A note on unramified extensions of quadratic number fields

Kwang-Seob Kim and Joachim König

Abstract

We show the existence of quadratic number fields possessing an everywhere unramified Galois extension with Galois group $\widetilde{A}_n$, the double covering group of the alternating group, under the assumption of Bunyakovsky's conjecture.

1 Introduction

Unramified extensions of number fields (and, indeed, of function fields) and their Galois groups have been studied for a long time, due to their relevance in, e.g., class field theory and inverse Galois theory. In particular, a problem of interest is to realize prescribed finite groups as the Galois groups of unramified Galois extensions of low degree number fields. It is expected (although of course way out of reach to prove in general) that every finite group occurs as an unramified Galois group over infinitely many quadratic number fields. For certain solvable groups, this conjecture can be answered positively via class field theory (see, e.g., [23]); for nonsolvable groups, the most classical results concern the construction of quadratic fields having unramified extensions with alternating and symmetric groups (e.g., [20], [22], [3], [8], and [6]). Some further almost simple groups were realized in this sense in [12], making crucial use of specialization of function field extensions as well as Abhyankar's lemma (together with the fact that these groups are generated by involutions). Additional problems arise for non-solvable groups which are not almost-simple, notably central extensions of almost simple groups, whose treatment may require the combination of established techniques for the solvable and nonsolvable cases. A step in this direction was undertaken in [7], dealing with direct products of alternating and cyclic groups. A yet different direction was explored in [9] and [10], yielding the first realizations of certain perfect groups not generated by involutions as unramified Galois groups over infinitely many quadratic number fields. These included in particular the realization of infinitely many quadratic number fields having unramified Galois extensions with Galois group (the double covering group) $\widetilde{A}_n$ for $n = 5$ and $n = 7$.[1]

[0] 2020 Mathematics Subject Classification. Primary 12F05 ; Secondary 12F12 and 11R32.

[0] Key words and phrases: inverse Galois problem with restricted ramification, unramified extensions of number fields

[1] On a related note, see [18] for unramified realizations with Galois group $\widetilde{A}_4 \cong \mathrm{SL}_2(3)$.

In this note, we investigate these covering groups $\widetilde{A}_n$ in more generality. We will prove the following general result, which, albeit conditional, reduces the problem to a well-accepted number-theoretical conjecture.

Theorem 1.1. *Assume that the Bunyakovsky conjecture holds. Then for every $n \geq 4$, there exist infinitely many quadratic number fields possessing an everywhere unramified Galois extension with group $\widetilde{A}_n$, the unique double covering group of the alternating group A_n.*

The relevance of Bunyakovsky's conjecture, or indeed the more general Schinzel Hypothesis, for certain problems in inverse Galois theory is known. Our proof of Theorem 1.1 in Section 3.2 adapts previous arguments leading to a conditional proof of the so-called minimal ramification problem for the symmetric groups S_n. Before this, in Section 3.1 we review an approach using trinomials, which has also been successfully applied to many problems in inverse Galois theory, and which can be applied to deduce some, but not all, cases of Theorem 1.1.

2 Preliminaries

We begin by collecting some terminology and results crucial to the proof of Theorem 1.1.

2.1 Hilbert's irreducibility theorem

We will make use of several aspects of Hilbert's irreducibility theorem. All of these are well-known, but may be useful to recall here. The first is (a special case of) the irreducibility theorem as shown by Hilbert himself in [4].

Theorem 2.1. *Let $T_1, \dots, T_r$ and X be independent transcendentals ($r \geq 1$), and let $f(T_1, \dots, T_r, X) \in \mathbb{Q}[T_1, \dots, T_r, X]$ be an irreducible polynomial, nonconstant in X. Then there exist infinitely many values $(t_1, \dots, t_r) \in \mathbb{Q}^r$ such that $f(t_1, \dots, t_r, X) \in \mathbb{Q}[X]$ is irreducible. Moreover, given any arithmetic progressions $a_i + b_i\mathbb{Z}$ ($i = 1, \dots, r$), these infinitely many values $(t_1, \dots, t_r)$ may additionally be chosen such that $t_i \in a_i + b_i\mathbb{Z}$ for all $i = 1, \dots, r$.*

The following corollary on the preservation of Galois groups under specialization is also well-known, see, e.g., [17, Prop. 3.3.3].

