Asymptotic Results for Primitive Permutation Groups and Irreducible Linear Groups

A. Lucchini
Dipartimento di Elettronica per l'Automazione, Università degli Studi di Brescia,
Via Branze, 25123 Brescia, Italy

F. Menegazzo
Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova,
Via Belzoni 7, 35131 Padova, Italy

and

M. Morigi
Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova,
Via Belzoni 7, 35131 Padova, Italy

Communicated by Jan Saxl
Received July 13, 1998

A well-developed branch of asymptotic group theory studies the properties of classes of linear and permutation groups as functions of their degree. We refer to the surveys of Cameron [4] and Pyber [17, 18] and the recent paper by Pyber and Shalev [19] for a detailed exposition of this subject. In this paper we concentrate our attention on the number of generators. Our results, like most recent results in this area, depend on the classification of finite simple groups (which will be referred to hereafter as CFSG).

Concerning linear groups, in 1991, Kovács and Robinson [11] proved that every finite completely reducible linear group of dimension \(d\) can be generated by \(\lfloor \frac{3}{2}d \rfloor\) elements, and afterwards, in 1993, Bryant, et al. [3] proved the following result: to each field \(F\) whose degree over its prime subfield is finite,
there is a number $c_0$ such that every finite soluble irreducible linear group of degree $d \geq 2$ over $F$ can be generated by $[c_0 d / \sqrt{\log d}]$ elements. (Here, and in the sequel, the square brackets indicate the “integer part.”)

It was conjectured that a similar result would hold also removing the solvability hypothesis, and our Theorem A shows that this is the case, if the field considered is finite. Namely, denoting by $d(G)$ the number of generators of a group $G$, we have:

**Theorem A.** Let $V$ be a vector space of finite dimension $n \geq 2$ over the finite field $K$, and let $G \leq \text{GL}_K(V)$ be irreducible. Then there exists a constant $\tilde{d}_K$ depending on $K$ such that $d(G) \leq \tilde{d}_K n / \sqrt{\log n}$ (more precisely, $\tilde{d}_K$ is of the form $\tilde{d} \log |K|$ for some absolute constant $\tilde{d}$).

To prove Theorem A, another result is needed, which solves the problem of bounding the number of generators of a primitive semi-linear group, when the field considered is finite. More precisely, we have:

**Theorem B.** Let $V$ be a vector space of finite dimension $n \geq 2$ over the finite field $K$, and let $G \leq \Gamma \text{L}_K(V)$ be a $K$-primitive group. Then there exists a constant $\bar{c}$ such that $d(G) \leq \bar{c} \log n$.

Note that in this case the constant $\bar{c}$ is independent of the field.

Finally, we are able to handle the case of finite primitive permutation groups, obtaining:

**Theorem C.** There exists a constant $d$ such that if $G$ is a primitive permutation group of degree $n \geq 3$ then

$$d(G) \leq \frac{d \log n}{\sqrt{\log \log n}}.$$

We also observe that the bounds which we obtain are, apart from the choice of the constant, of the right order.

Throughout this paper, all the logarithms will be to base 2.

For the proof of Theorem B, to which this section is devoted, we use the approach introduced by Dalla Volta and Lucchini [5]. First, we need to introduce some notation.

Let $H$ be a finite group with a unique minimal normal subgroup, $N$. If $N$ is abelian, assume also that $N$ has a complement in $H$.

For each positive integer $k$, let $H^k$ be the $k$-fold direct power of $H$ and define the subgroup $H_k$ by

$$H_k = \{(h_1, \ldots, h_k) \in H^k \mid h_1 \equiv \cdots \equiv h_k \mod N\}.$$
Moreover, for every finite group $G$, let $g(H, G)$ be the largest integer $k$ such that $H_k$ is an epimorphic image of $G$, and let

$$t_1 = \max_R g(R, G) - 2\dim_{\text{End}_N N}, \quad t_2 = \max_S g(S, G),$$

where $R$ runs over the set of finite groups with a unique minimal normal subgroup $N$, which is abelian and complemented, and $S$ runs over the set of finite groups with a unique minimal normal subgroup, which is non-abelian. The minimal number of generators can be bounded in terms of $t_1$ and $t_2$. In fact, we have the following result [14, Corollary 2.2].

**Proposition 1 (CFSG).** If $d(G) > 2$ then either $d(G) \leq t_1 + 3$ or $t_2 \geq 2$ and $d(G) \leq \lceil \log(t_2 - 1) + 3 \rceil$.

**Lemma 2.** Let $V$ be a vector space of finite dimension $n \geq 2$ over the finite field $K$, and let $G \leq \Gamma L_K(V)$. Let $N$ be the socle of a finite group $H$ with a unique minimal normal subgroup; if $N$ is non-abelian then $g(H, G) \leq \frac{2}{2}n$.

**Proof.** Let $t := g(H, G)$ and let $M_1, M_2 \leq G$ be such that $M_1/M_2 \cong N^t$. If $S$ is the composition factor of $N$, there is a prime number $r \neq \text{char} \ K$ dividing $|S|$. We have that $M_1/M_2(M_1 \cap GL_K(V))$ is a homomorphic image of $M_1/M_2$, so it is perfect. Moreover, by Dedekind’s law,

$$\frac{M_1}{M_1(M_1 \cap GL_K(V))} = \frac{M_1}{M_1 \cap M_2 GL_K(V)} \cong \frac{M_1 GL_K(V)}{M_2 GL_K(V)}.$$

As $\Gamma L_K(V)/GL_K(V)$ is cyclic, it follows that $M_1/M_2(M_1 \cap GL_K(V))$ is also cyclic, so $M_1 = M_2(M_1 \cap GL_K(V))$. Let $R$ be an $r$-Sylow subgroup of $M_1 \cap GL_K(V)$. Then $RM_2/M_2$ is an $r$-Sylow subgroup of $M_1/M_2$, so it is isomorphic to the direct product of $t$ copies of an $r$-Sylow subgroup of $N$. As the number of generators of the direct product of $r$-groups is equal to the sum of the number of generators of the factors, it follows that $d(R/R \cap M_2) = d(RM_2/M_2) \geq t$, so $t \leq d(R)$. As $R \leq GL_K(V)$ and $r \neq \text{char} \ K$, $R$ is completely reducible, so by [11] $d(R) \leq \frac{3}{2}n$. It follows that $g(H, G) \leq \frac{3}{2}n$, as we wanted to prove.

