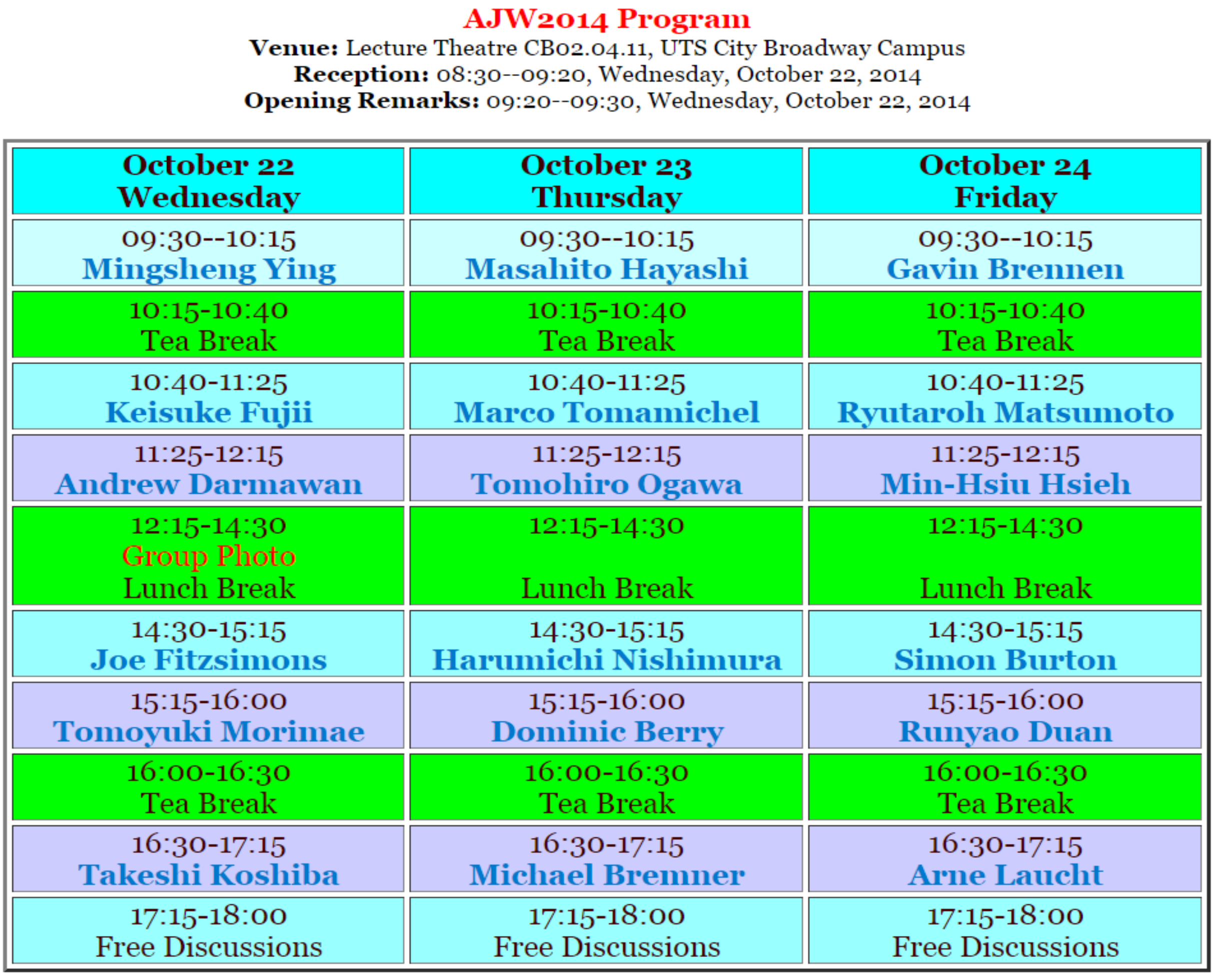
Australia-Japan Workshop on Multi-user Quantum Networks 2014

October 22 - 24, 2014, UTS, Sydney, Australia
http://quantum-lab.org/ajw2014.php

Organising Chairs: Runyao Duan (QCIS, UTS), Masahito Hayashi (Nagoya University & CQT, NUS)

