Smooth skew-morphisms of the dihedral groups

Kan Hu
Joint work with
Naer Wang, Kai Yuan and Junyang Zhang

Zhejiang Ocean University

Sanya, 2018
Definition (Skew-morphism)

A skew-morphism of a finite group $A$ is a permutation $\varphi$ on $A$ such that

$$\varphi(1) = 1 \quad \text{and} \quad \varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$$

for all $a, b \in A$, where $\pi : A \to \mathbb{Z}$ is an integer function.
Theorem (Jajcay, Širáň, 2002)

A Cayley map $\text{Cay}(A, X, P)$ is regular iff $P$ extends to a skew-morphism $\varphi$ of $A$ (Cayley skew-morphism), namely, $P = \varphi \upharpoonright X$ such that

$$A = \langle X \rangle \quad \text{and} \quad X^{-1} = X.$$ 

Definition

A Cayley map $\text{Cay}(A, X, P)$ is

$\triangleright$ balanced if $P(x^{-1}) = P(x)^{-1},$

$\triangleright$ antibalanced if $P(x^{-1}) = (P^{-1}(x))^{-1},$

$\triangleright$ $t$-balanced if $P^t(x^{-1}) = (P^t(x))^{-1}$ for some fixed $t.$
Theorem (Conder, Jajcay and Tucker, 2016)

If \( \varphi \in \text{Skew}(A) \), then \( L_A\langle \varphi \rangle = \langle \varphi \rangle L_A \), so \( G = L_A\langle \varphi \rangle \) is a transitive permutation group with a cyclic complement. Note that \( \langle \varphi \rangle \) in core-free in \( G \), so in particular, \( \langle \varphi \rangle \cap L_A = 1 \).

Conversely, if \( G \) admits a cyclic complementary factorisation \( G = AB \), where \( A, B \leq G \), \( B = \langle y \rangle \) and \( A \cap B = 1 \), then the commuting rule

\[
ya = \varphi(a)y^{\pi(a)}, \quad \forall a \in A
\]

determines a skew-morphism \( \varphi \) of \( A \). Note that \( \varphi \) has order \( |B : B_G| \) where \( B_G = \bigcap_{g \in G} B^g \).
Two important subgroups

Let \( \varphi \in \text{Skew}(A) \). Define two sets

\[
\ker \varphi = \{ a \in A \mid \pi(a) \equiv 1 \pmod{|\varphi|} \}
\]

and

\[
\text{Core} \varphi = \bigcap_{i=1}^{|\varphi|} \varphi^i(\ker \varphi).
\]

Then \( \ker \varphi \leq A \) (kernel of \( \varphi \)) and \( \text{Core} \varphi \trianglelefteq A \) (core of \( \varphi \)).

- If \( A \neq 1 \) then \( \ker \varphi > 1 \) and \( |\varphi| < |A| \).
- Core \( \varphi \) is the largest \( \varphi \)-invariant subgroup contained in \( \ker \varphi \).
- \( \varphi(\ker \varphi) = \ker \varphi \iff \ker \varphi = \text{Core} \varphi \) (kernel-preserving).
- The index \( k = |A : \ker \varphi| \) is called the skew-type of \( \varphi \).
Important properties of skew-morphisms

Proposition

Let \( \varphi \in \text{Skew}(A) \). Then

(1) For any positive integer \( k \),

\[
\varphi^k(ab) = \varphi^k(a)\varphi^{\sigma(a,k)}(b), \quad \forall a, b \in A
\]

where

\[
\sigma(a, k) = \pi(x) + \pi(\varphi(x)) + \cdots + \pi(\varphi^{k-1}(a)) = \sum_{i=1}^{k} \pi(\varphi^{i-1}(a));
\]

Moreover, \( \mu = \varphi^k \) is a skew-morphism of \( A \) iff the congruences

\[
kx \equiv \sigma(a, k) \pmod{n}
\]

are solvable for all \( a \in A \).
(2) For all \( a, b \in A \),

\[
\pi(ab) \equiv \sigma(b, \pi(a)) \equiv \sum_{i=1}^{\pi(a)} \pi(\varphi^{i-1}(b)) \pmod{\varphi^\prime(b)}.
\]

Moreover, \( \pi(a) = \pi(b) \iff Ka = Kb \), where \( K = \text{Ker} \varphi \).

(3) Fix \( \varphi = \{ a \in A \mid \varphi(a) = a \} \) is a \( \varphi \)-invariant subgroup of \( A \).

(4) For any \( \gamma \in \text{Aut}(A) \), \( \psi = \gamma^{-1} \varphi \gamma \) is a skew-morphism of \( A \).

(5) For any \( a \in A \), \( O_{a^{-1}} = O_a^{-1} \), where \( O_a^{-1} = \{ x^{-1} \mid x \in O_a \} \).

