From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking [*]

Omar Fawzi [†] Patrick Hayden [† ‡] Pranab Sen [§ †]

October 14, 2010

Abstract

We exploit a connection between uncertainty relations and low-distortion embeddings of ℓ_2 into ℓ_1, which allows us to adapt an explicit low-distortion embedding to obtain efficient entropic uncertainty relations. This is the first explicit construction of entropic uncertainty relations for a number of measurements that is polylogarithmic in the dimension d that achieves an average measurement entropy of $(1-\epsilon)\log d$ for arbitrarily small ϵ. In fact, the bases defined by this construction verify a stronger notion of uncertainty relation that we call a metric uncertainty relation. We apply this construction to obtain the first strong information locking scheme that is efficiently computable using a quantum computer. This locking scheme can be interpreted as a method for encrypting classical messages using a key of size much smaller than the message length. We also apply our metric uncertainty relations to get efficient encodings for amortized quantum identification over a classical channel. Moreover, using probabilistic arguments, we establish the existence of strong metric uncertainty relations for an arbitrary number of measurements. In addition to giving better parameters, our analysis of the uncertainty relations satisfied by random bases is considerably simpler than earlier proofs.

Uncertainty relations Uncertainty relations express the fundamental incompatibility of certain measurements in quantum mechanics. Far from just being puzzling constraints on our ability to know the state of a quantum system, uncertainty relations are arguably the main reason that some classically impossible cryptographic primitives become possible when quantum communication is allowed. Therefore, it is of particular interest to construct measurements that satisfy strong uncertainty relations. The best known explicit constructions are based on mutually unbiased bases. Orthonormal bases $\{\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_{t-1}\}$ are said to be mutually unbiased if the inner product of any pair of vectors in different bases is $1/\sqrt{d}$, where d is the dimension of the ambient Hilbert space. In the case of $t = 2$ measurements, Maassen and Uffink [12] showed that mutually unbiased bases verify maximally strong entropic uncertainty relations: for all $|\psi\rangle$,

$$\frac{1}{2}\left(\mathbf{H}(p_{\mathcal{B}_0,|\psi\rangle}) + \mathbf{H}(p_{\mathcal{B}_1,|\psi\rangle})\right) \geq \frac{1}{2}\log d$$

where $p_{\mathcal{B},|\psi\rangle}$ is the outcome distribution of the measurement of $|\psi\rangle$ in the basis $\mathcal{B}$ and $\mathbf{H}$ refers to the Shannon entropy. It is easy to show that the prefactor of $1/2$ cannot be improved. In fact, more generally, the average entropy of the outcomes of t measurements is at most $(1-1/t)\log d$. Therefore, to make the average entropy larger than $1/2 \cdot \log d$, one has to consider a larger set of measurements. For $t = d+1$ measurements, mutually unbiased bases almost attain this upper bound, at least when such bases exist. Ivanovic [11] and Sanchez [13] showed that in this case the average entropy is at least $\log(d+1) - 1$. For $2 < t < d+1$, the behaviour of mutually unbiased bases is not well understood. It was even shown in [1] that there are arbitrarily large sets of mutually unbiased bases $\{\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_{t-1}\}$ that only satisfy an entropic uncertainty relation as good as one satisfied by $\{\mathcal{B}_0, \mathcal{B}_1\}$, i.e., the average entropy is $1/2 \cdot \log d$. The survey paper [14] asks whether there even exists a growing function f of t such that there exist t bases $\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_{t-1}$ such that for all $|\psi\rangle$, the average measurement entropy verifies

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{\mathcal{B}_k,|\psi\rangle}) \geq \left(1 - \frac{1}{f(t)}\right)\log d$$

for large d. One of our results is to answer this question affirmatively by studying random bases. We find $f(t) = \sqrt{ct/\log t}$ where c is an absolute constant. Moreover, we give the first *explicit* construction of strong entropic uncertainty

[*] A technical version of the paper can be found in [6]

[†] School of Computer Science, McGill University, Montréal, Québec, Canada

[‡] Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

[§] School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India relations in the region $2 < t < d+1$. More precisely, we show that for any ϵ, there exist efficiently quantum computable bases $\mathcal{B}_0, \dots, \mathcal{B}_{t-1}$ with $t = (\log d/\epsilon)^{c \log(1/\epsilon)}$ for some constant c such that for all $|\psi\rangle \in \mathbb{C}^d$, the average measurement entropy is at least $(1-\epsilon)\log d$. Our construction actually satisfies a stronger notion of uncertainty relation that we call a metric uncertainty relation. A metric uncertainty relation quantifies uncertainty using the total variation distance between (a marginal of) the outcome distribution and the uniform distribution. We refer the reader to the full paper [6] for a precise definition.

