NSUCRYPTO 2020: Orthomorphisms

Ioan Dragomir[1], Gabriel Tulba-Lecu[2], and Mircea-Costin Preoteasa[3]

[1] ioandr@gomir.pw – Technical University of Cluj-Napoca
[2] gabi_tulba_lecu@yahoo.com – Polytechnic Univeristy of Bucharest
[3] mircea_costin84@yahoo.com – Polytechnic Univeristy of Bucharest

Table of Contents

1 Problem summary

The dihedral group of order 2^m, denoted D_{2^m}, $m \geq 4$, is generated by a, u so that:

$$a^{2^{m-1}} = e, \quad u^2 = e, \quad ua = a^{-1}u$$

Intuitively, it describes the symmetries of a regular polygon with 2^{m-1} vertices and two distinct faces, where a is a rotation which circularly permutes the vertices by one position, and u flips it over. By applying a 2^{m-1} times, we do a full rotation and end up at the identity element. Flipping twice has no effect. Applying a rotation (a^k) and then flipping (u) is equivalent to flipping (u) and them applying the opposite rotation (a^{-k}).

Bob proposes the following morphism family, parameterised by:

$$r_1, r_2, c_1, c_2, q_1, q_2, b_1, b_2 \in \{0, \dots, 2^{m-1} - 1\}$$

$$\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}(a^i) = \begin{cases} a^{r_1 i + c_1}, & \text{if } 0 \leq i < 2^{m-2} \\ a^{r_2 i + c_2}u, & \text{if } 2^{m-2} \leq i < 2^{m-1} \end{cases}$$

$$\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}(a^i u) = \begin{cases} a^{q_2 i + b_1}u, & \text{if } 0 \leq i < 2^{m-2} \\ a^{q_2 i + b_2}, & \text{if } 2^{m-2} \leq i < 2^{m-1} \end{cases}$$

θ is an orthomorphism if the mapping $\pi : x \to x^{-1}\theta(x)$ is a permutation on the respective group. In other words, there are no two distinct x_1, x_2 for which $x_1^{-1}\theta(x_1) = x_2^{-1}\theta(x_2)$.

While the visual complexity of the last few ideas may seem daunting, after some closer inspection, they become much tamer beasts.

Question 1: Describe all orthomorphisms θ in D_{2^4} and find their number.

Question 2: For each $m \geq 4$, describe all orthomorphisms θ in D_{2^m}.

2 Solution

2.1 Exploring the $\mathbf{D}_{2^m}$ structure

We start by studying the product of two D_{2^m} elements,

$$\begin{aligned} a^i &\cdot a^j &&= a^{i+j} \\ a^i u &\cdot a^j &&= a^{i-j} u \\ a^i &\cdot a^j u &&= a^{i+j} u \\ a^i u &\cdot a^j u &&= a^{i-j} \end{aligned}$$

the inverse of an element,

$$\begin{aligned} (a^i)^{-1} &= a^{-i} = a^{2^{m-1}-i} \\ (a^i u)^{-1} &= a^i u \end{aligned}$$

and a reduced formula for $\pi(x) \overset{def}{=} x^{-1}\theta(x)$:

$$\pi(a^i) = (a^i)^{-1}\theta(a^i) = \begin{cases} a^{-i} a^{r_1 i + c_1} \\ a^{-i} a^{r_2 i + c_2} u \end{cases} = \begin{cases} a^{r_1 i + c_1 - i}, & \text{if } i < 2^{m-2} \\ a^{r_2 i + c_2 - i} u, & \text{if } i \geq 2^{m-2} \end{cases}$$

$$\pi(a^i u) = (a^i u)^{-1}\theta(a^i u) = \begin{cases} a^i u a^{q_1 i + b_1} \\ a^i u a^{q_2 i + b_2} u \end{cases} = \begin{cases} a^i a^{-q_1 i - b_1} u, & \text{if } i < 2^{m-2} \\ a^i a^{-q_2 i - b_2} u u, & \text{if } i \geq 2^{m-2} \end{cases}$$

$$\pi(a^i) = \begin{cases} a^{i(r_1 - 1) + c_1}, & \text{if } i < 2^{m-2} \\ a^{i(r_2 - 1) + c_2} u, & \text{if } i \geq 2^{m-2} \end{cases}$$

$$\pi(a^i u) = \begin{cases} a^{i(1 - q_1) - b_1} u, & \text{if } i < 2^{m-2} \\ a^{i(1 - q_2) - b_2}, & \text{if } i \geq 2^{m-2} \end{cases}$$

