

# 情報の物理学

F. ALEXANDER BAIS

J. DOYNE FARMER

2022 年 2 月 23 日

## この文書について

この文書は THE PHYSICS OF INFORMATION(arXiv:0708.2837v2) の内容に興味をもち学習するために個人的翻訳です。内容の正確性を保証するものではありません。

This document is a personal translation\* of THE PHYSICS OF INFORMATION (arXiv:0708.2837v2<sup>†</sup>) into Japanese for the purpose of learning and interest in its contents. The accuracy of the content is not guaranteed. It was very educational and inspiring for me. I would like to acknowledge the authors, F. ALEXANDER BAIS and J. DOYNE FARMER.

In addition, as of now, the translation is only up to section 6.

## 概要

(理論) 物理学と情報の接点について、専門家ではない人のために解説する。エントロピーの概念に関連した情報の起源を、最初は熱力学の文脈で、次に統計力学の文脈で説明する。統計力学の基礎を詳しく調べ、確率的世界観と決定論的世界観を両立させる必要性から、予測可能性を定量化する上で情報が重要な役割を果たすカオス力学の議論へと進める。次に、情報を定義する際に浮上する様々な基本的な問題と、秩序、無秩序、不完全な知識などの概念を議論する際に注意しなければならないことを議論する。また、ほかの形式のエントロピーと、その非平衡熱力学との関連性についても議論する。最後に、量子力学がどのようにして量子情報という全く異なる概念を生み出すのかを説明する。量子力学では、大規模な並列処理が可能のため、情報の保存や計算にまったく新しい可能性が生まれる。また、エントロピーを量子力学に応用することで、量子もつれを測定するのに役立つことを指摘する。最後に、量子論と一般相対性理論との接点に少しだけ立ち寄り、ブラックホールの物理学が提起する「究極の情報パラドックス」に直面する。このレビューでは、物理学と情報に関連するすべてのトピックをカバーすることはできず、トピックを限定している。

---

\* translated by T. Konishi. Twitter account @guppi524

<sup>†</sup> <https://arxiv.org/abs/0708.2837>

# 1 情報の物理学

なぜ『ブリタニカ百科事典』全 24 巻をピンの頭には書けないのか？

R.P. ファインマン

情報は、コンピュータであれ、生物であれ、それらの機構によって運ばれ、保存され、取り出され、処理される。すべての情報は、抽象的には 0 と 1 の文字列と考えられるが、紙であれ、シリコンチップであれ、プログラムであれ、物理的な基盤によって運ばなければならない、この情報の取り扱いには物理的なものがある。情報は物理的なものであり、情報は最終的に物理学の基本法則に制約される。したがって、物理学と情報の間に豊かな接点があるのは当然のことといえる。

シャノンが用いた情報の概念は、熱力学で初めて登場したエントロピーの概念を一般化したものである。熱力学では、エントロピーは熱や温度に依存する抽象的な量であり、その解釈は明らかではない。しかし、熱力学を説明し、一般化した統計力学の理論が登場してからは変わった。統計力学とは、システムを原子などのミクロな単位に分解して、温度や圧力などのマクロな現象をミクロな単位の統計的性質で説明する理論である。統計力学では、エントロピーを微視的な無秩序の尺度と見なすことができることを明らかにしている。エントロピー  $S$  は  $S = -\sum p_i \log p_i$  のように記述される。ここで、 $p_i$  はあるミクロの状態の確率のことであり、例えば、ある原子の速度と位置が一定の範囲内にある可能性のことである。

シャノンは、エントロピーが、原子や物理学とは関係のない、もっと一般的な場面での無秩序を表現するのに有効であることに気づいた。確率分布  $\{p_i\}$  のエントロピーは、 $p_i$  が定義されていれば、明確に定義される。このより一般的な文脈において、彼は、秩序の測定と無秩序の測定は本質的に同じであると主張した。高度に無秩序な状況では、測定を行うことで多くの情報が得られ、逆に高度に秩序化された状況では、測定を行っても得られる情報は少ない。したがって、いくつかの異なる状態のうちの 1 つにランダムになることができるシステムの場合、その分布のエントロピーは、どの状態  $i$  にあるかを知ることによって得られる情報と同じになる。エントロピー、あるいはそれに代わる情報という概念は、物理学とは関係のない多くの用途に役立つことがわかった。

また、このような一般的な言葉で考えることは、物理学にも有効であることがわかった。例えば、シャノンの研究では、エントロピーはある意味、元々の由来として導出された量よりも根本的なものであることが明らかになっている。これを受けてジェインズは、統計力学のすべてをエントロピーの最大化の問題として定式化した。実際、すべての科学は最大エントロピーの原理を応用したものと考えることができ、説明の単純さと正確さの間のトレードオフを定量化する手段を提供する。物理系がどのようにして計算を行ったり、コンピュータのメモリを構築したりすることができるのかを理解したい場合、熱力学的なエントロピーとは異なるエントロピーを定義することが有効である。しかし、計算の限界を理解するためには、熱力学や統計学の用語で考えることが非常に有効である。このことは、量子力学を利用して計算を改善する方法を理解する上で、特に重要となった。このような考察から、物理学の一分野として「情報の物理学」と呼ばれる分野が誕生した。

この章では、物理学者ではない人に、情報という考え方がどこから来たのかを説明しようとしている。まず初めに、熱力学におけるエントロピーの概念の起源について説明する。エントロピーは、熱の流れや温度に関連する巨視的な状態変数に過ぎず、むしろ、具体的な物理的解釈のない数学的な表現と言える。そして、原子の微視的な理論が統計力学につながり、熱力学の導出と拡張が可能になったことを説明する。これにより、システムのアクセス可能な微視的な状態の集合に対する確率からエントロピーが定義され、シャノンの重要な研究

に始まる現代の情報理論のインスピレーションとなった [54]。統計力学の基礎を精査し、確率的世界観と決定論的世界観を両立させる必要性から、予測可能性を定量化するために情報が重要な役割を果たすカオス力学の議論に至る。その上で、情報を定義する際に生じる様々な基本的な問題や、秩序、無秩序、不完全な知識などの概念を議論する際に注意しなければならないことを議論する。また、エントロピーの別の形と、その非平衡熱力学との関連性についても議論する。

本章の最後には、量子力学がどのように量子情報という概念を生み出したことを説明する。量子力学に内在する膨大な並列処理により、情報の保存や計算に全く新しい可能性が生まれる。また、エントロピーを拡張して量子力学に適用することで、量子もつれの測定に役立つことを指摘しておく。最後に、量子論と一般相対性理論の接点に少しでも立ち寄って、ブラックホールの物理学が提起する「究極の情報パラドックス」に向かい合う。このレビューでは、我々自身に限定し、物理学や情報に関連するすべてのトピックを網羅しているわけではない。

情報の保存や処理において、より多くの量とスピードを求めると、自然と物理的に操作できる最小のスケールに導かれる。私たちはまず、ファインマンが 1959 年に行った先見性のある講演「プレッティ・オブ・ルウム・アット・ザ・ボトム」[23] を引用し、原子レベルでの情報の保存と操作について述べる。現在市販されているプロセッサは、60nm ( $1\text{nm} = 1 \text{ ナノメートル} = 10^{-9} \text{ メートル}$ ) のスケールで動作する。2006 年には IBM が 30nm スケールの回路を発表し、確かにブリタニカ百科事典をピンの頭を書くことができるようになったので、1959 年のファインマンの推測に基づく発言は、現在の計算機のスケールを示す指標に過ぎなくなった。これがどれほど原子スケールに近いかというと、一辺が 30nm の正方形の中に約 1000 個の原子が入っている。ムーアの法則と呼ばれる歴史的なパターンでは、2 年ごとに集積回路のサイズが半分になる。このまま改良を続けていくと、約 20 年後には部品が原子 1 個分の大きさになり、コンピュータがこれ以上小さくなることは考えられない。これが実現すれば、原子スケールの情報は、マクロスケールの情報の使い方に直結することになりうる。それは、こういう詩として表せる。コンピュータが量子スケールの部品を持つようになると、その原子の動きはもはやランダムではなく、ある意味で古典的な統計力学では記述できなくなり、同時に巨視的なスケールでの情報処理にも使われるようになるだろう。

## 2 熱力学

なぜなら、私たちが扱う物体は何百万もの分子で構成されており、単一の分子を手に入れることは決してできないという事実依存しているからです。

J.C. マクスウェル

熱力学は、巨視的な物理系の学問である。<sup>1</sup>。これらの物理系には多数の自由度があり、典型的にはアボガドロ数のオーダー ( $N_A \approx 10^{23}$ ) になる。熱力学の 3 つの法則は、それぞれの系が相互に、あるいは環境とエネルギーを交換するプロセスを説明するものである。例えば、系が仕事をしたり、拡散プロセスで熱や質量を交換したりする。重要な考え方が「平衡」である。熱力学でいうところの平衡とは、2 つの系の間のエネルギーや質量の交換が両方向で同じであると仮定する。これは通常、2 つの系を長期間放置した場合にのみ成り立つ。プロセスが常に平衡に近い状態を保つ場合は**準静的**であり、これは**可逆的**であることも意味している。つまり、プロセスは元に戻すことができ、系は外部からのエネルギー入力なしに元の状態に戻ることができる。例えば、系の温度が保たれたリザーバーと熱的に接触している等温プロセスなど、様々な種類のプロセスを

<sup>1</sup> 熱力学と統計力学についてここで簡単に紹介した内容は、これらの分野の標準的な教科書に記載されています。[51, 38, 31, 42].

区別する。また、システムを熱的に絶縁しておき、温度を変化させる断熱プロセスもその一例です。また、気体の自由膨張や2つの流体の混合など、非平衡プロセスによってシステムがある平衡状態から別の平衡状態になることもあるが、この場合は可逆的ではない。完全に可逆的なシステムは存在しないものの、それでも非常に有用な概念である。

平衡状態にある系の注目すべき特徴は、マクロな状態が、体積  $V$ 、圧力  $P$ 、温度  $T$ 、エントロピー  $S$ 、化学ポテンシャル  $\mu$ 、粒子数  $N$  など、ごく少ない変数で特徴づけられることである。これらの状態変数は一般的に独立したものではなく、物理学的に課せられた制約を記述した**状態方程式**で結ばれている。身近な例では、理想気体の法則  $PV = N_A kT$  がある。ここで  $k$  は、温度とエネルギーの関係を表すボルツマン定数 ( $k = 1.4 \times 10^{-23} \text{ J/K}$ ) である。一般的に、状態変数は2つのペアで構成されており、一方が**示強性**であるのに対し、もう一方の共役変数は**示量性**である。圧力や温度などの示強変数は系の大きさに依存せず、体積やエントロピーなどの示量変数は系の大きさに比例する。

このライトニングレビューでは、情報理論との関連性が最も高い熱力学の本質的な特徴のみを紹介する。

## 2.1 法則

熱力学の第一法則は<sup>2</sup>

$$dU = dQ - dW \quad (2.1)$$

という式で示され、熱はエネルギーの一形態であり、エネルギーは保存されるということを述べている。より正確には、内部エネルギーの変化  $dU$  は、システムが吸収した熱量  $dQ$  からシステムが行った仕事量  $dW$  を差し引いたものに等しい。

第二法則では、温度に対する熱の流れの比として定義されるエントロピー  $S$  の概念が導入される。この法則は、閉鎖系（エネルギー、体積、粒子数が一定）のエントロピーは決して減少しないということを述べている。数学的には

$$dS = \frac{dQ}{T}, \quad \frac{dS}{dt} \geq 0. \quad (2.2)$$

標準的な例として気体を用いて、第一法則を正しい微分により次のように書き換えることができる。

$$dU = TdS - PdV, \quad (2.3)$$

ここで、 $PdV$  は、ピストンで気体を圧縮するなど、容器の体積を変化させることで得られる仕事である。エントロピー、熱、温度の関係から、エントロピーの差は温度計で温度を、熱量計で熱量の変化を測定すればよいことになる。これは、熱力学の観点から見ると、エントロピーは純粋に巨視的な量であることを示している。

第二法則には2つの異なる定式化がある。ケルビンの定式化は、熱を仕事に変えることだけを目的とした機関は存在し得ないということを述べている。熱を利用して仕事をすることはできるものの、そのためには必然的に他の変化を加えなければならない。例えば、熱いところから冷たいところへ熱を流して、それにより系を

---

<sup>2</sup> 微分の横棒は、それに続く量が状態変数ではないことを示している。したがって、 $d$  バーは、正しい微分ではなく、微小量を示している。

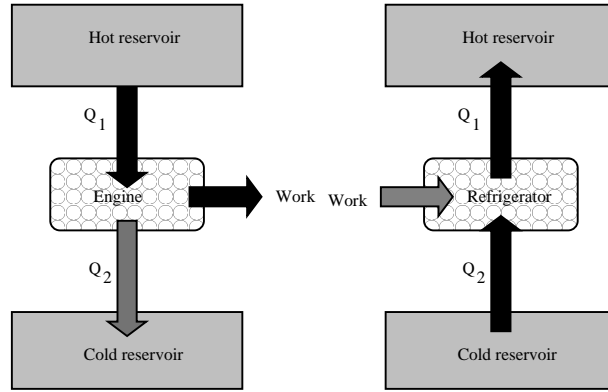


図1 熱力学の第二法則の2つの定式化を示した熱と仕事の関係。左側にはケルビンの定式化がある。理想的なエンジンは、黒い矢印だけの図に対応している。第二法則では、3番目の灰色の矢印が必然的に存在することになる。右側の黒い矢印だけの図が理想的な冷蔵庫に相当し、3番目の灰色の矢印は、再び第二法則で求められる。

平衡状態に近づけるようなことである。クラウジウスの定式化では、低温の熱源から熱だけを取り出し、同じ量の熱を高温の熱源に供給する機関はあり得ないということを言っている。これらの定式化を言い換えると、ケルビンは「理想的なエンジンは存在できない」と言い、クラウジウスは「理想的な冷蔵庫は存在できない」と言っている(図1参照)。

熱機関や冷凍機の動作は、カルノーサイクルと呼ばれる可逆的な一連の状態が閉じた曲線になっている図で表現することができる。図2にケルビンの定式化の例を示す。容器の中のピストンを想像してみよう。その目的は、2つの熱源の温度差を利用して仕事をするすることである。このサイクルは4つのステップで構成される。ステップ  $a \rightarrow b$  の等温膨張では、高温  $T_1$  の熱源から熱量  $Q_1$  を吸収することで、気体が膨張してピストンを押し、仕事をする。ステップ  $b \rightarrow c$  の断熱膨張では、気体は膨張を続けて仕事をするが、容器は熱源から切り離され、熱を吸収しなくなる。ここで、気体が膨張すると、温度は  $T_2$  になるまで冷える。ステップ  $c \rightarrow d$  の等温圧縮では、環境が気体に仕事をして熱が低温の熱源に流れ込み、熱量  $Q_2$  を放出する。そしてステップ  $d \rightarrow a$  の断熱圧縮では、気体がさらに圧縮されて(熱の移動なしに)元の温度に戻るため、環境が仕事をし続けることになる。この機関が行う正味の仕事は、線積分で与えられる。

$$W = \oint_{\text{cycle}} PdV = \text{囲まれた領域} \quad (2.4)$$

ここで、サイクルの最初と最後では内部エネルギーが同じであるため、第一法則により  $W = Q_1 - Q_2$  にもなるはずである。また、2つの熱源のエントロピーの純変化の合計は次のように計算することができる。

$$\Delta S = \frac{-Q_1}{T_1} + \frac{Q_2}{T_2} \geq 0, \quad (2.5)$$

ここで、最後の不等式は、第二法則により成り立たなければならない。なお、後者の2つの方程式は、正の  $W$  を持つ解を持つことができる。エンジンの効率  $\eta$  は、定義上、系に入る熱に対する仕事の割合である。つまり

$$\eta = \frac{W}{Q_1} = 1 - \frac{Q_2}{Q_1} \leq 1 - \frac{T_1}{T_2}. \quad (2.6)$$

となる。 $\eta$  は理想的な熱機関では1に等しいが、実際のエンジンでは1よりも小さくなる。

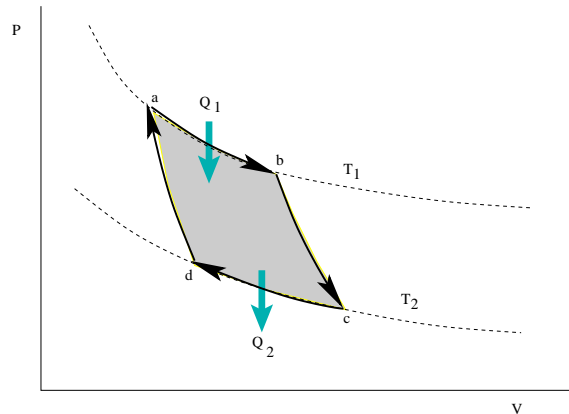


図2 第二法則のケルビンの定式化に対応するカルノーサイクル。エンジンが行う仕事は、閉じた輪郭に沿った線積分に等しく、したがって閉じた面積にも等しい。

第二法則の現代的な定式化として、統計力学の世界ではケルビンやクラウジウスの記述に相当する**ランダウアーの原理**がある。これは、情報を消すことだけを目的とした機関は存在しないということを述べている。忘却には代償が伴う。この原理は、情報の消去（これは不可逆過程）には、必然的に熱の発生を伴うというものである。言い換えると、論理的不可逆性には必ず熱力学的不可逆性が含まれる。1 ビットの情報を取り除くためには、少なくとも  $kT \ln 2$  を生成しなければならない [39, 40]。ランダウアーの原理については、統計力学の項で再び説明する。

先ほど、第二法則は、蒸気機関や冷蔵庫、情報処理装置などの現実の機関の効率に基本的な限界を設けていることを示した。誰もが知っているように、本物のエンジンは熱を発し、本物の冷蔵庫やコンピュータは仕事をするために電力を必要とする。第二法則は、熱を利用してどの程度の仕事ができるかを示すものである。ある平衡状態から別の平衡状態に移行する際のエントロピーの増加は、散逸と熱の生成に関連しており、これは**不可逆性**という重要な概念と密接に関連している。閉鎖系におけるある操作が、外部からの入力なしに、その操作が行われる前の状態に戻ることを不可能にする場合、その操作は不可逆的である。不可逆性は、熱の生成と常に関連している。なぜなら、熱は他のエネルギーに自由に変換することができないからである（一方、他のエネルギーは常に熱に変換することができる）。ある系に仕事をすれば、その系のエントロピーを減少させることができるが、その仕事をするためには、他の系（またはその系の環境）のエントロピーを同じかそれ以上に増加させなければならない。

熱力学の理論だけでは、エントロピーと情報は関連しない。これは、結果を微視的な理論で解釈した場合にのみ生じるものであり、その場合、温度は粒子の位置の不確かさやインコヒーレンス（支離滅裂さ）に関係していると解釈することができる。そのためには、次項で行うような統計力学の議論が必要となる。

第二法則には、運用面でも哲学面でも重要な、もう一つの基本的な側面がある。第二法則の深い意味は、「時間の矢」を定義すること、つまり、過去と未来を区別することができることを示している。このことは、物理学の基本的な微視的法則が時間反転不変であることと対照的である（地球上で見られるような通常の条件では、ごくまれにしか見られないいくつかのエキゾチックな相互作用を除いて）。ミクロの世界の基本的なプロセスの動画を見ると、それが前に走っているのか後ろに走っているのか区別はできない。一方、マクロ的な事象の動画を見ると、煙が巻きながら登っていたり、コップの水がこぼれたり、パン生地をこねたりといった不可逆的な動作を確認することは難しくなく、それによって自分が順走しているのか逆走しているのかを簡単に

判断することができる。もっと形式ばって言えば、時間の流れがわからなくても、無作為にいくつかの系を選び、その系のエントロピーを  $t_1, t_2, \dots$  の時点で測定することができる。エントロピーが増大する方向は、時間に沿って進んでいる方向である。注意すべき点は、第二法則の定式化にあたっては、時間の方向性を演繹的に定義したわけではないことである。第二法則は、原子論やその他の物理法則を一切無視して、勝手に時間の方向性を決めてしまう。

熱力学の第二法則は、異なる巨視的状態のエントロピーの差についてのみ述べている。エントロピーの絶対的な尺度は、熱力学の第三法則によって与えられる。この法則は、系の温度が絶対零度に近づくとき、エントロピーがゼロになる。つまり

$$T \rightarrow 0 \quad \Rightarrow \quad S \rightarrow 0. \quad (2.7)$$

である。 $T = 0$  のとき、熱はゼロになり、古典的には原子の動きがないことに対応し、エネルギーは可能な限り一番低い値をとる。量子論では、そのような最もエネルギーの低い「基底状態」も存在することが知られているが、系の基底状態が縮退している場合、絶対零度でのエントロピーはゼロでない定数に近づくことになる。締めくくりとして、熱力学の法則は適用範囲が広く、それらを明解に裏付ける豊富な現象学があることを強調しておく。

## 2.2 自由エネルギー

物理学者が特に注目するのは、(ヘルムホルツの) **自由エネルギー** と呼ばれるもので、 $F$  と表記される。これは、仕事をするために利用できるエネルギーの量を定義するもので、非常に重要な量である。次項で述べるように、自由エネルギーは、熱力学と統計力学の関係を確立する際に、特にエントロピーの微視的な定義を確率の観点から導き出す上で、中心的な役割を果たす。

自由エネルギーは次のように定義される。

$$F \equiv U - TS. \quad (2.8)$$

これは、微分形式では次のようになることを意味する。

$$dF = dU - TdS - SdT, \quad (2.9)$$

式 (2.3) を用いると次のように書くことができる。

$$dF = -PdV - SdT. \quad (2.10)$$

つまり、気体の自由エネルギーを表す自然な独立変数は、体積と温度である。

自由エネルギーの意味を簡単に考えてみよう。一定の温度  $T_0$  に保たれた熱浴  $A'$  に熱的に接している系  $A$  を考える。系  $A$  が熱源から熱  $dQ$  を吸収したとする。系と熱浴を合わせた全体  $A^0 = A + A'$  を閉鎖系と呼ぶことがある。 $A^0$  では、第二法則  $dS^0 = dS + dS' \geq 0$  により、エントロピーは増加することしかできない。熱浴  $A^0$  の温度は一定であり、その吸収熱は  $-dQ$  であるので、 $T_0 dS' = -dQ$  と書くことができる。系  $A$  に適用された第一法則から、 $-dQ = -dU - dW$  が得られるので、 $T_0 dS' = -dU - dW$  の式を  $T_0 dS + T_0 dS' \geq 0$  に代入し、 $-dU + T_0 dS \geq dW$  が得られる。系  $A$  が一定の温度に保たれているので、左辺はちょうど  $-dF$  になり、次のことがわかる。

$$-dF \geq dW. \quad (2.11)$$

熱浴に接している系ができる最大の仕事は  $(-dF)$  である。系のパラメータを固定にしたまま、すなわち  $dW = 0$  とすると、 $dF \leq 0$  となり、熱浴に結合した系では自由エネルギーは減少するしかなく、結果的に熱平衡状態では自由エネルギーは最小となる。これは、平衡状態で最大となるエントロピーと比較されるべきことである。

第二法則は、異なる種類のエネルギーがどのように変換されるかを示すものと考えることができる。孤立系では、仕事を熱に変えることはできるが、熱を仕事に変えることはできない。ミクロの視点で見ると、光のような「組織化された」エネルギー形態は、粒子のランダムな運動のような「組織化されていない」エネルギー形態に変換することができるものの、その逆はできない。

式 (2.10) から、気体の圧力とエントロピーは、自由エネルギーの偏微分として書くことができる。

$$P = \left( \frac{\partial F}{\partial V} \right)_T, \quad S = \left( \frac{\partial F}{\partial T} \right)_V. \quad (2.12)$$

つまり、熱平衡状態にある系では、エントロピーは状態変数であり、閉じた経路を可逆的にたどると同じ値に戻るということがわかる（熱などの他の量はこの性質を満たさないが）。変数  $P$  と  $S$  は従属変数である。このことは、2つの二次導関数

$$\frac{\partial^2 F}{\partial T \partial V} = \frac{\partial^2 F}{\partial V \partial T}, \quad (2.13)$$

を等しくすることで得られる

$$\left( \frac{\partial P}{\partial T} \right)_V = \left( \frac{\partial S}{\partial V} \right)_T. \quad (2.14)$$

のマクスウェルの関係から明らかである。

### 3 統計力学

物質の塊を扱う際には、個々の分子を認識することはできないので、これまで述べてきたような統計的な計算方法を採用せざるを得ず、すべての動きを微積分で追うような厳密な力学の方法は放棄しなければなりません。

J.C. マクスウェル

私たちは、力学の統計的分野に関連するより明白な命題のいくつかを推論するという、より控えめな目的で満足せざるを得ません。ここでは、自然界の事実との一致について、間違いは許されません。

