Finding Roots of Unity among Quotients of the Roots of an Integral Polynomial

Kazuhiro Yokoyama *
ISIS, FUJITSU LABORATORIES LIMITED
140 Miyamoto, Numazu-shi, Shizuoka 410-03, Japan.
momoko@iias.flab.fujitsu.co.jp

Ziming Li †
Research Institute for Symbolic Computation
Johannes Kepler University, A-4040 Linz, Austria.
Ziming.Li@risc.uni-linz.ac.at

István Nemes ‡
Research Institute for Symbolic Computation
Johannes Kepler University, A-4040 Linz, Austria.
Istvan.Nemes@risc.uni-linz.ac.at

Abstract

We present an efficient algorithm for testing whether a given integral polynomial has two distinct roots α, β such that α/β is a root of unity. The test is based on results obtained by investigation of the structure of the splitting field of the polynomial. By this investigation, we found also an improved bound for the least common multiple of the orders of roots of unity appearing as quotients of distinct roots.

1 Introduction

Two distinct algebraic numbers α, β form a *unitary pair* if α/β is a root of unity. By the *order* of a unitary pair (α, β) we mean the order of the multiplicative group generated by α/β. We consider a univariate polynomial $f(x)$ of degree n with non-zero constant over the rational number field $\mathbf{Q}$. We say that f *has a unitary pair* if there is a unitary pair among the roots of f.

We present efficient solutions for the following problems.

Problem 1 *Decide whether a polynomial has a unitary pair.*

Problem 2 *If a polynomial has a unitary pair, compute the order of this pair.*

The problem of deciding whether a polynomial has a unitary pair originates in the theory of linear recurrence sequences. By a classical result, it is necessary for the appearance of infinitely many zeros in a linear recurrence sequence that the characteristic polynomial of the sequence has a unitary pair, and if the sequence has infinitely many zeros, then the sequence of the indices of the zero terms, up to finitely many indices, is a union of finitely many arithmetic progressions. In this case the least common multiple (LCM) of the orders of unitary pairs is a multiple of the LCM of the differences of the arithmetic progressions [1].

Problem 1 can be considered also as one of the simplest ways of finding an abelian extension field in the minimal splitting field of a polynomial. If a polynomial has a unitary pair (α, β), the field obtained by adjoining all α/β is cyclotomic, contained in the minimal splitting field of the polynomial.

A straightforward approach to the problems is to compute $\bar{f}(x) = \mathrm{res}_y(f(y), f(xy))/(1-x)^n$, whose roots are exactly the quotients of roots of $f(x)$, and as a next step to find cyclotomic factors of $\bar{f}(x)$. The resultant computation in this method tends to be time-consuming for large n. In [1] the resultant $\bar{f}(x)$ was used for obtaining a bound on the LCM of the orders of unitary pairs of f.

Recently Ge [3] found a solution for a long standing problem of computational number theory. From his solution we can derive algorithms for Problem 1 and Problem 2. However, since the problems we are going to solve are very special instances, they deserve particular study.

The main contribution of our paper is Theorem 3.1 which gives a bound on the smallest order of unitary pairs. Based on this result we propose an efficient algorithm for solving Problem 1, which can be extended for handling Problem 2. Another useful result is Corollary 3.3 which improves the bound found by Berstel and Mignotte [1].

2 Preliminaries

Throughout this paper we consider polynomials over $\mathbf{Q}$ and also the ground field is assumed to be $\mathbf{Q}$. For a polynomial $g(x)$ we denote by Ω_g the set of all roots of g and by G_g the Galois group of g, Ω and G will stand for Ω_f and G_f, respectively. The group G_g acts on the minimal splitting field of g and particularly, it acts on Ω_g as a permutation group.

To solve Problem 1, we need only to consider distinct non-zero roots of $f(x)$. Therefore in the rest of the paper $f(x)$ will stand for a square-free, monic polynomial.

*Current address : Research Institute for Symbolic Computation, Johannes Kepler University, A-4040 Linz, Austria.

†Supported in part by "Fonds zur Förderung der wiss. Forschung", Project P9181-TEC PoSSo.

‡Supported in part by FUJITSU LABS. LTD.

ISSAC'95 - 7/95 Montreal, Canada

2.1 Relation between roots

We define α, β in Ω_g to be equivalent, if (α, β) is a unitary pair or $\alpha = \beta$. It is immediate that this relation is an equivalence relation and elements of G_g map equivalence class to equivalence class.

