Accelerating the Tower Number Field Sieve with Galois Automorphisms

Haetham Al Aswad, Cécile Pierrot, Emmanuel Thomé

Abstract. The number field sieve algorithm and its variants are the best algorithms to solve the discrete logarithm problem in finite fields. When the extension degree is composite, the tower variant TNFS is the most efficient one. The interest in finite fields with composite extension degrees such as 6 and 12 is highly motivated by pairing based cryptography, which for the moment do not have a good quantum-resistant equivalent. The two most costly steps in TNFS are the *relation collection* and the *linear algebra*. While the use of order k Galois automorphism allow to accelerate the relation collection step by factor k, using them to accelerate the linear algebra step remains an open problem. This problem is solved for $k = 2$, leveraging a quadratic acceleration factor equal to 4.
In this work we solve this problem for $k = 6$ and $k = 12$. We present a new construction that allows the use of an order 6 (resp. 12) Galois automorphism in any finite field $\mathbb{F}_{p^6}$ (resp. $\mathbb{F}_{p^{12}}$), thus accelerating the linear algebra step with approximately a factor 36 (resp. 144). Moreover, we provide a SageMath implementation of TNFS and our new construction and validate our findings on small examples.

1 Introduction

Context. The discrete logarithm problem in a cyclic group $\mathbb{G}$ with a generator $g \in \mathbb{G}$ is the computational problem of finding an integer x modulo $|\mathbb{G}|$ for a given target $T \in \mathbb{G}$, such that $T = g^x$. Despite the growing interest in post-quantum cryptography, the discrete logarithm problem is still at the basis of many currently-deployed public key protocols. This article deals with the discrete logarithm problem in the group of invertible elements of a finite field, $\mathbb{G} = \mathbb{F}_{p^n}^*$, excluding small characteristic finite fields due to the existence of quasi-polynomial time algorithms [4,18,29]. With the usual notation $L_Q(\alpha, c) = \exp(c \cdot (\log Q)^\alpha (\log\log Q)^{1-\alpha})$, a family of finite fields of size Q and characteristic p is said to be of medium or large characteristic if there exists $1/3 \leq \alpha \leq 1$ and $c > 0$ such that $p = L_Q(\alpha, c)$.

The Number Field Sieve. Initially proposed as an integer factoring algorithm in the 90's [9,31], the Number Field Sieve (NFS) was later adapted to the discrete logarithm problem in prime fields [17], and medium and large characteristic finite fields [26]. Currently, the most efficient algorithms to compute discrete logarithm in medium or large characteristic finite fields is still (a variant of) NFS. Numerous variants exist, depending on the sub-case, but they all compute discrete logarithms in finite fields in time $L_Q(1/3, c)^{1+o(1)}$, for some constant

$0 < c < 2.3$ that depends on the variant and the characteristic size, where $o(1)$ tends to 0 as the finite field size Q tends to infinity.

The Tower variant, TNFS[1] [27,28,38] applies when the extension degree n is composite and its asymptotic complexity is lower that NFS for medium characteristic finite fields. Recent works have shown that the TNFS variant is practical as well. De Micheli, Gaudry and Pierrot [13] reported in 2021 the first implementation of TNFS and performed a record computation on a 521-bit finite field with extension degree $n = 6$. One year later, Robinson [36] reported a record computation using TNFS on a 512-bit finite field of extension degree $n = 4$. These records confirm that TNFS is currently the best algorithm that computes discrete logarithms in composite extension degree finite fields. Table 1 compares the performances of NFS and TNFS on the last discrete logarithm records with composite extension degrees. NFS and all its variants functions in four main

Year	Finite field	Bitsize of p^n	Cost in core-years	Algorithm	Work
2022	$\mathbb{F}_{p^4}$	512	6.3	TNFS	[36]
2021	$\mathbb{F}_{p^6}$	521	2.8	TNFS	[13]
2020	$\mathbb{F}_{p^6}$	423	9.3	NFS	[33]
2017	$\mathbb{F}_{p^6}$	422	26.1	NFS	[20]

Table 1: Cost in core-years of the last discrete logarithm records on finite fields with composite extension degrees. The two most recent records were carried with an implementation of TNFS and the two before with an implementation of NFS. The two TNFS-records are approximately 100 bits larger, and yet their cost is lower.

steps, *polynomial selection*, *relation collection*, *linear algebra*, and *individual logarithm*. Asymptotically speaking, the *relation collection* and the *linear algebra* are equally hard and are the two most costly steps in all NFS variants. Further, the discrete logarithm records show that they are the two most costly steps in practice as well. Table 2 shows the cost of the relation collection step, the linear algebra step and the the whole computation of recent records with various extension degrees. Although the relation collection have a higher cost than the linear algebra in these records except one, it is important to note that the relation collection is significantly more parallelisable than the linear algebra step. Additionally, adjusting some parameters—such as increasing the smoothness bound—could balance the costs of these steps.

Composite extension degrees in cryptographic applications. Considering finite fields with composite extensions is highly motivated by pairing-based cryptography. Pairings first appeared in 1940 when Weil showed a way to map points of order r on a supersingular elliptic curve to elements of order r in a finite field,

[1] Sometimes referred to as the extended Tower Number Field Sieve (exTNFS).

Bitsize of p^n	Finite Field	Cost in core days			Work
		Relation collection	Linear algebra	Total	
795	$\mathbb{F}_p$	876,000	228,125	116,800,0	[8]
595	$\mathbb{F}_{p^2}$	157	18	175	[3]
593	$\mathbb{F}_{p^3}$	3287	5113	8400	[16]
521	$\mathbb{F}_{p^6}$	388	23	413	[13]
512	$\mathbb{F}_{p^4}$	878	20	368	[36]
324	$\mathbb{F}_{p^5}$	359	11.5	386	[19]
203	$\mathbb{F}_{p^{12}}$	10.5	0.28	11	[24]

Table 2: Costs of the relation collection, the linear algebra and the whole computation in the last discrete logarithm records with various extension degrees.

but the first algorithm to efficiently compute the Weil pairing was only published in 2004 thanks to Miller [34]. In the early 2000s, efficient pairing-based protocols were presented [6, 7, 25]. Nowadays pairings have a wide range of applications, for example they are used in the Elliptic Curve Direct Anonymous Attestation protocol that is embedded in the current version of the Trusted Platform Module [40] (TPM2.0 Library), released in 2019. The security of these protocols relies on both the discrete logarithm problem in the group of points of a pairing-friendly elliptic curve, and on the discrete logarithm problem in a non prime finite field, which means where the extension degree $n > 1$. The curves which must be chosen with very restrictive properties to guarantee efficiency determine the extension degree of the finite field involved. While some of the finite fields used have prime extension degrees such as $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$, composite extension degrees are the most used ones such as $\mathbb{F}_{p^6}$ with the Cocks–Pinch modified curve or the MTN6 curves, and $\mathbb{F}_{p^{12}}$ with the BLS12 curves. Interestingly, there is no good post-quantum candidates to replace pairing-based protocols yet.

vous êtes d'accord ou je dis n'imp ?

Use of Galois automorphisms to accelerate the two hardest steps in NFS. The use of Galois automorphisms in the NFS context necessitate additional restrictive requirements to the *polynomial selection* step to construct the commutative diagram with adequate automorphisms. Given adequate automorphisms of order k, they can be used to accelerate the relation collection by approximately a factor k. Further, when the automorphisms order is 2, these automorphisms can be leveraged to accelerate the linear algebra step by approximately a factor 4 [3, 14, 44]. This was put into practice in the last discrete logarithm record on $\mathbb{F}_{p^6}$ [14] which allowed to accelerate the linear algebra step by approximately factor 4. However, the general problem of accelerating the linear algebra step by approximately factor k^2 using adequate order k automorphisms remains open for $k > 2$. We refer to this problem by $\mathcal{P}_k$.

Our work. We solve $\mathcal{P}_6$ and $\mathcal{P}_{12}$. Specifically, our work focuses on accelerating the linear algebra step in the TNFS algorithm when applied to finite fields with extension degrees 6 and 12. Given any finite field of extension degree 6,

resp. 12, we first show using the work in [3] a method to construct a TNFS diagram with adequate automorphisms of order 6, resp. 12. Second, we present a new construction that allows the use of these automorphisms to accelerate the linear algebra step in TNFS with a factor approximately equal to 36, resp. 144. Third, we provide an implementation of TNFS in SageMath together with our construction to illustrate our findings on small size finite fields.

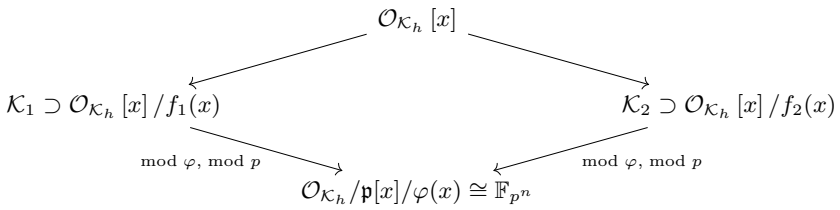
Outline of the article. We start with a description of TNFS in Section 2. Section 3 defines the Galois automorphisms that are useful in this work and shows how to use them to accelerate the relation collection step. Section 4 exposes the conditions and obstacles and reviews the literature on using automorphisms to accelerate the linear algebra step. In Section 5 we present a new construction and we show in Section 6 that the new construction allows to accelerate the linear algebra step with factors 36 and 144 in finite fields of extension degrees 6 and 12 respectively. Finally, Section 7 presents our experiments that validate our findings.

2 Background on the Tower Number Field Sieve

We target a finite field $\mathbb{F}_{p^n}$ where n is composite. Let η be a non-trivial divisor of n and denote $\kappa = n/\eta$. Since the computation of a discrete logarithm in a group can be reduced to its computation in one of its prime subgroups by Pohlig-Hellman's reduction, we work modulo ℓ, a non trivial prime divisor of $\Phi_n(p)$, with Φ_n the n-th cyclotomic polynomial. The classical TNFS setup considers the intermediate number field $\mathcal{K}_h = \mathbb{Q}(\iota)$ where ι is a root of h, a polynomial of degree η over $\mathbb{Z}$ that remains irreducible modulo p. For a number field $\mathcal{K}$, we let $\mathcal{O}_{\mathcal{K}}$ be its ring of integers. For simplicity, we assume throughout this article that $\mathcal{O}_{\mathcal{K}_h} = \mathbb{Z}[\iota]$. This implies in particular that h is monic.

Above $\mathcal{K}_h$, define two number fields $\mathcal{K}_1 = \mathcal{K}_h[x]/f_1(x)$ and $\mathcal{K}_2 = \mathcal{K}_h[x]/f_2(x)$ where f_1, f_2 are irreducible polynomials over $\mathcal{O}_{\mathcal{K}_h}$ that share an irreducible factor φ of degree κ modulo the unique ideal $\mathfrak{p}$ over p in $\mathcal{K}_h$. In particular, f_1 and f_2 have degree at least κ. Let α_i be root of f_i in $\mathcal{K}_i$ for $i = 1, 2$. Because of the conditions on the polynomials h, f_1 and f_2, there exist two ring homomorphisms from $\mathcal{O}_{\mathcal{K}_h}[x]$ to the target finite field $\mathbb{F}_{p^n}$ through the number fields $\mathcal{K}_1$ and $\mathcal{K}_1$. This allows to build a commutative diagram as in Figure 3. When η and κ are coprime (which is always possible with $n = 6$ or $n = 12$), then f_1 and f_2 can be defined over $\mathbb{Z}$. We make this choice for the rest of the article.

The general framework of TNFS is common to all its variants. The *polynomial selection* step sets up the commutative diagram of Figure 3 by selecting adequate polynomials h, f_0 and f_1. Thereafter, by finding many small to medium size smooth numbers and factoring them, the *relation collection* step establishes linear relations involving prime ideals of small norms in the number fields $\mathcal{K}_1$ and $\mathcal{K}_2$. The unknowns of these equations are the values on the small prime ideals of a linear map called the *virtual logarithm map*. When enough equations are found, the *linear algebra* step solves the system. Given a target T in the



Diag. 3: Commutative diagram of Tower NFS.

finite field, the last step called the *individual logarithm* step establishes a linear equation between the logarithm of T and the the virtual logarithms of the small ideals, which reveals the logarithm of the target.

Polynomial selection. Several methods to do TNFS polynomial selection are known. For example, the Conjugation, JLSV or Sarkar-Singh's methods [3, 26, 37] can be used. Each polynomial selection method yields different degrees and coefficient sizes which influence the whole performance of the algorithm. Based on the recent records [13, 36], the Conjugation method seems to perform the best in practice, and further, the work in [3] shows how to construct adequate automorphisms using this method. Therefore, it is the only polynomial selection method considered in this work.

Conjugation polynomial selection [3]. First a polynomial h of degree η and with small integer coefficients that remains irreducible modulo p is chosen. In order to reduce the number of duplicate relations, h should be selected with the value $\zeta_{\mathcal{K}_h}(2)$ as close to 1 as possible, where $\zeta_{\mathcal{K}_h}$ denotes the Dedekind zeta function of the number field. Second, a quadratic irreducible polynomial μ over $\mathbb{Z}$ with small coefficients is initially selected, which possesses a root λ modulo p. Third, two polynomials g_0 and g_1 with small integer coefficients are chosen with the condition that $\deg(g_1) < \deg(g_0) = \kappa$ and $\varphi := g_0 + \lambda g_1$ is irreducible modulo p. The polynomial f_1 is defined as $f_1 := \mathrm{Res}_Y(\mu(Y), g_0 + Y g_1)$, and f_2 is defined as $f_2 := v g_0 + u g_1$ where $\frac{u}{v} \equiv \lambda \mod p$ is a rational reconstruction of λ. Given that $f_1 \equiv 0 \mod p \mod \varphi$ and $f_2 \equiv v\varphi \mod p$, both share φ as a factor modulo p. Their respective degrees are 2κ and κ, and their coefficient sizes are within $O(1)$ and $O(\sqrt{p})$.

Relation collection. The goal of the relation collection step is to select, among the set of polynomials $\phi(x, \iota) \in \mathcal{O}_{\mathcal{K}_h}[x]$ at the top of the diagram, the candidates that yield a relation. A relation is found if the polynomial $\phi(x, \iota)$ mapped to principal ideals in $\mathcal{O}_{\mathcal{K}_1}$ and $\mathcal{O}_{\mathcal{K}_2}$ are *smooth* (respectively B_1- and B_2-smooth for some bounds B_1 and B_2.). Most often the search space for relation collection consists of linear polynomials $\phi(x, \iota) = a(\iota) - b(\iota)x \in \mathcal{O}_{\mathcal{K}_h}[x]$. The ideals that occur in the factorizations in $\mathcal{O}_{\mathcal{K}_1}$ and $\mathcal{O}_{\mathcal{K}_2}$ constitute the factor basis $\mathcal{F}$. More

precisely, we define it as the disjoint union $\mathcal{F} = \mathcal{F}_1 \sqcup \mathcal{F}_2$ with, for $i = 1, 2$:

$$\mathcal{F}_i(B_i) = \{\text{prime ideals of } \mathcal{O}_{\mathcal{K}_i} \text{ of norm} \leq B_i \text{ and inertia degree 1 over } \mathcal{K}_h\}.$$

To test the B_i-smoothness on each side, one needs to evaluate the norms $N_i(a(\iota) - b(\iota)\alpha_i)$ for $i = 0, 1$ where $\mathcal{N}_i$ defines the algebraic norm in $\mathcal{K}_i$. this allows to test the B_i-smoothness over integer values. The relation collection stops when we have enough relations to construct a system of linear equations that may be full rank. The unknowns of these equations are the *virtual logarithms* of the ideals of the factor basis. The definition and construction of the virtual logarithm map is detailed in Section 2.1.

Linear algebra. A good feature of the linear system created is that the number of non-zero coefficients per line is very small. This allows to use sparse linear algebra algorithms in $\mathbb{Z}/l\mathbb{Z}$ such as the Wiedmann algorithm that we describe in Appendix B, or Coppersmith's block Wiedemann algorithm [11] for which parallelization is partly possible. The output of this step is a kernel vector corresponding to the virtual logarithms of the ideals in the factor basis.

Individual discrete logarithm. The final step consists in finding the discrete logarithm of one or several target elements. This step is subdivided into two substeps: a smoothing step and a descent step. The smoothing step is an iterative process where the target element is randomized until the randomized value lifted back to one of the number fields $\mathcal{K}_i$ is B_i'-smooth for a smoothness bound $B_i' > B_i$. The second step consists in decomposing every factor of the lifted value, in our case prime ideals with norms less than a smoothness bound B_i', into elements of the factor basis for which we now know the virtual logarithms. This eventually makes it possible to reconstruct the discrete logarithm of the target element.

TNFS differs from NFS in this step as there exist improvements for the smoothing step when the target finite field has proper subfields [2, 23].

2.1 The Shcirokauer and the virtual logarithm maps

This Section follows the presentation in [42]. A relation is found when an element at the top of Diagram 3 is smooth in both $\mathcal{K}_1$ and $\mathcal{K}_2$. Let us drop the subscript and consider $\mathcal{K}$ one of the two number fields. In the previous section we presented the smooth elements of $\mathcal{K}$ by the factorization of the principal ideals they generate. However, this is a simplified presentation and is not sufficient as it does not allow to distinguish between two elements that generate the same ideal. The goal of this section is to show how to correctly represent the elements of the following set Γ and how to define the virtual logarithm map on it.

$$\Gamma := \{\phi \in \mathcal{K}^* | (\phi) \text{ factors in the factor basis}\}.$$

Since two elements that generate the same ideal only differ by a unit, the unit group of $\mathcal{K}$ denoted as $\mathcal{O}^\times$ is our way to complete the representation.