Corollary 2.2. *Let $f(T, X) \in \mathbb{Q}[T, X]$ be an irreducible polynomial with Galois group G. Then there exist infinitely many $t \in \mathbb{Q}$ such that $f(t, X) \in \mathbb{Q}[X]$ has Galois group G. If furthermore the splitting field of $f(T, X)$ is a $\mathbb{Q}$-regular extension of $\mathbb{Q}(T)$ (i.e., it contains no nontrivial algebraic extension of $\mathbb{Q}$), then these infinitely many values t may additionally be chosen such that the splitting fields of the polynomials $f(t, X)$ are pairwise linearly disjoint over $\mathbb{Q}$.*

2.2 On Bunyakovsky's conjecture

The Bunyakovsky conjecture (see [2]) is a classical conjecture on prime values of polynomials, stating the following:

(BC) If $f \in \mathbb{Z}[X]$ is an irreducible polynomial and $D \in \mathbb{N}$ is the largest integer dividing all values $f(n)$ ($n \in \mathbb{Z}$), then there are infinitely many $n \in \mathbb{Z}$ for which $f(n)/D \in \mathbb{Z}$ is prime.[2]

Although it is supported by computational evidence and has been widely extended (e.g., into the Schinzel Hypothesis and the Bateman-Horn conjecture), it is not known for any non-linear f. On the other hand, it has many applications to number-theoretical problems.

In this paper, we will invoke the the Bunyakovsky conjecture in its "multivariate" form, i.e., use the following claim:

(MBC) For any $r \geq 1$ and any irreducible integer polynomial $f(X_1, \ldots, X_r)$ there exist infinitely many different primes of the form $f(x_1, \ldots, x_r)/D$, where $x_1, \ldots, x_r \in \mathbb{Z}$, and $D \in \mathbb{N}$ denotes the largest integer dividing all integer specializations $f(x_1, \ldots, x_r)$ ($x_i \in \mathbb{Z}$).

We note that this is in fact implied by the univariate form of the conjecture.

Lemma 2.3. *The "classical" Bunyakovsky conjecture (BC) and the multivariate Bunyakovsky conjecture (MBC) are equivalent.*

Proof. Trivially (MBC) implies (BC). To show the converse, let $f(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$ be irreducible and let $D \in \mathbb{Z}$ be the greatest common divisor of all integer specializations of f. It suffices to find polynomials $g_1(U), \ldots, g_r(U) \in \mathbb{Z}[U]$ such that $F(U) := f(g_1(U), \ldots, g_r(U)) \in \mathbb{Z}[U]$ is irreducible and the greatest common divisor of all its values is still D. We assume additionally that $f(0, \ldots, 0) =: N \neq 0$; this assumption can be made without loss of generality via a simple linear shift in the variables X_i. It is elementary (see, e.g., [16, Theorem 5.6]) that there exist $a_1, \ldots, a_r \in \mathbb{Z}$ such that $\gcd(N, f(a_1, \ldots, a_r)) = D$, and thus automatically $\gcd(N, f(x_1, \ldots, x_r)) = D$ for all $x_1 \equiv a_i \bmod N$ ($i = 1, \ldots, r$). We now consider the auxiliary polynomial $f_U(X_1, \ldots, X_r, U) := f(X_1U, \ldots, X_rU) \in \mathbb{Z}[X_1, \ldots, X_r, U]$. We claim that f_U is irreducible. Firstly, f_U is certainly irreducible when viewed as a polynomial in $X_1, \ldots, X_r$ over $\mathbb{Q}(U)$, since f is irreducible and $X_i \mapsto X_iU$ is an invertible transformation over $\mathbb{Q}(U)$. Furthermore, f_U is primitive as a polynomial over the ring $\mathbb{Z}[U]$. Indeed, all its coefficients equal the coefficients of f (which is irreducible over $\mathbb{Z}$, hence primitive) up to powers of U, whence the gcd of all coefficients of f_U must be a power of U; on the other hand the constant coefficient $f_U(0, \ldots, 0) = f(0, \ldots, 0)$ is a non-zero constant, whence the gcd of all coefficients must be 1. Since $\mathbb{Z}[U]$ is a UFD with field of fractions $\mathbb{Q}(U)$, the above observations imply that f_U is irreducible in $\mathbb{Z}[U][X_1, \ldots, X_r] = \mathbb{Z}[X_1, \ldots, X_r, U]$. Hilbert's irreducibility theorem (Theorem 2.1) now implies the existence of infinitely many $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ such that $x_i \equiv a_i \bmod N$ for all $i = 1, \ldots, r$, and $F(U) := f(x_1U, \ldots, x_rU)$ is irreducible. This also automatically yields $\gcd(F(0), F(1)) = \gcd(f(0, \ldots, 0), f(x_1, \ldots, x_r)) = D$, i.e., the greatest common divisor of all values of F is still D. This completes the proof. □

[2]Here, we count negatives of prime numbers as prime. Note that, strangely enough, many modern sources explicitly demand the extra assumption $D = 1$. This is, however, not in the spirit of Bunyakovsky's original paper, which is in fact dedicated primarily to the investigation of such "fixed divisors" D.

