The 6th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC 2011)

Book of Abstracts

Universidad Complutense de Madrid
May 24–26, 2011

Invited talks

Héctor Bombín (Perimeter Institute)
Structure of 2D Topological Stabilizer Codes

Abstract: By characterizing codes in terms of "lattice groups" on infinite lattices, we show that they can all be understood in terms of topological charges and string operators. This is true either for subspace or subsystem codes, and it has direct applications for error correction, for example. Subspace codes are directly connected to topologically ordered condensed matter systems. We show that all 2D topological stabilizer codes are equivalent up to local transformations to several copies of one universal phase: Kitaev's topological code.

Hans Briegel (Innsbruck)
Projected simulation for artificial intelligence

Abstract: We introduce a notion of a learning agent whose interaction with the environment is governed by a simulation-based projection, which allows the agent to project itself into future situations before it takes real action. Projective simulation is based on a random walk through a network of clips, which are elementary patches of episodic memory. The network of clips changes dynamically, both due to new perceptual input and due to certain compositional principles of the simulation process. During simulation, the clips are screened for specific features which trigger factual action of the agent. The scheme is different from other, computational, notions of simulation, and it provides a new element in an embodied cognitive science approach to intelligent action and learning. While the scheme works entirely classically, it also provides a natural route for generalization to quantum-mechanical operation.

Joint work with Gemma De las Cuevas.

Nicolas Gisin (Geneva)
Futures of Quantum Communication: Device-Independent QKD, Quantum Networks and bi-locality

Abstract: There are two main Grand Challenges for academic research in quantum communication. The first one concerns "device independent QKD", that is an implementation of Quantum Key Distribution that exploits the nonlocal correlation observed in violations of Bell's inequality to realize "self testing QKD apparatuses". The second one aims at futuristic continental scale quantum networks. The latter requires, among others, multimode quantum memories with close to a second memory times, a fascinating challenge. Interestingly, quantum networks also lead us to a refreshing revisit of nonlocality.

Joint work with Hugo Zbinden, Mikael Afzelius, and Rob Thew.

Mio Murao (Tokyo)
"Globalness" of unitary operations on quantum information

Abstract: One of the essential differences between quantum information processing (QIP) and the classical counterpart is that QIP sometimes involves global operations on unknown input states, namely, arbitrary superpositions of quantum states where their superposition coefficients are unknown. Quantum teleportation and quantum error corrections are typical examples. We call such unknown states. Quantum information cannot be measured (i.e., estimating the unknown coefficients by finite measurements) perfectly and cannot be copied perfectly either. In contrast, classical information in QIP can be encoded in a set of known orthogonal states and can be perfectly measured. Classical information can be also obtained by the result of measurements in QIP. QIP can be analyzed by investigating how input quantum information is transformed to output quantum information due to global operations. Therefore, evaluation of the "globalness" of global operations on quantum information is desirable. In this talk, I present our recent results from investigating the globalness of unitary operations on quantum information in terms of delocalizing power [1], entanglement cost [2], and implementation over a butterfly network [3].

[1] A. Soeda, M. Murao, New J. Phys. 12, 093013 (2010).
[2] A. Soeda, T.S. Turner, M. Murao, arXiv:1008.1128.
[3] A. Soeda, Y. Kinjo, T.S. Turner and M. Murao, arXiv:1010.4350.

Tobias Osborne (Hannover)
The continuum limit of a quantum circuit: variational classes for quantum fields

Abstract: in recent years we've seen many developments in the study of strongly correlated quantum systems spurred by insights from the study of entanglement in quantum information theory. In particular, new variational classes manifestly exploiting the entropy/area law have been applied to successfully study a wide range of settings from real-time evolution to finite fermion densities. These developments have been mostly centered in the lattice setting. In this talk I'll describe recent work in generalizing the two most successful variational classes developed, matrix product states and the multiscale entanglement renormalization ansatz, to the quantum field setting by exploiting a continuum limit of their quantum circuit descriptions.

Umesh Vazirani (Berkeley)
TBD

Contributed talks

Telescopic Relative Entropy

Koenraad M.R. Audenaert

Department of Mathematics,
Royal Holloway, University of London,
Egham TW20 0EX, United Kingdom

The quantum relative entropy between two quantum states ρ and σ, $S(\rho||\sigma) = \operatorname{Tr}\rho(\log\rho - \log\sigma)$, is a non-commutative generalisation of the Kullback-Leibler distance between probability distributions. Because of its strong mathematical connections with von Neumann entropy, and its interpretation as an optimal asymptotic error rate in quantum hypothesis testing (in the context of Stein's lemma) relative entropy is widely used as a (non-symmetric) distance measure between states.

One of its drawbacks, however, is that for non-faithful (rank-deficient) states the relative entropy can be infinite. In particular, relative entropy is useless as a distance measure between pure states, since it is infinite for pure ρ and σ, unless ρ and σ are exactly equal (in which case it always gives 0).

There are various possibilities to overcome this deficiency. One is to apply a smoothing process. One can define the *smooth relative entropy* between states ρ and σ as the infimum of the ordinary relative entropy between ρ and another state τ, where τ is constrained to be ϵ-close to σ in trace norm distance:

$$S_\epsilon(\rho||\sigma) = \inf_\tau \left\{ S(\rho||\tau) : \tau \geq 0, \operatorname{Tr}\tau \leq 1, ||\tau - \sigma||_1 \leq \epsilon \right\}.$$

This form of smoothing has already been applied to Renyi entropies and max-relative entropy, giving rise to a quantity with an operational interpretation, but it could equally well be applied to ordinary relative entropy.

In the case of the ordinary relative entropy there is a simple canonical choice for τ that achieves the same purpose of regularisation but without having to find the exact minimiser. Namely, we can take that τ that is collinear with ρ and σ; i.e. $\tau = a\rho + (1-a)\sigma$.

It is easy to show that $S(\rho||\tau)$ is bounded above by $-\log a$, which is finite for $0 < a < 1$. It therefore makes perfect sense to normalise $S(\rho||\tau)$ by dividing it by $-\log a$, producing a quantity that is always between 0 and 1.

These observations led us to define what we call the *telescopic relative entropy* (TRE). For fixed $a \in (0,1)$, the a-telescopic relative entropy

between states ρ and σ is given by

$$S_a(\rho||\sigma) := \frac{1}{-\log(a)}\ S(\rho||a\rho + (1-a)\sigma). \tag{1}$$

Furthermore, we define

$$S_0(\rho||\sigma) := \lim_{a\to 0} S_a(\rho||\sigma) \tag{2}$$

$$S_1(\rho||\sigma) := \lim_{a\to 1} S_a(\rho||\sigma), \tag{3}$$

and show that these limits exist and provide explicit formulas.

It is the purpose of this paper to initiate the study of this quantity. The telescoping operation $\sigma \mapsto a\rho + (1-a)\sigma$ has a number of far-reaching and sometimes unexpected consequences. Because of its linearity, the TRE inherits most of the desirable properties of the ordinary relative entropy. However, a host of additional relations in the form of sharp inequalities may be derived that in the case of the ordinary relative entropy simply make no sense, because the constants appearing in the inequality would be infinite.

When ρ and σ are pure, there is an explicit one-to-one relation between $S_a(\rho||\sigma)$ and the trace norm distance $T(\rho,\sigma)$ for any value of $a \in [0,1]$. Although the relation is somewhat complicated, in practice it shows that $S_a(\rho||\sigma)$ is only slightly bigger than $T(\rho,\sigma)^2$.

We also provide bounds on the TRE in terms of the trace norm distance. While there is no upper bound on the ordinary relative entropy in terms of the trace norm distance, we can find a sharp upper bound on the TRE: for any $a \in (0,1)$,

$$S_a(\rho||\sigma) \leq T(\rho,\sigma). \tag{4}$$

An unsuspected corollary is a strengthening of a very well-known inequality. For any two states ρ, σ and $(p, 1-p)$ a probability distribution,

$$S(p\rho + (1-p)\sigma) - (pS(\rho) + (1-p)S(\sigma)) \leq h(p)\ T(\rho,\sigma). \tag{5}$$

Further properties of the TRE will be explored in forthcoming papers. This includes an interesting connection with Hamiltonian reconstruction. There is some evidence that the difference $S_a(\rho||\sigma_1) - S_a(\rho||\sigma_2)$ might provide non-trivial lower bounds on the time needed for state σ_1 to evolve unitarily into state σ_2 under the influence of a Hamiltonian with bounded energy.

Large violation of Bell inequalities using both particle and wave measurements

Daniel Cavalcanti[1], Nicolas Brunner[2], Paul Skrypczyk[2], Alejo Salles[3], and Valerio Scarani[1]

[1] Centre for Quantum Technologies, National University of Singapore, 3 Science drive 2, Singapore 117543

[2] H.H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom

[3] Niels Bohr Institute, Blegdamsvej 17, 2100 Copenhagen, Denmark

When separated measurements on entangled quantum systems are performed, the theory predicts correlations that cannot be explained by any classical mechanism: communication is excluded because the signal should travel faster than light; pre-established agreement is excluded because Bell inequalities are violated. All optical demonstrations of such violations [1] have involved discrete degrees of freedom and are plagued by the detection-efficiency loophole. A promising alternative is to use continuous variables combined with highly efficient homodyne measurements. However, all schemes proposed so far use states or measurements that are extremely difficult to achieve [2], or produce very weak violations [3, 4]. Here we present a simple method for generating large violations for feasible states using both photon counting and homodyne detections. Our scheme may lead to the first violation of Bell inequalities using continuous-variable measurements and pave the way for a loophole-free Bell test.

