Journal of the Iranian Mathematical Society
ISSN (on-line): 2717-1612
J. Iran. Math. Soc. 3 (2022), no. 2, 49-60

MINIMAL GENERATING SEQUENCES OF $\mathfrak{F}$-SUBGROUPS

A. LUCCHINI

Dedicated to Professor Derek J. S. Robinson

Abstract. The behaviour of generating sets of finite groups has been widely studied, from several points of view. The purpose of this note is to investigate what happens when, instead of sets of elements generating a group, sets of subgroups belonging to a prescribed family are considered. Some known results on generating set can be extended and generalized, using similar arguments and techniques, but interesting open questions also arise.

1. Generating sequences

Let $\mathfrak{F}$ be a family of finite groups. An $\mathfrak{F}$-sequence (of length n) of a finite group G is a sequence $(H_1, \dots, H_n)$ of $\mathfrak{F}$-subgroups of G, i.e. subgroups of G isomorphic to a group belonging to $\mathfrak{F}$. Moreover we say that an $\mathfrak{F}$-sequence $(H_1, \dots, H_n)$ of G is a generating $\mathfrak{F}$-sequence if $G = \langle H_1, \dots, H_n \rangle$ and that a generating $\mathfrak{F}$-sequence $(H_1, \dots, H_n)$ is minimal if $\langle H_1, \dots, H_{i-1}, H_{i+1}, \dots, H_n \rangle \neq G$ for every $1 \leq i \leq n$. We say that G is $\mathfrak{F}$-generated if G admits an $\mathfrak{F}$-generating sequence.

When G is $\mathfrak{F}$-generated we may define $d_{\mathfrak{F}}(G)$ and $m_{\mathfrak{F}}(G)$ as, respectively, the smallest and largest length of a minimal generating $\mathfrak{F}$-sequence of G. When $\mathfrak{F}$ is the family of all finite cyclic groups, then $d_{\mathfrak{F}}(G)$ and $m_{\mathfrak{F}}(G)$ coincide with the smallest and largest cardinality, $d(G)$ and $m(G)$ respectively, of a minimal generating set of G. While several results in the literature yield good estimates for $d(G)$, very little is known about $m(G)$. An exhaustive investigation [3, 15] was carried out for the finite symmetric groups, proving that $m(\mathrm{S}_n) = n - 1$ for each n, and giving a complete description of the

Communicated by Alireza Abdollahi

MSC(2020): Primary: 20F05; Secondary: 20D60, 20P05.

Keywords: Groups, subgroups, generating sets

Received: 30 October 2022, Accepted: 24 December 2022.

DOI: https://doi.org/10.30504/jims.2022.367761.1079

.

minimal generating sets of S_n having cardinality $n-1$. The problem of determining $m(G)$ in general remains open, even for finite simple groups, though partial results for certain families of these groups are given in [16].

We think that it would be interesting to study to which extent, and for which choices of $\mathfrak{F}$, known results about the cardinalities of minimal generating sets of finite groups can be generalized to results concerning the length of minimal generating $\mathfrak{F}$-sequences. There are some assumptions on the family $\mathfrak{F}$ that is reasonable to add. Assuming that $\mathfrak{F}$ contains all the finite cyclic groups ensures that every finite group G is $\mathfrak{F}$-generated, and indeed $d_{\mathfrak{F}}(G) \leq d(G)$ (of course the converse inequality is in general false, for example we have $d_{\mathfrak{F}}(G) = 1$ whenever $G \in \mathfrak{F}$). Also assuming that $\mathfrak{F}$ contains all the cyclic groups of prime power order is sufficient to ensure that every finite group G is $\mathfrak{F}$-generated (although in this case the inequality $d_{\mathfrak{F}}(G) \leq d(G)$ is not true anymore in general). Computing $d_{\mathfrak{F}}(G)$ is a difficult task. It is worth mentioning that a result proved by Aschbacher and Guralnick [1, Theorem A] ensures that $d_{\mathfrak{S}}(G) \leq 2$ for every finite group G, denoting by $\mathfrak{S}$ the family of finite soluble groups. By contrast, it has been shown by Cossey and Hawkes in [4] that there exists no bound for the number of nilpotent subgroups necessary to generate a finite group. In fact, for every natural number n, they construct a finite soluble group G_n which cannot be generated by fewer than n nilpotent subgroups. Much more can be said about $m_{\mathfrak{F}}(G)$. An easy but interesting result is the following:

Proposition 1.1. *If $\mathfrak{F}$ contains all the cyclic groups of prime power order, then $m(G) = m_{\mathfrak{F}}(G)$.*

Proof. Let $m = m(G)$ and $\mu = m_{\mathfrak{F}}(G)$. By [12, Lemma 2.3], G contains a minimal generating set $g_1, \dots, g_m$ with the property that $|g_i|$ is a prime power for $1 \leq i \leq m$. Clearly $(\langle g_1 \rangle, \dots \langle g_m \rangle)$ is a minimal generating sequence for G, and therefore $m \leq \mu$. Conversely, assume that $(H_1, \dots, H_\mu)$ is a minimal generating $\mathfrak{F}$-sequence for G. Clearly the union $H_1 \cup \cdots \cup H_\mu$ is a generating set of G and therefore it contains a minimal generating set, say Y, of G. For $1 \leq i \leq \mu$, there exists $y \in H_i \setminus (\cup_{j \neq i} H_j)$ (otherwise $G = \langle H_j \mid j \neq i \rangle$), but then $\mu \leq |Y| \leq m$. □

2. The Tarski irredundant basis theorem

A nice result in universal algebra, due to Tarski and known with the name of Tarski irredundant basis theorem (see for example [2, Theorem 4.4]), implies that, for every positive integer k with $d(G) \leq k \leq m(G)$, G contains a minimal generating set of cardinality k.

