Relativistic commitment and zero-knowledge proofs

André Chailloux

Relativistic commitment and zero-knowledge proofs

André Chailloux

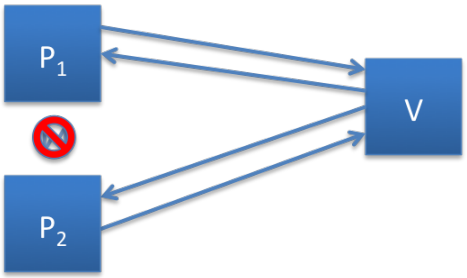
Inria, Paris

Bellairs, March 4-8 2018

Interactive proofs

- Interactive proofs: a great model with many applications both in cryptography and in complexity.

- Multi-prover interactive proofs: split the prover into 2 or more non communicating agents [BGKW88].



If the verifier knows that the provers are split and cannot communicate then they can actually prove more things to the verifier.

Multi-prover interactive proofs

- First goal was to remove computational assumptions from cryptographic protocols. However, non realistic model.
- Still a lot of developments in cryptography and in complexity theory (2 player games, PCP theorem).
- Relativistic cryptography: use special relativity theory to make non communicating provers a realistic model.
- Hope: increase the possibilities for unconditional cryptography. Of notable importance regarding retroactive security.

Special relativity theory

- Developed by Einstein in 1905, precedes general relativity.
- Governing principles
  - The laws of physics are identical in all non-accelerating frames of reference.
  - The speed of light in a vacuum is the same for all observers (hence finite).
- A lot of unexpected consequences for objects travelling close to the speed of light (for eg. twin paradox)
  - Unfortunately, we won't use most of these cool things in relativistic cryptography.

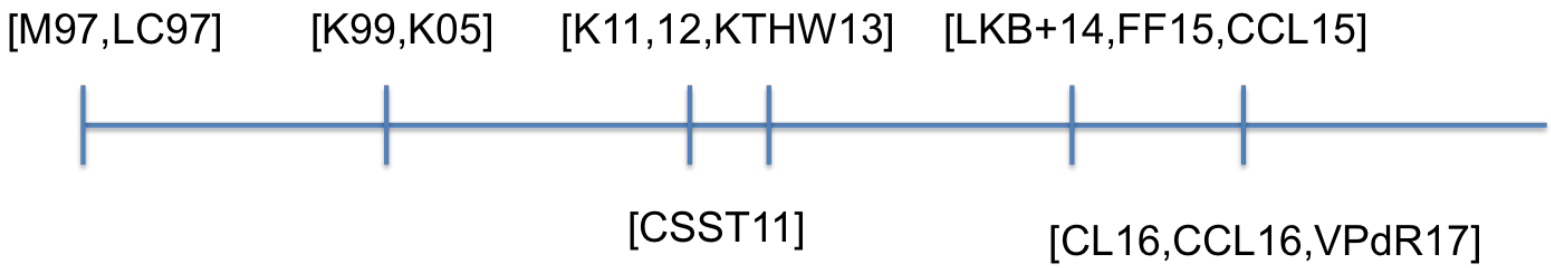
Non superluminal signaling

- What we use from special relativity theory = non superluminal signaling.
- NSS : no information carrier can travel faster than the speed of light.
- Doesn't disallow instantaneous effects that don't transmit information such as entanglement.
- We use NSS to enforce that some parties don't have access to some information at a given time.

How to enforce non-communicating provers

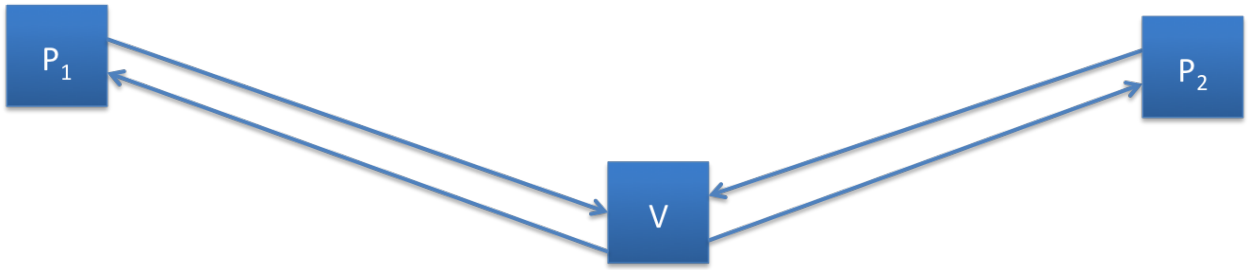
- Put the 2 provers at some distance D.
- Since any information carrier travels at a speed $c \approx 300000 km/sec$, information takes time $\tau = \frac{D}{c}$ to travel between the 2 provers.
- Simplest idea: make sure the whole protocol runs in time $< \tau$ to ensure that no-communication could be done between the provers.
  - For ex: if $D = 6880 km$ (distance between Paris and Barbados), $\tau \approx 22.9 ms$. Actually quite large.
- Different space-time constraints can also be used, at a given time during the protocol, each prover has access only to the information that could have physically traveled to it. Also, could be used to disallow a joint cheating strategy for the provers.

(Highly non exhaustive) historical timeline



Classical relativistic bit commitment secure against quantum adversaries

- Enforce the non communication constraint: put the provers very far apart and use timing constraints.



- By the triangle inequality, V is at least $\frac{\text{very far}}{2}$ apart from one of the provers. This implies that timing constraints are hard to achieve.
- Idea to circumvent this: also split the verifiers.

- Each player has a clock and all players agree on some absolute time.

Bit commitment

Bit commitment: protocol that performs the 2 following phases

- A commit phase $\mathrm{comm} = (\mathrm{comm}_P, \mathrm{comm}_V)$: an interactive protocol involving $P = (P_1, P_2)$ and V_1, V_2. The provers have an input $b \in \{0, 1\}$ - the bit they want to commit to.
- An open phase $\mathrm{open} = (\mathrm{open}_P \mathrm{open}_V)$: an interactive protocol involving P, V. At the end of the protocol, V outputs a value $b' \in \{0, 1\} \cup \perp$.

Provers and verifiers have access to some shared randomness.

Security requirements for the bit commitment scheme

- Perfect completeness: if P and V follow the protocol honestly then after the open phase, we always have $b = b'$. In particular, we never have $b' = \perp$.
- Perfect Hiding property: For any strategy comm_V^*, the transcript of $(\mathrm{comm}_P, \mathrm{comm}_V^*)$ should be independent of b.
- Perfect binding property (very informally): P should not be able to "change his mind" during the open phase.

Those requirements can also be extended to the imperfect setting.

On the binding property

Several ways to define binding property.

- Sum-binding property: $\forall\ \mathrm{comm}_P^*$,

$$\sum_{b' \in \{0,1\}} \max_{\mathrm{open}_P^*} \left(\Pr[\mathrm{V\ outputs}\ b' | (\mathrm{comm}_P^*, \mathrm{open}_P^*)]\right) \leq 1 + \varepsilon$$

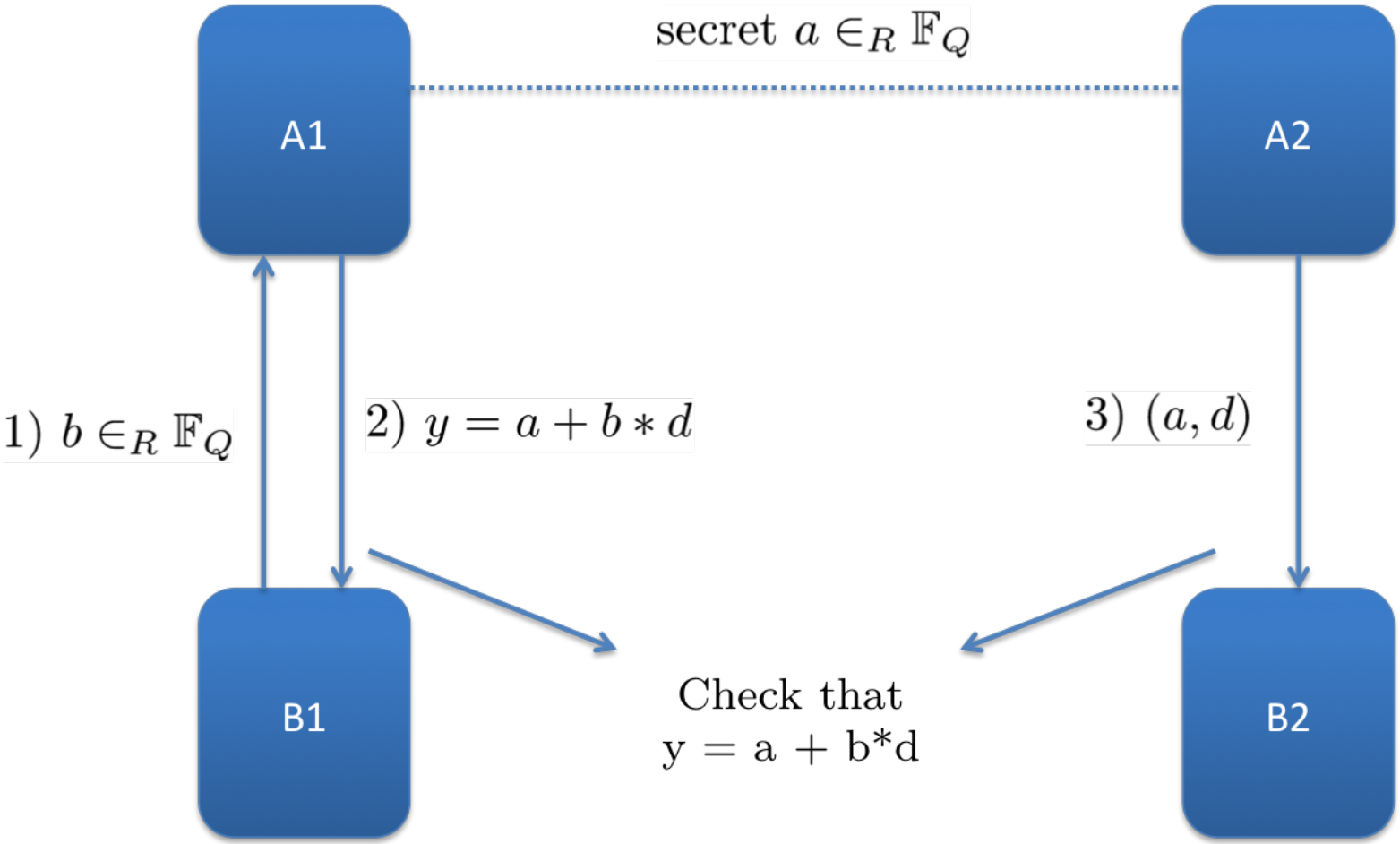
Weak definition. For example, it could allow a cheating strategy comm_P^* such that

- wp. $\frac{1}{2}$, P can reveal whatever value b' he wants and V will accept it.
- wp. $\frac{1}{2}$, V will always output $\perp$.

Still standard as a (weak) binding property. Well defined against quantum adversaries. We will present a strengthening of the sum-binding definition to avoid such behavior.

The relativistic F_Q bit commitment protocol. A = Prover.

Commit to a bit $d \in \{0, 1\}$.



- Non signaling condition: message 3 should be independent of message 1.

Proposition

The relativistic $\mathbb{F}_Q$ bit commitment protocol is perfectly hiding and $\sqrt{\frac{2}{Q}}$ sum-binding.

- Hiding property: perfectly satisfied if we can enforce different randomness (here $a \in_R \mathbb{F}_Q$) at each run of the commit phase.
- Sum-binding property: satisfied if message 3 is independent of message 1.

Let T be the time when B_1 sends message 1. Let T' be the time when B_2 receives message 3 and let D the distance between B_1 and B_2. If:

$$(T' - T) * c \leq D$$

then the non-signaling constraint is satisfied. Requires only to know the positions and timing of honest Bobs.

