J Algebr Comb
DOI 10.1007/s10801-016-0664-z

Three-valued Gauss periods, circulant weighing matrices and association schemes

Tao Feng[1] · **Koji Momihara**[2] · **Qing Xiang**[3]

Received: 29 September 2014 / Accepted: 8 January 2016

Abstract Gauss periods taking exactly two values are closely related to two-weight irreducible cyclic codes and strongly regular Cayley graphs. They have been extensively studied in the work of Schmidt and White and others. In this paper, we consider the question of when Gauss periods take exactly three rational values. We obtain numerical necessary conditions for Gauss periods to take exactly three rational values. We show that in certain cases, the necessary conditions obtained are also sufficient. We give numerous examples where the Gauss periods take exactly three values. Furthermore, we discuss connections between three-valued Gauss periods and combinatorial structures such as circulant weighing matrices and three-class association schemes.

Dedicated to Chris Godsil, on the occasion of his 65th birthday

T. Feng research supported in part by the Fundamental Research Funds for Central Universities of China and the National Natural Science Foundation of China under Grant 11422112. K. Momihara research supported by JSPS under Grant-in-Aid for Young Scientists (B) 25800093 and Scientific Research (C) 24540013.

✉ Qing Xiang
qxiang@udel.edu

Tao Feng
tfeng@zju.edu.cn

Koji Momihara
momihara@educ.kumamoto-u.ac.jp

[1] Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, People's Republic of China

[2] Faculty of Education, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan

[3] Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

Published online: 20 January 2016

Keywords Association scheme · Circulant weighing matrix · Cyclotomy · Gauss period · Gauss sum

1 Introduction

Let $\mathbb{F}_q$ be the finite field of order q, where q is a power of a prime p. Let ξ_p be a complex primitive pth root of unity and $\mathrm{Tr}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$. Define

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \qquad \psi(x) = \xi_p^{\mathrm{Tr}_{q/p}(x)},$$

which is easily seen to be a nontrivial character of $(\mathbb{F}_q, +)$, the additive group of $\mathbb{F}_q$. Let $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ be a multiplicative character of $\mathbb{F}_q$. Define the *Gauss sum* by

$$G_q(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi(a).$$

Gauss sums are ubiquitous in number theory and in many areas of combinatorics. Closely related to Gauss sums are the Gauss periods which we define below. As before, q is a power of a prime p. Let $N > 1$ be an integer such that $N|(q-1)$ and γ a primitive element of $\mathbb{F}_q$. Then the cosets $C_a^{(N,\mathbb{F}_q)} = \gamma^a\langle\gamma^N\rangle$, $0 \le a \le N-1$, of $\langle\gamma^N\rangle$ in $\mathbb{F}_q^*$ are called the *cyclotomic classes of order* N of $\mathbb{F}_q$. We often write $C_a^{(N,q)}$ or simply C_a for $C_a^{(N,\mathbb{F}_q)}$, if there is no confusion. The corresponding *Gauss periods* are defined by

$$\eta_a = \sum_{x \in C_a^{(N,q)}} \psi(x), \quad 0 \le a \le N-1.$$

Even though Gauss sums and Gauss periods were first introduced by Gauss to study cyclotomy ("circle-splitting"), they have played an important role in the investigations of many combinatorial objects, such as difference sets, irreducible cyclic codes, and strongly regular Cayley graphs, cf. [4,6,7,9,11,13]. In particular, we note that Gauss sums were used extensively in the work of Baumert and McEliece ([1,11]) on weights of irreducible cyclic codes. The current paper can be thought as a natural continuation of [13] in which two-weight irreducible cyclic codes were studied by using Gauss sums. The Gauss periods involved in [13] take two distinct rational values as they correspond to the (nonzero) weights of two-weight irreducible cyclic codes. In this paper, we consider Gauss periods which take three distinct rational values, and use them to construct various combinatorial objects such as circulant weighing matrices and association schemes.

A *circulant weighing matrix of order N* is a square matrix M of the form

$$M = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} \tag{1.1}$$

with $a_i \in \{-1, 0, 1\}$ for all i and $MM^\top = wI$, where w is a positive integer and I is the identity matrix of order N. The integer w is called the *weight* of the weighing matrix. A circulant weighing matrix of order N and weight w will be denoted by $\mathbf{CW}(N, w)$.

Let G be an abelian group of order N. To facilitate the study of circulant weighing matrices, we use the group ring language. The elements of $\mathbb{C}[G]$ are

$$A = \sum_{g \in G} a_g g,$$

with $a_g \in \mathbb{C}$; for any integer t, we write

$$A^{(t)} := \sum_{g \in G} a_g g^t.$$

For a subset A of G, it is customary to identify A with the corresponding group ring element $\sum_{g \in A} g$, which will again be denoted by A. We will be using the Fourier inversion formula quite frequently.

Lemma 1.1 (Inversion formula) *Let G be an abelian group of order N and $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then*

$$a_g = \frac{1}{N} \sum_{\chi \in \widehat{G}} \chi(A)\chi(g^{-1})$$

for all $g \in G$, where $\widehat{G}$ is the group of complex characters of G. Hence if $A, B \in \mathbb{C}[G]$ satisfy $\chi(A) = \chi(B)$ for all $\chi \in \hat{G}$, then $A = B$.

Now set $G = Z_N$, a cyclic group of order N with a generator $\overline{\gamma}$. That is, $Z_N = \{1, \overline{\gamma}, \ldots, \overline{\gamma}^{N-1}\}$. A circulant matrix M in (1.1) satisfies $MM^\top = wI$ if and only if $DD^{(-1)} = w$, where D is the group ring element in $\mathbb{C}[Z_N]$ defined by $D = \sum_{i=0}^{N-1} a_i \overline{\gamma}^i$. Since $a_i = 0, \pm 1$, we can write $D = A - B$, where $A = \{\overline{\gamma}^i \mid 0 \le i \le N-1, a_i = 1\}$ and $B = \{\overline{\gamma}^i \mid 0 \le i \le N-1, a_i = -1\}$. Thus, a circulant weighing matrix of order N and weight w is equivalent to a group ring element $A - B$, where A and B are disjoint subsets of Z_N, such that

$$(A - B)(A - B)^{(-1)} = w \cdot 1 \text{ in } \mathbb{C}[Z_N].$$

Next we give a short introduction to association schemes. Let X be a finite set. A (symmetric) *association scheme* with d classes on X is a partition of $X \times X$ into subsets $R_0, R_1, \ldots, R_d$ (called *associate classes* or *relations*) such that

(1) $R_0 = \{(x, x) \mid x \in X\}$ (the diagonal relation),
(2) R_i is symmetric for $i = 1, 2, \ldots, d$,
(3) for all i, j, k in $\{0, 1, 2, \ldots, d\}$ there is an integer p_{ij}^k such that, for all $(x, y) \in R_k$,

$$|\{z \in X \mid (x, z) \in R_i \text{ and } (z, y) \in R_j\}| = p_{ij}^k.$$

We denote such an association scheme by $(X, \{R_i\}_{0 \le i \le d})$. For $i \in \{0, 1, \ldots, d\}$, let A_i be the adjacency matrix of the relation R_i, that is, the rows and columns of A_i are both indexed by X and

$$(A_i)_{xy} := \begin{cases} 1 & \text{if } (x, y) \in R_i, \\ 0 & \text{if } (x, y) \notin R_i. \end{cases}$$

The matrices A_i are symmetric $(0, 1)$-matrices and

$$A_0 = I, \ A_0 + A_1 + \cdots + A_d = J,$$

where J is the all-1 matrix of size $|X|$ by $|X|$.

By the definition of an association scheme, we have $A_i A_j = \sum_{k=0}^d p_{ij}^k A_k$ for any $i, j \in \{0, 1, \ldots, d\}$, so $A_0, A_1, \ldots, A_d$ form a basis of the commutative algebra generated by $A_0, A_1, \ldots, A_d$ over the reals, which is called the *Bose–Mesner algebra* of the association scheme. Moreover, this algebra has a unique basis $E_0, E_1, \ldots, E_d$ of primitive idempotents; one of the primitive idempotents is $\frac{1}{|X|} J$. We may assume that $E_0 = \frac{1}{|X|} J$. Let $m_i = \text{rank } E_i$. Then

$$m_0 = 1, \quad m_0 + m_1 + \cdots + m_d = |X|.$$

The numbers $m_0, m_1, \ldots, m_d$ are called the *multiplicities* of the scheme. Since we have two bases of the Bose–Mesner algebra, we consider the transition matrices between them. Define $P = \big(p_j(i)\big)_{0 \le i, j \le d}$ (the *first eigenmatrix or character table*) and $Q = \big(q_j(i)\big)_{0 \le i, j \le d}$ (the *second eigenmatrix*) as the $(d + 1) \times (d + 1)$ matrices with rows and columns indexed by $0, 1, 2, \ldots, d$ such that

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d)P,$$

and

$$|X|(E_0, E_1, \ldots, E_d) = (A_0, A_1, \ldots, A_d)Q.$$

Let $k_j = p_j(0)$, $0 \le j \le d$. The k_j's are called *valencies* of the scheme.

We call an association scheme $(X, \{R_i\}_{i=0}^d)$, where X is an additively written finite abelian group, a *translation association scheme* or a *Schur ring* if there is a partition $D_0 = \{0\}, D_1, \ldots, D_d$ of X such that for each $i = 0, 1, \ldots, d$,

$$R_i = \{(x, x + y) \mid x \in X, y \in D_i\}. \tag{1.2}$$

Assume that $(X, \{R_i\}_{0 \le i \le d})$ is a translation association scheme with relations defined in (1.2). There is an equivalence relation defined on the character group $\widehat{X}$ of X as

follows: $\chi \sim \chi'$ if and only if $\chi(D_i) = \chi'(D_i)$ for all $0 \le i \le d$. Here $\chi(D) = \sum_{g \in D} \chi(g)$, for any $\chi \in \widehat{X}$ and $D \subseteq X$. Denote by $D'_0, D'_1, \ldots, D'_d$ the equivalence classes, with D'_0 consisting of only the principal character. Define

$$R'_i = \{(\chi, \chi\chi') | \chi \in \widehat{X}, \chi' \in D'_i\}.$$

Then, $(\widehat{X}, \{R'_i\}_{i=0}^d)$ also forms a translation association scheme, called the *dual* of $(X, \{R_i\}_{0 \le i \le d})$. The first eigenmatrix of the dual scheme is equal to the second eigenmatrix of the original scheme. We refer the reader to [3, p. 68] for more details. A translation scheme is called *self-dual* if it is isomorphic to its dual.

