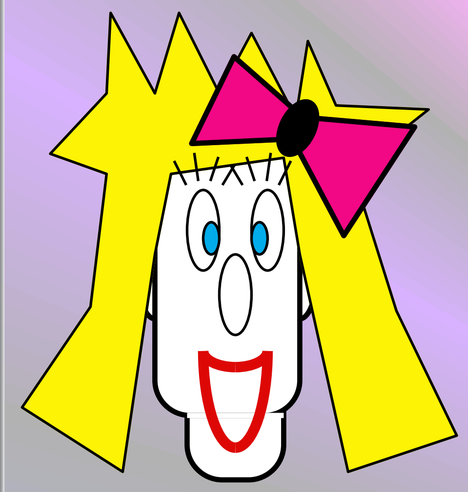
Interactive Proofs and Arthur-Merlin games

Claude Crépeau

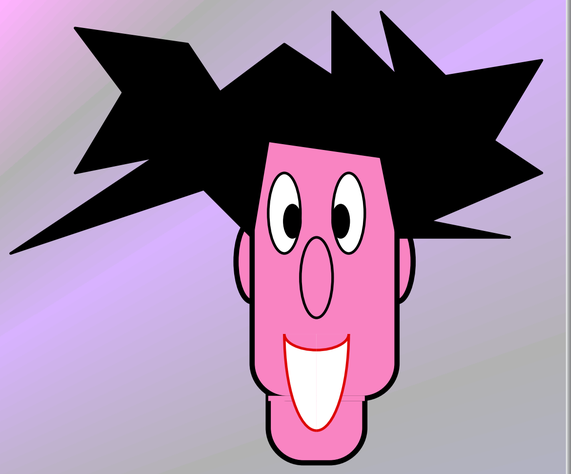
School of Computer Science
McGill University

Proofs

Proofs



$x \in L$

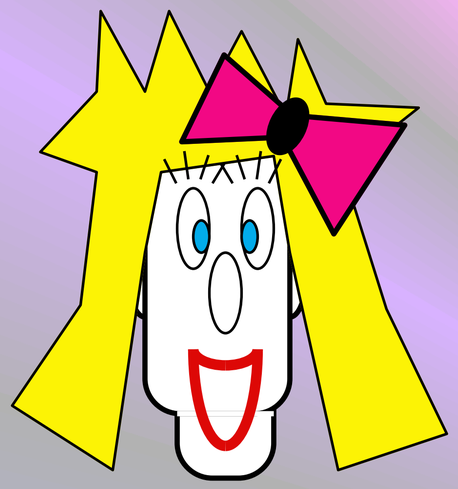


YES !

w

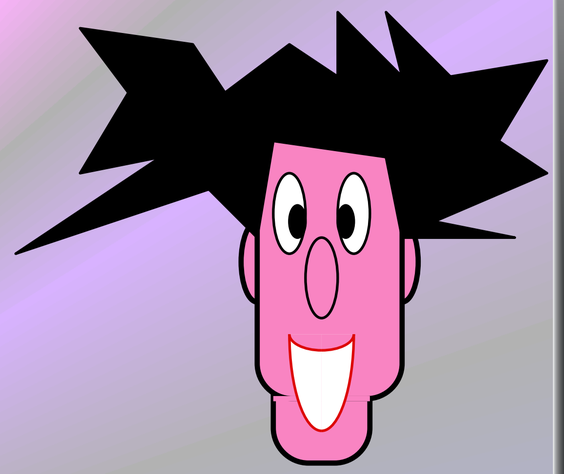
$\forall x \in L \exists w \Pr([\,\text{  }\,](x,w)=\text{YES}) = 1$

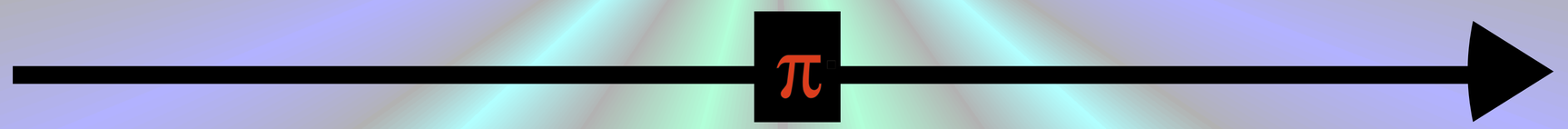
Proofs



$(G_0,G_1)\in ISO$

$(G_0=\pi(G_1))$



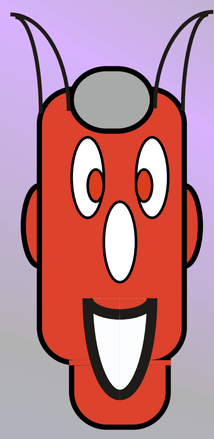


$G_0=\pi(G_1)$

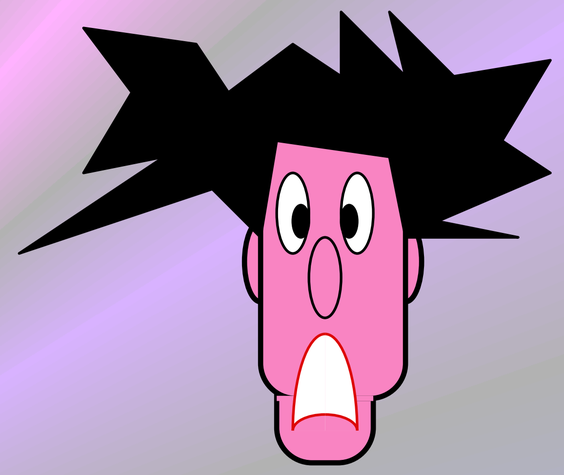
YES !

$\forall x\in L \exists \pi$ Pr([🤪](x,π)=YES) = 1

Proofs



$x \notin L$

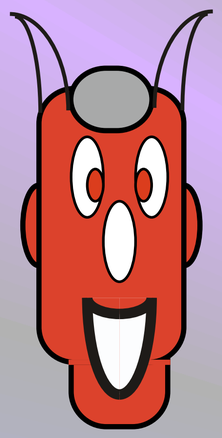


w

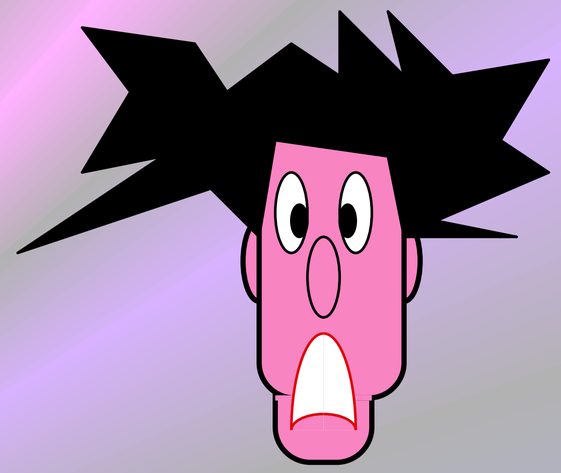
NO !

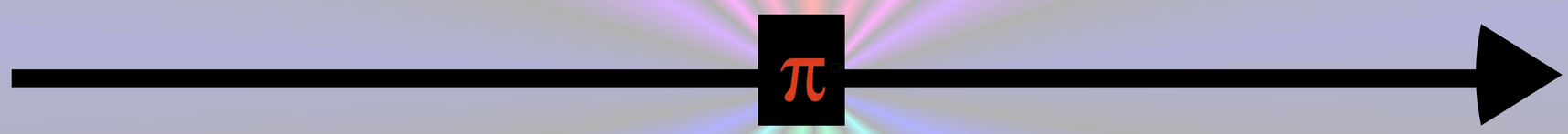
$\forall x \notin L \forall w \Pr([\text{face}](x,w)=\text{YES}) = 0$

Proofs



$(G_0, G_1) \notin ISO$





$G_0 \neq \pi(G_1)$

NO !

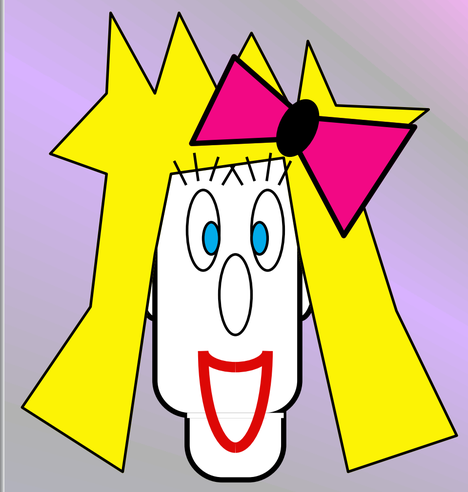
$\forall x \notin L \ \forall \pi D \ Pr(\ [\text{  }](x,\pi)=YES \ ) = 0$

