Invariable generation of permutation groups



*Published version:*
DOI: 10.1007/s00013-015-0749-2

# INVARIABLE GENERATION OF PERMUTATION GROUPS

ELOISA DETOMI AND ANDREA LUCCHINI

Abstract. Let $G$ be a finite permutation group of degree $n$ and let $d = 2$ if $G = \mathrm{Sym}(3)$, $d = [n/2]$ otherwise. We prove that there exist $d$ elements $g_1, \dots, g_d$ in $G$ with the property that $G = \langle g_1^{x_1}, \dots, g_d^{x_d} \rangle$ for every choice of $(x_1, \dots, x_d) \in G^d$.

## 1. Introduction

Following [4] we say that a subset $S$ of a group $G$ invariably generates $G$ if $G = \langle s^{g(s)} \mid s \in S \rangle$ for each choice of $g(s) \in G$, $s \in S$. Any finite group $G$ contains an invariable generating set (consider the set of representatives of each of the conjugacy classes).

Several papers deal with the question of bounding the minimal cardinality $d_I(G)$ of an invariable generating set for a finite group $G$ together with an analysis of the probability that $d$ independently and uniformly randomly chosen elements of $G$ invariably generate $G$ with good probability (see for example [2], [4], [5], [6], [7], [8], [10], [14]).

Clearly $d_I(G)$ is not less than the minimal cardinality $d(G)$ of a generating set of the finite group $G$. On the other hand, it follows from [7, Proposition 2.5] and [3, Theorem 1] that the difference $d_I(G)-d(G)$ can be arbitrarily large. Many results in the literature provide bounds for $d(G)$ in relation with different structural properties of $G$, so it is an open and interesting problem to which extent results on $d(G)$, the smallest cardinality of a generating set, can be generalized to comparable results on the smallest cardinality $d_I(G)$ of an invariable generating set. In this paper we consider the question of bounding the cardinality of an invariable generating set of a permutation group in terms of its degree.

The best bound for the cardinality of a generating set of a permutation group is due to A. McIver and P. Neumann: the so call "McIver-Neumann Half-$n$ Bound" says that if $G$ is a subgroup of $\mathrm{Sym}(n)$ and $G \neq \mathrm{Sym}(3)$, then $d(G) \leq [n/2]$. This result is stated without a proof in [11, Lemma 5.2] and a sketch of the proof is given in [1, Section 4]. It cannot be improved without imposing more restrictive conditions (for example transitivity) as is shown by

$$G = \langle (1,2), (3,4), \dots, (2m-1, 2m) \rangle \leq \mathrm{Sym}(2m).$$

Despite the fact that the difference $d_I(G) - d(G)$ can be quite large, the McIver-Neumann Half-$n$ Bound remains true with respect to the invariable generation of finite permutation groups. Indeed we have:

---

The research was partially supported by GNSAGA (INdAM).

2010 *Mathematics Subject Classification.* 20B05; 20F05.

Keywords: Invariable generation; finite permutation groups.

**Theorem 1.** *Let $G$ be a subgroup of* $\mathrm{Sym}(n)$*: either* $G = \mathrm{Sym}(3)$ *and* $d_I(G) = 2$ *or* $d_I(G) \le [n/2]$.

## 2. Preliminaries

If $N$ is a normal subgroup of $G$, then clearly $d_I(G/N) \le d_I(G)$ and we denote by $d_I(G, N)$ the difference $d_I(G) - d_I(G/N)$. When $N$ is a normal abelian subgroup of $G$, $d_G(N)$ denotes the minimal number of generators of $N$ as a $G$-module.

We collect in the following lemma some basic results on invariable generation.

