ON THE BASE SIZE AND MINIMAL DEGREE OF TRANSITIVE GROUPS

LORENZO GUERRA, ATTILA MARÓTI, FABIO MASTROGIACOMO, SAVELIY V. SKRESANOV, 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 there exists a universal constant $c > 0$ such that for infinitely many n there is a transitive permutation group G of degree n with

$$\mu(G)b(G) \geq c \cdot n^2.$$

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 $(\omega_1, \ldots, \omega_\ell)$ of Ω with trivial pointwise stabilizer, that is,

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

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 [2, Excercise 3.3.7]. Note that for every permutation group G of degree n both $\mu(G)$ and $b(G)$ are at most n, hence there is a trivial upper bound $\mu(G)b(G) \leq n^2$.

Known results on base size provide a natural upper bound for this product. For instance, it is shown in [9] that if G is a primitive group of degree n which is not large-base (for the definition see [9, p. 412]) and not the Mathieu group of degree 24, then

$$b(G) \leq 1 + \lceil \log_2 n \rceil. \tag{1}$$

Using this, we can easily obtain that the bound

$$\mu(G)b(G) \leq n(1 + \lceil \log_2 n \rceil).$$

holds for such primitive groups.

Nonetheless, this bound is not optimal and admits numerous exceptions. A more refined estimate was provided in [8], where a bound holds for all but one primitive group. Specifically, [8, Theorem 1.2] states that if G is a primitive group of degree n, different from the Mathieu group of degree 24, then

$$\mu(G)b(G) \leq n \log_2 n.$$

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

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

L. Guerra, F. Mastrogiacomo and P. Spiga are members of the GNSAGA INdAM research group and kindly acknowledge their support.

for intransitive—groups. Noteworthy in this context is [5, 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 [8, Theorem 1.2] holds for some classes of transitive or even intransitive groups. In particular, Lemma 2.1 shows that the bound holds for wreath products in their imprimitive action, while Lemma 2.2 establishes the bound for Sylow subgroups of symmetric groups and for maximal subgroups of symmetric groups, and provides an analogous bound for certain quasiprimitive groups.

Motivated by the results in Section 2, we initially conjectured that a bound similar to the one established in [8] would also hold for all transitive groups. In fact, in all classical and natural examples of transitive groups, the parameters $b(G)$ and $\mu(G)$ vary inversely, consider for instance the symmetric group $\mathrm{Sym}(n)$ in its natural action, for which $\mu(\mathrm{Sym}(n)) = 2$ and $b(\mathrm{Sym}(n)) = n-1$ or a regular group G, in which $b(G) = 1$ and $\mu(G)$ is the degree. It therefore seems difficult to conceive of examples where this phenomenon does not occur.

Our main result shows that there is a series of transitive groups G for which $\mu(G)b(G)$ grows as n^2 up to a constant factor, disproving our original conjecture.

Theorem 1.1. *There exists a universal constant $c > 0$ and infinitely many positive integers n such that there is a transitive permutation group G of degree n with $\mu(G)b(G) \geq c \cdot n^2$.*

The proof of Theorem 1.1, relies on a construction of asymptotically good binary codes invariant under the action of a dihedral group (see Section 3 for details). The groups constructed in Theorem 1.1 are isomorphic to a semidirect product of an elementary abelian 2-group and a dihedral group of order $2m$, where $n = 4m$ and m can be chosen to be a prime. We also note that in [5, Remark after Theorem A] the authors also use coding theory to construct a series of intransitive elementary abelian 2-groups with $\mu(G)b(G) \geq c \cdot n^2$ for some constant $c > 0$.

For groups of prime power order our bound is a bit weaker.

Theorem 1.2. *For every $\varepsilon > 0$, there exists a transitive permutation group of prime power order and degree n such that $\mu(G)b(G) \geq n^{2-\varepsilon}$.*

The proof of Theorem 1.2 is presented in Section 4, and relies on the descending series of wreath products of two vector spaces over the field with p elements, for some prime number p. Since G has a system of imprimitivity with n/p blocks of size p, we have $b(G) \leq n/p$. In our construction p tends to infinity, so $\mu(G)b(G)/n^2 \to 0$ when $n \to \infty$.

Inspired by this work, we propose two questions.