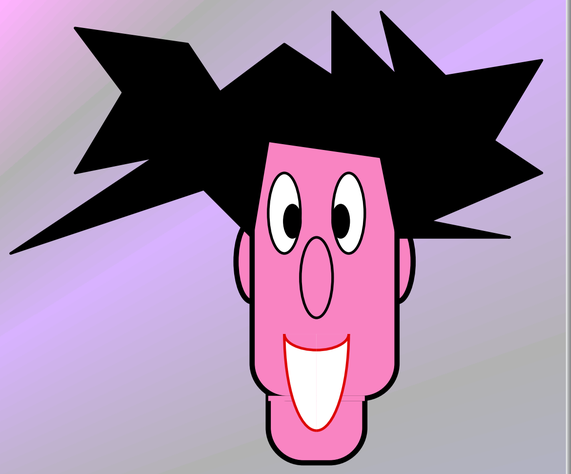
Interactive

Proofs

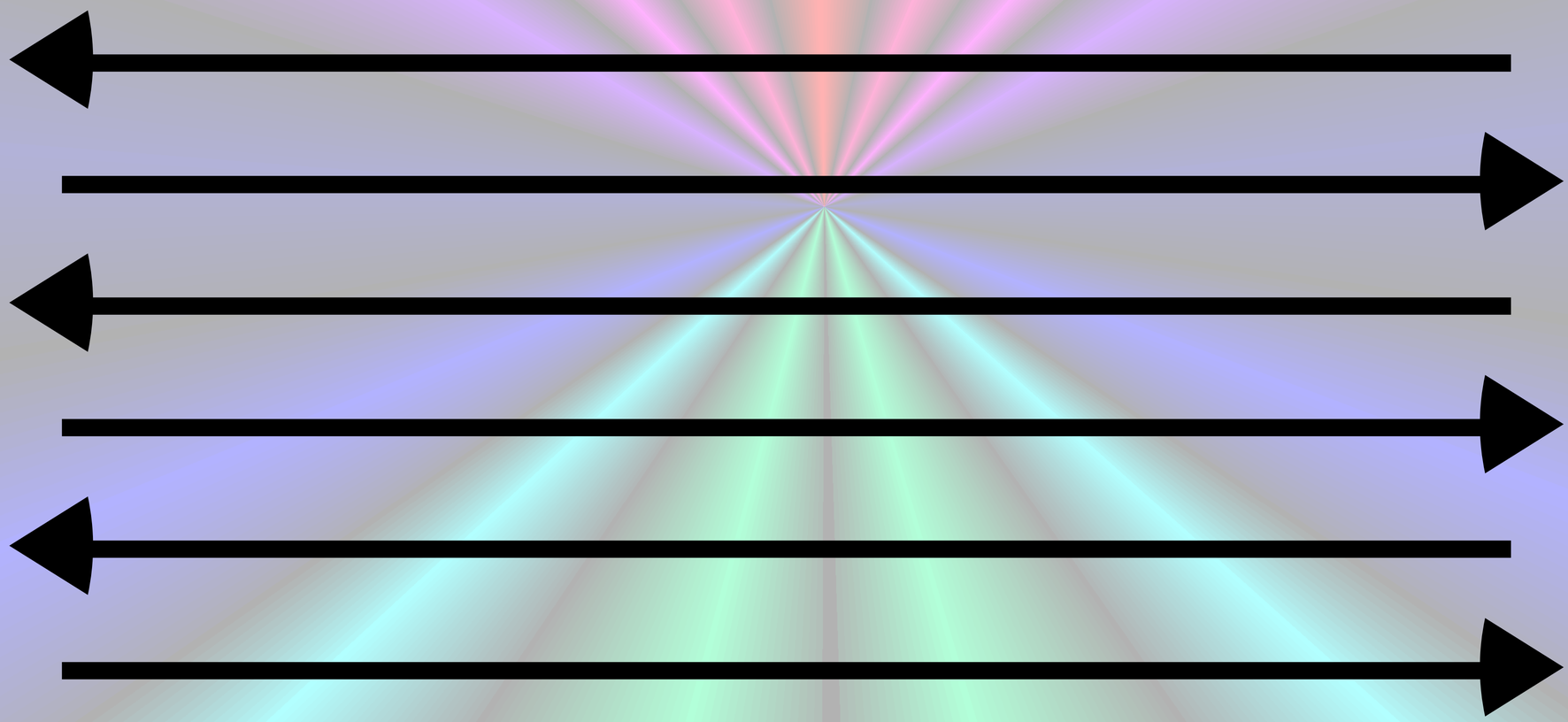
Interactive Proofs

Poly-Time





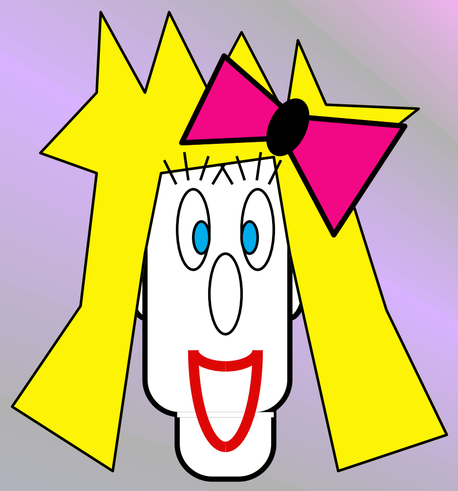
$x \in L$



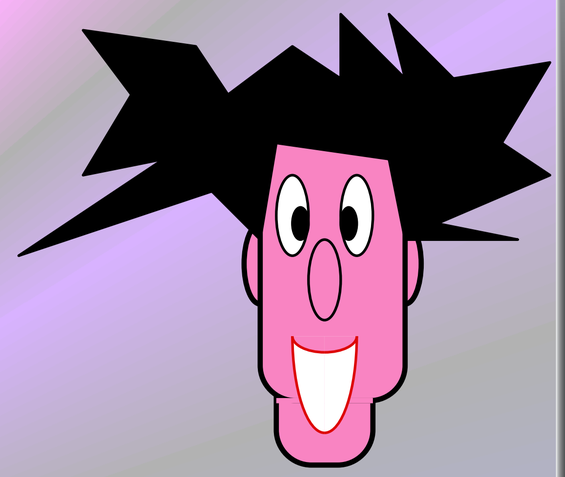
YES !

$\forall x \in L \Pr([\,,\,](x)=\text{YES}) > 2/3$

Interactive Proofs

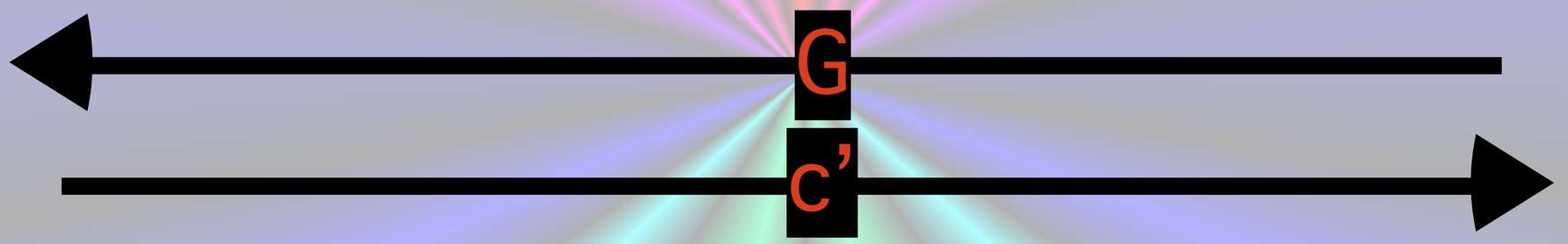


$(G_0, G_1) \in$ NON-ISO



$G \approx G_{c'}$

$G = \rho(G_c)$



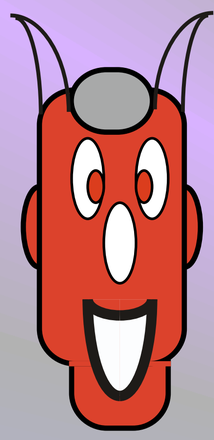
$c' = c$?

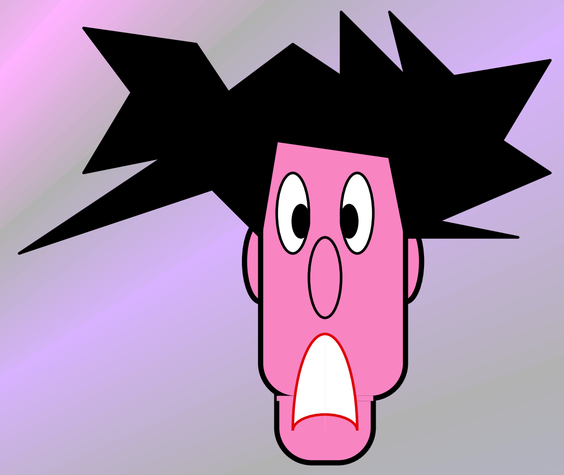
YES !

