Cyclotomic schemes and related problems

Koji Momihara (Kumamoto University)

momihara@educ.kumamoto-u.ac.jp

16-06-2014

Definition

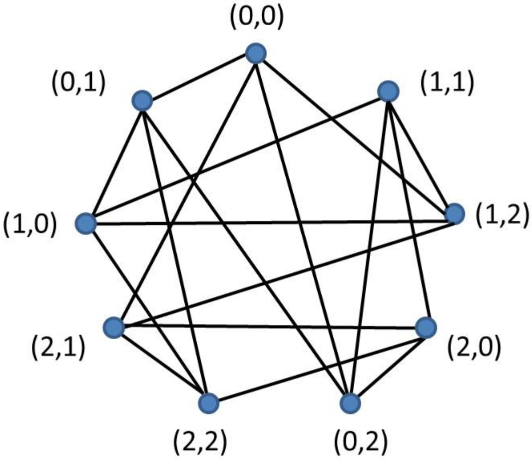
Definition: Cayley graph

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

(G, E) is called a Cayley graph, denoted by $Cay(G, D)$.

D is called the connection set of (G, E).

Paley graph



$$G = \mathbb{Z}_3 \times \mathbb{Z}_3,\ D = \{(0,1),(0,2),(2,1),(1,2)\}$$

Definition

Definition: Translation scheme

$\Gamma_i := (G, E_i)$, $1 \le i \le d$: 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 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 ℓ s.t. $(x, y) \in E_\ell$.
  $\Leftrightarrow |\{z \mid x - z \in R_i, y - z \in R_j\}|$ is const. according to ℓ s.t. $x - y \in R_\ell$.
  $\Leftrightarrow |(R_i + x - y) \cap R_j|$ is const. according to ℓ s.t. $x - y \in R_\ell$.
  $\Leftrightarrow |(R_i + w) \cap R_j|$ is constant according to ℓ s.t. $w \in R_\ell$.

Fundamentals of characters of abelian groups

A character ψ 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 ψ is an eth root of unity since

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

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

Fundamentals of characters of abelian groups

Remark

- Define $\psi_0(g) := 1$ for $\forall g \in G$. Then ψ_0 is a character, called the trivial character.
- Define $\psi^{-1}(g) := \psi(g)^{-1}$ for a character ψ. Then ψ^{-1} is a character, called the inverse of ψ.
- Define $\psi_1\psi_2(g) := \psi_1(g)\psi_2(g)$ for characters ψ_1, ψ_2. Then $\psi_1\psi_2$ is a character.

Theorem

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

Example

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 $\psi, \psi' \in \widehat{G}$,

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

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

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

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

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

Eigenvalues of Cayley graphs

Γ: 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 (ψ, g)-entry is defined by $\psi(g)$.)
A: the adjacency matrix of Γ (Each row and column are labeled similar to the columns of M.)

Theorem: Eigenvalues and character sums

$$\frac{MA\overline{M}^T}{|G|} = \mathrm{diag}\left(\sum_{x\in D}\psi(x)\right)_{\psi\in\widehat{G}},$$

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

Proof

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

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

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

we have

$$\begin{aligned}(MA\overline{M}^T)_{\psi,\psi'} &= \sum_{g\in G}\sum_{e\in D}\psi(e+g)\overline{\psi'(g)} = \sum_{e\in D}\psi(e)\sum_{g\in G}\psi(g)\overline{\psi'(g)} \\ &= \sum_{e\in D}\psi(e)\sum_{g\in G}\psi\psi'^{-1}(g) \\ &= \begin{cases} |G|\sum_{e\in D}\psi(e) & \text{if } \psi = \psi', \\ 0 & \text{if } \psi \neq \psi'. \end{cases}\end{aligned}$$

Primitivity of translation schemes

Γ: a Cayley graph on an abelian group G with connection set D

Lemma

Γ is connected $\Leftrightarrow \psi(D) \neq |D|$ for any nontrivial $\psi \in \widehat{G}$.

Remark

For any graph Γ,

- Γ has valency $k \Rightarrow \Gamma$ contains k as an eigenvalue.
- Γ has valency k and is connected $\Leftrightarrow$ k occurs exactly once as an eigenvalue.

