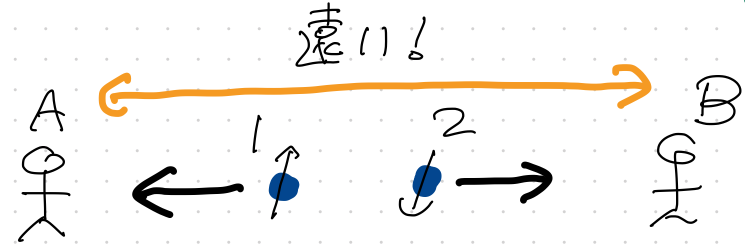
<量子力学と情報>

§ エンタングルメントと超光速通信

→ 光速を超えた情報の伝達



▷ 設定と問題

スピン$\frac{1}{2}$の2つの粒子(区別できる) 1, 2

全状態　　座標部分

(1) $|\Psi_{total}\rangle = \underbrace{|\varphi_1\rangle_1}_{\text{左へ進む}} \otimes \underbrace{|\varphi_2\rangle_2}_{\text{右へ進む}} \otimes \frac{1}{\sqrt{2}}\{|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\} = |\Psi_0\rangle$

スピン部分 = singlet ← 1と2はエンタングルしている

離れたところにいるAとBがそれぞれ粒子1と粒子2をうけとる.

Aが状態を測定すると
- Bの状態も一瞬で変わるのか? → 「Bの状態」の定ギによる.
- Bになんらかの情報が一瞬で伝わるのか?
  - 情報 → Yes or No, 0 or 1

AとBは同じ状態$|\Psi_0\rangle$をたくさん共有　　様々な実験をくり返す

$\hat{S}_z$ の測定

(1) $|\Phi_0\rangle = \frac{1}{\sqrt{2}}\{|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\}$

- まずAが粒子1の $\hat{S}_z$ を測定する

(2) $\begin{cases} \hat{S}_z^{(1)}|\uparrow\rangle_1|\downarrow\rangle_2 = \frac{\hbar}{2}|\uparrow\rangle_1|\downarrow\rangle_2 \\ \hat{S}_z^{(1)}|\downarrow\rangle_1|\uparrow\rangle_2 = -\frac{\hbar}{2}|\downarrow\rangle_1|\uparrow\rangle_2 \end{cases}$ より

測定結果 (3)
- 確率 $\frac{1}{2}$ で ↑ $\left(\frac{\hbar}{2}\right)$ → 測定後の状態 $|\uparrow\rangle_1|\downarrow\rangle_2$ ①
- 確率 $\frac{1}{2}$ で ↓ $\left(-\frac{\hbar}{2}\right)$ → 測定後の状態 $|\downarrow\rangle_1|\uparrow\rangle_2$ ②

このあと Bが粒子2の $\hat{S}_z$ を測定すれば 結果は確定している ① ↓ ② ↑

AからBに情報が伝わったのか?

- まずBが粒子2の $\hat{S}_z$ を測定 　　あとからAが $\hat{S}_z$ を測定

(4)
- 確率 $\frac{1}{2}$ で ↑ → 測定後の状態 $|\downarrow\rangle_1|\uparrow\rangle_2$ → ↓
- 確率 $\frac{1}{2}$ で ↓ → 測定後の状態 $|\uparrow\rangle_1|\downarrow\rangle_2$ → ↑

- いずれの場合も測定結果は (5)

$\boxed{\begin{array}{l} \text{確率 } \frac{1}{2} \text{ で　A は↑　B は↓} \\ \text{確率 } \frac{1}{2} \text{ で　A は↓　B は↑} \end{array}}$

測定結果が相関しているだけで情報は伝わっていない!

▷ 測定する物理量を変えることによる通信 [?]

$\hat{S}_x$ の固有状態 (1) $\begin{cases} \hat{S}_x|\rightarrow\rangle = \frac{\hbar}{2}|\rightarrow\rangle \\ \hat{S}_x|\leftarrow\rangle = -\frac{\hbar}{2}|\leftarrow\rangle \end{cases}$ (2) $\begin{cases} |\rightarrow\rangle = \frac{1}{\sqrt{2}}\{|\uparrow\rangle + |\downarrow\rangle\} \\ |\leftarrow\rangle = \frac{1}{\sqrt{2}}\{|\uparrow\rangle - |\downarrow\rangle\} \end{cases}$

