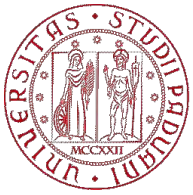

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO MATEMATICA
DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI–CIVITA"
Corso di Laurea Magistrale in Matematica

MASTER'S DEGREE THESIS

Generating sequences of finite groups

Candidate:
Emanuele Di Bella

Supervisor:
Chiar.mo Prof. Andrea Lucchini

Academic year 2021-2022

Contents

Introduction

This thesis deals with finite groups and the study of some generation properties. In particular, one has that a set S is a generating set for a finite group G if $\langle S \rangle = G$ and, if we suppose that S does not contain generating subsets, then we say S is irredundant or minimal. In recent decades, researchers focused on studying properties of minimal generating sets, for example its maximal and minimal size, which are denoted by $m(G)$ and $d(G)$, respectively.
At the beginning, it is necessary to cite the most remarkable result about the existence of generating sets: indeed, for any integer k such that $d(G) \leq k \leq m(G)$, Tarski's Theorem guarantees the existence of a minimal generating set of size k.
After that, we should mention a significant purpose about the study of generating sets, which is the computation of $m(G)$. Actually, the most relevant results are about symmetric and alternating group ($m(S_n) = n - 1$ and $m(A_n) = n - 2$, [13]) and about projective special linear groups ($m(PSL_2(p))$ was computed for p prime and it was given an upper bound for p a prime-power, [14]).
Chapter 1 focuses on irredundant generating sequences, i.e. sequences of elements of a finite group G which are generating but do not contain generating subsequences. In particular, we aim to show a formula that computes the exact number of irredundant generating sequences; to do this, we use the Möbius function, which is a function on a partially ordered set with a manageable recursive definition; it is often used and has many applications in Number Theory. Thanks to Möbius function (defined on the lattice of subgroups of a finite group) and the related Möbius inversion theorem, together with a tricky construction that is described step by step, we are able to give an elegant proof of the formula; then, we want to show how the formula can be applied to the most common finite groups and what are the most significant implications. For this purpose we make an intense use of GAP, describing in details the implementation of the formula.
Chapter 2 examines sequences composed of subgroups of a finite group G, requiring that the subgroups belong to a fixed family of finite groups. Similarly as for sequences of elements, we are interested in the computation of the maximal size of a generating sequence of subgroups, we aim to show a formula for the computation of the exact number of such sequences and we are able to prove an existence theorem similar to Tarski's one. However, we will see that the results listed above are not true in general but only under certain assumptions. In particular, we wish to put in evidence a strong dependence on the choice of the initial fixed family of finite groups. We mostly study generating sequences when the choice of the family of finite groups is one of the following: family containing all cyclic groups, family containing all solvable groups and family containing cyclic groups only of prime-power order. It is clear that these are strong assumptions and we provide many examples to show how things can

be challenging when one tries to relax some of those. For the reasons explained above, one can imagine how much the study of sequences of subgroups can be diversified, consequently this can be also interesting for future researches (in this regard we will put in evidence some open problems concerning this topic).
We conclude the thesis with some insights related to the study of the probability to generate a finite group. Specifically, we would like to consider not only the probability to generate with elements, but also with subgroups, as in Chapter 2. Then we compare the expected number of elements to generate a finite group with the expected number of subgroups to generate it (again, we assume the subgroups belong to a fixed family of finite groups), providing suitable examples.

Chapter 1

Irredundant generating sequences

1.1 First definitions and Tarski's theorem

Let G be a finite group.

Definition 1.1. A generating sequence of G is a sequence $(g_1, \ldots, g_n)$ such that $\langle g_1, \ldots, g_n \rangle = G$.

Definition 1.2. A generating sequence $(g_1, \ldots, g_n)$ is irredundant if no proper subsequence generates G, and is redundant otherwise.

Definition 1.3. We say:

(i) $m(G)$ is the largest size of an irredundant generating sequence of G;

(ii) $i(G)$ is the largest size of any irredundant sequence of G;

(iii) $d(G)$ is the smallest size of a generating sequence of G. Observe that the fact that there are no generating sequences of length smaller than $d(G)$ means that there are no sequences of length $d(G)$ with a generating proper subsequence, i.e. $d(G)$ is also the smallest size of an irredundant generating sequence of G.

We have $d(G) \leq m(G) \leq i(G)$.

Definition 1.4. We denote by $\Gamma_n(G)$ the set of all length-n generating sequences of G and with $\Gamma_n^*(G)$ the set of all lenght-n sequences of G. Moreover, $\varphi_n(G) := |\Gamma_n(G)|$, i.e. $\varphi_n(G)$ is the number of length-n generating sequences.

Now fix a positive integer n and denote by $\varphi_n^n(G)$ the number of irredundant generating sequences in G of length n. The aim of this chapter is to compute $\varphi_n^n(G)$.

At first, observe that $\varphi_n^n(G) = 0$ when $n < d(G)$. If $n = d(G)$ we reduce to $\varphi_n^n(G) = \varphi_n(G) > 0$ thanks to the observation in Definition 1.3(iii). If $n = m(G)$ we have $\varphi_n^n(G) > 0$ just by definition of $m(G)$, and for the same reason $\varphi_n^n(G) = 0$ if $n > m(G)$. We are left to check what happens when $d(G) < n < m(G)$. In particular, we know that in this case $\varphi_n^n(G) > 0$ thanks to the following result by Tarski:

Theorem 1.1 (Tarski)**.** If $d(G) \leq n \leq m(G)$ then G has an irredundant generating sequence of length n.

Proof. Clearly, we can suppose $m(G) - d(G) \geq 2$. Fix t such that $d(G) < t \leq m(G)$ and such that there is an irredundant generating sequence $s = (g_1, \ldots, g_t)$ (for sure we can do this for $t = m(G)$). Since s is generating, every $g \in G$ can be expressed as a word of length $l(g)$ composed of elements of s. Say $\mathcal{A}$ the family of irredundant generating sequences of G with length smaller than t. For any sequence $a \in \mathcal{A}$, set $\delta(a) = \max_{g \in a} l(g)$, $\nu(a) = |\{g \in a \mid l(g) = \delta(a)\}|$. Fix $a = (a_1, \ldots, a_u) \in \mathcal{A}$ ($\Longrightarrow u < t$) minimizing $\delta(a)$ and $\nu(a)$, and fix $i \in \{1, \ldots, u\}$ such that $l(a_i) = \delta(a)$, in particular we get $a_i = b_1 b_2$ with $l(b_1), l(b_2) < l(a_i)$. The sequence $(a_1, \ldots, a_{i-1}, b_1, b_2, a_{i+1}, \ldots, a_u)$ is clearly a generating sequence, hence we can fix an irredundant generating subsequence a^*. By construction, $\delta(a^*) \leq \delta(a)$ and if equality holds we have $\nu(a^*) < \nu(a)$ by our choice of a_i. In particular, we get $a^* \notin \mathcal{A}$ (by the minimazing condition on a), i.e. the length of a^* is larger or equal than t. But we also have that the length of a^* is smaller or equal than $u + 1 \leq t$, hence the only possibility is that equality holds, obtaining $u = t - 1$. In particular a is an irredundant generating sequence of length $t - 1$. Obviously we can repeat this construction until $t = d(G) + 2$ and the theorem is proved. □

1.2 Möbius function and Hall's formula

From now on, our purpose is to compute the exact number of irredundant generating sequences. We start with the well-known construction by Möbius on partially-ordered sets.

Let P be a finite poset. We can define a map $\mu_P : P \times P \to \mathbb{Z}$ such that:

$$\mu_P(a, b) = 0 \text{ if } a > b$$

$$\mu_P(b, b) = 1$$

$$\sum_{a \leq c \leq b} \mu_P(c, b) = 0 \text{ if } a < b$$

Theorem 1.2 (Möbius inversion)**.** Let f be a function from a poset P into an additive abelian group. For a fixed $a \in P$ define

$$F(b) = \sum_{a \leq x \leq b} f(x).$$

Then, for $b \geq a$, we have

$$f(b) = \sum_{a \leq x \leq b} \mu_P(x,b) F(x).$$

Proof. For a fixed element $b \geq a$, we have

$$\sum_{a \leq x \leq b} \mu_P(x,b) F(x) = \sum_{a \leq x \leq b} \mu_P(x,b) \left(\sum_{a \leq y \leq x} f(y) \right) =$$

$$= \sum_{a \leq x \leq b} \sum_{a \leq y \leq x} \mu_P(x,b) f(y) = \sum_{a \leq y \leq x \leq b} \mu_P(x,b) f(y) =$$

$$= \sum_{a \leq y \leq b} \sum_{y \leq x \leq b} f(y) \mu_P(x,b) = \sum_{a \leq y \leq b} f(y) \left(\sum_{y \leq x \leq b} \mu_P(x,b) \right).$$

Now observe that $\sum_{y \leq x \leq b} \mu_P(x,b) = 1$ if and only if $y = b$, and is zero otherwise. Hence

$$\sum_{a \leq y \leq b} f(y) \left(\sum_{y \leq x \leq b} \mu_P(x,b) \right) = f(b)$$

and the proof is concluded. □

Consider now the lattice $\mathcal{G}$ of the subgroups of a finite group G. This is a poset with a larger element, G, hence we can define the Möbius function μ_G in the following way:

$$\mu_G(H) := \mu_{\mathcal{G}}(H, G)$$

for any subgroup H, and by the above construction, we get

$$\mu_G(G) = 1$$

$$\sum_{H \leq K \leq G} \mu_G(K) = 0 \text{ if } H < G$$

Observe that the function $\psi(H) := \sum_{K \leq H} \varphi_n(K)$ satisfies the assumptions of Theorem 1.2 and since $\varphi_n(G)$ is the number of length-n generating sequences, we just have $\psi(H) = \sum_{K \leq H} \varphi(K) = |H|^n$ and we get the Hall's formula

$$\varphi_n(G) = \sum_{H \leq G} \mu_G(H) |H|^n.$$

1.3 Counting irredundant generating sequences

In this section our goal is to show a formula to compute the exact number of irredundant generating sequences.

