Modular Arithmetic and Integration Problems in #P Complexity Class

Ohad Asor

January 5, 2016

Abstract

Given n integers $x_1, ..., x_n$, it is obvious that calculating the n LSB bits of the integer part of $\prod_{k=1}^{n} [2^{nx_k} + 2^{-nx_k}]$ 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. In particular, we show that deciding whether definite integrals are zero or infinite is NP-Complete under some settings. We also show how to count all integer partitions that are divisible by a given factor, and relate it to the Trapezoid rule from numerical analysis.

Our setting is counting the number of solutions given an instance of 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 to determine the number of zero partitions given $\mathbf{x}$. The problem PART is deciding whether a zero partition exists or not for $\mathbf{x}$. The *Weak* setting of the problem is when $\mathbf{x}$ is supplied in unary radix, and the *Strong* setting is when it is supplied in binary radix (or another format with same efficiency), therefore the input size is logarithmically smaller on the strong setting.

#PART is in #P complexity class. The setting of the #PART after being reduced from the counting Boolean Satisfiability problem (SAT) is n integers to partition each having up to $\mathcal{O}(n)$ binary digits, demonstrating why the

rather strong setting is of interest. In fact, there exists polynomial time algorithms given the weak setting of PART, notably Dynamic Programming algorithms, as well as the formula we derive here. However, solving PART on the strong setting is not possible in polynomial time (as a function of the input length), unless P=NP.

Theorem 2. *Given* $n \in \mathbb{N}, \mathbf{x} \in \mathbb{N}^n$*, denote* $M = \prod_{k=1}^{n} [1 + 4^{nx_k}]$ *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:

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

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

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

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

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

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

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

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 $\mathbf{x}$

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

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

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

Set

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

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.

Proof. Following (1):

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

where c is defined in (4), and 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. □

Note that the expression in (10) is nothing but the trapezoid rule of order N applied to the following integral:

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

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

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

Proof. Following (1):

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

and integrating both sides. □

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

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

and does not have a zero partition if and only if

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

Proof. Follows from Theorem 4, 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 inversion theorems over the characteristic function we show now:

Corollary 7. *Given* $\mathbf{x} \in \mathbb{C}^n$*, the function* $\prod_{k=1}^{n} \cos(x_k t)$ *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. The characteristic function is generally defined as $\mathbb{E}\left[e^{itX}\right]$ and on our case follows from reading (1) as

$$\prod_{k=1}^{n} \cos(x_k t) = \mathbb{E}_{\sigma \in \{-1,1\}^n} \left[\cos t \langle \mathbf{x}, \sigma \rangle\right] = \mathbb{E}_{\sigma \in \{-1,1\}^n} \left[e^{it\langle \mathbf{x}, \sigma \rangle}\right] \tag{16}$$

□

Corollary 8. *There is no algorithm that takes any function that can be evaluated in polynomial time, and decides in polynomial time whether its integral over the real line is zero (conversley, infinity) unless P=NP.*

Proof. Follows from Corollary 5. □

Theorem 9. *Let $c > 1$ and let w and satisfy*

$$|x_k w(x+iy)| \leq 2\pi \;\; |w'(x+iy)| \leq 1 \tag{17}$$

for all real x and $|y| \leq c$ and holomorphic there, and denote

$$g(t) = w'(t) \prod_{k=1}^{n} \cos(x_k w(t)) \tag{18}$$

Then

$$\left| \int_0^1 \prod_{k=1}^{n} \cos(2\pi x_k t)\, dt - \frac{1}{N} \sum_{m=1}^{N} g\left(2\pi i \frac{m}{N}\right) \right| \leq \frac{2c^{-N}}{c-1} e^{2\pi n} \tag{19}$$

Proof. Since g is analytic, it has a uniformly and absolutly convergent Fourier series for $0 \leq r \leq c$:

$$g\left(re^{i\theta}\right) = \sum_{d=0}^{\infty} b_d r^d e^{id\theta} \tag{20}$$

by (20) we can see that differentiating d times and evaluating on $r = 0$ simply yields $d!b_d$. By Cauchy's integral formula and recalling that $|g(z)| \leq e^{2n\pi}$ for $z \leq 1$, we see that the d'th derivative satisfy

$$\left|g^{(d)}(0)\right| = \left| \frac{d!}{2\pi i} \int\limits_{|z|=1} \frac{g(z)}{z^{d+1}} dz \right| \leq \frac{d!}{c^d} e^{2n\pi} \tag{21}$$

implying

$$b_d \leq c^{-d} e^{2n\pi} \tag{22}$$

rewriting the sum (19) using the Fourier series:

$$\frac{1}{N} \sum_{m=1}^{N} \sum_{d=0}^{\infty} b_d e^{2\pi i d \frac{m}{N}} = \sum_{d=0}^{\infty} b_{dN} \equiv S_N \tag{23}$$

where the first equality is by eliminating the roots of unity that sum to one or zero. We observe that

$$|S_N - S_{N-1}| \leq 2 \sum_{d=N+1}^{\infty} |b_{dN}| \leq e^{2n\pi} \sum_{d=N+1}^{\infty} c^{-dN} = \frac{c^{-N^2}}{c^N - 1} e^{2n\pi} \tag{24}$$

bounding the sum of all increments up to infinity:

$$\sum_{m=N}^{\infty} |S_m - S_{m-1}| \leq e^{2n\pi} \sum_{m=N}^{\infty} \frac{c^{-m^2}}{c^m - 1} \leq 2e^{2n\pi} \sum_{m=N}^{\infty} c^{-m} = \frac{2c^{-N}}{c-1} e^{2n\pi} \tag{25}$$

note that the last inequality in (25) has a lot of room to be tightened and the asymptotic decrease in rather $\mathcal{O}\left(c^{-3N}\right)$. The proof is complete recalling that $\lim_{N\to\infty} S_N$ indeed equals to the integral as the trapezoid rule is nothing but a Riemann partition, and the changing the integration varuable into w. □

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)