ACA2015, Augst 26-30, 2015, Michigan Tech. Univ.

Resolvability of a cyclic orbit of a subset of $\mathbb{Z}_v$ and spread decomposition of Singer cycles of projective lines

Masakazu Jimbo (Chubu University)
jimbo@isc.chubu.ac.jp
&
Miwako Mishima (Gifu University)
&
Koji Momihara (Kumamoto University)

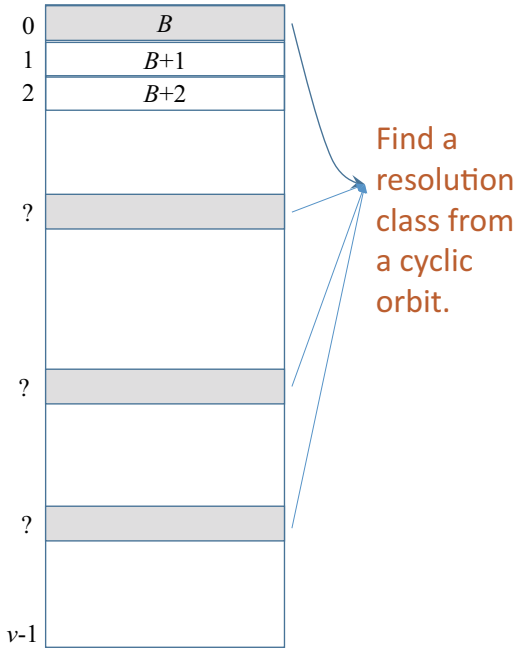
Resolvability of a cyclic orbit

v, k: positive integers such that $k \mid v$

$\mathbb{Z}_v$: a residue ring of integers modulo v.

For a subset (block) $B \subset \mathbb{Z}_v$ of size k, $\mathrm{Orb}_{\mathbb{Z}_v}(B) = \{B + i \mid i \in \mathbb{Z}_v\}$ is called a cyclic orbit of B.

$\mathrm{Orb}_{\mathbb{Z}_v}(B)$ is said to be full if $|\mathrm{Orb}_{\mathbb{Z}_v}(B)| = v$, otherwize short.



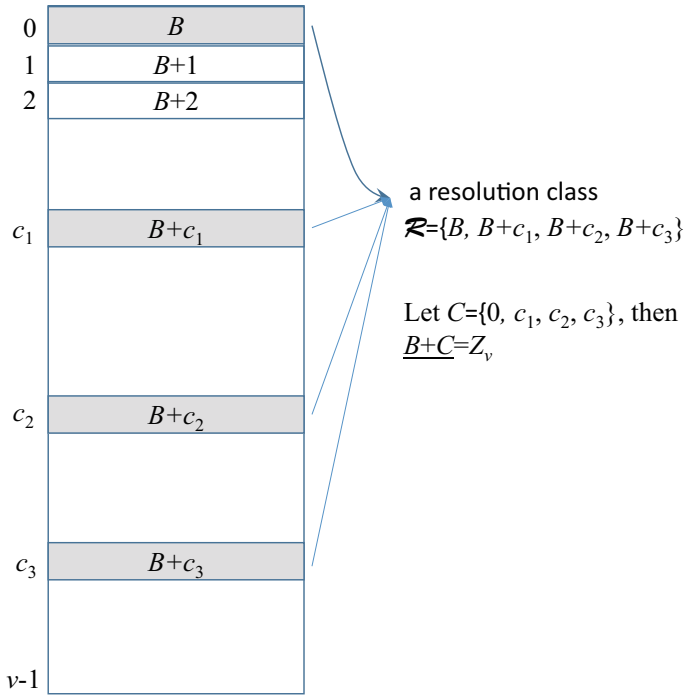
A subfamily $\mathcal{R} \subset \mathrm{Orb}_{\mathbb{Z}_v}(B)$ satisfying $\cup_{E \in \mathcal{R}} E = \mathbb{Z}_v$ is called a resolution class. If $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ is decomposed into disjoint resolution classes then $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ is said to be resolvable.

For any $A, B \subset \mathbb{Z}_v$, let $A + B = \{a + b | a \in A, b \in B\}$, which is considered as a mulitiset.

If $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ has a resolution class, then there is a subset $C \subset \mathbb{Z}_v$ satisfying

$$B + C = \mathbb{Z}_v. \qquad (1)$$

If (1) holds, we say that (B, C) is a factorization of $\mathbb{Z}_v$. Note that if (B, C) is a factorization of $\mathbb{Z}_v$, then $(B + x, C + y)$ is also a factorization for $x, y \in \mathbb{Z}_v$.



