入門量子ゲーム理論

J. Orlin Grabbe 著、盛川英典訳

2021 年 12 月 31 日

この文章は、J. Orlin Grabbe 著「An Introduction to Quantum Game Theory」arXiv:quant-ph/0506219v1 ,27/Jun/2005 の日本語訳です。残念なことに JOG は 2008 年 3 月亡くなられているとのことです。ご本人に連絡が取れないので著作権的に問題がありましたらご遺族からでもご連絡いただければ幸いです。

概要

このエッセイは量子ゲーム理論とそれに関連する経済学分野を量子力学の近い関係を紹介するものです。この文章を読むには初歩の代数幾何学の知識が必要です。量子力学のノート、結果を紹介するのに必要だからです。そして、人間の行動の問題をゲーム理論として量子力学の数式を用いて記述することが可能だからです。

キーワード；量子ゲーム理論、量子コンピュータ、経済物理学

量子ゲーム理論は量子的なコンピュータ（量子コンピュータ）を作るのに、また古典的な経済学でのゲーム理論、そして量子力学においてとても重要な役割を担います。しかしながら、量子力学及び量子コンピュータの知識は、ほとんどの経済学者とコニュニケーションをするのには大きな壁になります。他の見方をすると、量子ゲーム理論は、古典的なゲーム理論でわかっていることとは異なる認識を示すこともあります。このエッセイは、そのギャップの橋渡しをして、ゲーム理論を勉強している経済学者が自分で、量子ゲーム理論を学べるようにする試みです。このエッセイはベクトルなどの代数幾何学の知識、量子力学、量子コンピューティングの知識が必要になるでしょう。キーコンセプトはグローバーの探索アルゴリズム、ショアの因数分解アルゴリズム、そして、量子テレポーテーション、量子同士がつながっているような見せかけのテレパシーなど、量子もつれ（量子エンタングルメント）に基づいて詳細を説明し、１２の量子ゲーム理論により、古典的なゲーム理論と量子ゲーム理論の違いを解き明かします。これらの途中で、量子力学の中に、たくさんの古典的な問題の中にゲーム理論に基づいた定式化が出てくることになります。

1 Some background history: 歴史的な背景

ゲーム理論は公には 1944 にフォン・ノイマンとモルゲンシュタインによる「ゲームの理論と経済行動」（The Theory of Games and Economic Behavior, by John von Neumann and Oscar

Morgenstern) にて、はじまったとされている。しかし、それには、ハンガリーの数学者ノイマンにより、早い時期にゲーム理論と量子力学の基礎に同時に興味を見出し先例を止めたところにある。量子ゲームに興味があるので、その開発について簡単に説明していきます。

1900 年にマックスプランクは、暗黙の合意されている無限エネルギーを取り除くことを試みました。黒体放射の当時の公式は、電磁気学、放射エネルギーは、離散エネルギー単位または量子、倍数でのみ放出または吸収されることを提案しました。基本単位 h : $h\nu$, $2h\nu$, $3h\nu$... ここで、ν は放射発振器の周波数、h は現在、プランク定数として知られています 1905 年、アルバートアインシュタインは光電効果をプランクの量子を説明として使用しました。それにより、電子を放出する前に、金属は最小周波数の入射光を必要としました。周波数 ν の入射光は、粒子（光電子）を集めたように振る舞いが確認できる。そしてエネルギー $E = h\nu$ を伴います。ニールス・ボーアは、満足できない場合でも、有用なものを開発しました。軌道が仮定された惑星の電子に囲まれた原子核としての原子のモデルで、角運動量の離散値のみで、プランクの量子のエネルギーの倍数に対応します。：$\frac{h}{2\pi}, \frac{2h}{2\pi}, \frac{3h}{2\pi}$ ... 1924 年ルイ・ド・ブロイは、物質と波との結びつきについて、絵を明確にするのを助けしました。閉ループの波を記述しました。原子核を「周回する」電子などは、ループの周りに均等にフィットする必要がありました。つまり整数サイクルを持ちます。$1, 2, 3, ..$ の整数サイクルです。したがって、プランクの量子（定数 a の倍数）に関連付けられていました：$1ah, 2ah, 3ah, ...$ これは古い量子論でした。

新しい量子理論は 1925 年に、ハイゼンベルクは、時間依存の複素数のセットによって物理的な量を表すことを考えました。ハイゼンベルグの行列力学は本質的に $N \times N$ の入出力行列 H を含んでいて、物質の状態間遷移を表します。時間 t で関心のあるシステムの状態を ψ で表す（今のところ t をゼロに設定します）と、ψ は $N \times 1$ のベクトルで、ハイゼンベルグは固有ベクトル-固有値システムを使用していました。

$$H\psi = E\psi \tag{1}$$

ここで、E はスカラーで、量子化されたエネルギーレベルを表します。N 方程式のシステムが非縮退であると仮定し、E には N 個の解があります。たとえば、$E_n, n = 1, 2, ..., N$ です。E_N は固有値、つまりエネルギー準位は、ψ の状態空間の N 固有ベクトル基底に関連付けられています。

翌年、エルヴィン・シュレーディンガーは、同じ現象の電磁的解釈を探して、彼の有名な波動方程式を発表しました

$$i\hbar\frac{\partial\psi}{\partial t} = \frac{-\hbar^2}{2m}\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}\right)\psi + V\psi, \tag{2}$$

ここで、$i = \sqrt{-1}$ であり $\hbar$ はプランクのエネルギー量 h を 2π で割ったもので、V はポテンシャルエネルギーである。

シュレーディンガーは彼のアプローチとハイゼンベルグの行列力学が数学的に同等であることを発見し、喜びました。この同等性の 1 つの形式は、$\frac{-\hbar^2}{2m} = H\psi$ 方程式によって示唆されて

います。もし、私たちが、式 2のシュレーディンガー方程式の中に、$\psi = Aexp^{(-i\frac{E}{\hbar}t)}$、そして、$H = \frac{-\hbar^2}{2m}\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}\right)\psi + V$ とした場合、$E\psi = H\psi$ を得ることができ、すなわち式 1のハイゼンベルグの式である。

数年後、ジョン・フォン・ノイマンは、ハイゼンベルクに刺激され、量子力学への関心ができ、「量子力学はヒルベルト空間におけるエルミート演算子の微積分として形式化できること、そしてハイゼンベルグとシュロディンガーの理論はこの微積分の単なる特定の表現であることを示した。」エルミート行列（参考文献 35 の P22）に示すもので、それ自身が複素共役転置である。例えば、行列 $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ を考える。これの転置行列は $\sigma_y^{\mathrm{T}} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ である。そして、複素共役とると、虚数は $i \to -i, -i \to i$ となる。そしてまた σ_y を得ることができ、σ_y はエルミート行列である。エルミート行列は、ヒルベルト空間のベクトルの演算子と見なすことができる。ヒルベルト空間は、複素数 $\mathbb{C}$ で定義された単なるベクトル空間であり、定義されたノルム、長さ、または内積があることです。ベクトル ψ の場合、ノルムは $\parallel \psi \parallel = \sqrt{\psi^\dagger \psi}$ のようになります。$\psi^\dagger$ は複素共役の転置です。ヒルベルト空間は無限次元である可能性がありますが、このエッセイでは有限次元空間のみを考慮します。

その間にゲーム理論は生まれました。「ゲーム」という名前は、1921 年にフランスの数学者エミールボレルによって導入されました。ポーカーでのブラフに夢中になり、「la théorie du jeu(フランス語でゲーム理論)」を始めた人です。カールメンガーがウィーン学団のために書かれた 1928 年の論文 49 で、フォンノイマンは 2 人のゼロサムゲームを定義し、完全に解決しました。彼は、協力（連携）の可能性のためにもっと複雑だった N 人のゲームについて推測しました。それは 3 人以上で協力することで恩恵を受ける人もいます。その後、1932 年にプリンストン経済クラブに提出された有名な論文で、同じ年に量子力学の基礎に関する彼の本が出版されました。フォンノイマンは、線形計画法に必要な道具となるもの一式と、後に、モーゲンシュテルンとの共著になるゲーム理論の書籍の基礎を説明しました。（この文章 (参考文献 51) は 1937 まで出版されませんでした。）

多くの結果の中心は、線形計画問題とその双対問題 (参考文献 24) でした。線形計画問題は次のような問題です。$m \times n$ 行列 A、$n \times 1$ のベクトル b、および $m \times 1$ ベクトル c が与えられた場合、次のような非負の $m \times 1$ ベクトル x を見つる問題です。

$$x^{\mathrm{T}} c \text{ is a maximum} \tag{3}$$

$$\text{subject to}$$

$$x^{\mathrm{T}} A \leq b^{\mathrm{T}}. \tag{4}$$

双対問題は、次のような非負の $n \times 1$ ベクトル y を見つけることです。

$$y^{\mathrm{T}} b \text{ is a minimum} \tag{5}$$

subject to

$$Ay \leq c. \tag{6}$$

フォンノイマン-モルゲンシュテルンから欠落している唯一の主要なゲーム理論の結果 (そして確かに量子ゲーム理論の文献から欠落しているもの) は、コア (参考文献 40 の 8 章) の概念です。コアは N 人のゲーム理論で発生します。N 人のゲーム理論では、プレーヤーの利益は必ずしも反対ではありません、一部のプレイヤーは、他のプレイヤーと連合を形成することにより、(期待される) ペイオフを改善する場合があります。プレーヤーのサブセットごとに最大値を決定できます。これにより、ゲームの特性関数が生まれます。S を N のサブセットのセットのメンバーとします。特性関数 $v(S)$ は、プレーヤーのサブセット（つまり連合）のセットから実数 $\mathbb{R}$ のセットの（予想される）ペイオフ値へのマッピングです。

$$v(S) : S \to R. \tag{7}$$

値 $v(S)$ は、連合 S と残りのすべてのプレーヤーの連合 $N - S$ との間の 2 人のゲームで S が取得できる最大値として決定されます。データの補完は、N の各プレーヤー i に割り当てられた一連の数字（割り当てまたはペイオフ）πi です。コア C_x は、次のような代入 $C_x = \pi ix$ のセットで、

$$v(S) \leq \sum_{i \in S} \pi_i \ for\ every\ subset\ S\ in\ N,\ and\ \sum_{i \in N} \pi_i = v(N). \tag{8}$$

となります。

コア（空の場合もある）は経済均衡にとって重要です。コアは、連合の価値を、連合の各メンバーに個別に帰属するペイオフの合計以下に制限します。

Debreu と Scarf (参考文献 12) は、複製された市場ゲームでは、コアが一連の代入に縮小することを示しました。これは、限界として出現する価格システムの観点から解釈できます。

一方、量子力学では、決定論の反動力が働いていた。1935 年の論文 (参考文献 18) で、アインシュタイン-ポドルスキー-ローゼン（EPR）は、異なる方向に進む粒子の絡み合った（エンタングルな）ペアを検討することにより、量子力学の不完全性を証明しようとしました。粒子は光年によって分離される可能性があります。それにもかかわらず、一方の粒子の測定は、もう一方の粒子の状態に即座に影響を与えます。これは、量子力学のアインシュタインが言うところの「不気味な遠隔作用」の例です。(エンタングルメントについては、このエッセイの本文で後で説明しますが、波動関数をテンソル積として記述できない場合、本質的に 2 つの粒子がエンタングルメントされます。) この瞬間的な効果は「EPR チャネル」と呼ばれることもありますが、EPR が反対しているのに対し、ボーアはその存在を主張しているため、適切に言えばボーアチャネルと呼ばれるべきです。ジョン・ベル [1] は、量子力学が不完全であるかどうか、または物理学が非局所的であるかどうかを実験的に区別する一連の不等式を定式化し、いくつかの原因のいくつかの効果の瞬間的な伝

播（プロパゲーソン）を可能にしました。幸いなことに、実験的証拠が決定的に実証されているように、ボーアは正しく、EPR は間違っていました（参考文献 25)。ボーアチャネルは現在、量子テレポーテーションの基礎であり、実際、すべての量子コンピューターは、ある意味でボーア効果のデモンストレーションです。

現在のところ、量子ゲーム理論はおそらく量子計算のサブブランチと見なすことができます。後者の開発に関しては、量子コンピューターの異常な力を最初に予見したのは明らかにリチャード・ファインマン (参考文献 22) であり、古典的なコンピューターでの量子進化のシミュレーションは時間の指数関数的な減速を招くと指摘した。子ゲーム理論は、おそらく量子計算のサブブランチと見なすことができます。量もう一度、フォンノイマン (参考文献 52)（スタンウラム (参考文献 68) との）から直接的な関係があり、以下のように述べています。「1950 年代に、スタニスワフ・マルチン・ウラムとフォンノイマンは、セルオートマトンと呼ばれる計算モデルについて議論し始めました。このモデルでは、多くの自由度を持つシステムに適用される単純な計算規則によって、複雑な動作パターンが生成される可能性があります。彼らの考えの根底にあるのは、連続的な空間と時間に基づく物理学の従来の記述に対する不満でした。」（参考文献 34）

デービッドドイチェ (参考文献 13) は、量子重ね合わせが多くの古典的な計算の並列実行を可能にするかもしれないと示唆しました。確かに、重ね合わせは、もつれの状態どうかに関係なく、量子ゲームを古典的なゲームとは異なるものにする重要な新しい要素であることがわかります。動的ゲームの場合、重ね合わせで十分ですが、静的ゲームでは通常、エンタングルメントも必要です。動的ゲームの場合、重ね合わせで十分ですが、静的ゲームでは通常、エンタングルメントも必要です。（重ね合わせは、同時に 2 つ以上の状態の線形結合になることができる量子の能力です。）

量子計算への関心の嵐を生み出した「キラーアプリ」は、ピーターショア（参考文献 62）が、量子力学アルゴリズムが多項式時間で数値を因数分解できることを示したときに生まれました。これは、従来のコンピューターで利用可能な素因数分解アルゴリズムよりも指数関数的に高速化されました。ショアのアルゴリズムは、主に重ね合わせと量子フーリエ変換の独創的なアプリケーションに依存しています。

別の結果は、ロブ・グローバー (参考文献 28) によって示されました。彼は、$O(N)$ ステップから $O(\sqrt{N})$ ステップまで N アイテムデータベース内のアイテムの検索を高速化する量子力学的方法を示しました。 グローバーの結果は、ヒルベルト空間での量子状態（ベクトル）の回転に基づいています。

量子ゲーム理論は、デビッド・マイヤーがマイクロソフトでこのテーマについて講演したときに具体化したようです（これについては (参考文献 46) を参照)。このエッセイで検討されている 12 の量子ゲームのうち、3 つはマイヤーによるものです（スピンフリップゲーム、および数ゲーム I と II です。）

フォンノイマンとモルゲンシュテルンが以下のように述べたように (参考文献 53)、「私たちが経済学に適用している概念を解明するために、物理学からいくつかの実例を示しました。さまざまな理由でそのような類似点を描くことに反対する多くの社会科学者がいますが、その中には、経済理論は社会科学であり、人間の現象の科学であるため、心理学を考慮に入れる必要があるため、物理

学に基づいてモデル化することはできないという主張が一般的に見られますが、そのような声明は少なくとも時期尚早です。」逆に、経済概念と量子力学の概念を混合することに同様に反対する人もいるかもしれませんが、そのような反対は少なくとも時期尚早です。確かに、人間の脳は間違いなく量子コンピューターです (参考文献 65, 66, 55, 14, 15)、精神はそれ以上かもしれませんが、心理学の問題で量子力学を無視することは、経済学ではなく、とても愚かなことです。逆に言えば、量子測定問題における人間の精神の役割は、フォン・ノイマンによって最初に明確に描写されて以来、論争の的となっています (参考文献 36)。 いずれにせよ、量子ゲームには経済学と量子力学の両方の教訓があるかもしれません。

2 Preliminary mathematical pieces: 準備のための数学

ゲームを定義する前に、その例を示します。次のセクション 3のスピンフリップゲームでは、従来のゲーム理論と量子ゲーム理論のいくつかの違いを取り上げます。スピンフリップゲームがどのように機能するかを説明するために、2×1 のベクトルと 2×2 の行列を含むいくつかの簡単な数学の予備知識が必要になります。

次の単純なベクトルは、私たちの目的に非常に役立つことがわかります。

$$u = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, d = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{9}$$

もちろん、これらは 2 次元（複素）空間の基底ベクトルです。任意の点を $au + bd$ の形式で表現できるためです。（ここで一般に a と b は複素数スカラー、$a, b \in \mathbf{C}$ であると想定されます。）ただし、u と d は、ジオメトリの外側にある多くの「スペース」または状態を表すこともできます。たとえば Yes または No の応答、電子のスピン状態のアップまたはダウン（スピンは z 方向で測定)、確率シーケンスのヘッドまたはテール、入札プロセスまたは電子デバイスの成功または失敗などです。

u または d の選択は、ゲーム内のプレーヤーの動きを表すこともでき、そのような動きのシーケンスを 2 進数のビットまたはそれと量子的に等価なキュービット（*qubit*）で表すことができます。ビットとキュービットは、ビット b が $b \in 0, 1$ という単一の数値であるという事実によって異なります。一方でキュービット q は 2 次元ヒルベルト空間のベクトル $q \in au + bd$ です。

（後で $|0\rangle, |1\rangle$ というディラック記法を紹介します。そしてこのエッセイには $u \leftrightarrow |u\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \leftrightarrow |0\rangle \leftrightarrow bit\ 0$ のような対応があります。また、同じように d には、$d \leftrightarrow |d\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \leftrightarrow |1\rangle \leftrightarrow bit\ 1$ と対応します。）

たとえば、これから何が起こるかを予見すると 5 量子ビットのレジスタまたはシーケンス $|10011\rangle$ は、ベクトルのテンソル積と数 $19 (= 2^4 + 2^1 + 2^0)$ を表すことができます。

$$|10011\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{10}$$

$= (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0)^T$ 後者のベクトルでは、我々は 0 からカウントを開始し 0 が最初の状態を利用してしまうので 1 は 19 番目ではなく 20 番目のスロットにあります。 同じシーケンスが不明瞭に書かれている可能性もあります。）

次に、ある状態を別の状態に変換（移転）する方法が必要です。 2 状態系の場合、パウリスピン行列を使用してこれを行うと便利です。 3 つの 2×2 パウリスピン行列は次のとおりです。

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{11}$$

これらの 3 つの行列は、次の単位行列 $\mathbf{1}$ とともに

$$\mathbf{1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{12}$$

スパン 2×2 エルミート行列空間（エルミート行列には実数の対角要素と、互いに複素共役である鏡像の非対角要素があることを思い出してください）各スピン行列は、基本状態 u と d に単純な影響を及ぼします。 特に、

$$\mathbf{1}u = u, \qquad \mathbf{1}d = d \tag{13}$$

$$\sigma_x u = d, \qquad \sigma_x d = u \tag{14}$$

$$\sigma_z u = u, \qquad \sigma_z d = -d \tag{15}$$

式 2は、パウリスピン行列のいくつかの行列プロパティをまとめたものです。

表 1　パウリスピン行列

$\sigma_x^2 = \mathbf{1}$
$\sigma_y^2 = \mathbf{1}$
$\sigma_x^2 = \mathbf{1}$
$\sigma_x\sigma_y = -\sigma_y\sigma_x = i\sigma_z$
$\sigma_y\sigma_z = -\sigma_z\sigma_y = i\sigma_x$
$\sigma_z\sigma_x = -\sigma_x\sigma_z = i\sigma_y$

3 The spin flip game: スピンフリップゲーム

電子には 2 つのスピン状態があり、スピンアップとスピンダウンです。アリスとボブの間で行われる電子スピンフリップの簡単なゲームを考えてみましょう。アリスは最初にスピンアップ状態 u の電子を準備します。この最初のステップの後、ボブは σ_x または $\mathbf{1}$ 行列のいずれかを u に適用し、次のいずれかになります。

$$\sigma_x u = d \,\text{or}\, \mathbf{1}u = u. \tag{16}$$

次に、アリス（ボブの行動や電子の状態を知らない）が順番を取り、電子スピンに σ_x または $\mathbf{1}$ のいずれかを適用します。次に、ボブ（アリスの行動や電子の状態を知らない）の順番となります。最後に電子のスピン状態が測定されます。u 状態の場合、ボブは 1 ドルを獲得し、アリスは 1 ドルを失います。d 状態の場合、アリスは 1 ドルを獲得し、ボブは同じ金額を失います。

ボブ（列）とアリス（行）による可能な選択肢のシーケンスを表 2に要約します。アリスの動きは、右から左に読んだ 3 つのシーケンスの真ん中であることに注意してください。

表 2　プレイヤーの動きのシーケンス

$Alice\backslash Bob$	$\mathbf{1},\mathbf{1}$	$\mathbf{1},\sigma_x$	$\sigma_x,\mathbf{1}$	σ_x,σ_x
$\mathbf{1}$	$\mathbf{1},\mathbf{1},\mathbf{1}$	$\mathbf{1},\mathbf{1},\sigma_x$	$\sigma_x,\mathbf{1},\mathbf{1}$	$\sigma_x,\mathbf{1},\sigma_x$
σ_x	$\mathbf{1},\sigma_x,\mathbf{1}$	$\mathbf{1},\sigma_x,\sigma_x$	$\sigma_x,\sigma_x,\mathbf{1}$	$\sigma_x,\sigma_x,\sigma_x$

たとえば、$\mathbf{1},\mathbf{1},\sigma_x$ は、ボブが σ_x を適用し、次にアリスが $\mathbf{1}$ を適用し、次にボブが $\mathbf{1}$ を適用したことを意味します。最終的な結果は $\mathbf{11}\sigma_x u = d.$ です。したがって、アリスは 1 ドルを獲得します。初期の u 状態から各移動後のスピン状態の配列は、表 3に示されています。繰り返しますが、3 つの各シーケンスは右から左に読む必要があります。

表 3　スピン状態のシーケンス

$Alice\backslash Bob$	$\mathbf{1},\mathbf{1}$	$\mathbf{1},\sigma_x$	$\sigma_x,\mathbf{1}$	σ_x,σ_x
$\mathbf{1}$	u,u,u	d,d,d	d,u,u	u,d,d
σ_x	d,d,u	u,u,d	u,d,u	d,u,d

最後に、表 4は、アリスへのペイオフ（利得）を示しています。最終スピンが d 状態の場合は正であり、u 状態であれば負です。

表 4　アリスのペイオフ

$Alice \backslash Bob$	$\mathbf{1},\mathbf{1}$	$\mathbf{1},\sigma_x$	$\sigma_x,\mathbf{1}$	σ_x,σ_x
$\mathbf{1}$	-1	$+1$	$+1$	-1
σ_x	$+1$	-1	-1	$+1$

これは基本的なスピンフリップゲームであり、これを 2 つの方向に拡張していきます。1 つは確率的な動きを考慮すること、もう 1 つは状態の量子重ね合わせ（量子もつれなし）を考慮することです。ただし、これを行う前にいくつかの基本的なゲーム理論の用語について考えてみましょう。

4　First game definitions and strategies: 最初のゲームの定義と戦略

前のセクションで暗示されているように、あるゲーム Γ は集合 $\Gamma = \Gamma$（プレーヤー、行動またはアクション、結果、利得）として定義できます。スピンフリップゲームでは、プレーヤーはアリスとボブであり、行動は行列 σ_x または $\mathbf{1}$ の適用であり、結果はスピン状態 u または d であり、アリスの利得は $+1$ または -1 でした。最終状態がそれぞれ d か u かです。これは 2 人のゼロサムゲームだったので、ボブへの見返りはアリスへの見返りとは正反対でした。

これまでのところ、ゲームの説明ではアリスとボブがどのように動きを決定したか、つまり σ_x と $\mathbf{1}$ のどちらを適用するかをどのように決定したかの説明は省略されています。戦略は、ゲームの任意の段階で行動を決定するためのルールです。つまり、この例では行動は集合 $\{\mathbf{1},\sigma_x\}$ のある要素ですが、戦略はゲームの状態を一連の行動にマッピングする関数 f : ゲームの状態 $\rightarrow \{\mathbf{1},\sigma_x\}$ です（量子ゲーム理論の文献では、この点について不明瞭があるようです)。「ゲームの状態」はプレイヤーに知られていない可能性があるためこれはあまり適切な定義ではありません。つまりあるプレイヤーは自分の行動以上のことをほとんど知らないかもしれません。それでは、これを次のように修正しましょう。アリスの戦略はマッピング f_A : { アリスの情報 } $\rightarrow$ { アリスの行動 } です。そして、ボブも同様です。スピンフリップゲームでは、アリスは電子の最初の準備の後、行動を選択する機会が 1 つしかないため、3 つの動きのシーケンスの 2 番目、つまり中間のステップで 1 つの戦略があります。ボブは最初と最後のステップのための 2 つの戦略を持っています。したがって、一連の行動に関連するのは一連の戦略です。経済学では、戦略はプレーヤーの情報に大きく依存しています。特に興味深いのは非対称情報であり、あるプレーヤーが別のプレーヤーよりも情報の利点がある場合、またはプレーヤーの情報の集合が同じではない場合です。もしボブがアリスができない量子操作ができれば、明らかにボブは少なくともその点で情報の利点があります。ゲームの許可された動きとペイオフを考えると、戦略はゲームに内生的（endogenous）であるため、戦略はゲームの定義の一部ではありません。むしろ、ゲームを解くことは本質的にプレイヤーにとって最適な戦略を決定することを意味します。

