RANK AND STATUS IN SEMIGROUP THEORY[1][2]

Alessandra Cherubini

Dipartimento di Matematica, Politecnico di Milano
Piazza L. da Vinci 32, 20133 Milano, Italy
aleche@mate.polimi.it

John M. Howie

Mathematical Institute, University of St Andrews
North Haugh, St Andrews, Fife KY16 9SS, U.K.
jmh@st-and.ac.uk

Brunetto Piochi

Dipartimento di Matematica "U. Dini"
Università degli Studi di Firenze
viale Morgagni 67/a - I 50134 Firenze, Italy
piochi@math.unifi.it

Abstract

For each generating set A of a finite semigroup S the integer $\Delta(A)$ is defined as the least n for which every element of S is expressible as a product of at most n elements of A. The *status* of S is defined as the least value of $|A|\Delta(A)$ among generating sets of A. Some general bounds are obtained, and the notion is explored in more detail for certain well understood classes of semigroups.

[1]1991 *Mathematics Subject Classification:* 20M10. *Key words:* Finite semigroup, rank, status.

[2]The first and third authors acknowledge support from the GNAMPA/GNSAGA intergroup project of INDAM: "Aspetti analitici, geometrici e combinatorici dei sistemi dinamici e dei linguaggi formali". The COFIN project "Strutture geometriche, combinatoria e loro applicazioni" supported a one month visit of the second author to Italy, during which this paper was begun.

1 Introduction

In a finite semigroup S we normally have many choices for a generating set: in particular, if A is a generating set for S then so is any subset of S containing A. For an arbitrary non-empty subset V of S and for all $n \geq 1$, define

$$V^{[n]} = V \cup V^2 \cup \ldots \cup V^n \,. \tag{1}$$

It is clear that

$$V \subseteq V^{[2]} \subseteq \cdots \subseteq V^{[n]} \subseteq \cdots \,, \tag{2}$$

and equally clear that

$$\langle V \rangle = \bigcup_{n \geq 1} V^n = \bigcup_{n \geq 1} V^{[n]} \,.$$

If $\langle V \rangle = S$, then the *V-depth* $d_V(s)$ of an element s in S is the unique n for which $s \in V^{[n]} \setminus V^{[n-1]}$.

Let S be a finite semigroup. Associated with each generating set A of S is a natural number $\Delta(A)$, called the *radix* of A, defined by

$$\Delta(A) = \min\{m \,:\, A^{[m]} = S\} \,. \tag{3}$$

Thus, for example, if S is the cyclic group of order 12 generated by a, then $\Delta(\{a\}) = 12$. If we choose another generating set $A = \{a^3, a^4\}$, we find that

$$\begin{array}{lcllcl} A^2 & = & \{a^6, a^7, a^8\} \,, & A^3 & = & \{a^9, a^{10}, a^{11}, 1\} \,, \\ A^4 & = & \{1, a, a^2, a^3, a^4\} \,, & A^5 & = & \{a^3, a^4, a^5, a^6, a^7, a^8\} \,; \end{array}$$

thus $A^{[4]} \subset S$, $A^{[5]} = S$, and so $\Delta(A) = 5$.

Roughly speaking, a larger set of generators might be expected to have a smaller value of $\Delta(A)$, and we may reasonably measure the effectiveness of a set of generators using the product $|A|\Delta(A)$. We define the *status* $\mathrm{Stat}\,(S)$ of a finite semigroup S by

$$\mathrm{Stat}\,(S) = \min\{|A|\Delta(A) \,:\, \langle A \rangle = S\} \,. \tag{4}$$

It is on the whole easy to find upper bounds for $\mathrm{Stat}\,(S)$; for example, we have established that $\mathrm{Stat}\,(\mathbf{Z}_{12}) \leq 10$. What is harder is to show that a particular generating set gives us the smallest possible value of $|A|\Delta(A)$.

2 Preliminaries, trivialities and generalities

For undefined terms in semigroup theory, see [4]. Throughout the paper, log will denote the natural logarithm.

Clearly questions regarding status are related to those regarding rank, where the *rank* $r(S)$ of a semigroup S is defined by

$$r(S) = \min\{|A| : \langle A\rangle = S\}\,,$$

and it is useful at this stage to recall the work of Giraldes and Howie ([3], [2]) on 'royal' semigroups (those with the highest possible rank), where $r(S) = |S|$, and 'noble' semigroups, where $r(S) = |S| - 1$. Their structure is described in some detail in [3] and [2]; here we need only note that

1. left and right zero semigroups are royal, and so is a chain (with $xy = \min\{x, y\}$);
2. a null semigroup, in which all products are equal to 0, is noble.

It is obvious that $\mathrm{Stat}\,(S) = |S|$ if S is royal or noble. Indeed, if we follow the whimsical precedent of [3] and call a semigroup S *genteel* if $r(S) \geq |S|/2$, we obtain the obvious result that $\mathrm{Stat}\,(S) = |S|$ for every genteel semigroup. (The whimsy continues: genteel, noble and royal semigroups have high status.) It is, however, not the case that every semigroup for which $\mathrm{Stat}\,(S) = |S|$ is genteel: an obvious example is $\mathbf{Z}_6$.

The following theorem shows how easy it is to construct genteel semigroups:

Theorem 2.1 *Every finite semigroup is embeddable in a genteel semigroup.*

Proof Let S be a finite semigroup, and let E be the chain

$$e_1 < e_2 < \cdots < e_n\,,$$

with $e_i e_j = \min\{e_i, e_j\}$. Let $T = S \cup E$ (a disjoint union) and, for each s in S and each e_i in E, let

$$e_i s = s e_i = s\,.$$

Then T is a semigroup containing S as a subsemigroup. Every generating set of T must contain E, and so $r(T) > n$. If we choose $n > |S|$, we deduce that $r(T) > |T|/2$, and so T is genteel. □

The status concept does have one friendly property:

Theorem 2.2 *Let S be a finite semigroup and let ρ be a congruence on S. Then* $\mathrm{Stat}\,(S/\rho) \leq \mathrm{Stat}\,(S)$.

