Reaching the minimum ideal in a finite semigroup

Nasim Karimi

University of Porto, Portugal

June 7, 2013

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

CMUP

Overview

Preliminaries

Parameter $N(S, A)$

Parameters N, M and M'

Questions

Parameters N, M and M'

How do these parameters relate to the Černý conjecture?

How far apart can N, M and M' be?

How do these parameters behave with respect to decompositions?

Conjecture

Directed diameter of a finite group

Directed diameter of a direct power of a finite group

References

References

Notation

Let S be a finite semigroup and $A \subseteq S$ be a generating set of S. For every $s \in S$, denote by $\ell_A(s)$ the minimum length of a sequence which represents s in terms of generators in A.

Notation

Let S be a finite semigroup and $A \subseteq S$ be a generating set of S. For every $s \in S$, denote by $\ell_A(s)$ the minimum length of a sequence which represents s in terms of generators in A.

Definition

Let S be a finite semigroup with a generating set $A \subseteq S$ and the minimum ideal I. Define

$$N(S, A) = \min\{\ell_A(s) : s \in I\}.$$

Example

- If G is a finite group, then $N(G, A) = 1$, for every generating set A.

Example

- If G is a finite group, then $N(G, A) = 1$, for every generating set A.

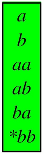


Figure: Group $N(G, A) = 1$

Example

- If G is a finite group, then $N(G, A) = 1$, for every generating set A.
- If $C_{i,n} = \langle a : a^i = a^{i+n} \rangle$, then $N(C_{i,n}, \{a\}) = i$.

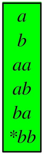


Figure: Group $N(G, A) = 1$

Example

- If G is a finite group, then $N(G, A) = 1$, for every generating set A.

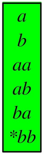
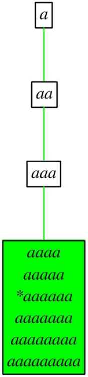


Figure: Group $N(G, A) = 1$

- If $C_{i,n} = \langle a : a^i = a^{i+n} \rangle$, then $N(C_{i,n}, \{a\}) = i$.

Figure: cyclic semigroup $N(C_{4,6}, \{a\}) = 4$



Example

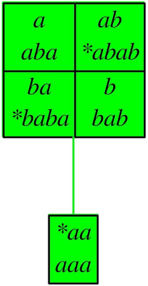


Figure: Semigroup $S = \langle a, b \rangle$, $N(S, \{a, b\}) = 2$

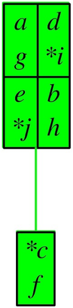


Figure: Semigroup $S = \langle S \rangle$, $N(S, S) = 1$

Parameters which only depend on the semigroup S:

Parameters which only depend on the semigroup S:

Definition

- $N(S) = \min\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.

Parameters which only depend on the semigroup S:

Definition

- $N(S) = \min\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.
- $M(S) = \max\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.

Parameters which only depend on the semigroup S:

Definition

- $N(S) = \min\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.
- $M(S) = \max\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.
- $M'(S) = \max\{N(S, A) : S = \langle A \rangle\}$.

Parameters which only depend on the semigroup S:

Definition

- $N(S) = \min\{N(S,A) : S = \langle A\rangle, |A| = \mathrm{rank}(S)\}$.
- $M(S) = \max\{N(S,A) : S = \langle A\rangle, |A| = \mathrm{rank}(S)\}$.
- $M'(S) = \max\{N(S,A) : S = \langle A\rangle\}$.

Remark

- $\min\{N(S,A) : S = \langle A\rangle\} = 1$.

Parameters which only depend on the semigroup S:

Definition

- $N(S) = \min\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.
- $M(S) = \max\{N(S, A) : S = \langle A \rangle, |A| = \mathrm{rank}(S)\}$.
- $M'(S) = \max\{N(S, A) : S = \langle A \rangle\}$.

Remark

- $\min\{N(S, A) : S = \langle A \rangle\} = 1$.
- *If* $A \subseteq B$*, then* $N(S, B) \leq N(S, A)$*. Hence*
- $M'(S) = \max\{N(S, A) : A$ *is a minimal generating set*$\}$.

- How do these parameters relate to the Černý conjecture?

- How do these parameters relate to the Černý conjecture?
- How far apart can $N(S)$, $M(S)$ and $M'(S)$ be?