情報セットの概念は重要です。スピンフリップゲームでは、ボブもアリスも相手の行動を知ることができないと言いました。この仮定を緩和したとしましょう。つまりアリスはボブの最初の行動

を知り、それに応じて彼女の行動を選ぶことができますが、しかしそれは変化をもたらしません。ボブは、アリスの行動が分かって（かつ彼自身の最初の行動は知っていて)、電子をスピンアップ状態 u のままにする最終的な行動をいつでも選択できました。彼は 100 パーセントの確率で勝ちます。それは「ゲーム」ではなくラケット（racket）です。したがって、この場合そもそもゲームにするために、アリスとボブの情報セットを制限する必要があります。

ここで例として、アリスとボブのそれぞれについて、次の戦略 f_A と f_B を考えてみましょう。これらは、何らかの確率メカニズムを使用した行動の選択を伴うため**混合戦略**と呼ばれます。

$$f_A = \text{play}\,\mathbf{1}\,\text{with probability}\,p = \frac{1}{2}, \text{play}\,\sigma_x\,\text{with probablity}\,q = \frac{1}{2} \tag{17}$$

$$f_B = \text{play}\,\mathbf{1}\,\text{with probability}\,p = \frac{1}{2}, \text{play}\,\sigma_x\,\text{with probablity}\,q = \frac{1}{2} \tag{18}$$

次に、表 4の列を見ると、ボブが何をしてもアリスの期待されるペイオフ $\bar{\pi}_A$ は常に次のようになります。

$$\bar{\pi}_A = \frac{1}{2}(+1) + \frac{1}{2}(-1) = 0 \tag{19}$$

一方、表 4の行を見ると、ボブの期待される見返りは常に次のようになります。

$$\bar{\pi}_B = \frac{1}{4}(+1) + \frac{1}{4}(-1) + \frac{1}{4}(-1) + \frac{1}{4}(+1) = 0 \tag{20}$$

もちろん、混合戦略と期待されるペイオフの概念が理にかなっているためには、連続した N 個のゲームについて検討する必要があります。

$$\Gamma_N \Gamma_{N-1} \Gamma_{N-2} \cdots \Gamma_3 \Gamma_2 \Gamma_1 \tag{21}$$

アリスへの実際のペイオフは、x が N 個のゲームのうちの勝利数を表し、かつペイオフ集合の元（集合の要素）になります。

$$\Pi = \{f(x;N)\} = \{2x - N, \text{for}\, x = 0, 1, \ldots, N\} \tag{22}$$

これらのペイオフの確率は次のようになります。

$$P(\Pi) = \{f(x;N,p)\} = \{ \begin{pmatrix} N \\ x \end{pmatrix} p^x q^{N-x}, \text{for}\, x = 0, 1, \ldots, N\} \tag{23}$$

たとえば $N = 3$ の場合、アリスの可能なペイオフは $\{-3, -1, 1, 3\}$ です。そして $p = 1$ の場合、これらはそれぞれの確率 $\{\frac{1}{8}, \frac{3}{8}, \frac{3}{8}, \frac{1}{8}\}$ です。アリスの期待されるペイオフ $\bar{\pi}_A$ は 0 ですが、N が奇数の場合、彼女の実際のペイオフが 0 になることはありません。

物理学者は式 22を、スピン $\frac{N\hbar}{2}$ の粒子の大規模に測定した場合に考えられる結果の状態を与えるものとして認識します。この場合のスピンは式 22で与えられるスピン値の可能な結果（基本単位 $\frac{\hbar}{2}$ に関して）についての $(N+1)$ 状態の量子システムを定義します。したがって、大規模な粒子の測定されたスピン状態は、アリスとボブの間の N スピンフリップゲームによって決定されると考えてよいでしょう。

表 4に類似したペイオフのマトリックスで、一般的な 2 人のゼロサムゲームの場合、アリスの行動を混合戦略（行動に対する確率の集合）で、$P_A = \{a_1, a_2, \ldots, a_m\}$ 表すようにします。一方でボブの混合戦略は $P_B = \{b_1, b_2, \ldots, b_n\}$ によって表されます。アリスのペイオフを $m \times n$ の行列 $[\pi_{ij}]$ で表すとします。次にアリスの期待されるペイオフは次のようになります。

$$\pi_A = \sum_{j=1}^{n} \sum_{i=1}^{m} \pi_{ij} a_i b_j. \tag{24}$$

これに関連して、すべての有限の 2 人の次のゼロサムゲームについて言及している**ミニマックス定理**について述べる必要があります。

$$max_{P_A}(min_{P_B}\bar{\pi}_A) = min_{P_B}(max_{P_A}\bar{\pi}_A). \tag{25}$$

つまりアリスは期待できるペイオフを最大化するために可能な行動を選択し、ボブはアリスの期待されるペイオフを最小化するために可能な行動を選択します。ミニマックス定理は、ボブの確率の最小化セットが与えられた場合のアリスの確率を最大化する集合のペイオフは、アリスの確率の最大化セットが与えられた場合のボブの確率を最小化する集合のペイオフに等しいと言えます。

5 Amplitudes and superpositions and his cheatin' heart: 振幅と重ね合わせと彼の心をだます

次の形式の量子状態（ベクトル）ψ を考えてみましょう。ここで、a と b は複素スカラーである可能性があります。

$$\psi = au + bd \tag{26}$$

量子計算では、この重ね合わされた 2 次元状態はキュービットと呼ばれ、後で詳しく説明します。ここで、a と b は振幅であり、ψ（フォンノイマン）測定は確率 $|a|^2$ で基本状態 u を取得します。一方、測定により、確率 $|b|^2$ で基本状態 d が生成されます。ここで、$|a| + |b| = 1$ です。（複素数 a とその複素共役 a^* の場合、$aa^* = a^*a = |a|^2$ であることを思い出してください。）

これにより、古典的なアナログにないスピンフリップゲームのバリエーションを含むゲームの可能性が高まります。 たとえば、$a = b = \frac{1}{\sqrt{2}}$ に設定します。

その場合、u または d のいずれかの確率は $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ です。 したがって、混合戦略がボブまたはアリスのどちらによって選択されたかに関係なく、確率は状態ベクトルの測定値に組み込まれます。

ここで、u と d は正規直交です（つまり、u と d の内積は 0 であり、u または d とそれ自体の内積は 1 です)。したがって、内積として a を取得できます。

$$\langle \psi, u \rangle = a \langle u, u \rangle + b \langle d, u \rangle = a(1) + b(0) = a \tag{27}$$

同様の計算で b が得られます。

アリスの戦略。 ここで、スピングリップゲームのバリエーションを考えてみましょう。これをアリスチートと呼びます。ここで、アリスは電子のスピン状態の初期準備で不正行為をする方法を持っています。まず、ボブが電子をスピン状態 u にすると考えていることを知って、彼女が最初にスピン状態 d の電子を準備するとします。それ以外の点では、ゲームは以前とまったく同じです。ボブとアリスの両方が $\mathbf{1}$ または σ_x のいずれかをプレイします。スピン状態の配置が表 III で変化し、アリスへのペイオフの配置が表 IV で変化することは簡単にわかりますが、ペイオフのセット Π は同じであり、対応するペイオフ確率 $P(\Pi)$ アリスへは変わりません。したがって、アリスはだまされて無駄になりました。彼女は初期状態を u から d に変更しただけで、ゲームの結果に影響はありませんでした。 以前は $+1$ でしたが、現在は -1 で、その逆も同様です。

それで、アリスは何か他のことを試みます。 彼女は初期状態を $\frac{1}{\sqrt{2}}(u + d)$ に選択します。次に、ボブが 1 をプレイするか σ_x をプレイするかにかかわらず、彼の動きはゲームの状態を変更しません。

$$\mathbf{1}[\frac{1}{\sqrt{2}}(u + d)] = \frac{1}{\sqrt{2}}(\mathbf{1}u + \mathbf{1}d) = \frac{1}{\sqrt{2}}(u + d) \tag{28}$$

$$\sigma_x[\frac{1}{\sqrt{2}}(u + d)] = \frac{1}{\sqrt{2}}(\sigma_x u + \sigma_x d) = \frac{1}{\sqrt{2}}(d + u) \tag{29}$$

$u + d = d + u$ なので、1 または σ_x のいずれかをしても状態は変化しません。しかし、電子の（変更されていない）状態の最終測定が行われると、アリスは、最終的な重ね合わせ状態の測定が等しい確率で u または d を生成するため、彼女がもう一度同じ確率でドルを勝ち取るか失うことに不満を感じます。単一のゲームの場合、ペイオフセット Π と対応する確率 $P(\Pi)$ は次のとおりです。

$$\Pi = -1, +1 \tag{30}$$

$$P(\Pi) = \{(\frac{1}{\sqrt{2}})^2, (\frac{1}{\sqrt{2}})^2\} = \{\frac{1}{2}, \frac{1}{2}\} \tag{31}$$

ボブの戦略。基本的なスピンフリップゲームに戻りましょう。ここでは、悔い改めたアリスが初期の u 状態で電子を準備し、混合戦略に従うという詳細を追加し、確率 $p = 1$ でそれぞれ $\mathbf{1}$ または σ_x を設定します。しかし今、私たちはボブにチートを許可します。 ボブは初期電子状態を準備しないため、ボブの不正行為の方法はアリスの方法とは異なります。ボブはどんな卑劣なことをすることができますか？ ボブは、袖の上にいくつかの余分なパウリスピン行列、つまり σ_x と σ_z、およびこれらの線形結合を持っています。さらに、ボブは最後の動きをしています。 ボブがいわゆるアダマール演算子 $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_x)$ をするとします。

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{32}$$

ボブの最初の動きの後、スピン状態は次のようになります。

$$Hu = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(u + d) \tag{33}$$

式（28-29）で見たように、アリスの混合戦略はこの状態を変更しません。 それからボブはもう一度 H を取得します。

$$H(Hu) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = u \tag{34}$$

ボブは常に勝ちます。 これは、状態の重ね合わせを作成するボブの能力（および彼が最後の動きをすること）に起因します。ボブがアダマール行列 H を u に適用した後、同時に生きていると同時に死んでいる Schrödinger の猫のように、電子スピンは同時に u と d の両方になります。 アリスは、確率 p で $\mathbf{1}$ をプレイし、確率 $1 - p$ で σ_x をプレイするという古典的な混合戦略をプレイして結果を変更することはできません。

6 Guess a number games: ナンバーゲームを推測する

ナンバーゲームを推測するために、最初に、キュービット、ウォルシュ-アダマール変換（アダマール変換の n ビットアナログ)、グローバー検索アルゴリズムのいくつかの要素など、いくつかの概念を紹介する必要があります (参考文献 28)。 グローバー検索アルゴリズムは、量子計算の基本的な手法の 1 つであるため、量子ゲーム理論に現れるのは当然のことです。

Dirac のブラ-ケット記法。便宜上、u と d の指定を、各 2×1 ベクトルとその 1×2 複素共役転置を表す形式に変更します。

$$|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \langle u| = (1, 0),\ |d\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \langle d| = (0, 1). \tag{35}$$

次の場合に注意してください。$|x\rangle = \begin{pmatrix} 1 \\ -i \end{pmatrix}$ そして、$\langle x| = (1, i)$ です。

これはディラックブラケット記法です。ここで $\langle x|$ はブラ、$|x\rangle$ はケットです。ブラは水平で、ケッツは垂直です。 次に、$|u\rangle\langle d|$ の形式を使用できることに注意してください。

$$|u\rangle\langle d| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0, 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{36}$$

ここで $|u\rangle\langle d|$ は、$|d\rangle$ を $|u\rangle$ に変えます。 つまり、$|u\rangle\langle d|d\rangle = |u\rangle$ で、 そして $|u\rangle$ を 2×1 のゼロベクトルに、$|u\rangle\langle d|u\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ に変換します。

量子ビットについて。 n ビットの 2 進数 x を考えてみましょう。

$$x = b_{n-1}b_{n-2}\cdots b_1 b_1 b_0, \tag{37}$$

ここで、各 b_i は 0 または 1 のいずれかであり、$b_i \in 0$、1 です。 x に相当する 10 進数は

$$x = b_{n-2}2^{n-1} + b_{n-2}2^{n-2} + \cdots b_1 2^2 b_1 2^1 b_0 2^0, \tag{38}$$

です。

量子コンピューターでは、各 b_i はそれぞれ $|u\rangle$ または $|d\rangle$ で表すことができます。対応 $|u\rangle \to |0\rangle, |d\rangle \to |1\rangle$ を作成し、 $\{|0\rangle, |1\rangle\}$ を計算基底と呼びます。

ただし、後者の表現では、2 次元ヒルベルト空間で量子ビットまたは量子ビットベクトルになります。 各キュービットは、任意の線形結合 $a|0\rangle + c|1\rangle$ にすることができます。ここで、$|a|^2 + |c|^2 = 1$ です。たとえば、3 キュービット状態を考えます。

$$|\psi\rangle = |q_2\rangle \otimes |q_1\rangle \otimes |q_o\rangle \; where \tag{39}$$

$$|q_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{40}$$

$$|q_1\rangle = |1\rangle \tag{41}$$

$$|q_0\rangle = |1\rangle. \tag{42}$$

その場合、量子レジスタは $|3\rangle$ と $|7\rangle$ の重ね合わせです。

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle \tag{43}$$

$$= \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle) \tag{44}$$

$$= \frac{1}{\sqrt{2}}(|3\rangle + |7\rangle) \tag{45}$$

この計算については、以下でさらに詳しく説明します。

n キュービットの集合は、サイズ n の量子レジスタと呼ばれます。 $N = 2^n$ のような数がありますまたは量子レジスターは、計算基底 $b_i, b_i \in \{|0\rangle, |1\rangle\}$ の観点から x を状態します。したがって、$x \in S = \{0, 1, 2, \cdots, N-1\}$。そして、ヒルベルト空間の次元は $N = 2^n$ です。 つまり、n ビットの古典的なコンピューターには合計 2^n の可能な状態があります。 対照的に、n キュービットの量子コンピューターは、これらの 2^n 状態の任意の重ね合わせになり、2^n 次元ヒルベルト空間で任意の状態またはベクトルになります。 すべての計算基底状態の重ね合わせ $ket\psi_s$ で、振幅 a_x を数または状態 x に関連付けられた確率振幅とするのは、次のように指定されます。

$$|\psi_s\rangle = \sum_{x=0}^{2^n-1} a_x |x\rangle . \tag{46}$$

もし、すべての振幅 a_x が等しい場合、この重ね合わせは指定されます。

$$|\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle . \tag{47}$$

式（47）の総和では、$|x\rangle$ はすべての基底状態または数、およびすべてを通過することに注意してください。基本状態は互いに直交しています。 したがって、与えられた数または状態 $|z\rangle$ に対して、$|z\rangle$ の振幅は内積であることがわかります。

$$\langle z|\psi_s\rangle = \frac{1}{\sqrt{2^n}}. \tag{48}$$

したがって、$|\psi_s\rangle$ を測定すると、確率で $|z\rangle$ が得られます。

$$|\langle z|\psi_s\rangle|^2 = \frac{1}{2^n}. \tag{49}$$

さて、このような $|u\rangle\, s$ と $|d\rangle\, s$ (つまり、$|0\rangle\, s$ と $|1\rangle\, s$）の多状態システムがある場合、それぞれ 2 次元のヒルベルト空間 $\mathbf{H}_2$ の場合、状態を並べて配置するだけです。 このような 2 つの状態が並んで、$\mathbf{H}_4 = \mathbf{H}_2 \otimes \mathbf{H}_2$ 次元のヒルベルト空間を形成します。 したがって、2 キュービット量子レジスタの基底ベクトルを表すことができます。

$$|0\rangle\,|0\rangle = |u\rangle \otimes |u\rangle \begin{pmatrix} 0 \\ 1 \end{pmatrix} |u\rangle = \begin{pmatrix} u \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{50}$$

$$|0\rangle|1\rangle = |u\rangle \otimes |d\rangle \begin{pmatrix} 0 \\ 1 \end{pmatrix} |d\rangle = \begin{pmatrix} d \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}. \tag{51}$$

$$|1\rangle|0\rangle = |d\rangle \otimes |u\rangle \begin{pmatrix} 0 \\ 1 \end{pmatrix} |u\rangle = \begin{pmatrix} \mathbf{0} \\ u \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}. \tag{52}$$

$$|1\rangle|0\rangle = |d\rangle \otimes |d\rangle \begin{pmatrix} 0 \\ 1 \end{pmatrix} |d\rangle = \begin{pmatrix} \mathbf{0} \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{53}$$

過度の表記法に飽きてしまった物理学者は、通常、キュービットのテンソル積を次のように圧縮します。

$$|u\rangle \otimes |u\rangle \otimes \cdots \otimes |u\rangle \to |u\rangle|u\rangle \cdots |u\rangle. \tag{54}$$

そして、しばしばそれを再び圧縮します

$$|u\rangle|u\rangle \cdots |u\rangle \to |uu \cdots u\rangle. \tag{55}$$

複数の状態を記述するこれらの異なる方法はすべて、同じことを意味します。 したがって、n 量子ビットベクトルとして表される数は、次元 2^n の空間にあり、1×2^n 列ベクトル（n 量子ビットの状態によって決定される列ベクトルの 2^n スロットのそれぞれ）として記述できます。 上記の $\mathbf{H}_2 \otimes \mathbf{H}_2$。 ここで、これらのベクトルを操作する行列 W_{2^n} を紹介します。

ウォルシュ-アダマール変換。 Walsh-Hadamard Transformation、W_{2^n} は、次のように再帰的に定義されます。

$$W_2 = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{56}$$

$$W_{2^n} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} W_{2^{n-1}} & W_{2^{n-1}} \\ W_{2^{n-1}} & -W_{2^{n-1}} \end{pmatrix}, for \quad n > 1. \tag{57}$$

W4 は

$$W_4 = W_{2^n} \otimes W_{2^n} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1W_2 & 1W_2 \\ 1W_2 & -1W_2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{58}$$

そして、例としては、

$$W_4 \left|uu\right\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \tag{59}$$

出力を再配置すると、$S = \{0, 1, 2, 3\}$ の要素の重ね合わせであることがわかります。

$$\frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2} \left[\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right] = \frac{1}{2} \left[\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle \right] \tag{60}$$

$$= \frac{1}{2} \left[\left|0\right\rangle + \left|1\right\rangle + \left|2\right\rangle + \left|3\right\rangle \right] = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left|x\right\rangle \tag{61}$$

ここで、$n = 2$ であり、2 進数を 10 進数にマッピングしました。 したがって、$\left|\psi\right\rangle = W_4 \left|uu\right\rangle$ で $\left|\psi\right\rangle$ を測定すると、与えられた数 y、$y \in S$ が確率 $\left[\frac{1}{2}\right]^2 = \frac{1}{4}$ 見つかります。ヒルベルト空間 $\mathbf{H}_4$ の基底ベクトルとしてベクトル $\left|x\right\rangle$ を取ることができます。すべて状態 $\left|0\right\rangle$ の n ビットに W_{2^n} を適用すると、$S = 0, 1, \cdots, 2n-1$ のすべての状態（数値）が均等に重み付けされて重ね合わされます。

$$W_{2^n} \left|00\cdots000\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left|x\right\rangle. \tag{62}$$

量子レジスタの初期状態のキュービットがすべて $\left|0\right\rangle$ ではない（すべて $\left|u\right\rangle$ ではない）場合はどうなりますか？ $x = x_{n-1}x_{n-2}\cdots x_2x_1x_0$、$y = y_{n-1}y_{n-2}\cdots y_2y_1y_0$ のビット単位の内積 $x \cdot y$ を $x \bullet y = x_{n-1}y_{n-1} + x_{n-2}y_{n-2} + \cdots + x_2y_2 + x_1y_1 + x_0y_0 \ mod\ 2$ として定義します。（この例では、結果 mod 2 を取得することは冗長です。）次に、レジスタが最初に状態 $\left|y\right\rangle$ であった場合、変換は次のようになります。

$$\left|\psi\right\rangle = W_{2^n} \left|y\right\rangle = \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} \left|x\right\rangle. \tag{63}$$

たとえば、$\left|y\right\rangle$ が 3 量子ビット状態 $\left|110\right\rangle$ であるとします。 次に、ビット単位の内積と符号を表 V に示します。したがって、出力状態 $\left|\psi\right\rangle$ を次のように書くことができます。

$$|\psi\rangle = W_{2^n}|y\rangle = \frac{1}{\sqrt{2^3}}\left(|000\rangle + |001\rangle - |010\rangle - |011\rangle - |100\rangle - |101\rangle + |110\rangle + |111\rangle\right) \tag{64}$$

$$= \frac{1}{\sqrt{2^3}}\left(|0\rangle + |1\rangle - |2\rangle - |3\rangle - |4\rangle - |5\rangle + |6\rangle + |7\rangle\right). \tag{65}$$

キュービットの変換はユニタリでなければなりません。 行列 U は、その逆数がその複素共役転置に等しい場合、ユニタリ行列 $U^{-1} = U^{\dagger}$ であることを思い出してください。 したがって、$U^{\dagger}U = \mathbf{1}$ です（エルミート行列 M の場合、$M^{\dagger} = M$ であるため、$M^2 = \mathbf{1}$ の場合、エルミート行列はユニタリです。）パウリスピン行列、アダマール行列 H、およびウォルシュ行列 W_{2^n} はすべてユニタリです。

表 5　初期キュービットを使用したウォルシュ変換 $|110\rangle$

$\|y\rangle$	$\|x\rangle$	$x \cdot y$	$(-1)^{xy}$
$\|110\rangle$	$\|000\rangle$	0	1
$\|110\rangle$	$\|001\rangle$	0	1
$\|110\rangle$	$\|010\rangle$	1	-1
$\|110\rangle$	$\|011\rangle$	1	-1
$\|110\rangle$	$\|100\rangle$	1	-1
$\|110\rangle$	$\|101\rangle$	1	-1
$\|110\rangle$	$\|110\rangle$	2	1
$\|110\rangle$	$\|111\rangle$	2	1

ユニタリ変換は、ベクトルの長さを保存します。 これは、$|\psi\rangle$ と $U|\psi\rangle$ の長さの 2 乗を比較するとわかります。

$$\langle\psi|\psi\rangle = |\psi|^2 \tag{66}$$

$$\langle\psi|U^{\dagger}U|\psi\rangle = \langle\psi|\mathbf{1}|\psi\rangle = |\psi|^2. \tag{67}$$

必要なもう 1 つのユニタリ変換は次のとおりです。

$$U_f|x\rangle|y\rangle = |x\rangle|y +_2 f(x)\rangle \tag{68}$$

ここで、$f : \{0,1\} \to \{0,1\}$、および $+_2$ は、$2(modulo)$ を法とする加算を意味します。U_f は、2 つのキュービット $|x\rangle|y\rangle$ で同時に動作することに注意してください。 この場合、$|x\rangle$ キュービットは制御キュービットと見なされ、操作中に変化しません。 $|y\rangle$ はデータまたはターゲットキュービットであり、$f(x) = 0$ または $f(x) = 1$ のどちらであるかによって変化します。$f(x) = x$ 場合、ここでの U_f は $c - NOT$ または XOR ゲートと呼ばれます。 、多くの場合、否定記号 $\neg$ で示さ

れます。 制御キュービットとターゲットキュービットを入力として受け取り、ターゲットキュービットを 2 を法とする 2 つの入力の合計に置き換えます。

$$\neg |x\rangle |y\rangle = |x\rangle |y +_2 x\rangle \tag{69}$$

グローバー検索アルゴリズムに関する将来の参照のために、$|y\rangle = |0\rangle - |1\rangle$ の場合の U_f の影響に注意してください。

$$U_f |x\rangle \otimes (|0\rangle - |1\rangle) = |x\rangle \otimes [(|0\rangle - |1\rangle) +_2 f(x)] . \tag{70}$$

$f(x) = 0$ のときに、

$$|x\rangle \otimes [(|0\rangle - |1\rangle) +_2 f(x)] = |x\rangle \otimes (|0\rangle - |1\rangle) = |x\rangle \otimes (-1)^{f(x)} (|0\rangle - |1\rangle) . \tag{71}$$

です。
そして、$f(x) = 1$ のときに、

$$|x\rangle \otimes [(|0\rangle - |1\rangle) +_2 f(x)] = |x\rangle \otimes (|1\rangle - |0\rangle) = |x\rangle \otimes (-1)^{f(x)} (|0\rangle - |1\rangle) . \tag{72}$$

です。 したがって要約すると、

$$U_f |x\rangle \otimes (|0\rangle - |1\rangle) = |x\rangle \otimes (-1)^{f(x)} (|0\rangle - |1\rangle) . \tag{73}$$

$S = \{0, 1, 2, \cdots, 2^{n-1}\}$ のドメイン全体で定義されるように $f\,(x)$ の定義を変更すると、$f\,(x)$: $x \in S \to \{0, 1\}$ となります。次に、いくつかの $a \in S$ に対して $f(a) = 1$ とし、すべての $x = a$ に対して $f(x) = 0$ とすることにより、$f(x)$ を指標または特性関数として使用できます。このバージョンの $f(x)$ を $f_a(x)$ として表し、関連するユニタリ変換を $U_{f_a} |x\rangle |y\rangle = |x\rangle |y +_2 f_a(x)\rangle$ として表します。 次に、前と同じように、

$$U_{f_a} |x\rangle \otimes (|0\rangle - |1\rangle) = |x\rangle \otimes (-1)^{f_a(x)} (|0\rangle - |1\rangle) . \tag{74}$$

