CDMTCS
Research
Report
Series

Coins, Quantum Measurements, and Turing's Barrier: Preliminary Version

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

CDMTCS-156
June 2001

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: Preliminary Version

Cristian S. Calude[*] and Boris Pavlov[†]

June 2001

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/undecidable problems. Are there alternatives? Quantum computing offers one realistic alternative (see [8, 10, 2]). 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. Is there any hope for quantum computing to challenge the Turing barrier, i.e. to solve an undecidable problem, to compute an uncomputable function? See Feynman's argument (see [6], a paper reproduced also in [7]), regarding the possibility of simulating a quantum system on a (probabilistic) Turing machine.[1] simulation.

The current paper discusses solutions of a few simple problems, which suggest that quantum computing might be capable of computing uncomputable functions. In what follows a "silicon" solution is a solution tailored for a silicon (classical) computer; a "quantum" solution is a solution designed to work on a quantum computer.

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

[*] 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.

[1] Working with probabilistic Turing machines instead of Turing machines makes no difference in terms of computational capability: see [5].

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 nth stack contains false coins.

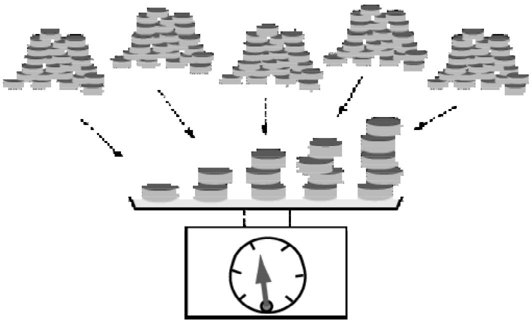

Figure 1: Coin selection.

The above "silicon" 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) in which the result produced is processed via a *classical calculation* and produces the desired final result.

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.

We note that any "silicon" solution of the Merchant's problem requires individual weighting coins from each stack and can't be solved with only one measurement.

3 The Merchant's Problem: The First Variant

We now consider the case when we have again five stacks of coins, but none or more than one stack of coins contains false coins. This means, we might have a situation when all five stacks contain true coins, or when only one stack contains false coins, or when 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?

4 The Merchant's Problem: The Second Variant

Consider the simplest case when 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. 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 the space $\mathbf{R}^N$, 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 $\mathbf{x}, \mathbf{y}$ 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, 9]; for specific relations with quantum physics see [4].

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 ith stack; if the ith stack contains true coins, then $q_i = \Gamma = 1$, otherwise, $q_i = \Gamma + \gamma = 1 + \gamma$.

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

$$\begin{aligned} \mathbf{Q}(\mathbf{x}) &= (q_1\mathbf{P}_1, \ldots, q_N\mathbf{P}_N)(\mathbf{x}) \\ &= (q_1x_1, \ldots, q_Nx_N). \end{aligned}$$

The tth 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 scalar product $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle$. In case all coins are true $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle = 1$, for all $\mathbf{x} \in \mathbf{R}^N$; if there are false coins in some stack, for some $\mathbf{x} \in \mathbf{R}^N$, $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle > 1$, and the value increases at 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 measurable function

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

a function which will be used in what follows.

We can interpret the measure generated by the density as a probability measure, hence we can calculate the probability of some event $\{\mathbf{x} \mid x \in \Omega\}$, as an integral, $\text{Prob}(\Omega) = \int_\Omega \rho dm$. Then, because of continuity of the density, we deduce that the probability of any "low-dimensional event" is equal to zero. In particular the event $x_s = 0$ is $\int_{x_s=0} \rho dm = 0$, 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, $t = 1, 2, \ldots$. Our procedure will be *probabilistic*: it will indicate a method to decide whether there exist any false coins with a probability as close to one as we want.

Fix a computable real $\eta \in (0, 1)$. Assume that both η and γ are computable reals.

