Nasim Karimi

Reaching the minimum ideal in a finite semigroup

U.PORTO
FACULDADE DE CIÊNCIAS UNIVERSIDADE DO PORTO
DEPARTAMENTO DE MATEMÁTICA

February 2015

Nasim Karimi

Reaching the minimum ideal in a finite semigroup

Tese submetida à Faculdade de Ciências da Universidade do Porto para obtenção do grau de Doutor em Matemática

October 2014

U.PORTO
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO
DEPARTAMENTO DE MATEMÁTICA

To My Parents

Acknowledgments

First of all I would like to mention the contribution of my supervisors Prof. Jorge Almeida and Prof. Pedro Silva, whose ideas, guidance, patience, and support have been essential at all stages. I would also like to thank my supervisors for giving me an insight into their perception of mathematics, for hours of mathematical and non-mathematical conversation, for careful reading of the drafts of the papers and this thesis, for trying to teach me many useful tricks in producing a LaTeXdocument.

I would like to thank Prof. Manuel Delgado who always answers my questions kindly, and for several helpful comments concerning the technical computer problems and using GAP. I would like to thank Prof. Christian Lomp for sending me some useful papers and helping me to read some papers in german language. I would like to thank Dr. Markus Pfeffer, which I met in a conference in Novi Sad, Serbia in 2013, for his help to write some codes in GAP. I wish to express my thanks to Prof. Nicola Ruskuc, Prof. Robert Gray, Prof. Harald Helfgott, Prof. John Wilson, and Prof. Mikhail Volkov, for their attention and patience to answer me plenty of questions which I asked them personally or through emails. I wish to thank my friends Fahime and Saeid for thinking together at same stage and many stimulating conversations. I would also thank my colleague Dr. Emanuel Rodaro, for giving me some time to discuss about my work and his helpful comments. I also gratefully acknowledge the financial support of the FCT (Fundação para a Ciência e a Tecnologia).

At a personal level, I wish to express my special thanks to my family, specially my parents who tolerate all the difficulties to let me do my favorite things freely and for their encouragements in all the stages of my life. I thank specially my husband, Mohammad, for his constant and unconditional support during the four years of my PhD which was also the first four years of our married life in Portugal. His support and his love helped me to adapt

to a new life and made it easier for me to live far from the family. Last but by no means least, I would like to thank my lovely sisters and kind brothers who are always standing by me even in the most difficult moments in my life.

Resumo

Nesta dissertação estamos interessados em dois parâmetros envolvendo o comprimento de elementos em termos de um conjunto de geradores. Um deles é o comprimento mínimo de elementos no ideal mínimo (núcleo) de um semigrupo finito e o outro é o diâmetro de uma potência de um grupo finito.

No Capítulo 3 estudamos o comprimento mínimo de elementos do ideal mínimo de um semigrupo finito. Denotamos este parâmetro por $N(S, A)$, onde A é um conjunto de geradores do semigrupo finito S, e designamo-lo por A-profundidade de S. Introduzimos parâmetros de profundidade N', N, M' e M da seguinte forma: Seja $N(S)(M(S))$ o mínimo (máximo) $N(S, A)$ sobre conjuntos de geradores de tamanho mínimo; e seja $N'(S)(M'(S))$ o mínimo (máximo) $N(S, A)$ sobre todos os conjuntos de geradores. Estimamos os parâmetros de profundidade para algumas famílias de semigrupos finitos. Calculamos um majorante para $N(S)$, onde S é um produto em coroa ou um produto direto de dois monóides (de transformações) finitos.

No Capítulo 4 estamos interessados no diámetro de uma potência de um grupo finito. Denotemos por G^n a n-ésima potência do grupo G. Apresentamos as duas seguintes conjeturas.

Conjetura (forte). *Seja G um grupo finito. Então o diâmetro $D(G^n)$ é no máximo $n(|G| - \ rank(G))$.*

Conjetura (fraca). *Seja G um grupo finito. Existe um conjunto de geradores A de G^n de tamanho mínimo tal que* $\mathrm{diam}(G^n, A)$ *é no máximo $n(|G| - rank(G))$.*

Mostramos que os grupos Abelianos satisfazem a conjetura forte. Em seguida lidamos com geradores de tamanho mínimo para potências de grupos finitos. Mostramos que a conjetura fraca é válida para grupos nilpotentes, grupos simétricos e o grupo alternado A_4. Mostramos que se impusermos algumas restrições em n a conjetura fraca é válida para groupos diedrais.

Por fim, apresentamos alguns majorantes polinomiais para o diâmetro de potências de grupos solúveis.

Palavaras-chave. *semigrupos, conjunto de geradores, ideal minímo, diâmetro de um grupo, A-profundidade de um semigrupo*

Abstract

In this work we are interested in two parameters involving the length of elements in terms of a generating set. One is the minimum length of elements in the minimum ideal (kernel) of a finite semigroup and the other is the diameter of a direct power of a finite group.

In Chapter 3 we investigate the minimum length of elements in the minimum ideal of a finite semigroup. We denote this parameter by $N(S, A)$, where A is a generating set of the finite semigroup S, and we call it A-depth of S. We introduce depth parameters N', N, M' and M as follows: Let $N(S)$ ($M(S)$) be the minimum (maximum) $N(S, A)$ over generating sets of minimum size; and $N'(S)$ ($M'(S)$) be the minimum (maximum) $N(S, A)$ over all generating sets. We estimate the depth parameters for some families of finite semigroups. We give an upper bound for $N(S)$ where S is a wreath product or a direct product of two finite (transformation) monoids.

In Chapter 4 we are interested in the diameter of a direct power of a finite group. Denote by G^n the n-th direct power of the group G. We present the two following conjectures.

Conjecture (strong)**.** *Let G be a finite group. Then the diameter $D(G^n)$ is at most $n(|G| - \mathrm{rank}(G))$.*

Conjecture (weak)**.** *Let G be a finite group. Then there exists a generating set A for G^n of minimum size such that $\mathrm{diam}(G^n, A)$ is at most $n(|G| - \mathrm{rank}(G))$.*

We show that Abelian groups satisfy the strong conjecture. Then we deal with generating sets of minimum size for direct powers of finite groups. It is shown that the weak conjecture is true for nilpotent groups, symmetric groups and the alternating group A_4. We show that the weak conjecture is true for dihedral groups under some restrictions on n. Finally, we present

some polynomial upper bounds for the diameter of direct powers of solvable groups.

Keywords. *semigroups, generating sets, minimum ideal, diameter of a group, A-depth of a semigroup*

Contents

Contents **viii**

1 Introduction **1**

2 Preliminaries **5**
2.1 Depth parameters 5
2.2 Semilattices 7
2.3 Transformation semigroups 8
2.4 Finite automata and A-depth of a semigroup 10
2.5 Diameter of a finite group 11

3 A-depth of a finite semigroup **13**
3.1 A-depth for some families of finite semigroups 13
3.1.1 Examples 14
3.1.2 A-depth of transformation semigroups 17
3.2 A-depth and products of semigroups 30
3.2.1 Direct product 30
3.2.2 Wreath product 39

4 The diameter of a finite group **47**
4.1 Abelian groups and the strong conjecture 48
4.2 Generating sets of minimum size 52
4.2.1 Symmetric groups S_n 54
4.2.2 Dihedral groups D_n 54
4.2.3 Alternating groups A_n 55
4.2.4 Solvable Groups 56
4.3 Diameter of direct powers of groups 56
4.3.1 Symmetric groups S_n and the weak conjecture 58

4.3.2 Upper bound for the diameter of direct power of dihedral groups 62
4.3.3 Alternating groups and the weak conjecture 64
4.3.4 Upper bounds for the diameter of a direct power of a solvable group 67

5 Final remarks **74**

Bibliography **76**

Notation **80**

Chapter 1

Introduction

Consider a finite semigroup S with a generating set A. Every element in S can be represented as a product of generators in A. By the length of an element s in S, with respect to A, we mean the minimum length of a sequence which represents s in terms of generators in A. In finite semigroup (group) theory, several parameters may be defined involving the length of elements in terms of a generating set. In this work we are interested in two of these parameters. One is the minimum length of elements in the minimum ideal (kernel) of a finite semigroup and the other is the diameter of a direct power of a finite group. In the first part of this thesis we investigate the minimum length of elements in the minimum ideal of a finite semigroup. We denote this parameter by $N(S, A)$, where A is a generating set of the finite semigroup S, and we call it A-depth of S. We define the following parameters, called depth parameters, which depend only on the semigroup S,

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

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

and

$$N'(S) = \min\{N(S, A) : A \text{ is a minimal generating set}\},$$

$$M'(S) = \max\{N(S, A) : S = \langle A \rangle\}.$$

Note that the minimum over all generating sets is zero in case of a group and is one otherwise, so it is of no interest.

Part of our motivation to estimate such kind of parameters comes from a famous conjecture in automata theory attributed to Černý, a Slovak mathematician. In 1964 Černý conjectured that any n-state synchronizing automaton has a reset word of length at most $(n-1)^2$ [5]. In fact, the transition semigroup of any finite automaton is a finite transformation semigroup. A reset word in a synchronizing automaton is a constant transformation, which belongs to the minimum ideal of the transition semigroup. Hence the length of a reset word in a synchronizing automaton is equal to the length of an element in the minimum ideal of the transition semigroup, with respect to a generating set. Also, there is a generalization of Černý's conjecture, known as the Černý-Pin conjecture, which gives the upper bound $(n-r)^2$ for the length of a word of rank r in an automaton with n states in which the minimum rank of words is r. This version of conjecture is a reformulation of the stronger conjecture in [21], which was disproved in [16].[1] Here the automaton is not necessarily synchronizing but the words of minimum rank r represent elements in the minimum ideal of the transition semigroup.

We are also interested in investigating how the parameter $N(S, A)$ behaves with respect to the wreath product. In fact, the prime decomposition theorem states that any finite semigroup S is a divisor of an iterated wreath product of its simple group divisors and the three-element monoid U_2 consisting of two right zeros and one identity element [23]. So, it should be interesting to be able to say something about $N(S, A)$ provided that S is a wreath product of two finite transformation semigroups.

In the first section of Chapter 3 we estimate the depth parameters for some families of finite semigroups. More precisely, we establish that the depth parameters are equal, considerably small and easily calculable for any finite 0-simple semigroup. We show that semilattices have a unique minimal generating set. So, the depth parameters for semilattices are equal and again easily calculable. The third family of semigroups which we have considered is that of completely regular semigroups. For them the problem is reduced to the semilattice case. Afterward, we deal with transformation semigroups. We present in Theorem 1 a lower bound for $N'(S)$, where S is any finite transformation semigroup, and we show that it is sharp for several families of such semigroups. Applying this lower bound helps us to estimate the depth parameters for the transformation semigroups PT_n, T_n and I_n; their ideals $K'(n,r)$,$K(n,r)$ and $L(n,r)$; and the semigroups of order preserving

[1]The historical assessment appears at the end of Subsection 2.4.

transformations PO_n, O_n and POI_n. The main theorem in that section is Theorem 1 which is proved by two easy lemmas based on simple facts about construction of finite semigroups. Moreover, we use several results concerning the generating sets of minimum size of finite transformation semigroups (see for example [6, 7, 8, 9, 13, 14]).

In the second section of Chapter 3 we are interested in the behavior of the parameter $N(S)$ with respect to the wreath product and the direct product. For instance, we establish some lemmas to present a generating set of minimum size for the direct product (wreath product) of two finite monoids (transformation monoids). We compute the rank of the products (direct product or wreath product) in terms of their components.[2] Applying those results we give an upper bound for $N(S)$ where S is a wreath product or direct product of two finite transformation monoids.

In Chapter 4 we are interested in the diameter of a direct power of a finite group. In fact, since in some of the proposed upper bounds in 3.2 the diameter of a direct power of a finite group appears, our research leads to work in a different direction, namely the estimation of the diameter of a direct power of a finite group. Let G be a finite group with a generating set A. By the diameter of G with respect to A we mean the maximum over $g \in G$ of the length of the shortest word in A representing g. Our definition here is a bit different from which has been usually considered in the literature. Usually group theorists define the diameter to be the maximum over $g \in G$ of the length of a shortest word in $A \cup A^{-1}$ representing g. Let us call this version of the diameter to be "symmetric diameter". Asymptotic estimate of the symmetric diameters of non-Abelian simple groups with respect to various types of generating sets can be find in the survey [4], which also lists related work, e.g., on the diameters of permutation groups. We are interested in the behavior of the diameter with respect to the direct product. Specially, we focus on the direct power of a finite group. More precisely, let G be a finite group and G^n be the n-th direct power of G. Let A be a minimal generating set of G^n. Our objective is to find a reasonable answer to the following question. How large may be the diameter of G^n with respect to A? A simple argument shows that the diameter of a group with respect to any generating set is bounded above by the group order minus the group rank (see Proposition 1) . The cyclic groups are examples whose diameter is as large as the group order minus the group rank. It is obvious that G^n

[2] The interested reader may find very similar results in [24].

is not cyclic for $n \geq 2$ and $|G| \neq 1$. Then the following natural question arises. Is there any smaller upper bound (less than $|G^n| - \mathrm{rank}(G^n)$) for the diameter of G^n? In fact, $|G|^n - \mathrm{rank}(G^n)$ is exponentially large in terms of $|G|$. The more precise question in which we are really interested is whether the diameter of a direct power of a finite group is polynomially bounded. These questions lead to the conjectures which are the topic of Chapter 4. Denote by G^n the n-th direct power of the group G.

Conjecture (strong). *Let G be a finite group. Then the diameter $D(G^n)$ is at most $n(|G| - \mathrm{rank}(G))$.*

Conjecture (weak). *Let G be a finite group. Then there exists a generating set A for G^n of minimum size such that* $\mathrm{diam}(G^n, A)$ *is at most $n(|G| - \mathrm{rank}(G))$.*

In the first section of Chapter 4 we show that Abelian groups satisfy the strong conjecture. The second section deals with generating sets of minimum size for direct power of finite groups. Finding a generating set of minimum size for a direct power of a group is itself a problem. Nevertheless, there exist in the literature many results regarding the computation of the rank of a direct power of a finite group, e.g., [27, 28, 29, 30, 31]. We use such kind of results to find generating sets of minimum size for direct powers of some families of finite groups such as the symmetric group S_n and the dihedral group D_n. With a different approach (see [11]) we establish generating sets of minimum size for the direct powers A_5^2, A_5^3, A_5^4, where A_5 is the alternating group of degree five. In the third section of Chapter 4, we show that the weak conjecture is true for nilpotent groups, symmetric groups and the alternating group A_4. We show that the weak conjecture holds for dihedral groups under some restrictions on n. Finally, we present some polynomial upper bounds for the diameter of a direct power of a solvable group.

Chapter 2

Preliminaries

In this chapter we present the notation and definitions which we use in the sequel. For standard terms in semigroup theory see [22].

2.1 Depth parameters

A *semigroup* is a non-empty set with an associative binary operation. Note that in this work we are only interested in finite semigroups. A semigroup with an identity element, usually denoted by 1, is called a monoid. Let S be a finite semigroup. The non-empty subset $S' \subseteq S$ is a *subsemigroup* of S if it is closed under the binary operation of S. The subsemigroup I is an *ideal* of S if $SI \cup IS \subseteq I$. An ideal I of a semigroup S is minimal if, for every ideal J of S, $J \subseteq I$ implies $I = J$. We note that if such an ideal exists it is necessarily unique so we may call it the *minimum ideal*. It is obvious that every finite semigroup has a minimum ideal which we call the *kernel* of S and denote by $\ker(S)$. A non-empty subset $A \subseteq S$ is a *generating set*, if every element in S can be represented as a product of elements (generators) in A. We use the notation $S = \langle A \rangle$ when A is a generating set of S. A generating set A is called *minimal* if no proper subset of A is a generating set of S. By the *rank* of a semigroup S, denoted by $\mathrm{rank}(S)$, we mean the cardinality of any of the smallest generating sets of S.[1]

[1] When S is a non trivial finite group, our notion of (semigroup) rank coincides with the notion of rank used in group theory (which allows the uses of inverses) since the inverse of an element a equals necessarily some power of a. The rank of the trivial group is determined by Convention 1.

Convention 1. *Since in chapter 3 we deal with semigroups it is more convenient to consider the rank of the trivial group to be one. While in Chapter 4 we consider the rank of the trivial group to be zero as usual.*

We suppose that the reader is familiar with the Green relations in the classical theory of finite semigroups. For a convenient reference see [22].

Remark 1. We use the fact that $\mathcal{J} = \mathcal{D}$ for a finite semigroup (the equality may fail for an infinite semigroup) several times in our proofs without mentioning it explicitly.

Definition 1. Let S be a finite semigroup with a generating set A. For every non identity element $s \in S$, the *length* of s with respect to A, denoted by $l_A(s)$, is defined to be

$$l_A(s) := \min\{k : s = a_1 a_2 \cdots a_k, \text{ for some } a_1, a_2, \ldots, a_k \in A\},$$

and the length of the identity (if there is any) is zero by convention. Furthermore, for any non empty subset T of S, the maximum (minimum) length of T with respect to A, denoted by $Ml_A(T)$ ($ml_A(T)$), is the maximum (minimum) length of elements, with respect to A, in T.

Definition 2. Let S be a finite semigroup with a generating set A. By the *A-depth* of S we mean the number

$$N(S, A) := ml_A(\ker(S)).$$

We may consider the following parameters, defined in terms of the notion of A-depth, but which depend only on S:

Definition 3. Let S be a finite semigroup. Define

$$\begin{aligned}
N(S) &:= \min\{N(S, A) : S = \langle A \rangle, |A| = \operatorname{rank}(S)\},\\
N'(S) &:= \min\{N(S, A) : \ A \text{ is a minimal generating set}\}\\
M(S) &:= \max\{N(S, A) : S = \langle A \rangle, |A| = \operatorname{rank}(S)\},\\
M'(S) &:= \max\{N(S, A) : S = \langle A \rangle\}.
\end{aligned}$$

These are henceforth called the *depth parameters* of S.

Example 1. If G is a group then $N(G, A) = 0$, for every generating set A of G. Hence all the depth parameters of G are equal to zero.

Remark 2. Note that the minimum A-depth over all generating sets of a finite semigroup which is not a group is one.

Remark 3. If $A \subseteq B$, then $N(S,B) \leq N(S,A)$. Hence

$$M'(S) = \max\{N(S,A) : \ A \text{ is a minimal generating set}\}.$$

Remark 4. It is easy to see that

$$N'(S) \leq N(S) \leq M(S) \leq M'(S).$$

Notation 1. Let $i \geq 1, \ n \geq 1$ and $C_{i,n} := \langle a : a^i = a^{i+n} \rangle$ be the *monogenic semigroup* with index i and period n.

Example 2. For $i > 1$ we have $N(C_{i,n}, A) = i$ for every minimal generating set A of $C_{i,n}$. Hence all the depth parameters are equal for all finite monogenic semigroups with index $i > 1$.

2.2 Semilattices

A *semilattice* is a semigroup $(S, .)$ such that, for any $x, y \in S$, $x^2 = x$ and $xy = yx$. Let $(S, \wedge)$ be a semilattice. For every $x, y \in S$ define: $x \leq y$ if $x = x \wedge y$. It is easy to see that $(S, \leq)$ is a *partially ordered set* that has a meet (a greatest lower bound) for any nonempty finite subset [1].

Example 3. Let X be a set. The set $P(X)$ (set of subsets of X) with the binary operation of union is a semigroup. Since this semigroup is a free object in the variety of semilattices we call it the free semilattice generated by X.

Definition 4. Let S be a semilattice. An element $s \in S$ is *irreducible* if $s = ab$ $(a, b \in S)$ implies $a = s$ or $b = s$. Denote by $I(S)$ the set of all irreducible elements of S.

Let $(S, \leq)$ be a partially ordered set. As usual let $<$ be the relation on S such that $u < v$ if and only if $u \leq v$ and $u \neq v$. Let u, v be elements of S. Then v covers u , written $u \prec v$, if $u < v$ and there is no element w such that $u < w < v$. By the *diagram* of $(S, \leq)$ we mean the directed graph with the vertex set S such that there is an edge $u \rightarrow v$ between the pair $u, v \in S$ if $u \prec v$.

Notation 2. Given a vertex v of a directed graph, the *in-degree* of v denoted by $\mathrm{d}^{\mathrm{in}}(v)$, is the number of w such that (w, v) is an edge; the *out-degree* of v, denoted by $\mathrm{d}^{\mathrm{out}}(v)$, is the number of w such that (v, w) is an edge.

Remark 5. Consider a finite semilattice S. By definition, the set S has an infimum, which is the zero of S. Notice that in the diagram of S, the vertex corresponding to zero is the unique vertex which has in-degree zero.

Remark 6. Consider a finite semilattice S with the property that the subset $\{x \in S : x \leq s\}$ is a chain for all $s \in S$. Then the diagram of S is a rooted tree in which the root represents the zero of S.

2.3 Transformation semigroups

The notation and the definitions in this section can be find in [6, 7, 9, 13, 14, 8, 23].

Notation 3. Let $\mathbb{N}$ be the set of all natural numbers. For $n \in \mathbb{N}$ denote by X_n the chain with n elements, say $X_n = \{1, 2, \cdots, n\}$ with the usual ordering.

As usual, we denote by PT_n the semigroup of all partial functions of X_n (under composition) and we call the elements of PT_n transformations. We introduce two formally different (yet equivalent) definitions of a transformation semigroup:

Definition 5. By transformation semigroup, with degree n, we mean a subsemigroup of the partial transformation semigroup PT_n.

Let S be a finite semigroup and X be a finite set. The semigroup S faithfully acting on the right of the set X means that there is a map $X \times S \to X$, written $(x, s) \mapsto xs$, satisfying:

- $x(s_1 s_2) = (xs_1)s_2$;
- If for every $x \in X$ $xs_1 = xs_2$, then $s_1 = s_2$.

Definition 6. By a transformation semigroup (X, S) we mean a semigroup S faithfully acting on the right of a set X.

