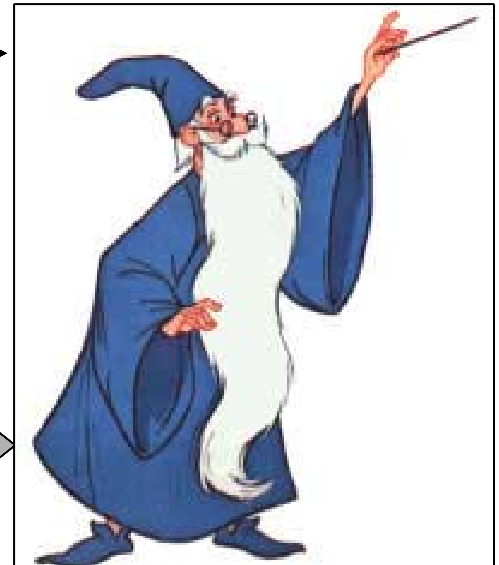
Upper Bounds for Quantum Interaction

Gus Gutoski
University of Calgary
Calgary, Alberta, Canada

Interactive Proofs

$x \in \{0,1\}^*$



communication

Verifier
Poly-time & coin flips

Prover
All-powerful

Accept or **Reject** x

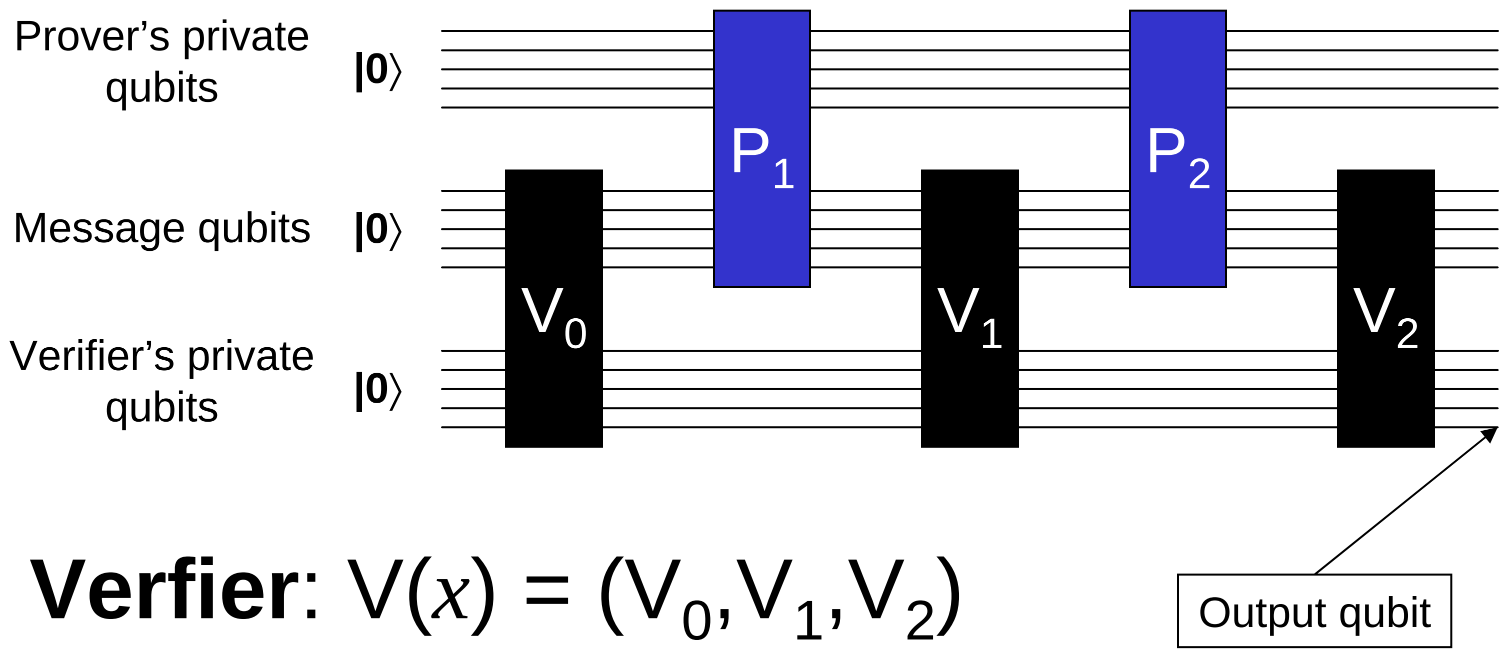
Interactive Proofs

A language L has an interactive proof if there exists a verifier V such that:

1. (completeness condition)
   If $x \in L$ then there exists a prover P that can convince V to accept x with probability > 3/4.
2. (soundness condition)
   If $x \notin L$ then *no* prover can convince V to accept x except with probability < 1/4.

- IP = PSPACE [LFKN92] [S92].