The Australia-Japan Workshop on Multi-user Quantum Networks focuses on the recent advances in quantum computing and quantum information processing. It aims at providing a forum for Australian and Japanese researchers in these fields to exchange their latest research results. All talks of the workshop are by invitation only. This workshop is jointly organised by Quantum Computation Laboratory (QCL) at the Centre for Quantum Computation & Intelligent Systems (QCIS), University of Technology, Sydney (UTS), Australia, and Japanese research fund Grant-in-Aid for Scientific Research (A) "Project on Multi-user Quantum Network" in cooperation with Japanese research fund Grant-in-Aid for Scientific Research (A) "Deepening Quantum Protocol Theory"



AJW2014 Program

Venue: Lecture Theatre CB02.04.11, UTS City Broadway Campus
Reception: 08:30--09:20, Wednesday, October 22, 2014
Opening Remarks: 09:20--09:30, Wednesday, October 22, 2014

October 22 Wednesday	October 23 Thursday	October 24 Friday
09:30--10:15 Mingsheng Ying	09:30--10:15 Masahito Hayashi	09:30--10:15 Gavin Brennen
10:15-10:40 Tea Break	10:15-10:40 Tea Break	10:15-10:40 Tea Break
10:40-11:25 Keisuke Fujii	10:40-11:25 Marco Tomamichel	10:40-11:25 Ryutaroh Matsumoto
11:25-12:15 Andrew Darmawan	11:25-12:15 Tomohiro Ogawa	11:25-12:15 Min-Hsiu Hsieh
12:15-14:30 Group Photo Lunch Break	12:15-14:30 Lunch Break	12:15-14:30 Lunch Break
14:30-15:15 Joe Fitzsimons	14:30-15:15 Harumichi Nishimura	14:30-15:15 Simon Burton
15:15-16:00 Tomoyuki Morimae	15:15-16:00 Dominic Berry	15:15-16:00 Runyao Duan
16:00-16:30 Tea Break	16:00-16:30 Tea Break	16:00-16:30 Tea Break
16:30-17:15 Takeshi Koshiba	16:30-17:15 Michael Bremner	16:30-17:15 Arne Laucht
17:15-18:00 Free Discussions	17:15-18:00 Free Discussions	17:15-18:00 Free Discussions

October 22, Wednesday Morning, Session Chair: Masahito Hayashi

Mingsheng Ying (UTS) **09:30—10:15**

Quantum recursion and second quantisation

This paper introduces a new notion of quantum recursion of which the control flow of the computation is quantum rather than classical as in the notions of recursion considered in the previous studies of quantum programming. A typical example is recursive quantum walks, which are obtained by slightly modifying the construction of the ordinary quantum walks. The operational and denotational semantics of quantum recursions are defined by employing the second quantisation method, and they are proved to be equivalent.

Keisuke Fujii (Kyoto University) **10:40—11:25**

Measurement-based quantum computation using thermal states of many-body Hamiltonian

Measurement-based quantum computation employs many-body entangled states as resources for quantum computation. This paradigm provides a good framework to discuss a connection between quantum information science and many-body physics. In this talk, we report measurement-based quantum computation on thermal states of the interacting cluster Hamiltonian that undergoes thermal phase transitions. We show that the long-range order of the symmetry breaking thermal states drastically enhances the robustness of MBQC against thermal excitations. Specifically, we show that MBQC is topologically protected below the critical temperature in three-dimensional cases.

Andrew Darmawan (The University of Sydney) **11:25—12:15**

Graph states as ground states of two-body frustration-free Hamiltonians

The framework of measurement-based quantum computation (MBQC) allows us to view the ground states of local Hamiltonians as potential resources for universal quantum computation. A central goal in this field is to find models with ground states that are universal for MBQC and that are also natural in the sense that they involve only two-body interactions and have a small local Hilbert space dimension. Graph states are the original resource states for MBQC, and while it is not possible to obtain graph states as exact ground states of two-body Hamiltonians here we construct two-body frustration-free Hamiltonians that have arbitrarily good approximations of graph states as unique ground states. The construction involves taking a two-body frustration-free model that has a ground state convertible to a graph state with stochastic local operations, then deforming the model such that its ground state is close to a graph state. Each graph state qubit resides in a subspace of a higher dimensional particle. This deformation can be applied to two-body frustration-free Affleck-Kennedy-Lieb-Tasaki (AKLT) models, yielding Hamiltonians that are exactly solvable with exact tensor network expressions for ground states. For the star-lattice AKLT model, the ground state of which is not expected to be a universal resource for MBQC, applying such a deformation appears to enhance the computational power of the ground state, promoting it to a universal resource for MBQC. Transitions in computational power, similar to percolation phase transitions, can be observed when Hamiltonians are deformed in this way. Improving the fidelity of the ground state comes at the cost of a shrinking gap. While analytically proving gap properties for these types of models is difficult in general, we provide a detailed analysis of the deformation of a spin-1 AKLT state to a linear graph state.