$\forall x \in L \Pr([\,,\,](x) = \text{YES}) = 1$

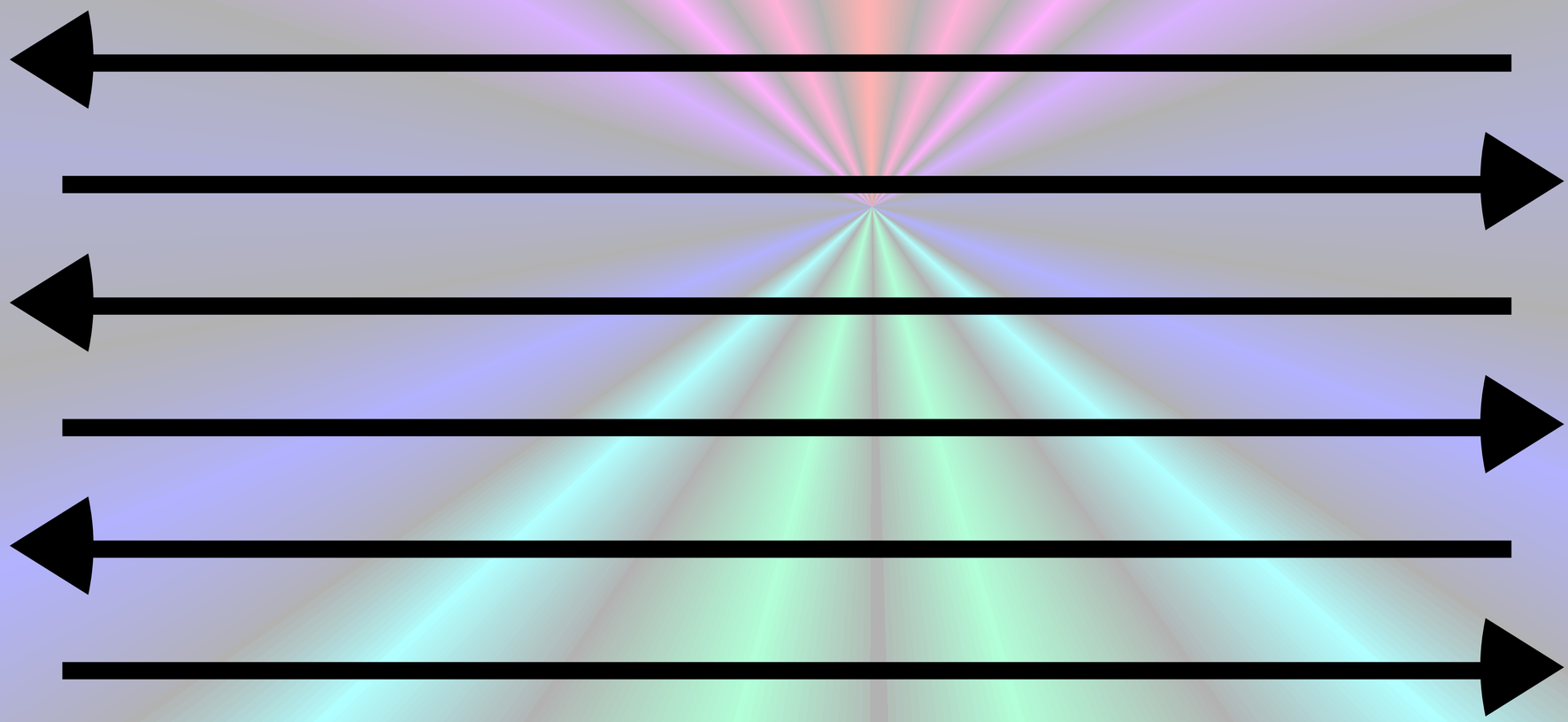
Interactive Proofs

Poly-Time

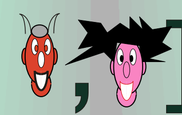




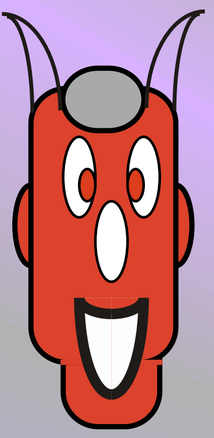
$x \notin L$



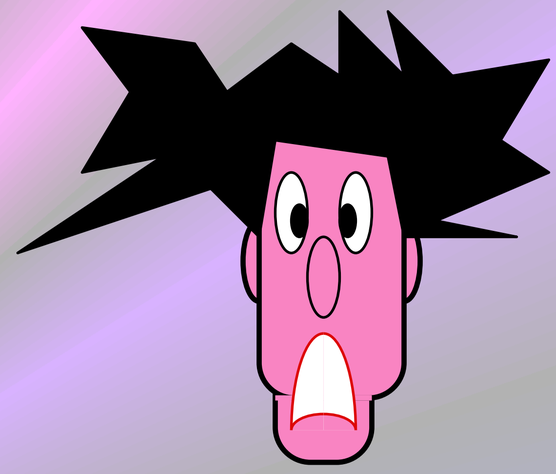
NO !

$\forall x \notin L \; \forall$  $\Pr([$  $](x)=YES) < 1/3$

Interactive Proofs

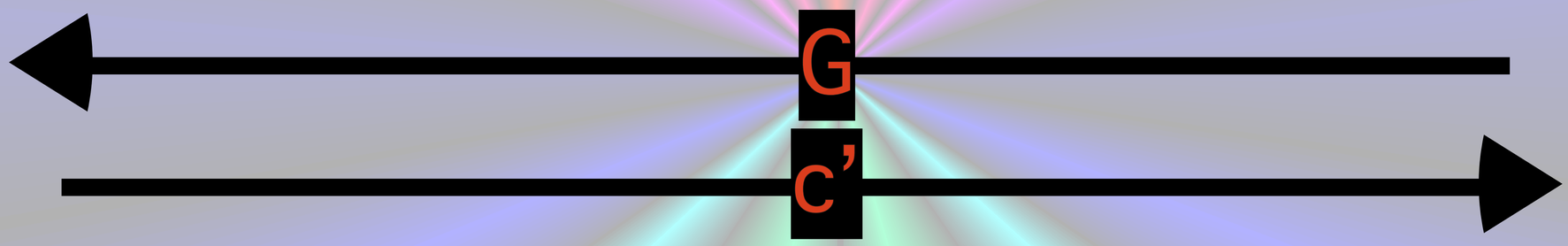


$(G_0, G_1) \notin$ NON-ISO



$G_0 \approx G \approx G_1$

$G = \rho(G_c)$

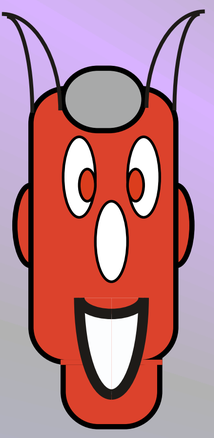


c'=c ?

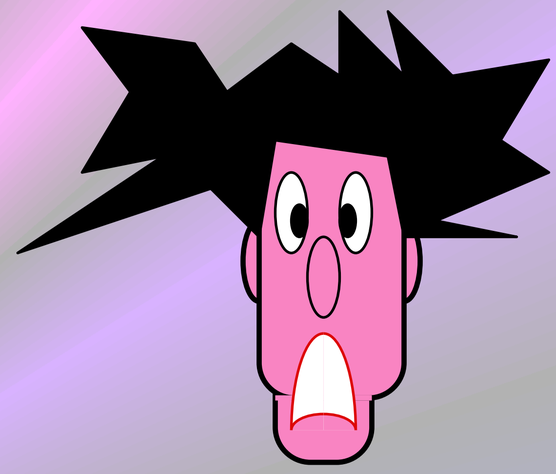
NO !

$\forall x \notin L \; \forall$  $\Pr([$  $](x)=\text{YES}) \leq 1/2$

Interactive Proofs



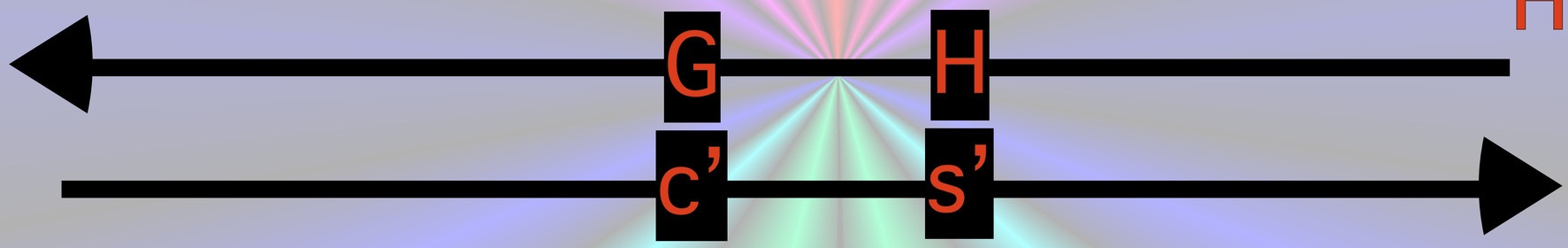
$(G_0, G_1) \notin$ NON-ISO



$G = \rho(G_c)$

$H = \pi(G_s)$

$G_0 \approx G \approx H \approx G_1$



REPEAT 2 TIMES
and say "YES" only if both "YES"

c'=c ?

s'=s ?

NO !

$\forall x \notin L \; \forall$  $\Pr([$  $](x)=\text{YES}) \leq 1/4$

Interactive Proof Definition

two-sided error

$\forall x \in L$ Pr([ , ](x)=YES) > 2/3

$\forall x \notin L$ $\forall$  Pr([ , ](x)=YES) < 1/3

$(G_0,G_1) \notin$ NON-ISO

one-sided error

$\forall x \in L$ Pr([ , ](x)=YES) = 1

$\forall x \notin L$ $\forall$  Pr([ , ](x)=YES) $\leq 1/2$

one-sided error

$\forall x \in L$ Pr([](x)=YES) = 1

$\forall x \notin L$ $\forall$  Pr([](x)=YES) $\leq \varepsilon < 1$

REPEAT k TIMES
and say "YES" only if k "YES"

$\forall x \in L$ Pr([](x)=YES) = 1

$\forall x \notin L$ $\forall$  Pr([](x)=YES) $\leq \varepsilon^k$

two-sided error

$\forall x \in L \Pr([\text{Alice},\text{Bob}](x)=\text{YES}) > 1/2+\varepsilon$

$\forall x \notin L \ \forall \text{Eve} \ \Pr([\text{Eve},\text{Bob}](x)=\text{YES}) < 1/2-\varepsilon$

REPEAT k TIMES

and say "YES" only if majority of "YES"

$\forall \varepsilon > 0$

$\exists \delta > 0$

$\forall x \in L \ \Pr([\text{Alice},\text{Bob}](x)=\text{YES}) > 1-\delta^k$

$\forall x \notin L \ \forall \text{Eve} \ \Pr([\text{Eve},\text{Bob}](x)=\text{YES}) < \delta^k$

Tail Bounds

Let $X = \sum_i X_i$ be a sum of independent random indicator variables X_i. For each i, let $p_i = \Pr[X_i = 1]$, and let $\mu = \mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = \sum_i p_i$.

