Quantum computation

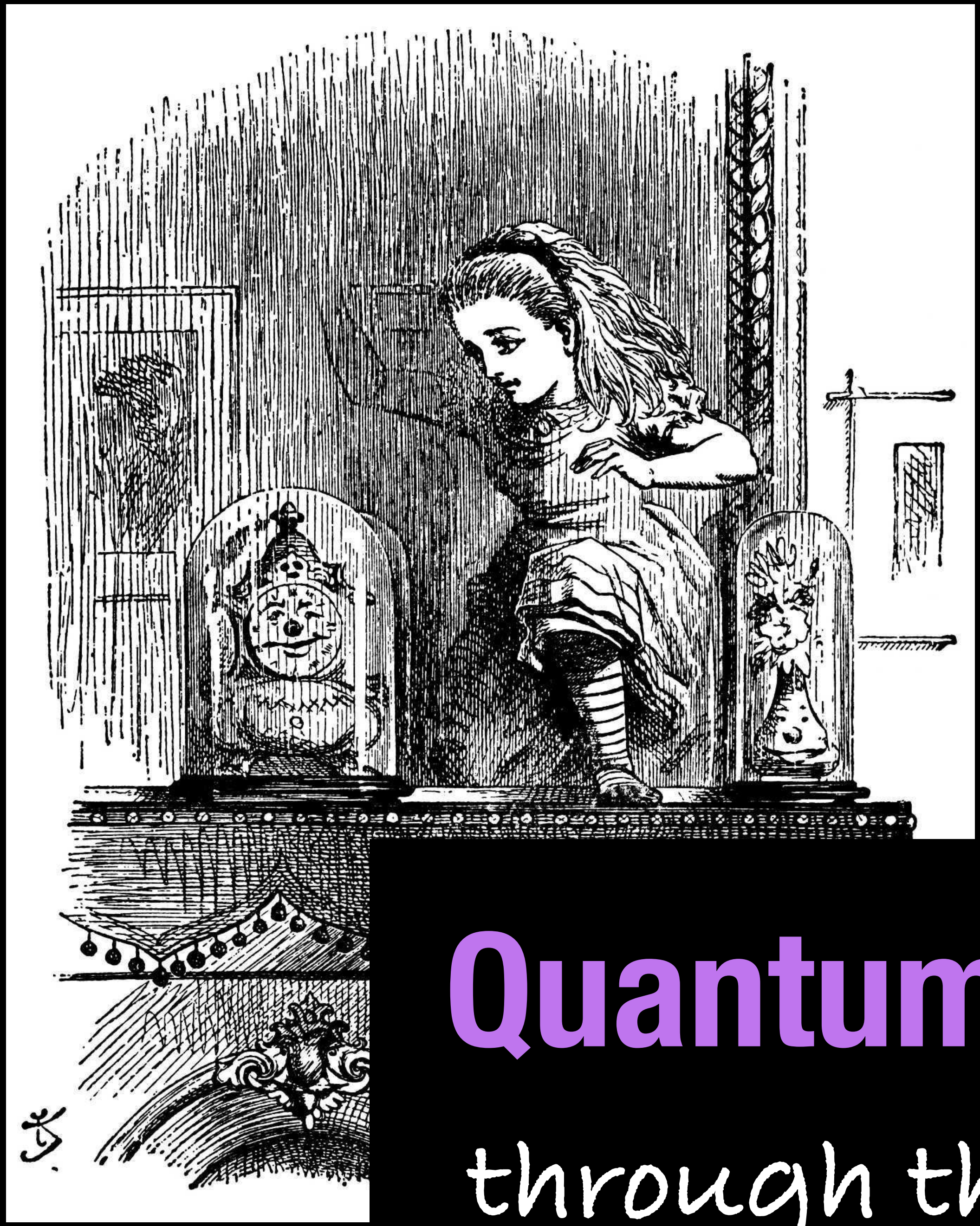
in the hall of mirrors

Niel de Beaudrap (Oxford)
CVQT, Edinburgh

Quantum computation

~~in the hall of mirrors~~

Niel de Beaudrap (Oxford)
CVQT, Edinburgh



Quantum computation

through the looking-glass

Niel de Beaudrap (Oxford)

CVQT, Edinburgh

The power of quantum

- It is commonly believed that quantum computation is a powerful model
- I don't disagree — but:

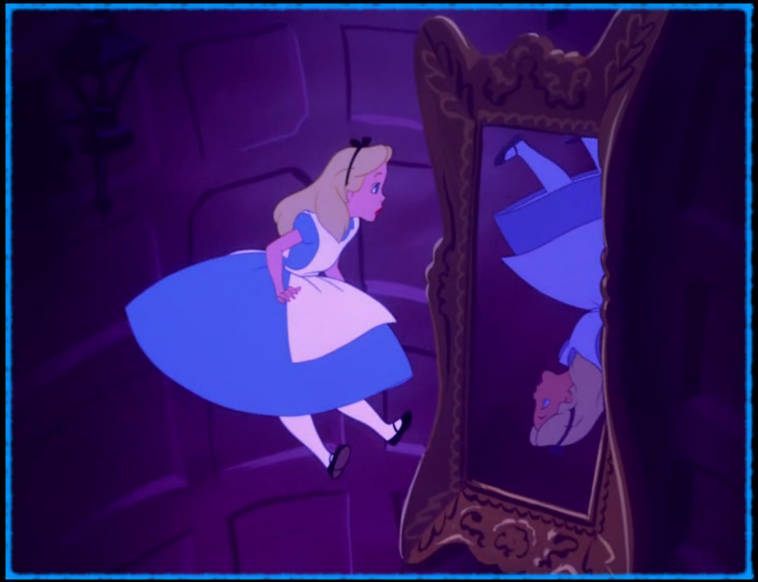
why?

- Three kinds of arguments:
  - Fundamental strangeness
  - Lack of known classical simulation techniques
  - Conjectures leading to "quantum advantage"

The power of quantum

- It is commonly believed that quantum computation is a powerful model
- I don't disagree — but:

why?



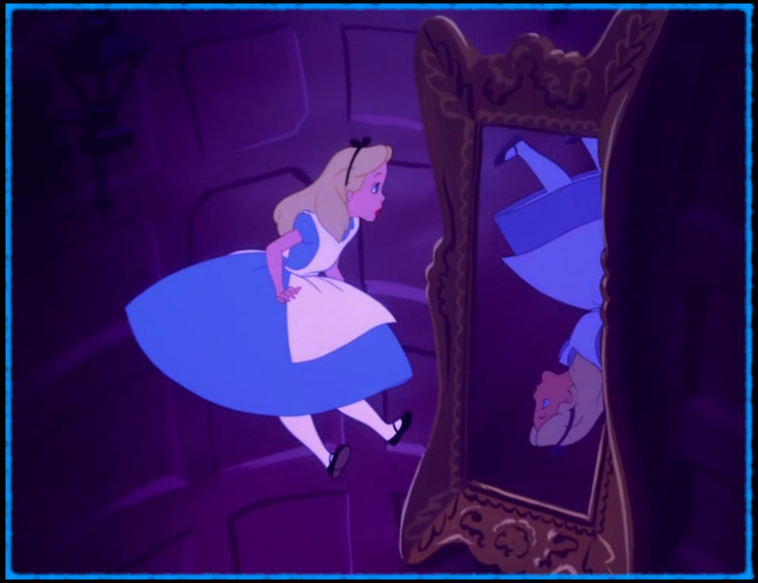
- Three kinds of arguments:
  - Fundamental strangeness
  - Lack of known classical simulation techniques
  - Conjectures leading to "quantum advantage"

The power of quantum

- It is commonly believed that quantum computation is a powerful model

- I don't disagree — but:

why?



- Three kinds of arguments:
    - Fundamental strangeness
    - Lack of known classical simulation techniques
    - Conjectures leading to "quantum advantage"

“Fundamental strangeness?”

- Quantum mechanical phenomena resist easy description in classical terms

"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as "lack of known classical simulation techniques"

"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as "lack of known classical simulation techniques"

Entanglement — or non-local correlations more generally

“Fundamental strangeness?”

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as “lack of known classical simulation techniques”

Entanglement — or non-local correlations more generally

Contextuality — *i.e.*, the lack of hidden-variable representations

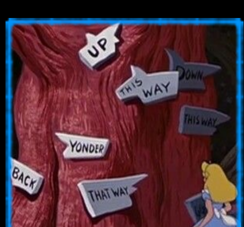
"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as "lack of known classical simulation techniques"


Entanglement — or non-local correlations more generally


Contextuality — *i.e.*, the lack of hidden-variable representations



Multiple bases which can store information

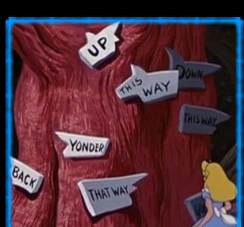
“Fundamental strangeness?”

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as “lack of known classical simulation techniques”

Entanglement — or non-local correlations more generally

Contextuality — *i.e.*, the lack of hidden-variable representations



Multiple bases which can store information

Destructive interference of potential outcomes

"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as "lack of known classical simulation techniques"

Entanglement — or non-local correlations more generally

how is this advantageous for computation?

Contextuality — *i.e.*, the lack of hidden-variable representations

Multiple bases which can store information

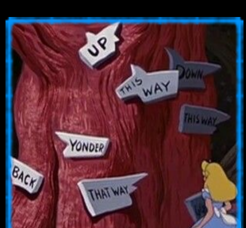
Destructive interference of potential outcomes

"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

Entanglement — or non-local correlations more generally

Contextuality — *i.e.*, the lack of hidden-variable representations



Multiple bases which can store information

Destructive interference of potential outcomes

careful — this is nearly the same as "lack of known classical simulation techniques"

how is this advantageous for computation?

this is **exactly** about the failure of a classical technique

"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as "lack of known classical simulation techniques"

Entanglement — or non-local correlations more generally

how is this advantageous for computation?

Contextuality — *i.e.*, the lack of hidden-variable representations

this is **exactly** about the failure of a classical technique

Multiple bases which can store information

better — if a bit vague

Destructive interference of potential outcomes

"Fundamental strangeness?"

- Quantum mechanical phenomena resist easy description in classical terms

careful — this is nearly the same as "lack of known classical simulation techniques"

Entanglement — or non-local correlations more generally

how is this advantageous for computation?

Contextuality — *i.e.*, the lack of hidden-variable representations

this is **exactly** about the failure of a classical technique

Multiple bases which can store information

better — if a bit vague

Destructive interference of potential outcomes

very promising

“Destructive Interference”?

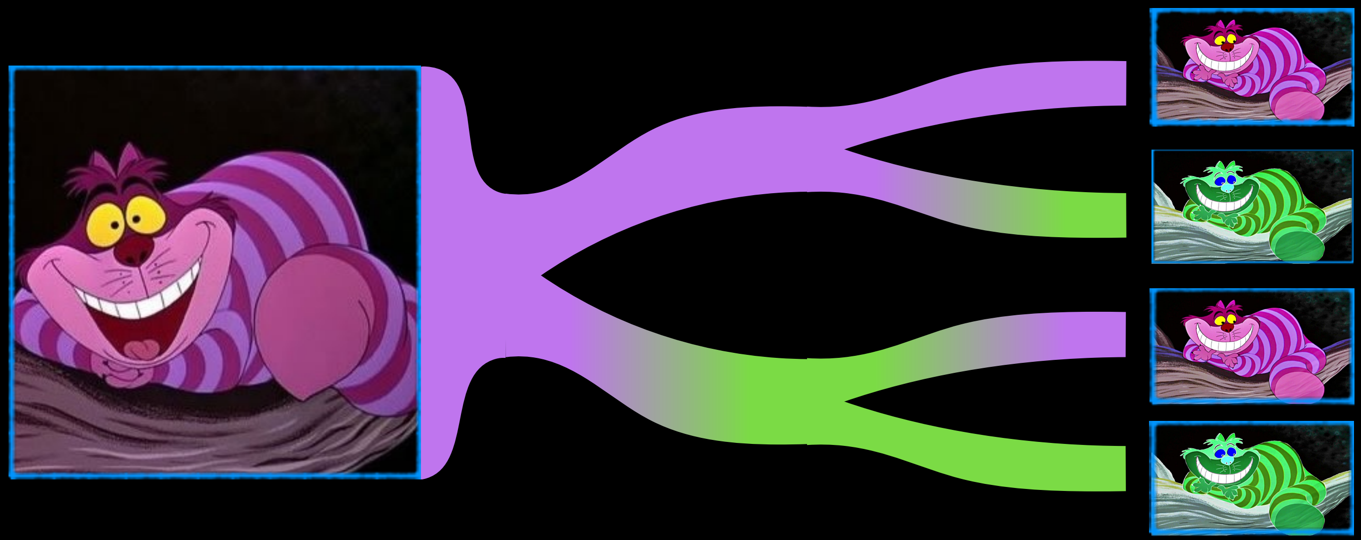
- **Interference**
  - *of wave patterns or external forces:*
    the cumulation or cancelation of deviations from some “relaxed” state
  - *by extension, motivated by quantum computation:*
    the adding or cancelling of the propensity of a physical process to yield one of several “possible outcomes”

“Destructive Interference”?

- **Interference**
  - *of wave patterns or external forces:*
    the cumulation or cancelation of deviations from some “relaxed” state
  - *by extension, motivated by quantum computation:*
    the adding or cancelling of the propensity of a physical process to yield one of several “possible outcomes”

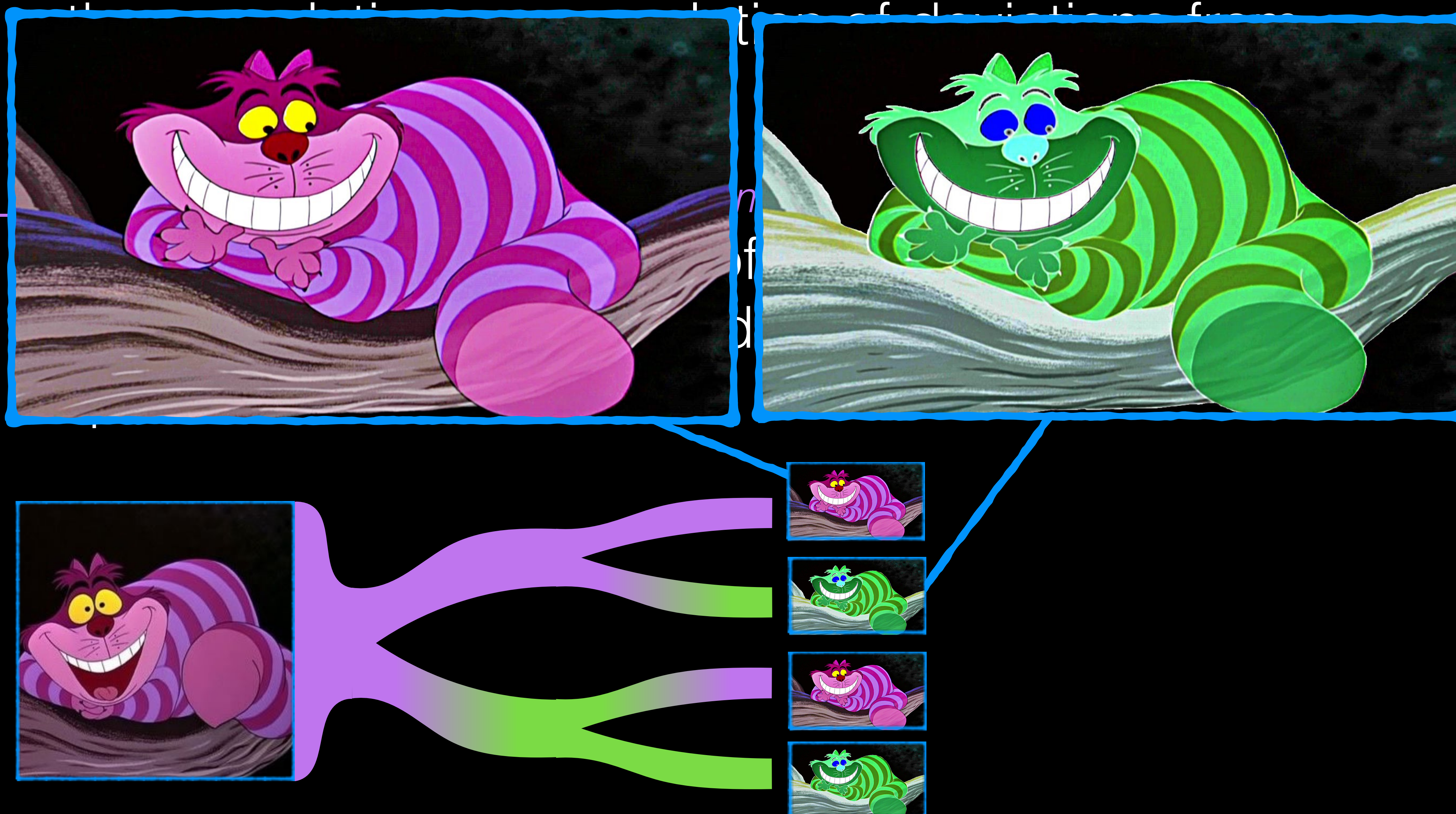
“Destructive Interference”?

- **Interference**
  - *of wave patterns or external forces:*
    the cumulation or cancelation of deviations from some “relaxed” state
  - *by extension, motivated by quantum computation:*
    the adding or cancelling of the propensity of a physical process to yield one of several “possible outcomes”



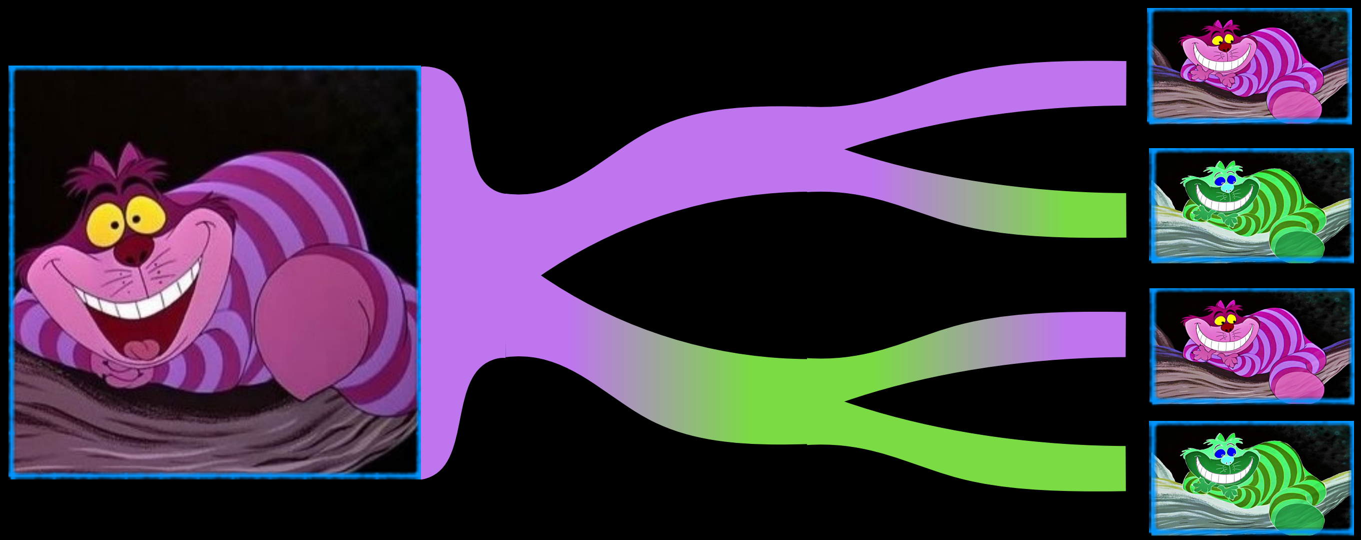
“Destructive Interference”?