Quantum Interactive Proofs

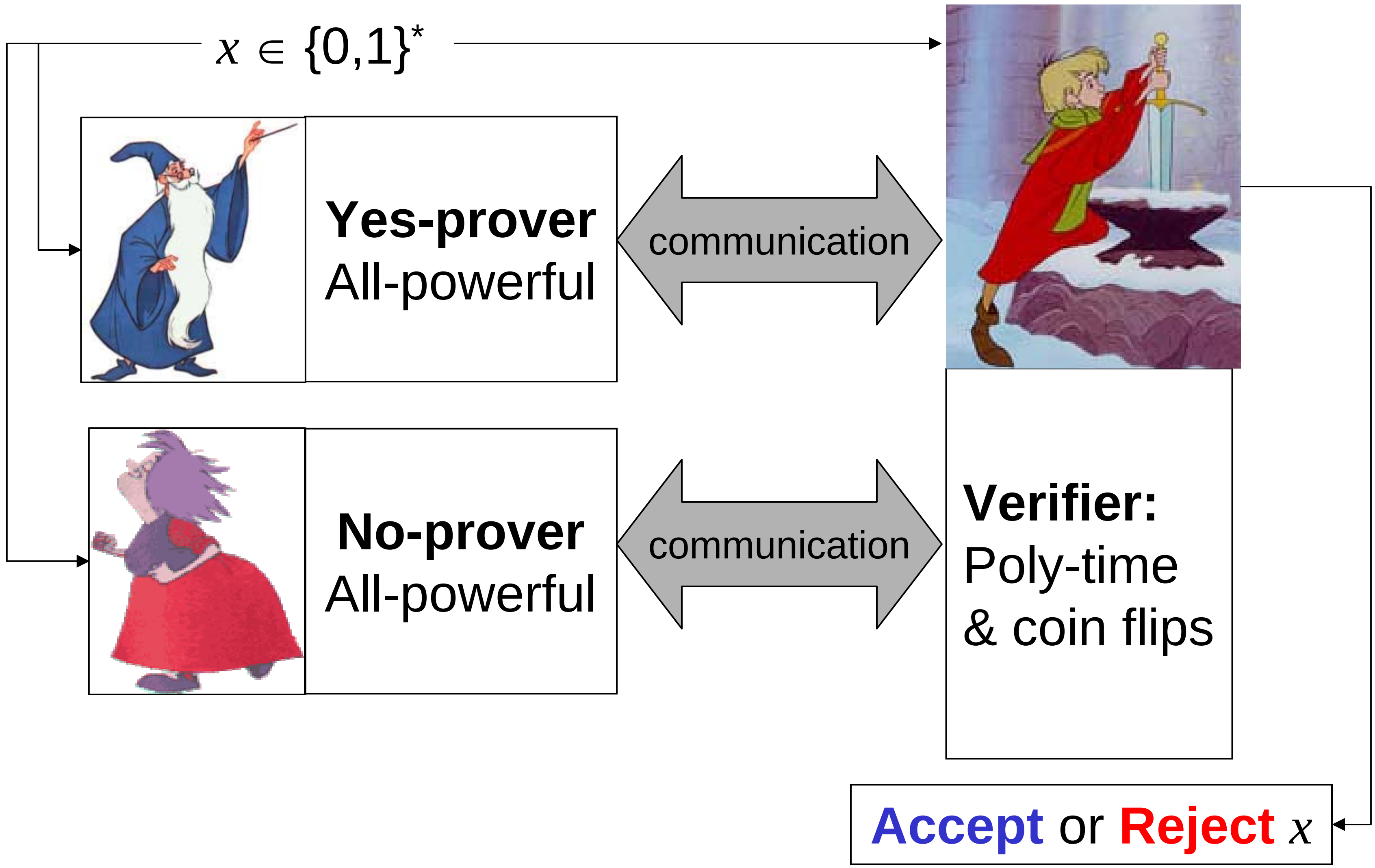


Verfier: $V(x) = (V_0, V_1, V_2)$

Prover: $P(x) = (P_1, P_2)$

PSPACE $\subseteq$ QIP $\subseteq$ EXP [KW00].