Fix a "test" vector $\mathbf{x} \in \mathbf{R}^N$. The device 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 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 devices hasn't (yet?) clicked, so $\langle \mathbf{Q}^T(\mathbf{x}), \mathbf{x}\rangle \leq (1+\varepsilon) \parallel \mathbf{x} \parallel^2$. This may happen because either all coins are true, i.e., $\langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle = 1$, 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 t stage the test vector $\mathbf{x}$ produces "true" information. 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 weren't detected at time T; we say that $\mathbf{x}$ produces "false" information at time T.

For example, the null vector produces "false" information at any time. If the system has false coins and they are located in the jth stack, then each test vector $\mathbf{x}$ whose jth coordinate is 0 produces "false" information at any time. If the system has false coins and they are located in the jth stack, but

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

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

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

after this time the device will start clicking.

The major problem is to distinguish between the above two cases, *a task beyond the capability of any (probabilistic) Turing machine.* We will show how to compute the time T such that when presented a randomly chosen test vector $\mathbf{x} \in \mathbf{R}^N$ with non-null components to a device with sensitivity ε and the device fails to click in time T, then with probability larger than $1 - \eta$ the system doesn't contain false coins.

Assume first that the system contains false coins. Then

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

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 jth stack, q_j, is $\Gamma + \gamma = 1 + \gamma$. So, for every $t \geq 1$,

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

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

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

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

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

Consider now the set

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

If the system contains only true coins, then $F_{\varepsilon,t} = \mathbf{R}^N$, for all $\varepsilon > 0, t \geq 1$. Next we compute $\mathrm{Prob}(F_{\varepsilon,t})$ in case the system contains false coins.

For every $1 \leq i \leq N$, put

$$\Omega_{\varepsilon,t,i} = \{\mathbf{x} \in \mathbf{R}^N \mid (1+\gamma)^t |x_i|^2 \leq \langle \mathbf{Q}^t(\mathbf{x}), \mathbf{x}\rangle \leq (1+\varepsilon) \parallel \mathbf{x} \parallel^2\},$$

and note that if the system contains false coins then

$$F_{\varepsilon,t} \subset \bigcup_{i=1}^{N} \Omega_{\varepsilon,t,i}.$$

Each set $\Omega_{\varepsilon,t,i}$ can be decomposed into two disjoint sets as follows (here $M > 0$ is a large enough real which will be determined later):

$$\Omega_{\varepsilon,t,i} = \{\mathbf{x} \in \Omega_{\varepsilon,t,i} \mid \parallel \mathbf{x} \parallel^2 \leq M\} \cup \{\mathbf{x} \in \Omega_{\varepsilon,t,i} \mid \parallel \mathbf{x} \parallel^2 > M\}.$$

In view of the inclusion

$$\{\mathbf{x} \in \Omega_{\varepsilon,t,i} \mid \parallel \mathbf{x} \parallel^2 \leq M\} \subset \{\mathbf{x} \in \mathbf{R}^N \mid (1+\gamma)^t |x_i|^2 \leq (1+\varepsilon) M^2\},$$

we deduce that

$$\mathrm{Prob}(\Omega_{\varepsilon,t,i}) \leq \frac{1}{\sqrt{\pi}} \int_{-\frac{M\sqrt{1+\varepsilon}}{(1+\gamma)^{t/2}}}^{\frac{M\sqrt{1+\varepsilon}}{(1+\gamma)^{t/2}}} e^{-y^2} dy \leq \frac{2}{\sqrt{\pi}} \frac{M\sqrt{1+\varepsilon}}{(1+\gamma)^{t/2}}. \tag{3}$$

To estimate $\mathrm{Prob}(\{\mathbf{x} \in \Omega_{\varepsilon,t,i} \mid \parallel \mathbf{x} \parallel^2 > M\})$ we consider the set

$$C_M = \{\mathbf{x} \in \mathbf{R}^N \mid |x_i| > \frac{M}{\sqrt{N}}, \text{ for all } 1 \leq i \leq N\}.$$

As

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

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

$$\mathrm{Prob}(\{\mathbf{x} \in \mathbf{R}^N \mid\parallel \mathbf{x} \parallel > M, |x_j| \leq \frac{M}{\sqrt{N}}, \text{ for all } 1 \leq j \leq N\}) \leq \frac{N\sqrt{N}}{M\sqrt{\pi}}e^{-\frac{M^2}{N}}. \tag{4}$$