Hiding property:

- After the commit phase, a is a purely random string so $y = a \oplus b \cdot d$ is, from Bob's point of view, a totally random string.

How does a cheating $(\mathrm{comm}^*(P), \mathrm{open}^*(P))$ strategy for Alice look like?

- Alice 1 and Alice 2 can share an entangled state $|\psi\rangle$.
- Alice 1 receives $b \in_R \mathbb{F}_Q$ from Bob 1, performs a measurement defined by comm^* on her part of the entangled state and outputs $y \in \mathbb{F}_Q$.
- Alice 2, depending on the value d she wants to decommit to, perform a measurement defined by $\mathrm{open}^*(d)$ and outputs some value $a \in \mathbb{F}_Q$.

Relate to a CHSH game

We consider the following game

$CHSH_{Q,2}$

2 player entangled game between Alice and Bob. Alice receives a uniformly random $b \in \mathbb{F}_Q$, Bob receives a random $d \in \{0,1\}$. They produce respective outputs $y, a \in \mathbb{F}_Q$. They win iff. $y - a = x * y$ ($x * 0 = 0$ and $x * 1 = x$).

We can show the following:

Bit commitment to entangled games equivalence

If the relativistic $\mathbb{F}_Q$ bit commitment scheme is ε sum-binding then $\omega^*(CHSH_{Q,2}) = \frac{1}{2} + \frac{\varepsilon}{2}$.

Consider a strategy $S_0 = (\text{comm}_P^*, \text{open}_P^*)$ for the relativistic $\mathbb{F}_Q$ bit commitment scheme such that

$$\sum_d \frac{1}{2} \left(\Pr[\text{Alice succ. reveals } d | \text{comm}_P^*, \text{open}_P^*(d)]\right) = 1 + \varepsilon.$$

Transforming such a strategy into a strategy for the $CHSH_{Q,2}$ game

- A_1 and A_2 share the same entangled state $|\psi\rangle$.
- On input b, Adeline performs $COMM_P^*(b)$ to get outcome y.
- On input d, Bastian performs $OPEN_P^*(d)$ to get outcome a.
- They win $y - a = b * d$.

Let S_1 the above strategy for the $\text{CHSH}_{Q,2}$. We have $\omega^*(\text{CHSH}_{Q,2}|S_1) = \frac{1}{2} + \frac{\varepsilon}{2}$. From there we have the following statement:

From bit commitment to entangled games

If the relativistic $\mathbb{F}_Q$ bit commitment scheme is ε sum-binding then $\omega^*(CHSH_{Q,2}) \geq \frac{1}{2} + \frac{\varepsilon}{2}$.

In a very similar fashion, we can transform any strategy for the game $\omega^*(CHSH_{Q,2})$ into a cheating strategy for the $\mathbb{F}_Q$ commitment. So:

Bit commitment to entangled games equivalence

If the relativistic $\mathbb{F}_Q$ bit commitment scheme is ε sum-binding then $\omega^*(CHSH_{Q,2}) = \frac{1}{2} + \frac{\varepsilon}{2}$.

We can equivalently study the 2. We can show:

$$\omega^*(\mathrm{CHSH}_{Q,2}) \leq \frac{1}{2} + \frac{1}{\sqrt{2Q}}$$

How?, via consecutive measurements lemmata.

Theorem

Let P and Q be two projectors and $|\psi\rangle$ a quantum pure state. Let:

$$p = \mathrm{Tr}(P|\psi\rangle\langle\psi|P) \quad ; \quad q := \mathrm{Tr}(Q|\psi\rangle\langle\psi|Q) \quad ; \quad E := \mathrm{Tr}(QP|\psi\rangle\langle\psi|PQ).$$

If $p + q \geq 1$ then $E \geq p(p + q - 1)^2$.

- Idea of proof, use a geometric argument
- We write $|\psi\rangle = \cos(\alpha)|\psi_P\rangle + \sin(\alpha)|\psi_P^\perp\rangle$ st. $P|\psi\rangle = \cos(\alpha)|\psi_P\rangle$ and $|\psi_P\rangle$ of norm 1.
- Similarly, we write $|\psi\rangle = \cos(\beta)|\psi_Q\rangle + \sin(\alpha)|\psi_Q^\perp\rangle$ st. $Q|\psi\rangle = \cos(\beta)|\psi_Q\rangle$ and $|\psi_Q\rangle$ of norm 1.
- We have $p = \cos^2(\alpha)$; $q = \cos^2(\beta)$ and $E = p\mathrm{Tr}(Q|\psi_P\rangle\langle\psi_P|Q)$.

We now compute $E = \cos^2(\alpha) tr(Q|\psi_P\rangle\langle\psi_P|Q)$.

- Since $|\psi_Q\rangle \in Im(Q)$ and is of norm 1, we can construct an orthonormal basis $|e_1\rangle, \ldots, |e_k\rangle$ of $Im(Q)$ with $|e_1\rangle = |\psi_Q\rangle$.
- We can write $Q = \sum_{i=1}^{k} |e_i\rangle\langle e_i|$ so $Q \succcurlyeq |\psi_Q\rangle\langle\psi_Q|$.
- This implies $E \geq cos^2(\alpha)|\langle\psi_P|\psi_Q\rangle|^2$.

To conclude, use the Angle distance

Angle Distance

$Angle(|\phi\rangle, |\phi'\rangle) := Arccos(|\langle\phi|\phi'\rangle|)$. It's a distance (in particular, it has the triangular inequality).

- $\mathit{Angle}(|\psi\rangle, |\psi_P\rangle) = \alpha$; $\mathit{Angle}(|\psi\rangle, |\psi_Q\rangle) = \beta$. From triangle inequality: $\mathit{Arccos}(|\langle\psi_P|\psi_Q\rangle|) \leq \alpha + \beta$.
- This implies $|\langle\psi_P|\psi_Q\rangle| \geq \cos(\alpha + \beta)$. If $\alpha + \beta \leq \pi$, we get

$$|\langle\psi_P|\psi_Q\rangle|^2 \geq \cos^2(\alpha + \beta) \quad \Rightarrow \quad E \geq \cos^2(\alpha)\cos^2(\alpha + \beta)$$

- Using the trigonometric inequality

$$\cos^2(\alpha + \beta) \geq \cos^2(\alpha) + \cos^2(\beta) - 1$$

we can conclude that

$$E \geq \cos^2(\alpha)\left(\cos^2(\alpha) + \cos^2(\beta) - 1\right)^2 = p(p + q - 1)^2.$$

Optimality of the bound

- This bound is optimal for 1 dimensional projectors $P = |\psi_P\rangle\langle\psi_P|$ and $Q = |\psi_Q\rangle\langle\psi_Q|$ if $|\psi\rangle \in span(|\psi_P\rangle, |\psi_Q\rangle)$.
- If $p + q = 1$, we indeed have $E = 0$. Take for example $P = |0\rangle\langle 0|; Q = |1\rangle\langle 1|; |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
- Here: $p = tr(P|\psi\rangle\langle\psi|)q = tr(Q|\psi\rangle\langle\psi|) = \frac{1}{2}$ and $E = tr(PQ|\psi\rangle\langle\psi|QP) = 0$ since $QP = 0(matrix)$.

Theorem

Let P and Q be two projectors and $|\psi\rangle$ a quantum pure state. Let:

$$p = \mathrm{Tr}(P|\psi\rangle\langle\psi|) \quad ; \quad q := \mathrm{Tr}(Q|\psi\rangle\langle\psi|) \quad ; \quad E := \mathrm{Tr}(QP|\psi\rangle\langle\psi|PQ).$$

If $p + q \geq 1$ then $E \geq p(p + q - 1)^2$.

Extension to mixed states:

Theorem

Let P and Q be two projectors and ρ a quantum mixed state. Let:

$$p = \mathrm{Tr}(P\rho) \quad ; \quad q := \mathrm{Tr}(Q\rho) \quad ; \quad E := \mathrm{Tr}(QP\rho PQ).$$

If $p + q \geq 1$ then $E \geq p(p + q - 1)^2$.

- ρ is in some quantum register A. Consider a purification $|\psi\rangle$ of ρ in registers AB.
- P and Q are projectors on A. Let $P' = P \otimes I_B$ and $Q' = Q \otimes I_B$, which are projectors on AB. We have

$$p = \mathrm{Tr}(P\rho) = \mathrm{Tr}(P'|\psi\rangle\langle\psi|) \quad ; \quad q = \mathrm{Tr}(Q\rho) = \mathrm{Tr}(Q'|\psi\rangle\langle\psi|)$$

- If we define $E' = \mathrm{Tr}(Q'P'|\psi\rangle\langle\psi|P'Q')$, we can easily show that $E' = E$.
- By using the theorem on pure states, we can conclude.

Applications to quantum encodings

- 2 parties Alice and Bob, which share a quantum state

$$\sigma = \sum_{x_0,x_1 \in \{0,1\}} p_{x_0,x_1} |x_0, x_1\rangle\langle x_0, x_1|_{X_0,X_1} \otimes \sigma_B(x_0, x_1).$$

- Bob can guess x_0 with probability p_0, Bob can guess x_1 with probability p_1. We can assume wlog that this can be done via projective measurements (eventually by adding ancilla qubits to $\sigma_B(x_0, x_1)$).
- We relate p_0,p_1 and the probability of learning (x_0, x_1).

Proposition

Suppose Alice and Bob share a state

$$\sigma = \sum_{x_0,x_1 \in \{0,1\}} p_{x_0,x_1} |x_0, x_1\rangle\langle x_0, x_1|_A \otimes \sigma_B(x_0, x_1).$$

If there is a strategy for Bob to guess x_0 wp. p_0 and x_1 wp. p_1 then there exists a strategy to guess $x_0 \oplus x_1$ wp. $(p_0 + p_1 - 1)^2$.

Proof:

- Let $P^0 = \{P^0_x\}_{x\in\{0,1\}^n}$ and $P^1 = \{P^1_x\}_{x\in\{0,1\}^n}$ those measurements. For any $b \in \{0,1\}$, each P^b_x is a projector and $\sum_{x\in\{0,1\}^n} P^b_x = I$ (which also implies $P^b_x P^b_{x'} = \delta_{x,x'} P^b_x$).

Using this strategy, the probability that Bob respectively guesses x_0 and x_1 are:

$$p_0 = \sum_{x_0,x_1} p_{x_0,x_1} \mathrm{Tr}(P^0_{x_0} \sigma_B(x_0,x_1)) \quad ; \quad p_1 = \sum_{x_0,x_1} p_{x_0,x_1} \mathrm{Tr}(P^1_{x_0} \sigma_B(x_0,x_1))$$

Projectors on winning subspace

Let the following 2 projectors

$$W^0 = \sum_{x_0,x_1} |x_0,x_1\rangle\langle x_0,x_1| \otimes P^0_{x_0} \quad ; \quad W^1 = \sum_{x_0,x_1} |x_0,x_1\rangle\langle x_0,x_1| \otimes P^1_{x_1}.$$

These are the projectors on the winning subspace. We have $p_0 = tr(W^0\sigma)$ and $p_1 = tr(W^1\sigma)$.

If Bob applies, P^0 and then P^1, the probability of getting both outcomes correctly is

$$p_{01} = \sum_{x_O,x_1} p_{x_0,x_1} \mathrm{Tr}(P^1_{x_1} P^0_{x_0} \sigma_B(x_0,x_1) P^0_{x_0} P^1_{x_1}).$$

which can be written also $p_{01} = \mathrm{Tr}(W^1 W^0 \sigma W^0 W^1)$.