Refereed Games



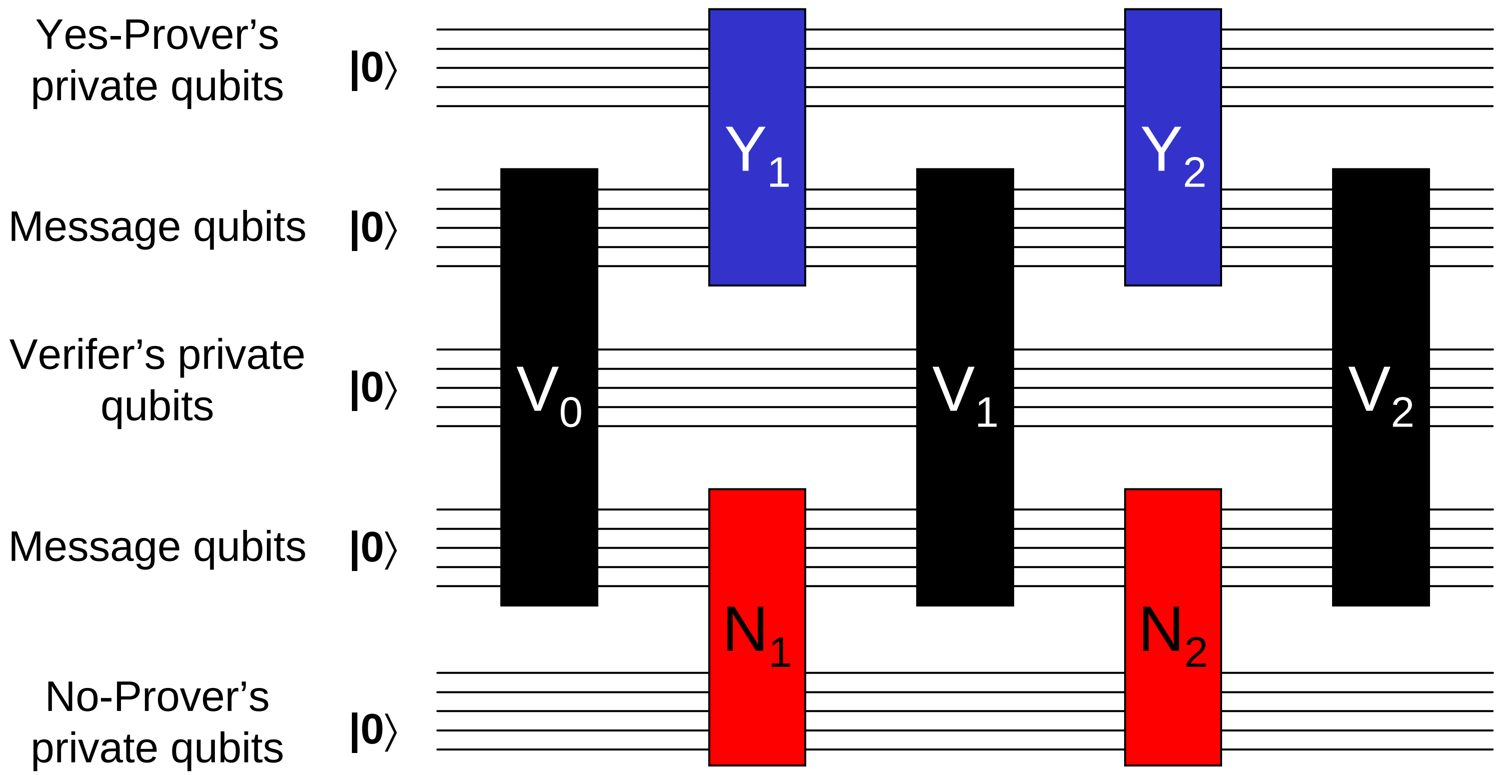
Refereed Games

A language L has a refereed game if there exists a verifier V such that:

1. (completeness condition)
   If $x \in L$ then there exists a yes-prover Y that can convince V to accept x *regardless of the no-prover* with probability > 3/4.
2. (soundness condition)
   If $x \notin L$ then there exists a no-prover N that can convince V to reject x *regardless of the yes-prover* with probability > 3/4.

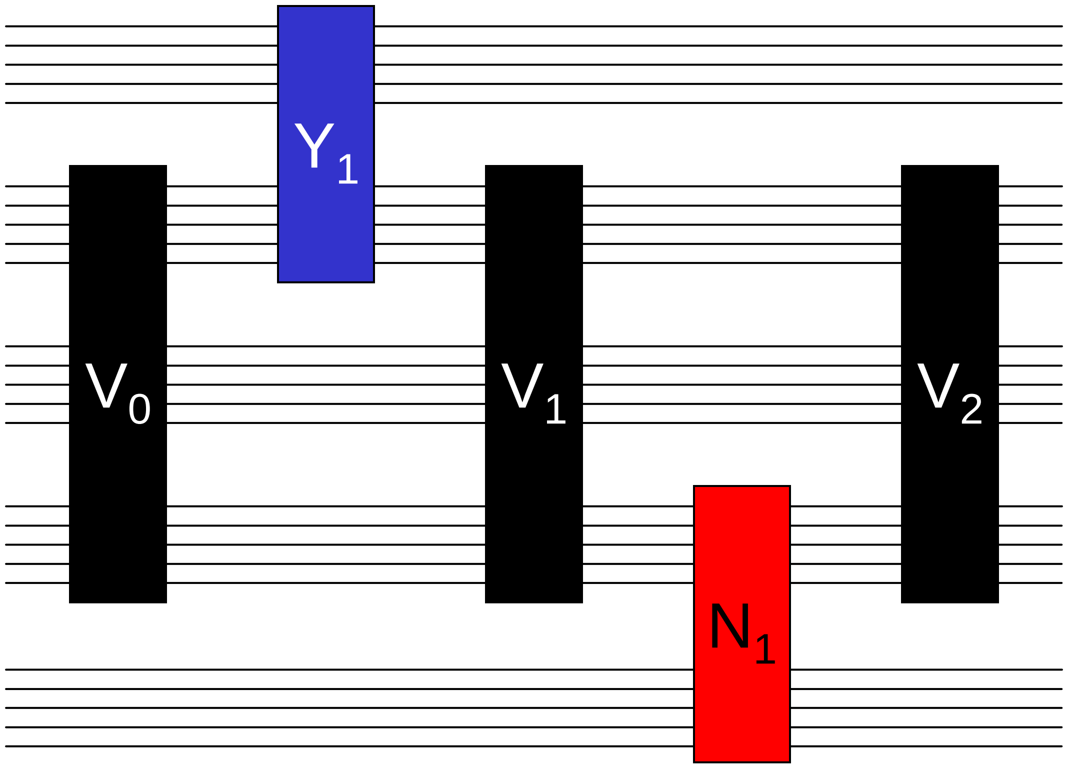
- RG = EXP [KM92] [FK97].

Quantum Refereed Games



New complexity class: QRG

Short Quantum Games



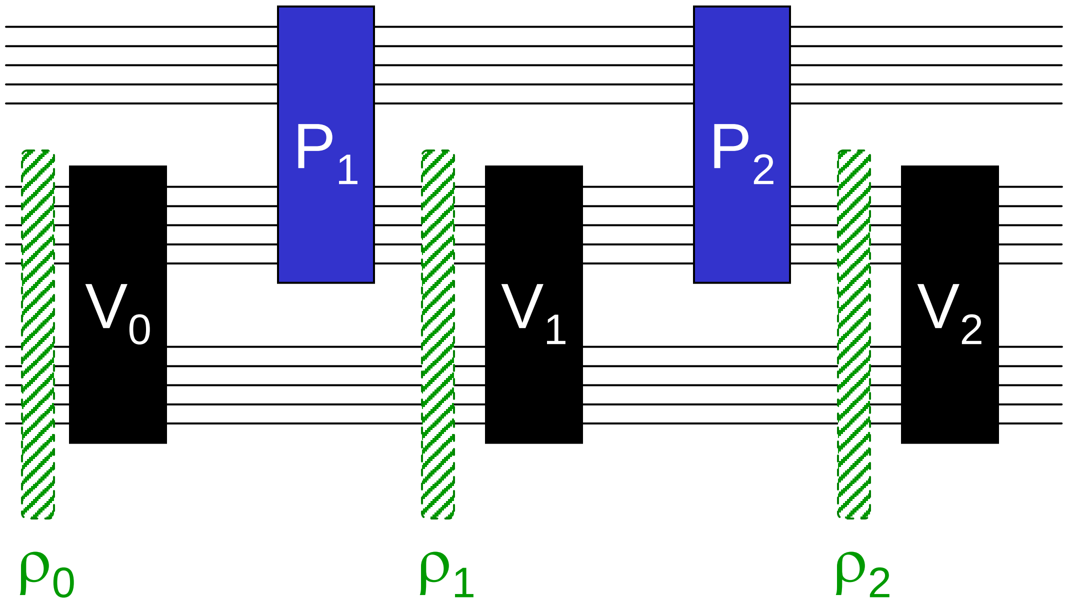
- New complexity class: SQG
- QIP ⊆ SQG [GW05].

