Supercon 2018 本選問題

8 月 20 日

1　はじめに

今年は東京工業大学のスーパーコンピュータ TSUBAME 3.0 を使って量子コンピュータのシミュレーションをしてもらう。量子コンピュータは素因数分解など従来のコンピュータでは効率的に解けないと信じられている問題を効率的に解くことができる。そのような理論的な事実は 90 年代に分かっていたが、量子コンピュータを実際に作るためには技術的な困難が多く、実現するのは当分先のことだと考えられていた。しかし、この数年で劇的に量子コンピュータに関する技術が進展し、IBM や Google は去年から今年にかけて 50 量子ビット程度のサイズの量子コンピュータを作ったと発表した。この本選問題では 30 量子ビット以下の量子コンピュータの計算を TSUBAME 3.0 を使って、いかに高速にシミュレーションするかを競ってもらう。

2　量子ビット

私達が普段ビットの列を使って情報を表現しているように、量子コンピュータでは量子ビット (qubit) を使って情報を表現する。古典ビット `0` と `1` に対応する量子ビットは $|0\rangle$ と $|1\rangle$ である。量子ビットは直接「見る」ことはできず、量子ビットを「測定」することで初めて情報が得られる。$|0\rangle$ を測定すると `0` が $|1\rangle$ を測定すると `1` が確率 1 で得られる。しかし量子ビットはこの 2 つだけではない。基本的な量子ビットを $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ というように 2 次元ベクトルと同一視することにしよう。一般の量子ビットは次のように表せる。

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}.$$

ここで α と β は $\alpha^2 + \beta^2 = 1$ を満たす実数である[1]。この量子状態 $|\psi\rangle$ を「測定」すると測定結果 `0` と `1` がそれぞれ確率 α^2 と β^2 で得られる。「なあんだ、量子ビットというのは確率的なビットのことか」と思うかもしれないが、その理解は正しくないことを付録 Aで説明する。

次に 2 量子ビットとして基本的なものは次の 4 つである。

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \qquad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \qquad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \qquad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

[1]本当は実数だけじゃなく複素数も許されているのだが、簡単のため実数としておく。

そして一般の 2 量子ビットは次のように表せる。

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{bmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{bmatrix}.$$

ここで、係数 $\alpha, \beta, \gamma, \delta$ は $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$ を満たす実数である。この量子状態 $|\psi\rangle$ を「測定」すると測定結果 `00`, `01`, `10`, `11` がそれぞれ確率 α^2, β^2, γ^2, δ^2 で得られる。3 量子ビット以上も同様である。n 量子ビットは 2^n 次元ベクトルで表される。この 2^n 次元ベクトルの要素を上から順に 0 から $2^n - 1$ とインデックスをつけると都合がよい。ビット列 $b_0 b_1 \cdots b_{n-1}$ について、n 量子ビット状態 $|b_{n-1}b_{n-2}\cdots b_0\rangle$ はインデックスが $\sum_{i=0}^{n-1} 2^i b_i$ の成分が 1 でそれ以外の成分が 0 のベクトルと同一視できる。例えば、3 量子ビットの状態 $|110\rangle$ は $2^3 = 8$ 次元ベクトルで

$$|110\rangle = \begin{array}{c@{\quad}c} \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix} & \begin{array}{c}000\\001\\010\\011\\100\\101\\110\\111\end{array} \end{array}$$

というようにインデックスの二進数表現が `110` の成分が 1 でそれ以外の成分が 0 のベクトルと見なせる。

3　量子回路

古典計算の計算モデルの一つに古典回路がある。古典回路はビット列を入力にとり、NOT(否定)、AND(論理積)、OR(論理和) という 3 種類のゲートを適用することで出力を計算する。任意の二元関数はこれら 3 種類のゲートの組み合わせで書ける。量子計算の一番標準的な計算モデルである量子回路はこの古典回路を量子ビットと量子ゲートに置き換えたものである。今回考える量子回路は X (パウリ X 変換), Z (パウリ Z 変換), H (アダマール変換)、CX (コントロール X 変換)、CZ (コントロール Z 変換)、CCX (トフォリ変換) という 6 種類の量子ゲートからなる。この 6 種類の量子ゲートを組み合わせれば任意の「量子状態の変換」が任意の精度で近似できることが知られている[2]。これらの量子ゲートを説明する。まず始めにこれらの量子ゲートは「線形変換」である。1 量子ビットに対する量子ゲート A の場合、$|0\rangle$ と $|1\rangle$ の変換先を $A|0\rangle$ と $A|1\rangle$ と書くことにすると、任意の 1 量子ビット $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ は $A|\psi\rangle = \alpha(A|0\rangle) + \beta(A|1\rangle)$ に変換される。なので 1 量子ビットゲートの場合は $|0\rangle$ と $|1\rangle$ の変換先を決めれば、一般の量子状態の変換先は自動的に定まる。以下、$|0\rangle$ と $|1\rangle$ が各量子ゲートによって何に変換されるかを定義していく。