Γ has valency $|D|$, and all eigenvalues are given by $\psi(D)$.
For trivial $\psi_0 \in \widehat{G}$, $\psi_0(D) = |D|$.
Γ is connected iff $\psi(D) \neq |D|$ for any nontrivial $\psi \in \widehat{G}$.

Dual of translation schemes

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

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

Theorem (Bridges-Mena, 1982)

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

	R_0	R_1	R_2	R_3
$\psi_0 \in S_0$	1	$\lvert R_1\rvert$	$\lvert R_2\rvert$	$\lvert R_3\rvert$
$\psi \in S_1$	1	a_1	a_2	a_3
$\psi' \in S_2$	1	b_1	b_2	b_3
$\psi'' \in S_3$	1	c_1	c_2	c_3

If $(G, \{R_i\}_{i=0}^d)$ forms a TS, then so does $(\widehat{G}, \{S_i\}_{i=0}^d)$, which is called the dual of $(G, \{R_i\}_{i=0}^d)$. $|G|P^{-1}$ is the first eigenmatrix of $(\widehat{G}, \{S_i\}_{i=0}^d)$ 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 $\mathbb{F}_q$
$C :\leq \mathbb{F}_q^*$ 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

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

where $N \mid q-1$ is a positive integer and γ is a fixed primitive element of $\mathbb{F}_q$. For $w \in C_\ell^{(N,q)}$,

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

Hence, $p_{i,j}^\ell$ is depending on ℓ not w.

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 $\gamma \in \mathbb{F}_q$, $\chi_j : \mathbb{F}_q^* \to \mathbb{C}^*$, $0 \le j \le q-2$, 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 $\mathrm{Tr}_{q^m/q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ by

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

which is a homomorphism from $(\mathbb{F}_{q^m}, +)$ to $(\mathbb{F}_q, +)$.

Lemma

The function $\psi_j : \mathbb{F}_q \to \mathbb{C}^*$, $j \in \mathbb{F}_q$, defined by

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

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

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

ψ_1 is called canonical.
Note that $\psi_a(x) = \psi_1(ax)$ and $\overline{\psi(x)} = \psi(-x)$.

Gauss sums and Jacobi sums

Definition

For the canonical additive character ψ of $\mathbb{F}_q$ and a nontrivial multiplicative character χ of $\mathbb{F}_q$, the sum

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

is called a Gauss sum.

Definition

For two multiplicative characters χ_1, χ_2 of $\mathbb{F}_q$, the sum

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q \setminus \{0,1\}} \chi_1(1-x)\chi_2(x)$$

is called a Jacobi sum.

Basic properties of Gauss sums and Jacobi sums

Lemma

For any nontrivial multiplicative characters χ_1, χ_2 of $\mathbb{F}_q$ s.t. $\chi_1\chi_2$ is nontrivial, then

$$J(\chi_1, \chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}. \tag{1}$$

Lemma

For any nontrivial multiplicative character χ of $\mathbb{F}_q$,

$$G(\chi)\overline{G(\chi)} = q.$$

The lemma above implies that $|G(\chi)| = \sqrt{q}$.
Furthermore, by (1), we have $|J(\chi_1, \chi_2)| = \sqrt{q}$.

$G(\chi)\overline{G(\chi)} = q$

Proof:

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{x,y\in\mathbb{F}_q^*} \psi_1(x)\psi_1(-y)\chi(x)\chi^{-1}(y) \\ &= \sum_{x,y\in\mathbb{F}_q^*} \psi_1(x-y)\chi(xy^{-1}). \qquad (2) \end{aligned}$$

Write $z = xy^{-1}$. Then,

$$\begin{aligned} (2) &= \sum_{y,z\in\mathbb{F}_q^*} \chi(z)\psi_1(y(z-1)) \\ &= \sum_{z\in\mathbb{F}_q^*} \chi(z) \sum_{y\in\mathbb{F}_q} \psi_1(y(z-1)) - \sum_{z\in\mathbb{F}_q^*} \chi(z) = q. \end{aligned}$$

Intersection numbers of cyclotomic schemes

Definition

$|(C_i^{(N,q)}+1)\cap C_j^{(N,q)}|$, $0\le i,j\le N-1$, are called cyclotomic numbers, denoted by $(i,j)_N$.

