A Modular Method for Computing the Splitting Field of a Polynomial

Guénaël Renault[1]* and Kazuhiro Yokoyama[2]

[1] LIP6-SPIRAL - Université Paris 6, 4, place Jussieu, F-75005 Paris, France
guenael.renault@lip6.fr
[2] Department of Mathematics, Rikkyo University, 3-34-1 Nishi Ikebukuro, Toshima-ku, Tokyo, 171-8501, Japan
yokoyama@rkmath.rikkyo.ac.jp

Abstract. We provide a modular method for computing the splitting field K_f of an integral polynomial f by suitable use of the byproduct of computation of its Galois group G_f by p-adic Stauduhar's method. This method uses the knowledge of G_f with its action on the roots of f over a p-adic number field, and it reduces the computation of K_f to solving systems of linear equations modulo some powers of p and Hensel liftings. We provide a careful treatment on reducing computational difficulty. We examine the ability/practicality of the method by experiments on a real computer and study its complexity.

1 Introduction

This paper is a continuation of Section 5.3 in [21], where, in order to compute the splitting field of an integral polynomial f, the use of the approximations of its roots was suggested. Here we give its details, show its practicality by experiments and provide its complexity study. Moreover we give some techniques in order to increase the feasibility of this new method.

To compute the Galois group G_f of a monic integral polynomial f, the approach of p-adic approximation is very practical (see [21, 9, 8]). In this approach, one used the approximation of roots of f in a p-adic number field $\mathbb{Q}_p$ (or one of its extensions) in order to find integral roots of the relative resolvents used in Stauduhar's method (see [18]).

For computing the splitting field K_f, there are two approaches: one is constructing this field as a *simple extension* and the other, which is ours, as a *successive extension* given by the *splitting ideal*. Constructing the splitting field as a simple extension can be done by rather simpler computation, where the minimal polynomial of a primitive element of K_f is constructed. (Using p-adic approximations of all its conjugates, it can be computed efficiently.) But, in this setting, if one wants to compute products and sums of several roots of f, i.e.

* We wish to acknowledge the Japanese Ministry of Education, Science and Culture which supported the invitation of the first author in the University of Kyushu during September 2004 where this collaboration has been initiated.

one wants to do arithmetic operations in $K_f \cong \mathbb{Q}[x_1, ..., x_n]/\mathcal{M}$, where each variable corresponds each root of f and $\mathcal{M}$ is the *splitting ideal* generated by all algebraic relations of roots of f, one have to compute the expressions of roots with respect to the primitive element. On the other hand, in our approach, we compute a Gröbner basis $\mathcal{G}$ of the splitting ideal $\mathcal{M}$ and hence, it is easy to perform arithmetic operations in $\mathbb{Q}[x_1, ..., x_n]/\mathcal{M}$. Moreover, in general, expressions by primitive elements tend to be suffered "expression swell", that is, huge coefficients appear and those harm the efficiency. So, for our purpose, simple extension does not seem suited.

In order to compute the splitting ideal $\mathcal{M}$ of a polynomial, there is a classical approach due to Kronecker using algebraic factoring algorithms. But, as shown in [2], it does not seem practical for polynomials having large Galois groups. Here, to overcome the difficulty, we use the knowledge of certain algebraic structures: the p-adic approximation of roots and the explicit action of the Galois group G_f. For the computation of a Gröbner basis of $\mathcal{M}$ we compute a theoretical form of our output with indeterminate coefficients representing the polynomials generating the basis. Then, we compute these polynomials by solving linear systems modulo a power of p and Hensel liftings. For the theoretical form, there is a well known dense generic one based on the knowledge of the degrees of the polynomials (see [21, 4]). In Section 3, we show how a *careful study* on the symmetric representation of G_f allows to produce a sparser theoretical form and how to avoid the computation of polynomials in the basis. From this study we obtain, for a given symmetric representation of G_f, a *scheme* for the computation of $\mathcal{G}$. In Section 4, we show how to compute the polynomials of $\mathcal{G}$ with linear algebra and Hensel lifting and provide an effective test for an *early detection* strategy. We emphasise that one can combine other methods for the computation of $\mathcal{G}$ with the proposed scheme. For example we could combine sparse interpolations strategy effectively (dense interpolation formulas are given in [6, 12]), this will be study in a future work. We also note that it is possible to translate the results presented in this article to polynomials over global fields.

2 Preliminaries

We provide necessary notions and summarize some results of [21].

2.1 Splitting field and Galois group over $\mathbb{Q}$

Let $f(x)$ be a monic square-free integral polynomial of degree n and $\underline{\alpha}$ the set of all its roots in an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. The splitting field K_f of f is the extension field $\mathbb{Q}(\underline{\alpha})$ obtained by adjoining $\underline{\alpha}$ to $\mathbb{Q}$. The group G_f of $\mathbb{Q}$-automorphisms of K_f acts faithfully on $\underline{\alpha}$, thus one can consider the permutation representation G_f of this group. Fixing a numbering of the roots $\underline{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ of f, G_f is viewed as a subgroup of S_n. The group G_f is called the Galois group of f.

To express K_f symbolically, the following epimorphism ϕ of $\mathbb{Q}$-algebra is considered:

$$\mathbb{Q}[x_1, \ldots, x_n] \ni x_i \longmapsto \alpha_i \in K_f$$

For simplicity, we write $X = \{x_1, \ldots, x_n\}$ and, more generally, for a subset E of $\{1, \ldots, n\}$ we write $X_E = \{x_i : i \in E\}$. Then K_f is represented by the residue class ring $\mathcal{A}$ of the polynomial ring $\mathbb{Q}[X]$ factored by the kernel $\mathcal{M}$ of ϕ. We call $\mathcal{M}$ *the splitting ideal of* f *associated with the assignment of the roots* $\alpha_1, \ldots, \alpha_n$. In this setting, computing K_f means to compute a *Gröbner basis* $\mathcal{G}$ of $\mathcal{M}$ (see [5]). If we choose the lexicographic order $\prec$ on terms with $x_1 \prec \cdots \prec x_n$, then the reduced Gröbner basis of $\mathcal{M}$ coincides with the generating set $\{g_1, g_2, \ldots, g_n\}$ obtained by *successive extensions*, that is, for each i,

1. g_i is a polynomial in $x_1, \ldots, x_i$ and monic with respect to x_i, and
2. $\mathbb{Q}(\alpha_1, \ldots, \alpha_i) \cong \mathbb{Q}[X_{\{1,\ldots,i\}}]/\langle g_1, \ldots, g_i\rangle$, where $\langle F\rangle$ denotes the ideal generated by an element or a set F. This implies that g_i is an irreducible factor of $f(x_i)$ over $\mathbb{Q}[X_{\{1,\ldots,i-1\}}]/\langle g_1, \ldots, g_{i-1}\rangle$ such that $g_i(\alpha_1, \ldots, \alpha_i) = 0$.

Thus this reduced Gröbner basis can be obtained by "algebraic factoring methods" (see [2]) and is said to be a *triangular basis* (see [11, 6]). For a Gröbner basis $\mathcal{G} \subset \mathbb{Q}[X]$ and a polynomial P, let $\mathrm{NF}(P, \mathcal{G})$ denote the normal form of P in $\mathbb{Q}[X]$ with respect to $\mathcal{G}$ (see [5]).

The group S_n acts naturally on $\mathbb{Q}[X]$ with $x_i^\sigma = x_{i^\sigma}$ for $1 \leqslant i \leqslant n$ and $\sigma \in S_n$. Thus G_f is the $\mathbb{Q}$-automorphisms group of $\mathcal{A}$ denoted by $\mathrm{Aut}_{\mathbb{Q}}(\mathcal{A})$ (see [2, 1]). We use the following notation for groups: for a group G acting on a set $\mathcal{S}$, the stabilizer in G of an element or a subset A of $\mathcal{S}$ is denoted by $\mathrm{Stab}_G(A)$, i.e. $\mathrm{Stab}_G(A) = \{\sigma \in G : A^\sigma = A\}$. If G is the full symmetric group on $\mathcal{S}$, we simply write $\mathrm{Stab}(A)$ for $\mathrm{Stab}_G(A)$. We denote by $\mathrm{Stab}_G([a_1, \ldots, a_k])$ the pointwise stabilizer of a subset $A = \{a_1, \ldots, a_k\}$ of $\mathcal{S}$, i.e. $\mathrm{Stab}_G([a_1, \ldots, a_k]) = \{\sigma \in G \mid a_i^\sigma = a_i,\ \forall i \in \{1, \ldots, k\}\}$. The set of right cosets of H in G is denoted by $H\backslash G$ and the set of all representatives of $H\backslash G$ by $H\backslash\backslash G$.

