Quantum Covert Lottery

高速化ではない量子コンピュータの応用

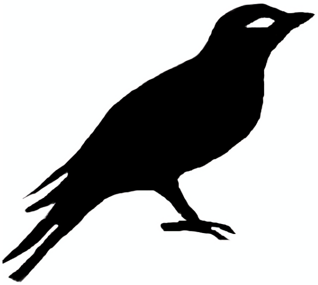
吉村 優（Yoshimura Hikaru）

yyu@mental.poker

October 8, 2023 @ 第 56 回 情報科学若手の会

https://github.com/y-yu/quantum-covert-lottery-slide（7bc1a4f）

自己紹介



Twitter @_yyu_
GitHub y-yu

- 筑波大学 情報学群 情報科学類卒（2011-15, 学士）
  - プログラム論理研究室で型システムの研究
- 未踏ターゲット 2018（ゲート式量子コンピュータ）
- CTF（`https://urandom.team/`）
  - SECCON CTF 2023 Quals 72 位（国内 26 位）
- iOS・macOS 向けコーヒー抽出支援アプリ☕
- プログラミング
  - Scala, LaTeX, Rust, Swift
  - SATySFiのバージョン `0.1.0` 待ってます！ 🙏

目次

1. Covert Lottery とは？
2. 古典 Covert Lottery と情報リーク
3. 量子コンピュータとシュレディンガーの猫
4. 量子ゲートテレポーテーション
5. Quantum Covert Lottery
6. まとめ

Covert Lottery とは？

- *Covert Lottery* は [1] で提案された、ちょっと変わった抽選

Covert Lotteryとは？

- *Covert Lottery* は [1] で提案された、ちょっと変わった抽選

> 参加者 2 人が 1bit（= 0 or 1）のいずれかの希望があるとき、
> 1. 二人の希望が一致していれば、それが採用される
> 2. 衝突していたらランダムにする

Covert Lottery とは？

- *Covert Lottery* は [1] で提案された、ちょっと変わった抽選

“

参加者 2 人が 1bit（= 0 or 1）のいずれかの希望があるとき、

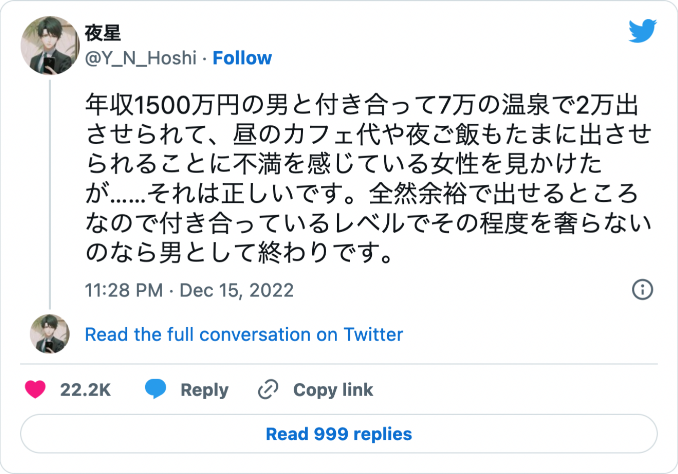
1. 二人の希望が一致していれば、それが採用される
2. 衝突していたらランダムにする

”

いったい何に使えるのか？

🤔

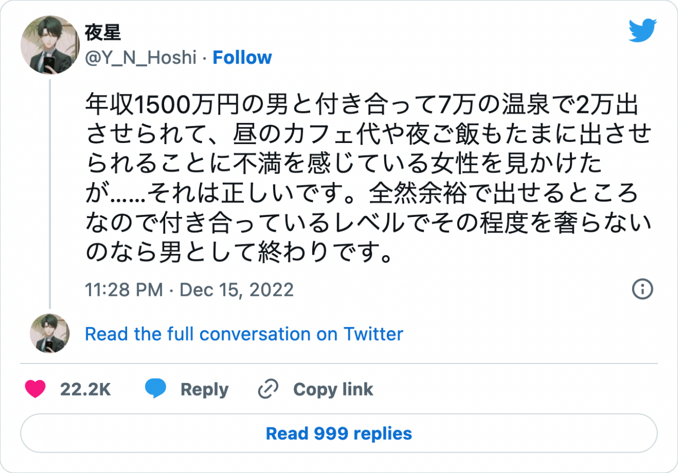
奢り・割り勘問題†



[2]

† [1] では将棋などの先攻・後攻を決める問題を例にしている。

奢り・割り勘問題†



[2]

👉 これか！？

†[1] では将棋などの先攻・後攻を決める問題を例にしている。

奢り・割り勘問題

“

アリスとボブの飲食費について下記のいずれにするか決定する問題

1. ボブが全額を奢る
2. 割り勘とする

”

アリス（*Alice*）

ボブ（*Bob*）

カードを用いた古典 Covert Lottery§

次のように物理的なカード‡を用いて行う

‡これらのカードはトランプのようにいずれも裏が $\boxed{?}$ となっており、裏向きになった状態でどちらのカードなのか特定することができない。

§[1] では 3 人以上への拡張も踏まえてやや複雑な方法が説明されており、このプロトコルは発表者が 2 人を前提に独自に簡略化したものとなっている。

カードを用いた古典 Covert Lottery§

次のように物理的なカード‡を用いて行う

1. アリス・ボブに 2 枚のカード ♥, ♣ を配る
2. アリス・ボブは表 1 に従って希望を裏向き ? にして提出する
3. 2 で提出されたカードをシャッフルする
4. どちらか 1 枚をドローして表向きにする

4 のカードを表 1 に対応させてプロトコルの結果とする

表 1: カードの意味

カード	意味
♥	ボブの奢り
♣	割り勘

‡これらのカードはトランプのようにいずれも裏が ? となっており、裏向きになった状態でどちらのカードなのか特定することができない。

§[1] では 3 人以上への拡張も踏まえてやや複雑な方法が説明されており、このプロトコルは発表者が 2 人を前提に独自に簡略化したものとなっている。

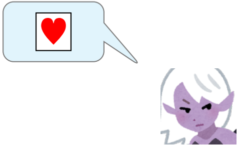
ケーススタディ❶ — 2 人の希望が一致

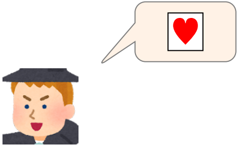
ケーススタディ❶ — 2 人の希望が一致

- 2 人の希望が一致しているので次のようなケース

ケーススタディ❶ — 2 人の希望が一致

- 2 人の希望が一致しているので次のようなケース





- これらをシャッフルして 1 枚選んだときは必ず♥となる

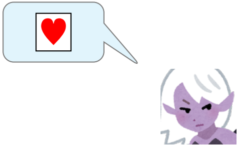
ケーススタディ❶ — 2 人の希望が一致

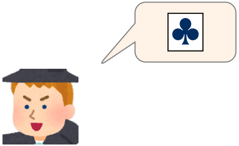
- 2 人の希望が一致しているので次のようなケース

- これらをシャッフルして 1 枚選んだときは必ずとなる
- 2 人の希望が一致していればこのように必ずそちらが選ばれる

ケーススタディ❷ — 2 人の希望が衝突

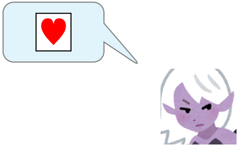
- 2 人の希望が衝突しているので次のようなケース

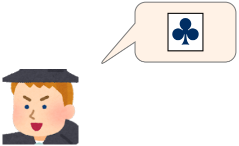




ケーススタディ❷ — 2 人の希望が衝突

- 2 人の希望が衝突しているので次のようなケース

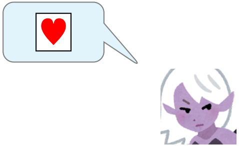


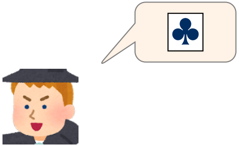


- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

ケーススタディ❷ — 2 人の希望が衝突

- 2 人の希望が衝突しているので次のようなケース





- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

結果が♥ アリスの希望どおり

ケーススタディ❷ — 2 人の希望が衝突

- 2 人の希望が衝突しているので次のようなケース

- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

結果が♥ アリスの希望どおり
結果が♣ ボブの希望どおり

ケーススタディ❷ — 2 人の希望が衝突

- 2 人の希望が衝突しているので次のようなケース

- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

  結果が♥ アリスの希望どおり
  結果が♣ ボブの希望どおり
  このように 2 つの結果がそれぞれ 50%のランダムとなる

Covert Lottery と情報リーク

- Covert Lottery は場合によって**情報リーク**を起こす

Covert Lottery と情報リーク

- Covert Lottery は場合によって**情報リーク**を起こす

アリスが不本意に
割り勘となってしまった場合、
ボブの希望は割り勘だと特定する

- アリスが不本意に割り勘となった場合、アリスは奢りを希望していたがボブは割り勘を希望しており、ランダムで割り勘となった

Covert Lottery と情報リーク

- Covert Lottery は場合によって**情報リーク**を起こす

アリスが不本意に
割り勘となってしまった場合、
ボブの希望は割り勘だと特定する

しかしこのときボブは
アリスの希望が分からない

- アリスが不本意に割り勘となった場合、アリスは奢りを希望していたがボブは割り勘を希望しており、ランダムで割り勘となった
- このように希望通りになった側は相手の希望が分からず、希望通りにならかった側は相手の希望を知ることができる

