Journal of Universal Computer Science, vol. 1, no. 3 (1995), 201-204
submitted: 20/1/95, accepted: 27/2/95, appeared: 28/3/95, ©Springer Pub. Co.

Halting probability amplitude of quantum computers*

K. Svozil
Institute for Theoretical Physics, Technische Universät Wien,
Wiedner Hauptstraße 8–10/136, A-1040 Vienna, Austria
e-mail:svozil@tph.tuwien.ac.at

Abstract

The classical halting probability Ω introduced by Chaitin is generalized to quantum computations.

Chaitin's Ω [1, 2, 3] is a magic number. It is a measure for arbitrary programs to take a finite number of execution steps and then halt. It contains the solution for all halting problems, and hence to questions codable into halting problems, such as Fermat's theorem. It contains the solution for the question of whether or not a particular exponential Diophantine equation has infinitely many or a finite number of solutions. And, since Ω is provable "algorithmically incompressible," it is Martin-Löf/Chaitin/Solovay random. Therefore, Ω is both: a mathematicians "fair coin," and a formalist's nightmare.

Here, Ω is generalized to quantum computations.

Consider a (not necessarily universal) quantum computer C and its ith program p_i, which, at time $t \in Z$, can be described by a quantum state [4, 5, 6, 7, 8, 9, 10, 11, 12])

$$|C(t, p_i)\rangle \quad . \tag{1}$$

A typical realisation of C would be by an array of generalized four-port beam splitters [13].

In what follows we shall assume that the program p_i is coded *classically.* That is, we choose a finite code alphabet A and denote by A^* the set of all strings over A. Any program p_i is coded as a classical sequence $\#(p_i) = s_{1i}s_{2i}\cdots s_{ni} \in A^*$, $s_{ji} \in A$. (In what follows, $\#(p_i)$ will be abbreviated by p_i.) We assume prefix coding [14, 1, 15, 3]; i.e., the domain of C is prefix-free such that no admissible program is the prefix of another admissible program. Furthermore, without loss of generality, we consider only empty input strings.

*The quantum omega was invented in a meeting of G. Chaitin, A. Zeilinger and the author (K. S.) in a Viennese coffee house (Café Bräunerhof) in January 1991. Thus, the group should be credited for the original invention, whereas any blame should remain with the author.

In quantum information theory, the state $|C(t,p_i)\rangle$ of the computer C with program p_i is representable by quantum bits (qbits). Every qbit is in a coherent superposition of the classical bit basis $|0\rangle$ and $|1\rangle$. Assume that the states (1) are orthogonal and normalized. The computer C evolves according to a unitary operator U such that (discrete time evolution)

$$\begin{aligned} |C(t,p_i)\rangle &= U|C(t-1,p_i)\rangle && (2)\\ &= U^t|C(0,p_i)\rangle \quad . && (3) \end{aligned}$$

More specifically, a quantum computer can be in a coherent superposition of the halting and the non-halting state [6, 16]

$$|a,b\rangle = a|HALT\rangle + b|GO\rangle \quad , \qquad |a|^2+|b|^2=1 \tag{4}$$

We shall call this quantum bit $|a,b\rangle$ the *halting bit.* The symbols "$|HALT\rangle$" and "$|GO\rangle$" represent orthonormal vectors [17] in the twodimensional complex Hilbert space spanned by them. Let the halting state $|e^{i\varphi},0\rangle = |HALT\rangle$, $\varphi \in R$ be the physical realization that the computer has "halted;" likewise let $|0,e^{i\varphi}\rangle = |GO\rangle$, $\varphi \in R$ be the physical realization that the computer has not "halted." Note that, since quantum computations are governed by unitary evolution laws which are reversible, the halting state does not mean that the computer does not change as time evolves. It just means that it has set a signal — the halting bit — to indicated that it has finished its task. a and b are complex numbers which are a quantum mechanical measure of the probability amplitude that the computer is in the halting and the non-halting states, respectively. (The corresponding probabilities are $|a|^2$ and $|a|^2$, respectively.) One important feature of the quantum information concept ist that it does not merely allow two-valued states but a coherent superposition thereof.

In the orthonormal halting basis $\{|HALT\rangle, |GO\rangle\}$, the computer C with classical input p_i can be represented by

$$|C(t,p_i)\rangle = |HALT\rangle\langle HALT|C(t,p_i)\rangle + |GO\rangle\langle GO|C(t,p_i)\rangle \quad . \tag{5}$$

In the spirit of quantum recursion theory [16], assume that initially, i.e., at time $t=0$, the computer is prepared such that its halting bit is in a coherent 50:50-superposition; i.e., in terms of the halting basis,

$$|C(0,p_i)\rangle = \frac{1}{\sqrt{2}}\left(|HALT\rangle + |GO\rangle\right) \tag{6}$$

for all $p_i \in A^*$. This corresponds to the fact that initially it is unknown whether or not the computer halts on p_i. When during the time evolution the computer has completed its task, the halting bit value is switched to $|HALT\rangle$ by some internal operation, otherwise it remains in the coherent 50:50-superposition of equation (6). [Alternatively, the computer could be initially prepared in the non-halting state $|GO\rangle$. After completion of the task, the halting bit is again switched to the halting state $|HALT\rangle$. In this case, the subtractions of $\langle GO|C(t,p_i)\rangle$ in equations (7), (8) and (9) below would have to be eliminated.]