Question 1.3. *Could one classify all quasiprimitive permutation groups G of degree n such that $\mu(G)b(G) > n \log_2 n$?*

Question 1.4. *Is it possible to find a family of transitive p-groups of degree n for which $\mu(G)b(G)$ is bounded below by $c \cdot n^2$ for some universal constant $c > 0$? If so, can such a family be found with p bounded, or even with $p = 2$?*

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 $\mu(G)b(G) \leq n \log_2 n$.*

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 by [8, Theorem 1.2] we have $\mu(G)b(G) \leq (k \log_2 k)(n/k) = n \log_2 k \leq n \log_2 n$, otherwise with a computation we have $\mu(G)b(G) \leq (16 \cdot 7)(n/24) \leq n \log_2 48 \leq n \log_2 n$. □

Lemma 2.2. *Let G be a permutation group acting on a finite set Ω of size n.*

(1) *If G is a Sylow subgroup of $\mathrm{Sym}(\Omega)$, then $\mu(G)b(G) \leq n \log_2 n$.*
(2) *If G is a maximal subgroup of $\mathrm{Sym}(\Omega)$ different from the 5-transitive Mathieu group of degree 24, then $\mu(G)b(G) \leq n \log_2 n$.*
(3) *Let G be quasiprimitive, but not primitive. Let Δ be a maximal block of size at least 3. Let $\mathcal{B}$ be the associated system of blocks. If the action of G on $\mathcal{B}$ is non large-base and is different from the Mathieu group of degree 24, then $\mu(G)b(G) \leq n(1 + \lceil \log_2(n/3) \rceil)$.*

Proof. If G is primitive, then the claim follows from [8, Theorem 1.2].

Let G be imprimitive. If G is a (transitive) Sylow p-subgroup of $\mathrm{Sym}(\Omega)$ for some prime p, then (1) 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 $\mathrm{Sym}(\Omega)$, then $\mu(G)b(G) \leq n \log_2 n$, again by Lemma 2.1 by taking both H and T to be symmetric groups. This completes the proof of (2) 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 $\mathrm{Sym}(\Omega)$ where each G_i is a transitive Sylow subgroup of $\mathrm{Sym}(\Omega_i)$ 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 $\mu(G)b(G) \leq \sum_{i=1}^r |\Omega_i| \log_2 |\Omega_i| \leq \sum_{i=1}^r |\Omega_i| \log_2 n = n \log_2 n$. This completes the proof of (1). Similarly, if G is maximal (and intransitive) in $\mathrm{Sym}(\Omega)$, then $\mu(G)b(G) = 2(n-2) \leq n \log_2 n$, completing the proof of (2).

Let G act quasiprimitively on Ω. Let Δ be a maximal block of size at least 3. Let $\mathcal{B}$ be a maximal system of blocks in Ω defined from Δ. The action of G on $\mathcal{B}$ is primitive. Suppose that this group is not large-base and is different from the Mathieu group of degree 24. Let $b_{\mathcal{B}}(G)$ be the minimal base size of the permutation group induced by G on $\mathcal{B}$. We have $b(G) \leq b_{\mathcal{B}}(G)$ by [11, Lemma 5.1] and $b_{\mathcal{B}}(G) \leq 1 + \lceil \log_2(n/3) \rceil$ by (1). Thus $\mu(G)b(G) \leq n(1 + \lceil \log_2(n/3) \rceil)$. □

3. Proof of Theorem 1.1

Recall that a subspace C of $\mathbb{F}_2^m$ is called a *binary linear code* of length m. The number of nonzero coordinates of an element from C is called its *weight*. The smallest weight of a nontrivial element from C is called *minimal distance*. The integer k such that $|C| = 2^k$ is called the *dimension*. An infinite series of codes is called *asymptotically good* if k/m and d/m are uniformly bounded away from 0.

Given a permutation group $H \leq \mathrm{Sym}(m)$, note that H acts on $\mathbb{F}_2^m$ by permuting the coordinates. We will say that C is an H-invariant code if it is invariant under this action of H. In 2006 Bazzi and Mitter [1] provided a construction of asymptotically good binary linear codes which are invariant under the regular action of a dihedral group.

Proposition 3.1 ([1, Section III])**.** *There exists a constant $\delta > 0$ and infinitely many positive integers m such that there exists a binary linear code C of length $2m$, dimension k and minimal distance d with $k/(2m) > \delta$, $d/(2m) > \delta$, and C is invariant under the regular action of the dihedral group of size $2m$.*

It is mentioned in [1, Section III] that m in the proposition above can be chosen to be a prime number.

Proof of Theorem 1.1. Let $\delta > 0$ be the constant from Proposition 3.1, and let C be a code of length $2m$, dimension k and minimal distance d given by that proposition. We can naturally identify C with a subgroup of $\mathrm{Sym}(2)^{2m}$, by mapping $(c_1, \ldots, c_{2m}) \in C$ to $(1,2)^{c_1}(3,4)^{c_2} \cdots (4m-1, 4m)^{c_{2m}}$. As a permutation group C has $2m$ orbits of length 2.