Dirichlet's unit theorem provides the structure of the unit group by the following abelian group isomorphism

$$\mathcal{O}^\times \simeq \mu_\mathcal{K} \times \mathbb{Z}^r,$$

where r is an integer called the *unit rank* of $\mathcal{K}$ and $\mu_\mathcal{K}$ is the group of roots of unity of $\mathcal{K}$. A $\mathbb{Z}$-basis of the non-torsion part (i.e, $\mathbb{Z}^r$) is called a *system of fundamental units*.

Since the virtual logarithm map is a linear map with value in $\mathbb{Z}/\ell\mathbb{Z}$, all ℓ-th power elements fall in its kernel. For this reason, all groups will be considered modulo the group of their ℓ-th powers. The following proposition provides the structure of Γ/Γ^ℓ as an $\mathbb{F}_\ell$-vector space.

Proposition 1. *Let $\mathcal{F}$ the factor basis on side $\mathcal{K}$, $\mathcal{I}$ the group of fractional ideals that completely factor in $\mathcal{F}$, Γ and $\mu_\mathcal{K}$ defined as above, and recall that ℓ is a prime divisor of $\Phi_n(p)$. Then, Γ/Γ^ℓ is a $\mathbb{F}_\ell$-vector space. Further, suppose that the class number of $\mathcal{K}$ denoted as $h_\mathcal{K}$ and $|\mu_\mathcal{K}|$ are both coprime to ℓ, then we have the following vector space isomorphism*

$$\Gamma/\Gamma^\ell \simeq \mathcal{O}^\times/(\mathcal{O}^\times)^\ell \times \mathcal{I}/\mathcal{I}^\ell,$$

with basis $\{u_1, \ldots, u_r\} \cup \mathcal{F}/\mathcal{F}^\ell$, where, $\{u_1, \ldots, u_r\}$ is a system of fundamental units of $\mathcal{K}$ considered modulo $(\mathcal{O}^\times)^\ell$.

Note that in practice $|\mu_\mathcal{K}|$ and $h_\mathcal{K}$ are both coprime to ℓ with very large probability as ℓ is large.

Proof. The proof is presented in Appendix A.1.

The Schirokauer map If it was easy to compute a system of fundamental units (which is not the case), then by Proposition 1 an element of Γ/Γ^ℓ could be represented by the factorization of the ideal it generates and its valuation on a system of fundamental units. By the mean of a new hypothesis, Schirokauer maps [39] allow to get around the hard computational problem of computing a system of fundamental units.

Definition 1 (Usual definition of a Schirokauer map). *Consider Γ from Proposition 1 and denote r the unit rank of $\mathcal{K}$. A Schirokauer map on Γ/Γ^ℓ is any full-rank $\mathbb{F}_\ell$-linear map $\Gamma/\Gamma^\ell \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^r$ that still has full rank when restricted to $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$.*

In other words, when restricted to $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$ a Schiorokauer map on $\mathcal{K}$ is a dual basis of a system of fundamental units.

Construction of a Schirokauer map. Let $F \in \mathbb{Q}[X]$ irreducible such that $\mathcal{K} = \mathbb{Q}[X]/(F)$ and suppose that ℓ does not divide its discriminant which is denoted $\mathrm{Disc}(F)$. Consider the decomposition of F modulo ℓ as the product of irreducible factors: $F = \prod_j F_j \mod \ell$, where all factors are distinct thanks to the above requirement. Denote α a root of F in $\mathcal{K}$ and for simplicity suppose that F is monic (otherwise replace α by the dominant coefficient times α). By the Chinese remainder theorem we have the ring homomorphism:

$$\mathbb{Z}[\alpha]/\ell\mathbb{Z}[\alpha] \simeq \mathcal{O}/\ell\mathcal{O} \simeq \mathbb{F}_\ell[X]/(F) \simeq \prod_j \mathbb{F}_\ell[X]/(F_j),$$

where the first equivalence is due to the fact that ℓ does not divide the index of α defined as $[\mathcal{O} : \mathbb{Z}[\alpha]]$, which is a divisor of $\mathrm{Disc}(F)$. Define $\omega := \mathrm{lcm}\left(\ell^{\deg(F_j)} - 1\right)$ and consider $x \in \Gamma$. First, by the second isomorphism above, $x \bmod \ell\mathcal{O}$ can be seen as an element of $\mathbb{F}_\ell[X]/(F)$. Second, by the third isomorphism, we have $x^\omega \equiv 1 \mod \ell\mathcal{O}$. Further, lifting the congruence modulo $\ell^2\mathcal{O}$ we get $x^\omega \equiv 1 + \ell \cdot P(x) \bmod \ell^2\mathcal{O}$, where P is a polynomial over $\mathbb{Z}$ with degree bounded by $\deg(F) - 1$. By taking the quotient by Γ^ℓ we get the following linear map

$$\mathbf{A} : \begin{cases} \Gamma/\Gamma^\ell \longrightarrow & \mathbb{F}_\ell[X]/(F) \\ x \longmapsto \frac{x^\omega - 1}{\ell} & \mod \ell\mathcal{O} := P(x) \end{cases} \tag{1}$$

As far as we know, all Schirokauer map constructions (including ours presented in later sections) are based on the map $\mathbf{A}$.

The Schirokauer map used in the literature is constructed from $\mathbf{A}$ as follows. Since the unit rank r of $\mathcal{K}$ is smaller than the degree of $\mathcal{K}$ over $\mathbb{Q}$, a map $\Lambda : \Gamma/\Gamma^\ell \to (\mathbb{Z}/\ell\mathbb{Z})^r$ is *defined* over an element x as the first r coefficients of $\mathbf{A}(x)$. We emphasize that the choice of the *first* r coordinates is arbitrary and non canonical (depends on the choice of F), one could choose any r distinct coefficients or even any r independent integer linear combinations of the coefficients. However, the integer linear combinations must be the same independently of x. This provides a linear map that is computable in polynomial time. We empathize that there is no efficient way for testing whether it is a Schirokauer map or not, in particular because there is no efficient way of computing a system of fundamental units. For the purpose of TNFS (and all NFS variants), this map is *supposed* to be a Schirokauer map, which is stated by the following assumption.

Assumption 1 *Λ have maximal rank on $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$.*

Under assumption 1, an element $\phi \in \Gamma/\Gamma^\ell$ is represented by its Schirokauer map value together with the factorization of the ideal it generates. That is, if $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_b\}$ is the factor basis on side $\mathcal{K}$, then we use the representation

$$\phi \leftrightarrow (\Lambda(\phi)_1, \ldots, \Lambda(\phi)_r, \mathrm{val}_{\mathfrak{p}_1}(\phi), \ldots, \mathrm{val}_{\mathfrak{p}_b}(\phi)) \tag{2}$$

The virtual logarithm map and the matrix of relations Consider back both number fields $\mathcal{K}_1$ and $\mathcal{K}_2$ as in Diagram 3 with the corresponding sets Γ_1 and Γ_2 and with a Schirokauer map on each side: Λ_1 and Λ_2.

Definition 2 (Virtual logarithm). *A virtual logarithm is a couple of $\mathbb{F}_\ell$-linear forms* $(\mathrm{vlog}_1, \mathrm{vlog}_2)$ *where for* $i = 1, 2$ $\mathrm{vlog}_i : \Gamma_i/\Gamma_i^\ell \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$ *and such that for all* $\phi \in \mathcal{O}_{\mathcal{K}_h}[x]$ *that project to both* $\phi_1 \in \Gamma_1$ *and* $\phi_2 \in \Gamma_2$ *we have*

$$\mathrm{vlog}_1(\phi_1) = \mathrm{vlog}_2(\phi_2).$$

The goal of the relation collection and the linear algebra is to compute a virtual logarithm map. Under Assumption 1 on Λ_1 and Λ_2, denote $\{u_{j,i}\}_{i=1}^{r_j}$ for $j = 1, 2$ for the dual basis of Λ_j, which is *not computed*. When an element ϕ is smooth on both sides, we get the following equation

$$\begin{aligned} &\sum_{i=1}^{r_1} \Lambda(\phi_1)_i \mathrm{vlog}(u_{1,i}) + \sum_{i=1}^{b_1} \mathrm{val}_{\mathfrak{p}_{1,i}}(\phi_1)\mathrm{vlog}(\mathfrak{p}_{1,i}) \\ =&\sum_{i=1}^{r_2} \Lambda(\phi_2)_i \mathrm{vlog}(u_{2,i}) + \sum_{i=1}^{b_2} \mathrm{val}_{\mathfrak{p}_{2,i}}(\phi_2)\mathrm{vlog}(\mathfrak{p}_{2,i}), \end{aligned} \tag{3}$$

where the unknowns are the virtual logarithm values. Such an equation is represented as a row in the matrix of relations by its scalars which belong to $\mathbb{Z}/\ell\mathbb{Z}$ (and by putting a negative sign to the right side). Hence, each column represents either the virtual logarithm of an ideal in the factor basis, or the virtual logarithm of one of the units. When enough relations are found, a non trivial kernel element of the matrix contains the values of a virtual logarithm map.

One hopes that a virtual logarithm map "correspond" to a $\mathbb{Z}/\ell\mathbb{Z}$ linear form of the finite field, which is nothing else than the logarithm modulo ℓ in some basis $\tilde{g}$. This is formulated by the following assumption, which is always assumed for TNFS and all variants.

Assumption 2 *Let* Γ *denote* Γ_1 *or* Γ_2*, and* vlog *a virtual logarithm map on the corresponding side. For all* $\phi, \tilde{\phi} \in \Gamma/\Gamma^\ell$ *that project to the same element in the finite field we have*

$$\mathrm{vlog}(\phi) = \mathrm{vlog}(\tilde{\phi}).$$

Assumption 2 provides a linear map $\overline{\log}$ on $\mathbb{F}_{p^n}^\times/(\mathbb{F}_{p^n}^\times)^\ell$ that is partially defined. Indeed, for $\overline{\phi} \in \mathbb{F}_{p^n}^\times/(\mathbb{F}_{p^n}^\times)^\ell$ that lifts to $\phi \in \Gamma/\Gamma^\ell$, we define $\overline{\log}(\overline{\phi}) := \mathrm{vlog}(\phi)$. The map $\overline{\log}$ is the logarithm modulo ℓ in $\mathbb{F}_{p^n}^\times$ in some basis $\tilde{g}$, as it is a linear map of rank 1 over $\mathbb{F}_{p^n}^\times/(\mathbb{F}_{p^n}^\times)^\ell$.

Remark 1. Assumption 2 is needed as its constraints do not appear as equations in the matrix of relations. One could add such equations, however, it is costly to test whether lifts of the same element are smooth and it is rare that two elements that project to the same element are smooth. One generally gets at the end of the linear algebra a virtual logarithm map that verifies this Assumption. In the rare scenario where it does not, the algorithm fails.

3 TNFS Automorphisms

A desirable property of the polynomials h, f_1, and f_2, is to ensure the presence of field automorphisms in $\mathcal{K}_1$ and $\mathcal{K}_2$. However, not any automorphisms would be useful in the TNFS context, we need TNFS automorphisms, defined below.

Definition 3 (TNFS Automorphism). *Let n denote the finite field's degree and consider the absolute fields $\mathcal{K}_1$ and $\mathcal{K}_2$ (i.e, defined over $\mathbb{Q}$). Two automorphisms $\sigma_1 \in \mathrm{Aut}(\mathcal{K}_1)$ and $\sigma_2 \in \mathrm{Aut}(\mathcal{K}_2)$ of same order k constitute a TNFS automorphism if the following two conditions are fulfilled:*

- ***Both are Frobenius.*** *Each fix a degree n prime ideal $\mathfrak{p}_i$ over p in the corresponding absolute ring $\mathcal{O}_i$.*
- ***Project to the same Frobenius.*** *There exists an order k Frobenius of the finite field $\overline{\sigma} \in \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ such that for all $(\phi_1, \phi_2) \in \mathcal{O}_h[x]/(f_1) \times \mathcal{O}_h[x]/(f_2)$:*

$$\Psi_1\left(\sigma_1(\phi_1)\right) = \overline{\sigma}\left(\Psi_1(\phi_1)\right) \quad \textit{and} \quad \Psi_2\left(\sigma_2(\phi_2)\right) = \overline{\sigma}\left(\Psi_2(\phi_2)\right),$$

  where for $i = 1, 2$, Ψ_i are the projection morphisms to the finite field defined in diagram 3 by $\bmod \varphi \bmod p$.

Note that the restrictive condition is the "both are Frobenius". Indeed, the other condition is just a matter of choosing the right automorphisms σ_1 and σ_2 so that they project to the *same* Frobenius in the finite field. Concretely, since σ_1 fixes a prime ideal of degree n over p, denoted as $\mathfrak{p}$, it can be defined modulo $\mathfrak{p}$. This provides a Frobenius $\overline{\sigma}_1 \in \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$. Further, $\overline{\sigma}_1$ has order k because p is not ramified in $\mathcal{K}_1$. Similarly, an automorphism $\overline{\sigma}_2 \in \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ is defined with σ_2. If $\overline{\sigma}_1 \neq \overline{\sigma}_2$, it is sufficient to replace σ_1 by σ_1^s with s coprime to k until the equality is fulfilled, which will happen for an $1 \leq s \leq k$ coprime to k.

3.1 Galois automorphisms with the Conjugation polynomial selection

Using the Conjugation polynomial selection, this section exposes a method to construct a TNFS Diagram (3) with two automorphisms $\sigma_1 \in \mathrm{Aut}(\mathcal{K}_1)$ and $\sigma_2 \in \mathrm{Aut}(\mathcal{K}_2)$ both of order equal to n, the finite field's extension degree for various values of n. Recall that $n = \eta\kappa$, with η and κ non trivial and coprime.

Galois automorphisms with Conjugation. To construct a degree n automorphisms in both $\mathcal{K}_1$ and $\mathcal{K}_2$ with the Conjugation method, it is sufficient to choose the three polynomials such that $\mathcal{K}_h$ has a degree η automorphism that we term as σ_h and each of $\mathcal{K}_{f_i} := \mathbb{Q}[x]/(f_i)$ has a degree κ automorphism denoted as σ_{f_i} for $i = 1, 2$. Indeed, for $i = 1, 2$, since η and κ are coprime, the automorphism σ_i of $\mathcal{K}_i$ defined by the joint action of σ_h and σ_{f_i} has order $\eta \times \kappa = n$.

In [3], the authors provide choices of g_0 and g_1 in the Conjugation method presented in §2 that provide automorphisms on $\mathcal{K}_{f_1}$ and $\mathcal{K}_{f_2}$ of orders equal

to 2, 3, 4 and 6. We transcript theses choices in Table 4 and use them in our constructions in the rest of the paper.

To sum up, to construct a TNFS diagram over $\mathbb{F}_{p^n}$ with two automorphisms (σ_1, σ_2) on $(\mathcal{K}_1, \mathcal{K}_2)$ of order n, first choose h of degree η with cyclic Galois group (for instance, $h = g_0 + g_1$ and $\deg(g_0) = \eta$ from Table 4), and second, apply the Conjugation method with $(\tilde{g}_0, \tilde{g}_1)$ from Table 4 where $\deg(\tilde{g}_0) = \kappa$.

It is not clear whether this construction provides TNFS automorphisms as in Definition 3. We prove later this statement for the automorphisms that we use.

Degree of $(\mathcal{K}_{f_1}, \mathcal{K}_{f_2})$	Automorphism's order	g_0	g_1	Automorphism $\alpha \mapsto$
$(4, 2)$	2	$x^2 + 1$ $x^2 - 1$ x^2	ax ax a	$1/\alpha$ $-1/\alpha$ $-\alpha$
$(6, 3)$	3	$x^3 - 3x - 1$	$-a(x^2 + x)$	$-(\alpha + 1)/\alpha$
$(8, 4)$	4	$x^4 - 6x^2 + 1$	$a(x^3 - x)$	$-(\alpha + 1)/(\alpha - 1)$
$(12, 6)$	6	$x^6 + 6x^5 -$ $20x^3 - 15x^2 + 1$	$a(2x^5 + 5x^4 -$ $5x^2 - 2x)$	$-(2\alpha + 1)/(\alpha - 1)$

Table 4: Table from [3]. Automorphisms with the Conjugation polynomial selection. The letter a designate any non-zero integer. The rational expression of the automorphism and its order are the same for both number fields. Further, the automorphism is also an automorphism of $g_0 + g_1$.

3.2 Acceleration of the relation collection with TNFS automorphisms

Using field automorphisms to accelerate the relation collection step is a quite straightforward idea. Suppose the existence of a TNFS automorphism of order k as in Definition 3: $\sigma_1 \in \mathrm{Aut}(\mathcal{K}_1)$, $\sigma_2 \in \mathrm{Aut}(\mathcal{K}_2)$ that correspond to $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Let $\phi \in \mathcal{O}_h[x]$ generates a relation:

$$(\phi_1) = \prod_{\mathfrak{p} \in \mathcal{F}_1} \mathfrak{p}^{\mathrm{val}_{\mathfrak{p}}(\phi_1)} \qquad \text{and} \qquad (\phi_2) = \prod_{\mathfrak{p} \in \mathcal{F}_2} \mathfrak{p}^{\mathrm{val}_{\mathfrak{p}}(\phi_2)}.$$

since two conjugate ideals have the same norm, the factor basis $\mathcal{F}_1$ and $\mathcal{F}_2$ are stable under the automorphisms σ_1 and σ_2 respectively. Therefore, applying the automorphisms on both sides produces a new relation

$$(\phi_1)^{\sigma_1} = \prod_{\mathfrak{p} \in \mathcal{F}_1} (\mathfrak{p}^{\sigma_1})^{\mathrm{val}_{\mathfrak{p}}(\phi_1)} \qquad \text{and} \qquad (\phi_2)^{\sigma_2} = \prod_{\mathfrak{p} \in \mathcal{F}_2} (\mathfrak{p}^{\sigma_2})^{\mathrm{val}_{\mathfrak{p}}(\phi_2)},$$

where for an ideal I, the notation I^{σ_i} refers to its conjugate ideal $\sigma(I)$. Indeed, this is a relation since both $\phi_1^{\sigma_1}$ and $\phi_2^{\sigma_2}$ project to the same element in the finite

field, that is $\overline{\phi}^{\overline{\sigma}}$, where $\overline{\phi}$ is the projection of ϕ_1 and ϕ_2 to the finite field. The process is applied similarly with $(\sigma_1^2, \sigma_2^2) \dots (\sigma_1^{k-1}, \sigma_2^{k-1})$, thus generating $k-1$ new relations for each known relation. Overall, using automorphisms of degree k divides the cost of the relation collection by approximately a factor k.

