> A good idea has a way of becoming simpler and solving problems other than that for which it was intended. – Robert Tarjan

量子Fourier变换

正如引言所述，解决一个问题的好思路可以超越原本问题。傅里叶变换就是其中之一，传统傅里叶变换将时域信号变换到频域。时域上原本杂乱无章的信号波形可能在频域上呈现人们一眼就能看出的规律，大大地简化分析过程。

量子Fourier变换基本形式

那么，我们如何将傅里叶变换扩展到量子领域呢?

我们先来观察时域上的离散傅里叶变换公式:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{-2\pi i j \frac{k}{N}}$$

从信号的角度来讲，如果x_i是时域上的一组彼此正交的离散数据点，y_i是这组数据点经过离散傅里叶变换后表现在频域上的信号，由一组彼此正交的$e^{2\pi ij/N}$基本信号叠加。那么频域上的一个离散点是时域上N个数据点的叠加。

简单地用$|k\rangle$替换x_i,用$|j\rangle$替换y_k,。在量子语境下，同样的变换则是将一个量子态$|j\rangle$映射到$|0\rangle, |1\rangle, ..., |N-1\rangle$，一共$N$个量子态之和。量子傅里叶变换公式为:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} |k\rangle$$

这两个公式几乎一模一样。值得注意的是，量子傅里叶变换是一个酉变换，根据酉变换的内积不变性可以证明这一点。
证明：量子傅里叶变换是一个酉变换

量子Fourier变换的积形式

为了更加高效地实现量子电路，我们将量子Fourier变换写成如下形式:

$$|j_1, ..., j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 \dot{j}_n}|1\rangle)}{2^{n/2}}$$

其中$0.j_1j_2...j_n$是二进制表示，计算方法与二进制小数相同。这个变换的构造过程用到了$e^{2\pi i}$的周期性。

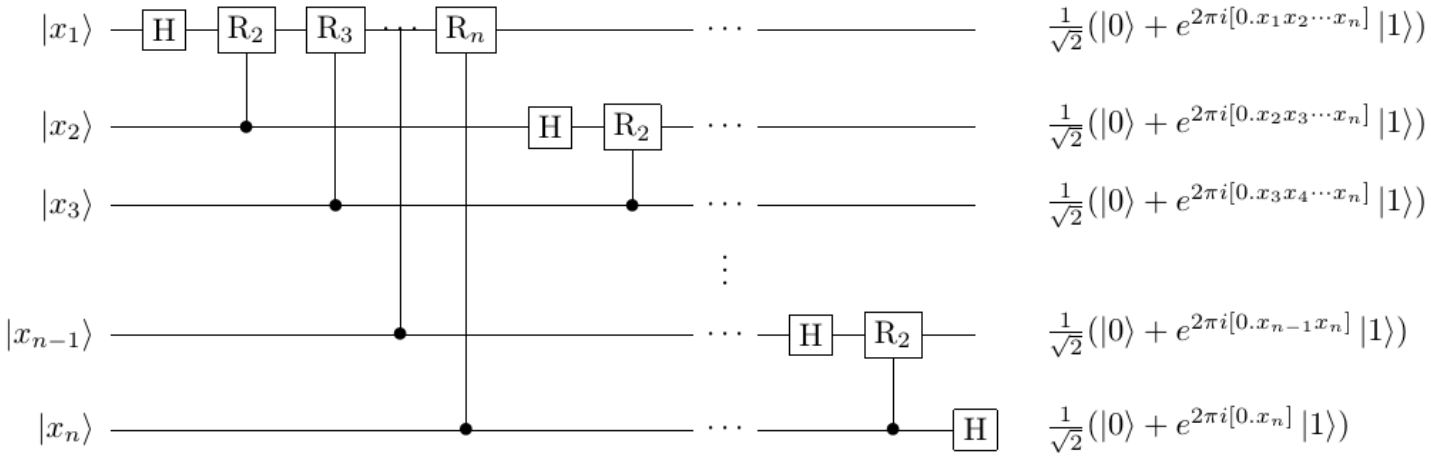
其中$|1\rangle$前面的系数可以写成很多项形如$e^{2\pi i0.k}$相乘的形式，那么假设有一个R_k门：

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ \\ 0 & e^{2\pi i/2k} \end{bmatrix} = e^{\frac{2\pi i}{2^{k+1}}} XR_z(-\frac{2\pi}{2^{k+1}})XR_z(\frac{2\pi}{2^{k+1}})$$

这个R_k门可以分解成单量子比特门和Pauli-X门的乘积。每个量子态经过一次阿达马变换，然后通过不同数量的与其余量子态有关的受控R_k门，可以完成上述公式的操作。

