On the sign of a trigonometric expression
Pierre-Vincent Koseleff, Fabrice Rouillier, Cuong Tran

To cite this version:
Pierre-Vincent Koseleff, Fabrice Rouillier, Cuong Tran. On the sign of a trigonometric expression. 2015. hal-01108656

HAL Id: hal-01108656
https://inria.hal.science/hal-01108656
Preprint submitted on 28 Jan 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
On the sign of a trigonometric expression

Pierre-Vincent Koseleff
INRIA, Paris-Rocquencourt,
Oouragan
CNRS, UMR 7586, IMJ-PRG
pierre-vincent.koseleff@imj-prg.fr

Fabrice Rouillier
INRIA, Paris-Rocquencourt,
Oouragan
CNRS, UMR 7586, IMJ-PRG
fabrice.rouillier@inria.fr

Cuong Tran
UPMC-Sorbonne Universités
CNRS, UMR 7586, IMJ-PRG
cuong.tran@imj-prg.fr

ABSTRACT

We propose a set of simple and fast algorithms for evaluating and using trigonometric expressions in the form \( F = \sum_{k=0}^{d} f_k \cos k \tau \), \( f_k \in \mathbb{Q} \), \( d < n \) for a fixed \( n \in \mathbb{Z}_{>0} \): computing the sign of such an expression, evaluating it numerically and computing its minimal polynomial in \( \mathbb{Q}[x] \). As critical byproducts, we propose simple and efficient algorithms for performing arithmetic operations (multiplication, division, gcd) on polynomials expressed in a Chebyshev basis (with the same bit-complexity than in the monomial basis) and for computing the minimal polynomial of \( 2 \cos \frac{\pi}{n} \) in \( O(n^2 \delta) \) bit operations with \( n_0 < n \) is the odd squarefree part of \( n \). Within such a framework, we can decide if \( F = 0 \) in \( O(d(\tau + d)) \) bit operations, compute the sign of \( F \) in \( O(d^2 \tau) \) bit operations and compute the minimal polynomial of \( F \) in \( O(n^2 \tau) \) bit operations, where \( \tau \) denotes the maximum bitsize of the \( f_k \)'s.

Keywords

Chebyshev polynomial, minimal polynomial, cyclotomic polynomial, root isolation

1. INTRODUCTION

The present contribution was initially motivated by the computation of Chebyshev knots with the objective of decreasing the complexity bound of the algorithm proposed in [12]. The bottleneck for this algorithm was the computation of the sign of a multivariate polynomial at the zeroes of a zero-dimensional system. It has been shown later ([11]) that this problem finally reduces to the computation of the sign of a polynomial with rational coefficients at some particular real points in the form \( \cos \frac{\pi}{n}, n \in \mathbb{Z}_{>0} \), which can easily be turn into the computation of the sign of an expression in the form \( F = \sum_{k=0}^{d} f_k \cos k \tau \), \( f_k \in \mathbb{Z} \) for a fixed \( n \in \mathbb{Z}_{>0} \).

Evaluating numerically such an expression can be done straightforwardly, but getting its sign (in particular deciding if it is null or not) or computing its minimal polynomial to follow using it for further exact computations need some efforts to be done efficiently in practice. As \( F = f(2 \cos \frac{\pi}{n}) \) with \( f(x) = f_0 + \sum_{k=1}^{d} f_k T_k(x) \), where \( T_k(x) \in \mathbb{Z}[x] \) is the \( k \)-th monic Chebyshev polynomial, evaluating \( F \) can be seen as evaluating \( f \in \mathbb{Q}[x] \) at the real value \( 2 \cos \frac{\pi}{n} \), testing if \( F = 0 \) can resume to testing if the minimal polynomial \( M_n \in \mathbb{Q}[x] \) of \( 2 \cos \frac{\pi}{n} \) divides \( f \) and, finally, computing the minimal polynomial \( M_F \in \mathbb{Q}[x] \) of \( F \) remains to computing the minimal polynomial \( M_f \) of \( f \) in \( \mathbb{Q}[x]/(M_n) \).

Our primary objective was thus to find a way for computing efficiently \( M_n \in \mathbb{Q}[x] \), the minimal polynomial of \( 2 \cos \frac{\pi}{n} \) in order, for example, to use state of the art algorithms for testing if \( F = 0 \) (which then resumes to a single polynomial division) or computing \( M_F \) (for example using [15]).

The algorithm we propose in section 4 for computing \( M_n \) is an adaptation of the algorithm from [1] that basically computes \( \Phi_n \), the minimal polynomial of the \( n \)-th primitive root of unity. The relation between \( \Phi_n \) and \( M_n \) is simple: \( \Phi_{2n} = D(M_n) \), where \( D \) is the transformation \( \mathbb{Q}[x] \) defined by \( D(P) = x^{\deg P} P(x + \frac{1}{2}) \).

This simple transformation is also used in Section 2 to set simple and fast algorithms for multiplying, dividing, computing greatest common divisors for polynomials expressed in the Chebyshev basis. In particular, we provide, for the multiplication, a very simple alternative to [7] with an equivalent bit complexity. More generally, the complexity of these operations is the same as for polynomials in the monomial basis (see [16]).

It turns out that expressing the polynomials in the Chebyshev basis instead of in the usual monomial basis simplifies some parts of the algorithms and make easier the computation of complexity bounds. For example, we show that the computation of \( M_n \) can be done in \( O(n^2 \delta) \) bit operations where \( n_0 < n \) is the odd squarefree part of \( n \).

The efficiency of this algorithm depends also on the way the transformations from the Chebyshev basis to the monomial basis and vice-versa are computed. In order not to reinvent the wheel, we have considered these transformations as a particular case of composition method developed in [9] with additional refinements linked to the properties of Chebyshev polynomials.

In section 3, we show that passing from the monomial basis to the Chebyshev basis consists essentially to inject in the algorithm from [9] the fast operations we have introduced in Section 2. For the reverse operation, we make use of the linear recurrence introduced in [4] and essentially keep the structure of the composition algorithm from [9], thanks to some remarkable properties of Chebyshev polynomials. We finally show that the two transformations we propose perform \( O(d) \) arithmetic operations in \( \mathbb{Z} \) and \( O(d(\tau + d)) \) bit operations if \( \tau \) is the maximal bitsize of the \( f_k \)'s.

