ACTA ARITHMETICA
140.3 (2009)

Fast computation of Gauss sums and resolution of the root of unity ambiguity

by

Dang Khoa Nguyen and Bernhard Schmidt (Singapore)

1. Introduction. The evaluation of Gauss sums is a celebrated problem which has been studied since [11]. Gauss himself found an explicit formula for quadratic Gauss sums over prime fields. The general case of Gauss sums over finite fields is known to be much harder—only partial solutions in special cases are known (see [5, 15, 23, 28], for instance). The difficulty of the problem is apparent from the fact that some of these results, which in fact deal with the "easiest cases", already give rise to formulas involving class numbers of quadratic number fields. Thus, in general, it is hopeless to try to obtain simple explicit formulas for the values of Gauss sums.

However, in many circumstances it is still of great worth to find the exact values of Gauss sums, as complicated as they may be. For instance, these values can be used to determine the number of solutions of certain polynomial equations of finite fields [12]. Furthermore, the knowledge of exact values of Gauss sums is important in finite geometry: the intersection numbers of hyperplanes in finite projective spaces with certain point sets are linear combinations of Gauss sums [8, 21]. This is useful in searching for projective two-intersections sets and strongly regular graphs [8]. A further application of Gauss sums, which has been investigated for decades [4, 5, 10, 14, 16, 21, 22, 28], is the determination of weight distributions of irreducible cyclic codes. We will apply our algorithm to this problem to demonstrate its efficiency.

Since the exact values of Jacobi sums can be obtained from those of Gauss sums by a simple identity [31, Lemma 6.2], our algorithm can be used to compute Jacobi sums too. This opens up a whole range of further applications. One of the most important of these is finding cyclotomic numbers [5, 24] in cases which are too intricate to be settled by explicit formulas.

2010 *Mathematics Subject Classification*: Primary 11T24; Secondary 11Y40.
Key words and phrases: Gauss sums, H-polynomials, Fincke–Pohst algorithm, irreducible cyclic codes.

DOI: 10.4064/aa140-3-1

Cyclotomic numbers are useful for a vast number of combinatorial problems, including the study of difference sets [24] and Hadamard matrices [13]. Jacobi sums have further important applications, including primality testing [1, 9, 17, 18], units in cyclotomic fields [25], Vandiver's conjecture [26], and irreducible polynomials of Gaussian periods [27].

Our paper is organized as follows. In Section 2, we list some technical results mainly due to Baumert [3]. These will be used for the resolution of the root of unity ambiguity. In Section 3, we introduce "H-polynomials" on which our recursive procedure for computing Gauss sums is based. Though our H-polynomials are closely related to those used in [4, 16], our modifications are essential and indispensable for the proofs of our key results.

In Section 4, we deal with an ambiguity issue which is ubiquitous in the study of Gauss sums: it is nontrivial to specify the multiplicative characters involved in Gauss sums in a consistent way. In fact, in the literature on the evaluation of Gauss sums, this has sometimes led to results which give the values of Gauss sums only up to application of automorphisms of the underlying cyclotomic field. In our case, we cannot allow any ambiguity of this kind, as our recursive procedure would break down completely. A conceivable approach to specifying the multiplicative characters would be to prescribe primitive elements of the finite fields involved. However, this is inefficient as the fields we are considering can be so large that finding a primitive element is impossible. Our solution is to introduce "start polynomials" which help to deal with this issue efficiently, and which are also convenient to use in the application of Stickelberger's theorem which is a crucial step in our algorithm.

In Section 5, we present our method for computing Gauss sums up to multiplication with a root of unity. This algorithm is an enhancement and adaptation of the method described in [29, Section 7] for the fast computation of Jacobi sums. The main difference is that we are working in a subfield of the underlying cyclotomic field instead of this field itself. Working in a field of smaller absolute degree gives us huge speed advantages, but this comes at a price: we have to overcome several obstacles as the arithmetic of a general abelian number field is more difficult to handle than that of a full cyclotomic field. For instance, cyclotomic fields have integral bases consisting of consecutive powers of a root of unity and thus Kummer's theorem [20, pp. 196–198] can be applied to compute generators of prime ideals. For subfields, Kummer's theorem cannot be used in this way. Our main tools for the arithmetic of the subfields are Zumbroich bases [5] and a result (Proposition 14) which allows us to efficiently "transfer" Kummer's theorem from the full cyclotomic field to the subfield.

The resolution of the root of unity ambiguity will be presented in Section 6. First we exploit the integrality of the coefficients of H-polynomials to deal with a large number of cases. The remaining cases are settled by considering the values of the derivative of H-polynomials at certain roots of unity.

In Section 7 we show how our recursive algorithm can be implemented efficiently using a kind of Möbius inversion. This procedure is based on ideas of Baumert [3]. Section 8 contains the complete description of our algorithm for computing Gauss sums. Finally, in Section 9, we apply our method to the computation of weight distributions of binary irreducible cyclic codes. We are able to compute the weight distribution of all such codes of length n and dimension k with $\frac{2^k-1}{n} \leq 5000$. This substantially extends previously known results [30].

2. Preliminaries. For a positive integer w write $\zeta_w = \exp 2\pi i/w$.

RESULT 1. *Let n be a positive integer, and let $f = \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in \mathbb{Z}$. Then*

$$a_i = \frac{1}{n}\sum_{j=0}^{n-1} f(\zeta_n^j)\zeta_n^{-ij}$$

for $i = 0, \ldots, n-1$. In particular, if $f, g \in \mathbb{Z}[x]$ are polynomials of degree less than n and $f(\zeta_d) = g(\zeta_d)$ for all divisors d of n, then $f = g$.

We will need the following result of Kronecker [5, Thm. 2.1.12].

RESULT 2. *An algebraic integer all of whose conjugates have absolute value 1 is a root of unity.*

We denote by Φ_w the wth cyclotomic polynomial over $\mathbb{Q}$, i.e., $\Phi_w \in \mathbb{Z}[x]$ is the minimum polynomial of ζ_w over $\mathbb{Q}$. Let R be a ring, and let $I = xR + yR$ be the ideal of I generated by $x, y \in R$. If $r, s \in R$ with $r - s \in I$, we write $r \equiv s \pmod{x, y}$.

The following result has been used extensively by Baumert [3]. For the convenience of the reader, we include a proof.

LEMMA 3. *Let $w = p^b w_1$ where p is a prime and b, w_1 are positive integers with $\gcd(p, w_1) = 1$. Then*

$$x^{w/p} - 1 \equiv 0 \pmod{p, \Phi_{w_1}^{p^{b-1}}} \quad \text{and} \quad \Phi_w \equiv 0 \pmod{p, \Phi_{w_1}^{p^{b-1}}}.$$

Proof. We have $\Phi_{w_1}^{p^{b-1}}(x) \equiv \Phi_{w_1}(x^{p^{b-1}}) \pmod{p}$. Furthermore, note that the roots of $\Phi_{w_1}(x^{p^{b-1}})$ in $\mathbb{C}$ are exactly $\zeta_{w_1}^i \zeta_{p^{b-1}}^j$, $i, j \in \mathbb{Z}$, $\gcd(i, w_1) = 1$. Each of these roots is a root of $x^{w/p} - 1$ as well. Hence $x^{w/p} - 1 \equiv 0 \pmod{\Phi_{w_1}(x^{p^{b-1}})}$ and thus $x^{w/p} - 1 \in (p, \Phi_{w_1}^{p^{b-1}})$.

Note that $\Phi_{w_1}(x^{p^{b-1}})\Phi_w(x) = \Phi_{w_1}(x^{p^b})$ since the polynomials on both sides have the same complex roots. Hence

$$\Phi_{w_1}^{p^{b-1}}(\Phi_w - \Phi_{w_1}^{p^b-p^{b-1}}) \equiv 0 \pmod{p}.$$

This implies $\Phi_w \in (p, \Phi_{w_1}^{p^{b-1}})$. ∎

Lemma 3 implies the following important result of Baumert [3].

Result 4. *Let $w = p^a w_1$ where p is a prime and a, w_1 are positive integers with* $\gcd(p, w_1) = 1$. *Let $F, G, H \in \mathbb{Z}[x]$ with*

$$F \equiv G \pmod{\Phi_w} \quad \textit{and} \quad F \equiv H \pmod{x^{w/p} - 1}.$$

Then

$$G \equiv H \pmod{p, \Phi_{w_1}^{p^{a-1}}}.$$

3. Gauss sums and H-polynomials. Let p be a prime and $q = p^r$ where r is a positive integer. We denote by Tr the absolute trace function of $\mathbb{F}_q$. Let N be a divisor of $q-1$, and χ be a multiplicative character of $\mathbb{F}_q$ of order dividing N. The corresponding Gauss sum is defined by

$$G(\chi) = \sum_{\alpha \in \mathbb{F}_q^*} \chi(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)}. \tag{1}$$

Note that $G(\chi) \in \mathbb{Q}(\zeta_{Np})$.

Let γ be a generator of $\mathbb{F}_q$ and for $\alpha \in \mathbb{F}_q^*$ let $\mathrm{ind}_\gamma(\alpha)$ be the unique integer with $\gamma^{\mathrm{ind}_\gamma(\alpha)} = \alpha$ and $0 \le \mathrm{ind}_\gamma(\alpha) < q-1$. It will be convenient to define the function ind_γ for integer arguments too. Let 1_q be the multiplicative identity element of $\mathbb{F}_q$. For $c \in \mathbb{Z}^+$, set $\bar{c} = \sum_{i=1}^{c} 1_q$ and $\mathrm{ind}_\gamma(c) = \mathrm{ind}_\gamma(\bar{c})$.

Definition 5. Let $q = p^r$ where p is a prime and r is a positive integer, and let N be a divisor of $q-1$. Let $f \in \mathbb{F}_p[x]$ be an irreducible factor of Φ_N over $\mathbb{F}_p$, and γ a primitive element of $\mathbb{F}_q$ with $f(\gamma^{(q-1)/N}) = 0$. We define $H_{q,N,f} \in \mathbb{Z}[x]$ as the unique polynomial of degree less than Np with

$$H_{q,N,f} \equiv \sum_{\alpha \in \mathbb{F}_q^*} x^{q\,\mathrm{ind}_\gamma(\alpha) + (p-1)(q-1)\mathrm{Tr}(\alpha)} \pmod{x^{Np} - 1}. \tag{2}$$

We refer to $H_{q,N,f}$ as an *H-polynomial* and call f the *start polynomial* of $H_{q,N,f}$.

It will turn out that H-polynomials are very useful for the computation of Gauss sums and weights of irreducible cyclic codes. Our H-polynomials are a modified version of the polynomial introduced in [4, p. 159]. Our modifications are crucial for determining the exact roots of unity involved in the computation of Gauss sums, see Section 6.

If an H-polynomial is computed a naive way by (2), a primitive element of $\mathbb{F}_q$ has to be constructed. When q is large, this may be impossible. Moreover, the summation according to (2) becomes intractable for large q. We will be interested in more efficient methods for computing H-polynomials which avoid computations in $\mathbb{F}_q$. In particular, we will remove the necessity of constructing a primitive element of $\mathbb{F}_q$.

We first show that our H-polynomials are properly defined, i.e., that $H_{q,N,f}$ does not depend on the choice of γ.

LEMMA 6. *Let $H_{q,N,f}$ be defined by* (2). *Let τ be a primitive element of $\mathbb{F}_q$ with $f(\tau^{(q-1)/N}) = 0$, and let $G \in \mathbb{Z}[x]$ with* $\deg(G) < Np$ *and*

$$G \equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{q\,\mathrm{ind}_\tau(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \pmod{x^{Np}-1}.$$

Then $G = H_{q,N,f}$.

