

# 光コンピューターと量子コンピューター

谷田 純

## Optical Computers and Quantum Computers

Jun TANIDA

Relationship between optical and quantum computers capable of implementing a large scale parallel computation is discussed. Optical computers use spatial parallelism of optical information, whereas quantum computers utilize parallelism of quantum states. Consideration on the relation is expected to be useful for developing a new class of optical information processing merged with the concepts of quantum computing. In this article, the fundamentals and the optical implementations of quantum computers and the current status of optical computer researches are described. Then the common features of the both computers and possible future directions are considered.

**Key words:** optical computer, quantum computer, information photonics, photon, parallel processing

情報科学の進展にともない、ネットワークを利用したさまざまな情報サービスの提供が始まっているが、その一方で、情報セキュリティの重要性はますます高くなっている。この情報セキュリティへの関心の高まりにおいて、量子通信による暗号鍵配付や量子コンピューターによる因数分解の高速解法は、多くの光関連研究者にとっても気になる対象である。

量子コンピューターを論じる場合、光分野で対応するシステムとして、光コンピューターがあげられる。量子コンピューターのすぐれた演算能力は、おもに量子状態の重ね合わせに基づいた並列処理性に起因するが、空間に分布する光情報の並列性を利用する光コンピューターとの間に何らかの関連が考えられる。そこで、これらの関係を明らかにすることにより、量子情報処理の考え方を加えた新しい光情報処理の展開への糸口が期待される。しかし、量子コンピューターは、多くの解説書や論文<sup>1,2)</sup>があるにもかかわらず、専門外の研究者にとって敷居の高い分野である。ここでは、筆者なりにこの問題をかみ砕き、新しい光情報処理技術の開発に向けた手がかりとなりうる解説を試みる。

以下、量子コンピューターに関する基本的な概念をまとめ、光による実装例を紹介する。光コンピューター研究の現状の紹介を行い、いくつかの観点により、光コンピューターと量子コンピューターの接点について考察する。

### 1. 量子コンピューターの基本概念

#### 1.1 量子計算

量子計算は、量子力学の原理に基づく新しい情報処理パラダイムである。これは、物理的実装を出発点にしたパラダイムではなく、量子力学が示す興味深い特性を有効利用するように構築された理論先行型の学問領域といえる。Shor が示した多項式計算時間による因数分解アルゴリズム<sup>3)</sup>は、既存の情報セキュリティ技術の根幹を揺るがすものであり、量子コンピューター開発への強い動機づけとなった。

#### 1.2 量子ビット

量子計算の特徴を明らかにするために、既存の(古典的)デジタル演算との比較を行う。デジタル演算は2つの値(0または1)をとるビットを情報単位とするが、量子計

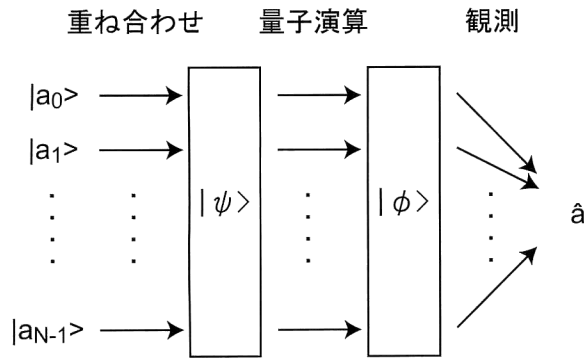


図1 量子計算の流れ。

算では、量子ビットと呼ばれる量子状態を用いる。量子状態は、量子力学における波動関数  $\psi$ 、あるいは状態ベクトル  $|\psi\rangle$  として表される。2つの基底 ( $|0\rangle$  または  $|1\rangle$ ) をとる量子状態  $|q\rangle$  を考えると、量子状態  $|q\rangle$  は各基底の重ね合わせ状態として存在する。すなわち、

$$|q\rangle = a|0\rangle + b|1\rangle, \quad |a|^2 + |b|^2 = 1 \quad (1)$$

これが量子ビットであり、量子計算における情報単位となる。

### 1.3 量子ゲート

デジタル演算は、論理積や論理和などの基本的な論理ゲートの組み合わせにより任意の論理演算を実現する。量子計算においても、基本的な量子ゲートの組み合わせとして量子回路を構成する。代表例として、アダマール変換ゲートと制御ノットゲートなどがあげられる。これらは、量子ビットを入力とし、量子ビットを出力とする。量子ゲートは、入力とする量子状態に対するユニタリー演算子で表され、重ね合わされているすべての基底に対して一括処理を行う。