If g is irreducible, then the equivalence classes are conjugate to each other by the action of G_g. Following [8] we say that such conjugate equivalence classes form a *complete block system.* We shall make use of one property of complete block systems: the size of each block is the same and consequently it divides $\deg(g)$.

2.2 Cyclotomic extensions

For ζ root of unity let the order of ζ be its order in the multiplicative group of the complex numbers and denote it by $\mathrm{ord}(\zeta)$. By the degree of ζ we mean the extension degree $|\mathbf{Q}(\zeta) : \mathbf{Q}|$. We recall $\deg(\zeta) = \phi(\mathrm{ord}(\zeta))$, where ϕ is the Euler's function. The minimal splitting field of $x^m - 1$ is called the *cyclotomic field of order* m.

Let $g(x)$ be irreducible with root α. We denote by $\mathbf{K}_g$ the largest cyclotomic field included in $\mathbf{Q}(\alpha)$. Since $\mathbf{K}_g$ is a Galois extension, $\mathbf{K}_g$ does not depend on the choice of α.

Definition 2.1 *For an irreducible polynomial g, we call the order of $\mathbf{K}_g$ the* cyclotomic order *of g and denote it by r_g.*

Since $\mathbf{K}_g$ is a subfield of $\mathbf{Q}(\alpha)$, $\phi(r_g) = |\mathbf{K}_g : \mathbf{Q}|$ divides $\deg(g)$.

Definition 2.2 *By the* degree *of the unitary pair (α, β) we mean the degree of α/β.*

Definition 2.3 *The unitary order f is the LCM of the orders of unitary pairs of f if f has a unitary pair, and 1 otherwise.*

3 Bounds on orders of unitary pairs

We consider bounds for orders of unitary pairs of $f(x)$.

Theorem 3.1 *If f has a unity pair, then it has a unitary pair whose order is not greater than $3n^{3/2}$.*

Theorem 3.2 *If the irreducible factors of f are $f_1, \ldots, f_\ell$ with degrees $n_1, \ldots, n_\ell$ and with cyclotomic orders $r_1, \ldots, r_\ell$, respectively, then the unitary order of f divides $LCM(n_1, \ldots, n_\ell) \times LCM(r_1, \ldots, r_\ell)$.*

Corollary 3.3 *The unitary order of f is bounded by $exp(2\sqrt{6n \log n})$. Moreover, if f is irreducible, then the unitary order of f is bounded by $3n^{5/2}$.*

Proof By Theorem 3.2, the unitary order of f is a divisor of $LCM(n_1, \ldots, n_\ell) \times LCM(r_1, \ldots, r_\ell)$. By applying the argument in the proof of (Theorem 1 in [1]), $LCM(n_1, \ldots, n_\ell)$ and $LCM(r_1, \ldots, r_\ell)$ are both bounded by $exp(\sqrt{6n \log n})$.

If f is irreducible, then the order of f divides $n r_f$. The statement for irreducible f can be shown by this fact and by the argument in the proof of Theorem 3.1. □

The bound found by Berstel and Mignotte [1] is $exp(2n\sqrt{3 \log n})$. This was improved by [7], where polynomials with algebraic number coefficients were considered, in the special case of rational polynomials the bound is 2^{n+1}. The bound we obtained in Corollary 3.3 is an improvement also of this latter result.

Remark. We note that even with the application of this improved bound to decide whether a linear recurrence sequence has infinitely many zeros still needs exponential time. However, having a polynomial bound on the unitary order of irreducible polynomials, if the characteristic polynomial of the considered sequence is irreducible, then the decision can be carried out in polynomial time.

3.1 Proofs

For σ in G and for γ in the minimal splitting field of f, we denote by γ^σ the action of σ on γ and we denote by G_γ the stabilizer of γ in G.

Lemma 3.4 *If f has a unity pair, then it has a unitary pair whose degree is not greater than n.*

Proof Assume that f has a unitary pair (α, β) and let Λ be the equivalence class of f containing this pair. Let g be an irreducible factor of f. Considering how many roots of g lies in Λ, the proof splits into two parts.