Proof. Since $\gamma^{(q-1)/N}$ and $\tau^{(q-1)/N}$ are roots of the same irreducible polynomial, they are conjugate in $\mathbb{F}_q$, i.e., $\gamma^{(q-1)/N} = \tau^{p^a(q-1)/N}$ for some nonnegative integer $a < r$. This implies $\mathrm{ind}_\tau(\alpha) \equiv p^a\,\mathrm{ind}_\gamma(\alpha)$ (mod N) and thus $x^{p\,\mathrm{ind}_\tau(\alpha)} \equiv x^{p^{a+1}\mathrm{ind}_\gamma(\alpha)}$ (mod $x^{Np}-1$) for all $\alpha \in \mathbb{F}_q^*$. We find

$$\begin{aligned} G &\equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{qp^a\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \\ &\equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{qp^a\,\mathrm{ind}_\gamma(\alpha^{p^{r-a}})+(p-1)(q-1)\mathrm{Tr}(\alpha^{p^{r-a}})} \\ &\equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{q^2\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{q\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \\ &\equiv H_{q,N,f} \pmod{x^{Np}-1}. \ \blacksquare \end{aligned}$$

For every character χ of $\mathbb{F}_q^*$ of order dividing N, the Gauss sum $G(\chi)$ can be computed from $H_{q,N,f}$ as follows:

$$\begin{aligned} G(\chi) &= \sum_{\alpha\in\mathbb{F}_q^*} \chi(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)} = \sum_{\alpha\in\mathbb{F}_q^*} \chi(\gamma)^{\mathrm{ind}_\gamma(\alpha)}\zeta_p^{\mathrm{Tr}(\alpha)} \\ &= \sum_{\alpha\in\mathbb{F}_q^*} (\chi(\gamma)\zeta_p)^{q\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} = H_{q,N,f}(\chi(\gamma)\zeta_p). \end{aligned} \tag{3}$$

LEMMA 7. *Let $H = H_{q,N,f}$ be given by* (2). *Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{pN})/\mathbb{Q}(\zeta_p))$ be defined by $\tau(\zeta_N) = \zeta_N^p$. For $c \in \{1,\ldots,p-1\}$, define $\sigma_c \in \mathrm{Gal}(\mathbb{Q}(\zeta_{pN})/\mathbb{Q}(\zeta_N))$ by $\zeta_p^{\sigma_c} = \zeta_p^c$. We have*

$$
\begin{aligned}
H(1) &= q-1, \\
H(\zeta_N\zeta_p)^{\tau} &= H(\zeta_N\zeta_p), \\
H(\zeta_N^j\zeta_p^i)^{\sigma_c} &= \zeta_N^{-j\,\mathrm{ind}_\gamma(c)}H(\zeta_N^j\zeta_p^i) && \textit{for } j=1,\dots,N-1,\ i=1,\dots,p-1, \\
H(\zeta_p^i) &= -1 && \textit{for } i=1,\dots,p-1, \\
H(\zeta_N^j) &= 0 && \textit{for } j=1,\dots,N-1, \\
|H(\zeta_N^j\zeta_p^i)|^2 &= q && \textit{for } j=1,\dots,N-1,\ i=1,\dots,p-1.
\end{aligned} \tag{4}
$$

Proof. The first five equations can be proved by straightforward computation. For the last equation, let χ be the character of $\mathbb{F}_q^*$ with $\chi(\gamma)=\zeta_N^j$ and note that

$$H(\zeta_N^j\zeta_p^i) = H(\zeta_N^j\zeta_p)^{\sigma_i} = \zeta_N^{-j\,\mathrm{ind}_\gamma(i)}H(\zeta_N^j\zeta_p) = \zeta_N^{-j\,\mathrm{ind}_\gamma(i)}G(\chi) \tag{5}$$

by the third equation and by (3). Now the last equation follows from a standard property of Gauss sums [5]. ∎

4. Synchronizing H-polynomials. It will turn out that, in order to compute an H-polynomial $H_{q,N,f}$ defined by (2), we need to know polynomials h_M with

$$H_{q,N,f} \equiv h_M \pmod{x^{Mp}-1}$$

for all proper divisors M of N. These polynomials h_M can be computed recursively from H-polynomials H_{q,M,f_M} where the f_M's are appropriate start polynomials. The difficulty here is that $H_{q,N,f} \equiv H_{q,M,f_M} \pmod{x^{Mp}-1}$ in general only holds for a certain choice of the start polynomials f_M. The following result provides an efficient solution to this algorithmic problem.

Theorem 8. *Let p be a prime and $q=p^r$ where r is a positive integer. Let N be a divisor of $q-1$, and let M be a divisor of N. Let f_N, respectively f_M, be an irreducible factor of Φ_N, respectively Φ_M, over $\mathbb{F}_p$. Let $z\in\mathbb{F}_p[x]/(f_N)$ be a root of f_N. Then there is a positive integer t with*

$$t\equiv 1 \pmod p \quad \textit{and} \quad f_M(z^{tN/M})=0. \tag{6}$$

Furthermore, if t is any positive integer satisfying (6), *then*

$$H_{q,N,f_N}(x) \equiv H_{q,M,f_M}(x^t) \pmod{x^{Mp}-1}. \tag{7}$$

Proof. We view $\mathbb{F}_p[x]/(f_N)$ as a subfield of $\mathbb{F}_q$. Note that z is a primitive Nth root of unity in $\mathbb{F}_q$. Since M divides $q-1$, the polynomial f_M splits into linear factors over $\mathbb{F}_q$. Hence there is $w\in\mathbb{F}_q$ with $f_M(w)=0$. Note that w is a primitive Mth root of unity. Hence there is an integer s with $(s,M)=1$ and $w=z^{sN/M}$. This implies $f_M(z^{sN/M})=0$. Since p does not divide M, there is a positive integer t with $t\equiv 1 \pmod p$ and $t\equiv s \pmod M$. Then $f_M(z^{tN/M})=f_M(z^{sN/M})=0$. This proves the existence of a positive integer t satisfying (6).

Now let t be any positive integer t satisfying (6). Then $z^{tN/M}$ is a primitive Mth root of unity in $\mathbb{F}_q$, and thus t is coprime to M. Hence there is a positive integer u coprime to $q-1$ such that $u \equiv t \pmod{Mp}$. Let γ be a primitive element of $\mathbb{F}_q$ with $\gamma^{(q-1)/N} = z$. Then

$$H_{q,N,f_N} \equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{q\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \pmod{x^{Np}-1} \tag{8}$$

by Lemma 6. Let $\tau := \gamma^u$. Then $f_M(\tau^{(q-1)/M}) = f_M(\gamma^{u(q-1)/M}) = f_M(z^{tN/M}) = 0$. Hence

$$H_{q,M,f_M} \equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{q\,\mathrm{ind}_\tau(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \pmod{x^{Mp}-1} \tag{9}$$

by Lemma 6. Note that $\mathrm{ind}_\gamma(\alpha) \equiv u\,\mathrm{ind}_\tau(\alpha) \equiv t\,\mathrm{ind}_\tau(\alpha) \pmod{M}$ for all $\alpha \in \mathbb{F}_q^*$. Furthermore, $x^{t(q-1)} \equiv x^{q-1} \pmod{x^{Mp}-1}$ since $t \equiv 1 \pmod{p}$. Using (8), we get

$$\begin{aligned} H_{q,M,f_M}(x^t) &\equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{qt\,\mathrm{ind}_\tau(\alpha)+t(p-1)(q-1)\mathrm{Tr}(\alpha)} \\ &\equiv \sum_{\alpha\in\mathbb{F}_q^*} x^{q\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} \pmod{x^{Mp}-1}. \end{aligned} \tag{10}$$

Now (7) follows from (8) and (10), since $x^{Np}-1 \equiv 0 \pmod{x^{Mp}-1}$. ■

The Davenport–Hasse theorem on Gauss sums [5, Thm. 11.5.2] shows how to compute Gauss sums $G(\chi)$ over $\mathbb{F}_{q^s}$ from Gauss sums over $\mathbb{F}_q$ if the order of χ divides $q-1$. The following result provides an analog for H-polynomials.

Theorem 9. *Let p be a prime, let r and s be positive integers, and $q = p^r$. Let M be a divisor of $q-1$, and write $S = \sum_{i=0}^{Mp-1} x^i$. Let f be an irreducible factor of Φ_M over $\mathbb{F}_p$. Then*

$$H_{q^s,M,f} - \frac{q^s-1}{pM}\,S \equiv (-1)^{s-1}\left(H_{q,M,f} - \frac{q-1}{pM}\,S\right)^s \pmod{x^{Mp}-1}. \tag{11}$$

Proof. By Result 1, in order to prove (11), it suffices to show

$$\begin{aligned} H_{q^s,M,f}(\zeta_M^i\zeta_p^j) = (-1)^{s-1}&\left(H_{q,M,f}(\zeta_M^i\zeta_p^j) - \frac{q-1}{pM}\,S(\zeta_M^i\zeta_p^j)\right)^s \\ &+ \frac{q^s-1}{pM}\,S(\zeta_M^i\zeta_p^j) \end{aligned} \tag{12}$$

for $i = 0, \dots, M-1$, $j = 0, \dots, p-1$.

Case 1: $i = j = 0$. Then (12) holds since $H_{q^s,M,f}(1) = q^s - 1$ and $H_{q,M,f}(1) = q-1$ by Lemma 7, and $S(1) = pM$.

Case 2: $i = 0$, $j > 0$. Then $H_{q^s,M,f}(\zeta_M^i \zeta_p^j) = H_{q,M,f}(\zeta_M^i \zeta_p^j) = -1$ by Lemma 7, and $S(\zeta_M^i \zeta_p^j) = 0$. Hence (12) holds.

Case 3: $i > 0$, $j = 0$. Then $H_{q^s,M,f}(\zeta_M^i \zeta_p^j) = H_{q,M,f}(\zeta_M^i \zeta_p^j) = 0$ by Lemma 7, and $S(\zeta_M^i \zeta_p^j) = 0$. Hence (12) holds.

Case 4: $i > 0$, $j > 0$. Then $S(\zeta_M^i \zeta_p^j) = 0$. Let $\gamma \in \mathbb{F}_q$ be a primitive element of $\mathbb{F}_q$ with $f(\gamma^{(q-1)/M}) = 0$, and let χ be the character of $\mathbb{F}_q^*$ with $\chi(\gamma) = \zeta_M^j$. By Lemma 6 and (5), we have

$$H_{q,M,f}(\zeta_M^i \zeta_p^j) = \zeta_M^{-j \operatorname{ind}_\gamma(i)} G(\chi). \tag{13}$$

Let τ be a primitive element of $\mathbb{F}_{q^s}$ with $\gamma = \tau^{(q^s-1)/(q-1)}$. By Lemma 6 and (5), we have

$$H_{q^s,M,f}(\zeta_M^i \zeta_p^j) = \zeta_M^{-j \operatorname{ind}_\tau(i)} G(\chi') \tag{14}$$

where χ' is the character of $\mathbb{F}_{q^s}^*$ defined by $\chi'(\tau) = \zeta_M^i$. Note $\chi'(\tau) = \zeta_M^i = \chi(\gamma) = \chi(\tau^{(q^s-1)/(q-1)})$. Hence

$$G(\chi') = (-1)^{s-1} G(\chi)^s \tag{15}$$

by [5, Thm. 11.5.2]. Note $\operatorname{ind}_\tau(i) \equiv \frac{q^s-1}{q-1} \operatorname{ind}_\gamma(i) \equiv s \operatorname{ind}_\gamma(i) \pmod{M}$. Thus

$$\begin{aligned} H_{q^s,M,f}(\zeta_M^i \zeta_p^j) &= \zeta_M^{-j \operatorname{ind}_\tau(i)} G(\chi') = (-1)^{s-1} \zeta_M^{-j\, s \operatorname{ind}_\gamma(i)} G(\chi)^s \\ &= (-1)^{s-1} H_{q,M,f}(\zeta_M^i \zeta_p^j)^s \end{aligned}$$

by (13), (14), and (15). This, together with $S(\zeta_M^i \zeta_p^j) = 0$ shows that (12) holds in Case 4 too. ■

5. Computing Gauss sums up to multiplication with a root of unity. Van Wamelen [29] introduced an algorithm for computing Jacobi sums which is based on Stickelberger's factorization of Gauss sums [5, Thm. 11.2.2] and the LLL algorithm. We use a modified and enhanced version of this algorithm for computing Gauss sums up to multiplication with a root of unity. We will need the following facts from algebraic number theory (see [6, 12, 20]).