4 Acceleration of the linear algebra step with TNFS automorphisms

A TNFS automorphism of order k allows to accelerate the relation collection step by approximately a factor k. As for the linear algebra step, one hopes that the virtual logarithms of k conjugate ideals can be recovered from the virtual logarithm of one of these ideals. This would reduce the matrix size by a factor k and hence accelerate the linear algebra step by approximately a factor k^2 since its complexity is *almost quadratic*. Unfortunately, this is not true in general. The reason of failure is due to complications related to the Schirokauer map and the units, as we examine in the subsequent.

Notations. All the subsequet applies on both number fields $\mathcal{K}_1$ and $\mathcal{K}_2$ from Diagram 3. We drop the subscript and consider $\mathcal{K}$ one of the two number fields together with $\sigma \in \mathrm{Aut}(\mathcal{K})$ the corresponding component of a TNFS automorphism of order k. Denote $\overline{\sigma}$ the corresponding Frobenius of the finite field which expresses as $\overline{\sigma} : x \mapsto x^{\zeta}$, where ζ is a k-th primitive root of unity modulo ℓ. Further, the set $\{\mathfrak{p}_i\}_{i=1}^{b}$ consists of the prime ideals in the factor basis, and Λ is a Schirokauer map on side $\mathcal{K}$. Additionally, Assumption 1 is assumed on Λ and the set $\mathbf{u} := \{u_i\}_{i=1}^{r}$ denotes the system of fundamental units in $\mathcal{K}$ that is the dual basis of Λ—here r denotes the unit rank of $\mathcal{K}$. The notation $\mathrm{vlog}(\mathbf{u})$ refers to the r dimensional vector $(\mathrm{vlog}(u_1), \dots, \mathrm{vlog}(u_r))$. If ϕ belongs to Γ defined in Section 2.1, we abusively write $\mathrm{vlog}(\phi)$ and $\Lambda(\phi)$ instead of $\mathrm{vlog}\left(\phi \bmod \Gamma^{\ell}\right)$ and $\Lambda\left(\phi \bmod \Gamma^{\ell}\right)$. Last but not least, recall that ℓ is supposed coprime to the class number of $\mathcal{K}$, to the unit rank r, and to the cardinal of the roots of unity $|\mu_{\mathcal{K}}|$, which is true in practice with large probability.

Remark 2. Note that for all $x \in \mathbb{F}_{p^n}^{\times}$, $\log\left(x^{\overline{\sigma}}\right) \equiv \zeta \log(x) \bmod \ell$. To accelerate the linear algebra step using TNFS automorphisms, we need to construct a virtual logarithm map that verifies $\mathrm{vlog}(\mathfrak{p}^{\sigma}) \equiv \zeta\, \mathrm{vlog}(\mathfrak{p}) \bmod \ell$ for all prime ideals $\mathfrak{p}$ that belong to the factor basis.

4.1 Virtual logarithms of conjugate ideals

We start by proving the following central lemma which states that the virtual logarithm map vanishes on the elements fixed by a TNFS automorphism.

Lemma 1. *Let σ one of the two components of a TNFS automorphism and $\phi \in \Gamma$ such that $\sigma(\phi) = \phi$, then* $\mathrm{vlog}(\phi) = 0$.

Proof. By Assumption 2 on the virtual logarithm map, there exists $\tilde{g}$ a generator of the finite field's group $\mathbb{F}_{p^n}^\times$ such that $\mathrm{vlog}(\phi) = \log_{\tilde{g}}(\overline{\phi}) \bmod \ell$, where $\overline{\phi}$ denotes the projection of ϕ to the finite field. Moreover, $\overline{\phi}$ belongs to the proper subfield of $\mathbb{F}_{p^n}$ that is fixed point-wise by $\overline{\sigma}$. Indeed, by Definition 3 we have $\overline{\sigma}(\overline{\phi}) = \overline{\sigma(\phi)} = \overline{\phi}$. Lemma 1 from [22] states that the logarithm of an element that belongs to a proper subfield of $\mathbb{F}_{p^n}$ vanishes modulo ℓ, hence, $\log_{\tilde{g}}(\overline{\phi}) \equiv 0 \mod \ell$.

Applying the lemma to powers of σ, we get the following corollary.

Corollary 1. *Let σ a component of a TNFS automorphism of order k. Consider $\phi \in \Gamma$ such that there exists s a proper divisor of k with $\sigma^s(\phi) = \phi$. Then* $\mathrm{vlog}(\phi) = 0$.

The above lemma provides a link between the virtual logarithms of conjugate ideals, which is the subject of the following proposition.

Proposition 2. *Let σ one of the two components of a TNFS automorphism of order k, and $\mathfrak{p}$ a prime ideal. Then there exists $a \in \mathcal{K}^\sigma$ such that*

$$\sum_{i=0}^{k-1} \mathrm{vlog}\left(\mathfrak{p}^{\sigma^i}\right) = -h_\mathcal{K}\ \Lambda(a) \cdot \mathrm{vlog}(\mathbf{u}).$$

Proof. By the class group theorem, there exists $\gamma \in \mathcal{K}$ such that $(\gamma) = \mathfrak{p}^{h_\mathcal{K}}$. Therefor, for all $i \in [\![0, k-1]\!]$, $(\gamma^{\sigma^i}) = (\mathfrak{p}^{\sigma^i})^{h_\mathcal{K}}$. Applying the virtual logarithm map we get for all $0 \leq i \leq k-1$, $\mathrm{vlog}\left(\gamma^{\sigma^i}\right) = \Lambda\left(\gamma^{\sigma^i}\right) \cdot \mathrm{vlog}(\mathbf{u}) + h_\mathcal{K}\ \mathrm{vlog}\left(\mathfrak{p}^{\sigma^i}\right)$. Summing the k equations we get

$$\mathrm{vlog}\left(\prod_{i=0}^{k-1} \gamma^{\sigma^i}\right) = \Lambda\left(\prod_{i=0}^{k-1} \gamma^{\sigma^i}\right) \cdot \mathrm{vlog}(\mathbf{u}) + h_\mathcal{K} \sum_{i=0}^{k-1} \mathrm{vlog}\left(\mathfrak{p}^{\sigma^i}\right).$$

The left hand side is zero by Lemma 1 and the result follows with $a = \prod_{i=0}^{k-1} \gamma^{\sigma^i}$.

Computing the class number $h_\mathcal{K}$, the fundamental units $\mathbf{u}$ or the generators γ^{σ^i} in the above proof are hard computational problems. For this reason, the link between the virtual logarithms of conjugate ideals stated by Proposition 2 is *in general* not useful in practical computations. However, if it happens that $\Lambda(a) = 0$ or $\mathrm{vlog}(\mathbf{u}) = 0$, then the sum of the virtual logarithms of conjugate ideals is zero. In this scenario, there might exist a virtual logarithm map that verifies the equality $\mathrm{vlog}(\mathfrak{p}^\sigma) = \zeta\, \mathrm{vlog}(\mathfrak{p})$, where ζ is a k-th primitive root of unity modulo ℓ, since this would be compatible with the sum over conjugates being zero. All the constructions that allow to accelerate the linear algebra step do so by guaranteeing the above mentioned vanishing.

4.2 Condition to accelerate the linear algebra step with TNFS automorphisms

The key idea to use automorphisms in the linear algebra step is to identify constructions such that the following condition is satisfied in both number fields.

Condition 1 *Let σ one of the two components of a TNFS automorphism of order k. For each prime ideal $\mathfrak{p}$*

$$\sum_{i=0}^{k-1} \mathrm{vlog}\left(\mathfrak{p}^{\sigma^i}\right) = 0.$$

In constructions that verify Condition 1, one can add to the equations in the matrix of relations the *constraints* (on both sides)

$$\forall j \in [\![1, b]\!], \quad \mathrm{vlog}\left(\mathfrak{p}_j^{\sigma}\right) = \zeta\, \mathrm{vlog}(\mathfrak{p}_j),$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_b$ are the ideals in the factor basis. Indeed, these constraints are compatible with Condition 1 since for $\mathfrak{p}$ an ideal in the factor basis we have

$$\sum_{i=0}^{k-1} \mathrm{vlog}(\mathfrak{p}^{\sigma^i}) = \mathrm{vlog}(\mathfrak{p}) \sum_{i=0}^{k-1} \zeta^i = 0.$$

Therefore, adding the above constraints results in asking the linear algebra step to compute a virtual logarithm map that equates conjugate ideals up to a multiplication by a primitive root of unity. We emphasize that if Condition 1 is not satisfied, then adding the above constraints would result in an incompatible linear system with no solution. When Condition 1 is satisfied, these constraints are added to the matrix in the following way. Each k columns $C_0, \ldots, C_{k-1}$ representing k conjugate ideals $\mathfrak{p}, \ldots, \mathfrak{p}^{\sigma^{k-1}}$ are replaced by one column equal to $C := \sum_{i=0}^{k-1} \zeta^i C_i$.

When the orbit of the ideal $\mathfrak{p}$ has length s a proper divisor of k, then there exists a virtual logarithm map that verifies the above constraints and that vanishes on such ideals. Indeed, replacing σ by $\sigma^{k/s}$ in Condition 1 shows that $\sum_{i=0}^{s-1} \mathrm{vlog}(\mathfrak{p}^{\sigma^i}) = 0$. That is, there exists a virtual logarithm map verifying both equations $\mathrm{vlog}\left(\mathfrak{p}^{\sigma}\right) = \zeta\, \mathrm{vlog}(\mathfrak{p})$ and $\mathrm{vlog}\left(\mathfrak{p}^{\sigma}\right) = \zeta^{k/s}\, \mathrm{vlog}(\mathfrak{p})$, which implies $\mathrm{vlog}(\mathfrak{p}) = 0$. The columns corresponding to such ideals are simply removed from the matrix.

In order to estimate the gain in performance in the linear algebra brought by the automorphisms, it is crucial to examine the coefficient sizes of the new matrix and not only its dimension. Indeed, since the original matrix is sparse with coefficients mostly equal to -1, 0, or 1, the Wiedemann algorithm which is presented in Appendix B, or Block-Wiedemann algorithm for better parallelization, accomplishes the linear algebra step in approximately λN^2 arithmetic operations, where λ designates the average number of non-zero coefficients per row and N denotes the matrix dimension. The use of an order k automorphism

reduces the matrix dimension to approximately N/k, while maintaining the average number of non-zero coefficients per row roughly at λ. Indeed, in most relations, a maximum of one ideal per orbit tends to appear. Further, the coefficients in the matrix become mostly equal to $\{-\zeta^i, 0, \zeta^i\}_{0\leq i\leq k-1}$. The trick is to decompose the matrix $\mathcal{M}$ in basis ζ. We get $\mathcal{M} = \mathcal{M}_0 + \mathcal{M}_1\zeta + \cdots + \mathcal{M}_{k-1}\zeta^{k-1}$, where each matrix $\mathcal{M}_i$, with dimension approximately N/k, mostly contains coefficients equal to $\{-1, 0, 1\}$, with an average count of non-zero coefficients per row around λ/k. Afterwards, each matrix-vector multiplication $\mathcal{M}v$ in the Wiedemann algorithm can be instead accomplished by k matrix-vector multiplications with the matrices $\mathcal{M}_i$, and $k \cdot N/k$ multiplication with k-roots of unity in $\mathbb{Z}/\ell\mathbb{Z}$:

$$\mathcal{M}v = \sum_{i=0}^{k-1} \zeta^i \left(\mathcal{M}_i v\right).$$

Therefore, the number of arithmetic operations needed to perform a matrix-vector multiplication this way is $k \cdot \lambda/k \cdot (N/k) = \lambda \cdot N/k$ addition in $\mathbb{Z}/\ell\mathbb{Z}$ and $k \cdot N/k$ multiplications with k-roots of unity in $\mathbb{Z}/\ell\mathbb{Z}$. Counted in number of arithmetic operations, the cost of a matrix-vector multiplication comes down to approximately $(\lambda + k) \cdot N/k$. Overall, multiplying the cost of a matrix-vector multiplication by the matrix dimension we get the cost of the linear algebra using order k TNFS automorphisms, that is $(\lambda + k)(N/k)^2$. This is to be compared with the cost of the linear algebra if the automorphisms are not used, which is λN^2. In conclusion, we expect an approximate performance improvement by a factor of

$$\frac{\lambda}{\lambda + k} \cdot k^2. \tag{4}$$

Since the order k ($k = 6, 12$ in our applications) is small compared to λ (for instance $\lambda = 200$ in a record-size computation), we approximate the acceleration factor to k^2.

4.3 Literature on the use of Galois automorphisms to accelerate the linear algebra step

In this section we examine constructions from the literature in which Condition 1 is satisfied. All these constructions work only with order 2 TNFS automorphisms.

Vanishing virtual logarithm for order two automorphism: CM fields A *complex multiplication field* (CM field) is a number field that is a totally imaginary and that has a totally real subfield of index 2.

Let $\mathcal{K}$ one of the two middle number fields in the TNFS diagram with a TNFS automorphism σ of order k—here we abusively write σ for the component defined over $\mathcal{K}$. Suppose that $\mathcal{K}$ is CM, and further, suppose that the totally real subfield of $\mathcal{K}$ is isomorphic to $\tilde{\mathcal{K}} := \mathcal{K}^{\sigma^{k/2}}$. We refer to such a field by the term *CM TNFS-compatible with* σ. We emphasize the importance of the last condition as the only useful subfields in this work are the ones related to the automorphism—those fixed point-wise by a power of the automorphism.

Proposition 3. *Let $\mathcal{K}$ a CM TNFS-compatible field with a TNFS automorphism σ of order k. Denote $\tilde{\mathcal{K}} := \mathcal{K}^{\sigma^{m/2}}$ its real subfield of index 2. Then, the index $v := [\mathcal{O}_{\mathcal{K}}^{\times} : \mathcal{O}_{\tilde{\mathcal{K}}}^{\times}]$ is finite and if v is coprime to ℓ we have*

$$\forall u \in \mathcal{O}_{\mathcal{K}}^{\times}/(\mathcal{O}_{\mathcal{K}}^{\times})^{\ell}, \quad \mathrm{vlog}(u) = 0.$$

Note that since ℓ is very large, the index v will be coprime with ℓ with very large probability.

Proof. The proof is presented in Appendix A.2.

The above proposition and Proposition 2 imply that Condition 1 is satisfied, i.e., the virtual logarithm map vanishes on the *orbits* of the prime ideals. In conclusion, if both number fields $\mathcal{K}_1$ and $\mathcal{K}_2$ are CM TNFS-compatible with a TNFS automorphism (σ_1, σ_2) of order k, then the automorphism can be used to accelerate the linear algebra step by a factor k^2. In fact, as the virtual logarithm of units are all zero, the Schirokauer map is not needed in this setup and the corresponding columns in the matrix can be removed. Nevertheless, requiring such constructions is very restrictive and the only known methods to do so are with order 2 automorphisms as we explain next.

Construction of CM fields. In [3], the authors deal with finite fields of degree 4 and 6. For theses degrees, the authors provide modifications to the polynomial selection methods to construct the two number fields $\mathcal{K}_1$ and $\mathcal{K}_2$ to be CM and with a TNFS automorphism of order 2. The work of [44] generalizes this work to any even degree finite field, thus constructs CM fields on both sides with an automorphism of order 2. These constructions allow to accelerate the linear algebra by approximately a factor 4. However, to our knowledge, there are no known constructions for double sided CM fields with an automorphism of order larger than 2.

Partial vanishing over the units. Additionally to the above cited works, in a non published work (slides, How to get rid of units [2]), Barbulescu proposes other diagram constructions in which the virtual logarithm map vanishes on not all but a fraction of the units. The examples provided consist in number fields $\mathcal{K}$ with automorphisms σ of orders $2, 3, 4$, and 6, in which the subfield $\mathcal{K}^{\sigma}$ forces a part of the units in $\mathcal{K}$ to have a zero virtual logarithm.

Our work is an extension of this idea. We not only consider the field $\mathcal{K}^{\sigma}$, but also the other subfields related to the automorphism $\mathcal{K}^{\sigma^2} \cdots$ together with a new adequate Schirokauer map.

Vanishing Schirokauer map for order two automorphism The other alternative to guarantee that Condition 1 is verified is to construct a Schirokauer map that vanishes on the field elements fixed by the automorphism. Indeed, the

[2] `https://www.lix.polytechnique.fr/~guillevic/catrel-workshop/Razvan_Barbulescu_CATRELworkshop.pdf`

right term in the equation of Proposition 2 would be zero. The challenge lies in the construction of a Schirokauer map with this additional property. In the 521-bit record [14] on $\mathbb{F}_{p^6}$, the authors manage to construct such a Schirokauer map with an order 2 TNFS-automorphism σ. Let us examine this construction.

