

ON THE BASE SIZE AND MINIMAL DEGREE OF TRANSITIVE GROUPS

LORENZO GUERRA, ATTILA MARÓTI, FABIO MASTROGIACOMO, AND PABLO SPIGA

ABSTRACT. Let G be a permutation group, and denote with $\mu(G)$ and $b(G)$ its minimal degree and base size respectively. We show that for every $\varepsilon > 0$, there exists a transitive permutation group G of degree n with

$$\mu(G)b(G) \geq n^{2-\varepsilon}.$$

We also identify some classes of transitive and intransitive groups whose base size and minimal degree have a smaller upper bound, shared with primitive groups.

1. INTRODUCTION

Let G be a finite permutation group acting on a set Ω . The *minimal degree* of G , denoted by $\mu(G)$, is the smallest number of elements of Ω that are moved by any non-identity element of G . A base for G is a sequence of points $(\omega_1, \dots, \omega_\ell)$ of Ω with trivial pointwise stabilizer, that is,

$$G_{\omega_1, \dots, \omega_\ell} = 1.$$

The *base size* of G , denoted by $b(G)$, is the smallest cardinality of a base for G .

Both the base size and the minimal degree have been extensively studied, especially in the context of primitive groups. Except for their product, most results in the literature treat these two invariants separately. A simple yet fundamental inequality relating these quantities is the following: if G is a transitive group of degree n , then

$$\mu(G)b(G) \geq n,$$

see for example [1, Exercise 3.3.7].

Known results on base size provide a natural upper bound for this product. For instance, it is shown in [7] that if G is a primitive group of degree n which is not large-base (i.e., not a wreath product action of two symmetric groups where the first acts on subsets), then

$$b(G) \leq 2 + \log n.$$

Using this, we can easily obtain that the bound

$$\mu(G)b(G) \leq n(2 + \log n).$$

holds for such primitive groups.

Nonetheless, this bound is not optimal and admits numerous exceptions. A more refined estimate was provided in [6], where a bound holds for all but one primitive group. Specifically, [6, Theorem 1.2] states that if G is a primitive group of degree n , different from the Mathieu group of degree 24, then

$$\mu(G)b(G) \leq n \log n.$$

These results heavily rely on the deep structural knowledge of primitive groups, and much less is known for non primitive groups.

Key words and phrases. base size, minimal degree, transitive, p -group, multinomial coefficient.

The first three authors are members of the GNSAGA INdAM research group and kindly acknowledge their support. The first and fourth authors are funded by the European Union via the Next Generation EU (Mission 4 Component 1 CUP B53D23009410006, PRIN 2022, 2022PSTWLB, Group Theory and Applications). The second author was supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K138596, No. K132951 and Grant No. K138828.

This is a common fact: while results concerning base size and minimal degree abound for primitive groups, considerably less is known for transitive—and even less for intransitive—groups. Noteworthy in this context is [4, Theorem A], where a bound on the order of an arbitrary permutation group is given in terms of its minimal degree.

The goal of this paper is to investigate the product $\mu(G)b(G)$ for imprimitive groups. In Section 2, we give evidences that a bound similar to the one of [6, Theorem 1.2] holds for some classes of transitive or even intransitive groups. In particular, Lemma 2.1 shows that the bound holds for a wreath product group endowed with its imprimitive action, while Lemma 2.2 establishes the bound for quasiprimitive groups, for Sylow subgroups of symmetric groups and for maximal subgroups of symmetric groups.

Motivated by the results in Section 2, we initially conjectured that a bound similar to the one established in [6] would also hold for all transitive groups. However, to our surprise, this is not the case. Indeed, recall that since for every permutation group G of degree n both $\mu(G)$ and $b(G)$ are at most n , then $\mu(G)b(G) \leq n^2$. We show that $\mu(G)b(G)$ can, in fact, be arbitrarily close to n^2 . Our main result provides a precise characterization of this behavior.

Theorem 1.1. *For every $\varepsilon > 0$, there exists a transitive permutation group of degree n such that*

$$\mu(G)b(G) \geq n^{2-\varepsilon}.$$

The proof of Theorem 1.1 is presented in Section 3, and it relies on the descending series of a wreath product of two vector spaces over the field with p element, for some prime number p .

