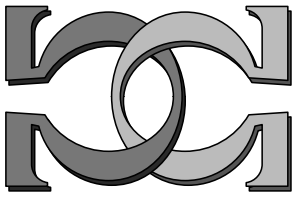
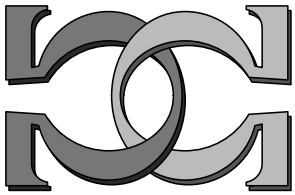
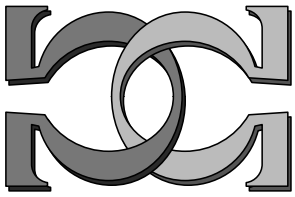
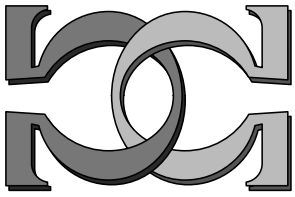


CDMTCS
Research
Report
Series

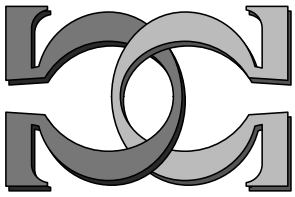




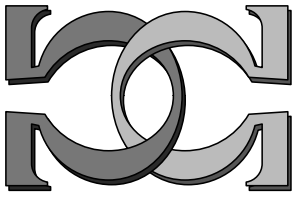
Coins, Quantum Measurements, and Turing's Barrier



C. S. Calude, B. Pavlov
University of Auckland, New Zealand



CDMTCS-170
November 2001/ Revised February 2002



Centre for Discrete Mathematics and
Theoretical Computer Science

If you can look into the seeds of time,

And say which grain will grow, and which will not,

Speak then to me.

W. Shakespeare, *Macbeth*, I, 3.

Coins, Quantum Measurements, and Turing's Barrier*

Cristian S. Calude† and Boris Pavlov‡

November 2001/ Revised February 2002

Abstract

Is there any hope for quantum computing to challenge the Turing barrier, i.e. to solve an undecidable problem, to compute an uncomputable function? According to Feynman's '82 argument, the answer is *negative*. This paper re-opens the case: we will discuss solutions to a few simple problems which suggest that *quantum computing is theoretically capable of computing uncomputable functions*.

Turing proved that there is no "halting (Turing) machine" capable of distinguishing between halting and non-halting programs (undecidability of the Halting Problem). Halting programs can be recognized by simply running them; the main difficulty is to detect non-halting programs. In this paper a mathematical quantum "device" (with sensitivity ε) is constructed to solve the Halting Problem. The "device" works on a randomly chosen test-vector for T units of time. If the "device" produces a click, then the program halts. If it does not produce a click, then either the program does not halt or the test-vector has been chosen from an *undistinguishable set of vectors* $\mathcal{F}_{\varepsilon,T}$. The last case is not dangerous as our main result proves: *the Wiener measure of* $\mathcal{F}_{\varepsilon,T}$ *constructively tends to zero when* T *tends to infinity*. The "device", working in time T, appropriately computed, will

*A preliminary version of this paper has appeared in [9].

†Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand. E-mail: cristian@cs.auckland.ac.nz.

‡Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand. E-mail: pavlov@math.auckland.ac.nz.

determine with a pre-established precision whether an arbitrary program halts or not. *Building the "halting machine" is mathematically possible.*

To construct our "device" we use the quadratic form of an iterated map (encoding the whole data in an infinite superposition) acting on randomly chosen vectors viewed as special trajectories of two Markov processes working in two different scales of time. The evolution is described by an unbounded, exponentially growing semigroup; finally a single measurement produces the result.

1 Introduction

For over fifty years the Turing machine model of computation has defined what it means to "compute" something; the foundations of the modern theory of computing are based on it. Computers are reading text, recognizing speech, and robots are driving themselves across Mars. Yet this exponential race will not produce solutions to many intractable and undecidable problems. Is there any alternative? Indeed, quantum computing offers one such alternative (see [11, 7, 23, 35, 10]). To date, quantum computing has been very successful in "beating" Turing machines in the race of solving intractable problems, with Shor and Grover algorithms achieving the most impressive successes; the progress in quantum hardware is also impressive. Is there any hope for quantum computing to challenge the Turing barrier, i.e. to solve an undecidable problem, to compute an uncomputable function? According to Feynman's argument (see [20], a paper reproduced also in [25], regarding the possibility of simulating a quantum system on a (probabilistic) Turing machine[1]) the answer is *negative*.

This paper re-opens the case:[2] We will discuss solutions to a few simple problems which suggest that *quantum computing is theoretically capable of computing uncomputable functions*. The main features of our quantum "device" are: *a special type of continuity, the choice of test-vectors from a special class of trajectories of two Markov processes working in two different scales of time and realized as elements of an infinitely-dimensional Hilbert space (infinite superposition), the ability to work with "truly random" test-vectors in an evolution described by an exponentially growing semigroup and the possibility to obtain the result from a single measurement.*

In deciding the halting/non-halting status of a non-halting machine, our "device" is capable to 'announce' (with a positive probability) the non-halting status in a finite amount of time, well before the 'real' machine reaches it (in an infinite amount of time). Hence, the challenge was to design a procedure that detects and measures this tiny, but non-zero probability.

In what follows a *quantum* solution is a solution designed to work on a quantum computer. The discussion is *mathematical* and no engineering claims will be made; in particular, when speaking about various quantum devices which will be constructed, we will use quotes to emphasize the mathematical nature of our constructs.

[1] Working with probabilistic Turing machines instead of Turing machines makes no difference in terms of computational capability: see [17].

[2] See [8, 10, 16, 27] for related ideas and results.

2 The Merchant's Problem

One possible way to state the famous Merchant's Problem is as follows:

> *A merchant learns than one of his five stacks of* $\Gamma = 1$ *gram coins contains only false coins,* $\gamma = 0.001$ *grams heavier than normal ones. Can he find the odd stack by a single "weighting"?*

The well-known solution of this problem is the following: We take one coin from the first stack, two coins from the second stack, ..., five coins from the last stack.

Then by measuring the weight of the combination of coins described above we obtain the number $Q = 15 + \gamma \times n$ grams ($1 \leq n \leq 5$), which tells us that the n-th stack contains false coins.

The above solution is, in spirit, "quantum". It consists of the following steps: a) *preparation*, in which a single object encoding the answer of the problem is created in a special format, b) *measurement*, in which a measurement is performed on the object, c) *classical calculation*, in which the measurement data is processed and the desired final result is obtained.

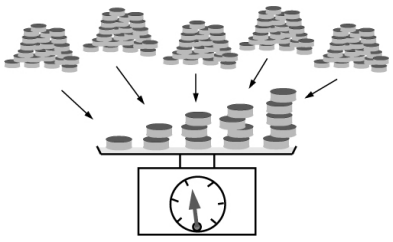


Figure 1. Coin selection

In our case, the selection of coins from various stacks as presented in Figure 1 is the object a) prepared for measurement b); finally, the calculation $n = (Q - 15) \times 1000$ gives the number of the stack containing false coins.

3 The Merchant's Problem: Two Finite Variants

Consider now the case when we have five stacks of coins, but a few (maybe none) may contain false coins. This means, all five stacks contain true coins, or only one stack contains false coins, or two stacks contain false coins, etc. Can we, again with only one single "weighting", find all stacks containing false coins? A possible solution is to choose 1, 2, 4, 8, 16 coins from each stack, and use the uniqueness of base two representation.