Similarly, we define

$$p_{10} = \mathrm{Tr}(W^0 W^1 \sigma W^1 W^0).$$

x_0, x_1 are bits so $p_0, p_1 \geq \frac{1}{2}$. We can use the consecutive projection lemma to get

$$p_{01} \geq p_0(p_0 + p_1 - 1)^2 \quad ; \quad p_{10} \geq p_1(p_0 + p_1 - 1)^2.$$

To conclude, we use the following strategy to try to learn (x_0, x_1):

- wp. $\frac{1}{2}$, Bob applies measurement P^0 and gets y_0 then P^1 on the resulting state and gets y_1, he outputs (y_0, y_1).
- wp. $\frac{1}{2}$ Bob applies measurement P^1 and gets y_1 then P^0 on the resulting state and gets y_0, he outputs (y_0, y_1).

$$\Pr[\text{Bob guesses } (x_0, x_1)] \geq \frac{1}{2}(p_{01} + p_{10}) \geq p(2p-1)^2.$$

where recall that $p = \frac{p_0 + p_1}{2}$. If needed:

$$\Pr[\text{Bob guesses } (x_0, x_1)] \geq \max\{p_0, p_1\} \cdot (2p-1)^2.$$

Improvement: if we want to learn $x_0 \oplus x_1$.

Lemma

Let P and Q be two projectors and ρ a quantum mixed state. Let:

$$p = \mathrm{Tr}(P\rho)\,; q := \mathrm{Tr}(Q\rho)\,; E := \mathrm{Tr}(QP\rho PQ + (I-Q)(I-P)\rho(I-P)(I-Q))$$

If $p + q \geq 1$ then $E \geq (p+q-1)^2$.

Proposition

Suppose Alice and Bob share a state

$$\sigma = \sum_{x_0, x_1 \in \{0,1\}} p_{x_0,x_1} |x_0, x_1\rangle\langle x_0, x_1|_A \otimes \sigma_B(x_0, x_1).$$

If there is a strategy for Bob to guess x_0 wp. p_0 and x_1 wp. p_1 then there exists a strategy to guess $x_0 \oplus x_1$ wp. $(p_0 + p_1 - 1)^2$.

This proposition is actually tight for non trivial examples.

Extension to $x_0, x_1 \in \{0,1\}^n$.

- The above arguments (for learning (x_0, x_1)) can be extended without problems.
- But we still need the constraint

$$\Pr[\text{Bob can guess } x_0] + \Pr[\text{Bob can guess } x_1] \geq 1.$$

- The improvement when considering $x_0 \oplus x_1$ is not known to work when $x_0, x_1 \in \{0,1\}^n$.

- Performing consecutive measurement doesn't seem to be the best strategy in most cases.
- This bound is even worse sometimes than random guessing.
- We don't of generic form to do better than consecutive measurements.
- It will still be good enough for many cases, even if it's rarely tight.

Idea used several times:

- Gentle measurements
- Two provers in isolation
- FF15,CCL16,CL17

CHSH

2 player entangled game between Alice and Bob. They receive respective uniformly random inputs $x, y \in \{0,1\}$ and produce respective outputs $a, b \in \{0,1\}$. They win iff. $a \oplus b = x \cdot y$.

Idea: use the $\oplus$ learning lemma to bound the value of the CHSH. To do this, fix a cheating strategy S for Alice and Bob

- Let Alice perform her strategy on input x to get output a. Let $X_0 = a$ and $X_1 = x \oplus a$. Notice that $X_0 \oplus X_1 = x$.
- The winning condition of CHSH can be rephrased as follows
  1. if $y = 0$, Bob must output $b = a$.
  2. if $y = 1$, Bob must output $b = a \oplus y$
- This means that:

$$\Pr[\text{Alice and Bob win CHSH using S}] = \frac{1}{2} \sum_{y \in \{0,1\}} (\Pr[\text{Bob guesses } X_y]$$

From non signaling, we know that $E := \Pr[\text{Bob guesses } x] = \frac{1}{2}$. If we define $V := \frac{1}{2}\sum_{y\in\{0,1\}} (\Pr[\text{Bob guesses } X_y]) =$
$\Pr[\text{Alice and Bob win CHSH using S}]$., we have

$$\frac{1}{2} = E \geq (2V-1)^2 \Rightarrow V \leq \cos^2(\pi/8).$$

Extension to $CHSH_{Q,2}$

$CHSH_{Q,2}$

2 player entangled game between Alice and Bob. Alice receives a uniformly random $x \in \mathbb{F}_Q$, Bob receives a random $y \in \{0,1\}$. They produce respective outputs $a, b \in \mathbb{F}_Q$. They win iff. $a + b = x * y$ $(x * 0 = 0 \text{ and } x * 1 = x)$.

Again, fix a cheating strategy S for Alice and Bob. Let $X_0 = a$ and $X_1 = x + a$. Again, notice that $X_1 - X_0 = x$ so if Bob learns (X_0, X_1), he can learn x. We write again

$$E := \Pr[\text{Bob guesses } x]$$

and

$$V := \frac{1}{2} \sum_{y \in \{0,1\}} (\Pr[\text{Bob guesses } X_y])$$

$$= \Pr[\text{Alice and Bob win } CHSH_{2,Q} \text{ using S }]$$

Applying the consecutive measurements lemma, we have

$$\frac{1}{Q} = E \geq V(2V-1)^2 \geq \frac{1}{2}(2V-1)^2.$$

From there, we get $V \leq \frac{1}{2} + \frac{1}{\sqrt{2Q}}$. Since this is true for any cheating strategy S, we conclude that

$$\omega^*(CHSH_{Q,2}) \leq \frac{1}{2} + \frac{1}{\sqrt{2Q}}$$

Used crucially the fact that there is a single possible opening for each d.

Relativistic string commitment

Relativistic string commitment

- Committing to a single bit is not always enough.
- We would like to commit to string of bits at the same time and say something about this commitment
- But the sum-binding definition is weak and is not well suited for such statements. We have also access to the special binding property
- Having access to those, can we manage to say something about string commitment? Yes but requires some work.

String sum binding

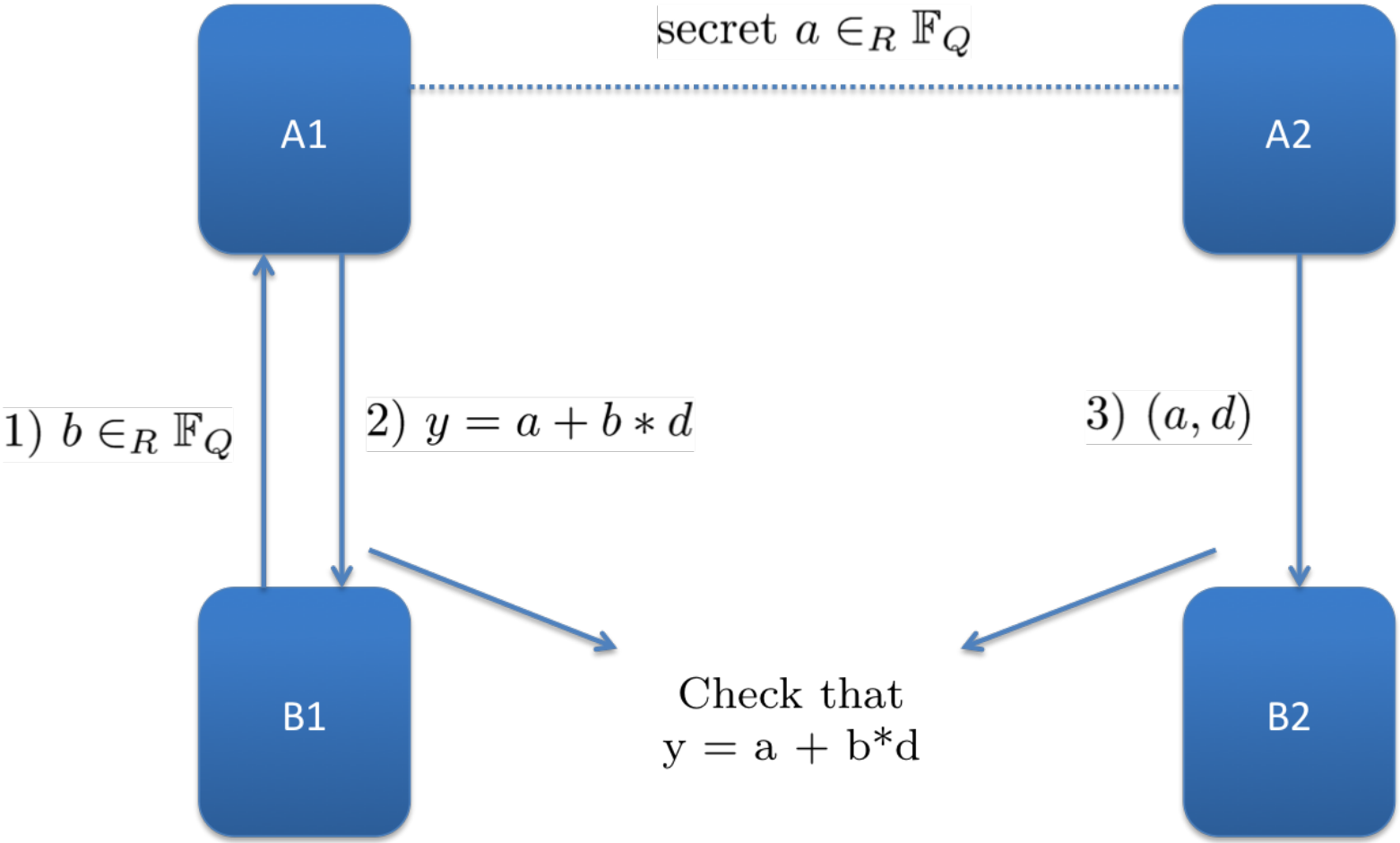
A minimal requirement we would want from a T-string commitment is the following

$$\forall(\mathrm{comm}_P^*, \mathrm{open}_P^*)$$

$$\sum_{x \in \mathbb{F}_T} \Pr[\textit{Alice succ. reveals } x | (\mathrm{comm}_P^*, \mathrm{open}_P^*(x))] \leq 1 + \varepsilon.$$

Proposal for string commitment: T-generalization of the F_Q bit commitment

Commit to a string $d \in \mathbb{F}_T$.



- Non signaling condition: msg. 3 should be independent of msg. 1.

Again, we can reduce to the $CHSH_{Q,T}$ game.

$CHSH_{Q,T}$

2 player entangled game between Alice and Bob. Alice receives a uniformly random $x \in \mathbb{F}_Q$, Bob receives a random $y \in \mathbb{F}_T$. They produce respective outputs $a, b \in \mathbb{F}_Q$. They win iff. $a + b = x * y$.

Again, we map a cheating strategy for the string commitment to an entangled strategy for the $CHSH_{Q,T}$ game.

Proposition

The above mentioned relativistic T-string commitment scheme is $(T\omega^*(CHSH_{Q,T}) - 1)$ sum-binding

We need to bound $\omega^*(CHSH_{Q,T})$.

Cases where we know the value:

- $\omega^*(CHSH_{Q,Q}) \leq O(\frac{1}{\sqrt{Q}})$.
- When Q is an even power of a prime, $\omega(CHSH_{Q,Q}) = \omega^*(CHSH_{Q,Q}) = \Theta(\frac{1}{\sqrt{Q}})$.

When Q is an even power of a prime, the resulting Q-string commitment scheme is $\Theta(\sqrt{Q})$ sum-binding (we hoped for ε sum-binding with $\varepsilon \ll 1$).

The scheme is still $\frac{1}{Q}$ special binding so in the case of string commitment, special binding doesn't imply sum-binding.

Can we say interesting things for some values of $T > 2$? Yes.

Proposition

$$\omega^*(CHSH_{Q,T}) \leq \frac{1}{T} + \frac{4}{Q^{1/3}}.$$

Idea, use a generalization of the consecutive measurement lemma.

Corollary

The F_Q based T-string commitment is $\frac{4T}{Q^{1/3}}$ sum-binding. If we want an 2^{-k} sum-binding protocol for some $k \in \mathbb{N}$, we can take $Q = 64T^3 2^{3k}$.

Recall that each message in the protocol is $\lceil \log(Q) \rceil$ so we can achieve an n-bit string commitment (i.e. $T = 2^n$) with the F_Q protocol where each message is $3n + 3k + 8$ bits.

Now we need to prove the proposition and dive into the generalization of consecutive measurements.