Chernoff Bound (Upper Tail).

$$\Pr[X > (1+\delta)\mu] < \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu} \textit{ for any } \delta > 0.$$

$$\boxed{\Pr[X > (1+\delta)\mu] < e^{-\mu\delta^2/3}} \quad \text{for any } 0 < \delta < 1.$$

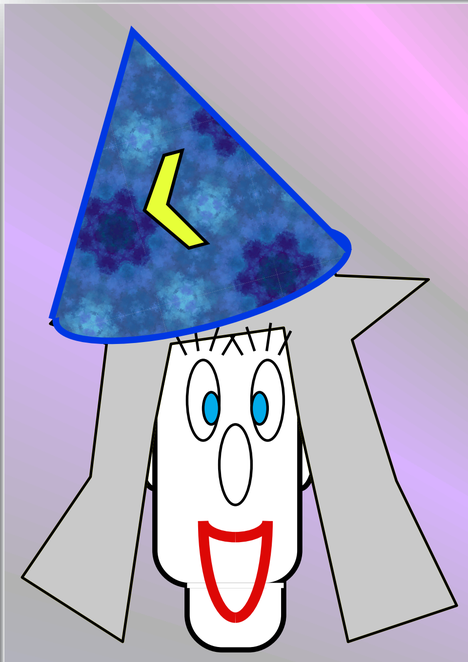
Chernoff Bound (Lower Tail).

$$\Pr[X < (1-\delta)\mu] < \left(\frac{e^{\delta}}{(1-\delta)^{1-\delta}}\right)^{\mu} < e^{-\mu\delta^2/2} \textit{ for any } \delta > 0.$$

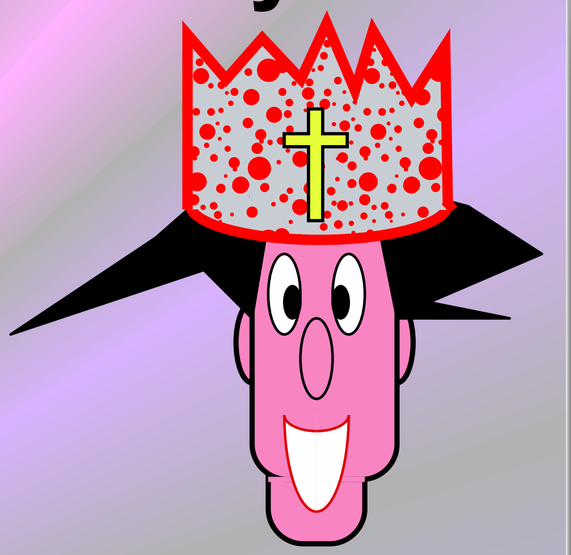
Arthur-Merlin

GAMES

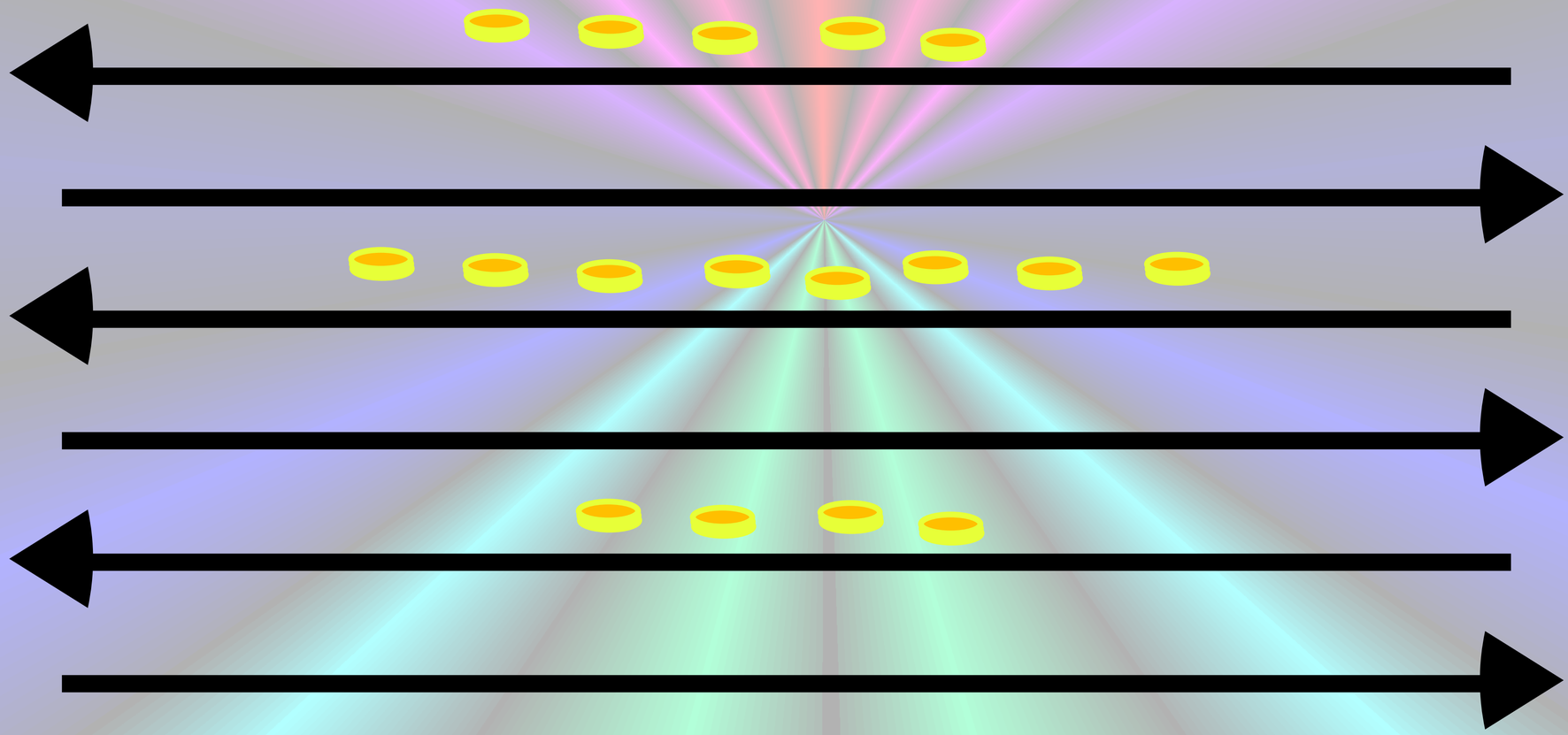
Arthur-Merlin Games



Poly-Time



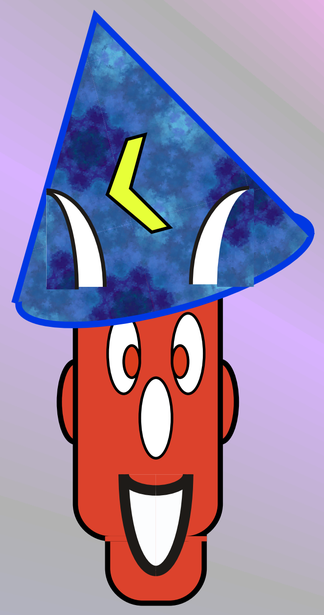
$x \in L$



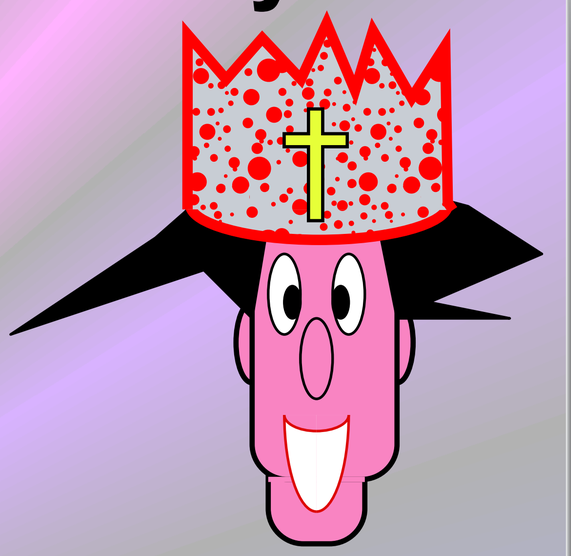
YES !

