Gauss periods and related Combinatorics

Koji Momihara (Kumamoto University)

momihara@educ.kumamoto-u.ac.jp

23-01-2015
A character $\psi$ of $G$ is a homomorphism from $G$ to $\mathbb{C}^*$. 

$\widehat{G}$: the set of all characters of $G$

e: the exponent of $G$

**Remark**

The image of $\psi$ is an $e$th root of unity since

$$\psi(x)^e = \psi(x^e) = \psi(1_G) = 1.$$ 

Note that $\psi(1_G) = 1$ by $\psi(1_G)^2 = \psi(1_G)$. 
### Remark

- Define $\psi_0(g) := 1$ for $\forall g \in G$. Then $\psi_0$ is a character, called the **trivial character**.
- Define $\psi^{-1}(g) := \psi(g)^{-1}$ for a character $\psi$. Then $\psi^{-1}$ is a character, called the **inverse** of $\psi$.
- Define $\psi_1 \psi_2(g) := \psi_1(g) \psi_2(g)$ for characters $\psi_1, \psi_2$. Then $\psi_1 \psi_2$ is a character.

### Theorem

The set $\widehat{G}$ forms a group isomorphic to $G$. 

---

Koji Momihara (Kumamoto University)

Gauss periods and related Combinatorics
Example: $\mathbb{Z}_3$

Possible cases:

$$
\psi((0, 1, 2)) = (1, 1, 1), (1, 1, \omega), (1, 1, \omega^2), (1, \omega, 1), (1, \omega^2, 1), \\
(1, \omega, \omega), (1, \omega, \omega^2), (1, \omega^2, \omega^2), (1, \omega^2, \omega).
$$

By noting that

$$
\psi(1)\psi(2) = \psi(1 + 2) = \psi(0) = 1,
$$

Only $\psi((0, 1, 2)) = (1, 1, 1), (1, \omega, \omega^2), (1, \omega^2, \omega)$ are possible. These three are all characters of $\mathbb{Z}_3$. 
Orthogonal relations

Theorem

(1) For $\psi, \psi' \in \widehat{G}$,

$$\sum_{g \in G} \psi(g)\psi'(g) = \delta_{\psi_1,\psi_2}|G|,$$

where $\delta_{\psi,\psi'} = \begin{cases} 1 & \text{if } \psi = \psi', \\ 0 & \text{if } \psi \neq \psi'. \end{cases}$

(2) For $g, h \in G$,

$$\sum_{\psi \in \widehat{G}} \psi(g)\psi(h) = \delta_{g,h}|G|.$$

where $\delta_{g,h} = \begin{cases} 1 & \text{if } g = h, \\ 0 & \text{if } g \neq h. \end{cases}$
Orthogonal relations

Proof of (1): Put $\phi = \psi \psi'^{-1}$.

If $\phi = \psi_0$, 

$$
\sum_{g \in G} \phi(g) = \sum_{g \in G} 1 = |G|.
$$

If $\phi \neq \psi_0$, 

$$
\phi(g') \sum_{g \in G} \phi(g) = \sum_{g \in G} \phi(g') \phi(g) = \sum_{g \in G} \phi(g'g) = \sum_{g \in G} \phi(g),
$$

which implies that $\sum_{g \in G} \phi(g) = 0$. 

Koji Momihara (Kumamoto University)  Gauss periods and related Combinatorics
Definition: Cayley graph

\[ G \]: a finite abelian group
\[ D \]: an inverse-closed subset of \( G \) \((0 \notin D \) and \( D = -D)\)
\[ E := \left\{ (x, y) \mid x, y \in G, x - y \in D \right\} \]

\((G, E)\) is called a Cayley graph, denoted by \( \text{Cay}(G, D) \).

\( D \) is called the connection set of \((G, E)\).
$G = \mathbb{Z}_3 \times \mathbb{Z}_3$, $D = \{(0, 1), (0, 2), (2, 1), (1, 2)\}$
Eigenvalues of Cayley graphs

$\Gamma$: a Cayley graph on an abelian group $G$ with connection set $D$

$\widehat{G}$: the character group of $G$

$M$: the character table of $G$. (Each of rows and columns are labeled by the elements of $\widehat{G}$ and the elements of $G$, respectively. The $(\psi, g)$-entry is defined by $\psi(g)$.)

$A$: the adjacency matrix of $\Gamma$ (Each row and column are labeled similar to the columns of $M$.)

**Theorem: Eigenvalues and character sums**

$$\frac{MAM^T}{|G|} = \text{diag}\left(\sum_{x \in D} \psi(x)\right)_{\psi \in \widehat{G}},$$

i.e., the eigenvalues of $A$ are given by $\psi(D)$, $\psi \in \widehat{G}$. 
Proof

$$\langle \mathbf{M} \mathbf{M}^T \rangle_{\psi, \psi'} = \sum_{h \in G} \psi(h) \psi'(h) = \sum_{h \in G} \psi \psi'^{-1}(h) = \begin{cases} |G| & \text{if } \psi = \psi', \\ 0 & \text{if } \psi \neq \psi', \end{cases}$$

This implies that $\mathbf{M}/ \sqrt{|G|}$ is an orthogonal matrix. By

$$(\mathbf{M} \mathbf{A})_{\psi, g} = \sum_{h \in G; h-g \in D} \psi(h) = \sum_{e \in D} \psi(e + g),$$

we have

$$\langle \mathbf{M} \mathbf{A} \mathbf{M}^T \rangle_{\psi, \psi'} = \sum_{g \in G} \sum_{e \in D} \psi(e + g) \psi'(g) = \sum_{e \in D} \psi(e) \sum_{g \in G} \psi(g) \psi'(g)$$

$$= \sum_{e \in D} \psi(e) \sum_{g \in G} \psi \psi'^{-1}(g)$$

$$= \begin{cases} |G| \sum_{e \in D} \psi(e) & \text{if } \psi = \psi', \\ 0 & \text{if } \psi \neq \psi'. \end{cases}$$
\( \mathbb{F}_q \): the finite field of order \( q \)
\( \mathbb{F}_q^* \): the multiplicative group of \( \mathbb{F}_q \)
\( C \leq \mathbb{F}_q^* \) s.t. \( C = -C \)

Each coset (called a **cyclotomic coset**) of \( \mathbb{F}_q^*/C \) is expressed as

\[
C_i^{(N,q)} = \gamma^i \langle \gamma^N \rangle, \quad 0 \leq i \leq N - 1,
\]

where \( N \mid q - 1 \) is a positive integer and \( \gamma \) is a fixed primitive element of \( \mathbb{F}_q \).
Characters of finite fields

There are two kinds of characters for finite fields, which are additive characters and multiplicative characters.