Computation of $(i,j)_N$: The characteristic function of $C_i^{(N,q)}$ on $\mathbb{F}_q^*$ is given by

$$f_i(\gamma^a)=\frac{1}{N}\sum_{k=0}^{N-1}\zeta_N^{-ik}\chi^k(\gamma^a),$$

where χ is a multiplicative character of order N of $\mathbb{F}_q$ s.t. $\chi(\gamma^a)=\zeta_N^a$. Then, we have

$$(i,j)_N=\sum_{x\in\mathbb{F}_q\setminus\{0,1\}} f_j(x)f_i(x-1). \tag{3}$$

$$
\begin{aligned}
(3) &= \frac{1}{N^2} \sum_{x \in \mathbb{F}_q \setminus \{0,1\}} \sum_{k,\ell=0}^{N-1} \zeta_N^{-(ik+j\ell)} \chi^k(x)\chi^\ell(x-1) \\
&= \frac{1}{N^2} \sum_{k,\ell=0}^{N-1} \zeta_N^{-(ik+j\ell)} \chi^\ell(-1) \sum_{x \in \mathbb{F}_q \setminus \{0,1\}} \chi^k(x)\chi^\ell(-x+1) \\
&= \frac{1}{N^2} \sum_{k,\ell=0}^{N-1} \zeta_N^{-(ik+j\ell)} J(\chi^k, \chi^\ell).
\end{aligned}
$$

$p_{i,j}^{\ell}$ could be expressed as a linear combination of Jacobi sums!

Remark

Since $|J(\chi^k,\chi^\ell)| = \sqrt{q}$ for $k, \ell, k+\ell \not\equiv 0 \pmod{N}$,

$$
\left| (i,j)_N - \frac{q-3N+1}{N^2} \right| \le \frac{(N^2-3N+2)\sqrt{q}}{N^2}.
$$

Eigenvalues of cyclotomic schemes

The eigenvalues are given by $\psi(C_i^{(N,q)})$, $\psi \in \widehat{G}$, called Gauss periods.

We can write $\psi(x) = \psi_1(ax)$ for some $a \in \mathbb{F}_q$, where ψ_1 is the canonical additive character of $\mathbb{F}_q$.

Thus, $\psi(C_i^{(N,q)}) = \psi_1(C_{i+\ell}^{(N,q)})$, where $a \in C_\ell^{(N,q)}$.

Write $\eta_i = \psi_1(C_i^{(N,q)})$. Then, the first eigenmatrix of the cyclotomic scheme is given by

$$\begin{pmatrix} 1 & \frac{q-1}{N} & \frac{q-1}{N} & \frac{q-1}{N} & \cdots & \frac{q-1}{N} \\ 1 & \eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{N-1} \\ 1 & \eta_1 & \eta_2 & \eta_3 & \cdots & \eta_0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \eta_{N-1} & \eta_0 & \eta_1 & \cdots & \eta_{N-2} \end{pmatrix}.$$

Gauss periods and Gauss sums

Lemma: Gauss periods and Gauss sums

(i) $$\psi_1(C_i^{(N,q)}) = \frac{1}{N}\sum_{h=0}^{N-1} G(\chi^h)\chi^{-h}(\gamma^i),$$

(ii) $$G(\chi) = \sum_{i=0}^{N-1} \psi_1(C_i^{(N,q)})\chi(\gamma^i),$$

where χ is a multiplicative character of order N of $\mathbb{F}_q$.

Eigenvalues of cyclotomic schemes

$$\begin{aligned}
\psi_1(C_i^{(N,q)}) &= \frac{1}{N}\sum_{x\in\mathbb{F}_q^*}\psi_1(\gamma^i x^N) \\
&= \frac{1}{N}\sum_{x\in\mathbb{F}_q^*}\frac{1}{q-1}\sum_{y\in\mathbb{F}_q^*}\psi_1(y)\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(\gamma^i x^N)\overline{\chi(y)} \\
&= \frac{1}{(q-1)N}\sum_{x\in\mathbb{F}_q^*}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi^{-1})\chi(\gamma^i x^N) \\
&= \frac{1}{(q-1)N}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}G(\chi^{-1})\chi(\gamma^i)\sum_{x\in\mathbb{F}_q^*}\chi(x^N) \\
&= \frac{1}{N}\sum_{\chi\in C_0^\perp}G(\chi^{-1})\chi(\gamma^i),
\end{aligned}$$

where $C_0^\perp$ is the subgroup of $\widehat{\mathbb{F}_q^*}$ consisting of all χ trivial on $C_0^{(N,q)}$.