2. THE BOUND FOR SOME PERMUTATION GROUPS

Lemma 2.1. *Let $G = H \wr T$ be a finite transitive permutation group acting on a set Ω of size n where H is a primitive permutation group acting on a set Σ which is a block for G in Ω and where T is a nontrivial transitive permutation group acting on the system of imprimitivity defined by Σ . Then $\mu(G)b(G) \leq n \log n$.*

Proof. Put $n = |\Omega|$ and $k = |\Sigma|$. We have $b(G) \leq b_\Sigma(H)(n/k)$ and $\mu(G) \leq \mu_\Sigma(H)$ where $b_\Sigma(H)$ denotes the minimal base size of H acting on Σ and $\mu_\Sigma(H)$ denotes the minimal degree of H acting on Σ . If H is different from the 5-transitive Mathieu group of degree 24, then $\mu(G)b(G) \leq (k \log k)(n/k) = n \log k \leq n \log n$, otherwise $\mu(G)b(G) \leq (16 \cdot 7)(n/24) \leq n \log 48 \leq n \log n$ by [6, Theorem 1.2] \square

Lemma 2.2. *Let G be a permutation group acting on a finite set Ω of size n . Let G be different from the 5-transitive Mathieu group of degree 24. If G*

- (1) *is quasiprimitive, or*
- (2) *is a Sylow subgroup of $\text{Sym}(\Omega)$ or*
- (3) *is a maximal subgroup therein,*

then $\mu(G)b(G) \leq n \log n$.

Proof. First let G be transitive. If G is primitive, then the claim follows from [6, Theorem 1.2]. Let G be different from a primitive group. Let G be quasiprimitive. Let \mathcal{B} be a maximal system of blocks in Ω defined from a nontrivial block Σ . Let $k = |\Sigma|$. Since G is quasiprimitive, $b(G) \leq b_{\mathcal{B}}(G)$ and $\mu(G) \leq \mu_{\mathcal{B}}(G)k$. This gives $\mu(G)b(G) \leq (n/k) \log(n/k)k$ by [6, Theorem 1.2], which is at most $n \log n$. This proves (1).

We continue to assume that G is transitive. If G is a (transitive) Sylow p -subgroup of $\text{Sym}(\Omega)$ for some prime p , then (2) follows from Lemma 2.1 by taking H to be the cyclic group of order p and T a Sylow p -subgroup of the symmetric group of degree n/p . If G is a maximal imprimitive subgroup of $\text{Sym}(\Omega)$, then $\mu(G)b(G) \leq n \log n$, again by Lemma 2.1 by taking both H and T to be symmetric groups. This completes the proof of (3) in case G is transitive.

Let G act intransitively on Ω . Let $G = G_1 \times \cdots \times G_r$ be a Sylow subgroup of $\text{Sym}(\Omega)$ where each G_i is a transitive Sylow subgroup of $\text{Sym}(\Omega_i)$ for subsets Ω_i of Ω partitioning Ω . We may assume that each G_i is nontrivial. We have $\mu(G) \leq \min_i \{\mu_{\Omega_i}(G_i)\}$ and $b(G) \leq \sum_{i=1}^r b_{\Omega_i}(G_i)$. This and the previous paragraph give $\mu(G)b(G) \leq \sum_{i=1}^r |\Omega_i| \log |\Omega_i| \leq \sum_{i=1}^r |\Omega_i| \log n = n \log n$. This completes the proof of (2). Similarly, if G is maximal (and intransitive) in $\text{Sym}(\Omega)$, then $\mu(G)b(G) = 2(n-2) \leq n \log n$, completing the proof of (3). \square

3. PROOF OF THEOREM 1.1

Let a be a positive integer, let p a prime number, and let V be an a -dimensional vector space over the field \mathbb{F}_p with p elements. We regard V as a transitive regular subgroup of the symmetric group $\text{Sym}(V)$.