Theorem 2.1. *Suppose that the family $\mathfrak{F}$ contains all the finite cyclic groups and is closed under taking subgroups. For every finite group G and every $d_{\mathfrak{F}}(G) \leq k \leq m_{\mathfrak{F}}(G)$, there exists a minimal generating $\mathfrak{F}$-sequence of G of length k.*

Proof. Let $d = d_{\mathfrak{F}}(G)$ and $m = m_{\mathfrak{F}}(G) = m(G)$. Let X be a minimal generating set of G of cardinality m, and for any $g \in G$, denote by $l(g)$ the smallest length of a word expressing g as a product of elements of X. For any $H \leq G$, let $\mathcal{S}(H)$ be the set of the subsets of G generating H and define

$$l(H) := \min_{Y \in \mathcal{S}(H)} \left(\sum_{y \in Y} l(y) \right).$$

DOI: https://doi.org/10.30504/jims.2022.367761.1079

We are going to prove that if $k > d$ and there exists a minimal generating $\mathfrak{F}$-sequence of length k, then there exists also a minimal generating $\mathfrak{F}$-sequence of length $k-1$. Let Ω be the set of the minimal generating $\mathfrak{F}$-sequences of length strictly smaller than k. For any $\omega = (H_1, \dots, H_u) \in \Omega$, we set

$$\delta(\omega) = \max_{1 \leq i \leq u} l(H_i), \quad \nu(\omega) = |\{i \in \{1, \dots, u\} \mid l(H_i) = \delta(\omega)\}|.$$

Choose $\omega = (H_1, \dots, H_u) \in \Omega$ with the property that $(\delta(\omega), \nu(\omega))$ is minimal (in lexicographical order). Set $\delta = \delta(\omega)$. Without loss of generality, we may assume $l(H_u) = \delta$. Let $H_u = \langle h_1, \dots, h_t \rangle$ with $\sum_{1 \leq j \leq t} l(h_j) = \delta$. It cannot be $\delta = 1$, otherwise, for every $1 \leq i \leq u$, there exists $x_i \in X$ such that $H_i = \langle x_i \rangle$, and this would imply $G = \langle x_1, \dots, x_u \rangle$ with $u < k \leq m$, against the fact that X is a minimal generating set of G of cardinality m. If $t = 1$, then $\delta = l(h_1) \geq 2$, so there exist $g_1, g_2 \in G$ such that $h_1 = g_1 g_2$ and $l(g_1), l(g_2) < \delta$. In this case we set $\tilde{H}_u = \langle g_1 \rangle$ and $\tilde{H}_{u+1} = \langle g_2 \rangle$. If $t \geq 2$, we set $\tilde{H}_u = \langle h_1, \dots, h_{t-1} \rangle$ and $\tilde{H}_{u+1} = \langle h_t \rangle$. In both cases, let

$$\tilde{\omega} = (H_1, \dots, H_{u-1}, \tilde{H}_u, \tilde{H}_{u+1}).$$

Since $\mathfrak{F}$ contains all finite cyclic groups and is closed under taking subgroups, $\tilde{H}_u, \tilde{H}_{u+1} \in \mathfrak{F}$, and $\tilde{\omega}$ is a generating $\mathfrak{F}$-sequence of G. Hence $\tilde{\omega}$ contains a subsequence ω^*, which is a minimal generating $\mathfrak{F}$-sequence. Since $l(\tilde{H}_u), l(\tilde{H}_{u+1}) < l(H_u) = \delta$, we have that $\delta(\tilde{\omega}) \leq \delta(\omega)$ and if equality holds then $\nu(\tilde{\omega}) < \nu(\omega)$. Hence $(\delta(\omega^*), \nu(\omega^*)) \leq (\delta(\tilde{\omega}), \nu(\tilde{\omega})) < (\delta(\omega), \nu(\omega))$. By the minimality of $(\delta(\omega), \nu(\omega))$, it follows that $\omega^* \notin \Omega$, i.e. the length of the sequence ω^* is at least k. On the other hand, by construction, the length of ω^* is at most $u + 1 < k + 1$. This implies $u = k - 1$. □

Notice that the previous statement does not remain in general true if the assumptions that G contains all cyclic groups and is closed under taking subgroups are omitted. Suppose for example that $G \cong C_p^d$ is an elementary abelian p-group of rank $d \geq 3$ and that $\mathfrak{F}$ contains G and all finite cyclic groups, but does not contain C_p^u when $2 \leq u \leq d-1$. In this case (G) is a minimal generating $\mathfrak{F}$-sequence of length 1 but all the other minimal generating $\mathfrak{F}$-sequences have length d. A more interesting example is the following. Assume that $\mathfrak{F} = \{C_2, C_{73}\}$. The group $G = \mathrm{PSU}(3, 9)$ contains a minimal generating set consisting of four involutions and can also be generated by a pair of elements, one of order 2 and one of order 73. Thus there exist minimal generating $\mathfrak{F}$-sequences of length 2 and of length 4. However G cannot be generated with three involutions and every element x of order 73 generates G together with any involution or with any element y of order 73 such that $y \notin \langle x \rangle$. This implies that G does not admit minimal generating $\mathfrak{F}$-sequences of length 3.

3. Generating with elements of prime power order

An interesting but difficult question is whether an analogous of Theorem 2.1 holds for the family $\mathfrak{F}$ of the finite cyclic groups of prime power order. It can be reformulated in the following way. For a finite group G denote by $d_p(G)$ and $m_p(G)$ the smallest and largest cardinality of a minimal generating set of G consisting only of elements of prime power order. We have $d(G) \leq d_p(G) \leq m_p(G) = m(G)$, where the last equality follows from [12, Lemma 2.3].