Definition 1.5. We say that a generating sequence $(g_1, \dots, g_n)$ has irredundancy rank k if it has a subsequence of length k that generates G but no such subsequence of length $k-1$. Moreover, let $\varphi_n^k(G)$ denote the number of generating sequences of G of length n and irredundancy rank k, and similarly let $\varphi_n^{\leq k}(G)$ denote the number of generating sequences of G of length n and irredundancy rank smaller or equal to k.

Remark 1.1. Observe that a sequence of length n is irredundant if and only if it has irredundancy rank n; this, together with the definition above, clarifies the notation $\varphi_n^n(G)$.

Now fix k, n positive integers. Let $N = \binom{n}{k}$, so that there are N subsets $\pi \subseteq \{1, \dots, n\}$ with $|\pi| = k$. Let $P := \{(H_1, \dots, H_N) : H_i < G\} \cup \{(G, \dots, G)\}$ and $P' = P \setminus (G, \dots, G)$. The relation $(H_1, \dots, H_N) \leq (K_1, \dots, K_N)$ if $H_i \leq K_i$ for each i makes P a partially ordered set. We can denote by μ_P the Möbius function for P, defined as follows:

$$\mu_P(G, \dots, G) = 1, \qquad \sum_{(H_1,\dots,H_N)\leq(X_1,\dots,X_N)} \mu_P(X_1, \dots, X_N) = 0 \tag{1.1}$$

for any $(H_1, \dots, H_N) < (G, \dots, G)$ in P.

Lemma 1.1. If $(H_1, \dots, H_N) < (G, \dots, G)$ in P then

$$\mu_P(H_1, \dots, H_n) = (-1)^{N-1} \mu_G(H_1) \cdots \mu_G(H_N)$$

Proof. Proceed by induction on N and $\prod_i |G : H_i|$. Given $\gamma < N$ and $H_1, \dots, H_\gamma$ proper subgroups of G, we can define $P(H_1, \dots, H_\gamma) := \{(X_1, \dots, X_\gamma) \text{ such that } H_i \leq X_i < G\}$ and $P'(H_1, \dots, H_\gamma) = P(H_1, \dots, H_\gamma) \setminus \{(H_1, \dots, H_\gamma)\}$. Combining together the two equations (1.1) and using induction, one easily gets

$$-\mu_P(H_1, \dots, H_N) = 1 + \sum_{(X_1,\dots,X_N)\in P'(H_1,\dots,H_N)} \mu_P(X_1, \dots, X_N) =$$

$$1 + (-1)^{N-1} \sum_{(X_1,\dots,X_N)\in P'(H_1,\dots,H_N)} \mu_G(X_1) \cdots \mu_G(X_N) =$$

$$1 + (-1)^{N-1} \mu_G(H_1) \sum_{(X_2,\dots,X_N)\in P'(H_2,\dots,H_N)} \mu_G(X_2) \cdots \mu_G(X_N) +$$

$$(-1)^{N-1} \sum_{H_1<K<G} \mu_G(K) \sum_{(X_2,\dots,X_N)\in P(H_2,\dots,H_N)} \mu_G(X_2) \cdots \mu_G(X_N).$$

Again, by (1.1), we get

$$1 + \sum_{(X_2,\dots,X_N)\in P(H_2,\dots,H_N)} \mu_P(X_2, \dots, X_N) = 0,$$

hence, by induction,

$$(-1)^N \sum_{(X_2,\dots,X_N)\in P(H_2,\dots,H_N)} \mu_G(X_2)\cdots\mu_G(X_N) = -1,$$

and we get

$$1 + (-1)^{N-1} \sum_{H_1<K<G} \mu_G(K) \sum_{(X_2,\dots,X_N)\in P(H_2,\dots,H_N)} \mu_G(X_2)\cdots\mu_G(X_N) =$$

$$1 + \sum_{H<K<G} \mu_G(K) = -\mu_G(H_1).$$

Putting everything together we get that

$$\mu_P(H_1,\dots,H_N) = \mu_G(H_1)\left(1 + (-1)^N \sum_{(X_2,\dots,X_N)\in P'(H_2,\dots,H_N)} \mu_G(X_2)\cdots\mu_G(X_N)\right).$$

Again by (1.1) applied to $(H_2,\dots,H_N)$ we get

$$1 + \mu_P(H_2,\dots,H_N) + \sum_{(X_2,\dots,X_N)\in P'(H_2,\dots,H_N)} \mu_P(X_2,\dots,X_N) = 0$$

and by induction

$$1 + (-1)^N \sum_{(X_2,\dots,X_N)\in P'(H_2,\dots,H_N)} \mu_G(X_2)\cdots\mu_G(X_N) = (-1)^{N-1}\mu_G(H_2)\cdots\mu_G(H_N).$$

Combining the latter computation with the one above we can conclude:

$$\mu_P(H_1,\dots,H_N) = \mu_G(H_1)(-1)^{N-1}\mu_G(H_2)\cdots\mu_G(H_N).$$

□

Let $P_k = \{\pi_1,\dots,\pi_N\}$ be the set of the subsets of $\{1,\dots,n\}$ of cardinality k. To any sequence $s = (g_1,\dots,g_n) \in G^n$ we associate a sequence $(H_1,\dots,H_N)$ in the following way. We define $H_m = \langle g_j \mid j \in \pi_m\rangle$ and set $i(s) = (H_1,\dots,H_N)$ if $H_i < G$ for each i and $i(s) = (G,\dots,G)$ otherwise.

Remark 1.2. On one hand observe that if $s \in G^n$ and $i(s) = (G,\dots,G)$, then there is a subsequence of length k generating G (the one composed of the generators of the subgroup H_m such that $H_m = G$), i.e. s has irredundancy rank at most k. On the other hand, if $s \in G^n$ is a generating sequence with rank at most k, there exists $\pi_m \in P_k$ such that $H_m = G$ and therefore $i(s) = (G,\dots,G)$.

Now define a function in the following way: $f : P \to \mathbb{N}$ maps any $(H_1,\dots,H_N) \in P$ into the number of sequences $s \in G^n$ such that $i(s) = (H_1,\dots,H_N)$, clearly we have

$$\sum_{(H_1,\dots,H_N)\in P} f(H_1,\dots,H_N) = |G|^n. \tag{1.2}$$

Thanks to Remark 1.2 we immediately get $\varphi_n^{\leq k}(G) = f(G,\dots,G)$.

Theorem 1.3. For any finite group G, we have

$$\varphi_n^{\leq k}(G) = |G|^n + (-1)^{N-1} \sum_{(H_1,\ldots,H_N)\in P'} \mu_G(H_1)\cdots\mu_G(H_N) \prod_{i=1}^{n} |Y_i(H_1,\ldots,H_N)|,$$

where $N = \binom{n}{k}$ and $Y_i(H_1,\ldots,H_N) = \bigcap_{j:i\in\pi_j} H_j$.

Remark 1.3. If we consider $n = k$ the formula reduces to Hall's. Indeed, $N = 1$, $\varphi_n^{\leq n}(G)$ is just $\varphi_n(G)$ and $Y_i(H) = H$, so that we have

$$\varphi_n(G) = |G|^n + \sum_{H<G} \mu_G(H) \prod_{i=1}^{n} |H| = |G|^n + \sum_{H<G} \mu_G(H)|H|^n = \sum_{H\leq G} \mu_G(H)|H|^n.$$

Proof of Theorem 1.3. Define $F : P \to \mathbb{N}$ by setting $F(H_1,\ldots,H_N) = \sum_{(K_1,\ldots,K_N)\leq(H_1,\ldots,H_N)} f(K_1,\ldots,K_N)$, so by (1.2) we have $F(G,\ldots,G) = |G|^n$. For $(H_1,\ldots,H_N) < (G,\ldots,G)$, $F(H_1,\ldots,H_N)$ equals the number of sequences $(g_1,\ldots,g_n)$ such that $\langle g_i : i \in \pi_m\rangle \leq H_m$ for each m. The latter is equivalent to the fact that a sequence $(g_1,\ldots,g_n)$ is such that $g_i \in Y_i(H_1,\ldots,H_N)$ for each i. Thus

$$F(H_1,\ldots,H_N) = |Y_1(H_1,\ldots,H_N) \times \cdots \times Y_n(H_1,\ldots,H_N)| = \prod_{i=1}^{n} |Y_i(H_1,\ldots,H_N)|.$$

By applying Möbius inversion we obtain

$$f(G,\ldots,G) = \sum_{(H_1,\ldots,H_N)\in P} \mu_P(H_1,\ldots,H_N)F(H_1,\ldots,H_N).$$

Now, $f(G,\ldots,G) = \varphi_n^{\leq k}(G)$, $F(G,\ldots,G) = |G|^n$, we get

$$\varphi_n^{\leq k}(G) = |G|^n + (-1)^{N-1} \sum_{(H_1,\ldots,H_N)\in P'} \mu_G(H_1)\cdots\mu_G(H_N) \prod_{i=1}^{n} |Y_i(H_1,\ldots,H_N)|.$$

□

Corollary 1.1. For any finite group G, the number $\varphi_n^n(G)$ of irredundant generating sequences of length n in G is given by:

$$\sum_{H<G} \mu_G(H)|H|^n + (-1)^n \sum_{(H_1,\ldots,H_n)\in P'} \prod_{i=1}^{n} \mu_G(H_i) \left|\bigcap_{j\neq i} H_j\right| \text{ for } n > 1$$

$$\sum_{H\leq G} \mu_G(H)|H| \text{ for } n = 1$$

Proof. The case $n = 1$ is trivial: clearly $k = 1$, hence we are in the situation discussed in Remark 1.3 and we get Hall's formula with $n = 1$. Now suppose $n > 1$ and observe that $\varphi_n^n = \varphi_n^{\leq n} - \varphi_n^{\leq n-1} = \varphi_n(G) - \varphi_n^{\leq n-1}$, so that using Hall's and the previous formulas, we get

$$\sum_{H\leq G} \mu_G(H)|H|^n - |G|^n - (-1)^{n-1} \sum_{(H_1,\ldots,H_n)\in P'} \prod_{i=1}^{n} \mu_G(H_i) \left|\bigcap_{j\neq i} H_j\right| =$$

$$= \sum_{H<G} \mu_G(H)|H|^n + (-1)^n \sum_{(H_1,\dots,H_n)\in P'} \prod_{i=1}^{n} \mu_G(H_i) \left| \bigcap_{j\neq i} H_j \right|$$

□

1.4 Some examples

In this section we wish to provide some examples on the computation of irredundant generating sequences for some finite groups, using Corollary 1.1.

