

Pure Gauss sums and skew Hadamard difference sets

Koji Momihara

ABSTRACT. Chowla (1962), McEliece (1974), Evans (1977, 1981) and Aoki (1997, 2004, 2012) studied Gauss sums, some integral powers of which are in the field of rational numbers. Such Gauss sums are called *pure*. In particular, Aoki (2004) gave a necessary and sufficient condition for a Gauss sum to be pure in terms of Dirichlet characters modulo the order of the multiplicative character involved. In this paper, we study pure Gauss sums with odd extension degree f and classify them for $f = 5, 7, 9, 11, 13, 17, 19, 23$ based on Aoki's theorem. Furthermore, we characterize a special subclass of pure Gauss sums in view of an application for skew Hadamard difference sets. Based on the characterization, we give a new construction of skew Hadamard difference sets from cyclotomic classes of finite fields.

1. Introduction

Let p be a prime and f be a positive integer. Let \mathbb{F}_{p^f} denote the finite field of order p^f . The canonical additive character ψ of \mathbb{F}_{p^f} is defined by

$$\psi: \mathbb{F}_{p^f} \rightarrow \mathbb{C}^*, \quad \psi(x) = \zeta_p^{\text{Tr}_{p^f/p}(x)},$$

where $\zeta_p = \exp(\frac{2\pi i}{p})$ is a complex primitive p -th root of unity and $\text{Tr}_{p^f/p}$ is the absolute trace from \mathbb{F}_{p^f} to \mathbb{F}_p . All complex characters of $(\mathbb{F}_{p^f}, +)$ are given by ψ_a , where $a \in \mathbb{F}_{p^f}$. Here ψ_a is defined by

$$(1.1) \quad \psi_a(x) = \psi(ax), \quad \forall x \in \mathbb{F}_{p^f}.$$

Let N be a positive divisor of $p^f - 1$. For a multiplicative character η_N of order N of \mathbb{F}_{p^f} , we define the *Gauss sum* of \mathbb{F}_{p^f}

$$G_{p^f}(\eta_N) = \sum_{x \in \mathbb{F}_{p^f}^*} \psi(x) \eta_N(x).$$

The Gauss sum is one of important and fundamental objects in number theory. The concept of Gauss sums was introduced by Gauss in 1801 [19], who evaluated the *quadratic* Gauss sums as in Theorem 2.1. After Gauss' work, many researchers have tried to evaluate Gauss sums for larger N . However, in general, the explicit evaluation of Gauss sums is a very difficult problem. There are only a few cases where the Gauss sums have been completely evaluated. For example, the Gauss sums for $N = 3, 4, 5, 6, 8, 12, 16, 24$ have been evaluated (but not explicit in some cases). See [6] for more details. The next important case is the so-called *semi-primitive case* (also referred to as uniform cyclotomy or supersingular), where there exists an integer s such that $p^s \equiv -1 \pmod{N}$. See Theorem 2.2 for the explicit evaluation in this case. The next interesting case is the

2010 *Mathematics Subject Classification.* 11L05, 11T22, 11T24, 05B10.

The author acknowledges the support by JSPS under Grant-in-Aid for Scientific Research (C) 20K03719.

index 2 case, where the subgroup $\langle p \rangle$ generated by $p \in \mathbb{Z}$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^\times$. Many authors have studied this case, see, e.g., [22, 25, 26, 31, 33]. In particular, a complete solution to the problem of evaluating Gauss sums in this case was given in [33]. As a large generalization, Aoki [4] studied Gauss sums such that $(\mathbb{Z}/N\mathbb{Z})^\times/\langle p \rangle$ is an elementary abelian 2-group. The *index 4 case* including the case where $(\mathbb{Z}/N\mathbb{Z})^\times/\langle p \rangle$ is cyclic was also studied in [15, 16, 32].

On the other hand, there were studies on Gauss sums from another point of view. Chowla [9, 10] showed that if a Gauss sum defined in a prime field has the form $\epsilon p^{\frac{1}{2}}$ with ϵ a root of unity, it is in the quadratic case. McEliece [24] studied for which (N, p, h) , some nonzero integral power of the corresponding Gauss sum is an integer, i.e., $p^{-h/2}G_{p^h}(\eta_N)$ is a root of unity, related to weight distribution of irreducible cyclic codes. Such Gauss sums are called *pure*. It is clear that the quadratic Gauss sums and the semi-primitive Gauss sums are examples of pure Gauss sums. Evans [12] showed that pure Gauss sums for prime powers N are in the semi-primitive case. Furthermore, Evans [13] gave some nontrivial families of pure Gauss sums which are not semi-primitive. On the other hand, Aoki [2] classified pure Gauss sums for small extension degrees as follows.

THEOREM 1.1. [2] *Assume that $f \in \{1, 2, 3, 4\}$ and the order of p modulo N is f . Then, the corresponding Gauss sum $G_{p^f}(\eta_N)$ is pure if and only if it is of semi-primitive except for the following cases:*

$$f = 3 : (N, [p]_N) = (14, 9), (14, 11), (42, 25), (42, 37), (78, 55), (78, 71),$$

$$f = 4 : (N, [p]_N) = (20, 13), (20, 17), (30, 17), (30, 23), (60, 17), (60, 53), (120, 83), (120, 107),$$

where $[p]_N$ is an integer such that $[p]_N \equiv p \pmod{N}$ and $1 \leq [p]_N \leq N - 1$.

Furthermore, as a remarkable result, Aoki [3, 5] gave a necessary and sufficient condition for a Gauss sum to be pure in terms of Dirichlet characters of modulo N , see Theorem 2.13. Based on the result, Aoki [3, Theorem 1.2] proved that for any fixed f , the set of pairs $(N, [p]_N)$ such that the Gauss sum $G_{p^f}(\eta_N)$ is pure but not semi-primitive is finite.

The evaluating Gauss sums is an important work also in view of applications in Combinatorics. In fact, Gauss sums have rich applications in the studies of combinatorial objects, such as difference sets, irreducible cyclic codes, strongly regular Cayley graphs, cyclotomic association schemes, sequences with good auto-correlation property, highly nonlinear functions, etc. See, e.g., [1, 18, 20, 24, 29, 30]. In particular, pure Gauss sums were used for constructing skew Hadamard difference sets inequivalent to the classical Paley difference sets [8, 17, 27].

Let G be an additively written group. We call a subset D of G a *difference set* if the list of differences “ $x - y, x, y \in D, x \neq y$ ” represents every element of $G \setminus \{0_G\}$ exactly λ times. In this paper, we are concerned with difference sets in the additive group of the finite field, i.e., G is an elementary abelian group. We say that a difference set is *skew Hadamard* if D is a skew-symmetric $(|G| - 1)/2$ -subset of G , i.e., $D \cup -D = G \setminus \{0_G\}$ and $D \cap -D = \emptyset$, where $-D = \{-x : x \in D\}$. The primary example of skew Hadamard difference sets is the classical *Paley difference set* in the additive group of the finite field \mathbb{F}_q of order q with $q \equiv 3 \pmod{4}$, which consists of all nonzero squares of \mathbb{F}_q . The Paley difference set was the only known example in abelian groups for many years. Therefore, many researchers had believed that up to equivalence the Paley difference sets are the only skew Hadamard difference sets in elementary abelian groups. In 2006, Ding and Yuan [11] disproved this conjecture by giving counterexamples of skew Hadamard difference sets in $(\mathbb{F}_{35}, +)$. After their work, there have been many studies on constructions and classification of skew Hadamard difference sets. See short surveys in Introduction of [8, 17, 27]. In particular,

Feng and Xiang [17] gave a construction of skew Hadamard difference sets based on pure Gauss sums, which are also in the index 2 case. Furthermore, Chen and Feng [8] generalized the construction using pure Gauss sums satisfying $2 \equiv p^j \pmod{N/2}$ for some integer j , see Theorem 2.16. Their constructions are very flexible as explained in the next section, and give rise to many skew Hadamard difference sets inequivalent to the Paley difference sets [27]. The study in this paper is a continuation of those in [8, 17].

In this paper, we will study pure Gauss sums with f odd and their application for constructing skew Hadamard difference sets. The objectives of this paper are three-fold. First, we give some necessary conditions for pure Gauss sums with f odd based on Aoki's Theorem 2.13, and update the result of Theorem 1.1 for $f \in \{5, 7, 9, 11, 13, 17, 19, 23\}$ in Theorem 3.9. Second, we characterize pure Gauss sums such that f is odd and $\langle p \rangle$ has index at most 8 in $(\mathbb{Z}/N\mathbb{Z})^\times$, and see that almost all pure Gauss sums for $N \leq 5000$ and odd f fall into those classes. Third, we give a characterization for a special class of pure Gauss sums with the following property in view of applications for skew Hadamard difference sets: for $N = 2m_1m_2 \cdots m_r$, $G_{p^f}(\eta_2 \prod_{i \in J} m_i)$ is pure for any subset J of $\{1, 2, \dots, r\}$ containing 1, where m_i 's are distinct odd prime powers. Based on the characterization of pure Gauss sums, we give a new construction of skew Hadamard difference sets from cyclotomic classes of finite fields, which gives rise to two existence results. One of the results (that is, Corollary 4.18) is covered by the result in [8], and the other (that is, Corollary 4.19) is completely new not within the framework of previous studies.

2. Preliminaries

2.1. Basic properties of Gauss sums. From the definition of Gauss sums, we see clearly that $G_{p^f}(\eta_N)$ is in the ring of algebraic integers of the field $\mathbb{Q}(\zeta_p, \zeta_N)$. Let $\sigma_{a,b}$ be the automorphism of $\mathbb{Q}(\zeta_p, \zeta_N)$ defined by

$$\sigma_{a,b}(\zeta_N) = \zeta_N^a, \quad \sigma_{a,b}(\zeta_p) = \zeta_p^b,$$

where $\gcd(a, N) = \gcd(b, p) = 1$. Below we list several basic properties of Gauss sums [6].

- (i) $G_{p^f}(\eta_N) \overline{G_{p^f}(\eta_N)} = p^f$ if η_N is nontrivial.
- (ii) $G_{p^f}(\eta_N^p) = G_{p^f}(\eta_N)$.
- (iii) $G_{p^f}(\eta_N^{-1}) = \eta_N(-1) \overline{G_{p^f}(\eta_N)}$.
- (iv) $G_{p^f}(\eta_N) = -1$ if η_N is trivial.
- (v) $\sigma_{a,b}(G_{p^f}(\eta_N)) = \eta_N^{-a}(b) G_{p^f}(\eta_N^a)$.

In general, explicit evaluations of Gauss sums are very difficult. There are only a few cases where the Gauss sums have been evaluated. The most well-known case is the *quadratic* case, i.e., the $N = 2$ case.

THEOREM 2.1. ([23, Theorem 5.15]) *Let η_2 be the quadratic character of \mathbb{F}_{p^f} . Then, $G_{p^f}(\eta_2) = \epsilon p^{f/2}$, where*

$$\epsilon = \begin{cases} (-1)^{f-1} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{f-1} i^f & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

The next simple case is the so-called *semi-primitive case* (also referred to as uniform cyclotomy or supersingular), where there exists an integer s such that $p^s \equiv -1 \pmod{N}$.

THEOREM 2.2. ([6, Theorem 11.6.1]) *Suppose that $N > 2$ and p is semi-primitive modulo N , i.e., there exists an s such that $p^s \equiv -1 \pmod{N}$. Choose s minimal and*

write $h = 2st$. Let η_m be a multiplicative character of order m . Then,

$$p^{-h/2}G_{p^h}(\eta_m) = \begin{cases} (-1)^{t-1} & \text{if } p = 2; \\ (-1)^{t-1+(p^s+1)t/m} & \text{if } p > 2. \end{cases}$$

In this paper, we will need the *Davenport-Hasse product formula*, which is stated below.

THEOREM 2.3. ([6, Theorem 11.3.5]) *Let θ be a multiplicative character of order $\ell > 1$ of \mathbb{F}_{p^f} . For any nontrivial multiplicative character η of \mathbb{F}_{p^f} ,*

$$(2.1) \quad G_{p^f}(\eta) = \frac{G_{p^f}(\eta^\ell)}{\eta^\ell(\ell)} \prod_{i=1}^{\ell-1} \frac{G_{p^f}(\theta^i)}{G_{p^f}(\eta\theta^i)}.$$

It is not easy to determine $\eta^\ell(\ell)$ in general. The following transformation of (2.1) is sometimes useful.

COROLLARY 2.4. *With notation as in Theorem 2.3, if ℓ is odd,*

$$G_{p^f}(\eta^\ell) = p^{-f\frac{\ell-1}{2}} \sigma_{1,\ell-1} \left(\prod_{i=0}^{\ell-1} G_{p^f}(\eta\theta^i) \right).$$

PROOF. Note that

$$\prod_{i=1}^{\ell-1} G_{p^f}(\theta^i) = \prod_{i=1}^{\frac{\ell-1}{2}} G_{p^f}(\theta^i) G_{p^f}(\theta^{\ell-i}) = p^{f\frac{\ell-1}{2}} \prod_{i=1}^{\frac{\ell-1}{2}} \theta^i(-1).$$

Here, $\theta(-1) = 1$; otherwise $\theta^\ell(-1) = -1$, a contradiction to that θ^ℓ is trivial. Hence, $\prod_{i=1}^{\ell-1} G_{p^f}(\theta^i) = p^{f\frac{\ell-1}{2}}$. Furthermore, note that

$$G_{p^f}(\eta^\ell) \eta^{-\ell}(\ell) = \sigma_{1,\ell}(G_{p^f}(\eta^\ell)).$$

Then, (2.1) is reformulated as

$$(2.2) \quad \sigma_{1,\ell}(G_{p^f}(\eta^\ell)) = p^{-f\frac{\ell-1}{2}} \prod_{i=0}^{\ell-1} G_{p^f}(\eta\theta^i).$$

Finally, by acting $\sigma_{1,\ell-1}$ to both sides of (2.2), we obtain the assertion of the corollary. \square

We will also need the *Davenport-Hasse lifting formula*, which is stated below.