As an example of translation association schemes, we mention the cyclotomic scheme, which we define below. Let q be a prime power, $N > 1$ be a divisor of $q - 1$. Let $C_a, 0 \le a \le N - 1$, be the cyclotomic classes of order N of $\mathbb{F}_q$. Assume that $-1 \in C_0$. Define $R_0 = \{(x, x) \mid x \in \mathbb{F}_q\}$, and for $a \in \{1, 2, \ldots, N\}$, define $R_a = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in C_{a-1}\}$. Then $(\mathbb{F}_q, \{R_a\}_{0 \le a \le N})$ is an association scheme. This is the so-called *cyclotomic association scheme of class N over* $\mathbb{F}_q$. The first eigenmatrix P of the cyclotomic scheme of class N is given by the following $(N + 1)$ by $(N + 1)$ matrix (with the rows of P arranged in a certain way)

$$P = \begin{pmatrix} 1 & k & k & k & \cdots & k \\ 1 & \eta_{N-1} & \eta_0 & \eta_1 & \cdots & \eta_{N-2} \\ 1 & \eta_{N-2} & \eta_{N-1} & \eta_0 & \cdots & \eta_{N-3} \\ \vdots & & & & & \\ 1 & \eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{N-1} \end{pmatrix} \tag{1.3}$$

where $k = \frac{q-1}{N}$ and $\eta_a, 0 \le a \le N - 1$, are the Gauss periods of order N defined above. For future use, the submatrix $P_0 = (p_j(i))_{1 \le i,j \le N}$ of P will be called *the principal part* of P. Note that the cyclotomic scheme $(\mathbb{F}_q, \{R_a\}_{0 \le a \le N})$ is self-dual.

The rest of the paper is organized as follows. In Sect. 2, we obtain necessary conditions for Gauss periods to take exactly three rational values. Connections between three-valued Gauss sums and combinatorial structures such as circulant weighing matrices and three-class association schemes are also developed. In Sect. 3, we show that in certain cases, the necessary conditions we obtained in Sect. 2 are also sufficient. Finally in Sect. 4, we provide five infinite classes of examples where the Gauss periods take exactly three values. Some sporadic examples are also obtained by computer search. From these examples, we obtain circulant weighing matrices and three-class self-dual association schemes.

2 Three-valued Gauss periods: necessary conditions

Let $q = p^f$ be a prime power and $N > 2$ be a positive integer such that $N \mid (q-1)$. Set $k = (q-1)/N$. Let $\mathbb{F}_q$ be the finite field of order q, γ a fixed primitive element of $\mathbb{F}_q$, and $C_0 = \langle \gamma^N \rangle$. Suppose that the Gauss periods $\eta_a = \psi(\gamma^a C_0), a = 0, 1, \ldots, N-1$, take exactly three distinct rational values α_1, α_2, and α_3. We will be working with the quotient group $Z_N := \mathbb{F}_q^*/C_0$, a cyclic group of order N with a generator $\overline{\gamma} = \gamma C_0$. For $1 \le i \le 3$, define subsets I_i of Z_N by $I_i = \{\overline{\gamma}^a \in Z_N \mid \eta_a = \alpha_i\}$.

Lemma 2.1 *With the above assumptions and notation, we have*

$$(\alpha_1 I_1 + \alpha_2 I_2 + \alpha_3 I_3)(\alpha_1 I_1^{(-1)} + \alpha_2 I_2^{(-1)} + \alpha_3 I_3^{(-1)}) = q \cdot 1 - \frac{q-1}{N} Z_N, \quad (2.1)$$

in the group ring $\mathbb{Q}[Z_N]$.

Proof As above, Z_N is the (cyclic) quotient group $\mathbb{F}_q^*/C_0$ with a generator $\overline{\gamma}$. Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$ whose restriction to C_0 is trivial, so that we may view χ as a character of the quotient group $\mathbb{F}_q^*/C_0$. Such a character of $\mathbb{F}_q^*/C_0$ will again be denoted by χ and we have $\chi(\overline{\gamma}) = \chi(\gamma)$. Note that every nontrivial character of $Z_N := \mathbb{F}_q^*/C_0$ can be obtained in this manner. We have

$$\begin{aligned} G_q(\chi) &= \sum_{i=0}^{N-1} \sum_{x \in C_i} \chi(x)\psi(x) \\ &= \eta_0 + \chi(\gamma)\eta_1 + \cdots + \chi(\gamma^{N-1})\eta_{N-1} \\ &= \alpha_1 \chi(I_1) + \alpha_2 \chi(I_2) + \alpha_3 \chi(I_3). \end{aligned}$$

Since α_i, $1 \le i \le 3$, are rational integers, we have $\overline{\alpha}_i = \alpha_i$ for $1 \le i \le 3$. It follows that

$$\left(\sum_{i=1}^{3} \alpha_i \chi(I_i)\right)\left(\sum_{i=1}^{3} \alpha_i \overline{\chi(I_i)}\right) = G_q(\chi)\overline{G_q(\chi)} = q.$$

If χ is the trivial multiplicative character of $\mathbb{F}_q$, we have $\alpha_1\chi(I_1) + \alpha_2\chi(I_2) + \alpha_3\chi(I_3) = G_q(\chi) = -1$, and

$$\left(\sum_{i=1}^{3} \alpha_i \chi(I_i)\right)\left(\sum_{i=1}^{3} \alpha_i \overline{\chi(I_i)}\right) = G_q(\chi)\overline{G_q(\chi)} = 1.$$

The claimed group ring equation now follows from the inversion formula stated in Lemma 1.1. □

Using Lemma 2.1, we can express the sizes of I_i's in terms of $\alpha_1, \alpha_2, \alpha_3$.

Lemma 2.2 *Suppose that* η_a, $0 \le a \le N-1$, *take three distinct rational values* α_1, α_2, *and* α_3. *With notation as above and* $k = \frac{q-1}{N}$, *we have*

$$\begin{aligned} |I_1| &= -\frac{\alpha_2\alpha_3(q-1) + k(q-k+\alpha_2+\alpha_3)}{k(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)}, \\ |I_2| &= -\frac{\alpha_1\alpha_3(q-1) + k(q-k+\alpha_1+\alpha_3)}{k(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)}, \\ |I_3| &= -\frac{\alpha_1\alpha_2(q-1) + k(q-k+\alpha_1+\alpha_2)}{k(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)}. \end{aligned}$$

Proof First of all, it is clear that $|I_1|+|I_2|+|I_3| = N$. Next we have $\alpha_1|I_1|+\alpha_2|I_2|+\alpha_3|I_3| = \sum_{i=0}^{N-1}\eta_i = -1$. Finally, by comparing the coefficient of the identity element in the two sides of the group ring equation (2.1), we get $\alpha_1^2|I_1| + \alpha_2^2|I_2| + \alpha_3^2|I_3| = q-k$. These three equations now uniquely determine $|I_1|$, $|I_2|$, and $|I_3|$. The proof is complete. □

Next we derive necessary conditions when the Gauss periods take exactly three values.

Proposition 2.3 *Let $q = p^f$ be a prime power and $N > 2$ be a positive integer such that $N \mid (q-1)$. Assume that the Gauss periods η_a, $0 \le a \le N-1$, take exactly three rational values $\alpha_1, \alpha_2, \alpha_3$, say, $\alpha_1 - \alpha_2 = -tu < 0$ and $\alpha_3 - \alpha_2 = tv > 0$ with $t > 0$ and $\gcd(u, v) = 1$. Then t is a power of p, and there exist two positive integers r, s, $0 < r, s < N$, such that*

(i) $t(-ur + vs) \equiv -1 \pmod N$;
(ii) $(N-1)q + t^2(-ur+vs)^2 = Nt^2(u^2r + v^2s)$.

In particular, t is the largest power of p dividing $G_q(\chi)$ for all nontrivial multiplicative character χ of $\mathbb{F}_q$ of order dividing N.

Proof As before, let $Z_N = \mathbb{F}_q^*/C_0 = \langle\overline{\gamma}\rangle$. So $\widehat{Z}_N = C_0^\perp := \{\chi \mid \chi \in \widehat{\mathbb{F}}_q^*,\ \chi|_{C_0} = 1\}$. We define a function $\sigma : Z_N \to \mathbb{C}$ by $\sigma(\overline{\gamma}^a) = \eta_a - \alpha_2$. In order to simplify notation, we will sometimes write $\sigma(\overline{\gamma}^a)$ simply as $\sigma(a)$. The Fourier transform of σ is $\widehat{\sigma} : \widehat{Z}_N \to \mathbb{C}$, which is defined by

$$\widehat{\sigma}(\chi) = \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} \sigma(\overline{\gamma}^a)\chi(\overline{\gamma}^a).$$

Computing the Fourier transform of σ, we have

$$\widehat{\sigma}(\chi) = \begin{cases} \frac{1}{\sqrt{N}} G_q(\chi) & \text{if } \chi \text{ is a nontrivial character of } Z_N, \\ -\frac{1}{\sqrt{N}} - \alpha_2\sqrt{N} & \text{if } \chi \text{ is trivial.} \end{cases}$$

By assumption η_a, $0 \le a \le N-1$, take exactly three values, we see that $\sigma(a) \in \{0, -tu, tv\}$. Note that if $\chi \in \widehat{Z}_N$ is nontrivial, then

$$G_q(\chi) = \sum_{a=0}^{N-1} \eta_a\chi(\gamma^a) = \sum_{a=0}^{N-1} (\eta_a - \alpha_2)\chi(\gamma^a) = t(-u\chi(I_1) + v\chi(I_3)),$$

where I_1 and I_3 are defined as before. From the above equation, we see that $t \mid G_q(\chi)$ for all nontrivial $\chi \in C_0^\perp$. It follows that $t = p^\theta$ for some integer θ.

Let $(C_0^\perp)^* := C_0^\perp \backslash \{\chi_0\}$ with χ_0 the trivial character. Since for any a, $0 \le a \le N-1$,

$$\eta_a = \frac{1}{N} \sum_{\chi \in C_0^\perp} G_q(\chi)\chi^{-1}(\gamma^a),$$

we have

$$\sigma(\overline{\gamma}^a) = \frac{1}{N} \sum_{\chi \in (C_0^{\perp})^*} G_q(\chi)(\chi^{-1}(\gamma^a) - \chi^{-1}(\gamma^e)), \tag{2.2}$$

where χ^{-1} is the inverse of $\chi \in C_0^{\perp}$ and α_2 is assumed to be equal to η_e for some e. Let t' be the largest power of p dividing all $G_q(\chi)$, $\chi \in (C_0^{\perp})^*$. Then (2.2) implies that $t = t'$ since $\gcd(N, t') = 1$.

Moreover, by the definition of $\widehat{\sigma}$ we have

$$\widehat{\sigma}(\chi_0) = \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} \sigma(\overline{\gamma}^a) = \frac{t(-ur + vs)}{\sqrt{N}},$$

where $r = |I_1|$, $s = |I_3|$, and $0 < r, s < N$. Hence $-\frac{1}{\sqrt{N}} - \frac{N}{\sqrt{N}}\alpha_2 = \frac{t(-ur+vs)}{\sqrt{N}}$. It follows that $t(-ur + vs) \equiv -1 \pmod{N}$.