デジタル演算における演算自由度は使用ビット数によって決められるが、量子計算においても、量子ビット数を取り扱おう情報のサイズを決定する。複数の量子ビットは、単一量子ビットの直積として表される。例えば、 $n$  量子ビット ( $|q_1 q_2 \dots q_n\rangle$ ) の場合、 $2^n$  元のベクトルを用いて表現される。複数量子ビットを処理するためには、複数入力の量子ゲートが必要である。これは、複数の量子状態に対してユニタリー演算子を一括作用させることに相当する。

### 1.4 量子アルゴリズム

量子計算における重要な成果には、Shor の因数分解アルゴリズムのほか、Deutsch-Jozsa の量子並列化アルゴリズム<sup>4)</sup>、Grover の量子検索アルゴリズム<sup>5)</sup> があげられる。量子計算の演算能力の本質は、重ね合わせ量子状態に対する一括的な操作による並列処理性にある。図1に、その概念

表1 量子コンピューターの提案例。

方式	量子ビット	演算方法
核磁気共鳴	原子・分子・原子核スピン	外部磁場
イオントラップ	イオン電子準位	レーザー光
量子ドット	電子準位	マイクロ波
光子	偏光・光路	線形光学素子

を示す。多数の情報が重ね合わせられた入力量子状態を用意し、量子回路に対応する操作を適用する。この出力量子状態には、すべての入力量子状態に対応した演算結果が含まれる。そのため、一度の操作で多数の情報に対する演算結果を得ることができる。ただし、量子力学の要請により、量子状態は一度観測すると壊れてしまうため、一度の観測で有用な解を検出できるように、出力量子状態の形式を適切に設計しなければならない。

### 1.5 量子コンピューター

量子アルゴリズムで記述された演算を実現する物理システムが量子コンピューターである。量子ビットや量子ゲートをいかにして実現するかが課題であり、多くの研究者がしのぎを削っている。表1にまとめたように、核磁気共鳴<sup>6)</sup>、イオントラップ<sup>7)</sup>、量子ドット<sup>8)</sup>、そして光子<sup>9)</sup>を用いた量子コンピューターの検討がなされている。量子ビットとしての光子のみならず、演算方法にレーザー光やマイクロ波などが用いられている点は注目すべきである。

## 2. 光による量子計算の実装

光子の偏光状態を量子ビットとして用いることができる。この場合、直交する2つの偏光状態（垂直偏光と水平偏光、あるいは右円偏光と左円偏光）を基底とする重ね合わせ状態が情報を保持する。しかし、これだけでは1量子ビットだけしか実現できず、複数の量子ビットを必要とする大規模な量子コンピューターを構成することはできない。そこで、図2に示すように、光子が通過する光路も量子状態として用いられる。ビームスプリッターに入射した光子は、その光子自身の量子状態に応じて、直進あるいは反射のいずれかの光路をとるため、光子が通過する光路に量子状態を対応づけることが可能になる。その結果、ビームスプリッターや反射鏡などの線形光学素子により量子回路を構成することができる<sup>10)</sup>。さらに、光子は物質との相互作用がない限り、その偏光状態や光路を変えることがないため、容易に実験光学系を構成することができる。具体的な量子回路として、Deutsch-Jozsa アルゴリズム<sup>11)</sup> や制御ノット量子ゲート<sup>12)</sup> の実装が報告されている。

線形光学素子による量子回路構成法の問題としては、多量子ビットの実装方法と処理効率の低さがあげられる。光

路を量子ビットとして用いる場合、量子ビット数  $n$  に対して、 $2^n$  本の光路が必要となり、多くの量子ビットを実装することは困難である。また、演算に用いる光子の量子状態は光源まかせであるため、演算に適さない量子状態の光子は捨てなければならず、演算効率の低下は避けられない。ただし、これらの問題については、最近ブレイクスルーが得られている<sup>2)</sup>。このような問題はあるものの、容易に量子回路を構成することができる点は、光による実装の最大の特徴であり、この特徴を有効に生かした発展が期待されている。

