CONSTRUCTION OF AN N-SIDED QUANTUM DIE OR RESPECTIVELY A QUANTUM RANDOM NUMBER GENERATOR

MORITZ FINK

Contents

1. Introduction

The goal of this document is to define an algorithm that constructs a quantum circuit for an arbitrary number $n \in \mathbb{N}^{>1}$, so that the target state ψ_n is

$$\psi_n = \frac{1}{\sqrt{n}} \sum_{i=0}^{n} |s_i\rangle \tag{1}$$

This represents a state in which each possible outcome $|s_i\rangle$ is equally likely, i.e. an n-sided quantum die. Since N qubits can represent 2^N states $|s_0\rangle \dots |s_{2^N-1}\rangle$, we will at least need $N = \log_2(n)$ qubits to construct this state.
Furthermore, if $n \neq 2^N$ for all $N \in \mathbb{N}$, we define the desired quantum die to be an equal distribution of n of the 2^N possible outcomes, i.e. N satisfies $n < 2^N$ and

Date: June 6, 2021.

there exists a subset $S^* \subset S_N$ of all possible outcomes $S_N = \{|s_i\rangle \, | i = 0...2^N - 1\}$, so that

$$\psi_n = \frac{1}{\sqrt{n}} \sum_{s_i \in S^*} |s_i\rangle \tag{2}$$

Then, all (none-zero) outcomes $|s\rangle \in S^*$ have an equal probability of $\frac{1}{n}$.[1]

2. Trivial cases

First, we consider only the trivial cases $n = 2$ (e.g. coin flip) and $n = 3$. We will then show that all other cases can be constructed using those simple circuits.

2.1. n=2. The simplest case of a quantum die is a two-sided die, i.e. a coin flip. The desired target state is

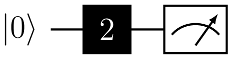
$$\psi_2 = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) \tag{3}$$

which gives equal probability for all outcomes $|0\rangle$ and $|1\rangle$:

$$| \langle 0|\psi_2\rangle |^2 = |\frac{1}{\sqrt{2}} \langle 0|0\rangle |^2 = \frac{1}{2} \tag{4}$$

$$| \langle 1|\psi_2\rangle |^2 = |\frac{1}{\sqrt{2}} \langle 1|1\rangle |^2 = \frac{1}{2} \tag{5}$$

ψ_2 is obviously the Hadamard state, so constructing a quantum circuit for $n = 2$ is straightforward and uses one Hadamard gate on a single qubit (see fig. 1).

We will refer to this circuit as 

.

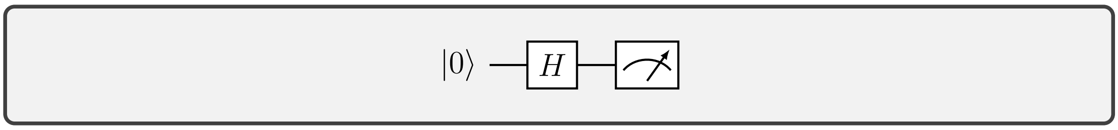


Figure 1. Quantum circuit of a two-sided quantum die using one Hadamard gate on a single qubit.

2.2. n=3. For a three-sided quantum die, the target state is

$$\psi_3 = \frac{1}{\sqrt{3}} \left(|00\rangle + |01\rangle + |11\rangle\right) \tag{6}$$

[1] Note, that all $|s\rangle \in S_N \setminus S^*$ have probabilities equal to zero.

Its construction starts by taking the state $|00\rangle$ to $\frac{1}{\sqrt{3}}|00\rangle + \frac{\sqrt{2}}{\sqrt{3}}(|01\rangle + |11\rangle)$ which is a single qubit operation U on the first qubit[2]. We define

$$U = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{\sqrt{2}}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{pmatrix} \tag{7}$$

so that U is unitary[3] and

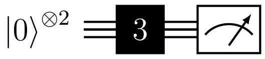
$$U|0\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle \tag{8}$$

$$(I \otimes U)|00\rangle = \frac{1}{\sqrt{3}}|00\rangle + \frac{\sqrt{2}}{\sqrt{3}}|01\rangle \tag{9}$$

where I is the canonical Identity matrix. The second and last step is to take the second qubit to the Hadamard state ψ_2 if the first qubit is 1.
In terms of a quantum circuit the two operations can be implemented by a $U3$ gate followed by a controlled Hadamard gate (see fig. 2), where

$$U3 := \begin{pmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\Phi}\sin(\frac{\theta}{2}) & e^{i(\lambda+\Phi)}\cos(\frac{\theta}{2}) \end{pmatrix} \tag{10}$$

with $\theta = 2\arccos(\frac{1}{\sqrt{3}})$, $\lambda = \pi$ and $\Phi = 0$.

