研究会、セミナー開催報告、支部報告

■【量子コンピュータの概要と研究・開発の状況 （第 169 回月例研参加記録）】

会員 No.1750　舘岡　均

日時:平成 23 年 12 月 21 日（水） 18:30～20:00
場所:総評会館
講演テーマ:量子コンピュータの概要と研究・開発の状況
講師:NTT 物性科学基礎研究所　量子光物性研究部長　都倉　康弘氏
参加者:76 名

＜講演骨子＞

現代の情報処理に用いられている電気信号や光信号は、電子及び光子の古典的な性質、例えば電流値や光強度、光の位相等、を活用したものです。しかし、電子も光子も素粒子であり、20世紀初頭に確立した量子力学に支配されています。最近この量子力学の性質をうまく活用した全く新しい情報処理である、量子情報処理が提案され、（スーパーコンピュータを含む）従来の古典コンピュータをはるかにしのぐ計算能力を持つと予想される量子コンピュータに注目が集まっています。本講演ではこの「夢のコンピュータ」の原理と世界中の研究・開発の現状と今後の見通しをできるだけ分かりやすく解説いたします。　（都倉様から頂いた講演骨子）

＜講演概要＞

高度に専門的な量子力学、暗号、量子コンピュータのことを、基礎から、やさしく噛み砕いて、講演をしていただきました。目次は次の通りです。

目次
1. 量子力学の不思議
　－波の干渉
　－重ね合わせ
　－量子もつれ
2. 現代暗号と量子暗号
3. 量子コンピュータの原理とパワー
4. 量子コンピュータ研究・開発の状況
5. まとめ

＜講演内容＞

あまりにも高度で専門的なテーマであり、従来の月例会報告のように解説することは困難なため、講演された内容の説明資料の項目／キーワードを示し、最後に報告者所感を記述します。

1. 量子力学の不思議

量子って何？、 量子力学の世界、
光＝電磁波について、 電磁波の基本、 ヤングのダブルスリット干渉実験、 干渉の様子、
光は波、 干渉する理由は、 モノの波の幅？、 冷たい原子は干渉する、コヒーレンス、 コヒーレンスの重要性
光の粒子性、 一個の粒子は干渉する？、 一つのスリットでは、 二つのスリット、 沢山の粒子の結果を集めると
偏向のしくみ、 偏光フィルタ、 垂直と水平の偏光フィルタ2枚では、斜めの編光フィルタでは、
各光子が特定の偏光を持つと、 光子は「特定」の編光を持っていない、 重ね合わせ
もつれた二つの量子、 量子テレポーテ―ション

2. 現代暗号と量子暗号

通信と暗号、
暗号の説明の前に算数のおさらい、
暗号の仕組み、
公開鍵暗号、
素因数分解は難しい、
難しさは指数関数的、
現代の暗号通信、
絶対安全な暗号？
開くと消えてしまう情報なら安全？

量子暗号（量子鍵配送）とは、
量子暗号（量子鍵配送）の仕組み、
具体的な手続き、
東京 QKD ネットワーク、
UQCC2010 におけるライブデモンストレーション、
量子もつれの不思議な性質、
量子もつれを使えば量子暗号ができる、
量子もつれ光子対光源の例、
100km光ファイバーの量子暗号、
量子テレポ―テ―ションを用いた量子中継、

3. 量子コンピュータの原理とパワー

「計算できる」とはどういうことか？
（定義一）計算機が解を見つけて停止すること。
　　かけ算（容易）と素因数分解（困難）
（定義二）問題のサイズの増大に対し計算ステップ数が高々その多項式程度にしか増えないこと。
（定義三）現実的な計算ステップを数を超えない。

量子情報処理が注目される背景、
量子コンピュータ、
ムーアの法則、
ムーアの法則の終焉、
情報の最小単位、
逐次計算と並列計算、
量子力学的　逐次計算、

超並列の源：重ね合わせ、
超並列性　―迷路問題を例に―　、

アルゴリズムの説明、
量子フーリエ変換、
Crover のデータ探索アルゴリズム、
アルゴリズムの説明、
データ数が多くなると、
Shor の素因数分解アルゴリズム、

4. 量子コンピュータ研究・開発の状況

物理システム開発の状況、
その一例として：人工原子、
電子数を一個単位で自由に操る技術、
人工原子を二つならべて→人工分子、
量子コンピュータ：将来システム実現に向けて、

5. まとめ

まとめにかえて、R.P.Feynman のノーベル賞受賞時の言葉の引用

It is my task to convince you not to turn away because you don't understand it.

・・・

＜報告者所感＞

本講演は、専門的で、難解なテーマでしたが、量子コンピュータへの高い関心からか、師走にかかわらず、多くの方々が参加されました。講師は専門家ですが、目線を下げて丁寧な解説をして下さりました。拝聴して、講演内容で印象的であった個所を、簡単に述べて所感とします。

最初に、量子情報処理が注目された背景には、現代の情報セキュリティは、素因数分解が「解けない問題」であることを前提としていたが、1994 年に「量子コンピューティングで素因数が解ける」ことが示され、その後、1997 年には「量子暗号は量子コンピューティングでも破れない」ことが示された、等があるようです。

その量子コンピュータは、異なる分野の科学が融合した新しい分野であり、量子情報科学は情報工学／計算機科学と量子力学の学際的研究を必要とし、量子ネットワーク、量子ナノエレクトロニクス、量子暗号、量子数学、量子生物、量子化学、量子光学、材料工学などが柱としてあるようです。

これまでの古典コンピュータ（従来のコンピュータ）と量子コンピュータを比較すると、量子コンピュータは想像を絶する桁違いの性能を有します。

具体的には、これまでの古典コンピュータはビット（0 または1）が単位であり、レジスターとして、nビットで表わされるのは、2 のn乗個の情報のうちの1個である。多数の計算を同時に行うには、分散コンピューティング、並列計算で行っている。

一方、量子コンピュータは、量子ビットが単位で、1ビットにつき0と1が確率的に重ね合わさっている。量子レジスターとして、n 量子ビットで、2 のn乗個の情報の組み合わせを、重ね合わせで表現できる。多数の計算を、“重ね合わせ”、で行う量子コンピュータは古典コンピュータでは実現できない超並列処理を実現できる。

たとえば、30個の粒子を使用すると、全世界の総人口と等しいくらいの入力値を同時に表わせて、計算ができ、140個の粒子を使用すると、地球を構成する全原子数に等しいくらいの入力値を同時に表わせて計算ができるようです。まさしく想像を絶する性能であり、実現された場合には、科学の発展へ大きく貢献し、大変革をもたらすと思われます。

さらに、量子コンピュータの将来システムは、量子コンピュータクラウドとして、社会情報（サービス情報）、知識情報（刊行物データベース）、環境知能（センサネットワーク）、最先端科学（創薬、宇宙シミュレーション）、人間情報（ライフログ、ヘルスケア）等に活用されると期待されています。

しかし、量子コンピュータの課題としては、作成が極めて困難（ハードウェア）、デコヒーレンスに弱い（ハードウェア）、アルゴリズム不足（ソフトウェア）があります。量子コンピュータの利点としては、大規模情報の並行処理、低消費電力、科学の発展への大きな貢献、等があるとされています。

これらは、講演内容の一部でしたが、量子コンピュータの実現は 50 年後くらいという予想もあり、人類の将来において多大に貢献することは確かであり、明るい夢の一つであり、今後の発展の推移に関心を持って行きたいと思います。

以上