We study schemes in which both Alice and Bob alternate between counting and homodyne measurements [5] (see Fig. 1), then locally post-process their data to extract bits and check the Clauser-Horne-Shimony-Holt (CHSH) inequality. A significant violation $S \approx 2.25$ (while $S \leq 2$ for any local model) can be achieved by the state

$$|\Psi_2\rangle = \frac{|2\rangle_A|0\rangle_B + |0\rangle_A|2\rangle_B}{\sqrt{2}}. \quad (1)$$

where $|0\rangle$ and $|2\rangle$ refer to states of well defined photon-number. This state can be created by having two heralded single photons from down-conversion sources bunch on a beam-splitter, in a Hong-Ou-Mandel setup.

The experimental implementation of our scheme seems feasible with present day technology, though probably challenging. However homodyne measurements on one and two-photon states coming from down-conversion have been reported [6]. Our scheme opens new possibilities

for a loophole-free Bell test. We study the influence of experimental imperfections, in particular focusing on the limited efficiency of the photon counting measurement and the transmission between the source and the detectors. We find that our scheme is resistant to imperfections. The requirements in terms of detection efficiency and transmission are comparable to the most favorable feasible schemes known to date for discrete variables.

Finally, the combination of counting and homodyne measurements can be applied to many more scenarios. Notably, the two-mode squeezed state violates CHSH for some values of the squeezing parameter λ. Although the violation found is small ($S \approx 2.05$ for $\lambda = 0.83$), it is remarkable, since this state is Gaussian and easily produceable in the lab.

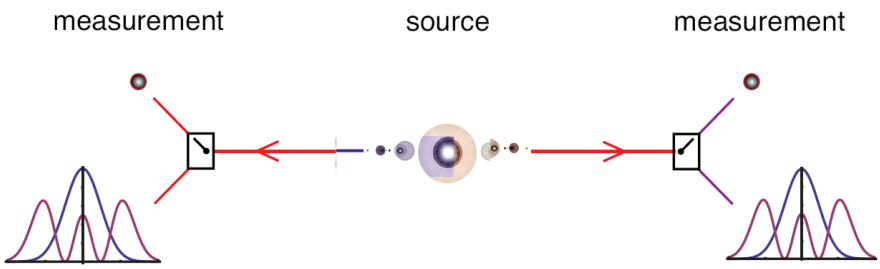

Fig. 1. A source sends a photonic entangled state to two space-like separated locations. In these locations each subsystem is subjected to one of two measurements: number of photons (photon counting) or quadrature (homodyning) measurements. In this way both wave and particle characteristics of the systems are tested.

References

1. A. Aspect, "To be or not to be local", Nature **446**, 866 (2007).
2. K. Banaszek, K. Wódkiewicz, Nonlocality of the Einstein-Podolski-Rosen state in the Wigner representation, Phys. Rev. A **58**, 4345 (1998)
3. R. García-Patrón Sánchez, J. Fiurášek, N.J. Cerf, J. Wenger, R. Tualle-Brouri, P. Grangier, Proposal for a loophole-free Bell test using homodyne detection, Phys. Rev. Lett. **93**, 130409 (2004)
4. H. Nha, H.J. Carmichael, Proposed test of quantum nonlocality for continuous variables, Phys. Rev. Lett. **93**, 020401 (2004)
5. D. Cavalcanti, N. Brunner, P. Skrzypczyk, A. Salles, V. Scarani, "Large violation of Bell inequalities using both particle and wave measurements", preprint arXiv:1012.1916.
6. S.A. Bimbard, N. Jain, A. MacRae, and A.I. Lvovski, Quantum-optical state engineering up to the two-photon level. Nat. Photon. **4**, 243 (2010).

Local unitary group stabilizers and entanglement for multiqubit symmetric states

Curt D. Cenci[1], David W. Lyons[1], and Scott N. Walck[2]

[1] Mathematical Sciences, Lebanon Valley College, Pennsylvania USA
[2] Physics, Lebanon Valley College, Pennsylvania USA

Abstract. We refine recent local unitary entanglement classification for symmetric pure states of n qubits (that is, states invariant under permutations of qubits) using local unitary stabilizer subgroups and Majorana configurations.

1 Overview

The question of when a given multiparty state can be converted to another by local operations and measurements of subsystems is crucial in quantum information science [1]. The fact that entangled states play a role as resources in computation and communication protocols motivates problems of measurement and classification of entanglement. In general, these are difficult problems, already rich for the case of pure states of n-qubits, where the number of real parameters necessary for classifying entanglement types grows exponentially in n.

A promising special case for the general problem of entanglement measurement and classification is that of the symmetric states, that is, states of composite systems that are invariant under permutation of the subsystems. Symmetric states admit simplified analyses, and they are of interest in their own right. Examples of recent work in which permutation invariance has made possible results where the general case remains intractable include: geometric measure of entanglement [2–4], efficient tomography [5], classification of states equivalent under stochastic local operations and classical communication (SLOCC) [6, 7], and our own work on classification of states equivalent under local unitary (LU) transformations [8].

The main result of this paper is a classification of LU equivalence classes of n-qubit symmetric states that refines our own previous work [8], which is based on the following idea. Suppose states ρ, ρ' are local unitary equivalent via some LU transformation U, that is, we have $\rho' = U\rho U^\dagger$. If a local unitary operator V stabilizes ρ, then $UVU^\dagger$ stabilizes ρ'. The

consequence is that stabilizer subgroups of locally equivalent states are isomorphic via conjugation. Thus the isomorphism class of the stabilizer is an LU invariant. This inspires a two-stage classification program.

1. Classify LU stabilizer subgroup conjugacy classes.
2. Classify LU classes of states for each of the stabilizer classes from stage 1.

Analysis of both stages 1 and 2 is aided by the following geometric observations regarding symmetric states. A Bloch sphere rotation of the Majorana configuration of points representing a symmetric state $|\psi\rangle$ results in an LU equivalent state $|\psi'\rangle = V^{\otimes n} |\psi\rangle$, where V is the 2×2 unitary operator corresponding to the given rotation of the sphere. Not obvious, but true nonetheless, is that given *any* LU operation $U = U_1 \otimes U_2 \otimes \cdots \otimes U_n$ that transforms a symmetric state $|\psi\rangle$ to another symmetric state $|\psi'\rangle$, there is a 1-qubit operation V such that $|\psi'\rangle = V^{\otimes n} |\psi\rangle$. This was proved by Mathonet et al. [9] for SLOCC operations on pure symmetric states. We show that this holds more generally for LU operations on *mixed* symmetric states.

We show there are six classes of infinite LU stabilizer groups and classify their corresponding LU-inequivalent states. Discrete LU stabilizer subgroups are isomorphic to finite subgroups of $SO(3)$. These are the cyclic groups, the dihedral groups, and the symmetry groups of the five Platonic solids.

References

1. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000)
2. M. Aulbach, D. Markham, M. Murao, New J. Phys. **12**, 073025 (2010). ArXiv:1003.5643v2 [quant-ph]
3. M. Aulbach, D. Markham, M. Murao, URL http://arxiv.org/abs/1010.4777. ArXiv:1010.4777v1 [quant-ph]
4. D.J.H. Markham, (2010). ArXiv:1001.0343v1 [quant-ph]
5. G. Toth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, H. Weinfurter, (2010). ArXiv:1005.3313v3 [quant-ph]
6. T. Bastin, S. Krins, P. Mathonet, M. Godefroid, L. Lamata, E. Solano, Phys. Rev. Lett. **103**, 070503 (2009). ArXiv:0902.3230v3 [quant-ph]
7. T. Bastin, P. Mathonet, E. Solano, (2010). ArXiv:1011.1243v1 [quant-ph]
8. C.D. Cenci, D.W. Lyons, L.M. Snyder, S.N. Walck, Quantum Information and Computation **10**, 1029 (2010). URL http://arxiv.org/abs/1007.3920. ArXiv:1007.3920v1 [quant-ph]
9. P. Mathonet, S. Krins, M. Godefroid, L. Lamata, E. Solano, T. Bastin, Phys. Rev. A **81**, 052315 (2010). ArXiv:0908.0886v2 [quant-ph]

The locking-decoding frontier for generic dynamics

Frédéric Dupuis[1], Jan Florjanczyk[2], Patrick Hayden[2,4], Debbie Leung[3,4]

[1] Institute for Theoretical Physics, ETH Zurich, Switzerland
[2] School of Computer Science, McGill University, Canada
[3] Institute for Quantum Computing, University of Waterloo, Canada
[4] Perimeter Institute for Theoretical Physics, Waterloo, Canada

One of the most basic and intuitive properties of most information measures is that the amount of information carried by a physical system must be bounded by its size. For example, if one receives ten physical bits, then one's information, regardless of what that information is "about", should not increase by more than ten bits. While this is true for most information measures, in quantum mechanics there exist natural ways of measuring information that violate this principle by a wide margin. In particular, this violation occurs when one defines the information contained in a quantum system as the amount of classical information that can be extracted by the best possible measurement. To construct examples of this effect, we take a classical message and encode it into a two-part quantum message: a *cyphertext*, which is roughly as large as the message, and a much smaller *key*. Given both the cyphertext and the key, the message can be perfectly retrieved. We can then look at the amount of information that can be extracted about the message the message by a measurement given only access to the cyphertext. Locking occurs if this amount of information is less than the amount of information in the message minus the size of the key.

Our results are stronger than previous results in the sense that instead of using the accessible information, we define locking in terms of the trace distance between measurement results on the real state and measurement results on a state completely uncorrelated with the message . Unlike the accessible information, this has a very natural operational interpretation: it bounds the largest probability with which we can guess, given a message m and the result x of a measurement done on a cyphertext, whether x comes from a valid cyphertext for m or from a cyphertext generated independently from m.

Despite this stronger definition, we are also be able to show that the locking phenomenon is generic. Instead of having a classical key revealing the basis in which the information is encoded, we consider the case where there is a single unitary, and the key is simply a small part of the quantum

system after the unitary is applied. In particular, we are be able to show that locking occurs with high probability in physical systems whose internal dynamics are sufficiently random to be adequately modelled by a Haar-distributed unitary. This can therefore give interesting results in the context of thermodynamics, or of the black hole information problem.

