**量子プログラミング入門**

**－前提知識とJavaScriptシミュレータによる実践－**

Masayuki Otoshi

courseml@gmail.com

***Revision History***

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Name** | **Date** | **Description** |
| 1.00 | Masayuki Otoshi | 8/1/2015 | Document Created |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. はじめに 3](#_Toc426186002)

[2. 量子計算 4](#_Toc426186004)

[量子ビット(qubit) 4](#_Toc426186005)

[重ね合わせ状態 5](#_Toc426186006)

[二次元複素ベクトル表現 8](#_Toc426186007)

[確率振幅 9](#_Toc426186008)

[複数qubitの計算 11](#_Toc426186009)

[観測する 16](#_Toc426186010)

[エンタングルメント状態（量子もつれ） 18](#_Toc426186011)

[2. 量子論理ゲート 20](#_Toc426186014)

[パウリXゲート（NOTゲート） 20](#_Toc426186015)

[アダマール(Hadamard)ゲート 21](#_Toc426186016)

[3. Function 22](#_Toc426186018)

[Ufゲート 22](#_Toc426186019)

[超並列実行 24](#_Toc426186020)

[4. JavaScriptシミュレータによる量子プログラミング 26](#_Toc426186022)

[クラス図 26](#_Toc426186023)

[NOT演算 29](#_Toc426186024)

[テンソル積 31](#_Toc426186025)

[qubitの観測 33](#_Toc426186026)

[エンタングルメント状態の観測 36](#_Toc426186027)

[パウリXゲート 38](#_Toc426186028)

[アダマールゲート 39](#_Toc426186029)

[Functionの実行 41](#_Toc426186030)

[5. Deutsch's algorithm 44](#_Toc426186032)

[アルゴリズムの概要 44](#_Toc426186033)

[JavaScriptでの実装 45](#_Toc426186034)

[量子コンピュータでの実装 47](#_Toc426186035)

[6. おわりに 52](#_Toc426186042)

# はじめに

プログラミングを初めて学んだ頃を思い出して欲しい。おそらく、2進数での数え方やAND、ORなどのビット演算を学習したはずである。特に1+1が1になるというOR演算は、それまでの数学で学んだ常識を覆すインパクトがあり、不思議な印象を受けたことと思う。このように、我々は何か新しいことを学ぶ時、その世界の常識を理解することから始めなければならない。そして、まさに今、新たな常識がプログラミングの世界に押し寄せようとしている。それが量子コンピュータ上でのプログラミングである。

現在のコンピュータ（以降、古典コンピュータと呼ぶ）では、電圧の高低をビットの1, 0に割り当てて表現したが、量子コンピュータでは、電子の回転（スピン）方向や光子(Photon)の偏向方向といった量子の状態に対して、ビットを割り当てていく。量子のように極小の世界になると、我々の住む世界の常識が通用しない。例えば、ある一個の電子の回転方向が、ある一瞬において上向きであり、かつ下向きである、という複数の状態が同時に存在可能なのである。これは、あなたが空を見上げつつ地面を見るという、相反する行為を同時に行うことが可能だと言っていることに等しい。

そうした奇妙な量子の現象が量子コンピュータの動作原理となっているため、古典コンピュータでのプログラミングに慣れたプログラマーにとっては、理解し難いかもしれない。また、使われている用語が量子力学から拝借したものが多い点も更にハードルを高めている。

現時点では、量子コンピュータはまだ基礎研究の段階であり、実用的プログラムを書くというレベルではない。しかしながら、量子コンピューティングの基本原理は既に数理モデルにより明確に定義されており、それに基づいて開発されたシミュレータを用いることで量子プログラミングを体験することが可能である。ただ、量子プログラミングを始めるには、ある程度の量子力学および数学の知識が必要となる。それは、我々が古典コンピュータに対して、2進数や論理演算を学ぶことから始めたようなものだと理解して欲しい。

とは言え、現時点での量子プログラミングは非常に原始的な操作の羅列に過ぎず、それは、ちょうどアセンブラによるプログラミングを行っているレベルだと思って差し支えない。今後、より高度で複雑な実用的プログラミングへと発展させるために、我々には量子プログラミングにおける高級言語やフレームワークを考案していく責務があるものと思う。

そこで、本稿では古典コンピュータでのプログラミング経験はあるが、量子コンピュータや量子力学については初めて、という方を対象にしている。量子コンピュータ上でのプログラミングに必要な基礎知識だけでなく、JavaScriptで書かれたシミュレータを用いて具体的なコードとその実行結果も紹介しながら説明していく。



# 量子計算

## 量子ビット(qubit)

古典コンピュータでの1ビットに相当する単位を、量子コンピュータではqubitと言う（または、 Qbit、 量子ビットとも言う）。1ビットは0または1の値を持つが、1 qubitはそれらに対応する状態 (state) を |0> または |1> で表現する。

余談だが、|0>は「0ケット」と読み、qubitの状態が|0>であることを示す。同様に、|1>は「1ケット」と読み、状態が|1>であることを表している。このケットという呼び名はbracketが由来で、|>はbracketの右半分なので「ket」と呼ばれている。ここでは出てこないが、<0|という状態もあり、こちらはbra（ブラ）と呼ぶ。

ところで、古典コンピュータでの0と1は電圧の低い（基準値）と高い状態に対応したものだが、qubitの「状態」とは具体的に何なのであろうか？それは、量子コンピュータを構築する実体に依存する。例えば、電子のスピンで表現した場合、電子が右回りしている状態を基準にしたとすると、上向きに回転している状態を|0>、下向きに回転している状態を|1>と定義できる。また、光子(photon)を用いた場合は、光子を偏向させた向きで表現する。例えば、x軸方向を向いた状態を|0>、y軸方向を向いた状態を|1>と定義できる。

**|1>**

**|0>**

## 重ね合わせ状態

qubitは|0>、|1>と決まった値をとる状態（独立の状態）だけでなく、それらが重ね合わさった状態もとることができる。それら全ての状態を|ψ>で表し、以下の式で定義される。

|  |  |
| --- | --- |
| |ψ> = α|0> + β|1> | 式(1) |

ただし、α、βは**複素数**（実数と虚数で構成され、a+biで表される数）であり、以下の条件（**規格化条件**）を満たすものとする。

|  |  |
| --- | --- |
| |α|2+|β|2 = 1 | 式(2) |

具体的には、αは|0>の確率振幅(probability amplitude)、βは|1>の確率振幅を表しており、このqubitを観測すると|α|2の確率で|0>になり、同様に|β|2の確率で|1>になることを示している。しかし、ひとたび観測すると0または1の値に収束する。

これらの式が意味する内容を理解することは、非常に重要である。そこで、qubitを平面上の単位ベクトルとして図示してみよう。横軸を|0>、縦軸を|1>とすると以下のように描かれる。

|0>

|1>

α|0> + β|1>

β

α

つまり、qubitの「状態」とは大きさ1のベクトルであり、「演算」とはこの単位円の円周上を動き回ること、と言える。

さて、重ね合わせのない独立した状態である|0>や|1>もこれらの式で表現できる。例えば|0>はα=1, β=0の状態と言え、同様に、|1>はα=0, β=1の場合を示している。図示すると以下のようになる。

|0>

|1>

|1>

|0>

これに対し、重ね合わさった状態はベクトルの向きが水平や垂直でなく、傾いた状態と言える。つまり、式(2)の規格化条件「 |α|2+|β|2 = 1」を満たすαとβであれば、いかような比率でのブレンドも可能なので、重ねあった状態は無限に多数存在しえるのである。ここでは、その一例として1/2の確率で|0>、残りの1/2の確率で|1>かもしれない状態を示そう。

まず、確率|α|2、および|β|2がそれぞれ1/2であるので、

|α|2 = |β|2 =

となり、α = 、β = であることが分かる。そこで、この|0>と|1>が半々の確率で存在するqubitは以下の式で表される。

|0> + |1>

これを先ほどのベクトルの単位円にあてはめると、|0>軸方向の成分は「半径 \* cosθ」、|1>軸方向の成分は「半径\*sinθ」で求められるが、単位円の半径は1なので、結局、傾いた角度θが分かれば、α、βは以下のように求まる。