Proof Suppose that A is a generating set of S, chosen so that $|A|\Delta(A) = \mathrm{Stat}\,(S)$. Every element s of S is expressible as a product

$$s = a_1 a_2 \dots a_n\,,$$

where $a_1, a_2, \dots, a_n \in A$ and $n \leq \Delta(A)$. The set $A\rho = \{a\rho : a \in A\}$ generates S/ρ, and $|A\rho| \leq |A|$. Since

$$s\rho = (a_1\rho)(a_2\rho)\dots(a_n\rho)\,,$$

with $n \leq \Delta(A)$, we deduce that $\Delta(A\rho) \leq \Delta(A)$. Thus

$$\mathrm{Stat}\,(S/\rho) \leq |A\rho|\Delta(A\rho) \leq |A|\Delta(A) = \mathrm{Stat}\,(S)\,.$$

□

It is reasonable to ask whether $\mathrm{Stat}\,(U) \leq \mathrm{Stat}\,(S)$ for every subsemigroup U. In general this is not true, as the following example shows.

Example 2.3 Let $S = FSL_n$ be the free semilattice on a set

$$E = \{e_1, e_2, \dots, e_n\}$$

of n generators, where $n \geq 6$. It is in effect the semilattice of all non-empty subsets of the set E, and the semigroup multiplication corresponds to the operation $\cup$ on subsets. The order of the semigroup is $2^n - 1$. It is clear that $\Delta(E) = n$, since the minimum element $e_1 e_2 \dots e_n$ is the longest possible product. Hence $\mathrm{Stat}\,(S) \leq n^2$. Now let U be the subsemigroup of S consisting of all elements of depth not less than 3. This is generated by the set E^3 of all elements of depth precisely 3, and any generating set of U must contain E^3. However, $|E^3| = n(n-1)(n-2)/6$, and so

$$\mathrm{Stat}\,(U) \geq 2|E^3| = \frac{1}{3}n(n-1)(n-2)\,.$$

This lies between n^2 and $|U|$ for all $n \geq 6$.

Remark As we shall see in Section 5, the upper bound n^2 for $\mathrm{Stat}\,(FSL_n)$ is certainly not best possible.

In Example 2.3 above, we incidentally used the obvious lower bound result that $\mathrm{Stat}\,(U) \geq 2r(U)$ if U is not genteel.

3 Groups

Related questions have been asked for groups. Let G be a finite group of order N and let A be a subset of G. Then A is called an *h-basis* of G if $A^h = G$. It follows that $|G| \leq |A|^h$, or equivalently that $|A| \geq |G|^{1/h}$. In 1937 Rorbach [12, 13] asked if for every $h \geq 2$ there is a function $c(h)$ with the property that, in every finite group G, there exists an h-basis A for which $|A| < c(h)|G|^{1/h}$.

Rohrbach himself proved that such a function $c(h)$ exists for cyclic groups. Much later, in 1980, Cherley [1] proved that every finite abelian group G of order N has a 2-basis A such that $|A| \leq 2\sqrt{N \log N} + 2$. Nathanson [10] improved this result: if $h \geq 3$ then, for every $\delta > 0$ and for sufficiently large N, there exists an h-basis A such that $|A| \leq (h + \delta)[N \log N]^{1/h}$.

Jia [6, 7] proved that Rohrbach's question has a positive answer for finite abelian and finite nilpotent groups, obtaining values $c(h) = h(1 + 2^{-1/h})^{h-1}$ in the abelian case, and $c(h) = h2^{h-1}$ in the nilpotent case. Kozma and Lev [9] obtained the value $c(h) = 2h - 1$ for solvable or alternating groups. This is the strongest result so far, since the class of solvable groups includes all nilpotent and all abelian groups.

These results give rise to an upper bound on the status of groups since trivially $\Delta(A) \leq h$ for every h-basis A of G; in particular, for solvable groups we have

$$\begin{aligned} \mathrm{Stat}\,(G) &\leq \min\{h|A| \,:\, h \geq 2 \text{ and } A \text{ is an } h\text{-basis of } G\} \\ &\leq \min\{hc(h)n^{1/h} \,:\, h \geq 2\}\,. \end{aligned} \tag{5}$$

Given a real number x, we shall use the notations

$$\lfloor x \rfloor = \max\{n \in \mathbf{Z} \,:\, n \leq x\}\,, \quad \lceil x \rceil = \min\{n \in \mathbf{Z} \,:\, n \geq x\}\,.$$

Theorem 3.1 *Let G be a solvable group of order $N \geq 19$, and let $s(h) = h(2h-1)N^{1/h}$. Then* $\mathrm{Stat}\,(G) \leq \lfloor s(\bar{h}) \rfloor$, *where $\bar{h}$ is the nearest integer to*

$$\frac{1}{8}\left(2\log n + 1 + \sqrt{4(\log n)^2 - 12\log n + 1}\right)\,.$$

Proof We determine $\min\{hc(h)N^{1/h} \,:\, h \geq 2\}$, with $c(h) = 2h - 1$, and this can be done using elementary calculus. Taking h as a real variable, we find that

$$s'(h) = \frac{N^{1/h}}{h}[4h^2 - (2\log N + 1)h + \log N]\,.$$

For $N \leq 18$ the discriminant of the quadratic inside the square brackets is negative; otherwise there is a zero of $s'(h)$, giving a minimum of $s(h)$ at

$$h = \frac{1}{8}\left(2\log N + 1 + \sqrt{4(\log N)^2 - 12\log N + 1}\right).$$

Let $\bar{h}$ be the nearest integer number to this minimum point. (Since h is irrational, it cannot be a half-integer, and so $\bar{h}$ is well defined.) Then $\mathrm{Stat}\,(G) \leq s(h) \leq s(\bar{h})$, and, being an integer, cannot exceed $\lfloor s(\bar{h}) \rfloor$. □

If $N \leq 18$ then the function $s(h)$ is increasing for all $h(\geq 2)$, and so its minimum value is $s(2)$. The bound obtained in this way is of no interest, since it exceeds the order of the group.

It is of interest to do some calculations:

$\lvert G\rvert$	$\bar{h}$	$\mathrm{Stat}\,(G) \leq$
50	2	42
100	2	60
500	3	119
1000	3	150
5000	4	235
10,000	4	280
50,000	5	391
100,000	5	450
10^6	7	654
10^9	10	1509
10^{12}	14	2720

It was also shown by Kozma and Lev [8] that every finite group has a 2-basis A such that $|A| \leq 4\sqrt{|G|}/\sqrt{3}$, and so we have the bound

$$\mathrm{Stat}\,(G) \leq \frac{8\sqrt{N}}{\sqrt{3}},$$

applying to *every* finite group of order N. This new bound is lower than or equal to the one given for solvable groups in Theorem 3.1 for $N \leq 1170$ (apart from $N = 19, 20, 21$ where both of the bounds are anyway greater than $N - 1$) but it becomes quickly much weaker for greater values of N: asymptotically, $s(\bar{h}) \sim \frac{1}{2}e^2(\log N)^2$.