Result 10. *Let $q = p^r$ where p is a prime, and let N be a divisor of $q-1$ such that $r = \operatorname{ord}_N(p)$. For $h \in \mathbb{Z}[x]$, let $\bar{h}$ denote the image of h under the natural epimorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$. Let $h \in \mathbb{Z}[x]$ be such that $\bar{h}$ is an irreducible factor of Φ_N over $\mathbb{F}_p$. Then:*

(i) *The ideal $P := h(\zeta_N)\mathbb{Z}[\zeta_N] + p\mathbb{Z}[\zeta_N]$ is a prime ideal of $\mathbb{Z}[\zeta_N]$, and $\mathbb{Z}[\zeta_N]/P$ is a finite field of order q. Furthermore, for every $\alpha \in \mathbb{Z}[\zeta_N]$, $\alpha \notin P$, there is a unique $j(\alpha) \in \{0, \ldots, N-1\}$ such that*

$$\alpha^{(q-1)/N} \equiv \zeta_N^{j(\alpha)} \pmod{P}.$$

The map

$$\chi_P : (\mathbb{Z}[\zeta_N]/P)^* \to \mathbb{C}, \qquad \alpha + P \mapsto \zeta_N^{j(\alpha)} \tag{16}$$

is a character of $(\mathbb{Z}[\zeta_N]/P)^*$ *of order* N.

(ii) *If* $g \in \mathbb{Z}[x]$ *such that* $\bar{g}$ *is an irreducible factor of* Φ_N *over* $\mathbb{F}_p$, *and* $\bar{g} \neq \bar{h}$, *then* $g(\zeta_N)\mathbb{Z}[\zeta_N] + p\mathbb{Z}[\zeta_N] \neq P$.

Definition 11. Let χ_P be the character of $(\mathbb{Z}[\zeta_N]/P)^*$ defined by (16). Let $f \in \mathbb{F}_p[x]$ be the unique irreducible factor of Φ_N over $\mathbb{F}_p$ such that $P = h(\zeta_N)\mathbb{Z}[\zeta_N] + p\mathbb{Z}[\zeta_N]$ for some $h \in \mathbb{Z}[x]$ with $\bar{h} = f$. Then f is called the *start polynomial* of the Gauss sum

$$G(\chi_P) = \sum_{\alpha \in \mathbb{Z}[\zeta_N]/P} \chi_P(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)}. \tag{17}$$

Lemma 12. *Let* $q = p^r$ *where* p *is a prime*, *and let* N *be a divisor of* $q - 1$ *such that* $r = \mathrm{ord}_N(p)$. *Let* χ_P *be the character of* $(\mathbb{Z}[\zeta_N]/P)^*$ *defined by* (16), *and let* f *be the start polynomial of* $G(\chi_P)$. *Then*

$$H_{q,N,f}(\zeta_N\zeta_p) = G(\chi_P).$$

Proof. Let γ be a primitive element of $\mathbb{F}_q$ such that $f(\gamma^{(q-1)/N}) = 0$. We define a map $\sigma : \mathbb{Z}[\zeta_N]/P \to \mathbb{F}_q$ by

$$\sigma(g(\zeta_N) + P) = g(\gamma^{(q-1)/N}) \quad \text{for } g \in \mathbb{Z}[x].$$

We first show that σ is well defined. Let $g, h \in \mathbb{Z}[x]$ be such that $g(\zeta_N) + P = h(\zeta_N) + P$. Then $g(\zeta_N) - h(\zeta_N) \in P = k(\zeta_N)\mathbb{Z}[\zeta_N] + p\mathbb{Z}[\zeta_N]$ where $k \in \mathbb{Z}[x]$ with $\bar{k} = f$. Hence there are $a, b, c \in \mathbb{Z}[x]$ such that $g - h = ka + pb + c\Phi_N$ in $\mathbb{Z}[x]$. Since $\bar{k}$ is an irreducible factor of Φ_N over $\mathbb{F}_p$, there are $d, e \in \mathbb{Z}[x]$ with $\Phi_N = ke + pd$. Furthermore, $k(\gamma^{(q-1)/N}) = 0$ since $f(\gamma^{(q-1)/N}) = 0$. Hence $g(\gamma^{(q-1)/N}) - h(\gamma^{(q-1)/N}) = 0$, i.e., $\sigma(g(\zeta_N) + P) = \sigma(h(\zeta_N) + P)$. This shows that σ is well defined. It is straightforward to check that σ is a field homomorphism. Now assume $\sigma(g(\zeta_N) + P) = 0$, i.e., $g(\gamma^{(q-1)/N}) = 0$. Since $\bar{k}$ is the minimum polynomial of $\gamma^{(q-1)/N}$ over $\mathbb{F}_p$, there are $l, m \in \mathbb{Z}[x]$ with $g = pl + mk$. Hence $g(\zeta_N) \in P$. This shows that σ is injective. Since $\mathbb{Z}[\zeta_N]/P$ and $\mathbb{F}_q$ are fields of the same order, σ is a field isomorphism.

Let $g \in \mathbb{Z}[\zeta_N]$ be such that $g + P$ is the primitive element of $\mathbb{Z}[\zeta_N]/P$ with $\sigma(g + P) = \gamma$. Then $\sigma(g^{(q-1)/N} + P) = \gamma^{(q-1)/N} = \sigma(\zeta_N + P)$. Hence $g^{(q-1)/N} + P = \zeta_N + P$. Let $i \in \{0, 1, \ldots, q-2\}$ be arbitrary. Then $(g^i)^{(q-1)/N} \equiv \zeta_N^i \pmod{P}$. Hence, by the definition of j in Result 10, we have $j(g^i) \equiv i \pmod{N}$. We find

$$\begin{aligned}G(\chi_P) &= \sum_{u\in(\mathbb{Z}[\zeta_N]/P)^*} \chi_P(u)\zeta_p^{\mathrm{Tr}(u)} = \sum_{i=0}^{q-2} \chi_P(g^i+P)\zeta_p^{\mathrm{Tr}(g^i+P)}\\ &= \sum_{i=0}^{q-2} \zeta_N^{j(g^i)}\zeta_p^{\mathrm{Tr}(g^i+P)} = \sum_{i=0}^{q-2} \zeta_N^{i}\zeta_p^{\mathrm{Tr}(g^i+P)} = \sum_{i=0}^{q-2} \zeta_N^{i}\zeta_p^{\mathrm{Tr}(\sigma^{-1}(\gamma^i))}\\ &= \sum_{i=0}^{q-2} \zeta_N^{i}\zeta_p^{\sigma^{-1}(\mathrm{Tr}(\gamma^i))} = \sum_{i=0}^{q-2} \zeta_N^{i}\zeta_p^{\mathrm{Tr}(\gamma^i)} = \sum_{\beta\in\mathbb{F}_q^*} \zeta_N^{\mathrm{ind}_\gamma(\beta)}\zeta_p^{\mathrm{Tr}(\beta)}\\ &= H_{q,N,f}(\zeta_N\zeta_p). \ \blacksquare\end{aligned}$$

The following simple fact is crucial for the efficiency of our computations.

Lemma 13. *Let $G(\chi_P)$ be given by* (17). *Let K be the subfield of $\mathbb{Q}(\zeta_{Np})$ fixed by τ, where τ is the automorphism of $\mathbb{Q}(\zeta_{Np})$ defined by $\zeta_N^\tau = \zeta_N^p$ and $\zeta_p^\tau = \zeta_p$. Then $G(\chi_P) \in K$.*

Proof. This follows from (4) and Lemma 12. ■

Lemma 13 gives us substantial computational advantages since the degree of K over $\mathbb{Q}$ is usually much smaller than that of $\mathbb{Q}(\zeta_{Np})$. However, the implementation is far from straightforward and requires overcoming several algorithmic problems. For instance, it is inefficient to implement the arithmetic in K based on the usual representation $K \cong \mathbb{Q}[x]/(g)$ where $g \in \mathbb{Z}[x]$ is a suitable irreducible polynomial. Experiments show that the coefficients of g will be too large to allow efficient computations. In particular, the integral bases for the ring of algebraic integers of K that can be obtained in this way contain elements whose coefficients are rational numbers with huge denominators.

To overcome these problems, we represent the ring A of algebraic integers of K by Zumbroich bases (see [7]) which are ideally suited for fast computations. This process is quite tedious and the details are skipped here. A complete description of the construction of these integral bases, adapted to the problem of computing Gauss sums, can be found in [19].

Once we have obtained suitable integral bases for A, we need to find the prime ideal factorization of p in A, and the prime ideals involved have to be expressed in terms of the integral bases. As a preparation, we need the following result. We refer to [6, 12, 20] for the necessary background on prime ideal factorization in cyclotomic fields.

Proposition 14. *We use the notation of Lemma* 13. *Let A be the ring of algebraic integers of K. We write $\lambda = 1 - \zeta_p$. Let α be an element of $\mathbb{Z}[\zeta_N]$ such that $D = \alpha\mathbb{Z}[\zeta_N] + p\mathbb{Z}[\zeta_N]$ is a prime ideal of $\mathbb{Z}[\zeta_N]$ above p.*

(a) *Let δ be the unique prime ideal of $\mathbb{Z}[\zeta_{Np}]$ containing D, and $\varDelta = \delta \cap K$. Then*

$$\delta = \alpha\mathbb{Z}[\zeta_{Np}] + \lambda\mathbb{Z}[\zeta_{Np}], \qquad \varDelta = N_{\mathbb{Q}(\zeta_{Np})/K}(\alpha)A + \lambda A.$$

(b) *Let β be an element of A such that $\varDelta = \beta A + \lambda A$. Then* $\gcd(\varDelta^2, \beta A) = \varDelta$ *if and only if* $\gcd(p^2, N_{K/\mathbb{Q}}(\beta)) = p$. *Furthermore*, *if* $\gcd(\varDelta^2, \beta A) \neq \varDelta$ *then* $\gcd(\varDelta^2, (\beta+\lambda)A) = \varDelta$.

(c) *Let $\varDelta_1, \ldots, \varDelta_m$ be*, *not necessarily distinct*, *prime ideals of A above p. Let $\beta_1, \ldots, \beta_m$ be elements of A such that*

$$\beta_i A + \lambda A = \varDelta_i = \gcd(\varDelta_i^2, \beta_i A)$$

for $i = 1, \ldots, m$. Then

$$\prod_{i=1}^{m} \varDelta_i^{c_i} = \Big(\prod_{i=1}^{m} \beta_i^{c_i}\Big) A + \lambda^{c_1+\cdots+c_m} A \tag{18}$$

for all positive integers $c_1, \ldots, c_m$.

