概 要

前部の第 9 部で量子論情報論、観測問題の理論的な側面をみてきた。2020 年の現在、量子的な重ね合わせの原理から量子コンピューターの実機が稼働するようになった。デバイスではまだ、課題が多いがソフトウェアとして量子論を扱えるものが増えてきている。Python グループの qutip や Microsoft の Q#などがある。機械学習が AI の進歩が激しく Mathematica や MatLAB なども量子情報を扱うことができるようになってきている。

その中でも IBM の Qisikit は一般端末の PC からクラウドを経由して実機にアクセスできるようになった。今後急速に進歩していくことも予想される。そこで本部では量子論の理論的な課題は第 9 部で考察するとし、とりあえず確率解釈を含む量子原理を認めて、その応用として量子コンピュータを扱う。

本部では本部は未完成部分が多く、今後加筆修正する予定である。参考文献を見て学習に役立ててほしい。

1 量子コンピューター

第 9 部で見たように量子論は観測の問題や相対論との関係など多くの課題を持つが、確率密度の流れとして、解釈し、多くの疑問はとりあえず保留しておいて、現実的な結果を利用していくことで発展してきた分野が量子コンピューターである。

古典的なスーパーコンピューターより、複雑な問題ほど早く結果を出せる可能性があり、近年では IBM や Google 等でその結果が実際に実験できるようになってきた。さらに注目すべきはこれらを扱うソフトウエアは Mathematica や Python などで個人的にシミュレーションできる環境が充実してきたことである。ここでも主目的からそれるようではあるが、応用例をいくつかみて、逆にそこから理論へのフィードバックを見いだし、主目的にせまれるか考察してみたい。まず、量子コンピュータの基礎をしっかりと学ぶ。

1.1 古典的計算機

コンピューターは input と output の関係からできている。古典的な関係を復習しておく。
実際には次のようなトランジスタ MOSFET を利用する。

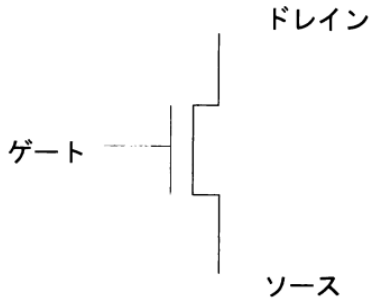


図 1.1: n 型 MOSFET

n 型半導体がソース S とドレイン D にあり、ゲート G には導体がある。
従って DS 間の電流は GS 間の電圧がある閾値を超えた時のみ流れる。
通常は $V_{DS} = 5.0V$ で $V_{GS} = 0.2V_{DS}$ である。

1.1.1 NOT 回路

NOT 回路をこのトランジスタで組むと次のようになる。$|0\rangle$ は電圧が LOW、$|1\rangle$ は HIGH とする。
この例ではあらかじめ V_{DS} は HIGH にしておく。
入力に V_{GS} をあてたので、これが HIGH になると I_{DS} が流れる。従って出力は LOW である。
逆に V_{GS} が LOW であれば I_{DS} は流れない。従って出力は HIGH である。

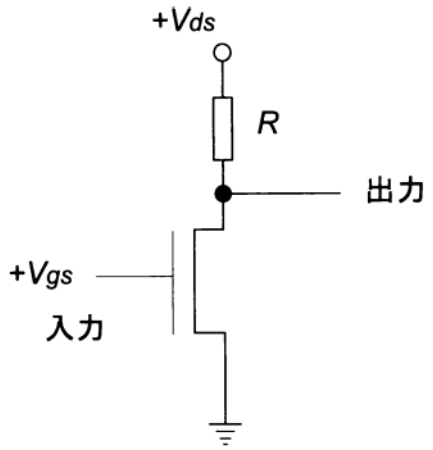


図 1.2: NOT 回路

これは 1 ビットのフリップとみることができる。すなわち

$$|0\rangle \to |1\rangle$$

$$|1\rangle \to |0\rangle$$

となる。

1.1.2 OR 回路

これは 2 ビットから 1 ビットを次のように出力する。すなわち $|1\rangle$ が含まれていれば $|1\rangle$ を出力する。

$$|0\rangle\,|0\rangle \to |0\rangle$$

$$|0\rangle\,|1\rangle \to |1\rangle$$

$$|1\rangle\,|0\rangle \to |1\rangle$$

$$|1\rangle\,|1\rangle \to |1\rangle$$

となる。

1.1.3 NOR 回路

OR の否定をとれば NOR である。これについてトランジスタ回路で表してみよう。

入力を a_i, b_i、出力を c_f とする。この場合はトランジスタを 2 つ並列に利用する。

下図のように a_i, b_i のどちらかが HIGH であれば I_{DS} が流れるので出力 c_f は LOW である。

a_i, b_i のどちらも LOW の時のみ電流 I_{DS} は流れないので c_f は HIGH になる。これを真理値表で表すと下のようになる。

これに NOT 回路を組み合わせれば OR 回路ができる。

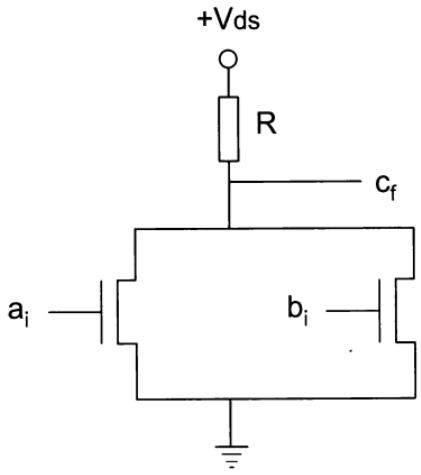


図 1.3: NOR 回路

a_i	b_i	c_f
0	0	1
0	1	0
1	0	0
1	1	0

表 1: NOR 回路の真理値表

1.1.4 AND 回路

これも 2 ビットから 1 ビットを次のように出力する。かけ算を表している。

$$|0\rangle\,|0\rangle \to |0\rangle$$

$$|0\rangle\,|1\rangle \to |0\rangle$$

$$|1\rangle\,|0\rangle \to |0\rangle$$

$$|1\rangle\,|1\rangle \to |1\rangle$$

となる。

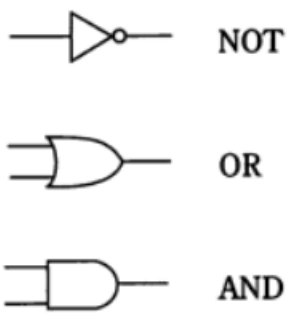


図 1.4: 古典的論理ゲート

1.1.5 NAND 回路

AND を否定した、この例もトランジスタを使って表してみよう。こんどは 2 つのトランジスタを直列に利用する。

下図のように a_i, b_i のどちらかが LOW であれば I_{DS} が流れないので出力 c_f は HIGH である。

a_i, b_i のどちらも HIGH の時のみ電流 I_{DS} は流れるので c_f は LOW になる。これを真理値表で表すと下のようになる。

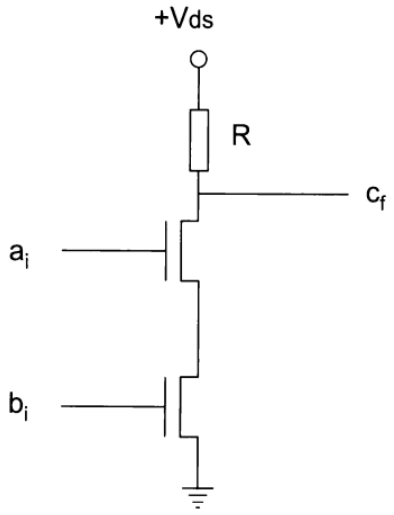


図 1.5: NAND 回路

a_i	b_i	c_f
0	0	1
0	1	1
1	0	1
1	1	0

表 2: NAND 回路の真理値表

1.1.6 XOR 回路

これも 2 ビットから 1 ビットを次のように出力する。異なった積になっているときのみ $|1\rangle$ を出力する。

$$|0\rangle |0\rangle \to |0\rangle$$

$$|0\rangle |1\rangle \to |1\rangle$$

$$|1\rangle |0\rangle \to |1\rangle$$

$$|1\rangle |1\rangle \to |0\rangle$$

となる。この回路は後に重要な役割を果たす。

回路記号では次のように書く。

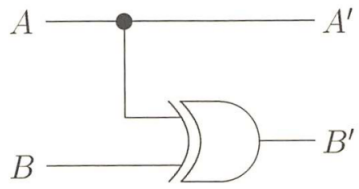
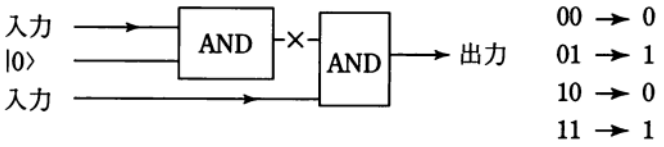


図 1.6: [131] より：XOR 回路

さらに 3 ビットの入力回路を 1 ビット $|0\rangle$ に固定すると、次の図のようになる。
× は NOT が入ることをあらわす。
例えば 1 行目は 00 で 0 になるが反転して 1 と 0 で 10 の AND で 0 になる。
2 行目は同じく 00 で 0 になるが反転して 1 と 1 で 11 の AND で 1 になる。
3 行目は 10 で 0 になるが反転して 1 と 0 の AND で 0 になる。
4 行目では 10 で 0 になり、反転して 1 と 1 の AND で 1 になる。



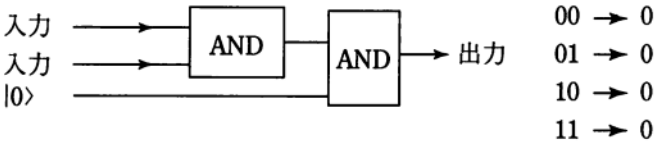
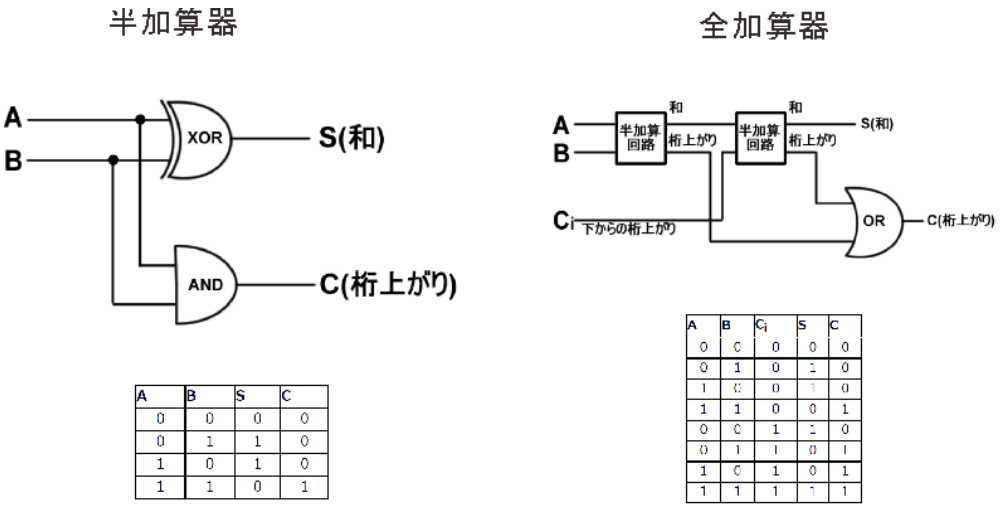


図 1.7: [98] より：AND と NO があればあと 1 つビットを足し、全ての出力が作れる

1.1.7 全加算器と半加算器

論理演算で和をとるとき、桁上げを設けないものが**半加算器**で、桁上げのための bit を追加したものが**全加算器**である。
次に回路記号と真理表を示す。



A	B	S	C
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

A	B	C_i	S	C
0	0	0	0	0
0	1	0	1	0
1	0	0	1	0
1	1	0	0	1
0	0	1	1	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	1

図 1.8: 半加算器と全加算器

1.2 量子計算機 [98]

1.2.1 ユニタリー演算子と複製 [124]

古典情報でればデジタル的に複製をすることができる。では量子状態を複製することを考えよう。
そこで**制御量子ビット (controlled qubit)** を量子ビット C とし、
標的量子ビット (target_quibit) を T とする。
そこでこれらの合成として次のユニタリー演算子を考える。ただしテンソル積 $\otimes$ は省略する。

$$\hat{U}^{(CNOT)} = |0\rangle_C \langle 0|_C (|0\rangle_T \langle 0|_T + |1\rangle_T \langle 1|_T) + |1\rangle_C \langle 1|_C (|1\rangle_T \langle 0|_T + |0\rangle_T \langle 1|_T)$$

これは $|0\rangle\langle 0|$ や $|1\rangle\langle 1|$ が射影演算子であったので $|0\rangle_C \langle 0|_C$ や $|1\rangle_C \langle 1|_C$ は C のヒルベルト空間に射影演算子を作用させ、
T のヒルベルト空間には $|1\rangle_T \langle 0|_T$ や $|0\rangle_T \langle 1|_T$ の単位演算子が作用する。

$$\hat{P}_C = |0\rangle_C \langle 0|_C + |1\rangle_C \langle 1|_C$$

$$\hat{I}_T = |1\rangle_T \langle 0|_T + |0\rangle_T \langle 1|_T$$

C の添え字と T の添え字間は交換する。
この $\hat{U}^{(CNOT)}$ を実装しているデバイスは量子制御ノットゲート (Quantum Not gate) と呼ばれ、
量子計算機 (Quantum computation) の基礎的な素子となっている。
例えば標的ビットの始状態を $|0\rangle_T$ とし、制御ビットの始状態を互いに直交している $|0\rangle_C$ か $|1\rangle_C$ のどちらかにとる。
これに $\hat{U}^{(CNOT)}$ を作用させると

$$\hat{U}^{(CNOT)} |0\rangle_C |0\rangle_T = |0\rangle_C |0\rangle_T$$
$$\hat{U}^{(CNOT)} |1\rangle_C |0\rangle_T = |1\rangle_C |1\rangle_T$$

これで見るように C については保存されて、T の終状態は C の状態と一致する。
これを制御ビットにある古典的な情報を**標的ビットに複製**したとみる。

ただし、これはビット対が増えると指数関数的に**合成ユニタリ演算子**が必要になる。

$$\left(\hat{U}^{(CNOT)}\right)^{\otimes N}$$

この演算子を扱えるコンピューターができれば、
次のように確定的古典情報に対応する N 量子ビット列の複製機をつくることができる。

$$\begin{aligned}\left(\hat{U}^{(CNOT)}\right)^{\otimes N}&\left(|b_1\rangle_{C1}|b_2\rangle_{C2}\cdots|b_N\rangle_{C_N}\right)\left(|0\rangle_{T1}|0\rangle_{T2}\cdots|0\rangle_{T_N}\right)\\&=\left(|b_1\rangle_{C1}|b_2\rangle_{C2}\cdots|b_N\rangle_{C_N}\right)\left(|b_1\rangle_{T1}|b_2\rangle C_{T2}\cdots|b_N\rangle C_{T_N}\right)\end{aligned}$$

これは標的ビット状態 $|0\rangle_{T1}|0\rangle_{T2}\cdots|0\rangle_{T_N}$ が複製機により、2 つの同じ古典ビット列が出力されたことを表している。
しかし、後で示すように、この制御 NOT ゲートに量子的な重ね合わせ

$$|\psi\rangle_C=\alpha|0\rangle_C+\beta|1\rangle_C$$

をいれても**量子複製不可能定理**が働くので

$$\left(\hat{U}^{(CNOT)}\right)|\psi\rangle_C|0\rangle_T=\alpha|0\rangle_C|0\rangle_T+\beta|1\rangle_C|1\rangle_T \tag{1.1}$$

となり、C 状態が保存され、T の終状態は C の状態に一致する。この時、

$$\alpha\beta|0\rangle_C|1\rangle_T$$

のような干渉項が出てこない。面白い l ことに**重ね合わせになる量子状態は複製ができない。**
これは量子力学の観測とユニタリー演算子との操作にある普遍的なことである。

1.2.2 量子複製禁止定理

一般化して**量子複製禁止定理**をみておく。複製の原本を $|\psi\rangle$ に書き込んでおく。
この量子系を S として、複製をつくる量子系を S' とする。そして、コピー機として働くデバイスを含む補助量子系を D とする。
ただし、S と S' の次元は等しく、一方で D はいくらでも大きな次元を持てるとし、マクロな系でもよいとする。
この合成系をヒルベルト空間上に考えて、コピー操作を表す演算子を

$$\hat{U}_{SS'D}$$

とする。合成系 $S'D$ の始状態 $|0\rangle_{S'D}$ には $|\psi\rangle$ は依存しないとする。
仮に複製を実現することを要求すると $|\phi\rangle_D$ を $|\psi\rangle$ に依存してもよい D の純粋状態として

$$\hat{U}_{SS'D}|\psi\rangle_S|0\rangle_{S'D}=|\psi\rangle_S|\psi\rangle_{S'}|\phi\rangle_D$$

という関係が満たされる必要がある。
ここで、直交しない、異なる 2 つの量子状態を $|\psi_1\rangle, |\psi_2\rangle$ とする。この複製をつくると

$$\hat{U}_{SS'D}|\psi_1\rangle_S|0\rangle_{S'D}=|\psi_1\rangle_S|\psi_1\rangle_{S'}|\phi_1\rangle_D \tag{1.2}$$

$$\hat{U}_{SS'D}|\psi_2\rangle_S|0\rangle_{S'D}=|\psi_2\rangle_S|\psi_2\rangle_{S'}|\phi_2\rangle_D \tag{1.3}$$

が成り立つことになるが、$\hat{U}_{SS'D}$ はユニタリだから

$$\hat{I} = \hat{U}^{\dagger}_{SS'D}\hat{U}_{SS'D}$$

が成り立つ。よって $|0\rangle_{S'D}|\psi_2\rangle = |\psi_2\rangle|0\rangle_{S'D}$ だから

$$\begin{aligned}\langle\psi_1|_S\langle 0|_{S'D}\hat{U}^{\dagger}_{SS'D}\hat{U}_{SS'D}|0\rangle_{S'D}|\psi_2\rangle &= \langle\psi_1|\psi_2\rangle \\ &= \langle\psi_1|\psi_2\rangle\end{aligned}$$

が得られるが、一方で 1.2,1.3 より

$$\begin{aligned}\langle\psi_1|_S\langle 0|_{S'D}\hat{U}^{\dagger}_{SS'D}\hat{U}_{SS'D}|\psi_2\rangle|0\rangle_{S'D} &= (\langle\phi_1|_D\langle\psi_1|_{S'}\langle\psi_1|_S)(|\psi_2\rangle_S|\psi_2\rangle_{S'}|\phi_2\rangle_D) \\ &= \langle\psi_1|\psi_2\rangle^2\langle\phi_1|\phi_2\rangle\end{aligned}$$

と表すこともできる。左辺が等しいとすると右辺も等しくなり、

$$\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2\langle\phi_1|\phi_2\rangle$$

となる。両辺を 2 乗すると

$$\langle\psi_1|\psi_2\rangle^2 = \langle\psi_1|\psi_2\rangle^4\langle\phi_1|\phi_2\rangle^2$$

となるので

$$|\langle\psi_1|\psi_2\rangle|^2|\langle\phi_1|\phi_2\rangle|^2 = 1$$

となる。これは量子測定で $\psi_1 \neq \psi_2$ の時に状態の一致はあり得ないという仮定

$$|\langle\psi_1|\psi_2\rangle|^2 < 1$$

を用いると

$$|\langle\phi_1|\phi_2\rangle|^2 > 1$$

となってしまうので矛盾をきたす。

例えば素粒子の散乱で結合定数 g を測定し、決まった粒子の散乱における g を確定する実験をしたとしよう。

量子複製ができるということは 1 回の実験で得たデータからいくつかの g を複製で得て、決定することと、実験を複数回繰り返して、g を決定することが同じになってしまう。

この考察の結果、そのようなことがおこらないということで、実験をごまかせない。

1.2.3 混合状態の複製禁止定理

重要なのは混合状態の場合への拡張である。原本である S の任意の密度行列を $\hat{\rho}$ とする。コピーが作られる S' 側の始状態は $\hat{\rho}$ に依存しない、$\hat{\omega}$ とする。この混合系の始状態は

$$\hat{\rho}_S \otimes \hat{\omega}_{S'}$$

で表す。この状態から $\hat{\rho}$ に依存しない量子操作をしたとして、

$$\hat{\rho}_S \otimes \hat{\omega}_{S'} \to \hat{\rho}_S \otimes \hat{\rho}_{S'}$$

という状態になったとすると、混合状態にコピー機能が存在したことになる。

これは少し、条件を緩和して、複製を定義すると

操作後の状態が S と S' の直積状態 $\hat{\rho}_S \otimes \hat{\rho}_{S'}$ にならなく、$\hat{\Omega}_{SS'}$ になったとするとしても、対角和

$$\hat{\rho}_S = \mathrm{Tr}_S[\hat{\Omega}_{SS'}], \hat{\rho}_{S'} = \mathrm{Tr}_{S'}[\hat{\Omega}_{SS'}] \tag{1.4}$$

が成り立てば密度行列が複製されたことと実質的に同じである。

つまり、S と S' が離れた場所にあって $\hat{\Omega}_{SS'}$ に対して、S と S' の書く領域内の局所的な操作しかできないとすると、

$\hat{\Omega}_{SS'}$ と $\hat{\rho}_S \otimes \hat{\rho}_{S'}$ は原理的に区別できない。

従って、式 1.4 で表される操作は操作後に直積状態 $\hat{\rho}_S \otimes \hat{\rho}_{S'}$ にならなく、$\hat{\Omega}_{SS'}$ になり、

これは広域的に

$$S \to S'$$

の複製がされているので、これを**量子ブロードキャスティング** (quantum broadcasting) という。ただし、

$$\hat{\Omega}_{SS'} = \hat{\rho}_S \otimes \hat{\rho}_{S'}$$

となる場合も特殊例として含むとする。

重要なのは**非可換な 2 つの混合状態を送る量子ブロードキャスティングは不可能**であることである。

これは任意の密度演算子の完全な複製はできないことを示す**複製禁止定理**でもある。

では**近似的にはどうか**という問題がある。次に示すように、**近似的には複製できる**のである。

そこで次の物理操作を考えよう。

$$\hat{\rho}_S \otimes \hat{\omega}_{S'} \to \hat{\Omega}_{SS'}$$

この状態変化において、対環境が入れ替わるので対角和の $S \to S'$ として

$$\hat{\rho}'_S = \mathrm{Tr}_{S'}[\hat{\Omega}'_{SS'}], \hat{\rho}_{S'} = \mathrm{Tr}_S[\hat{\Omega}_{SS'}]$$

これから同じ $\hat{\rho}'$ を作ることはできるが、同じ原本 $\hat{\rho}$ を入力して得られる $\hat{\rho}'$ は

$$\hat{\rho} \neq \hat{\rho}'$$

となり、必ずずれる。そこでこの時の複製忠実度 F を

$$\hat{\rho} = |\psi\rangle \langle\psi|$$

$$F = \langle\psi| \hat{\rho}' |\psi\rangle$$

として定義する。

$\hat{\rho} = \hat{\rho}'$ の時のみ

$$F = \langle\psi| \hat{\rho}' |\psi\rangle = \langle\psi|\psi\rangle \langle\psi|\psi\rangle = 1$$

