COMPUTATION OF STARK-TAMAGAWA UNITS

W. BLEY

ABSTRACT. Let \( K \) be a totally real number field and let \( l \) denote an odd prime number. We design an algorithm which computes strong numerical evidence for the validity of the “Equivariant Tamagawa Number Conjecture” for the \( \mathbb{Q}[G] \)-equivariant motive \( h^0(\text{Spec}(L)) \), where \( L/K \) is a cyclic extension of degree \( l \) and group \( G \). This conjecture is a very deep refinement of the classical analytic class number formula. In the course of the algorithm, we compute a set of special units which must be considered as a generalization of the (conjecturally existing) Stark units associated to first order vanishing Dirichlet \( L \)-functions.

1. Introduction

Let \( L/K \) denote a finite Galois extension of number fields of group \( G \). In this paper we provide numerical evidence for the so-called “Equivariant Tamagawa Number Conjecture” for the \( \mathbb{Q}[G] \)-equivariant motive \( h^0(\text{Spec}(L)) \) formulated in [3] and [6]. Our approach is based on the results of [2], where for a large class of abelian extensions \( L/K \) the conjectural vanishing of the Tamagawa number \( T\Omega(L/K) \) of \( h^0(\text{Spec}(L)) \) is interpreted in terms of the existence of \( S \)-units satisfying a variety of explicit conditions.

These conditions are in the same spirit as the conditions studied by Rubin in [16] and Popescu in [14], but are in general much finer. Indeed, recent work of Burns [5] shows that in the context of this paper the “Equivariant Tamagawa Number Conjecture” implies a certain natural refinement of the conjectures of Rubin and Popescu. In turn, their conjectures are generalizations of the well-known refined Stark conjecture “over \( \mathbb{Z} \)” for first order vanishing Dirichlet \( L \)-functions (cf. [18, Chap. IV]). Therefore our examples also provide new evidence in favour of these Stark-type conjectures.

The article is organized in the following way: in Section 2 we recall the main result of [2]. In Section 3 we describe an algorithm which verifies the above mentioned conjecture (up to the precision of the computation) for cyclic extensions \( L \) of odd prime degree of a totally real number field \( K \), and Section 4 contains a worked-out example.

2. The equivariant Tamagawa number conjecture

We fix a Galois extension \( L/K \) of number fields and set \( G = \text{Gal}(L/K) \). Let \( K_0(\mathbb{Z}[G], \mathbb{R}) \) denote the Grothendieck group of the fibre category of the functor...

Received by the editor November 7, 2001 and, in revised form, April 26, 2002.
2000 Mathematics Subject Classification. Primary 11R27, 11R29, 11R42.
The author was supported in part by a DFG Grant.
In [4] Burns used complexes arising from étale cohomology to define a canonical element $T\Omega(L/K) \in K_0(\mathbb{Z}[G], \mathbb{R})$. For a precise definition in the general case the reader is referred to loc.cit.; an easier accessible version in the abelian case is contained in [1]. In [3] it is shown that the Stark conjecture [18, Ch.1, 5.1] is equivalent to asserting $T\Omega(L/K) \in K_0(\mathbb{Z}[G], \mathbb{Q})$, the Strong Stark conjecture [8, Conj. 2.2] is equivalent to the containment $T\Omega(L/K) \in K_0(\mathbb{Z}[G], \mathbb{Q})_{tor}$, and finally, the “equivariant Tamagawa number conjecture” (for short, ETNC) of [4] for the special motive $h^0(\text{Spec}(L))$ is equivalent to the equality $T\Omega(L/K) = 0$.

Very recently, Burns and Greither [2] have proven ETNC for all abelian extensions $L/\mathbb{Q}$ of odd conductor, but beyond this, very little concerning ETNC is known so far.

From now on we assume that $G$ is abelian and fix the following notation. For any finite set $S$ of places of $K$ which contains the set $S_\infty$ of archimedian places, we write $S(L)$ for the set of places of $L$ lying above places in $S$, $\mathcal{O}_S$ for the $(S(L))$-integers of $L$, $d_S$ for the $S(L)$-class group, and we set $h_S := |d_S|$. We let $U_S$ denote the $S(L)$-units of $L$, $\mu_L$, the torsion subgroup of $U_S$, and we set $E_S := U_S/\mu_L$. Analogously we write $U_{K,S}$ and $E_{K,S}$ for the corresponding groups on the base field level. We let $Y_S$ denote the free abelian group on the set $S(L)$ and write $X_S$ for the kernel of the homomorphism $Y_S \to \mathbb{Z}$ which sends each element of $S(L)$ to 1. For later reference we recall that if $(h_S, |G|) = 1$, then there exists an exact sequence of finitely generated $G$-modules

$$0 \to U_S \to A \to B \to X_S \to 0$$

(1)

with $A, B$ of finite projective dimension. (This is shown in [17] under the assumption $h_S = 1$, but the same argument works with our slightly weaker hypothesis.)

For each place $w$ of $L$ we let $| \cdot |_w$ denote the absolute value of $w$, which is normalised as in [18, Chap. 0, 0.2]. We let $R_S : U_S \otimes_\mathbb{Z} \mathbb{R} \to X_S \otimes_\mathbb{Z} \mathbb{R}$ denote the $\mathbb{R}[G]$-equivariant isomorphism given by

$$R_S(u) = - \sum_{w \in S(L)} \log |u|_w \cdot w$$

for each $u \in U_S$.