**Lemma**

For a fixed primitive element $\gamma \in \mathbb{F}_q$, $\chi_j : \mathbb{F}_q^* \rightarrow \mathbb{C}^*$, $0 \leq j \leq q - 2$, defined by

$$
\chi_j(\gamma^k) := \zeta_{q-1}^{jk}
$$

are all multiplicative characters of $\mathbb{F}_q^*$, where $\zeta_{q-1} = e^{\frac{2\pi i}{q-1}}$.

Define the trace $\text{Tr}_{q^m/q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ by

$$
\text{Tr}_{q^m/q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}},
$$

which is a homomorphism from $(\mathbb{F}_{q^m}, +)$ to $(\mathbb{F}_q, +)$.
The function $\psi_j : \mathbb{F}_q \to \mathbb{C}^*$, $j \in \mathbb{F}_q$, defined by

$$\psi_j(x) = \zeta_p^{\text{Tr}_{q/p}(jx)}$$

are all additive characters of $\mathbb{F}_q$.

It holds that $\psi_j(x + y) = \psi_j(x)\psi_j(y)$ since $\text{Tr}$ is a homomorphism from $\mathbb{F}_q$ to $\mathbb{F}_p$.

$\psi_1$ is called canonical.

Note that $\psi_a(x) = \psi_1(ax)$ and $\psi(x) = \psi(-x)$. 
Gauss sums

**Definition**

For the canonical additive character \( \psi \) of \( \mathbb{F}_q \) and a nontrivial multiplicative character \( \chi \) of \( \mathbb{F}_q \), the sum

\[
G(\chi) := \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x)
\]

is called a **Gauss sum**.

**Lemma**

For any nontrivial multiplicative character \( \chi \) of \( \mathbb{F}_q \),

\[
G(\chi)\overline{G(\chi)} = q.
\]

The lemma above implies that \( |G(\chi)| = \sqrt{q} \).
\[ G(\chi)G(\chi) = q \]

Proof:

\[
\begin{align*}
G(\chi)G(\chi) &= \sum_{x, y \in \mathbb{F}_q^*} \psi(x)\psi(-y)\chi(x)\chi^{-1}(y) \\
&= \sum_{x, y \in \mathbb{F}_q^*} \psi(x - y)\chi(xy^{-1}).
\end{align*}
\]

(1)

Write \( z = xy^{-1} \). Then,

\[
\begin{align*}
(1) &= \sum_{y, z \in \mathbb{F}_q^*} \chi(z)\psi(y(z - 1)) \\
&= \sum_{z \in \mathbb{F}_q^*} \chi(z) \sum_{y \in \mathbb{F}_q} \psi(y(z - 1)) - \sum_{z \in \mathbb{F}_q^*} \chi(z) = q.
\end{align*}
\]
For the canonical additive character $\psi$ of $\mathbb{F}_q$,

$$\eta_i := \sum_{x \in C_i^{(N,q)}} \psi(x), \quad 0 \leq i \leq N - 1,$$

are called Gauss periods of order $N$ of $\mathbb{F}_q$.

Gauss periods are all eigenvalues of $\text{Cay}(\mathbb{F}_q, C_i^{(N,q)})$. 
Lemma: Gauss periods and Gauss sums

(i) \[ \psi(C_i^{(N,q)}) = \frac{1}{N} \sum_{h=0}^{N-1} G(\chi^h)\chi^{-h}(\gamma^i), \]

(ii) \[ G(\chi) = \sum_{i=0}^{N-1} \psi(C_i^{(N,q)})\chi(\gamma^i), \]

where \( \chi \) is a multiplicative character of order \( N \) of \( \mathbb{F}_q \).
Eigenvalues of cyclotomic schemes

\[ \psi(C_i^{(N,q)}) = \frac{1}{N} \sum_{x \in \mathbb{F}_q^*} \psi(\gamma^i x^N) = \frac{1}{N} \sum_{x \in \mathbb{F}_q^*} \frac{1}{q-1} \sum_{y \in \mathbb{F}_q^*} \psi(y) \sum_{\chi \in \mathbb{F}_q^*} \chi(\gamma^i x^N) \overline{\chi(y)} = \frac{1}{(q-1)N} \sum_{x \in \mathbb{F}_q^*} \sum_{\chi \in \mathbb{F}_q^*} G(\chi^{-1}) \chi(\gamma^i x^N) = \frac{1}{(q-1)N} \sum_{\chi \in \mathbb{F}_q^*} G(\chi^{-1}) \chi(\gamma^i) \sum_{x \in \mathbb{F}_q^*} \chi(x^N) = \frac{1}{N} \sum_{\chi \in C_{0}^\perp} G(\chi^{-1}) \chi(\gamma^i), \]

where \( C_{0}^\perp \) is the subgroup of \( \mathbb{F}_q^* \) consisting of all \( \chi \) trivial on \( C_{0}^{(N,q)} \).

Koji Momihara (Kumamoto University)  Gauss periods and related Combinatorics
Evaluating Gauss sums

- **(Small order)** Gauss sums of order $N \leq 24$ have been partially evaluated (Berndt et al., 1997).

- **(Purenness)** When Gauss sums take the form $\zeta_N \sqrt{q}$ was determined (Aoki, 2004, 2012). In particular, if $-1 \in \langle p \rangle \pmod{N}$, then $G(\chi_N)$ takes a rational value (Baumert et al., 1982).

- **(Index 2 or 4 case)** In the case where $[\mathbb{Z}_N^* : \langle p \rangle] = 2$, Gauss sums have been completely evaluated (Yang et al., 2010). In the case where $[\mathbb{Z}_N^* : \langle p \rangle] = 4$, Gauss sums have been partially evaluated (Feng et al., 2005).
The computation of Gauss periods is equivalent to that of weight distributions of certain cyclic codes, called irreducible cyclic codes.