Definition 1. *We call the ideal generated by* $t_1 + a_1, \ldots, t_n + (-1)^{n-1}a_n$, *where* t_i *is the* i*-th elementary symmetric function on* X *and* $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, *the* universal splitting ideal *of* f *and denote it by* $\mathcal{M}_0$. *We call the residue class ring* $\mathbb{Q}[X]/\mathcal{M}_0$ the universal splitting ring of f over $\mathbb{Q}$ *and denote it by* $\mathcal{A}_0$.

The reduced Gröbner basis of $\mathcal{M}_0$ is composed of the n *Cauchy's modules* of f (see [16]). Since S_n stabilizes $\mathcal{M}_0$, S_n also acts faithfully on $\mathcal{A}_0$, i.e. $S_n \subset \mathrm{Aut}_{\mathbb{Q}}(\mathcal{A}_0)$. We have the following theorem (see [14, 3, 21] for details and other references).

Theorem 1. *There is a one-to-one correspondence between the set of all primitive idempotents of* $\mathcal{A}_0$ *and the set of all prime divisors of* $\mathcal{M}_0$. *Let* e *be the primitive element corresponding to the fixed prime divisor* $\mathcal{M}$. *Then,* $G_f = \mathrm{Stab}(\mathcal{M}) = \mathrm{Stab}(e)$ *and* $\mathcal{M}^\sigma = \{g \in \mathbb{Q}[X] \mid ge^\sigma = 0 \in \mathcal{A}_0\}$. *Moreover, we have* $\mathcal{M}_0 = \cap_{\sigma \in G_f\backslash\backslash S_n} \mathcal{M}^\sigma$ *and* $\mathcal{A}_0 = \oplus_{\sigma \in G_f\backslash\backslash S_n} e^\sigma \mathcal{A}_0 = \oplus_{\sigma \in G_f\backslash\backslash S_n} \mathbb{Q}[X]/\mathcal{M}^\sigma$.

2.2 Splitting field over p-adic number field

Now we consider the relation between the splitting ring over $\mathbb{Q}$ and that over a p-adic field $\mathbb{Q}_p$. The n-tuple $\underline{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ and the splitting ideal $\mathcal{M}$

associated with the assignment x_i to α_i are fixed. The primitive idempotent of $\mathcal{A}$ corresponding to $\mathcal{M}$ is denoted by e. For a prime integer p, we denote by $\mathbf{Z}_p^0$ (resp. $\mathbf{Z}_p$) the localization of $\mathbf{Z}$ at p (resp. the completion of $\mathbf{Z}_p^0$). We denote by π_p the projection from $\mathbf{Z}_p[X]$ to $\mathbb{F}_p[X]$ (the natural extension of the projection from $\mathbf{Z}$ to $\mathbb{F}_p$).

From now on, we fix a prime number p such that $\pi_p(f)$ is square-free. Let $\bar{\mathcal{M}}_0$ denote the ideal $\pi_p(\mathcal{M}_0 \cap \mathbf{Z}_p^0[X])$ in $\mathbb{F}_p[X]$ and $\mathcal{G}_0$ denotes the standard generating set of $\mathcal{M}_0$. By construction, the Cauchy's modules of f are polynomials with integral coefficients and monic in their greatest monomial. Thus, the set $\pi_p(\mathcal{G}_0)$ is a Gröbner basis of $\pi_p(\mathcal{M}_0 \cap \mathbf{Z}_p^0[X])$. Moreover, $\mathcal{G}_0$ is a Gröbner basis of the universal splitting ideal $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M}_0$ of f as a polynomial with coefficients in $\mathbb{Q}_p$ and that of $\mathbf{Z}_p[X] \otimes_{\mathbf{Z}_p^0} (\mathcal{M}_0 \cap \mathbf{Z}_p^0[X])$ over $\mathbf{Z}_p$. The ideal $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M}_0$ is denoted by $\mathcal{M}_0^{(\infty)}$. We denote $\mathbb{F}_p[X]/\bar{\mathcal{M}}_0$ by $\bar{\mathcal{A}}_0$ and $\mathbb{Q}_p[X]/\mathcal{M}_0^{(\infty)}$ by $\mathcal{A}_0^{(\infty)}$.

Theorem 2. *We have the following assertions:*
1. The projection π_p gives a one-to-one correspondence between the set of all primitive idempotents of $\mathcal{A}_0^{(\infty)}$ and that of $\bar{\mathcal{A}}_0$. Moreover, for each pair $(\bar{e}, e^{(\infty)})$ of corresponding primitive idempotents, $\mathrm{Stab}(\bar{e}) = \mathrm{Stab}(e^{(\infty)})$.
2. The idempotent e of $\mathcal{A}_0$ is also an idempotent of $\mathcal{A}_0^{(\infty)}$. Let $\bar{e}$ be a component of $\pi_p(e)$ and $e^{(\infty)}$ the primitive idempotent of $\mathcal{A}_0^{(\infty)}$ corresponding to $\bar{e}$. Then $\mathrm{Stab}(e)$ *contains* $\mathrm{Stab}(\bar{e})(= \mathrm{Stab}(e^{(\infty)}))$ *and* $\mathrm{Stab}(\pi_p(e)) = \mathrm{Stab}(e)$. *Moreover, by letting* $\mathcal{S} = \mathrm{Stab}(\bar{e})\backslash\backslash\mathrm{Stab}(e)$, $\pi_p(e) = \sum_{\sigma\in\mathcal{S}} \bar{e}^{\sigma}$ *and* $e = \sum_{\sigma\in\mathcal{S}} {e^{(\infty)}}^{\sigma}$.

Now we fix a component $\bar{e}$ of $\pi_p(e)$ and its corresponding idempotent $e^{(\infty)}$ of $\mathcal{A}_0^{(\infty)}$. Let $\bar{\mathcal{M}}$ be the maximal ideal of $\mathbb{F}_p[X]$ corresponding to $\bar{e}$ and $\mathcal{M}^{(\infty)}$ the maximal ideal of $\mathbb{Q}_p[X]$ corresponding to $e^{(\infty)}$. Moreover, let $\mathcal{G}^{(\infty)}$ and $\bar{\mathcal{G}}$ be the reduced Gröbner basis of $\mathcal{M}^{(\infty)}$ and that of $\bar{\mathcal{M}}$ respectively.

Definition 2. *Let $\mathcal{G}^{(\infty)} = \{g_1^{(\infty)}, \ldots, g_n^{(\infty)}\}$. For a positive integer k, we call the set $\{g_1^{(\infty)} \bmod p^{k+1}, \ldots, g_n^{(\infty)} \bmod p^{k+1}\}$ the* k-th approximation to $\mathcal{G}^{(\infty)}$ *and denote it by $\mathcal{G}^{(k)}$. We note that $\mathcal{G}^{(0)} = \bar{\mathcal{G}}$.*

We can lift $\bar{\mathcal{G}}$ to $\mathcal{G}^{(\infty)}$ by Hensel construction. More precisely we have:

Theorem 3. *The reduced Gröbner basis $\mathcal{G}^{(\infty)}$ of $\mathcal{M}^{(\infty)}$ with respect to $\prec$ is contained in $\mathbf{Z}_p[X]$, and $\bar{\mathcal{G}}$ is lifted uniquely to $\mathcal{G}^{(\infty)}$ by Hensel construction.*

Proof. Theorem 21 in [21] gives the result and a construction based on a *linear iteration Hensel lifting*. Actually, its *quadratic iteration* version can be restated for this construction (see [15]) □

3 The computation scheme

In this section, we propose a framework for the computation of a Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_n\}$ of the splitting ideal $\mathcal{M}$ of f with indeterminate coefficients

strategy. We now assume the Galois group G_f of f is already computed as a subgroup of S_n. We show how the knowledge of the symmetric representation G_f can give a *good* theoretical form of $\mathcal{G}$, and then we provide some *techniques* which permit us to avoid computations of some g_i.

