Modular Arithmetic Problem in #P

Ohad Asor

January 4, 2016

Abstract

Given n integers $x_1, ..., x_n$, it is obvious that calculating the n LSB bits of the integer part of $\prod_{k=1}^{n}\left[2^{nx_k}+2^{-nx_k}\right]$ has polynomial time complexity if the integers are supplied in unary radix. We show that if the input is supplied in binary (or higher) radix, then this problem is in #P and is actually the counting version of the Partition problem. We also state additional properties of the Partition problem following our analysis.

Our setting is counting the number of solutions to the NP-Complete problem the Partition problem:

Definition 1. Given $n \in \mathbb{N}, \mathbf{x} \in \mathbb{N}^n$, a Partition σ of $\mathbf{x}$ is some $\sigma \in \{-1,1\}^n$. The size of the partition σ $\langle \mathbf{x}, \sigma \rangle = \sum_{k=1}^{n} \sigma_k x_k$. A partition is called a zero partition if its size is zero.

The problem #PART is the following: "Given $\mathbf{x} \in \mathbb{N}^n$, how many zero partition does it have?". This problem is in #P complexity class. The setting of the Partition problem after being reduced from the Boolean Satisfiability problem is n integers to partition each having up to $\mathcal{O}(n)$ binary digits, and this setting is considered Strong-NP. A polynomial time algorithm does not exist for such setting but for the less interesting case where the input is supplied in unary radix, which is exponentially larger than the binary (or higher) one. We now state and prove the main result of this note:

Theorem 2. *Given $n \in \mathbb{N}, \mathbf{x} \in \mathbb{N}^n$, denote $M = \prod_{k=1}^{n}\left[1+4^{nx_k}\right]$ and $s = n\langle \mathbf{x},1\rangle$. Denote the binary digits of M by m_i such that $M = \sum_i m_i 2^i$. Then $\sum_{j=0}^{n} m_{s+j}2^j$ is the number of $\mathbf{x}$'s zero partition out of all possible 2^n partitions.*

Proof. Consider the formula $2\cos a \cos b = \cos(a+b)+\cos(a-b)$ and the cosine being even function to see that:

$$\psi(t) = 2^n \prod_{k=1}^{n} \cos(x_k t) = \sum_{\sigma\in\{-1,1\}^n} \cos t \langle \mathbf{x}, \sigma \rangle = \sum_{\sigma\in\{-1,1\}^n} e^{it\langle \mathbf{x},\sigma\rangle} \qquad (1)$$

We write down the following sum and perform substitution according to (1):

$$S = \frac{1}{n}\sum_{m=1}^{n} \psi\left(\frac{2\pi m}{n} + i\ln 2\right) = \sum_{\sigma\in\{-1,1\}^n} \frac{2^{-\langle \mathbf{x},\sigma\rangle}}{n} \sum_{m=1}^{n} e^{\frac{2\pi i m}{n}\langle \mathbf{x},\sigma\rangle} \qquad (2)$$

multiplying all x_k by n[1] puts $e^{\frac{2\pi i m}{n}\langle n\mathbf{x},\sigma\rangle} = 1$ and we get:

$$S = \sum_{\sigma\in\{-1,1\}^n} 2^{-n\langle \mathbf{x},\sigma\rangle} \tag{3}$$

Denoting the number of partitions that sum to u by

$$c_u = \left|\{\sigma \in \{-1,1\}^n \,|\, \langle n\mathbf{x},\sigma\rangle = u\}\right| \tag{4}$$

then

$$S = \sum_{u=-\infty}^{\infty} c_u 2^{-u} \tag{5}$$

Recalling that $\sum_{u=-\infty}^{\infty} c_u = 2^n$ and c_u are all positive, while in (3) being multiplied by distinct powers $2^{\pm n}$, therefore the summands' binary digits never interfere with each other and can never grow as large as 1, except when $u = 0$. Recalling that c_0 is our quantity of interest, we have proved that the number of zero partitions in $\mathbf{x}$

$$\left\lfloor \frac{2^n}{n} \sum_{m=1}^{n} \prod_{k=1}^{n} \cos\left[nx_k \left(\frac{2\pi m}{n} + i\ln 2 \right) \right] \right\rfloor \mod 2^n \tag{6}$$

$$= \left\lfloor \prod_{k=1}^{n} \left[2^{nx_k} + 2^{-nx_k} \right] \right\rfloor \mod 2^n \tag{7}$$

$$= \left\lfloor 2^{-n\sum_{k=1}^{n} x_k} \prod_{k=1}^{n} \left[1 + 2^{2nx_k} \right] \right\rfloor \mod 2^n \tag{8}$$

