Complementarity of NP-complete problems and their solutions in quantum phase space

1. The easiest hard problem

Given $n \in \mathbb{N}$ and $\{z_k\}_{k=1}^{n} \subset \mathbb{Z}$, we seek $\omega \in \{-1,1\}^n$ such that $\langle \omega, \mathbf{z} \rangle = 0$, where $\langle \omega, \mathbf{z} \rangle = \sum_{k=1}^{n} \omega_k z_k$ denotes the inner product. Deciding whether such ω exists is a NP Complete problem, while counting how many such ω's exist, is in #P. We assume that the inputs $\{z_k\}$ are given in binary radix and denote by d_k the number of binary digits of z_k. The partition problem is known to be Weak-NP since it has a polynomial-time algorithm if the input is supplied in unary radix. To get a feeling about typical dimensions of hard problems, the reduction of n-clause and k-variables 3SAT into the partition problem ends up with $\mathcal{O}(n+k)$ integers to partition, each having $\mathcal{O}(n+k)$ digits [1]. The exponential time hypothesis therefore implies that it is impossible to solve the partition problem in runtime complexity of $\mathcal{O}\left(\text{poly}\left(\sum_{k=1}^{n} d_k\right)\right)$.

The counting version of the partition problem is equivalent to the following definite integral:

Lemma 1. *Let $\{z_k\}_{k=1}^{n} \subset \mathbb{Z}$ be integers given in binary radix. Let also $\psi(x) = \prod_{k=1}^{n} \cos(\pi z_k x)$. Then evaluating $I_{\#P} = \frac{1}{2}\int_{-1}^{1} \psi(x)\, dx$ up to accuracy of n binary digits is in #P.*

Proof. This lemma can be proved in many interesting ways, all seem to go back to the classical monograph by Kac [2]. Slightly different proofs of this lemma may be found in [3, 4]. Our derivation is based on the formula

$$\prod_{k=1}^{n} \cos(z_k) = 2^{-n} \sum_{\omega \in \{-1,1\}^n} \cos\langle \omega, \mathbf{z} \rangle \tag{1}$$

for every $\mathbf{z} \in \mathbb{C}^n$, which follows from a repeated application of the identity

$$4\cos(z_1)\cos(z_2) = \cos(z_1+z_2) + \cos(z_1-z_2) + \cos(-z_1+z_2) + \cos(-z_1-z_2) \tag{2}$$

Using this the integral reads

$$I_{\#P} = 2^{-n-1} \sum_{\omega \in \{-1,1\}^n} \int_{-1}^{1} \cos(\pi x \langle \omega, \mathbf{z} \rangle)\, dx = 2^{-n} \sum_{\omega \in \{-1,1\}^n} \frac{\sin \pi \langle \omega, \mathbf{z} \rangle}{\pi \langle \omega, \mathbf{z} \rangle} = 2^{-n} \sum_{\omega \in \{-1,1\}^n} \delta_{\langle \omega, \mathbf{z} \rangle} \tag{3}$$

where $\delta_m = 1$ if $m = 0$ and $\delta_m = 0$ otherwise. Thus, $I_{\#P}$ is precisely the fraction of zero partitions for $\{z_k\}_{k=1}^{n}$ divided by 2^n. This also explains why an accuracy of at least 2^{-n} is required.

2. Phase space encoding

Suppose that we encode the set of integers $\{z_k\}_{k=1}^{n}$ into $\psi(x)$, the position wave function of a quantum particle, in such a way that

$$\psi(x) \propto \text{rect}\left(\frac{x}{2\alpha}\right) \prod_{k=1}^{n} \cos(\pi z_k x) \tag{4}$$

for some $\alpha \in \mathbb{N}$, where the rectangular function $\mathrm{rect}(x)$ is 1 for $x \in [-1/2,\ 1/2]$, and 0 otherwise. It follows that the solution of the partition counting problem is now manifested in

$$\begin{aligned} \varphi(p) \propto \int_{-\infty}^{\infty} \psi(x) e^{ixp} dx &= 2^{-n} \sum_{\omega \in \{-1,1\}^n} \int_{-\infty}^{\infty} \mathrm{rect}\left(\frac{x}{2\alpha}\right) \cos\left(\pi x \langle \omega, \mathbf{z} \rangle\right) e^{ixp} dx \\ &= \frac{\alpha}{2^n} \sum_{\omega \in \{-1,1\}^n} \mathrm{sinc}\left(\alpha(p - \pi \langle \omega, \mathbf{z} \rangle)\right) + \mathrm{sinc}\left(\alpha(p + \pi \langle \omega, \mathbf{z} \rangle)\right) \quad (5) \end{aligned}$$

the particle's momentum wave function. In particular, $\varphi(\pi m)$ is proportional to the number of m-partitions, those for which the two subsets of integers differ by m, i.e., $\langle \omega, \mathbf{z} \rangle = m$.