**Lemma 2.** *Let $N$ be a normal subgroup of a group $G$.*

1. $d_I(G, N) \le d_I(N)$.
2. *If $N$ is abelian, then* $d_I(G, N) \le d_G(N)$.
3. *If $N$ is a minimal normal subgroup, then* $d_I(G, N) \le 1$ *if $N$ is abelian and* $d_I(G, N) \le 2$ *if $N$ is non-abelian.*

*Proof.* Parts (1) and (2) follow from the proofs of [8, Lemma 2.8] and [8, Lemma 2.10], respectively. Part (3) is Theorem 3.1 in [7]. □

By a wreath product $H \wr \mathrm{Sym}(s)$ we mean the usual semidirect product $W$ of the symmetric group $\mathrm{Sym}(s)$ and the $s$-fold direct power $H^s$ of the group $H$. The projection of $W$ onto $\mathrm{Sym}(s)$ corresponding to the semidirect decomposition will be denoted by $\pi$, the kernel $H^s$ of $\pi$ will be called base subgroup of $W$. If we consider $\pi$ as a permutation representation of $W$, a point stabiliser $W_i$ has a direct decomposition

$$W_i = H \times (H \wr \mathrm{Stab}_{\mathrm{Sym}(s)}(i)) \cong H \times (H \wr \mathrm{Sym}(s-1));$$

we denote by $\pi_i$ the projection of $W_i$ onto the first direct factor $H$. Following [9] we will use the following definition.

**Definition 3.** *A subgroup $G$ of $W = H \wr \mathrm{Sym}(s)$ is called* large *if*

- $\pi(G)$ *is transitive on* $\{1, \dots, s\}$,
- $\pi_1(G \cap W_1) = H$.

Note that, since $\pi(G)$ is transitive, the condition $\pi_1(G \cap W_1) = H$ is equivalent to have that $\pi_i(G \cap W_i) = H$ for all $i \in \{1, \dots, n\}$.

**Lemma 4.** *Let $A$ be a non-abelian minimal normal subgroup of $H$ and let $G$ be a large subgroup of $H \wr \mathrm{Sym}(s)$. If $A^s \cap G \neq 1$, then $A^s \cap G$ is a minimal normal subgroup of $G$.*

*Proof.* Suppose $M = A^s \cap G \neq 1$ and let $L$ be a minimal normal subgroup of $G$ contained in $M$. Since $G$ is large and $A$ is a minimal normal subgroup of $H$, both $M$ and $L$ are subdirect products of $A^s$. In particular $M$ is a centerless completely reducible group and $L$ is a direct factor of $M$. On the other hand, $C_{A^s}(L) = 1$, since $L$ is a subdirect product of $A^s$, hence $C_M(L) = 1$. Therefore $M = L$. □

**Lemma 5.** *Let $G$ be a large subgroup of $H \wr \mathrm{Sym}(s)$.*

1. $d_I(G, G \cap H^s) \le sa + 2b$ *where $a$ is the number of abelian factors in a composition series of $H$ and $b$ is the number of non-abelian factors in a chief series of $H$.*
2. *If* $u = \max\{d_I(X) \mid X \text{ subnormal subgroup of } H\}$*, then* $d_I(G, G \cap H^s) \le su$.

(3) *If $A$ is a minimal normal subgroup of $H$ of order $p^t$ for some prime $p$, then $d_I(G, G \cap A^s) \leq st - 1$.*

*Proof.* (1) We consider a chief series of $G$ passing through $G \cap H^s$ and we look at the factors $X/Y$ in this series with $X \leq G \cap H^s$. By Lemma 4 the number of the non-abelian factors is at most $b$. The number of the abelian factors is at most $sa$, since it is trivially bounded by the number of the abelian composition factors of $G \cap H^s$. Then we apply part 3 of Lemma 2.

(2) Let $K = \pi_1(G \cap H^s)$, and denote by $\tilde{\pi}_i$ the restriction of the projection $\pi_i$ to $G \cap H^s$, for $i = 1, \dots, s$. As $G$ is large, $K \trianglelefteq H$. Then $d_I(K) \leq u$ and, by part 1 of Lemma 2, we get

$$d_I(G \cap H^s) \leq d_I(K) + d_I(\ker(\tilde{\pi}_1)) \leq u + d_I(\ker(\tilde{\pi}_1)).$$

Now $\ker(\tilde{\pi}_1) \trianglelefteq G \cap H^s$, hence $\tilde{\pi}_2(\ker(\tilde{\pi}_1))$ is a normal subgroup of $K = \tilde{\pi}_2(G \cap H^s)$, and therefore it is subnormal in $H$. Then $d_I(\tilde{\pi}_2(\ker(\tilde{\pi}_1))) \leq u$ and thus

$$d_I(\ker(\tilde{\pi}_1)) \leq u + d_I(\ker(\tilde{\pi}_1) \cap \ker(\tilde{\pi}_2)).$$

By a repeated use of these arguments and the fact that $\cap_{i=1}^{s} \ker(\tilde{\pi}_i) = 1$, we deduce that $d_I(G \cap H^s) \leq su$.