Again, the most generic way to look at this is to go back through the notion of encodings.

Proposition

Let $P_1, \ldots, P_T$ be projectors and $|\psi\rangle$ a quantum pure state. Let:
$p_i = \mathrm{Tr}(P_i|\psi\rangle\langle\psi|P_i)$; $V := \frac{1}{T}\sum_i p_i$ *and*
$E := \frac{1}{T(T-1)}\sum_{i,j\neq i} \mathrm{Tr}(P_jP_i|\psi\rangle\langle\psi|P_iP_j)$. *We have*

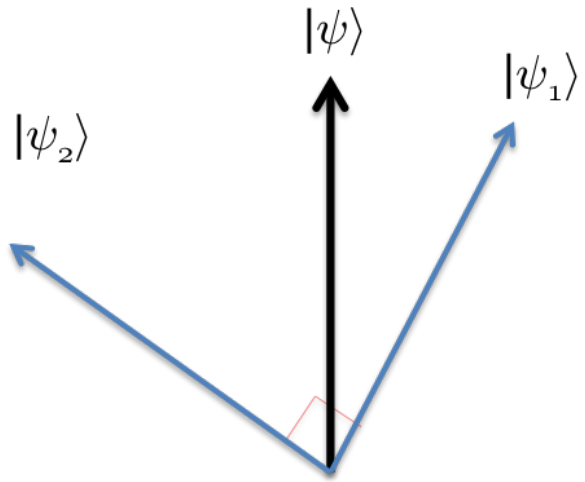
$$E \geq \frac{1}{64}(V - \frac{1}{T})^3.$$

Notice that this is an average case statement and not a worst case statement. Also, the bound is useful only for $V > \frac{1}{T}$.

Tight in the sense that we can find an example with $V = \frac{1}{T}$ and $E = 0$. Take $|\psi\rangle = \frac{1}{\sqrt{T}}\sum_{i=1}^{T}|i\rangle$ and $P_i = |i\rangle\langle i|$.

Difficulty of the statement

Recall for $T = 2$, we could have $p_1 = p_2 = \frac{1}{2}$ and $E = 0$. Idea behind this worst case:



with $P_i = |\psi_i\rangle\langle\psi_i|$ and $|\langle\psi_1|\psi_2\rangle| = 0$. If those 3 vectors lie in a 2 dimensional subspace, we have $V = \frac{1}{2}$ and $E = 0$.

Known similar results?

Yes, proven for the study of sigma protocols with special soundness (i.e. in a similar context)

Proposition (Unr12)

Let $P_1, \ldots, P_T$ be projectors and $|\psi\rangle$ a quantum pure state. Let:
$p_i = \mathrm{Tr}(P_i|\psi\rangle\langle\psi|P_i)$; $V := \frac{1}{T}\sum_i p_i$ *and*
$E := \frac{1}{T(T-1)}\sum_{i,j\neq i} \mathrm{Tr}(P_j P_i|\psi\rangle\langle\psi|P_i P_j)$. *If* $V \geq \frac{1}{\sqrt{T}}$ *then*

$$E \geq \frac{T}{(T-1)} V(V^2 - \frac{1}{T}).$$

Proposition

Let $P_1, \ldots, P_T$ be projectors and $|\psi\rangle$ a quantum pure state. Let:
$p_i = \mathrm{Tr}(P_i|\psi\rangle\langle\psi|P_i)$; $V := \frac{1}{T}\sum_i p_i$ *and*
$E := \frac{1}{T(T-1)}\sum_{i,j\neq i} \mathrm{Tr}(P_jP_i|\psi\rangle\langle\psi|P_iP_j)$. *We have*

$$E \geq \frac{1}{64}(V - \frac{1}{T})^3.$$

We define $|\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{p_i}}$. One can check that the $|\psi_i\rangle$ are of norm 1 and that $|\langle\psi|\psi_i\rangle|^2 = p_i$. Fix any $i, j \neq i$. As in the $T = 2$, we get

$$E_{i,j} := \mathrm{Tr}(P_jP_i|\psi\rangle\langle\psi|P_iP_j) = p_i\mathrm{Tr}(P_j|\psi_i\rangle\langle\psi_i|P_j) \geq p_i|\langle\psi_i|\psi_j\rangle|^2.$$

with $E = \frac{1}{T(T-1)}\sum_{i,j\neq i} E_{i,j}$.

Extremal case: when can we get $E = 0$? If for any $i, j \neq i$, we have

- $\langle \psi_i | \psi_j \rangle = 0$.
- OR $\langle \psi | \psi_i \rangle = 0$.

a quick analysis gives $V = \frac{1}{T} \sum_i |\langle \psi | \psi_i \rangle|^2 \leq \frac{1}{T}$.

By a counterpositive, if $V > \frac{1}{T}$ then $E > 0$.

So we need to show that the $|\langle\psi_i|\psi_j\rangle|^2$ are not too small on average. We show the following

Lemma

Let

$$S = T \cdot V = \sum_i |\langle\psi|\psi_i\rangle|^2 \quad ; \quad C = \sum_{i,j\neq i} |\langle\phi_i|\phi_j\rangle|^2.$$

We have

$$S \leq 1 + \sqrt{\frac{(n-1)C}{n}}.$$

Proof of the lemma

Let $M = \sum_{i=1}^{T} |\psi_i\rangle\langle\psi_i|$. Let $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_T$ the T (not necessarily distinct) eigenvalues of M. We first have

$$\sum_{i=1}^{T} \lambda_i = \mathrm{Tr}(M) = \sum_{i=1}^{T} \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|) = T.$$

Notice that

$$\lambda_1 = \max_{|\Omega\rangle} \sum_{i=1}^{T} |\langle\psi|\Omega\rangle|^2 \geq S.$$

Next we write $M^2 = \sum_{i,j=1}^{T} \langle\psi_i|\psi_j\rangle|\psi_i\rangle\langle\psi_j|$ and

$$\sum_{i=1}^{T} \lambda_i^2 = tr(M^2) = \sum_{i,j=1}^{T} \langle\psi_i|\psi_j\rangle^2 \leq \sum_{i,j=1}^{T} |\langle\psi_i|\psi_j\rangle|^2 = T + C$$

This gives us

$$T + C \geq \sum_{i=1}^{T} \lambda_i^2 = \lambda_1^2 + \sum_{i=2}^{T} \lambda_i^2 \geq S^2 + \frac{(T-S)^2}{T-1}$$

From there, we can conclude $S \leq 1 + \sqrt{\frac{(T-1)C}{T}}$ or equivalently

$$V \leq \frac{1}{T} + \frac{T-1}{T}\sqrt{\frac{1}{T(T-1)}\sum_{i,j\neq i} |\langle \phi_i | \phi_j \rangle|^2}. \quad (1)$$

Recall that we want to relate $V = \frac{1}{T}\sum_i |\langle \phi | \phi_i \rangle|^2$ and $E = \frac{1}{T(T-1)}\sum_{i,j\neq i} |\langle \phi | \phi_i \rangle|^2 |\langle \phi_i | \phi_j \rangle|^2$.

Easy case: if $\forall i, |\langle \phi | \phi_i \rangle|^2 = V$ (symmetric case), we can rewrite $E = \frac{V}{T(T-1)}\sum_{i,j\neq i} |\langle \phi_i | \phi_j \rangle|^2$ and plugging this in Eq 1:

$$V \leq \frac{1}{T} + \frac{T-1}{T}\sqrt{\frac{E}{V}} \quad \Rightarrow \quad E \geq \left(\frac{T}{T-1}\right)^2 V(V - \frac{1}{T})^2$$

General case, more cumbersome calculations.

- Let $Z = \{i : p_i \geq \frac{V}{\kappa}\}$ for a parameter $\kappa > 1$ that will be fixed later.
- $S_Z := \sum_{i \in Z} p_i \geq \frac{1}{(1+\frac{1}{\kappa-1})} S$. $C_Z = \sum_{i,j \neq i \in Z} |\langle \phi_i | \phi_j \rangle|^2$.

$$S_Z \leq 1 + \sqrt{C_Z}.$$

$$\begin{aligned} E &= \frac{1}{T(T-1)} \sum_{i,j \neq i} |\langle \phi | \phi_i \rangle|^2 |\langle \phi_i | \phi_j \rangle|^2 \\ &\geq \frac{1}{T(T-1)} \sum_{i,j \neq i \in Z} |\langle \phi | \phi_i \rangle|^2 |\langle \phi_i | \phi_j \rangle|^2 \\ &\geq \frac{1}{T(T-1)} \sum_{i,j \neq i \in Z} \frac{V}{\kappa} |\langle \phi_i | \phi_j \rangle|^2 = \frac{V C_Z}{\kappa T(T-1)} \end{aligned}$$

$$S_Z \leq 1 + \sqrt{\frac{\kappa E T(T-1)}{V}} \leq 1 + T\sqrt{\frac{\kappa E}{V}}.$$

$$S \leq (1 + \frac{1}{\kappa - 1})S_Z \leq (1 + \frac{1}{\kappa - 1})(1 + T\sqrt{\frac{\kappa E}{V}}).$$

$$V \leq (1 + \frac{1}{\kappa - 1})(\frac{1}{T} + \sqrt{\frac{\kappa E}{V}}).$$

Optimization in κ, relation between E and V. $\kappa = \max\left(2, (\frac{V}{T^2 E})^{1/3}\right)$. We get

$$E \geq \frac{1}{64}(V - \frac{1}{T})^3.$$

Interpretation in terms of encodings

Proposition (General learning lemma for pairs of strings)

Suppose Alice and Bob share a state

$$\sigma = \sum_{x_1,\ldots,x_n} p_{x_1,\ldots,x_n} |x_1,\ldots,x_n\rangle\langle x_1,\ldots,x_n|_A \otimes \sigma_B(x_1,\ldots,x_n).$$

If for each i, there is a strategy for Bob to guess x_i wp. p_i then there exists a couple (i,j) and a strategy for Bob to guess (x_i,x_j) wp.

$$p_{i,j} \geq \frac{1}{64n^3}\left(\left(\sum_{i=1}^{n} p_i\right) - 1\right)^3.$$

Proposition (Counterpositive: the special soundness lemma)

Suppose Alice and Bob share a state

$$\sigma = \sum_{x_1,\ldots,x_n} p_{x_1,\ldots,x_n} |x_1,\ldots,x_n\rangle\langle x_1,\ldots,x_n|_A \otimes \sigma_B(x_1,\ldots,x_n).$$

If for each $i, j \neq i$, Bob can guess (x_i, x_j) wp. $\leq \varepsilon$ then

$$\sum_i \Pr[\textit{Bob can guess } x_i] \leq 1 + 4n\varepsilon^{1/3}.$$

We can recognize here already the relation between the sum binding property and the special binding property. If $\varepsilon \leq \frac{2^{-3k}}{(4n)^{1/3}}$ for some k then $\sum_i \Pr[\text{Bob can guess } x_i] \leq 1 + 2^{-k}$.

Proposition

$$\omega^*(CHSH_{Q,T}) \leq \frac{1}{T} + \frac{4}{Q^{1/3}}.$$

Proof:

- Fix Alice's input/output pair $x, a \in \mathbb{F}_Q$. Let $X_y = a + x * y$. Bob has a random $y \in \mathbb{F}_P$ and wins the game if he guesses X_y.
- For any $y, y' \neq y$, we have $x = \frac{X_{y'} - X_y}{y' - y}$ so if Bob can guess X_y and X'_y then he can guess x. On average on x, a, this happens wp. $\frac{1}{Q}$ by non-signaling.
- By using the special soundness lemma, we have

$$\omega^*(CHSH_{Q,T}) = \frac{1}{T} \sum_{y \in \mathbb{F}_P} \Pr[\text{Bob can guess } X_y] \leq \frac{1}{T} + \frac{4}{Q^{1/3}}.$$

- We deal with averaging on (x, a) similarly as for the $T = 2$ case.