Set

$$M = \prod_{k=1}^{n} \left[1 + 2^{2nx_k} \right] = \sum_{\sigma\in\{0,1\}^n} 2^{2n\langle \mathbf{x},\sigma\rangle} \tag{9}$$

then (8) tells us that the number of zero partitions is encoded as a binary number in the binary digits of M, from the s'th dight to the $s+n$ digit. □

Theorem 3. *Given $n \in \mathbb{N}, N \in \mathbb{N}, \mathbf{x} \in \mathbb{N}^n$ then*

$$\frac{1}{N} \sum_{m=1}^{N} \prod_{k=1}^{n} \cos\left(2\pi x_k \frac{m}{N} \right) \tag{10}$$

is the number of partitions of $\mathbf{x}$ having size that is divisible by N without remainder.

[1] While preserving partitions, since we can always multiply all x_k at the same number and keep the exact number of zero partitions.

Proof. Following (1):

$$\frac{1}{N}\sum_{m=1}^{N}\prod_{k=1}^{n}\cos\left(2\pi x_k\frac{m}{N}\right)=\sum_{\sigma\in\{-1,1\}^n}\frac{1}{N}\sum_{m=1}^{N}e^{2\pi i\frac{m}{N}\langle\mathbf{x},\sigma\rangle} \tag{11}$$

the sum of the roots of unity on the rhs is zero if N does not divide $\langle\mathbf{x},\sigma\rangle$, and is one if N does divide it. □

Theorem 4. *Given $n\in\mathbb{N},\mathbf{x}\in\mathbb{N}^n$ then*

$$\int_0^{\pi}\prod_{k=1}^{n}\cos\left(2\pi x_k t\right)dt \tag{12}$$

is the number of zero partitions of $\mathbf{x}$.

Proof. Following (1):

$$2^n\prod_{k=1}^{n}\cos\left(x_k t\right)=\sum_{\sigma\in\{-1,1\}^n}e^{it\langle\mathbf{x},\sigma\rangle} \tag{13}$$

and integrating both sides. □

Corollary 5. $\mathbf{x}\in\mathbb{Q}^n$ *has a zero partition if and only if*

$$\int_0^{\infty}\prod_{k=1}^{n}\cos\left(2\pi x_k t\right)dt=\infty \tag{14}$$

and does not have a zero partition if and only if

$$\int_0^{\infty}\prod_{k=1}^{n}\cos\left(2\pi x_k t\right)dt=0 \tag{15}$$

Proof. Follows from Theorem 4 and, the integrand being periodic, and change of variable to support rationals. □

Remark 6. Corollary 6 is true for all reals too, but a little harder to show and can be proved using characteristic function inversions theorems over the characteristic function we show now:

Corollary 7. *Given $\mathbf{x}\in\mathbb{C}^n$, the function $\prod_{k=1}^{n}\cos\left(x_k t\right)$ is the characteristic function of the random variable that takes uniformly distributed $\sigma\in\{-1,1\}^n$ and returns $\langle\mathbf{x},\sigma\rangle$.*

Proof. Follows from reading (1) as

$$\prod_{k=1}^{n}\cos\left(x_k t\right)=\mathbb{E}_{\sigma\in\{-1,1\}^n}\left[\cos t\left\langle\mathbf{x},\sigma\right\rangle\right]=\mathbb{E}_{\sigma\in\{-1,1\}^n}\left[e^{it\langle\mathbf{x},\sigma\rangle}\right]$$

□

References

[1] Sipser, "Introduction to the Theory of Computation". International Thomson Publishing (1996).

[2] Kac, "Statistical Independence in Probability, Analysis and Number Theory". Carus Mathematical Monographs, No. 12, Wiley, New York (1959)