An explicit counterexample to Kourovka Notebook Problem 20.75

KYRYLO MULIARCHYK

Abstract. We give a negative answer to Problem 20.75 of the Kourovka Notebook, proposed by L. Pyber. For the explicit integer $N = 2^{124210350}$, we construct a finite 2-group G of order 2^{110N+1} such that every abelian normal subgroup of G can be generated by at most $32N + 1$ elements, while G has an elementary abelian subgroup requiring $65N$ generators. The field, coefficients, and group multiplication are specified by finite deterministic formulas. The proof is self-contained and does not require enumeration of the group or its subgroups.

1. The question and the answer

Question. The following problem appears in the Kourovka Notebook [KN, p. 157].

> **20.75.** Let G be a finite p-group and assume that all abelian normal subgroups of G can be generated by k elements. Is it true that every abelian subgroup of G can be generated by $2k$ elements?
>
> The k-th direct power of D_{16} shows that this bound would be best possible.
>
> *L. Pyber*

For a finite group A, let $d(A)$ denote the least size of a generating set. The same question appears in [HPPS, Question 3.9], using the notation

$$r(G) = \max_{\substack{B \le G \\ B \text{ abelian}}} d(B), \qquad \mathrm{nr}(G) = \max_{\substack{A \trianglelefteq G \\ A \text{ abelian}}} d(A).$$

Thus the proposed inequality is $r(G) \le 2\,\mathrm{nr}(G)$. We construct a counterexample for $p = 2$.

Theorem 1.1. *Let $N = 2^{124210350}$. There is an explicitly specified finite 2-group G of order 2^{110N+1} with the following properties:*

$$d(A) \le 32N + 1 \qquad \text{for every abelian normal subgroup } A \trianglelefteq G, \tag{1.1}$$

$$d(E) = 65N \qquad \text{for an elementary abelian subgroup } E \le G. \tag{1.2}$$

In particular, $r(G) > 2\,\mathrm{nr}(G)$, and Problem 20.75 has a negative answer.

The construction has an index-two subgroup T with a central subgroup W whose underlying additive group is K^{20}. The outer involution interchanges the two copies of K^{45} in T/W. For a normal elementary abelian subgroup H, the image of $H \cap T$ is invariant under this interchange; its fixed subspace has at least half its dimension. Squares of lifts of fixed vectors are controlled by ten quadratic forms. Excluding a common seven-dimensional zero subspace bounds the rank of every abelian normal subgroup.

All fields below have characteristic two. We write $\dim_{\mathbb{F}_2} V$ for the dimension of an $\mathbb{F}_2$-vector space V. When a different ground field is intended, it is displayed explicitly.

2. An explicit field and its coefficients

Set

$$M = 10350, \qquad L = 10336, \qquad D = 2^{12000}, \qquad B = D + 1, \tag{2.1}$$

$$s = 12001M = 124210350, \qquad N = 2^s. \tag{2.2}$$

Starting with $K_0 = \mathbb{F}_2$ and $a_0 = 1$, define recursively, for $0 \le i < s$,

$$K_{i+1} = K_i[t_i]/(t_i^2 + t_i + a_i), \qquad a_{i+1} = a_i t_i. \tag{2.3}$$

Key words and phrases. Finite 2-groups, abelian normal subgroups, number of generators, quadratic forms.

Here t_i also denotes its residue class in the quotient. Put $K = K_s$ and $\alpha = a_s$.

Lemma 2.1. *Every quotient in* (2.3) *is a field. Moreover,*

$$[K : \mathbb{F}_2] = N, \qquad |K| = 2^N, \qquad [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = N.$$

Proof. We prove inductively that K_i is a field and $\operatorname{Tr}_{K_i/\mathbb{F}_2}(a_i) = 1$. This is true for $i = 0$. In a finite field of characteristic two, the $\mathbb{F}_2$-linear map $z \mapsto z^2 + z$ has kernel $\{0, 1\}$, and its image lies in the kernel of the absolute trace. At the inductive step the trace is nonzero because it takes the value 1 on a_i. Both subspaces therefore have index two, so the image is exactly the trace-zero subspace. Consequently $t^2 + t + a_i$ has no root in K_i and is irreducible.

The two roots of this polynomial differ by 1. Hence

$$\operatorname{Tr}_{K_{i+1}/K_i}(a_i t_i) = a_i(t_i + (t_i + 1)) = a_i.$$

Trace transitivity proves the induction. Each extension in the tower has degree two, so $[K : \mathbb{F}_2] = 2^s = N$ and $\operatorname{Tr}_{K/\mathbb{F}_2}(\alpha) = 1$.