Example 1.1. Consider the dihedral group of order $2p$, with p prime. In particular, we have that $D_{2p} = \langle a, b \mid a^p = b^2 = e, bab = a^{-1}\rangle$ and it is immediate to check that the only subgroups are the trivial group, the whole group, $\langle a\rangle$ and $\langle ba^j\rangle$ for $j = 0, \dots, p-1$ (which are $p+1$ cyclic maximal subgroups, the first of order p and the others of order 2). Moreover, it is immediate to compute the Möbius function: $\mu_{D_{2p}}(D_{2p}) = 1$, $\mu_{D_{2p}}(H) = -1$ for any non-trivial $H < G$ and $\mu_{D_{2p}}(\{1\}) = p$.
It is obvious that $d(D_{2p}) = m(D_{2p}) = 2$, so that it makes sense only to compute $\varphi_2^2(D_{2p})$. We then obtain: $\varphi_2^2(D_{2p}) = \sum_{H<D_{2p}} \mu_{D_{2p}}(H)|H|^2 + \sum_{(H_1,H_2)\in P'} \mu_{D_{2p}}(H_1)\mu_{D_{2p}}(H_2)|H_1||H_2|$. To make the computation of the second term easy to understand, we use the following table:

	sequences in P'containing the underlying elements	$\mu_{D_{2p}}(H_1)\mu_{D_{2p}}(H_2)$	$\lvert H_1\rvert\lvert H_2\rvert$
$\{1\}$, $\{1\}$	1	p^2	1
$\{1\}$, $\langle a\rangle$	2	$-p$	p
$\{1\}$, $\langle ba^j\rangle$	$2p$	$-p$	2
$\langle a\rangle$, $\langle ba^j\rangle$	$2p$	1	$2p$
$\langle ba^j\rangle$, $\langle ba^j\rangle$	p^2	1	4
$\langle a\rangle$, $\langle a\rangle$	1	1	p^2

It is now enough to make products of rows and sum up, getting $4p^2$. The first term is a straightforward computation and it gives $-p^2-3p$. In conclusion, we get $\varphi_2^2(D_{2p}) = 3p(p-1)$.

Example 1.2. Fix two primes p, q and consider the cyclic group of order pq, $\mathbf{C}_{pq} = \langle a \rangle$. We have 4 subgroups: the trivial one, $\mathbf{C}_{pq}$ itself, $\langle a^q \rangle$ and $\langle a^p \rangle$. First, we can compute directly the number of generating sequences of length 2, in particular of irredundant ones. Indeed, observe that in this group we have the following distinct elements: $(p-1)(q-1)$ elements which generate the whole group, $p-1$ elements of the subgroup $\langle a^q \rangle$, $q-1$ elements of the subgroup $\langle a^p \rangle$ and the identity element. The generating sequences are: $(p-1)^2(q-1)^2$ when we have two generators, $2(p-1)(q-1)(p+q-1)$ when we have only a generator and $2(p-1)(q-1)$ which are the sequences with two elements each in a proper subgroup of the group, i.e. one is in the subgroup $\langle a^q \rangle$ and one in the subgroup $\langle a^p \rangle$. It is clear that the latters are the only irredundant sequences. Summing up we get that the group has $(p^2-1)(q^2-1)$ generating sequences.
Observe that we can easily generalize the computation of the number of irredundant generating sequences for a cyclic group of order the product of k primes. Indeed, the number of irredundant generating sequences of length k in this case is just $n!(p_1-1)\cdots(p_k-1)$: the only way to have an irredundant generating sequence is to pick a generator for each subgroup of the form $\langle a^{p_i} \rangle$, where a is the generator of the group and $i = 1, \ldots, k$; in particular we have $(p_1-1)\cdots(p_k-1)$ irredundant generating sets, hence $n!(p_1-1)\cdots(p_k-1)$ irredundant generating sequences.
Now let's go back to the case where the cyclic group has order the product of two primes. We show we get the same result with the formula of Corollary 1.1. First, compute the Möbius function. By definition, $\mu_G(\mathbf{C}_{pq}) = 1$; $\langle a^q \rangle$ and $\langle a^p \rangle$ are contained only in $\mathbf{C}_{pq}$, hence their Möbius is just -1; the trivial subgroup is contained in the previous three subgroup, hence the Möbius is 1. We get then:

$$\sum_{H<G} \mu_G(H)|H|^n = 1 - p^2 - q^2.$$

The second term reduces to

$$\sum_{(H_1,H_2)\in P'} \mu_G(H_1)\mu_G(H_2)|H_1||H_2|$$

To make things clearer, consider the following table (H_1 is the term on the left column, H_2 the term on the top row and in the other cells the result of $\mu_G(H_1)\mu_G(H_2)|H_1||H_2|$):

	$\{1\}$	$\langle a^q \rangle$	$\langle a^p \rangle$
$\{1\}$	1	$-p$	$-q$
$\langle a^q \rangle$	$-p$	p^2	pq
$\langle a^p \rangle$	$-q$	pq	q^2

Now we have to sum the results in the table, getting

$$1 + p^2 + q^2 + 2(-p - q + pq).$$

Combining the two parts of the formula we get

$$1 - p^2 - q^2 + 1 + p^2 + q^2 + 2(-p - q + pq) = 2(1 - p - q + pq) = 2(p-1)(q-1)$$

as we wanted.
Now we are left to compute the case $n > 2$. Similarly as before, we have

$$\sum_{H<G} \mu_G(H)|H|^n = 1 - p^n - q^n.$$

For the second part we should compute a sum over 3^n terms, which can be a little tricky. However, we can observe that just for a few sequences the term $\left|\bigcap_{j\neq i} H_j\right|$ is non-trivial, hence we may try to compute $\sum_{(H_1,\dots,H_n)\in P'} \prod_{i=1}^n \mu_G(H_i)$ at first. If we say j the number of non-trivial subgroups in the sequence (i.e. in the sequence there are j subgroups which are $\langle a^p\rangle$ or $\langle a^q\rangle$ and $n-j$ the trivial subgroup). In such a sequence the Möbius depends on $(-1)^j$. Moreover, there are 2^j ways of choosing the elements (depending on whether we choose $\langle a^p\rangle$ or $\langle a^q\rangle$) and once the elements are fixed, $\binom{n}{j}$ is the number of possible ordered sequences. Then we have

$$\sum_{(H_1,\dots,H_n)\in P'} \prod_{i=1}^n \mu_G(H_i) = \sum_{j=0}^n \binom{n}{j}(-2)^j.$$

Now we need to look for the sequences where the term $\left|\bigcap_{j\neq i} H_j\right|$ is non-trivial, but this is straightforward, indeed these are just the sequences with $n-1$ times the subgroup $\langle a^p\rangle$ (resp. $\langle a^q\rangle$) and the other subgroup which is different, i.e. $\langle a^q\rangle$ or $\{1\}$ (resp. $\langle a^p\rangle$ or $\{1\}$), and also the two sequences with n subgroups equal to $\langle a^p\rangle$ or $\langle a^q\rangle$. Say $\overline{P}$ the family of these sequences. We get

$$\sum_{(H_1,\dots,H_n)\in\overline{P}} \prod_{i=1}^n \mu_G(H_i) = 2n(-1)^{n-1} + 2n(-1)^n + 2(-1)^n = 2(-1)^n.$$

And now we are left to compute

$$\sum_{(H_1,\dots,H_n)\in\overline{P}} \prod_{i=1}^n \mu_G(H_i)\left|\bigcap_{j\neq i} H_j\right| =$$

$$= np(-1)^{n-1} + np(-1)^n + nq(-1)^{n-1} + nq(-1)^n + (-1)^n p^n + (-1)^n q^n = (-p)^n + (-q)^n.$$

The number of irredundant generating sequences is then

$$\sum_{H<G} \mu_G(H)|H|^n + (-1)^n \left(\sum_{(H_1,\dots,H_n)\in P'} \prod_{i=1}^n \mu_G(H_i) - \right.$$

$$\left. - \sum_{(H_1,\dots,H_n)\in\overline{P}} \prod_{i=1}^n \mu_G(H_i) + \sum_{(H_1,\dots,H_n)\in\overline{P}} \prod_{i=1}^n \mu_G(H_i)\left|\bigcap_{j\neq i} H_j\right| \right) =$$

$$1 - p^n - q^n + (-1)^n \left(\sum_{j=0}^n \binom{n}{j}(-2)^j - 2(-1)^n + (-p)^n + (-q)^n \right) =$$

$$= 1 + (-1)^n \left(\sum_{j=0}^{n} \binom{n}{j} (-2)^j \right) - 2 = -1 + (-1)^n \left(\sum_{j=0}^{n} \binom{n}{j} (-2)^j \right).$$

Now it is enough to prove this is zero. Proceeding by induction:

$$(-1)^{n+1} \left(\sum_{j=0}^{n+1} \binom{n+1}{j} (-2)^j \right) = (-1)^{n+1} \left(\sum_{j=1}^{n} \binom{n+1}{j} (-2)^j + 1 + (-2)^{n+1} \right) =$$

$$= (-1)^{n+1} \left(\sum_{k=0}^{n-1} \binom{n+1}{k+1} (-2)^{k+1} + 1 + (-2)^{n+1} \right) =$$

$$= (-1)^{n+1} \left(\sum_{k=0}^{n-1} \binom{n}{k+1} (-2)^{k+1} + \sum_{k=0}^{n-1} \binom{n}{k} (-2)^{k+1} + 1 + (-2)^{n+1} \right) =$$

$$= (-1)^{n+1} \left(\sum_{k=0}^{n-1} \binom{n}{k+1} (-2)^{k+1} + 1 + (-2) \left(\sum_{k=0}^{n-1} \binom{n}{k} (-2)^k + (-2)^n \right) \right) =$$

$$= (-1) \left((-1)^n \sum_{j=0}^{n} \binom{n}{j} (-2)^j - 2(-1)^n \sum_{k=0}^{n} \binom{n}{k} (-2)^k \right) = 1.$$