It is clear from the definition of σ that $\sum_{a=0}^{N-1} \sigma(a)\overline{\sigma(a)} = t^2(u^2r + v^2s)$. On the other hand, we have

$$\begin{aligned} \sum_{\chi \in C_0^{\perp}} \widehat{\sigma}(\chi)\overline{\widehat{\sigma}(\chi)} &= \frac{1}{N} \sum_{\chi \in (C_0^{\perp})^*} G_q(\chi)\overline{G_q(\chi)} + \frac{t^2(-ur + vs)^2}{N} \\ &= \frac{1}{N}((N-1)q + t^2(-ur + vs)^2). \end{aligned}$$

It now follows from Parseval's identity that

$$(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2r + v^2s).$$

The proof is now complete. □

Remark 2.4 (1) As seen from the proof above, t is the largest power of p dividing all $G_q(\chi)$, $\chi \in (C_0^{\perp})^*$. By the Stickelberger theorem on the prime ideal factorization of Gauss sums, we have $t = p^{\theta} = p^{d\theta'}$ with $\theta' = \frac{1}{p-1}\min\{s_p(jk) \mid 1 \le j \le N-1\}$ and $d = f/f'$, where f' is the order of p modulo N and $s_p(\cdot)$ is the p-adic digit sum function.

(2) In Sect. 4, we will show that the two simple necessary conditions in Proposition 2.3 are sometimes also sufficient.

2.1 Circulant weighing matrices

Let $q = p^f$ be a prime power, γ be a primitive element of $\mathbb{F}_q$, and $N > 1$ be a positive integer such that $N \mid \frac{q-1}{p-1}$. In [13], it was shown that if the Gauss periods $\eta_a = \psi(\gamma^a C_0)$, $0 \le a \le N-1$, take exactly two values α_1 and α_2, then each of the index sets $I_i = \{a \in \mathbb{Z}_N \mid \eta_a = \alpha_i\}$, $1 \le i \le 2$, forms a difference set in $\mathbb{Z}_N$, which is a *subdifference set* of the Singer difference set. It is natural to ask: if the

Gauss periods take exactly three values, what combinatorial structures can we obtain from the index sets I_1, I_2 and I_3? In this subsection, we will see that under certain conditions, three-valued Gauss periods lead to circulant weighing matrices.

Lemma 2.5 *Let $q = p^f$ be a prime power and $N > 2$ be a positive integer such that $N \mid (q-1)$. Assume that the Gauss periods η_a, $0 \le a \le N-1$, take exactly three rational values $\alpha_1, \alpha_2, \alpha_3$ which form an arithmetic progression, say, $\alpha_1 - \alpha_2 = -t < 0$ and $\alpha_3 - \alpha_2 = t > 0$. Then*

$$|I_1| = \frac{N(\alpha_2^2 + \alpha_2 t + k) + 2\alpha_2 - k + t + 1}{2t^2},$$
$$|I_3| = \frac{N(\alpha_2^2 - \alpha_2 t + k) + 2\alpha_2 - k - t + 1}{2t^2},$$
$$|I_2| = \frac{N(t^2 - \alpha_2^2 - k) - 1 - 2\alpha_2 + k}{t^2}, \quad |I_1| - |I_3| = \frac{\alpha_2 N + 1}{t}.$$

Moreover, we have

$$(I_1 - I_3)(I_1 - I_3)^{(-1)} = \frac{q}{t^2} \cdot 1 + \frac{\alpha_2^2 N + 2\alpha_2 - k}{t^2} Z_N \tag{2.3}$$

in $\mathbb{Q}[Z_N]$. In particular, t must be a power of p.

Proof The fact that t is a power of p follows from Proposition 2.3. The sizes of I_1, I_2, and I_3 can be obtained from Lemma 2.2 and the assumptions that $\alpha_1 = \alpha_2 - t$ and $\alpha_3 = \alpha_2 + t$. Finally by Lemma 2.2 and the assumptions that $\alpha_1 = \alpha_2 - t$ and $\alpha_3 = \alpha_2 + t$, we have

$$(\alpha_2 Z_N - t(I_1 - I_3))(\alpha_2 Z_N - t(I_1 - I_3))^{(-1)} = q \cdot 1 - \frac{q-1}{N} Z_N,$$

from which (2.3) follows. This completes the proof. □

We further consider the question of when $I_1 - I_3$ generates a circulant weighing matrix.

Proposition 2.6 *Let $q = p^f$ be a prime power and $N > 2$ be a positive integer such that $N \mid (q-1)$. Assume that the Gauss periods η_a, $0 \le a \le N-1$, take exactly three rational values $\alpha_1, \alpha_2, \alpha_3$ which form an arithmetic progression, say, $\alpha_1 - \alpha_2 = -t < 0$ and $\alpha_3 - \alpha_2 = t > 0$. Then $I_1 - I_3$ generates a circulant weighing matrix $\mathbf{CW}(N, \frac{q}{t^2})$ if and only if $\alpha_2 = (\sqrt{q} - 1)/N$ and q is a square.*

Proof Let q be a square and $\alpha_2 = (\sqrt{q} - 1)/N$. Then $\alpha_2^2 N + 2\alpha_2 - k = 0$; in this case (2.3) becomes

$$(I_1 - I_3)(I_1 - I_3)^{(-1)} = \frac{q}{t^2} \cdot 1,$$

that is, $I_1 - I_3$ generates a circulant weighing matrix of order q and weight $\frac{q}{t^2}$.

Conversely, if $I_1 - I_3$ generates a circulant weighing matrix $\mathbf{CW}(N, \frac{q}{t^2})$, then $\alpha_2^2 N + 2\alpha_2 - k = 0$. It follows that $\alpha_2 = \frac{\sqrt{q}-1}{N}$ or $\alpha_2 = -\frac{1+\sqrt{q}}{N}$. In the latter case, $\sqrt{q} \equiv -1 \pmod N$, from which we know that the Gauss periods take only two values [13]. Therefore, we must have $\alpha_2 = \frac{\sqrt{q}-1}{N}$. Since α_2 is rational, we see that q is a square. □

2.2 Related association schemes

As we remarked in Sect. 1, when the Gauss periods η_a, $0 \le a \le N-1$, take exactly two distinct values, and $-1 \in C_0$, then we naturally obtain a strongly regular Cayley graphs defined on $\mathbb{F}_q$ with connection set C_0 (which is denoted by $\mathrm{Cay}(\mathbb{F}_q, C_0)$). Strongly regular graphs are the same objects as two-class association schemes. We will see in this section that if the Gauss periods take exactly three values, under certain conditions, we obtain three-class self-dual association schemes. Before stating our main theorem, we give some remarks on translation schemes.

Let $G = \{g_1, \ldots, g_v\}$ be a multiplicative abelian group of order v, with character group $\widehat{G}$. Let $\rho : G \to GL_v(\mathbb{C})$ be the regular representation of G, namely $(\rho(g))_{(h_1,h_2)} = 1$ if $h_2 = h_1 g$, and $= 0$ otherwise. Also, for a character $\chi \in \widehat{G}$, let $\mathbf{v}_\chi := \frac{1}{\sqrt{v}}(\chi(g_1), \ldots, \chi(g_v))$ and $E_\chi := \mathbf{v}_\chi^\top \cdot \overline{\mathbf{v}_\chi}$. Then the $\mathbf{v}_\chi^\top$ are the common eigenvectors of $\rho(g)$, $g \in G$, since $\rho(g)\mathbf{v}_\chi^\top = \chi(g)\mathbf{v}_\chi^\top$. The E_χ's are the primitive idempotents of the algebra $\mathcal{A} := \langle \rho(g) : g \in G \rangle \cong \mathbb{C}[G]$, as can be easily checked by using the orthogonality relations of characters. Moreover, by using the fact that $\big(E_\chi\big)_{(g,h)} = \frac{1}{v}\chi(gh^{-1})$, we have

$$(vE_\chi) \circ (vE_{\chi'}) = (vE_{\chi\chi'}). \tag{2.4}$$

Now assume that $D_0, D_1, \ldots, D_d$ form a partition of G which yields a translation scheme, and its dual scheme is given by the following partition of $\widehat{G}$: $D_0', D_1', \ldots, D_d'$. Write $A_i = \rho(D_i)$, $0 \le i \le d$, and let $E_0, E_1, \ldots, E_d$ be the primitive idempotents of the Bose–Mesner algebra $\mathcal{A} := \langle A_0, A_1, \ldots, A_d \rangle$ with respect to the matrix multiplication. We have $E_i = \sum_{\chi \in D_i'} E_\chi$ with respect to a proper ordering of the E_i's.

Similarly, if we use ρ' for the regular representation of $\widehat{G}$, and write $A_i' = \rho'(D_i')$, then $A_0', \ldots, A_d'$ span $\widehat{\mathcal{A}}$, the Bose–Mesner algebra of the dual scheme.

Let Ψ be the linear map from $\widehat{\mathcal{A}}$ to $\mathcal{A}$ that maps A_i' to vE_i, $0 \le i \le d$. It follows from (2.4) that Ψ is an algebra isomorphism from $(\widehat{\mathcal{A}}, +, \cdot)$ to $(\mathcal{A}, +, \circ)$. An easy corollary is that, Ψ maps the idempotents of $(\widehat{\mathcal{A}}, +, \cdot)$ to those of $(\mathcal{A}, +, \circ)$, namely the A_i's.

Theorem 2.7 *Let $q = p^f$ be a prime power and $N > 2$ be a positive integer such that $N \mid (q-1)$. Assume that $-1 \in C_0$ and the Gauss periods η_a, $0 \le a \le N-1$, take exactly three rational values $\alpha_1, \alpha_2, \alpha_3$, say, $\alpha_1 - \alpha_2 = -tu < 0$ and $\alpha_3 - \alpha_2 = tv > 0$ with $t > 0$. Let*

$$R_0 = \{0\},\ R_1 = \bigcup_{i \in I_1} C_i,\ R_2 = \bigcup_{i \in I_2} C_i,\ R_3 = \bigcup_{i \in I_3} C_i,$$

where $I_i = \{a \in \mathbb{Z}_N \mid \eta_a = \alpha_i\}$ *for* $i = 1, 2, 3$. *If* $|I_1| = 1$ *or* $|I_3| = 1$, *then* $(\mathbb{F}_q, \{\mathcal{R}_i\}_{i=0}^3)$ *is a self-dual three-class association scheme. (Here for* $0 \le i \le 3$, $(x, y) \in \mathcal{R}_i$ *if and only if* $x - y \in R_i$.*)*

Proof Let $A_0, A_1, \ldots, A_N$ and $E_0, E_1, \ldots, E_N$ be the first and the second standard bases of the Bose–Mesner algebra $\mathcal{A}$ of the cyclotomic scheme of class N of $\mathbb{F}_q$. We may assume that the cyclic permutation $\sigma = (1, 2, \ldots, N)$ is an algebraic automorphism of the association scheme; namely, the linear map that maps $A_i \mapsto A_{\sigma(i)}$, $0 \le i \le d$, is an automorphism of the Bose–Mesner algebra with respect to both the matrix multiplication and the Schur product. Notice that $\mathcal{A}$ consists of symmetric matrices.

