1 Quantum Computing Simulation using the Auxiliary Field Decomposition

Kurt Fischer[2], Hans-Georg Matuttis[1], Satoshi Yukawa[2], and Nobuyasu Ito[2]

[1] University of Electro-Communications, Department of Mechanical and Control Engineering, E-Mail: hg@mce.uec.ac.jp
[2] University of Tokyo, Department of Applied Physics

1.1 Introduction

Instead of using classical bits which are 0 or 1, quantum computers make use of "quantum bits" which are similar to XY-Spins. The total information described by N quantum bits is vector in the Kronecker product space

$$\left(a_1\ b_1\right) \otimes \left(a_2\ b_2\right) \otimes \left(a_3\ b_3\right) \otimes \ldots \left(a_N\ b_N\right), \quad \text{with } a_i^2 + b_i^2 = 1. \tag{1.1}$$

The dimension is the same as the space spanned by the same number of classical bits

$$a_1 a_2 a_3 \ldots a_n, \quad a_i \in \{0, 1\}, \tag{1.2}$$

but the intention is to sample the problem via a quantum mechanical wavefunction "quantum parallel". To allow the representation of the gates of a quantum circuit with quantum mechanical states, the minimum requirement is that the circuit is reversible, so that the number of input states must be the same as the number of output states. Examples for forbidden and allowed states are given in Fig. 1.1. All the final output of the quantum computation

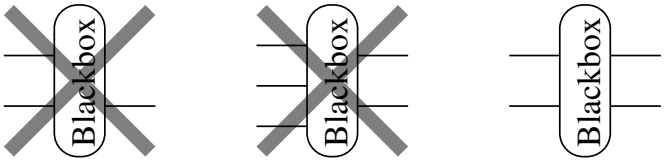


Fig. 1.1. Forbidden (left and middle) and allowed (right) types of gates for quantum computers.

must be must be representable in the sense of quantum mechanics. The difference between quantum computing and mere "reversible computing" is that in the quantum circuit a quantum mechanical wave function is propagated. The aim is to realize the propagation of a quantum mechanical wave function in such a way that the "all the solutions" are obtained "at once," an idea which usually referred to under as "quantum parallelism". Most of the quantum parallel algorithms proposed so far seem only to work for algorithms which

select from discrete alternatives, like Shor's prime factoring [8] or Grover's database search [9], with the exception of a proposal for the computation of densities of states [2].

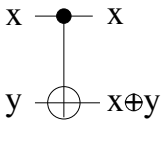
A recent investigation [1]indicates that for systems for which existence and functionality can be proven mathematically, the actual realization in terms of physical terms may be rather more problematic than mere existence proofs indicate. For certain straightforward implementations, this does not allow the successful execution of the implemented quantum algorithms. Even if the initial wave functions are optimized to be resistant to noise for certain solutions of the algorithms, there are still remaining solution possibilities which are not recovered without error even for systems of only a few quantum bits. We therefore decided to circumvent the problem by simply simulating the quantum circuit on the level of the functionality of the quantum gates, without taking into account a physical realization of the circuit [5, 6].

1.2 Auxiliary Field approach to Quantum Computing

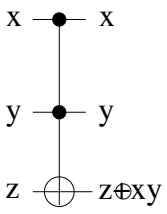
We simulate the quantum computer circuit using techniques from Quantum-Monte-Carlo on a classical computer. We focus on the simulation of the "pure" quantum gates because for physical circuits, already the "identity-operation" may be too noisy. We will also not comment on implementation possibilities, e.g. spin chains, NMR-Processes, quantum-dots for the circuit discussed. Our main interest whether we can simulate larger systems than those accessible to experiments currently or in the near future. The other interest is to find out whether we can simulate a quantum algorithm on a classical computer via Quantum-MC-type of algorithms with a CPU-time-scaling comparable to the time-scaling of quantum computers. This seems at least possible, because it is known that "good" results for non-polynomial complete problems can be obtained using Monte-Carlo methods in "polynomial time", e.g. for optimization problems, for example via simulated annealing type of algorithms. Moreover, quantum Monte Carlo methods which reduce the dimensionality of the simulated problem have a long history in statistical physics.