(6) For any \( a, b \in A \), \( |O_{ab}| \) divides \( \text{lcm}(|O_a|, |O_b|) \). Moreover, if \( A = \langle a_1, \cdots, a_r \rangle \) then \( |\varphi| = \text{lcm}(|O_{a_1}|, \cdots, |O_{a_r}|) \), and \( \varphi \) and \( \pi \) are completely determined by their actions on \( O_{a_1}, \cdots, O_{a_r} \).
Let $\Pi$ be a finite set of primes, a positive integer $k$ will be called a $\Pi$-number if all prime factors of $k$ belong to $\Pi$. We define 1 to be a $\Pi$-number for any set $\Pi$ of primes.

**Lemma (\(\Pi\)-orbit subgroup)**

For any finite set $\Pi$ of primes, 

$$\text{Orbit}^\Pi \varphi = \{x \in A \mid |O_x| \text{ is a } \Pi\text{-number}\}$$

is a $\varphi$-invariant subgroup of $A$ containing $\text{Fix} \varphi$.

**Example**

Let $\varphi \in \text{Skew}(\mathbb{Z}_{21})$ be given by 

$$\varphi = (0)(1, 2, 4, 8, 16, 11)(3, 6, 12)(5, 10, 20, 19, 17, 13)(7, 14)(9, 18, 15).$$

Then $\text{Orbit}^{\{2\}} \varphi = \langle 7 \rangle$, $\text{Orbit}^{\{3\}} \varphi = \langle 3 \rangle$, and $\text{Orbit}^{\{2,3\}} \varphi = \mathbb{Z}_{21}$. 
(7) If $N$ is a $\varphi$-invariant normal subgroup of $A$, then $\varphi$ induces a skew-morphism $\bar{\varphi}$ of $\bar{A} = A/N$ defined by

$$\bar{\varphi}(\bar{x}) = \varphi(x)$$

with the associated power function $\bar{\pi}$ given by

$$\bar{\pi}(\bar{x}) \equiv \pi(x) \pmod{m}$$

where $m = |\bar{\varphi}|$. 
Definition (Covering of skew-morphisms)

Let $\varphi_i$ be skew-morphisms of finite groups $A_i$ ($i = 1, 2$). If there is an epimorphism $\theta : A_1 \to A_2$ such that for all $x \in A_1$

$$\theta \varphi_1(x) = \varphi_2 \theta(x),$$

then $\varphi_1$ will be called a covering of $\varphi_2$, and $\varphi_2$ will be called a projection of $\varphi_1$.

Lemma

*With above notation,*

- every $\varphi_1$-invariant subgroup $M$ of $A_1$ projects to a $\varphi_2$-invariant subgroup $\theta(M)$ of $A_2$,
- every $\varphi_2$-invariant subgroup $N$ of $A_2$ lifts to a $\varphi_1$-invariant subgroup $\theta^{-1}(N)$ of $A_1$. 
**Smooth subgroup**

**Lemma**

Let $\varphi \in \text{Skew}(A)$ and $\bar{\varphi} \in \text{Skew}(A/\text{Core } \varphi)$, with $\theta : A \to A/\text{Core } \varphi$. Then

$$\text{Smooth } \varphi := \theta^{-1}(\text{Fix } \bar{\varphi})$$

is a $\varphi$-invariant subgroup of $A$.

**Example**

Let $\varphi \in \text{Skew}(\mathbb{Z}_{18})$ be given by

$$\varphi = (0)(1, 15, 17, 7, 3, 5, 13, 9, 11)(2, 14, 8)(4, 10, 16)(6)(12),$$

$$\pi = [1][2, 5, 8, 2, 5, 8, 2, 5, 8] [7, 7, 7] [4, 4, 4] [1][1].$$

Then $\text{Core } \varphi = \langle 6 \rangle$, so $\bar{\varphi} = (0)(1, 3, 5)(2)(4)$. Therefore

$$\text{Smooth } \varphi = \{0, 2, 14, 8, 4, 10, 16, 6, 12\} = \langle 2 \rangle.$$
Lemma
Smooth $\varphi = A \iff \text{Fix } \bar{\varphi} = \bar{A}$.

Definition
If Smooth $\varphi = A$ then $\varphi$ will be called smooth.

Lemma
$\varphi$ is smooth $\iff \pi(\varphi(x)) \equiv \pi(x) \pmod{|\varphi|}$, $\forall x \in A$.

Remark
Under the name of coset-preserving skew-morphisms, smooth skew-morphisms of the cyclic groups $C_n$ have been determined by Bachratý and Jajcay.

Theorem

Let $\varphi \in \text{Skew}(A)$ and $\bar{\varphi} \in \text{Skew}(A/\text{Core } \varphi)$, $m = |\bar{\varphi}|$. If $\varphi$ is kernel-preserving, then

(1) $\mu = \varphi^m$ is a smooth skew-morphism of $A$.