Covert Lottery と情報リーク

逆にボブが不本意に奢った場合はアリスの奢られ希望が分かる

Covert Lottery と情報リーク

逆にボブが不本意に奢った場合はアリスの奢られ希望が分かる

このときアリスはボブの奢りが本意か
不本意か分からないが、奢られを得る

量子コンピュータとシュレディンガーの猫

1. Covert Lottery とは？
2. 古典 Covert Lottery と情報リーク
3. 量子コンピュータとシュレディンガーの猫
4. 量子ゲートテレポーテーション
5. Quantum Covert Lottery
6. まとめ

- Covert Lottery をカードで実装した

量子コンピュータとシュレディンガーの猫

1 Covert Lottery とは？

2 古典 Covert Lottery と情報リーク

3 量子コンピュータとシュレディンガーの猫

4 量子ゲートテレポーテーション

5 Quantum Covert Lottery

6 まとめ

- Covert Lottery をカードで実装した
- カードではなくて量子コンピュータでやりたい

量子コンピュータとシュレディンガーの猫

1. Covert Lottery とは？
2. 古典 Covert Lottery と情報リーク
3. 量子コンピュータとシュレディンガーの猫
4. 量子ゲートテレポーテーション
5. Quantum Covert Lottery
6. まとめ

- Covert Lottery をカードで実装した
- カードではなくて量子コンピュータでやりたい
- まずは量子コンピュータの基礎的なところを解説

量子コンピュータ

量子コンピュータ

- 古典コンピュータは 1bit で ♥, ♣ のような 2 つの値 0, 1 しか持たない

量子コンピュータ

- 古典コンピュータは 1bit で♥,♣のような 2 つの値 0, 1 しか持たない
- 一方で量子コンピュータの 1bit に相当する**量子ビット**（*qubit*）は 2 つの複素数 c_0, c_1 によって式 1 のように拡張される

$$c_0 |0\rangle + c_1 |1\rangle \tag{1}$$

量子コンピュータ

- 古典コンピュータは 1bit で♥,♣のような 2 つの値 0, 1 しか持たない
- 一方で量子コンピュータの 1bit に相当する**量子ビット**（*qubit*）は 2 つの複素数 c_0, c_1 によって式 1 のように拡張される

$$c_0 |0\rangle + c_1 |1\rangle \tag{1}$$

- 古典コンピュータの 1bit と同じ $|0\rangle, |1\rangle$ のとき、c_0, c_1 はそれぞれ次のようになる
  - $|0\rangle$ $c_0 = 1, c_1 = 0$
  - $|1\rangle$ $c_0 = 0, c_1 = 1$

量子コンピュータ

- 古典コンピュータは 1bit で♥, ♣のような 2 つの値 0, 1 しか持たない
- 一方で量子コンピュータの 1bit に相当する**量子ビット**（*qubit*）は 2 つの複素数 c_0, c_1 によって式 1 のように拡張される

$$c_0 \left|0\right\rangle + c_1 \left|1\right\rangle \tag{1}$$

- 古典コンピュータの 1bit と同じ $\left|0\right\rangle, \left|1\right\rangle$ のとき、c_0, c_1 はそれぞれ次のようになる
  - $\left|0\right\rangle$ $c_0 = 1, c_1 = 0$
  - $\left|1\right\rangle$ $c_0 = 0, c_1 = 1$
- ちなみに $\left|0\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \left|1\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ のように行列で表せる

$$c_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

量子コンピュータ

$$c_0 |0\rangle + c_1 |1\rangle \tag{1}$$

- 式 1 の複素数 c_0, c_1 は**確率振幅**と呼ばれ、次のように $|0\rangle, |1\rangle$ が観測される確率を得ることができる

  $|0\rangle$ が観測される確率 $|c_0|^2$
  $|1\rangle$ が観測される確率 $|c_1|^2$

量子コンピュータ

$$c_0 |0\rangle + c_1 |1\rangle \tag{1}$$

- 式 1 の複素数 c_0, c_1 は**確率振幅**と呼ばれ、次のように $|0\rangle, |1\rangle$ が観測される確率を得ることができる

  $|0\rangle$ が観測される確率 $|c_0|^2$
  $|1\rangle$ が観測される確率 $|c_1|^2$
- 確率なので、c_0, c_1 は次の条件式 2 を満たす

$$|c_0|^2 + |c_1|^2 = 1 \tag{2}$$

量子コンピュータ

$$c_0 |0\rangle + c_1 |1\rangle \tag{1}$$

- 式 1 の複素数 c_0, c_1 は**確率振幅**と呼ばれ、次のように $|0\rangle, |1\rangle$ が観測される確率を得ることができる
  $|0\rangle$ が観測される確率　$|c_0|^2$
  $|1\rangle$ が観測される確率　$|c_1|^2$
- 確率なので、c_0, c_1 は次の条件式 2 を満す

$$|c_0|^2 + |c_1|^2 = 1 \tag{2}$$

- 一方で c_0, c_1 の具体的な値を直接知る方法はない

ブロッホ球

- 複素数は実数 a, b を用いて $a + b\sqrt{-1}$ のように表現される

ブロッホ球

- 複素数は実数 a, b を用いて $a + b\sqrt{-1}$ のように表現される
- 1qubit の表現に 2 つの複素数 c_0, c_1 が必要なので、4 変数の自由度があるが下記 2 つの条件により**球の表面座標**と考えることができる
  1. 確率の満す条件式 2
  2. c_0 が実数になるように c_1 を調整してもいい（同じとみなせる qubit が存在する）

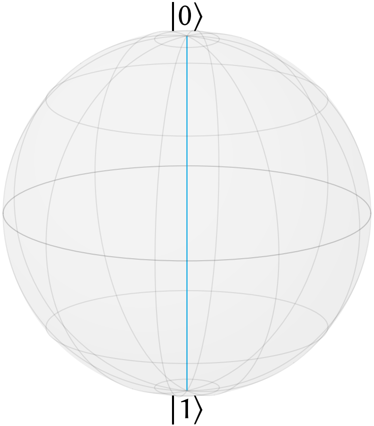


図 1: ブロッホ球

ブロッホ球

- 複素数は実数 a, b を用いて $a + b\sqrt{-1}$ のように表現される
- 1qubit の表現に 2 つの複素数 c_0, c_1 が必要なので、4 変数の自由度があるが下記 2 つの条件により**球の表面座標**と考えることができる
  1. 確率の満す条件式 2
  2. c_0 が実数になるように c_1 を調整してもいい（同じとみなせる qubit が存在する）
- この球を**ブロッホ球**と呼び、たとえば $|0\rangle$ や $|1\rangle$ はそれぞれ球の北極と南極の座標に対応する

