Improving the security of device-independent weak coin flipping protocols

Atul Singh Arora   Jamie Sikora   Thomas Van Himbeeck

The Problem

(Strong) Coin Flipping. Two remote players, Alice and Bob, don't trust each other, but wish to agree on a random bit.

Weak Coin Flipping. Alice wants 0 (heads) and Bob wants 1 (tails).

Correctness: When both parties are honest, a uniformly random bit is agreed upon.

Soundness: Max. prob. with which cheating Alice/Bob succeed against honest Bob/Alice is p_A^*, p_B^*.

The bias is $\epsilon = \max\{p_A^*, p_B^*\} - 1/2$.

State of the Art

Classically: $\epsilon = 1/2$ viz. at least one player can always cheat and win [Kitaev]

Quantumly: $\epsilon \to 0$ [Moc07,ACGKM14,ARW19,ARV21]

Device Independent:

Protocol $\mathscr{S}$ — A Strong Coin Flipping protocol. From over 10 years ago!

[Silman, Chailloux, Aharon, Kerenidis, Pironio, Massar 11]

Security: $p_A^* = \cos^2(\pi/8) \approx 0.853$ and $p_B^* = 3/4$

$\epsilon \leq 0.33664$ when composed

Alice has one box and Bob has two boxes.
Each box
takes one binary input and gives one binary output,
and is designed to play the optimal GHZ game strategy.

1. Alice chooses a uniformly random input to her box $x \in_R \{0,1\}$ and obtains the outcome a. She chooses another uniformly random bit $r \in_R \{0,1\}$ and computes $s = a \oplus (x \cdot r)$. She sends s to Bob.
2. Bob chooses a uniformly random bit $g \in_R \{0,1\}$ and sends it to Alice. (We may think of g as Bob's "guess" for the value of x.)
3. Alice sends x to Bob. They both compute the output $c = x \oplus g$.
(This is the outcome of the protocol if no-one aborts)
4. Bob tests Alice
   I. Alice sends a to Bob. Bob sees if $s = a$ or $s = a \oplus x$. If this is not the case, he aborts.
   II. Bob chooses $y, z \in_R \{0,1\}$ s.t. $x \oplus y \oplus z = 1$ and then performs a GHZ test using x, y, z as the inputs and a, b, c as the output from the three boxes.
5. They both accept the value c as the outcome (assuming no abort).

Recall: GHZ test: Given binary inputs $x, y, z \in \{0,1\}$ satisfying $x \oplus y \oplus z = 1$ produce $a, b, c \in \{0,1\}$ such that $a \oplus b \oplus c = xyz \oplus 1$

Protocol $\mathscr{W}$ —A Weak Coin Flipping variant of Protocol $\mathscr{S}$.

Steps 1–3 and 5 are the same.

4. Test rounds:

(a) If $x \oplus g = 0$, Bob tests Alice as in Protocol $\mathscr{S}$.

(b) If $x \oplus g = 1$, Alice tests Bob:

III. Alice chooses $y, z \in_R \{0,1\}$ s.t. $x \oplus y \oplus z = 1$ and sends them to Bob. Bob inputs y, z into his boxes, obtains and sends b, c to Alice. Alice tests if x, y, z as inputs and a, b, c as outputs, satisfy the GHZ test. She aborts if they do not.

First Technique: Self-Testing

Protocol $\mathscr{P}$—Alice self-tests

Alice starts with n boxes, indexed $1_1, \ldots 1_n$. Bob starts with $2n$ boxes, the first half indexed by $2_1 \ldots 2_n$ and the other half by $3_1 \ldots 3_n$. The triple of boxes $(1_i, 2_i, 3_i)$ is meant to play the optimal GHZ strategy.

1. Alice selects $i \in_R \{1 \ldots n\}$ and asks Bob to send her all the boxes *except* those indexed by 2_i and 3_i.
2. Alice performs $n-1$ GHZ tests using the $n-1$ triples of boxes she has.
3. Alice aborts if *any* of the GHZ tests fail. Otherwise, she announces to Bob that they can use the remaining boxes for Protocol W.

Protocol $\mathscr{Q}$—Bob self-tests

Analogous. Boxes are the same but Bob picks i and requests 1_i.

Result—Advantage

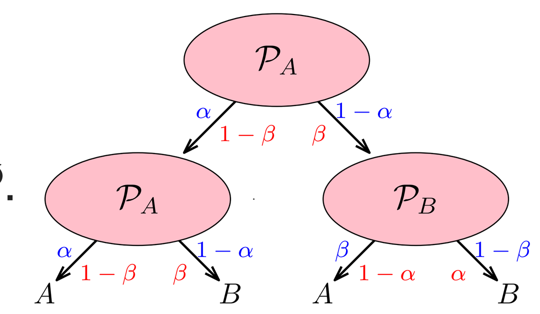
For Protocol $\mathscr{P}$, for large n,

$p_A^* = \cos^2(\pi/8) \approx 0.8535$ (unchanged) and $p_B^* \approx 0.666$ (improved from 0.75).