We let $G^*$ denote the group of abelian characters of $G$. For each $\chi \in G^*$ we write $L_S(s, \chi)$ for the associated $S$-truncated Dirichlet $L$-function and $e_\chi$ for the primitive idempotent $|G|^{-1} \sum_{g \in G} \chi(g) g^{-1}$. In this way we obtain a $\mathbb{C}[G^*]$-valued function of the complex variable $s$ by setting

$$L_S(s) := \sum_{\chi \in G^*} L_S(s, \chi^{-1}) e_\chi.$$  

We let $L^*_S(0, \chi)$ denote the leading coefficient in the Taylor expansion of $L_S(s, \chi)$ at $s = 0$, and set $L^*_S(0) := \sum_{\chi \in G^*} L^*_S(0, \chi^{-1}) e_\chi$. Roughly speaking, ETNC predicts a conjectural formula for the $\mathbb{Z}[G]$-sublattice of $\mathbb{R}[G]$ which is generated by $L^*_S(0)$ (note that $L_S(s, \chi) = L_S(s, \chi^{-1})$ for $s \in \mathbb{R}$ implies $L^*_S(0) \in \mathbb{R}[G]$).

Let $E$ be the field generated over $\mathbb{Q}$ by the values of elements of $G^*$, and write $O$ for its ring of algebraic integers. For any commutative ring $R$ and each $R$-module
$M$ we write $\text{Fitt}_R(M)$ for the (first) Fitting ideal of $M$. (We refer the reader to [11, App.] or [13, Sec. 1.4] for the basic properties of Fitting ideals.) If $M$ is any finite $G$-module with $(|M|, |G|) = 1$, then each $e_\chi$ acts naturally on $\mathcal{O} \otimes \mathbb{Z} M$, and we set

$$\text{Fitt}_\chi(M) := \text{Fitt}_\mathcal{O}(e_\chi(\mathcal{O} \otimes \mathbb{Z} M)).$$

Note that $\text{Fitt}_\chi(M)$ coincides with the usual $\mathcal{O}$-order ideal of the finitely generated $\mathcal{O}$-torsion module $e_\chi(\mathcal{O} \otimes \mathbb{Z} M)$.

We now introduce a natural simplifying hypothesis on the extension $L/K$ under which ETNC can be interpreted as asserting the existence of special units in $L$. For each place $v$ of $K$ we write $G_v$ for the decomposition subgroup in $G$.

**Hypothesis (S).** There exists a finite set $S$ of places of $K$ which satisfies all of the following conditions: $S$ contains all archimedean places and all places which ramify in $L/K$; $(|G|, h_S) = 1$; there exists a place $v_0 \in S$ for which $G_{v_0} = G$; and for each place $v \in S_0 := S \setminus \{v_0\}$, the group $G_v$ is cyclic.

Assuming that $S$ is as described in Hypothesis (S), we fix a generator $g_v$ of $G_v$ for each $v \in S_0$. We let $w_0$ denote the (unique) place of $L$ lying above $v_0$, and for each $v \in S_0$ we choose a place $w_v$ of $L$ lying above $v$. For each $v \in S_0$, and each place $w \in S(L) \setminus \{w_0\}$, we define $\delta_{v,w}$ to be 1 if $w = w_v$ and to be 0 otherwise. If $w \in S(L)$, we write $v(w)$ for the unique place in $S$ defined by $w$. For each $\chi \in G^*$ we let $S_\chi$ denote the set \{ $\chi(g_v) = 1$\}, and we define $S_{\chi}^\times := S_0 \setminus S_\chi$.

If $N/M$ is a finite abelian extension of $p$-adic fields, we write $(-, N/M)$ for the associated Artin map $M^\times \rightarrow \text{Gal}(N/M)$. If $U$ is a subgroup of $\text{Gal}(N/M)$, then $N^U$ denotes the subfield of $N$ fixed by $U$.

The next two theorems are just reformulations of [2, Th. 3.2].

**Theorem 2.1.** Assume that $(|\mu_L|, |G|) = 1$ and in addition that $S$ is as described in Hypothesis (S). Then there exist elements $e_v \in U_{L,G_v,S}$ for each $v \in S_0$ such that

(i) the index of $E_S := (e_v : v \in S_0 |Z[G]|$ in $U_S$ is finite and coprime to $|G|$,

(ii) for each place $v \in S_0$ and each place $w$ of $S(L) \setminus \{w_0\}$ one has

$$(e_v, L_w/L_w^{G_v \cap G(w)}) = g_{v,w}^\delta_{v,w}.$$ 

**Proof.** This is immediate from [2, Prop. 2.1] and the first part of the proof of [2, Th. 3.2].

**Theorem 2.2.** Assume the notation of Theorem 2.1. Then $T\Omega(L/K) = 0$ if and only if for each $\chi \in G^*$ there exists an element $a_\chi$ of $E^*$ such that

(i) \( \prod_{v \in S_X} (\chi(g_v) - 1) \cdot \bigwedge_{v \in S_X} \frac{1}{|G_v|} R_S(e_\chi(e_v)) = a_\chi L^*_S(0, \chi^{-1}) \cdot \bigwedge_{v \in S_X} e_\chi(w_v - w_0), \)

(ii) $a_\chi \mathcal{O} = Fitt_\chi(U_S/E_S)Fitt_\chi(cl_S)^{-1}$, and

(iii) $h_S a \in \mathbb{Z}[G]$, where $a := \sum_{\chi \in G^*} a_\chi e_\chi$.

**Proof.** This is proved in the second part of the proof of [2, Th. 3.2].

**Remarks 2.3.** a) Equality (i) in Theorem 2.2 is an equality in the one-dimensional $\mathbb{C}$-vector space $\bigwedge_{v \in S_X} e_\chi(\mathcal{O} \otimes \mathbb{Z} X_S)$ and therefore uniquely determines complex numbers $a_\chi$ for each $\chi \in G^*$ equivalent to the assertion $a \in \mathbb{Q}[G]$. If we assume Stark’s conjecture, then equality (ii) holds
if and only if the Strong Stark conjecture is true. Finally, (ii) and (iii) together imply
\[ a\mathbb{Z}[G] = \text{Fitt}_\mathbb{Z}[G](U_S/E_S)\text{Fitt}_\mathbb{Z}[G](cl_S)^{-1}. \]
This statement in turn is equivalent to the equality \( T\Omega(L/K) = 0 \).