In section 5, we first come back to our initial problem and propose some algorithms together with their complexity analysis. We show that we can test whether \( F = 0 \) in \( O(n^2 + n \tau) \) binary operations and can decide the sign of \( F \) in \( O(n^2 \tau) \) binary operations, using an algorithm of [6] for a
fast evaluation of \( \cos x \).

As \( F \) could also be used inside other algebraic expressions, we propose in section 6 an algorithm for computing efficiently the minimal polynomial of \( F \) in \( \mathcal{O}(n^r) \) binary operations.

2. CHEBYSHEV POLYNOMIALS

As seen in the introduction, Chebyshev polynomials and their algebraic properties play a central role in the present contribution. We consider the Chebyshev monic polynomials defined by

\[
T_n(x) = 2 \cos nx, \quad U_n(x) = \frac{\sin nt}{\sin t}
\]

where \( x = 2 \cos t \). Both of them satisfy the linear recurrence relation:

\[
P_{n+1}(x) = 2P_n(x) - P_{n-1}(x),
\]

but their first terms differ:

\[
\{T_0(x) = 2, T_1(x) = x\}, \quad \{U_0(x) = 0, U_1(x) = 1\}.
\]

The roots of \( T_n \) and \( U_n \) are real roots and we have:

\[
T_n(x) = \sum_{k=0}^{n-1} (-1)^k \binom{n-k}{k} x^{n-2k},
\]

\[
U_n(x) = \sum_{k=0}^{n-1} (-1)^k \frac{n-k}{n} x^{n-2k}.
\]

By deriving the relation \( \sin t T_n(2 \cos t) = 2 \sin nt \) that is

\[
T_n = nU_n.
\]

By deriving once again we get

\[
4(\sin t)^2 T_n''(2 \cos t) + 2 \cos t T_n'(2 \cos t) = 2n^2 \cos nt,
\]

or

\[
(4 - x^2)T_n''(x) - xT_n'(x) + n^2 T_n(x) = 0.
\]

It means that \( T_n \) is an hypergeometric function. By identifying the coefficients, we get

\[
T_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n-k}{n-k} x^{n-2k}.
\]

From Equation (3) and Formula (5), we also obtain

\[
U_{n+1}(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} x^{n-2k}.
\]

The family \( \mathcal{T} = \{1, T_j, j \geq 1\} \) is therefore a basis of \( \mathbb{Z}[x] \).

Proposition 1. We have \( \tau_T(T_n) \leq n \), \( \tau_T(U_n) \leq n - 1 \), \( \tau_T(x^n) \leq n \).

Proof. From \( (s-k) \leq \frac{n}{s-k} (s-k) \), we obtain first that \( \tau_T(U_{n+1}) \leq \tau_T(T_n) \), using Formulas (5) and (7). The sum of the absolute values of the coefficients of \( T_n \) is \( \sum_k \frac{1}{n-k} = \phi^n + (-1/\phi)^n \), where \( \phi \) is the golden ratio. We thus deduce that \( \tau_T(x^n) \leq 2^n \) and \( \tau_T(T_n) \leq n \). We get \( \tau(x^n) \leq n \) because that \( \sum_k (\phi)^k = 2^n \). □

We thus deduce

Corollary 2. Let \( P \) be a polynomial of degree \( d \). Then we have \( \tau_P(P) \leq \tau_P(P + d + \log_2 d, \tau_T(P) \leq \tau_T(P) + d + \log_2 d \).

Chebyshev forms

Let \( f \in \mathbb{Q}[x] \). We will say that \( f \) is in Chebyshev form when it is expressed in the Chebyshev basis: \( \{T\}f = f_0 + \sum_{j=1}^{d} T_j f_j \). The set of Chebyshev forms with rational coefficients is an Euclidean ring and we focus on computing efficiently in this ring, starting with elementary operations.

Let us introduce a simple shortcut that will straightforwardly offer a simple link between basic operations in the Chebyshev basis and in the usual monomial basis:

Definition 3. \( D \) is the transformation from \( \mathbb{Q}[x] \) to the space of even degree reversible polynomials given by

\[
D(P) = x^{\log_2 P} P(x + \frac{1}{2}).
\]

Note that \( D \) satisfies the following relation:

\[
D(f \cdot g) = D(f) \cdot D(g).
\]

so that, as \( T_n(x + \frac{1}{2}) = x^n + \frac{1}{2} \), then

\[
D(a_0 + \sum_{j=1}^{n} a_j T_j) = a_0 x^n + \sum_{j=1}^{n} a_j (x^{n-j} + x^{n+j}).
\]

Note that Equation (9) shows that passing from \( \{X\}D(P) \) to \( \{T\}P \) and vice versa is just a way of changing the numbering of the coefficients, having in mind that \( \{X\}D(P) \) is a reversible polynomial. In particular, \( \tau_T(D(P)) = \tau_T(P) \) and \( \deg D(P) = 2 \deg P \). Also, passing from \( \{X\}D(P) \) to \( \{T\}P \) and vice-versa can be done in \( \mathcal{O}(d) \) bit operations.

From this remark, it is then sufficient to apply the classical fast multiplication for polynomials in \( \mathbb{Q}[x] \) after applying \( D \) on the operands. We will denote by \( M(\delta, r) = \mathcal{O}(\delta r) \) the number of bit operations for multiplying two polynomials of \( \mathbb{Z}[x] \) with degrees at most \( \delta \) and coefficients of bitsize at most \( t \) with respect to the usual monomial basis \( X \) and by \( M(\tau) = \mathcal{O}(\tau) \) the cost of the multiplication of two integers of bitsize dominated by \( \tau \). We obtain

Proposition 4. Let \( f, g \in \mathbb{Z}[x] \) given by their Chebyshev forms \( \{T\}f \) and \( \{T\}g \). Then we have \( \tau_T(f \cdot g) \leq \tau_T(f) + \tau_T(g) + \log_2 \min(\deg f, \deg g) + 1 \).