We also allow the measuring device to share entanglement with the cyphertext-key compound system. While this may not correspond to a very meaningful cryptographic scenario, it allows us to study the behavior of entanglement in physical systems, and to know to what extent the presence of entanglement can allow us to beat this locking effect.

Finally, unlike previous work, we do not limit the message (or the entanglement) to be uniform; the size of the key instead depends on the min-entropy of the message. This assumption is easier to justify in cryptographic applications. Indeed, while the locking results we present here can be interpreted as demonstrating the possibility of encrypting classical messages in quantum systems using only very small keys, care must be taking when composing such encryption with other protocols. We use our results to exhibit a quantum key distribution protocol, for example, that appears to be secure if the eavesdropper's information about the secret key is measured using the accessible information, but in which leakage of a logarithmic amount of key causes the entire key to be compromised.

The proof follows the basic strategy of many concentration of measure arguments. We allow the decoding party access to POVMs, but since we cannot directly discretize the space of all POVMs, we rely on a more involved argument based on the operator Chernoff bound to reduce the problem to a discretizable set. The basic idea is to start from the fact that, given a fixed measurement superoperator, the probability over the choice of unitaries that this measurement yields non-negligible correlations is extremely small. Then, we would like to discretize the space of all measurement superoperators and use the union bound to show that the probability that *any* measurement superoperator yields non-negligible correlations is still very small. For this to work, the "number" of measurements has to be much smaller than the reciprocal of the probability of choosing a non-locking unitary. However, the set of measurement superoperators cannot be discretized directly, since (among other things) the measurements contain a potentially unbounded number of outputs. Hence, we bootstrap the above argument on new quasi-measurement objects which yield similar stastics to POVMs.

Unconditionally-secure and reusable public-key authentication (Extended Abstract)

Lawrence M. Ioannou[1,2] and Michele Mosca[1,2,3]

[1] Institute for Quantum Computing, University of Waterloo,
200 University Avenue, Waterloo, Ontario, N2L 3G1, Canada
[2] Department of Combinatorics and Optimization, University of Waterloo,
200 University Avenue, Waterloo, Ontario, N2L 3G1, Canada
[3] Perimeter Institute for Theoretical Physics
31 Caroline Street North, Waterloo, Ontario, N2L 2Y5, Canada

Public-key cryptography has proved to be an indispensable tool in the modern information security infrastructure. Most notably, digital signature schemes form the backbone of Internet commerce, allowing trust to be propagated across the network in an efficient fashion. In turn, public-key encryption allows the private communication of messages (or, more usually, the establishment of symmetric secret keys) among users who are authenticated via digital signatures. The security of these classical public-key cryptosystems relies on assumptions on the difficulty of certain mathematical problems [1]. Gottesman and Chuang [2] initiated the study of quantum-public-key cryptography, where the public keys are quantum systems, with the goal of obtaining the functionality and efficiency of public-key cryptosystems but with information-theoretic security. They presented a secure one-time digital signature scheme for signing classical messages, based on Lamport's classical scheme [3].

Given the importance of the public-key paradigm in classical cryptography, it is perhaps surprising that its quantum incarnation is not as richly a developed field. One possible explanation for the relative lack of papers on the subject is the no-go theorem in Ref. [4], which forbids the digital signing of arbitrary pure states. However, it should be noted that the theorem itself is quite specific in scope, and there remains a range of interesting open problems: no theorem is currently known to rule out quantum-public-key schemes for encryption of classical or quantum states, authentication (signing) of classical messages or all subsets of quantum states, or authentication of entities. Our paper concerns entity authentication—often called *identification*.

Authentication schemes are not concerned with ensuring the *privacy* of information, but rather seek to ensure its *integrity*. For example, digital signature schemes ensure the integrity of origin of messages, whereas

identification schemes ensure the integrity of origin of communication in real time [1]. Identification protocols are said to ensure "aliveness"—that the entity proving its identity is active at the time the protocol is executed. In practice, they are used in smart-card readers in bank machines and next to controlled-access doorways.

We prove that an identification scheme based on the one in Ref. [5] is secure against a computationally-unbounded adversary (only restricted by finite cheating strategies), demonstrating for the first time that unconditionally-secure and reusable public-key authentication is possible in principle. We regard our result more as a proof of concept than a (potentially) practical scheme. Still, we are confident that an extension of the techniques used here may lead to more efficient protocols.

To prove security of our protocol, we employ some elements of the polynomial method (as in Ref. [6]), the theory of estimation of black-box group transformations [7], and the theory of bounded quantum reference frames [8]. We also use the quantum Fourier transform in a new and rather surprising way. Thus, we hope our techniques open the door not only to the discovery of more robust or more efficient identification schemes, but also to the advancement of the above areas of quantum information theory.

References

1. A. J . Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press LLC, Boca Raton, 1996.
2. Daniel Gottesman and Isaac L. Chuang. Quantum digital signatures, 2001. quant-ph/0105032.
3. L. Lamport. Constructing digital signatures from a one-way function. CSL 98, SRI International, October 1979.
4. Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In IEEE Press, editor, *Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02)*, pages 449–458, 2002.
5. Lawrence M. Ioannou and Michele Mosca. Public-key cryptography based on bounded quantum reference frames. http://arxiv.org/abs/0903.5156.
6. Wim van Dam, G. Mauro D'Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Optimal phase estimation in quantum networks. *Journal of Physics A: Mathematical and Theoretical*, 40:7971–7984, 2007.
7. G. Chiribella, G. M. D'Ariano, and M. F. Sacchi. Optimal estimation of group transformations using entanglement. *Phys. Rev. A*, 72(4):042338, 2005.
8. Stephen D. Bartlett, Terry Rudolph, Robert W. Spekkens, and Peter S. Turner. Degradation of a quantum reference frame. *New J. Phys.*, 8:58, 2006.

Approximating the Turaev-Viro Invariant of Mapping Tori is Complete for One Clean Qubit

Stephen P. Jordan[1] and Gorjan Alagic[2]

[1] Institute for Quantum Information, Caltech. *sjordan@caltech.edu*
[2] Institute for Quantum Computing, University of Waterloo. *galagic@iqc.ca*

In 1998, Knill and Laflamme proposed that exponential speedups over classical computers could still be possible even if one can only initialize a single qubit into a pure state, with the rest of the qubits in the maximally mixed state [4]. The complexity class thus defined is called DQC1. Estimating the trace of a unitary operator is a DQC1-complete problem, while estimating a single matrix entry is a BQP-complete problem; no efficient classical algorithms are known in either case.

Finding other natural BQP-complete and DQC1-complete problems is essential to our understanding of the computational power afforded by quantum computers. Groundbreaking work by Freedman, Kitaev, Larsen and Wang [3] in the 1990s, along with later work [1] showed that approximating the Jones polynomial, a famous invariant of links, is in fact a BQP-complete problem[3]. In these works, the input is an element of the braid group, and the output is an estimate of the Jones polynomial of the so-called *plat closure* of the input braid. In 2008, Shor and Jordan [5] showed that estimating the Jones polynomial of the so-called *trace closure* of the input braid is a complete problem for DQC1.

Our work shows that the above results are an example of a more general relationship between estimation of topological invariants on one hand, and quantum computational complexity classes on the other. Recently, Alagic, Jordan, König and Reichardt [2] showed that approximating certain invariants of 3-manifolds is a BQP-complete problem. In this formulation, the input is a so-called *Heegaard splitting* of a 3-manifold, specified as an element of the mapping class group; the output is an estimate of the Turaev-Viro invariant of the input manifold. In this work, we complete the picture formed by the above results by showing that approximating the Turaev-Viro invariant of a 3-manifold specified as a *mapping torus* is a complete problem for DQC1. We also use the language of Topological Quantum Field Theories (or TQFTs) to outline the mathematical underpinnings of the relationship between approximating

[3] Technically, we are always dealing with the decision versions of these problems.

the Jones polynomial of the plat and trace closures, and approximating the Turaev-Viro invariant of Heegaard splittings and mapping tori.

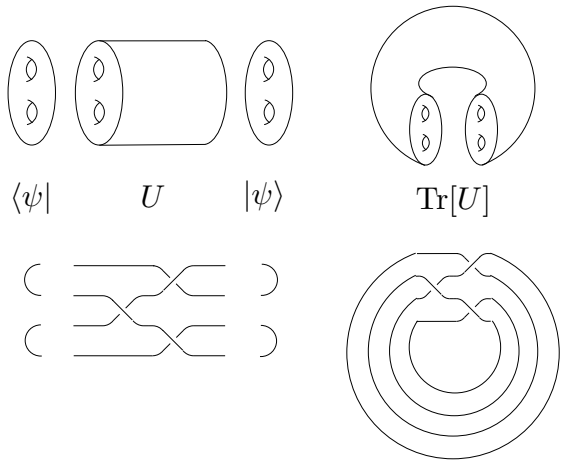

Fig. 1. Left, bottom to top: the BQP-complete problems of estimating *(i.)* the Jones polynomial of the plat closure of a braid, *(ii.)* the matrix entry of a unitary operator U, and *(iii.)* the Turaev-Viro invariant of a Heegaard splitting. **Right, bottom to top:** the DQC1-complete problems of estimating *(i.)* the Jones polynomial of the trace closure of a braid, *(ii.)* the trace of a unitary operator U, and *(iii.)* the Turaev-Viro invariant of a mapping torus. These situations are fundamentally analogous. Note: the 3-manifolds are drawn only as illustrations, not two-dimensional projections of the 3-manifolds themselves; in particular, after gluing (along the handlebody boundaries, as shown) the 3-manifolds do not in reality have a boundary at all.