J.W. ギブス

統計力学とは、個々の粒子の位置や速度などの微視的な状態が未知であっても、その背後にある微視的な物理法則を用いて、物理系の巨視的な挙動を説明するものである。19世紀後半、統計力学の発展に大きく貢献したのは、マクスウェル、ボルツマン、ギブスだった [45, 9, 25]。未解決の問題のうちの一つは、熱力学の法則を導き出すこと、特にエントロピーという概念を微視的に定義することだった。もう一つの目的は、輸送現象など熱力学だけでは計算できない現象を理解することだった。この項では、情報理論との関連性を強調する目的のために、簡単に、そしてやや偏った形で紹介する。私たちの主な目的は、ギブスによるエントロピーの有名な表現  $S = -\sum_i p_i \ln p_i$  の起源を示すことである。そして、これは後にシャノンが情報の定義に用いることになる。



### 3.1 定義と前提

予測問題と解釈問題を区別せず、1つの形式主義で両方を行おうとしたために、かなりの意味上の混乱が生じました。

T.S. J ジェインズ

統計力学は、気体中の原子や格子上のスピンのように、多くの自由度を持つ系を対象とする。例えば、気体が入っている容器の中のすべての粒子の位置と速度である系の微視的状态という観点から考えることができる。可能な微視的状态の空間を**位相空間**と呼ぶ。 $N$  個の粒子を持つ単原子気体の場合、位相空間は  $6N$  次元となる。これはニュートン力学の下では、各粒子の未来の状態を決定するために、測定しなければならない3つの位置と3つの速度があることに対応する。このように、系全体の微視的状态は、位相空間の一点に対応している。

統計力学では、微視的状态が存在することはわかっている、その実際の値についてはほとんどわからないという前提がある。私たちが持っている唯一の情報は、巨視的な量から得られる。巨視的な量とは、全エネルギー、温度、体積、圧力、磁化などひとかたまりの特性のことである。私たちは無知であるがゆえに、微視的状态を統計的に扱わなければならない。しかしながら、巨視的な量の知識と微視的な状態が従う物理法則があれば、微視的な状態を制約し、他の方法では明らかにならない巨視的な変数間の関係を計算することができる。巨視的な変数の値が固定されると、通常、その変数と互換性のある微視的な状態のサブセットのみが存在し、これを**到達可能な状態** (accessible state) と呼ぶ。到達可能な状態の数は通常膨大となるが、この数の違いは非常に重要な意味を持つ。この章では、簡単のために微視的状态のセットを離散的に仮定するが、この形式は連続的なケースにも簡単に一般化できる。

統計力学の第一の基本的な仮定は、平衡状態にある閉鎖系は、その到達可能な状態のいずれかになる確率が先験的 (a priori) に等しいというものである。熱的に接していたり、粒子数が一定でないなど、閉じていない系の場合は、到達可能な状態のセットが異なり、その確率を計算する必要がある。いずれの場合も、許容される微視的状态に対して特徴づけられる確率分布を持つ系の**統計集団** (アンサンブル) と関連付けられる。トルマン [60] は、アンサンブルの概念を明確に説明している。

アンサンブルを統計的な目的で使用する場合、個々の系の区別を維持する必要があることに注意する必要がある。なぜなら、我々は単に、位相空間の異なる領域に対応する異なる状態にある、ある時点での系の数にのみ興味があるからである。さらに、統計的な観点から、位相空間のある領域にある状態から別の領域にある状態に移行する際に、そのような異なる状態にある系の数が連続的に変化すると考えられるように、別々のメンバーの十分に大きな集団を含むアンサンブルを使用したいと考えていることに注意すべきである。したがって、この目的のためには、任意の時間におけるアンサンブルの状態は、代表点が位相空間上に分布する密度  $r$  によって適切に規定されたとみなすことができることが明らかである。

統計力学の2つ目の前提は**エルゴード性**と呼ばれ、時間平均はアンサンブル平均に一致すると言われている。つまり、一方では、系を構成するすべての粒子のすべての微視的な変数の決定論的な動きを追うことで、時間平均を取ることができる。反対に、ある瞬間では発生する確率で重み付けをされたとりうるすべての到達可能な状態の平均を取ることができる。エルゴード仮説では、この2つの平均値は同じであるということを主張している。この仮説の制約については、後ほど非線形力学の項の中で振り返る。

### 3.2 磁気スピン系の微視的状態の計算

以下の例では、等分配の仮定と簡単な計算の議論によって、微視的状態の分布を導き出すことができることを示している。また、熱力学的（つまり、 $N \rightarrow \infty$  の極限）には、微視的状態の分布が極端に狭くなることも示している。上向きか下向きかに対応する 2 つの値  $s_j = \pm 1$  しかとれない  $N$  個の磁気スピンの系を考えてみよう（しばしば**イジングスピン**と呼ばれる）。可能な配置の総数は  $2^N$  になる。便宜上、 $N$  は偶数で、スピンは相互作用しないと仮定する。次に、これらのスピンを上向きの磁場  $H$  の中に置き、それぞれの可能なエネルギーの値に一致するスピンの構成がいくつあるかを問う。それぞれのスピンのエネルギーは  $e_j = \mp \mu H$  であり、相互作用しないため、系の全エネルギーは単に各スピンのエネルギーの合計となる。 $k$  個のスピンが上を向き、 $N - k$  個のスピンが下を向く配置の場合、全エネルギーは  $\varepsilon_m = 2m\mu H$  ( $m \equiv (N - 2k)/2$ 、 $-N/2 \leq m \leq N/2$ ) と書ける。 $\varepsilon_m$  の値は、 $-N\mu H \leq \varepsilon_m \leq N\mu H$  に制限され、隣接する 2 つのエネルギー準位の差は、1 個のスピンの反転に対応して、 $\Delta\varepsilon = 2\mu H$  となる。エネルギー  $\varepsilon_m$  を持つ微視的配置の数は次のようになる。

$$g(N, m) = g(N, -m) = \frac{N!}{(\frac{1}{2}N + m)!(\frac{1}{2}N - m)!}. \quad (3.1)$$

状態の総数は、 $\sum_m g(N, m) = 2^N$  となる。熱力学系の場合、 $N$  は非常に大きいため、スターリングの公式で階乗を近似することができる。

$$N! \cong \sqrt{2\pi N} N^N e^{-N+\dots} \quad (3.2)$$

基礎的な数学によれば、 $N$  が大きいとき、二項分布は正規分布に近似できるため、次のように書ける。

$$g(N, m) \cong 2^N \left( \frac{2}{\pi N} \right)^{\frac{1}{2}} e^{-2m^2/N}. \quad (3.3)$$

この系については後ほど説明するが、ここでは単に、 $N$  が大きいと分布が急激なピークを持つことを示したいだけである。大雑把に言えば、分布の幅は  $\sqrt{N}$  で大きくなり、ピークの高さは  $2^N$  で大きくなるので、 $m = 0$  付近の状態の縮退が急激に増加する。例えば、 $g(50, 0) = 1.264 \times 10^{14}$  となるが、 $N \approx N_A$  の場合、 $g(N_A, 0) \cong 10^{10^{22}}$  となる。次の項では、この例に従って、熱平衡状態にあるスピン系の磁化を計算してみることにする。

### 3.3 マクスウェル-ボルツマン-ギブス分布

マクスウェルは、熱平衡状態、つまり、一定の温度  $T$  に保たれた熱源と熱的に接触している状態にある系の確率分布  $p_i$  の式を初めて導出した。この結果は、後にボルツマンやギブスによって一般化された。外力が加わっていない理想気体の平衡分布関数は、位置にも時間にも依存せず、個々の粒子の速度にのみ依存するはずである。一般的には、粒子間の相互作用を考慮に入れる必要がある。確率論的な計算によって十分に正当化される単純化された仮定は、2 つの粒子が一度に相互作用する過程は、3 つ以上の粒子が相互作用する過程よりもはるかに普遍的であるというものです。2 つの粒子の速度が相互作用する前に独立していると仮定すると、速度  $v_1$  と  $v_2$  を持つ同時確率は、それぞれの粒子単独の確率の積として書くことができる。つまり、 $p(v_1, v_2) = p(v_1)p(v_2)$  を意味する。相互作業した後も同様に、 $p(v'_1, v'_2) = p(v'_1)p(v'_2)$  と書ける。時間に依存しない平衡状態では、前後の確率は同じでなければならず、 $p(v_1, v_2) = p(v'_1, v'_2)$  となる。これらの条件を相互作用の前後でどのようにつなぎ合わせるか。重要な点は、相互作用の間に保存され

る保存量があり、平衡分布関数はその保存量にのみ依存するということである。分布関数の均質性と等方性は、分布が依存する唯一の関数として、粒子の全エネルギーを選択する。この状況でのエネルギー保存は、 $\frac{1}{2}mv_1^2 + \frac{1}{2}mv_2^2 = \frac{1}{2}mv_1'^2 + \frac{1}{2}mv_2'^2$  という単純な記述に要約される。これらの関係から、マクスウェルはよく知られた熱平衡速度分布を導き出した。

$$p_0(v) = n \left( \frac{m}{2\pi T} \right)^{3/2} e^{-mv^2/2kT}. \quad (3.4)$$

この分布は、正規分布である。先ほど見たように、マクスウェルがこの理論を導き出すためには、物理学の基本法則からは導き出せない、もっともらしいいくつかの仮定をしなければならなかった。ボルツマンはこの結果を一般化して、外部の保存力の影響を含めるようにした。その結果、(3.4) の運動エネルギーは、運動エネルギーだけでなく、位置エネルギーも含めた全保存エネルギーに置き換えられた。

マクスウェルの結果をボルツマンが一般化したことにより、熱平衡状態にある一般的な系の確率分布  $p_i$  が次のように与えられることが明らかになった。

$$p_i = \frac{e^{-\varepsilon_i/T}}{Z}. \quad (3.5)$$

$Z$  は確率の保存を確実にするための規格化係数で、すなわち  $\sum_i p_i = 1$  である。これは次のことを意味する。

$$Z \equiv \sum_i e^{-\varepsilon_i/T}. \quad (3.6)$$

$Z$  は**分配関数**と呼ばれる。ボルツマン分布は**カノニカルアンサンブル**を記述するものであり、系が熱平衡状態にあり、環境とエネルギーを交換しているあらゆる状況に適用される。このことは、エネルギーが一定の孤立した系に適用される**ミクロカノニカルアンサンブル**や、エネルギーと粒子の両方を環境と交換している系に適用される**グランドカノニカルアンサンブル**とは対照的である<sup>3</sup>。ボルツマン分布の威力を説明するために、外部磁場中の格子上的イジングスピンの熱分布の例を簡単に振り返ってみよう。(3.2) 項で指摘したように、1 個のスピンのエネルギーは  $\pm\mu H$  である。ボルツマン分布によると、スピンの上向きまたはスピンの下向きの確率は、次のようになる。

$$p_{\pm} = \frac{e^{\mp\mu H/T}}{Z}. \quad (3.7)$$

磁場に反比例するスピンはエネルギーが最も低く、そのため有利となる。これにより 磁場に依存した平均磁化  $m_H$  (1 スピンあたり) は、次のようになる。

$$m_H = \langle \mu \rangle = \frac{\mu p_+ + (-\mu) p_-}{p_+ + p_-} = \mu \tanh \frac{\mu H}{T}. \quad (3.8)$$

この例は、統計力学を用いて、熱力学だけでは得られない巨視的な変数間の関係を確立することができることを示している。

### 3.4 自由エネルギー再考

2.2 項の熱力学の説明では、式 2.8 で定義される自由エネルギー  $F$  の概念を紹介し、熱浴と熱的に接している系、つまり一定の温度  $T$  に保たれている系では、自由エネルギー  $F$  が中心的な役割を果たしていることを

<sup>3</sup> ギブスは、ボルツマンの結果を粒子の数が固定されていない状況に拡張し、**化学ポテンシャル**を導入した。この指数分布は、その複雑な歴史から、ギブス、ボルツマン、ボルツマン-マクスウェル、ボルツマン-ギブスなど、さまざまな名称で呼ばれている。

論じた。前項では、式 3.6 で定義される分配関数  $Z$  の概念を紹介した。すべての熱力学量がこの関数から計算できるため、分割関数  $Z$  の重要性は、規格化因子としての役割をはるかに超えている。自由エネルギーは特に重要で、その関数形は確率の観点からのエントロピーの定義に直接つながるからである。これにより、熱力学量を統計力学で定義された量に直接結びつけることができる。これは、自由エネルギーと分配関数の関係を次のように仮定<sup>4</sup>することによって行われる。<sup>5</sup>

$$F = -T \ln Z, \quad (3.9)$$

あるいは、 $Z = e^{-F/T}$  である。この定義から、例えば式 (2.12) を用いて、すべての熱力学量を計算することができる。次に、統計力学におけるエントロピーの表現を、確率の観点から導出する。

### 3.5 ギブスエントロピー

自由エネルギーの定義式 ((2.8) より、

$$S = \frac{U - F}{T}. \quad (3.10)$$

である。式 (3.9) と式 (3.5) から次のようになる。

$$F = \varepsilon_i + T \ln p_i. \quad (3.11)$$

なお、右辺の 2 つの項が  $i$  に依存していても、自由エネルギー  $F$  は  $i$  に依存しない。内部エネルギーの平衡値は、定義により

$$U = \langle \varepsilon \rangle \equiv \sum_i \varepsilon_i p_i. \quad (3.12)$$

である。これらの  $S$ 、 $F$ 、 $U$  の式と、 $F$  が  $i$  に依存しないこと、 $\sum_i p_i = 1$  であることを利用して、エントロピーを確率  $p_i$  で書き換えると、有名なエントロピーの式が得られる。

$$S = - \sum_i p_i \ln p_i. \quad (3.13)$$

この式は通常、ギブスエントロピーと呼ばれる。<sup>6</sup>

全エネルギーが固定されている特殊なケースでは、 $w$  個の異なる（到達可能な）状態はすべて、先験的に等しい確率  $p_i = p = 1/w$  である。ギブス式に代入すると、到達可能な状態の数を表す式が得られるが、これは元々ボルツマンによるもので、彼の墓石に刻まれている。

$$S = \ln w. \quad (3.14)$$

エントロピーは、到達可能な状態の数に対して対数的に大きくなることを強調しておく<sup>7</sup>。2 つの状態のいずれかになることができる 1 個の粒子からなる系を考えてみよう。等分配を仮定すると、エントロピーは

<sup>4</sup> 自由エネルギーのような巨視的な量を微視的な表現と同一とみなしてしまえば、ほかの量も当然それに従うことになる。どの表現を同一化の出発点とするかは非常に恣意的である。その正当性は、よく知られた熱力学的な関係が回復されるべきであるという意味で、**後天的なもの** (*a posteriori*) である。

<sup>5</sup> ボルツマン定数  $k$  は、エネルギーと温度を関係づける。通常の単位では  $1.4 \times 10^{-23} \text{ J/K}$  であるが、ここでは 1 として、エネルギーや温度の便利な単位を選んだ。

<sup>6</sup> 量子論では、この式は  $S = -\text{Tr } \rho \ln \rho$  ( $\rho$  は系の密度行列) に置き換えられる。

<sup>7</sup> この数字は圧倒的に大きい。室温で 1 ミリカロリーの差がある 2 つの微視的な状態を想像してみよう。エントロピーの差は  $\Delta S = -\Delta Q/T = 10^{-3}/293 \approx 10^{-5}$  となる。したがって、到達可能な状態の数の比率は、 $w_2/w_1 = \exp(\Delta S/k) \approx \exp(10^{18})$  という、とても大きな数字となる。

$S_1 = \ln 2$  となる。アボガドロ数  $N \sim 10^{23}$  の粒子を持つ系では、 $2^N$  個の状態があるため、独立性を仮定するとエントロピーは  $S_N = \ln 2^N = NS_1$  という、非常に大きな数になる。系がそのエントロピーを最大化する傾向は、確率論的表現となる。ある状態にある半分の粒子の状態の数と、もう一方の半分の粒子の状態の数は、すべての粒子が同じ状態にある数よりも膨大に多く、系を自由にしておくと、最も確率の高い到達可能な状態に緩和される。気体粒子の状態は、その許容される位置（すなわち容器の容積）だけでなく、その許容される速度の範囲にも依存する。容器が熱い場合は容器が冷たい場合よりもその範囲が大きくなる。つまり、理想気体の場合、エントロピーは温度の対数に比例して増加することがわかる。この法則が確率的なものであるということは、系が極めてありえない初期状態に戻ることが完全に不可能ではないということの意味している。ポアンカレは、それが必ず起こることを示し、再帰時間の推定値を与えた（巨視的な系では、宇宙の寿命よりもはるかに大きい）。

ギブスエントロピーは、統計力学での起源から超越している。これは、状態  $\{\psi_i\}$  と与えられた確率分布  $\{p_i\}$  を持つ任意の系を記述するために使用できる。これを実現したのは、通常、シャノン [54] の功績とされているが、先行していたのは、シラード、ナイキスト、ハートリーなどである。シャノンは、エントロピー  $S$  との類推によって、情報は次のように定義できると提唱した。

$$H \equiv - \sum_i p_i \log_2 p_i. \quad (3.15)$$

情報理論では、対数の底を 2 とし、ボルツマン定数を落とすのが一般的である<sup>8</sup>。2 進数を扱うときの単位としては対数の底が 2 であることが自然であり、この場合のエントロピーの単位は**ビット**と呼ばれる。一方、自然対数を使う場合、単位は**ナット**と呼ばれ、1 ナット = 1.443 ビットという換算になる。例えば、5 ビットのメモリ（これは 5 個のイジングスピンの系と同じ）は、 $N = 2^5$  の状態を持つ。さらなる制約がなければ、これらの状態（メッセージ）はすべて等しい確率となる。つまり、 $p_i = 1/N$  なので、情報量は  $H = -N \frac{1}{N} \log_2 \frac{1}{N} = \log_2 2^5 = 5$  ビットとなる。同様に、100 億個の塩基対を持つ DNA 分子を考えてみよう。それぞれの塩基対は、4 つの組み合わせ（A-T、C-G、T-A、G-C）のいずれかになる。分子は先験的に  $4^{10^{10}}$  通りの配置が可能なので、（独立性を仮定した）単純計算の情報量は  $H = 2 \times 10^{10}$  ビットとなる。この定義のもつ対数的な性質は、ビットの追加の下での情報の加法的な特性を望むならば、避けることはできない。先ほどのスピンの例において、さらに 3 ビットの文字列を追加すると、状態の総数は  $N = N_1 N_2 = 2^5 \times 2^3 = 2^8$  となり、 $H = H_1 + H_2 = 8$  という結果になる。第一原理となる関係や制約を追加すると、独立した配位の数が減り、結果的に  $H$  はさらに小さくなる。

第 5 章で述べるように、情報の定量的な定義とその応用は、従来の熱力学や統計力学の限られた起源と範囲を超越しており、また、シャノンの当初の目的である通信チャネルの特性を記述することも同じく超えてしまっている ([11] 参照)。

## 4 非線形力学

自然界のシステムの現在の状態は、明らかに前の瞬間の状態の結果であり、ある瞬間にこの宇宙の実体のすべての関係を理解する知性を考えれば、過去や未来のどの時点においても、これらすべての実体のそれぞれの位置、運動、一般的な影響を述べることができる。

ピエール＝シモン・ラプラス (1776)

<sup>8</sup> 我々の慣習では  $k = 1$  のため、 $H = S / \ln 2$  である

私たちが気づかないような非常に小さな原因が、私たちが見過ごせないような大きな効果を生み出し、その効果が偶然によるものだと言うのである。

アンリ・ポアンカレ (1903).

素朴な見方をすれば、統計力学はニュートン力学の決定論と矛盾するように見える。任意の初期状態  $x(0)$  (位置と速度のベクトル) に対して、ニュートンの法則は  $x(0)$  を将来の状態  $x(t) = \phi^t(x(0))$  に対応づける力学系  $\phi^t$  (微分方程式の集合) を定義する。これは完全に決定論的である。ラプラスの有名な言葉にあるように、機械的なものがニュートンの法則に従うのであれば、なぜ完全な確実性を統計的に議論する必要があるのか。ラプラスは彼自身の質問に部分的に答えている。

... しかし、事象の発生に関与する様々な原因に対する無知とその複雑さ、そして分析の不完全さが相まって、大多数の現象について (天文学と同様の) 確実性を得ることができないのだ。このように、私たちにとって不確かなもの、多かれ少なかれ可能性のあるものがあり、私たちはその可能性の度合いを決定することで、それらを知ることの不可能性を補おうとしている。このように、人間の心の弱さのおかげで、数学の中でも最も繊細で独創的な理論の一つである、偶然性や確率の科学が成り立っているのだ。

ラプラスは、統計的な記述の必要性を明確に理解していたが、その時点では、非線形力学の重要性を十分に認識していなかった。ポアンカレが後に示したように、人間の不確定性 (あるいは量子力学) がなくても、ニュートンの法則がカオス的な動力学を持つ微分方程式を生み出すとき、我々は必然的に自然の確率的な記述にたどり着く。ポアンカレは、天体力学の三体問題を研究する過程でこのことを発見したが、彼が見つけた答えは決定論的なラプラス的宇宙と統計力学との調和に関連するものであることがわかった。

## 4.1 エルゴード仮説

以前の章で述べたように、ボルツマンの統計力学の定式化における重要な基礎の 1 つがエルゴード仮説である。大雑把に言えば、ある軌道は最終的に系の到達可能なすべての微視的状态、例えばエネルギー保存に適合するすべての状態を通過するだろうという仮説である。平衡状態では、軌道が状態空間の特定の領域に滞在する平均時間は、その領域に含まれる到達可能な状態の数に比例する。エルゴード仮説が正しければ、時間平均はアンサンブル平均に等しく、等分配は有効な仮定である。

エルゴード仮説は大きな議論を呼んだが、それには理由があった。それは一般的には真ではない。1947 年、ロスアラモス研究所でフェルミ、パスタ、ウラムの 3 人がエルゴード仮説を検証するためにコンピュータを使った最初の数値実験を行った。彼らは、非線形バネで結ばれた質量系をシミュレーションした。彼らは質量のうちの 1 つを擾乱し、その擾乱が他のすべての質量に急速に伝播して平衡することを期待し、長い時間の後にすべての質量が多かれ少なかれランダムに揺れていることを発見した。代わりに、外乱が明瞭に残っていることに驚いた。系の中を伝播していくにもかかわらず、正体を保ち、比較的短時間で系は初期状態に近い状態に戻った。実は、彼らは局所的だが非常に安定した動作障害であるソリトンと呼ばれる現象を再発見したのであった。ソリトンを支持する非線形系には多くの例がある。そのような系は、すべての到達可能な状態になる確率が等しくないため、エルゴード的ではない。

このような問題があるにもかかわらず、統計力学が非常にうまく機能していることがわかっている例はたくさんある。剛体球気体のように、いくつかのケースではエルゴード仮説が実際に証明されている。しかし、一般的にはそうではない。統計力学の根拠は、ほとんどが経験的なものである。少なくとも非常に高い近似度で

機能することがわかっている。その後の研究により、典型的な状況は当初の想像よりもはるかに複雑であることが明らかになった。ある軌道では、到達可能な位相空間の大部分を多かれ少なかれランダムにさまようが、KAM（コルモゴロフ-アーノルド-モザー）トーラスと呼ばれる特定の領域に入るのを阻止される。ほかの初期条件では、規則的な動きをする軌跡が得られ、KAM トーラスの軌跡上に位置する。KAM トーラスは互いに分離しており、完全に到達可能な位相空間よりも低い次元を持っている。そのような KAM トーラスは、エネルギー保存則の他に、初期条件や他のパラメータに依存する保存則が存在する状況に対応している<sup>9</sup>。ソリトンはその例で、解が幾何学的に孤立したパルスとして解釈できる。

現在、非線形力学におけるエルゴード性の研究は非常に多く行われている。これを決定的に解決する正式な定理はないものの、これらの研究で蓄積された知識によれば、隠された対称性を持たない非線形系では、相互作用する成分の数が増えて非線形性が強くなると、一般的な挙動としてカオス的な振る舞いをするようになると言われている。KAM トーラスが縮小すると、そこにトラップされる初期条件が少なくなり、排除される領域も小さくなる。エルゴード仮説はますます良い近似となり、典型的な単一の軌道はほとんどすべての到達可能な状態に達することができ、等分配は良い仮定となる。問題は、ソリトンのような現象を支える対称性がどのように隠されているかを理解することである。エルゴード性が良い仮定であるための必要条件と十分条件は、依然として活発な研究分野である。