(2) if $\varphi$ is non-trivial, then $\mu = \varphi^m$ is also non-trivial.
Theorem

Let $\varphi \in \text{Skew}(A)$. If $\varphi$ is smooth, then

(1) $\varphi$ is kernel-preserving,

(2) $\pi : A \to \mathbb{Z}_n$ is a group homomorphism from $A$ to the multiplicative group $\mathbb{Z}_n^*$ with $\text{Ker} \, \pi = \text{Ker} \, \varphi$,

(3) for any $\varphi$-invariant normal subgroup $N$ of $A$, $\bar{\varphi} \in \text{Skew}(A/N)$ is also smooth; in particular, if $N = \text{Ker} \, \varphi$ then $\bar{\varphi} = \text{id}$,

(4) for any positive integer $k$, $\mu = \varphi^k$ is a smooth skew-morphism,

(5) for any $\gamma \in \text{Aut}(A)$, $\psi = \gamma^{-1} \varphi \gamma$ is a smooth skew-morphism of $A$. 
Problem

For the dihedral group $D_n$ given by

$$D_n = \langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle,$$  \quad n \geq 3,

classify all regular Cayley maps of $D_n$, and more generally, determine all skew-morphisms of $D_n$.


Outline for the full classification

Let $\varphi \in \text{Skew}(D_n), \ n \geq 3$. Then

- If $\varphi\langle a \rangle \neq \langle a \rangle$, then $\varphi$ is a Cayley skew-morphism of $D_n$ (Kovacs and Kwon, 2018+).

- If $\varphi\langle a \rangle = \langle a \rangle$, then $|D_n : \ker \varphi| = 1, 2, 4$ (Zhang and Du, 2016), and in particular $\varphi$ is smooth (Kwon, 2018+).
Lemma

Let $\varphi$ be a smooth skew-morphism of $D_n$, $n \geq 3$.

- If $n$ is odd, then $\varphi$ is an automorphism of $A$,
- if $n$ is even and $\varphi$ is not an automorphism of $D_n$ then
  $\ker \varphi = \langle a^2 \rangle$, $\ker \varphi = \langle a^2, ab \rangle$ or $\ker \varphi = \langle a^2, b \rangle$.

Moreover, in case of $\ker \varphi = \langle a^2, b \rangle$, $\psi = \gamma^{-1} \varphi \gamma$ is a smooth skew-morphism with $\ker \psi = \langle a^2, ab \rangle$ where $\gamma : a \mapsto a, b \mapsto ab$ is an automorphism of $D_n$. 
Theorem

For \( n \geq 4 \) even, every smooth skew-morphism \( \varphi \) of \( D_n \) with \( \text{Ker} \varphi = \langle a^2 \rangle \) is given by

\[
\begin{align*}
\varphi(a^{2i}) &= a^{2iu}, \\
\varphi(a^{2i+1}) &= a^{2iu+2r+1}, \\
\varphi(a^{2i}b) &= a^{2iu+2s}, \\
\varphi(a^{2i+1}b) &= a^{2iu+2r+2s\sigma(u,e)+1}b
\end{align*}
\]

and

\[
\begin{align*}
\pi(a^{2i}) &= 1, \\
\pi(a^{2i+1}) &= e, \\
\pi(a^{2i}b) &= f, \\
\pi(a^{2i+1}b) &= ef,
\end{align*}
\]

where \( r, s, u, k, e, f \) are nonnegative integers satisfying the following conditions
(i) \( r, s \in \mathbb{Z}_{n/2} \) and \( u \in \mathbb{Z}^*_n \),

(ii) \( k \) is the smallest positive integer such that \( r\sigma(u,k) \equiv 0 \pmod{n/2} \) and \( s\sigma(u,k) \equiv 0 \pmod{n/2} \) where

\[
\sigma(u,k) = \sum_{i=1}^{k} u^{i-1}, \quad \text{(N.B. } k = |\varphi|) \]

(iii) \( e, f \in \mathbb{Z}^*_k \) such that \( e \not\equiv 1 \pmod{k} \), \( f \not\equiv 1 \pmod{k} \), \( ef \not\equiv 1 \pmod{k} \), \( e^2 \equiv 1 \pmod{k} \) and \( f^2 \equiv 1 \pmod{k} \),

