

# 問題G: XOR回路

---

Writer: 吉田

Tester: 平澤

# 問題

- \* 関数 $f(x_1, \dots, x_n)$ がオラクルとして与えられる。
  - \* 引数を渡すと、 $f$ の値が返って来る。
- \* ある $j_1, \dots, j_k$ が存在して、以下を満たす。
$$f(x_1, \dots, x_n) = x_{j_1} + \dots + x_{j_k} \pmod{2}$$
- \*  $f$ へのクエリ回数 $\leq 200$ で $j_1, \dots, j_k$ を求めよ。
- \*  $j_1, \dots, j_k$ のことを**関係ビット**と呼ぶ。

# 解法その1: アイデア

- \* XORであることを利用。
- \*  $f(x_1, \dots, x_n) = 1$ な  $x_1, \dots, x_n$  が与えられたとする。
- \*  $\{i \mid x_i = 1\}$ は関係ビットを必ず含む。

$$f(\begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline \end{array}) = 1$$

$j_1$        $j_2$        $j_3$        $j_4$

- \* 更にどう絞り込む？

# 解法その1: アイデア

$f(x_1, \dots, x_{n/2}, 0, \dots, 0) + f(0, \dots, 0, x_{n/2+1}, \dots, x_n) = 1$  が成立

$$\left. \begin{array}{l} f(\boxed{0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0}) = 1 \\ \qquad\qquad\qquad j_1 \qquad\qquad\qquad j_2 \qquad\qquad\qquad j_3 \qquad\qquad\qquad j_4 \\ + \\ f(\boxed{0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1}) = 0 \\ \qquad\qquad\qquad j_1 \qquad\qquad\qquad j_2 \qquad\qquad\qquad j_3 \qquad\qquad\qquad j_4 \\ || \\ f(\boxed{0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1}) = 1 \\ \qquad\qquad\qquad j_1 \qquad\qquad\qquad j_2 \qquad\qquad\qquad j_3 \qquad\qquad\qquad j_4 \end{array} \right\} \text{どちらか片方は1}$$

# 解法その1: アイデア

- \*  $f(x_1, \dots, x_{n/2}, 0, \dots, 0) = 1$  の時：
    - \*  $\{i \in \{1, \dots, n/2\} \mid x_i = 1\}$  は関係ビットを含む。
  - \*  $f(0, \dots, 0, x_{n/2+1}, \dots, x_n) = 1$  の時も同様。
  - \* 関係ビットが存在する範囲を半分に狭められた。
- 
- \*  $\log n$  回繰り返せば、関係ビット一個を突き止めることが出来る。

# 解法その1: 初期解の発見

- \*  $f(x_1, \dots, x_n) = 1$ な  $x_1, \dots, x_n$  をどうやって得る?
  - \* ランダム!
  - \* ランダムに  $x_1, \dots, x_n$  を決めれば  $f(x_1, \dots, x_n) = 1$  になる確率は  $1/2$ 。
- \* 二つ目以降の関係ビットはどう探す?
  - \*  $x_1, \dots, x_n$  をランダムに決める際に、既に関係ビットと分かっている箇所は 0 に設定。
  - \* 関係ビットが残っている限り  $f(\dots) = 1$  になる確率は  $1/2$ 。

# 解法その1: クエリ数

- \*  $q_{\text{init}}$ : 初期解の発見にかかる総クエリ数
- \* 総クエリ数  $q$  は、以下で抑えられる。

$$q = k(q_{\text{init}} + \log n)$$

- \*  $q_{\text{init}}$  の平均は 2、 $q_{\text{init}} \geq t$  となる確率は  $1/2^{t-1}$  なので、 $q$  は十分小さい。

# 解法その2

- \*  $f(x_1, \dots, x_n) \neq f(y_1, \dots, y_n)$  なる  $\{x_i\}, \{y_i\}$  が有るとする。
- \* 以下の様なビット列の列を考える。

$$f(\begin{array}{|c|c|c|c|c|c|c|c|} \hline x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ \hline y_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ \hline \end{array}) = 0$$

⋮

$$\begin{array}{|c|c|c|c|c|c|c|c|} \hline y_1 & y_2 & y_3 & y_4 & x_5 & x_6 & x_7 & x_8 \\ \hline \end{array}$$

⋮

$$f(\begin{array}{|c|c|c|c|c|c|c|c|} \hline y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & y_8 \\ \hline \end{array}) = 1$$

# 解法その2

- \* 先のビット列の上で二分探索を行うと、

$f(y_1, \dots, y_{i-1}, x_i, x_{i+1}, \dots, x_n) \neq f(y_1, \dots, y_{i-1}, y_i, x_{i+1}, \dots, x_n)$   
な $i$ を見つけることが出来る。

- \* 明らかに $i$ は関係ビット。

- \* クエリ数の解析はほぼ同じ。

# 統計

---

- \* First Accept: OgieKako (73:13)
- \* 正解者: 7人
- \* 挑戦者: 15人
- \* 投稿数: 30
- \* 正答率: 23%