# Shor's 算法

赵晓菲

2023 年 8 月 6 日

# 因式分解和周期查找

**加密:** 通常我们使用两个大素数 P 和 Q 生成一个非常大的整数 N，使得 $N = P \times Q$。N 是公开的，只有持有密钥的人可以快速找到 P 和 Q。
**质整数因式分解:** N 的素数因子分解与某个函数的周期性有关。假设我们想要分解 $N = 21$。选择一个 a（稍后我们将讨论如何选择 a）。找到函数 $f_{a,N}(x) = a^x \mod N$ 的周期 r。我们将通过从 0 开始代入 x 来找到它。

# 因式分解和周期查找

**加密:**

$$
\begin{aligned}
f_{a,N}(0) &= a^0 \mod 21 = 1 \\
f_{a,N}(1) &= a^1 \mod 21 = 11 \\
f_{a,N}(2) &= a^2 \mod 21 = 16 \\
f_{a,N}(3) &= a^3 \mod 21 = 8 \\
f_{a,N}(4) &= a^4 \mod 21 = 4 \\
f_{a,N}(5) &= a^5 \mod 21 = 2 \\
f_{a,N}(6) &= a^6 \mod 21 = 1
\end{aligned}
$$

我们可以看到答案在周期 6 内重复（$f_{a,N}(0) = f_{a,N}(0+6)$）。因此，$r = 6$。

# 因式分解和周期查找

由于周期性，我们有：

$$f_{a,N}(0) = a^0 \mod N = 1$$

$$f_{a,N}(r) = f_{a,N}(r+0) = a^r \mod N = f_{a,N}(0) = 1$$

其中我们使用了代数中的规则，如
$(a^2-1)(a^2+1) = a^4-1$ $r$ $a^{r/2}+1 \mod N \neq 0$，那么素因子由以下给出：

$$P = \gcd(a^{r/2}+1, N)$$

$$Q = \gcd(a^{r/2}-1, N)$$

# 因式分解和周期查找

由于周期性，我们有：

$$f_{a,N}(0) = a^0 \mod N = 1$$

$$f_{a,N}(r) = f_{a,N}(r+0) = a^r \mod N = f_{a,N}(0) = 1$$

其中我们使用了代数中的规则，如 $(a^2-1)(a^2+1) = a^4-1$。然后，我们将使用一个定理，如果 $r$ 是偶数且 $a^{r/2}+1 \mod N \neq 0$，那么素因子由以下给出：

$$P = \gcd(a^{r/2}+1, N)$$

$$Q = \gcd(a^{r/2}-1, N)$$

# 因式分解和周期查找

现在我们来检查 $r = 6$ 是否为偶数，并且计算 $a^{r/2} + 1 \mod N$：

$a^{r/2}+1 \mod N = 11^{6/2}+1 \mod 21 = 11^3+1 \mod 21 = 1331+1 \mod 2$

因此，我们可以继续计算 $P$ 和 $Q$：

$$P = \gcd(11^{6/2} + 1, 21) = \gcd(9, 21) = 3$$

$$Q = \gcd(11^{6/2} - 1, 21) = \gcd(7, 21) = 7$$

因此，$21 = 3 \times 7$，我们找到了 N 的素因子化。

# Shor's 算法的步骤

1. 创建指数级别的参数的叠加态：$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$，其中 $n$ 是计算素数周期所需的比特数。
2. 在 $n$ 个 qubit 上对这个叠加态进行函数计算：$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$，其中 $f(x)$ 是需要计算的函数，$f(x) = a^x \mod N$。
3. 对上述叠加态进行并行傅里叶变换：$\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} e^{2\pi ixy/2^n}|y\rangle|f(x)\rangle$，使用量子傅里叶变换 (QFT)。
4. 对傅里叶变换结果进行测量，得到函数的周期。

# 任意的正整数

对于任意的正整数 $N$，我们总是可以找到 $n$ 使得 $2^n \geq N$。例如，如果 $N = 21$，我们需要 $n = 5$，使得 $2^5 = 32 \geq 21$。