In what follows we use the notation $E_S = \sum_{s \in S} E_s$, $A_S = \sum_{s \in S} A_s$ for any $S \subseteq \{1, 2, \ldots, N\}$. Let $P = (p_j(i))$ and $Q = (q_j(i))$ be the first and second eigenmatrix of the cyclotomic scheme, respectively. With a proper ordering of the E_i's, we have $P = Q$, and the principal part of P is symmetric. The principal part of P has only three distinct rational entries, namely $\alpha_1, \alpha_2, \alpha_3$.

Since the Gauss periods have three values from $\{\alpha_1, \alpha_2, \alpha_3\}$, we have

$$A_1 = kE_0 + \alpha_1 E_{L_1} + \alpha_2 E_{L_2} + \alpha_3 E_{L_3},$$

where the L_i's form a partition of $\{1, 2, \ldots, N\}$ (and they come from the I_i's in the statement of the theorem). Since the cyclotomic scheme is self-dual, by the algebra isomorphism Ψ described right before the statement of this theorem, we have

$$E_1 = q^{-1}(kA_0 + \alpha_1 A_{M_1} + \alpha_2 A_{M_2} + \alpha_3 A_{M_3}),$$

where the M_i's form a partition of $\{1, 2, \ldots, N\}$, and $|M_i| = |L_i|$, for all $i = 1, 2, 3$.

Assume now that $|L_1| = 1$, i.e., $L_1 = \{\ell\}$ for some $\ell \in \{1, 2, \ldots, N\}$. We have $\alpha_1 = p_1(\ell)$. Consider the vector space $\mathcal{B}$ spanned by A_0, A_1, E_0, E_ℓ. Noting that $\alpha_2 \ne \alpha_3$, it follows from

$$\begin{aligned} A_0 &= E_0 + E_\ell + E_{L_2} + E_{L_3}, \\ A_1 &= kE_0 + \alpha_1 E_\ell + \alpha_2 E_{L_2} + \alpha_3 E_{L_3}, \end{aligned}$$

that $\mathcal{B} = \langle E_0, E_\ell, E_{L_2}, E_{L_3} \rangle$. In particular, $\mathcal{B}$ is closed with respect to the matrix multiplication.

Since σ is an algebraic automorphism of $\mathcal{A}$, we have $E_\ell = q^{-1}(kA_0 + \alpha_1 A_{M_1'} + \alpha_2 A_{M_2'} + \alpha_3 A_{M_3'})$, where $M_i' = \sigma^{\ell-1}(M_i)$. It follows from $|M_i'| = |M_i| = |L_i|$ that $M_1' = \{m\}$ for some $m \in \{1, 2, \ldots, N\}$. So, $E_\ell = q^{-1}(kA_0 + \alpha_1 A_m + \alpha_2 A_{M_2'} + \alpha_3 A_{M_3'})$. On the other hand, we have

$$qE_\ell \circ A_1 = q_\ell(1) A_1 = \alpha_1 A_1,$$

It follows that $m = 1$. Together with $E_0 = q^{-1}(A_0 + A_1 + A_{M_2'} + A_{M_3'})$, we see that $\mathcal{B} = \langle A_0, A_1, A_{M_2'}, A_{M_3'} \rangle$. In particular, $\mathcal{B}$ is closed with respect to the Schur product.

Since $A_0, E_0 \in \mathcal{B}$ and $\mathcal{B}$ is symmetric, we conclude that $(\mathbb{F}_q, \{\mathcal{R}_i\}_{i=0}^3)$ is a self-dual association scheme with $\mathcal{B}$ as its Bose–Mesner algebra. □

Remark 2.8 We comment that the condition $|I_1| = 1$ (or $|I_3| = 1$) in Theorem 2.7 is needed. Below is an example in which the Gauss periods take three values, but the partition of $\mathbb{Z}_N$ by I_1, I_2 and I_3 does not yield a three-class association scheme. Let $q = 11^3$, $N = 19$, $I_1 = \{0, 2, 3, 4, 5, 6, 9, 14, 16, 17\}$, $I_2 = \{8, 10, 12, 13, 15, 18\}$, and $I_3 = \{1, 7, 11\}$. In this case, $\psi(\gamma^a C_0)$, $a = 0, 1, \ldots, N-1$, take the values -7, 4, and 15 according as $a \in I_i$, $1 \le i \le 3$, but the partition I_1, I_2, I_3 of $\mathbb{Z}_N$ does not yield a three-class association scheme.

3 Sufficient conditions for Gauss periods to take exactly three values

In this section, we consider the question when the necessary conditions obtained in Proposition 2.3 are also sufficient. We pay special attention to the case where either $u = 1$ or $v = 1$. Here we are using the notation of Proposition 2.3. (Many examples given in Sect. 4 fall into this case.) Furthermore, we show that the partition of $\mathbb{Z}_N$ by I_1, I_2, and I_3 yields a three-class association scheme if $u = |I_3| = 1$ or $v = |I_1| = 1$.

3.1 Sufficient conditions for Gauss periods to take three values

In this subsection, we give sufficient conditions for Gauss periods to take exactly three distinct values. First, we give a general sufficient condition. Below, we use $\mathbb{N}$ to denote the set of positive integers.

Proposition 3.1 *Let $q = p^f$ be a prime power, $N > 2$ be an integer such that $N \mid (q-1)$, and $C_0 = \langle \gamma^N \rangle$, where γ is a fixed primitive element of $\mathbb{F}_q$. Assume that there are four positive integers u, v, r, s such that*

(i) $t(-ur + vs) \equiv -1 \pmod N$;
(ii) $(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2 r + v^2 s)$,

where t is the largest power of p dividing all $G_q(\chi)$, $\chi \in (C_0^\perp)^* = (C_0)^\perp \backslash \{\chi_0\}$. If all nonnegative solutions $(t_x)_{x \in \mathbb{Z} \backslash \{0\}}$ to the following system of equations

$$\begin{cases} \sum_{x \in \mathbb{N}} x(x-1)t_x + \sum_{x \in \mathbb{N}} x(x+1)t_{-x} = u(u+1)r + v(v-1)s \\ \sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N}} x(x-1)t_{-x} = u(u-1)r + v(v+1)s \end{cases}$$

satisfy $t_x \neq 0$ if $x = i_1$ or i_2, $t_x = 0$ for all $x \neq i_1, i_2$, and $t_{i_1} + t_{i_2} < N$, where i_1, i_2 are two distinct integers, then the Gauss periods $\eta_a = \psi(\gamma^a C_0)$, $0 \le a \le N-1$, take exactly three distinct values.

Proof Let $y = \frac{-t(-ur+vs)-1}{N}$. Define a map $\tau : \mathbb{Z}_N \to \mathbb{C}$ by

$$\tau(a) = \frac{\psi(\gamma^a C_0) - y}{t}.$$

Since

$$\psi(\gamma^a C_0) + \frac{1}{N} = \frac{1}{N} \sum_{\chi \in (C_0^\perp)^*} G_q(\chi)\chi^{-1}(\gamma^a),$$

by $t \mid G_q(\chi)$ and assumption (i), we see that $\tau(a) \in \mathbb{Z}$, that is, τ is integer valued. Computing the Fourier transform of τ, we have

$$\widehat{\tau}(\chi) = \frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} \tau(a)\chi(\gamma^a) = \begin{cases} \frac{1}{t\sqrt{N}} G_q(\chi) & \text{if } \chi \text{ is nontrivial,} \\ \frac{-ur+vs}{\sqrt{N}} & \text{if } \chi \text{ is trivial.} \end{cases}$$

It follows from Parseval's identity that

$$\sum_{a \in \mathbb{Z}_N} \tau(a)^2 = \sum_{\chi \in C_0^\perp} \widehat{\tau}(\chi)\overline{\widehat{\tau}(\chi)} = (N-1)\frac{q}{Nt^2} + \frac{(-ur+vs)^2}{N}.$$

By assumption (ii), we have

$$\sum_{a \in \mathbb{Z}_N} \tau(a)^2 = u^2 r + v^2 s. \tag{3.1}$$

On the other hand, we have

$$\sum_{a \in \mathbb{Z}_N} \tau(a) = -ur + vs. \tag{3.2}$$

Equations (3.1) and (3.2) can be rewritten as

$$\sum_{x \in \mathbb{N}} x^2 t_x + \sum_{x \in \mathbb{N}} x^2 t_{-x} = u^2 r + v^2 s \quad \text{and} \quad \sum_{x \in \mathbb{N}} x t_x - \sum_{x \in \mathbb{N}} x t_{-x} = -ur + vs,$$

where $t_x = |\{a \in \mathbb{Z}_N \mid \tau(a) = x\}|$, $x \in \mathbb{N}$. It follows that

$$\sum_{x \in \mathbb{N}} x(x-1)t_x + \sum_{x \in \mathbb{N}} x(x+1)t_{-x} = u(u+1)r + v(v-1)s \tag{3.3}$$

and

$$\sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N}} x(x-1)t_{-x} = u(u-1)r + v(v+1)s. \tag{3.4}$$

By assumption, the nonnegative solutions $(t_x)_{x \in \mathbb{Z} \setminus \{0\}}$ to the above system of equations all satisfy $t_x \neq 0$ when $x = i_1$ or i_2 and $t_x = 0$ for all $x \neq i_1, i_2$. This implies that $\tau(a) \in \{0, i_1, i_2\}$ for all $a \in \mathbb{Z}_N$. Consequently, $\eta_a = \psi(\gamma^a C_0)$, $0 \leq a \leq N-1$, take exactly three distinct values since $t_{i_1} + t_{i_2} < N$. The proof is complete. □

As an immediate corollary, we have the following.

Corollary 3.2 *Let $q = p^f$ be a prime power, $N > 2$ be an integer such that $N \mid (q-1)$, and $C_0 = \langle \gamma^N \rangle$, where γ is a fixed primitive element of $\mathbb{F}_q$. Assume that there are four positive integers u, v, r, s satisfying*

(i) $t(-ur + vs) \equiv -1 \pmod N$;
(ii) $(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2 r + v^2 s)$,

where t is the largest power of p dividing all $G_q(\chi)$, $\chi \in (C_0^{\perp})^* = (C_0)^{\perp} \backslash \{\chi_0\}$. If $u = v = r = 1$ and $s + 1 < N$, or $u = v = s = 1$ and $r + 1 < N$, then $\eta_a = \psi(\gamma^a C_0)$, $0 \le a \le N-1$, take exactly three distinct values; in this case, the three values taken by η_a form an arithmetic progression.