If α belonged to a proper subfield $F \subset K$, then $[K : F]$ would be an even integer, since $[K : \mathbb{F}_2]$ is a power of two. As $\alpha \in F$, we would have $\operatorname{Tr}_{K/F}(\alpha) = [K : F]\alpha = 0$, and thus $\operatorname{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$, a contradiction. Therefore α has degree N over $\mathbb{F}_2$. $\square$

For $0 \le j < M$, define

$$c_j = \alpha^{B^j}. \tag{2.4}$$

Lemma 2.2. *For every nonzero polynomial $P \in \mathbb{F}_2[Z_0, \dots, Z_{M-1}]$ of total degree at most D,*

$$P(c_0, \dots, c_{M-1}) \neq 0. \tag{2.5}$$

Proof. Make the substitution $Z_j = T^{B^j}$. A monomial $\prod_j Z_j^{e_j}$ becomes $T^{\sum_j e_j B^j}$. Since $0 \le e_j \le D = B - 1$, distinct monomials give distinct exponents by uniqueness of base-B expansions. Thus the resulting polynomial $\widetilde{P}(T)$ is nonzero. Its degree is at most

$$D \sum_{j=0}^{M-1} B^j = B^M - 1 < N,$$

because $B < 2^{12001}$ and $N = 2^{12001M}$. By Lemma 2.1, a nonzero polynomial over $\mathbb{F}_2$ of degree less than N cannot vanish at α. Since $\widetilde{P}(\alpha) = P(c_0, \dots, c_{M-1})$, the result follows. $\square$

3. Quadratic forms with no common seven-dimensional zero subspace

Order the triples (i, j, k) with $1 \le i \le 10$ and $1 \le j \le k \le 45$ lexicographically, assigning indices $0, \dots, M - 1$. There are indeed $10\binom{46}{2} = 10350 = M$ triples. If the index of (i, j, k) is ℓ, put $C_{i,j,k} = c_\ell$. For $x, y \in K^{45}$, define

$$Q_i(x) = \sum_{1 \le j \le k \le 45} C_{i,j,k} x_j x_k, \tag{3.1}$$

$$F_i(x, y) = \sum_{1 \le j \le k \le 45} C_{i,j,k} x_j y_k. \tag{3.2}$$

Then $F = (F_1, \dots, F_{10})$ is a K-bilinear map $K^{45} \times K^{45} \to K^{10}$, and

$$F(x, x) = (Q_1(x), \dots, Q_{10}(x)). \tag{3.3}$$

A *common zero subspace* means a K-linear subspace on which every Q_i vanishes. Vanishing of the polar forms alone is not sufficient.

Lemma 3.1. *Every common zero subspace of $Q_1, \dots, Q_{10}$ has K-dimension at most six.*

Proof. Fix a set $I = \{i_1 < \dots < i_7\}$ of coordinate positions. Every seven-dimensional subspace whose projection onto these coordinates is an isomorphism has a basis matrix with the identity matrix in columns I and a 7×38 matrix R in the other columns. Equivalently, its vectors are obtained by substituting

$$x_{i_r} = z_r \quad (1 \le r \le 7), \qquad x_j = \sum_{r=1}^{7} R_{r,j} z_r \quad (j \notin I).$$

The parameters in R number $7 \cdot 38 = 266$.

The restriction of one quadratic form has $\binom{8}{2} = 28$ coefficients. Its being identically zero is equivalent to the vanishing of these coefficients: evaluate at the coordinate vectors to recover the diagonal coefficients, and at sums of two distinct coordinate vectors to recover the remaining coefficients. This observation is valid in characteristic two.

The original coefficient C_{i,i_r,i_t}, for $r \le t$, contributes exactly $C_{i,i_r,i_t} z_r z_t$ after substitution. No other coefficient involving only coordinates in I contributes to this monomial. Thus the 28 vanishing equations uniquely solve for the 28 coefficients involving only I. Each solved coefficient is a polynomial of total degree at most three in the entries of R and the remaining coefficients: at most two entries of R are multiplied by one original coefficient. No division occurs.

Consequently, all coefficient tuples for ten forms admitting a common zero subspace in this chart lie in the image of a polynomial map, defined over $\mathbb{F}_2$,

$$f_I : K^L \longrightarrow K^M, \qquad L = M - 10 \cdot 28 + 266 = 10336, \tag{3.4}$$

whose component polynomials have degree at most three.