3.1 The form of $\mathcal{G}$

Since we compute polynomials g_i with indeterminate coefficients strategy, we need to know the *potential terms* which may appear in g_i. The following allows to deduce $\deg_i(g_i)$, the degree in x_i of g_i, from $G_f = \mathrm{Stab}(\mathcal{M})$.

Proposition 1 (Theorem 5.3 [4]). *The degree d_i of g_i in x_i is given by*

$$d_i = |\mathrm{Stab}_{G_f}([1,\ldots,i-1])|/|\mathrm{Stab}_{G_f}([1,\ldots,i])|\,.$$

Reciprocally, the next proposition gives the characterization of all the Gröbner bases of $\mathcal{M}$. Its proof is immediate (see [5]).

Proposition 2. *Let $\mathcal{G} = \{g_1,\ldots,g_n\}$ be a triangular set of polynomials of $\mathcal{M}$ such that $\deg_i(g_i) = d_i$. Then, $\mathcal{G}$ is a Gröbner basis of $\mathcal{M}$. Note that $\mathcal{G}$ is not necessarily reduced but it is minimal (see [5]).*

Thus, we want to compute such a triangular set $\mathcal{G}$. A generic form for such a Gröbner basis $\mathcal{G}$ can be retrieved from this: the terms of g_i's monomials are potentially $x_i^{k_i}x_{i-1}^{k_{i-1}}\cdots x_1^{k_1}$ with $0 \leqslant k_j < d_j$. In this case, the number of indeterminate coefficients is of the order of G_f which may be very large (this dense form is considered in [12]). Clearly, the sparser the basis $\mathcal{G}$ is, the most efficient the computation is, thus we are interested in finding a sparse one. For this task we introduce a definition.

Definition 3. *Let i be an integer in $\{1,\ldots,n\}$. A subset E of $\{1,\ldots,i\}$ containing i is said to be an* i-relation *if there exists a polynomial r_i in $\mathbb{Q}[X_E]$ such that*

$$\alpha_i^{d_i} + r_i(\underline{\alpha}) = 0 \text{ and } \deg_i(r_i) < d_i\,.$$

An i-relation corresponds to a potential g_i in any $\mathcal{G}$, for example, the sets $\{1,\ldots,i\}$, for $i = 1,\ldots,n$, are the i-relations corresponding to the generic form of $\mathcal{G}$. The following proposition permits us to easily find an i-relation which may be smaller. Its proof is immediate by considering a minimal polynomial of α_i (see [15]).

Proposition 3. *Let i be an integer in $\{1,\ldots,n\}$ and m be the minimal integer in $\{1,\ldots,i-1\}$ such that $|\mathrm{Stab}_{G_f}([1,\ldots,m])|/|\mathrm{Stab}_{G_f}([1,\ldots,m,i])| = d_i$. Then, there exists an i-relation in $\{1,\ldots,m,i\}$.*

If E_i is the maximal i-relation $\{1,\ldots,i\}$ then, as one can see above, it is easy to identify the potential terms of the corresponding polynomial. The following result, which is a consequence of classical Galois theory, gives us the way of doing the same for more general i-relations:

Proposition 4. *Let $E = \{e_1 < e_2 < \cdots < e_s = i\}$ be an i-relation. Then, there exists a polynomial r_i as in Definition 3 such that*

$$deg_j(r_i) < |\mathrm{Stab}_{G_f}([e_1, \ldots, e_{j-1}])|/|\mathrm{Stab}_{G_f}([e_1, \ldots, e_j])|,\ \forall j \in \{1, \ldots, s\}\,.$$

The preceding proposition provides a relation between an i-relation and the maximal degree of each variable of the corresponding polynomial g_i. We now want to know the size of g_i.

Definition 4. *Let $E_i = \{e_1 < e_2 < \cdots < e_s = i\}$ be an i-relation. We define the finite sequence $d(E_i)_{e_1}, \ldots, d(E_i)_{e_s}$ by*

$$d(E_i)_{e_j} = |\mathrm{Stab}_{G_f}([e_1, \ldots, e_{j-1}])|/|\mathrm{Stab}_{G_f}([e_1, \ldots, e_j])|,\ \forall j \in \{1, \ldots, s\}\,.$$

The degree of E_i *is defined by $\prod_{j=1}^{s} d(E_i)_{e_j}$ and is denoted by $D(E_i)$.*

Given an i-relation $E_i = \{a < b < \cdots < l = i\}$, then the number of terms $x_a^{k_a} x_b^{k_b} \cdots x_l^{k_l}$ which potentially appear in the corresponding g_i is $D(E_i)$. There might be different i-relations, so we give a *partial order* among all the i-relations.

Definition 5. *Let i be an integer in $\{1, \ldots, n\}$. An i-relation E_i is said to be* minimal *if $D(E_i)$ is minimal (among all the i-relation) and not any proper subset of E_i is an i-relation.*

We note that a minimal i-relation $E_i = \{e_1 < e_2 < \cdots < e_s = i\}$ verifies $d(E_i)_{e_j} \geqslant 2$ for all j, $1 \leqslant j < s$. Minimal i-relations for each $i = 1, \ldots, n$ correspond to polynomials g_i with a minimal number of coefficients and thus to a Gröbner basis $\mathcal{G}$ which have a sparse form. Note that an i-relation satisfying conditions of Proposition 3 may not be minimal.

3.2 Reducing the number of polynomials to compute

We assume that the symmetric representation of G_f and an i-relation E_i for each i in $\{1, \ldots, n\}$ are known. Here we give techniques to avoid some computations of elements of $\mathcal{G}$. These techniques were already used in [13] with a partial knowledge of G_f. However, since we know the exact symmetric representation of G_f, we make use here of the whole power of these techniques.

Cauchy modules technique. Let $\mathcal{G} = \{g_1, \ldots, g_n\}$ be a triangular Gröbner basis of the ideal $\mathcal{M}$ with $\deg_i(g_i) = d_i$. Let $\mathcal{O} = \{i_1 < i_2 < \cdots < i_k\}$ be the orbit of i under the action of $\mathrm{Stab}_{G_f}([1, \ldots, i-1])$. Then $i_1 = i$ and $k = d_i$. For a multivariate polynomial g, we denote by $\mathrm{E}(g, u)$ the multivariate polynomial obtained by replacing the greatest variable in g by a newly introduced indeterminate u. Then, the d_i (generalised) *Cauchy modules* of g_i are defined by: $c_1(g_i) = g_i$,

$$c_2(g_i) = \frac{\mathrm{E}(c_1, x_{i_2}) - \mathrm{E}(c_1, x_{i_1})}{(x_{i_2} - x_{i_1})},\ \cdots,\ c_{d_i}(g_i) = \frac{\mathrm{E}(c_{d_i-1}, x_{i_{d_i}}) - \mathrm{E}(c_{d_i-1}, x_{i_{d_i-1}})}{(x_{i_{d_i}} - x_{i_{d_i-1}})}.$$

By construction, the following holds:

Lemma 1. *The Cauchy module $c_j(g_i)$ is a polynomial of $\mathbb{Q}[X_{\{1,\ldots,i_j\}}]$ which is monic as a polynomial in x_{i_j} with $deg_{i_j}(c_j(g_i)) = d_i - j + 1$. Moreover, the polynomial $c_j(g_i)$ is in $\mathcal{M}$.*

As we know the symmetric representation of G_f we can know in advance if $c_j(g_i)$ has the same degree, in x_{i_j}, as g_{i_j}. In this case, in $\mathcal{G}$, g_{i_j} can be replaced by $c_j(g_i)$ and this set is still a Gröbner basis of $\mathcal{M}$ (see Proposition 2). So, in the construction of $\mathcal{G}$ we avoid the computation of g_{i_j}.

