/\ln n$.

For $SG \in \mathfrak{T}^*(A)$ set

$$G_{ax} = \{b \in B\colon ab = x\} \qquad \text{for } a \in A,\ x \in [n].$$

Set

$$F(a) = \max_{x\in[n]} |G_{ax}|$$

and

$$\delta = t - \min_{a\in A} F(a). \tag{4.3}$$

The number δ defined above may be thought of as follows. Consider the rows aB, $a \in A$. Each row has a most frequent entry. δ gives a uniform upper bound (over $a \in A$) for the number of entries in aB not equal to the most frequent one. Trivial semigroups have $\delta = 0$. Let $\mathfrak{T}^*_\delta(A)$ be those semigroups in $\mathfrak{T}^*(A)$ with given δ and $N^*_\delta(A) = |\mathfrak{T}^*_\delta(A)|$.

We now bound $N_\delta^*(A)$. The semigroups in $\mathfrak{T}_\delta^*(A)$ may be constructed by the following procedure.

(i) Pick $g \in A$ so that $t - \delta = F(g)$. (This may be done in $n - t \leqq n$ ways.)

(ii) Set A' equal a minimal subset of A containing g so that $A'A \supseteq AA \cap B$. fix A'. (Since $|A'| \leqq t$, this may be done in at most n^t ways.)

(iii) Determine $A'B$. For each $a \in A'$, $F(a) \geqq t - \delta$; so there exists $x \in [n]$, $|G_{ax}| \geqq t - \delta$. Now aB may be determined by selecting x (in at most n ways), G_{ax} (in $\sum_{i=t-\delta}^{t} \binom{t}{i} \leqq 1 + t^\delta \leqq n^\delta$ ways), and determining ab for $b \in B - G_{ax}$ (in $n^{|B|-|G_{ax}|} \leqq n^\delta$ ways.) Thus each row has at most $n^{2\delta+1}$ possibilities, and therefore $A'B$ has at most $n^{(2\delta+1)|A'|} \leqq n^{(2\delta+1)t}$ possibilities.

(iv) Determine gA. For each $a \in A$ we have $ga \in B$ (by property E). There are at most t^{n-t} possible gA.

(v) Define an equivalence class on A by $a \equiv b$ if $ga = gb$. Since $gA \subseteq B$ there are at most t equivalence classes and we select representatives $g = a_1, \ldots, a_s$, $s \leqq t$, of the classes in an arbitrary fashion. For $2 \leqq i \leqq s$ we determine a_iA, each in at most t^{n-t} ways, for a total of $t^{(n-t)(s-1)}$ possibilities.

(vi) Determine the remainder of AA. Let $a, c \in A$, $a \neq a_1, \ldots, a_s$. Then $a \equiv a_i$ for some i, $1 \leqq i \leqq s$. Then

$$g(ac) = (ga)c = (ga_i)c = g(a_ic) \quad \text{and} \quad ac \in G_{g,g(a_ic)}.$$

Now a_ic has already been determined, so $g(a_ic)$ has been determined, as has $G_{g,g(a_ic)}$. From the definition of δ,

$$|G_{g,g(a_ic)}| \leqq t - \delta.$$

The product ac can be determined in at most $t - \delta$ ways. This holds for $(n - t)(n - t - s)$ pairs (a, c), giving $(t - \delta)^{(n-t)(n-t-s)}$ possibilities.

By Claim 1 the semigroup is now determined.

$$N_\delta^*(A) \leqq nn^t n^{(2\delta+1)t} t^{(n-t)s} (t - \delta)^{(n-t)(n-t-s)} \tag{4.4}$$

$$\leqq n^{1+(2\delta+2)t} (1 - \delta/t)^{n^2(1+o(1))} t^{(n-t)^2} \tag{4.5}$$

and

$$\sum_{\delta=1}^{t-1} N_\delta^*(A) = o\left[t^{1+(n-t)^2}\right] \tag{4.6}$$

by an elementary calculation (using $t \sim n/(2 \ln n)$). That is, *almost all semigroups in* $\mathfrak{T}^*(A)$ *have* $\delta = 0$. Intuitively, for $\delta \geqq 1$, $N_\delta^*(A) = o(t^{(n-t)^2})$ because for most $a, c \in A$ the product ac can take at most $(t - \delta)$ values versus t in the $\delta = 0$ case.

