Modular Arithmetic and Integration Problems in #P Complexity Class

Ohad Asor

January 7, 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.

1 Preliminaries

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.

2 #PART as Modular Arithmetic Problem

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

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

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

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.

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. □

3 Hardness of Integration

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*

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

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, 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:

Theorem 7. *Given $\mathbf{x} \in \mathbb{C}^n, c > 1$ and w satisfying*

$$|w\left(t + iy\right)| \leq 1 \; w\left(0\right) = 0 \; w\left(1\right) = 1 \; \left|g\left(t + iy\right)\right| \leq 1 \tag{16}$$

for all real t and $|y| \leq c$ and holomorphic there, and g is defined as

$$g(t) = w'(t) \prod_{k=1}^{n} \cos(x_k w(t)) \tag{17}$$

Then

$$\left| \int_0^1 \prod_{k=1}^{n} \cos(2\pi x_k t)\, dt - \frac{1}{N} \sum_{m=1}^{N} g\left(e^{2\pi i \frac{m}{N}}\right) \right| \leq \frac{2c^{-N}}{c-1} \tag{18}$$

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

$$g\left(re^{i\theta}\right) = \sum_{d=0}^{\infty} b_d r^d e^{id\theta} \tag{19}$$

$$\left|g\left(re^{i\theta}\right)\right| \leq e^{-\pi r \sum_k x_k} \prod_{k=1}^{n} \cos(\pi i r x_k) \leq e^{-\pi r \sum_k x_k} \left(e^{\sum_{k=1}^{n} \pi r x_k}\right) = 1 \tag{20}$$

for $z \leq 1$, we see that the d'th derivative of (20) evaluated on $r = 0$ simply yields $d!b_d$. By Cauchy's integral formula

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

implying

$$b_d \leq c^{-d} \tag{22}$$

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

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

bounding the sum of all increments up to infinity:

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

Note that the last inequality in (26) 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. □

4 Probabilistic Setting

Corollary 8. *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

$$\prod_{k=1}^{n} \cos(x_k t) = \mathbb{E}_{\sigma\in\{-1,1\}^n}\left[\cos t \langle \mathbf{x}, \sigma \rangle\right] = \mathbb{E}_{\sigma\in\{-1,1\}^n}\left[e^{it\langle \mathbf{x}, \sigma \rangle}\right] \tag{26}$$

□

Corollary 9. *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 10. *Given $n \in \mathbb{N}, N \in \mathbb{N}, \mathbf{x} \in \mathbb{N}^n$, the variance of the sizes of all partitions is the sum of the squares of the input. Formally:*

$$\sum_{k=1}^{n} x_k^2 = 2^{-n} \sum_{\sigma\in\{-1,1\}^n} \langle \mathbf{x}, \sigma \rangle^2 \tag{27}$$

while

$$\frac{2^n}{N^3} \sum_{m=1}^{N} \frac{\partial^2}{\partial t^2} \prod_{k=1}^{n} \cos(2\pi x_k t)\Bigg|_{t=\frac{m}{N}} \tag{28}$$

is the variance of the sizes of all partitions that their size is divisible by N without remainder.

Proof. Following (1) and differentiating:

$$\prod_{k=1}^{n} \cos\left(\pi x_k t\right) = 2^{-n} \sum_{\sigma \in \{-1,1\}^n} \cos\left(\pi t \left\langle \mathbf{x}, \sigma \right\rangle\right) \tag{29}$$

$$\implies \sum_{\ell=1}^{n} x_\ell \sin\left(\pi x_\ell t\right) \prod_{k \neq \ell}^{n} \cos\left(\pi x_k t\right) = 2^{-n} \sum_{\sigma \in \{-1,1\}^n} \left\langle \mathbf{x}, \sigma \right\rangle \sin\left(\pi t \left\langle \mathbf{x}, \sigma \right\rangle\right) \tag{30}$$

$$\implies \sum_{\ell=1}^{n} \sum_{\ell\prime=1}^{n} -x_\ell \sin\left(\pi x_\ell t\right) x_{\ell\prime} \sin\left(\pi x_{\ell\prime} t\right) \prod_{k \neq \ell, \ell\prime}^{n} \cos\left(\pi x_k t\right) + x_\ell^2 \prod_{k=1}^{n} \cos\left(\pi x_k t\right) \tag{31}$$

$$= 2^{-n} \sum_{\sigma \in \{-1,1\}^n} \left\langle \mathbf{x}, \sigma \right\rangle^2 \cos\left(\pi t \left\langle \mathbf{x}, \sigma \right\rangle\right) \tag{32}$$

and (27) follows by substituting $t = 0$. (27) can be proved using Parseval identity as well. Turning to (28):

$$\frac{2^n}{N} \sum_{m=1}^{N} \frac{\partial^2}{\partial t^2} \prod_{k=1}^{n} \cos\left(2\pi x_k t\right) \Bigg|_{t=\frac{m}{N}} = \sum_{\sigma \in \{-1,1\}^n} \left\langle \mathbf{x}, \sigma \right\rangle^2 \cos\left(2\pi \frac{m}{N} \left\langle \mathbf{x}, \sigma \right\rangle\right) \tag{33}$$

$$= \sum_{u=-\infty}^{\infty} u^2 N^2 c_{Nu} \tag{34}$$

due to aliasing of roots of unity, and c_{Nu} the number of partitions whose size is divisible by Nu as in (4). □