Corollary

The F_Q based T-string commitment is $\frac{4T}{Q^{1/3}}$ sum-binding. If we want an 2^{-k} sum-binding protocol for some $k \in \mathbb{N}$, we can take $Q = 64T^3 2^{3k}$.

Parallel repetition of bit commitment

- We proved the sum-binding property for a string commitment.
- Problem: We can only reveal the whole string or nothing. In most cases, it's nice to be able to reveal some bits of the string.
- With the special soundness lemma, we can also prove that the parallel repetition of the $\mathbb{F}_Q$ bit commitment preserves the sum-binding property as a string commitment.

- The generic $\mathbb{F}_Q$ Q-string commitment scheme is not sum-binding even though it is special binding.
- Can we still say something about its security as a string commitment?
- Yes: $\mathrm{distributionally}^+$ sum-binding.

Definition

A bit commitment is ε distributionally$^+$ sum-binding if $\forall$ comm_P^*, there is a pr. distr. r st $\forall d$ and $\forall \mathrm{open}_P^*(d)$, we have

$$\Pr[\mathrm{V\ outputs}\ d|(\mathrm{comm}_P^*, \mathrm{open}_P^*(d))] \leq r(d) + \varepsilon.$$

Proposition

The $\mathbb{F}_Q$ Q-string commitment is $\frac{4}{Q^{1/6}}$ $distributionally^+$ secure against quantum adversaries.

Relativistic zero-knowledge for *NP*

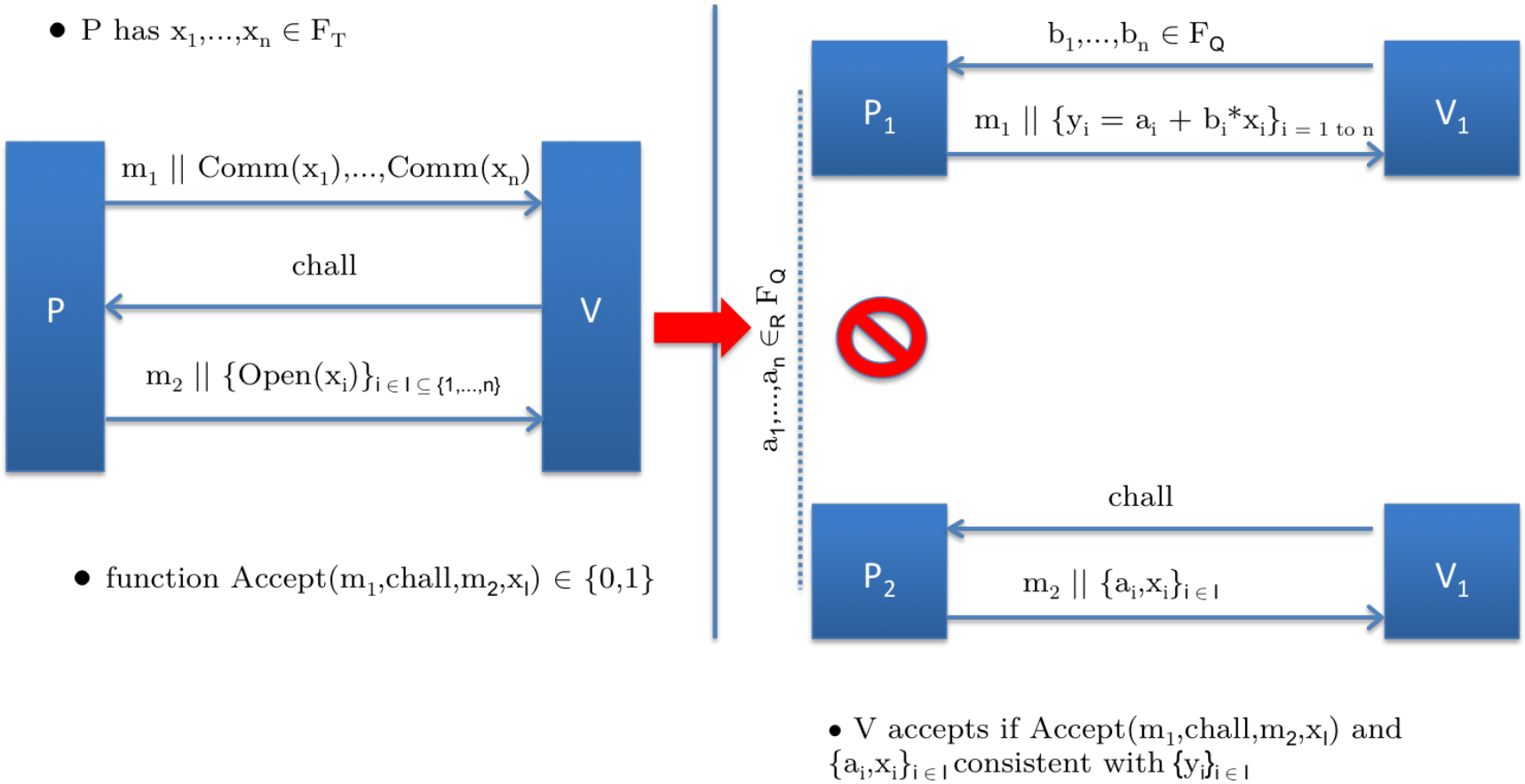
Sigma protocols

Consider protocols between a single prover P and a single verifier V of the following form:

1. P commits to n bits (or strings) $x_1, \ldots, x_n$.
2. V sends a challenge *chall* to the prover.
3. Depending on *chall*, P opens some of the x_i. He also sends an answer a to the verifier.

Many (zero-knowledge) protocols can be expressed in the above form.

Using the $\mathbb{F}_Q$ relativistic bit commitment in order to transform a Σ-protocol into a relativistic protocol.



In order to analyze cheating provers, the relativistic protocol can then be directyl transformed into an entangled 2 player game between P_1 and P_2.

A zero-knowledge protocol for a language L is an interactive protocol between a prover P and verifier V, parametrized by a security parameter k, with the following properties:

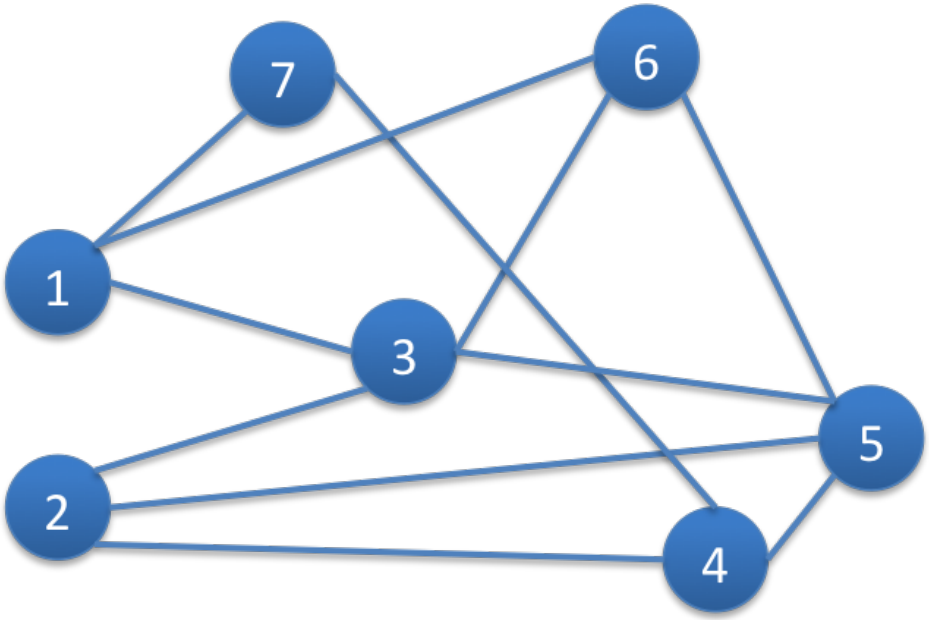
- Completeness: $\forall x \in L$, $\Pr[\mathrm{V\ accepts}] \geq 1 - \mathit{negl}(k)$.
- Soundness: $\forall x \notin L$, $\Pr[\mathrm{V\ accepts}] \leq \mathit{negl}(k)$.
- Zero-knowledge: there is polynomial time simulator S st. $\forall x \in L$, $\forall$ cheating V^* and $\forall \rho$ (auxiliary state),

$$\mathrm{StatDiff}\left(S_{V^*}(x,\rho), \mathit{view}_{V^*}(x,\rho)\right) \leq \mathit{negl}(k).$$

where $\mathit{view}_{V^*}(x,\rho)$ is verifier's view of the protocol (the transcript as well as his quantum and classical registers).

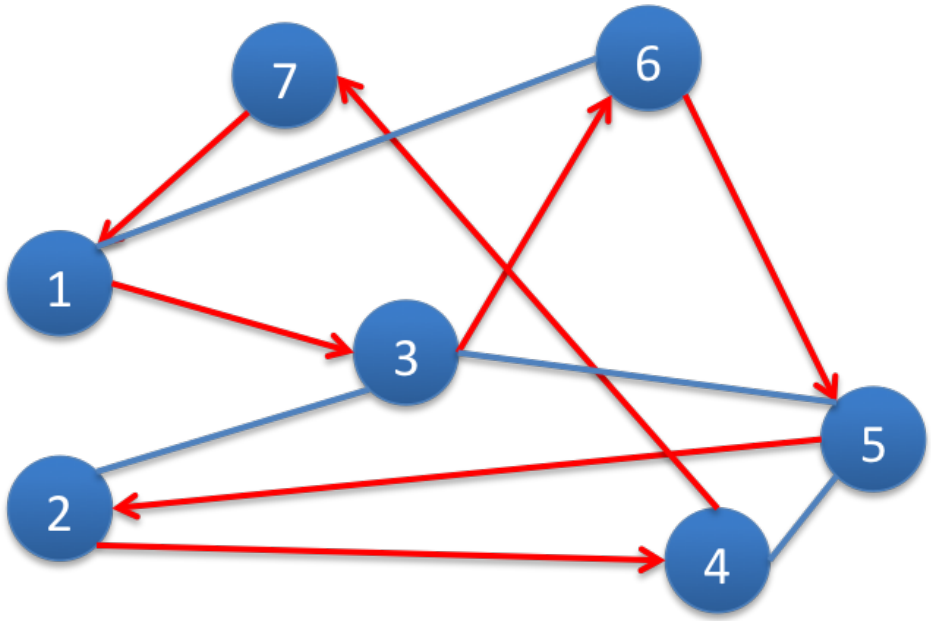
Hamiltonian cycle problem

We consider an undirected graph $G = (V, E)$.



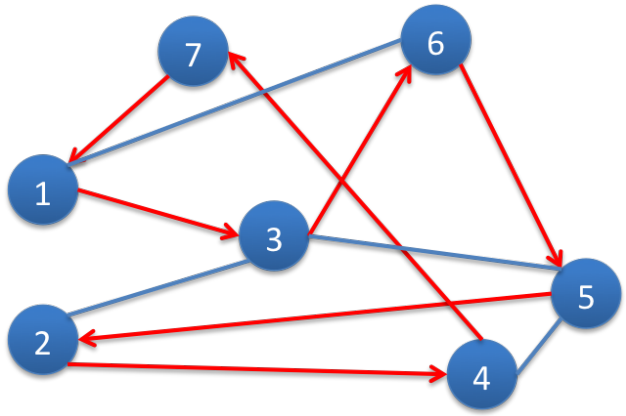
Hamiltonian cycle problem

We consider an undirected graph $G = (V, E)$ without self loops.



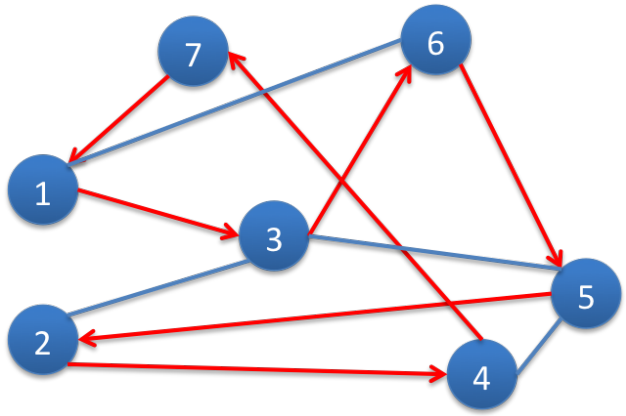
A Hamiltonian cycle is a cycle going through each vertex exactly once. Determining whether a graph contains a Hamiltonian cycle is an NP-complete problem.