Proof. (a) We have $\lambda\mathbb{Z}[\zeta_{Np}] = \pi_1 \cdots \pi_g$ where $g = \varphi(N)/r$ and $\pi_1, \ldots, \pi_g$ are the prime ideals of $\mathbb{Z}[\zeta_{Np}]$ above p. Furthermore, $\pi_i = \varPi_i\mathbb{Z}[\zeta_{Np}]$ for $i = 1, \ldots, g$ where $\varPi_1, \ldots, \varPi_g$ are the prime ideals of A above p. Hence $\delta = \pi_i$ and $\varDelta = \varPi_i$ for some i. Since $\delta^{p-1} = D\mathbb{Z}[\zeta_{Np}] = \alpha\mathbb{Z}[\zeta_{Np}] + p\mathbb{Z}[\zeta_{Np}]$, we conclude that δ is the only prime ideal of $\mathbb{Z}[\zeta_{Np}]$ above p containing α. Hence $\alpha\mathbb{Z}[\zeta_{Np}] + \lambda\mathbb{Z}[\zeta_{Np}] = \gcd(\alpha\mathbb{Z}[\zeta_{Np}], \lambda\mathbb{Z}[\zeta_{Np}]) = \delta$, as the evaluation of $\lambda\mathbb{Z}[\zeta_{Np}]$ at δ is 1.

Since the prime ideals above p are inert in the extension $\mathbb{Q}(\zeta_{Np})/K$, we conclude that $\varDelta$ is the only prime ideal of A containing $N_{\mathbb{Q}(\zeta_{Np})/K}(\alpha)$. Since $\lambda A = \varPi_1 \cdots \varPi_g$, we get $\varDelta = N_{\mathbb{Q}(\zeta_{Np})/K}(\alpha)A + \lambda A$.

(b) As before, note that $\varDelta$ is the only prime ideal of A above p containing β. Since $N_{K/\mathbb{Q}}(\varDelta) = p$, we conclude that $N_{K/\mathbb{Q}}(\beta)$ is divisible by p^2 if and only if $\beta \in \varDelta^2$. Using $\lambda A = \varPi_1 \cdots \varPi_g$, we see that this is the case if and only if $\gcd(\varDelta^2, \beta A) = \varDelta^2$. This proves the "if and only if" statement. Now assume $\gcd(\varDelta^2, \beta A) \neq \varDelta$. Then $\gcd(\varDelta^2, \beta A) = \varDelta^2$ and thus $\gcd(\varDelta^2, (\beta+\lambda)A) = \varDelta$ as $\lambda \notin \varDelta^2$.

(c) Note that, for each i, the only prime ideal of A above p containing β_i is $\varDelta_i$. Moreover, the evaluation of $\beta_i A$ at $\varDelta_i$ is 1 since $\gcd(\varDelta_i^2, \beta_i A) = \varDelta_i$. Hence $\beta_i A = \varDelta_i J_i$ where J_i is a ideal of A coprime to λA. Hence

$$\begin{aligned}\Big(\prod_{i=1}^{m} \beta_i^{c_i}\Big) A + \lambda^{c_1+\cdots+c_m} A &= \gcd\Big(\prod_{i=1}^{m} (\beta_i A)^{c_i}, \lambda^{c_1+\cdots+c_m} A\Big) \\ &= \gcd\Big(\prod_{i=1}^{m} (\varDelta_i J_i)^{c_i}, (\varPi_1 \cdots \varPi_g)^{c_1+\cdots+c_m}\Big) = \prod_{i=1}^{m} \varDelta_i^{c_i}. \ \blacksquare\end{aligned}$$

Remark 15. The purpose of Proposition 14 is to provide an efficient way to decompose ideals of A into products of prime ideals, and this will be applied to $G(\chi_P)A$ in our main algorithm. Identity (18) will provide two elements of A which generate $G(\chi_P)A$. Using these two elements and an integral basis of A, we can apply the algorithm from [9, p. 68] to obtain a $\mathbb{Z}$-basis of $G(\chi_P)A$. We will need such a $\mathbb{Z}$-basis for the application of the Fincke–Pohst algorithm (see [9]).

Similarly to [29], we will view the ideal $G(\chi_P)A$ as a lattice. Here, by a *lattice* we mean a free $\mathbb{Z}$-module equipped with a positive-definite bilinear form. It is well known [6, 12, 20] that $G(\chi_P)A$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}] = (p-1)\varphi(N)/r$. It remains to specify the bilinear form we are using.

Definition 16. We use the notation of Lemma 13. Let A be the ring of algebraic integers of K. We define the bilinear map T on $G(\chi_P)A$ as follows:

$$T(a,b) = \mathrm{Tr}_{K/\mathbb{Q}}(a\bar{b}) \qquad \forall a,b \in G(\chi_P)A.$$

The *T-norm* of an element $a \in A$ is defined as the nonnegative real number $\sqrt{T(a,a)}$, denoted by $\|a\|_T$.

The following result is crucial for computing $G(\chi_P)$ up to a root of unity. A proof can be found in [29].

Result 17. *The element $G(\chi_P)$ is a nonzero element in the lattice $G(\chi_P)A$ whose T-norm is minimal in the lattice. If α is any element of $G(\chi_P)A$ with $\|\alpha\|_T = \|G(\chi_P)\|_T$ then there is a root of unity $\zeta \in K$ such that $G(\chi_P) = \zeta\alpha$.*

By Result 17, we need to find a shortest vector in the lattice $G(\chi_P)A$. To this end, we use the Fincke–Pohst algorithm (see [9]). For the application of this algorithm, we need a Gram matrix for the bilinear form T, and this, in turn, requires a $\mathbb{Z}$-basis for $G(\chi_P)A$. To find such a $\mathbb{Z}$-basis, we use Proposition 14 and Stickelberger's factorization of Gauss sums. We will employ the theorem of Stickelberger in the form given in [5, pp. 342–346]. We summarize the most important facts in this context for the convenience of the readers.

Let P be the prime ideal from Result 10. For each integer i coprime to N, an automorphism σ_i of $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is given by $\zeta_N^{\sigma_i} = \zeta_N^i$. The decomposition group of P in the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is the cyclic group $H = \langle\sigma_p\rangle$, which is isomorphic to the subgroup $\langle p\rangle$ of $(\mathbb{Z}/N\mathbb{Z})^*$. Thus the order of H is $\mathrm{ord}_N(p)$. Let W denote a complete set of coset representatives of the subgroup $\langle p\rangle$ of $(\mathbb{Z}/N\mathbb{Z})^*$. Write $P_j = P^{\sigma_j}$. We have the following factorization of $p\mathbb{Z}[\zeta_N]$

into a product of distinct prime ideals:

$$p\mathbb{Z}[\zeta_N] = \prod_{j\in W} P_j.$$

For the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, we write $\lambda = 1 - \zeta_p$ and have

$$p\mathbb{Z}[\zeta_p] = (\lambda\mathbb{Z}[\zeta_p])^{p-1}.$$

For the extension $\mathbb{Q}(\zeta_{Np})/\mathbb{Q}(\zeta_N)$, there is only one prime ideal of $\mathbb{Z}[\zeta_{Np}]$ lying above P, which is denoted by Q. For each $j \in W$, we denote by Q_j the prime ideal of $\mathbb{Z}[\zeta_{Np}]$ lying above P_j. For $j \in W$, we have

$$P_j\mathbb{Z}[\zeta_{Np}] = Q_j^{p-1}.$$

For every integer a that is not divisible by N, let $L(a)$ denote the smallest positive integer congruent to a modulo N. Let $a_0, \dots, a_{r-1} \in \{0, \dots, p-1\}$ be the unique numbers with

$$L(a)\,\frac{q-1}{N} = a_0 + a_1p + \dots + a_{r-1}p^{r-1}.$$

We define

$$s(a) = a_0 + a_1 + \dots + a_{r-1}.$$

Now we are ready to state Stickelberger's theorem. For a proof, see [5, p. 346].

Result 18. *For every integer a not divisible by N, we have*

$$G(\chi_P^{-a})\mathbb{Z}[\zeta_{Np}] = \prod_{j\in W} Q_{j^{-1}}^{s(aj)}.$$

In particular,

$$G(\chi_P)\mathbb{Z}[\zeta_{Np}] = \prod_{j\in W} Q_{j^{-1}}^{s(-j)}.$$

Corollary 19. *We use the notation introduced above. For a prime ideal Q of $\mathbb{Z}[\zeta_{Np}]$ let $\tilde{Q}$ be unique prime ideal of K contained in Q. Then*

$$G(\chi_P)A = \prod_{j\in W} \tilde{Q}_{j^{-1}}^{s(-j)}.$$

Proof. This follows from Stickelberger's theorem since $\tilde{Q}\mathbb{Z}[\zeta_{Np}] = Q$. ∎

Now we can finally introduce our algorithm; its correctness follows from the previous results of this section.

Algorithm 20 (Computing Gauss sums up to a root of unity). We use the notation introduced in this section.

Input:

- a positive integer $N > 1$, a prime number p coprime to N, and $q = p^r$ where $r = \operatorname{ord}_N(p)$,
- an irreducible divisor f of $\Phi_N(X)$ over $\mathbb{F}_p$.

Output: $\alpha \in A$ such that $G(\chi_P) = \eta\alpha$ for some root of unity η.

Step 1. Find the coset representatives W of $\langle p \rangle$ in $(\mathbb{Z}/N\mathbb{Z})^*$.

Step 2. Compute $g = N_{\mathbb{Q}(\zeta_{Np})/K}(f(\zeta_N))$ to get the prime ideal $\tilde{Q} = gA + \lambda A$ of A. If $N_{K/\mathbb{Q}}(g) \equiv 0 \pmod{p^2}$, replace g by $g + \lambda$. For each i in W, apply the automorphism σ_i of $\mathbb{Q}(\zeta_{Np})$ to g to get all the prime ideals $\tilde{Q}_i = g_i A + \lambda A$ of A above p.

Step 3. For each j in W, compute the exponent $s(-j)$ as described in Result 18. Compute

$$h_1 = \lambda^{\sum_{j\in W} s(-j)}, \qquad h_2 = \prod_{j\in W} g_{j^{-1}}^{s(-j)}.$$

Then $G(\chi_P)A = h_1A + h_2A$ by Proposition 14 and Result 18.

Step 4. Compute an integral basis for K as in [7]. A complete description of this procedure, adapted to the case we are considering, can be found in [19].

Step 5. Given $G(\chi_P)A = h_1A + h_2A$ and an integral basis of A, apply the algorithm [9, p. 68] to obtain a $\mathbb{Z}$-basis for the lattice $G(\chi_P)A$. Compute the Gram matrix of the bilinear form T with respect to this $\mathbb{Z}$-basis.

Step 6. Given a $\mathbb{Z}$-basis of $G(\chi_P)A$ and the corresponding Gram matrix, find a shortest vector α in $G(\chi_P)A$ by the Fincke–Pohst algorithm [9, p. 104].

Step 7. Return α.

Remark 21. The third identity in (4) implies that $G(\chi_P)$ is often contained in a proper subfield of K. This can be used to speed up Algorithm 20 further and only requires straightforward modifications.

