KNUTH'S NON-ASSOCIATIVE "GROUP" ON $\mathcal{P}(\mathbb{N})$

DOMINIC VAN DER ZYPEN

Abstract. Donald Knuth introduced in [1] a fast approximation to the addition of integers (given in binary) in terms of bit-wise operations by

$$a+b \;\approx\; a\oplus b\oplus((a\wedge b)\ll 1).$$

Generalizing this to infinite bit-strings we get a binary operation on $\mathcal{P}(\mathbb{N})$, the power-set of $\mathbb{N}$ (which we identify with the collection of infinite bit-strings). We show that this operation is "group-like" in that it has a neutral element, inverses, but it is not associative. There are a lot of questions left, which the author has not been able to answer.

1. Introduction

Addition of integers is an important operation in computer science (and in daily life). Knuth [1] noted that for integers a, b given in binary, we have

$$a+b=(a\oplus b)+((a\wedge b)\ll 1),$$

where $\oplus$ denotes bit-wise `XOR`, $\wedge$ is bit-wise `AND` and $\ll 1$ means shifting to left by 1 position.

This identity can be used for an approximation of $+$ using exclusively bit-wise operations[1]:

$$a+b \;\approx\; a\oplus b\oplus((a\wedge b)\ll 1).$$

Note that $((a\wedge b)\ll 1)$ is used to simulate the *carry-bit propagation*.

This approximation is not only of academic interest; it is used in the cryptographic scheme NORX [2], for instance.

[1]These operations are very fast operations in computers, often using only 1 or a very low number of CPU-cycles

2. The binary operation $\oplus$ on $\mathcal{P}(\mathbb{N})$

Let $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ be the collection of non-negative integers and $\mathcal{P}(\mathbb{N})$ be the power-set of $\mathbb{N}$, that is the collection of all subsets of $\mathbb{N}$. By slight abuse of notation, we are going to define an operation $\oplus : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ and will not use $\oplus$ any more as bit-wise `XOR` on finite bit-strings.

For any set $A \in \mathcal{P}(\mathbb{N})$, let $A + 1 = \{a + 1 : a \in A\}$, so $A + 1$ simulates the *left-shift*. Moreover, given $A, B \in \mathcal{P}(\mathbb{N})$, we let

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

be the symmetric difference of A, B. Note that $A \triangle B$ plays the role of bit-wise `XOR`.

Finally, we define for all $A, B \in \mathcal{P}(\mathbb{N})$:

$$A \oplus B := (A \triangle B) \triangle ((A \cap B) + 1).$$

3. Basic properties of $\oplus$

3.1. **Commutativity.** The definition is clearly symmetric on the two variables, so $\oplus$ is commutative.

3.2. **Neutral element.** It is easy to see that the empty set $\emptyset \in \mathcal{P}(\mathbb{N})$ is the neutral element with respect to $\oplus$.

3.3. **Non-associativity.** Let $A = B = \{0\}$ and $C = \{1\}$. Then $(A \oplus A) \oplus C = \{2\}$, but $A \oplus (A \oplus C) = \emptyset$.

4. Inverse elements in $\oplus$

The goal of this section is to show that for every $A \in \mathcal{P}(\mathbb{N})$ there is $A' \in \mathcal{P}(\mathbb{N})$ such that $A \oplus A' = (A \oplus A') \oplus ((A \cap A') + 1) = \emptyset$.

First, a basic observation will be useful later:

Fact 4.1. For any sets X, Y we have $X \triangle Y = \emptyset$ if and only if $X = Y$, so $A \oplus A' = \emptyset$ amounts to saying $A \triangle A' = (A \cap A') + 1$.

Let us first consider a few examples:

- Let $A = \{0\} \in \mathcal{P}(\mathbb{N})$. Then let $A' = \{0, 1\}$.
- More generally, let $A = \{n\}$ for some $n \in \mathbb{N}$. Then $A' = \{n, n + 1\}$.
- Let $A = \{3, 4, 5\}$. Then $A' = \{3, 5, 6\}$.

Note that always we need $\min(A) \in A'$ for $A \neq \emptyset$. Now we are ready to construct A' for general $A \in \mathcal{P}(\mathbb{N})$.

We assume that $A \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$ for the remainder of this section.