をとるが、後に示すように近似複製をすると

$$F \leq \frac{2}{3}$$

となる。

1.2.4 ゲートモデル

量子的な演算がユニタリ行列で表されることを見たので、計算機を考える時に大切なのは、はじめをどうするかである。

いつでも初期状態をつくれないと利用価値が下がる。そのためにいつでも全てのビットを

$$|0\rangle$$

にして、これにユニタリ変換 U を施し、測定結果を得る次の図のモデルが基本になる。

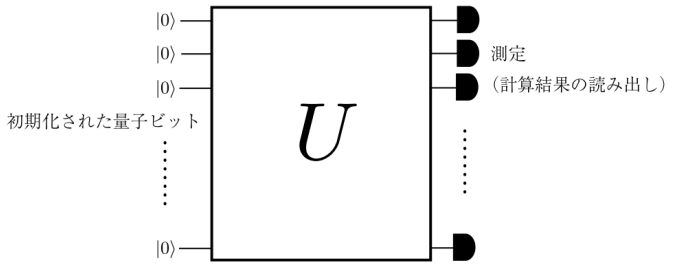


図 1.9: [128] より：量子コンピューター

しかし、これだと巨大なユニタリー行列ができてしまうので現実的ではない。そこでユニタリー変換を

1 つの量子ビットと、2 つの量子ビットのエンタングルメントの状態で 2 量子ビットの**量子ゲート**を定義して 1 つの単位にしてしまう方法が考えられた。このメリットは 1 量子ビットの量子操作と、制御ビットとなる 2 量子ビットの量子操作で、どんな複雑な計算もこなせることになる。特に有限個のゲートで任意の量子計算ができるようなものに現在次のようなものが見つかっている。

詳しくは次節でみるがこれらは**ユニバーサルゲート集合** (universal_gete_set) と呼ばれる。

- 1 量子ビットとエンタングルド (2 量子ビット）
- Hadamard ゲート、フェーズゲート、$\pi/8$ ゲートと CNOT ゲート
- Toffoi ゲート (3 量子ビットゲート) と Hadamard ゲート

次に巨大なユニタリー変換を分解する例として**量子アルゴリズム**が必要になる。

例えば素因数分解を高速にする **Shor のアルゴリズム**の例が次の表になる。

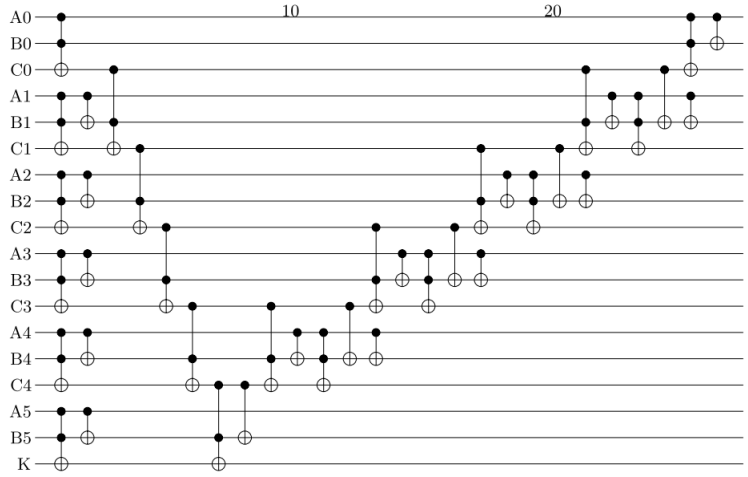


図 1.10: [128] より：量子計算回路の例

1.2.5 量子誤り訂正

古典的なコンピュータでも 1 ビットの情報を正確に保持していくかを判断するためにいくつかの情報を付加してセットにするロジカルビットという処理をさせることがある。この量子版を考えておこう。

ここには量子論独特の方法が必要になる。なぜなら、量子的な情報は直接観測できない。前章で見たきたようにこれをするとその情報が壊れてしまうのである。

そこで次の図のように、射影空間でその成分変化を見ようというわけである。本来のベクトル $|\psi\rangle$ が誤りを含み $|\psi'\rangle$ にわずかに変化したとする。

量子情報を表すベクトルがヒルベルト空間でユニタリ変換により回転したので、本来あるべき状態がわかっていれば

$$1 - |\langle\psi'|\psi\rangle|^2$$

の確率で間違った状態へ変化する。これは状態の中身を見ないで得られるので、

この測定を**誤り兆候測定** (error_syndorome_mesurement) という。

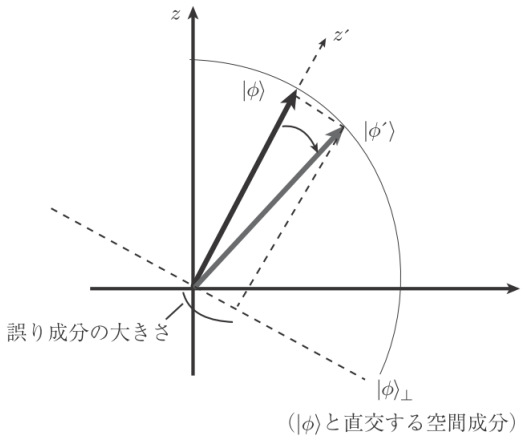


図 1.11: [128] より：状態ベクトルの誤り成分による回転

この補正をして、1 量子ビットを守るには最低でも回転と並進の自由度分の 5 量子ビットが必要になる。

ここでは単純化して、1 つの方向成分のみを扱うことにする。

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

とすると状態ベクトルの変化 $|0\rangle \to |1\rangle$ の回転を σ_x、位相の回転を σ_y が担うとし、ここでは σ_x の方向のずれのみを直すことを考えよう。これは古典的な **Hamming 符号**と同じで次のように 3 つの量子ビットを用いる。

$$\alpha\,|0\rangle + \beta\,|1\rangle \to \alpha\,|000\rangle + \beta\,|111\rangle$$

これは次の図のように制御 NOT と呼ばれる方法と同じなる。

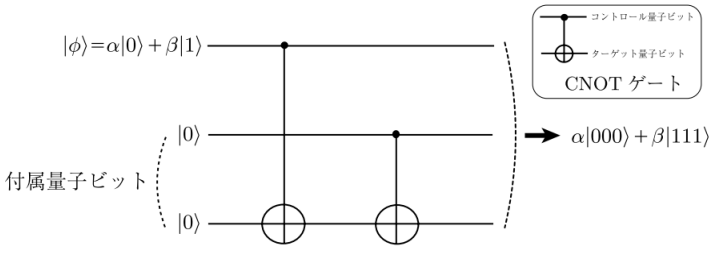


図 1.12: [128] より：3 量子ビットの誤り訂正

まず、1 つめの量子ビットがずれた場合を見ていく。σ_x によるずれは x 軸の回転であるから、この回転角を θ_1 とすると

$$\alpha\,|0\rangle + \beta\,|1\rangle \to \cos\theta_1\,(\alpha\,|0\rangle + \beta\,|1\rangle) + i\sin\theta_1\,(\alpha\,|1\rangle + \beta\,|0\rangle)$$

先の回転図のように回転したので y 成分にはじめには見えていない直交成分が見えてくることに留意する。
これを 1 番目の量子ビットにあてはめると

$$\alpha|000\rangle + \beta|111\rangle \to \cos\theta_1 (\alpha|000\rangle + \beta|111\rangle) + i\sin\theta_1 (\alpha|100\rangle + \beta|011\rangle) \tag{1.5}$$

次に 2 番目の量子ビットに回転 θ_2 のずれを生じさせると

$$\begin{aligned}\alpha|000\rangle + \beta|111\rangle \to &\cos\theta_1\cos\theta_2 (\alpha|000\rangle + \beta|111\rangle)\\ &+ i\cos\theta_1\sin\theta_2 (\alpha|010\rangle + \beta|101\rangle)\\ &+ i\sin\theta_1\cos\theta_2 (\alpha|100\rangle + \beta|011\rangle)\\ &+ i\sin\theta_1\sin\theta_2 (\alpha|110\rangle + \beta|001\rangle)\end{aligned} \tag{1.6}$$

となり、これは 1 行目が正しい状態、2，3 行目が 1 つのビットが反転した誤りの状態、4 行目は 2 つのビットが反転した誤りの状態を表している。
よって式 1.5 の第 2 項以後の大きさをとれば、これが、誤りベクトル成分の大きさになる。これを p_e とすると

$$|p_e|^2 = |i\sin\theta_1|^2$$

である。
同様にして 3 つめのビットにも同じことをすると式 1.6 の第 1 項に対応する正しい状態の成分が

$$\cos\theta_1\cos\theta_2\cos\theta_3$$

となる。量子ビットの誤りは反転することに等しいので、まとめると次のようになる。
1. 正しい状態：

$$\alpha|000\rangle + \beta|111\rangle$$

2. 量子ビット 1 つが反転した状態：確率は p_e

$$\alpha|100\rangle + \beta|011\rangle$$

$$\alpha|010\rangle + \beta|101\rangle$$

$$\alpha|001\rangle + \beta|110\rangle$$

3. 量子ビット 2 つが反転した状態：確率は p_e^2

$$\alpha|110\rangle + \beta|001\rangle$$

$$\alpha|101\rangle + \beta|010\rangle$$

$$\alpha|011\rangle + \beta|100\rangle$$

4. 量子ビット 2 つが反転した状態：確率は p_e^3

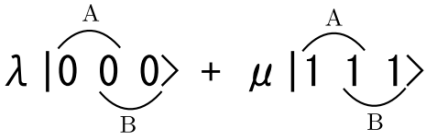
$$\alpha|111\rangle + \beta|000\rangle$$

誤り確率 p_e が小さければ p_e^2, p_e^3 は無視できる。

1.2.6 パリティチェック

古典的に信号の正誤チェックをパリティで行うことがよく用いられたのでここでもそれを利用する。

ここでは p_e と p_e^2 が区別できる測定をしたとして、次の図のように 1,2 番目の量子ビットと、2,3 番目の量子ビットのパリティを測定することを考える。状態を符号化して、A のパリティを測るために**付属量子ビット (ancilla_qubit)** を 1 つ初期状態に用意する。このビットのみを注目して、パリティを測る。



A: 量子ビット 1，2 のパリティ
B: 量子ビット 2，3 のパリティ

図 1.13: [128] より：量子ビットのパリティ

量子計算機をつくろうとすると、状態を反転させる NOT 演算子がユニタリー性によく合う。

そこで制御 NOT(controlled-Not_gate) をが古典計算機の XOR に対応した 2 キュービットゲートで次のように定義する。

これは 1 であれば付属量子ビットを反転する。$CNOT_n$ の添え字 n でペアになっている 1，2 番目に作用させるとして

パリティが偶の場合

$$(\alpha|00\rangle+\beta|11\rangle)|0\rangle \xrightarrow{CNOT_1} \alpha|00\rangle|0\rangle+\beta|11\rangle|1\rangle \xrightarrow{CNOT_2} (\alpha|00\rangle+\beta|11\rangle)|0\rangle \tag{1.7}$$

1 回目で量子ビットに CNOT を作用させて、第 2 項の付属量子ビットは $|0\rangle \to |1\rangle$ に反転するが、
2 回目の量子ビットに CNOT を作用させた時に第 2 項の付属量子ビットは $|1\rangle \to |0\rangle$ で元に戻る。

パリティが奇の場合

$$(\alpha|10\rangle+\beta|01\rangle)|0\rangle \xrightarrow{CNOT_1} \alpha|10\rangle|1\rangle+\beta|01\rangle|0\rangle \xrightarrow{CNOT_2} (\alpha|10\rangle+\beta|01\rangle)|1\rangle \tag{1.8}$$

1 回目で量子ビットに CNOT を作用させて、第 1 項の付属量子ビットは $|0\rangle \to |1\rangle$ に反転し、
2 回目の量子ビットに CNOT を作用させた時に第 2 項の付属量子ビットも $|0\rangle \to |1\rangle$ に反転する。
よって付属ビットを見て、**測定結果が 0 であれば偶パリティ、1 であれば奇パリティ**となる。

これを 1 番目だけでなく 2，3 番目にも施すとパリティが 2 つなので全部で 4 つの測定パターンが、付属ビットに対して次のように出てくる。

$$0,0 \to \alpha|000\rangle+\beta|111\rangle$$

$$1,0 \to \alpha|100\rangle+\beta|011\rangle$$
$$1,1 \to \alpha|010\rangle+\beta|101\rangle$$
$$0,1 \to \alpha|001\rangle+\beta|110\rangle$$

つまり、4 つの状態がパリティチェックで区別できる。付属量子ビットの測定結果が 0,1 であれば、上式の 4 行目のように

3 番目の量子ビットに反転操作である**ビットフリップゲート**をかけて誤りが訂正できる。

同様に結果が 1,1 であれば 2 番目、1,0 であれば 1 番目をビットフリップすれば訂正ができる便利な方法である。

これを次の図で表す。これは**量子回路**と呼ばれ、ゲートがつきた時に終了になるとする。
量子回路は時間の流れを左から右とする。

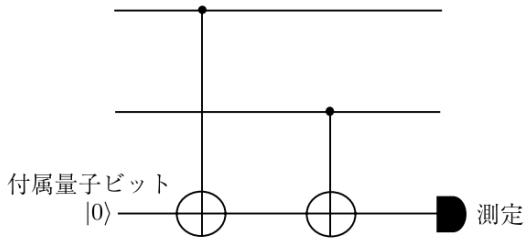


図 1.14: パリティチェックの量子回路

このように 2 進法のビットで補正をするときにはビットフリップの単純操作になるので便利である。
ただし、はじめに指摘したように、さらにもう一つの向きである位相方向のエラーをここでは考えなかった。
これもビット操作として**位相フリップエラー**と呼ばれるエラーに対して補正をすればよい。
これは σ_x の固有状態である $|+\rangle, |-\rangle$ を反転させるエラーと考えて同じように扱うことができ、これらは**Shor の誤り符号補正**として知られている。

1.2.7 量子制御

前節の内容を一般的にして、より複雑な量子回路を扱えるために次のように改めて定義する。
次の図にあるように 2 つの入力ビットのうち 1 方を**制御ビット** (control_bit)、
他方を**標的ビット** (target_bit) という。
制御ビットには • がつけられている。図左から入力され、図右に出力される。
このような図を**量子回路図**という。
時間の流れは左から右向きで、縦の線がビット数に対応する。

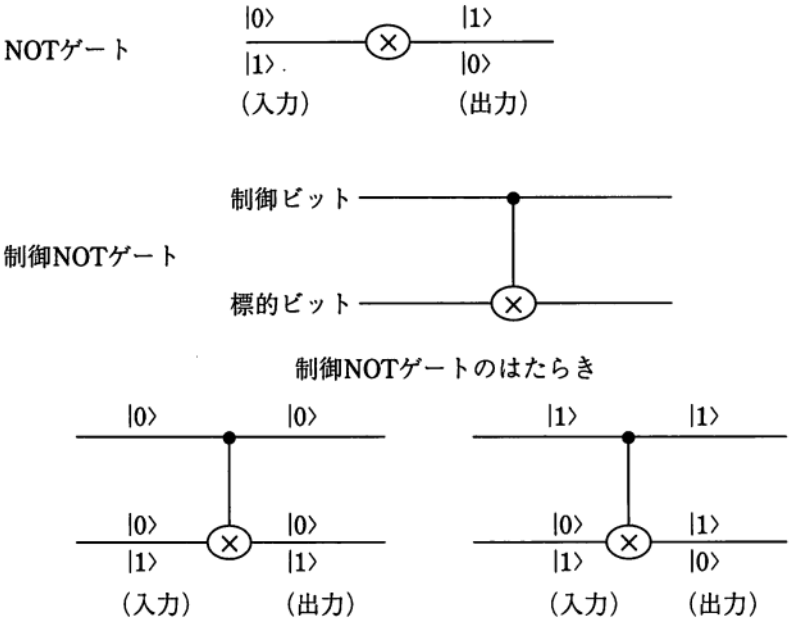


図 2.3 制御 NOT ゲート.

図 1.15: [98] より：制御 NOT ゲート

制御ビットが $|0\rangle$ の時には標的ビットに遷移はおこらない。制御ビットが $|1\rangle$ の時には NOT ゲートとして働く。

これは制御ビット、標的ビットを $|a\rangle, |b\rangle$ の時に標的ビットに

$$|a + b \, mod \, 2\rangle \tag{1.9}$$

が現れる。従って古典計算機の XOR に対応する。

これが重要なのはこの**制御 NOT と 1 ビットのユニタリー変換の組み合わせで全てのユニタリー変換が実行できる**ことである。

この詳しい証明は後節で見る。

図の横線が古典チューリングマシンの 1 マスに相当し、量子では $|0\rangle$ と $|1\rangle$ の重ね合わせで **qubit** を表す。

縦線はゲートと呼ばれ、qbit 間の相互作用を表す。ゲートを通過すると何らかのユニタリー変換を qbit が受けることになる。

従って次のような 1 つ飛びの制御 NOT ゲートは複数の制御 NOT ゲートの組み合わせと同等である。

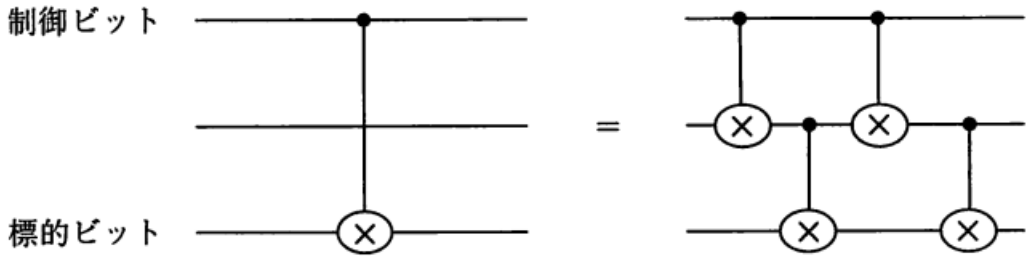


図 1.16: [98] より：1 つ飛びの制御 NOT ゲート

右の回路では左から右に読むのではじめに制御 NOT を作り、3 番目の bit にコピーする。

次に 2 番目を制御 NOT で元に戻す。

改めて、2 番目と 3 番目で制御 NOT をつくる。

制御ビットと標的ビットのテンソル積を次で表す。

$$|0\rangle |0\rangle \rightarrow^t (1000)$$

$$|0\rangle |1\rangle \rightarrow^t (0100)$$

$$|1\rangle |0\rangle \rightarrow^t (0010)$$

$$|1\rangle |1\rangle \rightarrow^t (0001) \tag{1.10}$$

ここでは基底ベクトルのように考えればよい。

制御ビットが $|0\rangle$ の場合を行列の 1,2 行、1,2 列で表し、制御ビットが $|1\rangle$ の場合を行列の 3,4 行、3,4 列で表すと

制御 NOT を表す行列を A は次を満たす。

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

つまり対角の 2×2 の部分行列は制御ビット $|0\rangle$ に対応し、単位行列になるが、下部分の 2×2 の部分行列は反転の行列になる。

この行列が可逆になることに留意する。

制御ビットと標的ビットを $|0\rangle$ に作用させた場合の式

$$|a\rangle\,|b\rangle\,|0\rangle \to |a\rangle\,|b\rangle\,|a+b \mod 2\rangle \tag{1.11}$$

これを量子回路で書くと次のようになる。

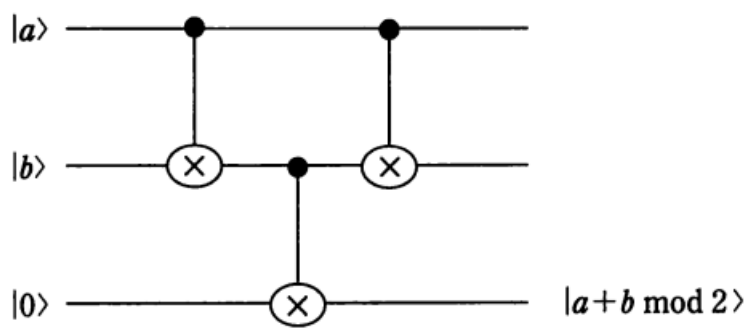


図 1.17: [98] より：$|a+b\,mod\,2\rangle$ をつくる回路

具体的に

$$\begin{aligned}
|0\rangle\,|0\rangle\,|0\rangle &\to |0\rangle\,|0\rangle\,|0+0 \mod 2\rangle = |0\rangle\,|0\rangle\,|0\rangle \\
|0\rangle\,|1\rangle\,|0\rangle &\to |0\rangle\,|1\rangle\,|0+1 \mod 2\rangle = |0\rangle\,|0\rangle\,|1\rangle \\
|1\rangle\,|0\rangle\,|0\rangle &\to |1\rangle\,|0\rangle\,|1+0 \mod 2\rangle = |1\rangle\,|0\rangle\,|1\rangle \\
|1\rangle\,|1\rangle\,|0\rangle &\to |1\rangle\,|1\rangle\,|1+1 \mod 2\rangle = |1\rangle\,|0\rangle\,|0\rangle
\end{aligned}$$

1.2.8 量子複製不可能定理

量子情報は観測の原理から極めて特徴のある**量子複製不可能定理** (no_cloning_thorem) がある。

前節の制御 NOT は古典的にはターゲットを $|0\rangle$ に固定した時、制御ビットが $|0\rangle$ であれば出力は標的ビットが $|0\rangle$ になり、制御ビットが $|1\rangle$ であれば出力は標的ビットが $|1\rangle$ になる。これは 1 つのコピーと考えることとができる。

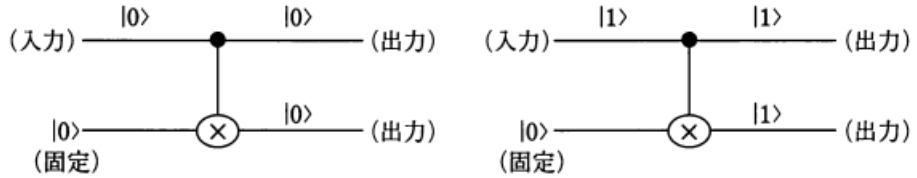


図 1.18: [98] より：制御 NOT によるコピー

しかし、重ね合わせの状態をコピーすることができない。

背理法で証明する。

コピーができるとすると独立な $|a\rangle, |b\rangle$ について制御ビットを標準ビットへコピーする作用 C を

$$C\,|a\rangle\,|0\rangle = |a\rangle\,|a\rangle$$

$$C\left|b\right\rangle\left|0\right\rangle = \left|b\right\rangle\left|b\right\rangle$$

とする。これを重ね合わせに適応すると $\alpha \neq 0, \beta \neq 0$ として

$$C\left(\alpha\left|a\right\rangle + \beta\left|b\right\rangle\right)\left|0\right\rangle = \alpha\left|a\right\rangle\left|a\right\rangle + \beta\left|b\right\rangle\left|b\right\rangle$$

となるが $\alpha\left|a\right\rangle + \beta\left|b\right\rangle$ の複製は

$$\left(\alpha\left|a\right\rangle + \beta\left|b\right\rangle\right)\left(\alpha\left|a\right\rangle + \beta\left|b\right\rangle\right) = \alpha^2\left|a\right\rangle\left|a\right\rangle + \beta^2\left|b\right\rangle\left|b\right\rangle + \alpha\beta\left|a\right\rangle\left|b\right\rangle + \beta\alpha\left|b\right\rangle\left|a\right\rangle$$