Very recently, Burns and Greither have proven ETNC for any abelian extension \( L/\mathbb{Q} \) of odd conductor. Furthermore, ETNC is known to be valid for a natural family of non-abelian extensions \( L/\mathbb{Q} \) for which \( G \) is isomorphic to the quaternion group of order 8 (cf. \[12\]). Apart from these extensions and their subextensions, we are not aware of any other abelian extensions \( L/K \) for which ETNC is known to be true. In fact, the extensions we will consider in the next section are not even known to validate Stark’s conjecture or the Strong Stark conjecture.

b) If we assume in addition to Hypothesis (S) that \( S \) contains precisely \( r \) places that split completely in \( L/K \), then the \((r-1)\)-st derivative \( L_S^{(r-1)}(0, \chi) \) equals 0 for all \( \chi \in G^* \) (cf. \[18\] Chap. I, Prop. 3.4]). Therefore \( L_S^{(r)}(0, \chi) \) is of particular interest, and Rubin in \[16\], and subsequently Popescu in \[17\], conjectured certain natural integrality properties for the \( r \)-th derivative \( L_S^{(r)}(0) \) of \( L_S(s) \). Their conjectures generalize the refined conjecture “over \( \mathbb{Z} \)” formulated by Stark in the case \( r = 1 \) (cf. \[18\] Chap. IV).

If \( \mu_L \) is cohomologically trivial, then Rubin’s and Popescu’s conjecture are equivalent as a consequence of \[14\] Th. 5.5.1. In addition, the main result of \[5\] Sec. 3.2 shows that under our hypothesis ETNC implies a strong refinement of Popescu’s conjecture (cf. \[5\] Rem. 3.3(iv)).

For a brief discussion about what is known about these Stark-type conjectures of Rubin and Popescu, we recommend the interested reader to consult \[14\] §6.

3. An algorithm

Let \( K \) denote a totally real number field of degree \( n \). We fix an odd prime number \( l \) and let \( L/K \) denote a cyclic extension of number fields of degree \( l \). Note that for each such extension there exists a set \( S \) such that the assumptions of Theorems 2.1 and 2.2 are satisfied. Our aim is to use these results to develop an algorithm to check the validity of ETNC for \( L/K \) up to the precision of the computation.

We assume that \( L/K \) is given by class field theoretic data as described in \[9\] Chap. 3 and 4. In particular, we let \( \mathfrak{f} = \mathfrak{f}_{L/K} \) denote the conductor of \( L/K \) and write \( c_l(K) \) for the ray class group modulo \( \mathfrak{f} \). Let \( \mathcal{H} \leq c_l(K) \) denote the subgroup of index \( l \) corresponding to the given extension \( L \). Then recently developed algorithms due to Cohen and Roblot (cf. \[9\] Chap. 6) allow us to compute the defining polynomials for \( L \). Based on this, we further assume that we are able to compute all basic invariants of \( L \), such as the ring of algebraic integers, the ideal class group and a system of fundamental units (and also the \( S \)-versions of these objects).

In the following we write \( S_\infty = \{\infty_1, \ldots, \infty_n\} \), \( S_{ram} = \{p_0, \ldots, p_r\} = \{p : p \mid \mathfrak{f}\} \) and choose a set \( S' = \{q_1, \ldots, q_s\} \) of primes which split completely in \( L/K \) and such that for \( S = S_\infty \cup S_{ram} \cup S' \) one has \( l \nmid h_S \). We will use \( p_0 \) as the distinguished place \( v_0 \) of Hypothesis (S). Then

\begin{equation}
X_S = \bigoplus_{i=1}^n \mathbb{Z}[G](\infty_i - \hat{p}_0) \oplus \bigoplus_{i=1}^s \mathbb{Z}[G](\hat{q}_i - \hat{p}_0) \oplus \bigoplus_{i=1}^r \mathbb{Z}(\hat{p}_i - \hat{p}_0),
\end{equation}
where for each place $p \in S$ we choose a place $\hat{p}$ of $L$ above $p$.

The $\mathbb{Z}$-rank of $U_S$ is then given by $m := l(n+s)+r$, and we let $\delta_1, \ldots, \delta_m$ denote a system of fundamental $S(L)$-units. Finally we assume that the representation of $G$ induced by its action on $E_S$ and this choice of fundamental units is explicitly known: for $g \in G$ we denote by $D(g)$ the corresponding matrices. Each element $u = \prod_{i=1}^m e_i^{s_i}$ of $E_S$ is then represented by the vector $x := (x_1, \ldots, x_m)^t$, and the action of $g \in G$ on $u$ is translated into the matrix multiplication $D(g)x$. We will perform all our computations in $U_{S,Q} := U_S \otimes \mathbb{Q}$ and thus represent each $u \in E_S$ by a vector $x \in \mathbb{Q}^m$.

We will simply view this data as input for our algorithm. Its actual computation is, of course, a very hard problem on its own. It is remarkable that the PARI system provides almost all routines to compute this input, at least for small degrees $l$ and small conductors.

Let $\zeta$ denote a primitive $l$-th root of unity and set $E = \mathbb{Q}(\zeta)$. We fix a generator $g_0$ of $G$ and define a character $\chi \in \hat{G}^*$ by $\chi(g_0) = \zeta$. Thus $G^* = \langle \chi \rangle$. We also write $\chi_0$ for the trivial character of $G$, $e_0 = \frac{1}{l} \sum_{g \in G} g$ and $e_1 = 1 - e_0$ for the primitive idempotents of $\mathbb{Q}[G]$, and note that the map $\lambda \mapsto (\chi_0(\lambda), \chi(\lambda))$, $\lambda \in \mathbb{Q}[G]$, defines a natural identification of $\mathbb{Q}[G]$ and $\mathbb{Q} \oplus E$. Without further mention we will henceforth identify $\mathbb{Q}[G]$ and $\mathbb{Q} \oplus E$. The lattice $e_1 E_S \subseteq U_{S,Q}$ is then naturally endowed with the structure of an $O$-module.