October 22, Wednesday Afternoon, Session Chair: Runyao Duan

Joe Fitzsimons (Singapore University of Technology and Design & CQT, NUS) **14:00-15:15**

Blind and verifiable quantum computation

Blind Quantum Computing (BQC) allows a client to have a server carry out a quantum computation for them such that the client's inputs, outputs and computation remain private. In this talk I will present a family of protocols for universal unconditionally secure BQC, based on the measurement-based quantum computing model. In the simplest of these protocols the client only needs to be able to prepare single qubits in separable states randomly chosen from a finite set and send them to the server, who has the balance of the required quantum computational resources. I will describe how verification mechanisms can be built on top of such protocols to ensure that any deviation from the prescribed computation by a malicious server is detected with high probability.

Tomoyuki Morimae (Gunma University) **15:15-16:00**

Developments of blind quantum computing

Blind quantum computing [Broadbent, Fitzsimons, and Kashefi, FOCS2009] is a secure protocol of delegated quantum computing where a client who does not have any quantum computer can delegate her quantum computing to a remote server who has a universal quantum computer in such a way that client's privacy is guaranteed. In this talk, I will explain our recent results about blind quantum computing including topological blind quantum computing and device-independent blind quantum computing.

Takeshi Koshiba (Saitama University) **16:30—17:15**

Private information retrieval via blind quantum computation

Quantum physics provides unconditionally secure blind computation schemes. We show that the framework of blind quantum computation provides a methodology to discuss the communication complexity of one-sided secure cryptographic protocols. For the methodology, we introduce a notion of partially blind quantum computation and incorporate it into a technique of reducing communication complexity of some tasks with respect to the privacy by using the advantage of quantum algorithms over classical ones. As example, we take quantum private information retrieval and show a quantum PIR protocol that has the communication complexity poly(log N), where N is the database size. We note that our results do not contradict the lower bounds on the communication complexity of QPIR.

October 23, Thursday Morning, Session Chair: Mingsheng Ying

Masahito Hayashi (Nagoya University & CQT, NUS) **09:30-10:15**

Generalized entropies and quantum security

Security problem is a central issue in quantum information. To discuss this topic, we usually employ information quantities. In this talk, we explain several kinds of generalized entropies in quantum system. Then, I explain how to use these generalized entropies in quantum security. I also explain how to use the other information quantities in other tasks.

Marco Tomamichel (The University of Sydney) **10:40—11:25**

Strong converse bounds for quantum communication

The strong converse property in classical information theory is the fact that any attempt at transmitting information at a rate above capacity will be successful only with a probability that vanishes (exponentially fast) as the number of channel uses increases. In quantum communication we only know a weak converse, which states that the above probability does not converge to one as the number of channel uses goes to infinity. Consequently, it has been an open question to establish a strong converse for the quantum capacity of any non-trivial quantum channel ever since the original works on quantum capacity explicitly stated this as an open question. Our main result is to establish the "Rains information" of a quantum channel as a strong converse bound for quantum communication. We then show how this settles the strong converse question for the quantum capacity of all generalized dephasing channels. (This is joint work with Mark M. Wilde and Andreas Winter.)

Tomohiro Ogawa (The University of Electro-communications) **11:25—12:15**

Quantum relative Renyi relative entropies and strong converse theorems

The classical Renyi relative entropies play a central role in classical information theory through large deviation theory such as Cramer's theorem or Sanov's Theorem. The Renyi relative entropies also provide an information geometrical point of view in large deviation theory, as the potential functions (the logarithm of the partition function) of exponential families connecting probability distributions by e-geodesic. In quantum systems, however, we can consider various non-equivalent analogues of the Renyi relative entropy, due to non-commutativity of operators. In this presentation, we treat the following three different quantities and elucidate their properties, relations, and operational roles. Then we show formulas to determine the strong converse exponent in quantum hypothesis testing and classical-quantum channel coding.