Transporters technique. Here we use the fact that the group G_f is the stabilizer of the ideal $\mathcal{M}$. Let $E_i = \{e_1 < e_2 < \cdots < e_s = i\}$ be an i-relation and $j \in \{i+1, \ldots, n\}$. A permutation $\sigma \in G_f$ is said to be an (i,j)-*transporter* if it satisfies:

$$\sigma(i) = j \text{ and } j = \max(\{\sigma(e) \,:\, e \in E_i\})$$

Proposition 5. *Let σ be an (i,j)-transporter and g_i the polynomial corresponding to E_i. Then, $\mathrm{NF}(g_i^\sigma, \{g_1, \ldots, g_{j-1}\})$ is a multiple of g_j as polynomials in $\mathcal{A} = (\mathbb{Q}[X_{\{1,\ldots,j-1\}}]/\langle g_1, \ldots, g_{j-1}\rangle)[x_j]$.*

Proof. Since σ is an (i,j)-transporter, the polynomial $\mathrm{NF}(g_i^\sigma, \{g_1, \ldots, g_{j-1}\})$ can be viewed as a univariate polynomial h in x_j over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$. Moreover, since $g_i^\sigma \in \mathcal{M}$, we have $h(\alpha_j) = 0$. Thus h is a multiple of the minimal polynomial of α_j over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$, hence h is a multiple of g_i as a polynomial of $\mathcal{A}$ □

Corollary 1. *With the same notations as in Proposition 5, if the degree d_j is equal to d_i then g_i^σ can take the place of g_j in $\mathcal{G}$.*

As for the Cauchy's techniques, from the knowledge of an (i,j)-transporter σ satisfying conditions of Corollary 1, we can avoid the computation of the polynomial g_j since it can be replaced by g_i^σ.

4 Computing splitting fields by linear systems solving

In this section, we assume the knowledge of G_f with its action over approximations of the roots of f in $\bar{\mathbb{Q}}_p$. Moreover, we assume that the *computation scheme* attached to G_f is known, in particular we know a corresponding i-relation E_i for each polynomial g_i of $\mathcal{G}$. We show how these knowledges can be used for the computation of $\mathcal{G}$ by linear systems solving. We denote by $Z(I)$ the algebraic variety associated to an ideal I of $\mathbb{Q}[X]$ or $\mathbb{F}_p[X]$.

4.1 Computation by solving systems of linear equations

Here we compute $g_1, \ldots, g_n$ by a *method of indeterminate coefficients*. Assume that the n-tuple $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of roots of f lie in $Z(\mathcal{M})$. Recall that G_f is already presented as a sub-group of S_n and $\mathrm{Stab}(\mathcal{M}^{(\infty)}) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p[X]/\bar{\mathcal{M}}) = G_{\pi_p(f)} \subset G_f$. We denote $|G_f|$ and $|G_{\pi_p(f)}|$ by N and $\bar{N}$, respectively.

Systems over the rationals. We fix an integer $i \in \{1, \ldots, n\}$. Each coefficient of g_i is replaced with an indeterminate, for simplicity, the terms $\prod_{e \in E_i} x_e^{m_e}$, where $0 \leqslant m_e < d(E_i)_e$, are sorted with respect to the lexicographic order and denoted by $t_1, \ldots, t_{D(E_i)}$. Then, with indeterminates $a_j^{(i)}$, we have $g_i = x_i^{d_i} + \sum_{j=1}^{D(E_i)} a_j^{(i)} t_j$. Since $\mathcal{G}$ is supposed to be a Gröbner basis of $\mathcal{M}$, the following equation holds for i.

$$g_i(\gamma) = 0 \ \text{ for every } \gamma \in Z(\mathcal{M}). \tag{1}$$

Let $E_i = \{e_1 < e_2 < \cdots < e_s\}$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$ be an element of $Z(\mathcal{M})$. We denote by $\gamma(E_i)$ the projection of γ on the indexes given by E_i (i.e. $(\gamma_{e_1}, \ldots, \gamma_{e_s})$) and $Z(\mathcal{M})(E_i) = \{\gamma(E_i) \ : \ \gamma \in Z(\mathcal{M})\}$. Thus, we have $|Z(\mathcal{M})(E_i)| = D(E_i)$. Let G_{E_i} be the group $\mathrm{Stab}_{G_f}([e_1, \ldots, e_s])$ and $G_{E_i} \backslash\backslash G_f = \{\sigma_1, \ldots, \sigma_{D(E_i)}\}$. Then, we have $Z(\mathcal{M})(E_i) = \{\alpha(E_i)^{\sigma_1}, \ldots, \alpha(E_i)^{\sigma_{D(E_i)}}\}$ and

$$g_i(\gamma) = 0 \ \text{ for every } \gamma \in Z(\mathcal{M})(E_i). \tag{2}$$

The system (2) of equations becomes a linear system of $D(E_i)$ equations and $D(E_i)$ variables with matrix representation $-V_i = M_i A_i$, where $A_i = (a_j^{(i)})$, $V_i = ((\alpha_i^{d_i})^{\sigma_r})$ and $M_i = (t_c(\alpha(E_i)^{\sigma_r}))_{r,c}$ with $(r, c) \in \{1, \ldots, D(E_i)\}^2$. Since the set $\{t_1(\alpha(E_i)), \ldots, t_{D(E_i)}(\alpha(E_i))\}$ is a $\mathbb{Q}$-linear basis of $\mathbb{Q}(\{\alpha_e \ : \ e \in E_i\})$, this system has a unique solution. Thus we can compute g_i by solving the system of linear equations if we already know the *exact value of each root* α_i *of* f.

Systems over p-adic numbers. As we do not know the exact value of each α_i, we use the approximate value of roots of f in $\bar{\mathbb{Q}}_p$. In the sequel we use the same notations as Section 2. The ideal $\mathcal{M}$ may not be maximal if it is considered as an ideal in $\mathbb{Q}_p[X]$, more precisely we have:

Proposition 6. *Let* $\mathcal{S}$ *be the transversal* $\mathrm{Stab}(\bar{e}) \backslash\backslash \mathrm{Stab}(e)$. *Then* $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M} = \cap_{\sigma \in \mathcal{S}} (\mathcal{M}^{(\infty)})^{\sigma}$, *and* $\pi_p(\mathcal{M} \cap \mathbf{Z}_p^0) = \cap_{\sigma \in \mathcal{S}} (\bar{\mathcal{M}})^{\sigma}$.

Proof. Let e be the idempotent of $\mathcal{A}_0$ corresponding to $\mathcal{M}$. As $\mathcal{M} = \{h \in \mathbb{Q}[X] \mid eg = 0 \in \mathbb{Q}[X]/\mathcal{M}_0\}$, the first equation can be derived directly from Theorem 1 (2) and Theorem 2 (2). The second equation can be also derived by considering the projection π_p $\square$

By Proposition 6, we can reduce the system (2) to the following.

$$g_i(\gamma) = 0 \ \text{ for every } \gamma \in \cup_{\sigma} Z((\mathcal{M}^{(\infty)})^{\sigma})(E_i), \tag{3}$$

where σ ranges in $\mathcal{S} = G_{\pi_p(f)} \backslash\backslash G_f$. The system (3) consists of $D(E_i)$ variables and $D(E_i)$ linear equations over $\mathbb{Q}_p[X]/\mathcal{M}^{(\infty)}$ and it is equivalent to

$$\mathrm{NF}(g_i, (\mathcal{G}^{(\infty)})^{\sigma}) = 0 \ \text{ for every } \sigma \in G_{E_i} \backslash\backslash G_f. \tag{4}$$

Moreover, replacing $\mathcal{G}^{(\infty)}$ with $\mathcal{G}^{(k)}$, we have the following system which g_i mod p^{k+1} must satisfy.