これを使えば (3) $|\Phi_0\rangle = \frac{1}{\sqrt{2}}\{|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\} = -\frac{1}{\sqrt{2}}\{|\rightarrow\rangle_1|\leftarrow\rangle_2 - |\leftarrow\rangle_1|\rightarrow\rangle_2\}$

- $|\Phi_0\rangle$ で A が $\hat{S}_x$ を測定 (4) $\begin{cases} \text{確率}\ \frac{1}{2}\ \text{で}\ \rightarrow (\frac{\hbar}{2}) \rightarrow \text{測定後の状態}\ |\rightarrow\rangle_1|\leftarrow\rangle_2 \\ \text{確率}\ \frac{1}{2}\ \text{で}\ \leftarrow (-\frac{\hbar}{2}) \rightarrow \text{測定後の状態}\ |\leftarrow\rangle_1|\rightarrow\rangle_2 \end{cases}$

- (4) と P2-(3) を利用して、A から B へ 1 bit の情報 (yes or No) を一瞬で送る

(5)
- yes → A は $\hat{S}_z$ を測定 → 測定後の B の状態 $|\uparrow\rangle_2$ or $|\downarrow\rangle_2$
- no → A は $\hat{S}_x$ を測定 → 測定後の B の状態 $|\rightarrow\rangle_2$ or $|\leftarrow\rangle_2$

B が $|\uparrow\rangle$ or $|\downarrow\rangle$ と $|\rightarrow\rangle$ or $|\leftarrow\rangle$ を区別できれば

超光速で情報が伝えられる!!

・Bが $\hat{S}_z$ を測定すると

(1) yesのとき
- 確率$\frac{1}{2}$で $|\uparrow\rangle_z$ → 測定結果 ↑
- 確率$\frac{1}{2}$で $|\downarrow\rangle_z$ → 測定結果 ↓

(2) noのとき
- 確率$\frac{1}{2}$で $|\rightarrow\rangle_z$ →
  - 確率$\frac{1}{4}$で測定結果 ↑
  - 確率$\frac{1}{4}$で測定結果 ↓
- 確率$\frac{1}{2}$で $|\leftarrow\rangle_z$ →
  - 確率$\frac{1}{4}$で測定結果 ↑
  - 確率$\frac{1}{4}$で測定結果 ↓

→ 確率$\frac{1}{2}$（↑）、確率$\frac{1}{2}$（↓）

この測定ではyesとnoを区別できない → 他の量を測ったら？（次のページ）

もしBが測定前の状態をそのままコピーできれば
- yes → $|\uparrow\rangle_z$ → $|\uparrow\rangle\otimes|\uparrow\rangle\otimes|\uparrow\rangle\otimes\cdots$ → $\hat{S}_z$を次々と測定するといつも↑
- no → $|\rightarrow\rangle_z$ → $|\rightarrow\rangle\otimes|\rightarrow\rangle\otimes|\rightarrow\rangle\otimes\cdots$ → $\hat{S}_z$を次々と測定するとランダムに↑と↓

区別できる!!　しかしこのようなコピーは不可能（クローン禁止定理）

▷ 一般的な設定

$|\Phi_0\rangle$ は $\mathcal{H}_1 \otimes \mathcal{H}_2$ の任意の状態

$\mathcal{H}_1$: Aが扱える　　$\mathcal{H}_2$: Bが扱える

$|\Phi_0\rangle$: { エンタングルした粒子ES / さまざまな装置

状態 $|\Phi_0\rangle$ において { Aは $\mathcal{H}_1$ 上の物理量 $\hat{A}$ を測定 / Bは $\mathcal{H}_2$ 上の物理量 $\hat{B}$ を測定

これを何度もくり返す。

結果　任意の $\hat{B}$ について、Bの測定結果の期待値 $\langle\hat{B}\rangle$ は $\hat{A}$ に依存しない

先ほどの例の一般化。

- Aは $\hat{A}$ を変えることでBに情報を伝えようとする。
- しかしBが得る結果 $\langle\hat{B}\rangle$ は $\hat{A}$ の選び方によらない

超光速通信はできない…

証明　$\hat{A}$の規格化された固有状態 (1) $\hat{A}|\Phi_j\rangle_1 = a_j|\Phi_j\rangle_1$

縮退なし

- $|\Phi_j\rangle_1$への射影演算子 (2) $\hat{P}_j := |\Phi_j\rangle_1 {}_1\langle\Phi_j| \otimes \hat{1}_2$