### 3.1. Computation of $E_S$.

In this subsection we explain how to compute a $\mathbb{Z}[G]$-sublattice $E_S$ of $U_S$ such that the assertions of Theorem 2.1 are satisfied. Concretely, we have to exhibit $S$-units $\epsilon_{\infty}, \ldots, \epsilon_{\infty}, \epsilon_q, \ldots, \epsilon_q$, $e_q, \ldots, e_q$, $e_q, \ldots, e_q$, $e_q, \ldots, e_q$, $e_q, \ldots, e_q$, $e_q, \ldots, e_q$, $e_q, \ldots, e_q$, $e_q, \ldots, e_q$ such that the assertions of Theorem 2.1 are satisfied.

#### Lemma 3.1.

Suppose that $A = \{\epsilon_1, \ldots, \epsilon_{n+s}\} \subseteq U_S$ satisfies $l \nmid [e_1 E_S : e_1 A]$. Then there exist $S$-units $\eta_1, \ldots, \eta_r \in U_{K,S} \subseteq \mathbb{Q}[G]$ such that $l \nmid [U_{K,S} : \langle \epsilon_0 A, \eta_1, \ldots, \eta_r \rangle \mathbb{Q}[G]]$. In addition, if one sets $E_S := \{\epsilon_1, \ldots, \epsilon_{n+s}, \eta_1, \ldots, \eta_r\} \mathbb{Q}[G]$, then $l \nmid [U_S : E_S]$.

**Proof.** For any finitely generated $\mathbb{Z}$-module $M$ we write $M_l := M \otimes \mathbb{Z}_l$ for its $l$-completion. By [2] Prop. 2.1 we know there exist $\omega_1, \ldots, \omega_{n+s} \in U_{K,S} \subseteq \mathbb{Q}[G]$ such that $U_{S,l} = \langle \omega_1, \ldots, \omega_{n+s}, \nu_1, \ldots, \nu_r \rangle \mathbb{Q}[G]$. This will be the key observation in the proof of Lemma 3.1.

The short exact sequence $0 \rightarrow E_{K,S} \rightarrow E_S \rightarrow e_1 E_S \rightarrow 0$ together with our assumption $l \nmid [e_1 E_S : e_1 A]$ implies

\[ U_{S,l} = \langle \epsilon_1, \ldots, \epsilon_{n+s}, \nu \rangle \mathbb{Q}[G] = \langle \omega_1, \ldots, \omega_{n+s}, U_{K,S} \rangle \mathbb{Q}[G]. \]

We let $O_l$ denote the localization of $O$ with respect to the unique prime of $E$ above $l$, and recall that the maximal $\mathbb{Z}_l$-order in $\mathbb{Q}_l[G]$ is isomorphic to $\mathbb{Z}_l \otimes O_l$. Via this identification one has $\mathbb{Q}_l[G] = \{ (a, \alpha) \in \mathbb{Z}_l \otimes O_l \mid a \equiv \alpha (\text{mod } (1 - \zeta)) \}$.

Let $A \in \text{Mat}_{n+s}(O_l)$ denote the matrix such that

\[ (e_1 \epsilon_1, \ldots, e_1 \epsilon_{n+s}) = (e_1 \omega_1, \ldots, e_1 \omega_{n+s}) A, \]

and choose a matrix $A_1 \in \text{Mat}_{n+s,n+s}(Z_l)$ such that $A \equiv A_1 (\text{mod } (1 - \zeta))$, where here and in the following congruences of matrices are meant componentwise. Then $A + A_1 \in \text{Mat}_{n+s,n+s}(Z_l[G])$, $\det(A_1) \in Z_l^\times$ and

\[ (e_0 \epsilon_1, \ldots, e_0 \epsilon_{n+s}) \equiv (e_0 \omega_1, \ldots, e_0 \omega_{n+s}) A_1 (\text{mod } U_{K,S,l}). \]
We write $H^i$ for the Tate cohomology groups and let $N_G$ denote the norm operator. From (1) and (2) we obtain $U_{K,S}/N_G U_S = H^0(G,U_S) = H^0(G,X_S) = \bigoplus_{i=1}^n \mathbb{Z}/\mathbb{Z}$. Since $rk_Z(U_{K,S}) = n + s + r$ we conclude that $e_0 \omega_1 \notin U_{K,S}$ for $i = 1, \ldots, n + s$, and $U_{K,S,l} = \langle le_0 \omega_1, \ldots, le_0 \omega_{n+s}, \nu_1, \ldots, \nu_r \rangle \mathbb{Z}_i$.

If we let $u_1, \ldots, u_{n+r+s}$ denote a system of fundamental units of $U_{K,S}$, then there exists an invertible matrix $B \in \text{GL}_{n+r+s}(\mathbb{Z}_i)$ such that

$$<(le_0 \omega_1, \ldots, le_0 \omega_{n+s}, \nu_1, \ldots, \nu_r) = (u_1, \ldots, u_{n+r+s})B>.$$ 

Writing $B = (B_1 \mid B_2)$ with $B_1 \in \text{Mat}_{n+r+s,n+s}(\mathbb{Z}_i), B_2 \in \text{Mat}_{n+r+s,r}(\mathbb{Z}_i)$, it follows that $B_1$ has an invertible $(n + s) \times (n + s)$ minor.

From (1) we deduce

$$e_0 \langle e_1, \ldots, e_{n+s} \rangle = \langle e_0 \omega_1, \ldots, e_0 \omega_{n+s} \rangle A_1 + \langle v_1, \ldots, v_{n+s} \rangle$$

with $v_1, \ldots, v_{n+s} \in U_{K,S,l}$, and furthermore

$$(le_0 e_1, \ldots, le_0 e_{n+s}) = (u_1, \ldots, u_{n+r+s}) B_1 A_1 + \langle v_1, \ldots, v_{n+s} \rangle$$

$$(u_1, \ldots, u_{n+r+s}) H$$

with a matrix $H \in \text{Mat}_{n+r+s,n+s}(\mathbb{Z}_i)$. Since $B_1 A_1 \equiv H \pmod{l}$ and $\det(A_1) \in \mathbb{Z}_i^\times$, the matrix $H$ also contains an invertible $(n+s) \times (n+s)$ minor. Therefore we can complement $le_0 e_1, \ldots, le_0 e_{n+s}$ with $\eta_1, \ldots, \eta_r$ to obtain a basis of $U_{K,S,l}$, and it is now obvious from (3) that $U_{S,l} = \langle e_1, \ldots, e_{n+s}, \eta_1, \ldots, \eta_r \rangle \mathbb{Z}_i$.