Lemma 1 If $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ has a resolution class then $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ is resolvable.

Proof: A resolution class is represented as $\mathcal{R} = \cup_{c \in C}(B + c)$ with $C \subset \mathbb{Z}_v$. Take $\mathcal{R} + b_1, \mathcal{R} + b_2, \ldots$ as resolution classes for $b_i \in B$.

What is the condition for B that $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ is resolvable?

A subset $A \subset \mathbb{Z}_v$ is said to be periodic if its stabilizer $N = \{g \in \mathbb{Z}_v \big| A + g = A\}$ is a nontrivial subgroup of $\mathbb{Z}_v$.

Theorem 1 (see, Szabo and Sands (2009)) In the case when $k = |B|$ is a power of a prime, if $B + C = \mathbb{Z}_v$, then B or C is periodic.

Hereafter, we consider only the case when $k = |B|$ is a power of a prime.

The structure of a factor (B, C) of $\mathbb{Z}_v$

Theorem 2 For a factorization (B, C) of $\mathbb{Z}_v$, assume that $k = |B|$ is a power of a prime and $0 \in B$, $0 \in C$. Then, B and C are represented by

$$B = N_1 + \cdots + N_{t-1} + B_t, \quad C = M_0 + M_1 + \cdots + M_{t'-1} + C_{t'},$$

where $n_0 = v$, $N_0 = \{0\}$,

$$m_i = \frac{n_i}{|N_i|}, M_i = \{0 \le g < m_i \big| C + g (\text{mod } m_i) = C\}, \text{ for } i' = 0, 1, \ldots$$

$$n_i = \frac{m_{i-1}}{|M_{i-1}|}, N_i = \{0 \le g < n_i \big| B + g (\text{mod } n_i) = B\}, \text{ for } i = 1, 2, \ldots$$

and $t = \max_i\{i \big| N_i \neq \{0\}\}$, $t' = \max_i\{i \big| M_i \neq \{0\}\}$, $B_t = N_t$ (mod n_t), $B_t \subset \mathbb{Z}_{m_{t-1}}$, $M_{t'} = M_{t'}$ (mod $m_{t'}$), $M_{t'} \subset \mathbb{Z}_{n_{t'}}$.

Example 1 For $v = 48$, let $B = \{0, 9, 24, 33\}$ and $C = \{0, 1, 2, 6, 7, 8, 12, 13, 14, 18, 19, 20\}$. Then, $B + C = \mathbb{Z}_{48}$.

$$B = N_1 + B_2 = \{0, 24\} + \{0, 9\},$$
$$C = M_1 + C_2 = \{0, 6, 12, 18\} + \{0, 1, 2\}$$

Then $\{0, 24\}$ is a subgroup of $\mathbb{Z}_{48}$, $\{0, 6, 12, 18\}$ is a subgroup of $\mathbb{Z}_{24}$, $\{0, 9\} \equiv \{0, 3\}$ is a subgroup of $\mathbb{Z}_6$, and $\{0, 1, 2\}$ is $\mathbb{Z}_3$.

Is this true for any $k = |B|$?

Example 2 (Zsabo and Sands (2009)) For $v = 72$, let $B = \{0, 8, 16\} + \{0, 8\}$ and $C = (\{0, 24, 66\} + \{0, 36\}) \cup (\{0, 24, 48\} + \{0, 44\} + \{1\})$ Then, $B + C = \mathbb{Z}_{72}$. But both of B and C are not periodic in $\mathbb{Z}_{72}$. That is, a "bad" factorization!!

Minimum factorization theorem

Theorem 3 For a prime p and integrs r, t, m satisfying $r \leq t$ and $(m, p) = 1$, let $v = p^t m$. For a subset $B \subset \mathbb{Z}_v$ with $|B| = k = p^r$, assume that there is a subset $C \subset \mathbb{Z}_v$ such that (B, C) is a factorization of $\mathbb{Z}_v$. Then

$$e = \min\{n \mid \exists C,\ (B, C) \text{ is a factorization of } \mathbb{Z}_n,\ n|v\}.$$

is a divisor of p^t.

By this theorem, in order to check the resolvablity of a cyclic orbit $\mathrm{Orb}_{\mathbb{Z}_v}(B)$ for $|B| = p^r$, we have only to check whether $\mathrm{Orb}_{\mathbb{Z}_{p^i}}(B)$ has a resolution class, or not for each $i \leq t$.

