Simon's problem

From Wikipedia, the free encyclopedia
(Redirected from Simon's algorithm)

In computational complexity theory and quantum computing, **Simon's problem** is a computational problem in the model of decision tree complexity or query complexity, conceived by Daniel Simon in 1994.[1] Simon exhibited a quantum algorithm, usually called **Simon's algorithm**, that solves the problem exponentially faster than any (deterministic or probabilistic) classical algorithm.

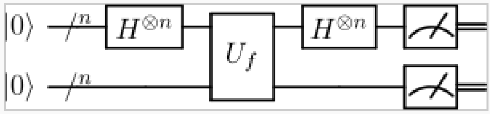
Simon's algorithm uses $O(n)$ queries to the black box, whereas the best classical probabilistic algorithm necessarily needs at least $\Omega(2^{n/2})$ queries. It is also known that Simon's algorithm is optimal in the sense that *any* quantum algorithm to solve this problem requires $\Omega(n)$ queries.[2][3] This problem yields an oracle separation between BPP and BQP, unlike the separation provided by the Deutsch-Jozsa algorithm, which separates P and EQP.

Although the problem itself is of little practical value it is interesting because it provides an exponential speedup over any classical algorithm[*citation needed*]. Moreover, it was also the inspiration for Shor's algorithm. Both problems are special cases of the abelian hidden subgroup problem, which is now known to have efficient quantum algorithms.

Problem description and algorithm [edit]

The input to the problem is a function (implemented by a black box) $f : \{0,1\}^n \to \{0,1\}^n$, promised to satisfy the property that for some $s \in \{0,1\}^n$ we have for all $y, z \in \{0,1\}^n$, $f(y) = f(z)$ if and only if $y = z$ or $y \oplus z = s$. Note that the case of $s = 0^n$ is allowed, and corresponds to f being a permutation. The problem then is to find *s*.

The set of *n*-bit strings is a $\mathbb{Z}_2$ vector space under bitwise XOR. Given the promise, the preimage of *f* is either empty, or forms cosets with *n*-1 dimensions. Using quantum algorithms, we can, with arbitrarily high probability determine the basis vectors spanning this *n*-1 subspace since *s* is a vector orthogonal to all of the basis vectors.



Quantum subroutine in Simon's algorithm

Consider the Hilbert space consisting of the tensor product of the Hilbert space of input strings, and output strings. Using Hadamard operations, we can prepare the initial state

$$\sum_x |x\rangle\,|0\rangle$$

and then call the oracle to transform this state to

$$\sum_x |x\rangle\,|f(x)\rangle$$

Hadamard transforms convert this state to

$$\sum_y \sum_x (-1)^{x \cdot y} |y\rangle\,|f(x)\rangle$$

We perform a simultaneous measurement of both registers. If $s \cdot y = 1$, we have destructive interference. So, only the subspace $s \cdot y = 0$ is picked out. Given enough samples of *y*, we can figure out the *n*-1 basis vectors, and compute *s*.

See also [edit]

- Deutsch-Jozsa algorithm

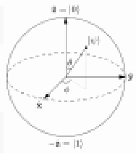
References [edit]

1. ^ Simon, D.R. (1994), "On the power of quantum computation", *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*: 116–123, retrieved 2011-06-06
2. ^ Koiran, P.; Nesme, V.; Portier, N. (2007), "The quantum query complexity of the abelian hidden subgroup

problem", *Theoretical Computer Science* **380** (1-2): 115–126, doi:10.1016/j.tcs.2007.02.057, retrieved 2011-06-06
3. ^ Koiran, P.; Nesme, V.; Portier, N. (2005), "A quantum lower bound for the query complexity of Simon's Problem", *Proc. ICALP* **3580**: 1287–1298, arXiv:quant-ph/0501060, retrieved 2011-06-06

Quantum information science

General		Quantum computer · Qubit · Quantum information · Quantum programming · Timeline of quantum computing
Quantum communication		Quantum capacity · Classical capacity · Entanglement-assisted classical capacity · Quantum channel (Quantum network) · Quantum cryptography (Quantum key distribution) · Quantum energy teleportation · Quantum teleportation · Superdense coding · LOCC · Entanglement distillation
Quantum algorithms		Universal quantum simulator · Deutsch–Jozsa algorithm · Grover's algorithm · Quantum Fourier transform · Shor's algorithm · **Simon's problem** · Quantum phase estimation algorithm · Quantum annealing · Algorithmic cooling
Quantum complexity theory		Quantum Turing machine · BQP · QMA · PostBQP
Quantum computing models		Quantum circuit (Quantum gate) · One-way quantum computer (cluster state) · Adiabatic quantum computation · Topological quantum computer
Decoherence prevention		Quantum error correction · Stabilizer codes · Entanglement-Assisted Quantum Error Correction · Quantum convolutional codes
Physical implementations	**Quantum optics**	Cavity QED · Circuit QED · Linear optical quantum computing
	Ultracold atoms	Trapped ion quantum computer · Optical lattice
	Spin-based	Nuclear magnetic resonance QC · Kane QC · Loss–DiVincenzo QC · Nitrogen-vacancy center
	Superconducting quantum computing	Charge qubit · Flux qubit · Phase qubit



Categories: Quantum algorithms