Given the result of Lemma 3.1, we achieve the computation of $E_S$ in three steps.

**Step 1: Computation of $A := \langle e_1, \ldots, e_{n+s} \rangle \mathbb{Z}[G] \subseteq U_S$ such that $l \nmid \langle e_1 E_S : e_1 A \rangle$.**

**Step 2: Computation of $\eta'_1, \ldots, \eta'_r \in U_{K,S}$ such that $l \nmid \langle E_{K,S} : \langle le_0 A, \eta'_1, \ldots, \eta'_r \rangle \mathbb{Z} \rangle$.**

**Step 3: Adaption of $\eta'_1, \ldots, \eta'_r$ such that part (ii) of Theorem 2.1 is satisfied.**

We begin with the description of Step 1. Recall that we always identify $e_1 \mathcal{O}[G]$ and $E_i$. Inductively we construct an $E$-basis $\xi_1, \ldots, \xi_{n+s}$ of $e_1 U_{S,Q}$: suppose that $\xi_1, \ldots, \xi_{i-1}$ are already computed. Then we choose $\delta \in \{\delta_1, \ldots, \delta_m\}$ such that $e_1 \delta \in e_1 U_{S,Q} \setminus \langle \xi_1, \ldots, \xi_{i-1} \rangle e_1 \mathcal{O}[G]$ (a condition which is easily checked by solving a system of linear equations) and set $\xi_i := e_1 \delta$.

Next we compute the $(n+s) \times m$ matrix $A$ with coefficients in $E$ such that

$$(e_1 \delta_1, \ldots, e_1 \delta_m) = (\xi_1, \ldots, \xi_{n+s}) A.$$

We will use the Hermite normal form algorithm in Dedekind domains (cf. [9 Th. 1.4.6 and Alg. 1.4.7]) and also stick to the notation of loc.cit. In this way we obtain a matrix $U \in \text{GL}_m(E)$ and nonzero fractional $\mathcal{O}$-ideals $e_1, \ldots, e_{n+s}$ such that

$$e_1 U S = e_1 \omega_1 + \ldots + e_{n+s} \omega_{n+s}$$

with

$$\omega_i = (e_1 \delta_1, \ldots, e_1 \delta_m) v_i, \quad i = 1, \ldots, n + s,$$

where $v_i$ is the $(m - n - s + i)$-th column of $U$. For $i = 1, \ldots, n + s$ we choose integral ideals $\mathcal{O}_i$ such that $(i, \mathcal{O}_i) = 1$ and $e_i \mathcal{O}_i = (e_i), e_i \in E$. We then define the $e_i$-component of $e_i$ by

$$e_i e_i := c_i \omega_i, \quad i = 1, \ldots, n + s.$$
By [9] Th. 1.4.6(1) $c_i v_i$ has coefficients in $c_i' \subseteq \mathcal{O}$. Hence we may choose a vector $w_i \in \mathbb{Z}^m$ such that $c_i v_i \equiv w_i \pmod{(1 - \zeta)}$. Then the element

$$
e_i := (e_1 \delta_1, \ldots, e_1 \delta_m) c_i v_i + (e_0 \delta_1, \ldots, e_0 \delta_m) w_i$$

is actually an $S$-unit with $e_1$-component $c_i v_i$. By construction we have

$$[e_1 E_S : e_1 A_{\mathcal{O}}] = \prod_{i=1}^{n+s} \frac{c_i}{c_i'} = \prod_{i=1}^{n+s} c_i' =: c' ,$$

which is prime to $l$, as desired.

To accomplish Step 2 we compute the matrix $H \in \text{Mat}_{n+r+s,n+s}(\mathbb{Z})$ such that $(l_e \epsilon_1, \ldots, l_e \epsilon_{n+s}) = (u_1, \ldots, u_{n+r+s}) H$, where $u_1, \ldots, u_{n+r+s}$ denotes a system of fundamental units for $U_{K,S}$. As shown at the end of the proof of Lemma 3.1 there exists an $(n+s) \times (n+s)$ minor $H_1$ of $H$ with $(\det(H_1), l) = 1$. Without loss of generality we may assume $H = \begin{pmatrix} \ast & \ast \\ H_1 & \ast \end{pmatrix}$, so that we can take $\eta_i' = u_i$ for $i = 1, \ldots, r$.

Note that by now we have constructed a sublattice $E'_S$ of $U_S$ generated over $\mathbb{Z}[G]$ by $e_1, \ldots, e_{n+s}, \eta'_1, \ldots, \eta'_r$ with the following property:

$$[e_1 U_S : e_1 E'_S] = N_{E/Q}(c') , \quad [e_0 U_S : e_0 E'_S] = 2 \abs{\det(H_1)} .$$

For $j = 0, \ldots, r$ we let $L_j/K_j$ denote the completion of $L/K$ at the totally ramified prime $p_j$. In the final Step 3 we will compute a matrix $C \in \text{Mat}_{r,r}(\mathbb{Z})$ and set $(\eta_1, \ldots, \eta_r) = (\eta'_1, \ldots, \eta'_r) C$. The matrix $C$ will be chosen such that $l \parallel \det(C)$ and $(\eta_i, L_j/K_j) = g_i^{d_{ij}}$ Kronecker delta purpose we consider the matrix $D = (d_{ij}) \in \text{Mat}_{r,r}(\mathbb{Z}/l\mathbb{Z})$ defined by

$$(\eta'_i, L_j/K_j) = g_i^{d_{ij}} .$$

**Lemma 3.2.** $D \in \text{Gl}_r(\mathbb{Z}/l\mathbb{Z})$.

**Proof.** By [2] Prop. 2.1 we know that there exist $\omega_1, \ldots, \omega_{n+s} \in U_S$ and $\nu_1, \ldots, \nu_r \in U_{K,S}$ such that

$$U_{S,l} = (\omega_1, \ldots, \omega_{n+s}, \nu_1, \ldots, \nu_r) \mathbb{Z}[G]$$

and $(\nu_i, L_j/K_j) = g_i^{d_{ij}}, \quad 1 \leq i, j \leq r$.