- How do these parameters relate to the Černý conjecture?
- How far apart can $N(S)$, $M(S)$ and $M'(S)$ be?
- How do these parameters behave with respect to decompositions (direct product and semidirect product)?

- How do these parameters relate to the Černý conjecture?
- How far apart can $N(S)$, $M(S)$ and $M'(S)$ be?
- How do these parameters behave with respect to decompositions (direct product and semidirect product)?
- Is it true that $M(S) = M'(S)$?

- How do these parameters relate to the Černý conjecture?
- How far apart can $N(S)$, $M(S)$ and $M'(S)$ be?
- How do these parameters behave with respect to decompositions (direct product and semidirect product)?
- Is it true that $M(S) = M'(S)$?
- How do these parameters behave with respect to division?

Definition

A deterministic complete automaton $\mathscr{A} = (Q, A)$ *is called synchronizing if there is a word* $w \in A^*$ *such that* $|Qw| = 1$*, that is* w *acts as a constant map in* Q*. We call such a word* w *a reset word.*

Definition

A deterministic complete automaton $\mathscr{A} = (Q, A)$ is called synchronizing if there is a word $w \in A^*$ such that $|Qw| = 1$, that is w acts as a constant map in Q. We call such a word w a reset word.

Notation

Denote by $\ell_{srw}(\mathscr{A})$ the length of the shortest reset words of the synchronizing automaton $\mathscr{A} = (Q, A)$.

Example

$Q = \{0, 1, 2, 3\},\ A = \{a, b\}$

$0 \overset{ba^3ba^3b}{\longrightarrow} 0$

$1 \overset{ba^3ba^3b}{\longrightarrow} 0$

$2 \overset{ba^3ba^3b}{\longrightarrow} 0$

$3 \overset{ba^3ba^3b}{\longrightarrow} 0$

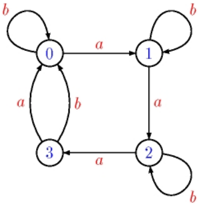


Figure: Synchronizing automaton $\mathscr{A} = (Q, A)$

The shortest reset word is ba^3ba^3b, then $\ell_{srw}(\mathscr{A}) = 9$.

Černý's conjecture

Notation

For every $n \in N$ denote,

$$c(n) = \max\{\ell_{srw}(\mathscr{A}) \mid \mathscr{A} = (Q, A) \textit{ is synchronizing}, |Q| = n\}.$$

Černý's conjecture

Notation

For every $n \in N$ denote,

$$c(n) = \max\{\ell_{srw}(\mathscr{A}) \mid \mathscr{A} = (Q, A) \textit{ is synchronizing}, |Q| = n\}.$$

Conjecture

Černý's conjecture states that $c(n) = (n-1)^2$.

Let $\mathscr{A} = (Q, A)$ be a synchronizing automaton. If S is the transition semigroup of $\mathscr{A}$, then

$$N(S, A') = \ell_{srw}(\mathscr{A}),$$

where $A' = \{\rho_a : q \mapsto qa \mid a \in A\}$.

Let $\mathscr{A} = (Q, A)$ be a synchronizing automaton. If S is the transition semigroup of $\mathscr{A}$, then

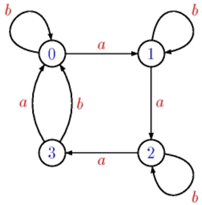
$$N(S, A') = \ell_{srw}(\mathscr{A}),$$

where $A' = \{\rho_a : q \mapsto qa \mid a \in A\}$.

Example

$Q = \{0, 1, 2, 3\}$, $A = \{a, b\}$
$\rho_a = (1, 2, 3, 0)$, $\rho_b = (0, 1, 2, 0)$.

Figure: Automaton $\mathscr{A} = (Q, A)$



The transition semigroup S is the semigroup generated by A', where $A' = \{\rho_a, \rho_b\}$.

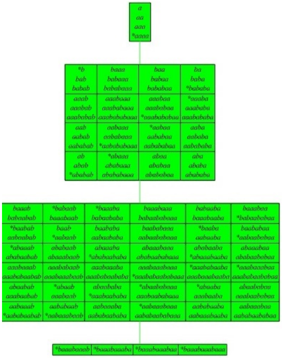


Figure: The transition Semigroup of $\mathscr{A} = (Q, A)$

How do these parameters relate to the Černý conjecture?