量子Fourier变换的量子线路

如图所示是量子傅里叶的量子线路图。



如图变换之后，量子态再经过一次逆转量子比特的顺序，得到与上面公式一样的形式

量子傅里叶变换的复杂度

很容易看出，我们一个使用了n个Hadamdard门，使用$1+2+\cdots+n$个受控R_k门，最后的交换过程我们使用$\frac{3}{2}n$个CNOT门。因此量子傅里叶变换的复杂度为$\Theta(n^2)$

相位估计

> 酉矩阵的特征值是模为1的复数，不同特征值对应的特征向量两两正交。

背景

假设酉矩阵 U, 其特征向量为$|u\rangle$, 特征值为$e^{2\pi i\varphi}$。那么根据酉矩阵的性质$U|u\rangle = e^{2\pi i\varphi}|u\rangle$。并且对量子态进行变换操作的酉算子可以用酉矩阵来表示。相位估计做的事情，就是把这个φ估计出来。

相位估计：

- 输入： 执行酉运算U的量子线路Q，以及U的特征向量$|u\rangle$
- 输出： 估计的U的相位$\varphi \in [0,1)$

相位估计的量子线路构造

定义 $\Lambda_m(U)$ 为一种对$m+n$个量子比特操作的酉运算，满足

$$\Lambda_m(U)|k\rangle|\psi\rangle = |k\rangle(U^k|\psi\rangle)$$

前面的m个量子比特状态决定 $|\psi\rangle$ 进行的酉运算U的次数。后一个量子态 $|\psi\rangle$ 是酉矩阵U的特征向量。我们用下面这张图来表示 $\Lambda_m(U)$ 这种变换

如图所示，完成相位估计一共需要两个寄存器，显然，得到和测量相位估计的结果需要消耗一个寄存器；除此之外另一个寄存器做什么呢？注意到U的特征向量还没有出现，但是实现 $U|u\rangle = e^{2\pi i\varphi}|u\rangle$ 必须要利用特征向量 $|u\rangle$,另一个寄存器是不是应该存储U矩阵的特征向量呢?

除此之外，我们需要对前m个量子比特进行阿达马变换，当 $|0^m\rangle$ 通过一个阿达马门后，我们得到

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}|k\rangle|\psi\rangle$$

再经过一次 $\Lambda_m(U)$ 变换，我们得到

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}|k\rangle(U^k|\psi\rangle)$$

根据特征值和特征向量的关系 $U|u\rangle = e^{2\pi i\varphi}|u\rangle$ 得到，

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle|\psi\rangle$$

因为第二个寄存器始终保持状态 $|\psi\rangle$, 我们在描述里可以忽略该状态，

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle$$

估计 φ

目前为止我们已经将待估计量 φ 放进表达式里，但是还没能估计出具体数字。接下来怎么做呢？本着未知问题向已知问题转化的科学思想，并且上面得到的式子与量子Fourier变换颇有神似。我们试着把剩下的部分交给量子Fourier变换。

如果相位 φ 正好能被一个二进制数 t 表示， 数 t 一共有 m 位。那$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle$就恰好可以被表示成Fourier变换的积形式

$$\frac{(|0\rangle+e^{2\pi i0.\varphi_t}|1\rangle)(|0\rangle+e^{2\pi i0.\varphi_{t-1}\varphi_t}|1\rangle)...(|0\rangle+e^{2\pi i0.\varphi_1\varphi_2\dot{\varphi}_t}|1\rangle)}{2^{m/2}}$$

再经过一次逆Fourier变换，得到 $|\varphi_1\varphi_2\dots\varphi_t\rangle$ ，再将二进制数转化为十进制数，得到关于 φ 的准确相位。

但是现实往往并非如人所愿， φ 不能表示成二进制数又该怎么办呢？同样的算法是不是也行得通的呢？估计的精度是多少？得到满足要求的结果的概率有多大呢？

考虑对一个任意的 φ 进行逆Fourier变换，

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle\rightarrow\frac{1}{2^m}\sum_{k=0}^{2^m-1}\sum_{j=0}^{2^m-1}e^{2\pi i(k\varphi-kj/2^m)}|j\rangle=\sum_{j=0}^{2^m-1}(\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik(\varphi-j/2^m)}|j\rangle)$$

测量结果为 $|j\rangle$ 的概率为

$$p_j=|\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik(\varphi-j/2^m)}|^2$$

当 φ 正好能被表示成二进制数时，测量出准确结果概率为 1 。但当在更加一般的情况里$p_j\neq1$ ，我们使用等比数列求和公式进行计算

$$p_j=\frac{1}{2^{2m}}|\frac{e^{2\pi i(2^m\varphi-j)}-1}{e^{2\pi i(\varphi-j/2^m)}-1}|^2$$