The proof of Lemma 3.1 shows that there exists a matrix $X = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \in \text{Gl}_{n+r+s}(\mathbb{Z}_d)$ such that

$$(l_e \epsilon_1, \ldots, l_e \epsilon_{n+s}, \eta'_1, \ldots, \eta'_r) = (l_e \epsilon_1, \ldots, l_e \epsilon_{n+s}, \nu_1, \ldots, \nu_r) X .$$

Moreover, it follows from [9] that $R \equiv 0 \pmod{l}$ and therefore $S \in \text{Gl}_r(\mathbb{Z}_d)$. We now conclude that

$$(\eta'_i, L_j/K_j) = \prod_{k=1}^{n+s} (l_e \omega_k, L_j/K_j)^{q_{ki}} \prod_{l=1}^r (\nu_l, L_j/K_j)^{s_{li}} = \prod_{l=1}^r (\nu_l, L_j/K_j)^{s_{li}} = g_0^{s_{li}} ,$$

where $Q = (q_{kl}), S = (s_{kl})$ and all exponents are read in $\mathbb{Z}/l\mathbb{Z}$. Hence $D \equiv S^t \pmod{l}$.

Now let $C \in \text{Mat}_{r,r}(\mathbb{Z})$ such that $C \equiv D^{-1} \pmod{l}$, and define $\eta_1, \ldots, \eta_r$ by the equality $(\eta_1, \ldots, \eta_r) = (\eta'_1, \ldots, \eta'_r) C$.

**Remark 3.3.** Lemmas 3.1 and 3.2 should be considered as very explicit versions of the main results of Holland (cf. [10] Th. 3.1) applied to our very special situation.
For the computation of $D$ it remains to show how to determine the local Artin symbols $(\eta_j', L_j / K_j)$. We let $v_j = v_{p_j}$ denote the $p_j$-valuation of $K$ for $j = 0, \ldots, r$. Set $e_{ij} = v_j(\eta'_j)$ and choose an element $\pi_j \in \mathcal{O}_K$ such that $v_j(\pi_j) = \delta_{ij}$ (Kronecker delta). Let $f = \prod_{k=0}^{l} p_k^{e_k}$ be the prime ideal factorization of the conductor $f$. If we let $\xi_{ij} \in \mathcal{O}_K$ denote a solution of the simultaneous congruences

$$
\begin{align*}
\xi_{ij} &\equiv \pi_{ij}^{e_{ij}} \pmod{p_k^{e_k}}, \quad k = 0, \ldots, r, k \neq j, \\
\xi_{ij} &\equiv \pi_{ij}^{e_{ij}} / \eta_j'(\mod{p_j^{e_j}}),
\end{align*}
$$

then class field theory shows that $(\eta'_j, L_j / K_j) = (\epsilon_{ij}, L / K)$, where

$$
\epsilon_{ij} = \xi_{ij} \prod_{p | \pi_j, p \not\equiv p_j} p^{-e_{ij}v_p(\pi_j)}.
$$

Recall that $L / K$ is given by $cl_l(K)$ and a subgroup $\mathcal{H}$ of index $l$. Assume that the integral ideal $\epsilon_0$ corresponds to $g_0$ via the global reciprocity isomorphism. Using [9, Alg. 4.3.2], it is then easy to compute $d_{ij} \in \mathbb{Z}/l\mathbb{Z}$ such that $\epsilon_{ij} = \epsilon_0^{d_{ij}}$ in $cl_l(K)/\mathcal{H}$.

### 3.2. Computation of $a_\chi$.

We assume that we have computed a sublattice $\mathcal{E}_S = \langle \epsilon_v : v \in S_0 \rangle[G]$ of $U_S$ satisfying the assumptions of Theorem 2.1. In this subsection we show how to compute complex approximations to the elements $a_\chi, \chi \in G^*$, which are uniquely determined by part (i) of Theorem 2.2. Writing $S_1 = \{\infty_1, \ldots, \infty_n, q_1, \ldots, q_s\}$ and $S_2 = \{p_1, \ldots, p_s\}$, we have

$$
R_S(\epsilon) = -\sum_{v \in S_1} \sum_{g \in G} \log |\epsilon|_{g w, g(w_v - w_0)} - \sum_{v \in S_2} \log |\epsilon|_{w_v}(w_v - w_0)
$$

for any $\epsilon \in U_S$. Considering the trivial character $\chi_0$, we have $S_{\chi_0} = S_0, S^{\chi_0} = \emptyset$, and from (6) we conclude that

$$
R_S(\epsilon_{\chi_0} \epsilon) = -\sum_{v \in S_1} \sum_{g \in G} \log |g^{-1}\epsilon|_{w_v, \epsilon_{\chi_0}(w_v - w_0)} - \sum_{v \in S_2} \log |\epsilon|_{w_v, \epsilon_{\chi_0}}(w_v - w_0).
$$

Hence $a_{\chi_0}$ is given by

$$
a_{\chi_0} = \frac{1}{l^r} \cdot \frac{\det(R_{\chi_0}(\mathcal{E}_S))}{L_S(0, \chi_0)^r},
$$

where $R_{\chi_0}(\mathcal{E}_S)$ denotes the matrix $(r_{st})_{s, t \in S_0}$ with

$$
r_{st} = \begin{cases} 
-\sum_{g \in G} \log |g^{-1}\epsilon|_{w_t}, & \text{if } t \in S_1, \\
-\log |\epsilon|_{w_t}, & \text{if } t \in S_2.
\end{cases}
$$