Application: Spread decomposition of a line orbit of PG$(2n-1,q)$

For a prime power q, the lines of PG$(2n-1,q)$ consist of a number of Singer cycles of length $v = \frac{q^{2n}-1}{q-1}$ and a single short orbit.

Among them, some Singer cycle of full length may be decomposed into spreads (resolution classes).

We want to decide the number of Singer cycles which are decomposed into spreads.

In this talk, we consider the cases of $q = 3$ and 4. In these cases the sizes of lines L are $q+1 = 4, 5$, which are a prime or a prime power.

The case of $q = 3$: PG$(2n-1, 3)$

Let $\langle g \rangle = \mathrm{GF}(3^{2n})^{\times}/\mathrm{GF}(3)^{\times}$. Then, $|\langle g \rangle| = v = \frac{3^{2n}-1}{2}$.

A base line L of $\mathrm{Orb}_{\langle g \rangle}(L)$ is represented by

$$L = \{1 = q^0, x = g^{b_1}, x+1 = g^{b_2}, x-1 = g^{b_3}\},$$

or simply by $\mathrm{pow}(L) = \{0, b_1, b_2, b_3\} \subset \mathbb{Z}_v$.

A line orbit is decomposed into spreads.

$\Leftrightarrow$

There is a subset $C \subset \mathbb{Z}_v$ such that $\mathrm{pow}(L) + C = \mathbb{Z}_v$.

$\Leftrightarrow$

There is a subset $C \subset \mathbb{Z}_{2^i}$ such that $\mathrm{pow}(L) + C = \mathbb{Z}_{2^i}$ for some i such that $2^i | v$. (by Theorem 3)

$\Leftrightarrow$

There is a "proper" distribution of the elements of $L = \{1, x, x+1, x-1\}$ in cyclotomic cosets $C_j^{(2^i)}$ for some i such that $4 \mid 2^i \mid v$.

What is the proper disribution

Lemma 2 If a Singer cycle $\mathrm{Orb}_{\langle g \rangle}(L)$ of a line $L = \{1, x, x+1, x-1\}$ has a resolution then the four elements must fall in $C_0^{(2^i)}, C_j^{(2^i)}, C_{2^{i-1}}^{(2^i)}, C_{2^{i-1}+j}^{(2^i)}$, respectively. That is

$$\mathrm{pow}(L) \pmod{2^i}$$
$$\equiv \{0, j_1, j_2, j_3\} = \{0, 2^{i-1}\} + \{0, j\} = \{0, j, 2^{i-1}, 2^{i-1}+j\}$$

for $1 \leq j < 2^{i-2}$.

We call i the depth of cyclotomic cosets.

Counting the Singer cycles which is decomposed into spreads.

Theorem 4 Let

$$\mathcal{M}_i = \{x \Big| x, (x+1)^{-1}(x-1) \in C_{2^{i-1}}^{(2^i)} \wedge x+1 \notin C_0^{(2^i)}\}.$$

Then, for any $x \in \mathcal{M}_i$, a Singer cycle of a line $L = \{1, x, x+1, x-1\}$ is decomposed into four spreads. And

$$\text{total \# of spreads within Singer cyclces} = \frac{1}{2}|\mathcal{M}_i|.$$

We count $|\mathcal{M}_i|$ by using a number theoretical technique.

Counting methods

e: a divisor of v

$\zeta_e \in \mathbb{C}$: a primitive e-th root

$\psi(g^h) = \zeta_e^h$: a multiplicative character of order e of $\mathbb{F}_{3^{2n}}$

$$f_{C_j^{(e)}}(z) = \frac{1}{e}\sum_{u=0}^{e-1} \zeta_e^{-uj}\psi^u(z) = \begin{cases} 1 & \text{if } z \in C_j^{(e)} \\ 0 & \text{otherwize} \end{cases}$$

Note that

$$\begin{aligned}\mathcal{M}_i =& \{x \mid x, (x+1)^{-1}(x-1) \in C_{2^{i-1}}^{(2^i)} \wedge x+1 \notin C_0^{(2^{i-1})}\} \\ =& \{x \mid x, (x+1)^{-1}(x-1) \in C_{2^{i-1}}^{(2^i)}\} \\ & \setminus \{x \mid x, (x+1)^{-1}(x-1) \in C_{2^{i-1}}^{(2^i)} \wedge x+1 \in C_0^{(2^{i-1})}\}\end{aligned}$$

Representation of $|\mathcal{M}_i|$ by Jacobi-like sum.