5 Additional Results and Conjectures

Theorem 11. *Let $Z^{\mathbf{x}}$ be the number of zero partitions of a vector of naturals X. Let $D_x^{\mathbf{x}}$ be the number of zero partitions of X after multiplying one if its elements by two, where this element is denoted by x. Let $A_x^{\mathbf{x}}$ be the number of zero partitions of X after appending it x (so now x appears at least twice). Then*

$$Z^{\mathbf{x}} = D_x^{\mathbf{x}} + A_x^{\mathbf{x}} \tag{35}$$

Proof. Denote

$$\psi\left(x_1, \ldots, x_n\right) = 2^n \int_0^{\pi} \prod_{k=1}^{n} \cos\left(x_k t\right) dt \tag{36}$$

then, using the identity $\cos 2x = 2\cos^2 x - 1$:

$$\psi\left(x_1, \ldots, 2x_m, \ldots, x_n\right) = 2^n \int_0^\pi \cos\left(2x_m t\right) \prod_{k \neq m}^{n} \cos\left(x_k t\right) dt \tag{37}$$

$$= 2^n \int_0^\pi \left[2\cos^2\left(x_m t\right) - 1\right] \prod_{k \neq m}^{n} \cos\left(x_k t\right) dt$$

$$\implies \psi\left(x_1, \ldots, x_m, \ldots, x_n\right) - \psi\left(x_1, \ldots, 2x_m, \ldots, x_n\right) = \tag{38}$$

$$2^{n+1} \int_0^\pi \cos^2\left(x_m t\right) \prod_{k \neq m}^{n} \cos\left(x_k t\right) dt = \psi\left(x_1, \ldots, x_m, \ldots, x_n, x_m\right)$$

and the result follows by Theorem 3. □

Conjecture 12. *For all even n, for all $\mathbf{x} \in \mathbb{N}^n$ the number of $\mathbf{x}$'s zero partitions is no more than the number of zero partitions of vector of size n with all its elements equal* 1.

Furthermore, for all odd n, for all $\mathbf{x} \in \mathbb{N}^n$ the number of $\mathbf{x}$'s zero partitions is no more than the number of zero partitions of vector of size n with all its elements equal 1 *except one element that equals* 2.

6 #SAT Reduction

#SAT can be reduced to #SUBSET-SUM using an algorithm described in [1], while various slight variations appear on the literature. #SUBSET-SUM is then trivially reduced into the #PART. The #SAT reduction produces roughly about $4n$ numbers each with n digits, where n is the number of variables plus the number of clauses in the CNF formula. The important aspect we focus here is that those produced numbers have digits that does not exceed 4, and if using radix 6, they never even carry. Therefore the very same digits produced by the reduction can be interpreted in any radix larger than 5, being reduced to a different #PART problem, we're still guaranteed that the number of solution to those #PART problems are independent of the radix, as they're all reduced from the same #SAT problem.

This property might be used to approximate #SAT using the result of Theorem 3. We can see that we can obtain the number of partitions that their size divides a given number N in polynomial time wrt n and the number of digits of x_k, and in exponential time in the number of digits of N. Pick

N to be some small odd prime. The reason that $N = 2$ is uninteresting is the following: it is easy to observe that all 2^n possible partitions of a given vector of naturals are either all even or all odd, and this can be decided in linear time. If they're all odd, then zero partition does not exist.

After we pick prime N, we reduce a #SAT problem into K different #PART problems, each by using different radix. Hueristically and intuitively, the number of partitions divisible by N among those K problems is independent between different problems. We could then use probabilistic reasoning to decide whether the CNF formula is satisfiable or not, without actually solving a single #PART problem, but with multiplying probabilistic estimates of intuitively-independent K #PART problems.

7 Further Research

By using (11) we can get successive estimates to (12) with selecting primes $N = 2, 3, 5, \ldots$. We then could accelerate this sequence using Shanks, Romberg, Pade or similar sequence-acceleration method.

It is also interesting to consider a paper-and-pencil algorithm for calculating a single digit of the result of numbers that are given in the following form: all numbers have the form $1000 \ldots 0001$ so they're fully characterized by the number of zeros in the middle. The numbers are then given as naturals expressing the numbers of zeros, and we'd like to calculate the k'th digit of the result of the multiplication of all those numbers, as (9) and Theorem 1 suggest.

Acknowledgments

Thanks to HunterMinerCrafter for many valuable discussions.

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)