2.3 Stem extensions of alternating and symmetric groups

In this section, we recall some basic facts around stem extensions of the symmetric and alternating groups. See [21, Chapter 2.7] for more details. Recall that a *stem extension* of a group G is an extension

$$1 \to H \to G_0 \to G \to 1, \tag{2.1}$$

where $H \subset Z(G_0) \cap G_0'$ is a subgroup of the intersection of the center of G_0 and the derived subgroup of G_0. If the group G is finite, then there is a largest size for such a group G_0, and for every G_0 of that size the subgroup H is isomorphic to one and the same group, called the *Schur multiplier of* G. Moreover, if the finite group G is a perfect group, then G_0 is unique up to isomorphism and is itself perfect. Such G_0 are often called *universal perfect central extensions* of G, or *covering groups*. The following summarizes some important properties of stem covers of A_n and S_n.

Lemma 2.4. *a) The Schur multiplier of A_n is C_2 for $n = 4, 5$ or $n > 7$ and it is C_6 for $n = 6$ or 7. In particular, for all $n \geq 5$,[3] there is a unique degree-2 stem cover of A_n, denoted by $\widetilde{A}_n$.*

b) For all $n \geq 4$, the Schur multiplier of S_n is C_2. Furthermore, there are two degree-2 stem covers of S_n: in the first one, denoted by $\widetilde{S}_n$, the transpositions of S_n lift to elements of order 2, whereas in the second one, denoted by $\widehat{S}_n$, they lift to elements of order 4. Both these stem covers contain $\widetilde{A}_n$ as a subgroup of index 2.

2.4 Embedding problems

The proof of the main theorem requires the solution of certain central embedding problems (with kernel of order 2). We recall some basic terminology and key results around these.

A *finite embedding problem* over a field K is a pair $(\varphi : G_K \to G, \varepsilon : \tilde{G} \to G)$, where φ is a (continuous) epimorphism from the absolute Galois group G_K of K onto G, and ε is an epimorphism between finite groups $\tilde{G}$ and G fitting in an exact sequence $1 \to N \to \tilde{G} \to G \to 1$. The kernel $N = \ker(\varepsilon)$ is called the kernel of the embedding problem. An embedding problem is called *central* if $\ker(\varepsilon) \leq Z(\tilde{G})$. A (continuous) homomorphism $\psi : G_K \to \tilde{G}$ is called a *solution* to (φ, ε) if the composition $\varepsilon \circ \psi$ equals φ. In this case, the fixed field of $\ker(\psi)$ is called a *solution field* to the embedding problem. A solution ψ is called a *proper solution* if it is surjective. In this case, the field extension of the solution field over K has full Galois group $\tilde{G}$.

If K is a number field and $\mathfrak{p}$ is a prime of K, every embedding problem (φ, ε) induces an associated *local embedding problem* $(\varphi_\mathfrak{p}, \varepsilon_\mathfrak{p})$ defined as follows: $\varphi_\mathfrak{p}$ is the restriction of φ to $G_{K_\mathfrak{p}}$ (well defined up to fixing an embedding of $\overline{K}$ into $\overline{K_\mathfrak{p}}$), and $\varepsilon_\mathfrak{p}$ is the restriction of ε to $\varepsilon^{-1}(G(\mathfrak{p}))$, where $G(\mathfrak{p}) := \varphi_\mathfrak{p}(G_{K_\mathfrak{p}})$.

Proposition 2.5 ([14], Chapter IV, Cor. 10.2)**.** *Let $\Gamma = C.G$ be a central extension of G by a cyclic group C of prime order and $\varepsilon : \Gamma \to G$ the canonical projection. Let $\varphi : G_\mathbb{Q} \to G$ be a continuous epimorphism. Then the following hold:*

[3] In fact, this uniqueness property holds for $n = 4$ as well, even though A_4 is not perfect.

a) The embedding problem (φ, ε) is solvable if and only if all associated local embedding problems $(\varphi_p, \varepsilon_p)$ are solvable, where p runs through all primes of $\mathbb{Q}$ (including the infinite one).

b) If additionally $|C| = 2$, the equivalence of a) holds already when the set of all primes is replaced by "the set of all primes, with one exception" (hence, e.g., with the set of all finite primes).

