Nikita M. Skybytskyi

Linear Upper Bound on a Segment XOR Cardinality

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

In theoretical computer science, bitwise XOR (exclusive or) is a fundamental binary operation on nonnegative integers. We study the properties of bitwise XOR of sets, extending concepts from combinatorial set theory [1]. Namely, for two sets X and Y of nonnegative integers, we denote $X \oplus Y = \{x \oplus y \mid x \in X, y \in Y\}$.

We focus on XORs of segments of consecutive integers, leveraging insights from algorithmic number theory [2]. We use a shorthand notation: $[x, x+k) = \{x, x+1, \ldots, x+k-1\}$ for a nonnegative integer x and a positive integer k. The following result emerged experimentally:

Conjecture. $|[x, x+k) \oplus [y, y+k)| \leq 4(k-1)$ *for any positive integer* k *and nonnegative integers* x, y.

Remark. This bound is tight for infinitely many values of k. One series of particular interest is $k = 2^m + 2$ with $x = 2^m - 1$ and $y = 3 \cdot 2^m$.

This linear upper bound is much stronger than a naive quadratic upper bound of $|X \oplus Y| \leq |X| \cdot |Y| = k^2$. Even though we verified it computationally for all $k \leq 2^9 + 2$, we ultimately failed to prove it rigorously. However, we managed to produce a slightly weaker result:

Theorem. $|[x, x+k) \oplus [y, y+k)| \leq 5(k-2)$ *for any positive integer* $k \geq 5$ *and any nonnegative integers* x, y.

The following lemmas are central to the proof:

Lemma 1. *For any fixed* k*, the optimization problem* $g(k; x, y) = |[x, x+k) \oplus [y, y+k)| \to \max_{x,y}$ *has an optimal solution* (x_0, y_0) *with* $x_0, y_0 \leq 4k$.

Lemma 2. *If we denote* $f(k) = \max_{x,y} g(k; x, y)$ *then two inequalities hold:* $f(2k) \leq 2f(k+1)$ *and* $f(2k+1) \leq 2f(k+1)$*, as inspired by [3].*

The proof of our main result proceeds by induction with the first lemma establishing base cases and the second lemma helping with inductive steps.

[1] R. P. Stanley. *Enumerative Combinatorics.* Cambridge University Press, 1997.
[2] E. Bach and J. Shallit. *Algorithmic Number Theory: Efficient Algorithms.* MIT Press, 1996.
[3] R. Sedgewick and K. Wayne. *Algorithms.* Addison-Wesley, 2011.

E-mail: ✉ *n.skybytskyi@knu.ua.*