We will refer to this circuit as 

.

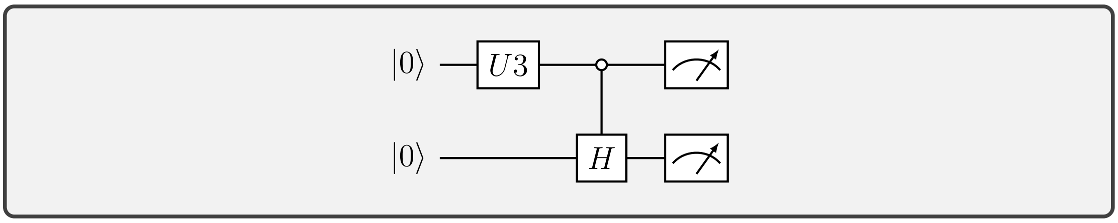


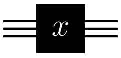
FIGURE 2. Quantum circuit of a three-sided quantum die using a $U3$ gate and a controlled Hadamard gate.

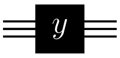
3. Non-trivial cases

Based on the results of the previous section, we can now build quantum dice with the number of sides being greater than three. Those can be recursively constructed by splitting the number of desired sides n into its prime factors and combining the smaller n_{prime}-sided quantum die circuits.

[2] The first qubit is the rightmost qubit q_0 inside the Ket $|q_1 q_0\rangle$ (with index 0).

[3] $U^\dagger U = I$

3.1. **Products.** If $n = xy$ for $x, y \in \mathbb{N}^{>1}$, then 

and 

can be combined in the way depicted in fig. 3. Basically, instead of 'throwing' one die, we just 'throw' several dice and combine the results. In that way, a six-sided quantum die is a combination of a two-sided and a three-sided quantum die (see fig. 4) with

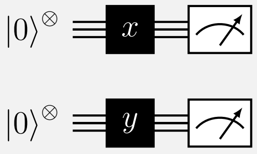


FIGURE 3. Combined quantum die that forms the product $n = xy$.

$$\psi_6 = \psi_3 \otimes \psi_2 = \frac{1}{\sqrt{6}} (|000\rangle + |010\rangle + |110\rangle + |001\rangle + |011\rangle + |111\rangle) \tag{11}$$

We can use this approach to build n-sided quantum dice, if the prime factorisation of n is given.

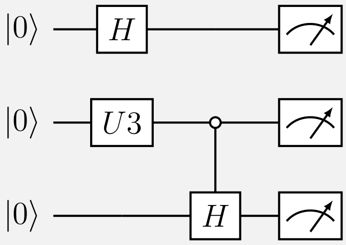


FIGURE 4. Quantum circuit of a six-sided quantum die using a two-sided and a three-sided quantum die.

3.2. **Prime numbers.** Since we can now build an n-sided quantum die using its prime factors, we recursively construct an n_{prime}-sided quantum die by combining the $(n_{prime} - 1)$-sided quantum die with one additional control qubit q_c. Similar to the construction in section 2.2, we first construct the state

$$\psi_{n_{prime}} = \psi_{n_{prime}-1} \otimes \frac{1}{\sqrt{n_{prime}}} \left(|0\rangle + \sqrt{n_{prime} - 1}\,|1\rangle\right) \tag{12}$$

The respective quantum circuit is depicted in fig. 5, using a $U3$ gate with $\theta = 2\arccos(\frac{1}{\sqrt{n_{prime}}})$, $\lambda = \pi$ and $\Phi = 0$.

Since $\psi_{n_{prime}-1}$ can be decomposed in terms of prime factors, we can repeat this

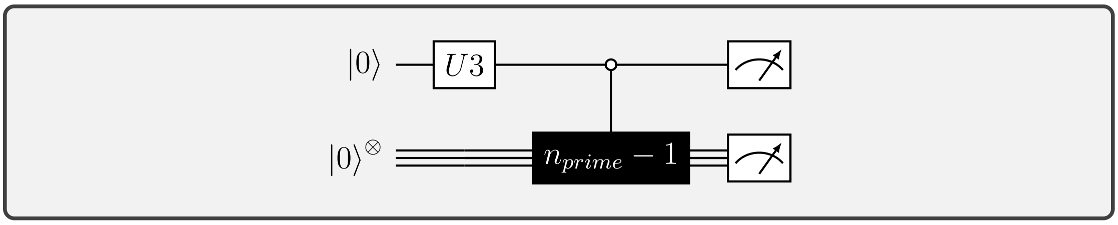
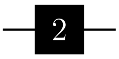
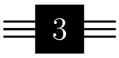


Figure 5. Quantum circuit decomposition of an n_{prime}-sided quantum die.

recursion until the circuit is built only using  . Note, that the circuit  is just a special case of this construction. An example for a five-sided quantum die, constructed in this way, is given in fig. 6.