We use the first definition in 3.1.2 and the second one in 3.2.2. We define the families of transformation semigroups whose A-depth is estimated in 3.1.2. Define the full transformation semigroup T_n and the symmetric inverse monoid I_n as follows:

$$\begin{aligned} T_n &:= \{\alpha \in PT_n : \mathrm{Dom}(\alpha) = X_n\}, \\ I_n &:= \{\alpha \in PT_n : \alpha \text{ is an injective transformation}\}. \end{aligned}$$

We can define more transformation semigroups which are subsemigroups of PT_n, T_n or I_n. For instance, for $1 \leq r < n$ the following semigroups are ideals of PT_n, T_n and I_n, respectively.

$$\begin{aligned} K'(n,r) &:= \{\alpha \in PT_n : \mathrm{rank}(\alpha) \leq r\}, \\ K(n,r) &:= \{\alpha \in T_n : \mathrm{rank}(\alpha) \leq r\}, \\ L(n,r) &:= \{\alpha \in I_n : \mathrm{rank}(\alpha) \leq r\}. \end{aligned}$$

Also, we can define more transformation semigroups when we consider the (partial) transformations to be order preserving. We say that a transformation s in PT_n is *order preserving* if, for all $x, y \in \mathrm{Dom}(s)$, $x \leq y$ implies $xs \leq ys$. Clearly, the product of two order preserving transformations is an order preserving transformation. Let

$$\begin{aligned} PO_n &:= \{\alpha \in PT_n \setminus \{1\} : \alpha \text{ is order preserving}\}, \\ O_n &: \{\alpha \in T_n \setminus \{1\} : \alpha \text{ is order preserving}\}, \\ POI_n &:= \{\alpha \in I_n \setminus \{1\} : \alpha \text{ is order preserving}\}. \end{aligned}$$

Note that PO_n, O_n and POI_n are aperiodic semigroups (i.e., have trivial $\mathcal{H}$-classes). Denote by $J_{n-1}(PO_n)$, $J_{n-1}(O_n)$ and $J_{n-1}(POI_n)$ the maximum $\mathcal{J}$-class in PO_n, O_n and POI_n, respectively. The $\mathcal{J}$-classes $J_{n-1}(PO_n)$, $J_{n-1}(O_n)$ and $J_{n-1}(POI_n)$ have n $\mathcal{L}$-classes which consist of (partial) transformations of rank $n-1$ with the same image. The $\mathcal{J}$-class $J_{n-1}(PO_n)$ has two kinds of $\mathcal{R}$-classes, n $\mathcal{R}$-classes consisting of proper partial transformations of rank $n-1$ and $n-1$ $\mathcal{R}$-classes consisting of total transformations of rank $n-1$; the $\mathcal{J}$-class $J_{n-1}(O_n)$ has $n-1$ $\mathcal{R}$-classes consisting of transformations of rank $n-1$; and the $\mathcal{J}$-class $J_{n-1}(POI_n)$ has n $\mathcal{R}$-classes consisting of proper partial transformations of rank $n-1$.

2.4 Finite automata and A-depth of a semigroup

We follow in this section the terminology of [25].

A *finite automaton* is a pair $A = (Q, \Sigma)$, where Q is a finite state set and Σ is a finite set of input symbols, each associated with a mapping on the state set $\sigma : Q \longrightarrow Q$ (note that we use the same notation for the symbols in Σ and the associated mappings). A sequence of input symbols of the automaton will be called for brevity an *input word*. To every input word $w = \sigma_1\sigma_2 \ldots \sigma_k$ is associated a mapping on the state set, which is a composition of the mappings corresponding to σ_i, $1 \leq i \leq k$. By the action of an input word we mean the action of the associated mapping. The action of the input word w on the state q is denoted $(q)w$ and the action of the input word w on the subset of states T is denoted $(T)w$. Denote by S_A the *transition semigroup* of A generated by the associated mappings of input symbols. In fact, (Q, S_A) is the transformation semigroup generated by Σ.

Definition 7. The *rank* of a finite automaton is the minimum rank of its input words (the *rank* of a mapping is the cardinality of its image). An input word of minimum rank is called *terminal*.

A finite automaton with rank one is called synchronizing and every terminal word in a synchronizing automaton is a *reset word*. It is clear that the minimum ideal of the transition semigroup S_A consists of the terminal words of the automaton A. Meanwhile, the parameter $N(S_A, \Sigma)$ is the minimum length of terminal words in the automaton $A = (Q, \Sigma)$. In fact, to compute the number $N(S, A)$, where S is a finite transformation semigroup with a generating set A, is equivalent to finding the minimum length of terminal words in a finite automaton with transition semigroup S. The importance of knowing the length of the terminal words in a finite automaton is motivated by the two following conjectures attributed to Černý and Pin, respectively.

Conjecture. *[5] Every n-state synchronizing automaton has a reset word of length at most $(n-1)^2$.*

Conjecture. *Every n-state automaton of rank r has a terminal word of length at most $(n-r)^2$.*

We mention that Pin generalized the Černý conjecture as follows [21]. Suppose $A = (Q, \Sigma)$ is an automaton such that some word $w \in \Sigma^*$ acts on Q

as a transformation of rank r. Then he proposed that there should be a word of length at most $(n-r)^2$ acting as a rank r transformation. This generalized conjecture was disproved by Kari [16]. However, the above conjecture is a reformulation of the Pin conjecture that is still open (and that was introduced by Rystsov as being the Pin conjecture [25]).

2.5 Diameter of a finite group

In Chapter 4 we deal with the notion of diameter of a finite group. Since this notion has different definitions in the literature we introduce here our definitions and notation precisely.

Let G be a finite group with a generating set A. Denote by A^{-1} the set $\{a^{-1} : a \in A\}$. By the *symmetric length* of an element $g \in G$, with respect to A, we mean the minimum length of a sequence which represents g in terms of elements in $A \cup A^{-1}$. Denote this parameter by $l^s_A(g)$.

Now we have the following different definitions for the diameter of a finite group with respect to a generating set.

Definition 8. Let G be a finite group with generating set A. By the *diameter* of G with respect to A we mean

$$\operatorname{diam}(G, A) := \max\{l_A(g) : g \in G\}.$$

Definition 9. Let G be a finite group with generating set A. By the *symmetric diameter* of G with respect to A we mean

$$\operatorname{diam}^s(G, A) := \max\{l^s_A(g) : g \in G\}.$$

Notation 4. Denote by $D(G)$ (respectively $D^s(G)$) the maximum diameter (respectively symmetric diameter) over all generating sets of G.

Remark 7. Let G be a finite group with a generating set A. For $g \in G$ we have $l^s_A(g) \leq l_A(g)$ and $D^s(G) \leq D(G)$.

The terminology of diameter and symmetric diameter of a group comes from the diameter of the Cayley graph and the directed Cayley graph of a group.

Definition 10. By the *Cayley graph* of a group G with respect to a generating set A we mean the graph whose set of vertices is G and such that there is an edge between $g_1, g_2 \in G$ if and only if $g_1^{-1}g_2 \in A \cup A^{-1}$. We denote this graph by $\operatorname{Cay}(G, A)$.

Definition 11. By *directed Cayley graph* of group G with respect to a generating set A we mean the directed graph whose set of vertices is G and such that there is an edge from g_1 to g_2 if and only if $g_1^{-1}g_2 \in A$. We denote this graph by $\overrightarrow{\mathrm{Cay}}(G, A)$.

Definition 12. A directed graph is called *strongly connected* if it contains a directed path from u to v and a directed path from v to u for every pair of vertices u, v.

The distance between two vertices in a connected graph is the length of the shortest path between them. In the case of a strongly connected directed graph the distance between two vertices u and v is defined as the length of the shortest path from u to v. Notice that, in contrast with the case of undirected graphs, the distance between u and v dose not necessarily coincide with the distance between v and u, so it is not a distance in the metric sense of the word. We consider the *diameter* of a (strongly connected directed) graph as usual, that is, the maximum of distances between two vertices over all pairs of vertices in the vertex set. It is easy to see that the symmetric diameter of a group with respect to a generating set is equal to the diameter of the corresponding Cayley graph; and the diameter of a group with respect to a generating set is equal to the diameter of the corresponding directed Cayley graph (note that the directed Cayley graph of a group is always strongly connected).

The following proposition gives a general upper bound for the diameter of a finite group.

Proposition 1. *Let G be a finite group. We have $D(G) \leq |G| - \mathrm{rank}(G)$.*

Proof. Let X be an arbitrary generating set of G. It is enough to show that $\mathrm{diam}(G, X) \leq |G| - \mathrm{rank}(G)$. Without loss of generality suppose that $1 \notin X$. Let $\mathrm{diam}(G, X) = t$. There exist $g \in G$ and $x_1, x_2 \ldots, x_t \in X$ such that $g = x_1 x_2 \cdots x_t$ and t is the smallest number for which g has such a kind of decomposition in X. Hence $x_1, x_1x_2, \ldots, x_1x_2 \cdots x_t$ are t distinct non identity elements of G. On the other hand, X has $|X| - 1$ elements distinct from $x_1, x_1x_2, \ldots, x_1x_2 \cdots x_t$. By adding the identity to these distinct elements we get $|G| \geq t + |X| - 1 + 1$, which gives the inequality $\mathrm{diam}(G, X) \leq |G| - |X|$. Now the result follows from $\mathrm{rank}(G) \leq |X|$. $\square$

Chapter 3

A-depth of a finite semigroup

This chapter is organised as follows. In the first section our goal is estimating the depth parameters for some families of finite semigroups. In the second section we investigate the behaviour of those parameters with respect to products (direct product and wreath product).

3.1 A-depth for some families of finite semigroups

In this section we estimate the depth parameters for some families of finite semigroups. We start with 0-simple semigroups. We establish that the depth parameters are equal, considerably small and easily computable for any finite 0-simple semigroup. Then we show that semilattices have a unique minimal generating set. So, the depth parameters are equal and again easily computable. The third family of semigroups which we have considered is that of completely regular semigroups. For them the problem is reduced to the semilattice case.

In all of the above examples, we did not represent semigroups as transformation semigroups. On the other hand, representing the elements of a semigroup as transformations make us able to do some calculations. In the second section of this chapter we deal with transformation semigroups. We present in Theorem 1 a lower bound for $N'(S)$, where S is any finite transformation semigroup, and we show that it is sharp for several families of such semigroups. Applying this lower bound helps us to estimate the depth parameters for some families of finite transformation semigroups.

3.1.1 Examples

The following lemma is an easy observation which we are going to use frequently.

Lemma 1. *Let S be a finite semigroup and I be an ideal of S. If I is contained in the subsemigroup generated by the set $S \setminus I$, then every minimal generating set of S must be contained in $S \setminus I$.*

Proof. Let A be a minimal generating set of S. Suppose that $a \in I \cap A$. Because I is contained in the subsemigroup generated by the set $S \setminus I$, a can be written as a product of elements in $S \setminus I$. Moreover, because I is an ideal and A is a generating set, every factor of this product can be written as a product of generators in $A \setminus I$. Therefore, a can be written as a product of elements in $A \setminus I$, which contradicts the minimality of A. This shows that $A \cap I = \emptyset$. Hence we have $A \subseteq S \setminus I$. □

A semigroup S is called 0-*simple* if it possesses a zero, which is denoted by 0, if $S^2 \neq 0$, and if ϕ, $\{0\}$ and S are the only ideals of S [22]. The 0-simple semigroups are examples of semigroups whose parameters M, N, M', N' are equal, considerably small and easily computable.

Lemma 2. *If S is a finite 0-simple semigroup then*

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

Proof. If S is a finite 0-simple semigroup then it is isomorphic to a regular Rees matrix semigroup [22]. 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 every generating set must contain the zero element (since the other elements do not generate it). Therefore $N(S) = M(S) = M'(S) = N'(S) = 1$. Suppose that P does contain at least one 0 entry. In this case, no minimal generating set can contain the zero element of S, since then 0 forms an ideal of S and the subsemigroup generated by $S \setminus \{0\}$ contains 0 (see Lemma 1). Let A be any generating set of S. We show that there are at least two not necessarily distinct elements of A whose product is 0. Let for some $k \geq 2$

$$(i_1, g_{i_1}, j_1)(i_2, g_{i_2}, j_2) \cdots (i_k, g_{i_k}, j_k) = 0.$$

Then there exists $1 \leq l < k$ such that $p_{j_l i_{l+1}} = 0$. Hence

$$(i_l, g_{i_l}, j_l)(i_{l+1}, g_{i_{l+1}}, j_{l+1}) = 0.$$

Therefore there are two not necessarily distinct elements of A whose product is 0, which shows that $N(S, A) = 2$. It follows that

$$N(S) = M(S) = M'(S) = N'(S) = 2. \quad \square$$

Let S be a finite semilattice. We show that $I(S)$, the set of all irreducible elements of S, is the unique minimal generating set of S. This leads to the equality of all parameters M, N, M', N' . Then we find a sharp upper bound for $I(S)$-depth of S. Finally, the special case where the diagram of S is a rooted tree is considered.

Lemma 3. *Let S be a semilattice. The set $I(S)$ is the unique minimal generating set of S.*

Proof. Let A be a generating set. First we show that $I(S) \subseteq A$. Let $s \in I(S)$. If $s \notin A$ then s is a product of some elements in A none of which is equal to s. This is in contradiction with irreducibility of s. Hence $s \in A$.

Now we show that $I(S)$ is a generating set of S. Let $s \in S \setminus I(S)$. Then there exist $a, b \in S$ such that $s = a \wedge b$ while $s \neq a, s \neq b$. If both a, b are irreducible then we are done, otherwise we repeat this process for a, b. This process must end after a finite number of steps because S is finite and the elements which are produced at each step are strictly larger than the elements encountered in the previous step. $\square$

The following corollary is an immediate consequence of Lemma 3.

Corollary 1. *Let S be a finite semilattice. Then*

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

Proposition 2. *The inequality $N(S, I(S)) \leq |I(S)|$ holds for every finite semilattice S. The equality holds if and only if S is the free semilattice generated by $I(S)$.*

Proof. First we show that the product of all elements in $I(S)$ is zero. Let $I(S) = \{a_1, a_2, \ldots, a_n\}$ and denote $a_1 a_2 \cdots a_n$ by t. If $s \in S$, then there exist

$a_{i_1}, a_{i_2}, \ldots, a_{i_k} \in I(S)$ such that $s = a_{i_1} a_{i_2} \cdots a_{i_n}$. Now we have $st = ts = t$ because S is commutative and idempotent. Therefore $t = 0$.

For the second statement, first suppose that S is the free semilattice generated by $I(S)$. We show that $N(S) = |I(S)|$. Since $I(S)$ is a generating set of S, there exist $a_{i_1}, a_{i_2}, \ldots, a_{i_k} \in I(S) = \{a_1, a_2, \ldots, a_n\}$ such that $a_{i_1} a_{i_2} \cdots a_{i_k} = 0$; because S is commutative and idempotent we can suppose the a_{i_j}'s to be distinct. Therefore, by the preceding paragraph, we have $a_{i_1} a_{i_2} \cdots a_{i_k} = a_1 a_2 \cdots a_n = 0$. Now because S is a free semilattice

$$\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\} = \{a_1, a_2, \ldots, a_n\}$$

so that $k = n$.

Conversely, suppose $N(S, I(S)) = |I(S)|$, we show that S is the free semilattice generated by $I(S)$. Suppose

$$a_{i_1} a_{i_2} \cdots a_{i_k} = a_{j_1} a_{j_2} \cdots a_{j_\ell}. \tag{3.1}$$

Let $\{a_{i_{k+1}}, a_{i_{k+2}}, \ldots a_{i_n}\}$ be the set $I(S) \setminus \{a_{i_1}, \ldots, a_{i_k}\}$. By equality (3.1), we have

$$a_{i_1} a_{i_2} \cdots a_{i_k} a_{i_{k+1}} a_{i_{k+2}} \cdots a_{i_n} = a_{j_1} a_{j_2} \cdots a_{j_l} a_{i_{k+1}} a_{i_{k+2}} \cdots a_{i_n}.$$

Since $N(S) = M'(S) = |I(S)|$ the subset $\{a_{j_1}, a_{j_2}, \ldots a_{j_\ell}, a_{i_{k+1}}, a_{i_{k+2}}, \ldots a_{i_n}\}$ must be the whole set $I(S)$. This shows that

$$\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\} \subseteq \{a_{j_1}, a_{j_2} \ldots, a_{j_\ell}\}.$$

By symmetry, the reverse inclusion $\{a_{j_1}, \ldots, a_{j_\ell}\} \subseteq \{a_{i_1}, \ldots, a_{i_k}\}$ also holds. It follows that S is the semilattice freely generated by $I(S)$. $\square$

Proposition 3. *If the diagram of a finite semilattice S is a rooted tree then $N(S, I(S)) \leq 2$.*

Proof. Denote the diagram of S by T. It is clear that

$$I(S) = \{v \in V(T) : \mathrm{d}^{\mathrm{out}}(v) \leq 1\}.$$

Let v_0 be the root of the tree T. If v_0 belongs to $I(S)$ then $N(S, I(S)) \leq 1$. Suppose that $v_0 \notin I(S)$. We show that there are two elements in $I(S)$ whose product is zero. Because $\mathrm{d}^{\mathrm{out}}(v_0) \geq 2$, there exist two distinct vertices v_1, v_2 such that $v_0 \to v_1$ and $v_0 \to v_2$. Denote by T_i the rooted sub-tree of T with v_i as its root. Note that $V(T_i) \cap I(S) \neq \varnothing$ because every sub-tree contains leaves and leaves are irreducible. If u_i belongs to $V(T_i) \cap I(S)$ then $u_1 u_2 = 0$. $\square$

Let S be a completely regular semigroup. Green's relation $\mathcal{D}$ is a congruence in S and $S/\mathcal{D}$ is a semilattice of $\mathcal{D}$-classes which are simple semigroups [12]. Hence by the results obtained for semilattices, we have the following lemma for completely regular semigroups.

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

Lemma 4. *Let S be a completely regular semigroup. Then the following inequality holds*

$$M'(S) \leq N(S/\mathcal{D}) \leq |\mathrm{IRD}(S)|.$$

Proof. Let A be a generating set of S. First we show that $D \cap A \neq \varnothing$ for every $D \in \mathrm{IRD}(S)$. Let $D \in \mathrm{IRD}(S)$ and $d \in D$. There exist $a_1, a_2, \ldots, a_j \in A$ such that $d = a_1 a_2 \cdots a_j$. Therefore $D_{a_1} D_{a_2} \cdots D_{a_j} \subseteq D_d = D$. Because D is an irreducible $\mathcal{D}$-class of S there exists $k \in \{1, 2, \ldots, j\}$ such that $D_{a_k} = D$. Therefore $a_k \in D \cap A \neq \varnothing$.

We now prove the first inequality. Let $t = N(S/\mathcal{D})$. By Corollary 1, there are irreducible $\mathcal{D}$-classes $D_1, D_2, \ldots, D_t$ of S such that $D_1 D_2 \cdots D_t = \ker(S)$. Let $a_i \in A \cap D_i$ (we have shown that it exists). Then $a_1 a_2 \cdots a_t \in \ker(S)$, whence $N(S, A) \leq t$. Since A is arbitrary, we get $M'(S) \leq N(S/\mathcal{D})$. The second inequality follows from Proposition 2. □

3.1.2 A-depth of transformation semigroups

Our main goal in this section is estimating the depth parameters for some families of finite transformation semigroups.

First we find a lower bound for $N'(S)$ where S is any finite transformation semigroup. Let S be a finite transformation semigroup and A be a minimal generating set of S. Denote by $r(S, A)$ the minimum of the ranks of elements in A; and denote by $t(S)$ the rank of elements in the minimum ideal of S. The following corollary of Lemma 1 shows that $r(S, A)$ is independent of the choice of the minimal generating set A.

Corollary 2. *Let $S \leq PT_n$ be a finite transformation semigroup. Let A and B be two minimal generating sets of S. We have $r(S, A) = r(S, B)$.*

Proof. It is enough to show that

$$\min\{\mathrm{rank}(f) : f \in A\} \leq \min\{\mathrm{rank}(f) : f \in B\}.$$

Let $\min\{\text{rank}(f) : f \in A\} = r$. Consider the subsemigroup

$$I = \{f \in S : \text{rank}(f) < r\}.$$

It is easy to see that I is an ideal of S. Since $A \subseteq S \setminus I$, by Lemma 1 we have $B \subseteq S \setminus I$. Hence $\min\{\text{rank}(f) : f \in B\} \geq r$. $\square$

From now on, we use $r(S)$ instead, since it depends only on S.

Lemma 5. *Let $X = \{f \in PT_n : \text{rank}(f) \geq r\}$. For $f_1, f_2, \ldots, f_k \in X$ the inequality*

$$\text{rank}(f_1 f_2 \cdots f_k) \geq n - k(n - r), \tag{3.2}$$

holds.

Proof. We use induction on k. For $k = 1$, the lower bound given by (3.2) is obvious. Now, let $f_1, f_2, \ldots, f_{k+1}$ be $k+1$ not necessarily distinct elements of X. Denote the composite transformation $f_1 f_2 \cdots f_k$ by f. By the induction hypothesis, we know that $\text{rank}(f) \geq n - k(n-r)$. Then, it is enough to show for $f_{k+1} \in X$ that

$$\text{rank}(f f_{k+1}) \geq n - (k+1)(n - r).$$

Let $\text{rank}(f) = t$ and $\text{Im}(f) = \{a_1, a_2, \ldots, a_t\}$. Suppose that

$$\text{rank}(f f_{k+1}) < n - (k+1)(n - r).$$

Because $\text{rank}(f_{k+1}) \geq r$, it follows that

$$|(X_n \setminus \{a_1, a_2, \ldots, a_t\}) f_{k+1}| > r - (n - (k+1)(n - r)).$$

On the other hand,

$$|(X_n \setminus \{a_1, a_2, \ldots, a_t\}) f_{k+1}| \leq n - t.$$

Hence $r - (n - (k+1)(n - r)) < n - t$ which gives $t < n - k(n - r)$. Since $t = \text{rank}(f) \geq n - k(n - r)$, this contradiction implies that

$$\text{rank}(f f_{k+1}) \geq n - (k+1)(n - r),$$

which completes the proof. $\square$

The next theorem gives a lower bound for $N'(S)$ where S is a finite transformation semigroup.

Notation 5. For any number k denote by $\lceil k \rceil$ the least integer greater than or equal to k.

Theorem 1. *If $S \leq PT_n$ and S is not a group with $r(S) \leq n-1$, then*

$$N'(S) \geq \left\lceil \frac{n-t(S)}{n-r(S)} \right\rceil .$$

Proof. Let A be a minimal generating set of S. We have

$$A \subseteq \{f \in S : \mathrm{rank}(f) \geq r(S)\}.$$

Let $f_1, f_2, \ldots, f_k \in A$ be such that $f_1 f_2 \ldots f_k \in \ker(S)$. Since

$$\mathrm{rank}(f_1 f_2 \ldots f_k) = t(S),$$

then by Lemma 5 we have $k \geq \left\lceil \frac{n-t(S)}{n-r(S)} \right\rceil$. Hence $N(S, A) \geq \left\lceil \frac{n-t(S)}{n-r(S)} \right\rceil$, which is the desired conclusion. $\square$

Theorem 1 presents a lower bound for N' for finite transformation semigroups which are not groups. For estimating the other parameters N, M, M' we should know more about generating sets. Nevertheless, the following very simple lemma provides the main idea to estimate those parameters for some families of finite transformation semigroups.

Lemma 6. *Let S be a finite semigroup such that $S \setminus \{1\}$ [1] is its subsemigroup and has a unique maximal $\mathcal{J}$-class J. Let A be a generating set of S. Then each $\mathcal{L}$-class and each $\mathcal{R}$-class of J has at least one element in A.*

Proof. Given $x \in J$. Since every finite semigroup is stable, for x to be a product of elements in A it is necessary that at least one element of A be $\mathcal{L}$-equivalent to x and at least one element of A be $\mathcal{R}$-equivalent to x. Thus A must cover the $\mathcal{L}$-classes and also the $\mathcal{R}$-classes of J. $\square$

[1] Note that $S \setminus \{1\} = S$ if S is not a monoid.