DOI: https://doi.org/10.30504/jims.2022.367761.1079

Question 3.1. *Let G be a finite group and k be a positive integer with $d_p(G) \leq k \leq m_p(G)$. Does there exist a minimal generating set of G of cardinality k and consisting only of elements of prime power order?*

The question has an affirmative answer in the particular case when G is a finite soluble group.

Proposition 3.2. *If G is a finite soluble group and k is a positive integer with $d_p(G) \leq k \leq m_p(G)$, then G contains a minimal generating set of cardinality k and consisting only of elements of prime power order.*

Proof. For a finite group X denote by $\Delta_{\mathrm{pp}}(X,k)$ the set of the minimal generating sets of X of cardinality k and consisting only of elements of prime power order. We prove the statement by induction on the order of G. Let N be a minimal normal subgroup of G. Then N is a p-group for some prime p and for any element g having order a prime power modulo N, there exists a power of g, say $\tilde{g}$, such that $\tilde{g}$ has prime power order and $\langle g, N\rangle = \langle \tilde{g}, N\rangle$. If $N \leq \mathrm{Frat}(G)$, then $d_p(G) = d_p(G/N)$, $m_p(G) = m_p(G/N)$ and if $\{g_1N, \dots, g_kN\} \in \Delta_{\mathrm{pp}}(G/N,k)$, then $\{\tilde{g}_1, \dots, \tilde{g}_k\} \in \Delta_{\mathrm{pp}}(G,k)$. So we may assume $N \not\leq \mathrm{Frat}(G)$. In this case, N has a complement, say H, in G. Moreover $d_p(H) \leq d_p(G) \leq d_p(H)+1$ and, by [10, Lemma 12], $m_p(G) = m_p(H)+1$. Clearly we may assume $k > d_p(G)$. Hence $d_p(H) \leq k-1 \leq m_p(H)$, and, by induction, there exists $\{h_1, \dots, h_{k-1}\} \in \Delta_{\mathrm{pp}}(H, k-1)$. But then, for any $1 \neq n \in N$, $\{h_1, \dots, h_{k-1}, n\} \in \Delta_{\mathrm{pp}}(G,k)$. □

Question 3.1 has an affirmative answer also in the case of symmetric and alternating groups.

Proposition 3.3. *For any $n \geq 3$ and any $2 \leq k \leq n-1 = m_p(\mathrm{S}_{n-1})$, the symmetric group S_n contains a minimal generating set of length k consisting only of elements of prime power order.*

Proof. By [15, Theorem 1], $m_p(\mathrm{S}_n) = m(\mathrm{S}_n) = n-1$. For $r \geq 3$ define $\delta_r, \gamma_r \in \mathrm{S}_r$ as follows:

- $\gamma_3 = (1,2)$, $\delta_3 = (2,3)$;
- $\gamma_4 = (1,2,3)$, $\delta_4 = (3,4)$;
- $\gamma_5 = (1,2,3)$, $\delta_5 = (2,3,4,5)$;
- $\gamma_6 = (1,2,3,4,5)$, $\delta_6 = (2,4,5,6)$;
- $\gamma_7 = (1,2,3,4,5)$, $\delta_7 = (4,5,6,7)$;
- if $r > 7$, then $\gamma_r = (1,2,\dots,p)$, $\delta_r = (u, u+1, \dots, r)$, where p is a prime with $r/2 < p \leq r-3$ and $r-u+1$ is the largest 2-power smaller or equal than r.

We have in particular that $\langle \gamma_r, \delta_r\rangle = \mathrm{S}_r$. It can be easily checked that, if $r \geq 3$, then

$$\{\gamma_r, \delta_r, (r, r+1), (r+1, r+2), \dots, (n-1, n)\}$$

is a minimal generating set of S_n of cardinality $n-r+2$. □

Proposition 3.4. *For any $n \geq 4$ and any $2 \leq k \leq m_p(\mathrm{A}_n) = n-2$, the alternating group A_n contains a minimal generating set of length k consisting only of elements of prime order.*

Proof. In [15, Section 2] it is noticed that $m(\mathrm{A}_n) \leq n-2$. For $r \geq 4$ define $\delta_r, \gamma_r \in \mathrm{A}_r$ as follows:

DOI: https://doi.org/10.30504/jims.2022.367761.1079

- $\gamma_4 = (1,2,3)$, $\delta_4 = (2,3,4)$;
- $\gamma_5 = (1,2,3)$, $\delta_5 = (3,4,5)$;
- $\gamma_6 = (1,2,3,4,5)$, $\delta_6 = (2,3,4,5,6)$;
- $\gamma_7 = (1,2,3,4,5)$, $\delta_7 = (3,4,5,6,7)$;
- if $r > 7$, then $\gamma_r = (1,2,\dots,p)$, $\delta = (r-p+1,\dots,r)$, where p is a prime with $r/2 < p \leq r-3$.