- **パウリ X 変換**
  パウリ X 変換は $|0\rangle$ を $|1\rangle$ に $|1\rangle$ を $|0\rangle$ に変換する量子ゲートである。古典ゲートの NOT に対応するものである。回路図による表現は次のようになる。

  $$|x\rangle \;—\boxed{X}—\; |\overline{x}\rangle$$

  ここで、$\overline{x}$ は $1 - x$ である。

[2] 今回複素数を導入しないので、「限定された量子状態の上の変換」と言った方が正しい。

- **パウリ Z 変換**
  パウリ Z 変換は $|0\rangle$ を $|0\rangle$ に $|1\rangle$ を $-|1\rangle$ に変換する量子ゲートである。回路図による表現は次のようになる。

$$|x\rangle \;—\boxed{Z}—\; (-1)^x\,|x\rangle$$

- **アダマール変換**
  アダマール変換は $|0\rangle$ を $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ に $|1\rangle$ を $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ に変換する量子ゲートである。回路図による表現は次のようになる。

$$|x\rangle \;—\boxed{H}—\; \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^x\,|1\rangle)$$

例えば、アダマール変換してからパウリ X 変換してアダマール変換する操作は

$$\begin{aligned}
HXH\,|0\rangle &= HX\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |0\rangle \\
HXH\,|1\rangle &= HX\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} - \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = -|1\rangle
\end{aligned}$$

を満たす。よって $HXH = Z$ という量子ゲートに関する等式が得られる。

一般に n 量子ビットの k 番目の量子ビットに上記の 1 量子ビット向けの量子ゲートを適用した場合は、「対応する量子ビットだけが変換される」。量子ゲート U を k 番目の量子ビットに適用する操作を $U^{(k)}$ と書くことにすると、

$$\begin{aligned}
X^{(k)}\,|b_{n-1}\cdots b_0\rangle &= |b_{n-1}\cdots b_{k+1}\overline{b_k}b_{k-1}\cdots b_0\rangle \\
Z^{(k)}\,|b_{n-1}\cdots b_0\rangle &= (-1)^{b_k}\,|b_{n-1}\cdots b_0\rangle \\
H^{(k)}\,|b_{n-1}\cdots b_0\rangle &= \frac{1}{\sqrt{2}}\left(|b_{n-1}\cdots b_{k+1}\,0\,b_{k-1}\cdots b_0\rangle + (-1)^{b_k}\,|b_{n-1}\cdots b_{k+1}\,1\,b_{k-1}\cdots b_0\rangle\right)
\end{aligned}$$

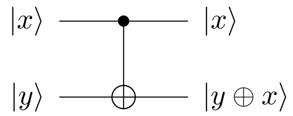
が成り立つ。

次に複数量子ビットに対する量子ゲートを定義する。1 量子ビットの場合と同様に、2 量子ビットゲートは $|00\rangle$ から $|11\rangle$ までの変換先を定義すればよい (3 量子ビットゲートは $|000\rangle$ から $|111\rangle$ までの変換先を定義すればよい)。以下では、$x, y \in \{0, 1\}$ について、$|yx\rangle$ の変換先を定義していく (3 量子ビットゲートについては $x, y, z \in \{0, 1\}$ について、$|zyx\rangle$ の変換先を定義していく)。

- **コントロール X 変換**
  $|x\rangle$ を「コントロール量子ビット」、$|y\rangle$ を「ターゲット量子ビット」とするコントロール X 変換は x が 0 のときは何もせず、1 のときは y を反転させる量子ゲートである。2 量子ビット $|yx\rangle$ は次のルールで変換される。

$$\begin{aligned}
|00\rangle &\longmapsto |00\rangle \\
|01\rangle &\longmapsto |11\rangle \\
|10\rangle &\longmapsto |10\rangle \\
|11\rangle &\longmapsto |01\rangle
\end{aligned}$$