The subfield $\mathcal{K}^\sigma$ has index two, therefore, let $\omega \in \mathcal{K}$ such that $\mathcal{K} = \mathcal{K}^\sigma(\omega)$. For $\gamma \in \Gamma/\Gamma^\ell$, compute first $\mathbf{A}(\gamma)$, where $\mathbf{A}$ is defined in (1). Then, it decomposes as $\mathbf{A}(\gamma) = \gamma_0 + \gamma_1\omega \bmod \ell\mathcal{O}$ with γ_0 and γ_1 having polynomial representation over $\mathbb{F}_\ell$ of degree $m/2-1$, where m is the absolute degree of $\mathcal{K}$. The Schirokauer map Λ on γ is defined by taking r independent integer linear combinations of the coefficients of γ_1. This construction is possible if the unit rank r is smaller or equal to the number of coefficients of γ_1 which is $m/2$. This Schirokauer map vanishes on the elements fixed by σ. Indeed, If γ belongs to $\mathcal{K}^\sigma$, then so does any lift of $\mathbf{A}(\gamma)$, and hence γ_1 is zero. Therefore, $\Lambda(\gamma) = 0$. The authors provide two such constructions on two instances, the first on a degree 6 finite field, and the second on a degree 12 finite field. This construction is however specific to degree 2 automorphisms which provides a factor 4 acceleration in the linear algebra step. If one tries to generalize the construction to an order k automorphism, this would require the unit rank r to be smaller or equal to m/k, which becomes too restrictive. Indeed, Dirichlet's theorem implies that $r \geq m/2+1$. Consequently, if $k \geq 4$ or ($k = 3$ and $m > 6$), the condition $r \leq m/k$ cannot be fulfilled.

5 New construction: Galois Schirokauer map

Given a TNFS automorphism σ of *arbitrary* order k, we propose a new Schirokauer map that vanishes on the field elements fixed by σ. In fact, our Schirokauer map vanishes on the field elements that are fixed by σ^s where s is any proper divisor of k (including 1). This comes at the expense of *reducing* the rank of the Schirokauer map. We call such a Schirokauer map a Galois Schirokauer map. Let $\mathcal{K}$ one of the two middle number fields in Diagram 3 together with σ the corresponding component of an order k TNFS automorphism. Recall the set Γ associated to $\mathcal{K}$ from Section 2.1, and ℓ a prime divisor of $\Phi_n(p)$.

Definition 4 (Galois Schirokauer map (GSM)). *A Galois Schirokauer map (GSM) on side $\mathcal{K}$ is linear map $\Lambda : \Gamma/\Gamma^\ell \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^w$ for some integer w, such that $\Lambda(\phi) = 0$ whenever there exists s a proper divisor of k with $\sigma^s(\phi) = \phi$. The integer w is referred to as Λ's dimension.*

The dimension of a GSM is smaller than the unit rank of the corresponding number field (as opposed to the usual construction in Definition 1). Nevertheless, we prove that the property of vanishing on the subfields related to the powers of σ is enough compensation in many cases. Specifically, Galois Shirokauer maps allow the use of order 6 and 12 automorphisms in *any* finite field of extension degree 6 and 12 respectively. This allows to accelerate the linear algebra step by approximately a factor 36 for the degree 6 order and approximately a factor 144 for the degree 12 order. We underline that degree 6 and 12 finite fields are widely deployed in pairing-based cryptography [10, 15, 21].

Construction. Denote m the absolute degree of $\mathcal{K}$. Then k divides m, and let $\omega := m/k$. Moreover, let d be a divisor of k that will be determined later. First, we need a $\mathbb{Q}$-*Galois-compatible-basis* of $\mathcal{K}$. Consider $\alpha_0, \ldots, \alpha_{\omega-1} \in \mathcal{K}^\sigma$ and $y \in \mathcal{K}$ such that $\{a_i y^{\sigma^j}\}_{0 \le i \le \omega-1,\ 0 \le j \le k-1}$ is a $\mathbb{Q}$-basis of $\mathcal{K}$. Second, recall that $\zeta \in \mathbb{F}_\ell$ denotes the k-th primitive root of unity such that the Frobenius of the finite field related to σ is $\overline{\sigma} : x \mapsto x^\zeta$. Then the GSM is defined as follows.

Definition 5 (Construction of GSM). *For $\gamma \in \Gamma/\Gamma^\ell$, the new Schirokauer map $\Lambda_d : \Gamma/\Gamma^\ell \to (\mathbb{Z}/\ell\mathbb{Z})^{d\cdot\omega}$ on γ is defined by the following procedure.*

- *First, compute the image of γ by $\mathbf{A}$ defined in* (1).
- *Second, decompose $\mathbf{A}(\gamma)$ in the above basis as*

$$\mathbf{A}(\gamma) \equiv \sum_{i=0}^{\omega-1} \sum_{j=0}^{k-1} \tilde{\gamma}_{i,j}\ a_i y^{\sigma^j} \mod \ell\mathcal{O},$$

  where for $0 \le i \le \omega-1$ and $0 \le j \le k-1$, the scalar $\tilde{\gamma}_{i,j}$ belongs to $\mathbb{F}_\ell$.
- *Third, Λ_d is defined on γ in matrix form by:*

$$\Lambda_d : \begin{cases} \Gamma/\Gamma^\ell \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^{d\cdot\omega} \\ \gamma \quad \longmapsto & \begin{pmatrix} \sum\limits_{\substack{j=0 \\ j\equiv 0[d]}}^{k-1} \tilde{\gamma}_{0,j}\ \zeta^j & \cdots & \sum\limits_{\substack{j=0 \\ j\equiv 0[d]}}^{k-1} \tilde{\gamma}_{\omega-1,j}\ \zeta^j \\ \vdots & \cdots & \vdots \\ \sum\limits_{\substack{j=0 \\ j\equiv d-1[d]}}^{k-1} \tilde{\gamma}_{0,j}\ \zeta^j & \cdots & \sum\limits_{\substack{j=0 \\ j\equiv d-1[d]}}^{k-1} \tilde{\gamma}_{\omega-1,j}\ \zeta^j \end{pmatrix} \end{cases}.$$

The application Λ_d is a linear map. However, not any divisor d of k is convenient. The divisor d must be selected to guarantee that Λ_d is GSM, i.e., vanishes on the elements of $\mathcal{K}$ that are fixed by the automorphism σ or its powers. The following lemma announces the behavior of Λ_d with respect to the automorphism.

Lemma 2. *Let Λ_d from Definition 5. Then, $\forall \gamma \in \Gamma/\Gamma^\ell$, $\quad \Lambda_d(\gamma^\sigma) = \zeta \mathbf{J}_d \Lambda_d(\gamma)$, where $\mathbf{J}_d$ is the following $d \times d$ circular matrix,*

$$\mathbf{J}_d = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ 1 & & & 0 \end{pmatrix}$$

Proof. Since the automorphism σ fixes $\ell\mathcal{O}$, it is well defined on $\mathcal{O}/\ell\mathcal{O}$, and in particular on the image of $\mathbf{A}$. We abusively still refer to it as σ. First, since $\mathbf{A}(\gamma)$ is a polynomial expression in γ, then $\mathbf{A}(\gamma^\sigma) \equiv \mathbf{A}(\gamma)^\sigma \mod \ell\mathcal{O}$. Second, $\mathbf{A}(\gamma)^\sigma$ decomposes as:

$$\mathbf{A}(\gamma)^\sigma \equiv \sum_{i=0}^{\omega-1} \sum_{j=0}^{k-1} \tilde{\gamma}_{i,j}\ y^{\sigma^{j+1}} \equiv \sum_{i=0}^{\omega-1} \sum_{j=1}^{k} \tilde{\gamma}_{i,j-1}\ y^{\sigma^j} \mod \ell\mathcal{O},$$

Third, we have,

$$\begin{aligned}\Lambda_d(\gamma^\sigma) &= \zeta \begin{pmatrix} \sum_{\substack{j=0\\ j\equiv 0[d]}}^{k-1} \tilde{\gamma}_{0,j-1}\,\zeta^{j-1} & \cdots & \sum_{\substack{j=0\\ j\equiv 0[d]}}^{k-1} \tilde{\gamma}_{\omega-1,j-1}\,\zeta^{j-1} \\ \vdots & \cdots & \vdots \\ \sum_{\substack{j=0\\ j\equiv d-1[d]}}^{k-1} \tilde{\gamma}_{0,j-1}\,\zeta^{j-1} & \cdots & \sum_{\substack{j=0\\ j\equiv d-1[d]}}^{k-1} \tilde{\gamma}_{\omega-1,j-1}\,\zeta^{j-1} \end{pmatrix} \\ &= \zeta \mathbf{J}_d \Lambda_d(\gamma).\end{aligned}$$

From the lemma we deduce the following corollary that provides the largest integer d such that Λ_d still enjoys the desired property of vanishing over elements fixed by σ or its powers.

Corollary 2. *Define d as $d := \prod_{p,\mathrm{val}_k(p)>0} p^{\mathrm{val}_p(k)-1}$. Then, Λ_d from Definition 5 is GSM.*

Proof. Let e denote a proper divisor of k and γ an element fixed by σ^e. From Lemma 2, we have $\Lambda_d(\gamma) = \Lambda_d\left(\gamma^{\sigma^e}\right) = \zeta^e \mathbf{J}_d^e \Lambda_d(\gamma)$. Thus, $(\zeta^e \mathbf{J}_d^e - \mathbf{I}_d)\,\Lambda_d(\gamma) = 0$. It is sufficient to prove that $\zeta^e \mathbf{J}_d^e - \mathbf{I}_d$ is invertible. Its determinant is equal to $(-1)^d \zeta^{ed} \chi_{J_d^e}(\zeta^{-e})$, where $\chi_{J_d^e}$ is the characteristic polynomial of J_d^e. Let us compute it. The eigenvalues of J_d^e are $\{\zeta^{i\cdot e\cdot k/d}\}_{i=0}^{d-1}$, therefore we have:

$$\begin{aligned}\chi_{J_d^e}(X) &= \prod_{i=0}^{d-1} \left(X - \zeta^{i\cdot e\cdot k/d}\right) \\ &= \left(\prod_{i=0}^{\frac{d}{\gcd(e,d)}-1} \left(X - \zeta^{i\cdot e\cdot k/d}\right)\right)^{\gcd(e,d)} \\ &= \left(X^{\frac{d}{\gcd(e,d)}} - 1\right)^{\gcd(e,d)},\end{aligned}$$

where the second equality comes from the fact that the smallest integer i such that $\zeta^{i\cdot e\cdot k/d}$ equals 1 is the smallest i such that ie/d is an integer which is equal to $d/\gcd(e,d)$. Therefore, $\zeta^e \mathbf{J}_d^e - \mathbf{I}_d$ is invertible if and only if $\zeta^{-ed/\gcd(ed)} \neq 1$, which is equivalent to $k \nmid \mathrm{lcm}(e,d)$. This last condition is fulfilled. On the one hand, recall that e is a proper divisor of k, hence, there exists a prime number p such that $0 \leq \mathrm{val}_p(e) < \mathrm{val}_p(k)$. On the other hand, by construction of d we have $\mathrm{val}_p(d) < \mathrm{val}_p(k)$. Therefore, $\mathrm{val}_p(\mathrm{lcm}(e,d)) < \mathrm{val}_p(k)$, and thereby, $k \nmid \mathrm{lcm}(e,d)$.

It is noteworthy that our choice of d is the largest possible such that Λ_d vanishes on the elements fixed by σ or its powers, i.e, such that Λ_d is GSM. If the order k is square-free (equal to 6 for instance), then the largest d stated by Corollary 2 is 1. However, if one considers an order k that is *not square-free* (12 for instance), then the corresponding d is strictly greater than 1 (equal to 2 with $k = 12$) and the above construction provides a Schirokauer map Λ_d of dimension $d \cdot m/k$, where $d = \prod_{p,\mathrm{val}_k(p)>0} p^{\mathrm{val}_p(k)-1}$.

Example 1. Consider a finite field of degree 6 (i.e, $n = 6$) and a corresponding TNFS diagram constructed with the Conjugation polynomial selection providing the two middle number fields $(\mathcal{K}_1, \mathcal{K}_2)$ of absolute degrees $(m_1 = 12, m_2 = 6)$. Denote Γ_1, Γ_2 the corresponding sets defined in Section 2.1. Suppose the existence of a TNFS automorphism (σ_1, σ_2) of order 6 (hence $k = 6$). Let us examine the GSM construction $(\Lambda_{d,1}, \Lambda_{d,2})$ on $(\mathcal{K}_1, \mathcal{K}_2)$.

- **GSM on side $\mathcal{K}_2$.** Since the automorphism has order 6, then by Corollary 2 the integer d is set to 1. Further, since the absolute degree of $\mathcal{K}_2$ is 6, then the dimension of the GSM $\Lambda_{1,2}$ is $d \cdot m_2/k = 1$. Concretely, given $\mathbb{Q}$-basis of $\mathcal{K}_2$ that expresses as $\{y, y^{\sigma_2}, \ldots, y^{\sigma_2^5}\}$, with $y \in \mathcal{K}_2$, the image of $\gamma \in \Gamma_2/\Gamma_2^\ell$ is computed as follows. The image under $\mathbf{A}$ is decomposed as $\mathbf{A}(\gamma) \equiv \sum_{j=0}^{5} \tilde{\gamma}_j y^{\sigma_2^j} \mod \ell\mathcal{O}$, and $\Lambda_{1,2}(\gamma)$ is equal to $\sum_{j=0}^{5} \tilde{\gamma}_j \, \zeta^j$, which belongs to $\mathbb{Z}/\ell\mathbb{Z}$. Moreover, we have $\Lambda_{1,2}(\gamma^{\sigma_2}) = \zeta\Lambda_{1,2}(\gamma)$.
- **GSM on side $\mathcal{K}_1$.** The integer d that only depends on the automorphism's order is still set to 1. The absolute degree of $\mathcal{K}_1$ is 12, thus the dimension of the GSM $\Lambda_{1,1}$ on $\mathcal{K}_1$ is $d \cdot m_1/k = 2$. Concretely, given $\mathbb{Q}$-basis of $\mathcal{K}_1$ that expresses as $\{y, y^{\sigma_1}, \ldots, y^{\sigma_1^5}, ay, ay^{\sigma_1}, \ldots, ay^{\sigma_1^5}\}$, with $y \in \mathcal{K}_1$ and $a \in \mathcal{K}_1^{\sigma_1}$, the image of $\gamma \in \Gamma_1/\Gamma_1^\ell$ is computed as follows. $\mathbf{A}$ is decomposed as $\mathbf{A}(\gamma) \equiv \sum_{j=0}^{5} \tilde{\gamma}_{0,j} y^{\sigma_1^j} + \sum_{j=0}^{5} \tilde{\gamma}_{1,j} a y^{\sigma_1^j} \mod \ell\mathcal{O}$. Then we have

$$\Lambda_{1,1}(\gamma) = \left(\sum_{j=0}^{5} \tilde{\gamma}_{0,j} \, \zeta^j, \; \sum_{j=0}^{5} \tilde{\gamma}_{1,j} \, \zeta^j \right) \in (\mathbb{Z}/\ell\mathbb{Z})^2.$$

  Moreover, we have $\Lambda_{1,1}(\gamma^{\sigma_1}) = \zeta\Lambda_{1,1}(\gamma)$.

5.1 Computing virtual logarithms with Galois Schirokauer maps

A Galois Schirokauer map differs from the usual construction presented in Section 2.1 by several aspects. First, its dimension is usually smaller than the unit rank. Second, its definition depends on the automorphism so that it enjoys the property of vanishing on the field elements that are fixed by the automorphism. When the Schirokauer map's dimension is *large enough* (see conditions of Proposition 4 at the end of the section), the second property ensures that Condition 1 is satisfied (see Proposition 2), allowing thus the use of the automorphism to accelerate the linear algebra step by a approximately a factor quadratic in the automorphism's order. Third, a GSM not only vanishes on the elements that are fixed by σ, but it also vanishes on the elements that are fixed by any of the automorphisms σ^s where s is a proper divisor of k. We will show how this last property compensate the decrease in the dimension (compared to the usual construction) when $k = 6, 12$, thus ensuring that its dimension is *large enough*.

Condition to compute virtual logarithms with GSM. Let Λ_d as in Definition 5. Recall that the dimension of Λ_d is $\omega := d \cdot m/k$, where k is the order of the

automorphism, d is a divisor of k provided by Corollary 2, and m is the absolute degree of the number field $\mathcal{K}$. If $\omega \geq r$, then under the Assumption of Λ_d having maximal rank on the units equal to r, it can be used to compute virtual logarithms and to accelerate the linear algebra.