Example 1.3. Consider $\mathbf{S}_3 = \{\{1\}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. We have the following distinct subgroups (for simplicity we write $\langle x\ y \rangle$ for $\langle (x\ y) \rangle$):

- $\mathbf{S}_3$
- $\langle 1\ 2 \rangle = \{\{1\}, (1\ 2)\}$
- $\langle 1\ 3 \rangle = \{\{1\}, (1\ 3)\}$
- $\langle 2\ 3 \rangle = \{\{1\}, (2\ 3)\}$
- $\langle 1\ 2\ 3 \rangle = \{\{1\}, (1\ 2\ 3), (1\ 3\ 2)\}$
- $\{1\}$

As before, we easily compute the Möbius:

- $\mu(\mathbf{S}_3) = 1$
- $\mu(\langle 1\ 2 \rangle) = -1$
- $\mu(\langle 1\ 3 \rangle) = -1$
- $\mu(\langle 2\ 3 \rangle) = -1$
- $\mu(\langle 1\ 2\ 3 \rangle) = -1$
- $\mu(\{1\}) = 3$

We can compute the irredundant generating sequences of length 2. Using our formula we get:

$$\mu(\{1\})\,|\{1\}|^2+\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|^2+\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|^2+\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|^2+\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|^2+$$
$$2(\mu(\{1\})\,|\{1\}|\,\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|+\mu(\{1\})\,|\{1\}|\,\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|+\mu(\{1\})\,|\{1\}|\,\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|+$$
$$\mu(\{1\})\,|\{1\}|\,\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|+\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|\,\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|+\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|\,\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|+$$
$$\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|\,\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|+\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|\,\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|+$$
$$\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|\,\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|+\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|\,\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|)+$$
$$\mu(\{1\})\,|\{1\}|\,\mu(\{1\})\,|\{1\}|+\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|\,\mu(\langle 1\ 2\rangle)\,|\langle 1\ 2\rangle|+\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|\,\mu(\langle 1\ 3\rangle)\,|\langle 1\ 3\rangle|+$$
$$\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|\,\mu(\langle 2\ 3\rangle)\,|\langle 2\ 3\rangle|\ +\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|\,\mu(\langle 1\ 2\ 3\rangle)\,|\langle 1\ 2\ 3\rangle|=$$
$$3-4-4-4-9+2(-6-6-6-9+4+4+6+4+6+6)+9+4+4+4+9=18.$$

1.5 GAP implementation

At this point it is clear that the formula is an interesting way to compute irredundant generating sequences, but making all the computations by hand can often be challenging, as we have seen in the previous examples. To make things easier, we are going to show a way to implement the formula on GAP:

At first, we have to define the group we want to work with and a list with his subgroups:

```
G:=...;
list:=AllSubgroups(G);;
```

Then we want to compute the Möbius function

```
tom:=TableOfMarks(G);;
moebius:=MoebiusTom(tom);;
moebius.mu;
[x_1,...,x_n]
```

Observe that we may get a list with non-assigned values instead of zeros, so that we need the following:

```
firstml:=[]
for i in [1..Size(moebius.mu)] do
    firstml[i]:=GetWithDefault(moebius.mu,i,0);
od;
```

Now we want to define a list such that the i-th slot of this list is the value of the Möbius of the i-th subgroup in our list of subgroups of G. For this purpose it is enough to observe that moebius.mu returns the values of the Möbius with respect to the list of subgroups up to conjugation:

```
s:=1;;
secondml:=[];;
secondml[1]:=firstml[1];;
for i in [1..Size(list)-1] do
    if IsConjugate(G, list[i+1], list[i]) then
        secondml[i+1]:=firstml[s];
    else secondml[i+1]:=firstml[s+1];
        s:=s+1;
fi;
od;
```

Now we can define a new list removing the zeros of secondml. This new list is the one that we will use for the main computation:

```
ml:=[];;
for i in [1..Size(secondml)] do
    if secondml[i]<>0 then
        Add(ml,secondml[i]);
fi;
od;
```

Now we do the same for the list of subgroups:

```
sl:=[];;
for i in [1..Size(secondml)] do
    if secondml[i]<>0 then
        Add(sl,list[i]);
fi;
od;
```

Now we can proceed with the implementation of the formula. The idea is to define two empty lists and add in these lists the elements of the two summands. The first part is then:

```
el1:=[];;
for i in [1..Size(sl)-1] do
    Add(el1,ml[i]*Size(sl[i])^n);
od;
```

The second part is:

```
el2:=[];;
for x_1 in [1..Size(sl)-1] do
    ...
        for x_n in [1..Size(sl)-1] do
         Add(el2,ml[x_1]*...*ml[x_n]*Size(Intersection(sl[x_2],...,al[x_n])*...
         *Size(Intersection(sl[x_1],...,sl[x_i-1],sl[x_i+1],...,sl[x_n])*...*
         Size(Intersection(sl[x_1],...sl[x_n-1])));
```

```
od;
...
od;
```

Then we just have to put the two parts together following the formula:

```
Sum(el1)+(-1)^n*Sum(el2);
```

Let's try to use the code for S_3 and check we get the same results of Example 1.3:

```
G:=SymmetricGroup(3);;
list:=AllSubgroups(G);;
tom:=TableOfMarks(G);;
moebius:=MoebiusTom(tom);;
moebius.mu;
[3,-1,-1,1]
firstml:=moebius.mu;;
s:=1;;
secondml:=[];;
secondml[1]:=firstml[1];;
for i in [1..Size(list)-1] do
    if IsConjugate(G, list[i+1], list[i]) then
        secondml[i+1]:=firstml[s];
    else secondml[i+1]:=firstml[s+1];
        s:=s+1;
fi;
od;
secondml;
[3,-1,-1,-1,-1,1]
ml:=secondml;;
sl:=list;;
el1:=[];;
for i in [1..Size(sl)-1] do
    Add(el1,ml[i]*Size(sl[i])^2);
od;
Sum(el1);
-18
el2:=[];;
for x_1 in [1..Size(sl)-1] do
    for x_2 in [1..Size(sl)-1] do
         Add(el2,ml[x_1]*ml[x_2]*Size(sl[x_1])*Size(sl[x_2]));
od;
od;
Sum(el2);
36
Sum(el1)+(-1)^2*Sum(el2);
18
```

1.6 Irredundant generating sequences of S_4

Before the explicit computation of the irredundant generating sequences of length 3 of S_4, we discuss the following results from [3] (Theorem 2.1, Corollary 2.2, Remark p. 6):

Theorem 1.4. Let S be an irredundant generating set for S_n of size $n-1$, where $n \geq 7$, and $S(T)$ a set of $n-1$ transpositions. Then S can be of two different types:

(a) $S = S(T)$;

(b) S is a set composed of a transposition s and $n-2$ elements of the form st (or ts if this is a 3−cycle) for any $t \in S(T) \setminus s$;

Corollary 1.2. For $n \geq 7$, the number of irredundant generating sets of S_n are n^{n-2} of the type (a) and $n^{n-2}(n-2)$ of the type (b).

As per the statement, the theorem works for $n \geq 7$. However, in [3] they discuss the case for $n = 4$, stating that it is enough to add the sets composed of two transpositions with a common element and a double transposition. In particular, we have 36 sets of this type: there are 6 ways to choose the first transposition, 4 ways to choose the second with an only element in common with the first and 3 ways of choosing the double transposition, then divide by 2 in order not to count two times the same pair of transpositions. Now we have to add 16 sets of the type (a) and 48 elements of the type (b). Therefore, there should be 100 generating irredundant sets.
Now we want to repeat the computations above using our GAP procedure, as follows:

```
G:=SymmetricGroup(4);;
list:=AllSubgroups(G);;
tom:=TableOfMarks(G);;
moebius:=MoebiusTom(tom);;
moebius.mu;
[-12,,2,1,3,,,-1,-1,-1,1]
firstml:=[]
for i in [1..Size(moebius.mu)] do
    firstml[i]:=GetWithDefault(moebius.mu,i,0);
od;
firstml;
[-12,0,2,1,3,0,0,-1,-1,-1,1]
s:=1;;
secondml:=[];;
secondml[1]:=firstml[1];;
for i in [1..Size(list)-1] do
    if IsConjugate(G, list[i+1], list[i]) then
        secondml[i+1]:=firstml[s];
    else secondml[i+1]:=firstml[s+1];
        s:=s+1;
fi;
od;
```

```
ml:=[];;
for i in [1..Size(secondml)] do
    if secondml[i]<>0 then
        Add(ml,secondml[i]);
fi;
od;
sl:=[];;
for i in [1..Size(secondml)] do
    if secondml[i]<>0 then
        Add(sl,list[i]);
fi;
od;
el1:=[];;
for i in [1..Size(sl)-1] do
    Add(el1,ml[i]*Size(sl[i])^3);
od;
el2:=[];;
for x_1 in [1..Size(sl)-1] do
    for x_2 in [1..Size(sl)-1] do
        for x_3 in [1..Size(sl)-1] do
         Add(el2,ml[x_1]*ml[x_2]*ml[x_3]*
         Size(Intersection(sl[x_2],sl[x_3]))*
         Size(Intersection(sl[x_1],sl[x_3]))*
         Size(Intersection(sl[x_1],sl[x_2])));
od;
od;
od;
Sum(el1)+(-1)^3*Sum(el2);
888
```