- **Interference**
  - *of wave patterns or external forces:*



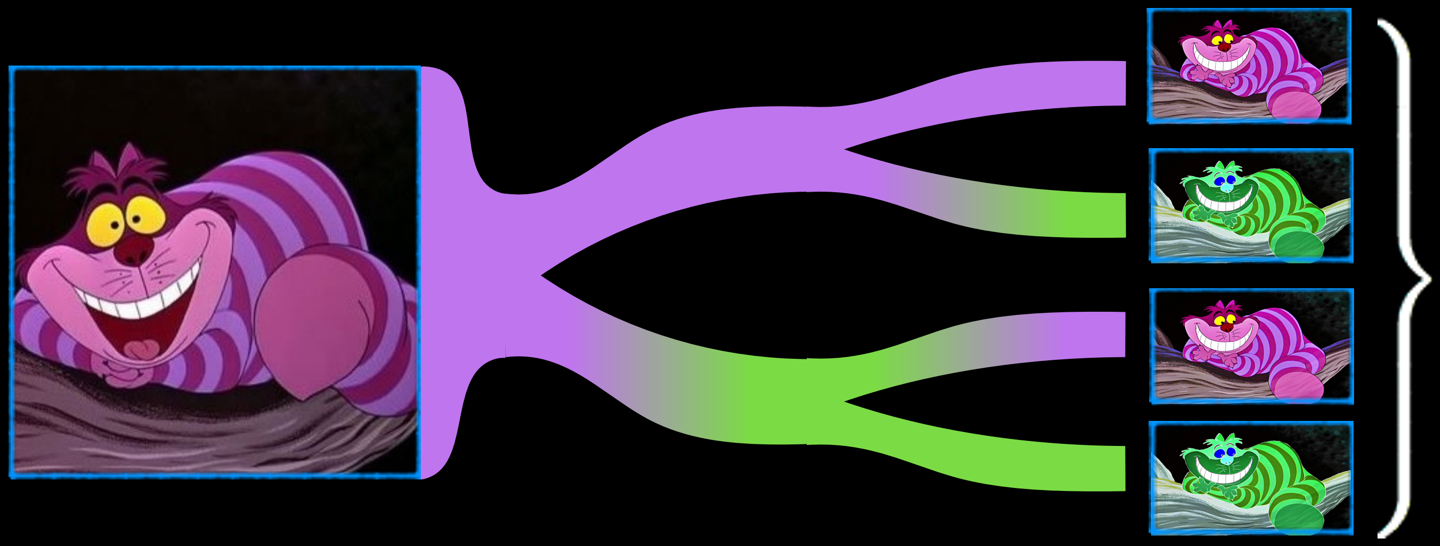
“Destructive Interference”?

- **Interference**
  - *of wave patterns or external forces:*
    the cumulation or cancelation of deviations from some “relaxed” state
  - *by extension, motivated by quantum computation:*
    the adding or cancelling of the propensity of a physical process to yield one of several “possible outcomes”



“Destructive Interference”?

- **Interference**
  - *of wave patterns or external forces:*
    the cumulation or cancelation of deviations from some “relaxed” state
  - *by extension, motivated by quantum computation:*
    the adding or cancelling of the propensity of a physical process to yield one of several “possible outcomes”

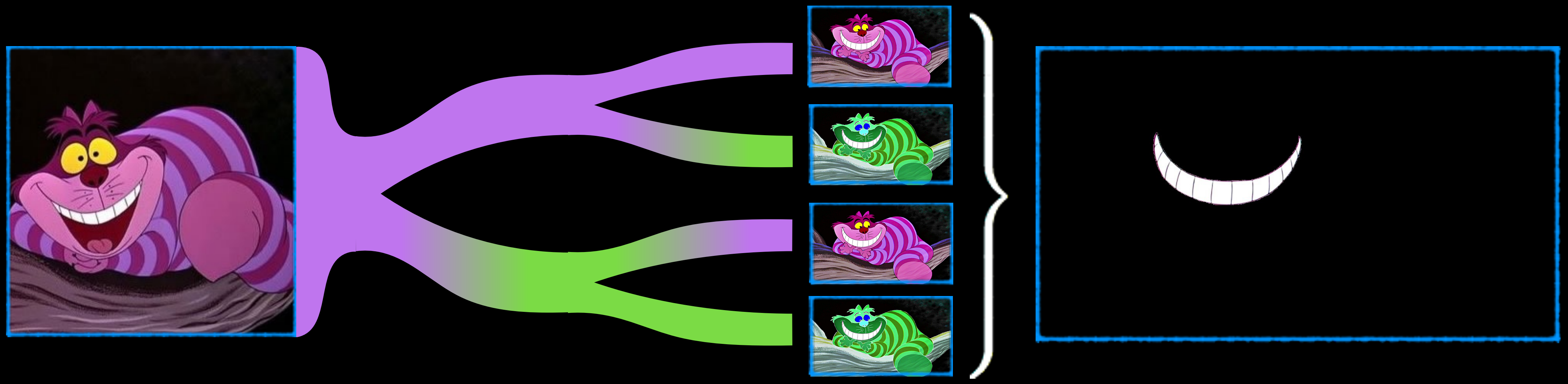


“Destructive Interference”?

- **Interference**

  of wave patterns or external forces:
  the cumulation or cancelation of deviations from some “relaxed” state

  by extension, motivated by quantum computation:
  the adding or cancelling of the propensity of a physical process to yield one of several “possible outcomes”



Questions

- Could destructive interference yield intuitions about the power of quantum computing?
- How to even explore this question, if destructive interference *presumes* quantum computing?

Questions

- Could destructive interference yield intuitions about the power of quantum computing?
- How to even explore this question, if destructive interference *presumes* quantum computing?

Results

- An approach to studying **quasi-quantum** models of computation — funhouse-mirror physics
- Characterisations of some quasi-quantum models, in terms of *counting complexity*

Preliminaries

sums over paths
& counting complexity

Sums over paths

- **Computational "paths"** —
  a (counterfactual) description of the state of the system over time, along with an amplitude for the entire path

Sums over paths

- **Computational "paths" —**
  a (counterfactual) description of the state of the system over time, along with an amplitude for the entire path
  - a sequence of standard basis states for each instant — like a computational branch of an NTM

Sums over paths

- **Computational "paths"** —
  a (counterfactual) description of the state of the system over time, along with an amplitude for the entire path
  - a sequence of standard basis states for each instant — like a computational branch of an NTM
- Evolution given by **sum of the amplitudes of each path,** associated with reaching each possible endpoint — a form of Huygen's principle for computation

Sums over paths

- **Computational "paths"** —
  a (counterfactual) description of the state of the system over time, along with an amplitude for the entire path
  - a sequence of standard basis states for each instant — like a computational branch of an NTM
- Evolution given by **sum of the amplitudes of each path,** associated with reaching each possible endpoint — a form of Huygen's principle for computation
- This is the principle behind all known relations between quantum computation and **counting classes**

Sums over paths *for NTMs*

- **Counting complexity** —
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:

Sums over paths *for NTMs*

- **Counting complexity —**
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
  - Uniformly assign weights to accepting / rejecting branches

Sums over paths *for NTMs*

- **Counting complexity —**
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
  - Uniformly assign weights to accepting / rejecting branches
  - Sum over all branches (possibly depending on contents of the tapes)

Sums over paths *for NTMs*

- **Counting complexity —**
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
  - Uniformly assign weights to accepting / rejecting branches
  - Sum over all branches (possibly depending on contents of the tapes)
  - Ask questions about the resulting sum

Sums over paths *for NTMs*

- **Counting complexity —**
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
  - Uniformly assign weights to accepting / rejecting branches
  - Sum over all branches (possibly depending on contents of the tapes)
  - Ask questions about the resulting sum

NP — is the total zero, or is it non-zero? ($w_A > 0$, $w_R = 0$)

Sums over paths *for NTMs*

- **Counting complexity** —
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
  - Uniformly assign weights to accepting / rejecting branches
  - Sum over all branches (possibly depending on contents of the tapes)
  - Ask questions about the resulting sum

NP — is the total zero, or is it non-zero? ($w_A > 0$, $w_R = 0$)

BPP — is the total $\leqslant \frac{1}{3}$, or is it $\geqslant \frac{2}{3}$? ($w_A = 1/N$, $w_R = 0$)

Sums over paths *for NTMs*

- **Counting complexity —** given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
    - Uniformly assign weights to accepting / rejecting branches
    - Sum over all branches (possibly depending on contents of the tapes)
    - Ask questions about the resulting sum

NP — is the total zero, or is it non-zero? ($w_A > 0$, $w_R = 0$)

BPP — is the total $\leqslant \frac{1}{3}$, or is it $\geqslant \frac{2}{3}$? ($w_A = 1/N$, $w_R = 0$)

PP — is the total $< \frac{1}{2}$, or is it $\geqslant \frac{1}{2}$? ($w_A = 1/N$, $w_R = -1/N$)

Sums over paths *for NTMs*

- **Counting complexity —**
  given a fixed **nondeterministic Turing Machine** (NTM) in which the branches form a complete k-ary tree with N leaves:
  - Uniformly assign weights to accepting / rejecting branches
  - Sum over all branches (possibly depending on contents of the tapes)
  - Ask questions about the resulting sum

NP — is the total zero, or is it non-zero? ($w_A > 0$, $w_R = 0$)

BPP — is the total $\leqslant \frac{1}{3}$, or is it $\geqslant \frac{2}{3}$? ($w_A = 1/N$, $w_R = 0$)

PP — is the total $< \frac{1}{2}$, or is it $\geqslant \frac{1}{2}$? ($w_A = 1/N$, $w_R = -1/N$)

AWPP — is the $|\text{total}|^2 \leqslant \frac{1}{3}$, or is it $\geqslant \frac{2}{3}$? ($w_A = +1/h(N)$, $w_R = -1/h(N)$)

Counting complexity

$P^{\#P}$

PP

AWPP

"very very hard"

"hard" NP

BPP

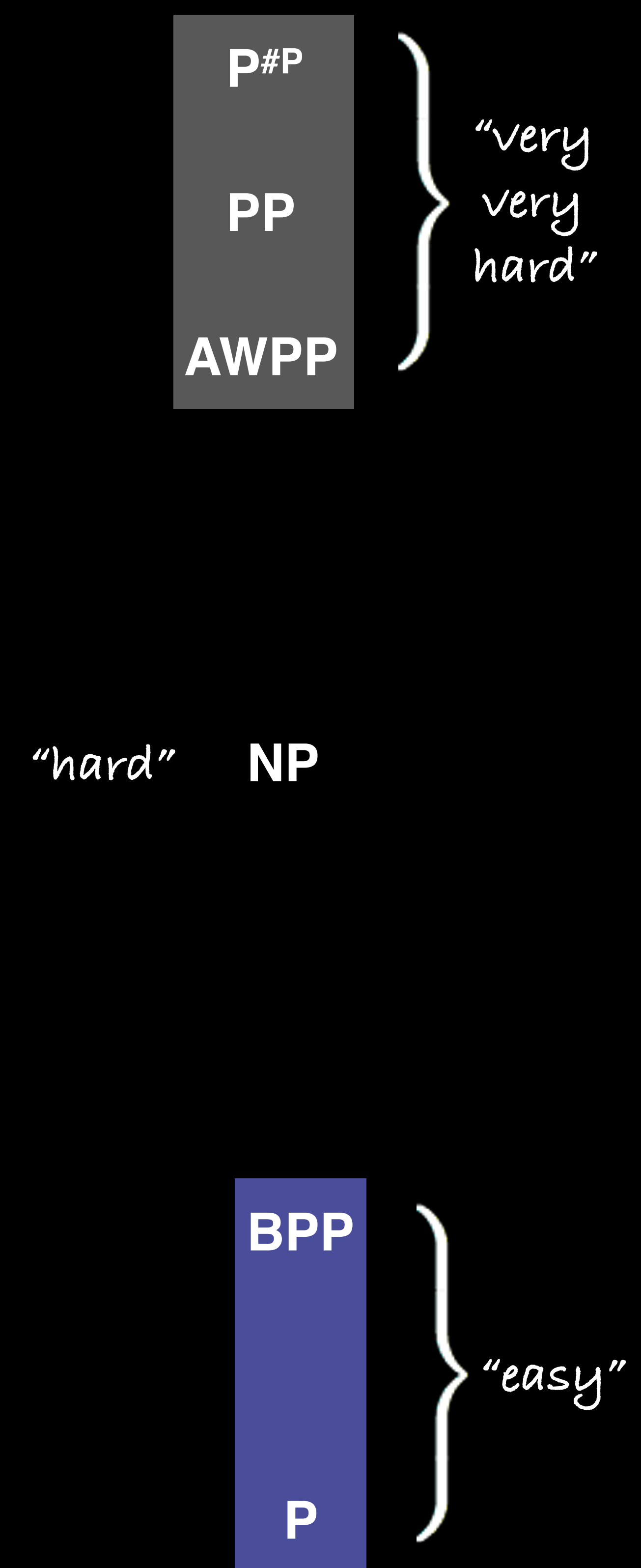
P

"easy"

Counting complexity

BPP: bounded error probabilistic poly-time

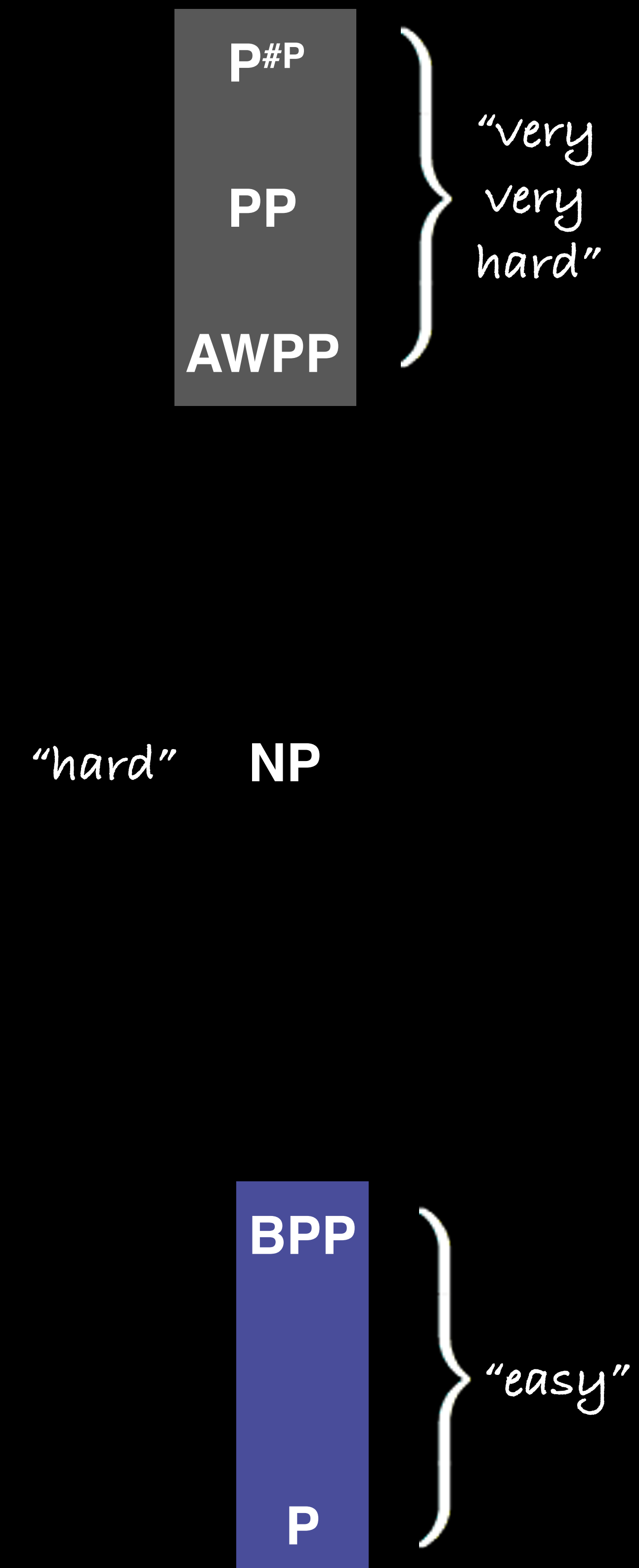
— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error



Counting complexity

BPP: **bounded error probabilistic poly-time**

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error



ZPP: **zero-error probabilistic poly-time**

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability

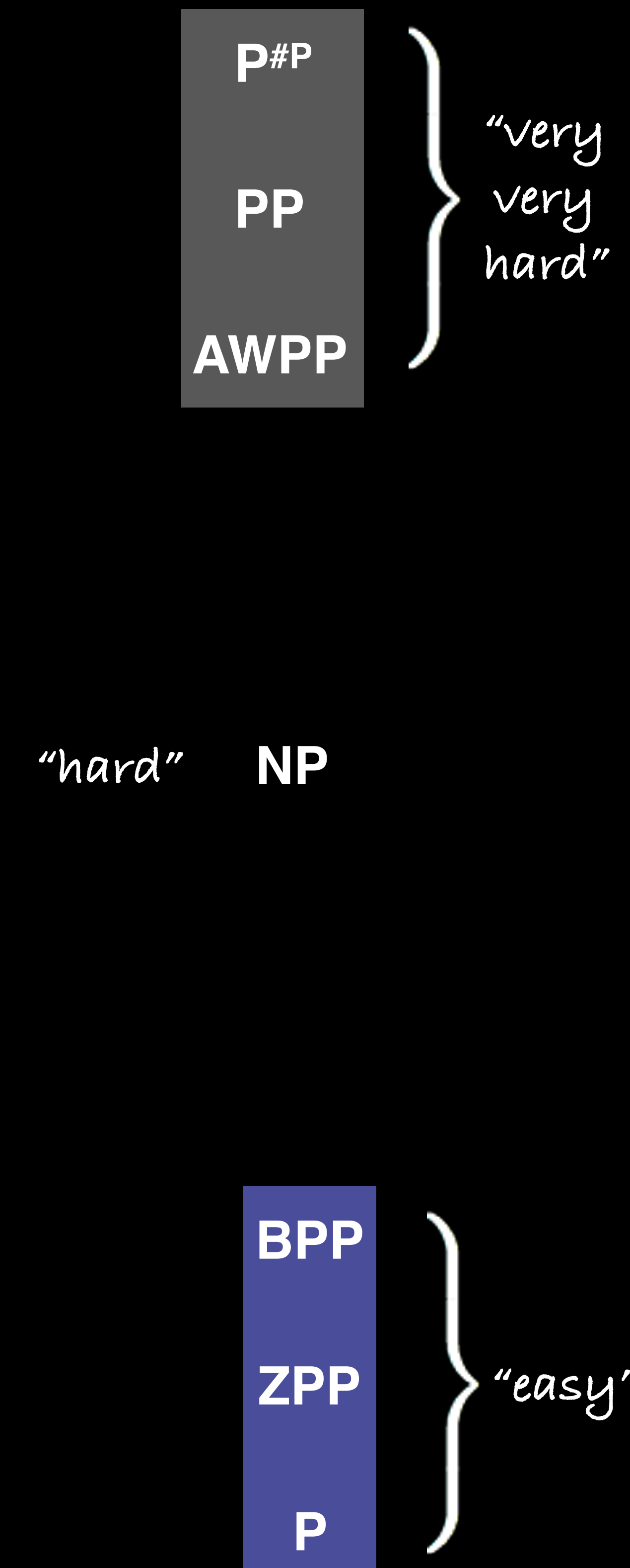
Counting complexity

BPP: bounded error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error

ZPP: zero-error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability



Counting complexity

BPP: bounded error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error

$P^{\#P}$

PP

AWPP

"very very hard"