Suppose that \( \tau_T(f), \tau_T(g) \leq r \) and \( \deg f, \deg g \leq d \) then computing \( \{T\}(f \cdot g) \) claims \( M(2d, r) + \mathcal{O}(d) \) bit operations.

Note that this very simple algorithm might be replaced by the one from Giorgi ([7]) which claims the equivalent of two multiplications between polynomials of degree \( d \) with coefficients of bitsize in \( \mathcal{O}(\tau) \).
Let us now extend these results to the division. Applying the transformation $D$ on both side of the relation $f = g \cdot q + r$, we then get:

$$D(f) = D(g)D(q) + x^{d \log x}D(r). \quad (10)$$

In particular, Formulas (8) and (10) imply that $g | f$ iff $D(g) | D(f)$. Also, applying the same strategy as for the product two Chebyshev forms, we immediately get:

**Corollary 5.** Let $f, g \in \mathbb{Z}[x]$ given by their Chebyshev forms $[T]f$ and $[T]g$. Suppose that $\deg f, \deg g \leq d$ and $\tau_T(f), \tau_T(g) \leq \tau$. Then,

1. (a) deciding if $g$ divides $f$ knowing $[T]f$ and $[T]g$ can be done in $O(d^2 + \log d)$ bit operations;
   
   (b) if $g$ divides $f$ then computing $[T]\text{Quo}(f, g)$ from $[T]f$ and $[T]g$ can be done in $O(d^2 + \log d)$ bit operations;

2. (a) if $g | f$ then $\tau_T(g) = O(\tau_T(f) + d)$.
   
   (b) $\tau_T(gcd(f, g)) \leq O(\tau + d)$.

**Proof.** The first items are direct consequences of [16, exercise 9.14] while the third item is a direct consequence of [16, Corollary 11.20]. The two last items come from the Mignotte bound ([16, p. 166]). $\Box$

### 3. BASES CHANGE

It is a classical result that $T$ is an orthogonal basis. Bostan \textit{et al.} (see [4]) give a fast general conversion method from the monomial basis to orthogonal bases. The alternatives we propose are based on the general method of Hart \& Novocin for polynomial composition (see [9]) which lead to simpler descriptions and complexity analysis. Given $f = \sum_{i=0}^{d} a_i x^i$ in the Chebyshev basis and $f = f_0 + \sum_{i=1}^{d} f_i T_i$ in the monomial basis, in both cases, the method is based on the same divide and conquer principle as in [9]: splitting $f$ into $\lfloor \frac{d}{2} \rfloor$ sub-polynomials of length 2.

Suppose that we have to evaluate the sum $S = \sum_{j=0}^{d} u_j v^j$. We first define:

$$d_0 = d, v_0 = v, S_{0,j} = u_j, j = 0, \ldots, d.$$ Let $c = \lfloor \log_2 d \rfloor - 1$. Then we define for $k = 0, \ldots, c$:

$$d_{k+1} = \lfloor \frac{d}{2^k} \rfloor, v_{k+1} = v_{k}^2, S_{k+1,j} = S_{k,j} + S_{k,j+1} \cdot v_k, j = 0, \ldots, d_{k+1}.$$ Then, for $k = 0, \ldots, c$,

$$S = \sum_{j=0}^{d} S_{k,j} \cdot v^j_k.$$ At the end, we get $S = S_{c,0}$.

Algorithm 1 is a direct application of this strategy for the evaluation of $f = \sum_{j=1}^{d} a_j x^j$ in the Chebyshev basis $T$.

**Proposition 6.** Let $f = \sum_{i=0}^{d} a_i x^i$ be a polynomial of bitsize $\tau$. One can compute the Chebyshev form of $f$ in $O(d)$ arithmetic operations, or in binary complexity $O(d^2 + \tau d)$. The Chebyshev form $[T]f$ has bitsize $\tau + O(d)$.

**Algorithm 1:** From $X$ to $T$

**Input:** $f = \sum_{i=0}^{n} a_i x^i$

**Output:** $[T]f = f_0 + \sum_{i=1}^{n} f_i T_i$

1. begin
2.   $d \leftarrow \lfloor \frac{d}{2} \rfloor$; $c \leftarrow 0; v \leftarrow T_1$;
3.   for $j \leftarrow 0$ to $d$ do
4.     $S_{c,j} \leftarrow a_{2j} + a_{2j+1} \cdot T_1$
5.     $v \leftarrow ([T]v)^2$;
6.   while $d > 0$ do
7.     $d \leftarrow \lfloor \frac{d}{2} \rfloor$;
8.     for $j \leftarrow 0$ to $d$ do
9.       $S_{c+1,j} \leftarrow [T]S_{c,2j} + [T]S_{c,2j+1} \cdot [T]v$
10.      $c \leftarrow c + 1; v \leftarrow ([T]v)^2$;
11. return $S_{c,0}$

**Proof.** We use Algorithm 1. Let $c = \lfloor \log_2 d \rfloor$. We start with $v = [T]x = T_1$, and compute successively $v = x^{2^k}, k = 0, \ldots, c$. We know that $x^{2^k}$ has size $O(2^k)$ in the Chebyshev basis. From Proposition 4, one can compute $[T]x^{2^k}$ from $[T]x^{2^k}$ in $O(2^k)$ bit operations.

At each step, the bitsize $\tau_{k+1}$ of the Chebyshev form $S_{k+1,j} = [T]S_{k,2j} + [T]S_{k,2j+1}$ of $[T]x^{2^k}$ satisfies $\tau_{k+1} \leq \tau_k + 2^k + 1$. We therefore obtain $\tau_k = \tau + O(2^k)$. One can compute the Chebyshev form $S_{k+1,j} = S_{k,2j} + S_{k,2j+1} \cdot x^{2^k}$ in $O(2^k \tau_k)$ binary operations from Proposition 4.