$$\mathrm{NF}(g_i, (\mathcal{G}^{(k)})^{\sigma}) \equiv 0 \pmod{p^{k+1}} \ \text{ for every } \sigma \in G_{E_i} \backslash\backslash G_f. \tag{5}$$

The system (5) is considered as a system of $D(E_i)$ variables and $D(E_i)$ linear equations with coefficients in $(\mathbf{Z}/p^{k+1}\mathbf{Z})[X]/\mathcal{M}^{(k)}$. Especially, for the case $k=0$, the system (5) is translated to the following system which $\pi_p(g_i)$ must satisfy: Fix a zero $\bar{\alpha}=(\bar{\alpha}_1,\ldots,\bar{\alpha}_n)$ in $Z(\bar{\mathcal{M}})$, and set $\pi_p(g_i)=x_i^{d_i}+\sum_{j=1}^{D(E_i)}\bar{a}_j^{(i)}t_j$. Let $\bar{A}_i=(\bar{a}_j^{(i)})$, $\bar{V}_i=((\alpha_i^{d_i})^{\sigma_r})$ and $\bar{M}_i=(t_c(\bar{\alpha}(E_i)^{\sigma_r}))_{r,c}$ with $(r,c)\in\{1,\ldots,D(E_i)\}^2$. Then we have the identity $-\bar{V}_i=\bar{M}_i\bar{A}_i$.

Theorem 4. *For each i, $1\leqslant i\leqslant n$, the following holds.*
1. The linear system corresponding to $-\bar{V}_i=\bar{M}_i\bar{A}_i$ has a unique solution over $\mathbb{F}_p$ which gives $\pi_p(g_i)$.
2. For a positive integer k, the system (5) has a unique solution which gives the approximation $g_i \bmod p^{k+1}$. Moreover, we can construct $g_i \bmod p^{k+1}$ from $\pi_p(g_i)$ by Hensel lifting.

Proof. Consider the expansion of $\det(M_i)$ and that of $\mathrm{disc}(f)$, where we consider each root α_i as an indeterminate y_i. Then, it can be shown that $\mathrm{disc}(f)=\prod_{j\neq k}(y_j-y_k)$ and by *discriminant composition formula* (see [14]) there exist integers $e_{j,k}$ such that $\det(M_i)=\prod_{1\leqslant j<k\leqslant n}(y_j-y_k)^{e_{j,k}}$. As $\pi_p(f)$ is square-free, we conclude that $\det(\bar{M}_i)\neq 0$ and so the linear system corresponding to $-\bar{V}_i=\bar{M}_i\bar{A}_i$ has a unique solution and thus, the unique solution gives $\pi_p(g_i)$. We can show the second statement by the same argument and the fact that $\det(\bar{M}_i)\neq 0$. For the Hensel lifting we would like to apply the same construction as in Theorem 3. Since the ring $A=\mathbb{F}_p[X]/\pi_p(\mathcal{M}\cap\mathbf{Z}_p^0)$ is not a field, two cases are possible when we compute the *Bézout relation* with the *Extended Euclidean Algorithm* (EEA) with pseudo division in the first step of this lifting: At the end of the EEA a gcd is computed and it is invertible, in this case the lifting can continue; when EEA does not work, we can compute the Bézout relation by other methods. In this second case, we may use combination of EEA over A and *Chinese Remainder Theorem* or solving a system of linear equations derived from this relation. One can see also [17] for a general study about *Newton-Hensel* operator for general triangular sets □

Remark 1. At each step k, the Hensel lifting of a polynomial g_i which corresponds to an i-relation $E_i=\{e_1<\cdots<e_s=i\}$ can be done with two different points of view. The first one is to considerate g_i as a univariate polynomial with coefficients in the ring $R_{2k}=(\mathbb{Z}/p^{2k}\mathbb{Z})[X_{\{1,\ldots,i-1\}}]/\langle g_1,\ldots,g_{i-1}\rangle$. The second one is to see g_i in the univariate polynomial ring with coefficients in $R'_{2k}=(\mathbb{Z}/p^{2k}\mathbb{Z})[X_{E_i\setminus\{x_i\}}]/\langle g_1^*,\ldots,g_{s-1}^*\rangle$ where the polynomials g_j^* lying in $(\mathbb{Z}/p^{2k}\mathbb{Z})[X_{\{e_1,\ldots,e_j\}}]$ are the approximations of the polynomials which defines the extensions $\mathbb{Q}(\alpha_{e_1})$, $\mathbb{Q}(\alpha_{e_1},\alpha_{e_2})$, …, $\mathbb{Q}(\alpha_{e_1},\alpha_{e_2},\ldots,\alpha_{e_s})$. ($\{g_1^*,\ldots,g_{s-1}^*,g_i\}$ is the reduced Gröbner basis of the elimination ideal $\mathcal{M}\cap\mathbb{Q}[X_{E_i}]$.) In the latter case, we compute each g_j^* by solving linear system and Hensel lifting in the same manner as computation of g_i, recursively from g_1^* to g_{s-1}^*. We may also obtain g_j^* by transporter techniques by inspecting the action of G_f. In the former case, at the end of the lifting procedure the Gröbner basis $\mathcal{G}$ is necessarily reduced, but not in the latter case.

Theorem 4 gives two possible strategies (which can be mixed) for the computation of $\mathcal{G}_k = \{g_1 \bmod p^{k+1}, \ldots, g_n \bmod p^{k+1}\}$ a k-approximation of a triangular Gröbner basis $\mathcal{G}$ of $\mathcal{M}$:
1: By Hensel lifting, $\mathcal{G}^{(k)}$ is constructed from $\overline{\mathcal{G}}$ (see Theorem 3). From $\mathcal{G}^{(k)}$ we construct and solve the system 5 for each i, $1 \leqslant i \leqslant n$, the solutions are then $\mathcal{G}_k$.
2: From $\overline{\mathcal{G}}$ we construct and solve the systems 5 for each i, $1 \leqslant i \leqslant n$. The solutions are $\mathcal{G}_0$ and we can construct $\mathcal{G}_k$ by Hensel lifting.

Now, assume $\mathcal{G}_k = \{g_1 \bmod p^{k+1}, \ldots, g_n \bmod p^{k+1}\}$ is computed. Then we convert each $g_i \bmod p^{k+1}$ to a polynomial over $\mathbb{Q}$ by the well-known *rational reconstruction* technique. Let B_i be a bound on all absolute values of the numerators and denominators of coefficients of g_i. Then, as soon as $2B_i^2 < p^{k+1}$, the polynomial converted from $g_i \bmod p^{k+1}$ coincides with g_i (see [7]).

4.2 Estimation of the bound B_i

Here we give details on the bound B_i for the rational reconstruction. Since coefficients of g_i correspond to the solution of the system (2), by Cramer's rule, the denominator of each coefficient of g_i divides $\det(M_i)$ and the numerator of the j-th coefficient of g_i divides $\det(M_i^{(j)})$, where $M_i^{(j)}$ is the matrix obtained by replacing the j-th column with V_i.

Lemma 2. *Let B_0 be the maximum of the absolute values of roots α_i's of f in $\mathbb{C}$. Then, for each i, B_i can be computed from $\{d(E_i)_e : e \in E_i\}$ and B_0.*

Proof. We assume w.l.o.g. that the bound B_0 is greater than 1. For each row of $M_i^{(j)}$ and each row of M_i, by replacing each α_k with B_0 and by denoting $d(E_i)_e$ by d_e we can bound the square-norm of these rows by the integer $\mathbb{B}_i^2 = \prod_{e\in E_i}(1 + B_0^2 + \cdots + B_0^{2(d_e-1)}) + B_0^{2d_i} = \prod_{e\in E_i} \frac{B_0^{2d_e}-1}{B_0^2-1} + B_0^{2d_i}$. Thus, as the determinant of a matrix is bounded by the product of square-norms of its rows (by the inequality of Hadamard), we can set $B_i = \mathbb{B}_i^{D(E_i)}$ $\square$

If $B_0 > 2$, then we can set B_i as $B_0^{D(E_i)(\sum_{e\in E_i} d(E_i)_e)}$ and, since $\sum_{e\in E_i} d(E_i)_e \leqslant \sum_{1\leqslant k\leqslant i} d_k \leqslant \sum_{1\leqslant k\leqslant i} k$, the bit size of B_i is bounded by $O(n^2 D(E_i)\log(B_0))$. For the denominator, we can give a precise bound (see [10]).

