XOR of $a_i \oplus x$ and Behavior When XORed Together

Step 1: Write the Expression Clearly

$$\bigoplus_{i=1}^{n} (a_i \oplus x)$$

This means:

$$(a_1 \oplus x) \oplus (a_2 \oplus x) \oplus \cdots \oplus (a_n \oplus x)$$

Step 2: Use XOR Properties (Associative and Commutative)

Because XOR is associative and commutative, we can rearrange terms freely:

$$\bigoplus_{i=1}^{n} (a_i \oplus x) = \left(\bigoplus_{i=1}^{n} a_i \right) \oplus \left(\bigoplus_{i=1}^{n} x \right)$$

Step 3: Simplify $\bigoplus_{i=1}^{n} x$

Since x is XORed with itself n times:

- If n is even, then: $x \oplus x \oplus \cdots \oplus x = 0$
- If n is odd, then: $x \oplus x \oplus \cdots \oplus x = x$

Final formula:

$$\bigoplus_{i=1}^{n} (a_i \oplus x) = \left(\bigoplus_{i=1}^{n} a_i \right) \oplus \begin{cases} 0 & \text{if } n \text{ even} \\ x & \text{if } n \text{ odd} \end{cases}$$

Intuition

XORing all the a_i first, then XORing with x if the count n is odd. If n is even, all the x's cancel out.

How Does This Combination Happen?

Starting with:

$$\bigoplus_{i=1}^{n} (a_i \oplus x) = (a_1 \oplus x) \oplus (a_2 \oplus x) \oplus \cdots \oplus (a_n \oplus x)$$

Step 1: Expand XORs inside parentheses:

$$= a_1 \oplus x \oplus a_2 \oplus x \oplus \cdots \oplus a_n \oplus x$$

Step 2: Use commutativity to rearrange:

$$= a_1 \oplus a_2 \oplus \cdots \oplus a_n \oplus x \oplus x \oplus \cdots \oplus x$$

Step 3: Use associativity to regroup:

$$= \left(\bigoplus_{i=1}^{n} a_i \right) \oplus \left(\bigoplus_{i=1}^{n} x \right)$$

Step 4: Simplify the x's:

$$x \oplus x = 0$$

So, depending on n:

$$\bigoplus_{i=1}^{n} x = \begin{cases} 0 & \text{if } n \text{ even} \\ x & \text{if } n \text{ odd} \end{cases}$$

Summary:

$$\bigoplus_{i=1}^{n} (a_i \oplus x) = \left(\bigoplus_{i=1}^{n} a_i \right) \oplus \begin{cases} 0 & \text{if } n \text{ even} \\ x & \text{if } n \text{ odd} \end{cases}$$

Why Does This Happen?

Because XOR is like addition modulo 2, and it cancels pairs of identical elements. So repeated x's pair up and vanish if even in count, but if odd, one x remains.

Quick Example

Let $n = 3$, $a_1 = 5$, $a_2 = 7$, $a_3 = 2$, $x = 4$
Compute:

$$(5 \oplus 4) \oplus (7 \oplus 4) \oplus (2 \oplus 4)$$

Step-by-step:

$$\begin{aligned} 5 \oplus 4 &= 1 \\ 7 \oplus 4 &= 3 \\ 2 \oplus 4 &= 6 \\ 1 \oplus 3 \oplus 6 &= (1 \oplus 3) \oplus 6 = 2 \oplus 6 = 4 \end{aligned}$$

Now compute XOR of a_i's:

$$5 \oplus 7 \oplus 2 = (5 \oplus 7) \oplus 2 = 2 \oplus 2 = 0$$

Since $n = 3$ is odd:

$$0 \oplus 4 = 4$$

Matches the earlier result!

Why Can You Remove Brackets in XOR Expressions?

Because XOR is:

- **Associative:** $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
- **Commutative:** $a \oplus b = b \oplus a$

What Does This Imply?

With associativity, you can remove brackets safely and XOR everything in a single chain:

$$(a_1 \oplus a_2) \oplus a_3 = a_1 \oplus a_2 \oplus a_3$$

With commutativity, you can reorder terms however you like without changing the result.

Removing Brackets Step-by-Step

Starting with:

$$((a_1 \oplus x) \oplus (a_2 \oplus x)) \oplus (a_3 \oplus x)$$

Remove brackets:

$$= a_1 \oplus x \oplus a_2 \oplus x \Rightarrow a_1 \oplus a_2 \oplus x \oplus x = a_1 \oplus a_2 \oplus 0 = a_1 \oplus a_2$$

Now XOR with $a_3 \oplus x$:

$$(a_1 \oplus a_2) \oplus a_3 \oplus x = a_1 \oplus a_2 \oplus a_3 \oplus x$$

Summary

Removing brackets in XOR is safe because XOR is associative. You can rearrange and regroup terms freely. No ambiguity or issues arise from dropping parentheses in XOR expressions.

Conclusion

$$\bigoplus_{i=1}^{n}(a_i \oplus x) = \left(\bigoplus_{i=1}^{n} a_i\right) \oplus \begin{cases} 0 & \text{if } n \text{ is even} \\ x & \text{if } n \text{ is odd} \end{cases}$$

This identity is valid due to XOR's properties: associativity, commutativity, and self-cancellation.