Beyond NP: The Work and Legacy of Larry Stockmeyer

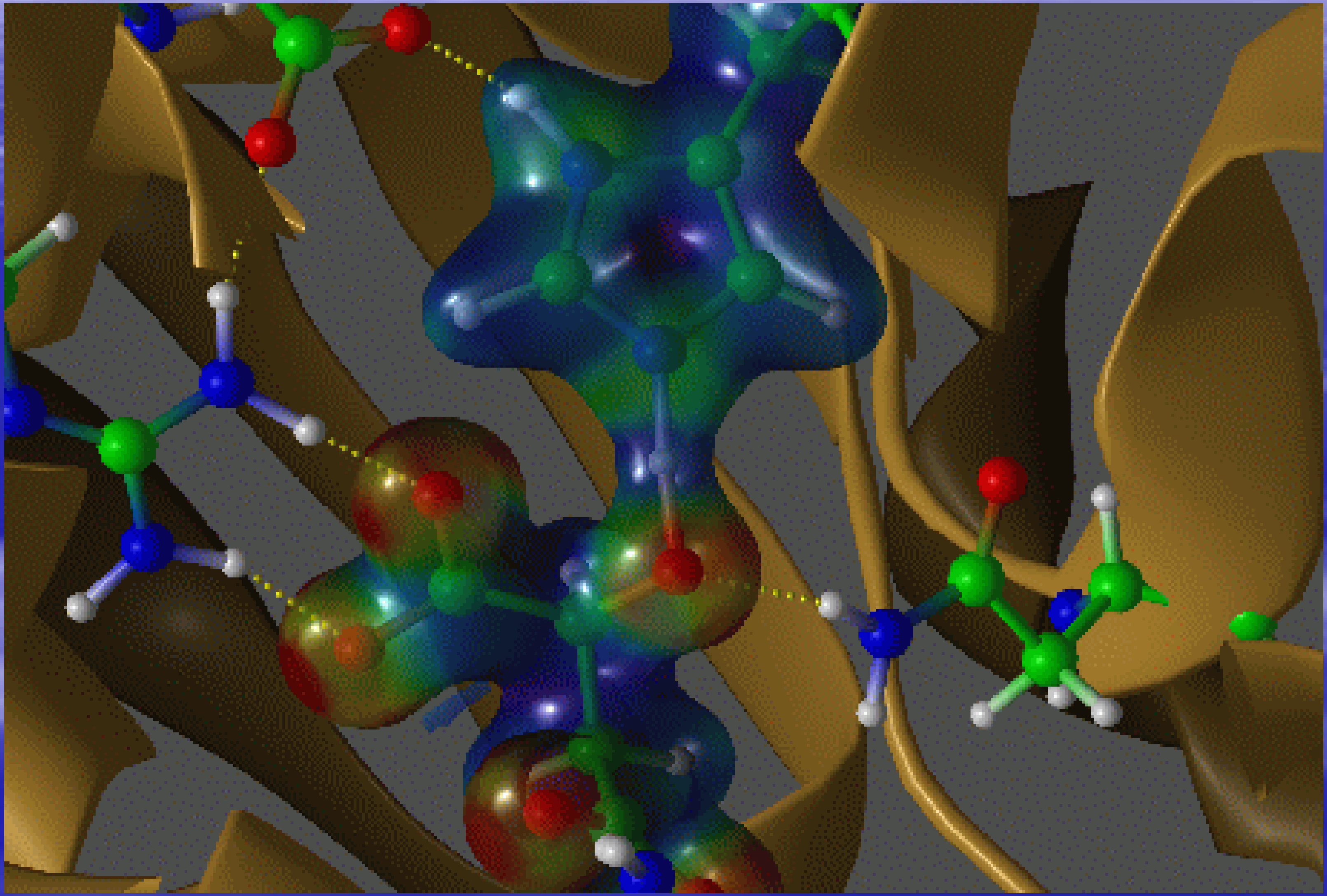
Lance Fortnow
University of Chicago

Larry Joseph Stockmeyer

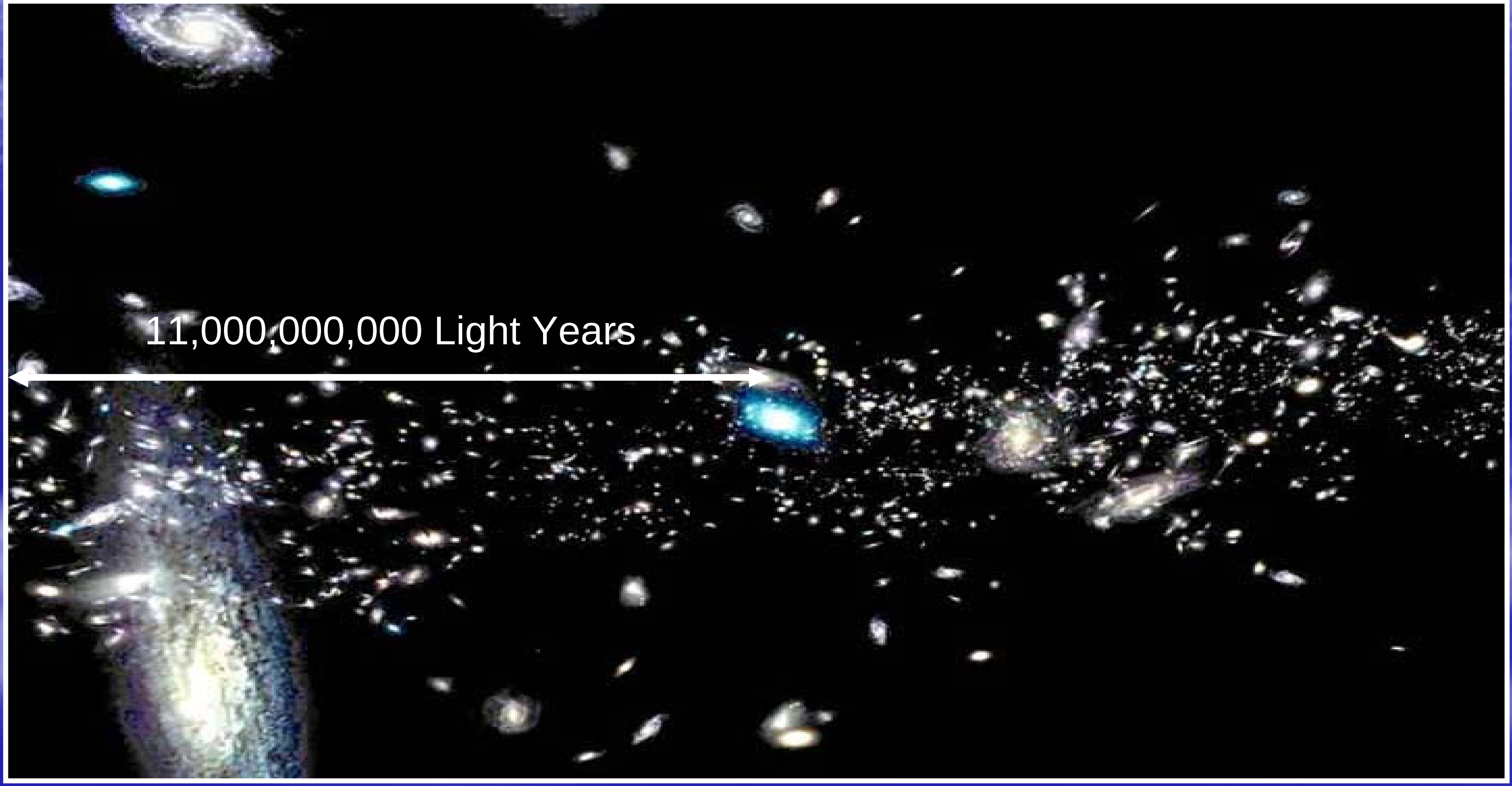
- 1948 – Born in Indiana
- 1974 – MIT Ph.D.
- IBM Research at Yorktown and Almaden for most of his career
- 82 Papers (11 JACM)
  - 49 Distinct Co-Authors
- 1996 – ACM Fellow
- Died July 31, 2004

The Universe

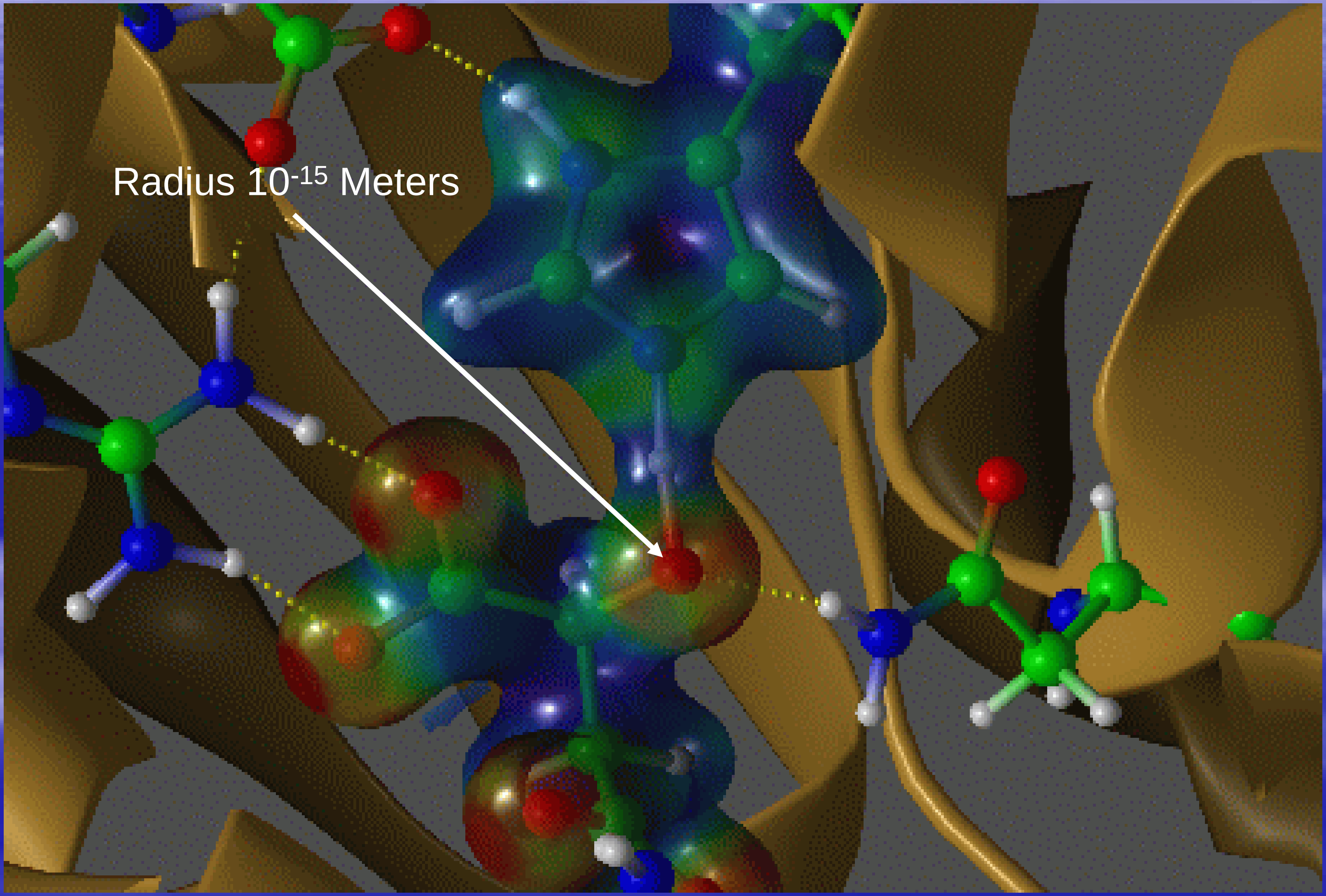
Computer of Protons



The Universe



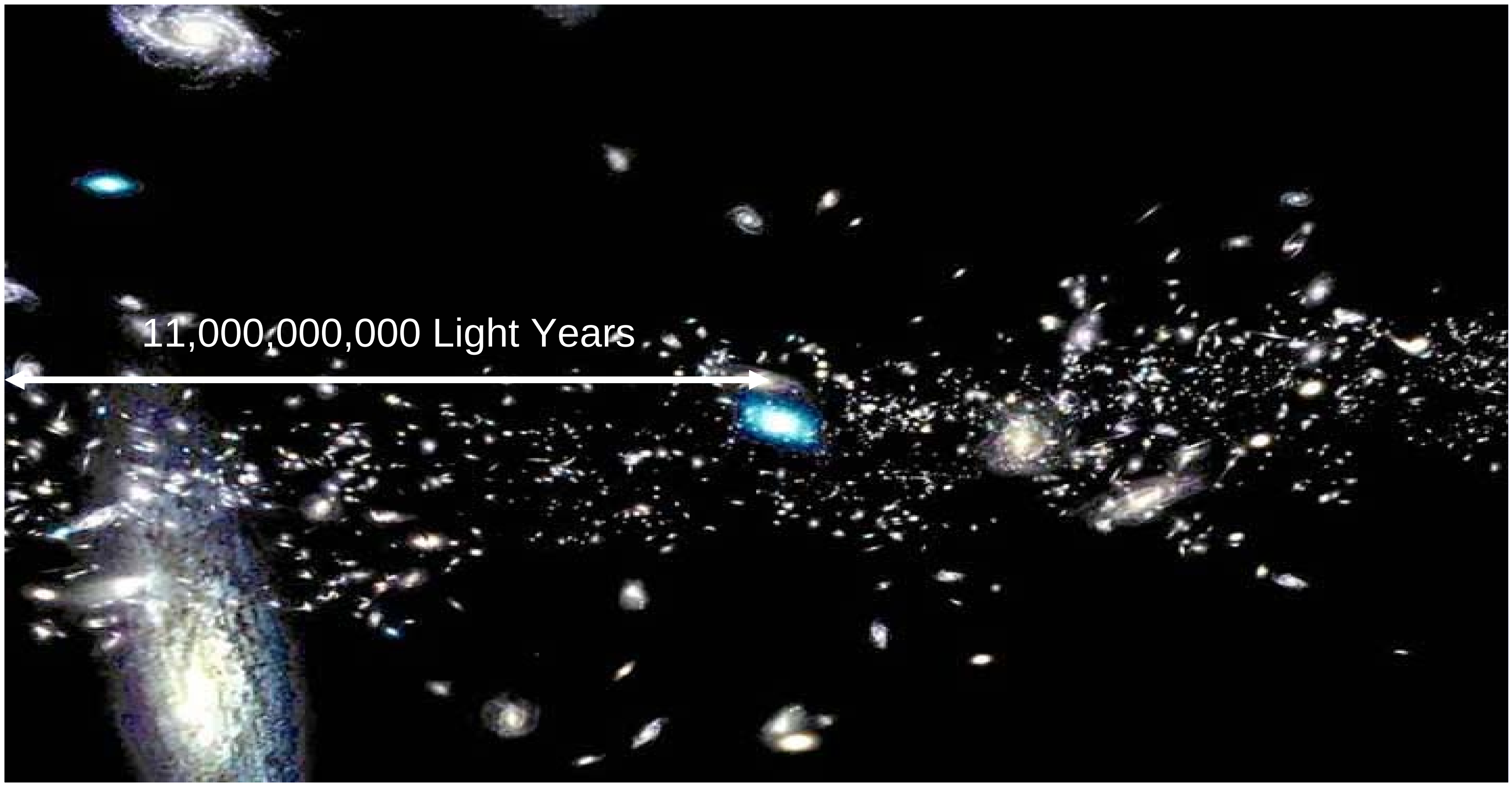
Computer of Protons



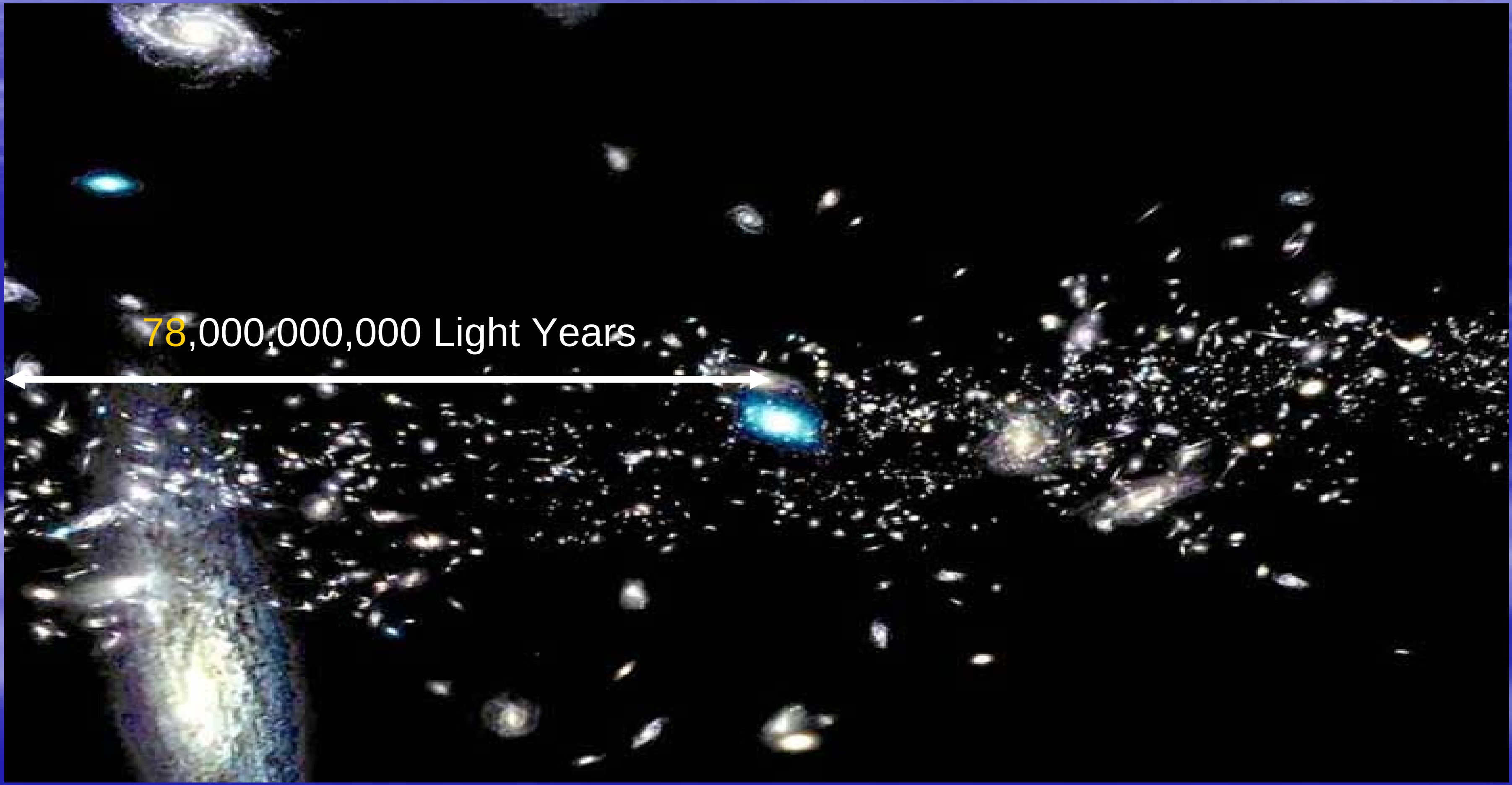
Computing with the Universe

- Universe can only have 10^{123} proton gates.
- Consider the true sentences of weak monadic second-order theory of the natural numbers with successor (EWS1S).
  - $\exists A\ \forall B\ \exists x\ (x \in A \rightarrow x+1 \in B)$
- Cannot solve EWS1S on inputs of size 616 in universe with proton-sized gates.
  - Stockmeyer Ph.D. Thesis 1974
  - Stockmeyer-Meyer JACM 2002

The Universe



The Universe



Computing with the Universe

- Universe can have 10^{123} proton gates.