α = cosθ, β=sinθ

今、|0>と|1>が1/2ずつの確率で表される状態のα、βはどちらもなので、

cosθ=, sinθ=

であることが導き出され、sin, cosがともにとなるθはラジアン、つまり、45度の方向を指していることが分かる。これは|0>を反時計回りに45度回転させた状態である。

|0>

|1>

|0> + |1>

この重ね合わせ状態を電子のスピンに置き換えて考えてみた場合、電子はどちらを向いているのだろうか？先に定義したように、ここでも上向き回転を|0>、下向き回転を|1>とする。上図のようにベクトルは|0>と|1>の中間を向いているので、電子は上向きと下向きの中間、つまり横向きに回転している、と考えるかもしれない。

**これが、|0> + |1> なの?**

この問いに対する量子力学の答えは、そうかもしれないし、そうでないかもしれない、である。実のところ、電子がどの向きに回転しているかは観測するまで分からない。もしくは、全ての方向を向いて回転している、とも言える。しかし、全く分からないのかというと、そうではなく、だいたいどの方向に向いているか確率で割り出せる。

説明を簡単にするために、ここでは電子は上向き、下向きの二方向にしか回転しないものとしよう。そして、電子の回転方向を十分に多い回数、例えば1万回観測したとする。すると、「|0> + |1>」で表される状態では、5000回上向きの状態で観測され、残りの5000回は下向きの状態で観測されるのである。

一方、独立状態である|0>の場合は、1万回観測して、1万回とも上向きと観測されることを意味している。

## 二次元複素ベクトル表現

正式にはqubitの状態はℂ2（2-dimensional complex vector space）の単位ベクトルで表される。ここからは、qubitをベクトルで表現し、具体的な演算方法を説明する。

式(1)「α|0> + β|1>」をベクトルと書き表した場合、|0>および|1>は以下のように定義できる。

|  |  |
| --- | --- |
| |0> =  |1> = |  |

これは、以下のように変形できることからも明らかであろう。

= +

= α + β

= α|0> + β|1>

こうすることで、qubitに対する操作を行列計算として数理モデル化でき、その操作過程や結果も数値演算によりシミュレーションすることが可能となる。

例えば、行列と|0>の積を計算してみよう。

|0>

=

=

=

= |1>

すると|0>が|1>に変換された。同様に|1>に対して掛けると|0>を得るはずである。つまり、この行列は1-qubitに対してNOT操作として作用することが分かる。

## 確率振幅

ここでは式(1)および(2)で現れたαやβが示す確率振幅ついて二つの疑問について説明する。特にこの内容を知らなくても以降を読み進むことができるので、興味ない方、すでに理解されている方は読み飛ばして構わない。

1. 確率振幅の2乗が確率になる

式(2)の規格化条件はで|0>が出現する確率と|1>が出現する確率を足し合わせれば1になることを規定している。部分の確率を合算すれば全体で1になるのは当たり前なので、α、βはこの式が成り立つ値しかとりえないと言っているのである。では、なぜαやβ（確率振幅）を2乗する必要があるのだろうか？

例えば電子の場合で説明すると、それは電子の振幅と電子の発見確率の関係に依存している。ご存知のように、電子がどこに存在するかは確率的にしか分からない。電子はいつもある一点に存在しているというよりも雲のように空間にぼんやり広がったモノ、つまり電子場として捉えられる。電子場はどこも均一の濃さで広がっているのではなく、場所によって密度が異なる。そして密度が高いところほど電子が発見される確率が高くなることが分かっている。つまり、電子の発見確率は、電子場の密度に比例する。

そして、電子場の密度は、電子の振幅の2乗に比例することも分かっている。したがって、電子の発見確率は、電子の振幅の2乗にも比例するのである。

|  |
| --- |
| 電子の発見確率　∝　電子場の密度  電子場の密度　∝　電子の振幅の2乗  よって  電子の発見確率　∝　|振幅|2 |

1. 確率振幅は複素数の値をとる

確率振幅を示すα、βは実数を取る場合もあるが、基本的には複素数で表される。なぜ複素数なのだろうか？その理由は複素数を用いて数理モデル化すると、数々の実験で得られた結果と合致するからではあるが、ここではもう少し詳しく考察してみたい。

電子や光子といった量子が存在する場所が確率的にしか分からないという現象は、量子が粒子としての性質と同時に、波としての性質も持ち合わせており、干渉現象が生じるからである。

波は上図のような周期性を持つが、実数だけではこの周期性を表現できない。実数は一直線上を埋め尽くす点の集合でしかない。

…

-1

-2

…

2

1

0

これに対し、複素数は複素平面で表されることからも分かるように二次元の広がりを持ち、今、あるqubitの状態を大きさ1のベクトルとすれば、そのqubitへの演算は大きさ1を保ったまま、ベクトルを回転させることを意味する。

θ

例えば、1 \* i = i という演算はx軸方向を向いた1(1 + 0i)を反時計回りに90度回転させた結果i (0 + 1i)となったと捉えることもできる。この性質が波の持つ周期運動とマッチし、量子の挙動を数式で表す上で都合がいいのである。

## 複数qubitの計算

ここまでは、計算を行うレジスタとして1ビットのqubitを対象にして考察したが、ここでは複数のqubitを組み合わせた例として、2-qubitでの計算を行う。

古典コンピュータでbitが複数桁になる場合、例えば2ビットでは01と書くが、qubitの場合は各々の状態の組み合わせで表す。例えば、|0>と|1>の組み合わせた2-qubitは以下のように記述する。

|  |  |
| --- | --- |
| |0> 　|1> |  |

または、演算記号を省略して単に

|01>

と書くことも多い。また、本稿では使用しないが、ケット内の数列の桁が増えた場合、10進数で表すこともある。

|101> = |5>

なお、○に×の記号は、|0>と|1>の直積（テンソル積 Tensor Product）をとることを意味している。そこで、テンソル積について復習しておこう。ここではqubitを行列で表現しているので、行列に対してのテンソル積について説明する。

今、下記の値を持つ2 x 2行列A、Bが与えられたとしよう。

A = , B =

このとき、AとBのテンソル積は以下の行列で定義される。

A B =

Aの各要素についてBの全ての要素を掛けていく。そのため、Aがk \* l行列でBがm \* n行列の時、AとBのテンソル積はkm \* ln行列になる。この例の場合、2 x 2行列を与えたので、そのテンソル積後の行列は4 x 4行列となった。また、結合法則も成り立つ。

(A B) C = A (B C)

それでは、話を複数qubitsでの計算に戻そう。1-qubitをベクトルで表現できたように、

2-qubitもベクトル表現可能である。では、どのように表現するのだろうか？|0> (x) |1>ををベクトルで計算してみよう。

|0> 　 |1>

=

=

=

この様に2-qubitは4行のベクトルで表現される（2行1列と2行1列のテンソル積なので、その積は4行1列のベクトルとなる）。なお、この4行1列のベクトルは、上から|00>, |01>, |10>, |11>の4つの状態を表している。そして、今、このベクトルは上から2番目のみ1なので、|01>という状態であることが分かる。

|00> = 0

**|01> = 1**

|10> = 2

|11> = 3

他の2-qubit列についても同様に計算すると以下のようになり、これが2-qubit版ベクトル表現である。

|  |  |
| --- | --- |
| |00> =  |01> =  |10> =  |11> = |  |

ついでに式(1)と式(2)の2-qubit版も以下に定義しておく。

|  |  |
| --- | --- |
| |ψ> = c0|00> + c1|01> + c2|10> + c3|11> | 式(3) |

ただし、cnは複素数であり、以下の規格化条件を満たすものとする。

|  |  |
| --- | --- |
| |c0|2+|c1|2+|c2|2+|c3|2 = 1 | 式(4) |

それでは、重ね合わせの状態にあるqubitが2ビットあった場合は、どうなるだろうか？ここでは、|0>と|1>が1/2の確率で重ね合わさっている状態で考えてみる。

|0> + |1>) (|0> + |1>)

= (|0> + |1>) (|0> + |1>)

= (\*)((|0> + |1>) (|0> + |1>))

= (( + ) ( + ))

= ( )

