Quantum Weak Coin Flipping

talk at

SUMA 2019

Reunión anual de la UMA junto a la SOMACHI

Universidad Nacional de Cuyo, Mendoza, Argentina

September 27th, 2019

speaker

Stephan Weis

joint work with

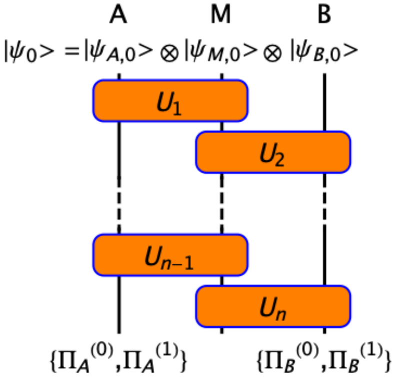
Atul Singh Arora and Jérémie Roland

QuIC - Ecole Polytechnique de Bruxelles, Université libre de Bruxelles, Belgium

Exciting Moments in the Quantum Sciences

- today, quantum key distribution works up to 100km distance (telecom optical fiber) and allows secure communication relying only on the laws of physics; within the next 5 years we will see quantum key distribution over a large scale network in the Netherlands (Wehner et al. '18)
- the parties trust each other in key distribution; two-party tasks between distrustful, cooperative parties are more difficult, many of them are insecure even in quantum mechanics, e.g. secure computation or bit commitment
- an exception is weak coin flipping (WCF), the task of two distrustful parties, Alice and Bob, to agree on a random bit by following a communication protocol; in a breakthrough result in 2007, Mochon proved quantum WCF to be almost secure (see also Aharonov et al. '16); classical WCF is completely insecure (Kitaev, QIP '02)

The Protocol (Simplified)



- Alice and Bob have private registers A, B; they exchange a message register M in n rounds and act in turns with unitaries U_i on AM and MB
- if they follow the protocol (are honest) then the state evolves as

$$|\psi_i\rangle = U_i \dots U_2 U_1 |\psi_0\rangle$$

- they measure the state ρ after round n, obtaining random variables A, B with ($i = 0, 1$)

$$\mathrm{Prob}(X = i) = \mathrm{tr}(\rho \Pi_X^{(i)})$$

- if Alice and Bob are honest then $\mathrm{Prob}(X = i) = \langle\psi_n|\Pi_X^{(i)}|\psi_n\rangle$; a consistency assumption is that if they are honest, then $A = B$ with certainty and $\mathrm{Prob}(X = i) = \frac{1}{2}$ for $X = A, B$ and $i = 0, 1$

The Bias of a WCF Protocol

- the parties of a weak coin flip have preferred outcomes, say Alice wants 0 and Bob wants 1
- the cheating probability P_A^* of Alice is the probability that an honest Bob outputs 0, maximized over all quantum operations a cheating Alice could replace her unitaries with:

$$P_A^* = \max \mathrm{Prob}(B = 0);$$

similarly, the cheating probability P_B^* of Bob is

$$P_B^* = \max \mathrm{Prob}(A = 1)$$

- the bias of a WCF protocol is $\epsilon = \max\{P_A^*, P_B^*\} - \frac{1}{2}$

Example (flip and declare protocol)**.**
Alice flips a coin, sends the result to Bob. They both output the result. Here $P_A^* = 1$ and $P_B^* = \frac{1}{2}$, so $\epsilon = \frac{1}{2}$.

The Cheating Probability as an SDP

Primal SDP $P_A^* = \max \operatorname{tr}[(\mathbb{1}_M \otimes \Pi_B^{(0)})\rho_n]$

maximization over states $\rho_0, \rho_1, \ldots, \rho_n$ on MB subject to

- $\operatorname{tr}_M(\rho_0) = \operatorname{tr}_{AM} |\psi_0\rangle\langle\psi_0| = |\psi_{B,0}\rangle\langle\psi_{B,0}|$
- for i even $\operatorname{tr}_M(\rho_i) = \operatorname{tr}_M(U_i \rho_{i-1} U_i^*)$
- for i odd $\operatorname{tr}_M(\rho_i) = \operatorname{tr}_M(\rho_{i-1})$