Computing with the Universe

- Universe can have $3.5*10^{125}$ proton gates.

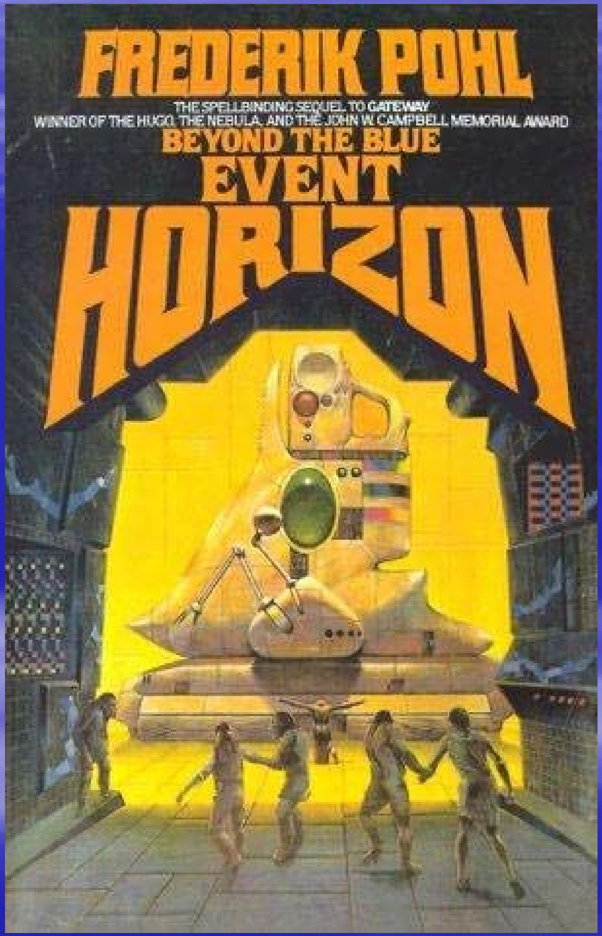
Computing with the Universe

- Universe can have $3.5*10^{125}$ proton gates.
- Cannot solve EWS1S on inputs of size 616 in universe with proton-sized gates.

Computing with the Universe

- Universe can have $3.5*10^{125}$ proton gates.
- Cannot solve EWS1S on inputs of size 619 in universe with proton-sized gates.

Science Fiction?

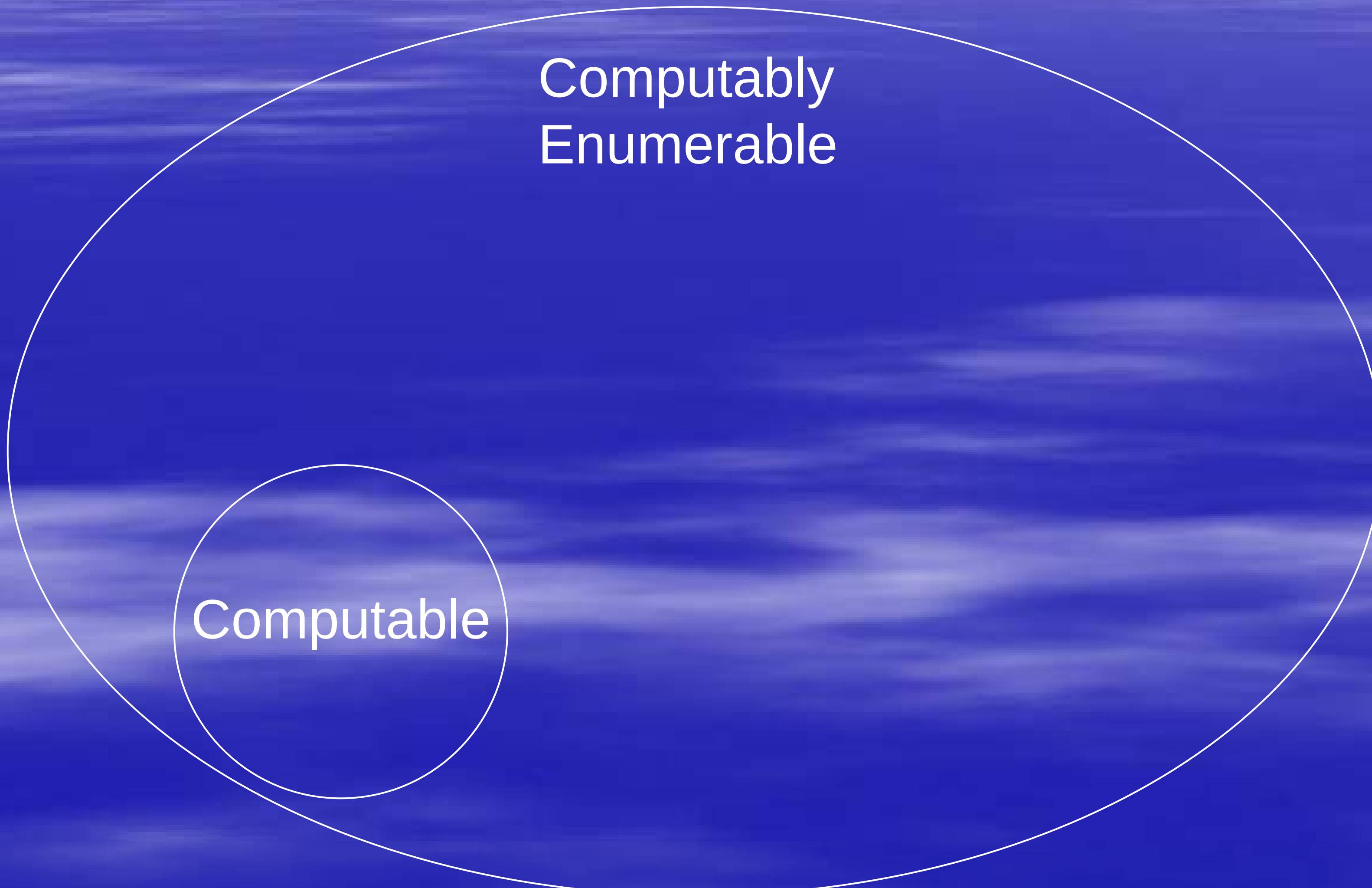


- The complexity of algorithms tax even the resources of sixty billion gigabits---or of a universe full of bits; Meyer and Stockmeyer had proved, long ago, that, regardless of computer power, problems existed which could not be solved in the life of the universe.