## 4.2 カオスと予測の限界

カオスの発見により、ボルツマンの確率の使い方は、彼が考えていた以上に正当なものであることが明らかになった。運動がカオスである場合、無限小に近い 2 つの軌道が指数関数的な速度で分離する [44, 55, 12, 58]。これは、基礎となる非線形力学の幾何学的特性である。線形的な観点から見ると、その動力学は局所的に不安定である。このことを正確に説明するために、無限小のベクトル  $\delta x(0) = x(0) - x'(0)$  によってあらかじめ分離されている 2 つの  $N$  次元の初期状態  $x(0)$  と  $x'(0)$  を考える。動力学系が微分可能であれば、分離状態は次のようになる。

$$\delta x(t) = D\phi^t(x(0))\delta x(0), \quad (4.1)$$

ここで、 $D\phi^t(x(0))$  は、初期条件  $x(0)$  で評価された力学系  $\phi^t$  の微分である。任意の固定時間  $t$  と初期条件  $x(0)$  に対して、 $D\phi^t$  は単なる  $N \times N$  の行列であり、これは単なる一次方程式である。運動がカオスであれば、図 3 が示すように、分離ベクトル  $\delta x$  の長さは、少なくとも 1 つの方向において、 $t$  とともに指数関数的に成長する。この図は、カオスが予測不可能な状態に陥る根本的な原因が、近くの軌道の発散にあることを示している。完全な測定は状態空間の一点に対応するものの、実際の測定は不正確であり、不確実性の雲が発生する。真の状態は、クラウド内のどこかにあるかもしれない。ここでローレンツ方程式（3 つの非線形微分方程式が結合した単純な系 [44]）について示すように、初期測定の不確かさは、最初は区別がつかないほど近くにある 1 万個の赤い点で表されている。一つの軌跡が、参考として水色で表示されている。各点が方程式の作用を受けて動くと、雲は細長い糸のように引き伸ばされ、それが何度も折り重なって、アトラクター全体に点が多かれ少なかれランダムに混ざるようになる。最終的な状態がアトラクターのどこにあってもおかしくないもので、予測は不可能になった。一方、規則的な動きの場合は、すべての最終状態が近接したままである。このことを情報理論的に考えてみよう。カオス的な動きの場合、最初は線形的な比率で情報が失われ、最終的には

<sup>9</sup> エネルギーを保存しニュートンの法則に従う力学系は、KAM トーラスの存在の原因となる特殊な性質を持っている。散逸系には通常、軌道が収束する状態空間の部分集合であるアトラクターが存在する。エネルギー保存系はアトラクターを持たず、規則的な軌道とカオス的な軌道が混在していることが多い。



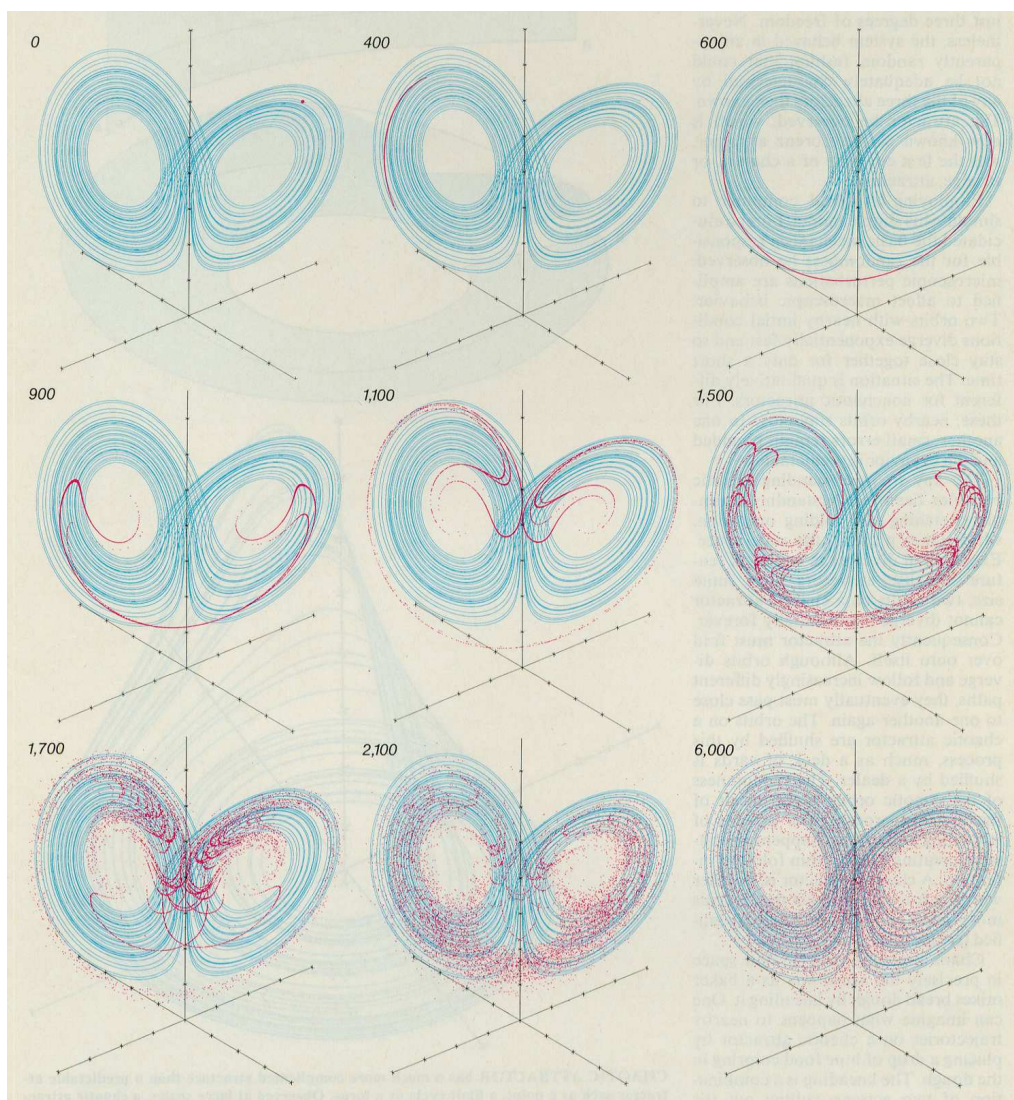


図3 ローレンツ方程式の近傍軌道の発散。説明は本文を参照のこと。

すべての情報が失われる。規則的な動きの場合は、情報の損失は比較的小さくなる。図の上の数字は、ローレンツ方程式の自然な時間単位の  $1/200$  の単位である ([12] より)。

しかしながら、同時にこの運動は全体的に安定しており、位相空間の有限体積内に収まっていることもある。これは、伸ばしたり折ったりすることで実現している。非線形力学は、パン屋さんがパンを作るように、



局所的に伸ばしたり、全体的に折ったりして、位相空間を練っていく。最初は近くにあった2つの軌道が、後になってかなり離れてしまったり、さらに後になって再び近くなったりすることがある。この性質を**混合**という。より正式には、動力学は与えられた集合  $\Sigma$  とサポート  $\Sigma$  を持つ不変測度<sup>10</sup>  $\mu$  の上で混合され、任意の部分集合  $A$  と  $B$  に対して

$$\lim_{t \rightarrow \infty} \mu(\phi^t B \cap A) = \mu(A)\mu(B). \quad (4.2)$$

となる。直感的には、このことは  $B$  がフローによって  $\Sigma$  全体に広がっていることを意味する。 $A$  の内部で  $B$  を起点とする点を見つける確率は、 $B$  の元の確率を  $A$  の確率で加重したものに過ぎない。幾何学的には、 $B$  の未来の軌道が  $\phi^t$  の伸縮作用によって  $\Sigma$  全体に細かく「混合されている」場合にのみ、このことが起こる。

混合はエルゴード性を意味するので、 $\Sigma$  上で混合している任意の力学系は  $\Sigma$  上でもエルゴード性を持つことになる。ただし、 $\Sigma$  が到達可能な状態の集合である場合にのみ、エルゴード仮説を満たす。その必要はない。このように、ある系がカオス的な動力学の軌道を持っているからといって、必ずしもエルゴード仮説を満たすとは限らない。位相空間にある有限体積の部分集合は、例えば KAM トーラスのように、規則的な動きをすることができないことがある。

それにもかかわらず、カオス動力学は統計力学に大きな影響を与えた。力学系がエルゴード的であるが混合ではない場合<sup>11</sup>、微視的状态を測定することにより、ラプラスが提案したようにそのすべての微視的状态の位置と速度を測定して、詳細な長距離予測を行うことが原理的に可能である。一方、混合であれば、微視的状态の初期値を高い（しかし有限の）精度で知っていたとしても、その情報はすべて漸近的に失われ、統計力学は避けられなくなる<sup>12</sup>。

### 4.3 予測可能性の定量化

予測可能性の定量化には、情報理論を用いることができる [55]。議論を始めるにあたり、均一な分解能の目盛り  $\epsilon$  を持つ測定器を考える。例えば、定規の場合、 $\epsilon$  は隣り合う目盛りの間の距離である。このような測定器が力学系の  $N$  個の実変数のそれぞれに割り当てられている場合、これらの測定器の目盛りは位相空間の**分割  $\Pi$** を誘導し、これはラベル  $C_i$  が付けられた重ならない  $N$  次元立方体の集合であり、これを測定の結果と呼ぶことにする。測定は系の状態が所定の立方体  $C_i$  にあることを決定する。トランジェント（過渡運動）を消滅させ、外部からの摂動がない漸近運動に限定して考えると、運動はある集合  $\Sigma$  (一般的には初期条件に依存する) に限定されていると仮定することになる。そして、ある測定値の出現頻度  $p_i$  を測定することで、その測定値の漸近確率を計算することができる。また、その運動が  $\Sigma$  上でエルゴード的であるならば、 $p_i = \mu(C_i)$  となるような不変測度  $\mu$  が存在することがわかる。不変測度  $\mu$  を知っていながら、系の状態について他に何も知らない人にとって、測定を行うことで得られる平均情報量が、まさにエントロピー

$$I(\epsilon) = - \sum_i p_i \log p_i. \quad (4.3)$$

<sup>10</sup>  $A$  が  $\Sigma$  の任意の部分集合のとき、 $\mu(A) = \mu(\phi^{-t}(A))$  という条件を満たす場合、測度はダイナミクス  $\phi^t$  に関して集合  $\Sigma$  上で不変である。多くの不変測度がありえるが、私たちが終始念頭に置いているのは、時間平均に対応する速度である。

<sup>11</sup> エルゴード的ではあるが混合ではない系の簡単な例として、解が非合理的に関連した周波数を持つ2つの正弦波の和である力学系が挙げられる。

<sup>12</sup> 例外として、カオス状態であっても位相不変性を示す系もある。軌道はアトラクターの周りを動き、進行方向に対して横向きにカオス的に乱れているものの、アトラクターを一周するタイミングは保たれている [21]。

である。我々は、測定を行う際の驚きの要素を表しているこのことをシャノンに倣って「情報」と呼ぶことにしている。この情報を  $I(\epsilon)$  と表記することで、測定の分解能の目盛りに依存することを強調している。これを利用して、 $\mu$  の次元を定義することができる。これはちょうど、解像度による情報量の漸近的増加率、すなわち

$$D = \lim_{\epsilon \rightarrow 0} \frac{I(\epsilon)}{|\log \epsilon|}. \quad (4.4)$$

である。これを**情報次元**という [20]。なお、これは  $p_i$  が十分に滑らかな場合、すなわち  $\sum_i p_i \log p_i \approx \log n$  の場合、一般にフラクタル次元と呼ばれるものに還元される。ここで  $n$  は  $p_i$  の値がゼロでない測定結果の数である。

この次元の概念は、レニーエントロピー  $R_\alpha$  を用いることで一般化できる。

$$R_\alpha = \frac{1}{1-\alpha} \log \sum_i p_i^\alpha \quad (4.5)$$

ここで、 $\alpha \geq 0$ 、 $\alpha \neq 1$  である。 $\alpha = 1$  の場合の値は、 $\alpha \rightarrow 1$  として極限を取ることで定義され、通常のシャノンエントロピーとなる。シャノンエントロピーをレニーエントロピーに置き換えることで、一般化された次元  $d_\alpha$  を定義することができる。これは、特殊ケースである  $\alpha = 1$  の情報次元を含んでいる。これは、マルチフラクタル現象（スケーリングが不規則なフラクタル）の研究に非常に有効であることがわかっている。このような代替エントロピーの使用については、次の章で詳しく説明する。

ここまでの議論では、観測者が単一の孤立した測定を行うことで得られる情報量、すなわち力学系の「スナップショット」を取ることで得られる情報量について議論してきた。別の言い方をすれば、力学系の動画を見ている観測者が、単位時間あたりにどれだけの新しい情報を得られるか、を意味する。さらに言い換えれば、力学系の振る舞いを監視するために一連の測定を行う実験者の情報取得率とは何か。規則的な力学系（後でより正確に定義する）では、新しい測定値は、 $t \rightarrow \infty$  の極限において、漸近的にそれ以上の情報を提供しない。しかし、力学系がカオス的な場合、系の状態に関する観測者の知識を同じ解像度に保つためには、観測者の知識を更新するための新しい測定が常に必要となる。

このことをより正確に表現すると次のようになる。 $m$  個の測定値の列  $(x_1, x_2, \dots, x_m) = X_m$  を考えてみよう。各測定値は、特定の  $N$  次元立方体で系を観察することに対応する。配列  $X_m$  を観測する確率を  $p(X_m)$  とすると、この一連の測定のエントロピーは

$$H_m = - \sum_i p(X_m) \log p(X_m) \quad (4.6)$$

となる。そして、情報取得率を次のように定義することができる。

$$h = \lim_{m \rightarrow \infty} \frac{H_m}{m \Delta t}. \quad (4.7)$$

$\Delta t$  は測定を行う際のサンプリングレートである。 $\Delta t$  が十分に小さく、その他の条件が満たされていれば、 $h$  は**コルモゴロフ・シナイ (KS) エントロピー**とも呼ばれる**計量エントロピー**に等しくなる<sup>13</sup>。なお、これは本当のエントロピーではなく、エントロピー生成率であり、（対数の底を 2 に取ると）ビット/秒の単位になる。 $h > 0$  の場合はカオス的な動き、 $h = 0$  の場合は規則的な動きとなる。このように、系がカオスである場合に

<sup>13</sup> ここでの計量エントロピーの議論では、多くの重要な数学的形式を無視している。例えば、この定義を正確にするためには、すべての分割とサンプリングレートの上限を取る必要がある。また、 $N$  次元での測定を行う必要はなく、典型的には最適な分割の下で十分な 1 次元の射影が存在する。

は、測定値の列に含まれるエントロピー  $H_m$  は、列が非常に長くなると限界まで増加し続ける。反対に、規則的な動きの場合は、これは限界値に達する。

ここまでは確率の話をしてきたが、計量エントロピーは幾何学的に決まる。力学系の軌跡における平均膨張収縮率は、リアプノフ指数のスペクトルによって特徴づけられる。これらは、式 4.1 で定義される力学系の微分である  $D\phi^t$  の固有値で定義される。 $N$  次元の力学系において、行列  $D\phi^t(x(0))$  の  $N$  個の固有値を  $\alpha_i(t)$  とする。 $D\phi^t$  は正定値行列であるため、 $\alpha_i$  はすべて正である。リアプノフ指数は、 $\lambda_i = \lim_{t \rightarrow \infty} \log \alpha_i(t)/t$  と定義される。これをより幾何学的に考えて、時刻  $t = 0$  で半径  $\epsilon(0)$  を持つ無限小のボールを想像してみよう。このボールが力学系の作用を受けて進むと、ボールは歪む。しかし、ボールは無限小なので、進んでも楕円体のままである。この楕円体の主軸の長さを  $\epsilon_i(t)$  とする。初期のボールを通過する任意の軌道に対するリアプノフ指数のスペクトルは

$$\lambda_i = \lim_{t \rightarrow \infty} \lim_{\epsilon(0) \rightarrow 0} \frac{1}{t} \log \frac{\epsilon_i(t)}{\epsilon(0)}. \quad (4.8)$$

となる。 $N$  次元の力学系には  $N$  個のリアプノフ指数がある。正のリアプノフ指数  $\lambda^+$  は指数関数的な発散の速度を、負のリアプノフ指数  $\lambda^-$  は収束の速度を測っている。これらは**ペシンの定理**

$$h = \sum_i \lambda_i^+. \quad (4.9)$$

により計量エントロピーと関係づけられる。言い換えれば、計量エントロピーは正のリアプノフ指数の総和であり、位相空間における平均指数関数的膨張率と一致する。

計量エントロピーと情報次元を組み合わせて、予測が有効である時間の長さを推定することができる。情報次元により初期の測定値に含まれる情報を推定することができ、計量エントロピーによってこの情報が減衰する速度を推定することができる。

すでに見たように、一連の測定について、計量エントロピーは、各測定で得られる情報を教えてくれる。しかし、それぞれの測定が同じ精度で行われた場合、得られた情報はその測定を行わなかった場合に失われたであろう情報と同じでなければならない。したがって、計量エントロピーは、測定後にシステムの状態に関する知識が失われる初速度も定量化する。

これをより正確にするために、時間 0 での測定が結果  $i$  である条件のもと、 $p_{ij}(t)$  を時間  $t$  での測定の結果が  $j$  である確率とする。言い換えれば、時間 0、分割要素  $C_i$  で状態が測定されたとすると、時間  $t$ 、分割要素  $C_j$  での確率はどれくらいか。定義によれば、 $i = j$  の場合は  $p_{ij}(0) = 1$ 、それ以外の場合は  $p_{ij}(0) = 0$  となる。初期情報がない場合、測定から得られる情報は、漸近測度  $\mu$  だけで決まり、 $-\log \mu(C_j)$  となる。それに対して、 $C_i$  が既知の場合、学習成果  $j$  について得られる情報は  $-\log p_{ij}(t)$  となる。初期データからの予測を用いた場合の追加の情報は、両者の差、すなわち  $\log(p_{ij}(t)/\mu(C_j))$  となる。このことは、時間  $t$  におけるすべての可能な測定値  $C_j$  と、すべての可能な初期測定値  $C_i$  に対して平均化する必要がある。測定値  $C_j$  はその発生確率  $p_{ij}(t)$  で重み付けされ、初期測定値は  $\mu(C_i)$  で重み付けされている。これにより

$$I(t) = \sum_{i,j} \mu(C_i) p_{ij}(t) \log \left( \frac{p_{ij}(t)}{\mu(C_j)} \right). \quad (4.10)$$

となる。初期測定が任意の精度で行われる極限では、 $I(t)$  は最初は直線的に減衰し、その傾きは計量エントロピーに等しいことが容易に示される。 $S/N$  比が  $s$  の測定、つまり  $\log s \approx |\log \epsilon|$  の測定では、 $I(0) \approx D_I \log s$  となる。したがって、 $I(t)$  は  $I(t) \approx D_I \log s - ht$  と近似でき、初期データは特性時間  $\tau = (D_I/h) \log s$  後に役に立たなくなる。

結論として、カオス動力学は、決定論的な力学と確率を結びつけるリンクを与える。カオス的な系について完全に決定論的に議論することができるものの、測定や長期的な予測の問題に取り組むとすぐさま、確率論的に考えざるを得なくなる。これまでに使ってきた用語、つまり情報次元、リアプノフ指数、計量エントロピーは、幾何学的な見方と確率的な見方をつなぐものである。カオス動力学は数次元でも起こり得るが、高次元のシステムに移行すると、例えば多くの粒子間の相互作用を議論する際には、次の2つの理由から確率が突きつけられる。すべての自由度を把握することが難しく、非線形な相互作用がカオス動力学を生み出す「可能性が高まった」からである。「可能性が高まった」と引用されているのは、一世紀以上の努力にもかかわらず、統計力学の有効性のための必要十分条件を理解することが未解決の問題であるためである。

## 5 エントロピーについて

この章では、エントロピーの様々な側面、情報理論との関係、そして秩序、無秩序、無知、不完全な知識といった、時に混乱を招くような意味合いについて説明する。これは、エントロピーの概念に関連するいくつかのよく知られたパズルやパラドックスを扱うことによって行われる。**粗視化**と呼ばれる手続きを用いた第二法則の導出を紹介する。エントロピーの定義の非標準的な拡張を議論する際にも、また、エントロピーの拡張性や加法性について詳細に検討していく。

### 5.1 エントロピーと情報

シャノンが行った重要な新機軸は、情報の尺度としてのエントロピーの概念の妥当性が、熱力学に限らず、確率が定義できるあらゆる文脈で使用できることを示したことである。彼はこれを通信理論の問題に応用し、最適な符号を用いた情報伝達速度の境界を計算できることを示した。

シャノンが得た最も基本的な成果の一つは、不確定性を記述するためにギブス形式のエントロピーを選択することは、それが非常に一般的な文脈で使用される場合でも、恣意的ではないことを示したことである。シャノンとヒンチン [37] は、エントロピー関数が満たすべき条件がある場合、ギブスが最初に提案した関数形式が唯一の選択肢であることを証明した。ヒンチンが指摘した基本的な条件は以下のとおりである。

1. 与えられた  $n$  に対して  $\sum_{i=1}^n p_i = 1$  の場合、要求される関数  $H(p_1, \dots, p_n)$  は、すべての  $p_i$  が  $p_i = 1/n$  となるとときに最大となる。
2. この関数は、 $H(p_1, \dots, p_n, 0) = H(p_1, \dots, p_n)$  を満たす必要がある。不可能な事象が含まれていても  $H$  の値を変えてはならない。
3.  $A$  と  $B$  が必ずしも独立ではない2つの有限な事象の集合である場合、同時事象  $A$  と  $B$  の発生に対するエントロピー  $H(A, B)$  は、集合  $A$  のみに対するエントロピーに、 $A$  における  $i$  番目の事象  $A_i$  の発生を前提とした  $B$  の条件付きエントロピー  $H(B|A_i)$  の加重平均を加えたものである。

$$H(A, B) = H(A) + \sum_i p_i H(B|A_i) \quad (5.1)$$

ここで、事象  $A_i$  は確率  $p_i$  で起こる。

重要な結果は、これらの条件を与えると、式 (3.15) で与えられる関数  $H$  が**唯一**の解になることである。シャノンの重要な洞察は、ボルツマンやギブスがエントロピーを統計力学的に説明した結果には、意図しない重大な副作用があり、エントロピーという物理的な起源を超えた、より広く根本的な意味を持っていたということ

である。シャノンとヒンチンが定式化した抽象的な条件の重要性は、ギブス・シャノン関数が唯一の答えとなる非常に一般的な筋道を示している。後ほど、この3つの条件が揃わない状況において、別のエントロピーの表現があるのではないかという疑問が出てくるだろう。

## 5.2 ランダウアーの原理

情報とエントロピーの関係については、第1章で述べたように、熱力学の第2法則を情報理論の文脈に適した形で具体化したランダウアー原理 [39, 40] に軽く立ち返ってみよう。この原理は、系内のデータの消去には必ず熱が発生し、エントロピーが増大することを表している。この原理を図4に示した。熱浴に接した体積

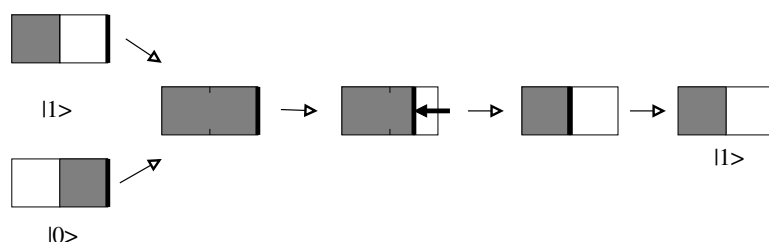


図4 極めて単純な熱力学系を用いたランダウアー原理の説明。

$2V$  の対称形の容器に入った1個の原子からなる「気体」を考える。粒子の位置は、原子が左にあるか右にあるかに対応する1ビットの情報を持つメモリとして機能していると想像しよう。この情報を消去することは、初期状態とは無関係に、デバイスを「基準」状態1にリセットすることになる。したがって、消去は、測定を行うのではなく、システムを再初期化することに相当する。そのためには、まず中央の仕切りを開き、次に右からピストンを可逆的に動かし、最後に仕切りを閉じてピストンを戻すことで可能になる。第1段階で、気体は自由膨張し体積が2倍になる。粒子は仕事をしておらず、エネルギーは保存されているので、熱浴から熱は吸収されない。これは不可逆的な断熱過程であり、気体のエントロピー  $S$  は  $k \ln 2V/V = k \ln 2$  の割合で増加する(粒子が取り得る状態の数は体積だけで、平均速度は熱浴との接触により保存され、エントロピーの変化には寄与しない)。)。消去手順の第2段階で、系を初期状態と同じエントロピーを持つ状態に戻す。これは、温度  $T$  での準静的な(つまり可逆的な)等温過程によって行われる。圧縮時には、エントロピーは  $k \ln 2$  だけ減少する。このエントロピーの変化は、気体が熱浴に与える熱量を温度で割ったものにほかならず、すなわち、 $\Delta S = \int dS = \int dQ/T = \Delta Q/T$  となる。発生した熱  $\Delta Q$  は、圧縮時にピストンを動かすことによってサイクル内で行われた正味の仕事量  $W$  に等しい。結論としては、1ビットの情報を消去する際には、少なくとも  $\Delta Q = kT \ln 2$  の熱を発生させなければならないということである。