Lemma 3. *For each i, there is a positive integer C_i computed from the set of degrees $\{d(E_i)_e : e \in E_i\}$ such that each $d(f)^{C_i} g_i$ belongs to $\mathbb{Z}[X]$.*

Proof. By the discriminant identity given in the proof of Theorem 4, $\det(M_i)$ is considered as a polynomial in each α_i. Then estimating the degree of $\det(M_i)$ in each α_j, we can obtain a bound on the denominators of coefficients of g_i. In fact, the degree of $\det(M_i)$ in α_j is bounded by $D_i = \frac{D(E_i)(\sum_{e\in E_i} d_e)}{n_0}$, where $n_0 = n$ if f is irreducible over $\mathbb{Q}$, and $n_0 = 1$ otherwise. Then, from the shape of $\mathrm{disc}(f)$, it can be shown easily that $C_i = \frac{D_i}{2}$ satisfies the statement. Moreover, if f is irreducible, we can set $C_i = \frac{D_i}{2(n-1)}$ $\square$

The bound B_i given in Lemma 2 is in general very pessimistic. We will see in Section 4.3 how the problem of pessimistic theoretical bound can be avoided.

4.3 Check of correctness and early detection

To improve the efficiency of the method, we can incorporate "early detection strategy" which is widely used in computer algebra. As the bound B_i tends to be large compared to the exact value, the technique is supposed to work very well in our case.

Conversion at Early Stage. Assume that we have computed $\mathcal{G}_k$, even though p^{k+1} does not exceed the theoretical bound. Suppose that we have obtained the first $j-1$ polynomials $\{g_1, \ldots, g_{j-1}\}$ of $\mathcal{G}$. We want to test if the Hensel lifting is enough for $g_j \mod p^{k+1}$. Thus, we try to convert it to a candidate polynomial over $\mathbb{Q}$ by rational reconstruction. Then we first check the following:
1. The conversion is done successfully for every coefficients of $g_i \mod p^{k+1}$.
2. The denominator of each coefficient of a candidate polynomial divides a certain power of $\mathrm{disc}(f)$ (See Lemma 3).
If the conversion does not satisfy the criteria above then p^{k+1} is not sufficient to afford the correct g_j. Thus, we continue the lifting process again. If, in the contrary, the conversion, say h_j, satisfy the criteria we have to prove that $h_j = g_j$ this is what we do now.

Correctness of Solution. Assume that we have a candidate polynomial h_j for the polynomial g_j corresponding to the j-relation E_j. We can check if $h_j = g_j$ by the following theorem.

Theorem 5. *We have $h_j = g_j$ if and only if* $\mathrm{NF}(c_j(f), \{g_1, \ldots, g_{j-1}, h_j\}) = 0$.

Proof. The *only-if-part* is clear, we have only to show the *if-part*. Let H be the triangular set $\{g_1, \ldots, g_{j-1}, h_j\}$. By the hypothesis, the ideal $\langle H \rangle$ contains $\{c_1(f), \ldots, c_j(f)\}$ which is the reduced Gröbner basis of the elimination ideal $\mathcal{M}_0 \cap \mathbb{Q}[X_{\{1,\ldots,j\}}]$. Thus, $\langle H \rangle$ is contained in a maximal ideal $\mathcal{M}'$ of $\mathbb{Q}[X_{\{1,\ldots,j\}}]$, which coincides with $\mathcal{M}^\sigma \cap \mathbb{Q}[X_{\{1,\ldots,j\}}]$ for some $\sigma \in S_n$. But, comparing the dimensions of the residue class rings, it follows that $\langle H \rangle = \mathcal{M}' = \mathcal{M}^\sigma \cap \mathbb{Q}[X_{\{1,\ldots,j\}}]$. Seeing their stabilizers, σ is the identity and $h_j = f_j$ $\square$

By the similar manner and considering $\mathbb{Q}[X_{E_j}]$, we have alternative test for h_j in the case where Hensel liftings are done over R'_{2k}, see Remark 1.

Theorem 6. *Let $h_j^*, \ldots, h_{s-1}^*, h_j$ be constructed polynomials by Hensel lifting using R'_{2k}, where $E_j = \{e_1, \ldots, e_{s-1}, e_s = j\}$. We have $h_j = g_j$ if and only if* $\mathrm{NF}(f(x_{e_m}), \{g_1^*, \ldots, g_{s-1}^*, h_j\}) = 0$ *for all m, $1 \leqslant m \leqslant s$.*

5 Algorithms

Here we give a brief survey on the algorithms underlying of this method. We first give an algorithm for the construction of a *computation scheme*, then we give an algorithm for the computation of *splitting ideals*.

5.1 A database of computation schemes

Given a subgroup G of S_n the following algorithm computes a corresponding *computation scheme*.

Algorithm 1: ComputationScheme(G)

Step 1 Compute the degrees $\deg_i(g_i)$ for $i = 1, \ldots, n$ (see Proposition 1).
Step 2 Apply the *Cauchy's technique* (see Lemma 1). Let $\mathcal{I}$ be the set of integers corresponding to the indexes of the g_i which cannot be obtained with this technique.
Step 3 For each integer i in $\mathcal{I}$, compute a minimal i-relation and store it in $\mathcal{E}$.
Step 4 Apply *transporter technique* on the i-relations in $\mathcal{E}$. Let $\mathcal{E}$ be the set of i-relations corresponding to the g_i which must be computed.
Return $\mathcal{E}$ with the techniques for retrieving the other polynomials.

The set $\mathcal{E}$ depends only on the choice of the representative for G and on the chosen i-relations in **Step 3**. This set represents all the linear systems which are solved in our method. Thus, a measure of complexity is given by $|\mathcal{E}| = \sum_{E \in \mathcal{E}} D(E)$ and, in Algorithm 1, we compute $\mathcal{E}$ with minimal $|\mathcal{E}|$.

Definition 6. *For a given sub-group G of S_n, the minimal value of $|\mathcal{E}|$ is called the* c-size *of G and is denoted by $c(G)$.*

A conjugate of G with minimal c-size is called *c-minimal*. In a conjugacy class there may be a big difference, in term of c-size, between two of its representatives. For example, in the conjugacy class of $[2^4]S_4$ there are two representatives G_1 and G_2 with $c(G_1) = 8$ and $c(G_2) = 632$.

5.2 Algorithm for the computation of splitting fields

Assume that the *computation scheme* of G_f is pre-computed (w.l.o.g. we can choose a representative of G_f which is c-minimal). We also suppose that all transversals of groups needed in our algorithm are pre-computed.

Given the polynomial f of degree n, our method for computing a Gröbner basis $\mathcal{G} = \{g_1, g_2, \ldots, g_n\}$ is describe with the following algorithm. We give only the algorithm where early detections are used. One could use the theoretical bounds by applying some minor modifications (fix the exponent of p, cancel the *early detection* tests). A variant of Algorithm 2 is presented in [15].

Algorithm 2: SplittingIdeal($\mathcal{G}^{(k_0)}$,G_f,p)

Let $\mathcal{I}$ be the indexes of the g_i we have to compute with linear systems.
for $i = 1$ to n **do**
  if $i \in \mathcal{I}$ **then**
    Construct/Solve $\mathcal{S}$ the linear system mod p^{k_0+1} corresponding to E_i.
    S1: try to convert the solution s_i of $\mathcal{S}$ to a rational polynomial h_i
    if the conversion of s_i above succeed **and** h_i satisfies the correctness test
    then The polynomial h_i is g_i.
    else Apply an Hensel lifting to s_i and goto step **S1**.
  else
    Apply a Cauchy/Transporter technique in order to obtain g_i from g_j with $j < i$
  end if
end for
Return $\mathcal{G}$, G_f.