Call an $SG \in \mathfrak{T}^*(A)$ *absurd* if $\delta = 0$ but is not trivial. Since $\delta = 0$ each aB, $a \in A$, is constant.

Claim 2. If $SG \in \mathfrak{T}^*(A)$ and $AB =$ constant, then SG is trivial.

PROOF. Say $AB = e$. For any $a \in A$, $aa \in B$ so $aaa = e$. Now $e \notin A$, since, if it were, $A - \{e\}$ would generate e and, therefore, $[n]$, contradicting the minimality of $|A|$. So $e \in B$. Let $b \in B$, $x \in [n]$. Since A generates $[n]$, b

$= a_1 \cdots a_s$ $(s \geqq 2)$, $x = a_{s+1} \cdots a_{s+t}$ $(t \geqq 1)$ so $bx = a_1 \cdots a_{s+t} = e$ as $s + t \geqq 3$. That is, $B[n] = e$ so SG is trivial.

Claim 3. Let $SG \in \mathfrak{T}^*(A)$, $\delta = 0$, $a_1, a_2 \in A$, $a_1 B = e_1 \neq e_2 = a_2 B$. Then $a_1 A \cap a_2 A = \varnothing$.

PROOF. Suppose $x, y \in A$, $a_1 x = a_2 y$. For any $z \in A$, $xz, yz \in B$ so $e_1 = a_1(xz) = (a_1 x)z = (a_2 y)z = a_2(yz) = e_2$, a contradiction.

The conditions on absurd $SG \in \mathfrak{T}^*(A)$ imposed by Claim 3 are sufficiently stringent that we may easily show (details omitted) that they are "small" in number (i.e. $o(t^{1+(n-t)^2})$). Hence, almost all $SG \in \mathfrak{T}^*(A)$ are trivial, yielding (4.2).

5. **The general case–outline.** Theorem 1 is implied by (4.1). We give a brief outline of the proof of (4.1).

We let $\mathfrak{T}(A, \delta, \ldots)$ and $N(A, \delta, \ldots)$ denote the set, and number, of semigroups with parameters A, δ, ... By $N(A, \delta, \ldots)$ "small" we always mean in comparison to $t^{(n-t)^2}$.

For a particular counting scheme let $\nu(a)$ denote the number of possible rows aA and $\mu(a) = \nu(a)/t^{n-t}$. By (3.2) all $\nu(a) \leqq (t+2)^{n-t}$ so $\mu(a) \leqq n^4$.

For $a \in A$ set

$$S_a = \{x \in A\colon ax = x\} \quad \text{and} \quad L = \{a \in A\colon |S_a| \geqq .01n\}, \qquad l = |L|.$$

If $a \in L$ there are less than 2^n choices for S_a and $n^{.99n}$ choices for $a([n] - S_a)$. There are less than $2^n n^{.99n} = t^{(.99+o(1))n}$ choices for $a[n]$. We may determine $SG \in \mathfrak{T}(A, L)$ by determining LA, then $(A - L)\, A$, then defining A' and determining $A'B$. If l is "large", $N(A, L)$ is "small". Most $SG \in \mathfrak{T}(A)$ have $l = o(n)$ –which we assume for the duration.