THEOREM 2.5. ([23, Theorem 5.14]) *Let η be a nontrivial multiplicative character of \mathbb{F}_{p^f} and let η' be the lift of η to $\mathbb{F}_{p^{fs}}$, i.e., $\eta'(\alpha) = \eta(\text{Norm}_{p^{fs}/p^f}(\alpha))$ for $\alpha \in \mathbb{F}_{p^{fs}}$, where $s \geq 2$ is an integer. Then*

$$G_{p^{fs}}(\eta') = (-1)^{s-1} (G_{p^f}(\eta))^s.$$

2.2. Pure Gauss sums. Let η_N be a multiplicative character of order N of \mathbb{F}_{p^f} . We say that the Gauss sum $G_{p^f}(\eta_N)$ is *pure* if $\epsilon = G_{p^f}(\eta_N)p^{-f/2}$ is a root of unity. We call the ϵ as the *sign* or the *root of unity* of the pure Gauss sum $G_{p^f}(\eta_N)$.

LEMMA 2.6. *If $G_{p^f}(\eta_N)$ is pure, so is $G_{p^f}(\eta_N^a)$ for any a with $\gcd(a, N) = 1$.*

PROOF. Let $\sigma_{a,1} \in \text{Gal}(\mathbb{Q}(\zeta_p, \zeta_N)/\mathbb{Q})$. Then, $\sigma_{a,1}(G_{p^f}(\eta_N)) = G_{p^f}(\eta_N^a)$ is also pure. \square

The lemma above implies that the purity of Gauss sums is depending on N but not depending on the choice of η_N . Then, denote by \mathcal{P} the set of triples (N, f, p) such that $G_{p^f}(\eta_N)$ is pure.

From now on, let f be the order of p modulo N and η_N be a multiplicative character of order N of \mathbb{F}_{p^f} . Let s be any positive integer and η'_N be the lift of η_N to $\mathbb{F}_{p^{fs}}$. If $G_{p^f}(\eta_N)$ is pure, then so is $G_{p^{fs}}(\eta'_N)$ by Theorem 2.5. Hence, the purity problem of $G_{p^{fs}}(\eta'_N)$ is reduced to that of $G_{p^f}(\eta_N)$. Hence, we consider

$$\mathcal{P}^* := \{(N, f, p) \in \mathcal{P} \mid \text{ord}_N(p) = f\}.$$

The following characterization of pure Gauss sums is obtained from the well-known *Stickelberger* theorem on ideal factorizations of Gauss sums [6, Theorem 11.2.2].

PROPOSITION 2.7. ([3, 12, 21]) $(N, f, p) \in \mathcal{P}^*$ if and only if

$$\sum_{i=0}^{f-1} [tp^i]_N = \frac{fN}{2}$$

for any integer t prime to N , where $[x]_N$ is an integer such that $0 \leq [x]_N \leq N-1$ and $[x]_N \equiv x \pmod{N}$.

The proposition above gives the following characterization.

LEMMA 2.8. ([12, 13]) If $(N, f, p) \in \mathcal{P}^*$, it holds that $N \mid (p^f - 1)/(p - 1)$ or $N/2 \mid (p^f - 1)/(p - 1)$ depending on whether f is even or odd.

On the other hand, Proposition 2.7 implies that the purity of Gauss sums for a fixed N depends only on the residue class of p modulo N . Furthermore, the proposition implies that if $(N, f, p) \in \mathcal{P}^*$, then $(N, f, r) \in \mathcal{P}^*$ for any prime $r \equiv p^i \pmod{N}$, where i is an arbitrary integer such that $1 \leq i \leq f-1$ and $\gcd(i, f) = 1$.

The Gauss sums in semi-primitive case are clearly pure. Hence, we have

$$(\mathcal{P}^{(-1)} :=) \{(N, f, p) \mid \exists i \text{ s.t. } p^i \equiv -1 \pmod{N}\} \subseteq \mathcal{P}.$$

It is clear that f is even if $(N, f, p) \in \mathcal{P}^{(-1)}$. Evans [12] showed that pure Gauss sums for prime powers m are in the semi-primitive case. Furthermore, Evans [13] also gave the following nontrivial sufficient conditions for Gauss sums to be pure.

THEOREM 2.9. Suppose that $m = cd$ with $\gcd(c, d) = \gcd(\text{ord}_c(p), \text{ord}_d(p)) = 1$ and let $f = \text{ord}_m(p)$, where $\text{ord}_n(x)$ is the order of x in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then, $G_{p^f}(\eta_m)$ is pure if any of the following holds.

- (1) $\text{ord}_c(p) = \phi(c)$ and $\ell \in \langle p \rangle \pmod{d}$ for some prime $\ell \mid c$.
- (2) $-1 \notin \langle p \rangle \pmod{c}$, $2\text{ord}_c(p) = \phi(c)$, $\ell \in \langle p \rangle \pmod{d}$ for some prime $\ell \mid c$, and all of them hold with c and d interchanged.
- (3) $2 \parallel m$, $2 + m/2 \notin \langle p \rangle \pmod{c}$, $2\text{ord}_c(p) = \phi(c)$, -1 or ℓ is in $\langle p \rangle \pmod{d}$ for some prime $\ell \mid c$, and all of them hold with c and d interchanged.

Here, ϕ is Euler's totient function.

On the other hand, Aoki [3, Theorem 7.2] proved that the converse of the assertion of Theorem 2.9 also holds if c and d are both odd prime powers.

In this paper, we are concerned with pure Gauss sums with f odd. There were not so many studies on pure Gauss sums for odd f in the literature.

PROPOSITION 2.10. ([13, Corollary 3]) If f is odd and $(N, f, p) \in \mathcal{P}^*$, then $2 \parallel N$.

The following proposition comes from Theorem 2.9 (1) as $c = \ell = 2$ or Corollary 8 in [13]. (Note that Theorem 2.13 below is a large generalization of Theorem 2.9.) Chen-Feng [8] also gave a proof for the result based on Davenport-Hasse product formula.

PROPOSITION 2.11. Assume that $2 \parallel N$. If there exists j such that $p^j \equiv 2 \pmod{N/2}$, then $(N, f, p) \in \mathcal{P}^*$. In particular, $G_{p^f}(\eta_N) = G_{p^f}(\eta_2)$.

The proposition above defines a class of pure Gauss sums with f odd:

$$\mathcal{P}^{(2)} := \{(N, f, p) \mid f \text{ is odd, } \exists i \text{ s.t. } p^i \equiv 2 \pmod{N/2}\} \subseteq \mathcal{P}.$$

We will study in Section 4 whether there is a class of pure Gauss sums other than $\mathcal{P}^{(2)}$ compatible with a construction of skew Hadamard difference sets.

Next, we give one basic property of pure Gauss sums.

LEMMA 2.12. *Let p_1 be an odd prime and t be a positive integer. Assume that $p_1^t \parallel N$. If $(N, f, p) \in \mathcal{P}$, then $(N/p_1^s, f, p) \in \mathcal{P}$ for any $s \leq t - 1$.*

PROOF. Let η_N be a multiplicative character of order N of \mathbb{F}_{p^f} and θ be a multiplicative character of order p_1^s of \mathbb{F}_{p^f} . Then, by Theorem 2.3 as $\ell = p_1^s$, we have

$$G_{p^f}(\eta_N) = \frac{G_{p^f}(\eta_N^\ell)}{\eta_N^\ell(\ell)} \prod_{i=1}^{\ell-1} \frac{G_{p^f}(\theta^i)}{G_{p^f}(\eta_N \theta^i)}.$$

Since $\eta_N \theta^i$ is of order N , $G_{p^f}(\eta_N \theta^i)$ is also pure. On the other hand, $\prod_{i=1}^{\ell-1} G_{p^f}(\theta^i) = \left(\prod_{i=1}^{\frac{\ell-1}{2}} \theta^i(-1) \right) p^{f \frac{\ell-1}{2}}$. Hence, $G_{p^f}(\eta_N^\ell)$ is pure, i.e., $(N/p_1^s, f, p) \in \mathcal{P}$. \square

We will need the following powerful characterization of pure Gauss sums given by Aoki [5]. To state it, let $D(N)$ denote the set of Dirichlet characters modulo N , and define

$$D^-(N, p) := \{\chi \in D(N) \mid \chi(p) = 1, \chi \text{ is an odd character}\},$$

$$X^-(N, p) := \{\chi \in D^-(N, p) \mid \text{The conductor of } \chi \text{ is divisible by any prime factor of } N\}.$$

THEOREM 2.13. ([5, Proposition 4.9]) *$(N, f, p) \in \mathcal{P}^*$ if and only if the following two conditions hold.*

- (1) $X^-(N, p) = \emptyset$.
- (2) *For any $\chi \in D^-(N, p)$, there exists a prime divisor ℓ of N but not dividing the conductor of χ such that $\chi(\ell) = 1$.*

Define

$$\mathcal{P}_f^* := \{(N, \bar{p}) \mid (N, f, p) \in \mathcal{P}^* \setminus \mathcal{P}^{(-1)}\},$$

where \bar{p} denotes a minimum representative in $\{[p^i]_N \mid 1 \leq i \leq f-1, \gcd(i, f) = 1\}$. Based on the theorem above, Aoki [5, Theorem 1.1] proved that \mathcal{P}_f^* is a finite set for every positive integer f .

2.3. Skew Hadamard difference sets. Let $q = p^f$ be a prime power and let $N > 1$ be a divisor of $q-1$. Let $C_i^{(N, q)} = \omega^i \langle \omega^N \rangle$, $0 \leq i \leq N-1$, be the *cyclotomic classes* of order N of \mathbb{F}_q , where ω is a fixed primitive element of \mathbb{F}_q . We assume that $q \equiv 3 \pmod{4}$ and N is even. Then, it is clear that $N/2$ is odd. In this paper, we will give a construction for a skew Hadamard difference set D as a union of suitable $m = N/2$ cyclotomic classes. To do this, we will use the following well-known characterization of skew Hadamard difference sets.

LEMMA 2.14. *Let G be an abelian group of order $v \equiv 3 \pmod{4}$, and let D be a skew symmetric $(v-1)/2$ -subset of G . The set D is a skew Hadamard difference set if and only if $\psi(D) \in \{\frac{-1+\sqrt{-v}}{2}, \frac{-1-\sqrt{-v}}{2}\}$ for any nontrivial character of G .*

Note that $D^\perp = \{\psi \in G^\perp \mid \psi(D) = \frac{-1+\sqrt{-q}}{2}\}$ (and its inverse) also forms a skew Hadamard difference set, called the *dual* of D , in the character group G^\perp of G . The following result is also known (cf. [7, Lemma 2.1]).

LEMMA 2.15. *Let G be an abelian group of order p^h , where p is a prime such that $p \equiv 3 \pmod{4}$ and h is an odd integer. Let D be a skew symmetric $(p^h - 1)/2$ -subset of G such that D is invariant under the multiplication by x^2 for $x \in \mathbb{F}_p^*$. If $2\psi(D) + 1 \equiv 0 \pmod{p^{\frac{h-1}{2}}}$ for any nontrivial character ψ of G , then D is a skew Hadamard difference set in G .*

Let I be a $N/2$ -subset of $\{0, 1, \dots, N-1\}$. To check whether a candidate subset $D = \bigcup_{i \in I} C_i^{(N,q)}$ is a skew Hadamard difference set, by Lemma 2.14, it suffices to show that $(\psi_a(D) := \sum_{x \in D} \psi_a(x)) \in \{\frac{-1 \pm \sqrt{-q}}{2}\}$ for any nonzero $a \in \mathbb{F}_q$. Note that the character value $\psi_a(D)$ can be expressed as a linear combination of Gauss sums (cf. [17]) by using the orthogonality of characters:

$$(2.3) \quad \psi_a(D) = \frac{1}{N} \sum_{i=0}^{N-1} G_q(\eta_N^{-i}) \sum_{i \in I} \eta_N(a\gamma^i),$$

where η_N is a fixed multiplicative character of order N of \mathbb{F}_q . Thus, the computations needed to check whether a candidate subset $D = \bigcup_{i \in I} C_i^{(N,q)}$ is a skew Hadamard difference set are essentially reduced to evaluating Gauss sums. For example, if $N = 2$, we have

$$(2.4) \quad \psi_a(C_i^{(2,q)}) = \frac{-1 + (-1)^{a+i} G_q(\eta_2)}{2},$$

where η_2 is the quadratic character of \mathbb{F}_q . By Theorem 2.1, we have $\psi_a(C_i^{(2,q)}) \in \{\frac{-1 \pm \sqrt{-q}}{2}\}$ if $q \equiv 3 \pmod{4}$. Hence, each $C_i^{(2,q)}$, $i = 0, 1$, is a skew Hadamard difference set in $(\mathbb{F}_q, +)$, that is, the so-called Paley difference set.

Let X be a subset of $\mathbb{F}_{q^\ell}^*/\mathbb{F}_q^*$, and $\pi : \mathbb{F}_{q^\ell}^* \rightarrow \mathbb{F}_{q^\ell}^*/\mathbb{F}_q^*$ be the natural projection homomorphism. Define

$$D(X) = \{x \in C_0^{(2,q^\ell)} \mid \pi(x) \in X\} \cup \{x \in C_1^{(2,q^\ell)} \mid \pi(x) \notin X\}.$$

Chen-Feng [8] showed that under the assumptions that ℓ is odd and X is a difference set with parameters $((q^\ell - 1)/(q - 1), q^{\ell-1}, q^{\ell-2}(q - 1))$, $D(X)$ is a skew Hadamard difference set or a Paley type partial difference set if and only if X is an *Arasu-Dillon-Player difference set*. Furthermore, they gave the following construction of skew Hadamard difference sets based on the class $\mathcal{P}^{(2)}$ of pure Gauss sums, which is a generalization of that given by Feng-Xiang [17].