5.3 Complexity analysis

In this section, we study the complexity of Algorithm 2 *focusing on effects of the quantity* $c(G)$. We assume that a database containing a computation scheme of a c-minimal representative of each conjugacy class is already known. For *simplifying our analysis and extracting its typical behavior related to* $c(G)$, we choose liftings over R'_{2k} (see Remark 1) and consider a case where $k_0 = 0$ in input and EEA with pseudo division always works in the first step of the lifting. Also we assume that $\overline{N} = 1$, as this property is desired in efficient Galois group computation [9, 21], and $\log\log(B_0)$ is quite small compared with n for B_0 defined in Lemma 2.

Since we use the *early detection strategy*, the complexity of our algorithm also depends on the size of the coefficients of the output $\mathcal{G}$. Let B_{true} be the maximum of the absolute values of denominators and numerators of coefficients of g_j^* and g_i appearing in the computation. By Lemma 2, the theoretical bound B_i on the coefficients of g_i can be also on those of g_j^*. Thus, B_{true} is supposed very much smaller than $B_1, \ldots, B_n$. In the sequel, for each integer $k \geqslant 0$, we denote by $\mathbb{M}(k)$ the cost of arithmetic over $\mathbb{Z}/p^{k+1}\mathbb{Z}$ as number of word operations. As the size of necessary p^{k+1} tends to be huge, we may apply fast multiplication techniques over $\mathbb{Z}/p^{k+1}\mathbb{Z}$. On the other hand, as the size n which can be handled here is not so large, we use ordinary techniques for polynomial multiplication.

We now sketch the complexity of each step of Algorithm 2 for computing one polynomial g_i with respect to the pre-computed i-relation $E_i = \{e_1, \ldots, e_s\}$. We note that the number of iterations is bounded by $O(\log\log(B_{true}))$.

Linear algebra: To compute a polynomial $g_i \mod p$ with respect to the i-relation E_i, we have to construct the matrix $\bar{M}_i$ and solve $-\bar{V}_i = \bar{M}_i\bar{A}_i$ for $\bar{A}_i$. Under the assumption, the matrix $\bar{M}_i$ is constructed directly as a matrix over $\mathbb{F}_p$, and its construction takes $O(D(E_i)^2\mathbb{M}(0))$ word operations. Then we solve the resulted $D(E_i) \times D(E_i)$ linear system which requires $O(D(E_i)^\omega\mathbb{M}(0))$ word operations. (Here, ω represents a feasible matrix multiplication exponent and $2 \leqslant \omega \leqslant 3$, see [20].) Thus, in total, it takes $O(D(E_i)^\omega\mathbb{M}(0))$ word operations.

Hensel lifting: At each step k, $g_i \bmod p^k$ is lifted to $g_i \bmod p^{2k}$ and this computation is executed over $R'_{2k} = (\mathbb{Z}/p^{2k}\mathbb{Z})[X_{E_i} \setminus \{x_i\}]/\langle g_1^*, \ldots, g_{s-1}^*\rangle$ (see Remark 1). At this step, by using ordinary polynomial multiplication, it takes $O(n^2)$ arithmetic operations over R'_{2k}, and hence it takes $O(n^2D(E_i)^2\mathbb{M}(2k-1))$ word operations. At the first step of the lifting, we also compute s, t in $R_1[x_i]$ such that (Bézout relation) $s\pi_p(f(x_i)) + t(g_i \bmod p) = 1$ by EEA, which takes $O(n^2D(E_i)^2\mathbb{M}(0))$ word operations. As we use quadratic Hensel construction, the total cost is dominated by the same order for the final step, and thus, it takes $O(n^2D(E_i)^2\mathbb{M}(\log(B_{true})))$ word operations.

Rational reconstruction: As each coefficient $a_j^{(i)}$ of $g_i \bmod p^{2k}$ can be converted to a rational number by EEA of $a_j^{(i)}$ and p^{2k}. By applying fast GCD computation techniques [20], it takes $O(\mathbb{M}(\log(B_{true}))\log\log(B_{true}))$ word operations for each $a_j^{(i)}$, as we can use the same symbol $\mathbb{M}(\log(B_{true}))$ for the cost of one multiplication of integers of word size $O(\log(B_{true}))$. Then, in total, it

takes $O(D(E_i)\mathbb{M}(\log(B_{true}))(\log\log(B_{true}))^2)$ word operations. From the computed bound in Lemma 2 for B_{true}, $\log\log(B_{true}) = O(n\log(n))$ and the total cost of rational reconstruction is dominated by the cost of Hensel construction.
Auxiliary computation: As the computation of g_i is executed over R'_{2k}, $g_1^*, \ldots, g_{i-1}^*$ must already computed. (Some can be easily converted from already constructed g_j, $j < i$.) Each g_j^* is constructed by linear algebra and Hensel construction in the same manner as g_i, and it takes $O(D_j^\omega \mathbb{M}(0) + n^2 D_j^2 \mathbb{M}(\log(B_{true}))$ word operations, where $D_j = \prod_{\ell=1}^{j} d(E_i)_{e_\ell}$. As E_i is set to be minimal, $d(E_i)_{e_j} \geqslant 2$ for each $j < s$ and it follows easily that $\sum_{\ell=1}^{s-1} n^2 D_j^2 = O(n^2 D(E_i)^2)$ and $\sum_{\ell=1}^{s-1} D_j^\omega = O(D(E_i)^\omega)$. Hence the cost of auxiliary computation is dominated by the cost of Hensel construction steps for g_i.
Normal form computation: We use the same notation as in Auxiliary computation. For the correctness of g_i, normal forms of $f(x_{e_1}), \ldots, f(x_{e_{s-1}}), f(x_i)$ with respect to $\{g_1^*, \ldots, g_{s-1}^*, g_i\}$ are computed. These computations can be executed via powers of x_{e_j} and so it takes $O(\log(n)D_1^2 + \cdots + \log(n)D_{s-1}^2) = O(\log(n)D(E_i)^2)$ arithmetic operations over $\mathbb{Z}$.

Thus, by summing the quantities above among all the polynomials g_i, we obtain the following result:

Theorem 7. *Algorithm 2 with $k_0 = 0$ takes*

$$O(c(G)^\omega \mathbb{M}(k_0) + n^2 c(G)^2 \mathbb{M}(\log(B_{true})) + L)$$

word operations, where L is the total cost of normal form computations in correctness tests. Letting B' be the maximum of absolute values of integers appearing in normal form computations, L can be bounded by $O(\log(n)c(G)^2\mathbb{M}(\log(B'))\log\log(B_{true}))$. (When k_0 is general we have almost the same result.) Moreover, for cases where the word size of B' is the almost same order as that of B_{true}, the above estimation can be simplified to $O(c(G)^\omega\mathbb{M}(k_0) + n^2c(G)^2\mathbb{M}(\log(B_{true}))$.

As B_{true} is a bound on coefficients of g_j^* and g_i, it might be greater than the actual bound B on coefficients of g_i's. But, in many cases for computation of successive extensions, the final element has coefficients of the maximal absolute value. Thus, for representing actual behaviors of computation, it may be allowed to use B_{true} instead of B.

6 Experiments and remarks

We have implemented Algorithm 2 with the *computer algebra system* Magma (version 2.11) in the case of an irreducible monic integral polynomial. We choose Magma since it has all the functionalities needed (Galois group computation, multivariate polynomial ring, permutation group). We have computed a database of c-minimal representatives (with their *computation scheme*) of each conjugacy class of transitive groups of degree up to 11. The experiments we made show that this first implementation is already very efficient. **Choice of the prime** p:

By Tchebotarev's density theorem, it is possible to compute a prime p such that $\overline{N} = 1$ and it may find among $\mathcal{O}(|G_f|)$ number of primes. In our implementation, we choose the smallest such prime. One can see in the table that the time taken by this procedure is not significant compared with the rest of the computation.