  回路図による表現は次のようになる。

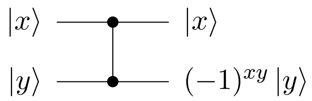


  ここで $\oplus$ は排他的論理和 ($x \oplus y = 0 \iff x = y$ で定義される $\{0, 1\}$ 上の二項演算) である。

- **コントロール Z 変換**
  コントロール Z 変換は x と y がともに 1 の時に -1 を掛ける量子ゲートである。x もしくは y が 0 の時は何もしない。2 量子ビット $|yx\rangle$ は次のルールで変換される。

$$
\begin{aligned}
|00\rangle &\longmapsto |00\rangle \\
|01\rangle &\longmapsto |01\rangle \\
|10\rangle &\longmapsto |10\rangle \\
|11\rangle &\longmapsto -|11\rangle
\end{aligned}
$$

  回路図による表現は次のようになる。

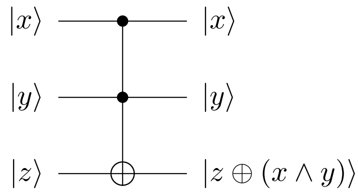


  コントロール Z 変換は x と y について対称であり、どちらがコントロール量子ビットでどちらがターゲット量子ビットであるという区別はない。

- **トフォリ変換**
  $|x\rangle$ と $|y\rangle$ を「コントロール量子ビット」、$|z\rangle$ を「ターゲット量子ビット」とするトフォリ変換は x と y がともに 1 の時に z を反転させる量子ゲートである。x もしくは y が 0 の時は何もしない。3 量子ビット $|zyx\rangle$ は次のルールで変換される。

$$
\begin{aligned}
|000\rangle &\longmapsto |000\rangle \\
|001\rangle &\longmapsto |001\rangle \\
|010\rangle &\longmapsto |010\rangle \\
|011\rangle &\longmapsto |111\rangle \\
|100\rangle &\longmapsto |100\rangle \\
|101\rangle &\longmapsto |101\rangle \\
|110\rangle &\longmapsto |110\rangle \\
|111\rangle &\longmapsto |011\rangle
\end{aligned}
$$

  回路図による表現は次のようになる。



  ここで $\wedge$ は論理積 ($x \wedge y = 1 \iff x = y = 1$ で定義される $\{0,1\}$ 上の二項演算) である。

1 量子ビットに対する量子ゲートと同様に、n 量子ビットの一部に複数量子ビットのゲートを適用した場合は「それらの量子ビットだけが変換される」。例えば、$n-1 \geq i > j > k \geq 0$ について、i 番目と j 番目の量子ビットをコントロール量子ビットとして k 番目の量子ビットをターゲット量子ビットとするトフォリ変換は次のように作用する。

$$
|b_{n-1} \cdots b_i \cdots b_j \cdots b_k \cdots b_0\rangle \longmapsto |b_{n-1} \cdots b_i \cdots b_j \cdots (b_k \oplus (b_i \wedge b_j)) \cdots b_0\rangle
$$

4　本選問題: 量子回路のシミュレーション

4.1　概要

問題の入力として量子回路を与える。$|00\cdots0\rangle$ をその量子回路への入力とした場合の量子回路の出力を測定した時に、得られる確率が一番高い測定結果とその確率を問題の解とする。

4.2　問題の入力

入力は

$$
\begin{array}{ll}
N & K \\
G_1 & O_1 \\
G_2 & O_2 \\
& \vdots \\
G_K & O_K
\end{array}
$$

で与えられる。各変数の取り得る値は

$$
\begin{aligned}
&25 \le N \le 30 \\
&500 \le K \le 2000 \\
&G_i \in \{\,\mathsf{X}, \mathsf{Z}, \mathsf{H}, \mathsf{CX}, \mathsf{CZ}, \mathsf{CCX}\,\}, \qquad \forall i \in \{1, 2, \ldots, K\}, \qquad \text{ただし H の総数は 125 以下} \\
&O_i = \begin{cases} a, & \text{if} \quad G_i \in \{\,\mathsf{X}, \mathsf{Z}, \mathsf{H}\,\} \\ a\ b, & \text{if} \quad G_i \in \{\,\mathsf{CX}, \mathsf{CZ}\,\} \\ a\ b\ c, & \text{if} \quad G_i = \mathsf{CCX} \end{cases}, \qquad \begin{array}{l} 0 \le a, b, c \le N-1, \\ a, b, c \text{ は相異なる} \end{array} \qquad \forall i \in \{1, 2, \ldots, K\}
\end{aligned}
$$