We have in particular that $\langle \gamma_r, \delta_r \rangle = \mathrm{A}_r$. It can be easily checked that, if $r \geq 4$, then

$$\{\gamma_r, \delta_r, (2,3)(r,r+1), (2,3)(r+1,r+2), \dots, (2,3)(n-1,n)\}$$

is a minimal generating set of A_n of cardinality $n-r+2$. □

4. **Counting the generating sequences**

The Möbius function of a finite partially ordered set (poset) P is the map $\mu_P : P \times P \to \mathbb{Z}$ satisfying $\mu_P(x,y) = 0$ unless $x \leq y$, in which case it is defined inductively by the equations $\mu_P(x,x) = 1$ and $\sum_{x \leq z \leq y} \mu_P(x,z) = 0$ for $x < y$. Let f, g be functions defined from P to a commutative ring R with unity. The Möbius inversion formula states that

$$g(x) = \sum_{y \leq x} f(y) \text{ if and only if } f(x) = \sum_{y \leq x} \mu_P(y,x) g(y).$$

In a celebrated paper [6], P. Hall used for the first time the Möbius function $\mu_{\mathcal{L}(G)}$ of the subgroup lattice $\mathcal{L}(G)$ of a finite group G to compute the number $\phi(G,t)$ of generating t-tuples of G. Using the abbreviated notation $\mu_G(H)$ in place of $\mu_{\mathcal{L}(G)}(H,G)$, the formula proved by P. Hall can be written as follows:

$$\phi(G,n) = \sum_{H \leq G} \mu_G(H) |H|^n. \tag{4.1}$$

The argument used by P. Hall can be adapted to compute the cardinality $\phi_{\mathfrak{F}}(G,n)$ of the set $\Phi_{\mathfrak{F}}(G,n)$ of the generating $\mathfrak{F}$-sequences of G of length n. Indeed, denoting by $\sigma_{\mathfrak{F}}(X)$ the number of subgroups of X which belong to $\mathfrak{F}$, we have:

Proposition 4.1.

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

Proof. We clearly have $\sum_{K \leq H} \phi_{\mathfrak{F}}(K,n) = (\sigma_{\mathfrak{F}}(H))^n$, so the conclusion follows immediately by applying the Möbius inversion formula. □

Notice that $\phi_{\mathfrak{F}}(G,1) \neq 0$ if and only (G) is a generating $\mathfrak{F}$-sequence i.e. if and only if $G \in \mathfrak{F}$. Hence

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

By an unpublished result by D. Collins and K. Dennis, using the Möbius function of the subgroup lattice of a finite group G, the number $\psi(G,n)$ of the minimal generating sets of G of cardinality n

DOI: https://doi.org/10.30504/jims.2022.367761.1079

can also be computed. Indeed, denoting by $\Sigma_n(G)$ the set of the sequences $(H_1,\dots,H_n)$ of proper subgroups of G, we have

$$\psi(G,n)=|G|^n+(-1)^{n-1}\sum_{(H_1,\dots,H_n)\in\Sigma_n(G)}\left(\mu_G(H_1)\cdots\mu_G(H_n)\prod_{1\le i\le n}|\bigcap_{j\neq i}H_j|\right).$$

Let $\Phi_{\mathfrak{F}}(G,n)$ be the set of the generating $\mathfrak{F}$-sequences of G of length n. Given $(H_1,\dots,H_n)\in\Phi_{\mathfrak{F}}(G,n)$, we denote by $r(H_1,\dots,H_n)$ the smallest length of a subsequence of $(H_1,\dots,H_n)$ which still generates G. Moreover define

$$\Phi_{\mathfrak{F}}(G,k,n)=\{(H_1,\dots,H_n)\in\Phi_{\mathfrak{F}}(G,n)\mid r(H_1,\dots,H_n)\le k\}.$$

Notice that $\Psi_{\mathfrak{F}}(G,n):=\Phi_{\mathfrak{F}}(G,n,n)$ is the set of minimal generating $\mathfrak{F}$-sequences of G. Set $\phi_{\mathfrak{F}}(G,k,n)=|\Phi_{\mathfrak{F}}(G,k,n)|$ and $\psi_{\mathfrak{F}}(G,n)=|\Psi_{\mathfrak{F}}(G,n)|$.

Let $\tilde{\Sigma}_n(G)=\Sigma_n(G)\cup\{(G,\dots,G\}$. We may define a partial order on $\tilde{\Sigma}_n(G)$ by setting $(X_1,\dots,X_n)\le(Y_1,\dots,Y_n)$ if $X_i\le Y_i$ for each $1\le i\le n$.

Lemma 4.2. *If $(H_1,\dots,H_n)\in\Sigma_n(G)$, then*

$$\mu_{\tilde{\Sigma}_n(G)}((H_1,\dots,H_n),(G,\dots,G))=(-1)^{n-1}\mu_G(H_1)\cdots\mu_G(H_n).$$

Proof. It can be easily proved using the recursive definition of the Möbius function. □

Given $k\le n$, let $N=\binom{n}{k}$ and let $\pi_1,\dots,\pi_N$ be the subsets of $\{1,\dots,n\}$ of cardinality k. To any $(H_1,\dots,H_N)\in\Sigma_N(G)$ and any $i\in\{1,\dots,n\}$, we associate a subgroup of G defined as follows:

$$\tau_i(H_1,\dots,H_N)=\bigcap_{j\in\pi_i}H_j.$$

Let $\Lambda_{\mathfrak{F},n}(G)=\{(K_1,\dots,K_n)\mid K_i\le G \text{ and } K_i\in\mathfrak{F} \text{ for each } 1\le i\le n\}$. We define a function $\iota:\Lambda_{\mathfrak{F},n}(G)\to\tilde{\Sigma}_N(G)$ as follows: for $1\le j\le N$, let $H_j=\langle K_r\mid r\in\pi_j\rangle$; then $\iota(K_1,\dots,K_n)=(H_1,\dots,H_N)$ if $H_j\neq G$ for each j, $\iota(K_1,\dots,K_n)=(G,\dots,G)$ otherwise.