同じプロセスをもう少し抽象的に、純粋に情報の観点から見てみよう。単純なメモリデバイスの情報消去を、図5のような一連のダイアグラムにマッピングしてみる。粒子が左または右にある場合(A)、左と右にある場合(B)、左の区画にある場合(C)の違いを明確に示すために、到達可能な(位相)空間のこの表現を選んだ。Aは粒子が左または右の区画に入っているメモリに相当する。Bでは仕切りがなくなり、自由膨張によって位相空間が2倍になり、その結果、エントロピーが  $\ln 2$  増加している。Cでは、系が基準状態に戻され、粒子が左の区画に運ばれる。これは、右からピストンを入れて、仕切りを挿入し、再びピストンを出すことで行われる。位相空間が2分の1になり、それゆえエントロピーが  $\ln 2$  だけ減るのは、圧縮の段階である。これが可能なのは、仕事をして、それに応じた量の熱 ( $\Delta Q \geq T \ln 2$ ) を発生させたからである。なお、この表

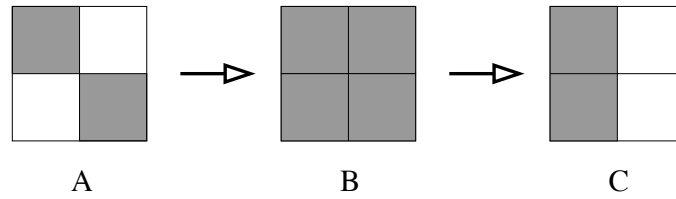


図5 ランダウアーの原理を位相空間で表したもの。説明は本文を参照。

現では、水平方向の仕切りの大きさや垂直方向の事前確率を原理的に変更することで、メモリデバイスのさまざまなタイプや様相をモデル化することができることを注記しておく。

### 5.3 相対概念としてのエントロピー

不可逆性は、基本法則に無知を明示的に導入した結果である。

M. ボルン

エントロピーという概念の解釈や意味については、驚くほど多くの混乱がある [29, 15]。「エントロピー原理」は、どこまでが「人間原理」なのか、という疑問もあるだろう。つまり、エントロピーは人間の認識だけで決まるのか、それとももっと根本的なものなのか。それは観察者の領域における主観的な属性なのか、それとも我々が研究している物理系の本質的な特性なのか。ここで、一般的なエントロピーの定義である無秩序の尺度について考えてみよう。この定義は、秩序や無秩序が何を意味するのかを慎重に説明しなければ、混乱を招く恐れがある。例えば、過冷却液体が閉鎖系、つまり環境とのエネルギー交換がない状態で結晶化する様子を見てみよう。最初は液体分子は自由に動き回っているが、その後（多くの場合、対称性を壊すような小さな摂動を加えることによって）液体は突然固体に変わり、分子が規則的な格子の部位に固定された結晶を形成するようになる。ある意味では、混沌から秩序を生み出す見事な例と言えるだろう。しかし、統計力学の標準的な計算では、結晶化の際にエントロピーが増加することがわかっている。それは、目に見えるものは物語の一部に過ぎないからである。結晶化の際には、エントロピーが潜熱の形で発生し、格子内の分子の振動モードに蓄えられる。このように、結晶の中では個々の分子はほぼ特定の場所に拘束されているにもかかわらず、自由に動き回っていたときよりもエネルギーに格子サイトの周りを振動している。微視的に見ると、液体の時よりも結晶の時の方が到達可能な状態が多くなり、エントロピーが増加する。熱力学的なエントロピーは、運動がミクロであるかマクロであるかには関係がなく、到達可能な状態の数とその確率を数えるだけである。

これに対して、結晶がより整然としているという意味を測るには、別の確率を測らなければならない。そのためには、粒子の位置のみに依存し、速度には依存しない確率を定義する必要がある。これをさらに明確にするために、より巨視的な分割を使用することもできる。これは、格子サイトの周りの分子の熱運動が同じ区画要素内に留まる傾向があるような大きさである。この確率に関連したエントロピーは「空間秩序エントロピー (spatial order entropy)」と呼ばれ、熱力学的エントロピーとは全く異なる挙動を示す。液体の場合、すべての粒子が容器内のどこにでも自由に移動できると、空間秩序エントロピーは高くなり、実質的に最大の値になる。一方、結晶化した後は、空間秩序エントロピーは劇的に低下する。もちろん、これは熱力学的なエントロピーではなく、我々が直感的に感じている結晶秩序の様相を定量的に捉えるために考案したエントロピーである。

前にも強調したように、シャノンの偉大な洞察は、エントロピーを任意の確率の集合に関連付けることが可

能であるということだった。しかし、先ほどの例は、エントロピーをシャノンのいう広い意味で使う場合には、問題の文脈を特定することに細心の注意を払わなければならないことを示している。シャノンエントロピーとは、確率の集合を数値に還元する関数で、ゼロではない可能性がどれだけあるか、ゼロではない確率の集合がどの程度一様か、あるいは集中しているかを反映している。固定された文脈の中では、確率の集合がより小さく、より集中していることは、可能性の集合を特定するために必要な数が少ないという意味で、より「整然」としていると解釈することができる。熱力学では特殊な文脈が必要であり、完全な状態空間で確率を測定しなければならない。熱力学的エントロピーは、シャノンエントロピーの特殊ケースである。一方、シャノンのより一般的な文脈では、確率は、やりたいことに応じて、好きなように定義できる。しかし、混乱を避けるためには、この文脈を常に念頭に置き、自分の計算が何を意味するのかを知るように注意しなければならない。

## 5.4 マクスウェルの悪魔

その「存在」は、自然界の秩序を破壊するほどの影響力を持っていることから、やがてマクスウェルの悪魔と呼ばれるようになった。主な効果として、石油、ウラン、太陽光などのエネルギー源が不要になることが挙げられる。

C.H. ベネット

熱力学の第二法則は、分子の個々の運動を観察したり制御したりすることができないという事実に由来する統計的なものである。分子レベルの大きさでの介入が可能になれば、状況は変わるのだろうか。この問題は、1872年にマクスウェルが彼の**熱の理論** [45] の中で提起した重要なパラドックスを引き起こす。このことは、その後、シラード [59]、ブリルアン [11]、ランダウアー [39]、ベネット [6] など、何世代にもわたって物理学者たちによって議論されてきた。

マクスウェルは彼の悪魔的な設定を次のように説明した。「容器が小さな穴の開いた仕切りで A と B に分けられ、個々の分子を見ることのできる存在がこの穴を開け閉めして、速い粒子だけが A から B へ、遅い粒子だけが B から A へと通過するようにしたとする。このようにして、その存在は仕事を消費することなく、熱力学の第二法則に反しながら、B の温度を上げ、A の温度を下げる。」この崩壊から第二法則を救うために、ブラウン運動や量子不確定性、さらにはゲーデルの定理など、様々な側面から問題解決のための提案がなされてきた。このパラドックスの解決は、悪魔が実際にどのように破壊的な介入を実現するかという問題を中心とした、非常に根本的な問題に触れている。

シラードは、図 6 の左半分に描かれているエンジン (熱力学的サイクル) を紹介して、議論を明確にした。彼とブリルアンが注目したのは、仕切りを入れた後に粒子が容器のどちらにあるのかを知るために、悪魔が行わなければならない測定である。悪魔が実際の分子を「見る」ためには、光源 (光子) と光子検出器のような測定装置を使わなければならない。原理的には、光子を散乱させることで、ある分子が熱平均よりも速いか遅いかを測定できるようになる。ブリルアンは、測定が行われた時点での系全体のエントロピー増加は、その後の悪魔の行動によって得られるエントロピー増加よりも、常に大きいと同じであると主張しようとした。しかし、この議論は通用しなかった。人々は、測定の問題を回避する装置を発明し、悪魔が第二法則を打ち負かすことができるように見えたのである。

代わりに、パラドックスの解決は、まったく別のところからもたらされた。1982年、ベネットは第二法則を救済するために、まったく別の議論を展開した。根本的な問題は、ランダウアーの原理により、情報の消去には熱の発生が必要だということである (5.2 項参照)。ベネットは、原理的に可逆的な測定が可能であることを示し、測定が必ずしもエントロピーを生まないというブリルアンの最初の議論が間違っていることを示した。

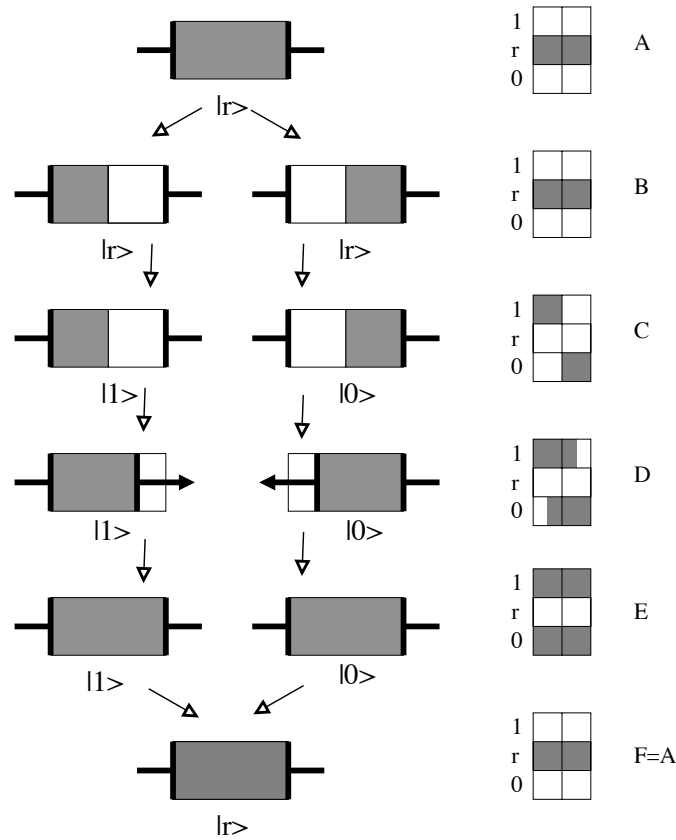


図6 ベネットが想定した1粒子マクスウェル悪魔の装置 [6, 7]。説明は本文を参照。

しかし、本当の意味で熱力学サイクルを完成させるためには、悪魔が得た気体分子の位置に関する情報を消去しなければならない。5.2 項ですでに述べたように、その情報を消去するとエントロピーが発生する。悪魔の記憶を消すために必要な仕事は、少なくとも元々得ていたものと同じであることがわかった。

図6は、シラード [59] が提案したエンジンを一般化したもので、ベネット [6, 7] が想定している1粒子マクスウェル悪魔の装置を示している。(A)の列の左側には、1つの分子が入った気体の容器があり、仕切りと2つのピストンが付いている。右側に、悪魔を含む系の位相空間を模式図で表している。悪魔の心の状態は、次の3つの異なる状態になる。悪魔は、分子が右にあることを知っていたり(状態0)、左にあることを知っていたり(状態1)、あるいは、何の情報もない基準状態や空白状態 $r$ になっていて、粒子がどこにあるかわからないことを知っていたりする。右側の位相空間の模式図では、縦方向が悪魔の記憶状態、横方向が粒子の位置を示している。ステップ(B)では、容器内に薄い仕切りを設置し、粒子を左右どちらかに捕らえる。ステップ(C)では、悪魔が粒子の位置を決定するための(可逆的な)測定を行う。これにより、悪魔の心の状態が図に示されたように、粒子が右にある場合は状態0に、左にある場合は状態1に変化する。ステップ(D)では、悪魔は測定の結果に応じて右または左のピストンを動かし、仕切りを外す。(E)では、気体が自由に膨張してピストンを動かし、それによって仕事をする。状態(E)では、体積、温度、エントロピーが同じであるため、系が元の状態に戻ったように見えるが、仕事が行われている。何が足りないのか。問題は(E)で悪魔の心が元の真っ白な状態に戻っていないことである。悪魔は、粒子の位置がわからないことを知る必要がある。悪魔の記憶を元の状態に戻すには、1ビットの情報を消す必要がある。このことは、(E)から(F)に移る際に、位相



空間の占有部分が2分の1になっていることからわかる。このエントロピーの減少は、ランダウアーの原理により、熱の発生を伴わなければならない(図4、図5参照)。1ビットの情報を消去するために行う仕事は、悪魔が得た仕事よりも大きい。このことにより、完全系の全サイクルが、結局は第二法則を尊重することを保証する。

このパラドックスの解決は注目に値する。なぜなら、不可逆的で熱力学的にコストのかかる情報の獲得(測定)ではなく、論理的にも熱力学的にも不可逆的な消去の過程こそが、第二法則で要求されるエントロピーの増大につながるからである。情報は無料で手に入るが、コストのかかる廃棄物処理の問題が発生する。情報理論が、最も大切にされてきた物理法則の一つを救うことになったのは喜ばしいことである。

## 5.5 ギブスのパラドクス

ギブスのパラドクスは、エントロピーの意味をめぐる議論において、もう一つの興味深い一節を提供している。基本的な問題は、エントロピーがどこまで主観的な概念であるかということである。このパラドックスは、最も単純な形では、2つの理想気体(同じ温度と圧力に保たれている)が、仕切りを取り除いた後に混ざり合うことに関するものである。取り除かれた場合、気体は混合し、2つの気体の粒子が区別できる場合は、この混合によってエントロピーが増加する。しかし、気体が同一で、その粒子がもう一方のものと区別できないような場合は、エントロピーは増加しない。マクスウェルは、最初は同じものと思われていた気体が、後になって違うものだとなったという状況を想像した。この推論は、不可逆性やエントロピーの概念が物理学の知識に依存するという苦しい結論を導き出した。彼は、エントロピーは実験者の心の状態に左右されるため、客観的な根拠がないと結論づけた。このときも、単純な質問をしたマクスウェルが、不快な状況を作り出し、長い議論を引き起こした。量子力学が発達してからは、同じ種の粒子は本当に区別がつかないことが明らかになった。個々の電子に  $N$  個のラベルを貼るようなことはないので、電子を交換しても状態は変わらず、この事実が状態の数を相対的に  $N!$  倍に減らしてくれる。したがって、結論としては、気体を構成する粒子が同じであればエントロピーは増加せず、異なる場合には増加するということになる。

しかし、ギブスのパラドックスの解決は、実は量子力学に依存していない。ジェインズは、ギブスの初期の著作では(量子力学が登場するはるか以前に)正しい議論がすでになされていたことを強調している[34]。ギブスは、「同一」という意味があるとすれば、ある分子が箱の特定の面から来たものかどうかは、その分子の全軌跡をたどらない限り、「不混合」装置では判断できない、という運用上の定義をした。したがって、この意味で気体の粒子が同一であれば、エントロピーは変化しない。エントロピーの適切な定義は、系にかかる客観的な物理的制約、すなわち、どのような測定が可能であるか、または許容されるかを反映していると結論づける。これは、知識を欠いていることとは関係なく、私たちの選択の問題である。「我々の知識の不完全さ」は、我々が記述したい物理システムに課せられた特定の巨視的な制約の集合を正確かつ客観的に反映したものである。系の挙動はこれらの制約に依存しており、エントロピーも同様である。

## 5.6 ジェインズの最大エントロピー原理

物理学者の統計学の実践は、基礎的な確率・統計分野の発展に比べて20年ほど遅れている傾向がある。

E.T. ジェインズ (1963)

統計力学で平衡分布を導き出すための基礎となりうる仮説の出発点には、等価なものが2つある。一つは、平衡は自由エネルギーの最小値に一致するという仮説から始めること、もう一つは、平衡はエントロピーの最

大値と一致するという仮説から始めることである。後者のアプローチは比較的最近になって発展した。シャノンに触発されたジェインズは、統計力学のプログラムをひっくり返してしまった [33]。彼は、非常に一般的な公理から出発して、平衡を仮定した場合、エントロピーのギブスの公式が一意であることを示した。ジェインズのアプローチでは、平衡統計力学の問題はすべて、巨視的な条件を指定する一連の制約の下で、エントロピーが最大となる  $p_i$  の集合を見つけることに還元される [32]。その巨視的な条件は、理論から来している場合もあれば、観測データから直接来している場合もある。この変分法により、これまで統計力学の基礎にあった恣意性が取り除かれた。最大エントロピーの原理は非常にシンプルで、応用範囲が広い。例えば、正規化条件  $\sum_i p_i = 1$  の下でのみ  $S$  を最大化する場合、 $p_i = 1/N$  ( $N$  は全状態数) という一意の解が得られる。これは、等分配の原理に基づく一様確率分布である。同様に、エネルギーが保存されているという制約、すなわち  $\sum_i \varepsilon_i p_i = U$  を加えると、ボルツマン分布である式 (3.5) が唯一の解となる。最大エントロピー原理を出発点とすることで、理論に入る物理的な入力と純粋に確率的な議論を明確に分けることができる。最大エントロピー原理を説明するために、マクスウェル-ボルツマン分布を導出してみよう。まず、確率分布に依存する関数  $L(p_i, \alpha, \beta)$  と、制約を課すための 2 つのラグランジュ乗数を用意する。

$$L(p_i, \alpha, \beta) = - \sum_{i=1}^N p_i \ln p_i - \alpha \left( \sum_{i=1}^N p_i - 1 \right) - \beta \left( \sum_{i=1}^N p_i \varepsilon_i - U \right) \quad (5.2)$$

最大値は、 $L$  の偏微分をゼロにすることで決定される。

$$\frac{\partial L}{\partial p_i} = -\ln p_i - 1 - \alpha - \beta \varepsilon_i = 0 \quad (5.3)$$

$$\frac{\partial L}{\partial \alpha} = \sum_{i=1}^N p_i - 1 = 0 \quad (5.4)$$

$$\frac{\partial L}{\partial \beta} = \sum_{i=1}^N p_i \varepsilon_i - U = 0 \quad (5.5)$$

最初の式から、すぐに次のことがわかる。

$$p_i = e^{-(1+\alpha+\beta\varepsilon_i)} \Rightarrow p_i = \gamma e^{-\beta\varepsilon_i} \quad (5.6)$$

パラメーター  $\gamma$  と  $\beta$  は、拘束方程式によって決定される。まず、上記の解を正規化制約に代入し、分配和の定義式 (3.6) を用いると、 $\gamma = 1/Z$  となる。 $\beta$  の解は、次のような論法で至極簡単に得られる。まず、 $S$  の定義 (3.13) に (5.6) を代入して関係式を得る。

$$S = \beta U - \text{定数} . \quad (5.7)$$

次に、エネルギーとエントロピーの熱力学的な関係 (2.3) を用いて、ハット  $\partial U / \partial S = T$  を求めることができる。この 2 つの関係を組み合わせると、 $\beta = 1/T$  となり、熱平衡分布 (3.5) が得られる。

**最大エントロピー形式論** (*maximal entropy formalism*) は、統計力学だけでなく、もっと広い範囲で有用である。データ転送の最適化や統計的な画像の改善などの用途で、統計的な推論に広く利用されている。このような文脈では、「問題について知っている制約がある中で、これらの制約のもとで可能な限りランダムな（すなわち、最小のバイアスでの）モデルは何か」という問いに対して、きれいな答えを与える。ありふれた応用例として、データの欠落がある。一連の点  $x_i$  を一定の時間間隔で観測していて、観測値の一部が欠けているとする。欠落している値について、既知のデータ点の制約を受けながら、エントロピーを最大化する分布を解くことで、良い推測ができる。

しかしながら、物理学では最大エントロピー原理は平衡状態にのみ適用され、それは物理学の問題のごく一部に過ぎないことを常に念頭に置かなければならない。平衡状態にない系では、別のアプローチを取る必要がある。非平衡統計力学を理解しようとする試みから、5.11 項で議論するように、エントロピーの別の概念の使用を模索する研究者もいる。

## 5.7 オッカムの剃刀

*Entia non sunt multiplicanda praeter necessitatem*

(厳密に必要な場合を除き、エンティティを増やすべきではない。)

オッカムのウィリアム (1285-1347)

情報の興味深い重要な応用例として、モデリングのプロセスそのものがある。モデルを開発する際には、単純すぎてデータを正しく説明できないモデルと、複雑すぎて実際にはノイズでしかないデータの変動に適合するモデルとの間で、常にトレードオフの関係にあることが必要である。よりシンプルなモデルが望ましいことは、しばしば「オッカムの剃刀」と呼ばれる。2つのモデルが既存のデータに同じように適合する場合、最もシンプルなモデルが好ましいとされている。これは、シンプルなモデルの方が、まだ見ぬデータを正しく予測できる可能性が高いという意味である。シンプルなモデルを使うことの価値は誰もが認めるところだと思うものの、実際の問題ではそのトレードオフはそれほど明白ではない。仮に、モデル A はモデル B よりも少しだけより良くデータに適合するが、パラメータが1つ多いとする。パラメータの数に対して適合の良さを、どれくらいのトレードオフと考えるか。

赤池 [2] は、情報理論のアイデアを用いて、適合度とモデルの複雑さの間にトレードオフを行う方法を紹介し、これを単純な線形モデルに適用した。その後、リッサネンは、この問題を考えるために、最小記述長 (MDL) と呼ばれる原則に基づいたより一般的なフレームワークを導入した [52, 27, 28]。基本的な考え方は、予測する能力と情報を圧縮する能力は本質的に表裏一体であるということである。データに規則性がある場合、つまりデータの構造が少なくとも部分的には予測可能な場合にのみ、データを圧縮することができる。それゆえ、今あるデータを最も短く説明できるモデルを求めることで、良い予測モデルを見つけることができる。その際には、モデルの記述長と、モデルの予測と実際のデータとの間の偏差の記述長を考慮しなければならない。モデルとデータの間の偏差は、確率的な事象として扱うことができる。適合度の高いモデルは、データからの乖離が少なく、したがって、よりタイトな確率分布を意味し、データからの偏差に対するエントロピーが小さくなる。このエントロピーは、モデルとそのパラメータを特定するために必要な情報に加えられる。最適なモデルは、最小の和、すなわち最小の総記述長を持つモデルである。適合度をビット数で表すことで、モデルの複雑さと適合度を同じ土俵に乗せ、適合度とモデルの複雑さを正しくトレードオフすることで、少なくとも原理的には2つのモデルの品質を比較することができる。

これは、エントロピーという概念が、科学的手法の根底にあることを示しており、私たちが世界を理解する能力にも通じるものがある。世界のパターンを表現するためには、オーバーフィッティング（過剰適合。ランダムな変化であってもすべての凹凸にフィットさせること、つまりノイズをフィットさせること）とオーバージェネライゼーション（過剰汎化。実際には異なる事象を特定すること）の間にトレードオフを行う必要がある。同様のトレードオフは、ある事象の発生に因果関係のあるメカニズムを割り当てる場合と、ランダムに発生したと説明する場合にも生じる。このようなトレードオフを時系列解析に基づいて正確に行う方法という問題は、かなり長い歴史を持っているが、一方で今でも活発な研究テーマとなっている [1, 13, 57]。このような

トレードオフを完璧に行わず、定量的に考えなくても、世界の規則性を発見してモデル化するときには、暗黙のうちにこの種のモデル選択プロセスに頼っていることになる。どのような一般化も、モデルを特定するために必要な情報と、モデルの世界への適合性のエントロピーとのトレードオフの判断を行っている。

## 5.8 粗視化と不可逆性

私たちの目的は「不可逆性を説明する」ことではなく、「観察可能な事実を説明し、予測する」ことである。もし、これを第一原理から正しく行うことができれば、「不可逆性の本質」に関する哲学的な疑問は、自動的に答えが得られるか、さもなければ、検討不足で無関係だとみなされることになるだろう。

E.T. ジェインズ

熱力学の第二法則によると、閉じた系では、エントロピーは平衡値に達するまで増加するとされている。これは、私たちが日常的に経験している不可逆性と一致する。水の入ったグラスにインクを一滴入れると、その一滴は水の中を拡散し、インクが水の中に均一に広がるまで希釈される。エントロピーの増加は、インクが最初は小さな領域にあり、この領域以外は  $p_i = 0$  であることから、空間の小さな領域に集中した確率分布となり、したがってエントロピーが小さくなることからわかる。系は元の状態には戻らない。これは原理的には不可能ではないものの、あまりにもあり得ないことなので、観測されることはないだろう<sup>14</sup>。

