Linear Upper Bound on a Segment XOR Cardinality

Nika Skybytska, n.skybytskyi@knu.ua

Taras Shevchenko National University of Kyiv

April 10, 2025

Bitwise XOR (exclusive or) is a fundamental operation in theoretical computer science. Example: $10 \oplus 3$ (in binary):

$$\begin{array}{rl} 10 & = 1010_2 \\ 3 & = 0011_2 \\ \hline 10 \oplus 3 & = 1001_2 = 9 \end{array}$$

Definition

We study properties of XOR applied to sets, defined as $X \oplus Y = \{x \oplus y \mid x \in X, y \in Y\}$.

Let $X = \{1, 2\}$ and $Y = \{3, 4\}$. $X \oplus Y = \{1, 2, 5, 6\}$:

$\oplus$	3	4
1	2	5
2	1	6

Let $X = \{1, 2, 3\}$ and $Y = \{2, 3, 4\}$. $X \oplus Y = \{0, 1, 2, 3, 5, 6, 7\}$:

$\oplus$	2	3	4
1	3	2	5
2	**0**	*1*	6
3	*1*	**0**	7

Definition

Focus on XORs of segments of consecutive integers:
$[l, r) = \{l, l + 1, \ldots, r - 1\}$.

Problem

Given a positive integer k, solve $|[x, x + k) \oplus [y, y + k)| \to \max_{x,y}$ over nonnegative integers x, y.

Remark 1

Two subproblems: establish an **upper bound** and provide an efficient **construction**. Both experimental and analytical methods are fine.

Theorem

$|[x, x+k) \oplus [y, y+k)| \leq 5(k-2)$ for all $k \geq 5$.

Remark 2

Our result improves on the naive quadratic upper bound:

$$|X \oplus Y| \leq |X| \cdot |Y| = k^2. \tag{1}$$

Proposition

$|[x, x+k) \oplus [y, y+k)| \leq 4(k-1)$ for all $k > 1$.

Remark 3

This bound is tight for infinitely many values of $k = 2^m + 2$. The construction is $x = 2^m - 1$, $y = 3 \cdot 2^m$.

Lemma

For any fixed k, the optimization problem

$$g(k; x, y) = |[x, x + k) \oplus [y, y + k)| \to \max_{x,y} \tag{2}$$

has an optimal solution (x_0, y_0) with $x_0, y_0 \leq 4k$.

Corollary

Hence, base cases can be established computationally.

Lemma

If $f(k) = \max_{x,y} g(k; x, y)$*, then:*

$$f(2k) \leq 2f(k+1), \quad f(2k+1) \leq 2f(k+1). \tag{3}$$

Proof

Inductive proof follows from these inequalities:

$$\begin{aligned} f(2k) \leq 2f(k+1) \leq 5(2k-2) \\ f(2k+1) \leq 2f(k+1) \leq 5(2k-1). \end{aligned} \tag{4}$$

- We established a linear upper bound on segment XOR cardinality.
- It is stronger than naive $O(k^2)$ bound.
- Future work: refinement of constant factors.

References

R. P. Stanley. *Enumerative Combinatorics*. Cambridge University Press, 1997.

E. Bach, J. Shallit. *Algorithmic Number Theory*. MIT Press, 1996.

R. Sedgewick, K. Wayne. *Algorithms*. Addison-Wesley, 2011.