Now we set $G = C \rtimes D_{2m}$, where D_{2m} is the dihedral group of size $2m$ acting regularly on C by permuting the coordinates of the code. Since C is D_{2m}-invariant, G is a transitive permutation group of degree $4m$. We will show that $\mu(G) = 2d$ and $b(G) = k$.

Let $g \in G$. If $g \notin C$, then it cannot stabilize any orbit of C, since D_{2m} acts regularly on the orbits, so g does not have fixed points and has degree $4m$. If $g \in C$, then g moves at least $2d$ points by the definition of minimal distance. Since minimal distance is achieved on some element, we get $\mu(G) = \mu(C) = 2d$.

Note that $b(G) = b(C)$. Let $\alpha_1, \ldots, \alpha_b$, $b = b(C)$, be points whose pointwise stabilizer in C is trivial. Since every orbit of every subgroup of C has size at most 2, we have $|C_{\alpha_1,\ldots,\alpha_i} : C_{\alpha_1,\ldots,\alpha_{i+1}}| \leq 2$ for all $i = 0, \ldots, b-1$. This implies $b \geq k$, and hence $b(C) = k$.

Now, G is a transitive permutation group of degree $n = 4m$. We have

$$\mu(G)b(G) = 2dk = \frac{2dk}{n^2} \cdot n^2 = \frac{1}{2}\frac{d}{2m}\frac{k}{2m} \cdot n^2 \geq \frac{\delta^2}{2} \cdot n^2$$

and the theorem follows by setting $c = \delta^2/2$. □

It is a famous open problem in coding theory whether there is a series of asymptotically good linear codes invariant under the regular action of a cyclic group, see, for instance, [7]. A positive solution to that problem would imply a construction similar to Theorem 1.1 but with a cyclic group instead of a dihedral group.

4. Proof of Theorem 1.2

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 $\mathrm{Sym}(V)$.

Next, we let $W = \mathbb{F}_p \wr V$ 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 $\mathrm{Sym}(\mathbb{F}_p \times V)$ 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 $X_1, \ldots, X_a$ be indeterminates, and consider the polynomial ring $\mathbb{F}_p[X_1, \ldots, X_a]$ with coefficients in $\mathbb{F}_p$. Now consider the evaluation map

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

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

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

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

$$f = \sum_{\lambda_1,\ldots,\lambda_a=0}^{p-1} a_{\lambda_1,\ldots,\lambda_a} x_1^{\lambda_1} \cdots x_a^{\lambda_a}, \tag{2}$$

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

Now, let $f \in B_0$ be as in (2) 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

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

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 of degree at most $d-1$. From this, arguing inductively, it immediately follows that

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

We claim that

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

To this end, for the moment, let C_d denote the vector space appearing on the right-hand side of (3). We prove that $C_d = B_d + C_{d+1}$ by induction on d. From this, (3) immediately follows. Clearly, the base case of the induction, namely $d = 0$, goes without saying, since $C_0 = B_0$. Let $\{e_1, \ldots, e_a\}$ be the canonical basis for V. Now let $\bar{\lambda} = (\lambda_1, \ldots, \lambda_a) \in \mathbb{N}^a$ with $\sum_i \lambda_i = a(p-1) - d$ and $\lambda_i \leq p-1$ for each i. Thus $x_{\bar{\lambda}} \in C_d = B_d + C_{d+1}$. Observe that, for every $1 \leq i \leq a$ with $\lambda_i \geq 1$, we have

$$\begin{aligned} x_{\bar{\lambda}}^{e_i} - x_{\bar{\lambda}} &= \prod_{j \neq i} x_j^{\lambda_j} \left((x_i + 1)^{\lambda_i} - x_i^{\lambda_i} \right) = \prod_{j \neq i} x_j^{\lambda_j} \sum_{k=0}^{\lambda_i - 1} \binom{\lambda_i}{k} x_i^k \\ &= \lambda_i x_{\bar{\lambda} - e_i} + \prod_{j \neq i} x_j^{\lambda_j} \sum_{k=0}^{\lambda_i - 2} \binom{\lambda_i}{k} x_i^k. \end{aligned}$$

Observe that none of the binomial coefficients is zero, since $\lambda_i \leq p-1$. This shows that $x_{\bar{\lambda} - e_i} \in B_{d+1} + C_{d+2}$. As the elements $x_{\bar{\lambda} - e_i}$ (with $\bar{\lambda}$ running over the a-tuples summing to $a(p-1) - d$ and i ranging over those with $\lambda_i \geq 1$) span C_{d+1}, we obtain $C_{d+1} = B_{d+1} + C_{d+2}$. Hence our claim is proven.