=

=

= + + +

= |00> + |01> + |10> + |11>

となり、|00>, |01>, |10>, |11>までのすべての組み合わせが同確率（1/4）で存在する状態を表すことが分かる。各状態の係数（確率振幅）が1/2ということは

2 + 2 + 2 + 2 = 4 \* = 1

となり、式(4)の規格化条件も満たしていることに注意されたい。

ちなみに、上記では計算過程を詳しく示すために、ベクトルに変換して計算したが、ケット記号のまま計算しても同じ結果が得られる。

|0> + |1>) (|0> + |1>)

= (|0> + |1>) (|0> + |1>)

= (\*)((|0> + |1>) (|0> + |1>))

= (|0> |0> +|0> |1> + |1> |0> + |1> |1>)

= (|00> +|01> + |10> + |11>)

= |00> + |01> + |10> + |11>

この2-qubitでの計算で注目すべき点は、重ね合わせ状態の1-qubitでは|0>と|1>の2通りの状態を表現したが、2-qubitに拡張すると|00>, |01>, |10>, |11>の4通りが表現できたところである。同様に3-qubitにすると|000>, |001>, |010>, |011>, |100>, |101>, |110>, |111>,の8通りが表現できる。つまり、ビット数がn倍になると、同時に表現できる情報量は2n倍になるのである。

古典コンピュータの2 ビットも00, 01, 10, 11の4通りを表現できると思うかもしれないが、それはデータの組み合わせとして4通りあるだけで、その2ビットがある瞬間に持てる値はその4通りの中の1つだけである。しかし、量子コンピュータではその全てを同時に保持でき、一度に並列計算できる点で大きく異なる。これこそが組み合わせ問題を解く際に大量計算を一気にこなす秘密なのである。

## 観測する

「観測する」とは、qubitの値が0なのか1なのかを調べることである。古典コンピュータではビット情報を参照する行為にわざわざ「観測」などという大げさな言葉は使わない。値が0のビットは常に0だし、値が1のビットは常に1だからである。しかし、量子の世界では観測する前と後とでは状態が変わるため、観測という行為をいつ行うかが演算結果に影響を及ぼす。

独立状態であるqubitを観測する場合は、古典コンピュータ同様に一意に決定される。

|0>を観測すると、0が得られる。同様に、|1>を観測すると、1が得られる。

しかし、問題は重ね合わさった状態の時に起きる。今、ある1-qubitが以下の式で表される状態（確率1/2で重ね合わさった状態）だとしよう。

|0> + |1>

このqubitを観測すると値は0になるだろうか？それとも1になるだろうか？この段階ではどちらとも断定できない。ただ言えるのは確率1/2で0、確率1/2で1となるだろうということである。実際、観測を実行すると、0が返却されたり、1が返却されたりする。ただし、ひとたび観測すると、重ね合わせの状態は独立状態へと変わり、それ以降は同一qubitを何度観測しても同じ値を返却するようになる。

0

or

1

**?**

*X*

この観測するまでは2つの状態が同時に存在し、そのどちらであるかは確率的にしか分からない。しかし、観測するとどちらか一方の状態に収束し、それ以降もその状態のままでい続けるという奇妙な概念は量子の世界から導入されたものである。物理学の世界では長年、量子（例えば、原子、電子、光子など）は粒なのか、それとも波なのかが議論されているが、現在では、その両方の性質を持つ、とされている。そして、観測しない場合、量子は波としての性質を示すが、ひとたび観測すると粒子としての性質を示す。この奇妙な振る舞いの正体はまだ解明されていないが、この量子の振る舞いが発見された以降の百年以上の間、多くの物理学者が実験を重ねてきて、皆同じ結果を得ている。つまり、何故そうなるのかは分からないが、「こうすれば、こうなる」的な操作は把握でき、かつ、同じ結果を再現できるため、この現象を量子コンピュータに応用できるのだ。

しかしながら、計算結果が0なのか1なのか決定しないというのでは困ってしまう。そこで、通常のプログラミングでは並列計算を行っている間だけ重ね合わせの状態を維持し、結果を求める前に、何らかの変換操作で一意に決定できる値へと収束させる工夫を行っている。

または、式(1)で係数α、βで表した確率振幅を増大させ、取り出したい値の振幅だけ増大させておき、観測するということも行われたりする。

## エンタングルメント状態（量子もつれ）

これまで、qubitの取り得る状態として独立した状態と重ね合わさった状態の二種類を紹介した。独立状態とは|0>, |1>のように特定の値しか含まない状態であった。そして、|0>と|1>の重なり合った状態を重ね合わせ状態といい、|0>と|1>が同時に存在する状態を指した。この重ね合わせ状態は、更に二つの状態に分類できる。それは分離可能な状態とエンダングルメント状態（量子もつれ）である。

独立した状態

分離可能な状態

重ね合わせ状態

エンタングルメント状態

エンタングルメント状態とは、qubitの構成要素が絡み合って分離できない状態を指す。例えば、以下に示す2-qubitの状態を見てみよう。

(|00> + |01>)

係数（確率振幅）がなので、このqubitを観測すると1/2の確率で|00>、残り1/2の確率で|01>が得られるはずである。まず、左ビットを観測すると常に|0>が得られる。これは両方の状態の左ビットが0だから、どちらが選ばれても0となるからである。次に、右側のビットが|0>であるか|1>であるかは、その右ビットを観測するまで分からない。つまり、左ビットは右ビットと何ら関係なく値が決まる。確かに、上記式は以下のようにも変形できる。

(|00> + |01>)

= (|0> |0> + |0> |1>)

= (|0> (|0> + |1>))

この式は、左ビットが常に|0>となり、それとは無関係に右ビットは|0>または|1>になることを示している。このようにテンソル積で分離可能な状態はエンタングルメントな状態とは言わない。

次の例として、以下の2-qubitの状態を見てほしい。

(|00> + |11>)

先の例とよく似ているが、右側のケットが11になっている点が違う。

この左ビットを観測すると1/2の確率で|0>、残り1/2の確率で|1>となることが分かる。そして重要なのは、一度左ビットの値を得れば、右ビットを観測しなくてもその値を知ることができる。つまり、左ビットが|0>ならば、右ビットも|0>であり、左ビットが|1>ならば右ビットも|1>となる。先の節でも述べたとおり、一度観測するとそのビットは|0>または|1>に収束するため、このような結果を得るのである。

ここで、この2-qubitの左ビットを観測して値0を得たとしよう。その瞬間、左ビットの値は0に確定され、1をとる可能性は0となる。つまり、右の項|11>は状態として、もはや存在し得ないのである。そのため、|00>だけがqubit内に残り、その確率振幅は1となる（|00>しか存在しないので、以降、確率1で|00>が観測される）。

(|00> + |11>)

🡺qubit内に|00>と|01>の二つの状態がある

🡺左ビットを観測して、0を得た！（|11>は消える）

🡺qubit内の状態は「|00>」だけとなる

同様に以下の2-qubitもエンタングルメント状態となっている。

(|01> + |10>)

この場合は、右ビットは常に左ビットの反転となる値をとる。つまり、左ビットで0が観測されれば右ビットは1となり、左ビットで1が観測されれば右ビットは0となる。

これらの2-qubitは分離可能な状態のようにテンソル積で分けることができない（分離可能でないため）。

この状態を電子の場合で説明すると、観測によって電子が上向きに回転していることが確定すると、もう一方の電子は瞬時に下向きに確定される。これら二つの電子の間にある種の保存則が働き、後者の電子は前者の電子の回転を打ち消す向きに回転しなければいけないためである。



# 量子論理ゲート

古典コンピュータで論理演算を行う素子をゲートと呼び、NOT, AND, OR, XOR, NANDゲートを組み合わせて複雑な計算を行うように、量子コンピュータでもゲートがある。

ここでは量子論理ゲートの基本概念（ユニタリゲート、制御NOTゲート）の説明は省略し、実際の演算で多用するゲートの紹介のみに留めたい。

## パウリXゲート（NOTゲート）

1-qubitに対するゲートで、入力ビットを反転し、出力ビットとする。つまり、入力が|0>なら|1>を出力し、入力が|1>なら|0>を出力する。いわゆるNOTゲートのことであり、回路図では以下の図で表される。