The difference between the above solutions is only in the specific way we chose the sample, i.e. in *coding*. Further on, note that the above solutions work *only* if we have *enough coins in each stack*. For example, if each of the five stacks contains only four coins, then neither of the above solutions works. In such a case is it still possible to have a solution operating with just one measurement?

In the simplest case we have N stacks of coins and we know that *at most one stack may contain false coins*. We are allowed to take just one coin from each stack and we want to see whether all coins are true or there is a stack of false coins (and which). Can we solve this problem with just one "weighting"?

Assume that a true coin has $\Gamma = 1$ grams and a false coin has $\Gamma+\gamma$ grams ($0 < \gamma < 1$). Consider as quantum space the space $H_N = \mathbf{R}^N$, a real Hilbert space of dimension N. The elements of $\mathbf{R}^N$ are vectors $\mathbf{x} = (x_1, x_2, \ldots, x_N)$. The scalar product of $\mathbf{x}$ and $\mathbf{y}$ is defined by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{N} x_i y_i$. The norm of the vector $\mathbf{x}$ is defined by $\| \mathbf{x} \| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$. Let $0 < n < N$, and consider $\Omega^n \subset \mathbf{R}^n$. A set $X \subset \mathbf{R}^N$ is called *cylindrical* if $X = \Omega^n \times \mathbf{R}^{N-n}$. Let us denote by μ^k the Lebesgue measure in $\mathbf{R}^k$. If $\Omega^n \subset \mathbf{R}^n$ is measurable, then the cylinder $X = \Omega^n \times \mathbf{R}^{N-n}$ is measurable and $\mu^N(X) = \mu^n(\Omega^n)$. For more on Hilbert spaces see [1, 24]; for specific relations with quantum physics see [12].

Next we consider the standard basis $(e_i)_{i=1,N}$ and the projections $\mathbf{P}_i : \mathbf{R}^N \to \mathbf{R}^N$, $\mathbf{P}_i(\mathbf{x}) = (0, 0, \ldots, x_i, 0, \ldots, 0)$. Denote by q_i the weight of a coin in the i-th stack; if the i-th stack contains true coins, then $q_i = \Gamma = 1$, otherwise, $q_i = \Gamma + \gamma = 1 + \gamma$.

Consider the operator $\mathbf{Q} = \sum_{i=1}^{N} q_i \mathbf{P}_i$.[3] For every vector $\mathbf{x} \in \mathbf{R}^N$,

$$\mathbf{Q}(\mathbf{x}) = (q_1 \mathbf{P}_1, \ldots, q_N \mathbf{P}_N)(\mathbf{x}) = (q_1 x_1, \ldots, q_N x_N).$$

The t-th ($t > 1$) iteration of the operator $\mathbf{Q}$ can be used to distinguish the case in which all coins are true from the case in which one stack contains false coins: we construct the quadratic form $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle$ and consider its dynamics.[4] In case all coins are true $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle = \| \mathbf{x} \|^2$, for all $\mathbf{x} \in \mathbf{R}^N$; if there are false coins in some stack, for some $\mathbf{x} \in \mathbf{R}^N$, $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle > \| \mathbf{x} \|^2$, and the value increases with every new iteration.

Now we can introduce a "weighted Lebesgue measure" with proper non-negative continuous density ρ. For example, this can be achieved with the density equal to the Gaussian distribution

$$\rho(\mathbf{x}) = \frac{1}{\pi^{N/2}} \; e^{-\sum_{s=1}^{N} |x_s|^2},$$

a function which will be used in what follows.

We can interpret the measure generated by the density as the probability distribution corresponding to the standard $Normal\,(N; 0, \frac{1}{2}\mathbf{I})$. Hence the probability of the event $\{\mathbf{x} \mid x_1 \in \Omega\}$ is the integral $\mathrm{Prob}(\Omega) = \int_{\Omega \times \mathbf{R}^{N-1}} \rho dm$. Then, because of the continuity of

[3] As suggested by [26], different operators can be considered, e.g. $\mathbf{Q}(x) = \sum_i^N 2^{(q_i - \Gamma)} \mathbf{P}_i$.

[4] To speed-up the computation one can accelerate the iterations of $\mathbf{Q}$, for example by considering the quadratic form $\langle \mathbf{Q}^{2^t}(\mathbf{x}), \mathbf{x} \rangle$ instead of $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle$.

the density, we deduce that the probability of any "low-dimensional event" is equal to zero. In particular, the event $\{\mathbf{x} \mid x_s = 0\}$ has probability zero, that is, with probability one all components of a randomly chosen normalized vector $\mathbf{x}$ are non-zero.

We are now ready to consider our problem. We will assume that time is discrete, $t = 1, 2, \ldots$. The procedure will be *probabilistic:* it will indicate a method to decide, with a probability as close to one as we want, whether there exist any false coins.

Fix a computable real $\eta \in (0, 1)$ as probability threshold. Assume that both η and γ are computable reals. Choose a "test" vector $\mathbf{x} \in \mathbf{R}^N$. Assume that we have a quantum "device"[5] which measures the quadratic form and clicks at time T on $\mathbf{x}$ when

$$\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle > (1 + \varepsilon) \parallel \mathbf{x} \parallel^2 . \tag{1}$$

In this case we say that the quantum "device" has sensitivity ε. In what follows we will assume that $\varepsilon > 0$ is a positive computable real.

Two cases may appear. If for some $T > 0$, $\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle > (1 + \varepsilon) \parallel \mathbf{x} \parallel^2$, then the "device" has clicked and we know for *sure* that there exist false coins in the system. However, it is possible that at some time $T > 0$ the "device" hasn't (yet?) clicked because $\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle \leq (1 + \varepsilon) \parallel \mathbf{x} \parallel^2$. This may happen because either all coins are true, i.e., $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle = \parallel \mathbf{x} \parallel^2$, for all $t > 0$, or because at time T the growth of $\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle$ hasn't yet reached the threshold $(1 + \varepsilon) \parallel \mathbf{x} \parallel^2$. In the first case the "device" will *never* click, so at each stage t the test-vector $\mathbf{x}$ produces "true" information; we can call $\mathbf{x}$ a "true" vector. In the second case, the test-vector $\mathbf{x}$ is "lying" at time T as we *do* have false coins in the system, but they were not detected at time T; we say that $\mathbf{x}$ produces "false" information at time T.

Hence, the "true" vector has non-zero coordinates corresponding to stacks of false coins (if any); a vector "lying" at time T may have zero or small coordinates corresponding to stacks of false coins. For instance, the null vector produces "false" information at any time. If the system has false coins and they are located in the j-th stack, then each test vector $\mathbf{x}$ whose j-th coordinate is 0 produces "false" information at any time. If the system has false coins and they are located in the j-th stack, $x_j \neq 0$, but

$$\parallel \mathbf{x} \parallel^2 + ((1 + \gamma)^T - 1)|x_j|^2 \leq (1 + \varepsilon) \parallel \mathbf{x} \parallel^2,$$

then $\mathbf{x}$ produces "false" information at time T. If $|x_j| \neq 0$, then $\mathbf{x}$ produces "false" information only a finite period of time, that is, only for

$$T \leq \log_{1+\gamma} \left(1 + \frac{\varepsilon \parallel \mathbf{x} \parallel^2}{|x_j|^2} \right);$$

after this time the quantum "device" starts clicking.

