

■報告書■ 2004 年度神奈川大学総合理学研究所助成共同研究

NMR 量子コンピュータ

小澤 宏¹ 天野 力^{2,6} 岡部建次³ 坂口 潮⁴ 福見俊夫⁵ 峯岸安津子²

NMR Quantum Computer

Hiroshi Ozawa¹, Chikara Amano^{2,6}, Kenji Okabe³, Ushio Sakaguchi⁴,
Toshio Fukumi⁵, Atsuko Minegishi²

¹ Department of Function Production, Faculty of Engineering, Yokohama National University, Yokohama-City, Kanagawa 240-8501, Japan

² Department of Chemistry, Faculty of Science, Kanagawa University, Hiratsuka-City, Kanagawa 259-1293, Japan

³ Department of Information Systems, Faculty of Information and Culture, Surugadai University, Hanno-City, Saitama 357-8555, Japan

⁴ Department of General Education, Faculty of Commerce, Kumamoto Gakuen University, Kumamoto-City, Kumamoto 862-8680, Japan

⁵ Department of Management, Faculty of Management, Matsuyama University, Matsuyama-City, Ehime 790-8578, Japan

⁶ To whom correspondence should be addressed. E-mail: amano@chem.kanagawa-u.ac.jp

Abstract: The quantum computer is a potential computing machine which employs interacting quantum two level systems as quantum bits. We studied a problem simulating a C^n NOT gate by a combination of CNOT gates and 1-bit phase rotation gates. The results are that, of $8(n-3)$ C^2 NOT gates, $8(n-5)$ gates can be simulated by two CNOT and two 1-bit gates, 8 gates by 3 CNOT and 4 1-bit gates, and residual 8 gates by 48 CNOT and 52 1-bit gates.

Keywords: quantum computer, C^2 NOT gate, Shor's algorithm, oracle unitary transformation

量子コンピュータ (Deutsch, 1985; Feynman, 1986) は、相互作用する量子 2 準位系の集合 (例えば分子内核スピン) を量子的なビットとして用いることにより、情報処理を行なおうという発想である。量子ビットの状態をユニタリー変換して計算を実行し、その最終状態を観測して結果を得る。量子コンピュータが魅力的なのは、量子コンピュータによれば、ある種の問題が、もっとも優れた古典的な方法に比べ、指数関数的に高速に解けるからである。一例として、Shor (1994) による整数の素因数分解アルゴリズムをあげることができる。

Shor の方法を含む多くの量子アルゴリズムは、ユニタリー変換 $U_f: |x\rangle|y\rangle \rightarrow |x\rangle|y+f(x)\rangle$ (+は 2 進和) をオラクルとして用いている。この変換は、1 番目、2 番目のレジスターの長さをそれぞれ n , m とするとき、各 x に対し、高々 m 個の C^n NOT ゲート (n 個の量子ビットで条件付けられた NOT ゲート) でインプリメントすることができる。また n が 5 以上の C^n NOT ゲートは、量子ビットが 1 つ余分

に存在するとき (すなわち $n+2$ 量子ビットの系において)、 $8(n-3)$ 個の C^2 NOT ゲートでシミュレート可能であることが見いだされている (Barenco ら, 1995)。

ユニバーサルな量子コンピュータを構成するための基本ゲートには、いくつかの組み合わせがある。我々は、2 量子ビットに対する CNOT ゲートと 1 ビットゲート (1 量子ビットの位相回転) とを基本ゲートに選び、これらのゲートで C^n NOT ゲートを効率よくシミュレートする方法について考察した。

(C^2 NOT ゲート単独のシミュレートには少なくとも 6 個の CNOT ゲートと 8 個の 1 ビットゲートが必要であると推定されている。) 結果は、 $8(n-3)$ 個の C^2 NOT のうち、 $8(n-5)$ 個は 2 個の CNOT と 2 個の 1 ビットゲートのみで、8 個は 3 個の CNOT と 4 個の 1 ビットゲートで、残る 8 個は合計 48 個の CNOT と 52 個の 1 ビットゲートでシミュレートできる、という点に集約される。すなわち量子ビットが 1 つだけ余分に存在すれば、 n が 5 以上の C^n NOT

ゲートは $32n-4$ 個の基本ゲート ($16n-8$ 個の CNOT ゲートと $16n+4$ 個の 1 ビットゲート) でシミュレートすることができ、これは Barenco らが得た基本ゲート数のおよそ $2/3$ に相当する。

なお、 U_f において x は $\{0, \dots, 2^n-1\}$ の範囲に広がっているため、 U_f 全体をインプリメントするには、

指数関数的に多数のゲートが必要である。すなわち Shor の方法のようなオラクル U_f の存在を仮定したアルゴリズムは、それが古典的方法に比べ指数関数的に高速なものではあっても、量子コンピュータを用いてもなお、実行は指数関数的に困難である。