Proposition 2.6 ([17], Prop. 2.1.7)**.** *Let $\Gamma = C.G$ be a central extension of G by a finite abelian group C, let $\varepsilon : \Gamma \to G$ be the canonical projection, and let $\varphi : G_{\mathbb{Q}} \to G$ be a continuous epimorphism such that the embedding problem (φ, ε) has a solution. For each finite prime p, let $\tilde{\varphi}_p : G_{\mathbb{Q}_p} \to \Gamma$ be a solution of the associated local embedding problem (φ_p, ϵ_p), chosen such that all but finitely many $\tilde{\varphi}_p$ are unramified. Then there exists a (not necessarily proper) solution $\tilde{\varphi} : G_{\mathbb{Q}} \to \Gamma$ of (φ, ϵ) such that for all finite primes p, the restrictions of $\tilde{\varphi}$ and $\tilde{\varphi}_p$ to the inertia group inside $G_{\mathbb{Q}_p}$ coincide. In particular, $\tilde{\varphi}$ is ramified exactly at those finite primes p for which $\tilde{\varphi}_p$ is ramified.*

Remark 2.7. *Note also that the local embedding problem $(\varphi_p, \varepsilon_p)$ as in Propositions 2.5 and 2.6 is always solvable in the case where φ_p is unramified (simply lift the image of Frobenius at p in G to any cyclic preimage in Γ).*

3 Proof of Theorem 1.1

We now proceed to the proof of Theorem 1.1. There are several ways to construct A_n-unramified extensions over quadratic fields. A well-known approach works with trinomials, i.e., polynomials of the form $X^n + aX^k + b$. We demonstrate this approach and its limitations for identifying $\widetilde{A}_n$-unramified extensions of quadratic number fields in Section 3.1, thereby motivating the necessity of the more general approach of the following Section 3.2. Both approaches construct suitable $\widetilde{S}_n$-extensions[4] of $\mathbb{Q}$, making use of the following observation.

Lemma 3.1. *Let $K \supset \mathbb{Q}$ be the splitting field of an irreducible degree-n polynomial, and assume that the following hold:*

i) $K/\mathbb{Q}$ is ramified only at one finite prime $p \geq 3$ and at the infinite prime, and

ii) the inertia groups at p and at ∞ are generated by a transposition and by an involution with $4j + 1$ transpositions ($j \geq 0$), respectively.

Then $K/\mathbb{Q}$ is an S_n-extension and embeds into an $\widetilde{S}_n$-extension $L/\mathbb{Q}$ such that L/F is an $\widetilde{A}_n$-unramified extension, where $F \subset K$ denotes the fixed field of A_n.

Proof. First, note that $\mathrm{Gal}(K/\mathbb{Q}) = S_n$, since the Galois group of a Galois extension of $\mathbb{Q}$ is generated by the set of all inertia subgroups at finite ramified primes, and furthermore it is well known that a transitive permutation group $G \leq S_n$ generated by transpositions is necessarily S_n itself, see e.g. [17, Lemma 4.4.4]. Now consider the embedding problem induced by $\widetilde{S}_n \to \mathrm{Gal}(K/\mathbb{Q}) \cong S_n$.

[4]Recall that $\widetilde{S}_n$ denotes the unique degree-2 stem cover of S_n in which the tranpositions of S_n split.

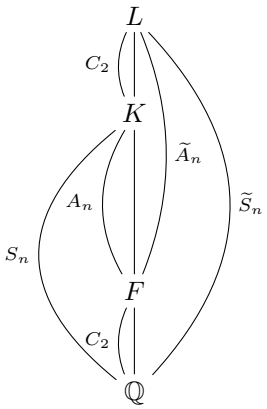

Figure 1: Diagram of fields and Galois groups in Lemma 3.1

The induced local embedding problems are automatically solvable at all unramified primes by Remark 2.7. Also, due to Condition ii), the local embedding problem at infinity is solvable since the decomposition group at ∞ in $K/\mathbb{Q}$ is generated by an involution with $4j+1$ transpositions, and such an element is necessarily split in $\widetilde{S}_n$, cf., e.g., [5]. Thus, from Condition i), the local embedding problem is solvable at all primes except possibly at p, and hence the global embedding problem is solvable due to Proposition 2.5b). The solutions are automatically proper, since the extension $\widetilde{S}_n \to S_n$ is non-split. Next, apply Proposition 2.6 to conclude that such solution fields $L \supset K \supset \mathbb{Q}$ may be chosen without any newly ramified finite primes (compared to $K/\mathbb{Q}$), and even without further ramification at the prime p (since the inertia group at p is generated by a transposition, hence split in $\widetilde{S}_n$, i.e., doesn't have any cyclic preimage of order larger than 2). In total, all inertia groups in $L/\mathbb{Q}$ are generated by involutions outside of the index 2 normal subgroup $\widetilde{A}_n$ of $\widetilde{S}_n$. This implies that, if $F \supset \mathbb{Q}$ denotes the quadratic number field fixed by $\widetilde{A}_n$, then L/F is an everywhere unramified $\widetilde{A}_n$-extension. □

