MTAT.05.118 Quantum Computing I
Homework # 2

Assoc. Prof. Dirk Oliver Theis

Handed out:	Monday, Feb 17
Ask questions:	Wednesday, Feb 19 (in class)
Due:	Monday Feb 24, by 12:15
	(in class on paper or as PDF by email to `rafieh.mosaheb@ut.ee`)

Your First Quantum Algorithm

We denote the binary representation of an n-bit "unsigned" integer $\sum_{j=0}^{n-1} b_j 2^j$ by $[b_{n-1}b_{n-2}\cdots b_0]_2$. Here's a quantum algorithm.

Input : n
Output: x drawn uniformly at random $\in \{0,\dots,2^n-1\}$

1 Take a quantum register q with n qubits $q[j]$, $j=0,\dots,n-1$
/* mark 1 */
2 **for** $j=0,...,n-1$ **do**
3 | Prepare qubit j in state $|0\rangle$
/* mark 2 */
4 **for** $j=0,...,n-1$ **do**
5 | Apply the Hadamard gate to qubit j
/* mark 3 */
6 Measure q in the computational basis $\to [x_{n-1}\dots x_0]_2 =: x$
/* mark 4 */
7 Output x
8 (Optional step)

(a) Write down the state of the n-qubit quantum computer in each of the lines with a "mark". (Mark 1 is a trick question.)
(b) Prove that the algorithm is correct (i.e., output is related to input as desired).
(c) (No proof required.) We now modify the algorithm by replacing "(Optional step)" by "Goto step 2". Now the algorithm runs forever, and outputs an infinite list of bit strings. Denote the output by $X_1, X_2, X_3, \dots$ (infinite sequence of random variables). What's the relationship among the random variables X_j, $j=1,2,3,\dots$?
(d) (Blah-blah.) Make yourself aware of the possibility to generate truely random numbers using quantum technology, and of the applications of that possibility in cryptography, and, more importantly, online gambling. There are in fact several companies[1] for which generating random numbers using quantum-tech is an integral part of their core products or services.

[1] Crypto companies, of course — not gambling companies.