We next find a nonzero polynomial $P_I \in \mathbb{F}_2[Z_0, \dots, Z_{M-1}]$ of degree at most D for which $P_I \circ f_I$ is the zero polynomial. Substitution by the component polynomials of f_I defines a linear map over $\mathbb{F}_2$ from polynomials in M variables of degree at most D to polynomials in L variables of degree at most $3D$. The respective dimensions are

$$\binom{M+D}{M} \qquad \text{and} \qquad \binom{L+3D}{L}.$$

The first is larger. Indeed, since $M < 2^{14}$ and $L < D$,

$$\binom{M+D}{M} \ge \frac{D^M}{M^M} > 2^{12000M-14M},$$

$$\binom{L+3D}{L} \le (L+3D)^L \le (4D)^L = 2^{12002L},$$

and

$$12000(M-L) - 14M - 2L = 2428 > 0. \tag{3.5}$$

The substitution map therefore has a nonzero kernel element P_I. The identity $P_I \circ f_I = 0$ is a formal polynomial identity over $\mathbb{F}_2$, so it remains valid on parameters in K.

By Lemma 2.2, however, $P_I(c_0, \dots, c_{M-1}) \neq 0$. Hence our coefficient tuple is not in the image of f_I. This holds for every I. Every seven-dimensional subspace has an invertible seven-column minor, so these charts cover all such subspaces. No common zero subspace has dimension seven; any higher-dimensional one would contain a seven-dimensional one. The lemma follows. □

4. The group and a large abelian subgroup

On the set

$$T = K^{45} \times K^{45} \times K^{10} \times K^{10}$$

define multiplication by

$$\begin{aligned}(a,b,u,v)&(a',b',u',v') \\ &= \big(a+a',\ b+b',\ u+u'+F(a,b'),\ v+v'+F(b',a)\big).\end{aligned} \tag{4.1}$$

The additional term in the last two coordinates is bilinear in (a,b) and (a',b'). For any bilinear map c,

$$c(x,y) + c(x+y,z) = c(y,z) + c(x,y+z),$$

so (4.1) is associative. The zero tuple is the identity, and

$$(a,b,u,v)^{-1} = \big(a,b,u+F(a,b),v+F(b,a)\big).$$

In particular,

$$(a,b,u,v)^2 = \big(0,0,F(a,b),F(b,a)\big). \tag{4.2}$$

Define

$$\sigma(a,b,u,v) = \big(b, a, v + F(b,a), u + F(a,b)\big). \tag{4.3}$$

Applying σ twice cancels the extra terms, so $\sigma^2 = \mathrm{id}$. It is also multiplicative. For $x = (a,b,u,v)$ and $y = (a',b',u',v')$, the third and fourth coordinates of both $\sigma(xy)$ and $\sigma(x)\sigma(y)$ are, respectively,

$$v + v' + F(b,a) + F(b,a') + F(b',a'),$$
$$u + u' + F(a,b) + F(a',b) + F(a',b').$$

The first two coordinates agree as well. Thus σ is an involutory automorphism of T.

Let

$$G = T \rtimes \langle t\rangle, \qquad t^2 = 1, \tag{4.4}$$

where conjugation by t acts on T as σ. Explicitly, elements are pairs (x,e) with $x \in T$ and $e \in \mathbb{F}_2$, and

$$(x,e)(y,f) = \big(x\sigma^e(y), e+f\big). \tag{4.5}$$

We identify T with the subgroup of pairs $(x,0)$. The order is

$$|G| = 2|K|^{110} = 2^{110N+1}, \tag{4.6}$$

so G is a finite 2-group.

The subset

$$E = \{(a,0,u,v) : a \in K^{45},\ u,v \in K^{10}\} \leq T \tag{4.7}$$

is a subgroup with coordinatewise addition, by (4.1). Hence E is the additive group of K^{65} and is elementary abelian of rank

$$d(E) = 65N. \tag{4.8}$$

5. A bound for every abelian normal subgroup

Let

$$W = \{(0,0,u,v) : u,v \in K^{10}\} \leq T.$$

Then W is central in T, normal in G, and elementary abelian of rank $20N$. The map

$$\pi : T \longrightarrow K^{45} \oplus K^{45}, \qquad \pi(a,b,u,v) = (a,b),$$

is a homomorphism with kernel W. On this quotient, conjugation by t induces the interchange

$$S(a,b) = (b,a).$$

Proposition 5.1. *For every abelian normal subgroup $A \trianglelefteq G$, one has $d(A) \leq 32N+1$.*

Proof. Put

$$H = \Omega_1(A) = \{x \in A : x^2 = 1\}.$$

Because A is abelian, H is an elementary abelian characteristic subgroup of A, and therefore $H \trianglelefteq G$. The decomposition of a finite abelian 2-group into cyclic factors gives

$$d(A) = \dim_{\mathbb{F}_2} H. \tag{5.1}$$

This is why it suffices to control normal elementary abelian subgroups, even though the problem allows abelian subgroups of larger exponent.