3.1 A partial proof using trinomial extensions

Theorem 3.2. *Assume Bunyakovsky's conjecture. Then, for each $n \geq 4$ with $n \equiv 2, 3, 4$ or 5 mod 8, there exists a trinomial $f = X^n + aX + b \in \mathbb{Q}[X]$ whose splitting field embeds into a $\widetilde{S}_n$-extension $K/\mathbb{Q}$, such that $K/\mathbb{Q}(\sqrt{D(f)})$ is a $\widetilde{A}_n$-unramified extension where $D(f)$ is the discriminant of f.*

Proof. It suffices to show the existence of infinitely many different Galois extensions $K/\mathbb{Q}$ which are splitting fields of trinomials $f(X) = X^n + aX + b$ ($a, b \in \mathbb{Z}$) and fulfill the assumptions of Lemma 3.1. For this, note that, as a special case of [19, Theorem 2], the discriminant of f equals $\Delta(a,b) = (-1)^{(n-1)(n-2)/2}((n-1)^{n-1}a^n - (-n)^n b^{n-1})$. In particular, $\Delta(a,b)$ is irreducible as a bivariate integer polynomial and without any fixed divisor $D > 1$ (since, e.g., it takes the coprime values $\Delta(1,0) = \pm(n-1)^{n-1}$ and $\Delta(0,1) = \pm n^n$). Furthermore, one of the two variables a and b occurs of odd degree. It then follows from Bunyakovsky's conjecture that Δ takes infinitely many different values of

the form $\Delta(a,b) = -p$, for some prime number p.[5] Choose now such values $a, b \in \mathbb{Z}$. The inertia groups at primes extending p in $K/\mathbb{Q}$ are then generated by a transposition, since p strictly divides the discriminant. Furthermore, due to $\Delta(a,b) < 0$, the inertia group at ∞ is generated by an odd involution; on the other hand, since f is a trinomial, it has at most three real roots. Thus complex conjugation acts as an involution $\sigma \in S_n$ with at most three fixed points. The latter leaves, for each n, only two possible cycle types, namely consisting of either $\lfloor \frac{n}{2} \rfloor$ or $\lfloor \frac{n}{2} \rfloor - 1$ transpositions. Use now that $n \equiv 2, 3, 4$ or $5 \bmod 8$ to see immediately that an odd involution of this form must consist of $4j+1$ transpositions ($j \geq 0$). We have thus verified conditions i) and ii) of Lemma 3.1. This completes the proof. □

Remark 3.3. *In analogy with the above proof, one verifies that for $n \equiv 0, 1, 6$ or $7 \bmod 8$ and for any trinomial $X^n + aX^k + b$ with Galois group S_n, the only candidates for a complex conjugation $\sigma \in S_n$ which are compatible with our problem (namely, which are odd involutions and fix at most three points) have $4j-1$ transpositions. Since these are nonsplit in $\widetilde{S}_n$, in order to make the trinomial approach work for these residues, one would then have to use instead the second stem cover $\widehat{S}_n$ of S_n (in which the involutions with $4j-1$ transpositions split). In this group, however, the transpositions are non-split, and hence prime (or indeed squarefree) discriminants as obtained in the above argument are of no use since a prime with transposition inertia in the S_n-extension would then necessarily ramify further in the $\widehat{S}_n$-extension. This demonstrates the necessity of an argument beyond the trinomial approach for a full proof of Theorem 1.1.*

3.2 The general proof

We now present a construction which works for general $n \in \mathbb{N}$. As before, it suffices to justify the existence of infinitely many extensions $K/\mathbb{Q}$ fulfilling Conditions i) and ii) of Lemma 3.1. The following lemma is more than we need for our purposes, but may be useful in other contexts as well.

Lemma 3.4. *Let $n \in \mathbb{N}$, and let $n_1, \ldots, n_r$ and $m_1, \ldots, m_s$ be positive integers such that $\sum_{i=1}^r n_i = \sum_{j=1}^s m_j = n$. For each $i = 1, \ldots, r$ (resp. $j = 1, \ldots, s$), let $f_i(X)$ (resp. $g_j(X)$) be a "generic" monic polynomial of degree n_i (resp., m_j) over $\mathbb{Q}$, i.e., its coefficients are independent transcendentals over $\mathbb{Q}$. Denote the vector of all coefficients of all f_i by $\underline{a}$, and the vector of coefficients of the g_j by $\underline{b}$; set $f(X) = \prod_{i=1}^r f_i(X)$, $g(X) = \prod_{j=1}^s g_j(X)$, and choose another independent transcendental t. Then the discriminant $D \in \mathbb{Z}[\underline{a}, \underline{b}, t]$ of $f(X) - tg(X)$ is irreducible in $\mathbb{Q}(\underline{a}, \underline{b})[t]$.*

