

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 02-06-2014		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 18-Aug-2009 - 17-Aug-2012	
4. TITLE AND SUBTITLE Final Report on the Design of Quantum Algorithms Using Physics Tools				5a. CONTRACT NUMBER W911NF-09-1-0438	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHORS Edward Farhi, Jeffrey Goldstone, Peter Shor				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Massachusetts Institute of Technology (MIT) 77 Massachusetts Ave. NE18-901 Cambridge, MA 02139 -4307				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211				10. SPONSOR/MONITOR'S ACRONYM(S) ARO	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) 56291-PH-OC.10	
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT The PIs investigated quantum computation and information at the intersection of physics and computer science. They worked on a wide range of topics with some common themes related by the study of quantum Hamiltonians. Ground state properties of Hamiltonians and the gap between the ground state and first excited state were related to computational questions. The PIs relied on abstract mathematical reasoning as well as computer simulation. Topics covered included investigations of the performance of the quantum adiabatic algorithm, studies of the ground state properties of one-dimensional spin chains, the development of a novel quantum money scheme, a					
15. SUBJECT TERMS quantum computings, physics, algorithms, continuous time evolution, simulation, quantum money					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Edward Farhi
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 617-253-4871

Report Title

Final Report on the Design of Quantum Algorithms Using Physics Tools

ABSTRACT

The PIs investigated quantum computation and information at the intersection of physics and computer science. They worked on a wide range of topics with some common themes related by the study of quantum Hamiltonians. Ground state properties of Hamiltonians and the gap between the ground state and first excited state were related to computational questions. The PIs relied on abstract mathematical reasoning as well as computer simulation. Topics covered included investigations of the performance of the quantum adiabatic algorithm, studies of the ground state properties of one-dimensional spin chains, the development of a novel quantum money scheme, a study of quantum interactive proof systems, research on Hamiltonians on graphs realizing two-dimensional topological quantum field theories as well as the development of a novel method for performing quantum Monte Carlo simulations.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

<u>Received</u>	<u>Paper</u>
03/08/2013	4.00 Graeme Smith, John A. Smolin, Bei Zeng, Peter W. Shor. High Performance Single-Error-Correcting Quantum Codes for Amplitude Damping, IEEE Transactions on Information Theory, (10 2011): 0. doi: 10.1109/TIT.2011.2165149
03/08/2013	3.00 Edward Farhi, David Gosset, Itay Hen, A. W. Sandvik, Peter Shor, A. P. Young, Francesco Zamponi. Performance of the quantum adiabatic algorithm on random instances of two optimization problems on regular hypergraphs, Physical Review A, (11 2012): 0. doi: 10.1103/PhysRevA.86.052334
03/08/2013	5.00 Edward Farhi, David Gosset, Avinandan Hassidim, Andrew Lutomirski, Daniel Nagaj, Peter Shor. Quantum State Restoration and Single-Copy Tomography for Ground States of Hamiltonians, Physical Review Letters, (11 2010): 0. doi: 10.1103/PhysRevLett.105.190503
03/08/2013	7.00 Ramis Movassagh, Edward Farhi, Jeffrey Goldstone, Daniel Nagaj, Tobias J. Osborne, Peter W. Shor. Unfrustrated qudit chains and their ground states, Physical Review A, (07 2010): 0. doi: 10.1103/PhysRevA.82.012318
03/08/2013	8.00 Libor Caha, Ramis Movassagh, Daniel Nagaj, Sergey Bravyi, Peter W. Shor. Criticality without Frustration for Quantum Spin-1 Chains, Physical Review Letters, (11 2012): 0. doi: 10.1103/PhysRevLett.109.207202
TOTAL:	5

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

<u>Received</u>	<u>Paper</u>
03/08/2013 9.00	Edward Farhi, Jeffrey Goldstone, David Gosset, Sam Gutmann, Peter Shor. Unstructured Randomness, Small Gaps and Localization , Quantum Information & Computation, (09 2011): 840. doi:
TOTAL:	1

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
TOTAL:	