THEOREM 2.16. ([8, Theorem 1.4]) *Let $q = p^f \equiv 3 \pmod{4}$ be a prime power with p a prime, and let ℓ be any odd positive integer. Let m be a divisor of $(q^\ell - 1)/(q - 1)$ satisfying $2 \equiv p^j \pmod{m}$ for some integer j , and $\tau : \mathbb{F}_{q^\ell}^*/\mathbb{F}_q^* \rightarrow \mathbb{Z}/m\mathbb{Z}$ be the natural projection. Then, for any subset X of $\mathbb{Z}/m\mathbb{Z}$, the set $D(\tau^{-1}(X))$ is a skew Hadamard difference set in $(\mathbb{F}_{q^\ell}, +)$.*

The original statement of the theorem above in [8] assumed that q^ℓ is an odd prime power not necessarily $q^\ell \equiv 3 \pmod{4}$ and m is a divisor of $(q^\ell - 1)/(q - 1)$ satisfying $-1 \equiv p^j \pmod{m}$ or $2 \equiv p^j \pmod{m}$ for some integer j since the authors treated also Paley type partial difference sets not only skew Hadamard difference sets. However, in our situation, $-1 \equiv p^j \pmod{m}$ is impossible since $f\ell$ is odd. Note that the assumption $2 \equiv p^j \pmod{m}$ implies that $(p^j - 1) \equiv 1 \pmod{m}$ for some positive integer j . Hence, $p - 1$ and m are coprime, i.e., m is a divisor of $(p^f - 1)/(p - 1)$. Hence, we can not remove the condition $m \mid (q^\ell - 1)/(q - 1)$. It is clear that $D(\tau^{-1}(X))$ in the theorem above is a union of cyclotomic classes of order $N = 2m$ of \mathbb{F}_{q^ℓ} . In particular, it is expressed as $D(\tau^{-1}(X)) = \bigcup_{i \in I} C_i^{(2m,q^\ell)}$, where $I = \{(m+1)i \pmod{2m} \mid i \in X\} \cup \{(m+1)i +$

$m \pmod{2m} \mid i \in (\mathbb{Z}/m\mathbb{Z}) \setminus X\}$. In other words, one can take I as an arbitrary m -subset of $\mathbb{Z}/2m\mathbb{Z}$ such that $\{i \pmod{m} \mid i \in I\} = \{0, 1, \dots, m-1\}$. Thus, the theorem above is very powerful. In fact, the choice of the set X is very flexible and $f\ell$ can be taken as an arbitrary odd positive integer divisible by the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then, Theorem 2.16 yields infinite families of skew Hadamard difference sets inequivalent to the Paley difference sets [27]. In Section 4, we give a construction of skew Hadamard difference sets based on a class of pure Gauss sums not belonging to $\mathcal{P}^{(2)}$.

3. Some necessary conditions for pure Gauss sums with f odd

Throughout this section, we assume that $f = \text{ord}_N(p)$ is odd and $(N, f, p) \in \mathcal{P}^*$. Then, by Proposition 2.10, we have $2 \parallel N$. Let $p_i, i = 1, 2, \dots, r$, be distinct odd primes and $u_i, i = 1, 2, \dots, r$, be positive integers. Let $N = 2m = 2m_1 m_2 \cdots m_r$, where $m_i = p_i^{u_i}$, $i = 1, 2, \dots, r$. Let $f_i, i = 1, 2, \dots, r$, denote the orders of p modulo m_i , respectively. Then, $f = \text{lcm}(f_1, f_2, \dots, f_r)$.

In this section, we characterize $(N, \bar{p}) \in \mathcal{P}_f^*$ for $f \in \{3, 5, 7, 9, 11, 13, 17, 19, 23\}$, $N \leq 5000$ or $\phi(N)/f \leq 8$ with f odd.

3.1. Necessary conditions. Aoki [3] proved the following theorem.

THEOREM 3.1. [3, Theorem 5.1] *Assume that f is odd and $(N, f, p) \in \mathcal{P}^*$.*

- (1) *If r is odd, $m_i \mid 2^{2f} - 1$ for each $i, i = 1, 2, \dots, r$;*
- (2) *If r is even, either $m_i \mid 2^{2f} - 1$ or $\phi(m_i) \mid 4f$ for each $i, i = 1, 2, \dots, r$.*

Since $\phi(m_i) \mid 4f$ implies that $m_i \mid 2^{4f} - 1$ by Fermat's little theorem, we have the following corollary.

COROLLARY 3.2. ([3, Corollary 5.2]) *Assume that f is odd and $(N, f, p) \in \mathcal{P}^*$. Then, $m \mid 2^{4f} - 1$.*

The corollary above implies that the set of pairs $(N, \bar{p}) \in \mathcal{P}_f^*$ is finite for any fixed f . To classify $(N = 2m, \bar{p}) \in \mathcal{P}_f^*$ for a fixed odd f , we may take positive divisors m of $2^{4f} - 1$ in view of Corollary 3.2. However, even if f is small, some divisor m of $2^{4f} - 1$ is too large to check whether $(N, \bar{p}) \in \mathcal{P}_f^*$ by a computer. So, we will give some new necessary conditions for divisors m of $2^{4f} - 1$ such that $(N, \bar{p}) \in \mathcal{P}_f^*$, which are all based on Aoki's Theorem 2.13.

Let χ_i be a character of order $\phi(m_i)$ of $(\mathbb{Z}/m_i\mathbb{Z})^\times$. Then, we have $\chi_i^{f_i}(p) = \chi_i(p^{f_i}) = 1$. Furthermore, $\chi_i^{f_i}(-1) = \chi_i(-1) = -1$ since f_i is odd. Hence, $\chi_i^{f_i} \in \mathcal{D}^-(N, p)$ for $i = 1, 2, \dots, r$.

PROPOSITION 3.3. *Assume that f is odd and $(N, f, p) \in \mathcal{P}^*$. If there is j such that $m_j \nmid 2^f - 1$, there is h with $h \neq j$ such that $m_j \mid p_h^f - 1$.*

PROOF. By Theorem 2.13, we have $\chi_j^{f_j}(2) = 1$ or $\chi_j^{f_j}(p_h) = 1$ for some $h = 1, 2, \dots, r$ with $h \neq j$. If $\chi_j^{f_j}(2) = \chi_j(2^{f_j}) = 1$, we have $m_j \mid 2^{f_j} - 1$, which contradicts to $m_j \nmid 2^f - 1$. Hence, we have $\chi_j^{f_j}(p_h) = 1$ for some $h = 1, 2, \dots, r$ with $h \neq j$. This implies that $m_j \mid p_h^{f_j} - 1 \mid p_h^f - 1$. \square

Next, we give two necessary conditions for $(N, f, p) \in \mathcal{P}^*$ with r even.

PROPOSITION 3.4. *Assume that f is odd, r is even and $(N, f, p) \in \mathcal{P}^*$. If there is j such that $m_j \nmid 2^{2f} - 1$, it holds that $\phi(m_h) \leq 2f$ for any m_h such that $m_h \mid 2^{2f} - 1$.*

PROOF. Assume that $\phi(m_h) > 2f$ for some h such that $m_h \mid 2^{2f} - 1$. Note that χ_h^{2f} is nontrivial. Consider the character

$$\theta = \prod_{i=1}^r \chi_i^{f_i}.$$

Since r is even, θ is an even character. Next, we consider the characters

$$\theta' = \chi_h^{2f-f_h} \theta = \chi_h^{2f} \prod_{i \neq h} \chi_i^{f_i}$$

and

$$\theta'' = \prod_{i \neq h} \chi_i^{f_i}.$$

Since $\theta' \in X^-(m, p)$, by Theorem 2.13, we have $\theta'(2) = 1$. On the other hand, since $\chi_h^{2f}(2) = \chi_h(2^{2f}) = 1$, we have $\theta''(2) = 1$. Similarly, for any k with $k \neq h$, let

$$\theta''' = \chi_k^{-f_k} \prod_{i \neq h, k} \chi_i^{f_i}.$$

Then, $\theta'''(2) = 1$. Hence, we have $\chi_k^{2f_k}(2) = 1$. Then, $m_k \mid 2^{2f} - 1$ for any k with $k \neq h$, which contradicts to $m_j \nmid 2^{2f} - 1$ for some j . Hence, $\phi(m_h) \leq 2f$ for any h such that $m_h \mid 2^{2f} - 1$. \square

REMARK 3.5. We can improve Proposition 3.4 in the $r = 2$ case as “If $m_1 \nmid 2^{2f} - 1$ and $m_2 \mid 2^{2f} - 1$, it holds that $\phi(m_2) \leq 2f$.” Let $j = 1$ and $h = 2$ in the proof of Proposition 3.4. Then, we can similarly prove that $\theta''(2) = \chi_1^{f_1}(2) = 1$. Then, we have $m_1 \mid 2^{f_1} - 1$, which contradicts to $m_1 \nmid 2^{2f} - 1$.

PROPOSITION 3.6. Assume that f is odd, r is even and $(N, f, p) \in \mathcal{P}^*$. If there is j such that $m_j \nmid 2^{2f} - 1$, it holds that $m_k \mid p_j^{2f} - 1$ for any k with $k \neq j$.

PROOF. If $\phi(m_j) \leq 2f_j$, since $2f_j$ divides $\phi(m_j)$, we have $\phi(m_j) = 2f_j$, which implies that $\phi(m_j) \mid 2f$. However, this contradicts to $m_j \nmid 2^{2f} - 1$. Hence, we have $\phi(m_j) > 2f_j$, and then $\chi_j^{2f_j}$ is nontrivial. Let

$$\theta = \chi_j^{f_j} \prod_{i=1}^r \chi_i^{f_i} = \chi_j^{2f_j} \prod_{i \neq j} \chi_i^{f_i}.$$

Since $\theta \in X^-(m, p)$, we have $\theta(2) = 1$. Let

$$\theta' = \prod_{i \neq j} \chi_i^{f_i}.$$

Since $\theta' \in X^-(m/m_j, p)$, by Theorem 2.13, we have either $\theta'(2) = 1$ or $\theta'(p_j) = 1$. If $\theta'(2) = 1$, we have $\chi_j^{2f_j}(2) = 1$, which contradicts to $m_j \nmid 2^{2f} - 1$. Hence, $\theta'(p_j) = 1$. For any m_k with $k \neq j$, let

$$\theta'' = \chi_k^{-f_k} \prod_{i \neq j, k} \chi_i^{f_i}.$$

Then, we similarly have $\theta''(p_j) = 1$. Hence, $\chi_k^{2f_k}(p_j) = 1$. This implies that $m_k \mid p_j^{2f} - 1$. \square

The statement of the proposition above is similar to [3, Theorem 11.1] but not exactly same. We next give a necessary condition for $(N, f, p) \in \mathcal{P}^*$ with r odd.

PROPOSITION 3.7. Assume that f is odd, r is odd and $(N, f, p) \in \mathcal{P}^*$. If there are j and h such that $m_j \nmid 2^f - 1$ and $m_h \mid 2^f - 1$, then either $\phi(m_h) \leq 2f$ or $m_k \mid p_j^{2f} - 1$ for any k with $k \neq j, h$ and $m_h \mid p_j^{4f} - 1$.

PROOF. If $\chi_j^{f_j}(2) = 1$, we have $m_j \mid 2^{f_j} - 1$, which contradicts to $m_j \nmid 2^f - 1$. Hence, $\chi_j^{f_j}(2) \neq 1$.

Assume that $\phi(m_h) > 2f$. Noting that χ_h^{2f} is nontrivial, let

$$\theta = \chi_h^f \prod_{i \neq h} \chi_i^{f_i}$$

and

$$\theta' = \chi_h^{2f} \prod_{i \neq j, h} \chi_i^{f_i}.$$

Since $\theta \in X^-(m, p)$, we have $\theta(2) = 1$ by Theorem 2.13. Furthermore, since $\theta' \in X^-(m/m_j, p)$, we have $\theta'(2) = 1$ or $\theta'(p_j) = 1$. If $\theta'(2) = 1$, we have $\chi_h^f(2) = \chi_j^{f_j}(2) \neq 1$, which contradicts to $m_h \mid 2^f - 1$. Hence, $\theta'(p_j) = 1$. For k with $k \neq j, h$, let

$$\theta'' = \chi_h^{2f} \chi_k^{-f_k} \prod_{i \neq j, h, k} \chi_i^{f_i}.$$

Then, we similarly have $\theta''(p_j) = 1$. Hence, we obtain $\chi_k^{2f_k}(p_j) = 1$. This implies that $m_k \mid p_j^{2f} - 1$. Furthermore, let

$$\theta''' = \chi_h^{-2f} \prod_{i \neq j, h} \chi_i^{f_i}.$$

Then, we similarly have $\theta'''(p_j) = 1$. Hence, we obtain $\chi_h^{4f}(p_j) = 1$. This implies that $m_h \mid p_j^{4f} - 1$. \square

EXAMPLE 3.8. Let $f = 7$. Then, all integers $N > 2$ satisfying the condition of Theorem 3.1 are

$$6, 30, 86, 174, 254, 258, 290, 430, 762, 1270, 2494, 7366, \\ 10922, 32766, 37410, 110490, 163830, 950214, 1583690.$$

Proposition 3.3 reduces the list above to 254, 762, 10922, 32766. Furthermore, 762 and 10922 are excluded by Remark 3.5, and 32766 is excluded by Proposition 3.7. For the remaining $N = 254$, we have $(254, 129) \in \mathcal{P}_7^*$. Thus, $(N, \bar{p}) \in \mathcal{P}_7^*$ are classified.

The following is our main theorem in this subsection.

THEOREM 3.9. For $f = 3, 5, 7, 9, 11, 13, 17, 19, 23$, all $(N, \bar{p}) \in \mathcal{P}_f^*$ are listed below:

$$\begin{aligned} f = 3 : & \quad (N, \bar{p}) = (14, 9), (42, 25), (78, 55); \\ f = 5 : & \quad (N, \bar{p}) = (62, 33), (110, 31); \\ f = 7 : & \quad (N, \bar{p}) = (254, 129); \\ f = 9 : & \quad (N, \bar{p}) = (146, 37), (1022, 513); \\ f = 11 : & \quad (N, \bar{p}) = (46, 3), (178, 39), (4094, 2049); \\ f = 13 : & \quad (N, \bar{p}) = (16382, 8193); \\ f = 17 : & \quad (N, \bar{p}) = (262142, 131073); \\ f = 19 : & \quad (N, \bar{p}) = (1048574, 524289); \\ f = 23 : & \quad (N, \bar{p}) = (94, 3), (356962, 83663), (16777214, 8388609). \end{aligned}$$

PROOF. First, we list all $N = 2m$ satisfying the condition of Theorem 3.1. Then, similarly to Example 3.8, we reduce the candidates of N such that $(N, f, p) \in \mathcal{P}^*$ by applying Propositions 3.3, 3.4, 3.6, 3.7, and Remark 3.5. For remaining candidates, we used a computer to directly check whether there is p such that $(N, f, p) \in \mathcal{P}^*$ based on Proposition 2.7. \square

3.2. Characterization of pure Gauss sums of small index. In Tables 1 and 2 of the appendix, we will give a list of $(N, \bar{p}) \in \mathcal{P}_f^*$ for $N \leq 5000$ and odd f by using a computer. Almost all examples listed in the tables belong to $\mathcal{P}^{(2)}$ or satisfy $\phi(N)/f \leq 8$. Therefore, in this subsection, we characterize $(N, \bar{p}) \in \mathcal{P}_f^*$ such that f is odd and $\phi(N)/f \leq 8$. Note that $\phi(N)/f$ must be even since f is odd. Hence, we consider the cases where $\phi(N)/f = 2, 4, 6, 8$.