(1) Quantum f-divergence (quasi-entropy by Petz) of Wigner-Yanase-Dyson type
(2) Sandwiched Renyi relative entropy recently proposed in [1,2]
(3) Canonical correlation related to Mori-Kubo-Bogoliubov inner product
(Joint work [3,4,5] with Milan Mosonyi)

[1] M. M.-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, J. Math. Phys., 54, 122203, 2013.
[2] M. Wilde, A. Winter, D. Yang, Commun. Math. Phys., 331, pp. 593-622, 2014.
[3] M. Mosonyi and T. Ogawa, arXiv:1309.3228, 2013, (to appear Commun. Math. Phys., 2014).
[4] M. Mosonyi and T. Ogawa, arXiv:1407.3567, 2014.
[5] M. Mosonyi and T. Ogawa, arXiv:1409.3562, 2014.

October 23, Thursday Afternoon, Session Chair: Joe Fitzsimons

Harumichi Nishimura (Nagoya University) **14:30—15:15**

Generalized quantum Arthur-Merlin games

This work investigates the role of interaction and coins in public-coin quantum interactive proof systems (also called quantum Arthur-Merlin games). While prior works focused on classical public coins even in the quantum setting, the present work introduces a generalized version of quantum Arthur-Merlin games where the public coins can be quantum as well: the verifier can send not only random bits, but also halves of EPR pairs. First, it is proved that the class of two-turn quantum Arthur-Merlin games with quantum public coins, denoted qq-QAM, does not change by adding a constant number of turns of classical interactions prior to the communications of the qq-QAM proof systems. This can be viewed as a quantum analogue of the celebrated collapse theorem for AM due to Babai. To prove this collapse theorem, this work provides a natural complete problem for qq-QAM: deciding whether the output of a given quantum circuit is close to a totally mixed state. This complete problem is on the very line of the previous studies investigating the hardness of checking the properties related to quantum circuits, and is of independent interest. It is further proved that the class qq-QAM_1 of two-turn quantum-public-coin quantum Arthur-Merlin proof systems with perfect completeness gives new bounds for standard well-studied classes of two-turn interactive proof systems. Finally, the collapse theorem above is extended to comprehensively classify the role of interaction and public coins in quantum Arthur-Merlin games: it is proved that, for any constant m>1, the class of problems having an m-turn quantum Arthur-Merlin proof system is either equal to PSPACE or equal to the class of problems having a two-turn quantum Arthur-Merlin game of a specific type, which provides a complete set of quantum analogues of Babai's collapse theorem. This is a joint work with Hirotada Kobayashi and Francois Le Gall.

Dominic Berry (Macquarie University) **15:15—16:00**

Exponential improvement in precision for simulating sparse Hamiltonians

Simulation of quantum mechanical systems is a major potential application of quantum computers. Typically the task that needs to be performed is simulation of the evolution of the quantum state under a Hamiltonian. This simulation is not exact, but an approximation to within some allowable error epsilon. Previous methods had computational complexity scaling polynomially 1/epsilon (for example, as 1/sqrt(epsilon)). This is poor scaling in comparison to algorithms in may other areas, where the complexity scales as the logarithm of 1/epsilon, allowing high accuracy. We provide a new algorithm for simulating Hamiltonian evolution with complexity scaling as log(1/epsilon). The method is based on using a product formula, as with many previous algorithms, but we then compress the product formula, providing greatly improved performance.

Michael Bremner (UTS) **16:30—17:15**

Towards a proof of the classical intractability of quantum simulation

The efficient simulation of quantum systems is considered to be one of the most exciting potential applications of quantum computing technologies. There is an expectation that specialized quantum simulators can be engineered as a stepping stone to the development of fully universal, fault-tolerant, quantum computers. If this expectation is to be realized we must identify physical systems and sets of observables that are both simple enough to robustly implement in a near-term quantum device, yet remain a challenge to classically simulate. In this talk I will discuss several simple quantum systems that cannot be easily simulated classically that might lead to a convincing demonstration of the classical intractability of quantum simulators.