Hence,

$$\begin{aligned}|\mathcal{M}_i| &= \sum_{x\in\mathbb{F}_{3^{2n}}\setminus\mathbb{F}_3} f_{C_{2^{i-1}}^{(2^i)}}(x) f_{C_{2^{i-1}}^{(2^i)}}((x+1)^{-1}(x-1)) \\ &\quad - \sum_{x\in\mathbb{F}_{3^{2n}}\setminus\mathbb{F}_3} f_{C_{2^{i-1}}^{(2^i)}}(x) f_{C_{2^{i-1}}^{(2^i)}}((x+1)^{-1}(x-1)) f_{C_0^{(2^{i-1})}}(x+1) \\ &= \frac{1}{2^{2i}} \sum_{(u,v)\in\mathbb{Z}_{2^i}^2} (-1)^{u+v} T_{\psi_i}(u,-v,v) \\ &\quad - \frac{1}{2^{3i-1}} \sum_{(u,v,w)\in\mathbb{Z}_{2^i}^2\times\mathbb{Z}_{2^{i-1}}} (-1)^{u+v} T_{\psi_i}(u,2w-v,v),\end{aligned}$$

where

$$T_{\psi_i}(u,v,w) = \sum_{x\in\mathbb{F}_{3^{2n}}\setminus\mathbb{F}_3} \psi_i^u(x)\psi_i^v(x+1)\psi_i^w(x-1).$$

and ψ_i is a multiplicative character of $\mathbb{F}_q$ of order 2^i.

Evaluation of $T_{\psi_i}(u,v,w)$ for $i \leq 2$

If $i \leq 2$, then we can compute the "exact values" of $T_{\psi_i}(u,v,w)$ for any $(u,v,w) \in \mathbb{Z}_{2^i}^3$ since $T_{\psi_i}(u,v,w)$ can be reduced to computable Jacobi sums.

Lemma 3 Let q be a power of 3. For any $a, b \in \mathbb{Z}_m$,

$$T_\psi(a,b,0) = \begin{cases} q-3 & \text{if } a = b = 0, \\ -1 - \psi^a(-1) & \text{if } a \neq 0 \text{ and } b = 0, \\ \psi^a(-1)J(\psi^a, \psi^b) - \psi^{2a+b}(-1) & \text{if } a, b \neq 0. \end{cases}$$

Lemma 4 Let q be a power of 3, ψ_i be a multiplicative character of $\mathbb{F}_q$ of order 2^i and
η be the quadratic character of $\mathbb{F}_q$. Then, for any $u, v, w \in \mathbb{Z}_4^\times$,

$$T_{\psi_2}(u,v,w) = \begin{cases} J(\psi_3, \eta) + J(\psi_3^5, \eta) & \text{if } u, v \text{ and } w \text{ are distinct}, \\ J(\psi_3^i, \psi_2^j) + J(\psi_3^{i+4}, \psi_2^j) & \text{if } (u,v,w) \in \{(i,j,j),(j,i,j),(j,j,i)\}. \end{cases}$$

of spreads for depth $i \leq 2$

Theorem 5 The total number K of spreads obtained by decomposing every Singer cycle of lines in $PG(2n-1,3)$ depth at most $i = 2$ is

$$K = \begin{cases} \frac{1}{64}\left\{3^{2n} - 2\cdot 3^{n+1} + 2I(n) + 2\right\} & \text{if } n \text{ is even,} \\ \frac{1}{64}\left\{3^{2n} + 14\cdot 3^{n} + 6\cdot I(n) + 1\right\} & \text{if } n \text{ is odd,} \end{cases}$$

where $I(n) = (1 - \mathrm{i}\sqrt{2})^n + (1 + \mathrm{i}\sqrt{2})^n$, $\mathrm{i} = \sqrt{-1}$.

If n is odd, $v = 4m$ with m odd. Thus Theorem 5 gives the best decomposition in the sense that the total number of spreads within Singer cycles is maximum.

More decomposition for even n

For even n, as for $i \geq 3$, unlike the case $i \leq 2$, not every $T_{\psi_i}(u, v, w)$ can be reduced to Jacobi sums, and thus we need to find another way to compute $T_{\psi_i}(u, v, w)$.