となります。

グローバー検索アルゴリズム。コンピュータサイエンスでは、オラクル (神のみぞ知るようなランダムオラクル) は理論的ブラックボックスのサブルーチンです。そして、見ることは許されていません。 オラクルの例は、特性関数 $f_a(x) : x \in S \to \{0, 1\}$ です。 それは $f_a(a) = 1$ を設定し、そうでない場合は $fa\,(x) = 0, x \neq a$ を設定します。 $f_a(x)$ が動作可能である場合 a が何であるかについての知識がなければ、$f_a(x)$ はオラクルです。 x の値はソートされていない可能性があります。リスト、たとえばランダム化された電話番号（またはアルファベット順にソートされた電話番号所有者の名前)。 目的は、$f_a(x)$ の出力に依存してを見つけることです。 $N = 2n$ の場合アイテ

ム、50 %の確率でを見つけるための $f_a(x)$ への予想されるクエリ数は $\frac{N}{2}$ になります。 しかし、グローバーは、量子コンピューターが約 $\frac{\pi}{4}\sqrt{N}$ 回の検索でほぼ 100 %の確率で同じアイテムを見つけることができることを示しました。

数 a を探していると仮定します。ここで、a は n ビットです。 インジケーター関数 $f_a(x)$ をオラクルとして使用して、を見つけやすくします。

初期準備を行います。 最初に、$n+1$ の状態でエリアキュービットレジスタを準備します。これらはすべて $|0\rangle$ です。

$$|0\rangle|0\rangle\cdots|0\rangle|0\rangle|0\rangle\otimes|0\rangle\,, \tag{75}$$

ここで、テンソル積は、残りのキュービットからそれを引き立たせるために、右端のキュービットに対して明示的に書き出されています。左の $n|0\rangle$ キュービットに ウォルシュ変換の W_{2^n} を適用し、最後のキュービットに単純な $\mathbf{H}\sigma_x$ 変換を適用します。 前に見たように、

$$|\psi_s\rangle = W_{2^n}|0\rangle|0\rangle\cdots|0\rangle|0\rangle|0\rangle\otimes|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \tag{76}$$

$$H\sigma_x|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \tag{77}$$

コンピュータ全体の状態が、

$$|\psi_s\rangle\otimes H\sigma_x|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\otimes\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \tag{78}$$

ステップ１として、 次に、ユニタリ変換 U_{f_a} を適用します。

$$U_{f_a}|x\rangle\otimes\left(|0\rangle - |1\rangle\right) = |x\rangle\otimes(-1)^{f_a(x)}\left(|0\rangle - |1\rangle\right), \tag{79}$$

これにより以下を得ます。

$$U_{f_a}(|\psi\rangle\otimes H\psi_x|0\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\otimes\frac{1}{\sqrt{2}}(-1)^{f_a(x)}\left(|0\rangle - |1\rangle\right) \tag{80}$$

$$= \frac{1}{\sqrt{2^n}}(-1)^{f_a(x)}\sum_{x=0}^{2^n-1}|x\rangle\otimes\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{81}$$

U_{f_a} の効果は、サインオン $|x\rangle = |x\rangle$ を変更し、他のすべての重ね合わせた状態を変更しないことです。 符号 $(-1)^{f_a}(x)$ が式（80）の右端のキュービットから式（81）のキュービットの重ね合わせ

にどのように転送されたのか疑問に思われるかもしれません。 答えは、右端のキュービットがデコヒーレンスし、環境と相互作用し、$|0\rangle$ または $|1\rangle$ に「崩壊」することを許可されているということです。 これにより、2 部状態を記述するパラメータが左側の n キュービットレジスタに強制されます。

ステップ 2 として。 左端の n キュービットに W_{2^n} を再度適用します。 （または、$W_{2^n} \otimes \mathbf{1}_2$ を $n+1$ キュービットに適用します。ここで、$\mathbf{1}_2$ は 2×2 単位行列です。）

ステップ 3 として。 $f0\,(x)$ を状態 $|x\rangle = |0\rangle$ のインジケーター関数とします。 キュービットレジスタの現在の状態に $-U_{f_0}$ を適用します（否定に注意してください）。 この操作は、$|x\rangle = |0\rangle$ を除くすべての状態 $|x\rangle$ の符号を変更します。

つまり、U_{f_0} のマップ　$|0\rangle \in -|0\rangle$ であり、U_{f_0}, $-\ U_{f_0}$ の否定は、$|0\rangle$ の元の符号を復元しますが、他のすべての状態の符号を変更します。

ステップ 4 として。 左端の n キュービットに W_{2^n} を再度適用します。手順 1〜4 を $\frac{\pi}{4}$ 回繰り返します。 次に、最終状態（左端の n キュービット）$|\psi_f\rangle$ をサンプリングします。確率 1 に近い場合、$|\psi_f\rangle = |a\rangle$ となる。

これがグローバーの検索アルゴリズムですが、どういう意味ですか？ ステップ 1、2、3、および 4 は何をしますか？ 簡単な答え：$|a\rangle$ にできるだけ近づくまで、原点を中心に最初の重ね合わせ $|\psi_s\rangle$ を回転させます。 詳細を見てみましょう。

ステップ 1 での U_{f_a} の別の考え方は、行列 $\mathbf{1} - 2\,|a\rangle\langle a|$ です。 左端の n キュービットで動作します。 この操作を $|x\rangle$ に適用すると、すべての基本状態 $|x\rangle \neq |a\rangle$ に対して $|x\rangle$ が生成されますが、$|x\rangle = |a\rangle$ に対しては $-|x\rangle$ が生成されます。 同様に、ステップ 3 で U_{f_0} を考える別の方法は、行列 $\mathbf{1} - 2\,|0\rangle\langle 0|$ です。 この演算を $|x\rangle$ に適用すると、すべての基底状態 $|x\rangle \neq |a\rangle$ に対して $|x\rangle$ が生成されますが、$|x\rangle = |a\rangle$ にに対しては $-|0\rangle$ が生成されます。

ステップ 1 は、幾何学的に、ベクトル $|\psi_s\rangle$ に対して $|a\rangle$ に直交する超平面の周りの $|\psi_s\rangle$ の反射 R_a です。$W_{2^n}^2 = \mathbf{1}$ であるため、ステップ 2 から 4 は $-W_{2^n}U_{f_0}W_{2^n}^{-1}$ に対応します。演算 $-W_{2^n}U_{f_0}W_{2^n}^{-1}$ は、元の $|\psi\rangle$ $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$ の直交する超平面の周りの $|\psi_s^R\rangle$ のさらなる反射に対応します。しかし、これは私たちが望んでいることではありません。 代わりに、$|{\psi_s}^{\perp}\rangle$ を $|\psi_s\rangle$ に垂直な単位ベクトルとします。演算 $-W_{2^n}U_{f_0}W_{2^n}^{-1}$ は、$|{\psi_s}^{\perp}\rangle$ に直交する超平面の周りの $|{\psi_s}^{R}\rangle$ のさらなる反射 R_s に対応します。これをさらに反射されたベクトル $|{\psi_s}'\rangle$ と呼びます。

正味の効果は、$|\psi\rangle$ と $|a\rangle$ がまたがる平面内での $|\psi_s\rangle \to |\psi_s'\rangle$ の回転 $R_sR_a = -\ W_{2^n}U_{f_0}W_{2^a}^{-1}U_{f_a}$ です。($|\psi_s\rangle$ と $|a\rangle$ がまたがる平面とは、$c\,|\psi_s\rangle + d\,|a\rangle$ の形式のすべての状態を意味します。ここで、$c, d \in C$ です。）

要約すると、θ を $|\psi_s\rangle$ と $|a\rangle$ に直交する単位ベクトルの間の角度とします。後者は $|a^{\perp}\rangle$ と指定されます。 簡単にするために、反時計回りの順序 $|a^{\perp}\rangle$、$|\psi_s\rangle$、$|a\rangle$ を想定しています。 次に、組み合わせ R_sR_a は $|\psi_s\rangle$ を 2θ 反時計回りに回転させるため、$|a^{\perp}\rangle$ と $|\psi_s\rangle$ の間の角度は 3θ になります。つまり、R_sR_a は $|\psi_s\rangle$ を $|a\rangle$ に直交するベクトルである $|a^{\perp}\rangle$ から遠ざけるため、$|\psi_s\rangle$ を $|a\rangle$ の自体

に向かって角度 2θ だけ移動します。

グローバー検索アルゴリズムの全体的な考え方は、$|\psi_s\rangle$ が $|a\rangle$ にできるだけ近づくまで、$|\psi_s\rangle$ と $|a\rangle$ がまたがる平面内で、原点を中心に状態 $|\psi_s\rangle$ を回転させることです。 次に、$|\psi_s\rangle$ を測定すると、高い確率で $|a\rangle$ が得られます。

どのくらい回転しますか（R_sR_a を何回適用しますか）？ 回転が多すぎたり少なすぎたりして、オーバーシュートやアンダーシュートをしたくありません。 $|\psi_s\rangle$ を $|a\rangle$ まで回転させてから停止します。 $|\psi_s\rangle$ と $|a^{\perp}\rangle$ の間の角度が θ に等しく、$|a^{\perp}\rangle$ と $|a\rangle$ によって形成される平面に最初にあるベクトルまたは状態 $|\psi_s\rangle$ を考えます。 つまり、最初の重ね合わせとして $|\psi_s\rangle$ を書くことができます。

$$|\psi_s\rangle = \cos\theta\,|a^{\perp}\rangle + \sin\theta\,|a\rangle \tag{82}$$

$R_sR_a = -W_{2^n}U_{f_0}W_{n^n}^{-1}U_{f_a}$ を k 回適用した後、状態は次のようになります。

$$(R_sR_a)^k\,|\psi_s\rangle = \cos(2k+1)\theta\,|a^{\perp}\rangle + \sin(2k+1)\theta\,|a\rangle \tag{83}$$

ここで、$(2k+1)\theta = \pi$ の場合、$\cos(2k+1)\theta = 0$、$\sin(2k+1)\theta = 1$ であるため、次のようになります。

$$(R_sR_a)^k\,|\psi_s\rangle = |a\rangle \tag{84}$$

k は整数でなければならないため、これは達成できない可能性がありますが、最も近い整数を解いてみましょう。ここで、$[\cdot]_{nint}$ は最も近い整数を示します。

$$k = [\frac{\pi}{4\theta} - \frac{1}{2}]_{nint}. \tag{85}$$

2 つの単位ベクトルの内積は、それらの間の角度の余弦を与えることを忘れないでください。また、$|a\rangle$ と $|\psi_s\rangle$ の間の初期角度は $\pi - \theta$ です。 したがって、

$$\langle a|\psi_s\rangle = \frac{1}{\sqrt{2^n}} = \cos(\frac{\pi}{2} - \theta) = \sin(\theta) \tag{86}$$

$N = 2^n$ の場合、$\sin\theta \approx \theta$ に設定できます。 したがって、k の式に $\frac{1}{\sqrt{N}} = \theta$ を代入すると、次のようになります。

$$k = \left[\frac{\pi}{4}\sqrt{N} - \frac{1}{2}\right]_{nint} \tag{87}$$

したがって、この k の値は、1 に近い確率で $(R_s R_a)^k |\psi_s\rangle = |a\rangle$ を取得します。

グローバー検索アルゴリズムの例。これは、$n = 3$ キュービット（$N = 2^n = 8$）のグローバー検索の例です。(状態は、$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ にあり、変化しないキュービット $n+1$ への参照は省略します。 したがって、この例のユニタリ演算子の次元も $2^n = 8$ です。）未知の数が $|a\rangle = |5\rangle$ であると仮定します。マトリックスまたはブラックボックスオラクル U_{f_a} は次のようになります。

$$U_{f_5} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{88}$$

(番号付けは 0 で始まり、7 で終わるため、ここでの -1 は $|5\rangle$ のスロットにあることに注意してください。)

この行列は、サインオン状態 $|5\rangle$ を反転し、他の状態を変更せずに残します。 ウォルシュ行列 W_8 は

$$W_8 = \frac{1}{2^3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}. \tag{89}$$

行列 $-U_{f_0}$ は

$$-U_{f_0} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}. \tag{90}$$

この行列は、$|0\rangle$ を除くすべての状態の符号を変更します。 最後に、グローバーアルゴリズムでステップ R_sR_a を繰り返します。

$$R_sR_5 = -W_8U_{f_0}W_8^{-1}f_{f_5} = \frac{1}{4}\begin{pmatrix} -3 & 1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -3 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -3 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & -3 \end{pmatrix}. \tag{91}$$

最初の準備は

$$W_8\,|0\rangle\,|0\rangle\,|0\rangle = \frac{1}{\sqrt{2^3}}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \tag{92}$$

$N = 2^3 = 8$ なので、回転数 k を最も近い整数として計算します。

$$k = \left[\frac{\pi}{4}\sqrt{8} - \frac{1}{2}\right]_{nint} = 2. \tag{93}$$

したがって、最初の回転後、状態は次のようになります。

$$R_s R_5 W_8 \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle = \frac{1}{4\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 5 \\ 1 \\ 1 \end{pmatrix} \tag{94}$$

そして、2 回目の回転の後、

$$(R_s R_5)^5 W_8 \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle = \frac{1}{8\sqrt{2}} \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ 11 \\ -1 \\ -1 \end{pmatrix}. \tag{95}$$

$|5\rangle$ の振幅が $\frac{11}{8\sqrt{2}}$ になっていることに注意してください。 したがって、$(R_s R_5)^2 W_8 \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle$ の測定値は、確率 $(\frac{11}{8\sqrt{2}})^2 = .9453$　　を得られます。

The guess a number game I.　ボブはアリスに次のゲームに挑戦します。 アリスの、数 a は、$S = \{0, 1, \cdots, N - 1\}$ からであり、彼は特定の試行回数 k でそれを推測しようとします。アリスは、ボブの各ターンの後、オラクル U_{f_a} として機能します。彼らは $N = 2^{30} = 1,073,741,824$ で同意します。アリスは、古典的に、ボブは $N = 2^{29} = 536,870,912$ が 50 %の確率で数を推測しようとすることを要求するので、彼女はボブに最大 $k = 100,000,000$ を許可することに同意します。利点はすべて彼女のものだということ。 ただし、ボブはグローバー検索アルゴリズムを使用するつもりであり、$k = [\frac{\pi}{4}\sqrt{2^{30}} - \frac{1}{2}]_{nint} = 25,735$ 回を超えて推測するつもりはありません。

ボブは最初に $N + 1$ キュービットを次のように設定します

$$\left|\psi_s\right\rangle \otimes H\sigma_x \left|0\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \left|x\right\rangle \otimes \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle), \tag{96}$$

式（78）のように、彼は左端の n キュービット $\left|\psi_s\right\rangle$ をアリスに提示します。 これに続いて、アリスによる R_a の移動、ボブによる R_s の再生などが続き、k が移動した後、n キュービットシステムの状態は次のようになります。

$$(R_s R_a)^k \left|\psi_s\right\rangle = \cos(2k+1)\theta \left|a^{\perp}\right\rangle + \sin(2k+1)\theta \left|a\right\rangle \tag{97}$$

次に、システムが測定され、ボブが $|\sin(2k+1)\theta^2|$ の確率で勝ちます。アリスの驚いたことに、彼女はボブが許可された動きの数が少ないにもかかわらず、繰り返し勝つことに気づきました。（ボブの勝率は $p \geq 1 - \frac{1}{N}$ です。）いくつかのゲームの後、彼女はボブが常に同じ数の動き $k = 25,735$ をプレイしていることに気付きます。彼女は進行中の陰謀があるのではないかと疑うようになります。

Bernstein – Vazirani オラクル。以前、ビット単位の内積 $x \cdot y$ を定義しました。 y の代わりに $0s$ と $1s$ の定数ベクトル a を使用し、$f_{bv}^a : 0,1^n \to 0,1$ を次のように定義します。

$$f_{bv}^a(x,a) = x \cdot a \tag{98}$$

関連する変換を伴う

$$T_{bv}^a |x\rangle = (-1)^{f_{bv}^a} |x\rangle = (-1)^{x \cdot a} |x\rangle . \tag{99}$$

これは Bernstein-Vazirani のオラクルです。 a を見つけるには、$f_{bv}^a(x,a)$ の測定値がいくつ必要ですか？古典的には、x のすべての可能な値に対して測定を実行してから、a の線形方程式のセットを解く必要があります。 しかし、量子機械的に解くのはたった 1 つのステップです。理由を確認するには、式（63）と、初期状態 $|y\rangle \neq |0\rangle$ のウォルシュ変換の表 5 の計算を参照してください。次に、すべての状態の等しい重ね合わせに対する変換 T_{bv}^x の効果を比較します。

$$T_{bv}^a |\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot a} |x\rangle . \tag{100}$$

これは、初期状態のウォルシュ変換です $|a\rangle$! したがって、Walsh 変換の別のアプリケーション（それ自体の逆）で $|a\rangle$ を見つけることができます。

$$W_{2^n} T_{bv}^a |\psi_s\rangle = |a\rangle . \tag{101}$$

The guess a number game II. ナンバーゲーム II アリスはボブに言います、あなたはあまりにも多くの推測を得ています。 ゲームを変更するか、もうプレイしません。 ボブは言います：なぜあなたが不平を言っているのか分かりません。 合意した推測の数のごく一部しか作成していません。 しかし、私はあなたに何を話すでしょう。2 つの推測のみを行うための予備的な推測です。フィードバック情報を提供してから、数の 2 番目の最後の推測を行います。必要なフィードバックは、最初の推測にオラクルとして適用されるために T_{bv}^a が必要です。（もちろん、ボブは最初の推測として $|\psi_s\rangle$ を提出する予定です。）

アリスは同意し、ゲームは次のように進行します。

ボブ：準備 $|\psi_s\rangle = W_{2^n} |0 \cdots 00\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$

アリス： $T_{bv}^{\psi_s} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$

ボブ：$W_{2^n} T_{bv}^a |\psi_s\rangle = |a\rangle .$

ボブが勝ちます。 繰り返しになりますが、重要な機能は、状態の重ね合わせをアリスのオラクルに提示する機能でした。

7 Shor's factoring algorithm：ショアの素因数分解アルゴリズム

ショアのアルゴリズムは量子計算の重要な結果であるため、少し詳しく見ていきたいと思います。 それはRSA ゲームの基礎を形成します。 予備として、オイラーの定理と量子フーリエ変換 F が必要になります。

Euler' s theorem　オイラーの定理。N を整数とし、a を N 未満の整数とし、N と互いに素とします。オイラーの定理（参考文献 54、12 章) はそれを言います。

$$a^{\phi} = 1 \mod N. \tag{102}$$

ここで、ϕ はオイラーのトーティエント関数であり、比較的素数 N である N 未満の整数の総数です。 例：$N = 77$ とします。 この場合、$\phi = 60$ であるため、$23^{60} = 1 \mod 77, 39^{60} = 1 \mod 77$ などです。オイラーの定理は、任意の数の累乗が N サイクルの $\mod N$ に対して互いに素であることを意味します。

$$a, a^2, a^3, \cdots, a^{\phi-1}, a^{\phi} = 1, a, a^2, a^3, \cdots. \tag{103}$$

したがって、ϕ はサイクルまたは期間の最大長です。 もちろん、与えられた a に対して、$a^{\phi} = 1 \mod N$ のように小さい $s < \phi$ が存在する可能性があります。しかし、その場合、s が ϕ を除算することは明らかです。 $a^s = 1 \mod N$ のような s の最小値は、a の次数と呼ばれます。これは、以下のショアのアルゴリズムでは、r で表されます。ϕ、または与えられた a の任意の s または r の知識が与えられると、N を因数分解できます.$a^{\phi} = 1 \mod N$ なので、ϕ に対しても $(a^{\frac{\phi}{2}} + 1)(a^{\frac{\phi}{2}} - 1) = 0 \mod N$ となります。 $gcd\,(x, y)$ は、x と y の最大公約数を示します。次に、$gcd\,(N, a^{\frac{\phi}{2}} + 1)$ と $gcd\,(N, a^{\frac{\phi}{2}} - 1)$ の因子をチェックします。 要因がわからない場合は、ϕ を再度 2 で除算するか（前の除算で偶数の指数が残っている場合)、別の値 a を試します。例：$N = 77$ と $a = 2$ とします。$2^{60} = 1 \mod 77$ であり、ϕ を 2 で除算すると、$2^{30} = 1 \mod 77$ であることがわかります。したがって、$2^{15} \mod N = 43$ を調べます。 $gcd(77, 44) = 11$ および $gcd(77, 42) = 7$ であることがわかります。これらは 77 の 2 つの因数分解です。明らかに、これは通常、数を因数分解する最良の方法ではありませんが、量子アルゴリズムに理想的に適しています。

Quantum Fourier transform. 量子フーリエ変換量子フーリエ変換は、離散フーリエ変換によく似ています。 与えられた状態に対して $|y\rangle$ は、量子フーリエ変換はユニタリ変換です

$$F\,|y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{2\pi i x y / 2^n}\,|x\rangle\,. \tag{104}$$

この定義では、用語 xy は通常の乗算を示します。 これは、ビット内積 $x \cdot y$ ではありません。 む

しろ、$|x\rangle = 7$ および $|y\rangle = 6$ の場合、$xy = 42$ です。（対照的に、内積は $x \cdot y = 7 \cdot 6 \mod 2 = 111 \cdot 110 \mod 2 = 2 \mod 2 = 0$ です。）$F|y\rangle$ は、期間 2^n で xy の周期的です。 前に見たアダマール行列 H は、単に $n = 1$ のフーリエ変換です。これを確認するには、項の x, y をそれぞれ 0 または 1 とします。

$$\frac{1}{\sqrt{2^n}} e^{2\pi i xy/2^n} \tag{105}$$

ここで、n = 1 の場合。以下の行列を取得します。

$$\frac{1}{\sqrt{2}} \begin{pmatrix} e^0 & e^0 \\ e^0 & e^{\pi i} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{106}$$

ここで、$e^{\pi i} = \cos(\pi) + i\sin(\pi) = -1 + 0 = -1.$ を思い出してください。

逆量子フーリエ変換 F-1 は、i の符号を単純に反転します。

$$F^{-1}|y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{-2\pi i xy/2^n} |x\rangle . \tag{107}$$

Shor′ s factoring algorithm. ショアの因数分解アルゴリズム $2^{2n-2} < N^2 < 2^{2n}$ である数 N の因数を見つけたいと思います。量子コンピューター上のショアの因数分解アルゴリズムは、$O((\log N)^3)$ ステップで実行されます。2 つのレジスタを備えた量子コンピュータが必要です（これを単に左と右と呼びます)。左側のレジスタには $2n$ キュービットが含まれ、右側のレジスタには $log_2 N$ キュービットが含まれます。 両方のレジスタのキュービットの値は $|0\rangle$ に初期化されます。

$$|00\cdot 0\rangle \otimes |00\cdot 0\rangle . \tag{108}$$

ステップ 1： $m, 2 \le m \le N-2$ を選択します。 $gcd(m, N) \ge 2$ の場合、N の適切な因数が見つかりました。それ以外の場合は、手順 2〜5 で次のように進めます。

ステップ 2：左レジスタのキュービットの Walshtrans フォーム W_2^{2n} を実行して、左レジスタのすべての状態の重ね合わせを作成します。

$$(W_2^{2n} \otimes \mathbf{1}_{log_2 N})(|00\cdot 0\rangle \otimes |00\cdot 0\rangle) = |\psi_s\rangle \otimes |00\cdots 0\rangle = \frac{1}{\sqrt{2^{2n}}} \sum_{x=0}^{2^{2n-1}} |x\rangle \otimes |00\cdots 0\rangle . \tag{109}$$

ステップ 3：変換 $f_m(|x\rangle \otimes |00\cdots 0\rangle) \to |x\rangle \otimes |m^x \mod N\rangle$ を適用します。

$$f_m(|\psi_s\rangle \otimes |00\cdot 0\rangle \otimes |00\cdot 0\rangle) = \frac{1}{\sqrt{2^{2n}}} \sum_{x=0}^{2^{2n-1}} |x\rangle \otimes |m^x \mod N\rangle . \tag{110}$$

この時点で、正しいレジスタを測定したり、デコヒーレンスを許可したりすると、崩壊することに注意してください。$Z = m^z \mod N$ などの $m^x \mod N$ の特定の値に変換します。したがって、

左側のレジスタでは、$m^x \mod N = Z$ となるような状態 x を除いて、状態のすべての振幅がゼロになります。たとえば、m の次数が 5 の場合、状態の振幅は次のようになります。

$$\cdots, 0, 0, 0, c, 0, 0, 0, 0, c, 0, 0, 0, 0, c, 0, 0, 0, 0, c, 0, 0 \cdots \tag{111}$$