We can get better bounds for special classes of groups. For example let us consider the symmetric group S_n (of order $n!$) on $n \geq 3$ elements:

Theorem 3.2

$$\mathrm{Stat}\,(S_n) \leq \lfloor \tfrac{3}{2}(n-1) \rfloor (n-1)\,.$$

Proof Let

$$A = \{(1\ j)\ :\ j = 2, 3, \ldots, n\}$$

be a generating set for S_n, of cardinality $n-1$; for distinct $i_1, i_2, \ldots, i_f$ in $\{2, 3, \ldots, n\}$, we have:

$$(i_1\ i_2\ \ldots\ i_f) = (1\ i_1\ i_2\ \ldots\ i_f)(1\ i_1) = (1\ i_1)(1\ i_2)\ldots(1\ i_f)(1\ i_1)\,.$$

Now, each permutation moving exactly s elements is the product of k disjoint cycles of length f_j, with $s = \sum_{j=1}^{k} f_j$ and $f_j \geq 2$, and so we have at most $k = \lfloor s/2 \rfloor$ cycles. A cycle of length f_j can be written as the product of $f_j + 1$ generators in A, though from this we can subtract two generators if the cycle involves 1. Thus each permutation of length $s = \sum_{j=1}^{k} f_j$ can be written as the product of at most

$$\sum_{j=1}^{k} (f_j + 1) \leq \sum_{j=1}^{k} f_j \ + \ \lfloor \tfrac{s}{2} \rfloor = s + \lfloor \tfrac{s}{2} \rfloor = \lfloor \tfrac{3s}{2} \rfloor$$

generators (minus 2 if the permutation moves 1).

The maximum number of moved elements is $s = n$, and in this case we can subtract 2, since one of the cycles must involve 1. Thus we use at most

$$n + \lfloor \tfrac{n}{2} \rfloor - 2 \leq \lfloor \tfrac{3}{2}(n-1) \rfloor$$

generators to generate such a permutation. The same bound is still obtained if the permutation moves less than n elements, and we deduce that

$$\mathrm{Stat}\,(S_n) \leq \lfloor \tfrac{3}{2}(n-1) \rfloor (n-1)\,.$$

□

A comparable result can be obtained for the alternating group A_n:

Theorem 3.3 *For all $n \geq 4$,*

$$\mathrm{Stat}\,(A_n) \leq 2(n-2)^2\,.$$

Proof Let

$$A = \{(1\ 2\ n)\,,\ (1\ 3\ n)\,,\ \ldots,\ (1\ n-1\ n)\} \tag{6}$$

be a generating set for A_n, of cardinality $n-2$. The following equalities, in which h and k are distinct elements of $\{2,\dots,n-1\}$, are easy to check:

$$\left.\begin{array}{rcl} (1\ n\ h) &=& (1\ h\ n)(1\ h\ n)\,, \\ (h\ k\ n) &=& (h\ n)(k\ n) \;=\; (1\ h\ n)(1\ h\ n)(1\ k\ n)\,, \\ (1\ h\ k) &=& (1\ h\ n)(1\ k\ n)(1\ k\ n)\,, \\ (1\ h)(k\ n) &=& (k\ n)(1\ h) = (1\ h\ n)(1\ k\ n)\,. \end{array}\right\} \tag{7}$$

Each permutation α in A_n can be expressed as a product of disjoint cycles. Consider a cycle in α of odd length $2r+1$; it can be expressed as a product of cycles of length 3 as follows :

- If $a_1 = 1$, then

  $$(a_1\ a_2\ \dots\ a_{2r+1}) = (1\ a_2\ a_3)(1\ a_4\ a_5)\ \dots\ (1\ a_{2r}\ a_{2r+1})\,.$$

  (If $a_{2s+1} = n$, with $1 \le s \le r$, then one of the factors in the product is $(1\ a_{2s}\ n)$; if $a_{2s} = n$, with $1 \le s \le r$, then one of the factors is $(1\ n\ a_{2s+1})$.)

  We get a dual identity if $a_{2r+1} = n$.

- If $a_1 \neq 1$ and $a_{2r+1} \neq n$ then

  $$\begin{array}{rcl} (a_1\ a_2\ \dots\ a_{2r+1}) &=& (1\ a_1\ a_2\ \dots\ a_{2r+1}\ n)\,(1\ n\ a_1) \\ &=& (1\ a_1\ n)(a_2\ a_3\ n)\ \dots\ (a_{2r}\ a_{2r+1}\ n)\,(1\ n\ a_1)\,. \end{array}$$

Hence by (7) we get that a cycle of odd length $2r+1$ can be expressed as the product of at most $3r+3$ generators (minus 3 if it moves 1 or n; minus 4 or 5 if it moves both of them, as in that case the product includes either $(1\ n\ h)$ or $(1\ h\ n)$ for some h).

Now consider a cycle of even length $2r$; of course it does not belong to A_n, but it can be expressed anyway as follows:

- If $a_1 = 1$ then

  $$\left.\begin{array}{rcl} (a_1\ a_2\ \dots\ a_{2r}) &=& (1\ a_2\ a_3)\ \dots\ (1\ a_{2r-2}\ a_{2r-1})\,(1\ a_{2r}) \\ &=& (1\ a_2)(1\ a_3\ a_4)\ \dots\ (1\ a_{2r-1}\ a_{2r})\,, \end{array}\right\} \tag{8}$$

  and if $a_{2r} = n$ then

  $$\left.\begin{array}{rcl} (a_1\ a_2\ \dots\ a_{2r}) &=& (a_1\ a_2\ n)\ \dots\ (a_{2r-3}\ a_{2r-2}\ n)\,(a_{2r-1}\ n) \\ &=& (a_1\ n)(a_2\ a_3\ n)\ \dots\ (a_{2r-2}\ a_{2r-1}\ n)\,. \end{array}\right\} \tag{9}$$

  In both cases the cycle can be expressed as the product of $3(r-1)$ generators and a cycle of two elements; note that if $a_1 = 1$ and $a_s = n$ for some $s \neq 1$ then we need at least one or two generators less.