Lemma 4.3. *For any finite group G, we have*

$$\phi_{\mathfrak{F}}(G,k,n)=(\sigma_{\mathfrak{F}}(G))^n+(-1)^{N-1}\sum_{(H_1,\dots,H_N)\in\Sigma_N(G)}\left(\mu_G(H_1)\cdots\mu_G(H_N)\prod_{1\le i\le n}\sigma_{\mathfrak{F}}(\tau_i(H_1,\dots,H_N))\right).$$

Proof. We define $f:\tilde{\Sigma}_N(G)\to\mathbb{N}$ as follows: $f(H_1,\dots,H_N)$ is the number of $(K_1,\dots,K_n)\in\Lambda_{\mathfrak{F},n}(G)$ such that $\iota(K_1,\dots,K_n)=(H_1,\dots,H_N)$. Notice that

$$\phi_{\mathfrak{F}}(G,k,n)=f(G,\dots,G). \tag{4.2}$$

Define also $F:\tilde{\Sigma}_N(G)\to\mathbb{N}$ by setting:

$$F(H_1,\dots,H_n)=\sum_{(X_1,\dots,X_N)\le(H_1,\dots,H_N)}f(X_1,\dots,X_N).$$

DOI: https://doi.org/10.30504/jims.2022.367761.1079

In particular,

$$F(G,\dots,G)=\sum_{(H_1,\dots,H_N)\in\tilde{\Sigma}_N(G)} f(H_1,\dots,H_n)=(\sigma_{\mathfrak{F}}(G))^n. \tag{4.3}$$

If $(H_1,\dots,H_N)\in\Sigma_N(G)$, then $F(H_1,\dots,H_N)$ is the number of $(K_1,\dots,K_n)\in\Lambda_{\mathfrak{F},n}(G)$ such that $\langle K_i \mid i\in\pi_r\rangle\leq H_r$ for each $1\leq r\leq N$, or, equivalently, the number of $(K_1,\dots,K_n)\in\Lambda_{\mathfrak{F},n}(G)$ such that $K_s\in\tau_s(H_1,\dots,H_N)$ for each $1\leq s\leq n$. Thus

$$F(H_1,\dots,H_N)=\prod_{1\leq i\leq n}\sigma_{\mathfrak{F}}(\tau_i(H_1,\dots,H_N)).$$

By applying the Möbius inversion formula and Lemma 4.2, we obtain

$$\begin{aligned}\phi_{\mathfrak{F}}(G,k,n)=f(G,\dots,G)&=\sum_{(H_1,\dots,H_N)\in\tilde{\Sigma}_N(G)}\mu_{\tilde{\Sigma}_n(G)}((H_1,\dots,H_n),(G,\dots,G))F(H_1,\dots,H_n)\\&=F(G,\dots,G)+\sum_{(H_1,\dots,H_N)\in\Sigma_N(G)}(-1)^{N-1}\mu_G(H_1)\cdots\mu_G(H_N)F(H_1,\dots,H_n)\\&=(\sigma_{\mathfrak{F}}(G))^n+(-1)^{N-1}\sum_{(H_1,\dots,H_N)\in\Sigma_N(G)}\left(\mu_G(H_1)\cdots\mu_G(H_N)\prod_{1\leq i\leq n}\sigma_{\mathfrak{F}}(\tau_i(H_1,\dots,H_N))\right).\end{aligned}$$

□

Since $\psi_{\mathfrak{F}}(G,n)=\phi_{\mathfrak{F}}(G,n,n)$, the previous lemma implies the following corollary.

Corollary 4.4. *For any finite group G, we have*

$$\psi_{\mathfrak{F}}(G,n)=(\sigma_{\mathfrak{F}}(G))^n+(-1)^{n-1}\sum_{(H_1,\dots,H_n)\in\Sigma_n(G)}\left(\mu_G(H_1)\cdots\mu_G(H_n)\prod_{1\leq i\leq n}\sigma_{\mathfrak{F}}(\cap_{j\neq i}H_j)\right).$$

5. Probabilistic results

There are several important results in the literature estimating the probability $P(G,n)$ that n randomly chosen elements in G generates G. Notice that if follows immediately from (4.1) that

$$P(G,n)=\sum_{H\leq G}\frac{\mu_G(H)|H|^n}{|G|^n}. \tag{5.1}$$

In a similar way, it follows from Proposition 4.1, that the probability $P_{\mathfrak{F}}(G,n)$ that n randomly chosen $\mathfrak{F}$-subgroups of G generate G can be expressed by the formula:

$$P_{\mathfrak{F}}(G,n)=\sum_{H\leq G}\frac{\mu_G(H)(\sigma_{\mathfrak{F}}(H))^n}{(\sigma_{\mathfrak{F}}(G))^n}. \tag{5.2}$$

Let G be a nontrivial finite group and let $x=(x_n)_{n\in\mathbb{N}}$ be a sequence of independent, uniformly distributed G-valued random variables. We may define a random variable τ_G (a waiting time) by

$$\tau_G=\min\{n\geq 1 \mid \langle x_1,\dots,x_n\rangle=G\}\in[1,+\infty]$$

DOI: https://doi.org/10.30504/jims.2022.367761.1079

and consider the expectation $e(G) = \mathrm{E}(\tau_G)$ of this random variable. In other word $e(G)$ is the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. It follows from (5.1) (see [11, Theorem 1] and its proof) that

$$e(G) = -\sum_{H<G} \frac{\mu_G(H)|G|}{|G|-|H|}. \tag{5.3}$$

In a similar way, given a family $\mathfrak{F}$ of finite groups, let $y_{\mathfrak{F}} = (y_n)_{n\in\mathbb{N}}$ be a sequence of independent, uniformly distributed random variable taking value in the set of $\mathfrak{F}$-subgroups of G. We may consider the expectation $e_{\mathfrak{F}}(G)$ of the random variables $\min\{n \geq 1 \mid \langle y_1, \dots, y_n\rangle = G\}$, i.e. the expected number of $\mathfrak{F}$-subgroups of G needed to generate G. Using (5.2, the proof of [11, Theorem 1] can be adapted to obtain:

$$e_{\mathfrak{F}}(G) = -\sum_{H<G} \frac{\mu_G(H)\sigma_{\mathfrak{F}}(G)}{\sigma_{\mathfrak{F}}(G)-\sigma_{\mathfrak{F}}(H)}. \tag{5.4}$$