X

パウリという名前はパウリのスピン行列と同じ働きをすることから由来している。パウリゲートにはパウリXの他にパウリY、パウリZゲートもあるが、ここではパウリXのみ取り上げる。

パウリXは以下の行列で表される。

パウリX =

それでは、この行列を使って、実際に演算してみよう。

X|0> = = = = |1>

X|1> = = = = |0>

期待通り、どちらのビット入力に対しても反転ビットが得られた。電子で言うと、上向きのスピンを下向きのスピンに変えるような操作を指す。

## アダマール(Hadamard)ゲート

1-qubitに対するゲートで、重ね合わさったqubitを出力する。|0>または|1>の入力に対して、以下のような値を出力する。

|0> 🡺 (|0> + |1>)

|1> 🡺 (|0> - |1>)

回路図では以下のように表される。

H

そして、演算においては以下の行列Hで表される。

H =

ここでも行列Hを利用して演算してみよう。

H|0> = = = = ( + ) = (|0> + |1>)

H|1> = = = = ( - ) = (|0> - |1>)

このように、|0>または|1>といった値の決まったqubitの入力に対し、|0>と|1>が半々の確率で存在する重ね合わさった値を出力している。そのため、多くの量子アルゴリズムで、並列計算を行う前に計算量を増やす目的でアダマールゲートを呼び出す操作が見られる。

光子の場合で説明すると、x偏光（x軸方向に偏向された光子）を反時計回りに45度回転させ、y偏光（y軸方向に偏向された光子）を右下45度の向きに回転させる操作にあたる。

このように重ね合わさった状態を作り出すと、ビット列が一体になったかのように振る舞い、一つのqubitに対する操作で他方のビットも同時に操作できるようになる。これこそが、量子コンピュータは単なる並列処理でなく、並列を超えた「超並列処理」と呼ばれる所以である。



# Function

量子論理ゲートは、システム側であらかじめ用意されたbuilt-in関数のようなもので、どのようなアルゴリズムを実装するにしても、よく使われる基本なビット操作を提供している。しかし、特定のアルゴリズムを実装する場合、そのような基本操作の組み合わせだけでなく、独自のロジックを組み込んだcustom関数が必要になることが多い。

本章では、そうしたアプリケーション固有のビット操作を行う関数の作成と実行方法について説明する。

## Ufゲート

まず、関数を実行するための論理ゲート（ここではUfと記述する）を考える。以下にUfゲートの一般的な図を示す。

x0

Uf

xn-1

n個

x

x

…

…

y0

ym-1

…

m個

…

y

y f(x)

このゲートは入力にn個のx（x0, x1, x2, …, xn-1）とm個のy（y0, y1,yx2, …, ym-1）を受け取る。そして、xは何も変換せずにそのまま出力し、yは関数f(x)を実行した結果とyの元の値と加算し、その一桁目のみを出力する（つまり桁あふれした部分は捨てる）。ここでは、＋に○の記号は1ビットの加算を意味している。なお、ここで単にx, yと記した場合、それは要素x0, x1, x2, …, xn-1を含む集合としてのx, yを意味することに注意されたい。

Ufゲート自体はシステム側から提供され、関数f(x) がプログラマーによって作成するカスタム関数だと理解してもよい。

ところで、古典コンピュータの概念で考えると、出力側にxは不要なのでは？と疑問に思うかもしれない。確かに変換しないのだからわざわざゲートを通して出力する必要はない。しかし、量子論理ゲートでは入力数と出力数が同じなければならないという制約がある。それは、量子計算では二つの基底状態（|0>と|1>）をもつ2次元複素空間内での操作と等価であるため、出力側から入力側へ逆方向にも戻れなければならないためである。このような変換をユニタリー変換（Unitary transformation）といい、複素平面上で大きさ1のベクトルを保ったまま方向を変える変換と理解して欲しい（単位円の円周上をグルグル回っている様子を想像してもらえると理解しやすいかもしれない）。

ここで具体例を示そう。問題を簡単にするため、ここでは入力qubitはxとyの2ビットだけだとしよう。

Uf

x

y

x

y f(x)

そして、入力ビットxを反転する関数f(x)を作成したとする。その関数は以下のように実装できる。

|  |
| --- |
| function f(x) {  return x == 0 ? 1 : 0;  } |

この他にも実装方法はあるだろうが、要は、x = { 0, 1 }であれば、0が渡されれば1を返し、1が渡されれば0を返す関数である。

さて、今、Ufゲートに|00>が渡されたとしよう。左ビットからx,yに割り当てるものとした場合、入力値は以下のようになる。

x = 0,

y = 0

そして、出力は以下のようになる。

x = 0,

y = 0 f(0) = 1

つまり、|00>の入力に対して|01>が出力された（y=0がy=1に変換された）。

同様に|01>に対しては|00>、|10>に対しては|10>、|11>に対しては|11>となる。

これよりUfはビット反転関数f(x)とともに操作すると、入力x（左ビット）が|1>の場合は何も変更しないが、|0>だと右ビットを反転させるゲートとして作用することが分かる。

## 超並列実行

前節で定義した関数が超並列的に実行されることを理解するため、古典コンピュータ向けのプログラミング言語で同等の処理を実装してみる。

ここでは、x0, x1, yの3ビットを入力とするUfゲートを考える。

x0

x

x

Uf

x1

y

y

y f(x)

例えば、|100>を左ビットからx0, x1, yに割当ると、

x0 = 1, x1 = 0, y = 0

を入力として受け取り、

x0 = 1,

x1 = 0,

y = 0 f(2) = 0 f(1) f(0) = 1

を出力として得る。つまり、|100>の入力に対し、|101>を得た。

以上の処理をJavaScriptで実装すると以下のようになる。

**リスト1 : JavaScriptによるUfゲートの実装**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17 | <script>  function f(x) {  return x == 0 ? 1 : 0;  }  window.onload = function() {  var bits = [0, 0, 1];  bits[0] += f(bits[1]);  bits[0] += f(bits[2]);  bits[0] %= 2;  console.log("result = "+bits[0]);  };  </script> |

|100>は配列[0, 0, 1]として表され、bits[1]およびbits[2]に対して関数fを実行している。最後に%=2としているのは桁あふれの部分を切り落とし、1桁目のみのビット値を得るためである。

実行すると、期待通り結果が1と表示される。

|  |
| --- |
| result = 1 |

このJavaScriptのコードを擬似的な回路図として描き表したのか以下の図である。

f

x0

y

y’

x1

f

fゲートが2回出現しているのが見て取れる。これは、関数fが2回コールされることを意味している。それに比べ、Ufゲート図ではUfは1回しか出現しない。つまり、同じ演算を行うために関数fは1回しか呼び出されないのである。これが更に重ね合わせの状態を入力として得た場合は、さらにその倍の4つの状態を一気に1回の関数コールで処理するのである。それに対し、JavaScriptでは4回の関数コールが必要となる。これこそが量子プログラミングにおける超並列処理の威力なのである。



# JavaScriptシミュレータによる量子プログラミング

いよいよ量子プログラミングを実際に体験してみよう。本稿ではJavaScriptで実装したシミュレータであるjsqbを用いる。jsqbは本稿で説明した内容を実体験する目的で作られたものである。そのため、機能は少ないがソースコードも500行以下と非常に小さく、コードを追って理解できるように配慮している。