这下得到正确结果的概率变低，我们试着找一下 p_j 概率的下界，因为这对我们能多大程度上保证估计结果正确有关。假设 $\varphi=\frac{j}{2^m}+\epsilon$,其中 $|\epsilon|\leq2^{-(m+1)}$. 也就是说，测量结果误差在一个量子比特的范围内的概率。

$$p_j=\begin{cases}1 & ,\epsilon=0\\ |\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik(\varphi-j/2^m)}|^2 & ,\epsilon\neq0\end{cases}$$

为了找到 p_j 的下界， 我们对 p_j 的分子分母单独进行变换。

- 分子部分需要找到下界
  令 $a=e^{2\pi i\epsilon2^m}-1$, 这是一个可以被画成如下形式的复数

根据模长与相位的关系，得到 $\frac{2\pi|\epsilon|2^m}{|a|} \leq \frac{\pi}{2}$ 也就是

$$a \geq 4|\epsilon|2^m$$

- 分母部分需要找到上界
  令 $b = e^{2\pi i\epsilon} - 1$ ，如图所示

  我们可以得到 $\frac{2\pi|\epsilon|}{b} \geq 1$,即 $b \leq 2\pi|\epsilon|$

因此我们可以得到一个不出错的下界

$$p_j \geq \frac{4}{\pi^2}$$

相位估计的应用：求阶和质因数分解

目前看来，相位估计本身似乎没有什么用处，我们得到了一个酉变换的相位。这个相位可以拿来做什么呢?

接下来，我们要介绍相位估计的一个大应用和几个小缺点。

数论补充

首先，需要亿点数论知识
假设 $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$, 并且 $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$。

- Euler φ-function:

  $$\varphi(N) = |\mathbb{Z}_N|$$

  函数返回 $1, 2, \ldots, N$ 中与 N互质的元素个数。若 N 为素数，$\varphi(N) = N - 1$.
- Fermat's Little Theorem: 当 $a \in \mathbb{Z}$, p 是素数时，

  $$a^p \equiv a \mod p$$

- Euler Theorem：当 a, N 互质时，

  $$a^{\varphi(N)} \equiv 1 \mod N$$

- Theorem 1:若 x 是

  $$x^2 = 1 \mod N$$

  的非平凡解，则至少在 $\gcd(x-1, N)$ 和 $\gcd(x+1, N)$ 中有一个是 N 的非平凡因子。
- Theorem 2: 若整数 r 使得，

$$a^r = 1 \mod N$$

，则 r 是 a 的阶。

- Theorem 3：整数 $N = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_m^{\alpha m}$ 可以分解成以上形式。若在整数 $[1, N-1]$ 中随机找一个整数 x，且 X 与 N 互质，r 是 x 的阶，则

$$P(r是偶数且x^{\frac{r}{2}} \neq -1 \mod N) \geq 1 - \frac{1}{2^m}$$

背景

求阶：

- 输入： 整数 $N, a \in \mathbb{Z}_N^*$
- 输出： a, N 的阶 r

质因数分解：

- 输入：整数 N
- 输出：整数 N 的因子

求阶

假设 x 是一个整数，N 是一个大于 x 的整数。求阶就是估算如下酉算子的相位

$$U|y\rangle \equiv |xy \mod N\rangle$$

，其中 $x \in (0, N)$， $y \in \{0,1\}^L$。

要怎么做呢？注意到如果这里的 y 是 U 的特征向量，那么我们就可以利用相位估计进行分析

假设 $|u_s\rangle$ 是酉算子 U 的特征向量， $s \in [0, r-1]$

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[\frac{-2\pi i s k}{r}] |x^k \mod N\rangle$$

因为，

$$U|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[\frac{-2\pi i s k}{r}] |x^{k+1} \mod N\rangle$$

$$= \exp[\frac{2\pi i s}{r}] \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[\frac{-2\pi i s (k+1)}{r}] |x^{k+1} \mod N\rangle$$

其中的复指数以 r 为周期，因此

$$= \exp[\frac{2\pi i s}{r}]|u_s\rangle$$

因此进行相位估计，我们可以得到 s/r

质因数分解

质因数分解所需的全部知识就是求阶和数论

- 根据定理1，如果我们能找到 $x^2 = 1 \mod N$ 的非平凡解，那我们至少能在$\gcd(x-1, N)$ 和 $\gcd(x+1, N)$ 中的一个找到 N 的非平凡因子。
- 如果一个与 N 互质的 y 的阶是偶数，那么 $y^{r/2} = x$ 是一个可能的解。

量子搜索

Oracle

假设搜索范围是 $[1, N]$，其中 $N = 2^n$，在搜索范围内有 M 个元素是我们的搜索目标

过程描述

几何分析

性能