振幅は、5 番目の値ごとにゼロ以外になります。 状態は、以前は振幅 $\frac{1}{\sqrt{2^{2n}}}$ と等しい重ね合わせでしたが、生き残った値の振幅は約 $c = \frac{1}{\sqrt{\frac{2^{2n}}{5}}}$ になります。これはアイデアですが、（Shor に続いて）この時点では実際には正しいレジスタを観察していません。 代わりに、ステップ 4 に進みます。

ステップ 4：左側のレジスタのキュービットに対して量子フーリエ変換 F を実行します。

$$(F \otimes \mathbf{1})(f_m(|\psi_s\rangle \otimes |00\cdot 0\rangle \otimes |00\cdot 0\rangle)) = \frac{1}{\sqrt{2^{2n}}} \sum_{x=0}^{2^{2n-1}} \sum_{y=0}^{2^{2n-1}} e^{2\pi i x y / 2^{2n}} |y\rangle \otimes |m^x \mod N\rangle . \tag{112}$$

ステップ 5：システムレジスタを観察します。 これにより、y の場合は w の具体的な値が、$m^x \mod N$ の場合は $m^z \mod N$ が得られます。

$$(F \otimes \mathbf{1})(f_m(|\psi_s\rangle \otimes |00\cdot 0\rangle \otimes |00\cdot 0\rangle)) \rightarrow |w, m^z \mod N\rangle \tag{113}$$

関連する振幅の 2 乗に等しい確率で：

$$|\frac{1}{2^{2n}} \sum_{x: m^x = m^z \mod N} e^{2\pi i x y / 2^{2n}}|^2. \tag{114}$$

したがって、高い確率で、観測された w は $\frac{2^{2n}}{r}$ の整数倍に近くなります。 これで計算の量子部分は終了です。 ここで、結果を使用して期間 r を決定します。

まず、分母 $r' < N < 2n$ で w を最もよく近似する分数を見つけます。

$$|\frac{w}{2^{2n}} - \frac{d'}{r'} < \frac{1}{2^{2n+1}}| \tag{115}$$

これは、連分数を使用して行うことができます（参考文献 29、第 12 章を参照）。

次に、r の役割で r' を試してください。 もし、$mr' = 1 mod N$ の場合、$r', (m^{\frac{m'}{2}} - 1)(m^{\frac{m'}{2}} + 1)$ に対しても、$gcd(N, m^{\frac{r'}{2}} - 1)$ と $gcd(Z, m^{\frac{r'}{2}} - 1)$ の係数 N をチェックします。

r' が奇数の場合、または r' が偶数で係数が得られない場合は、m に同じ値を使用してステップ $O(\log \log N)$ 回繰り返します。 それでも問題が解決しない場合は、m を変更して最初からやり直します。

8 The RSA game

RSA は、銀行やその他の場所で広く使用されている暗号化システムです。整数環 Z_N について考えてみます。ここで、2 つの異なる大きな素数 p と q の $N = pq$ です。暗号化の場合、RSA

は Z_N の単位のみを許可します（つまり、Z_N から p または q のすべての倍数を削除します)。Z_N^* と呼ばれる残りの整数のセットは、オイラーの ϕ 関数（オイラーのトーティエント関数）$\phi = (p-1)(q-1) = (n+1) - (p+q)$ と呼ばれ、乗算中のアーベル群です。RSA 暗号システムは、比較的小さい奇数の整数 e を選択し、$d = e^{-1} \mod \phi$ を計算します。次に、Z_n^* のメッセージ M は $M^e \mod N$ として暗号化され、$M^{ed} = M^{\phi+1} = M \mod N$ として復号化されます。番号 e と N は公開されていますが、復号化キー d はメッセージの受信者だけが知っています。

アリスはボブに次のゲームに挑戦します。 彼女は公開鍵 N と e を作成し、メッセージ M を暗号化します。3 つのコンポーネント (N, e, M^e) がボブに送信されます。 ボブが $(\log N^3$ のステップ以内にメッセージ $M^e \to M$ を復号化できる場合、ボブは 1,000 ドルを獲得します。 そうでなければ、彼は 1,000 ドルを失います。

現在、RSA は非常に大きな数 N を使用しています。ただし、Shor のアルゴリズムの手順を説明するために、非常に単純な例を使用します。アリスがボブにトリプレット $(77, 11, 67)$ を送信すると仮定します。最初に、$77^2 = 5929$、および $2^{12} < 5929 < 214$ であることに注意してください。左側の量子レジスタには 14 キュービットが必要であり、右側のレジスタには 7 キュービットが必要です。

ステップ 1：ボブはランダムに $m = 39$ を選択します。ここで、$2 \leq 39 \leq 75$ です。$gcd(39, 77) = 1$ なので、ボブはステップ 2 に進みます。

ステップ 2：左側の量子ビットレジスタで、ボブは 0 から $16383 = 2^{14} - 1$ までのすべての数値の重ね合わせを作成します。

ステップ 3：ボブは、重ね合わせの各 x に関連付ける変換 f_m、値 $39^x \mod 77$ を適用します。$39^{30} \mod 77 = 1$ なので、$x \in S = 30, 60, 90, 120, 150, \cdots, 16380$。 つまり、$m = 39$ の周期は $r = 30$ です。しかし、ボブはまだこれを知りません。

ステップ 4：ボブは、x の値を含む左側のレジスターで量子フーリエ変換を実行します。 次に、両方のレジスタを観察し、左側のレジスタの状態で $w = 14,770$、右側のレジスタの $39^z \mod 77$ の値で $Z = 53$ を取得します。

ボブは、分母が 77 未満の $\frac{14770}{16384}$ に最も近い分数を見つけたいと考えています。この分数は 27 に非常に近いため、ボブは $r' = 30$、または $r' = 15$ を試します。 彼は $39^{15} - 1 \mod 77 = 42$、$39^{15} + 1 \mod 77 = 44$、および $gcd(77, 2) = 7$、$gcd(77, 44) = 11$ を取得します。これらの 2 つの要素を使用して、ボブは $\phi = (7 - 1)(11 - 1) = 60$ を計算します。したがって、復号化キー d の場合、$d = e^{-1} \mod 60$ が必要です。これにより、$d = 11^{-1} \mod 60 = 11$。復号化キーは暗号化キーと同じです。（これは、使用したモジュラス $N = 77$ が非常に小さいためです。）ボブは、アリスの暗号化されたメッセージ $(M^e)^d = 67^{11} \mod 77 = 23$ を復号化します。ボブはアリスにメッセージ $M = 23$ を伝え、1,000 ドルを収集します。

9 Nash equilibrium and prisoner's dilemma ナッシュ均衡と囚人のジレンマ

ゼロサムではない 2 × 2 のゲームと、ナッシュ均衡の伝統的なゲーム理論の概念を見て、それを量子ゲームに拡張したいと思います。 アリスとボブの両方がゲームから利益を得る可能性がありますが、得られる最大値と同様に利益を得る場合とそうでない場合があります。 両方とも効用、または混合戦略または不確実な結果を伴う期待効用を最大化しようとし、効用には基数を割り当てることができると想定しています（参考文献 23)。

非ゼロサムゲームは、伝統的に静的な形式で提示されます。 動きに対応するペイオフのマトリックスが与えられ、プレーヤーがどのようにしてそのポイントに到達したかを説明せずに、平衡の概念が提示されます。 しかし、彼らがそこに着くと、彼らはとどまることが期待されます。 それは、彼らが対応する動きをする方が良いことを示す支配戦略を持っているからです。

$s_A^i \in S_A$ をアリスが利用できる移動（必要に応じて単純な移動の凸結合を含む）とし、$s_B^j \in S_B$ をボブが利用できる移動とします。次に、アリスの支配戦略は、アリスへのペイオフ π_A がプロパティを持つように s_A を移動することです。

$$\pi_A(s_a, s_B^j) \geq \pi_A(s_a^i, s_B^j) \tag{116}$$

すべての $s_A^i \in S_A$、$s_B^j \in S_B$ について、そのような動きが存在する場合。 例として、表 VI について考えてみます。 アリスとボブにはそれぞれ、C（協力）または D（欠陥）というラベルの付いた 2 つの可能な動きがあります。 括弧内の値はペイオフ π を表します。 最初の数字はアリスへの見返りであり、2 番目の数字はボブへの見返りです。 明らかにアリス sA = D の場合、ボブが C をプレイする場合、$\pi_A(D, C) = 5 > 3$ であるのに対し、ボブがプレイする場合、$D, \pi_A(D, D) = 1 > 0$ となります。

表 6　囚人のジレンマ

	Bob C	Bob D
Alice C	$(3, 3)$	$(0, 5)$
Alice D	$(5, 0)$	$(1, 1)$

同様の理由で、$s_B = D$ でもあるため、ゲームは $\{s_A, s_B\} = \{D, D\}$ および $\{\pi(s_A), \pi(s_B)\} = \{1, 1\}$ と平衡状態になります。この結果は囚人のジレンマと呼ばれます。なぜなら、ボブとアリスの両方が C をプレイした方が明らかに良いため、$\pi_A = \pi_B = 3$ になるからです。

ナッシュ均衡は、移動 $\{s_A, s_B\}$ の組み合わせであり、どちらの当事者も、与えられた均衡点から一方的に逸脱することによって、ペイオフを増やすことはできません。

$$\pi_A(s_a, s_B) \geq \pi_A(s_a^i, s_B) \tag{117}$$

$$\pi_B(s_a, s_B) \geq \pi_B(s_a, s_B^j) \tag{118}$$

表 6 の $\{D, D\}$ では、ペイオフ $\{1, 1\}$ を生み出すことはナッシュ均衡です。アリスが C に切り替えると、彼女のペイオフは 1 から 0 になり、ボブも同様です。

ペイオフポイント $\{\pi_A, \pi_B\}$ は、$\pi_A^* \geq \pi_A$ および $\pi_B^* \geq \pi_B$ であり、不等式の 1 つが厳密である場合、別のポイント $\{\pi_A^*, \pi_B^*\}$ によって共同で支配されます。表 6 では、ポイント $\{1, 1\}$ は $\{3, 3\}$ によって支配されています。ペイオフのペア $\{\pi_A, \pi_B\}$ は、他のポイントが共同で支配しておらず、どちらの当事者も相手へのペイオフを減らさずに自分のペイオフを増やすことができない場合、パレート最適です。表 6 では、ポイント $\{3, 3\}$ はパレート最適です。これは、アリスまたはボブのいずれかによる一方的な離脱により、相手方へのペイオフが減少するためです。 $\{1, 1\}$ はどうですか？ ここでも、どちらの当事者も、相手方へのペイオフを減らさずにペイオフを増やすことはできません（実際、どちらも一方的にペイオフを増やすことはできません)。 ただし、$\{1, 1\}$ は $\{3, 3\}$ によって共同で支配されているため、パレート最適ではありません。

進化的に安定な戦略（ESS）は、ナッシュ均衡よりも制限的な概念です。 （つまり、進化的に安定している戦略は、ナッシュ均衡のサブセットを形成します。）十分に小さい η に対して s_i が $s_i + (1 - \eta)s_j$ に対して s_j よりも優れている場合、戦略 s_i は s_j に対して進化的に安定しています。概念は、s_j を再生するミュータントによって侵入される s_i を再生する集団の概念です。 ESS は、他のすべての戦略に対して進化的に安定している戦略として定義されます。 ESS は η が十分に小さい場合、たとえば $\eta \in [0, \eta_0)$ であることに注意してください。 値 η_0 は invasion barrier(侵入バリア) と呼ばれます。 $\eta > \eta_0$ の値の場合、s_i は組み合わせに対して s_j よりもパフォーマンスが優れていないため、母集団のメンバーは s_j に切り替わります。 後で検討する進化的に安定した戦略ゲームで、この概念に戻ります。

10 Escaping prisoner’s dilemma in a quantum game 量子ゲームの囚人のジレンマ

これで、量子ゲームを暫定的に定義するのに十分な背景ができました。 量子ゲーム Γ は、$\Gamma = \Gamma(\mathbf{H}, \Lambda, \{s_i\}_j, \{\pi_i\}_j)$. の要素を持つ 2 人以上のプレーヤー間の相互作用です。$\mathbf{H}$ はヒルベルト空間、Λ はゲームの初期状態、$\{s_i\}_j$ はプレーヤー j の動きのセット、π i j はプレーヤー j へのペイオフのセットです。ゲームの目的は、プレーヤー j へのペイオフを最大化する戦略を内生的に決定することです。そうする過程で、ゲームとの均衡、およびプレーヤー j に対するゲームの値 $\bar{\pi}_j$ を決定する場合としない場合があります。

最終的な詳細はのちほど述べますが、この時点で、囚人のジレンマの量子バージョンを紹介したいと思います。囚人のジレンマの量子バージョン（参考文献 20）では、アリスとボブはそれぞれキュービットを持っており、自分のキュービットを操作することができます。各キュービットは基底ベクトル $|C\rangle$ と $|D\rangle$ を持つ $\mathbf{H}_2$ にあり、ゲームは基底ベクトル $|CC\rangle, |CD\rangle, |DC\rangle, |DD\rangle$ を持つ $\mathbf{H}_2 \otimes \mathbf{H}_2$ にあります。アリスのキュービットは各ペアの左端のキュービットであり、ボブのキュー

ビットは右端です。 ゲームは単純な量子ネットワークです。

ゲームの初期状態 Λ は

$$\Lambda = U\left|CC\right\rangle, \tag{119}$$

ここで、U は、アリスとボブの両方に知られている、両方のキュービットを操作するユニタリ演算子です。アリスとボブは戦略的な動きとして s_A, s_B,

$$s_A = U_A \tag{120}$$

$$s_B = U_B \tag{121}$$

ここで、UA と UB は、それぞれのプレーヤーのキュービットでのみ動作するユニタリ行列です。アリスとボブが動き出した後のゲームの状態は

$$(U_A \otimes U_B)U\left|CC\right\rangle. \tag{122}$$

アリスとボブは、最終測定のためにキュービットを転送します。 ユニタリ演算子 U の逆数が適用され、ゲームが次の状態になります。

$$U^{\dagger}(U_A \otimes U_B)U\left|CC\right\rangle. \tag{123}$$

次に、測定が行われ、$\mathbf{H}_2 \otimes \mathbf{H}_2$ の 4 つの基底ベクトルの 1 つが生成されます。 アリスとボブに関連するペイオフ値は、前に表 6 に示したものです。

アリスとボブがそれぞれのユニタリ行列 U_A, U_B を選択することにより、この量子ゲームで囚人のジレンマをどのように回避するかは、エンタングルメント関連の戦略を実行することに依存します。 したがって、次のセクションでエンタングルメントを検討するまで、量子囚人のジレンマゲームのさらなる議論を延期します。 ただし、純粋な量子戦略は、プレーヤーのキュービットに作用するユニタリ作用素であるということを強調したかったのです。

11 Entanglement エンタングルメント

ヒルベルト空間 $\mathbf{H}$ のベクトル $|\psi\rangle$ を検討してきました。ベクトルまたは状態 $|\psi\rangle$ は、ヒルベルト空間の特定のテンソル積分解に対して因数分解されない場合、エンタングルメント（絡み合い）します。$\mathbf{H} = \mathbf{H}_{\otimes}\mathbf{H}_2$。 たとえば、状態 $|\psi_1\rangle = a\left|00\right\rangle + b\left|01\right\rangle$ は次のようにテンソル積に分解できます。

$$|\psi_1\rangle = a\left|00\right\rangle + b\left|01\right\rangle = |0\rangle \otimes (a\left|0\right\rangle + b\left|1\right\rangle), \tag{124}$$

そうこれはエンタングルメントしない。 一方、状態 $|\psi_2\rangle = a\,|00\rangle + b\,|11\rangle$ はテンソル積に分解できないため、絡み合っています。 絡み合った状態は、空間や時間に関係なく、単一の全体として機能します。 1 つのエンタングルされたキュービットに対して実行される操作は、エンタングルされたキュービットの状態に即座に影響します。 エンタングルメントは「離れた場所での不気味な行動」を生み出します。

ヒルベルト空間に使用してきた正規直交計算基底の代わりに、ベル基底と呼ばれる別の正規直交基底が使用されることがあります。 ベル基底は、最大に絡み合った状態のセットです。 $\mathbf{H}_4$ の 2 量子ビットの場合、この絡み合った基底を次のように表すことができます。

$$|b_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{125}$$

$$|b_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{126}$$

$$|b_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{127}$$

$$|b_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{128}$$

アダマール変換 H と c-NOT ゲートの組み合わせを使用することにより、計算基底をベル基底に変換するのは簡単です。 まず、アダマール変換を左端のキュービットに適用します。 次に、左キュービットをソースとして、右キュービットをターゲットとして c-NOT（式 69 を確認）を適用します。 この変換の省略形は $\neg(H \otimes 1)$ です。

$$\neg(H \otimes \mathbf{1})\,|00\rangle \to \neg\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle \to |b_0\rangle \tag{129}$$

$$\neg(H \otimes \mathbf{1})\,|01\rangle \to \neg\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|1\rangle \to |b_1\rangle \tag{130}$$

$$\neg(H \otimes \mathbf{1})\,|10\rangle \to \neg\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|0\rangle \to |b_2\rangle \tag{131}$$

$$\neg(H \otimes \mathbf{1})\,|11\rangle \to \neg\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|1\rangle \to |b_3\rangle\,. \tag{132}$$

ここで、量子もつれがどのようにして囚人のジレンマからプレイヤーを解放できるかを示します。

12 Return to the quantum Prisoner's Dilemma 量子の囚人のジレンマに戻る

再度、囚人のジレンマの量子バージョンに戻りましょう。 表記の一貫性を保つために、$|C\rangle \to |0\rangle$ と $|D\rangle \to |1\rangle$ をマップします。ゲームの最終状態である式（123）を離れると、次の形式になります。

$$|\psi_f\rangle = U^\dagger (U_A \otimes U_B) U |00\rangle . \tag{133}$$

システムの測定が行われると、4 つの基底ベクトル $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ のいずれかに投影され、関連する確率で、アリスへの期待どおりのペイオフ $\bar{\pi}_A$ が得られます（表 6 を参照）:

$$\bar{\pi}_A = 3|\langle\phi_F|00\rangle|^2 + 0|\langle\phi_F|01\rangle|^2 + 5|\langle\phi_F|10\rangle|^2 + 1|\langle\phi_F|11\rangle|^2. \tag{134}$$

ペイオフ確率はゲームの最終状態に依存し、最終状態はユニタリ行列 U に依存し、プレーヤーは U_A と U_B を移動します。 これらのそれぞれを順番に考えてみましょう。

ユニタリ行列 U の目的は、アリスとボブのキュービットを絡ませることです。 この絡み合いがなければ、ボブとアリスへの見返りは古典的なゲームと同じままです（つまり、$(1,1)$ のナッシュ均衡）。

ユニタリ行列 U を次のようにしましょう（ここで、$\otimes n$ は単にテンソル積 n 回を意味します）。

$$U = \frac{1}{\sqrt{2}}(\mathbf{1}^{\otimes 2} + i\sigma_x^{\otimes 2}). \tag{135}$$

逆は、

$$U^\dagger = \frac{1}{\sqrt{2}}(\mathbf{1}^{\otimes 2} - i\sigma_x^{\otimes 2}). \tag{136}$$

次に、U を最初に適用した後、システム状態は次のようになります。

$$U|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle). \tag{137}$$

ここで、最初に、協力（行列 $UA = UB = \mathbf{1}$ を適用）または欠陥（スピンフリップパウリ行列 $U_A = U_B = \sigma_x$ を適用）のいずれかである、アリスとボブのいくつかの従来の動きについて考えてみましょう。

$$both\ cooperate : (\mathbf{1} \otimes \mathbf{1})U|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle) \tag{138}$$

$$Alice\ defects : (\sigma_x \otimes \mathbf{1})U|00\rangle = \frac{1}{\sqrt{2}}(|10\rangle + i|01\rangle) \tag{139}$$

$$Bob\ defects : (\mathbf{1} \otimes \sigma_x)U\,|00\rangle = \frac{1}{\sqrt{2}}(|01\rangle + i\,|10\rangle) \tag{140}$$

$$both\ defects : (\sigma_x \otimes \sigma_x)U\,|00\rangle = \frac{1}{\sqrt{2}}(|11\rangle + i\,|00\rangle). \tag{141}$$

次に、単一変換の逆 U、つまり $U^{-1} = U^\dagger$ を適用すると、次のようになります。

$$both\ cooperate : U^\dagger \frac{1}{\sqrt{2}}(|00\rangle + i\,|11\rangle) = |00\rangle\, with\ probability\ 1 \tag{142}$$

$$Alice\ defects : U^\dagger \frac{1}{\sqrt{2}}(|10\rangle + i\,|01\rangle) = |10\rangle\, with\ probability\ 1 \tag{143}$$

$$Bob\ defects : U^\dagger \frac{1}{\sqrt{2}}(|01\rangle + i\,|10\rangle) = |01\rangle\, with\ probability\ 1 \tag{144}$$

$$both\ defect : U^\dagger \frac{1}{\sqrt{2}}(|11\rangle + i\,|00\rangle) = |11\rangle\, with\ probability\ 1. \tag{145}$$

これらは、表 6 の 4 つの古典的な結果に対応しており、古典的なゲームが囚人のジレンマに含まれていることを示しています。

それでは、アリスとボブによるあまり伝統的ではない量子運動について考えてみましょう。 たとえば、アリスが $\mathbf{1}$ をプレイし、ボブがアダマール行列 H をプレイするとします。

$$(\mathbf{1} \otimes H)U\,|00\rangle = \frac{1}{2}\,|0\rangle\,(|0\rangle + |1\rangle) + \frac{i}{2}\,|1\rangle\,(|0\rangle - |1\rangle) = \frac{1}{2}[|00\rangle + |01\rangle\, i\,|10\rangle - i\,|11\rangle)]. \tag{146}$$

次に、$U^\dagger$ を最後の方程式に適用すると、次のような最終状態が得られます。

$$U^\dagger(\mathbf{1} \otimes H)U\,|00\rangle = \frac{1}{\sqrt{2}}(|01\rangle - i\,|11\rangle). \tag{147}$$

以来 $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ および $|\frac{-i}{\sqrt{2}}|^2 = \frac{1}{2}$ で、後者の状態を測定すると、アリスに 0 のペイアウトまたは 1 のペイアウトが等しい確率で与えられるため、$\bar{\pi}_A = 0.5$、$\bar{\pi}_B = 3$ になります。

逆に、ボブが $\mathbf{1}$ をプレイし、アリスがアダマール行列 H をプレイするとします。

$$(H \otimes \mathbf{1})U\,|00\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |10\rangle + i\,|01\rangle - i\,|11\rangle]. \tag{148}$$

次に、$U^\dagger$ を最後の方程式に適用すると、逆プレイの最終状態が次のようになります。

$$U^\dagger(H \otimes \mathbf{1})U\,|00\rangle = \frac{1}{\sqrt{2}}(|10\rangle - i\,|11\rangle). \tag{149}$$

後者の状態を測定すると、アリスは 5 のペイアウトまたは 1 のペイアウトを同じ確率で与えるので、$\bar{\pi}_A = 3, \bar{\pi}_B = 0.5$ になります。

検討したい残りのケースを要約します。

$$(H \otimes \sigma_x)U\,|00\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |11\rangle + i\,|01\rangle - i\,|10\rangle] \tag{150}$$

$$(\sigma_x \otimes H)U\,|00\rangle = \frac{1}{\sqrt{2}}[|10\rangle + |11\rangle + i\,|01\rangle - i\,|01\rangle] \tag{151}$$

$$(H \otimes H)U\,|00\rangle = \frac{1}{\sqrt{2^3}}[|00\rangle + |10\rangle + |01\rangle + |11\rangle + i\,|00\rangle - i\,|10\rangle - i\,|01\rangle - i\,|11\rangle], \tag{152}$$

$$U^\dagger(H \otimes \sigma_x)U\,|00\rangle = \frac{1}{\sqrt{2}}[|11\rangle - i\,|10\rangle], \bar{\pi}_A = 3, \bar{\pi}_B = 0.5 \tag{153}$$

$$U^\dagger(\sigma_x \otimes H)U\,|00\rangle = \frac{1}{\sqrt{2}}[|11\rangle - i\,|01\rangle], \bar{\pi}_A = 0.5, \bar{\pi}_B = 3 \tag{154}$$

$$U^\dagger(H \otimes H)U\,|00\rangle = \frac{1}{2}[|00\rangle + |11\rangle - i\,|01\rangle - i\,|10\rangle], \bar{\pi}_A = \bar{\pi}_B = 2.25. \tag{155}$$

「$\succ$」は「優先される」ことを示します。 アリスはもはや好ましい戦略を持っていません。 $\sigma_x \succ_A \mathbf{1}$ で、ボブが σ_x または H をプレイすると、$H \succ_A \sigma_x$ になります。 これを表 7 に示します。 また、ペイオフ状態

表 7　σ x、H の量子移動が許可された囚人のジレンマ。

	Bob $\mathbf{1}$	Bob σ_x	Bob H
Alice $\mathbf{1}$	$(3,3)$	$(0,5)$	$(\frac{1}{2},3)$
Alice σ_x	$(5,0)$	$(1,1)$	$(\frac{1}{2},3)$
Alice H	$(3,\frac{1}{2})$	$(3,\frac{1}{2})$	$(2\frac{1}{4},2\frac{1}{4})$