References

1. Dorit Aharonov, Vaughan Jones, and Zeph Landau. A polynomial quantum algorithm for approximating the Jones polynomial. *STOC 06*, 2006. arXiv:quant-ph/0511096.
2. Gorjan Alagic, Stephen Jordan, Robert König, and Ben Reichardt. Approximating turaev-viro 3-manifold invariants is universal for quantum computation. *Physical Review A*, 82:040302(R), 2010. arXiv:1003.0923.
3. Michael Freedman, Michael Larsen, and Zhenghan Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, 227:605, 2002. arXiv:quant-ph/0001108.
4. E. Knill and R. Laflamme. Power of one bit of quantum information. *Physical Review Letters*, 81(25):5672–5675, 1998. arXiv:quant-ph/9802037.
5. Peter W. Shor and Stephen P. Jordan. Estimating Jones polynomials is complete for one clean qubit. *Quantum Information and Computation*, 8(8/9):681–714, 2008. arXiv:0707.2831.

Long distance quantum key distribution with continuous variables

Anthony Leverrier[1,2] and Philippe Grangier[3]

[1] ICFO-Institut de Ciencès Fotòniques,
Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
[2] Institut Telecom / Telecom ParisTech, CNRS LTCI,
46, rue Barrault, 75634 Paris Cedex 13, France
[3] Laboratoire Charles Fabry, Institut d'Optique, CNRS, Univ. Paris-Sud,
Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France

Quantum key distribution (QKD) is a cryptographic primitive allowing two distant parties, Alice and Bob, to establish a secret key in an untrusted environment controlled by some eavesdropper, Eve [1]. One of the great interests of QKD is that it can be implemented with present day technology, at least for reasonable distances.

Whereas discrete-variable protocols are quite resistant to losses, continuous-variable (CV) protocols do not seem to display the same quality: the present experimental record is around 25 km [2, 3]. The main limitation in terms of range for CV QKD stems from the finite reconciliation efficiency, especially for a Gaussian modulation in the low signal-to-noise ratio (SNR) regime.

Here, we introduce a new continuous-variable QKD protocol using a continuous but non-Gaussian modulation, allowing for an efficient reconciliation scheme and thus for improved performances. More precisely, the modulation we consider crucially uses algebraic properties of the octonions, which can be seen as points on the unit sphere in $\mathbb{R}^8$.

In this protocol, Alice sends $4N$ coherent states to Bob such that the coordinates of all quadruples $\{|\alpha_{4k}\rangle, |\alpha_{4k+1}\rangle, |\alpha_{4k+2}\rangle, |\alpha_{4k+3}\rangle\}$ for $k \in \{1, \cdots, N\}$ are drawn with the uniform probability on the seven-dimensional sphere of radius 2α in phase space:

$$\mathcal{S}^7 \equiv \{(\alpha_{4k}, \alpha_{4k+1}, \alpha_{4k+2}, \alpha_{4k+3}) \in \mathbb{C}^4 \quad \text{such} \quad \text{that} \\ |\alpha_{4k}|^2 + |\alpha_{4k+1}|^2 + |\alpha_{4k+2}|^2 + |\alpha_{4k+3}|^2 = 4\alpha^2\}, \quad (1)$$

where Alice's modulation variance is $2\alpha^2$ (in shot noise units). Bob then proceeds with an *heterodyne measurement* (as in Ref. [4] for instance). Here, it is crucial that both quadratures are measured in order to use the property of Eq. 1. The rest of the protocol consists of an estimation step, a reconciliation step (which combines techniques introduced in [5] and [6]) and finally a privacy amplification procedure.

We establish the security of this protocol against collective attacks, *provided that the quantum channel is linear*. This can be done by using extremality properties of Gaussian states [7] in order to upper-bound Eve's information. An important question at that stage is how to avoid the extra hypothesis that the channel should be linear. A possible solution consists in introducing decoy states in order to embed the non-Gaussian modulation into an overall Gaussian modulation [8].

Acknowledgments

We acknowledge support from the European Union under project SECOQC (IST-2002-506813) and the ERC Starting grant PERCENT, and from Agence Nationale de la Recherche under projects PROSPIQ (ANR-06-NANO-041-05) and SEQURE (ANR-07-SESU-011-01).

References

1. Valerio Scarani et al. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301, 2009.
2. Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76(4), 2007.
3. Quyen Dinh Xuan, Zheshen Zhang, and Paul L. Voss. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express*, 17(26):24244–24249, 2009.
4. Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93(17):170504, Oct 2004.
5. Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 77(4):042325, 2008.
6. Anthony Leverrier and Philippe Grangier. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.*, 102(18):180504, 2009.
7. Raúl García-Patrón and Nicolas J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.*, 97(19):190503, 2006.
8. Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A*, 83(4):042312, Apr 2011.

Quantum discord in quantum information theory - From strong subadditivity to the Mother protocol

Vaibhav Madhok[1] and Animesh Datta[2]

[1] Center for Quantum Information and Control, University of New Mexico, Albuquerque, NM 87131-0001, USA

[2] Clarendon Laboratory, Department of Physics, University of Oxford, OX1 3PU, United Kingdom

There exist instances of computations involving mixed quantum states where the quantum advantages over the best known classical algorithm cannot be ascribed to quantum entanglement. For such a scenario, quantum discord [1–3] has been proposed as the resource behind the quantum speedup [4]. Since then, quantum discord has been studied in a variety of settings, and shown to be of relevance in dynamics of open quantum systems and quantum phase transitions. It has also been used to explain the performance of quantum and classical Maxwell demons. However, there has been a lack of interpretation of quantum discord as a resource in the information theoretic sense. This requires the identification of an information processing task which is made easier by the presence of discord, or more expensive the lack it. Such a task has recently been identified, in terms of quantum state merging [5, 6]. In this work, we present a more general, and fundamental role played by quantum discord in quantum information processing.

One of our main results is a connection between quantum discord and the strong subadditivity of von Neumann entropy. Strong subadditivity of entropy is one of the most vital and powerful expressions in information theory [7]. It is therefore interesting in its own right to prove that the strong subadditivity of the Von Neumann entropy implies nonnegativity of the quantum discord. We use this result to revisit the connection between quantum discord and quantum state merging [5]. We provide an intuitive understanding of how quantum discord is the markup in the cost of state merging [8] when one of the parties in subjected to measurements.

Our second main result gives an operational interpretation of quantum discord by establishing its role in an important class of quantum information protocols. To that end, we show that quantum discord measures how coherently one performs the Mother protocol [9], and its generalization as the FQSW (Fully quantum Slepian Wolf) protocol, in the presence of decoherence. The Mother protocol can be viewed as an entanglement distillation between two parties, A and B, when the only type of communication permitted is the ability to send

qubits from A to B. It is the unification of an important class of quantum information protocols, those that are bipartite, unidirectional and memoryless.

The Mother protocol has as its children several protocols that are well known, such as quantum teleportation, entanglement distillation, superdense coding [10]. Our results allow us to study the behaviour of these protocols in the presence of measurements or decoherence on one of the subsystems. Our results thus show that quantum discord is one of the quantities that certifies the performance of almost all quantum protocols.

Acknowledgements

This work was supported in part by the EPSRC (Grant No. EP/H03031X/1), the EU Integrated Project (QESSENCE), the Center for Quantum Information and Control (CQuIC) at UNM, and NSF Grant Nos. 0903953 and 0903692.

References

1. W. H. Zurek, Annalen der Physik (Leipzig), **9**, 855 (2000).
2. H. Ollivier and W. H. Zurek, Phys. Rev. Lett., **88**, 017901 (2002).
3. L. Henderson and V. Vedral, J. Phys. A: Math. Gen., **34**, 6899 (2001).
4. A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett, **100**, 050502 (2008).
5. V. Madhok and A. Datta, Phys. Rev. A, **83** , 032323 (2011).
6. D. Cavalcanti. L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter, **83** , 032324 (2011).
7. E. H. Lieb and M. B. Ruskai, J. Math. Phys. **12**, 1938 (1973).
8. M. Horodecki, J. Oppenheim, and A. Winter, Nature, **436**, 673 (2005); M. Horodecki, J. Oppenheim, and A. Winter, Comm. Math. Phys., **268**, 107 (2007).
9. A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, Proc. R. Soc. A **465**, 2537, (2009).
10. I. Devetak, A.W. Harrow, and A. Winter, IEEE Trans. Inf. Th., **54**, 4587, (2008).

Information-theoretic approach to the study of symmetric dynamics

Iman Marvian[1,2] and Robert W. Spekkens[2]

[1] Perimeter Institute for Theoretical Physics, Waterloo, Canada
[2] Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

Finding the consequences of symmetries in dynamics is a subject with broad applications in physics, from the smallest scales in high energy scattering experiments, to the largest scales in astrophysical observations. In many cases the dynamics is sufficiently complicated that one cannot find its exact characterization and one must rely heavily on a consideration of the symmetries. Perhaps the most prominent and powerful example of the consequences of symmetry is the existence of conservation laws for closed systems. We are interested to find tools to study the consequences of symmetry which apply to open as well as closed quantum systems.

We say a time evolution described by the quantum channel $\mathcal{E}$ respects the symmetry G or is *G-covariant* if $\forall g \in G: \quad \mathcal{E} \circ \mathcal{U}(g) = \mathcal{U}(g) \circ \mathcal{E}$ where $\mathcal{U}(g)[\rho] \equiv U(g)\rho\, U^\dagger(g)$ and $\{U(g) : g \in G\}$ is the unitary representation of the group on the Hilbert space. If there is a G-covariant channel under which ρ evolves to σ we write $\rho \xrightarrow{G-cov} \sigma$. The central question we wish to answer is the following: For any given ρ and σ is $\rho \xrightarrow{G-cov} \sigma$ possible or not? The relevant properties of a state which specify whether the transformation $\rho \xrightarrow{G-cov} \sigma$ is possible or not can be called *the asymmetry properties* of that state. More precisely, τ_1 and τ_2 have exactly the same *asymmetry properties* or are *G-equivalent* if both $\tau_1 \xrightarrow{G-cov} \tau_2$ and $\tau_2 \xrightarrow{G-cov} \tau_1$ exist. Then to answer the question of whether $\rho \xrightarrow{G-cov} \sigma$ is possible or not we only need to know the equivalence classes of ρ and σ; all other information about ρ and σ are useless. It turns out that for the case of pure states we can find a simple characterization of the G-equivalence classes of states.