The adjacency matrix M_G of G is a $V \times V$ st. $M_G(i,j) = 1 iff . (i,j) \in E$.
For our example:



$$M_G = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

The adjacency matrix M_G of G is a $V \times V$ st. $M_G(i,j) = 1$ iff. $(i,j) \in E$.



$$M_G = \begin{pmatrix} 0 & 0 & \mathbf{1} & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \mathbf{1} & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & \mathbf{1} & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

If you are given the $\mathbf{1}$ corresponding to a Hamiltonian cycle, one can check whether it indeed forms such a cycle or not. We don't need to look at the rest of the matrix to determine this.

Zero-knowledge protocol for Hamiltonian cycle using bit commitment

1. The prover picks a random permutation $\Pi : V \to V$. He commits to each of the bits of the adjacency matrix $M_{\Pi(G)}$ of $\Pi(G)$.
2. The verifier sends a random bit (called the challenge) $chall \in \{0, 1\}$ to the prover.
3.
   - If $chall = 0$, the prover decommits to all the elements of $M_{\Pi(G)}$, and reveals Π.
   - If $chall = 1$, he reveals only the bits (of value 1) of the adjacency matrix that correspond to a Hamiltonian cycle $\mathcal{C}'$ of $\Pi(G)$.
4. The verifier checks that these decommitments are valid and correspond, for $chall = 0$ to $M_{\Pi(G)}$ and, for $chall = 1$, to a Hamiltonian cycle.

The relativistic zero-knowledge protocol for Hamiltonian cycle will exactly be plugging in the $\mathbb{F}_Q$ parallel relativistic bit commitment in the zero-knowledge protocol.

Relativistic zero knowledge protocol for Hamiltonian cycle

Input — The provers and the verifiers are given a graph $G = (V, E)$.
Auxiliary Input — The provers P_1 and P_2 know a Hamiltonian cycle $\mathcal{C}$ of G.
Preprocessing — P_1 and P_2 agree beforehand on a random permutation $\Pi : V \to V$ and on an $n \times n$ random matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$.

1. Commitment to each bit of $M_{\Pi(G)}$: V_1 sends a matrix $B \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of B is chosen uniformly at random in $\mathbb{F}_Q$. P_1 outputs the matrix $Y \in \mathcal{M}_n^{\mathbb{F}_Q}$ such that $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$.
2. The verifier sends a random bit $chall \in \{0, 1\}$ to the prover.
3. - If $chall = 0$, P_2 decommits to all the elements of $M_{\Pi(G)}$, *i.e.* he sends all the elements of A to V_2 and reveals Π.
   - If $chall = 1$, P_2 reveals only the bits (of value 1) of the adjacency matrix that correspond to a Hamiltonian cycle $\mathcal{C}'$ of $\Pi(G)$, *i.e.* for all edges (u, v) of $\mathcal{C}'$, he sends $A_{u,v}$ as well as $\mathcal{C}'$.
4. The verifier checks that those decommitments are valid:
   - if $chall = 0$, the prover's opening A must satisfy $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$.
   - if $chall = 1$, the prover's opening A must satisfy $\forall (u, v) \in \mathcal{C}',\ Y_{u,v} = A_{u,v} + B_{u,v}$.

What do we need to prove?

- **Completeness**: The single prover/verifier zero-knowledge protocol for Hamiltonian cycle is perfectly complete and so is the $\mathbb{F}_Q$ bit commitment scheme. If both parties are honest and we are in a yes instance, the protocol always succeeds.
- **Soundness**: This will be the hardest part. An extra difficulty will arise because there are several valid openings.
- **Zero-knowledge**: The commitment is perfectly hiding and the original zero-knowledge protocol is perfectly zero-knowledge. We will show that this relativistic zero-knowledge protocol remains perfectly zero-knowledge.

Generic idea to use special learning lemma for bounding entangled games

A game is projective if for each x, a, y there is a unique $b_{x,a}(y)$ such that the players win the game on inputs (x, y) and outputs (a, b).

When fixing (x, a), the probability of winning the game is the probability for Bob of guessing $b_{x,a}(y)$. If we can bound the probability of guessing a couple $b_{x,a}(y), b_{x,a}(y')$ for $y \neq y$ then we can use the special learning lemma to bound the value of the game.

The projective property is crucial for this argument.

All the CHSH type games we considered were projective (even unique) so the argument worked well.

In terms of commitment, given a fixed transcript for the commit phase and a fixed string s, there is a unique opening string for s.

However, in the zero-knowledge protocol, there are many valid strings that can be opened (one for each permutation).

Consider a graph G with no Hamiltonian cycle. The cheating provers must win the following entangled game in order to convince the verifiers.

RZK-HAM game

- P_1 receives a matrix $B \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of B is chosen uniformly at random in $\mathbb{F}_Q$. P_2 receives a random input bit *chall*.
- P_1 outputs a matrix $Y \in \mathcal{M}_n^{\mathbb{F}_Q}$. If $chall = 0$ then P_2 outputs a permutation Π and a matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$. If $chall = 1$ then P_2 outputs a cycle $\mathcal{C}'$ and n strings $\{A'_{(u,v)}\}_{(u,v)\in\mathcal{C}'}$ in $\mathbb{F}_Q$.
- If $chall = 0$, the two players win if $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$. If $chall = 1$, the two players win if for all edges (u, v) of $\mathcal{C}'$, $Y_{u,v} = A_{u,v} + B_{u,v}$, which corresponds to revealing 1 for each edge of the cycle $\mathcal{C}'$.

An entangled 2 player game G is said to be α-projective iff.

$$\forall x, y, a \ |\{b : \text{A and B win G on inputs } (x, y) \text{ and ouputs } (a, b)\}| \leq \alpha.$$

Proposition

The RZK-HAM game is $n!$ projective.

Proof.

When P_2 decides the string he wants to reveal, there is a unique way to open this string, this comes from the property of our $\mathbb{F}_Q$ string commitment.

- If $chall = 0$, there is an opening that the verifier will accept for each permutation Π, so $n!$ valid outputs for P_2.
- If $chall = 1$, there is an opening that the verifier will accept for each cycle $\mathcal{C}'$. There are again $n!$ such cycles.

This shows that the game is $n!$-projective □

Proposition

The RZK-HAM protocol has special soundness $\frac{1}{Q}$.

Proof

Proving this is equivalent to proving that for any strategy used by P_1, P_2 can send a valid opening for both $chall = 0$ and $chall = 1$ wp. $\frac{1}{Q}$. We fix an input/output pair (B, Y) for P_1 and we consider winning outputs for P_2 for both inputs. For $chall = 0$, we have a permutation Π and a matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$ which is a valid opening of $M_{\Pi(G)}$ meaning that

$$\forall (i,j),\ A_{i,j} = Y_{i,j} - B_{i,j} * (M_{\Pi(G)})_{i,j}. \tag{2}$$

For $chall = 1$, we have a cycle $\mathcal{C}'$ of $\{1, \ldots, |V|\}$ as well as openings $A'_{u,v}$ for each $(u, v) \in \mathcal{C}'$. Because it is a winning output, the openings must satisfy

$$\forall (u,v) \in \mathcal{C}',\ A'_{u,v} = Y_{u,v} - B_{u,v}. \tag{3}$$

Proof continued

If the graph G (hence also $\Pi(G)$) does not contain a Hamiltonian cycle then there has to be an edge (u, v) of $\mathcal{C}'$ such that $\left(M_{\Pi(G)}\right)_{u,v} = 0$. For this specific (u, v), we combine Equations 2 and 3 and get:

$$A_{u,v} = Y_{u,v} \quad ; \quad A'_{u,v} = Y_{u,v} - B_{u,v}.$$

This implies that $A_{u,v} - A'_{u,v} = B_{u,v}$ which happens with probability at most $\frac{1}{Q}$ from non-signaling.

How we transformed special soundness security into sum-binding security

Proposition

Let $P_1, \ldots, P_T$ be projectors and $|\psi\rangle$ a quantum pure state. Let:
$p_i = \mathrm{Tr}(P_i|\psi\rangle\langle\psi|P_i)$; $V := \frac{1}{T}\sum_i p_i$ *and*
$E := \frac{1}{T(T-1)}\sum_{i,j\neq i} \mathrm{Tr}(P_j P_i|\psi\rangle\langle\psi|P_i P_j)$. *We have*

$$E \geq \frac{1}{64}(V - \frac{1}{T})^3.$$

Use it to bound the value of projective games from special soundness

Proposition

Let $P_1, \ldots, P_T$ be projectors that can be written as $P_i = \sum_{s=1}^{\alpha} P_i^s$ where P_i^s are orthogonal projectors for any fixed i. Let $|\psi\rangle$ be a quantum pure state and let

$$p_i = \mathrm{Tr}(P_i|\psi\rangle\langle\psi|) = \sum_{s=1}^{\alpha} \mathrm{Tr}(P_i^s|\psi\rangle\langle\psi|) \; ; \; V := \frac{1}{T}\sum_i p_i$$

and

$$E := \frac{1}{T(T-1)} \sum_{s,s' \neq s=1}^{\alpha} \sum_{i,j \neq i} \mathrm{Tr}(P_j^{s'} P_i^s |\psi\rangle\langle\psi| P_i^s P_j^{s'}).$$

We have

$$E \geq \frac{1}{64\alpha}(V - \frac{1}{T})^3.$$

Use it to bound the value of α-projective games from special soundness

Proof of the proposition. We can sum the outside projector to get

$$E = \frac{1}{T(T-1)} \sum_{s=1}^{\alpha} \sum_i \mathrm{Tr}(P_j P_i^s |\psi\rangle\langle\psi| P_i^s P_j).$$

Lemma (Pinching inequality)

For any projector $P_i = \sum_{s=1}^{\alpha} P_i^s$ where P_i^s are orthogonal projectors and $|\psi\rangle$, we have

$$\sum_{s=1}^{\alpha} P_i^s |\psi\rangle\langle\psi| P_i^s \succcurlyeq P_i |\psi\rangle\langle\psi| P_i.$$

This gives us immediately

$$\begin{aligned} E &= \frac{1}{T(T-1)} \sum_{s=1}^{\alpha} \sum_i \mathrm{Tr}(P_j P_i^s |\psi\rangle\langle\psi| P_i^s P_j) \\ &\geq \frac{1}{\alpha} \left(\frac{1}{T(T-1)} \sum_i \mathrm{Tr}(P_j P_i |\psi\rangle\langle\psi| P_i P_j) \right) \\ &\geq \frac{1}{64\alpha} (V - \frac{1}{T})^3 \end{aligned}$$

This can also be extended when we only have 2 projectors with an improved bound.

Proposition

Let P_0, P_1 be projectors that can be written as $P_i = \sum_{s=1}^{\alpha} P_i^s$ where P_i^s are orthogonal projectors for any fixed $i \in \{0,1\}$. Let $|\psi\rangle$ be a quantum pure state and let

$$p_i = \mathrm{Tr}(P_i|\psi\rangle\langle\psi|) = \sum_{s=1}^{\alpha} \mathrm{Tr}(P_i^s|\psi\rangle\langle\psi|) \; ; \; V := \frac{1}{2}\sum_i p_i$$

and

$$E := \frac{1}{T(T-1)} \sum_{s,s' \neq s=1}^{\alpha} \mathrm{Tr}(P_1^{s'} P_0^s |\psi\rangle\langle\psi| P_0^s P_1^{s'}).$$

We have

$$E \geq \frac{2}{\alpha}(V - \frac{1}{2})^2.$$

We have the formula $E \geq \frac{2}{\alpha}(V - \frac{1}{2})^2$. The RKZ-HAM protocol (or entangled game) has special soundness $\frac{1}{Q}$ so we can plug in $E = \frac{1}{Q}$. We obtain

$$\omega^*(G_{\text{RZK-HAM}}) \leq \frac{1}{2} + \sqrt{\frac{n!}{2Q}}.$$

by taking $Q = \frac{n!}{2^{k+1}}$, we get that the soundness of the protocol is $\frac{1}{2} + 2^{-k}$.