Evaluated Gauss sums

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

- (**Pureness**) 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).

Useful formulas on Gauss sums

Hasse-Davenport product formula

η: a mult. character of order $\ell > 1$ of $\mathbb{F}_{p^f}$.
For ∀ nontrivial mult. character χ of $\mathbb{F}_{p^f}$,

$$G(\chi) = \frac{G(\chi^\ell)}{\chi^\ell(\ell)} \prod_{i=1}^{\ell-1} \frac{G(\eta^i)}{G(\chi\eta^i)}.$$

Hasse-Davenport lifting formula

χ': a nontrivial mult. character of $\mathbb{F}_q$

χ: the lift of χ to $\mathbb{F}_{q^m}$, i.e., $\chi'(\alpha) = \chi(\alpha^{\frac{q^m-1}{q-1}})$ for $\alpha \in \mathbb{F}_{q^m}$.
Then

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

Useful formulas on Gauss sums

Stickelberger's formula

N: a positive integer
p: a prime s.t. $\gcd(p, N) = 1$
f: the order of p in $\mathbb{Z}_N^*$
O_M: the rings of integers of $M = \mathbb{Q}(\zeta_N, \zeta_p)$
$\mathfrak{p}$: a prime ideal of O_M lying over p
$\sigma_j :\in \mathrm{Gal}(M/\mathbb{Q}(\zeta_p))$ by $\sigma_j(\zeta_N) = \zeta_N^j$, $j \in \mathbb{Z}_N^*$
$T := \mathbb{Z}_N^*/\langle p \rangle$
Then, it holds that

$$G_f(\chi^{-1})O_M = \mathfrak{p}^{\sum_{t\in T} s_p(\frac{t(q-1)}{k})\sigma_t^{-1}},$$

where $s_p(\frac{t(q-1)}{N})$ is the sum of all a_i for $\frac{t(q-1)}{N} = \sum_{i=0}^n a_i p^i$.

Useful formulas on Gauss sums

A useful algorithm for computing the p-divisibility of Gauss sums was found by Helleseth et al., 2009, called the modular p-ary add-with-carry algorithm.

A generalization of Stickelberger's formula (congruence) in p-adic fields was found by Gross and Koblitz, 1979.

Remarks

- The computation of eigenvalues of cyclotomic schemes is equivalent to that of weight distributions of certain cyclic codes, called irreducible cyclic codes.
- A strongly regular graph obtained as a fusion of a cyclotomic scheme is described in terms of projective geometry.

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
- $q := p^f = 1 + km$
- γ: 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

$$S = \{\ell \mid 0 \le \ell \le m-1, \ell \not\equiv \text{a power of } p \pmod{m}\}.$$

Irreducible cyclic codes

Lemma

C: the cyclic code generated by $g(x)$

The q codewords in C are given by

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

Proof:

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

For any $\ell \in S$,

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

Hence, $g(x) \mid h_\alpha(x)$, i.e., $\overline{h_\alpha(x)} \in C$.

Proof

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

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

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

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

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

Theorem (McEliece)

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

$$w(\overline{h_\alpha(x)}) = \frac{m(p-1)}{p} - \frac{p-1}{pk}\psi_1(\alpha C_0^{(N,p^f)}).$$

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

$$\begin{aligned} w(\overline{h_\alpha(x)}) &= m - \frac{1}{p}\sum_{i=0}^{m-1}\sum_{x\in\mathbb{F}_p}\psi_1(x\alpha\gamma^{ki}) \\ &= \frac{m(p-1)}{p} - \frac{1}{p}\sum_{i=0}^{m-1}\sum_{x\in\mathbb{F}_p^*}\psi_1(x\alpha\gamma^{ki}) \\ &= \frac{m(p-1)}{p} - \frac{1}{pk}\sum_{j=0}^{k-1}\sum_{x\in\mathbb{F}_p^*}G(\chi^{-j})\chi^j(x\alpha). \end{aligned}$$