October 24, Friday Morning, Session Chair: Michael Bremner

Gavin Brennen (Macquarie University) **09:30—10:15**

Quantum algorithms for complex and real temperature partition functions

Statistical Mechanics has provided us with straightforward recipes to compute various physical quantities like magnetisation and energy density of many body classical systems. But more often than not, the application of these recipes is computationally inefficient, as can be seen from very idealised systems. It may be expected that quantum algorithms could help in this regard. I will describe a quantum algorithm for measuring complex temperature partition functions of Ising models which, through appropriate Wick rotations, can be analytically continued to yield estimates for real temperatures. Notably the circuits used are low depth and an estimation of the entire partition function is available. Generically, the problem is still hard even with quantum algorithms but in certain cases of weak frustration the scaling is favourable. Finally I'll discuss how to use these methods to address the dual problem concerning the BQP-hardness of estimating partition functions for classical ferromagnetic Ising models in 2D.

Ryutaroh Matsumoto (Tokyo Institute of Technology) **10:40—11:25**

Recent progress in quantum ramp secret sharing

A secret sharing scheme encodes a secret to multiple shares so that only qualified sets of shares can perfectly reconstruct the secret. Secret and shares can be either classical or quantum. Most studies on the secret sharing scheme focus on the perfect scheme, with which a non-qualified share set has zero information about the secret. The main drawback of the perfect scheme is that the share size must be larger than or equal to the secret. The ramp secret sharing schemes overcome this drawback by allowing partial information leakage from non-qualified sets. But the ramp schemes also introduce a new risk. Suppose that the secret is username:password, a share set has 8-symbol information about the secret, which does not enable the perfect reconstruction. The partial information recoverable by the share set may be the "password" part, which is very undesirable. To exclude such a possibility, Yamamoto introduced the notion of strong security for the classical ramp schemes. In this study, we introduce a corresponding quantum definition of the strong security, and propose an explicit construction.

Min-Hsiu Hsieh (UTS) **11:25—12:15**

The learnability of quantum measurements

Quantum machine learning has received significant attention in recent years and promising progress has been made in the development of quantum algorithms to speed up traditional machine learning tasks. In this work, however, we focus on the study of the information-theoretic upper bounds of sample complexity—how many training samples are sufficient to predict the future behaviour of an unknown target function. This kind of problem is, arguably, one of the most fundamental problems in statistical learning theory and the bounds for practical settings can be completely characterised by a simple measure of complexity.

Our main result in the paper is that, for learning an unknown quantum measurement, the upper bound, given by the fat-shattering dimension, is linearly proportional to the dimension of the underlying Hilbert space. Learning an unknown quantum state [1] becomes a dual problem to ours, and as a byproduct, we can recover Aaronson's famous result solely using a classical machine learning technique. In addition, we are able to connect measures of sample complexity with various areas such as quantum state/measurement tomography, quantum state discrimination and quantum random access codes, which may be of independent interest. Lastly, with the assistance of general Bloch- sphere representation, we show that learning quantum measurements/states can be mathematically formulated as a neural network. Consequently, classical ML algorithms can be applied to efficiently accomplish the learning tasks.

[1] S. Aaronson, "The learnability of quantum states," Proc. R. Soc. A, vol. 463, no. 2088, pp. 3089-3144, 2007.

October 24, Friday Afternoon, Session Chair: Tomohiro Ogawa

Simon Burton (The University of Sydney) **14:30—15:15**

Error correction in a Fibonacci anyon code

Standard classical error correcting codes use a parity check matrix. Error correction in the quantum case proceeds similarly, but after the removal of violated parity checks (defects), we allow certain "local" operations to have occurred. This leads to a topological view of error correction. In this talk we extend to the non-abelian setting: defects can now braid around each other in non-trivial ways. Condensed matter physicists think of these defects as particles, and we examine a system where such particles behave as "Fibonacci anyons". We use numerics to demonstrate a threshold for error correction below which quantum information can be recovered with asymptotic certainty.