The major problem is to distinguish between the presence/absence of false coins in the system. We will show how to compute the time T such that when presented a

[5]The construction of such a "device" is a difficult problem in nanoelectronics; see, for example, [13, 29, 30].

randomly chosen test-vector[6] $\mathbf{x} \in \mathbf{R}^N \setminus \{\mathbf{0}\}$ to a quantum "device" with sensitivity ε that fails to click in time T, then the system doesn't contain false coins with probability larger than $1 - \eta$.

Assume first that the system contains false coins in some stack j. Then

$$\lim_{t\to\infty} \frac{\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle}{\| \mathbf{x} \|^2} = \infty, \tag{2}$$

for all $\mathbf{x} \in \mathbf{R}^N$ such that $|x_i| \neq 0$, for all $1 \leq i \leq N$. Indeed, in view of the hypothesis, there exists $j \in \{1, 2, \ldots, N\}$ such that the weight of any coin in the j-th stack, q_j, is $\Gamma + \gamma = 1 + \gamma$. So, for every $t \geq 1$,

$$\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle = \sum_{i=1}^{N} q_i^t \| \mathbf{x} \|^2 \ = \| \mathbf{x} \|^2 + ((1+\gamma)^t - 1)|x_j|^2.$$

If $|x_j| \neq 0$, for all $j \in \{1, 2, \ldots, N\}$, then

$$\lim_{t\to\infty} \frac{\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle}{\| \mathbf{x} \|^2} = \lim_{t\to\infty} 1 + \frac{((1+\gamma)^t - 1)|x_j|^2}{\| \mathbf{x} \|^2} = \infty.$$

If the system contains only true coins, then for every $\mathbf{x} \in \mathbf{R}^N \setminus \{\mathbf{0}\}$,

$$\lim_{t\to\infty} \frac{\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle}{\| \mathbf{x} \|^2} = 1.$$

Consider now the *indistinguishable set at time t*

$$\mathcal{F}_{\varepsilon,t} = \{\mathbf{x} \in \mathbf{R}^N \mid \langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle \leq (1+\varepsilon) \| \mathbf{x} \|^2\}.$$

If the system contains only true coins, then $\mathcal{F}_{\varepsilon,t} = \mathbf{R}^N$, for all $\varepsilon > 0, t \geq 1$. If there is one stack (say, the j-th one) containing false coins, then $\mathcal{F}_{\varepsilon,t}$ is a cone $\mathcal{F}_{\varepsilon,t,j}$ centered at the "false" plane $x_j = 0$:

$$((1+\gamma)^t - 1)\, |x_j|^2 \ \leq \ \varepsilon \| \ x \ \|^2 \, .$$

Next we compute Prob($\mathcal{F}_{\varepsilon,t}$) in case the *system contains false coins*. Each set $\mathcal{F}_{\varepsilon,t} = \mathcal{F}_{\varepsilon,t,j}$ can be decomposed into two disjoint sets as follows (here $M > 0$ is a large enough real which will be determined later):

$$\mathcal{F}_{\varepsilon,t,j} = \{\mathbf{x} \in \mathcal{F}_{\varepsilon,t,j} \mid M \geq \| \mathbf{x} \|\} \cup \{\mathbf{x} \in \mathcal{F}_{\varepsilon,t,j} \mid M < \| \mathbf{x} \|\}.$$

[6] A different approach would be to consider the (constant) test vector $\mathbf{x} = (\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \ldots, \frac{1}{\sqrt{N}})$ playing the role of an equal "superposition" of all stacks.

In view of the inclusion

$$\{\mathbf{x} \in \mathcal{F}_{\varepsilon,t,j} \mid M \geq \| \mathbf{x} \|\} \subset \{\mathbf{x} \in \mathbf{R}^N \mid ((1+\gamma)^t - 1)\,|x_j|^2 \leq \varepsilon M^2\},$$

we deduce that

$$\begin{aligned} \mathrm{Prob}(\{\mathbf{x} \in \mathcal{F}_{\varepsilon,t,j} \mid M \geq \| \mathbf{x} \|\}) &\leq \frac{1}{\sqrt{\pi}} \int_{-\frac{M\sqrt{\varepsilon}}{\sqrt{(1+\gamma)^t-1}}}^{\frac{M\sqrt{\varepsilon}}{\sqrt{(1+\gamma)^t-1}}} e^{-y^2} dy \\ &\leq \frac{2M\sqrt{\varepsilon}}{\sqrt{\pi}\sqrt{(1+\gamma)^t - 1}}, \end{aligned} \tag{3}$$

To estimate $\mathrm{Prob}(\{\mathbf{x} \in \mathcal{F}_{\varepsilon,t} \mid M < \| \mathbf{x} \|\})$ we note that the set

$$C_M = \bigcup_{i=1}^{N} \{\mathbf{x} \in \mathbf{R}^N \mid |x_i| > \frac{M}{\sqrt{N}}\},$$

contains the set $\{\mathbf{x} \in \mathcal{F}_{\varepsilon,t} \mid M < \| \mathbf{x} \|\}$, hence from the estimation

$$\mathrm{Prob}(C_M) \leq \frac{2N}{\sqrt{\pi}} \int_{\frac{M}{\sqrt{N}}}^{\infty} e^{-y^2} dy,$$

we deduce (using the inequality $\int_a^\infty e^{-y^2} dy \leq \frac{1}{2a}\, e^{-a^2}$ for $a > 0$) that

$$\mathrm{Prob}(\{\mathbf{x} \in \mathbf{R}^N \mid M < \| \mathbf{x} \|, |x_j| \leq \frac{M}{\sqrt{N}}\}) \leq \frac{N\sqrt{N}}{M\sqrt{\pi}}\, e^{-\frac{M^2}{N}}. \tag{4}$$

From (3) and (4) we obtain the inequality:

$$\mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) = \mathrm{Prob}(\mathcal{F}_{\varepsilon,t,j}) \leq \frac{2M\sqrt{\varepsilon}}{\sqrt{\pi}\sqrt{(1+\gamma)^t - 1}} + \frac{N\sqrt{N}}{M\sqrt{\pi}}\, e^{-\frac{M^2}{N}}. \tag{5}$$

Selecting

$$M = N^{3/4} \cdot \left(\frac{(1+\gamma)^t - 1}{\varepsilon}\right)^{1/4},$$

in (5) we get[7]

$$\mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) \leq \frac{3N^{3/4}\varepsilon^{1/4}}{\sqrt{\pi}((1+\gamma)^t - 1)^{1/4}} \tag{6}$$

[7]Lemma 4 in [22], p. 325-326, can be used to obtain a similar, but less tight estimation; cf. [28].

hence,

$$\lim_{t\to\infty} \mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) = 0.$$