Now we are ready to apply the results in this section to the transformation semigroups PT_n, T_n, I_n, their ideals $K'(n,r), K(n,r), L(n,r)$ and the semigroups of order preserving transformations PO_n, O_n, POI_n. If S is one of the semigroups PO_n, O_n or POI_n, then $S \setminus \{1\}$ is a subsemigroup of S with a unique maximum $\mathcal{J}$-class [9, 6]. Moreover, if S is one of $K'(n,r),\ K(n,r)$ or $L(n,r)$, then $S \setminus \{1\} = S$ has a unique maximum $\mathcal{J}$-class [13, 7]. Hence, except for T_n, PT_n and I_n the above semigroups satisfy the hypothesis of Lemma 6. Thus, our strategy for estimating the depth parameters is different for these semigroups. First, we need to identify the generating sets of minimum size for $T_n, PT_n,\ I_n$. It is well known that, for $n \geq 3$,

$$\mathrm{rank}(T_n) = 3, \mathrm{rank}(I_n) = 3,{}^{2}\mathrm{rank}(PT_n) = 4.$$

But we need to know exactly what are the generating sets of minimum size. So we establish the following lemmas for completeness.

Notation 6. We use the notation (i,j) for denoting a transposition.

Lemma 7. *Let $A = \{a,b,c\} \subseteq T_n$ $(n \geq 3)$ such that $\{a,b\}$ generates S_n and c is a function of rank $n-1$. Then A is a generating set of T_n with minimum size. Furthermore, all generating sets of T_n with minimum size are of this form.*

Proof. Since the symmetric group S_n cannot be generated by less than two elements for $n \geq 3$, we need at least 3 elements to generate T_n. Then it suffices to show that such a set A generates T_n. We know that every element of $T_n \setminus S_n$ is a product of idempotents of rank $n-1$ [14]. Therefore we show that A generates all idempotents of rank $n-1$ (because $\{a,b,c\}$ already generates all permutations). Since c is a function of rank $n-1$, there exist exactly two distinct numbers $1 \leq i < j \leq n$ such that $ic = jc = l$, and there exists a unique number $1 \leq k \leq n$ such that $k \notin \mathrm{Im}(c)$. Suppose that α is an idempotent of rank $n-1$ which implies that α has the form

$$\alpha = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_1 & a_1 & a_3 & \dots & a_n \end{pmatrix},$$

[2] Usually by a generating set of an inverse semigroup one means a subset $A \subseteq S$ such that every element in S is a product of elements in A and their inverses. But we do not include inverses here.

where $\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_n\}$. Let $\rho = \begin{pmatrix} a_1 & a_2 & \ldots & a_i & \ldots & a_n \\ 1 & 2 & \ldots & i & \ldots & n \end{pmatrix}$, and define permutations τ, σ as follows. If $i = 2$ let τ be the cycle $(i, j, 1)$ and

$$t\sigma = \begin{cases} a_r & \text{if} \quad t = rc, r \notin \{j, 1, 2\} \\ a_1 & \text{if} \quad t = l \\ a_2 & \text{if} \quad t = k \\ a_j & \text{if} \quad t = 1c. \end{cases} \tag{3.3}$$

If $i = 1,\ j = 2$ let τ be the identity function and let

$$t\sigma = \begin{cases} a_r & \text{if} \quad t = rc, r \notin \{1, 2\} \\ a_1 & \text{if} \quad t = l \\ a_2 & \text{if} \quad t = k. \end{cases} \tag{3.4}$$

In the remaining cases let $\tau = (i, 1)(j, 2)$ and let

$$t\sigma = \begin{cases} a_r & \text{if} \quad t = rc, r \notin \{i, j, 1, 2\} \\ a_1 & \text{if} \quad t = l \\ a_2 & \text{if} \quad t = k \\ a_i & \text{if} \quad t = 1c \\ a_j & \text{if} \quad t = 2c. \end{cases} \tag{3.5}$$

Now it is easy to check that $\alpha = \rho\tau c\sigma$.

The last statement of the lemma follows from the structure of $\mathcal{J}$-classes of T_n. More precisely, $J_{n-1} = \{f \in T_n : \text{rank}(f) = n - 1\}$ is a $\mathcal{J}$-class of T_n which is $\mathcal{J}$-above all the other $\mathcal{J}$-classes except the maximum $\mathcal{J}$-class. Therefore every generating set of T_n must have at least one element in the $\mathcal{J}$-class J_{n-1}. □

Lemma 8. *Let $A = \{a, b, c, d\} \subseteq PT_n$ $(n \geq 3)$ such that $\{a, b, c\}$ generates T_n and d is a proper partial function of rank $n - 1$. Then A is a generating set of PT_n with minimum size. Furthermore, all generating sets of PT_n with minimum size are of this form.*

Proof. By Lemma 7, the full transformation semigroup T_n cannot be generated by less than three elements for $n \geq 3$. On the other hand, elements of T_n cannot generate any proper partial function so we need at least 4 elements to generate PT_n. Then it suffices to show that such a set A generates PT_n. First we prove this for the particular case in which

$$d = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ - & 1 & \ldots & n-2 & n-1 \end{pmatrix}.$$

Since $\{a, b, c\}$ generates T_n, we must show that, by adding d, we reach all proper partial functions. For $k \geq 1$, let

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_k & a_{k+1} & \dots & a_n \\ - & - & \dots & - & b_{k+1} & \dots & b_n \end{pmatrix}$$

be a proper partial function which is undefined in exactly k elements. Then it is easy to check that $f = \sigma d^k g$ where σ is the permutation

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_k & a_{k+1} & \dots & a_n \\ 1 & 2 & \dots & k & k+1 & \dots & n \end{pmatrix},$$

and g is the function

$$g = \begin{pmatrix} 1 & 2 & \dots & n-k & n-k+1 & \dots & n \\ b_{k+1} & b_{k+2} & \dots & b_n & n-k+1 & \dots & n \end{pmatrix}.$$

For the general case let

$$d' = \begin{pmatrix} a'_1 & a'_2 & \dots & a'_n \\ - & b'_2 & \dots & b'_n \end{pmatrix}.$$

where

$$\{1, 2, \dots, n\} = \{a'_1, a'_2, \dots, a'_n\} = \{b'_1, b'_2, \dots, b'_n\}.$$

We show that $\{a, b, c, d'\}$ generates PT_n. It is enough to show that d is a product of elements in $\{a, b, c, d'\}$. Define the permutations ρ, δ as follows

$$\rho = \begin{pmatrix} 1 & 2 & \dots & n \\ a'_1 & a'_2 & \dots & a'_n \end{pmatrix},$$

and

$$\delta = \begin{pmatrix} b'_1 & b'_2 & \dots & b'_n \\ n & 1 & \dots & n-1 \end{pmatrix}.$$

Now it is easy to check that $d = \rho d' \delta$.

Finally, we show that all generating sets of PT_n of minimum size are of the stated form. Let A be any generating set of PT_n. Since $T_n \subseteq PT_n$ and $PT_n \setminus T_n$ is an ideal, then A must contain a generating set of T_n. On the other hand elements of T_n cannot generate any proper partial function. Therefore A must contain at least one proper partial function. Since all the proper partial functions of rank $n-1$ are in the $\mathcal{J}$-class which is $\mathcal{J}$-above all $\mathcal{J}$-classes but the maximum $\mathcal{J}$-class, then A must contain at least one partial function of rank $n-1$. $\square$

Lemma 9. *Let $A = \{a, b, c\} \subseteq I_n$ $(n \geq 3)$ be such that $\{a, b\}$ generates S_n and c is an element of $J_{n-1} = \{\alpha \in I_n : rank(\alpha) = n-1\}$. Then A is a generating set of I_n with minimum size. Furthermore, all generating sets of I_n with minimum size are of this form.*

Proof. We know that $\{a, b, c, c^{-1}\}$ is a generating set of I_n [8]. We only need to show that $c^{-1} \in \langle a, b, c\rangle$. Let $\mathrm{Dom}(c) = X_n \setminus \{i\}, \mathrm{Im}(c) = X_n \setminus \{j\}$. For $i \neq j$, let $\alpha = (i, j)$ be a transposition and for $i = j$, let α be the identity function. We may complete c^{-1} to an element θ of S_n by defining $j\theta = i$. It is easy to check that $\alpha c\theta\alpha\theta = c^{-1}$.

For the second statement, let A be any generating set of I_n. Since S_n is the maximum $\mathcal{J}$-class of I_n, A must contain a generating set of S_n, which has at least 2 elements for $n \geq 3$. On the other hand, since S_n is a group the elements of S_n are not enough to generate the whole semigroup I_n. So, we need at least one element in $I_n \setminus S_n$. Since J_{n-1} is $\mathcal{J}$-above all $\mathcal{J}$-classes but the maximum $\mathcal{J}$-class, then A must contain at least one element in J_{n-1}. $\square$

Part of the following corollary is immediate by Theorem 1.

Corollary 3. *For $n \geq 3$,*

$$\begin{aligned} N'(T_n) &= N(T_n) = n-1, \\ N'(PT_n) &= N(PT_n) = n, \\ N'(I_n) &= N(I_n) = n. \end{aligned}$$

Proof. Since

$$\begin{aligned} &t(T_n) = 1, \\ &t(I_n) = t(PT_n) = 0, \\ &r(T_n) = r(PT_n) = r(I_n) = n-1, \end{aligned}$$

then by Theorem 1

$$N'(T_n) \geq n-1,\ N'(PT_n) \geq n,\ N'(I_n) \geq n.$$

What is left is to show that

$$N(T_n) \leq n-1,\ N(PT_n) \leq n,\ N(I_n) \leq n.$$

We do this by showing that each of the above semigroups has a generating set A of minimum size for which A-depth is at most the proposed upper bound. By Lemma 8 the rank of PT_n is four and the set $A = \{\alpha, \beta, \theta, \gamma\}$ is a generating set of T_n provided that $\{\alpha, \beta\}$ is a generating set of the symmetric group S_n, θ is a transformation of rank $n-1$, and γ is a proper partial transformation of rank $n-1$. If we choose γ to be the partial transformation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ - & 1 & 2 & \dots & n-1 \end{pmatrix},$$

then γ^n is the empty map, which lies in the minimum ideal of T_n. This shows that $N(PT_n, A) \leq n$. With the above notation and by Lemma 9 the set $A' = \{\alpha, \beta, \gamma\}$ is a generating set of I_n of minimum size and the above argument gives $N(I_n, A') \leq n$. For T_n, again with the above notation and by Lemma 7 the set $A = \{\alpha, \beta, \theta\}$ is a generating set of minimum size. If we choose θ to be the transformation

$$\theta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 1 & 2 & \dots & n-1 \end{pmatrix},$$

then θ^{n-1} is the constant map, which lies in the minimum ideal of T_n. Hence $N(T_n, A) \leq n-1$. □

Now we show that $N = N'$ for the remaining semigroups, and indeed $N' = N = M = M'$ (except for the semigroup O_n).

Proposition 4. *For $n \geq 3$,*

$$N'(PO_n) = N(PO_n) = M(PO_n) = M'(PO_n) = n,$$
$$N'(O_n) = N(O_n) = n-1,$$
$$N'(POI_n) = N(POI_n) = M(POI_n) = M'(POI_n) = n.$$

Proof. We start with the semigroup PO_n. We know that PO_n is generated by the $\mathcal{J}$-class J_{n-1} consisting of transformations or partial transformations of rank $n-1$ [9], and the empty transformation is the zero of PO_n. Hence, we have $r(PO_n) = n-1$ and $t(PO_n) = 0$. So Theorem 1 implies that $N'(PO_n) \geq n$. It remains to show that $M'(PO_n) \leq n$. Let A be a minimal generating set of PO_n. By Lemma 6, A intersects each $\mathcal{R}$-class of J_{n-1}. Hence we can find proper partial transformations $f_1, f_2, \dots, f_n \in A$ such that $1 \notin \mathrm{Dom}(f_1)$ and for $1 \leq i \leq n-1$, $(i+1)f_1 f_2 \dots f_i \notin \mathrm{Dom}(f_{i+1})$. It is easy to see that $f_1 f_2 \dots f_n$ is the empty function. This shows that $N(PO_n, A) \leq n$. Since A is an arbitrary minimal generating set, then $M'(PO_n) \leq n$.

The next semigroup in the statement of the proposition is the semigroup O_n. Since the maximum $\mathcal{J}$-class J_{n-1} generates O_n [9], $r(O_n) = n-1$. By Theorem 1, $N'(O_n) \geq n-1$. We show that $N(O_n) \leq n-1$. It is enough to show that $N(O_n, A) \leq n-1$ for some generating set A of minimum size. For $1 \leq i \leq n-1$ let

$$\alpha_i = \left(\begin{array}{cccccc} 1 & 2 & 3 & \dots & i & i+1 & \dots n \\ 1 & 2 & 3 & \dots & i+1 & i+1 & \dots n \end{array} \right)$$

and

$$\beta = \left(\begin{array}{cccccccc} 1 & 2 & 3 & \dots & i & i+1 & n-1 & \dots n \\ 1 & 1 & 2 & \dots & i-1 & i & n-2 & \dots n-1 \end{array} \right).$$

The set $\{\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \beta\}$ is a generating set of O_n of minimum size as has been proved in [9]. On the other hand, β^{n-1} is a constant transformation. This shows that $N(O_n, A) \leq n-1$, and so $N(O_n) \leq n-1$.

We now apply this argument again for POI_n. With the same reason as the previous cases $N'(POI_n) \geq n$ [6]. We show that $N(POI_n, A) \leq n$ for every minimal generating set A. Again A intersects each $\mathcal{R}$-class of J_{n-1}. Hence we can find proper partial transformations $f_1, f_2, \dots, f_n \in A$ such that $1 \notin \mathrm{Dom}(f_1)$ and for $1 \leq i \leq n-1$, $(i+1)f_1 f_2 \dots f_i \notin \mathrm{Dom}(f_{i+1})$. It is easy to see that $f_1 f_2 \dots f_n$ is the empty function. Hence $N(POI_n, A) \leq n$, which completes the proof. □

We use the following lemmas to prove Proposition 5.

Lemma 10. *The transformation semigroup $L(n,r)$ is generated by its maximum $\mathcal{J}$-class.*

Proof. For $0 \leq k \leq r$ denote

$$J_k := \{\alpha \in L(n,r) : \mathrm{rank}(\alpha) = k\}.$$

It is easy to see that J_k is a $\mathcal{J}$-class of $L(n,r)$. Now we prove that the maximum $\mathcal{J}$-class J_r generates $L(n,r)$. For $k < r$, consider an arbitrary $\beta \in J_k$. Suppose that

$$\beta = \left(\begin{array}{cccc} a_1 & a_2 & \dots & a_k \\ b_1 & b_2 & \dots & b_k \end{array} \right).$$

Choose $a_{k+1} \notin \mathrm{Dom}(\beta)$ and $b_{k+1} \notin \mathrm{Im}(\beta)$ and let

$$\beta' = \left(\begin{array}{ccccc} a_1 & a_2 & \dots & a_k & a_{k+1} \\ b_1 & b_2 & \dots & b_k & b_{k+1} \end{array} \right).$$

Now choose $f \in J_r$ such that $f(b_i) = b_i$ for $1 \leq i \leq k$ and $b_{k+1} \notin \mathrm{Dom}(f)$. It is easy to see that $\beta = \beta' f$. Therefore, $J_k \subseteq J_{k+1} J_r$ for $0 \leq k \leq r-1$. It follows that $J_k \subseteq J_r^{r-k+1}$. Hence $L(n,r)$ is generated by J_r. □

Lemma 11. *The $\mathcal{R}$-class in $K'(n,r)$ of a partial permutation consists only of partial permutations. Moreover, two partial permutations which are $\mathcal{R}$-equivalent in $K'(n,r)$ are also $\mathcal{R}$-equivalent in $L(n,r)$.*

Proof. Let $f, g \in K'(n,r)$. Suppose that $f \mathcal{R} g$ and f is a partial permutation. There exist $h, k \in K'(n,r)$ such that $f = gh$ and $g = fk$. First we show that g is a partial permutation. Since $f = gh$, then $\mathrm{Dom}(f) \subseteq \mathrm{Dom}(g)$ and $\mathrm{rank}(f) \leq \mathrm{rank}(g)$. Since $g = fk$, then $\mathrm{Dom}(g) \subseteq \mathrm{Dom}(f)$ and $\mathrm{rank}(g) \leq \mathrm{rank}(f)$. Hence we have $\mathrm{Dom}(f) = \mathrm{Dom}(g)$ and $\mathrm{rank}(f) = \mathrm{rank}(g)$. Since f is a partial permutation, then $|\mathrm{Dom}(f)| = \mathrm{rank}(f)$. It follows that $|\mathrm{Dom}(g)| = \mathrm{rank}(g)$, hence g is a partial permutation. Now define the partial permutations h', k' as follows. Let $\mathrm{Dom}(h') = \mathrm{Im}(g)$ and $xh = xh'$ for every $x \in \mathrm{Im}(g)$. Let $\mathrm{Dom}(k') = \mathrm{Im}(f)$ and $xk = xk'$ for every $x \in \mathrm{Im}(f)$. Hence we have $f = gh'$ and $g = fk'$ and $h', k' \in L(n,r)$. It shows that f, g are $\mathcal{R}$-equivalent in $L(n,r)$. □

Proposition 5. *For every $n > 1$ and $1 \leq r \leq n-1$,*

$$N'(K(n,r)) = N(K(n,r)) = M(K(n,r)) = M'(K(n,r)) = \left\lceil \frac{n-1}{n-r} \right\rceil,$$

$$N'(K'(n,r)) = N(K'(n,r)) = M(K'(n,r)) = M'(K(n,r)) = \left\lceil \frac{n}{n-r} \right\rceil,$$

$$N'(L(n,r)) = N(L(n,r)) = M(L(n,r)) = M'(L(n,r)) = \left\lceil \frac{n}{n-r} \right\rceil.$$

Proof. To see that the semigroups $K(n,r)$ and $K'(n,r)$ are generated by their maximum $\mathcal{J}$-classes see [13, 7], respectively; and by Lemma 10, this assertion is true for $L(n,r)$. Hence, by Lemma 1 every minimal generating set for these semigroups is contained in their maximum $\mathcal{J}$-classes. On the other hand, the rank of elements in the maximum $\mathcal{J}$-class for these semigroups is

r. Hence, Theorem 1 implies that

$$N'(K(n,r)) \geq \left\lceil \frac{n-1}{n-r} \right\rceil,$$
$$N'(K'(n,r)) \geq \left\lceil \frac{n}{n-r} \right\rceil,$$
$$N'(L(n,r)) \geq \left\lceil \frac{n}{n-r} \right\rceil.$$

The proof is completed by showing that

$$M'(K(n,r)) \leq \left\lceil \frac{n-1}{n-r} \right\rceil,$$
$$M'(K'(n,r)) \leq \left\lceil \frac{n}{n-r} \right\rceil,$$
$$M'(L(n,r)) \leq \left\lceil \frac{n}{n-r} \right\rceil.$$

First, we prove that $M'(K(n,r)) \leq \lceil \frac{n-1}{n-r} \rceil$. Let A be a minimal generating set of $K(n,r)$. We show that there exists some product of at most $\lceil \frac{n-1}{n-r} \rceil$ generators in A which is a constant transformation. Denote by J the maximum $\mathcal{J}$-class of $K(n,r)$. By Lemma 6, A covers the $\mathcal{L}$-classes of J and the $\mathcal{R}$-classes of J. Since A covers the $\mathcal{L}$-classes of J, there exists a transformation $f_1 \in A$ such that $\mathrm{Im}(f_1) = \{1, 2, \ldots, r\}$. Since A also covers the $\mathcal{R}$-classes of J, we can define $f_2, f_3, \ldots, f_\ell \in A$ as follows: for $i \geq 2$, if $\mathrm{rank}(f_1 f_2 \cdots f_{i-1}) > n-r+1$, then choose $f_i \in A$ that collapses $n-r+1$ elements in the image of $f_1 f_2 \cdots f_{i-1}$; otherwise, choose $f_i \in A$ that collapses all the elements in the image of $f_1 f_2 \cdots f_{i-1}$. It is enough to check that $f_1 f_2 \cdots f_{\lceil \frac{n-1}{n-r} \rceil}$ is a constant transformation. If $r = 1$, this is trivial. Let $r \geq 2$. If $r \leq n-r+1$, then $f_1 f_2$ is a constant transformation. On the other hand, the inequalities $2 \leq r \leq n-r+1$ imply $2 = \lceil \frac{n-1}{n-r} \rceil$. Suppose next that $r > n-r+1$. There exists $k \geq 2$ such that $\mathrm{rank}(f_1 f_2 \cdots f_k) \leq n-r+1$ and $\mathrm{rank}(f_1 f_2 \cdots f_{k-1}) > n-r+1$. Since f_{k+1} collapses all the elements in the image of $f_1 f_2 \cdots f_k$, then $f_1 f_2 \cdots f_{k+1}$ is a constant transformation. It remains to show that $k+1 = \lceil \frac{n-1}{n-r} \rceil$. Note that

$$\mathrm{rank}(f_1 f_2 \cdots f_i) = r - (i-1)(n-r), \text{ for } 1 \leq i \leq k.$$

Hence
$$\operatorname{rank}(f_1 f_2 \cdots f_k) = r - (k-1)(n-r) \leq n - r + 1, \tag{3.6}$$
and
$$\operatorname{rank}(f_1 f_2 \cdots f_{k-1}) = r - (k-2)(n-r) > n - r + 1. \tag{3.7}$$
The inequalities (3.6) and (3.7) imply that
$$k < \frac{n-1}{n-r} \leq k+1,$$
which is the desired conclusion.

Next we prove that
$$M'(L(n,r)) \leq \left\lceil \frac{n}{n-r} \right\rceil.$$
Let B be a minimal generating set of $L(n,r)$. We show that there exists some product of at most $\lceil \frac{n}{n-r} \rceil$ generators in B which is the empty transformation. By Lemma 6, B covers the $\mathcal{R}$-classes of J_r. Hence, there exists a transformation $g_1 \in B$ such that $1, 2, \ldots, n-r \notin \operatorname{Dom}(g_1)$. We can define $g_2, g_3, \ldots, g_\ell \in B$ as follows: for $i \geq 2$, if $\operatorname{rank}(g_1 g_2 \cdots g_{i-1}) \geq n - r + 1$ choose $g_i \in B$ such that $n - r$ elements in the image of $g_1 g_2 \cdots g_{i-1}$ are excluded from $\operatorname{Dom}(g_i)$; otherwise, choose $g_i \in A$ such that all elements in the image of $g_1 g_2 \cdots g_{i-1}$ are excluded from $\operatorname{Dom}(g_i)$. It is enough to check that $g_1 g_2 \cdots g_{\lceil \frac{n}{n-r} \rceil}$ is the empty transformation. If $r = 1$, then $g_1 g_2$ is the empty transformation and $\lceil \frac{n}{n-1} \rceil = 2$. Let $r \geq 2$. If $r < n - r + 1$, then $g_1 g_2$ is the empty transformation. On the other hand the inequalities $2 \leq r < n - r + 1$ imply $\lceil \frac{n}{n-r} \rceil = 2$. Suppose next that $r \geq n - r + 1$. There exists $k \geq 2$ such that
$$0 < \operatorname{rank}(g_1 g_2 \ldots g_k) < n - r + 1, \tag{3.8}$$
$$\operatorname{rank}(g_1 g_2 \cdots g_{k-1}) \geq n - r + 1. \tag{3.9}$$
Since none of the elements in the image of $g_1 g_2 \ldots g_k$ is in the domain of g_{k+1}, then $g_1 g_2 \cdots g_{k+1}$ is the empty transformation. It remains to show that $k + 1 = \lceil \frac{n}{n-r} \rceil$. By definition of g_k, we have
$$\operatorname{rank}(g_1 g_2 \cdots g_k) = n - k(n-r), \tag{3.10}$$
and
$$\operatorname{rank}(g_1 g_2 \cdots g_{k-1}) = n - (k-1)(n-r). \tag{3.11}$$

Substituting (3.10) in (3.8) and (3.11) in (3.9) we obtain

$$k < \frac{n}{n-r} \leq k+1,$$

which is the desired conclusion.

