**量子计算入门与shor’s algorithm学习**

# 什么是计算？

1. 计算本质是一个物理过程，它必须基于实现计算的物理过程;
2. 计算作为物理系统，其性能被物理规律所限定，计算的时间和空间性能被我们的基本物理规律限定。 计算系统的数学模型为

其中，S是完成计算的物理系统的状态空间，G是系统状态的演化操作空间。

1. 对于时间性能而言，不确定性原理决定了，一个物理可实现的计算系统用于表述不同信息的系统状态之间必须有一个最小距离，等价的，在两个状态之间进行变换的计算过程就是在G空间的一条曲线，其最小曲线长度有一个下线。
2. 对于空间性能而言，我们知道普朗克长度给定了并行的物理比特之间的最小距离，全息原理决定了一个给定三维空间中可以存储的最大信息量正比于这个空间的表面积而非体积，这揭示了我们的物理时空的一个奇怪的性质。
3. 计算复杂度是有物理含义和物理实在性的概念，我们通过不同的计算机构造验证，复杂度不会凭空消失，而只会进行转换，这提醒我们思考量子计算优越性的物理可实现性。

# 量子比特qubit？

比特（Bit）：数学上的 0 或者 1，物理上，一个比特可以被任何一种物理系统所表示，只要这种物理系统总是处在两个不同状态中的一个。常见的例子有：具有正反两面的银币，只有开和关的电子开关，只允许两个不同电压的电路。

计算机是由许多比特组成的，与之相似，量子计算机是由量子比特（Qubit）组成的。像比特一样，量子比特也有状态。比特的状态要么是 0，要么是 1。量子比特的状态却是一个矢量。更准确地说，量子比特的状态是一个存在于二维复矢量空间的矢量。这个矢量空间被叫做状态空间。

物理上，量子比特可以是任何一种双态系统，它拥有两个不同的基态，对应于二维矢量空间中的基矢。比如，电子的自旋，向上或向下。又或者是光子的极化，垂直极化和水平极化。在一个经典的系统中，一个比特必须处在两个状态中的一个，这时100%确定的。然而，量子力学允许量子比特处在一种两个基态的叠加态中，即一个任意二维矢量可以被两个基矢量表示。当您观察量子比特时，结果总是随机的从两个基态种挑选一个，您永远无法预先确定的知道它的结果。**叠加态是量子力学和量子计算的基本性质。[[1]](#footnote-1)**

# 量子比特的任意状态

一般来说，量子态是复矢量，也就是说， 和 为复数。因为量子态是复矢量，更准确的可视化方法是[布洛赫球](https://learn.qiskit.org/course/ch-states/representing-qubit-states#3.-The-Bloch-Sphere-)（Bloch Sphere）。

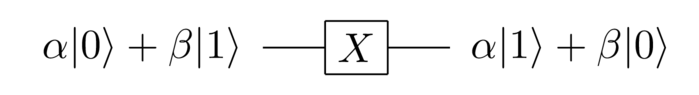
这里有一个限制条件，振幅模的平方和必须等于一，这叫做归一化条件。

一句话总结：一个量子比特的状态用一个存在于二维复矢量空间的单位矢量来表述，这个空间叫做状态空间

# 量子逻辑门

## 量子非门

毫无疑问，量子非门（Quantum NOT Gate）是经典非门的推广。在计算基础状态上测量，模仿经典非门，它将 状态变为 ，反之亦然。



门可以表示为2\*2的矩阵形式：

## 哈达玛门

介绍一个明确涉及量子效应的门，即哈达玛（Hadamard）门。与 门一样，我们将首先解释哈达玛门如何作用于计算基础状态。用  表示该门，这是它的作用：

当然，|0⟩ 和 |1⟩ 并不是唯一的量子态。 哈达玛门如何作用于更一般的量子态？

就像量子非门一样，它是线性的：

门的矩阵形式表示为：

## 通用单量子比特量子门

酉矩阵

矩阵  是幺正矩阵[[2]](#footnote-2)是什么意思？用代数方式回答这个问题最容易，它只是意味着  ，即的共轭转置乘以，等于单位矩阵。

非门是由物理学家 Wolfgang Pauli 在量子力学的早期引入的。他还引入了了另外两个矩阵， 和 ，它们也是有用的量子门。三个门，、 和 统称为泡利矩阵。  和  门将是我们量子门工具包中有用的额外工具；就前面的类比而言，它们扩展了我们可以使用的所有运算。例如，它们在量子隐形传态和量子纠错等协议中至关重要。