From now on, if $G$ is a group $r(G)$ will denote the maximal rank of the subnormal abelian sections of $G$ and $rk(G)$ will denote the rank of an abelian group $G$. The notation $X \leq G$ indicates that the subgroup $X$ is subnormal in $G$. The proof of the two following lemmas is an easy exercise and is left to the reader.

**Lemma 3.** If $G$ is a group such that $r(G)$ is finite and $K \leq G$, then $r(G) \leq r(G/K) + r(K)$.
**Lemma 4.** Let $G$ be a finite group such that the socle of $G$ is the direct product of $k$ non-abelian simple groups. Then, for every normal subgroup $M$ of $G$, $\text{soc}(M) \leq \text{soc}(G)$, and $\text{soc}(M)$ is the direct product of at most $k$ simple groups.

**Lemma 5.** Assume that $H = AB$ is a finite group, with $B$ cyclic and normal in $H$. Then $\text{rk}(A/A') \leq \text{rk}(H/H')$.

**Proof.** Suppose that $H$ is a counterexample of minimum order. If $A' \neq 1$, as $[A', B] = 1$, we see that $A' \leq H$ and $\text{rk}(A/A') \leq \text{rk}(H/H')$, a contradiction. So $A$ is abelian. Consider $N \leq A$ such that $A/N$ is an elementary abelian $p$-group and $\text{rk}(A/N) = \text{rk}(A/A') = r$. If the $p'$-Hall subgroup $B_0$ of $B$ is non-trivial, then $A \cap B_0 \leq N$, $AB_0/NB_0 \cong A/N$, and again we reach a contradiction, so we may assume that $B$ is a $p'$-group. If $[A, B] = B$, then there exists a $p'$-element $g \in A$ not centralizing $B$. For this element $1 = [g, A \cap B] = A \cap B$ and $A \cong H/B$, so that $\text{rk}(A) \leq \text{rk}(H/H')$. So $[A, B]$ is a proper subgroup of $B$. As, obviously, $A < H$, also $(A \cap B)[A, B]$ is proper in $B$. It follows (denoting with bars the images modulo $(A \cap B)[A, B]$) that $\bar{H} = \bar{A} \times \bar{B}$ and, since $(A \cap B)[A, B]$ is cyclic, $\text{rk}(A) \leq 1 + \text{rk}(\bar{A}) + \text{rk}(\bar{A}) = \text{rk}(\bar{H}) \leq \text{rk}(H/H')$.

**Corollary 6.** Let $V$ be a finite dimensional vector space over the finite field $K$, $G \leq \Gamma L_K(V)$, and $Z := Z(GL_K(V))$. If $X \leq G$, then $\text{rk}(XZ)/(XZ) \geq \text{rk}(X/Z)$.

**Proof.** The group $H := XZ$ satisfies the hypothesis of Lemma 5, so the conclusion follows.

The following theorem bounds the rank of the subnormal abelian sections of a semi-linear primitive group, and it plays a crucial role in bounding $t_1$ in the hypothesis of Theorem B.

**Theorem 7.** Let $V$ be a vector space of finite dimension $n \geq 2$ over the finite field $K$, and let $G \leq \Gamma L_K(V)$ be a $K$-primitive group. Then there exists an absolute constant $c$ ($c = 7$) such that $\tau(G) \leq c \log n$.

**Proof.** Let $Z := Z(GL_K(V))$. If $X \leq G$, then $XZ \leq GZ$, so by Corollary 6 we may assume that $Z \leq G$.

We actually will prove by induction on $n$ that $\tau(G/Z) \leq (c - 1)\log n$; from this and from Lemma 3, as $Z \cong K^\times$ is cyclic, it follows immediately that $\tau(G) \leq \tau(G/Z) + 1 \leq (c - 1)\log n + 1 \leq c \log n$.

The reduction techniques which we use are those introduced in [1] and used also in [9].

We note that if $n = 1$ then $G \leq \Gamma L_K(K) \cong K^\times \rtimes \text{Aut}(K)$. As $\text{Aut}(K)$ is cyclic and $Z \cong K^\times \leq G$, we have that $\tau(G/Z) = 1$. 

Assume that we have proved the assertion for \( n = 2 \) (we will deal with this case later).

We may assume that the assertion holds for \( K \)-primitive groups \( \hat{G} \leq \Gamma L_K(V) \) where \( \dim_K(V) < n \).

**Step I.** Consider
\[
N_G := \{ N \leq G \mid Z < N \leq G \cap GL_K(V) \}.
\]

Arguing as in [9], we obtain that as \( G \) is \( K \)-primitive there is only one isomorphism type of irreducible \( K \N \)-submodules of \( V \) for each \( N \in N_G \).

**Step II.** Assume that there exists a normal subgroup \( M \in N_G \) such that \( K < S := \text{End}_{KM}(W_M) \), where \( W_M \) is a non-trivial irreducible \( KM \)-submodule of \( V \). For all irreducible \( KM \)-submodules \( W \in \text{Irr}_{KM}(V) \) of \( V \) we have \( W \cong KMW \) and \( \text{End}_{KM}(W) \cong S \). By some standard arguments (see [1, 3.11]), we have
\[
C_{\text{End}_K(V)}(M) \cong \text{End}_S(U) \quad \text{for} \quad U = \text{Hom}_{KM}(W_M, V).
\]

Denote by \( F \) the center of \( C_{\text{End}_K(V)}(M) \) and let \( F^* := F \cap GL_K(V) \). We have that \( F \cong S \) and \( V \) is a homogeneous \( F \)-module; in particular, \( V \) is an \( F \)-vector space. As \( M \leq G \), \( G \) acts on \( C_{\text{End}_K(V)}(M) \) by conjugation; in particular, \( G \) acts on \( F \subseteq \text{End}_K(V) \) by conjugation \( F \)-linearly, and every element of \( G \) induces a field automorphism on \( F \). It follows that \( G \) is \( F \)-semi-linear; that is, \( G \leq \Gamma L_F(V) \). Moreover, \( G \) is \( K \)-primitive and therefore \( F \)-primitive on \( G \). By Corollary 6 we have that \( r(G) \leq r(GF^*) \), so by Lemma 3, using induction or the information on the case \( n = 1 \), we obtain that
\[
\begin{align*}
\left( \frac{G}{Z} \right) & \leq r(G) \leq r(GF^*) \\
& \leq r \left( \frac{GF^*}{F^*} \right) + 1 \leq (c-1) \log \frac{n}{|F : K|} + 1 \\
& \leq (c-1)(\log n - 1) + 1 \leq (c-1)\log n.
\end{align*}
\]

So we may assume that \( \text{End}_{KM}(W) = K \) for all \( M \in N_G \) and all \( W \in \text{Irr}_{KM}(V) \).