2.2 Splitting the problem in half

We can separate all D_{2^m} elements into two classes:

$$A = \{a^i \mid 0 \leq i < 2^{m-2}\} \cup \{a^i u \mid 2^{m-2} \leq i < 2^{m-1}\}$$
$$B = \{a^i u \mid 0 \leq i < 2^{m-2}\} \cup \{a^i \mid 2^{m-2} \leq i < 2^{m-1}\}$$

Observation 1
When put through π, any element of A will become something of the form a^i, and any element of B will become $a^i u$.

Observation 2
If (r_1, c_1, q_2, b_2) produce a bijective mapping from A to $\{a^i \mid 0 \leq i < 2^{m-1}\}$, and so do (r_2, c_2, q_1, b_1) from B to $\{a^i u \mid 0 \leq i < 2^{m-1}\}$, the morphism θ, given by their combination, will be bijective from D_{2^m} to D_{2^m}. Thus the two sub-problems are independent.

We will study the sub-problem (r_1, c_1, q_2, b_2) and change our focus from A to $\mathbb{Z}_{2^{m-1}}$, by considering the following mapping, which "extracts" a's exponent, as well as its inverse which constructs an element of A given its a exponent:

$$f_A : A \to \mathbb{Z}_{2^{m-1}}$$
$$f_A(a^i u^j) = i, \quad i \in \{0, \ldots, 2^{m-1}\}, \quad j \in \{0, 1\}$$
$$f_A^{-1}(i) = \begin{cases} a^i, & \text{if } i < 2^{m-2} \\ a^i u, & \text{if } i \geq 2^{m-2} \end{cases}$$

These help us define a function g_A which describes how π acts on the a exponents of elements in A:

$$g_A : \mathbb{Z}_{2^{m-1}} \to \mathbb{Z}_{2^{m-1}}$$
$$g_A(i) = f_A(\pi(f_A^{-1}(i)))$$
$$g_A(i) = \begin{cases} f_A(\pi(a^i)) \\ f_A(\pi(a^i u)) \end{cases} = \begin{cases} f_A(a^{i(r_1-1)+c_1}), & \text{if } i < 2^{m-2} \\ f_A(a^{i(1-q_2)-b_2}), & \text{if } i \geq 2^{m-2} \end{cases}$$
$$g_A(i) = \begin{cases} i(r_1 - 1) + c_1, & \text{if } i < 2^{m-2} \\ i(1 - q_2) - b_2, & \text{if } i \geq 2^{m-2} \end{cases}$$

Similarly, if we define these functions' counterparts for B:

$$f_B : B \to \mathbb{Z}_{2^{m-1}}$$
$$f_B(a^i u^j) = i$$
$$f_B^{-1}(i) = \begin{cases} a^i u, & \text{if } i < 2^{m-2} \\ a^i, & \text{if } i \geq 2^{m-2} \end{cases}$$

$$
\begin{aligned}
&g_B : \mathbb{Z}_{2^{m-1}} \to \mathbb{Z}_{2^{m-1}} \\
&g_B(i) = f_B(\pi(f_B^{-1}(i))) \\
&g_B(i) = \begin{cases} i(r_2 - 1) + c_2, & \text{if } i < 2^{m-2} \\ i(1 - q_1) - b_1, & \text{if } i \geq 2^{m-2} \end{cases}
\end{aligned}
$$

Observation 3

g_A and g_B have identical structures. Given any solution (r_1, c_1, q_2, b_2) for which g_A is bijective, the same parameters will also make g_B bijective, and vice versa. Thus, the two sub-problems are equivalent.