An asymmetry measure quantifies how much the symmetry is broken by a given state. The defining property of an asymmetry measure is that it be non-increasing under G-covariant time evolutions. In other words a function γ from states to real numbers is an asymmetry measure if $\rho \xrightarrow{G-cov} \sigma$ implies $\gamma(\rho) \geq \gamma(\sigma)$. Therefore any asymmetry measure puts a necessary condition on the possibility of $\rho \xrightarrow{G-cov} \sigma$. Note that an asymmetry measure should have the same value for all states which are G-

equivalent and therefore it can only depends on the G-equivalence classes of states.

But how can we find nontrivial asymmetry measures? In the case of rotational symmetry one might expect that the (absolute value of the expectation value of) components of angular momentums are asymmetry measures. However, it turns out that this is not true and angular momentum can be amplified.

To find a recipe for finding asymmetry measures we introduce a different point of view for thinking about asymmetry which is not based on symmetric dynamics; instead it is based on the intuition that a state which breaks symmetry can be thought as a signal which carries information about the group element. In other words, to study the asymmetry properties of state ρ relative to the group G, we think of the set $\{\mathcal{U}(g)[\rho] : g \in G\}$ as an encoding of G that is, the element $g \in G$ is encoded in $\mathcal{U}(g)[\rho]$. Now one can show that G-equivalence classes of states can be defined in terms of the interconvertability of the encodings introduced by the states.

Using this point of view to asymmetry we can use information measures to build asymmetry measures. In particular using the Holveo quantity as an information measure we can easily see that for arbitrary probability distribution $p(g)$ over the symmetry group G, the quantity

$$\gamma_p(\rho) \equiv S\left(\int dg\ p(g)\mathcal{U}(g)[\rho]\right) - S(\rho)$$

is an asymmetry measure, i.e. if $\rho \xrightarrow{G-cov} \sigma$ then $\gamma_p(\rho) \geq \gamma_p(\sigma)$

All asymmetry measures are constants of the motion in the case of closed system symmetric time evolutions. On the other hand, in the case of closed systems we can also use Noether's theorem to derive the consequences of symmetry. Now the question is: does the conservation of asymmetry measures imply constraints that are not implied by Noether's theorem? Interestingly, the answer is different for the case of pure and mixed states. We show that for pure states Noether's theorem includes all the possible implications of the symmetry of dynamics. We show this by proving that if $\langle\psi|U(g)|\psi\rangle = \langle\phi|U(g)|\phi\rangle$ then there exists a G-covariant closed system dynamics which transforms $|\psi\rangle$ to $|\phi\rangle$. On the other hand, we present a simple example which shows that in the case of mixed states conservation of asymmetry measures imply more constraints than those prescribed by Noether's theorem.

Secure device-independent quantum key distribution with causally independent measurement devices

Lluís Masanes[1], Stefano Pironio[2], and Antonio Acín[1,3]

[1] ICFO–Institut de Ciències Fotòniques, E–08860 Castelldefels, Barcelona, Spain
[2] Laboratoire d'Infomation Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium
[3] ICREA–Institució Catalana de Recerca i Estudis Avançats, E–08010 Barcelona, Spain

Abstract. Device-independent quantum key distribution aims to provide key distribution schemes whose security is based on the laws of quantum physics but which does not require any assumptions about the internal working of the quantum devices used in the protocol. This strong form of security, unattainable with standard schemes, is possible only when using correlations that violate a Bell inequality. We provide a general security proof valid for a large class of device-independent quantum key distribution protocols in a model in which the raw key elements are generated by causally independent measurement processes. The validity of this independence condition may be justifiable in a variety of implementations and is necessarily satisfied in a physical realization where the raw key is generated by N separate pairs of devices. Our work shows that device-independent quantum key distribution is possible with key rates comparable to those of standard schemes.

Self-testing graph states

Matthew McKague

Centre for Quantum Technologies, National University of Singapore

Self-testing was introduced by Mayers and Yao in [3], with later developments in [2], [5] and [4]. The goal of self-testing is to verify the operation of a group of non-communicating quantum devices using only classical interaction with the devices and without trusting any of them *a priori*. A self-test, then, is simply a protocol for doing so. In this article we describe two different self-tests which verify that a group of devices share a graph state and implement Pauli X and Z measurements on this state.

Theorem 1. *Let G be a connected graph with an odd cycle. Then there exists a self-test for the graph state $|G\rangle$ with $|V(G)|+1$ measurement settings. Furthermore, this test is robust.*

The measurement settings for this test correspond to the standard stabilizer generators for $|G\rangle$ along with one other stabilizer defined by the odd cycle.

Theorem 2. *Let G be any connected graph. Then there exists a self-test for the graph state $|G\rangle$ with $|V(G)|+3$ measurement settings. Furthermore, this test is robust.*

For this test the measurement settings are again derived from the standard stabilizer generators for $|G\rangle$ along with three additional measurements which are similar to those used in the Mayers-Yao test for EPR pairs [3].

These self-tests can be reinterpreted as Bell inequalities which have a unique strategy that achieves the quantum bound. The self-tests are also interesting from the point of view of computation since graph states, along with certain measurements, are universal for quantum computation. This opens the door for a type of interactive proof with efficient quantum provers, similar to that achieved by Broadbent et al. [1].

References

1. A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *FOCS 2009*.
2. F. Magniez, D. Mayers, M. Mosca, and H. Ollivier. Self-testing of quantum circuits. In *ICALP 2006*.
3. D. Mayers and A. Yao. Self testing quantum apparatus. *QIC*, 4(4):273–286, July 2004.
4. M. McKague. *Quantum Information Processing with Adversarial Devices*. PhD thesis, University of Waterloo, June 2010.
5. M. McKague and M. Mosca. Generalized self-testing and the security of the 6-state protocol. *TQC 2010*.

Multi-query quantum sums

David A. Meyer[1] and James Pommersheim[1,2]

[1] Department of Mathematics, UCSD, La Jolla, CA 92093-0112 USA
[2] Department of Mathematics, Reed College, Portland, OR 97202 USA

Extended abstract

PARITY is the oracle (or black-box) problem of determining the parity of an n-bit string by querying positions in the string. Since even a single unqueried bit can change the parity, n classical queries are required to solve this problem with probability 1, assuming all n-bit strings are possible.

When $n = 2$, this is Deutsch's problem [6], for which a single quantum query, used properly, suffices [4]. Beals, *et al.*, show that in general $\lceil n/2 \rceil$ quantum queries suffice by applying the solution to Deutsch's problem to the bits in pairs [2]. In their algorithm the quantum queries are *independent* of one another—they can be asked in parallel since none depends on the responses of the oracle to the others—and the measurements are also *independent*—after each query is processed, the state is measured and the resulting information (the parity of a pair of the bits) is combined classically at the end of the algorithm.

This same independence of multiple queries is a feature of existing multi-query quantum algorithms for abelian and non-abelian hidden subgroup problems (see [10] for a survey); although while in the former case the measurements can be independent [12], for many of the latter *joint* or *entangled* measurements are necessary to obtain more than an exponentially small amount of information [8]. Grover's quantum search algorithm [7], and quantum (random walk) search algorithms on graphs [11, 1] more generally, however, utilize coherent sequences of *adapted* queries—the quantum state is modified by each oracle response before it is returned to the oracle for the next query, so the queries are not independent. These algorithms all use *amplitude amplification* [3] to adapt their sequential queries.

But amplitude amplification, which identifies an element in the preimage of 1 for some bit-valued function, does not apply to PARITY, nor to its generalization:

SUM. Let $f : \mathbb{Z}_n \to \mathbb{Z}_k$, where f is accessed *via* an oracle that responds with $f(x)$ when queried about $x \in \mathbb{Z}_n$. Find $\sum_{x\in\mathbb{Z}_n} f(x)$.

Inspired by our prior results on the *uselessness* of $\lfloor (n-1)/2 \rfloor$ quantum queries for SUM when f is chosen uniformly at random [9], we construct an $n-r$ quantum query algorithm that computes the sum correctly with probability $\min\{\lfloor n/r \rfloor/k, 1\}$, for each $1 \leq r \in \mathbb{N}$. This quantum algorithm utilizes the $n-r$ queries sequentially and adaptively, like quantum search algorithms, but in a different way that is not amplitude amplification.

We motivate the development of our algorithm by considering the simplest new instances of SUM—computing the sum of two or three trits—and then construct the algorithm for the general problem. We conclude by recalling the result of van Dam that strings of n bits can be identified with high probability using $n/2 + O(\sqrt{n})$ queries, and hence any function of them can be computed with the same probability [5]. We generalize this result to $k > 2$ and show that it gives success probabilities less than those of our algorithm.

References

1. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. In: Proceedings of FOCS'03. pp. 200–209. IEEE, Los Alamitos, CA (2003)
2. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM 48, 778–797 (2001)
3. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. In: Lomonaco, Jr., S.J., Brandt, H.E. (eds.) Quantum Computation and Information, Contemporary Mathematics, vol. 305, pp. 53–74. AMS, Providence, RI (2002)
4. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Quantum algorithms revisited. Proc. Roy. Soc. London A 454, 339–354 (1998)
5. van Dam, W.: Quantum oracle interrogation: getting all information for almost half the price. In: Proceedings of FOCS'98. pp. 362–367. IEEE, Los Alamitos, CA (1998)
6. Deutsch, D.: Quantum theory, the church-turing principle and the universal quantum computer. Proc. Roy. Soc. London A 400, 97–117 (1985)
7. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of STOC'96. pp. 212–219. ACM, New York (1996)
8. Hallgren, S., Moore, C., Rötteler, M., Russell, A., Sen, P.: Limitations of quantum coset states for graph isomorphism. In: Proceedings of STOC'06. pp. 604–617. ACM, New York (2006)
9. Meyer, D.A., Pommersheim, J.: On the uselessness of quantum queries. Theoretical Computer Science (to appear)
10. Mosca, M.: Quantum algorithms. In: Meyers, R.A. (ed.) Encyclopedia of Complexity and Systems Science, pp. 7088–7118. Springer, New York (2009)
11. Shenvi, N., Kempe, J., Whaley, K.B.: Quantum random walk search algorithm. Phys. Rev. A 67, 052307/1–11 (2003)
12. Simon, D.R.: On the power of quantum computation. In: Goldwasser, S. (ed.) Proceedings of FOCS'94. pp. 116–123. IEEE, Los Alamitos, CA (1994)

Which graph states are useful for quantum information processing?