门类似于 ，但在非对角线上不是1，而是有 和

  门保持不变，并将 带到  ：

另一个有用的单量子位量子门是  门，它有一个参数  ，表示绕着布洛赫球的  轴旋转的度数。

## 为什么是酉矩阵

事实证明，酉矩阵保留其输入的长度。换句话说，如果我们取任何矢量并计算长度它总是等于原始矢量的长度 。在这方面，它们很像普通（真实）空间中的旋转或反射，它们也不会改变长度。从某种意义上说，酉矩阵是真实旋转和反射的复杂推广。

对于酉矩阵也是正确的，即  对于  维度的任何矢量  为真。

事实上，酉矩阵是唯一能保持矢量长度的矩阵。这就是代数条件  的几何解释（和直观意义）。

**现在让我们证明酉矩阵确实能够保持矢量的长度。**

Proof：主要是计算

请注意，我使用 来表示 的第  个分量，下一步，我们将展开上面的等式，并寻找机会应用  的幺正性。特别地，分量  由 出，对于复共轭项也类似。所以我们可以将上面的等式改写为：

为了利用  的幺正性，我们将把  项移到一起，并以  的形式重写。这给出：

我们交换了第一个  上的  的顺序，以便将其改写为。  指标出现在此等式中的唯一位置是  项。因此，我们可以对  进行求和，这些项变为 ，这只是单位矩阵中的第  项，因为。所以上面的等式变成：

当我们求和时， 当  时，其他情况下它是 0。因此我们可以去一个求和指标，方程简化到

显然，右侧等于  范数的平方。所以我们已经证明了   ，

因此  。这就完成了酉矩阵是长度保持矩阵的证明。

事实上，也可以证明酉矩阵是唯一以这种方式保持长度的矩阵。

**定理：** 让  是一个矩阵。然后    对于所有矢量 当且仅当   是幺正的。

下面是一些新的定义和说明，可以帮助我们进行证明

让我们证明酉矩阵是唯一一种能够保持矢量长度的矩阵。

我们将定义一个新对象，也用  标记，但现在用另一个方向的括号：

也就是说， 是一个行矢量，其条目与 相同，但复共轭。矢量  被称为 ket，并且 被称为 bra，使其成为 bra-ket 或 bracket符号。由理论物理学家保罗·狄拉克 (Paul Dirac) 在 1939 年命名，通常称为狄拉克符号(Dirac Notation)

关于bra 的一个关键事实是它通过匕首操作（共轭转置）与 相关：

另一个有用的恒等式是用狄拉克符号表示的长度：

将其写为：

另一个有用的恒等式：

我将引入一个单位矢量（矢量），表示为 ，意思是在第  个分量为 1，其他地方为 0 的矢量。因此，例如，对于一个量子位：

Proof：

假设我们已经知道  是长度保留的，我们需要分析矩阵乘积  。我们的目标是证明该乘积是单位矩阵，因此   是酉矩阵。为此，我们将首先分析对角元素，并证明它们都等于1。然后我们将注意力转向非对角元素并表明它们都等于 0。

由于  是长度保留的，后者只是 ，即 1。因此我们得出结论，所有对角线元素确实都是 1。

非对角元素呢，即 当 ？我们需要证明这些都等于 0 。

好吧，我们想要做的是以某种方式将  与某个矢量  的长度相关联，然后使用长度保留属性。一种想法是尝试使用，因为这涉及  和  方向。从长度保持属性我们有：

我们还有：

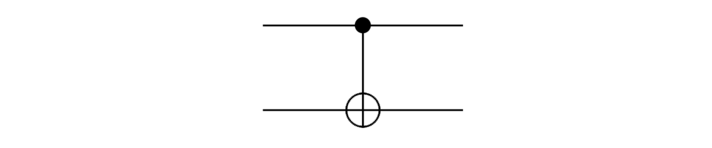
比较两个方程得到：

我们使用将得到：

我们可以把它与前面的方程联立，推导出  当  时，我们得出结论 ，即,  是幺正的。

## 受控非门

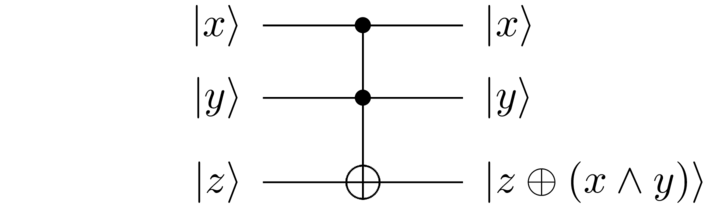
为了计算，我们需要以某种方式让量子位相互影响。也就是说，我们需要涉及两个（或更多）量子位的量子门。这种门的一个例子是受控非门（CNOT Gate）。在量子电路语言中，我们有两条线，代表两个量子位，以及表示 受控非门的符号：



CNOT 门就像量子非门一样，直接受到经典门的启发。它的作用非常简单。如果控制量子位设置为 1，如状态 和 ，则它翻转目标量子位。否则它什么都不做。它在我们拥有的所有四个计算基础状态上的作用分别是：