Two-weight irreducible cyclic code is related to the problem of finding cyclic difference sets in design theory.

Gauss periods are eigenvalues of cyclotomic schemes.

A 2-class fusion (strongly regular graph) of a cyclotomic scheme is related to the problem of finding two-intersection sets in finite projective geometry.
Cyclic codes

An \((m, r)\)-code \(C\) is an \(r\)-dimensional subspace of \(\mathbb{F}_q^m\). If \((c_{m-1}, c_0, \ldots, c_{m-2}) \in C\) for any \((c_0, c_1, \ldots, c_{m-1}) \in C\), then \(C\) is called cyclic.

One may identify each vector \((c_0, c_1, \ldots, c_{m-1}) \in \mathbb{F}_p^m\) with \(h(x) \in \mathbb{F}_p[x]\) s.t.

\[
h(x) \equiv \sum_{i=0}^{m-1} c_i x^i \pmod{x^m - 1}
\]

by using the isomorphism between the principal ideal ring \(A := \mathbb{F}_p[x]/(x^m - 1)\mathbb{F}_p[x]\) and \(\mathbb{F}_p^m\).

Note that every ideal of \(A\) is given by \(Ag(x)\) for some \(g(x) \mid x^m - 1\). If \(deg(g(x)) = m - r\), then \(C = Ag(x)\) forms a cyclic \((m, r)\)-code.
Irreducible cyclic codes

**Definition: Irreducible cyclic code**

\( f(x) \): an irreducible divisor of \( x^m - 1 \in \mathbb{F}_p[x] \), where \( \gcd(m, p) = 1 \).

The cyclic code of length \( m \) over \( \mathbb{F}_p \) generated by \( (x^m - 1)/f(x) \) is called an *irreducible cyclic code*. (This code has no proper cyclic subcodes.)

- \( f \): the order of \( p \) modulo \( m \)
- \( q := p^f = 1 + km \)
- \( \gamma \): a primitive root of \( \mathbb{F}_q \)
- \( f(x) := \prod_{i=0}^{f-1} (x - \gamma^{kp^i}) \in \mathbb{F}_p[x] \) irreducible over \( \mathbb{F}_p \)
- \( g(x) := \prod_{\ell \in S} (x - \gamma^{k\ell}) \), where

\[
S = \{ \ell | 0 \leq \ell \leq m - 1, \ell \not\equiv \text{a power of } p \pmod{m} \}.
\]
Lemma

$C$: the cyclic code generated by $g(x)$
The $q$ codewords in $C$ are given by

\[
\overline{h_\alpha(x)} := (\text{Tr}(\alpha), \text{Tr}(\alpha \gamma^{-k}), \text{Tr}(\alpha \gamma^{-2k}), \ldots, \text{Tr}(\alpha \gamma^{-(m-1)k})), \quad \alpha \in \mathbb{F}_q.
\]

Proof:

\[
h_\alpha(x) := \sum_{j=0}^{m-1} \text{Tr}(\alpha \gamma^{-jk})x^j, \quad \alpha \in \mathbb{F}_q.
\]

For any $\ell \in S$,

\[
h_\alpha(\gamma^{k\ell}) = \sum_{j=0}^{m-1} \text{Tr}_{q/p}(\alpha \gamma^{-jk})\gamma^{k\ell j} = \sum_{i=0}^{f-1} \alpha^{p^i} \sum_{j=0}^{m-1} \gamma^{jk(\ell-p^i)} = 0.
\]

Hence, $g(x) | h_\alpha(x)$, i.e., $\overline{h_\alpha(x)} \in C$. 
Since $|C| = q$, it remains to show that $h_\alpha(x)$ are all distinct. Assume $h_\alpha(x) = h_\beta(x)$. Then, for $\omega := \alpha - \beta \in \mathbb{F}_q$

$$\text{Tr}(\omega) = \text{Tr}(\omega \gamma^{-k}) = \text{Tr}(\omega \gamma^{-2k}) = \cdots = \text{Tr}(\omega \gamma^{-(m-1)k}) = 0.$$ 

For any choice of $a_j \in \mathbb{F}_p$,

$$0 = \sum_{j=0}^{f-1} a_j \text{Tr}(\omega \gamma^{-jk}) = \text{Tr}(\omega \sum_{j=0}^{f-1} a_j \gamma^{-jk}).$$

Since $\{1, \gamma^{-k}, \ldots, \gamma^{-(f-1)k}\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, the above is impossible. \qed
Theorem (McEliece)  

Let $N := \gcd (k, (q - 1)/(p - 1))$. Then,

$$w(h_\alpha(x)) = \frac{m(p - 1)}{p} - \frac{p - 1}{pk} \psi (\alpha C_0^{(N,p^f)}).$$

Proof: Let $\chi$ be a mult. character of order $k$ of $\mathbb{F}_q$.

$$w(h_\alpha(x)) = m - \frac{1}{p} \sum_{i=0}^{m-1} \sum_{x \in \mathbb{F}_p} \psi (x \alpha \gamma^{ki})$$

$$= \frac{m(p - 1)}{p} - \frac{1}{p} \sum_{i=0}^{m-1} \sum_{x \in \mathbb{F}_p^*} \psi (x \alpha \gamma^{ki})$$

$$= \frac{m(p - 1)}{p} - \frac{1}{pk} \sum_{j=0}^{k-1} \sum_{x \in \mathbb{F}_p^*} G(\chi^{-j}) \chi^j (x \alpha).$$
Since for any \( y \in \mathbb{F}_p^* \)

\[
\sum_{x \in \mathbb{F}_p^*} \chi^j(x) = \sum_{x \in \mathbb{F}_p^*} \chi^j(yx) = \chi^j(y) \sum_{x \in \mathbb{F}_p^*} \chi^j(x),
\]

\[
\sum_{x \in \mathbb{F}_p^*} \chi^j(x) = 0 \text{ iff } \chi^j \text{ is nontrivial on } \mathbb{F}_p^*.
\]

Let \( \chi' \) be a mult. character of order \( N \) of \( \mathbb{F}_q \). Then,

\[
w(h_{\chi}(x)) = \frac{m(p - 1)}{p} - \frac{p - 1}{pk} \sum_{j=0}^{N-1} G(\chi'^{-j}) \chi'^j(\alpha)
\]

\[
= \frac{m(p - 1)}{p} - \frac{p - 1}{pk} \psi(\alpha C(N,p^f)_0).
\]

Problem

Characterize all two or three weight irreducible cyclic codes.
Two-valued Gauss periods

Two-valued Gauss period was studied by Schmidt-White (2002). In this case, $Cay(\mathbb{F}_{p^f}, C_{0}^{(N,p^f)})$ has exactly two nontrivial eigenvalues, i.e., it is strongly regular.