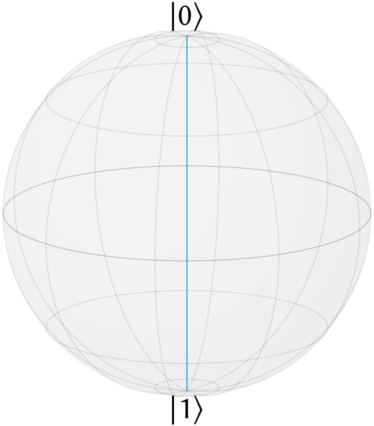


図 1: ブロッホ球

シュレディンガーの猫

- **シュレディンガーの猫**で有名なように、量子ビットは $|0\rangle, |1\rangle$ の“重なった”状態を表現できる

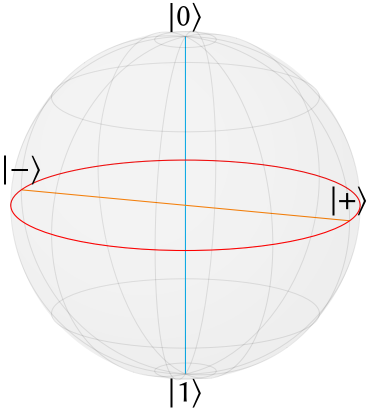


図 2: ブロッホ球上の $|\pm\rangle$

- **シュレディンガーの猫**で有名なように、量子ビットは $|0\rangle, |1\rangle$ の "重なった" 状態を表現できる
- $c_0 = \frac{1}{\sqrt{2}}, c_1 = \pm\frac{1}{\sqrt{2}}$ な量子ビット $|\pm\rangle$ を考える

$$\begin{cases} |+\rangle & \equiv & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle & \equiv & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

  - $|\pm\rangle$ はブロッホ球の赤道上（図 2）となる

シュレディンガーの猫

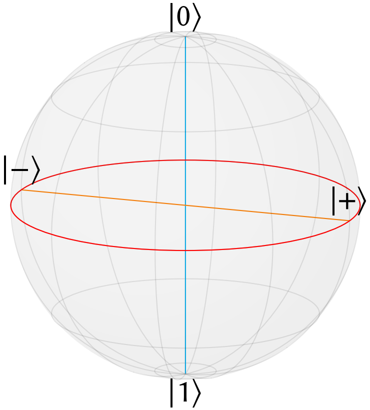


図 2: ブロッホ球上の $|\pm\rangle$

- **シュレディンガーの猫**で有名なように、量子ビットは $|0\rangle, |1\rangle$ の "重なった" 状態を表現できる
- $c_0 = \frac{1}{\sqrt{2}}, c_1 = \pm\frac{1}{\sqrt{2}}$ な量子ビット $|\pm\rangle$ を考える

$$\begin{cases} |+\rangle & \equiv & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle & \equiv & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

  - $|\pm\rangle$ はブロッホ球の赤道上（図 2）となる
- $|\pm\rangle$ は $|0\rangle, |1\rangle$ が観測される確率がそれぞれ $\left|\pm\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ になる

シュレディンガーの猫のシミュレータ実験

シュレディンガーの猫のシミュレータ実験

- IBM Quantum Composer[†]でシミュレーション してみる

[†] https://quantum-computing.ibm.com/composer/
[‡] "アダマールゲート" と読む。

シュレディンガーの猫のシミュレータ実験

- IBM Quantum Composer† でシミュレーションしてみる
- 初期値である $|0\rangle$ から $|+\rangle$ を作るために**量子ゲート**を使う

† https://quantum-computing.ibm.com/composer/
‡ "アダマールゲート" と読む。

シュレディンガーの猫のシミュレータ実験

- IBM Quantum Composer[†]でシミュレーションしてみる
- 初期値である $|0\rangle$ から $|+\rangle$ を作るために**量子ゲート**を使う
- H ゲート[‡]は図 3 の n を中心に π 回転させるので、$|0\rangle$ が $|+\rangle$ へ移る

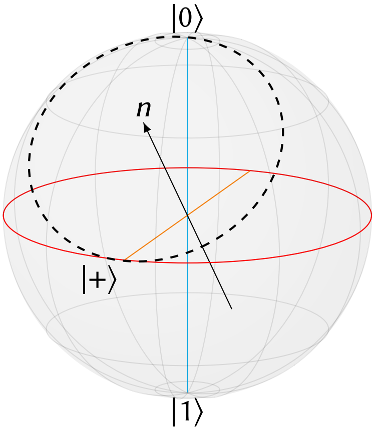
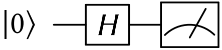


図 3: H ゲートの回転中心 n

[†] https://quantum-computing.ibm.com/composer/
[‡] “アダマールゲート” と読む。

シュレディンガーの猫のシミュレータ実験

- IBM Quantum Composer† でシミュレーションしてみる
- 初期値である $|0\rangle$ から $|+\rangle$ を作るために**量子ゲート**を使う
- H ゲート‡は図 3 の $\boldsymbol{n}$ を中心に π 回転させるので、$|0\rangle$ が $|+\rangle$ へ移る
- $|+\rangle$ を $\{|0\rangle, |1\rangle\}$ で測定する次のような回路をやってみる



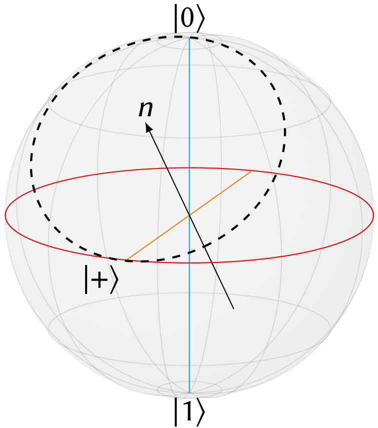


図 3: H ゲートの回転中心 $\boldsymbol{n}$

†https://quantum-computing.ibm.com/composer/
‡"アダマールゲート" と読む。

シュレディンガーの猫のシミュレータ実験

- 結果は図 4 のように、$|0\rangle$ と $|1\rangle$ が $\frac{1}{2}$ の確率でそれぞれ測定されている

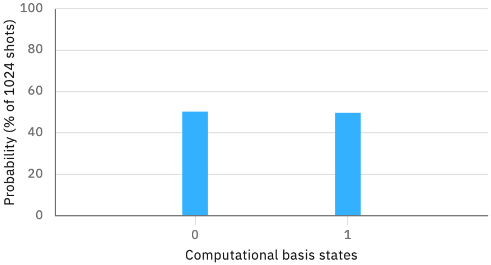


図 4: H ゲート回路の測定結果

シュレディンガーの猫のシミュレータ実験

- 結果は図 4 のように、$|0\rangle$ と $|1\rangle$ が $\frac{1}{2}$ の確率でそれぞれ測定されている
- これで量子回路としてシュレディンガーの猫が完成🐱

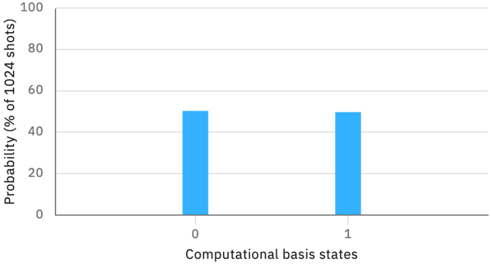
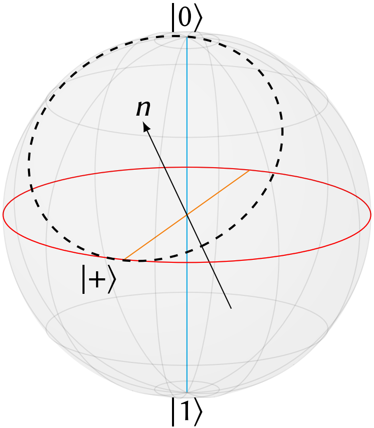
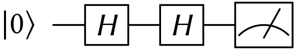


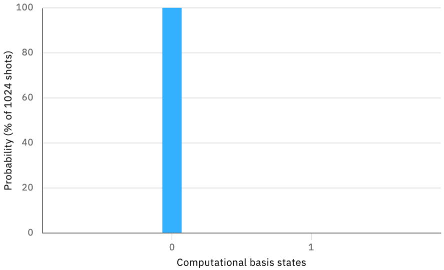
図 4: H ゲート回路の測定結果

シュレディンガーの猫のシミュレータ実験



- H ゲートは n 中心に π 回転なので次のように 2 回やれば元の $|0\rangle$ に戻る





- 同様に $H\,|1\rangle = |-\rangle$ かつ $H\,|-\rangle = |1\rangle$ となる

他の量子ゲート❶ – X ゲート

他の量子ゲート❶ — X ゲート

- X ゲートは図 5 の X 軸を中心に π 回転させるゲート

$$X\left|0\right\rangle = \left|1\right\rangle, X\left|1\right\rangle = \left|0\right\rangle$$