Since we have the number of irredundant generating sequences, we have to identify sequences which are equal up to the order of the elements, so that we get 148 irredundant generating sets. This means that there is something wrong with the results from [3]. In particular Theorem 1.3 (b) considers the irredundant generating sets with a transposition s, a 3-cycle st and a 3-cycle st', which are 24, and the irredundant generating sets with a transposition s, a 3-cycle st and a double transposition st', which are 24, but also the sets with the other two double transpositions should be considered, hence we should add 48 to the previous computation and we get again 148. Indeed, suppose $s = (1\ 2)$ and $t = (1\ 3)$. According to the discussion above, we are interested in the three sets containing s, st and a double transposition, which are $K_1 = \{(1\ 2), (1\ 2\ 3), (1\ 2)(3\ 4)\}$, $K_2 = \{(1\ 2), (1\ 2\ 3), (1\ 3)(2\ 4)\}$ and $K_3 = \{(1\ 2), (1\ 2\ 3), (1\ 4)(2\ 3)\}$. K_1 has been counted in Theorem 1.3 (b). We want to show that K_2 is irredundant and generating. Since $\{(1\ 2), (1\ 2\ 3)\} \subseteq S_3$ and $\{(1\ 2), (1\ 3)(2\ 4)\}$ is contained in a 2-Sylow, these cannot generate S_4. Clearly, also $\{(1\ 2\ 3), (1\ 3)(2\ 4)\}$ is not generating, since both elements are in A_4, hence we are left to prove that K_2 is a generating set. Observe that $(1\ 2)(1\ 2\ 3) = (1\ 3)$ and $(1\ 3)(1\ 3)(2\ 4) = (2\ 4)$, hence $\{(1\ 2), (1\ 3), (2\ 4)\} \subseteq K_2$, but the first one is a set of type (a), hence it generates the whole group and so does K_2. The same arguments hold for K_3, since $(1\ 2\ 3)(1\ 2) = (2\ 3)$ and $(1\ 4)(2\ 3)(2\ 3) = (1\ 4)$. Clearly, the same procedure can be applied for any choice of s and t, whenever st is a 3-cycle.

Chapter 2

Irredundant generating sequences of subgroups

2.1 First definitions and generalization of Tarski's theorem

In this section we want to discuss what happens if we consider sequences of subgroups instead of sequences of elements. Fix a family of finite groups $\mathcal{F}$.

Definition 2.1. We say $(H_1, \dots, H_n)$ is an irredundant generating $\mathcal{F}$-sequence of G if $\langle H_1, \dots, H_n \rangle = G$ but $\langle H_1, \dots, H_{i-1}, H_{i+1}, \dots, H_n \rangle \neq G$ where $H_i \leq G$ and $H_i \in \mathcal{F}$, for any $i = 1, \dots, n$.

Remark 2.1. Suppose $\mathcal{F}$ is a family containing all cyclic finite groups. It is clear that there is a correspondence between irredundant generating sequences of elements of G, $(g_1, \dots, g_n)$, and irredundant generating $\mathcal{F}$-sequences of cyclic subgroups of G, $(\langle g_1 \rangle, \dots, \langle g_n \rangle)$.

Exactly as for sequences of elements, we can consider the maximal and minimal length of an irredundant generating $\mathcal{F}$-sequence, denoted by $m_{\mathcal{F}}(G)$ and $d_{\mathcal{F}}(G)$, respectively. Observe that they are closely related with the choice of $\mathcal{F}$, e.g. if $G \in \mathcal{F}$ then $d_{\mathcal{F}}(G) = 1$, while if $\mathcal{F}$ is the family of cyclic groups we just have $d_{\mathcal{F}}(G) = d(G)$ by Remark 2.1. However, things are easier for $m_{\mathcal{F}}(G)$:

Proposition 2.1. For any finite group G and family of finite groups $\mathcal{F}$ containing all the cyclic groups, we have $m_{\mathcal{F}}(G) = m(G)$.

Proof. By Remark 2.1, $m(G) \leq m_{\mathcal{F}}(G)$. Conversely, let $s = (H_1, \dots, H_{m_{\mathcal{F}}(G)})$ be an irredundant generating $\mathcal{F}$-sequence. Clearly, $H_i = \langle X_i \rangle$ for a certain set X_i, for any

$i = 1, \ldots, m_{\mathcal{F}}(G)$. Since the union of the X_i's is a generating set, it also contains an irredundant generating set, say Y. Then we can observe that $Y \cap H_i \neq \emptyset$ for any $i = 1, \ldots, m_{\mathcal{F}}(G)$, otherwise s would not be irredundant. Therefore, we get $m_{\mathcal{F}}(G) \leq |Y| \leq m(G)$. □

At this point one could ask whether an irredundant generating $\mathcal{F}$-sequence of a certain length exists. To answer this question, here is a generalization of Theorem 1.1:

Theorem 2.1. For any finite group G and family of finite groups $\mathcal{F}$, containing all cyclic groups and closed under subgroups, there exists an irredundant generating $\mathcal{F}$-sequence of length n for any n such that $d_{\mathcal{F}}(G) \leq n \leq m_{\mathcal{F}}(G)$.

Proof. Let Ω be an irredundant generating set of elements of G, such that $|\Omega| = m(G)$. For any $g \in G$, let $l(g)$ be the length of g when it is expressed as a word of elements of Ω. Moreover, for any $H \leq G$, let $l(H) = \min_{\langle X \rangle = H} \sum_{x \in X} l(x)$. Now suppose that there is an irredundant generating $\mathcal{F}$-sequence of length t (for sure this happens for $t = m_{\mathcal{F}}(G)$) and let $\mathcal{B}$ be the set of the irredundant generating $\mathcal{F}$-sequences of length smaller than t. To prove the theorem we need to find an irredundat generating $\mathcal{F}$-sequence of length $t-1$ and then iterate the process for any $t > d_{\mathcal{F}}(G)$. For any $B \in \mathcal{B}$, let $\delta_\Omega(B) = \max_{H \in B} l(H)$ and $\nu_\Omega(B) = |\{H \in B \mid l(H) = \delta_\Omega(B)\}|$. Fix $\overline{B} = \{H_1, \ldots, H_u\} \in \mathcal{B}$ minimizing $\delta_\Omega(\overline{B})$ and $\nu_\Omega(\overline{B})$. Observe that if H_i is cyclic for any $i = 1, \ldots, u$, we conclude by Remark 2.1 and Theorem 1.1. Without loss of generality, suppose H_u not cyclic and $\delta_\Omega(\overline{B}) = l(H_u)$. In particular, we have $H_u = \langle g_1, \ldots, g_r \rangle$, for $r \geq 2$, with $l(H_u) = \sum_{i=1}^{r} l(g_i)$. Now, set $K_u = \langle g_1, \ldots, g_{r-1} \rangle$ and $K_{u+1} = \langle g_r \rangle$ so that we can consider the $\mathcal{F}$-sequence $\{H_1, \ldots, H_{u-1}, K_u, K_{u+1}\}$. Clearly, the latter is a generating $\mathcal{F}$-sequence since $\overline{B}$ is, hence it contains an irredundant generating $\mathcal{F}$-sequence B^*. By construction, $\delta_\Omega(B^*) \leq \delta_\Omega(\overline{B})$ and if equality holds $\nu_\Omega(B^*) \leq \nu_\Omega(\overline{B})$. By our choice of $\overline{B}$, it has to be $B^* \notin \mathcal{B}$, therefore $|B^*| \geq t$. But we also know that $|B^*| = |\overline{B}| + 1 \leq t$, hence the only possibility is that equality holds, i.e. $u = t - 1$. □

Example 2.1. If we assume $\mathcal{F} = \{C_2, C_{73}\}$, then $G = PSU_3(9)$ has irredundant generating $\mathcal{F}$-sequences of length 2 and 4 but not 3. Specifically, a sequence with three subgroups generated by elements of order 2 would not be generating (four elements of order 2 are needed to generate G); a sequence of length 3 containing a group generated by an element of order 73 would not be irredundant, since an element of order 73 generates the whole group together with any element of order 2 or any another element of order 73. All this implies that there are no irredundant generating sequences of length 3. However, for the reasons explained above, any sequence of length 2 containing two cyclic groups generated by an element of order 73 and any sequence of length 4 containing only cyclic groups generated by an element of order 2 would be irredundant and generating. In other words, it turns out that the assumption on cyclic groups is necessary in general.
Moreover, observe that the theorem is not true if we don't assume that $\mathcal{F}$ is closed under subgroups. Indeed, assume $\mathcal{F}$ contains only the cyclic groups and $G = C_2 \times C_2 \times C_2$. Clearly, $d_{\mathcal{F}}(G) = 1$. However, since $d(G) = 3$, there are no irredundant generating $\mathcal{F}$-sequences of G of length 2.

We conclude this section with a simple but interesting result for a different choice of $\mathcal{F}$. Consider the following theorem from [1]:

Theorem 2.2. In every finite group G there exists a pair of conjugate solvable subgroups $H, K \leq G$, such that $\langle H, K \rangle = G$. In particular, if $x \in G$ is such that $H = xKx^{-1}$ then $\langle H, x \rangle = G$.

We can then immediately deduce the following:

Corollary 2.1. Let $\mathcal{F}$ be the family of all solvable finite groups, then $d_F(G) \leq 2$.

2.2 Counting irredundant generating sequences of subgroups

In this section we want to discuss the computation of irredundant generating sequences of subgroups, in particular we will proceed similarly as for sequences of elements and we will get similar results. To avoid confusion, we will use $\phi_n(G)$ in place of $\varphi_n(G)$ to indicate the number of length-n generating sequences of subgroups, $\phi_n^{\leq k}(G)$ in place of $\varphi_n^{\leq k}(G)$ to indicate the number of length-n generating sequences of irredundancy rank smaller or equal than k and $\phi_n^n(G)$ in place of $\varphi_n^n(G)$ to indicate the number of length-n irredundant generating sequences.

Definition 2.2. For any $X \subseteq G$, we define $\sigma_{G,\mathcal{F}}(X)$ to be the number of subgroups of G which are in $\mathcal{F}$ and are contained in X.

