Shor's algorithm. To find a nontrivial factor of a large number n one can try the following steps:

1. Guess a random $p < n$ such that $\gcd(p, n) = 1$ (the greatest common divisor of p and n);
2. Quantum state observations allow us to detect an even integer r such that $p^r = 1 \mod n$ (half of p's will have such r);
3. Since
$$(p^{r/2} - 1)(p^{r/2} + 1) = 0 \mod n$$
so probably $(p^{r/2} \pm 1)$ has a common factor with n; use Euclidean algorithm to find it.

An integer value r is called the *period* of p if $p^r = 1 \mod n$.

Quantum state in Shor's algorithm. Let r be the period of p for the group of residues mod n. Shor proposed a construction of quantum state

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp(2\pi i ac/q) \, |c\rangle |p^a \bmod n\rangle$$

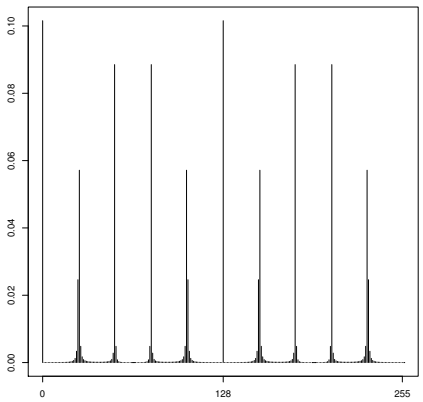
and demonstrated that the chance $P(c)$ of observing $|c\rangle$ is most likely at $c \approx qd/r$ with some integer $0 \le d < r$. This probability mass function (pmf) $P(c)$ is fairly accrately obtained by

$$\frac{r}{q^2} \left(\left[\sum_{a=0}^{q-1} h_1(a) \sin(2\pi ac/q) \right]^2 + \left[\sum_{a=0}^{q-1} h_1(a) \cos(2\pi ac/q) \right]^2 \right) \tag{7.1}$$

where h_1 is a function of period r, and defined by

$$h_1(a) = \begin{cases} 1 & \text{if } (p^a \bmod n) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Example. The following figure exhibits the pmf $P(c)$ when $n = 33$, $p = 2$, and $q = 2^8$ are chosen. The sharp peaks are observed at $c = 26, 51, 77$, and so on, and the corresponding values qd/c are 9.85, 10.04, 9.97, respectively with $d = 1, 2, 3$. Thus, we can guess $r = 10$.



Increasing a chance to detect the period. Let $S = \{0, 1, \ldots, q-1\}$ be the state space. When q is prohibitively large, a chance to observe $h_1(a) = 1$ by randomly sampling $a \in S$ is practically zero. We can instead choose a small number $d \ll n$, and set $A_d = \{a \in S : (p^a \bmod n) \le d\}$. Then we can propose a different indicator function h_d of period r by

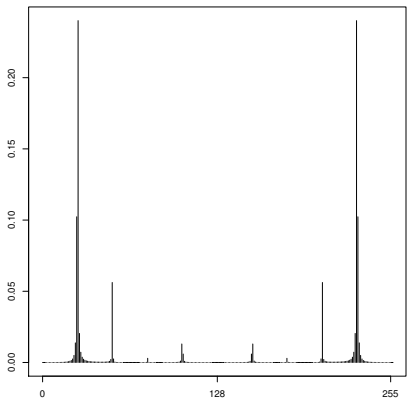
$$h_d(a) = \begin{cases} 1 & \text{if } a \in A_d; \\ 0 & \text{otherwise,} \end{cases}$$

and replace $P_1(c)$ with

$$P_d(c) = \frac{1}{z_d} \left[\sum_{a=0}^{q-1} h_d(a) \sin(2\pi ac/q) \right]^2, \quad c \in S \tag{7.2}$$

where z_d is the normalizing constant.

Example, continued. The following figure exhibits the pmf $P_d(c)$ with $d = 8$ when $n = 33$, $p = 2$, and $q = 2^8$ are chosen as before.



Is Monte Carlo simulation applicable? Monte Carlo simulation is readily applicable when a model of interest is formulated in terms of probability distributions. In particular it provides a method to sample $(Y, X_1, \ldots, X_k)$ from the probability mass function (pmf)

$$f(x_0, x_1, \ldots, x_k), \quad (x_0, x_1, \ldots, x_k) \in S^{k+1},$$

when a sample space S^{k+1} is discrete. This allows us to view an observation $Y = c$ as if it comes from the marginal pmf

$$F(c) = \sum_{(x_1, \ldots, x_k) \in S^k} f(c, x_1, \ldots, x_k)$$

without calculating the summation.