Figure: The minimum ideal of S

$$N(S, A') = 9$$

Černý-Pin conjecture [Rys92]

Let $\mathscr{A} = (Q, A)_r$ be a deterministic complete automaton, in which r is the minimal rank of a transformation in the transition semigroup of $\mathscr{A}$. Denote by $\ell_{sw}(\mathscr{A})$ the minimum length of the words with rank r.

Černý-Pin conjecture [Rys92]

Let $\mathscr{A} = (Q, A)_r$ be a deterministic complete automaton, in which r is the minimal rank of a transformation in the transition semigroup of $\mathscr{A}$. Denote by $\ell_{sw}(\mathscr{A})$ the minimum length of the words with rank r.

Remark

The automaton $\mathscr{A} = (Q, A)_1$ is synchronizing.

Černý-Pin conjecture [Rys92]

Let $\mathscr{A} = (Q, A)_r$ be a deterministic complete automaton, in which r is the minimal rank of a transformation in the transition semigroup of $\mathscr{A}$. Denote by $\ell_{sw}(\mathscr{A})$ the minimum length of the words with rank r.

Remark

The automaton $\mathscr{A} = (Q, A)_1$ is synchronizing.

Definition

For every $n \in N$ define,

$$cp(n) = \max\{\ell_{sw}(\mathscr{A}) \mid \mathscr{A} = (Q, A)_r, |Q| = n\}.$$

Conjecture

Černý-Pin conjecture *states that* $cp(n) = (n - r)^2$.

Conjecture

Černý-Pin conjecture states that $cp(n) = (n-r)^2$.

Let $\mathscr{A} = (Q, A)_r$ be a deterministic complete automaton. If S is the transition semigroup of $\mathscr{A}$, then

$$N(S, A') = \ell_{sw}(\mathscr{A}),$$

where $A' = \{\rho_a : q \mapsto qa \mid a \in A\}$.

Conjecture

Černý-Pin conjecture states that $cp(n) = (n-r)^2$.

Let $\mathscr{A} = (Q, A)_r$ be a deterministic complete automaton. If S is the transition semigroup of $\mathscr{A}$, then

$$N(S, A') = \ell_{sw}(\mathscr{A}),$$

where $A' = \{\rho_a : q \mapsto qa \mid a \in A\}$.

Conclusion

To calculate the shortest length of small rank words (reset words) in a deterministic complete automaton (synchronizing automaton)is equivalent to calculating the parameter $N(S, A)$ *for a finite transformation semigroup* S.

- How far apart can N, M and M' be?
  We present some results relating to the following semigroups
  - Certain families of transformation semigroups
  - Semilattices
  - Completely regular semigroups
  - 0-simple semigroups

Example 1

$a = (2,3,1)$, $b = (2,1,3)$,

$c = (1,2,1)$

$T_3 = \langle \{a, b, c\} \rangle$

$N(T_3, \{a,b,c\}) = 4$

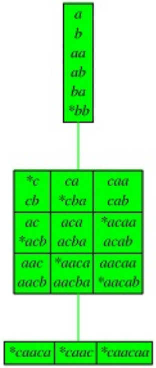


Figure: $\mathscr{D}$-classes in T_3

Example 2

$a = (2,3,1),\ b = (2,1,3),$

$c = (1,1,2)$

$T_3 = \langle\{a,b,c\}\rangle$

$N(T_3, \{a,b,c\}) = 2$

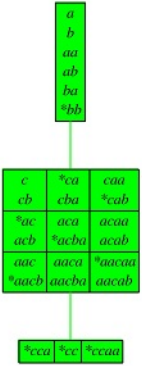


Figure: $\mathscr{D}$-classes in T_3

Fact

$$N(T_3) = 2,\ M(T_3) = 4$$

More generally:

$$N(T_n) = n - 1,\ M(T_n) = ?$$

Even more generally:

Proposition

The parameter $N(S)$ is equal to n, if S is one of the transformation semigroups $\mathcal{PT}_n, \mathcal{I}_n, \mathcal{PO}_n, \mathcal{POI}_n$ or $\mathcal{POPI}_n$; and it is equal to $n-1$, if S is one of the transformation semigroups $\mathcal{T}_n, \mathcal{O}_n$ or $Sing_n$.

Proof sketch

The half part of proof is an immediate consequence of the following lemma; and the other part is straightforward by using the results which have been proved in [GH87, GH92, How78, Fer00, Fer01].