The above limit is *constructive*, that is, from (6) and every computable $\eta \in (0,1)$ we can construct the computable bound

$$T_\eta = \log_{1+\gamma}\left(\frac{3^4 N^3 \varepsilon}{\eta^4 \pi^2} + 1\right) \tag{7}$$

such that *assuming that the system contains false coins, if* $t \geq T_\eta$, *then we get*

$$\mathrm{Prob}(\mathcal{F}_{\varepsilon,t}) \leq \eta.$$

Recall that we have a finite system of N stacks in which at most one stack contains false coins. So, if we assume that there are $N+1$ equiprobable possibilities, then either all coins are true or only the first stack contains false coins, or only the second stack contains false coins, or only the Nth stack contains false coins.[8] Let us now denote by $\mathcal{N}$ the event "the system contains no false coins" and by $\mathcal{Y}$ the event "the system contains false coins". By $P(\mathcal{N})$ $(P(\mathcal{Y}))$ we denote the *a priori* probability that the system contains no false coins (the system contains false coins). In the simplest case $P(\mathcal{Y}) = \frac{N}{N+1}, P(\mathcal{N}) = 1 - P(\mathcal{Y}) = \frac{1}{N+1}$. We can use Bayes' formula to obtain the *a posteriori probability that the system contains only true coins when at time* t *the quantum "device" didn't click*:

$$P_{\text{non-click}}(\mathcal{N}) = \frac{P(\mathcal{N})}{P(\mathcal{N}) + (1 - P(\mathcal{N}))\mathrm{Prob}(\mathcal{F}_{\varepsilon,t})} \geq 1 - N \cdot \mathrm{Prob}(\mathcal{F}_{\varepsilon,t}).$$

When $t \to \infty$, $\mathrm{Prob}(\Omega_{\varepsilon,t})$ goes to 0, so $P_{\text{non-click}}(\mathcal{N})$ goes to 1. More precisely, if $t \geq T_\eta$, as in (7), then

$$P_{\text{non-click}}(\mathcal{N}) \geq 1 - \eta N.$$

In conclusion,

> *for every computable* $\eta \in (0,1)$ *we can construct a computable time* T_η *such that picking up at random a test-vector* $\mathbf{x} \in \mathbf{R}^N \setminus \{\mathbf{0}\}$ *and using a quantum "device" with sensitivity* ε *up to time* T_η *either*
>
> - ◇ *we get a click at some time* $t \leq T_\eta$, *so the system contains false coins; the* j*th stack, where* j *is the unique coordinate such that* $(Q^T(\mathbf{x})/((1+\gamma)^T - 1))_j > x_j$, *contains false coins;*
> - ◇ *we don't get a click in time* T_η, *so with probability greater than* $1 - \eta N$ *all coins are true.*

[8] Of course, other distributions can be considered.

4 The Merchant's Problem: The Infinite Variant

Let us assume that we have now a countable number of stacks, all of them, except at most one, containing true coins only. Can we determine whether there is a stack containing false coins? It is not difficult to recognize that the infinite variant of the Merchant's Problem is equivalent to the Halting Problem: Decide whether an arbitrary program (Turing machine, probabilistic Turing machine, Java program, etc.) eventually halts. This problem is undecidable, i.e., no Turing machine can solve it.[9]

One of the most important quests of science is to determine those (natural) processes whose final state may be determined directly, without a need to exhaustively carry out each step of their evolutions. Usually, this is done by a "model" that "simulates" the process. The essence of the undecidability of the Halting Problem is the following: If our models are only Turing machines, then the outcome of the computation performed by a Turing machine can, in general, be determined *only* by explicitly carrying out each step of it. No short-cut is possible. Can we do it better if we enlarge the class of models? We shall prove that this is indeed the case.

4.1 A Tentative Solution

The first idea would be to follow the solution discussed in Section 3, but to select the random test vector $\mathbf{x} = (x_0, x_1, x_3, \ldots)$ from the Hilbert space $H = l_2$ of quadratically summable sequences of probabilistically independent variables x_i, equipped with the Gaussian distribution on all cylindrical sets with finite-dimensional sections parallel to coordinate planes.

We define

$$\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle = \sum_{i=1}^{\infty} q_i^T |x_i|^2.$$

The analogue of the *indistinguishable set* in l_2 is

$$\begin{aligned} \mathcal{F}_{\varepsilon,T} &= \{\mathbf{x} \in l_2 \mid \langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle \leq (1+\varepsilon)\langle \mathbf{x}, \mathbf{x} \rangle\} \\ &= \{\mathbf{x} \in l_2 \ \langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x} \rangle \leq \langle \mathbf{x}, \mathbf{x} \rangle + \langle \varepsilon \mathbf{I}(\mathbf{x}), \mathbf{x} \rangle\}. \end{aligned} \tag{8}$$

so, the measuring "device" is the operator εI. If for a given test-vector $\mathbf{x}$ we have $\langle Q^T(\mathbf{x}), \mathbf{x} \rangle \geq (1+\varepsilon) \parallel \mathbf{x} \parallel^2$ ($\| \cdot \|$ is the l_2–norm), then the "device" clicks, which means that there is a false coin in some stack j (represented by a non-zero component x_j of the test-vector $\mathbf{x}$). If the "device" does not click, then the result of the experiment is not conclusive: either we do not have false coins in the system, or, we have, but the test vector "lies" since it belongs to the set $\mathcal{F}_{\varepsilon,T}$ of indistinguishable elements.

Assume that the system contains false coins in some stack j. For large T such that $(1+\gamma)^T > 1+\varepsilon$, the coordinate description of the set $\mathcal{F}_{\varepsilon,T}$ can be given in the form of a cone centered at the "false plane" $x_j = 0$ in H:

[9] Arguably, the most famous undecidable problem. See, for example, [6].

$$\mathcal{F}_{\varepsilon,T} = \left\{ \mathbf{x} \mid |x_j|^2 \leq \frac{\varepsilon}{(1+\gamma)^T - 1} \ \| \mathbf{x} \|^2 \right\}.$$

Consider now the intersection of the indistinguishable set $\mathcal{F}_{\varepsilon,T}$ with the finite-dimensional subspace $H_{2n} = \{\mathbf{x} \mid x_i = 0, i > 2n\}$, $\mathcal{F}_{\varepsilon,T,2n} = \mathcal{F}_{\varepsilon,T} \cap H_{2n}$. It is clear that $\mathcal{F}_{\varepsilon,T,2n} \subset \mathcal{F}_{\varepsilon,T,2n+1}$. Let $\varepsilon \cdot ((1+\gamma)^T - 1)^{-1}$ be denoted by α^2. Assume for a moment that the Gaussian distribution may be extended by Lebesgue procedure to a probability measure Prob. Then, we can calculate the measure of the finite-dimensional section $\mathcal{F}_{\varepsilon,T,N}$ of the indistinguishable set $\mathcal{F}_{\varepsilon,T}$ (if $N = 2n$):

$$\mathrm{Prob}(\mathcal{F}_{\varepsilon,T,N}) = \frac{\int_0^{\alpha\sqrt{n}} \frac{dv}{(1+v^2/n)^n}}{\int_0^{\infty} \frac{dv}{(1+v^2/n)^n}}.$$

In view of the Lebesgue dominant convergence theorem ($\int_0^A dv/(1+v^2/n)^n \to \int_0^A e^{-v^2} dv$) the limit of $\mathrm{Prob}(\mathcal{F}_{\varepsilon,T,N})$ can be estimated as follows: when $n \to \infty$, $\mathrm{Prob}(\mathcal{F}_{\varepsilon,T,2n}) \to \frac{\int_0^{\alpha\sqrt{n}} e^{-v^2} dv}{\int_0^{\infty} e^{-v^2} dv}$ uniformly in α, $0 < \alpha < \infty$, and

$$\frac{\int_0^{\alpha\sqrt{n}} e^{-v^2} dv}{\int_0^{\infty} e^{-v^2} dv} = \frac{2}{\sqrt{\pi}} \int_0^{\alpha\sqrt{n}} e^{-v^2} dv. \tag{9}$$

If the duration of the experiment is fixed (T is constant), but n tends to infinity, then the measure $\mathrm{Prob}(\mathcal{F}_{\varepsilon,T,2n})$ of the finite-dimensional indistinguishable set $\mathcal{F}_{\varepsilon,T,2n}$ tends to 1. Hence, in view of the assumption on Prob, monotonicity and the inclusion $\mathcal{F}_{\varepsilon,T,2n} \subset \mathcal{F}_{\varepsilon,T}$ we conclude that $\mathrm{Prob}(\mathcal{F}_{\varepsilon,T}) = 1$, for all T, hence $\lim_{T\to\infty} \mathrm{Prob}(\mathcal{F}_{\varepsilon,T}) = 1$.