Dual SDP $P_A^* = \min \operatorname{tr}[Z_{B,0} |\psi_{B,0}\rangle\langle\psi_{B,0}|]$

minimization over $Z_{B,0}, Z_{B,1}, \ldots, Z_{B,n} \geq 0$ on B subject to

- for i even $\mathbb{1}_M \otimes Z_{B,i-1} \geq U_i^* (\mathbb{1}_M \otimes Z_{B,i}) U_i$
- for i odd $Z_{B,i-1} = Z_{B,i}$
- $Z_{B,n} = \Pi_B^{(0)}$

Dual SDP $P_B^* = \min \ldots$ with dual variables $Z_{A,0}, Z_{A,1}, \ldots, Z_{A,n}$

Point Games

- analogous to measurement probabilities, if $|\psi\rangle$ is a vector and $Z = \sum zP_z \geq 0$, we define $\mathrm{prob}[Z, |\psi\rangle](z) = \langle\psi|P_z|\psi\rangle$ if $z \in \mathrm{sp}(Z)$ is an eigenvalue, otherwise $\mathrm{prob}[Z, |\psi\rangle](z) = 0$

- consider the delta function $[x, y]$ with $[x, y](a, b) = 1$ if $x = a \wedge y = b$, otherwise $[x, y](a, b) = 0$; for each pair $Z_{A,i} = \sum_x xP_x$ and $Z_{B,i} = \sum_y yQ_y$ of a dual feasible point let

$$p_{n-i} = \sum_{(x,y)\in\mathrm{sp}(Z_{A,i})\times\mathrm{sp}(Z_{B,i})} \langle\psi_i|P_x \otimes \mathbb{1}_M \otimes Q_y|\psi_i\rangle\, [x, y]$$

- the sequence $p_0 \to p_1 \to \cdots \to p_n$ of finitely supported functions $[0, \infty)^2 \to [0, \infty)$ is called a point game

- we assume that $Z_{A,0}\,|\psi_{A,0}\rangle = \beta\,|\psi_{A,0}\rangle$ and $Z_{B,0}\,|\psi_{B,0}\rangle = \alpha\,|\psi_{B,0}\rangle$; then the point game starts at $p_0 = \frac{1}{2}([0, 1] + [1, 0])$ and ends at $p_n = [\beta, \alpha]$; the cheating probabilities are $P_A^* \leq \alpha$ and $P_B^* \leq \beta$; Goal: Get α, β as close as possible to 1/2

Operator Monotone Functions

observations on the construction (for even i, similarly for odd)

■ the transition $p_i \to p_{i+1}$ is vertical (horizontal for odd i), that is to say, $p_{i+1} - p_i = \sum_{x,y} f_x(y)[x, y]$ where $\sum_y f_x(y) = 0$

■ the vertical line transitions of $p_i \to p_{i+1}$ are EBM transitions (expressible by matrices), that is to say, for each $x \geq 0$ there are diagonal matrices $X, Y \geq 0$, a unitary U, and vectors $|v\rangle, |w\rangle$ satisfying $UXU^* \leq Y$ and $|w\rangle = U|v\rangle$, such that

$$p_i[x, \cdot] = \mathrm{prob}[X, |v\rangle] \quad \text{and} \quad p_{i+1}[x, \cdot] = \mathrm{prob}[Y, |w\rangle]$$

■ the vertical line transitions of $p_i \to p_{i+1}$ lie in the dual cone to the cone of operator monotone functions $[0, \infty) \to \mathbb{R}$, in other words, $\sum_y f_x(y)h(y) \geq 0$ for each operator monotone function h

From Point Games Back to Unitaries

Mochon's Breakthrough Result from 2007. For all $\epsilon > 0$ there exists a quantum WCF protocols with bias ϵ.

Mochon exploited operator monotone functions and reversed the construction of point games from protocols. However, he returns non-constructively to EBM transitions and unitaries.

Our Results.

- Framework to build a protocol from EBM line transitions
- Explicit protocol of bias $1/10$; the best was $1/6$ by Mochon in '07 and $1/\sqrt{2} - 1/2$ by Spekkens and Rudolph in '02
- Numerical algorithm for computing unitaries of EBM transitions (arbitrary bias); uses geometry of ellipsoids

Thank you

Reference: A. Singh Arora, J. Roland, and S. Weis, *Quantum Weak Coin Flipping*, in Proceedings of the 51st Annual ACM SIGACT Symposium on the Theory of Computing (STOC ’19), 2019.