Problem Author: Reinier Schmiermann

■ **Problem:** Reverse engineer the  $\leq$  20000 operators using  $\leq$  1400 queries:

$$f_n(a_0,\ldots,a_n) := (\ldots(((a_0 \circ p_1 a_1) \circ p_2 a_2) \circ p_3 a_3) \ldots \circ p_n a_n) \bmod 10^9 + 7$$

Statistics: 14 submissions, 0 accepted, 10 unknown

BAPC 2021 November 1, 2021

Problem Author: Reinier Schmiermann

**Problem:** Reverse engineer the  $\leq 20000$  operators using  $\leq 1400$  queries:

$$f_n(a_0,\ldots,a_n) := (\ldots(((a_0 \circ p_1 a_1) \circ p_2 a_2) \circ p_3 a_3) \ldots \circ p_n a_n) \bmod 10^9 + 7$$

• First solve the problem for 15 operators with a single query  $0, q_1, \ldots, q_{15}$ .

Statistics: 14 submissions, 0 accepted, 10 unknown

BAPC 2021 November 1, 2021

9 / 24

П

Problem Author: Reinier Schmiermann

■ **Problem:** Reverse engineer the  $\leq$  20000 operators using  $\leq$  1400 queries:

$$f_n(a_0,\ldots,a_n) := (\ldots(((a_0 \circ p_1 a_1) \circ p_2 a_2) \circ p_3 a_3) \ldots \circ p_n a_n) \bmod 10^9 + 7$$

- First solve the problem for 15 operators with a single query  $0, q_1, \ldots, q_{15}$ .
- Use this to find all operators in 20000/15 < 1400 queries.

Statistics: 14 submissions, 0 accepted, 10 unknown

BAPC 2021 November 1, 2021

9/24

•

Problem Author: Reinier Schmiermann

**Problem:** Reverse engineer the  $\leq$  20000 operators using  $\leq$  1400 queries:

$$f_n(a_0,\ldots,a_n):=(\ldots(((a_0 op_1 a_1) op_2 a_2) op_3 a_3)\ldots op_n a_n) \bmod 10^9+7$$

- First solve the problem for 15 operators with a single query  $0, q_1, \ldots, q_{15}$ .
- Use this to find all operators in 20000/15 < 1400 queries.
- Example with 30 operators:

Recover last 15 operators:

????	? ??	? ???	Ор	S	
00000	00 919	$q_1 \dots q_1$	5 Qu	ery	1
16					

+0 and  $\times 1$  do not change the query outcome.

Continue with the next 15 operators.

?????	+x++x	Ops
$0q_1 \dots q_{15}$	01001	Query 2

Statistics: 14 submissions, 0 accepted, 10 unknown

Problem Author: Reinier Schmiermann

■ We consider the case with 15 operators.

10 / 24

Problem Author: Reinier Schmiermann

- We consider the case with 15 operators.
- Let  $0, q_1, ..., q_{15}$  where  $q_i$  is random in  $\{1, ..., 10^9 + 6\}$ .

BAPC 2021 November 1, 2021

10 / 24

ш

Problem Author: Reinier Schmiermann

- We consider the case with 15 operators.
- Let  $0, q_1, \ldots, q_{15}$  where  $q_i$  is random in  $\{1, \ldots, 10^9 + 6\}$ .
- For all 2<sup>15</sup> possibilities for the 15 operators compute the query outcome.

BAPC 2021 November 1, 2021

10 / 24

ш

Problem Author: Reinier Schmiermann

- We consider the case with 15 operators.
- Let  $0, q_1, \ldots, q_{15}$  where  $q_i$  is random in  $\{1, \ldots, 10^9 + 6\}$ .
- For all 2<sup>15</sup> possibilities for the 15 operators compute the query outcome.
- If all outcomes are distinct  $(\text{mod }10^9 + 7)$  we have a lookup table.

BAPC 2021 November 1, 2021

10 / 24

•

Problem Author: Reinier Schmiermann

- We consider the case with 15 operators.
- Let  $0, q_1, \ldots, q_{15}$  where  $q_i$  is random in  $\{1, \ldots, 10^9 + 6\}$ .
- For all 2<sup>15</sup> possibilities for the 15 operators compute the query outcome.
- If all outcomes are distinct  $(\text{mod }10^9 + 7)$  we have a lookup table.
- If not, repeat with a new random query.

BAPC 2021 November 1, 2021

10 / 24

•