Next, we let $W = \mathbb{F}_p \text{wr} V$ and $B = \mathbb{F}_p^V$ be the base group of the wreath product W . We regard W as a transitive subgroup of the symmetric group $\text{Sym}(\mathbb{F}_p \times V)$ endowed with its imprimitive action of degree $n = |\mathbb{F}_p \times V| = p^{a+1}$.

We let $B_0 = B$ and, for each positive integer i , we define recursively

$$B_i = [B_{i-1}, V].$$

An element of $B_0 = \mathbb{F}_p^V$ is a function from V to \mathbb{F}_p . For what follows, it is useful to identify B_0 with a certain coordinate ring.

Let X_1, \dots, X_a be indeterminates, and consider the polynomial ring $\mathbb{F}_p[X_1, \dots, X_a]$ with coefficients in \mathbb{F}_p . Now consider the evaluation map

$$\mathbb{F}_p[X_1, \dots, X_a] \rightarrow \mathbb{F}_p^V = B$$

that sends a polynomial $f(X_1, \dots, X_a)$ to the function which maps each $v = (v_1, \dots, v_a) \in V = \mathbb{F}_p^a$ to $f(v_1, \dots, v_a) \in \mathbb{F}_p$. This is a surjective map whose kernel is the ideal

$$(X_1^p - X_1, \dots, X_a^p - X_a).$$

We write x_i for the image of X_i in the quotient ring, and identify B_0 with the coordinate ring $\mathbb{F}_p[x_1, \dots, x_a]$. In particular, each element f of B_0 is a polynomial function

$$(1) \quad f = \sum_{\lambda_1, \dots, \lambda_a=0}^{p-1} a_{\lambda_1, \dots, \lambda_a} x_1^{\lambda_1} \cdots x_a^{\lambda_a},$$

where $a_{\lambda_1, \dots, \lambda_a} \in \mathbb{F}_p$ for each atuple $(\lambda_1, \dots, \lambda_a)$. For not making the notation too cumbersome, given an atuple $\bar{\lambda} = (\lambda_1, \dots, \lambda_a)$, we denote with $x_{\bar{\lambda}}$ the monomial $\prod_i x_i^{\lambda_i}$.

Now, let $f \in B_0$ be as in (1) and let $v \in V$. Then,

$$[f, v] = -f + f^v = \sum_{\bar{\lambda}} a_{\bar{\lambda}} (x_{\bar{\lambda}}^v - x_{\bar{\lambda}}).$$

Observe that

$$\begin{aligned} (x_{\bar{\lambda}}^v - x_{\bar{\lambda}})(w_1, \dots, w_a) &= x_{\bar{\lambda}}(v_1 + w_1, \dots, v_a + w_a) - x_{\bar{\lambda}}(w_1, \dots, w_a) \\ &= \prod_i (v_i + w_i)^{\lambda_i} - \prod_i w_i^{\lambda_i}, \end{aligned}$$

and hence,

$$x_{\bar{\lambda}}^v - x_{\bar{\lambda}} = \prod_i (x_i + v_i)^{\lambda_i} - x_{\bar{\lambda}}.$$

Expanding the product $\prod_i (x_i + v_i)^{\lambda_i}$, we see that the term $\prod_i x_i^{\lambda_i}$ cancels out with $x_{\bar{\lambda}}$. Therefore, the commutator of an element $f \in B_0$ of degree d and an element $v \in V$ is an element of B_0 degree at most $d-1$. From this, arguing inductively, it immediately follows that

$$B_d \subseteq \{f \in B_0 \mid \deg f \leq a(p-1) - d\}.$$

Observe now that, for every $1 \leq i \leq a$, we have

$$(2) \quad x_{\bar{\lambda}+e_i} = \prod_{j \neq i} x_j^{\lambda_j} (x_i + 1) - \prod_{j=1}^i x_j^{\lambda_j} = x_{\bar{\lambda}}^{e_i} - x_{\bar{\lambda}},$$

where $\{e_1, \dots, e_a\}$ is the canonical basis of V . Now, (2) and an elementary induction yields