These constructions are based on a connection between uncertainty relations and low-distortion embeddings of $(\mathbb{C}^d, \ell_2)$ into $(\mathbb{C}^{d'}, \ell_1(\ell_2))$ where $\ell_1(\ell_2)$ is a norm that is closely related to ℓ_1. The non-explicit construction we provide can be thought of as a strengthening of Dvoretzky's theorem for the $\ell_1(\ell_2)$ norm. Our explicit constructions of uncertainty relations are based on a low-distortion embedding of ℓ_2 into ℓ_1 due to Indyk [10]. The main new ingredient that makes our "quantization" of Indyk's construction verify stronger uncertainty relations than do general mutually unbiased bases is the additional use of strong permutation extractors, which are a special kind of randomness extractor. A strong permutation extractor is a small family of permutations of bit strings with the property that for any probability distribution on input bit strings with high min-entropy, applying a typical permutation from the family to the input induces an almost uniform probability distribution on a prefix of the output bits. Our construction of efficiently computable bases satisfying a strong metric uncertainty relation involves an alternating application of mutually unbiased bases and strong permutation extractors. In fact, both the permutations and their inverses have to be efficiently computable for our construction. We build such strong permutation extractors using the results of Guruswami, Umans and Vadhan [7].

Locking classical correlations We apply these results to find the first efficient locking scheme. A locking scheme can be viewed as a cryptographic protocol in which a uniformly random n-bit classical message is encoded in a quantum system using a key of size much smaller than n (e.g., logarithmic in n). Knowing the key, it is possible to recover (or "unlock") the message from the quantum system. However, without the key, for any measurement and any measurement outcome i, the distribution of the message conditioned on getting outcome i is still ϵ-close to uniform in total variation distance. Locking was first discovered in [3] as the possibility of an arbitrarily large increase in the classical mutual information[1] of a bipartite quantum state using only one bit of communication. The authors of [8] used a probabilistic construction to prove the existence of bipartite states for which communicating a number of bits that is logarithmic in n can make the classical mutual information increase from 3 to n for n large enough. Recently, the authors of [4, 5] found stronger locking behaviour using a probabilistic argument. They used the trace distance rather than the classical mutual information to quantify the information leaked by a measurement. It should be noted that all known instances of strong locking behaviour are non-explicit. It is also worth stressing that standard derandomization techniques are not known to work in this setting. For example, unitary t-designs use far too many bits of randomness. Moreover, using a δ-biased subset of the set of Pauli matrices fails to produce a locking scheme unless the subset has a size of the order of 2^n.

In this paper, using our explicit construction of a metric uncertainty relation, we give an explicit locking scheme with a definition that is even stronger than the one proposed by [4, 5]. The encoding and decoding operations of our locking scheme can be implemented by a quantum circuit of almost linear size with polynomial time classical precomputations. This locking scheme can be used to obtain string commitment protocols [2] that are efficient in terms of computation and communication. Furthermore, we show that locking using a small key is still possible if the message distribution has sufficiently large min-entropy. We also prove a non-explicit result about the existence of locking schemes with key size depending only on the error parameter ϵ and not the message size. Our results are summarized in Table 1. All these results can be re-interpreted in terms of locking the entanglement of formation.

Efficient encoding for quantum identification We also give an application of our uncertainty relations to quantum identification codes. Quantum identification is a communication task between two parties Alice and Bob, where Alice is given a quantum state $|\psi\rangle$ and Bob wants to simulate measurements of the form $(|\varphi\rangle\langle\varphi|, \mathbb{1} - |\varphi\rangle\langle\varphi|)$ on $|\psi\rangle$. This task can be seen as a quantum analogue of the problem of identification in information theory where Alice and Bob hold n-bit strings x and y and Bob wants to determine whether $x = y$ using a one-way classical channel from Alice to Bob. Hayden and Winter [9] showed that a classical channel alone is useless for quantum identification. However, having access to a noiseless quantum channel makes classical communication useful. Their proof is non-explicit. Using our explicit metric uncertainty relations, we give an efficient encoder for this task, and we prove a better bound on the number of uses of the noiseless qubit channel. More precisely, we describe an efficient encoding circuit that allows the identification of an n-qubit state by communicating only $O(\log^2 n)$ qubits and n classical bits.