なお、jsqbのJavaScriptファイルやサンプルコードは以下のサイトで公開している。また、本ドキュメントも同サイトで公開しているので、更新、訂正についてはそちらを参照願いたい。

|  |
| --- |
| https://github.com/jsqb |

## クラス図

qubitの構成要素を復習する意味でもjsqbのクラス図の一部を示す。

1..2n

1

<<Class>>  
**BasisState**

<<Class>>  
**Qubit**

amplitude  
value  
bitLength

state

operate  
operateMatrix  
x  
hadamerd  
tensor  
measure

<<Class>>  
**State**

<<Class>>  
**Complex**

real  
img

add  
multiply  
magnitude

これらクラスが、qubitおよびそれが保持する状態(state)を表している。まず、qubitは|0>や|1>などのbasis state(basis vector)の線形的な集まりであり、例えば、1-qubitの場合は以下の式で表された。

|ψ> = α|0> + β|1>

ここで、α、βは|0>、|1>が出現する確率振幅を表しており、値としては複素数をとり得る。2-qubitになるとbasis stateとしてとり得る値が|00>、|01>、|10>、|11>の4種類となり、以下の式で表された。

|ψ> = c0|00> + c1|01> + c2|10> + c3|11>

つまり、n-qubitの中に2n個のbasis stateをcnの割合で保持することになる。jsqbのクラスもその構成をとっている。クラス図に戻って見てみると、Qubitクラスは一つの状態をstateプロパティとして保持し、そのstateは複数のBasisStateクラスと関連付けられている。そして、BasisStateクラスには確率振幅を格納するamplitudeプロパティ、qubit値を格納するvalueプロパティ、そしてqubit値のビット長を格納するbitLengthプロパティから成る。この3つのプロパティで一つの項（basis state）を表現している。例えば、上記式のc3|11>の項は以下のようにBasisStateクラスに格納される。

amplitude = **c3**  
value = **3**  
bitLength = 2

<<Instance>>  
**BasisState**

なお、valueプロパティには10進数で格納するため、11は3として格納する。しかし、それだと3を2進数に戻す時、11、011、0011等のどの値を表していたかが分からなくなるため、ビット長「2」をbitLengthプロパティに保持しておく。

また、確率振幅を表すamplitudeプロパティは複素数の値をとるため、Complexクラスのインスタンスを格納することになる。

以上がクラス図の概要である。より細かい説明は後回しにして、まずはコードを実行して、どのような動きになるかを体感しよう。

新しい言語を学ぶ際、各入門書の最初のサンプルとしてHello Worldを出力することが慣例となっているが、残念ながらjsqbではそんな高度なコードは書けない。マシン語で文字列を表示する時はシステムコールで行うようにjsqbもJavaScriptの機能をコールすることで可能とも言えるが、ここでは、これまでに紹介した量子計算や論理ゲートをコード化し、計算どおりに動作することを確認したい。

## NOT演算

パウリ行列X = が1-qubitを反転させることを示し、以下の演算を紹介した。

X |0> = |1>

X |1> = |0>

上記をjsqbで実装すると以下のコードとなる。

**リスト2 : Pauli Xによるビット反転**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13 | <script src="jsqb.js"></script>  <script>  window.onload = function() {  var X = [[0, 1],  [1, 0]];  debug("X |0> = " + jsqb('|0>').operateMatrix(0, X));  debug("X |1> = " + jsqb('|1>').operateMatrix(0, X));  };  </script> |

jsqbを利用するため、1行目でJavaScriptファイル「jsqb.js」を読み込む。

そして、ページの読み込みが完了してからコードを実行したいので、window.onloadに設定したfunction内に処理コードを記述している（3行目）。これはdebug関数でブラウザ画面上にメッセージを表示するためである。

次に、5, 6行目でパウリ行列Xを二次元配列として定義する。

そして、いよいよjsqbの登場である。まずは、jsqbにケット文字列を与え、qubitオブジェクトを作成する（8行目の「jsqb('|0>')」の部分）。

|  |
| --- |
| Qubit = **jsqb** ( *ketString* ); |

引数にケット文字列、例えば、|0>, |1>, |101>等を指定すると、その値を表現するQubitオブジェクトが返却される。

そして、次にパウリXとの積をとるため、operateMatrix関数をコールする。

|  |
| --- |
| Qubit = *qubit*.**operateMatrix** ( *targetBit, matrix* ); |

targetBitはqubitのどのビットに対して処理をするかを指定する。右から左に向かって、0ビット目、1ビット目、2ビット目、…と数える。

ここでは「0」が指定されているので、|0>の0ビット目、つまり「0」に対して変換を行う。|0>はベクトルで与えられるので、ここでは行列とベクトルの積を計算して「0」のあった場所にセットする、という操作を行っている。

10行目も入力値が|1>となるだけで同様な処理となる。実行すると以下のように表示され、期待通り反転した値が得られた。

|  |
| --- |
| X |0> = |1>  X |1> = |0> |

## テンソル積

複数のqubitを組み合わせて処理する場合、その組み合わせはテンソル積で表現できる。例えばここに|0>と|1>があり、それらをつなぎ合わせ、2-qubitとして処理する場合、それは、

|0> |1>

と書き表した。また、演算記号を省略し、単に|01>と書いてもよい。

重ね合わさった状態の場合も同様に、例えば

|0> + |1>) (|0> + |1>)

と書き表された。この式の場合、直積計算を進め、より単純化すると以下のように表される。

= |00> + |01> + |10> + |11>

上記に示した二通りの計算を行うコードを以下に示す。

**リスト3 : Tensor Product**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11 | <script src="jsqb.js"></script>  <script>  window.onload = function() {  debug("|0> (x) |1> = " + jsqb('|0>').tensor(jsqb('|1>')));  var qubit = jsqb('|0>+|1>');  debug(qubit+" (x) "+qubit+" = " + qubit.tensor(qubit));  };  </script> |

そして、以下がその実行結果である。

|  |
| --- |
| |0> (x) |1> = |01>  0.7071 |0> +0.7071 |1> (x) 0.7071 |0> +0.7071 |1> = 0.5 |00> +0.5 |01> +0.5 |10> +0.5 |11> |

まず、5行目では|0> (x) |1>の計算を行っている。テンソル積はQubitオブジェクトのtensorメソッドで求められる。

|  |
| --- |
| Qubit = *qubit*.**tensor** ( qubit ); |

メソッドtensorにqubitオブジェクトを与えると、自身のqubitとのテンソル積を行った結果のqubitを返却する。

ここでは、|0>を表すQubitオブジェクトでtensorメソッドを実行し、|1>を表すQubitオブジェクトを引数に渡している。したがって、その答えは|01>となる。

7, 8行目では、|0>と|1>が重ね合わさった状態同士のテンソル積を求めている。まず、重ね合わせ状態のqubitを作成するため、jsqbに”|0> + |1>”という文字列を与えている（7行目）。なお、本来この表現は正しくない。規格化条件（|α|2+|β|2 = 1）より、確率振幅の二乗の和は1でなければならない。そのため、正しくは”|0> + |1>”と書くべきだが、ここでは確率振幅を省略している。Qubitオブジェクトを生成する際、規格化条件に合致するよう確率振幅を自動で再計算してくれるからだ。実際に、その次の行でqbuit変数を表示しているが、その実行結果をみると「0.7071 |0> +0.7071 |1>」という正しい値になっている。なお、0.7071はを小数で表した値である。

これで変数qubitに重ね合わせ状態のqubitオブジェクトが格納できたので、あとはそれをtensorメソッドで積をとればよい。

実行結果には先に手計算した結果と同じ値（00, 01, 10, 11の四状態がそれぞれ振幅1/2で重ね合わさった状態）が表示されている。

## qubitの観測

独立状態のqubitの観測は|0>なら0、|1>なら1と一意に求められる。しかし、重ね合わせ状態にあるqubitの場合、その観測結果は確率的に決定される。

その様子をjsqbのコードを用いて確認しよう。qubitを観測するにはmeasureメソッドを用いる。

|  |
| --- |
| Measurement = *qubit*.**measure** ( targetBit ); |

このmeasureメソッドは観測したいビット番号（右から数え、0から始まる）を受け取ると、その位置のビット値と観測後のqubitオブジェクトをプロパティとして保持したMeasurementオブジェクトを返却する。

<<Class>>  
**Measurement**

qubit  
value

「観測する」の節でも述べたが、qubitは観測すると観測したビットは0または1に収束し、その値以外のビット値を含む状態は消滅する。そのため、measureを実行する前と後とではqubitの状態が異なるため注意が必要である。以下がそのことを確認するための具体的なコードである。

**リスト4 :Measurement**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18 | <script src="jsqb.js"></script>  <script>  window.onload = function() {  debug("|0> measure(0) = " + jsqb('|0>').measure(0));  debug("|100> measure(2) = " + jsqb('|100>').measure(2));  var qubit = jsqb('|0> + |1>');  var qubit2 = qubit.clone();  debug(qubit+" measure(0) = " + qubit.measure(0));  debug(qubit+" measure(0) = " + qubit.measure(0));  debug(qubit+" measure(0) = " + qubit.measure(0));  debug(qubit2+" measure(0) = " + qubit2.measure(0));  };  </script> |