$$(3) \quad B_d = \{f \in B \mid \deg f \leq a(p-1) - d\}.$$

Observe that $B_{a(p-1)}$ consists of all constant functions. We have

$$0 = B_{a(p-1)+1} < B_{a(p-1)} < \dots < B_1 < B_0 = B = \mathbb{F}_p^V.$$

For every $d \in \{0, \dots, a(p-1)\}$, we let

$$G_d = B_{a(p-1)-d} \rtimes V.$$

In particular, $G_0 = B_{a(p-1)} \rtimes V = B_{a(p-1)} \times V$ acts regularly on its domain. Observe that if $b_1 \leq b_2$, then $G_{b_1} \geq G_{b_2}$. In particular, G_b is transitive for every $b \in \{0, \dots, a(p-1)\}$.

Lemma 3.1. *Let $b \in \{0, \dots, a(p-1)\}$ and write $b = r(p-1) + s$, where $r, s \in \mathbb{N}$ and $0 \leq s < p-1$. We have $\mu(G_b) = (p-s)p^{a-r}$. In particular, if $b = r(p-1)$, then $\mu(G_{r(p-1)}) = p^{a-r+1}$.*

Proof. Let $g \in G_b$ such that the support of g has cardinality $\mu(G_b)$. As $g \in B_0 \rtimes V$, we may write $g = fv$, for some $v \in V$ and for some $f \in B_0$ with $\deg f \leq b$, by (3). If $v \neq 0$, then g acts fixed point freely. Therefore, we may suppose that $v = 0$ and $g = f \in B_{a(p-1)-b}$.

Let $Z(f) = \{v \in V \mid f(v) = 0\}$. Now, let (x, v) be in the domain of G_b , from the definition of the wreath product we deduce that

$$(x, v)^f = x + f(v).$$

In particular, if $v \in Z(f)$, then $g = f$ fixes all the points of the form (x, v) ; whereas, if $v \in V \setminus Z(f)$, then f acts as a cycle of length p on $\{(x, v) \mid x \in \mathbb{F}_p\}$. This shows that

$$\mu(G) = p(|V \setminus Z(f)|).$$

Now, the result follows from [3, Theorem 5.11]. \square

Next, we compute the cardinality of $|G_b|$. To this end, let x be an indeterminate and consider the polynomial

$$p(x) = (1 + x + \dots + x^{p-1})^a \in \mathbb{Z}[x].$$

This polynomial has degree $(p-1)a$. Actually, the polynomial $p(x)$ enumerates something very important for our example. Let

$$p(x) = \sum_{k=0}^{(p-1)a} \binom{a}{k}^{(p-1)} x^k$$

be the expansion of $p(x)$ in its monomials. The coefficients $\binom{a}{k}^{(p-1)}$ are usually called the extended binomial coefficients or multinomial coefficients. They do not have a standard notation, and we use the notation from [8]. When $p = 2$, the extended binomial coefficients are equal to the usual binomial coefficients. We also give another example

$$(1 + x + x^2)^4 = x^8 + 4x^7 + 10x^6 + 16x^5 + 19x^4 + 16x^3 + 10x^2 + 4x + 1.$$

In particular, $\binom{4}{6}^{(2)} = \binom{4}{2}^{(2)} = 10$ and $\binom{4}{4}^{(2)} = 19$.

From the definition of $p(x)$, we see that $\binom{a}{k}^{(p-1)}$ counts the number of a -tuples $(\lambda_1, \dots, \lambda_a)$ with $k = \sum_{i=1}^a \lambda_i$ and with $0 \leq \lambda_i \leq p-1$, $\forall i \in \{1, \dots, a\}$. Thus, (3) gives

$$\dim_{\mathbb{F}_p}(B_{a(p-1)-k}/B_{a(p-1)-k+1}) = \binom{a}{k}^{(p-1)}.$$

Therefore,

$$\dim_{\mathbb{F}_p} B_{a(p-1)-b} = \sum_{k=0}^b \binom{a}{k}^{(p-1)}.$$

Lemma 3.2. *For every $b \in \{0, \dots, a(p-1)\}$, $b(G_b) = \sum_{k=0}^b \binom{a}{k}^{(p-1)}$.*