**Step III.** Now assume that \( V \) is a reducible \( KN \)-module for some \( N \in N_G \). Let \( W \in \text{Irr}_{KN}(V) \), \( W \neq V \). We note that \( m := \dim W > 1 \). Namely, if \( \dim W = 1 \), as \( G \) is a homogeneous \( KN \)-module we have that \( N \acts V \) as a group of scalar matrices, and \( N \leq Z \), contrary to the choice of \( N \).

We can now apply Clifford’s second Theorem [22, Theorem 1.15] to \( G_0 := G \cap GL_K(V) \) (note that the hypothesis of \( K \) being algebraically closed may be replaced by the fact that every irreducible \( KN \)-submodule of \( V \) is absolutely irreducible). So we have that \( V \), as a \( KN \)-module, is the direct sum of \( r \) irreducible submodules isomorphic to \( W \), where \( n = mr \).
\( V \cong W \otimes_k U \) with \( \dim_K U = r \), and there exist \( A \leq GL_K(W), B \leq GL_K(U) \) such that \( Z(GL_K(W)) \leq A \), \( Z(GL_K(U)) \leq B \). \( G_0 \) is a subgroup of the central product \( A \circ B \), and \( G_0 A = G_0 B = A \circ B \). Let \( H := GA = GB \). As \( A, B \leq H \), we may consider the homomorphisms \( \alpha: G \to H/B \) and \( \beta: G \to H/A \). We note that \( H/B \) is isomorphic to a subgroup of \( \Gamma L_K(W)/Z(GL_K(W)) \) and analogously \( H/A \) is isomorphic to a subgroup of \( \Gamma L_K(U)/Z(GL_K(U)). \)

Let \( \tilde{G}_1, \tilde{G}_2 \) be the preimages of \( \alpha(G) \) and \( \beta(G) \) in \( \Gamma L_K(W) \) and \( \Gamma L_K(U) \). Then \( \tilde{G}_1 \) and \( \tilde{G}_2 \) are \( K \)-primitive semi-linear groups, so by induction

\[
\text{rk}(\alpha(G)) = \text{rk}\left(\frac{\tilde{G}_1}{Z(GL_K(W))}\right) \leq (c-1) \log m
\]

and

\[
\text{rk}(\beta(G)) = \text{rk}\left(\frac{\tilde{G}_2}{Z(GL_K(U))}\right) \leq (c-1) \log r.
\]

We want to prove that \( \text{rk}(G/Z) \leq (c-1) \log n \). As every abelian group of finite rank has an elementary abelian homomorphic image of the same rank, it is enough to prove that if \( X \leq G \), \( Z \leq Y \leq X \), and \( X/Y \) is elementary abelian, then \( \text{rk}(X/Y) \leq (c-1) \log n \).

We have

\[
\text{rk}\left(\frac{X}{Y}\right) = \text{rk}\left(\frac{X}{Y(X \cap B)}\right) + \text{rk}\left(\frac{Y(X \cap B)}{Y}\right).
\]

Moreover,

\[
\frac{X}{X \cap YB} \cong \frac{XB}{YB} \cong \frac{(XB)/B}{(YB)/B} \cong \frac{\alpha(X)}{\alpha(Y)}.
\]

As \( X \leq G \), we have that \( \alpha(X) \leq \alpha(G) \), so \( \text{rk}(X \cap YB) \leq (c-1) \log m \).

Now consider \( Y(X \cap B)/Y \cong (X \cap B)/(Y \cap B) \). As \( \text{Ker}(\beta) \cap (X \cap B) = Z \leq Y \cap B \), we have that \( \beta(X \cap B)/\beta(Y \cap B) \cong (X \cap B)/(Y \cap B) \). Moreover, \( \beta(X \cap B) \leq \beta(G) \) because \( X \cap B \leq G \), so we may conclude that \( \text{rk}(Y(X \cap B)/Y) \leq (c-1) \log r \). As \( Y(X \cap B) = X \cap YB \) by Dedekind's law, we have that \( \text{rk}(X/Y) \leq (c-1) \log m + (c-1) \log r = (c-1) \log n \), and the result is established.

**Step IV.** Let \( T \) be a minimal element of \( \mathcal{N}_G \). Then \( T/Z \) is characteristically simple and either elementary abelian or a direct product of some finite non-abelian simple groups.
1. Assume that $T/Z$ is an elementary abelian $q$-group of rank $r$, where, of course, $q \neq \text{char}(K)$. Let $Q^*$ be the $q$-Sylow subgroup of $T$. Then $Q^*$ is non-abelian of symplectic type (see [21, pp. 75–76]); that is, every abelian characteristic subgroup is cyclic. Define

\[
Q := \{ g \in Q^* | g^q = 1 \}, \quad \text{for } q \text{ odd},
\]

\[
Q := \{ g \in Q^* | g^4 = 1 \}, \quad \text{for } q = 2.
\]

Then $Q$ is a non-abelian characteristic subgroup of $T$ of symplectic type of exponent $q$ (respectively 4), and $QZ = T$. The structure of $Q$ and further information concerning $Z(Q)$ and $C_{\text{Aut}(Q)}(Z(Q))$ can be read from Table 4.6.A in [10]. Moreover, the absolutely irreducible representations of $Q$ over a field of characteristic $p \neq q$ are well known: $Q$ has $|Z(Q)| - 1$ inequivalent absolutely irreducible representations of degree $q^m$, where $2m = r$ [10, Prop. 4.6.3].

We have that $Q/Z(Q)$ is an elementary abelian $q$-group of rank $2m$. As $Z \cong K^*$, every $KQ$-submodule of $V$ is also a $KT$-submodule and $\text{End}_{KQ}(V) = \text{End}_{KT}(V)$ so $V$ is an absolutely irreducible $KQ$-module. It follows that $q^m = \dim_K(V) = n$, and $m \leq \log n$.