PROPOSITION 3.10. *Assume that $\phi(N)/f = 2$. Then, $(N, f, p) \in \mathcal{P}^*$ if and only if $r = 1$, $p_1 \equiv 7 \pmod{8}$ and $p \equiv g^2 \pmod{N}$, where g is a generator of $(\mathbb{Z}/N\mathbb{Z})^\times$.*

PROOF. It is clear that $r = 1$ since f is odd and $\phi(N)/f = 2$. Then, by Theorem 2.13, $(N, f, p) \in \mathcal{P}^*$ if and only if $\chi_1^{f_1}(-1) = -1$ and $\chi_1^{f_1}(2) = 1$, where $\chi_1^{f_1}$ is of order 2. Note that $\chi_1^{f_1}(-1) = -1$ if and only if $p_1 \equiv 3 \pmod{4}$. On the other hand, by the supplementary law of quadratic reciprocity, $\chi_1^{f_1}(2) = 1$ if and only if $p_1 \equiv 1, 7 \pmod{8}$.

Furthermore, we need to choose p so that $\phi(N) = 2\text{ord}_N(p)$, i.e., $p \equiv g^2 \pmod{N}$. \square

The claim above is also obtainable from the complete characterization of index 2 Gauss sums [33].

PROPOSITION 3.11. *Assume $\phi(N)/f = 6$. Then, $(N, f, p) \in \mathcal{P}^*$ if and only if $r = 1$, $p_1 \equiv 7 \pmod{24}$ such that $p_1 = a^2 + 27b^2$ for some integers a, b , and $p \equiv g^6 \pmod{N}$, where g is a generator of $(\mathbb{Z}/N\mathbb{Z})^\times$.*

PROOF. Since f is odd and $\phi(N)/2f$ is odd, we have $r = 1$. Then, by Theorem 2.13, $(N, f, p) \in \mathcal{P}^*$ if and only if $\chi_1^{f_1}(-1) = -1$ and $\chi_1^{f_1}(2) = 1$, where $\chi_1^{f_1}$ is of order 6. If $6 \nmid p_1 - 1$, it must be $p_1 = 3$ since $6 \mid \phi(m_1)$. In this case, 2 is not a 6th power modulo m_1 since 2 is a generator of $(\mathbb{Z}/m_1\mathbb{Z})^\times$. Hence, we have $6 \mid p_1 - 1$. Note that $\chi_1^{f_1}(-1) = -1$ if and only if $p_1 \equiv 7 \pmod{12}$. On the other hand, by the supplementary law of quadratic reciprocity and the cubic reciprocity law [6, Corollary 2.6.4], $\chi_1^{f_1}(2) = 1$ if and only if $p_1 \equiv 1, 7 \pmod{8}$ and $p_1 = a^2 + 27b^2$ for some integers a and b .

Furthermore, we need to choose p so that $\phi(N) = 6\text{ord}_N(p)$, i.e., $p \equiv g^6 \pmod{N}$. \square

The claims (1) and (2) in Theorem 2.9 give two sufficient conditions for $(N, f, p) \in \mathcal{P}^*$ in the case where $\phi(m)/f = 4$ and f is odd. The two cases in Proposition 3.12 below correspond to those two conditions. In particular, we prove that the two conditions are also necessary.

PROPOSITION 3.12. *Assume that $\phi(N)/f = 4$. Then, $(N, f, p) \in \mathcal{P}^*$ if and only if $r = 2$, $\gcd(f_1, f_2) = 1$, and either of the following conditions holds:*

- (1) $p_1, p_2 \equiv 7 \pmod{8}$;
- (2) $p_1 \equiv 7 \pmod{8}$, $p_2 \equiv 3 \pmod{4}$ and p_1 is quadratic modulo p_2 .

Furthermore, p is chosen so that $p \equiv g_1^2 \pmod{2m_1}$ and $p \equiv g_2^2 \pmod{2m_2}$, where g_1 and g_2 are generators of $(\mathbb{Z}/2m_1\mathbb{Z})^\times$ and $(\mathbb{Z}/2m_2\mathbb{Z})^\times$, respectively.

PROOF. Since $\phi(m_i)/f_i \geq 2$, we have $r = 1$ or 2. In the $r = 1$ case, by Theorem 2.13, $(N, f, p) \in \mathcal{P}^*$ if and only if $\chi_1^{f_1}(-1) = -1$ and $\chi_1^{f_1}(2) = 1$, where $\chi_1^{f_1}$ is a character of order 4. Then, $\chi_1^{f_1}(-1) = -1$ if and only if $p_1 \equiv 5 \pmod{8}$. On the other hand, $\chi_1^{2f_1}(2) = 1$ if

and only if $p_1 \equiv 1, 7 \pmod{8}$ by the supplementary law of quadratic reciprocity. Hence, this case is impossible.

Next, we assume that $r = 2$. It is clear that $\gcd(f_1, f_2) = 1$; otherwise, $\phi(N)/f > 4$. Then, we have $\phi(m_i)/f_i = 2$, $i = 1, 2$. In this case, all characters in $D^-(N, p)$ are $\chi_1^{f_1}$ and $\chi_2^{f_2}$, both of which are of order 2. Then, by Theorem 2.13, $(N, f, p) \in \mathcal{P}^*$ if and only if $\chi_1^{f_1}(-1) = \chi_2^{f_2}(-1) = -1$ and either of the following holds: $\chi_1^{f_1}(2) = \chi_2^{f_2}(2) = 1$, $\chi_1^{f_1}(2) = \chi_2^{f_2}(p_1) = 1$ (or switching p_1 and p_2 , $\chi_1^{f_1}(p_2) = \chi_2^{f_2}(2) = 1$), or $\chi_1^{f_1}(p_2) = \chi_2^{f_2}(p_1) = 1$. It is clear that $\chi_1^{f_1}(-1) = \chi_2^{f_2}(-1) = -1$ if and only if $p_1, p_2 \equiv 3 \pmod{4}$. On the other hand, since $\chi_1^{f_1}(p_2)\chi_2^{f_2}(p_1) = -1$ by the quadratic reciprocity law, the condition that $\chi_1^{f_1}(p_2) = \chi_2^{f_2}(p_1) = 1$ is impossible. Noting that $\chi_i^{f_i}(2) = 1$ if and only if $p_i \equiv 1, 7 \pmod{8}$, the former two conditions are corresponding to the cases (1) and (2) in the statement, respectively. In these cases, noting that $\gcd(f_1, f_2) = 1$, we need to choose p so that $p \equiv g_1^2 \pmod{2m_1}$ and $p \equiv g_2^2 \pmod{2m_2}$. \square

In the following proposition, we treat pure Gauss sums with $\phi(N)/f = 8$ and f odd, which have not been characterized in the literature.

PROPOSITION 3.13. *Assume that $\phi(N)/f = 8$. Then, $(N, f, p) \in \mathcal{P}^*$ if and only if either of the following holds:*

- (1) $r = 1$, $p_1 = a^2 + 64b^2$ for some odd integers a, b , and $p \equiv g^8 \pmod{N}$, where g is a generator of $(\mathbb{Z}/N\mathbb{Z})^\times$;
- (2) $r = 2$, $p_1 \equiv 5 \pmod{8}$, $p_2 \equiv 3 \pmod{8}$, $\gcd(f_1, f_2) = 1$, p_1 is quadratic modulo p_2 and p_2 is quartic modulo p_1 . Furthermore, $p \equiv g_1^4 \pmod{2m_1}$ and $p \equiv g_2^2 \pmod{2m_2}$, where g_1 and g_2 are generators of $(\mathbb{Z}/2m_1\mathbb{Z})^\times$ and $(\mathbb{Z}/2m_2\mathbb{Z})^\times$, respectively.
- (3) $r = 3$, $\gcd(f_i, f_j) = 1$ for any distinct $i, j \in \{1, 2, 3\}$ and either one of the following holds:
 - i) $p_1, p_2, p_3 \equiv 7 \pmod{8}$;
 - ii) $p_1 \equiv 7 \pmod{8}$, $p_2, p_3 \equiv 3 \pmod{8}$ and p_1 is quadratic modulo p_i for both $i = 2, 3$;
 - iii) $p_1 \equiv 7 \pmod{8}$, $p_2, p_3 \equiv 3 \pmod{8}$, p_1 is quadratic modulo p_2 and p_2 is quadratic modulo p_3 .

Furthermore, $p \equiv g_i^2 \pmod{2m_i}$ for all $i = 1, 2, 3$, where g_i is a generator of $(\mathbb{Z}/2m_i\mathbb{Z})^\times$, respectively.

PROOF. Since $\phi(m_i)/f_i \geq 2$, we have $r = 1, 2$ or 3 . In the case where $r = 1$, by Theorem 2.13, $(N, f, p) \in \mathcal{P}^*$ if and only if $\chi_1^{f_1}(-1) = -1$ and $\chi_1^{f_1}(2) = 1$, where $\chi_1^{f_1}$ is a character of order 8. Then, $\chi_1^{f_1}(-1) = -1$ if and only if $p_1 \equiv 9 \pmod{16}$. On the other hand, by [6, Corollary 7.5.8], $\chi_1^{f_1}(2) = 1$ under the assumption that $p_1 \equiv 9 \pmod{16}$ if and only if $p_1 = a^2 + 64b^2$ for some odd integers a, b . In this case, p must be chosen so that $\phi(N) = 8\text{ord}_N(p)$, i.e., $p \equiv g^8 \pmod{N}$.

Assume that $r = 2$. If $\phi(m_i)/f_i = 2$ for $i = 1, 2$, it follows that $\gcd(f_1, f_2) = 2$, which contradicts to that f is odd. Hence, we can assume that $\phi(m_1)/f_1 = 4$, $\phi(m_2)/f_2 = 2$ and $\gcd(f_1, f_2) = 1$. Then, all characters in $D^-(N, p)$ are given as

$$\chi_1^{f_1}, \chi_1^{3f_1}, \chi_2^{f_2}, \chi_1^{2f_1}\chi_2^{f_2}.$$

Note that $\chi_1^{f_1}(-1) = -1$ if and only if $p_1 \equiv 5 \pmod{8}$. Then, by the supplementary law of quadratic reciprocity, we have $\chi_1^{2f_1}(2) = -1$. Since $\chi_1^{2f_1}\chi_2^{f_2}(2) = 1$ by Theorem 2.13, we have $\chi_2^{f_2}(2) = -1$. Noting that $\chi_2^{f_2}(-1) = -1$ if and only if $p_2 \equiv 3 \pmod{4}$, by the supplementary law of quadratic reciprocity, we have $p_2 \equiv 3 \pmod{8}$. On the other

hand, by Theorem 2.13, either $\chi_2^{f_2}(2) = 1$ or $\chi_2^{f_2}(p_1) = 1$ holds. Since $\chi_2^{f_2}(2) = -1$, we have $\chi_2^{f_2}(p_1) = 1$. Similarly, we have $\chi_1^{f_1}(p_2) = 1$. These conditions correspond to the case (2) in the statement. In this case, p must be chosen so that $p \equiv g_1^4 \pmod{2m_1}$ and $p \equiv g_2^2 \pmod{2m_2}$.

We finally assume that $r = 3$. Then, we have $\phi(m_i)/f_i = 2$ for every $i = 1, 2, 3$ and $\gcd(f_i, f_j) = 1$ for any distinct $i, j \in \{1, 2, 3\}$. In this case, all characters in $D^-(N, p)$ are

$$\chi_1^{f_1}, \chi_2^{f_2}, \chi_3^{f_3} \text{ and } \chi_1^{f_1} \chi_2^{f_2} \chi_3^{f_3}.$$

Note that $\chi_1^{f_1}(-1) = \chi_2^{f_2}(-1) = \chi_3^{f_3}(-1) = -1$ if and only if $p_1, p_2, p_3 \equiv 3 \pmod{4}$. It follows that $\chi_1^{f_1} \chi_2^{f_2} \chi_3^{f_3}(2) = 1$ by Theorem 2.13. Then, by the supplementary law of quadratic reciprocity, $\chi_i^{f_i}(2) = 1$ for all i if and only if $p_i \equiv 7 \pmod{8}$ for all i . This corresponds to the case (3)-i) in the statement. In other cases, we can assume that $\chi_1^{f_1}(2) = 1$ and $\chi_2^{f_2}(2) = \chi_3^{f_3}(2) = -1$. These are equivalent to that $p_1 \equiv 7 \pmod{8}$ and $p_2, p_3 \equiv 3 \pmod{8}$, respectively. Furthermore, by Theorem 2.13, we have either $\chi_2^{f_2}(p_1) = \chi_3^{f_3}(p_1) = 1$, $\chi_2^{f_2}(p_1) = \chi_3^{f_3}(p_2) = 1$ or $\chi_2^{f_2}(p_3) = \chi_3^{f_3}(p_2) = 1$. Since $\chi_2^{f_2}(p_3) \chi_3^{f_3}(p_2) = -1$ by the quadratic reciprocity law, $\chi_2^{f_2}(p_3) = \chi_3^{f_3}(p_2) = 1$ is impossible. The remaining two conditions are corresponding to (3)-ii) and (3)-iii) in the statement. In these cases, p must be chosen so that $p \equiv g_i^2 \pmod{2m_i}$ for $i = 1, 2, 3$. This completes the proof. \square

We list all $(\bar{p}, N) \in \mathcal{P}_f^*$ for $N \leq 5000$ and odd f in Tables 1 and 2 in the appendix. From the computational results, we have the following remark.

REMARK 3.14. For $N \leq 5000$ and odd f , $(N, f, p) \in \mathcal{P}^*$ is in $\mathcal{P}^{(2)}$ or satisfies $\phi(N)/f \leq 8$ except for $(N, f, \bar{p}) = (4042, 161, 21)$. This exception will be characterized in Theorem 4.6 (see Remark 4.7).

4. An application of pure Gauss sums to skew Hadamard difference sets

We begin with the following general construction of skew Hadamard difference sets based on pure Gauss sums.