$\forall x \in L \Pr([A, M](x)=YES) > 2/3$

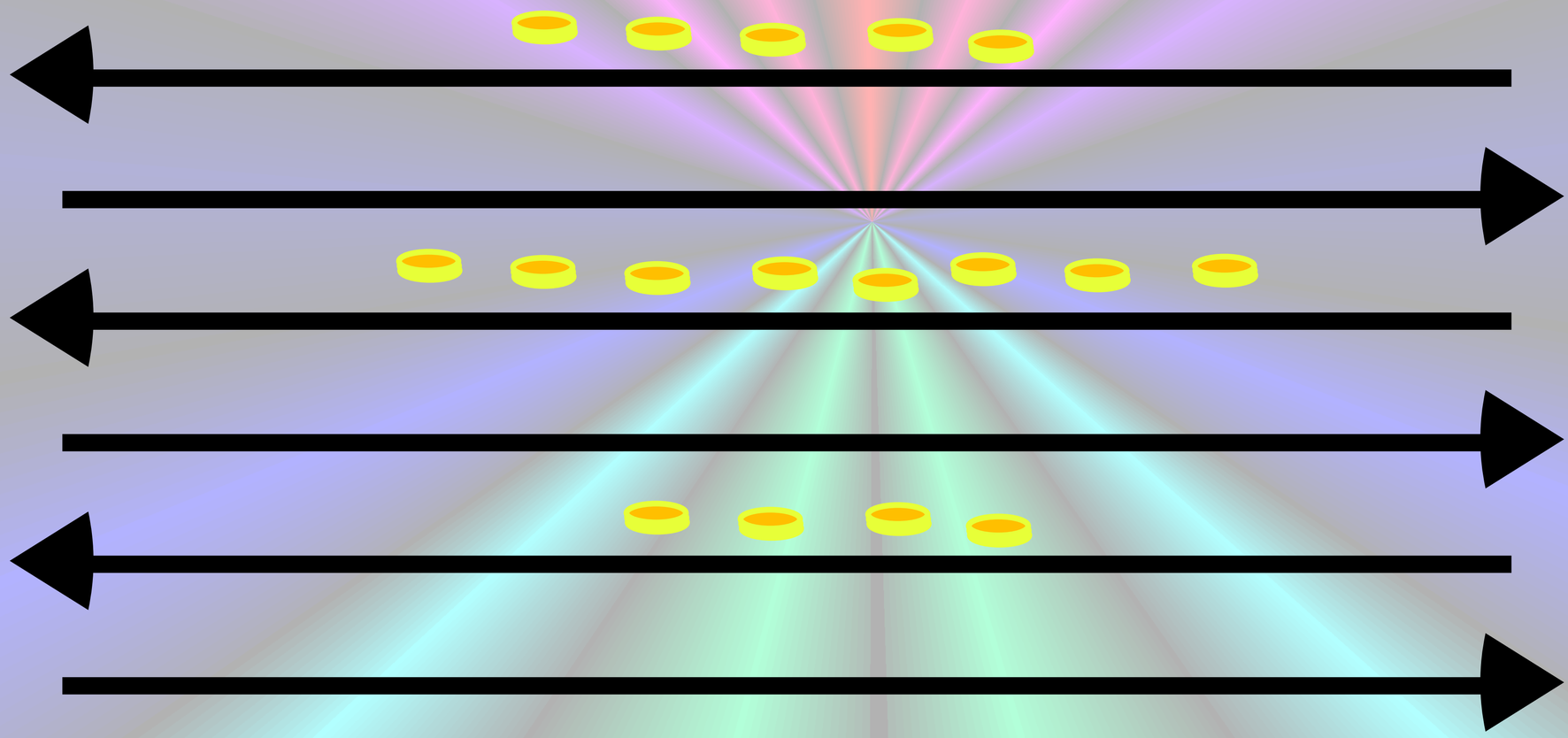
Interactive Proofs



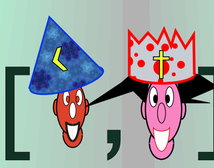
Poly-Time

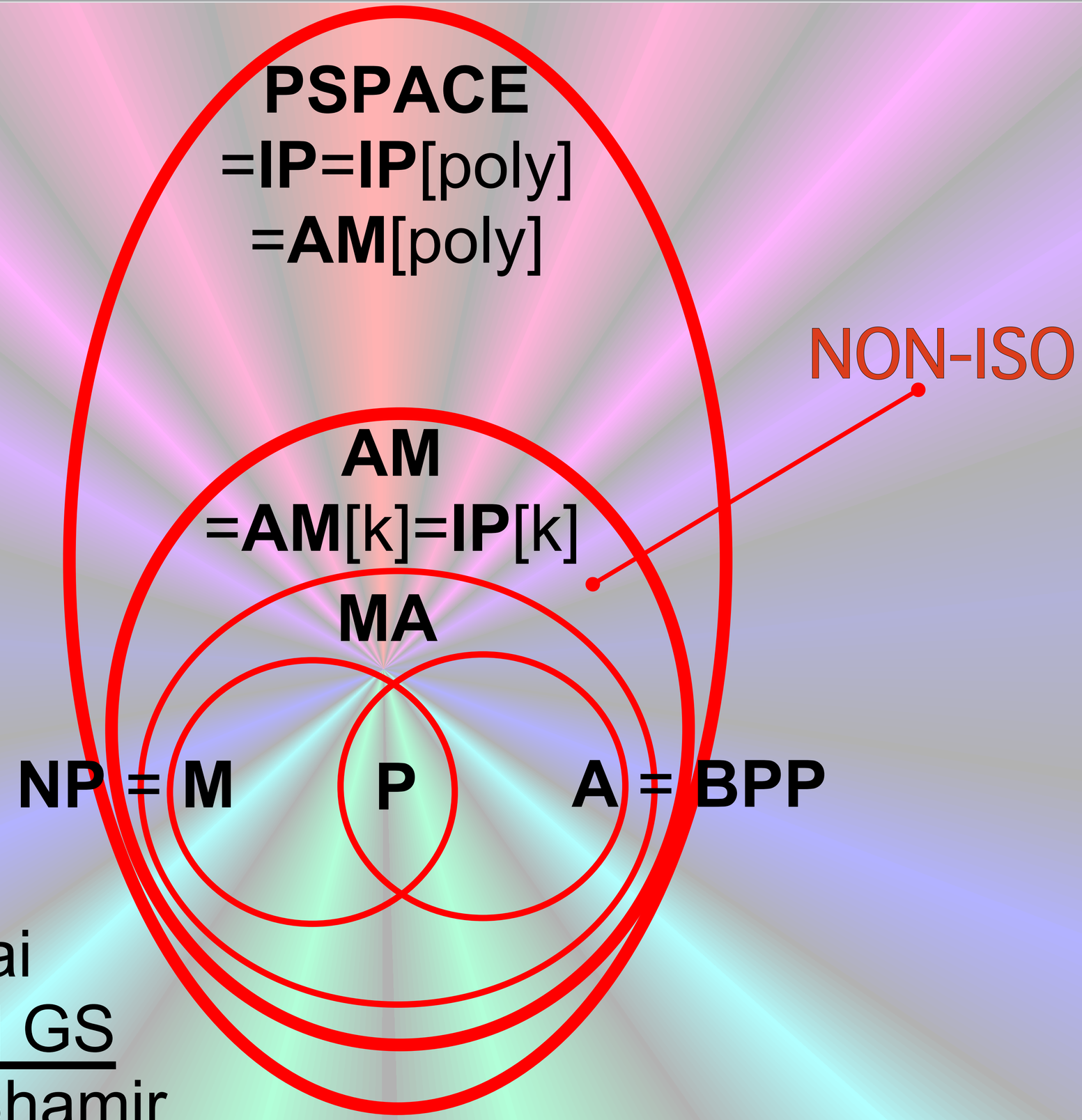


$x \notin L$



NO !