The normalized momentum wave function is obtained upon noticing that

$$\int_{-\infty}^{\infty} |\varphi(p)|^2 \, dp = \int_{-\infty}^{\infty} |\psi(x)|^2 \, dx = \int_{-\alpha}^{\alpha} \prod_{k=1}^{n} \cos^2\left(\pi z_k x\right) dx = \frac{2\alpha Z_{2n}}{2^{2n}} \tag{6}$$

where Z_{2n} is the number of zero partitions of the union $\{z_k\}_{k=1}^{n} \cup \{z_k\}_{k=1}^{n}$. Therefore,

$$\varphi(p) = \sqrt{\frac{\alpha}{2Z_{2n}}} \sum_{\omega \in \{-1,1\}^n} \mathrm{sinc}\left(\alpha(p - \pi \langle \omega, \mathbf{z} \rangle)\right) + \mathrm{sinc}\left(\alpha(p + \pi \langle \omega, \mathbf{z} \rangle)\right) \tag{7}$$

The hard instances of the partition problems are characterized by a handful of zero partitions. The problem is known to undergo a phase transition from easy to hard when the ratio $\max_k \log z_k / n$ exceeds 1. We note that the number of partitions $Z_{2n} \geq 2^n$, and $Z_{2n} \approx 2^n$ for hard instances, which renders (with slight abuse of notation)

$$\varphi(p) = \frac{\sqrt{\alpha}}{2^{n/2}} \sum_{\omega \in \{-1,1\}^n} \mathrm{sinc}\left(\alpha(p - \pi \langle \omega, \mathbf{z} \rangle)\right) + \mathrm{sinc}\left(\alpha(p + \pi \langle \omega, \mathbf{z} \rangle)\right) \tag{8}$$

and

$$\varphi(m\pi) = \frac{\sqrt{\alpha}}{2^{n/2}} (1 + \delta_m) Z_m \tag{9}$$

where Z_m denotes the number of m-partitions.

2.1. **Discretization.** The momentum wave function has the interesting property that for large α (of the order of n) it nearly vanishes for non integer multiples of π. This naturally leads to the discretization of $\varphi(p)$. Note that the probability of the particle's momentum to be found in the vicinity of $m\pi$ is

$$P\left(p \in \left[m\pi - \frac{1}{2\alpha},\ m\pi + \frac{1}{2\alpha}\right]\right) = \int_{-\frac{1}{2\alpha}}^{\frac{1}{2\alpha}} \varphi(m\pi + p)^2 dp \approx \frac{\varphi(m\pi)^2}{\alpha} = \frac{(1 + \delta_m)^2 Z_m^2}{2^n} \tag{10}$$

and therefore,

$$|\varphi_d(p)\rangle = 2^{-n/2} \left[2Z_0 |0\rangle + \sum_{m \neq 0} Z_m |m\rangle + \mathcal{O}(\alpha^{-1}) |\text{non integer } m\rangle \right] \tag{11}$$

where the ket $|m\rangle$ represents the momentum eigenfunction associated with $p = m\pi$. Commonly, one is interested in the number of balanced partitions and for that reason $|\varphi_d(p)\rangle$ may be written rather symbolically as

$$|\varphi_d(p)\rangle = \sin\theta |\circ\rangle + \cos\theta |\bullet\rangle \tag{12}$$

where the probability amplitude $\sin\theta = 2^{-n/2+1} Z_0$ is proportional to the number of balanced partitions, $|\circ\rangle$, and $|\bullet\rangle$ is the ket associated with the remaining momentum values.