- If $a_1 \neq 1$ and $a_{2r} \neq n$, then

$$\left.\begin{array}{rcl} (a_1\ a_2\ \ldots\ a_{2r}) & = & (1\ a_1\ a_2\ \ldots\ a_{2r}\ n)\,(1\ n\ a_1) \\ & = & (1\ a_1)\ (1\ a_2\ a_3)\ \ldots\ (1\ a_{2r}\ n)\,(1\ n\ a_1) \\ & = & (1\ n\ a_{2r})\ (1\ a_1\ a_2\ \ldots\ a_{2r}\ n) \\ & = & (1\ n\ a_{2r})\,(1\ a_1\ n)\ \ldots\ (a_{2r-2}\ a_{2r-1}\ n)\ (a_{2r}\ n)\,, \end{array}\right\} \tag{10}$$

  and so the cycle can be expressed as the product of $3r$ generators and a cycle of two elements.

Since all our permutations are even, and since cycles of even length are odd permutations, there must be an even number of cycles of even length. A product of two disjoint cycles

$$\beta = (b_1\ b_2\ \ldots\ b_{2p}) \text{ and } \gamma = (c_1\ c_2\ \ldots\ c_{2q})$$

of even lengths $2p$ and $2q$ can be expressed as the product of generators in different ways; consider the following cases:

- If $\beta = (1\ n)$, then

  $$\beta\gamma = (1\,n)(c_1\,c_2\ \ldots\ c_{2q}) = (1\,c_2\,n)(c_3\,c_4\,n)\ \ldots\ (c_{2q-1}\,c_{2q}\,n)(1\,n\,c_1)(1\,c_2\,n)\,,$$

  and so is expressed as a product of generators of length at most $3(q-1)+4 = 3(p+q)-2$.

- If $p > 1$ and β moves both 1 and n, with $b_1 = 1$ and $b_s = n$ for some $s \geq 2$, then by (9) and (10) we need at most $3(p-1)-1+3q$ generators plus two generators for the product

  $$(b_{2p}\ n)(1\ c_1) = (1\ c_1\ n)(1\ b_{2p}\ n)\,,$$

  making $3(p+q)-2$ generators in all.

- If β moves 1 and γ moves n, with $b_1 = 1$ and $c_{2q} = n$, then by (8) and (9) we need $3(p-1)+3(q-1)$ generators plus 2 generators for the product

  $$(1\ b_{2p})(c_1\ n) = (1\ b_{2p}\ n)(1\ c_1\ n)\,,$$

  making $3(p+q)-4$ generators in all.

- If β moves 1 (with $b_1 = 1$) and neither β nor γ moves n, then by (8) and (10) we need $3(p-1)+3q$ generators plus 3 generators for the product $(1\ b_{2p})(1\ c_1) = (1\ b_{2p}\ c_1)$, making $3(p+q)$ generators in all.

- If β and γ move neither 1 nor n, then by (10) we need $3p+3q$ generators plus 2 generators for the product $(b_{2p}\ n)(1\ c_1)$, making $3(p+q)+2$ generators in all.

Since other cases are dual, the product $\beta\gamma$ of a pair of cycles of even lengths $2p$ and $2q$ can be expressed as the product of at most $3(p+q)+2$ generators (minus 4 if both 1 and n are moved by the same one of the two cycles, minus 6 if 1 is moved by one and n is moved by the other of them, and minus 2 if the cycles move just one among 1 and n).

Suppose that a permutation α moves exactly s elements, then:

$$s = \sum_{i=1}^{m}(2r_i+1) \ + \ \sum_{j=1}^{k}(2p_j+2q_j)\,,$$

and we need at most

$$3\Big(\sum_{i=1}^{m} r_i \ + \ \sum_{j=1}^{k}(p_j+q_j)\Big) \ + \ 3m \ +2k \tag{11}$$

generators to express it. But

$$\sum_{i=1}^{m} r_i \ + \ \sum_{j=1}^{k}(p_j+q_j) \ = \ \frac{s-m}{2}\,. \tag{12}$$

(Note that this equality carries the implication that $s-m$ is even.) Now, by assumption, $2r_i+1 \geq 3$ and $2p_j+2q_j \geq 4$; hence

$$4k \leq \sum_{j=1}^{k} 2(p_j+q_j) \ = \ s - \sum_{i=1}^{m}(2r_i+1) \ \leq \ s-3m\,,$$

and so

$$k \ \leq \left\lfloor \frac{s-3m}{4} \right\rfloor \ \leq \ \frac{s-3m}{4}\,. \tag{13}$$

It now follows from (11), (12) and (13) that the number of generators in A which are needed to express a permutation α moving s elements is at most

$$\begin{aligned} & 3\Big(\sum_{i=1}^{m}(r_i) \ + \ \sum_{j=1}^{k}(p_j+q_j)\Big) \ + \ 3m \ +2k \\ = \ & 3\,\frac{s-m}{2} \ +3m \ +2k \leq 3\,\frac{s-m}{2} \ +3m \ +2\,\frac{s-3m}{4} \\ = \ & 2s\,. \end{aligned}$$

If $s \leq (n-2)$ then we need at most $2(n-2)$ generators, but this is also true for $s=n$ or $n-1$. In fact if $s=n$ then both 1 and n are moved: in the worst

cases we need $2n-4 = 2(n-2)$ generators. Similarly, if $s = n-1$ then the worst case is when only one among 1 and n is moved by one even cycle and we need $2(n-1)-2$ generators.

Since the generating set A has $n-2$ elements, we conclude that

$$\mathrm{Stat}\,(A_n) \leq 2(n-2)^2\,.$$

□

4 Lower bounds for status

Let S be a finite semigroup, of order N. Given a generating set A containing g elements, there is an obvious limit on the number of elements in $A^{[m]}$, namely the number of words of length not exceeding m that can be formed from the alphabet A. Thus A can be a generating set with $\Delta(A) = m$ only if

$$N \leq |A^{[m]}| \leq g + g^2 + \cdots + g^m = \frac{g(g^m-1)}{g-1}\,.$$

Thus

$$m \geq \log_g[N(g-1)+g] - 1\,. \tag{14}$$

For a given N, the minimum value of mg, subject to (14), is a lower bound for $\mathrm{Stat}\,(S)$.

For example, if $N = 1000$, we easily obtain the following table:

g	2	3	4	5	6	7	8	9	10
m	9	6	5	5	4	4	4	4	3
mg	18	18	20	25	24	28	32	36	30

Further routine calculation reveals that

$$m = \begin{cases} 3 & \text{for } g \in \{10,\ldots,32\} \\ 2 & \text{for } g \in \{33,\ldots,999\}, \end{cases}$$

and so $\mathrm{Stat}\,(S) \geq 18$ for every semigroup of order 1000.