Evolution of Complexity

Evolution of Complexity

Turing-Church-Kleene-Post 1936

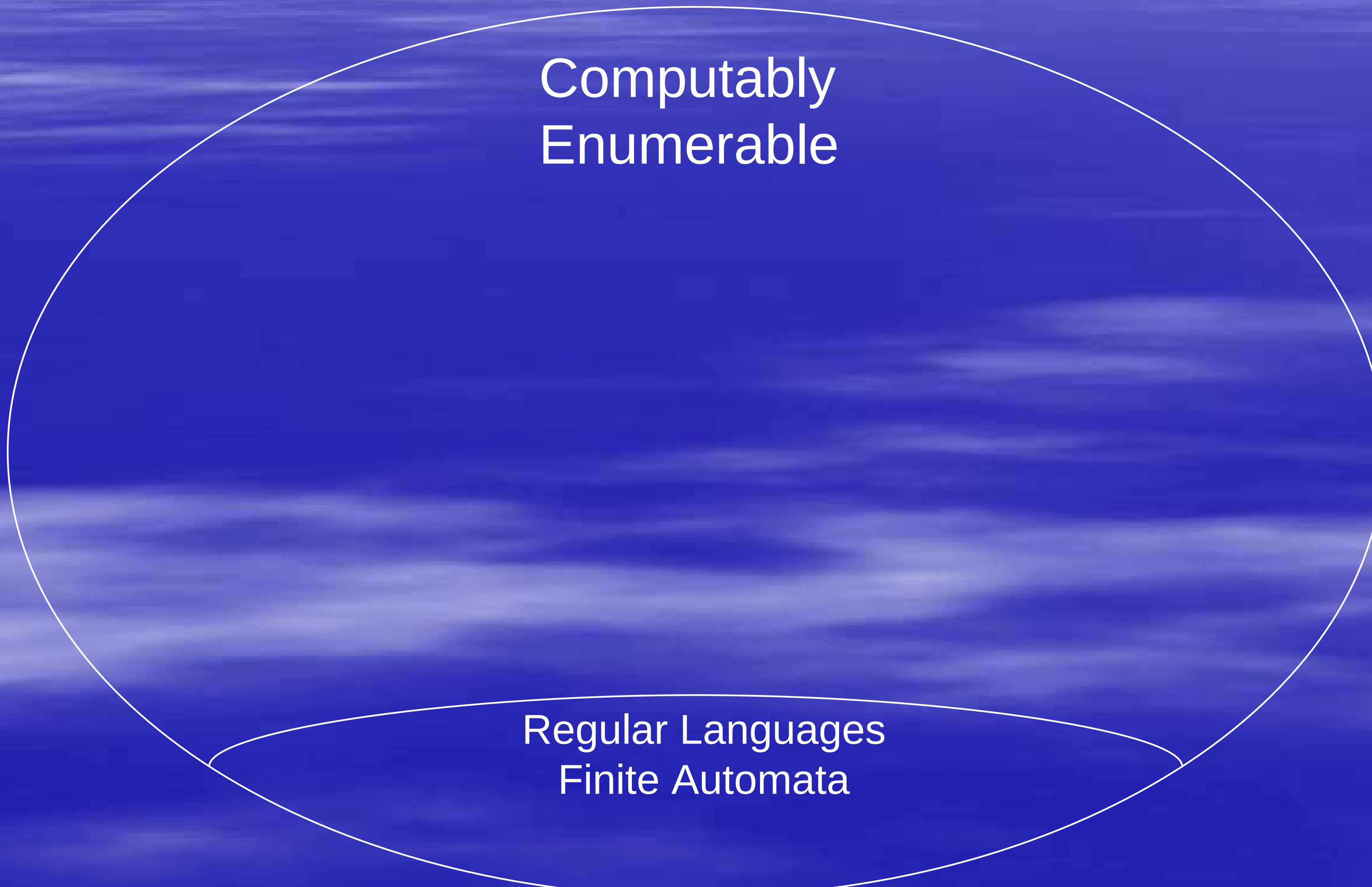


Evolution of Complexity

Computably
Enumerable

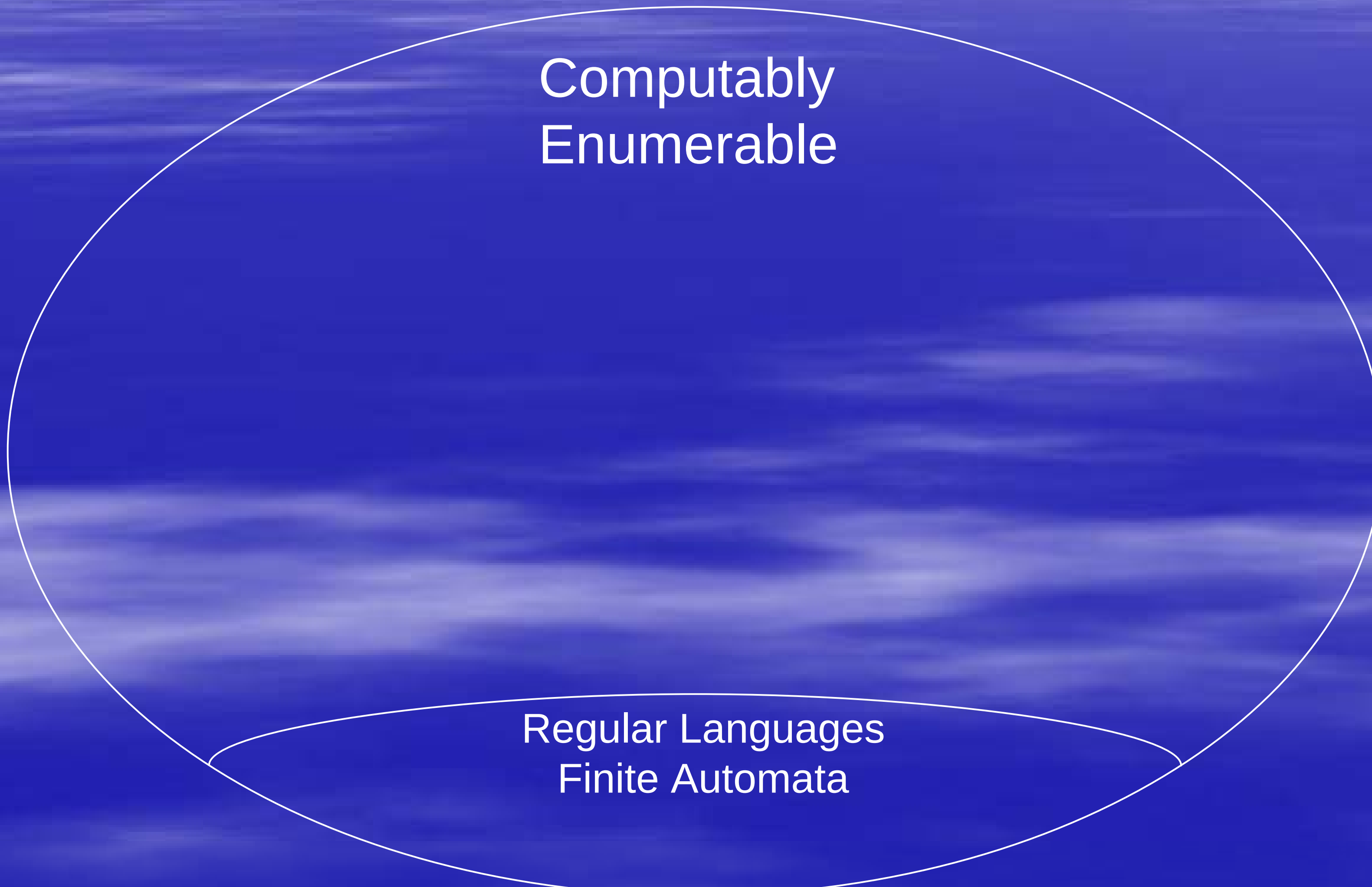
Evolution of Complexity

Kleene 1956



Evolution of Complexity

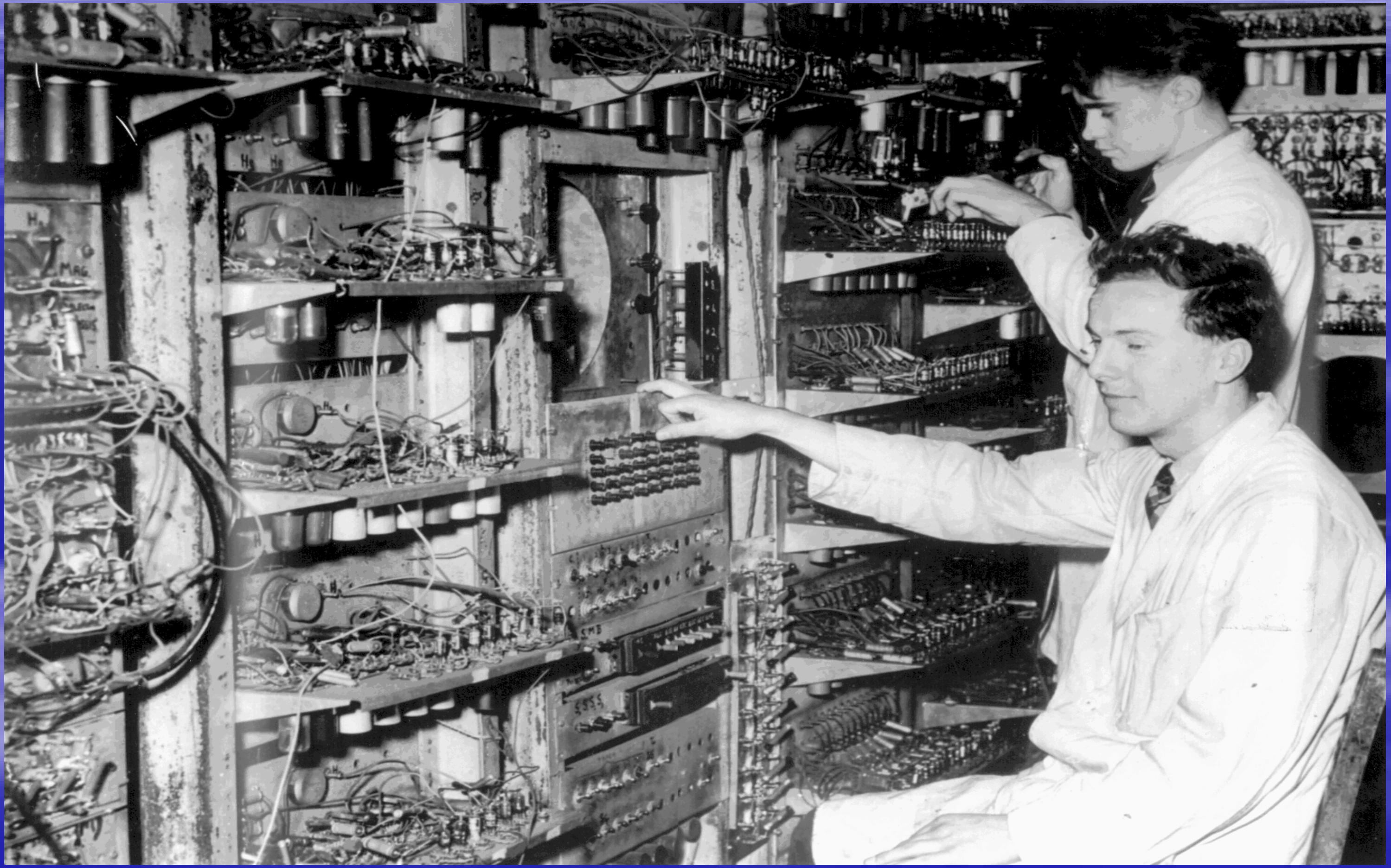
Chomsky Hierarchy 1956



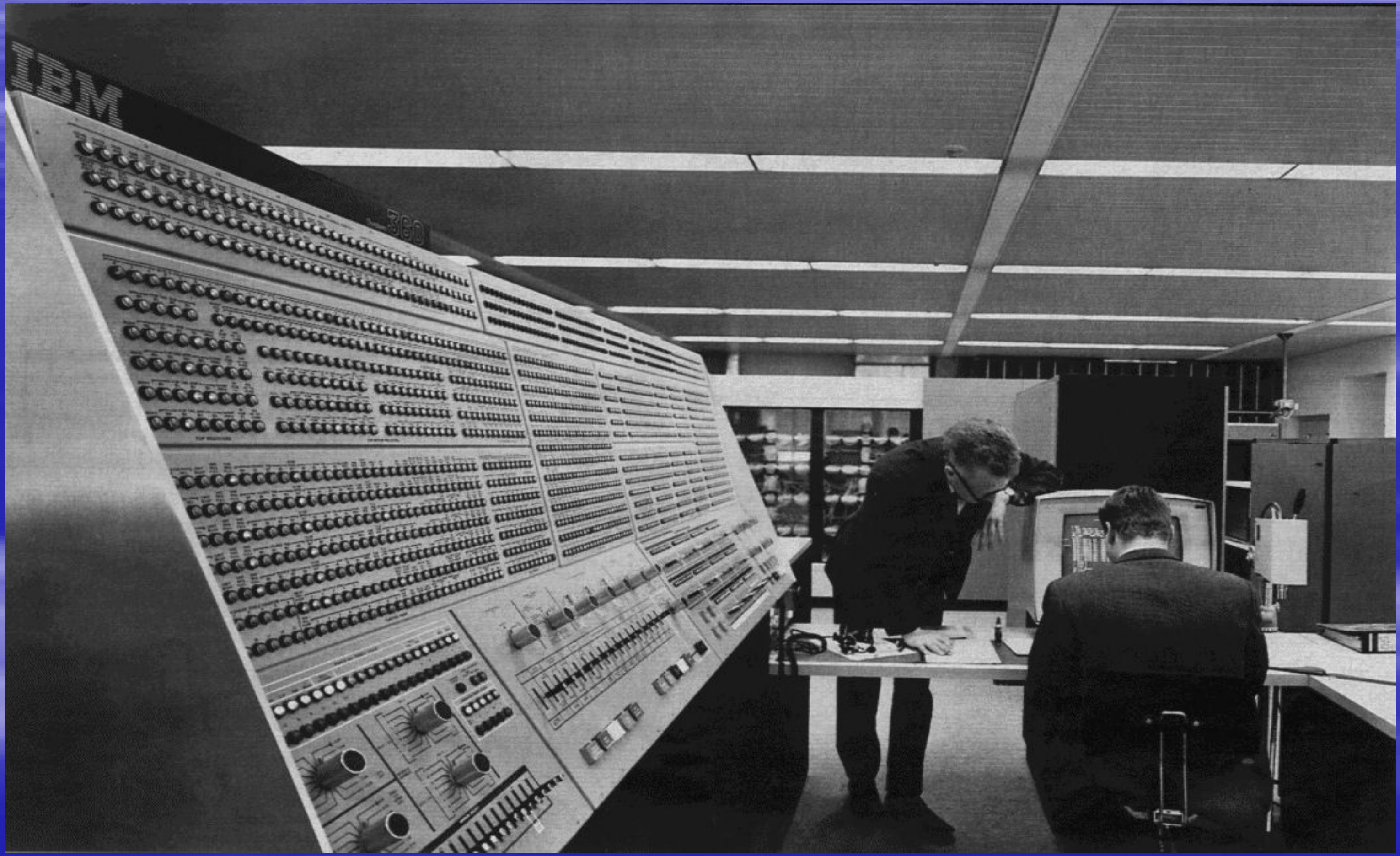
Evolution of Complexity

Chomsky Hierarchy 1956

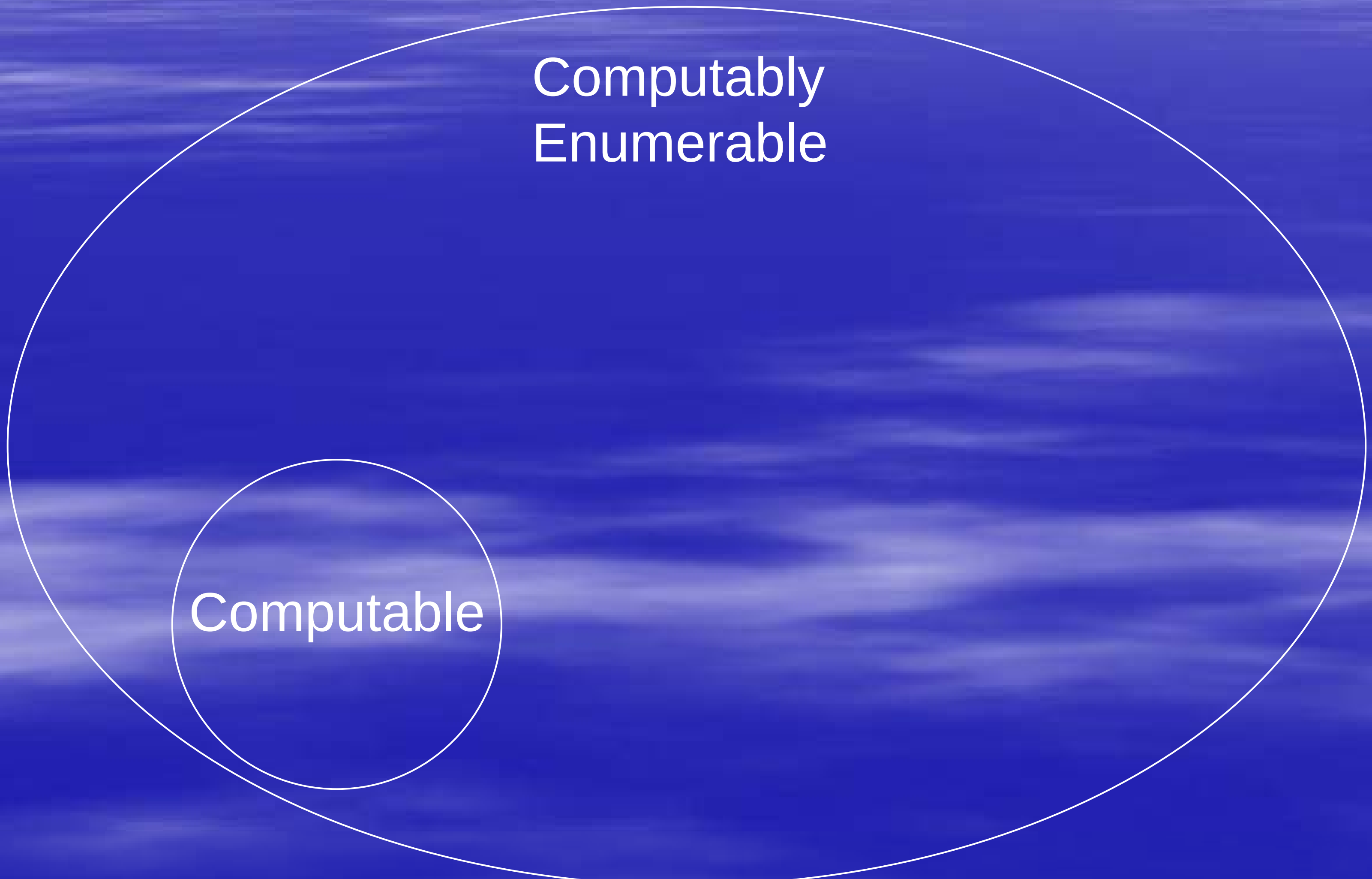
Real Computers



Faster Computers



Evolution of Complexity



Evolution of Complexity

Evolution of Complexity

Computable

Evolution of Complexity

Hartmanis-Stearns 1965

Computable

Evolution of Complexity

Hartmanis-Stearns 1965

Computable

TIME(n^2)

Evolution of Complexity

Hartmanis-Stearns 1965

Computable
TIME(2^n)
TIME(n^5)
TIME(n^2)

Evolution of Complexity

Hartmanis-Stearns 1965

Computable

TIME(n)

Limitations of DTIME(t(n))

- Not Machine Independent.
- Separations are by diagonalization and not by natural problems.
- No clear notion of efficient computation.

Evolution of Complexity

Cobham 1964 Edmonds 1965

Computable

Evolution of Complexity

Cobham 1964 Edmonds 1965

Computable

$P = \cup DTIME(n^k)$

Evolution of Complexity

Cobham 1964 Edmonds 1965

Computable

- Matching

$P = \cup DTIME(n^k)$

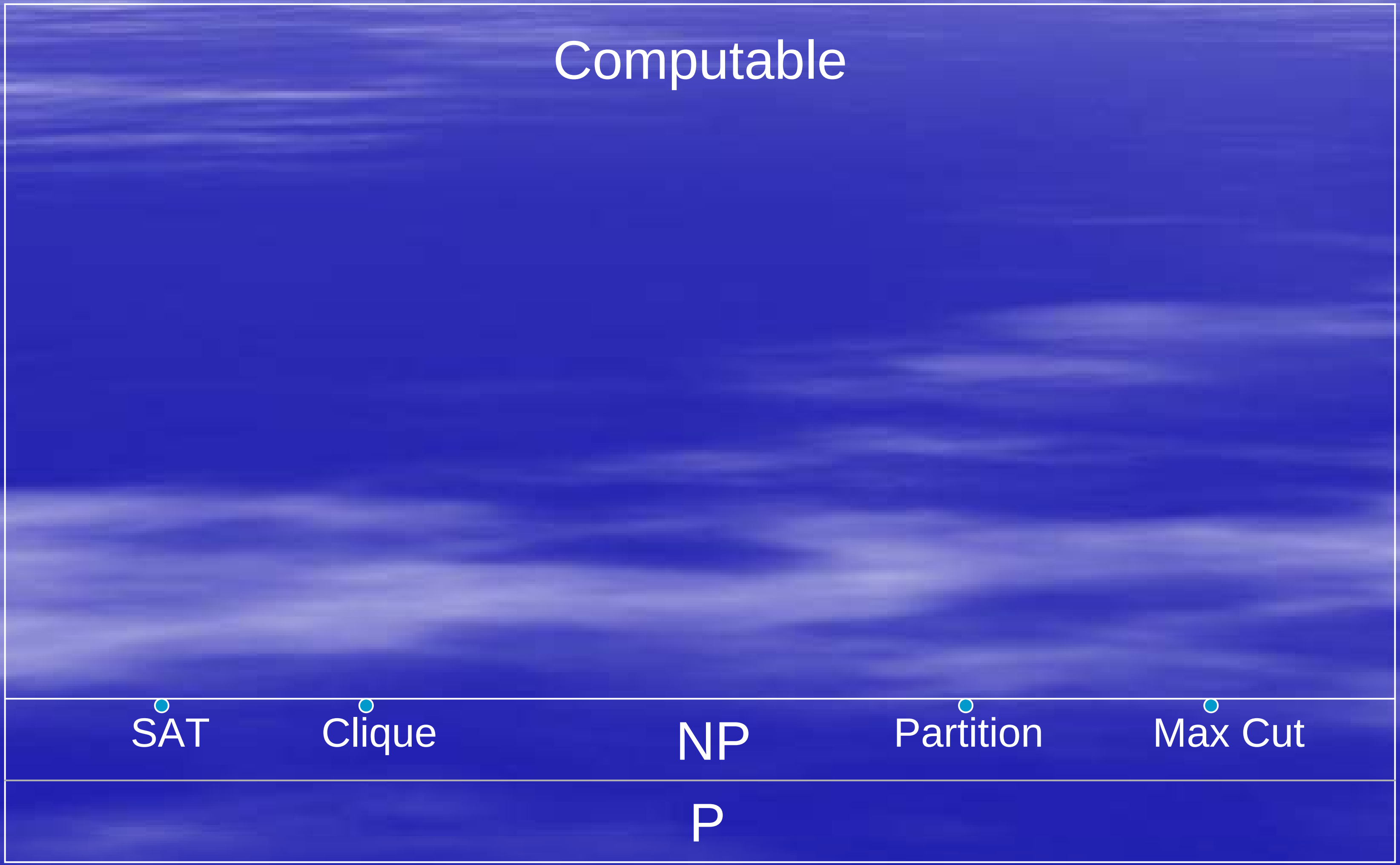
Evolution of Complexity

Computable

P

Evolution of Complexity

Cook 1971 Levin 1973 Karp 1972



State of Complexity 1972

Computable

NP

P

Enter Larry Stockmeyer

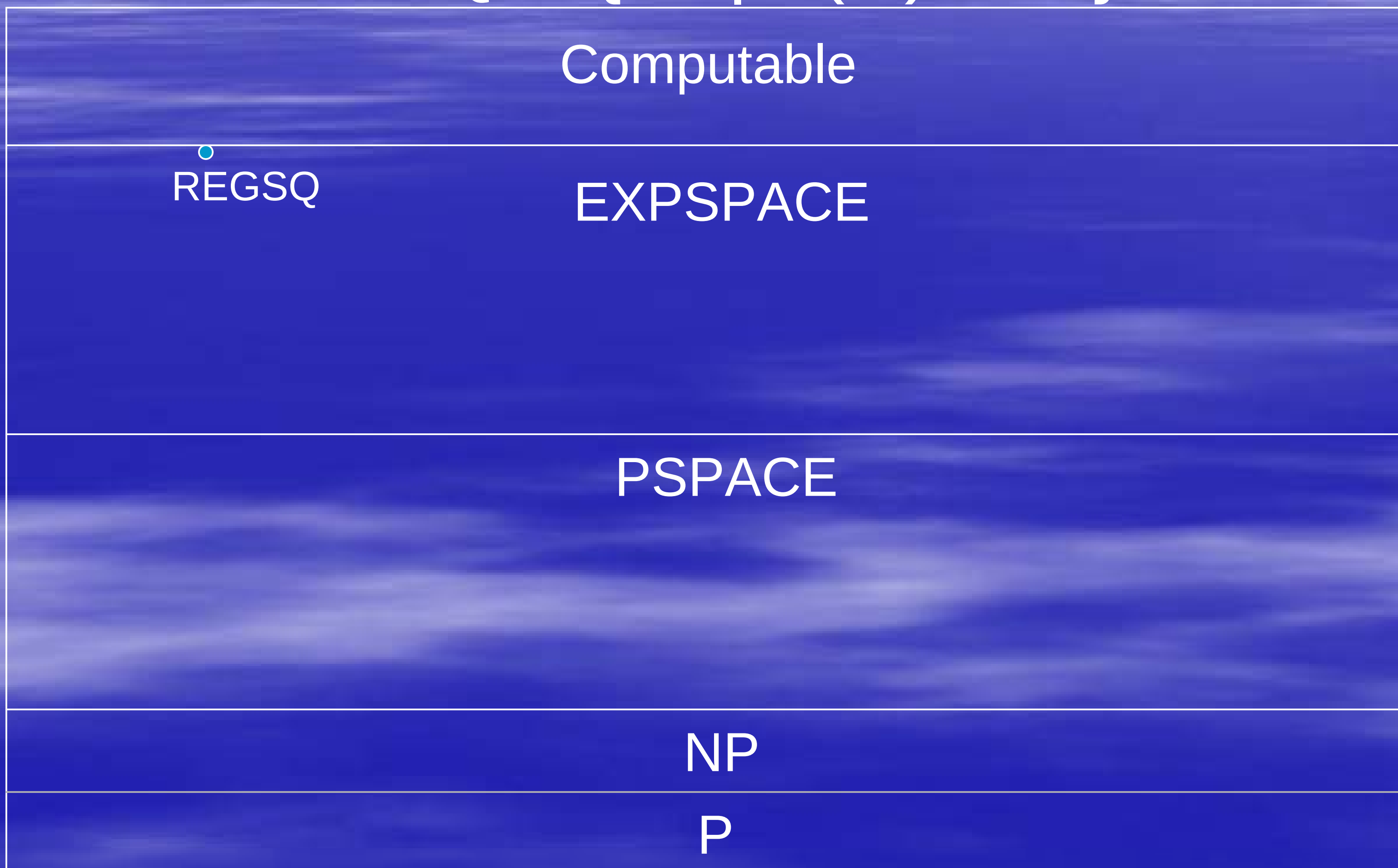
- January 1972 – Bachelors/Masters at MIT
  - Bounds on Polynomial Evaluation Algorithms
- Can we find natural hard problems?
  - Diagonalization methods do not lead to natural problems.
  - There are natural NP-complete problems but cannot prove them not in P.
  - With Advisor Albert Meyer