Proof We assume that $u = v = s = 1$. (The case where $u = v = r = 1$ is similar.) In this case, (3.4) is reduced to

$$\sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N} \backslash \{1\}} x(x-1)t_{-x} = 2.$$

The nonnegative solutions $(t_x)_{x \in \mathbb{Z} \backslash \{0\}}$ to the system of equations

$$\begin{cases} \sum_{x \in \mathbb{N} \backslash \{1\}} x(x-1)t_x + \sum_{x \in \mathbb{N}} x(x+1)t_{-x} = 2r \\ \sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N} \backslash \{1\}} x(x-1)t_{-x} = 2 \end{cases}$$

must satisfy $t_1 = 1$, $t_{-1} = r$ and $t_x = 0$ for all other x, or $t_{-2} = 1$, $t_{-1} = r - 3$ and $t_x = 0$ for all other x. It follows that $\tau(a) \in \{0, -1, 1\}$ or $\tau(a) \in \{0, -1, -2\}$ for all $a \in \mathbb{Z}_N$. Consequently, η_a, $a \in \mathbb{Z}_N$, take exactly three distinct values since $s + 1 < N$. The proof of the corollary is complete. □

The conditions $u = v = r = 1$ and $s + 1 < N$ in the above corollary are quite restrictive. Below, we consider more general situations where we can still guarantee that the Gauss periods take only three values. We start with the following lemma.

Lemma 3.3 *Let $q = p^f$ be a prime power, $N > 1$ be an integer such that $N \mid (q-1)$, and $C_0 = \langle \gamma^N \rangle$, where γ is a fixed primitive element of $\mathbb{F}_q$. Assume that $\eta_a = \psi(\gamma^a C_0)$, $0 \le a \le N-1$, take exactly ℓ distinct values, say, $\alpha_1, \alpha_2, \ldots, \alpha_\ell$. Let $I_i = \{a \in \mathbb{Z}_N \mid \eta_a = \alpha_i\}$ for $1 \le i \le \ell$. Then each I_i is invariant under the multiplication by p. Moreover, assume that $m := \gcd\{\mathrm{ord}_n(p) \mid n > 1 \text{ and } n \text{ divides} N\} \ge 2$. Then there exists a unique i_0, $1 \le i_0 \le \ell$, such that $|I_{i_0}| \equiv 1 \pmod m$ and $|I_i| \equiv 0 \pmod m$ for all $i \ne i_0$.*

Proof Since $\mathrm{Tr}_{q/p}(x^p) = \mathrm{Tr}_{q/p}(x)$ for $x \in \mathbb{F}_q$, we have $\eta_{pa} = \eta_a$ for all $a \in \mathbb{Z}_N$. It follows that each I_i is invariant under the multiplication by p. Note that under the multiplication by p (i.e., under the map $x \mapsto px$, $x \in \mathbb{Z}_N$), 0 forms a singleton orbit, and all other orbits have sizes divisible by m. The second conclusion of the lemma follows. This completes the proof of the lemma. □

Theorem 3.4 *Let $q = p^f$ be a prime power, $N > 2$ be an integer such that $N \mid (q-1)$, and $C_0 = \langle \gamma^N \rangle$, where γ is a fixed primitive element of $\mathbb{F}_q$. Assume that there are four positive integers u, v, r, s such that*

(i) $t(-ur + vs) \equiv -1 \pmod{N}$;
(ii) $(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2r + v^2s)$,

where t is the largest power of p dividing all $G_q(\chi)$, $\chi \in (C_0^{\perp})^* = (C_0)^{\perp} \backslash \{\chi_0\}$. Let $m = \gcd\{\mathrm{ord}_n(p) \mid n > 1$, and n divides $N\}$ and assume that $m \geq 2$. If one of the following conditions holds,

(1) $u = s = 1$, $v(v+1) < 2m$, *and* $r + 1 < N$;
(2) $u = s = 1$, $v(v+1) = 2m$, *and* $r + v^2 < N$;
(3) $v = r = 1$, $u(u+1) < 2m$, *and* $s + 1 < N$;
(4) $v = r = 1$, $u(u+1) = 2m$, *and* $s + u^2 < N$;
(5) $u = v = 1$, $s = m$, *and* $r + m < N$;
(6) $u = v = 1$, $r = m$, *and* $s + m < N$,

then $\eta_a = \psi(\gamma^a C_0)$, $0 \leq a \leq N-1$, take exactly three values.

Proof First we note that by Lemma 3.3, the t_x, $x \in \mathbb{Z}\backslash\{0\}$, in Eqs. (3.3) and (3.4) satisfy that $t_x \equiv 1 \pmod{m}$ for at most one x and $m \mid t_x$ for all other x.

We consider Cases (1) and (2) where $u = s = 1$. (For Cases (3) and (4), the claims can be proved in a similar way. We omit the proof.) In these cases, (3.4) is reduced to

$$\sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N}\backslash\{1\}} x(x-1)t_{-x} = v(v+1). \tag{3.5}$$

(1) If $v(v+1) < 2m$, noting the divisibility conditions on the t_x's, we see that the nonnegative solutions $(t_x)_{x \in \mathbb{Z}\backslash\{0\}}$ to the following system

$$\begin{cases} \sum_{x \in \mathbb{N}\backslash\{1\}} x(x-1)t_x + \sum_{x \in \mathbb{N}} x(x+1)t_{-x} = 2r + v(v-1) \\ \sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N}\backslash\{1\}} x(x-1)t_{-x} = v(v+1) \end{cases}$$

must satisfy $t_v = 1, t_{-1} = r$ and $t_x = 0$ for all other x, or $t_{-(v+1)} = 1, t_{-1} = r - 2v - 1$, and $t_x = 0$ for all other x. It follows that $\tau(a) \in \{0, -1, v\}$ or $\tau(a) \in \{0, -1, -v-1\}$ for all $a \in \mathbb{Z}_N$. Therefore η_a, $a \in \mathbb{Z}_N$, take exactly three values since $r + 1 < N$.

(2) If $v(v+1) = 2m$, the above system has further nonnegative solutions $t_1 = m$, $t_{-1} = r + m - v$ and $t_x = 0$ for all other x, or $t_{-2} = m, t_{-1} = r - 2m - v$, and $t_x = 0$ for all other x. So $\tau(a) \in \{0, -1, 1\}$ or $\tau(a) \in \{0, -1, -2\}$ for all $a \in \mathbb{Z}_N$. It follows that η_a, $a \in \mathbb{Z}_N$, take exactly three values since $r + v^2 < N$.

Next, we consider the case where $u = v = 1$ and $s = m$ or $r = m$.

(3) We assume that $s = m$. (The case where $r = m$ can be handled similarly). In this case, (3.4) is reduced to

$$\sum_{x \in \mathbb{N}} x(x+1)t_x + \sum_{x \in \mathbb{N}\backslash\{1\}} x(x-1)t_{-x} = 2m.$$

If $2m \neq \ell(\ell+1)$ for all $\ell \in \mathbb{Z}$, then the nonnegative solutions $(t_x)_{x\in\mathbb{Z}\setminus\{0\}}$ to the following system

$$\begin{cases} \sum_{x\in\mathbb{N}\setminus\{1\}} x(x-1)t_x + \sum_{x\in\mathbb{N}} x(x+1)t_{-x} = 2r \\ \sum_{x\in\mathbb{N}} x(x+1)t_x + \sum_{x\in\mathbb{N}\setminus\{1\}} x(x-1)t_{-x} = 2m \end{cases}$$

must satisfy $t_1 = m$, $t_{-1} = r$, and $t_x = 0$ for all other x, or $t_{-2} = m$, $t_{-1} = r - 3m$, and $t_x = 0$ for all other x. It follows that $\tau(a) \in \{0, 1, -1\}$ or $\tau(a) \in \{0, -1, -2\}$ for $a \in \mathbb{Z}_N$. Therefore η_a, $a \in \mathbb{Z}_N$, take exactly three values.

If $2m$ can be written as $2m = \ell(\ell+1)$ for some positive integer ℓ, then the above system has further nonnegative solutions $t_\ell = 1$, $t_{-1} = r - \ell(\ell-1)/2$, and $t_x = 0$ for other x, or $t_{-\ell-1} = 1$, $t_{-1} = r - (\ell+1)(\ell+2)/2$, and $t_x = 0$ for other x. Again we have $\tau(a) \in \{0, \ell, -1\}$ or $\tau(a) \in \{0, -1, -\ell-1\}$ for $a \in \mathbb{Z}_N$. □

4 Examples of three-valued Gauss periods and related weighing matrices and association schemes

In this section, we give examples of three-valued Gauss periods. These examples often lead to interesting combinatorial structures such as circulant weighing matrices and association schemes.

As a preparation, we consider a group ring version of the Hasse–Davenport theorem.

Theorem 4.1 ([2, Theorem 11.5.2]) *Let χ be a nonprincipal multiplicative character of $\mathbb{F}_q = \mathbb{F}_{p^f}$ and let χ' be the lifted character of χ to the extension field $\mathbb{F}_{q'} = \mathbb{F}_{p^{fe}}$, that is, $\chi'(\alpha) := \chi(\mathrm{Norm}_{q'/q}(\alpha))$ for any $\alpha \in \mathbb{F}_{q'}^*$. Then, it holds that*

$$G_{q'}(\chi') = (-1)^{e-1}(G_q(\chi))^e.$$

Let χ be a multiplicative character of $\mathbb{F}_q$ of order $N > 1$, γ a primitive element of $\mathbb{F}_q$, and $C_0 = \langle \gamma^N \rangle$. As we saw in the proof of Lemma 2.1, we have

$$G_q(\chi) = \eta_0 + \eta_1\chi(\gamma) + \cdots + \eta_{N-1}\chi(\gamma)^{N-1},$$

where $\eta_a = \psi(C_a^{(N,q)})$ for $0 \le a \le N-1$. This motivated us to define the following group ring element

$$g_{F,N} = \sum_{a\in\mathbb{Z}_N} \eta_a[a] \in \mathbb{C}[\mathbb{Z}_N],$$

where $F = \mathbb{F}_q$. (See [5].) Let E be the finite field with q^e elements, $e > 1$ a positive integer. Then it follows from Theorem 4.1 that

$$g_{E,N} = (-1)^{e-1} g_{F,N}^e. \tag{4.1}$$

The advantage of this group ring version of the Hasse–Davenport theorem is that starting with a pair of small (q, N) with $N|(q-1)$ we are able to determine the Gauss periods corresponding to the subgroup of index N of $\mathbb{F}_{q^e}^*$ efficiently.

