

多光子間のもつれ合い状態の大量生成に成功

小林 孝嘉 (物理学専攻 教授) 三上 秀治 (物理学専攻 博士課程 2年)

量子力学は日常的な直感に反する数多くの現象を示すことが知られているが、近年はそれらの不可解な性質を、情報処理などに応用するための研究が活発に行われている。その中で、もつれ合い状態と呼ばれる非局所的な相関^{注)}をもった量子力学的な状態が、さまざまな場面で重要な役割を担うため、研究者の間で注目を集めている。私たちは、ある種の多光子間のもつれ合い状態を、従来の手法よりも桁違いに高い効率で大量生成することに成功した。また、得られた状態の性質を完全に特定することに世界で初めて成功した。

もつれ合い状態とは、光子や原子、電子といった量子力学的にふるまう粒子どうしの間に、非局所的な相関がある状態のことである。量子力学の誕生当初はその不可解な性質をもとに量子力学の正当性を疑う議論がなされていたが、現在はむしろその性質を積極的に利用して従来の技術の壁を打破することを目指した研究が活発に行われており、実験的にも、もつれ合い状態を生成することが可能である。従来は2つの粒子間のもつれ合い状態が主に研究されており、より多くの粒子間のもつれ合い状態を効率よく生成することは一般に困難とされてきた。私たちは今回、光パラメトリック増幅という非線型光学の分野で知られた光学過程を応用することにより、3つの光子間のある種のもつれ合い状態を、1秒間に約1.5個の割合で発生させることに成功した。従来の報告では1秒あたり0.035個程度しか生成できなかったため、これは従来の40倍以上の効率になる。光パ

ラメトリック増幅とは、ある波長の光を、別の波長の光からのエネルギーを与えることによって増幅させる過程のことである。通常は強い光に対して利用されるが、今回はこれをきわめて微弱な光である光子に応用した。

従来の技術では、多粒子間もつれ合い状態は非常に低い効率でしか生成できなかったため、その性質を調べることも困難であった。今回ひじょうに高い効率での生成が可能になったことにより、その性質を完全に特定することができた。これにより、これまでは間接的にしかその特徴を知ることができなかった多粒子間のもつれ合い状態の性質が、手に取るようにわかるようになった。

今回ここで開発した装置は拡張も容易であるために、今後の技術の進展により、さらに多くの光子のもつれ合い状態を生成させることが可能である。また、装置等の改良により、効率をさらにもう1桁ほど向上させることも可能である。

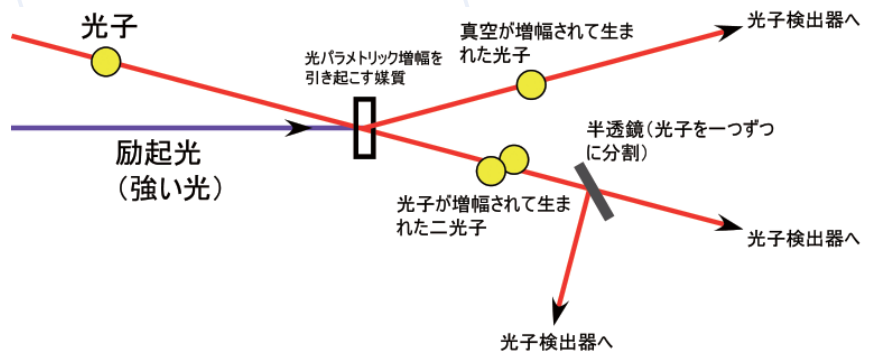
もつれ合い状態は、きわめて高い計算処理能力をもつことで知られる量子コンピュータの開発に不可欠な要素であり、

とくに大規模な量子コンピュータを作るためには、多数の粒子間のもつれ合い状態が必要である。したがって今回の成果は、量子コンピュータ開発のための重要なステップであると言える。もつれ合い状態はまた、量子力学の原理に基づいた絶対的なセキュリティをもつ量子暗号技術に応用することができることも知られており、通信の分野への応用も期待される。さらに、もつれ合い状態の性質そのものに関する研究も現在たいへん活発に行われているため、基礎研究の観点からも興味深い結果であると言える。

本研究は、三上が主筆者の論文として、Physical Review Letters 95, 150404 (2005) に掲載されている。

(2005年9月7日プレスリリース)

注) 「非局所的な相関」 通常は量子力学で取り扱わないと考えられるほど大きく離れた複数の粒子がもつ物理量の間、相関があること。すなわち複数の粒子の一方がある特性をもっている時に、遠く隔たった位置にある他方が、それによって決まる特性をもつこと。今回の成果では、複数光子の偏光特性に関する相関を扱った。



■ 多光子間のもつれ合い状態を作るための実験装置

量子コンピュータ — 対称性によるブレークスルー

今井 浩 (情報科学科 教授)