Regular Expressions with Squaring

- (0+1)*00(0+1)*00(0+1)*
  - – All strings with two sets of consecutive zeros.
- Allow Squaring operator: $r^2=rr$
- $(0+1)^*(0^2(0+1)^*)^2$
- No more expressive power but can be much shorter when used recursively.
  - – $((((((0^2)^2)^2)^2)^2)^2)=$ 0000000000000000000000000000000000000000000000000000000000000000

Meyer-Stockmeyer 1972

$$REGSQ = \{ R \mid L(R) \neq \Sigma^* \}$$

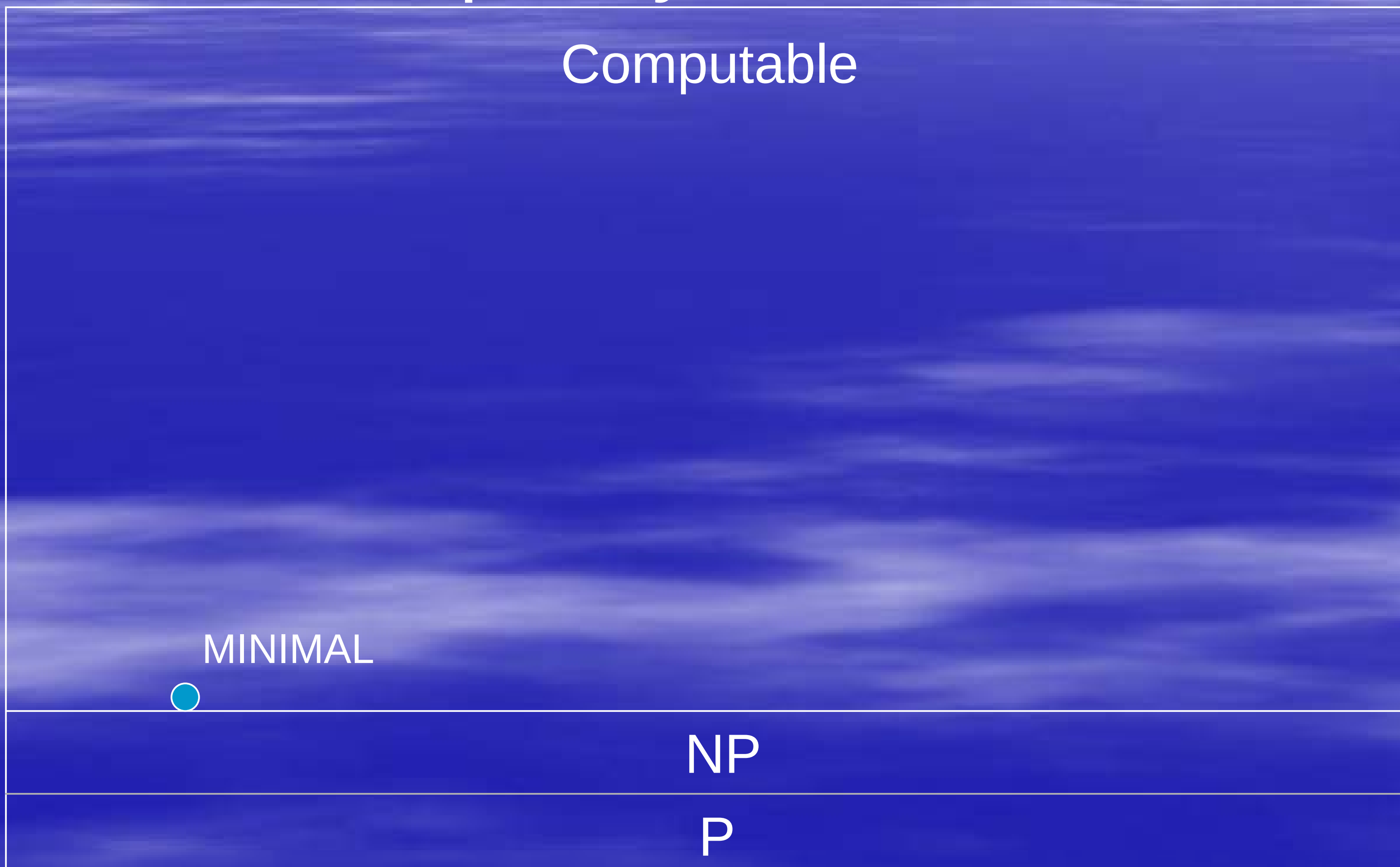


Regular Expressions with Squaring

- Meyer and Stockmeyer, “The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space” – SWAT 1972
- MINIMAL
  - Set of Boolean formulas with no smaller equivalent formula.

Meyer-Stockmeyer 1972

Complexity of MINIMAL

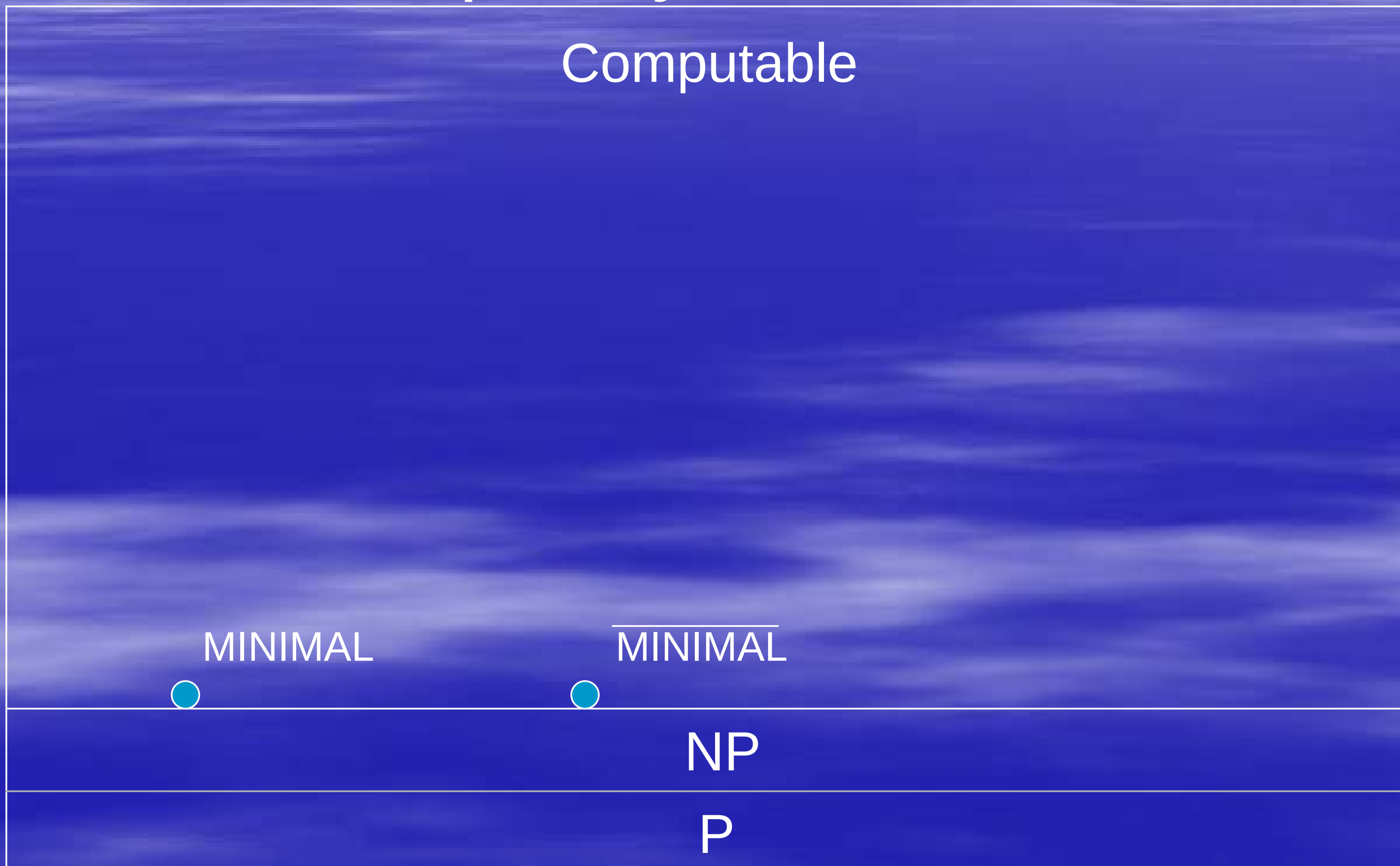


MINIMAL

- MINIMAL
  - Set of Boolean formulas with no smaller equivalent formula.
- MINIMAL in NP?
  - Can’t check all smaller formulas.

Meyer-Stockmeyer 1972

Complexity of MINIMAL



MINIMAL

- MINIMAL
  – Set of Boolean formulas with no smaller equivalent formula.
- MINIMAL in NP?
  – Can’t check all smaller formulas.

- MINIMAL in NP?
  – Can’t check equivalence.

MINIMAL

- MINIMAL
  - Set of Boolean formulas with no smaller equivalent formula.
- MINIMAL in NP?
  - Can’t check all smaller formulas.

- MINIMAL in NP?
  - Can’t check equivalence.

- MINIMAL is in NP with an “oracle” for equivalence.

MINIMAL in NP with Equivalence Oracle

$$(x \vee y) \wedge (x \vee \overline{y}) \wedge z$$

Guess: $x \wedge z$

$(x \wedge z\ ,\ (x \vee y) \wedge (x \vee \overline{y}) \wedge z)$ →

Equivalence

EQUIVALENT ←

MINIMAL

- MINIMAL is in NP with an “oracle” for equivalence or non-equivalence.

MINIMAL

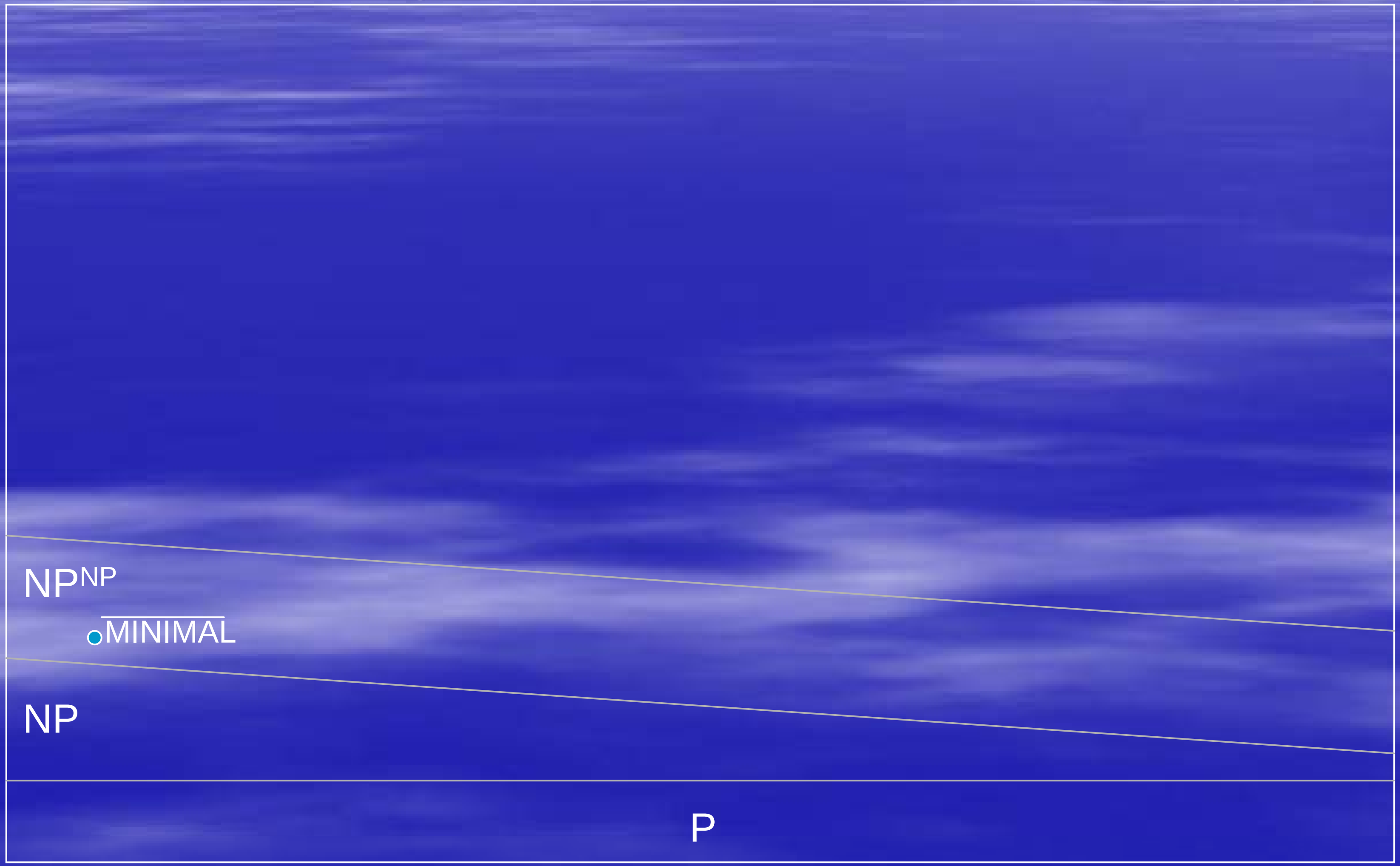
- $\overline{\text{MINIMAL}}$ is in NP with an "oracle" for equivalence or non-equivalence.
- Since non-equivalence is in NP we can solve $\overline{\text{MINIMAL}}$ in NP with NP oracle.

MINIMAL

- $\overline{\text{MINIMAL}}$ is in NP with an “oracle” for equivalence or non-equivalence.
- Since non-equivalence is in NP we can solve $\overline{\text{MINIMAL}}$ in NP with NP oracle.
- Suggests a “hierarchy” above NP.