Runyao Duan (UTS) **15:15—16:00**

Quantum unambiguous capacity

We study the possibility of communicating classical information unambiguously with noisy quantum channels where the receiver can either correctly recover the classical message sent by the sender or simply claim an uncertain outcome. A notion of unambiguous capacity is introduced to characterize the optimal communication rates one can achieve under unambiguous decoding strategies. We provide a necessary and sufficient condition for the feasibility of unambiguous communication by establishing a connection to the extendibility of Kraus operator space of quantum channels. Consequently, we show that unambiguous capacity can be super-activated: there are two quantum channels both having zero unambiguous capacity can be used jointly to send classical information unambiguously. Finally, we find auxiliary resources such as shared entanglement, classical feedback, or quantum feedback, can considerably improve the unambiguous capacity to achieve the ordinary (small-error) capacity.

Arne Laucht (University of New South Wales) **16:30—17:15**

Single donor qubits in ^{28}Si: New benchmarks for solid state qubits

Please see the appendix at the end of this pdf for a detailed abstract! ☺

AJW2014 Participants List

Name	Affiliation	Email
ARMSTRONG, Seiji	Australian National University	seiji.armstrong@gmail.com
BERRY, Dominic	Macquarie University	dmwberry@gmail.com
BREMNER, Michael	QCIS, UTS	bremner@gmail.com
BRENNEN, Gavin	Macquarie University	gbrennen@gmail.com
BURTON, Simon	The University of Sydney	sburton@physics.usyd.edu.au
CAVALCANTI, Eric	The University of Sydney	e.cavalcanti@physics.usyd.edu.au
CHEN, Weien	QCIS, UTS	cenbiqing@gmail.com
DARMAWAN, Andrew	The University of Sydney	darmawan@physics.usyd.edu.au
DEHOLLAIN, Juan-Pablo	University of New South Wales	jpd@unsw.edu.au
DUAN, Runyao	QCIS, UTS	runyao@gmail.com
FANG, Caishi	QCIS, UTS	thinliber@gmail.com
FENG, Yuan	QCIS, UTS	flyt77@gmail.com
FITZSIMONS, Joe	SUTD & CQT, NUS	joe.fitzsimons@gmail.com
FLAMMIA, Steve	The University of Sydney	sflammia@gmail.com
FUJII, Keisuke	Kyoto University	keisuke.fujii@i.kyoto-u.ac.jp
GUAN, Ji	QCIS, UTS	guanji1992@gmail.com
GUO, Cheng	QCIS, UTS	cheng323232@gmail.com
HAYASHI, Masahito	Nagoya University & CQT, NUS	masahito@math.nagoya-u.ac.jp
HOSSEINI, Neda	University of New South Wales	neda.hosseini@unsw.edu.au
HSIEH, Min-Hsiu	QCIS, UTS	minhsiuh@gmail.com
HUANG, Zixin	The University of Sydney	zhua8897@uni.sydney.edu.au
KOSHIBA,Takeshi	Saitama University	koshiba@mail.saitama-u.ac.jp
LAI, Ching-Yi	QCIS, UTS	cylai0616@gmail.com
LAUCHT, Arne	University of New South Wales	a.laucht@unsw.edu.au
LI, Yinan	QCIS, UTS	liyinan9252@gmail.com
LIU, Wenjie	Nanjing Univ. of Inf. Sci. and Tech.	wenjiel@163.com
MALANEY, Robert	University of New South Wales	r.malaney@unsw.edu.au
MATSUMOTO, Ryutaroh	Tokyo Institute of Technology	ryutaroh@rmatsumoto.org
MENICUCCI, Nicolas	The University of Sydney	ncmenicucci@gmail.com
MORIMAE, Tomoyuki	Gunma University	morimae@gunma-u.ac.jp
NISHIMURA, Harumichi	Nagoya University	hnishimura@is.nagoya-u.ac.jp
OGAWA, Tomohiro	University of Electro-communications	ogawa@is.uec.ac.jp
PFEIFER, Robert	Macquarie University	robert.pfeifer@mq.edu.au
QIAO, Youming	QCIS, UTS	jimmyqiao86@gmail.com
SHI, Zhan	University of New South Wales	zhan.shi.f@gmail.com
SU, Zhaofeng	QCIS, UTS	youngpath2012@gmail.com
TOMAMICHEL, Marco	The University of Sydney	marcotom.ch@gmail.com
WANG, Xin	QCIS, UTS	wangxinfelix@gmail.com
WARDROP, Matthew	The University of Sydney	mister.wardrop@gmail.com
XIE, Wei	QCIS, UTS	xxiewwei@gmail.com
YING, Mingsheng	QCIS, UTS	mingshengying@gmail.com
YING, Shenggang	QCIS, UTS	yingshenggang@gmail.com