We just need to perform this protocol in parallel to reduce the soundness to a negligible quantity. This can be done similarly, since we know the $\mathbb{F}_Q$ bit commitment behaves well when run in parallel.

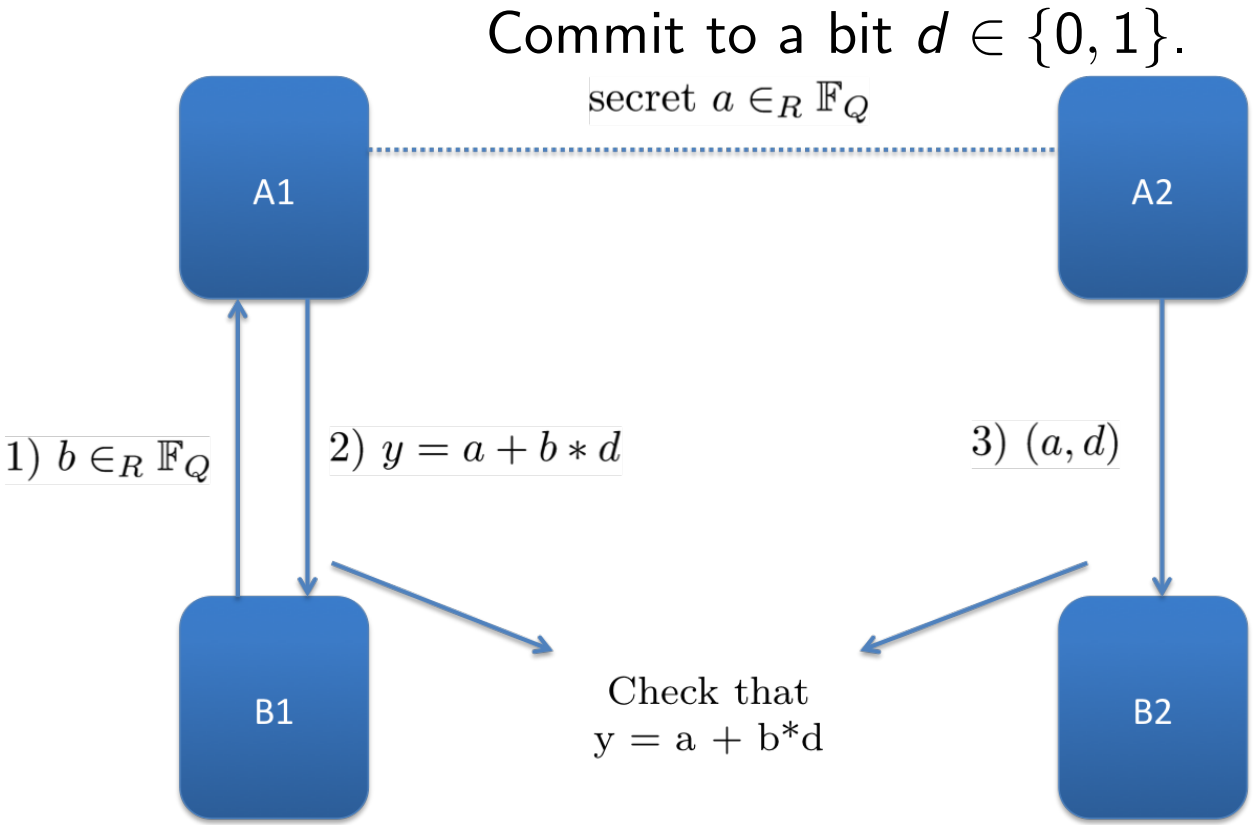
What about the zero-knowledge property? What is the verifier's view of the protocol?

- No matter what the verifier sends during the commit step, he obtains uniformly random strings from the prover.

Multi-round protocols

- We presented the $\mathbb{F}_Q$ bit/string commitment protocol with an application to a zero-knowledge protocol for Hamiltonian cycle.
- We could commit and immediately after perform an opening.
- But the underlying bit/string commitment protocol works only for a very short of time.
- Here, we show to increase the commit time.

The relativistic F_Q bit commitment protocol



- If P_1, P_2 are at a distance D, the commitment is valid for a time $< \frac{D}{c}$.
- Idea: instead of revealing a, P_2 commits to a using a $\mathbb{F}_Q$ string commitment scheme.
- 2 possibilities: make the alphabet size explode with the number of rounds or use a bad string commitment.

Multi-round $\mathbb{F}_Q$ bit commitment

In this form, first proposed in [LKB+14].

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share k random numbers $a_1, \ldots, a_k$ (resp. $b_1, \ldots, b_k$) $\in \mathbb{F}_q$, for even k. Here, q is a prime power p^n for some prime p and $\mathbb{F}_q$ refers to the Galois field of order q.
2. *Commit phase*: $\mathcal{B}_1$ sends b_1 to $\mathcal{A}_1$, who returns $y_1 = a_1 + (d * b_1)$ where $d \in \{0, 1\}$ is the committed bit.
3. *Sustain phase, starting at $i = 2$*: at round i, $\mathcal{B}_{i \mod 2}$ sends $b_i \in \mathbb{F}_q$ to $\mathcal{A}_{i \mod 2}$, who returns $y_i = a_i + (a_{i-1} * b_i)$.
4. *Reveal phase*: $\mathcal{A}_1$ reveals d and a_k to $\mathcal{B}_1$. $\mathcal{B}_1$ checks that $a_k = y_k + (a_{k-1} * b_k)$.

Timing constraints: round j finishes before any information about b_{j-1} reaches the other Alice.

How to include the sustain phase in the security? Give as much power as possible to the cheating parties.
The bit commitment protocol consists of $\mathrm{comm} = (\mathrm{comm}(P), \mathrm{comm}(V))$; $\mathrm{sust} = (\mathrm{sust}(P), \mathrm{sust}(V))$; $\mathrm{open} = (\mathrm{open}(P), \mathrm{open}(V))$.

Perfect hiding property

For any strategy $\mathrm{comm}^*(V), \mathrm{sust}^*(V)$, the transcript of $(\mathrm{comm}(P), \mathrm{comm}^*(V), \mathrm{sust}(P), \mathrm{sust}^*(V))$ should be independent of d.

Sum-binding property

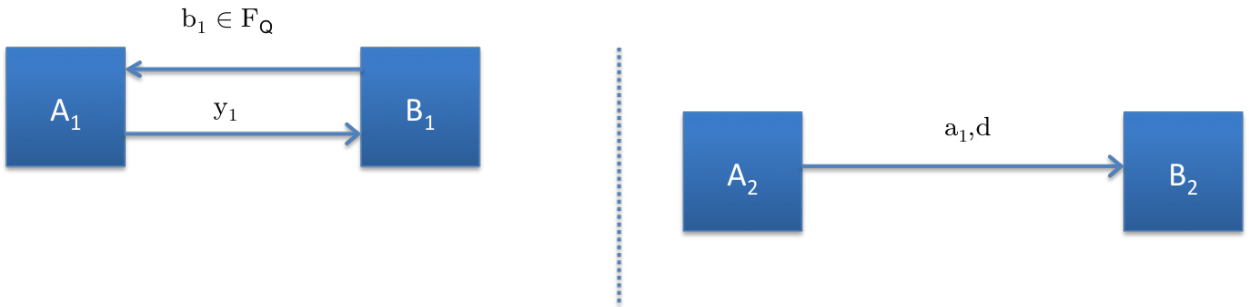
$$\forall\ \mathrm{comm}^*(P), \sum_{b' \in \{0,1\}} \max_{\mathrm{open}^*(P), \mathrm{sust}^*(P)}$$

$$\Pr[\mathrm{V\ outputs}\ b' | (\mathrm{comm}^*(P), \mathrm{sust}^*(P), \mathrm{open}^*(P))] \leq 1 + \varepsilon$$

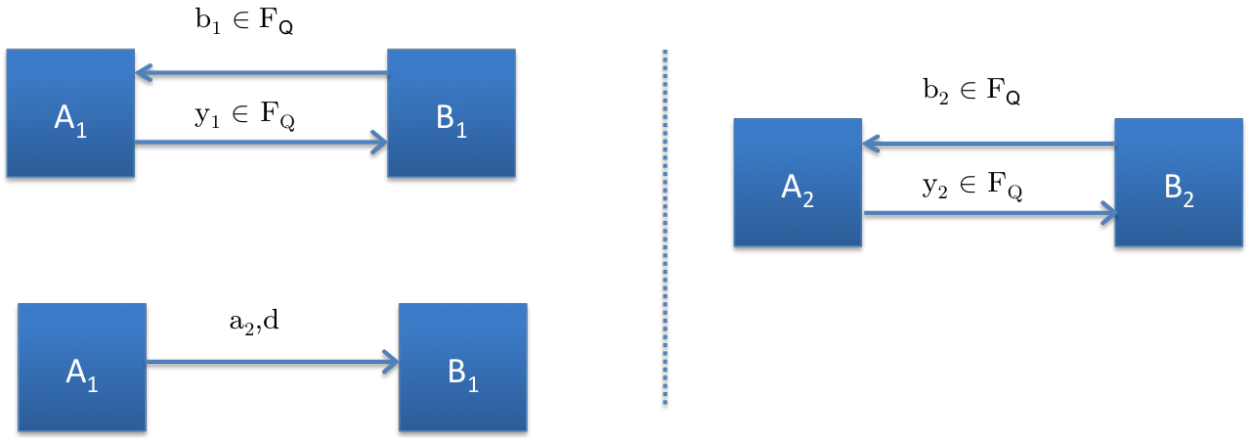
Even though the string commitment used in the sustain phase doesn't have the sum-binding property, it's still possible to prove the binding property, at least in the classical case. For r rounds:

- LKB+14 : $\varepsilon \approx O((\frac{1}{\sqrt{Q}})^{1/2^r})$. Proof idea, reduce to a single game.
- [FF15,CCL15] : $\varepsilon = O(\frac{r}{\sqrt{Q}})$. [FF15]: based on composition of relativistic bit commitment schemes. [CCL15] : recursive analysis using 2 player games.

[CCL15] proof



Let $\widetilde{a}_i(d) := y_i - \widetilde{a}_{i-1} * b_i$ with $\widetilde{a}_0 = d$. For single-round protocol, A_2 must guess $\widetilde{a}_i(d)$ in order to successfully reveal d.



For double-round protocol, A_1 must guess $\widetilde{a}_2(d) = y_2 + b_2 * \widetilde{a}_1(d)$. We can reduce to the following 2 player game.

b_1 doesn't intervene directly in the winning condition (it does only in the sense that A_1 knows $\widetilde{a}_1$) and d is known by both players.

So we can reduce to the following game:

For a fixed d, they win the game if $\widetilde{a}_2(d) - y_2 = b_2 * \widetilde{a}_1(d)$. Exactly (up to the $-$ sign) the $CHSH_{Q,Q}$ game.
However, $\widetilde{a}_1$ is not necessarily a uniform random string unknown from A_2.
If $p_1(d) = \Pr[A_2 \text{ can guess } \widetilde{a}_1(d)]$, we have that

$$p_1(0) + p_1(1) \leq 1 + 2\sqrt{\frac{2}{Q}}.$$

from the sum-binding security of the single round protocol.