Further calculations, available in [11], yield the following result:

Theorem 4.1 *Let S be a finite semigroup of order N and let A be a set of generators with $|A| = g$. Denote by m_g the element $\lceil log_g[N(g-1)+g] - 1\rceil$. If $N = 3$, then* $\mathrm{Stat}\,(S) = 3 = N$. *If $N \neq 3$ then* $\mathrm{Stat}\,(S) \geq \min\{2m_2, 3m_3\}$. *Indeed, if $N > 67,108,862$ then $Stat(S) \geq 3m_3 = 3\lceil log_3[2N+3] - 1\rceil$.*

In the case of a commutative semigroup we can obtain a better lower bound:

Theorem 4.2 *Let S be a finite commutative semigroup with a generating set A consisting of g elements. Then*

$$|A^{[m]}| \leq \binom{m+g}{g}. \tag{15}$$

Proof Let $A = \{a_1, a_2, \ldots, a_g\}$, and let $F(m, g)$ denote the number of words of length exactly m in the g commuting variables $a_1, a_2, \ldots, a_g$. It is clear that $|A^m| \leq F(m, g)$. Among the $F(m, g)$ words of length m, we have $F(m-1, g)$ words that contain a_1 (since we may assume that each such word begins with a_1) and $F(m, g-1)$ words that do not contain a_1. Hence, for all $m, g \geq 2$,

$$F(m, g) = F(m-1, g) + F(m, g-1)\,. \tag{16}$$

It is now easy to prove by induction that, for all $m, g \geq 1$,

$$F(m, g) = \binom{m+g-1}{g-1} = \binom{m+g-1}{m}. \tag{17}$$

the key step, motivated by (16), being the Pascal identity

$$\binom{m+g-2}{g-1} + \binom{m+g-2}{g-2} = \binom{m+g-1}{g-1}.$$

From the definition it is clear that, for all $m \geq 1$,

$$|A^{[m+1]}| \leq |A^{[m]}| + F(m+1, g)\,.$$

If we suppose inductively that

$$|A^{[m]}| \leq \binom{m+g}{g},$$

(which is obviously true if $m = 1$) then it follows, again by the Pascal identity, that

$$|A^{[m+1]}| \leq \binom{m+g}{g} + \binom{m+g}{g-1} = \binom{m+g+1}{g}.$$

□

The minimum value of mg, subject to

$$N \leq \binom{m+g}{g}, \tag{18}$$

is a lower bound for Stat (S).

Taking $N = 1000$ once again as an example, we easily obtain the table

g	2	3	4	5	6	7	8	9	10
m	44	17	10	8	7	6	5	5	4
mg	88	51	40	40	42	42	40	45	40

Further routine calculation reveals that

$$m = \begin{cases} 4 & \text{for } g \in \{10, \ldots, 16\} \\ 3 & \text{for } g \in \{17, \ldots, 43\} \\ 2 & \text{for } g \in \{44, \ldots, 999\}, \end{cases}$$

and so Stat $(S) \geq 40$ for every commutative semigroup of order 1000.

5 Rectangular bands and semilattices

It is natural to begin the investigation of status by looking at particular cases in which the structure of the semigroup is well understood. The easiest case is the rectangular band:

Theorem 5.1 *Let $B = P \times Q$, with $|P|, |Q| \geq 2$, be a finite rectangular band. Then*

$$\text{Stat}\,(B) = 2\max\{|P|, |Q|\}\,.$$

Proof The multiplication in B is given by

$$(p_1, p_2)(q_1, q_2) = (p_1, q_2)\,,$$

and from this it is clear that B satisfies the identical relation $xyz = xz$. Thus $\Delta(A) = 2$ for all generating sets A (with the obvious exception of B itself) and so all we require is to determine the smallest possible generating set for B. From [5] we have that $r(B) = \max\{|P|, |Q|\}$, and so Stat $(B) = 2\max\{|P|, |Q|\}$, as required. □

For a general semilattice E we do not have as straightforward a description as we do for rectangular bands. We do, however, have a lower bound for Stat (E):

Theorem 5.2 *If E is a semilattice of order N, then*

$$\text{Stat}\,(E) \geq 2\log_2(N+1)\,.$$

Proof Let A be a set of generators for E. Since the number of elements generated by A is at most $2^{|A|}-1$, we must have $N \leq 2^{|A|}-1$, and so $|A| \geq \log_2(N+1)$, the bound being attained if and only if E is a free semilattice. The result follows. □

For the free semilattice on n generators (which is isomorphic to the set of all non-empty subsets of a set of n elements under the operation $\cup$) we have the following upper bound:

Theorem 5.3 *Let FSL_n be the free semilattice on n generators, where $n \geq 2$. Then*

$$\mathrm{Stat}\,(FSL_n) \leq \begin{cases} n^2 - \lfloor n/2 \rfloor^2 & \text{if } n \text{ is even} \\ n^2 - \lfloor n/2 \rfloor^2 - 1 & \text{if } n \text{ is odd.} \end{cases}$$

Proof The free semilattice, generated by

$$X = \{e_1, e_2, \ldots, e_n\},$$

is of order $2^n - 1$, and every generating set must contain $e_1, e_2, \ldots, e_n$.

Suppose first that n is even, say $n = 2k$. We add k extra generators

$$e_1e_2\,,\ e_3e_4\,, \ldots\,, e_{2k-1}e_{2k} \tag{19}$$

to obtain a generating set A. Every element

$$e_{i_1}e_{i_2}\ldots e_{i_l} \quad (1 \leq l \leq k)$$

lies in $X^{[k]}$, and so certainly in $A^{[k]}$. Every element

$$e_{i_1}e_{i_2}\ldots e_{i_{k+r}} \quad (1 \leq r \leq k)$$

in FSL_n must contain at least r of the elements (19). This is perhaps not quite obvious, but we can prove it by 'reverse induction', it being obvious that the statement is true when $r = k$. If we suppose it true for r, consider a product p of length $k+r-1$, and the product pe_i (where e_i does not appear in p) of length $k+r$. We suppose inductively that pe_i contains at least r of the generators (19). The addition of one extra generator to p cannot have increased the count of generators from (19) by more than 1, and so p must contain at least $r-1$ generators from (19).