"hard" **NP**

ZPP: zero-error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability

BPP

ZPP

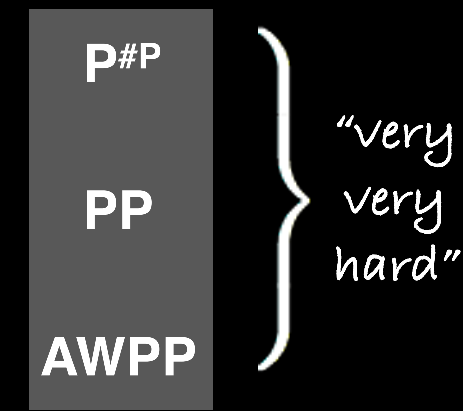
P

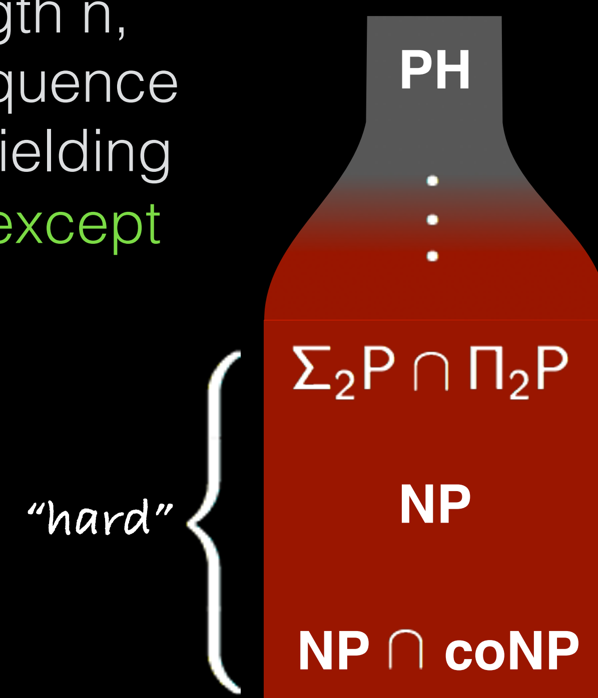
"easy"

Counting complexity

BPP: bounded error probabilistic poly-time

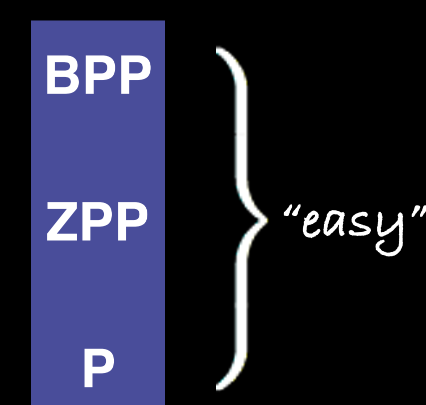
— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error





ZPP: zero-error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability



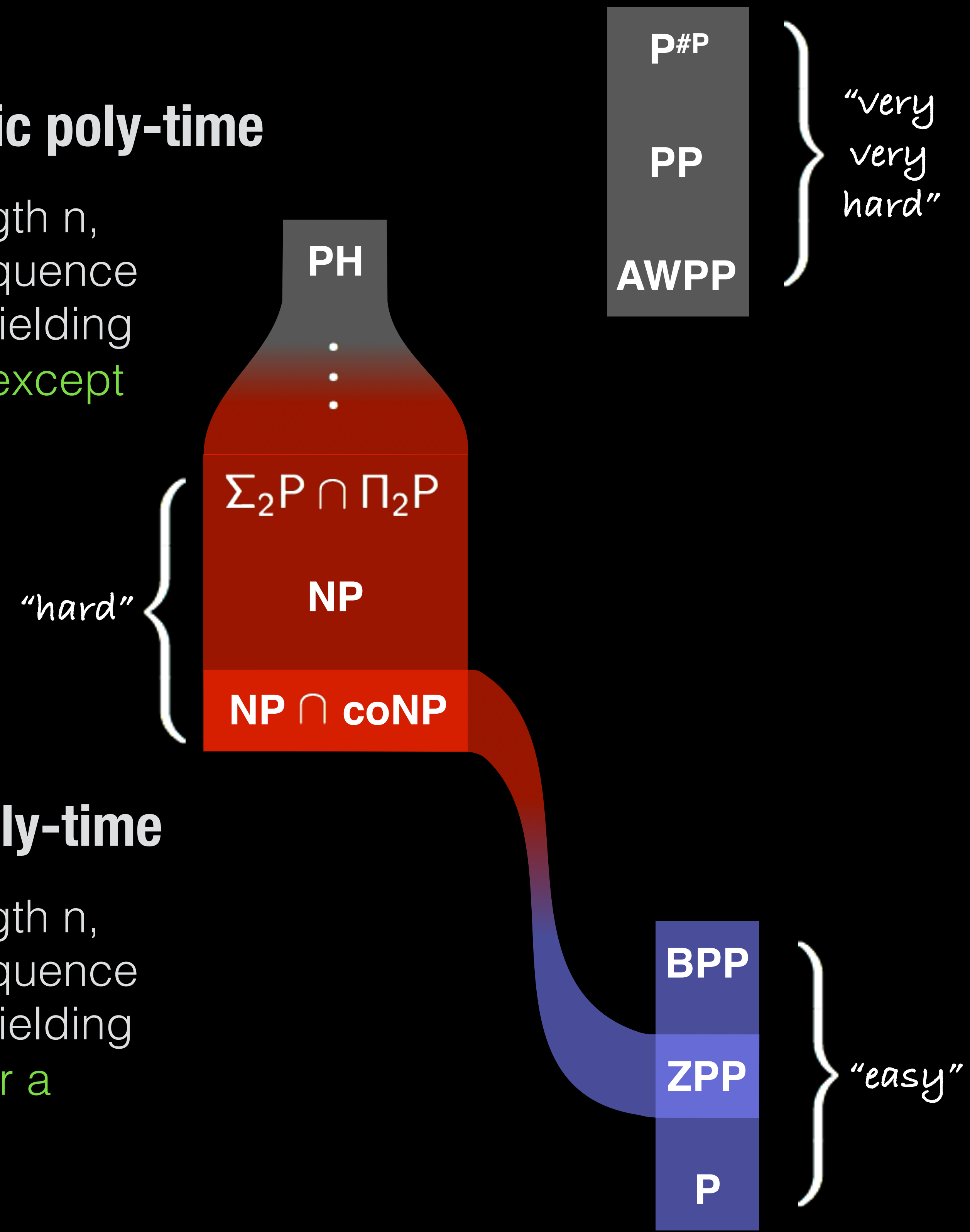
Counting complexity

BPP: bounded error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error

ZPP: zero-error probabilistic poly-time

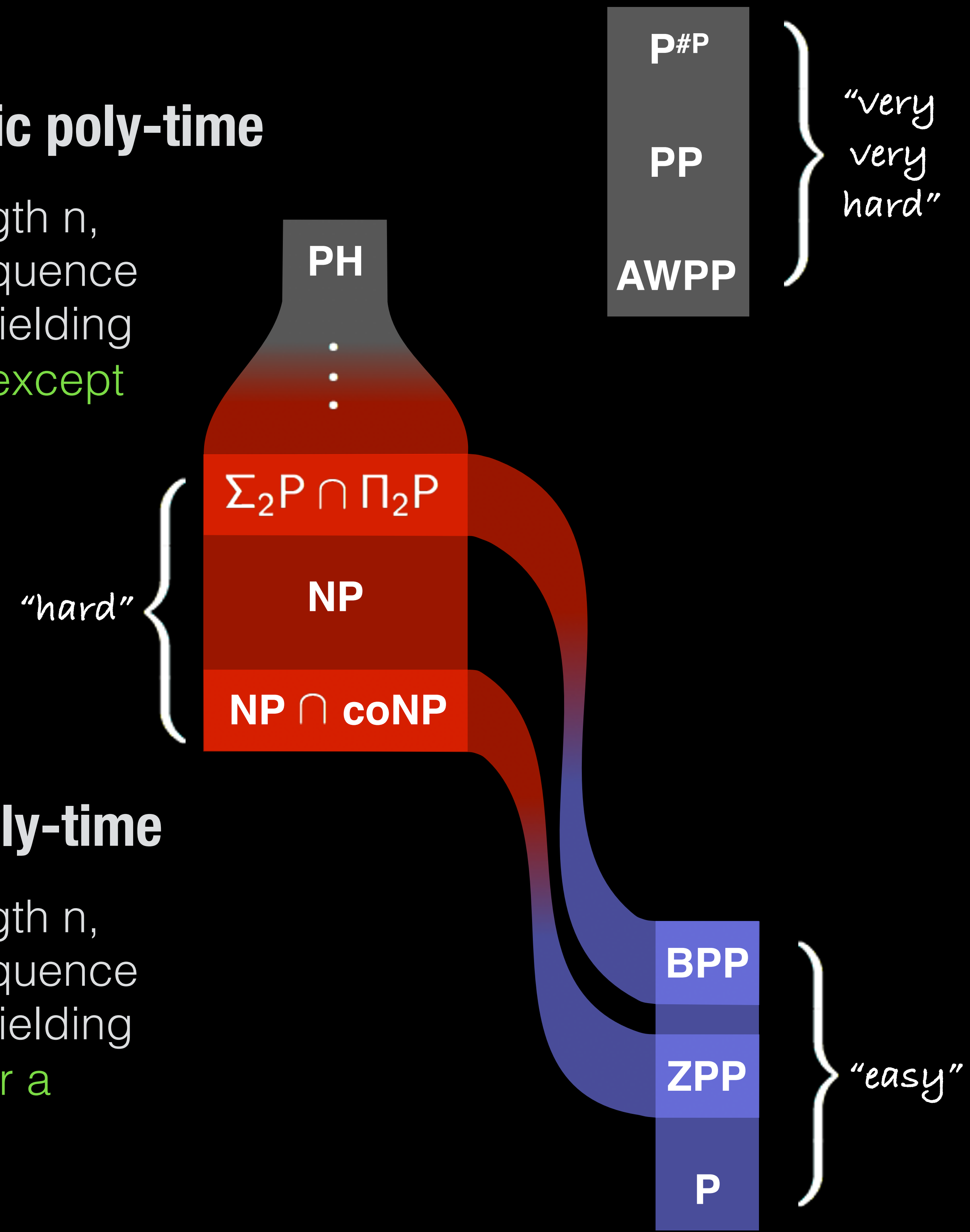
— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability



Counting complexity

BPP: bounded error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error



ZPP: zero-error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability

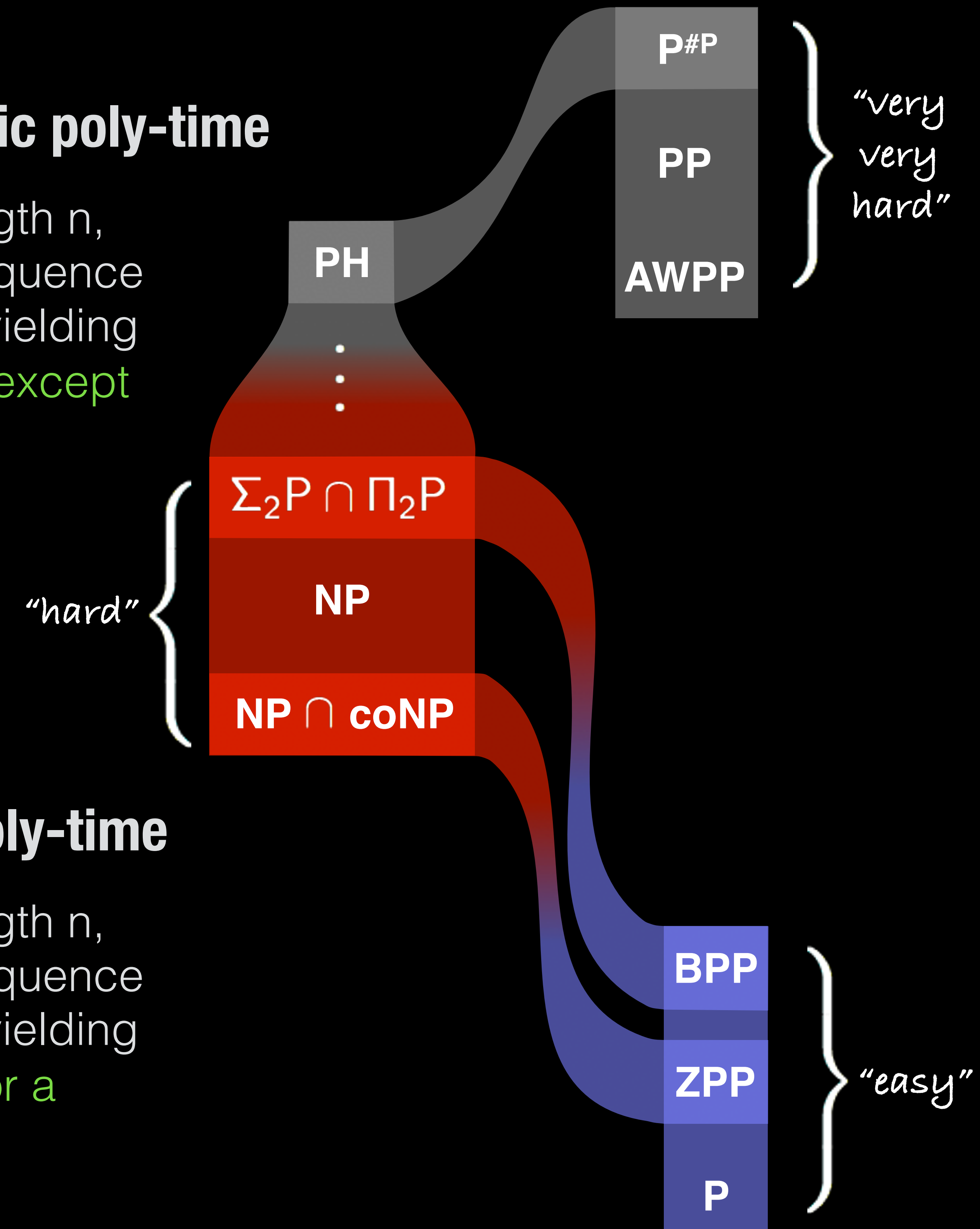
Counting complexity

BPP: bounded error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error

ZPP: zero-error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability



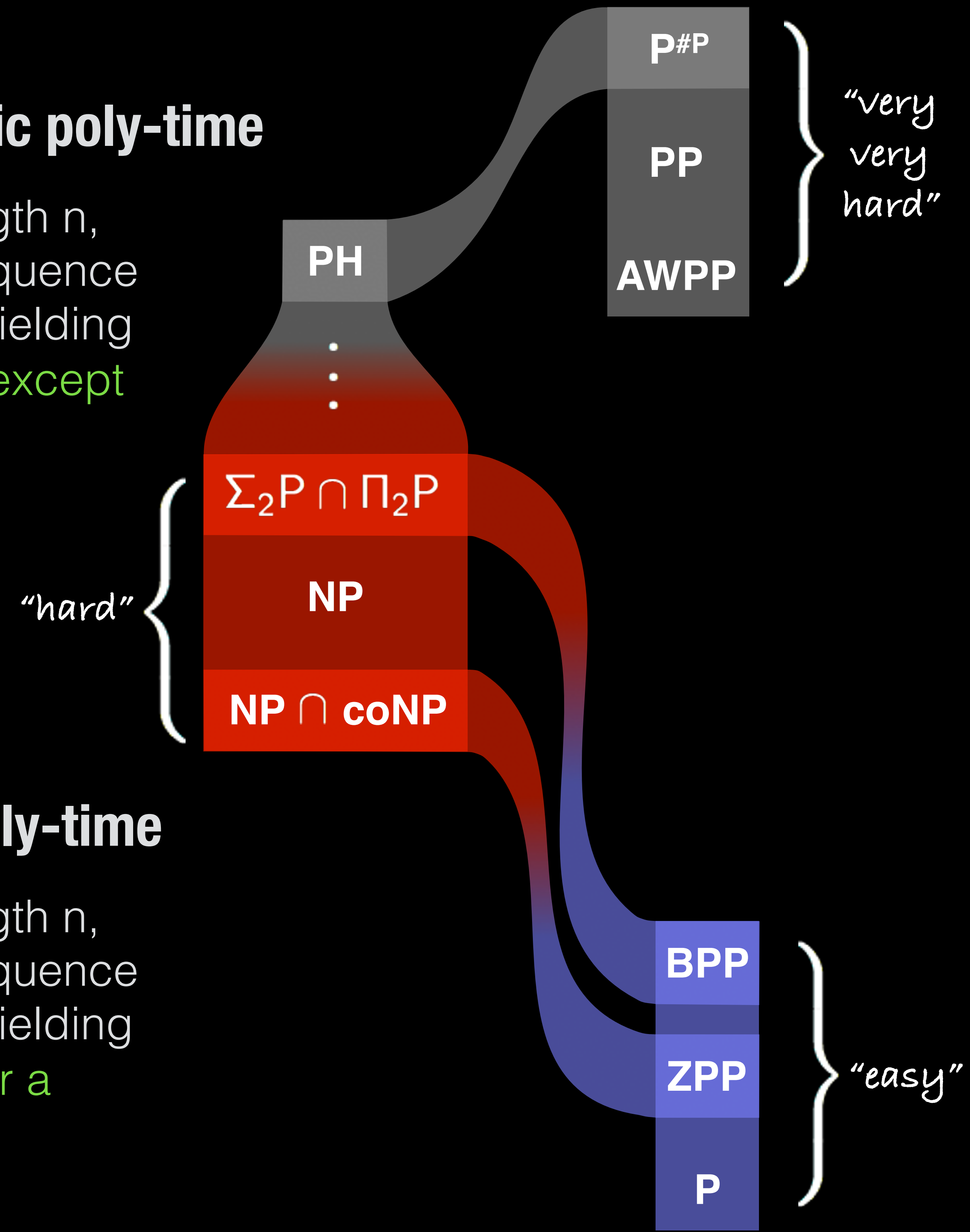
~~Counting~~ complexity

BPP: bounded error probabilistic poly-time

—— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error

ZPP: zero-error probabilistic poly-time

—— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability



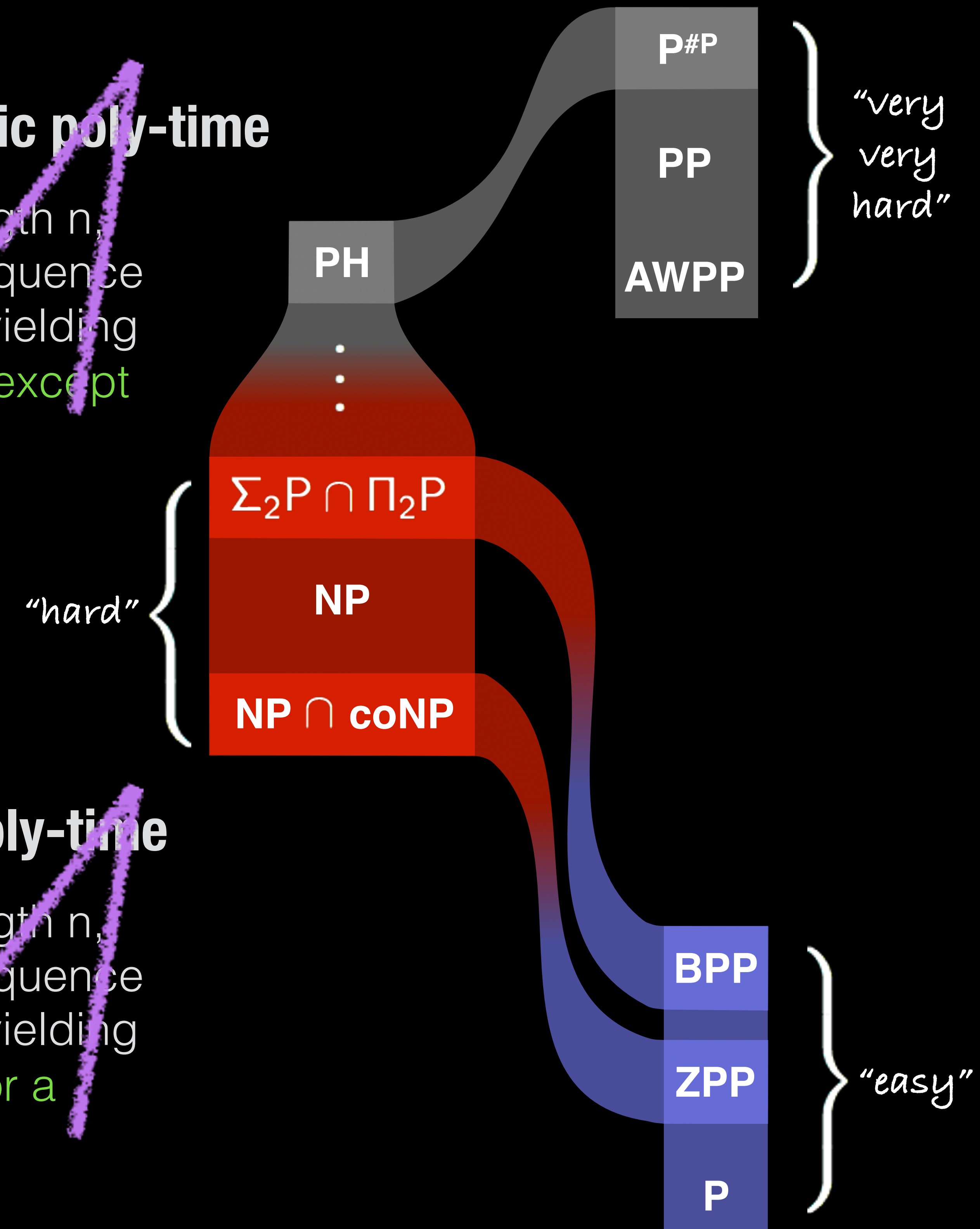
Quantum complexity

BPP: bounded error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a **YES** / **NO** answer which is correct except for bounded error