コンピュータの動作原理を量子力学に

今やコンピュータとインターネットは生活基盤として普及したものの、その能力の限界も実は身近になってきている。限界を打破するため、コンピュータの根本の動作原理を変革するという発想転換で、量子力学原理で動作する計算機が「量子コンピュータ」である。今のコンピュータが情報を0, 1のデジタル表現し処理するのに対し、情報を量子状態で表現・操作する。たとえば、スピン量子系を用いると、上向きのスピンの0, 下向きのスピンの1を表し、赤道向きスピンの0と1を半々に重ね合わせて方位角まで含めて表現し、これらを量子操作していくのである。

量子コンピュータの得意とするもの—対称性

物理的な動作原理を古典系から量子系に変えても、計算方式(アルゴリズム)がこれまでと同じでは、単に素子レベルで速度が改善されるだけである。しかし、量子コンピュータ特有のアルゴリズムを考えると、ブレークスルーが起こる。10進300桁の整数の素因数分解は、2010年頃の実現が計画されている京速計算機をもってしても難しいのに、量子コンピュータなら瞬時にできるアルゴリズムがある。今のインターネットで電子マネーのやりとりを支える暗号システムは、この素因数分解が現代コンピュータにとって超難問であるという情報科学の成果に基づいているが、量子コンピュータはその安全性を崩壊させるほどのインパクトをもっているのである。

量子コンピュータによって初めて解くことが可能になる問題を研究する学問は、量子情報科学と呼ばれ、そこでのキー

ワードは「対称性」である。理学において、対称性は群の理論によって扱われる。素因数分解は巡回群の部分群のもつ対称構造を求める問題と等価で、量子コンピュータ専用の高速アルゴリズムがある。

対称性を発見する光量子コンピュータ

量子コンピュータだけがどうやって問題に潜む対称性を見つけられるのだろうか。その鍵は量子フーリエ変換にある。量子コンピュータは、量子重ね合わせ状態を用いて、1兆次元の離散フーリエ変換を、1兆を10進数で表したときの桁数の13にほぼ比例した時間で計算することができる。これに対し、今のコンピュータでの最速のアルゴリズムでは、計算時間は次元数に比例する以上に増大してしまう。

科学技術振興機構(JST)が推進してきたERATO今井量子計算機構プロジェクトでは、これまでの5年間で、実際にこの量子フーリエ変換を専用で行う量子コンピュータを光ファイバ回路として実現している。これは、光の量子性を用いて、量子観測の精緻な理論と実験によって達成されている。

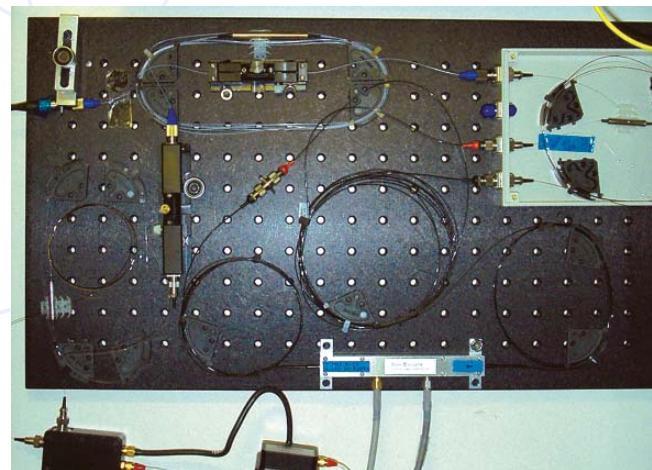
量子コンピュータの得意とする対称性の追求

対称性は群構造で表され、素因数分解は巡回群の問題に対応していた。素因数分解と同様に暗号システムでの利用が検討されている最短格子点問題は2面体群に対応し、自分の秘密をもらさずに自分を認証させる暗号方式(今の銀行キャッシュカードは自分の秘密の暗証番号をシステムに直接提示するので安全でない)のキーとなるグラフ同型問題は対称群に対応す

る。ERATOプロジェクトでは、この対称性を追求するために、まず2面体群を含む半直積群を考え、その分解定理を示して量子フーリエ変換を高次に活用することによって、2面体群の問題の解決に肉薄するところまで量子コンピュータで解けるクラスを広げている。

量子情報システムアーキテクチャへ

新しい量子情報科学をさらに展開するプロジェクトとして、これより3年の予定でJST ERATO—SORST量子情報システムアーキテクチャの研究が開始されている。これは、計算素子が量子力学的に動作するという量子ハードウェアと、情報数理の立場から対称性を処理するアルゴリズムを考える量子ソフトウェアを両輪としたシステムアーキテクチャを目指すものである。そこでは量子力学の原理によって安全性が保証される量子暗号システムの開発から、量子情報の理論まで、さらに推進されていく予定である(www.qci.jst.go.jp 参照)。



ERATO 光ファイバ量子フーリエ回路