4.1 Examples from a conic

Let p be a prime, f a positive integer, $F = \mathbb{F}_{p^{3f}}$, and $E = \mathbb{F}_{p^{3fe}}$ with $e > 1$. Let γ and ω be primitive elements of F and E, respectively, such that $\gamma = \mathrm{Norm}_{E/F}(\omega)$. Let $N = \frac{p^{3f}-1}{p^f-1}$. Then $C_0^{(N,F)} = \mathbb{F}_{p^f}^* < F^* = \mathbb{F}_{p^{3f}}^*$, and the Gauss periods $\eta_a = \psi(\gamma^a C_0^{(N,F)}) = p^f - 1$ if $\mathrm{Tr}_{F/L}(\gamma^a) = 0$ and -1 otherwise, where $L = \mathbb{F}_{p^f}$. Denote by

$$S := \left\{ i \in \mathbb{Z}_N : \mathrm{Tr}_{F/L}(\gamma^i) = 0 \right\}.$$

Then $|S| = p^f + 1$, and $g_{F,N} = p^f S - \mathbb{Z}_N$. As in [8], we identify the points of the projective plane $PG(2, p^f)$ with the elements of $\mathbb{Z}_N$. Then S represents a line of $PG(2, p^f)$, and is the well-known Singer difference set in $\mathbb{Z}_N$; see [12] for instance.

Now set $e = 2$. Then by (4.1), we have

$$g_{E,N} = -(p^f S - \mathbb{Z}_N)^2 = -p^{2f} S^2 + (p^{2f} + p^f - 1)\mathbb{Z}_N.$$

Note that here $g_{E,N} = \sum_{a \in \mathbb{Z}_N} \psi'(\omega^a C_0^{(N,E)})[a] \in \mathbb{C}[\mathbb{Z}_N]$, ψ' is the canonical additive character of E. In order to know how many values the Gauss periods $\psi'(\omega^a C_0^{(N,E)})$, $0 \le a \le N-1$, take, it suffices to compute S^2 in the group ring $\mathbb{C}[\mathbb{Z}_N]$. For any $a \in \mathbb{Z}_N$, the coefficient of $[a]$ in S^2 is equal to the size of

$$\left\{ i \in \mathbb{Z}_N : \mathrm{Tr}_{F/L}(\gamma^{-i}) = 0, \mathrm{Tr}_{F/L}(\gamma^{i+a}) = 0 \right\} = \mathcal{Q} \cap (S - a),$$

where $\mathcal{Q} = \{ i \in \mathbb{Z}_N : \mathrm{Tr}_{F/L}(\gamma^{-i}) = 0 \}$ and $S - a = \{ x - a \mid x \in S \}$. Since $\mathcal{Q}$ is a conic in $PG(2, p^f)$ (cf. [10]) and $S - a$ is a line of $PG(2, p^f)$, we have $|\mathcal{Q} \cap (S-a)| = 0$, 1 or 2, according as $S-a$ is passant, tangent or secant. It follows that the Gauss periods $\psi(\omega^a C_0^{(N,E)})$, $0 \le a \le N-1$, take three values $\alpha_1 = p^{2f} + p^f - 1$, $\alpha_2 = p^f - 1$, and $\alpha_3 = -p^{2f} + p^f - 1$, which form an arithmetic progression with common difference $t = p^{2f}$. Here $|E| = q^{6f}$ and $\alpha_2 = p^f - 1 = \frac{\sqrt{p^{6f}}-1}{N}$. So by Proposition 2.6 we obtain a $\mathbf{CW}(p^{2f+p^f+1}, p^{2f})$. We remark that the circulant weighing matrix $\mathbf{CW}(p^{2f+p^f+1}, p^{2f})$ obtained here is not new (cf. [14]), but the connection with three-valued Gauss periods is new.

Note that with the same notation as above, in the special case where $p = 2$, the authors of [8] already showed that the Cayley graph $Cay(\mathbb{F}_q, C_0^{(N,q)})$, with $q = 2^{6f}$ and $N = (2^{3f} - 1)/(2^f - 1)$, has three restricted eigenvalues $-2^{2f} + 2^f - 1$, $2^f - 1$, $2^{2f} + 2^f - 1$, and $\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid x - y \in C_0^{(N,q)}\}$ is a relation in a three-class association scheme, see [8, p. 1210].

4.2 More examples from two-valued Gauss periods

Let p be a prime, $f \geq 1$ and $e > 1$ be integers, and $F = \mathbb{F}_{p^f}$, $E = \mathbb{F}_{p^{fe}}$. Assume that $k|(p^f - 1)$. Then certainly $k|(p^{fe} - 1)$. Let $N = (p^f - 1)/k$ and $N' = (p^{fe} - 1)/k$. Then $C_0^{(N,F)} = C_0^{(N',E)}$. This can be seen as follows. Let ω and γ be primitive elements of E and F, respectively, such that $\gamma = \omega^{\frac{p^{fe}-1}{p^f-1}}$. Then $C_0^{(N,F)} = \langle \gamma^N \rangle = \langle \omega^{\frac{(p^{fe}-1)N}{p^f-1}} \rangle = \langle \omega^{N'} \rangle = C_0^{(N',E)}$.

Assume that the Gauss periods $\eta_a = \psi(\gamma^a C_0^{(N,F)})$, $0 \leq a \leq N-1$, take exactly two distinct values α_1 and α_2 according as $a \in S$ or not for some $S \subseteq \mathbb{Z}_N$. Let ψ' be the canonical additive character of E. Then, we have

$$\psi'(\omega^a C_0^{(N',E)}) = \sum_{x \in C_0^{(N,p^f)}} \xi_p^{\mathrm{Tr}_{p^f/p}(x \cdot (\mathrm{Tr}_{E/F}(\omega^a)))} = \psi(\mathrm{Tr}_{E/F}(\omega^a) C_0^{(N,p^f)})$$
$$= \begin{cases} k & \text{if } \mathrm{Tr}_{E/F}(\omega^a) = 0, \\ \alpha_1 & \text{if } \mathrm{Tr}_{E/F}(\omega^a) = \gamma^b \text{ and } b \in S, \\ \alpha_2 & \text{if } \mathrm{Tr}_{E/F}(\omega^a) = \gamma^b \text{ and } b \in \mathbb{Z}_N \backslash S. \end{cases}$$

That is, the Gauss periods $\psi'(\omega^a C_0^{(N',E)})$, $0 \leq a \leq N'-1$, take three distinct values k, α_1 and α_2. Furthermore, it is routine to check that $C_0^{(N,F)}$, $F^* \setminus C_0^{(N,F)}$, $E^* \backslash F^*$ give a three-class association scheme.

4.3 Examples from union of 1-dimensional subspaces

Let $q \equiv 1 \pmod 3$ and γ an element of order $k = 3(q-1)$ in $\mathbb{F}_{q^3}$, and set $N = \frac{q^3-1}{k}$. Then the degree of the minimal polynomial of γ over $\mathbb{F}_q$ is equal to $\mathrm{ord}_k(q)$. Assume that $\mathrm{ord}_k(q) = 3$. Then $1, \gamma, \gamma^2$ are linearly independent over $\mathbb{F}_q$, and it follows that $C_0^{(N,q^3)} = \langle \gamma^N \rangle = \{\lambda \cdot 1 \mid \lambda \in \mathbb{F}_q^*\} \cup \{\lambda \cdot \gamma \mid \lambda \in \mathbb{F}_q^*\} \cup \{\lambda \cdot \gamma^2 \mid \lambda \in \mathbb{F}_q^*\}$. For any nontrivial additive character ψ' of $\mathbb{F}_{q^3}$, we have

$$\psi'(C_0^{(N,q^3)}) = \begin{cases} -3 & \text{if } \psi'|_{\mathbb{F}_q}, \psi'|_{\mathbb{F}_q\gamma}, \psi'|_{\mathbb{F}_q\gamma^2} \text{ are all nontrivial}, \\ -3+q & \text{if exactly one of } \psi'|_{\mathbb{F}_q}, \psi'|_{\mathbb{F}_q\gamma}, \psi'|_{\mathbb{F}_q\gamma^2} \text{ is trivial}, \\ -3+2q & \text{if exactly two of} \psi'|_{\mathbb{F}_q}, \psi'|_{\mathbb{F}_q\gamma}, \psi'|_{\mathbb{F}_q\gamma^2} \text{ are trivial}. \end{cases}$$

Therefore the Gauss periods η_a, $0 \leq a \leq N-1$, of $\mathbb{F}_{q^3}$ take three values $\alpha_1 = -3, \alpha_2 = -3+q, \alpha_3 = -3+2q$, which form an arithmetic progression with common difference $t = q$. By Lemma 2.5, we have

$$|I_1| = \frac{(q-1)^2}{3}, |I_2| = q-1, |I_3| = 1.$$

Since $|I_3| = 1$, by Theorem 2.7, the subsets $\cup_{i\in I_j} C_i^{(N,q^3)}$, $j = 1, 2, 3$, give a three-class self-dual association scheme. Note that with assumptions as above, $\alpha_2^2 N + 2\alpha_2 - k = 0$ if and only if $(q, N) = (4, 7)$. Therefore, we obtain a $\mathbf{CW}(7, 4)$ in the case when $(q, N) = (4, 7)$, and we do not obtain circulant weighing matrices in other cases.

4.4 Examples from products of subfields

Let e, f be two positive integers such that $e/\gcd(e, f) = 3$ and let $q = p^{\mathrm{lcm}(e,f)} = p^{3f}$. Let $C_0^{(N,q)}$ be the subgroup of $\mathbb{F}_q^*$ generated by $\mathbb{F}_{p^e}^*$ and $\mathbb{F}_{p^f}^*$. Then

$$|C_0^{(N,q)}| = (p^e - 1)(p^f - 1)/(p^\ell - 1),$$

where $\ell = \gcd(e, f)$ and $N = \frac{(p^{3f}-1)(p^\ell-1)}{(p^e-1)(p^f-1)}$. Let γ be a primitive element of $\mathbb{F}_q$. We compute the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $0 \le a \le N-1$, as follows.

$$\begin{aligned}\psi(\gamma^a C_0^{(N,q)}) &= \frac{1}{p^\ell - 1} \sum_{x\in\mathbb{F}_{p^e}^*} \sum_{y\in\mathbb{F}_{p^f}^*} \xi_p^{\mathrm{Tr}_{p^f}(y\mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a))} \\ &= \frac{1}{p^\ell - 1} \sum_{x\in\mathbb{F}_{p^e}^*} (p^f \delta_{\mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a)} - 1),\end{aligned}$$

where

$$\delta_{\mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a)} = \begin{cases} 1 & \text{if } \mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Define

$$W_a := \left\{x \in \mathbb{F}_{p^e} \mid \mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a) = 0\right\},$$

and set $s_a = |W_a|$. Then we have

$$\psi(\gamma^a C_0^{(N,q)}) = \frac{p^f(s_a - 1) - (p^e - 1)}{p^\ell - 1} = \frac{p^f s_a - p^f - p^e + 1}{p^\ell - 1}.$$

Since W_a is an $\mathbb{F}_{p^\ell}$-subspace of $\mathbb{F}_{p^e}$, we have $s_a = 1, p^\ell, p^{2\ell}, p^{3\ell} = p^e$. Since a basis of $\mathbb{F}_{p^e}$ over $\mathbb{F}_{p^\ell}$ is also a basis of $\mathbb{F}_{p^{3f}}$ over $\mathbb{F}_{p^f}$, and $\gamma^a \neq 0$, it is impossible to have $W_a = \mathbb{F}_{p^e}$. Therefore, the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $0 \le a \le N-1$, take exactly three values

$$\alpha_1 = \frac{1 - p^e}{p^\ell - 1},\ \alpha_2 = p^f + \frac{1 - p^e}{p^\ell - 1},\ \alpha_3 = p^f(p^\ell + 1) + \frac{1 - p^e}{p^\ell - 1}.$$

By Lemma 2.2, it is routine to compute that

$$|I_1| = \frac{p^{3\ell} + p^{2f} - p^{2\ell+f} - p^{\ell+f}}{1 + p^{\ell} + p^{2\ell}},\ |I_2| = p^f - p^{\ell},\ |I_3| = 1.$$

Since $|I_3| = 1$, by Theorem 2.7, the subsets $\bigcup_{i\in I_j} C_i^{(N,q)}$, $j = 1, 2, 3$, give a three-class association scheme.