ZPP: zero-error probabilistic poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of logical operations and bit-flips, yielding a correct **YES** / **NO** answer except for a bounded failure probability



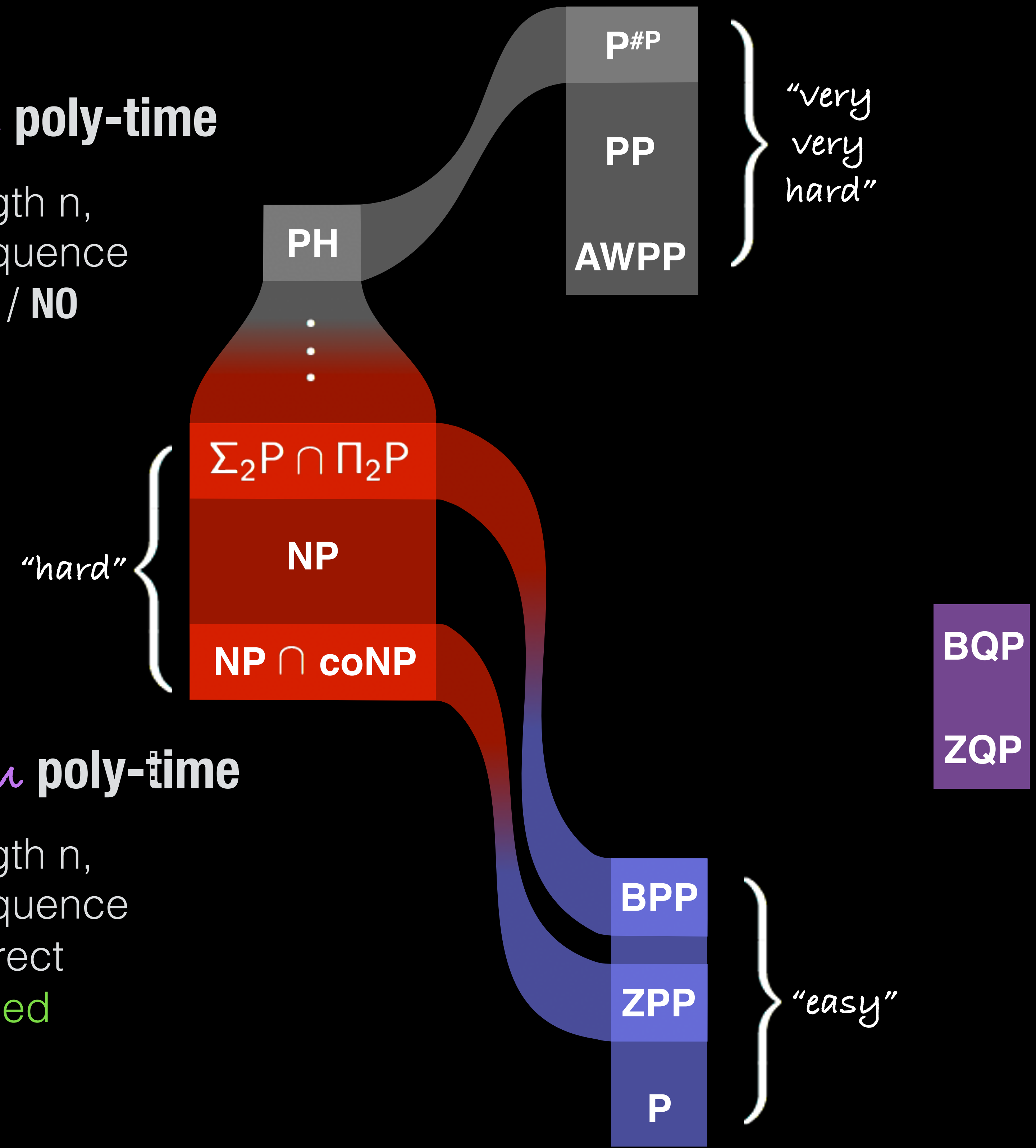
Quantum complexity

BQP: bounded error *quantum* poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a **YES** / **NO** answer which is correct except for bounded error

ZQP: zero-error error *quantum* poly-time

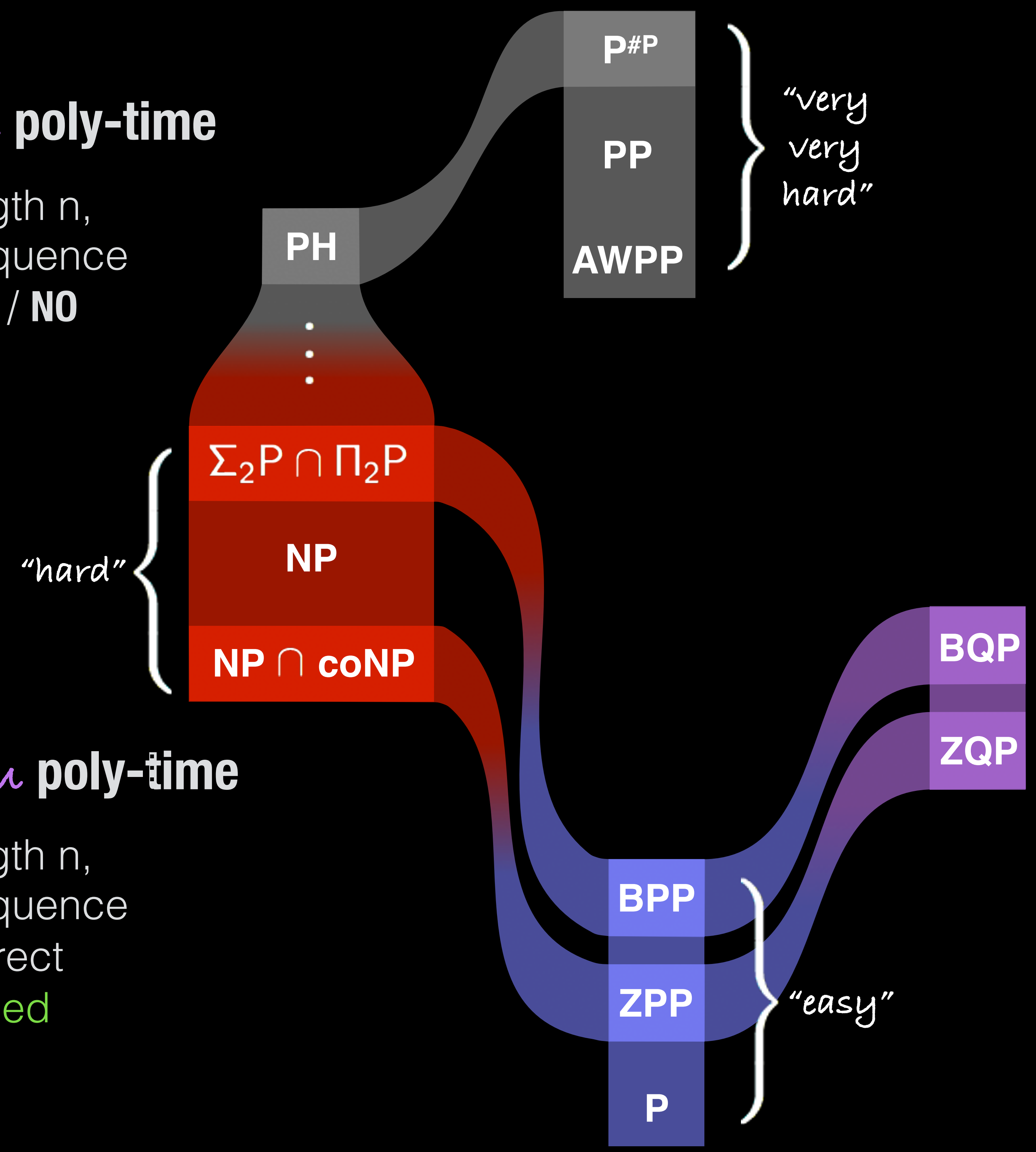
— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a correct **YES** / **NO** answer except for a bounded failure probability



Quantum complexity

BQP: bounded error *quantum* poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a **YES** / **NO** answer which is correct except for bounded error



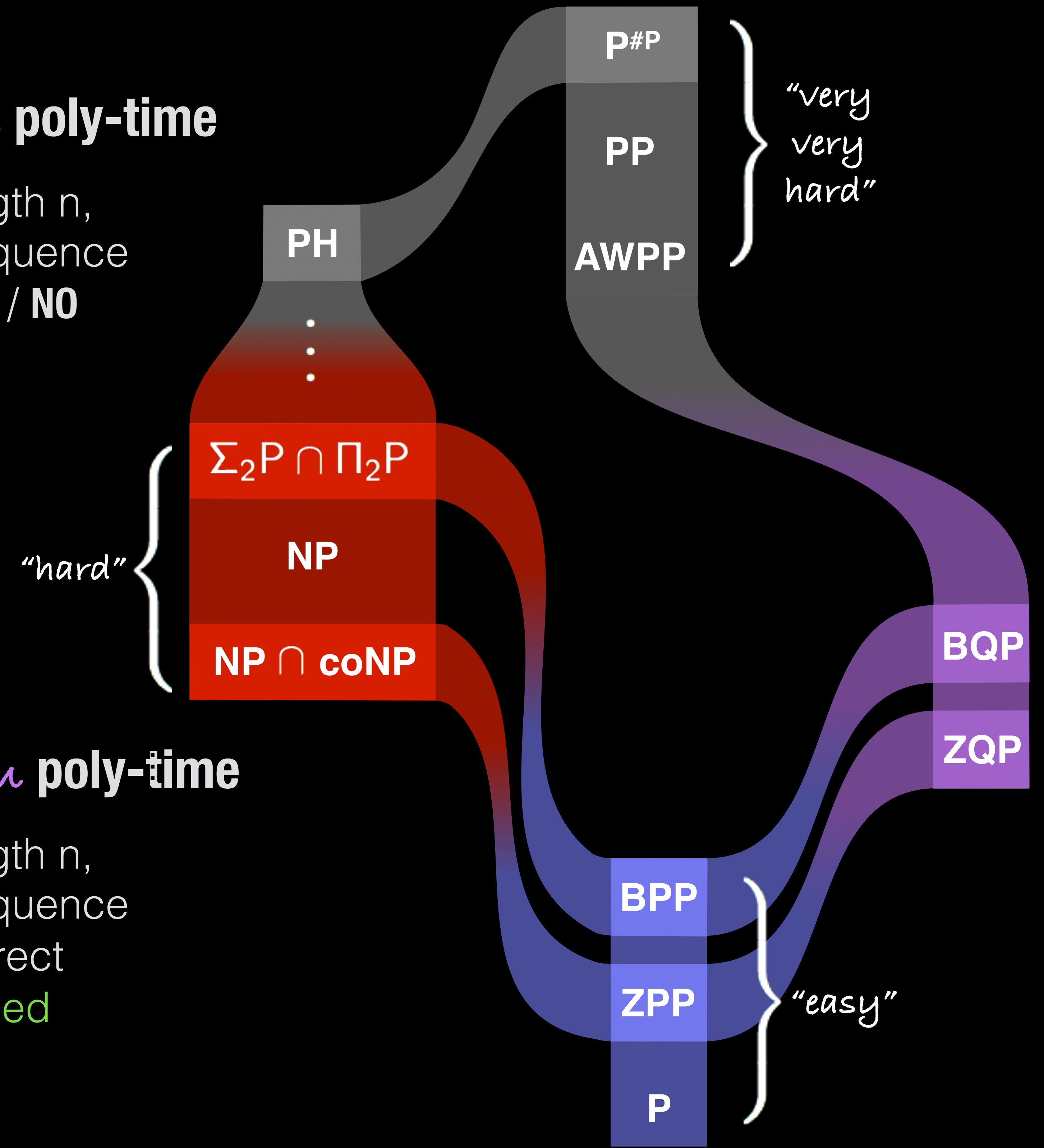
ZQP: zero-error error *quantum* poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a correct **YES** / **NO** answer except for a bounded failure probability

Quantum complexity

BQP: bounded error *quantum* poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a **YES** / **NO** answer which is correct except for bounded error



ZQP: zero-error error *quantum* poly-time

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a correct **YES** / **NO** answer except for a bounded failure probability

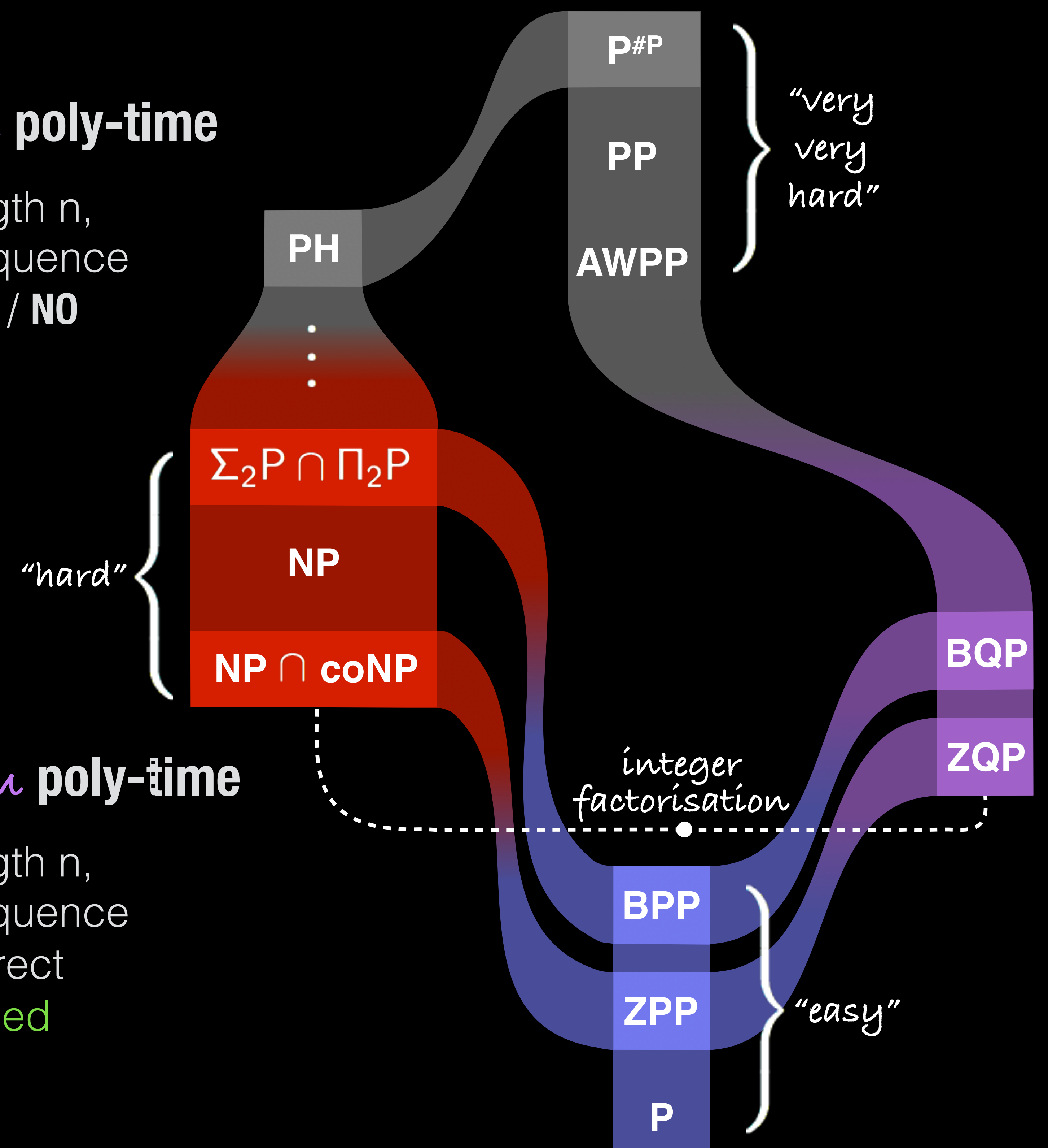
Quantum complexity

BQP: **bounded error** *quantum* **poly-time**

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a **YES** / **NO** answer which is correct except for bounded error

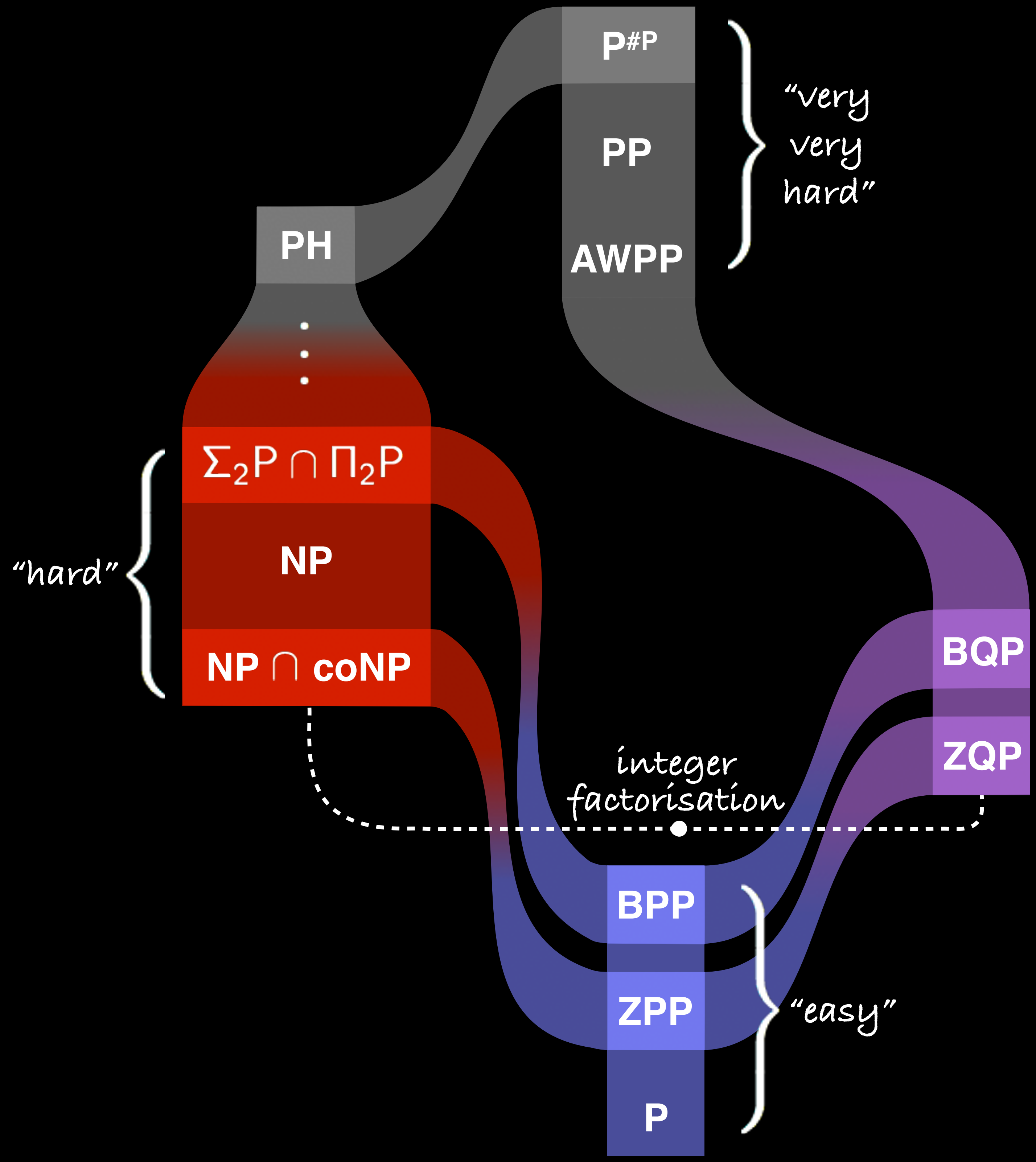
ZQP: **zero-error error** *quantum* **poly-time**