The total computing time is bounded by $\sum_{k=1}^{c} \tau_k 2^k = O(d^2 + \tau d)$. $\Box$

Conversely, given a Chebyshev form $f = f_0 + \sum_{j=1}^{d} f_j T_j$, we have to find the expression $f = \sum_{j=0}^{d} a_j x^j$. We use a key idea from the general method of [4], considering the characteristic matrix of the Chebyshev polynomials:

$$X = \begin{bmatrix} 0 & 1 \\ -1 & x \end{bmatrix}.$$ Using the recurrence (1), we have:

$$T_{j+1} = X^j T_0 / T_1, j \geq 0.$$ Algorithm 2 computes the matrix polynomial

$$M(f) = \sum_{i=0}^{d} [f_{2i} \quad f_{2i+1}] X^{2i}$$

using the composition method in [9]. Then, following [4], we get (because $T_0 = 2$)

$$f = -f_0 + M(f) \cdot \begin{bmatrix} T_0 \\ T_1 \end{bmatrix}.$$ **Proposition 7.** Let $f = f_0 + \sum_{i=1}^{d} f_i T_i$ be a Chebyshev form of bitsize $\tau$. One can compute $f$ in the monomial basis in $O(d)$ arithmetic operations, or in binary complexity $O(d^2 + \tau d)$. $[X]f$ has bitsize $\tau + O(d)$.

**Proof.** An induction shows that $X^n = \begin{bmatrix} -U_{n-1} & U_n \\ -U_n & U_{n+1} \end{bmatrix}$. Thus the bitsize of $X^n$ is $O(n)$, using Proposition 1.
The number of factors of \(T_n\) is given in [10]. We give here the complete factorization of the Chebyshev polynomials \(T_n\) and \(U_n\) as products of polynomials \(M_n\), see also [11]:

**Proposition 10.** We have

\[
U_{2k}(2m+1) = (-1)^m \prod_{d|2m+1} \left( M_d(-t) \right) \prod_{1 \leq i \leq k} M_d(T_{2i})
\]

\[
T_{2k}(2m+1) = \prod_{d|2m+1} M_d(T_{2k+d})
\]

where \(M_n\) is the minimal polynomial of \(\cos \frac{x}{n}\).

**Proof.** The factorization of \(U_n\) is obtained by comparing its roots with those of \(M_d(\pm t)\), when \(d|2m+1\) and using the Euler identity \(n = \sum_{d|n} \varphi(d)\).

Let \(d\) be an odd divisor of \(n\). We write \(n = 2^k \cdot d_1 \cdot d\), where \(d_1\) is odd, \(\cos \frac{2\pi n}{d_1}\) is a root of \(T_{d_1}\) so \(M_{2k+d_1} | T_{d_1}\).

We conclude by comparing the leading terms.

From \(M_n(\zeta_{2^n+1} / \zeta_{2^n}) = 0\) when \(n > 2\), we deduce a relation between the Chebyshev form of \(M_n\) and \(\Phi_{2^n}\), see also [14, Chapter 5]:

**Proposition 11.** We have \(\Phi_{2^n} = D(M_n)\), for \(n > 2\).

Let \(x = 2 \cos t\) and \(V_n(x) = \sin(x + \frac{1}{2}t)\) then \(V_n = \prod_{d | 2m+1} M_d\).

This is an analogous formula to \(T_n - 1 = \prod_{d | n} \Phi_d\), see [12].

**Computation of \(M_n\)**

The relation \(T_n \circ T_m = T_{n+m} = T_{nm}\) makes the Chebyshev basis very convenient for the computation of the minimal polynomial \(M_n\). Lemma 12 is a generalization of Lemma 9:

**Lemma 12.** Let \(n = 2^p p_1^{a_1} \cdots p_k^{a_k}\) where the \(p_i\) are distinct odd primes. Let \(n_0 = p_1 \cdots p_k\). Then we have

\[
\begin{align*}
M_n &= M_{n_0}(T_{n/n_0}) & \text{if } k \geq 1 \\
M_{2n} &= T_{2n-1}.
\end{align*}
\]

**Proof.** If \(n = 2^p > 1\) then \(T_{n/2}(2 \cos \pi / n) = 2 \cos \pi / 2 = 0\). On the other hand \(T_{n/2}\) and \(M_n\) are monic with the same degree. Thus they are equal.

If \(n_0 > 1\) then \(M_{n_0}(T_{n_0/n}(2 \cos \pi / n)) = M_{n_0}(2 \cos \pi / n) = 0\). We thus have \(M_n | M_{n_0}(T_{n_0/n_0})\). On the other hand, \(M_n\) and \(M_{n_0}(T_{n_0/n_0})\) are monic with the same degree. Thus they are equal.

Lemma 12 shows that the Chebyshev basis is particularly adapted for the computation of \(M_n\).

**Lemma 13.** \(n = 2^a p_1^{a_1} \cdots p_k^{a_k}\) where the \(p_i\) are distinct odd primes. Let \(n_0 = p_1 \cdots p_k\). Then the coefficients of \(M_n\) (in the monomial basis, as well as in the Chebyshev basis) have bitsize \(O(n_0)\).

**Proof.** As \(M_{n_0}(U_{n_0})\) the conclusion is a consequence of Proposition 5, because we deduce from

\[
U_n = \sum_{k=1}^{\frac{n}{2}} T_{n-2k-1} + \frac{1}{2} (1 - (-1)^n),
\]

that the Chebyshev form \(U_n\) has maximum bitsize 1.

When \(n\) is an odd prime, we get:
Lemma 14. Let $p$ a prime odd number, then
\[ M_p = T_k - T_{k-1} + \cdots + (-1)^{k-1}T_1 + (-1)^k, \]
where $k = 1/(2(p-1))$.

Proof. Let $p = 2k + 1$ and $h = T_k - T_{k-1} + \cdots + (-1)^{k-1}T_1 + (-1)^k$. We have
\[ \sum_{i=1}^{2k+1} h(2\cos\frac{2\pi i}{2k+1}) = 0. \]
But $\deg h = k = \frac{1}{2}p$ and thus $h = M_p$. \hfill \Box

Lemma 15. Let $p$ be an odd prime and $n$ such that $p \nmid n$, then $M_{np} = M_n(T_p)$. \hfill \Box

Proof. We just need to show that both $M_{np}$ and $M_n$ divide $M_n(T_p)$ because these polynomials are monic and their degrees satisfy $2(\deg M_n + \deg M_{np}) = \varphi(2n) + \varphi(2pn) = p\varphi(n) = 2\deg M_n(T_p)$.

