ON THE MINIMAL RAMIFICATION PROBLEM FOR SEMIABELIAN GROUPS

HERSHY KISILEVSKY, DANNY NEFTIN, AND JACK SONN

Abstract. It is known ([10], [12]) that for any prime \( p \) and any finite semiabelian \( p \)-group \( G \), there exists a (tame) realization of \( G \) as a Galois group over the rationals \( \mathbb{Q} \) with exactly \( d = d(G) \) ramified primes, where \( d(G) \) is the minimal number of generators of \( G \), which solves the minimal ramification problem for finite semiabelian \( p \)-groups. We generalize this result to obtain a theorem on finite semiabelian groups and derive the solution to the minimal ramification problem for a certain family of semiabelian groups that includes all finite nilpotent semiabelian groups \( G \). Finally, we give some indication of the depth of the minimal ramification problem for semiabelian groups not covered by our theorem.

1. Introduction

Let \( G \) be a finite group. Let \( d = d(G) \) be the smallest number for which there exists a subset \( S \) of \( G \) with \( d \) elements such that the normal subgroup of \( G \) generated by \( S \) is all of \( G \). One observes that if \( G \) is realizable as a Galois group \( G(K/\mathbb{Q}) \) with \( K/\mathbb{Q} \) tamely ramified (e.g. if none of the ramified primes divide the order of \( G \)), then at least \( d(G) \) rational primes ramify in \( K \) (see e.g. [10]). The minimal ramification problem for \( G \) is to realize \( G \) as the Galois group of a tamely ramified extension \( K/\mathbb{Q} \) in which exactly \( d(G) \) rational primes ramify. This variant of the inverse Galois problem is open even for \( p \)-groups, and no counterexample has been found. It is known that the problem has an affirmative solution for all semiabelian \( p \)-groups, for all rational primes \( p \) ([10], [12]). A finite group \( G \) is semiabelian if and only if \( G \in \mathcal{SA} \), where \( \mathcal{SA} \) is the smallest family of finite groups satisfying: (i) every finite abelian group belongs to \( \mathcal{SA} \). (ii) if \( G \in \mathcal{SA} \) and \( A \) is finite abelian, then any semidirect product \( A \rtimes G \) belongs to \( \mathcal{SA} \). (iii) if \( G \in \mathcal{SA} \), then every homomorphic image of \( G \) belongs to \( \mathcal{SA} \). In this paper we generalize this result to arbitrary finite semiabelian groups by means of a “wreath product length” \( \text{wl}(G) \) of a finite semiabelian group \( G \). When a finite semiabelian group \( G \) is nilpotent, \( \text{wl}(G) = d(G) \), which for nilpotent groups \( G \) equals the (more familiar) minimal number of generators of \( G \). Thus the general result does not solve the minimal ramification problem for all finite semiabelian groups, but does specialize to an affirmative solution to the

\[ \text{The research of the first author was supported in part by a grant from NSERC.} \]
minimal ramification problem for nilpotent semiabelian groups. Note that for a nilpotent group \( G \), \( d(G) = \max_p |G| d(G_p) \) and not \( \sum_p|G| d(G_p) \), where \( G_p \) is the \( p \)-Sylow subgroup of \( G \). Thus, a solution to the minimal ramification problem for nilpotent groups does not follow trivially from the solution for \( p \)-groups.

2. Properties of wreath products

2.1. Functoriality. The family of semiabelian groups can also be defined using wreath products. Let us recall the definition of a wreath product. Here and throughout the text the actions of groups on sets are all right actions.

Definition 2.1. Let \( G \) and \( H \) be two groups that act on the sets \( X \) and \( Y \), respectively. The \textit{(permutational) wreath product} \( H \wr_X G \) is the set \( H \times X \times G = \{ (f,g) \mid f : X \to H, g \in G \} \) which is a group with respect to the multiplication:

\[
(f_1,g_1)(f_2,g_2) = (f_1f_2g_1^{-1},g_1g_2),
\]

where \( f_2^{-1} \) is defined by \( f_2^{-1}(x) = f_2(xg_1) \) for any \( g_1, g_2 \in G, x \in X, f_1, f_2 : X \to H \).

The group \( H \wr_X G \) acts on the set \( Y \times X \) by \( (y,x) \cdot (f,g) = (yf(x),xg) \), for any \( y \in Y, x \in X, f : X \to H, g \in G \).

Definition 2.2. The \textit{standard (or regular) wreath product} \( H \wr G \) is defined as the permutational wreath product with \( X = G, Y = H \) and the right regular actions.

The functoriality of the arguments of a wreath product will play an important role in the sequel. The following five lemmas are devoted to these functoriality properties.

Definition 2.3. Let \( G \) be a group that acts on \( X \) and \( Y \). A map \( \phi : X \to Y \) is called a \( G \)-map if \( \phi(xg) = \phi(x)g \) for every \( g \in G \) and \( x \in X \).

Note that for such \( \phi \), we also have \( \phi^{-1}(y)g = \{ xg | \phi(x) = y \} = \{ x' \phi(x') = yg \} = \phi^{-1}(yg) \).

Lemma 2.4. Let \( G \) be a group that acts on the finite sets \( X, Y \) and let \( A \) be an abelian group. Then every \( G \)-map \( \phi : X \to Y \) induces a homomorphism \( \tilde{\phi} : A \wr_X G \to A \wr_Y G \) by defining: \( (\tilde{\phi}(f,g)) = (\hat{\phi}(f),g) \) for every \( f : X \to A \) and \( g \in G \), where \( \hat{\phi} : Y \to A \) is defined by:

\[
\hat{\phi}(f)(y) = \prod_{x \in \phi^{-1}(y)} f(x),
\]

for every \( y \in Y \). Furthermore, if \( \phi \) is surjective then \( \tilde{\phi} \) is an epimorphism.
Proof. Let us show the above $\tilde{\phi}$ is indeed a homomorphism. For this we claim: $\tilde{\phi}((f_1,g_1)(f_2,g_2)) = \tilde{\phi}(f_1,g_1)\tilde{\phi}(f_2,g_2)$ for every $g_1,g_2 \in G$ and $f_1,f_2 : X \to A$. By definition:

$$\tilde{\phi}(f_1,g_1)\tilde{\phi}(f_2,g_2) = (\hat{\phi}(f_1),g_1)(\hat{\phi}(f_2),g_2) = (\hat{\phi}(f_1)\hat{\phi}(f_2)^{g_1^{-1}},g_1g_2),$$

while: $\tilde{\phi}((f_1,g_1)(f_2,g_2)) = \tilde{\phi}(f_1f_2^{g_1^{-1}},g_1g_2) = (\hat{\phi}(f_1)f_2^{g_1^{-1}},g_1g_2)$. We shall show that $\hat{\phi}(f_1f_2) = \hat{\phi}(f_1)\hat{\phi}(f_2)$ and $\hat{\phi}(f^g) = \hat{\phi}(f)^g$ for every $f_1,f_2,f : X \to A$ and $g \in G$. Clearly this will imply the claim. The first assertion follows since:

$$\hat{\phi}(f_1f_2)(y) = \prod_{x \in \phi^{-1}(y)} f_1(x)f_2(x) = \prod_{x \in \phi^{-1}(y)} f_1(x) \prod_{x \in \phi^{-1}(y)} f_2(x) = \hat{\phi}(f_1)(y)\hat{\phi}(f_2)(y).$$

As to the second assertion we have:

$$\hat{\phi}(f^g)(y) = \prod_{x \in \phi^{-1}(y)} f^g(x) = \prod_{x \in \phi^{-1}(y)} f(xg^{-1}) = \prod_{x' \in \phi^{-1}(yg^{-1})} f(x') = \prod_{x' \in \phi^{-1}(g^{-1})} f(x').$$

Since $\phi$ is a $G$-map we have $\phi^{-1}(yg^{-1}) = \phi^{-1}(yg^{-1})$ and thus

$$\hat{\phi}(f^g)(y) = \prod_{x \in \phi^{-1}(yg^{-1})} f(x) = \prod_{x \in \phi^{-1}(y)} f(x) = \hat{\phi}(f)^g(y).$$

This proves the second assertion and hence the claim. It is left to show that if $\phi$ is surjective then $\tilde{\phi}$ is surjective. Let $f' : Y \to A$ and $g' \in G$. Let us define an $f : X \to A$ that will map to $f'$. For every $y \in Y$ choose an element $x_y \in X$ for which $\phi(x_y) = y$ and define $f(x_y) := f'(y)$. Define $f(x) = 1$ for any $x \notin \{x_y | y \in Y\}$. Then clearly

$$\hat{\phi}(f)(y) = \prod_{x \in \phi^{-1}(y)} f(x) = f(x_y) = f'(y).$$

Thus, $\tilde{\phi}(f,g') = (\hat{\phi}(f),g') = (f',g')$ and $\tilde{\phi}$ is onto.$\square$

Lemma 2.5. Let $B$ and $C$ be two groups. Then there is a surjective $B \wr C$-map $\phi : B \wr C \to B \times C$ defined by: $\phi(f,c) = (f(1),c)$ for every $f : C \to B, c \in C$.

Proof. Let $(f,c),(f',c')$ be two elements of $B \wr C$. We check that $\phi((f,c)(f',c')) = \phi(f,c)(f',c')$. Indeed,

$$\phi((f,c)(f',c')) = \phi(ff'^{-1},cc') = (f(1)f'^{-1}(1),cc') = (f(1)f'(c),cc') = (f(1),c)(f',c) = \phi(f,c)(f',c').$$
Note that the map $\phi$ is surjective: For every $b \in B$ and $c \in C$, one can choose a function $f_b : C \to B$ for which $f_b(1) = b$. One has: $\phi(f_b, c) = (b, c)$.

The following Lemma appears in [11] Part I, Chapter I, Theorem 4.13] and describes the functoriality of the first argument in the wreath product.

**Lemma 2.6.** Let $G, A, B$ be groups and $h : A \to B$ a homomorphism (resp. epimorphism). Then there is a naturally induced homomorphism (resp. epimorphism) $h_\ast : A \wr G \to B \wr G$ given by $h_\ast(f, g) = (h \circ f, g)$ for every $g \in G$ and $f : G \to A$.

The functoriality of the second argument is given in [12, Lemma 2.15] whenever the first argument is abelian:

**Lemma 2.7.** Let $A$ be an abelian group and let $\psi : G \to H$ be a homomorphism (resp. epimorphism) of finite groups. Then there is a homomorphism (resp. epimorphism) $\tilde{\psi} : A \wr G \to A \wr H$ that is defined by: $\tilde{\psi}(f, g) = (\psi(f), \psi(g))$ with $\tilde{\psi}(f)(h) = \prod_{k \in \psi^{-1}(h)} f(k)$ for every $h \in H$.

These functoriality properties can now be joined to give a connection between different bracketing of iterated wreath products:

**Lemma 2.8.** Let $A, B, C$ be finite groups and $A$ abelian. Then there are epimorphisms:

$$A \wr (B \wr C) \to (A \wr B) \wr C \to (A \times B) \wr C.$$ 

**Proof.** Let us first construct an epimorphism $h_\ast : (A \wr B) \wr C \to (A \times B) \wr C$. Define $h : A \wr B \to A \times B$ by:

$$h(f, b) = (\prod_{x \in B} f(x), b),$$

for any $f : B \to A, b \in B$. Since $A$ is abelian $h$ is a homomorphism. For every $a \in A$, let $f_a : B \to A$ be the map $f_a(b') = 0$ for any $1 \neq b' \in B$ and $f_a(e) = a$. Then clearly $h(f_a, b) = (a, b)$ for any $a \in A, b \in B$ and hence $h$ is onto. By Lemma 2.6, $h$ induces an epimorphism $h_\ast : (A \wr B) \wr C \to (A \times B) \wr C$. To construct the epimorphism $A \wr (B \wr C) \to (A \wr B) \wr C$, we shall use the associativity of the permutational wreath product (see [11] Theorem 3.2]). Using this associativity one has:

$$(A \wr B) \wr C = (A \wr_B B) \wr_C C \cong A \wr_{B \times C} (B \wr_C C).$$

It is now left to construct an epimorphism:

$$A \wr (B \wr C) = A \wr_{B \wr C} (B \wr_C C) \to A \wr_{B \times C} (B \wr_C C).$$

By Lemma 2.5, there is a $B \wr C$-map $\phi : B \wr C \to B \times C$ and hence by Lemma 2.4 there is an epimorphism $A \wr_{B \wr C} (B \wr C) \to A \wr_{B \times C} (B \wr C)$. 