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

$$\mathrm{Prob}(\Omega_{\varepsilon,t,i}) \leq \frac{2M\sqrt{1+\varepsilon}}{\pi(1+\gamma)^{t/2}} + \frac{N\sqrt{N}}{M\sqrt{\pi}}e^{\frac{M^2}{N}},$$

hence

$$\mathrm{Prob}(F_{\varepsilon,t}) \leq \frac{N}{\sqrt{pi}}\left(\frac{2M\sqrt{1+\varepsilon}}{(1+\gamma)^{t/2}} + \frac{N\sqrt{N}}{M}e^{\frac{M^2}{N}}\right). \tag{5}$$

Putting

$$M = \left(N\log(1+\gamma)^{t/2}\right)^{1/2},$$

in (5) we get

$$\lim_{t\to\infty} \mathrm{Prob}(F_{\varepsilon,t}) = 0. \tag{6}$$

For large t,

$$\frac{N}{\sqrt{\pi}}\frac{2N\sqrt{1+\varepsilon}\log(1+\gamma)^{t/2}+N}{\log(1+\gamma)^{t/2}\sqrt{(1+\gamma)^{t/2}}} = \frac{N}{\sqrt{\pi}}\frac{2\sqrt{N(1+\varepsilon)}+N}{\sqrt{(1+\gamma)^{t/2}}}. \tag{7}$$

In conclusion, from (7) we deduce the following: *assuming that the system contains false coins, if*

$$T \geq \frac{2N^2(2\sqrt{N(1+\varepsilon)}+N)^2}{\pi\log(1+\gamma)\eta^2},$$

then

$$\mathrm{Prob}(F_{\varepsilon,T}) \leq \eta.$$

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", $\mathrm{Prob}(\mathcal{Y}) = 1 - \mathrm{Prob}(\mathcal{N})$. Hence,

$$\begin{aligned}
\mathrm{Prob}_{F_{\varepsilon,t}}(\mathcal{N}) &= \frac{\mathrm{Prob}((\mathcal{N})}{\mathrm{Prob}((\mathcal{N}) + (1-\mathrm{Prob}((\mathcal{N}))\mathrm{Prob}(F_{\varepsilon,t})} \\
&= \frac{1}{1+(\frac{1}{\mathrm{Prob}(\mathcal{N})}-1)\mathrm{Prob}(F_{\varepsilon,t})} \\
&\geq 1-(\frac{1}{\mathrm{Prob}(\mathcal{N})}-1)\mathrm{Prob}(F_{\varepsilon,t}).
\end{aligned}$$

Consequently, if $\mathrm{Prob}(\mathcal{N}) = \frac{N}{N+1}$, then $\mathrm{Prob}_{F_{\varepsilon,t}}(\mathcal{N}) \geq 1 - \frac{\mathrm{Prob}(F_{\varepsilon,t})}{N}$.

In conclusion,

> *for every $\eta \in (0,1)$ we can compute a time T_η such that picking up at random a test vector $\mathbf{x} \in \mathbf{R}^N$ with all non-null components and using a device with sensitivity ε up to time T_η without getting a click implies that with probability greater than $1-\eta$ all coins are true. If we get a click in time T_η, then the system contains false coins.*

5 The Merchant's Problem: The Infinite Variant

Let us assume that we have now a countable number of stacks, all of them, except perhaps one, containing true coins only. Can we determine whether there is a stack containing false coins?