Proof. Let $F(X)$ and $G(X)$ be generic monic degree-n polynomials (with mutually independent coefficient vectors $\underline{\alpha}, \underline{\beta}$). Then the discriminant Δ of $F(X) - tG(X)$ is irreducible in $\mathbb{Q}[\underline{\alpha}, \underline{\beta}, t]$, e.g., as a special case of [11, Lemma 4.3]. By Hilbert's irreducibility theorem, there exist infinitely many rational specialization vectors $\underline{\alpha} \to \underline{\alpha}_0$, $\underline{\beta} \to \underline{\beta}_0$ which preserve the irreducibility of Δ (while also

[5] To see that the minus sign can be achieved, one may, e.g., consider $\Delta(a, (-1)^{\frac{n}{2}-1}b^2)$ (for $n \equiv 2, 4 \bmod 8$) and $\Delta((-1)^{\frac{n+1}{2}}a^2, b)$ (for $n \equiv 3, 5 \bmod 8$), which are still irreducible without fixed divisor > 1, and are now even degree polynomials with negative leading coefficient in one of the variables. Now it is easy, via specializing first the other variable, to reduce to the case of a one-variable irreducible polynomial taking only finitely many positive values in total.

preserving its degree). Denote the specialized polynomials by $F_0, G_0 \in \mathbb{Q}[X]$, and $\Delta_0 \in \mathbb{Q}[t]$, and let $\Omega \supset \mathbb{Q}(t)$, resp. $L \supset \mathbb{Q}$, be the splitting field of $F_0 - tG_0$, resp. of Δ_0. Since Δ_0 is irreducible and hence in particular separable, all non-trivial inertia groups of $\Omega\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(t)$ are generated by transpositions. Consequently, $\mathrm{Gal}(\Omega\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(t))$ is generated by transpositions, hence isomorphic to S_n. Since this group is on the other hand a subgroup of $\mathrm{Gal}(\Omega/\mathbb{Q}(t))$, it follows that $\Omega/\mathbb{Q}(t)$ is a $\mathbb{Q}$-regular[6] S_n-extension. Corollary 2.2 then implies that there are two (in fact, infinitely many) values $t_0, t_1 \in \mathbb{Q} \cup \{\infty\}$[7] such that the splitting fields of $F(X) - t_i G(X)$ have Galois group S_n ($i = 0, 1$) and their compositum is linearly disjoint from L over $\mathbb{Q}$. By applying a suitable fractional $\mathbb{Q}$-linear transformation $\mu := \mu(t)$, we may thus assume that $t_0 = 0$ and $t_1 = \infty$ are such values, i.e., the splitting fields of F_0 and G_0 themselves are linearly disjoint from L. Importantly, μ does not change L (the splitting field of Δ_0), since it merely induces a fractional linear change on the multiple values of the rational function $t(X) := \frac{F_0(X)}{G_0(X)}$, i.e., on the roots of the discriminant Δ_0, thus leaving the splitting field of Δ_0 invariant.

Denote the splitting field of F_0 by Ω_1 and the one of G_0 by Ω_2. We thus have that L is linearly disjoint over $\mathbb{Q}$ from $\Omega_1\Omega_2$. In particular, Δ_0 is irreducible over $\Omega_1\Omega_2$. Let $E_1 \subset \Omega_1$ be the fixed field of the (intransitive) subgroup $S_{n_1} \times \cdots \times S_{n_r} \leq S_n$, and $E_2 \subset \Omega_2$ the fixed field of $S_{m_1} \times \cdots \times S_{m_s} \leq S_n$. By definition, F_0 factors over E_1 into irreducible factors of degrees $n_1, \ldots, n_r$ (i.e., the factorization pattern of our polynomial $f(X)$ from the assertion), and G_0 factors over E_2 into irreducible factors of degrees $m_1, \ldots, m_s$ (i.e., the factorization pattern of $g(X)$). This means that, for the polynomial $f(X) - tg(X) \in \mathbb{Q}(\underline{a}, \underline{b})[t, X]$ from the assertion, we have found specialization vectors $\underline{a} \mapsto \underline{a}_0$ and $\underline{b} \mapsto \underline{b}_0$ with entries in $\Omega_1\Omega_2$, at which the discriminant D specializes to an irreducible polynomial in $(\Omega_1\Omega_2)[t]$ (of non-decreasing degree). This can only happen if D itself was irreducible in $(\Omega_1\Omega_2)(\underline{a}, \underline{b})[t]$, and hence a fortiori in $\mathbb{Q}(\underline{a}, \underline{b})[t]$. □

We are now ready to complete the proof of Theorem 1.1.