Remark 22. Let α be the output of Algorithm 20. Then $\alpha = \pm\zeta_N^i\zeta_p^j G(\chi_P)$ for some integers i, j. Let σ be the automorphism of $\mathbb{Q}(\zeta_{Np})$ defined by $\zeta_N^\sigma = \zeta_N$ and $\zeta_p^\sigma = \zeta_p^c$ where c is a primitive root mod p. By Lemmas 7 and 12, we have

$$\alpha^\sigma = \pm\zeta_N^{i-\mathrm{ind}_\gamma(c)}\zeta_p^{cj}G(\chi_P) = \zeta_N^{-\mathrm{ind}_\gamma(c)}\zeta_p^{(c-1)j}\alpha. \tag{19}$$

Note that, given α, we can compute j efficiently using (19). Let $\beta = \zeta_p^{-j}\alpha$. Then

$$\beta^\sigma = \zeta_p^{-cj}\zeta_N^{-\mathrm{ind}_\gamma(c)}\zeta_p^{(c-1)j}\alpha = \zeta_N^{-\mathrm{ind}_\gamma(c)}\zeta_p^{-j}\alpha = \zeta_N^{-\mathrm{ind}_\gamma(c)}\beta.$$

Let $\Gamma \in \mathbb{Z}[x]$ be such that $\Gamma(\zeta_N\zeta_p) = \beta$. Let τ be defined as in Lemma 13. Note $\alpha^\tau = \alpha$ and thus $\beta^\tau = \beta$ since $\alpha \in K$. We have

$$\Gamma(\zeta_N\zeta_p)^\sigma = \zeta_N^{-\mathrm{ind}_\gamma(c)}\Gamma(\zeta_N\zeta_p), \qquad \Gamma(\zeta_N\zeta_p)^\tau = \Gamma(\zeta_N\zeta_p),$$

and from Lemma 12 and Algorithm 20, we conclude that $\Gamma(\zeta_N\zeta_p)$ and $H_{q,N,f}(\zeta_N\zeta_p)$ differ only by multiplication with a root of unity. It will be the polynomial Γ we have just obtained that will be used in the further sections.

6. Finding the root of unity. We have seen how to compute Gauss sums up to multiplication with a root of unity. In this section, we show how to use H-polynomials to find the exact root of unity by a recursive method. To this end, we need to be able to distinguish an H-polynomial $H_{q,N,f}$ from its "translates" $x^j H_{q,N,f}$, $j = 1, \ldots, Np-1$. This is the purpose of the results in this section.

We first introduce some notation which we use throughout Sections 6 and 7.

Notation 23. Let $q = p^r$ where p is a prime and r is a positive integer. Let N be a divisor of $q-1$. By $\mathcal{D}(N)$ we denote the set of prime divisors of N. For $s \in \mathcal{D}(N)$, we write $N = N_s s^{j_s}$ with $(N_s, s) = 1$.

(i) Let f be an irreducible factor of Φ_N over $\mathbb{F}_p$, and let $z \in \mathbb{F}_p[x]/f$ be a root of f. For each divisor d of N, let f_d be an irreducible factor of Φ_d over $\mathbb{F}_p$, and let t_d be a positive integer with $f_d(z^{t_d N/d}) = 0$. The existence of t_d is guaranteed by Theorem 8.

(ii) For $\Gamma \in \mathbb{Z}[x]$, $\delta \in \{-1, 1\}$ and $i = 0, \ldots, Np-1$, we define $T_{\Gamma,\delta,i} \in \mathbb{C}[x]$ as the unique polynomial of degree less than Np such that

$$T_{\Gamma,\delta,i}(\zeta_d) = H_{q,N,f}(\zeta_d) \text{ for every proper divisor } d \text{ of } Np, \text{ and} \qquad (20)$$
$$T_{\Gamma,\delta,i}(\zeta_{Np}) = \delta\zeta_{Np}^{i}\Gamma(\zeta_{Np}).$$

(iii) Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q}(\zeta_p))$ be defined by $\tau(\zeta_N) = \zeta_N^p$. Let c be a primitive root mod p, and define $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q}(\zeta_N))$ by $\zeta_p^\sigma = \zeta_p^c$.

Remark 24. The significance of the polynomials $T_{\Gamma,\delta,i}$ lies in the following. Assume that H-polynomials H_{q,M,f_M} are known for every proper divisor M of N. Then the results of Sections 5 and 6 will enable us to find Γ, δ and i such that $H_{q,N,f} = T_{\Gamma,\delta,i}$. Hence the computation of $H_{q,N,f}$ is reduced to a recursive computation of $T_{\Gamma,\delta,i}$. The efficient calculation of $T_{\Gamma,\delta,i}$ is treated in Section 7.

Theorem 25. *Let $\Gamma \in \mathbb{Z}[x]$ be a polynomial satisfying the following conditions*:

$$\Gamma(\zeta_N\zeta_p)^\sigma = \zeta_N^{-\mathrm{ind}_\gamma(c)}\Gamma(\zeta_N\zeta_p), \qquad (21)$$

$$\Gamma(\zeta_N\zeta_p)^\tau = \Gamma(\zeta_N\zeta_p), \qquad (22)$$

(23) *$\Gamma(\zeta_N\zeta_p)$ and $H_{q,N,f}(\zeta_N\zeta_p)$ differ only by multiplication with a root of unity.*

We consider the following conditions for $\delta \in \{-1,1\}$ *and* $i = 0,\ldots,Np-1$:

(24) $\delta = 1$ *if* Np *is even*,

(25) $$i \equiv \begin{cases} 0 \pmod{Np/\gcd(N,p-1)} & \textit{if } p > 2, \\ 0 \pmod{N} & \textit{if } p = 2, \end{cases}$$

(26) $\delta x^i \Gamma(x) \equiv H_{q,N/s,f_{N/s}}(x^{t_{N/s}}) \pmod{s, \Phi_{N_s p}^{s^{j_s-1}}}$ *for every* $s \in \mathcal{D}(N)$.

Then:

(i) *There is a solution* (δ, i) *of* (24)–(26).

(ii) *If* N *is not a power of a prime* u *such that* u *divides* $p-1$, *then there is only one solution* (δ, i) *of* (24)–(26), *and* $H_{q,N,f} = T_{\Gamma,\delta,i}$ *where* $T_{\Gamma,\delta,i}$ *is defined by* (20).

(iii) *Let* N *be a power of a prime* u *such that* u *divides* $p-1$, *and let* (δ_1, i_1) *be any solution of* (24)–(26). *Then the solutions of* (24)–(26) *are exactly those pairs* (δ, i) *with* $\delta = \delta_1$ *and* $i = i_1 + jNp/u$, $j = 0,\ldots,u-1$. *Furthermore*, $T_{\Gamma,\delta,i} \in \mathbb{Z}[x]$ *for every solution* (δ, i) *of* (24)–(26), *and*

(27) $$H_{q,N,f}(x) = x^{i_1+jNp/u} T_{\Gamma,\delta_1,i_1}(x) \pmod{x^{Np}-1}$$

for some $j \in \{0,\ldots,u-1\}$.

Proof. By (23), there are $\delta_0 \in \{-1,1\}$ and $i_0 \in \{0,\ldots,Np-1\}$ such that

(28) $$H_{q,N,f}(\zeta_N\zeta_p) = \delta_0(\zeta_N\zeta_p)^{i_0}\Gamma(\zeta_N\zeta_p),$$

and $\delta_0 = 1$ if Np is even. We will show that (δ_0, i_0) is a solution of (24)–(26). Note that (24) is satisfied by the choice of δ_0. We now show that (26) holds for $(\delta, i) = (\delta_0, i_0)$. Let s be any prime divisor of N. By (28), we have

(29) $$H_{q,N,f}(x) \equiv \delta_0 x^{i_0}\Gamma(x) \pmod{\Phi_{Np}}.$$

Moreover,

(30) $$H_{q,N,f}(x) \equiv H_{q,N/s,f_{N/s}}(x^{t_s}) \pmod{x^{Np/s}-1}$$

by Theorem 8. From (29), (30) and Result 4, we see that (26) holds for (δ_0, i_0).

We now show that (25) holds for $(\delta, i) = (\delta_0, i_0)$. By Lemma 7, we have $H_{q,N,f}(\zeta_N\zeta_p)^\sigma = \zeta_N^{-\mathrm{ind}_\gamma(c)} H_{q,N,f}(\zeta_N\zeta_p)$. Since $\Gamma(\zeta_N\zeta_p)^\sigma = \zeta_N^{-\mathrm{ind}_\gamma(c)}\Gamma(\zeta_N\zeta_p)$ by (21), we infer

(31) $$((\zeta_N\zeta_p)^{i_0})^\sigma = (\zeta_N\zeta_p)^{i_0}$$

from (28). Assume $p > 2$. Then (31) implies $i_0 \equiv 0 \pmod{p}$. Write $i_0 = kp$ where k is an integer. We have $H_{q,N,f}(\zeta_N\zeta_p)^\tau = H_{q,N,f}(\zeta_N\zeta_p)$ by Lemma 7, and $\Gamma(\zeta_N\zeta_p)^\tau = \Gamma(\zeta_N\zeta_p)$ by (22). In view of (28), this shows $((\zeta_N\zeta_p)^{i_0})^\tau =$

$(\zeta_N\zeta_p)^{i_0}$. Hence $\zeta_N^k = \zeta_{Np}^{i_0} = (\zeta_{Np}^{i_0})^\tau = (\zeta_N^k)^\tau = \zeta_N^{pk}$. This implies $\zeta_N^{k(p-1)} = 1$ and thus

$$k \equiv 0 \pmod{N/\gcd(N, p-1)}.$$

Assume $p = 2$; we use (22) and (28) to get the identity $((\zeta_N\zeta_p)^{i_0})^\tau = (\zeta_N\zeta_p)^{i_0}$, which implies $\zeta_N^{i_0} = 1$ and hence $i_0 \equiv 0 \pmod N$. This shows that (25) holds for $(\delta, i) = (\delta_0, i_0)$ in every case. In summary, we have shown that (δ_0, i_0) is a solution of (24)–(26).

We now proceed to the proof of parts (ii) and (iii) of Theorem 25.

Claim 1. *If N has at least two distinct prime divisors, then (δ_0, i_0) is the unique solution of* (24)–(26). *Furthermore, if N is a power of a prime u, then*

$$\delta\delta_0\zeta_{Np}^{i-i_0} = \zeta_u^j \quad \textit{for some } j \in \{0, \ldots, u-1\} \tag{32}$$

for any solution (δ, i) of (24)–(26).