Theorem (Schmidt-White, 2002)

Assume that $N | \frac{p^f - 1}{p - 1}$.
Then, Gauss periods take exactly two values iff $\exists k \in \mathbb{N}$ s.t.

(i) $k | N - 1$

(ii) $kp^{s\theta} \equiv \pm 1 \pmod{N}$,

(iii) $k(N - k) = (N - 1)p^{s(m - 2\theta)}$,

where $f = ms$, $m = \text{ord}_N(p)$, and $p^\theta \parallel G_{p^m}(\chi) = \sum_{x \in \mathbb{F}_{p^m}} \chi(x)\psi(x)$ for all nontrivial multiplicative characters $\chi$ of exponent $N$ of $\mathbb{F}_{p^f}$.
Conjecture (Schmidt-White, 2002)

Assume that \( N \mid \frac{p^f - 1}{p - 1} \). If Gauss periods take exactly two values, either one of the following holds.

- (subfield case) \( C^{(N,p^f)}_0 = \mathbb{F}_p^* \) where \( e \mid f \),
- (semi-primitive case) \(-1 \in \langle p \rangle \leq \mathbb{Z}_N^*\),
- (exceptional case) it has either of the following parameters:

<table>
<thead>
<tr>
<th>No.</th>
<th>( N )</th>
<th>( p )</th>
<th>( f )</th>
<th>No.</th>
<th>( N )</th>
<th>( p )</th>
<th>( f )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>107</td>
<td>3</td>
<td>53</td>
</tr>
<tr>
<td>2</td>
<td>19</td>
<td>5</td>
<td>9</td>
<td>8</td>
<td>133</td>
<td>5</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>35</td>
<td>3</td>
<td>12</td>
<td>9</td>
<td>163</td>
<td>41</td>
<td>81</td>
</tr>
<tr>
<td>4</td>
<td>37</td>
<td>7</td>
<td>9</td>
<td>10</td>
<td>323</td>
<td>3</td>
<td>144</td>
</tr>
<tr>
<td>5</td>
<td>43</td>
<td>11</td>
<td>7</td>
<td>11</td>
<td>499</td>
<td>5</td>
<td>249</td>
</tr>
<tr>
<td>6</td>
<td>67</td>
<td>17</td>
<td>33</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Definition: abelian difference set

\( G \): an abelian group of order \( v \)

A \( k \)-subset \( D \subseteq G \) is called a \((v, k, \lambda)\) difference set (DS) if

\[
\{xy^{-1} \mid x, y \in D; x \neq y\}
\]

covers every nonzero element of \( G \) exactly \( \lambda \) times.

Note that \( D \) is a difference set in \( G \) iff

\[
DD^{(-1)} = (k - \lambda) \cdot [1_G] + \lambda \cdot G,
\]

i.e.,

\[
\chi(D)\chi^{-1}(D) = k - \lambda
\]

for any nontrivial character \( \chi \) of \( G \).
Assume that $\psi(C_a^{(N,q)})(= \psi(\gamma^a C_0^{(N,q)}))$, $a = 0, 1, \ldots, N - 1$, take exactly two values, say $\alpha_1$ and $\alpha_2$. Set

$$I_i = \{a \mid \psi(\gamma^a C_0^{(N,q)}) = \alpha_i, \ 0 \leq a \leq N - 1\}, \ i = 1, 2.$$

$I_i$ forms a difference set in $\mathbb{Z}_N$, called a *subdifference set*. Why?
Then,

\[ G_q(\chi) = \alpha_1 \sum_{a \in I_1} \chi(\gamma^a) + \alpha_2 \sum_{a \in I_2} \chi(\gamma^a) = (\alpha_1 - \alpha_2) \sum_{a \in I_1} \chi(\gamma^a). \]

By \( G_q(\chi)G_q(\chi^{-1}) = q \),

\[ \left( \sum_{a \in I_1} \chi(\gamma^a) \right) \left( \sum_{a \in I_1} \chi^{-1}(\gamma^a) \right) \]

is constant, i.e., \( I_1 \) is a difference set in \( \mathbb{Z}_N \).
Subdifference sets

In subfield case, the corresponding subdifference sets are the **Singer difference sets**. In the sporadic case, the corresponding subdifference sets are listed below:

<table>
<thead>
<tr>
<th>No.</th>
<th>$v$</th>
<th>$k$</th>
<th>$\lambda$</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>5</td>
<td>2</td>
<td>Quadratic residue DS</td>
</tr>
<tr>
<td>2</td>
<td>19</td>
<td>9</td>
<td>4</td>
<td>Quadratic residue DS</td>
</tr>
<tr>
<td>3</td>
<td>35</td>
<td>17</td>
<td>8</td>
<td>Twin-prime DS</td>
</tr>
<tr>
<td>4</td>
<td>37</td>
<td>9</td>
<td>2</td>
<td>Biquadratic residue DS</td>
</tr>
<tr>
<td>5</td>
<td>43</td>
<td>21</td>
<td>10</td>
<td>Hall’s sextic DS</td>
</tr>
<tr>
<td>6</td>
<td>67</td>
<td>33</td>
<td>16</td>
<td>Quadratic residue DS</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>53</td>
<td>26</td>
<td>Quadratic residue DS</td>
</tr>
<tr>
<td>8</td>
<td>133</td>
<td>33</td>
<td>8</td>
<td>Hall’s sporadic DS</td>
</tr>
<tr>
<td>9</td>
<td>163</td>
<td>81</td>
<td>40</td>
<td>Quadratic residue DS</td>
</tr>
<tr>
<td>10</td>
<td>323</td>
<td>161</td>
<td>80</td>
<td>Twin-prime DS</td>
</tr>
<tr>
<td>11</td>
<td>499</td>
<td>249</td>
<td>124</td>
<td>Quadratic residue DS</td>
</tr>
</tbody>
</table>
Definition: Translation scheme

\( \Gamma_i := (G, E_i), \ 1 \leq i \leq d \): Cayley graphs on an abelian group \( G \)

\( R_i \): connection sets of \((G, E_i)\)

\( R_0 := \{0\} \).