である。ここで N は量子ビットの数、K は量子ゲートの数である。その後の K 行に量子ゲートの内容が示されている。各 G_i は量子ゲートの種類を表しており、X, Z, H, CX, CZ, CCX のいずれかである。ここで、X, Z, H, CX, CZ, CCX はそれぞれ、パウリ X 変換、パウリ Z 変換、アダマール変換、コントロール X 変換、コントロール Z 変換、トフォリ変換を表す。各 O_i は量子ゲートが適用される量子ビットのインデックス (0 以上 $N-1$ 以下) の列である。複数の量子ビットにかかる量子ゲートについては、最後のインデックスがターゲット量子ビットである。例えば

```
CX 4 3
```

は 4 番目の量子ビットがコントロール量子ビットで 3 番目の量子ビットがターゲット量子ビットである。同様に

```
CCX 0 19 2
```

は 0 番目, 19 番目の量子ビットがコントロール量子ビットで 2 番目の量子ビットがターゲット量子ビットである。これらの量子ゲートを G_1 から G_K まで順番に適用する量子回路を C とおく。

4.3　問題の解

$|00\cdots0\rangle$ を量子回路 C の入力としたときに、量子回路 C から出力される量子状態を測定した際に得られる確率が一番高い測定結果とその確率を問題の解とする。ただし、測定結果 $b_{N-1}b_{N-2}\cdots b_0$ について、$\sum_{i=0}^{N-1} 2^i b_i$ の十進数表現を出力する。確率は相対誤差 10^{-5} 未満を正解とする。測定確率が等しいものが複数ある場合はどれを出力しても構わない。出力のフォーマットは

測定確率最大の測定結果の一つの十進数表現
その測定確率

とする。測定確率の出力は `printf("%e\n", max_probability);` のようにすればよい。

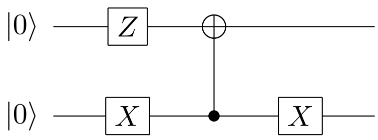
4.4 入出力例

簡単のため、N や K が小さい場合の入出力例を示す。実際の評価では $25 \leq N \leq 30$, $500 \leq K \leq 2000$ の範囲の場合だけを考える。

4.4.1 入出力例 1

```
2 4
X 1
Z 0
CX 1 0
X 1
```

回路図は次のようになる。



量子ゲートを順に適用しておくと量子ビットは順に

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

と変換される。そのため量子回路の出力は $|01\rangle$ となる。これを測定すると、`01` が確率 1 で得られる。そのため、問題の出力は

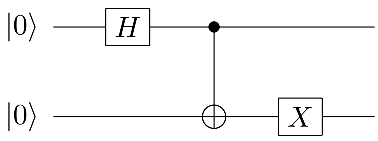
```
1
1.0
```

となる。

4.4.2 入出力例 2

```
2 3
H 0
CX 0 1
X 1
```

回路図は次のようになる。



量子ゲートを順に適用しておくと量子ビットは順に

$$|00\rangle \longmapsto \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \longmapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \longmapsto \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

と変換される。そのため量子回路の出力は $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$ となる。これを測定すると、`10` と `01` がそれぞれ確率 1/2 で得られる。そのため、問題の出力は

```
1
0.5
```

もしくは

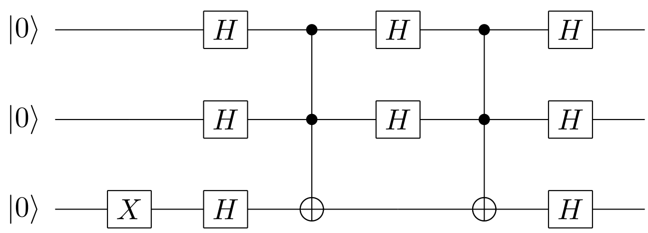
```
2
0.5
```

となる。

4.4.3 入出力例 3

```
3 11
X 2
H 0
H 1
H 2
CCX 0 1 2
H 0
H 1
CCX 0 1 2
H 0
H 1
H 2
```

回路図は次のようになる。



量子ゲートを順に適用しておくと量子ビットは順に

$$
\begin{aligned}
&|000\rangle \longmapsto |100\rangle \longmapsto \frac{1}{\sqrt{2}}(|100\rangle + |101\rangle) \longmapsto \frac{1}{2}(|100\rangle + |110\rangle + |101\rangle + |111\rangle) \\
&\longmapsto \frac{1}{2\sqrt{2}}(|000\rangle - |100\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle + |011\rangle - |111\rangle) \\
&\longmapsto \frac{1}{2\sqrt{2}}(|000\rangle - |100\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle + |111\rangle - |011\rangle) \\
&\longmapsto \frac{1}{2}(|000\rangle - |100\rangle + |011\rangle - |111\rangle) \\
&\longmapsto \frac{1}{2\sqrt{2}}(|000\rangle + |010\rangle - |100\rangle - |110\rangle + |001\rangle - |011\rangle - |101\rangle + |111\rangle) \\
&\longmapsto \frac{1}{2\sqrt{2}}(|000\rangle + |010\rangle - |100\rangle - |110\rangle + |001\rangle - |111\rangle - |101\rangle + |011\rangle) \\
&\longmapsto \frac{1}{2}(|000\rangle + |010\rangle - |100\rangle - |110\rangle) \\
&\longmapsto \frac{1}{\sqrt{2}}(|000\rangle - |100\rangle) \\
&\longmapsto |100\rangle
\end{aligned}
$$