となるべきで、これは

$$\alpha = 1, \beta = 0 \ or \ \alpha = 0, \beta = 1$$

の場合でしか成立しない。この場合ははじめに重ね合わせに状態にあることに矛盾している。

1.2.9 量子チューリングマシン

量子計算は任意の SU(2) 行列 U に対して制御 NOT が 2 個と 1qbit の 3 個のユニタリー行列 A, B, C を持ってくれば下図にあるような一般的な制御-U ゲートを作ることができる。
これは制御ビットが $|1\rangle$ の時のみに標的ビットが変換を受ける量子論理ゲートである。

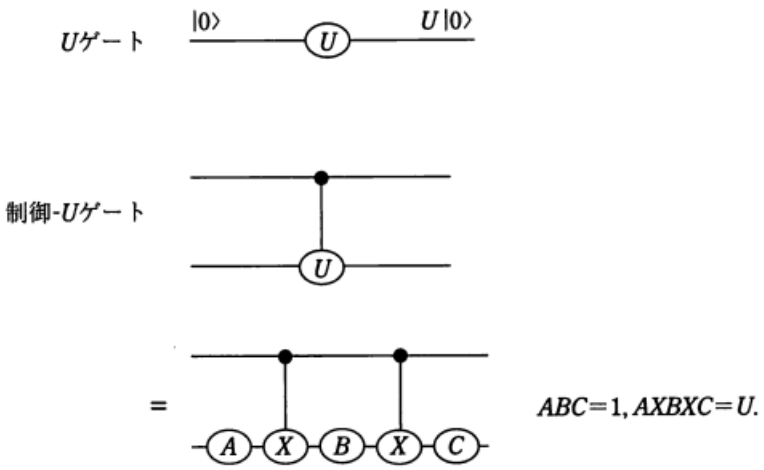


図 1.19: [98] より：U ゲートと制御 U ゲート

ただし、NOT ゲートは $\left|0\right\rangle, \left|1\right\rangle$ の基底ではパウリ行列

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

であり、

$$ABC = 1$$

$$AXBXC = U$$

となるように選ぶ。すると U は次のように z 軸、y 軸、z 軸での連続回転に対応し

$$U = R_z(\alpha)R_y(\beta)R_z(\gamma)$$

とえらび、例えば

$$A = R_z\left(\frac{\alpha-\gamma}{2}\right)$$

$$B = R_z\left(-\frac{\alpha+\gamma}{2}\right) R_y\left(-\frac{\beta}{2}\right)$$

$$C = R_y\left(\frac{\beta}{2}\right) R_z\left(\gamma\right)$$

と選べばよい。
1 ビットのユニタリー変換と 2 ビットの CNOT で任意のユニタリー変換をつくることができる。
これから量子万能コンピューター（チューリングマシン）ができあがる。
次節で詳しく見る。

1.2.10 基本回路 [131]

はじめに、今後利用する量子回路素子が文献 [130] でまとめられているので引用する。

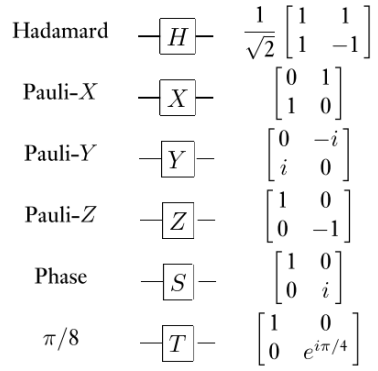


図 1.20: [130] より：回路記号 1

回路記号と行列表示の続き

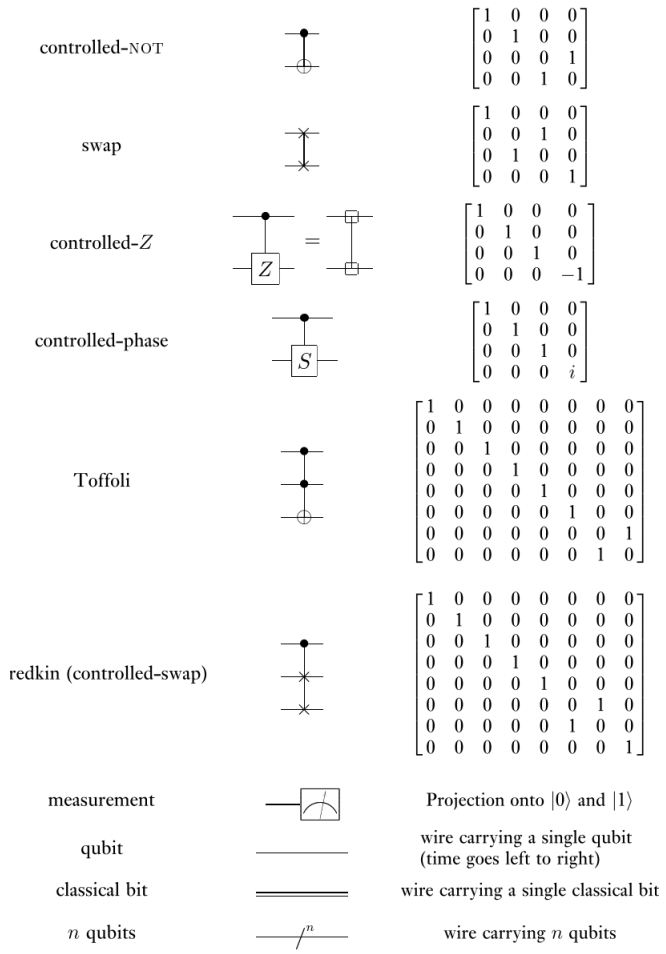


図 1.21: [130] より：回路記号 2

1.2.11 qubit[130]

前章の式から改めて量子情報の基本単位になる **qubit** と呼ばれる 1 ビットの量子的な重ね合わせを

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

で定義する。基底ベクトルは直交しているとする。大きさは 1 として

$$|\alpha|^2 + |\beta|^2 = 1$$

であるとする。
例えば、次のような qbit の状態が考えられる。

$$\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

この場合は 0 または 1 が得られる確率が共に 50%になる。
具体的には次の図のように 2 状態の原子モデルで基底状態と励起状態がそれぞれ $|0\rangle$ と $|1\rangle$ に対応する。

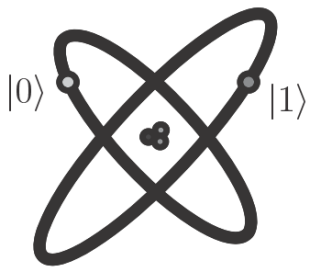


図 1.22: [130] より:2 準位状態のある原子

このベクトルの大きさは 1 であるが、次の図のように 3 次元空間では回転の 2 つの自由度がある。
一般には次のように位相項をかけて表すことができる。

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

だだし、後節で議論するが大局的にかかる位相 γ は観測値に影響を与えないのでここでは無視する。
または常に

$$\gamma = 0$$

を選択していると考えてよい。
従って次のように状態ベクトルを表すことができる。

$$|\psi\rangle\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

このような重ね合わせの状態は **SuperPosition** と呼ばれる。
これを表したのが前章でも扱った下図の**ブロッホ球**である。

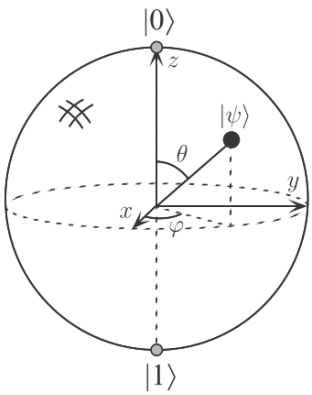


図 1.23: [130] より:ブロッホ球

この $|1\rangle, |0\rangle$ の重ね合わせを表すベクトルは **qubit** と呼ばれ、ブロッホ球の表面に無限につくることができる。

しかし、前章でみたようにいったん観測が行われると 1 か 0 しかとらない。前章で議論したように、観測により情報を失う。

つまり、位相情報は消えてスカラー値を実軸上に得るわけである。

ただし、図の $|0\rangle$ と $|1\rangle$ は π **離れて直交**している。

$$|0\rangle \neq -|1\rangle$$

のように結ばれないので注意する。

1.3 基本ゲート [130]

基本的に量子ゲートは入力状態に時間の進行に伴う演算子を作用して出力状態を得ることである。従って、量子コンピューターでも今のところ時間の進みは順方向のみを考える。

$$\Delta E \cdot \Delta t \geq \hbar$$

が効いてくるような短い時間は考えない。
これまでみてきたように 1bit は

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

から重ね合わせ

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

を基本として、α, β は複素数とする。

1.3.1 位相ゲート

例えば状態ベクトルの時間変化をユニタリ演算子

$$U \equiv \begin{pmatrix} \langle 0|\,U\,|0\rangle & \langle 0|\,U\,|1\rangle \\ \langle 1|\,U\,|0\rangle & \langle 1|\,U\,|1\rangle \end{pmatrix}$$

を用いて一般に

$$|\psi\rangle_{IN} = U\,|\psi\rangle_{OUT}$$

のようにかける。
これから

$$U\,|\psi\rangle = (\langle 0|\,U\,|0\rangle\,\alpha + \langle 0|\,U\,|1\rangle\,\beta)\,|0\rangle + (\langle 1|\,U\,|0\rangle\,\alpha + \langle 1|\,U\,|1\rangle\,\beta)\,|1\rangle$$

のように展開ができる。以前用いた

$$U = |0\rangle\,\langle 0| + e^{i\phi}\,|1\rangle\,\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

とすると、これは次のように作用した。

$$U\,|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$U\,|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\phi} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\phi}\,|1\rangle$$

これからそれぞれの固有値が $1, e^{i\phi}$ であることがわかる。さらにこのユニタリ演算子 U は
状態ベクトルの位相をグローバルに変化させる。例えば

$$|+\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle)$$

を考え、これに U を作用させると

$$U\left(\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right)=\frac{1}{\sqrt{2}}\left(|0\rangle+e^{i\phi}|1\rangle\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ e^{i\phi}\end{pmatrix}$$

となる。
そこで次を**位相ゲート** (phase_gate) という。

$$U(\phi)=\begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix} \tag{1.12}$$

1.3.2 NOT ゲート

さらにすでに登場しているものに**否定ゲート** (NOT_gate)

$$U_{NOT}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

これによって次のように状態は入れ替わる。

$$U_{NOT}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}\beta\\ \alpha\end{pmatrix}$$

恒等変換も 1 つの重要なゲートになる。

$$U_I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

これらはユニタリである。

1.3.3 Z ゲート

ブロッホ球状でのユニタリ変換は他にもいくつかあり、
例えば **Z ゲート** (z_gate) として次を定義する。これはパウリ行列 σ_z である。

$$Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \tag{1.13}$$

これはブロッホ球上で、$|0\rangle$ 成分は変えないで、$|1\rangle$ 成分は反転させる。

1.3.4 ハダマールゲート

量子コンピューターで重要なのは重ね合わせをつくるハダマールゲート H である。
次の図のように y 軸回転を加えて**ハダマールゲート** (Hadamard_gate) を次で定義する。

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{1.14}$$

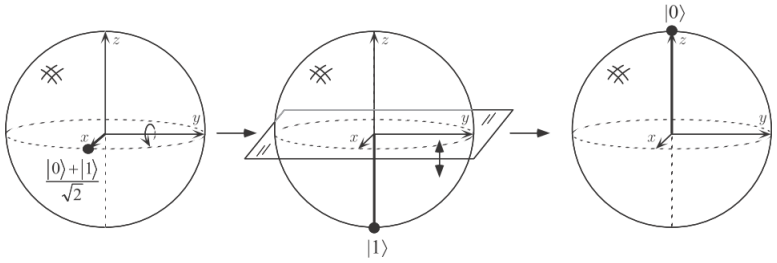


図 1.24: [130] より:ブロッホ球状での y 軸回転と z 軸反転でハダマールゲートをつくる

このゲートははじめの列で $|0\rangle$ ベクトルを

$$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

として、$|0\rangle$ と $|1\rangle$ の間の状態をつくり、次に 2 番目の列で

$$|1\rangle \to \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

つまり、

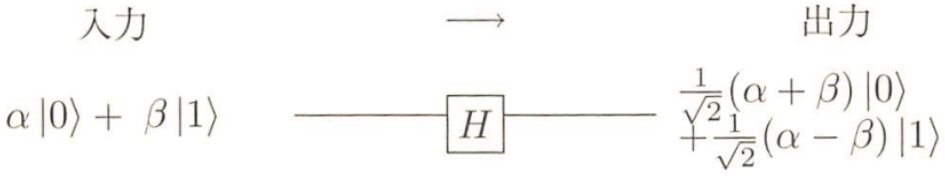


図 1.25: [131] より:ハダマールゲートは和と差を作る

このハダマール演算子は

$$H^2 = I$$

という関係があるので 2 回作用させると元にもどる。つまり、密度行列を同じような作用をする。

1.4 論理ゲート

3 つの基本ゲート X, Z, H は**ロジックゲート** (logic_gate) と呼ばれ次の図のようになる。

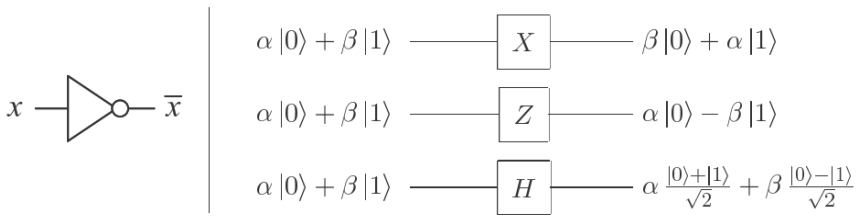


図 1.26: [130] より:基本的な論理ゲート X,Z,H

例えばはじめに扱ったシュテルン・ゲルラッハの実験では次の図のように

$$|0\rangle \to HSTH \to \left(\frac{1}{2} - \frac{1}{2}e^{\frac{3\pi i}{4}}\right)|0\rangle + \left(\frac{1}{2} + \frac{1}{2}e^{\frac{3\pi i}{4}}\right)|1\rangle$$

となるので $|0\rangle$ の期待値は 85.3%、$|1\rangle$ は14.7%となる。

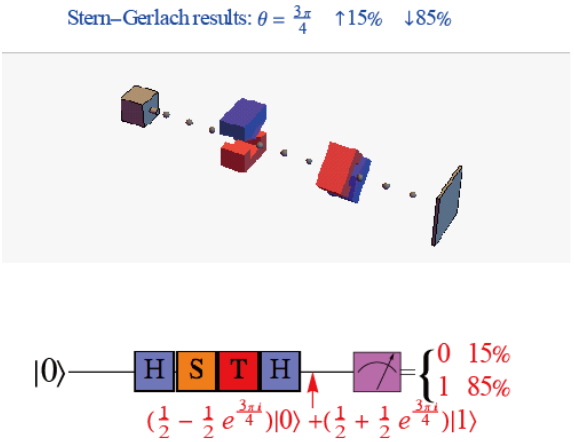


図 1.27: S. M. Blinder より：シュテルンゲルラッハの実験

そこで一般に単一 quibit の変換 U を表すことを考えると。実数 $\alpha, \beta, \gamma, \delta$ の 4 つを使って次のような回転演算子で表すことができる。α は大局的な位相変換で、γ は y 軸の任意の回転、β, δ は z 軸の任意の回転である。

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

これは一般的に角運動量で扱ったスピン演算子で一般には次のようにパウリ行列で書くことができた

$$D_j^s(\alpha) = \cos(\alpha/2) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} - i\sin(\alpha/2)\,\sigma_j$$

具体的に x, y, z 軸周りの回転は

$$D_x^s(\alpha) = \begin{pmatrix} \cos\frac{\alpha}{2} & -i\sin\frac{\alpha}{2} \\ -i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$

$$D_y^s(\alpha) = \begin{pmatrix} \cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$

$$D_z^s(\alpha) = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix}$$

これらから次が導ける。

$$D_y^s(\pi/2)\,\sigma_z D_y^s(\pi/2) = \sigma_x$$

$$D_y^s(\pi/2)\,\sigma_z = H$$

$$D_y^s(-\pi/2)\,\sigma_z = H$$

1.4.1 制御 NOT ゲート

前節でみた**制御 NOT ゲート** (CNOT ゲート) は入力 A, B, 出力を A', B' とすると

$$A' = A$$
$$B' = A \oplus B$$

となった。つまり、A' については A がそのまま出力され、B' は $A=0$ の時に B をそのまま、$A=1$ の時に $\bar{B}$ が出力される。

B' は XOR と同じである。回路記号と真理表は次のようになる。

A	B	A'	B'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

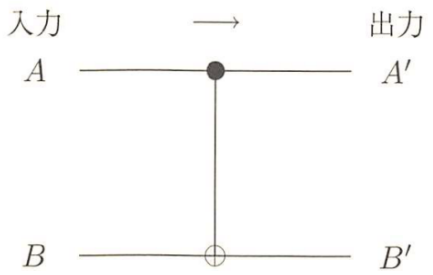
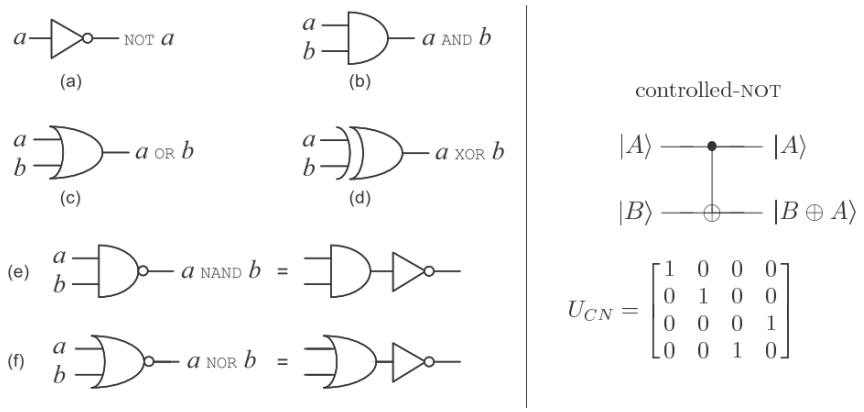


図 1.28: [131] より CNOT ゲート

これらの回路記号と、CNOT の行列表示 U_{CN} を次に示す。

CNOT はターゲットビットに XOR をつくる。

これから CNOT は一般化 XOR ゲート (general) とみなすことができる。



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

図 1.29: [130] より

確率を保存するために U_{CN} はユニタリであることが確かめられる。

$$U_{CN}^{\dagger} U_{CN} = I$$

この CNOT の性質は後に重要な役割をする。

では他の論理回路を表す行列はユニタリになるだろうか

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

とすると

$$U_{NOT}^{\dagger} U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

となるが、XOR や NAND は古典的に表してしまうと逆がつくれない。

たとえば XOR は

$$|00\rangle \to |0\rangle$$
$$|01\rangle \to |1\rangle$$
$$|10\rangle \to |1\rangle$$
$$|11\rangle \to |0\rangle$$

となり、ビット数が消えてしまう。このような XOR は標準 (regular) とよぶ。
したがって、古典的な論理ゲートが qubit になれるためには、回転や反転といった演算ができないといけない。
これは量子回路が**可逆**である必要性を意味している。
つまり、前章でみたようにエトロピーが増大していく過程では干渉性の維持は難しい。

1.4.2 論理回路の量子化

次に複数の quibit を扱う。前節での古典回路と基本的には同じである。
特に古典的な NAND はユニバーサルゲートと呼ばれた。これに対し、XOR や NOT はユニバーサルではない。
つまり、入力する x, y が同じパリティをもっていれば式 1.7,1.8 のように同じパリティを返す。
では量子ゲートの場合はどうか、留意すべきはこれらは直積になることである。
つまり、1 ビットの場合次のように $|q_A\rangle \otimes |q_B\rangle$ は 2×2 の 4 元ベクトルになるはずである。
式 1.10 に対応して

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{1.15}$$

のように縦ベクトルで構成しておかないといけない。
複合的な quibit となる論理 gate は前節でみた CNOTgate である。
このゲートはターゲットと制御の 2 つの入力ゲートをもつ。
次のように制御ビットが 1 であれば反転をするが、0 であれば何もしない。

$$U|00\rangle \to |00\rangle$$
$$U|01\rangle \to |01\rangle$$
$$U|10\rangle \to |11\rangle$$
$$U|11\rangle \to |10\rangle$$

後半 2 行が逆転しているのでこれまでも見てきたように 2 ビット CNOT は次のようにかけることがわかる。

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

これは式 1.11 と同じで次のようにかくことができる。

$$|A, B\rangle \to |A, B \oplus A\rangle$$

$$|A, B\rangle \to |A, XOR(A, B)\rangle \tag{1.16}$$

一般に n 量子ビットは 2^n 元のベクトルになる。
以下でいくつかの 2 ビットの場合の量子ゲート例を紹介する。

1.4.3 制御位相ゲート

CNOT を見たのでいくつかの 2 量子ビットの場合の制御ゲートを考えよう。
次のようなゲートを**制御位相ゲート**という。

$$A = 0 \to A' = A = 0 \cap B' = 0$$
$$A = 1 \to A' = A = 1 \cap B' \neq B$$

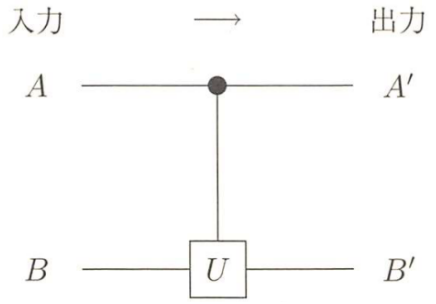


図 1.30: [131] より CPhase ゲート

この制御位相ゲートを U_{Cph} とすると 1.12 から次のようにおけばよい。

$$U_{Cph}(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \langle 0|U|0\rangle & \langle 0|U|1\rangle \\ 0 & 0 & \langle 1|U|0\rangle & \langle 1|U|1\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \tag{1.17}$$

1.4.4 独立ハダマールゲート

次に

$$A \to H \to A'$$
$$B \to H \to B'$$

を考える。

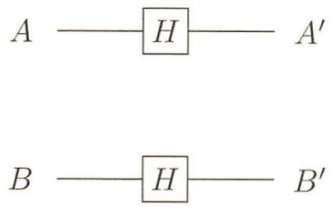


図 1.31: [131] より:独立 H ゲート

具体的な計算は次のようにおこなう。このゲートを U_{IH} とすると

$$
\begin{aligned}
U_{IH}\left|00\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)_A \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)_B \\
&= \frac{1}{2}\left(\left|00\right\rangle+\left|01\right\rangle+\left|10\right\rangle+\left|11\right\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
U_{IH}\left|01\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)_A \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)_B \\
&= \frac{1}{2}\left(\left|00\right\rangle-\left|01\right\rangle+\left|10\right\rangle-\left|11\right\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
U_{IH}\left|10\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)_A \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)_B \\
&= \frac{1}{2}\left(\left|00\right\rangle+\left|01\right\rangle-\left|10\right\rangle-\left|11\right\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
U_{IH}\left|11\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)_A \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)_B \\
&= \frac{1}{2}\left(\left|00\right\rangle-\left|01\right\rangle-\left|10\right\rangle+\left|11\right\rangle\right)
\end{aligned}
$$