Lemma

If $S \leq \mathcal{PT}_n$ is a finite transformation semigroup with a generating set $A \subseteq \{f \in S : \mathrm{rank}(f) \geq n-1\}$, then

$$N(S) \geq n - r,$$

where r is the rank of elements in the minimum ideal of S.

Semilattices

Definition

Let S be a finite semilattice. An element $s \in S$ is irreducible if $s = a \wedge b$ $(a, b \in S)$ implies $a = s$ or $b = s$. Denote by $I(S)$ the set of all irreducible elements of S.

Lemma

The set $I(S)$ is the unique generating set of S with minimum size. Furthermore, every generating set of S contains $I(S)$.

Corollary

If S is a finite semilattice, then

$$N(S) = M(S) = M'(S).$$

Proposition

The inequality $M'(S) \leq |I(S)|$ holds for every finite semilattice S. The equality holds when S is the free semilattice generated by $I(S)$.

Fact

Let S be a completely regular semigroup. Green's relation $\mathscr{D}$ is a congruence in S and $S/\mathscr{D}$ is a semilattice of $\mathscr{D}$-classes which are simple semigroups [Hig92].

Notation

Denote the semilattice $S/\mathscr{D}$ by S'. If a $\mathscr{D}$-class of S is an irreducible element of S' , then we call it an irreducible $\mathscr{D}$-class of S. Denote by $\mathrm{IRD}(S)$ the set of all irreducible $\mathscr{D}$-classes of S.

Lemma

Let S be a completely regular semigroup,

$$M'(S) \leq |\mathrm{IRD}(S)|.$$

0-Simple semigroups

Lemma

Let S be a finite regular 0-simple semigroup. Let $S = M^0[G, I, L, P]$ be represented as a Rees matrix semigroup over a group G, where P is a regular matrix with entries from $G \cup \{0\}$.

- *If P does not contain any entry equal to 0, then*

$$N(S) = M(S) = M'(S) = 1.$$

- *If P does contain at least one 0 entry, then*

$$N(S) = M(S) = M'(S) = 2.$$

- How do these parameters behave with respect to decompositions?

  We present an upper bound for $N(S)$ provided that S is a wreath product of two transformation semigroups.

Wreath product

Definition

Define $(X, S) \wr (Y, T) = (X \times Y, S^Y \rtimes T)$, *where the action of the semidirect product is given by*

$$\begin{aligned} T \times S^Y &\to S^Y \\ (t, f) &\mapsto {}^t f, \end{aligned}$$

$$\begin{aligned} {}^t f : Y &\to S \\ y &\mapsto ytf \end{aligned}$$

and the action of $S^Y \rtimes T$ *on the set* $X \times Y$ *is described by*

$$(x, y)(f, t) = (x(yf), yt).$$

Diameter

Definition

The directed diameter of a finite group G with respect to a set of generators A denoted by $d^+(G, A)$, is the maximum over $g \in G$ of the length of the shortest words in A representing g.

Special cases

Given two transformation monoids (X, S) and (Y, T).

- If T has trivial group of units, then

$$N(S^Y \rtimes T) \leq \max\{|Y|, d^+(U_S^Y, A')\}N(S) + N(T),$$

for every generating set A' of U_S^Y with minimum size.

Special cases

Given two transformation monoids (X, S) and (Y, T).

- If T has trivial group of units, then

$$N(S^Y \rtimes T) \leq \max\{|Y|, d^+(U_S^Y, A')\}N(S) + N(T),$$

for every generating set A' of U_S^Y with minimum size.

- If T has trivial group of units and $\mathrm{rank}(U_S^n) = n\,\mathrm{rank}(U_S)$, then

$$N(S^Y \rtimes T) \leq nN(S) + N(T),$$

where $n = |Y|$.

Special cases

Given two transformation monoids (X, S) and (Y, T).

- If T has trivial group of units, then

$$N(S^Y \rtimes T) \leq \max\{|Y|, d^+(U_S^Y, A')\}N(S) + N(T),$$

for every generating set A' of U_S^Y with minimum size.

- If T has trivial group of units and $\mathrm{rank}(U_S^n) = n\,\mathrm{rank}(U_S)$, then

$$N(S^Y \rtimes T) \leq nN(S) + N(T),$$

where $n = |Y|$.