Background and Overview

- QIP $\subseteq$ SQG [GW05].
- QIP $\subseteq$ EXP [KW00].
- How does SQG relate to EXP?
- We prove SQG $\subseteq$ EXP.
  - First, we review QIP $\subseteq$ EXP.
  - Next, we note that QRG $\subseteq$ NEXP.
  - Finally, we show SQG $\subseteq$ EXP.

QIP ⊆ EXP

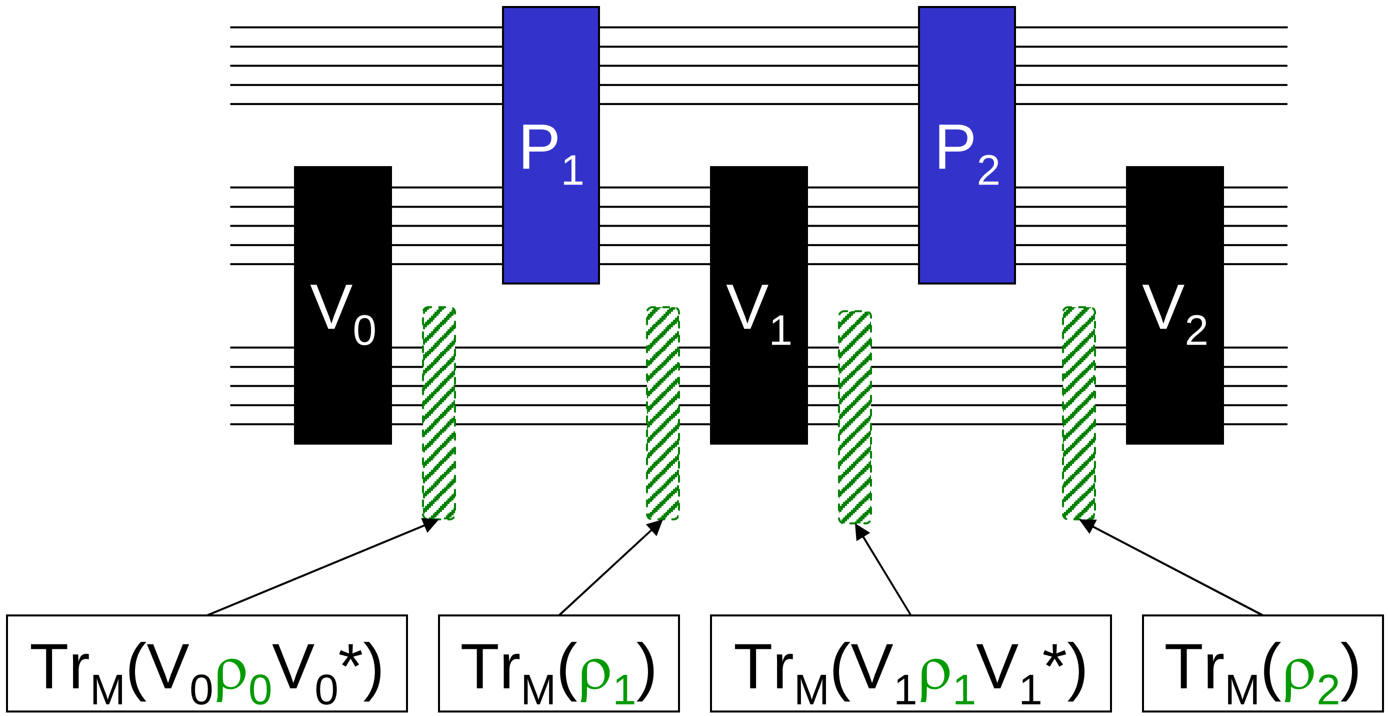
Consider the states ρ_0, ρ_1, ρ_2:



1. $\rho_0 = |0\rangle\langle 0|$; and
2. The verifier accepts x with probability $\mathrm{Tr}(\Pi_{accept} V_2 \rho_2 V_2^*)$ (linear function of ρ_2).

$QIP \subseteq EXP$

What else can we say about ρ_0, ρ_1, ρ_2?



(linear constraints on ρ_0, ρ_1, ρ_2.)

$QIP \subseteq EXP$

It turns out that ρ_0, ρ_1, ρ_2 can be *any* states with this property!

Proof:

- Given any ρ_0, ρ_1, let $|u_0\rangle$, $|u_1\rangle$ be purifications.
- Then $V_0|u_0\rangle$ purifies $Tr_M(V_0 \rho_0 V_0^*)$.
- As

$$Tr_M(V_0 \rho_0 V_0^*) = Tr_M(\rho_1),$$

  there must exist a unitary P_1 with

$$P_1 V_0 |u_0\rangle = |u_1\rangle.$$

- Similar construction for P_2.