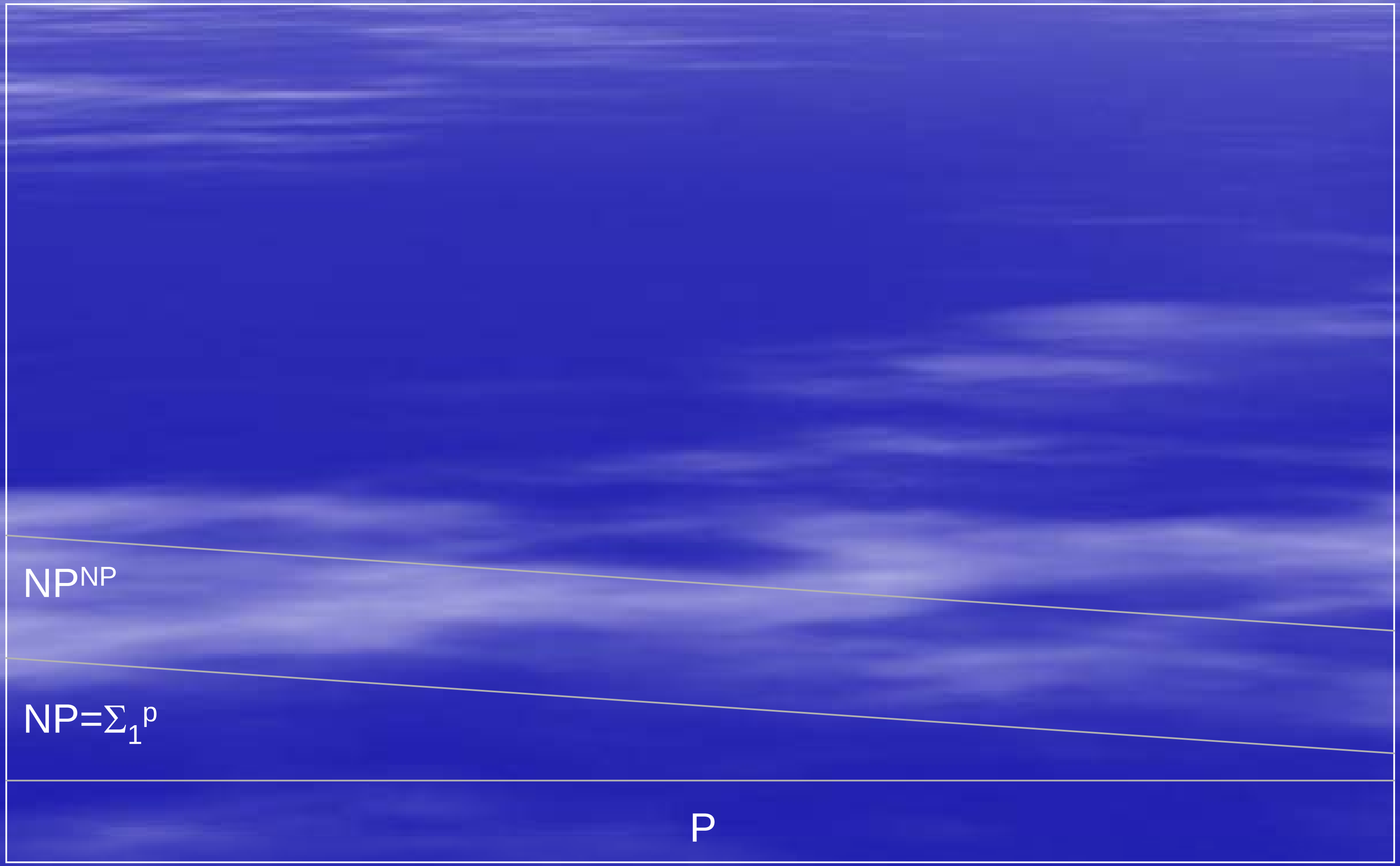
Meyer-Stockmeyer 1972

The Polynomial Time Hierarchy



Meyer-Stockmeyer 1972

The Polynomial Time Hierarchy



Meyer-Stockmeyer 1972

The Polynomial Time Hierarchy

$NP^{\Sigma_3^p} = \Sigma_4^p$

$NP^{\Sigma_2^p} = \Sigma_3^p$

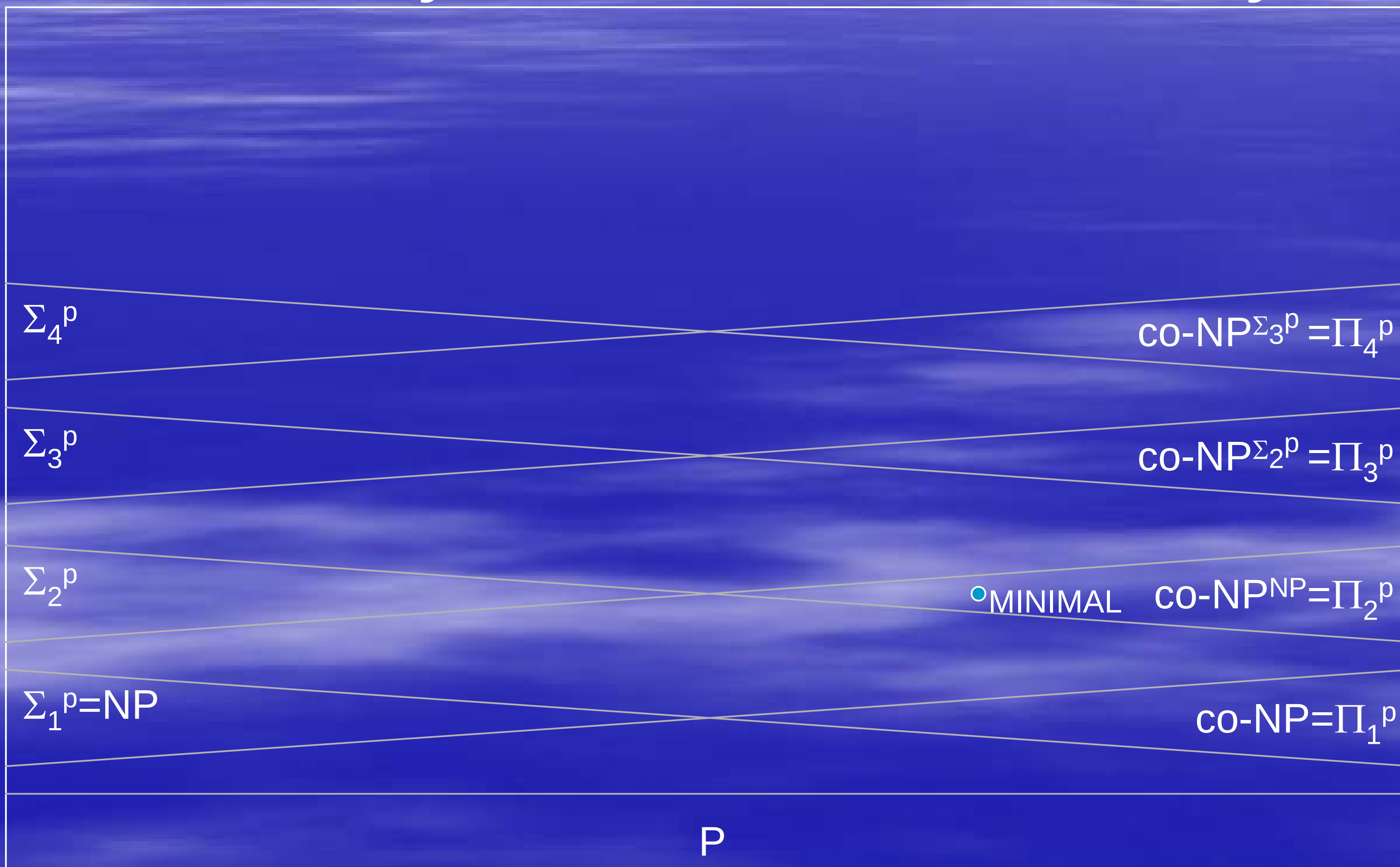
$NP^{NP} = \Sigma_2^p$

$NP = \Sigma_1^p$

P

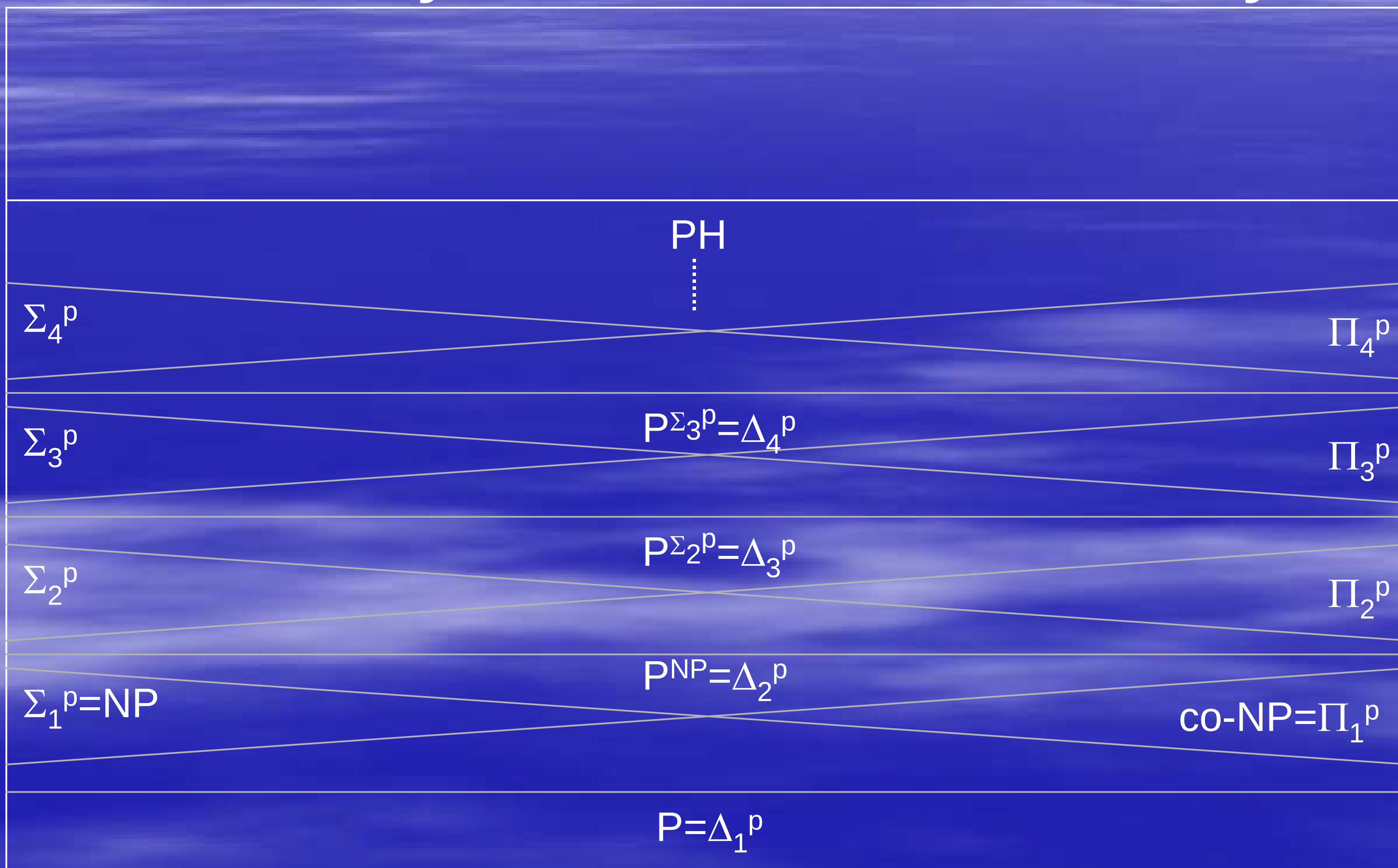
Meyer-Stockmeyer 1972

The Polynomial Time Hierarchy



Meyer-Stockmeyer 1972

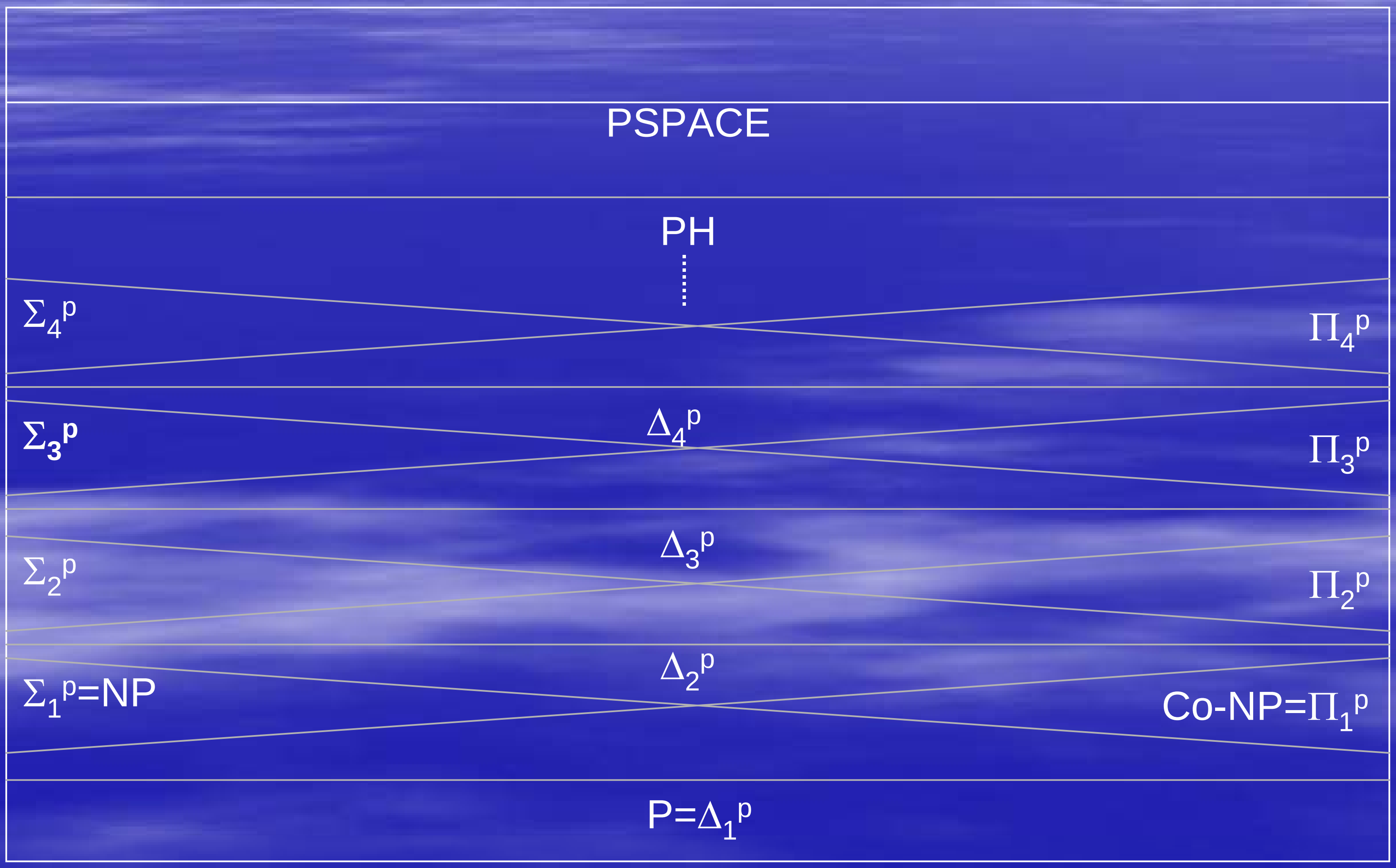
The Polynomial Time Hierarchy



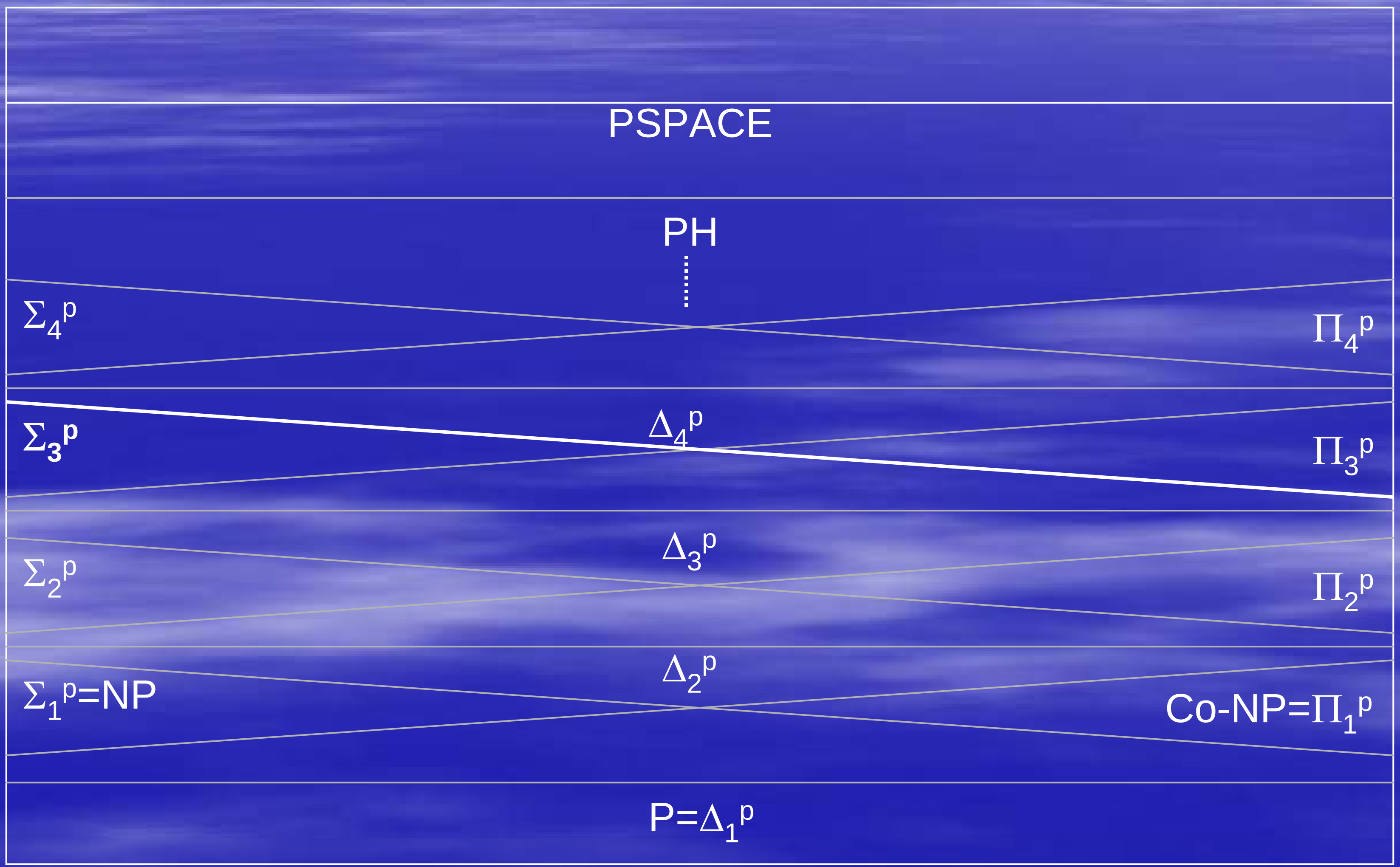
Properties of the Hierarchy

- Meyer-Stockmeyer, “The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space”, SWAT 1972
- Stockmeyer, “The Polynomial-Time Hierarchy”, TCS, 1977.
- Wrathall, “Complete Sets and the Polynomial-Time Hierarchy”, TCS, 1977.