A consequence of the Classification of the Finite Simple Groups is that every finite simple group is 2-generated. So, for finite simple groups, it is natural to consider the asymptotic behaviour of $P(G,2)$ with respect to $|G|$. A nineteenth-century conjecture of Netto asserts that almost all pairs of permutations in A_n generate A_n . This was confirmed by J. D. Dixon in 1969 [5]. Dixon proposed the more general conjecture that if G a finite simple group, then $P(G,2) \to 1$ as $|G| \to \infty$. The proof of Dixon's conjecture was eventually completed in the 1990s. In [7], Kantor and Lubotzky established the result for classical groups and low rank exceptional groups, and the remaining groups of Lie type were handled by Liebeck and Shalev [9]. This suggests the following question.

Question 5.1. *Let $\mathfrak{F}$ be a family of finite groups containing all finite cyclic groups. Is it true that, when G runs in the family of the finite simple groups, $P_{\mathfrak{F}}(G,2) \to 1$ as $|G| \to \infty$?*

The proof of Dixon's conjecture relies on the easy observation that, denoting by $\mathcal{M}(G)$ the set of the maximal subgroups of a finite group G, the following inequality holds:

$$P(G,2) \geq 1 - \sum_{M\in\mathcal{M}(G)} |G:M|^{-2}. \tag{5.5}$$

The amount of information on the maximal subgroups of a finite simple group made available by the Classification of the Finite Simple Groups allows to prove that $\sum_{M\in\mathcal{M}(G)} |G:M|^{-2} \to 0$ as $|G| \to \infty$. In order to study $P_{\mathfrak{F}}(G,2)$, one should use, instead of (5.5), the following inequality:

$$P_{\mathfrak{F}}(G,2) \geq 1 - \sum_{M\in\mathcal{M}(G)} \frac{(\sigma_{\mathfrak{F}}(M))^2}{(\sigma_{\mathfrak{F}}(G))^2} \tag{5.6}$$

Thus in order to answer Question 5.1, one should deal with the problem of comparing $\sigma_{\mathfrak{F}}(G)/\sigma_{\mathfrak{F}}(M)$ with $|G|/|M|$, when M is a maximal subgroup of a finite simple group G. This is an interesting but not easy task. The first obstacle is the difficulty in giving good estimations of $\sigma_{\mathfrak{F}}(G)$ (even in the apparently easier case when $\mathfrak{F}$ is the family of all finite groups).

In the paper in which he settled Netto's conjecture, Dixon proved a more general result: the probability that a random pair of elements of the symmetric group S_n generates either S_n or the

DOI: https://doi.org/10.30504/jims.2022.367761.1079

alternating group A_n tends to 1 as n tends to infinity. Again we can ask whether this statement can be generalized to pairs of randomly chosen $\mathfrak{F}$-subgroups of S_n.

Question 5.2. *Denote by $\mathcal{P}_{\mathfrak{F}}(\mathrm{S}_n)$ the probability that a random pair of $\mathfrak{F}$-subgroups of the symmetric group S_n generates either S_n or the alternating group A_n. Does $\mathcal{P}_{\mathfrak{F}}(\mathrm{S}_n)$ tend to 1 as n tends to infinity?*

In the remaining part of this section we give an affirmative answer to the previous question in the particular case when $\mathfrak{F}$ is the family of finite cyclic groups. This requires some preliminary remarks and results.

Denoting by φ the Euler's totient function, by $o(x)$ the order of an element x of the finite group G and by $\sigma_c(G)$ the number of cyclic subgroups of G, we have that

$$\sigma_c(G) = \sum_{x \in G} \frac{1}{\varphi(o(x))}.$$

Lemma 5.3. *Let $k := \lfloor \log_2(n) \rfloor$. If $n \geq 32$ then*

$$\sigma_c(\mathrm{S}_n) \geq \frac{\sigma_c(\mathrm{S}_{n-1}) \cdot n}{k}.$$

More generally, if $1 \leq t \leq n/2$ and $n - t \geq 31$, then

$$\sigma_c(\mathrm{S}_n) \geq \frac{\sigma_c(\mathrm{S}_{n-t}) \cdot n \cdot (n-1) \cdots (n-t+1)}{k^t} = \frac{\sigma_c(\mathrm{S}_{n-t}) \cdot t!}{\lfloor \log_2(n) \rfloor^t} \cdot \binom{n}{t}.$$

Proof. Let $X := \{g \in \mathrm{S}_n \mid g(n) = n\} \cong \mathrm{S}_{n-1}$. For any $g \in \mathrm{S}_n$, denote by $\mathrm{fix}(g)$ the number of elements of $\{1, \ldots, n\}$ fixed by g. Similarly, if $H \leq \mathrm{S}_n$, denote by $\mathrm{fix}(H)$ the number of elements fixed by every element of H. Moreover, for any subgroup K of S_n, let $\sigma_c(K, t)$ be the number of cyclic subgroups C of K with $\mathrm{fix}(C) = t$. If $g \in X$, let α_g be the number of conjugates of g in S_n and let β_g be the number of conjugates of g in X. Notice that

$$\frac{\alpha_g}{\beta_g} = \frac{|G : C_G(g)|}{|X : C_X(g)|} = \frac{|G : X|}{|C_G(g) : C_X(g)|} = \frac{n}{\mathrm{fix}(g)}.$$