(σ_x, σ_x) に対応する $(1,1)$ は、もはやナッシュ均衡ではありません。ただし、(H,H) に対応する結果 $(2\frac{1}{4},2\frac{1}{4})$ は、パレート最適ではありませんが、ナッシュ均衡になります。 明らかに、量子移動を追加すると、ゲームの結果が変わります。

パレート最適性を誘導するために、許可された動きのセットを拡張して、$S = 1, \sigma_x, H, \sigma_z$ のメンバーにしましょう。 結果を表 8 に示す。 結果 $(21,21)$ は、もはやナッシュ均衡ではありませんが、(σ_z, σ_z) に対応する $(3,3)$ に新しいナッシュ均衡があります。 ペイオフは非平衡戦略ポイント $(1,1)$ のペイオフと等しいため、共同で支配されることはありません。 このナッシュ均衡はパレート最適です。 囚人のジレンマの終わりです。

ゲームの開始時と終了時に適用されるユニタリ行列 U の意味は何ですか？ それはまだ決定されていません。 時々それは第三者のプレーヤー、審判またはコーディネーターに帰せられます。 し

かし、他の解釈もあります。 おそらく最良の方法は、「プレーヤーの協力者として機能し、ナッシュ均衡での見返りを最大化するのに役立つ」(参考文献 10) とのことです。 これには囚人のジレンマの見えざる手？ より多くの作業が必要です。

表 8　σ_x, H, σ_z の量子移動が許可された囚人のジレンマ。 動きに (σ_z, σ_z) 対応する結果 $(3,3)$ は、ナッシュ均衡であるだけでなく、パレート最適でもあります。

	Bob $\mathbf{1}$	Bob σ_x	Bob H	Bob σ_z
Alice $\mathbf{1}$	$(3,3)$	$(0,5)$	$(\frac{1}{2},3)$	$(1,1)$
Alice σ_x	$(5,0)$	$(1,1)$	$(\frac{1}{2},3)$	$(0,5)$
Alice H	$(3,\frac{1}{2})$	$(3,\frac{1}{2})$	$(2\frac{1}{4},2\frac{1}{4})$	$(1\frac{1}{2},4)$
Alice σ_x	$(1,1)$	$(5,0)$	$(4,1\frac{1}{2})$	$(3,3)$

13　Battle of the sexes game: a quantum game with entanglement. 男女の戦いゲーム：絡み合いのある量子ゲーム

いわゆる「男女の戦い」ゲームは、実際には戦いではありません。それは、相反する価値観を持つラブフェストです。アリスとボブは一緒に夜を過ごしたいと思っています、そして彼らがそれを別々に過ごすならば、彼らのそれぞれの見返りは $\{\gamma,\gamma\}$ です。いつものように、アリスのペイオフが最初にリストされ、ボブのペイオフが 2 番目にリストされます。アリスは夜をオペラ座で過ごすことを好み（O)、ボブは夜をテレビを見ることを好みます（T)。オペラでの両方のペイオフは $\{\alpha,\beta\}$ ですが、テレビを見ている両方のペイオフは β,α です。$\alpha > \beta > \gamma$ と仮定します。アリスとボブはどちらもそれぞれの仕事で働いており、通信できません（携帯電話はありません)。それぞれがオペラかボブのテレビの家に現れる予定で、その場所でお互いに会うことを望んでいます。したがって、それぞれの動きは、セット O,T のメンバーです。 ゲームを表 9 に示します。

表を調べると、移動中の 2 つのナッシュ均衡 (O,O) と (T,T) がわかります。 これらの均衡のいずれかからいずれかのプレーヤーが一方的に逸脱すると、見返りが少なくなります。 しかし・・・、アリスの各行とボブの各列にはナッシュ均衡があります。 では、どちらのプレイヤーが何をすべきかをどのように決定するのでしょうか？

さらに、混合戦略には、アリスが確率 p で O をプレイし、確率 $1-p$ で T をプレイする一方で、ボブが確率 q で O をプレイし、確率 $1-q$ で T をプレイすることから生じる、3 番目の隠れたナッシュ均衡があります。 0 でも 1 でもありません。

表 9　男女の戦い $(\alpha > \beta > \gamma)$

	Bob O	Bob T
Alice O	(α,β)	(γ,γ)
Alice T	(γ,γ)	(β,α)

計算では、$p = \frac{\alpha-\gamma}{\alpha+\beta-2\gamma}, \frac{\beta-\gamma}{\alpha+\beta-2\gamma}$ が示されています。 これらの確率は、アリスとボブに期待される見返りを与えます。

$$\bar{\pi}_A(p,q) = \bar{\pi}_B(p,q) = \frac{\alpha\beta - \gamma^2}{\alpha + \beta - 2\gamma}. \tag{156}$$

表 9 に示されているコーナーのナッシュ均衡では、アリスまたはボブの一方が α のペイオフを受け取り、もう一方が β のペイオフを受け取ります。 しかし $\alpha > \beta > \bar{\pi}_A(p,q)$。 したがって、アリスとボブの両方が 3 番目のナッシュ均衡で悪化します。

この 3 番目のナッシュ均衡を見つけるために、最初に、アリスとボブの各動きの想定される確率を考慮して、アリスの期待される見返りを記述します。

$$\bar{\pi}_A = pq\alpha + p(1-q)\gamma + (1-p)q\gamma + (1-p)(1-q)\beta. \tag{157}$$

次に、p を最大化して、

$$\frac{\partial \bar{\pi}_A}{\partial p} = q\alpha + (1-q)\gamma - q\gamma - (1-q)\beta = 0. \tag{158}$$

後者の方程式を q について解くと、$q = \beta - \gamma$ になります。 ボブの予想ペイオフを最大化する同様の計算により、p が得られます。

量子戦略では、どのように物事を変えるのですか？ $|O\rangle \to |0\rangle$ と $|T\rangle \to |1\rangle$ をマッピングし、ユニタリ行列 U を適用して状態をエンタングルしましょう。

$$U = \frac{1}{\sqrt{2}}(\mathbf{1}^{\otimes 2} + i\sigma_x^{\otimes 2}), \tag{159}$$

初期状態 $|00\rangle$ に。 次に、U を最初に適用した後、システム状態は次のようになります。

$$U\,|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + i\,|11\rangle), \tag{160}$$

従来通り。 アリスとボブはどちらも U と初期状態 $|00\rangle$ を知っています。

アリスとボブが戦略セット $S = \{1, \sigma_x, H, \sigma_z\}$ から移動できるようにします。それらの個々のキュービット。 次に、結果に $U^\dagger$ を適用します。 最終的な状態は、囚人のジレンマで以前に計算された状態ですが、次の表 10 に示すように、期待されるペイオフは異なります。

左上のエントリは、古典的なゲームが量子ゲームに含まれていることを示しています。表の唯一のナッシュ均衡は、(σ_x, σ_x) に対応する (β, α) です。アリスとボブは一緒にテレビを見ながら夜を過ごします。アリスのペイオフはボブの α のペイオフよりも β だけ少なくなっています。(σ_x, σ_x) では、アリスもボブも一方的にペイオフを増やすことはできません。また、このペイオフのセットは別のペイオフのセットによって共同で支配されないため、パレート最適でもあります。これこそテレビのルールですね！

表 10　量子移動を伴う男女ゲームの戦い。 ナッシュ均衡は (σ_x, σ_x) に対応する (α, β) です。 アリスとボブは夜をテレビを見ながら過ごします。

	Bob $\mathbf{1}$	Bob σ_x	Bob H	Bob σ_z
Alice $\mathbf{1}$	(α, β)	(γ, γ)	$(\frac{\beta+\gamma}{2}, \frac{\alpha+\gamma}{2})$	(β, α)
Alice σ_x	(γ, γ)	(β, α)	$(\frac{\beta+\gamma}{2}, \frac{\alpha+\gamma}{2})$	(γ, γ)
Alice H	$(\frac{\beta+\gamma}{2}, \frac{\alpha+\gamma}{2})$	$(\frac{\beta+\gamma}{2}, \frac{\alpha+\gamma}{2})$	$(\frac{\alpha+\beta+2\gamma}{4}, \frac{\alpha+\beta+2\gamma}{4})$	$(\frac{\beta+\gamma}{2}, \frac{\alpha+\gamma}{2})$
Alice σ_z	(β, α)	(γ, γ)	$(\frac{\alpha+\gamma}{2}, \frac{\beta+\gamma}{2})$	(α, β)

混合戦略を検討することは残っています。 表の四隅のペイオフが凸集合の極値であることは明らかです。 したがって、$\mathbf{1}$ と σ_z の凸結合を考慮するだけで済みます。 アリスの期待される見返りは次の形をとります。

$$\bar{\pi}_A = pq\alpha + p(1-q)\beta + (1-p)q\beta + (1-p)(1-q)\alpha. \tag{161}$$

p で最大化、

$$\frac{\partial \bar{\pi}_A}{\partial p} = q\alpha + (1-q)\beta - q\beta - (1-q)\alpha. \tag{162}$$

q を解くと $q = \frac{1}{2}$ になります。同様に、$p = \frac{1}{2}$ です。混合戦略 $(\frac{1}{2}\mathbf{1} + \frac{1}{2}\sigma_z, \frac{1}{2}\mathbf{1} + \frac{1}{2}\sigma_z$ は $(\frac{\alpha+\beta}{2}, \frac{\alpha+\beta}{2})$ のペイオフをもたらします。 ついにボブとアリスの平等！ このナッシュ均衡は、(α, β) または (β, α) のいずれかによって共同で支配されていないため、パレート最適でもあります。

14　Newcomb’s Game: a game against a Superior Being:Newcomb のゲーム: 優れた存在との戦い

アリスは、優れた存在（Superior Being: SB）に対して次のゲームをプレイします。 SB は、神、別の惑星からの優れた知性、またはアリスの思考プロセスを予測するのに非常に優れたスーパーコンピューターと考えることができます (参考文献 4)。ボックス B_1 と B_2 が 2 つあります。 B_1 には 1000 ドルが含まれています。 B_2 には、SB がボックスに入れた金額に応じて、1,000,000 ドルまたは 0 ドルのいずれかが含まれます。 アリスは、両方のボックスを使用するか、B2 のみを使用するかを選択できます。

SB がアリスが両方のボックスを選択すると予測した場合、SB は B_2 に 0 ドルを入れ、SB がアリスがボックス B_2 のみを受け取ると予測した場合、SB は B_2 に 1,000,000 ドルを入れます。

ゲームは表 11 に示されています。 2 行目の各ペイオフは、1 行目の対応するペイオフよりも大きいため、アリスには明らかに支配的な戦略があります。これは、両方のボックスを使用することです。

一方、支配戦略は期待効用理論と矛盾します（ここでは効用はペイオフで線形であると見なされます)。

SB の予測精度が p であると仮定します。 次に、期待効用理論によれば、アリスは両方のボック

表 11　Newcomb のゲーム

	SB predicts Alice will take only box B_2	SB predicts Alice will take both boxes
Alice takes only box B_2	1,000,000 ドル	0 ドル
Alice takes both boxes	1,001,000 ドル	1,000 ドル

スを使用するか、B_2 のみを使用するかを区別しません。

$$p\ \$1,000,000 + (1\ -\ p)\ \$0 = (1\ -\ p)\ \$1,001,000 + p\ \$1000. \tag{163}$$

$p > .5005$ の場合、アリスはボックス B_2 のみを使用する戦略を好み、支配戦略と矛盾します。このジレンマを解決するにはさまざまな方法があります（参考文献４）。たとえば、SB が全知である場合 ($p = 1$)、テーブルには 1000 ドルと 1,000,000 ドルの 2 つのエントリしかありません。したがって、オートマトンのアリスは SB が予測したものを選択し、パラドックスは解決されます。

しかし、ここでは量子ゲームに興味があります（参考文献 58)。SB は、宇宙が古典物理学ではなく、量子物理学に基づいていることを確かに知っています。古典物理学は、高さが約 2 メートルの存在の偏った見方にすぎません。量子ニューコムのゲームはヒルベルト空間 $\mathbf{H}_1 \otimes \mathbf{H}_2$ で行われ、これを 2 キュービット空間とします。左キュービットはアリスのアクションを示し、右キュービットは SB のアクションを示します。SB の場合、$|0\rangle$ はボックス B_2 への 1,000,000 ドルの配置を表し、$|1\rangle$ は B_2 への 0 ドルの配置を表します。 アリスの場合、$|0\rangle$ は B_2 のみを取得することを表し、$|1\rangle$ は両方のボックスを取得することを表します。$\mathbf{H}_1 \otimes \mathbf{H}_2$ の基底ベクトルは $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ であり、表 11 のペイオフ状態に対応します。

ゲームの初期状態は、SB がボックス B_2 に 1,000,000 ドルを入れた場合は $\Lambda = |00\rangle$、SB が B_2 に何も入れなかった場合は $\Lambda = |11\rangle$ です。 ゲームの流れは以下の通りです。

ステップ 1：SB は、$|0\rangle$ または $|1\rangle$ の選択を行います。 一度行うと、この選択を変更することはできません。

ステップ 2：SB は、アダマール行列 H をアリスのキュービットに適用します。 つまり、演算子 $H \otimes \mathbf{1}$ から初期状態 Λ になります。

ステップ 3：アリスは、確率 w のスピンフリップ演算子 $\sigma_x \otimes \mathbf{1}$ または確率 $1\ -\ w$ の単位行列 $\mathbf{1} \otimes \mathbf{1}$ をゲームの現在の状態に適用します。 （これらは彼女自身のキュービットでのみ動作します。）

ステップ 4：SB は $H \otimes \mathbf{1}$ をゲームの現在の状態に適用し、アリスへのペイオフが決定されます。

SB が $|0\rangle$ を選択した場合、ゲームの手順の順序は次のようになります。

$$(H \otimes \mathbf{1})\,|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{164}$$

$$w(\sigma_x \otimes \mathbf{1})(H \otimes \mathbf{1})\,|00\rangle \to \frac{w}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{165}$$

$$\Rightarrow (w(\sigma_x \otimes \mathbf{1}) + (1-w)(\mathbf{1} \otimes \mathbf{1}))(H \otimes \mathbf{1}) |00\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{166}$$

$$(H \otimes \mathbf{1})(w(\sigma_x \otimes \mathbf{1}))(1-w)(\mathbf{1} \otimes \mathbf{1}))(H \otimes \mathbf{1}) |00\rangle \rightarrow |00\rangle . \tag{167}$$

したがって、アリスはボックス B_0 のみを受け取り、1,000,000 ドルを受け取ります。 SB はアリスの動きを正しく予測しました。

SB が $|1\rangle$ を選択した場合、ゲームの手順の順序は次のようになります。

$$(H \otimes \mathbf{1}) |11\rangle \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \tag{168}$$

$$w(\sigma_x \otimes \mathbf{1})(H \otimes \mathbf{1}) |11\rangle \rightarrow \frac{w}{\sqrt{2}}(|11\rangle - |01\rangle) \tag{169}$$

$$\Rightarrow (w(\sigma_x \otimes \mathbf{1}) + (1-w)(\mathbf{1} \otimes \mathbf{1}))(H \otimes \mathbf{1}) |11\rangle \rightarrow \frac{1-2w}{\sqrt{2}}(|01\rangle - |11\rangle) \tag{170}$$

$$(H \otimes \mathbf{1})(w(\sigma_x \otimes \mathbf{1}))(1-w)(\mathbf{1} \otimes \mathbf{1}))(H \otimes \mathbf{1}) |11\rangle \rightarrow (1-2w) |11\rangle . \tag{171}$$

最終的な値は、$w = 0$ のときに最大になります。したがって、アリスは両方のボックスを受け取り、1,000 ドルを受け取ります。 SB は再びアリスの動きを完全に予測しました。 SB は、この結果を達成するためにオミサイエンスを必要とせず、量子力学の知識のみを必要としました。 ゲームの初期状態にアダマール行列（量子フーリエ変換）を適用することにより、SB はアリスに SB の予測を確認するような振る舞いをさせるように誘導しました。

15 Evolutionarily stable strategy game: 進化的に安定した戦略ゲーム

量子ゲームは私たちの周りで分子レベルで毎日行われているようです。 Gogonea と Merz（参考文献 26）は、タンパク質の折り畳みにおいて量子力学的レベルでゲームが行われていることを示しています。 ターナーとチャオ（参考文献 67）は、RNA ファージ内のウイルス間の競合的相互作用の進化を研究し、ファージの適応度が 2 人の囚人のジレンマゲームに準拠したペイオフマトリックスを生成することを発見しました。 生物学のゲーム理論の側面について簡単に触れたいと思います。

ナッシュ均衡の概念に関連して以前に定義した進化的安定戦略（ESS）の概念は、集団生物学のいくつかの問題に対処するためにゲーム理論（参考文献 64）に導入され、複数のナッシュ均衡が存在する可能性があります。進化論とゲーム理論（参考文献 44）で、メイナードスミスは、「ゲーム理論は、それが最初に設計された経済行動の分野よりも生物学に容易に適用される」と述べた。

対称的なバイマトリックス（つまり、2 × 2）ゲームをプレイするために、ペアでランダムに一致する N 人のメンバーの母集団を考えてみます。

対称とは、次のことを意味します。 S をプレーヤーの動きのセットとし、s_i、s_j をアリスとボブの両方が利用できる動きとします。

次に、彼女が s_i をプレイしてボブが s_j をプレイしたときのアリスの期待されるペイオフは、ボブが s_i をプレイしてアリスが s_j をプレイした場合のボブの期待されるペイオフと同じです。

$$\bar{\pi}_A(s_i, s_j) = \bar{\pi}_B(s_j, s_i) \tag{172}$$

つまり、アリスのペイオフマトリックス Π_A は、ボブのペイオフマトリックスの転置です：$\Pi_A = \quad \Pi_B^T$。 これは、ゲームの対称性を定義します。 時間の経過とともに高いペイオフで s_i が移動すると、ゲームは進化的になり、徐々にそれらの s_j を低いペイオフに置き換えます。 そのようなゲームで、メイナード・スミスとプライス（参考文献 43）は、ESS を採用する集団が小さな侵入グループに耐えることができることを示しました。

しかし、古典的な動きをしている間に平衡状態にある現在の人口が、量子の動きをしている人口によって侵略された場合はどうなるでしょうか？ これは Iqbal と Toor によって検討された問題です（参考文献 33)。対称バイマトリックスゲームでムーブ s_i をプレイする母集団の割合が p_i であり、ムーブ s_j をプレイする割合が p_j であると仮定します。 動き s_i と s_j の適合度 w を次のように定義します。

$$w(s_i) = p_i\bar{\pi}(s_i, s_j) + p_j\bar{\pi}(s_i, s_j) \tag{173}$$

$$w(s_j) = p_i\bar{\pi}(s_j, s_i) + p_j\bar{\pi}(s_j, s_j) \tag{174}$$

最初の方程式は、$move\ s_i$ の適合性は、s_i をプレイしている対戦相手に対して s_i をプレイした場合のペイオフと、s_j をプレイしている対戦相手に対して s_i をプレイした場合のペイオフの加重平均であることを示しています。 それぞれの重みは、s_i と s_j をプレイしている母集団の比率です。2 番目の式は、インデックスが切り替えられた最初の式と実際には同じです。

量子進化的に安定した戦略ゲームでは、2 つの集団グループ間でプレイされる対称バイマトリックスゲームが囚人のジレンマゲームであると想定します。 このゲームのペイオフマトリックスは、前に表 VI に示したものです。 一方のプレーヤーのペイオフマトリックスは、もう一方のプレーヤーのペイオフマトリックスの転置であり、対称性に必要であることに注意してください。量子囚人のジレンマゲームで使用されるユニタリ行列 $U = \frac{1}{\sqrt{2}}(\mathbf{1}^{\otimes 2} + i\sigma_x^{\otimes 2})$ も 2 人のプレーヤー間で対称であることに注意してください。

古典的な動きの場合、ペイオフ状態 $sA, sB = D, D$ および $\pi(s_A), \pi(s_B) = 1, 1$ は、ナッシュ均衡であり、進化的に安定した戦略でもあります。 ただし、量子運動を行う変異体の侵入力の影響を考慮してください。

参照しやすいように、ここでは表 VIII を表 XII として再現します。 $\mathbf{1}, \sigma_x$ を古典としてラベル付けします。移動し、ミュータントが移動すると H, σ_z になります。

表 12　1 の古典的な動きをしている集団、σ_x は、量子の動き H をしている突然変異体によって侵略されています。 後の変異体の侵入は σ_z を再生し、前の変異体を一掃します。

	Classical $\mathbf{1}$	Classical σ_x	Mutant H	Mutant σ_z
Classical $\mathbf{1}$	$(3,3)$	$(0,5)$	$(\frac{1}{2},3)$	$(1,1)$
Classical σ_x	$(5,0)$	$(1,1)$	$(\frac{1}{2},3)$	$(0,5)$
Mutant H	$(3,\frac{1}{2})$	$(3,\frac{1}{2})$	$(2\frac{1}{4},2\frac{2}{4})$	$(1\frac{1}{2},4)$
Mutant σ_z	$(1,1)$	$(5,0)$	$(4,1\frac{1}{2})$	$(3,3)$

σ_x は H に対して進化的に安定していないことがわかります。σ_x をプレイしているメンバーは消滅し、人口はまもなく H をプレイしている変異体で構成されます。新しい ESS は、どちらかのミュータントパーティに $2\frac{1}{4}$ のペイオフをもたらします。この新しい集団が σ_z を再生するさまざまな変異体によって侵略された場合、H はもはや ESS ではありません。H をプレイしているメンバーは消滅し、人口はまもなく σ_z をプレイしているミュータントで構成されます。これらの変異体は 3 の見返りを享受し、元の集団と比較すると肥えて幸せに見えます。

16　Card game:　a quantum game without entanglement　カードゲーム：エンタングルメントのない量子ゲーム

次のゲームはエンタングルメントを使用していませんが、数学的な設定ではヒューリスティックであり、後続のより複雑なゲームの準備として適しています。 ボブとアリスは次のカードゲームをプレイします (参考文献 17)。次のマークを除いて、3 枚のカードがあります。それ以外は同じです。最初のカードの両側に円があります。 2 枚目のカードには両側にドットがあります。 3 枚目のカードは片面に円、もう片面にドットがあります。 アリスは 3 枚のカードをブラックボックスに入れ、それを振って 3 枚のカードをランダム化します。ボブは箱から盲目的に 1 枚のカードを引くことができます。 両側に同じマークがある場合、アリスはボブから+1 を獲得します。 カードの両面に異なるマークが付いている場合、ボブはアリスから+1 を獲得します。もちろん、両側に同じマークが付いている 2 枚のカードであるアリスはペイオフ $\bar{\pi}_A = \frac{2}{3}(1) + \frac{1}{3}(-1) = \frac{1}{3}$ を期待し、ボブはペイオフ $\bar{pi}_B = \frac{1}{3}(1) + \frac{2}{3}(-1) = -\frac{1}{3}$ を期待しています 。 ゲームはボブにとって不公平です。

古典的な意味でゲームを公平にする 1 つの方法は、ボブがブラックボックスを見て、3 枚のカードの 1 枚を引く前に上面を見ることができるようにすることです。次に、ボブが 3 枚のカードの中で 2 つの円が上を向いているのを見た場合、彼はそれら 2 つのカードの 1 つをランダムに描きます。一方、2 つのドットが上を向いているのを見た場合、彼は後者の 2 つのカードの 1 つをめったに描きません。同じ上向きのマークが付いた 2 枚のカードの 1 つは、それぞれの面に異なるマークがなければならないので、これはボブに期待されるペイオフ $\pi_B = 0$ を与えます。ゲームは今や公平になるでしょう。 ただし、ボブにこれを行わせるつもりはありません。 実際、それは彼が中を

見ることができないようにブラックボックスですが、彼は手を差し込んで 1 枚のカードを引き出すことができます。

代わりに、3 つのカードすべての上面を見るのと同等の量子を作成するために、1）ボブがブラックボックスまたはキュービットデータベースに単一のクエリを実行できるようにします $|r\rangle$; そして、2）ボブが引いたカードの上面を見て、ゲームから撤退できるようにします。この設定は非常に人工的であり、同じゲームについて説明していることすら疑わしいですが、この量子化されたバージョンのカードゲームでは、いくつかのヒューリスティックなポイントを作成できます。

$$|r\rangle = |r_0 r_1 r_2\rangle \tag{175}$$

ここで、$r_k \in \{0, 1\}$ です。

ボブのクエリの一部として、次のユニタリ行列 U_k が必要になります。

$$U_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi r_k} \end{pmatrix}. \tag{176}$$

$rk = 0$ の場合、$U_k = \mathbf{1}$ であり、$r_k = 1$ の場合、$U_k = \sigma_z$ であることに注意してください。 ここで、アダマール行列 H を U_k に適用して、HU_kH を形成し、次の式を取得します。

$$HU_kH = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi r_k} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi r_k} & 1-e^{i\pi r_k} \\ 1-e^{i\pi r_k} & 1+e^{i\pi r_k} \end{pmatrix}. \tag{177}$$

したがって、この変換を状態—0⟩に適用すると、次のようになります。

$$HU_kH\,|0\rangle = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi r_k} & 1-e^{i\pi r_k} \\ 1-e^{i\pi r_k} & 1+e^{i\pi r_k} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi r_k} \\ 1-e^{i\pi r_k} \end{pmatrix} = \frac{1+e^{i\pi r_k}}{2}\,|0\rangle + \frac{1-e^{i\pi r_k}}{2}\,|1\rangle\,. \tag{178}$$