光子の量子状態の性質を効果的に利用した量子情報技術として、量子暗号が報告されている。量子状態は観測により破壊されてしまうが、この性質と通信プロトコルの組み合わせにより、通信路における盗聴者の存在を発見する暗号通信方式が Bennett と Brassard によって考案された<sup>13)</sup>。この場合、光子の偏光を量子状態として用いるが、光子 1 個ずつに情報を載せる場合には、多量子ビット化は必要ない。量子アルゴリズムの実装は難しいが、光子の特性を利用した量子暗号通信は実用化に向けた開発が進められている。

### 3. 光コンピューターの現状

光コンピューターは、光の物理的特性の有効利用に基づく情報処理システムとして構想された。特に、自由空間における光波伝搬などにみられる光学現象の並列性が着目され、大規模並列処理システムの実現に向けた研究が進められた<sup>14)</sup>。1980 年代初頭の光コンピューター研究は、従来の光情報処理技術とデジタル演算技術の融合にあった。並列光論理ゲートをはじめ、並列光論理回路、並列アルゴリズム、そして独自アーキテクチャーに基づくデモンストレーションシステムが開発された。しかし、エレクトロニクスの飛躍的な発展は、デジタル演算の単純な物理実装としての光コンピューターの魅力を色あせたものにした。新規な情報システムを構築するには多大な周辺技術の支えが必要であったが、その進展を上回る速さでエレクトロニクスが発展し、当初考えられた光コンピューターの開発研究は停滞してしまった。

現在、光コンピューターを直接の目標とした研究はほとんど行われていないが、情報フォトニクス<sup>15)</sup> という概念のもとで、いくつかの流れが生まれている。VLSI (very large scale integration; 超大規模集積回路) フォトニクスは、半導体集積回路素子と受発光素子の組み合わせによる新しい情報システムの開発をめざす。これは、最新のエレクトロニクスによる光コンピューターアーキテクチャーの実装と

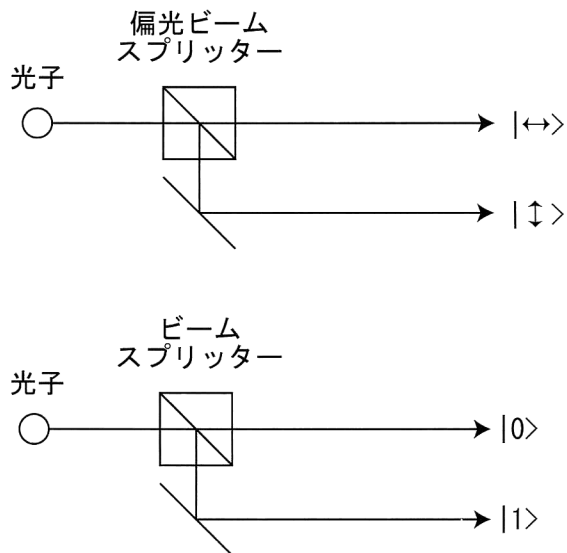


図2 光による量子ビット。下図の  $|0\rangle$ ,  $|1\rangle$  は光子数状態ではなく、光路に光子の量子状態を対応させたものを意味する。

みなすことができる。きわだった成果として、光バックプレーンモジュール<sup>16)</sup>、ビジョンチップを中心とする Ocular System<sup>17)</sup>、三次元光エレクトロニクス集積プロセッサ<sup>18)</sup>などがあげられる。

一方、光コンピューターという複雑なシステムではなく、特定の演算処理に特化することで光技術の特性を生かそうとする光情報処理技術への回帰の流れもある。手法自体は既存の光情報処理に基づくものが多いが、特定の応用を目標としたシステム開発が特徴である。光相関演算による顔認識システム<sup>19)</sup>、ランダム信号による画像暗号化<sup>20)</sup>、時空間変換に基づく超高速信号処理<sup>21)</sup>、各種の三次元情報技術<sup>22)</sup>などがあげられる。