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
03/08/2013 2.00	Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, Peter Shor. Quantum money from knots, the 3rd Innovations in Theoretical Computer Science Conference. 08-JAN-12, Cambridge, Massachusetts. : ,
TOTAL:	1

(d) Manuscripts

<u>Received</u>	<u>Paper</u>
-----------------	--------------

Number of Manuscripts:

<u>Received</u>	<u>Book</u>
1890	1890
1891	1891
1892	1892
1893	1893
1894	1894
1895	1895
1896	1896
1897	1897
1898	1898
1899	1899
1900	1900
1901	1901
1902	1902
1903	1903
1904	1904
1905	1905
1906	1906
1907	1907
1908	1908
1909	1909
1910	1910
1911	1911
1912	1912
1913	1913
1914	1914
1915	1915
1916	1916
1917	1917
1918	1918
1919	1919
1920	1920
1921	1921
1922	1922
1923	1923
1924	1924
1925	1925
1926	1926
1927	1927
1928	1928
1929	1929
1930	1930
1931	1931
1932	1932
1933	1933
1934	1934
1935	1935
1936	1936
1937	1937
1938	1938
1939	1939
1940	1940
1941	1941
1942	1942
1943	1943
1944	1944
1945	1945
1946	1946
1947	1947
1948	1948
1949	1949
1950	1950
1951	1951
1952	1952
1953	1953
1954	1954
1955	1955
1956	1956
1957	1957
1958	1958
1959	1959
1960	1960
1961	1961
1962	1962
1963	1963
1964	1964
1965	1965
1966	1966
1967	1967
1968	1968
1969	1969
1970	1970
1971	1971
1972	1972
1973	1973
1974	1974
1975	1975
1976	1976
1977	1977
1978	1978
1979	1979
1980	1980
1981	1981
1982	1982
1983	1983
1984	1984
1985	1985
1986	1986
1987	1987
1988	1988
1989	1989
1990	1990
1991	1991
1992	1992
1993	1993
1994	1994
1995	1995
1996	1996
1997	1997
1998	1998
1999	1999
2000	2000
2001	2001
2002	2002
2003	2003
2004	2004
2005	2005
2006	2006
2007	2007
2008	2008
2009	2009
2010	2010
2011	2011
2012	2012
2013	2013
2014	2014
2015	2015
2016	2016
2017	2017
2018	2018
2019	2019
2020	2020
2021	2021
2022	2022
2023	2023
2024	2024
2025	2025
2026	2026
2027	2027
2028	2028
2029	2029
2030	2030
2031	2031
2032	2032
2033	2033
2034	2034
2035	2035
2036	2036
2037	2037
2038	2038
2039	2039

<u>Received</u>	<u>Book Chapter</u>
-----------------	---------------------

TOTAL:

Patents Awarded

Awards

Graduate Students

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	Discipline
Cedric Lin	0.43	
FTE Equivalent:	0.43	
Total Number:	1	

Names of Post Doctorates

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	National Academy Member
Peter Shor	0.09	Yes
Edward Farhi	0.14	
Jeffrey Goldstone	0.04	
FTE Equivalent:	0.27	
Total Number:	3	

Names of Under Graduate students supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

<u>NAME</u>
Total Number:

Names of personnel receiving PhDs

<u>NAME</u>
Total Number:

Names of other research staff

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Summary of Significant Results

The PIs, Farhi, Goldstone and Shor worked on a wide variety of problems in quantum information and quantum computation which resulted in many publications and stimulated much discussion in the wider community. Some of the research highlights are outlined below.

In joint work with David Gosset, Itay Hen, Anders Sandvik, Peter Young and Francesco Zamponi, two of the PIs of this grant, Farhi and Shor, used a variety of techniques to study the performance of the Quantum Adiabatic Algorithm on random instances of two combinatorial optimization problems. The first problem was 3-regular 3-XORSAT which is known to be difficult for conventional search algorithms. Here it was possible to use the cavity method to show that the gap governing the quantum algorithm is exponentially small meaning that the simplest version of the quantum adiabatic algorithm, with a stoquastic Hamiltonian, does indeed have difficulty with this problem. Numerical simulation confirmed these results. For the problem of 3-regular Max-Cut random instances were generated out to 160 bits. Here as the bit number increased the fraction of instances with small gaps increased. In this case the median gaps appear to decrease exponentially in the number of bits, but with a small exponent and in fact the data could also be well fit with an exponential decrease with an exponent proportional to the square root of the number of bits.