$\Box$
Let us iterate Lemma 2.8. Let $G_1, \ldots, G_n$ be groups. The ascending iterated standard wreath product of $G_1, \ldots, G_n$ is defined as

$$
(\cdots ((G_1 \wr G_2) \wr G_3) \wr \cdots) \wr G_n,
$$

and the descending iterated standard wreath product of $G_1, \ldots, G_n$ is defined as

$$
G_1 \wr (G_2 \wr (G_3 \cdots \wr G_n)) \cdots.
$$

These two iterated wreath products are not isomorphic in general, as the standard wreath product and non-associative (as opposed to the “permutation” wreath product). We shall abbreviate and write $G$ for a perfect group.

By iterating the epimorphism in Lemma 2.8 one obtains:

**Corollary 2.9.** Let $A_1, \ldots, A_r$ be abelian groups. Then $(A_1 \wr \ldots \wr A_{r-1}) \wr A_r$ is an epimorphic image of $A_1 \wr (A_2 \wr \ldots \wr A_r)$.

**Proof.** By induction on $r$. The cases $r = 1, 2$ are trivial; assume $r \geq 3$. By the induction hypothesis there is an epimorphism

$$
\pi_1 : (A_1 \wr \ldots \wr A_{r-1}) \rightarrow (A_1 \wr \ldots \wr A_{r-2}) \wr A_{r-1}.
$$

By Lemma 2.8, $\pi_1$ induces an epimorphism $\pi_1 : (A_1 \wr (A_2 \wr \ldots \wr A_{r-1})) \wr A_r \rightarrow (A_1 \wr \ldots \wr A_{r-1}) \wr A_r$. Applying Lemma 2.8 with $A = A_1, B = A_2 \wr (A_3 \wr \ldots \wr A_{r-1}), C = A_r$, one obtains an epimorphism:

$$
\pi_2 : A_1 \wr (A_2 \wr \ldots \wr A_r) \rightarrow (A_1 \wr (A_2 \wr \ldots \wr A_{r-1})) \wr A_r.
$$

Taking the composition $\pi = \pi_1 \pi_2$ one obtains an epimorphism

$$
\pi : A_1 \wr (A_2 \wr \ldots \wr A_r) \rightarrow (A_1 \wr \ldots \wr A_{r-1}) \wr A_r.
$$

2.2. Dimension under epimorphisms. Let us understand how the “dimension” $d$ behaves under the homomorphisms in Lemma 2.8 and Corollary 2.9. By Lemma 2.8, for any finite group $G$ that is not perfect, i.e. $[G, G] \neq G$, where $[G, G]$ denotes the commutator subgroup of $G$, one has $d(G) = d(G/[G, G])$. According to our definitions, for a perfect group $G$, $d(G/[G, G]) = d(\{1\}) = 0$, but if $G$ is nontrivial, $d(G) \geq 1$. As nontrivial semiabelian groups are not perfect, this difference will not effect any of the arguments in the sequel.

**Definition 2.10.** Let $G$ be a finite group and $p$ a prime. Define $d_p(G)$ to be the rank of the $p$-Sylow subgroup of $G/[G, G]$, i.e. $d_p(G) := d((G/[G, G])_p)$.

Note that if $G$ is not perfect one has $d(G) = \max_p(d_p(G))$.

Let $p$ be a prime. An epimorphism $f : G \rightarrow H$ is called $d$-preserving (resp. $d_p$-preserving) if $d(G) = d(H)$ (resp. $d_p(G) = d_p(H)$).
Lemma 2.11. Let $G$ and $H$ be two finite groups. Then:

$$H \wr G/[H \wr G, H \wr G] \cong H/[H, H] \times G/[G, G].$$

Proof. Applying Lemmas 2.6 and 2.7 one obtains an epimorphism

$$H \wr G \to H/[H, H] \wr G/[G, G].$$

By Lemma 2.8 (applied with $C = 1$) there is an epimorphism

$$H/[H, H] \wr G/[G, G] \to H/[H, H] \times G/[G, G].$$

Composing these epimorphisms one obtains an epimorphism

$$\pi: H \wr G \to H/[H, H] \times G/[G, G],$$

that sends an element $(f : G \to H, g) \in H \wr G$ to

$$\left( \prod_{x \in G} f(x)[H, H], g[G, G] \right) \in H/[H, H] \times G/[G, G].$$

The image of $\pi$ is abelian and hence $\ker(\pi)$ contains $K := [H \wr G, H \wr G]$.

Let us show $K \supseteq \ker(\pi)$. Let $(f, g) \in \ker(\pi)$. Then $g \in [G, G]$ and $\prod_{x \in G} f(x) \in [H, H]$. As $g \in [G, G]$, it suffices to show that the element $f = (f, 1) \in H \wr G$ is in $K$.

Let $g_1, \ldots, g_n$ be the elements of $G$ and for every $i = 1, \ldots, n$, let $f_i$ be the function for which $f_i(g_i) = f(g_i)$ and $f(g_j) = 1$ for every $j \neq i$. One can write $f$ as $\prod_{i=1}^n f_i$. Now for every $i = 1, \ldots, n$, the function $f_{1,i} = f_i^{g_i^{-1}}$ satisfies $f_{1,i}(1) = f(g_i)$ and $f_{1,i}(g_j) = 1$ for every $j \neq 1$. Thus $f_i$ is a product of an element in $[H[G], G]$ and $f_i$. So, $f$ is a product of elements in $[H[G], G]$ and $f' = \prod_{i=1}^n f_{1,i}$. But $f'(1) = \prod_{x \in G} f(x) \in [H, H]$ and $f'(g_i) = 1$ for every $i \neq 1$ and hence $f' \in [H[G], H[G]]$. Thus, $f \in K$ as required and $K = \ker(\pi)$.

The following is an immediate conclusion:

Corollary 2.12. Let $G$ and $H$ be two finite groups. Then

$$d_p(H \wr G) = d_p(H) + d_p(G)$$

for any prime $p$.