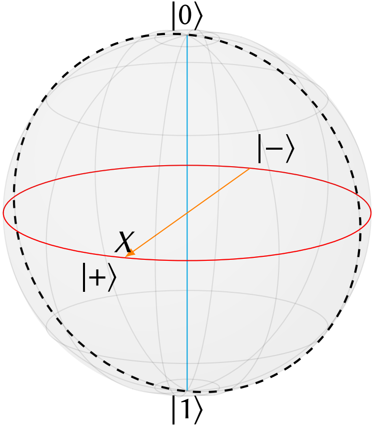


図 5: X ゲートの回転中心

他の量子ゲート❶ — X ゲート

- X ゲートは図 5 の X 軸を中心に π 回転させるゲート

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

- 古典コンピュータの NOT ゲートと似ている

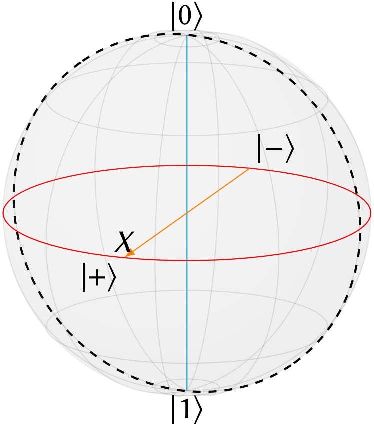


図 5: X ゲートの回転中心

他の量子ゲート❶ – X ゲート

- X ゲートは図 5 の X 軸を中心に π 回転させるゲート

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

- 古典コンピュータの NOT ゲートと似ている
- X 軸上の $|\pm\rangle$ に X ゲートを作用させても何も起きない

$$X|\pm\rangle = |\pm\rangle$$

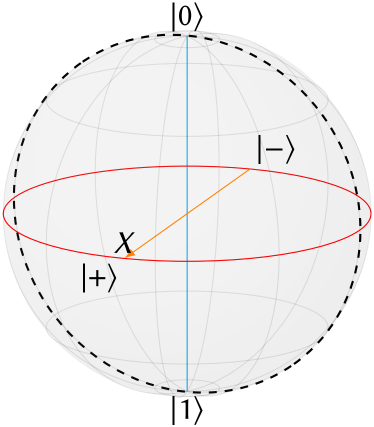


図 5: X ゲートの回転中心

他の量子ゲート❷ − Z, S ゲート

他の量子ゲート❷ − Z, S ゲート

- Z ゲートは図 6 の Z 軸を中心に π 回転させる

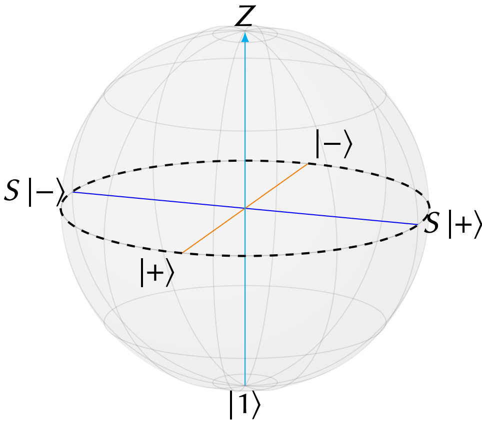


図 6: Z, S ゲートの回転中心

他の量子ゲート❷ – Z, S ゲート

- Z ゲートは図 6 の Z 軸を中心に π 回転させる
- S ゲートは Z 軸を中心に $\frac{\pi}{2}$ 回転させる

$$Z\left|+\right\rangle = \left|-\right\rangle, Z\left|-\right\rangle = \left|+\right\rangle, SS\left|+\right\rangle = Z\left|+\right\rangle = \left|-\right\rangle$$

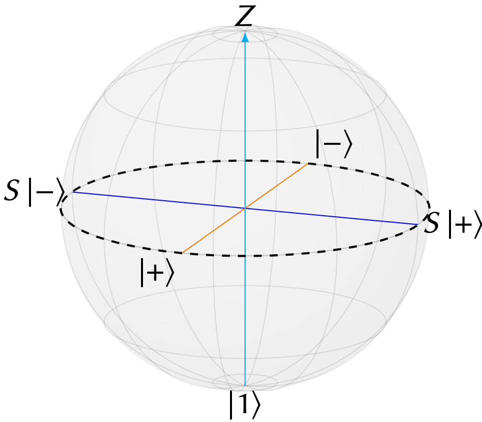


図 6: Z, S ゲートの回転中心

他の量子ゲート❷ — Z, S ゲート

- Z ゲートは図 6 の Z 軸を中心に π 回転させる
- S ゲートは Z 軸を中心に $\frac{\pi}{2}$ 回転させる

$$Z\left|+\right\rangle = \left|-\right\rangle, Z\left|-\right\rangle = \left|+\right\rangle, SS\left|+\right\rangle = Z\left|+\right\rangle = \left|-\right\rangle$$

- $S\left|\pm\right\rangle$ は $\{\left|0\right\rangle, \left|1\right\rangle\}$ で次のように表現できる

$$S\left|\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle \pm \sqrt{-1}\left|1\right\rangle\right)$$

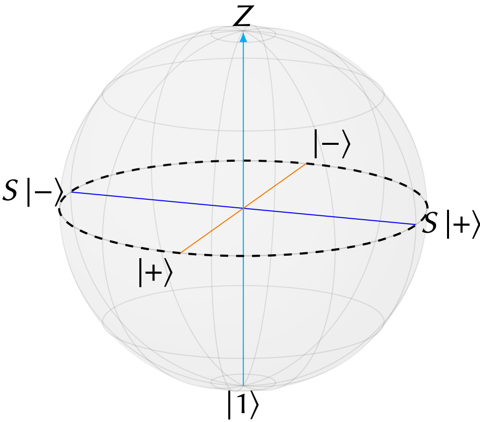


図 6: Z, S ゲートの回転中心

他の量子ゲート❷ — Z, S ゲート

- Z ゲートは図 6 の Z 軸を中心に π 回転させる
- S ゲートは Z 軸を中心に $\frac{\pi}{2}$ 回転させる

$$Z|+\rangle = |-\rangle, Z|-\rangle = |+\rangle, SS|+\rangle = Z|+\rangle = |-\rangle$$

- $S|\pm\rangle$ は $\{|0\rangle, |1\rangle\}$ で次のように表現できる

$$S|\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm \sqrt{-1}|1\rangle\right)$$

- Z 軸上の $|0\rangle, |1\rangle$ に Z, S ゲートを作用させても何も起きない

$$Z|0\rangle = |0\rangle, S|1\rangle = |1\rangle$$

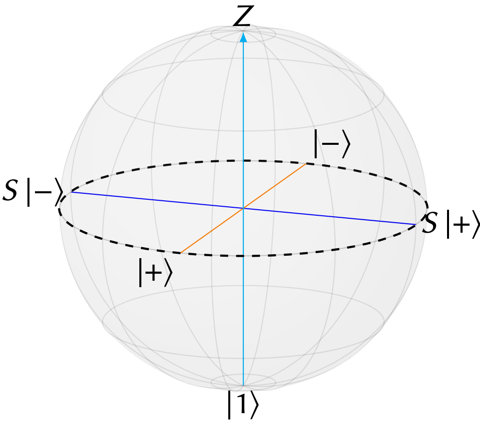


図 6: Z, S ゲートの回転中心

2 量子ビットゲート

- ここまでは次のような 1 量子ビットに対する量子ゲートを扱った
  - H ゲート
  - X ゲート
  - Z ゲート
  - S ゲート

2 量子ビットゲート

- ここまでは次のような 1 量子ビットに対する量子ゲートを扱った
  - H ゲート
  - X ゲート
  - Z ゲート
  - S ゲート
- 古典コンピュータの NAND ゲートのように、量子コンピュータにも 2 量子ビットを入力に持つゲートが存在する

CZ ゲート

CZ ゲート

- CZ ゲートは 2 量子ビットを入力に持ち、
  1. 1 量子ビット目が $|0\rangle$ であれば何もせず、
  2. 一方で 1 量子ビット目が $|1\rangle$ であれば 2 量子ビット目に Z ゲートを作用させる

CZ ゲート

- CZ ゲートは 2 量子ビットを入力に持ち、
  1. 1 量子ビット目が $|0\rangle$ であれば何もせず、
  2. 一方で 1 量子ビット目が $|1\rangle$ であれば 2 量子ビット目に Z ゲートを作用させる