This motivates defining the game $\mathrm{CHSH}^{-}_{Q,Q}(p)$ as follows:

$CHSH^{-}_{Q,Q}(p)$

2 player entangled game between A_1 and A_2. Alice receives a string $\widetilde{a}_1 \in \mathbb{F}_Q$ st. $\max_c\{\Pr[\widetilde{a}_1 = c]\} = p$, Bob receives a random $b_2 \in \mathbb{F}_Q$. They produce respective outputs $\widetilde{a}_2, y_2 \in \mathbb{F}_Q$. They win iff. $y_2 - \widetilde{a}_2 = \widetilde{a}_1 * b_2$.

Notice that $\omega(CHSH^{+}_{Q,Q}(p)) \geq p$ and $\omega(CHSH^{+}_{Q,Q}(\frac{1}{Q})) = \omega(CHSH^{+}_{Q,Q}(\frac{1}{Q}))$. From the previous analysis, we have (for classical adversaries) that the 2-round $\mathbb{F}_Q$ bit commitment is ε sum-binding for ε such that

$$\omega(\mathrm{CHSH}^{-}_{Q,Q}(p_1(0))) + \omega(\mathrm{CHSH}^{-}_{Q,Q}(p_1(1))) = 1 + \varepsilon.$$

with

$$p_1(0) + p_1(1) \leq 1 + \sqrt{\frac{2}{Q}}.$$

We can prove the following bound

$$\omega(\mathrm{CHSH}_{Q,Q}(p)) \leq p + \sqrt{\frac{2}{Q}}.$$

Plugging this in the previous, we get

$$p_1(0) + p_1(1) + 2\sqrt{\frac{2}{Q}} = 1 + \varepsilon$$

which gives $\varepsilon \leq 4\sqrt{\frac{2}{Q}}$.

We proved the following:

- The 1 round protocol is ε-binding for $\varepsilon = 2\sqrt{\frac{2}{Q}}$.
- The 2 round protocol is ε-binding for $\varepsilon = 4\sqrt{\frac{2}{Q}}$.

The recursive statement actually works: the r round protocol is ε-binding for $\varepsilon = 2r\sqrt{\frac{2}{Q}}$.

Proof idea of the classical bound: actually very close to the quantum setting for $CHSH_Q$.

Proposition (Classical learning lemma)

Suppose Alice has a string $x = x_1, \ldots, x_n$ and Bob has a string $c(x)$, all given with some joint probability distribution $q(x, c(x))$. Suppose that Bob has a strategy to learn x_i wp. p_i and let $V = \frac{1}{n}\sum_i p_i$. There is a strategy to guess (x_i, x_j) wp. $p_{i,j}$ such that

$$E := \frac{1}{n(n-1)} \sum_{i,j \neq i} p_{i,j} \geq \frac{nV}{n-1}(V - \frac{1}{n})$$

Fix a strategy S. For a fixed $(x, c(x))$, this strategy is deterministic (the randomness can be included in c(x). For each i, let $s_i(x, c(x)) \in \{0, 1\} = \Pr[\text{Bob guesses } x_i | S]$. We use the consecutive measurement strategy to try to learn (x_i, x_j) for any $i, j \neq i$. Let:

- $V(x, c(x))$ the probability of guessing x_i for a random i for a fixed $(x, c(x))$
- $E(x, c(x))$ the probability of guessing a random (x_i, x_j) for a random $i, j \neq i$ and a fixed $(x, c(x))$.

We have

$$V(x, c(x)) = \frac{1}{n} \sum_{i=1}^{n} s_i(x, c(x)) = \frac{\kappa}{n} \text{ for some } \kappa \in \mathbb{N}.$$

$$E(x, c(x)) = \frac{1}{n(n-1)} \sum_{i,j \neq i} s_i(x, c(x)) s_j(x, c(x)) = \frac{\kappa(\kappa - 1)}{n(n-1)}$$
$$= \frac{nV(x, c(x))}{n-1} (V(x, c(x)) - \frac{1}{n}).$$

If we define $f_n(X) = \frac{nX}{n-1}\left(X - \frac{1}{n}\right)$ we can see that f_n is convex and by rewriting the above equation, we have $E(x, c(x)) = f_n(V(x, c(x)))$. We can now conclude

$$E = \mathbb{E}_{x,c(x)}[E(x, c(x))] = \mathbb{E}_{x,c(x)}[f_n(V(x, c(x)))]$$
$$\geq f_n(\mathbb{E}_{x,c(x)}[E(x, c(x))]) = f_n(V) = \frac{nV}{n-1}(V - \frac{1}{n}).$$

Similarly as before, we can use this to bound the value of the $CHSH_{Q,Q}(p)$ game.

Issue with the quantum case? We need to bound the quantum value of

$CHSH^{-}_{Q,Q}(p)$

2 player entangled game between A_1 and A_2. Alice receives a string $\widetilde{a}_1 \in \mathbb{F}_Q$ st. $\Pr[A_2 \text{ can guess } \widetilde{a}_1] \leq p$, Bob receives a random $b_2 \in \mathbb{F}_Q$. They produce respective outputs $\widetilde{a}_2, y_2 \in \mathbb{F}_Q$. They win iff. $y_2 - \widetilde{a}_2 = \widetilde{a}_1 * b_2$.

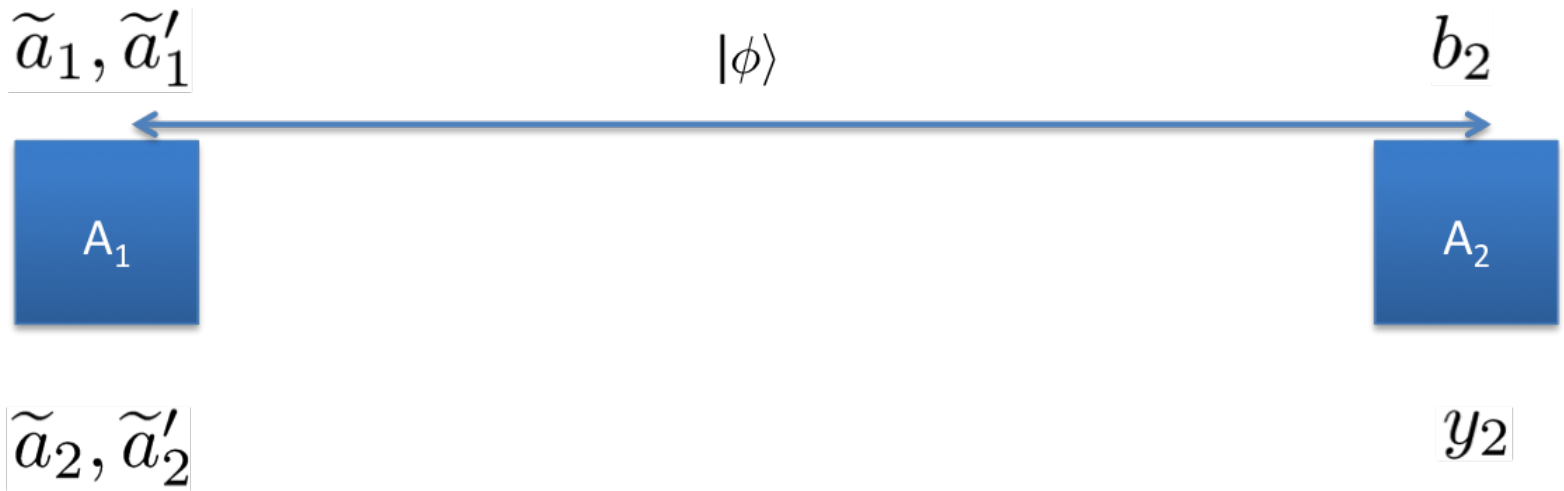
but with a subtelty. A_2 has some information about $\widetilde{a}_1$ which could be of the form of a shared state $|\psi_{\widetilde{a}_1}\rangle$ with A_1. This means that

- It is no longer a 2 player entangled game in the usual sense.
- Our proof technique does not work here.

If we can show that the entangled value of the above game (with share state $|\psi_{\widetilde{a}_1}\rangle$ is smaller than $p + f(q)$ then the r-round $\mathbb{F}_Q$ protocol would be ε sum-binding secure against quantum adversaries with $\varepsilon = 2rf(q)$.

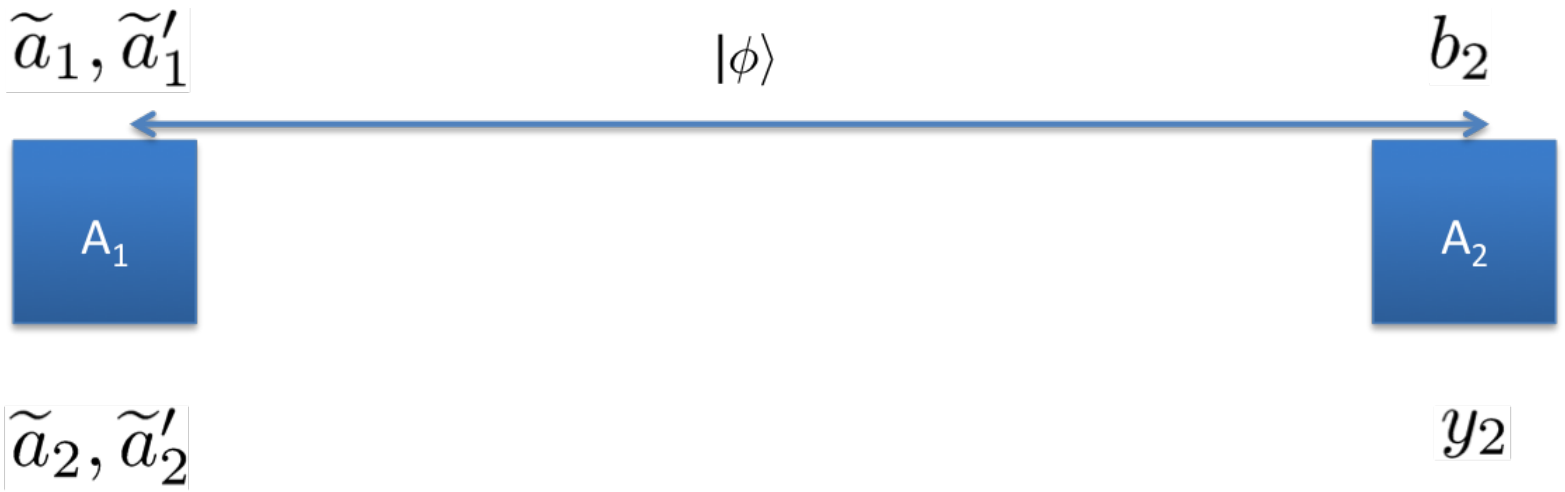
It is possible to show a bound for the above problem of the form $\sqrt{p} + f(q)$. Behaves very poorly when considering multiple rounds.

In the case, where the shared state is independent of the inputs, we can use the consecutive learning lemma and use the fact that A_1 can guess b_2 wp. $\frac{1}{Q}$. This gives the bound $p + \sqrt{\frac{2}{Q}}$.



However, if we considered the opposite strategy i.e. trying to apply the consecutive measurements on A_2, we would only get $\frac{1}{Q} + \sqrt{p}$ which is potentially much worst. (For example, for $\mathrm{CHSH}_{2,Q}$ i.e. $p = \frac{1}{2}$, this would give a bound larger than $\sqrt{\frac{1}{2}}$ while we know a bound of $\frac{1}{2} + \frac{1}{\sqrt{Q}}$.

In the case, where the shared state is independent of the inputs, we can use the consecutive learning lemma and use the fact that A_1 can guess b_2 wp. $\frac{1}{Q}$. This gives the bound $p + \sqrt{\frac{2}{Q}}$.



If there is an entangled state that depends on $\widetilde{a}_i$ then the above scenario doesn't make sense.
What we can do is to consider the opposite strategy i.e. trying to apply the consecutive measurements on A_2, we would only get $\frac{1}{Q} + \sqrt{p}$ which is potentially much worst. (For example, for $\mathrm{CHSH}_{2,Q}$ i.e. $p = \frac{1}{2}$, this would give a bound larger than $\sqrt{\frac{1}{2}}$ while we know a bound of $\frac{1}{2} + \frac{1}{\sqrt{Q}}$.