So, for groups $A, B, C$ as in Lemma 2.8 we have:

$$d_p(A \wr (B \wr C)) = d_p((A \times B) \wr C) = d_p(A \times B \times C) = d_p(A) + d_p(B) + d_p(C)$$

for every $p$. In particular, the epimorphisms in Lemma 2.8 are $d$-preserving.

The same observation holds for Corollary 2.9 so one has:
Lemma 2.13. Let $A_1, \ldots, A_r$ be finite abelian groups. Then
$$d_p(A_1 \wr (A_2 \wr \ldots \wr A_r)) = d_p((A_1 \wr \ldots \wr A_{r-1}) \wr A_r) = d_p(A_1 \times \ldots \times A_r)$$
are all $\sum_{i=1}^r d_p(A_i)$ for any prime $p$.

For cyclic groups $A_1, \ldots, A_r$, $d_p(A_1 \wr (A_2 \wr \ldots \wr A_r))$ is simply the number of cyclic groups among $A_1, \ldots, A_r$ whose $p$-part is non-trivial. Thus:

Corollary 2.14. Let $C_1, \ldots, C_r$ be finite cyclic groups and $G = C_1 \wr (C_2 \wr \ldots \wr C_r)$. Then $d(G) = \max_{p \mid |G|} d(C_1(p) \wr (C_2(p) \wr \ldots \wr C_r(p)))$.

Let us apply Lemma 2.8 in order to connect between descending iterated wreath products of abelian and cyclic groups:

Proposition 2.15. Let $A_1, \ldots, A_r$ be finite abelian groups and let $A_i$ have invariant factors $C_{i,j}$ for $j = 1, \ldots, l_i$, i.e. $A_i = \prod_{j=1}^{l_i} C_{i,j}$ and $|C_{i,j}| = |C_{i,j+1}|$ for any $i = 1, \ldots, r$ and $j = 1, \ldots, l_i - 1$. Then there is an epimorphism from the descending iterated wreath product $\tilde{G} := \prod_{i=1}^{l_i} C_{i,j}$ (here the groups $C_{i,j}$ are ordered lexicographically: $C_{1,1}, C_{1,2}, \ldots, C_{1,l_1}, C_{2,1}, \ldots, C_{r,l_r}$) to $G := A_1 \wr (A_2 \wr \ldots \wr A_r)$.

Proof. Let us assume $A_1 \neq \{0\}$ (otherwise $A_1$ can be simply omitted). Let us prove the assertion by induction on $\sum_{i=1} l_i$. Let $G_2 = A_2 \wr (A_3 \wr \ldots \wr A_k)$. Write $A_1 = C_{1,1} \times A_1'$. By Lemma 2.8 there is an epimorphism $\pi_1 : C_{1,1} \wr (A_1' \wr G_2) \to (C_{1,1} \times A_1') \wr G_2 = A_1 \wr G_2 = G$. By applying the induction hypothesis to $A_1', A_2, \ldots, A_r$, there is an epimorphism $\pi_2'$ from the descending iterated wreath product $\tilde{G}_2 = \prod_{i=2}^{l_i} C_{i,j} \wr (\prod_{i=2}^{l_i} C_{i,j} \wr G_2)$ to $A_1' \wr G_2$. By Lemma 2.7, $\pi_2'$ induces an epimorphism $\pi_2 : C_{1,1} \wr G_2 \to C_{1,1} \wr (A_1' \wr G_2)$. Taking the composition $\pi = \pi_2 \pi_1$, we obtain the required epimorphism: $\pi : \tilde{G} = C_{1,1} \wr \tilde{G}_2 \to G$. \qed

Remark 2.16. Note that:
$$d_p(\tilde{G}) = \sum_{i=1}^r \sum_{j=1}^{l_i} d_p(C_{i,j}) = \sum_{i=1}^r d_p(A_i) = d_p(G)$$
for every $p$ and hence $\pi$ is $d$-preserving.

Therefore, showing $G$ is a $d$-preserving epimorphic image of an iterated wreath product of abelian groups is equivalent to showing $G$ is a $d$-preserving epimorphic image of an iterated wreath product of finite cyclic groups.

3. Wreath Length

The following lemma is essential for the definition of wreath length:
Lemma 3.1. Let $G$ be a finite semiabelian group. Then $G$ is a homomorphic image of a descending iterated wreath product of finite cyclic groups, i.e. there are finite cyclic groups $C_1, \ldots, C_r$ and an epimorphism $C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.

Proof. By Proposition 2.15 it suffices to show $G$ is an epimorphic image of a descending iterated wreath product of finite abelian groups. We shall prove this claim by induction on $|G|$. The case $G = \{1\}$ is trivial. By [3], $G = A_1H$ with $A_1$ an abelian normal subgroup and $H$ a proper semiabelian subgroup of $G$. First, there is an epimorphism $\pi_1 : A_1 \wr H \to A_1H = G$. By induction there are abelian groups $A_2, \ldots, A_r$ and an epimorphism $\pi_2 : A_2 \wr (A_3 \wr \cdots \wr A_r) \to H$. By Lemma 2.6 $\pi_2'$ can be extended to an epimorphism $\pi_2 : A_1 \wr (A_2 \wr \cdots \wr A_r) \to A_1 \wr H$. So, by taking the composition $\pi = \pi_1 \pi_2$ one obtains the required epimorphism $\pi : A_1 \wr (A_2 \wr \cdots \wr A_r) \to G$.

We can now define:

Definition 3.2. Let $G$ be a finite semiabelian group. Define the wreath length $\text{wl}(G)$ of $G$ to be the smallest positive integer $r$ such that there are finite cyclic groups $C_1, \ldots, C_r$ and an epimorphism $C_1 \wr (C_2 \wr \cdots \wr C_r) \to G$.

Let $\tilde{G} = C_1 \wr (C_2 \wr \cdots \wr C_r)$ and $\pi : \tilde{G} \to G$ an epimorphism. Then by Corollary 2.14

$$\text{d}(G) \leq \text{d}(\tilde{G}) \leq r.$$

In particular $\text{d}(G) \leq \text{wl}(G)$.