From now on, we will study a sub-problem (r, c, q, b) which has a solution if g is bijective:

$$
\begin{aligned}
&g : \mathbb{Z}_{2^{m-1}} \to \mathbb{Z}_{2^{m-1}} \\
&g(i) = \begin{cases} i(r - 1) + c, & \text{if } i < 2^{m-2} \\ i(1 - q) - b, & \text{if } i \geq 2^{m-2} \end{cases}
\end{aligned}
$$

2.3 Solving the sub-problem

We continue by further subdividing the problem into three cases, based on the congruence of $r - 1$ and $1 - q$ modulo 4:

Multiples of 4

$$
\begin{aligned}
r - 1 \equiv 0 \pmod 4 \quad &\Rightarrow \quad g(0) = g(2^{m-3}) = c \\
1 - q \equiv 0 \pmod 4 \quad &\Rightarrow \quad g(2^{m-2}) = g(2^{m-3} + 2^{m-2}) = -b
\end{aligned}
$$

If either is true, g is not a bijection. Thus no solutions exist for $r = 4k+1$ or $q = 4k+1$.

Other multiples of 2, i.e. $4k + 2$

Studying the first branch of g, (i.e. $0 \leq i < 2^{m-2}$) we show that $i(r-1) + c$ covers only elements with the same parity as c:

$$
i(r-1) + c \;\equiv\; i(4k+2) + c \;\equiv\; 2i(2k+1) + c \;\equiv\; c \pmod 2
$$

and that all of those elements are visited. We can prove this by contradiction. Suppose there exist $i_1 \neq i_2$ such that $g(i_1) = g(i_2)$, then:

$$
\begin{aligned}
&i_1(r-1) + c - i_2(r-1) - c = \alpha 2^{m-1}, \text{ for some } \alpha \in \mathbb{Z} \\
&i_1(r-1) - i_2(r-1) = \alpha 2^{m-1} \\
&(r-1)(i_1 - i_2) = \alpha 2^{m-1} \\
&(4k+2)(i_1 - i_2) = \alpha 2^{m-1}, \text{ for some } k \in \mathbb{Z} \\
&(2k+1)(i_1 - i_2) = \alpha 2^{m-2} \\
\iff &(2k+1)(i_1 - i_2) \equiv 0 \pmod{2^{m-2}}
\end{aligned}
$$

$2k+1$ is invertible modulo 2^{m-2}, because $\gcd(2k+1, 2^{m-2}) = 1$, therefore the only solution is when $i_1 - i_2 \equiv 0 \pmod{2^{m-2}}$. Since $i_1, i_2 < 2^{m-2}$, $i_1 = i_2$, which is a contradiction.

By the same logic, the branch $i(1-q)-b,\ 2^{m-2} \leq i < 2^{m-1}$ also maps to all elements with the same parity as b.

Sufficiency: If $r-1$ and $1-q$ are both of the form $4k+2$, then g is a bijection if b and c have opposite parities, so that the image of one branch is all the even elements, and the image of the other branch is all the odd elements.

Necessity: If $r-1$ is of the form $4k+2$, then $1-q$ must also be. Otherwise, it's either $4k$, which we proved to be invalid, or $2k+1$. In the latter case, $i(1-q)+b$ will cover elements of both parities. As $i(r-1)+c$ covers all elements of some parity, there will be at least some overlapping between the two branches' images. Therefore the only option for $1-q$ is $4k+2$. If we fix $1-q$ to have this form, $r-1$ is also forced to be the same.

Odd numbers

The only case left is when $r-1$ and $1-q$ are both odd.

Given a linear function $F(x) = ax + b$ on $x \in \{0, \ \ldots, \ 2^{m-2}-1\}$, we can create $F'(x) = -ax + a2^{m-2} - a + b$ which generates the same results, but in opposite order $(F'(x) = F(2^{m-2} - x - 1))$.

Observation 4 *Given an image which is generated by a linear function from $\mathbb{Z}_{2^{m-2}}$ to $\mathbb{Z}_{2^{m-1}}$, there are exactly 2 linear functions which generate that image, of the forms $F(x)$ and $F'(x)$.*

We fix the first branch of g to be $ax+b$. Since a is odd, we know it covers exactly half of $\mathbb{Z}_{2^{m-1}}$. The image of the second branch, let it be B, must then correspond to all the additive inverses of the values generated by the first branch.