If $\chi$ is non-trivial, then $S_{\chi} = S_1, S^{\chi} = S_2$ and

$$
R_S(\epsilon_{\chi} \epsilon) = -\sum_{v \in S_1} \sum_{g \in G} \log |g^{-1}\epsilon|_{w_v, \epsilon_{\chi}}(w_v - w_0).
$$

Thus $a_{\chi}$ is given by

$$
a_{\chi} = (\chi(g_0) - 1)^r \cdot \frac{\det(R_{\chi}(\mathcal{E}_S))}{L_S(0, \chi^{-1})^r},
$$

where $R_{\chi}(\mathcal{E}_S)$ is given by

$$
R_{\chi}(\mathcal{E}_S) = \left(-\sum_{g \in G} \log |g^{-1}\epsilon|_{w_v, \epsilon_{\chi}}(g)\right)_{s, t \in S_1}.
$$
In conclusion, the complex approximations to $R_\chi(E_S), \chi \in G^*$, can easily be computed provided that we know how to evaluate $|a_\chi|_w$ for $\alpha \in L$ and a place $w$ of $L$. This is straightforward and left to the reader. An algorithm for the computation of complex approximations of the $L$-values is already implemented in the PARI system and explained in [9, Ch. 6].

3.3. Numerical verification of ETNC. This subsection is devoted to the verification (up to the precision of the computation) of the conjectural assertions

$$h_\alpha a \in \mathbb{Z}[G] \quad \text{and} \quad a_\chi \mathcal{O} = \text{Fitt}_\chi(U_S/E_S)/\text{Fitt}_\chi(cl_S).$$

We first describe how to compute the relevant Fitting ideals. Since $(l, |U_S/E_S|) = 1$, one easily shows that $e_\chi(\mathcal{O} \otimes_{\mathbb{Z}} U_S)/e_\chi(\mathcal{O} \otimes_{\mathbb{Z}} E_S) \simeq e_\chi(\mathcal{O} \otimes_{\mathbb{Z}} U_S/E_S)$ for each $\chi \in G^*$. By construction we have

$$\text{Fitt}_\chi(U_S/E_S) = \text{Fitt}_\chi(e_0 U_S/e_0 E_S)\mathcal{O} = 2|\det(H_1)|\det(C)|\mathcal{O}.$$  

If, in addition, $h_E = 1$, then our algorithm produces a sublattice $E_S$ such that $e_1 U_S = e_1 E_S$, and hence $\text{Fitt}_\chi(U_S/E_S) = \mathcal{O}$ for each $\chi \neq \chi_0$. In general, we observe that $e_\chi e_1, \ldots, e_\chi e_{n+s}$ constitutes an $E$-basis of $e_\chi U_S$. We compute the matrix $A \in \text{Mat}_{m,n+s}(E)$ such that

$$(e_\chi \delta_1, \ldots, e_\chi \delta_m) = (e_\chi e_1, \ldots, e_\chi e_{n+s})A.$$ 

Applying the HNF algorithm of [11, Alg. 1.4.7] to $A$, we obtain fractional $\mathcal{O}$-ideals $c_1, \ldots, c_{n+s}$ such that $\text{Fitt}_\chi(U_S/E_S) = \left( \prod_{i=1}^{n+s} c_i \right)^{-1}$.

For the computation of $\text{Fitt}_\chi(cl_S)$ we assume that the $S$-class group $cl_S$ is given by a direct product of cyclic subgroups $\langle [g_1] \rangle \times \ldots \times \langle [g_k] \rangle$, where for an integral $\mathcal{O}_L$-ideal $\mathfrak{a}$ we write $\langle \mathfrak{a} \rangle$ for its class in $cl_S$. Let $n_i$ denote the order of $[g_i]$. We further assume that the action of $G$ on $cl_S$ is known and given by $g \cdot ([g_1], \ldots, [g_k]) = ([g_1], \ldots, [g_k]) T(g)$ with $T(g) \in \text{Mat}_{k,k}(\mathbb{Z})$. Then $e_\chi [g_i]$ is represented by a column vector $v_i \in E^k$. We write $e_i$ for the $i$-th unit vector and let $A$ denote the matrix with columns $v_1, v_2, n_1 e_1, \ldots, n_k e_k$. Again applying the HNF algorithm for Dedekind domains, we compute ideals $c_1, \ldots, c_k$ such that

$$\text{Fitt}_\chi(cl_S) = \frac{h_S}{(\prod_{i=1}^k c_i)}.$$ 

At this stage of the algorithm we already have approximations to the complex numbers $a_\chi$ for all $\chi \in G^*$, so that it remains to identify $a_\chi, \chi \in G^*$, as elements of $E^\times$. By Stark’s conjecture $h_S a_{\chi_0}$ should be a rational integer. If this is confirmed by our computations, we round $h_S a_{\chi_0}$ to the nearest integer and consider $a_{\chi_0}$ as a rational number.

The elements $h_S a_\chi$ are conjecturally (again by Stark) conjugated integral numbers of $E$, so that the polynomial

$$f(x) = \prod_{\chi \neq \chi_0} (x - h_S a_\chi)$$

should have coefficients in $\mathbb{Z}$. If this is true up to the precision of the computation, we again round the coefficients of $f$ and factor $f$, $f = \prod_{i=1}^r f_i^{s_i}$. Each of the irreducible polynomials $f_i$ is expected to define a subextension of $E$, and if this is true, we can identify the $a_\chi$ as elements of $E$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Finally, after checking the equality \( a_\chi \mathcal{O} = \text{Fitt}_\chi(U_S/E_S)/\text{Fitt}_\chi(\mathcal{O}_S) \), we need to test whether \( h_{S\chi} a_\chi \equiv h_{S\chi} a_\chi \pmod{(1 - \zeta)} \) for all \( \chi \neq \chi_0 \). If these congruences hold, then \( h_\chi a \in \mathbb{Z}[G] \), and the numerical confirmation of ETNC is complete.