Remark 2.2. At first we try to develop an analogous of Hall's formula. Fix n and let $\psi(H) := \sum_{K \leq H} \phi_{n,\mathcal{F}}(K) = \sigma_{G,\mathcal{F}}(H)^n$. Applying Theorem 1.2 we get

$$\phi_{n,\mathcal{F}}(G) = \sum_{H \leq G} \mu_G(H)\sigma_{G,\mathcal{F}}(H)^n.$$

In particular, observe that if $n = 1$, then:

$$\sum_{H \leq G} \mu_G(H)\sigma_{G,\mathcal{F}}(H) = \begin{cases} 1 \text{ if } G \in \mathcal{F} \\ 0 \text{ if } G \notin \mathcal{F} \end{cases}.$$

After that, we want a formula for irredundant generating $\mathcal{F}$-sequences. Recall that we defined $P_k = \{\pi_1, \ldots, \pi_N\}$ as the set of the subsets of $\{1, \ldots, n\}$ of cardinality k. Now fix a family of finite groups $\mathcal{F}$ and as in the previous chapter, to any sequence $s = (K_1, \ldots, K_n) \in \mathcal{F}^n$, $K_i \leq G$ for any $i = 1, \ldots, n$, we associate a sequence $(H_1, \ldots, H_N)$ where $H_m = \langle K_j \mid j \in \pi_m \rangle$ and $i(s) = (H_1, \ldots, H_N)$ if $H_i < G$ for each i and $i(s) = (G, \ldots, G)$ otherwise.
Again, $i(s) = (G, \ldots, G)$ is equivalent to say that s has irredundancy rank at most k.
Now define a function in the following way: $f : P \to \mathbb{N}$ maps each $(H_1, \ldots, H_N) \in P$ into the number of sequences s composed of subgroups of G in $\mathcal{F}$ such that $i(s) = (H_1, \ldots, H_N)$; clearly we have

$$\sum_{(H_1,\ldots,H_N) \in P} f(H_1, \ldots, H_N) = \sigma_{G,\mathcal{F}}(G)^n. \tag{2.1}$$

As before, we get $\phi_n^{\leq k}(G) = f(G, \ldots, G)$.

Theorem 2.3. For any finite group G, we have

$$\phi^{\leq k}_{n,\mathcal{F}}(G) = \sigma_{G,\mathcal{F}}(G)^n + (-1)^{N-1} \sum_{(H_1,\ldots,H_N)\in P'} \mu_G(H_1)\cdots\mu_G(H_N) \prod_{i=1}^{n} \sigma_{G,\mathcal{F}}(Y_i(H_1,\ldots,H_N)),$$

where $N = \binom{n}{k}$ and $Y_i(H_1,\ldots,H_N) = \bigcap_{j:i\in\pi_j} H_j$.

Proof of Theorem 1.3.
Define $F : P \to \mathbb{N}$ by setting $F(H_1,\ldots,H_N) = \sum_{(S_1,\ldots,S_N)\leq(H_1,\ldots,H_N)} f(S_1,\ldots,S_N)$, so we have $F(G,\ldots,G) = \sigma_{G,\mathcal{F}}(G)^n$. For $(H_1,\ldots,H_N) < (G,\ldots,G)$, $F(H_1,\ldots,H_N)$ equals the number of sequences $(K_1,\ldots,K_n)$ such that $\langle K_i : i \in \pi_m\rangle \leq H_m$ for each $m = 1,\ldots,N$. The latter is equivalent to the fact that a sequence $(K_1,\ldots,K_n)$ is such that $K_i \in Y_i(H_1,\ldots,H_N)$ for each $i = 1,\ldots,n$. Thus

$$F(H_1,\ldots,H_N) = \prod_{i=1}^{n} \sigma_{G,\mathcal{F}}(Y_i(H_1,\ldots,H_N)).$$

By applying Möbius inversion we obtain

$$f(G,\ldots,G) = \sum_{(H_1,\ldots,H_N)\in P} \mu_P(H_1,\ldots,H_N)F(H_1,\ldots,H_N).$$

Now, $f(G,\ldots,G) = \phi^{\leq k}_n(G)$, $F(G,\ldots,G) = \sigma_{G,\mathcal{F}}(G)^n$, hence we get

$$\phi^{\leq k}_{n,\mathcal{F}}(G) = \sigma_{G,\mathcal{F}}(G)^n + (-1)^{N-1} \sum_{(H_1,\ldots,H_N)\in P'} \mu_G(H_1)\cdots\mu_G(H_N) \prod_{i=1}^{n} \sigma_{G,\mathcal{F}}(Y_i(H_1,\ldots,H_N)).$$

□

Corollary 2.2. For any finite group G and family of finite groups $\mathcal{F}$, the number $\phi^n_{n,\mathcal{F}}(G)$ of irredundant generating $\mathcal{F}$-sequences of length n in G is given by:

$$\sum_{H<G} \mu_G(H)\sigma_{G,\mathcal{F}}(H)^n + (-1)^n \sum_{(H_1,\ldots,H_n)\in P'} \prod_{i=1}^{n} \mu_G(H_i)\sigma_{G,\mathcal{F}}\left(\bigcap_{j\neq i} H_j\right) \text{ for } n > 1$$

$$\sum_{H\leq G} \mu_G(H)\sigma_{G,\mathcal{F}}(H) \text{ for } n = 1$$

Proof. The proof is exactly as the one of Corollary 1.1. □

2.3 A particular choice of $\mathcal{F}$

In this section, we focus on a particular choice of the family of finite groups $\mathcal{F}$; indeed it is interesting to check whether previous results still work if $\mathcal{F}$ is the family of all cyclic groups with a prime-power order. Thanks to Remark 2.1, we can equivalently deal with sequences of elements with the desired condition. For the sake of clarity, we denote by $\mathcal{S}$ the family of irredundant generating sequences of elements of order a prime-power, and denote by $\widetilde{d}(G)$ and $\widetilde{m}(G)$ the minimal and maximal length, respectively, of an element in $\mathcal{S}(G)$.

Lemma 2.1. For any finite group G, $\widetilde{m}(G) = m(G)$.

Proof. If $(x_1, \dots, x_n) \in \mathcal{S}$ then it is also, trivially, an irredundant generating sequence of elements of G, therefore $\widetilde{m}(G) \leq m(G)$.
Conversely, let $(g_1, \dots, g_m)$ be an irredundant generating sequence, with $m = m(G)$. Let $g_i = \prod_{j=1}^{t_i} x_{i,j}$ with $|x_{i,j}| = p_i^{l_i}$ for $i = 1, \dots, m$. Now, if we consider the set $X = \{x_{i,j} : 1 \leq i, j \leq n\}$, then there is an irredundant generating sequence $Y \subseteq X$. Observe that $Y \cap \{x_{i,1}, \dots, x_{i,t_i}\} \neq \emptyset$ for any $i = 1, \dots, m$, otherwise $(g_1, \dots, g_m)$ would not be irredundant. Therefore, by construction we have $\widetilde{m}(G) \geq |Y| \geq m(G)$. □

We are interested in investigating if the generalization of Tarski's Theorem still works. Here we show that this is true under certain assumptions. First, observe the following:

Theorem 2.4. Let G be a solvable finite group and fix an integer k such that $\widetilde{d}(G) \leq k \leq \widetilde{m}(G)$, then there is an irredundant generating $\mathcal{S}$-sequence of length k.

Proof. We proceed by induction on the order of G. Since G is solvable, we can fix a minimal normal subgorup N of G, such that $|N| = p^t$ for some prime p. Fix an irredundant generating sequence in $\mathcal{S}(G/N)$, say $(g_1N, \dots, g_rN)$. Now we define a sequence $(\widetilde{g_1}, \dots, \widetilde{g_r})$ in the following way: if $|g_iN|$ is a p-power, then g_i has order a power of p and we set $\widetilde{g_i} = g_i$; if $|g_iN|$ is a q-power, for a prime $q \neq p$, then there exists $\widetilde{g_i}$ with order q^n and such that $\widetilde{g_i}N = g_iN$. At this point, we can have two distinct situations:

- Suppose $N \leq \mathrm{Frat}(G)$. Then, for any $(g_1N, \dots, g_rN) \in \mathcal{S}(G/N)$, we can define $(\widetilde{g_1}, \dots, \widetilde{g_r}) \in \mathcal{S}(G)$ as above (the two sequences have the same length). In particular, $\widetilde{d}(G) = \widetilde{d}(G/N)$ and $\widetilde{m}(G) = \widetilde{m}(G/N)$, hence we are done using induction.
- Suppose $N \not\leq \mathrm{Frat}(G)$. In this case we can fix $H < G$, a maximal subgroup of G not containing N, such that $G = N \rtimes H$. We have $\widetilde{m}(G) = m(G) = m(H) + 1 = \widetilde{m}(H) + 1$ (where the first and last equality hold thanks to Lemma 2.1 and the second equality thanks to Lemma 12 [8]). Moreover, $\widetilde{d}(G) = \widetilde{d}(H)$ or $\widetilde{d}(H) + 1$. Indeed, for any $(g_1, \dots, g_{\widetilde{d}(H)}) \in \mathcal{S}(H)$ and $n \neq 1 \in N$, $(g_1, \dots, g_{\widetilde{d}(H)}, n) \in \mathcal{S}(G)$. By induction, for any integer k such that $\widetilde{d}(H) \leq k \leq \widetilde{m}(H)$, there exists an irredundant generating sequence $(g_1, \dots, g_k) \in \mathcal{S}(H)$. Again, if we fix $n \neq 1 \in N$, then $(g_1, \dots, g_k, n) \in \mathcal{S}(G)$, hence we can find a sequence of length t in $\mathcal{S}(G)$ for any integer t such that $\widetilde{d}(H) + 1 \leq t \leq \widetilde{m}(H) + 1$, i.e. for any integer t such that $\widetilde{d}(G) < t \leq \widetilde{m}(G)$ (and of course also for $t = \widetilde{d}(G)$ by definition).

□

However, we aim to show that we can relax the assumption on solvability for symmetric and alternating groups. At first, observe the following result [9]:

Theorem 2.5. For any integer $n \geq 25$, it is always possible to find a prime between n and $\frac{6}{5}n$.

We can then deduce the following:

Corollary 2.3. For any integer $n > 7$, there exists a prime p such that $n/2 < p \leq n - 3$.