Assume now $\omega < r$. Suppose the existence of a system of fundamental units defined modulo ℓ-th powers, $\{u_1, \ldots, u_r\}$, such that enough of them belong to subfields fixed point-wise by the automorphism or its powers. More precisely, assume that at least $r - \omega$ of them are fixed by a power of σ. Rearranging them, this is equivalent to assuming that for all $\omega + 1 \leq i \leq r$,

$$\exists s | k, \ s \neq k, \quad \sigma^s(u_i) = u_i.$$

Then by Corollary 1 and Corollary 2, we have for all $\omega + 1 \leq i \leq r$,

$$\mathrm{vlog}(u_i) = 0 \quad \text{and} \quad \Lambda_d(u_i) = 0.$$

On the one hand, the vanishing of the virtual logarithms tells us that in order to compute virtual logarithms, it is sufficient to construct a Schirokauer map that has rank ω on $\mathrm{span}(u_1, \ldots, u_\omega)$ (see (3)). On the other hand, the vanishing of Λ_d tells us that $\mathrm{rank}(\Lambda_d(\mathrm{span}(u_1, \ldots, u_r)) = \mathrm{rank}(\Lambda_d(\mathrm{span}(u_1, \ldots, u_\omega))$. Consequently, the assumption that Λ_d has maximal rank on the units equal to its dimension stated in Assumption 1 implies the desired property of having maximal rank on $\mathrm{span}(u_1, \ldots, u_\omega)$ equal to ω. The following proposition recapitulates the condition needed to accelerate the linear algebra step with the new GSM.

Proposition 4 (Conditions to accelerate the linear algebra step with GSM). *Let $\mathcal{K}_1$ and $\mathcal{K}_2$ of absolute degrees m_1 and m_2 be the two middle number fields in a TNFS diagram with a TNFS automorphism (σ_1, σ_2) of order k. Let $\omega_i = d \cdot m_i/k$, where $d = \prod_{p, \mathrm{val}_k(p)>0} p^{\mathrm{val}_p(k)-1}$. Consider $(\Lambda_{d,1}, \Lambda_{d,2})$ the GSM from Definition 5 over $(\mathcal{K}_1, \mathcal{K}_2)$ with dimension equal to (ω_1, ω_2).*

Assume Assumption 1, i.e., that the rank of $(\Lambda_{d,1}, \Lambda_{d,2})$ on the units is (ω_1, ω_2). Suppose further that for $i = 1, 2$, there exists a system of fundamental units in $\mathcal{K}_i$ in which at most ω_i units do not belong to $\cup_{s|k, s\neq k} \mathcal{K}_i^{\sigma_i^s}$.

Then, $(\Lambda_{d,1}, \Lambda_{d,2})$ can be used to compute a virtual logarithm map that verifies Condition 1. Consequently, this accelerates the linear algebra step by a factor approximately equal to k^2.

6 Application: Acceleration of the linear algebra step with order 6 and 12 TNFS automorphisms

Let $\mathbb{F}_{p^6}$ (resp. $\mathbb{F}_{p^{12}}$) any finite field of characteristic p and extension degree 6 (resp. 12). We show in this section how to construct a TNFS diagram on $\mathbb{F}_{p^6}$ (resp. $\mathbb{F}_{p^{12}}$) using the *Conjugation* polynomial selection method such that the following two properties are verified. On the one hand, the diagram enjoys an order 6 (resp. 12) TNFS automorphism, and on the other hand, the new GSM from Definition 5 has dimension large enough for the computation of virtual

logarithms (i.e., the conditions of Proposition 4 are fulfilled). As a consequence, the automorphism can be used to accelerate the relation collection by an approximate factor of 6 (resp. 12) and the linear algebra step by an approximate factor of 36 (resp. 144).

6.1 Construction of order 6 and 12 TNFS automorphisms

The extension degree n is 6 or 12. It decomposes as $n = \eta\kappa$ with η and κ coprime and non-trivial (hence two possible setups for $n = 6$, and two setups for $n = 12$). In all these setups, the Conjugation method presented in §2 with the choices of Table 4 provides a TNFS diagram with two automorphisms $\sigma_1 \in \mathrm{Aut}(\mathcal{K}_1)$ and $\sigma_2 \in \mathrm{Aut}(\mathcal{K}_2)$, both of order n. The following proposition states that they constitute a TNFS automorphism as in Definition 3.

Proposition 5. *For each of the setups $(\eta = 3, \kappa = 2)$ or $(\eta = 2, \kappa = 3)$ for $n = 6$, or $(\eta = 3, \kappa = 4)$ or $(\eta = 4, \kappa = 3)$ for $n = 12$, let h, f_1 and f_2 three polynomials selected by the Conjugation method, where h of degree η has cyclic Galois group and, f_1 and f_2 of respective degrees 2κ and κ are selected with Table 4. Additionally, suppose that p does not divide their discriminant. Denote $\sigma_1 \in \mathrm{Aut}(\mathcal{K}_1)$ and $\sigma_2 \in \mathrm{Aut}(\mathcal{K}_2)$ the resulting order n automorphisms. Then they each fix a prime ideal of degree n above p, that is, (σ_1, σ_2) is a TNFS automorphism.*

Proof. Denote σ_h, σ_{f_1} and σ_{f_2} the automorphisms corresponding to the polynomials of respective orders η, κ, and κ. Recall that since η and κ are coprime, the automorphisms σ_1 and σ_2 are defined by the joint action of σ_h and σ_{f_1}, and σ_h and σ_{f_2}. To prove the proposition, it is sufficient to prove that σ_h fixes a prime ideal of degree η above p, and σ_{f_1} and σ_{f_2} each fixes a prime ideal of degree κ above p.

Denote $\mathcal{O}_h$, $\mathcal{O}_{f_1}$, and $\mathcal{O}_{f_2}$ the ring of integers of $\mathcal{K}_h$, $\mathcal{K}_{f_1}$ and $\mathcal{K}_{f_2}$. By construction, h is irreducible modulo p, which means that $p\mathcal{O}_h$ is irreducible of degree η. Therefore, $p\mathcal{O}_h$ is fixed by σ_h since the conjugate of a prime ideal above p is a prime ideal above p. The same scenario occurs in $\mathcal{K}_{f_2}$, the automorphism σ_{f_2} fixes $p\mathcal{O}_{f_2}$ which is an irreducible prime ideal of degree κ.

It remains to prove that σ_{f_1} fixes a prime ideal of degree κ above p. We know that $p\mathcal{O}_{f_1}$ is not prime. In fact, by construction f_1 has an irreducible factor of degree κ modulo p, hence, $p\mathcal{O}_{f_1}$ splits into a degree κ prime ideal $\mathfrak{p}$ times a remaining part of total degree κ. If the remaining part is not a prime ideal of degree κ, then $\sigma(\mathfrak{p}) = \mathfrak{p}$ since the conjugate of a prime ideal above p is a prime ideal above p with the *same* residual degree. Hence, we restrict to the case $p\mathcal{O}_{f_1} = \mathfrak{pq}$, with $\mathfrak{p}$ and $\mathfrak{q}$ are both irreducible prime ideals of degree κ.

A root of the polynomial μ (from the Conjugation method in §2) in $\mathcal{K}_{f_1} := \mathbb{Q}(\alpha_1)$ is $-g_0(\alpha_1)/g_1(\alpha_1)$ which is stable under the action of σ_1 for all the choices of (g_0, g_1) in Table 4. Therefore, the number field $\mathcal{K}_\mu := \mathbb{Q}[x]/(\mu)$ is isomorphic to $\mathcal{K}_{f_1}^{\sigma_{f_1}}$, and σ_{f_1} is a $\mathcal{K}_\mu$-automorphism of $\mathcal{K}_{f_1}$.

We conclude the proof by looking at the decomposition pattern of the characteristic p along the tower $\mathbb{Q} \subset \mathcal{K}_\mu \subset \mathcal{K}_{f_1}$. Denote $\mathcal{O}_\mu$ the ring of integer of $\mathcal{K}_\mu$.

By construction, μ has two roots modulo p, which means that $p\mathcal{O}_\mu$ decomposes as a product of two prime ideals $\mathfrak{p}_a$ and $\mathfrak{p}_b$, each of residual degree 1. Further, recall that $p\mathcal{O}_{f_1} = \mathfrak{p}\mathfrak{q}$, therefore, after reordering the ideals, we have $\mathfrak{p}_a\mathcal{O}_{f_1} = \mathfrak{p}$ and $\mathfrak{p}_b\mathcal{O}_{f_1} = \mathfrak{q}$. Since σ_{f_1} is a $\mathcal{K}_\mu$-automorphism of $\mathcal{K}_{f_1}$, we must have $\sigma_{f_1}(\mathfrak{p})$ a prime ideal above $\mathfrak{p}_a$, thus equal to $\mathfrak{p}$.

It is noteworthy that the reliance on the choice of (g_0, g_1) is not required if κ is odd. Indeed, we have $\sigma_{f_1}(\mathfrak{p}) = \mathfrak{p}$ as the alternative $\sigma_{f_1}(\mathfrak{p}) = \mathfrak{q}$ would imply that $\sigma_{f_1}^{\kappa}(\mathfrak{p}) = \mathfrak{q}$. This contradicts the fact that the order of σ_{f_1} is κ.

6.2 Large Enough Dimension for the Galois Schirokauer Map

Once the TNFS diagram is constructed with an order n TNFS automorphism (σ_1, σ_2) as described in Proposition 5 where $n = 6$ or $n = 12$, Construction 5 defines a GSM $(\Lambda_{d_n,1}, \Lambda_{d_n,2})$ equal to

- $(\Lambda_{1,1}, \Lambda_{1,2})$ of dimension $(2, 1)$ if $n = 6$,
- $(\Lambda_{2,1}, \Lambda_{2,2})$ of dimension $(4, 2)$ if $n = 12$.

Indeed, this is a consequence of Corollary 2 since the absolute degrees of $(\mathcal{K}_1, \mathcal{K}_2)$ are $(2n, n)$. This construction allows the use of the order n TNFS-automorphism to accelerate the linear algebra step with a factor n^2 if the following conditions from Proposition 4 are satisfied.

- **if** $n = 6$**:**
  - There exists a system of fundamental units in $\mathcal{K}_1$ in which at most 2 units do not belong to $\mathcal{K}_1^{\sigma_1^2} \cup \mathcal{K}_1^{\sigma_1^3}$.
  - There exists a system of fundamental units in $\mathcal{K}_2$ in which at most 1 unit does not belong to $\mathcal{K}_2^{\sigma_2^2} \cup \mathcal{K}_2^{\sigma_2^3}$.
- **if** $n = 12$**:**
  - There exists a system of fundamental units in $\mathcal{K}_1$ in which at most 4 units do not belong to $\mathcal{K}_1^{\sigma_1^4} \cup \mathcal{K}_1^{\sigma_1^6}$.
  - There exists a system of fundamental unit in $\mathcal{K}_2$ in which at most 2 units do not belong to $\mathcal{K}_2^{\sigma_2^4} \cup \mathcal{K}_2^{\sigma_2^6}$.

In Theorem 1, we provide restrictions on the number of real roots of the selected polynomials to ensure that the subfields related to the automorphisms have unit rank large enough, and thus that the above conditions are met. To this end, we need to assume the following Assumption.

Assumption 3 (Unit lift assumption) *Consider a TNFS diagram with $\mathcal{K}_1$ and $\mathcal{K}_2$ the two middle number fields with an order n TNFS automorphism (σ_1, σ_2) where $n = 6$ or $n = 12$. For a number field $\mathcal{K}$, let $r_{\mathcal{K}}$ denote its unit rank. Then for both $i = 1, 2$, there exists a system of fundamental units of $\mathcal{K}_i$ in which*

- $r_{\mathcal{K}_i^{\sigma_i^3}} + r_{\mathcal{K}_i^{\sigma_i^2}} - r_{\mathcal{K}_i^{\sigma_i}}$ *units belong to* $\mathcal{K}_i^{\sigma_i^3} \cup \mathcal{K}_i^{\sigma_i^2}$ *if* $n = 6$.

- $r_{\mathcal{K}_i^{\sigma_i^6}} + r_{\mathcal{K}_i^{\sigma_i^4}} - r_{\mathcal{K}_i^{\sigma_i^2}}$ *units belong to* $\mathcal{K}_i^{\sigma_i^6} \cup \mathcal{K}_i^{\sigma_i^4}$ *if* $n = 12$.

This assumption states that fundamental units in subfields lift into fundamental units in the field. Under this assumption, the conditions of Proposition 4 (restated above for the order 6 and 12) will be satisfied whenever for both $i = 1, 2$, the dimension of $\Lambda_{d_n,i}$ is greater or equal to

- $r_{\mathcal{K}_i} - (r_{\mathcal{K}_i^{\sigma_i^3}} + r_{\mathcal{K}_i^{\sigma_i^2}} - r_{\mathcal{K}_i^{\sigma_i}})$ if $n = 6$.
- $r_{\mathcal{K}_i} - (r_{\mathcal{K}_i^{\sigma_i^6}} + r_{\mathcal{K}_i^{\sigma_i^4}} - r_{\mathcal{K}_i^{\sigma_i^2}})$ if $n = 12$.

These quantities are (under the assumption) an upper bound on the dimension of the units that do not belong to $\ker(\Lambda_{d_n,i}) \cap \ker(\mathrm{vlog})$.

Unit rank of compositum. It will be useful in the subsequent to compute the unit rank of a compositum of two *linearly disjoint* number fields. Recall that two number fields $\mathbb{E}$ and $\mathbb{F}$ are said linearly disjoint over $\mathbb{Q}$ if every finite subset of $\mathbb{E}$ that is $\mathbb{Q}$-linearly independent is also $\mathbb{F}$-linearly independent in their compositum. In particular in our TNFS context, for $i = 1, 2$, the number fields $\mathcal{K}_h$ and $\mathcal{K}_{f_i}$ are linearly disjoint over $\mathbb{Q}$ since we have by construction $\deg_{\mathbb{Q}}(\mathcal{K}_i) = \deg_{\mathbb{Q}}(\mathcal{K}_h) \times \deg_{\mathbb{Q}}(\mathcal{K}_{f_i})$. Let r_h and r_{f_i} designate the number of real roots of h and f_i for $i = 1, 2$. Then, the unit rank $r_{\mathcal{K}_i}$ of $\mathcal{K}_i$ is equal to

$$r_{\mathcal{K}_i} = 1/2\,(\eta \deg(f_i) + r_h r_{f_i}) - 1. \tag{5}$$

Indeed, since the absolute degree of $\mathcal{K}_i$ is $\eta \times \deg(f_i)$, it is clear that the embeddings of $\mathcal{K}_i$ are $\{(e_h, e_{f_i}) | e_h$ embedding of $\mathcal{K}_h, e_{f_i}$ embedding of $\mathcal{K}_{f_i}\}$. Therefore, the number of real embeddings of $\mathcal{K}_i$ is $r_h \times r_{f_i}$ and formula (5) follows from Dirichlet's unit theorem.

The following theorem states the result about accelerating the linear algebra step for extension 6 and 12 finite fields.

Theorem 1. *Let $n = 6$ or $n = 12$. Let h, f_1 and f_2 constructed with the Conjugation polynomial selection with an order n TNFS automorphism (σ_1, σ_2) as described in Proposition 5, hence with the requirement that p does not divide their discriminant. Suppose further the following restrictions on the number of real roots of h, f_1 and f_2:*

1. ***If** η **is even**, then h has no real roots.*
2. ***If** η **is odd**, then f_1 and f_2 have no real roots.*

Table 5 recapitulates these restrictions. Then, under Assumption 3, the field $\mathcal{K}_1$ (resp. $\mathcal{K}_2$) admits a system of fundamental units with:

- *At most 2 (resp. 1) fundamental units that do not belong to $\mathcal{K}_1^{\sigma_1^2} \cup \mathcal{K}_1^{\sigma_1^3}$ (resp. $\mathcal{K}_2^{\sigma_2^2} \cup \mathcal{K}_2^{\sigma_2^3}$) if $n = 6$.*
- *At most 4 (resp. 2) fundamental units that do not belong to $\mathcal{K}_1^{\sigma_1^6} \cup \mathcal{K}_1^{\sigma_1^4}$ (resp. $\mathcal{K}_2^{\sigma_2^6} \cup \mathcal{K}_2^{\sigma_2^4}$) if $n = 12$.*

Consequently, the GSM of Definition 5 satisfy the conditions of Proposition 4, i.e., they accelerate the linear algebra step by a factor approximately equal to 36 *if* $n = 6$*, and* 144 *if* $n = 12$*.*

n	6		12	
Setup	$(\eta = 2, \kappa = 3)$	$(\eta = 3, \kappa = 2)$	$(\eta = 3, \kappa = 4)$	$(\eta = 4, \kappa = 3)$
Requirement: Polynomials with no real roots	h	f_1 and f_2	f_1 and f_2	h

Table 5: Requirements on the polynomials output by the Conjugation method so that the GSM of Definition 5 allows to use an order n TNFS automorphism to accelerate the linear algebra step.

Proof. The theorem heavily depends on the subfields trellis of the number fields $\mathcal{K}_1$ and $\mathcal{K}_2$. For this reason we must consider each setup. In particular, we prove the theorem separately when $n = 6$ and when $n = 12$.

The extension degree $n = 6$*.* Let us consider the two setups $\eta = 3$ and $\eta = 2$.