Single donor qubits in isotopically purified ^{28}Si: New benchmarks for solid-state qubits

Arne Laucht[1], Juha T. Muhonen[1], Juan P. Dehollain[1], Fay E. Hudson[1], Takeharu Sekiguchi[2], Kohei M. Itoh[2], David N. Jamieson[3], Jeffrey C. McCallum[3], Andrew S. Dzurak[1], Andrea Morello[1]

[1] Centre for Quantum Computation and Communication Technology, School of Electrical Engineering and Telecommunication, University of New South Wales, NSW 2052, Australia
[2] School of Fundamental Science and Tech., Keio University, 3-14-1 Hiyoshi, 223-8522, Japan
[3] Centre for Quantum Computation and Communication Technology, School of Physics, University of Melbourne, VIC 3010, Australia

A phosphorus donor in silicon is, almost literally, the equivalent of a hydrogen atom in vacuum. It possesses electron and nuclear spins of 1/2 which act as natural qubits [1], and the host material can be isotopically purified to be almost perfectly free of other spin species, ensuring extraordinary coherence times (~180 s) [2]. It is, however, still embedded in a semiconductor host material, allowing electric gates to be used to manipulate its electrostatic environment and a microwave transmission line to apply spin resonant pulses.

The single-shot readout [3] and coherent control of both the electron [4] and the nuclear spin [5] of a single P atom in silicon have been recently demonstrated, using ion-implanted donors in MOS nanostructures. It is known from bulk experiments that P donors in isotopically purified ^{28}Si exhibit record coherences [2], but it is also suspected that the proximity to a Si/SiO$_2$ interface will deteriorate the coherence time. Here, we present the first experiment on single electron and nuclear spin qubits in an isotopically engineered ^{28}Si nanostructure [6]. We measure free induction decay-limited electron spin resonance lines (< 2 kHz FWHM), and we obtain average single-qubit control fidelities of 99.95% for the electron and 99.99% for the nucleus. Noise spectroscopy experiments indicate that, contrary to widespread belief, the ultimate limit for single-spin coherence in our nanostructure is not set by charge noise and interface effects, but simply by broadband thermal radiation coupled to the qubit through a high-bandwidth transmission line. Using dynamical decoupling, we measured coherence times up to $T_{2e}^{DD} = 0.5$ s for the electron, and $T_{2n}^{DD} = 35$ s for the ^{31}P nucleus.

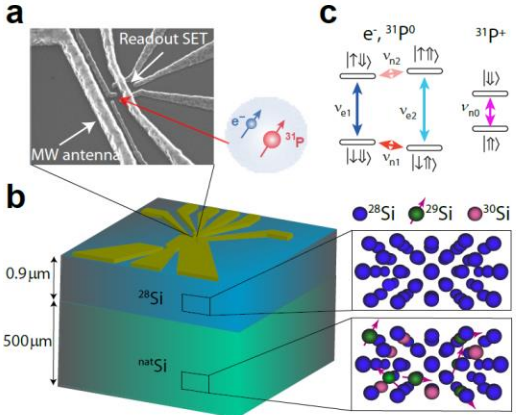


Figure 1: a) SEM image of the device, b) schematic of the substrate, and c) energy level diagram of the qubit states.

Finally, we will present an innovative qubit control scheme, which employs the Stark shifts of the gyromagnetic ratio and hyperfine coupling to electrically tune the spin transitions in resonance with the microwave source. The ability to electrically control the resonance frequency greatly simplifies the operation of a multi-qubit device, as it allows independent, high-fidelity qubit operations without the need to pulse the microwave source.

References

[1] Kane B, *Nature* **393**, 133 (1998)
[2] Steger M, *et al.*, *Science* **336**, 1280 (2012)
[3] Morello A, *et al.*, *Nature* **467**, 687 (2010)
[4] Pla J J, *et al.*, *Nature* **489**, 541 (2012)
[5] Pla J J, *et al.*, *Nature* **496**, 334 (2013)
[6] Muhonen J T, *et al.*, *arxiv:1402.7140*, (2014)