(3) Since $G$ is large and $A$ is minimal normal in $H$, if $G \cap A^s = A^s$, then $G \cap A^s$ is a cyclic $G$-module. Otherwise, $G \cap A^s < A^s$, hence $G \cap A^s$ has at most $st - 1$ abelian composition factors, and thus $d_G(G \cap A^s) \leq st - 1$. Therefore, by Lemma 2, $d_I(G, G \cap A^s) \leq d_G(G \cap A^s) \leq st - 1$.

□

Let $G$ be a subgroup of $H \wr \mathrm{Sym}(s)$. If $U$ is an $\mathbb{F}_p H$-module, then $V = U^s$ can be viewed as an $\mathbb{F}_p G$-module by setting

$$(v_1, \dots, v_s)^{(h_1, \dots, h_s)\sigma} = (v_{1\sigma}^{h_{1\sigma}}, \dots, v_{s\sigma}^{h_{s\sigma}}),$$

where $(v_1, \dots, v_s) \in V$ and $(h_1, \dots, h_s)\sigma \in G$.

**Lemma 6.** *Let $G$ be a large subgroup of $H \wr \mathrm{Sym}(s)$ and let $U$ be an $\mathbb{F}_p H$-module. For any $\mathbb{F}_p G$-submodule $W$ of $V = U^s$ we have $d_G(W) \leq \frac{ds}{2}$, where $d$ is the dimension of $U$ over $\mathbb{F}_p$.*

*Proof.* Reverting to additive notation, we write $V = \sum_{1 \leq i \leq s} U_i$. Since $\pi(G)$ is transitive, there exists an element $g \in G$ such that $\pi(g)$ is fixed-point-free on $I = \{1, \dots, s\}$; $\pi(g)$ has $t$ orbits $I_1, \dots, I_t$ on $I$ with $t \leq [\frac{s}{2}]$. We can view $V$ as $\mathbb{F}_p[x]$-module, $x$ acting as $g$ does: $V$ is then the direct sum of the $\mathbb{F}_p[x]$-submodules $\tilde{U}_r = \sum_{i \in I_r} U_i$, $1 \leq r \leq t$ which have at most $d$ generators each, so that the $\mathbb{F}_p[x]$-module $V$ is $m$-generated for some $m \leq \frac{ds}{2}$; as $\mathbb{F}_p[x]$ is a principal ideal domain, the same is true for every submodule. Finally, if $W$ is an $\mathbb{F}_p G$-submodule of $V$, any set of $\mathbb{F}_p[x]$-generators of $W$ is also a set of $\mathbb{F}_p G$-generators.

□

## 3. Proof of Theorem 1

The case where $G$ is primitive follows from a bound on the length of a chief series.

**Proposition 7.** *Let $G$ be a primitive subgroup of degree $n$. Then $d_I(G) \leq 4 \log(n)$.*

*Proof.* By [12, Theorem 10.0.6], the chief length of a primitive subgroup of degree $n$ is at most $2\log(n)$. By Lemma 2 it follows that $d_I(G) \leq 4\log(n)$. □