$rk = 0$ の場合、$HU_kH\,|0\rangle = |0\rangle$ であるのに対し、$r_k = 1$ の場合、$HU_kH\,|0\rangle = |1\rangle$ であることに注意してください。 したがって、

$$HU_kH\,|0\rangle = |r_k\rangle\,. \tag{179}$$

それでは、ボブがブラックボックスの状態 $|r\rangle$ に依存するクエリマシンを持っていると仮定しましょう。 マシンには 3 つの入力があり、3 つの出力を提供します。 3 枚のカードのアップサイドマークを決定するために、ボブは $|000\rangle$ を入力して以下を取得します。

$$(HU_kH \otimes HU_kH \otimes HU_kH)\,|000\rangle = |r_0 r_1 r_2\rangle\,. \tag{180}$$

したがって、ボブの質問の後、彼は 3 枚のカードの逆さまのマークを知っています。セット $S0 = \{3 - qubits$ の順列 $\{|0\rangle, |0\rangle, |1\rangle\}\}$ のある要素またはセット $S1 = \{3 - qubits$ の順列 $\{|0\rangle, |1\rangle, |1\rangle\}\}$ のある要素のいずれかです。

S_0 がブラックボックスの状態を説明している場合、ボブは勝ったカードの表側に円があることを知っています。S_1 がブラックボックスの状態を表す場合、ボブは勝ったカードが上向きの面にドットを持っていることを知っています。だから今、ボブは自分のカードを引き、表向きの顔だけを見るようになります。 描かれたカードの表側に円があり、$black\ box \in S_0$ の場合、ボブは同じ確率で勝ちます。しかし、$black\ box \in S_1$ の場合、ボブは、引いたカードが負けたカードであることを知っているため、プレーを拒否します。描かれたカードの表側にドットがある場合も同様の分析が当てはまります。

したがって、データベースへのクエリは、ブラックボックスに表向きに表示されている 2 つの円または 2 つのドットがあるかどうかをボブに示します。したがって、彼がカードを引くと、2 つの逆さまのマークと一致する場合、50-50 のチャンスがあることがわかります。 引き分けたカードが 2 つの上向きのマークと一致しない場合、そのカードは間違いなく敗者であり、彼はゲームから撤退するオプションを行使する必要があります。

エンタングルメントに関しては、演算子 H と U_k はキュービットの単純な線形結合を形成しますが、量子クエリマシンはこれらの演算のテンソル積です。したがって、このゲームには状態の絡み合いはありません。Du et. al によれば、一般的なルールは、静的量子ゲームでは古典的な結果との違いを生み出すためにエンタングルメントが必要であるように見えるが、動的ゲームではそうではないことに注意すると記述しています。重要なのは、他のキュービットの状態に影響を与えるプレーヤーの能力です。これは、エンタングルメントまたは動的ゲームのタイムステップを通じて実行できます。

17 Quantum teleportation and pseudo-telepathy 量子テレポーテーションと疑似テレパシー

アリスとボブは 7 光年離れており、絡み合った量子ビットのペアを共有しています。たとえば、$|b_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ です。　アリスが自分のキュービットを測定し、それが状態 $|0\rangle$ にあることを検出した場合、ボブのキュービットも状態 $|0\rangle$ にあることが保証されます。 アリスが測定によって彼女のキュービットが状態 $|1\rangle$ にあることを検出した場合、ボブのキュービットも状態 $|1\rangle$ に検出されます。 つまり、アリスの測定値はボブのキュービットの状態に影響を与えます。 私たちが知る限り、ボーアチャネルを介したこの影響の伝達は瞬時に行われます。 距離の影響を受けたり、光速の影響を受けたりすることはありません。 遠隔作用で不気味なアクションです。 また、量子テレポーテーションの基礎でもあります。

テレポーテーション対照的に、量子テレポーテーションプロトコル (参考文献 2) は、ボーア（EPR）チャネルだけでなく古典的なチャネルも使用するため、瞬時には実行されません。一方、量子状態はある場所で消え、別の場所で再び現れるため、テレポートされます。 従来のテレポーテーションプロトコルはこのように機能します。アリスは未知の量子状態を持っています $|\psi\rangle$ 彼女

はボブに送信したいと思っています。 彼女はこれを 2 つの部分で行います。エンタングルされたボーアチャネルと、いくつかのクラシックビットを送信するための追加のクラシックチャネルを使用します。アリスとボブは、絡み合った粒子のペアを共有するために以前の取り決めをしました。今回はベル状態で $|b_3\rangle$：

$$|b_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{181}$$

アリスが送信しようとしている未知の状態は、未知の振幅 $a, b, |a|^2 + |b|^2 = 1$ で記述できます。

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,. \tag{182}$$

3 量子ビットシステムの初期状態を次のように書くことができます。

$$|\psi\rangle \otimes |b_3\rangle = (a\,|0\rangle + b\,|1\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{183}$$

$$= \frac{a}{\sqrt{2}}\,|001\rangle - \frac{a}{\sqrt{2}}\,|010\rangle + \frac{b}{\sqrt{2}}\,|101\rangle - \frac{b}{\sqrt{2}}\,|110\rangle\,. \tag{184}$$

明らかになる理由から、この状態をベル基底の観点から書き直したいと思います。 これを行うには、各ベル状態の乗数を見つけるために、$|psi\rangle \otimes |b_3\rangle$ と各ベルベクトルの内積を取ります。 式（184）の左端の 2 つのキュービットを持つ内積をとることに注意してください。 これらのキュービットはアリスの管理下にあります。

$$\langle b_0|(|\psi\rangle \otimes |b_3\rangle)\rangle = +\frac{a}{\sqrt{2}}\,|1\rangle - \frac{b}{\sqrt{2}}\,|0\rangle \tag{185}$$

$$\langle b_1|(|\psi\rangle \otimes |b_3\rangle)\rangle = -\frac{a}{\sqrt{2}}\,|1\rangle + \frac{b}{\sqrt{2}}\,|1\rangle \tag{186}$$

$$\langle b_2|(|\psi\rangle \otimes |b_3\rangle)\rangle = +\frac{a}{\sqrt{2}}\,|1\rangle + \frac{b}{\sqrt{2}}\,|1\rangle \tag{187}$$

$$\langle b_3|(|\psi\rangle \otimes |b_3\rangle)\rangle = -\frac{a}{\sqrt{2}}\,|0\rangle - \frac{b}{\sqrt{2}}\,|1\rangle\,. \tag{188}$$

これらの残差状態乗数を使用して、ベル基底の観点から状態 $|psi\rangle \otimes |b_3\rangle$ を書くことができます。

$$|\psi\rangle \otimes |b_3\rangle = \frac{1}{\sqrt{2}}[\begin{pmatrix} -b \\ +a \end{pmatrix}|b_0\rangle + \frac{1}{\sqrt{2}}\begin{pmatrix} -a \\ +a \end{pmatrix}|b_1\rangle + \frac{1}{\sqrt{2}}\begin{pmatrix} +b \\ +a \end{pmatrix}|b_2\rangle + \frac{1}{\sqrt{2}}\begin{pmatrix} -a \\ -b \end{pmatrix}|b_3\rangle]. \tag{189}$$

次に、最後の方程式を 2×2 行列で書き直してみましょう。

$$|\psi\rangle \otimes |b_3\rangle = \frac{1}{\sqrt{2}}[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} |b_0\rangle + \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} |b_1\rangle + \tag{190}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} |b_2\rangle + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} |b_3\rangle]. \tag{191}$$

これをパウリスピン行列の観点からもう一度書き直すことができます。

$$|\psi\rangle \otimes |b_3\rangle = \frac{1}{\sqrt{2}}[-i\sigma_y \begin{pmatrix} a \\ b \end{pmatrix} |b_0\rangle - \sigma_z \begin{pmatrix} a \\ b \end{pmatrix} |b_1\rangle + \sigma_x \begin{pmatrix} a \\ b \end{pmatrix} |b_2\rangle - \mathbf{1} \begin{pmatrix} a \\ b \end{pmatrix} |b_3\rangle]. \tag{192}$$

さて、彼女のキュービットをボブにテレポートするには、アリスは未知の状態 $|\psi\rangle$ を絡み合ったキュービットペアのメンバーと結合する必要があります。これを行うために、彼女はこれら 2 つのキュービットのジョイント（フォンノイマン）測定を行います。これは、$|\psi\rangle \otimes |b_3\rangle$ の左端の 2 つのキュービットを構成します。アリスの測定は、彼女の 2 つのキュービットを 4 つのベル状態の 1 つに投影します。 これにより、未知の状態 $|\psi\rangle$ が破壊されます。しかし、心配しないでください。アリスの測定では、ボブのキュービットも次の 4 つの状態のいずれかになります。

$$|\psi\rangle \otimes |b_3\rangle \to |b_0\rangle \longrightarrow Bob's\ qubit = -i\sigma_y \begin{pmatrix} a \\ b \end{pmatrix} \tag{193}$$

$$|\psi\rangle \otimes |b_3\rangle \to |b_1\rangle \longrightarrow Bob's\ qubit = -\sigma_z \begin{pmatrix} a \\ b \end{pmatrix} \tag{194}$$

$$|\psi\rangle \otimes |b_3\rangle \to |b_2\rangle \longrightarrow Bob's\ qubit = -\sigma_x \begin{pmatrix} a \\ b \end{pmatrix} \tag{195}$$

$$|\psi\rangle \otimes |b_3\rangle \to |b_3\rangle \longrightarrow Bob's\ qubit = -\mathbf{1} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{196}$$

次に、アリスは古典的なチャネルを介して、測定結果、つまり彼女が取得したベル状態をボブに送信します。それから、ボブは対応するスピン演算子（それ自体の逆）をキュービットに適用して、状態 $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} : i\sigma_y\ for\ |b_0\rangle, -\sigma_z\ for\ |b_1\rangle, \sigma_x\ for\ |b_2\rangle, -\mathbf{1}\ for\ |b_3\rangle$ を回復します。（実際には、$-|\psi\rangle$ は $|\psi\rangle$ と同じ状態であるため、全体的な符号 [a と b の両方を等しく乗算する符号] は重要ではありません。たとえば、$|\sigma_z\rangle$ または $\mathbf{1}$ を乗算するだけで十分です。）

要約すると、アリスとボブは 2 つのキュービットのもつれ状態 $|\theta\rangle$ を共有します。 アリスは未知の状態 $|\psi\rangle$ をボブにテレポートしたいと思っています。 これを行うために、彼女は最初に 2 つの

キュービットに基づいてベル基底で $|\psi\rangle \otimes |\theta\rangle$ の測定を実行します。（未知の状態、および絡み合った状態の彼女のキュービット）彼女は、取得したベル状態の情報をボブに送信します。 ボブは対応するパウリスピン演算子を彼のキュービットに適用し、未知の状態 $|\psi\rangle$ を回復します。

Pseudo − telepathy 疑似-テレパシー「エンタングルメントは、おそらく量子力学の最も非古典的な兆候です。 情報処理への多くの興味深いアプリケーションの中で、それを利用して、さまざまな分散計算タスクを処理するために必要な通信の量を減らすことができます。 コミュニケーションを完全になくすために使用できますか？ リモートパーティ間で情報を通知することはできませんが、パーティが事前の絡み合いを共有していれば、通信を必要とせずに実行できる分散タスクがあります。これは疑似テレパシーの領域です。」（参考文献５）

N 人のプレイヤー間の次の疑似テレパシーゲーム Γ_N を考えてみましょう。 2 人以上のプレーヤーがいるため、それらをアリスとボブと呼ぶことはできません。そのため、すべてのプレーヤーを下付き文字のアリス：$A_1, A_2, \cdots, A_N$ とします。 また、2 つの関数 f と g があり、それぞれが N キュービット入力を受け取ります。 ゲームには次の手順があります。

ステップ 1：プレイヤーは交わり、戦略について話し合い、確率変数（古典的な設定）またはエンタングルメント（量子設定）を共有します。

ステップ 2：プレーヤーは分離し、いかなる形式のコミュニケーションにも関与することは許可されていません。 各プレーヤー A_i には、単一の量子ビット入力 x_i が与えられ、単一の量子ビット出力 y_i を生成するように要求されます。 次の場合、プレイヤーは $+1$ を獲得します

$$f(x_1, x_2, \cdots, x_N) = g(y_1, y_2, \cdots, y_N). \tag{197}$$

そうでなければ、彼らはこの金額を失います。 関数 f と g は次のように定義されます。 プレイヤーは、与えられたキュービットの合計が偶数であることが保証されます。$\sum_i x_i$ は偶数です。（これが何を意味するかを考えてください。$\sum_i x_i$ が偶数の場合、2 で割り切れます。したがって、$\frac{1}{2}\sum_i x_i$ は、奇数または偶数の整数です。奇数の場合、$\frac{1}{2}\sum_i x_i \mod 2 = 1$ です。偶数の場合、 次に $\frac{1}{2}\sum_i x_i \mod 2 = 0$ です。ただし、後者の場合は、$\frac{1}{2}\sum_i x_i \mod 2$ も 2 で割り切れるので、元の合計 $\sum_i x_i$ は 4 で割り切れます。）入力ビット $\sum_i x_i$ の合計が 4 で割り切れる場合に限り、プレーヤーは出力ビット $\sum_i y_i$ の偶数の合計を生成するように求められます。したがって、N プレーヤーが勝つための基準は次のとおりです。

$$\sum_i y_i \mod 2 = \frac{1}{2}\sum_i x_i \mod 2. \tag{198}$$

この方程式の左辺は g で、右辺は f です。 各プレーヤーが制御するのは 1 キュービットのみであり、他のプレーヤーとの通信は許可されていませんが、勝利は N キュービットのグローバル状態にのみ依存します。ここで、 mod 2 は 2 つの結果しか生成しないため、プレーヤー i が y_i の送信をランダム化した場合のプレーヤーへの期待されるペイオフは 0 であることに注意してください。これは、プレイヤー間の協力の問題を浮き彫りにし、ゲームが任意の数 N のプレイヤーに拡張可能であるため、非常に優れたゲームです。

さて、驚くべきことは、ステップ 1 のように、プレーヤーが以前のエンタングルメントを共有することを許可されている場合、プレーヤーは常に Γ_N を獲得することです。これをどのように行うかを確認するには、ベル状態 $|b_0\rangle$ と $|b_2\rangle$、アダマール変換 H、およびカードゲームで導入されたユニタリ行列または回転行列をコンポーネントとして必要とします。ただし、ここでは次のように定義します。

$$U_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{199}$$

ここで、$\cos(\frac{\pi}{2}) + i\sin(\frac{\pi}{2}) = i$ であることを思い出してください。$U_{\frac{\pi}{2}}|0\rangle = |0\rangle$ ですが、$U_{\frac{\pi}{2}}|1\rangle = |1\rangle$ であることに注意してください。

N 人のプレイヤーが絡み合ったベル状態を共有するため、後者は N-キュービットのベル状態である必要があります。 N-キュービットのベル状態を次の簡略化された形式で記述しましょう。

$$|b_0^N\rangle = \frac{1}{\sqrt{2}}(|0^N\rangle + |1^N\rangle) \tag{200}$$

$$|b_2^N\rangle = \frac{1}{\sqrt{2}}(|0^N\rangle - |1^N\rangle). \tag{201}$$

最初の N キュービット状態 $|b_0^N\rangle$ は、すべてのプレーヤーが共有することに同意するエンタングル状態です。 2 番目の状態は、プレイの過程で進化する可能性があります。

ここで、$|b_0^N\rangle$ の単一キュービットで動作するユニタリ行列の効果を考えてみましょう。

$$U_{\frac{\pi}{2}}|b_2^N\rangle = \frac{1}{\sqrt{2}}(|0^N\rangle + i|1^N\rangle). \tag{202}$$

i の累乗は $i, i^2 = -1, i^3 = -i, i^4 = 1$ です。 したがって、$U_{\frac{\pi}{2}}$ が 2 つのキュービットに適用される場合、$|1^N\rangle$ の符号は -1 になり、したがって $|b_0^N\rangle \to |b_2^N\rangle$ になります。 4 キュービットに適用した場合、符号は変更されないため、$|b_0^N\rangle \to |b_2^N\rangle$ です。 したがって、m 人のプレーヤーが個々のキュービットに $U_{\frac{\pi}{2}}$ を適用する場合、$m = 0 \mod 4$ の場合、初期状態 $|b_0^N\rangle$ は変更されません。$m = 2 \mod 4$ の場合、$|b_0^N\rangle \to |b_2^N\rangle$ です。

エンタングル状態が $|b_0^N\rangle$ のときに各プレーヤーがアダマール行列をキュービットに適用すると、結果は 1 ビットの偶数であるすべての状態の重ね合わせになります。

$$(\mathbf{H}^{\otimes N})|b_2^N\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_{even\ bit\ y}^{2^{N-1}} |y\rangle . \tag{203}$$

これは、合計の状態 $|y\rangle$ が偶数であることを意味するものではないことに注意してください。たとえば、$|101\rangle = |5\rangle$ は奇数ですが 1 ビットは偶数ですが、$|100\rangle = |4\rangle$ は偶数ですが 1 ビットは奇数です。N 倍アダマール変換（ウォルシュ変換）がベル状態 $|b_0^N\rangle$ を偶数ビット数（1 ビットの偶数を

意味する）の重ね合わせに変換することを確認するには、表 5 の類似物である表 13 を検討してください。マイナス記号は、奇数の 1 ビットの数値に表示されることに注意してください。

表 13　初期量子ビットを使用したウォルシュ変換 $|111\rangle$

$\|b\rangle$	$\|y\rangle$	$b \cdot y$	$(-1)^{b \cdot y}$
$\|111\rangle$	$\|000\rangle$	0	1
$\|111\rangle$	$\|001\rangle$	1	-1
$\|111\rangle$	$\|010\rangle$	1	-1
$\|111\rangle$	$\|011\rangle$	0	1
$\|111\rangle$	$\|100\rangle$	1	-1
$\|111\rangle$	$\|101\rangle$	0	1
$\|111\rangle$	$\|110\rangle$	0	1
$\|111\rangle$	$\|111\rangle$	1	-1

したがって、$(\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{H})$ を $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ に適用すると、$\frac{2}{\sqrt{2^4}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle + |0\rangle - |1\rangle - |2\rangle + |3\rangle - |4\rangle + |5\rangle + |6\rangle - |7\rangle) = \frac{2}{\sqrt{2^4}}(|0\rangle + |3\rangle + |5\rangle + |6\rangle)$ が得られます。これは、すべてが 1 ビットの偶数である数値の重ね合わせです。

プレーヤーのアクションによって状態が状態 $|b_0^N\rangle$ に進化し、各プレーヤーがアダマール行列を自分のキュービットに適用すると、結果はすべての奇数ビット状態（奇数の 1 ビットの状態を意味する）の重ね合わせになります。

$$(\mathbf{H}\otimes^N)\,|b_2^N\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_{odd\ \ bit\ \ y}^{2^{N-1}} |y\rangle\,. \tag{204}$$

それで、ここに、ゲーム Γ_N での彼または彼女のキュービットに関して各プレーヤーがとるステップがあります：

プレーヤーのステップ $2a$：プレーヤーがキュービット $x_i = 1$ を受け取った場合、プレーヤーは絡み合ったベル状態 $|b_0^N\rangle$ で自分のキュービットに $u_{\frac{\pi}{2}}$ を適用します。それ以外の場合、プレーヤーは何もしません。 結果：ビット $\sum_i x_i$ の合計が偶数であるため、偶数のプレーヤーがこのステップを実行します。$\sum_i x_i$ が 4 で割り切れる場合、ベル状態 $|B_0^N\rangle$ は変更されません。しかし、$\sum_i x_i \bmod 4$ の場合、$|b_0^n\rangle \to |b_2^N\rangle$ です。プレーヤーステップ $2b$：各プレーヤーはアダマール行列 H を自分のキュービットに適用します。結果：エンタングル状態がまだステップ $2a$ の状態 $|b_0^n\rangle$ にある場合、この現在のステップはエンタングル状態をすべての偶数ビット状態の重ね合わせに変換します。しかし、エンタングル状態が $|b_2^n\rangle$ に変換されている場合、このステップはエンタングル状態をすべての奇数ビット状態の重ね合わせに変換します。

プレーヤーのステップ $2c$：各プレーヤーは、計算ベース（$|0\rangle$ 対 $|1\rangle$）で自分のキュービットを測定して、y_i を生成します。

$\sum_i x_i$ が 4 で割り切れる場合、絡み合ったキュービットは偶数ビット状態の重ね合わせであるため、測定の下で偶数 1 ビットの数に投影されます。$\sum_i y_i \mod 2 = 0$ であるため、プレーヤーが勝ちます。$\sum_i x_i = 2 \mod 4$ の場合、絡み合ったキュービットは奇数ビット状態の重ね合わせになります。そのため、測定の下で 1 ビットの奇数の数値に投影されます。$\sum_i y_i mod 2 = 1$ であるため、プレイヤーは再び勝ちます。

プレイヤー間のコミュニケーションがなかったとしても、プレイヤーはお互いが何をしているのかを知っているかのように振る舞うことで、疑似テレパシーを示しました。これは、量子見えざる手として機能する共有エンタングル状態 b_0^N によって可能になりました。

この疑似テレパシーゲームは、従来の N 人ゲーム理論の観点から次のように特徴付けることができます。 プレイヤーは自分で値を確保できないため、1 人の連立 $\{i\}$ の値は 0： $\nu\{i\} = 0$ です。すべてのプレイヤーの連立の値は 1： $\nu(N) = 1$ です。 ゲームは $(0, 1)$-正規化にあると言われます。 S をプレーヤー N のセットのサブセットとします。すべての $S \subset N$ について、$\nu(S) = 0$ または $\nu(S) = 1$ の場合、ゲームは単純であると言われます。したがって、疑似テレパシーゲームも単純です。 実際、すべての S に対して $\nu(S) = 0$ であり、$S = N$ を除きます。最後に、$\nu(S) + \nu(N - S) = \nu(N)$ の場合、ゲームは一定の合計であると言われます。疑似テレパシーゲームは、$S \neq N$ に対して $\nu(S) + \nu(N - S) = 0$ であるため、一定の合計ではありませんが、$\nu(N) = 1$ です。

このゲームの帰属のセットは、確率ベクトルのセット $P = \{p1, p2, \cdots, p_N\}$ です。これは、すべての $i \in N$ について、$\sum_{i \in N} p_i = \nu(N) = 1$ であるという要件と、$p_i \geq v(\{i\}) = 0$ であるという要件を満たします。$S \subset N$ の場合、これらの割り当てベクトルはいずれも別の割り当てベクトルによって支配されません。したがって、このゲームのコアは、確率ベクトル P の凸集合です。

18 Quantum secret sharing 量子秘密共有

IRA には、メンバー間で保存したい秘密情報がいくつかありますが、一部は MI5 の情報提供者であり、他の人は逮捕され、尋問の下で知っていることを明らかにする可能性があることを恐れています。したがって、彼らは彼ら自身の間に秘密を埋め込むための安全な方法を必要としています。(k, n) しきい値スキーム (参考文献 11) は、$k \leq n$ のメンバーはシークレットを再構築できますが、$k - 1$ のメンバーはシークレットに関する情報をまったく見つけることができないスキームです。

ただし、最初に、秘密の量子状態を発見するために 2 つのパーティが協力しなければならない簡単な例を考えてみましょう（参考文献 31)。 アリス、ボブ、ジェラルドは次のもつれ状態を共有しています（左のキュービットはアリス、右のキュービットはジェラルドです)。

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle). \tag{205}$$

最初に、これを別の基準で書き直すことができることに注意してください。 させて

$$|x^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{206}$$

$$|x^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{207}$$

これは相互関係を意味します

$$|0\rangle = \frac{1}{\sqrt{2}}(|x^+\rangle + |x^-\rangle) \tag{208}$$

$$|1\rangle = \frac{1}{\sqrt{2}}(|x^+\rangle - |x^-\rangle). \tag{209}$$

したがって、新しい基準に関する元の状態は次のようになります。

$$|\psi\rangle = \frac{1}{2\sqrt{2}}[(|x^+x^+\rangle + |x^-x^-\rangle)(|0\rangle + |1\rangle) + (|x^+x^-\rangle + |x^-x^+\rangle)(|0\rangle - |1\rangle)]. \tag{210}$$

アリスは、ボブとジェラルドが秘密を学ぶために協力しなければならないような方法で、秘密のキュービット $|\phi_{secret}\rangle\, a\,|0\rangle - b\,|1\rangle$ をボブとジェラルドに送りたいと思っています。彼女は基本的にテレポーテーションプロトコルを介してこれを行いますが、手順の一部として $(|x^+\rangle, |x^-\rangle)$ の定義も必要になります。 アリスは秘密量子ビット $|\phi_{secret}\rangle$ と共有状態 $|\psi\rangle$ を組み合わせて全体的な状態を形成します

$$|\phi_{secret}\rangle \otimes |\psi\rangle = \frac{1}{\sqrt{2}}(a\,|0000\rangle + b\,|1000\rangle + a\,|0111\rangle + b\,|1111\rangle). \tag{211}$$