このサンプルを実行すると以下の出力を得る。なお、これは一例であり、実行のたびに異なる値を出力するので注意されたい。

|  |
| --- |
| |0> measure(0) = 0  |100> measure(2) = 1  0.7071 |0> +0.7071 |1> measure(0) = 0  |0> measure(0) = 0  |0> measure(0) = 0  0.7071 |0> +0.7071 |1> measure(0) = 1 |

まず、5行目は|0>を観測し、0を得ている。|0>は独立状態なので、F5ボタンを押してブラウザ画面を何度リロードしても常に0が表示されるはずである。

6行目は独立状態にある3-qubitの2ビット目（0ビット目から始まるので、実際には右から3ビット目）を観測している。|100>の2ビット目は1なので常に1が返却される。

8行目は|0>と|1>が同確率で重ね合わさった状態のQubitオブジェクトを生成し、変数qubitに格納ている。そして、9行目でそのqubitと同じ状態のコピーをもつqubit2も作成しておく。今、qubitおよびqubit2変数は下記の式で表される状態にある。

|0> + |1>

確率振幅がなので、確率1/2で|0>、残り1/2で|1>になることを意味している。つまり、同確率で0または1が観測されるはずである。

まず、11行目でqubit変数に対して観測を行う。すると、0が表示されたり1が表示されたりと、定まった値にはならない。しかし、例えば11行目で0が観測されたとすれば、12, 13行目でも必ず0が観測される。それは11行目の観測によってqubitの状態は重ね合わせ状態から|0>という独立状態へと収束したためである。

しかし、観測前にコピーしたqubit2では収束は起こっていないため、15行目で観測を行うと、11行目の観測結果に関係なく、0であったり、1であったりする。

なお、余談であるがcloneメソッドは便宜上用意した機能で、現時点では実際の量子コンピュータ上では実装できない機能であることに留意して欲しい。なぜなら、qubitの状態を一度観測するとその状態が変化するため、元の状態を知ることができないからである。コピーするためにはqubitの中を覗かなければならないが、そうすると変化した状態をコピーすることになる。このことは数学的にも「量子複製不可能定理」として証明されている。完全なコピーでなくてもコーディング上、簡単にクローンオブジェクト作成できる方法が発見されるまで量子コンピュータ上ではcloneメソッドの実装は不可能なのである。

## エンタングルメント状態の観測

次に、重ね合わせ状態の更に特殊な状態であるエンタングルメント状態のqubitを観測してみる。エンタングルメント状態のqubitとはビット同士が絡み合い、分離できない場合を指す（「量子もつれ」とも言う）。例えば2-qubitの場合、左ビットを観測したら、右ビットを観測しなくてもその値が分かる場合である。

そのことを以下のコードを実行して確認しよう。

**リスト5 : Measure entangled qubits**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16 | <script src="jsqb.js"></script>  <script>  window.onload = function() {  var qubit = jsqb('|00> + |11>');  var value1 = qubit.measure(1).value;  var value0 = qubit.measure(0).value;  debug("|00> + |11> measure => ("+value1+", "+value0+")");  var qubit = jsqb('|01> + |10>');  var value1 = qubit.measure(1).value;  var value0 = qubit.measure(0).value;  debug("|01> + |10> measure => ("+value1+", "+value0+")");  };  </script> |

実行結果はランダムに変化する。起こりうる実行結果の内、代表的な二通りを以下に示す。

**実行結果1**

|  |
| --- |
| |00> + |11> measure => (0, 0)  |01> + |10> measure => (0, 1) |

**実行結果2**

|  |
| --- |
| |00> + |11> measure => (1, 1)  |01> + |10> measure => (1, 0) |

まず、5行目で|00>と|11>の重ね合わせ状態にあるqubitを作成する。そして、6行目で1ビット目（左ビット）を観測し、観測結果の値をvalue1に格納する。7行目では同様に0ビット目（右ビット）を観測し、値をvalue0に格納する。そして、8行目でそれらの値を表示している。

ここで、このコードを何度か実行してみて欲しい。実行する毎に得られる値が変化するかもしれないが、その値は(0, 0)または(1, 1)の二通りしかないことに気づくだろう。決して(0, 1)のように値が混ざることはない。これは、左ビットを観測して、もしそれが0ならば、状態|00>に収束するからである。その後で右ビットを観測するのだから、右ビットも必ず0となる。反対に、左ビットが1と観測されれば|11>に収束し、右ビットも1となる。

エンタングルメント状態のもう一つの例として|01> + |10>の場合も試してみよう。11行目で”|01> + |10>”を指定している以外は、先の例と同じ操作を行っている。こちらは、(0, 1)か(1, 0)のどちらかかの結果しか現れない。それは左ビットが0と観測されれば|01>に収束し、右ビットは1となる。同様に、左ビットが1と観測されれば|10>に収束し、右ビットは0となるためである。

## パウリXゲート

パウリ行列Xはビットを反転させる作用があった。この操作は頻繁に使われるため、jsqbではその簡易版としてxメソッドも提供している。

|  |
| --- |
| Qubit = *qubit*.**x** ( targetBit ); |

引数のtargetBitに反転させたいビット番号（右から数え、0から始まる）を指定し、xメソッドをコールすると、該当のビットだけが反転した新しいQubitオブジェクトが得られる。リスト2をxメソッドで書き換えると以下のようになる。

**リスト6 :Pauli X**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | <script src="jsqb.js"></script>  <script>  window.onload = function() {  debug("X |0> = " + jsqb('|0>').x(0));  debug("X |1> = " + jsqb('|1>').x(0));  };  </script> |

実行結果もリスト2と同じで、それぞれ反転した値が返される。

|  |
| --- |
| X |0> = |1>  X |1> = |0> |

## アダマールゲート

アダマール(Hadamard)ゲートは重ね合わせ状態のqubitを作成する場合に、よく用いられる。

|  |
| --- |
| Qubit = *qubit*.**hadamard** ( [ targetBits ] ); |

引数のtargetBitsに反転させたいビット番号を指定し、hadamardメソッドをコールすると、アダマール変換を行った後のQubitオブジェクトが得られる。targetBitsには複数の番号を配列を用いて指定することができる。例えば、0, 1,2ビット目を変換したい場合は[0, 1, 2]を指定する。また、targetBitsの指定を省略すると全ビットに対して変換される。

var qubit = qubit.hadamard( [0, 1, 2] ); // apply on bit #0, 1 and 2

var qubit = qubit.hadamard(); // apply on all bits

それでは、独立状態のqubitである|0>や|1>が重ね合わせ状態へ変換される様子をコードでみてみよう。

**リスト7 :Hadamard**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | <script src="jsqb.js"></script>  <script>  window.onload = function() {  debug("H |0> = " + jsqb('|0>').hadamard(0));  debug("H |1> = " + jsqb('|1>').hadamard(0));  };  </script> |

実行結果は以下の通りである。

|  |
| --- |
| H |0> = 0.7071 |0> +0.7071 |1>  H |1> = 0.7071 |0> -0.7071 |1> |

5行目では、|0>にhadamardメソッドを実行し、「0.7071 |0> +0.7071 |1>」という結果を得ている。|0>が|0>と|1>が半々に出現する状態へと変換された。

同様に7行目では|1>に対してhadamard変換を実行している。こちらも「0.7071 |0> -0.7071 |1>」という結果が示す通り、|0>と|1>の重ね合わせ状態となっている。

## Functionの実行

jsqbではJavaScriptのfunctionを実行するoperateメソッドを提供している。これはFunctionの章で説明したUfゲートを実装したものである。

|  |
| --- |
| Qubit = *qubit*.**operate** ( srcBitRange, destBitRange, func ); |

このメソッドの引数には、関数へ渡すビット範囲、関数から出力された値を反映するビット範囲、そしてあなたが作成したJavaScript関数の3つを指定する。ビット範囲とはqubit内の部分ビットの開始ビット番号と終了ビット番号の組のことであり、jsqbでは要素が2つの配列で指定する。例えば、右から3番目のビットから5番目までのビットを計算対象とする場合は、[2,4]と指定する（0始まりなので、3番目のindex番号は「2」、5番目は「4」となる）。1ビットのみを対象とする場合は、[2,2]と指定してもよいし、単に数値の2を指定してもよい。