If $t = 2\cos\frac{n}{2p}$ then $T_p(t) = 2\cos\frac{n}{p}$ and $M_n(T_p)(t) = 0$ so that $M_{np}|M_n(T_p)$. If $t = 2\cos\frac{n}{p}$ then $T_p(t) = 2\cos\frac{np}{n}$ is a root of $M_n$. \hfill \Box

Following Arnold and Monagan in [1] for the computation of $\Phi_n$, we deduce Algorithm 3 to compute the Chebyshev form of $M_n$.

Algorithm 3: Compute $[T]M_n$  
Input: $n$  
Output: $[T]M_n$  
begin  
2 Factorize $n = 2^\alpha_0p_1\cdots p_k^\alpha_k$; $\alpha_0 \leftarrow p_1 \cdots p_k$;  
3 if $k = 0$ then  
4 \textbf{if} $\alpha_0 = 0$ then  
5 \textbf{return} 1  
6 else  
7 \textbf{return} $T_{2^{\alpha_0}-1}$  
8 $i \leftarrow \frac{1}{2}(p_1 - 1)$;  
9 $m \leftarrow T_i - T_{i-1} + \cdots + (-1)^{i-1}T_1 + (-1)^i$;  
10 for $j \leftarrow 2$ to $k$ do  
11 \textbf{m} $\leftarrow [T]\left(m(T_{p_j})\right)$  
12 \textbf{return} $m(T_{\alpha_0}/\alpha_0)$  
end

Proposition 16. One computes $M_n$, in the Chebyshev basis in complexity $O(n\alpha_0)$ or $O(n\alpha_0^2)$ bit operations.

Proof. We will use Algorithm 3. The factorization of $n$ requires $O(\log n)$ binary operations, see [10, Chap. 19].

We have to compute successively $M_{q_i+1} = (M_{q_i}T_{p_{i+1}})/M_{q_i}$, where $q_i = p_1 \cdots p_i$.

We know that $\tau(M_{q_i}) = (M_{q_i}, \tau(M_{q_i}(T_{p_{i+1}}))) = (M_{q_i})$ and $\deg(M_{q_i}(T_{p_{i+1}})) = \varphi(2q_i)p_i/2 \leq q_i + 1$. By Proposition 4, we compute $M_{q_i+1}$ from $M_{q_i}$ in $O(\alpha_0+1)$ arithmetic operations or $O(q_i+1)$ binary operations.

Finally we compute $M_{\alpha_0}$ in $O(q_2 + \cdots + q_k) = O(n\alpha_0^2)$ arithmetic operations and $O(q_1^2 + \cdots + q_k^2) = O(n\alpha_0^3)$ binary operations. \hfill \Box

The analogy between $M_n$ and the cyclotomic polynomial $\Phi_n$ allows us to deduce the following complexity bound for the computation of $\Phi_n$, from the algorithm proposed by Arnold and Monagan in [1] :

Corollary 17. One can compute $\Phi_n$ in the complexity $O(n\alpha_0)$ and in the running time $O(n\alpha_0^2)$, where $n\alpha_0$ is the odd squarefree part of $n$.

Example

The minimal polynomial $M_{1260}$ is
\[ M_{1260}(T_{12}) = T_{288} - T_{276} + T_{264} + T_{228} - T_{216} + 2T_{204} - T_{192} + T_{180} + T_{144} - T_{132} + T_{120} - T_{108} + T_{96} - T_{84} - T_{48} - T_{24} - 1. \]

The maximum bitsize of $[X]M_{1260}$ is $\tau([X]M_{1260}) = 197$ while the total bitsize of its coefficients is $20329$.

The minimal polynomial $M_{936}$ is
\[ M_{936}(T_{24}) = T_{288} + T_{264} - T_{216} - T_{192} + T_{144} + T_{120} - T_{72} - T_{48} + 1. \]

Its maximum bitsize is also $197$ while the total bitsize of its coefficients is $20338$.

5. SUM OF COSINES

The aim of this section is to give methods for determining the sign of $F = f(\gamma)$ where $\gamma$ is one root of $M_n$, for evaluating $F$ and for getting the minimal polynomial of $F$.

We consider here the expression
\[ F = f_0 + 2\sum_{j=1}^{d} f_j \cos \frac{j\pi}{n}, \]
where $d \leq n$ and $f_j \in \mathbb{Z}$. It is convenient to write $F$ as $f(\gamma)$ where $\gamma$ is the algebraic number $2\cos\frac{\pi}{n}$ and $f = f_0 + \sum_{k=1}^{d} f_k T_k \in \mathbb{Z}[x]$.

Evaluating the sum

The first step is the approximation of $\gamma = 2\cos\frac{k\pi}{n}$, using Brent’s methods ([5, 6])

Lemma 18. Let $0 \leq k \leq n$ and $\gamma = 2\cos\frac{k\pi}{n}$. Let $\ell \in \mathbb{Z}_{>0}$. One can compute $c \in \mathbb{Q}$, of bitsize $\tau(c) \leq \ell$ such that $|c - \gamma| \leq 2^{-\ell}$ in $\tilde{O}(\ell + \log n)$ bit operations.

Proof. We first compute $r \in \mathbb{Q}$ of bitsize $2(\ell + \log n)$ such that $|r - k \frac{\pi}{n}| < 2^{-\ell-1}$. It claims $\tilde{O}(1 + \log n)$ bit operations, using [5].

Then we compute $c$ such that $|c - \cos r| < 2^{-\ell-1}$, using [6], in $\tilde{O}(\ell + \log n)$ binary operations. \hfill \Box

We thus deduce

Corollary 19. Let $0 \leq k \leq n$ and $\gamma = 2\cos\frac{k\pi}{n}$. Let $\ell \in \mathbb{Z}_{>0}$. Let $f$ be the Chebyshev form $f_0 + \sum_{i=1}^{n-1} f_i T_i$. One computes $\tilde{F} \in \mathbb{Q}$ of bitsize $O(\tau(f) + \ell)$ such that $|\tilde{F} - f(\gamma)| \leq 2^{-\ell}$ in $\tilde{O}(n\ell + \tau\ell)$ bit operations.