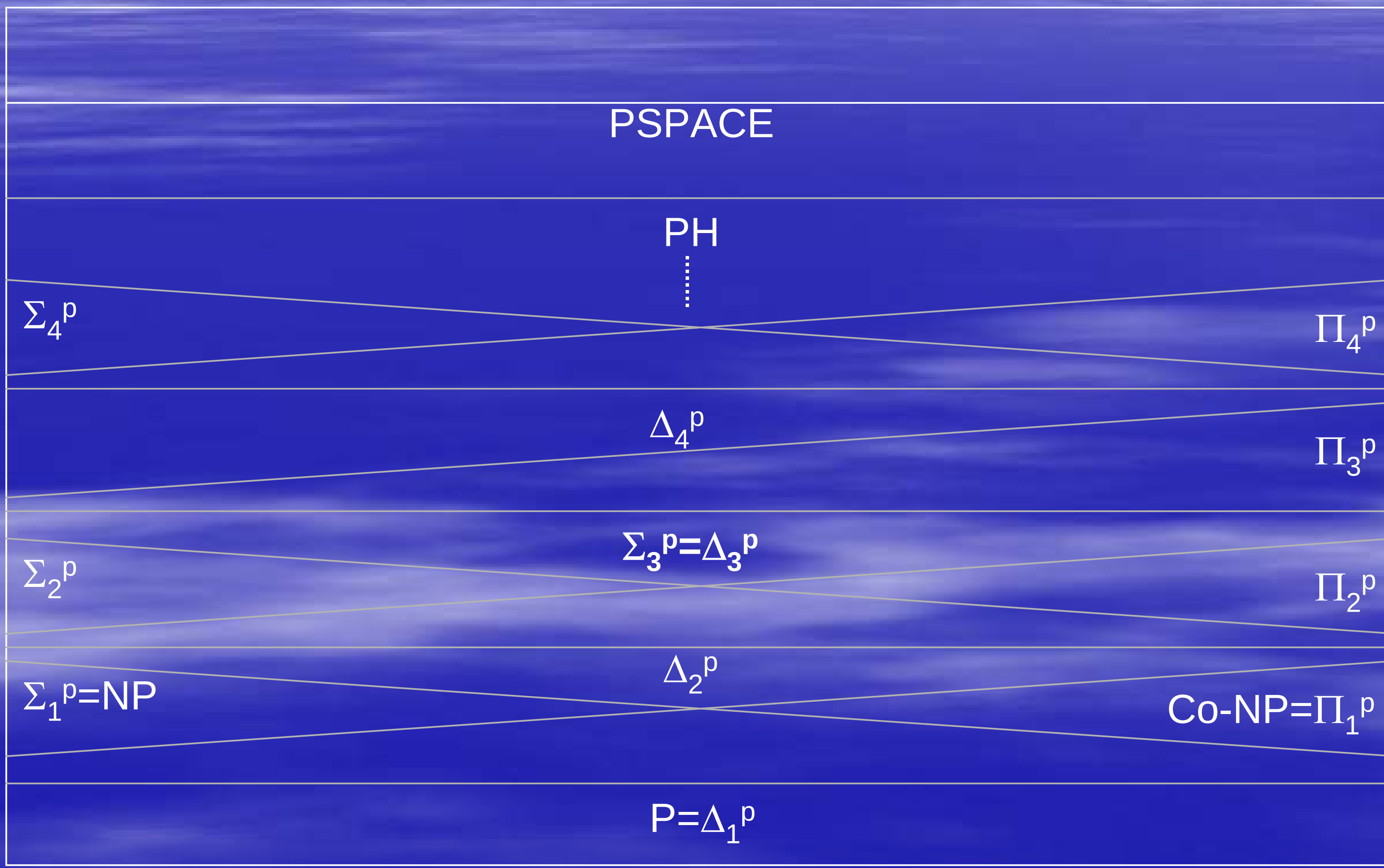
Properties of the Hierarchy



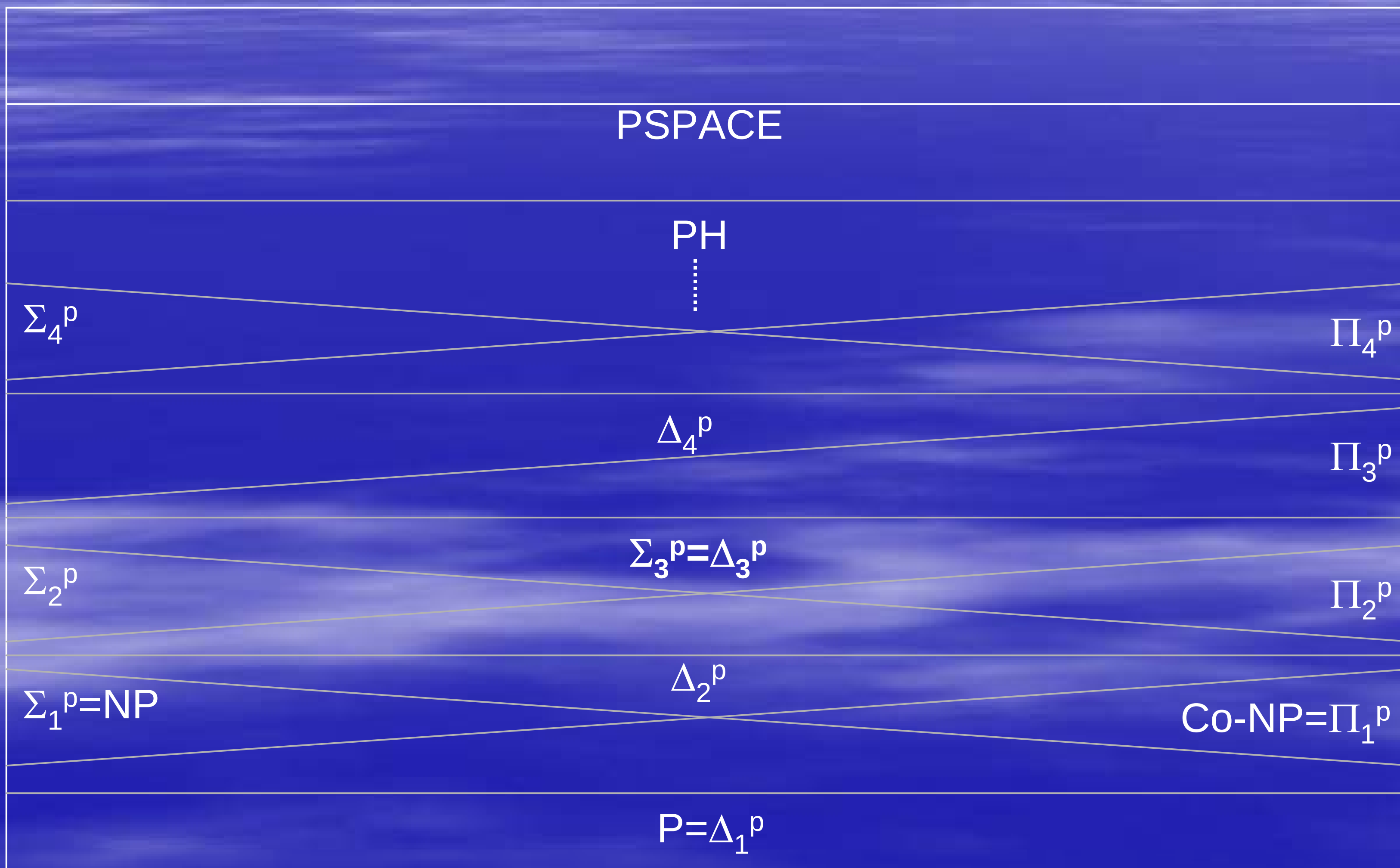
Properties of the Hierarchy



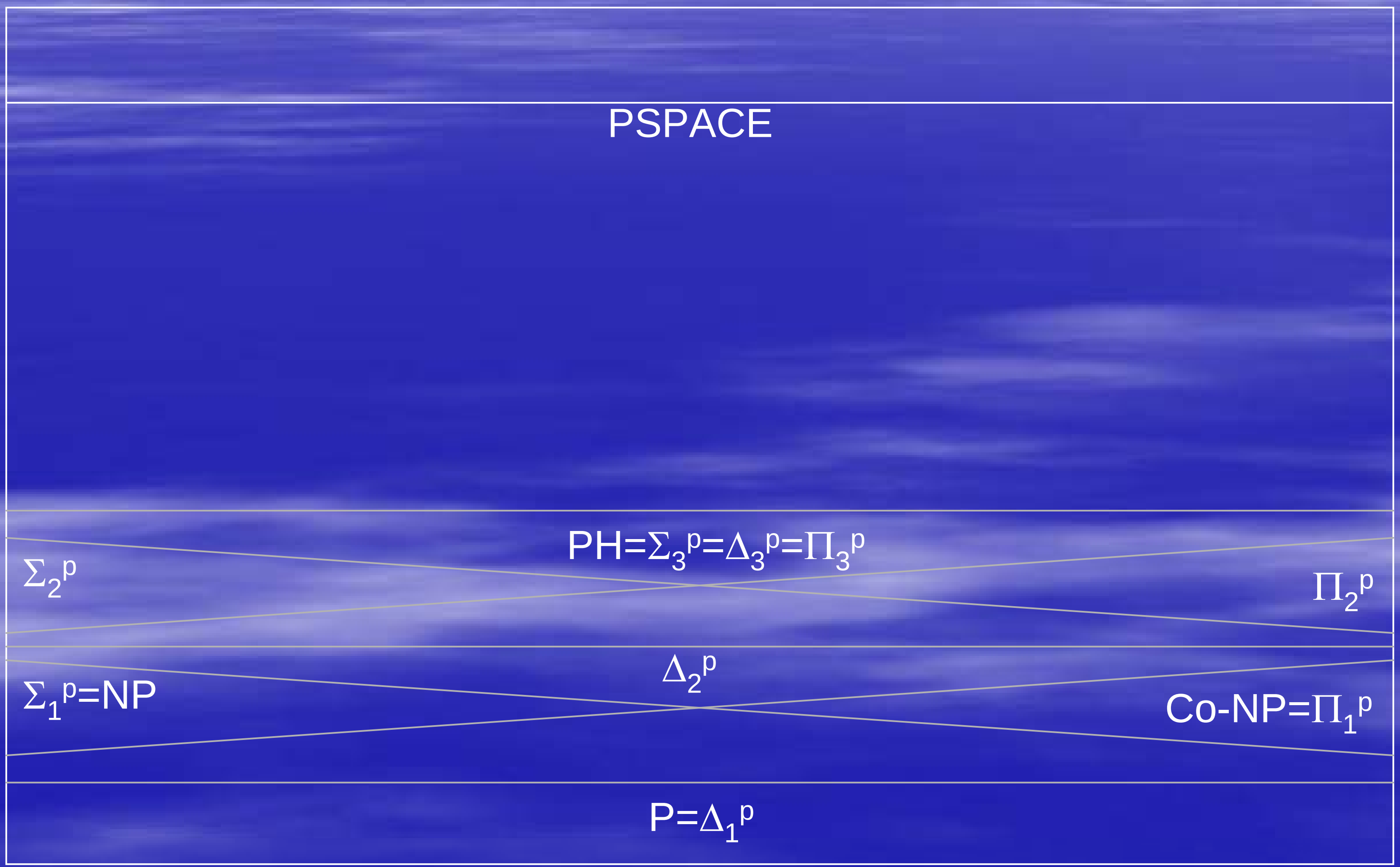
Properties of the Hierarchy



Properties of the Hierarchy



Properties of the Hierarchy



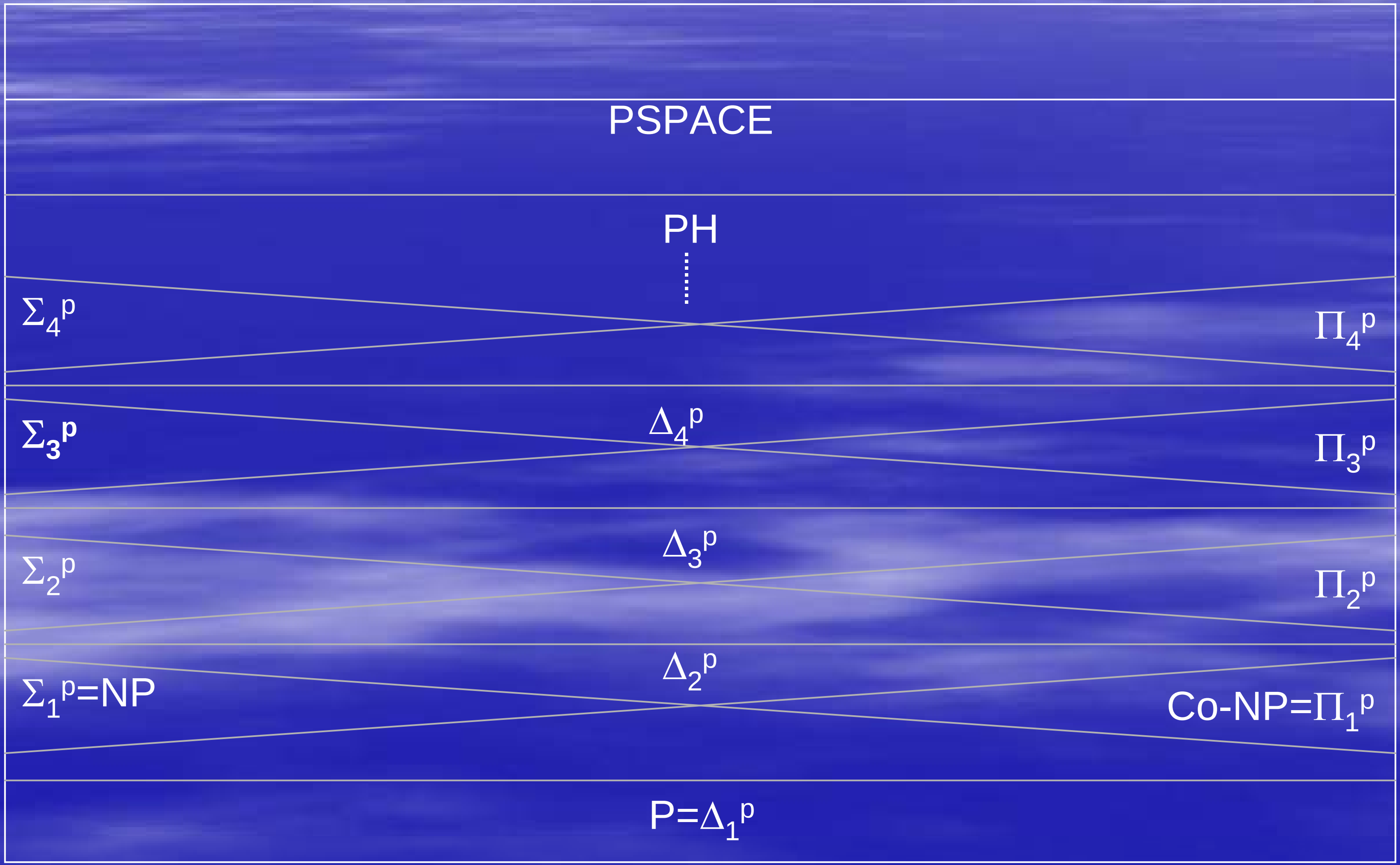
Properties of the Hierarchy

If P = NP

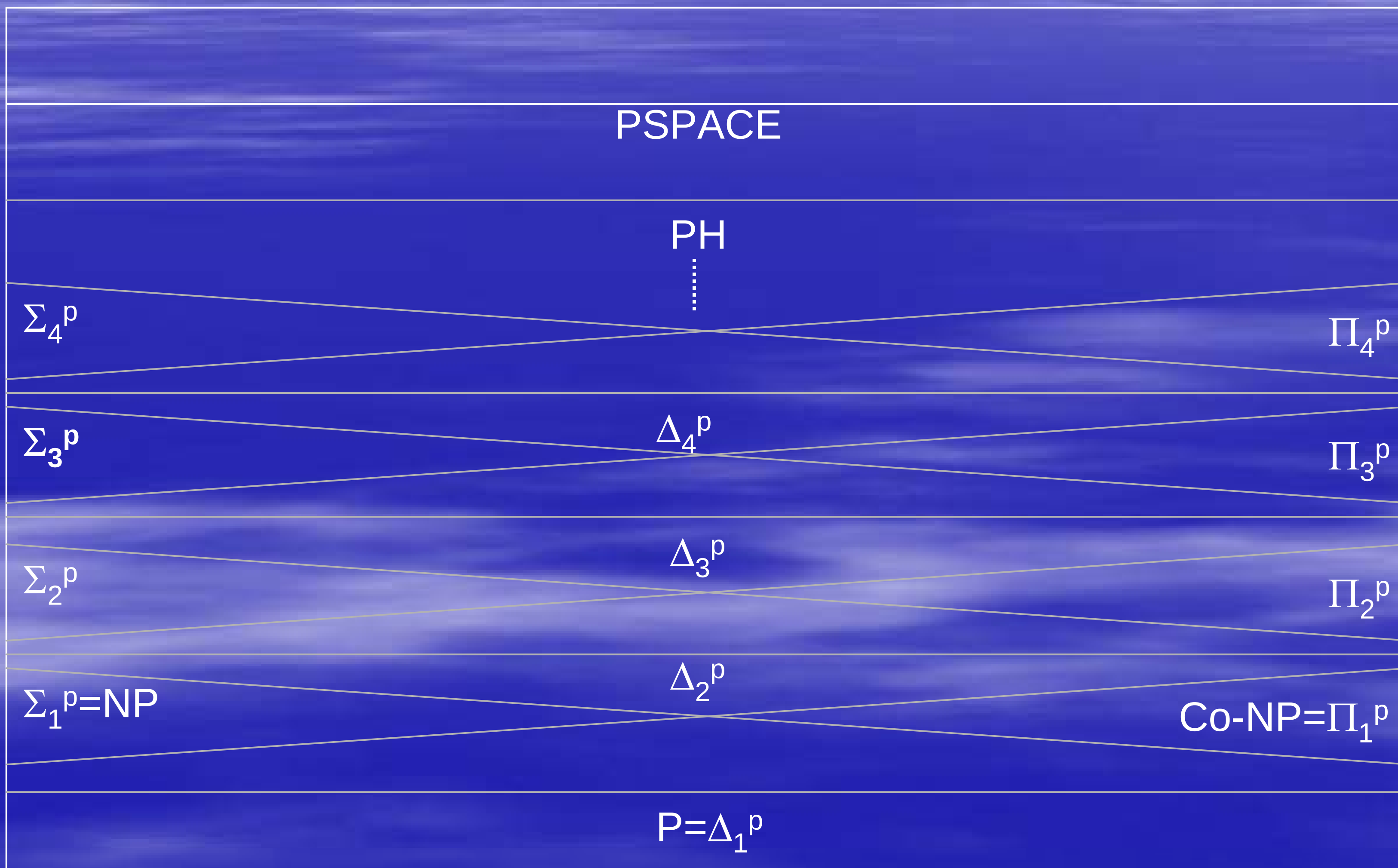
PSPACE

P=NP=PH

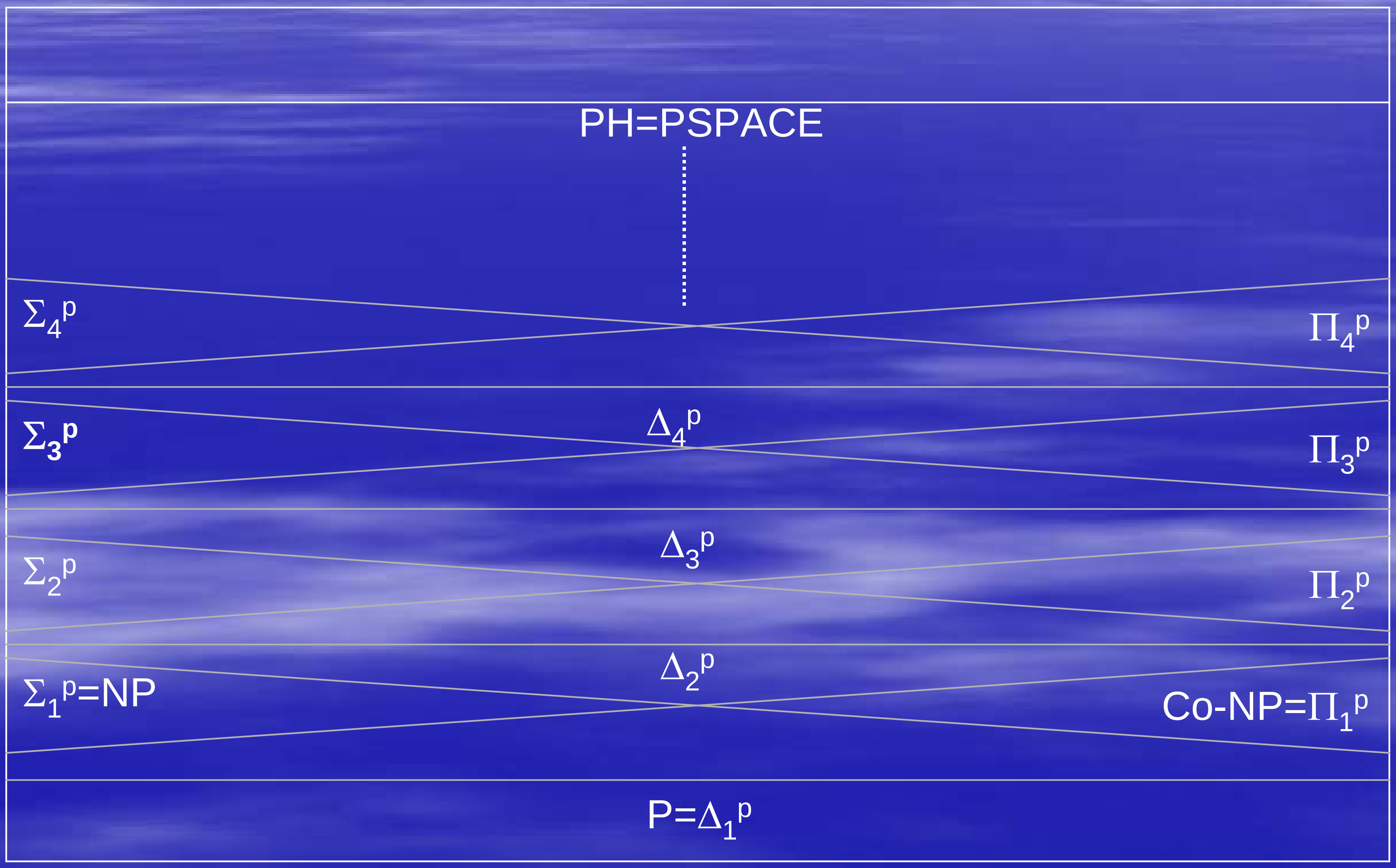
Properties of the Hierarchy



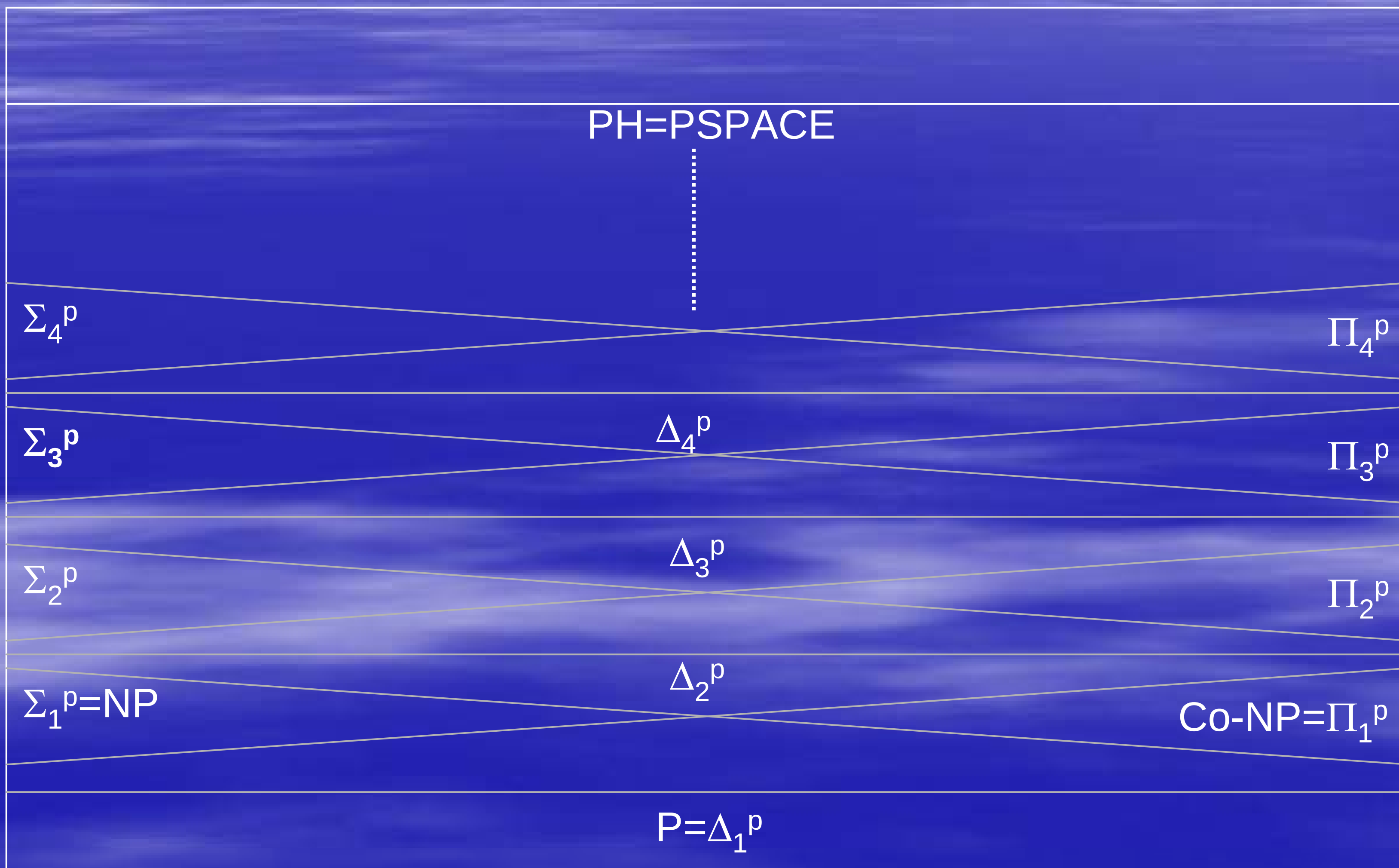
Properties of the Hierarchy



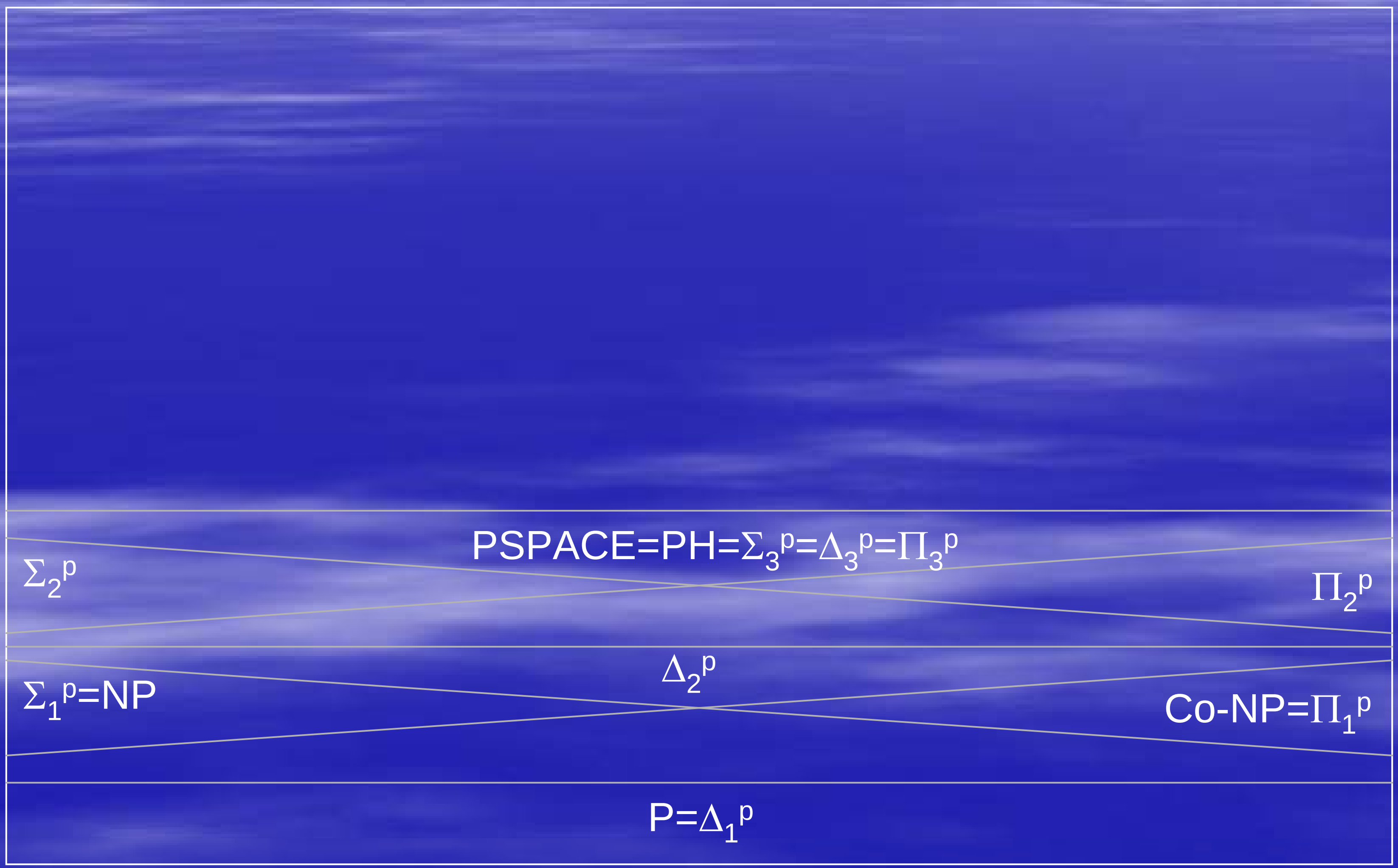
Properties of the Hierarchy



Properties of the Hierarchy



Properties of the Hierarchy



Quantifier Characterization

A language L is in Σ_3^P if for all x in Σ^*

x is in L $\Leftrightarrow \exists u\ \forall v\ \exists w\ P(x,u,v,w)$

A language L is in Π_3^P if for all x in Σ^*

x is in L $\Leftrightarrow \forall u\ \exists v\ \forall w\ P(x,u,v,w)$