もちろん (3) $\hat{P}_j{}^2 = \hat{P}_j$　(4) $\sum_j \hat{P}_j = \hat{1}$

- $|\Phi_0\rangle$で$\hat{A}$を測定してa_jが得られる確率 (5) $p_j = \|\hat{P}_j|\Phi_0\rangle\|^2 = \langle\Phi_0|\hat{P}_j|\Phi_0\rangle$

規格化しておく

a_jが得られたあとの状態 (6) $|\Phi_j\rangle = \dfrac{\hat{P}_j|\Phi_0\rangle}{\|\hat{P}_j|\Phi_0\rangle\|} = \dfrac{\hat{P}_j|\Phi_0\rangle}{\sqrt{p_j}}$

- $|\Phi_j\rangle$で$\hat{B}$の測定をくり返したときの期待値は $\langle\Phi_j|(\hat{1}_1\otimes\hat{B})|\Phi_j\rangle$ だから

$\hat{P}_j$と$(\hat{1}_1\otimes\hat{B})$が可換であることに注意すれば、Bの測定結果の期待値は

(7) $\langle\hat{B}\rangle = \sum_j p_j\langle\Phi_j|(\hat{1}_1\otimes\hat{B})|\Phi_j\rangle = \sum_j\langle\Phi_0|\hat{P}_j(\hat{1}_1\otimes\hat{B})\hat{P}_j|\Phi_0\rangle$

$= \sum_j\langle\Phi_0|\hat{P}_j(\hat{1}_1\otimes\hat{B})|\Phi_0\rangle = \langle\Phi_0|(\hat{1}_1\otimes\hat{B})|\Phi_0\rangle$

$\hat{A}$によらない!

§クローン禁止定理　様々なバージョンのうちのひとつ

未知の量子状態をそのままコピーする量子系

(1) $|\psi\rangle \otimes |\psi_0\rangle \otimes |\Phi_0\rangle \xrightarrow{\text{時間発展}} |\psi\rangle \otimes |\psi\rangle \otimes |\Phi'\rangle$

コピーしたい未知の状態　コピー用紙　コピー機

定理 $|\psi\rangle$が$|\uparrow\rangle, |\downarrow\rangle, |\rightarrow\rangle, |\leftarrow\rangle$ のいずれかをとるとする。
$|\psi\rangle$を忠実にコピーする系は存在しない

証明 可能とする

(2) $|\uparrow\rangle \otimes |\psi_0\rangle \otimes |\Phi_0\rangle \longrightarrow |\uparrow\rangle \otimes |\uparrow\rangle \otimes |\Phi_1\rangle$

(3) $|\downarrow\rangle \otimes |\psi_0\rangle \otimes |\Phi_0\rangle \longrightarrow |\downarrow\rangle \otimes |\downarrow\rangle \otimes |\Phi_2\rangle$

(4) $|\rightarrow\rangle \otimes |\psi_0\rangle \otimes |\Phi_0\rangle \longrightarrow |\rightarrow\rangle \otimes |\rightarrow\rangle \otimes |\Phi_3\rangle$　まったくちがう

しかし

(5) $\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \otimes |\psi_0\rangle |\Phi_0\rangle \longrightarrow \frac{1}{\sqrt{2}}\{|\uparrow\rangle \otimes |\uparrow\rangle \otimes |\Phi_1\rangle + |\downarrow\rangle \otimes |\downarrow\rangle \otimes |\Phi_2\rangle\}$

線形性

(注) $|\psi\rangle = |\uparrow\rangle, |\downarrow\rangle$ ならコピーは可能)

◎ 参考 $|\psi\rangle = |\uparrow\rangle$ or $|\downarrow\rangle$ をコピーする方法

(1) $|\psi\rangle_1 \otimes \underbrace{\frac{1}{\sqrt{2}}\{|\uparrow\rangle_2 + i|\downarrow\rangle_2\}}_{}$ から出発し ハミルトニアン (2) $\hat{H} = \gamma \hat{S}_z^{(1)} \hat{S}_x^{(2)}$

→ y 方向上向き

$\tau = \dfrac{\pi}{\gamma\hbar}$ だけ時間発展させると $|\psi\rangle_1 \otimes |\psi\rangle_2$ になる ($\psi = \uparrow, \downarrow$)