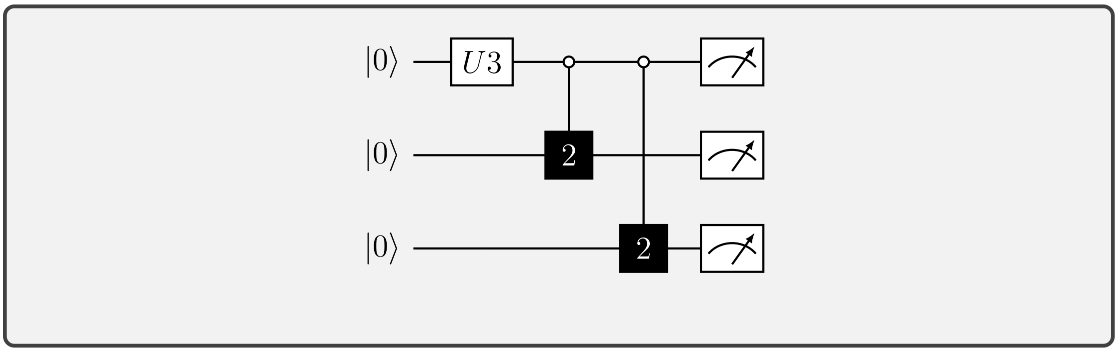


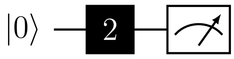
Figure 6. Quantum circuit of a five-sided quantum die using the decomposition of a four-sided quantum die together with a control qubit.

4. The algorithm

Finally, we are able to write down the resulting algorithm for the construction of an n-sided quantum die:

(1) Find the prime factorisation T_n of n (see Shor's Algorithm[4]).
(2) If T_n contains prime factors other than two, write those prime factors n_{prime} as $(n_{prime} - 1) + 1$ and write $(n_{prime} - 1)$ as product of its prime factors.
(3) Repeat the previous step until the resulting term T_n only contains factors of two and addends of one.
(4) Construct the quantum circuit according to algebraic priority from smallest to largest terms:

[4] https://arxiv.org/abs/quant-ph/9508027

(a) For each factor of two, add  to the product's sub-circuit.

(b) For each sum n_{prime}, add a control qubit q_c to the circuit, that passes a $U3$ gate with $\theta = 2\arccos(\frac{1}{\sqrt{n_{prime}}})$, $\lambda = \pi$ and $\Phi = 0$ before it controls[5] the already constructed sub-circuit of the $n_{prime} - 1$ addend (see fig. 5).

4.1. **Complexity.** The complexity of the given algorithm heavily depends on the number of prime factors two and addends one in the decomposition of the number of outcomes n. This decomposition can be found by applying Shor's Algorithm as many times as needed. In general, it is hard to tell how much factors and addends the desired decomposition of a given n has. In the worst case, n is a prime number with $n - 1$ being a product of 2 and another prime number which in turn is again a product of 2 and another prime number and so on. This number n would be decomposed into $\log_2 n$ factors of two and addends of one each.

For each factor of two, the algorithm requires one additional qubit and one additional gate (Hadamard). For each addend of one, we need a dedicated control qubit which controls the already added gates of the controlled sub-circuit and one additional gate ($U3$).

All in all, if n can be decomposed into $n_{\times 2}$ factors of two and n_{+1} addends of one, then the quantum circuit requires in total $N = n_{\times 2} + n_{+1}$ qubits and $N_{gates} = n_{\times 2} + n_{+1} = N$ gates.

4.2. **Pseudocode.** The following pseudocode describes the given algorithm:

```
def buildCircuit(n, control_qubits[]):
  if n==2:
    add qubit with Hadamard gate which is controlled by all qubits in
  else:
    prime_factors = find_prime_factors(n)
    for(prime_factor in prime_factors):
      add control qubit q_c with U3 gate
      control_qubits.append(q_c)
      buildCircuit(n-1, control_qubits)
```

5. Implementation on a quantum computer

5.1. **Qiskit code.**

5.2. **Results.**

6. Conclusion

[5] Apply all gates of the sub-circuit only if the control bit q_c is $|1\rangle$.