One computes $F^{-}$ and $F^{+}$ of bitsize $O(\tau(f) + \ell)$ such that $F^{-} \leq F \leq F^{+}$ and $F^{+} - F^{-} \leq 2^{-\ell}$ in $\tilde{O}(n\ell + \tau\ell)$ bit operations.

Proof. Using Lemma 18, one can compute the rational numbers $c_i, i = 1, \ldots, n - 1$ such that $|c_i - \cos ik\frac{\pi}{n}| \leq 2^{-\ell-\tau}/n$. They are of bitsize $O(\tau + \ell + \log n)$ and we can compute them in $\tilde{O}(n\tau + n\ell)$ bit operations.
If \( \tilde{F} = f_0 + 2 \sum_{i=1}^{n-1} f_i c_i \), then
\[
|\tilde{F} - F| \leq 2 \sum_{i=1}^{n-1} |f_i| |c_i - \cos ik\hat{z}_i| \leq 2^{-\ell}.
\]
Here, the \( f_i c_i \) have bitsize \( \tau + \ell + \log n \) and each can be computed in \( \mathcal{O}(\tau + \ell + \log n) \) bit operations, using the fast multiplication described in [16, Chap. 8]. \( F \) has bitsize \( \mathcal{O}(\tau + \ell + \log n) \) and can be computed in \( \mathcal{O}(n\tau + n\ell) \) bit operations.

The proof of the second part of the Lemma is similar. \( \square \)

### Evaluating the sign of the sum

Here we want to evaluate the sign of \( f(\gamma) \) where \( \gamma = 2 \cos \frac{k\pi}{n} \), and \( f \) is the Chebyshev form \( f_0 + \sum_{i=1}^{n-1} f_i T_i \). Without loss of generality, we can suppose that \( (k, 2n) = 1 \), that is to say that \( \gamma \) is a root of \( M_n \). If \( (k, n) = d > 1 \), then we can change \( n \) by \( n/d \). If \( k \) is even, then \( \gamma \) will be a root of \( M_n(t) \).

As \( M_n \) is the minimal polynomial of \( \gamma \), then \( f(\gamma) = 0 \) iff \( M_n \mid f \). If \( M_n \) does not divide \( f \) then we have \( |\text{Res}(M_n, f)| \geq 1 \). As \( M_n \) is monic, we have also
\[
\text{Res}(M_n, f) = \prod_{\gamma \in M_n(\gamma) = 0} f(\gamma).
\]
Let \( \gamma \) be a root of \( M_n \), then we have \( |f(\gamma)| \leq ||f||_1 \), where \( ||f||_1 = |f_0| + 2 \sum_{i=1}^d |f_i| \). We thus obtain for every root \( \gamma \) of \( M_n \):
\[
|f(\gamma)| \geq (||f||_1)^{1-\deg M_n} = \delta. \quad (12)
\]
Then, it is then sufficient to compute an approximation \( \tilde{F} \) of \( f(\gamma) \) such that \( |\tilde{F} - f(\gamma)| < \frac{1}{2} \) in order to ensure that this approximation has the same sign than \( f(\gamma) \). We thus deduce

**Proposition 20.** Let \( f \) of degree \( d < n \) with \( \tau_T(f) \leq \tau \). Let \( \gamma = 2 \cos \frac{k\pi}{n} \) where \( (k, 2n) = 1 \).

1. we can decide whether \( f(\gamma) = 0 \) in \( \mathcal{O}(n^2 + n\tau) \) bit operations,
2. we can compute \( \text{sign} f(\gamma) \) in \( \mathcal{O}(n^2 \tau) \) bit operations,
3. we can evaluate \( f(\gamma) \) with precision \( 2^{-\ell} \) in the complexity \( \mathcal{O}(n(n + n\tau)) \).

**Proof.** We first decide if \( f(\gamma) = 0 \) by testing if \( M_n \mid f \). It claims \( \mathcal{O}(n^2 + n\tau) \) bit operations by Propositions 16 and 5.

If \( f(\gamma) \neq 0 \), then we compute an approximation \( F \) of \( f(\gamma) \) with accuracy \( \frac{1}{2} \delta \) where \( \delta = ||f||_1^{1-\deg M_n} \). But \( -\log_2 \delta \leq (\deg M_n - 1)(\log_2(2n + 1) + 1) = \mathcal{O}(n\tau) \). We deduce, using Corollary 19, that \( F \) can be computed in \( \mathcal{O}(n^2 \tau) \) bit operations.

The last point of the Proposition is a consequence of Corollary 19. \( \square \)

Algorithm 4: Determine the sign of \( f(\gamma) \)

**Input:** \( f = f_0 + \sum_{i=1}^{n-1} f_i T_i \), \( k \) such that \( (k, 2n) = 1 \)

**Output:** \( \text{sign} f(\gamma) \) where \( \gamma = 2 \cos \frac{k\pi}{n} \)

1. Compute \( |T|M_n \);
2. if \( |M_n \mid f \) then
3. \( \text{return} f(2\cos k\frac{\pi}{n}) = 0 \)
4. \( \ell \leftarrow 1, F^- \leftarrow -1, F^+ \leftarrow 1 \);
5. while \( F^- \cdot F^+ < 0 \) do
6. Compute \( |F^-|, |F^+| \) of length \( 2^{-\ell} \), containing \( f(\gamma) \);
7. \( \ell \leftarrow 2\ell \);
8. \( \text{return} \text{sign} (F^+) \)

**Example**

In [13], Myerson pointed out that
\[
a = 16 \sin \frac{\pi}{9} \sin \frac{5\pi}{18} \sin \frac{11\pi}{39} \sin \frac{3\pi}{8}
\]
is very closed to \( 3 \). We write \( a \) as \( f(\gamma) \) where
\[
f = -7771 - T_{459} - T_{251} + T_{253} + T_{259} + T_{277} + T_{279} + T_{283} + T_{285} - T_{43}.
\]
and \( \gamma = 2 \cos \frac{771\pi}{288} \) is the biggest root of \( M_{283} \). Equation (12) asserts that
\[
|f(\gamma) - 3| \geq ||f - 3||_{288} = 19 - 288 \approx 2^{-1224}.
\]
Indeed, \( \min_{M_n(\gamma) = 0} |f(x) - 3| \geq 2^{-29} \) and Algorithm 4 provides the value and the sign of \( f(\gamma) \) very quickly.