The power k_0: In our implementation we take $k_0 = 10$. In this case, none of the tests presented in table need to be lifted after the linear resolution: the *early detection tests* pass. We will investigate, in a future work, some other power k_0 and compare the efficiency with the case where the Hensel lifting is needed.

Experiments timings: We tested polynomials from the database `galpols` of MAGMA. We give, for each example, the name of the group G in Butler and McKay's nomenclature, the order of G and the integer $c(G)$ (as the sum of the i-relations degrees). The column `Tcheb.` shows the timings of computing a prime p such that $\overline{N} = 1$, the column p gives this prime. The column `Galois` shows the timings of computing the Galois group, `Matrix/Solve` those for constructions and resolutions of the matrices respectively, `NF` the timings for the normal forms computations and `Total` the total timing of the procedure. The measurements were made on a personal computer with a 1.5Ghtz Intel Pentium 4 and 512MB of memory running GNU/Linux. As one can see, the size of $c(G)$ and the size of p^{k_0} heavily influenced the timings of constructions and resolutions of matrices like Theorem 7 shows. When $c(G)$ is big, two cases are possible: few big matrices to compute or a lot of little matrices to compute. The first case is more time consuming than the second. This is why there are some differences between examples with same size of $c(G)$ and p^{k_0} (for example, see the lines $8T_{37}$ and $6T_{15}$).

group	$\|G\|$	$c(G)$	Tcheb.	p	Galois	Matrix/Solve	NF	Total
$6T_{12}$	60	60 + 60	0.13	929	0.06	0.22 / 0.17	0.04	0.66
$6T_{13}$	72	12	0.11	619	0.03	0.01 / 0.01	0	0.18
$6T_{14}$	120	120	0.15	1447	0.05	0.44 / 0.44	0.06	1.18
$6T_{15}$	360	360	0.22	2437	0.0	3.69 / 6.51	0.21	10.79
$7T_5$	168	42	0.19	1879	0.06	0.05 / 0.04	0.04	0.41
$8T_{32}$	96	8 + 96 + 96	0.34	3413	0.13	0.55 / 0.59	0.14	1.870
$8T_{33}$	96	96 + 32	0.23	2099	0.14	0.32 / 0.3	0.34	1.42
$8T_{34}$	96	24 + 24 + 95	0.09	229	0.14	0.34 / 0.24	0.09	0.99
$8T_{35}$	128	8 + 16	0.31	2909	0.06	0.01 / 0.01	0.01	0.45
$8T_{36}$	168	168 + 168	0.06	211	0.14	1.78 / 1.59	1.63	5.360
$8T_{37}$	168	168 + 168	0.31	2969	0.1	1.76 / 2.26	1.15	5.72
$8T_{38}$	192	96 + 8	0.26	2503	0.1	0.29 / 0.29	0.05	1.09
$8T_{39}$	192	8 + 192	0.16	947	0.06	1.14 / 1.44	0.2	3.11
$8T_{41}$	192	24 + 96	0.4	4271	0.13	0.33 / 0.32	0.06	1.32
$8T_{42}$	288	24 + 24	0.46	5051	0.1	0.05 / 0.02	0.02	0.71
$8T_{43}$	336	336	0.29	3209	0.12	3.48 / 6.09	3.84	14.0
$8T_{44}$	384	8	1.05	14071	0.06	0.01 / 0.01	0.05	1.24
$8T_{45}$	576	24 + 576	0.36	3719	0.06	10.21 / 22.87	1.18	35.1
$8T_{46}$	576	24 + 576	0.56	6269	0.1	10.25 / 23.72	1.1	36.14
$8T_{47}$	1152	24	1.27	17299	0.05	0.03 / 0.02	0.0	1.44
$8T_{48}$	1344	336	5.56	78497	0.08	3.56 / 8.56	20.33	38.3
$9T_{21}$	162	54 + 54	0.59	6047	1.08	0.2 / 0.16	0.54	2.72
$9T_{22}$	162	27 + 54	0.12	461	0.16	0.13 / 0.09	0.08	0.65
$9T_{23}$	297	216 + 72	0.16	727	0.31	3.13 / 5.17	1.37	10.4
$9T_{24}$	324	18 + 108	0.24	1801	1.07	0.4 / 0.38	2.23	4.45
$9T_{25}$	324	27 + 324	0.16	953	1.03	3.41 / 5.49	0.33	10.63
$9T_{26}$	432	72	0.98	10273	0.3	0.18 / 0.16	7.43	9.15
$9T_{27}$	504	504	0.79	10103	0.42	7.98 / 18.6	105.49	133.64
$9T_{28}$	648	27	0.33	3037	1.38	0.03 / 0.02	0.01	1.87
$9T_{29}$	648	18 + 648	0.75	7883	0.43	13.17 / 38.74	1.44	55.21
$9T_{31}$	1296	18	0.33	2801	1.0	0.01 / 0.01	0.03	1.53
$9T_{32}$	1512	1512 + 1512	0.46	5167	0.27	142.17 / 608.1	1761.84	2523

7 Conclusion and future works

We have presented a new method, with theoretical and practical aspects, for the computation of the splitting field of a polynomial f where the knowledge of the action of the Galois group over p-adic approximations of its roots is used.

We have introduced the notion of *computation scheme*. This new approach seems a good way for efficient computation of splitting fields. This framework is not limited to be used with linear systems solving. For example, we will study

the integration of sparse interpolation formulas (like the dense ones in [6, 12]) in our algorithm. Also, it would be interesting to study the possibility of using this approach in a dynamical strategy like the one of MAGMA (see [19]).

References

1. I. Abdeljaouad, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *AAECC*, 15(3-4):279–294, 2004.
2. H. Anai, M. Noro, and K. Yokoyama. Computation of the splitting fields and the Galois groups of polynomials. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, volume 143 of *Progr. Math.*, 29–50. Birkhäuser, Basel, 1996.
3. J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118:23–40, 1997. Algorithms for algebra (Eindhoven, 1996).
4. Ph. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6):635–651, 2000. Algorithmic methods in Galois theory.
5. T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. In cooperation with H. Kredel.
6. X. Dahan and É. Schost. Sharp estimates for triangular sets. In *Proceedings of ISSAC '04*, pages 103–110, New York, NY, USA, 2004. ACM Press.
7. J. H. Davenport, Y. Siret, and E. Tournier. *Computer algebra*. Academic Press Ltd., London, second edition, 1993.
8. K. Geissler. *Berechnung von Galoisgruppen über Zhal- und Funktionenkörpern*. PhD thesis, Universität Berlin, 2003.
9. K. Geissler and J. Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30(6):653–674, 2000. Algorithmic methods in Galois theory.
10. L. Langemyr. Algorithms for a multiple algebraic extension. II. In *Proceedings of AAECC-9*, volume 539 of *LNCS*, pages 224–233. Springer, Berlin, 1991.
11. D. Lazard. Solving zero-dimensional algebraic systems. *J. Symbolic Comput.*, 13(2):117–131, 1992.
12. M. Lederer. Explicit constructions in splitting fields of polynomials. *Riv. Mat. Univ. Parma (7)*, 3*:233–244, 2004.
13. S. Orange, G. Renault, and A. Valibouze. Calcul efficace de corps de décomposition. LIP6 Research Report 005, Laboratoire d'Informatique de Paris 6, 2003.
14. M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge Univ. Press, Cambridge, 1989.
15. G. Renault. *Calcul efficace de corps de décomposition*. PhD thesis, Université Paris 6, 2005.
16. N. Rennert and A. Valibouze. Calcul de résolvantes avec les modules de Cauchy. *Experiment. Math.*, 8(4):351–366, 1999.
17. É. Schost. *Sur la résolution des systèmes polynomiaux à paramètres*. PhD thesis, École polytechnique, 2000.
18. R. Stauduhar. The determination of galois groups. *Math. Comp.*, 27:981–996, 1973.
19. A. K. Steel. A new scheme for computing with algebraically closed fields. In *ANTS-V*, Volume 2369 of *LNCS*, pages 491–505. Springer, Berlin, 2002.
20. J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.
21. K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118:617–636, 1997. Algorithms for algebra (Eindhoven, 1996).