One linear function on $x \in \{2^{m-2}, \ \ldots, \ 2^{m-1}-1\}$ which has the image B is $ax+b$ once again. Therefore there must be only one other linear function which generates the image, but in reversed order: $-ax-a+b$. It follows from Obs. 4 that there are no other linear functions on $x \in \{2^{m-2}, \ \ldots, \ 2^{m-1}-1\}$ which generate B.

Going back to the initial notation for g, we have two valid bijections:

$$g_1(i) = \begin{cases} (r-1)i + c, & \text{if } 0 \leq x < 2^{m-2} \\ (r-1)i + c, & \text{if } 2^{m-2} \leq x < 2^{m-1} \end{cases}$$
$$\Rightarrow \quad q_1 \equiv -r, \ b_1 \equiv -c$$

$$g_2(i) = \begin{cases} (r-1)i + c, & \text{if } 0 \leq x < 2^{m-2} \\ -(r-1)i + 2^{m-2} - r + 1 + c, & \text{if } 2^{m-2} \leq x < 2^{m-1} \end{cases}$$
$$\Rightarrow \quad q_2 \equiv r, \ b_2 \equiv -2^{m-2} + r - c - 1$$

2.4 Question 2: Describing and counting all θ orthomorphisms

The sub-problem (r, c, q, b) has the following solution cases:

$\mathrm{p}(2k) = 0$
$\mathrm{p}(2k+1) = 1$

$$(4i+3,\ j,\ 4k+3,\ l),\quad 0 \le i,k < 2^{m-3},\quad 0 \le j,l < 2^{m-1},\quad \mathrm{p}(j) \ne \mathrm{p}(l)$$
$$\Rightarrow \quad 2^{m-3} \cdot 2^{m-1} \cdot 2^{m-3} \cdot 2^{m-2} = 2^{4m-9} \text{ solutions.}$$

$$(2i+1,\ j,\ -2i-1,\ -j),\quad 0 \le i < 2^{m-2},\quad 0 \le j < 2^{m-1}$$
$$\Rightarrow \quad 2^{m-2} \cdot 2^{m-1} = 2^{2m-3} \text{ solutions.}$$

$$(2i+1,\ j,\ 2i+1,\ 2^{m-2}+2i+1-j),\quad 0 \le i < 2^{m-2},\quad 0 \le j < 2^{m-1}$$
$$\Rightarrow \quad 2^{m-2} \cdot 2^{m-1} = 2^{2m-3} \text{ solutions.}$$

For a total of $2^{4m-9} + 2^{2m-3} + 2^{2m-3} = 2^{2m-2}(2^{2m-7}+1)$ solutions for the sub-problem. The orthomorphisms θ are decomposed into two independent such sub-problems, so the number of θ solutions is the square of the number of solutions to the sub-problems, or

$$(2^{2m-2}(2^{2m-7}+1))^2 = 2^{4m-4}(2^{4m-14} + 2^{2m-6} + 1) =$$
$$\mathbf{2^{8m-18} + 2^{6m-10} + 2^{4m-4}}$$

2.5 Question 1

In the special case $m = 4$, $\theta^{(r_1,r_2,c_1,c_2)}_{(q_1,q_2,b_1,b_2)}$ is an orthomorphism when both (r_1, c_1, q_2, b_2) and (r_2, c_2, q_1, b_1) are of one of the forms:

$$\begin{array}{lll}
(4i+3,\ j,\ 4k+3,\ l), & i,k \in \{0,1\}, \quad j,l \in \{0,\dots,7\}, & \mathrm{p}(j) \ne \mathrm{p}(l) \\
(2i+1,\ j,\ -2i-1,\ -j), & i \in \{0,1,2,3\}, \quad j \in \{0,\dots,7\} & \\
(2i+1,\ j,\ 2i+1,\ 5+2i-j), & i \in \{0,1,2,3\}, \quad j \in \{0,\dots,7\} &
\end{array}$$

The number of solutions is $2^{8\cdot 4-18} + 2^{6\cdot 4-16} + 2^{4\cdot 4-4} = 36864$