Finally, we consider the semigroup $K'(n,r)$. Let C be a minimal generating set of $K'(n,r)$. By Lemma 6, C covers the $\mathcal{R}$-classes of the maximum $\mathcal{J}$-class of $K'(n,r)$. On the other hand, the maximum J class of $L(n,r)$ is contained in the maximum $\mathcal{J}$-class of $K'(n,r)$. Then by Lemma 11, we may choose $g_1, g_2, \ldots, g_{\lceil \frac{n}{n-r} \rceil} \in C$. This shows that $N(K'(n,r), C) \leq \lceil \frac{n}{n-r} \rceil$ and so $M'(K'(n,r)) \leq \lceil \frac{n}{n-r} \rceil$. □

In the sequel we try to calculate the maximum A-depth over all minimal generating sets. We just apply the following simple lemma to establish an upper bound for $M'(S)$ provided that S is a semigroup generated by the maximal $\mathcal{J}$-classes. First we need to introduce some notation.

Notation 7. Let S be a finite semigroup. Denote by J_M the set of all the maximal $\mathcal{J}$-classes of S. For every $\mathcal{J}$-class J of S denote by h_J, ℓ_J and r_J the number of elements in the $\mathcal{H}$-classes of J, the number of $\mathcal{L}$-classes of J and the number of $\mathcal{R}$-classes of J, respectively.

Lemma 12. *Let J be a maximal $\mathcal{J}$-class of a semigroup S. Let A be a generating set of S. The length of elements in J with respect to A is at most* $\min\{\ell_J h_J, r_J h_J\}$.

Proof. Let $x \in J$ and $l_A(x) = k$. There exist $a_1, a_2, \ldots, a_k \in A \cap J$ such that $x = a_1 a_2 \ldots a_k$. Since, $a_1, a_1a_2, \ldots, a_1a_2\ldots a_k$ are k distinct elements in the same $\mathcal{R}$-class, then $k \leq \ell_J h_J$. On the other hand, $a_k, a_{k-1}a_k, \ldots, a_1a_2\ldots a_k$ are k distinct elements in the same $\mathcal{L}$-class, then $k \leq r_J h_J$. Hence

$$k \leq \min\{\ell_J h_J, r_J h_J\}. \quad \square$$

Proposition 6. *Let S be a finite semigroup. If S is generated by the maximal $\mathcal{J}$-classes, then*

$$M'(S) \leq N(S, \cup_{J \in J_M} J) \max_{J \in J_M} \min\{\ell_J h_J, r_J h_J\}.$$

Proof. Let A be a minimal generating set of S. It suffices to show that $N(S, A)$ is bounded above by the proposed bound. Let $N(S, \cup_{J \in J_M} J) = k$. There exist $x_1, x_2, \ldots, x_k \in \cup_{J \in J_M} J$ such that $x = x_1 x_2 \ldots x_k \in \ker(S)$. We have $l_A(x) \leq \sum_{i=1}^{k} l_A(x_i)$. According to Lemma 12, $l_A(x_i) \leq \min\{\ell_J h_J, r_J h_J\}$ for some maximal $\mathcal{J}$-class of S containing x_i. If M is the maximum of $\min\{\ell_J h_J, r_J h_J\}$ over all maximal $\mathcal{J}$-classes of S, then $l_A(x_i) \leq M$ for $1 \leq i \leq k$. This shows that $l_A(x) \leq kM$. Hence $N(S, A) \leq kM$ which is the desired conclusion. $\square$

3.2 A-depth and products of semigroups

We did some attempt to understand the behavior of the depth parameters with respect to products (direct product and wreath product) of semigroups. Here we deal mostly with monoids rather than semigroups because it is easier to say something about minimal generating sets when the components of the product are two monoids.

3.2.1 Direct product

Let S, T be two finite semigroups. We are interested in estimating the parameters

$$N'(S \times T),\ N(S \times T),$$

with respect to the corresponding parameters for S and T. First, we observe that the kernel of the direct product of two finite semigroups is the product of the kernels of its components.

Lemma 13. *Let S, T be two finite semigroups. Then*

$$\ker(S \times T) = \ker(S) \times \ker(T).$$

Proof. It is easy to see that $\ker(S) \times \ker(T)$ is an ideal of $S \times T$. Since $\ker(S \times T)$ is the minimum ideal of $S \times T$, then $\ker(S \times T) \subseteq \ker(S) \times \ker(T)$. It remains to show that $\ker(S) \times \ker(T)$ is just one $\mathcal{J}$-class. It follows from the fact that the direct product of two simple semigroups is a simple semigroup; it is easy to justify this fact by considering that a semigroup S is simple if and only if $SaS = S$ for every $a \in S$ [22]. $\square$

Now we need to establish a relationship between generating sets of the direct product and generating sets of its components. We could not find a nice general method for constructing a generating set of minimum size for $S_1 \times S_2$ when the semigroups S_1, S_2 do not contain an identity element. Just as an easy example we consider the product of two monogenic semigroups.

Example 4. Let $i, n, j, m \geq 1$. Then the depth parameters are all equal for $C_{i,n} \times C_{j,m}$ and they are given by the formula

$$N(C_{i,n} \times C_{j,m}) = \begin{cases} 0 & \text{if} \quad i = j = 1 \\ i & \text{if} \quad j = 1, i \neq 1 \\ j & \text{if} \quad i = 1, j \neq 1 \\ 2 & \text{if} \quad i, j \neq 1 \end{cases}$$

Furthermore, if $i \neq 1$, or $j \neq 1$, then $C_{i,n} \times C_{j,m}$ has a unique minimal generating set.

Proof. Let $C_{i,n} = \langle a : \ a^{i+n} = a^i \rangle$ and $C_{j,m} = \langle b : \ b^{j+m} = b^j \rangle$. In case both i, j are equal to 1, these cyclic semigroups are groups and, therefore, so is their product. Because $N(G) = 0$ for any group G then $N(C_{1,n} \times C_{1,m}) = 0$. If $j = 1, i \neq 1$, then the maximum $\mathcal{J}$-class of $C_{i,n} \times C_{1,m}$ is $\{a\} \times C_{1,m}$. If A is any generating set of $C_{i,n} \times C_{1,m}$ then A must contain $\{a\} \times C_{1,m}$ because a can not be written as a product of two elements. On the other hand, $\{a\} \times C_{1,m}$ generates $C_{i,n} \times C_{1,m}$ because, if $(a^k, b^l) \in C_{i,n} \times C_{1,m}$ for some $k > 1$, then $(a^k, b^l) = (a, b^l)(a, 1)^{k-1}$. Therefore, $\{a\} \times C_{1,m}$ is the unique generating set of $C_{i,n} \times C_{1,m}$ of minimum size and

$$\ker(C_{i,n} \times C_{1,m}) = \{a^i, a^{i+1}, \ldots, a^{i+n}\} \times C_{1,m}.$$

Note that $(a, 1)^i \in \ker(C_{i,n} \times C_{1,m})$ and, because the first component of every element in the generating set is a, the product of generators with less than i factors can not reach the minimum ideal. Therefore $N(C_{i,n} \times C_{1,m}) = i$. The case where $i = 1, j \neq 1$ is similar. Now let $i, j \neq 1$. We show that

$$A = \{(a, b^k) | 1 \leq k \leq j + m - 1\} \cup \{(a^l, b) | 1 \leq l \leq i + n - 1\}$$

is the unique minimal generating set of $C_{i,n} \times C_{j,m}$. Every generating set must contain A because a and b cannot be written as products of any other elements. Furthermore, if $(a^s, b^t) \in C_{i,n} \times C_{j,m}$ for some $s, t > 1$ then $(a^s, b^t) = (a, b^{t-1})(a^{s-1}, b)$. Hence, A generates $C_{i,n} \times C_{j,m}$. We have $a^i \in \ker(C_{i,n})$ and $a^j \in \ker(C_{j,m})$. In view of Lemma 11, it follows that $(a, b^{j-1})(a^{i-1}, b) = (a^i, b^j) \in \ker(C_{i,n} \times C_{j,m})$. This proves that $N(C_{i,n} \times C_{j,m}) = 2$. $\square$

In the next example, we treat the case where just one of the components in the direct product is a cyclic semigroup.

Example 5. Let S be a semigroup and let $i > 1,\ n \geq 1$. Then

$$M'(S \times C_{i,n}) \leq i.$$

Proof. Let

$$C_{i,n} = \{a, a^2, \ldots, a^i, a^{i+1}, \ldots, a^{n+i-1}\}.$$

If A is any generating set of $S \times C_{i,n}$ then $S \times \{a\} \subseteq A$. Let $x \in \ker(S)$. We have $(x, a) \in A$ and $(x, a)^i = (x^i, a^i) \in \ker(S) \times \ker(C_{i,n})$, whence $N(S \times C_{i,n}, A) \leq i$. □

From now on, we consider monoids rather than semigroups. Let A_1, A_2 be two minimal generating sets of the monoids $M_1 \neq \{1\}$ and $M_2 \neq \{1\}$, respectively. If $(1,1) \notin (A_1 \times \{1\}) \cup (\{1\} \times A_2)$, then $A = (A_1 \times \{1\}) \cup (\{1\} \times A_2)$ is a minimal generating set of $M_1 \times M_2$; otherwise $A = (A_1 \times \{1\}) \cup (\{1\} \times A_2) \setminus \{(1,1)\}$ is a minimal generating set of $M_1 \times M_2$. Let $N'(M_1) = t_1,\ N'(M_2) = t_2$. There exist $a_1, a_2, \ldots, a_{t_1} \in A_1 \setminus \{1\},\ a'_1, a'_2, \ldots, a'_{t_2} \in A_2 \setminus \{1\}$ such that $a_1 a_2 \ldots a_{t_1} \in \ker(M_1),\ a'_1 a'_2 \ldots a'_{t_2} \in \ker(M_2)$. So we have $(a_1 a_2 \ldots a_{t_1}, a'_1 a'_2 \ldots a'_{t_2}) \in \ker(M_1 \times M_2)$. On the other hand, the length of $(a_1 a_2 \ldots a_{t_1}, a'_1 a'_2 \ldots a'_{t_2})$ with respect to A is $t_1 + t_2$. It follows that

$$N'(M_1 \times M_2) \leq N'(M_1) + N'(M_2). \tag{3.12}$$

It is natural to ask whether there is an expression like inequality (3.12) for the other parameters N, M, M'. In fact, if A or $A \setminus \{(1,1)\}$ is a generating set of minimum size then we could derive a similar inequality for N. But A may not be a generating set of minimum size. In general, we may establish the following lemma concerning the rank of the direct product of two finite monoids.

Definition 13. For a finite monoid M with group of units U, the rank of M modulo U is the minimum number of elements in $M \setminus U$ which together with U generate M.

Lemma 14. *Let M_1, M_2 be two finite monoids. Denote by U_i the group of units of M_i and by k_i the rank of M_i modulo U_i. Let $A'_i \subseteq M_i \setminus U_i$ be such that $|A'_i| = k_i$ and $M_i = \langle U_i \cup A'_i \rangle$. Let B be a generating set of $U_1 \times U_2$. Then the set*

$$C = B \cup (A'_1 \times \{1\}) \cup (\{1\} \times A'_2),$$

is a generating set of $M_1 \times M_2$. *Furthermore, we have*

$$\operatorname{rank}(M_1 \times M_2) = \operatorname{rank}(U_1 \times U_2) + k_1 + k_2.$$

Proof. Let $(x, y) \in M_1 \times M_2$. We show that $(x, y) \in \langle C\rangle$. It is enough to show that $(x, 1), (1, y) \in \langle C\rangle$. We know that x is a product of elements in $U_1 \cup A_1'$. Let $x = x_1x_2 \dots x_t$ for some $x_i \in U_1 \cup A_1'$. Hence we have $(x, 1) = \prod_{i=1}^{t}(x_i, 1)$. For $1 \leq i \leq t$; if $x_i \in A_1'$ then we have $(x_i, 1) \in C$; if $x_i \in U_1$ then we have $(x_i, 1) \in U_1 \times U_2 = \langle B\rangle$. Thus $(x_i, 1) \in \langle C\rangle$, which implies that $(x, 1) \in \langle C\rangle$. In the same manner we can see that $(1, y) \in \langle C\rangle$.

The rest of the proof consists in showing that C is a generating set of minimum size when B is a generating set of minimum size or $U_1 \times U_2$. Let X be a generating set of $M_1 \times M_2$. Write $\bar{M}_1 = M_1 \setminus U_1$ and $\bar{M}_2 = M_2 \setminus U_2$. We have

$$M_1 \times M_2 = (U_1 \times U_2) \cup (U_1 \times \bar{M}_2) \cup (\bar{M}_1 \times U_2) \cup (\bar{M}_1 \times \bar{M}_2). \tag{3.13}$$

It is clear that X has at least $\operatorname{rank}(U_1 \times U_2)$ elements in $U_1 \times U_2$. Furthermore, $(U_1 \times \bar{M}_2) \cup (\bar{M}_1 \times \bar{M}_2)$ and $(\bar{M}_1 \times U_2) \cup (\bar{M}_1 \times \bar{M}_2)$ are ideals of $M_1 \times M_2$, then X has at least k_1 elements in $\bar{M}_1 \times U_2$ and k_2 elements in $U_1 \times \bar{M}_2$. These facts combining with the pairwise disjointness of the subsets in the right side of (3.13) gives $|X| \geq \operatorname{rank}(U_1 \times U_2) + k_1 + k_2$, which completes the proof. $\square$

Remark 8. Let A_1, A_2 be two generating sets of M_1, M_2 with minimum size. If $(1, 1) \notin (\{1\} \times A_2) \cup (A_1 \times \{1\})$ the size of the generating set $A = (\{1\} \times A_2) \cup (A_1 \times \{1\})$ is equal to $\operatorname{rank}(M_1) + \operatorname{rank}(M_2) = \operatorname{rank}(U_1) + k_1 + \operatorname{rank}(U_2) + k_2$, where k_i is the rank of M_i modulo U_i. Therefore, by Lemma 14, if $\operatorname{rank}(U_1 \times U_2) = \operatorname{rank}(U_1) + \operatorname{rank}(U_2)$, then the generating set A is a generating set of minimum size. On the other hand, by the minimality of A_1 and A_2, $(1, 1) \in A = (\{1\} \times A_2) \cup (A_1 \times \{1\})$ if and only if $U_1 = U_2 = \{1\}$. Whence, if $(1, 1) \in A$ then $|A \setminus \{(1, 1)\}| = \operatorname{rank}(U_1) + k_1 + \operatorname{rank}(U_2) + k_2 - 1 = k_1 + k_2 + 1$. But also by Lemma 14, $\operatorname{rank}(M_1 \times M_2) = k_1 + k_2 + 1$. So $A \setminus \{(1, 1)\}$ is a generating set of minimum size of $M_1 \times M_2$.

Theorem 2. *Let* M_1 *and* M_2 *be two finite monoids. Then we have*

$$N(M_1 \times M_2) \leq (N(M_1) + N(M_2))D(U_1 \times U_2),$$

provided that $D(U_1 \times U_2) \neq 0$. *Furthermore, if* $\operatorname{rank}(U_1 \times U_2) = \operatorname{rank}(U_1) + \operatorname{rank}(U_2)$ *(and also in the case* $D(U_1 \times U_2) = 0$*) then we have*

$$N(M_1 \times M_2) \leq N(M_1) + N(M_2).$$

Proof. Let A_1, A_2 be generating sets of minimum size of M_1, M_2, respectively, such that $N(M_1, A_1) = N(M_1)$ and $N(M_2, A_2) = N(M_2)$. Let B be a generating set of $U_1 \times U_2$ of minimum size. Let

$$C = B \cup (A_1' \times \{1\}) \cup (\{1\} \times A_2'),$$

where $A_i' = A_i \backslash U_i$. There exist $x_1, x_2, \ldots, x_{N(M_1)} \in A_1$ and $y_1, y_2, \ldots, y_{N(M_2)} \in A_2$ such that $x_1 x_2 \ldots x_{N(M_1)} \in \ker(M_1)$ and $y_1 y_2 \ldots y_{N(M_2)} \in \ker(M_2)$. Hence the pair $(x_1 x_2 \ldots x_{N(M_1)}, y_1 y_2 \ldots y_{N(M_2)})$ belongs to $\ker(M_1 \times M_2)$. The following equality

$$(x_1 x_2 \ldots x_{N(M_1)}, y_1 y_2 \ldots y_{N(M_2)}) = \prod_{i=1}^{N(M_1)} (x_i, 1) \prod_{j=1}^{N(M_2)} (1, y_j),$$

implies that

$$l_C((x_1 x_2 \ldots x_{N(M_1)}, y_1 y_2 \ldots y_{N(M_2)})) \leq \sum_{i=1}^{N(M_1)} l_C(x_i, 1) + \sum_{j=1}^{N(M_2)} l_C(1, y_j).$$

For $1 \leq i \leq N(M_1)$, if $x_i \in A_1'$ then we have $l_C(x_i, 1) = 1$; otherwise, we have $l_C(x_i, 1) \leq \operatorname{diam}(U_1 \times U_2, B)$. For $1 \leq i \leq N(M_2)$, if $y_i \in A_2'$ then we have $l_C(1, y_i) = 1$; otherwise, we have $l_C(1, y_i) \leq \operatorname{diam}(U_1 \times U_2, B)$. Let

$$s_1 = |\{x_1, x_2, \ldots, x_{N(M_1)}\} \cap A_1'|,$$

and

$$s_2 = |\{y_1, y_2, \ldots, y_{N(M_2)}\} \cap A_2'|.$$

Then the length of $(x_1 x_2 \ldots x_{N(M_1)}, y_1 y_2 \ldots x'_{N(M_2)})$, in the generating set C, is at most

$$\begin{aligned} & s_1 + s_2 + (N(M_1) + N(M_2) - (s_1 + s_2))\operatorname{diam}(U_1 \times U_2, B) \qquad (3.14) \\ =& (N(M_1) + N(M_2))\operatorname{diam}(U_1 \times U_2, B) \\ +& (1 - \operatorname{diam}(U_1 \times U_2, B))(s_1 + s_2). \end{aligned}$$

The upper bound in (3.14) depend on the integers s_1, s_2 and the generating set B. Now we try to remove these parameters from the proposed upper bound. Since $1 - \operatorname{diam}(U_1 \times U_2, B) \leq 0$ and $s_1 + s_2 \geq 0$ then

$$\begin{aligned} & (N(M_1) + N(M_2))\operatorname{diam}(U_1 \times U_2, B) \\ +& (1 - \operatorname{diam}(U_1 \times U_2, B))(s_1 + s_2) \\ \leq& (N(M_1) + N(M_2))\operatorname{diam}(U_1 \times U_2, B). \qquad (3.15) \end{aligned}$$

Substituting $D(U_1 \times U_2)$ for $\operatorname{diam}(U_1 \times U_2, B)$ in (3.15) establishes the first statement of the theorem.

Now we prove the second statement. Let $\operatorname{rank}(U_1 \times U_2) = \operatorname{rank}(U_1) + \operatorname{rank}(U_2$. According to Remark 8, the set $A = (\{1\} \times A_2) \cup (A_1 \times \{1\})$ is a generating set of $M_1 \times M_2$ of minimum size. Suppose that $N(M_1, A_1) = N(M_1) = t_1$ and $N(M_2, A_2) = N(M_2) = t_2$. There exist $a_1, a_2, \ldots, a_{t_1} \in A_1$, $a'_1, a'_2, \ldots, a'_{t_2} \in A_2$ such that $a_1 a_2 \ldots a_{t_1} \in \ker(M_1)$, $a'_1 a'_2 \ldots a'_{t_2} \in \ker(M_2)$. So we have $(a_1 a_2 \ldots a_{t_1}, a'_1 a'_2 \ldots a'_{t_2}) \in \ker(M_1 \times M_2)$. On the other hand, the length of $(a_1 a_2 \ldots a_{t_1}, a'_1 a'_2 \ldots a'_{t_2})$ with respect to A is at most $t_1 + t_2$. It follows that

$$N(M_1 \times M_2) \leq N(M_1) + N(M_2), \tag{3.16}$$

which is the desired conclusion. For the case that $D(U_1 \times U_2) = 0$ we have $U_1 \times U_2 = U_1 = U_2 = \{1\}$. According to Remark 8, the set $A = (\{1\} \times A_2) \cup (A_1 \times \{1\}) \setminus \{(1,1)\}$ is a generating set of $M_1 \times M_2$ of minimum size. Suppose that $N(M_1, A_1) = N(M_1) = t_1$ and $N(M_2, A_2) = N(M_2) = t_2$. There exist $a_1, a_2, \ldots, a_{t_1} \in A_1 \setminus \{1\}$, $a'_1, a'_2, \ldots, a'_{t_2} \in A_2 \setminus \{1\}$ such that $a_1 a_2 \ldots a_{t_1} \in \ker(M_1)$, $a'_1 a'_2 \ldots a'_{t_2} \in \ker(M_2)$. So we have $(a_1 a_2 \ldots a_{t_1}, a'_1 a'_2 \ldots a'_{t_2}) \in \ker(M_1 \times M_2)$. On the other hand, the length of $(a_1 a_2 \ldots a_{t_1}, a'_1 a'_2 \ldots a'_{t_2})$ with respect to $A \setminus \{(1,1)\}$ is at most $t_1 + t_2$. It follows that

$$N(M_1 \times M_2) \leq N(M_1) + N(M_2), \tag{3.17}$$

which is the desired conclusion.

□

The remainder of this section is devoted to the computation of $N(T_n \times T_m)$ for $n, m \geq 3$.

Lemma 15. *For $n \geq 3$ the symmetric group S_n can be generated by two elements of coprime order.*

Proof. Define the permutations a, a' and b as follows:

$$a = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 3 & 4 & \ldots & 1 \end{pmatrix}, a' = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 3 & 4 & \ldots & 2 \end{pmatrix}$$

and

$$b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}.$$

It is known that the full cycle a and the transposition b generate S_n [15]. On the other hand, note that $a'b = a$. Hence the sets $\{a, b\}$ and $\{a', b\}$ are generating sets of S_n. Note that

$$\mathrm{ord}(a) = n,\ \mathrm{ord}(b) = 2,\ \mathrm{ord}(a') = n - 1.$$

Therefore, for odd n, the set $A = \{a, b\}$ and, for even n, the set $A' = \{a', b\}$ are the desired generating sets. $\square$

For $n, m \geq 3$, let U_1 and U_2 be the group of units of T_n and T_m, respectively. We show that $N(T_n \times T_m) = N(T_n) \times N(T_m)$, while $U_1 \times U_2$ is neither trivial nor $\mathrm{rank}(U_1 \times U_2) = \mathrm{rank}(U_1) + \mathrm{rank}(U_2)$. More precisely, we have $U_1 = S_n$ and $U_2 = S_m$. Let $S_n = \langle a, b\rangle$ and $S_m = \langle c, d\rangle$ such that both of the pairs a, c and b, d are of coprime orders (see Lemma 15). We show that $S_n \times S_m = \langle (a, c), (b, d)\rangle$. It is enough to show that $(a, 1), (b, 1), (1, c), (1, d) \in \langle (a, c), (b, d)\rangle$. This is because a, c and b, d are of coprime orders. In fact, if x, y are of coprime order then there exists a power of (x, y) which is equal to $(x, 1)$ and there exists a power of (x, y) which is equal to $(1, y)$. Hence, we have $\mathrm{rank}(S_n \times S_m) = 2$, which is not equal to $\mathrm{rank}(S_n) + \mathrm{rank}(S_m)$.