Negative sign problem. One may wish to use Monte Carlo simulation by viewing the summation of (7.2) as a marginal pmf. However, Monte Carlo method is not immediately applicable since $h_d(a) \sin(2\pi ac/q)$ can be negative. We can instead consider the pmf proportional to

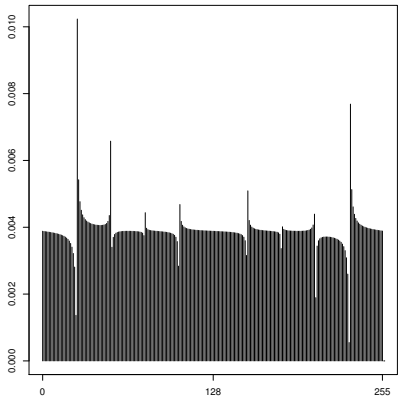
$$g_2(c, a_1, a_2) = h_d(a_1) h_d(a_2) \left[\sin(2\pi a_1 c/q) + 1\right] \left[\sin(2\pi a_2 c/q) + 1\right],$$

and generate a sample (Y, X_1, X_2) from S^3. Then an observation $Y = c$ comes from the marginal pmf

$$G_2(c) = \frac{1}{z_2} \sum_{(a_1,a_2)\in S^2} g_2(c, a_1, a_2) = \frac{1}{z_2} \left[\sum_{a=0}^{q-1} h_d(a)[\sin(2\pi ac/q) + 1] \right]^2 \tag{7.3}$$

where z_2 is the normalizing constant.

Example, continued. The plot below shows $G_2(c)$ in order to compare with $P_d(c)$ with $d = 8$ when $n = 33$, $p = 2$, and $q = 2^8$ are chosen. The pmf $G_2(c)$ clearly loses a sharp contrast for peaks, and a random sample from g_2 may not be able to distinguish the peaks.



Simulation on a higher dimension One may possibly break this curse by constructing a state space of higher dimemsion. Here we sample $(Y, X_1, \ldots, X_k)$ from a pmf proportional to

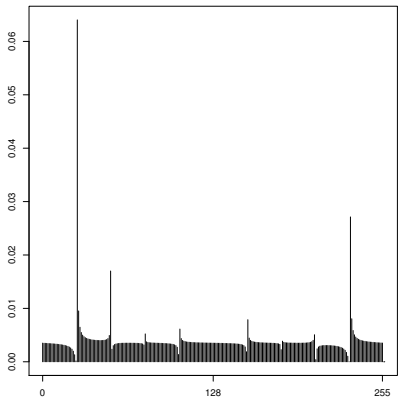
$$g_k(c, a_1, \ldots, a_k) = \prod_{i=1}^{k} h_d(a_i) \left[\sin(2\pi a_i c/q) + 1\right] \tag{7.4}$$

on the state space S^{k+1}. Then a marginal observation $Y = c$ comes from the pmf

$$G_k(c) = \frac{1}{z_k} \left[\sum_{a=0}^{q-1} h_d(a)[\sin(2\pi ac/q) + 1] \right]^k$$

where z_k is the normalizing constant.

Example, continued. The plot (below left) demonstrates how the pmf $G_6(c)$ improves the sharpness of its peaks.



Range of distribution. In addition if we can narrow the domain of marginal distribution to isolate one peak then we may be able to detect the peak more efficiently. For example, let $n = m_1 m_2$ be a semiprime number, and let $r = \text{lcm}(m_1 - 1, m_2 - 1)$ be the Carmichael lambda. An effective lower bound b for the Carmichael lambda may be used to restrict the sampling range up to $\lceil q/b \rceil$. For choosing q in a large simulation study of Monte Carlo methodology one may need a sharper upper bound in order to isolate the first mode around q/r.

Example, continued. The plot (below right) is generated when the pmf $G_2(c)$ is restricted to $c = 1, \ldots, 43$ when $n = 33$, $b = 6 = \lceil \sqrt{n} \rceil$, $p = 2$, and $q = 2^8$ are chosen. We can use an upper bound $\lceil q/b \rceil = 43$, and isolate a single mode at $c = 26$, which may allow us to guess $r = 10$.