1 量子ビット目が $|+\rangle$ だったら？

CZ ゲート

- CZ ゲートは 2 量子ビットを入力に持ち、
  1. 1 量子ビット目が $|0\rangle$ であれば何もせず、
  2. 一方で 1 量子ビット目が $|1\rangle$ であれば 2 量子ビット目に Z ゲートを作用させる

1 量子ビット目が $|+\rangle$ だったら？

1 量子ビット目を測定した結果、
$|0\rangle$ が観測される　なにも起きない
$|1\rangle$ が観測される　2 量子ビット目に Z ゲートが作用する

CZ ゲート

- CZ ゲートを次のような量子回路 7 で確認してみる

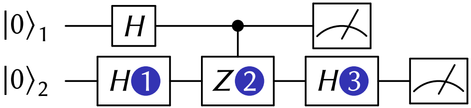


図 7: CZ ゲートを用いた回路

CZ ゲート

- CZ ゲートを次のような量子回路 7 で確認してみる

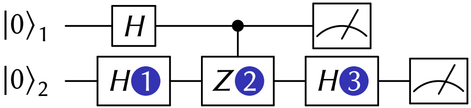


図 7: CZ ゲートを用いた回路

- 2 量子ビット目の $|0\rangle_2$ について考えると
  1. H ゲートにより $|+\rangle$ となる
  2. CZ ゲートによって、Z ゲートが作用しなければ $|+\rangle$ のままであり、Z ゲートが作用すれば $|-\rangle$ となる
  3. 最後に H ゲートを作用させるが、このとき $|+\rangle$ であれば $H|+\rangle = |0\rangle$ となり、一方で $|-\rangle$ であれば $H|-\rangle = |1\rangle$ となる

CZ ゲート

- CZ ゲートを次のような量子回路 7 で確認してみる

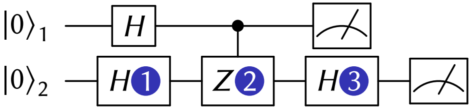
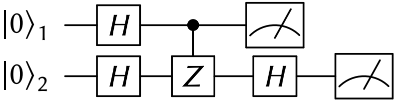


図 7: CZ ゲートを用いた回路

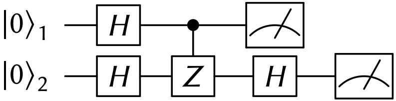
- 2 量子ビット目の $|0\rangle_2$ について考えると
  1. H ゲートにより $|+\rangle$ となる
  2. CZ ゲートによって、Z ゲートが作用しなければ $|+\rangle$ のままであり、Z ゲートが作用すれば $|-\rangle$ となる
  3. 最後に H ゲートを作用させるが、このとき $|+\rangle$ であれば $H\,|+\rangle = |0\rangle$ となり、一方で $|-\rangle$ であれば $H\,|-\rangle = |1\rangle$ となる
- 1 量子ビット目は $|+\rangle$ なので、$|0\rangle\,,|1\rangle$ のどちらかになるかは確率 $\frac{1}{2}$ となる

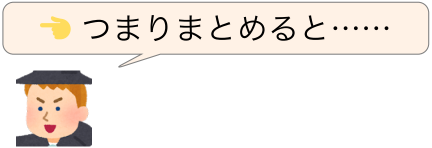
CZ ゲート



👉 つまりまとめると……

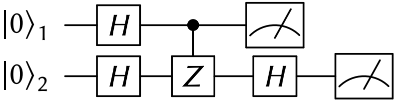
CZ ゲート





- 確率 $\frac{1}{2}$ で 1 量子ビット目の測定結果が $|0\rangle$ なら 2 量子ビット目も $|0\rangle$
- 確率 $\frac{1}{2}$ で 1 量子ビット目の測定結果が $|1\rangle$ なら 2 量子ビット目も $|1\rangle$

CZ ゲート



👉 つまりまとめると……

- 確率 $\frac{1}{2}$ で 1 量子ビット目の測定結果が $|0\rangle$ なら 2 量子ビット目も $|0\rangle$
- 確率 $\frac{1}{2}$ で 1 量子ビット目の測定結果が $|1\rangle$ なら 2 量子ビット目も $|1\rangle$

シミュレーターでやってみる！

CZ ゲートのシミュレーション結果

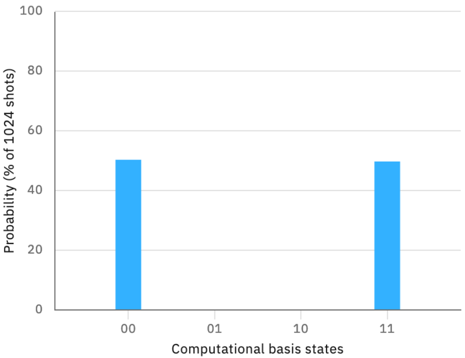


図 8: CZ ゲートを使った回路のシミュレーション結果¶

¶図の最下位ビットが 1 量子ビット目、最上位ビットが 2 量子ビット目となる。

CZ ゲートのシミュレーション結果

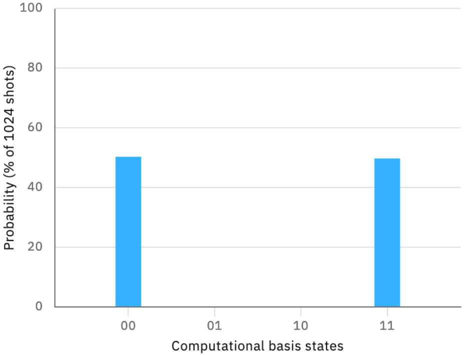


図 8: CZ ゲートを使った回路のシミュレーション結果¶

- このように☝ シミュレーション結果は $|00\rangle$ か $|11\rangle$ が $\frac{1}{2}$ となる🙆

¶図の最下位ビットが 1 量子ビット目、最上位ビットが 2 量子ビット目となる。

CZ ゲート後の量子操作と測定

CZ ゲート後の量子操作と測定

- 2 つの量子ビットが $|+\rangle$ のとき、CZ ゲートを用いた図 9 の回路を考える
  1. Z 軸の回転ゲートを作用させ
  2. H ゲートを作用させ
  3. 測定を行う

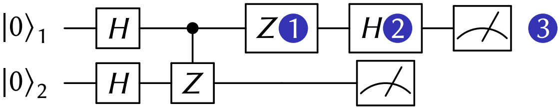


図 9: CZ ゲートの後で Z, H ゲートを作用させ測定

CZ ゲート後の量子操作と測定

- 2 つの量子ビットが $|+\rangle$ のとき、CZ ゲートを用いた図 9 の回路を考える
  1. Z 軸の回転ゲートを作用させ
  2. H ゲートを作用させ
  3. 測定を行う

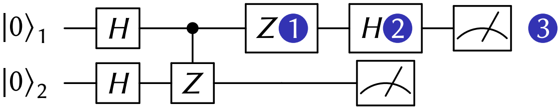


図 9: CZ ゲートの後で Z, H ゲートを作用させ測定

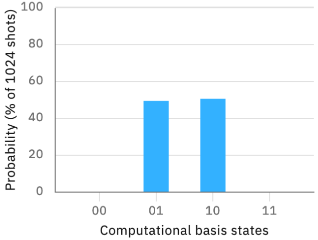


図 10: 回路 9 のシミュレーション結果

CZ ゲート後の量子操作と測定

- 2 つの量子ビットが $|+\rangle$ のとき、CZ ゲートを用いた図 9 の回路を考える
  1. Z 軸の回転ゲートを作用させ
  2. H ゲートを作用させ
  3. 測定を行う

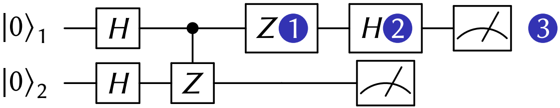


図 9: CZ ゲートの後で Z, H ゲートを作用させ測定

1 量子ビット目は常に $|1\rangle$ では？

$$HZH\,|0\rangle_1 = HZ\,|+\rangle_1 = H\,|-\rangle_1 = |1\rangle_1$$

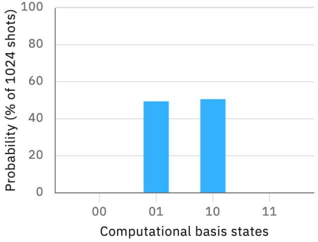
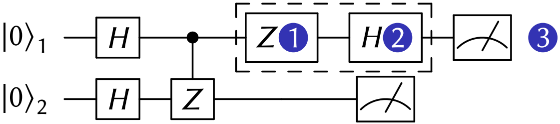
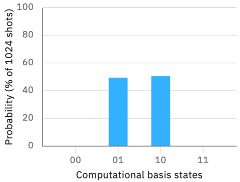