$\forall x \notin L \; \forall$  $\Pr([$  $](x)=\text{YES}) < 1/3$

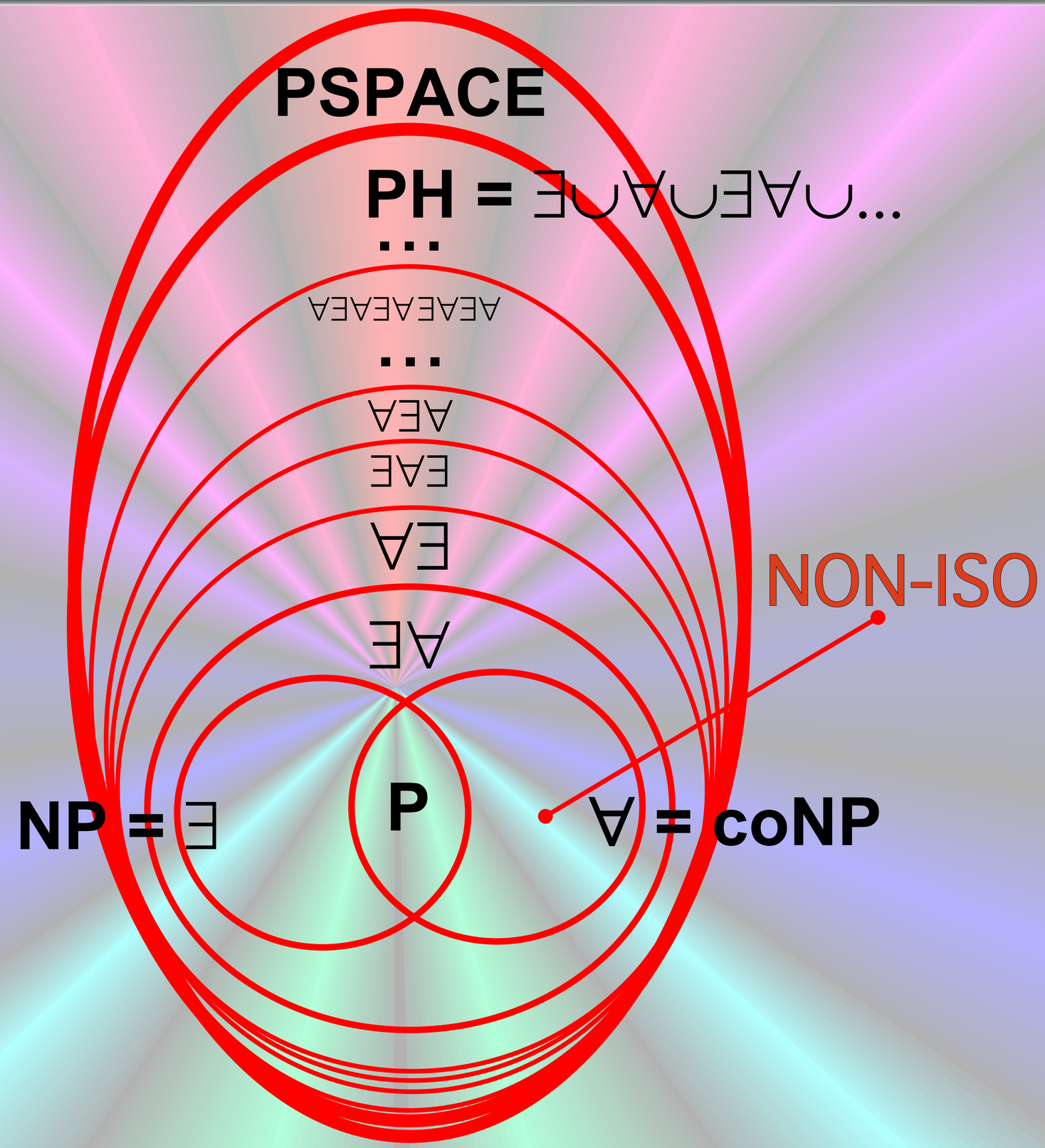


AM=**AM**[k] Babai

IP[Q]⊂**AM**[Q+2] GS

IP = **PSPACE** Shamir

Arthur-Merlin Hierarchy



Polynomial-time Hierarchy

PSPACE
=IP=IP[poly]
=AM[poly]

AM
=AM[k]**=IP**[k]

MA

NP = **M** **P** **A** = **BPP**

NON-ISO

PSPACE

PH = ∃∪∀∪∃∀∪...

...

∀∃∀∃∀∃∀

...

∀∃∀

∃∀∃

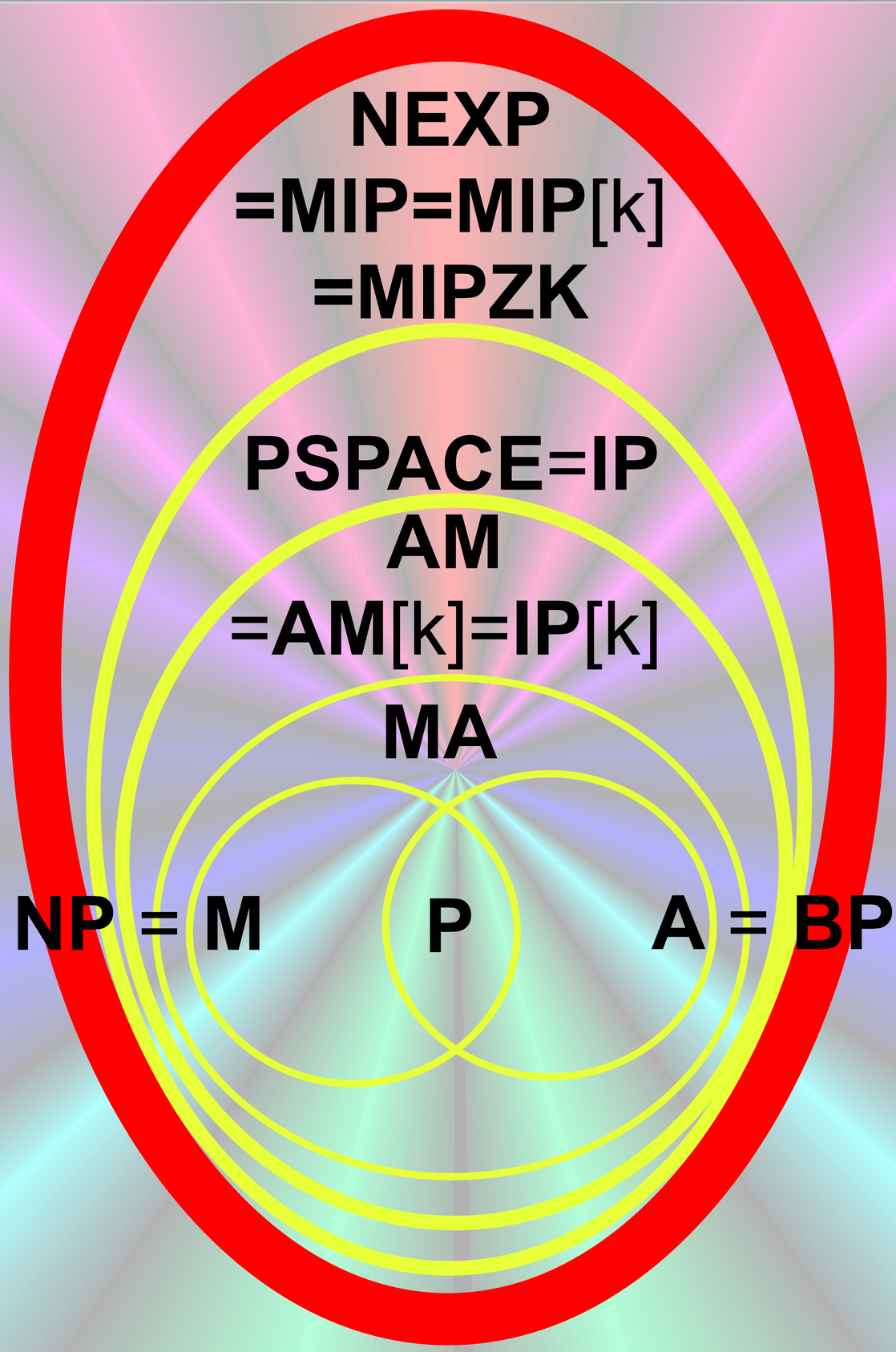
∃∀

∀∃

∃∀

NP = ∃ **P** ∀ = **coNP**

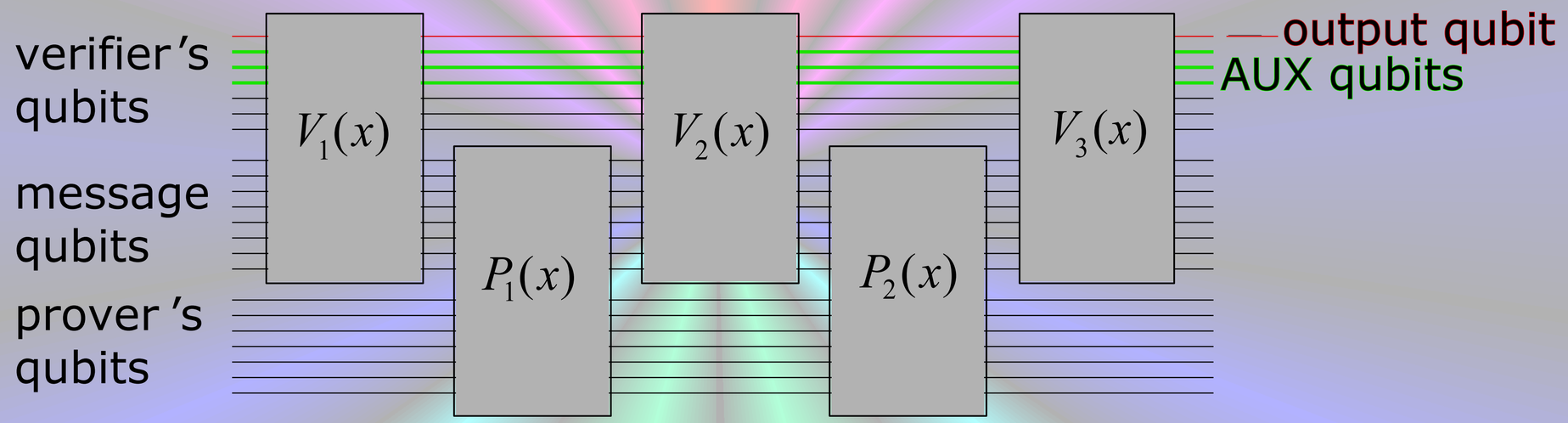
Arthur-Merlin vs Polynomial-time Hierarchy