Proof. Let (δ, i) be any solution of (24)–(26), and let s be any prime divisor of N. Then

$$\delta x^i \Gamma(x) \equiv \delta_0 x^{i_0}\Gamma(x) \equiv H_{q,N,f}(x) \pmod{s, \Phi_{Nsp}^{s^{j_s-1}}} \tag{33}$$

by (26), (29), and Lemma 3. From (33), we get

$$\delta x^i H_{q,N,f}(x) \equiv \delta\delta_0 x^{i+i_0}\Gamma(x) \equiv \delta_0 x^{i_0} H_{q,N,f}(x) \pmod{s, \Phi_{Nsp}^{s^{j_s-1}}}$$

and thus

$$(\delta x^i - \delta_0 x^{i_0})H_{q,N,f}(x) \equiv 0 \pmod{s, \Phi_{Nsp}^{s^{j_s-1}}}. \tag{34}$$

Note

$$\Phi_{Nsp}^{s^{j_s-1}}(\zeta_{Np/s}) \equiv \Phi_{Nsp}(\zeta_{Np/s}^{s^{j_s-1}}) \equiv \Phi_{Nsp}(\zeta_{Nsp}) \equiv 0 \pmod s.$$

Hence (34) implies $(\delta\zeta_{Np/s}^i - \delta_0\zeta_{Np/s}^{i_0})H_{q,N,f}(\zeta_{Np/s}) \equiv 0 \pmod s$. Note that $\delta^s = \delta$ and $\delta_0^s = \delta_0$ since $\delta = \delta_0 = 1$ if s is even. Thus

$$(1 - \eta^s)H_{q,N,f}(\zeta_{Np/s}) \equiv 0 \pmod s$$

where $\eta = \delta\delta_0\zeta_{Np}^{i_0-i}$. The ideals $s\mathbb{Z}[\zeta_{Np/s}]$ and $H_{q,N,f}(\zeta_{Np/s})\mathbb{Z}[\zeta_{Np/s}]$ of $\mathbb{Z}[\zeta_{Np/s}]$ are coprime, by Lemma 7. Hence we get

$$\eta^s \equiv 1 \pmod s \qquad \text{for every prime divisor } s \text{ of } N. \tag{35}$$

If $\eta^s \notin \{-1, 1\}$, then η^s is a primitive eth root of unity for some $e \geq 3$. Since any $\varphi(e)$ consecutive powers of η^s then form an integral basis of $\mathbb{Z}[\eta^s]$, the set $\{1, \eta^s\}$ is contained in an integral basis B of $\mathbb{Z}[\eta^s]$. But then $1 - \eta^s \equiv 0 \pmod s$ implies that all coefficients y_b in a representation $1 - \eta^s = \sum_{b\in B} y_b b$, $y_b \in \mathbb{Z}$, are divisible by s. But this is impossible, since, for instance, $y_1 = 1$. This shows

$$\eta^s \in \{-1, 1\} \qquad \text{for every prime divisor } s \text{ of } N. \tag{36}$$

Case 1: $\eta = 1$. Since $\eta = \delta\delta_0\zeta_{Np}^{i_0-i}$, this implies $\delta = \delta_0$ and $i = i_0$.

Case 2: $\eta \neq 1$ and $\eta^s = 1$ for all prime divisors s of N. This implies that N is a power of some prime u. Furthermore, (35) shows that η is a primitive uth root of unity.

Case 3: $\eta^s = -1$ for some prime divisor s of N. Then (35) implies that $s = 2$ and $\eta^2 = -1$. If N has a prime divisor $s' \neq s$ then (36) implies $\eta^{s'} = \pm 1$, a contradiction. Write $N = 2^a$ where a is a positive integer. From (34) we get

$$(x^i + x^{i_0})H_{q,N,f}(x) \equiv 0 \pmod{2, \Phi_p^{2^{a-1}}}. \tag{37}$$

Note $\zeta_{2^a}^{2^{a-1}} = -1$ and $\Phi_p(-\zeta_p^{2^{a-1}}) \equiv \Phi_p(\zeta_p^{2^{a-1}}) \equiv 0 \pmod 2$. Hence (37) implies

$$(\zeta_{Np}^i + \zeta_{Np}^{i_0})H_{q,N,f}(\zeta_{Np}) \equiv 0 \pmod 2.$$

By Lemma 7, the ideals $2\mathbb{Z}[\zeta_{Np}]$ and $H_{q,N,f}(\zeta_{Np})\mathbb{Z}[\zeta_{Np/s}]$ of $\mathbb{Z}[\zeta_{Np}]$ are coprime. Hence $\zeta_{Np}^i + \zeta_{Np}^{i_0} \equiv 0 \pmod 2$. This implies $\eta = \pm 1$. Since we assume $\eta^s = \eta^2 = -1$ in Case 3, we conclude that this case cannot happen. This completes the proof of Claim 1.

Claim 2. *If N is a power of a prime u such that u does not divide $p-1$, then (δ_0, i_0) is the unique solution of* (24)–(26).

Proof. Let (δ, i) be a solution of (24)–(26). If $p = 2$, we have $i \equiv i_0 \pmod N$ and $\delta = \delta_0 = 1$. Thus $\eta = \zeta_{Np}^{i_0-i} \in \{\pm 1\}$. If $\eta = -1$ then (35) implies every prime divisor s of N is 2, contradicting the fact that $\gcd(N,p) = 1$. Thus $\eta = 1$, hence $(\delta, i) = (\delta_0, i_0)$. Now we assume $p > 2$. Since u does not divide $p - 1$, we have $\gcd(Np, p-1) = 1$ and thus $i - i_0 \equiv 0 \pmod{Np}$ by (25), hence $\eta = \delta\delta_0 \in \pm 1$ and $i = i_0$. If $u = 2$, then p is odd and 2 divides $p - 1$, a contradiction. Hence $u \neq 2$. Thus (35) shows $\eta = 1$. Therefore $\delta = \delta_0$. This proves Claim 2.

Claim 3. *$H_{q,N,f} = T_{\Gamma,\delta_0,i_0}$ where T_{Γ,δ_0,i_0} is defined by* (20).

Proof. In view of (20) and (28), we have $T_{\Gamma,\delta_0,i_0}(\zeta_d) = H_{q,N,f}(\zeta_d)$ for all divisors d of Np. Thus $T_{\Gamma,\delta_0,i_0} = H_{q,N,f}$ by Result 1. This proves Claim 3.

Claim 4. *If $p > 2$, N is a power of a prime u, and (δ, i) is a solution of* (24)–(26), *then $\delta = \delta_0$ and $i = i_0 + kNp/u$ for some integer k.*

Proof. Let (δ, i) be any solution of (24)–(26). By Cases 1 and 2 of Claim 1 (note that Case 3 of Claim 1 cannot happen), we have

$$\eta = \delta\delta_0\zeta_{Np}^{i_0-i} = \zeta_u^j \tag{38}$$

for some $j \in \{0, \ldots, u-1\}$. If Np is even, then $\delta = \delta_0 = 1$. If Np is odd, then (38) implies $\delta\delta_0 = (\delta\delta_0)^{Np} = 1$, i.e., $\delta = \delta_0$. This shows that $\delta = \delta_0$ in every case. By (38), we have $i \equiv i_0 \pmod{Np/u}$. This completes the proof of Claim 4.

CLAIM 5. *Assume that N is a power of a prime u and $p > 2$. If $\delta = \delta_0$ and $i = i_0 + jNp/u$, with $j \in \{0, \ldots, u-1\}$, then $T_{\Gamma,\delta,i} \in \mathbb{Z}[x]$.*

Proof. Let t be the unique polynomial with $\deg(t) < w$ and

$$t(x) \equiv x^{i-i_0} H_{q,N,f}(x) \pmod{x^{Np} - 1}. \tag{39}$$

Note that $t \in \mathbb{Z}[x]$ since $H_{q,N,f} \in \mathbb{Z}[x]$. Furthermore, $i - i_0 \equiv jNp/u \equiv 0 \pmod{Np/u}$. Let d be any divisor of w. If d divides Np/u, then $t(\zeta_d) = H_{q,N,f}(\zeta_d) = T_{\Gamma,\delta,i}(\zeta_d)$ by (20). If $d = N$, then $t(\zeta_d) = \zeta_d^{i-i_0} H_{q,N,f}(\zeta_d) = 0 = T_{\Gamma,\delta,i}(\zeta_d)$ by (20) and Lemma 7. Note that (28) implies $H_{q,N,f}(\zeta_{Np}) = \delta_0 \zeta_{Np}^{i_0} \Gamma(\zeta_{Np})$. Hence

$$\begin{aligned} t(\zeta_{Np}) &= \zeta_{Np}^{i-i_0} H_{q,N,f}(\zeta_{Np}) = \delta_0 \zeta_{Np}^{i} \Gamma(\zeta_{Np}) = \delta_0 \zeta_{Np}^{i} \delta \zeta_{Np}^{-i} T_{\Gamma,\delta,i}(\zeta_{Np}) \\ &= T_{\Gamma,\delta,i}(\zeta_{Np}). \end{aligned}$$

In summary, we have shown $t(\zeta_d) = T_{\Gamma,\delta,i}(\zeta_d)$ for every divisor d of Np. Hence

$$t = T_{\Gamma,\delta,i} \tag{40}$$

by Result 1, and thus $T_{\Gamma,\delta,i} \in \mathbb{Z}[x]$. This proves Claim 5.

CLAIM 6. *Assume that N is a power of a prime u such that u divides $p - 1$ (hence $p > 2$). If $\delta = \delta_0$ and $i = i_0 + jNp/u$, with $j \in \{0, \ldots, u-1\}$, then (δ, i) is a solution of (24)–(26).*

Proof. Since δ_0 satisfies (24), the same is true for δ. As u divides $p-1$, we have $\gcd(N, p-1) \equiv 0 \pmod{u}$. Hence (δ, i) also satisfies (25). By Claim 5, we have $T_{\Gamma,\delta,i} \in \mathbb{Z}[x]$. To prove that (δ, i) satisfies (26), we have to show

$$\delta x^i \Gamma(x) \equiv H_{q,N/u,f_{N/u}}(x^{t_u}) \pmod{u, \Phi_p^{N/u}}. \tag{41}$$

By (20) we have

$$\delta x^i \Gamma(x) \equiv T_{\Gamma,\delta,i}(x) \pmod{\Phi_{Np}}. \tag{42}$$

Using (39) and (40) we get

$$T_{\Gamma,\delta,i}(x) \equiv H_{q,N,f} \pmod{x^{Np/u} - 1}. \tag{43}$$

Now (41) follows from (30), (42), (43), and Lemma 3. This proves Claim 6.

Now we are ready to complete the proof of Theorem 25. We have proved part (i) already, since we have shown that (δ_0, i_0) is a solution of (24)–(26). Part (ii) follows from Claims 2 and 3. The first assertion of (iii) follows from Claims 4 and 6. The second assertion of (iii), namely, $T_{\Gamma,\delta,i} \in \mathbb{Z}[x]$, follows from the first assertion and Claim 5. Finally, (27) follows from Claim 3 and the first assertion of (iii). ■

In the case where N is a power of a prime u such that u divides $p-1$, Theorem 25 is insufficient to completely remove the root of unity ambiguity involved in the computation of H-polynomials. The following lemma is a preparation for the complete resolution of this problem.

Lemma 26. *Let $q = p^r$ where p is a prime, let* Tr *be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, and let γ be a primitive element of $\mathbb{F}_q$. Then*

$$\sum_{\substack{i=0\\ \mathrm{Tr}(\gamma^i)=k}}^{q-2} i \equiv \mathrm{ind}_\gamma(k) \pmod{q-1} \quad \textit{for every } k \in \mathbb{F}_p.$$

Proof. For $k \in \mathbb{F}_p$ define

$$P_k = \prod_{\substack{\alpha\in\mathbb{F}_q^*\\ \mathrm{Tr}(\alpha)=k}} x.$$

Note that

$$\prod_{\substack{\alpha\in\mathbb{F}_q^*\\ \mathrm{Tr}(\alpha)=k}} (x-\alpha) = -k + \sum_{i=0}^{r-1} x^{p^i}$$

since the polynomials on the left and the right hand side have the same roots. Substituting $x = 0$, we find $(-1)^p P_k = -k$. Since $(-1)^p \equiv 1 \pmod p$, we have $P_k = k$. Write

$$T = \sum_{\substack{i=0\\ \mathrm{Tr}(\gamma^i)=k}}^{q-2} i.$$

Then

$$g^T = \prod_{\substack{i=0\\ \mathrm{Tr}(g^i)=k}}^{q-2} g^i = P_k = k.$$

Hence $T \equiv \mathrm{ind}_\gamma(k) \pmod{q-1}$. ∎

Lemma 27. *Let $H = H_{q,N,f}$ be the polynomial defined by* (2), *and let H' denote the derivative of H. Then*

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(H'(\zeta_p)) \equiv \begin{cases} (q-1)/2 \pmod N & \textit{if } q \textit{ is odd},\\ 0 \pmod N & \textit{if } q \textit{ is even}.\end{cases}$$