なぜか? $|\psi\rangle_1 = |\uparrow\rangle_1$ のとき

(3)
$$\begin{cases} \hat{H}\,|\uparrow\rangle_1 \otimes |\rightarrow\rangle_2 = \gamma\left(\frac{\hbar}{2}\right)^2 |\uparrow\rangle_1 \otimes |\rightarrow\rangle_2 \\ \hat{H}\,|\uparrow\rangle_1 \otimes |\leftarrow\rangle_2 = -\gamma\left(\frac{\hbar}{2}\right)^2 |\uparrow\rangle_1 \otimes |\leftarrow\rangle_2 \end{cases}$$

Sch. eq. の一般解 (4) $|\Phi(t)\rangle = \alpha\, e^{-i\gamma\frac{\hbar}{4}t} |\uparrow\rangle_1 |\rightarrow\rangle_2 + \beta\, e^{i\gamma\frac{\hbar}{4}t} |\uparrow\rangle_1 |\leftarrow\rangle_2$

初期条件より (5) $\alpha = \dfrac{1+i}{2} = \dfrac{e^{i\pi/4}}{\sqrt{2}}$, $\beta = \dfrac{1-i}{2} = \dfrac{e^{-i\pi/4}}{\sqrt{2}}$ なので

(6) $$|\Phi(t)\rangle = \underbrace{|\uparrow\rangle_1}_{\text{変わらない}} \otimes \underbrace{\left\{\cos\left(\gamma\frac{\hbar}{4}t - \frac{\pi}{4}\right)|\uparrow\rangle_2 - i\sin\left(\gamma\frac{\hbar}{4}t - \frac{\pi}{4}\right)|\downarrow\rangle_2\right\}}_{\text{才差運動}}$$

$|\psi\rangle_1 = |\downarrow\rangle_1$ の場合も同様 (2つ目のスピンが感じる「磁場」が反転)

§ 量子暗号（量子鍵配送）

△ 暗号とは？　送信者Aから受信者Bに第3者Eに内容がわからないようにメッセージを送る

↗ eavsedropper

送信者A　平文 P(メッセージ)　　　受信者B　平文 $P=f^{-1}(C)$

f ↓ 暗号化　　　　　　　　f^{-1} ↑ 復号

暗号文 —— C ——→ 暗号文

$C=f(P)$　　盗聴者E ?　　C

△ 古くからの暗号　AとBが事前にこっそりと暗号のルール（fとf^{-1}）を共有

A　「あほかい」↓「いまきう」 ——→ B　「いまきう」↑「あほかい」

ずっと使っていると解読されてしまう

△ 公開鍵暗号　Bはある方法でfとf^{-1}をつくり、fだけを世界に公開

- もちろんfがわかれば誰でも（原理的には）f^{-1}が計算できるが、その計算に極めて長い時間が必要なようにしてある。→ 計算機・計算法の進歩で解読？

◎ one-time pad　絶対に安全な暗号 → (確率 $\frac{1}{2}$ で 0 or 1)

AとBは事前に 0と1のランダムな列(秘密鍵)をこっそりと共有

A								
平文	0	1	1	0	0	1	1	0
秘密鍵	1	0	1	1	0	1	0	1
各々の0,1を足す	1	1	0	1	0	0	1	1

(0+0=0, 1+0=1, 0+1=1, 1+1=0)

B								
各々の0,1を足す	0	1	1	0	0	1	1	0
秘密鍵	1	0	1	1	0	1	0	1
暗号文	1	1	0	1	0	0	1	1

暗号文はただの乱数列!!

秘密鍵は1回しか使ってはいけない!　(くり返し使うと解読されてしまう)

AとBでどうやって秘密鍵を共有するかが問題　量子鍵配送
(Quantum Key Distribution)

BB84プロトコル　量子鍵配送の例 (Bennett, Brassard 1984)

復習　スピン$\frac{1}{2}$の状態 $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle = \frac{1}{\sqrt{2}}\{|\uparrow\rangle + |\downarrow\rangle\}$, $|\leftarrow\rangle = \frac{1}{\sqrt{2}}\{|\uparrow\rangle - |\downarrow\rangle\}$

- $\hat{S}_z$を測定 ▶ $|\uparrow\rangle$ かならず↑　▶ $|\downarrow\rangle$ かならず↓　▶ $|\rightarrow\rangle, |\leftarrow\rangle$ 確率$\frac{1}{2}$で ↑ or ↓
- $\hat{S}_x$を測定 ▶ $|\uparrow\rangle, |\downarrow\rangle$ 確率$\frac{1}{2}$で → or ←　▶ $|\rightarrow\rangle$ かならず→　▶ $|\leftarrow\rangle$ かならず←