Case 1. For any g there is at most one root of g in Λ.
Let g and h be those irreducible factors of f which have α and β as roots, respectively. Set $\zeta = \alpha/\beta$. It suffices to show

$$\mathbf{Q}(\alpha) = \mathbf{Q}(\beta), \tag{1}$$

because it implies $\zeta \in \mathbf{Q}(\alpha)$ which shows

$$\deg(\zeta) = |\mathbf{Q}(\zeta) : \mathbf{Q}| \leq |\mathbf{Q}(\alpha) : \mathbf{Q}| = \deg(g) < n.$$

To prove (1) we show $G_\alpha = G_\beta$. Note that G acts on Ω_g and also on Ω_h. With an arbitrary σ from G_α,

$$\beta\zeta = \alpha = \alpha^\sigma = (\beta\zeta)^\sigma = \beta^\sigma \zeta^\sigma.$$

Thus, $\beta^\sigma = \beta\zeta(\zeta^\sigma)^{-1}$. Since $\zeta(\zeta^\sigma)^{-1}$ is a root of unity, we see that (β, β^σ) is a unitary pair. Since β^σ is also a root of g and there is at most one root of g in Λ, $\beta = \beta^\sigma$ and hence $G_\alpha \subset G_\beta$. Replacing the roles of α and β, we can show also $G_\beta \subset G_\alpha$.

Case 2. There is a g with at least two roots in Λ.
Since $\deg(g) \leq n$, to prove the lemma it is enough to show that any irreducible polynomial g that has a unitary pair, has a unitary pair whose degree is not greater than $\deg(g)$. For the sake of simplicity, in the sequel we consider f as an irreducible polynomial instead of g.

Since f is irreducible, the equivalence classes form a complete block system and so every block has the same size, say m. By the definition of the equivalence we can write $\Lambda = \{\alpha\zeta_1, \alpha\zeta_2, \ldots, \alpha\zeta_m\}$, where ζ_i's are some roots of unity. Let λ be the product of the elements of Λ and $\zeta_0 = \prod_{i=1}^m \zeta_i$. Then ζ_0 is a root of unity and $\lambda = \alpha^m \zeta_0$.

By the fact that Λ is a block, the set-wise stabilizer G_Λ of Λ in G acts transitively on Λ and G_Λ contains G_α. Then G_α fixes both λ and α^m. This implies that G_α fixes ζ_0 and

$$\lambda, \zeta_0 \in \mathbf{Q}(\alpha). \tag{2}$$

Thus, we have the following tower of fields

$$\mathbf{Q}(\alpha^m) \subset \mathbf{Q}(\lambda, \zeta_0) \subset \mathbf{Q}(\alpha). \tag{3}$$

Moreover, we can show

$$G_\lambda = G_\Lambda. \tag{4}$$

To prove (4), it suffices to see that every element σ in G_λ stabilizes the set Λ. Consider an element σ in G_λ and let $\alpha' = \alpha^\sigma$. Then,

$$\alpha^m \zeta_0 = \lambda = \lambda^\sigma = (\alpha^m \zeta_0)^\sigma = (\alpha^\sigma)^m \zeta_0{}^\sigma = \alpha'^m \zeta_0{}^\sigma.$$

Thus, $\alpha'^m = \alpha^m \zeta'$, where $\zeta' = (\zeta_0{}^\sigma)^{-1}\zeta_0$ is a root of unity. By letting k the order of ζ', we have $(\alpha'/\alpha)^{mk} = 1$ and so $\alpha' \in \Lambda$. This implies that $\Lambda^\sigma \cap \Lambda \neq \emptyset$, hence $\Lambda^\sigma = \Lambda$.

To complete the proof of the lemma, we consider (3) and distinguish the cases when $\mathbf{Q}(\alpha^m)$ and $\mathbf{Q}(\alpha)$ coincides or not. First assume $\mathbf{Q}(\alpha^m) = \mathbf{Q}(\alpha)$. By (3), $\mathbf{Q}(\lambda, \zeta_0) = \mathbf{Q}(\alpha)$ and so $G_\lambda \cap G_{\zeta_0} = G_\alpha$. Since $\mathbf{Q}(\zeta_0)$ is a Galois extension, G_{ζ_0} is a normal subgroup of G. Therefore, $G_\alpha = G_\lambda \cap G_{\zeta_0}$ is also a normal subgroup of G_λ. Since G_Λ acts transitively on Λ and $G_\Lambda = G_\lambda$ by (4), for each α_i in Λ, there exists $\sigma_i \in G_\lambda$ such that $\alpha^{\sigma_1} = \alpha_i$, hence $G_{\alpha_i} = G_{\alpha^{\sigma_i}} = G_\alpha{}^{\sigma_i} = G_\alpha$. Therefore, $\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha_i)$ and $\zeta_i \in \mathbf{Q}(\alpha)$, hence

$$\deg(\zeta_i) = |\mathbf{Q}(\zeta_i) : \mathbf{Q}| \leq |\mathbf{Q}(\alpha) : \mathbf{Q}| = n.$$