\((G, \{R_i\}_{i=0}^d)\) is called a \textit{translation scheme} (TS)
if \((G, \{\Gamma_i\}_{i=0}^d)\) is an association scheme (AS).

In other words...

- \( \bigcup_{i=0}^d R_i = G, \ R_i \cap R_j = \emptyset \)
- \(|\{z \mid (x, z) \in E_i, (y, z) \in E_j\}| \) is const. according to \( \ell \) s.t. 
  \((x, y) \in E_\ell \).
  \( \Leftrightarrow |\{z \mid x - z \in R_i, y - z \in R_j\}| \) is const. according to \( \ell \) s.t. 
  \( x - y \in R_\ell \).
  \( \Leftrightarrow |(R_i + x - y) \cap R_j| \) is const. according to \( \ell \) s.t. \( x - y \in R_\ell \).
  \( \Leftrightarrow |(R_i + w) \cap R_j| \) is constant according to \( \ell \) s.t. \( w \in R_\ell \).
Dual of translation schemes

\[ R_0 = \{0\}, \; R_1, R_2, \ldots, R_d: \text{an (inverse-closed) partition of } G \]

This partition induces a partition \( S_0 = \{\psi_0\}, S_1, S_2, \ldots, S_e, \) of \( \tilde{G} \): \( \psi, \phi \in \tilde{G} \setminus \{\psi_0\} \) are in the same \( S_j \) iff \( \psi(R_i) = \phi(R_i) \) for \( 1 \leq \forall i \leq d \).

**Theorem (Bridges-Mena, 1982)**

It holds that \( d \leq e \). In particular, \((G, \{R_i\}_{i=0}^d)\) forms a TS iff \( d = e \).

<table>
<thead>
<tr>
<th>( R_0 )</th>
<th>( R_1 )</th>
<th>( R_2 )</th>
<th>( R_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \psi_0 \in S_0 )</td>
<td>1</td>
<td>(</td>
<td>R_1</td>
</tr>
<tr>
<td>( \psi \in S_1 )</td>
<td>1</td>
<td>( a_1 )</td>
<td>( a_2 )</td>
</tr>
<tr>
<td>( \psi' \in S_2 )</td>
<td>1</td>
<td>( b_1 )</td>
<td>( b_2 )</td>
</tr>
<tr>
<td>( \psi'' \in S_3 )</td>
<td>1</td>
<td>( c_1 )</td>
<td>( c_2 )</td>
</tr>
</tbody>
</table>

If \((G, \{R_i\}_{i=0}^d)\) forms a TS, then so does \((\tilde{G}, \{S_i\}_{i=0}^d)\), which is called the **dual** of \((G, \{R_i\}_{i=0}^d)\). \(|G|P^{-1}\) is the first eigenmatrix of \((\tilde{G}, \{S_i\}_{i=0}^d)\) for the first eigenmatrix \(P\) of \((G, \{R_i\}_{i=0}^d)\).
Cyclotomic scheme

\( \mathbb{F}_q \): the finite field of order \( q \)
\( \mathbb{F}_q^* \): the multiplicative group of \( \mathbb{F}_q \)
\( C \subseteq \mathbb{F}_q^* \) s.t. \( C = -C \)

**Lemma: Cyclotomic scheme**

The partition \( \mathbb{F}_q^*/C \) of \( \mathbb{F}_q^* \) gives a TS on \((\mathbb{F}_q, +)\), called a cyclotomic scheme.

Each coset (called a cyclotomic coset) of \( \mathbb{F}_q^*/C \) is expressed as

\[
C_i^{(N,q)} = \gamma^i \langle \gamma^N \rangle, \quad 0 \leq i \leq N - 1,
\]

where \( N \mid q - 1 \) is a positive integer and \( \gamma \) is a fixed primitive element of \( \mathbb{F}_q \).

For \( w \in C_i^{(N,q)} \),

\[
p_{i,j}^\ell = \left| (C_i^{(N,q)} + w) \cap C_j^{(N,q)} \right| = \left| (C_{i-\ell}^{(N,q)} + 1) \cap C_{j-\ell}^{(N,q)} \right|.
\]

Hence, \( p_{i,j}^\ell \) is depending on \( \ell \) not \( w \).
Given a \( d \)-class AS \( (X, \{R_i\}_{i=0}^d) \), we can take union of classes to form graphs with larger edge sets (this process is called a fusion).

**Big problem!**

Given an \( N \)-class cyclotomic scheme on \( \mathbb{F}_q \), determine its fusion schemes.

\( X_j, j = 1, 2, \ldots, d \): a partition of \( \mathbb{Z}_N \)

The Bridges-Mena theorem (more generally, the Bannai-Muzychuk criterion) implies that \( \bigcup_{i \in X_j} C_i^{(N,q)} \)'s forms a TS iff \( \exists \) a partition \( Y_h, h = 1, 2, \ldots, d \), of \( \mathbb{Z}_N \) s.t. each \( \psi(\gamma^a \bigcup_{i \in X_j} C_i^{(N,q)}) \) is const. according to \( a \in Y_h \).
We consider 2-class fusion schemes (strongly regular graphs) of a cyclotomic scheme of order \( N = \frac{q^m - 1}{q-1} \).