**Corollary 8.** *Let $G$ be a primitive subgroup of degree $n \neq 3$. Then $d_I(G) \leq n/2$.*

*Proof.* For $n \geq 44$, by Proposition 7, $d_I(G) \leq 4\log(n) \leq n/2$. In the remaining cases, using the list of the primitive permutation groups of small degree, it is straightforward to check that $a+2b \leq n/2$ where $a$ in the number of abelian factors and $b$ is the number of non-abelian factors in a chief series of $G$ (and so we may conclude by Lemma 2), except when $G = \mathrm{Sym}(5)$ or $G = \mathrm{AGL}(1,5)$ and $n = 5$ or $G = \mathrm{Sym}(4)$ and $n = 4$. Then it is sufficient to check that $\mathrm{Sym}(5)$ is invariably generated by the set $\{(1,2),(1,2,3,4,5)\}$, $\mathrm{Sym}(4)$ is invariably generated by the set $\{(1,2,3),(1,2,3,4)\}$ and $\mathrm{AGL}(1,5)$ is invariably generated by any set consisting of an element of order 5 and an element of order 4. □

*Proof of Theorem 1.* Let $G$ be a finite permutation group of degree $n$. We have to show that

$$d_I(G) \leq \frac{n+\epsilon}{2}$$

where $\epsilon = 1$ if $n = 3$, $\epsilon = 0$ otherwise.

The proof is by induction on $n$, the cases $n \leq 3$ being trivial.

The case where $G$ is primitive, is actually Corollary 8.

**Case $G$ intransitive.** Suppose that $G \leq \mathrm{Sym}(n)$ is intransitive. Let $s$ be the size of an orbit and identify $G$ with a subgroup of $\mathrm{Sym}(s) \times \mathrm{Sym}(n-s)$. Let $\rho = \rho_{/G}$ the restriction to $G$ of the projection of $\mathrm{Sym}(s) \times \mathrm{Sym}(n-s)$ on the second factor of the direct product; then $\rho(G) \leq \mathrm{Sym}(n-s)$ and $\ker(\rho) \leq \mathrm{Sym}(s)$. By Lemma 2,

$$d_I(G) \leq d_I(\rho(G)) + d_I(\ker(\rho)).$$

If both $s$ and $n-s$ are not 3, then the inductive hypothesis gives $d_I(G) \leq (n-s)/2 + s/2 = n/2$ and we are done.

Now assume $s = 3$. If $\ker(\rho)$ is cyclic, then $d_I(\ker(\rho)) = 1$ and we have $d_I(G) \leq (n-3+\epsilon)/2+1 \leq n/2$ as desired. Otherwise $\ker(\rho) = \mathrm{Sym}(3)$. This implies that $G$ is actually isomorphic to a direct product of $\mathrm{Sym}(3)$ and a subgroup $H \leq \mathrm{Sym}(n-3)$; clearly we can assume $H \neq 1$. Let $h_1, \ldots, h_t$ be invariable generators for $H$. Then the set

$$\{((1,2),1),\ ((1,2,3),h_1),(1,h_2),\ldots,(1,h_t)\}$$

invariably generates $G$. Indeed, let $g_1, g_2, \ldots, g_t \in G$, with $g_1 = (x_1, y_1)$ and $g_2 = (x_2, y_2)$, and define

$$\begin{aligned} X &= \{((1,2),1)^{g_1},\ ((1,2,3),h_1)^{g_2},(1,h_2)^{g_3},\ldots,(1,h_t)^{g_t}\} \\ &= \{((1,2)^{x_1},1),\ ((1,2,3)^{x_2},h_1^{y_2}),(1,h_2)^{g_3},\ldots,(1,h_t)^{g_t}\}. \end{aligned}$$

Since $X$ contains $((1,2)^{x_1},1)^{((1,2,3)^{x_2},h_1^{y_2})} = (((1,2)^{x_1})^{(1,2,3)^{x_2}},1)$ and this element is not equal to $((1,2)^{x_1},1)$, $X$ contains the whole subgroup $\mathrm{Sym}(3) \times \{1\}$. Then, as $h_1, \ldots, h_t$ invariably generate $H \cong X/(\mathrm{Sym}(3) \times \{1\})$, we conclude that $X = G$. Therefore, $d_I(G) \leq d_I(H) + 1 \leq (n-3+\epsilon)/2 + 1 \leq n/2$ and the case when $G$ is intransitive is complete.