# Shor's 算法

- 对于给定的 $N$ 和 $a$，我们使用 Shor's 算法来找到函数 $f(x) = a^x \mod N$ 的周期 $r$。
- 在计算过程中，我们创建了指数级别的参数的叠加态：$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$，并对其进行函数计算和傅里叶变换。
- 最终，我们测量傅里叶变换结果以获得函数的周期 $r$。
- 一旦我们获得了 $r$，我们可以根据 Shor's 算法的定理计算出 $N$ 的素因子：$P = \gcd(a^{r/2} + 1, N)$ 和 $Q = \gcd(a^{r/2} - 1, N)$。
- 因此，Shor's 算法为求解质因数分解问题提供了一个高效的量子算法。

- 在 Shor's 算法的执行中，我们创建了两个叠加态：$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$ 和 $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$。
- 我们通过对第一个叠加态进行傅里叶变换来计算函数 $f(x)$ 的周期 $r$。
- 接下来，我们对第二个叠加态进行傅里叶变换以获得关于函数 $f(x)$ 的更多信息。
- 最后，我们测量第二个叠加态，并通过后续的经典计算来找到 $N$ 的素因子。
- Shor's 算法是一种重要的量子算法，它对于破解 RSA 加密等问题有重要的应用。

# Shor's 算法

- 现在，我们通过傅里叶变换操作来计算 $2^n$ 个周期函数的叠加态：$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$。
- 对这个叠加态应用傅里叶变换，并测量第一个寄存器，我们得到一个幂次谱（power spectrum）的概率分布，它的峰值位置对应于函数 $f(x)$ 的周期 $r$ 的可能值。
- 经过一些经典计算，我们可以从幂次谱中找到 $r$ 的一个近似值。
- 最后，我们通过计算一些最大公约数（GCD）来找到 $N$ 的可能素因子，这些素因子可能是 $r$ 的因子。
- 注意：Shor's 算法在经典计算上的开销较大，对于大型 $N$ 来说可能不太实际，但在量子计算机上，Shor's 算法的复杂度远远低于传统的经典算法。

# Shor's 算法

- 接下来，我们对叠加态应用傅里叶变换，以计算 $2^n$ 个周期函数的叠加态：$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$。
- 对这个叠加态应用傅里叶变换，并测量第一个寄存器，我们得到一个幂次谱（power spectrum），其中的峰值位置对应于函数 $f(x)$ 的可能周期 $r$ 的近似值。
- 经过一些经典计算，我们可以从幂次谱中找到 $r$ 的近似值。
- 最后，我们通过计算一些最大公约数（GCD），可以找到 $N$ 的可能素因子，这些素因子可能是 $r$ 的因子。
- 注意：Shor's 算法在经典计算上的开销较大，对于大型 $N$ 来说可能不太实际，但在量子计算机上，Shor's 算法的复杂度远远低于传统的经典算法。

# Shor's 算法

- 现在，我们将对具有最重要的 $2n$ 个量子比特的第一个寄存器进行测量。假设它将坍缩为 $|k\rangle$。那么测量结果为：

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\alpha_x|x\rangle\left(\sum_{k=0}^{2^n-1}e^{\frac{-i2\pi kf(x)}{2^n}}|k\rangle\right)$$

$$\propto \sum_{k=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}\alpha_x e^{\frac{-i2\pi kf(x)}{2^n}}\right)|k\rangle$$

- 我们可以观察到测量后的态的系数与 $e^{-i2\pi ky/2^n}$ 成正比，其中 $y$ 表示测量结果 $k$ 对应的可能周期 $r$ 的近似值。
- 让我们令 $w = e^{-i2\pi y/2^n}$，再次强调 $y$ 在一对括号内。然后我们可以计算：

$$\sum_{k=0}^{2^n-1}w^k = \begin{cases} 2^n, & \text{如果} w = 1 \\ 0, & \text{如果} w \neq 1 \end{cases}$$

- 假设我们得到的 $y$ 值为 4，即 $w = e^{-i\pi/8}$，那么上式为 0。这意味着我们没有成功找到周期，需要重复算法以获取更准确的结果。