1. **The case** $\eta = 3$ **represented in Figure 6.** Suppose η is taken equal to 3. The polynomial h is chosen such that $\mathcal{K}_h$ is Galois. Therefore, $\mathcal{K}_h$ is totally real (since its degree is odd), and its unit rank is equal to 2. The rest of the proof for the case $\eta = 3$ is divided into the examination of the units in the two fields $\mathcal{K}_1$ and $\mathcal{K}_2$.
   - **Distribution of the units along the subfields of** $\mathcal{K}_2$**.** Since h has three real roots, then the unit rank of $\mathcal{K}_2$ is $r_{\mathcal{K}_2} = 2+3r_{f_2}/2$. The field $\mathcal{K}_2$ has two subfields related to the automorphism σ_2 which are $\mathcal{K}_2^{\sigma_2^2}$ that is isomorphic to $\mathcal{K}_{f_2}$, and $\mathcal{K}_2^{\sigma_2^3}$ that is isomorphic to $\mathcal{K}_h$. Their respective absolute degrees are 2 and 3. By Dirichlet's theorem, the sum of their unit ranks is $2+r_{f_2}/2$. Further, the subfield $\mathcal{K}^\sigma$ is isomorphic to $\mathbb{Q}$, hence its unit rank is 0. Under Assumption 3, if $2 + 3r_{f_2}/2 - (2 + r_{f_2}/2) \leq 1$, then there exists a system of fundamental units in $\mathcal{K}_2$ with at most 1 unit not in $\mathcal{K}_2^{\sigma_2^2} \cup \mathcal{K}_2^{\sigma_2^3}$. This is equivalent to asking for $r_{f_2} \leq 1$. Since f_2 has degree 2 and the number of real roots of f_2 is necessarily even, this is equivalent to requiring f_2 with no real roots.
   - **Distribution of the units along the subfields of** $\mathcal{K}_1$**.** The field $\mathcal{K}_1$ has unit rank $r_{\mathcal{K}_1} = 5 + 3r_{f_1}/2$. Further, its subfield $\mathcal{K}_1^{\sigma_1^2}$ is isomorphic to $\mathcal{K}_{f_1}$ which is of absolute degree 4 and has unit rank $r_{f_2}/2 + 1$. The subfield $\mathcal{K}_1^{\sigma_1^3}$ has unit rank larger or equal to 2 since it contains $\mathcal{K}_h$ which has unit rank 2 ($\mathcal{K}_h$ is fixed point-wise by σ_1). Further, since the absolute degree of $\mathcal{K}_1^{\sigma_1}$ that is 2 is coprime to the absolute degree of $\mathcal{K}_h$

that is 3, the field $\mathcal{K}_1^{\sigma_1}$ cannot be a subfield of $\mathcal{K}_h$. That is to say that $r_{\mathcal{K}_h} + r_{\mathcal{K}_1^{\sigma_1^2}} \leq r_{\mathcal{K}_1^{\sigma_1^3}} + r_{\mathcal{K}_1^{\sigma_1^2}} - r_{\mathcal{K}_1^{\sigma_1}}$. Therefore, if $r_{\mathcal{K}_1} - (r_{f_2}/2+3) \leq 2$, then $r_{\mathcal{K}_1} - (r_{\mathcal{K}_1^{\sigma_1^3}} + r_{\mathcal{K}_1^{\sigma_1^2}} - r_{\mathcal{K}_1^{\sigma_1}}) \leq 2$, and Assumption 3 implies the existence of a system of fundamental units of $\mathcal{K}_1$ with at most 2 fundamental units that do not belong to $\mathcal{K}_1^{\sigma_1^2} \cup \mathcal{K}_1^{\sigma_2^3}$. This is the case when $r_{f_1} = 0$.

2. **The case $\eta = 2$ represented in Figure 7** Here η is set to 2. The unit rank of $\mathcal{K}_h$ is equal to 0 since h has no real roots. The rest of the proof for the case $\eta = 2$ is divided into the examination of the unit distribution along the subfields of $\mathcal{K}_1$ and $\mathcal{K}_2$.
   - **Distribution of the units along the subfields of $\mathcal{K}_2$.** The polynomial f_2 has 3 real roots since it has odd degree 3 and an automorphism of order 3. Thus, by (5), the unit rank of $\mathcal{K}_2$ is $3r_h/2 + 2 = 2$. The sum of the unit ranks of $\mathcal{K}_2^{\sigma_2^2}$ which is isomorphic to $\mathcal{K}_h$ and $\mathcal{K}_2^{\sigma_2^3}$ which is isomorphic to $\mathcal{K}_{f_2}$ is $r_h/2 + 2 = 2$. Since $\mathcal{K}_2^{\sigma_2} \simeq \mathbb{Q}$, Assumption 3 implies the existence of a system of fundamental units of $\mathcal{K}_2$ that completely belongs to $\mathcal{K}_2^{\sigma_2^2} \cup \mathcal{K}_2^{\sigma_2^3}$.
   - **Distribution of the units along the subfields of $\mathcal{K}_1$.** Since h has no real roots, then by Equation (5), the unit rank of $\mathcal{K}_1$ is 5. Let us distinguish two cases whether the extension field $\mathcal{K}_1^{\sigma_1}$, which is of absolute degree 2, is totally real or totally imaginary. Suppose first that $\mathcal{K}_1^{\sigma_1}$ is totally real. The field $\mathcal{K}_1^{\sigma_1^3}$ which is isomorphic to $\mathcal{K}_{f_1}$ is a relative extension 3 field over $\mathcal{K}_1^{\sigma_1}$. Thus, $\mathcal{K}_1^{\sigma_1^3}$ cannot be totally complex. Its units rank can only take values equal to 3, 4, or 5 (not 2). In all three cases, we have under Assumption 3, a system of fundamental units of $\mathcal{K}_1$ with at most 2 units that do not belong to $\mathcal{K}_1^{\sigma_1^3} \subset \mathcal{K}_1^{\sigma_1^2} \cup \mathcal{K}_1^{\sigma_1^3}$. Suppose now that $\mathcal{K}_1^{\sigma_1}$ is totally imaginary. Then, the unit rank of $\mathcal{K}_1^{\sigma_1}$ is 0. On the one hand, $\mathcal{K}_1^{\sigma_1^3}$ has absolute degree 6, hence, its unit rank is at least 2. On the other hand, the field $\mathcal{K}_1^{\sigma_1^2}$ has absolute degree 4, hence, its unit rank is at least 1. Hence we count 3 independent units in $\mathcal{K}_1^{\sigma_1^2} \cup \mathcal{K}_1^{\sigma_1^3}$ and the result follows under Assumption 3.

The extension degree $n = 12$. Consider the two setups $\eta = 3$ and $\eta = 4$.

- **The case $\eta = 3$ represented in Figure 8.** The polynomial h has three real roots and the unit rank of $\mathcal{K}_h$ is 2. Let us examine the distribution of the units along the subfields of $\mathcal{K}_2$ and $\mathcal{K}_1$.
  - **Distribution of the units along the subfields of $\mathcal{K}_2$.** The unit rank of $\mathcal{K}_2$ is $5 + 3r_{f_1}/2$. We require f_2 to have no real roots, hence, $r_{\mathcal{K}_2} = 5$. Further, we count 2 for the unit rank of $\mathcal{K}_h$ which is isomorphic to a subfield of $\mathcal{K}_2^{\sigma_2^6}$, and 1 for the unit rank of $\mathcal{K}_{f_2} \simeq \mathcal{K}_2^{\sigma_2^4}$. Since the absolute degree of $\mathcal{K}_h$ that is 3 is coprime to the absolute degree of $\mathcal{K}_2^{\sigma_2^2}$ that is 2, we necessarily have $r_{\mathcal{K}_2^{\sigma_2^6}} + r_{\mathcal{K}_2^{\sigma_2^4}} - r_{\mathcal{K}_2^{\sigma_2^2}} \geq 3$. Therefore, there exists under

Assumption 3 a family of fundamental units of $\mathcal{K}_2$ in which at most 2 units do not belong to subfields related to σ_2.

- **Distribution of the units along the subfields of $\mathcal{K}_1$.** Let us now examine the field $\mathcal{K}_1$. We require f_1 to have no real roots. Hence, the unit rank of $\mathcal{K}_1$ is 11. On the one hand, the unit rank of $\mathcal{K}_1^{\sigma_1^4}$ which is isomorphic to $\mathcal{K}_{f_1}$ is 3. On the other hand, we shall count the unit ranks of $\mathcal{K}_1^{\sigma_1^6}$ and the intersection $\mathcal{K}_1^{\sigma_1^4} \cap \mathcal{K}_1^{\sigma_1^6} = \mathcal{K}_1^{\sigma_1^2}$.

  To this end, let g be a defining polynomial of $\mathcal{K}_1^{\sigma_1^2}$ over $\mathbb{Q}$, and denote r_g the number of its real roots. The polynomial g has degree 4, and the unit rank of $\mathcal{K}_1^{\sigma_1^2}$ is equal to $1 + r_g/2$. Further, $\mathcal{K}_1^{\sigma_1^6}$ is the compositum of $\mathcal{K}_1^{\sigma_1^2}$ and $\mathcal{K}_h$ which are of respective absolute degrees 4 and 3. Since the degrees are coprime, we deduce that the unit rank of $\mathcal{K}_1^{\sigma_1^6}$ is $5 + 3r_g/2$. Therefore, we have $r_{\mathcal{K}_1^{\sigma_1^6}} + r_{\mathcal{K}_1^{\sigma_1^4}} - r_{\mathcal{K}_1^{\sigma_1^2}} = 7 + r_g$. Since $r_g \geq 0$, and the unit rank of $\mathcal{K}_1$ is 11, Assumption 3 implies the existence of a system of fundamental units of $\mathcal{K}_1$ with at most 4 fundamental units that do not belong to subfields related to σ_1.

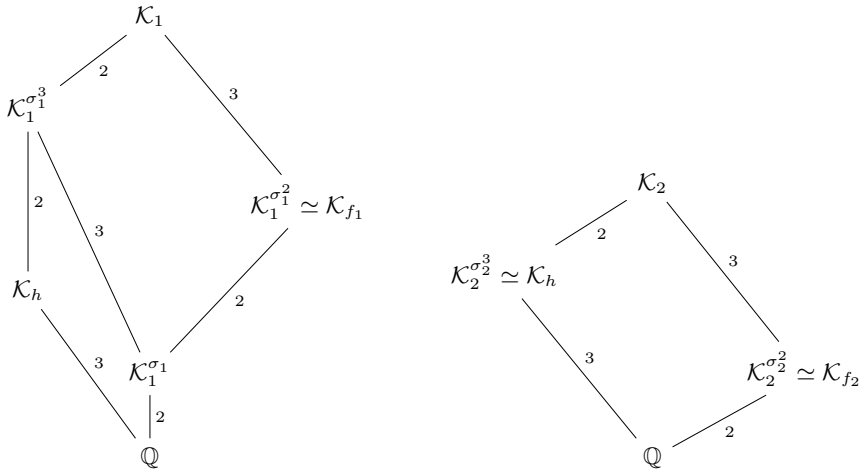
– **The case $\eta = 4$ represented in Figure 9.** We require the polynomial h to have no real roots. Therefore, the unit rank of $\mathcal{K}_h$ is 1. We continue the proof by examining the units in both number fields $\mathcal{K}_2$ and $\mathcal{K}_1$.

  - **Distribution of the units along the subfields of $\mathcal{K}_2$.** The unit rank of $\mathcal{K}_2$ is 5. Since f_2 has an automorphism of order 3, the unit rank of $\mathcal{K}_{f_2} \simeq \mathcal{K}_2^{\sigma_2^3}$ is 2. Additionally, we count 1 for the unit rank of $\mathcal{K}_h \simeq \mathcal{K}_2^{\sigma_2^4}$. Since these two subfields have coprime absolute degrees equal respectively to 3 and 4, we conclude under Assumption 3.
  - **Distribution of the units along the subfields of $\mathcal{K}_1$.** Now we consider the field $\mathcal{K}_1$. Since h has no real roots, the unit rank of $\mathcal{K}_1$ is 11. We want to prove that the quantity $\nu := r_{\mathcal{K}_1^{\sigma_1^6}} + r_{\mathcal{K}_1^{\sigma_1^4}} - r_{\mathcal{K}_1^{\sigma_1^2}}$ is greater or equal to $11 - 4 = 7$.

    Denote e the number of real embeddings of $\mathcal{K}_1^{\sigma_1^2}$. Hence, its unit rank is $1 + e/2$. Further, consider a polynomial U that defines $\mathcal{K}_1^{\sigma_1^6}$ over $\mathcal{K}_1^{\sigma_1^2}$, i.e, $\mathcal{K}_1^{\sigma_1^6} = \mathcal{K}_1^{\sigma_1^2}[X]/(U)$. The polynomial U can be taken with rational coefficients since its degree that is equal to 3 is coprime with the absolute degree of $\mathcal{K}_1^{\sigma_1^2}$ that is equal to 4. From the fact that the number of real roots of U is at least 1, we deduce by (5) that the unit rank of $\mathcal{K}_1^{\sigma_1^6}$ is at least $5 + e/2$. Moreover, since the absolute degree of $\mathcal{K}_1^{\sigma_1^4}$ is 8, its unit rank is at least 3. Overall, we get that $\nu \geq 5 + e/2 + 3 - (1 + e/2) = 7$. This concludes the proof provided Assumption 3.

In conclusion, it is sufficient to restrict the number of real roots of the selected polynomials as indicated in Table 5, which is practically easy, in order to ensure that the GSM construction from Definition 5 is sufficient to compute discrete

logarithms while using order 6 or 12 TNFS automorphisms to accelerate the linear algebra step. These restrictions allow to construct the number fields $\mathcal{K}_1$ and $\mathcal{K}_2$ with enough fundamental units that belong to subfields related to the automorphisms, and therefore, the few remaining units that do not vanish by both the GSM and the virtual logarithm can be controlled by the GSM.



(a) Lattice of σ_1-related subfields of $\mathcal{K}_1$ of absolute degree 12.

(b) Lattice of σ_2-related subfields of $\mathcal{K}_2$ of absolute degree 6.

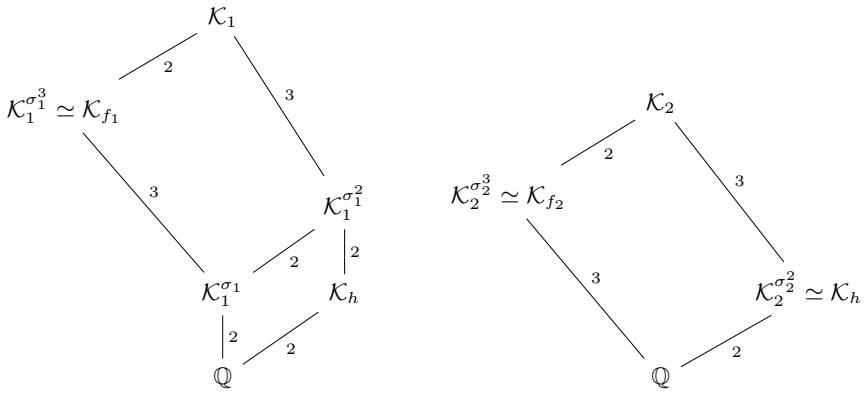
Fig. 6: Lattices of automorphism-related subfields with the setup $n = 6$ and $\eta = 3$. Each edge indicates a field extension and is labeled with the corresponding extension degree.

6.3 Application to other Automorphism Orders?

When applied on a degree n finite field with $n = \eta \times \kappa$, the Conjugation polynomial selection constructs a TNFS-diagram by selecting the polynomials h, f_1, and f_2 of respective degrees η, 2κ, and κ.

When n equals 6 or 12, we showed how to select the polynomials in order to have an order n TNFS automorphism. This allows the construction of a GSM as in Definition 5. Under the restrictions on the number of real roots of the polynomials presented in Table 5 and the Assumptions 1 and 3 we proved that these GSM allow the computation of a virtual logarithm map while accelerating the linear algebra step by approximately a factor n^2.

The natural continuation of this work is to extend the use of these Schirokauer maps to other composite orders. Provided a finite field of degree n, if we are



(a) Lattice of σ_1-related subfields of $\mathcal{K}_1$ of absolute degree 12.

(b) Lattice of σ_2-related subfields of $\mathcal{K}_2$ of absolute degree 6.

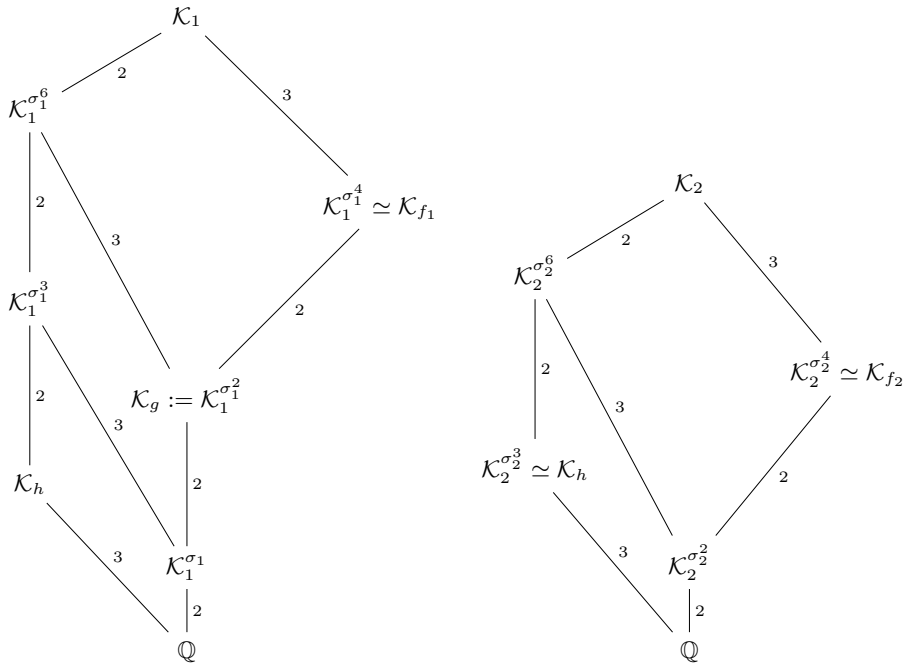
Fig. 7: Lattices of automorphism-related subfields with the setup $n = 6$ and $\eta = 2$. Each edge indicates a field extension and is labeled with the corresponding extension degree.

able to construct a TNFS automorphism of order n with say the Conjugation polynomial selection (hence the absolute degrees of the middle number fields are $2n$ and n), then we are able to define a GSM over the TNFS diagram. The dimensions of these GSM are provided by Corollary 2 and their values are exhibited in Table 10 for various values of n. Thereafter, if some restriction on the polynomials restrict enough fundamental units to belong to subfields related to the automorphism, then theses GSM allow to accelerate the linear algebra step with approximately a factor n^2.