**Proposition**

Let \( \chi \) be a mult. character of order \( N \) of \( \mathbb{F}_{q^m} \). Let \( S_0 := \{ \log x \pmod{N} \mid \text{Tr}_{q^m/q}(x) = 0, x \neq 0 \} \). Then,

\[
G(\chi) = q \sum_{i \in S_0} \chi(\omega^i).
\]

\( L := \) a system of representatives of \( \mathbb{F}^*_{q^m}/\mathbb{F}^*_q \).

\[
G(\chi) = \sum_{a \in \mathbb{F}^*_q} \sum_{x \in L} \chi(xa) \zeta_p^{\text{Tr}_{q^m/p}(xa)} = \sum_{x \in L} \chi(x) \sum_{a \in \mathbb{F}^*_q} \zeta_p^{\text{Tr}_{q/p}(a \text{Tr}_{q^m/q}(x))}
\]

\[
=(q - 1) \sum_{i \in S_0} \chi(\gamma^i) - \sum_{i \in L \setminus S_0} \chi(\gamma^i) = q \sum_{i \in S_0} \chi(\gamma^i).
\]
Geometric understanding

$X$: a subset of $\mathbb{Z}_N$
When is $\Gamma = \text{Cay}(\bigcup_{i \in X} C_i^{(N,q^m)})$ strongly regular?
($\Gamma$ is strongly regular iff $\psi(\gamma^a \bigcup_{i \in X} C_i^{(N,q^m)}), a = 0, 1, \ldots, N - 1,$
take exactly two values.)

\[
\psi(\gamma^a \bigcup_{i \in X} C_i^{(N,q^m)}) = \frac{1}{N} \sum_{i \in X} \sum_{\chi \neq \chi_0} G(\chi^{-1})\chi(\gamma^{a+i}) - \frac{|X|}{N}
\]
\[
= \frac{q}{N} \sum_{\chi} \sum_{i \in X} \sum_{j \in S_0} \chi(\gamma^{a+i-j}) - \frac{|X|(1 + q|S_0|)}{N}
\]
\[
= q|X \cap (S_0 - a)| - |X|,
\]

where $\chi$ ranges through all mult. characters of exponent $N$ of $\mathbb{F}_{q^m}$. 

Koji Momihara (Kumamoto University)  Gauss periods and related Combinatorics
Geometric understanding

Proposition (Delsarte, 1972)

\[ \text{Cay}(\bigcup_{i \in X} C_i^{(N,q^m)}) \text{ is strongly regular iff } |X \cap (S_0 - a)|, a \in \mathbb{Z}_N, \text{ take exactly two values.} \]

What is \( S_0 - a \)?

Consider the \((m - 1)\)-dimensional projective space \( \text{PG}(m - 1, q) \) on the point set \( \mathbb{Z}_N \cong \mathbb{F}_q^* / \mathbb{F}_q^* \). All hyperplanes \((m - 1)\)-dimensional subspaces of \( \mathbb{F}_q^m \) of \( \text{PG}(m - 1, q) \) are given by \( S_0 - a, a \in \mathbb{Z}_N \).
Problem

Find a subset $X$ of $\text{PG}(m - 1, q)$, which has two intersection numbers with the hyperplanes of $\text{PG}(m - 1, q)$. 
($X$ is called a two-intersection set in $\text{PG}(m - 1, q)$.)

See Calderbank-Kantor (1986) for more on the geometric aspect of strongly regular graphs on $\mathbb{F}_q$. 

Koji Momihara (Kumamoto University) 
Gauss periods and related Combinatorics
Problems on three-valued Gauss periods

<table>
<thead>
<tr>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Necessary condition</td>
</tr>
<tr>
<td>Sufficient condition</td>
</tr>
<tr>
<td>Examples</td>
</tr>
<tr>
<td>Related combinatorial structures.</td>
</tr>
</tbody>
</table>
  - When do the index sets in $\mathbb{Z}_N$ yield an interesting design? 
  - When does the partition of $\mathbb{F}_q$ derived from the index sets form a three-class (translation) association scheme?
Assume that $\psi(\gamma^a C^{(N,q)}_0)$, $a = 0, 1, \ldots, N - 1$, take exactly three values $\alpha_1, \alpha_2, \alpha_3$. Set

$$I_i = \{a \mid \psi(\gamma^a C^{(N,q)}_0) = \alpha_i, 0 \leq a \leq N - 1\}, \ i = 1, 2, 3.$$

By the orthogonality of characters,

$$G_q(\chi) = \alpha_1 \sum_{a \in I_1} \chi(\gamma^a) + \alpha_2 \sum_{a \in I_2} \chi(\gamma^a) + \alpha_3 \sum_{a \in I_3} \chi(\gamma^a)$$

$$= (\alpha_1 - \alpha_2) \sum_{a \in I_1} \chi(\gamma^a) + (\alpha_3 - \alpha_2) \sum_{a \in I_3} \chi(\gamma^a).$$
Designs appeared in the index sets

By $G_q(\chi)G_q(\chi^{-1}) = q$, we have

$$((\alpha_1 - \alpha_2)I_1 + (\alpha_3 - \alpha_2)I_3)((\alpha_1 - \alpha_2)I_1 + (\alpha_3 - \alpha_2)I_3)^{-1} = k[0] + \lambda \mathbb{Z}_N.$$  

Then,

$$A = (\alpha_1 - \alpha_2)I_1 + (\alpha_3 - \alpha_2)I_3 \in \mathbb{Z}[\mathbb{Z}_N]$$

forms a cyclic weighted design.

In particular, if $\alpha_1 - \alpha_2 = \alpha_2 - \alpha_3$, then $A/(\alpha_1 - \alpha_2)$ gives a cyclic balanced ternary design.

Furthermore, if $\lambda = 0$, then $A/(\alpha_1 - \alpha_2)$ gives a circulant weighing matrix.
Designs appeared in the index sets

**Definition: balanced weighted design**

A square matrix $M$ with entries from $\mathbb{Z}$ s.t. $MM^T = (k - \lambda)I + \lambda J$ is called a *weighted design*.

If its entries are from $\{0, 1, -1\}$, it is called a *balanced ternary design*.

Furthermore, if $\lambda = 0$, it is called a *weighing matrix*.