PROPOSITION 4.1. *Let $p_i, i = 1, 2, \dots, r$, be distinct odd primes and $u_i, i = 1, 2, \dots, r$, be positive integers. Let $N = 2m = 2m_1 m_2 \cdots m_r$, where $m_i = p_i^{u_i}, i = 1, 2, \dots, r$, and let p be a prime such that $p \equiv 3 \pmod{4}$. Assume that $(N, f, p) \in \mathcal{P}^*$ with f odd. Define*

$$Y = \{h > 1 \mid h \text{ is a divisor of } m \text{ s.t. } (2h, f, p) \notin \mathcal{P}\},$$

and I as an m -subset of $\{0, 1, \dots, N-1\}$ satisfying the following conditions:

- (1) $\{x \pmod{m} \mid x \in I\} = \{0, 1, \dots, m-1\}$.
- (2) $\sum_{x \in I} \zeta_{2h}^x = 0$ for any $h \in Y$.

Then, for every odd positive integer s ,

$$(4.1) \quad D = \bigcup_{x \in I} C_i^{(N, p^{fs})}$$

forms a skew Hadamard difference set in $(\mathbb{F}_{p^{fs}}, +)$.

PROOF. First, note that $m \mid (p^f - 1)/(p - 1)$ by Lemma 2.8. Then, D is invariant under the multiplication of x^2 for any $x \in \mathbb{F}_p^*$.

Let γ be a primitive element of $\mathbb{F}_{p^{fs}}$ and let η'_N be a fixed multiplicative character of order N of $\mathbb{F}_{p^{fs}}$. Furthermore, let X be the set of all divisors of m and Z be the set

of odd $1 \leq j \leq N-1$ such that $N/2 \gcd(j, N) \in X \setminus Y$. Then, by the orthogonality of characters and the conditions (1) and (2), we have for any $a = 0, 1, \dots, p^{fs} - 2$,

$$\begin{aligned} \psi_{\mathbb{F}_{p^{fs}}}(\gamma^a D) &= \frac{1}{N} \sum_{j=0}^{N-1} \sum_{i \in I} G_{p^{fs}}(\eta_N'^j) \eta_N'^{-j}(\gamma^{a+i}) \\ (4.2) \quad &= \frac{|I|}{N} G_{p^{fs}}(\eta_N'^0) + \frac{1}{N} \sum_{j \in Z} \sum_{i \in I} G_{p^{fs}}(\eta_N'^j) \eta_N'^{-j}(\gamma^{a+i}). \end{aligned}$$

Since $G_{p^{fs}}(\eta_N'^j)$ is pure for any $j \in Z$, we have

$$\sum_{j \in Z} \sum_{i \in I} G_{p^{fs}}(\eta_N'^j) \eta_N'^{-j}(\gamma^{a+i}) \equiv 0 \pmod{p^{\frac{fs-1}{2}}}.$$

Finally, noting that $G_{p^{fs}}(\eta_N'^0) = -1$ and $\gcd(m, p) = 1$, we have $2\psi_{\mathbb{F}_{p^{fs}}}(\gamma^a D) + 1 \equiv 0 \pmod{p^{\frac{fs-1}{2}}}$. Then, by Lemma 2.15, the claim follows. \square

Even if we determine the set Y , i.e., for which h we have $(2h, f, p) \notin \mathcal{P}$, in the proposition above, it may happen that there is no nontrivial subset I satisfying the conditions (1) and (2) as commented in Section 5. Moreover, it is difficult to determine the dual of D in general. Indeed, to do this, we need to evaluate the signs (or roots of unity) of the corresponding pure Gauss sums. Thus, we have to choose suitable $(N, f, p) \in \mathcal{P}^*$ such that a nontrivial subset I exists satisfying the conditions (1) and (2) and we can evaluate the signs (or roots of unity) in some sense. From this point of view, we consider pure Gauss sums satisfying a special property defined below.

Throughout this section, we assume that the order f of p modulo N is odd and N has the prime factorization $N = 2m_1 m_2 \cdots m_r$, where $m_i = p_i^{u_i}$ with p_i an odd prime and u_i a positive integer. We consider $(N, f, p) \in \mathcal{P}^*$ such that

(\star) $(2 \prod_{i \in J} m_i, f, p) \in \mathcal{P}$ for any subset $J \subseteq \{1, 2, \dots, r\}$ such that $1 \in J$.

4.1. Characterization of pure Gauss sums with property (\star). In this subsection, we give a characterization of pure Gauss sums with property (\star).

LEMMA 4.2. *If $(N, f, p) \in \mathcal{P}^*$ and $(2 \prod_{i \in J} m_i, f, p) \in \mathcal{P}$ for a subset $J \subseteq \{1, 2, \dots, r\}$, then $(2 \prod_{i \in J} m_i, f', p) \in \mathcal{P}^*$, where $f' = \text{lcm}(f_i : i \in J)$.*

PROOF. Note that $f = \text{lcm}(f_1, f_2, \dots, f_r)$ and $f' \mid f$. Then, by Theorem 2.5, we have $(2 \prod_{i \in J} m_i, f', p) \in \mathcal{P}^*$. \square

PROPOSITION 4.3. *Assume that $(N, f, p) \in \mathcal{P}^*$ with property (\star). Then, either of the following holds:*

- (1) $\chi_i^{f_i}(2) = 1$ for any $i \in \{1, 2, \dots, r\}$; or
- (2) $\chi_1^{f_1}(2) = 1$, $\chi_i^{f_i}(2) \neq 1$ for any $i \in \{2, 3, \dots, r\}$, and $\chi_i^{f_i}(p_1) = 1$ for any $i \in \{2, 3, \dots, r\}$.

PROOF. Since $(2m_1, f, p) \in \mathcal{P}$, we have $(2m_1, f_1, p) \in \mathcal{P}^*$ by Lemma 4.2. Then, by Theorem 2.13, we have $\chi_1^{f_1}(2) = 1$. Furthermore, since $(2m_1 m_i, f, p) \in \mathcal{P}$ for any $i \in \{2, 3, \dots, r\}$, we have $(2m_1 m_i, \text{lcm}(f_1, f_i), p) \in \mathcal{P}^*$ by Lemma 4.2 again. Then, by Theorem 2.13, we have either $\chi_i^{f_i}(2) = 1$ or $\chi_i^{f_i}(p_1) = 1$.

We assume that $\chi_i^{f_i}(2) = 1$ for some $i \in \{2, 3, \dots, r\}$. Since $(2m_1 m_i m_j, f, p) \in \mathcal{P}$ for any $j \in \{2, 3, \dots, r\} \setminus \{i\}$, $(2m_1 m_i m_j, \text{lcm}(f_1, f_i, f_j), p) \in \mathcal{P}^*$ follows by Lemma 4.2. Then, by Theorem 2.13, we have $\chi_1^{f_1} \chi_i^{f_i} \chi_j^{f_j}(2) = 1$. Since $\chi_1^{f_1}(2) = \chi_i^{f_i}(2) = 1$, we have $\chi_j^{f_j}(2) = 1$. This implies that $\chi_h^{f_h}(2) = 1$ for any $h \in \{1, 2, \dots, r\}$. If $\chi_i^{f_i}(2) \neq 1$ for

any $i \in \{2, 3, \dots, r\}$, we have $\chi_i^{f_i}(p_1) = 1$ for any $i \in \{2, 3, \dots, r\}$. This completes the proof. \square

REMARK 4.4. If (N, f, p) satisfies the condition (2) in Proposition 4.3, $(2m_1, f, p) \in \mathcal{P}$ but $(2m_i, f, p) \notin \mathcal{P}$ for any $i \in \{2, 3, \dots, r\}$ by Theorem 2.13.

We now give a sufficient condition for $(N, f, p) \in \mathcal{P}^*$ with property (\star) .

THEOREM 4.5. Assume that $f = \text{ord}_N(p)$ is odd. If $(N, f, p) \in \mathcal{P}^{(2)}$, $(N, f, p) \in \mathcal{P}^*$ with property (\star) .

PROOF. Since $2 \in \langle p \rangle \pmod{m'}$ for any divisor m' of m , the assertion holds. \square

The theorem above implies that $(N, f, p) \in \mathcal{P}^{(2)}$ belongs to the class (1) of Proposition 4.3. The pure Gauss sums in this case were used for constructing skew Hadamard difference sets as in Theorem 2.16. Next, we give a sufficient condition for $(N, f, p) \in \mathcal{P}^*$ to belong to the class (2) of Proposition 4.3.

THEOREM 4.6. Assume that f_i are all odd and $\gcd(f_1, f_i) = 1$ for any $i \in \{2, 3, \dots, r\}$. If (N, f, p) satisfies that $\phi(m_1)/f_1 = 2$, $2 \in \langle p \rangle \pmod{m_1}$, $-2 \in \langle p \rangle \pmod{m/m_1}$ and $p_1 \in \langle p \rangle \pmod{m/m_1}$, then $(N, f, p) \in \mathcal{P}^*$ with property (\star) .

PROOF. By the assumption that $\gcd(f_1, f_i) = 1$ for any $i \in \{2, 3, \dots, r\}$, any odd character in $D^-(N, p)$ has the form $\tau_1 = \chi_1^{f_1} \chi$ for some even character χ modulo m/m_1 such that $\chi(p) = 1$ or $\tau_2 = \chi'$ for some odd character χ' modulo m/m_1 such that $\chi'(p) = 1$. By the assumptions that $\phi(m_1)/f_1 = 2$, $2 \in \langle p \rangle \pmod{m_1}$ and $-2 \in \langle p \rangle \pmod{m/m_1}$, we have

$$\tau_1(2) = \chi_1^{f_1}(2) \chi(2) = \chi(-1) \chi(p^i) = 1$$

for some i . On the other hand, since $p_1 \in \langle p \rangle \pmod{m/m_1}$, we have

$$\tau_2(p_1) = \chi'(p_1) = 1.$$

Then, by Theorem 2.13, it follows that $(N, f, p) \in \mathcal{P}^*$. Furthermore, it is clear that the property (\star) is satisfied. \square

The theorem above is a generalization of Proposition 3.12 (2).

REMARK 4.7. The exception $(N, \bar{p}) = (4042, 21) \in \mathcal{P}_{161}^*$ listed in Table 2 satisfies the condition in Theorem 4.6 as $m_1 = 47$ and $m_2 = 43$.

COROLLARY 4.8. Assume that

- (1) $p_1 \equiv 7 \pmod{8}$ and $p_i \equiv 3 \pmod{8}$ for all $i \in \{2, 3, \dots, r\}$;
- (2) p_1 is quadratic modulo p_i for all $i \in \{2, 3, \dots, r\}$;
- (3) $f_i = \phi(m_i)/2$ for all i ;
- (4) $\phi(m_i)/2$'s are mutually coprime.

Then, $(N, f, p) \in \mathcal{P}^*$ with property (\star) .

PROOF. By the supplementary law of quadratic reciprocity, we have $\chi_1^{f_1}(2) = 1$ and $\chi_i^{f_i}(2) = -1$ for all $i > 1$. Then, the conditions of Theorem 4.6 are fulfilled. \square

One can see that there are infinitely many tuples of m_1, m_2, \dots, m_r, p satisfying the condition of Corollary 4.8.

EXAMPLE 4.9. Fix $m_2 = 3$ and $m_3 = 11$. Let $m_1 \equiv 7 \pmod{8}$ be a prime such that m_1 is quadratic modulo both 3 and 11, i.e., $m_1 \equiv 1 \pmod{3}$ and $m_1 \equiv 1, 3, 4, 5, 9 \pmod{11}$. Furthermore, we need the restriction $m_1 \equiv 3, 5, 7, 9 \pmod{10}$ in order to satisfy that

$\gcd(\phi(m_1)/2, \phi(11)/2) = 1$. There are infinitely many such primes m_1 by the Dirichlet theorem in arithmetic progressions. For example, we can take $m_1 = 103, 199, 223, 367, 463, \dots$. Let p' be any integer with $1 \leq p' \leq N - 1$ determined by the congruences

$$\begin{cases} p' \equiv 1 \pmod{6} \\ p' \equiv 1, 3, 5, 9 \text{ or } 15 \pmod{22} \\ p' \equiv g^2 \pmod{2m_1} \end{cases}$$

for any generator g of $(\mathbb{Z}/2m_1\mathbb{Z})^\times$. Then, $\langle p' \rangle$ is of index 2 modulo $2m_i$ for each i . Then, $(N, f, p) \in \mathcal{P}^*$ with property (\star) for any odd prime $p \equiv p' \pmod{N}$, where $f := 5(m_1 - 1)/2$.

4.2. The signs or roots of unity of pure Gauss sums with property (\star) .

In this subsection, we study the signs or roots of unity of pure Gauss sums satisfying property (\star) . The following result was known.

LEMMA 4.10. ([13, Lemma 6]) *If $G_q(\eta_N)$ is pure, then $\epsilon = G_q(\eta_N)/q^{\frac{1}{2}}$ is a $2 \gcd(N, p - 1)$ th root of unity.*

The sign (root of unity) ambiguities of pure Gauss sums in the class $\mathcal{P}^{(2)}$ was completely determined as in Theorem 2.11. However, it is difficult to explicitly determine them for pure Gauss sums in general. In fact, it sometimes becomes complicated as in [13, Theorem 10]. In this subsection, we show that if $G_{p^f}(\eta_N)$ is pure with property (\star) , the sign (or root of unity) of $G_{p^f}(\eta_N)$ is determined from those of $G_{p^f}(\eta_{2m_1m_i})$'s, $1 \leq i \leq r$. This property will be used to determine the duals of skew Hadamard difference sets obtained from the construction in Theorem 4.16.

For positive integers x and y with $\gcd(x, y) = 1$, let $\text{inv}(x; y)$ denote an integer such that $x \cdot \text{inv}(x; y) \equiv 1 \pmod{y}$. The claim of the following lemma was given in the proof of [13, Theorem 7].