不可逆性は、ミクロの観点からだ理解しがたいものであるが、その理由は、あらゆる物理系の時間発展を根源レベルで決定するミクロな自然法則が、時間反転のもとではすべて対称性を持つからである。つまり、 $F = ma$  といった微視的な物理学の方程式は、 $t \rightarrow -t$  という代入では変化しない。ミクロの世界に不可逆性がないのに、なぜマクロの世界に不可逆性が生まれるのか。

実際、完全にミクロなレベルでエントロピーを計算すると保存されているが、これは熱力学の第二法則を破っているように思える。これは、運動量が保存されていることから、位相空間での体積が保存されていることを意味している。これはリウヴィルの定理と呼ばれる。これによりエントロピー  $S$  が保存されていることを意味することを証明することはたやすい。これは連続変数を使うかどうかではなく、物理法則をミクロのレベルで適用するかどうかにかかっている。これはラプラスの思想を反映したもので、細かいところまで測って追いかけることができれば、統計力学は本当は必要ないということを言っているようにも解釈できる。このことを明らかにし、統計力学と熱力学第二法則を両立させるために、ギブスは**粗視化**という概念を導入するという独創的な議論を展開した。その手続きは「ズームアウト」と呼べるものを体系的に記述したものに相当する。すでに述べたように、このズームアウトには、分配  $\Pi$  に従って位相空間を有限の領域  $\delta$  に分割することが含まれる。例えば、ミクロなレベルでは、各状態に対する離散的な確率  $p_i$  で系が記述できるとする。到達可能な状態を一様分布させた、平衡状態にある閉鎖系から始めよう。例えば、イジング系の場合、 $p_i = 1/g(N, i)$  は、ある特定のスピンの配置の確率である。ここで、各小領域  $\delta$  において、 $p_i$  の値を  $\delta$  上の平均値  $\bar{p}_i$  に置き

<sup>14</sup> 「決してあきらめないで (Never say never)」というのは、誰もが認める名言である。ここでいう「決して (never)」というのは、「一生に一度も」とか「宇宙の一生に一度も」とかではなく、考えられないほど強い。大まかに見積もってみよう。体積  $V$  の容器の左半分に希薄な不活性気体、例えばヘリウムが入っているとすると。その後、容器全体に気体を放出し、再帰時間、つまり、すべての粒子が再び左半分に集まるまでの時間を考える。単純に考えれば、次のようになるだろう。ある瞬間、ある粒子が左半分に入る確率は  $1/2$  であるが、粒子は独立しているので、 $N \sim N_A$  粒子が左半分に入る確率は  $P = (1/2)^{10^{23}} \approx 10^{(-10^{20})}$  となる。容器内のすべての粒子が完全に再配置される典型的な時間スケールを、例えば  $\tau_0 = 10^{-3}$  秒とすると、このような変動が起こるまでの典型的な時間は、 $\tau = \tau_0/P = 10^{10^{20}} 10^{-3} \approx 10^{10^{20}}$  秒となる。

換える。

$$\bar{p}_i \equiv \frac{1}{\delta} \sum_{i \in \delta} p_i, \quad (5.8)$$

そして、それに関連した粗視化エントロピー

$$\bar{S} \equiv - \sum_i \bar{p}_i \ln \bar{p}_i. \quad (5.9)$$

を考える。時刻  $t = 0$  において一様な確率分布でスタートすると、 $S(0) = \bar{S}(0)$  である。次に、系の制約を取り除くことで状況を変化させて、もはや平衡状態ではないものとする。言い換えれば、到達可能な状態の空間を拡大するが、新しい状態では確率がゼロであることを初期条件とする。新しい状況では、 $S(0) = \bar{S}(0)$  であることは変わらず、精視化 (細かい粒度の) エントロピー  $S(t)$  と粗視化エントロピー  $\bar{S}(t)$  の時間発展を比較することができる。 $S(t)$  の時間発展は、可逆的な微視的ダイナミクスに支配されているため、 $S(t) = S(0)$  となり、一定に保たれる。粗視化エントロピーの時間発展を調べるには、いくつかの簡単な数学的トリックを使うことができる。まず、 $\bar{p}_i$  は  $\delta$  の要素を持つ各領域で一定であることに注意し、

$$\bar{S}(t) = - \sum_i \bar{p}_i \ln \bar{p}_i = - \sum_i p_i \ln \bar{p}_i. \quad (5.10)$$

と書ける。そして、

$$\bar{S}(t) - \bar{S}(0) = \sum_i p_i (\ln p_i - \ln \bar{p}_i) = \sum_i p_i \ln \frac{p_i}{\bar{p}_i} = \sum_i \bar{p}_i \left( \frac{p_i}{\bar{p}_i} \ln \frac{p_i}{\bar{p}_i} \right), \quad (5.11)$$

と書くことができ、情報理論ではカルバック・ライブラー・ダイバージェンスと呼ばれる形になる。 $x = p_i/\bar{p}_i$  と置くと、不等式  $x \ln x \geq (x - 1)$  より、ギブスの不等式が成り立つ。

$$\bar{S}(t) - \bar{S}(0) \geq \sum_i p_i - \sum_i \bar{p}_i = 1 - 1 = 0. \quad (5.12)$$

等式は全体を通じて  $p_i/\bar{p}_i = 1$  の場合にのみ成立し、この特殊な場合を除いてこれは厳密な不等式であるため、エントロピーは増大する。粗視化の結果として第二法則が得られることがわかる。

第二法則は、人が空気中で煙を吹いたときに見られる不可逆性を数学的に記述したものである。仮に、煙の雲の動きを映画化したとする。もし、映画を巨大な倍率で撮影し、個々の粒子が行き来しているように見えたとしたら、映画が順方向、逆方向のどちらに向かって再生されているのかを見分けることはできない。統計的な観点から見ると、映画を前に流しても後ろに流しても同じように見える。しかし、それを通常のマクロスケールの解像度で撮影すれば、答えは一目瞭然である。時間の進む方向は、煙がはっきりとした細い流れから拡散して雲になることから明らかである。

哲学的な観点からは、粗視化によって理論に主観的な要素がどの程度導入されるのかを問うべきだろう。粗視化は、物理学によって決められているのではなく、計算をする人が決めているのではないかという反論もありうる。重要なのは、物理学の他の多くの状況と同様に、常識を働かせて、観測可能な量と観測不可能な量を区別しなければならないということである。ラプラスが思い描いた高度に理想化された古典的世界では、ミクロの自由度をすべて観測でき、カオス的な動力学がない限り、エントロピーは増大しない。しかし、この条件に反して、(どんなに正確であっても) 有限の解像度で世界を観測した途端に、カオス動力学によって情報が失われ、エントロピーが増大することになる。粗視化は主観的なものかもしれないが、それは当然のことで、測定は本質的に主観的な操作である。ほとんどの系では、エントロピーがある範囲の細かさや粗さに対応したブ

ラトール (平坦域) で安定することがある。多くの応用例では、エントロピーの増加は一定である (つまり、明確である) ため、粗視化のスケールを適切に選択することができる。ミクロなスケールとマクロなスケールの間の (平衡) エントロピーの増加は、ミクロなスケールからマクロなスケールへと粒度を上げることによって失われる情報量とも言える。ここで重要なことは、系が完全に閉じていることはないということである。常に環境からの小さな摂動があり、それが系の確率的な摂動として作用することで、位相空間における実際の分布が継続的に不鮮明になり、粗視化の効果がシミュレートされる。粗視化は、エントロピーが我々の不確実性の尺度であるという事実を正しく捉えている。この不確かさが規則的な運動や完璧な測定には存在しないという事実は、ほとんどの物理的問題には関係ないことである。

## 5.9 粗視化とくりこみ

書き言葉の自然言語では、文字の有限の組み合わせがすべて単語になるわけではなく、単語の有限の組み合わせがすべて文章になるわけでもなく、文章の有限の並びがすべて意味をなすわけでもない。つまり、意味のあるものを到達可能なものと識別することで、今言ったことは、任意の文字の組み合わせに比べて、言語のエントロピーは極めて小さいということである。

それは、科学の世界でも同じことが言える。私たちは、生物学的、化学的、物理的構造の豊かな多様性を巨大なものと考えていることに慣れているが、想像に反して、可能性の集合は非常に制約されている。**レプトン**や**クォーク**といった物質の最も基本的な構成要素に始まり、生物に至るまでの完全な階層は、驚くほど制限されている。これは、これらの構成要素間の相互作用が非常に特異なものであることと関係している。私たちの知る限り、ミクロの世界ですべての相互作用を制御する基本的な力は、4つだけである。新しい構造レベル (クォーク、陽子、中性子、原子核、原子、分子など) ごとに、そのレベルの物理を記述する多かれ少なかれ自律的な理論があり、そのスケールでの関係する自由度だけを含んでいる。したがって、レベルを1つ上げることは、相互作用がない場合に基本的な自由度が利用できる位相空間の膨大な部分を捨てることになる。例えば、最も高い、最もマクロなレベルの階層では、長距離の相互作用 (電磁気力と重力) だけが重要な役割を果たしている。そこでは、量子力学の構造と、他の2つの基本的な力の詳細は、多かれ少なかれ関係がない。

先ほど説明した構造的な階層を、大きく「粗視化」と呼ぶことがある。このように各レベルの詳細を残して次のレベルに進むことが科学には必要ではあるものの、どうすればいいのかという切り口の手順はない。唯一の例外は、状況によっては、**くりこみ** (renormalization) と呼ばれる手順によって、この粗視化を正確に行うことができることである [67]。これは、あるレベルの微視的な自由度の集合が、次のレベルの自由度を記述するために、どのように平均化されるかを体系的に研究することによって行われる。相転移のように、このプロセスを繰り返して、あるレベルから次のレベルへのマッピングの固定点の存在を示すことができる状況もある (相転移の例としては、液体から気体への変化がある)。この方法により、相転移の性質について重要な洞察が得られ、多くの場合、相転移の特性の一部は、微視的な相互作用の詳細に依存しないという意味で、普遍的であることが示された。

## 5.10 部分系のエントロピーの追加

一般的にエントロピーの拡張性とは、基本的な線形スケーリング特性を満たさなければならないことを意味する。

$$S(T, qV, qN) = qS(T, V, N), \quad 0 < q < \infty. \quad (5.13)$$

拡張性はエントロピーの加法性に変換される。エントロピーが  $S_1$  と  $S_2$  の 2 つの非相互作用系（1 と 2 と表示されている）を組み合わせると、状態の総数はちょうど個々の系の状態の積になる。対数をとると、系全体の  $S$  のエントロピーは次のようになる。

$$S = S_1 + S_2. \quad (5.14)$$

これを外部場のない 2 つのスピンの系に適用すると、結合系の状態数は  $w = 2^{N_1+N_2}$ 、つまり  $w = w_1 w_2$  となる。対数をとることで、エントロピーの加法性が成立する。

しかし、少しでも磁場がある場合、この結果はもはや明白ではない。3.2 項では、与えられたエネルギー  $\varepsilon_k = -k\mu H$  を持つ配置の数を  $g(N, k)$  として計算した。ここで、2 つの系がエネルギーを交換しても、総エネルギーが固定されていれば、2 つの系の間に依存性が発生し、総エントロピーが低下してしまう。このことを例を挙げて説明する。

系 1 の上向きスピンの数を  $k_1$ 、粒子の数を  $N_1$  とし、同様に系 2 のそれらを  $k_2$ 、 $N_2$  とする。総エネルギー  $k = k_1 + k_2$  は保存されているが、どちらの部分系（ $k_1$  と  $k_2$ ）でもエネルギーは保存されていない。スピンの総数  $N = N_1 + N_2$  は固定されており、どちらの部分系のスピンの数（ $N_1$  と  $N_2$ ）も固定されている。この 2 つの系が相互作用するのは、一方の系の上向きスピンの数が変化するとき（つまり、もう一方の系も変化するとき）だけなので、結合した系の状態の総数を次のように書くことができる。

$$g(N, k) = \sum_{k_1} g_1(N_1, k_1) g_2(N_2, k_2), \quad (5.15)$$

ここでは、 $k_1$  が固定されている限り、系 1 と 2 は独立しているという事実を利用している。上式の対数をとると、 $k_1$  について和をとらなければならないので、明らかにエントロピーの加法性は成り立たない。このちょっとした計算が、先ほどの言葉を物語っている。各々の系が固定エネルギーを持つという制約を緩和し、それらのエネルギーの総和のみが固定されるという条件にしたため、系全体として到達可能な状態の数が増えている。部分系自体がもはや閉じていないため、エントロピーが変化してしまうのである。

上記の例において熱力学的極限、すなわち  $N \rightarrow \infty$  のとき、エントロピーの拡張性が回復する。式 (5.15) の和への寄与を  $k_1$  の関数として考え、 $g$  が最大となる  $k_1$  の値を  $k_1 = \hat{k}_1$  とする。ここで、和の寄与を  $\delta = k_1 - \hat{k}_1$  の項で書くと次のようになる。

$$\Delta g(N, k) = g_1(N_1, \hat{k}_1 + \delta) g_2(N_2, \hat{k}_2 - \delta) = f(\delta) g_1(N_1, \hat{k}_1) g_2(N_2, \hat{k}_2), \quad (5.16)$$

ここで、補正係数は関数  $g$  をそれぞれの  $\hat{k}$  の値で展開することにより計算できる。当然のことながら、 $N$  が大きい極限では、 $f$  は  $f \sim \exp(-2\delta^2)$  のオーダーになり、和 (5.15) の最大でない項の  $g(N, k)$  への寄与は指数関数的に抑制されることが分かる。したがって、粒子の数が無限大になる極限では、エントロピーは加法的なものになる。この練習問題では、系が大きくなったとき、直感的にわかるように、ある量の平均を最も確率の高い構成における値で置き換えることができることを示している。数学的な観点からは、この結果は、二項分布が  $N$  の大きな値に対してガウス分布に近づき、 $N \rightarrow \infty$  となるにつれてますます鋭くなることに起因する。この単純な例は、物理的状況の文脈、特に粒子間力の範囲によって、エントロピーの拡張性が正しい場合とそうでない場合があることを示している。

2 つの部分系が相互作用するとき、一方のエントロピーが他方を犠牲にして減少することは確かにあり得る。例えば、系 1 が系 2 に働きかけることで、系 1 のエントロピーが上がり、系 2 のエントロピーが下がることが起こり得る。これは、環境から自由エネルギーを集め、熱エネルギーを廃棄物として排出する生体系にとって非常に重要なことである。それでもなお、生物とその環境の全エントロピー  $S$  は増大し、相互作用

のない部分系の独立したエントロピーの総和も増大する。つまり、時刻ゼロの時点で

$$S(0) = S_1(0) + S_2(0), \quad (5.17)$$

であれば、時刻  $t$  で次のようになる。

$$S(t) \leq S_1(t) + S_2(t), \quad (5.18)$$

これは、系の他の部分との相互作用のみが、ある部分系のエントロピーを低下させることができるためである。このような場合、もちろん個々の系のエントロピーとその結合エントロピーの差を負の相関エントロピーと呼ぶことは自由である。しかし、このように見かけ上エントロピーが減少しているにもかかわらず、全体のエントロピーも個々のエントロピーの合計も増加している。すなわち、

$$\begin{aligned} S(t) &\geq S(0) \\ S_1(t) + S_2(t) &\geq S_1(0) + S_2(0). \end{aligned} \quad (5.19)$$

ここでの要点はこのように式 (5.18) と式 (5.19) が矛盾しないことである。

## 5.11 ボルツマン、ギブス、シャノンエントロピーを超えて: ツァリスエントロピー

$S = k \log W + \text{const}$  という方程式は、初等理論なしに、あるいはどのように言おうと、現象学的な観点からは何の意味もなく現れるものである。

A. アインシュタイン (1910)

すでに強調したように、エントロピーを  $-\sum_i p_i \log p_i$  と定義し、それに関連した指数関数的な状態分布は、平衡状態にある系にのみ適用される。同様に、シャノンとヒンチンが示したエントロピー関数の要件は、唯一の可能性ではない。これらの仮定を修正することで、有用なエントロピーが他にも存在する。マルチフラクタルを記述するのに有効であることが証明されたレニーエントロピーについては、すでに述べたとおりである。

エントロピーの別の定義を考えることが有用と思われるもう一つの文脈は、べき乗則に関するものである。べき乗則は、自然界、社会システムの両方の至るところで姿をあらわす。べき乗則<sup>15</sup>とは、大きな  $x$  に対して  $f(x) \sim x^{-\alpha}$ 、ただし  $\alpha > 0$  のように振る舞うものである。べき乗則の確率分布は、指数分布に比べて  $x$  の値が大きい場合に減衰が非常に遅く、その結果、統計的性質が大きく異なり、上手く振舞わない<sup>16</sup>。べき乗則は、宇宙線のエネルギー、流体の乱れ、地震、河川の氾濫水位、保険金請求の規模、物価変動、個人の富の分布、都市の規模、企業の規模、政府プロジェクトのコスト超過、映画の売り上げ、言葉の使用頻度など、様々な現象で観測されている [48, 22]。べき乗則は様々なモデルで生成されるが、今のところ統一的な理論はなく、そのような統一的な理論が可能かどうかはまだ明らかでない。例えば、エネルギーにおけるべき乗則は、結果の分布が常に指数関数的である平衡統計力学では説明できないことは明らかである。べき乗則を持つことが知られているすべての物理系と、それらを説明しようとするモデルの共通の性質は、それらがある意味で非平衡系であるということである。べき乗則の遍在性は、平衡系で指数関数が標準であるのと同様に、べき乗則が標準的な確率分布となる統計力学の非平衡一般化が存在する可能性を示唆するものである。

長距離の相互作用をもつモデル系（銀河の星など）や「カオスの縁」に長期間留まる系のシミュレーションから、そのような系が最終的に平衡に緩和するまでに、非常に長い時間、べき乗則確率分布をもつ非平衡準安

<sup>15</sup> ゼロまたは他の極限でべき乗則を持ち、 $\alpha < 0$  とすることも可能ではあるものの、ここでの目的で興味のあるほとんどの例において、極限  $x \rightarrow \infty$  と正の  $\alpha$  を意味している。

<sup>16</sup>  $m > \alpha$  のとき、べき乗則分布  $p(x) \sim x^{-\alpha}$  の  $m$  番目のモーメント  $\int x^m p(x) dx$  は存在しない。



定状態に陥ることがあるという証拠が次々に得られている。あるいは、平衡から離れた定常状態に維持される多くの駆動系でもべき乗則が発生する。また、有限系における小さな部分系の挙動を記述することも応用分野として考えられる。

純粋に統計学的な観点から、どのようなエントロピー関数が許されるかを問うのは興味深いことである。自然な仮説は、5.1 節で説明した ヒンチンの定理の最後の部分を変更することである。問題は、残りの 2 つの条件を満たすエントロピー関数と、3 つ目の条件に対する道理にかなった代替案があるかということだ。1988 年にツァリスによって紹介された  $q$  エントロピーと呼ばれる解には、少なくとも一つの興味深いクラスが存在することが判明した [61, 24]。パラメータ  $q$  は通常、**バイアス**または**相関パラメータ**と呼ばれる。 $q \neq 1$  の場合、 $q$  エントロピー  $S_q$  の式は次のようになる。

$$S_q[p] \equiv \frac{1 - \sum_i p_i^q}{q - 1}. \quad (5.20)$$

$q = 1$  の場合、 $S_q$  は  $q \rightarrow 1$  の極限をとることで、標準のギブスエントロピーに還元される。ジェインズの統計力学のアプローチに従うと、適切な制約の下でこのエントロピー関数を最大化し、 $q \neq 1$  に対してべき乗則の振る舞いを示す分布関数を得ることができる。これらの関数は  $q$  指数関数と呼ばれ、次のように定義される。

$$e_q(x) \equiv \begin{cases} [1 + (1 - q)x]^{1/(1-q)} & (1 + (1 - q)x)0) \\ 0 & (1 + (1 - q)x)0). \end{cases} \quad (5.21)$$

$q$  指数関数の重要な性質は、 $q > 1$  かつ  $x \ll -1$  のとき、べき乗則で減衰することである。 $q$  指数関数の逆関数は  $\ln_q(x)$  関数であり、次のようになる。

$$\ln_q \equiv \frac{x^{1-q} - 1}{1 - q}. \quad (5.22)$$

$q$  指数関数はまた、次の方程式の解として得ることができる。

$$\frac{dx}{dt} = x^q. \quad (5.23)$$

これは、線形安定性の端にある力学系において、そのテイラー級数の第 1 項が消失する典型的な挙動である。このことは、このような解が広く認められる理由の一つの可能性を示している。その他の典型的な状況としては、長距離相互作用（銀河形成における星間の重力相互作用など）や、強い相関を持つ変数に対する中心極限定理の非線形一般化 [64] などが挙げられる。

一見したところ、 $q$  エントロピーの問題は、 $q \neq 1$  の場合、加法的でないことである。実際には、次の等式が成り立つ。

$$S_q[p^{(1)}p^{(2)}] = S_q[p^{(1)}] + S_q[p^{(2)}] + (1 - q)S_q[p^{(1)}]S_q[p^{(2)}] \quad (5.24)$$

これは、 $q$  指数関数

$$e_q(x)e_q(y) = e_q(x + y + (1 - q)xy) \quad (5.25)$$

に対応する積則に置き換えたものである。このため、 $q$  エントロピーはしばしば非示量性 (non-extensive) エントロピーと呼ばれる。しかし、これは実は不幸中の幸いなのだ。もし、部分系間のスケール不変相関の適切なタイプが典型的なものであれば、 $q \neq 1$  での  $q$  エントロピーは厳密に加法的となる。十分に長距離の相互作用がある場合、シャノンエントロピーは非示量的である。ツァリスエントロピーは、(適切なクラスの長距離相互作用の下で) 加法的であることにより代替を提供し、それによって、単純な記述で根本的な規則性を捕らえることができる。

この統計力学の代替理論には、形式論全体を「古い」ものに見せてしまうような、もう一つの便利な定義がある。ツァリスエントロピーがすべての確率を  $p_i^q$  に従って重み付けすることに動機づけられることにより、ベックによって紹介された「エスコート」分布  $P_i^{(q)}$

$$P_i^{(q)} \equiv \frac{(p_i)^q}{\sum_j (p_j)^q}, \quad (5.26)$$

を定義することが可能である [5]。そして、エスコート分布の観点から、変数  $A$  の対応する期待値を次のように定義することができる。

$$\langle A \rangle_q = \sum_i P_i^{(q)} A_i. \quad (5.27)$$

これらの定義により、形式論全体がボルツマン-ギブスの枠組みと並行して進む。

もちろん、ツァリスエントロピーの「意味」は何かと問われるかもしれない。エントロピー  $S_q$  は、ボルツマン・ギブス・シャノンエントロピーと同じように、情報の欠如を表す指標である。特に、系の微視的状态を完全に知ることができれば  $S_q = 0$  となり、不確実性が最大（つまり、 $W$  の微視的状态の可能性がすべて等しい）であれば、エントロピーは  $S_q = \ln_q W$  と最大になる。このような相関がどの程度一般的なのか、どのような物理系に見られるのかという疑問は残るが、現時点では、このような関数が少なくとも多くの状況において良い近似であることを示す経験則がかなり蓄積されつつある。さらに最近の結果では、 $q$  指数関数は適切な長距離相関を持つランダム変数の組み合わせに対して中心極限的な振る舞いに従うことが示されている。

中心的な問題は、何が  $q$  を決定するのか、ということだ。自然や人工物、社会システムの中には、エントロピーが示量的であると同時に（すなわち、 $S_q(N)$  が要素数  $N \gg 1$  のとき、 $N$  に比例）、単位時間当たりのエントロピー生産が有限である（すなわち、 $S_q(t)$  が時間  $t \gg 1$  のとき、 $t$  に比例）ような  $q$  の一意の値を選ぶことが可能なクラスがある [63, 62]。指数  $q$  の性質と意味については、次のような類推によりある程度直感的に得ることが可能である。理想化された平面表面を考えると、有限であるのはその  $d = 2$  ルベーク測度だけである。測度は  $d > 2$  では消失し、 $d < 2$  では発散する。フラクタル系であれば、 $d_f$  がハウスドルフ次元として、 $d = d_f$  測度だけが有限となる。 $d > d_f$  の測度は消失し、 $d < d_f$  の測度は発散する。同様に、特殊な  $q$  の値においてのみ、エントロピー  $S_q$  は熱力学的な示量性の要求と、同様に物理的な有限のエントロピー生成の要求とが一致する。 $q$  の値は、確率が集中する位相空間における測度の幾何学的な形状を反映している。

単一と異なる  $q$  の値は、最近の中心極限定理の  $q$ -一般化と  $\alpha$  安定分布（レヴィ分布）に一致する。実際、多数の完全独立またはほぼ独立の確率変数を加える代わりに、大域的に相関のある確率変数を加えると、アトラクタは正規分布とレヴィ分布からそれぞれ  $q$  ガウス分布と  $(q, \alpha)$  安定分布にそれぞれ遷移する [47, 64, 65]。