### 6. THE MINIMAL POLYNOMIAL OF A SUM

We give an algorithm for the minimal polynomial of \( F = f(\gamma) \). It is classical to consider the monic polynomial (because \( M_n \) is monic)
\[
P_f(z) = \text{Res}(z - f(x), M_n(x)) = \prod_{M_n(\gamma) = 0} (z - f(\gamma)). \quad (13)
\]

The roots of \( P_f \) are \( z_k = f(2\cos k\frac{\pi}{n}) = f(T_k(2\cos \frac{\pi}{n})) \) where \( (k, 2n) = 1 \). We thus deduce that

**Proposition 21.** There exists \( \nu \in \mathbb{N}^* \) such that \( P_f = M_\nu \), where \( M_\nu \) is the minimal polynomial of \( f(2\cos \frac{\pi}{n}) \).

**Proof.** Let \( \gamma_k = 2 \cos \frac{k\pi}{n} \), a root of \( M_n \). The minimal polynomial \( \mu_\nu \) of \( f(\gamma_k) \) satisfies \( \mu_\nu \circ f(\gamma_k) = 0 \). Thus \( M_\nu \) divides \( \mu_\nu \circ f, \mu(f(\gamma_k)) = 0 \) for every root \( \gamma_k \) of \( M_n \).

We thus deduce that \( \mu_\nu \) divides \( \mu_k \) and that \( \mu_\nu = \mu_j = M_\nu, \quad P_f \) factorizes into \( P_f = M_\nu \). \( \square \)

We will compute \( M_\nu \) by computing first \( P_f \) and then \( M_f = P_f \text{gcd}(P_f, P_{f'}) \).

On might directly compute \( P_f \) using a general algorithm, following [16, Section 11.2]. It would then require \( \mathcal{O}(\delta_T) \) bit operations where \( \delta = \deg f + \deg M_n \) and \( \tau \) is a bound on the total bitsize required to store any principal subresultant coefficient which are all polynomials of degree in \( \mathcal{O}(\delta) \) in \( z \) with coefficients of bitsizes in \( \mathcal{O}(\delta_T) \) (see Proposition 8.50 in [2]). Such an algorithm would then perform, in our case, \( \mathcal{O}(n^2 \tau) \) bit operations, and we do not pretend to give a better theoretical upperbound. However, in practice, this classical strategy is based on the Half-Ged algorithm and
makes use if fast operations on univariate polynomials, both
starting to be being efficient for rather high degrees (sev-
eral hundred). The algorithm we propose in the sequel runs efficiently even for small
degrees.

It is natural to consider \( P_F \) as a polynomial whose coeffi-
cients are in \( \mathbb{Q}[x]/(M_n) \).

As \( T_n(t)(\gamma) = 2\cos(n + 1)\eta \) we have
\[
T_n(t) = T_{n-1}(t) \pmod{M_n}.
\]

The Chebyshev basis \( (1, T_1, \ldots, T_{n-1}) \) is then particularly adapted as generating family of \( \mathbb{Q}[x]/(M_n) \):

**LEMMA 22.** \( f = f_0 + \sum_{i=0}^{n-1} f_i T_i \) and \( g = g_0 + \sum_{i=0}^{n-1} g_i T_i \) be Chebyshev forms. Then one can compute \( h = h_0 + \sum_{i=0}^{n-1} h_i T_i \) where \( h \equiv f \cdot g \pmod{M_n} \) in \( \mathcal{O}(n \tau) \ bit operations and \( \tau(h) \leq \tau(f) + \tau(g) + \log_2 n + 1 \).

**Proof.** We compute \( h = [f \cdot g] \pmod{M_n} \) bit operations. We obtain \( h = h_0 + \sum_{i=0}^{n-1} h_i T_i = h_0 + \sum_{i=0}^{n-1} (h_i - h_{n-i}) T_i. \)

Let \( N = \frac{3}{2} \) be the degree of \( P_F \). The \( N \) roots of \( P_F \) are the \( f(T_k(x)) \) where \( (k, 2n) = 1 \).

We shall consider the \( i \)-th Newton sum:
\[
S_i(P_F) = \sum_{\frac{1}{2} \leq k \leq n} f(T_k(x))^i.
\]

Consider first \( f_i = f(x)^i = f_{i,0} + \sum_{j=1}^{n-1} f_{i,j} T_j \) in \( \mathbb{Q}[x]/(M_n) \), then \( f(T_k(x))^i \equiv f_{i,0} + \sum_{j=1}^{n-1} f_{i,j} T_j \pmod{M_n} \).

We thus deduce that
\[
S_i(P_F) = N f_{i,0} + \sum_{\frac{1}{2} \leq j \leq n} f_{i,j} \left( \sum_{\frac{1}{2} \leq k \leq n} T_{j,k} \right) \pmod{M_n}
\]

**LEMMA 23.** Let \( j \) and \( n \) be nonnegative integers, then
\[
\sum_{\frac{1}{2} \leq k \leq n} T_{j,k} \equiv 2 S_j(\Phi_{2n}) \pmod{M_n}
\]

**Proof.** Let \( \gamma = 2 \cos \frac{\pi}{n} \) then
\[
\sum_{\frac{1}{2} \leq k \leq n} T_{j,k} = 2 \Re \left( \sum_{\frac{1}{2} \leq k \leq n} \frac{e^{2\pi i k j}}{n} \right) = 2 S_j(\Phi_{2n})
\]

because \( S_j(\Phi_{2n}) \) is real.

Note that the sums \( S_j(\Phi_{2n}) \) are known as Ramanujan sums, see Remark 25. We thus deduce that one can obtain \( S_j(P_F) \) from coefficients \( f_{i,j} \) of \( f(T_k(x))^i \) in \( \mathbb{Q}[x]/(M_n) \) with
\[
S_j(P_F) = f_{i,0} N + \sum_{\frac{1}{2} \leq j \leq n} f_{i,j} S_j(\Phi_{2n})
\]

\[ \text{(14)} \]

Equation (14) gives a linear relation between the Newton sums of \( \Phi_{2n} \) and the Newton sums of \( P_F \). The associated matrix is \( (f_{i,j}) = [T_j(x) f(x)] \). Note that \( (f_{i,j}) \) are not unique but the Formula (14) does not depend on them. We thus deduce Algorithm 5.