Proof. Let $F \in \mathbb{Z}[x]$ be such that

$$H(x) = \sum_{\alpha\in\mathbb{F}_q^*} x^{q\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)} + (x^{Np}-1)F(x)$$

in $\mathbb{Z}[x]$. We compute

$$\begin{aligned} H'(x) = \sum_{\alpha\in\mathbb{F}_q^*} &(q\ \mathrm{ind}_\gamma(\alpha) + (p-1)(q-1)\mathrm{Tr}(\alpha))x^{q\,\mathrm{ind}_\gamma(\alpha)+(p-1)(q-1)\mathrm{Tr}(\alpha)-1}\\ &+ Npx^{Np-1}F(x) + (x^{Np}-1)F'(x). \end{aligned}$$

Hence

$$H'(\zeta_p) \equiv \sum_{\alpha\in\mathbb{F}_q^*} \mathrm{ind}_\gamma(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)-1} \pmod N.$$

We find

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(H'(\zeta_p)) &= \sum_{\alpha\in\mathbb{F}_q^*} \mathrm{ind}_\gamma(\alpha)\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{\mathrm{Tr}(\alpha)-1}) \equiv \sum_{i=0}^{q-2} i\,\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{\mathrm{Tr}(\gamma^i)-1}) \\
&\equiv (p-1)\sum_{\substack{i=0\\ \mathrm{Tr}(\gamma^i)=1}}^{q-2} i - \sum_{\substack{i=0\\ \mathrm{Tr}(\gamma^i)\neq 1}}^{q-2} i \equiv -\sum_{i=0}^{q-2} i + p\sum_{\substack{i=0\\ \mathrm{Tr}(\gamma^i)=1}}^{q-2} i \\
&\equiv \frac{-(q-2)(q-1)}{2} + p\sum_{\substack{i=0\\ \mathrm{Tr}(\gamma^i)=1}}^{q-2} i \pmod N.
\end{aligned}$$

Note

$$\frac{-(q-2)(q-1)}{2} \equiv \begin{cases} (q-1)/2 \pmod{q-1} & \text{if } q \text{ is odd,} \\ 0 \pmod{q-1} & \text{if } q \text{ is even.} \end{cases}$$

Since N divides $q-1$, Lemma 26 implies

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(H'(\zeta_p)) \equiv \begin{cases} (q-1)/2 \pmod N & \text{if } q \text{ is odd,} \\ 0 \pmod N & \text{if } q \text{ is even.} \ \blacksquare \end{cases}$$

The following theorem, together with Theorem 25, will provide the key to the complete resolution of the problem of computing H-polynomials. The algorithm described in Section 5 enables us to find a polynomial Γ satisfying the conditions of Theorem 25. If N is not a power of a prime u dividing $p-1$, then Theorem 25 yields an efficient method to find δ and i such that $H_{q,N,f} = T_{\Gamma,\delta,i}$. The only remaining case is resolved by the following result.

THEOREM 28. *Let $H_{q,N,f}$ be defined by* (2), *and assume that N is a power of a prime u such that u divides $p-1$. Let $\Gamma \in \mathbb{Z}[x]$ be a polynomial satisfying conditions* (21)–(23) *of Theorem* 25, *and let (δ, i) be a solution of* (24)–(26). *Write $T = T_{\Gamma,\delta,i}$, and let T' denote the derivative of T. Let*

$$(44)\qquad k = \begin{cases} -\dfrac{u}{N}\,(\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(T'(\zeta_p)) - (q-1)/2) & \textit{if } q \textit{ is odd,} \\ -\dfrac{u}{N}\,\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(T'(\zeta_p)) & \textit{if } q \textit{ is even.} \end{cases}$$

Then k is an integer and

$$(45)\qquad H_{q,N,f}(x) \equiv x^{Np-i+k'Np/u}T(x) \pmod{x^{Np}-1},$$

where k' is the unique integer with

$$(46)\qquad k' \in \{0,\ldots,u-1\} \quad \textit{and} \quad k' \equiv k \pmod u.$$

Proof. Write $H = H_{q,N,f}$. By part (iii) of Theorem 25, we have

$$T(x) \equiv x^{i+jNp/u} H(x) \pmod{x^{Np}-1} \tag{47}$$

for some positive integer j. In order to prove (45), it remains to show

$$k \equiv -j \pmod{u}.$$

By (47), there is $K \in \mathbb{Z}[x]$ with

$$T(x) = x^{jNp/u} H(x) + K(x)(x^{Np}-1).$$

We compute

$$T'(x) = x^{jNp/u} H'(x) + \frac{jNp}{u}\, x^{jNp/u-1} H(x) + K'(x)(x^{Np}-1) + NpK(x)x^{Np-1}.$$

We find

$$T'(\zeta_p) \equiv H'(\zeta_p) + \frac{jNp}{u}\, \zeta_p^{-1} H(\zeta_p) \pmod{N}. \tag{48}$$

By Lemma 7, we have $H(\zeta_p) = -1$. Taking traces in (48), we obtain

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(T'(\zeta_p)) \equiv \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(H'(\zeta_p)) + \frac{jNp}{u} \pmod{N}. \tag{49}$$

Note that Nk/u is an integer. By Lemma 27, the definition of k, and (49), we have

$$\frac{Nk}{u} \equiv \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(H'(\zeta_p)) - \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(T'(\zeta_p)) \equiv -\frac{jNp}{u} \pmod{N}. \tag{50}$$

This shows that k is an integer. Recall that $p \equiv 1 \pmod{u}$ by the assumptions of Theorem 28. Hence (50) implies and $k \equiv -jp \equiv -j \pmod{u}$. ∎

7. Computing the polynomials $T_{\Gamma,\delta,i}$. When we compute an H-polynomial $H_{q,N,\gamma}$ based on Theorems 25 and 28, the polynomial Γ will be available by the method described in Section 5. Furthermore, the necessary numbers δ, i can be computed efficiently by using the conditions (24)–(26) of Theorem 25. Since our method is recursive, polynomials H_{q,M,f_M} will be available for every proper divisor M of N. It only remains to provide a method for computing the polynomial $T_{\Gamma,\delta,i}$ from Γ, δ, i, and the polynomials H_{q,M,f_M}. In principle, this can simply be done by using the definition (20) of $T_{\Gamma,\delta,i}$ together with Result 1. However, the next theorem, which is similar to results of Baumert [3], provides a much more efficient method.

In the following, we use the notation introduced before Theorem 25. Let μ denote the Möbius function.

THEOREM 29. *Let Γ be a polynomial satisfying conditions* (21)–(23) *of Theorem* 25. *Let* (δ, i) *be a solution of* (24)–(26). *Let $\mathcal{D}(Np)$ denote the set* *of prime divisors of Np. We have*

$$T_{\Gamma,\delta,i}(x) \equiv \delta x^i \Gamma(x) \prod_{s\in\mathcal{D}(Np)} \left(1 - \frac{1}{s}\,\frac{x^{Np}-1}{x^{Np/s}-1}\right) - \frac{1}{N} \sum_{\substack{d\mid N\\ d\neq N}} d\mu(N/d) H_{q,d,f_d}(x^{t_d})\,\frac{x^{Np}-1}{x^{dp}-1} \pmod{x^{Np}-1}. \tag{51}$$

Proof. Write $U_t(x) = (x^{Np}-1)/(x^t-1)$. Let

$$R(x) = \delta x^i \Gamma(x) \prod_{s\in\mathcal{D}(Np)} \left(1 - \frac{1}{s}\,U_s(x)\right),$$

$$S(x) = \frac{1}{N} \sum_{\substack{d\mid N\\ d\neq N}} d\mu(N/d) H_{q,d,f_d}(x^{t_d}) U_{dp}(x).$$

By Result 1, it suffices to show

$$T_{\Gamma,\delta,i}(\zeta_e) = R(\zeta_e) - S(\zeta_e) \tag{52}$$

for every divisor e of Np. Thus let e be an arbitrary divisor of Np. Note that

$$U_t(\zeta_e) = \begin{cases} Np/t & \text{if } e \text{ divides } t,\\ 0 & \text{otherwise} \end{cases} \tag{53}$$

for every divisor t of Np. Using (53), we get

$$R(\zeta_e) = \begin{cases} \delta\zeta_{Np}^i \Gamma(\zeta_{Np}) & \text{if } e = Np,\\ 0 & \text{if } e \mid Np,\ e \neq Np. \end{cases} \tag{54}$$

By Theorem 8, we have

$$H_{q,N,f}(x) \equiv H_{q,d,f_d}(x^{t_d}) \pmod{x^{dp}-1} \quad \text{for every divisor } d \text{ of } N. \tag{55}$$

Let d be a divisor of N. By (53) and (55), we have

$$H_{q,N,f}(\zeta_e) = H_{q,d,f_d}(\zeta_e^{t_d}) \quad \text{if } U_{dp}(\zeta_e) \neq 0. \tag{56}$$

Using (53) and (56), we get

$$\begin{aligned} S(\zeta_e) &= \frac{1}{N} \sum_{\substack{d\mid N\\ d\neq N}} d\mu(N/d) H_{q,N/d,f_d}(\zeta_e^{t_d}) U_{dp}(\zeta_e) \\ &= \frac{1}{N} \sum_{\substack{d\mid N\\ d\neq N}} d\mu(N/d) H_{q,N,f}(\zeta_e)\,\frac{Np}{dp} = H_{q,N,f}(\zeta_e) \sum_{\substack{d\mid N\\ e\mid dp,\, d\neq N}} \mu(N/d). \end{aligned}$$

Let e_1 be the largest divisor of e coprime to p. Since $\sum_{a|k}\mu(a)=0$ for every integer $k>1$, we get

$$\sum_{\substack{d|N\\ e|dp,\, d\neq N}} \mu(N/d) = \sum_{\substack{d|N\\ e_1|d,\, d\neq N}} \mu(N/d) = \sum_{\substack{a|(N/e_1)\\ a\neq 1}} \mu(a)$$
$$= \begin{cases} 0 & \text{if } e\equiv 0 \pmod{N},\\ -1 & \text{otherwise.}\end{cases}$$

We conclude

$$S(\zeta_e)=\begin{cases} 0 & \text{if } e\equiv 0 \pmod{N},\\ -H_{q,N,f}(\zeta_e) & \text{otherwise.}\end{cases} \tag{57}$$

Now we are ready to verify (52). First let $e=Np$. Then $R(\zeta_e)=\delta\zeta_{Np}^i\Gamma(\zeta_{Np})=T_{\Gamma,\delta,i}(\zeta_{Np})$ by (20) and (54), and $S(\zeta_e)=0$ by (57). Hence (52) holds for $e=Np$. Now assume $e\not\equiv 0 \pmod{N}$. Then $R(\zeta_e)-S(\zeta_e)=H_{q,N,f}(\zeta_e)=T_{\Gamma,\delta,i}(\zeta_e)$ by (20), (54), and (57). The last remaining case is $e=N$. In this case, $R(\zeta_e)-S(\zeta_e)=0$ by (54), (57), and $T_{\Gamma,\delta,i}(\zeta_e)=H_{q,N,f}(\zeta_e)=0$ by (20) and Lemma 7. Hence (52) holds for $e=N$. This completes the proof of Theorem 29. ■

8. An algorithm for the computation of *H*-polynomials and Gauss sums. In this section, we put everything together and formulate our algorithm for computing H-polynomials and thus Gauss sums.

Algorithm 30 (Recursive step of computation of H-polynomials).