We have that $C_{G(K)}(V) = C_{G_k}(Q) \leq \text{End}_{KQ}(V) \cong K$, so $C_{G_k}(Q) = Z$. Moreover, $Z(Q) = C_{G_k}(Q) \cap Q = Z \cap Q$.

As $Q$ is normal in $G$, $G$ acts on $Q$ by conjugation; moreover, $G$ centralizes $\Phi(Q)$. Let $C := C_{G_k}(Q/Z(Q))$; then $C/C_{G_k}(Q) = C/Z$ is a subgroup of the group of automorphisms of $Q$ which induce the identity on $Q/Z(Q)$ and on $\Phi(Q)$. If $Q$ is as in the first three cases of Table 4.6.A of [10], then all the automorphisms of $Q$ with this property are inner, so $C = QZ = T$. In the remaining case either $C = QZ$ or $C/QZ = C/T$ is cyclic of order 2 (consider the automorphism of $Q$ that centralizes the central product of $m$ copies of $D_8$ and inverts the generator of $Z_4$).

We have that $QZ/Z \cong Q/(Q \cap Z) = Q/Z(Q)$ is elementary abelian of rank $2m$, so we can conclude that $r(C/Z) \leq 1 + 2m \leq 2 \log n + 1$.

Let $M/Z$ be a subnormal subgroup of $G/Z$. Applying repeatedly Clifford’s first theorem, we obtain that $M/(M \cap C) = M/(M \cap C_{G}(Q/Z(Q)))$ is a completely reducible linear group acting on the irreducible $F_q G$-module $Q/Z(Q)$, so by [11] it is generated by at most $\frac{1}{2} \dim_{F_q}(Q/Z(Q)) = \frac{1}{2}(2m) \leq 3 \log n$ elements. It follows that if $N$ is a normal subgroup of $M$ such that $Z \leq N$ and $M/N$ is elementary abelian, then $\text{rk}(M/N(M \cap C)) \leq 3 \log n$.

Moreover,

\[
\text{rk} \left( \frac{N(M \cap C)}{M \cap C} \right) = \text{rk} \left( \frac{M \cap C}{N \cap C} \right) \leq \text{rk} \left( \frac{C}{Z} \right),
\]
because \((M \cap C)/Z \leq C/Z\). It follows that
\[
\text{rk}(M_N) = \text{rk}\left(\frac{M}{N(M \cap C)}\right) + \text{rk}\left(\frac{N(M \cap C)}{N}\right) \leq 5\log n + 1 \leq 6\log n.
\]

To prove that \(r(G/Z) \leq (c-1)\log n\), it is enough to prove that \(\text{rk}(M/N) \leq (c-1)\log n\) for every elementary abelian subnormal section \(M/N\) of \(G\) such that \(Z \leq N\), and we have what we wanted.

2. We may assume that all the minimal normal subgroups of \(G/Z\) contained in \((G \cap GL_K(V))/Z = G_0/Z\) are the direct product of non-abelian simple groups. It follows that the socle of \(G_0/Z\) is the direct product of \(k\), say, non-abelian simple groups. Let \(M/Z\) be a subnormal subgroup of \(G_0/Z\); then the socle of \(M/Z\) is the direct product of at most \(k\) non-abelian simple groups, by repeated application of Lemma 4. Now we may apply the result in [7], which depends on CFSG, to conclude that \(M/Z\) is generated by at most \(3k\) elements, and it follows that the rank of every subnormal abelian section of \(G_0/Z\) is at most \(3k\).

Let \(L/Z := \text{soc}(G_0/Z)\). Then \(L \in \mathcal{N}_G\), so \(C_G(L) = Z\). Moreover, \(L\) is the central product of \(k\) quasi-simple groups and \(L = L'Z\). As before, we have that every \(KL\)-submodule of \(V\) is also a \(KL\)-submodule and \(\text{End}_{KL}(V) = \text{End}_{KL}(L)\) so \(V\) is an absolutely irreducible \(KL\)-module. By [3, Lemma 3.1], \(n \geq 2^k\), so \(k \leq \log n\). We obtain that \(r(G_0/Z) \leq 3\log n\). As \(G/G_0\) is cyclic, it follows that \(r(G/Z) \leq r(G/G_0) + r(G_0/Z) \leq 1 + 3\log n \leq (c-1)\log n\), as we wanted to prove.

It remains to prove the assertion for the case \(n = 2\).

We can now use the technique described above: the arguments in Step I remain unchanged; in Step II, using the information for the case \(n = 1\) instead of induction, we obtain that \(r(G/Z) \leq 2 \leq (c-1)\log 2\); the case in Step III does not occur because it must be \(\dim_K(W) > 1\); and in Step IV all the arguments remain unchanged. So we have proved what we wanted.

**Proof of Theorem B.** Let \(R\) be a finite group with a unique minimal normal subgroup \(N\), which is abelian and complemented, and such that \(t_1 = (g(R,G) - 2)/\dim_{\text{End}_R N}\). Let \(M \trianglelefteq G\) such that \(G/M \cong R_{g(R,G)}\). Then there exists a normal subgroup \(S\) of \(G\) such that \(S/M\) is isomorphic to the direct product of \(t_1 \dim_{\text{End}_R N} N + 2\) copies of \(N\). As \(r(G) \leq c\log n\) by Theorem 7, it follows that \(t_1 \leq c\log n - 2\). Moreover, by Lemma 2 we have that \(t_2 \leq \frac{3}{2}n\). Now we can apply Proposition 1 and we obtain that \(d(G) \leq \max\{c\log n + 1, \log(\frac{3}{2}n - 1) + 3\} = c\log n + 1 \leq \tilde{c}\log n\), for a suitable constant \(\tilde{c}\).