On the other hand, $\mathcal{F}_{\varepsilon,T'} \subset \mathcal{F}_{\varepsilon,T}$, if $T' > T$ and $\bigcap_{T>0} \mathcal{F}_{\varepsilon,T} = \lim_{T\to\infty} \mathcal{F}_{\varepsilon,T} = \{\mathbf{x} \mid x_j = 0\}$ is a cylindrical set with measure 0. This implies that our assumption about the possibility to construct the Lebesgue extension of the Gaussian distribution was wrong. This is the mathematical reason why our "device" will work only 'locally', on the observed finite part of the system, not 'globally', on the whole infinite system.

Assume that we are dealing with a class of systems where the *a priori* probability of absence of false coins is $P(\mathcal{N})$. We select at random one of these systems and perform experiments using our "device". Then, due to Bayes' formula, the *a posteriori* probability of absence of false coins in the system *subject to the assumption that the "device" did not click in time* T is

$$P_{\text{non-click}}(\mathcal{N}) = \frac{P(\mathcal{N})}{P(\mathcal{N}) + (1 - P(\mathcal{N}))\mathrm{Prob}(\mathcal{F}_{\varepsilon,T})},$$

so if $\mathrm{Prob}(\mathcal{F}_{\varepsilon,T}) = 1$, then

$$P_{\text{non-click}}(\mathcal{N}) = P(\mathcal{N}),$$

hence the "non-click" result is not conclusive. Still, formula (9) suggests a procedure for estimating the *a posteriori* probability of presence of false coins in the *observed* finite part of the system.

Assume that we have observed the first $2n$ elements of the system. Further, suppose that the duration of the experiment T and the above number n satisfy the following condition:

$$\alpha\sqrt{n} = \sqrt{\frac{\varepsilon n}{(1+\gamma)^T - 1}} \longrightarrow 0, \tag{10}$$

when $n \to \infty$. Let $\Gamma(n) = \alpha\sqrt{n}$. Then, according to (9) we have:

$$\lim_{n\to\infty} \mathrm{Prob}(\mathcal{F}_{\varepsilon,T,2n}) = \lim_{n\to\infty} \frac{1}{\sqrt{\pi}} \int_0^{\Gamma(n)} e^{-x^2} dx = 0.$$

Hence, using again Bayes's formula, if $T \to \infty$ and T, n satisfy (10), then

$$P_{\text{non-click}}(\mathcal{N}) = \frac{P(\mathcal{N})}{P(\mathcal{N}) + (1 - P(\mathcal{N}))\frac{1}{\sqrt{\pi}} \int_0^{\Gamma(n)} e^{-x^2} dx} \longrightarrow 1,$$

when $n \to \infty$.

Because of the revealed "discontinuity" of the Gaussian distribution in l_2,[10] the probability of the high-dimensional sections of the indistinguishable set (8) is not uniformly small in n, for large T. This is in agreement with the view that "only a finite number of subjects may be observed in finite time".[11] In fact, the problem is related to the mathematical notion of finiteness, which appears to be "inadequate to the task of telling us which physical processes are finite and which are infinite" (see [18]).

4.2 A Brownian Solution

The failure of the tentative approach was caused by the structure of the stochastic space of test-vectors. A more elaborated approach, developed in this section, will permit the estimation of the probability of absence of false coins in the whole *infinite* sequence by observing the behaviour of the quadratic form of the iterated map

$$\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x} \rangle = \sum_{i=1}^{\infty} q_i^t \, |x_i|^2$$

[10] Lack of countable additivity of its extension.

[11] According to Theorem 2 in [22], p. 345, the Lebesgue extension of the Gaussian measure in a countably Hilbert space exists if and only if the distribution function is equal to $e^{-\langle Ax,x\rangle}$, where A is a Hilbert-Schmidt operator. If the condition is not satisfied, then the Lebesgue extension of the Gaussian measure still exists, but in a larger Hilbert space, in which the initial Hilbert space has measure zero.

on randomly chosen test-vectors $\mathbf{x}$ viewed *as special trajectories* of a Markov process.[12]

To this aim we drop the assumption of probabilistic independence and consider a "device" detecting the false coins which is based on *continuous* probability measures induced by Markov processes, see [4]. We construct two Markov processes working in *two different discrete time scales*. To capture the idea of "continuity" referred to in Sections 1 and 4.1 the construction makes use of the Green function of the Cauchy problem for the heat equation

$$\frac{\partial G}{\partial t} = \frac{1}{4}\frac{\partial^2 G}{\partial x^2}, \quad G(x, y, 0) = \delta(x - y), \tag{11}$$

which may be interpreted (see, for example, [21]) as a probability–density of the space–distribution of a Brownian particle on the real axis which begins diffusion from the initial position y at the initial moment $t = 0$:

$$G(x, t|y, 0) = \frac{1}{\sqrt{\pi t}} e^{-\frac{|x-y|^2}{t}}. \tag{12}$$

The Green function is a positive analytic function of each variable in the half-plane $0 < t < \infty,\ -\infty < x < \infty$. It provides information on the distribution of the Brownian particle on the whole infinite axis *for any positive time* $t > 0$, which corresponds to diffusion with *infinite speed*.

We are going to use three spaces. The first is the stochastic space of all trajectories $\mathbf{x}$ of Brownian particles equipped with the Wiener measure W (see [32]). The measure W is defined on the algebra of all finite-dimensional cylindrical sets $C^{t_1,t_2,\ldots,t_N}_{\Delta_1,\Delta_2,\ldots,\Delta_N}$ of trajectories with fixed initial point $x_0 = 0$ and "gates" Δ_l, $l = 1, \ldots, N$ (which are open intervals on the real line):

$$C^{t_1,t_2,\ldots,t_N}_{\Delta_1,\Delta_2,\ldots,\Delta_N} = \{\mathbf{x} \mid x_{t_l} \in \Delta_l, l = 1, 2, \ldots, N\},$$

via multiple convolutions of the Green functions $G(x_{l+1}, t_{l+1}|x_l, t_l)$ corresponding to the steps $\delta_{l+1} = t_{l+1} - t_l$:

$$W^N(C^{t_1,t_2,\ldots,t_N}_{\Delta_1,\Delta_2,\ldots,\Delta_N}) = \frac{\int\ldots\int_{\Delta_N,\Delta_{N-1},\ldots,\Delta_1} \frac{dx_1 dx_2 \ldots dx_N}{\pi^{\frac{N}{2}}\sqrt{\delta_N \delta_{N-1}\cdots\delta_1}}\, e^{-\frac{|x_N - x_{N-1}|^2}{\delta_N}} \ldots e^{-\frac{|x_1 - x_0|^2}{\delta_1}}}{\int\ldots\int_{\mathbf{R}_N,\mathbf{R}_{N-1},\ldots,\mathbf{R}_1} \frac{dx_1 dx_2 \ldots dx_N}{\pi^{\frac{N}{2}}\sqrt{\delta_N \delta_{N-1}\cdots\delta_1}}\, e^{-\frac{|x_N - x_{N-1}|^2}{\delta_N}} \ldots e^{-\frac{|x_1 - x_0|^2}{\delta_1}}}, \tag{13}$$

where $\mathbf{R}_N = \mathbf{R}_{N-1} = \ldots = \mathbf{R}_1 = \mathbf{R}$. Using the convolution formula, the denominator of (13) can be reduced to the Green function $G(x_N, t_N \mid 0, 0)$, for any $\tau \in (s, t)$:

[12] As in the finite case, various other choices of operators can be considered in order to speed-up the computation.

$$G(x,t \mid y,s) = \int_{-\infty}^{\infty} G(x,t \mid \xi,\tau) G(\xi,\tau \mid y,s) d\xi.$$

Our "device" (with sensitivity ε) will distinguish the values of the iterated quadratic forms by observing the difference between the non-perturbed and perturbed sequences t_l, $\tilde{t}_l$. Instead of the Hilbert space l_2 we will work with its intersections with the discrete Sobolev class l_2^1 of summable sequences with the square norm

$$\mid \mathbf{x} \mid_1^2 \; = \sum_{m=1}^{\infty} |x_m - x_{m-1}|^2,$$

and the discrete Sobolev class $\tilde{l}_2^1$ of weighted-summable sequences with the square norm

$$\parallel \mathbf{x} \parallel_1^2 \; = \sum_{m=1}^{\infty} \frac{1-\tilde{\delta}_m}{\tilde{\delta}_m} \; |x_m - x_{m-1}|^2.$$

We consider two discrete stochastic processes corresponding to the *equidistant sequence* of moments of time $t_l = l,\ l = 0,1,\ldots,\ \delta_s = 1$ and to the *perturbed sequence* of moments of time $\tilde{t}_l = \sum_{m=0}^{l} \tilde{\delta}_m,\ \tilde{\delta}_m < 1$. We assume that $\tilde{t}_l$ are computable and for large values of m, $\sum_m (1-\tilde{\delta}_m) < \infty$, that is

$$\tilde{t}_N = N - \sum_{m=1}^{N} (1-\tilde{\delta}_m) = N \left(1 - \frac{\sum_{m=1}^{N} (1-\tilde{\delta}_m)}{N} \right) \approx N,$$

for large N. By natural extension from cylindrical sets we can define the Wiener measures $\tilde{W}$ and W on these spaces. In what follows we are going to use the following relation between $\tilde{W}$ and W (see [32]): for every W–measurable set Ω,

$$\tilde{W}(\Omega) = \frac{1}{\prod_{l=1}^{\infty} \sqrt{\delta_l}} \int_{\Omega} e^{-\sum_{m=1}^{\infty} \frac{1-\tilde{\delta}_m}{\tilde{\delta}_m} |x_m - x_{m-1}|^2} dW. \tag{14}$$

Further we consider the class of *quasi-loops*, that is the class of all trajectories of the perturbed process which begins from $(x_0, t_0) = (0,0)$ and there exists a constant C such that $\max_{0<s<t} |x_s|^2 < Ct$. We note that

- *every* $\mathbf{x} \in l_2^1$ *is a quasi-loop (with* $C = \mid \mathbf{x} \mid_1^2$*),*
- *due to the reflection principle* (see [32], p. 221)*, the class of all quasi-loops has Wiener measure one.*

We assume that our "device" cannot identify the false coin at time T in case the test vector $\mathbf{x}$ belongs to the *indistinguishable set*

$$\begin{aligned}\mathcal{F}_{\varepsilon,T} &= \{\mathbf{x}\in l_2\cap l_2^1 \mid \langle \mathbf{Q}^t(\mathbf{x}),\mathbf{x}\rangle < \| \mathbf{x}\|^2 \\ &\quad + \varepsilon\left(\sum_{m=1}^{\infty}\frac{1-\tilde{\delta}_m}{\tilde{\delta}_m}|x_m - x_{m-1}|^2\right)\} \\ &= \{\mathbf{x}\in l_2\cap l_2^1 \mid \langle \mathbf{Q}^t(\mathbf{x}),\mathbf{x}\rangle < \| \mathbf{x}\|^2 + \varepsilon \| \mathbf{x}\|_1^2\}.\end{aligned}$$

If we assume that there exist false coins in the system, say at stack j, then

$$\mathcal{F}_{\varepsilon,T} = \{\mathbf{x}\in l_2^1 \mid ((1+\gamma)^T - 1) \mid x_j \mid^2 < \varepsilon \| \mathbf{x}\|_1^2, \text{ for some } j\}.$$

Next we will show that the *Wiener measure of the indistinguishable set* $\tilde{W}(\mathcal{F}_{\varepsilon,T})$ *converges constructively to zero when* $T\to\infty$. More precisely, we are going to prove that

$$\tilde{W}(\mathcal{F}_{\varepsilon,T}) \le \left(\frac{\varepsilon}{((1+\gamma)^T - 1 - \varepsilon)\cdot\prod_{m=1}^{\infty}\tilde{\delta}_m}\right)^{\frac{1}{2}}. \tag{15}$$

We now have:

$$\begin{aligned}&\tilde{W}(\mathcal{F}_{\varepsilon,T}) \\ &\le \frac{1}{\sqrt{\prod_{l=1}^{\infty}\tilde{\delta}_l}}\sup_k \int_{\text{quasi-loops}} e^{-\frac{(1+\gamma)^T-1}{\varepsilon}|x_k|^2} dW \\ &= \frac{1}{\sqrt{\prod_{l=1}^{\infty}\tilde{\delta}_l}}\sup_k \lim_{C\to\infty}\lim_{N\to\infty} \\ &\quad \frac{\int_{|x_N|<C\sqrt{N}}\int_{-\infty}^{\infty} G(x_N,N\mid\xi,k)\, e^{-\frac{(1+\gamma)^T-1}{\varepsilon}|\xi|^2} G(\xi,k\mid 0,0)\, dx_N d\xi}{\int_{|x_N|<C\sqrt{N}} G(x_M,\ M\mid 0,0)\, dx_N} \\ &= \frac{1}{\sqrt{\prod_{l=1}^{\infty}\tilde{\delta}_l}}\sup_k \lim_{C\to\infty}\lim_{N\to\infty}\frac{\sqrt{\pi N}}{\pi\sqrt{k(N-k)}} \\ &\quad \frac{\int_{-C\sqrt{N}}^{C\sqrt{N}}\int_{-\infty}^{\infty} e^{-\frac{|\xi|^2}{k}-\frac{(1+\gamma)^T-1}{\varepsilon}|\xi|^2-\frac{|x_N-\xi|^2}{N-k}} d\xi dx_N}{\int_{-C\sqrt{N}}^{C\sqrt{N}} e^{-\frac{|x_N|^2}{N}} dx_N}\end{aligned}$$

The inner integral in the numerator may be explicitly calculated as:

$$\int_{-\infty}^{\infty} e^{-\left(\frac{1}{k}+\frac{(1+\gamma)^T-1}{\varepsilon}+\frac{1}{N-k}\right)\xi^2}\, e^{2\frac{\xi x_N}{N-k}}\, e^{-\frac{1}{|N-k|}|x_N|^2}\, d\xi$$

$$= \frac{e^{-\frac{1}{|N-k|}|x_N|^2}\sqrt{\pi}e^{\frac{|x_N|^2}{|N-k|^2}\frac{1}{\left(\frac{1}{k}+\frac{(1+\gamma)^T-1}{\varepsilon}+\frac{1}{N-k}\right)}}}{\sqrt{\frac{1}{k}+\frac{(1+\delta)^T-1}{\varepsilon}+\frac{1}{N-k}}}.$$