**Case $G$ imprimitive.** Suppose $G \leq \mathrm{Sym}(n)$ is transitive and imprimitive. Let $\Delta$ be a minimal block containing 1; then $n = rs$ where $r = |\Delta|$ and $s$ is the number of blocks in the system of imprimitivity containing $\Delta$. We denote by

$$\pi : G \mapsto \mathrm{Sym}(s)$$

the representation of $G$ on the blocks of the system, by $T$ the image of $\pi$, by $N$ the setwise stabiliser of $\Delta$ in $G$ and by $H$ the image of the representation of $N$ on $\Delta$. Thus $G$ is isomorphic to a large subgroup of $H \wr T$, where $H \leq \mathrm{Sym}(r)$ is primitive and $T \leq \mathrm{Sym}(s)$ is transitive.

Let $a$ be the number of abelian factors in a composition series of $H$ and let $b$ be the number of non-abelian factors in a chief series of $H$. By point 1 of Lemma 5,

$$d_I(G, G \cap H^s) \leq sa + 2b.$$

The inductive hypothesis gives $d_I(G/G \cap H^s) \leq (s + \epsilon)/2$ where $\epsilon = 1$ if $s = 3$, $\epsilon = 0$ otherwise, hence

$$d_I(G) \leq \frac{s+\epsilon}{2} + sa + 2b. \tag{3.1}$$

We want to prove that $d_I(G) \leq rs/2 = n/2$.

As $H$ is a primitive subgroup of $\mathrm{Sym}(r)$, by [13, Theorem 2.10] a composition series of $H$ has at most $\log(r)$ non-abelian factors and at most $3.25\log(r)$ abelian factors.

Then, by (3.1),

$$d_I(G) \leq \frac{s+\epsilon}{2} + 2\log(r) + 3.25\log(r)s.$$

Note that $\epsilon/2 + 2\log(r) \leq s\log(r)$, hence

$$d_I(G) \leq \frac{s}{2} + s\log(r) + 3.25\log(r)s = s(1/2 + 4.25\log(r)).$$

When $r > 48$ we have $1/2 + 4.25\log(r) \leq r/2$ and therefore

$$d_I(G) \leq \frac{rs}{2} = \frac{n}{2},$$

as desired.

We are left with the case where $r \leq 48$. We note that

$$\text{if } \; l(H) \leq \frac{r}{2} - 1, \;\text{ then } \; d_I(G) \leq \frac{n}{2}, \tag{3.2}$$

where $l(H)$ is the composition length of $H$. Indeed, as $(s + \epsilon)/2 \leq s$,

$$d_I(G) \leq \frac{s+\epsilon}{2} + sa + 2b \leq s + sl(H) \leq s + s\left(\frac{r}{2} - 1\right) = \frac{sr}{2} = \frac{n}{2}.$$

It is straightforward to check that for all primitive subgroups of degree $r \leq 48$ and $r \neq 2, 3, 4, 5, 7, 8, 9, 16$, we have $l(H) \leq r/2 - 1$ and hence, by (3.2), $d_I(G) \leq n/2$.

We are left to prove that $d_I(G) \leq n/2$ in the cases where $r = 2, 3, 4, 5, 7, 8, 9, 16$, and $H$ is a primitive subgroup of $\mathrm{Sym}(r)$ with composition length $l(H) > r/2 - 1$.

**Cases $r = 5, 7, 9$.**

If $s \neq 3$, then by induction $d_I(G/(G \cap H^s)) \leq s/2$. As $r$ is odd and $r \neq 3$, every subnormal subgroup of $H$ is invariably generated by at most $[r/2] = (r - 1)/2$

elements. By point (2) of Lemma 5, this implies that $d_I(G, G\cap H^s) \leq s(r-1)/2$ and we conclude that

$$d_I(G) \leq d_I(G/(G\cap H^s)) + d_I(G, G\cap H^s) \leq \frac{s}{2} + \frac{s(r-1)}{2} = \frac{sr}{2} = \frac{n}{2}.$$