4.5 Examples from index 2 Gauss sums

Let $q = p^f$, where p is a prime and f a positive integer. Let $N > 1$ be a divisor of $q - 1$. We now focus on the index 2 case, that is, $[\mathbb{Z}_N^* : \langle p\rangle] = 2$, or equivalently, $\mathrm{ord}_N(p) = \phi(N)/2$, where ϕ is Euler's phi function. In this case, the Gauss sums $G_q(\chi)$, where χ has order N, have been evaluated (cf. [15]). In [6], the authors used these Gauss sums to construct several new families of strongly regular graphs. In particular, they evaluated the Gauss periods in the index 2 case. The following theorem is a specialized version of Theorem 4.1 and Theorem 5.1 from [6].

Theorem 4.2 (i) ([6, Theorem 4.1]) *Let $N = p_1 \equiv 3 \pmod 4$ be a prime with $p_1 > 3$, and let p be a prime such that $\gcd(p, N) = 1$ and $\mathrm{ord}_N(p) = (N-1)/2$. Let $q = p^f$, where $f = (p_1 - 1)/2$. Then the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $a = 0, 1, \ldots, N-1$, take at most three values*

$$\alpha_1 = \frac{-2 + p^{\frac{f-h}{2}} b(p_1 - 1)}{2p_1},\quad \alpha_2 = \frac{-2 + p^{\frac{f-h}{2}} cp_1 - p^{\frac{f-h}{2}} b}{2p_1},$$
$$\alpha_3 = \frac{-2 - p^{\frac{f-h}{2}} cp_1 - p^{\frac{f-h}{2}} b}{2p_1}, \tag{4.2}$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and b and c are integers determined by $b, c \not\equiv 0 \pmod p$, $4p^h = b^2 + p_1c^2$, and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

(ii) ([6, Theorem 5.1]) *Let $N = p_1p_2$, where p_1 and p_2 such that $p_1 \equiv 1 \pmod 4$ and $p_2 \equiv 3 \pmod 4$. Let p be a prime such that $\mathrm{ord}_{p_1}(p) = p_1 - 1$, $\mathrm{ord}_{p_2}(p) = p_2 - 1$, $\mathrm{ord}_{p_1p_2}(p) = (p_1 - 1)(p_2 - 1)/2$. Let $q = p^f$, where $f = (p_1 - 1)(p_2 - 1)/2$. Then the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $a = 0, 1, \ldots, N-1$, take at most five values*

$$\alpha_1 = \frac{-1 + \frac{1}{2}p^{\frac{f-h}{2}}(b + cp_1p_2)}{N},\quad \alpha_2 = \frac{-1 + p^{\frac{f}{2}}\left(-\frac{1}{2}bp^{\frac{-h}{2}}(-1 + p_1) + p_1\right)}{N},$$
$$\alpha_3 = \frac{-1 + \frac{1}{2}p^{\frac{f-h}{2}}(b - cp_1p_2)}{N},\quad \alpha_4 = \frac{-1 + p^{\frac{f}{2}}\left(-\frac{1}{2}bp^{\frac{-h}{2}}(-1 + p_2) - p_2\right)}{N},$$
$$\alpha_5 = \frac{-1 + p^{\frac{f}{2}}\left(p_1 + \frac{1}{2}bp^{\frac{-h}{2}}(-1 + p_1)(-1 + p_2) - p_2\right)}{N},$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, and b and c are integers determined by $b, c \not\equiv 0 \pmod{p}$, $4p^h = b^2 + p_1p_2c^2$, and $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$.

From this theorem, we immediately have the following proposition.

Proposition 4.3 *(i) With assumptions and notation the same as in* Theorem 4.2 *(i), the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $a = 0, 1, \ldots, N-1$, take exactly three values which form an arithmetic progression if and only if $p_1 + 9 = 4p^h$ and $\pm 3p^{(f-h)/2} \equiv -2 \pmod{p_1}$.*

(ii) With assumptions and notation the same as in Theorem 4.2 *(ii), the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $a = 0, 1, \ldots, N-1$, take at most three values if $4p^{\frac{h}{2}} \equiv 0 \pmod{p_1 + p_2}$ and $2p^{\frac{f}{2}}(p_1 - p_2)/(p_1 + p_2) \equiv 2 \pmod{p_1p_2}$. In particular, they take exactly three values forming an arithmetic progression if and only if $p_1p_2 + 9 = 4p^h$ and $\pm 3p^{(f-h)/2} \equiv 2 \pmod{p_1p_2}$.*

Proof (i) First we remark that from the explicit computations of the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$ in the proof of Theorem 4.1 in [6], we know that if α_1, α_2 and α_3 are distinct, then the Gauss periods take exactly three values, and α_1 is taken precisely once.

It is clear that $\alpha_1, \alpha_2, \alpha_3$ form an arithmetic progression if and only if $b = \pm 3c$. Since $b, c \not\equiv 0 \pmod{p}$, we have $b = \pm 3c$ if and only if $c \in \{-1, 1\}$ and $b = \pm 3$. It follows that the Gauss periods take exactly three values in arithmetic progression if and only if $p_1 + 9 = 4p^h$ and $\pm 3p^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

(ii) Assume that $4p^{\frac{h}{2}} \equiv 0 \pmod{p_1 + p_2}$ and $2p^{\frac{f}{2}}(p_1 - p_2)/(p_1 + p_2) \equiv 2 \pmod{p_1p_2}$. We set

$$b = \frac{2p^{\frac{h}{2}}(p_1 - p_2)}{p_1 + p_2} \text{ and } c = \pm\frac{4p^{\frac{h}{2}}}{p_1 + p_2}.$$

Both b and c are integers, and they satisfy $4p^h = b^2 + p_1p_2c^2$ and $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$. Note that the above b, c are all the integer solutions to $4p^h = b^2 + p_1p_2c^2$ and $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$. If $b = \frac{2p^{\frac{h}{2}}(p_1-p_2)}{p_1+p_2}$ and $c = \frac{4p^{\frac{h}{2}}}{p_1+p_2}$, then $\alpha_1 = \alpha_2$ and $\alpha_3 = \alpha_4$. On the other hand, if $b = \frac{2p^{\frac{h}{2}}(p_1-p_2)}{p_1+p_2}$ and $c = -\frac{4p^{\frac{h}{2}}}{p_1+p_2}$, then $\alpha_1 = \alpha_4$ and $\alpha_2 = \alpha_3$. In both cases, the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $a = 0, 1, \ldots, N-1$, take at most three values $\alpha_1, \alpha_3, \alpha_5$ (also, from the computations in the proof of Theorem 5.1 in [6], α_5 occurs precisely once); in particular, these $\alpha_1, \alpha_3, \alpha_5$ form an arithmetic progression if and only if $p_1 - p_2 = \pm 6$ (i.e., $b = \pm 3c$). Since $b, c \not\equiv 0 \pmod{p}$, we have $b = \pm 3c$ if and only if $c \in \{-1, 1\}$ and $b = \pm 3$. It follows that n this case the Gauss periods take three values in arithmetic progression if and only if $p_1p_2 + 9 = 4p^h$ and $\pm 3p^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$. □

Example 4.4 There are only five examples satisfying the index 2 condition, and $p_1 + 9 = 4p^h$ and $\pm 3p^{(f-h)/2} \equiv -2 \pmod{p_1}$ stated in Proposition 4.3 (i) for $p_1 \leq 20000$:

$$(p_1, p, h) = (11, 5, 1), (23, 2, 3), (43, 13, 1), (67, 19, 1), (163, 43, 1).$$

There are only two examples satisfying the index 2 condition, and $p_1 p_2 + 9 = 4p^h$ and $\pm 3p^{(f-h)/2} \equiv 2 \pmod{p_1 p_2}$ stated in Proposition 4.3 (ii) for $p_1 p_2 \leq 20000$:

$$(p_1, p_2, p, h) = (5, 11, 2, 4), (17, 11, 7, 2).$$

These results are obtained by a computer search.

Remark 4.5 Let q be a power of a prime p, γ be a primitive element of $\mathbb{F}_q$, and $N > 1$ be a divisor of $q-1$. In the semi-primitive case, i.e., the case where $-1 \in \langle p \rangle \pmod{N}$, it is well known that the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $0 \leq a \leq N-1$, take exactly two values. Note that the condition $-1 \in \langle p \rangle \pmod{N}$ does not involve the extension degree of $\mathbb{F}_q$ over $\mathbb{Z}_p$. Therefore, for any $e > 1$, the Gauss periods corresponding to the subgroup of index N of $\mathbb{F}_{q^e}^*$ also take exactly two values. One is thus led to the following question: are there examples of (q, N), where $N|(q-1)$ and $N > 1$, such that the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $0 \leq a \leq N-1$, take exactly three values, and for any $e > 1$, the Gauss periods corresponding to the subgroup of index N of $\mathbb{F}_{q^e}^*$ also take exactly three values? The index 2 case with $N = p_1$ gives a positive answer to this question. The reason is given below. Note that since $\mathrm{Tr}_{q/p}(x) = \mathrm{Tr}_{q/p}(x^p)$ for any $x \in \mathbb{F}_q$, each index set I_i is invariant under the multiplication by p; in the index 2 case, it follows that each I_i is a union of $\{0\}$, $\langle p \rangle$, $-\langle p \rangle$. It is clear that this conclusion holds, irrelevant of the extension degree of $\mathbb{F}_q$ over $\mathbb{Z}_p$. Therefore, in this case, if the Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $0 \leq a \leq N-1$, take exactly three values, then for any $e > 1$, the Gauss periods corresponding to the subgroup of index N of $\mathbb{F}_{q^e}^*$ also take exactly three values. Here, we should remark that the index 2 case sometimes gives two-valued Gauss periods; all such possibilities are determined under the generalized Riemann hypothesis in [13]. Except for those examples of two-valued Gauss periods determined in [13], the index 2 case with $N = p_1$ provides a positive answer to the question above.