Lemma 16. *Let $S = \{f \in T_n | \ \mathrm{rank}(f) \geq n - 1\}$. If $\mathrm{rank}(f_1 f_2 \ldots f_k) = 1$ for some $f_1, f_2, \ldots, f_k \in S$ then at least $n - 1$ elements of $f_1, f_2, \ldots, f_k$ are of* rank $n - 1$.

Proof. For every $f, g \in T_n$, if $\mathrm{rank}(f) = n$ then $\mathrm{rank}(fg) = \mathrm{rank}(gf) = \mathrm{rank}(g)$. Thus, without loss of generality, we can suppose that all the f_i have rank $n - 1$ and apply Lemma 5. $\square$

Lemma 17. *Let $n, m \geq 2$. Let A be a generating set of $S_n \times S_m$ of minimum size and $a \in T_n$ be a function of rank $n - 1$, $b \in T_m$ be a function of rank $m - 1$. Then $B = A \cup \{(a, a')\} \cup \{(b', b)\}$, where $(a', b') \in S_m \times S_n$, is a generating set of $T_n \times T_m$ of minimum size. Furthermore, all generating sets of $T_n \times T_m$ of minimum size are of this form.*

Proof. First we show that B generates $T_n \times T_m$. Since

$$(a, 1) = (a, a')(1, a'^{-1}) \quad \text{and} \quad (1, b) = (b', b)(b'^{-1}, 1),$$

B generates $(a, 1), (1, b)$. Let $(f, g) \in T_n \times T_m$. Because $f \in T_n$, there exist $f_1, f_2, \ldots, f_k \in S_n \cup \{a\}$ such that $f = f_1 f_2 \ldots f_k$. Because $g \in T_m$, there exist $g_1, g_2, \dots, g_l \in S_m \cup \{b\}$ such that $g = g_1 g_2 \dots g_l$. Then we have

$$(f, g) = (f_1, 1)(f_2, 1) \dots (f_k, 1)(1, g_1)(1, g_2) \dots (1, g_l).$$

Every $(f_i, 1)$ either is $(a, 1)$ or belongs to $S_n \times S_m$ and every $(1, g_i)$ either is $(1, b)$ or belongs to $S_n \times S_m$. Therefore B generates $(f_i, 1), (1, g_j)$ for $i = 1, 2, \dots, k$ and $j = 1, 2, \dots, l$. Consequently B generates (f, g).

Let C be a generating set of $T_n \times T_m$ of minimum size. Then C must contain a generating set of the maximum $\mathcal{J}$-class which is $S_n \times S_m$. On the other hand, the maximum $\mathcal{J}$-class $S_n \times S_m$ is a subsemigroup; hence, one cannot obtain any elements in the $\mathcal{J}$-classes below by multiplying just elements on the maximum $\mathcal{J}$-class. Therefore, C must contain some elements of some $\mathcal{J}$-classes below the maximum $\mathcal{J}$-class. There are exactly two $\mathcal{J}$-classes which are below the maximum $\mathcal{J}$-class and above all other $\mathcal{J}$-classes. Therefore, C must intersect each of them in at least one element. Note that all such elements have the respective forms (a, a') and (b', b) as described in the statement of the lemma. This shows that $A \cup \{(a, a')\} \cup \{(b', b)\}$ is a generating set of minimum size and all generating sets of minimum size are of this form. □

Proposition 7. *If T_n, T_m are two full transformation semigroups, then*

$$N(T_n \times T_m) = m + n - 2.$$

Proof. If $n = m = 1$ then we have $N(T_1 \times T_1) = 0 = 1 + 1 - 2$. If $n = 1$ or $m = 1$ the equality holds by Corrolary 3. Then suppose $n, m \geq 2$. Let A be a generating set of $S_n \times S_m$ of minimum size. Consider functions α, β defined by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 1 & 2 & \dots & n-1 \end{pmatrix},$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & \dots & m \\ 1 & 1 & 2 & \dots & m-1 \end{pmatrix}.$$

By Lemma 17, $B = A \cup \{(\alpha, 1)\} \cup \{(1, \beta)\}$ is a generating set of $T_n \times T_m$ of minimum size. We have

$$(\alpha, 1)^{n-1}(1, \beta)^{m-1} = (\alpha^{n-1}, 1)\,(1, \beta^{m-1}) = (\alpha^{n-1}, \beta^{m-1}).$$

Since the functions α^{n-1} and β^{m-1} are constant, we have $(\alpha, 1)^{n-1}(1, \beta)^{m-1} \in \ker(T_n) \times \ker(T_m)$. This shows that $N(T_n \times T_m) \leq n - 1 + m - 1 = m + n - 2$.

Next, we prove that $N(T_n \times T_m) \geq m + n - 2$. Suppose

$$B = A \cup \{(a, a')\} \cup \{(b', b)\}$$

is a generating set of $T_n \times T_m$ of minimum size and there are

$$(f_1, g_1), (f_2, g_2), \dots, (f_k, g_k) \in B$$

such that

$$(f_1, g_1)(f_2, g_2) \dots (f_k, g_k) \in \ker(T_n) \times \ker((T_m).$$

Then $f_1 f_2 \dots f_k \in \ker(T_n)$ and $g_1 g_2 \dots g_k \in \ker(T_m)$. By Lemma 16, at least $n - 1$ elements in $\{f_1, f_2, \dots, f_k\}$ are of rank $n - 1$ and $m - 1$ elements of $g_1, g_2, \dots g_k$ are of rank $m - 1$. Since every generator has at least one invertible component, the two conditions cannot be met by the same factor and therefore there are at least $m + n - 2$ factors. □

With the same argument we can generalize Lemma 17 and Proposition 7 for any finite product of full transformation semigroups.

Lemma 18. *Let A be a generating set of $S_{n_1} \times S_{n_2} \times \cdots \times S_{n_k}$ of minimum size and*

$$\alpha_t = (a_1, a_2, \dots, a_t, \dots, a_k) \in T_{n_1} \times T_{n_2} \times \cdots \times T_{n_k} \quad t = 1, 2, \dots k$$

such that

$$\operatorname{rank}(a_t) = n_t - 1 \text{ and } \quad a_i \in S_{n_i} \quad i \in \{1, 2, \dots, k\} \setminus \{t\}.$$

Then $B = A \cup (\bigcup_{t=1}^{k} \{\alpha_t\})$ is a generating set of $T_{n_1} \times T_{n_2} \times \cdots \times T_{n_k}$ of minimum size. Furthermore, all generating sets of $T_{n_1} \times T_{n_2} \times \cdots \times T_{n_k}$ of minimum size are of this form.

Proposition 8. *If T_{n_i} for $1 \leq i \leq k$ are full transformation semigroups, then*

$$N(T_{n_1} \times T_{n_2} \times \cdots \times T_{n_k}) = n_1 + n_2 + \cdots + n_k - k.$$

3.2.2 Wreath product

By the prime decomposition theorem, every finite semigroup is a divisor of an iterated wreath product of its simple group divisors and the three-element monoid U_2 consisting of two right zeros and one identity element [23]. So we are looking for the analogues for the wreath product of the results which we have obtained for the direct product. We consider the *wreath product* of transformation monoids as usual, that is

$$(X, S) \wr (Y, T) = (X \times Y, S^Y \rtimes T),$$

where the action defining the *semidirect product* is given by

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

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

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

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

Note that we apply functions on the right. Our aim is to give an upper bound for $N(S^Y \rtimes T)$ in which (X, S) and (Y, T) are two transformation monoids and $S^Y \rtimes T$ is the semigroup of the wreath product $(X, S) \wr (Y, T)$. Here we introduce some notation which we use subsequently. For $s \in S$ and $y \in Y$ let $(s)_y : Y \to S$ be the function defined by

$$z(s)_y = \begin{cases} s & \text{if } z = y \\ 1 & \text{otherwise} \end{cases}$$

and for every $s \in S$ let $\bar{s} : Y \to S$ be the function defined by $y\bar{s} = s$.

For a given monoid S denote by U_S its *group of units*. We use the notation $\prod_{i=1}^{n} s_i$ for $s_1 s_2 \ldots s_n$ even in the case when the multiplication is not commutative.

Lemma 19. *Let (X, S) and (Y, T) be two transformation monoids. The set*

$$E = \{(f, t) : f \in \ker(S)^Y,\ t \in \ker(T),\ f \textit{ is a constant map}\}$$

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

Proof. It is easy to check that every two elements in E are $\mathcal{J}$-related and $\ker(S)^Y \times \ker(T)$ is an ideal of $S^Y \rtimes T$. Hence given $(f,t) \in E$ and $(g,t') \in \ker(S)^Y \times \ker(T)$, it suffices to show that there exist $h,k \in S^Y, t_1, t_2 \in T$ such that

$$(h,t_1)(g,t')(k,t_2) = (f,t).$$

Since $t,t' \in \ker(T)$, there exist $t_1,t_2 \in \ker(T)$ such that $t_1t't_2 = t$. For each $s,s' \in \ker(S)$, there exist elements $h_{s,s'}, k_{s,s'} \in \ker(S)$ such that $s' = h_{s,s'}sk_{s,s'}$. Define the functions $h,k \in S^Y$ as follows: for each $y \in Y$, let

$$yh = h_{(yt_1)g,yf},$$

$$yk = \begin{cases} k_{(xt_1)g,xf} & \text{if } y = xt_1t' \text{ for some } x \in Y, \\ 1 & \text{otherwise.} \end{cases}$$

Note that the function k is well-defined since, as t_1 and t_1t' are in the same $\mathcal{R}$-class, the equality $\ker(t_1) = \ker(t_1t')$ holds. Now we have

$$(h,t_1)(g,t')(k,t_2) = (h\,{}^{t_1}g\,{}^{t_1t'}k, t_1t't_2) = (f,t)$$

and the proof is complete. $\square$

Note that by Lemma 19, the following inequalities hold:

$$E \subseteq \ker(S^Y \rtimes T) \subseteq \ker(S)^Y \times \ker(T). \tag{3.18}$$

The following examples show that for some wreath products the inclusions in the inequalities (3.18) are proper and for the others are not.

In all the following examples we consider the transformation semigroup (Y,U_2) to be as following. Let $Y = \{1,2\}$ and $\alpha,\beta : Y \to Y$ be the constant functions $1,2$, respectively. Let $U_2 = \{1,\alpha,\beta\}$. Then U_2 acts faithfully on Y and so (Y,U_2) is a transformation semigroup.

Example 6. Let (X,G) be a finite permutation group. Consider the wreath product $(X,G) \wr (Y,U_2)$. It is easy to see that the minimum ideal of $G^Y \rtimes U_2$ is the whole $\ker(G)^Y \times \ker(U_2)$.

Example 7. Let (X,T_3) be the full transformation semigroup of degree three. Consider the wreath product $(X,T_3) \wr (Y,U_2)$. Computer calculations give the minimum ideal of $T_3^Y \rtimes U_2$ to be the set

$$E = \{(f,t) : f \in \ker(T_3)^Y,\ t \in U_2,\ f \text{ is a constant map}\}.$$

Example 8. Let V be the transformation monoid generated by identity and two transformations

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 1 & 4 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 3 & 2 & 2 \end{pmatrix}. \tag{3.19}$$

Computer calculations (using the semigroup package in Mathematica) give the minimum ideal of $V^Y \rtimes U_2$ to have 16 elements, while E has 8 elements and $\ker(V)^Y \times \ker(U_2)$ has 32 elements. Hence in this example the inequalities (3.18) are proper.

Lemma 20. *Let (X, S) and (Y, T) be two transformation monoids. Then*

$$\operatorname{rank}(S^Y \rtimes T) \geq \operatorname{rank}(S^Y \rtimes U_T) + \operatorname{rank}(T) - \operatorname{rank}(U_T). \tag{3.20}$$

Proof. Let $S_1 = S^Y \rtimes U_T$ and $S_2 = S^Y \rtimes (T \setminus U_T)$. It is easy to check that $S^Y \rtimes T = S_1 \cup S_2$ is a partition into two subsemigroups. Because S_2 is an ideal of $S^Y \rtimes T$, every generating set of $S^Y \rtimes T$ must contain a generating set of S_1. Moreover, we need at least $\operatorname{rank}(T) - \operatorname{rank}(U_T)$ elements for generating S_2, since the set of second components of the elements in any generating set of $S^Y \rtimes T$ is a generating set of T. Combining these two facts gives precisely the assertion of the lemma. □

Lemma 21. *If (X, S) is a transformation monoid and (Y, G) is a permutation group then*

$$\operatorname{rank}(S^Y \rtimes G) \geq |Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S)) + \operatorname{rank}(U_S^Y \rtimes G). \tag{3.21}$$

Proof. It is easy to check that

$$S^Y \rtimes G = ((S^Y \setminus U_S^Y) \rtimes G) \cup (U_S^Y \rtimes G),$$

is a partition into two subsemigroups of $S^Y \rtimes G$. Because $(S^Y \setminus U_S^Y) \rtimes G$ is an ideal, every generating set of $S^Y \rtimes G$ must contain a generating set of $U_S^Y \rtimes G$. To complete the proof, it is enough to show that every generating set of $S^Y \rtimes G$ has at least $|Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S))$ elements in $(S^Y \setminus U_S^Y) \rtimes G$. Let A be a generating set of $S^Y \rtimes G$. One can easily check that, denoting by π_1 the projection on the first component,

$$A' = \{{}^t f : f \in A\pi_1, t \in G\}$$

is a generating set of S^Y. The equality

$$\operatorname{rank}(S^Y) = \operatorname{rank}(U_S^Y) + |Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S))$$

has been proved in [31, Theorem 1]. Hence, A' has at least

$$|Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S))$$

elements in $S^Y \setminus U_S^Y$. On the other hand, if f belongs to U_S^Y and t belongs to G then ${}^t f \in U_S^Y$. Therefore $A\pi_1$ must contain at least

$$|Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S))$$

elements in $S^Y \setminus U_S^Y$. This implies that A has at least

$$|Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S))$$

elements in $(S^Y \setminus U_S^Y) \rtimes G$ and the proof is complete. $\square$

Proposition 9. *Let (X, S) and (Y, T) be two transformation monoids. Then the rank of $S^Y \rtimes T$ is greater than or equal to*

$$\operatorname{rank}(U_S^Y \rtimes U_T) + |Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S)) + \operatorname{rank}(T) - \operatorname{rank}(U_T). \quad (3.22)$$

Proof. This is straightforward using Lemmas 20 and 21 . $\square$

Proposition 10. *Let (X, S) and (Y, T) be two transformation monoids. Let A', A and B be generating sets of minimum size of $U_S^Y \rtimes U_T$, S, and T, respectively. The set*

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

is a generating set of $S^Y \rtimes T$ with minimum size. Consequently, the rank of $S^Y \rtimes T$ is equal to

$$\operatorname{rank}(U_S^Y \rtimes U_T) + |Y|(\operatorname{rank}(S) - \operatorname{rank}(U_S)) + \operatorname{rank}(T) - \operatorname{rank}(U_T). \quad (3.23)$$

Proof. First we show that C is a generating set. Consider a pair

$$(f, t) \in S^Y \rtimes T.$$

Because B is a generating set of T, there exist $b_1, b_2, \ldots, b_k \in B$ such that $t = b_1 b_2 \ldots b_k$. This leads to the following factorization:

$$(f,t) = (f,1)(\bar{1},t) = \prod_{y \in Y} ((yf)_y, 1) \prod_{i=1}^{k} (\bar{1}, b_i). \tag{3.24}$$

Because A is a generating set of S and $yf \in S$, for every $y \in Y$ there exist $a_{y1}, a_{y2}, \ldots, a_{yk_y} \in A$ such that

$$yf = \prod_{i=1}^{k_y} a_{yi}.$$

Accordingly, we obtain the factorization

$$((yf)_y, 1) = \prod_{i=1}^{k_y} ((a_{yi})_y, 1). \tag{3.25}$$

Consider the pair $((a_{yi})_y, 1)$ in (3.25). If $a_{yi} \in U_S$ then $((a_{yi})_y, 1) \in U_S^Y \rtimes U_T$ can be factorized into elements of A'; otherwise, $((a_{yi})_y, 1) \in C$. This shows that the first product in (3.24) can be rewritten in terms of elements of C. Now consider the pair $(\bar{1}, b_i)$ in the second product in (3.24). If $b_i \in U_T$ then $(\bar{1}, b_i) \in U_S^Y \rtimes U_T$ can be factorized into elements of A'; otherwise, $(\bar{1}, b_i) \in C$. This shows that the second product in (3.24) can be rewritten in terms of elements of C. Thus, (f,t) can be factorized into elements of C, whence C is a generating set of $S^Y \rtimes T$, which is the desired conclusion. Now, according to Proposition 9, the size of C is equal to $\mathrm{rank}(S^Y \rtimes T)$. $\square$

Notation 8. For a finite group G denote by $\mathrm{diam}_{min}(G)$ the minimum of $\mathrm{diam}(G, A)$ over all generating sets of minimum size.

Theorem 3. *Given two transformation monoids (X, S) and (Y, T), there exist integers $0 \le m_1 < N(S)$ and $0 \le m_2 < N(T)$ such that*

$$\begin{aligned} N(S^Y \rtimes T) \le & (m_1 + m_2)\mathrm{diam}_{min}(U_S^Y \rtimes U_T) \\ & + |Y|(N(S) - m_1) + N(T) - m_2. \end{aligned} \tag{3.26}$$

Proof. Let A and B be generating sets of minimum size of S and T, respectively, 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 $a_1 a_2 \ldots a_{N(S)} \in \ker(S)$ and $b_1 b_2 \ldots b_{N(T)} \in \ker(T)$. Denote by m_1 and m_2 the number of invertible factors in the words $a_1 a_2 \ldots a_{N(S)}$ and $b_1 b_2 \ldots b_{N(T)}$, respectively. Define the function f from Y to $\ker(S)$ to be the constant map with image $a_1 a_2 \ldots a_{N(S)}$. By Lemma 19, the pair $(f, b_1 b_2 \ldots b_{N(T)})$ is an element of the minimum ideal of $S^Y \rtimes T$.

Let A' be a generating set of $U_S^Y \rtimes U_T$ of minimum size such that $\operatorname{diam}(U_S^Y \rtimes U_T, A') = \operatorname{diam}_{min}(U_S^Y \rtimes U_T)$. By Proposition 10, the set

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

is a generating set of $S^Y \rtimes T$ of minimum size. To establish the inequality (3.26), it is enough to show that the pair $(f, b_1 b_2 \ldots b_{N(T)})$ is a product of at most

$$(m_1 + m_2)\operatorname{diam}_{min}(U_S^Y \rtimes U_T) + |Y|(N(S) - m_1) + N(T) - m_2$$

elements of C. We have

$$(f, b_1 b_2 \ldots b_{N(T)}) = (f, 1)(\bar{1}, b_1 b_2 \ldots b_{N(T)}) = \prod_{i=1}^{N(S)} (\bar{a}_i, 1) \prod_{i=1}^{N(T)} (\bar{1}, b_i). \qquad (3.27)$$

Consider the pair $(\bar{a}_i, 1)$ in the first product of (3.27). If $a_i \in A \setminus U_S$, then

$$(\bar{a}_i, 1) = \prod_{y \in Y} ((a_i)_y, 1),$$

which is a product of $|Y|$ elements in

$$\{((a)_y, 1) : a \in A \setminus U_S, y \in Y\}.$$

If $a_i \in U_S$, then $(\bar{a}_i, 1)$ can be written as a product of at most $\operatorname{diam}_{min}(U_S^Y \rtimes U_T)$ elements in A'. Accordingly, the first product in (3.27) can be rewritten as a product of at most

$$|Y|(N(S) - m_1) + m_1 \operatorname{diam}_{min}(U_S^Y \rtimes U_T)$$

elements in C. Now consider the factor $(\bar{1}, b_i)$ of the second product in (3.27). If $b_i \in B \setminus U_T$ then $(\bar{1}, b_i) \in C$; otherwise, $(\bar{1}, b_i) \in U_S^Y \rtimes U_T$ can be written as a product of at most $\mathrm{diam}_{min}(U_S^Y \rtimes U_T)$ elements in A'. Thus, the second product in (3.27) can be rewritten as a product of at most

$$N(T) - m_2 + m_2 \mathrm{diam}_{min}(U_S^Y \rtimes U_T)$$

elements in C. Combining these two facts shows that $(f, b_1 b_2 \ldots b_{N(T)})$ can be written as a product of at most

$$(m_1 + m_2)\mathrm{diam}_{min}(U_S^Y \rtimes U_T) + |Y|(N(S) - m_1) + N(T) - m_2$$

elements in C, which proves the theorem. □

In the rest of this section we study some special cases.

Theorem 4. *Given two transformation monoids (X, S) and (Y, T), suppose that $T \neq \{1\}$ has trivial group of units and $|Y| = n$. Then the following inequality holds:*

$$N(S^Y \rtimes T) \leq \max\{n, \mathrm{diam}(U_S^Y, A')\}N(S) + N(T), \tag{3.28}$$

where A' is a generating set of U_S^Y with minimum size. Furthermore, if $\mathrm{rank}(U_S^k) = k\,\mathrm{rank}(U_S)$ for $k \geq 1$, then

$$N(S^Y \rtimes T) \leq nN(S) + N(T). \tag{3.29}$$

Proof. Let A and B be two generating sets of minimum size of S and T, respectively, 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 $b_1, b_2, \ldots, b_{N(T)} \in B \setminus \{1\}$ such that

$$a_1 a_2 \ldots a_{N(S)} \in \ker(S)$$

and

$$b_1 b_2 \ldots b_{N(T)} \in \ker(T).$$

Define the function f from Y to $\ker(S)$ to be the constant map with image $a_1 a_2 \ldots a_{N(S)}$. By Lemma 19, the pair $(f, b_1 b_2 \ldots b_{N(T)})$ is an element of the minimum ideal of $S^Y \rtimes T$. Let A' be a generating set of U_S^Y with minimum size. By Proposition 10, the set

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

is a generating set of $S^Y \rtimes T$ with minimum size. To establish the inequality (3.28), it is enough to show that the pair $(f, b_1 b_2 \dots b_{N(T)})$ is a product of at most

$$\max\{n, \operatorname{diam}(U_S^Y, A')\}N(S) + N(T)$$

elements of C'. We have

$$(f, b_1 b_2 \dots b_{N(T)}) = (f, 1)(\bar{1}, b_1 b_2 \dots b_{N(T)}) = \prod_{i=1}^{N(S)} (\bar{a}_i, 1) \prod_{i=1}^{N(T)} (\bar{1}, b_i). \quad (3.30)$$

For $i = 1, 2, \dots, N(T)$, the pair $(\bar{1}, b_i)$ belongs to C'. Consider next the pairs $(\bar{a}_j, 1)$ with

$$j = 1, 2, \dots, N(S).$$

If $a_j \in A \setminus U_S$, then $(\bar{a}_j, 1) = \prod_{y \in Y} ((a_j)_y, 1)$, which is a product of n elements in

$$\{((a)_y, 1) : a \in A \setminus U_S, y \in Y\}.$$

If $a_j \in U_S$, then $(\bar{a}_j, 1)$ can be written as a product of at most $\operatorname{diam}(U_S^Y, A')$ elements in $\{(g, 1) : g \in A'\}$. Therefore, the product on the rightmost side of (3.30) can be rewritten as a product of at most

$$\max\{n, \operatorname{diam}(U_S^Y, A')\}N(S) + N(T)$$

elements in C' as we required.