4. An Example

The algorithm described in Section 3 was implemented under PARI-GP, Version 2.0.20. We describe an explicit example. All computations were done with a real precision of 28 significant digits. Let \( K = \mathbb{Q}(\sqrt{5}) \) and set \( \omega = (1 + \sqrt{5})/2 \). We let \( f = p_0 p_1 p_2 \) with

\[
p_0 = (19, -10 + 2\omega), \quad p_1 = (31, -7 + 2\omega), \quad p_2 = (61, -27 + 2\omega).
\]

The PARI function \texttt{bnrinit} computes the ray class group \( cl_l(K) \), which is of order 90, generated by two elements \([g_1],[g_2]\), where \( g_1 = (15191), g_2 = (-15 + 42\omega) \) and \( \text{ord}([g_1]) = 30, \text{ord}([g_1]) = 3 \). There is precisely one subgroup \( H \) of \( cl_l(K) \) of index \( l = 3 \) such that the corresponding class field has conductor \( f \). Explicitly, \( H \) is generated by \( 3[g_1] \) and \( 2[g_1] + [g_2] \). We let \( L \) denote the extension corresponding to \( H \) and use the PARI-routine \texttt{bnrstark} to compute the defining polynomial

\[
h(x) = x^6 - x^5 - 127x^4 + 182x^3 + 4192x^2 - 8472x - 17776.
\]

Let \( \alpha \) denote a root of \( h \) so that \( L = \mathbb{Q}(\alpha) \).

By applying \texttt{bnfinit} we obtain the ring of integers, the ideal class group and a system of fundamental units for \( L \). The class number of \( L \) is 3, and it is easily checked that the ideal class group is generated by the ramified primes. Therefore we may use \( \{\infty_1, \infty_2, p_0, p_1, p_2\} \) as our set \( S \).

We let \( c_0 = g_0 \) be a fixed representative of \( cl_1(K)/H \) and use \texttt{nfgaloisconj} to compute \( G = \text{Gal}(L/K) \). It is absolutely essential for the subsequent computations that we choose \( g_0 \in G \) such that \( (c_0, L/K) = g_0 \). In this specific example \( g_0 \) is given by the substitution

\[
x = \frac{19}{7616}x^5 + \frac{223}{7616}x^4 - \frac{2579}{7616}x^3 - \frac{69}{28}x^2 + \frac{2353}{238}x + \frac{23999}{952}.
\]

If we carry out the algorithm of Section 3 we obtain the special units

\[
\begin{align*}
e_1 &= \frac{-53}{19040} \alpha^5 - \frac{869}{19040} \alpha^4 + \frac{8665}{19040} \alpha^3 + \frac{1011}{28} \alpha^2 - \frac{20142}{119} \alpha - \frac{66125}{238}, \\
e_2 &= \frac{47}{7616} \alpha^5 - \frac{565}{7616} \alpha^4 - \frac{2543}{7616} \alpha^3 + \frac{139}{28} \alpha^2 + \frac{571}{119} \alpha - \frac{77493}{952}, \\
e_3 &= \frac{7}{2} \omega + \frac{123}{2}, \\
e_4 &= \frac{11}{2} \omega + \frac{19}{2}.
\end{align*}
\]

We have \( \text{Fitt}_\chi(U_S/E_S) = 16\mathcal{O} \) and \( \text{Fitt}_\chi(U_S/E_S) = \mathcal{O}, \chi \neq \chi_0 \). We let \( \chi \) be the character determined by \( \chi(g_0) = \exp(2\pi i/l) \). For the extensions \( \infty_1 \) and \( \infty_2 \) we choose the embeddings uniquely determined by

\[
\begin{align*}
\infty_1 &: \alpha \mapsto -8.179796812075983731456745607, \\
\infty_2 &: \alpha \mapsto -7.947029995151366546855650171.
\end{align*}
\]
Then the computation of the regulator matrices and its determinants leads to
\[
\begin{align*}
\det(R_{x_0}(E_S)) &= -1440.138197903160150434022976, \\
\det(R_x(E_S)) &= -27.50768822513241632074447034 + 25.64332412284744888482277685i, \\
\det(R_{\tilde{x}}(E_S)) &= -27.50768822513241632074447034 - 25.64332412284744888482277685i.
\end{align*}
\]

We use the routine \texttt{bnrL1} to compute approximations to the \(L\)-values, and obtain
\[
\begin{align*}
L_S(0, \chi_0) &= 10.0000000000000000000010, \\
L_S(0, \chi) &= 25.3617780458999999999999258, \\
L_{\tilde{x}}(0, \tilde{\chi}) &= 25.36177804589999999999999237 + 0.00000000000000000000108i.
\end{align*}
\]

Putting everything together, approximations of the complex numbers \(a_x\) (defined in (7) and (8)) are given by
\[
\begin{align*}
a_{x_0} &\approx 16.0000000000000000000010, \\
a_{\chi} &\approx 0.9999999999999999999999258 - 0.00000000000000000000106i, \\
a_{\tilde{x}} &\approx 0.9999999999999999999999237 + 0.00000000000000000000108i.
\end{align*}
\]

This suggests that \(a_{x_0} = 16, a_{\chi} = a_{\tilde{x}} = 1\) and hence \(a = 6 + 5g_0 + 5g_0^2\). Altogether these numerical results confirm the validity of ETNC in this example.

The algorithm has been applied to a lot more examples, each time establishing the validity of ETNC. These numerical results can be found under
\[
http://www.math.uni-augsburg.de/~bley.
\]

ACKNOWLEDGMENTS

The algorithm has been implemented under PARI-GP for extensions \(L/K\) of a real quadratic field \(K\). I am very grateful to Dimitrij Kusnezow, who did most of the programming. I am in addition grateful to the referee for his very careful reading of the manuscript and several helpful remarks.

REFERENCES


Institut für Mathematik, Universität Augsburg, Universitätsstrasse 8, D-86159 Augsburg, Germany
E-mail address: bley@math.uni-augsburg.de