Proof of Theorem 1.1. We apply Lemma 3.4 with $(n_1, \ldots, n_r) = (1, \ldots, 1)$ and $(m_1, \ldots, m_s) = (2, \ldots, 2, 1, \ldots, 1)$, where, in view of Lemma 3.1, we demand the number of 2's to be congruent to 1 modulo 4. By Hilbert's irreducibility theorem, there exist infinitely many specializations of the coefficient vectors $\underline{a}$ and $\underline{b}$ maintaining the irreducibility (in $\mathbb{Q}[X]$) of the discriminant Δ_0 of the thus specialized polynomial $f_0(X) - tg_0(X)$. Moreover, we may additionally demand each quadratic factor of g_0 to remain irreducible over $\mathbb{R}$; indeed, this additional condition merely amounts to saying that the discriminant of each quadratic factor $X^2 + b_i X + b_{i+1}$ should be negative, i.e., b_{i+1} should be chosen sufficiently large compared to b_i, something obviously compatible with Hilbert's irreducibility theorem.

Now let E be the splitting field of $f_0 - tg_0$ over $\mathbb{Q}(t)$, and let $\mathcal{S}$ be the set of primes dividing all integer values of Δ_0. Since f_0 is totally split over $\mathbb{Q}$, for any $p \in \mathcal{S}$ and any p-adically sufficiently small value $t_0 \in \mathbb{Q}$, the polynomial $f_0(X) - t_0 g_0(X)$ is totally split over $\mathbb{Q}_p$ by Krasner's lemma. In particular, p is then unramified in the splitting field of $f_0 - t_0 g_0$. We wish to restrict to integer specializations at such p-adically small values (for all $p \in \mathcal{S}$ simultaneously)

[6] I.e., $\Omega \cap \overline{\mathbb{Q}} = \mathbb{Q}$.

[7] Here, for convenience, we define the specialization of $F_0(X) - tG_0(X)$ at $t = \infty$ as $G_0(X)$.

from now on, which may be achieved by considering all integer specialization values of $f_0 - Nt \cdot g_0(X)$ for a suitable non-zero integer N (namely, a product of suitable high powers of the primes in $\mathcal{S}$). Note also that, if t_0 is of sufficiently large absolute value, then its factorization pattern over the reals equals the one at $t = \infty$, i.e., the one of g_0, which by assumption splits into $4j + 1$ quadratic irreducible factors and linear factors otherwise over $\mathbb{R}$. In particular, complex conjugation in the splitting field is an involution with $4j + 1$ transpositions. Assuming Bunyakovsky's conjecture, there are infinitely many integers t_0 for which $\Delta_0(Nt_0)$ is of the form qD, where q is a prime and D is divisible only by primes in $\mathcal{S}$ (we have used here that replacing t by Nt does not lead to any new fixed prime divisors $p \notin \mathcal{S}$, which is evident upon mod-p reduction, since $\gcd(p, N) = 1$). This means that the discriminant of the splitting field of $f_0(X) - Nt_0 g_0(X)$ is also a prime up to at most such a factor D. But also, by choice of N, we already know that the primes in $\mathcal{S}$ are unramified in the latter splitting field. Therefore, there is only one ramified finite prime, and its inertia group is generated by a transposition. Furthermore, for $|Nt_0|$ sufficiently large, the inertia group at the infinite prime generated by an involution with $4j + 1$ transpositions, as already explained. This yields infinitely many S_n-extensions of $\mathbb{Q}$ fulfilling the assumptions of Lemma 3.1, thus completing the proof. □

Remark 3.5. *An approach somewhat similar to the one taken above has been carried out in the proof of [1, Theorem 6.5] (improving over the earlier [15, Remark 3.10]), namely to show that (conditionally on Schinzel's Hypothesis - and, in fact, ultimately only on Bunyakovsky's conjecture) there exist S_n-extensions of $\mathbb{Q}$ ramified at only one (necessarily finite) prime. For this purpose, the authors necessarily require totally real S_n-extensions, whereas we deliberately avoid this special scenario, since Proposition 2.6 would then not be sufficient to exclude the solution field of the embedding problem acquiring new ramification over infinity.*

4 Some explicit examples

While unconditional results on the existence of infinitely many quadratic number fields as in the assertion of Theorem 1.1 may be hard (for arbitrary n), simple database checks (e.g., `lmfdb.org`, [13]) yield *some* fields of this form (for small n). In Table 1, we list, for small values of n, the "smallest" database hit (when counting by discriminant norm) of a quadratic number field F embedding into an S_n-extension $K/\mathbb{Q}$ which fulfills the assumptions of Lemma 3.1, and thus in particular possessing an unramified $\widetilde{A}_n$-extension.