Consider the case where $\operatorname{rank}(U_S^Y) = |Y| \operatorname{rank}(U_S)$. By Proposition 10, the set

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

is a generating set of $S^Y \rtimes T$ of minimum size. More precisely, since U_T is trivial and $\operatorname{rank}(U_S^Y) = |Y| \operatorname{rank}(U_S)$, substituting $\operatorname{rank}(U_S^Y \rtimes U_T)$ by $|Y| \operatorname{rank}(U_S)$ in formula (3.23) in Proposition 10, gives $|Y| \operatorname{rank}(S) + \operatorname{rank}(T)$ which is equal to $|C''|$. We can factorize the pair $(f, b_1 b_2 \dots b_{N(T)})$ in $nN(S) + N(T)$ elements of C'' as follows:

$$(f, b_1 b_2 \dots b_{N(T)}) = (f, 1)(\bar{1}, b_1 b_2 \dots b_{N(T)}) = \prod_{y \in Y} \prod_{i=1}^{N(S)} ((a_i)_y, 1) \prod_{i=1}^{N(T)} (\bar{1}, b_i). \quad (3.31)$$

This establishes the inequality (3.29) and completes the proof of the theorem. $\square$

Chapter 4

The diameter of a finite group

Some of the upper bounds of Theorems 2, 3 and 4 involve the diameter of a group. In this chapter we try to find an upper bound for the diameter of a direct power of a group. Recall that the diameter of a finite group G with respect to a generating set A is the maximum over $g \in G$ of the length of the shortest word in A representing g. A simple argument shows that the diameter of a group with respect to any generating set is bounded above by the group order minus the group rank (see Proposition 1). The cyclic groups are examples whose diameter is as large as the group order minus the group rank. If G is a finite group, then the direct power G^n is not cyclic for $n \geq 2$. Thus the following natural question arises. Is there any smaller upper bound (less than $|G^n| - \mathrm{rank}(G^n)$) for the diameter of G^n? In fact, $|G|^n - \mathrm{rank}(G^n)$ is exponentially large in terms of $|G|$. The more precise question in which we are really interested is whether the diameter of a direct power of a finite group is polynomially bounded. Investigating it, we were led to the following conjectures. Throughout this chapter, G^n denotes the n-th direct power of the group G.

Conjecture (strong)**.** *Let G be a finite group. Then the diameter $D(G^n)$ is at most $n(|G| - \mathrm{rank}(G))$.*

Conjecture (weak)**.** *Let G be a finite group. There exists a generating set A for G^n of minimum size such that*

$$\mathrm{diam}(G^n, A) \leq n(|G| - \mathrm{rank}(G)). \tag{4.1}$$

Remark 9. Both conjectures hold for trivial groups.

As the second conjecture is a consequence of the first one, it may be easier to establish. Anyway, each of the proposed conjectures has advantages and disadvantages when attempting to prove them. The difficulty in proving the weak conjecture is dealing with generating sets of minimum size for the direct powers of finite groups. Finding a generating set of minimum size for a direct power of a finite group is itself a problem. Nevertheless, there exist in the literature many results regarding the computation of the rank of a direct power of a finite group, e.g., [27, 28, 29, 30, 20]. On the other hand, every direct power G^n of a finite group has a generating set, called canonical generating set (Definition 14), which satisfies the inequality (4.1). So, the weak conjecture for groups whose rank is equal to the size of the canonical generating set is true. For instance, the canonical generating set for direct powers of nilpotent groups is a generating set of minimum size (Corollary 5). Therefore, nilpotent groups satisfy the weak conjecture easily. However, the canonical generating set is not always a generating set of minimum size. Then the difficulty of establishing the weak conjecture appears when we consider the groups for which the rank of their direct powers is not equal to the size of the canonical generating set. On the other hand, the strong conjecture concerns arbitrary generating sets. It has the advantage that there are many results in the literature regarding the computation of the diameter of a finite group with respect to an arbitrary generating set. Hence, we may use the upper bounds obtained by other authors to approach the strong conjecture .

This chapter is organized as follows. In the first section, we show that Abelian groups satisfy the strong conjecture. The second section deals with generating sets of minimum size for direct powers of finite groups. Finally, in the last section we present some families of finite groups which satisfy the weak conjecture.

4.1 Abelian groups and the strong conjecture

During this work I encountered a paper by John Wilson from 2005 which presents an exact formula for the symmetric diameter of Abelian groups [32]. After studying the paper I found that it is possible to find an upper bound for the diameter of Abelian groups by using the same methods. But there is a gap in one of the arguments in that paper. Therefore, it was not possible to use the same method unless I could fix it. I made some efforts to fix it but I could not do that. Finally, I decided to write to the author and ask him for his help. But at the same time I was thinking about finding another solution. Meanwhile, I found two other papers in which both the diameter and the symmetric diameter of Abelian groups had been computed [17, 18]. So I could reach my goal in another way. After a while, John Wilson sent me a correct argument so in the end I could use the initial idea. In fact, the idea is to use Theorem 6, which has been published in [18] with another proof. In this section we show that Abelian groups satisfy the strong conjecture. Before going to the main result we explain the gap in Wilson's paper and his correction.

A canonical decomposition of a finite Abelian group G is an expression of G as a direct product of cyclic subgroups whose orders $m_1, m_2, \dots, m_k$ satisfy $m_i \mid m_{i-1}$ for $i = 1, 2, \dots, k$. Then $m_1, m_2, \dots, m_k$ are the invariants of G. Following the notation in [17] we say G is of type $(m_1, m_2, \dots, m_k)$. The following theorem has been obtained following two different approaches [32, 17].

Notation 9. Denote by $\lfloor n \rfloor$ the greatest integer less than or equal to n.

Theorem 5. *A finite Abelian group G of type $(m_1, m_2, \dots, m_k)$ has symmetric diameter*

$$D^s(G) = \sum_{i=1}^{k} \lfloor m_i/2 \rfloor.$$

In [32] Wilson proved the following lemma for establishing Theorem 5.

Notation 10. For a finite Abelian group G of type $(m_1, m_2, \dots, m_k)$, write $s(G) = \sum_{i=1}^{k} \lfloor m_i/2 \rfloor$.

Lemma 22. *[32, Lemma 3.2] Let A be a finite Abelian group and B a subgroup with A/B cyclic of order r. Then*

$$s(B) + \left\lfloor \frac{r}{2} \right\rfloor \leq s(A).$$

Unfortunately, there is an error in the argument of the proof in [32, Lemma 3.2]. In fact, the author claims:

> "Let A be a direct product of non-trivial cyclic groups of orders $m_1, m_2, \dots, m_k$ with $m_{i+1} \mid m_i$ for each i and let B be a product of cyclic groups respectively of order $u_1, u_2, \dots, u_k$ with $u_{i+1} \mid u_i$ for each i. We have $u_i \mid m_i$ for each i; write $m_i = u_i v_i$. Since A/B is cyclic, no prime can divide v_i, v_j for distinct i, j."

which is not true in general. Consider the following counterexample:

Example 9. Let $A = \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ and $B = \{1\} \times \mathbb{Z}_4 \times \mathbb{Z}_2$. Then A/B is cyclic of order 8. On the other hand, we have $B \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \{1\}$. Hence the integers $v_1 = v_2 = v_3$ are all equal to 2, so they are not pairwise coprime.

Nevertheless, the statement of the lemma is still true. Now we will present the new proof of Lemma 22 suggested by John Wilson. He used the following easy observations in his proof. If A has exponent e (i.e. the least common multiple of the orders of all elements of the group), then any cyclic subgroup of order e is a factor in a canonical decomposition. If f divides e then the numbers $gcd(f, m_i)$ are the invariants of the subgroup $\{a \mid a^f = 1\}$.

Lemma 23 (J. Wilson)**.** *For each finite Abelian group A and subgroup B we have*

$$s(B) + s(A/B) \leq s(A).$$

Proof. We argue by induction on $|A|$, with a secondary induction on $|A/B|$. First we claim that it suffices to prove the result in the case when A/B is cyclic. Suppose that A/B is not cyclic and let A_1/B be a subgroup in a canonical decomposition of A/B; thus $s(A/B) = s(A_1/B) + s(A/A_1)$. By induction we have $s(B) + s(A_1/B) \leq s(A_1)$ and $s(A_1) + s(A/A_1) \leq s(A)$. Therefore,

$$S(B) + s(A/B) = s(B) + s(A_1/B) + s(A/A_1) \leq s(A_1) + s(A/A_1) \leq s(A)$$

as required.

Let A have exponent e. Suppose that B has a cyclic subgroup X of order e; then A has a canonical decomposition with one factor equal to X; let A_1 be the sum of the other factors and $B_1 = B \cap A_1$. Thus $B = X \times B_1$ and $A/B \cong A_1/B_1$, and we have

$$s(B) + s(A/B) = s(X) + s(B_1) + s(A_1/B_1) \leq s(X) + s(A_1) \leq s(A).$$

On the other hand, if A/B has order e then the pre-image of a generator of A/B generates a factor Y in a canonical decomposition of A; hence $A \cong Y \times B$ and $s(B) + s(A/B) = s(A)$.

So we can assume that the exponent f of B satisfies $f < e$ and $|A/B| < e$; hence $f \leq e/2$ and $|A/B| \leq e/2$. Let $A_1 = \{a \mid a^f = 1\}$. Let $m_1, m_2, \ldots, m_k$ be the invariants of A and $n_1, n_2, \ldots, n_k$ be the invariants of A_1. We know that $n_i = gcd(f, m_i)$. Since $m_1 = e$ then we get $n_1 = f$. Now we have $s(A) = \left\lfloor \frac{e}{2} \right\rfloor + \sum_{i=2}^{k} \left\lfloor \frac{m_i}{2} \right\rfloor$ and $s(A_1) = \left\lfloor \frac{f}{2} \right\rfloor + \sum_{i=1}^{k} \left\lfloor \frac{n_i}{2} \right\rfloor$. Since $f \leq e/2$ it follows that $s(A) - s(A_1) \geq \left\lfloor \frac{e}{2} \right\rfloor - \left\lfloor \frac{e}{4} \right\rfloor$. Then we have

$$s(A) - s(B) \geq s(A) - s(A_1) \geq \lfloor e/2 \rfloor - \lfloor e/4 \rfloor,$$

and

$$s(A/B) \leq \lfloor e/4 \rfloor,$$

and the conclusion follows. □

Analogously, introduce the notation s' for a finite Abelian group G of type $(m_1, m_2, \ldots, m_k)$ by letting $s'(G) = \sum_{i=1}^{k}(m_i - 1)$. Then it is easy to check that the same argument as in the proof of Lemma 23 works for the following lemma as well.

Lemma 24. *For each finite Abelian group A and subgroup B we have*

$$s'(B) + s'(A/B) \leq s'(A).$$

Now we have the following theorem.

Theorem 6. *Let G be a finite Abelian group of type $(m_1, m_2, \ldots, m_k)$. We have*

$$D(G) = s'(G).$$

Proof. Suppose $G = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k}$, where $C_{m_i} = \langle a_i \rangle$. The set $A = \{(1, \ldots, \overbrace{a_i}^{i\,\text{th}}, \ldots, 1) : a_i \in C_{m_i}\}$ is a generating set of G such that $\operatorname{diam}(G, A) = \sum_{i=1}^{k}(m_i - 1)$. Hence we have $D(G) \geq s'(G)$. Now we show that $D(G) \leq s'(G)$. If G is cyclic the result follows immediately. Suppose that G is not cyclic and let X be a generating set for G. We show that every element of G can be expressed as a word in X of length at most $s'(G)$. We argue by induction on $|G|$. We may suppose that no proper subset of X generates G. Choose $x \in X$, let $H = \langle X \setminus \{x\} \rangle$ and let r be the order of x modulo H. Let $a \in G$. There exists $0 \leq j \leq r - 1$ such that $a = x^j b$ for some $b \in H$. Since G is not cyclic, H is not trivial. Then b has length at most $s'(H)$ by induction and therefore a has length at most $r - 1 + s'(H)$ and so at most $s'(G)$, by Lemma 24. □

Another proof of Theorem 6 has been published in [18].

Corollary 4. *Let G^n be a direct power of a finite Abelian group G. The following inequality holds*

$$D(G^n) = nD(G) \leq n\,(|G| - \mathrm{rank}(G)).$$

Proof. Let $G = C_1 \times C_2 \times \cdots \times C_k$ be a canonical decomposition of G. We have

$$G^n \cong C_1^n \times C_2^n \times \cdots \times C_k^n.$$

Using Theorem 6, we obtain

$$D(G^n) = s'(G^n) = \sum_{i=1}^{k} n\,(|C_i| - 1) = n \sum_{i=1}^{k}(|C_i| - 1) \leq n\,(|G| - \mathrm{rank}(G)). \quad \square$$

4.2 Generating sets of minimum size

In this section we exhibit generating sets of minimum size for the direct powers of some families of finite groups.

Definition 14. Let G be a finite group with a generating set A. By the *canonical generating set* of G^n with respect to A, we mean the set

$$C^n(A) := \{(1, \ldots, \overbrace{a}^{i\,\mathrm{th}}, \ldots, 1) : i \in \{1, 2, \ldots, n\}, a \in A\}.$$

Lemma 25. *Let G be a finite group with a generating set A. For $n \geq 1$ we have* $\mathrm{diam}(G^n, C^n(A)) \leq n\ \mathrm{diam}(G, A)$.

Proof. For given $(g_1, g_2, \ldots, g_n) \in G^n$ we have

$$(g_1, g_2, \ldots, g_n) = \prod_{i=1}^{n}(1, \ldots, g_i, \ldots, 1).$$

Then $l_{C^n(A)}(g_1, g_2, \ldots, g_n) \leq \sum_{i=1}^{n} l_{C^n(A)}(1, \ldots, g_i, \ldots, 1)$. By the definition of $C^n(A)$, for $i \geq 1$, we have $l_{C^n(A)}(1, \ldots, g_i, \ldots, 1) \leq \mathrm{diam}(G, A)$ which gives the desired conclusion. $\square$

Lemma 26. [27] *Let G be a finite group and k be a positive integer. Then*

$$k\,\mathrm{rank}(G/G') \leq \mathrm{rank}(G^k) \leq k\,\mathrm{rank}(G), \tag{4.2}$$

where G' is the commutator subgroup of G.

The following is an application of Lemma 26.

Corollary 5. *Let G be a finite group. If* $\operatorname{rank}(G) = \operatorname{rank}(G/G')$*, then the following equality holds:*

$$\operatorname{rank}(G^n) = n \operatorname{rank}(G). \tag{4.3}$$

In particular, nilpotent groups satisfy this property.

Proof. The first statement is an immediate consequence of Lemma 26. We prove the second statement. Note that, if H is a homomorphic image of a finite group G, then $\operatorname{rank}(H) \leq \operatorname{rank}(G)$. Therefore, it is enough to show that $\operatorname{rank}(G) \leq \operatorname{rank}(G/G')$ for every finite nilpotent group G. Let $A = \{g_1G', g_2G', \ldots, g_kG'\}$ be a generating set of G/G' of minimum size. Consider an arbitrary element $g \in G$. There exist some $i_1, i_2, \ldots, i_l \in \{1, 2, \ldots, k\}$ such that $gG' = g_{i_1}g_{i_2}\ldots g_{i_l}G'$. This shows that G is generated by $\{g_1, g_2, \ldots, g_k\}$ together with some elements in G'. Because G is nilpotent, it is generated by $\{g_1, g_2, \ldots, g_k\}$ alone, see [19, page 350]. Therefore, $\operatorname{rank}(G) \leq \operatorname{rank}(G/G')$, which completes the proof. $\square$

Definition 15. A group is said to be *perfect* if it equals its own commutator subgroup.

Lemma 27. *Let G be a finite group which is not perfect. If G can be generated by k elements of mutually coprime orders, then*

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

for $n \geq k$.

Proof. Because G is not perfect, it follows from Lemma 26 that $\operatorname{rank}(G^n) \geq n$. Suppose

$$A = \{a_1, a_2, \ldots, a_k\}$$

is a generating set of G such that the a_i's are of mutually coprime orders. Let $n \geq k$. We construct a generating set of size n for G^n. For $1 \leq i \leq n$, define the elements $g_i \in G^n$ as follows:

$$g_i = (1, \ldots, \overbrace{a_1}^{i\,\text{th}}, a_2, \ldots, a_k, \ldots, 1) \text{ for } 1 \leq i \leq n-k+1,$$

$$g_i = (a_{n-i+2}, a_{n-i+3}, \ldots, a_k, 1, \ldots, 1, \overbrace{a_1}^{i\,\text{th}}, \ldots, a_{n-i+1}) \text{ for } n-k+2 \leq i \leq n.$$

We prove that

$$C = \{g_1, g_2, \dots, g_n\}$$

is a generating set of G^n. If we show that C generates $C^n(A)$, then we are done. Choose an arbitrary element $(1, \dots, a_i, \dots, 1) \in C^n(A)$. Since the a_i's are of mutually coprime orders, there exists a positive integer ℓ such that

$$(1, \dots, a_i, \dots, 1) = (1, \dots, a_1, \dots, a_i, \dots, a_k, \dots, 1)^\ell.$$

This yields the desired conclusion. □

4.2.1 Symmetric groups S_n

Denote by $\operatorname{ord}(g)$ the order of a group element g.

Corollary 6. *For $k \geq 2$, the equality*

$$\operatorname{rank}(S_n^k) = k,$$

holds.

Proof. Since the derived subgroup of S_n is A_n, S_n is not perfect. Now the assertion follows immediately by Lemmas 27 and 15. □

4.2.2 Dihedral groups D_n

Definition 16. The dihedral group D_n is the group of symmetries of a regular polygon with n sides.

We consider the *dihedral group* D_n as a subgroup of S_n.

Proposition 11. *For odd n and $k \geq 2$, the rank of D_n^k is k and, for even n, the rank of D_n^k is $2k$.*

Proof. Suppose for the moment that n is odd. Let

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & 1 \end{pmatrix}, \; b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}.$$

It is easy to check that $A = \{a, b\}$ is a generating set of D_n. Because a, b have coprime orders, Lemma 27 gives the desired conclusion.

Now let n be even. The commutator subgroup of D_n is a cyclic group of order $\frac{n}{2}$, and the quotient group is the Klein four-group and thus

$$\text{rank}(\frac{D_n}{D_n'}) = 2.$$

On the other hand,

$$\text{rank}(D_n) = 2.$$

Using Corollary 5, we get $\text{rank}(D_n^k) = 2k$. $\square$

4.2.3 Alternating groups A_n

The following example gives a generating set of minimum size for a direct power of the alternating group A_4.

Example 10. It is easy to see that A_4 is generated by the two elements

$$\alpha = (1\ 2)(3\ 4),\ \beta = (1\ 2\ 3).$$

Since A_4 is not perfect and α, β have coprime orders by Lemma 27, the rank of A_4^n is equal to n, for $n \geq 2$.

Recall that the alternating groups A_n for $n \geq 5$ are simple. Since non-Abelian simple groups are perfect, the alternating groups A_n for $n \geq 5$ are perfect. There is a different approach to compute the rank of the direct power of perfect groups using the Eulerian function of a group (see [11, 27]). The following lemma is a consequence of the results in [11].

Lemma 28. *Let G be a non-Abelian simple group. If G is generated by n elements, then the set $\{(a_{i1}, a_{i2} \ldots, a_{ik}) : i = 1, \ldots, n\}$ will generate G^k if and only if the following conditions are satisfied:*

1. *the set $\{a_{1i}, a_{2i}, \ldots, a_{ni}\}$ is a generating set of G for $i = 1, \ldots, k$;*

2. *there is no automorphism $f : G \to G$ which maps $(a_{1i}, a_{2i}, \ldots, a_{ni})$ to $(a_{1j}, a_{2j}, \ldots, a_{nj})$ for any $i \neq j$.*

Furthermore, in [11] Hall shows that the alternating group A_5 satisfies Lemma 28 with $n = 2$ for $1 \leq k \leq 19$ and not for $k \geq 20$.

Therefore, the following is an immediate consequence of Lemma 28.

Corollary 7. *A pair* $(s_1, \ldots, s_k), (t_1, \ldots, t_k)$ *will generate* A_5^k *if and only if the following conditions are satisfied:*

1. *the set* $\{s_i, t_i\}$ *is a generating set of* A_5 *for* $i = 1, ..., k$*;*
2. *there is no automorphism* $f : A_5 \to A_5$ *which maps* (s_i, t_i) *to* (s_j, t_j) *for any* $i \neq j$*.*

Furthermore, $k = 19$ *is the largest number for which these conditions can be satisfied. That is, the rank of* A_5^k *is equal to* 2*, if and only if* $1 \leq k \leq 19$*.*

4.2.4 Solvable Groups

The following theorem has been proved by Wiegold in [28].

Theorem 7. *[28] Let* G *be a finite non-trivial solvable group, and set*

$$\operatorname{rank}(G) = \alpha, \ \operatorname{rank}(G/G') = \beta.$$

Then

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

for $n \geq \alpha/\beta$*.*

4.3 Diameter of direct powers of groups

Here, we present some families of groups which satisfy the weak conjecture.

Remark 10. Every group G with the property

$$\operatorname{rank}(G^n) = n \operatorname{rank}(G), \tag{4.4}$$

satisfies the weak conjecture. More precisely, if A is a generating set of G with minimum size then $C^n(A)$ is a generating set of minimum size for G^n. So the statement is obvious by Lemma 25.

Then it suffices to justify the weak conjecture for groups that do not have property (4.4). In particular, by Corollary 5, every nilpotent group has property (4.4) .

Proposition 12. *Let* G *be a solvable group such that* $\alpha = \operatorname{rank}(G)$ *and* $\beta = \operatorname{rank}(G/G')$*. Then* G^n *satisfies the weak conjecture for* $n \geq \frac{\alpha}{\beta}$*.*

Proof. By Theorem 7, we have $\mathrm{rank}(G^n) = n\mathrm{rank}(G/G')$. Since G/G' is Abelian, we have $\mathrm{rank}((G/G')^n) = n\mathrm{rank}(G/G')$. Moreover, since $G^n/(G')^n \cong (G/G')^n$ and $(G')^n \cong (G^n)'$ we get $\mathrm{rank}(G^n) = \mathrm{rank}(G^n/(G^n)')$. It means G^n satisfies the property of Corollary 5. Now the result follows from Remark 10. $\square$

Remark 11. Let $(g_1, g_2, \ldots, g_n) \in G^n = \langle A \rangle$. Since $(g_1, g_2, \ldots, g_n)$ is a product of n elements of the form $(1, \ldots, g_i, \ldots, 1)$, then we have

$$l_A(g_1, g_2, \ldots, g_n) \leq \sum_{i=1}^{n} l_A(1, \ldots, g_i, \ldots, 1). \tag{4.5}$$

The following easy lemma gives an upper bound for the diameter of a direct power of a finite group G in terms of the diameter of the group G. We use this lemma in the next section to prove that the symmetric group S_n satisfies the weak conjecture.