Proof. The stabilizer of a point in $G_b = B_{a(p-1)-b} \rtimes V$ is a subgroup of $B_{a(p-1)-b}$ having index p , because the degree of the action is $n = p^{a+1}$ and $|V| = p^a$. Now, as all the orbits of $B_{a(p-1)-b}$ have cardinality p , we deduce that we need to fix $\dim_{\mathbb{F}_p} B_{a(p-1)-b} - 1$ more points to obtain a basis. \square

Now, fix $r \in \{0, \dots, a\}$. From Lemmas 3.1 and 3.2, we have

$$(4) \quad \mu(G_{r(p-1)})b(G_{r(p-1)}) = p^{a-r+1} \sum_{k=0}^{r(p-1)} \binom{a}{k}^{(p-1)}.$$

Before dealing with the general case, we use (4) to make an explicit computation when $p = 2$. Recall that, when $p = 2$, we have $\binom{a}{k}^{(p-1)} = \binom{a}{k}$. From [2, Exercise 9.42, page 492], we have

$$\sum_{k=0}^r \binom{a}{k} = 2^{a(\lambda \log_2(1/\lambda) + (1-\lambda) \log_2(\frac{1}{1-\lambda})) - \log_2(a) + O(1)},$$

where $\lambda = r/a$. Thus, from (6), we get

$$b(G_r)\mu(G_r) = 2^{a(1-\lambda)+a(\lambda \log_2(1/\lambda) + (1-\lambda) \log_2(\frac{1}{1-\lambda})) - \log_2(a) + O(1)}.$$

As the degree of the permutation group is $n = 2^{a+1}$, we deduce

$$(5) \quad \lim_{a \rightarrow \infty} \frac{\log_2(b(G_r)\mu(G_r))}{\log_2(n)} = 1 - \lambda - \lambda \log_2(\lambda) - (1 - \lambda) \log_2(1 - \lambda).$$

It is elementary to show that the maximum of the function appearing on the right hand side is attained when $\lambda = 1/3$. With $\lambda = 1/3$, the limit in (5) equals $\log(3)/\log(2)$. Therefore, we have proved the following.

Lemma 3.3. *For every $\varepsilon > 0$, there exists a transitive permutation 2-group of degree n such that $\mu(G)b(G) \geq n^{\log(3)/\log(2)-\varepsilon}$.*

We now turn to the general case. From (4), we have

$$(6) \quad \mu(G_{r(p-1)})b(G_{r(p-1)}) \geq p^{a-r+1} \binom{a}{r(p-1)}^{(p-1)}.$$

Proof of Theorem 1.1. Assume $p > 3$, a is a multiple of $p-1$ and write $a = (p-1)a_1$. Let $c = \lfloor \sqrt{p} \rfloor$. From [5, Theorem 5], we deduce that, for $p > 3$,

$$\binom{a}{ca}^{(p-1)}$$

is asymptotic to

$$\frac{\phi(x)}{\sqrt{2\pi a}} \left(\frac{1-x^p}{x-x^2} \right)^a,$$

as a tends to infinity, where

$$\phi(x) = \left(\frac{x}{(1-x)^2} - \frac{p^2 x^p}{(1-x^p)^2} \right)^{-1/2}, \quad x = \frac{1}{d} + \frac{p(d-1)^2}{d^{p+2}} + \theta \frac{p^3}{d^{2p}}, \quad d = 1 + \frac{1}{c}, \quad |\theta| \leq 1.$$

In [8], there is a much more informative asymptotic estimate on the extended binomial coefficients, but only for certain very special values of c .