Weight-distribution

Since for any $y \in \mathbb{F}_p^*$

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

$\sum_{x \in \mathbb{F}_p^*} \chi^j(x) = 0$ iff χ^j is nontrivial on $\mathbb{F}_p^*$.
Let χ' be a mult. character of order N of $\mathbb{F}_q$. Then,

$$w(\overline{h_\alpha(x)}) = \frac{m(p-1)}{p} - \frac{p-1}{pk} \sum_{j=0}^{N-1} G(\chi'^{-j}) \chi'^j(\alpha)$$
$$= \frac{m(p-1)}{p} - \frac{p-1}{pk} \psi_1(\alpha C_0^{(N,p^f)}).$$

□

Problem

Characterize all two or three weight irreducible cyclic codes.

Fusion schemes

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).

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 $a \in Y_h$.

Gauss sum and trace zero

W consider 2-class fusion schemes (strongly regular graphs) of cyclotomic schemes of order $N = \frac{q^m-1}{q-1}$.

Proposition

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

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

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

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

$$=(q-1) \sum_{i \in S_0} \chi(\gamma^i) - \sum_{i \in L \setminus S_0} \chi(\gamma^i) = q \sum_{i \in S_0} \chi(\gamma^i).$$

Geometric understanding

X: a subset of $\mathbb{Z}_N$

When is $\Gamma = Cay(\bigcup_{i\in X} C_i^{(N,q^m)})$ strongly regular?

(Γ 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 χ ranges through all mult. characters of exponent N of $\mathbb{F}_{q^m}$.

Proposition (Delsarte, 1972)

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

Note that each $S_0 - a$ is a hyperplane of PG$(m-1, q)$.

Problem

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

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

References

Gauss sums and related character sums

1. B. Berndt, R. Evans, K.S. Williams, *Gauss and Jacobi Sums*, 1997.
2. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., 2003.
3. R. Lidl, H. Niederreiter, *Finite Fields*, 1997.
4. W.M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, 2nd ed., 2004.
5. A. Robert, *A Course in p-adic Analysis*, 2000.

Linkage with difference sets

1. T. Storer, *Cyclotomy and Difference Sets*, 1967.
2. R.J. Turyn, Character sums and difference sets, *Pacific J. Math.,* (1965).

References

Linkage with codes

1. A.R. Calderbank, W.K. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.,* (1986).
2. B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields Appl.*, (2002).

Computations of Gauss sums

1. L.D. Baumert, W.H. Mills, R.L. Ward, Uniform cyclotomy, *J. Number Theory*, (1982).
2. K.Q. Feng, J. Yang, S.X. Luo, Gauss sums of index $\mathbf{4}$: (1) cyclic case, *Acta Math. Sin,* (2005).
3. J. Yang, S.X. Luo, K.Q. Feng, Gauss sums of index $\mathbf{4}$: (2) non-cyclic case, *Acta Math. Sin.,* (2006).
4. J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index $\mathbf{2}$ case, *Sci. China Ser. A*, (2010).
5. N. Aoki, On pure Gauss sums, *Com. Math. Univ. Sancti Pauli*, (2012).

References

General theory

1. A.E. Brouwer, W.H. Haemers, *Spectra of Graphs*, 2012.
2. A. Terras, *Fourier Analysis on Finite Groups and Applications*, 1999.

p-divisibility: Modular p-ary add-with-carry algorithm

1. T. Helleseth, H.D.L. Hollmann, A. Kholosha, Z. Wang, Q. Xiang, Proofs of two conjectures on ternary weakly regular bent functions, *IEEE Trans. Inform. Theory,* (2009).

Japanese book

1. ベルヌーイ数とゼータ関数, 荒川恒男, 金子昌宣, 伊吹山知義, 2001.
2. 有限数学入門-有限上半平面とラマヌジャングラフ-, 平松豊, 知念宏司, 2003.