LEMMA 4.11. *Let $n = st$ be a positive integer, where s is an odd prime power and $t > 1$ with $\gcd(s, t) = 1$. Let η_n be a multiplicative character of order n of \mathbb{F}_{p^f} . Assume that $(n, f, p) \in \mathcal{P}$ and $(t, f, p) \in \mathcal{P}$. Then, $G_{p^f}(\eta_n)/G_{p^f}(\eta_n^{s \cdot \text{inv}(s, t)})$ is a $\gcd(p - 1, s)$ th root of unity.*

Recall that $N = 2m = 2m_1m_2 \cdots m_r$, where $m_i = p_i^{u_i}$, $i = 1, 2, \dots, r$. For a subset $J \subseteq \{1, 2, \dots, r\}$, denote $m_J = \prod_{i \in J} m_i$ and $n_J = m/m_J$. Let ω be a primitive root of \mathbb{F}_{p^f} , and let η_N be a fixed multiplicative character of order N of \mathbb{F}_{p^f} such that $\eta_N(\omega) = \zeta_N$. We denote $\eta_{2m_J} = \eta_N^{n_J \cdot \text{inv}(n_J, 2m_J)}$, and also denote an arbitrary multiplicative character of order h of \mathbb{F}_{p^f} by θ_h . Note that for any $m_i \mid m/m_J$, $\eta_{2m_J} = \eta_{2m_i m_J}^{m_i \cdot \text{inv}(m_i, 2m_J)}$.

PROPOSITION 4.12. *Assume that $(N, f, p) \in \mathcal{P}^*$ with property (\star) . Then, the following hold:*

- There are integers s_i , $i = 1, 2, \dots, r$, such that

$$(4.3) \quad G_{p^f}(\eta_{2m_1}) = \zeta_{m_1}^{s_1} G_{p^f}(\eta_2) \quad \text{and} \quad G_{p^f}(\eta_{2m_1m_i}) = \zeta_{m_i}^{s_i} G_{p^f}(\eta_{2m_1}), \quad 2 \leq i \leq r.$$

- Let $J \subseteq \{1, 2, 3, \dots, r\}$ such that $1 \in J$. Then,

$$(4.4) \quad G_{p^f}(\eta_{2m_J}) = \left(\prod_{i \in J} \zeta_{m_i}^{s_i} \right) G_{p^f}(\eta_2),$$

where s_i 's are defined as in (4.3). In particular, $s_1 = 0$.

PROOF. (4.3) is a direct consequence of Lemma 4.11. Furthermore, we have $s_1 = 0$ by Proposition 2.11.

We prove that (4.4) holds. Let m_i, m_j be distinct prime power divisors of m/m_1 and J be any subset of $\{1, 2, \dots, r\} \setminus \{i, j\}$ containing 1. By Lemma 4.11, we have

$$\begin{cases} G_{p^f}(\eta_{2m_i m_J})/G_{p^f}(\eta_{2m_J}) = \zeta_{m_i}^u \\ G_{p^f}(\eta_{2m_j m_J})/G_{p^f}(\eta_{2m_J}) = \zeta_{m_j}^{u'} \end{cases} \quad \text{and} \quad \begin{cases} G_{p^f}(\eta_{2m_i m_j m_J})/G_{p^f}(\eta_{2m_i m_J}) = \zeta_{m_i}^v \\ G_{p^f}(\eta_{2m_i m_j m_J})/G_{p^f}(\eta_{2m_j m_J}) = \zeta_{m_j}^{v'} \end{cases}$$

for some integers u, u', v, v' . By combining these equations, we have $\zeta_{m_i}^u \zeta_{m_j}^{v'} = \zeta_{m_i}^v \zeta_{m_j}^{u'}$, i.e., $u = v$ and $u' = v'$. Hence, $G_{p^f}(\eta_{2m_i m_j m_J})/G_{p^f}(\eta_{2m_J}) = \zeta_{m_i}^u \zeta_{m_j}^{u'}$. This argument inductively shows (4.4). \square

PROPOSITION 4.13. Assume that $(N, f, p) \in \mathcal{P}^*$ with property (\star) . Let $J \subseteq \{1, 2, \dots, r\}$ such that $1 \in J$, and let $J' \subseteq J$. Furthermore, let $v = \prod_{i \in J'} p_i^{\ell_i}$ for some integers $1 \leq \ell_i \leq u_i - 1$. Then,

$$(4.5) \quad G_{p^f}(\eta_{2m_J}^v) = \left(\prod_{i \in J} \zeta_{m_i}^{v s_i} \right) G_{p^f}(\eta_2).$$

PROOF. By Corollary 2.4, we have

$$(4.6) \quad G_{p^f}(\eta_{2m_J}^v) = p^{-f \frac{v-1}{2}} \sigma_{1, v-1} \left(\prod_{j=0}^{v-1} G_{p^f}(\eta_{2m_J} \theta_v^j) \right),$$

where $\sigma_{1, v-1} \in \text{Gal}(\mathbb{Q}(\zeta_{2m_J}, \zeta_p)/\mathbb{Q})$ and θ_v is any multiplicative character of order v of \mathbb{F}_{p^f} . Noting that $\gcd(2m_J, 1 + 2m_J j/v) = 1$ for any $j = 0, 1, \dots, v-1$, we have $\sigma_{1+2m_J j/v, 1}(G_{p^f}(\eta_{2m_J})) = G_{p^f}(\eta_{2m_J}^{1+2m_J j/v})$. On the other hand, by Proposition 4.12, we have $\sigma_{1+2m_J j/v, 1}(G_{p^f}(\eta_{2m_J})) = \left(\prod_{i \in J} \zeta_{m_i}^{s_i(1+2m_J j/v)} \right) G_{p^f}(\eta_2)$. Hence, $G_{p^f}(\eta_{2m_J}^{1+2m_J j/v}) = \left(\prod_{i \in J} \zeta_{m_i}^{s_i(1+2m_J j/v)} \right) G_{p^f}(\eta_2)$. Then, by noting that v is odd,

$$\begin{aligned} \prod_{j=0}^{v-1} G_{p^f}(\eta_{2m_J} \theta_v^j) &= \prod_{j=0}^{v-1} G_{p^f}(\eta_{2m_J}^{1+2m_J j/v}) \\ &= \left(\prod_{i \in J} \zeta_{m_i}^{s_i v} \right) \left(\prod_{i \in J} \zeta_{m_i}^{s_i 2m_J (1+\dots+v-1)/v} \right) G_{p^f}(\eta_2)^v \\ &= \left(\prod_{i \in J} \zeta_{m_i}^{s_i v} \right) G_{p^f}(\eta_2)^v. \end{aligned}$$

Furthermore, we have

$$G_{p^f}(\eta_2)^v = \eta_2^{\frac{v-1}{2}} (-1) p^{f \frac{v-1}{2}} G_{p^f}(\eta_2).$$

Therefore, (4.6) is reformulated as

$$G_{p^f}(\eta_{2m_J}^v) = \eta_2^{\frac{v-1}{2}} (-1) \left(\prod_{i \in J} \zeta_{m_i}^{s_i v} \right) \sigma_{1, v-1}(G_{p^f}(\eta_2)) = \eta_2^{\frac{v-1}{2}} (-1) \eta_2(v) \left(\prod_{i \in J} \zeta_{m_i}^{s_i v} \right) G_{p^f}(\eta_2).$$

Finally, we see that $\eta_2^{\frac{v-1}{2}} (-1) \eta_2(v) = 1$. Note that $\eta_2(v) = \prod_{i \in J'} \left(\frac{p_i}{p} \right)^{\ell_i}$, where $\left(\frac{p_i}{p} \right)$ is the Legendre symbol. Since f is odd, we have $\left(\frac{p}{p_i} \right) = 1$. Then, by the quadratic reciprocity law, we have

$$\prod_{i \in J'} \left(\frac{p_i}{p} \right)^{\ell_i} = \prod_{i \in J'} (-1)^{\frac{(p-1)(p_i-1)\ell_i}{4}}.$$

Let h be the number of $i \in J'$ such that $p_i \equiv 3 \pmod{4}$ and ℓ_i is odd. Then, we have $\eta_2(v) = (-1)^{h(p-1)/2}$. On the other hand, $\eta_2^{\frac{v-1}{2}}(-1) = 1$ if and only if $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$ and $v \equiv 1 \pmod{4}$ (i.e., h is even). Hence, $\eta_2(v) = \eta_2^{\frac{v-1}{2}}(-1)$. This completes the proof of the proposition. \square

REMARK 4.14. (1) Recall that $\eta_{2m_J} = \eta_{2m}^{n_J \cdot \text{inv}(n_J, 2m_J)}$. Let

$$(4.7) \quad A = s_1 m_2 \cdots m_r + \cdots + s_r m_1 \cdots m_{r-1}.$$

Then, we have

$$\eta_{2m_J}(\omega^{2A}) = \prod_{i=1}^r \zeta_{m_i}^{s_i n_J \cdot \text{inv}(n_J, 2m_J)} = \prod_{i \in J} \zeta_{m_i}^{s_i n_J \cdot \text{inv}(n_J, 2m_J)}.$$

Since $n_J \cdot \text{inv}(n_J, 2m_J) \equiv 1 \pmod{m_i}$ for $i \in J$, we have $\eta_{2m_J}(\omega^{2A}) = \prod_{i \in J} \zeta_{m_i}^{s_i}$. Hence, by Propositions 4.12 and 4.13, for any odd j such that $p_1 \mid \frac{N}{\gcd(j, N)}$,

$$(4.8) \quad G_{p^f}(\eta_N^j) = \eta_N^j(\omega^{2A}) G_{p^f}(\eta_2).$$

- (2) If (N, p, f) satisfies the condition of Theorem 4.6, $\eta_N(\omega^{2A})$ is a cubic root of unity. In fact, the condition $-2 \in \langle p \rangle \pmod{m/m_1}$ implies that $\gcd(m_i, p-1) = 1$ or 3 for any $i = 2, 3, \dots, r$. Then, by Lemma 4.11 and Proposition 4.12, the claim follows.

4.3. A construction of skew Hadamard difference sets. In this subsection, we show that if $(N, f, p) \in \mathcal{P}^*$ with property (\star) , there are nontrivial choices of I satisfying the conditions (1) and (2) of Proposition 4.1. Furthermore, we can determine the dual of D in this case. First, we illustrate our construction giving one example below.

EXAMPLE 4.15. As in Table 1, we have $(42, 3, 67) \in \mathcal{P}^*$ and $(14, 3, 67) \in \mathcal{P}$, i.e., it satisfies the condition (\star) as $m_1 = 7$. Note that $(6, 3, 67) \notin \mathcal{P}$, i.e., $(42, 3, 67) \in \mathcal{P}^*$ belongs to the class (2) of Proposition 4.3. Let I be any 21-subset of $\{0, 1, \dots, 41\}$ satisfying the following conditions:

- (1) $\{x \pmod{21} \mid x \in I\} = \{0, 1, \dots, 20\}$;
- (2) $\sum_{x \in I} \zeta_6^x = 0$.

For example, we can take

$$I = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 40\}.$$

Then, for every odd positive integer s ,

$$D = \bigcup_{x \in I} C_i^{(42, 67^{3s})}$$

forms a skew Hadamard difference set in $(\mathbb{F}_{67^{3s}}, +)$. Furthermore, its dual is given as $D^\perp = \{\psi_a \in G^\perp \mid a \in \bigcup_{i \in I'} C_i^{(N, p^{fs})}\}$, where $I' = -I + 14s$.

THEOREM 4.16. With notations as in Proposition 4.1, assume that $(N, f, p) \in \mathcal{P}^*$ with property (\star) . Furthermore, redefine Y as

$$Y = \{h > 1 \mid h \text{ is a divisor of } \prod_{i=2}^r m_i\}.$$

Then, for every odd positive integer s , the set D defined in (4.1) forms a skew Hadamard difference set in $(\mathbb{F}_{p^{fs}}, +)$. In particular, its dual is given as $D^\perp = \{\psi_a \in G^\perp \mid a \in \bigcup_{i \in I'} C_i^{(N, p^{fs})}\}$, where $I' = -I + 2As$, where A is defined as in (4.7).

PROOF. Let γ be a primitive element of $\mathbb{F}_{p^{fs}}$ and let $\omega = \gamma^{(p^{fs}-1)/(p^f-1)}$. Furthermore, let η_N be a fixed multiplicative character of order N of \mathbb{F}_{p^f} such that $\eta_N(\omega) = \zeta_N$, and let η'_N be the lift of η_N to $\mathbb{F}_{p^{fs}}$. Continuing from (4.2), we have by Theorem 2.5 that

$$(4.9) \quad \psi_{\mathbb{F}_{p^{fs}}}(\gamma^a D) = -\frac{1}{2} + \frac{1}{N} \sum_{j \in Z} \sum_{i \in I} (G_{p^f}(\eta_N^j))^s \eta_N^{-j}(\omega^{a+i}).$$

By Proposition 4.13 and Remark 4.14, for any $j \in Z$

$$G_{p^f}(\eta_N^j) = \eta_N^j(\omega^{2A}) G_{p^f}(\eta_2).$$

Hence, continuing from (4.9), we have

$$\begin{aligned} \psi_{\mathbb{F}_{p^{fs}}}(\gamma^a D) &= -\frac{1}{2} + \frac{(G_{p^f}(\eta_2))^s}{N} \sum_{j \in Z} \sum_{i \in I} \eta_N^{-j}(\omega^{a+i}) \eta_N^{js}(\omega^{2A}) \\ &= -\frac{1}{2} + \frac{G_{p^{fs}}(\eta'_2)}{N} \sum_{j=1}^{N-1} \sum_{i \in I} \eta_N^{-j}(\omega^{a-2As+i}) \\ &= -\frac{1}{2} + \frac{G_{p^{fs}}(\eta'_2)}{N} \cdot \begin{cases} m & \text{if } -a + 2As \in I, \\ -m & \text{otherwise,} \end{cases} \end{aligned}$$

where η'_2 is the quadratic character of $\mathbb{F}_{p^{fs}}$. Hence, by (2.4), we obtain $\psi_{\mathbb{F}_{p^{fs}}}(\gamma^a D) \in \{\frac{-1 \pm \sqrt{-p^{fs}}}{2}\}$. This implies that D is a skew Hadamard difference set. Furthermore, its dual is determined as desired. \square

REMARK 4.17. There are nontrivial choices of I satisfying the conditions of Theorem 4.16. For example, let $S_i = \{2im/m_1 + j \mid 0 \leq j \leq 2m/m_1 - 1\}$ for $i = 0, 1, \dots, (m_1 - 3)/2$ and let A_0, A_1 be an arbitrary partition of $J = \{0, 1, \dots, (m_1 - 3)/2\}$. Then, we can take

$$\begin{aligned} I &= \left\{ x \mid x \in \bigcup_{i \in A_0} S_i \right\} \cup \left\{ x + m \mid x \in \bigcup_{i \in A_1} S_i \right\} \\ &\cup \left\{ \frac{(m_1 - 1)m}{m_1} + 2i \mid i = 0, 1, \dots, \frac{m/m_1 - 1}{2} \right\} \\ &\cup \left\{ \frac{(m_1 - 1)m}{m_1} + m + 2i - 1 \mid i = 1, 2, \dots, \frac{m/m_1 - 1}{2} \right\}. \end{aligned}$$

This is a generalization of I in Example 4.15.