In joint work with David Gosset and Sam Gutmann, the PIs of this grant investigated Hamiltonians associated with the quantum adiabatic algorithm with totally random cost functions. Because these cost functions lack any structure the investigators were able to prove results about the ground state. They found the ground state energy as the number of bits goes to infinity, showed that the minimum gap goes to zero exponentially quickly, and saw a localization transition. They proved that there are no levels approaching the ground state near the end of the evolution. It is not clear whether features of this model are shared by the quantum adiabatic algorithm applied to random instances of satisfiability since despite being random these instances do have clause structure.

Public-key quantum money is a cryptographic protocol in which a bank can create quantum states which anyone can verify but no one except possibly the bank can clone or forge. Farhi and Shor worked on the development of secure quantum money schemes, both in general and with a specific example. Together with Andrew Lutomirski, Scott Aaronson, David Gosset, Avinatan Hassidim and Jonathan Kelner they showed that a previous scheme, introduced by Aaronson, was insecure. The group also introduced a category of quantum money protocols which they called collision-free. For these protocols, even the bank cannot prepare multiple identical-looking pieces of quantum money. This approach was realized in a specific scheme called Quantum Money from Knots which was developed by Farhi, Gosset, Hassidim, Lutomirski and Shor. In this scheme, money states are quantum superpositions of diagrams that encode oriented links with the same Alexander polynomial. As of this report, this scheme has not been broken and we expect it to remain secure against computationally bounded adversaries.

In work with Salman Beigi and John Watrous, Shor investigated quantum interactive proofs. These are protocols in which a verifier and one or more provers send quantum messages (encoded in quantum states) to each other, the goal being to convince the verifier that some statement is true. They considered three variants of quantum interactive proof systems in which short (meaning logarithmic-length) messages are exchanged between a prover and a verifier. The first variant is one in which the verifier sends a short message to the prover, and the prover responds with a polynomial-length message; the second variant is one in which any number of messages can be exchanged, but where the combined length of all the messages is logarithmic; and the third variant is one in which the verifier sends polynomially many random bits to the prover, who responds with a short quantum message. They prove that in all of these cases the short messages can be eliminated without changing the power of the model, so the first variant has the expressive power of QMA and the second and third variants have the expressive power of BQP. These facts are proved through the use of quantum state tomography, semi-definite programming and the finite quantum de Finetti theorem.

Farhi, Goldstone and Shor along with Ramis Movassagh, Daniel Nagaj and Tobias Osborne investigated chains of d dimensional quantum spins (qudits) on a line with generic nearest neighbor interactions without translational invariance. They found the conditions under which these systems are not frustrated, i.e. when the ground states are also the common ground states of all the local terms in the Hamiltonians. The states of a quantum spin chain are naturally represented in the Matrix Product States (MPS) framework. Using imaginary time evolution in the MPS ansatz, they numerically investigated the range of parameters in which it was expected that the ground states be highly entangled and found them hard to approximate using the MPS method.

In follow on work Shor along with Sergey Bravyi, Libor Caha, Movassagh and Nagaj looked at frustration-free (FF) spin chains. These have the property that their ground states minimize all individual terms in the chain Hamiltonian. They asked how entangled the ground state of a FF quantum spin- s chain with nearest-neighbor interactions can be for small values of s . While FF spin-1/2 chains are known to have unentangled ground states, the case $s=1$ had been less explored. They proposed the first example of a FF translation-invariant spin-1 chain that has a unique highly entangled ground state and exhibits some signatures

of critical behavior. The entanglement entropy of one half of the chain scales as $\log(n)/2 + O(1)$, where n is the number of spins. They proved that the energy gap above the ground state is polynomial in $1/n$. The proof relies on a new result concerning statistics of Dyck paths which might be of independent interest.

Technology Transfer