Proposition 3.3. Let $C_1, \ldots, C_r$ be nontrivial finite cyclic groups. Then $\text{wl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r$.

Let $\text{dl}(G)$ denote the derived length of a (finite) solvable group $G$, i.e. the smallest positive integer $n$ such that the $n$th higher commutator subgroup of $G$ ($n$th element in the derived series $G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(i)} \geq \cdots$) is trivial. In order to prove this proposition we will use the following lemma:

Lemma 3.4. Let $C_1, \ldots, C_r$ be nontrivial finite cyclic groups. Then $\text{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) = r$.

Proof. It is easy (by induction) to see that $\text{dl}(C_1 \wr (C_2 \wr \cdots \wr C_r)) \leq r$. We turn to the reverse inequality. By Corollary 2.11, it suffices to prove it for the ascending iterated wreath product $G = (C_1 \wr \cdots \wr C_{r-1}) \wr C_r$. We prove this by induction on $r$. The case $r = 1$ is trivial. Assume $r \geq 1$. Write $G_1 := (C_1 \wr \cdots \wr C_{r-2}) \wr C_{r-1}$ so that $G = G_1 \wr C_r$. By induction hypothesis, $\text{dl}(G_1) = r - 1$. View $G$ as the semidirect product $G_1^r \rtimes C_r$. For any $g \in G_1$, the element $t_g := (g, g^{-1}, 1, 1, \ldots, 1) \in G_1^r \wr C_r$ lies in $[G_1^r, C_r]$ and hence in $[G_1^r, C_r] \leq G' \leq G''$. Let $H = \{t_g | g \in G_1\}$. The projection map $G_1^r \to G_1$ onto the first copy of $G_1$ in $G_1^r$ maps $H$ onto $G_1$. Since $H \leq G'$, the projection map also maps $G'$ onto $G$. Now $\text{dl}(G_1) = r - 1$ by the induction hypothesis. It follows that $\text{dl}(G') \geq r - 1$, whence $\text{dl}(G) \geq r$. \qed
To prove the proposition, we first observe that $\text{wl}(C_1 \wr (C_2 \wr \ldots \wr C_r)) \leq r$ by definition. If $C_1 \wr (C_2 \wr \ldots \wr C_r)$ were a homomorphic image of a shorter descending iterated wreath product $C'_1 \wr (C'_2 \wr \ldots \wr C'_s)$, then by Lemma 3.1 $s = \text{dl}(C'_1 \wr (C'_2 \wr \ldots \wr C'_s)) \geq \text{dl}(C_1 \wr (C_2 \wr \ldots \wr C_r)) = r > s$, contradiction.

Combining Proposition 3.3 with Corollary 2.14 we have:

**Corollary 3.5.** Let $C_1, \ldots, C_r$ be finite cyclic groups and $G = C_1 \wr (C_2 \wr \ldots \wr C_r)$. Then $\text{wl}(G) = \text{d}(G)$ if and only if there is a prime $p$ for which $p \mid |C_1|, \ldots, |C_r|$.

We shall now see that all examples of groups $G$ with $\text{wl}(G) = \text{d}(G)$ arise from Corollary 3.5.

**Proposition 3.6.** Let $G$ be a finite semiabelian group. Then $\text{wl}(G) = \text{d}(G)$ if and only if there is a prime $p$, finite cyclic groups $C_1, \ldots, C_r$ for which $p \mid |C_i|, i = 1, \ldots, r$, and a $d$-preserving epimorphism $\pi : C_1 \wr (C_2 \wr \ldots \wr C_r) \twoheadrightarrow G$.

**Proof.** Let $d = \text{d}(G)$. The equality $d = \text{wl}(G)$ holds if and only if there are finite cyclic groups $C_1, C_2, \ldots, C_d$ and an epimorphism $\pi : \tilde{G} = C_1 \wr (C_2 \wr \ldots \wr C_d) \twoheadrightarrow G$. Assume the latter holds. Clearly $d \leq \text{d}(\tilde{G})$ but by Corollary 2.14 applied to $\tilde{G}$ we also have $\text{d}(\tilde{G}) \leq d$. It follows that $\pi$ is $d$-preserving. Since $\text{d}(G) = \max_p (\text{d}_p(G))$, there is a prime $p$ for which $d = \text{d}_p(G)$ and hence $\text{d}_p(\tilde{G}) = d$. Thus, $p \mid |C_i|$ for all $i = 1, \ldots, r$.

Let us prove the converse. Assume there is a prime $p$, finite cyclic groups $C_1, \ldots, C_r$ for which $p \mid |C_i|, i = 1, \ldots, r$, and a $d$-preserving epimorphism $\pi : \tilde{G} := C_1 \wr (C_2 \wr \ldots \wr C_r) \twoheadrightarrow G$. Since $p \mid |C_i|$, it follows that $\text{d}_p(\tilde{G}) = r$. As $\text{d}_p(\tilde{G}) \leq \text{d}(\tilde{G}) \leq r$, it follows that $\text{d}(G) = \text{d}(\tilde{G}) = r$. In particular $\text{wl}(G) \leq r = \text{d}(G)$ and hence $\text{wl}(G) = \text{d}(G)$. \qed

**Remark 3.7.** Let $G$ be a semiabelian $p$-group. By [12, Corollary 2.15], $G$ is a $d$-preserving image of an iterated wreath product of abelian subgroups of $G$ (following the proof one can observe that the abelian groups were actually subgroups of $G$). So, by Proposition 2.15 $G$ is a $d$-preserving epimorphic image of $\tilde{G} := C_1 \wr (C_2 \wr \ldots \wr C_k)$ for cyclic subgroups $C_1, \ldots, C_k$ of $G$. By applying Proposition 3.6 one obtains $\text{wl}(G) = \text{d}(G)$.

**Remark 3.8.** Throughout the proof of [12, Corollary 2.15] one can use the minimality assumption posed on the decompositions to show directly that the abelian groups $A_1, \ldots, A_r$, for which there is a $d$-preserving epimorphism $A_1 \wr (A_2 \wr \ldots \wr A_r) \twoheadrightarrow G$, can be actually chosen to be cyclic.

