Quantum Weak Coin Flipping with an arbitrarily small bias.

§1 Introduction

Defn: Coin Flipping

Why Bother? : (1) Location of QIP 2050

(2) Secure 2 party communication

Bit commitment ✗

- secure with cheat detection
- (WCF as subroutine)

(3) "Hard" ⇒ new formalism : Kitaev's

Intuition : Kitaev's formalism : Point Game

(1) sequence of configurations
"
points in a plane (+ve quadrant) with prob. (+ve)

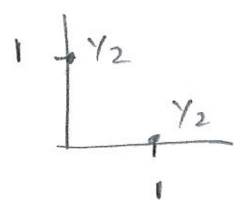
(2) 2 sequences should differ along vertical or horizontal points (not both)

(3) Rule: (a) Conserve prob on the line.

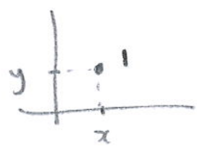
(b) $$\sum_{z} \frac{\lambda z}{\lambda + z} P_z \leq \sum_{z'} \frac{\lambda z'}{\lambda + z'} P_{z'}.$$

↑ before ↑ after.

(4) Boundary conditions: Initial



Final



(by conservation of prob)

(5) Claim : $P_A^* \leq y$, $P_B^* \leq x$.

(sub-intuition) : x-coordinates – eigenvalues of the dual SDP op on Alice's space.

y-coordinates – . . .

Prob weights – Assigned by the honest state to this space.

NB: Reverse time convention: Final measurements at $t=0$, initial state at $t=n$.

: Kitaev's 2nd Formalism :

Describes an entire Point Game as

(1) 2 f^s. $h(x,y)$ $v(x,y)$ with real values.