3. Quantum phase space solution

To read out the solution of the computation one needs to conduct a statistical experiment in which many similar systems are prepared and measured. It can be noted that simply counting the number of systems for which the momentum vanishes will give no advantage over classical brute force solution. It follows that the number of measurements that one needs to carry out in order to determine the smallest nonzero θ is of the order of $1/\theta^2 = \mathcal{O}(2^n)$. This can be recognized upon applying the following unitary to $|\varphi_d(p)\rangle$,

$$|\bar{\varphi}_d(p)\rangle \overset{\text{def}}{=} \left[\frac{1}{\sqrt{2}}|\circ\rangle\left(\langle\circ| + \langle\bullet|\right) + \frac{1}{\sqrt{2}}|\bullet\rangle\left(-\langle\circ| + \langle\bullet|\right)\right]|\varphi_d(p)\rangle \approx \frac{1}{\sqrt{2}}(1+\theta)|\circ\rangle + \frac{1}{\sqrt{2}}(1-\theta)|\bullet\rangle \quad (13)$$

where the approximation holds for hard instances with large n in which case $\sin\theta \approx \theta$ and $\cos\theta \approx 1$. The chances of measuring a vanishing momentum, $|\circ\rangle$, is only slightly above the odds in a fair coin tossing, $\approx \frac{1}{2} + \theta$. This deviation from $1/2$ may generally be detected using $\mathcal{O}(1/\theta^2)$ measurements, which is the essence of the central limit theorem.

3.1. Heisenberg limit speedup.

By (13) the density matrix of the system after the unitary is

$$\rho(\theta) = |\bar{\varphi}_d(p)\rangle\langle\bar{\varphi}_d(p)| \approx \begin{bmatrix} 1/2+\theta & 1/2 \\ 1/2 & 1/2-\theta \end{bmatrix} \quad (14)$$

This representation lends itself to the application of powerful techniques from the field of quantum metrology. Here, a nonzero deviation θ may potentially be detected using far less measurements than in any classical estimation approach. In theory, there exist quantum measurement techniques where the Cramer-Rao lower bound (on the error variance of any unbiased estimator) scales like $1/N^2$ rather than $1/N$, with N the number of measurements. This is known as the Heisenberg limit and has been proven to be the optimal scaling of the error variance of any unbiased estimator. The consequence of this observation in our case is that a nonzero θ may be estimated using $\mathcal{O}(1/\theta) = \mathcal{O}(\sqrt{2^n})$ rather than $\mathcal{O}(1/\theta^2) = \mathcal{O}(2^n)$ measurements. As θ encodes the solution of the NP-complete problem it follows that attaining the Heisenberg limit in quantum metrology amounts to a quadratic speedup.

Recently, arguments have been put forward that the Heisenberg limit may not always be the optimal lower bound. If such claims are proven correct then according to our construction speedups beyond the quadratic limit are potentially feasible.

3.2. Operator-driven speedup.

In this section we propose a different approach for reading out θ which offers a quadratic speedup compared with the classical brute-force solution. It relies on the capacity to actualize the unitary (black box) operator,

$$U_\varphi = 2|\bar{\varphi}_d(p)\rangle\langle\bar{\varphi}_d(p)| - \mathbb{1}, \quad (15)$$

and the operator $U_0 = \mathbb{1} - 2|\circ\rangle\langle\circ|$. The following theorem provides means to obtain θ using $\mathcal{O}(\sqrt{2^n})$ applications of $U_\varphi U_0$.

Theorem 1. *Let* $|+\rangle = \frac{1}{\sqrt{2}}(|\circ\rangle + |\bullet\rangle)$ *and* $|-\rangle = \frac{1}{\sqrt{2}}(|\circ\rangle - |\bullet\rangle)$. *Suppose the initial momentum state of some quantum particle is* $|+\rangle$. *The probability of this particle to evolve into an orthogonal state,* $|-\rangle$, *after* N *applications of the unitary* $U_\varphi U_0$ *is*

$$\left|\langle -|(U_\varphi U_0)^N|+\rangle\right|^2 = \mathcal{O}(N\theta)^2 \quad (16)$$

Proof will be provided later on. Therefore, if a balanced partition exists, $\theta > 0$, then the system evolves to an orthogonal state with probability approaching 1 after $\mathcal{O}(1/\theta) = \mathcal{O}(\sqrt{2^n})$ applications of the unitary. Otherwise, if no balanced partition exists, the system stays in its initial state.

How difficult is it to realize the black box operator U_φ ? If we believe that P $\neq$ NP we are lead to conclude that constructing U_φ is just as hard as the computation process itself, i.e., the resources required for this task scale like $\mathcal{O}(\sqrt{2^n})$. This observation is summarized as follows.

Theorem 2. *Unless the exponential time hypothesis is false, the computational resources required to realize the black box operator U_φ scale at least like $\mathcal{O}(\sqrt{2^n})$.*

4. Nature's ultimate NP-solvers

References

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

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

[3] Johnson, D. S., Garey, M. *Computers and Intractability.* W. H. Freeman and Company (1979).

[4] Moore, C., Mertens, S. *The Nature of Computation.* Oxford University Press, Inc., New York, NY, USA. (2010).