確率 1/2

手順
- Aはランダムに $\beta = X, Z$ と $\sigma = 0, 1$ を選ぶ
- Aは以下のルールに従ってスピン$\frac{1}{2}$の状態$|\varphi\rangle$をつくり、Bにおくる

$$\beta = X \quad |\varphi\rangle = \begin{cases} |\rightarrow\rangle & \sigma = 0 \\ |\leftarrow\rangle & \sigma = 1 \end{cases} \qquad \beta = Z \quad |\varphi\rangle = \begin{cases} |\uparrow\rangle & \sigma = 0 \\ |\downarrow\rangle & \sigma = 1 \end{cases}$$

- Bはランダムに $\beta' = X, Z$ を選び、以下のように $\sigma' = 0, 1$ を決める

$\beta' = X$ なら $|\varphi\rangle$で$\hat{S}_x$を測定　→なら $\sigma' = 0$　←なら $\sigma' = 1$

$\beta' = Z$ なら $|\varphi\rangle$で$\hat{S}_z$を測定　↑なら $\sigma' = 0$　↓なら $\sigma' = 1$

もし $\beta = \beta'$ なら $\sigma = \sigma'$　　$\beta \neq \beta'$ なら 確率$\frac{1}{2}$で $\sigma = \sigma'$ or $\sigma \neq \sigma'$

秘密鍵の生成

A宅 —1回?→ 宅B

- A,Bは先ほどの手順をくり返す　以下のような表ができる

Alice	β	X	Z	Z	X	Z	X	X	Z	X	X	Z	Z	Z
	σ	0	1	0	0	0	0	0	1	1	0	0	1	1
Bob	β'	Z	Z	X	X	X	Z	X	Z	X	Z	Z	X	Z
	σ'	0	1	1	0	0	1	0	1	1	0	0	0	1

Aしか知らない

Bしか知らない

- A,Bは通常の通信方法(盗聴されてもいい)でβとβ'を教え合う.

上の表でβ=β'となったところだけを残して,あとはすてる.

Alice	β	~~X~~	Z	~~Z~~	X	~~Z~~	~~X~~	X	Z	X	~~X~~	Z	~~Z~~	Z
	σ	~~0~~	1	~~0~~	0	~~0~~	~~0~~	0	1	1	~~0~~	0	~~1~~	1
Bob	β'	~~Z~~	Z	~~X~~	X	~~X~~	~~Z~~	X	Z	X	~~Z~~	Z	~~X~~	Z
	σ'	~~0~~	1	~~1~~	0	~~0~~	~~1~~	0	1	1	~~0~~	0	~~0~~	1

AとBの手元には共通の0,1のランダムな列が残る! 秘密鍵

盗聴者　Eveは Aliceから Bobへの通信に介入し $|\varphi\rangle$ を入手.

▶ Eveは $|\varphi\rangle$ が $\underbrace{|\uparrow\rangle, |\downarrow\rangle}_{\beta=Z}, \underbrace{|\rightarrow\rangle, |\leftarrow\rangle}_{\beta=X}$ のいずれかであることは知っている.

しかし

▶ $|\varphi\rangle$ をもっていても, βが X か Z かを知る方法はない! → できたら超光速通信!!!

▶ ともかく $\hat{S}_x$ か $\hat{S}_z$ かを測って, 結果に対応した $|\hat{\varphi}\rangle$ をBに送る.

Alice $\xrightarrow{|\varphi\rangle}$ Eve $\xrightarrow{|\hat{\varphi}\rangle}$ Bob

① $\beta=Z$, $\sigma=0$　$|\varphi\rangle=|\uparrow\rangle$　　$\hat{S}_z$測定 ↑　$|\hat{\varphi}\rangle=|\uparrow\rangle$ を送る　　$\beta'=Z$ ↑ $\sigma'=0$

Eve は Alice, Bob にばれずに $\sigma=\sigma'=0$ だと知った!

② $\beta=X$　$\sigma=0$　$|\varphi\rangle=|\rightarrow\rangle$　　$\hat{S}_z$測定 ↓　$|\hat{\varphi}\rangle=|\downarrow\rangle$ を送る　　$\beta'=X$ ← $\sigma'=1$

ちがった!

$\beta=\beta'$ だが $\sigma\neq\sigma'$ となっている!

Alice と Bob は $\beta=\beta'$ となった回の一部について σ と σ' を照合. → Eveの介入がばれる!!

(参考　Eve が何をやっても ばれずに盗聴するのは不可能なことが証明されている.)