The finite version of the problem, discussed in the above section, considers N stacks of coins. The "quantum solution" of the problem made use of a finite-dimensional Hilbert space, $\mathbf{R}^N$. Consider now the infinite countable number of stacks and the corresponding infinite-dimensional Hilbert space H which may be realized as a space of square-summable sequences or as a functional space. Again we assume that false coins weight $q_{i_0} = 1 + \gamma > 1$. A "trivial" answer to the problem of existence a "false" stack (a stack containing false coins) may be given in terms of a *selected orthogonal and normalized infinite basis* $\{e_l\}_{l=1}^{\infty}$ of the space. If the weight of all true coins is equal to one, we can form the quantum operator Q, $Qx = \sum_{l=1}^{\infty} q_l \langle x,\, e_l \rangle e_l$ as before and consider the trace of its iterations

$$\text{trace}\left[Q^T - I\right] = \sum_{l=1}^{\infty}\left[(q_l)^T - 1\right].$$

Then, $\text{trace}\left[Q^T - I\right] = 0$ if all coins are true, and $[(1+\gamma)^T - 1]$ if some stack contains false coins. In the second case, for a large number T of iterations, the trace will exceed the sensitivity threshold ε of the device, $[(1+\gamma)^T - 1] > \varepsilon$; in the first case, it will remain always under the sensitivity threshold (for any T). However, we can't use this "trivial" solution since it includes a forbidden step–the summation of an infinite series, though with only a finite number of non-zero terms!

Assume that the quadratic form of the quantum operator may be measured (calculated) directly on each test element of the infinite-dimensional Hilbert space H. The sensitivity of the device used to distinguish the possible "false" stack is defined by the following description of the set of "non-distinguishable elements" during an experiment of "length T":

$$\mathcal{F}_{\varepsilon,T} = \left\{\mathbf{x} \mid \langle Q^T\mathbf{x},\, \mathbf{x}\rangle < (1+\varepsilon) \parallel \mathbf{x} \parallel^2\right\}.$$

If for given test-vector $\mathbf{x}$ we have $\langle Q^T\mathbf{x}, \mathbf{x}\rangle \geq \parallel \mathbf{x} \parallel^2$, then the device clicks, which means that there is a false coin in some stack l (represented by a non-zero component x_l 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" with respect to the set $\mathcal{F}_{\varepsilon,T}$ of non-distinguishable elements.

The coordinate description of the set $\mathcal{F}_{\varepsilon,T}$ is given in the form of a cone centered at the "false plane" $x_{i_0} = 0$ in H:

$$\mathcal{F}_{\varepsilon,T} = \left\{\mathbf{x} \mid |x_{i_0}|^2 \leq \frac{\varepsilon}{(1+\gamma)^T - 1 - \varepsilon} \parallel \mathbf{x} \parallel^2\right\}.$$

An important question we could not answer concerns the measurability of the set $\mathcal{F}_{\varepsilon,T}$ with respect to the Gaussian measure extended from the algebra of all cylindrical sets based on finite-dimensional sets Ω_N in Hilbert space H:

$$\Omega_N \subset H_N \subset H, \quad \dim H_N < \infty.$$

If we could estimate the upper measure of the set $\mathcal{F}_{\varepsilon,T}$ from above and prove that it approaches 0 *when $T \to \infty$, the infinite-dimensional problem would be solved as well.* Unfortunately, *we can't do it now.* Hence, an *approximate* approach to the problem will be offered instead: we will construct a reasonably efficient family of finite experiments providing evidence that any finite-dimensional part $\mathcal{F}^N_{\varepsilon,T} = \mathcal{F}_{\varepsilon,T} \cap H_N$ of the cone $\mathcal{F}_{\varepsilon,T}$ with N and T related somehow, has small Gaussian measure. This means, that the probability of non-distinguishing false coins in $\mathcal{F}^N_{\varepsilon,T}$ goes to zero when "properly related" N and T go to ∞.

Further we use the notation $\alpha^2 = \frac{\varepsilon}{(1+\gamma)^T - 1 - \varepsilon}$, so that $\mathcal{F}_{\varepsilon,T} = \{\mathbf{x} \mid |x_{i_0}| \leq \alpha \parallel \mathbf{x} \parallel\}$. Together with the set $\mathcal{F}_{\varepsilon,T}$ in H we consider the set $\mathcal{F}^N_{\varepsilon,T}$ of all non-distinguishable vectors $\mathbf{x}$ in the finite-dimensional subspace $H_N \subset H$. The Gaussian measure on the Lebesgue-measurable sets Ω_N, $\Omega_N \in H_N$ is introduced as an integral $\frac{1}{\pi^{N/2}} \int_{\Omega_N} e^{-|x|^2} dm^N$, where m^N is the standard Lebesgue measure in H_N. The Gaussian measure of the cylindrical set in H based on Ω_N, $\Omega = \Omega_N \times (H \ominus H_N)$, is assumed to be equal to the Gaussian measure of the base Ω_N.