Let $\Delta_t = \{g \in \mathrm{S}_n \mid \mathrm{fix}(g) = t\}$ and let Γ_t be a set of representatives for the conjugacy classes of S_n contained in X. If $t \geq 1$, we may assume $\Gamma_t \subseteq X$ and

$$\sigma_c(\mathrm{S}_n, t) = \sum_{g \in \Delta_t} \frac{1}{\varphi(o(g))} = \sum_{y \in \Gamma_t} \frac{\alpha_y}{\varphi(o(y))} = \sum_{y \in \Gamma_t} \frac{\beta_y \cdot n}{t \cdot \varphi(o(y))} = \frac{n}{t} \cdot \sum_{g \in \Delta_t \cap X} \frac{1}{\varphi(o(g))} = \frac{n}{t} \cdot \sigma_c(X, t). \tag{5.7}$$

For any cyclic subgroup C of X, choose a generator for C and let A be the set of these generators. Moreover, for any $2 \leq t \leq n$, let $A_t = \{\alpha \in A \mid \mathrm{fix}(\alpha) = t\}$ and, for any $\alpha \in A$, let B_α be a set of generators for the cyclic subgroups of S_n whose support equal the set of elements fixed by α. Notice that $\Lambda_\alpha = \{\langle \alpha \cdot \beta \rangle \mid \beta \in B_\alpha\}$ consists of $(t-1)!/\varphi(t)$ fixed-point-free cyclic subgroups of S_n. Since $\Lambda_{\alpha_1} \cap \Lambda_{\alpha_2} = \emptyset$ whenever $\alpha_1 \neq \alpha_2$, we have that

$$\sigma_c(\mathrm{S}_n, 0) \geq \sum_{2 \leq t \leq n} \left(\sum_{\alpha \in A_t} |\Lambda_\alpha| \right) = \sum_{2 \leq t \leq n} \frac{\sigma_c(X, t)(t-1)!}{\varphi(t)} \geq \sum_{2 \leq t \leq n} \sigma_c(X, t)(t-2)!. \tag{5.8}$$

DOI: https://doi.org/10.30504/jims.2022.367761.1079

Combining (5.7) and (5.8), we obtain

$$\sigma_c(\mathrm{S}_n) = \sigma_c(\mathrm{S}_n, 0) + \sum_{1\le t\le n} \sigma_c(\mathrm{S}_n, t) \ge n\cdot\sigma_c(X,1) + \sum_{2\le t\le n} \sigma_c(X,t)\left(\frac{n}{t} + (t-2)!\right).$$

Let $k := \lfloor \log_2(n)\rfloor$. Since $n \ge 32$, we have $k \ge 5$. If $t \le k$, then $n/t + (t-2)! \ge n/t \ge n/k$. If $t > k$, then $n/t + (t-2)! \ge (t-2)! \ge (k-1)! \ge 2^{k+1}/k > n/k$. It follows

$$\sigma_c(\mathrm{S}_n) \ge \sum_{1\le t\le n} \sigma_c(X,t)\cdot\frac{n}{k} = \sigma_c(X)\cdot\frac{n}{k} = \sigma_c(\mathrm{S}_{n-1})\cdot\frac{n}{k}.$$

The proof of the more general statement is by induction on t. Suppose $2 \le t \le n/2$. Then

$$\begin{aligned}
\sigma_c(\mathrm{S}_n) &\ge \frac{\sigma_c(\mathrm{S}_{n-(t-1)})\cdot n\cdot(n-1)\cdots(n-(t-1)+1)}{k^{t-1}}\\
&= \frac{\sigma_c(\mathrm{S}_{n-t+1})\cdot n\cdot(n-1)\cdots(n-t+2)}{k^{t-1}}\\
&\ge \frac{\sigma_c(\mathrm{S}_{n-t})\cdot n\cdot(n-1)\cdots(n-t+2)\cdot(n-t+1)}{k^{t-1}\cdot\lfloor\log_2(n-t+1)\rfloor}\\
&\ge \frac{\sigma_c(\mathrm{S}_{n-t})\cdot n\cdot(n-1)\cdots(n-t+1)}{k^t}. \quad \square
\end{aligned}$$

Proposition 5.4. *Let $\mathfrak{M}$ be the family of the maximal subgroups of S_n, not containing A_n. Then*

$$\lim_{n\to\infty}\left(\sum_{M\in\mathfrak{M}}\left(\frac{\sigma_c(M)}{\sigma_c(\mathrm{S}_n)}\right)^2\right) = 0.$$

Proof. Since there are $(n-1)!/\varphi(n) \ge (n-2)!$ cyclic subgroups generated by the n-cycles, we have $\sigma_c(\mathrm{S}_n) \ge (n-2)!$.