— problems solvable for inputs of length n, using a poly(n)-time specifiable sequence of **unitary** operations, yielding a correct **YES** / **NO** answer except for a bounded failure probability



Quantum complexity

- **Observation:**
  - We know much less than we would like — *e.g.* unlike the "easy" classes, there is no known relationship yet between quantum classes and **PH**



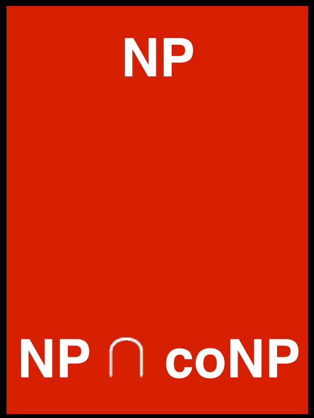
The best bounds on quantum

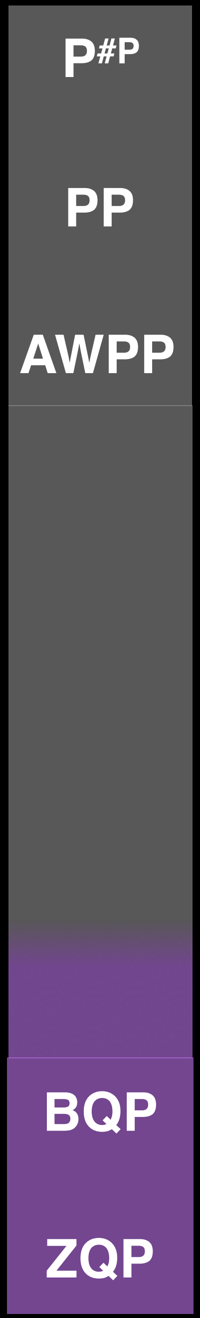
NP — is the total-branch weight zero, or non-zero? ($w_A > 0,\ w_R = 0$)

The best bounds on quantum

NP — is the total-branch weight zero, or non-zero? ($w_A > 0,\ w_R = 0$)

C$_=$P — is the total-branch weight zero, or non-zero? ($w_A = -w_R > 0$)

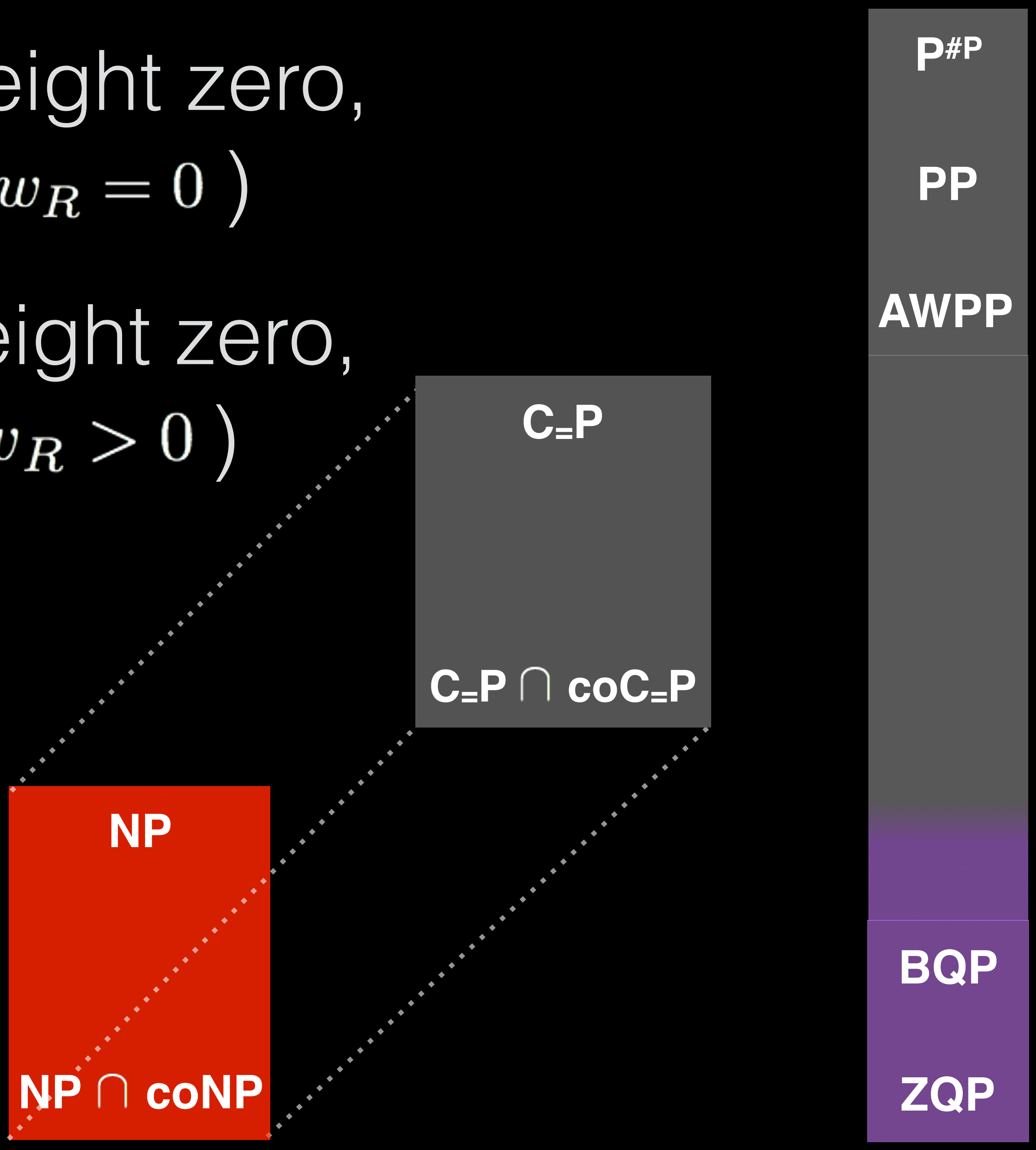




The best bounds on quantum

NP — is the total-branch weight zero, or non-zero? ($w_A > 0,\ w_R = 0$)

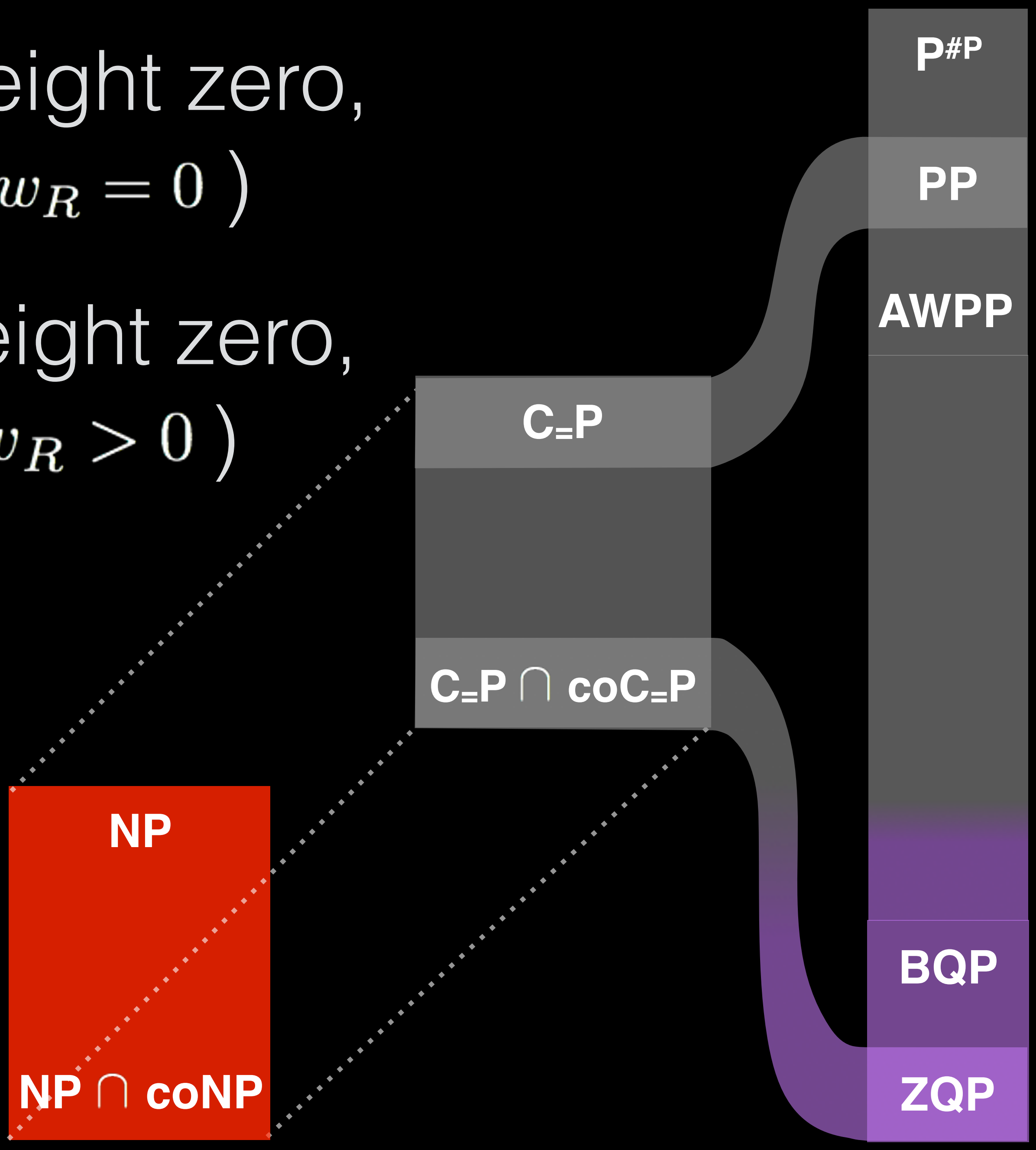
$\mathrm{C}_=\mathrm{P}$ — is the total-branch weight zero, or non-zero? ($w_A = -w_R > 0$)



The best bounds on quantum

NP — is the total-branch weight zero, or non-zero? $(w_A > 0,\ w_R = 0)$

C=P — is the total-branch weight zero, or non-zero? $(w_A = -w_R > 0)$

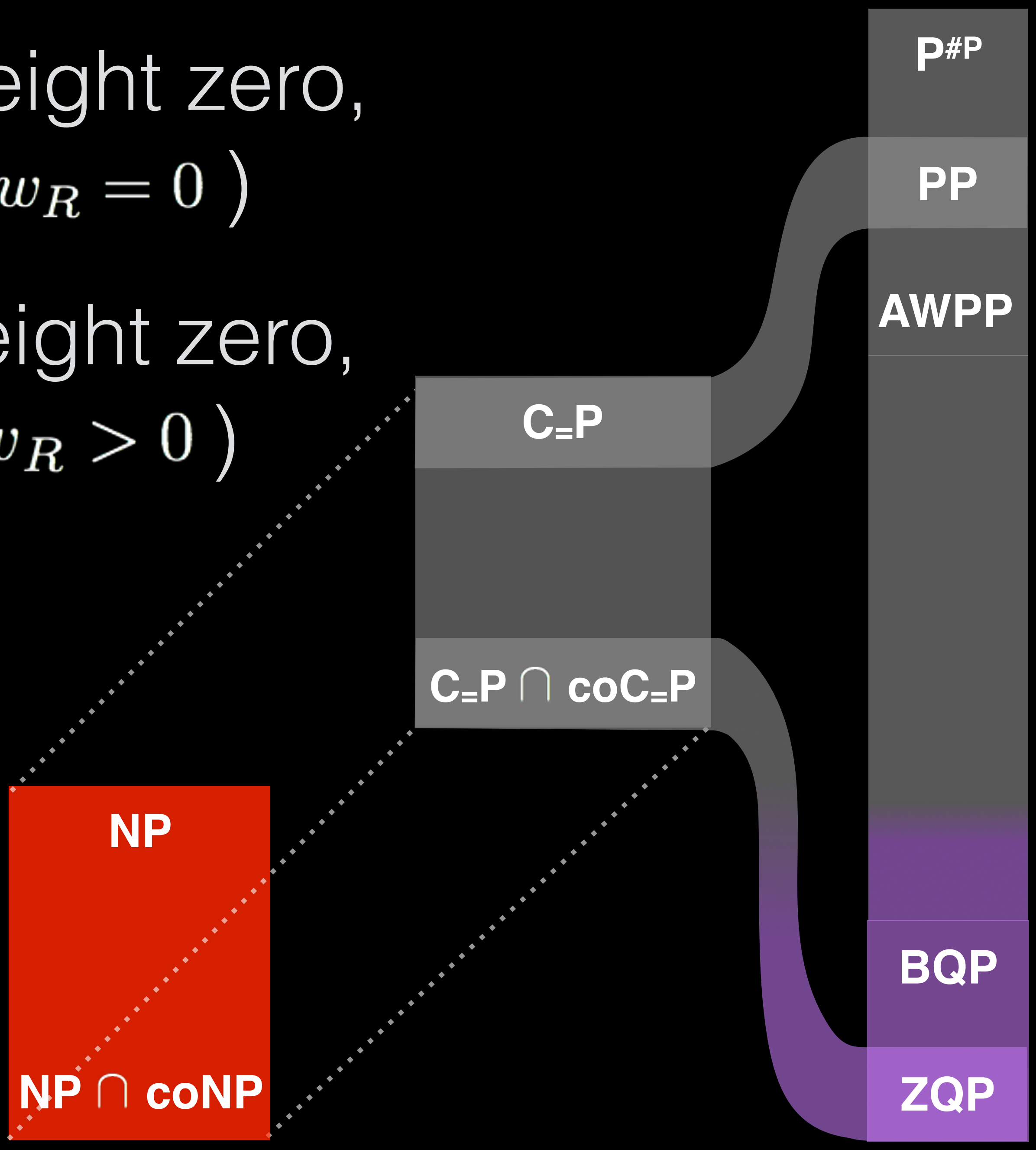


The best bounds on quantum

NP — is the total-branch weight zero, or non-zero? ($w_A > 0,\ w_R = 0$)

C$_=$P — is the total-branch weight zero, or non-zero? ($w_A = -w_R > 0$)

- **Observation:**
  - These bounds on quantum computation are expected to be very loose, and don't take unitarity of evolution into account

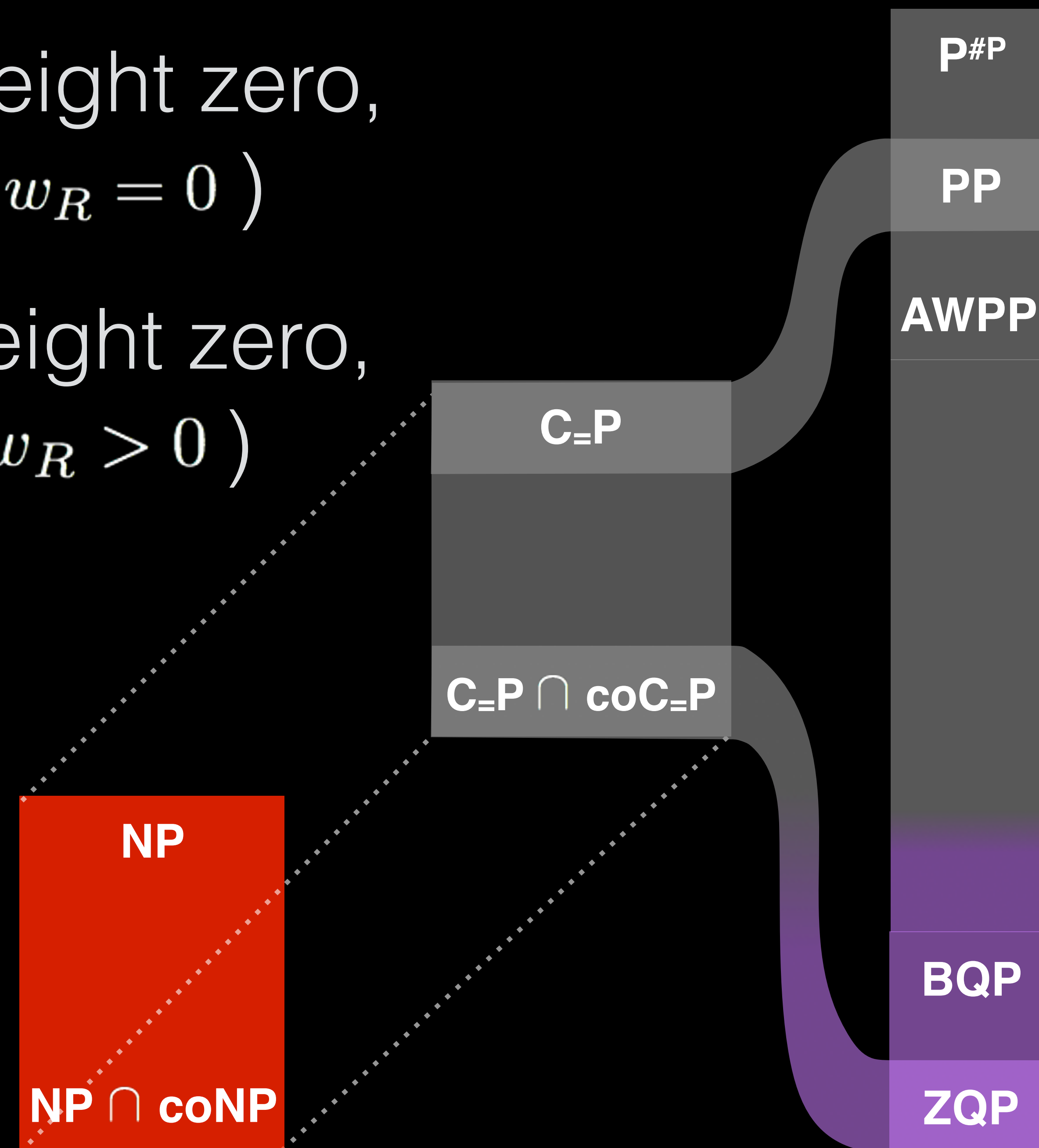


The best bounds on quantum

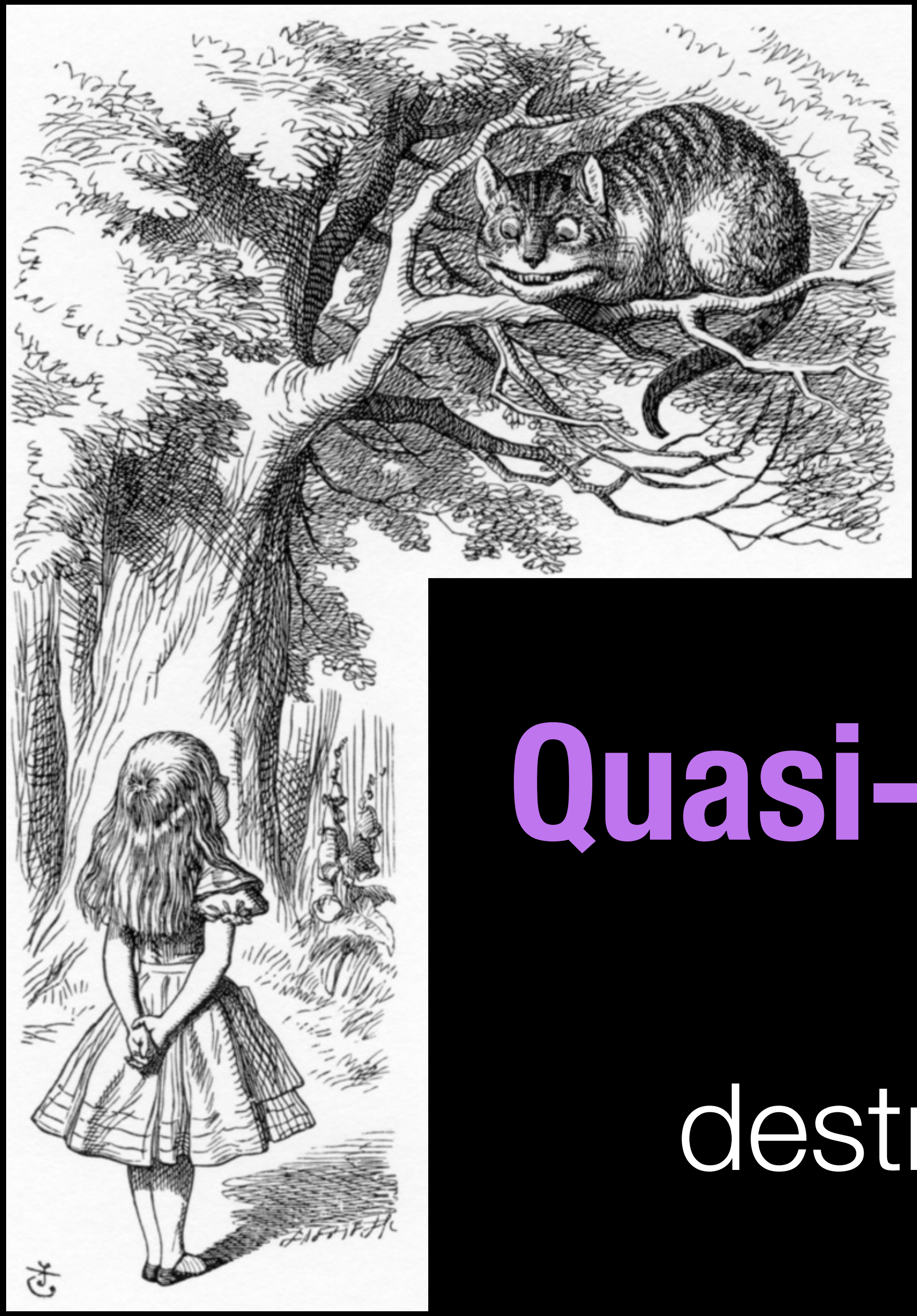
NP — is the total-branch weight zero, or non-zero? $(w_A > 0,\ w_R = 0\ )$

