3. 量子計算機研究の実験の現状と将来の方向

3.1 概要

Shor によって効率よく素因数分解ができる量子アルゴリズムが発見されて以来、量子計算機というものが注目を浴びている。それでは、素因数分解が実際できて、情報セキュリティの世界に衝撃を与えるような量子計算機は現に存在するのか、もしくは近い将来において実現できるのだろうか。残念ながら量子計算機はまだこれから黎明期を迎えつつあるという段階である。つまり、我々が日常用いているパソコン等の「古典計算機」が AND や OR のゲート素子から始まったように、基本的な量子ゲートを構成、もしくはいくつかのゲートを組合わせて簡単なアルゴリズムを検証しているという段階にある。この時点における量子計算機開発の指導原理とは、理論的に 1 キュービットの位相シフトと 2 キュービットの制御ノットが実現できれば物理的に量子計算機の回路が組める、即ちユニバーサルゲートであることが分かっていることである[35](図 3.1)。

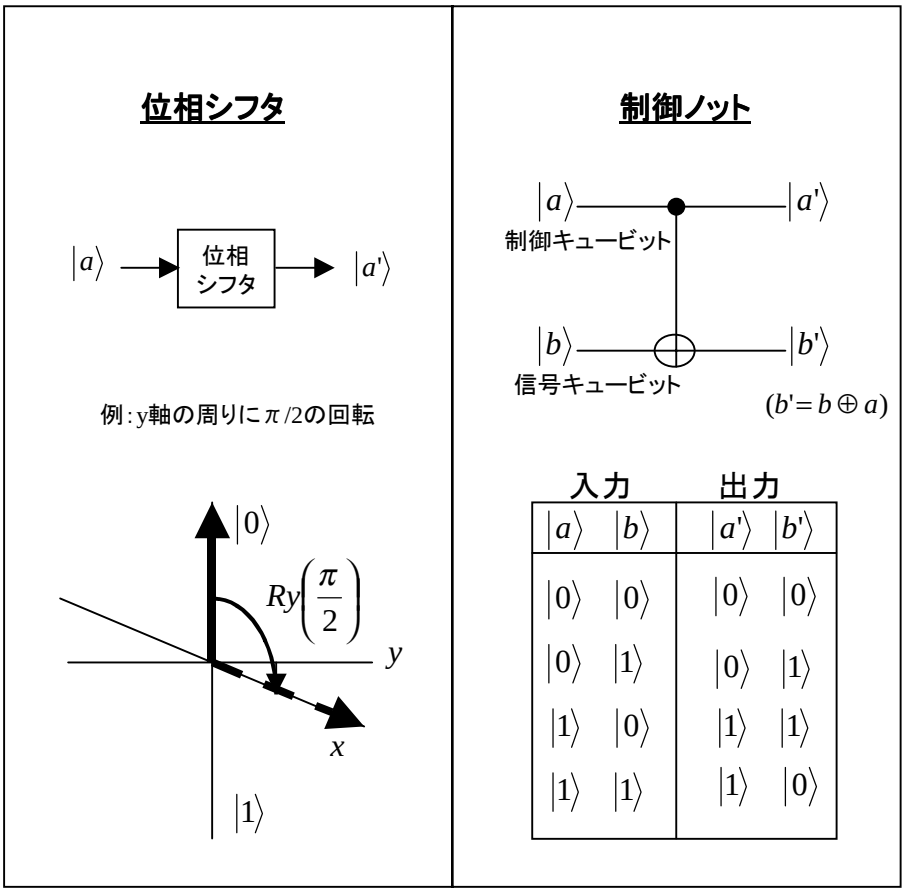

図 3.1 基本量子ゲート

従って、量子計算機を実現するためには、何をキュービットとして用い、どのようにゲートを構成するかを考えればよい。この構成方法により、様々な方式現在考案されている。表 3.1 はそのリストである。

表 3.1　量子計算機リスト（[3]より抜粋）

候補	方式	キュービット	現状	拡張性
線形光学素子[36,37]	弾道	単一	3 キュービットのアルゴリズムが実現	～10 キュービット
NMR 量子計算機[38]	固定	ﾊﾞﾙｸ	3 キュービットのアルゴリズムが実現	～10 キュービット
イオントラップ[39]	固定	単一	2 キュービット間のゲート操作	難
半導体不純物核スピン[44]	固定	単一	アイデアのみ	易
量子ドット(電子準位)[43]	固定	単一	重ね合わせ	易
フォトンロジック[40] (マイクロ波)	弾道	単一	2 キュービット間のゲート操作	難
フォトンロジック (可視)[41]	弾道	単一	制御ノットまであと少し	難
超伝導トンネル接合[42]	固定	単一	重ね合わせ	易

ここで、方式とは、キュービットおよびゲート操作の実現方法の観点からの分類である。大きく「弾道」方式と「固定」方式の 2 つに分類される。

固定型とは、キュービットを担う粒子を固定しておくことに由来する。ゲート操作は、レーザをあてる等の外力を加えることにより実現する。従って、プログラミングはレーザ光の照射順序、組合せにより表現される。これはプログラムの変更が容易にできるという利点を持っている。

弾道型とは、固定型とは逆にキュービット自身が量子計算機の中を移動しながらゲート操作を受けていく、ゲート素子の方が固定されている方式である。従って、プログラムはこのゲート素子の配列で表現される。

また、キュービットの種類で分類することもできる。但し、ここでの種類とは、キュービットが光子か、電子か、原子かという違いで分類するのではなく、キュ

ービットを担う「量子」自体を単一量子にするか、集団的な量子の振る舞いにするかという違いである。これをここでは「単一」と「バルク」と表現する。

このように様々なアイデアが提案されているが、量子計算機としての現状は、それぞれの方式により実現レベルは異なっている。これを簡単に表 3.1 にまとめてある。

量子計算機が現在注目を集めている理由の１つとして、多くの公開鍵暗号の安全性の基になっている因数分解や離散対数問題が簡単にとけるという理論上の成果があるが、これを実際の量子計算機で解くとなると、数キュービットではなく数千キュービットを扱えなければならない。このための拡張性についても、その難易度を表 3.１中に簡単に付した。

次のセクションで各方式の概要を述べる。