The integrated exponential in the numerator becomes:

$$\begin{aligned}
e^{-\frac{|x_N|^2}{N-k}\left(1-\frac{1}{(N-k)(\frac{1}{k}+\frac{(1+\gamma)^T-1}{\varepsilon}+\frac{1}{N-k})}\right)} &= e^{-\frac{|x_N|^2}{N-k}\left(1-\frac{1}{\frac{N}{k}+\frac{(1+\gamma)^T-1}{\varepsilon}}\right)} \\
&= e^{-\frac{|x_N|^2}{N-k}}\, e^{\frac{|x_N|^2}{N-k}\left(\frac{1}{\frac{N}{k}+\frac{(1+\gamma)^T-1}{\varepsilon}}\right)} \\
&= e^{-\frac{|x_N|^2}{N-k}}\, e^{\frac{|x_N|^2}{N-k}\left(\frac{\varepsilon}{\frac{N}{k}\varepsilon+(1+\gamma)^T-1}\right)} \\
&< e^{-\frac{|x_N|^2}{N-k}}\, e^{\frac{|x_N|^2}{N-k}\left(\frac{\varepsilon}{(1+\gamma)^T-1}\right)} \\
&= e^{-\frac{|x_N|^2}{N-k}\left(1-\frac{\varepsilon}{(1+\gamma)^T-1}\right)}.
\end{aligned}$$

Finally, in view of the relation

$$\lim_{C\to\infty}\int_{-C\sqrt{N}}^{C\sqrt{N}}\frac{e^{-\frac{|x_N|^2}{N}}\,dx_N}{\sqrt{N}} = \lim_{C\to\infty}\int_{-\sqrt{C}}^{\sqrt{C}} e^{-v^2}dv = \sqrt{\pi},$$

we obtain the estimation (15) of the measure of the indistinguishable set

$$\begin{aligned}
W(\mathcal{F}_{\varepsilon,T}) &\le \frac{\sqrt{\varepsilon}}{\sqrt{(1+\gamma)^T-1}}\frac{1}{\sqrt{\prod_{m=1}^{\infty}\tilde{\delta}_m}\sqrt{1-\frac{\varepsilon}{(1+\gamma)^T-1)}}} \\
&= \left(\frac{\varepsilon}{((1+\gamma)^T-1-\varepsilon)\cdot\prod_{m=1}^{\infty}\tilde{\delta}_m}\right)^{\frac{1}{2}}.
\end{aligned}$$

For example, if we put

$$T_\eta = \log_{1+\gamma}\left(\frac{\varepsilon}{\eta^2\prod_{m=1}^{\infty}\tilde{\delta}_m}+1+\varepsilon\right),$$

then $\tilde{W}(\mathcal{F}_{\varepsilon,T}) \le \eta$ provided $t > T_\eta$. For example, if $\tilde{\delta}_m = e^{-2^{-m}}$, for all $m \ge 1$, then $T_\eta = \log_{1+\gamma}(\varepsilon e\eta^{-2}+1+\varepsilon)$.

To conclude our analysis, we use Bayes' formula in (15) to estimate the probability of absence of false coins in the system when the "device" does not click in time T on randomly chosen test-vectors selected from the class of quasi-loops. Using the same notation as in the end of Section 3, we have

$$P_{\text{non-click}}(\mathcal{N}) > 1-\frac{1-P(\mathcal{N})}{P(\mathcal{N})}\cdot\frac{\sqrt{\varepsilon}}{\sqrt{(1+\gamma)^T-1-\varepsilon}\sqrt{\prod_{m=1}^{\infty}\tilde{\delta}_m}}.$$

5 Is the Brownian Solution "Quantum"?

It is now the time to ask ourselves the question: Is the method "quantum" or not? After all, as one referee and [26] have pointed out, "continuous evolution in time and space ... is a common property of physical systems, classical as well as quantum".

Not surprisingly, our approach goes, in a sense, beyond the "classical" model of quantum computing in which a quantum Turing machine is the prototype.[13] A quantum Turing machine is a straightforward generalization of a Turing machine, in which the main ingredients are (a) (entangled) qubits that can be in various superpositions (b) a universal set of one-qubit and two-qubit unitary gates. It is designed to construct large, but *finite* unitary operations that can speed up the classical computation, say, by using quantum *finite* parallelism. By "default" these models cannot cope with the task of solving an undecidable problem. The new ingredients built in our "device" include the use of an infinite superposition (in an infinite-dimensional Hilbert space) which creates an "infinite type of quantum parallelism" and the ability to work with "truly random" vectors in an evolution described by an exponentially growing semigroup.

At this stage the "device" is more mathematical than physical. To simplify the formalism we have used a real Hilbert space (which is not typical for quantum problems) because (a) it supports the superposition principle and (b) has the typical features of quantum computing. The method is essentially quantum because we code the whole (infinite) data in an infinite superposition (the Hilbert space), we assume that we have the ability to generate "truly random" vectors in the Hilbert space and finally we apply one single measurement (via the quadratic form) to obtain the result. The method was inspired by and is closer "in spirit" to Benioff and Feynman early works [5, 20].

An essential question concerns the type of evolution. The evolution we use is a semigroup, more precisely, an unbounded, exponentially growing semigroup. The ability of extracting the required (finite) information from an infinite data in a finite amount of time is given in part by the "huge" growth of this semigroup.[14] Clearly, this is not the typical evolution for "quantum" systems; it is not difficult, but tedious (see [2, 31]), to transform this evolution into an equivalent unitary one.[15]

6 Final Comments

We have discussed a few simple problems and their solutions in the quest of finding a quantum approach for an undecidable problem. To this aim we have chosen the infinite

[13] See, for example, [23, 10]. A similar remark can be made for the approaches discussed in [16, 27].

[14] Compare with the following paragraph from [19]: "It bothers me that, according to the laws as we understand them today, it takes a computing machine an infinite number of logical operations to figure out what goes on in no matter how tiny a region of space, and no matter how tiny a region of time. *How can all that be going on in that tine space?* Why should it take an infinite amount of logic to figure out what a tiny piece of space-time is going to do?"

[15] This will be the object of a separate paper.

variant of the Merchant's problem which is equivalent to the Halting Problem, the most well-known undecidable problem.

Halting programs can be recognized by simply running them; the main difficulty is to detect non-halting programs. In deciding the halting/non-halting status of a non-halting machine, our "device" is capable to 'announce' (with a positive probability) the non-halting status in a finite amount of time, well before the 'real' machine reaches it (in an infinite amount of time). The device detects and measures this tiny, but non-zero probability. The method (described in Section 4.2) uses a quadratic form of an iterated map (encoding the whole data in an infinite superposition) acting on randomly chosen vectors viewed as special trajectories of two Markov processes working in two different scales of time.[16]

The methods for trespassing Turing's barrier discussed by both Etesi and Németi [16] and Kieu [27], although drastically different, have been, in some sense, prefigured by the accelerated Turing machines first imagined by Hermann Weyl (see, for example, the discussion in Svozil [33]). The main task of their authors is not to describe their methods, but to argue/prove that they do not contradict any *known* physical law. If a method would be shown to not be "theoretically implementable", then the result would still be interesting as that would show a new type of computational limit, *physical*, not logical.