Finally consider the case $\mathbf{Q}(\alpha^m) \neq \mathbf{Q}(\alpha)$. We have $\sigma \in G_{\alpha^m} \setminus G_\alpha$, and $(\alpha^m)^\sigma = (\alpha^\sigma)^m = \alpha^m$. This implies that (α, α^σ) is a unitary pair whose order divides m and so also divides n. Therefore, its degree is smaller than n. □

Proof of Theorem 3.1. Theorem 3.1 is implied by Lemma 3.4 using the fact that $d \leq 3\phi(d)^{3/2}$ for $d \geq 2$ (Corollary in [2]). □

Lemma 3.5 *If f is irreducible, then the unitary order of f divides $n \times r_f$.*

Proof We have to consider only the case where f has a unitary pair. Since f is irreducible, like in Case 2 at the proof of Lemma 3.4, we can use arguments of that proof. Let (α, β) be a unitary pair and Λ be the equivalence class with m elements containing α, β. It suffices to show that with $\zeta = \alpha/\beta$, $\mathrm{ord}(\zeta)$ divides $n r_f$. Since f is irreducible, m divides n, thus it is enough to see that $\mathrm{ord}(\zeta)$ divides $m r_f$, i.e.

$$\alpha^{m r_f} = \beta^{m r_f}. \tag{5}$$

To establish (5) let λ be the product of the elements of Λ, and let $\zeta_0 = \lambda/\alpha^m$ and $\zeta_0' = \lambda/\beta^m$. Clearly, ζ_0 and ζ_0' are roots of unity and by (2), $\zeta_0 \in \mathbf{Q}(\alpha)$ and similarly $\zeta'_0 \in \mathbf{Q}(\beta)$. Thus both ζ_0 and ζ'_0 are from $\mathbf{K}_f$, consequently $\zeta_0^{r_f} = \zeta'_0{}^{r_f} = 1$ which implies (5). □

Proof of Theorem 3.2. We have to consider only the case where f has a unitary pair (α, β). It suffices to show that

$$\mathrm{ord}(\zeta) \mid LCM(n_1, \ldots, n_\ell) LCM(r_1, \ldots, r_\ell), \tag{6}$$

where $\zeta = \alpha/\beta$. If α and β are roots of the same irreducible factor, Lemma 3.5 implies (6). Thus, we need to consider only the case where α and β are roots of distinct factors. To conclude (6) we apply the following lemma. □

Lemma 3.6 *Let g and h be distinct irreducible polynomials with $\alpha \in \Omega_g$ and $\beta \in \Omega_h$. If (α, β) is a unitary pair, then*

$$\mathrm{ord}(\alpha/\beta) \mid LCM(\deg(g), \deg(h)) LCM(r_g, r_h). \tag{7}$$

Proof Let $f(x) = g(x)h(x)$ and Λ be the equivalence class containing α, β. Let Λ_g and Λ_h be the equivalence class of α in Ω_g and that of β in Ω_h, respectively. Clearly, $\Lambda = \Lambda_g \cup \Lambda_h$. Let $m_g = |\Lambda_g|$ and $m_h = |\Lambda_h|$. Since the action of the Galois group G is compatible with the equivalence relation, we obtain

$$G_\Lambda = G_{\Lambda_g} = G_{\Lambda_h} \tag{8}$$

for the set-wise stabilizers.

To prove (7) it suffices to show $\alpha^{m r} = \beta^{m r}$, where $m = LCM(m_g, m_h)$ and $r = LCM(r_g, r_h)$, because for irreducible g and h we have $m_g \mid \deg(g)$ and $m_h \mid \deg(h)$.