Let now $s = 3$. If $r = 5$ and $l(H) > 5/2 - 1$, then $H \in \{D_{10}, C_{20}, \mathrm{Sym}(5)\}$. If $H = \mathrm{Sym}(5)$, then by formula (3.1), with $\epsilon = 1$, $a = 1$ and $b = 1$, it follows $d_I(G) \leq 2 + 3a + 2b \leq 7 \leq 15/2$. Otherwise $H$ has a minimal normal subgroup $A \cong C_5$ and $G/(G\cap A^3)$ is isomorphic to a subgroup of $C_4 \wr \mathrm{Sym}(3) \leq \mathrm{Sym}(12)$, hence, by induction, $d_I(G/(G\cap A^3)) \leq 12/2 = 6$. Moreover, $A^3$ is a completely reducible $G$-module, since the action is coprime, and hence $G\cap A^3$ is a cyclic $G$-module. Therefore, by point 2 in Lemma 2, $d_I(G) \leq 6 + 1 = 7 \leq 15/2$.

If $r = 7$ and $l(H) > 2$, then $H$ has a minimal normal subgroup $A \cong C_7$ with $G/(G\cap A^3)$ isomorphic to a subgroup of $C_6 \wr \mathrm{Sym}(3) \leq \mathrm{Sym}(18)$. By induction, $d_I(G/(G\cap A^3)) \leq 18/2 = 9$. As $A^3$ is a completely reducible $G$-module, $G\cap A^3$ is a cyclic $G$-module and thus $d_I(G) \leq 9 + 1 = 10 \leq 21/2$.

If $r = 9$ and $l(H) > 3$, then $H = C_3^2 \rtimes P$ where $P$ is a 2-group and every subgroup of $P$ is 2-generated. Then $A = C_3^2$ is a minimal normal subgroup of $H$ and by point (3) of Lemma 5 we have $d_I(G, G\cap A^3) \leq 3\cdot 2 - 1 = 5$. By point 2 in Lemma 5, $G/(G\cap A^3) \leq P \wr \mathrm{Sym}(3)$ is invariably generated by $3\cdot 2 + 2 = 8$ elements, and therefore it follows that $d_I(G) \leq 8 + 5 = 13 \leq 27/2$.

**Cases** $r = 2$.

The intersection $N = \mathrm{Sym}(2)^s \cap G$ is a $G$-submodule of $V = \mathrm{Sym}(2)^s$. By Lemma 6, $d_G(N) \leq [s/2]$. But then $d_I(G) \leq [s/2] + [(s+1)/2] = s$. □

**Case** $r = 3$.

Let $N = \langle (1,2,3)\rangle^s \cap G$. Notice that $G/N \leq C_2 \wr \mathrm{Sym}(s)$ so, by induction, $d_I(G/N) \leq s$. Moreover, by Lemma 6, $d_I(G, N) \leq d_G(N) \leq [s/2]$. Thus $d_I(G) \leq 3s/2$.

**Case** $r = 4$.

Consider the intersection $N = H^s \cap G$. By induction, $d_I(G/N) \leq (s+\epsilon)/2$. Let $A$ be the Klein subgroup of $\mathrm{Sym}(4)$.

If $N \leq A^s$, then by Lemma 6, $d_I(G, N) \leq d_G(N) \leq s$, and we are done.

From now on we will assume that $N > G\cap A^s$. For $1 \leq i \leq s$, consider the projection $\pi_i : H^s \to H$ and, for $i \geq 2$, call

$$N_i = N \cap \ker \pi_1 \cap \cdots \cap \ker \pi_{i-1},$$

and set $N_1 = N$. Note that each $N_i$ is a normal subgroup of $N$, hence, since $G$ is large, $\pi_i(N_i)$ is trivial, or a Klein subgroup, or $\mathrm{Alt}(4)$ or $\mathrm{Sym}(4)$; in particular, as $N > G\cap A^s$, $\pi_1(N_1)$ contains $\mathrm{Alt}(4)$.