さらに、新しい情報処理手法の開拓をめざした萌芽的な研究も進められている。画像情報に対する再帰的変換と非線形処理により時空間発展パターンを生成する並列フィードバック系<sup>23)</sup>は、複雑系を模倣する光情報システムであり、複雑系科学への寄与が期待される。また、分子の自律反応性に基づく DNA コンピューティングに対して、光による局所的分子制御を導入したフォトニック DNA コンピューティング<sup>24)</sup>なども提案されている。

### 4. 光コンピューターと量子コンピューターの接点

デジタル光コンピューターを起源とする並列光コンピューター研究をみる限り、量子コンピューターとの接点は乏しい。しかし、光子の量子状態を光路に対応させる方式においては、光コンピューターで利用されてきた空間並列性が利用できる可能性がある。本章では、いくつかの観点

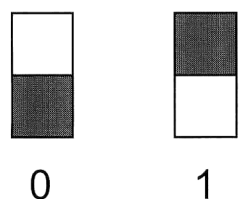


図3 空間符号パターン。

から、2つのコンピューターの関係を考える。

#### 4.1 古典光学と量子光学

従来の光コンピューターではエネルギーや波としての光が利用されるのに対し、量子コンピューターでは量子状態を保持する粒子としての光が用いられる。それぞれのコンピューターを理論的に記述し、実験系を構築する場合には、幾何光学や波動光学などの古典光学と量子論に基づく量子光学という本質的に異なる取り扱いをしなければならない。簡便に光子を利用するためには、光源からの光を減衰器を通して極微弱光にすればよい。光子相互間の量子状態の関係を考慮しなくてもよい場合には、この手法でも実験が行える。しかし、光源まかせの光子発生では、演算効率の向上を望めない。さらに、単一光子源や光子計数検出器などの特殊な光学装置を用いれば、ビームスプリッターや反射鏡などの線形光学素子で量子ゲートが実現可能である<sup>12)</sup>という報告がなされている。同じ対象や装置を利用する場合であっても、古典光学と量子光学とは本質的に異なるものであることを認識する必要がある。

#### 4.2 システム実装技術

現在の光コンピューターの一形態であるVLSIフォトリニクスは、システム実装の必然性から生み出された。システム実装を考慮した場合、半導体エレクトロニクスを有効利用することが最も効果的であり、発展性の点でも有利である。システム実装としての完成度でも、VLSIフォトリニクスは高いレベルに達している。この分野では、半導体集積回路素子と受発光素子の組み合わせによる演算素子だけではなく、それらを統合してシステムを構築する技術として、回折光学素子やMEMS素子などが利用されている。一方、光子を用いる量子コンピューターに関する研究は、原理開発を含めて始まったばかりであり、現時点でシステム実装を考慮するのはあまり意味がないかもしれない。しかし、光路による量子ビット表現を利用する場合、必要となる光路数は量子ビット数に対して指数関数的に増大する。そのため、コンパクトな光学システム実装が不可欠であるが、このような問題において光システム実装技術が重要な役割を果たすものと期待される。

#### 4.3 空間符号化技術

光路による光子の量子ビット表現は、デジタル光コンピューターにおける情報表現法として開発された空間符号化技術<sup>25)</sup>と等価なもののみならずとすることができる。空間符号化技術は、図3に示すように、論理値を局所的な空間符号パターンに変換する技術で、光学処理の空間並列性を利用するために導入された。光路による量子ビット表現では、必ずしも対応する光路を並べる必要はないが、それらを組にして局所領域に配置すると空間符号化技術と同等なものになる。空間符号化技術に関連してさまざまな演算光学系や符号化光学系が考案されており、量子コンピューターにおいて空間並列性を利用するうえでの何らかのヒントが得られるものと期待される。