The Gaussian measure of the finite-dimensional non-distinguishable set $\mathcal{F}^N_{\varepsilon,T}$ can be explicitly calculated as follows:

$$|\mathcal{F}^N_{\varepsilon,T}| = \frac{\int_0^\alpha \frac{d\beta}{(1+\beta^2)^{N/2}}}{\int_0^\infty \frac{d\beta}{(1+\beta^2)^{N/2}}}.$$

In particular, for $N = 2n$, we have the following expression for the denominator

$$\int_0^\infty \frac{d\beta}{(1+\beta^2)^n} = \frac{(2n-2)!}{2^{2(n-1)}[(n-1)!]^2},$$

which, by using Stirling's formula, gives, for $n \to \infty$, the asymptotical estimation:

$$\int_0^\infty \frac{d\beta}{(1+\beta^2)^n} \approx \frac{1}{2}\sqrt{\frac{\pi}{n-1}}.$$

Hence, we obtain for large n, the estimation:

$$|\mathcal{F}^{2n}_{\varepsilon,T}| \approx 2\sqrt{(n-1)/\pi}\int_0^\alpha \frac{d\beta}{(1+\beta^2)^n}. \tag{8}$$

Formula (asF) remains valid for odd N as well.

We suggest a series of experiments in which the number of iterations in each experiment depends upon the dimension of the finite-dimensional space where the test elements are selected: given a monotonically-decreasing function $\Gamma(n)$, $\Gamma(n) \longrightarrow \infty$ when $n \to \infty$, we assume that T and n are related by the formula

$$\frac{\Gamma(n)}{n} = \frac{\varepsilon}{(1+\gamma)^T - 1 - \varepsilon} = \alpha_n^2 \longrightarrow 0. \tag{9}$$

An elementary calculation based on (8) shows that the Gaussian measure of the non-distinguishable sets in the above series of experiments may be estimated as:

$$|\mathcal{F}^{2n}_{\varepsilon,T}| \approx \frac{2}{\sqrt{\pi}}\int_0^{\sqrt{\Gamma(n)}} e^{-s^2} ds \approx \frac{2\sqrt{\Gamma(n)}}{\sqrt{\pi}} \longrightarrow 0, \tag{10}$$

provided T, $n = \frac{N}{2} \longrightarrow \infty$.

For example, choosing $n \approx (1+\gamma)^{T/2}$ we obtain $\Gamma(n) = (1+\gamma)^{-T/2}$, the relation (9) is satisfied, hence

$$|\mathcal{F}^{2n}_{\varepsilon,T}| \approx \frac{2}{\sqrt{\pi}}(1+\gamma)^{-T/2}.$$

In this approach, the number of iterations T (the "time") and the dimension of the observed space $2n$ are related through the relation (9). Assume that we run the experiments for time T and N stacks. If we get a click, then we know (with certainty) that the system contains false coins. If we don't get a click on the device, then in the "approximation" space of dimension N the probability to have false coins is about $\frac{2\sqrt{\Gamma(n)}}{\sqrt{\pi}}$. This probability goes to 0 as N tends to infinity. For the above example of Γ, the probability is less than a fixed $\eta \in (0,1)$ provided $T \geq 4\log_{1+\gamma}\left(\frac{2}{\eta\sqrt{\pi}}\right)$.

Of course, the above η gives the estimation of the probability that the false coins are present in proper finite-dimensional cone, but *is not* the probability that the whole system contains false coins (and, unfortunately, we don't know how to compute this probability from the obtained approximation).

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

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

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

[5] 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.

[6] R.P. Feynman, Simulating physics with computers, *International Journal of Theoretical Physics*, 11 (1985), 11–20.

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

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

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

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