---

<table>
<thead>
<tr>
<th>2 symbols</th>
<th>Difference set</th>
<th>Symmetric design</th>
<th>Hadamard matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 symbols</td>
<td>Circulant balanced ternary design</td>
<td>Balanced ternary design</td>
<td>Weighing matrix</td>
</tr>
</tbody>
</table>
Remarks

\[ |I_1| + |I_2| + |I_3| = N, \]
\[ \alpha_1|I_1| + \alpha_2|I_2| + \alpha_3|I_3| = \sum_{i=0}^{N-1} \psi(C_i) = -1, \]

Since

\[(\alpha_1 I_1 + \alpha_2 I_2 + \alpha_3 I_3)(\alpha_1 I_1^{(-1)} + \alpha_2 I_2^{(-1)} + \alpha_3 I_3^{(-1)}) = q \cdot [0] - \frac{q - 1}{N} \mathbb{Z}_N,\]

by comparing the coefficient of \([0]\) of both sides,

\[ \alpha_1^2|I_1| + \alpha_2^2|I_2| + \alpha_3^2|I_3| = q - \frac{q - 1}{N}. \]

Thus,

\[ |I_1| = -\frac{\alpha_2 \alpha_3 (q - 1) + k (q - k + \alpha_2 + \alpha_3)}{k (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_1)}, \]
\[ |I_2| = -\frac{\alpha_1 \alpha_3 (q - 1) + k (q - k + \alpha_1 + \alpha_3)}{k (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)}, \]
\[ |I_3| = -\frac{\alpha_1 \alpha_2 (q - 1) + k (q - k + \alpha_1 + \alpha_2)}{k (\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)}. \]
Theorem

Assume that $\gcd (p - 1, N) = 1$, and $\psi (\gamma^a C_0^{(N,q)})$,
$a = 0, 1, \ldots, N - 1$, take exactly three values $\alpha_1, \alpha_2, \alpha_3$.
Take the partition of $\mathbb{F}_q$: 

$$R_0 = \{0\}, \quad R_1 = \bigcup_{i \in I_1} C_i^{(N,q)}, \quad R_2 = \bigcup_{i \in I_2} C_i^{(N,q)}, \quad R_3 = \bigcup_{i \in I_3} C_i^{(N,q)},$$

where $I_i = \{a \mid \psi (\gamma^a C_0^{(N,q)}) = \alpha_i\}, \ i = 1, 2, 3$. If $|I_1| = 1$ or $|I_3| = 1$,
then $(\mathbb{F}_q, \{R_i\}_{i=0}^{N-1})$ forms a self-dual 3-class TS.
Let \((p, f, N) = (7, 3, 19)\). Then, the Gauss periods take three values \(\{-3^{12}, 4^6, 11\}\), and we have

\[
I_1 = \{1, 2, 3, 4, 5, 6, 7, 9, 11, 14, 16, 17\}, \\
I_2 = \{8, 10, 12, 13, 15, 18\}, \quad I_3 = \{0\}.
\]

- This satisfies the AP property, i.e., \(I_1 - I_3 \in \mathbb{Z}[\mathbb{Z}_{19}]\) gives a cyclic BT design.
- For

\[
R_0 = \{0\}, \quad R_1 = \bigcup_{i \in I_1} C_i^{(N,q)}, \quad R_2 = \bigcup_{i \in I_2} C_i^{(N,q)}, \quad R_3 = \bigcup_{i \in I_3} C_i^{(N,q)},
\]

\((\mathbb{F}_q, \{R_i\}_{i=0}^{N-1})\) forms a 3-class TS.
We can assume that $|I_1| = 1$, and let $I_1 = \{\ell\}$. Since each $I_j$ is invariant under the multiplication by $p$, we have $\ell = 0$. Then,

$$
\psi(\gamma^a \bigcup_{i \in I_1} C_i^{(N,q)}) = \begin{cases} 
\alpha_1 & \text{if } a \in I_1; \\
\alpha_2 & \text{if } a \in I_2; \\
\alpha_3 & \text{if } a \in I_3.
\end{cases}
$$

Next, we must compute $\psi(\gamma^a \bigcup_{i \in I_2} C_i^{(N,q)})$. 

Koji Momihara (Kumamoto University) 
Gauss periods and related Combinatorics
Sketch of proof

Since the characteristic function $f_2$ of $I_2$ is given by

$$f_2(x) = \frac{(\psi(\gamma^x C_0^{(N,q)}) - \alpha_1)(\psi(\gamma^x C_0^{(N,q)}) - \alpha_3)}{(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)}$$

and $\psi(\gamma^a \bigcup_{i \in I_2} C_i^{(N,q)}) = \sum_{x \in \mathbb{Z}_N} f_2(x)\psi(\gamma^{a+x} C_0^{(N,q)})$, we need to compute

$$\sum_{x \in \mathbb{Z}_N} \psi(\gamma^{x+a} C_0^{(N,q)})\psi(\gamma^x C_0^{(N,q)})^2.$$

Let $\tau(x) = (\psi(\gamma^x C_0^{(N,q)}) - \alpha_2)/t$, where $t = \text{gcd} (\alpha_3 - \alpha_2, \alpha_2 - \alpha_1)$. Then, the above is equivalent to compute

$$\sum_{x \in \mathbb{Z}_N} \tau(x + a)\tau(x)^2.$$
Let \(-u = (\alpha_1 - \alpha_2)/t\) and \(v = (\alpha_3 - \alpha_2)/t\). By \(|I_1| = 1\), we have

\[
\sum_{x \in \mathbb{Z}_N} \tau(x + a)\tau(x) = -ux_1 + \sum_{i=\ell}^{N} vx_i = \begin{cases} 
    k & \text{if } a = 0; \\
    \lambda & \text{if } a \neq 0,
\end{cases}
\]

where \(x_i = -u, 0, \text{ or } v\). \((x_i = -u\) for exactly one \(i\).

\[
\begin{array}{cccccccc}
0\text{th} & -u & 0 & \cdots & 0 & v & v & \cdots & v \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
a\text{th} & x_1 & x_2 & \cdots & x_{\ell-1} & x_\ell & x_{\ell+1} & \cdots & x_N
\end{array}
\]

Then, for \(a \neq 0\) we obtain

\[
\sum_{x \in \mathbb{Z}_N} \tau(x + a)\tau(x)^2 = u^2x_1 + v \sum_{i=\ell}^{N} vx_i = u^2x_1 + v(\lambda + ux_1)
\]

\[
= \begin{cases} 
    v\lambda & \text{if } x_1 = 0, \text{ i.e., } a \in I_2; \\
    v\lambda + v(vu + u^2) & \text{if } x_1 = v, \text{ i.e., } a \in I_3.
\end{cases}
\]
Examples of three-valued Gauss periods