The following example shows that the bound given in Theorem B is of the right form.
Example. Let $q$ be an odd prime such that $4 \nmid q - 1$ and let $K$ be a finite field of characteristic $p \neq q$ containing a primitive $q$th root $\theta$ of unity and a square root $\lambda$ of $q$. The extra special group $P$ of order $q^3$ and exponent $q$ acts faithfully and absolutely irreducibly on a vector space $W$ of dimension $q$ over $K$ [10, Prop. 4.6.3]. More precisely (see [20]), we may assume that $P = \langle x, y \rangle$, where

$$x = \begin{bmatrix} \theta^q & \theta^q & \cdots & \theta^q \\ \theta^q & \theta^q & \cdots & \theta^q \\ \cdots & \cdots & \cdots & \cdots \\ \theta & \theta & \cdots & \theta \end{bmatrix}, \quad y = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Moreover, if we consider the matrix $b$ whose entries are $b_{ij} = \lambda^{-1} \theta^{i(j-1)(j-1)}$, for $i, j = 1, \ldots, q$, then $x^b = y^{-1}$ and $y^b = x$, so $b$ induces on $P$ an automorphism of order $4$ which centralizes $Z(P)$ [20]. As $4 \nmid q - 1$, $P/Z(P)$ is $\langle b \rangle$-irreducible. Also, we have that $H := \langle P, b \rangle = P \times \langle b \rangle$, where $\langle b \rangle$ is cyclic of order $4$, and $Z(P) = Z(H)$. As $H$ has no subgroup of index $q$, because $P/Z(P)$ is $\langle b \rangle$-irreducible, it follows that $H$ is primitive. Let $G := H \circ H \circ \cdots \circ H$ be the central product of $m$ copies of $H$; $G$ acts faithfully on the tensor product $V$ of $m$ copies of $W$. So $\dim_K V = q^m$. We now prove that $G$ is primitive. Assume by contradiction that $V = V_1 \oplus \cdots \oplus V_r$, where $\{V_1, \ldots, V_r\}$ is a system of imprimitivity. Then $N_1 := N_G(V_1)$ has index $t$ in $G$, where $t$ divides $q^m$, and $Z(G) \leq N_1$. We have that $G = QS$, where $S$ is the direct product of $m$ cyclic groups isomorphic to $\langle b \rangle$ and $Q = P_1 \cdots P_m$ is an extra special $q$-group of exponent $q$, with $|Q/Z(Q)| = q^{2m}$. Now $Q/Z(Q)$ is a completely reducible $\mathbb{F}_q S$-space. Namely, $Q/Z(Q)$ is the direct sum of $m$ $\mathbb{F}_q S$-subspaces $Q_1, \ldots, Q_m$, where $Q_i = P_i/Z(P_i)$ for $i = 1, \ldots, m$. Moreover, as $C_q(Q_i) \neq C_q(Q_j)$ if $i \neq j$, the $Q_i$'s are pairwise non-isomorphic, so the only $\mathbb{F}_q S$-subspaces of $Q/Z(Q)$ are the direct sum of some of the $Q_i$'s. As $t = |G : N_1|$ is a power of $q$, $N_1$ contains a $2$-Sylow subgroup of $G$, so $(N_1 \cap Q)/Z(Q)$ is $S$-invariant. It follows that $N_1 \cap Q$ is the product of some of the $P_i$'s. Also, $N_1 \cap Q$ is normal in $G$, so by Clifford's first theorem it is completely reducible. In particular, $N_1 \cap Q$ has an irreducible representation on a direct summand $W'_1$ of $V_1$. Also, $N_1 \cap Q$ has a unique minimal normal subgroup, $Z(Q)$, which acts non-trivially on $W'_1$ as a group of scalar matrices, so it is faithful on $W'_1$. As $K$ is a splitting field for $N_1 \cap Q$, we get $\dim_K W'_1 = q^r$, where $|N_1 \cap Q| = q^{2r+1}$ [10, Prop. 4.6.3]. It follows that $\dim_K V = q^r l$, for some natural number $l$. Also, as $N_1 = (N_1 \cap Q)S$, we have that $t = |G : N_1| = q^{2(m-r)}$, so $\dim_K V = q^r l t = q^{2m-r} l > q^m$, a contradiction. So $G$ is primitive, $d(G) \geq m$ (as $G/Q$ is abelian of rank $m$), and $m = \log_q \dim_K V = (\log q)^{-1} \log \dim_K V$. 


In this section we will prove Theorem A. We want to use some of the ideas contained in [13], but to do so we need some preliminary work.

The following is a result of Pyber [17, Theorem 2.10], stated in a slightly different form:

**Theorem 8** [17] (CFSG). (i) The number of abelian composition factors of a primitive permutation group of degree \(n\) is at most \(c_0 \log n\) for some absolute constant \(c_0\).

(ii) The number of non-abelian composition factors of a primitive permutation group of degree \(n\) is at most \(\log n\).

As a corollary we get:

**Proposition 9.** Let \(V\) be a vector space of finite dimension \(n\) over the finite field \(K\), and let \(G\) be an irreducible subgroup of \(\Gamma L_K(V)\); denote by \(a(G)\) the number of abelian composition factors of \(G\). Then there exists a constant \(c_K\) depending on \(K\) such that \(a(G) \leq c_K n\).

**Proof.** If \(Z := Z(GL_K(V))\), obviously \(a(G) \leq a(GZ)\), so we may assume that \(Z \leq G\). Now \(V\) is a vector space of dimension \(n|K : \mathbb{F}_p|\), over the prime field \(\mathbb{F}_p\) of \(K\), and, as \(Z \cong K^* \leq G\), we have that every \(\mathbb{F}_p G\)-submodule of \(V\) is also a \(KG\)-submodule, so \(V\) is an irreducible \(\mathbb{F}_p G\)-module. Now consider the semidirect product \(H := V \ltimes G\). As \(V\) is irreducible, \(G\) is a maximal subgroup of \(H\), so \(H\) is a primitive permutation group of degree \(|H : G| = p^{n|K : \mathbb{F}_p|}\). By Theorem 8(i), we have that \(a(H) \leq c_0 \log p^{n|K : \mathbb{F}_p|} = c_0 n \log |K|\) for some absolute constant \(c_0\). Putting \(c_K := c_0 \log |K|\), the result is established.

Assume that \(G\) is a subgroup of \(T = R \wr S\), where \(S\) is a transitive permutation group of degree \(s \geq 2\) and \(n = rs\). Let \(R_1 \times \cdots \times R_s\) be the base subgroup of \(T\) and consider \(T_i := N_T(R_i)\); since \(T_i \cong R_i \times (R : \text{Sym}(s-1))\) we may consider the projection \(\rho_i : T_i \to R_i\). We have the following:

**Lemma 10.** Consider a subgroup \(G\) of the wreath product \(T = R \wr S\), where \(S\) is a transitive permutation group of degree \(s \geq 2\) and \(R\) is a finite group. Assume that \(\rho_i(N_G(R_i)) = R_i\) for \(1 \leq i \leq s\). If \(B := R_1 \times \cdots \times R_s\) is the base group of \(T\) and \(U_1, U_2\) are normal subgroups of \(G\) such that \(U_1, U_2 \leq G \cap B\), \(U_2 \leq U_1\), and \(U_1/U_2\) is elementary abelian, then \(rk(U_1/U_2) \leq s \cdot r(R)\).