In our case, the main result is *mathematical*. We have proved that *the Wiener measure of the indistinguishable set $\mathcal{F}_{\varepsilon,T}$ constructively tends to zero when T tends to infinity.* The "device", working in time T, appropriately computed, will determine with a pre-established precision whether an arbitrary program halts or not. *Building the "halting machine" is mathematically possible.*

The discrete-time Brownian motion–used in the estimation of the probability of the indistinguishable set in the last section–can be represented as a "sum" of independent random variables with Gaussian distributions. It can be implemented as a "sum" of spins of a cascade of electrons formed by the shock-induced emission on a special geometrical structure of semiconductor elements with special random properties (cf. [34]).

Many problems are still open and much more remains to be done. Is the method used in this paper "natural"? Is it feasible?[17] Is it better or can we get more "insight" about the nature of the Halting Problem if we use unitary operators?

The results discussed in this paper, as well as [8, 10, 16, 27], go beyond the pure mathematical aspects; they might impose the re-examination of the mind–machine issue (see [14]).

[16] Various natural ideas fail to produce exactly the desired result; one of them was discussed in Section 4.1.

[17] See also [8].

Acknowledgements

Ya. Belopolskaya [3] has suggested the book [32] and the use of the reflection principle, and M. Dumitrescu [15] and R. Ionicioiu [26] have spotted a couple of errors; we are most grateful to them all. We thank Ya. Belopolskaya, L. Carter, J. Casti, G. Chaitin, M. Dinneen, M. Dumitrescu, T. Kieu, I. Ibragimov, R. Ionicioiu, A. Lodkin, G. Păun, J. Summhammera, K. Svozil, A. Yafyasov, D. Wilson and the anonymous referees for heated and most inspiring discussions and criticism. Of course, nobody except the authors, are responsible for possible remaining errors.

References

[1] N.I. Akhiezer, I.M. Glazman. *Theory of Linear Operators in Hilbert Space*, Frederick Ungar, Publ., New York, vol. 1, 1966 (translated from Russian by M. Nestell).

[2] S. Albeverio, P. Kurasov. *Singular Perturbations of Differential Operators: Solvable Schrödinger Type Operators*, Cambridge University Press, 2000.

[3] Ya.I. Belopolskaya. Email to B. Pavlov, 13 December 2001.

[4] Ya.I. Belopolskaya, Yu.L. Dalecky. *Stochastic Equations and Differential Geometry*, Translated from the Russian, Mathematics and its Applications (Soviet Series) 30, Kluwer Academic Publishers Group, Dordrecht, 1990.

[5] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, *J. Stat. Phys.* 22 (1980), 563–591.

[6] C.S. Calude. *Information and Randomness. An Algorithmic Perspective*, Springer-Verlag, Berlin, 1994.

[7] C.S. Calude, J. L. Casti. Parallel thinking, *Nature* 392, 9 April (1998), 549-551.

[8] C.S. Calude, M.J. Dinneen, K. Svozil. Reflections on quantum computing, *Complexity* 6, 1 (2000), 35-37.

[9] C. S. Calude, B. Pavlov. Coins, Quantum Measurements, and Turing's Barrier: Preliminary Version, *CDMTCS Research Report* 156, 2001, 13 pp.

[10] C.S. Calude, G. Păun. *Computing with Cells and Atoms*, Taylor and Francis Publishers, London, 2001.

[11] J.L. Casti. Computing the uncomputable, *The New Scientist*, 154/2082, 17 May (1997), 34.

[12] D.W. Cohen. *An Introduction to Hilbert Space and Quantum Logic*, Springer-Verlag, New York, 1989.

[13] R. Compano. *Roadmaps for Nanoelectronics*, European Commission IST Programme, Future and Emerging Technologies, Second edition, 2000, Luxembourg.

[14] J. Copeland. Narrow versus wide mechanism: Including a re-examination of Turing's views on the mind-machine issue, *Journal of Philosophy* XCVI, 1 (2000), 5-32.

[15] M. Dumitrescu. Email to C.S. Calude, 3 January 2002.

[16] G. Etesi, I. Németi. Non-Turing computations via Malament-Hogarth space-times, *International Journal of Theoretical Physics* 41 (2002), 341-370. Los Alamos preprint archive `http: //arXiv:gr-qc/ 0104023`, v1, 9 April 2001.

[17] K. De Leeuw, E.F. Moore, C.E. Shannon, N. Shapiro. Computability by probabilistic machines, in C.E. Shannon J. McCarthy (eds.). *Automata Studies*, Princeton University Press, Princeton, N.J., 1956, 183-212.

[18] D. Deutsch, A. Ekert, R. Lupacchini. Machines, logic and quantum physics, *Bull. of Symbolic Logic* 6 (2000), 265-283.

[19] R.P. Feynman. *The Character of Physical Law*, M.I.T. Press, Cambridge, 1965.

[20] R.P. Feynman. Simulating physics with computers, *International Journal of Theoretical Physics* 21 (1982), 467-488.

[21] M.I. Freidlin. *Functional Integration and Partial Differential Equations*, Annals of Mathematics Studies, 109, Princeton University Press, Princeton, NJ, 1985.

[22] I.M. Gel'fand, N.Ya. Vilenkin. *Generalized Functions*, Volume 4, *Applications of Harmonic Analysis*, Academic Press, New York, 1964.

[23] J. Gruska. *Quantum Computing*, McGraw-Hill, London, 1999.

[24] P.R. Halmos. *Measure Theory*, D. van Nostrand, Princeton, 1968.

[25] J.G. Hey (ed.). *Feynman and Computation. Exploring the Limits of Computers*, Perseus Books, Reading, Massachusetts, 1999.

[26] R. Ionicioiu. Email to C.S. Calude, 16 January 2002.

[27] T.D. Kieu. Quantum algorithm for the Hilbert's tenth problem, Los Alamos preprint archive `http://arXiv:quant-ph/0110136`, v2, 9 November 2001.

[28] A. Lodkin. Personal communication to B. Pavlov, January 2002.

[29] A. Mikhailova, B. Pavlov. Quantum domain as a triadic relay, in I. Antoniou, C.S. Calude, M.J. Dinneen (eds.). *Unconventional Models of Computations, UMC'2K*, Springer Verlag, London, 2001, 167-186.

[30] A. Mikhailova, B. Pavlov, I. Popov, T. Rudakova, A. Yafyasov. Scattering on a compact domain with few semi-infinite wires attached: Resonance case, *Mathematische Nachrichten* 235 (2002), 101-128.

[31] B. Pavlov. The Theory of extensions and explicitly solvable models, *Russian Mathematical Surveys* 42, 6 (1987), 127-168.

[32] D.W. Stroock. *Probability Theory. An Analytic View*, Cambridge University Press, Cambridge, 1993.

[33] K. Svozil. The Church-Turing Thesis as a guiding principle for physics, in C.S. Calude, J. Casti and M.J. Dinneen (eds.). *Unconventional Models of Computation*, Springer, Singapore, 1998, 371-385.

[34] A. Yafyasov. Private communication to B. Pavlov, January 2002.

[35] C.P. Williams, S.H. Clearwater. *Ultimate Zero and One: Computing at the Quantum Frontier*, Springer-Verlag, Heidelberg, 2000.