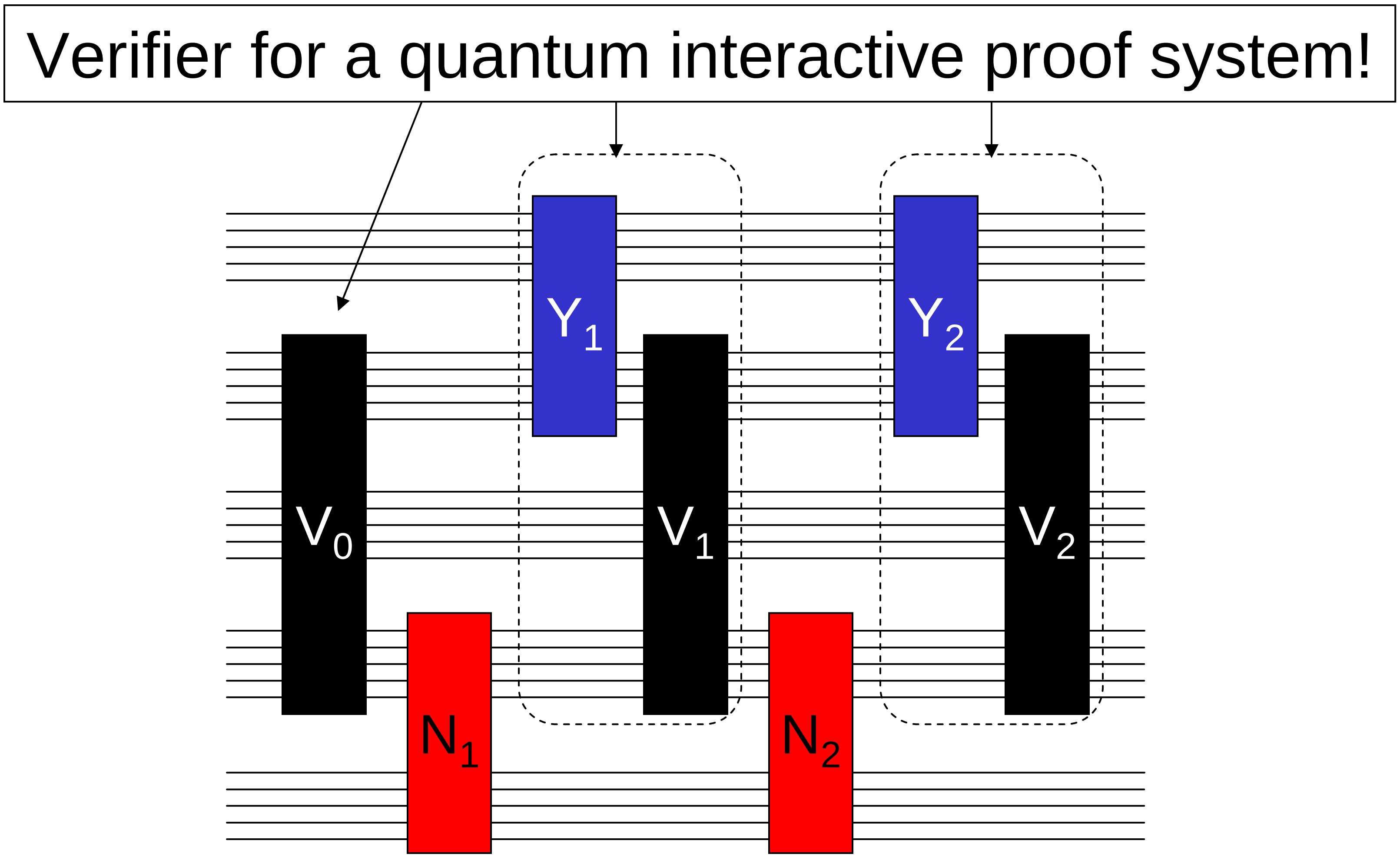
QIP ⊆ EXP

This characterization can be expressed as a <u>semidefinite program (SDP)</u>:

maximize	linear function of ρ_r
subject to	linear constraints on $\rho_0,\ldots,\rho_r$;
	$\rho_0,\ldots,\rho_r$ pos. semidefinite

- SDPs can be solved in poly-time.
- Our matrices have size exponential in $|x|$.
- QIP ⊆ EXP