Input:

- $q=p^r$ where p is a prime, r a positive integer,
- a divisor $N>1$ of p^r-1,
- for each divisor d of N, an irreducible factor $f_d\in\mathbb{F}_p[x]$ of Φ_d over $\mathbb{F}_p$,
- H-polynomials $H_{q,d,f_d}\in\mathbb{Z}[x]$ for each proper divisor d of N.

Output: H_{q,d,f_N}.

Step 1. Using Algorithm 20 and Remark 22, compute $\Gamma\in\mathbb{Z}[x]$ satisfying conditions (21)–(23) of Theorem 25 with $f=f_N$.

Step 2. Let $z\in\mathbb{F}_p[x]/(f_N)$ be a root of f_N. For each proper divisor d of N, find a positive integer t_d with $t_d\equiv 1 \pmod{p}$ and $f_d(z^{t_dN/d})=0$.

Step 3. Find a pair (δ,i) satisfying

$$\delta = 1 \text{ if } Np \text{ is even,}$$
$$i\equiv 0 \pmod{Np/\gcd(N,p-1)},$$
$$\delta x^i\Gamma(x)\equiv H_{q,f_{N/s},N/s}(x^{t_{N/s}}) \pmod{s,\Phi_{N_sp}^{s^{j_s-1}}}$$

for every prime divisor s of N.

STEP 4. Compute $T_{\Gamma,\delta,i}$ according to

$$T_{\Gamma,\delta,i}(x) \equiv \delta x^i \Gamma(x) \prod_{s\in\mathcal{D}(Np)} \left(1 - \frac{1}{s}\,\frac{x^{Np}-1}{x^{Np/s}-1}\right) - \frac{1}{N} \sum_{\substack{d\mid N\\ d\neq N}} d\mu(N/d) H_{q,d,f_d}(x^{t_d})\,\frac{x^{Np}-1}{x^{dp}-1} \pmod{x^{Np}-1}.$$

STEP 5. If N is a power of a prime u such that u divides $p-1$, compute k' by formulas (44), (46). Otherwise, set $k' = 0$ and $u = 1$.

STEP 6. Compute $H \in \mathbb{Z}[x]$ with $\deg(H) < Np$ such that

$$H \equiv x^{Np-i+k'Np/u} T_{\Gamma,\delta,i} \pmod{x^{Np}-1}$$

and output H.

Proof of the correctness of Algorithm 30. The correctness of Γ is guaranteed by Algorithm 20 and Remark 22. For each proper divisor d of N, the existence of t_d follows from Theorem 8. The existence of a pair (δ, i) satisfying the condition in Step 3 is given by Theorem 25. By Theorem 29, the computation of $T_{\Gamma,\delta,i}$ in Step 4 is correct. By Theorems 25, 28, and the choice of k', we have $H_{q,N,f_N} = H$ for the polynomial H computed in Step 6. ∎

The following is a complete algorithm for computing H-polynomials. Note that, when we compute H-polynomials $H_{p^r,N,f}$, we only need to deal with the case $r = r_0$ where $r_0 = \mathrm{ord}_N(p)$. For larger values of r, the polynomials $H_{p^r,N,f}$ can then be obtained from Theorem 9. We make use of this fact in Algorithm 31 to reduce the computational effort.

ALGORITHM 31 (Computation of H-polynomials).

INPUT:

- a prime p,
- a positive integer r,
- a divisor N of $p^r - 1$,
- an irreducible factor $f \in \mathbb{F}_p[x]$ of Φ_N over $\mathbb{F}_p$.

OUTPUT: $H_{p^r,N,f}$.

STEP 1. Set $f_1 = x - 1$, $H_{p,1,f_1} = \sum_{i=1}^{p-1} x^i$.

STEP 2. Let $\{d_1, \ldots, d_t\}$ be the set of all positive divisors of N, arranged in ascending order. Set $r_t = r$ and $r_i = \mathrm{ord}_{d_i}(p)$ for $i = 1, \ldots, t-1$.

STEP 3. For $i = 2, \ldots, t$, do the following:

(a) If $i = t$, then set $f_{d_i} = f$. If $i < t$, then choose an arbitrary irreducible factor $f_{d_i} \in \mathbb{F}_p[x]$ of Φ_{d_i} over $\mathbb{F}_p$.

(b) For each proper divisor d_j of d_i, do the following: Let $H_{p^{r_j},d_j,f_{d_j}}$ be the polynomial computed previously. Compute $H_{p^{r_i},d_j,f_{d_j}}$ using

$$H_{p^{r_i},d_j,f_{d_j}} \equiv (-1)^{r_i/r_j-1}\left(H_{p^{r_j},d_j,f_{d_j}} - \frac{q-1}{pd_j}S\right)^{r_i/r_j} + \frac{q^{r_i/r_j}-1}{d_j}S \pmod{x^{d_jp}-1}$$

where $S = \sum_{k=0}^{d_jp-1} x^k$.

(c) Compute $H_{p^{r_i},d_i,f_{d_i}}$ by Algorithm 30 with the H-polynomials $H_{p^{r_i},d_j,f_{d_j}}$ obtained in Step 3(b) as input.

STEP 4. Output H_{p^r,N,f_N}.

Proof of the correctness of Algorithm 31. The correctness of $H_{p,1,f_1}$ in Step 1 follows directly from the definition of H-polynomials. By Theorem 9, the formula for $H_{p^{r_i},d_j,f_{d_j}}$ in Step 3(b) is valid. The correctness of $H_{p^{r_i},d_i,f_{d_i}}$ computed in Step 3(c) follows from that of Algorithm 30. Finally, the output H_{p^r,N,f_N} is correct since $f_N = f$ by Step 3(a). ∎

9. H-polynomials and weights of irreducible cyclic codes.

Similarly to [4, p. 159], we can use H-polynomials to compute the weight distribution of irreducible cyclic codes. This is easily seen as follows.

Let p be a prime and $q = p^r$ where r is a positive integer, and let γ be a primitive element of $\mathbb{F}_q$. Let N be a divisor of $q-1$, and write $n = (q-1)/N$. Note that γ^N is a primitive nth root of unity in $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q$ we write

$$c(\alpha) = (\mathrm{Tr}(\alpha), \mathrm{Tr}(\alpha\gamma^N), \ldots, \mathrm{Tr}(\alpha\gamma^{(n-1)N})). \tag{58}$$

The subset $C := \{c(\alpha) : \alpha \in \mathbb{F}_q\}$ of $\mathbb{F}_p^n$ is called an *irreducible cyclic code of length n and dimension r over* $\mathbb{F}_p$. In the case $p = 2$, the code C is called a *binary* irreducible cyclic code.

The *weight* of a codeword $c(\alpha) = (c_0, \ldots, c_n) \in C$ is

$$w(\alpha) = |\{i \in \{0, \ldots, n-1\} : c_i \neq 0\}|.$$

Let f be an irreducible factor of $\Phi_N(X)$ over $\mathbb{F}_p$ such that $f(\gamma^{(q-1)/N}) = 0$. Let I denote the ideal of $\mathbb{Z}[X,Y]$ generated by $X^N - 1$ and $Y^p - 1$. We have the following:

$$H_{q,N,f}(XY) \equiv \sum_{\alpha\in\mathbb{F}_q^*} X^{\mathrm{ind}(\alpha)} Y^{\mathrm{Tr}(\alpha)} \equiv \sum_{s=0}^{N-1} X^s \sum_{t=0}^{n-1} Y^{\mathrm{Tr}(\gamma^{tN+s})} \equiv \sum_{s=0}^{N-1} X^s \sum_{t=0}^{p-1} c_{s,t} Y^t \pmod{I}. \tag{59}$$

If $\alpha, \beta \in \mathbb{F}_q^*$ are such that $\operatorname{ind}(\alpha) \equiv \operatorname{ind}(\beta) \equiv s \pmod N$ then $c(\alpha)$ is a cyclic shift of $c(\beta)$. Therefore $w(\alpha) = w(\beta)$. Now we have a formula to compute the weight of $c(\alpha)$:

$$w(\alpha) = n - c_{s,0}. \tag{60}$$

We have used Algorithm 31 together with (60) to compute the complete weight distributions of all binary irreducible cyclic codes with $N \leq 5000$. We have implemented Algorithm 31 in PARI/GP [2]. The complete results of our computations are available in electronic form upon request.

References

[1] L. M. Adleman, C. Pomerance and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. 117 (1983), 173–206.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI/GP (2000)*, http://pari.math.u-bordeaux.fr.

[3] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Math. 182, Springer, 1971.

[4] L. D. Baumert and R. J. McEliece, *Weights of irreducible cyclic codes*, Inform. and Control 20 (1972), 158–175.

[5] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1998.

[6] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[7] T. Breuer, *Integral bases for subfields of cyclotomic fields*, Appl. Algebra Engrg. Comm. Comput. 8 (1997), 279–289.

[8] R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. 18 (1986), 97–122.

[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, 1993.

[10] R. W. Fitzgerald and J. L. Yucas, *Sums of Gauss sums and weights of irreducible codes*, Finite Fields Appl. 11 (2005), 89–110.

[11] C. F. Gauß, *Disquisitiones arithmeticae*, English transl., Springer, 1986.

[12] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math. 84, Springer, 1990.

[13] K. H. Leung, S. L. Ma and B. Schmidt, *New Hadamard matrices of order* $4p^2$ *obtained from Jacobi sums of order* 16, J. Combin. Theory Ser. A 113 (2006), 822–838.

[14] J. MacWilliams and J. Seery, *The weight distributions of some minimal cyclic codes*, IEEE Trans. Inform. Theory 27 (1981), 796–806.

[15] O. D. Mbodj, *Quadratic Gauss Sums*, Finite Fields Appl. 4 (1998), 347–361.

[16] J. R. McEliece and H. Rumsey Jr., *Euler products, cyclotomy, and coding*, J. Number Theory 4 (1972), 302–311.

[17] P. Mihăilescu, *Cyclotomy of rings and primality testing*, PhD thesis, Swiss Federal Institute of Technology, Zurich, 1997.

[18] —, *Cyclotomy primality proving—recent developments*, in: Algorithmic Number Theory, Lecture Notes in Comput. Sci. 1423, Springer, 1998, 95–110.

[19] D. K. Nguyen, *Efficient computation of Gauss sums over finite fields*, honors thesis, Nanyang Technological Univ., Singapore (electronic copy available on request).

[20] P. Ribenboim, *Algebraic Numbers*, Wiley, 1972.

[21] B. Schmidt and C. White, *All two-weight irreducible cyclic codes?*, Finite Fields Appl. 8 (2002), 1–17.

[22] R. Segal and R. L. Ward, *Weight distributions of some irreducible cyclic codes*, Math. Comp. 46 (1986), 341–354.

[23] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Ann. 37 (1890), 321–367.

[24] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Adv. Math. 2, Markham, 1967.

[25] F. Thaine, *On the relation between units and Jacobi sums in prime cyclotomic fields*, Manuscripta Math. 73 (1991), 127–151.

[26] —, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Trans. Amer. Math. Soc. 351 (1999), 4769–4790.

[27] —, *Jacobi sums and new families of irreducible polynomials of Gaussian periods*, Math. Comp. 70 (2001), 1617–1640.

[28] M. van der Vlugt, *On the weight hierarchy of irreducible cyclic codes*, J. Combin. Theory Ser. A 71 (1995), 159–167.

[29] P. van Wamelen, *Jacobi sums over finite fields*, Acta Arith. 102 (2002), 1–20.

[30] R. L. Ward, *Weight enumerators of more irreducible cyclic binary codes*, IEEE Trans. Inform. Theory 39 (1993), 1701–1709.

[31] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, 1997.

Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371, Singapore
E-mail: bernhard@ntu.edu.sg

Received on 1.7.2008 (5752)