- If S is a group, then

$$N(S^Y \rtimes T) \leq N(T).$$

General case

Theorem

Given two transformation monoids (X, S) and (Y, T). There exist integers $0 \leq m_1 \leq N(S)$ and $0 \leq m_2 \leq N(T)$ such that

$$N(S^Y \rtimes T) \leq (m_1+m_2)d^+(U_S^Y \rtimes U_T, A')+|Y|(N(S)-m_1)+N(T)-m_2,$$

for every generating set A' of $U_S^Y \rtimes U_T$ with minimum size.

General case

Theorem

Given two transformation monoids (X, S) and (Y, T). There exist integers $0 \leq m_1 \leq N(S)$ and $0 \leq m_2 \leq N(T)$ such that

$$N(S^Y \rtimes T) \leq (m_1+m_2)d^+(U_S^Y \rtimes U_T, A')+|Y|(N(S)-m_1)+N(T)-m_2,$$

for every generating set A' of $U_S^Y \rtimes U_T$ with minimum size.

Question

How large can the directed diameter of a (semi)direct product of a finite group be?

A generating set of minimum size

We used [Wie87] for calculating the rank of direct power of a finite semigroup and proved the following lemma:

Lemma

Let $(X, S), (Y, T)$ be two transformation monoids. Let A', A and B be generating sets with minimum size of $U_S^Y \rtimes U_T$, S and T, respectively. The set

$$G = A' \cup \{((a)_y, 1) : a \in A \setminus U_S, y \in Y\} \cup \{(\bar{1}, b) : b \in B \setminus U_T\}$$

is a generating set of $S^Y \rtimes T$ with minimum size.

Minimum ideal

Lemma

Let (X, S) and (Y, T) be two transformation monoids. Let I_S and I_T be the minimum ideals of S and T, respectively. The set

$$E = \{(f, t) : f \in I_S^Y,\ t \in I_T,\ f \text{ is a constant map}\}$$

is contained in the minimum ideal of $S^Y \rtimes T$.

Proof sketch

- Choose A, B such that $N(S, A) = N(S)$ and $N(T, B) = N(T)$.

Proof sketch

- Choose A, B such that $N(S, A) = N(S)$ and $N(T, B) = N(T)$.
- There exist $a_1, a_2, \ldots, a_{N(S)} \in A$ and $b_1, b_2, \ldots, b_{N(T)} \in B$ such that $a_1 a_2 \ldots a_{N(S)} \in I_S$ and $b_1 b_2 \ldots b_{N(T)} \in I_T$.

Proof sketch

- Choose A, B such that $N(S, A) = N(S)$ and $N(T, B) = N(T)$.
- There exist $a_1, a_2, \ldots, a_{N(S)} \in A$ and $b_1, b_2, \ldots, b_{N(T)} \in B$ such that $a_1 a_2 \ldots a_{N(S)} \in I_S$ and $b_1 b_2 \ldots b_{N(T)} \in I_T$.
- Define the function f from Y to I_S to be the constant map with image $a_1 a_2 \ldots a_{N(S)}$.

Proof sketch

- Choose A, B such that $N(S, A) = N(S)$ and $N(T, B) = N(T)$.
- There exist $a_1, a_2, \ldots, a_{N(S)} \in A$ and $b_1, b_2, \ldots, b_{N(T)} \in B$ such that $a_1 a_2 \ldots a_{N(S)} \in I_S$ and $b_1 b_2 \ldots b_{N(T)} \in I_T$.
- Define the function f from Y to I_S to be the constant map with image $a_1 a_2 \ldots a_{N(S)}$.
- The pair $(f, b_1 b_2 \ldots b_{N(T)})$ is an element of the minimum ideal of $S^Y \rtimes T$.

Proof sketch

- Choose A, B such that $N(S, A) = N(S)$ and $N(T, B) = N(T)$.
- There exist $a_1, a_2, \ldots, a_{N(S)} \in A$ and $b_1, b_2, \ldots, b_{N(T)} \in B$ such that $a_1 a_2 \ldots a_{N(S)} \in I_S$ and $b_1 b_2 \ldots b_{N(T)} \in I_T$.
- Define the function f from Y to I_S to be the constant map with image $a_1 a_2 \ldots a_{N(S)}$.
- The pair $(f, b_1 b_2 \ldots b_{N(T)})$ is an element of the minimum ideal of $S^Y \rtimes T$.
- We show that the pair $(f, b_1 b_2 \ldots b_{N(T)})$ is a product of at most $(m_1 + m_2)d^+(U_S^Y \rtimes U_T) + |Y|(N(S) - m_1) + N(T) - m_2$ elements in G, where

$$m_1 = |\{a_1, a_2, \ldots, a_{N(S)}\} \cap U_S|, \; m_2 = |\{b_1, b_2, \ldots, b_{N(T)}\} \cap U_T|.$$

Trivial upper bound

Question

How large can the directed diameter of a finite group be?