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

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

For every $d \in \{0, \ldots, a(p-1)\}$, 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 $b \in \{0, \ldots, a(p-1)\}$.

Lemma 4.1. *Let $b \in \{0, \ldots, a(p-1)\}$ 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

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

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

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

Now, the result follows from [4, Theorem 5.11]. □

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

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

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 [10]. 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 $(\lambda_1, \ldots, \lambda_a)$ with $k = \sum_{i=0}^{a} \lambda_i$ and with $0 \leq \lambda_i \leq p-1$, for all $i \in \{0, \ldots, a\}$. 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 4.2. *For every $b \in \{0, \ldots, a(p-1)\}$, $b(G_b) = \sum_{k=0}^{b} \binom{a}{k}^{(p-1)}$.*

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. □

Now, fix $r \in \{0, \ldots, a\}$. From Lemmas 4.1 and 4.2, we have

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

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 [3, Exercise 9.42, page 492], we have

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

where $\lambda = r/a$. Thus, from (4), we get

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

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

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

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 $\log_2(3)$. Therefore, we have proved the following.

Lemma 4.3. *For every $\varepsilon > 0$, there exists a transitive permutation 2-group of degree n such that $\mu(G)b(G) \geq n^{\log_2(3)-\varepsilon}$.*

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

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

Proof of Theorem 1.2. Assume $p > 3$ and a is a multiple of $p-1$. Let $c = \lfloor\sqrt{p}\rfloor$ and define $r = ca/(p-1)$. From [6, 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

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

In [10], 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 4.1 and 4.2 and from (6), we have

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

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

Observe now that

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

Moreover, with an analogue argument, we deduce

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

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

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

This gives

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

Declarations

Funding. L. Guerra and P. Spiga are funded by the European Union via the Next Generation EU (Mission 4 Component 1 CUP B53D23009410006, PRIN 2022, 2022PSTWLB, Group Theory and Applications). A. Maróti was supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K138596, No. K132951 and Grant No. K138828. The research of S.V. Skresanov was carried out within the framework of the Sobolev Institute of Mathematics state contract (project FWNF-2026-0017).

Conflict of interest. We have no financial or non-financial interests that are directly or indirectly related to the work submitted for publication.

Competing interests. The authors have no relevant financial or non-financial interests to disclose.

Data availability. Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] L.M.J. Bazzi, S.K. Mitter, Some randomized code constructions from group actions, *IEEE Trans. Inform. Theory* **52**:7 (2006), 3210–3219.
[2] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer-Verlag, New York, 1996.
[3] R. Graham, D. Knuth, O. Patashnik, *Concrete Mathematics*, second edition, Pearson Education Limited, 1994.
[4] X. Hou, *Lectures on Finite Fields*, Graduate studies in Mathematics **190**, AMS, 2018.
[5] J. Kempe, L. Pyber, A. Shalev, Permutation groups, minimal degrees and quantum computing, *Groups Geom. Dyn.* **1** (2007), 553–584.
[6] J. Li, Asymptotic Estimate for the Multinomial Coefficients, *J. Integer Sequences* **23** (2020), Article 20.1.3.
[7] C. Martinez-Perez, W. Willems, Is the class of cyclic codes asymptotically good?, *IEEE Trans. Inform. Theory* **52**:2 (2006), 696–700.
[8] F. Mastrogiacomo, On the minimal degree and base size of finite primitive groups, *J. Algebra and its applications*, (2025).
[9] M. Moscatiello, C. Roney-Dougal, Base sizes of primitive permutation groups, *Monatsh. Math.* **198** (2022), 411-443.
[10] T. Neuschel, A note on extended binomial coefficients, *J. Integer Sequences* **17** (2014), Article 14.10.4.
[11] C. E. Praeger, A. Shalev, Bounds on finite quasiprimitive permutation groups. *J. Aust. Math. Soc.* **71** (2001), no. 2, 243–258.

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 Ferrata 5, 27100 Pavia, Italy
Email address: fabio.mastrogiacomo01@universitadipavia.it

Saveliy V. Skresanov, Sobolev Institute of Mathematics,
4 Acad. Koptyug avenue, 630090 Novosibirsk, Russia
Email address: skresan@math.nsc.ru

Pablo Spiga, Dipartimento di Matematica Pura e Applicata,
University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy
Email address: pablo.spiga@unimib.it