図 10: 回路 9 のシミュレーション結果





- 図 11,12 のように Z, H ゲートが 2 量子ビット目へ**テレポーテーション**する
  - 1 量子ビット目の測定結果に応じて X ゲートの有無の差がある

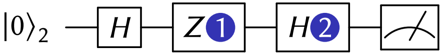


図 11: 1 量子ビット目の測定結果が 0

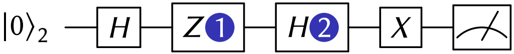
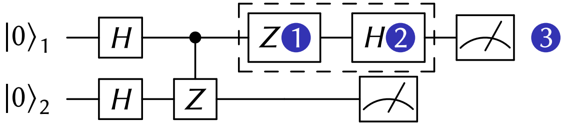
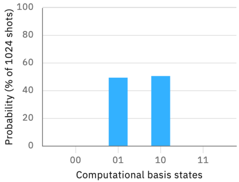


図 12: 1 量子ビット目の測定結果が 1

量子ゲートテレポーテーション





- 図 11,12 のように Z, H ゲートが 2 量子ビット目へ**テレポーテーション**する
  - 1 量子ビット目の測定結果に応じて X ゲートの有無の差がある

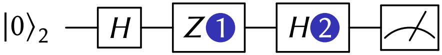


図 11: 1 量子ビット目の測定結果が 0

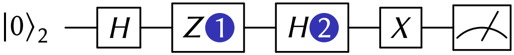


図 12: 1 量子ビット目の測定結果が 1

- Z 軸上の回転ゲートである S ゲートもテレポーテーションできる

量子ゲートテレポーテーション

- テレポーテーションなので 1 量子ビット目から Z, H ゲートが**消える**
  - テレポーテーションであってコピーではない

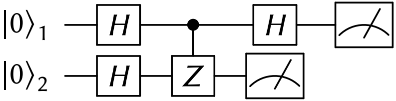


図 13: H ゲートだけのテレポーテーション

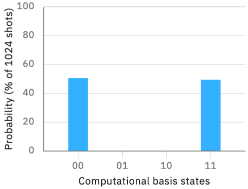


図 14: 回路 13 のシミュレーション結果

量子ゲートテレポーテーション

- テレポーテーションなので 1 量子ビット目から Z, H ゲートが**消える**
    - テレポーテーションであってコピーではない

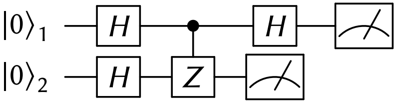


図 13: H ゲートだけのテレポーテーション

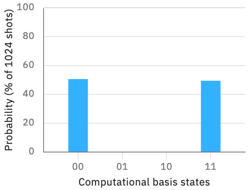


図 14: 回路 13 のシミュレーション結果

- 1 量子ビット目は H ゲートが 2 回作用しているので、CZ ゲートがなければキャンセルして常に $|0\rangle$ となる

量子ゲートテレポーテーション

- テレポーテーションなので 1 量子ビット目から Z, H ゲートが**消える**
  - テレポーテーションであってコピーではない

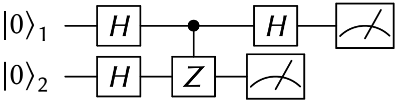


図 13: H ゲートだけのテレポーテーション

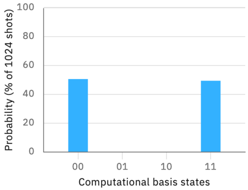


図 14: 回路 13 のシミュレーション結果

- 1 量子ビット目は H ゲートが 2 回作用しているので、CZ ゲートがなければキャンセルして常に $|0\rangle$ となる
- しかし図 14 では 1 量子ビット目が $|0\rangle, |1\rangle$ のランダムとなっている

量子ゲートテレポーテーション

CZ ゲートで Z, S, H ゲートをテレポーテーションできる！

量子ゲートテレポーテーション

CZ ゲートで Z, S, H ゲートをテレポーテーションできる！

そんなことある？ 🤔

量子ゲートテレポーテーション

CZ ゲートで Z, S, H ゲートをテレポーテーションできる！

そんなことある？ 🤔

量子コンピュータ（= 宇宙？）はこういうもの！

Quantum Covert Lottery

1. Covert Lottery とは？
2. 古典 Covert Lottery と情報リーク
3. 量子コンピュータとシュレディンガーの猫
4. 量子ゲートテレポーテーション
5. Quantum Covert Lottery
6. まとめ

- もっと色々な量子ゲートがある

Quantum Covert Lottery

1 Covert Lottery とは？
2 古典 Covert Lottery と情報リーク
3 量子コンピュータとシュレディンガーの猫
4 量子ゲートテレポーテーション
5 Quantum Covert Lottery
6 まとめ

- もっと色々な量子ゲートがある
- 量子コンピュータ上の Covert Lottery の説明はここまでの量子ゲートで OK 🙆
    - X, S, Z, H ゲート
    - CZ ゲート

Quantum Covert Lottery

1. Covert Lottery とは？
2. 古典 Covert Lottery と情報リーク
3. 量子コンピュータとシュレディンガーの猫
4. 量子ゲートテレポーテーション
5. Quantum Covert Lottery
6. まとめ

- もっと色々な量子ゲートがある
- 量子コンピュータ上の Covert Lottery の説明はここまでの量子ゲートで OK 🙆
  - X, S, Z, H ゲート
  - CZ ゲート
- シュレディンガーの猫と量子ゲートテレポーテーションで "Quantum Covert Lottery" を作っていく

プロトコル

プロトコル

1. アリスは表 2 にしたがって希望 $a \in \{0, 1\}$ と、乱数 $x \in \{0, 1\}$ を生成する

表 2: 希望とビットの対応

希望	意味
0	ボブの奢り
1	割り勘

プロトコル

1. アリスは表 2 にしたがって希望 $a \in \{0, 1\}$ と、乱数 $x \in \{0, 1\}$ を生成する
2. アリスは次のような回路 15 で表現される 3 量子ビットを用意する
   - $a = 1$ であれば、1 量子ビット目に S ゲートを作用させる
   - $x = 1$ であれば、3 量子ビット目に Z ゲートを作用させる

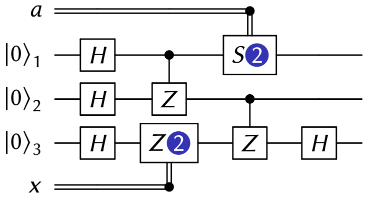


図 15: アリスの用意する 3 量子ビット

表 2: 希望とビットの対応

希望	意味
0	ボブの奢り
1	割り勘

プロトコル

1. アリスは表 2 にしたがって希望 $a \in \{0, 1\}$ と、乱数 $x \in \{0, 1\}$ を生成する
2. アリスは次のような回路 15 で表現される 3 量子ビットを用意する
   - $a = 1$ であれば、1 量子ビット目に S ゲートを作用させる
   - $x = 1$ であれば、3 量子ビット目に Z ゲートを作用させる
3. 3 量子ビットを量子通信回線でボブへ送信する

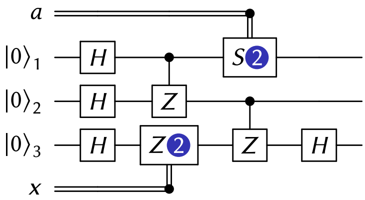


図 15: アリスの用意する 3 量子ビット

表 2: 希望とビットの対応

希望	意味
0	ボブの奢り
1	割り勘

プロトコル

4. ボブはアリスから 3 量子ビットを受けとる

プロトコル

4. ボブはアリスから 3 量子ビットを受けとる
5. ボブは希望 $b \in \{0, 1\}$ を選び図 16 のような量子操作を行う
    - $b = 1$ であれば 1 量子ビット目に S ゲートを作用させる