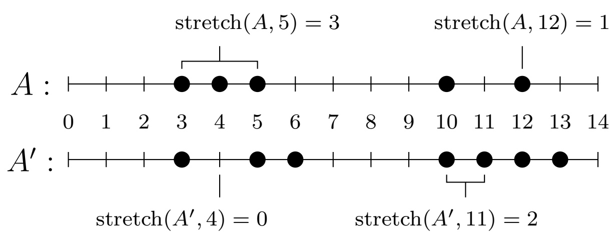
First, for $a \leq b \in \mathbb{N}$ we let $[a, b]$ denote the finite set of integers x with $a \leq x \leq b$. For $n \in \mathbb{N}$ we define the *(backward) stretch of* A with respect to n by

$$\mathrm{stretch}(A, n) = 0 \text{ if } n \notin A,$$

and

$$\mathrm{stretch}(A) = \max\{k \leq n : [n-k, n] \subseteq A\} + 1 \text{ if } n \in A.$$

We first illustrate and motivate graphically the notion of stretch(A, n), as well as the construction of A', for the example $A = \{3, 4, 5, 10, 12\} \in \mathcal{P}(\mathbb{N})$.



We can quickly verify that for $A' = \{3, 5, 6, 10, 11, 12, 13\}$ we have $A \oplus A' = \emptyset$.

Proposition 4.2. Let $A \in \mathcal{P}(\mathbb{N})$ be non-empty, and let

$$\begin{aligned} A' = \{&x \in A : \mathrm{stretch}(A, x) \text{ is odd}\} \cup \\ &\{y \in \mathbb{N} \setminus A : y > 0 \text{ and } \mathrm{stretch}(A, y-1) \text{ is odd}\}. \end{aligned}$$

Then $A \oplus A' = \emptyset$.

(*Note that we call* $n \in \mathbb{N}$ odd *if* $n = 2k + 1$ *for some* $k \in \mathbb{N}$.)

Proof of 4.2. By fact 4.1 we need to show that

$$A \triangle A' = (A \cap A') + 1.$$

In the following we show that either set is a subset of the other set.

$\subseteq$: Suppose that $x \in A \triangle A'$.

Case 1.1 : $x \in A \setminus A'$. This means that stretch$(A, x) > 0$. From $x \notin A'$ and the definition of A' we get that stretch(A, x) is *even*. So in particular stretch$(A, x) \geq 2$, implying $x - 1 \in A$ and $x \geq 1$. Therefore stretch$(A, x - 1)$ is *odd*, implying $x - 1 \in A'$ by definition of A'. So $x - 1 \in (A \cap A')$, whence $x \in (A \cap A') + 1$.

Case 1.2 : $x \in A' \setminus A$. By definition of A', this means that $x > 0$ and $\mathrm{stretch}(A, x-1)$ is odd. So $x - 1 \in A$, and the definition of A' implies $x - 1 \in A'$, yielding $x - 1 \in (A \cap A')$ and $x \in (A \cap A') + 1$.

$\supseteq$: Suppose that $x \in (A \cap A') + 1$. In particular, $x > 0$ and $x - 1 \in (A \cap A')$. The statements $x - 1 \in A'$ and $x - 1 \in A$ and the definition of A' collectively give us:

$$(\star) \qquad \mathrm{stretch}(A, x-1) \text{ is odd.}$$

Case 2.1 : $x \in A$. Statement $(\star)$ and the definition of $\mathrm{stretch}(\cdot, \cdot)$ imply $\mathrm{stretch}(A, x)$ is *even*, and by the definition of A' we get $x \notin A'$. So we get $x \in A \setminus A'$.

Case 2.2 : $x \notin A$. The definition of A' and $(\star)$ jointly imply $x \in A'$, therefore $x \in A' \setminus A$.

So we established that $A \triangle A' = (A \cap A') + 1$, which is equivalent to $A \oplus A' = \emptyset$. $\square$

5. Further inquiries

5.1. Uniquess of solutions to $A \oplus X = B$. I think that the inverses constructed in proposition 4.2 are unique, and there could be an inductive argument showing this. Moreover, it seems that the following more general statement holds:

> For all $A, B \in \mathcal{P}(\mathbb{N})$ there is a unique $X \in \mathcal{P}(\mathbb{N})$ such that $A \oplus X = B$.

5.2. Associative substructures of $(\mathcal{P}(\mathbb{N}), \oplus)$. One interesting direction in the analysis of $\oplus$ is the search for "sub-groups", that is, associative subsets of $\mathcal{P}(\mathbb{N})$ closed under $\oplus$ and inverses. Which finite or infinite Abelian groups are isomorphic to a sub-group of $(\mathcal{P}(\mathbb{N}), \oplus)$? Moreover, Zorn's Lemma implies that every sub-group of $(\mathcal{P}(\mathbb{N}), \oplus)$ is contained in a maximal sub-group with respect to set inclusion $\subseteq$. Does every maximal subgroup of $(\mathcal{P}(\mathbb{N}), \oplus)$ have the same cardinality?

References

[1] Donald E. Knuth, *The Art of Computer Programming, Volume 4A*, Addison-Wesley, Upper Saddle River, New Jersey (2011).

[2] Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves, *Analysis of NORX: Investigating differential and rotational properties*, `https://www.aumasson.jp/data/papers/AJ14a.pdf`