Applying Theorem 5.39 in "Finite Fields" by Lidl and Neiderreiter, we have

$$T_{\psi_i}(u, v, w) = \sum_{x \in \mathbb{F}_{3^{2n}} \setminus \mathbb{F}_3} \psi_i^u(x)\psi_i^v(x+1)\psi_i^w(x-1) = \sum_{x \in \mathbb{F}_{3^{2i-1}\ell} \setminus \mathbb{F}_3} \psi_i^{(\ell)}(f(x))$$
$$= -\omega_1^\ell - \omega_2^\ell - \psi_i^{(\ell)}(f(0)) - \psi_i^{(\ell)}(f(1)) - \psi_i^{(\ell)}(f(-1)),$$

where (ω_1, ω_2) is a solution to the system of equations

$$\begin{cases} \sum_{c \in \mathbb{F}_{3^{2i-1}}} \psi_i(c^u(1+c)^v(-1+c)^w) = -\omega_1 - \omega_2, \\ \sum_{(b,c) \in \mathbb{F}_{3^{2i-1}}^2} \psi_i(c^u(1+b+c)^v(1-b+c)^w) = \omega_1\omega_2. \end{cases}$$

of speads for depth $i \leq 3$

n	Numbers spreads	depth i
2	1	2
	5	3^*
3	13	2^*
4	97	2
	129	3
5	1021	2^*
6	8257	2
	11177	3^*
7	74929	2^*
8	671617	2
	923745	3
9	6058057	2^*
10	54479041	2
	74914145	3^*

'$*$' in the column for i means the best decomposition in the sense that the total number of spreads is maximum.

The case of PG$(2n-1,4)$

Evaluation of $|\mathcal{M}_i|$ leads us to a decomposition of the Singer cycles of lines in PG$(2n-1,4)$.

Theorem 6 Let s be the highest power of 5 in n and r be an integer within $1 \leq r \leq s+1$.
The Singer cycles in $PG(2n-1,4)$ can be decomposed into

$$K = \frac{1}{3}\left(\sum_{i=1}^{r} |\mathcal{M}_i|\right) + \delta$$

spreads, where $\delta = 0$ or 1 depending on if $r = s+1$ or otherwise.

To conut $|\mathcal{M}_i|$, instead of $T_{\psi_i}(u,v,w)$, we use

$$Q_{\psi_i}(u,v,w,z) = \sum_{x \in \mathbb{F}_{4^{2n}} \setminus \mathbb{F}_4} \psi_i^u(x)\psi_i^v(x+1)\psi_i^w(x+2)\psi_i^z(x+4)$$

where ψ_i is a multiplicative character of order 5^i.

Size of $\mathcal{M}_1$ for $q = 4$

By a similar manner to the case of $q = 3$, we obtain the following for $\mathcal{M}_1$.

$$
\begin{aligned}
|\mathcal{M}_1| = \frac{3}{625}\, 2^{-n} \Bigg(& 2^{1+n} + 2^{1+5n} - (-1)^n\, 8^{2+n} + 40\left(7 - i\sqrt{15}\right)^n + 40\left(7 + i\sqrt{15}\right)^n \\
& - 20\left(-3 - i\sqrt{55}\right)^n - 20\left(-3 + i\sqrt{55}\right)^n \\
& + 5\left(\frac{1}{2}\left(-1 - 5\sqrt{5} - i\sqrt{130 - 10\sqrt{5}}\right)\right)^n \\
& + 5\left(\frac{1}{2}\left(-1 - 5\sqrt{5} + i\sqrt{130 - 10\sqrt{5}}\right)\right)^n \\
& + 5\left(\frac{1}{2}\left(-1 + 5\sqrt{5} - i\sqrt{10\left(13 + \sqrt{5}\right)}\right)\right)^n \\
& + 5\left(\frac{1}{2}\left(-1 + 5\sqrt{5} + i\sqrt{10\left(13 + \sqrt{5}\right)}\right)\right)^n \Bigg)
\end{aligned}
$$

Number of spreads by Theorem 6 for PG$(2n-1,4)$

Considering just $\mathcal{M}_1$, the number of spreads obtained by our decomposition is calculated as follows.

n	Number of spreads
2^*	1
3^*	16
4^*	161
5	3426
6^*	52576
7^*	858481
8^*	13737761
9^*	219913936
10	3518321826

'$*$' in the column for n means the best decomposition in the sense that the total number of spreads is maximum.

Thank you.