なお、srcBitRangeに指定したビット範囲が関数への入力となり、destBitRangeに指定したビット範囲が関数からの出力を受け入れるビットとなる。ただし、srcBitRangeの範囲とdestBitRangeの範囲はオーバーラップしてはならない。

第3引数のfuncに、あなたが作成したカスタムfunctionを指定するが、それは一つの引数をとり、１つの値を返却する関数でなければならない。例えば、あなたは以下のように引数xに渡された値をそのまま返す関数funcを作成したとしよう。

|  |
| --- |
| function func(x) {  return x;  } |

すると、operateメソッドはsrcBitRange範囲内のビット列を10進数に変換し、func関数に渡す。そして、func関数からの戻り値を2進数に変換し、destBitRangeの値とビット単位で加算した結果を設定する。その際、加算は各ビット単位で行い、桁あふれは捨てられる。

例えば|1101>というqubitに対して、operate([2,3], [0,1], func)を実行したとしよう。するとfuncの引数xには「11」を10進数に変換した「3」が渡される。func関数はxの値をそのまま返却するので、「3」つまり2進数で「11」が0ビット目と1ビット目に加算される。

ここで注意して欲しいのは、ビット毎に独立して加算が行われる点である。つまり、0ビット目は「1 + 1 = 10」となるが、桁あふれした1は捨てられ、0が0ビット目に設定される。1ビット目は「1 + 0 = 1」となり、1が1ビット目に設定される。

結果、qubitの値は|1110>になる。「11 + 01 = 100」という計算にはならない。

左ビット: 1 (+) 0 = 1  
右ビット: 1 (+) 1 = 0

|1101>

1

1

0

1

1

1

x = 3

return 3;

**func**

上記の例を含めた関数実行のコードを以下に示す。

**リスト8 :Execute a function**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | <script src="../jsqb.js"></script>  <script>  function f(x) { return x; }  window.onload = function() {  debug("Uf |10> = " + jsqb('|10>').operate(1, 0, f));  debug("Uf |11> = " + jsqb('|11>').operate(1, 0, f));  debug("Uf |1000> = " + jsqb('|1000>').operate([2,3], [0,1], f));  debug("Uf |1101> = " + jsqb('|1101>').operate([2,3], [0,1], f));  };  </script> |

実行結果は以下の通りである。

|  |
| --- |
| Uf |10> = |11>  Uf |11> = |10>  Uf |1000> = |1010>  Uf |1101> = |1110> |

いずれの例も3行目で定義した関数fをコールしている。関数fは先の例と同じく、引数xをそのまま返却する関数である。

まず、7, 8行目は1ビットの入出力データに対する操作を行っている。

7行目は1ビット目の「1」を受け取り、「1 (+) 0」を0ビット目に設定する。なお、(+)は加算演算後、1ビット目のみ残すことを意味している。したがって、実行結果は|11>となる。

8行目も1ビット目の「1」を入力として受け取るが、0ビットとの加算で「1 + 1 = 10」となり、桁あふれが生じる。そのため、あふれた「1」は捨てられ「0」だけが残り、実行結果は|10>となる。

10, 11行目は2ビットの入出力データに対する操作の例で、10行目は桁あふれが発生しないので、入力ビットがそのまま下2桁の値となり、|1010>が出力される。

11行目は本節の例として説明したとおり、0ビット目で桁あふれが生じ、|1110>が出力される。



# Deutsch's algorithm

これまでの説明で量子コンピュータ上でのプログラミングの基礎知識とそれを実装したシミュレータの理解は一通りできたものと思う。そこで本章では「問題を解く」というスタイルのコーディングを見てもらいたい。その例として、量子コンピュータ向けのアルゴリズムの一つであるDeutsch's algorithmを紹介する。Deutschは真の量子アルゴリズムを示した最初の人である。Deutsch’s algorithmは実用的な仕事で役立つアルゴリズムとは言えないが、非常にシンプルなロジックで量子コンピュータの有効性を示した点で意義がある。また、量子コンピュータ向けのアルゴリズムを学ぶ最初の一歩として最適な教材でもある。

## アルゴリズムの概要

Deutsch's algorithm が解決する問題は、以下の通りである。

今、引数xに0または1のみをとり、戻り値も0または1のみを返す関数f(x)がある。すると、この関数は以下に示す4つのいずれかになるはずである。

1. 入力値に関わらず、常に0を返す。

Constant型

1. 入力値に関わらず、常に1を返す。
2. 入力値と常に同じ値を返す。

Balanced型

1. 入力値と常に反対の値を返す。

ここで、最初の二つは常に一定の値を返す点で同種であり、Constant型として分類できる。それに対し、下から二つは0または1が返ってくる点で同種であり、Balanced型と分類しよう。

ここで、あなたへの問題は、与えられた関数f(x)がConstant型なのかBalanced型なのかを判定することである。

## JavaScriptでの実装

まず、古典コンピュータを用いた場合のアルゴリズムを考えてみよう。入力は0または1しかないのだから、f(0)とf(1)を実行してそれらからの戻り値を比較すればよい。同じ値になればConstant型であり、異なる値であればBalanced型だと判定できる。

この考え方をJavaScriptで実装すると以下のようになる。

**リスト9 : Deutsch's Algorithm implemented with JavaScript**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21 | <script src="jsqb.js"></script>  <script>  function f0(x) { return 0; }; // Constant 0  function f1(x) { return 1; }; // Constant 1  function f2(x) { return x; }; // ID (balanced)  function f3(x) { return (x + 1) % 2; }; // NOT (balanced)  function deutsch(f) {  return (f(0) + f(1)) % 2;  }  window.onload = function() {  debug("0:constant, 1:balanced");  debug("deutsch(f0) = " + deutsch(f0));  debug("deutsch(f1) = " + deutsch(f1));  debug("deutsch(f2) = " + deutsch(f2));  debug("deutsch(f3) = " + deutsch(f3));  };  </script> |

そして、実行結果は以下の通りである。

|  |
| --- |
| 0:constant, 1:balanced  deutsch(f0) = 0  deutsch(f1) = 0  deutsch(f2) = 1  deutsch(f3) = 1 |

まず、3から6行目はConstant型およびBalanced型あわせて四通りの関数を定義している。ここではf0, f1がConstant型であり、f2, f3がBalanced型である。

そして、8から10行目で問題を解決する関数deutshが定義されている。f(0)とf(1)を計算し、その結果を足して2で割った余りを求めている。もし関数fがConstant型だとすると、

0 + 0 = 0　または、

(1 + 1) % 2 = 0

となり、いずれの場合も0が求まる。一方もしBalanced型であれば

0 + 1 = 1　または、

1 + 0 = 1

となり、いずれの場合も1が求まる。実行結果もその通りの値を出力している。

このように古典コンピュータでは関数fを**2回**実行することで、どちらの型かを判別することができた。

## 量子コンピュータでの実装

Deutschはこの問題を解決するため、以下のゲートを考え出した。

|0>

H

H

Uf

x

y

x

y f(x)

|1>

H

Ufゲートの入力と出力にアダマールゲートを通しただけの単純な回路であることが分かるだろう。そして、入力値として|01>を与えれば、出力の1ビット目がConstant型かBalanced方かを示すというのである。

上記回路を実装したのが以下のコードである。

**リスト10 : Deutsch's Algorithm**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25 | <script src="jsqb.js"></script>  <script>  function f0(x) { return 0; }; // Constant 0  function f1(x) { return 1; }; // Constant 1  function f2(x) { return x; }; // ID (balanced)  function f3(x) { return (x + 1) % 2; }; // NOT (balanced)  function deutsch(f) {  return jsqb('|01>')  .hadamard()  .operate(1, 0, f)  .hadamard()  .measure(1);  }  window.onload = function() {  debug("0:constant, 1:balanced");  debug("deutsch(f0) = " + deutsch(f0));  debug("deutsch(f1) = " + deutsch(f1));  debug("deutsch(f2) = " + deutsch(f2));  debug("deutsch(f3) = " + deutsch(f3));  };  </script> |