Now set $x_{1,1} = (1,2,3)$, $x_{1,2} = (1,2,3,4)$ if $\pi_1(N) = \mathrm{Sym}(4)$, and $x_{1,2} = (1,2)(3,4)$ if $\pi_1(N) = \mathrm{Alt}(4)$. Let $\Omega = \{z_1, \ldots, z_t\}$ be a set of invariant generators of $G$ modulo $N$ with $t \leq (s+\epsilon)/2$. To this set we add two elements $y_{1,1}, y_{1,2} \in N$ with $\pi_1(y_{1,1}) = x_{1,1}$ and $\pi_1(y_{1,2}) = x_{1,2}$ and then, for each $i > 1$ with $\pi_i(N_i)$ non trivial, we add one element $y_i \in N_i$ whose image $x_i = \pi_i(y_i)$ is

- $(1, 2)(3, 4)$, if $\pi_i(N_i)$ is a Klein group;
- $(1, 2, 3)$, if $\pi_i(N_i) = \mathrm{Alt}(4)$;
- $(1, 2)$, if $\pi_i(N_i) = \mathrm{Sym}(4)$.

In this way we get a set $\tilde{\Omega}$ containing at most $\frac{s+\epsilon}{2} + 2 + s - 1 \leq 2s$ elements. We claim that they are invariable generators for $G$. Indeed let $\{g_\omega\}_{\omega\in\tilde{\Omega}}$ be any family of elements of $G$ and consider the subgroup $X = \langle \omega^{g_\omega} \mid \omega \in \tilde{\Omega}\rangle$ of $G$. Since $\tilde{\Omega}$ contains $\Omega$, we have that $XN = G$. To conclude that $X = G$, if suffices to prove that $\pi_i(X \cap N_i) = \pi_i(N_i)$ for each $i \in \{1, \ldots, s\}$ with $\pi_i(N_i) \neq 1$. First notice that $X$ contains $\overline{y_{1,1}} = {y_{1,1}}^{g_1}$ and $\overline{y_{1,2}} = {y_{1,2}}^{g_2}$ for suitable $g_1, g_2 \in G$ and since $G = XN$ we may assume $g_1, g_2 \in N$. But then there exist $h_1, h_2 \in H$ such that $\pi_1(\overline{y_{1,1}}) = {x_{1,1}}^{h_1}$ and $\pi_1(\overline{y_{1,2}}) = {x_{1,2}}^{h_2}$. On the other hand $\langle {x_{1,1}}^{h_1}, {x_{1,2}}^{h_2}\rangle = \langle x_{1,1}, x_{1,2}\rangle = \pi_1(N)$, hence $\pi_1(X\cap N) = \pi_1(N)$. As $G = XN$, we have that $\pi(X)$ acts transitively on $H^s$ and consequently $\pi_i(X \cap N) = \pi_1(X \cap N) = \pi_1(N_1) \geq \mathrm{Alt}(4)$ for every $i$. Now let $i \geq 2$ with $\pi_i(N_i) \neq 1$. There exists $n \in N$ such that $y_i^n \in X \cap N_i$ and consequently $\pi_i(y_i^n) = x_i^m \in \pi_i(N_i \cap X)$ for some $m \in \pi_1(N)$. Since $X \cap N$ normalizes $X \cap N_i$ and $\pi_i(X \cap N) = \pi_1(N)$ we have that

$$\pi_i(X \cap N_i) \geq \langle x_i^l \mid l \in \pi_1(N)\rangle \geq \langle x_i^l \mid l \in \mathrm{Alt}(4)\rangle = \pi_i(N_i).$$

Therefore, $\pi_i(X \cap N_i) = \pi_i(N_i)$ for every $i \in \{1, \ldots, s\}$.

**Case** $r = 8$.

We have three possibilities for $H$, where $H$ is a primitive group of degree 8 whose composition length is at least 4: $\mathrm{AGL}(1, 8), \mathrm{A\Gamma L}(1, 8), \mathrm{ASL}(3, 2)$. In the first two cases every subnormal subgroup of $X$ can be invariably generated by 3 elements, so by Lemma 5, $d_I(G) \leq 3s + (s + 1)/2 \leq 4s$. In the third case $H$ has a minimal normal subgroup $N$ of order $2^3$ and $H/N \cong \mathrm{SL}(3, 2)$ is a non abelian simple group, so, by Lemma 5, $d_I(G) \leq (3s - 1) + 2 + (s + \epsilon)/2 \leq 4s$.