In analogy to the fully classical case [1, 18, 3], the quantum halting amplitude Ω can be defined as a weighted expectation over all computations of C with classical input p_i ($|p_i|$ stands for the length of p_i)

$$\Omega \equiv \lim_{t\to\infty} \sum_{p_i} 2^{-|p_i|} \left[\langle HALT|C(t,p_i)\rangle - \langle GO|C(t,p_i)\rangle \right] \quad . \tag{7}$$

Likewise, for particular output states $|s\rangle$,

$$\Upsilon(|s\rangle) \equiv \lim_{t\to\infty} \sum_{|C(t,p_i)\rangle = |s\rangle} 2^{-|p_i|} \left[\langle HALT|C(t,p_i)\rangle - \langle GO|C(t,p_i)\rangle \right] \quad . \tag{8}$$

For a set of output states $S = \{|s_1\rangle, |s_2\rangle, |s_3\rangle, \ldots, |s_n\rangle\}$ which correspond to mutually orthogonal vectors in Hilbert space,

$$\Upsilon(S) \equiv \lim_{t\to\infty} \sum_{|C(t,p_i)\rangle \in S} 2^{-|p_i|} \left[\langle HALT|C(t,p_i)\rangle - \langle GO|C(t,p_i)\rangle \right] \quad . \tag{9}$$

For nontrivial choices of the quantum computer C, several remarks are in order. (In what follows, we mention only Ω, but the comments apply to Υ as well.)

First, note that if the program is also coded in qbits, the above sum becomes an integral over continuously many states per code symbol of the programs. In this case, the Kraft sum needs not converge.

Second, just as for the classical analogue it is possible to "compute" Ω as a limit from below by considering in the t'th computing step (time t) all programs of length t which have already halted. (This "computation" suffers from a radius of convergence which decreases slower than any recursive function.)

Third, the quantum Ω is complex. $|\Omega|^2$ can be interpreted as a measure for the halting probability of C; i.e., the probability that an arbitrary (prefix-free) program halts on C. Both, the relative phases of approximations of Ω, as well as approximations to $|\Omega|^2$ are measurable.

Finally, any measurements of $|\Omega|^2$ causes irreversible state collapses. Since $|C(t,p_i)\rangle$ may not be in a pure state, the series in (7) and (8) will not be uniquely defined even for *finite* times. The *nondeterministic* character of Ω is not only based on classical recursion theoretic arguments [1] but also on the physical proposition that God plays the quantum dice.

References

[1] G. J. Chaitin, *Information, Randomness and Incompleteness, Second edition* (World Scientific, Singapore, 1987, 1990); *Algorithmic Information Theory* (Cambridge University Press, Cambridge, 1987); *Information-Theoretic Incompleteness* (World Scientific, Singapore, 1992).

[2] R. M. Solovay, *unpublished manuscript.*

[3] C. Calude, *Information and Randomness — An Algorithmic Perspective* (Springer, Berlin, 1994).

[4] D. Z. Albert, *Phys. Lett.* **94A**, 249 (1983).

[5] P. Benioff, *J. Stat. Phys.* **29**, 515 (1982); *Phys. Rev. Lett.* **48**, 1581 (1982).

[6] D. Deutsch, *Proc. R. Soc. Lond.* **A 400**, 97 (1985).

[7] R. P. Feynman, *Opt. News* **11**, 11 (1985).

[8] A. Peres, *Phys. Rev.* **A32**, 3266 (1985).

[9] P. Benioff, *Annals New York Akademy of Sciences* **480**, 475 (1986).

[10] N. Margolus, *Annals New York Akademy of Sciences* **480**, 487 (1986).

[11] D. Deutsch, *Proc. R. Soc. Lond.* **A 425**, 73 (1989).

[12] D. Deutsch and R. Jozsa, *Proc. R. Soc. Lond.* **A 439**, 553 (1992).

[13] A. Zeilinger, *Am. J. Phys.* **49**, 882 (1981); M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani, *Phys. Rev. Lett.* **73**, 58 (1994).

[14] R. W. Hamming, *Coding and Information Theory, Second Edition* (Prentice-Hall, Englewood Cliffs, New Jersey, 1980).

[15] K. Svozil, *Randomness and Undecidability in Physics* (World Scientific, Singapore, 1993).

[16] K. Svozil, *On the computational power of physical systems, undecidability, the consistency of phenomena and the practical uses of paradoxa*, in *International Conference on Fundamental Problems in Quantum Theory*, ed. by D. Greenberger (New York Academy of Sciences, in print); *Quantum recursion theory*, TU Vienna preprint.

[17] Let $d(\cdot,\cdot)$ be the inner product of the Hilbert space. Let further be $\langle x|y\rangle := d(|x\rangle,|y\rangle)$. Orthonormality states that $\langle HALT|HALT\rangle = \langle GO|GO\rangle = 1$ and $\langle HALT|GO\rangle = \langle GO|HALT\rangle = 0$.

[18] R. J. Solomonoff, *Information and Control* **7**, 1 (1964); *IEEE Transactions on Information Theory* **IT-24**, 422 (1978).