このコードはリスト9（JavaScriptで実装）とほとんど同じである。異なるのは関数deutshの中味だけである。そこでは、以下の操作を順に行っているだけである。

Step 1: |01>のqubitオブジェクトを生成する。

Step 2: hadamardゲートに通し、重ね合わせ状態を作り出す。

Step 3: 関数fを実行する。

Step 4: 再度、hadamardゲートに通す。

Step 5: 1ビット目を観測し、答えを得る。

机上で上記操作による状態変化を追うのは大変なので、次のようなプログラムを作成し、ステップ毎の状態を画面表示させてみよう。ここでは関数f3（引数xを反転した値を返却）を実行している。

**リスト11 : Deutsch's Algorithm – Process of calculation**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25 | <script src="jsqb.js"></script>  <script>  function f0(x) { return 0; }; // Constant 0  function f1(x) { return 1; }; // Constant 1  function f2(x) { return x; }; // ID (balanced)  function f3(x) { return (x + 1) % 2; }; // NOT (balanced)  window.onload = function() {  var qubit = jsqb('|01>');  debug("Step 1: |01> = " + qubit);  qubit.hadamard();  debug("Step 2: H|01> = " + qubit);  qubit.operate(1, 0, f3);  debug("Step 3: Uf(H|01>) = " + qubit);  qubit.hadamard();  debug("Step 4: H(Uf(H|01>)) = " + qubit);  debug("Step 5: Mesure qubit-#1 = " + qubit.measure(1));  };  </script> |

このコードの実行結果は以下のようになる。

|  |
| --- |
| Step 1: |01> = |01>  Step 2: H|01> = 0.5 |00> -0.5 |01> +0.5 |10> -0.5 |11>  Step 3: Uf(H|01>) = -0.5 |00> +0.5 |01> +0.5 |10> -0.5 |11>  Step 4: H(Uf(H|01>)) = -1 |11>  Step 5: Mesure qubit-#1 = 1 |

まず、Step 1では|01>を初期状態として持つqubitを作成した。今、このqubitオブジェクトには|01>という独立状態のbasis stateが一つ保持されている。

そして、Step 2ではアダマール(Hadamard)ゲートにより、|00>, |01>, |10>, |11>の4つが重ね合わさった状態にしている。具体的な操作を数式で表すと以下のようになる。まず、左ビット|0>に対して行列Hを掛ける。すると、|0>と|1>の重ね合わせ状態に変化する。

H|0> = = = = ( + ) = (|0> + |1>)

同様に右ビットに対しても行列Hを掛けると、|0>と|1>の重ね合わせ状態に変化する。上記とは符号が異なる点に注意されたい。

H|1> = = = = ( - ) = (|0> - |1>)

これらは2つのビットはテンソル積でつなぎ合わさっているので、テンソル積をとると、

= (|0> + |1>) (|0> - |1>)

= (\*)((|0> + |1>) (|0> - |1>))

= (|0> |0> -|0> |1> + |1> |0> - |1> |1>)

= (|00> -|01> + |10> - |11>)

= |00> - |01> + |10> - |11>

となり、Step 2の実行結果と一致する。これで2-qubitが取り得るすべての状態（00, 01, 10, 11の4種類の値）を作り出せ、関数を実行するための前準備が完了した。

次のStep 3ではUfゲートを使い、先の4つの値に対して関数を一気に実行している。以下のように計算前と後で項の位置が入れ替わっているため、混乱しやすいので注意して欲しい。

**実行前:** 0.5 |00> -0.5 |01> +0.5 |10> -0.5 |11>

**実行後:** -0.5 |00> +0.5 |01> +0.5 |10> -0.5 |11>

左のbasis state（項）からひとつ一つ計算過程を示しておこう。まず、最初の項「0.5|00>」の1ビット目「0」を関数f3の引数として渡して実行すると反転値「1」返ってくる。それを0ビット目の「0」と加算して結果を得るので、計算後は「0.5|01>」となる。

同様に二番目の項「-0.5|01>」の1ビット目「0」を関数f3の引数として渡して実行すると反転値「1」返ってくる。それを0ビット目の「1」と加算すると「10」となるが、ここは桁あふれした1は捨てるので、結果は「-0.5|00>」となる。

三番目と四番目は1ビット目が「1」なので反転すると「0」となり、0ビット目には何も影響を与えない。つまり、計算後も計算前と同じ値となる。

Step 4からは、計算結果を取り出すための操作となる。超並列計算を行うために重ね合わせの状態を作ったが、このままではどの値が観測されるかは確率的に決定されるため、常に決まった値が得られない。何らかの方法で値を独立状態に戻す必要がある。その方法の一つとして量子フーリエ変換があるが、2-qubitの場合はアダマール変換と等価であることが知られている。したがって、ここではStep 2同様に、再度hadamardゲートを通せばよい。

Step 2で行列Hと|01>との積の計算過程を示したように、

H|01> = |00> - |01> + |10> - |11>

という計算結果を得た。同様に他の|00>, |10>, |11>に対しても行列Hとの積をとると、

H|00> = |00> + |01> + |10> + |11>

H|10> = |00> + |01> - |10> - |11>

H|11> = |00> - |01> - |10> + |11>

よなる。以上をStep 3で得た計算結果にHとの積をとった以下の式に代入してみよう。

H (- |00> + |01> + |10> - |11>)

= - H|00> + H|01> + H|10> - H|11>

= - |00> - |01> - |10> - |11>

+ |00> - |01> + |10> - |11>

+ |00> + |01> - |10> - |11>

- |00> + |01> + |10> - |11>

= -|11>

計算途中、16項のまで増えたがその殆どが打ち消され、|11>だけが残った。

この状態でStep 5の1ビット目の観測を行うと、常に「1」という値を得る。この1は実行した関数がBalanced型であることを示している。確かに今回は関数f3を実行したので期待通りの結果を得た。

ここで重要なのは、答えを得るのにUfゲートによる関数実行は1回しか行われていない点である。Step 3の説明では00, 01, 10, 11の4つの値にそれぞれ関数を実行したので4回の関数実行が行われるかのように思われたかもしれない。確かにJavaScriptシミュレータ内では4回の関数実行を行っている。しかし、本物の量子コンピュータ上で実行すれば1回のゲート操作で4つのbasis stateに対する計算を行ってしまうのである。つまり、関数fは1回しか実行されない。

JavaScript版では2回の実行が必要であったが、それが1回で済むのだ。今回の例のように非常に単純なロジックであればその差は微々たるものであるが、関数fが入力データ数に対し、指数関数的に組み合わせが膨らむ問題の場合、非常に大きな効果を示すのである。



# おわりに

本稿では量子プログラミングを行うために習得しておくべき前提知識とJavaScriptシミュレータ上での基本的なコーディング方法について説明した。また、最後に最も単純な量子アルゴリズムの一つであるDeutsch's algorithmを紹介し、より実践的なプログラミングコードにもふれた。しかしながら、それだけではまだ不十分な点が多い。例えば、本稿では量子ゲートとして、パウリXゲートとアダマールゲートの2だけを紹介したが、その他にもプログラミングする上で必要となるゲートはいくつもあるし、コードの動きを真に理解するには量子力学の知識も不可欠となる。

本稿では、量子力学を学んだことの無い方を対象としているため、そうした難解な点はあえて避けてきた。しかし、今後、あなたがより実用的なプログラムを作成しようとコーディングを始めたなら、たちどころに未開の問題にぶつかってしまうだろう。まだ誰も解いていない、もしくはネットを検索しただけでは容易に解を得られない問題である。量子コンピュータ用にもすでに高級言語が用意されている段階であればそのような問題に遭遇することは稀だが、本稿で紹介したコードを見ても分かるとおり、今はまだアセンブリレベルの低レベルな操作を行っている段階である。また、十分な解説書も無い。そうした状況下ではコーディングのルールを作り出している基礎数理モデルを正しく理解し、計算過程を追える力がなければならない。

本稿を読破し、サンプルコードを理解できたなら、もう十分に次へのステップへ進む準備ができたはずである。是非、量子力学の基礎も学び、量子プログラミングの真の理解を目指して欲しい。