$QRG \subseteq NEXP$

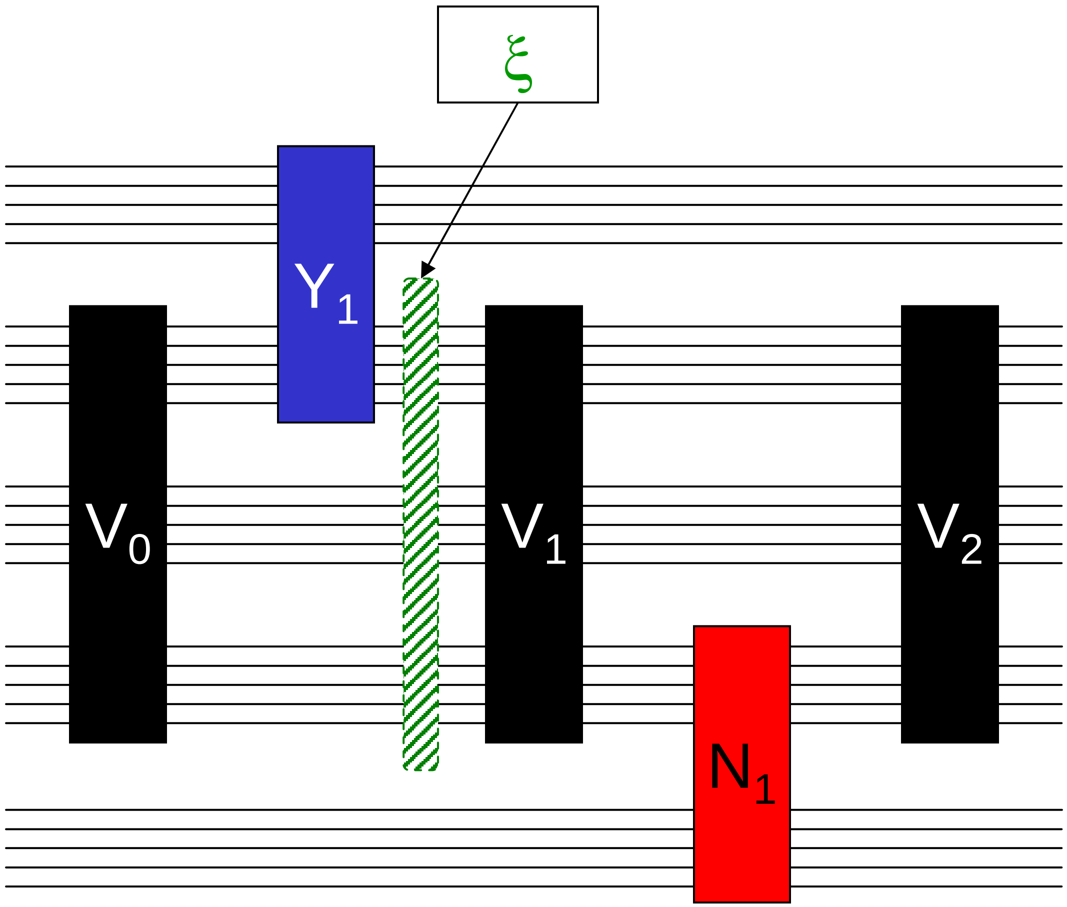


QRG $\subseteq$ NEXP

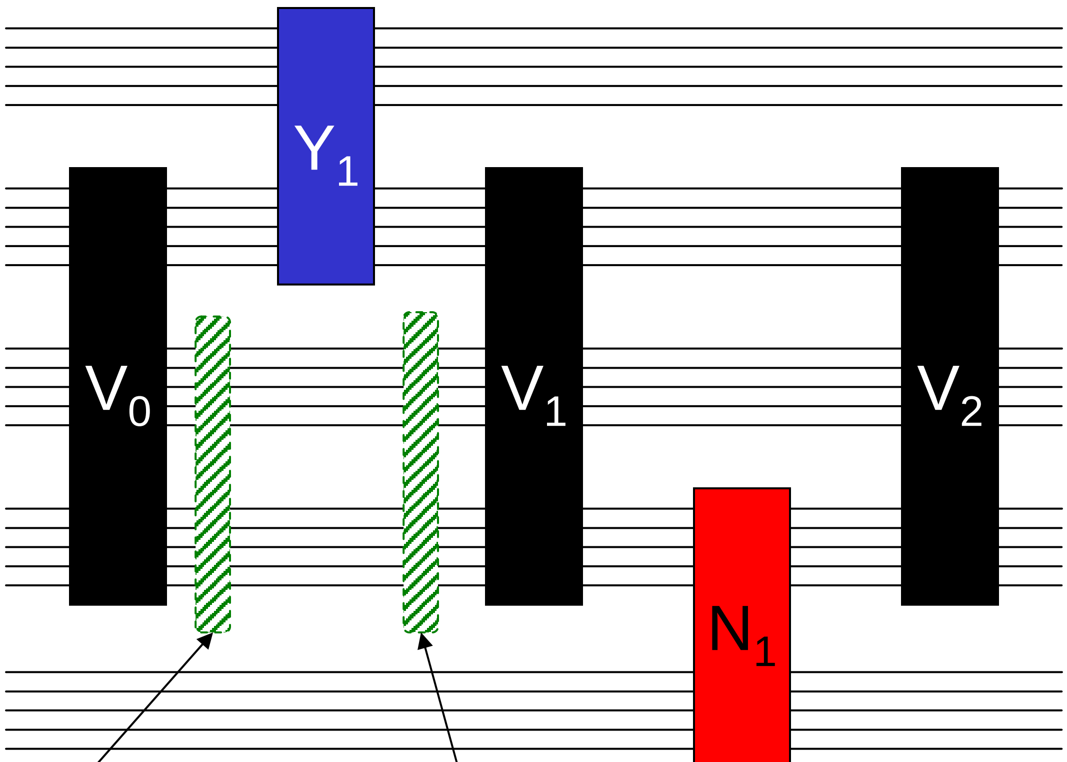
- Nondeterministic strategy: Guess the unitaries $(Y_1,\ldots,Y_r)$ for the yes-prover and solve the induced QIP as before.
- QRG $\subseteq$ NEXP

$SQG \subseteq EXP$

Suppose ξ is given. What can we say about ξ?