<table>
<thead>
<tr>
<th>No.</th>
<th>parameters</th>
<th>AP</th>
<th>AS</th>
<th>CW</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$p = 2, q = p^{6f}, N = \frac{p^{3f} - 1}{p^f - 1}$</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>2</td>
<td>$p$: odd, $q = p^{6f}, N = \frac{p^{3f} - 1}{p^f - 1}$</td>
<td>○</td>
<td>×</td>
<td>○</td>
</tr>
<tr>
<td>3</td>
<td>$q = p^{3f}, N = \frac{p^{3f} - 1}{3(p^f - 1)}, p^f \equiv 1 \pmod{3}$</td>
<td>○</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>4</td>
<td>$q = p^{fe}, k := \frac{p^{fe} - 1}{N}, k</td>
<td>p^f - 1, \frac{p^f - 1}{k}</td>
<td>\frac{p^f - 1}{p-1}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$Cay(\mathbb{F}_{p^f}, C_0^{(p^f - 1)/3, p^f})$ is an SRG</td>
<td>★</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>5</td>
<td>$q = p^{\text{lcm}(e, f)}, e / \gcd (e, f) = 3, C_0^{(N, q)} = \mathbb{F}^* \cdot \mathbb{F}^{*_{p^e \cdot p^f}}$</td>
<td>×</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>6</td>
<td>$N = p_1, [\mathbb{Z}_N^*, \langle p \rangle] = 2, f = d</td>
<td>\langle p \rangle</td>
<td>$ for any $d$</td>
<td>★</td>
</tr>
<tr>
<td>7</td>
<td>$N = p_1p_2, [\mathbb{Z}_N^* : \langle p \rangle] = 2, f =</td>
<td>\langle p \rangle</td>
<td>$</td>
<td>★</td>
</tr>
</tbody>
</table>
Remark

We searched the existence of three-valued GPs by computer for $q \leq 2^{25}$ with $p < 330$ and $N < 1001$.

- Most of examples with the AS property are covered by our examples, except for $(p, f, N) = (7, 7, 29), (2, 11, 89)$.
- All examples with the CW property are covered by the 1st and 2nd classes.
Open examples

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

Table: Computer search for $p < 330$, $p^f < 2^{25}$, $6 < N < 1001$, $N|\frac{p^f-1}{p-1}$ except for known examples.
Necessary and sufficient condition for a partial case

**Theorem**

Assume that there are four positive integers $u, v, r, s$ satisfying

(i) $t(-ur + vs) \equiv -1 \pmod{N}$;

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

where $t$ is the largest power of $p$ dividing $G_q(\chi)$ for all nontrivial multiplicative characters of exponent $N$.

If $u = v = r = 1$ and $s + 1 < N$, or $u = v = s = 1$ and $r + 1 < N$, then $\psi(\gamma^a C_0^{(N,q)})$, $0 \leq a \leq N - 1$, take exactly three values; in this case, the AP property is satisfied.

This allows us an efficient computer search for $N < 5000$:

Fix $N$ and $h := s + r$. ⇒ Determine $p$ and $f$ by (ii).
⇒ Determine $t$ by Stickelberger’s Thm. ⇒ Check (i).

New examples: $(p, f, N) = (13, 13, 53), (2, 36, 247)$
An analogy of Schmidt-White’s conjecture

Conjecture

If Gauss periods take three values satisfying the AP property and $|I_1| = 1$ or $|I_3| = 1$, either one of the following holds.

(i) $q = p^{3f}$, $N = \frac{p^{3f} - 1}{3(p^f - 1)}$, and $p^f \equiv 1 \pmod{3}$; or

(ii) it has either of the following parameters:

<table>
<thead>
<tr>
<th>No.</th>
<th>$N$</th>
<th>$p$</th>
<th>$f$</th>
<th>No.</th>
<th>$N$</th>
<th>$p$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>55</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>23</td>
<td>2</td>
<td>11</td>
<td>7</td>
<td>67</td>
<td>13</td>
<td>33</td>
</tr>
<tr>
<td>3</td>
<td>29</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>163</td>
<td>43</td>
<td>81</td>
</tr>
<tr>
<td>4</td>
<td>43</td>
<td>13</td>
<td>21</td>
<td>9</td>
<td>187</td>
<td>7</td>
<td>80</td>
</tr>
<tr>
<td>5</td>
<td>53</td>
<td>13</td>
<td>13</td>
<td>10</td>
<td>247</td>
<td>2</td>
<td>36</td>
</tr>
</tbody>
</table>
Examples of three-valued Gauss periods

Theorem

If \( q = p^{6f} \), \( N = \frac{p^{3f} - 1}{p^{f} - 1} \), then GPs take exactly three values. In this case, the index sets form a circulant weighing matrix.

Proof: We need to compute \( G_{p^{6f}}(\chi) \) for a nontrivial character \( \chi \) of exponent \( N \) of \( \mathbb{F}_q \).

By the Hasse-Davenport thm, we have \( G_{p^{6f}}(\chi) = -G_{p^{3f}}(\chi')^2 \) for some character \( \chi' \) of exponent \( N \) of \( \mathbb{F}_p^{3f} \).

Since \( G_{p^{3f}}(\chi') = p^f \sum_{i \in S} \chi'(\gamma^i) \), where \( S = \{i \in \mathbb{Z}_N : \text{Tr}_{3f/f}(\gamma^i) = 0\} \), we need to compute \( S^2 \) in \( \mathbb{Z}[\mathbb{Z}_N] \).
Examples of three-valued Gauss periods

The coefficient of $[a]$ in $S^2$ is equal to the size of

$$\{i \in \mathbb{Z}_N : \text{Tr}_{3f/f}(\gamma^{-i}) = 0, \text{Tr}_{3f/f}(\gamma^{i+a}) = 0\} = Q \cap (S - a),$$

where $Q = \{i \in \mathbb{Z}_N : \text{Tr}_{3f/f}(\gamma^{-i}) = 0\}$. Note that

$$\{x : \text{Tr}_{3f/f}(x^{-1}) = 0\} = \{x : x^{\frac{q^3-1}{q-1}} \text{Tr}_{3f/f}(x^{-1}) = 0\} = \{x : \text{Tr}_{3f/f}(x^{1+q}) = 0\}.$$

Since $Q$ is a conic in $PG(2, p^f)$ and $S - a$ is a line of $PG(2, p^f)$, we have $|Q \cap (S - a)| = 0, 1, \text{ or } 2$, according to $S - a$ is passant, tangent, or secant. \hfill \Box
Thank you very much for your attention!