Lemma 29. *For a given generating set A of G^n,*

$$\mathrm{diam}(G^n, A) \leq M l_A(C^n(X)) \sum_{i=1}^{n} \mathrm{diam}(G, A\pi_i),$$

where

$$X = \bigcup_{i=1}^{n} (A\pi_i \setminus \{1\}),$$

and $\pi_i : G^n \to G$ maps each element to its i-th cordinate.

Proof. Let $(g_1, g_2, \ldots, g_n) \in G^n$. Since, for $i = 1, 2, \ldots, n$, $A\pi_i \setminus \{1\}$ is a generating set of G, there exist

$$g_{i1}, g_{i2}, \ldots, g_{ik_i} \in A\pi_i \setminus \{1\}, \text{ for some } k_i \leq \mathrm{diam}(G, A\pi_i),$$

such that

$$g_i = g_{i1} g_{i2} \cdots g_{ik_i}.$$

This gives

$$(1, \ldots, g_i, \ldots, 1) = \prod_{j=1}^{k_i} (1, \ldots, g_{ij}, \ldots, 1),$$

hence,

$$l_A(1, \ldots, g_i, \ldots, 1) \leq \sum_{j=1}^{k_i} l_A(1, \ldots, g_{ij}, \ldots, 1). \tag{4.6}$$

Substituting (4.6) into (4.5), we get

$$\begin{aligned} l_A(g_1, g_2, \ldots, g_n) &\leq \sum_{i=1}^{n} \sum_{j=1}^{k_i} l_A(1, \ldots, g_{ij}, \ldots, 1) \\ &\leq \sum_{i=1}^{n} \sum_{j=1}^{k_i} M l_A(C^n(X)) \\ &= M l_A(C^n(X)) \sum_{i=1}^{n} k_i \\ &\leq M l_A(C^n(X)) \sum_{i=1}^{n} \mathrm{diam}(G, A\pi_i), \end{aligned}$$

in which the second inequality is due to the fact that

$$(1, \ldots, g_{ij}, \ldots, 1) \in C^n(X).$$

This finishes the proof. □

4.3.1 Symmetric groups S_n and the weak conjecture

Here, our goal is to show that the symmetric group S_n satisfies the weak conjecture. First, we apply Lemma 29 to show that S_n satisfies the weak conjecture for $n \geq 7$. Then we discuss the case $n \leq 6$.

Example 11. Let A, A' be the generating sets defined in Lemma 15 and C, C' be the corresponding generating sets of S_n^k constructed in the proof of Lemma 27, for odd and even n, respectively. Note that

$$X = \bigcup_{i=1}^{k} (C\pi_i \setminus \{1\}) = \{a, b\}, \;\; X' = \bigcup_{i=1}^{k} (C'\pi_i \setminus \{1\}) = \{a', b\}.$$

Therefore, we have

$$C^k(X) = \{(1,\ldots,a,\ldots,1) : 1 \le i \le k\} \cup \{(1,\ldots,b,\ldots,1) : 1 \le i \le k\}$$
$$C^k(X') = \{(1,\ldots,a',\ldots,1) : 1 \le i \le k\} \cup \{(1,\ldots,b,\ldots,1) : 1 \le i \le k\}.$$

If n is odd, for $i = 1, 2, \ldots, k$, we have

$$(1,\ldots,a,\ldots,1) = (1,\ldots,a,b,\ldots,1)^{n+1},$$
$$(1,\ldots,b,\ldots,1) = (1,\ldots,a,b,\ldots,1)^{n}.$$

If n is even, for $i = 1, 2, \ldots, k$, we have

$$(1,\ldots,a',\ldots,1) = (1,\ldots,a',b,\ldots,1)^{n},$$
$$(1,\ldots,b,\ldots,1) = (1,\ldots,a',b,\ldots,1)^{n-1}.$$

It follows that

$$Ml_C(C^k(X)) \le n+1, \text{if } n \text{ is odd}, \tag{4.7}$$

$$Ml_{C'}(C^k(X')) \le n, \text{if } n \text{ is even}. \tag{4.8}$$

Lemma 30. *Let A, A' be the generating sets defined in Lemma 15. Then the following inequalities hold:*

$$\mathrm{diam}(S_n, A) \le (n-1)(2n-3)(n+1),$$

$$\mathrm{diam}(S_n, A') \le (n-1)(2n-3)(2n+1).$$

Proof. A simple calculation shows that, for $1 \le i \le n-1$,

$$a^{n-i+1}ba^{i-1} = (a'b)^{n-i+1}b(a'b)^{i-1} = (i, i+1).$$

Therefore, we have

$$l_A(i, i+1) \le n+1, \quad l_{A'}(i, i+1) \le 2n+1.$$

Let $(i, i+k)$ be an arbitrary transposition in S_n. Since

$$\begin{aligned}(i, i+k) \;&=\; (i, i+1)(i+1, i+2)\cdots(i+k-1, i+k)(i+k-2, i+k-1)\\ &\quad\cdots(i+1, i+2)(i, i+1),\end{aligned}$$

every transposition is a product of at most $2n-3$ transpositions of the form $(i, i+1)$. It follows that

$$l_A(i, i+k) \leq (2n-3)(n+1), \quad l_{A'}(i, i+k) \leq (2n-3)(2n+1).$$

Consider a permutation σ in S_n. Because every permutation in S_n is a product of at most $n-1$ transpositions, we have

$$Ml_A(\sigma) \leq (n-1)(2n-3)(n+1), \quad Ml_{A'}(\sigma) = (n-1)(2n-3)(2n+1).$$

The proof is complete. □

Lemma 31. *Let A and A' be the generating sets defined in Lemma 15 and C and C' be the corresponding generating sets of S_n^k constructed in the proof of Lemma 27, for odd and even n, respectively. For $n \geq 3$ and $k \geq 2$, we have*

$$\operatorname{diam}(S_n^k, C) \leq k(n-1)(2n-3)(n+1)^2,$$

provided that n is odd, and we have

$$\operatorname{diam}(S_n^k, C') \leq kn(n-1)(2n-3)(2n+1),$$

provided that n is even.

Proof. Using Lemmas 29, 30 and the inequalities (4.7),(4.8) in Example 11, we have

$$\begin{aligned}
\operatorname{diam}(S_n^k, C) &\leq Ml_C(C^k(A)) \sum_{i=1}^{k} \operatorname{diam}(S_n, A) \\
&\leq k\ Ml_C(C^k(A)) \operatorname{diam}(S_n, A) \\
&\leq k\ Ml_C(C^k(A))(n-1)(2n-3)(n+1) \\
&\leq k\ (n+1)(n-1)(2n-3)(n+1),
\end{aligned}$$

provided that n is odd. Similar arguments apply to the case where n is even, which yields the second inequality. □

Corollary 8. *The symmetric group S_n satisfies the weak conjecture for $n \geq 7$.*

Proof. We have $(n-1)(2n-3)(n+1)^2 \leq 2(n^2-1)^2 \leq 2n^4$. We induct on $n \geq 7$ to show that $2n^4 \leq n! - 2$. The inequality holds for $n = 7$. For $n > 7$, since $2(n+1)^4 = 2n^4 + 8n^3 + 12n^2 + 8n + 2 \leq 10n^4$, then the induction hypothesis gives the required conclusion. Whence, for $n \geq 7$, we have

$$(n-1)(2n-3)(n+1)^2 \leq n! - 2.$$

Also we know $n(n-1)(2n-3)(2n+1) \leq 4(n^2-1)^2 \leq 4n^4$. By induction on $n \geq 8$ we show that $4n^4 \leq n! - 2$. The inequality holds for $n = 8$. For $n > 8$, since $4(n+1)^4 = 4n^4 + 16n^3 + 24n^2 + 16n + 4 \leq 20n^4$, then the induction hypothesis gives the required conclusion. Whence, for $n \geq 8$, we have

$$n(n-1)(2n-3)(2n+1) \leq n! - 2.$$

Now the result is immediate by Lemma 31. □

Note that the symmetric group S_2 is Abelian so satisfies the weak conjecture. We show that the weak conjecture is true for the symmetric group S_n, for $n = 4, 5, 6$. Let A, A' be the generating sets defined in Lemma 15 and C, C' be the corresponding generating sets constructed in the proof of Lemma 27. We can calculate the diameter of S_n with respect to A, A' for small values of n by using a package called GRAPE in GAP. Here is the result:

$$\begin{aligned} \operatorname{diam}(S_4, A') &= 7, \\ \operatorname{diam}(S_5, A) &= 11, \\ \operatorname{diam}(S_6, A') &= 17. \end{aligned}$$

Therefore, by Lemma 29 and the inequalities (4.7), (4.8) we have

$$\begin{aligned} \operatorname{diam}(S_4^k, C') &\leq 28k \\ \operatorname{diam}(S_5^k, C) &\leq 66k \\ \operatorname{diam}(S_6^k, C') &\leq 102k. \end{aligned}$$

It follows that the symmetric group S_n satisfies the weak conjecture for $n = 5, 6$ but the above upper bound for S_4 is greater than the upper bound of the weak conjecture. We perform an alternative computation to establish the weak conjecture for S_4. By Remark 11, it suffices to show that for $1 \leq i \leq k$, the elements $(1, \ldots, g_i, \ldots, 1)$ may be presented as products of at most 22 generators in the generating set C'. Since we have

$$(1, \ldots, a', b, \ldots, 1)^2 = (1, \ldots, 1, b^2, \ldots, 1), \tag{4.9}$$
$$(1, \ldots, a', b, \ldots, 1)^4 = (1, \ldots, 1, b, \ldots, 1), \tag{4.10}$$
$$(1, \ldots, a', b, \ldots, 1)^3 = (1, \ldots, a', 1, \ldots, 1), \tag{4.11}$$

then

$$l_{C'}(1, \ldots, b^2, \ldots, 1) \leq 2, \tag{4.12}$$
$$l_{C'}(1, \ldots, b, \ldots, 1) \leq 4, \tag{4.13}$$
$$l_{C'}(1, \ldots, a', \ldots, 1) \leq 3, \tag{4.14}$$

for $1 \leq i \leq n$. On the other hand, the elements of S_4 in the generating set $\{a', b\}$ can be represented as follows:

$$\begin{aligned} S_4 =& \{a', b, a'^2, a'b, ba', b^2, a'ba', a'b^2, ba'b, b^2a', (a'b)^2, a'b^2a', (ba')^2, \\ & ba'b^2, b^2a'b, (a'b)^2a', (a'b)^2b, a'b^2a'b, ba'b^2a', b^2a'ba', (a'b)^2ba', \\ & a'b^2a'ba', ba'b^2a'b, (a'b)^2ba'\}. \end{aligned}$$

Now it is easy to check that for every $g \in S_4$ and for $1 \leq i \leq k$ the elements $(1, \ldots, g, \ldots, 1)$ can be written as a product of at most 19 generators in the generating set C' as we required.

4.3.2 Upper bound for the diameter of direct power of dihedral groups

Proposition 13. *For $n \geq 3$ and $k \geq 1$, there exists a generating set C of minimum size for D_n^k such that*

$$\operatorname{diam}(D_n^k, C) \leq \begin{cases} k(2n-2) & \text{if } n \text{ is even,} \\ \frac{n+1}{2} + (k-1)(2n-1) & \text{if } n \text{ is odd.} \end{cases} \tag{4.15}$$

Proof. According to Proposition 11 and Remark 10, it is enough to consider the case where n is odd. Let $A = \{a, b\}$ be the generating set defined in Proposition 11 and C be the associated generating set of D_n^k constructed in the proof of Lemma 27. We prove that

$$\operatorname{diam}(D_n^k, C) \leq \frac{n+1}{2} + (k-1)(2n-1).$$

Note that every rotation in D_n is a power of a and every reflection in D_n is a power of a multiplied by b. It follows that every element in D_n can be written in the form $a^r b^s$ for some $0 \leq r \leq n-1$ and $s \in \{0,1\}$. Choose an arbitrary element $(x_1, x_2, \ldots, x_k) \in D_n^k$. In view of the relations $a^i b = ba^{n-i}$ and $a^i = ba^{n-i}b$, we may write x_1 as a word of length $\leq \frac{n+1}{2}$ on A. Then there exist $y_2, y_3, \ldots, y_k \in D_n$ such that

$$(x_1, x_2, \ldots, x_k) = (x_1, y_2, \ldots, y_k)(1, y_2^{-1}x_2, y_3^{-1}x_3, \ldots, y_k^{-1}x_k),$$

and

$$l_C(x_1, y_2, \ldots, y_k) \leq \frac{n+1}{2}.$$

Write $y_i^{-1}x_i = a^{r_i}b^{s_i}$ with $0 \leq r_i \leq n-1$ and $s_i \in \{0,1\}$. By Remark 11, the proof is completed by showing that for $2 \leq i \leq k$,

$$Ml_C(1, \ldots, a^{r_i}b^{s_i}, \ldots, 1) \leq 2n-1.$$

We will do this by considering the following four cases. The case where $s_i = 0$, r_i is even:

$$\begin{aligned}&(1, \ldots, a^{r_i}b^{s_i}, \ldots, 1)\\ &= (1, \ldots, a^{r_i}, \ldots, 1) = (1, \ldots, a^{r_i}, b^{r_i}, \ldots, 1) = (1, \ldots, a, b, \ldots, 1)^{r_i}.\end{aligned}$$

Hence, we have

$$l_C(1, \ldots, a^{r_i}b^{s_i}, \ldots, 1) \leq r_i \leq n-1 \leq 2n-1.$$

The case where $s_i = 0$, r_i is odd. We have

$$\begin{aligned}&(1, \ldots, a^{r_i}b^{s_i}, \ldots, 1)\\ &= (1, \ldots, a^{r_i}, \ldots, 1) = (1, \ldots, a^{r_i+n}, b^{r_i+n}, \ldots, 1) = (1, \ldots, a, b, \ldots, 1)^{r_i+n}.\end{aligned}$$

Hence, we have

$$l_C(1, \ldots, a^{r_i}b^{s_i}, \ldots, 1) \leq r_i + n \leq 2n-1.$$

The case where $s_i = 1$, r_i is even:

$$\begin{aligned}&(1, \ldots, a^{r_i}b, \ldots, 1)\\ =&(1, \ldots, a^{r_i}, \ldots, 1)(1, \ldots, \overbrace{b}^{i\,\mathrm{th}}, \ldots, 1)\\ =&(1, \ldots, a^{r_i}, b^{r_i}, \ldots, 1)(1, \ldots, a^n, \overbrace{b^n}^{i\,\mathrm{th}}, \ldots, 1)\\ =&(1, \ldots, a, b, \ldots, 1)^{r_i}(1, \ldots, a, \overbrace{b}^{i\,\mathrm{th}}, \ldots, 1)^n.\end{aligned}$$

Hence

$$l_C(1, \dots, a^{r_i} b^{s_i}, \dots, 1) \le r_i + n \le 2n - 1.$$

It remains to consider the case where $s_i = 1$, r_i is odd. Note that

$$a^{r_i} b = b a^{n-r_i},$$

which entails

$$\begin{aligned}
(1, \dots, a^{r_i} b, \dots, 1) &= (1, \dots, b a^{n-r_i}, \dots, 1) \\
&= (1, \dots, \overbrace{b}^{i\,\text{th}}, \dots, 1)(1, \dots, a^{n-r_i}, \dots, 1) \\
&= (1, \dots, a^n, \overbrace{b^n}^{i\,\text{th}}, \dots, 1)(1, \dots, a^{n-r_i}, b^{n-r_i}, \dots, 1) \\
&= (1, \dots, a, \overbrace{b}^{i\,\text{th}}, \dots, 1)^n (1, \dots, a, \overbrace{b}^{i+1-th}, \dots, 1)^{n-r_i}.
\end{aligned}$$

Hence, we have

$$l_C(1, \dots, a^{r_i} b^{s_i}, \dots, 1) \le 2n - r_i \le 2n - 1.$$

The proof is complete. $\square$

Now the following corollary is immediate by Proposition 13.

Corollary 9. *The weak conjecture holds for D_n^k if n is even or $k \le \frac{3(n-1)}{2}$.*

4.3.3 Alternating groups and the weak conjecture

Proposition 14. *The alternating group A_4 satisfies the weak conjecture.*

Proof. As we mentioned before in Example 10, the generating set C constructed in Lemma 27 is a generating set of minimum size for A_4^n for $n \ge 2$. We show that $\operatorname{diam}(A_4^n, C) \le 10n$. Let $(g_1, g_2, \dots, g_n) \in A_4^n$. By Remark 11, it is enough to show that $l_C(1, \dots, 1, g_i, 1, \dots, 1) \le 10$, for $1 \le i \le n$. Since

$$\begin{aligned}
(1, \dots, \overbrace{\alpha}^{i\,\text{th}}, \beta, \dots, 1)^3 &= (1, \dots, \overbrace{\alpha}^{i\,\text{th}}, 1, \dots, 1), \\
(1, \dots, \alpha, \overbrace{\beta}^{i\,\text{th}}, \dots, 1)^4 &= (1, \dots, 1, \overbrace{\beta}^{i\,\text{th}}, \dots, 1), \\
(1, \dots, \alpha, \overbrace{\beta}^{i\,\text{th}}, \dots, 1)^2 &= (1, \dots, 1, \overbrace{\beta^2}^{i\,\text{th}}, \dots, 1),
\end{aligned}$$

then

$$l_C(1,\ldots,\overbrace{\alpha}^{i\,\mathrm{th}},\ldots,1) \leq 3,$$
$$l_C(1,\ldots,\overbrace{\beta}^{i\,\mathrm{th}},\ldots,1) \leq 4,$$
$$l_C(1,\ldots,\overbrace{\beta^2}^{i\,\mathrm{th}},\ldots,1) \leq 2.$$

On the other hand, the elements of A_4 can be represented over the generating set $\{\alpha, \beta\}$ as follows:

$$A_4 = \{\alpha, \beta, \alpha^2, \alpha\beta, \beta\alpha, \beta^2, \alpha\beta\alpha, \alpha\beta^2, \beta\alpha\beta = \alpha\beta^2\alpha, \beta^2\alpha, \beta^2\alpha\beta, \beta\alpha\beta^2\}.$$

Now similarly to the proof of Proposition 13 the length of $(1,\ldots,\overbrace{g}^{i\,\mathrm{th}},\ldots,1)$ in the generating set C is at most 10 for every element $g \in A_4$, which completes the proof. □

Definition 17. By an *n-basis* of a group G we mean any ordered set of n elements $x_1, x_2, \ldots, x_n$ of G which generates G. Furthermore, two n-bases $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ of G will be called *equivalent* if there exists an automorphism θ of G which transforms one into the other:

$$x_i\theta = y_i,$$

for each $i = 1, 2, \ldots, n$. Otherwise the two bases will be called *non-equivalent.*

Example 12. We show that the weak conjecture is true for A_5^k for $k = 2, 3, 4$.

Proof. Let $a = (1\ 2)(3\ 4), b = (1\ 2\ 3\ 4\ 5)$. It is easy to see that the pairs

$$(a, b), (b, a), (a, b^2), (b^2, a)$$

are four non-equivalent 2-basis of A_5. Using Corollary 7 we build generating sets of size two for A_5^k, $k = 2, 3, 4$. The result is as follows. Let

$$C_1 = \{a, b\},$$
$$C_2 = \{(a, a), (b, b^2)\},$$
$$C_3 = \{(a, b, a), (b, a, b^2)\},$$
$$C_4 = \{(a, b, a, b^2), (b, a, b^2, a)\}.$$

Then the sets C_1, C_2, C_3 and C_4 are generating sets of minimum size for the groups A_5, A_5^2, A_5^3 and A_5^4, respectively. Using GAP we check that $\mathrm{diam}(A_5, C_1) = 10$ and $\mathrm{diam}(A_5^2, C_2) = 18$. Let (x, y, z) be an arbitrary element in A_5^3. Since $(x, z) \in A_5^2 = \langle (a, a), (b, b^2) \rangle$, there exists a word w representing (x, z) over the generating set C_2 of length at most 18. Hence, $(x, y, z) = (w_1, \bar{w}, w_2)(1, \bar{w}^{-1}y, 1)$, where w_1, w_2 are the first and second components of $w = (x, z)$, respectively. The word $\bar{w}$ is a word in the alphabet a, b corresponding to the word w, in which the pairs $(a, a), (b, b^2)$ are substituted by b, a, respectively. It follows that

$$l_{C_3}(x, y, z) \leq l_{C_3}(w_1, \bar{w}, w_2) + l_{C_3}(1, \bar{w}^{-1}y, 1).$$

It is clear that

$$l_{C_3}(w_1, \bar{w}, w_2) \leq 18.$$

On the other hand, $l_{C_3}(1, \bar{w}^{-1}y, 1) \leq 60$, since

$$\mathrm{diam}(A_5, C_1) = 10,\ (1, b, 1) = (a, b, a)^6,\ (1, a, 1) = (b, a, b^2)^5.$$

Therefore $l_{C_3}(x, y, z) \leq 18 + 60 = 78$, which implies $\mathrm{diam}(A_5^3, C_3) \leq 78$.

Let $(x, y, z, w) \in A_5^4$. Consider the factorization

$$(x, y, z, w) = (x, 1, z, 1)(1, y, 1, w)$$

and the equalities

$$\begin{gathered}(1, b, 1, b^2) = (a, b, a, b^2)^6,\ (a, 1, a, 1) = (a, b, a, b^2)^5,\\ (1, a, 1, a) = (b, a, b^2, a)^5,\ (b, 1, b^2, 1) = ((b, a, b^2, a)^6.\end{gathered}$$

This leads to the following inequalities,

$$\begin{aligned} l_{C_4}(x, y, z, w) &\leq l_{C_4}(x, 1, z, 1) + l_{C_4}(1, y, 1, w) \\ &\leq \mathrm{diam}(A_5^2, C_2) M l_{C_4}\{(a, 1, a, 1), (b, 1, b^2, 1)\} \\ &+ \mathrm{diam}(A_5^2, C_2) M l_{C_4}\{(1, a, 1, a), (1, b, 1, b^2)\} \\ &\leq 18 \times 6 + 18 \times 6 = 216, \end{aligned}$$

which gives $\mathrm{diam}(A_5^4, C_4) \leq 216$. $\square$

4.3.4 Upper bounds for the diameter of a direct power of a solvable group

Despite our attempts to establish the strong conjecture and the weak conjecture for solvable groups, we could not do it yet. In this section we will present two upper bounds for the diameter of G^n, where G is a solvable group. Although these upper bounds do not coincide with the proposed upper bound in the conjectures, they grow polynomially with respect to n. Since solvable groups have a derived series of finite length our strategy is to find a relation between the diameter of a solvable group and the diameter of its derived subgroup. For this we need to establish a relation between the generating sets of the group and the generating sets of its subgroups. The following lemma, well known as *Schreier Lemma*, gives a generating set for a subgroup of a group with respect to a generating set of the whole group. The generators of the subgroup are usually called Schreier generators. Using Schreier generators we derive a relation between the diameter of a group and the diameter of its subgroup.