次に係数を縦にして、左から行列をつくると

$$
U_{IH} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}
$$

となりこれは

$$
\mathrm{Tr}\left[U_{IH}\right] = 0
$$

である。

1.4.5 制御ハダマールゲート

制御ハダマールゲートを U_{CH} としよう。これは制御 NOT と同じように**何もしない** bit があるので回路記号は次のようになる。

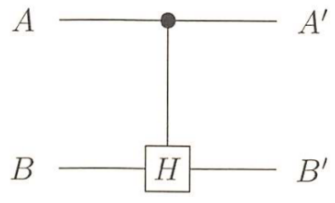


図 1.32: [131] より:制御ハダマールゲート

この行列は直接対角に I, H をおいてもよいが、具体的な計算は次のようにおこなう。

$$
U_{CH}\left|00\right\rangle = \left|00\right\rangle
$$

$$U_{CH}\left|01\right\rangle = \left|01\right\rangle$$

$$\begin{aligned} U_{CH}\left|10\right\rangle &= \left|1\right\rangle_A \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)_B \\ &= \frac{1}{\sqrt{2}}\left(\left|10\right\rangle + \left|11\right\rangle\right) \end{aligned}$$

$$\begin{aligned} U_{CH}\left|11\right\rangle &= \left|1\right\rangle_A \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)_B \\ &= \frac{1}{\sqrt{2}}\left(\left|10\right\rangle - \left|11\right\rangle\right) \end{aligned}$$

次に係数を縦にして、左から行列をつくると式 1.15 から

$$U_{CH} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \tag{1.18}$$

となりこれは

$$\mathrm{Tr}\left[U_{IH}\right] = 2$$

である。

1.4.6 Swap ゲート

2bit の状態ベクトルを交換するゲートは **swap ゲート**とよばれ次で表す。

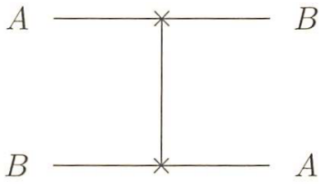


図 1.33: [131] より:swap ゲート

行列は U_{SWP} として

$$U_{CH} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

となる。例えば

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ c \\ b \\ d \end{pmatrix}$$

これは 2 つの qubit の状態を入れ替える。次のような過程をとっている。

$$\begin{aligned}|a,b\rangle &\to |a, a\oplus b\rangle \\ &\to |a\oplus(a\oplus b), a\oplus b)\rangle = |b, a\oplus b\rangle \\ &\to |b, (a\oplus b)\oplus b\rangle = |b,a\rangle\end{aligned}$$

つまり、次の図のように CNOT ゲート上下のビットで交互におこなっている。

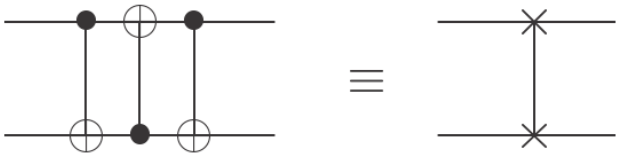


図 1.34: [130] より:swapping two qubits

このように量子回路の特徴は閉回路になっていない、環形式ではない。これを **acylic** という。

古典的なデジタル回路で知られている入出力の線の数、FANIN、FANOUT を増やせば、回路の深さを減らせる技術があるが、量子回路ではユニタリー性が優先するために、これらを完全に利用することができない。

また、このような交換ゲートは古典的には入力と出力をクロス結線すればよく、1 対 1 の通信等でよく用いる。

しかし、量子論の場合は量子状態の時間的変化を回路が表すので、別な粒子と交換することになるので単純ではない。

1.4.7 Fredkin-gate

制御交換ゲートと呼ばれるのが次の **Fredkin-gate** である。

3qubit の場合は次の働きをする。

$$\begin{aligned}A' &= A \\ B' &= \left(\bar{A}\cdot B\right)\oplus(A\cdot C) \\ C' &= \left(\bar{A}\cdot B\right)\oplus(A\cdot B)\end{aligned}$$

すなわち、A' には A がそのまま入り、B', C' には次のような条件が入る。

ケース 1.　$A=0$ の時、入力 B, C がそのまま出力 B', C' になる。

ケース 2.　$A=1$ の時、入力 B, C は交換され、主力 C', B' になる。

真理表と回路記号は次のようになる。

A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

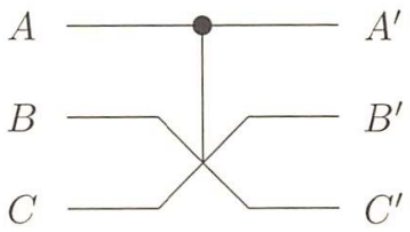


図 1.35: **Fredkin-gate**

1.4.8 Toffoli-gate

トッフォリゲートは制御 CNOT ゲートと呼ばれ、3qubit で、次の条件式を用いる。

$$A' = A$$
$$B' = B$$
$$C' = C \oplus (A \cdot B)$$

真理表と回路記号は次のようになる。

A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

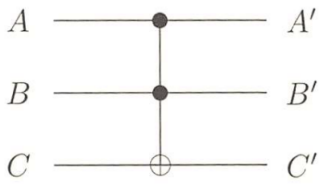


図 1.36: [131] より Toffoli ゲート

このゲートは $A = 1$ であれば CNOT ゲートであり、$C = 0$ であれば $C' = A \cdot B$ で AND 回路になっている。
つまり、入力のどこを固定して、出力のどこを観測するかは任意で、多くの組み合わせができる。
ただし、そのためには入力と出力が 1 対 1 の対応が必要で、そのため、このゲートは次のようなユニタリ演

算子 U_T で表される。行列のランクが 2^3 になっている。

$$U_T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{1.19}$$

例えばこの、Toffoli-gate と CNOT を使うと式の半加算器、全加算器を次のようにつくることができる。

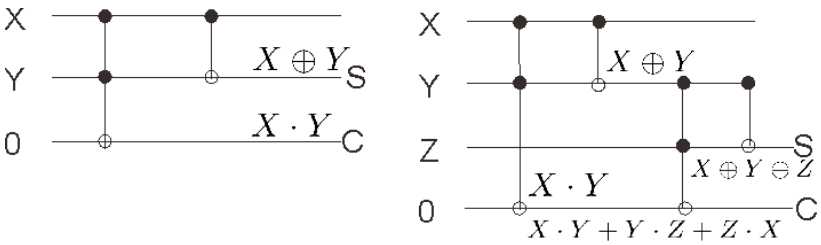


図 1.37: 図左が半加算器、図右は桁上 bit を加えた全加算器

1.4.9 制御ユニバーサルゲート

以上から量子コンピューターでは、論理ゲートのユニタリー性が重要になる。そこで一般に次の図で**制御ユニタリーゲート**を考えよう。これが、制御ユニバーサルゲートである。

これは n 個の qubit を扱うことができるとする。ただし、中身は常に 1 つの制御 qubit と、n 個のターゲット qubit が U の箱の中にあると考える。

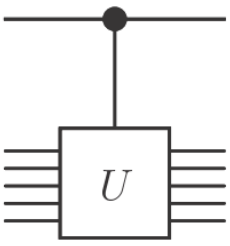


Figure 1.8. Controlled-U gate.

図 1.38: [130] より:制御 U ゲート

従って制御ビットが 0 にセットされれば、何もおこさないが、1 にセットされるとアクションをおこす。例えば次の図のように $U = X$ 演算子で置き換えれば、これは制御 NOT ゲートになる。

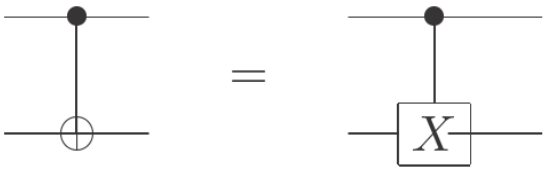


図 1.39: [130] より:制御 NOT の 2 つの表現

さらに重要なのは第 1 章でみたフォン・ノイマンのポインター測定のように、量子測定には確率密度波の解釈が入る。

観測が入ると、これは 1 つの古典的な観測値に収縮するので、観測がどこで行われたかを示す必要がある。

そのために次のような、ポインター絵を用いて観測を示すことにする。

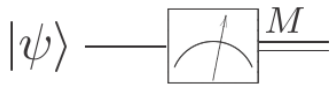


図 1.40: [130] より:観測の記号

2　スーパーポジション

2.1　ブロッホ球

前部で qubit がブッロホ球上の単位ベクトルで表されることをみた。

量子回路はこのブッロホ球面上で qubit を変化させていくことに等しい。まさに SU(2) 変換をしていくことになり、そのメインはユニタリー演算子である。しかし、ブロッホ球は 3 次元球とは異なるので注意がいる。ここでいくつかの基本的な例をみておこう。はじめに

X ゲートで反転をしみる。このときはじめの位置は

$$|\psi\rangle = 1\,|0\rangle + 0\,|1\rangle$$

であり次の図の赤い矢印のように北極を向く。これに X をかけると

$$X\,|\psi\rangle = 0\,|0\rangle + 1\,|1\rangle$$

のように反転する。これが図の緑の矢印である。これは元のベクトルにマイナスをかけたわけではないので注意する。

前節でみたように

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

という行列を演算させている。

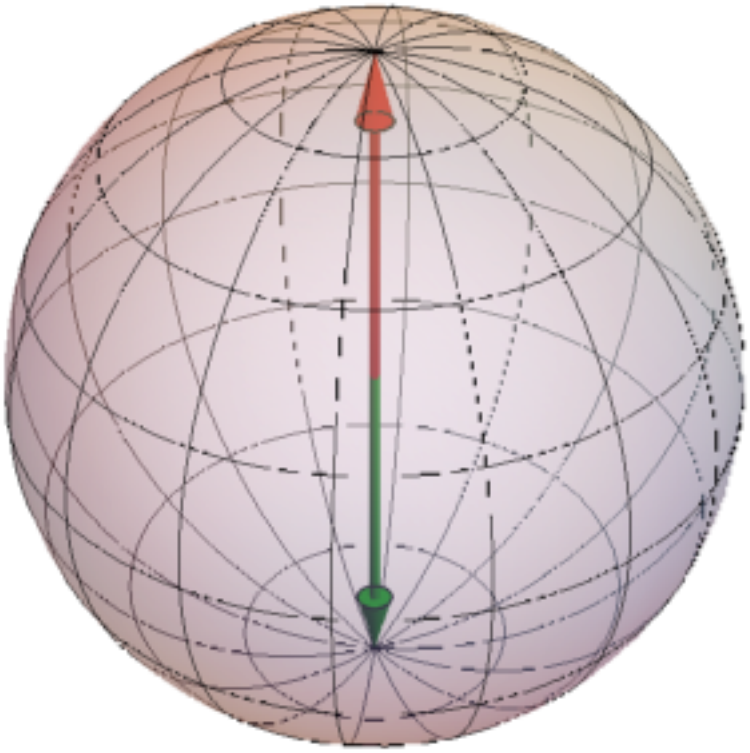


図 2.1: X ゲート：$|\psi\rangle = 1\,|0\rangle + 0\,|1\rangle$ と $X\,|\psi\rangle = 0\,|0\rangle + 1\,|1\rangle$

次に量子的な重ね合わせをつくるアダマールゲートを作用させてみよう

$$H\,|\psi\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle)$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

だから

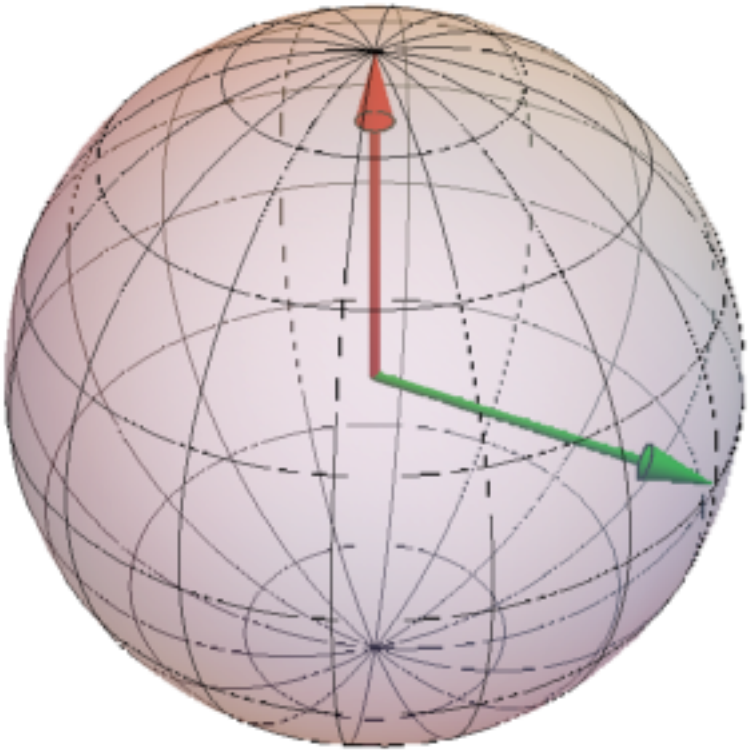


図 2.2: H ゲート

さらに位相反転の Z ゲートも見ておく。これは $|1\rangle$ のみを反転させるので、最初の $|\psi\rangle$ のままだと下図左のように結果は同じになる。

$$Z|\psi\rangle = 1|0\rangle - |1\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

そこで、はじめの状態を先に H ゲートで動かして、Z を作用させると図右のようになる。

$$|\psi'\rangle = H|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$Z|\psi'\rangle = ZH|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

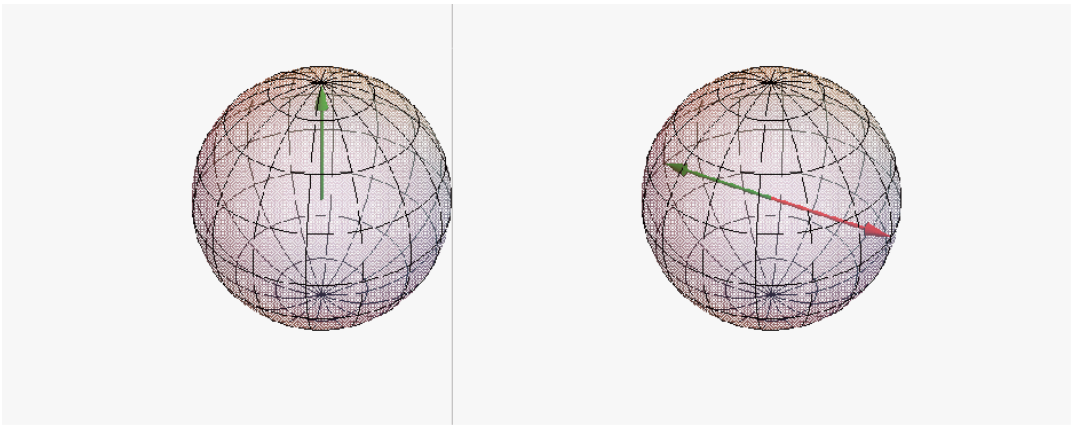


図 2.3: Z ゲート

2.2 Bell 状態

重ね合わせを 2 ビットでつくると興味あるエンタングルドな状態ができる。ここで、その取り扱いを考えよう。

古典的な 2 つのビットを含む時には $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ の 4 つの状態を考えた。

これらの状態が**スーパーポジション**にある場合はブロッホ球上で

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

のように拡張して表現でき、規格化条件も

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$$

である。ただし、ここでの記号 $\{0,1\}^2$ は 0 または 1 のペアを表す。

このような 2qubit の系では部分観測ができる。例えば始めに 1 つの qubit を観測して 0 を得られたとすると、測定後の状態は

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

のように**再規格化**をする。

これは第 1 章であつかった **EPR** 状態または**ベル状態**と呼ばれる。

簡単なのは $|00\rangle, |11\rangle$ のペアで

$$|\beta\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.1}$$

と表すことができる。第 1 章でみたように、$|00\rangle, |11\rangle$ の状態はエンタングルドしていて前部でみたように**エンタングルド状態とは部分系の量子状態の直積で記述できない場合である。**

そこで一般にベル状態を次のように定義する。2 進数を考えているので、$\bar{y} = -y$ の状態として次のようになる。

$$|\beta_{xy}\rangle \equiv \frac{|0,y\rangle + (-1)^x|1,\bar{y}\rangle}{\sqrt{2}} \tag{2.2}$$

これは次のように式 1.18 のハダマールゲートとの組合わせで表すことができる。

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

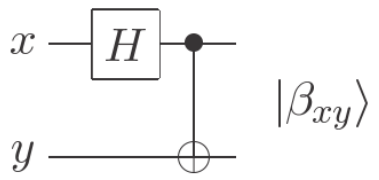


図 2.4: [130] より:ベル状態

各ケットベクトルには相互的な 1,0 が並ぶ。重ね合わせの符号 ± が第一ビットの x の累乗

$$(-1)^x \tag{2.3}$$

がかかり、これは**位相の見返り** (Phase_kickback) と呼ばれる。今後よく登場するので留意する。

2.2.1 エンタングルド状態

前節でもみたが、CNOT ゲートは quibt の複写の役割を果たす。
次の図のように重ね合わせの状態に CNOT を作用させる。
これははじめに未知な状態

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.4}$$

に CNOT をコントールビットを 0 にして入力すると

$$|\psi\rangle_1 = [a\,|0\rangle + b\,|1\rangle]\,|0\rangle \rightarrow a\,|00\rangle + b\,|10\rangle$$

という 2qubit 状態ができる。同様にコントールビットを 1 にして入力すると、反転されるから

$$|\psi\rangle_2 = [a\,|0\rangle + b\,|1\rangle]\,|1\rangle \rightarrow a\,|01\rangle + b\,|10\rangle$$

を得る。これはコントロールビットが 0 なら標的ビットが必ず 1 で、コントロールビットが 1 なら標的ビットが 0 になることを示す。
つまり、どちらか一方を観測すると、他方は必ず決まってしまうという **EPR 状態**である。

$$|01\rangle + |10\rangle$$

という状態は積にすることができない。**エンタングルドな状態**という。
この結果を見ると上位ビットに元の $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ が複製されているように見える。
出力は入力ゲートのテンソル和になる。

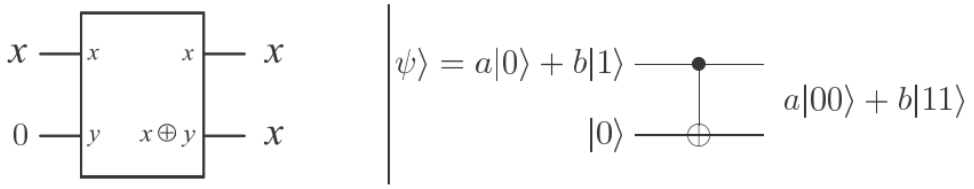


図 2.5: [130] より:CNOT ゲートの働き

しかし、前節でみた式 1.1 のように量子回路では古典的な情報は複製できるが、式 2.4 のような、重ね合わせの状態を複製することは原理的にできない。

例えば 2quibit 状態は

$$|\psi\rangle |\psi\rangle = a^2 |00\rangle + ab |01\rangle + ba |10\rangle + b^2 |11\rangle$$

となるが、$|\psi\rangle$ を CNOT に入れると

$$[a |0\rangle + b |1\rangle] |0\rangle = a |00\rangle + b |10\rangle$$

となり、

$$ab = ba = 0 \tag{2.5}$$

でないといけないことになるが、これは最初の状態が重ね合わせであることと矛盾する。

複製元の情報を知るために観測をおこなうと、その状態はもはや観測前の状態になることが不可能になる。

これが量子回路がループを持てない大きな問題である。

ところが基礎量子論の位置演算子と運動量演算子から次のような非エルミートの生成消滅演算子を作成した。

$$\hat{a^\dagger} = \frac{1}{\sqrt{2}} (\hat{x} - i\hat{p})$$

$$\hat{a} = \frac{1}{\sqrt{2}} (\hat{x} + i\hat{p})$$

とすると交換関係は

$$\begin{aligned} \left[\hat{a}, \hat{a}^\dagger\right] &= \frac{1}{2} \left([\hat{x}, \hat{x}] - i [\hat{x}, \hat{p}] + i [\hat{p}, \hat{q}] + [\hat{p}, \hat{p}]\right) \\ &= 1 \end{aligned}$$

である。また、反交換関係

$$\begin{aligned} \left[\hat{a}, \hat{a}^\dagger\right]_+ &= \hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a} \\ &= \frac{1}{2} (\hat{x}\hat{x} + i\hat{x}\hat{p} - i\hat{p}\hat{x} + \hat{p}\hat{p} + \hat{x}\hat{x} - i\hat{x}\hat{p} + i\hat{p}\hat{x} + \hat{p}\hat{p}) \\ &= \hat{x}\hat{x} + \hat{p}\hat{p} = 1 \end{aligned}$$

どちらにしても虚数単位を別側面から考えると、波の重ね合わせである。この詳細は第 6 部で議論をした。

従って 2.5 は重ね合わせがある条件でおきたと考えることができる。

2.3 量子テレポーテーション

第 1 章でみたようにベル状態はアインシュタインの局所原理を破る**量子テレポーテーション**が起きる。これを 2qubit で見ていこう。

はじめに EPR ペアである状態 $|\psi\rangle$ を用意して、これを Alice と Bob に重ね合わせを維持した状態で送る。

この状態の時にはまだ、$00, 01, 10, 11$ の係数を波動関数は持っている。

ところが次に Alice が観測すると観測結果は古典的に

$$00, 01, 10, 11$$

のどれかになる。この状態でも Bob の持っている波動関数は $00, 01, 10, 11$ の係数を維持している。

次に Alice はどの状態かを Bob に伝える。Bob はこの瞬間に持っていた最初の状態 $|\psi\rangle$ は失い、古典的な情報のみを見ることになる。これは量子論の特徴で前部で見たように、量子論の状態が環境の波動関数の対角和から作られることが関係する。量子論で話題になる分野であるが、基礎理論としては未だ不完全なところが多い。時空間の接続や計量とあわせて、相対論との関係を後に明らかにしていたい。ここでは量子コンピュータとしての応用を進めよう。

このベル状態を回路図にしたものが次の図のようになる。

テレポーテーションは状態

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

ただし、α, β の係数は未定である。

入力する状態を $|\psi_0\rangle$ として次のようなベル状態とする。

また、$|\beta_{00}\rangle$ は図のように上下 2 つのルートがある。

上のラインが Alice で、下のラインが Bob に相当する。

はじめはどちらも同じ“**ベル情報** $|00\rangle + |11\rangle$“を持っている。式 2.1 から

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

として、Alice と Bob に渡すと

$$\begin{aligned}|\psi_0\rangle &= |\psi\rangle\,|\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\left(|00\rangle + |11\rangle\right) + \beta\,|1\rangle\left(|00\rangle + |11\rangle\right)\right]\end{aligned}$$

となり、最初の項が Alice, 最後の項が Bob を表す。

この、Alice と Bob の第 2qubit ペアが EPR、ベル状態を表す。

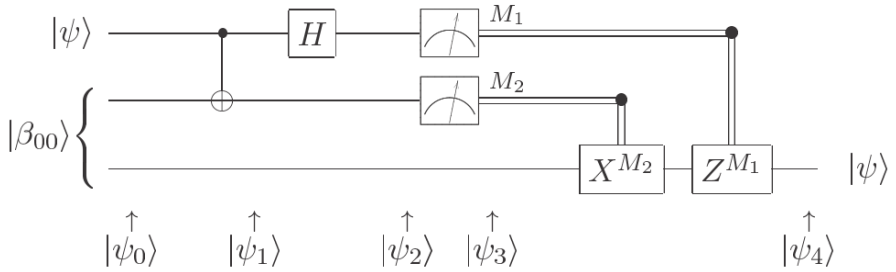


図 2.6: [130] より:ベル状態

はじめに Alice は自分の qubit を CNOT ゲートに入れる。この時、次のように $|1\rangle$ がある後者の上位ビットが反転する。

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\left(|00\rangle + |11\rangle\right) + \beta\,|1\rangle\left(|10\rangle + |01\rangle\right)\right]$$