**Proof.** For every \(i = 1, \ldots, s\) and \(j = 1, 2\) we have that \(U_j \leq N_G(R_i)\); moreover, \(U_j \triangleleft G\) and \(\rho_i(N_G(R_i)) = R_i\), so \(\rho_i(U_j) \leq R_i\).

Let \(L_i := R_i \times R_{i+1} \times \cdots \times R_s\). We have that \(U_j \cap L_i \leq U_j \leq N_G(R_i)\), so \(\rho_i(U_j \cap L_i) \leq \rho_i(U_j) \leq R_i\). Consider the following chain:

\[
U_1 = U_2(U_1 \cap L_1) \geq U_2(U_1 \cap L_2) \geq \cdots \geq U_2(U_1 \cap L_s) \geq U_2.
\]
Define \( L_{i+1} := 1 \) so that \( U_2 = U_2(U_1 \cap L_{i+1}) \). We have

\[
\frac{U_2(U_1 \cap L_i)}{U_2(U_1 \cap L_{i+1})} = \frac{U_2(U_1 \cap L_i)}{U_2(U_1 \cap L_{i+1})} \approx \frac{U_1 \cap L_i}{(U_1 \cap L_i) \cap (U_1 \cap U_2 L_{i+1})} = \frac{U_1 \cap L_i}{(U_1 \cap L_i) \cap (L_i \cap U_2 L_{i+1})}
\]

\[
\approx \frac{\rho_i(U_1 \cap L_i)}{\rho_i(U_2 \cap L_i)}.
\]

As \( \rho_i(U_1 \cap L_i) \leq \rho_i \), it follows that

\[
\text{rk}\left(\frac{U_1}{U_2}\right) = \sum_{i=1}^{s} \text{rk}\left(\frac{U_2(U_1 \cap L_i)}{U_2(U_1 \cap L_{i+1})}\right) = \sum_{i=1}^{s} \text{rk}\left(\frac{\rho_i(U_1 \cap L_i)}{\rho_i(U_2 \cap L_i)}\right) \leq \text{tr}(R),
\]

as we wanted to prove.

**Lemma 11 (CFSG).** Let \( R \) be a finite group and let \( a \) be the number of abelian composition factors of \( R \). Consider a subgroup \( G \) of the wreath product \( R \wr S \), where \( S \) is a transitive permutation group of degree \( s \geq 2 \), and assume that \( \rho_i(N_G(R_i)) = R_i \) for \( 1 \leq i \leq s \). Assume also that \( \pi(G) = S \), where \( \pi: R \wr S \rightarrow S \) is the projection on the top group. If \( H \) is a finite group with a unique minimal normal subgroup \( N \) which is abelian and complemented and \( b' \) is the constant which appears in [16, Lemma 4], then

\[
\frac{g(H, G)}{\dim_{\text{End}_N} N} \leq \frac{g(H, S)}{\dim_{\text{End}_N} N} + \left\lfloor \frac{ab's}{\sqrt{\log s}} \right\rfloor.
\]

**Lemma 12 (CFSG).** There exists a constant \( c_1 \) such that if \( S \) is a transitive subgroup of \( \text{Sym}(n) \), with \( n \geq 2 \), and \( H \) has a unique minimal normal subgroup \( N \), which is abelian and complemented, then

\[
\frac{g(H, S) - 2}{\dim_{\text{End}_N} N} + 3 \leq \frac{c_1n}{\sqrt{\log n}}.
\]

**Proof.** These lemmas are Lemmas 2.5 and 2.7 in [13], where the solvability hypotheses have been removed owing to the results proved in [16].

**Lemma 13.** Let \( V \) be a vector space of finite dimension \( n \geq 2 \) over the finite field \( K \), and let \( G \leq GL_K(V) \) be irreducible. If \( H \) is a finite group with a unique minimal normal subgroup which is abelian and complemented, then there exists a constant \( d_K \) depending on \( K \) such that

\[
\frac{g(H, G) - 2}{\dim_{\text{End}_N} N} + 3 \leq \frac{d_Kn}{\sqrt{\log n}}.
\]
Proof. Let $d_1$ be such that $c \log m \leq d_1 m / \sqrt{2 \log m}$ for every natural number $m \geq 2$ (here $c$ is as in Theorem 7). If $c_K$ is as in Proposition 9, $b'$ is as in Lemma 11, and $c_1$ is as in Lemma 12, define $d_K := \max\{c_1 + c_K b' \sqrt{2}, c_1 + d_1\}$. If $G$ is primitive, by Theorem 7 we have that $g(H, G) \leq r(G) \leq c \log n \leq d_1 n / \sqrt{\log n} \leq d_K n / \sqrt{\log n}$, so we may assume that $G$ is not primitive. Choose a system of imprimitivity $\{W = W_1, W_2, \ldots, W_s\}$ such that $W$ is of minimal dimension and let $R$ be the linear group induced by the normalizer $N_G(W)$ on $W$. By the minimality of $\dim_K(W)$, $R$ is a primitive linear group of degree $r = \dim_K(W)$. Then $G$ is a subgroup of $T := R \rtimes S$, where $S$ is a transitive permutation group of degree $s$ and $n = rs$.

Moreover, $G$ satisfies the hypothesis of Lemma 11.

We distinguish two cases:

1. $r \leq s$: In this case $\sqrt{n} \leq s$ and by Proposition 9, and Lemmas 11 and 12 we have

$$
\frac{g(H, G)}{\dim_{End_H} N} + 3 \leq \frac{g(H, S) - 2}{\dim_{End_H} N} + 3 + \frac{ab's}{\sqrt{\log s}} \leq \frac{c_1 n}{\sqrt{\log n}} + \frac{c_K b's}{\sqrt{\log n}}
$$

$$
\leq \frac{c_1 n}{\sqrt{\log n}} + \frac{c_K b's}{\sqrt{\log n}} \leq \frac{c_1 n}{\sqrt{\log n}} + \frac{c_K b's}{\sqrt{\log n}}.
$$

2. $r \geq s$: In this case $n \leq r^2$. There exists $M_2 \leq G$ such that $G/M_2 \cong H_{r(H, G)}$. Let $M_1 \leq G$ be such that $soc(G/M_2) = M_1/M_2 \cong N_{r(H, G)}$. Let $B := R_1 \times \cdots \times R_s$ be the base group of $T$.