#### 4.4 量子アルゴリズム

量子アルゴリズムが取り扱う問題は、既存の光コンピューター技術によって解くこともできる。図4に、Deutsch-Jozsa問題<sup>4)</sup>を並列光コンピューティング技術によって解く実験光学系を示す<sup>26)</sup>。Deutsch-Jozsa問題は状態の重ね合わせと位相シフトで実現されるもので、実験光学系では、それらを信号配置と空間光変調素子により実装している。ただし、一度に多数の状態を重ね合わせてしまうと出力信号の判定が困難になるため、2つずつの信号組みを複数用意し、それぞれの重ね合わせ結果を総合的に判定することで演算結果を得ている。異なる組み合わせの信号は平面領域を分割して配置され、それらを一括して重ね合わせ、空間光変調素子により領域ごとに異なった位相シフトを与え、効率的に演算を実行する。これは、光の空間並列性に基づいた情報処理形態にほかならず、従来の光コンピューター技術の延長といえる。

この実験光学系の場合、演算技術としては、量子計算ではなく古典論の枠組みに基づいたものになってしまう。しかし、このような試みは、光コンピューターと量子コンピューターの本質的な相違点を理解するうえで有用な情報を与える。一方、現在の量子コンピューターへの大きな期待は、すぐれた量子アルゴリズムの出現によるところが大きい。光コンピューターの研究過程では、剰余系演算<sup>27)</sup>などのアイデアが出されたものの、具体的な難問題を解くに至った例はみられなかった。量子アルゴリズムに啓発された、光コンピューターに適した演算アルゴリズム開発などの展開も考えられる。

光コンピューターと量子コンピューターの接点について、おもに保守的な光コンピューターの立場から著者の考えを中心に論じた。光の量子状態を直接的に利用する正統

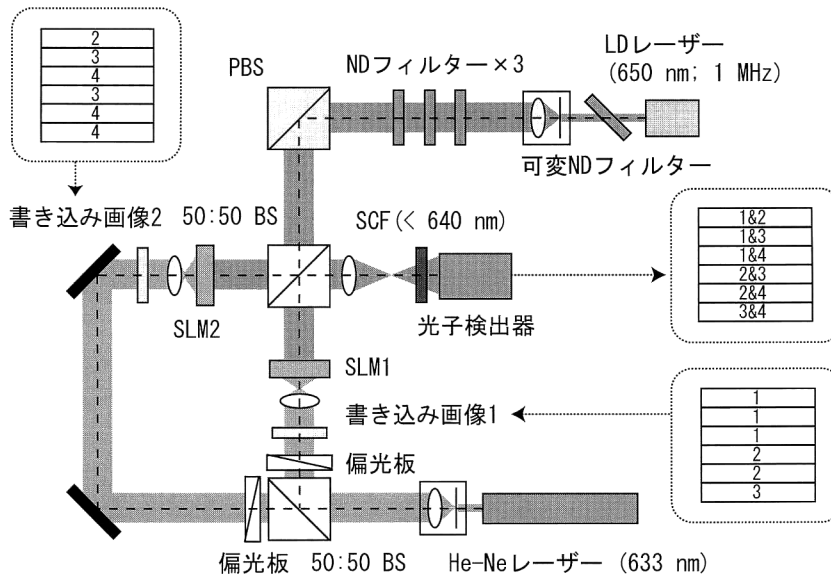


図4 並列光演算技術に基づく Deutsch-Jozsa 問題の解法。

的な量子光コンピューターが大きな可能性をもつことに疑いはないが、これまでに得られた光コンピューター研究の資産を有効に生かすことができれば、その世界は大きく広がるものと期待される。本稿が、このエキサイティングな研究分野を理解するうえでの一助となれば幸いである。