次に Alice はハダマールゲートを通す。これは式 1.14 から次のように和と差の形になる。

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + \beta\left(|0\rangle - |1\rangle\right)\left(|10\rangle + |01\rangle\right)\right]$$

これを次のように 4 つの項に書き換える。

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle\left(\alpha\,|0\rangle + \beta\,|1\rangle\right) + |01\rangle\left(\alpha\,|1\rangle + \beta\,|0\rangle\right) + |10\rangle\left(\alpha\,|0\rangle - \beta\,|1\rangle\right) + |11\rangle\left(\alpha\,|1\rangle - \beta\,|0\rangle\right)\right]$$

すると次のような解釈ができる。

第 1 項の $|00\rangle$ は Alice の qubits である。Bob の最初の状態は重ね合わせである。

$$\alpha|0\rangle + \beta|1\rangle$$

これらは Alice の**観測 M_1 により**次のように Bob の測定が変化する。

$$00 \to |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle]$$

$$01 \to |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle]$$

$$10 \to |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle]$$

$$11 \to |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]$$

留意すべきは Bob の状態は量子的な重ね合わせをこの時点では保っていることである。

この後 Bob が観測をすると、古典的な観測値が決まる。

従って、Alice が得た情報により、Bob の観測が影響を受けることになる。

EPR パラロックスや、ベル不等式のところで議論したように、この影響はアインシュタインの局所原理を破り、

超光速で伝達が可能になるかもしれない。これが**量子テレポーテーション**と呼ばれる現象である。

しかし、今のところ超光速な実験例はない。

それは次のように Alice の情報によって Bob は最初の状態に修正することができるが、そのためには、古典的な情報の伝達を含むこのになるからである。

例えば Alice から

00 の情報を受け取れば、何もしなくてよい。

01 の情報の場合は bit 反転する必要があるので X ゲートに入力する。

10 の情報を受け取れば、位相反転する必要があるので Z ゲートに入れる。

11 の情報を受け取れば、両方を反転する必要があるので X ゲートに入れてからさらに Z ゲートに入れればよい。

この変換を

$$Z^{M_1}X^{M_2}$$

のように書く。

これにより Bob ははじめの状態 $|\psi\rangle$ を保つことができる。

3　量子アルゴリズム [137]

2020 年の現在、いくつかの量子デバイスが実用化され、量子コンピューターが小 bit ながら動くようになっている。

しかし、ノイズの問題など、課題があるが、一般市民の端末からもアクセスができるようになってきた。

この章では現在いくつかあるシミュレーションソフトとして IBM の Qiskit を利用する。

クラウドから実機にアクセスできる上、QASM と Python の 2 つのプログラムインターフェイスを持っている。

具体的な量子コンピューターの基礎プログラムを作る基礎になるだろう。

3.1 古典コンピューターと量子コンピューター

古典的なコンピューターのロジック回路を量子コンピューターでシミュレーションできだろうか。

答えは Yes である。しかし、直接実現することはできない。

基本的に量子コンピューターは可逆であるが、前節で見た古典的な論理回路は不可逆なので、この問題を克服しないといけない。

そこで可逆な古典的なロジック回路で 3bit を持つ式 1.19 の **Toffoli ゲート**を考える。

これは次の図のような 3bit の INPUT と OUTPUT を持ったので次のように改めて割り当てる。

図の最初の 2bit が制御ビットと呼ばれる役割をする。

3 番目の bit が標的ビット (target_bit) とよばれる。

つまり、はじめの 2 つの bit が共に 1 にセットされた時のみ、標的ビットは値を反転する。

その真偽表も下図に共にあるで、これを見ると、OUTPUT は INPUT と 1 対 1 に対応しているので可逆であることがわかる。

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

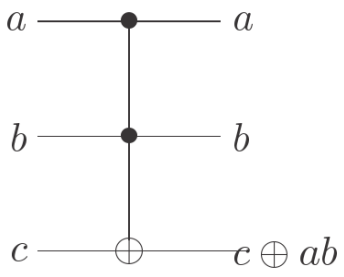


図 3.1: [130] より：古典的な Toffoli ゲート

このゲートのふるまいは後にも重要になる。特に図右側は回路図で表記され、次の操作と同じである。

$$(a, b, c) \to (a, b, c \oplus ab)$$

従って OUTPUT を input すると INPUT が得られる。

$$(a, b, c \oplus ab) \to (a, b, c)$$

従って $c = 1$ と固定すると Toffoli ゲートは次のように NAND ゲートをシミュレートできる。

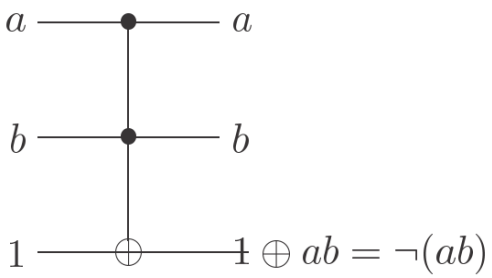


図 3.2: [130] より：Toffoli ゲートを NAND ゲートにする

さらに次のように入力を $(1, a, 0)$ と固定すると結果は a をコピーする FANOUT として動作する。

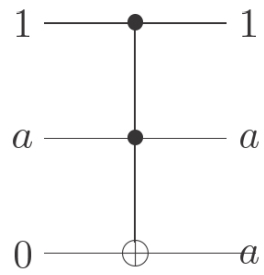


図 3.3: [130] より：Toffoli ゲートを FANOUT ゲートにする

このように上位に 2bit の制御 bit をおけば古典論理回路を量子コンピューターで再現できる。

量子コンピューターは古典的な結果である 1,0 から状態 $|0\rangle$ を選んでも、ハダマールゲートに入れると式 1.14 から

$$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

のような重ね合わせになる。その後測定をすると、1,0 はそれぞれ 50 %の確率で得られることになる。

さて、これでは量子コンピューターのメリットがないのではないかと思うかもしれない。

しかし、多くのゲートと大きな qubit を使う時に量子コンピューターはその本領を発揮する。

その例として Deutsch-Josa のアルゴリズムを次で見る。

3.2 量子並列化

量子コンピューターにおいて並列処理をどうするかはとても重要な問題になる。

これは古典コンピューターにはできない、重ね合わせの状態を入力できるので、一度に並列処理をしていくことが可能になる。

そこで、次のような 1bit の集合と範囲を持つ関数を用意する。

$$f(x) : \{0, 1\} \to \{0, 1\}$$

入力には 2qubit を持つ状態

$$|x, y\rangle$$

を考える。この下位ビットに次のように操作を与える U_f ゲートを考える。

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle \tag{3.1}$$

前節式 1.9 でもみたようにテンソル和 $\oplus$ は 2 の剰余を加えることに等しい。

$$y \oplus f(x) \to y + f(x) \mod 2$$

また、これは $y = 0$ であれば

$$U_f : |x, 0\rangle \to |x, f(x)\rangle \tag{3.2}$$

であり、下位ビットに $f(x)$ そのものを得ることになる。

この U_f は**オラクル演算子**と呼ばれる。

前節 1.16 でみた **CNOT ゲート**がこの役割をする。

例えば次のような回路を考える。

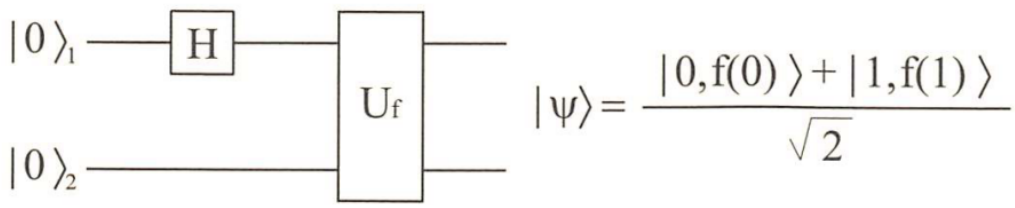


図 3.4: [132] より：量子並列化

これを式で表すと

$$|\psi\rangle = U_f H\,|0,0\rangle = U_f \frac{1}{\sqrt{2}}\{|0,0\rangle + |1,0\rangle\}$$
$$= \frac{1}{\sqrt{2}}\{|0,f(0)\rangle + |1,f(1)\rangle\}$$

となる。これは状態 $|\psi\rangle$ が関数 $f(0)$ と $f(1)$ を両方を線形結合として持っていることになる。
これは、**同時**に処理される。つまり、量子的な干渉状態であるかわりに、同じ時間で作用するわけである。
これが量子コンピューターの並列化になるわけであるが、量子論としての時間の考え方に示唆を与えている。
さらにこの回路は多重化できる。次のように重ね合わせた状態を制御ポートに入れることができる。

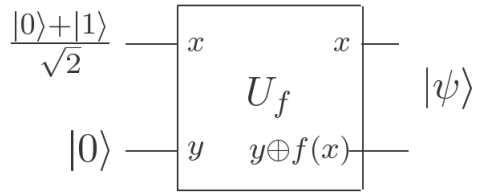


図 3.5: [130] より：U_f ゲート

このゲートは INPUT として、$|0\rangle$ をハダマールゲートに通して、**スーパーポジション**にある状態を選ぶことができる。
つまり、

$$U_f : \left|\frac{|0\rangle + |1\rangle}{\sqrt{2}}, |0\rangle\right\rangle \to \left|\frac{|0\rangle + |1\rangle}{\sqrt{2}}, f(x)\right\rangle = \frac{1}{\sqrt{2}}\left(|0,f(0)\rangle + |1,f(1)\rangle\right) \tag{3.3}$$

となる。
これは**量子並列化**と呼ばれ、量子論に独特なものである。
古典的な並列処理と異なるのは量子的な可干渉性を持つ、スパーポジションを維持していることである。
異なる状態である $f(0)$ と $f(1)$ は古典的には干渉することはあり得ない。
ハダマールゲートのこうした特性はさらに今後深い考察がいるだろう。
この手続きは大きな n-qubit に対しても簡単に応用が効く。これを **n-Hadamard 変換**と呼ぶことがある。
例えば $n = 2$ の場合について $|0\rangle$ を INPUT した場合には次のような OUTPUT になる。

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \Rightarrow \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

これを $H^{\otimes 2}$ と書く。つまり、2 つのハダマールゲートの平行作用である。

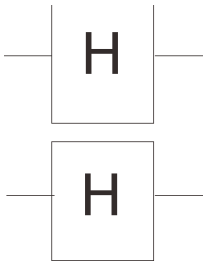


図 3.6: ハダマール変換 $H^{\otimes 2}$

さらに拡張し、**1-qubit を OUTPUT に n-bit を x に INPUT する**処理を考えよう。
これは $n+1$qubit の状態で

$$|0\rangle^{\otimes n}|0\rangle$$

とかけるから、次に上位の n-bit をハダマール変換に入れると式 3.3 の回路 U_f を用いて、次の状態に移る。

$$\begin{aligned}
|\psi\rangle &= H^{\otimes n}|0\rangle = H\otimes H\otimes\cdots\otimes H|00\cdots0\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\cdots\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \\
&= \frac{1}{\sqrt{2^n}}\{|00\cdots0\rangle+|00\cdots1\rangle+\cdots+|11\cdots1\rangle\} \\
&= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^{n-1}}|x\rangle
\end{aligned}$$

となる。
これは指数関数的な 2^n 個の状態を n 個の H ゲートで計算できることを示す。
つまり、式 3.3 のようにコンピューターにある関数

$$f: x \to f(x)$$

の処理をさせる演算を U_f で定義し、状態 $|\psi_i\rangle$ に作用させると

$$\begin{aligned}
|\psi'\rangle = U_f(|\psi\rangle|0\rangle) = U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x0\rangle\right) \\
\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle
\end{aligned} \tag{3.4}$$

となる。これは上位の x を観測すれば $f(x)$ が決まることを示す。
これは量子論の重ね合わせの原理が、並列処理として利用できる可能性を示す。
少ない bit では古典的な計算でも問題はないが、古典的に指数関数的に増える計算を、この並列処理の原理から多項式計算にまで落とせることが計算機としては有用になる。これは次節で詳しくみる。

3.3 Qiskit 計算例

ここで実際の量子コンピューターの動きを感覚的につかむために Qiskit を用いて具体的にみていこう。
3qubit をここでは用いる。ここに 2 つのハダマールで重ね合わせをつくり、2 つの CNOT を通して結果を見よう。
はじめに Qiskit の QASM を利用し次の回路をつくる。

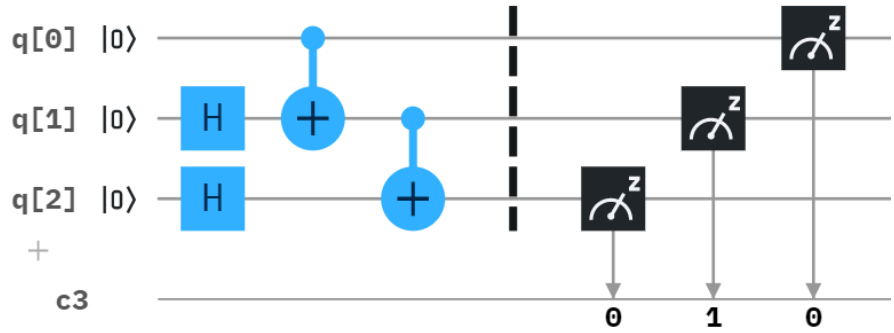


図 3.7: Qiskit による CNOT 回路 1

点線のある右では観測が行われ、古典レジスタに結果を入れている。
もちろん古典レジスタに入るのは 1 か 0 のどちらかしかない。
この回路で 3 つの量子ビットがどういう割合で重ねあわさっているかを予想してほしい。
最初の CNOT の制御ビットには 0 が目的ビットには重ね合わせが入力されている。
この時は CNOT は目的ビットはそのまま通す。
次に 2 番目の CNOT の目的ビットには重ね合わせが入り、目的ビット重ね合わせが入る。
従って、制御ビットが 0 か 1 でも目的ビットは 0 か、反転して 1 を通すことになる。
従って最終的に量子ビットの状態は第 2CNOT の制御ビットが 0 なら

$$|000\rangle, |001\rangle$$

の 2 つが等しい確率であらわれ、第 2CNOT の制御ビットが 1 なら

$$|011\rangle, |010\rangle$$

が等しい確率で現れる。この結果を Qiskit のヒストグラムを用いて表示すると次のようになる。

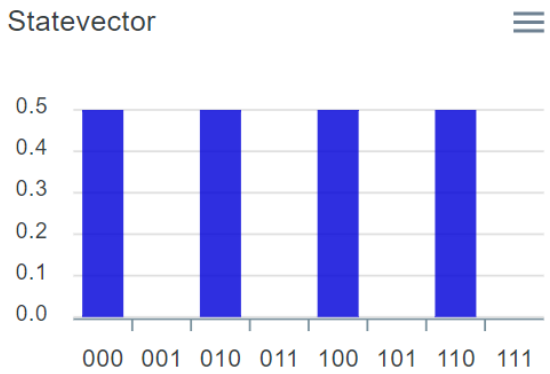


図 3.8: CNOT 回路 1 のヒストグラム

この結果表示は今後もよく使うが、留意点として回路の下段から上にビットを並べているので、3 ビットの並びが実際と反対になっているに注意する。
Qiskit には観測結果をヒストグラム化する方法もあるので、これを使うと並びは反対にならない。
しかし、ここでは全てのパターンを表示できる方法を選ぶ。Qiskit は密度行列を表示することもできる。
予想された結果に一致していることがわかる。
ではもう一つ例題として次の回路の結果のヒストグラムを予想してほしい。

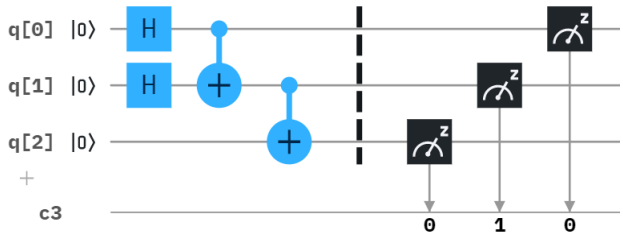


図 3.9: Qiskit による CNOT 回路 2

この回路では最初の CNOT の制御ビットに重ね合わせを入れて、目的ビットにも重ね合わせが入る。
次の CNOT には制御ビットに重ね合わせが入り、目的ビットには 0 が入る。
従って第一ビットは 0 か 1 が等しい確率でそのままはいる。第 2 ビットが 0 か 1 で第 3 ビットは 1 か 0 が出力される。
これはエンタングルドの状態で第 2 ビットと第 3 ビットは相関がある。
結果を表すと次のようになる。

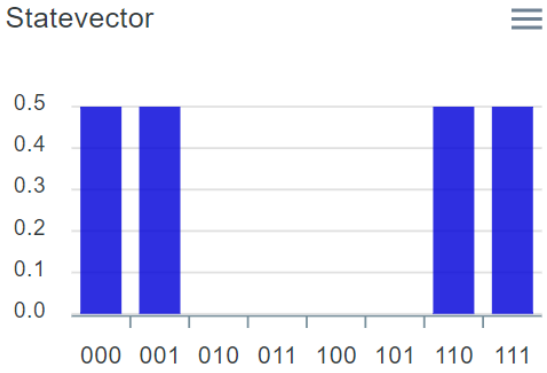


図 3.10: CNOT 回路 2 のヒストグラム

先の留意点に注意し、反対から読むと

$$|011\rangle, |111\rangle$$

が等しい確率で生じ

$$|000\rangle, |100\rangle$$

が等しい確率で生じている。
これらが重ね合わせって処理されているところが古典コンピューターとの違いである。
では次の問題を考えてみよう。ただし、3qubit でおこなうとする。H ゲート CNOT ゲートは最大 3 とする。

問題. 入力 $|a\rangle, |b\rangle$ から出力として $|a+b \mod 2\rangle$ をつくる量子回路をつくれ。

解. 次のような CNOT3 つの回路をつくる。2 進であるから次の 4 パターンしかない

$$|a=0\rangle, |b=0\rangle \to |a+b \mod 2\rangle = |0\rangle$$
$$|a=0\rangle, |b=1\rangle \to |a+b \mod 2\rangle = |1\rangle$$
$$|a=1\rangle, |b=0\rangle \to |a+b \mod 2\rangle = |1\rangle$$
$$|a=1\rangle, |b=1\rangle \to |a+b \mod 2\rangle = |0\rangle$$

従って次が等確率で出てくる回路を考えればよい。

$$|000\rangle, |011\rangle, |101\rangle, |110\rangle$$

これは次のように CNOT を 3 つ使う。

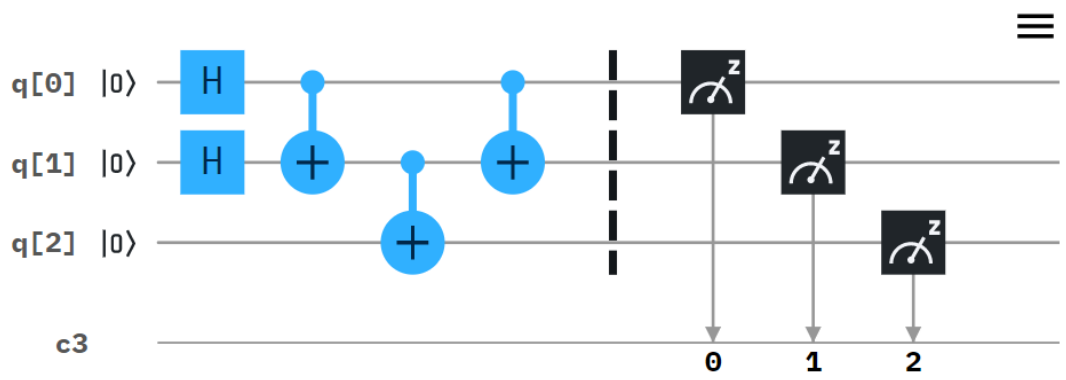


図 3.11: $a + b \mod 2$ を作る量子回路例

結果は次のようになる。ただし、せっかくなので実機にアクセスして結果を返してみた。
コロナウィルスが広がっていた 2020 年の 3 月に試行回数は標準の 1024 回を IBM の実機に入力している。
まもなくして次の結果が返ってきた。
これは観測結果を確率表記していることに注意する。
結果は全て 25 %ではない。いくつかのノイズの問題が実機にはあることがわかるが、だれもが自分の量子回路を実機で試行できるようになったことは数年前からみれは驚きである。

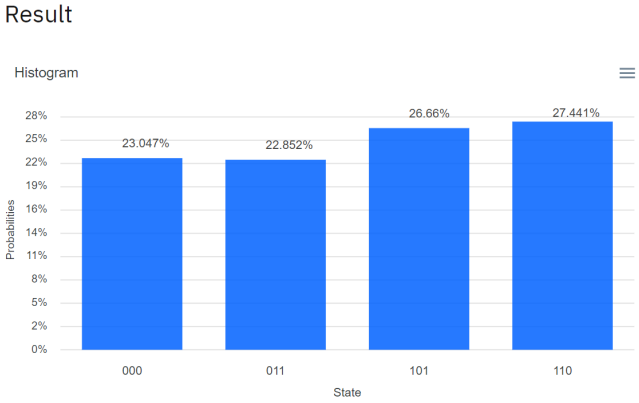


図 3.12: Qiskit による回路変更

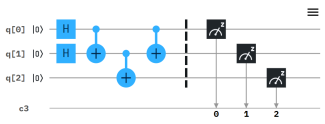


図 3.13: Qiskit による IBM 実機計算結果

これは順番を戻すと

$$|000\rangle, |011\rangle, |101\rangle, |110\rangle$$

3.4 ドイチェのアルゴリズム

3.4.1 Deutch-Joza のアルゴリズム

量子コンピューターの並列化の歴史となる Deutch-Josza のアルゴリズムを見てみよう。
これは次の問題から始まる。

問題. Deutch-Joza のアルゴリズム
2^n 個の整数の集合を考えて、

$$Z_{2^n} = \{0, 1, \cdots, 2^n - 1\}$$

から

$$Z_2 = \{0, 1\}$$

への関数 f

$$f : Z_{2^n} \to Z_2$$

が与えられたとする。この時、次の命題のうち、真となるものを見つける量子アルゴリズムを見つけよ。
a) f **は定数関数ではない**
b) $f(Z_i)(i = 0, 1, 2, \cdots, 2^n - 1)$ **の 0 の数は** 2^{n-1} **個ではない。**

この解は次のようになる。

解. 2 つの命題のうちすくなとも 1 つは真であることをまず、証明する。
この命題が否定形で書かれていので、その否定をとると肯定形になることに留意する。
a) が真ではないとすると、$f(Z_i)$ は定数関数であるので 0 または 1 になる。よって b) は真である。
b) が真ではないとすると、$f(Z_i)$ は 2^{n-1} 個の 0 と、$2^n - 2^{n-1} = 2^{n-1}(2-1) = 2^{n-1}$ 個の 1 を与える関数になる。
これは定数関数ではない。よって a) が真になる。
一般に $f(Z_i)$ が n' 個 $\left(n' \neq 2^{n-1}, n' \neq 2^n\right)$ の 0 を与え、$2^n - n'$ 個の 1 を与えたとすると a),b) 共に真になる。