Trivial upper bound

Question

How large can the directed diameter of a finite group be?

Fact

The directed diameter of a finite group with respect to every generating set is at most the order of the group.

Trivial upper bound

Question

How large can the directed diameter of a finite group be?

Fact

The directed diameter of a finite group with respect to every generating set is at most the order of the group.

Example

The directed diameter of a cyclic group with respect to a singleton generating set is the order of the group.

What can we say about the direct power of a finite group?

What can we say about the direct power of a finite group? We have

$$d^+(G^n, A) \leq |G^n| = |G|^n.$$

What can we say about the direct power of a finite group? We have

$$d^+(G^n, A) \leq |G^n| = |G|^n.$$

I have tried to show that

Conjecture

Let G^n be the n-th direct power of a non trivial finite group G. There exists a generating set A for G^n of minimum size such that

$$d^+(G^n, A) \leq n|G|.$$

Observations

The following groups satisfy the conjecture:

Observations

The following groups satisfy the conjecture:

- Every group G with the following property

$$\mathrm{rank}(G^n) = n\,\mathrm{rank}(G),$$

(eg. nilpotent groups).

Observations

The following groups satisfy the conjecture:

- Every group G with the following property

$$\mathrm{rank}(G^n) = n\,\mathrm{rank}(G),$$

  (eg. nilpotent groups).
- The symmetric group S_n.

Observations

The following groups satisfy the conjecture:

- Every group G with the following property

$$\mathrm{rank}(G^n) = n\,\mathrm{rank}(G),$$

  (eg. nilpotent groups).
- The symmetric group S_n.
- The dihedral group D_n.

Observations

The following groups satisfy the conjecture:

- Every group G with the following property

$$\operatorname{rank}(G^n) = n \operatorname{rank}(G),$$

  (eg. nilpotent groups).
- The symmetric group S_n.
- The dihedral group D_n.

For proving these results I used the Wiegold's papers about the generating sets of minimum size for direct power of a finite group. [Wie74, Wie75, Wie78, Wie80, MW81]

References I

V. H. Fernandes.
The monoid of all injective orientation preserving partial transformations on a finite chain.
Comm. Algebra, 28(7):3401–3426, 2000.

V. H. Fernandes.
The monoid of all injective order preserving partial transformations on a finite chain.
Semigroup Forum, 62(2):178–204, 2001.

M. S. Gomes and J. M. Howie.
On the ranks of certain finite semigroups of transformations.
Math. Proc. Cambridge Philos. Soc., 101(3):395–403, 1987.

References II

M. S. Gomes and J. M. Howie.
On the ranks of certain semigroups of order-preserving transformations.
Semigroup Forum, 45(3):272–282, 1992.

P. M. Higgins.
Techniques of semigroup theory.
Oxford University Press, New York, 1992.

J. M. Howie.
Idempotent generators in finite full transformation semigroups.
Proc. Roy. Soc. Edinburgh Sect. A, 81(3-4):317–323, 1978.

References III

D. Meier and James Wiegold.
Growth sequences of finite groups. V.
J. Austral. Math. Soc. Ser. A, 31(3):374–375, 1981.

I. C. Rystsov.
On the rank of a finite automaton.
Kibernet. Sistem. Anal., (3):3–10, 187, 1992.

J. Wiegold.
Growth sequences of finite groups.
J. Austral. math. Soc. 17, pages 133–141, 1974.

References IV

James Wiegold.
Growth sequences of finite groups. II.
J. Austral. Math. Soc., 20(part 2):225–229, 1975.

James Wiegold.
Growth sequences of finite groups. III.
J. Austral. Math. Soc. Ser. A, 25(2):142–144, 1978.

James Wiegold.
Growth sequences of finite groups. IV.
J. Austral. Math. Soc. Ser. A, 29(1):14–16, 1980.

References V

J. Wiegold.
Growth sequences of finite semigroups.
J. Austral. math. Soc. (Ser.A) 43, pages 16–20, 1987.