如果您熟悉经典编程语言，那么您可以将 CNOT 视为一种非常简单的“if-then”语句：“if”设置了控制量子位，“then”翻转目标量子位。虽然简单，但它可以被用来构建其他更复杂的条件行为

Toffoli门

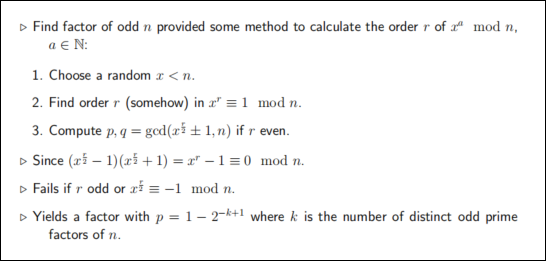


# 量子算法shor’s algorithm

大数质因子分解是当代密码体制的基础。比如常见的RSA加密体系，如果想破解就需要对大数进行质因子分解。对于经典的算法而言，目前最快的算法咋时间复杂度上来讲，需要

这里的n指的是编码这个大数需要的bit数目。很显然这个复杂度是指数级别的，对于经典的图灵机而言不是高效可求解的。

对于经典的求解大数分解的算法，如下



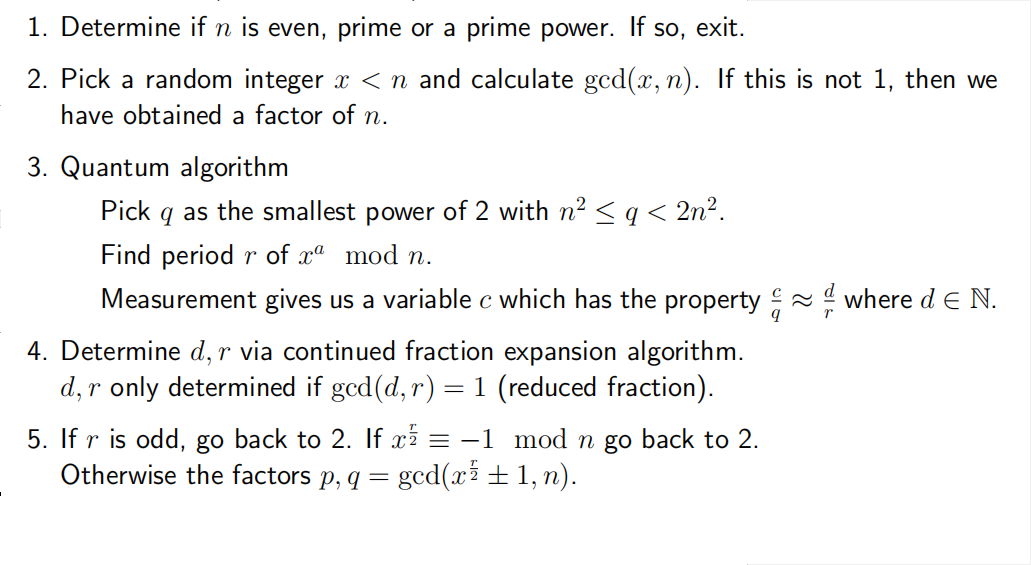
假设我们需要对 进行分解，那么

1. 找一个小于 的数 ，
2. 按顺序寻找一个 使得
3. 如果 是偶数 或 ，则继续寻找

很显然，上述算法需要不断的尝试 ，这种对于不确定的图灵机非常擅长，因为不确定图灵机每次可以同时寻找指数个 ，这样的加速就能抵消该算法的指数复杂度。

引入量子计算shor’s algorithm ：

* 具有多项式复杂度的因式分解算法
* 只能部分地在复杂的量子计算机上运行
* 在经典计算机上的预处理和后处理
* 利用因子分解问题简化为定序问题
* 以量子傅里叶变换的效率实现多项式时间



Shor’s Algorithm 的实验探索

参见：[shor's algorithm.ipynb](https://github.com/Frank2001Feng/project-submit/blob/master/%E9%87%8F%E5%AD%90%E4%BF%A1%E6%81%AF%E5%A4%84%E7%90%86%E4%B8%8E%E5%87%A0%E4%BD%95/shor's%20algorithm.ipynb)

# 课程建议

# 参考文献

[1] J. J. Sakurai Modern Quantum Mechanics

[2] https://learn.qiskit.org/course/ch-algorithms/shors-algorithm#shors-3-0

# 附录：课程学习心得

1. 是被狄拉克发明的ket符号，并在量子力学中被广泛运用。这种符号为量子状态的矢量表示增加了一层额外的抽象[1]。 [↑](#footnote-ref-1)
2. 幺正矩阵也被称为酉矩阵。 [↑](#footnote-ref-2)