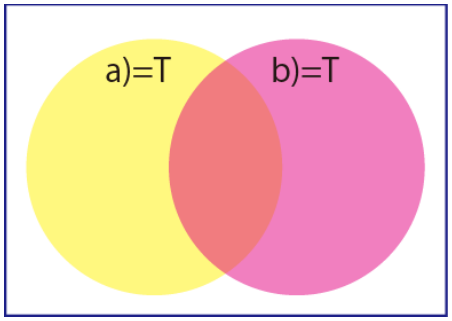


図 3.14: a),b) が真 (T) になる領域

これを古典的なコンピューターで解くと

$$2^{n-1} + 1$$

回の処理をさせるプログラムが必要になる。
ところが次のように量子コンピューターを使うとたかだか 2 回の処理で済む。
まず、入力ビットを x_i、出力ビットを $f(x_i)$ として、次のような状態を考える。

$$|x_i, f(x_i)\rangle$$

次に始状態として次のように 2^n 個の重ね合わせ状態を用意する。

$$|\psi_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_i=0}^{2^{n-1}} |x_i, 0\rangle$$

これを使って出力ビットに関数値が出るような演算が U_f であると見なせるので
中間状態 1 として

$$|\psi_1\rangle = U_f |\psi_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_i=0}^{2^n-1} |x_i, f(x_i)\rangle$$

をつくる。
さらに出力ビットの位相を求めるために

$$I \otimes \sigma_Z$$

を考える。これは式 1.13 の **Z ゲート** (z_gate) である。

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

中間状態 1 にこれを作用させ、中間状態 2 をつくると

$$\begin{aligned} |\psi_2\rangle &= Z |\psi_1\rangle = ZU_f |\psi_i\rangle \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sum_{x_i=0}^{2^n-1} |x_i, f(x_i)\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x_i)} |x, f(x)\rangle \end{aligned}$$

となる。Z ゲートがかかると $(-1)^{f(x)}$ のように符号が $f(x)$ 依存になるところが重要である。
さらに U_f^{-1} を作用させると、結局演算子

$$U_f^{-1} Z U_f$$

が対角化され、出力ビットに影響を与えなくなる。
よって式 3.4 から終状態 $|\psi_f\rangle$ として

$$\begin{aligned} |\psi_f\rangle &= U_f^{-1} |\psi_2\rangle = U_f^{-1} |\psi_2\rangle = U_f^{-1} Z |\psi_1\rangle = U_f^{-1} Z U_f |\psi_i\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x_i=0}^{2^n-1} (-1)^{f(x_i)} |x_i, 0)\rangle \end{aligned}$$

が得られる。この始状態から終状態への確率が求められ

$$\begin{aligned} P &\equiv |\langle \psi_f | \psi_i \rangle|^2 \\ &\left| = \langle x_i, 0| \frac{1}{\sqrt{2^n}} \sum_{x_i=0}^{2^n-1} (-1)^{f(x_i)} \frac{1}{\sqrt{2^n}} \sum_{x_i=0}^{2^{n-1}} |x_i, 0\rangle \right|^2 \\ &= \left(\frac{1}{2^n}\right)^2 \left| \sum_{x=0}^{2^n-1} (-1)^{f(x_i)} \right|^2 \end{aligned}$$

が得られる。

この後半部分 $||^2$ は量子論に特徴的なものである。つまり x_i は $1, 0$ であるが、$f(x_i)$ に符号が依存するので

$$P = \begin{cases} 1 & b) = \text{True}, a) = \text{Flase} \\ 0 & a) = \text{True}, b) = \text{False} \\ 0 < P < 1 & a) = \text{True}, b) = \text{True} \end{cases}$$

となる。これは実際の計算で U_f, U_f^{-1} を 1 回処理させれば可能になる。ここに注目がいきがちであるが、この結果は

$$0 \leq P \leq 1$$

のアナログ的な確率が U_f によりつくられる。P の領域を先の図にふると、次のようになる。

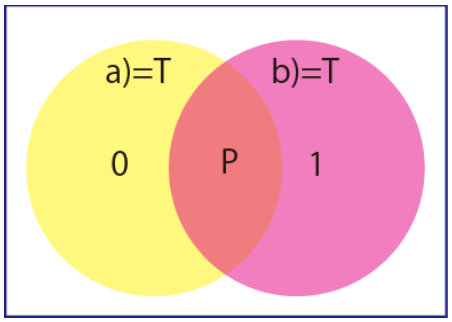


図 3.15: **Deutch-Joza のアルゴリズム**

3.4.2 ドイチェ問題

U_f ゲートを具現化した最初の例が 1992 年に Deutsch が示した前節の **Deutsch's-algolithum** である。

これを具体的に量子コンピューターで使う方法を考えよう。ドイチェは 2 進変数 $x = \{0, 1\}$ が同じ 2 進変数の関数

$$f(x) = \{0, 1\}$$

として、次の性質をもつものがあるとした。

$$1.Constant f(0) = f(1)$$
$$2.Balanced f(0) \neq f(1)$$

1 は Constant 関数 (定数) と呼ばれ、変数に何をいれてもつにに一定である。

2 は Balanced 関数 (均等) と呼ばれ、変数をいえると均一に変化を与える。

この時、ドイチェは変数 x に値を入れ、関数 $f(x)$ を 1 回だけ調べて 1 か 2 を判定できるかという問題を出した。

これが前節でみた**ドイチェ問題**である

古典的にはどうしても 2 回の調べる必要があるが、量子コンピューターを使うと 1 回ですませることができる。

これを量子回路に組んでいこう。

ドイチェ問題で関数 f(x) を調べることは**オラクル（神託）**と呼ばれる。

この部分は前節でみたいわばブラックボックスのユニタリー変換 U_f である。

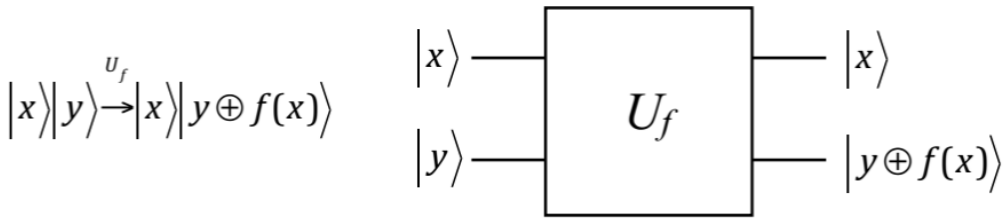


図 3.16: オラクルの中身、CNOT により $y \oplus f(x) \to y + f(x) \mod 2$ をつくる

はじめにハダマールゲートを用いて重ね合わせの状態を次のように作る。

$$|0\rangle \to H \to \frac{|0\rangle + |1\rangle}{\sqrt{2}} \to x$$

これを x レジスタに入れて、さらにハダマールゲートを用いて、次を y レジスタに入れる。

$$|1\rangle \to H \to \frac{|0\rangle - |1\rangle}{\sqrt{2}} \to y$$

これで INPUT 状態 $|01\rangle$ をつくる。

$$|\psi_0\rangle = |01\rangle$$

とおく。この回路は次の図のようになり、これを **Deutsch's-algolithum** という。

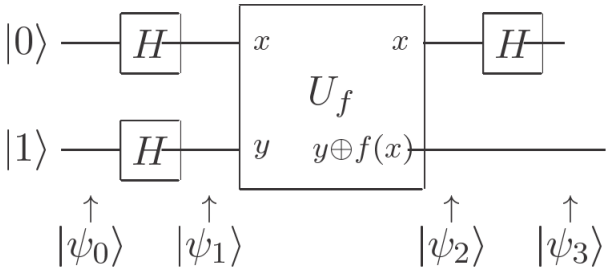


図 3.17: [130] より：Deutsch's-algolithum を利用した回路

従って図の $|\psi_1\rangle$ は $|\psi_0\rangle$ が 2 つのハダマールを通った結果次のようになる。

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

式 3.3 の U_f ゲートに次の状態を入れると

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \to^{U_f} \to (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.5}$$

となるので U_f を $|\psi_1\rangle$ にいれると次のようになる。

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if\ f(0) = f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & if\ f(0) \neq f(1) \end{cases} \tag{3.6}$$

3.4.3 シミュレーション

次に実際にプログラムとしてコンピュータ上で走らせる。

量子回路のシミュレーションはいくつかあるが、ここでは IBM の Qisikit が文献が豊富で、実機で実際に試すこともできる。

これをドイチェ問題に利用しみよう。

まず具体的に次のように第 2 ビットをアダマール変換で囲む。

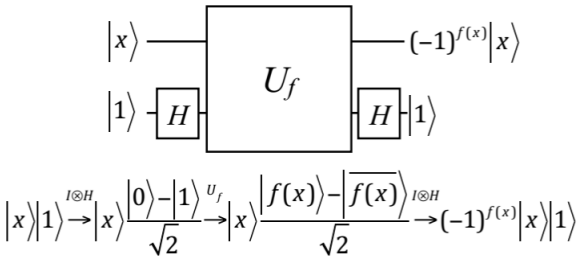


図 3.18: [137] より：U_f ゲートの作成

これにより、出力ビットには前節の式 3.5 から

$$(-1)^{f(x)}|x\rangle|1\rangle$$

が作られる。係数 $(-1)^{f(x)}$ は U_f に拡張されたときの位相の見返りである。

そこでドイチェ問題を解くために、次のようにオラクル U_f をアダマール変換で囲む。

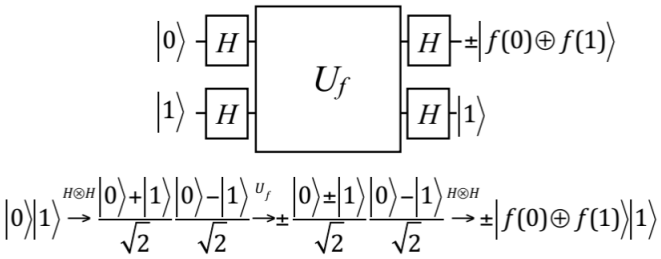


図 3.19: [137] より：4 つの H ゲートで挟んだ回路

これにより入力を $|0\rangle|1\rangle$ とすると

$$|f(0)\oplus f(1)\rangle|1\rangle$$

が得られる。つまり、出力ビットの上位ビットを観測すれば、一定な関数か、均等な関数かが 1 回で判別できる。

実際に Qiskit に次の回路を入力してみる。

結果は図のように $|11\rangle$ が 100 %である。Qiskit では結果の棒グラフと、密度行列を表示できる。

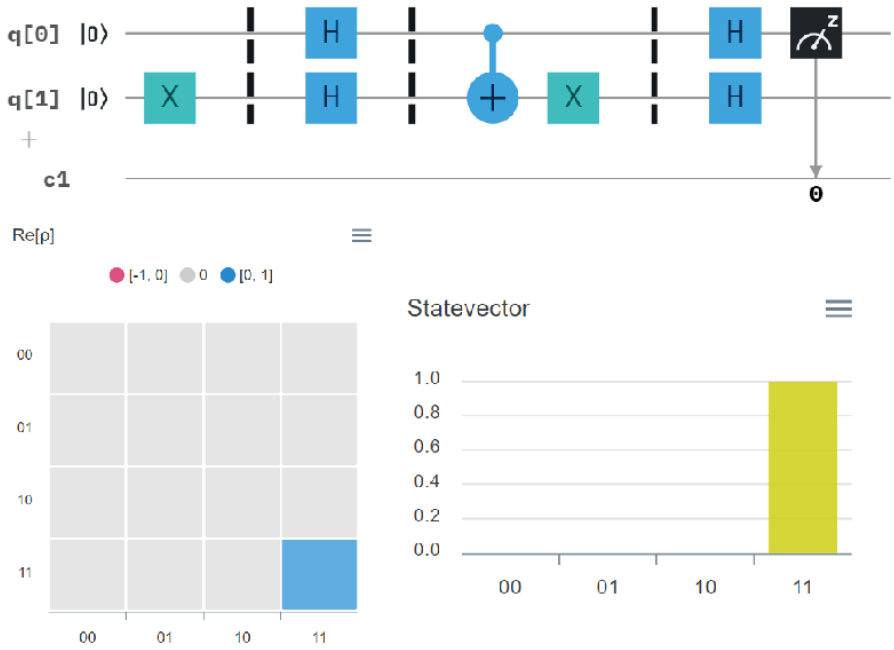


図 3.20: Qiskit の結果：上位ビットは 1

この回路の実行結果は $|11\rangle$ が 100 %になる。
従って出力の上位ビットが 1 であり、このオラクルは均等なランダム関数である。
この場合は均等になるのは

$$f(0) = 0, f(1) = 1 \, or \, f(0) = 1, f(1) = 0$$

この時の出力はどちらも

$$|f(0) \otimes f(1)\rangle = |1\rangle$$

になる。
定数になるのは

$$f(0) = f(1) = 1 \, or \, f(0) = f(1) = 0$$

の場合で、この時の出力はどちらも

$$|f(0) \otimes f(1)\rangle = |0\rangle$$

となる。
そこで次に 2 つのオラクルを並列に並べて、上位は定数を、下位には均等になるように回路をつくる。
4 つのアダマールを上位には Not、下位には CNOT で囲んで次のような回路をつくる。

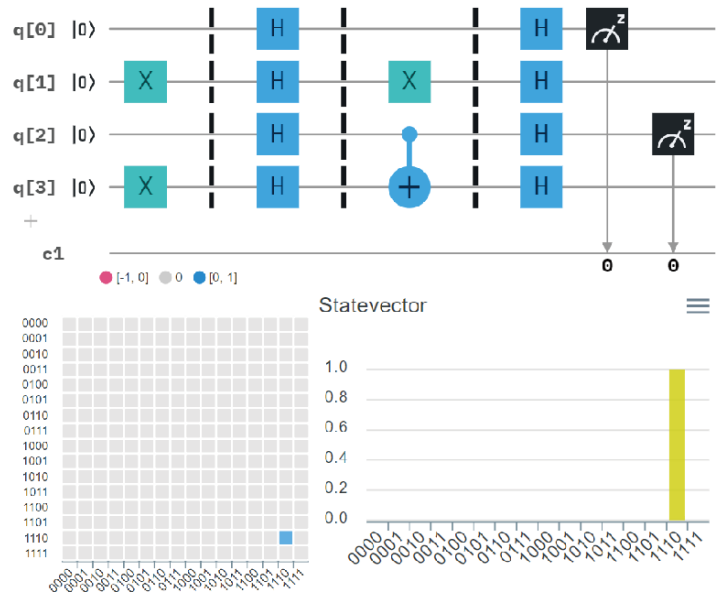


図 3.21: 上位に定数、下位に均等のドイチェ問題の判定

結果は 1110 が 100 %にっているがこれは Qiskit が下位のビットから先に読んでいるからで
次の結果表示のように |01⟩ が 100 %であることを表す。

```
{'01': 1024}
```

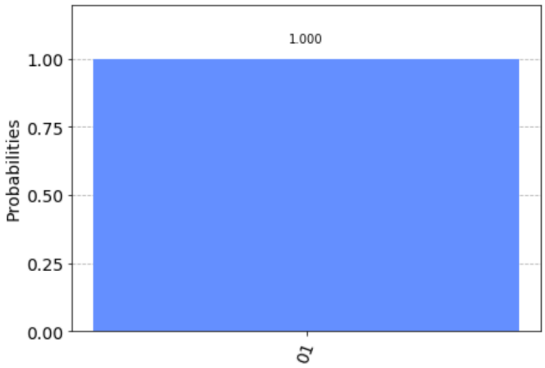


図 3.22: Qiskit による結果のヒストグラム

3.4.4 ドイチェ・ジョサ問題

前節の例を多ビットに拡張していくことは簡単のように思われる。
例えば、3 ビットの場合は次のようになる。Qiskit(IBM) をもちいてシミュレーションをする。次の回路をつくる。

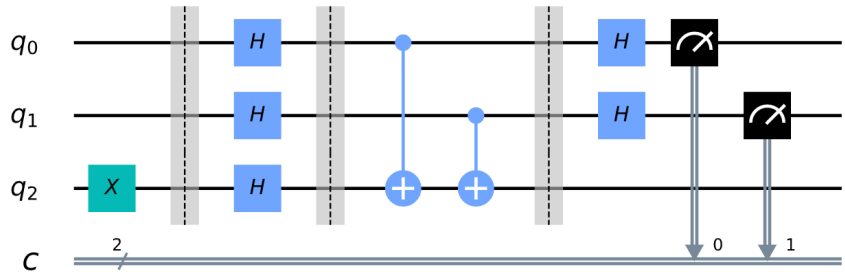


図 3.23: qiskit を用いた回路図

この回路の実行結果は $|11\rangle$ が 100 %になる。

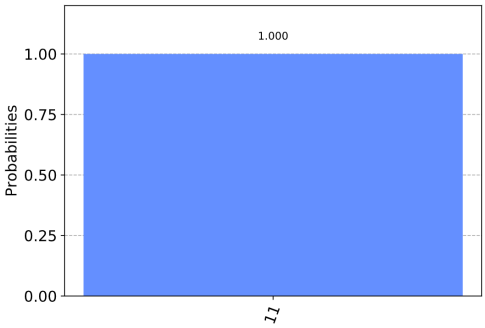


図 3.24: qiskit を用いた棒グラフ

3 ビット以上でも一定か、均等かの判定回路をつくることができるが、次のようにこのどちらかしかおこらない。という約束をつける必要がある。これを**約束アルゴリズム**と呼ぶことがある。

例えば変数 x が 2 ビットの時、2 進表記では

$$f(00), f(01), f(10), f(11)$$

の 4 通りがある。0,1 をとるので全部で

$$N = 2^4 = 16$$

通りあることになるが、約束アルゴリズムでは関数 f が一定か、均等かのどちらかしかとらないとするのでまず、一定な関数は

$$f(00) = f(01) = f(10) = f(11) = 0\, or\, 1$$

の 8 通りしかない。

次に均等な関数は

$$f(00) = f(01) = 0, f(10) = f(11) = 1$$
$$f(00) = f(11) = 0, f(01) = f(10) = 1$$
$$f(00) = f(10) = 0, f(01) = f(11) = 1$$
$$f(00) = f(01) = 1, f(10) = f(11) = 0$$
$$f(00) = f(11) = 0, f(01) = f(10) = 0$$
$$f(00) = f(10) = 0, f(01) = f(11) = 0$$

の 6 通りしかない。

従って約束アルゴリズムでは全部で $2^3 = 8$ 通りあることになり、これを判定していかないといけない。

従って、古典的なアルゴリズムで少なくとも 3 回の問い合わせが必要になる。
これに対し、量子的なアルゴリズムの問い合わせは 1 回ですむ。
これは N が増えても同じであり、量子コンピューターの優位なところである。

3.5 ショアの因数分解のアルゴリズム

3.5.1 古典コンピューターでの因数分解 [137]

はじめに古典的因数分解のアルゴリズムを見ておく。例として $N = 15$ を用いる。
15 を因数分解するために N より小さな互いに素の整数 a を次の範囲でランダムに選ぶ。

$$a \in [2, N-1]$$

ここでは

$$a = 7$$

とする。
次に N を法とした余り関数 $f(x)$ を

$$f(x) = a^x \mod N \tag{3.7}$$

これは**合同式**と呼ばれる。
幾何学のように $f(x)$ と a^x は N の整数倍であれば位置の差を無視して、同じものと見なそうというわけである。
この x を a の N を法とした**位数 (order)** と呼ぶ。
整数 a はランダムに与えたので次に

$$f(x) = f(x+r) \tag{3.8}$$

を満たす最小の周期 r を求める。そのために

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

となる最初の位数 x を求めればよい。そうすると式 3.7,3.8 から

$$f(x+r) = a^{x+r} \mod N = a^x \mod N = 1 = f(x)$$

となり、確かに周期性をもつ。
次にこの周期 r が偶数でれば次のようにユークリッドの互除法を用いて因数を求める。

$$a^r \mod N - 1 = 0$$
$$\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) \mod N = 0$$

これか最大公約数 gcd を

$$\gcd\left(a^r \pm 1, N\right) \tag{3.9}$$

を求めればよい。
この $f(x)$ の周期性を見いだすことで因数分解が次のように求まる。
$f(x)$ が周期関数で、$f(x) = 1$ の時式 3.13 は

$$a^r \equiv 1 \mod N \tag{3.10}$$

となり、r が a の $\mod N$ の位数で r が偶数なら

$$a^r - 1 = \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) = nN$$

とかける。この時 $a^{r/2} \pm 1$ と N の最大公約数 gcd から

$$\gcd\left(a^{r/2}+1, N\right), \gcd\left(a^{r/2}-1, N\right) \tag{3.11}$$

が N の因数になる確率が高い。ただし、$r \neq 0$ とする。
さらに $f(x)$ が周期関数であることは式 3.13,3.10 から位数 r も $f(x)$ と同じ周期性を持っている。
これから因数分解するのに $f(x)$ の周期を見つければよいことになる。
しかし、この方法では偶数の周期 r を求めるまで、a を選びなおさないといけない。
例えば $N = 15, a = 7$ の場合は

$$\begin{aligned}
f(0) &= 7^0 \mod 15 = 1 \\
f(1) &= 7 \mod 15 = 7 \\
f(2) &= 7^2 \mod 15 = 4 \\
f(3) &= 7^3 \mod 15 = 13 \\
f(4) &= 7^4 \mod 15 = 1 \\
f(5) &= 7^5 \mod 15 = 7 \\
\cdots &= \cdots \\
f(8) &= 7^8 \mod 15 = 1
\end{aligned} \tag{3.12}$$

となるので周期 $r = 4$ が得られ

$$a^{r/2} \pm 1 = 7^2 \pm 1 = 48, 50$$

となるから式 3.9 より

$$\begin{aligned}
\gcd\left(a^{r/2}-1, N\right) &= \gcd(48, 15) = 3 \\
\gcd\left(a^{r/2}+1, N\right) &= \gcd(50, 15) = 5
\end{aligned}$$

となり、$3, 5$ が $N = 15$ の因数であることがわかった。
しかし、$a = \{4, 11, 14\}$ の場合は

$$\begin{aligned}
f(0) &= 4^0 \mod 15 = 1 \\
f(1) &= 4 \mod 15 = 4 \\
f(2) &= 4^2 \mod 15 = 1 \\
f(3) &= 4^3 \mod 15 = 4
\end{aligned}$$

となるので周期 $r = 2$ が得られ式 3.9 より $a = 4$ の場合

$$\begin{aligned}
\gcd\left(4^{r/2}-1, N\right) &= \gcd(3, 15) = 3 \\
\gcd\left(4^{r/2}+1, N\right) &= \gcd(5, 15) = 5
\end{aligned}$$