The Hadamard gate mixes the first and second component of a qbit by multiplying them with the Hadamard matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. Other often used gates are the controlled not (CNOT) and Toffoli gate, which are given in Fig. 1.2. As can be seen, half of the possible cases the action of the CNOT-gate is that of the identity operator, and the action of the Toffoli gate is that of the identity operator for 75 % of the possible input patterns. This lets us hope that an auxiliary field approach can be implemented effectively, in contrast e.g. to the computation of partial sums for the full problem.

For the CNOT-gate which acts on two input qbits with a controlling bit n_x and a controlled bit n_y, can be represented as



x	y	x'	y'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



x	y	z	x'	y'	z'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Fig. 1.2. Symbols and truth tables for the CNOT-Gate (left) and the Toffoli gate (right).

$$CNOT = H_y(1 - 2n_x n_y)H_y \tag{1.3}$$

where the subscripts denote the bit on which these one-bit operators n_x, n_y, each with components n_{x1}, n_{y1} and n_{y1}, n_{y2}, act. H is the Hadamard matrix, and the number operator $n|s\rangle = s|s\rangle$ for $s \in \{0, 1\}$. A symmetric Hubbard-Stratonovic-transformation can be written as

$$CNOT = \frac{1}{2} \sum_{\sigma=0,1} \left(1 - (-1)^\sigma \sqrt{2} n_x)\right) H_y \left(1 + (-1)^\sigma \sqrt{2} n_y)\right) H_y, \tag{1.4}$$

where symmetric means that the contribution for $\sigma = 0$ and for $\sigma = 1$ are of the same size. For fermions, the discrete Hubbard-Stratonovich [4] transformation decouples the interacting Fermions to non-interacting Fermions feeling fluctuating potentials. In case of the quantum gates, the controlled NOT-gate is transformed to the action of a number of gates which are not controlling each other any more. Analogies and differences for auxiliary field simulations for fermionic systems and quantum gates are given in Ref. [5].

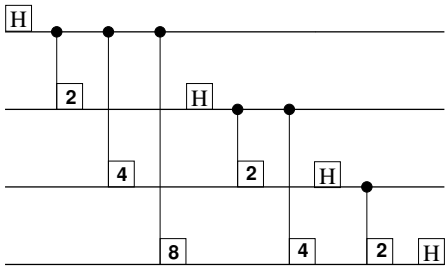


Fig. 1.3. Cirquit using controlled phase gates for the QFT for four qbits, which are CNOT-gates with an additional phase factor $\exp\left[\frac{2\pi i}{2^q} n_1 n_2\right]$ for $q = 2, 4, 8$.

1.3 Simulations of the Quantum-Fourier-Transformation

Previously, we have performed simulations for the period-finding kind of algorithm by Simon [5] and for the factoring of 15 [6] by Vandersypen [7]. Our long term aim is to obtain a feasible implementation of the full Shor-algorithm for integer factoring [8]. As one of the central functional in such a circuit is the quantum Fourier Transformation (QFT), the quantum variant of the Fast Fourier Transform, we investigated the Monte Carlo convergence for the auxiliary field decoupled QFT. We simulated the QFT with the symmetric HS-decomposition of Eq. 1.4 and with another, non-symmetric decomposition. Fig. 1.4 shows that for different decompositions, different distributions of values must be sampled. The convergence results in Fig. 1.5 show that the convergence for the symmetric decomposition is already significant for less than 1/100 of the total number of configurations, whereas for the non-symmetric decomposition, no convergence was observed even for MC-runs using as much samples as the number of total configurations.