と変換される。そのため量子回路の出力は $|100\rangle$ となる。これを測定すると、`100` が確率 1 で得られる。そのため、問題の出力は

```
4
1.0
```

となる。

4.5 評価方法

プログラムのコンパイルは

```
nvcc program.cu -O2 -arch=sm_60
```

で行う。速度を評価するための入力は配布の `gen.cpp` を用いて生成する。$25 \leq N \leq 30$, $500 \leq K \leq 2000$ の範囲で入力を生成し、計算結果と実行時間を評価する。速度差が判別できるくらい十分多くの入力を用いて評価する。順位付けは

- 計算結果が正しいものが多い方が上位
- 計算結果が正しいものが同数の場合は実行時間の総和が小さい方が上位

というルールに従って決める。上位は全問正解するものと期待している。結局のところ $N = 30$ の場合が一番時間がかかるので、そこで一番差がつくと考えている。

A　ベルの不等式 (本選問題と直接は関係がない)

そもそも量子力学とは何なのか？古典力学とどう違うのか？最短距離で説明する。次のゲームを考えよう。

CHSH ゲーム

遠く離れ通信ができないアリスとボブが次のようなゲームをする。アリスは $x \in \{0,1\}$ を受け取り、ボブは $y \in \{0,1\}$ を受け取る。アリスとボブはそれぞれ $a \in \{0,1\}$ と $b \in \{0,1\}$ を出力し、それらが $a \oplus b = x \wedge y$ を満たすとき、アリスとボブの勝ちとする。

さて、入力 x と y が一様な確率で選ばれるとしたときに、CHSH ゲームの最大勝率はいくつになるだろう？x から決まる a の値を a_x、y から決まる b の値を b_y と書くことにする。各 x, y について勝利条件を書き下すと次のようになる。

$$
\begin{aligned}
a_0 \oplus b_0 &= 0 \wedge 0 = 0,\\
a_0 \oplus b_1 &= 0 \wedge 1 = 0,\\
a_1 \oplus b_0 &= 1 \wedge 0 = 0,\\
a_1 \oplus b_1 &= 1 \wedge 1 = 1.
\end{aligned}
$$

この 4 つの式のうち 1 つが 1/4 の確率で選ばれ、それが満たされていれば勝ちということになる。この 4 つの式を足すと $0 = 1$ となるので、全ての式を満たすように (a_0, a_1, b_0, b_1) を決めることは不可能である。一方で、$a_0 = a_1 = b_0 = b_1 = 0$ とおくと、3 つの式は満たされる。よって、最大の勝率は $3/4 = 0.75$ となる。これは、アリスとボブがランダムビットを共有していても変わらない。しかし、量子状態を共有していると最大の勝率は $(2 + \sqrt{2})/4 \approx 0.854$ になる！この現象のことを「ベルの不等式の破れ (もしくは CHSH 不等式の破れ)」という。

実際にゲームの中で現れる値は a_x と b_y だが、現れない値 $a_{\overline{x}}$ と $b_{\overline{y}}$ も存在している、と考えるのが自然である。しかし、(a_0, a_1, b_0, b_1) の同時確率分布が存在していると、CHSH ゲームの最大勝率は 3/4 を超えない。よって、ベルの不等式の破れは a_0, a_1, b_0, b_1 という 4 つの値が同時に存在していないことを示している。観測するしないに関わらず、確率的にせよ観測値が存在しているという理解では量子力学を説明できないのである。このように、量子力学においては観測したときに観測値が定まると考えるほかない。

具体的に最大の勝率 $(2 + \sqrt{2})/4$ を達成するためには、アリスとボブは次の 2 量子ビット状態を共有している必要がある。

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

一つ目がアリスの持っている量子ビットで二つ目がボブが持っている量子ビットと考える。アリスとボブがそれぞれ x と y の値に応じて、量子ビットを操作してから測定することで勝率 $(2 + \sqrt{2})/4$ が達成できる。