Acknowledgments. The first-named author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2021R1F1A1054926). The second-named author was supported by the National Research Foundation of Korea (NRF Basic Research Grant RS-2023-00239917).

n	F
4	$\mathbb{Q}(\sqrt{-283})$
5	$\mathbb{Q}(\sqrt{-4903})$
6	$\mathbb{Q}(\sqrt{-92779})$
7	$\mathbb{Q}(\sqrt{-3444743})$
8	$\mathbb{Q}(\sqrt{-69367411})$
9	$\mathbb{Q}(\sqrt{-2307632671})$
10	$\mathbb{Q}(\sqrt{-215067767})$
11	$\mathbb{Q}(\sqrt{-5901091967})$

Table 1: Some quadratic fields with unramified $\widetilde{A}_n$-extension

References

[1] L. Bary-Soroker, A. Entin, A. Fehm, *The minimal ramification problem for rational function fields over finite fields.* Int. Math. Res. Not. Vol 2023 (21) (2023), 18199–18253.

[2] V. Bouniakowsky, *Sur les diviseurs numériques invariables des fonctions rationelles entières.* Mém. Acad. Sc. St. Pétersbourg, 6^e série, vol VI (1857), 305–329.

[3] J. Elstrodt, F. Grunewald, and J. Mennicke: *On unramified A_m-extensions of quadratic number fields,* Glasgow Math. J. **27** (1985), 31–37

[4] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.* J. Reine Angew. Math. 110 (1892), 104–129.

[5] P.N. Hoffman, J.F. Humphreys, *Projective representations of the symmetric groups.* Oxford Mathematical Monographs, 1992.

[6] K.S. Kedlaya, *A construction of polynomials with squarefree discriminants.* Proc. Amer. Math. Soc. 140 (2012), no. **9**, 3025–3033.

[7] K.-S. Kim, J. König, *On $A_n \times C_m$ unramified extensions over imaginary quadratic number fields.* To appear in Glasgow Math. J.

[8] T. Kondo, *Algebraic number fields with the discriminant equal to that of a quadratic number field.* J. Math. Soc. Japan **47** (1995), no. **1**, 31–36.

[9] J. König, *Unramified extensions of quadratic number fields with certain perfect Galois groups.* Int. J. Number Theory **19**(3) (2023). 639–653.

[10] J. König, *Quadratic number fields with unramified $SL_2(5)$-extensions.* J. Algebra **628** (2023), 634–649.

[11] J. König, F. Legrand, *Density results for specializations of Galois covers.* J. Inst. Math. Jussieu **20**(5) (2021), 1455–1496.

[12] J. König, D. Neftin, J. Sonn, *Unramified extensions over low degree number fields.* J. Number Theory **212** (2020), 72–87.

[13] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2023 [Online; accessed 28 July 2023].

[14] G. Malle, B.H. Matzat, *Inverse Galois Theory*. 2nd edition, Springer, 2018.

[15] B. Plans, *On the minimal number of ramified primes in some solvable extensions of* $\mathbb{Q}$. Pacific J. Math. 215(2) (2004), 381–391.

[16] K. Rajkumar, A.S. Reddy, D. Prasad Semwal, *Fixed divisor of a multivariate polynomial and generalized factorials in several variables.* J. Korean Math. Soc. 55 (6) (2018), 1305–1320.

[17] J.-P. Serre, *Topics In Galois Theory*. Research Notes in Math., vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992.

[18] J-P. Serre, *Modular forms of weight one and Galois representations,* Algebraic number fields: L-functions and Galois properties (A. Fröhlich, ed.), Academic Press, London, (1977), 193–268.

[19] R.G. Swan, Factorization of polynomials over finite fields. Pacific J. Math. **12** (1962), 1099–1106.

[20] K. Uchida, *Unramified extensions of quadratic number fields, II*, Tôhoku Math. J. **22** (1970), 220–224.

[21] R.A. Wilson, *The finite simple groups.* Graduate Texts in Mathematics, **251**. Springer-Verlag London, Ltd., London, 2009.

[22] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

[23] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors.* J. Théor. Nombres Bordeaux 9 (1997), no. **2**, 405–448.

Kwang-Seob Kim
Department of Mathematics,
Chosun University,
Gwangju 61452, South Korea
E-mail: kwang12@chosun.ac.kr

Joachim König
Department of Mathematics Education,
Korea National University of Education,
28173 Cheongju, South Korea,
E-mail: jkoenig@knue.ac.kr