On the analogy of the notation introduced in the proof of Lemma 3.4, let λ_g and λ_h be the product of the elements of Λ_g, and that of Λ_h. Let $\zeta_{g,0} = \lambda_g/\alpha^{m_g}, \zeta_{h,0} = \lambda_h/\beta^{m_h}$. We can apply (2) and (4) for g and h. By (2), $\zeta_{g,0}$ belongs to $\mathbf{Q}(\alpha)$ and so also to $\mathbf{K}_g$, similarly $\zeta_{h,0}$ belongs to $\mathbf{K}_h$. Moreover, by (2), (4) and (8), we have $G_{\lambda_g} = G_{\lambda_h}$ and $\mathbf{Q}(\lambda_g) = \mathbf{Q}(\lambda_h) \subset \mathbf{Q}(\alpha) \cap \mathbf{Q}(\beta)$.

Consider powers of λ_g and λ_h

$$\lambda_g^{m/m_g} = \alpha^m \zeta_{g,0}^{m/m_g} \quad \text{and} \quad \lambda_h^{m/m_h} = \beta^m \zeta_{h,0}^{m/m_h}. \tag{9}$$

Since $\zeta_{g,0} \in \mathbf{K}_g$, $\zeta_{g,0}^r = 1$ which shows $\lambda_g^{m r/m_g} = \alpha^{m r}$. Similarly, we have $\lambda_h^{m r/m_g} = \beta^{m r}$. Because α/β is a root of unity, from (9) we see that $\zeta' = \lambda_g^{m/m_g}/\lambda_h^{m/m_h}$ is a root of unity. Since $\mathbf{Q}(\lambda_g) = \mathbf{Q}(\lambda_h)$, ζ' belongs to $\mathbf{Q}(\lambda_h)$ and so also to $\mathbf{K}_h$. Thus, we have $\zeta'^r = 1$. This implies $\alpha^{m r} = \lambda_g^{m r/m_g} = \lambda_h^{m r/m_h} = \beta^{m r}$. □

4 Deciding the existence of unitary pairs

Based on Lemma 3.4 we are able to give an efficient method for solving Problem 1. Because, by this lemma it suffices to test whether f has a unitary pair whose degree is not greater than n. From now on, we deal with a square-free integral polynomial $f(x)$ with non-zero constant and let $f(x) = \sum_{i=0}^n a_i x^i = a_n \prod_{i=1}^n (x - \alpha_i)$.

Let $\Phi_d(x)$ denote the d-th cyclotomic polynomial and $\mathcal{C}_n$ the set of $\Phi_d(x)$ with degree not greater than n. We write c_n for the number of elements of $\mathcal{C}_n$. We set $\mathcal{D}_n = \{d \mid d \geq 2 \text{ and } \phi(d) \leq n\}$ and $d_n = max(\mathcal{D}_n)$. In [2] it is shown that $d_n \leq 3n^{3/2}$ and also $d_n \leq 5n$ if $d_n < 3000$.

4.1 Algorithms

We propose two methods for solving Problem 1.

Method 1 Construct an integral polynomial $\hat{f}(x) = c \prod_{1 \leq i \neq j \leq n} (x - \alpha_i/\alpha_j)$, where c is an integer. By the definition of resultant, $\hat{f}(x)$ can be taken either as $\mathrm{res}_y(f(y), f(y/x)x^n)/(x-1)^n$ or as $\bar{f}$ from the introduction.

Once we have computed $\hat{f}(x)$, then by testing that $\Phi_d(x) \in \mathcal{C}_n$ divides $\hat{f}(x)$ we can decide whether $f(x)$ has a unitary pair of order d. Using the following proposition we may avoid the extraneous factor $(x-1)^n$ and reduce the size of the coefficients in the resultant computation.

Proposition 4.1 *If $g(x, y) = (f(y/x)x^n - f(y))/(x-1)$ and $\deg_y(g) = m > 0$, then*

$$\mathrm{res}_y(f(y), f(xy))/(x-1)^n = (-1)^n a_n^{n-m} \mathrm{res}_y(f(y), g(x, y)).$$

Method 1 consists of one resultant computation, and c_n divisions of $\hat{f}(x)$ by cyclotomic polynomials.

Method 2 Construct an integral polynomial $\hat{f}_d(x) = c \prod_{1 \leq i \leq n} (x - \alpha_i^d)$, where c is an integer. We take $\hat{f}_d(x)$

as $\mathrm{res}_y(f(y), x - y^d)$.