We reach the conclusion that every element of FSL_n is expressible as a product of generators in A of length at most k. Hence

$$\mathrm{Stat}\,(FSL_n) \leq |A|\Delta(A) = 3k^2 = n^2 - \lfloor n/2 \rfloor^2\,.$$

Suppose now that $n = 2k + 1$, an odd number. From the even case above we may be sure that every element containing only factors from $\{e_1, e_2, \ldots, e_{2k-2}\}$ can be generated with not more than $k - 1$ factors chosen from

$$B = \{e_1, e_2, \ldots, e_{2k-2}\} \cup \{e_1e_2, e_3e_4, \ldots, e_{2k-3}e_{2k-2}\}\,.$$

Now let

$$A = B \cup \{e_{2k-1},\, e_{2k},\, e_{2k+1},\, e_{2k-1}e_{2k},\, e_{2k-1}e_{2k+1},\, e_{2k}e_{2k+1},\, e_{2k-1}e_{2k}e_{2k+1}\}\,.$$

It is clear that A is a generating set, with $|A| = |B|+7 = 3k+4$ and $\Delta(A^*) = k$. Hence

$$\mathrm{Stat}\,(FSL_n) = (3k+4)k = (2k+1)^2 - k^2 - 1 = n^2 - \lfloor n/2 \rfloor^2 - 1\,.$$

□

6 Monogenic semigroups

From [5] it is clear that we can ask algebraic questions about a finite monogenic semigroup $\langle a \mid a^{k+n} = a^k \rangle$ that are not easy to answer. It is certainly reasonable to consider the status of a monogenic semigroup S of order N, but we have to settle for a lower bound rather than an equality. It is clear that $\mathrm{Stat}\,(S) \leq N$, but it is clear also that we can do better than this: if $N = 7$ we may choose $A = \{a, a^3\}$ as a generating set and observe that $A^{[3]} = S$; thus $\mathrm{Stat}\,(S) \leq 6$. In this case we have equality, for if $3 \leq |A| \leq 6$ we must have $\Delta(A) \geq 2$, and so $|A|\Delta(A) \geq 6$.

The proof of the following theorem is adapted from [6].

Theorem 6.1 *Let M be a monogenic semigroup of order m. Then for every integer d such that $1 \leq d \leq m$ there exists a generating set A of radix d for M, with*

$$|A| = d(\lceil (m+1)^{1/d} \rceil - 1)\,.$$

Proof We shall write the elements of M simply as $1, 2, \ldots, m-1, m$ so as to avoid awkward notation. (In this notation we know that $m+1 = k$ for some k in $\{1, 2, \ldots, m\}$, but we shall not make use of this fact.) Let $u = \lceil (m+1)^{1/d} \rceil$, and let A consist of the $d(u-1)$ elements

$$\begin{aligned}
&1, 2, \ldots, u-1;\\
&u, 2u, \ldots, (u-1)u;\\
&u^2, 2u^2, \ldots, (u-1)u^2;\\
&\ldots\\
&u^{d-1}, 2u^{d-1}, \ldots, (u-1)u^{d-1}\,.
\end{aligned}$$

We prove by induction on k that each integer up to $u^k - 1$ is expressible as the sum of at most k elements of A. This is trivially true for $k = 1$. Suppose that it holds for k and consider an integer v such that $u^k \leq v \leq u^{k+1} - 1$. Then, by the division algorithm,

$$v = qu^k + r\,, \text{ where } 1 \leq q \leq u-1,\ 0 \leq r \leq u^k - 1\,.$$

By the induction hypothesis, r is a sum of at most k elements in A, and the required result follows immediately, since $qu^k \in A$.

Thus every integer up to $u^d - 1$ is expressible as a sum of at most d elements of A. □

Theorem 6.1 immediately gives an upper bound for $\mathrm{Stat}\,(S)$:

Corollary 6.2 *Let S be a monogenic semigroup of order N. Then*

$$\mathrm{Stat}\,(S) \leq \Phi(N,d) = \min\left\{d^2\left(\lceil (N+1)^{1/d}\rceil - 1\right)\,:\, 1 \leq d \leq m\right\}.$$

Remark 6.3 The presence of the function $\lceil\ \ \rceil$ in the formula means that a standard calculus approach to minimization is not necessarily very effective. For large N we can approximate $\mathrm{Stat}\,(S)$ by $\min\{d^2(N+1)^{1/d}\,:\, d \geq 1\}$, and this is attained when $d = (1/2)\log(N+1)$. The approximation, however, gives only a 'ballpark' value. For example, if $N+1 = 10^6$ we have $(1/2)\log(N+1) \approx 6.9$, but if we calculate $\Phi(N,d)$ we obtain the table

d	5	6	7	8	9	10	11	12	13	14
Φ	375	369	343	320	324	300	363	432	338	392

and so the minimum occurs when $d = 10$. As d increases, we obtain a low value when $\lceil (N+1)^{1/d}\rceil - 1$ jumps down an integer. In this case, $\lceil (N+1)^{1/d}\rceil - 1$ is equal to 4 when $d = 9$ but equals 3 when $d = 10$. The next jump downwards occurs at 13, when $\lceil (N+1)^{1/d}\rceil - 1$ drops from 3 to 2, and the final downward jump, from 2 to 1, occurs when $d = 20$.

7 Brandt semigroups

Let $n \geq 2$ and let B_n denote the aperiodic Brandt semigroup (see [4]) of degree n. Thus

$$B_n = (\{1,2,\ldots,n\} \times \{1,2,\ldots,n\}) \cup \{0\}\,,$$

where

$$\begin{aligned}(i,j)(k,l) &= \begin{cases}(i,l) & \text{if } j=k\\ 0 & \text{otherwise}\end{cases}\\ (i,j)0 &= 0(i,j) = 00 = 0\,.\end{aligned}$$

Denote the set $\{1,2,\ldots,n\}$ by $\mathbf{N}_n$ with its natural order. In the sequel we refer to the elements of B_n as *pairs*.

Theorem 7.1 *Let B_n be the aperiodic Brandt semigroup of degree n; then*

$$\mathrm{Stat}\,(B_n) = 4n-4\,.$$

Proof It is clear that

$$A = \{(1,2),\,(2,1),\,(1,3),\,(3,1),\ldots,(1,n),\,(n,1)\}$$

is a generating set for B_n, and that $\Delta(A)=2$. Hence $\mathrm{Stat}\,(S) \le 2|A| = 4n-4$.

To show equality, notice first that the rank of B_n is n, a minimal generating set being

$$\{(1,2),(2,3),\ldots,(n-1,n),(n,1)\}\,.$$

Thus every generating set U of B_n must have $|U| \ge n$. If $\Delta(U) \ge 4$, then certainly $|U|\Delta(U) > 4n-4$. So if we are to find U such that $|U|\Delta(U) < 4n-4$ we must look at generating sets U with $\Delta(U)=2$ or $\Delta(U)=3$.