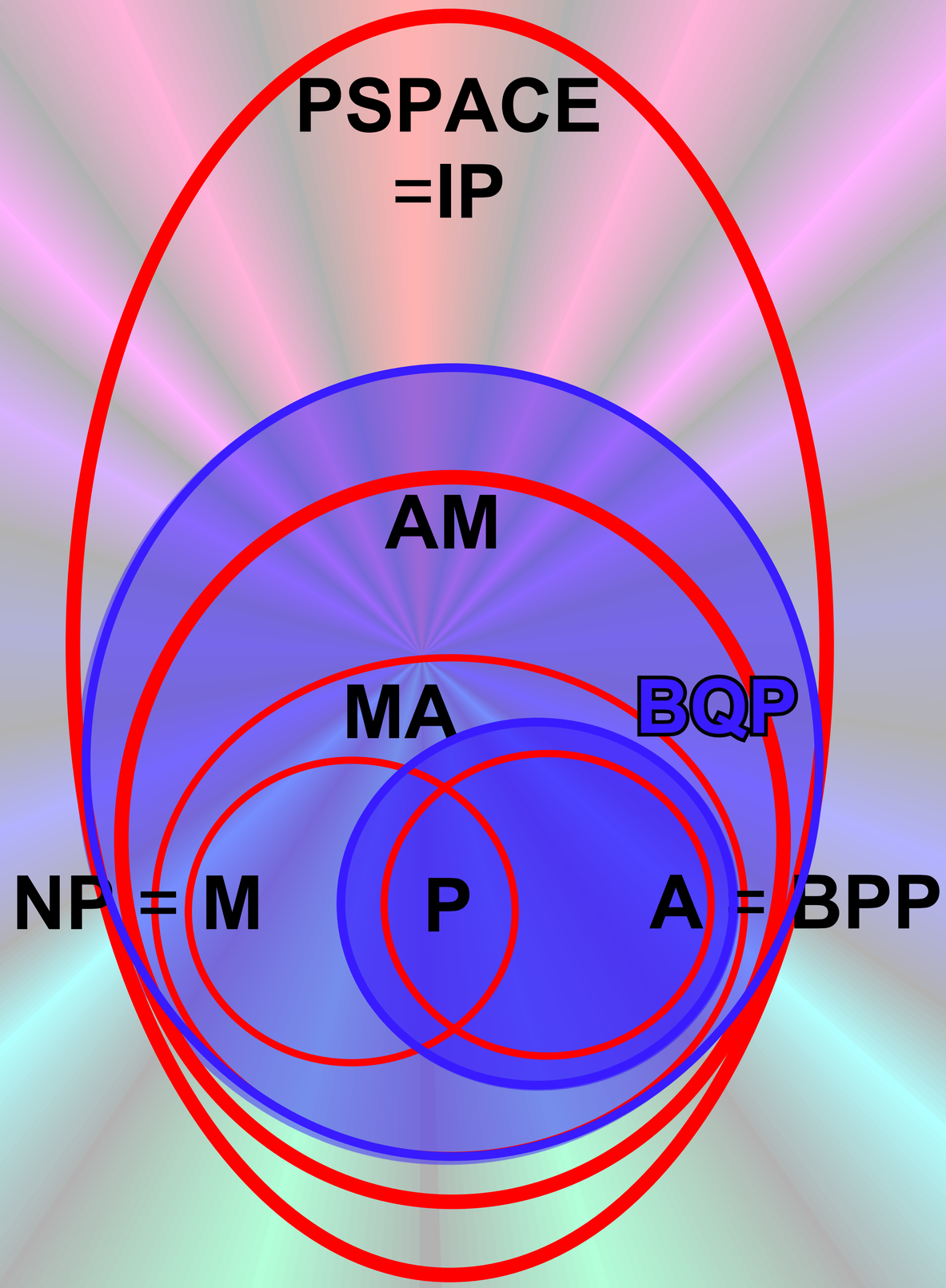


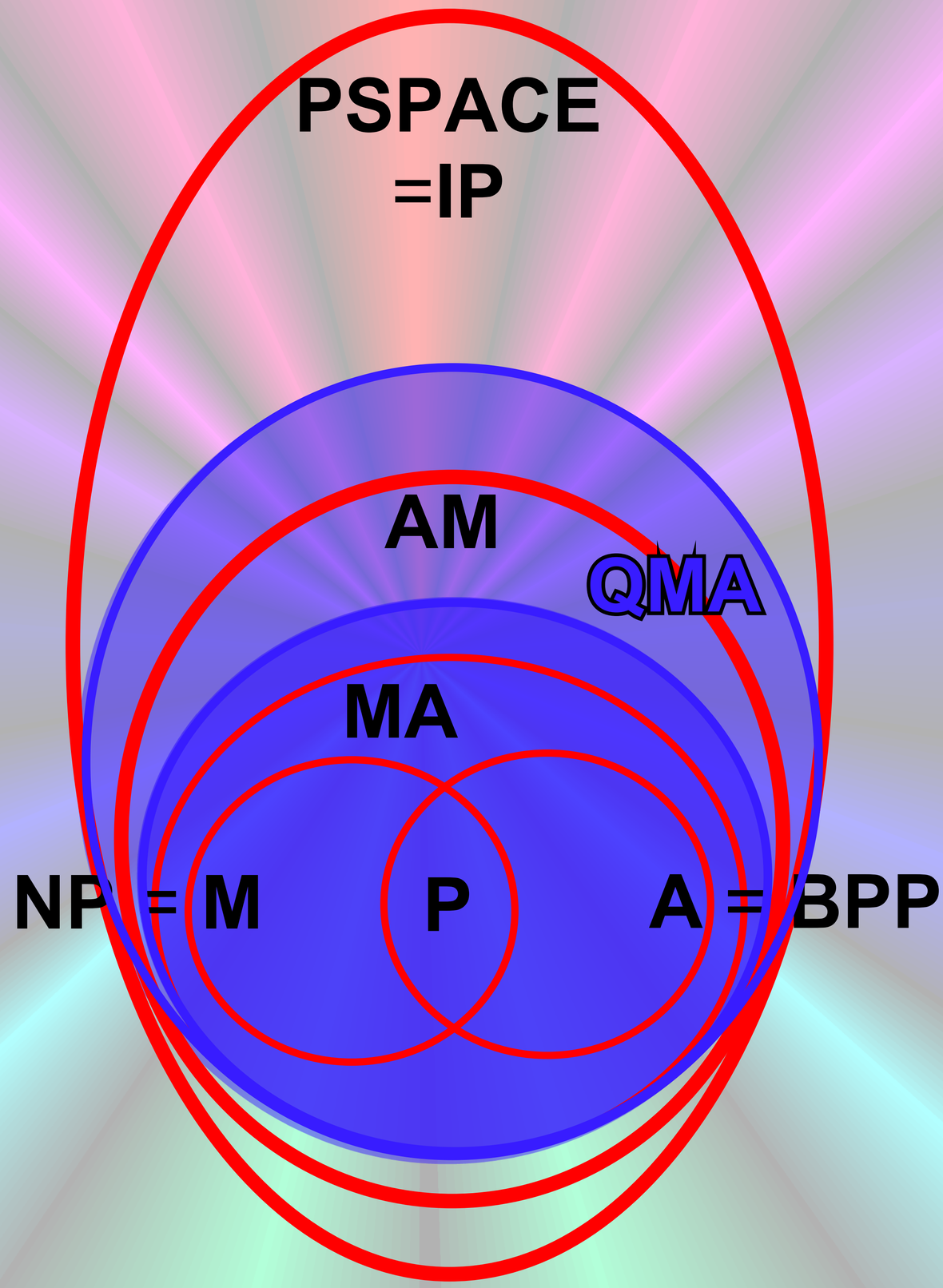
Multi-prover complexity: Arthur-Merlin vs MIP