Definition 18. Let H be a subgroup of a group G. By a right transversal for G mod H, we mean a subset of G which intersects every right coset Hg in exactly one element.

Remark 12. Let G be a finite group with a generating set X and a normal subgroup H. It is easy to see that the set $HX = \{Hx : \ x \in X\}$ is a generating set of G/H. Given an arbitrary element $Hg \in G/H$, Hg can be written as a product of at most $D(G/H)$ elements in HX. Hence, there exist $x_1, x_2, \dots, x_{D(G/H)} \in X$ such that $Hg = Hx_1Hx_2H \dots Hx_{D(G/H)} = Hx_1x_2 \dots x_{D(G/H)}$. It shows that there always exists a right transversal T for G mod H such that

$$Ml_X(T) \leq D(G/H), \ 1 \in T.$$

Lemma 32. [26] *Let $H \leq G = \langle X \rangle$ and let T be a right transversal for G mod H, with $1 \in T$. Then the set*

$$\{txt_1^{-1} \mid t, t_1 \in T, x \in X, txt_1^{-1} \in H\}$$

generates H.

Using Schreier's Lemma leads to the following observations which we are going to apply for establishing the main result. The first one is [3, Lemma 5.1].

Lemma 33. *If $1 \neq N$, $N \triangleleft G$, then the following inequalities hold:*

$$D^s(G) \leq 2D^s(G/N)\, D^s(N) + D^s(G/N) + D^s(N) \leq 4D^s(G/N)\, D^s(N).$$

Here we prove the non symmetric version of Lemma 33.

Lemma 34. *Let G be a finite group with a generating set X and a normal subgroup H. Let T be a right transversal of G/H such that*

$$Ml_X(T) \leq D(G/H),\ 1 \in T.$$

The following inequality holds:

$$\operatorname{diam}(G, X) \leq D(G/H) + (D(G/H) + 1 + Ml_X(\{t^{-1} \mid t \in T\}))D(H).$$

Furthermore, we have

$$D(G^n) \leq D(G^n/H^n) + (1 + |G|D(G^n/H^n))D(H^n).$$

Proof. Given $g \in G$, we have $g = ht$ for some $h \in H$ and $t \in T$. Hence

$$l_X(g) \leq l_X(t) + l_X(h).$$

Since $Ml_X(T) \leq D(G/H)$, then $l_X(g) \leq D(G/H) + l_X(h)$. Using Lemma 32 we get $l_X(h) \leq (D(G/H) + 1 + Ml_X(\{t^{-1} \mid t \in T\}))D(H)$. Combining these two facts gives the upper bound in the first inequality. Now we prove the second statement. Let X' be a generating set of G^n and let T' be a right transversal of G^n/H^n such that

$$Ml_{X'}(T') \leq D(G^n/H^n).$$

Proceeding as above for the case $n = 1$, it suffices to show that

$$Ml_{X'}(\{t^{-1} \mid t \in T'\}) \leq (|G| - 1)D(G^n/H^n).$$

For given $t \in T'$ we have

$$l_{X'}(t) \leq D(G^n/H^n).$$

Since

$$t^{-1} = t^{o(t)-1},$$

then we obtain

$$l_{X'}(t^{-1}) \leq (o(t)-1)l_{X'}(t).$$

Hence, we have

$$l_{X'}(t^{-1}) \leq (|G|-1)D(G^n/H^n),$$

since

$$o(g) \leq |G|,$$

for every element $g \in G^n$. The proof is complete. □

Now we are ready to present two upper bounds for the diameter of a direct power of a solvable group. First we need to prove the following elementary observation.

The following corollary is straightforward by using Lemma 34.

Corollary 10. *Let G be a non Abelian solvable group. Let*

$$\{1\} = G^{(l)} \lhd G^{(l-1)} \lhd \ldots \lhd G'' \lhd G' \lhd G$$

be the derived series of G. The following inequality holds:

$$D(G^n) \leq n^l |G| \prod_{i=0}^{l-2} (|G^{(i)}|+1).$$

Proof. For $n=1$ it is obvious. Let $n \geq 2$. Since $(G^k)' = (G')^k$ for $k \geq 1$, then the derived series of G^n is

$$\{1\} = (G^{(l)})^n \lhd (G^{(l-1)})^n \lhd \ldots \lhd (G'')^n \lhd (G')^n \lhd G^n. \tag{4.16}$$

Applying Lemma 34 to the group G^n with the subgroup $(G')^n$ gives

$$\begin{aligned} D(G^n) &\leq D(G^n/(G')^n) + (1+|G|D(G^n/(G')^n)D((G')^n) \\ &= D(G^n/(G')^n) + D((G')^n) + |G|D(G^n/(G')^n)D((G')^n) \\ &\leq D(G^n/(G')^n)D((G')^n) + |G|D(G^n/(G')^n)D((G')^n) \\ &= D(G^n/(G')^n)D((G')^n)(1+|G|), \end{aligned}$$

the second inequality follows from the fact that $D(G^n/(G')^n), D((G')^n) > 1$ and this is because the quotient group G/G' and the commutator subgroup

G' are not trivial and $n \geq 2$. By repeating the process for the other subgroups in the series (4.16) we have

$$D(G^n) \leq D(G^n/(G')^n)D((G')^n/(G'')^n)\dots D((G^{(l-1)})^n)\prod_{i=0}^{l-2}(|G^{(i)}|+1). \tag{4.17}$$

Since for every group G with a normal subgroup H we have $G^n/H^n \cong (G/H)^n$, then

$$D(G^n) \leq D((G/G')^n)D((G'/G'')^n)\dots D((G^{(l-1)})^n)\prod_{i=0}^{l-2}(|G^{(i)}|+1). \tag{4.18}$$

Since all the quotient groups in the inequality (4.18) and the group $G^{(l-1)}$ are Abelian by Corollary 4 we get

$$\begin{aligned} D(G^n) &\leq n^l D(G/G')D(G'/G'')\cdots \\ &\quad D(G^{(l-2)}/G^{(l-1)})D((G^{(l-1)})\prod_{i=0}^{l-2}(|G^{(i)}|+1) \\ &\leq n^l|G/G'||G'/G''|\cdots|G^{(l-2)}/G^{(l-1)}||G^{(l-1)}|\prod_{i=0}^{l-2}(|G^{(i)}|+1) \\ &= n^l|G|\prod_{i=0}^{l-2}(|G^{(i)}|+1). \end{aligned}$$

□

For finding the second upper bound we start by presenting an upper bound for the symmetric diameter of a direct power of a solvable group and then we apply this to find an upper bound for the diameter of such a group.

Proposition 15. *If G is a solvable group then*

$$D^s(G^n) \leq 4^{l-1}n^l\,|G|,$$

where l is the length of the derived series of G.

Proof. Let

$$\{1\} = G^{(l)} \triangleleft G^{(l-1)} \triangleleft \cdots \triangleleft G'' \triangleleft G' \triangleleft G$$

be the derived series of the group G. Since for $1 \leq i \leq l$ we have

$$(G^{(i)})^n = (G^n)^{(i)},$$

the series

$$\{1\} = (G^{(l)})^n \lhd (G^{(l-1)})^n \lhd \cdots \lhd (G'')^n \lhd (G')^n \lhd G^n$$

is the derived series of the group G^n. Using the second inequality in Lemma 33, the maximum of the diameter of the group G^n is bounded above by

$$4^{l-1}\, D^s(G^n/(G')^n)\, D^s((G')^n/(G'')^n) \cdots D^s((G^{(l-2)})^n/(G^{(l-1)})^n)\, D^s((G^{(l-1)})^n). \tag{4.19}$$

Whereas, for $0 \le i \le l-2$ we have

$$(G^{(i)})^n/(G^{(i+1)})^n \cong (G^{(i)}/G^{(i+1)})^n$$

and the factors in a derived series are Abelian, by Corollary 4 we get

$$D^s(G^{(i)})^n/(G^{(i+1)})^n \le n\,|G^{(i)}/G^{(i+1)}| = n\,|G^{(i)}|/|G^{(i+1)}| \tag{4.20}$$

for $0 \le i \le l-2$ and

$$D^s((G^{(l-1)})^n) \le n\,|G^{(l-1)}|. \tag{4.21}$$

Substituting the inequalities (4.20) and (4.21) in (4.19), we get

$$D^s(G^n) \le 4^{l-1} n^l\,|G|,$$

which is the desired conclusion. $\square$

We apply the following Lemma to give an upper bound for the diameter by using the symmetric diameter.

Lemma 35. *Let G be a finite group and X be a set of generators. The diameter and the symmetric diameter are related as follows:*

$$\operatorname{diam}(G, X) \le 2(\operatorname{diam}^s(G, X) + 1)(|X| + 1)\ln|G|.$$

Proof. See [2, Corollary 2.2]. $\square$

Corollary 11. *Let G be a solvable group of derived length l and let A be a generating set of G^n of minimum size. Set* $\operatorname{rank}(G) = \alpha$, $\operatorname{rank}(G/G') = \beta$. *The following inequality holds,*

$$\mathrm{diam}(G^n, A) \le 2(4^{l-1}n^l\,|G| + 1)(n\beta + 1)n \ln |G|,$$

for $n \ge \alpha/\beta$. *In particular, if* G *is a* p*-group, then*

$$D(G^n) \le 2(4^{l-1}n^l\,|G| + 1)(n\beta + 1)n \ln |G|,$$

for $n \ge 1$.

Proof. By Lemma 35 we have,

$$\mathrm{diam}(G^n, A) \le 2(\mathrm{diam}^s(G^n, A) + 1)(|A| + 1)n \ln |G|.$$

In addition, $\mathrm{diam}^s(G^n, A) \le D^s(G^n)$ by definition. Now by using Proposition 15 and Theorem 7 we get the desired conclusion. The second statement follows from these two facts: First, if G is a p-group then every minimal generating set is a generating set of minimum size, which follows from the Burnside's Basis Theorem [10]. Second, by Corollary 5, if G is a nilpotent group (note that every p-group is nilpotent) then $\mathrm{rank}(G) = \mathrm{rank}(G/G')$. $\square$

As an example of a non Abelian solvable group which is also a 2-group we verify the *quaternion group* Q_8. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group in which

$$i^2 = j^2 = k^2 = -1$$

and

$$ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j.$$

We have $Q_8' \cong Z_2$ and $Q_8/Q_8' \cong Z_2 \times Z_2$. The length of the derived series of Q_8 is 2. Hence, $l = 2$ and $\beta = \mathrm{rank}(Z_2 \times Z_2) = 2$ in the notations of corollaries 10,11. Therefore we have

$$D(Q_8^n) \le 72n^2$$

by Corollary 10 and

$$D(Q_8^n) \le 2n(32n^2 + 1)(2n + 1)ln(8)$$

by Corollary 11.

We now present another upper bound for the diameter of the direct power of the quaternion group Q_8 in the following example.

Example 13. For $n \ge 1$ we have $D(Q_8^n) \le 8n^2 + 3n$.

Proof. Consider the normal subgroup $H = \{1, -1\}$. Let X be a generating set of Q_8^n. We have $H^n \triangleleft Q_8^n$. Let T be a right transversal of Q_8^n mod H^n such that

$$1 \in T, Ml_X(T \setminus \{1\}) \leq D(Q_8^n/H^n).$$

Using Lemma 34 we have

$$\mathrm{diam}(Q_8^n, X) \leq D(Q_8^n/H^n) + (D(Q_8^n/H^n) + 1 + Ml_X(\{t^{-1} \mid t \in T\}))D(H^n).$$

On the other hand, since $H \cong Z_2$, $Q_8/H \cong Z_2 \times Z_2$, we have

$$\mathrm{diam}(Q_8^n, X) \leq 2n + (2n + 1 + Ml_X(\{t^{-1} \mid t \in T\})n. \tag{4.22}$$

Since for every $g \in Q_8^n$, $g^4 = 1$, for every $t \in T$, $t^{-1} = t^3$. Hence, the following inequality holds:

$$l_X(t^{-1}) \leq 3l_X(t) \leq 3D(Q_8^n/H^n) \leq 6n.$$

Substituting $6n$ for $Ml_X(\{t^{-1}|t \in T\}$ in (4.22) we get

$$D(Q_8^n) \leq 8n^2 + 3n. \quad \square$$

Chapter 5

Final remarks

We collect here plenty of questions which remain open:

Question 1. *In Lemma 4 we have just found an upper bound for $M'(S)$ where S is a completely regular semigroup. When does equality hold? What may we say for the other depth parameters?*

Question 2. *Theorem 1 gives a lower bound for $N'(S)$ where S is a finite transformation semigroup. Similarly, it would be nice to find an upper bound for $M(S)$ where S is a finite transformation semigroup.*

Question 3. *In Corollary 3 the parameters N and N' are computed for the transformation semigroups T_n, PT_n and I_n. What can we say about M, M' for them?*

Question 4. *The equalities $N = N'$ and $M = M'$ hold in all the semigroups which we have verified. Is there any example of a semigroup for which $N' < N$ and $M < M'$?*

Question 5. *In Section 3.1 we estimate the depth parameters for the families of transformation semigroups whose rank has been determined already in the literature. Other natural candidates who may be easy to verify are the semigroups SP_n, SPO_n or semigroups of orientation preserving transformations such as POP_n, OP_n or $POPI_n$.*

Question 6. *We have established upper bounds for $N(S)$ where S is a direct product or wreath product of two finite monoids. It would be interesting to obtain analogous results for the other depth parameters.*

Question 7. *Give examples to show that the inequalities in Theorems 2, 3 and 4 may not be improved.*

Question 8. *Prove or disprove the weak conjecture for dihedral groups and alternating groups.*

Question 9. *Improve the upper bounds in Corollaries 10 and 11 for solvable groups.*

And a very general question is

Question 10. *Prove or disprove the weak conjecture and the strong conjecture.*

Bibliography

[1] Jorge Almeida, *Finite semigroups and universal algebra*, Series in Algebra, vol. 3, World Scientific Publishing Co., Inc., River Edge, NJ, 1994, Translated from the 1992 Portuguese original and revised by the author. MR 1331143 (96b:20069) (Cited on page 7.)

[2] László Babai, *On the diameter of Eulerian orientations of graphs*, Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithms (New York), ACM, 2006, pp. 822–831. MR 2368881 (Cited on page 71.)

[3] László Babai and Ákos Seress, *On the diameter of permutation groups*, European J. Combin. **13** (1992), no. 4, 231–243. MR 1179520 (93h:20001) (Cited on page 67.)

[4] John Bamberg, Nick Gill, Thomas P. Hayes, Harald A. Helfgott, Ákos Seress, and Pablo Spiga, *Bounds on the diameter of Cayley graphs of the symmetric group*, J. Algebraic Combin. **40** (2014), no. 1, 1–22. MR 3226815 (Cited on page 3.)

[5] Ján Černý, *A remark on homogeneous experiments with finite automata*, Mat.-Fyz. Časopis Sloven. Akad. Vied **14** (1964), 208–216. MR 0168429 (29 #5692) (Cited on pages 2 and 10.)

[6] V. H. Fernandes, *The monoid of all injective order preserving partial transformations on a finite chain*, Semigroup Forum **62** (2001), no. 2, 178–204. MR 1831507 (2002a:20075) (Cited on pages 3, 8, 20, and 25.)

[7] G. U. Garba, *Idempotents in partial transformation semigroups*, Proc. Roy. Soc. Edinburgh Sect. A **116** (1990), no. 3-4, 359–366. MR 1084739 (92c:20123) (Cited on pages 3, 8, 20, and 26.)

[8] M. S. Gomes and J. M. Howie, *On the ranks of certain finite semigroups of transformations*, Math. Proc. Cambridge Philos. Soc. **101** (1987), no. 3, 395–403. MR 878889 (88e:20057) (Cited on pages 3, 8, and 23.)

[9] ———, *On the ranks of certain semigroups of order-preserving transformations*, Semigroup Forum **45** (1992), no. 3, 272–282. MR 1179851 (93h:20070) (Cited on pages 3, 8, 20, 24, and 25.)

[10] Marshall Hall, Jr., *The theory of groups*, Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition. MR 0414669 (54 #2765) (Cited on page 72.)

[11] P. Hall, *The eulerian functions of a group*, Quart. J. Math. (Oxford) **7** (1936), 134–151. (Cited on pages 4 and 55.)

[12] P. M. Higgins, *Techniques of semigroup theory*, Oxford University Press, New York, 1992. (Cited on page 17.)

[13] J. Howie and B. McFadden, *Idempotent rank in finite full transformation semigroups*, Royal Soc. (Edinburgh), no. 114, 1990, pp. 161–167. (Cited on pages 3, 8, 20, and 26.)

[14] J. M. Howie, *The subsemigroup generated by the idempotents of a full transformation semigroup*, J. London Math. Soc. 41 (1966), 707–716. (Cited on pages 3, 8, and 20.)

[15] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York-Berlin, 1980, Reprint of the 1974 original. MR 600654 (82a:00006) (Cited on page 36.)

[16] J. Kari, *A counter example to a conjecture concerning synchronizing words in finite automata*, Bull. Eur. Assoc. Theor. Comput. Sci. EATCS (2001), no. 73, 146. MR 1835978 (Cited on pages 2 and 11.)

[17] Benjamin Klopsch and Vsevolod F. Lev, *How long does it take to generate a group?*, J. Algebra **261** (2003), no. 1, 145–171. MR 1967159 (2004e:20093) (Cited on page 49.)

[18] ———, *Generating abelian groups by addition only*, Forum Math. **21** (2009), no. 1, 23–41. MR 2494883 (2010c:20068) (Cited on pages 49 and 51.)

[19] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory: presentations of groups in terms of generators and relations*, Dover publications, INC, New York, 1976. (Cited on page 53.)

[20] D. Meier and J. Wiegold, *Growth sequences of finite groups. V*, J. Austral. Math. Soc. Ser. A **31** (1981), no. 3, 374–375. MR 633445 (82i:20041b) (Cited on page 48.)

[21] J. E. Pin, *Le problème de la synchronisation et la conjecture de Černý*, Noncommutative structures in algebra and geometric combinatorics (Naples, 1978), Quad. "Ricerca Sci.", vol. 109, CNR, pp. 37–48. (Cited on pages 2 and 10.)

[22] ______, *Varieties of formal languages*, North Oxford, London and Plenum, New York, 1986. (Cited on pages 5, 6, 14, and 30.)

[23] John Rhodes and Benjamin Steinberg, *The q-theory of finite semigroups*, Springer Monographs in Mathematics, Springer, New York, 2009. MR 2472427 (2010h:20132) (Cited on pages 2, 8, and 39.)

[24] E. F. Robertson, N. Ruškuc, and M. R. Thomson, *Finite generation and presentability of wreath products of monoids*, J. Algebra **266** (2003), no. 2, 382–392. MR 1995120 (2004f:20098) (Cited on page 3.)

[25] I. C. Rystsov, *On the rank of a finite automaton*, Kibernet. Sistem. Anal. (1992), no. 3, 3–10, 187. MR 1190855 (93h:68097) (Cited on pages 10 and 11.)

[26] Ákos Seress, *Permutation group algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003. MR 1970241 (2004c:20008) (Cited on page 67.)

[27] J. Wiegold, *Growth sequences of finite groups*, J. Austral. Math. Soc. 17 (1974), 133–141. (Cited on pages 4, 48, 52, and 55.)

[28] ______, *Growth sequences of finite groups. II*, J. Austral. Math. Soc. **20** (1975), no. part 2, 225–229. MR 0376856 (51 #13031) (Cited on pages 4, 48, and 56.)

[29] ______, *Growth sequences of finite groups. III*, J. Austral. Math. Soc. Ser. A **25** (1978), no. 2, 142–144. MR 499355 (80c:20028) (Cited on pages 4 and 48.)

[30] ———, *Growth sequences of finite groups. IV*, J. Austral. Math. Soc. Ser. A **29** (1980), no. 1, 14–16. MR 566271 (82i:20041a) (Cited on pages 4 and 48.)

[31] ———, *Growth sequences of finite semigroups*, J. Austral. Math. Soc. (Ser.A) 43 (1987), 16–20. (Cited on pages 4 and 42.)

[32] John S. Wilson, *On the growth of residually soluble groups*, J. London Math. Soc. (2) **71** (2005), no. 1, 121–132. MR 2108251 (2006a:20069) (Cited on pages 48 and 49.)

Index

0-simple, 14
A- depth, vi, 1
A-depth, 6
n-basis, 65
    equivalent, 65
    non-equivalent, 65
Černý conjecture, 10

automaton
    synchronizing, 10

Cayley graph, 11

depth parameters, 6
diameter
    graph, 12
    group, 11
directed Cayley graph, 12

finite automaton, 10

generating set, 5
    canonical generating set, 52
    minimal generating set, 5
group
    dihedral group, 54
    perfect group, 53
    quaternion, 72
group of units, 39

ideal, 5
    minimum ideal, 5
in-degree, 8
irreducible
    D-class, 17
    element, 7

kernel, 5

length
    of elements, 6

order preserving, 9
out-degree, 8

partially ordered set, 7
    diagram, 7
Pin comjecture, 10
product
    semidirect product, 39
    wreath product, 39

rank
    of finite automaton, 10
    of mapping, 10
    of semigroup, 5

Schreier
    generators, 67
    Lemma, 67
semigroup, 5
    monogenic semigroup, 7

transition semigroup, 10
semilattice, 7
strongly connected, 12
subsemigroup, 5
symmetric diameter, 3, 11
symmetric length, 11

word
input word, 10
reset word, 10
terminal word, 10

Notation

(X, S), 8
$(X, S) \wr (Y, T)$, 39
$(s)_y$, 39
$C^n(A)$, 52
$C_{i,n}$, 7
$D(G)$, 11
$D^s(G)$, 11
G', 52
$I(S)$, 7
I_n, 9
J_M, 29
$L(n, r)$, 9
$M'(S)$, 6
$M(S)$, 6
$Ml_A(T)$, 6
$N'(S)$, 6
$N(S)$, 6
$N(S, A)$, 6
O_n, 9
POI_n, 9
PO_n, 9
Q_8, 72
$S^Y \rtimes T$, 39
T_n, 9
U_S, 39
X_n, 8
$\mathrm{Cay}(G, A)$, 11
$\bar{1}$, 39
$\mathrm{d}^{\mathrm{in}}(v)$, 8
$\mathrm{d}^{\mathrm{out}}(v)$, 8
$\mathrm{diam}_{min}(G)$, 43
ℓ_J, 29
$\ker(S)$, 5
$\langle A \rangle$, 5
$\lceil k \rceil$, 19
$\lfloor n \rfloor$, 49
$\mathbb{N}$, 8
$\mathrm{IRD}(S)$, 17
$\mathrm{ord}(g)$, 54
$\overrightarrow{\mathrm{Cay}}(G, A)$, 12
$\prod_{i=1}^{n} s_i$, 39
$\mathrm{rank}(S)$, 5
${}^t f$, 39
h_J, 29
$k'(n, r)$, 9
$k(n, r)$, 9
$l_A^s(g)$, 11
$l_A(s)$, 6
$ml_A(T)$, 6
$r(S)$, 18
$r(S, A)$, 17
r_J, 29
$t(S)$, 17
PT_n, 8