The following result is immediately obtained by applying Theorem 4.16 to the class $\mathcal{P}^{(2)}$.

COROLLARY 4.18. Assume that $2 \in \langle p \rangle \pmod{m}$. Let $Y = \{h > 1 \mid h \text{ is a divisor of } \prod_{i=2}^r m_i\}$, and let I be an arbitrary m -subset of $\{0, 1, \dots, N - 1\}$ such that $\{x \pmod{m} \mid x \in I\} = \{0, 1, \dots, m - 1\}$ and $\sum_{x \in I} \zeta_{2h}^x = 0$ for any $h \in Y$. Then, for any odd positive integer s , $D = \bigcup_{x \in I} C_i^{(N, p^{fs})}$ forms a skew Hadamard difference set in $(\mathbb{F}_{p^{fs}}, +)$.

PROOF. The assumption that $2 \in \langle p \rangle \pmod{m}$ implies that $(N, f, p) \in \mathcal{P}^{(2)}$ with property (\star) belonging to the class (1) of Proposition 4.3 by Theorem 4.5. Then, by Theorem 4.16, the claim follows. \square

Note that the result above is contained in Theorem 2.16. In fact, the construction given in Theorem 2.16 allows I as an arbitrary subset of $\{0, 1, \dots, N - 1\}$ satisfying the

condition (1) but not necessarily satisfying the condition (2) since $(2m', f, p) \in \mathcal{P}^*$ for any divisor m' of m . This also follows from Proposition 4.1 as $Y = \emptyset$.

The following is a new result not within the framework of Theorem 2.16.

COROLLARY 4.19. *Assume that f_i are all odd and $\gcd(f_1, f_i) = 1$ for any $i \in \{2, 3, \dots, r\}$. If (N, f, p) satisfies that $\phi(m_1)/f_1 = 2$, $2 \in \langle p \rangle \pmod{m_1}$, $2 \in -\langle p \rangle \pmod{m/m_1}$ and $p_1 \in \langle p \rangle \pmod{m/m_1}$, Let $Y = \{h > 1 \mid h \text{ is a divisor of } \prod_{i=2}^r m_i\}$, and let I be an arbitrary m -subset of $\{0, 1, \dots, N-1\}$ such that $\{x \pmod{m} \mid x \in I\} = \{0, 1, \dots, m-1\}$ and $\sum_{x \in I} \zeta_{2h}^x = 0$ for any $h \in Y$. Then, for any odd positive integer s , $D = \bigcup_{x \in I} C_i^{(N, p^{fs})}$ forms a skew Hadamard difference set in $(\mathbb{F}_{p^{fs}}, +)$.*

PROOF. The assumptions imply that $(N, f, p) \in \mathcal{P}^*$ with property (\star) belonging to the class (2) of Proposition 4.3 by Theorem 4.6. Then, by Theorem 4.16, the claim follows. \square

REMARK 4.20. We remark that any $(N, f, p) \in \mathcal{P}^*$ satisfying the condition of Proposition 3.12 (2) or 3.13 (3)-ii) also satisfies the condition of Corollary 4.19. Hence, by Tables 1 and 2, there exist $(N, f, p) \in \mathcal{P}^*$ satisfying the condition of Corollary 4.19 in abundance.

REMARK 4.21. In this remark, we discuss the inequivalence problem on skew Hadamard difference sets obtained from Theorem 4.16. Two skew Hadamard difference sets D_1 and D_2 in an abelian group G are called *equivalent* if there exists an automorphism $\sigma \in \text{Aut}(G)$ and an element $x \in G$ such that $\sigma(D_1) + x = D_2$.

Let D be a skew Hadamard difference set in $(\mathbb{F}_q, +)$. For a fixed $a \in \mathbb{F}_p^*$, define

$$T_{x,a}(D) := |D \cap (D - x) \cap (D - a \cdot x)|, \quad x \in \mathbb{F}_q^*,$$

and

$$n_a(D) = |\{T_{x,a}(D) \mid x \in \mathbb{F}_q^*\}|.$$

It is known that $n_a(D)$ is an invariant of the equivalence of skew Hadamard difference sets in $(\mathbb{F}_q, +)$, cf. [27].

It is clear that the Paley difference set D_P satisfies that $n_a(D_P) \leq 2$ for any $a \in \mathbb{F}_p^*$. If a skew Hadamard difference set D satisfies $n_a(D) \geq 3$ for some $a \in \mathbb{F}_p^*$, then D is inequivalent to D_P . Let $D_0 \subseteq \mathbb{F}_{67^3}$ be the skew Hadamard difference set in Example 4.15. We checked by a computer that $n_a(D_0) \geq 3$ for $a = 3$. On the other hand, since $(N, f, p) = (14, 3, 67) \in \mathcal{P}^{(2)}$, the set $D = \bigcup_{i \in I} C_i^{(14, 67^3)}$ is also a skew Hadamard difference set for any 7-subset I of $\{0, 1, \dots, 13\}$ such that $I \cap \{x + 7 \pmod{14} \mid x \in I\} = \emptyset$. Let

$$\begin{aligned} I_1 &= \{0, 1, 2, 3, 4, 5, 6\}, I_2 = \{0, 1, 2, 3, 4, 6, 12\}, \\ I_3 &= \{0, 1, 6, 9, 10, 11, 12\}, I_4 = \{0, 1, 2, 4, 6, 10, 12\} \end{aligned}$$

and define $D_j = \bigcup_{i \in I_j} C_i^{(14, 67^3)}$ for $j = 1, 2, 3, 4$. We checked by a computer that D_j , $j = 1, 2, 3, 4$, are mutually inequivalent and they are also inequivalent to the Paley difference set. Furthermore, it holds that $n_3(D_0) \neq n_3(D_j)$ for any $j = 1, 2, 3, 4$. Hence, D_0 is inequivalent to D_j 's. Thus, Corollary 4.19 can give rise to skew Hadamard difference sets not obtained from Theorem 2.16.

5. Concluding remarks

In this section, we give a comment on Proposition 4.1. The author could not find any nontrivial example of skew Hadamard difference sets fitting the general construction given in Proposition 4.1 other than those obtained from Theorem 4.16. Let us consider pure Gauss sums not satisfying property (\star) , e.g., Gauss sums in the $r = 2$ case such

that $(2p_i, f, p) \notin \mathcal{P}$ for each $i = 1, 2$ and $(2p_1p_2, f, p) \in \mathcal{P}$. Note that the pure Gauss sums in Proposition 3.13 (2) belong to this class. Then, the conditions (1) and (2) in Proposition 4.1 are equivalent to that $\sum_{i \in I} \zeta_t^i = 0$ for any $t \in \{p_1, p_2, p_1p_2, 2p_1, 2p_2\}$. By identifying the subset I with the polynomial $f(x) = \sum_{i \in I} x^i \pmod{x^N - 1}$, the condition above is equivalent to

$$(5.1) \quad f(x) \equiv 0 \pmod{\Phi_t}, \quad \forall t \in \{p_1, p_2, p_1p_2, 2p_1, 2p_2\},$$

where Φ_t is the t th cyclotomic polynomial. The problem is whether there is a polynomial $f(x) \pmod{x^N - 1}$ with coefficients from $\{0, 1\}$ and with exactly p_1p_2 nonzero coefficients such that $f(x) \not\equiv 0 \pmod{\Phi_{2p_1p_2}}$ and (5.1) is satisfied. For example, we checked by a computer that there is no such $f(x)$ for $(p_1, p_2) = (3, 5), (3, 7)$. This problem remains open in general, which is difficult but interesting besides evaluating Gauss sums.

References

- [1] K. T. Arasu, J. F. Dillon, K. J. Player, Character sum factorizations yield sequences with ideal two-level autocorrelation, *IEEE Trans. Inform. Theory* **61**, 3276–3304, (2015).
- [2] N. Aoki, On the purity problem of Gauss sums and Jacobi sums over finite fields, *Comm. Math. Univ. Sancti Pauli* **46**, 223–233, (1997).
- [3] N. Aoki, A fitness theorem on pure Gauss sums, *Comm. Math. Univ. Sancti Pauli* **53**, 145–168, (2004).
- [4] N. Aoki, On multi-quadratic Gauss sums, *Comm. Math. Univ. Sancti Pauli* **59**, 97–117, (2010).
- [5] N. Aoki, On pure Gauss sums, *Comm. Math. Univ. Sancti Pauli* **61**, 133–165, (2012).
- [6] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
- [7] Y. Q. Chen, Q. Xiang, S. K. Sehgal, An exponent bound on skew Hadamard abelian difference sets, *Des. Codes Cryptogr.* **4**, 313–317, (1994).
- [8] Y. Q. Chen, T. Feng, Paley type sets from cyclotomic classes and Arasu-Dillon-Player difference sets, *Des. Codes Cryptogr.* **74**, 581–600, (2015).
- [9] S. Chowla, On Gaussian sums, *Narske Vid. Selsk. Forh.* **35** 66–67, (1962).
- [10] S. Chowla, On Gaussian sums, *Proc. Nat. Acad. Sci.* **48** 1127–1128, (1962).
- [11] C. Ding, J. Yuan, A family of skew Hadamard difference sets, *J. Combin. Theory, Ser. A* **113**, 1526–1535, (2006).
- [12] R. J. Evans, Generalization of a theorem of Chowla on Gaussian sums, *Houston J. Math.* **3**, 343–349, (1977).
- [13] R. J. Evans, Pure Gauss sums over finite fields, *Mathematika* **28**, 239–248, (1981).
- [14] R. Evans, H. D. L. Hollmann, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums, and p -ranks of cyclic difference sets, *J. Combin. Theory, Ser. A* **87**, 74–119, (1999).
- [15] K. Feng, J. Yang, The evaluation of Gauss sums for characters of 2-power order in the index 4 case, *Algebra Colloq.* **18**, 571–588, (2011).
- [16] K. Feng, J. Yang, S. Luo, Gauss sum of index 4. I. Cyclic case. *Acta Math. Sin. (Engl. Ser.)* **21**, 1425–1434, (2005).
- [17] T. Feng, Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combin. Theory, Ser. A* **119**, 245–256, (2012).
- [18] T. Feng, F. Wan, Q. Xiang, Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes, *Des. Codes Cryptogr.* **65**, 247–257, (2012).
- [19] C. F. Gauss, *Disquisitiones arithmeticae*, translated by A.A. Clarke, Yale Univ. Press, (1966).
- [20] T. Hellesteth, H. D. L. Hollmann, A. Kholosha, Z. Wang, Q. Xiang, Proofs of two conjectures on ternary weakly regular bent functions, *IEEE Trans. Inform. Theory* **55**, 5272–5283, (2009).
- [21] D. S. Kubert, S. Lang, Independence of modular units on Tate curves, *Math. Ann.* **240**, 191–201, (1979).
- [22] P. Langevin, Calculs de Certaines Sommes de Gauss, *J. Number Theory* **32**, 59–64, (1997).
- [23] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.
- [24] R. J. McEliece, Irreducible cyclic codes and Gauss sums, *Math. Centre Tracts.* **55**, 179–196, (1974).
- [25] O. D. Mbodj, Quadratic Gauss sums *Finite Fields Appl.* **4**, 347–361, (1998).
- [26] P. Meijer, M. Van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J. Number Theory* **100**, 381–395, (2003).

- [27] K. Momihara, Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime, *Electron. J. Combin.* **20**, # P35, (2013).
- [28] K. Momihara, A recursive construction for skew Hadamard difference sets, *Electron. J. Combin.* **27**, # P3.36, (2020) (Corrigendum added).
- [29] K. Momihara, Q. Wang, Q. Xiang, Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures, in: K.-U. Schmidt, A. Winterhof (Eds.), *Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications*, 178–205 Radon Series on Computation and Applied Mathematics, **23**, De Gruyter (2019).
- [30] K.-U. Schmidt, Highly nonlinear functions over finite fields, *Finite Fields Appl.* **63**, 101640, (2020).
- [31] L. Xia, J. Yang, Sign or root of unity ambiguities of certain Gauss sums, and 4 cases, *Front. Math. China* **7**, 743–764, (2012).
- [32] J. Yang, S. Luo, K. Feng, Gauss sum of index 4. II. Non-cyclic case. *Acta Math. Sin. (Engl. Ser.)* **22**, 833–844, (2006).
- [33] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci China Math.* **53**, 2525–2542, (2010).

Appendix

In this appendix, we list all $(N, \bar{p}) \in \mathcal{P}_f^*$ for $N \leq 5000$ and odd f in Tables 1 and 2.

