**Tú N. Anh**
Hanoi University of Science and Technology


# Randomized Algorithm for Checking Associativity of Binary Operation

This paper described a randomized algorithm for checking whether a given binary operation has associative property. The solution will prove that the algorithm run in $O(n^2 log(\frac{1}{\delta}))$ time-complexity where n is the number of elements in the binary operation, and $\delta$ is the probality that the algorithm will give the wrong answer.

**Lemma 1.** Given set $S$ and binary operation $(C, \circ)$. We define set $G$ as follows. The element is $G$ are sums of elements of $S$ with coefficients is either 0 or 1. (i.e, $g \in G \Leftrightarrow g = \sum_{s \in S} \alpha_s s$ where $\alpha_s \in \{0, 1\} \forall s \in S$). G is equipped with the following operatation.
(1) Addition: $\sum_s \alpha_s s + \sum_s \beta_s s = \sum_s (\alpha_s + \beta_s) s$ (where $1 + 1 = 0; 0 + 0 = 0; 1 + 0 = 1 + 0 = 1$)
(2) The operation $\circ$ : $(\sum_s \alpha_s s) \circ (\sum_s \beta_s s) = \sum_r \sum_s \alpha_s \beta_s (r \circ s)$
Easily observe that $(C, \circ)$ is associative $\Leftrightarrow$ $(G, \circ)$ is also associative

**Lemma 2.** We can easily see that there are $2^n$ elements in set $G$. Therefore, checking for associativity require us to check for $8^n$ operations of 3 elements in $G$. We are going to prove that if the operation $\circ$ in $G$ is not associative, then more than $\frac{1}{8}$ of 3-element operation is not associative.
**Proof.**
Since $\circ$ is non-associative, there exists $a, b, c \in G$ $(a, b, c \neq 0)$, such that

$$a \circ (b \circ c) \neq (a \circ b) \circ c$$

By definition, we have $a = \sum_{i=1}^{n} \alpha_i s$. Since $a \neq 0$, exists $\alpha_m = 1$. We define set

$$A = \{x = \sum_{i=1}^{n} \alpha_i s | x \in G, \alpha_m = 0\}$$

For every $x \in A$, we consider $(a + x) \circ (b \circ c)$ and $((a + x) \circ b) \circ c$. If they don't equal, we have another 3-element operation that disatifies associativity. If they equal, then since $a, b, c$ disatifies associativity then $x, a, b$ also disatifies associativity.
We can easily observe that $(a + x_i) \neq x_j \forall x_i, x_j \in A$ since $\alpha_m = 1$ in $a$, and $(a + x_i) \neq (a + x_j) \forall x_i, x_j \in A, x_i \neq x_j$
We also have $|A| = 2^{n-1}$, therefore, there are another $2^{n-1}$ set that disatifies associativity. Prove similarly with $b$ and $c$, we have $8^{n-1}$ set that disatifies associativity

**Algorithm.**

1. Choosing randomly 3 element in $G$, from lemma 1, if they dissatify associativity then $S$ is also non-associative. From lemma 2, there is $\frac{1}{8}$ chance for dectecting non-associativity. Checking for associativity will take $O(n^2)$ time-complexity for a brute force solution

2. If we want the error to be an arbitrary $\delta > 0$, repeat step 1 $\log_{8/7} \frac{1}{\delta}$. Therefore, the algorithm runs in $O(n^2 log(\frac{1}{\delta}))$. Choosing $\delta = \frac{1}{n}$, we have an algorithm that runs in $O(n^2 logn)$ time-complexity

In conclusion, if there procedure results in non-associativity, then the outcome is guaranteed since it finds a set that dissatifies associativity. If procedure results in associativity, then the probability of error is $1/n$