Introduction to Quantum Computation Sevag Gharibian
Summer 2020, Paderborn University

Lecture 12: Independent reading - Quantum money

1 Quantum money

And now, we have arrived at the end of this course. As the topic of the final lecture, I felt it would be fitting to cover the first known suggested use of quantum information — *quantum money.* Indeed, quantum information processing was *not* first envisioned to solve fancy problems such as factoring or simulation of physical systems. Rather, in the early 1970's, Stephen Wiesner had the idea of using four single-qubit quantum states, $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, to implement an unforgeable notion of money. As the story goes (more accurately, as Gilles Brassard told the story at QIP 2010 in Zurich, and as far as my memory recalls), Wiesner actually proposed his idea as part of a university assignment or project of some sort. His professor did not understand it, and thus it was largely cast aside, only to be published about a decade later (1983, to be precise [Wie83]). In the meantime, however, Wiesner's idea of *conjugate coding* has triumphantly stood the test of time. For example, by happy coincidence, Wiesner happened to share his ideas with Charlie Bennett and Gilles Brassard, who went on to propose their now-famous BB84 protocol in 1984 [BB84] for quantum key distribution (also based on conjugate coding).

Our focus. There is more to quantum money which we will be able to cover in this lecture, as with most topics in this course. Here is what we will focus on. Wiesner's original scheme turns out to indeed be secure, meaning: Given a quantum banknote $|\psi\rangle$ consisting of n conjugate coding states, the probability of creating a duplicate copy of $|\psi\rangle$ is exponentially small in n, i.e. precisely $(3/4)^n$. (Remarkably, it was not until 2012 that this was explicitly shown rigorously by Molina, Vidick, and Watrous [MVW13] using *semidefinite programming.*) Note this security is *information-theoretic*, meaning no computational assumptions are required, other than having the adversary obey the laws of quantum mechanics.

However, security is a fickle thing, and it turns out that if we change the rules of engagement ever so slightly, Wiesner's scheme is *no longer secure.* In particular, as with current-day banknotes, a bank may wish to *verify* that a claimed quantum banknote $|\widetilde{\psi}\rangle$ is genuine. It turns out that, if the bank does what any normal person would, namely return a banknote which passes the authenticity test and confiscate a banknote which fails the authenticity test, then Wiesner's scheme can be *broken.* (Here, the key point is we are now allowing multiple rounds of interaction with an entity, the bank, which performs as its authenticity test the projective measurement $M = \{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$, for $|\psi\rangle$ the genuine banknote in question.)

Your task. You are to independently read the paper [NSBU16]:

> D. Nagaj, O. Sattath, A. Brodutch, and D. Unruh, An adaptive attack on Wiesner's quantum money. *Quantum Information & Computation*, 16(11&2):1048–1070, 2016. Open-access version at `https://arxiv.org/abs/1404.1507`.

This shows how to use the *quantum Zeno effect* (in the form of the Elitzur-Vaidman bomb testing problem) to successfully create many copies of $|\psi\rangle$, thus breaking Wiesner's scheme. In particular, you are required to read sections 1 to 3 inclusive of this paper.

Motivation. There are a few reasons for the setup of this final lecture. First, the study of quantum money highlights how careful one need be in formally modelling security in a cryptographic context. Second, Reference [NSBU16] will teach you a neat new trick: Applying the quantum Zeno effect via the Elitzur-Vaidman bomb tester, which is worth having in your toolkit. Finally, the aim of this course is to get you to become independent learners in the field, and so leaving you with an independent reading lecture is arguably quite appropriate. With this in mind, we thus say: Goodbye, farewell, and leave you with one final quote:

> *"Fly my pretties, fly!"*
> — Often (incorrectly) attributed to 1939 film The Wizard of Oz

2 What next?

There is much we have not been able to cover given our limited time. Below, we have compiled a short list (which is far from comprehensive) of various sources you may wish to consult to continue your learning (in alphabetical order):

- Andrew Childs `https://www.cs.umd.edu/~amchilds/qa/`: An advanced text focusing on quantum algorithms.
- Ronald de Wolf `https://arxiv.org/abs/1907.09415`: A recent set of introductory course notes to quantum computation, from a theoretical CS perspective.
- Sevag Gharibian `http://groups.uni-paderborn.de/fg-qi/courses/UPB_QCOMPLEXITY/2019/UPB_QCOMPLEXITY_syllabus.html`: An advanced text focusing on quantum complexity theory.
- Griffiths [Gri04]: For those interested in looking beyond our "quantum mechanics sandbox" to what undergraduate quantum mechanics is "really about".
- Nielsen and Chuang [NC00]: The course reference textbook, with much material we did not manage to cover.
- John Watrous `https://cs.uwaterloo.ca/~watrous/TQI/`: An advanced text on quantum information theory, with a computer science orientation.
- Mark Wilde `http://www.markwilde.com/qit-notes.pdf`: An advanced text on quantum information theory, with a strictly information theoretic focus (e.g. entropy, quantum channels, etc).

References

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems, and Signal Processing*, volume 175, page 8, 1984.

[Gri04] D. J. Griffiths. *Introduction to Quantum Mechanics (2nd Edition)*. Pearson Prentice Hall, 2004.

[MVW13] Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 7582 of *Lecture Notes in Computer Science*, pages 45–64. Springer Berlin Heidelberg, 2013.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[NSBU16] D. Nagaj, O. Sattath, A. Brodutch, and D. Unruh. An adaptive attack on Wiesner's quantum money. *Quantum Information & Computation*, 16(11&12):1048–1070, 2016.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.