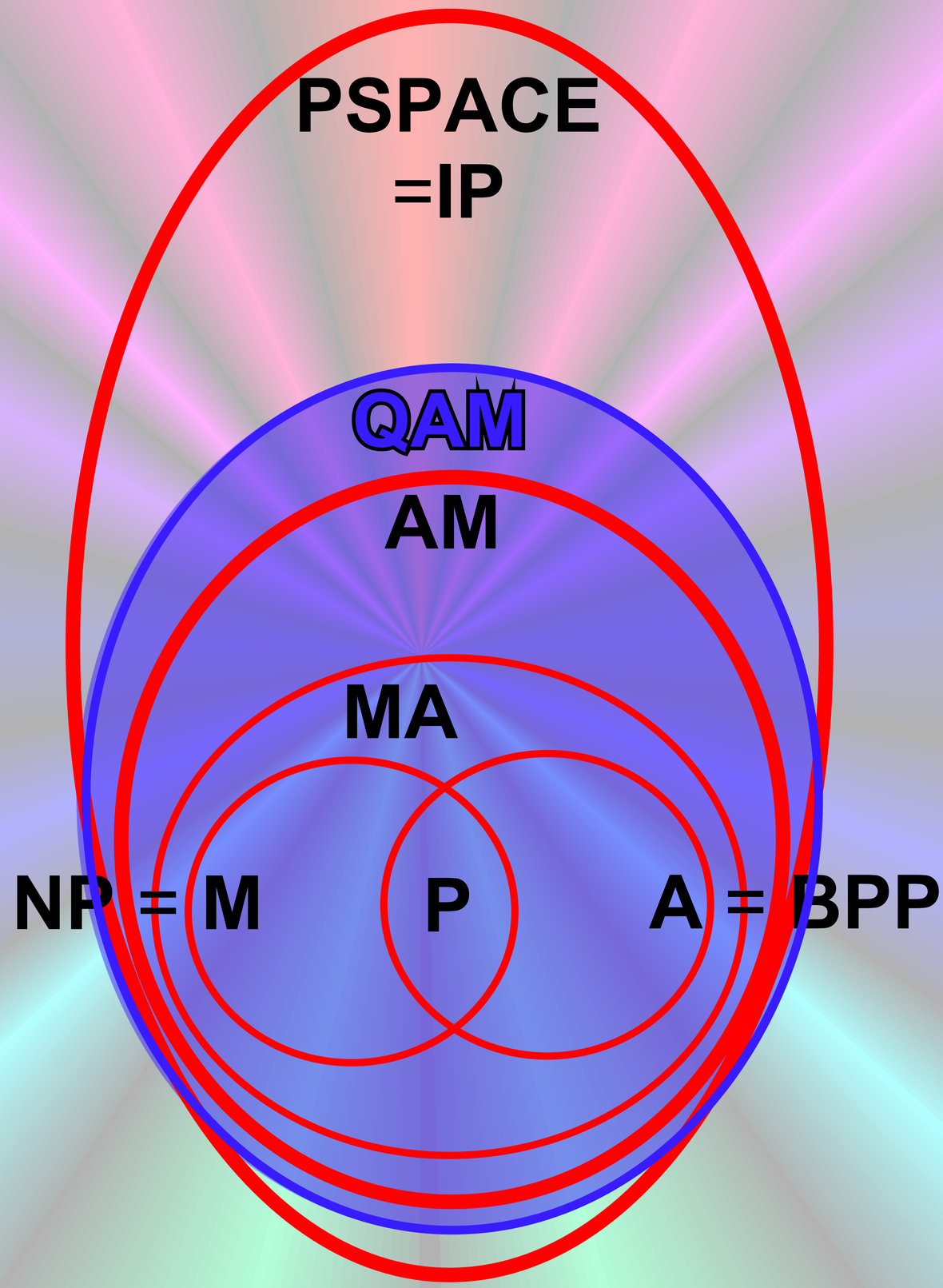
Quantum Interactive Proofs

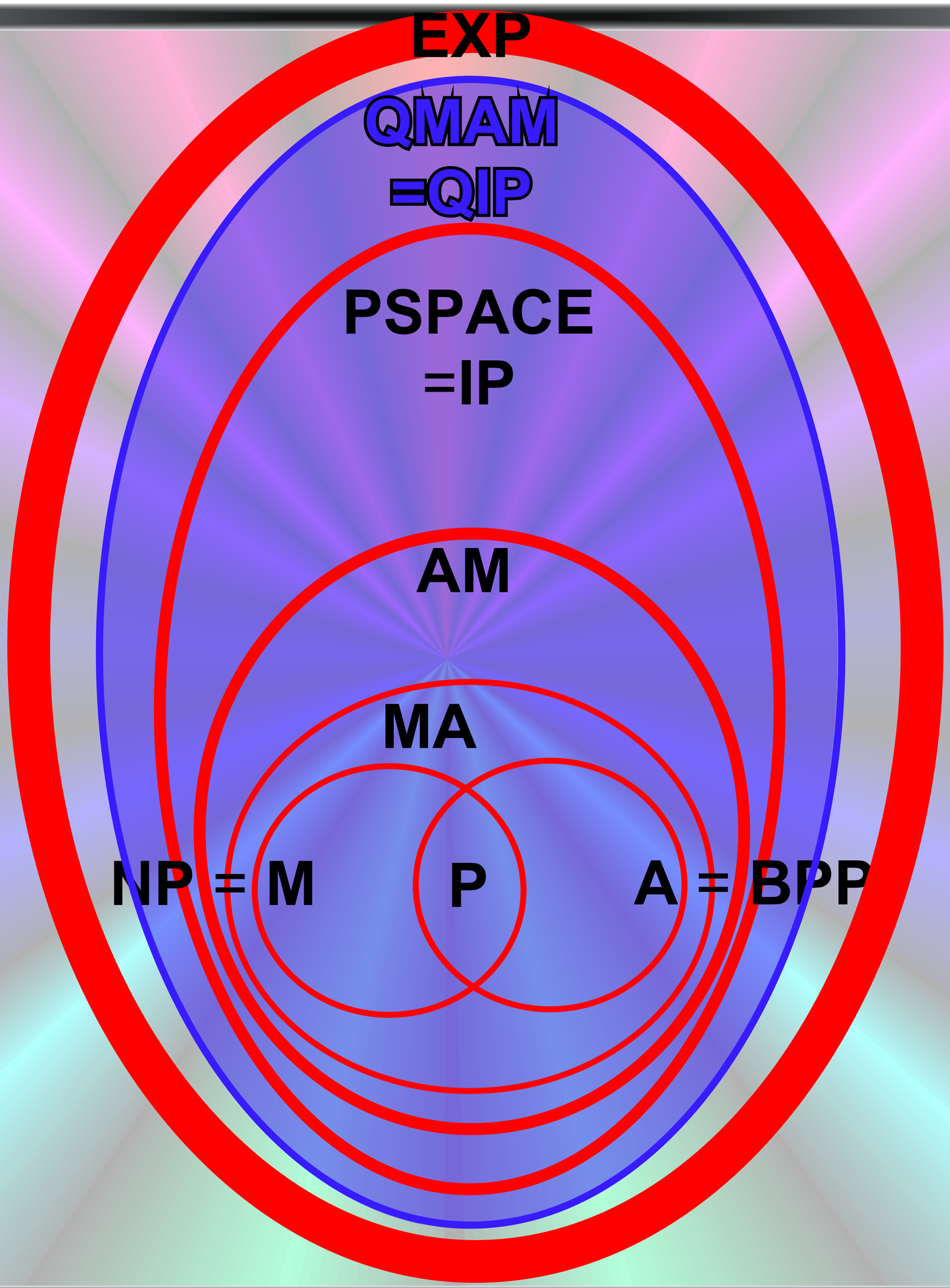
Quantum Interactive Proofs: Formalizing the Model

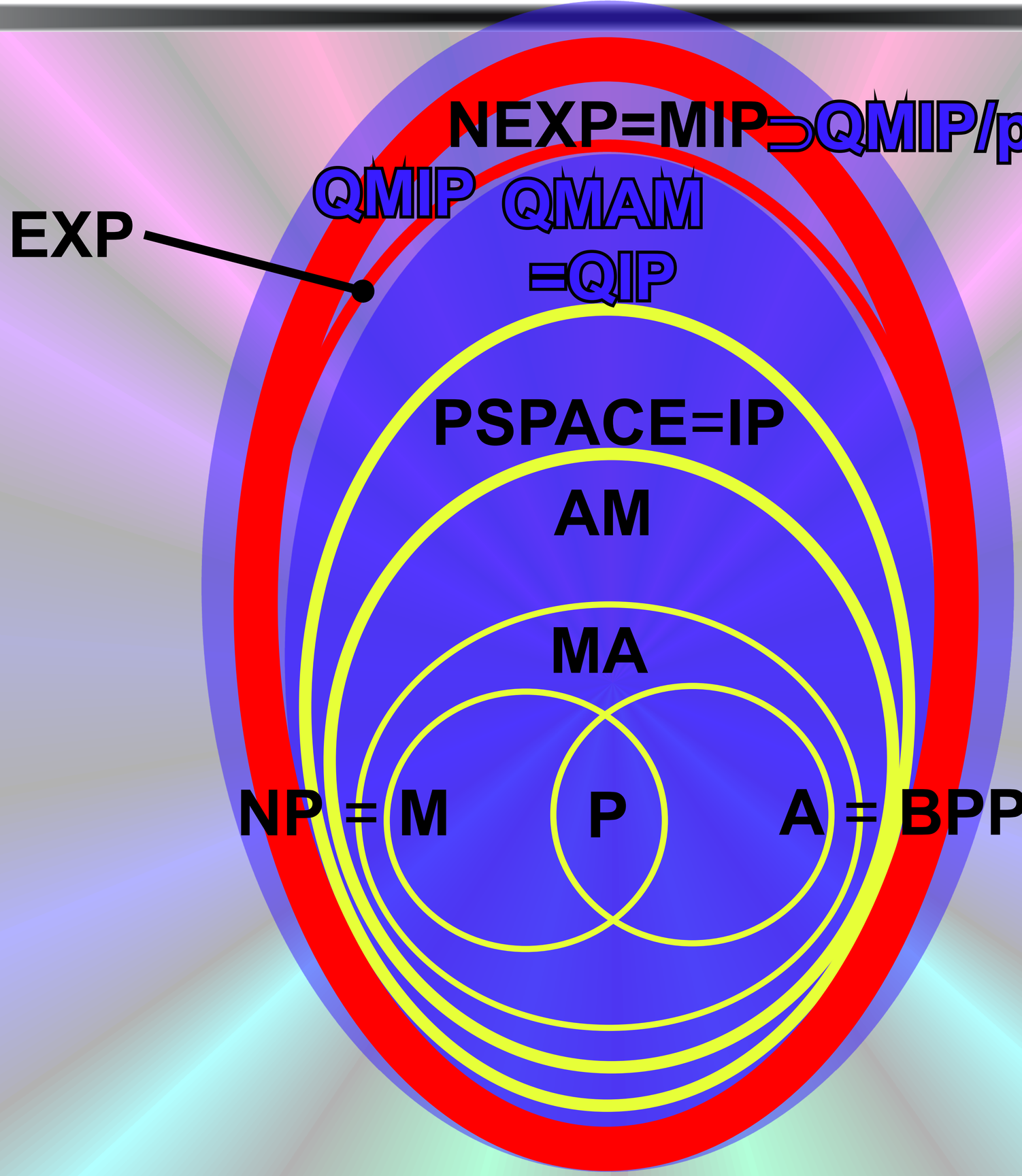









EXP
QMAM
=QIP
PSPACE
=IP
AM
MA
NP = M
P
A = BPP



Multi-prover complexity: Arthur-Merlin vs MIP

Interactive Proofs and Arthur-Merlin games

Claude Crépeau

School of Computer Science
McGill University