We shall generalize Remark 3.7 to nilpotent groups:

**Proposition 3.9.** Let $G$ be a finite nilpotent semiabelian group. Then $\text{wl}(G) = \text{d}(G)$.
Proof. Let \( d = d(G) \). Let \( p_1, \ldots, p_k \) be the primes dividing \( |G| \) and let \( P_i \) be the \( p_i \)-Sylow subgroup of \( G \) for every \( i = 1, \ldots, k \). So, \( G \cong \prod_{i=1}^k P_i \). By Remark 3.7 there are cyclic \( p_i \)-groups \( C_{i,1}, \ldots, C_{i,r_i} \) and a \( d \)-preserving epimorphism \( \pi_i : C_{i,1} \ast \ldots \ast C_{i,r_i} \to P_i \) for every \( i = 1, \ldots, k \). In particular for any \( i = 1, \ldots, k \), \( r_i = d(P_i) = d_p(G) \leq d \). For any \( i = 1, \ldots, k \) and any \( d \geq j > r_i \), set \( C_{i,j} = \{1\} \). For any \( j = 1, \ldots, d \) define \( C_j = \prod_{i=1}^k C_{i,j} \).

We claim \( G \) is an epimorphic image of \( \tilde{G} = C_1 \ast \ldots \ast C_d \). To prove this claim it suffices to show every \( P_i \) is an epimorphic image of \( \tilde{G} \) for every \( i = 1, \ldots, k \). As \( C_{i,j} \) is an epimorphic image of \( C_j \) for every \( j = 1, \ldots, d \) and every \( i = 1, \ldots, k \), one can apply Lemmas 2.6 and 2.7 iteratively to obtain an epimorphism \( \pi'_i : \tilde{G} \to C_{i,1} \ast \ldots \ast C_{i,r_i} \) for every \( i = 1, \ldots, k \). Taking the composition \( \pi'_1 \pi_i \) gives the required epimorphism and proves the claim. As \( G \) is an epimorphic image of an iterated wreath product of \( d(G) \) cyclic groups one has \( \text{wl}(G) \leq d(G) \) and hence \( \text{wl}(G) = d(G) \).

Example 3.10. Let \( G = D_n = \langle \sigma, \tau | \sigma^2 = 1, \tau^n = 1, \sigma \tau \sigma = \tau^{-1} \rangle \) for \( n \geq 3 \). Since \( G \) is an epimorphic image of \( \langle \tau \rangle \ast \langle \sigma \rangle \) and \( G \) is not abelian we have \( \text{wl}(G) = 2 \). On the other hand \( d(G) = d(G/[G,G]) \) is 1 if \( n \) is odd and 2 if \( n \) is even. So, \( G = D_3 = S_3 \) is the minimal example for which \( \text{wl}(G) \neq d(G) \).

4. A RAMIFICATION BOUND FOR SEMIABELIAN GROUPS

In this section we prove:

Theorem 4.1. Let \( G \) be a finite semiabelian group. Then there exists a tamely ramified extension \( K/\mathbb{Q} \) with \( G(K/\mathbb{Q}) \cong G \) in which at most \( \text{wl}(G) \) primes ramify.

The proof relies on the splitting Lemma from [10]: Let \( \ell \) be a rational prime, \( K \) a number field and \( p \) a prime of \( K \) that is prime to \( \ell \). Let \( I_{K,p} \) denote the group of fractional ideals prime to \( p \), \( P_{K,p} \) the subgroup of principal ideals that are prime to \( p \) and let \( P_{K,p,1} \) be the subgroup of principal ideals \( (\alpha) \) with \( \alpha \equiv 1 \pmod{p} \). Let \( P_{K,p}^\ell \) denote \( P_{K,p}/P_{K,p,1} \). The ray class group \( \text{Cl}_{K,p} \) is defined to be \( I_{K,p}/P_{K,p,1} \). Now, as \( I_{K,p}/P_{K,p} \cong \text{Cl}_K \), one has the following short exact sequence:

\[
1 \longrightarrow P_{K,p}^\ell \longrightarrow C_{K,p}^\ell \longrightarrow C_{K}^\ell \longrightarrow 1,
\]

where \( A^\ell \) denotes the \( \ell \)-primary component of an abelian group \( A \). Let us describe a sufficient condition for the splitting of (4.1). Let \( \bar{a}_1, \ldots, \bar{a}_r \in I_{K,p}, \bar{a}_1, \ldots, \bar{a}_r \) their classes in \( C_{K,p}^\ell \), with images \( \bar{a}_1, \ldots, \bar{a}_r \) in \( C_{K}^\ell \), so that \( C_{K,p}^\ell = \langle \bar{a}_1 \rangle \times \langle \bar{a}_2 \rangle \times \ldots \times \langle \bar{a}_r \rangle \). Let \( \ell^m_i := |\langle \bar{a}_i \rangle| \) and let \( a_i \in K \) satisfy \( \ell^m_i = (a_i) \), for \( i = 1, \ldots, r \).

Lemma 4.2. (Kisilevsky-Sonn [9]) Let \( p \) be a prime of \( K \) and let \( K' = K(\sqrt[n]{a_i}|i = 1, \ldots, r) \). If \( p \) splits completely in \( K' \) then the sequence (4.1) splits.
The splitting of (4.1) was used in [10] to construct cyclic ramified extensions at one prime only. Let \( m = \max\{1, m_1, \ldots, m_r\} \). Let \( U_K \) denote the units in \( \mathcal{O}_K \).

**Lemma 4.3.** (Kisilevsky-Sonn [10]) Let \( K'' = K(\mu_m, \sqrt{\zeta}, \sqrt[m]{a_i}) \xi \in U_K, i = 1, \ldots, r \) and \( p \) a prime of \( K \) which splits completely in \( K'' \). Then there is a cyclic \( \ell^m \)-extension of \( K \) that is totally ramified at \( p \) and is not ramified at any other prime of \( K \).

**Corollary 4.4.** Let \( K \) be a number field, \( n \) a positive integer. Then there exists a finite extension \( K'' \) of \( K \) such that if \( p \) is any prime of \( K \) that splits completely in \( K'' \), then there exists a cyclic extension \( L/K \) of degree \( n \) in which \( p \) is totally ramified and \( p \) is the only prime of \( K \) that ramifies in \( L \).