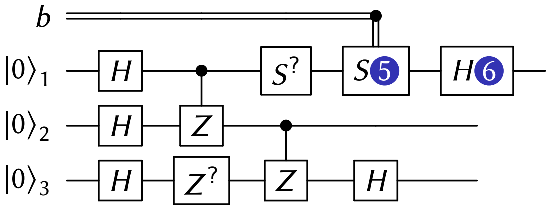


図 16: ボブが行う量子操作

プロトコル

4. ボブはアリスから 3 量子ビットを受けとる
5. ボブは希望 $b \in \{0, 1\}$ を選び図 16 のような量子操作を行う
   - $b = 1$ であれば 1 量子ビット目に S ゲートを作用させる
6. ボブは 1 量子ビット目に H ゲートを作用させる

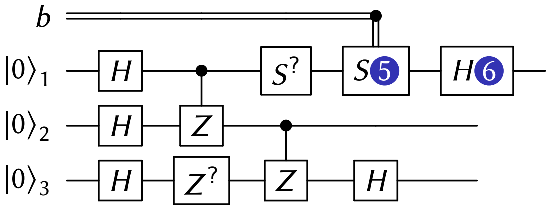
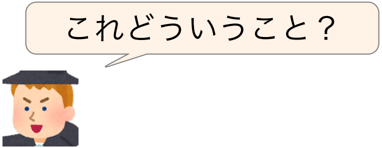


図 16: ボブが行う量子操作

プロトコル



プロトコル

これどういうこと？

1 量子ビット目だけ整理してみる

- 1 量子ビット目とアリス・ボブの希望 a, b に注目すると図 17 の回路になる

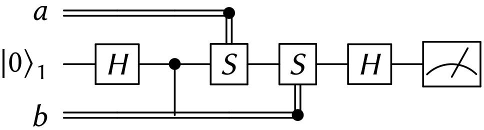


図 17: 1 量子ビット目とアリス・ボブの希望 a, b

プロトコル

これどういうこと？

1 量子ビット目だけ整理してみる

- 1 量子ビット目とアリス・ボブの希望 a, b に注目すると図 17 の回路になる

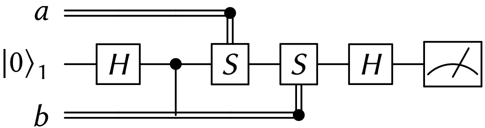


図 17: 1 量子ビット目とアリス・ボブの希望 a, b

- これをアリス・ボブの希望 a, b で場合わけして考える

ケーススタディ❶ – アリス・ボブの希望が一致

- アリス・ボブの希望が一致するときは $a = b$ なので次の 2 つになる

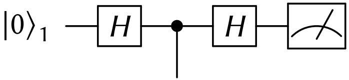


図 18: 両者がボブの奢り（0）で一致

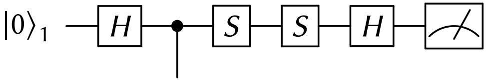


図 19: 両者が割り勘（1）で一致

ケーススタディ❶ – アリス・ボブの希望が一致

- アリス・ボブの希望が一致するときは $a = b$ なので次の 2 つになる

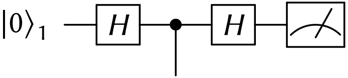


図 18: 両者がボブの奢り（0）で一致

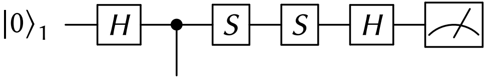


図 19: 両者が割り勘（1）で一致

- $SS = Z$ により、2 量子ビット目へのテレポーテーション内容は次のようになる
  $a = b = 0$　H ゲート（+ X ゲート）
  $a = b = 1$　H ゲートと Z ゲート（+ X ゲート）

ケーススタディ❶ — アリス・ボブの希望が一致

- アリス・ボブの希望が一致するときは $a = b$ なので次の 2 つになる

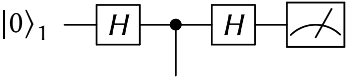


図 18: 両者がボブの奢り（0）で一致

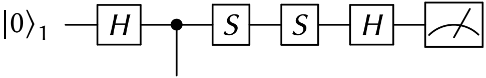


図 19: 両者が割り勘（1）で一致

- $SS = Z$ により、2 量子ビット目へのテレポーテーション内容は次のようになる

  $a = b = 0$　H ゲート（+ X ゲート）

  $a = b = 1$　H ゲートと Z ゲート（+ X ゲート）

S ゲートがテレポーテーションしないのがポイント！

ケーススタディ❷ – アリス・ボブの希望が不一致

ケーススタディ❷ – アリス・ボブの希望が不一致

- 一方で、アリス・ボブの希望が一致しない場合 $a \neq b$ なので次のようになる

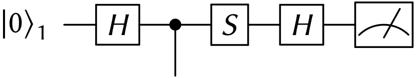


図 20: アリスは割り勘・ボブは奢り、またはアリスは奢り・ボブは割り勘

ケーススタディ❷ – アリス・ボブの希望が不一致

- 一方で、アリス・ボブの希望が一致しない場合 $a \neq b$ なので次のようになる

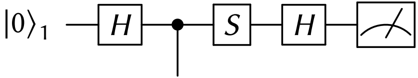


図 20: アリスは割り勘・ボブは奢り、またはアリスは奢り・ボブは割り勘

- いずれも S ゲートと H ゲートが 2 量子ビット目へテレポーテーションする

ケーススタディ❷ — アリス・ボブの希望が不一致

- 一方で、アリス・ボブの希望が一致しない場合 $a \neq b$ なので次のようになる

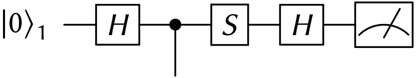


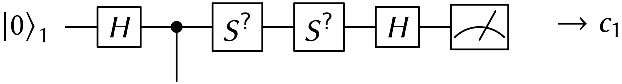
図 20: アリスは割り勘・ボブは奢り、またはアリスは奢り・ボブは割り勘

- いずれも S ゲートと H ゲートが 2 量子ビット目へテレポーテーションする

S ゲートが 2 量子ビット目へテレポーテーションされる！

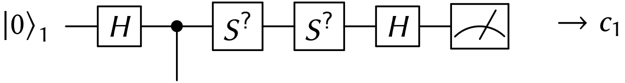
プロトコル

7. ボブは 1 量子ビット目の測定を行い測定結果を c_1 とする

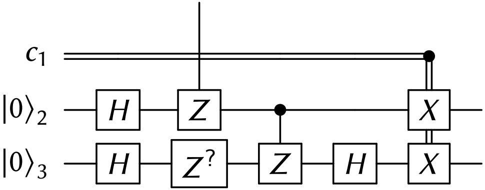


プロトコル

7. ボブは 1 量子ビット目の測定を行い測定結果を c_1 とする

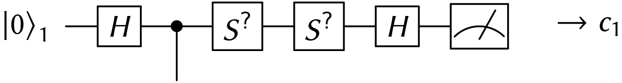


8. ボブは $c_1 = 1$ なら次のように X ゲートを 2, 3 量子ビット目に作用させる

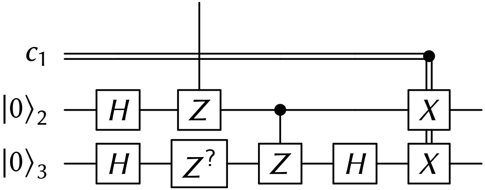


プロトコル

7. ボブは 1 量子ビット目の測定を行い測定結果を c_1 とする



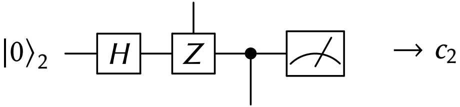
8. ボブは $c_1 = 1$ なら次のように X ゲートを 2, 3 量子ビット目に作用させる