We note that every normal subgroup of $H_{r(H, G)}$ either contains $N_{r(H, G)}$ or is contained in it.

Now consider $M_2(G \cap B)$. If $M_2(G \cap B) \leq M_1$, then $M_1/M_2(G \cap B) \cong N^t$, with $t \leq g(H, S)$. Moreover, as $rk(M_1/M_2) = rk(M_1/M_2(G \cap B)) + rk(M_2(G \cap B)/M_2)$, we have

$$
N_{r(H, G)}^{-1} \cong \frac{M_2(G \cap B)}{M_2} \cong \frac{G \cap B}{M_2 \cap B},
$$

so that $g(H, G) \leq g(H, S) + rk((G \cap B)/(M_2 \cap B))$. Using Lemma 10 and the fact that $r(R) \leq c \log r$ by Theorem 7, we obtain that $g(H, G) \leq g(H, S) + s \log r$.

If $M_1 \leq M_2(G \cap B)$ we have that $M_1 = M_1 \cap M_2(G \cap B) = M_2(M_1 \cap B)$, so

$$
\frac{M_1}{M_2} = \frac{M_2(M_1 \cap B)}{M_2} \cong \frac{M_1 \cap B}{M_2 \cap B}.
$$
and, as before, \( \text{rk}((M_1 \cap B)/(M_2 \cap B)) \leq sc \log r \). In both cases it follows that

\[
\frac{g(H, G) - 2}{\dim_{\text{End}_K} N} + 3 \leq \frac{g(H, S) - 2}{\dim_{\text{End}_K} N} + 3 + sc \log r \leq \frac{c_1 s}{\sqrt{\log s}} + \frac{d_1 rs}{\sqrt{\log r^2}}
\]

\[
\leq \frac{c_1 n}{\sqrt{\log n}} + \frac{d_1 n}{\sqrt{\log n}}.
\]

The result is now established.

**Proof of Theorem A.** We apply Proposition 1. By Lemma 13 we have that \( t_1 + 3 \leq d_K n/\sqrt{\log n} \), where \( d_K \) is a constant depending on \( K \), and by Lemma 2 we have that \( t_2 \leq \frac{3}{2} n \). It follows that \( d(G) \leq \max\{d_K n/\sqrt{\log n}, \log(\frac{3}{2} n - 1) + 3\} \leq \tilde{d}_K n/\sqrt{\log n} \), for a suitable constant \( \tilde{d}_K \). Also, from the proofs of Proposition 9 and Lemma 13, it is easily seen that \( \tilde{d}_K \) can be chosen of the form \( \tilde{d} \log |K| \).

**Remark.** Theorem 1.3 of [8] shows that the bound in Theorem A is actually achieved, with a suitable different choice of the constant.

### III

To prove our last theorem, we need three more results concerning the number of generators of a finite group.

A finite group \( G \) is said to be an *almost simple* group if it is an automorphism group of a non-abelian simple group \( S \) such that \( S \leq G \) (we identify \( S \) with \( \text{Inn}(S) \)). We have that:

**Theorem 14** [6] (CFSG). *If \( G \) is an almost simple group, then \( d(G) \leq 3 \).*

**Theorem 15** [15] (CFSG). *If the group \( G \) has a unique minimal normal subgroup \( N \), then \( d(G) \leq \max\{d(G/N), 2\} \).*

**Theorem 16** [16] (CFSG). *There exists a constant \( \tilde{c} \) such that any transitive permutation group of finite degree \( n \geq 2 \) can be generated by \([\tilde{c} n/\sqrt{\log n}]\) elements.*

**Remark.** To avoid confusion with the notation already introduced, in Theorem 16 we have called \( \tilde{c} \) the constant \( c \) appearing in Theorem 1 of [16].
Arguing as in [19, Corollary 1.2] and using Theorem A, we can deduce that:

**Proposition 17.** If $G$ is an irreducible subgroup of $\text{GL}(m, p)$, where $p$ is a prime, and $n = p^m$, then there exists a constant $c_2$ such that

$$d(G) \leq \frac{c_2 \log n}{\sqrt{\log \log n}}.$$ 

Now that the preparations have ended, we can finally prove the theorem.

**Proof of Theorem C.** We first note that if $n = 2$ then $d(G) = 1$ and if $n = 3$ then $d(G) \leq 2$. Also, there exists a constant $b_1$ such that $3 + \frac{c_0 \log \log r + 1}{b_1 \log \log r}$ for every $r \geq 3$ (here $c_0$ is as in Theorem 8(i)). Let now $d_1$ be such that $(b_1 + c_1) \log \log r \leq d_1 \log r/\sqrt{2 \log \log r}$ for every $r \geq 3$ and $d_2$ such that $\log(\log n - 1) + 3 \leq d_2 \log n/\sqrt{\log \log n}$ for every $n \geq 3$ and $d_2 \geq \max\{d_1, \sqrt{2(b_0 c_0 + c_1)}\}$ ($b_0$ and $c_1$ are as in Lemmas 11 and 12, respectively). We can now define $d := \max\{c, c_2, d_2, \bar{c}\}$ ($\bar{c}$ is as in Theorem 16 and $c_2$ as in Proposition 17).

Let $G$ be a primitive permutation group of degree $n > 3$. Then the structure of $G$ is described by the O'Nan–Scott theorem (see [12]) and we proceed to examine the various possibilities.

1. $G$ is a subgroup of the affine linear group $\text{AGL}(m, p)$ and $n = p^m$. We have that $B := \text{soc}(G) \cong \mathbb{Z}_p^m$ and $G/B \cong H$ is an irreducible subgroup of $\text{GL}(m, p)$. Moreover, $B$ is the unique minimal normal subgroup of $G$, so by Theorem 15 and Proposition 17 it follows that $d(G) = \max\{d(H), 2\} \leq c_2 \log n/\sqrt{\log \log n}$.

2. $G$ almost simple. In this case $d(G) \leq 3$ by Theorem 14.