Note that for each $i \in \mathbf{N}_n$ there must exist $j \in \mathbf{N}_n$ such that $(i,j) \in U$. If, for every $i \in \mathbf{N}_n$ there exist distinct pairs (i,j_1), (i,j_2) in U, then $|U| \ge 2n$. Hence we may choose i in $\{1,2,\ldots,n\}$ with the property that there is a *unique* j such that $(i,j) \in U$; such a j is surely different from i or it would be impossible to generate any other (i,j'), $j' \ne 1$. For notational simplicity we may suppose that $i=1$, $j=2$.

Let U be a generating set such that $\Delta(U)=2$. We shall show that $|U| \ge 2n-2$. Since $(1,1) \in U^{[2]}$ we must have $(2,1) \in U$. Also, since $(1,i) \in U^{[2]}$ for all $i \notin \{1,2\}$, we must have $(2,i) \in U$. Thus

$$|U| \ge |\{(1,2),(2,1)\} \cup \{(2,i) \,:\, i \ne 1,2\} \cup \{(i,*) \,:\, i \ne 1,2\}| = 2n-2\,,$$

and so $|U|\Delta(U) \ge 4n-4$.

Next, suppose that U is a generating set such that $\Delta(U)=3$. We aim to prove that $|U| \ge 2n-4$. Let B (respectively C) be the set of elements $y \in \mathbf{N}_n$ such that the U-depth of $(1,y)$ equals 2 (respectively 3), that is :

$$\begin{aligned}B &= \{i \in \mathbf{N}_n \,:\, (2,i) \in U\}\,,\\ C &= \{j \in \mathbf{N}_n \,:\, j \ne 2,\ (2,j) \notin U,\ (\exists i \ge 3)\ (2,i),(i,j) \in U\}\,.\end{aligned}$$

Then B and C are disjoint, $C \neq \emptyset$ and $B \cup C = \mathbf{N}_n \setminus \{2\}$. Let

$$x = \begin{cases} 1 & \text{if } 1 \in B \\ 0 & \text{if } 1 \in C. \end{cases}$$

Let $|C| = k$; then $|B| = n - k - 1$. We want now to count the elements in U. Let us start by defining a suitable subset $\overline{U}$ of U. Define a map f from C into B by putting $f(c) = b$ if and only if $(b, c) \in U$ and, for all $b' \in B$, if $(b', c) \in U$ then $b < b'$ in the natural order of $\mathbf{N}_n$. Let $U_0 = \{(f(c), c) : c \in C\}$ and let $B_1 = \{b \in B : f^{-1}(b) \neq \emptyset\}$. Denote $|B_1|$ by h. By our definition, f is a map from C onto B_1, and so $k \geq h$.

For each $b \neq 1$ belonging to $B \setminus B_1$ there is at least one (b, x_b) in U. Define a map g from $B \setminus (B_1 \cup \{1\})$ into $\mathbf{N}_n$ by putting $g(b) = x$, where $(b, x) \in U$ and, for all $x' \in \mathbf{N}_n$, $(b, x') \in U$ implies $x < x'$ in the natural order of $\mathbf{N}_n$. Let $U_1 = \{(b, g(b)) : b \in B \setminus (B_1 \cup \{1\})\}$.

Similarly for each $c \neq 1$ in C there is at least one $(c, x_c) \in U$. Note that if in U there exists only one pair $(c, *)$ for some $c \in C$, then $* \neq 1$, for otherwise it would be impossible to express (c, c) as a product of length at most 3: in fact $(c, 1)$, $(c, 2) = (c, 1)(1, 2)$, $(c, b) = (c, 1)(1, 2)(2, b)$ would be the only possible products which can be generated under our assumptions on the U-depth of elements of B_n. Hence we may define a map l from $C \setminus \{1\}$ into $\mathbf{N}_n \setminus \{1\}$ as follows: $l(c) = x$, where $x \neq 1$, $(c, x) \in U$ and, for all $x' \in \mathbf{N}_n \setminus \{1\}$, $(c, x') \in U$ implies $x < x'$ in the natural order of $\mathbf{N}_n$. Let $U_2 = \{(c, l(c)) : c \in C \setminus \{1\}\}$.

Obviously $U_i \subseteq U$, $i = 0, 1, 2$ and $U_i \cap U_j = \emptyset$ if $i \neq j$. Let $\overline{U} = \{(1, 2)\} \cup \{(2, b) : b \in B\} \cup U_0 \cup U_1 \cup U_2$. Hence $\overline{U}$ contains the following pairs:

- 1 pair $(1, 2)$;
- $n - k - 1$ pairs $(2, b) \quad (b \in B)$;
- $n - k - 1 - x - h$ pairs $(b, g(b)) \in U_1$;
- k pairs $(b, c) \in U_0 \quad (c \in f^{-1}(b))$;
- $k - 1 + x$ pairs $(c, l(c)) \in U_2$.

Thus

$$|U| \geq |\overline{U}| \geq 1 + (n - k - 1) + (n - k - 1 - x - h) + k + (k - 1 + x) = 2n - 2 - h\,.$$

If $h \leq 2$ we have proved the required result. So let $h > 2$. Our aim is to show that in U there must be at least $h - 2$ elements not in $\overline{U}$.

If there exist $h-2$ elements $b \in B_1$ such that (c_b, j_1), (c_b, j_2) are in U for some $c_b \in f^{-1}(b)$, $j_1 \neq j_2$, then we have finished because for each c_b at most one such pair is in $\overline{U}$. Let $\overline{B} = \{b_1, b_2, \ldots, b_t\}$, $2 < t \leq h$ be the set of elements in B_1 such that for all $c \in f^{-1}(b_i)$, $i = 1, \ldots, t$ there exists in U only the pair $(c, l(c))$.

Consider $b_1 \in \overline{B}$. It is not possible to have $l(c) \in \{2,\, b_1,\, c'\}$ (with $c' \in f^{-1}(b_1)$) for every c in $f^{-1}(b_1)$, for in this case it would be impossible to generate any pair (b_1, y), where $y \notin C \setminus f^{-1}(b_1)$, as a product of at most 3 pairs in U. Suppose now that, for all $b_i \in \overline{B}$ and all $c \in f^{-1}(b_i)$, we have either $l(c) \in \{2,\, b_i,\, c'\}$ (with c' in $f^{-1}(b_i)$) or $l(c) = b \in B_1 \setminus \overline{B}$. Then the latter case must hold for at least one $c_i \in f^{-1}(b_i)$. We must generate the pairs (b_1, c_i) for $c_i \in f^{-1}(b_i)$, $i \neq 1$, as a product of at most 3 pairs in U. By means of the pairs in $\overline{U}$ we get only (b_1, c_j), $(b_1, c_j)(c_j, b)$, $(b_1, c_j)(c_j, b)(b, c)$ for $c_j \in f^{-1}(b_1)$, $b \in B_1 \setminus \overline{B}$, $c \in f^{-1}(b)$. Thus there must exist in $U \setminus \overline{U}$ at least one pair (b_1, c_i) or (b, c_i) for all $c_i \in f^{-1}(b_i)$, $i \neq 1$. Hence there are at least $t-1$ new pairs, and so $|U \setminus \overline{U}| \geq h - t + t - 1 = h - 1$.