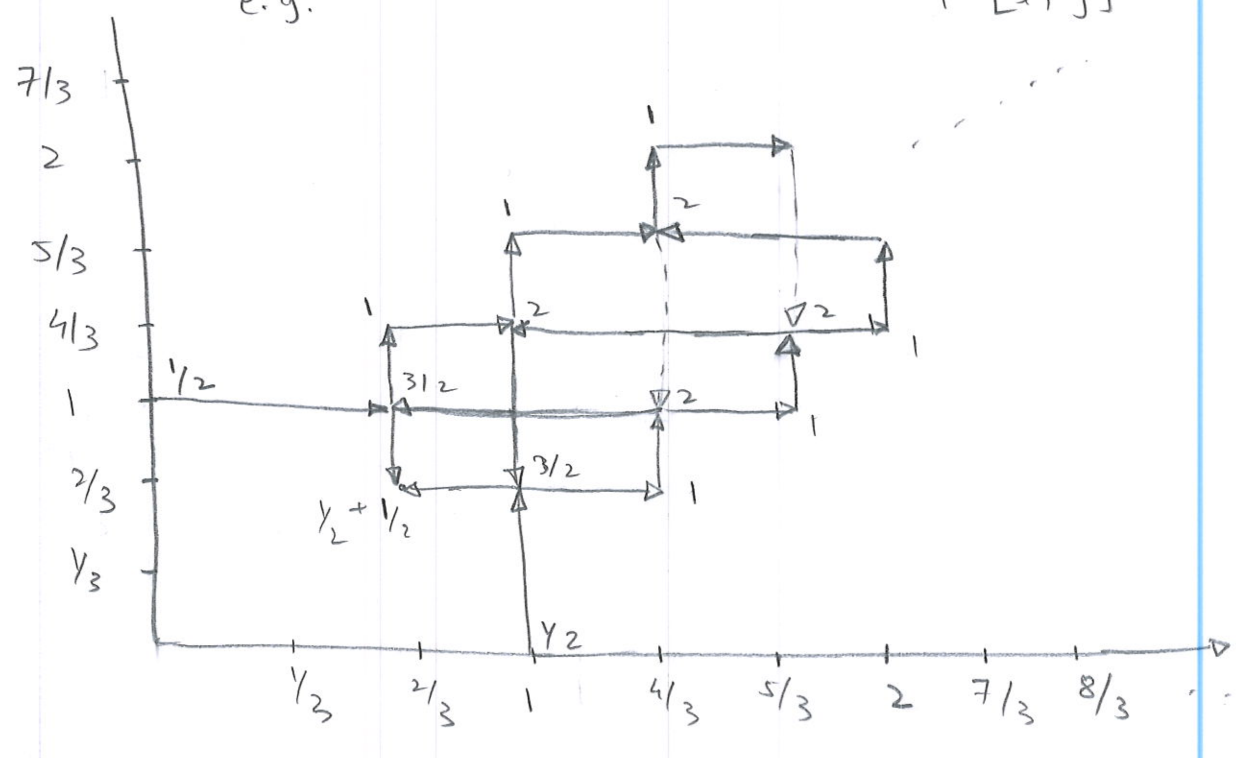
(2) Horizontal line on $h(x,y)$ &

Vertical line on $v(x,y)$

(a) sum to 0. (b) $\sum_z \frac{\lambda z}{\lambda + z} \geq 0$.

(3) $h(x,y) + v(x,y) = -\frac{1}{2}[1,0] - \frac{1}{2}[0,1] + [x,y]$

e.g.



Remark: Complete protocol in one image.

: Author's "protocol": $P_A^* = P_B^* = \frac{k+1}{2k+1}$

$k=0$ allows 'infinite' cheating
$k=1$ 1/6 protocol (Dip-dip boom)
$k \to \infty$ arbitrarily small bias

Remark:

"Sadly, mechanically transforming these protocols back into the language of unitaries, while possible, doesn't lead to particularly simple or efficient protocols (i.e. in terms of laboratory resources). Finding easy to implement protocols with a small bias remains an interesting open problem."

Appendixes: A: The dip-dip boom protocol.
B: Strong duality for coin flipping. (needed for both the first & second)
C: A lemma that's key to obtaining matrices from point games.

§ 1.1 Coin Flipping defined

Idea: Alice & Bob ← (a) distrustful
(b) remote (over a communication device)

↓

protocol: (prevents cheating) random bit

WCF: Alice & Bob have a priori desired outcomes.

NB: Can label Alice wins & Bob wins

NB2: Don't care if players cheat to decrease their probability of winning.

SCF: No apriori desired outcomes.

NB: Must prevent cheating / biasing in both directions.

Remark: SCF is harder (at least as hard) as WCF.

Defn: WCF: 2 party interactive protocol s.t. initially the state is uncorrellated & ends with both participants outputting the same bit.

: Convention: Alice wins 0
Bob wins 1

(1) When both honest: Alice's output is uniformly random
&
equals Bob's output.

(2) When Alice is honest & Bob deviates (cheats): Prob of Alice outputting 1 (Bob winning) $\leq P_B^*$.

3. Similarly for Bob honest & Alice cheating & P_A^*.

Remarks : P_A^*, P_B^* characterise the protocol.

Bias : $\max(P_A^*, P_B^*) - 1/2$

NB : No restrictions on the output of a cheating players. ($\because$ they're impossible to enforce).

e.g. When one player cheats, their outputs needn't agree.

e.g. When an honest player detects cheating he/she can declare him/herself to be a winner.

§ 1.1.1 Communication Model.

claim : Classically (without further assumptions) at least one player is guarenteed victory. (think : assymmetric protocols)

Story : • With extra assumptions, classically WCF is possible. Will not hold after QC are available.

• With certain relativistic settings WCF is possible

Requirement : Here we assume both players are connected by a Quantum Channel (noiseless) with arbitrary memory.

Claim : the resulting protocol will have information theoretic security.

§ 1.1.2 On the starting state

By defⁿ: completely uncorrelated.

Justificⁿ: (1) If a known entangled state is shared, a correlated bit can be obtained even without communication.
(Also holds for classically correlated states)

- If we assume randomly distr, then there's nothing to do.
- If they (say) buy these correlated states, acquisition of randomness is still not trivial ∵ both players can learn apriori the outcomes & order events to his/her advantage.
One must protect ordering of events & that's a different problem.

(2) A good protocol should prevent players from predicting the outcome before the protocol begins.