**Case** $r = 16$.

There are four possibilities for $H$ being primitive of degree 16 and with $l(H) \geq 8$. In any case $H = V \rtimes X$ where $V \cong C_2^4$ and $X$ is a soluble irreducible subgroup of $\mathrm{GL}(4, 2)$. More precisely

$$X \in \{\mathrm{Sym}(3)^2, \mathrm{Sym}(3)^2 \rtimes C_2, (C_3 \times C_3) \rtimes C_4, C_{15} \rtimes C_4.\}.$$

Let $N = V^s \cap G$. Since $N \leq C_2^{4s}$ we have $d_I(G, N) \leq d_I(N) \leq 4s$, so it suffices to prove that $d_I(G/N) \leq 4s$. We have that $G/N$ is a large subgroup of $X \wr \mathrm{Sym}(s)$. If $X \in \{\mathrm{Sym}(3)^2, \mathrm{Sym}(3)^2 \rtimes C_2\}$, then $X$ has a faithful permutational representation of degree 6, so $G/N$ can be identified with a subgroup of $\mathrm{Sym}(6s)$ and $d_I(G/N) \leq 3s$ by induction. Otherwise it can be easily seen that every subnormal subgroup of $X$ can be invariably generated by 2 elements, so by Lemma, 5, $d_I(G/N, (H^s \cap G)/N) \leq 2s$, while, by induction, $d(G/(H^s \cap G)) \leq (s + 1)/2$: we conclude that $d_I(G/N) \leq 2s + (s + 1)/2 \leq 4s$.

## References

1. P. Cameron, R. Solomon, A. Turull, Chains of subgroups in symmetric groups. J. Algebra 127 (1989), no. 2, 340–352.

2. E. Detomi, A. Lucchini, Invariable generation with elements of coprime prime-power order, Journal of Algebra (2015), pp. 683-701; doi:10.1016/j.jalgebra.2014.10.037.
3. E. Detomi, A. Lucchini, Invariable generation of prosoluble groups, to appear on Israel J. Math., arXiv:1410.5271
4. J. D. Dixon, Random sets which invariably generate the symmetric group, Discrete Math. 105 (1992) 25–39.
5. J. Fulman, R. Guralnick, Derangements in simple and primitive groups, in: A.A. Ivanov, M.W. Liebeck, J. Saxl (Eds.), Groups, Combinatorics and Geometry, Durham 2001, World Sci. Publ., River Edge, NJ, 2003, pp. 99–121.
6. R. Guralnick, G. Malle, Simple groups admit Beauville structures, J. Lond. Math. Soc. (2) 85 (2012), no. 3, 694–721.
7. W. M. Kantor, A. Lubotzky, A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, J. Algebra 348 (2011), 302–314.
8. W. M. Kantor, A. Lubotzky, A. Shalev, Invariable generation of infinite groups, J. Algebra 421 (2015), 296310.
9. L. G. Kovács, Primitive subgroups of wreath products in product action, Proc. London Math. Soc. (3) 58 (1989), no. 2, 306-322.
10. T. Luczak, L. Pyber, On random generation of the symmetric group, Combin. Probab. Comput. 2 (1993) 505–512.
11. A. McIver, P. Neumann, Enumerating finite groups. Quart. J. Math. Oxford Ser. (2) 38 (1987), no. 152, 473-488.
12. N. Menezes, Random generation and chief length of finite groups, PhD Thesis, http://research-repository.st-andrews.ac.uk/handle/10023/3578
13. L. Pyber, Asymptotic results for permutation groups. Groups and computation (New Brunswick, NJ, 1991), 197219, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 11, Amer. Math. Soc., Providence, RI, 1993.
14. A. Shalev, A theorem on random matrices and some applications, J. Algebra 199 (1998) 124–141.


Eloisa Detomi and Andrea Lucchini,, Università degli Studi di Padova,, Dipartimento di Matematica,, Via Trieste 63, 35121 Padova, Italy