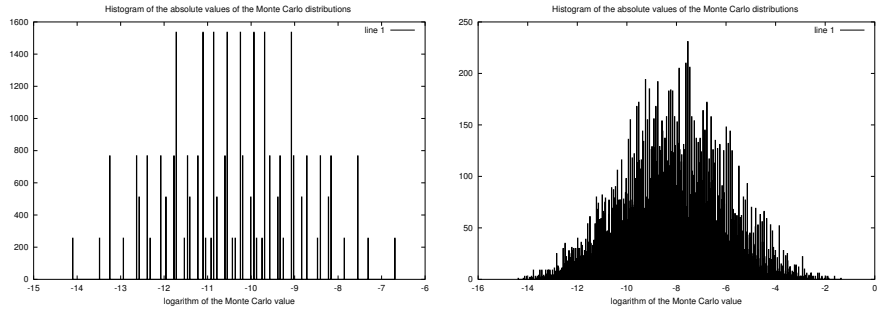


Fig. 1.4. Histogram of contributions for the symmetric decomposition (left) and for an asymmetric decomposition (right).

1.4 Conclusion

We have shown how the auxiliary field methods known from quantum Monte Carlo techniques can be applied to quantum computing problems. The Hubbard-Stratonovich transformation leads to a simple sampling procedure in contrast to the importance sampling of quantum Monte Carlo.

The initial simulations show that for small problems, the method is applicable. For problems which are realistically large, e.g. integer factoring for

numbers from hundreds of bits, the scaling of the necessary computer time is currently under investigation.

This work was partially supported by the program "Research and Development on Quantum-Communication Technology" of the Ministry of Public Management, Home Affairs, Posts and Telecommunications of Japan and by the Inoue Foundation, Japan.

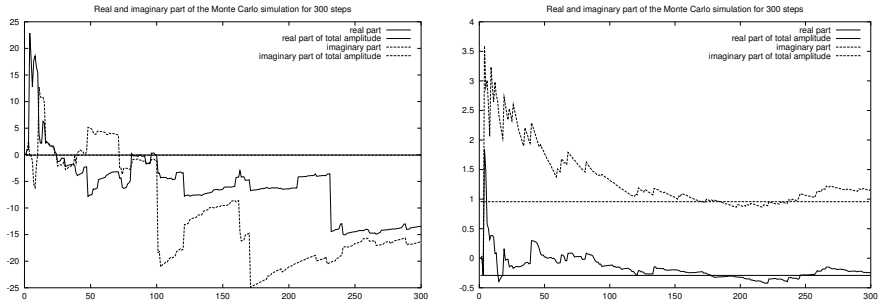


Fig. 1.5. Sample run for 6 bits for the symmetric decomposition (left) and for an assymetric decomposition (right) for a left input vector representing 11 and the right input vector representing 25.

References

1. H. De Raedt, K. Michielsen, A.H. Hams, S. Miyashita and K. Saito, Eur. Phys. J. B **27**, 15 - 28 (2002)
2. H. De Raedt, A. Hams, K. Michielsen, S. Miyashita and K. Saito, Prog. Theor. Phys. Suppl. **138**, 489 - 494 (2000)
3. M. A. Nielsen, I. Chuang: *Quantum Computation and Quantum Information* (Cambridge University Press 2000)
4. J.E.Hirsch, Phys.Rev. B **28**, 4049 (1983)
5. H.-G. Matuttis, K. Fischer, N. Ito, and M. Ishikawa, Int. Journ. Mod. Phys. C, **13**, Nr. 7 917 (2002)
6. K. Fischer, H.-G. Matuttis, N. Ito, and M. Ishikawa, Int. Journ. Mod. Phys. C, **13**, Nr. 7 931 (2002)
7. L.M.K. Vandersypen, M. Steffen, G. Beyta, C. Yannoni, M. H. Sherwood, I. L. Chuang, Nature **4**14, 883 (2001)
8. P.W. Shor: Algorithms for quantum compuataion: discrete logarithms and factoring. In: *Proc. 35th Annual Symposium on Foundations of Computer Science*, IEEE Press, Los Alamitos, California, pp. 124-134 (1994).
9. L. Grover, In: *Proc.* 28^{th} *Annual ACM Symposium on the Theory of Computation*, pp. 212-219