以上のような枠組みは、まだ発展途上のものである。非平衡物理学だけでなく、経済学などの全く異なる分野でも「統計力学」に関連することが分かるかもしれない。

## 6 量子情報

最近まで、量子力学といえば、不確定性原理や測定上の不可避な制約というイメージが強かった。アインシュタインとシュレーディンガーは、早くからエンタングルメントの重要性を理解していたが、多くの人は EPR パラドックスを哲学者の問題だと考えて、それに気づかなかった。量子効果の情報処理への積極的な応用に対する評価は、徐々に高まっていった。

ニコラス・ギジン

量子力学は、従来とは根本的に異なる計算方法を提供し、古典的なコンピュータでは解決できなかった問題を解決できる可能性がある。例えば、古典的なコンピュータではある数の因数分解にかかる時間は数の大

きさに応じて指数関数的に増大するが、ショアは量子計算を用いるとこれを多項式時間で行うことができることを示した [56]。因数分解は暗号の主要なツールの一つであるため、これは単なる学問的な関心事にとどまらない。指数関数的スケーリングと多項式スケーリングの重要性を理解するために、基本的な計算ステップに  $\Delta t$  秒かかると仮定しよう。ステップ数が指数関数的に増加する場合、 $N$  桁の数字を因数分解するのに  $\Delta t \exp(aN)$  秒かかる。ここでの  $a$  はアルゴリズムの詳細に依存する定数である。例えば、 $\Delta t = 10^{-6}$  とし、 $a = 10^{-2}$  とすると、 $N = 10,000$  桁の数の因数分解には  $10^{37}$  秒かかる。これは宇宙の寿命 (わずかに  $4.6 \times 10^{17}$  秒) よりもずっとずっと長い時間である。反対に、ステップ数が桁数の 3 乗に比例する場合は、同じ計算でも  $a' \Delta t N^3$  秒となり、 $a' = 10^{-2}$  とすると  $10^4$  秒、つまり 3 時間弱ですむことになる。もちろん定数  $a$ 、 $a'$ 、 $\Delta t$  は実装に依存するが、指数関数的スケーリングと多項式スケーリングの劇的な違いにより、十分に大きな  $N$  では常に速度に根本的な違いが生じる。実は、このような因数分解問題では、もっと微妙な状況にある。現在、古典的なアルゴリズムでは  $\exp(O(n^{1/3} \log^{2/3} n))$  回の演算が必要であるが、量子アルゴリズムでは  $O(n^2 \log n \log \log n)$  回の演算ですむ。因数分解は、量子計算の恩恵を受けられる可能性があるいくつかの問題の一つに過ぎない。その意味するところは、量子計算にとどまらず、量子暗号や量子通信などの多様な応用を含んでいる [49, 35, 46, 43]。

このような高速化の可能性は、量子系の本質的な並列性に由来する。その理由は非常に微妙であり、量子力学の発見から何十年も経ってから、その計算特性が根本的に違うということに誰も気づかなかった。近年、量子計算への関心が高まり、物理系における情報の概念が見直され、「量子情報理論」とも呼ばれる分野が生まれている。

量子情報・量子計算の具体的な内容に入る前に、量子論の基本的な設定を簡単に紹介し、古典論との対比を行う。量子系の物理状態、量子的可観測量 (オブザーバブル) の定義、シュレディンガー方程式に従った時間発展について述べる。次に、測定過程、量子テレポーテーションの基礎、量子計算について簡単に説明する。古典的な統計物理学との関連として、密度行列とフォン・ノイマンエントロピーについて述べる。実際の量子計算には、実験物理学の高度で専門性の高いいくつかの分野が関わっており、この短いレビューでは範囲を超えている。そのため、私たちは本質的な原則に基づいた議論にとどめるように努めた。

## 6.1 量子状態と量子ビットの定義

古典物理学では、ある瞬間の粒子の位置や速度など、力学的な変数の値を指定して系の状態を記述する。その時間発展はニュートンの法則で記述され、その発展における不確かさは、測定の精度によってもたらされる。4.2 節で述べたように、不確か性はカオス力学によって増幅されることがあるが、古典物理学の中では、測定精度に基本的な限界はない。より注意深く測定することで、系の時間発展をより正確に予測することができる。しかし、根本的なレベルでは、すべての物理学は量子力学の法則に従って振るまい、古典物理学の法則とは非常に異なっている。古典物理学が近似とする空間、時間、エネルギーの巨視的スケールでは、古典理論と量子理論の予測はほぼ同じでなければならない。このことを**対応原理**という。しかし、量子力学的な記述から古典物理学が生まれる過程を理解することは、必ずしも容易ではない。

量子領域のスケールは、エネルギー  $\times$  時間の (または運動量  $\times$  長さに等しい) 次元を持つプランク定数で設定される。それは、通常の単位<sup>17</sup>では  $\hbar = 1.05 \times 10^{-34}$  ジュール・秒と極めて小さい。このため、量子的な性質は非常に小さなスケールや非常に低い温度でしか現れない。しかし、原子や分子構造といったミクロなス

<sup>17</sup> 換算プランク定数  $\hbar = h/2\pi$  を使用している。

ケールで根本的に異なる性質を持つものは、マクロなスケールでも根本的に異なる集団的な振る舞いをするようになることを念頭に置いておかねばならない。結晶や、超伝導体、常伝導体、半導体、磁性体など、自然界で実現されている凝縮系のほとんどの相は、量子力学の観点からしか理解することができない。物質の安定性と構造は、その基本的な構成要素の量子的な振る舞いに大きく左右される。

量子情報理論の基本的な考え方を説明するために、量子情報系の基本的な構成要素である**量子ビット**の系に限定して話を進める。量子系の物理的な状態は、**ヒルベルト空間**と呼ばれる抽象的な多次元空間のベクトルと考えられる波動関数で記述される。ここでいう有限次元ベクトル空間とは、ベクトルが実数ではなく複素数の係数を持ち、ベクトルの長さがそのような空間での通常の長さ、すなわちその成分の平方振幅の和の平方根であることを意味する<sup>18</sup>。ヒルベルト空間は、古典力学での位相空間の概念を置き換えるものである。空間の軸を定義する直交基底ベクトルは、スピン、位置、運動量など、測定可能な量（オブザーバブルとも呼ばれる）の異なる値に対応する。

後述するように、古典力学との重要な違いは、位置と運動量、あるいは  $x$  軸方向のスピンと  $y$  軸方向のスピンなど、多くの量子力学的量が同時に測定できないことである。古典物理学とのもう一つの本質的な違いは、量子系の状態空間の次元が古典的位相空間のそれに比べて巨大であることだ。この大きな違いを説明するために、任意の運動量で無限の線上を移動できる粒子を考えてみる。古典的な観点から見ると、位相空間は 2 次元の実空間（位置  $x$  と運動量  $p$ ）であるが、量子的な観点から見ると、1 変数（通常は位置  $x$  か運動量  $p$ ）の波動関数  $\Psi$  で与えられる。この波動関数は、無限次元のヒルベルト空間の要素に対応する。

3.2 節で古典的なイジングスピンについて述べた。上向きのスピン、下向きのスピンと呼ばれる  $s = \pm 1$  で示される 2 つの状態のみを持つ系で、「0」と「1」の 2 つの状態が可能な古典ビットを表すと考えることができる。対して、イジングスピンを量子化したものは、まったく異なる種類のものとなる。イジングスピンが古典的なビットに相当するのに対し、量子スピンはいわゆる**量子ビット**に相当する。これから明らかにするように、量子ビットの状態空間は古典ビットの状態空間よりもはるかに大きく、より多くの情報を格納することが可能である。このことは、ある意味で正しい。というのも、状態はどこまで本当に観察可能なのか、正確に準備できるのか、ということを考えてしなければならないからだ。これらについて、後ほど改めて説明する。

よく定義された 2 準位の量子系は、量子ビットを表すと考えることができる。2 状態の量子系の例としては、2 つの偏光状態を持つ光子、2 つのスピン状態を持つ電子、2 つのエネルギー状態のうちの 1 つにある粒子などがある。最初の 2 つの例では、ヒルベルト空間内の物理量は文字通りスピンであり、角運動量に相当するが、最後の例ではそうではない。このことは問題とはならない。たとえ基礎となる量が角運動量と関係がなくても、それが 2 状態の量子系である限り、それを「スピン」と呼ぶことができる。一方の量子状態を「上向きスピン」と呼び、記号  $|1\rangle$  で表し、もう一方を「下向きスピン」 $|0\rangle$  と呼び、任意に指定することができる。

量子ビットの状態は、波動関数または状態ベクトル  $|\psi\rangle$  によって記述され、次のように書くことができる。

$$|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \quad \text{ここで } |\alpha|^2 + |\beta|^2 = 1. \quad (6.1)$$

ここで  $\alpha$  と  $\beta$  は複素数<sup>19</sup>であるから、 $|\psi\rangle$  を  $\mathbf{C}^2$  と表記される 2 次元複素ベクトル空間のベクトルと考え、状態を列ベクトル  $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$  として表現することができる。また、行ベクトルとして表現される双対ベクトルによる

<sup>18</sup> より一般的には、無限次元の可能性を考慮する必要があり、ここでは心配する必要のない級数の収束に関する複雑な問題が発生する。

<sup>19</sup> 複素数  $\alpha$  は実部と虚部  $\alpha = a_1 + ia_2$  を持ち（ここで  $a_1$  と  $a_2$  はともに実数）、 $i$  は  $i^2 = -1$  の性質を持つ虚数単位である。したがって、複素数は 2 次元の実空間におけるベクトルと考えることもできることに注意すること。複素共役は  $\alpha^* = a_1 - ia_2$  であり、母数、つまり絶対値の 2 乗は  $|\alpha|^2 = \alpha^* \alpha = a_1^2 + a_2^2$  と定義される。

$\mathbf{C}^2$  の双対ベクトル空間を定義し、次のように書くことができる。

$$\langle \psi | = \langle 0 | \alpha^* + \langle 1 | \beta^* . \quad (6.2)$$

これにより、2つの状態ベクトル  $|\psi\rangle$  と  $|\phi\rangle = \gamma|1\rangle + \delta|0\rangle$  の内積を次のように定義することができる。

$$\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^* = \gamma^* \alpha + \delta^* \beta . \quad (6.3)$$

古典系で状態 (または配位) を追加するごとに、量子系では直交する次元 (複素パラメータ) が追加される。したがって、有限状態の古典系は、対応する量子系に対して有限次元の複素ベクトル空間を導くことになる。

ここで、1個の量子ビットの量子配位空間の幾何学的形状をより詳細に説明しよう。制約条件  $|\alpha|^2 + |\beta|^2 = 1$  は、状態ベクトルが単位長さを持つことを意味し、 $\mathbf{C}^2$  における複素単位円を定義するが、複素数を実部と虚部分けて書くと  $\alpha = a_1 + ia_2, \beta = b_1 + ib_2$  となる。そうすると、 $|a_1 + ia_2|^2 + |b_1 + ib_2|^2 = a_1^2 + a_2^2 + b_1^2 + b_2^2 = 1$  が得られる。後者の式で記述される空間の幾何学は、4次元のユークリッド空間  $\mathbf{R}^4$  に3次元の単位球  $S^3$  を埋め込んだだけのものである。

重要な量子計算を行うには、複数の量子ビットを持つシステムを考える必要がある。物理的には、それぞれがスピンを持つ  $n$  個の粒子の系を想像するのが最も簡単である (前述したように、形式論はこれに依存せず、個々の量子ビットが他の物理的性質に対応するような例も可能である)。  $n$  個の量子ビットが存在する数学的空間は、個々の量子ビット空間のテンソル積であり、 $\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \dots \otimes \mathbf{C}^2 = \mathbf{C}^{2^n}$  と書くことができる。例えば、2個の量子ビットのヒルベルト空間は  $\mathbf{C}^2 \otimes \mathbf{C}^2$  である。これは、ベクトル  $|1\rangle \otimes |1\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |0\rangle \otimes |0\rangle$  によって広げられる4次元の複素ベクトル空間である。便宜上、テンソル積の記号を省略したり、単にスピンを列挙して省略することが多い。例えば、次のように記述される。

$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle .$$

波動関数  $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$  と  $|\phi\rangle = \gamma|1\rangle + \delta|0\rangle$  を持つ2個の量子ビットのテンソル積は次のようになる。

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = \alpha\gamma|11\rangle + \gamma\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|00\rangle .$$

テンソル積の最も重要な特徴は、それが多重線形であること、つまり、 $(\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle = \alpha|0\rangle \otimes |\psi\rangle + \beta|1\rangle \otimes |\psi\rangle$  となる。ここでも強調したいのは、古典的な  $n$  ビット系が  $2^n$  個の状態を持つのに対し、 $n$  量子ビット系は  $2^n$  次元の複素空間における単位長のベクトルに対応し、自由度はその2倍であることだ。例えば3量子ビットは次のように展開される。

$$\begin{aligned} |\psi\rangle = & \alpha_1|000\rangle + \alpha_2|001\rangle + \alpha_3|010\rangle + \alpha_4|011\rangle \\ & + \alpha_5|100\rangle + \alpha_6|101\rangle + \alpha_7|110\rangle + \alpha_8|111\rangle \end{aligned}$$

状態ベクトルをその成分の列ベクトル  $\alpha_1, \alpha_2, \dots, \alpha_{2^n}$  で表すと便利な場合がある。

## 6.2 オブザーバブル

エネルギー、位置、速度、スピンなどの通常の物理量は、どのようにして状態ベクトルから取り出すのだろうか。量子力学では、観測量 (オブザーバブル) は状態空間上で作用するエルミート演算子として定義される。量子力学では、**演算子**はある状態を別の状態に写す線形変換であり、状態空間が有限次元であれば、行列で表現することができる。エルミート演算子あるいは行列は、 $A = A^\dagger$  の条件を満たす。ここで、 $A^\dagger = (A^{tr})^*$  は  $A$  の転置行列の複素共役である。オブザーバブルが演算子で表現されるのは、測定によって状態が変化し、異

なる測定の結果が測定の順番に依存するという性質を反映したものである。一般に、量子力学ではオブザーバブルが必ずしも可換ではなく、2つのオブザーバブル  $A$  と  $B$  の積に対して  $AB \neq BA$  となることがある。オブザーバブルがエルミートでなければならない理由は、測定の結果がオブザーバブルの固有値であり、エルミート演算子の固有値が実数であることが保証されているからである。

例えば、1個の量子ビットを考えてみよう。物理的なオブザーバブルは、 $x$ 、 $y$ 、 $z$  方向に沿ったスピンの成分であり、慣例的に  $s_x = \frac{1}{2}\sigma_x$ 、 $s_y = \frac{1}{2}\sigma_y$ 、などと表記される。演算子  $\sigma$  は、パウリ行列

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (6.4)$$

であり、明らかに可換でない。このようにスピン演算子を記述することで、 $z$  軸が対角表現になるように任意に選択<sup>20</sup>し、 $z$  軸に沿ったスピンの固有状態<sup>21</sup>は列行列

$$|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

となる。

### 6.3 量子発展: シュレディンガー方程式

量子系の波動関数は、有名なシュレディンガー方程式に従って時間的に発展する。物理系の動的な変化は、系やその構成要素間に働く基礎的な力によって引き起こされ、その効果はエネルギー演算子またはハミルトニアン演算子  $H$  と呼ばれるもので表現することができる。1量子ビット系では演算子は  $2 \times 2$  行列、2量子ビット系では  $4 \times 4$  行列、というふうに表現される。シュレディンガー方程式は次のように書くことができる。

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle. \quad (6.5)$$

これは、量子系の時間発展がそのエネルギー演算子によって生成されるという性質を表す線形微分方程式である。 $H$  が一定であると仮定すると、初期状態  $|\psi(0)\rangle$  が与えられたときの解は、単に次のようになる。

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \quad \text{ここで } U(t) = e^{-iHt/\hbar}. \quad (6.6)$$

この時間発展はユニタリーであり、演算子  $U(t)$  は  $UU^\dagger = 1$  を満たすことを意味する。

$$U^\dagger = \exp(-iHt/\hbar)^\dagger = \exp(iH^\dagger t/\hbar) = \exp(iHt/\hbar) = U^{-1}. \quad (6.7)$$

ユニタリー時間発展とは、状態ベクトルの長さが不変であることを意味し、これは系がどの状態にもなりうる全確率を保存するために必要である。時間発展演算子  $U$  のユニタリー性は、 $H$  がエルミートであることから直接的に導かれる。任意の  $2 \times 2$  エルミート行列は次のように書くことができる。

$$A = \begin{pmatrix} a & b+ic \\ b-ic & -a \end{pmatrix}, \quad (6.8)$$

<sup>20</sup> 他の2軸のいずれかを対角化し、 $z$  軸を対角化しない別の表現に回転させることも可能ではあるものの、一度に3軸のうち1軸しか対角化できない。実験装置には、磁場をかけるなどして対称性を破る条件があることが多いが、その場合は対称性の破る方向を  $z$  軸とするのが最も便利である。

<sup>21</sup> 線形演算子  $A$  の固有状態  $|\chi_k\rangle$  は、 $A|\chi_k\rangle = \lambda_k|\chi_k\rangle$  という式で定義される。 $A$  がエルミートであれば、固有値  $\lambda_k$  は実数である。一般に固有値は正規直交系として選ぶことができ、 $\langle\chi_j|\chi_k\rangle = \delta_{jk}$  となる。ここで、 $i=j$  のとき  $\delta_{ij} = 1$ 、それ以外は  $\delta_{ij} = 0$  である。

ここでの、 $a$ 、 $b$ 、 $c$  は実数である<sup>22</sup>。

単純な例として、1 つの量子ビットの場合、初期状態が次の通りだとする。

$$|\psi(0)\rangle = \sqrt{\frac{1}{2}}(|1\rangle + |0\rangle) \equiv \sqrt{\frac{1}{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

右辺では、便宜上、状態を列ベクトルで書いている。正の  $z$  軸に沿った磁場  $B$  中におけるスピンのエネルギーを考える<sup>23</sup>。この場合、 $H$  は  $H = Bs_z$  で与えられる。式 (6.4) から

$$U(t) = \exp\left(\frac{-iBt}{2\hbar}\sigma_z\right) = \begin{pmatrix} \exp(-iBt/2\hbar) & 0 \\ 0 & \exp(iBt/2\hbar) \end{pmatrix}. \quad (6.9)$$

となる。式 (6.6) を用いると、状態の振動的な時間依存性が得られる、すなわち

$$|\psi(t)\rangle = \sqrt{\frac{1}{2}} \begin{pmatrix} e^{-iBt/2\hbar} \\ e^{iBt/2\hbar} \end{pmatrix} = \sqrt{\frac{1}{2}} \left[ \cos \frac{Bt}{2\hbar} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + i \sin \frac{Bt}{2\hbar} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right]. \quad (6.10)$$

となる。

このように、古典力学とは対照的に、量子力学の時間発展は常に線形であることがわかる。この意味で、古典力学よりはるかに単純である。複雑なのは、例えば惑星のような巨視的な物体に対応するようなより複雑な例を考えた時、量子力学が採用する空間の次元が非常に高くなるということである。

## 6.4 量子測定

古典物理学における測定は、概念的には取るに足りないことである。古典的な状態の値を有限の精度で推定し、その状態を有限桁の実数として近似するだけである。測定の精度は、バックグラウンドノイズと測定器の精度によってのみ制限される。これに対して、量子力学における測定過程は、まったく些細なことではない。古典力学との違いの 1 つは、測定可能な状態の集合が離散的で、観測量 (オブザーバブル) の値が量子化されている場合が多いことである。この性質が、量子力学という理論の名前の由来になっている。しかし、それ以上に大きな違いは、量子力学的な測定は、波動関数を根本的に変化させることが一般的であることだ。あるオブザーバブルを測定する前は、起こりうる結果を確率で表すことしかできないが、測定後は結果が確実にわかり、それを反映するように波動関数が不可逆的に変化する。量子力学における従来のコペンハーゲン解釈では、測定が行われると波動関数が「収縮 (collapse)」すると言われていた。量子力学が目を見張るような予言をしているにもかかわらず、量子測定が本質的に確率的であり、「瞬時に」系の状態を変えてしまうという事実が大きな論争を巻き起こしている。実際、歴史的に見ても、量子計算の分野は測定問題を注意深く考えることから生まれたと言える [16]。

量子力学の公式では、オブザーバブルな量  $A$  の観測結果は行列  $A$  の固有値で与えられる。例えば、式 6.4 で定義された 3 つのスピン演算子は、すべて同じ 2 つの固有値  $\lambda_{\pm} = \pm 1/2$  を持つ。つまり、どの方向のスピンを測定しても、プラスかマイナス 2 分の 1 にしかならないのである。これは、古典物理学でいうところの回転体とは全く異なるもので、回転体はどの方向へも可能な限りの速度で回転することができる。だから量子力学は直感的でない。

量子系がある固有状態にある場合、それに対応する方向の測定結果は確実である。例えば、 $\alpha = 1$ 、 $\beta = 0$ 、つまり  $|\psi\rangle = |1\rangle$  の状態の 1 量子ビットがあるとする。このとき、 $s_z$  の固有値は  $+\frac{1}{2}$  となり、 $s_z$  を測定する

<sup>22</sup> 単位行列に比例する成分は、どの状態にも作用するため省略した。

<sup>23</sup> 量子スピンは必ず磁気モーメントを持つので、角運動量だけでなく、磁場との相互作用もある。

と必ずその値が得られる。これは、 $z$  方向のスピン演算子  $A = s_z$  について、固有値  $\lambda_+ = +1/2$  を持つ固有ベクトルが  $|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ 、 $\lambda_- = -1/2$  を持つ固有ベクトルが  $|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  であるという事実による量子力学の数学的機構に反映されている。一方、固有状態に直交する方向、例えば  $A = s_x$  で測定すると、結果は確率的になる。上記の例では、 $s_x$  の固有ベクトルは  $|\chi_+\rangle = \sqrt{\frac{1}{2}}(|1\rangle + |0\rangle)$  と  $|\chi_-\rangle = \sqrt{\frac{1}{2}}(|1\rangle - |0\rangle)$  となる。一般に、ある測定において系がある状態にあることを発見する確率は、まず与えられた状態  $|\psi\rangle$  をオブザーバブルに対応する行列  $A$  の固有状態  $|\chi_k\rangle$  に展開することによって計算される。つまり、

$$|\psi\rangle = \sum_k \alpha_k |\chi_k\rangle \quad \text{ここで } \alpha_k = \langle \chi_k | \psi \rangle. \quad (6.11)$$

となる。固有値  $\lambda_k$  に一致する状態で系を測定する確率は、 $p_k = |\alpha_k|^2$  である。したがって、量子力学の予測は確率的であるが、その理論は古典的な確率論とは本質的に違っている。一方では、与えられた演算子がヒルベルト空間上の確率測度を定義することは明らかであるが、演算子は (行列のように) 非可換であるため、非可換確率論を扱うことになる [30]。オブザーバブルの非可換性が、量子測定の理論に複雑さをもたらしているのである。

分かりやすくするために、例を挙げて説明しよう。 $x$  方向のスピン、 $A = s_x$ 、 $|\psi\rangle = |1\rangle$ 、すなわち  $z$  方向に上向きのスピンを考える。 $s_x$  の固有値で展開すると、 $|\psi\rangle = |1\rangle = \sqrt{\frac{1}{2}}|\chi_+\rangle + \sqrt{\frac{1}{2}}|\chi_-\rangle$  が得られる。 $x$  方向にスピンの上向きとなる確率は  $|\alpha_+|^2 = 1/2$  であり、 $x$  方向にスピンの下向きとなる確率は  $|\alpha_-|^2 = 1/2$  である。量子力学に確率がどのように入り込んでいるのか、基本的なレベルで見ることができる。オブザーバブルの平均は、その期待値であり、下記のとおり加重和である。

$$\langle \psi | A | \psi \rangle = \sum_k |\alpha_k|^2 \lambda_k = \sum_k p_k \lambda_k. \quad (6.12)$$

この例では、 $\langle \sigma_x \rangle = 0$  となる。

測定という行為は、系の状態に影響を与える。 $s_x = +\frac{1}{2}$  を測定し、その直後にもう一度測定すれば、確実に同じ値を得ることができる。別の言い方をすれば、測定によって系が何らかの形で固有状態  $|\chi_+\rangle$  に追い込まれ、いったんその状態になると、それ以上の相互作用がない限り、その状態に留まるということだ。この観測された固有状態に波動関数が収縮するという測定の奇妙な性質は、もともとアドホックに理論に付け加えられたもので、**射影仮説**と呼ばれるものである。この仮説は、理論にかなり恣意的な要素を導入しており、矛盾しているように見える。この系は、測定が行われるまでは量子力学のもとでシュレディンガー方程式に従って発展し、古典的な測定装置に関連した何らかのマジックが起こり、それは理論の他の部分から完全に外れたところにある。