Proof. If $7 < n < 50$ one can check it immediately by hand. If n is even, apply the previous theorem to $n/2$, so that there is a prime p such that $n/2 < p \leq 6n/10 < n - 3$. If n is odd, just do the same for $(n + 1)/2$. □

Now we want to show a straightforward construction on S_n and A_n. At first, fix $n \geq 3$ and let α, β in S_n be as follows:

- If $n > 7$ then we fix a prime $n/2 < p \leq n - 3$ thanks to Corollary 2.3 and pick $\alpha = (1\ 2\ \ldots\ p)$ and $\beta = (u\ u + 1\ \ldots\ n)$ in such a way β has length the maximum power of 2 strictly smaller than n (and observe that this is obviously larger than $n/2$).
- $n = 7$, $\alpha = (1\ 2\ 3\ 4\ 5)$, $\beta = (4\ 5\ 6\ 7)$
- $n = 6$, $\alpha = (1\ 2\ 3\ 4\ 5)$, $\beta = (3\ 4\ 5\ 6)$
- $n = 5$, $\alpha = (1\ 2\ 3)$, $\beta = (2\ 3\ 4\ 5)$
- $n = 4$, $\alpha = (1\ 2\ 3)$, $\beta = (3\ 4)$
- $n = 3$, $\alpha = (1\ 2)$, $\beta = (2\ 3)$

Similarly, for A_n:

- If $n > 7$ then we fix a prime $n/2 < p \leq n - 3$ thanks to Corollary 2.3 and pick $\gamma = (1\ 2\ \ldots\ p)$ and $\delta = (n - p + 1\ \ldots\ n)$, so that δ has length p.
- $n = 7$, $\gamma = (1\ 2\ 3\ 4\ 5)$, $\delta = (3\ 4\ 5\ 6\ 7)$
- $n = 6$, $\gamma = (1\ 2\ 3\ 4\ 5)$, $\delta = (2\ 3\ 4\ 5\ 6)$
- $n = 5$, $\gamma = (1\ 2\ 3)$, $\delta = (3\ 4\ 5)$
- $n = 4$, $\gamma = (1\ 2\ 3)$, $\delta = (2\ 3\ 4)$

Before going on, one should keep in mind the following:

Definition 2.3. A group action $G \times X \to X$ is transitive if it possesses only a single group orbit, i.e., for every pair of elements $x, y \in X$, there is a group element g such that $gx = y$.

Definition 2.4. Consider a group action $G \times X \to X$. A group block is a subset Δ of X such that:

- $g\Delta = \Delta$, or
- $g\Delta \cap \Delta = \emptyset$.

Definition 2.5. A group action $G \times X \to X$ is said to be primitive if it is transitive and it has no nontrivial group blocks, i.e., denoting a group block with Δ, we can only have $\Delta = \{x\}$ for some $x \in X$ or $\Delta = X$. A group that has a faithful primitive group action is called a primitive group.

Theorem 2.6 (Jordan [5])**.** If a primitive permutation group G is a subgroup of the symmetric group S_n and contains a p-cycle for some prime number $p < n-2$, then G is either the whole symmetric group S_n or the alternating group A_n.

Lemma 2.2. Following the construction above, we get $S_n = \langle \alpha, \beta \rangle$ and $A_n = \langle \gamma, \delta \rangle$.

Proof. For $n \leq 7$ one can prove the result by hand. If $n > 7$, observe that $p + l(\beta) > n$, hence the support of the two permutations α and β intersect. For this reason $\langle \alpha, \beta \rangle$ is transitive. However, we can say more, because $\langle \alpha, \beta \rangle$ is transitive and it contains a cycle of length $p > n/2$, hence it is also primitive. By Jordan's Theorem, $\langle \alpha, \beta \rangle = A_n$ or S_n, and by our choice of the length of β it must be $\langle \alpha, \beta \rangle = S_n$. The same arguments show that $A_n = \langle \gamma, \delta \rangle$. □

Proposition 2.2. For any $n \geq 3$ and for any $2 \leq k \leq n-1$, S_n has an irredundant generating sequence of length k with elements of order a prime-power. Similarly, for any $n \geq 4$ and for any $2 \leq k \leq n-2$, A_n has an irredundant generating sequence of length k with elements of order a prime-power.

Proof. For any $t \geq 3$, we can construct $\alpha_t, \beta_t \in S_t$ as before, and observe that $\langle \alpha_t, \beta_t, (t\ t+1), (t{+}1\ t{+}2), \ldots, (n{-}1\ n) \rangle = S_n$, which is obvious by induction ($\langle S_{n-1}, (n{-}1\ n) \rangle = S_n$). It is also irredundant, indeed $\langle \alpha_t, \beta_t, (t\ t{+}1), \ldots, (x\ x{+}1), (x{+}2\ x{+}3), \ldots, (n{-}1\ n) \rangle$, for some integer $t \leq x \leq n-3$, maps $\{1, \ldots, x{+}1\}$ and $\{x{+}2, \ldots, n\}$ in themselves, respectively, hence it cannot be S_n; similarly, $\langle \beta_t, (t\ t+1) \ldots, (n-1\ n) \rangle$ fixes 1 and $\langle \alpha_t, (t\ t+1) \ldots, (n-1\ n) \rangle$ maps $\{1, \ldots, p\}$ in itself. Obviously, by construction, all the elements of the sequence have prime-power order.
Similarly, for any $t \geq 4$, we have $\langle \gamma_t, \delta_t, (t\ t+1\ t+2), (t\ t+1)(t+2\ t+3), (t\ t+1)(t+3\ t+4), \ldots, (t\ t+1)(n-1\ n) \rangle = A_n$ and this is again irredundant, indeed if we consider $\langle \gamma_t, \delta_t, (t\ t{+}1\ t{+}2), (t\ t{+}1)(t{+}2\ t{+}3), \ldots, (t\ t{+}1)(x\ x{+}1), (t\ t{+}1)(x{+}2\ x{+}3), \ldots, (t\ t{+}1)(n-1\ n) \rangle$ for some integer $t+2 \leq x \leq n-3$, we observe that it maps $\{x+2, \ldots, n\}$ in itself, hence it cannot be A_n; similarly, $\langle \gamma_t, \delta_t, (t\ t{+}1)(t{+}2\ t{+}3), \ldots, (t\ t{+}1)(n{-}1\ n) \rangle$ maps $\{(t\ t{+}1)\}$ in itself; finally, observe that $\langle \delta_t, (t\ t{+}1\ t{+}2), (t\ t{+}1)(t{+}2\ t{+}3), \ldots, (t\ t{+}1)(n{-}1\ n) \rangle$ and $\langle \gamma_t, (t\ t+1\ t+2), (t\ t+1)(t+2\ t+3), \ldots, (t\ t+1)(n-1\ n) \rangle$ map $\{1, \ldots, p\}$ and $\{n{-}p{+}1, \ldots, n\}$ in themselves, respectively. This construction provides then an irredundant generating sequence of elements of prime-power order for any k such that $2 \leq k < n-2$ (not for length $n-2$ because we did not define γ_3 and δ_3, however we already know the existence of a sequence in $\mathcal{S}(A_n)$ of length $n-2$ by Lemma 2.1 and the fact that $m(A_n) = n-2$ [13]), hence the proof is concluded. □

2.4 Expected number of subgroups in $\mathcal{F}$ to generate a finite group

Let G be a finite group and $\mathcal{F}$ a family of finite groups. If we fix a sequence $\{H_n\}_{n\in\mathbb{N}}$ of groups of $\mathcal{F}$, we can define a random variable $\tau_{G,\mathcal{F}}$ in the following way:

$$\tau_{G,\mathcal{F}} := \min\{n \geq 1 \mid \langle H_1, \dots, H_n\rangle = G\}$$

and also the probability that n elements of $\mathcal{F}$ generate G:

$$P_{G,\mathcal{F}}(n) := \frac{|\{(H_1, \dots, H_n) \text{ with } H_i \in \mathcal{F} \text{ and } H_i \leq G \mid \langle H_1, \dots, H_n\rangle = G\}|}{\sigma_{G,\mathcal{F}}(G)^n}.$$

In particular we get that $P(\tau_{G,\mathcal{F}} > n) = 1 - P_{G,\mathcal{F}}(n)$ so that we can introduce the expected number of subgroups of G in $\mathcal{F}$ needed to generate G:

$$e_{\mathcal{F}}(G) := \sum_{n\geq 1} nP(\tau_{G,\mathcal{F}} = n) = \sum_{n\geq 0}(1 - P_{G,\mathcal{F}}(n)).$$

Let $K \leq G$ and consider the probability to generate a subgroup of K with n subgroups of G in $\mathcal{F}$:

$$\left(\frac{\sigma_{G,\mathcal{F}}(K)}{\sigma_{G,\mathcal{F}}(G)}\right)^n = \sum_{H\leq K} P_{H,\mathcal{F}}(n).$$

Interpreting the first member of the above equality as a function of K, one can apply Theorem 1.2 and get the following equality:

$$P_{G,\mathcal{F}}(n) = \sum_{H\leq G} \mu_G(H) \left(\frac{\sigma_{G,\mathcal{F}}(H)}{\sigma_{G,\mathcal{F}}(G)}\right)^n.$$

Proposition 2.3. If G is a finite group and $\mathcal{F}$ a family of finite groups, then:

$$e_{\mathcal{F}}(G) = -\sum_{H<G} \frac{\mu_G(H)\sigma_{G,\mathcal{F}}(G)}{\sigma_{G,\mathcal{F}}(G) - \sigma_{G,\mathcal{F}}(H)}.$$

Proof.

$$e_{\mathcal{F}}(G) = \sum_{n\geq 0}(1 - P_{G,\mathcal{F}}(n)) = \sum_{n\geq 0}\left(1 - \sum_{H\leq G} \mu_G(H)\left(\frac{\sigma_{G,\mathcal{F}}(H)}{\sigma_{G,\mathcal{F}}(G)}\right)^n\right) =$$

$$= -\sum_{n\geq 0}\left(\sum_{H<G} \mu_G(H)\left(\frac{\sigma_{G,\mathcal{F}}(H)}{\sigma_{G,\mathcal{F}}(G)}\right)^n\right) = -\sum_{H<G}\left(\sum_{n\geq 0} \mu_G(H)\left(\frac{\sigma_{G,\mathcal{F}}(H)}{\sigma_{G,\mathcal{F}}(G)}\right)^n\right) =$$

$$= -\sum_{H<G} \frac{\mu_G(H)\sigma_{G,\mathcal{F}}(G)}{\sigma_{G,\mathcal{F}}(G) - \sigma_{G,\mathcal{F}}(H)}.$$