## 文 献

- 佐川弘幸, 吉田宣章: 量子情報理論(シュプリンガー・フェアラーク東京, 2003).
- 竹内繁樹: “量子コンピューター研究の近況レポート”, 応用物理, **71** (2002) 1367-1371.
- P. Shor: “Algorithm for quantum computations: Discrete logarithms and factoring,” *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994) pp. 124-134.
- D. Deutsch and R. Jozsa: “Rapid solution of problems by quantum computation,” *Proc. R. Soc. Lond.*, **439A** (1992) 553-558.
- L. Grover: “A fast quantum mechanical algorithm for database search,” *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (STOC, 1996) pp. 212-219.
- N. A. Gershenfeld and I. Chuang: “Bulk spin-resonance quantum computation,” *Science*, **275** (1997) 350-356.
- J. I. Cirac and P. Zoller: “Quantum computation with cold trapped ions,” *Phys. Rev. Lett.*, **74** (1995) 4091-4094.
- D. Loss and D. P. DiVincenzo: “Quantum computation with quantum dots,” *Phys. Rev. A*, **57** (1998) 120-126.
- E. Knill, R. Laflamme and G. Milburn: “A scheme for efficient quantum computation with linear optics,” *Nature*, **409** (2001) 46-52.
- 富田章久: “光による量子ゲートの実現について”, *Computer Today*, **18** (2001) 17-23.
- S. Takeuchi: “Experimental demonstration of a three-qubit quantum computation algorithm using a single photon and linear optics,” *Phys. Rev. A*, **62** (2000) 0320301.
- H. F. Hofmann and S. Takeuchi: “Quantum phase gate for photonic qubits using only beam splitters and postselection,” *Phys. Rev. A*, **66** (2002) 024308.
- C. H. Bennett and G. Brassard: “Quantum key distribution and coin tossing,” *Proc. IEEE Int. Conf. Computers, Systems and Signal Process* (IEEE, New York, 1984) pp. 175-179.
- J. Tanida and Y. Ichioka: “Optical computing,” *The Optics Encyclopedia*, eds. Th. G. Brown, K. Creath, H. Kogelnik, M. A. Kriss, J. Schmit and M. J. Weber (Wiley-VCH, 2004) pp. 1883-1902.
- 早崎芳夫: “情報フォトンクス: その概念とめざすもの”, *光学*, **32** (2003) 410-415.
- A. G. Kirk, D. V. Plant, T. H. Szymanski, Z. G. Vranesic, F. A. P. Tooley, D. R. Rolston, M. H. Ayliffe, F. K. Lacroix, B. Robertson, E. Bernier and D. F.-Brosseau: “Design and implementation of a modulator-based free-space optical backplane for multiprocessor applications,” *Appl. Opt.*, **42** (2003) 2465-2481.
- M. Naruse, H. Toyoda, Y. Kobayashi, D. Kawamata, N. McArdle, A. Goulet and M. Ishikawa: “An optically interconnected pipelined parallel processing system: OCULAR-II,” *Proc. SPIE*, **4089** (2000) 440-448.
- G. Li, D. Huang, E. Yuceturk, P. J. Marchand, S. C. Esener, V. H. Ozguz and Y. Liu: “Three-dimensional optoelectronic stacked processor by use of free-space optical interconnection and three-dimensional VLSI chip stacks,” *Appl. Opt.*, **41** (2002) 348-360.
- 渡邊恵理子, 小館香椎子: “光並列顔画像認識装置—垂直型面発光レーザーアレイモジュールによる小型化—”, *光学*, **32** (2003) 427-439.
- P. Refregier and B. Javidi: “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, **20** (1995) 767-769.
- 小西 毅: “超高速時空間変換を用いた超短パルス光の信号処理”, *光学*, **32** (2003) 619-622.
- 宮崎大介: “三次元情報技術と情報フォトンクス”, *光学*, **32** (2003) 424-430.
- Y. Hayasaki, H. Yamamoto and N. Nishida: “Self-scanning of isolated spots in a nonlinear optical system with two-dimensional feedback,” *J. Opt. Soc. Am. B*, **17** (2000) 1211-1215.

- 24) Y. Ogura, T. Kawakami, F. Sumiyama, A. Suyama and J. Tanida: "Parallel translation of DNA clusters by VCSEL array trapping and temperature control with laser illumination," *Ninth Annual International Meeting on DNA Based Computers*, eds. J. Chen and J. Reif (Madison, Wisconsin, June 1-4, 2003) pp. 19-27.
- 25) 谷田 純: "空間符号化並列演算技術とその応用", 生産と技術, **53** (2001) 15-20.
- 26) N. Tate and J. Tanida: "Implementation of a computation algorithm for Deutsch-Jozsa problem utilizing spatial distribution of photons," *Opt. Rev.*, **11** (2004) 72-75.
- 27) A. Huang, Y. Tsunoda, J. W. Goodman and S. Ishihara: "Optical computation using residue arithmetic," *Appl. Opt.*, **18** (1979) 149-162.

(2004年3月10日受理)