C=P — is the total-branch weight zero, or non-zero? $(w_A = -w_R > 0\ )$

- **Observation:**
  - These bounds on quantum computation are expected to be very loose, and don't take unitarity of evolution into account



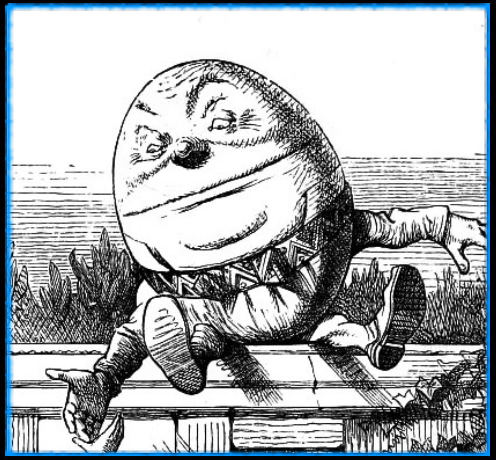
Can we describe the power of interference, without the notion of unitarity?



Quasi-quantum theories

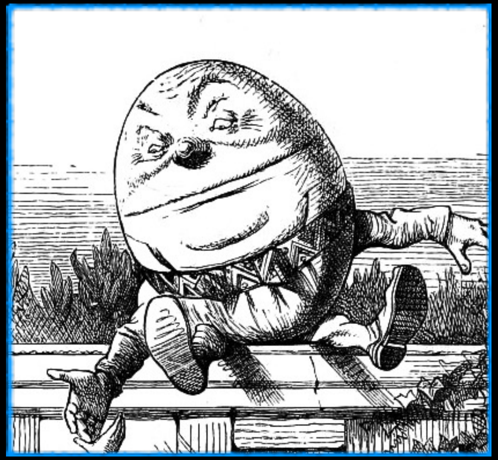
to explore
destructive interference

“Quasi-quantum”?



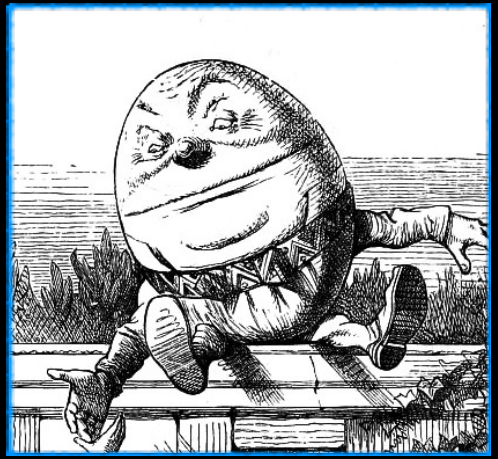
"Quasi-quantum"?

Like quantum computation (from a formal perspective) — but without the annoying adherence to physics



“Quasi-quantum”?

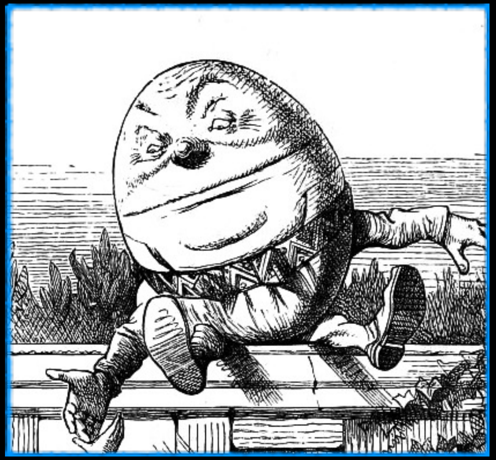
Like quantum computation (from a formal perspective) — but without the annoying adherence to physics



- Key ideas:
  - ❖ Computational states are a subclass of some **distributions** kX over “classical” outcomes X
  - ❖ The states include X itself, and exclude the null distribution **0**

$$\psi = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \end{pmatrix}$$

“Quasi-quantum”?



Like quantum computation (from a formal perspective) — but without the annoying adherence to physics

- Key ideas:
  - Computational states are a subclass of some **distributions** kX over “classical” outcomes X
  - The states include X itself, and exclude the null distribution **0**
  - Transformations act linearly on all distributions, and map each state to some other state
  - Measurement consists of “sampling” labels from the distribution (*only one primitive notion of measurement*)

$$\psi = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \end{pmatrix}$$

How is this different from quantum computation?

… different enough to be able to recover many unrelated ideas in counting complexity

How is this different from quantum computation?

… different enough to be able to recover many unrelated ideas in counting complexity

- Randomised computation:
  - Convex combinations of states $x \in X$, in the space $\mathbb{R}X$

How is this different from quantum computation?

… different enough to be able to recover many unrelated ideas in counting complexity

- Randomised computation:
  - Convex combinations of states $x \in X$, in the space $\mathbb{R}X$
- Nondeterministic computation:
  - Non-trivial distributions in $\mathbb{B}X$, where $\mathbb{B}X = \{\bot, \top\}$

How is this different from quantum computation?

… different enough to be able to recover many unrelated ideas in counting complexity

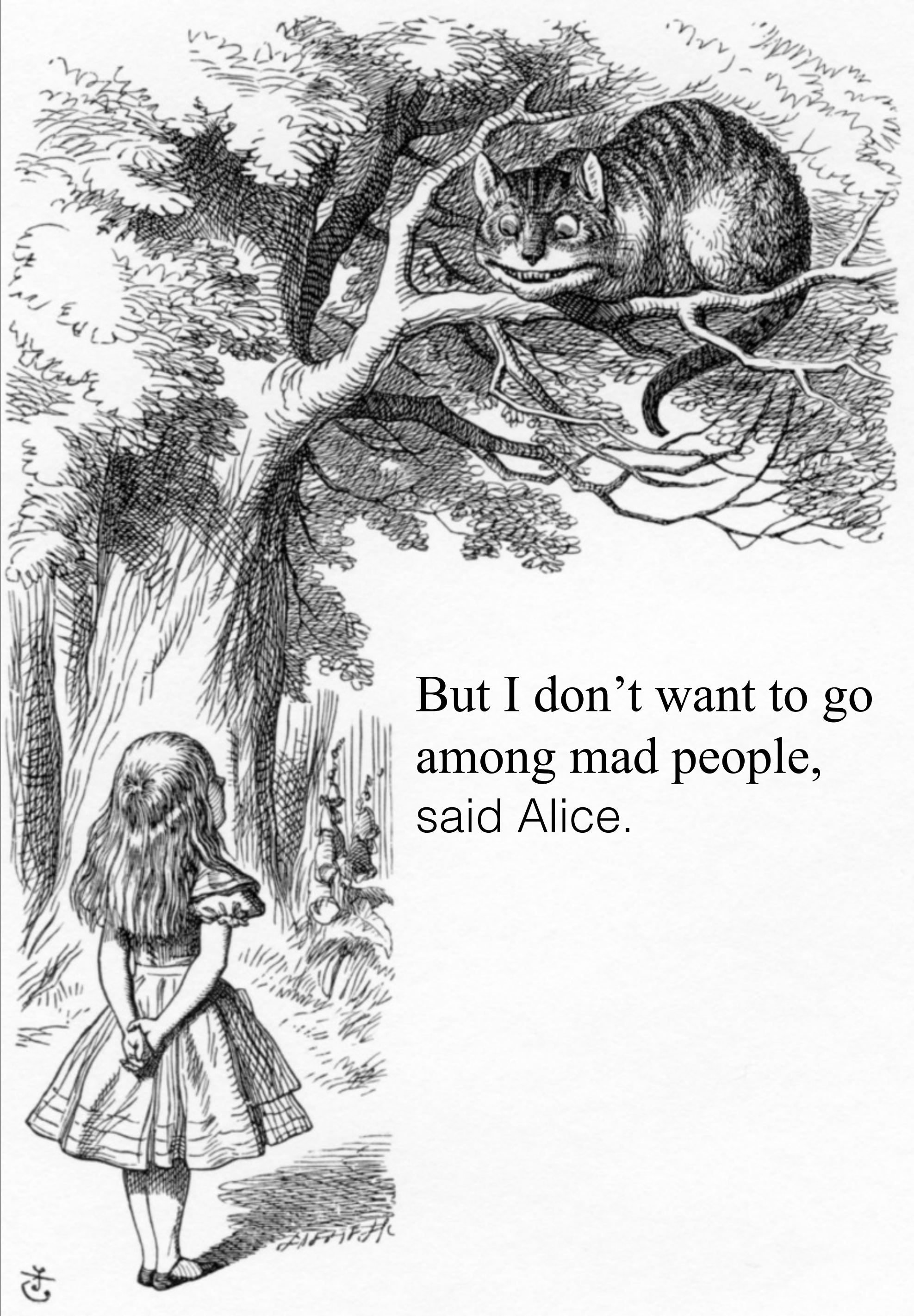
- Randomised computation:
  - Convex combinations of states $x \in X$, in the space $\mathbb{R}X$
- Nondeterministic computation:
  - Non-trivial distributions in $\mathbb{B}X$, where $\mathbb{B}X = \{\bot, \top\}$
- Stranger models of computation:
  - Distributions $\psi \in \mathbb{Z}_2 X$ satisfying $\psi^{\mathsf{T}} \psi = 1$

    — ***i.e.*** amplitudes are **integers mod 2** (not complex numbers)

What are such models ***for***?

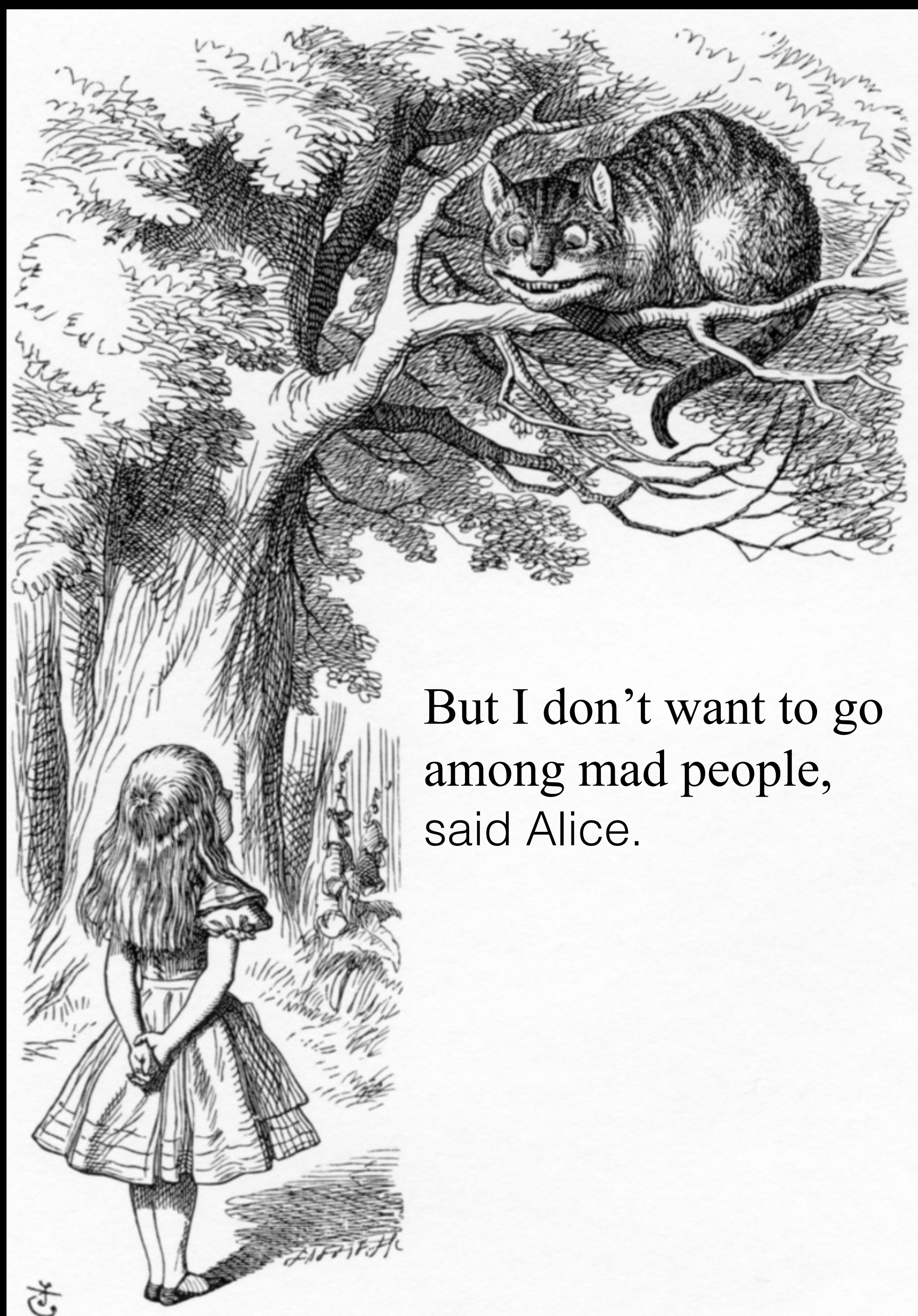
This framework allows for "fundamentally strange" models

What are such models ***for***?



This framework allows for "fundamentally strange" models

What are such models *for*?

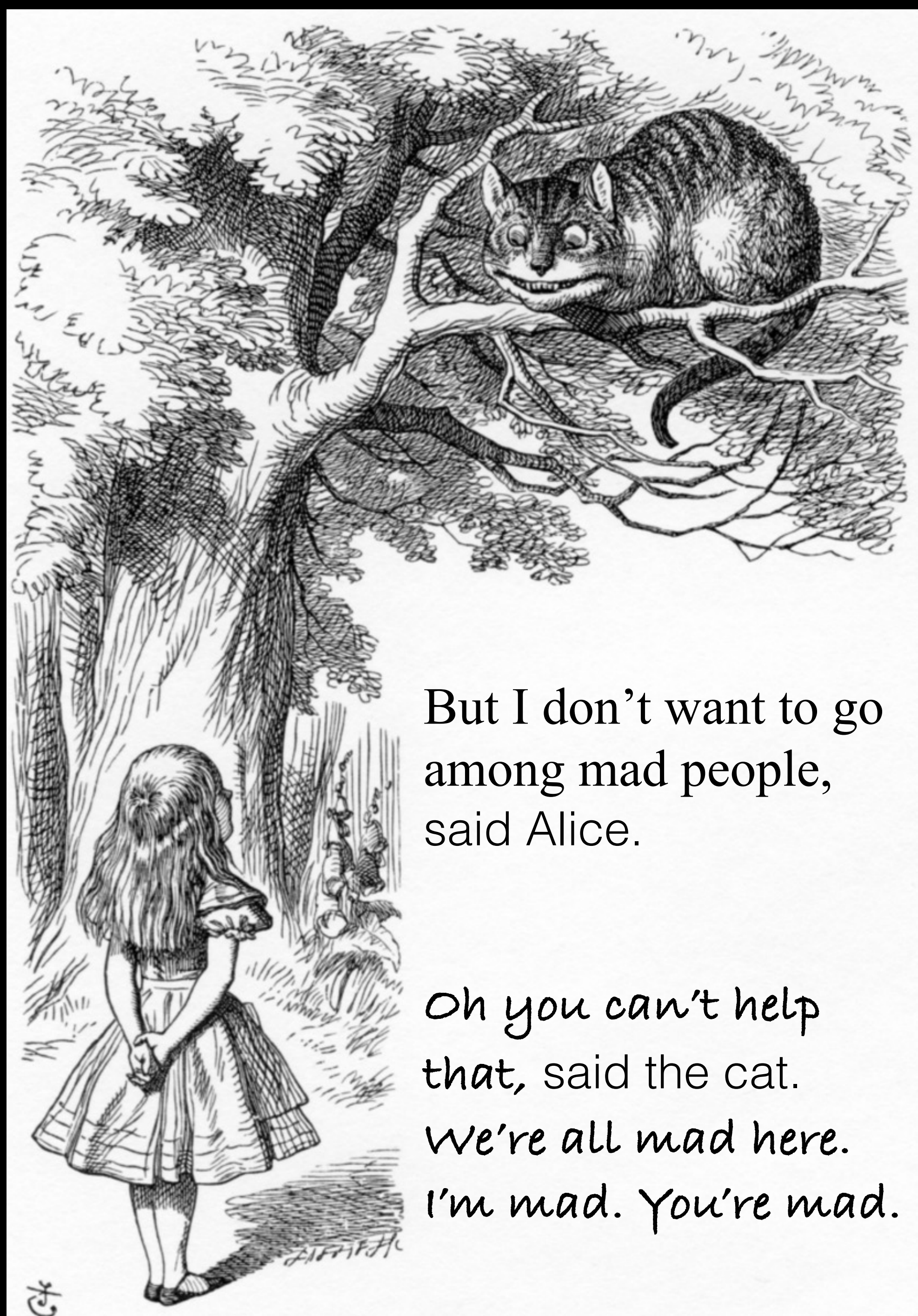


This framework allows for "fundamentally strange" models

But: our aim is

- to study computation in terms of linear transformations of distributions —*"sums" over computational paths*
- to do so in a way which includes but is not limited to quantum computation

What are such models ***for***?