Let $H_0 = H \cap T$ and $U = \pi(H_0)$. Then U is an $\mathbb{F}_2$-linear subspace invariant under S. Define

$$X = \{a \in K^{45} : (a,a) \in U\}.$$

The kernel of $(S+\mathrm{id})|_U$ is exactly $\{(a,a) : a \in X\}$. In characteristic two,

$$(S+\mathrm{id})^2 = 0,$$

so the image of $(S+\mathrm{id})|_U$ lies in its kernel. Rank–nullity yields

$$\dim_{\mathbb{F}_2} U \leq 2\dim_{\mathbb{F}_2} X. \tag{5.2}$$

For $a \in X$, choose a lift $(a,a,u,v) \in H_0$. Since its square is the identity, (4.2) gives $F(a,a) = 0$. Thus all ten quadratic forms vanish on X. The space X is $\mathbb{F}_2$-linear, so for $a,b \in X$,

$$F(a,b) + F(b,a) = F(a+b,a+b) + F(a,a) + F(b,b) = 0. \tag{5.3}$$

Although X need not be K-linear, its K-linear span is a common zero subspace. Indeed, for $a_1, \dots, a_r \in X$ and $\lambda_1, \dots, \lambda_r \in K$, bilinearity gives

$$F\left(\sum_j \lambda_j a_j, \sum_j \lambda_j a_j\right) = \sum_j \lambda_j^2 F(a_j, a_j) + \sum_{j<k} \lambda_j \lambda_k (F(a_j, a_k) + F(a_k, a_j)) = 0. \tag{5.4}$$

Lemma 3.1 therefore gives

$$\dim_K \operatorname{span}_K(X) \leq 6, \qquad \dim_{\mathbb{F}_2} X \leq 6N.$$

Together with (5.2), this implies $\dim_{\mathbb{F}_2} U \leq 12N$.

The kernel of $\pi|_{H_0}$ is $H_0 \cap W$, whence

$$\dim_{\mathbb{F}_2} H_0 = \dim_{\mathbb{F}_2}(H_0 \cap W) + \dim_{\mathbb{F}_2} U \leq 20N + 12N = 32N.$$

Finally, H/H_0 embeds in G/T, which has order two. Therefore $\dim_{\mathbb{F}_2} H \leq 32N + 1$, and (5.1) proves the proposition. □

6. Failure of the proposed bound

Proof of Theorem 1.1. The group specified by (2.3), (2.4), (3.1)–(3.2), and (4.1)–(4.5) has the order stated in (4.6). Proposition 5.1 proves (1.1), and (4.8) proves (1.2). Set $k = 32N + 1$. Then every abelian normal subgroup can be generated by at most k elements, whereas

$$d(E) - 2k = 65N - 2(32N + 1) = N - 2 > 0.$$

This contradicts the proposed conclusion of Problem 20.75. Equivalently,

$$r(G) \geq 65N > 2(32N + 1) \geq 2\,\mathrm{nr}(G).$$

□

The value of N is chosen only to make the coefficient selection fully deterministic with a direct degree bound. It is the degree $[K : \mathbb{F}_2]$, not the order of K. No assertion of minimality is made. A single counterexample for $p = 2$ answers the stated question; the construction makes no assertion for odd primes.

Acknowledgement. This work was carried out with assistance from ChatGPT.

References

[HPPS] Z. Halasi, K. Podoski, L. Pyber, and E. Szabó, *On p-groups with a maximal elementary abelian normal subgroup of rank k*, J. Algebra **647** (2024), 744–757. doi:10.1016/j.jalgebra.2024.02.026. See also arXiv:2305.02037v2, Question 3.9.

[KN] E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved Problems in Group Theory. The Kourovka Notebook*, 21st ed., Novosibirsk, 2026, version 46, Problem 20.75, p. 157. arXiv:1401.0300v46.

Email address: kyrylo.muliarchyk@biu.ac.il