測定過程をよりよく理解するためには、量子系と古典的な測定装置の関連をより詳細に議論する必要がある。文字盤上の針や光パルスの条件発光などの測定装置も量子力学系である。測定器を量子力学的に扱えば、波動関数の「収縮」は、測定器と元の量子系との結合系の量子発展とみなすことができ、射影仮説は不要である。この点については、6.7 節でデコヒーレンスについて説明するときに触れる。

なお、測定によって状態を完全に決定することはできない。2 量子ビット系を完全に測定した場合、古典的な情報は最大でも 2 ビットであるのに対し、量子状態を完全に決定するには 7 つの実数 (正規化条件付きで 4 つの複素数) を知る必要がある。この意味で、量子状態が古典状態よりはるかに多くの情報を「含んでいる」と言うことはできない。実際、オブザーバブルの非可換性のために、同時測定では対応する古典的な系から得られる情報よりも少ない情報を取り出すことができる。



量子論には2つの考え方がある。もし、量子論が単一系の理論であると主張するならば、量子論は物事が起こる確率を予測するだけであり、古典物理学の理想から後退しているという事実を受け入れなければならないだろう。あるいは、量子論は粒子の集合体にも適用される理論であるという考え方もある。確率分布を実際に測定するためには、「まったく同じように準備された」量子系に対して多くの測定を行う必要がある。この観点から、ヒルベルト空間の次元性は、古典的位相空間上で定義される古典的分布の次元性と比較されるべきであり、古典論と量子論の間の差ははるかに小さくなる。そのため、量子力学の基礎となる、単一系に適用される理論が求められているのである。今のところ、誰もそのような理論の構築に成功しておらず、それどころか、「隠れた変数」に基づく理論の構築の試みは失敗している。ベルの不等式は、そのような理論がおそらく不可能であることを示唆している [50]。

## 6.5 複数量子ビット状態とエンタングルメント

複数の量子ビットがある場合、ある量子ビットの測定が他の量子ビットの測定にいつ、どのように依存するかということが実用上の重要な問題となる。量子力学の深い特性により、量子ビットは微妙な結合が可能で、古典ビットとは全く異なる測定結果をもたらす。このことを理解することは、計算や情報伝達の問題を考える上で重要であることが分かってきた。これを説明するために、異なる量子ビットの測定値が統計的に独立か統計的に依存かを表す、分離可能性ともつれ (エンタングルメント) という対立概念を導入する必要がある。

$n$  量子ビット状態が  $n$  個の単一量子ビット状態に因数分解できる場合、すなわち、各因子が単一量子ビットにのみ依存する量子ビットの和の  $n-1$  個のテンソル積として書くことができる場合、その  $n$  量子ビット状態は**分離可能** (separable) である<sup>24</sup>。分離可能な2量子ビットの例としては、以下のとおりである。

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle). \quad (6.13)$$

$n$  量子ビットの状態が分離可能であれば、個々の量子ビットの測定は統計的に独立である。つまり、それぞれの量子ビットの一連の測定を行う確率は、それぞれの量子ビットの測定の確率の積として書くことができる。

$n$  量子ビットの状態が分離可能でない場合、**もつれ (エンタングル)** となる。もつれた2量子ビットの状態の例は、次の通りである。

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (6.14)$$

これは、1個の積に因数分解できない。もつれた状態の場合、個々の量子ビットの測定は相互に依存する。

ここで、上記の2つの例について説明する。例えば、1個目の量子ビットのスピンを測定し、それから2個目の量子ビットのスピンを測定する実験を行ったとする。分離可能な例ともつれた例の両方において、最初の測定で上向きのスピンまたは下向きのスピンの観測される確率は50%である。仮に上向きのスピンだったとする。分離可能な状態の場合、波動関数は次のように変換される。

$$\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|1\rangle) \otimes (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle).$$

ここで2番目の量子ビットのスピンを測定すると、上向きのスピンまたは下向きのスピンの測定確率は50%のままである。1個目の測定は2個目の測定に影響を及ぼさない。

<sup>24</sup> 厳密には、これは次節で定義する純粋状態の場合にのみ当てはまる。

これに対して、式 6.14 のもつれ状態に対して同様の実験を行い、最初の測定で上向きのスピンの観測されたとする。これにより、波動関数は次のように変換される。

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \longrightarrow |11\rangle. \quad (6.15)$$

(波動関数を正規化するため、係数  $1/\sqrt{2}$  が消えていることに注意)。2 個目の量子ビットのスピンを測定すれば、上向きのスピンの観測される。同様に、1 個目の測定で下向きスピンの観測すれば、2 個目の測定でも下向きスピンの観測することになる。上記のもつれの例では、測定は完全に結合しており、最初の測定結果が 2 個目の測定結果を決定している。このもつれ状態の特性は、もともとアインシュタイン、ポドルスキー、ローゼンによって指摘され [19]、量子ビットが空間的に大きく離れている場合に起こりうる結果について懸念を表明していたものである。この考え方は、彼らが当初期待したような量子力学の根本的な問題を指摘するものではなく、むしろ量子計測問題の理解を深め、6.9 節で述べるような量子テレポーテーションの実用化につながったのである。

量子ビットの系のもつれ具合は、その過去の履歴を反映している。適切な時間発展演算子を適用することで、つまり適切な相互作用を導入することで、分離可能な状態から始めてそれをもつれさせることも、もつれた状態から始めてそれを分離することもできる。例えば、量子力学は可逆的であるため、もつれを引き起こした演算子の逆演算子を適用することで、分離を実現することができる。あるいは、もつれを外部環境など別のものに移すことで、分離を実現することもできる。(後者の場合、もつれは存在するが、それは 2 個の元々の量子ビット間ではなく、1 つの量子ビットと環境との間のもつれである)。

## 6.6 エンタングルメントとエントロピー

これまで私たちは、粒子 1 個、あるいは数個の粒子の状態を完全に把握した上で議論できることを前提としてきた。これを統計的に純粋な状態、あるいはもっとシンプルに**純粋状態**と呼ぶことが多い。実験では、純粋状態の系を準備することが難しい場合がある。より一般的には、異なる状態にある粒子のアンサンブルが存在し、その状態について不完全な知識しか持っていないかもしれない。このような状況で、粒子が 2 つ以上の状態にある確率が 0 でない場合を**混合状態**と呼ぶ。後述するように、フォン・ノイマンは、量子力学の記述の初歩的なレベルとして、波動関数に代わる密度行列と呼ばれる形式を開発した。密度行列表現は混合状態を非常に簡単に扱うことができ、量子力学系のエントロピーを測定し、もつれを測定する自然な方法を導き出すことができる。

波動関数  $\psi_i$  と演算子  $A$  で特徴付けられるオブザーバブルを持つ系が確率  $p_i$  で存在する混合状態を考えてみよう。オブザーバブルの平均値 (期待値ともいう) は、次のとおりである。

$$\langle A \rangle = \sum_i p_i \langle \psi_i | A | \psi_i \rangle. \quad (6.16)$$

各波動関数  $\psi_i$  を基底  $|\chi_j\rangle$  の形で展開することができる。

$$|\psi_i\rangle = \sum_j \langle \chi_j | \psi_i \rangle |\chi_j\rangle,$$

ここで、先ほどの表記では  $\langle \chi_j | \psi_i \rangle = \alpha_j^{(i)}$  となる。この展開を双対ベクトル  $\langle \psi_i |$  に対して同様に行い、式

(6.16) に代入し、和の順序を入れ替えると次のようになる。

$$\begin{aligned}\langle A \rangle &= \sum_{j,k} \left( \sum_i p_i \langle \chi_j | \psi_i \rangle \langle \psi_i | \chi_k \rangle \right) \langle \chi_k | A | \chi_j \rangle \\ &= \sum_{j,k} \langle \chi_j | \rho | \chi_k \rangle \langle \chi_k | A | \chi_j \rangle \\ &= \text{tr}(\rho A),\end{aligned}$$

ここで、

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad (6.17)$$

は、**密度行列**と呼ばれる<sup>25</sup>。トレース  $\text{tr}(\rho A)$  は表現に依存しないため、任意の便利な基底で評価することができ、期待値を計算する簡単な方法を提供する。ただし、 $\text{tr}(\rho) = 1$  であることに注意する。純粋状態の場合、ある  $i$  の値に対して  $p_i = 1$ 、それ以外では  $p_i = 0$  となる。この場合、密度行列の階数は 1 である。これは、対角基底で書けば明らかで、ゼロでない要素は 1 つだけとなる。 $p_i$  のゼロでない値が複数ある場合は混合状態となり、階数は 1 より大きくなる。

この仕組みをよりよく理解するために、非常に単純な例として  $\psi_1 = |1\rangle$  の 1 個の量子ビットを考える。もしこれが純粋状態であれば、密度行列はちょうど

$$\rho = |1\rangle \langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

となる。 $z$  軸に沿ったスピンの期待値は  $\text{tr}(\rho s_z) = 1/2$  である。しかし、50% が上向きスピン、50% が下向きスピンの混合状態であれば、次のようになる。

$$\rho = \frac{1}{2} (|1\rangle \langle 1| + |0\rangle \langle 0|) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

このとき、 $z$  軸に沿ったスピンの期待値は  $\text{tr}(\rho s_z) = 0$  となる。

このことから、フォン・ノイマンは、古典的なアンサンブルのギブス・エントロピーになぞらえて、量子状態のエントロピーを次のように定義した。

$$S(\rho) = -\text{tr} \rho \log \rho = -\sum_i p_i \log p_i. \quad (6.18)$$

量子状態のエントロピーは、ある系が「どれだけ混ざり合っているか」を定量的に示すものである。純粋な状態のエントロピーはゼロに等しいが、混合状態のエントロピーはゼロより大きい。

ある状況では、もつれ状態と混合状態の間に密接な関係がある。高次元の複数量子ビット空間では、もつれながらも純粋な状態が、低次元の状態空間から見ると混合状態に見えることがある。低次元の部分空間からの波動関数の眺めは、形式的には**部分**トレースを用いてとられる。これは、無視したい部分空間に関連するすべての座標を合計することで行われる。これは、例えば、ある特定の量子ビットしか測定できず、部分トレースを行う量子ビットを測定できないため、ある部分系を考慮から外すことに相当する。例として、式 (6.14) のもつれ状態を考え、それを 2 個目の量子ビットに関してトレースしてみよう。そのために、 $\text{tr}(|\psi\rangle \langle \phi|) = \langle \psi | \phi \rangle$

<sup>25</sup> 密度行列は量子力学のもう一つの表現である。シュレディンガー方程式を密度行列で書き換えることができるため、波動関数を使う必要は全くなくなる。

という事実を利用する。ラベル  $A$  と  $B$  を使用して量子ビットをまっすぐに保ち、 $\langle 0|1 \rangle = 0$  の形の直交座標の項を使用しているため、次のように計算できる。

$$\begin{aligned}\mathrm{tr}(|\psi_{AB}\rangle\langle\psi_{AB}|) &= \frac{1}{2}\mathrm{tr}(|1\rangle_A\langle 1|_B + |0\rangle_A\langle 0|_B)(\langle 0|_B\langle 0|_A + \langle 1|_B\langle 1|_A) \\ &= \frac{1}{2}(|1\rangle_A\langle 1|_A\langle 1|_B + |0\rangle_A\langle 0|_A\langle 0|_B) \\ &= \frac{1}{2}(|1\rangle_A\langle 1|_A + |0\rangle_A\langle 0|_A)\end{aligned}$$

これは、確率  $1/2$  で上向きスピンの下向きスピンのどちらかになる混合状態である。また、エントロピーも高くなる。対数の底が  $2$  の場合は  $S = -\log(1/2) = 1$  ビット、元の純粋な状態の場合は  $S = \log 1 = 0$  ビットとなる。一般に、統計的に純粋な分離可能な状態から始めて部分トレースを行うと、純粋な状態のままとなるが、もつれた状態から始めて部分トレースを行うと、混合状態が得られる。前者の場合、エントロピーはゼロのままだが、後者の場合、エントロピーは増大する。したがって、フォン・ノイマン・エントロピーは、エンタングルメントの有効な指標となる。

## 6.7 測定とデコヒーレンス

この節では、測定問題に戻り、古典的な測定装置を量子系に結合させる場合に生じる複雑性を説明する。古典系は、定義上、マクロな状態で記述され、 $10^{40}$  個のマクロな状態は、 $10^{40}$  個のミクロな状態に容易に対応させることができる。ガイガーカウンターや光電子増倍管のような古典的な測定装置は、量子系との相互作用が測定の結果を示すより安定した状態への崩壊を生み出すことができる準安定状態で準備される。例えば、電子の存在を検出する場合を考えてみよう。そのためには、準安定原子からなる検出器を作ればよい。電子が電磁場を介して準安定原子と相互作用して通過すると、準安定原子の崩壊を引き起こすことができ、光子の放出が観測される。通り過ぎなければ、何も観測されない。電子と光子の異なる微小状態に対応する、非常に多くの最終状態が考えられる。しかし、我々はそのことに興味はない。私たちが知りたいのは、光子が放出されたかどうかだけである。したがって、可能な限りの光子と電子の組み合わせの総和を求めなければならない。これは、電子と測定器からなる完全な系の密度行列を、最終的に光子が存在するすべての状態について追跡することに等しい。これにより、測定後の電子を記述する還元密度行列 (reduced density matrix) が導かれ、多くの可能な光子の状態に対応する混合状態にある電子が記述されることになる。このように、電子と光子の結合系ではゼロエントロピーの純粋状態から出発したにもかかわらず、電子だけの空間では正のエントロピーの混合状態になってしまう。電子の状態は古典的な確率分布に還元され、平均化される微小状態の数が膨大であるため、測定過程は熱力学的に不可逆である。飛び出してきた光子を自分の目で見なくても、準安定原子が崩壊したかどうか、つまり電子が通り過ぎたかどうかはわかるのである。

上記の測定過程の記述は、量子力学系が古典的な確率に支配されているかのように振る舞うようになる過程、すなわちデコヒーレンスの例である。このような現象がよく起こるのは、量子系がその環境、あるいは他の量子系と相互作用することによって、対象となる系の還元密度行列が特定の基底で対角化するような場合である。測定後、系が混合状態にあることがわかるように、位相はランダム化されている。この考え方によれば、波動関数は実際には収縮しておらず、量子デコヒーレンスによって収縮しているように見えるだけである。この現象の詳細についてはまだ議論があり、活発な研究が行われている [68, 69, 53, 50]。6.11 節では、単純な系同士の相互作用でもデコヒーレンスが発生しうる例を挙げる。

## 6.8 複製不可能定理

これまで、計測を行うことで元の状態を壊してしまいかねないことを見てきた。この測定行為の破壊的性質に関連する重要な結果の1つは、量子状態の複製が作れないことである。あるレジスタから別のレジスタに状態を移すことはできても、与えられた量子状態のコピーを作ることにはできない。これは、複製不可能定理で表現される [66, 18]。言い方を変え、複製不可能定理とは、ある量子ビットの任意の状態  $|\psi_1\rangle$  と別の量子ビットのある特定の状態  $|\phi\rangle$  に対して、 $|\psi_1\rangle \otimes |\phi\rangle \rightarrow |\psi_1\rangle \otimes |\psi_1\rangle$  つまり、 $|\phi\rangle$  を  $|\psi_1\rangle$  に変換する量子装置  $A$  が存在しないことを示している。 $A$  を表すユニタリー演算子を  $U_A$  とすると、 $|\psi_1\rangle|\psi_1\rangle = U_A|\psi_1\rangle|\phi\rangle$  と書き換えることができる。真の複製装置では、この性質は他のどの状態  $|\psi_2\rangle$  に対しても成り立つ必要があり、すなわち  $|\psi_2\rangle|\psi_2\rangle = U_A|\psi_2\rangle|\phi\rangle$  でなければならない。ここで、そのような装置が存在すると矛盾が生じることを示そう。 $\langle\phi|\phi\rangle = 1$ 、 $U_A^\dagger U_A = 1$  であり、 $U_A|\psi_i\rangle|\phi\rangle = U_A|\phi\rangle|\psi_i\rangle$  なので、 $\psi_1$  と  $\psi_2$  の両方を複製できる装置の存在は、以下のことを意味することになる。

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= (\langle\psi_1|\langle\phi|)(|\phi\rangle|\psi_2\rangle) = (\langle\psi_1|\langle\phi|U_A^\dagger)(U_A|\phi\rangle|\psi_2\rangle) = (\langle\psi_1|\langle\psi_1|)(|\psi_2\rangle|\psi_2\rangle) \\ &= \langle\psi_1|\psi_2\rangle^2.\end{aligned}$$

$\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2$  という性質は、 $\psi_1$  と  $\psi_2$  が直交するか等しい場合にのみ成り立つ。つまり、 $\psi_1$  と  $\psi_2$  が任意の値の場合には成り立たないので、そのような汎用複製装置は存在し得ない。実際、量子測定の不確かさを考えれば、複製不可能定理は驚くようなことではない。もし、波動関数のクローンを作ることができれば、非常に多くの波動関数のコピーを作り、それぞれのコピーについて異なる性質を測定し、元の波動関数の状態を正確に復元することで、量子測定の不確かさを回避することができるようになる。

## 6.9 量子テレポーテーション

量子テレポーテーションは、誰かに盗聴されても受信者に確実に分かる方法で、メッセージを個人的に送信する方法を提供する。これは、スター・トレックでいうところの、文字通り量子状態がテレポートされるから可能となる。つまり、量子状態は、ある場所で消滅し、別の場所で再現される。複製不可能定理により、この量子状態のコピーを複数作成することは不可能であり、その結果、テレポートした新しい状態が現れると、元の状態は消滅されなければならないのである。さらに、意図した受信者と盗聴者の両方が同時に状態を持つことは不可能であり、通信の安全性を高めるのに役立つ。

量子テレポーテーションは、6.5 節で述べたように、もつれた状態間の相関を利用したものである。アリスが、ある場所（遠いかもしれない）にいるチャーリーに安全なメッセージを送りたい、と仮定する。テレポーテーションの過程は、アリスとチャーリーがもつれた状態の異なる量子ビットを共有することに依存する。アリスは、チャーリーにテレポートしたい状態と結合している自分の部分のもつれた状態を測定し、そのもつれた状態に関する古典的な情報をチャーリーに送る。古典的な情報と自分のもつれた状態の半分があれば、チャーリーはテレポートした状態を再構築することができる。図 7 にその様子を示した。ベネットらが提案し [8]、1997 年にツァイリingerのグループが実験セットアップで初めて実現した方法 [10] に沿っている。現実的なケースでは、必要な量子ビットの状態は、左巻きと右巻きの偏光した光量子（すなわち光子）として実装されるのが一般的である。

量子テレポーテーションの最も簡単な例は、3 個の量子ビットを使って実装することができる。(A) 量子

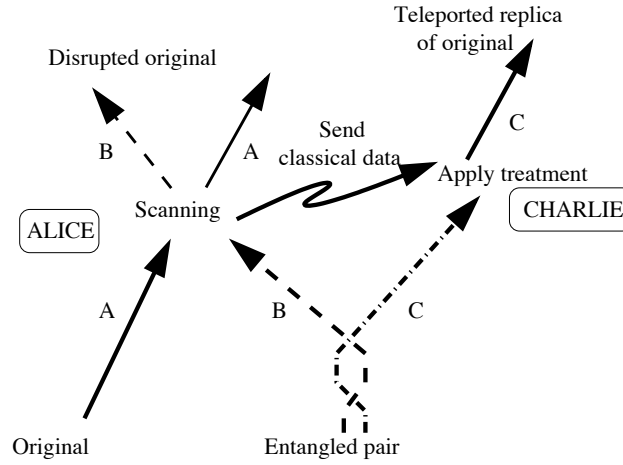


図7 ベネットらによって提案された量子状態のテレポーテーション [8]。エンタングルメント対を利用している。本文中の解説を参照。

ビットはテレポートされる未知の状態である。

$$|\psi_A\rangle = \alpha|1\rangle + \beta|0\rangle. \quad (6.19)$$

この状態は文字通り、ある場所から別の場所にテレポートしている。もしチャーリーが望むなら、量子測定によりテレポートされた状態を手に入れ、元の状態で測定したときと同じ  $\alpha$  と  $\beta$  の情報を取り出すことができるのだ。

この状態のテレポーテーションは、補助的な2量子ビットのもつれ状態によって可能となる。この2個の量子ビットに  $B$  と  $C$  のラベルを付ける。技術的な理由から、これをベル状態と呼ばれる4つの状態からなる特別な基底で表すと便利であり、次のように書かれる。

$$\begin{aligned} |\Psi_{BC}^{(\pm)}\rangle &= \sqrt{\frac{1}{2}}(|1_B\rangle|0_C\rangle \pm |0_B\rangle|1_C\rangle) \\ |\Phi_{BC}^{(\pm)}\rangle &= \sqrt{\frac{1}{2}}(|1_B\rangle|1_C\rangle \pm |0_B\rangle|0_C\rangle). \end{aligned} \quad (6.20)$$

このテレポーテーションの過程は、以下のように概説できる (図7参照)。

1. ある人がもつれた2量子ビットの状態  $BC$  (図中のエンタングルメント対) を用意する。
2. 量子ビット  $B$  はアリスに、量子ビット  $C$  はチャーリーに送られる。
3. 読み取りの段階では、アリスはベル状態の基底で、量子ビット  $A$  (図のオリジナル) ともつれた状態  $B$  の結合波動関数を測定し、崩壊したオリジナルを後に残す。
4. アリスは自分の測定結果を伝える2ビットの古典データをチャーリーに送信する (古典データ送信)。
5. アリスから受け取った古典的な情報をもとに、チャーリーは4つの演算子のうち1つを量子ビット  $C$  に適用し (処理の適用)、それによって  $A$  を再構成し、テレポートした元のレプリカを手に入れることができる。もし彼が望むなら、アリスが彼に送ったメッセージを復元するために、 $A$  を測定することができる。

ここで、この過程をより詳しく説明しよう。ステップ (1) では、(6.14) のようなのもつれた2量子ビット状

態  $\psi_{BC}$  を用意する。ステップ (2) では、量子ビット  $B$  がアリスに、量子ビット  $C$  がチャーリーに送信される。これは例えば、2 個のもつれた光子をそれぞれ 1 個ずつ送ることで実現できる。ステップ (3) では、アリスはベル状態の基底で量子ビット  $A$  と  $B$  の合同状態を測定し、2 つの古典ビット情報を得て、合同波動関数  $\psi_{AB}$  をベル状態の 1 つに射影する。ベル状態の基底は、測定の 4 つの可能な結果が等しい確率を持つという素晴らしい特性を持っている。この仕組みを見るために、便宜上、状態  $|\Psi_{BC}^{(-)}\rangle$  でもつれた状態  $BC$  を用意したとする。この場合、3 個の量子ビットの状態を合わせた波動関数は、

$$\begin{aligned} |\psi_{ABC}\rangle &= |\psi_A\rangle |\Psi_{BC}^{(-)}\rangle \\ &= \frac{\alpha}{\sqrt{2}}(|1_A\rangle|1_B\rangle|0_C\rangle - |1_A\rangle|0_B\rangle|1_C\rangle) + \frac{\beta}{\sqrt{2}}(|0_A\rangle|1_B\rangle|0_C\rangle - |0_A\rangle|0_B\rangle|1_C\rangle). \end{aligned} \quad (6.21)$$

となる。これを  $AB$  対のベル状態基底で展開すると、次のように書くことができる。

$$\begin{aligned} |\psi_{ABC}\rangle &= \frac{1}{2} \left[ |\Psi_{AB}^{(-)}\rangle(-\alpha|1_C\rangle - \beta|0_C\rangle) + |\Psi_{AB}^{(+)}\rangle(-\alpha|1_C\rangle + \beta|0_C\rangle) \right. \\ &\quad \left. + |\Phi_{AB}^{(-)}\rangle(\beta|1_C\rangle + \alpha|0_C\rangle) + |\Phi_{AB}^{(+)}\rangle(-\beta|1_C\rangle + \alpha|0_C\rangle) \right]. \end{aligned} \quad (6.22)$$

2 個の量子ビット  $AB$  は 4 つの可能な状態  $|\Psi_{AB}^{(-)}\rangle$ 、 $|\Psi_{AB}^{(+)}\rangle$ 、 $|\Phi_{AB}^{(-)}\rangle$ 、 $|\Phi_{AB}^{(+)}\rangle$  のそれぞれになる確率が等しいことがわかる。