For each $\hat{f}_d(x)$, $d \in \mathcal{D}_n$, we can test whether $f(x)$ has a unitary pair whose order divides d, by deciding square-freeness of $\hat{f}_d(x)$ or by testing whether the discriminant of $\hat{f}_d(x)$ vanishes.

This method needs at most c_n resultant computations and at most c_n square-free decomposition or discriminant computations.

4.2 Complexities

We estimate the complexities of the methods in terms of the number of arithmetic operations over the integers. To bound the complexity of resultant computations, we considered an interpolation method.

Proposition 4.2 (i) *The construction of $\hat{f}$ and $\hat{f}_d$ needs $O(n^5)$ and $O(nd^3 + n^4)$ arithmetic operations, respectively.* (ii) *Method 1 and Method 2 needs $O(n^5 + c_n d_n n^2)$ and $O(c_n d_n^3 n)$ arithmetic operations, respectively.*

We bound the magnitude of the coefficients of $\hat{f}$ and $\hat{f}_d$'s in terms of the square-norm by a Hadamard-type bound [4]: $|\hat{f}| < n^n |f|^{2n-1}$ and $|\hat{f}_d| < 2^{n/2} |f|^d$. The Landau-Mignotte bound gives $|\Phi_d| < 2^d$.

Having these coefficient bounds we are able to use modular algorithms for the subproblems in the methods, and we conclude that the methods need polynomial time.

4.3 An efficient test

Proposition 4.2 shows that Method 2 requires more arithmetic operations than Method 1. However, the computation of each $\hat{f}_d(x)$ can be carried out much easier than the computation of $\hat{f}(x)$, because we may assume that $d_n = O(n)$ when $d_n < 3000$. Based on this fact, combining Method 1 and Method 2 we propose the algorithm `Unitary-Test`, which does not compute $\hat{f}(x)$.

Instead of $\hat{f}(x)$, we compute $\hat{f}_d(x)$. To reduce the number of computations of $\hat{f}_d(x)$, we also apply a "quick test" (with parameter k) which can detect unnecessary Φ_d efficiently, and for the same purpose we provide additionally "discriminant test." We compute $\hat{f}_d(x)$ only for that d for which $\Phi_d(x)$ passes these tests.

Unitary-Test
Input: $f(x)$.
Output: *True* if f has a unitary pair, *False* otherwise.
  [`Choose k much smaller than n`]
  for $s = 0$ **to** k **do**;
    $\hat{f}(s) := \mathrm{res}_y(f(y), g(s, y))$,
    where $g(x, y) = (f(y/x)x^n - f(y))/(x - 1)$.
  $D := \mathcal{D}_n$.
(loop) **while** $D \neq \emptyset$ **do**;
    $D := D \setminus \{d\}$ with some d in D.
    [`Discriminant-Test`]
    if $\phi_d(1) \not| \mathrm{disc}(f)$, **then goto** (loop).
    [`Quick-Test`]
    for $s = 0$ **to** k **do**;
      if $\phi_d(s) \not| \hat{f}(s)$ **then goto** (loop).
    $\hat{f}_d(x) := \mathrm{res}_y(f(y), x - y^d)$.
    if $\hat{f}_d$ has a multiple factor, **then return** *True*.
  return *False*.

4.3.1 Quick-Test

The idea for checking divisibility of polynomials in `Quick-Test` is specialization. If $\Phi_d(x)$ does not divide $\hat{f}(x)$, then the probability of the existence of an integer s with $\Phi_d(s) \not| \hat{f}(s)$ seems to be very high, because there are only finitely many s for which the divisibility holds. Since from $\Phi_d(x) \not| \hat{f}(x)$ we have

$$||s| - 1|^{\phi(d)} < \Phi_d(s) \mid \mathrm{res}_x(\hat{f}(x), \Phi_d(x))$$

for each integer s with $\Phi_d(s) \mid \hat{f}(s)$.

Our experiment shows that `Quick-Test` eliminates unnecessary $\Phi_d(x)$ efficiently. Especially, it is well suited for randomly generated f.

4.3.2 Discriminant-Test

The correctness of `Discriminant-Test` is guaranteed by the following proposition.