を得る。
この方法から合同関数を先にコンパイルしておくコンパイラ版量子回路が次の量子コンピューターで用いられるようになった。

3.5.2 量子コンピューターの利用

量子コンピューターの並列化が有用な 1 つの例が因数分解である。

例えば次の 20 桁を因数分解させることを考えよう。

$$N = 3977291623907209103$$

そこでこの N が因数 p, q を持つとすると

$$N = pq$$

とかけるから、少なくと p, q のどちらかは $\sqrt{N}$ より小さい。よって N を 1 から $\sqrt{N}$ の数で実際に割ってみればよい。

しかし、これは桁数が多いと高性能な PC でも大変で、この場合は $\sqrt{N}$ が 10 桁になるので数十億回の割り算をすることになる。

この時の古典的なアルゴリズムは

$$\sqrt{N} = 2^{\frac{1}{2}\log_2 N}$$

回の処理をする。つまり、N は指数の型に入るので桁数が大きいと処理回数は指数関数的に増える。

しかし、

$$p = 6257493337$$
$$q = 6536046119$$

2 つの積を求める門内は 1 回程度の処理で済む。

ショアはこれを使い量子コンピューターを用いれば多項式程度の計算で因数分解ができることを示した。

そのために前節の合同式を

$$f(x) \equiv a^x \mod N \tag{3.13}$$

として再定義する。

具体的に $N = 15$ の場合の量子回路を考えよう。そのために次のようなプログラムを考えればよい。

まず、N より小さく N と互いに素な数 a を探求する。ここでは

$$a = 7$$

とする。

次に合同式

$$y = f(x) = 7^x \mod 15 \tag{3.14}$$

を量子関数にすることを考える。天下り的ではあるが、ここでは変数 x は前節の結果から 4 まで調べれば求まったから 3qubit を使う。

さらに関数値も最大で 13 であったのでこれには 4qubit を使う。

よって変数 x_0, x_1, x_2 関数 y_0, y_1, y_2, y_3 を用意して式 3.12 の結果から 2 進表記で

$$y_0 = f(x = 0) = 7^0 \mod 15 = 1$$
$$y_1 = f(x = 1) = 7^1 \mod 15 = 7 = 111$$
$$y_2 = f(x = 10) = 7^2 \mod 15 = 4 = 100$$
$$y_3 = f(x = 111) = 7^3 \mod 15 = 13 = 1101$$

となるので次の表のように対応する。

x_0	x_1	x_2	y_0	y_1	y_2	y_3
0	0	0	0	0	0	**1**
0	0	1	0	1	1	1
0	1	0	0	1	0	0
0	1	1	1	1	0	1
1	0	0	0	0	0	1
1	0	1	0	1	1	1
1	1	0	0	1	0	0
1	1	1	1	1	0	1

図 3.25: [137] より

これらを X ゲートや CX ゲートをつかって作成する。
Qiskit では QASM が使えるのでいろいろリアルタイムで試行してつくることができる。
例えば次のような回路を QASM で作る。
上位 3 ビットが x、下位 4 ビットが y である。

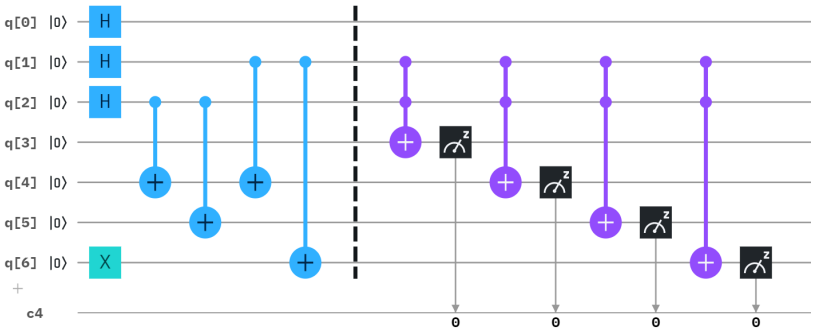


図 3.26: QSAM をつかった 15 の因数分解例

x では全てハダマールゲートを通して 1, 0 の重ね合わせにする。
こ k 3.3 から CNOT を使えば x レジスタに 0 を入力したときの y レジスタの出力が $f(x)$ そのものになった。
そのため第一ビットはそのままにして、x レジスタの第 2 ビットと第 3 ビットを CNOT の x ゲートに y レジスタを y ゲートに入れる。
最後に観測値を得るために y レジスタに CCX を利用して入れて、これを古典レジスタに入れ、観測値を得る。
この回路の実行例は次のようになる。

ただし、この結果はビットを反転して

$$0001 \to 1$$
$$0100 \to 4$$
$$0111 \to 7$$
$$1101 \to 13$$

に対応することに留意する。

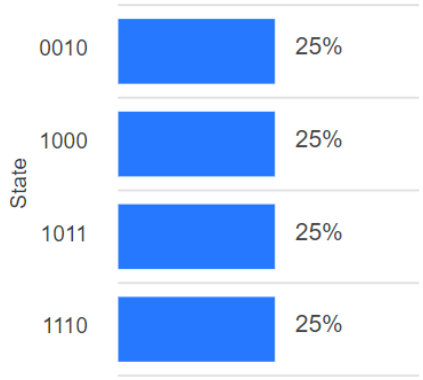


図 3.27: y レジスタの観測結果

結果は $\{1, 4, 7, 13\}$ の重ね合わせになっていることを表している。

次に周期を求める方法を考える。

一般的には合同式を満たす整数 r を探すために初期状態 $|0\rangle^{\otimes n} |1\rangle$ の第一レジスタに n 回アダマール変換を行う。

$$H^{\otimes n} |0\rangle^{\otimes n} |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^{n-1}} |x\rangle |1\rangle$$

ここで

$$f(x) \equiv a^x \mod N$$

を計算させて第 2 レジスタに書く。例えば

$$f(0) = 7^0 \mod 15 = 1$$
$$f(1) = 7 \mod 15 = 7$$
$$f(2) = 7^2 \mod 15 = 4$$
$$f(3) = 7^3 \mod 15 = 13$$
$$f(4) = 7^4 \mod 15 = 1$$
$$f(5) = 7^5 \mod 15 = 7$$
$$\cdots = \cdots$$
$$f(8) = 7^8 \mod 15 = 1$$

$$\frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^{n-1}} |x\rangle |a^x \mod N\rangle = \frac{1}{\sqrt{2^n}} [|0\rangle |1\rangle + |1\rangle |7\rangle + |2\rangle |5\rangle + |3\rangle |4\rangle + \cdots]$$

次に第 2 レジスタを観測して $a^r = 1 \mod N$ となる位数 r を探すと上の式から

$$r = 0, 4, 8, \cdots$$

この回路の例として Qikist を用いると次のようになる。

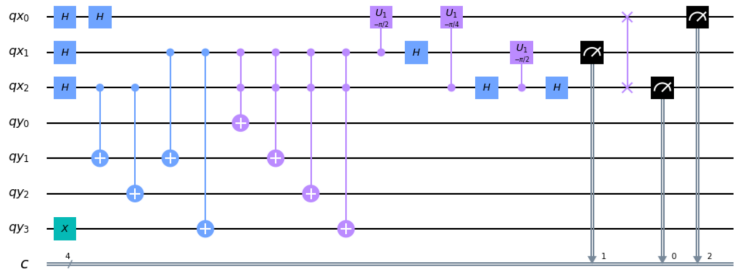


図 3.28: Shor のアルゴリズム:Qisikit による 15 の因数分解

3.6 量子フーリエ変換 [132]

前章での式の量子フーリエ変換をここで量子コンピューターに応用する。
q 個のデータ $u_0, u_1, \cdots u_{q-1}$ に重みをつけた和を

$$f_n = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} u_k e^{2\pi i n k/q} (n = 0, 1, \cdots q-1) \tag{3.15}$$

を考える。第 6 部での異なる波長、振幅の平面波の重ね合わせとみることができる。
この時に得られる $f_0 \cdots f_{q-1}$ を $u_0, \cdots u_{q-1}$ の**離散フーリエ変換**という。
また、逆変換を

$$u_k = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} e^{-2\pi i k n/q} (k = 0, 1, \cdots q-1) \tag{3.16}$$

と書くことができる。従って、f_n は u_k を

$$e^{-2\pi i k n/q} = \cos\left(\frac{2\pi n}{q} k\right) - i \sin\left(\frac{2\pi n}{q} k\right)$$

で展開しているときの係数とみなせる。これは角周波数

$$\omega_n = \frac{2\pi n}{q}$$

を単位ベクトルのように思えば、u_k はその成分に等しい。
このフーリエ変換を量子論理回路で実行することを**量子フーリエ変換** (quanrum_Fourier_transform) といい、**QFT** と呼ぶ。従って q 個の正規直交状態にあるベクトルに対し、$0 \leq k \leq q-1$ として、

$$U : |k\rangle \to \sum \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} e^{2\pi i k n/q} |n\rangle \tag{3.17}$$

と変換するユニタリ変換を見つければよい。これは、異なる波長の足し合わせでもあるが、無限和でないことに留意する。
しかし、前節で観測は環境の対角和をとったように、ある状態は双対する状態の全ての和をとらないといけない。
コンピューター上ではフーリエ変換はサンプリング数に留意がいるが、より高速な FFT のアルゴリズムを使うことができる。
例えば基底 $|a\rangle$ の成分が $u_0 \cdots u_{q-1}$ である状態ベクトル $|A\rangle$ を QFT で成分が $f_0 \cdots f_{q-1}$ の状態ベクトルに変換ができる。

$$|A\rangle = \sum_k u_k |a\rangle$$

とすると、式 3.17 は式 3.15 より

$$\begin{aligned}|B\rangle &= U|A\rangle \\ &= \sum_a u_a \left(\sum_n \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} e^{2\pi i a n/q} |n\rangle \right) \\ &= \sum_n \frac{1}{\sqrt{q}} \left(\sum_k u_k \sum_{n=0}^{q-1} e^{2\pi i a n/q} |n\rangle \right) \\ &= \sum_n f_n |n\rangle\end{aligned}$$

そこで 3bit の場合で具体的に考えてみよう。
この時、$q = 2^3 = 8$ になる。

$$a = 2^0 a_0 + 2^1 a_1 + 2^2 a_2$$

とし、変換後に

$$n = 2^0 n_0 + 2^1 n_1 + 2^2 n_2$$

となるとして、3 ビットの複合状態の変換を $2\pi m \to 0$ に注意して次のように計算できる。

$$\begin{aligned}|a_2 a_1 a_0\rangle \to \frac{1}{\sqrt{8}} \sum_{n_2=0}^{1} \sum_{n_1=0}^{1} \sum_{n_0=0}^{1} e^{2\pi i (a_0+2a_1+4a_2)(n_0+2n_1+4n_2)/8} |n_2 n_1 n_0\rangle \\ = \left(\frac{1}{\sqrt{2}} \sum_{n_2=0}^{1} e^{2\pi i (4n_2)(a_0+2a_1+4a_2)/8} |n_2\rangle_2 \right) \\ \otimes \left(\frac{1}{\sqrt{2}} \sum_{n_1=0}^{1} e^{2\pi i (2n_1)(a_0+2a_1+4a_2)/8} |n_1\rangle_1 \right) \\ \otimes \left(\frac{1}{\sqrt{2}} \sum_{n_0=0}^{1} e^{2\pi i (2n_0)(a_0+2a_1+4a_2)/8} |n_0\rangle_0 \right) \\ = \frac{1}{\sqrt{2}} \left(|0\rangle_2 + e^{2\pi i \cdot a_0/2} |1\rangle_2 \right) \\ \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_1 + e^{2\pi i \cdot (a_0/2+a_0/4)} |1\rangle_1 \right) \\ \otimes \frac{1}{\sqrt{2}} \left(|0\rangle_0 + e^{2\pi i \cdot (a_0/2+a_0/4+a_0/8)} |1\rangle_0 \right) \end{aligned} \tag{3.18}$$

となる。結果として $|0\rangle$ からの位相変化として、ブロッホ球内で $|1\rangle$ が回転していくとみなせる。
これらはテンソル積であり、bit 数が増えると計算も増えていく。
しかし、それが古典計算ほどではないことを示そう。
これを回路で表すことを考えてみよう。
最初の項を見ると $a_0 = 0$ の時に

$$\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$a_0 = 1$ の時には

$$\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

となるので、これは $|a_0\rangle$ のハダマール変換になっている。

$$|a_0\rangle \to H \to \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \cdot \frac{a_0}{2}} |1\rangle \right)$$

で表される。

次の項は $a_0 = 0$ の時に

$$e^{2\pi i \cdot a_0/4} = 1$$

$a_0 = 1$ の時には

$$e^{2\pi i \cdot a_0/4} = e^{\pi i/2} = i$$

となる。従って位相を $\pi/2$ ずらす必要が加わる。そこで 1.12 の位相ゲートを加えて次の図のようにつくる。

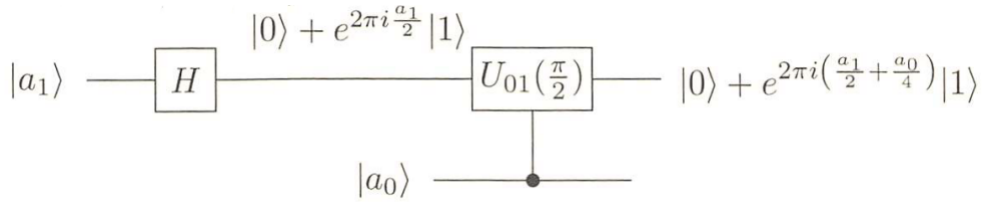


図 3.29: [132] より：$H + U_{01}$

同様に最後の項もさらに位相ゲートをたして次のようになる。

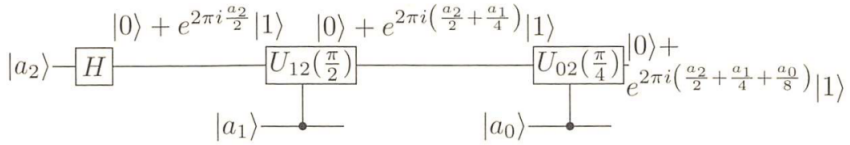


図 3.30: [132] より：$H + U_{01} + U_{12}$

よって、全ての項をまとめて式 3.18 は次のように書くことができる。
ただし、最後に上位ビットと下位ビットの反転をおこなう必要がある。

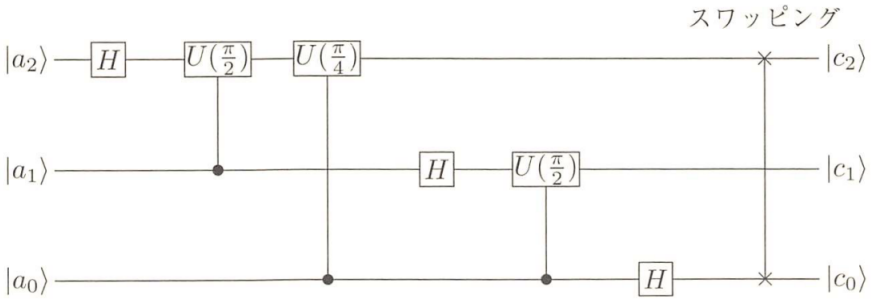


図 3.31: [132] より：3qubit のフーリエ変換

この 3qubit の FFT は次のように逐次計算で示すことがある。$u_0(0,0,0)$ と $u_4(1,0,0)$ から

$$u_0 + u_4, u_1 + W^4 u_4$$

をつくり、いったん保存し、以下図のように繰り返す。ただし、

$$W = e^{2\pi i/8} = (1+i)\sqrt{2}$$

であり、n ビットであれば 1 の n 乗根がかかる。この場合も上位と下位とを最後に反転する必要がある。

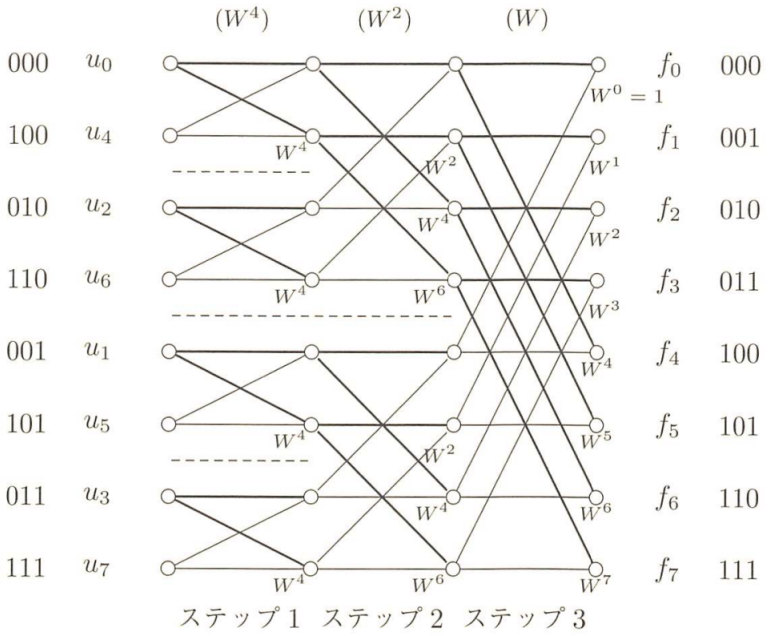


図 3.32: [130] より：3qubit の高速フーリエ変換

データが n bit、2^n ある場合、離散フーリエ変換の式 3.16 では $O(q^2) = O(2^{2n})$ の計算をすることになる。しかし、FFT が使えればステップが n 回になるので

$$q \log q = 2^n \times n \log 2 \sim n2^n$$

とできるから $O(n2^n)$ の計算まで減らすことができる。
ところが QFT ではさらに

$$n - \text{gates} \to (n-1)\text{gates} \to \cdots \to 1\text{gate}$$

までを 1 つの計算で終わらすことができる。よって全部で

$$O(n^2) = O\left((\log q)^2\right)$$

の計算で終わることになる。

3.7 ユニタリ変換 [98]

3.7.1 はきだし法

これまで見たように量子計算はユニタリ変換と観測のくみ合わせである。
これは固有値と演算子、ベクトルと組合わさる。固有方程式が無限に連結していくようなイメージであろうか。
古典論と異なり、我々は常に環境の影響を考えないといけない。そのためにどうしても制御線が 1 つ入り条件分離される。
ドイチらのグループにより、
任意のユニタリー変換が 2qubit の制御 NOT(CNOT) と、1qubit のユニタリー変換で表すとができることを示した。
これを**万能量子チューリングマシン**と呼ぶことにする。
この原理が、今後発展するであろう量子コンピューターの基本原理になる。そこでこのユニタリー変換の特性を見ておこう。

任意の $SU(2)$ 行列を U とする。CNOT を 2 つ、1qubit を 3 つのユニタリー行列を A, B, C とする。
これから次の図のような一般化制御 U ゲートが作れる。

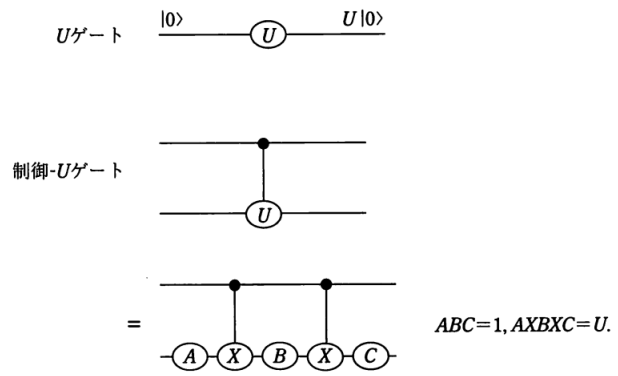


図 3.33: [98] より：制御 U ゲートのユニタリ変換での表現

つまり、制御 U ゲートは 2 つの制御 NOT ゲート X を挟んで連結するようにユニタリ変換が 3 つ入る。
一般的な $SU(2)$ は 3 次元の空間回転に対応できたから、第 2 部の角運動量で学んだオイラー回転をもちいて

$$U = R_z(\alpha)R_y(\beta)R_z(\gamma)$$

と表すことができる。ユニタリーの条件 3 つの行列 A, B, C については

$$ABC = \mathrm{I}, AXBXC = U \tag{3.19}$$

を満たすので

$$A = R_z(\frac{\alpha-\gamma}{2}), B = R_z\left(-\frac{\alpha+\gamma}{2}\right)R_y\left(-\frac{\beta}{2}\right), C = R_y\left(\frac{\beta}{2}\right)R_z\left(\gamma\right)$$

とすれば条件式 3.19 を満たす。
さらに、全体に位相ゲート 1.12 をかけても問題ない。

定義. 基本原理 1 : 1bit のユニタリー変換と 2bit の CNOT ートの組合わせが任意のユニタリー変換をつくる。

証明は次のように任意の 2bit の場合で示す。

Proof. まず任意の基底 $|1\rangle|1\rangle$ を任意の次の状態に変換する回路を考える。{} はあらゆる要素の組合わせをとるとして、

$$|1\rangle|1\rangle \to \sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle, c_{ab} \in \mathbb{C}$$

ただし、次のように規格化されている。

$$\sum_{a,b=\{0,1\}} |c_{ab}|^2 = 1$$

この逆変換を

$$\phi_{11} : \sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to |1\rangle|1\rangle \tag{3.20}$$

とする。

任意の CNOT ゲートを式 1.17 から基底をブロッホ球の全軸

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

を基底にとる。この恒等部分行列は次のように 2 通りでユニタリ行列の中に入れることができる。
第 1bit を制御 bit、第 2bit を標的 bit に選ぶと

$$U_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}$$

とおける。同様にして第 2bit を制御 bit、第 1bit を標的 bit に選ぶと

$$V_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & v_{11} & 0 & v_{12} \\ 0 & 0 & 1 & 0 \\ 0 & v_{21} & 0 & u_{22} \end{pmatrix}$$

となる。ただし、u, v は $1, 0$ の値しかとらない。
これらは既に式 1.15 などで、1bit のユニタリー変換と CNOT で表すことができたから
基底を先にもやったように $|0\rangle|0\rangle, |0\rangle|1\rangle$ と $|1\rangle|0\rangle, |1\rangle|1\rangle$ に分けて考える。
はじめに第 1bit を制御、第 2bit をターゲットにする U_{12} を用いると、

$$U_{12} \to \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ Ub \end{pmatrix}$$

とみなして $|1\rangle|1\rangle$ を掃き出すと

$$\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to \sum_{a=\{0,1\}} c_{a1}|a\rangle|1\rangle \to |1\rangle|1\rangle$$

のようにすすめると

$$|c_{10}|^2 + |c_{11}|^2 + |c_{01}|^2 + |c_{00}|^2 = 1$$

$$|c_{11}|^2 = |c_{01}|^2 + |c_{00}|^2 = 1$$

$$\sum_{a,b=\{0,1\},a,b=(1,0)} c_{ab}|a\rangle|b\rangle = c_{10}|1\rangle|0\rangle + c_{11}|1\rangle|1\rangle$$

となり、

$$U_{12}(c_{10}|1\rangle|0\rangle + c_{11}|1\rangle|1\rangle) = c_{10}|1\rangle|1\rangle + c_{11}|1\rangle|1\rangle$$

が成り立つので U_{12} を使うと式 3.20 から

$$\begin{aligned} U_{12}\psi_1 &= U_{12}\left(\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle\right) \\ &= \sum_{a,b=\{0,1\},a,b\neq(1,0)} c_{ab}|a\rangle|b\rangle + \sqrt{|c_{10}|^2 + |c_{11}|^2}|1\rangle|1\rangle \end{aligned}$$

となる。
次に $|0\rangle|1\rangle$ を掃き出すと

$$U_{12}\left(c_{00}|0\rangle|0\rangle + c_{01}|0\rangle|1\rangle\right) = c_{00}|0\rangle|1\rangle + c_{01}|0\rangle|1\rangle$$

$$U_{12}\psi_1 = \sum_{a,b=\{0,1\},a,b\neq(1,0)} c_{ab}|a\rangle|b\rangle + \sqrt{|c_{00}|^2+|c_{01}|^2}\,|0\rangle|1\rangle$$

次に第 1bit に NOT を書けて同様に $|0\rangle|0\rangle$ を書き出すと

$$\sqrt{|c_{00}|^2+|c_{01}|^2}\,|0\rangle|1\rangle + \sqrt{|c_{10}|^2+|c_{11}|^2}\,|1\rangle|1\rangle$$