By [14], $|M| \le 4^n$ for every M in the family $\mathfrak{P}$ of primitive maximal subgroups of S_n. Let $M_1,\dots,M_u$ be a set of representatives for the conjugacy classes of maximal subgroups in $\mathfrak{P}$. By [8, Theorem 4.4], if n is large enough, then $u \le n$. Since $\sigma_c(M) \le |M|$ for every $M \in \mathfrak{M}$, we have

$$\begin{aligned}
\sum_{M\in\mathfrak{P}}\left(\frac{\sigma_c(M)}{\sigma_c(\mathrm{S}_n)}\right)^2 &\le \sum_{M\in\mathfrak{P}}\left(\frac{|M|}{(n-2)!}\right)^2 = \sum_{1\le i\le u}\frac{|\,\mathrm{S}_n : M_i||M_i|^2}{((n-2)!)^2} = \sum_{1\le i\le u}\frac{n!|M_i|}{((n-2)!)^2}\\
&\le \sum_{1\le i\le u}\frac{n(n-1)4^n}{(n-2)!} \le \frac{n^2(n-1)4^n}{(n-2)!}.
\end{aligned}$$

If M varies in the family $\mathfrak{I}$ of imprimitive maximal subgroups of G, then we can use [13, Lemma 3.1(i)] and obtain that

$$\sum_{M\in\mathfrak{I}}\left(\frac{\sigma_c(M)}{\sigma_c(\mathrm{S}_n)}\right)^2 \le \sum_{M\in\mathfrak{I}}\left(\frac{|M|}{(n-2)!}\right)^2 = n^2(n-1)^2\sum_{M\in\mathfrak{I}}\frac{|M|^2}{|\,\mathrm{S}_n\,|^2} \le \frac{n^3(n-1)^2}{2^{(n+3)/2}}.$$

which tends to zero as $n\to\infty$.

DOI: https://doi.org/10.30504/jims.2022.367761.1079

Now assume M varies in the family $\mathcal{F}$ of intransitive subgroups of the form $\mathrm{S}_u \times \mathrm{S}_{n-u}$ with $6 \leq u < n/2$. Then

$$\sum_{M\in\mathcal{F}} \left(\frac{\sigma_c(M)}{\sigma_c(\mathrm{S}_n)}\right)^2 \leq \sum_{u=6}^{\lfloor n/2\rfloor} \binom{n}{u} \left(\frac{u!(n-u)!}{(n-2)!}\right)^2$$
$$= \sum_{u=6}^{\lfloor n/2\rfloor} \frac{n(n-1)u!(n-u)!}{(n-2)!} \leq \frac{n^2(n-1)6!(n-6)!}{(n-2)!}$$

Finally, if $n \geq 36$ and $u \leq 5$. then by Lemma 5.3,

$$\sum_{M\cong \mathrm{S}_u\times \mathrm{S}_{n-u}} \left(\frac{\sigma_c(M)}{\sigma_c(\mathrm{S}_n)}\right)^2 \leq \binom{n}{u} \left(\frac{(\log_2(n))^u}{\binom{n}{u}\cdot u!}\right)^2 \leq \frac{(\log_2(n))^{2u}}{\binom{n}{u}}.$$

We conclude that, if $n \geq 36$, then

$$\sum_{M\in\mathfrak{M}} \left(\frac{\sigma_c(M)}{\sigma_c(\mathrm{S}_n)}\right)^2 \leq \frac{n^2(n-1)4^n}{(n-2)!} + \frac{n^3(n-1)^2}{2^{(n+3)/2}} + \frac{n^2(n-1)6!(n-6)!}{(n-2)!} + \sum_{1\leq u\leq 5} \frac{(\log_2(n))^{2u}}{\binom{n}{u}},$$

which tends to zero as $n \to \infty$. □

Theorem 5.5. *Denote by $\mathcal{P}(\mathrm{S}_n)$ the probability that a random pair of cyclic subgroups of the symmetric group S_n generates either S_n or the alternating group A_n. Then $\mathcal{P}(\mathrm{S}_n)$ tends to 1 as n tends to infinity.*

Proof of Theorem 5.5. It suffices to notice that

$$\mathcal{P}(\mathrm{S}_n) \leq 1 - \sum_{M\in\mathfrak{M}} \left(\frac{\sigma_c(M)}{\sigma_c(G)}\right)^2$$

and apply the previous proposition. □

References

[1] M. Aschbacher and R. Guralnick, Solvable generation of groups and Sylow subgroups of the lower central series, *J. Algebra* **77** no. 1, (1982) 189–201.

[2] S. Burris and H. P. Sankappanavar, A course in universal algebra, Graduate Texts in Mathematics, **78**, Springer-Verlag, New York-Berlin, 1981.

[3] P. J. Cameron and P. Cara, Independent generating sets and geometries for symmetric groups, *J. Algebra* **258** (2002), no. 2, 641–650.

[4] J. Cossey and T. Hawkes, On generating a finite group by nilpotent subgroups, *J. Pure Appl. Algebra* **97** (1994), no. 3, 275–280.

[5] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969) 199–205.

[6] P. Hall, The Eulerian functions of a group, *Quart. J. Math. Oxford Ser.* **7** (1936) 134–151.

[7] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), no. 1, 67–87.

[8] M. W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups, *J. Combin. Theory Ser. A* **75** (1996), no. 2, 341–352 .

[9] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), no. 1, 103–113.

[10] A. Lucchini, The largest size of a minimal generating set of a finite group, *Arch. Math. (Basel)* **101** (2013), no. 1, 1–8.

DOI: https://doi.org/10.30504/jims.2022.367761.1079

[11] A. Lucchini, The expected number of random elements to generate a finite group, *Monatsh. Math.* **181** (2016), no. 1, 123–142.

[12] A. Lucchini and P. Spiga, Independent sets of generators of prime power order, *Expo. Math.* **40** (2022), no. 1, 140–154.

[13] A. Maróti and M. C. Tamburini, Bounds for the probability of generating the symmetric and alternating group, *Arch. Math. (Basel)* **96** (2011), no. 2, 115–121.

[14] C. Praeger and J. Saxl, On the orders of primitive permutation groups, *Bull. London Math. Soc.* **12** (1980), no. 4, 303–307.

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

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

Andrea Lucchini

Department of Mathematics Tullio Levi-Civita, University of Padova, Italy.

Email: lucchini@math.unipd.it

DOI: https://doi.org/10.30504/jims.2022.367761.1079