Mehdi Mhalla[1], Mio Murao[2,3], Simon Perdrix[1], Masato Someya[2], and Peter S. Turner[2] ⋆

[1] CNRS, LIG, Université de Grenoble, France
[2] Graduate School of Science, The University of Tokyo, Japan
[3] NanoQuine, The University of Tokyo, Japan

The graph state formalism [3] is an elegant and powerful formalism for quantum information processing. Graph states form a subfamily of the stabiliser states [2]. They provide a graphical description of entangled states and they have multiple applications in quantum information processing, in particular in measurement-based quantum computation (MBQC) [7], but also in quantum error correcting codes [2] and in quantum protocols like secret sharing [5, 4]. They offer a combinatorial approach to the characterisation of the fundamental properties of entangled states in quantum information processing. The invariance of the entanglement by local complementation of a graph [8]; the use of measure of entanglement based on the rank-width of a graph [9]; and the combinatorial *flow* characterisation [1] of deterministic evolutions in measurement-based quantum computation witness the import role of the graph state formalism in quantum information processing.

We focus on the application of graph states in MBQC and in particular on the characterisation of graphs that can be used to perform quantum information processing in this context. The existence of a graphical condition which guarantees that a deterministic MBQC evolution can be driven despite of the probabilistic behaviour of the measurements is a central point in MBQC. It has already been proven that the existence of a certain kind of flow called glfow characterises uniformly stepwise determinism [1] and that finding a gflow can be done in polynomial time [6]. We introduce a simpler but equivalent combinatorial characterisation using *focused gflow* and we provide a simple condition of existence of such a flow as the existence of a right inverse to the adjacency matrix of the graph. We also prove additional properties in the case where the number of input and output qubits of the computation are the same: the gflow

⋆ The authors want to thank E. Kashefi for discussions. This work supported by the CNRS-JST Strategic French-Japanese Cooperative Program, and Special Coordination Funds for Promoting Science and Technology in Japan. This work is also partially supported by the ANR JCJC 020801 *CausaQ*.

is then reversible and the stepwise condition [1] on determinism is not required to guarantee the existence of a gflow.

The main contribution of this work is the weakening of the determinism condition in order to consider the more general class of *information preserving* evolutions. Being information preserving is one of the most fundamental property that can be required for a MBQC computation. Indeed, some non-deterministic evolutions can be information preserving when one knows the classical outcomes of the measurements produced by the computation. Such evolutions are called *equi-probabilistic* – when each classical outcome occurs with probability $1/2$ – or *constant-probabilistic* in the general case. We introduce simple combinatorial conditions for equi-probabilistic and constant-probabilistic MBQC by means of excluded violating sets of vertices. We show, in the particular case where the number of input and output qubits are the same, that graphs guaranteeing equi-probabilism and determinism are the same. Using this graphical characterisation, we address the fundamental question of finding input and output vertices in an arbitrary graph for guaranteeing an equi-probabilistic (or deterministic) evolution. To this end, we show that the input and output vertices of a graph must form transversals of the violating sets induced by the equi-probabilistic characterisation. Finally, we investigate several properties of the most general and less understood class of constant probabilistic evolutions.

References

1. D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. *Generalized flow and determinism in measurement-based quantum computation. New J. Phys.* **9**, 250, 2007.
2. D. Gottesman, *Stabilizer Codes and Quantum Error Correction. Ph.D. thesis*, California Institute of Technology, Pasadena, CA, 1997.
3. M. Hein, J. Eisert, and H. J. Briegel. *Multi-party entanglement in graph states. Phys. Rev. A* **69**, 062311, 2004.
4. E. Kashefi, D. Markham, M. Mhalla and S. Perdrix. *Information Flow in Secret Sharing Protocols. Developments in Computational Models (DCM'09), EPTCS 9, pp. 87-97, 2009*
5. D. Markham and B. C. Sanders. *Graph states for quantum secret sharing. Phys. Rev. A* **78**, 042309, 2008.
6. M. Mhalla, and S. Perdrix. *Finding optimal flows efficiently. ICALP proceeding Track A*, LNCS, 2008.
7. R. Raussendorf and H. Briegel. *A one-way quantum computer. Phys. Rev. Lett.* **86**, 5188, 2001.
8. M. Van den Nest, J. Dehaene, and B. De Moor. *Graphical description of the action of local Clifford transformations on graph states. Phys. Rev. A* **69**, 22316, 2004.
9. M. Van den Nest, A. Miyake, W. Dür, and H.J. Briegel. *Universal resources for measurement-based quantum computation. Phys. Rev. Lett.* **97**, 150504, 2006.

Span-program-based quantum algorithm for evaluating unbalanced formulas

Ben W. Reichardt

Institute for Quantum Computing, University of Waterloo.

The formula-evaluation problem is defined recursively. A formula's evaluation is the evaluation of a gate, the inputs of which are themselves independent formulas. Despite this pure recursive structure, the problem is combinatorially difficult for classical computers. We give a quantum algorithm to evaluate formulas over any finite boolean gate set. Provided that the general adversary bound complexities of the input subformulas to any gate differ by at most a constant factor, the algorithm has optimal query complexity. Importantly, after efficient preprocessing, the algorithm is nearly *time* optimal. The algorithm is derived using the framework relating span programs and quantum algorithms from [1]. It corresponds to the composition of the individual span programs for each gate in the formula. Thus the algorithm's structure reflects the formula's recursive structure.

Previous work has used span programs to develop optimal quantum algorithms for evaluating formulas, provided that every gate's input subformulas have *exactly* equal general adversary bounds [2]. In order to relax this strict balance requirement, we must maintain better control in the recursive analysis. To help do so, we define a new span program complexity measure, the "full witness size." This complexity measure has implications for developing time- and query-efficient quantum algorithms based on span programs. Essentially, it allows quantum algorithms to be based on span programs with free inputs, which can simplify implementations.

Besides relaxing the balance requirement, our approach additionally makes the hidden constants in [2] more explicit, allowing a bound that is exponential in the maximum fan-in of a gate.

Our algorithm runs a quantum walk on a graph corresponding to a span program for the formula. For this approach to work, a bound is needed on the operator norm of the entry-wise absolute value of the weighted adjacency matrix of the graph. Further graph sparsity conditions are needed for the algorithm to be time efficient. Unfortunately, optimal span programs typically correspond to dense graphs with large norms.

An example should clarify the problem. Consider the AND-OR formula $\psi(x) = \big([(x_1 \wedge x_2) \vee x_3] \wedge x_4\big) \vee \big(x_5 \wedge [x_6 \vee x_7]\big)$, and consider the two graphs in Figure 1. For an input $x \in \{0,1\}^7$, modify the graphs by attaching dangling edges to every vertex j for which $x_j = 0$. Observe then that each graph has an eigenvalue-zero eigenvector supported on vertex 0—called a *witness*—if and only if $\psi(x) = 1$. The graphs correspond to different span programs computing ψ, and the quantum algorithm works essentially by running a quantum walk starting at vertex 0 in order to detect the witness. The graph on the left is a significantly simplified version of a canonical span program for ψ, and its density still makes it difficult to implement the quantum walk.

We will be guided by the second, simpler graph. We find optimal span programs for every gate in the formula, then compose them according to the formula using *direct-sum composition*. In terms of graphs, direct-sum composition attaches the output vertex of one span program's graph to an input vertex of the next [2]. This leads to a graph whose structure somewhat follows the structure of the formula φ, as the graph in Figure 1(b) follows the structure of ψ.

Direct-sum composition keeps the maximum degree and norm of the graph under control—each is at most twice its value for the worst single gate. However, direct-sum composition also

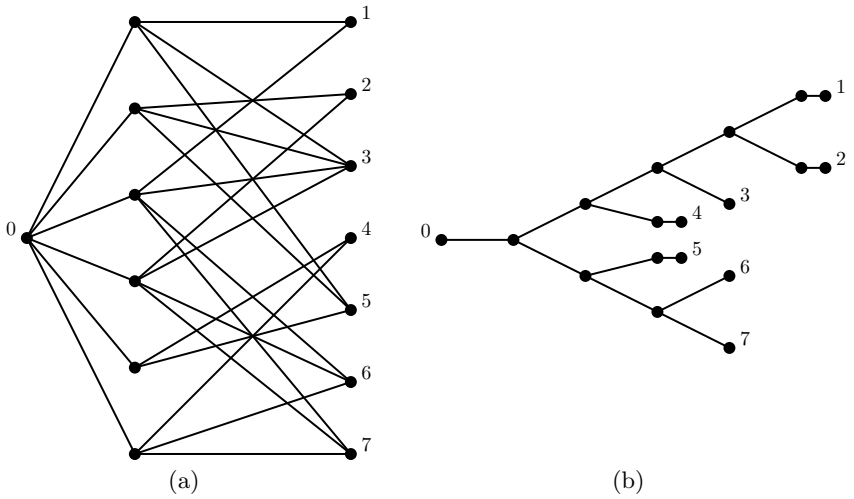

Fig. 1: Graphs corresponding to two span programs both computing the same function.

leads to additional overhead. In particular, a witness in the first graph will be supported only on numbered vertices, whereas a witness in the second graph will be supported on some of the internal vertices as well. This means roughly that the second witness will be harder to detect, because after normalization its overlap on vertex 0 will be smaller. Scale both witnesses so that the amplitude on vertex 0 is one. The *witness size* measures the squared length of the witness only on numbered vertices, whereas the *full witness size* measures the squared length on all vertices. In our analysis, we bound the full witness size in terms of the witness size, based on a recursion using the balance condition.