Thus we may now suppose that for every $b_i \in \overline{B}$ there exists at least one element in $f^{-1}(b_i)$ (denote it by c_i) such that $l(c_i) = b \in (\overline{B} \setminus \{b_i\}) \cup (B \setminus B_1)$ or $l(c_i) = c \in C \setminus f^{-1}(b_1)$. Suppose first that for all i and for all c_i we have $l(c_i) = b \in (\overline{B} \setminus \{b_i\}) \cup (B \setminus B_1)$.

Consider b_1 and c_1. Let us first suppose that $l(c_1) = b_2 \in \overline{B}$ and let $c_j \in f^{-1}(b_j)$, $j = 3, \ldots, t$. By means of pairs in $\overline{U}$ we can generate only (c_1, b_2), $(c_1, b_2)(b_2, \overline{c})$, $(c_1, b_2)(b_2, \overline{c})(\overline{c}, b)$ for $\overline{c} \in f^{-1}(b_2)$ and $b \in B$. Thus, in order to generate (c_1, c_j) as a product of at most 3 elements in U, we need in $U \setminus \overline{U}$ at least a pair (b_2, c_j), $\forall j = 3, \ldots, t$. Hence $|U \setminus \overline{U}| \geq h - t + t - 2 = h - 2$.

Now suppose that $l(c_1) = b' \in B \setminus B_1$ and let $b \in B_1$ and $c_b \in f^{-1}(b)$. The pair (c_1, c_b) must be generated as a product of at most 3 elements in U, and so the pair (b', c_b) must be generated as a product of at most 2 elements in U. If (b', c_b) is in U then we have done: suppose that this is the case for $r\,(< h)$ elements c_b. For the remaining $h - r$ elements c_b there must exist pairs in U (b', z) and (z, c_b) for some $z \in B \cup C$. Consider the minimum element z in the natural order of $\mathbf{N}_n$ for which this happens and suppose that we have s such elements z. Thus in U there must exist $r + s$ pairs having b' as first element. For at most one of them the second element is $g(b')$ and the corresponding pair is in $\overline{U}$. Now consider the $h - r$ pairs (z, c_b): in $\overline{U}$ we have at most one of them for every z, and so at most s of them are in $\overline{U}$. Thus we have at least $(r + s - 1) + (h - r - s) = h - 1$ pairs in $U \setminus \overline{U}$.

We have to consider the final case when for all $b_i \in \overline{B}$ and for all $c \in f^{-1}(b_i)$ we have that either $l(c) \in \{2,\, b_i,\, c'\}$ (with c' in $f^{-1}(b_i)$) or $l(c_i) = b \in (\overline{B} \setminus$

$\{b_i\}) \cup (B \setminus B_1)$ or $l(c_i) = c \in C \setminus f^{-1}(b_1)$, and that the latter case holds for at least one index i. Without loss of generality, let $i = 1$, consider b_1 and c_1 and suppose that $l(c_1) = c \in C \setminus f^{-1}(b_1)$. For every $b \in B_1 \setminus f(c)$ let $c_b \in f^{-1}(b)$. The pair (c_1, c_b) must be generated as a product of at most 3 elements in U, and by computations similar to those in the previous case we deduce that there are at least $(r + s - 1) + (h - 1 - r - s) = h - 2$ pairs in $U \setminus \overline{U}$.

In all cases there must be in U at least $h - 2$ pairs not in $\overline{U}$ and

$$|U| \geq 2n - 2 - h + h - 2 = 2n - 4\,.$$

It follows that $\operatorname{Stat} B_n \geq 3(2n - 4) \geq 4n - 4$ for all $n \geq 4$.

It remains to verify the result for $n = 2$ and $n = 3$. First, let $n = 2$. Then $4n - 4 = 4$. Since $|U| \geq 2$ it follows that $|U|\Delta(U) \geq 6$ if $\Delta(U) = 3$. If $n = 3$, so that $4n - 4 = 8$, then $\Delta(U) = 3$ and $|U| \geq 3$ gives $|U|\Delta(U) \geq 9$. □

References

[1] J. Cherley, On complementary sets of group elements, *Arch. Math.* **35** (1980), 313–318.

[2] Emilia Giraldes, Semigroups of high rank. II. Doubly noble semigroups, *Proc. Edinburgh Math. Soc.* (2) **28** (1985), 409–417.

[3] Emilia Giraldes and John M. Howie, Semigroups of high rank, *Proc. Edinburgh Math. Soc.* (2) **28** (1985), 13–34.

[4] John M. Howie, *Fundamentals of semigroup theory*, Oxford University Press, 1995.

[5] John M. Howie and Maria Isabel Marques Ribeiro, Rank properties in finite semigroups, *Comm. Algebra* **27** (1999), 5333–5347.

[6] X.-D. Jia, Thin bases for finite abelian groups, *J. Number Theory* **36** (1990), 254–256.

[7] X.-D. Jia, Thin bases for finite nilpotent groups, *J. Number Theory* **41** (1992), 303–313.

[8] G. Kozma and A. Lev, Bases and decomposition numbers of finite groups, *Arch. Math.* **58** (1992), 417–424.

[9] G. Kozma and A. Lev, On H-bases and H-decompositions of the finite solvable and alternating groups, *J. Number Theory* **49** (1994), 385–391.

[10] M. B. Nathanson, On a problem of Rohrbach for finite groups, *J. Number Theory* **41** (1992), 69–76.

[11] B. Piochi, Lower bound for Status of Semigroups, Dipartimento di Matematica "U. Dini", Università degli Studi di Firenze, Rapporto n. 7 (2003)

[12] H. Rohrbach, Ein betrag zur additiven Zahlentheorie, *Math. Z.* **42** (1937), 538–542.

[13] H. Rohrbach, Anvendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretsche Frage, *Math. Z.* **42** (1937), 1–30.