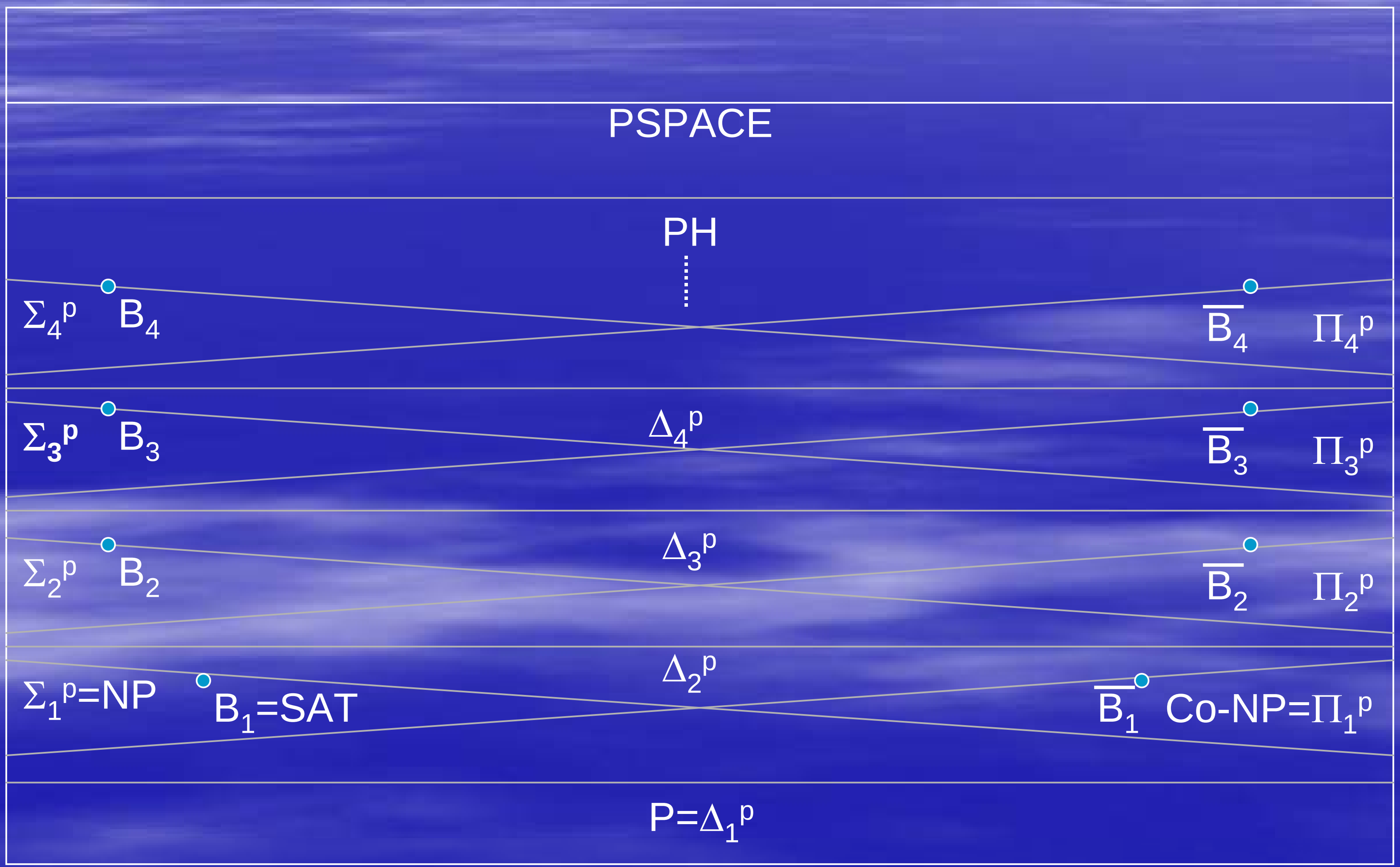
Complete Sets

- We define B_3 by the set of true quantified formula of the form

$$\exists x_1 \exists x_2 \cdots \exists x_n \forall y_1 \cdots \forall y_n \exists z_1 \cdots \exists z_n$$

$$\varphi(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n)$$

Complete Sets in the Hierarchy



Natural Complete Sets

- N-INEQ – Inequivalence of Integer Expressions with union and addition.

$$(50+(40\cup 20\cup 15))\cup((2\cup 5)+(7\cup 9))$$

- Meyer-Stockmeyer 1973 Stockmeyer 1977
  - N-INEQ is Σ_2^p-complete
- Umans 1999
  - Succinct Set Cover is Σ_2^p-complete
- Schafer 1999
  - Succinct VC Dimension is Σ_3^p-complete

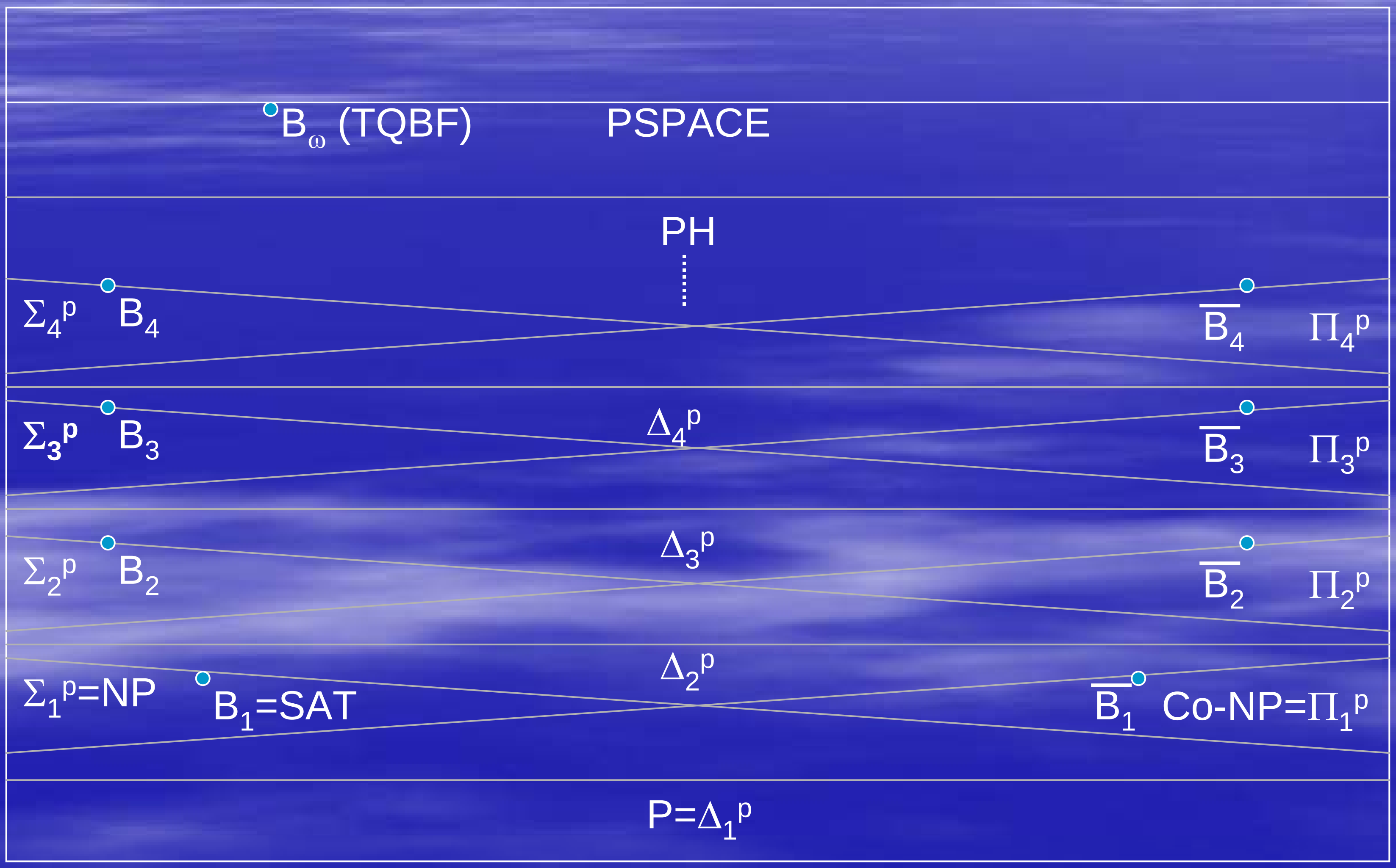
The ω-jump of the Hierarchy

- Meyer-Stockmeyer 1973, Stockmeyer 1977

$$B_\omega = \cup B_k$$

- Quantified Boolean Formula with an unbounded number of alterations.
- Now called QBF or TQBF.