TABLE 1. $(N, \bar{p}) \in \mathcal{P}_f^*$ for $N \leq 5000$ and odd f

| $[N, f, \bar{p}]$ | Ref. | $[N, f, \bar{p}]$ | Ref. | $[N, f, \bar{p}]$ | Ref. |
|-------------------|---------------------|-------------------|---------------------|-------------------|---------------------|
| [14, 3, 9] | Prop. 3.10 | [826, 87, 9] | Prop. 3.12 (2) | [1762, 55, 21] | $\mathcal{P}^{(2)}$ |
| [42, 3, 25] | Prop. 3.12 (2) | [862, 43, 3] | $\mathcal{P}^{(2)}$ | [1774, 443, 3] | Prop. 3.10 |
| [46, 11, 3] | Prop. 3.10 | [862, 215, 5] | Prop. 3.10 | [1778, 21, 135] | $\mathcal{P}^{(2)}$ |
| [62, 15, 7] | Prop. 3.10 | [874, 99, 9] | Prop. 3.12 (2) | [1786, 207, 9] | Prop. 3.12 (2) |
| [62, 5, 33] | Prop. 3.11 | [878, 219, 5] | Prop. 3.10 | [1822, 455, 3] | Prop. 3.10 |
| [78, 3, 55] | Prop. 3.13 (2) | [878, 73, 7] | Prop. 3.11 | [1822, 91, 15] | $\mathcal{P}^{(2)}$ |
| [94, 23, 3] | Prop. 3.10 | [906, 75, 25] | Prop. 3.12 (2) | [1834, 195, 9] | Prop. 3.12 (2) |
| [98, 21, 9] | Prop. 3.10 | [926, 231, 9] | Prop. 3.10 | [1838, 459, 5] | Prop. 3.10 |
| [110, 5, 31] | Prop. 3.13 (2) | [958, 239, 3] | Prop. 3.10 | [1838, 153, 9] | Prop. 3.11 |
| [142, 35, 3] | Prop. 3.10 | [974, 243, 9] | Prop. 3.10 | [1874, 117, 9] | Prop. 3.13 (1) |
| [146, 9, 37] | Prop. 3.13 (1) | [994, 105, 9] | Prop. 3.12 (1) | [1922, 465, 7] | Prop. 3.10 |
| [158, 39, 5] | Prop. 3.10 | [1006, 251, 3] | Prop. 3.10 | [1922, 155, 33] | Prop. 3.11 |
| [178, 11, 39] | Prop. 3.13 (1) | [1014, 39, 55] | Prop. 3.13 (2) | [1934, 483, 21] | Prop. 3.10 |
| [186, 15, 7] | Prop. 3.12 (2) | [1022, 9, 513] | $\mathcal{P}^{(2)}$ | [1966, 491, 3] | Prop. 3.10 |
| [206, 51, 7] | Prop. 3.10 | [1034, 115, 3] | Prop. 3.12 (2) | [1978, 231, 9] | Prop. 3.12 (2) |
| [254, 63, 9] | Prop. 3.10 | [1058, 253, 3] | Prop. 3.10 | [1982, 495, 5] | Prop. 3.10 |
| [254, 21, 25] | Prop. 3.11 | [1086, 45, 13] | Prop. 3.13 (2) | [2058, 147, 25] | Prop. 3.12 (2) |
| [254, 7, 129] | $\mathcal{P}^{(2)}$ | [1106, 39, 11] | $\mathcal{P}^{(2)}$ | [2062, 515, 3] | Prop. 3.10 |
| [294, 21, 25] | Prop. 3.12 (2) | [1162, 123, 9] | Prop. 3.12 (2) | [2078, 519, 7] | Prop. 3.10 |
| [302, 75, 5] | Prop. 3.10 | [1194, 99, 7] | Prop. 3.12 (2) | [2110, 105, 51] | Prop. 3.13 (2) |
| [302, 15, 85] | $\mathcal{P}^{(2)}$ | [1198, 299, 3] | Prop. 3.10 | [2114, 75, 25] | $\mathcal{P}^{(2)}$ |
| [322, 33, 9] | Prop. 3.12 i) | [1202, 75, 3] | Prop. 3.13 (1) | [2114, 15, 529] | $\mathcal{P}^{(2)}$ |
| [334, 83, 3] | Prop. 3.10 | [1202, 25, 27] | $\mathcal{P}^{(2)}$ | [2126, 531, 9] | Prop. 3.10 |
| [382, 95, 3] | Prop. 3.10 | [1210, 55, 31] | Prop. 3.13 (2) | [2162, 253, 3] | Prop. 3.12 (1) |
| [398, 99, 7] | Prop. 3.10 | [1214, 303, 9] | Prop. 3.10 | [2174, 543, 9] | Prop. 3.10 |
| [434, 15, 39] | $\mathcal{P}^{(2)}$ | [1246, 33, 39] | $\mathcal{P}^{(2)}$ | [2202, 183, 13] | Prop. 3.12 (2) |
| [446, 37, 7] | Prop. 3.11 | [1262, 315, 9] | Prop. 3.10 | [2206, 551, 3] | Prop. 3.10 |
| [446, 111, 9] | Prop. 3.10 | [1262, 45, 47] | $\mathcal{P}^{(2)}$ | [2206, 29, 69] | $\mathcal{P}^{(2)}$ |
| [462, 15, 25] | Prop. 3.13 (3)-iii) | [1294, 323, 3] | Prop. 3.10 | [2254, 231, 9] | Prop. 3.12 (1) |
| [466, 29, 19] | Prop. 3.13 (1) | [1310, 65, 11] | Prop. 3.13 (2) | [2266, 255, 15] | Prop. 3.12 (2) |
| [474, 39, 13] | Prop. 3.12 (2) | [1338, 111, 19] | Prop. 3.12 (2) | [2302, 575, 3] | Prop. 3.10 |
| [478, 119, 3] | Prop. 3.10 | [1374, 57, 19] | Prop. 3.13 (2) | [2338, 249, 9] | Prop. 3.12 (1) |
| [506, 55, 3] | Prop. 3.12 (2) | [1426, 165, 9] | Prop. 3.12 (1) | [2446, 611, 7] | Prop. 3.10 |
| [526, 131, 3] | Prop. 3.10 | [1426, 55, 35] | $\mathcal{P}^{(2)}$ | [2462, 615, 5] | Prop. 3.10 |
| [542, 135, 7] | Prop. 3.10 | [1438, 359, 3] | Prop. 3.10 | [2478, 87, 25] | Prop. 3.13 (3)-ii) |
| [618, 51, 7] | Prop. 3.12 (2) | [1442, 51, 121] | $\mathcal{P}^{(2)}$ | [2510, 125, 21] | Prop. 3.13 (2) |
| [622, 155, 3] | Prop. 3.10 | [1454, 363, 7] | Prop. 3.10 | [2526, 105, 25] | Prop. 3.13 (2) |
| [654, 27, 7] | Prop. 3.13 (2) | [1454, 121, 9] | Prop. 3.11 | [2558, 639, 5] | Prop. 3.10 |
| [658, 69, 9] | Prop. 3.12 (1) | [1486, 371, 3] | Prop. 3.10 | [2578, 161, 29] | Prop. 3.13 (1) |
| [674, 21, 13] | $\mathcal{P}^{(2)}$ | [1502, 375, 5] | Prop. 3.10 | [2606, 651, 23] | Prop. 3.10 |
| [686, 147, 9] | Prop. 3.10 | [1626, 135, 7] | Prop. 3.12 (2) | [2622, 99, 25] | Prop. 3.13 (3)-iii) |
| [718, 179, 3] | Prop. 3.10 | [1646, 411, 9] | Prop. 3.10 | [2634, 219, 13] | Prop. 3.12 (2) |
| [734, 183, 13] | Prop. 3.10 | [1662, 69, 49] | Prop. 3.13 (2) | [2638, 659, 9] | Prop. 3.10 |
| [762, 63, 13] | Prop. 3.12 (2) | [1678, 419, 3] | Prop. 3.10 | [2654, 663, 9] | Prop. 3.10 |
| [766, 191, 3] | Prop. 3.10 | [1726, 431, 3] | Prop. 3.10 | [2654, 221, 43] | Prop. 3.11 |

TABLE 2. $(N, \bar{p}) \in \mathcal{P}_f^*$ for $N \leq 5000$ and odd f

| $[N, f, \bar{p}]$ | Ref. | $[N, f, \bar{p}]$ | Ref. | $[N, f, \bar{p}]$ | Ref. |
|-------------------|---------------------|-------------------|---------------------|-------------------|---------------------|
| [2674, 285, 9] | Prop. 3.12 (2) | [3454, 195, 9] | Prop. 3.13 (2) | [4286, 153, 121] | $\mathcal{P}^{(2)}$ |
| [2734, 683, 3] | Prop. 3.10 | [3486, 123, 25] | Prop. 3.13 (3)-ii) | [4354, 465, 9] | Prop. 3.12 (1) |
| [2778, 231, 25] | Prop. 3.12 (2) | [3514, 375, 9] | Prop. 3.12 (2) | [4362, 363, 7] | Prop. 3.12 (2) |
| [2782, 159, 3] | Prop. 3.13 (2) | [3518, 879, 11] | Prop. 3.10 | [4378, 495, 9] | Prop. 3.12 (2) |
| [2786, 99, 23] | $\mathcal{P}^{(2)}$ | [3566, 891, 7] | Prop. 3.10 | [4398, 183, 31] | Prop. 3.13 (2) |
| [2798, 699, 5] | Prop. 3.10 | [3602, 225, 9] | Prop. 3.13 (1) | [4402, 105, 19] | $\mathcal{P}^{(2)}$ |
| [2798, 233, 9] | Prop. 3.11 | [3602, 75, 21] | $\mathcal{P}^{(2)}$ | [4402, 35, 225] | $\mathcal{P}^{(2)}$ |
| [2846, 711, 9] | Prop. 3.10 | [3602, 25, 175] | $\mathcal{P}^{(2)}$ | [4414, 1103, 3] | Prop. 3.10 |
| [2846, 237, 23] | Prop. 3.11 | [3634, 429, 9] | Prop. 3.12 (1) | [4418, 1081, 3] | Prop. 3.10 |
| [2866, 179, 15] | Prop. 3.13 (1) | [3642, 303, 13] | Prop. 3.12 (2) | [4478, 1119, 9] | Prop. 3.10 |
| [2878, 719, 3] | Prop. 3.10 | [3646, 911, 3] | Prop. 3.10 | [4494, 159, 25] | Prop. 3.13 (3)-iii) |
| [2894, 723, 9] | Prop. 3.10 | [3662, 305, 5] | Prop. 3.11 | [4506, 375, 13] | Prop. 3.12 (2) |
| [2914, 345, 7] | Prop. 3.12 (1) | [3662, 915, 9] | Prop. 3.10 | [4526, 45, 221] | $\mathcal{P}^{(2)}$ |
| [2914, 115, 97] | $\mathcal{P}^{(2)}$ | [3682, 393, 9] | Prop. 3.12 (1) | [4542, 189, 7] | Prop. 3.13 (2) |
| [2922, 243, 31] | Prop. 3.12 (2) | [3694, 923, 3] | Prop. 3.10 | [4574, 1143, 7] | Prop. 3.10 |
| [2942, 735, 5] | Prop. 3.10 | [3742, 935, 5] | Prop. 3.10 | [4574, 381, 9] | Prop. 3.11 |
| [2942, 245, 19] | Prop. 3.11 | [3758, 939, 5] | Prop. 3.10 | [4606, 483, 9] | Prop. 3.12 (1) |
| [2974, 743, 3] | Prop. 3.10 | [3786, 315, 31] | Prop. 3.12 (2) | [4622, 1155, 9] | Prop. 3.10 |
| [3022, 755, 5] | Prop. 3.10 | [3794, 135, 37] | $\mathcal{P}^{(2)}$ | [4702, 1175, 3] | Prop. 3.10 |
| [3038, 105, 39] | Prop. 3.12 (1) | [3818, 451, 3] | Prop. 3.12 (2) | [4702, 235, 11] | $\mathcal{P}^{(2)}$ |
| [3086, 771, 13] | Prop. 3.10 | [3826, 239, 17] | Prop. 3.13 (1) | [4702, 47, 15] | $\mathcal{P}^{(2)}$ |
| [3118, 779, 3] | Prop. 3.10 | [3838, 225, 5] | Prop. 3.13 (2) | [4718, 21, 1115] | $\mathcal{P}^{(2)}$ |
| [3122, 111, 289] | $\mathcal{P}^{(2)}$ | [3902, 975, 5] | Prop. 3.10 | [4738, 561, 25] | Prop. 3.12 (1) |
| [3134, 783, 7] | Prop. 3.10 | [3998, 999, 5] | Prop. 3.10 | [4766, 397, 7] | Prop. 3.11 |
| [3166, 791, 11] | Prop. 3.10 | [3998, 333, 13] | Prop. 3.11 | [4766, 1191, 13] | Prop. 3.10 |
| [3178, 339, 9] | Prop. 3.12 (2) | [4042, 483, 9] | Prop. 3.12 (2) | [4798, 1199, 3] | Prop. 3.10 |
| [3214, 803, 3] | Prop. 3.10 | [4042, 161, 21] | Exception | [4802, 1029, 9] | Prop. 3.10 |
| [3218, 201, 11] | Prop. 3.13 (1) | [4078, 1019, 3] | Prop. 3.10 | [4814, 287, 7] | Prop. 3.13 (2) |
| [3234, 105, 25] | Prop. 3.13 (3)-iii) | [4094, 11, 2049] | $\mathcal{P}^{(2)}$ | [4846, 1211, 3] | Prop. 3.10 |
| [3246, 135, 25] | Prop. 3.13 (2) | [4126, 1031, 3] | Prop. 3.10 | [4882, 305, 5] | Prop. 3.13 (1) |
| [3262, 87, 23] | $\mathcal{P}^{(2)}$ | [4174, 1043, 3] | Prop. 3.10 | [4894, 1223, 3] | Prop. 3.10 |
| [3266, 385, 3] | Prop. 3.12 (1) | [4178, 261, 15] | Prop. 3.13 (1) | [4898, 195, 95] | $\mathcal{P}^{(2)}$ |
| [3310, 165, 21] | Prop. 3.13 (2) | [4178, 87, 85] | $\mathcal{P}^{(2)}$ | [4906, 555, 9] | Prop. 3.12 (2) |
| [3326, 831, 9] | Prop. 3.10 | [4178, 29, 457] | $\mathcal{P}^{(2)}$ | [4910, 245, 11] | Prop. 3.13 (2) |
| [3346, 357, 9] | Prop. 3.12 (1) | [4222, 1055, 5] | Prop. 3.10 | [4922, 583, 3] | Prop. 3.12 (2) |
| [3358, 99, 55] | $\mathcal{P}^{(2)}$ | [4254, 177, 7] | Prop. 3.13 (2) | [4938, 411, 13] | Prop. 3.12 (2) |
| [3406, 195, 3] | Prop. 3.13 (2) | [4286, 1071, 9] | Prop. 3.10 | [4974, 207, 55] | Prop. 3.13 (2) |
| [3422, 203, 7] | Prop. 3.13 (2) | [4286, 357, 15] | Prop. 3.11 | | |
| [3442, 215, 17] | Prop. 3.13 (1) | [4286, 51, 67] | $\mathcal{P}^{(2)}$ | | |

DIVISION OF NATURAL SCIENCE, FACULTY OF ADVANCED SCIENCE AND TECHNOLOGY, KUMAMOTO UNIVERSITY, 2-40-1 KUROKAMI, KUMAMOTO 860-8555, JAPAN

Email address: momihara@educ.kumamoto-u.ac.jp