§量子コンピューター

通常の(古典的な)コンピューター

0 1 1 0 1 1 1 0 1 0 1 0 1 0

bit　0 or 1の2値をとる要素。　bit列　複数のbitの列 → n bitsなら2^n通りの値

コンピューター　bit列に様々な操作(演算)を施こして計算

量子コンピューター

qubit(量子ビット)　$|0\rangle$と$|1\rangle$という(規格化された)直交する2状態をもつ量子系。

一般の状態　$\alpha|0\rangle+\beta|1\rangle$　$(\alpha,\beta\in\mathbb{C})$

量子コンピューター　qubitsの集まりに様々な操作(ユニタリー変換)を施こして計算

n個のqubits　$n=2$　$|0\rangle_1\otimes|0\rangle_2$, $|0\rangle_1\otimes|1\rangle_2$, $|1\rangle_1\otimes|0\rangle_2$, $|1\rangle_1\otimes|1\rangle_2$

の4状態の線形結合

一般のn　$|\sigma_1\rangle_1\otimes\cdots\otimes|\sigma_n\rangle_n$　$(\sigma_1,\cdots,\sigma_n=0,1)$

の2^n状態の線形結合

量子コンピューターはすごいのか?

N桁の自然数の素因数分解

- 古典計算機で必要なステップ数 ~ $C^{N^{1/3}}$ 　定数
- 量子コンピューター(ショアのアルゴリズム)で必要なステップ数 ~ N^2 　(Shor 1994)

Nが大きくなったときの増え方が全くちがう

量子コンピューターには簡単にできて古典コンピューターには(すごく)難しい問題がある。

(Googleの実演 2019 53qubits)

量子コンピューターはなぜすごいのか? よくある説明

- 古典コンピューター　入力 0010010001 $\xrightarrow{\text{計算}}$ 出力 1010110 1
- 量子コンピューター　入力 (1) $|\Psi\rangle = \sum_{\sigma_1,\cdots,\sigma_n=0,1} \alpha_{\sigma_1,\cdots,\sigma_n} |\sigma_1\rangle_1 |\sigma_2\rangle_2 \cdots |\sigma_n\rangle_n$

出力 (2) $\hat{U}|\Psi\rangle = \sum_{\sigma_1,\cdots,\sigma_n=0,1} \alpha_{\sigma_1,\cdots,\sigma_n} \hat{U} |\sigma_1\rangle_1 |\sigma_2\rangle_2 \cdots |\sigma_n\rangle_n$

2^nとおりのbitの配列すべてについて並列でまとめて計算している!!!

さらに工夫が必要!

しかし(2)の状態をフツウに測定してしまうと、1つの配列しかわからない!

▷ ドイッチュのアルゴリズム (Deutsch 1985)　「やらせ」っぽい(が面白い)例

問題　$f(\sigma)$ は $\sigma=0,1$ の関数で値 0, 1 のみをとる。われわれは $f(\cdot)$ を知らない

$f(0)=f(1)$ かどうかを判定せよ。

そういう f は全部で4通り。

条件　ただし $f(\cdot)$ は1回しか使ってはいけない!!

古典的には絶対に不可能だが量子系ならば可能

スピン$\frac{1}{2}$の状態 (qubit) に　(1) $|\uparrow\rangle \to (-1)^{f(0)}|\uparrow\rangle$, $|\downarrow\rangle \to (-1)^{f(1)}|\downarrow\rangle$

のように作用する「しかけ」があるとする。

(2) $$\frac{1}{\sqrt{2}}\{|\uparrow\rangle+|\downarrow\rangle\} \to \frac{1}{\sqrt{2}}\{(-1)^{f(0)}|\uparrow\rangle+(-1)^{f(1)}|\downarrow\rangle\} = \frac{(-1)^{f(0)}}{\sqrt{2}}\{|\uparrow\rangle+(-1)^{f(1)-f(0)}|\downarrow\rangle\}$$

$$= \begin{cases} (-1)^{f(0)}|\rightarrow\rangle & f(0)=f(1) \text{ のとき} \\ (-1)^{f(0)}|\leftarrow\rangle & f(0)\neq f(1) \text{ のとき} \end{cases}$$

「しかけ」は1回しか使っていない!

$\hat{S}_x$ を測定して　$\rightarrow$ なら $f(0)=f(1)$,　$\leftarrow$ なら $f(0)\neq f(1)$

$f(0)$ も $f(1)$ もわからない　$(-1)^{f(0)-f(1)}$ だけがわかる。