SQG ⊆ EXP



$\mathrm{Tr}_M(V_0|0\rangle\langle 0|V_0^*)$

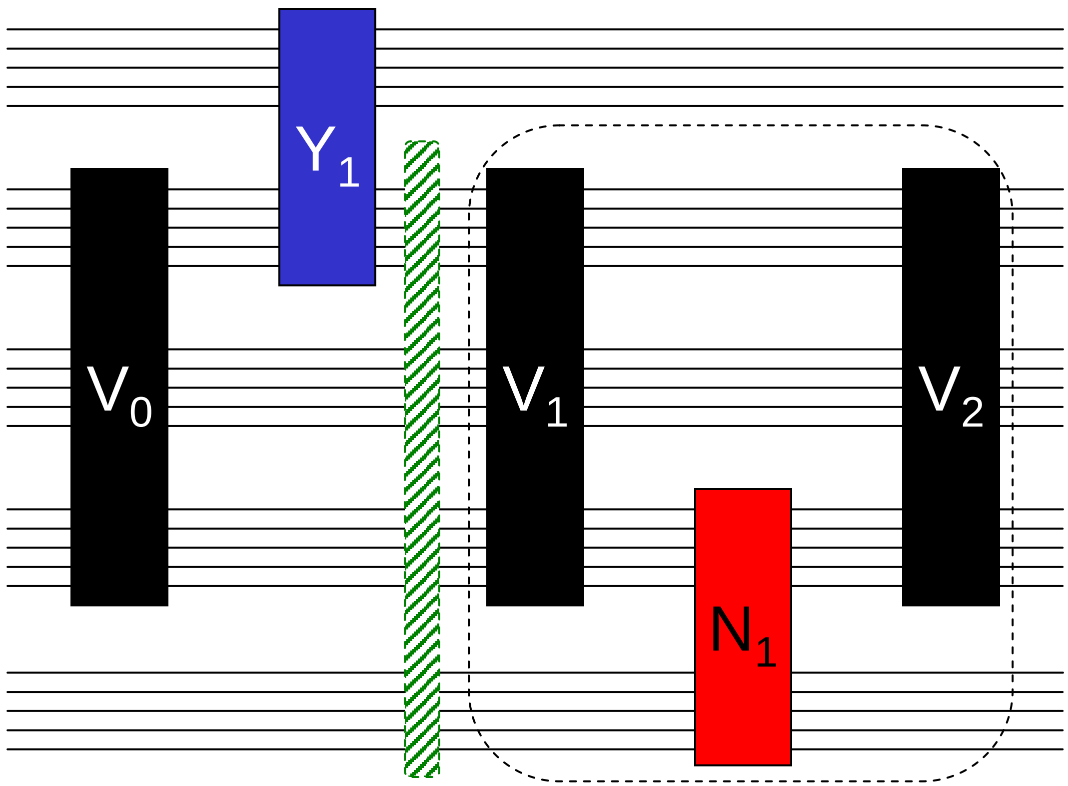
$\mathrm{Tr}_M(\xi)$

(linear constraint on ξ)

The verifier rejects x with probability

$$\mathrm{Tr}(\Pi_{reject} V_2 N_1 V_1 (\xi \otimes |0\rangle\langle 0|) V_1^* N_1^* V_2^*)$$

(given N_1, it's a linear function of ξ).



$\xi \otimes |0\rangle\langle 0|$

The Set of Winning Yes-Provers

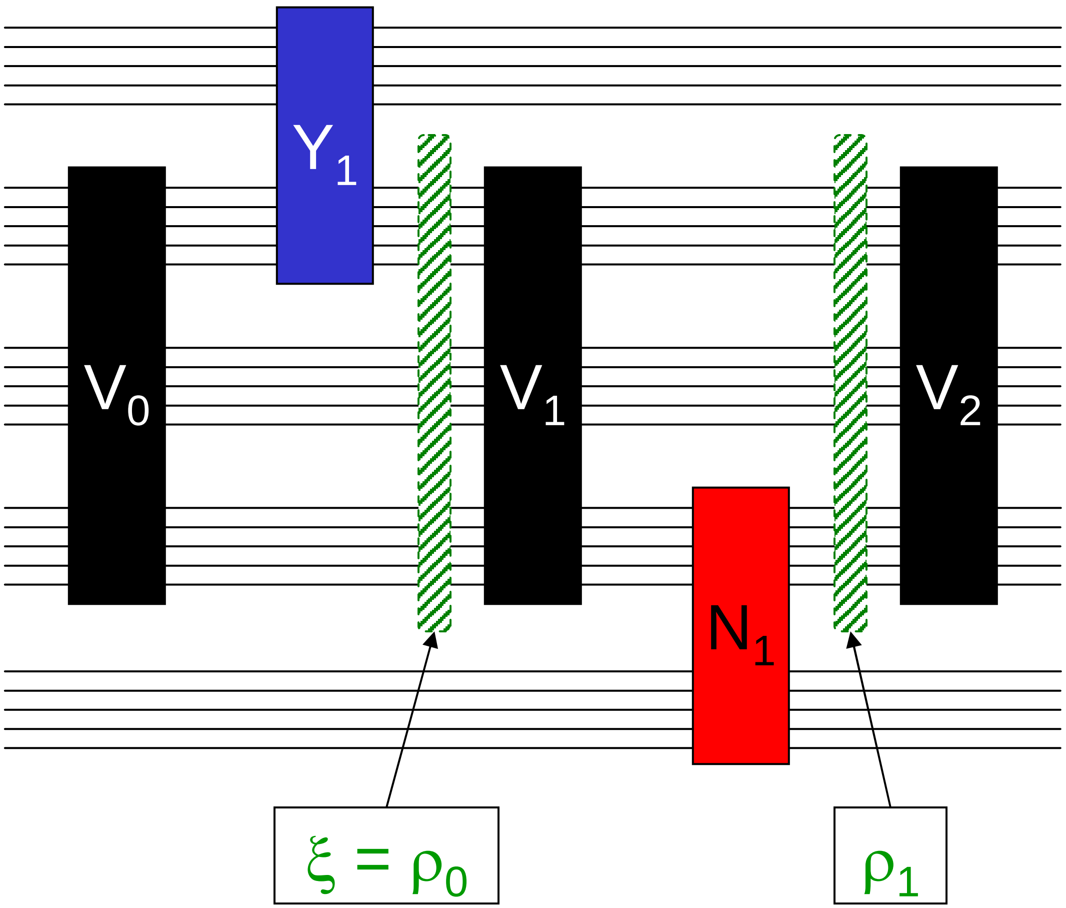
Define ***Win*** to be the set of all density matrices ξ such that:

- $Tr_M(V_0|0\rangle\langle 0|V_0^*) = Tr_M(\xi)$; and
- Pr. rejection < ¼ $\forall$ unitaries N_1.