□

At this point we can implement the above formula:

```
G:=...;
list:=AllSubgroups(G);;
tom:=TableOfMarks(G);;
moebius:=MoebiusTom(tom);;
moebius.mu;;
firstml:=[]
for i in [1..Size(moebius.mu)] do
    firstml[i]:=GetWithDefault(moebius.mu,i,0);
od;
s:=1;;
ml:=[];;
ml[1]:=firstml[1];;
for i in [1..Size(list)-1] do
    if IsConjugate(G, list[i+1], list[i]) then
        ml[i+1]:=firstml[s];
    else ml[i+1]:=firstml[s+1];
        s:=s+1;
fi;
od;
f:=[];;
for i in [1..Size(list)] do
    if Is*desiredproperty*(list[i]) then
        f[i]:=list[i];
    else f[i]:=0;
fi;
od;
sigma:=[];;
for i in [1..Size(list)] do
    sigma[i]:=0;
od;
for i in [1..Size(list)] do
    for j in [1..Size(f)] do
        if IsSubgroup(list[i],f[j]) then
            sigma[i]:=sigma[i]+1;
fi;
od;
od;
el:=[];
for i in [1..Size(list)-1] do
    el[i]:=ml[i]*sigma[Size(list)]/(sigma[Size(list)]-sigma[i]);
od;
-Sum(el);
Float(-Sum(el));
```

Example 2.2. Let $\mathcal{F}_1$ be the family of cyclic groups and $\mathcal{F}_2$ be the family of nilpotent groups, then $e_{\mathcal{F}_1}(S_4) = \frac{7837}{2340} \sim 3,35$ and $e_{\mathcal{F}_2}(S_4) = \frac{517052}{168245} \sim 3,07$, as one can easily verify

applying the implementation above setting G=SymmetricGroup(4) and using the commands "IsCyclic" and "IsNilpotent" at line 22, respectively.

We are now interested in comparing $e_1(G)$ (the expected number of elements of G which are needed to generate it, [7]) and $e_{\mathcal{F}_1}(G)$. In particular, keep in mind the following, again from [7]:

Proposition 2.4. If G is a finite group, then:

$$e_1(G) = -\sum_{H<G} \frac{\mu_G(H)|G|}{|G|-|H|}.$$

We can add the following lines to the code above:

```
44 el2:=[];
45 for i in [1..Size(list)-1] do
46         el2[i]:=ml[i]*Size(G)/(Size(G)-Size(list[i]));
47 od;
48 -Sum(el2);
49 Float(-Sum(el2));
```

At this point we can just apply the GAP procedure to some finite groups. The following table contains the most relevant results:

Group	$e_1(G)$	$e_{\mathcal{F}_1}(G)$
C_p	$\frac{p}{p-1}$	2
S_3	2,90	2,92
S_4	3,09	3,35
S_5	2,85	2,97
A_4	2,47	2,76
A_5	2,46	2,80
Q_8	3,33	4,17
D_8	3,33	3,62
D_{10}	2,69	2,57
D_{14}	2,63	2,41
D_{16}	3,33	3,63
D_{18}	2,90	2,88
D_{22}	3,04	2,93
$PSL_2(7)$	2,38	2,66

The results above show that $e_1(G) > e_{\mathcal{F}_1}(G)$ only when $G = D_{10}, D_{14}, D_{18}, D_{22}$. This suggests that this may be true in general for D_{2n} with n odd. This can be proved if, in particular, n is prime:

Proposition 2.5. Let $p \neq 3$ be a prime, then $e_{\mathcal{F}_1}(D_{2p}) \leq e_1(D_{2p})$ and equality holds if and only if $p = 2$. In particular $e_{\mathcal{F}_1}(D_{2p}) = \frac{1}{p+1} + \frac{2}{p} + 2$.

Proof. As we have seen in Example 1.1, we have that $D_{2p} = \langle a, b \mid a^p = b^2 = e, bab = a^{-1} \rangle$, the only subgroups are the trivial group, the whole group, $\langle a \rangle$ and $\langle ba^j \rangle$ for $j = 0, \ldots, p-1$ (which are $p+1$ cyclic maximal subgroups, the first of order p and the others of order 2) and the Möbius function is the following: $\mu_{D_{2p}}(D_{2p}) = 1$, $\mu_{D_{2p}}(H) = -1$ for any non-trivial $H < G$ and $\mu_{D_{2p}}(\{1\}) = p$. Moreover, we can observe that $\sigma_{D_{2p},\mathcal{F}_1}(D_{2p}) = p + 2$, $\sigma_{D_{2p},\mathcal{F}_1}(\langle H \rangle) = 2$ for any non-trivial $H < G$ and obviously $\sigma_{D_{2p},\mathcal{F}_1}(\{1\}) = 1$.
Summing up, we get:

- $e_1(D_{2p}) = -\sum_{H<D_{2p}} \frac{\mu_{D_{2p}}(H)|D_{2p}|}{|D_{2p}|-|H|} = -\left(\frac{\mu_{D_{2p}}(\{1\})|D_{2p}|}{|D_{2p}|-|\{1\}|} + \sum_{j=0}^{p-1} \frac{\mu_{D_{2p}}(\langle ba^j \rangle)|D_{2p}|}{|D_{2p}|-|\langle ba^j \rangle|} + \right.$
  $\left. + \frac{\mu_{D_{2p}}(\langle a \rangle)|D_{2p}|}{|D_{2p}|-|\langle a \rangle|} \right) = -\frac{2p^2}{2p-1} + \sum_{j=0}^{p-1} \frac{2p}{2p-2} + \frac{2p}{2p-p} = -\frac{2p^2}{2p-1} + \frac{2p^2}{2p-2} + 2 = \frac{2p^2}{(2p-1)(2p-2)} + 2.$
- $e_{\mathcal{F}_1}(D_{2p}) = -\sum_{H<D_{2p}} \frac{\mu_{D_{2p}}(H)\sigma_{D_{2p},\mathcal{F}_1}(D_{2p})}{\sigma_{D_{2p},\mathcal{F}_1}(D_{2p})-\sigma_{D_{2p},\mathcal{F}_1}(H)} = -\frac{\mu_{D_{2p}}(\{1\})\sigma_{D_{2p},\mathcal{F}_1}(D_{2p})}{\sigma_{D_{2p},\mathcal{F}_1}(D_{2p})-\sigma_{D_{2p},\mathcal{F}_1}(\{1\})} -$
  $- \sum_{\{1\}<H<G} \frac{\mu_{D_{2p}}(\{H\})\sigma_{D_{2p},\mathcal{F}_1}(D_{2p})}{\sigma_{D_{2p},\mathcal{F}_1}(D_{2p})-\sigma_{D_{2p},\mathcal{F}_1}(H)} = -\frac{p(p+2)}{p+2-1} + \frac{(p+1)(p+2)}{p+2-2} = \frac{1}{p+1} + \frac{2}{p} + 2.$

Thus we get $e_{\mathcal{F}_1}(D_{2p}) < e_1(D_{2p})$ for any $p > 3$ and $e_{\mathcal{F}_1}(D_{2p}) = e_1(D_{2p})$ if and only if $p = 2$ (observe that we knew that the inequality is not true for $p = 3$, since $D_6 \simeq S_3$ and S_3 is in the table). □

Example 2.3. Consider the group $C_p \times C_p$ where $C_p = \langle x \rangle$ and p is prime. If we set $b := (x, 1)$ and $a := (1, x)$ one can immediately check that the only non-trivial subgroups are the $p+1$ maximal cyclic subgroups $\langle a \rangle$ and $\langle ba^j \rangle$ for $j = 0, \ldots, p-1$. In particular, we get $e_{\mathcal{F}_1}(C_p \times C_p) = e_{\mathcal{F}_1}(D_{2p}) = \frac{1}{p+1} + \frac{2}{p} + 2$.

Bibliography

[1] Aschbacher M., Guralnick R., *Solvable generation of groups and Sylow subgroups of the lower central series*, Journal of Algebra 77, 189–201, 1982.

[2] Burris S., Sankappanavar H. P., *A Course in Universal Algebra*, Springer, 2012.

[3] Cameron P. J., Cara P., *Independent generating sets and geometry for symmetric groups*, Journal of Algebra 258, 641-650, 2002.

[4] Collins D., Dennis R. K., *Irredundant generating sequences of finite groups*, pp. 1-4, 11-13, 2013.

[5] Dixon J. D., Mortimer B., *Permutation Groups*, Springer, 1996.

[6] Hall P., *The Eulerian functions of a group*, Quarterly Journal of Mathematics 7, 134–834 151, 1936

[7] Lucchini A., *The expected number of random elements to generate a finite group*, Monatsh Math 181, 123–142, 2015.

[8] Lucchini A., *The largest size of a minimal generating set of a finite group*, Arch. Math. 101, 1–8, 2013.

[9] Nagura J., *On the interval containing at least one prime number*, Proceedings of the Japan Academy 28, 177-181, 1952.

[10] Rota G., *On the foundations of Combinatorial theory. I. Theory of Moebius functions*, Z. Wahrsch. Verw. Gebiete 2, 340-368, 1964.

[11] Tarski A., *An interpolation theorem for irredundant bases of closure structures*, Discrete Math. 12, 185–192, 1975.

[12] The GAP Group, GAP-Groups, Algorithms, and Programming, Version 4.2, 2000, http://www.gap-system.org.

[13] Whiston J., *Maximal independent generating sets of the symmetric group*, J. Algebra 232, no. 1, 255–268, 2000.

[14] Whiston J., Saxl J., *On the maximal size of independent generating sets of* $PSL_2(q)$, J. Algebra 258, no. 2, 651–657, 2002.