**Proof.** Let \( n = \prod \ell^m(\ell) \) be the decomposition of \( n \) into primes. Let \( K'' \) be the composite of the fields \( K'' = K''(\ell) \) in Lemma 4.3 \( (m = m(\ell)) \). Let \( L(\ell) \) be the cyclic extension of degree \( \ell^m(\ell) \) yielded by Lemma 4.3. The composite \( L = \prod L(\ell) \) has the desired property. \( \square \)

**Proof.** (Theorem 4.1) By definition, \( G \) is a homomorphic image of a descending iterated wreath product of cyclic groups \( C_1 \wr (C_2 \wr \cdots \wr C_r) \), \( r = \text{wr}(G) \). Without loss of generality \( G \cong C_1 \wr (C_2 \wr \cdots \wr C_r) \) is itself a descending iterated wreath product of cyclic groups. Proceed by induction on \( r \). For \( r = 1 \), \( G \) is cyclic of order \( N \). If \( p \) is a rational prime \( \equiv 1 \pmod{N} \), then the field of \( p \)th roots of unity \( \mathbb{Q}(\mu_p) \) contains a subfield \( L \) cyclic over \( \mathbb{Q} \) with Galois group \( G \) and exactly one ramified prime, namely \( p \). Thus the theorem holds for \( r = 1 \).

Assume \( r > 1 \) and the theorem holds for \( r - 1 \). Let \( K_1/\mathbb{Q} \) be a tamely ramified Galois extension with \( G(K_1/\mathbb{Q}) \cong G_1 \), where \( G_1 \) is the descending iterated wreath product \( C_1 \wr (C_2 \wr \cdots \wr C_r) \), such that the ramified primes in \( K_1 \) are a subset of \( \{p_2, \ldots, p_r\} \). By Corollary 4.4, there exists a prime \( p = p_1 \) not dividing the order of \( G \) which splits completely in \( K''_1 \), the field supplied for \( K_1 \) by Corollary 4.4, and let \( p = p_1 \) be a prime of \( K_1 \) dividing \( p \). By Corollary 4.3, there exists a cyclic extension \( L/K_1 \) with \( G(L/K_1) \cong C_1 \) in which \( p \) is totally ramified and in which \( p \) is the only prime of \( K_1 \) which ramifies in \( L \).

Now \( p \) has \( |G_1| \) distinct conjugates \( \{\sigma(p) \mid \sigma \in G(K_1/\mathbb{Q})\} \) over \( K_1 \). For each \( \sigma \in G(K_1/\mathbb{Q}) \), the conjugate extension \( \sigma(L)/K_1 \) is well-defined, since \( K_1/\mathbb{Q} \) is Galois. Let \( M \) be the composite of the \( \sigma(L) \), \( \sigma \in G(K_1/\mathbb{Q}) \). For each \( \sigma \), \( \sigma(L)/K_1 \) is cyclic of degree \( |C_1| \), ramified only at \( \sigma(p) \), and \( \sigma(p) \) is totally ramified in \( \sigma(L)/K_1 \). It now follows (see e.g. [10] Lemma 1) that the fields \( \{\sigma(L) \mid \sigma \in G(K_1/\mathbb{Q})\} \) are linearly disjoint over \( K_1 \), hence \( G(M/\mathbb{Q}) \cong C_1 \wr G_1 \cong G \). Since the only primes of \( K_1 \) ramified in \( M \) are \( \{\sigma(p) \mid \sigma \in G(K_1/\mathbb{Q})\} \), the only rational primes ramified in \( M \) are \( p_1, p_2, \ldots, p_n \). \( \square \)
Corollary 4.5. The minimal ramification problem has a positive solution for all finite semiabelian groups \( G \) for which \( \text{wl}(G) = d(G) \). Precisely, any finite semiabelian group \( G \) for which \( \text{wl}(G) = d(G) \) can be realized tamely as a Galois group over the rational numbers with exactly \( d(G) \) ramified primes.

By Proposition 3.9, we have

Corollary 4.6. The minimal ramification problem has a positive solution for all finite nilpotent semiabelian groups.

5. Arithmetic consequences

In this section we examine some arithmetic consequences of a positive solution to the minimal ramification problem. Specifically, given a group \( G \), the existence of infinitely many minimally tamely ramified \( G \)-extensions \( K/\mathbb{Q} \) is re-interpreted in some cases in terms of some open problems in algebraic number theory. We will be most interested in the case \( d(G) = 1 \).

Proposition 5.1. Let \( q \) and \( \ell \) be distinct primes. Let \( K/\mathbb{Q} \) be a cyclic extension of degree \( n := [K : \mathbb{Q}] \geq 2 \) with \( (n, q\ell) = 1 \). Suppose that \( K/\mathbb{Q} \) is totally and tamely ramified at a unique prime \( l \) dividing \( \ell \). Then \( q \) divides the class number \( h_K \) of \( K \) if and only if there exists an extension \( L/K \) satisfying the following:

i). \( L/\mathbb{Q} \) is a Galois extension with non-abelian Galois group \( G = G(L/\mathbb{Q}) \).

ii). The degree \( [L : K] = q^s \) is a power of \( q \).

iii). \( L/\mathbb{Q} \) is (tamely) ramified only at primes over \( \ell \).

Proof. First suppose that \( q \) divides \( h_K \). Let \( K_0 \) be the \( q \)-Hilbert class field of \( K \), i.e. \( K_0/K \) is the maximal unramified abelian \( q \)-extension of \( K \). Then \( K_0/\mathbb{Q} \) is a Galois extension with Galois group \( G := G(K_0/\mathbb{Q}) \), and \( H := G(K_0/K) \simeq (C_K)_q \neq 0 \), the \( q \)-part of the ideal class group of \( K \). Then \([G,G]\) is contained in \( H \). If \([G,G] \subseteq H\), then the fixed field of \([G,G]\) would be an abelian extension of \( \mathbb{Q} \) which contains an unramified \( q \)-extension of \( \mathbb{Q} \) which is impossible. Hence \([G,G] = H \neq 0 \) and so \( G \) is a non-abelian group, and \( L = K_0 \) satisfies \( i), ii)\), and \( iii) \) of the statement.