量子ゲートテレポーテーションで偶発的に生じる X ゲートをキャンセル！

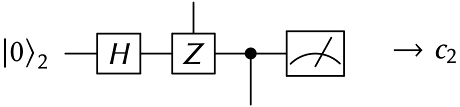
プロトコル

9. ボブは 2 量子ビット目の測定を行い結果を c_2 とする



プロトコル

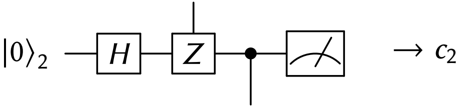
9. ボブは 2 量子ビット目の測定を行い結果を c_2 とする



10. プロトコルの結果として c_2 をアリスへ共有する

プロトコル

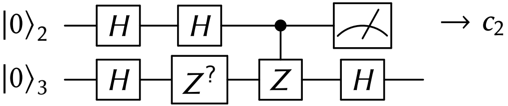
9. ボブは 2 量子ビット目の測定を行い結果を c_2 とする



10. プロトコルの結果として c_2 をアリスへ共有する

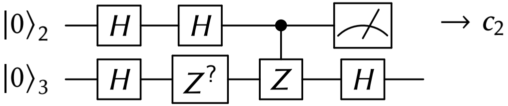
2, 3 量子ビット目は希望 a, b で場合わけ

$a = b = 0$ のとき



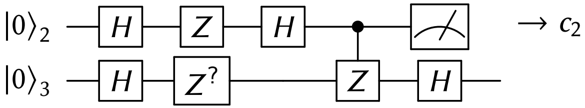
- H ゲートの相殺により 2 量子ビット目は $|0\rangle$ に確定し $c_2 = 0$ となる

$a = b = 0$ のとき



- H ゲートの相殺により 2 量子ビット目は $|0\rangle$ に確定し $c_2 = 0$ となる
- アリス・ボブの両方が「ボブの奢り」である 0 を希望しているため、プロトコルの結果として 0 となり OK 🙆

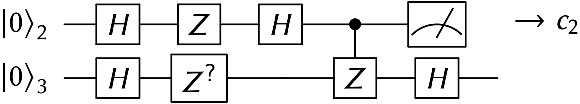
$a = b = 1$ のとき



- H, Z, H ゲート操作で 2 量子ビット目は $|1\rangle$ に確定し $c_2 = 1$ となる

$$HZH\,|0\rangle_2 = HZ\,|+\rangle_2 = H\,|-\rangle_2 = |1\rangle_2$$

ii $a = b = 1$ のとき

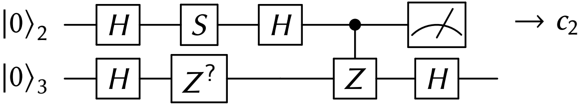


- H, Z, H ゲート操作で 2 量子ビット目は $|1\rangle$ に確定し $c_2 = 1$ となる

$$HZH\,|0\rangle_2 = HZ\,|+\rangle_2 = H\,|-\rangle_2 = |1\rangle_2$$

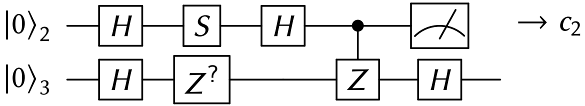
- アリス・ボブの両方が「割り勘」である 1 を希望しているため、プロトコルの結果として 1 となり OK 🙆‍♀️

ⅲ $a \neq b$ のとき



- H, S, H ゲート操作で 2 量子ビット目は $S\,|-\rangle$ となる
  - $S\,|-\rangle$ はブロッホ球の赤道上なので、測定結果は $|0\rangle, |1\rangle$ が $\frac{1}{2}$ となる

iii $a \neq b$ のとき



- H, S, H ゲート操作で 2 量子ビット目は $S\,|-\rangle$ となる
  - $S\,|-\rangle$ はブロッホ球の赤道上なので、測定結果は $|0\rangle\,, |1\rangle$ が $\frac{1}{2}$ となる
- アリス・ボブの希望が割れた場合は結果は 0, 1 の 50%ランダムとなり OK🙆

プロトコル

プロトコル

3 量子ビット目は？

プロトコル

3 量子ビット目は？

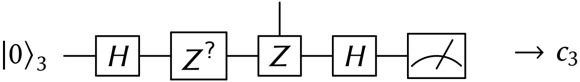
ボブの不正検知！

プロトコル

3 量子ビット目は？

ボブの不正検知！

⑪ ボブは 3 量子ビット目を測定し c_3 としアリスへ送信する

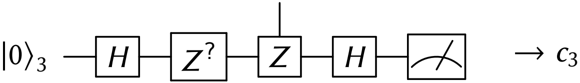


プロトコル

3 量子ビット目は？

ボブの不正検知！

⑪ ボブは 3 量子ビット目を測定し c_3 としアリスへ送信する



⑫ アリスはボブから c_2, c_3 を受け取り、式 3 を確認する

$$c_2 \ \mathtt{XOR} \ x \stackrel{?}{=} c_3 \tag{3}$$

- 式 3 が等しくなければプロトコルを中止する

ボブの不正検知

ボブの不正検知

- 二人の希望が衝突した場合、ボブは❾で都合がいい c_2 が観測されたと偽ることができる😈

ボブの不正検知

- 二人の希望が衝突した場合、ボブは⑨で都合がいい c_2 が観測されたと偽ることができる😈
- 式 3 により、アリスは確率 $\frac{1}{2}$ でボブの不正を検知できる

ボブの不正検知

- 二人の希望が衝突した場合、ボブは❾で都合がいい c_2 が観測されたと偽ることができる😈
- 式 3 により、アリスは確率 $\frac{1}{2}$ でボブの不正を検知できる
- 検証用の量子ビットを n qubit 用意すれば、ボブの不正の可能性を $\frac{1}{2^n}$ にできる
    - 図 21 の回路ではボブは x_1, x_2, x_3 の 3bit を全てあてなければ不正に成功しない

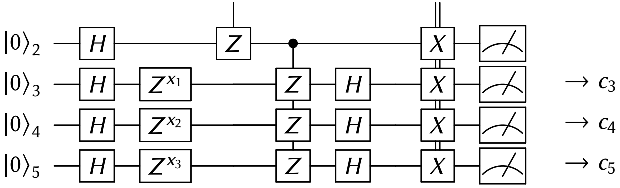


図 21: ボブの不正対策を増やした回路

まとめ

まとめ

- 量子コンピュータを用いた “Quantum Covert Lottery” で奢り・割り勘問題に決着をつけられるかもしれない
  - すでにインターネットで公開しているプロトコル [3] はボブの不正対策がない😇

まとめ

- 量子コンピュータを用いた "Quantum Covert Lottery" で奢り・割り勘問題に決着をつけられるかもしれない
  - すでにインターネットで公開しているプロトコル [3] はボブの不正対策がない😇
- ボブは困難とはいえ不正ができるが、アリスの不正が今のところない
  - アリスもボブと全く同じ困難性で不正ができるようにしたい

まとめ

- 量子コンピュータを用いた “Quantum Covert Lottery” で奢り・割り勘問題に決着をつけられるかもしれない
    - すでにインターネットで公開しているプロトコル [3] はボブの不正対策がない😇
- ボブは困難とはいえ不正ができるが、アリスの不正が今のところない
    - アリスもボブと全く同じ困難性で不正ができるようにしたい
- 今回は 2 人だったが、これを多人数拡張すると別のゲームに使えるかも
    - 量子版の多人数拡張はまだできてない……😇

まとめ

- 量子コンピュータを用いた “Quantum Covert Lottery” で奢り・割り勘問題に決着をつけられるかもしれない
  - すでにインターネットで公開しているプロトコル [3] はボブの不正対策がない😇
- ボブは困難とはいえ不正ができるが、アリスの不正が今のところない
  - アリスもボブと全く同じ困難性で不正ができるようにしたい
- 今回は 2 人だったが、これを多人数拡張すると別のゲームに使えるかも
  - 量子版の多人数拡張はまだできてない……😇
- 量子コンピュータには高速な素因数分解といったアルゴリズム高速化以外にも色々な応用の可能性があると思う
  - シュレディンガーの猫や量子ゲートテレポーテーションはそれだけで夢がある

参考文献 I

[1] Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone.
Card-Based Covert Lottery.
In Diana Maimut, Andrei-George Oprina, and Damien Sauveron, editors, *Innovative Security Solutions for Information Technology and Communications*, pp. 257–270, Cham, 2021. Springer International Publishing.

[2] @Y_N_Hoshi tweet.
`https://twitter.com/Y_N_Hoshi/status/1603396700453871618`.
Accessed: 2023-10-01.

[3] 量子コンピュータで 2 人の "Covert"！？ ガチャ.
`https://zenn.dev/yyu/articles/79c6c48226166aa0e875`.
Accessed: 2023-10-01.

Thank you for the attention!

Appendix

7 量子ゲートの行列表現

量子ゲートの行列表現

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ S := \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix},\ H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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