Remark: Exploring this: Weaken the no-correlation requirement to a no-prior-knowledge-of-outcome requirement might be interesting. Not pursued here.

$\boxed{5}$ 1.1.3 On the security guarantees

Honest: Alice & Bob control their labs exclusively.
: The remaining universe is untouched.

Cheating Players: control everything other than the honest players lab; including communication channel.

Consequences (Abstract)
(1) Cheaters quantum 'super' operators must act as $\mathbb{1}$ on the honest players laboratory.
(2) Honest players operations are applied as intended.
(3) An honest player can verify the dimension of the incoming message.

Requirements (Practical)
e.g.
(1) Magnetic shielding in the lab is good enough to prevent tampering by the cheater.
(2) Grad student working in the lab can't be bribed.
(3) A nanobot can't enter through the communication channel.

Remark : The security analysis will prove that the protocol is as secure as the laboratory.

§ 1.1.4 On the restriction to unitary operators

Usual : (1) Protocol only involves unitaries & a single measurement in the end.

(2) cheating strategies are implemented using unitaries only.

Claim : Bounds obtained this way apply to the most general case : Players can use measurements, superoperators, classical randomness & extra classical channels.

Story : This follows from 2 lemmas, roughly stated as

1. Given a general protocol P (incl. measure etc.) with bias ϵ under general cheating ∃ a protocol (with unitary + end measure) P' with ϵ bias under general cheating.

2. Given a P' (with unitary + end measure) & a general cheating strategy giving a bias ϵ, ∃ a (unitary ~~+ end measure~~) cheat strategy with bias ϵ.

Story : We don't prove these here ; proven across papers, e.g. [LC98] & [May96].

(a) First statement — used for proving lower bounds on the bias. Not vital here.

$\Downarrow$

enough to consider honest as unital.

NB : Also applies to potentially infinite round protocols (e.g. rock-paper-scissors) ; the bias comes arbitrarily close in this case, not same.

(b) Second statement

$\Downarrow$

enough to check unital cheaters — proof idea : Apply unitary & "discard" hilbert space.
Don't even need to measure (it doesn't increase prob. winning)

NB : Also holds for protocols that have projection (in the honest case).

Doubt : Where do we care about the actions of the opponent in the SDP?

§ 1.2 A brief history muddled by hindsight

Two problems : (1) Two honest players try to complete a task without disruption (encrypted communication)

(2) Two mutually distrustful players try to co-operate in a way that prevents the opposing player from cheating, effectively simulating a trusted third party
(choosing a common meeting time while keeping their schedules private)
("two-party secure computation")

1980s : (cat. 1) Quantum Key Distribution - success

90s : (cat 2) Bit commitment — impossible.

Story : Bit-commitment could be used to do all other two-party secure computation protocols.

: NB: Impossible under information theoretic security

: Surprisingly, most multi-party secure-computations are classically possible with information theoretic security, granted # cheating players is bounded & all parties share private pairwise communication channels.

: Similar results hold for the Quantum case.

: New goal (1990s) to find a two-party secure task that's modestly interesting & can be realised with information theoretic security using Quantum Information.

2000s : Quantum version of coin flipping over a telephone.

Focused on Strong : bound proven $\frac{1}{\sqrt{2}} - \frac{1}{2}$ on the bias. (mochon)

: Weak CF : $\frac{1}{\sqrt{2}} - \frac{1}{2} \simeq 0.207$ (Kitaev), then $\frac{1}{6} \simeq 0.167$ Ambainis

: # rounds $\geq O(\log \log 1/\epsilon)$

$\Rightarrow$ no finite round protocol can have $\to 0$ bias.

: Kitaev : Extended formalism (unpublished)

A different (Gutoski) extension

Story : Possibility : Instead of demanding no cheating, demand cheating be caught.

: Quantum protocols known; also known that amount of potential cheat detection is bounded.

: Outlook : Possibility of two-party secure with cheat detection & some otherwise info^n theoretically secure ⇒ Quantum Information fullfils its potential.

More work is required in this direction; tools presented maybe useful.

Rough