アリスはこれをベル基底の観点から書き直しました。 ベル状態の乗数は次のとおりです。

$$\langle b_0|(|\phi_{secret}\rangle \otimes |\psi\rangle)\rangle = \frac{a}{\sqrt{2}}\,|00\rangle + \frac{b}{\sqrt{2}}\,|11\rangle \tag{212}$$

$$\langle b_1|(|\phi_{secret}\rangle \otimes |\psi\rangle)\rangle = \frac{a}{\sqrt{2}}\,|11\rangle + \frac{b}{\sqrt{2}}\,|00\rangle \tag{213}$$

$$\langle b_2|(|\phi_{secret}\rangle \otimes |\psi\rangle)\rangle = \frac{a}{\sqrt{2}}\,|00\rangle - \frac{b}{\sqrt{2}}\,|11\rangle \tag{214}$$

$$\langle b_3|(|\phi_{secret}\rangle \otimes |\psi\rangle)\rangle = \frac{a}{\sqrt{2}}\,|11\rangle - \frac{b}{\sqrt{2}}\,|00\rangle\,. \tag{215}$$

アリスはベル基底で 2 つのキュービットを測定し、その結果をジェラルドに送信し、ボブに $(|x^+\rangle, |x^-\rangle)$ 基底でキュービットを測定するように指示します。 アリスのベルの測定後、ボブとジェラルドのキュービットは次のいずれかの状態になります。

$$|b_0\rangle \to a\,|00\rangle + b\,|00\rangle \tag{216}$$

$$|b_1\rangle \to a\,|11\rangle + b\,|00\rangle \tag{217}$$

$$|b_2\rangle \to a\,|00\rangle - b\,|11\rangle \tag{218}$$

$$|b_3\rangle \to a\,|11\rangle - b\,|00\rangle\,. \tag{219}$$

ボブが測定時に $|x^+\rangle$ を取得した場合、ジェラルドのキュービットは次のようになります。

$$a\,|00\rangle + b\,|11\rangle \to a\,|0\rangle + b\,|1\rangle \tag{220}$$

$$a\,|11\rangle + b\,|00\rangle \to a\,|1\rangle - b\,|0\rangle \tag{221}$$

$$a\,|00\rangle - b\,|11\rangle \to a\,|0\rangle - b\,|1\rangle\,. \tag{222}$$

$$a\,|11\rangle - b\,|00\rangle \to a\,|1\rangle - b\,|0\rangle \tag{223}$$

一方、ボブが ($|x^-\rangle$ を取得すると、ジェラルドのキュービットは次のようになります。

$$a\,|00\rangle + b\,|11\rangle \to a\,|0\rangle - b\,|1\rangle\,. \tag{224}$$

$$a\,|11\rangle + b\,|00\rangle \to a\,|1\rangle + b\,|0\rangle \tag{225}$$

$$a\,|00\rangle - b\,|11\rangle \to a\,|0\rangle + b\,|1\rangle \tag{226}$$

$$a\,|11\rangle - b\,|00\rangle \to a\,|1\rangle - b\,|0\rangle\,. \tag{227}$$

アリスのキュービットを再構築するには、ジェラルドがボブが取得した測定値を知る必要があります。これにより、ジェラルドは適切なパウリスピン行列を最終的なキュービット状態に適用できます。したがって、ジェラルドとボブは一緒にアリスのキュービットを再構築できますが、どちらも単独で再構築することはできません。 ジェラルドの最終状態に適用される適切なパウリスピン行列は次のとおりです。

表 14　ジェラルドの最終的なキュービット状態に適用されるパウリスピン行列

$Bell \setminus Bob$	$(\|x^+\rangle$	$(\|x^-\rangle$
$\|b_0\rangle$	$\mathbf{1}$	σ_z
$\|b_1\rangle$	σ_x	$\sigma_x\sigma_z$
$\|b_2\rangle$	σ_z	$\mathbf{1}$
$\|b_3\rangle$	$\sigma_z\sigma_x$	$-\sigma_x$

量子秘密共有とテレポーテーションの密接な関係を確認したので、少なくとも 1 つの例では、(k, n) しきい値の概念に戻り、$(2, 3)$ しきい値スキームの例を考えてみましょうこのスキームは、任意の 2 つが元の状態を再構築できるように、状態を 3 つのパーティに分割することによって機能します。まず、キュービット (qubit) ではなく、キュートリット (qutrit) である未知の秘密の状態から始めます。キュートリット (qutrit) は、$(|0\rangle, |1\rangle, |2\rangle)$ にまたがる 3 次元ヒルベルト空間で値をとることができる 3 進の「trit」です。キュービットにもう 1 つのディメンションを追加しただけです。 この例では、テンソル積は 3 の累乗で拡張するため、3 つのキュートリットが次元 27 のヒルベルト空間を占めることに注意してください。$\mathbf{H}_{27} = \mathbf{H}_3 \otimes \mathbf{H}_3 \otimes \mathbf{H}_3$

秘密の状態 $|\phi_{secret}\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$. があります。 この 1 キュートリット状態を混合 3 キュートリット状態にマッピングするエンコーディング変換があります。

$$|\phi_{secret}\rangle \to \alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |210\rangle). \quad (228)$$

これで、この混合 3 キュートリット状態をアリス、ボブ、ジェラルドの間で分割できます。 左のキュートリットはアリスに属し、右のキュートリットはジェラルドに属しています。 彼らのキュートリットを考えると、彼らが所有する状態は $|0\rangle, |1\rangle$ および $|2\rangle$ の等しい混合物を持っているので、誰も元の状態について何も知りません。ただし、2 人で秘密の状態 $|\phi_{secret}\rangle$ を再構築できます。 たとえば、アリスとボブは一緒になります。 アリスは自分のキュートリットをボブの modulo 3 に追加し、次にボブは自分の（新しい）キュートリットをアリスに追加します。 その結果は以下の状態です

$$(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)(|00\rangle + |12\rangle + |21\rangle). \quad (229)$$

これを確認するために、α の乗数だけを考えてみましょう。 アリスとボブが集まるとき、彼らは

$$\alpha(|000\rangle + |111\rangle + |222\rangle) + \cdots . \quad (230)$$

アリスのキュートリットをボブの modulo 3 に追加すると、

$$\alpha(|000\rangle + |111\rangle + |222\rangle) + \cdots \to \alpha(|000\rangle + |121\rangle + |212\rangle) + \cdots . \quad (231)$$

次に、ボブの（新しい）キュートリットをアリスのキュートリットに追加します。

$$\alpha(|000\rangle + |121\rangle + |212\rangle) + \cdots \rightarrow \alpha(|000\rangle + |021\rangle + |012\rangle) + \cdots \tag{232}$$

$$= (\alpha\,|0\rangle + \cdots)(|00\rangle + |12\rangle + |21\rangle). \tag{233}$$

アリスのキュートリットは、他のキュートリットから解き放たれた秘密の状態 $|\phi_{secret}\rangle$ と同じになりました。 同様のプロセスによって、ジェラルドとボブは秘密の状態、またはアリスとジェラルドを回復することができます。

19 The density matrix and quantum state estimation：密度行列と量子状態の推定

「量子複製不可能定理」は、次の種類の量子コピー機を禁止しています。コピーは 1 つの量子状態を入力として受け取り、同じ種類の 2 つのシステムを出力します。 量子複製不可能定理は、ニック・ハーバートが 1982 年に Foundations of Physics で公開された超光速通信装置を提案した後にその名前が付けられました (参考文献 30)。 これは広く注目を集め、議論の欠陥がすぐに発見されました：デバイスは量子クローニングを必要とし、量子状態の同一のコピーを生成することに問題がありました。 （さらなる背景は (参考文献 56) にあります。）

しかし、それだけではありません。 単一の測定でそれを行おうとしない限り、実質的に同一のコピーを準備することは問題ありません。 統計的手順により、入力状態を任意の精度で決定できます。 たとえば、未知の状態—ψ⟩の場合、

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{234}$$

計算ベースで n 個のそのような準備された状態を繰り返し測定すると、$|0\rangle\, n_a$ 回と $|1\rangle\, n_b$ 回が得られます。ここで、$n_a + n_b = n$ です。 その後、明らかに

$$\frac{n_a}{n} \simeq |a|^2 = |\,\langle\psi|0\rangle\,|^2 \tag{235}$$

$$\frac{n_b}{n} \simeq |b|^2 = |\,\langle\psi|0\rangle\,|^2. \tag{236}$$

つまり、n 個の測定値は $(x_1, x_2, \cdots, x_n)$ を生成します。ここで、各 x_i は 0 または 1 のいずれかです。これは、尤度関数が

$$L(p) = \prod_{i=1}^{n} p^{x_i} q^{1-x_i} = p^{\sum x_i} q^{n-\sum x_i}. \tag{237}$$

ここで、p は 1 の確率であり、$q = 1 - p$ は 0 の確率です。$L(p)$ を最大化すると、p の推定値は次のようになります。

$$\hat{p} = \frac{1}{n}\sum x_i = \frac{n_b}{n}. \tag{238}$$

これにより、統計ベースの密度行列 ρ が得られます。

$$\rho = \begin{pmatrix} \frac{n_a}{n} & 0 \\ 0 & \frac{n_b}{n} \end{pmatrix} = \frac{n_a}{n}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{n_b}{n}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{n_a}{n}|0\rangle\langle 0| + \frac{n_b}{n}|1\rangle\langle 1|. \tag{239}$$

統計的な観点から、量子状態は、この方法で収集できるすべてのデータの数学的エンコーディングです。

先に進む前に、純粋状態と混合状態の違いを説明する必要があります。量子状態 $|\psi\rangle$ が他の量子状態の凸結合である場合、それは混合状態にあると言われます。混合には、振幅ではなく、古典的な確率または組み合わせが含まれることに注意してください。しかし、状態 $|\psi\rangle$ が他の状態の凸結合として表現できない場合、それは純粋な状態であると言われます。純粋な状態は、凸状態のセットの極値です。

純粋な $|\phi\rangle$ 状態の場合、ケットブラ $|\phi\rangle\langle\phi|$ 射影演算子と呼ばれます。 $|\phi\rangle$ をそれ自体に投影し ($|\phi\rangle\langle\phi|\phi\rangle = |\phi\rangle$) となり、$|\phi\rangle$ に直交する任意の状態 $|\theta\rangle$ を $0(|\phi\rangle\langle\phi|\theta\rangle = 0)$ に投影します。純粋な状態 ϕ の場合、密度行列は単純に $\rho = |\phi\rangle\langle\phi|$ です。 システムが確率 p_j の極値点 ϕ_j の 1 つにある混合状態の場合、密度行列 ρ は、それぞれの確率で重み付けされたプロジェクターの合計として定義されます。

$$\rho = \sum_j p_j |\phi_j\rangle\langle\phi_j|. \tag{240}$$

確率は非負であり、合計が 1 であるため、これは、ρ が正の半確定エルミート演算子（固有値は非負）であり、ρ のトレース（行列の対角要素の合計、つまり 固有値）は 1 に等しい。

たとえば、純粋な状態 $|\psi\rangle$ を $|\psi\rangle = a|0\rangle + b|1\rangle$ とします。ここで、a と b は、それぞれの複素共役 a^* と b^* を持つ複素数です。 次に、$|\psi\rangle$ の密度行列 ρ は次のようになります。

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} aa* & ab* \\ ba* & bb* \end{pmatrix}. \tag{241}$$

a = 2、b = 1 の場合、これは次のようになります。

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \frac{2}{3} & \frac{\sqrt{2}}{3} \\ \frac{\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}. \tag{242}$$

計算ベースで $|\psi\rangle$ を測定すると、確率 $\frac{2}{3}$ で—$0\rangle$、または確率 $\frac{1}{3}$ で $|1\rangle$ が得られます。

これらの確率は、ρ のトレースにあります。 ρ を $\rho = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$ と書き直すと、 非対角要素の情報が失われる可能性があります。（これは、クローン作成中に発生することです。）測定後、確率 1 で $|\psi\rangle = |0\rangle$、または確率 1 で $|\psi\rangle = |1\rangle$ のいずれかであることに注意してください。

別の例として、状態のアンサンブル内の $\frac{3}{4}$ つの状態が状態 $|\psi\rangle_1 = .8\,|0\rangle + .6\,|1\rangle$ で準備され、$\frac{1}{4}$ が状態 $|\psi\rangle_2 = .6\,|0\rangle - .8i\,|1\rangle$ で準備されると仮定します。

次に、式（240）を使用した、この混合アンサンブルの密度行列は次のようになります。

$$\rho = .75\,|\psi_1\rangle\langle\psi_1| + .25\,|\psi_2\rangle\langle\psi_2| = \begin{pmatrix} .57 & .36 + 12i \\ .36 - 12i & .43 \end{pmatrix}. \tag{243}$$

このセットから引き出され、$(|0\rangle, |1\rangle)$ ベースで測定された粒子は、確率 .57 の状態 $|0\rangle$ または確率 .43 の状態 $|1\rangle$ で検出されます。ただし、ρ を使用して別の基準の確率を見つけたい場合は、トレースだけでなく、対角外の要素も必要になります。これを確認するために、同じアンサンブルから粒子を描画し、正規直交基底 $(|\phi_1\rangle, |\phi_2\rangle)$ で測定を行うと仮定します。ここで、$|\phi_1\rangle = .6\,|0\rangle + .8\,|1\rangle$ および $|\phi_2\rangle = .8\,|0\rangle + .6\,|1\rangle$ です。ここで、$\langle\phi_1|\phi_2\rangle = 0$ および $|\langle\phi_1|\psi_1\rangle|^2 = |\langle\phi_2|\phi_2\rangle|^2 = 1$ であることに注意してください。次に、ρ は観測の確率 P として $|\phi_1\rangle$ および $|\phi_2\rangle$ を与えます。

$$P(|\phi_1\rangle) = (.6, .8)\rho \begin{pmatrix} .6 \\ .8 \end{pmatrix} = .826 \tag{244}$$

$$P(|\phi_2\rangle) = (.8, -.6)\rho \begin{pmatrix} .8 \\ -.6 \end{pmatrix} = .174. \tag{245}$$

電子のスピン状態など、観測可能な א 選択するとします。次に、量子測定のフォンノイマン定式化では、各オブザーバブルはエルミート演算子 A に関連付けられ、$A\,|\psi_j\rangle = a_j\,|\psi_j\rangle$ です。ここで、$|\psi_j\rangle$ は A の固有ベクトルであり、a_j は固有値です。したがって、ρ と A に同じ基底、つまり A の固有ベクトルを使用すると、次のようになります。

$$A\rho = \sum_j p_j A\,|\psi_j\rangle\langle\psi_j| = \sum_j p_j a_j\,|\psi_j\rangle\langle\psi_j|. \tag{246}$$

これで、A の期待値 A は単純になります。

$$\bar{A} = \sum_j p_j a_j. \tag{247}$$

したがって、後者は次のように表すことができます。

$$\bar{A} = trace(A\rho). \tag{248}$$

密度行列 ρ を介した量子状態推定には多くのアプローチがあります。状態推定の問題は、クローンの問題と密接に関連しており、エンタングルメントの問題に関連しています。以前に検討した最尤法がおそらく最良です。 このエッセイのヒューリスティックな目的のために、ベイジアンフレームワーク (参考文献 63) が明らかになっています。

私たちは無関心、または不十分な理由の原則から始めて、密度が密度であるという最初の仮定をするかもしれません行列は完全に混合された形式です（$\mathbf{H}_2$ のシステムの場合)。

$$\rho = \frac{1}{2}\mathbf{1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \tag{249}$$

これはアンサンブルに対応し、その半分はアップ状態で、半分はダウン状態です。

$$\rho = \frac{1}{2}\left|u\right\rangle\left\langle u\right| + \frac{1}{2}\left|d\right\rangle\left\langle d\right| = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\mathbf{1}. \tag{250}$$

または、密度行列の一般的な形式から始めることもできます。これは、パウリスピン行列と実数 r_x, r_y および r_z で次のように記述できます。

$$\rho = \frac{1}{2}(\mathbf{1} + \mathbf{r}\cdot\sigma) \tag{251}$$

$$= \frac{1}{2}(\mathbf{1} + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z) \tag{252}$$

$$= \frac{1}{2}\begin{pmatrix} 1 + r_z & r_x - ir_y \\ r_x + ir_y & 1 - r_z \end{pmatrix}. \tag{253}$$

ここでは、ρ の行列式が非負である必要があります。$\mathbf{det}\rho \geq 0$ は、$\frac{1}{4}[1 - (r_x^2 + r_y^2 + r_z^2)] \geq 0$ を意味します。または、$\mathbf{r}^2 = r_x^2 + r_y^2 + r_z^2$ です。そのため、各密度行列は、ブロッホ球と呼ばれる半径 1 のボールに関連付けることができます。ボールの表面上の点は純粋な状態に対応し、内部の点は混合状態に対応します。

この形式の密度行列 ρ を仮定し、z 方向のスピンを測定して、周波数 n_u および n_d で一連の n 個の結果 u および d を取得すると、次のようになります。

$$L(n_u) = [\frac{1}{2}(1 + r_z)^{\frac{n_u}{n}}][\frac{1}{2}(1 - r_z)^{\frac{n-n_u}{n}}] \tag{254}$$

ここで、次の状態識別ゲーム Γ_{sd} について考えてみます。N 個の状態があり、集合 $S = \{\left|\psi_j\right\rangle, j = 0, 1, \cdots, N-1\}$ のメンバーです。これらの各状態は、密度行列 $\rho_j = \eta_j\left|\psi_j\right\rangle\left\langle\psi_j\right|$ で表されます。アリスは、ボブに知られていない状態 ρ_k を準備し、関連付けられた $\left|\psi_k\right\rangle$ が S のメンバーであるという情報とともに、それをボブに転送します。彼女はまた、S の各状態の確率 η_j を彼に伝えます。

η_j は事前確率と呼ばれます。 もちろん、これはすぐにベイジアンフレームワークを示唆するので、量子仮説検定と呼ばれるベイジアン戦略を考えてみましょう (参考文献 9)。

N 個の状態があるため、ボブは N 個の結果を与える手順に従います。これを a_j とラベル付けします。ボブが結果を取得した場合、彼は送信された状態が ρ_m であると想定します。$\rho_m \neq \rho_k$ であるエラー確率 p_E と、$\rho_m = \rho_k$ である確率 $1 - p_E = p_D$ があります。

ゲームの説明を完了するには、ρ_k が送信された場合にボブが見つける確率を表すチャネル行列 $[h(a_m\rho_k)]$ と、作成にコストを割り当てるコスト行列 $[c_{mk}]$ を定義する必要があります。 仮説は、ρ_k が送信されたときです。

送信された rho_k に関係なく、ボブの測定値は午前の 1 つを生成します。 これにより、次のような完全性条件が生じます。

$$\sum_{m=1}^{N} h(a_m|\rho_k) = 1. \tag{255}$$

その場合、合計エラー確率は次のようになります。

$$p_E = 1 - \sum_{k=1}^{N} \eta_k c_{mk} h(a_m|\rho_k). \tag{256}$$

ボブがアリスに支払う平均金額 c_B は、ベイジアンコストマトリックスによって与えられます

$$c_B = \sum_{mk} \eta_k c_{mk} h(a_m|\rho_k). \tag{257}$$

ボブの目標は、c_B を最小化することです。 ボブが制御するのは、チャネル行列 h の要素だけです。 したがって、ボブの問題は

$$\min_{\mathbf{h}} \sum_{mk} \eta_k c_{mk} h(a_m|\rho_k). \tag{258}$$

これにより、ゲーム理論のコンテキストで量子状態の識別（特定の状態のセットから状態を見つける）が行われます。コスト行列の対角要素を 0 に設定し（ボブは正しいことに対して何も支払わない)、他の要素を定数 c に等しく設定すると（すべてのエラーのコストは同じ)、式（256）と（257）を比較すると、ボブは 問題はに減少します

$$\min_{\mathbf{h}} p_E. \tag{259}$$

ここでの状態の数は有限です。 対照的に、量子状態の推定では、状態のセットは無限大です。量子状態自体は観測できないので、量子状態推定とは、すでに見てきたように、量子状態の密度行列 ρ を推定することを意味します。これもまた、ゲーム理論の文脈に置くことができます。

状態推定ゲーム (参考文献 38) では、アリスは任意の純粋な状態 $|\psi\rangle \in \mathbf{H}_d$ を選択し、$|\psi\rangle^{\otimes N}$ をボブに送信し、$|\psi\rangle$ を審判に送信します。アリスから N 状態を受け取った後、ボブはそれらの測定を実行し、純粋な状態 $|\psi\rangle$ を審判に送信します。ボブとアリスから 2 つの状態を受け取った後、審判はいくつかの基準に従ってそれらを比較し（以下のクローン作成を参照)、2 つの状態が十分に接

近していない場合はアリスに、接近している場合はボブに報酬を与えます。もちろん、ボブの仕事は、アリスから受け取った N 個の状態を与えることができる最高の量子状態測定を構築することです。

20 Quantum cloning 量子クローニング

計量経済学では、いくつかの手順によって、いくつかの未知のパラメータ a の推定値 $\hat{a}$ を生成しようとします。これは、推定手順によると、パラメーター a のクローンを作成する試みと見なすことができます。完全なクローンを作成することは期待していませんが、不確実性の範囲内にある最良の見積もりのみです。これにより、量子状態の複製が可能になります。最適なクローニングデバイス (参考文献 69) の目的は、オリジナルにできるだけ近いコピーを作成することです。

最適なクローン作成は、アリスとクローン作成の女王であるクレアの間で行われる量子ゲーム、クローン作成ゲームの観点から定式化できます。このゲームには、N 個の入力システムと M 個の出力システムがあります。 まず、2 次元ヒルベルト空間 $\mathbf{H}_2$ の密度行列 ρ で記述された純粋な状態を持つアリスから始めます。彼女は状態準備手順を N 回実行し、ヒルベルト空間 $\mathbf{H}_2{\otimes}^N$ で複合システムを生成します。

$$\mathbf{1}_2 \otimes^N \rho = \rho \otimes^N . \tag{260}$$

その後、アリスは $\rho{\otimes}^N$ をクレアに発送します。 クレアは、選択したクローンデバイス T_m を使用して、M 個の出力システム $T_m\rho{\otimes}^N$ を生成します。次に、アリスは元のシステム $\rho{\otimes}^M$ の M 個のコピーを作成します。 ゲームの結果は

$$T_m\rho \otimes^N vs.\ \rho \otimes^M . \tag{261}$$

T_m は密度行列を密度行列にマップするため、線形の完全に正のトレース保存マップに制限されます。

このゲームにペイオフを割り当てる 1 つの方法は、ノルム基準の違いに基づいてペイオフを行うことです。

$$||T_m\rho \otimes^N -\rho \otimes^M ||. \tag{262}$$

もう 1 つの方法は、$\mathbf{trace}(\rho \otimes^M T_m\rho{\otimes}^N)$ に基づいて fidelity(忠実度) を使用することです。クローン作成機が完璧だったら、これは 1 になります。fidelity(忠実度) は、入力密度行列 ρ に依存する可能性があります。F（T）を次のように定義します

$$F(T) = \inf_{\rho} trace(\rho \otimes^M T_m\rho{\otimes}^N) < 1. \tag{263}$$

次に、クレアの仕事は $F(T)$ を最大化することです。 これにより、クローンゲームが最大の問題になります。出力クローンの忠実度が入力状態に依存しない場合、クローン作成者は「ユニバーサル」と呼ばれます。ユニバーサルクローン作成者のクローン作成の最大忠実度は 5 であり、これは単一進化またはテレポートスキームによって達成できます (参考文献 8)。

$1qubit \to 2qubit$ のユニバーサル量子クローンは、未知の量子状態 $|\psi\rangle$ を入力として受け取り、$\rho = \eta \left|\psi\right\rangle \left\langle\psi\right| + (1-\eta)\frac{1}{2}\mathbf{1}$ の形式の密度行列で記述できる状態で 2 キュービットを出力として生成する量子機械です。パラメータ η は、密度演算子 $\left|\psi\right\rangle \left\langle\psi\right|$ に対応する元のブロッホベクトル r の縮小を表します。たとえば、$\left|\psi\right\rangle \left\langle\psi\right| = \frac{1}{2}(\mathbf{1} + \mathbf{r}\cdot\sigma)$ の場合、$\rho = \frac{1}{2}(\mathbf{1} + \eta\mathbf{r}\cdot\sigma)$ 次に、最適なクローン作成者は、$\eta < 1$ を最大化することによって fidelity(忠実度) を最大化することを含みます。

$$\max_{\eta} F = \langle\psi|\rho|\psi\rangle = \frac{1}{2}(1+\eta). \tag{264}$$

$\eta = \frac{2}{3}$ のブロッホ球のベクトル収縮は $\frac{5}{6}$ の最大 fidelity(忠実度) に対応します。

クローン作成プロセスは次のようになります。 $|B\rangle$ は、空白のコピーの初期状態（クローンの宛先）と、プロセスで必要な補助量子ビット（「アンシラ」）を示します。複製されるキュービット $|\psi\rangle$ は、基底 $(|0\rangle, |1\rangle)$ でエンコードされます。次に、ユニバーサル量子クローニングマシン（UQCM）変換 T_{UQCM} は、基底ベクトルまたは状態に基づいて次の変換を実行します。

$$T_{UQCM} \left|0\right\rangle \left|B\right\rangle \to \sqrt{\frac{2}{3}} \left|0\right\rangle \left|0\right\rangle \left|A_{\perp}\right\rangle + \sqrt{\frac{1}{6}}(\left|01\right\rangle + \left|10\right\rangle) \left|A\right\rangle \tag{265}$$

$$T_{UQCM} \left|1\right\rangle \left|B\right\rangle \to \sqrt{\frac{2}{3}} \left|1\right\rangle \left|1\right\rangle \left|A\right\rangle + \sqrt{\frac{1}{6}}(\left|01\right\rangle + \left|10\right\rangle) \left|A_{\perp}\right\rangle . \tag{266}$$