Then ***Win*** is nonempty iff $x \in L$.

SQG $\subseteq$ EXP

Given ξ, view the rest of the game as a QIP:



$SQG \subseteq EXP$

- Given $\rho_0 = \xi$, solve the SDP for (ρ_0,ρ_1) to maximize Pr. rejection (linear in ρ_1).
- If maximum Pr. rejection is < ¼ then
  $\xi \in$ ***Win***
  $\Rightarrow$ ***Win*** is nonempty
  $\Rightarrow x \in L$
- Otherwise, deduce a no-prover N that yields ρ_1 (easy).

SQG $\subseteq$ EXP

- N is a witness that $\xi \notin$ ***Win***:

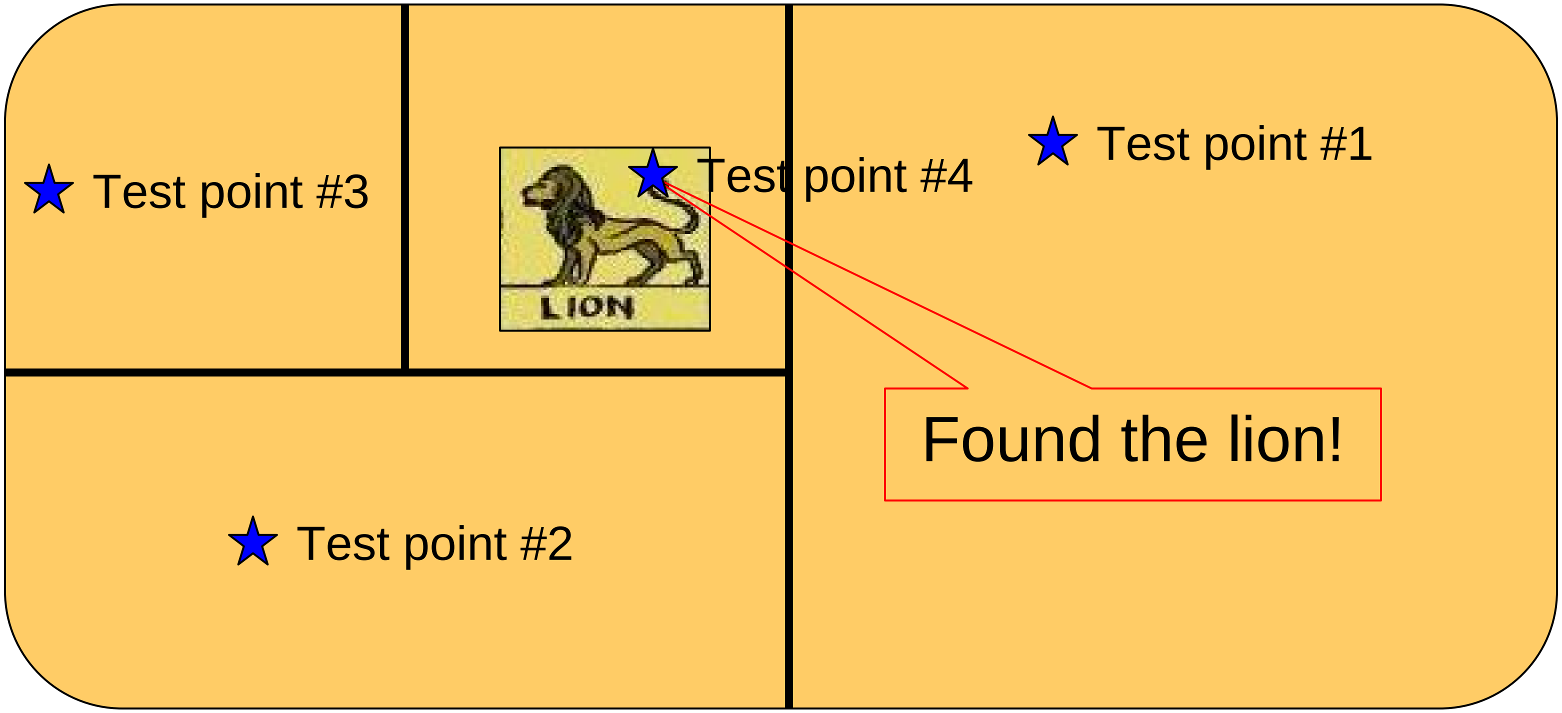
  linear$_N(\xi) > 1/4$ and

  linear$_N(\xi') < 1/4$ $\forall \xi' \in$ ***Win***

  $\Rightarrow \exists$ a *hyperplane* that separates ξ from ***Win***.
- Recap: Given ξ, we can use our SDP to decide if $\xi \in$ ***Win*** or to find a separating hyperplane for ξ.
- How does that help?

The Ellipsoid Method

How to find a lion in the desert…



SQG $\subseteq$ EXP

- Given a poly-time separation oracle, the ellipsoid method can decide the emptiness of a convex set in poly-time!
- Poly-time separation oracle: the SDP
- Convex set: ***Win***
- Dimension of ***Win*** is exponential in $|x|$
- SQG $\subseteq$ EXP

Conclusion

- We used SDP [KW00] to decide QIPs and QRGs:

$$\text{QIP} \subseteq \text{EXP}.$$
$$\text{QRG} \subseteq \text{NEXP}.$$

- We used the ellipsoid method to decide short quantum games

$$\text{SQG} \subseteq \text{EXP}.$$

- The emerging complexity map:

$$\text{PSPACE} \subseteq \text{QIP} \subseteq \text{SQG}$$
$$\subseteq \text{EXP} \subseteq \text{QRG} \subseteq \text{NEXP}.$$