Observe that $\phi(x)$ depends only on p , but not on a . Observe now that, from Lemmas 3.1 and 3.2 and from (6), we have

$$\begin{aligned}
\lim_{a \rightarrow \infty} \log_n(\mu(G_{ca})b(G_{ca})) &= \lim_{a \rightarrow \infty} \frac{\log_p(\mu(G_{ca})b(G_{ca}))}{\log_p(n)} \\
&\geq \lim_{a \rightarrow \infty} \frac{a - ca/(p-1) + 1 + \log_p(\phi(x)/\sqrt{2\pi a}) + a \log_p((1-x^p)/(x-x^2))}{a+1} \\
&= 1 - \frac{\lfloor \sqrt{p} \rfloor}{p-1} + \lim_{a \rightarrow \infty} \frac{\log_p(\phi(x)/\sqrt{2\pi a})}{a+1} + \log_p((1-x^p)/(x-x^2)) \\
&= 1 - \frac{\lfloor \sqrt{p} \rfloor}{p-1} + \log_p((1-x^p)/(x-x^2)),
\end{aligned}$$

observe that $\log_p(\phi(x)/\sqrt{2\pi a})/(a+1) \rightarrow 0$ because, as we remarked above, x does not depend on a .

Observe now that

$$\begin{aligned}
\lim_{p \rightarrow \infty} \frac{p(d-1)^2}{d^{p+2}} &= \lim_{p \rightarrow \infty} \frac{1}{d^{p+2}} = \lim_{p \rightarrow \infty} \left(1 + \frac{1}{c}\right)^{-p-2} = \lim_{p \rightarrow \infty} \left(\left(1 + \frac{1}{c}\right)^c\right)^{-(p+2)/c} \\
&= \lim_{p \rightarrow \infty} e^{-p/\sqrt{p}} = 0.
\end{aligned}$$

Moreover, with an analogue argument, we deduce

$$\lim_{p \rightarrow \infty} \frac{p^3}{d^{2p}} = \lim_{p \rightarrow \infty} \frac{p^3}{e^{2p/\sqrt{p}}} = 0.$$

This shows that $\lim_{p \rightarrow \infty} x = 1$ and hence

$$\lim_{p \rightarrow \infty} \log_p \left(\frac{1-x^p}{x-x^2} \right) = \lim_{p \rightarrow \infty} \log_p \left(\frac{1+x+\dots+x^{p-1}}{x} \right) = 1.$$

This gives

$$\lim_{p \rightarrow \infty} \lim_{a \rightarrow \infty} \log_n(\mu(G_{ca})b(G_{ca})) = 2. \quad \square$$

REFERENCES

- [1] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer-Verlag, New York, 1996.
- [2] R. Graham, D. Knuth, O. Patashnik, *Concrete Mathematics*, second edition, Pearson Education Limited, 1994..
- [3] X. Hou, *Lectures on Finite Fields*, Graduate studies in Mathematics **190**, AMS, 2018.
- [4] J. Kempe, L. Pyber, A. Shalev, Permutation groups, minimal degrees and quantum computing, *Groups Geom. Dyn.* **1** (2007), 553–584.
- [5] J. Li, Asymptotic Estimate for the Multinomial Coefficients, *J. Integer Sequences* **23** (2020), Article 20.1.3.
- [6] F. Mastrogiacomio, On the minimal degree and base size of finite primitive groups, *J. Algebra and its applications*.
- [7] M. Moscatiello, C. Roney-Dougal, Base sizes of primitive permutation groups, *Monatsh. Math.* **198** (2022), 411–443.

- [8] T. Neuschel, A note on extended binomial coefficients, *J. Integer Sequences* **17** (2014), Article 14.10.4.

LORENZO GUERRA, DIPARTIMENTO DI MATEMATICA PURA E APPLICATA,
UNIVERSITY OF MILANO-BICOCCA, VIA COZZI 55, 20126 MILANO, ITALY
Email address: `l.guerra@unimib.it`

ATTILA MARÓTI, HUN-REN ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, REÁLTANODA UTCA 13-15, H-1053,
BUDAPEST, HUNGARY
Email address: `maroti@renyi.hu`

FABIO MASTROGIACOMO, DIPARTIMENTO DI MATEMATICA “FELICE CASORATI”, UNIVERSITY OF PAVIA, VIA FER-
RATA 5, 27100 PAVIA, ITALY
Email address: `fabio.mastrogiacono01@universitadipavia.it`

PABLO SPIGA, DIPARTIMENTO DI MATEMATICA PURA E APPLICATA,
UNIVERSITY OF MILANO-BICOCCA, VIA COZZI 55, 20126 MILANO, ITALY
Email address: `pablo.spiga@unimib.it`