ステップ (4) では、アリスは 2 つの古典ビットをチャーリーに送信し、自分が観測した 4 つの基底関数のうちのどれかをチャーリーに伝える。チャーリーは今、ベル基底において、自分の持つもつれた量子ビットに 4 つの可能な状態があるという事実を利用している。そして、彼の量子ビット  $C$  は、アリスが測定を行う前にアリスの量子ビット  $B$  ともつれあっていた。特に、 $|\phi_C\rangle$  を  $C$  量子ビットの状態とすると、式 (6.22) より、4 つの状態のうちの 1 つとすることができる。

$$|\phi_C\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \begin{pmatrix} -\alpha \\ \beta \end{pmatrix}; \begin{pmatrix} \beta \\ \alpha \end{pmatrix}; \text{そして} \begin{pmatrix} -\beta \\ \alpha \end{pmatrix}. \quad (6.23)$$

ステップ (5) では、チャーリーはアリスから受け取った情報をもとに、4 つの演算子  $F_i$  の中から 1 つを選択し、それを使って  $C$  量子ビットを測定する。4 つの可能なベル状態に対して、それぞれ 1 個の演算子  $F_i$  が存在する。

$$F = - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \text{そして} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \quad (6.24)$$

チャーリーが正しい古典的情報と崩れていないもつれ状態を持っていれば、適切な演算子  $F_i$  を用いて  $|\phi_C\rangle$  を測定することで、元の  $A$  量子ビットを再構成することができる。

$$|\psi_A\rangle = \alpha|1\rangle + \beta|0\rangle = F_i|\phi_C\rangle. \quad (6.25)$$

4 つの可能性をそれぞれ掛け合わせるだけで、彼の情報が正しい限り、 $A$  量子ビット  $\alpha|1_A\rangle + \beta|0_A\rangle$  を正しく再構成することが容易に確認できる。

ここで、チャーリーはアリスから古典的な測定情報を必要とすることを強調しておく。もし、それがなければ、アリスからチャーリーへ瞬時に情報が伝達されるため、テレポーテーションの過程は因果関係を侵害することになる。つまり、アリスが  $B$  量子ビットを測定すると、 $B$  量子ビットと  $C$  量子ビットがもつれ合うので、素朴に考えると、 $C$  量子ビットが瞬時に崩壊し、チャーリーがどんなに遠くにいても、アリスの測定に関する情報を送ることができると思われるかもしれない。なぜそのような瞬時のコミュニケーションが不可能なのかを理解するために、チャーリーがただランダムに結果を推測し、4 つの演算子  $F_i$  の中からランダムに 1

つを選ぶとしよう。そして、元の状態は、4つの可能な受信状態のランダムな混合状態  $|\phi_C\rangle$  として再構成される。この混合状態は、元の状態  $|\psi_A\rangle$  についての何の情報を与えない。

また、イブという名の盗聴者の可能性についても、同じ推論が成り立つ。もし彼女がチャーリーより先に量子ビット (C) を傍受して測定することに成功すれば、2ビットの古典的情報が無くては元の状態を回復することはできないだろう。さらに彼女は、その状態に影響を与えたことになる。もし、チャーリーが何らかの方法で壊れた状態を手に入れても、元の状態  $A$  を再構築することはできない。アリスが最初に、再構成後にチャーリーによって確認される既知の状態のシーケンスを送信すれば、セキュリティは達成される。もし、元のシーケンスと再構成されたシーケンスが完全に相関していれば、イブが干渉していないことが保証される。アリスが測定を行うとき、量子ビット  $B$  と同様に状態  $\psi_A$  を変化させるので、複製不可能定理が満たされることに注意しなければならない。一度そうしてしまえば、元の  $\psi_A$  を復元する唯一の望みは、彼女が自分の測定値をチャーリーに送り、チャーリーが自分のもつれた量子ビット  $C$  に適切な演算子を適用することである。

テレポーテーションの量子セキュリティ機構は、強相関・高非局在のもつれた状態に基づいている。相関の非局所性は長所である反面、短所でもある。量子相関は非常に壊れやすく、環境とのランダムな相互作用、すなわちデコヒーレンスによって壊される可能性がある。先に述べたように、これは量子相関が破壊され、情報が失われる過程である。デコヒーレンスの問題は、量子技術の大規模な開発・応用を進める上で大きな障害となっている。それでも、2006年にジュネーヴ大学のギジンの研究グループが、スイスコムの光ファイバー網を使って 550m の距離のテレポーテーションに成功している [41]。

## 6.10 量子計算

量子計算は、個々の量子ビットを連続的に結合させ、波動関数の時間発展を所定の方法で変化させる非自明な力学を持つ制御された相互作用を設定することで実行される。多量子ビット系はまず、プログラムへの入力を表す既知の初期状態に準備される。次に、磁場などの力を加えて相互作用のスイッチを入れ、その状態空間で波動関数が回転する方向を決定する。したがって、量子プログラムは、初期状態に外部から適用される一連のユニタリ演算に過ぎない。実際には、これらはの対応する一連の量子ゲートによって実現される。計算が終わると測定が行われ、最終的な状態が読み出される。

量子計算は、基本的にはアナログ計算の一種である。物理系と数学系が同じ方程式に従うという事実を利用し、物理系で数学的問題をシミュレートする。数学的問題は、適切な運動方程式を生成する磁場等の適切な配置を見つけることで、物理系にマッピングされる。そして、初期状態を用意し、系を発展させ、答えを読み出す。アナログコンピュータは今に始まったことではない。例えば、ライプニッツは 1694 年に乗算を行うための機械式計算機を開発し、20 世紀半ばには、デジタルコンピュータに比べて圧倒的に速度が優れていたため、微分方程式を解くために電子式アナログコンピュータがよく使われた。

では、なぜ量子計算が特別なのか。その卓越したパワーの鍵は、計算の途中段階での大規模な並列処理にある。与えられた状態に対する演算は、すべての基底ベクトルに対して全く同じように働く。 $n$  量子ビット系の量子計算を定義する物理過程は、このように  $2^n$  個の複素数の集合に対して並列に作用し、これらの数の位相（古典計算では存在しない）は、状態の時間発展を決める上で重要である。計算の最後に測定して答えを読み出すと、 $n$  ビットの出力が残り、位相情報が失われる。

量子測定は一般に確率的であるため、「同じ」計算でも異なる「答え」が得られる可能性がある。なぜなら、測定過程によって系が異なる固有状態に投影されるからである。そのため、誤り訂正の仕組みが必要になることもあるが、いくつかの問題、例えば大きな数の因数分解などでは、答えが合っているかどうかを確認するだ



けで、結果の正しさを確認することが可能である。また、量子コンピュータはデコヒーレンス、つまり、計算に使われる量子状態と環境との間の本質的にランダムな相互作用によって、誤りを犯す可能性もある。このこともまた、誤り訂正の仕組みが必要な理由です。

このデコヒーレンス問題は、量子計算を物理的に実現する上で、おそらく最も困難な問題であろう。これらの問題は、量子状態が局所的にではなく、外部（局所）ノイズによって破壊されない系のトポロジカルな特性として、グローバルに符号化されるシステムを構築することで克服できる可能性がある。これを**トポロジカル量子コンピューティング**と呼ぶ。この興味深い可能性は、トポロジカル秩序を示すある種の二次元物理媒体において生じる。これは、本質的な量子自由度とその相互作用がトポロジカルである物質の状態を指す [36, 14]。

## 6.11 量子ゲートと量子回路

古典ゲートが古典コンピュータの構成要素であるのと同様に、量子ゲートは量子コンピュータの基本構成要素である。古典計算に使われるゲートは、2進数の入力に対して2進数の演算を行い、0を1に変えたり、その逆を行ったりするものである。例えば、唯一の非自明な1ビット論理演算は *NOT* で、0を1に、1を0にするものである。量子計算では、量子ビットが0と1の重ね合わせで存在することができるため、状況はまったく異なる。許容される単一量子ビット演算のセットは、 $U^\dagger U = 1$  となる  $2 \times 2$  複素行列  $U$  に対応するユニタリー変換で構成される。1つの量子ビットに対応する動作は、図8に示すような回路で表現される。量子

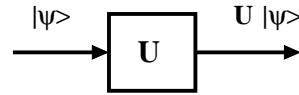


図8 量子ビットの状態  $|\psi\rangle$  に対する量子ゲートに対応するユニタリー行列  $U$  の作用を表す図。

ゲートには古典的な類似性を持つものもあるが、多くはそうではない。例えば、演算子  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  は、古典的な *NOT* ゲートに相当し、上向きスピンと下向きスピンを入れ替える機能を持つ。これに対して、操作  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  は波動関数の位相を180度回転させるもので、古典的な演算で同等なものはない。

汎用量子コンピュータは、任意の  $n$  量子ビットの入力を、計算結果に対応する  $n$  量子ビットの出力に変換できなければならない。このような計算を実現するには、原理的には、非常に複雑で、任意の順序と複雑さを持つ量子ゲートを作る必要があるかもしれない。幸いなことに、普遍的量子コンピュータを実現するために必要な変換は、例えば、1量子ビットと2量子ビットのゲートをうまく組み合わせることで、単純な（いわゆる普遍的）量子ゲートのセットで生成できることを証明することが可能である。1量子ビットゲートは、実数自由度3のユニタリー行列である。有限の精度で作業することを許せば、すべてのゲートの集合は、よく選ばれた小さな集合で任意によく近似することができる。これには多くの可能性があり、最適な選択は、量子ビットの物理的な実装に依存する。代表的な1量子ビットの論理ゲートとしては、例えば以下のようなものがある。

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (6.26)$$

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & \exp i\theta \end{pmatrix} \quad (6.27)$$

$$H = \sqrt{\frac{1}{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (6.28)$$

$X$  は古典的な  $NOT$  ゲートの量子版であり、 $|1\rangle$  と  $|0\rangle$  を入れ替える機能を持つ。他の 2 つは古典に相当するものがない。 $P(\theta)$  演算は位相ゲートに相当し、相対位相を  $\theta$  度変化させるもので、 $\theta$  は  $\pi$  の無理数倍となるのが一般的である。3 番目のゲートには、いわゆるアダマールゲート  $H$  を選ぶことができ、これは基底状態の重ね合わせ  $|1\rangle \Rightarrow \frac{1}{2}(|1\rangle + |0\rangle)$  を作るものである。

実験実装の観点から、便利な 2 量子ビットゲートは  $CNOT$  ゲートである。 $CNOT$  ゲートとアダマールゲートの組み合わせで普遍集合を形成することが示されている [4]。 $CNOT$  ゲートは、状態  $|A\rangle \otimes |B\rangle$  に対して次のように作用する。

$$CNOT : |A\rangle \otimes |B\rangle \Rightarrow |A\rangle \otimes |[A + B] \bmod 2\rangle \quad (6.29)$$

つまり、 $CNOT$  ゲートは、 $A = 1$  なら  $B$  の状態を反転させ、 $A = 0$  なら何もしない。行列形式で  $CNOT$  ゲートを書くと、次のようになる。

$$CNOT : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (6.30)$$

図 9 に基底状態での動作を詳細に示した。

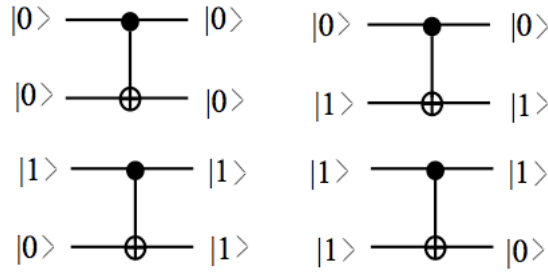


図 9 式 (6.30) で定義された  $CNOT$  ゲートが 4 つの可能な 2 量子ビットの基底状態に対して作用することを表す回路図。上側の量子ビットの塗りつぶされた点は制御を、十字は条件付き 1 量子ビットの  $NOT$  ゲートの記号を表している。

$CNOT$  ゲートを用いると、次のように分離可能な状態からもつれた状態を生成することができる。

$$CNOT : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \Rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (6.31)$$

実際、直感的に理解できるように、量子コンピュータが古典コンピュータに比べて大幅な高速化を実現できるのは、もつれ状態を含む高次元の状態空間を操作する能力に関係している。分離可能な  $n$  量子ビットの状態を  $k$  ビットの精度で記述するためには、個々の量子ビットを別々に記述すればよいので、 $nk$  ビットのオーダーで済む。一方、 $n$  量子ビットのもつれ状態を記述するためには、ヒルベルト空間の各次元に対して  $k$  ビットのオーダー、つまり  $k2^n$  ビットのオーダーが必要である。もし、古典的なコンピュータでもつれた状態の時間発展をシミュレーションしようとする、これらの情報をすべて処理しなければならず、計算が非常に遅くなってしまう。一方、量子計算では、これらの情報を一度に処理する。つまり、もつれた状態に対して行う量子計算も、分離可能な状態に対して行う量子計算と同じように高速に処理することができる。このように、もつれた状態の時間発展を解くことが難しい数学的問題にマッピングできる状況を見つければ、大幅なスピードアップが可能となるかもしれない。

また、 $CNOT$  ゲートは、デコヒーレンスがどのように発生するかを説明するために使用することができる。分離可能な状態からもつれた状態を生成するのと同じ作用で、1量子ビットの視点から見ると、結果として得られる状態はデコヒーレンスになる。つまり、式 (6.31) を密度行列表現で見た場合を考える。最初の量子ビットだけを見ると、分離可能な状態の波動関数は  $|\psi\rangle = 1/\sqrt{2}(|1\rangle + |0\rangle)$ 、つまり密度行列で表すと

$$\begin{aligned} |\psi\rangle\langle\psi| &= \frac{1}{2}(|1\rangle\langle 1| + |1\rangle\langle 0| + |0\rangle\langle 1| + |0\rangle\langle 0|) \\ &= \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

となる。 $CNOT$  の作用で、これは  $\frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 、つまり対角行列となる。

## 6.12 アプリケーション

現在、量子コンピュータの実現に向けて、さまざまな取り組みが行われている。原理的に必要なのは、簡単に操作でき、多数の量子ビットにスケールアップできる単純な2準位量子系である。最初の要件はあまり制限的ではなく、単一または少数の量子ビットを持つシステムの多くの異なる物理的実装が達成されている。例えば、NMR、スピン格子、光子1個による線形光学、量子ドット、ジョセフソン接合ネットワーク、イオントラップ、光学格子内の原子と極性分子などである [17]。これまで実用的な計算への進展を阻んできたはるかに難しい問題は、個々の量子ビットを制御可能な方法で結合させ、十分に低いレベルのデコヒーレンスを実現することである。現在行われている偉大な努力によって、今後の展開は驚くほど早くなる可能性がある<sup>26</sup>。もし、量子コンピュータが自由に使えるようになったら、どんな奇跡を起こすのだろうか。本節の冒頭で述べたように、量子発展に内在する大規模な並列性が劇的なスピードアップをもたらすにあたって、数多くの問題が存在する。重要なのは、古典的なコンピュータでは同じ計算ができないということではない。結局のところ、古典的なコンピュータで量子コンピュータをシミュレートすることはいつでも可能である。むしろ、必要なのは時間である。既に述べたように、最も目を見張るような高速化は、大きな数を素因数分解するショアのアルゴリズム (1994) である [56]。多くのセキュリティ鍵は、大きな数が素因数分解できないことに基づいているため、指数関数的に難しい問題から多項式的に難しいそれへの削減することで、暗号解読のために多くの実用的な応用例となる。もう一つの重要な応用例として、広い空間を探索する必要がある巡回セールスマンのような問題に対するグローバーのアルゴリズム (1996) による二次的な高速化が挙げられる [26]。最後に、重要な応用として、量子系そのもののシミュレーションがある [3]。量子コンピュータがあれば、当然、指数関数的にスピードアップし、それがそのまま新しい量子技術の開発にフィードバックされる。

量子計算とセキュリティは、物理学と情報理論の基本概念の驚くべき重要な相互作用のもう一つの挑戦的な例である。物理学者や技術者が量子技術の習得に成功すれば、情報科学における重要な転換点となることだろう。

## 参考文献

- [1] *Nonlinear time series analysis*, Cambridge University Press, Cambridge, UK, 2006.

<sup>26</sup> 16 量子ビットの量子コンピュータは、カリフォルニア州の D-Wave Systems Inc. が初めて発表した。本稿執筆時点ではこの製品はまだ発売されていない。

- [2] H. Akaike, *A new look at the statistical model identification*, IEEE Transactions on Automatic Control **19** (1974), no. 6, 716–723.
- [3] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon, *Simulated quantum computation of molecular energies*, Science **309** (2005), 1704.
- [4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Quantum Physics Archive (Los Alamos National Laboratory) (1995).
- [5] C. Beck, *Dynamical foundations of nonextensive statistical mechanics*, Phys.Rev.Lett. **87** (2001), 180601.
- [6] C.H. Bennett, *The thermodynamics of information - a review*, Int. Journ. of Theor. Phys **21** (1982), 905–940.
- [7] C.H. Bennett, *Demons, engines and the second law*, Scientific American **November** (1987), 108–116.
- [8] C.H. Bennett et al., *Teleporting an unknown quantum state via dual classical and epr channels*, Phys.Rev.Lett. **70** (1993), 1895–1899.
- [9] L. Boltzmann, *Vorlesungen über Gastheorie*, university of california press, berkeley, 1964 ed., translated by S.G. Brush, vol. I and II, J.A. Barth, Leipzig, *Lectures on Gas Theory*, 1896-1898.
- [10] D. Bouwmeester et al., *Experimental quantum teleportation*, Nature **390** (1997), 575–9.
- [11] L. Brillouin, *Science and information theory*, Academic Press, 1956.
- [12] J.P. Crutchfield, J.D. Farmer, N.H. Packard, and R.S. Shaw, *Chaos*, Scientific American **254** (1986), no. 12, 46–57.
- [13] J.P. Crutchfield and K. Young, *Inferring statistical complexity*, Phys.Rev.Lett. **63** (1989), 105–108.
- [14] S. DasSarma, M. Freedman, C. Nayak, S.H. Simon, and A. Stern, *Non-abelian anyons and topological quantum computation*, <http://arXiv:0707.1889> (2007).
- [15] K.G. Denbigh and J.S. Denbigh, *Entropy in relation to incomplete knowledge*, Cambridge University Press, 1985.
- [16] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London **A400** (1985), 97.
- [17] D.P. Di Vincenzo, *The physical implementation of quantum computation*, (2000).
- [18] D. Dieks, *Communication by epr devices*, Phys.Lett. **A 92** (1982), 271.
- [19] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete*, Phys. Rev. **47** (1935).
- [20] J.D. Farmer, *Information dimension and the probabilistic structure of chaos*, Zeitschrift in Naturforschung **37A** (1982), 1304–1325.
- [21] J.D. Farmer, J. P. Crutchfield, H. Froehling, N. H. Packard, and R. S. Shaw, *Power spectra and mixing properties of strange attractors*, Annals of the New York Academy of Science **375** (1980), 453–472.
- [22] J.D. Farmer and J. Geanakoplos, *Power laws in economics and elsewhere*, Tech. report, Santa Fe Institute, 2006.
- [23] R.P. Feynman, *There is plenty of room at the bottom*, Engineering and Science, Caltech (February,

- 1959) (and <http://www.zyvex.com/feynman.html>).
- [24] M. Gell-Mann and C. Tsallis, *Nonextensive entropy: Interdisciplinary applications*, Proceedings Volume in the Santa Fe Institute Studies in the Sciences of Complexity, Oxford University Press, 2004.
  - [25] J.W. Gibbs, *Elementary principles in statistical physics*, Yale University Press, 1902.
  - [26] L.K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (1996), 212–219.
  - [27] P.D. Grunwald, I.J. Myung, and M.A. Pitt, *Advances in minimum description length: Theory and applications*, MIT Press, 2004.
  - [28] P.D. Grunwald and P.M.B. Vitányi, *Algorithmic information theory*, Chapter 3 of this book.
  - [29] Y.M. Guttman, *The concept of probability in statistical physics*, Cambridge University Press, 1999.
  - [30] A.S. Holevo, *Probabilistic and statistical aspects of quantum theory*, North Holland Publishing Company, Amsterdam, 1982.
  - [31] K. Huang, *Statistical mechanics*, Wiley and Sons, 1987.
  - [32] E.T. Jaynes, *Information theory and statistical mechanics*, in Statistical Physics (K. Ford ed.), Benjamin, New York, 1963.
  - [33] E.T. Jaynes, *Papers on probability, statistics and statistical physics*, (R.D. Rosenkranz ed.), 1983.
  - [34] E.T. Jaynes, *The Gibbs paradox*, Tech. report, <http://bayes.wustl.edu/etj/articles/gibbs.paradox.pdf>, 1996.
  - [35] P.R. Kaye, R. Laflamme, and M. Mosca, *Introduction to quantum computing*, Oxford University Press, USA, 2007.
  - [36] A. Kitaev, *Fault tolerant quantum computation by anyons*, Annals of Physics **321** (2003), 2–111.
  - [37] A.I. Khinchin, *Mathematical foundations of statistical mechanics*, Dover, New York, 1949.
  - [38] C. Kittel, *Elementary statistical physics*, Wiley and Sons, 1966.
  - [39] R. Landauer, *Irreversibility and heat generation in the computing process*, IBM Journal of Research and Development **5** (1961), 183–191.
  - [40] R. Landauer, *Information is physical*, Physics Today **44** (1991), 23–29.
  - [41] O. Landry et al., *Quantum teleportation over the Swisscom telecommunication network*, Journ.Opt.Soc.Am. B **24** (2007), February 2007.
  - [42] E.M. Lifschitz and L.D. Landau, *Statistical physics*, Course of Theoretical Physics, vol. 5, Butterworth-Heinemann, 1980.
  - [43] S. Lloyd, *Quantum computers*, Wiley-International, 2008.
  - [44] E.N. Lorenz, *Deterministic nonperiodic flow*, Journal of Atmospheric Sciences **20** (1963), 130–141.
  - [45] J.C. Maxwell, *Theory of heat*, D. Appleton & Co, New York, 1872.
  - [46] N.D. Mermin, *Quantum computer science: An introduction*, Cambridge University Press, 2007.
  - [47] L.G. Moyano, C. Tsallis, and M. Gell-Mann, *Numerical indications of a q-generalised central limit theorem*, Europhys. Lett. **73** (2006), 813.
  - [48] M.E.J. Newman, *Power laws, Pareto distributions and Zipf’s law*, Contemporary Physics **46** (2005), 323–351.
  - [49] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University

- Press, 1990.
- [50] R. Omnes, *Understanding quantum mechanics*, Princeton University Press, 1999.
  - [51] F. Reif, *Fundamentals of statistical and thermal physics*, McGraw-Hill, 1965.
  - [52] J. Rissanen, *Modeling by the shortest data description*, Automatica **14** (1978), 465–471.
  - [53] M. Schlosshauer, *Decoherence, the measurement problem, and interpretations of quantum mechanics*, Reviews of Modern Physics **76** (2004), 1267–3105.
  - [54] C.E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal **27** (1948), 379–423, 623–656.
  - [55] R.S. Shaw, *Strange attractors, chaotic behavior and information flow*, Z. Naturfor **36A** (1981), no. 1, 80–112.
  - [56] P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press (1994), 124134.
  - [57] S. Still and J.P. Crutchfield, *Structure or noise*, <http://arXiv:physics.gen-ph/0708.0654> (2007).
  - [58] S. Strogatz, *Nonlinear dynamics and chaos*, Addison Wesley, 1994.
  - [59] L. Szilard, Z. Physik **53** (1929), 840.
  - [60] R.C. Tolman, *Principles of statistical physics*, Clarendon, Oxford, UK, 1938.
  - [61] C. Tsallis, *Possible generalization of Boltzmann-Gibbs statistics*, J.Stat.Phys. **52** (1988), 479.
  - [62] C. Tsallis, M. Gell-Mann, and Y. Sato, Europhysics News 36, Special Issue "Nonextensive Statistical Mechanics: New Trends, new perspectives", eds. J.P. Boon and C. Tsallis (2005), 186.
  - [63] C. Tsallis, M. Gell-Mann, and Y. Sato, *Asymptotically scale-invariant occupancy of phase space makes the entropy  $s_q$  extensive*, JProc. Natl. Acad. Sc. USA **102** (2005), 15377.
  - [64] S. Umarov, C. Tsallis, and S. Steinberg, *A generalization of the centrallimit theorem consistent with nonextensive statistical mechanics*, Tech. report, arXiv:cond-mat/0603593, 2006.
  - [65] S. Umarov et al.,  *$q$ -Generalization of symmetric alpha-stable distributions*, cond-mat/0606038/40 (2006).
  - [66] W.K. Wootters and W.H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.
  - [67] J. Zinn-Justin, *Quantum field theory and critical phenomena*, Clarendon Press, Oxford, UK, 1989.
  - [68] W.H. Zurek, *Decoherence and the transition from quantum to classical*, Physics Today **44** (1991), 36–44.
  - [69] W.H. Zurek, *Decoherence, einselection, and the quantum origins of the classical*, Reviews of Modern Physics **75** (2003), 715.