References

1. Ben W. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function. 2009, arXiv:0904.2759 [quant-ph], Extended abstract in *Proc. 50th IEEE FOCS*, pages 544–551, 2009.
2. Ben W. Reichardt and Robert Špalek. Span-program-based quantum algorithm for evaluating formulas. In *Proc. 40th ACM STOC*, pages 103–112, 2008, arXiv:0710.2630 [quant-ph].

Mistrustful Quantum Cryptography in a Device-Independent Setting

J. Silman[1], A. Chailloux[2], N. Aharon[3], I. Kerenidis[4], S. Pironio[1], and S. Massar[1]

[1] Laboratoire d'Information Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium
[2] LIAFA, Univ. Paris 7, F-75205 Paris, France & Univ. Paris-Sud, 91405 Orsay, France
[3] School of Physics and Astronomy, Tel-Aviv University, Tel-Aviv 69978, Israel
[4] LIAFA, Univ. Paris 7 - CNRS; F-75205 Paris France & Centre for Quantum Technologies, National University of Singapore, Singapore 117543

Abstract. Device-independent cryptographic protocols are by definition more secure than their device-dependent counterparts, since they do not rely on any assumptions regarding the internal workings of the apparatus used to implement them. Thus far, the device-independent approach has been successfully applied to problems such as quantum-key distribution and randomness generation, but it is not a priori clear whether it can be applied to protocols in the mistrustful cryptography class, where, as opposed to the examples mentioned above, the parties do not trust one another. In this work we show that for bit-commitment and coin flipping a device-independent treatment is possible.

The security of quantum cryptographic protocols often relies on assumptions that in practice may be hard to verify, such as, for example, the dimension of the Hilbert space of the system. For this reason, one would like to base security on a minimal set of assumptions, whose validity can in principle be checked [1]. For some quantum cryptographic protocols, such as quantum key-distribution [2, 3] and randomness generation [4, 5], it turns out that security can be based on nonlocality without any need to specify the internal workings of the apparatus used to implement the protocol. Such protocols are said to be device-independent. Yet, protocols in the mistrustful cryptography class, such as bit-commitment and oblivious transfer, have yet to receive a device-independent treatment. Indeed, it is not a priori clear that they are amenable to such a treatment, since in contrast to the examples mentioned above, where the parties taking part in the protocol trust each other and collaborate to estimate the degree of violation of some suitable Bell inequality, the different parties taking part in a mistrustful cryptographic protocol do not trust one another.

In this work we show that for bit-commitment and coin flipping a device-independent formulation is possible. Bit commitment is defined as the problem where a party must commit to a bit such that after the commitment stage he is unable to alter its value and the recipient is unable to learn it until the committing party chooses to reveal it, while coin flipping is defined as the problem of two remote parties having to agree on the value of a random bit. Specifically, we present a device-independent bit-commitment protocol, and then use it to construct a device-independent coin flipping protocol. In the bit-commitment protocol, the committing party can cheat with a probability of $\simeq 0.854$ and the recipient of the commitment, with a probability of 0.75, as compared to the optimal $\simeq 0.739$ [6] in the (balanced) device-dependent case. Whereas in the coin flipping protocol, a dishonest party can cheat with a probability of at most $\simeq 0.836$ as compared to $\simeq 0.707$ [7, 8] in the device-dependent case. (Classically, if no limitations are put on the computational power available, a dishonest party can cheat perfectly.)

Our protocols are not mere adaptations of existing device-independent techniques and include novel features. For one, our bit-commitment protocol is single shot and does not call for any statistical estimates to be made on the degree of violation of some Bell inequality. More specifically, the protocol is based on the GHZ paradox [9, 10], but at no point is any of the parties required to check its satisfaction. Indeed, Alice's security relies on the no-signaling principle, while Bob's is determined by Tsirelson's bound [11]; the GHZ paradox only serves to ensure that the protocol works when both parties are honest.

References

1. D. Mayers and A. Yao, Quantum Inform. Comput. 4, 273 (2004).
2. J. Barrett et al., Phys. Rev. Lett. 95, 010503 (2005).
3. A. Acín et al., Phys. Rev. Lett. 98, 230501 (2007).
4. R. Colbeck, PhD dissertation, Cambridge University (2007), arXiv:0911.3814.
5. S. Pironio et al., Nature 464, 1021 (2010).
6. A. Chailloux and I. Kerenidis, arXiv:1102.1678.
7. A. Kitaev, unpublished. Proof reproduced in A. Ambainis et al., in Proceedings of the 19th Annual IEEE Conference on Computational Complexity, (CS Press, 2004), p. 250.
8. A. Chailloux and I. Kerenidis, in Proceedings of the 50th Annual IEEE Symposium on the Foundations of Computer Science, (CS Press, 2009), p. 527.
9. D.M. Greenberger et al., in Bell's Theorem, Quantum Theory, and Conceptions of the Universe, edited by M. Kafatos (Kluwer, 1989), p. 74.
10. N.D. Mermin, Phys. Today 43, 9 (1990).
11. B.S. Cirel'son, Lett. Math. Phys. 4, 93 (1980).

Tight Finite-Key Analysis for Quantum Cryptography

Marco Tomamichel[1], Charles Lim[2], Nicolas Gisin[2], and Renato Renner[1]

[1] Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
[2] Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland

Quantum Key Distribution (QKD), invented by Bennett and Brassard [1] and Ekert [2] can be considered the first application of quantum information science. Accordingly, QKD has been an object of intensive study over the past few years. On the theory side, the security of various variants of QKD protocols against general attacks has been shown. At the same time, experimental techniques have reached a state of development that enables efficient key distribution over large distances. Despite these developments, there is still a large gap between theory and practice, in the sense that the security claims are based on assumptions that are not (or cannot be) met by experimental implementations. For example, the proofs often rely on theoretical models of the devices (such as photon sources and detectors) that do not take into account experimentally unavoidable imperfections.

In this contribution, we focus on the assumption that an arbitrarily large number M of signals can be exchanged between the legitimate parties (Alice and Bob) and subsequently used for the computation of the final key. This assumption is quite common in the literature, and security proofs are usually only valid asymptotically as M tends to infinity. However, in practical realizations, the key is often computed from a relatively small number of signals ($M \ll 10^6$). This problem has recently received increased attention and explicit bounds on the number of signals required to guarantee security have been derived (cf. [3–7]).

Here, we apply a novel proof technique [8] to the BB84 QKD protocol [1] and derive almost tight bounds on the minimum value M required to achieve a given level of security. The technique is based on a formulation of the uncertainty relation in terms of smooth entropies [8]. The smooth min-entropy, $H_{\min}^{\varepsilon}(\boldsymbol{X}|E)$, characterizes the amount of key — secret from a potential eavesdropper, E — that can be extracted from a binary string of data bits Alice encoded in the computational basis, $\boldsymbol{X}$. [9] Compared to preexisting methods, our approach via the uncertainty relation allows a rather direct evaluation of the smooth min-entropy, i.e., we have $H_{\min}^{\varepsilon}(\boldsymbol{X}|E) \geq n - H_{\max}^{\varepsilon}(\boldsymbol{Z}|\hat{\boldsymbol{Z}})$, where n is the length of $\boldsymbol{X}$ and $H_{\max}^{\varepsilon}(\boldsymbol{Z}|\hat{\boldsymbol{Z}})$

characterizes the amount of correlation between a test string containing bits Alice prepared in the diagonal basis and Bob's estimate of that string. This yields a bound on the extractable key length, ℓ, for ϵ-secure and composable protocols (see [10] for a complete derivation and precise security defintions):

$$\ell \leq n\big(1 - h(Q_{\text{tol}} + \mu)\big) - 3\log(3/\epsilon) - \text{leak}_{\text{EC}}\,, \tag{1}$$

where $\mu \approx \sqrt{1/k \cdot \ln(1/\epsilon)}$ is the statistical deviation from the tolerated channel noise, Q_{tol}, and k is the number of test bits used for statistics. Finally, $\text{leak}_{\text{EC}} \approx nh(Q_{\text{tol}})$ is the information about the key leaked during error correction. The achievable key rate, ℓ/M, deviates from its optimal asymptotic value, $1-2h(Q_{\text{tol}})$, only by (probably unavoidable) terms due to finite statistics.

We demonstrate significant improvements of the finite-key rate over existing results. Positive key rates can now be achieved with block sizes of $n = 10^4 - 10^5$ that correspond to current hardware limitations. Moreover, our security analysis is valid against the most general attacks and robust against device imperfections in the prepare-and-measure setting.

References

1. C. H. Bennett and G. Brassard. In *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pages 175–179, Bangalore, 1984.
2. Artur K. Ekert. *Phys. Rev. Lett.*, 67(6):661–663, August 1991.
3. Masahito Hayashi. *Phys. Rev. A*, 74(2):022307, 2006.
4. H. Inamori, Norbert Lütkenhaus, and Dominic Mayers. *Eur. Phys. J. D*, 41(3):599–627, 2007.
5. V. Scarani and R. Renner. *Phys. Rev. Lett.*, 100(20):200501, 2008.
6. Sylvia Bratzik, Markus Mertz, Hermann Kampermann, and Dagmar Bruß. *Phys. Rev. A*, 83(2):022330, 2011.
7. Lana Sheridan, Thinh Phuc Le, and Valerio Scarani. *New J. Phys.*, 12:123019, 2010.
8. M. Tomamichel and R. Renner. *Phys. Rev. Lett.*, 106(11), 2011.
9. R. Renner and R. König. In *Proc. TCC*, volume 3378 of *LNCS*, pages 407–425, Cambridge, USA, 2005.
10. M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight Finite-Key Analysis for Quantum Cryptography. 2011. `arXiv:1103.4130`

Bitwise Quantum Min-Entropy Sampling and New Lower Bounds for Random Access Codes

Jürg Wullschleger

DIRO, Université de Montréal, Quebec, Canada
McGill University, Quebec, Canada

1 Introduction

Extracting uniform randomness from a long string x of length n using a two-universal hash function or an extractor may be very inefficient. Vadhan proposed in [Vad04] a more efficient method using *min-entropy sampling*, where first a small subset of length $k \ll n$ is sampled, and the randomness is extracted from this small subset. This works because with high probability, the sampled subset has almost $\frac{k}{n} \cdot t$ bits of min-entropy, if the min-entropy of the original string is at least t.