ここで、A と $A_{\perp}$ は、アンシラキュービットの 2 つの可能な直交最終状態を表します。 これは、入力状態 $|\psi\rangle$、出力を意味することに注意してください。

$$T_{UQCM} \left|\psi\right\rangle \left|B\right\rangle \to \tag{267}$$

$$\Big(\sqrt{\tfrac{2}{3}} \left|0\right\rangle \left|0\right\rangle \left|A_{\perp}\right\rangle + \sqrt{\tfrac{1}{6}}(\left|01\right\rangle + \left|10\right\rangle) \left|A\right\rangle , \quad \sqrt{\tfrac{2}{3}} \left|1\right\rangle \left|1\right\rangle \left|A\right\rangle + \sqrt{\tfrac{1}{6}}(\left|01\right\rangle + \left|10\right\rangle) \left|A_{\perp}\right\rangle \Big) \begin{pmatrix} a \\ b \end{pmatrix}. \tag{268}$$

次のステップは、2 量子ビットの混合状態を生成する、補助量子ビットをトレースすることです。次に、個々のキュービットごとに別のトレースが実行され、同じ混合 1 キュービット状態の 2 つのコピーが得られます。これは、元の状態と比較した場合の fidelity(忠実度) が $\frac{5}{6}$ です。

21 Conclusion

この時点で、読者は量子ゲーム理論を始めるのに十分な背景を取得しました。 もちろん、参考文献が示すように、言うべきことはもっとたくさんあります。 読者は特に量子計算に関する注記

（参考文献 21, 45, 61）を参照してください。

このエッセイは、伝統的なゲーム理論が量子ゲーム理論のサブセットであり、後者ははるかに豊富な構造と幅広い結果のセットを持っていることを示しています。これが、量子ゲーム理論を実行するために必要なことすべての正当化です。 何も諦めず、後者に切り替えることでより多くが得られます。したがって、伝統的なゲーム理論の研究は、進化的に安定した戦略でもナッシュ均衡でもなく、絶滅した種のコミ箱と非均衡の見返りに委ねられます。そうは言っても、たとえるならば、量子ゲーム理論の現状は、突然変異体の侵入に耐えられるのだろうか？それらの侵入する突然変異体が、量子力学の何が悪いのかを修正するためにやってくる数理経済学者になることを願っています。確かに、ランベルティーニ (参考文献 37) は、数理経済学と量子力学は同型であると主張しています。

量子ゲーム $\Sigma = \Sigma(\mathbf{H}, \Lambda, U, \{s_i\}_j, \{\pi_i\}_j)$ ここで $\mathbf{H}$ はヒルベルト空間です。Λ はゲームの初期状態です。U は、ゲームの開始時と終了時にすべてのプレーヤーのキュービットに適用されるユニタリ行列です。$\{s_i\}_j$ は、凸結合を含む、プレーヤー j の一連の動きです。 および $\{\pi_i\}_j$ は、プレーヤー j へのペイオフのセットです。ゲームの目的は、プレーヤー j の期待される見返りを最大化する戦略を内生的に決定することです。一般に、純粋な量子移動 s_i は、プレーヤーの個々のキュービットに適用されるユニタリ行列です。

このエッセイの過程で、「The spin flip game: スピンフリップゲーム」、「Guess a number games: ナンバーゲームを推測する」I および II、RSA ゲーム、囚人のジレンマ、男女の戦い、Newcomb のゲーム、進化的に安定した戦略ゲーム、コインフリップゲーム、 疑似テレパシーゲームおよびテレポーテーション、「 Quantum secret sharing 量子秘密共有」、状態推定、および量子クローニングのゲーム理論的側面を述べた。 スピンフリップゲームでは、ボブはアダマール変換 H を介して量子重ね合わせを利用して常にゲームに勝つことができましたが、この結果はプレーヤーの動きのシーケンスにも依存することを確認しました。 ナンバーゲームを推測するための鍵は、グローバー検索アルゴリズムを使用して、ヒルベルト空間の状態ベクトルを未知の数のおおよその位置に回転させることでした。この検索は、重ね合わせと f_a オラクルの呼び出しを使用して、N 回の移動から $\sqrt{N}$ 回の移動に高速化されました。ナンバーゲームを推測する II では、Bernstein-Vazirani オラクルを使用して、オラクルを 1 回呼び出した後、不明な番号の Walsh 変換 W_{2^n} を作成しました。RSA ゲームでは、Shor の因数分解アルゴリズムを使用して、整数の重ね合わせた状態を、与えられた複合 RSA 素数 $N = pq$ に対して $\frac{2^{2n}}{r}$ の整数倍に投影しました。ここで、r はテストされた要素の次数です。確率は、量子フーリエ変換を使用して制御されました。

囚人のジレンマゲームでは、量子の追加により H と σ_z が 1 に移動し、σ_x が従来のゲームの結果に追加され、実際にナッシュ均衡としてパレート最適点に到達することがわかりました。男女の戦いのゲームでは、同じ量子の動きが、純粋な戦略でユニークなナッシュとパレートの最適な均衡を生み出しました。混合戦略におけるアリスとボブの平等、ナッシュ均衡とパレート最適を説明しました。Newcomb のパラドックスは、スーペリアビーイングの全知に取って代わった重ね合わせの使用を通じて、アリスの選択を完全に予測（制御）するスーペリアビーイングの能力と、アリスの側で不正行為をするインセンティブによって解決されました。これらのゲームは、ユニタリ行列 U

を使用することにより、「協調的」と「非協調的」のカテゴリの部分的な無関係性も示しています。プレーヤーのキュービットがゲームに巻き込まれている場合、プレーヤーが自分の期待効用を最大化することに単に焦点を合わせると、コミュニケーションの隠されたチャネル（見えざる手）があります。進化的に安定した戦略ゲームでは、量子の動きをしている侵入変異体は、古典的な動きだけをしている既存の種を一掃することができました。コイントスゲームは、エンタングルメントのないゲームで、量子オラクルを使用して不公平なゲームを公正なゲームに変えることを実証しました。

疑似テレパシーゲームでは、量子もつれ状態を共有している限り、プレイヤーが共謀してゲームに勝つために、プレイヤー間のコミュニケーションは必要ありませんでした。N の適切なサブセットは、0 のペイオフを期待していましたが、ゲームは N 人のプレーヤー全員の暗黙の連立で確実に勝つことができました。また、N 次元の確率空間が疑似テレパシーゲームのコアであることがわかりました。これは、量子もつれが量子確率を引き起こすことを意味しますか？キュービット状態は観測不能であり、測定中は測定ベース（通常は 0 または 1）に投影されるため、破壊されることがわかりました。これは機会と困難を生み出します。ベルベースでの測定は、テレポーテーションプロトコルの中心です。量子状態は特定の忠実度でのみ複製できますが、秘密分散と安全な通信に使用できます。ベイズフレームワークで最尤法を使用した量子状態識別の問題、または密度行列のブロッホ球表現に関連して同じものを使用した量子状態推定の問題は、経済学者にとって基本的に異質な概念ではありません。

Piotrowski と Sladkowski (参考文献 59) は、彼らが Quantum anthropic principle（量子人間原理）と呼んでいるものを述べています。文明市場の初期段階で古典的な法則が支配されていたとしても、比較優位を伝える際の量子アルゴリズムの比類のない効率は、量子 振る舞いは古典的なものよりも優先されます。 自然はすでに量子ゲームをしているので、人間は自分の量子コンピューター（人間の脳）も使ってそうしているように見えます。したがって、投機的ではありますが、Complexity Digest での Gottfried Mayer のコメントは、「人間の決定が微視的な量子イベントにたどることができれば、自然は進化する複雑な脳で量子計算を利用したであろうと予想されるでしょう。その意味で、量子コンピューターは量子ルールに従って市場ゲームをプレイしていると言うことができます。(参考文献 42)」とのこと。これについて、今のところハッキリしていません。

[1]␣Bell␣J.S.,␣‘On␣the␣Einstein␣Podolsky␣Paradox’ ,␣Physics,␣1(3),␣1964,␣195-200.
[2]␣Bennett␣Charles␣H.,␣Gilles␣Brassard,␣Claude␣Cre␣^^cc^^81peau,␣Richard␣Jozsa,␣Asher␣Peres,␣Willi
K.␣Wootters,␣‘Teleporting␣an␣unknown␣quantum␣state␣via␣dual␣classical␣and␣EPR␣channels’
,
http://www.enricozimuel.net/documenti/BBC+93.ps␣.
[3]␣Bernstein␣E.␣and␣U.␣Vazirani,␣‘Quantum␣complexity␣theory’ ,␣in␣Proceedings␣of␣the␣25th␣Annual␣AC
Symposium␣on␣the␣Theory␣of␣Computing,␣San␣Diego,␣Calif.,␣16-18␣May␣1993,␣New␣York:ACM,␣1993,
11-20,␣http://www.cs.berkeley.edu/^^e2^^88^^bcvazirani/pubs/bv.ps
[4]␣Brams␣Steven␣J.,␣Superior␣Beings:␣If␣they␣exist,␣how␣would␣we␣know?␣Game␣theoretic␣implications

omniscence,␣omnipotence,␣immortality,␣and␣incomprehensibility,␣New␣York:Springer-Verlag,␣1983.
[5]␣Brassard␣Gilles,␣Anne␣Broadbent,␣Alain␣Tapp,␣'Recasting␣Mermin's␣multi-player␣game␣into␣the␣fra
work␣of␣pseudo-telepathy' ,␣arXiv:␣quant-ph/0408052␣v1␣6␣Aug␣2004.
[6]␣Braunstein␣Samual␣L.,␣'Quantum␣Computation' ,␣http://www-users.cs.york.ac.uk/^^e2^^88^^bcschmuel
/comp␣best.pdf␣.
[7]␣Braunstein␣Samuel␣L.␣and␣H.␣J.␣Kimble,␣'Teleportation␣of␣continuous␣quantum␣variables'
,␣Physical
Review␣Letters␣80,␣4,␣26␣January␣1998,␣http://www-users.cs.york.ac.uk/^^e2^^88^^bcschmuel/papers/bk
[8]␣Bru^^c3^^9f␣Dagmar,␣David␣P.␣DiVincenzo,␣Artur␣Kert,␣Christopher␣A.␣Fuchs,␣Chiara␣Macchiavello,
'Optimal␣universal␣and␣state-dependent␣quantum␣cloning' ,␣arXiv:␣quant-ph/9705038␣v3␣6
Dec␣1997.
[9]␣Chefles␣Anthony,␣'Quantum␣state␣discrimination' ,␣arXiv:␣quant-ph/0010114␣v1␣31␣Oct␣2000.
65
␣␣[10]␣Cheon␣Taksu␣and␣Izumi␣Tsutsui,␣'Classical␣and␣quantum␣contents␣of␣solvable␣game␣theory␣on␣Hi
␣arXiv;␣quant-ph/0503233␣v1␣31␣Mar␣2005
[11]␣Cleve␣Richard,␣Daniel␣Gottesman,␣Hoi-Kwong␣Lo,␣ 'How␣to␣share␣a␣quantum␣secret'
,␣December␣1998,
http://www.hpl.hp.com/techreports/98/HPL-98-205.pdf
[12]␣Debreu␣G.␣and␣H.␣E.␣Scarf,␣'A␣limit␣theorem␣on␣the␣core␣of␣an␣economy' ,␣International␣Economic
Review,␣4,␣1963,␣235-246.
[13]␣Deutsch␣D.,␣'Quantum␣Theory,␣the␣Church-Turing␣principle␣and␣the␣universal␣quantum␣computer'
,
Proc.␣Roy.␣Lond.␣A400,␣1985,␣97-117.
[14]␣Deutsch,␣D.,␣'Quantum␣computational␣networks,'␣Proceedings␣of␣the␣Royal␣Society␣of␣London,␣A42
1989,␣73-90.
[15]␣Deutsch,D.,'ItfromQubit' ,Sept.2002,http://www.qubit.org/people/david/Articles/ItFromQubit.pdf
[16]␣Deutsch␣D.␣and␣R.␣Jozsa,␣ 'Rapid␣solution␣of␣problems␣by␣quantum␣computation,'
␣Proceedings␣Royal
Society␣London,␣A400,␣1992,␣73-90.
[17]␣Du␣Jianfeng,␣Xiaodong␣Xu,␣Hui␣Li,␣Mingjun␣Shi,␣Xianyi␣Zhou,␣Rongdian␣Han,␣
'Quantum␣strategy
without␣entanglement' ,␣arXiv:␣quant-ph/0011078␣v1␣19␣Nov␣2000.
[18]␣Einstein␣A.,␣B.␣Podolsky,␣N.␣Rosen,␣'Can␣quantum␣mechanical␣description␣of␣physical␣reality␣be
considered␣complete?' ,␣Phys.␣Rev.␣47,␣1935,␣777-780.
[19]␣Eisert␣Jens␣and␣Martin␣Wilkens,␣'Quantum␣Games,'␣arXiv:quant-ph/0004076␣v1␣19␣Apr␣2000.
[20]␣Eisert␣Jens,␣Martin␣Wilkens,␣and␣Maciej␣Lewenstein,␣'Quantum␣games␣and␣quantum␣strategies'
,

arXiv:␣quant-ph/9806088␣v3␣29␣Sept␣1999.
[21]␣Ekert␣Artur,␣Patrick␣Hayden␣and␣Hitoshi␣Inamori,␣Basic␣concepts␣in␣quantum␣computation,␣arXiv:
quant-ph/0011013␣v1␣2␣Nov␣2000,
[22]␣Feynman␣Richard␣P.,␣'Simulating␣Physics␣with␣Computers,'␣International␣Journal␣of␣Theoretical
Physcis,␣21,␣1982,␣467.
[23]␣Fishburn␣Peter␣C.,␣'Expected␣utility␣theories:␣a␣review␣note',␣in␣R.␣Henn␣and␣O.␣Moeschlin,␣ed
Mathematical␣Economics␣and␣Game␣Theory:␣Essays␣in␣honor␣of␣Oskar␣Morgenstern,␣Lecture␣Notes
in␣Economics␣and␣Mathematical␣Systems,␣141,␣Berlin:Springer-Verlag,␣1977.
[24]␣Gale␣David,␣The␣Theory␣of␣Linear␣Economic␣Models,␣New␣York:␣McGraw-Hill,␣1960.
[25]␣Gisin␣Nicolas,␣'How␣come␣the␣correlations?'␣http://arxiv.org/ftp/quant-ph/papers/0503/0503007.
[26]␣Gogonea␣V.␣and␣K.␣M.␣Merz,␣'Fully␣quantum␣mechanical␣description␣of␣proteins␣in␣solution␣combi
ning␣linear␣scaling␣quantum␣mechanical␣methodologies␣with␣the␣Poisson-Boltzmann␣equation'
,␣J.␣Phys.␣Chem.␣A,␣103␣(1999)␣51715188.
[27]␣Gottesman␣Daniel,␣'The␣Heisenberg␣representation␣of␣quantum␣computers',␣arXiv:␣quant-ph/980700
[28]␣GroverLovK.,'Afastquantummechanicalalgorithmfordatabasesearch',arXiv:quant-ph/9605043.
[29]␣Hardy␣G.␣H.␣and␣E.␣M.␣Wright,␣An␣Introduction␣to␣the␣Theory␣of␣Numbers,␣Fifth␣edition,␣Ox-
ford:Clarendon␣Press␣1979.
[30]␣Herbert,N.'FLASH^^e2^^80^^93asuperluminalcommunicatorbaseduponanewtypeofquantummeasurement"
,
Found.␣Phys.␣12,␣1982,␣1171.
[31]␣Hillary␣Mark,␣Vladimir␣Buzek,␣and␣Andre␣Berthiaume,␣'Quantum␣secret␣sharing'
,␣Physical␣Review␣A,
vol␣59,␣no␣3,␣March␣1999,␣1829-1834,␣http://www.quniverse.sk/buzek/mypapers/99pra1829.pdf
[32]␣Hunziker␣Markus␣and␣David␣A.␣Meyer,␣'Quantum␣algorithms␣for␣highly␣structured␣search␣problems,

http://www3.baylor.edu/^^e2^^88^^bcMarkus␣Hunziker/HunzikerMeyer2002.pdf␣.
[33]␣Iqbal␣A.␣and␣A.H.␣Toor,␣'Evolutionary␣stable␣strategies␣in␣quantum␣games'
,␣arXiv:␣quant-ph/0007100
v3␣11␣Dec␣2000.
[34]␣Jaroszkiewicz␣George␣and␣Jason␣Ridgway-Taylor,␣'Quantum␣Computational␣Representation␣of␣the
Bosonic␣Oscillator',␣arXiv:quant-ph/0502166␣v1␣25␣Feb␣2005
[35]␣Jammer␣Max,␣The␣Philosophy␣of␣Quantum␣Mechanics,␣New␣York:␣Wiley,␣1974.
[36]␣Johnson␣Joseph␣F.,␣'The␣problem␣of␣quantum␣measurement',␣arXiv␣quant-ph/0502124␣v1␣21␣Feb␣2005
[37]␣Lambertini,␣Luca,␣'Quantum␣mechaics␣and␣mathematical␣economics␣are␣isomorphic,'
␣29␣Feb␣2000,
http://www.dse.unibo.it/wp/370.pdf
[38]␣Lee␣Chiu␣Fan␣and␣Neil␣F.␣Johnston,␣'Game␣theoretic␣discussion␣of␣quantum␣state␣estimation␣and

cloning' ,␣arXiv:␣quant-ph/0207139␣v2␣29␣Nov␣2002.
[39]␣Lomonaco,␣Jr.␣Samuel␣J.,␣ 'A␣lecture␣on␣Grover' s␣quantum␣search␣algorithm'
,␣arXiv:quant-ph/0010040
v2␣18␣Oct␣2000.
[40]␣Luce␣R.␣Duncan␣and␣Howard␣Raiffa,␣Games␣and␣Decisions,␣New␣York:␣Wiley,␣1957.
[41]␣Marinatto␣Luca␣and␣Tullio␣Weber,␣ 'A␣quantum␣approach␣to␣static␣games␣of␣complete␣information'
,
arXiv:␣quant-ph/0004081␣v2␣27␣June␣2000␣.
[42]␣Mayer,␣Gottfried␣J.,␣Editor' s␣Note␣to␣Complexity␣Digest,␣27,␣2␣July␣2001.
[43]␣Maynard␣Smith␣J.␣and␣G.R.␣Price,␣ 'The␣logic␣of␣animal␣conflict' ,␣Nature,␣246,␣1973,␣15-18.
[44]␣Maynard␣Smith␣J.,␣Evolution␣and␣the␣Theory␣of␣Games,␣Cambridge:␣Cambridge␣University␣Press,
1982.
[45]␣Meglicki,␣Zdzislaw,␣ 'Introduction␣to␣quantum␣computing' ,␣February␣5,␣2002,http://beige.ucs.ind
[46]␣Meyer␣David␣A.,␣ 'Quantum␣Games␣and␣Quantum␣Algorithms' ,␣arXiv:quant-ph/0004092␣v2,␣3␣May
2000.
[47]␣Milman␣P.␣H.␣Ollivier,␣and␣J.␣M.␣Raimond,␣ 'Universal␣quantum␣cloning␣in␣cavity␣QED'
,
http://www.imperial.ac.uk/physics/qgates/papers/ENS␣QG04.pdf,␣23␣Jan␣2003.
[48]␣Nawaz␣Ahmad␣and␣A.␣H.␣Toor,␣ 'Dilemma␣and␣Quantum␣Battle␣of␣the␣Sexes' ,
arXchiv:quant-ph/0110096␣v3,␣26␣Mar␣2004.
[49]␣Neumann␣John␣von,␣ 'Zur␣Theorie␣der␣Gesellschaftspiele' ␣Mathematische␣Annalen,␣1928.␣100:295-
320.
[50]␣NeumannJohn␣von,␣Mathematische␣Grundlagen␣der␣Quantenmechanik,␣Berlin:␣Springer-Verlag,
1932.
[51]␣Neumann␣John␣von,␣ 'A␣Model␣of␣General␣Economic␣Equilibrium' ␣('U␣^^cc^^88ber␣ein␣o␣^^cc^^88kono
ichungssystem␣und␣eine␣Verallgemeinerung␣des␣Brouwerschen␣Fixpunktsatzes')␣in␣K.␣Menger,␣ed.,
Ergebnisse␣eines␣mathematischen␣Kolloquiums,␣1935-36,␣1937.
[52]␣Neumann,␣John␣von,␣ 'Probabilistic␣logics␣and␣the␣synthesis␣of␣reliable␣organisms␣from␣unreliab
components' ,␣Automata␣Studies,␣Princeton␣University␣Press,␣1956,␣329-378.
[53]␣Neumann␣John␣von␣and␣Oscar␣Morgenstern,␣The␣Theory␣of␣Games␣and␣Economic␣Behavior,␣New
York:␣Wiley,␣1944.
[54]␣Ore␣Oystein,␣Number␣Theory␣and␣Its␣History,␣New␣York:␣Dover␣(reprint␣of␣New␣York:␣McGraw-Hill,
1948),␣1988.
[55]␣Penrose,␣Roger,␣The␣Emperor' s␣New␣Mind,␣Oxford:␣Oxford␣University␣Press,␣1989.
[56]␣Peres␣Asher,␣ 'How␣the␣no-cloning␣theorem␣got␣its␣name,' ␣arXiv:␣quantum-ph/0205076␣v1␣14␣May
2002.
[57]␣Piotrowski␣Edward␣W.␣and␣Jan␣Sladkowski,␣ 'An␣invitation␣to␣quantum␣game␣theory'

,␣arXiv:
quant-ph/0211191␣v1␣28␣Nov␣2002.
[58]␣Piotrowski␣Edward␣W.␣and␣Jan␣Sladkowski,␣ 'Quantum␣solution␣to␣the␣Newcomb'
s␣paradox' ,␣arXiv:
quant-ph/0202074␣v1␣13␣Feb␣2002.
[59]␣Piotrowski␣Edward␣W.␣and␣Jan␣Sladkowski,␣'Trading␣by␣quantum␣rules^^e2^^80^^93quantum␣anthropi
,
http://alpha.uwb.edu.pl/ep/RePEc/sla/eakjkl/9.pdf␣.
[60]␣Pirandola␣Stefano,␣'A␣quantum␣teleportation␣game' ,␣arXiv:␣quant-ph/0407248␣v3␣17␣Nov␣2004.
[61]␣Preskill␣John,␣'Lecture␣notes␣for␣Physics␣229:␣quantum␣information␣and␣computation'
,␣California␣In-stitute␣of␣Technology,␣September␣1998,␣http://www.theory.caltech.edu/people/preskil
[62]␣Shor␣P.␣W.,␣'Algorithms␣for␣quantum␣computation:␣discrete␣logarithms␣and␣factor-␣ing'
,␣in␣Proc.␣35th␣Annual␣Symposium␣on␣the␣Foundations␣of␣Computer␣Science,␣edited␣by␣S.␣Goldwasser,␣L
http://www.ennui.net^^e2^^88^^bcquantum/papers/9508027.pdf␣.
[63]␣Srednick␣Mark,␣ 'Subjective␣and␣objective␣probabilities␣in␣quantum␣mechanics,'
␣arXiv:
quant-ph/0501009␣v2␣14␣Jan␣2005.
[64]␣Stanford␣Encyclopedia␣of␣Philsophy,␣ 'Evolutionary␣game␣theory' ,
http://plato.stanford.edu/entries/game-evolutionary/␣.
[65]␣Stapp␣Henry,␣'Why␣classical␣mechanics␣cannot␣naturally␣accomodate␣consciousness,␣but␣quantum
meachanics␣can,' ␣http://psyche.cs.monash.edu.au/v2/psyche-2-05-stapp.html␣.
[66]␣Stapp␣Henry,␣The␣Mindful␣Universe,␣http://www-physics.lbl.gov^^e2^^88^^bcstapp/MUA.pdf
[67]␣Turner␣P.E.␣and␣L.␣Chao,␣'Prisoner' s␣dilemma␣in␣an␣RNA␣virus,' ␣Nature,␣398(6726),␣April␣1,␣199
441-3.
[68]␣Ulam,␣S.M.,␣Adventures␣of␣a␣Mathematician,␣New␣York:Charles␣Scribner' s␣Sons,␣1976.
[69]␣Werner␣R.␣F.,␣'Optimal␣cloning␣of␣pure␣states' ,␣arXiv:␣quant-ph/9804001␣v1␣1␣April␣1998.
[70]␣Zalka␣Chris,␣'Grover' s␣quantum␣searching␣algorithm␣is␣optimal' ,␣arXiv:quant-ph/9711070␣v2,␣2␣D