Deterministic linear time algorithm finding zero-sums

Hanpil Kang, Seokhwan Choi, Dongjae Lim

August 18, 2022

Abstract

We provide a deterministic linear time algorithm finding zero-sums.

For any integer sequence of length $2n-1$, we can find subsequence of length n, whose sum is divisble by n. [2] We provide deterministic linear time algorithm finding zero-sums. This improves [1].

1 $n = p$ is prime

Let's consider elements in $\mathbb{Z}_p$. $\{a+b \mid a \in A, b \in B\}$ as $A \oplus B$. If a sequence $a = a_1, a_2, \cdots, a_{2p-1}$ contains p identical element, they are zero-sum. Otherwise, we aim to find 0 from $\{(a_1 + a_2 + \cdots + a_p)\} \oplus \{0, d_1\} \oplus \{0, d_2\} \oplus \cdots \oplus \{0, d_{p-1}\}$ where $d_i = a_{i+p} - a_i \neq 0$ with proper renumbering.

We will manage $T_i \subseteq (a_1 + a_2 + \cdots + a_p) \oplus \{0, d_1\} \oplus \{0, d_2\} \oplus \cdots \oplus \{0, d_i\}$ with $|T_i| \geq i$ as following:

$$T_i = \{X\} \oplus \{0, v_1, 2v_1, \cdots, l_1 v_1\} \oplus \{0, v_2, 2v_2, \cdots, l_2 v_2\} \oplus \cdots \oplus \{0, v_k, 2v_k, \cdots, l_k v_k\}$$

- Every $x_i v_i$ with $1 \leq x_i \leq l_1$ is distinct.
- $l_1 + l_2 + \cdots + l_k \geq i$, (especially, it takes $\mathcal{O}(i)$ time finding such representation.)

Start with $T_0 = \{a_1 + \cdots + a_p\}$ and repeat following for $k = 1, \cdots, p-1$:

1. If there exists any $X + x_i v_i = 0$, track which d_i's are added.
2. If d_k coincides with any v_i, change l_i to $l_i + 1$. Otherwise, add new $\oplus\{0, d_k\}$.
3. Repeat following until all sets are disjoint except 0.
   (a) Let $\{0, v_i, \cdots, l_i v_i\}$ and $\{0, v_j, \cdots, l_j v_j\}$ have same element $x_i v_i = x_j v_j$. We will find X', L, g such that $\{X'\} \oplus \{0, g, \cdots, Lg\} \subseteq \{X\} \oplus \{0, l_i v_i, \cdots, l_i v_i\} \oplus \{0, l_j v_j, \cdots, l_j v_j\}$
   (b) For minimum possible x_i, x_j with $x_i v_i = x_j v_j$, calculate $g = v_i / x_j = v_j / x_i$
   (c) If $x_i = 1$ or $x_j = 1$ two sets can be trivially joined, using $X' = X, L = l_i x_j + l_j x_i, g$
   (d) Since every integer greater than $x_i x_j - x_i - x_j$ can be represented as sum of non-negative multiple of x_i and x_j, $\{(x_i x_j - x_i - x_j + 1)g\} \oplus \{0, g, \cdots, (l_j x_i + l_i v_j - 2(x_i x_j - x_i - x_j + 1))g\} \subseteq \{0, v_i, \cdots, l_i v_i\} \oplus \{0, v_j, \cdots, l_j v_j\}$.
   (e) Replace $\{0, v_i, \cdots, l_i v_i\}, \{0, v_j, \cdots, l_j v_j\}$ to $\{X'\} + \{0, g, \cdots, Lg\}$ with $X' = (X + x_i x_j - x_i - x_j + 1)g, L = l_j x_i + l_i x_j - (x_i x_j - x_i - x_j + 1), g$.
   (f) If there exists any $X + x_i v_i = 0$, track which d_i's are added.

1.1 Time complexity

We can sort by counting the array a, calculate modulo inverse mod p for all $p = 1, \cdots, p-1$, so any preparation can be done in $O(p)$ time. If we mark $x_i v_i$ to array (with step v_i), 1, 2, 3(a), 3(f) can be done in $\mathcal{O}(1)$ time. 3(b) can be done in $\mathcal{O}(\min(x_i, x_j))$ time.

For case 3(c), without loss of generality $x_i = 1$, we only have only apply changes to extended element. This can be done by storing values of l_i indexed by v_i. For case 3(d), L extends at least $l_i + l_j - 2$.

Extension length is at least $\min(x_i, x_j)$, therefore 3(b) and 3(e), alongside with 3 can be done in time complexity proportional to the length of extension.

1, 2 runs at most p time, runtime of loop 3 is proportional to the length of extension, which does not exceed p, thus all procedures can be done in $\mathcal{O}(p)$ time.

2 Case for arbitrary n

If $n = 1$, answer is trivially a sequence itself.

If $n = pq$ for prime p, take arbitrary $2p-1$ element, find a zero-sum of size p, and group them $2q-1$ times. Now, calculate zero-sum recursively for $2q-1$ element, each being sum of each group divided by p.

This gives $T(pq) \leq (2q-1)O(p) + T(q) + \mathcal{O}(pq) = T(q) + \mathcal{O}(pq)$. Since $p \geq 2$, $T(pq) = \mathcal{O}(pq)$.

References

[1] Seokhwan Choi, Hanpil Kang, and Dongjae Lim. O(n log n) algorithm for finding a solution of erdős-ginzburg-ziv theorem, 2022.

[2] Paul Erdős, A. Ginzburg, and A. Ziv. A theorem in additive number theory. Bull. Res. Council Israel 10F, 41-43 (1961)., 1961.