(iv) \( u^{e-1} \equiv 1 \pmod{n/2} \) and \( u^{f-1} \equiv 1 \pmod{n/2} \),

(v) \( r\sigma(u,e-1) \equiv u - 2r - 1 \pmod{n/2} \),

(vi) \( s\sigma(u,f-1) \equiv 0 \pmod{n/2} \),

(vii) \( r\sigma(u,f-1) + s\sigma(u,e-1) \equiv u - 2r - 1 \pmod{n/2} \).
Remark

In the particular case where $u = 1$. By (ii) we have

$$k = \frac{n/2}{\gcd(r, n/2)} \cdot \frac{n/2}{\gcd(s, n/2)}.$$ 

The numerical conditions are reduced to

$$
\begin{cases}
    e^2 \equiv 1 \pmod{k}, \\
    f^2 \equiv 1 \pmod{k}, \\
    r(e + 1) \equiv 0 \pmod{n/2}, \\
    s(f - 1) \equiv 0 \pmod{n/2}, \\
    r(f + 1) + s(e - 1) \equiv 0 \pmod{n/2},
\end{cases}
$$

where $r, s \in \mathbb{Z}_{n/2}$, $e, f \in \mathbb{Z}_k$. If $n = 8m$ where $m \geq 3$ is an odd number, then $(r, s, u, e, f) = (m + 4, m, 1, 4m - 1, 2m - 1)$. This is an infinite family of skew-morphisms of $D_{8m}$ of order $4m$ with $\text{Ker} \, \varphi = \langle a^2 \rangle$, first discovered by Zhang and Du.
Theorem

For \( n \geq 8 \) even, if \( \varphi \) is a smooth skew-morphism of \( D_n \) with \( \text{Ker} \varphi = \langle a^2, b \rangle \), then \( \varphi \) lies in one of the following two families:

(I) skew-morphisms of order \( k \) defined by

\[
\begin{align*}
\varphi(a^{2i}) &= a^{2iu}, \\
\varphi(a^{2i+1}) &= a^{(2i+1)u+2r+1}, \\
\varphi(ba^{2i}) &= ba^{2iu+2s}, \\
\varphi(ba^{2i+1}) &= ba^{2r+2s+2iu+1}
\end{align*}
\]

and

\[
\begin{align*}
\pi(a^{2i}) &= 1, \\
\pi(a^{2i+1}) &= e, \\
\pi(ba^{2i}) &= 1, \\
\pi(ba^{2i+1}) &= e,
\end{align*}
\]

where \( r, s, u, k, e \) are nonnegative integers such that
(i) \( r, s \in \mathbb{Z}_{n/2}, u \in \mathbb{Z}_{n/2}^* \) such that \( u - 1 - 2r \not\equiv 0 \pmod{n/2} \),

(ii) \( k \) is the smallest positive integer such that \( r\sigma(u, k) \equiv 0 \pmod{n/2} \) and \( s\sigma(u, k) \equiv 0 \pmod{n/2} \) where 

\[
\sigma(u, k) = \sum_{i=1}^{k} u^{i-1},
\]

(iii) \( e \in \mathbb{Z}_{k}^* \) such that \( e \not\equiv 1 \pmod{k}, e^2 \equiv 1 \pmod{k} \),

(iv) \( u^{e-1} \equiv 1 \pmod{n/2}, \)

(v) \( r\sigma(u, e - 1) \equiv u - 2r - 1 \pmod{n/2}, \)

(vi) \( s\sigma(u, e - 1) \equiv -u + 2r + 1 \pmod{n/2}. \)
(II) skew-morphisms of order $2(e - 1)$ defined by

$$
\begin{align*}
\varphi(a^{2i}) &= a^{2iu}, \\
\varphi(a^{2i+1}) &= ba^{2r-2iu+1}, \\
\varphi(ba^{2i}) &= ba^{2s+2iu}, \\
\varphi(ba^{2i+1}) &= a^{2r-2s-2iu+1}
\end{align*}
$$

and

$$
\begin{align*}
\pi(a^{2i}) &= 1, \\
\pi(a^{2i+1}) &= e, \\
\pi(ba^{2i}) &= 1, \\
\pi(ba^{2i+1}) &= e,
\end{align*}
$$

where $r, s, u, e$ are nonnegative integers such that

(i) $r, s \in \mathbb{Z}_{n/2}, u \in \mathbb{Z}_{n/2}^*$ and $e > 1$ is an odd number,

(ii) $u^{e-1} \equiv -1 \pmod{n/2},$

(iii) $s\sigma(u, e - 1) \equiv u + 2r + 1 \pmod{n/2}$ where

$$
\sigma(u, e - 1) = \sum_{i=1}^{e-1} u^{i-1},$

(iv) $r\xi(u, e - 1) \equiv s\zeta(u, e - 1) - 1 \pmod{n/2}$ where

$$
\xi(u, e - 1) = \sum_{i=1}^{e-1} (-u)^{i-1} \quad \text{and} \quad \zeta(u, e - 1) = \sum_{i=1}^{(e-1)/2} u^{2(i-1)}.$$

Remark

The skew-morphisms from Class (II) give rise to \( e \)-balanced regular Cayley maps of \( D_n \) of even valency \( 2(e - 1) \), first classified by Kwak, Kwon and Feng in 2006.
Thank you for your attention!