We modify the bounding of $N_\delta^*(A)$ in §4 by (4.4) to $N(A, L, \delta)$. We need a slightly different definition for δ:

$$\delta = t - \min_{a \in A-L} F(a). \tag{5.1}$$

We fix $g \in A - L$ so that $F(g) = t - \delta$. We define A' as the minimal set so that $(A' \cup L)A \supseteq AA \cap B$. We bound $N(A, L, \delta)$ by first determining $L[n]$ and then following steps (i), ..., (vi) of §4. The equivalence classes, in step (v), are defined on $A - L$ and there will be $s \leqq t + 1 + .01n$ such classes (when $ga = a$, $\{a\}$ is an equivalence class). We find

$$\begin{aligned} N(A, L, \delta) \leqq\ & t^{(.99+o(1))nl} n n^t n^{(2\delta+1)t} \\ & \cdot (t+2)^{s(n-t)} (t + 2 - \delta)^{(n-t-l-s)(n-t)}. \end{aligned} \tag{5.2}$$

For $\delta \geqq 3$, $N(A, L, \delta)$ is "small". We assume $\delta \leqq 2$ for the duration. Note this implies $|aB| \leqq 3$ for all $a \in A - L$.

Set

$$I = \{a \in A - L\colon aa = a\},$$

$$V = \{a \in A - L - I\colon \exists x \in A - L, a \neq x, ax = a \text{ or } xa = a\},$$

$$|I| = i |V| = v.$$

For $a \in I$, $x \in A - \{a\}$,

$$ax = (aa)x = a(ax) \in \{a, x\} \cup aB,$$

at most 5 possibilities, so $\nu(a) \leqq 5^{n-t}$, $\mu(a) = t^{n(-1+o(1))}$.

Suppose $a \in V$, $x \in A - L$, $ax = a$ or $xa = a$ and xA has already been determined.

Case 1. $xa = a$. For all $c \in A$,

$$ac = (xa)c = x(ac) \in \{xa, xc\} \cup xB$$

at most 5 possibilities. Then $\nu(a) \leqq 5^{n-t}$, $\mu(a) \leqq t^{n(-1+o(1))}$.

Case 2. $ax = a$. For $c \in A$, $xc \neq c$ we have

$$ac = (ax)c = a(xc) \in \{ax\} \cup aB,$$

at most 4 possibilities. We determine aB (at most n^t ways), then aA. Since $x \notin L$, at most $.01n$ c's have $xc = c$. For these there are n possible ac. Then $\nu(a) \leqq n^t 5^n n^{.01n} = n^{n(.01+o(1))}$, so $\mu(a) \leqq t^{n(-.99+o(1))}$.

If i is large we may bound $N(A, I)$ by determining IA, then $(A - I)A$, then $A'A$. We assume $i = o(n)$ for the duration.

If v is large we may bound $N(A, V)$ by determining $(A - V)A$, then VA, then $A'A$. (A technical problem arises. For $a \in V$, $ax = a$ or $xa = a$, we want to determine aA after xA. But perhaps $x \in V$. One may order V (trying any ordering and its reverse) so at least half the $a \in V$ come after their respective x.) We may assume $v = o(n)$ for the duration.

We bound $N(A, L, I, V, \delta)$, where l, i, $v = o(n)$. We determine xA for $x \in L \cup I \cup V$–and when xA is needed before aA, $a \in V$. We define equivalence classes on the remaining $x \in A$, determining xA first for x a representative, then for the remainder of A. We achieve an expression analogous to (5.2) with a factor of $(t - \delta)^{m(n-t)}$ where m, the number of "remaining" A, is at least $(.99 + o(1))n$. The expression is "small" for $\delta > 0$. We assume $\delta = 0$.

If $L \cup I \cup V \neq \varnothing$ we have factors $\mu(a) \leqq t^{(-.99+o(1))n}$ that are not adequately counterbalanced so that $N(A, \delta, L, I, V)$ is "small". Most semigroups have $\delta = 0$, $L = I = V = \varnothing$ and are trivial.

(A final note on "filling in details". One shows $N(A, \delta, L, \ldots) \leqq t^{-.99n} t^{(n-t)^2}$ and there are less than, say, 5^n possible δ, L, $\ldots$ so that $\sum N(A, \delta, L, \ldots)$ taken over *all* δ, L, $\ldots$, except $\delta = 0$, $L = \cdots = \varnothing$, is small.)

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139 (Current address of Bruce Rothschild)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024 (Current address of Daniel Kleitman)

Current address: (Joel Spencer): Department of Mathematics, State University of New York at Stony Brook, Stony Brook, Long Island, New York 11794