**Algorithm 5: Compute \( P_F \)**

**Input:** \( [T_j] f_0 + \sum_{j=1}^{n-1} f_j T_j \)

**Output:** \( P_F = \text{Res}(z - f(x), M_n(x)) \)

1. \[ \text{begin} \]
2. \[ \text{Compute} [T_j] M_n = \sigma_0 + \sum_{i=1}^N \sigma_i T_i ; \]
3. \[ \text{for } i \leftarrow 2 \text{ to } N \text{ do} \]
4. \[ \text{Compute the Newton sums} \]
5. \[ S_i = i \sigma_i - (i-1) \sigma_{i-1} S_{i-1} ; \]
6. \[ \text{for } i \leftarrow 2 \text{ to } N \text{ do} \]
7. \[ \text{Compute} \]
8. \[ \text{Compute} \]
9. \[ \text{return} \]

**PROPOSITION 24.** We can compute \( P_F \) in \( \mathcal{O}(n^3 \tau) \ bit operations.

**Proof.** We first compute \( [T_j] M_n \) in \( \mathcal{O}(n^3 \tau) \ bit operations. We obtain \( [T_j] M_n = \sigma_0 + \sum_{i=1}^N \sigma_i T_i \). As \( \Phi_{2n} = \mathcal{O}(M_n) \) we deduce that \( \Phi_{2n} = \sum_{i=0}^{2N} b_i x^i \) where \( b_i = b_{2N-i} = \sigma_i \).

We then obtain the \( S_i(\Phi_{2n}) \) using the Newton relations:
\[
S_k = \sigma_k S_{k-1} + \ldots + \sigma_1 S_1 + \sigma_0 = 0, \quad 1 \leq k \leq N. \quad (15)
\]
Here the \( \sigma_i \)’s have size \( \mathcal{O}(n) \). We thus deduce by induction that all the \( S_k \) have size \( \mathcal{O}(n) \). \( S_k \) is computed from \( S_1, \ldots, S_{k-1} \) in \( \mathcal{O}(n \tau) \ bit operations. In conclusion \( S_k, \ldots, S_N \) may be computed in \( \mathcal{O}(n^2 \tau) \ bit operations. By induction \( f(T_k(x))^i \pmod{M_n} \) can be computed from \( f(T_k(x))^i \pmod{M_n} \) in \( \mathcal{O}(n \tau) \ bit operations, using Lemma 22. We can compute all \( f_{i,j}, 1 \leq i \leq N, 1 \leq j \leq \left\lfloor \frac{n-1}{2} \right\rfloor \) in \( \mathcal{O}(n^3 \tau) \ bit operations. We then compute each \( S_j(P_F) \) in \( \mathcal{O}(n^2 \tau) \ bit operations, using Formula (14). \text{I claim \( \mathcal{O}(n^3 \tau) \ bit operations. We then use the Newton formula (15) to get the coefficients \( \sigma_1(P_F), \ldots, \sigma_N(P_F) \) of \( P_F \):

\[
k \sigma_k(P_F) = -\sum_{i=1}^{k-1} S_i(P_F) \sigma_{k-i}(P_F).
\]

Also, all \( k \sigma_k \) have size \( \mathcal{O}(n \tau) \) and may be computed in \( \mathcal{O}(n^3 \tau) \ bit operations. As \( \sigma_k \in \mathbb{Z} \) they can all be obtained in \( \mathcal{O}(n^3 \tau) \ bit operations. \]

**REMARK 25.** The Ramanujan sums are known (see [8, Th. 272]) to satisfy
\[
S_{\nu}(\Phi_{2n}) = \mu(n / \gcd(n, m)) \varphi(n) / \gcd(n, m),
\]
where \( \mu \) is the Möbius function and \( \varphi \) is the Euler function. It means that \( S_{\nu}(\Phi_{2n}) \) may be computed in \( \mathcal{O}(n) \) binary op-

\[
\text{Once } P_F \text{ is computed, we can compute } M_F \text{ as } P_F / \gcd(P_F, P_i').
\]

\[
M_F \text{ as } P_F / \gcd(P_F, P_i').
\]
Here $P_f$ has degree $N$ and bitsize $O(n\tau)$. Then $h = \gcd(P_f, P_f')$ is calculated in time $O(n^3\tau)$, using Proposition 5.

Using Proposition 5, we know that $\tau(h) = O(n\tau)$ so that the last operation $M_f = P_f/h$ claims $O(n^2\tau)$ bit operations.

Finally we deduce

**Proposition 26.** We can compute the minimal polynomial $M_f$ of $f(2\cos \frac{\pi}{n})$ in $O(n^3\tau)$ binary operations.

**Example**

Consider $F = 2a\cos \frac{\pi}{n} + 2b\cos \frac{2\pi}{n}$. We write $F = f(2\cos \frac{\pi}{n})$ where $f = aT_5 + bT_7$.

The minimal polynomial of $2\cos \frac{\pi}{35}$ is

$$M_{35} = T_{12} + T_{11} - T_7 - T_5 - T_4 + T_3 + T_1 + 1$$

$$= t^{12} + t^{11} - 121t^9 - 11t^8 + 54t^6 + 43t^5$$

$$- 113t^4 - 71t^3 + 110t^2 + 46t^3 - 40t^2 - 8t + 1.$$

Computing $P_f = \text{Res}(z - aT_5 - bT_7, M_{35})$ we obtain $P_f = M_f$ where

$$M_f = z^6 - (3h + 2c)z^5 + c(-3c + 5b)z^4$$

$$+ (5b^3 + 6bc^2 + 6c^3)z^3$$

$$- c(5b^3 + 7bc + 9bc^2 - 2c^3)z^2$$

$$- (3b^5 - 4b^2c^2 - 7b^2c^3 + 2bc^4 + 4c^5)z$$

$$- b^5 + b^2c + 7c^2b^4 - 2b^3c^3 - 7b^2c^4 + 2bc^5 + c^6.$$ 

### 7. REFERENCES