This result can be interpreted in terms of the communication complexity of a quantum measurement simulation problem. Alice is given an n-qubit state $|\psi\rangle$ and Bob is given a classical description of $|\varphi\rangle$. Namely, Bob wants to output 1 with probability in the interval $[|\langle\psi|\varphi\rangle|^2 - \epsilon, |\langle\psi|\varphi\rangle|^2 + \epsilon]$ and 0 with probability in the interval $[1 - |\langle\psi|\varphi\rangle|^2 - \epsilon, 1 -$

[1] The classical mutual information of a bipartite state is the maximum value of the mutual information between the outcomes of local measurements.

	Inf. leakage	Size of message	Size of key	Size of ciphertext	Explicit ?
[3]	$n/2$	n	1	n	yes
[8]	3	n	$4\log(n)$	n	no
[4, 5]	ϵn	n	$\log(n/\epsilon) + O(\log\log(1/\epsilon))$	n	no
This paper	ϵn	n	$2\log(1/\epsilon) + O(\log\log(1/\epsilon))$	$n + 2\lceil\log(9/\epsilon)\rceil$	no
This paper	ϵn	n	$4\log(1/\epsilon) + O(\log\log(1/\epsilon))$	n	no
This paper	ϵn	n	$O(\log(n/\epsilon))$	$c \cdot n$, with $c > 1$	yes
This paper	ϵn	n	$O(\log(n/\epsilon)\log(n))$	n	yes

Table 1: Comparison of different locking schemes. The information leakage, the size of the message and the key are measured in bits and the size of the ciphertext in qubits. It should be noted that our locking definition is stronger than all the previous definitions. Note that the variable ϵ can depend on n. For example, one can take $\epsilon = \delta/n$ to make the information leakage arbitrarily small. The symbol $O(\cdot)$ refers to constants independent of ϵ and n, but there is a dependence on c for the next to last row.

$|\langle\psi|\varphi\rangle|^2 + \epsilon]$. Using our non-explicit result on metric uncertainty relations, we can show that this task can be accomplished using $O(\log(1/\epsilon))$ qubits and n bits of communication. In some sense, this result can be thought of as an analogue of the well-known fact that the public-coin randomized communication complexity of the equality function is $O(\log(1/\epsilon))$ for an error probability ϵ. Quantum communication replaces classical communication and classical communication replaces public randomness. Classical communication can be thought of as an extra resource because, on its own, it is useless for quantum identification.

References

[1] M. A. Ballester and S. Wehner. Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases. *Physical Review A* 75(2):022319, Feb 2007, arXiv:quant-ph/0606244.

[2] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Physical Review A* 78(2):22316, 2008, arXiv:quant-ph/0504078.

[3] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal. Locking classical correlations in quantum states. *Physical Review Letters* 92(6):67902, 2004, arXiv:quant-ph/0303088.

[4] F. Dupuis. *A decoupling approach to quantum information theory*. Ph.D. thesis, Université de Montreal, 2010, arXiv:1004.1641.

[5] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung. Locking classical information, 2010. in preparation.

[6] O. Fawzi, P. Hayden, and P. Sen. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. 2010, arXiv:1010.3007.

[7] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM* 56(4):1–34, 2009.

[8] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics* 250(2):371–391, 2004, arXiv:quant-ph/0307104.

[9] P. Hayden and A. Winter. The fidelity alternative and quantum measurement simulation. 2010, arXiv:1003.4994.

[10] P. Indyk. Uncertainty principles, extractors, and explicit embeddings of L2 into L1. *Proceedings of the 39th annual ACM Symposium on Theory of Computing*, pp. 615–620, 2007.

[11] I. D. Ivanovic. An inequality for the sum of entropies of unbiased quantum measurements. *Journal of Physics A: Mathematical and General* 25(7):L363, 1992.

[12] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters* 60(12):1103–1106, Mar 1988.

[13] J. Sanchez. Entropic uncertainty and certainty relations for complementary observables. *Physics Letters A* 173(3):233 – 239, 1993.

[14] S. Wehner and A. Winter. Entropic uncertainty relations—a survey. *New Journal of Physics* 12:025009, 2010, arXiv:0907.3704.