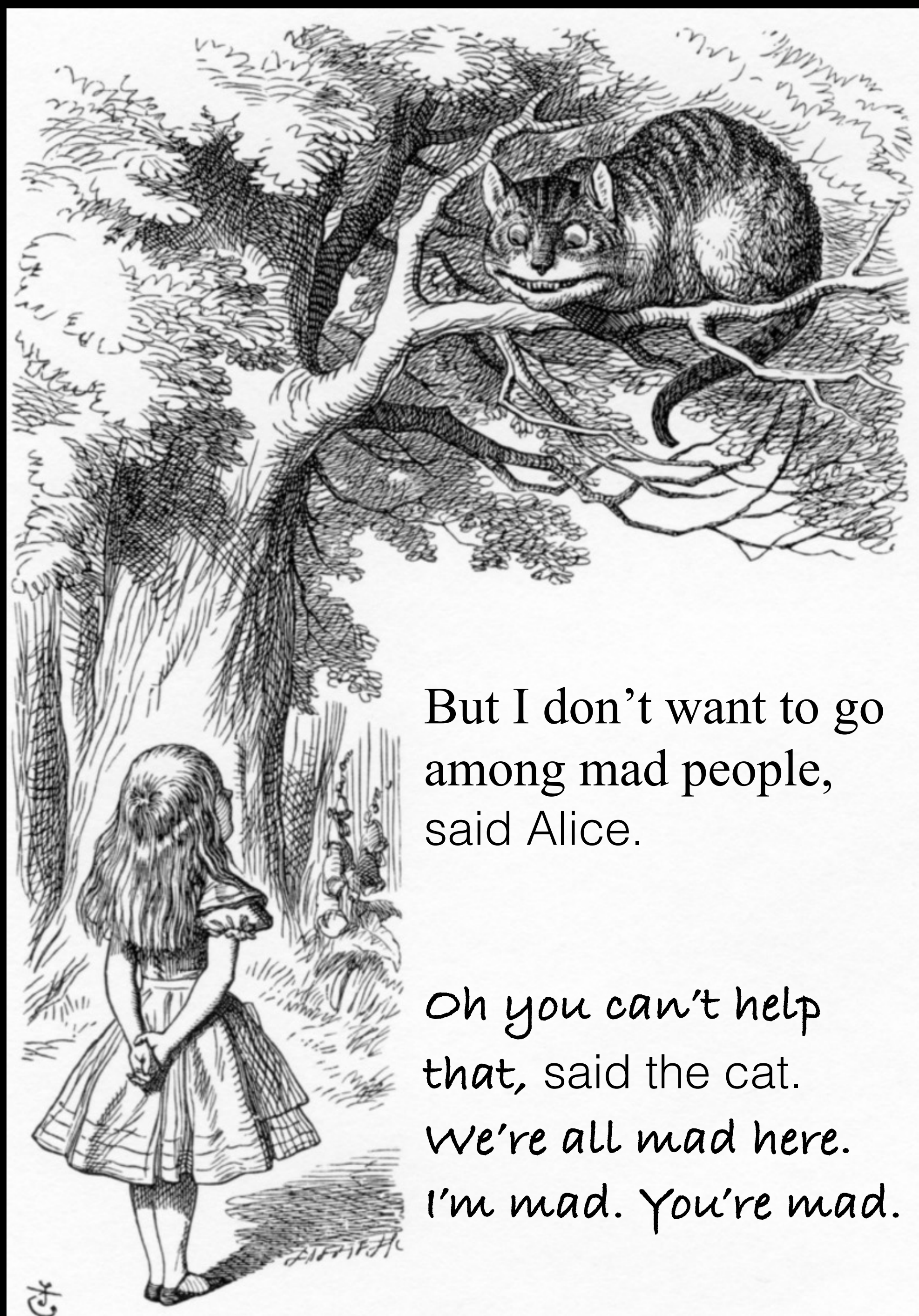


This framework allows for "fundamentally strange" models

But: our aim is

- to study computation in terms of linear transformations of distributions —*"sums" over computational paths*
- to do so in a way which includes but is not limited to quantum computation

What are such models ***for***?



This framework allows for "fundamentally strange" models

But: our aim is

- to study computation in terms of linear transformations of distributions —*"sums" over computational paths*
- to do so in a way which includes but is not limited to quantum computation

Question: what happens when distributions have amplitudes which could cancel?

Approach

- Look at computations with distributions over **rings**
  (cancellable amplitudes)

Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)

Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)


- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)

Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)


- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)
  - Define a “significance” order on amplitudes, respecting multiplication

Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)

- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)
    - Define a “significance” order on amplitudes, respecting multiplication
    - Require that incorrect results have **less significance** in the output distribution than the correct result

Approach

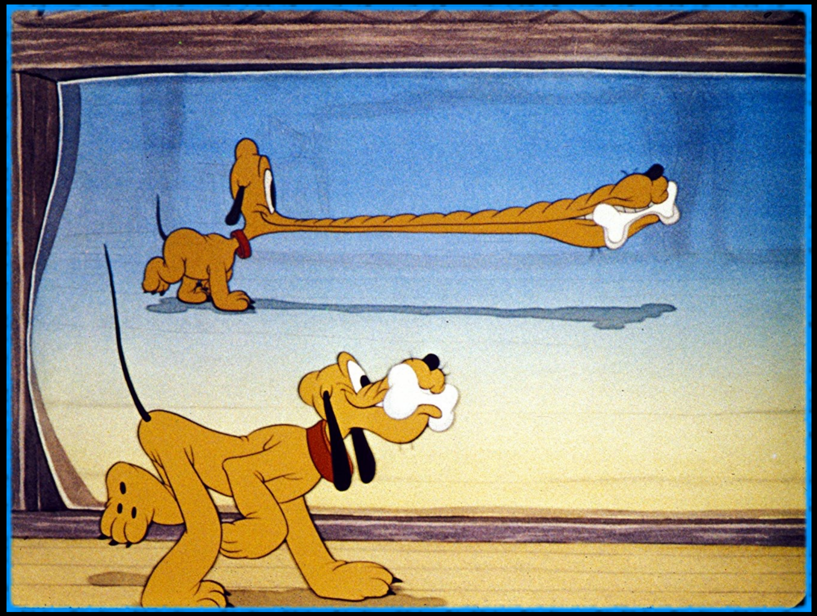
- Look at computations with distributions over **rings** (cancellable amplitudes)


- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)
  - ❖ Define a “significance” order on amplitudes, respecting multiplication
  - ❖ Require that incorrect results have **less significance** in the output distribution than the correct result (similarly, require failure to be less significant in the output distribution than success)

Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)

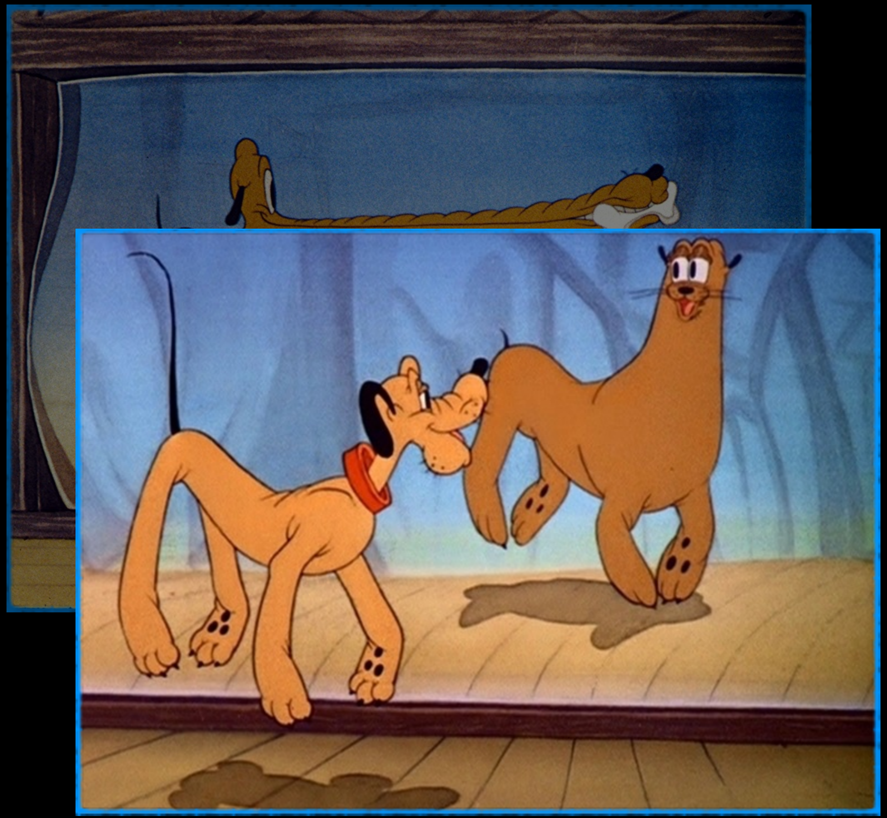
- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)
  - ❖ Define a “significance” order on amplitudes, respecting multiplication
  - ❖ Require that incorrect results have **less significance** in the output distribution than the correct result (similarly, require failure to be less significant in the output distribution than success)



Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)

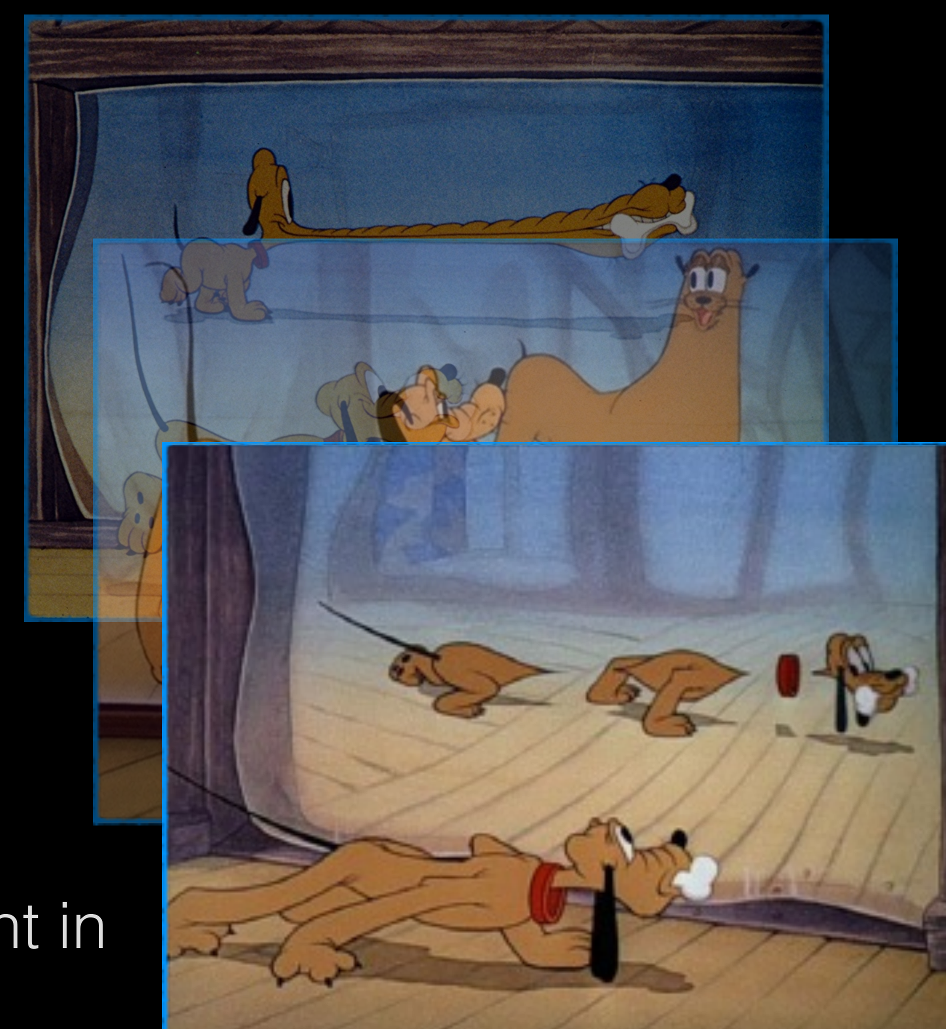
- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)
  - ❖ Define a “significance” order on amplitudes, respecting multiplication
  - ❖ Require that incorrect results have **less significance** in the output distribution than the correct result (similarly, require failure to be less significant in the output distribution than success)



Approach

- Look at computations with distributions over **rings** (cancellable amplitudes)


- Examine **polynomial-time** quasi-quantum computation with bounded error (or failure)
    - Define a “significance” order on amplitudes, respecting multiplication
    - Require that incorrect results have **less significance** in the output distribution than the correct result
      (similarly, require failure to be less significant in the output distribution than success)



Results

a quick peek through
the looking glass

Model #1: ***general linear***
“quantum” computing

Model #1: ***general linear*** “quantum” computing

- **States** —
  any non-zero complex vector $\psi \in \mathbb{C}X$

Model #1: ***general linear*** "quantum" computing

- **States** —
  any non-zero complex vector $\psi \in \mathbb{C}X$
- **Transformations** —
  any invertible operator

Model #1: ***general linear*** "quantum" computing

- **States** —
  any non-zero complex vector $\psi \in \mathbb{C}X$
- **Transformations** —
  any invertible operator

Model #1: ***general linear*** "quantum" computing

- **States** —
  any non-zero complex vector $\psi \in \mathbb{C}X$
- **Transformations** —
  any invertible operator
- **Significance order** —
  magnitude of norm-squared of amplitudes

Model #1: ***general linear*** "quantum" computing

- **States** —
  any non-zero complex vector $\psi \in \mathbb{C}X$
- **Transformations** —
  any invertible operator
- **Significance order** —
  magnitude of norm-squared of amplitudes

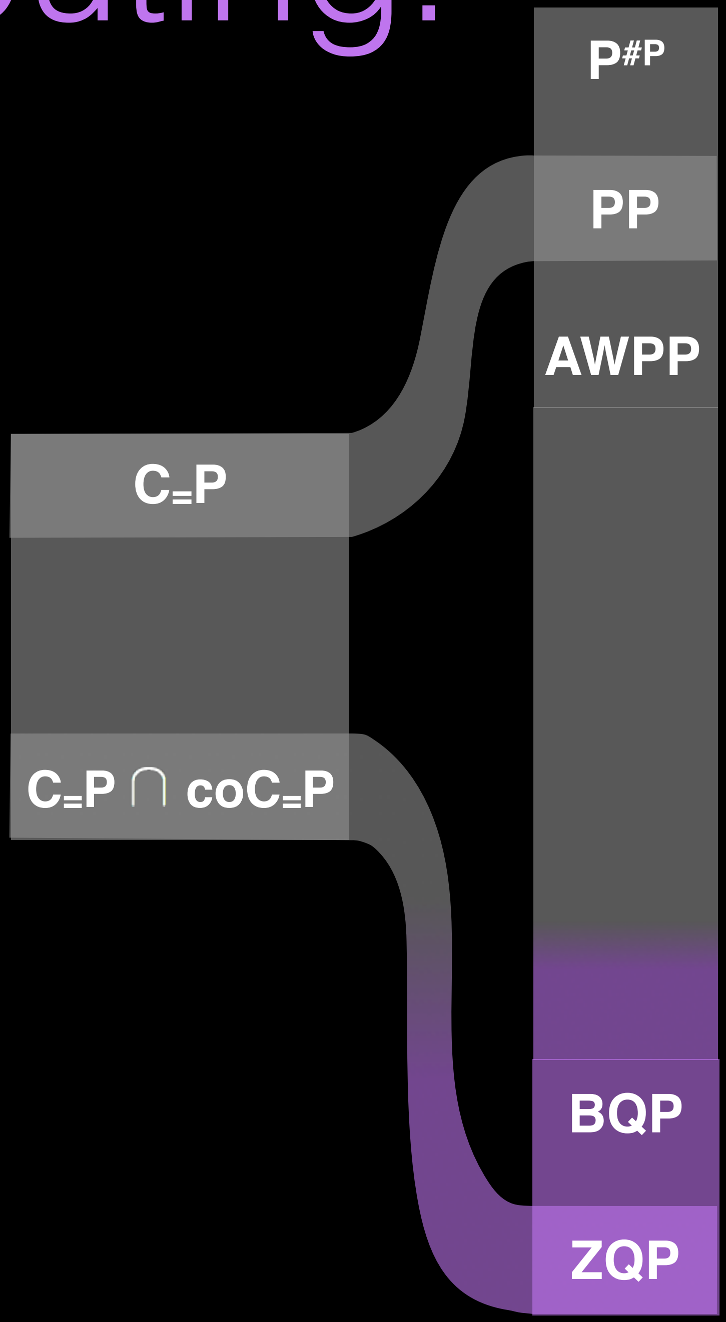
Can reduce "relative significance" of error (or failure), by **amplifying** outcomes of otherwise unitary computations

Model #1: ***general linear*** “quantum” computing

- **States** —
  any non-zero complex vector $\psi \in \mathbb{C}X$
- **Transformations** —
  any invertible operator
- **Significance order** —
  magnitude of norm-squared of amplitudes

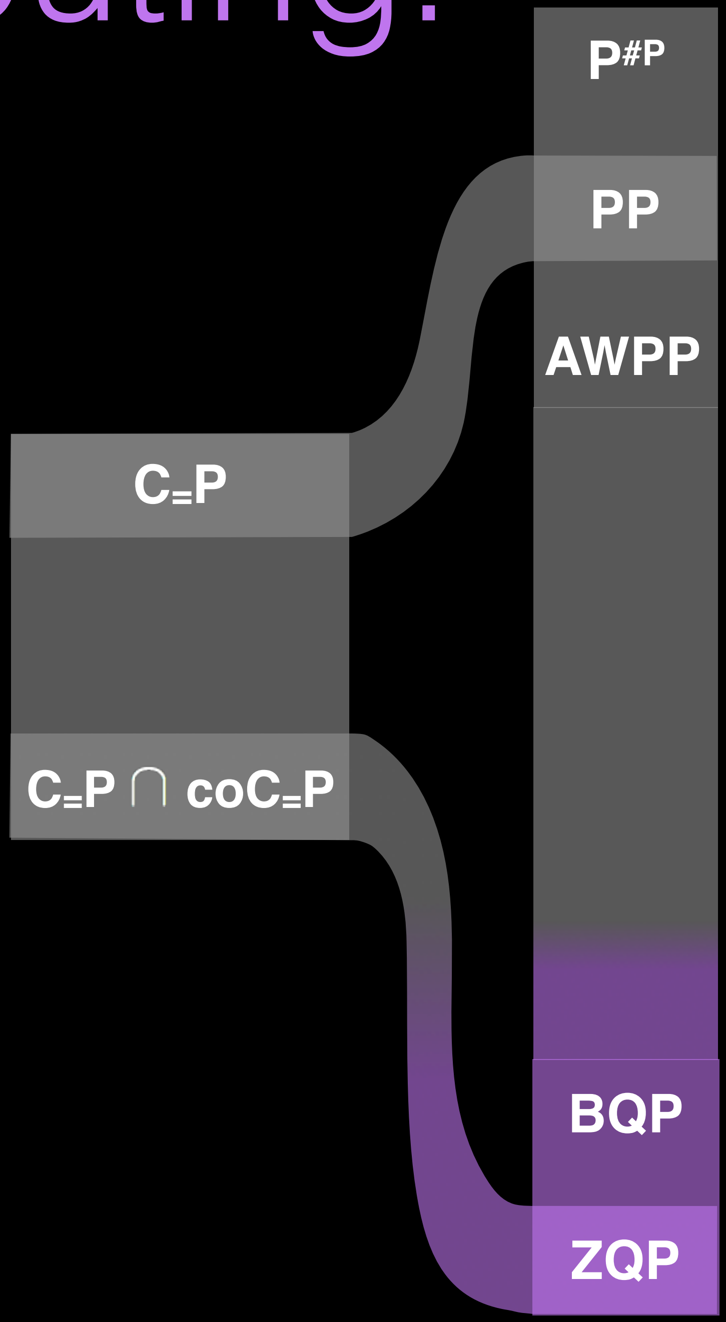
Can reduce “relative significance” of error (or failure), by **amplifying** outcomes of otherwise unitary computations

Complexity of ***general linear*** “quantum” computing:



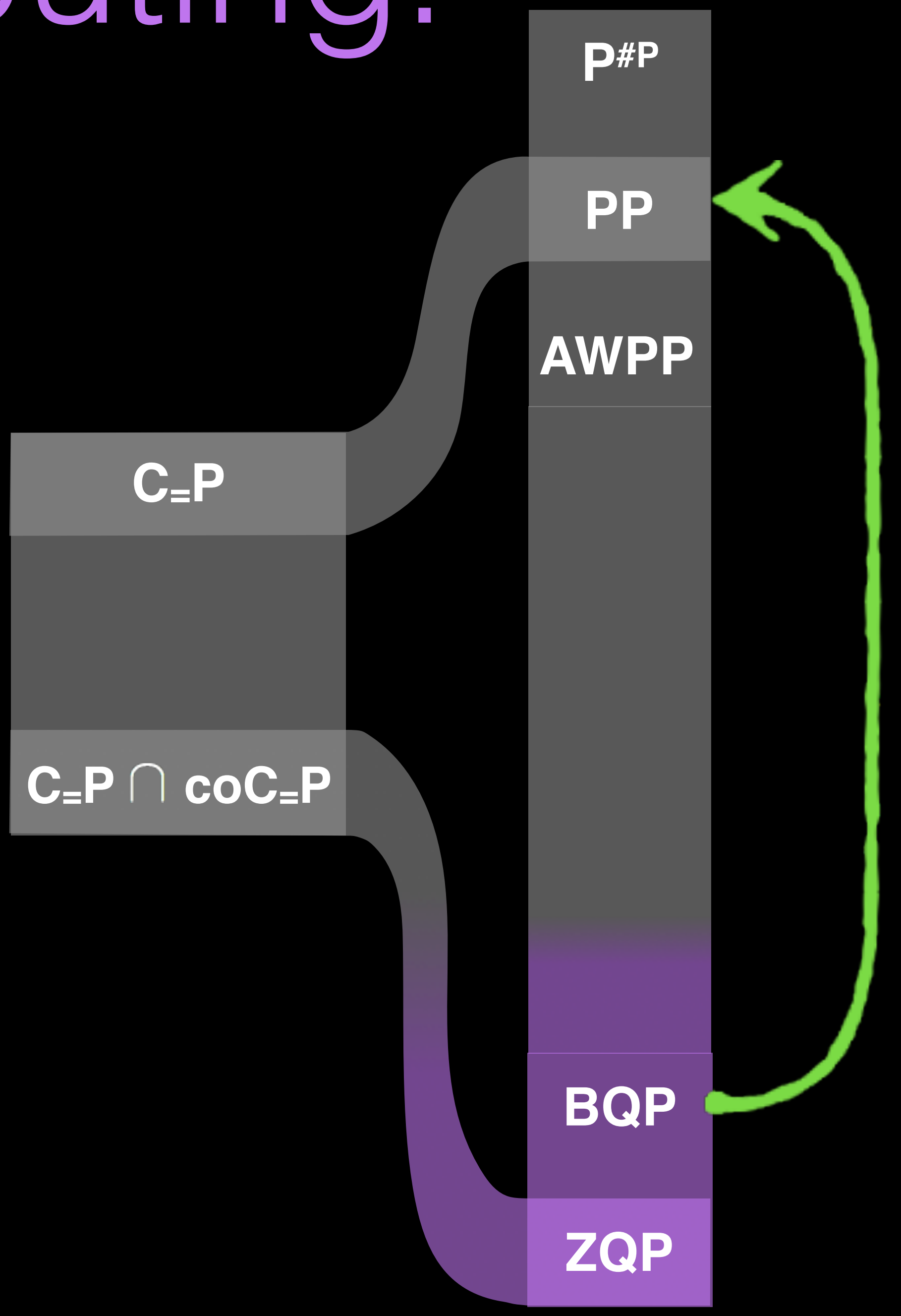
Complexity of ***general linear*** "quantum" computing:

- **Aaronson, 2005** —
  BQP$_{GL}$ = PP
  … a very large increase in (apparent) computational power



Complexity of *general linear* "quantum" computing:

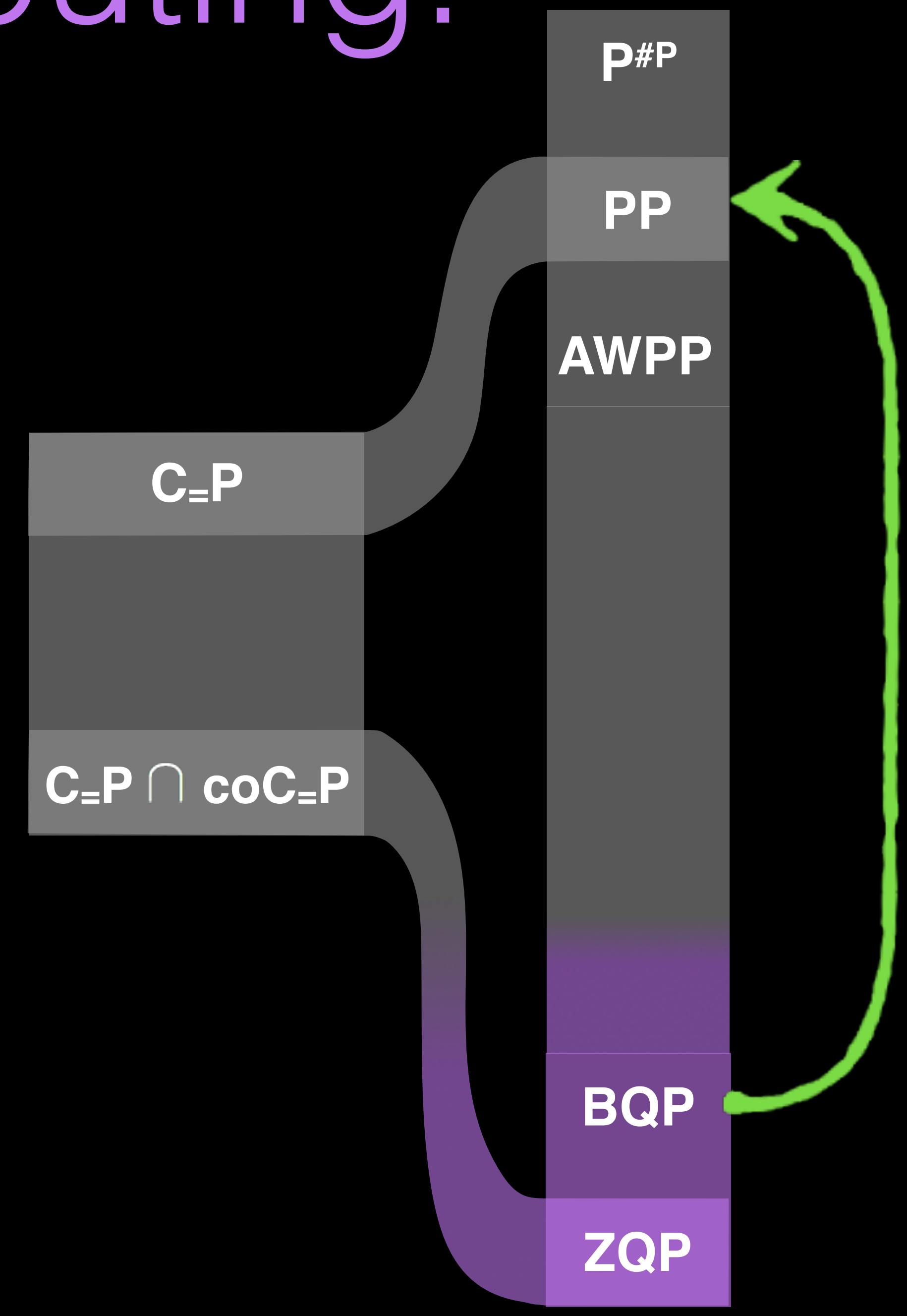
- **Aaronson, 2005** —
  BQP_{GL} = PP
  … a very large increase in (apparent) computational power



Complexity of ***general linear*** "quantum" computing:

- **Aaronson, 2005** —
  $\mathrm{BQP}_{\mathrm{GL}}$ = PP
  … a very large increase in (apparent) computational power

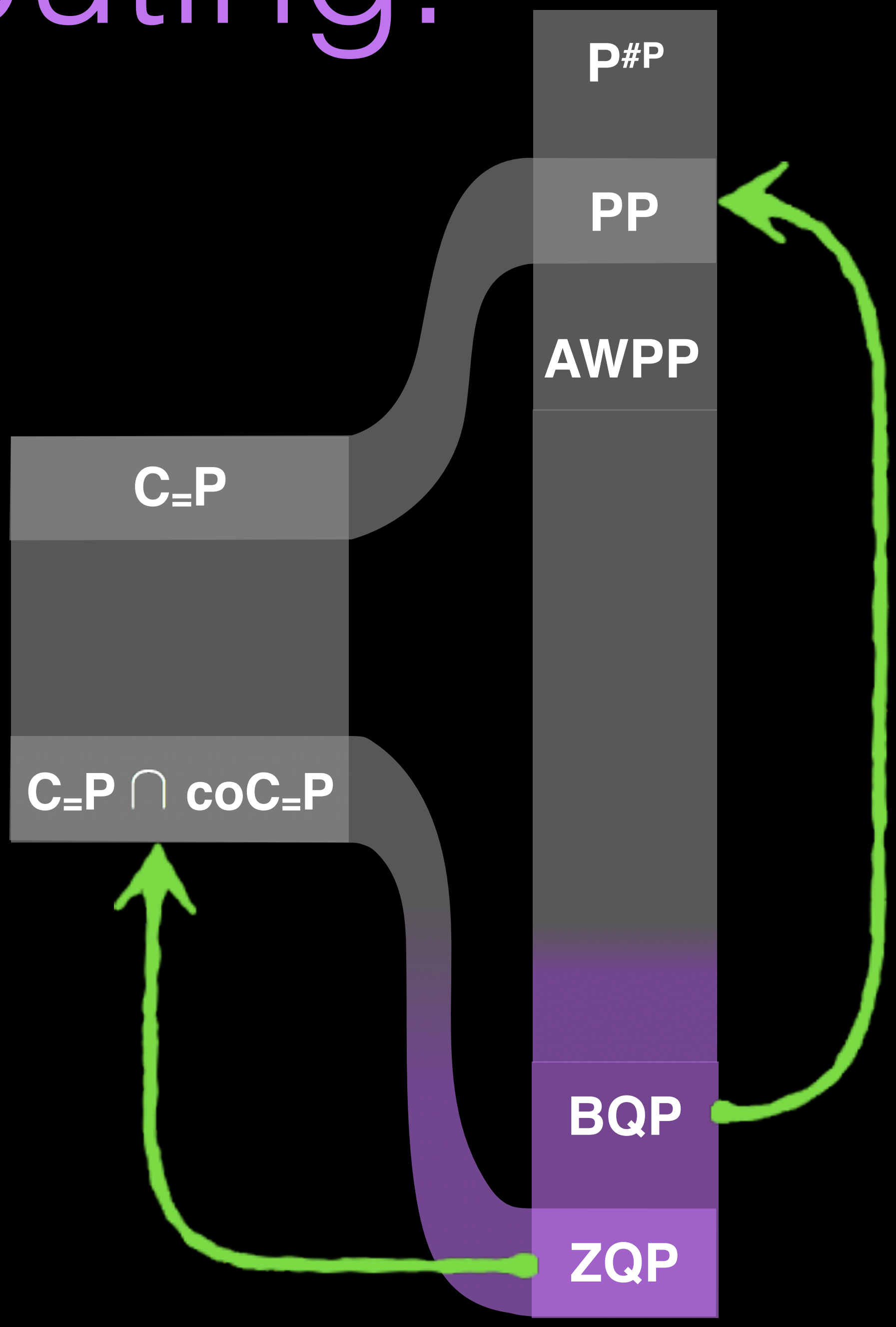
- **dB 2015** —
  $\mathrm{ZQP}_{\mathrm{GL}}$ = $\mathrm{C_{=}P} \cap \mathrm{coC_{=}P}$
  … saturating the known upper bound



Complexity of ***general linear*** "quantum" computing:

- **Aaronson, 2005** —
  $\text{BQP}_{\text{GL}} = \text{PP}$
  … a very large increase in (apparent) computational power

- **dB 2015** —
  $\text{ZQP}_{\text{GL}} = \text{C}_=\text{P} \cap \text{coC}_=\text{P}$
  … saturating the known upper bound

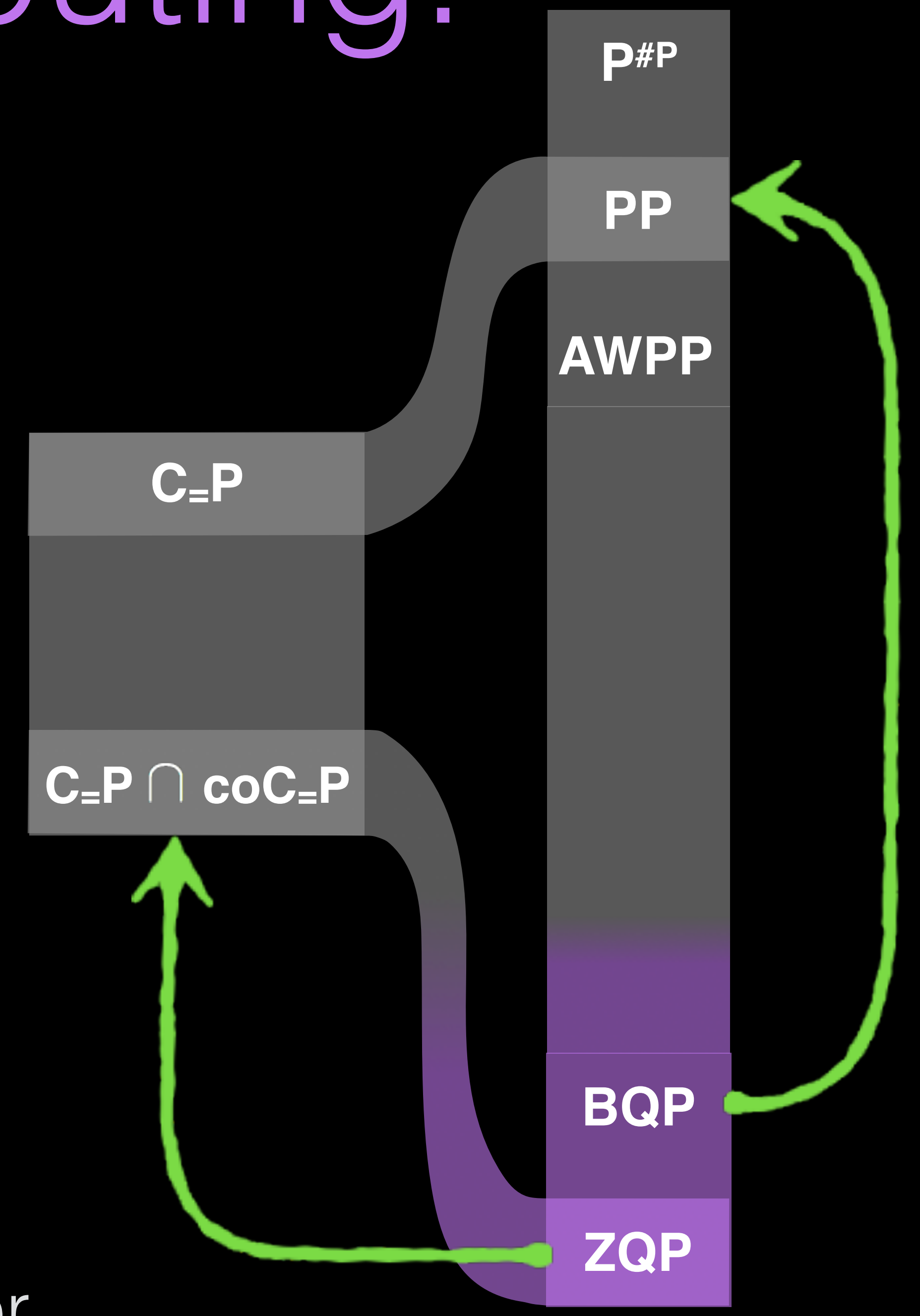


Complexity of ***general linear*** “quantum” computing:

- **Aaronson, 2005 —**
  $\mathrm{BQP}_{\mathrm{GL}} = \mathrm{PP}$
  … a very large increase in (apparent) computational power

- **dB 2015 —**
  $\mathrm{ZQP}_{\mathrm{GL}} = \mathrm{C_{=}P} \cap \mathrm{coC_{=}P}$
  … saturating the known upper bound

- **also:**
  Similar, but less dramatic, increases in power for *exact* (error-free and failure-free) computation with invertible gates



Model #2: "quantum" computing with amplitudes mod *p*

- **Amplitudes** —
  whichever cyclic ring R = $\mathbb{Z}/p$
  is your favourite

Model #2: "quantum" computing with amplitudes mod *p*

- **Amplitudes** —
  whichever cyclic ring R = $\mathbb{Z}/p$
  is your favourite

Model #2: "quantum" computing with amplitudes mod p

- **Amplitudes** —
  whichever cyclic ring R = $\mathbb{Z}/p$ is your favourite

- **States** —
  any vector $\psi \in RX$ with $\psi^{\mathsf{T}}\psi = 1$

Model #2: "quantum" computing with amplitudes mod *p*

- **Amplitudes** —
  whichever cyclic ring R = $\mathbb{Z}/p$ is your favourite

- **States** —
  any vector $\psi \in RX$ with $\psi^\mathsf{T}\psi = 1$

- **Transformations** —
  "norm"-preserving operations

Model #2: "quantum" computing with amplitudes mod p

- **Amplitudes** —
  whichever cyclic ring R = $\mathbb{Z}/p$ is your favourite
- **States** —
  any vector $\psi \in RX$ with $\psi^{\mathsf{T}}\psi = 1$
- **Transformations** —
  "norm"-preserving operations

Model #2: "quantum" computing with amplitudes mod p

- **Amplitudes** — whichever cyclic ring R = $\mathbb{Z}/p$ is your favourite
- **States** — any vector $\psi \in RX$ with $\psi^{\mathsf{T}}\psi = 1$
- **Transformations** — "norm"-preserving operations
- **Significance order** — $\alpha \preccurlyeq \beta$ iff $\alpha \in \beta$R (*c.f.* p-adic norm)

Complexity of "quantum" computing with amplitudes mod p:

Schumacher + Westmoreland, 2010 —
teleportation, superdense coding, etc. in "modal quantum mechanics" involving amplitudes mod p (or drawn from a finite field)

Complexity of “quantum” computing with amplitudes mod p:

Schumacher + Westmoreland, 2010 —
teleportation, superdense coding, etc. in “modal quantum mechanics” involving amplitudes mod p (or drawn from a finite field)

dB 2014 —

- for prime p: can reduce significance of error / failure to **zero**, by repetition

Complexity of "quantum" computing with amplitudes mod p:

Schumacher + Westmoreland, 2010 —
teleportation, superdense coding, etc. in "modal quantum mechanics" involving amplitudes mod p (or drawn from a finite field)

dB 2014 —

- for prime p: can reduce significance of error / failure to **zero**, by repetition
- Define $\mathbf{UnitaryP}_p$ as problems **exactly solvable** in this model — with **zero** significance of either failure or error in the output — in polynomial time

Complexity of "quantum" computing with amplitudes mod p:

Schumacher + Westmoreland, 2010 —
teleportation, superdense coding, etc. in "modal quantum mechanics" involving amplitudes mod p (or drawn from a finite field)

dB 2014 —

- for prime p: can reduce significance of error / failure to **zero**, by repetition
- Define **UnitaryP**$_p$ as problems **exactly solvable** in this model — with **zero** significance of either failure or error in the output — in polynomial time
- Can show that **UnitaryP**$_p$ = **Mod**$_p$**P** — a modulo-p variant of the class **NP**

Summary

the take-away
from Wonderland

What's the bottom line?

- These models of computation have in common:
  - ❖ Destructive interference is possible (like quantum computation)
  - ❖ Interference is **easier to realise** than in quantum computation
  - ❖ Bounded error / zero error computation is **very, very powerful**

Evidence of the power of destructive interference

— and that imposing constraints on realising it can have a dramatic impact on "expected computational power"

What’s the bottom line?

- These models of computation have in common:
  - ❖ Destructive interference is possible (like quantum computation)
  - ❖ Interference is **easier to realise** than in quantum computation
  - ❖ Bounded error / zero error computation is **very, very powerful**

Evidence of the power of destructive interference

— and that imposing constraints on realising it can have a dramatic impact on “expected computational power”

Intuition for quantum computation

— The class **EQP** (of problems exactly solvable by efficient quantum algorithms*) may be **much less** powerful than **BQP.**

Perhaps even **EQP** = **P** !

Thanks for listening!

Quantum Computing, Postselection, and Probabilistic Polynomial-Time
Aaronson, **[arXiv:quant-ph/0412187]**

On exact counting and quasi-quantum complexity
dB, **[arXiv:1509.07789]**

Modal quantum theory
Schumacher and Westmoreland, **[arXiv:1010.2929]**

On computation with 'probabilities' modulo k
dB, **[arXiv:1405.7381]**