4.6 Computer search

We conducted a computer search for examples of three-valued Gauss periods with the following restrictions: $p < 300$, $p^f < 2^{25}$, $3 < N < 1001$, $(p-1)|k = \frac{p^f-1}{N}$. The output is listed in Table 1. Note that in Tabel 1 we have removed the known examples given in the four subsections above because otherwise the table would take too much space. The multiplicities of the Gauss periods are given by the exponents; for example, in the first row of Table 1, -7^{10} means that the Gauss periods η_a, $0 \leq a \leq 18$, take the value -7 ten times. The AP column indicates whether the Gauss periods are in arithmetic progression or not, with "$\circ$" meaning YES and "$\times$" meaning No. The AS column indicates whether the index sets I_j, $j = 1, 2, 3$, yield a three-class association scheme or not.

Table 1 Computer search results for $p < 300$, $p^f < 2^{25}$, $6 < N < 1001$, $N | \frac{p^f-1}{p-1}$ except for the known examples given in Sects. 4.1, 4.2, 4.3, 4.4 and 4.5

p	f	N	Gauss periods	AP	AS	p	f	N	Gauss periods	AP	AS
11	3	19	$-7^{10}, 4^6, 15^3$	∘	×	53	3	409	$-7^{358}, 46^{48}, 99^3$	∘	×
7	7	29	$-414, -71^{21}, 272^7$	∘	∘	139	3	499	$-39^{378}, 100^{102}, 239^{19}$	∘	×
29	3	67	$-13^{43}, 16^{18}, 45^6$	∘	×	137	3	511	$-37^{391}, 100^{102}, 237^{18}$	∘	×
37	3	67	$-21^{39}, 16^{18}, 53^{10}$	∘	×	109	3	571	$-21^{471}, 88^{90}, 197^{10}$	∘	×
23	3	79	$-7^{58}, 16^{18}, 39^3$	∘	×	67	3	651	$-7^{586}, 60^{62}, 127^3$	∘	×
2	11	89	$-9^{11}, -1^{56}, 7^{22}$	∘	∘	11	6	703	$-21^{591}, 100^{102}, 221^{10}$	∘	×
5	6	93	$-7^{70}, 18^{20}, 43^3$	∘	×	149	3	721	$-31^{586}, 118^{120}, 267^{15}$	∘	×
37	3	201	$-7^{166}, 30^{32}, 67^3$	∘	×	11	6	777	$-19^{661}, 102^{113}, 343^3$	×	×
67	3	217	$-21^{159}, 46^{48}, 113^{10}$	∘	×	5	9	829	$-19^{712}, 106^{108}, 231^9$	∘	×
2	18	219	$-19^{163}, 45^{47}, 109^9$	∘	×	107	3	889	$-13^{787}, 94^{96}, 201^6$	∘	×
61	3	291	$-13^{235}, 48^{50}, 109^6$	∘	×	79	3	903	$-7^{826}, 72^{74}, 151^3$	∘	×
79	3	301	$-21^{231}, 58^{60}, 137^{10}$	∘	×	17	6	921	$-91^{676}, 198^{200}, 487^{45}$	∘	×
83	3	367	$-19^{292}, 64^{66}, 147^9$	∘	×	3	12	949	$-7^{870}, 74^{76}, 155^3$	∘	×
11	6	399	$-37^{295}, 84^{86}, 205^{18}$	∘	×	113	3	991	$-13^{883}, 100^{102}, 213^6$	∘	×

Furthermore, Corollary 3.2 makes it possible to search for (p, f, N) such that the Gauss periods corresponding to the subgroup of index N of $\mathbb{F}_q^*$, $q = p^f$, take exactly three values.

We will run the following algorithm to search for triples (p, f, N) satisfying the conditions in Corollary 3.2: (i) $t(vs - ur) + 1 \equiv 0 \pmod N$, (ii) $(N-1)q + t^2(vs - ur)^2 = (u^2r + v^2s)t^2N$, and (iii) $u = v = 1$ and $r = 1$ or $s = 1$. Put $g = s - r$ and $h = r + s$. In this case, we have $h = |g| + 2$. The algorithm goes as follows:

(1) For any positive integers N and h with $1 < h < N$, compute $(Nh - (h-2)^2)/(N-1)$ in order to know q/t^2.
(2) If this value is a prime power, say p^w, then compute the order of p modulo N, call it f', and the largest positive integer $p^{\theta'}$ dividing $G_{p^{f'}}(\chi)$ for all nontrivial characters χ of exponent N of $\mathbb{F}^*_{p^{f'}}$.
(3) Check whether $f' - 2\theta'$ divides w. Set $d = w/(f' - 2\theta')$ and $t = p^\theta = p^{d\theta'}$. Then, check whether $(h-2)t + 1 \equiv 0 \pmod N$ or $-(h-2)t + 1 \equiv 0 \pmod N$ holds.

We run the above algorithm for all $N < 5000$ using a computer. Note that p is determined as the unique prime factor of $(Nh - (h-2)^2)/(N-1)$ in steps (1) and (2), and f is determined as $f = df'$ in the steps (2) and (3). We find three quadruples (for convenience we give the value of θ also) satisfying the conditions of Corollary 3.2:

$$(p, f, N, \theta) = (7, 7, 29, 3), (13, 13, 53, 6), (2, 36, 247, 15). \tag{4.3}$$

Table 2 Known examples of three-valued Gauss periods

parameters	AP	AS	CW	ref
$p=2, q=p^{6f}, N=\frac{p^{3f}-1}{p^f-1}$	∘	∘	∘	Sect. 4.1
p odd, $q=p^{6f}, N=\frac{p^{3f}-1}{p^f-1}$	∘	×	∘	Sect. 4.1
$q=p^{3f}, N=\frac{p^{3f}-1}{p^f-1}$, $\mathrm{ord}_{3(p^f-1)}(p^f)=3$	∘	∘	×	Sect. 4.3
$q=p^{fe}$, $\frac{p^{fe}-1}{N} \mid p^f-1$, $\frac{(p^f-1)N}{p^{fe}-1} \mid \frac{p^f-1}{p-1}$, $Cay(\mathbb{F}_q, C_0^{(\frac{(p^f-1)N}{p^{fe}-1}, p^f)})$ is an SRG	⋆	∘	×	Sect. 4.2
$q=p^{\mathrm{lcm}(e,f)}=p^{3f}$, $e/\gcd(e,f)=3$, $C_0^{(N,q)}=\mathbb{F}_{p^e}^* \cdot \mathbb{F}_{p^f}^*$	×	∘	×	Sect. 4.4
$N=p_1$, $[\mathbb{Z}_N^*:\langle p\rangle]=2$, $f=e(N-1)/2$ for any $e\in\mathbb{N}$	⋆	∘	×	Sect. 4.5
$N=p_1p_2$, $[\mathbb{Z}_N^*:\langle p\rangle]=2$, $f=\phi(N)/2$	⋆	∘	×	Sect. 4.5

By Theorem 2.7, we obtain three new self-dual three-class association schemes from the three quadruples above. These self-dual three-class association schemes are different from the examples obtained in Sects. 4.3 and 4.5.

As a counterpart of Conjecture 4.4 in [13], we have the following conjecture.

Conjecture 4.6 *Let q be a power of a prime p, γ be a primitive element of $\mathbb{F}_q$, and $N>1$ be a divisor of $q-1$. The Gauss periods $\psi(\gamma^a C_0^{(N,q)})$, $a=0,1,\ldots,N-1$, take exactly three rational values in arithmetic progression, and one of the three values occurs exactly once, if and only if the Gauss periods arise from the examples in* Sect. 4.3*, or from* Example 4.4*, or from one of the sporadic cases listed in* (4.3).

5 Concluding remarks

In this paper, we study the problem of when the Gauss periods take exactly three rational values. Also, we give constructions of related combinatorial structures such as circulant weighing matrices and association schemes.

We have found five infinite classes of three-valued Gauss periods listed in Table 2. (The meaning of "AP," "AS" are the same as in Table 1. Here "CW" indicates whether I_1-I_3 gives a circulant weighing matrix or not. The symbols "⋆" means that the class includes some examples satisfying the condition.) Furthermore, we obtained several sporadic examples of three-valued Gauss periods as given in Sect. 4.6.

We conclude the paper by listing some problems for future work.

- Classify all triples (p, f, N) which lead to three-valued Gauss periods. A less challenging task is to find other infinite classes of three-valued Gauss periods not listed in Table 2.

- Determine when three-valued Gauss periods take three values in arithmetic progression. (Then, by Proposition 2.6 one will be able to characterize when $I_1 - I_3$ forms a circulant weighing matrix.)
- Determine when the index sets I_1, I_2, I_3 yield a three-class association scheme if the Gauss periods take exactly three values.

Acknowledgments The authors would like to thank both reviewers for their comments and constructive suggestions. In particular, we thank one of the reviewers who gave a short proof of Theorem 2.7, which is the proof presented here in this paper.

References

1. Baumert, L.D., McEliece, R.J.: Weights of irreducible cyclic codes. Inf. Control **20**, 158–175 (1972)
2. Berndt, B., Evans, R., Williams, K.S.: Gauss and Jacobi sums. Wiley, New York (1997)
3. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 18. Springer, Berlin (1989)
4. Evans, R., Hollmann, H.D.L., Krattenthaler, C., Xiang, Q.: Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets. J. Comb. Theory (A) **87**, 74–119 (1999)
5. Feng, T.: On cyclic codes of length 2^{2^r-1} with two zeros whose dual codes have three weights. Des. Code Cryptogr. **62**, 253–258 (2012)
6. Feng, T., Xiang, Q.: Strongly regular graphs from union of cyclotomic classes. J. Comb. Theory (B) **102**, 982–995 (2012)
7. Feng, T., Xiang, Q.: Cyclotomic constructions of skew Hadamard difference sets. J. Comb. Theory (A) **119**, 245–256 (2012)
8. Feng, T., Momihara, K.: Three-class association schemes from cyclotomy. J. Comb. Theory (A) **120**, 1202–1215 (2013)
9. Feng, T., Momihara, K., Xiang, Q.: Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes. Combinatorica **35**, 413–434 (2015)
10. Jungnickel, D., Vedder, K.: On the geometry of planar difference sets. Eur. J. Comb. **5**, 143–148 (1984)
11. McEliece, R.J.: Irreducible cyclic codes and Gauss sums. Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: theory of designs, finite geometry and coding theory. In: Math. Centre Tracts, vol. 55. Math. Centrum, Amsterdam, pp.179–196 (1974)
12. Pott, A.: Finite Geometry and Character Theory. Springer, Berlin (1995)
13. Schmidt, B., White, C.: All two-weight irreducible cyclic codes? Finite Fields Appl. **8**, 1–17 (2002)
14. Wallis, J.S., Whiteman, A.L.: Some results on weighing matrices. Bull. Aust. Math. Soc. **12**, 433–447 (1975)
15. Yang, J., Xia, L.: Complete solving of explicit evaluation of Gauss sums in the index 2 case. Sci. China Ser. A **53**, 2525–2542 (2010)