The problem of constructing a TNFS automorphism of degree n for any extension degree n is a hard problem. We were not able to solve it for $n = 4$ with η and κ not coprime, both equal to 2. The same difficulty appears whenever η and κ are not coprime, for instance with $n = 8$, $n = 9$ or $n = 16$.

For other degrees that are square-free, such as 10, 14, 15, while the construction of TNFS automorphisms might be feasible, the GSM presented in this work cannot be used to compute virtual logarithms with the Conjugation method. Indeed, their dimensions on ($\mathcal{K}_1$ of degree $2n$, and $\mathcal{K}_2$ of degree n) are $(2, 1)$, which are too small to control the unit part that does not belong to subfields related to the automorphism.

The investigation of other non square-free orders such as 18, 20 and the orders where η and κ cannot be taken coprime is left for a future work. Another interesting continuation is to apply the GSM construction to other polynomial selection methods.



(a) Lattice of σ_1-related subfields of $\mathcal{K}_1$ (absolute degree 24).

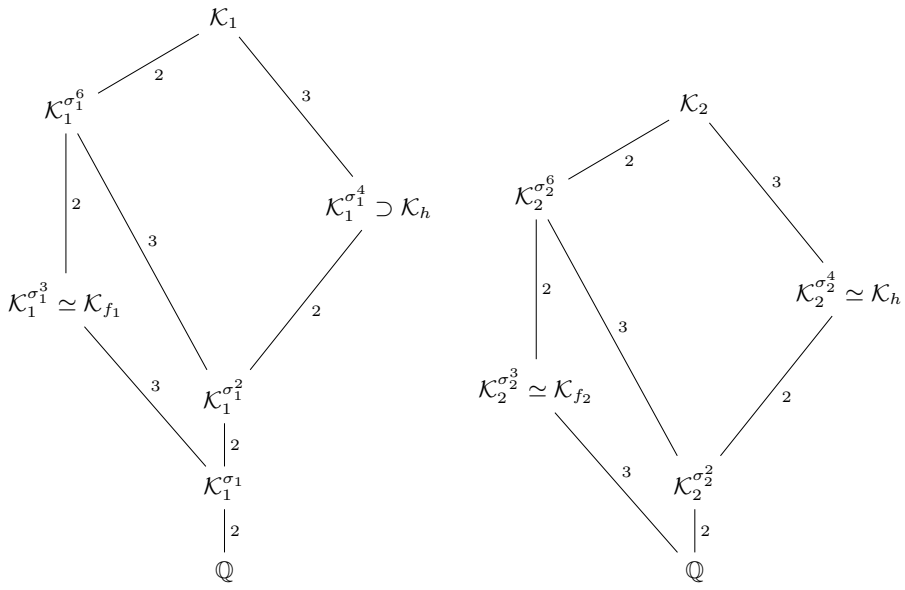
(b) Lattice of σ_2-related subfields of $\mathcal{K}_2$ (absolute degree 12).

Fig. 8: Lattices of automorphism-related subfields with the setup $n = 12$ and $\eta = 3$. Each edge indicates a field extension and is labeled with the corresponding extension degree.

n	4	6	8	9	10	12	14	15
Dimensions	$(4,2)$	$(2,1)$	$(8,4)$	$(6,3)$	$(2,1)$	$(4,2)$	$(2,1)$	$(2,1)$

n	16	18	20	21	22	24	25	26
Dimensions	$(16,8)$	$(6,3)$	$(4,2)$	$(2,1)$	$(2,1)$	$(8,4)$	$(10,5)$	$(2,1)$

Table 10: Dimensions of the GSM of Definition 5 on $(\mathcal{K}_1, \mathcal{K}_2)$ of absolute degrees $(2n, n)$, and constructed with an order n TNFS automorphism.



(a) Lattice of σ_1-related subfields of $\mathcal{K}_1$ (absolute degree 24).

(b) Lattice of σ_2-related subfields of $\mathcal{K}_2$ (absolute degree 12).

Fig. 9: Lattices of automorphism-related subfields with the setup $n = 12$ and $\eta = 4$. Each edge indicates a field extension and is labeled with the corresponding extension degree.

7 Experimental validation: acceleration of the linear algebra step

To validate our findings, we provide a Sagemath implementation of the Tower Number Field Sieve in which the user can choose to use the usual Schirokauer map, or our construction of Galois Schirokauer map together with TNFS automorphisms. We demonstrate our results by applying TNFS on degree 6 and 12 finite fields. Our implementation is available at [3] together with the complete data of our experiments (polynomials, TNFS parameters ...). We emphasize that our implementation is not optimized, in fact, all presented examples in this section can be solved with elementary algorithms. The goal of our implementation is twofold. First, it shows that our theoretical findings work and allow to compute discrete logarithms. Second, it demonstrates the factor 6 and 12 reduction of the size of the matrix in TNFS brought by our work. These results are presented in Table 11. Using automorphisms or not, no example worked with the setup ($n = 12$, $\eta = 3$, $\kappa = 4$). Our explanation is that the sieve dimension that is $2\eta = 6$ is too low given that the characteristic size is small. To make such examples work, it is necessary to consider sieve elements with degree larger than 1 over $\mathcal{K}_h$, which is not supported by our code, or to increase the characteristic size, thus reaching values that are out of the scope of what Sagemath can handle. The implementation works in the following steps.

Finite field	bitsize of p^n	Setup: $\eta =$	(Matrix dimension), rank	
			Without automorphism	**Our work**
$\mathbb{F}_{29^6}$	30	2	$(34686 \times 24006), 23334$	$(5849 \times 4001),\ 3878$
$\mathbb{F}_{37^6}$	32	3	$(1177 \times 510), 502$	$(202 \times 85),\ 81$
$\mathbb{F}_{53^6}$	35	2	*	$(15580 \times 9874),\ 9666$
$\mathbb{F}_{17^{12}}$	50	4	$(86934 \times 23196), 22647$	$(7311 \times 1936),\ 1874$
$\mathbb{F}_{53^{12}}$	69	4	*	$(22674 \times 15469),\ 15291$

Table 11: Experiment results. Comparison of the matrix size between the use or not of TNFS automorphisms of orders 6 and 12. A * indicates that SageMath killed the computation because of the large matrix size. The complete data of these computations are provided in the git repository.

Polynomial selection. For $n = 6, 12$, to perform a computation on a finite field $\mathbb{F}_{p^n}$ of characteristic p, the polynomials must be selected following the Conjugation method presented §2 and Table 4. This ensures the presence of an order n TNFS automorphism as proved in Propositions 5 Moreover, the polynomials must be chosen with the constraints on the number of real roots of Theorem 1 which are recapitulated in Table 5. The choice of the polynomials

[3] `gitlab.inria.fr/halaswad/accelerating_tnfs_with_galois_automorphisms`

is done by the method `polyselect` in `tnfs.py`. The user must set adequate polynomials $(h, f_1, \mu \dots)$ in the method `set_from_family`.

Relation collection. We use the special-q technique to collect relations [35]. Only one special-q ideal is considered per orbit. Thereafter, if the automorphisms are not used in the code, we simulate their "non-use" by expanding each relation into n conjugate relations which is done with the method `expand_list_phi`. If the automorphisms are used, then we do not expand the relations and proceed to the next step (hence, we only have one "representative" relation per orbit). The relation collection is carried by the method `relation_collection` in `tnfs.py`.

Linear algebra. Our contributions appears at this step. Let $\zeta \in \mathbb{F}_\ell$ denote the $n-th$ primitive root of unity corresponding to the TNFS-automorphism of $\mathbb{F}_{p^n}$ that expresses as $\overline{\sigma} : x \mapsto x^\zeta$. We define the GSM $(\Lambda_{d_n,1}, \Lambda_{d_n,2})$ from Definition 5, where $d_6 = 1$ and $d_{12} = 2$. With this construction and these Schirokauer maps, we proved the existence of a virtual logarithm map vlog with the following properties. If $\mathfrak{p}$ is a prime ideal in the factor basis of orbit size equal to n, then $\mathrm{vlog}(\mathfrak{p}^\sigma) = \zeta\,\mathrm{vlog}(\sigma)$—here we drop the subscripts as the statement is valid on both sides. Further, if the orbit size is a strict divisor of n, then $\mathrm{vlog}(\mathfrak{p}) = 0$.

We ask the linear algebra step to look for a virtual logarithm map fulfilling the above two properties as follows. If $\mathfrak{p}$ is an ideal in the factor basis, then it corresponds to a column in the matrix that we denote $C_\mathfrak{p}$. This column contains the valuations on $\mathfrak{p}$ in the relations. One the one hand, if $\mathfrak{p}$ has a size n orbit under σ, then the n columns $C_\mathfrak{p}, C_{\mathfrak{p}^\sigma}, \dots, C_{\mathfrak{p}^{\sigma^{n-1}}}$ are replaced by one column equal to $C_\mathfrak{p} + \zeta C_{\mathfrak{p}^\sigma} + \cdots + \zeta^{n-1} C_{\mathfrak{p}^{\sigma^{n-1}}}$ via a matrix multiplication in our code. On the other hand, if $\mathfrak{p}$ has an orbit size strictly smaller than n, then the columns corresponding to $\mathfrak{p}$ and its conjugates are removed.

Remark 3. It is noteworthy that if the relations were expanded, then the previous operation on the columns would result in a rank one family for each set of conjugate relations, which confirms that only one relation per orbit is useful when the automorphisms are deployed. Thus, the method `expand_list_phi` should not be used when the automorphisms are deployed.

Consequently, the number of columns is reduced by a factor slightly larger than n and the number of rows by a factor n. We did not implement the Wiedemann algorithm in Sagemath. We rather use the linear algebra solving algorithm implemented in Sagemath to check that our algorithm computes a virtual logarithm map as expected. Therefore, we only compare the sizes of the matrices depending on whether the order n TNFS automorphism is deployed or not. Table 11 presents the matrices sizes on several finite fields of degree 6 and 12. In the `tnfs.py` file, the methods `relation_matrices` constructs the matrix of relations, and the methods `linear_algebra` and `modified_linear_algebra` find a kernel element of the matrix. The first applies when the automorphisms are not used, and the second when they are used.

To estimate the gain in performance in the linear algebra brought by the automorphisms if the Wiedemann algorithm was deployed, recall from §4.2 that

decomposing the matrix in basis ζ allows the acceleration factor in (4) which we approximate to n^2. Integrating the GSM constructions in the cado-nfs software [1] and modifying the linear algebra to use order n automorphisms is left for a future work.

Final step : verification. While we did not implement the *individual logarithm* step—as our work does not improve it—we ensured the consistency of the virtual logarithm map computed by our linear algebra step. This was achieved by considering numerous sieve elements ϕ in one of the two middle number fields that correspond to relations from previous steps. Subsequently, we confirmed that their virtual logarithms correspond to logarithms, in some basis $\tilde{g}$, of their projection to the finite field. This is done as follows.

We choose g a generator of the sub-group of order ℓ of the finite field's multiplicative group. For each considered ϕ, we compute on the one hand its virtual logarithm $\mathrm{vlog}(\phi)$ using the output of our algorithm, and on the other hand its logarithm $\log_g(\phi)$ in basis g using the logarithm function implemented in Sagemath. While the quotient $\mathrm{vlog}(\phi)/\log_g(\phi) \bmod \ell$ is constant over the picked ϕ's, say equal to c, we continue with different sieve elements. If a sieve element provides a quotient different from c, then the virtual logarithm computed does not correspond to a logarithm map in the finite field and the algorithm fails. If the quotient is constant over all the $\phi's$ (in number of 40 in each of our experiments), then we assume that the algorithm succeeded in computing a virtual logarithm that "corresponds" to a logarithm in the finite field. This means that there exists a basis $\tilde{g}$ such that for each element t in the finite field that lifts to a smooth element $\bar{t}$ in one of the two number fields, we have $\mathrm{vlog}(\bar{t}) \equiv \log_{\tilde{g}}(t) \bmod \ell$. Here, the constant c is equal to $\log_{\tilde{g}}(g)$. The function `log_consistency_check` within `tnfs.py` performs this consistency check.

7.1 Performing a computation

In the following B, q_0, and q_1 denote respectively the smoothness bound, the smallest special-q prime and the largest special-q prime used. In each special-q lattice, the search for relations was performed in a ball of dimension $2 \times \eta$ and with a radius `rad`. The radius is set according to the input E so that the total search space is approximately of the size of the hypercube $[-E, E]^{2\cdot\eta}$. See the document `tnfs.py` for the exact expression of `rad`. Moreover, in some of the computations a *line-sieve* is performed to factor all elements ϕ with coefficients sizes bounded by the new parameter El. This allows to find relations that do not exhibit prime ideals belonging to the special-q range.

The reader can perform a computation by running the `play_tnfs.sage`. The variable `attempt` sets the parameters of the example that will be run, the boolean `use_auto` indicates to use or ignore the TNFS automorphism and the integer d must be set according to Corollary 2. Hence, the variable d must be set to 1 when employing an order 6 automorphism and to 2 when the order of the automorphism is 12.

References

1. The CADO-NFS Development Team. CADO-NFS, An Implementation of the Number Field Sieve Algorithm, https://cado-nfs.inria.fr/, development version of January 2021
2. Al Aswad, H., Pierrot, C.: Individual discrete logarithm with sublattice reduction. Designs, Codes and Cryptography pp. 1–33 (2023). https://doi.org/10.1007/s10623-023-01282-w
3. Barbulescu, R., Gaudry, P., Guillevic, A., Morain, F.: Improving NFS for the discrete logarithm problem in non-prime finite fields. pp. 129–155 (2015). https://doi.org/10.1007/978-3-662-46800-5_6
4. Barbulescu, R., Gaudry, P., Joux, A., Thomé, E.: A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. pp. 1–16 (2014). https://doi.org/10.1007/978-3-642-55220-5_1
5. Berlekamp, E.R.: Algebraic coding theory (revised edition). World Scientific (2015)
6. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. pp. 213–229 (2001). https://doi.org/10.1007/3-540-44647-8_13
7. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. pp. 514–532 (2001). https://doi.org/10.1007/3-540-45682-1_30
8. Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., Zimmermann, P.: Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment. pp. 62–91 (2020). https://doi.org/10.1007/978-3-030-56880-1_3
9. Buhler, J.P., Lenstra, A.K., Pomerance, C.: Factoring integers with the number field sieve. In: Lenstra and Lenstra, Jr. [30], pp. 50–94. https://doi.org/10.1007/BFb0091539
10. Chiesa, A., Hu, Y., Maller, M., Mishra, P., Vesely, P., Ward, N.P.: Marlin: Preprocessing zkSNARKs with universal and updatable SRS. pp. 738–768 (2020). https://doi.org/10.1007/978-3-030-45721-1_26
11. Coppersmith, D.: Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. Math. Comp. **62**(205), 333–350 (1994). https://doi.org/10.1090/S0025-5718-1994-1192970-7
12. Coppersmith, D.: Solving homogeneous linear equations over gf(2) via block wiedemann algorithm. Mathematics of Computation **62**(205), 333–350 (1994)
13. De Micheli, G., Gaudry, P., Pierrot, C.: Lattice enumeration for tower NFS: A 521-bit discrete logarithm computation. pp. 67–96 (2021). https://doi.org/10.1007/978-3-030-92062-3_3
14. De Micheli, G., Gaudry, P., Pierrot, C.: Lattice enumeration and automorphisms for Tower NFS: A 521-bit discrete logarithm computation. Journal of Cryptology **37**(1), 6 (2024)
15. Gabizon, A., Williamson, Z.J., Ciobotaru, O.: PLONK: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. Cryptology ePrint Archive, Report 2019/953 (2019), https://eprint.iacr.org/2019/953
16. Gaudry, P., Guillevic, A., Morain, F.: Discrete logarithm record in GF(p^3) of 592 bits (180 decimal digits) (Aug 2016), https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;ae418648.1608
17. Gordon, D.M.: Discrete logarithms in *GF(P)* using the number field sieve. SIAM J. Discret. Math. **6**(1), 124–138 (1993). https://doi.org/10.1137/0406010
18. Granger, R., Kleinjung, T., Zumbrägel, J.: On the discrete logarithm problem in finite fields of fixed characteristic. Transactions of the American Mathematical Society **370**(5), 3129–3145 (2018). https://doi.org/10.1090/tran/7027