König and Renner showed in [KR07] that min-entropy sampling is also possible in the more general case where an adversary has quantum information about x. Again, with high probability the string x' will have almost $\frac{k}{n} \cdot t$ bits of quantum min-entropy. However, their result has two drawbacks: for a small error term the size of the subset k needs to be quite large, and the sampling needs to be done in blocks.

Related to these results are lower bounds for *random access codes*. This is an encoding of n classical bits into $m < n$ qubits, such that from the encoding, a randomly chosen subset of size k can be guessed with probability at least p. For the general case where $k \geq 1$, a lower bound was presented by Ben-Aroya, Regev, and de Wolf in [BARdW08]. They showed that if $m < n/2 \ln 2$, then $p \leq 2^{-\Omega(k)}$.

2 Contributions

Bitwise Sampling from Blockwise Sampling. In the first part of our work, we show that the bounds given in Corollary 6.19 and Lemma 7.2 in [KR07] also apply to the case where the sample is chosen bitwise uniformly, instead of (recursively) in blocks. The proof is fairly simple. Intuitively, we shows that any blockwise sampling can be seen as bitwise uniforms sampling where the adversary forgets part of the sampling.

This result simplifies some protocols as it may eliminate an artificial extra step where the bits have to be grouped in blocks.

A Sampling Theorem from Quantum Bit Extractors. Our second result is a new min-entropy sampling theorem using a completely different approach than [KR07]. It uses ideas by De and Vidick in [DV10] and combines them with a result by Ben-Aroya, Regev, and de Wolf [BARdW08]. Our proof combines the following facts.

– Any bit-extractor is also a quantum bit-extractor (for slightly worse parameters). This has been shown by König and Terhal in [KT08].
– Using the same approach as De and Vidick in [DV10], we show that the XOR of a randomly chosen substring of a fixed size is a bit-extractor.
– Ben-Aroya, Regev, and de Wolf showed in [BARdW08] that a bound on the guessing probability of the XOR of a randomly chosen substring implies a bound on the guessing probability of the whole string.

The combination of the above fact gives a bound on the guessing probability of a uniformly chosen substring of a fixed size. Since the conditional min-entropy is nothing else than minus the logarithm of the guessing probability, we immediately get our sampling result. It implies the following corollary.

Corollary 1. *Let a cq-state ρ_{XQ} be given, where $X \in \{0,1\}^n$. Let T be a random subset of $[n]$ of size k. If for a constant $c \in [0,1]$ we have $H_{\min}(X \mid Q)_\rho \geq cn$, then*

$$H_{\min}(X_T \mid TQ)_\rho \geq H^{-1}(c/2)/6 \cdot k - 5 \; .$$

Note that this min-entropy sampling theorem has a smaller rate than the result in [KR07]. But—besides the fact that the proof is less technical—it has the advantage that the error converges faster, which makes it preferable for smaller sample sizes and for non-smooth min-entropy sampling.

Lower Bound for Random Access Codes. Corollary 1 directly implies a lower bound for random access codes: if the string $X \in \{0,1\}^n$ is chosen uniformly and the quantum system Q has at most $m \leq (1-\varepsilon)n$ qubits, then $H_{\min}(X \mid Q) \geq \varepsilon n$. Corollary 2 follows.

Corollary 2. *For any k-out-of-n random access code where the storage is bounded by $m \leq (1-\varepsilon)n$, the success probability is at most $2^{-\Omega(k)}$.*

Acknowledgements: This work was funded by the U.K. EPSRC grant EP/E04297X/1 and the Canada-France NSERC-ANR project FREQUENCY.

References

[BARdW08] A. Ben-Aroya, O. Regev, and R. de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, 2008.

[DV10] A. De and T. Vidick. Near-optimal extractors against quantum storage. In *Proceedings of the fourty-second annual ACM symposium on Theory of computing (STOC '10)*. ACM, 2010.

[KR07] R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. Available at arXiv:0712.4291, 2007.

[KT08] R. König and B. M. Terhal. The bounded storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2), 2008.

[Vad04] S. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17:2004, 2004.

Posters

- *Unified framework for correlations in terms of local quantum observables*
  Antonio Acín, Remigiusz Augusiak, Daniel Cavalcanti, Christopher Hadley, Jaroslaw Korbicz, Maciej Lewenstein, Lluis Masanes and Marco Piani

- *Perfect quantum privacy implies nonlocality*
  Antonio Acín, Remigiusz Augusiak, Giuseppe Prettico and Daniel Cavalcanti

- *Qubit and entanglement dynamics in the presence of spin environments*
  Tony John George Apollaro, Alessandro Cuccoli, Carlo Di Franco, Mauro Paternostro, Francesco Plastina and Paola Verrucchi

- *Bell inequalities with no quantum violation and unextendible product bases*
  Remigiusz Augusiak, Julia Stasinska, Christopher Hadley, Jaroslaw Korbicz, Maciej Lewenstein and Antonio Acín

- *Efficient quantum information transfer through a uniform channel*
  Leonardo Banchi, Tony J. G. Apollaro, Alessandro Cuccoli, Ruggero Vaia and Paola Verrucchi

- *Coherent evolution of quantum dots as a means for entanglement generation and teleportation*
  Abolfazl Bayat, Sougato Bose, John H. Jefferson and Charles E. Creffield

- *Long distance entanglement generation in 2D quantum networks*
  Stuart Broadfoot, Uwe Dorner and Dieter Jaksch

- *Graph approach to quantum non-locality*
  Adan Cabello

- *Harmonic analysis on finite groups, number theory and efficient quantum cryptographic algorithms*
  Manuel Calixto

- *Quantum bit commitment using non-stationary states*
  Chi-Yee Cheung

- *Extension of the GHJW theorem for operator ensembles*
  Jeong Woon Choi, Dowon Hong, Ku-Young Chang, Dong Pyo Chi and Soojoon Lee

- *Proposal for multiple rounds of error correction*
  Ben Criger, Osama Moussa and Raymond Laflamme

- *Limited path entanglement percolation in quantum complex networks*
  Marti Cuquet and John Calsamiglia

- *Quantum clock fugue: entangling ad-hoc groups for synchronization*
  Iaakov Exman and Radel Ben-Av

- *Resource-efficient fault-tolerant topological one-way quantum computation with probabilistic two-qubit gates*
  Keisuke Fujii and Yuuki Tokunaga

- *Device-independent tests of classical and quantum dimensions*
  Rodrigo Gallego, Nicolas Brunner, Christopher Hadley and Antonio Acín
- *Quantum packet switching networks with delayed commutation*
  Juan Carlos Garcia Escartin and Pedro Chamorro-Posada
- *Towards quantum queueing theory*
  Piotr Gawron, Zbigniew Puchała and Tadeusz Czachórski
- *Neighborhood relationships of flip and exchange symmetric entangled state classes*
  Zafer Gedik
- *Geometry of multi-qubits systems based on resolution of conifold singularity and toric variety*
  Hoshang Heydari
- *Quantum picturalism for topological cluster-state computing*
  Clare Horsman
- *Taming multiparticle entanglement*
  Bastian Jungnitsch, Tobias Moroder and Otfried Guhne
- *Criterion for interference between independently prepared non-interacting bosonic fields*
  Toru Kawakubo and Katsuji Yamamoto
- *Entanglement of bipartite systems possessing angular momentum states*
  Mohammad Khamedi, Sozha Sohaily and Ali Reza Bahrampour
- *Scaling behavior of the excitations in 1D spin-1/2 dimerized and frustated model*
  Saeed Mahdavifar
- *Quantum walk on hierarchical regular network*
  Franklin Marquezino, Renato Portugal and Stefan Boettcher
- *Correspondence between memory and entanglement in quantum walks*
  Michael Mc Gettrick
- *QKD with finite resources: comparison of achievable key rates*
  Markus Mertz
- *Performance of heralded qubit amplifiers for practical device-independent quantum key distribution*
  Tobias Moroder and Marcos Curty
- *General optimality of the Heisenberg limit for quantum metrology*
  Carlos A. Perez Delgado, Pieter Kok and Marcin Zwierz
- *Selection of initial state and entanglement sudden death in spin chains and rings*
  Mohammad Reza Pourkarimi, Mojtaba Jafarpour and Majid Rahnama
- *Fidelity bounds for the Holevo information*
  Wojciech Roga, Karol Zyczkowski, Fernando De Melo and Mark Fannes

- *Sequential measurement-based quantum computing with memories*
  Augusto José Roncaglia, Leandro Aolita, Alessandro Ferraro and Antonio Acín
- *Entanglement of indistinguishable particles*
  Toshihiko Sasaki, Tsubasa Ichikawa and Izumi Tsutsui
- *Fast quantum circuit simulation using an implicit approach and a look-up cache*
  Mehdi Sedighi, Afshar Kakaei and Morteza Saheb Zamani
- *An approximately universal set consisting of two observables*
  Yasuhiro Takahashi
- *Quantum query model: application to computing mathematical relations*
  Alina Vasilieva and Taisia Mischenko-Slatenkova
- *Complete set of operational measures for the characterization of 3-qubit entanglement*
  Julio de Vicente Majua, C. Streitberger, T. Carle and B. Kraus