Conversely suppose that there is an extension \( L/K \) satisfying \( i), ii)\), and \( iii) \) of the statement. Since \( H = G(L/K) \) is a \( q \)-group, there is a sequence of normal subgroups \( H = H_0 \supset H_1 \supset H_2 \cdots \supset H_s = 0 \) with \( H_i/H_{i+1} \) a cyclic group of order \( q \). Let \( L_i \) denote the fixed field of \( H_i \) so that \( K = L_0 \supset \cdots \supset L_s = L \). Let \( m \) be the largest index such that \( L_m/\mathbb{Q} \) is totally ramified (necessarily at \( \ell \)). If \( m = s \), then \( L/\mathbb{Q} \) is totally and tamely ramified at \( \ell \) and so the inertia group \( T(\mathfrak{L}/(\ell)) = G \), where in this case \( \mathfrak{L} \) is the unique prime of \( L \) dividing \( \ell \). Since \( L/\mathbb{Q} \) is tamely ramified it follows that \( T(\mathfrak{L}/(\ell)) \) is cyclic, but this contradicts the hypothesis that \( G \) is non-abelian. Therefore it follows that \( m < s \), and so \( L_{m+1}/L_m \) is unramified and therefore \( q \) must...
We now apply this to the case that $G \neq \{1\}$ is a quotient of the regular wreath product $C_q \wr C_p$ where $p$ and $q$ are distinct primes. Then $d(G) = 1$.

The existence of infinitely many minimally tamely ramified $G$-extensions $L/\mathbb{Q}$ would by Proposition 5.1 imply the existence of infinitely many cyclic extensions $K/\mathbb{Q}$ of degree $[K : \mathbb{Q}] = p$ ramified at a unique prime $\ell \neq p, q$ for which $q$ divides the class number $h_K$. (If there were only finitely many distinct such cyclic extensions $K/\mathbb{Q}$, then the number of ramified primes $\ell$ would be bounded, and there would be an absolute upper bound on the possible discriminants of the distinct fields $L/\mathbb{Q}$. By Hermite’s theorem, this would mean that the number of such $G$-extensions $L/\mathbb{Q}$ would be bounded).

The question of whether there is an infinite number of cyclic degree $p$ extensions (or even one) of $\mathbb{Q}$ whose class number is divisible by $q$ is in general open at this time.

For $p = 2$, it is known that there are infinitely many quadratic fields (see Ankeny, Chowla [1]), with class numbers divisible by $q$, but it is not known that this occurs for quadratic fields with prime discriminant.

This latter statement is also a consequence of Schinzel’s hypothesis as is shown by Plans in [13]. There is also some numerical evidence that the heuristic of Cohen-Lenstra should be statistically independent of the primality of the discriminant (see Jacobson, Lukes, Williams [6] or te Riele, Williams [15]). If this were true, then one would expect that there is a positive density of primes $\ell$ for which the cyclic extension of degree $p$ and conductor $\ell$ would have class number divisible by $q$.

For $p = 3$ it has been proved by Bhargava [11] that there are infinitely many cubic fields $K/\mathbb{Q}$ for which 2 divides their class numbers. That there are infinitely many cyclic cubics with prime squared discriminants whose class numbers are even (or more generally divisible by some fixed prime $q$) seems out of reach at this time.

In our view, there is a significant arithmetic interest in solving the minimal ramification problem for other groups (see also [4], [7], [14]).

References

[1] Ankeny, N. C.; Chowla, S. On the divisibility of the class number of quadratic fields. Pacific J. Math. 5 (1955), 321–324.
[2] Bhargava, M., The density of discriminants of quartic rings and fields, Annals of Math. 162 (2005), no. 2, 1031–1062
[3] Dentzer, R., On geometric embedding problems and semiabelian groups, Manuscripta Math. 86 (1995), no. 2, 199–216.
[4] Harbater, D. *Galois groups with prescribed ramification*, Proceedings of a Conference on Arithmetic Geometry (Arizona State Univ., 1993), AMS Contemporary Mathematics Series, vol. 174, (1994), pp. 35–60.

[5] Iwasawa, K. *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg, 20 (1956), 257–258. – also in Kenkichi Iwasawa Collected Papers, Volume 1, 32, p.372-373, Springer. ISBN4-431-70314-4

[6] Jacobson, M.J., Lukes, R.F., and Williams, H.C. *An investigation of bounds for the regulator of quadratic fields*, Experimental Mathematics, 4 (1995), no. 3, 211–225.

[7] Jones, J. W., Roberts, D. P. *Number fields ramified at one prime*, Lecture Notes in Comput. Sci., 5011, Springer, Berlin, (2008), 226–239.

[8] Kaplan, G., Lev, A. *On the dimension and basis concepts in finite groups*, Comm. Alg. 31 no. 6 (2003), 2707–2717.

[9] Kisilevsky, H., Sonn, J., *Abelian extensions of global fields with constant local degrees*, Math. Research Letters 13 no.4 (2006), 599–605.

[10] Kisilevsky, H., Sonn, J., *On the minimal ramification problem for \( \ell \)-groups*, Compositio Math. (to appear)

[11] Meldrum, J.D.P., *Wreath products of groups and semigroups*, Monographs and Surveys in Pure and Applied Mathematics.

[12] Neftin, D., *On semiabelian \( p \)-groups*, submitted.

[13] Plans, B., *On the minimal number of ramified primes in some solvable extensions of \( \mathbb{Q} \)*. Pacific J. Math. 215 (2004), no. 2, 381–391.

[14] Rabayev, D., *Polynomials with roots mod \( n \) for all \( n \)*, Master Thesis, (2009), Technion.

[15] te Riele, H.J., Williams, H.C., *New computations concerning the Cohen-Lenstra heuristics*, Experimental Mathematics 12 (2003), no. 1, 99–113.

Department of Mathematics and Statistics, Concordia University, Montreal, Quebec, Canada
E-mail address: kisilev@mathstat.concordia.ca

Department of Mathematics, Technion-Israel Institute of Technology, Haifa 32000, Israel
E-mail address: neftind@tx.technion.ac.il

Department of Mathematics, Technion-Israel Institute of Technology, Haifa 32000, Israel
E-mail address: sonn@math.technion.ac.il