Second Technique: Abort-phobic composition

Standard Composition

Polarity. if $\alpha := p_A^* > p_B^* =: \beta$ for a protocol $\mathscr{P}$ we write it as $\mathscr{P}_A$ and it is polarised towards a.



Winner gets polarity. Alice and Bob agree on a protocol $\mathscr{P}$.

1. Alice and Bob perform protocol $\mathscr{P}$.
2. If Alice wins, they use $\mathscr{P}_A$ to determine the final outcome.
3. If Bob wins, they use $\mathscr{P}_B$ to determine the final outcome.

Security: Alice's cheating probability = $\alpha^2 + (1-\alpha)\beta < \alpha$ and
Bob's cheating probability = $\beta\alpha + (1-\beta)\beta < \alpha$
viz. the resulting bias is smaller, if $\alpha > \beta$.

Cheat Vectors

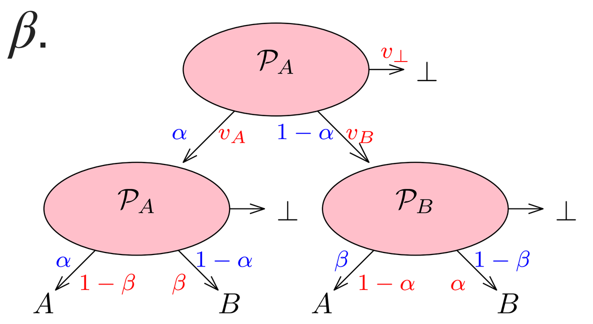
Given a protocol $\mathscr{R}$, we say $(v_A, v_B, v_\perp)$ is a **cheat vector** for (dishonest) Bob if there exists a cheating strategy where,

v_B is the probability with which Alice accepts the outcome $c = 1$,
v_A is the probability with which Alice accepts the outcome $c = 0$,
$v_\perp$ is the probability with which Alice aborts.

The set of cheat vectors for (dishonest) Bob is denoted by $\mathbb{C}_B(\mathscr{R})$.
Analogously, define $\mathbb{C}_A(\mathscr{R})$.

Abort Phobic Composition

For $\mathscr{R}$ in the first step, consider all three events: Bob wins, Alice wins, abort. Then,
Bob's cheating probability = $v_B \cdot \alpha + v_A \cdot \beta + v_\perp \cdot 0$.



NB: May be a strict improvement if $v_\perp > 0$ when $v_B = \beta$.

NB2: Bob's cheating probability is an optimisation over $\mathbb{C}_B$.

NB3: Because of the self-testing step, it can be cast as as SDP.

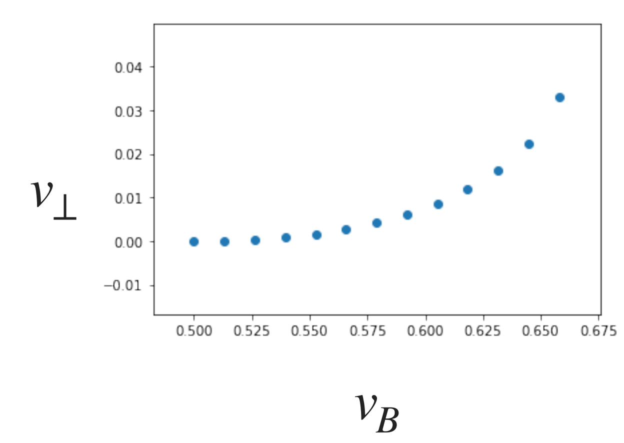
NB4: This can be repeated and analysed from the bottom up, again using SDPs.

Result—Advantage

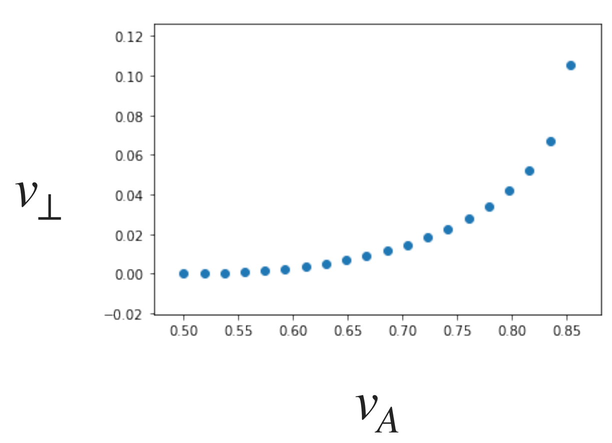
Using abort-phobic compositions repeatedly with Protocol $\mathscr{P}$, one gets $\epsilon \approx 0.3148$ (best known was 0.33664).

Using Protocol $\mathscr{P}$ at the bottom and Protocol $\mathscr{Q}$ (again, with abort-phobic composition), one gets
$\epsilon \approx 0.29104$ (but we assume a continuity/convergence conjecture holds to get this).

Protocol $\mathscr{P}$



Protocol $\mathscr{Q}$



References, Affiliation, PDF and related | QR

Caltech

QIP, 2022