Proposition 4.3 *If $f(x)$ has a unitary pair of order d, then $\Phi_d(1)$ divides $\mathrm{disc}(f)$.*

Proof We recall

$$\mathrm{disc}(f) = a_n^{2n-2}(\alpha_1 \cdots \alpha_n)^{n-1} \prod_{i \neq j} (1 - \alpha_j/\alpha_i).$$

Since for some i and j, α_j/α_i is a root of unity of order d, each primitive d-th root of unity appears as a root of the integral polynomial $\mathrm{disc}(f)$. Let they be $\alpha_{j_1}/\alpha_{i_1}, \ldots, \alpha_{j_{\phi(d)}}/\alpha_{i_{\phi(d)}}$. Then

$$\mathrm{disc}(f) = \prod_{k=1}^{\phi(d)} (1 - \alpha_{i_k}/\alpha_{j_k}) \times \delta = \Phi_d(1) \times \delta.$$

Expanding δ we get a sum, where each term is in the form $a_n^{2n-2}\alpha_1^{b_1} \cdots \alpha_n^{b_n}$ with $b_i \leq 2n - 2$. For distinct roots $\alpha_{k_1}, \ldots, \alpha_{k_\ell}$, $a_n\alpha_{k_1} \cdots \alpha_{k_\ell}$ is an algebraic integer (see [5] page 81). Using this fact, we can show that each summand is an algebraic integer and so is δ, but δ is also a rational number, hence it is an integer. □

4.4 Experiment

We present our experiment for examining the efficiency of `Unitary-Test` by taking $d_n \leq 5n$. We implemented the procedure in Risa/Asir [6], a computer algebra system developed at ISIS, FUJITSU LABS. By this experiment, we are convinced that `Unitary-Test` for deciding the existence of unitary pairs is efficient. Computing time was measured on SUN Sparc 10, it is given in seconds. The time for garbage collection is excluded. Instead of $\mathrm{res}_y(f(y), g(s, y))$, we used $\mathrm{res}_y(f(y), f(y/s)s^n - f(y))$. For the resultant computations we used the built-in resultant procedure based on the subresultant algorithm.

The table below shows the performance of `Unitary-Test` with respect to different choices of k for 1000 random polynomials. Row $\hat{f}$ shows the time for computing $\hat{f}(x)$ for 5 random polynomials. We added row C_n to show the time for generating necessary cyclotomic polynomials according to n.

		n		
		12	15	20
k	4	145	290	925
	9	364	942	3846
	$n-1$	508	1914	—
	$\hat{f}$	177	783	5735
	C_n	0.26	0.30	0.60

We conclude from the experiment:

- The total time used by `Unitary-Test` for checking 1000 polynomials is smaller than the time needed to compute $\hat{f}(x)$ for 5 polynomials. This shows that `Unitary-Test` is more efficient than possible implementations of Method 1.
- The proportion of polynomials with a unitary pair to the generated polynomials is very small. For instance, out of 1000 random polynomials of degree 15, there were only 15 having unitary pairs. This behavior emphasizes the importance of `Quick-Test`.
- The parameter $k = n-1$ serves very well for detecting unnecessary computations of $\hat{f}_d$. Even $k = 4$ works well for this purpose.

References

[1] Berstel J., Mignotte M.; Deux propriétés décidables des suites récurrentes linéaires, *Bull. Soc. Math. France* **104** (1976), 175-184.

[2] Bradford R.J., Davenport J.H.; Effective tests for cyclotomic polynomials, *Proc. ISSAC'88, L.N.C.S.* **358** (1988), 244-251.

[3] Ge G.; *Algorithms related to multiplicative representations of algebraic numbers*, Ph.D. thesis, University of California, 1993.

[4] Goldstein A.J., Graham R.L.; Problem 73-17, *SIAM Review* **16** (1974), 394-395.

[5] Hecke E.; *Lectures on the theory of algebraic numbers*, Springer-Verlag, New York, 1981.

[6] Noro M., Takeshima T.; Risa/Asir - computer algebra system, *Proc. ISSAC'92*, ACM Press, New York (1992), 387-396.

[7] Robba, Ph.; Zéros de suites récurrentes linéaires, *Groupe d'Etude d'Analyse Ultramétrique, 5e année* (1977/78) Exp. No. 13.

[8] Wielandt, H.; *Finite permutation groups*, Academic Press, New York, 1964.