となる。
最後に第 2 ビットを制御ビット、第 1 ビットを標的にする V_{21} を用いて $|0\rangle|1\rangle$ を掃き出すと $|1\rangle|1\rangle$ が得られる。
つまり、次が全て得られる。

$$\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to |0\rangle|0\rangle$$
$$\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to |0\rangle|1\rangle$$
$$\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to |1\rangle|0\rangle$$
$$\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to |1\rangle|1\rangle$$

□

例えば、

$$\sum_{a,b=\{0,1\}} c_{ab}|a\rangle|b\rangle \to |1\rangle|1\rangle$$

の回路図は次のようになる。

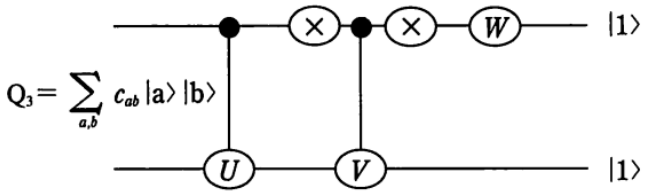


図 3.34: [98] より：$|1\rangle|1\rangle$ を作る回路

3.7.2 基本原理

任意の 2 ビットのユニタリー変換 S の固有ベクトルを $|\psi_n\rangle, n = 0,1,2,3$ とする。
ここでは標準基底を $\{|n\rangle\}$ で表す。

$$\{|0\rangle = |0\rangle|0\rangle, |1\rangle = |0\rangle|1\rangle, |2\rangle = |1\rangle|0\rangle, |3\rangle = |1\rangle|1\rangle\}$$

先の結果から基底をつくるユニタリー変換が存在し、

$$G(\psi_n)|\psi_n\rangle = |n\rangle$$

とおく、これを用いてユニタリー行列は

$$S = \prod_{n=0}^{3} G\left(\psi_n\right)^{-1} X_n G(\psi_n)$$

と書くことができる。
これは次のように示すことができる。X_n は CU と NOT を組み合わせてつくることができて、
パウリ行列を用いて、回転を表すと、

$$\begin{aligned}
X_0 &= e^{i\sigma_0} |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| \\
X_1 &= |0\rangle\langle 0| + e^{i\sigma_1} |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| \\
X_2 &= |0\rangle\langle 0| + |1\rangle\langle 1| + e^{i\sigma_2} |2\rangle\langle 2| + |3\rangle\langle 3| \\
X_3 &= |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + e^{i\sigma_3} |3\rangle\langle 3|
\end{aligned}$$

のように書くことができる。
まず、$G\left(\psi_0\right)^{-1} X_0 G(\psi_0)$ はユニタリ変換であり、第 4 部で見たようにこれは回転の演算子と見なせるから

$$G\left(\psi_0\right)^{-1} X_0 G(\psi_0) |\psi_0\rangle = e^{i\sigma_0} |\psi_0\rangle$$

$$e^{i\sigma_0} |0\rangle = |0\rangle$$

が成り立つ。そこでこれを $|\psi_n\rangle$ の状態に作用させると、完全性の条件 $\sum_n |n\rangle\langle n| = I$ から

$$\begin{aligned}
G\left(\psi_0\right)^{-1} X_0 G(\psi_0) |\psi_n\rangle &= G\left(\psi_0\right)^{-1} \left(e^{i\sigma_0} |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|\right) G(\psi_n) |\psi_n\rangle \\
&= G\left(\psi_0\right)^{-1} \left(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|\right) G(\psi_n) |\psi_n\rangle \\
&= G\left(\psi_n\right)^{-1} G(\psi_n) |\psi_n\rangle \\
&= |\psi_n\rangle
\end{aligned}$$

となる。従って、一般に

$$G\left(\psi_m\right)^{-1} X_m G(\psi_m) |\psi_m\rangle = e^{i\sigma_m} |\psi_m\rangle$$

$$G\left(\psi_n\right)^{-1} X_n G(\psi_n) |\psi_n\rangle = e^{i\sigma_m \delta_{nm}} |\psi_m\rangle$$

$$e^{i\sigma_n \delta_{mn}} |m\rangle = |m\rangle$$

が成り立つ。
今 $|\psi_m\rangle$ は S の任意の固有ベクトルであるが、S が $|\psi_m\rangle$ に作用すると、$n = m$ のところだけ位相が変化し、後は恒等変換である。
選択的に位相変換されることはある方向に対し、変化が伝達する。従って、

$$S |\psi_m\rangle = e^{i\sigma_m} |\psi_m\rangle \ \ (m = 0, 1, 2, 3)$$

が成り立ち、これから

$$S = \prod_{n=0}^{3} e^{i\sigma_n} |\psi_n\rangle\langle\psi_n| = \prod_{n=0}^{3} G\left(\psi_n\right)^{-1} X_n G(\psi_n)$$

が示された。
これを回路図で表すと次のように、量子回路 Q_n は G と CNOT から作ることができる。

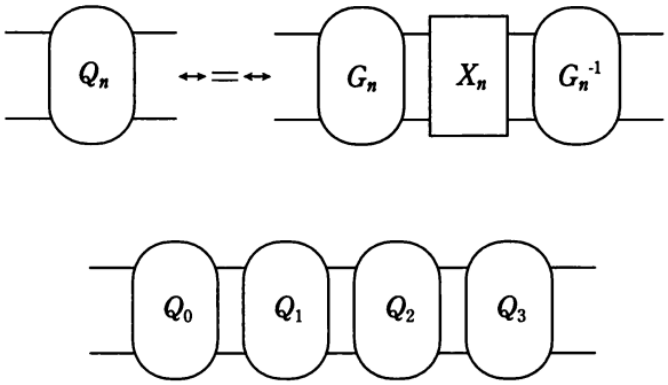


図 3.35: [98] より：量子回路の中身

3.8 並列計算例

CNOT と 1qubit の組み合わせで、量子的なエンタングルド状態を作る例として

$$|a\rangle\,|b\rangle\,|0\rangle \to |a\rangle\,|b\rangle\,|a+b \mod 2\rangle$$

をもう一度見てみよう。すでに式 1.11 で見たように次のような回路を作ればよい。

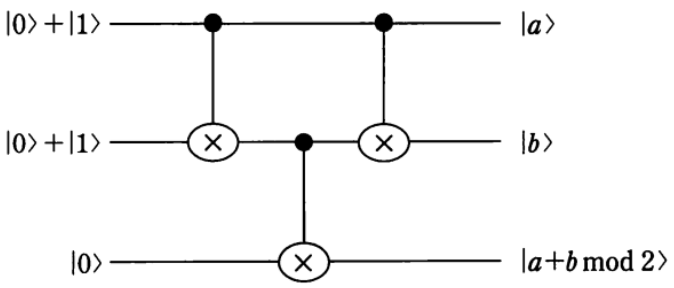


図 3.36: [98] より：並列計算例

この時の出力は最終状態が掛け合わされ、

$$\sum_{a,b} |a\rangle\,|b\rangle\,|a+b \mod 2\rangle$$

となる。この回路には CNOT が 3 つ入っている。量子回路は左から右に時間進行するので、順に見ていく。

はじめに左の CNOT で $a+b \mod 2$ を第 2 ビットに計算し、次の CNOT でこれを第 3 ビットにコピーしている。

そして最後の CNOT は第 2 ビットを元にもどすことをする。最終結果がそれぞれのビットの**テンソル積**になる。

一見すると何気ないかもしれないが、古典的なコンピューターでは 1 つ 1 つ掛けて演算する処理を量子コンピューターは 1 度におこなうことができることをしめしている。これを**平行処理**という。量子コンピューターの優れた特徴になる。

つまり、

$$\sum_{a,b=0,1} |a\rangle\,|b\rangle\,|0\rangle \to \sum_{a,b=0,1} |a\rangle\,|b\rangle\,|a+b \mod 2\rangle$$

は上図のように入力を

$$|0\rangle + |1\rangle$$

が許されるので、これをアダマール変換でつくれば

$$|0\rangle|0\rangle|0\rangle \to \left(\frac{1}{\sqrt{2}}\right)^2 \sum_{a,b=0,1} |a\rangle|b\rangle|0\rangle$$
$$\to \left(\frac{1}{\sqrt{2}}\right)^2 \sum_{a,b=0,1} |a\rangle|b\rangle|a+b \mod 2\rangle$$

となる。ただし、この回路には観測が入っていないので、$a+b \mod 2$ は見えていない。
観測するためには古典ゲートをプラスして、観測器をつければよい。

3.8.1 CNOT の拡張

前節で CNOT を使うことが量子コンピューターの特徴であることを見たが、ここでは、この CNOT で 2 つの制御をかけることを考える。

3qubit の場合を考えて、2 個の制御ビット、1 つの標的ビットをつくり、制御ビットが 2 つとも $|1\rangle$ であれば標的ビットを反転させる。

逆に残りのパターン

$$|1\rangle|0\rangle, |0\rangle|1\rangle, |0\rangle|0\rangle$$

の時は標的ビットは変化しない。

これを実現していくためにまず次の恒等式に注意する。

$$x + y - (x \oplus y) = 2xy$$

ただし、

$$(x \oplus y) \equiv x + y \mod 2$$

で定義する。明らかに

$$x + y - (x + y \mod 2) = y - y \mod 2$$

3.8.2 具体例 1 + 1

もっとも単純な 1 + 1 の量子計算をみておくことは教育的である。

2 進法でおこなうので前章でみた、全加算器の桁上げを処理する必要がある。

そのために次のような回路を考える。

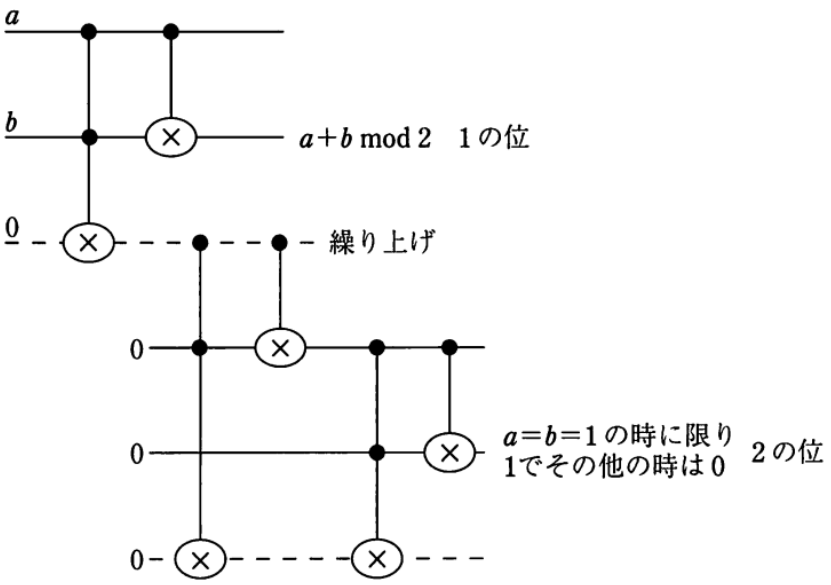


図 3.37: [98] より：1 の足し算

これは CNOT を利用しているので、古典的な処理ではなく、重ね合わせを用いて

参考文献

[1] 菅野礼治　**ゲージ理論の解析力学**　2007

[2] G.M. ザスラフスキー　三島信彦、斉藤徹也、新藤　茂　訳　1989 **カオス-古典および量子力学系-**

[3] 内山龍雄　**相対性理論**　1977　岩波全書

[4] Tristan Needham **Visual complex analysis**　1997　培風館

[5] J.W.Noh, A.Foug'eres, and L.Mandel **Operational approach to the phase of quantum field** 1992 Physical Review A 45

[6] D.T.Pegg, S.M.Barnett **Phase properties of quantized single-mode electromagnetic field** 1989 Physical Review A 39

[7] 小林昭七　**接続の微分幾何とゲージ理論** 1989　裳華房

[8] 野水克己　**現代微分幾何入門**　1969　裳華房

[9] 佐藤光　**群と物理**　1992　丸善株式会社

[10] Tristan Needham **Visual Complex Analysis** 1997 OXFORD

[11] 小沢哲也　**曲線・曲面と接続の幾何**　1997 倍風館

[12] 中原幹生　**理論物理学のための幾何学とトポロジー I,II**　2000 ピアソン・エデュケーション

[13] 丹羽雅昭　**超伝導の基礎**　2002 東京電機大学出版局

[14] 矢吹治一　**量子論における位相**　1998　日本評論社

[15] Tai Tsun Wu,Chen Ning Yang **Concept of nonintegrable factors and global formulation of gauge fields** 1975 Physical Review D 12

[16] R.Glies **Reconstruction of gauge potentials from Wilson loops** 1981 Physical Review D 24

[17] Pratul Bandyopadhyay **Geometry,Topology and Quantum Field Theory**

[18] 深谷賢治 **双曲幾何** 岩波書店 2004

[19] Shinichi Deguchi Kazuo Fujikawa **Second-quantized formulation of geometric phases** 2005 Physical Review A72

[20] 大貫義朗 鈴木増雄 柏太郎 **経路積分の方法** 岩波 現代の物理学

[21] 柏 太郎 サイエンス社 **新版 演習 場の量子論**

[22] J.David Jackson **Classic Electrodynamics** 2001

[23] 中村 哲・須藤彰三 **電磁気学** 朝倉書店 2012

[24] Matthew N.O. **Elements of Eletromagnetic**

[25] **Lectures on Clifford(Geometric) Algebras and Appliations** Rafal Ablamowicz Garret Sobczyk 2003

[26] Julian Schwinger **シュウインガ──量子力学** Springer 2000

[27] 野村健太郎 **トポロジカル絶縁体・超伝導体の基礎理論** September 11, 2013

[28] 安藤陽一 **トポロジカル絶縁体入門** 2014

[29] Brian R. Greene **STRING THEORY ON CALABI-YAU MANIFOLDS** Columbia University

[30] 深谷 賢治 **ゲージ理論とトポロジー** 1995 Springer

[31] Joseph L.Birman **Geometry,Particles,and Fields** Springer

[32] Charles Nash Sinddhartha Sen **Topoloy and geometry for Physics** Mineola,New York

[33] 二木 昭人 **微分幾何講義-一般理論と現代物理への応用** サイエンス社

[34] Andre Weil **ケーラー多様体論入門** 1958 Springer

[35] 天野勝利 **Hopf 代数とは** 筑波大学

[36] 谷村省吾 **トポロジー・圏論・微分幾何** サイエンス社 SGC-52

[37] 坪井 俊 **幾何学３ 微分形式** 東京大学出版

[38] Louis H.Kauffman **KNOTS AND PHYIC**S World Sientific 1993

[39] 服部昌夫 **多様体のトポロジー** 岩波 2003

[40] David W. Lyons **An Elementary Introduction to the Hopf Fibration** Lebanon Valley College

[41] Nicholas Wheeler **Transformational principles latent in the theory of CLIFFORD ALGEBRAS** Reed College Physics Department 2003

[42] Mathematica Demonstration Richard Hennigan **Rotating the Hopf Fibration** http://www.wolfram.com/

[43] Ana Cannas da Silva **Lectures on Symplectic Geometry** 2006

[44] **Rotations of the three-sphere and symmetry of the Cliford Torus** John McCuan and Lafe Spietz October 5,1998

[45] Maris Ozols **Geometry of qubit** 2007

[47] Rupert Way **Dynamics in the Hopf bundle, the geometric phase and implications for dynamical systems** University of Surrey U.K 2008

[48] Chris J Isham **Modern Differential Geometry for Physicists**

[50] Robert Gilmore **Lie Groups, Lie Algebras,and Some or Their Applications**

[51] Bo-Yu Hou, Bo-Yuan Hou **DIFFERRENTIAL GEOMETRY FOR PHYSICS** World Scientific 1997

[52] Thomas J.Briidges **The Orr-Sommerfeld equation on a manifold**

[53] 佐古彰史　**超対称性ゲージ理論と幾何学**　2007 日本評論社

[54] 早川尚男　**連続体力学**　京都大学大学院　平成 17 年

[55] 岡部洋一　**電磁気学**　放送大学 2015

[56] Bjorn Felsager **Geometry,Particles,and Fields** Springer 1997

[57] 及川正行　**偏微分方程式**　岩波書店 1955

[60] 三尾典克　**変形体の力学**　東京大学

[61] Daniel Z.Freedman and Antoine Van Proeyen **Supergravity** CAMBRIGE

[62] V.P Nair **Quantum Field Theory** 2005 Springer

[63] **Diagrammatica The Path to Feynman Rules** Martinus Veltman 1995 Cambride University Press

[64] Martin Ammon Johanna Erdmenger **Gauge/Gravity Duality: Foundations and Applications** 2005 Cambride University Press

[65] Kawamura Yoshiharu **相対論的量子力学**　裳華房

[66] 泰泉寺雅夫 **数物系のためのミラー対称性入門**　2014　サイエンス社

[67] 堀川穎二　**複素代数幾何学入門**　岩波書店

[68] Shiing-shen Chern **Complex Manifolds Without Potential Theory** 1995 Springer Verlag New York,LLC

[69] 安藤哲也　**コホモロジー**　2002 日本評論社

[70] Joseph Polchinski **String Theory I,II** Cambride University Press 1998

[71] 坂本眞人 **量子力学から超対称性へ** SGC ライブラリ 96 2012 サイエンス社

[72] Barton Zwiebach **A First Course in STRING THEORY** 2009 Cambride University Press

[73] 深谷 賢治 編 **ミラー対称性入門** 2009 日本評論社

[74] 白水 徹也 **アインシュタイン方程式** 2012 SGO ライブラリ サイエンス社

[75] 唐木田健一 **ひとりで学べる一般相対性理論** 講談社 2015

[76] 深谷賢治 **数学者による数学者のための StrigDualit**y 京都大学

[77] 坪井 俊 **幾何学▯ ホモロージ入門** 東京大学出版会

[78] 佐藤秀司・佐藤周友 **代数的サイクルとエタールコホモロジー** Springer 2012

[79] 石橋延幸・村上公一 **弦の場の理論** 2012 SGO ライブラリ サイエンス社

[80] 伊藤克司 **共形場理論** 2011 SGO ライブラリ サイエンス社

[81] 高柳 匡 **ホログラフィー原理と量子エンタングルメント** サイエンス社

[82] 江沢 洋、渡辺敬二、鈴木増雄、田崎晴明 **繰り込み群の方法** 1999 岩波書店

[83] 今村 洋介 **超弦理論の基礎** 2010 SGO ライブラリ サイエンス社

[84] 江口 徹 菅原 祐二 **共形場理論** 2015 岩波書店

[85] 西森 秀稔 **相転移・臨界現象の統計物理学** 倍風館

[86] Michael E.Peskin, Daniel V.Schroeder **An introduction to quantum Field Theory**

[87] Charles Kittel and Herbrt Kroemer **THERMAL PHYSICS** W.H.Freeman and Company 1980

[88] J.J Sakurai **Modern Quantum Mechanics** 1985 The Benbjamin/Cumming Publishng Company,Inc.

[89] 松田 哲 **複素関数** 理工系の基礎数学 5 岩波書店 1995

[90] 小林 昭七 **複素幾何** 岩波書店 2005

[91] 早川 尚男 **非平衡統計力学** サイエンス社 SGC ライブラリ 2006

[92] Mukund Rangamani & Tadashi Takayanagi **“Holographic Entanglement Entropy“** 2017

[93] 松枝 宏明 **量子系のエンタングルメントと幾何学** 森北出版 2016

[94] 治部眞里 高橋康 **添削形式による場の量子論** 日本評論社 1997

[95] V.P. ナイア著 阿部泰裕 磯暁 訳 **現代的視点からの場の量子論** Springer 2005

[96] 大津 元一 **現代光科学 ▯、▯ 光の物理的基礎** 朝倉書店 1994

[97] 日置 善郎 **相対論的量子場** 吉岡書店 2008

[98] 細谷 暁夫 **量子コンピューターの基礎** サイエンス社 1999

[99] Michael A. Nielsen & Isaac L. Chuang **Quantum Computation and Quantum Information** Cambride University press 2010

[100] Brian C.Hall **Lie Groups,Lie Algebras, and Represetations An Elementary Introduction** Springer 2015

[101] 谷村省吾 **ホロノミーと力学系** 名古屋大学

[102] Raffaele Rani **On Parallel Transport and Curvature** 2009

[103] 塩濱 勝博, 成 慶明 **曲面の微分幾何学** 日本評論社 2005

[104] 大槻 知忠 **結び目の不変量** 共立出版 2015

[105] 鈴木 増雄 **統計力学** 岩波書店 1994

[106] Anastasios Mallios **MODERN DIFFERENTIAL GEOMETRY IN GAUGE THEPRIES** Springer 2009

[107] **Lectures on Geometry** Edited by N.M,J.WOODHOUSE OXFORD university press 2017

[108] 田中利夫・村上斉 **トポロジー入門** サイエンス社 SGC ライブラリ 42 2005

[109] 川村嘉春 **基礎物理から理解するゲージ理論** サイエンス社 SGC ライブラリ 42 2017

[110] 細谷 裕 **ゲージヒッグス統合理論** サイエンス社 SGC ライブラリ 42 2018

[111] 堺井義秀 山田憲和 野尻美保子 **素粒子物理学** KEK 2012

[112] 鈴木 増雄 **経路積分と量子解析** サイエンス社 2017

[113] David Tong **Quantum Field Theory** Universith of Cambridge 2006

[114] 並木美喜雄 大場一郎 **散乱の量子力学** 岩波書店 1997

[115] 福田礼次郎 **フーリエ解析** 岩波書店 1995

[116] Adam Lupu-Sax **Quantum Scattering Theory and Applications** Harvard University 1998

[117] 佐藤文隆 児玉英雄 **一般相対性理論** 岩波書店 1992

[118] 松本幸夫 **多様体の基礎** 東京大学出版 1989

[119] Wulf Rossmann **Lie Groups** OXFORD 2002

[120] 佐武一郎 **リー群の話** 日本評論社 1982

[121] F. シャトラン **行列の固有値** Springer 1988

[122] 生西明夫 中神☒臣 **作用素環入門 1** 岩波 2006

[123] 黒田成俊 **関数解析** 共立出版 1980

[124] 堀田昌寛 **量子情報と時空の物理** 第 2 版 サイエンス社 2019

[125] 砂田利一 **行列と行列式** 岩波 2003

[126] 太田 浩一 **電磁気学の基礎☒☒** 東京大学出版会 2013

[127] J. マトウシェク著 岡本吉央訳 **離散幾何学講義** 丸善 2001

[128] 根本香絵　**量子力学の考え方　物理で読み解く量子情報論の基礎**　サイエンス社　2008

[129] 甘利　俊一　**情報幾何学の新展開**　サイエンス社　2014

[130] Michael A.Nielsen Isaac L. Cauang **Quantum Computation and Quantum Information**

[131] 佐川弘幸/吉田宣章 **量子情報理論　第 3 版**　丸善　2019

[132] Leo.P.Kadanoff and Gordon Baym 1962 **量子情報理論**　丸善プラネット

[133] Rodney Loudon **The quantum theory of light** Oxford University Press 1983

[134] Leo.P.Kadanoff and Gordon Baym **Quantum Statistical Mechanics** PerseusBooks Publishing 1962

[135] 長島順清 **粒子と場** 大阪大学

[136] MARK THOMSON **Modern Particle Physics** University of Cambridge 2013

[137] 中山　茂　Qsikit 量子プログラミング入門　Gaia 教育シリーズ 17 2019