3. (a) Simple diagonal action. Let $T$ be a finite non-abelian simple group and define $W := \{(a_1, \ldots, a_k) \pi \mid a_i \in \text{Aut}(T), \pi \in \text{Sym}(k), a_i \equiv a_i \mod \text{Inn}(T) \text{ for all } i, j\}$. $W$ has an action of degree $n = |T|^{k-1}$ with stabilizer $W_a = \{(a, \ldots, a) \pi \mid a \in \text{Aut}(T), \pi \in \text{Sym}(k)\}$. Let $B = T^k = \text{soc}(W)$; then $G$ is a transitive subgroup of $W$ such that $B \leq G$ and satisfying one of the following conditions:

   i. $P$ is primitive,
   ii. $k = 2$ and $P = 1$,

where $P$ is the projection of $G$ on $\text{Sym}(k)$.

In the first case we have also that $B$ is the unique minimal normal subgroup of $G$ and $G/B \leq \text{Out}(T) \times P$. As by Theorem 14 $d(X) \leq 3$ for every
Out, by Theorems 15 and 16 we have that, if \( k \geq 3 \),
\[
d(G) = \max \left\{ d \left( \frac{G}{B} \right), 2 \right\} \leq 3 + d(P) \leq 3 + \frac{ck}{\sqrt{\log k}}
\]
\[
\leq \frac{d \log |T|^k - 1}{\sqrt{\log \log |T|^k - 1}} = d \log n \sqrt{\frac{\log \log n}{n}},
\]
where we have used that \( |T| \geq 60 \) (because \( T \) is a non-abelian simple group). If \( k \leq 2 \), then we have
\[
d \left( \frac{G}{B} \right) = 3.
\]

In the second case \( G \) is the direct product of two simple groups and so, as by a well-known consequence of CFSG every finite non-abelian simple group is 2-generated (see [2]), we have that \( d(G) \leq 4 \).

(b) Product action. Let \( R \) be a primitive permutation group of degree \( r \geq 2 \) of type II or III(a) and let \( S \) be a transitive permutation group of degree \( s \). With the product action, \( W := R : S \) is a transitive group of degree \( n = rs \). Then \( G \) is a transitive subgroup of \( W \) such that \( (\text{soc}(R))^s \leq G \) and the canonical projection of \( G \) on \( S \) is surjective. We want to apply Proposition 1, so we need a bound for \( \delta(R) \). We distinguish two cases:

(i) \( \log r < s \): By Theorem 8(i) the number of abelian composition factors of \( R \) is at most \( c_0 \log r \), so by Lemmas 11 and 12, using the same hypothesis and notation introduced there, we have
\[
g(H, G) - 2 = \frac{g(H, S) - 2}{\dim_{\text{End}_N} N} + 3 + \frac{b'c_0(\log r)s}{\sqrt{\log s}}
\]
\[
\leq c_s \frac{b'c_0(\log r)s}{\sqrt{\log s}} \leq \frac{(b'c_0 + c_1)s \log r}{\sqrt{\log s}}
\]
\[
\leq \frac{\sqrt{2}(b'c_0 + c_1)s \log r}{\sqrt{2 \log s}}
\]
\[
\leq \frac{\sqrt{2}(b'c_0 + c_1) \log r}{\sqrt{\log s + \log \log r}} \leq \frac{\sqrt{2}(b'c_0 + c_1) \log n}{\sqrt{\log \log n}}.
\]

(ii) \( \log r \geq s \): As before, let \( r(X) \) be the maximal rank of the subnormal abelian sections of \( X \). We have that \( R \) contains a normal subgroup \( B \) which is the direct product of non-abelian simple groups all isomorphic to \( T \), so every subnormal abelian section of \( R \) is isomorphic to a subnormal abelian section of \( R/B \). As by Theorem 14 \( d(X) \leq 3 \) for every \( X \leq \text{Out}(T) \) we have that \( r(R) \leq 3 \) if \( R \) is of type II or III(a)(ii). If \( R \) is of type III(a)(i), then \( r(R) \leq r(\text{Out}(T)) + r(P) \leq 3 + c_0 \log k \). We have that \( \delta = |T|^k - 1 \), so \( k = \log |T| + 1 \leq \log r + 1 \) and by our choice of \( b_1 \) we have that \( r(R) \leq b_1 \log \log r \). Using this fact and Lemma 10, arguing as in
Lemma 13, case 2, we obtain that \( g(H, G) \leq g(H, S) + sb_1 \log \log r \) (the notation is as in Lemma 13). Keeping in mind the definition of \( d_1 \), we have

\[
g(H, G) - 2 \leq \frac{g(H, S) - 2}{\dim_{\text{End}_N N}} N + 3 + sb_1 \log \log r
\leq \frac{c_1 s}{\sqrt{\log s}} + sb_1 \log \log r \leq s(c_1 + b_1) \log \log r
\leq \frac{d_1 s \log r}{\sqrt{2 \log \log r}}
\leq \frac{d_1 \log r}{\sqrt{\log s + \log \log r}} \leq \frac{d_1 \log n}{\sqrt{\log \log n}}.
\]

As \( t_2(G) \leq \log n \) by Theorem 8(ii), by our choice of \( d_2 \) and Proposition 1 we obtain

\[
d(G) \leq \max \left\{ \frac{d_1 \log n}{\sqrt{\log \log n}}, \frac{\sqrt{2(b'c_0 + c_1)} \log n}{\sqrt{\log \log n}}, \log(\log n - 1) + 3 \right\}
\leq \frac{d_2 \log n}{\sqrt{\log \log n}}.
\]

(c) Twisted wreath action. \( G \) is the semidirect product \( T^k \rtimes P \) where \( P \) is a transitive permutation group of degree \( k \) and \( T \) a simple non-abelian finite group. Moreover, \( G \) has degree \( |T|^k \) and \( T^k \) is the unique minimal normal subgroup of \( G \). By Theorems 15 and 16 we have

\[
d(G) = \max \{ d(P), 2 \} \leq \frac{\tilde{c} k}{\sqrt{\log k}} \leq \frac{\tilde{c} \log |T|^k n}{\sqrt{\log(\log |T|^k n)}} \leq \frac{\tilde{c} \log n}{\sqrt{\log \log n}}.
\]

Now, by the definition of \( d \), we have obtained what we wanted.

Note that, as observed by Pyber and Shalev [19, observation after Corollary 1.6], the bound in Theorem C is best possible.

**References**