19. Grémy, L., Guillevic, A., Morain, F.: Breaking DLP in $GF(p^5)$ using 3-dimensional sieving (Jul 2017), https://inria.hal.science/hal-01568373, working paper or preprint
20. Grémy, L., Guillevic, A., Morain, F., Thomé, E.: Computing discrete logarithms in $\mathbb{F}_{p^6}$. pp. 85–105 (2017). https://doi.org/10.1007/978-3-319-72565-9_5
21. Groth, J.: On the size of pairing-based non-interactive arguments. pp. 305–326 (2016). https://doi.org/10.1007/978-3-662-49896-5_11
22. Guillevic, A.: Computing individual discrete logarithms faster in GF(p^n) with the NFS-DL algorithm. pp. 149–173 (2015). https://doi.org/10.1007/978-3-662-48797-6_7
23. Guillevic, A.: Faster individual discrete logarithms in finite fields of composite extension degree. Mathematics of Computation **88**(317), 1273–1301 (Jan 2019). https://doi.org/10.1090/mcom/3376
24. Hayasaka, K., Aoki, K., Kobayashi, T., Takagi, T.: An experiment of number field sieve for discrete logarithm problem over GF(p^n). JSIAM Letters **6**, 53–56 (2014). https://doi.org/10.14495/jsiaml.6.53
25. Joux, A.: A one round protocol for tripartite Diffie-Hellman **17**(4), 263–276 (Sep 2004). https://doi.org/10.1007/s00145-004-0312-y
26. Joux, A., Lercier, R., Smart, N., Vercauteren, F.: The number field sieve in the medium prime case. pp. 326–344 (2006). https://doi.org/10.1007/11818175_19
27. Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. pp. 543–571 (2016). https://doi.org/10.1007/978-3-662-53018-4_20
28. Kim, T., Jeong, J.: Extended tower number field sieve with application to finite fields of arbitrary composite extension degree. pp. 388–408 (2017). https://doi.org/10.1007/978-3-662-54365-8_16
29. Kleinjung, T., Wesolowski, B.: Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic. Journal of the American Mathematical Society **35**, 581–624 (2022). https://doi.org/10.1090/jams/985, https://hal.science/hal-03347994
30. Lenstra, A.K., Lenstra, Jr., H.W. (eds.): The development of the number field sieve, Lecture Notes in Math., vol. 1554. Springer–Verlag (1993). https://doi.org/10.1007/BFb0091534
31. Lenstra, A.K., Lenstra Jr., H.W., Manasse, M.S., Pollard, J.M.: The number field sieve. pp. 564–572 (1990). https://doi.org/10.1145/100216.100295
32. Massey, J.: Shift-register synthesis and bch decoding. IEEE transactions on Information Theory **15**(1), 122–127 (1969)
33. McGuire, G., Robinson, O.: Lattice Sieving in Three Dimensions for Discrete Log in Medium Characteristic. Journal of Mathematical Cryptology **15**(1), 223 – 236 (01 Jan 2021). https://doi.org/10.1515/jmc-2020-0008
34. Miller, V.: The Weil pairing, and its efficient calculation. Journal of Cryptology **17**, 235–261 (2004). https://doi.org/10.1007/s00145-004-0315-8
35. Pollard, J.M.: The lattice sieve. In: Lenstra and Lenstra, Jr. [30], pp. 43–49. https://doi.org/doi.org/10.1007/BFb0091538
36. Robinson, O.: An implementation of the extended tower number field sieve using 4d sieving in a box and a record computation in $\mathbb{F}_{p^4}$. arXiv preprint 2212.04999 (2022). https://doi.org/10.48550/arXiv.2212.04999
37. Sarkar, P., Singh, S.: New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields. pp. 429–458 (2016). https://doi.org/10.1007/978-3-662-49890-3_17

38. Sarkar, P., Singh, S.: A unified polynomial selection method for the (tower) number field sieve algorithm. Advances in Mathematics of Communications **13**(3), 435–455 (2019). https://doi.org/10.3934/amc.2019028
39. Schirokauer, O.: Discrete logarithms and local units. Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences **345**(1676), 409–423 (1993)
40. The Trusted Computing Group: Trusted Platform Module (2019), latest version Nov. 2019. https://trustedcomputinggroup.org/resource/tpm-library-specification/
41. Thomé, E.: Algorithmes de calcul de logarithmes discrets dans les corps finis. Theses, Ecole Polytechnique (May 2003), https://theses.hal.science/tel-00007532
42. Thomé, E.: Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques. Habilitation thesis, Université de Lorraine (2012), https://members.loria.fr/EThome/files/hdr.pdf
43. Wiedemann, D.: Solving sparse linear equations over finite fields. IEEE transactions on information theory **32**(1), 54–62 (1986)
44. Zhu, Y., Liu, J.: Constructing CM fields for NFS to accelerate DL computation in non-prime finite fields. IEEE Transactions on Information Theory (2023)

A Proofs of Proposition 1 and Proposition 3

A.1 Proof of Proposition 1

First, each of the three sets Γ/Γ^ℓ, $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$, and $\mathcal{I}/\mathcal{I}^\ell$ is clearly an $\mathbb{F}_\ell$-vector space where the underlaying scalar product is $(\lambda, x) \mapsto x^\lambda$. To prove the isomorphism statement, it is sufficient to prove that we have the following exact sequence and that it splits:

$$1 \longrightarrow \mathcal{O}^\times/(\mathcal{O}^\times)^\ell \xrightarrow{i} \Gamma/\Gamma^\ell \xrightarrow{j} \mathcal{I}/\mathcal{I}^\ell \longrightarrow 1.$$

In the following, an element x is written $\overline{x}$ when considered modulo ℓ-th powers.

The morphism i is injective. The morphism i is derived from $\mathcal{O}^\times \subset \Gamma$. To prove that it is one-to-one, consider $x \in \mathcal{O}^\times$ such that $i(\overline{x}) = \overline{1}$. That is, there exists $\gamma \in \Gamma$ such that $x\gamma^\ell = 1$. Then, γ^ℓ belongs to $\mathcal{O}$, and so do γ. Indeed, if $P(X)$ is a monic polynomial with integer coefficients vanishing on γ^ℓ, then $P(X^\ell)$ is a monic polynomial with integer coefficients vanishing on γ. Furthermore, γ belongs to $\mathcal{O}^\times$ since $\gamma(x\gamma^{\ell-1}) = 1$. In conclusion we have $x \equiv 1 \bmod (\mathcal{O}^\times)^\ell$.

The morphism j is surjective. The morphism j is defined by $\gamma \bmod \Gamma^\ell \mapsto (\gamma) \bmod \mathcal{I}^\ell$. It is clearly well defined, let us prove its surjectivity. Since the class number $h_\mathcal{K}$ is coprime to ℓ, let $a, b \in \mathbb{Z}$ such that $ah_\mathcal{K} + b\ell = 1$. Consider $I \in \mathcal{I}$. We have

$$I = I^{ah_\mathcal{K}+b\ell} = (I^a)^{h_\mathcal{K}}(I^b)^\ell,$$

which implies $I \equiv (I^a)^{h_\mathcal{K}} \bmod \mathcal{I}^\ell$. By definition of the class number, there exists $\gamma \in \Gamma$ such that $(I^a)^{h_\mathcal{K}} = (\gamma)$, and therefore, $j(\overline{\gamma}) \equiv I \bmod \mathcal{I}^\ell$.

The sequence is exact. It remains to prove that $\mathrm{Im}(i) = \mathrm{Ker}(j)$. We clearly have the direct inclusion. For the other inclusion, let $\overline{\gamma} \in \mathrm{Ker}(j)$, and

consider $\gamma \in \Gamma$ any representative. There exists $I \in \mathcal{I}$ such that $(\gamma) = I^\ell$, which means that I^ℓ is the identity element in the class group. Since ℓ is coprime to the class number, then I is the identity element in the class group as well, and so is I^{-1}. Therefore, there exists $\gamma' \in \Gamma$ such that $I^{-1} = (\gamma')$. Consequently, $(\gamma\gamma'^\ell) = I^\ell I^{-\ell} = \mathcal{K}$ which implies that $\gamma\gamma'^\ell$ belongs to $\mathcal{O}^\times$, and thus, $\overline{\gamma}$ belongs to $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell = \mathrm{Im}(i)$.

The sequence splits. For each ideal $I \in \mathcal{I}$, let $\gamma_I \in \Gamma$ a generator of $I^{h_\mathcal{K}}$. Recall Bezout's identity $ah_\mathcal{K} + b\ell = 1$ with $a, b \in \mathbb{Z}$ and define the section $s : \mathcal{I}/\mathcal{I}^\ell \to \Gamma/\Gamma^\ell$ as $s(\overline{I}) = \overline{\gamma_I^a}$. The morphism s is clearly well defined. Further, for all $\overline{I} \in \mathcal{I}/\mathcal{I}^\ell$, we have $j(s(\overline{I})) = j(\overline{\gamma_I^a}) = \overline{(\gamma_I^a)} = \overline{I^{ah_\mathcal{K}}} = \overline{I}$. Therefore $j \circ s = \mathrm{Id}$, and the sequence splits.

It remains to prove the basis statement. Direchlet's theorem states the following group isomorphism

$$\mathcal{O}^\times \simeq \mu_\mathcal{K} \times \mathbb{Z}^r.$$

Since $|\mu_\mathcal{K}|$ is coprime to ℓ, then by Bezout's identity, there exists $c, d \in \mathbb{Z}$ such that $c|\mu_\mathcal{K}| + d\ell = 1$. Then for any $\epsilon \in \mu_\mathcal{K}$, we have $\epsilon = \epsilon^{c|\mu_\mathcal{K}|+d\ell} = (\epsilon^d)^\ell$. This proves that $\mu_\mathcal{K}/\mu_\mathcal{K}^\ell$ is the trivial group. We have the following vector space isomorphism

$$\mathcal{O}^\times/(\mathcal{O}^\times)^\ell \simeq (\mathbb{Z}/\ell\mathbb{Z})^r,$$

thus proving the unique representation of units modulo $(\mathcal{O}^\times)^\ell$ in a system of fundamental units. The unique representation of ideals within $\mathcal{I}/\mathcal{I}^\ell$ in the set $\mathcal{F}/\mathcal{F}^\ell$ directly results from the unique factorization of ideals.

A.2 Proof of Proposition 3

By Dirichlet's theorem, the unit rank of $\mathcal{K}$ is $r_\mathcal{K} = m/2 - 1$ since its signature is $(0, m/2)$, and the unit rank of the subfield $\tilde{\mathcal{K}}$ is $m/2 - 1$ as well since its signature is $(m/2, 0)$. Therefore, the group of units $\mathcal{O}_\mathcal{K}^\times$ and $\mathcal{O}_{\tilde{\mathcal{K}}}^\times$ have the same rank, and hence their index v is finite. Suppose now that v is coprime to ℓ. To not encumber the notations, we write r instead of $r_\mathcal{K}$.

Let $\{u_1, \ldots, u_r\}$ a system of fundamental units of $\tilde{\mathcal{K}}$. When considered modulo $(\mathcal{O}_{\tilde{\mathcal{K}}}^\times)^\ell$, this family forms an $\mathbb{F}_\ell$-basis of the vector space $\mathcal{O}_{\tilde{\mathcal{K}}}^\times/(\mathcal{O}_{\tilde{\mathcal{K}}}^\times)^\ell$. We shall prove that it is also a basis of $\mathcal{O}_\mathcal{K}^\times/(\mathcal{O}_\mathcal{K}^\times)^\ell$. Since both spaces have the same dimension, it is sufficient to prove that the family is free.

Considered as elements of $\mathcal{O}_\mathcal{K}^\times$, let $\lambda_1, \ldots \lambda_r \in \mathbb{F}_\ell$ such that $u_1^{\lambda_1} \ldots u_r^{\lambda_r} \equiv 1 \bmod (\mathcal{O}_\mathcal{K}^\times)^\ell$. Then, there exists $\mu \in \mathcal{O}_\mathcal{K}^\times$ such that $u_1^{\lambda_1} \ldots u_r^{\lambda_r} \times \mu^\ell = 1$ where the equality is in $\mathcal{O}_\mathcal{K}^\times$. Raising both sides of the equality to the power the index $v = [\mathcal{O}_\mathcal{K}^\times : \mathcal{O}_{\tilde{\mathcal{K}}}^\times]$, we get

$$u_1^{\lambda_1 \cdot v} \ldots u_r^{\lambda_r \cdot v} \times (\mu^v)^\ell = 1.$$

Since μ^v belongs to $\mathcal{O}_{\tilde{\mathcal{K}}}^\times$, the above equality holds in $\mathcal{O}_{\tilde{\mathcal{K}}}^\times$. Therefore we have $u_1^{\lambda_1 \cdot v} \ldots ur^{\lambda_r \cdot v} \equiv 1 \bmod (\mathcal{O}_{\tilde{\mathcal{K}}}^\times)^\ell$, from which we deduce $\lambda_1 \times v \equiv \cdots \equiv \lambda_r \times v \equiv 0 \bmod \ell$. Since v is coprime to ℓ, we have $\lambda_i \equiv 0 \bmod \ell$ for all $1 \leq i \leq r$, which proves that $\{u_1, \ldots, u_r\} \bmod (\mathcal{O}_\mathcal{K})^\ell$ is a $\mathbb{F}_\ell$ basis of $\mathcal{O}_\mathcal{K}^\times/(\mathcal{O}_\mathcal{K}^\times)^\ell$.

Let $u \in \mathcal{O}_{\mathcal{K}}^{\times}/(\mathcal{O}_{\mathcal{K}}^{\times})^{\ell}$. We just proved that u belongs to $\mathcal{O}_{\widehat{\mathcal{K}}}^{\times}/(\mathcal{O}_{\widehat{\mathcal{K}}}^{\times})^{\ell}$, which means that $\sigma^{k/2}(u) = u$. Applying Corollary 1 we get $\mathrm{vlog}(u) = 0$.

B The Wiedmann algorithm

Consider M a square non-invertible matrix of size N over $\mathbb{Z}/\ell\mathbb{Z}$, and let λ designate the average number of non-zero coefficients per row. Wiedemann's algorithm [43] computes a non-trivial kernel element of M in time $O(\lambda N^2)$. The idea is to compute a non-zero polynomial that vanishes at M. Let us first show how to compute a solution to the linear equations given a vanishing polynomial. Consider $P = \sum_{i=0}^{s} p_i X^i \neq 0$ such that $P(M) = 0$. This vanishing writes as

$$\sum_{i=0}^{s} p_i M^i = 0.$$

We claim that $p_0 = 0$. Indeed, first, since the matrix is not invertible, there exists a non-trivial kernel element $\mathbf{v}$ of M. Second, since $0 = P(M)\mathbf{v} = \sum_{i=0}^{s} p_i(M^i\mathbf{v}) = 0$, we have

$$-p_0\mathbf{v} = \sum_{i=1}^{s} p_i(M^i\mathbf{v}) = 0,$$

where the last equality comes from $M\mathbf{v} = 0$. Consequently, since $\mathbf{v}$ is non-zero, we get $p_0 = 0$. Let k the lowest degree of P in X, then factoring by X^k we get $P = X^k\widetilde{P}$, with $\widetilde{P}(0) \neq 0$. Hence, $\widetilde{P}$ does not vanish on M. It is sufficient to compute a vector ω that does not belong to the kernel of $\widetilde{P}(M)$ to output a non-trivial kernel element of M. Indeed, one multiplies iteratively $\widetilde{P}(M)\omega$ by M at left until the result is non-zero and is in the kernel of M. The process finishes after at most k iterations. Wiedemann's algorithm reduces the computation of a kernel element of M to the computation of a vanishing polynomial on M.

Computing a vanishing polynomial on M. Wiedemann's algorithm uses the *Krylov* technique to compute a non-zero vanishing polynomial on M with high probability. First, the algorithm chooses two random vectors $\mathbf{a}$ and $\mathbf{b}$ of size N, and computes the Krylov sequence $\{\mathbf{a}^T M^i \mathbf{b}\}_{i=0}^{2N-1}$, where $\mathbf{a}^T$ is the transposed of $\mathbf{a}$. Because the matrix is of size N, there exists a vanishing polynomial of M of degree at most N, which implies that the Krylov sequence is generated by a recursive relation of order at most N. Hence, the $2N$ terms are sufficient to compute a recursive relation from which one extracts a polynomial P of degree at most N such that:

$$\mathbf{a}^T P(M)\mathbf{b} = 0.$$

Indeed, this can be done naively in $O(N^3)$ operations by solving a linear system of N equations from the Krylov sequence, where the unknowns are the coefficients of the recursive relations. However, this is too costly. Instead, the Berlekamp-Massey algorithm [5,32] computes a polynomial P verifying the above property

in time $O(N \log(N))$, essentially by applying the extended Euclidean algorithm. The polynomial P is in fact a vanishing polynomial on M with high probability. More precisely, the probability that P vanishes on M is $1 - O(1/\ell)$, which is very high. See [41] for a proof of this probability.

Conclusion and complexity of Wiedemann's algorithm. In conclusion, to compute a non-trivial kernel element of the matrix M the linear algebra step proceeds as follows. First, a sequence of $2N$ terms $\{\mathbf{a}^T M^i \mathbf{b}\}_{i=0}^{N-1}$ is computed. This can be done by first iteratively computing the sequence $\{M^i \mathbf{b}\}$ and second multiplying by $\mathbf{a}^T$. Each matrix-vector multiplication is done in $O(\lambda N)$ arithmetic operations. Hence, computing the sequence can be done in $O(\lambda N^2)$ arithmetic operations. Second, the algorithm computes a polynomial P that vanishes on M (with high probability), this is done using the Berlekamp-Massey algorithm in $O(N \log(N))$ arithmetic operations. Third, the lowest degree monomial is factored in P and the polynomial $\widetilde{P}$ is defined as $P = X^k \widetilde{P}$ with $\widetilde{P}(0) \neq 0$. Then a random vector ω is picked such that $\widetilde{P}(M)\omega \neq 0$. Then for incrementing $i = 1, \ldots, k$, the terms $\omega_i := M^i(\widetilde{P}(M)\omega)$ are computed until $\omega_{i_0} \neq 0$ and $\omega_{i_0+1} = 0$, which happens after at most $k < N$ iterations. The vector ω_{i_0} is the wanted vector that corresponds to virtual logarithms. Each iteration is a matrix-vector product, hence, all iterations together cost $O(\lambda N^2)$. In conclusion, the complexity of the linear algebra step is $O(\lambda N^2)$ in number of arithmetic operations.

Furthermore, a major improvement of Wiedemann's algorithm is its block variant [12] which allows parallelization, and hence significant accelerations in discrete logarithm computations.