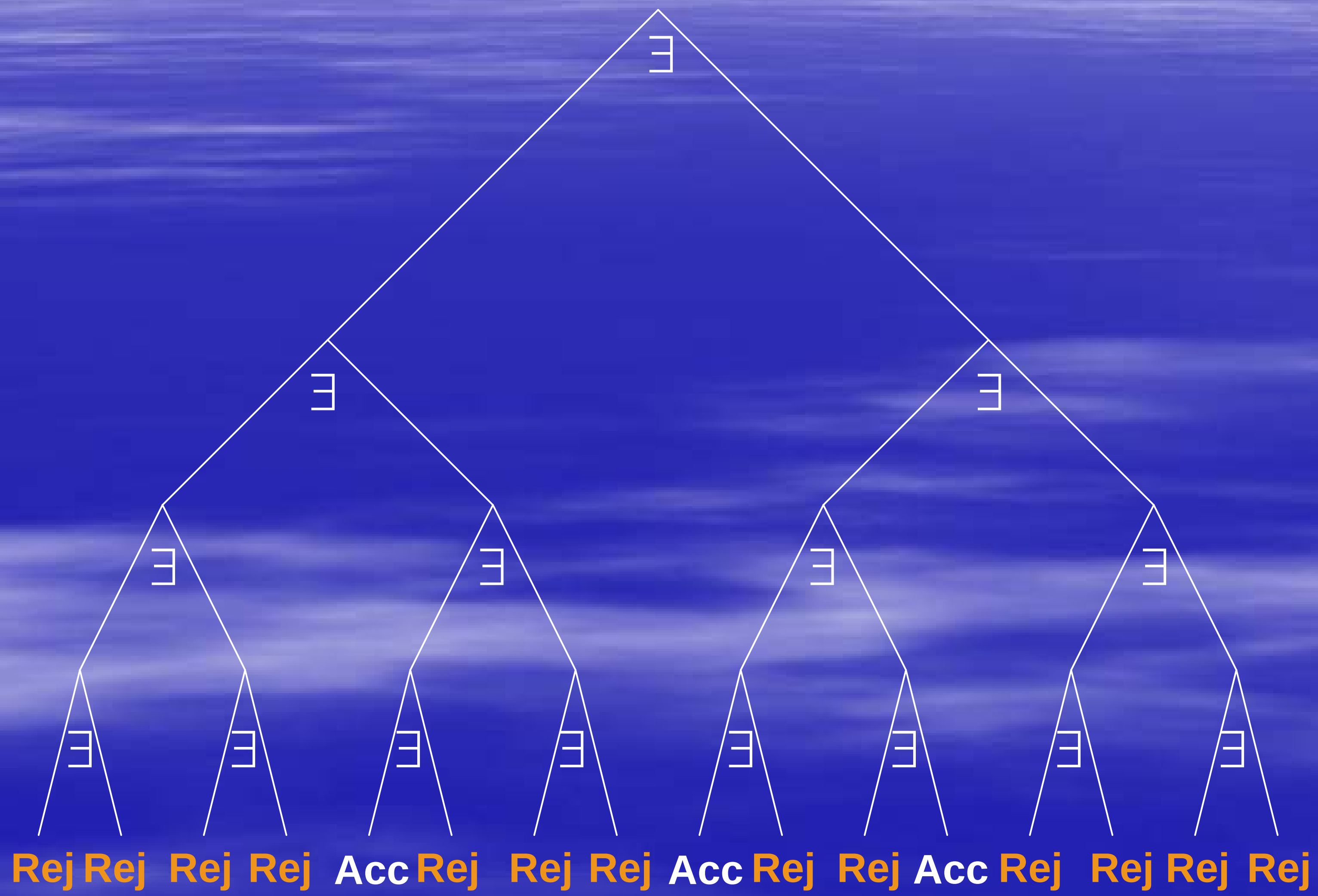
Complexity of ω-jump



Alternation

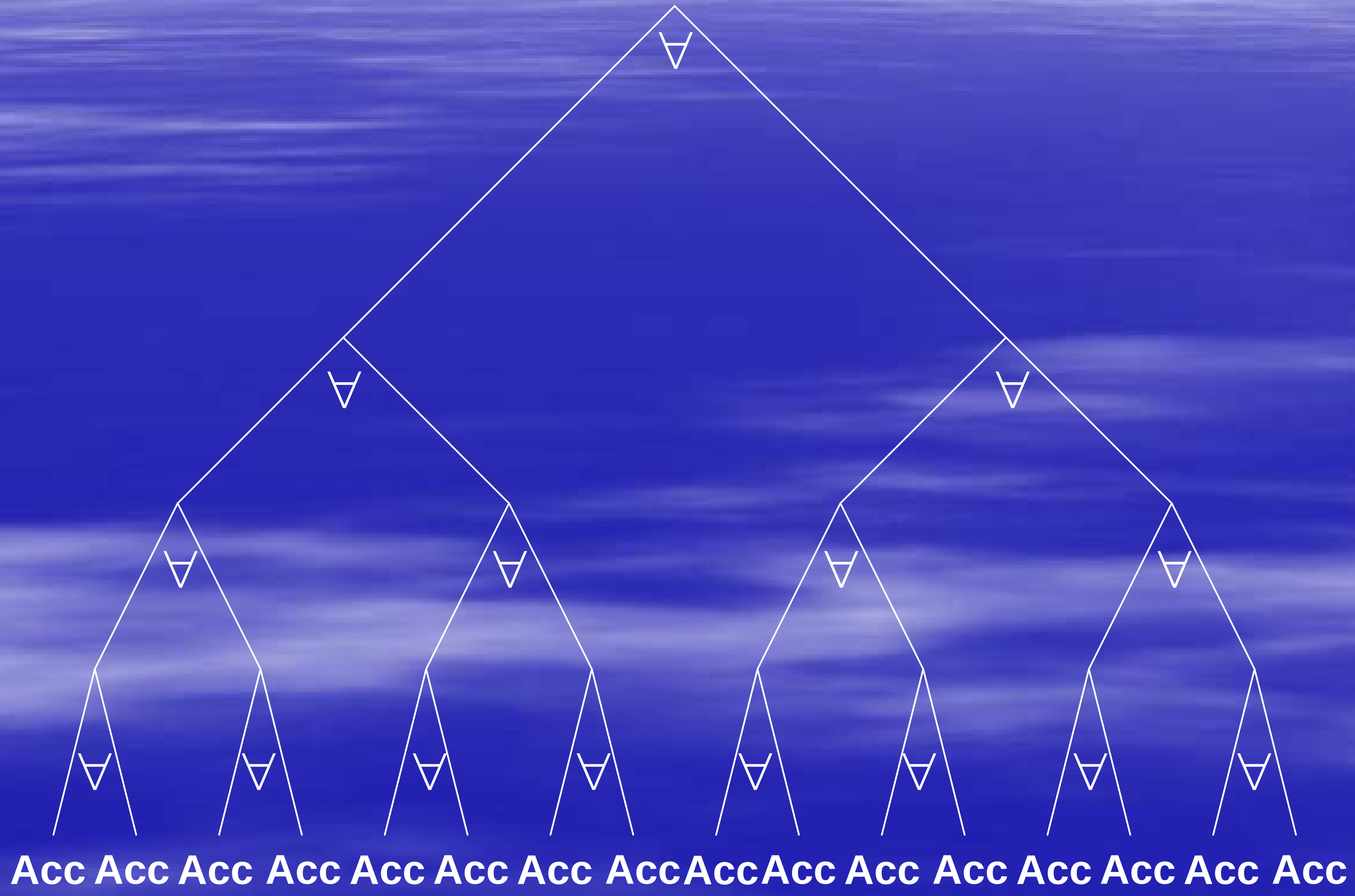
- Chandra-Kozen-Stockmeyer JACM 1981
- Chandra-Stockmeyer STOC 1976
- Kozen FOCS 1976

Alternation

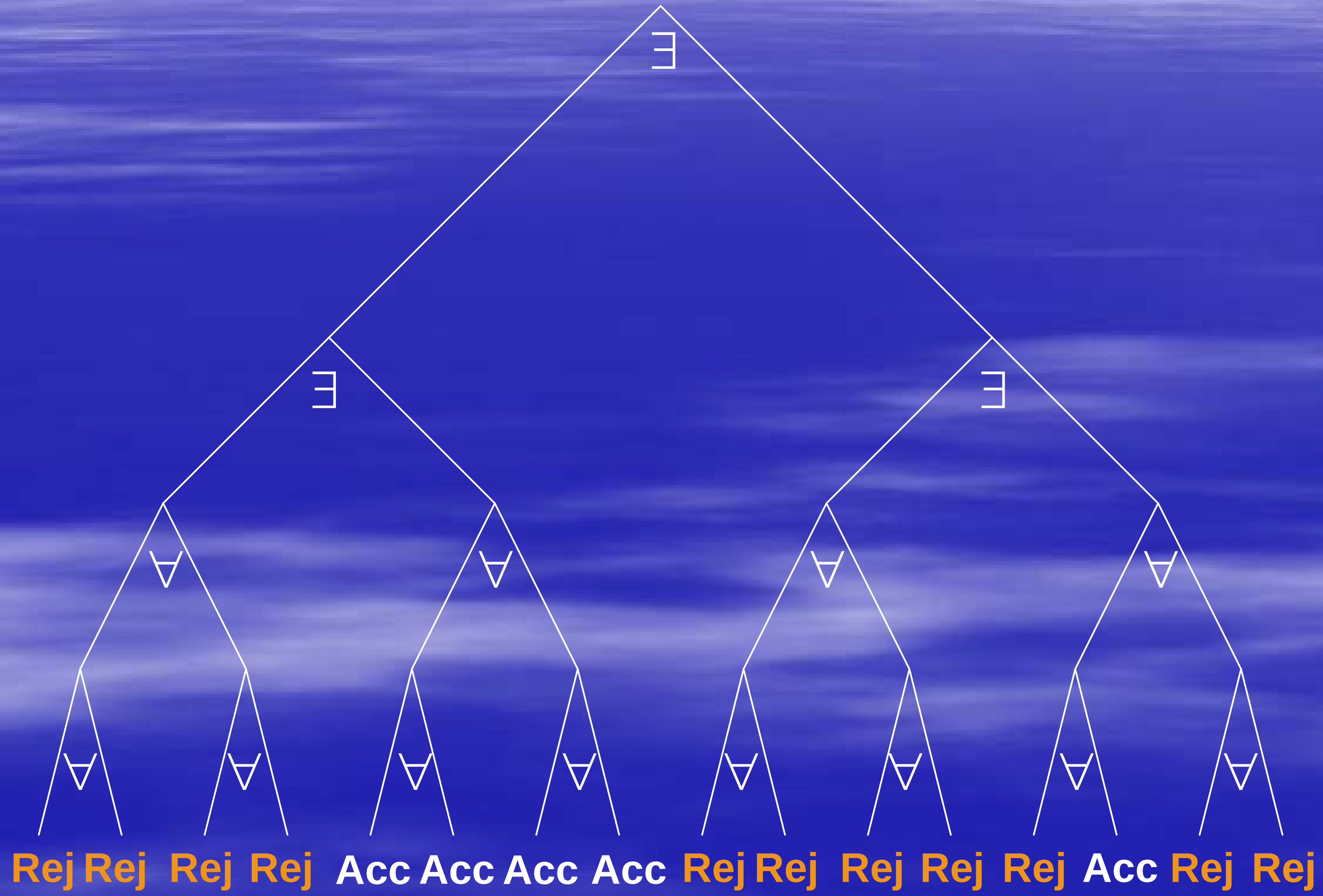


Alternation

Alternation



Alternation

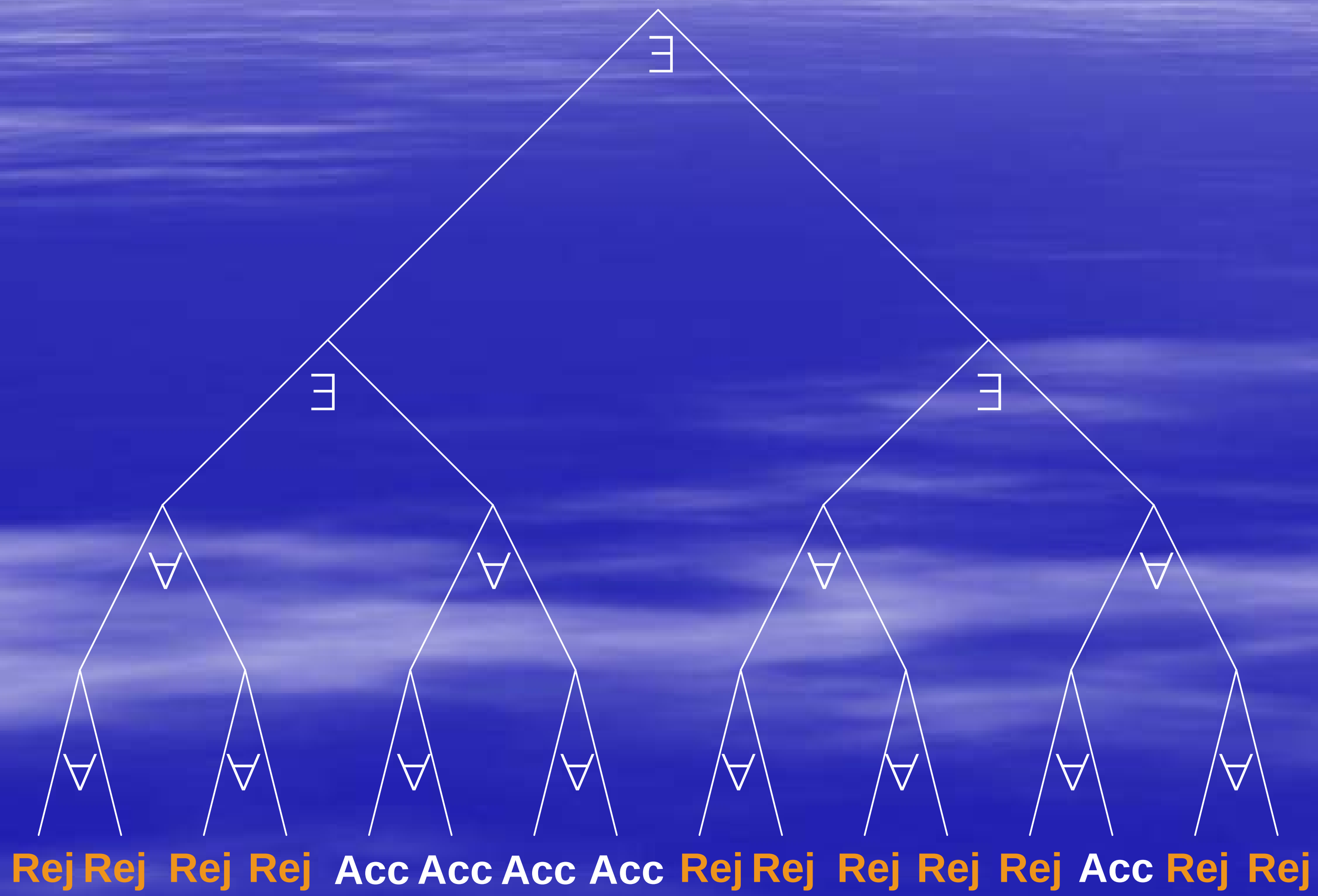


Alternation Theorems

- Chandra-Kozen-Stockmeyer
- $\mathrm{ATIME}(t(n)) \subseteq \mathrm{DSPACE}(t(n))$
- $\mathrm{NSPACE}(s(n)) \subseteq \mathrm{ATIME}(s^2(n))$
- $\mathrm{ASPACE}(s(n)) = \cup \mathrm{DTIME}(c^{s(n)})$

$$\begin{array}{ccccccccc} \mathrm{L} & \subseteq & \mathrm{P} & \subseteq & \mathrm{PSPACE} & \subseteq & \mathrm{EXP} & \subseteq & \mathrm{EXPSPACE} \subseteq \ldots \\ \| & & \| & & \| & & \| & & \\ \mathrm{AL} & \subseteq & \mathrm{AP} & \subseteq & \mathrm{APSPACE} & \subseteq & \mathrm{AEXP} & \subseteq & \ldots \end{array}$$

Alternate Characterization of Σ_2^p

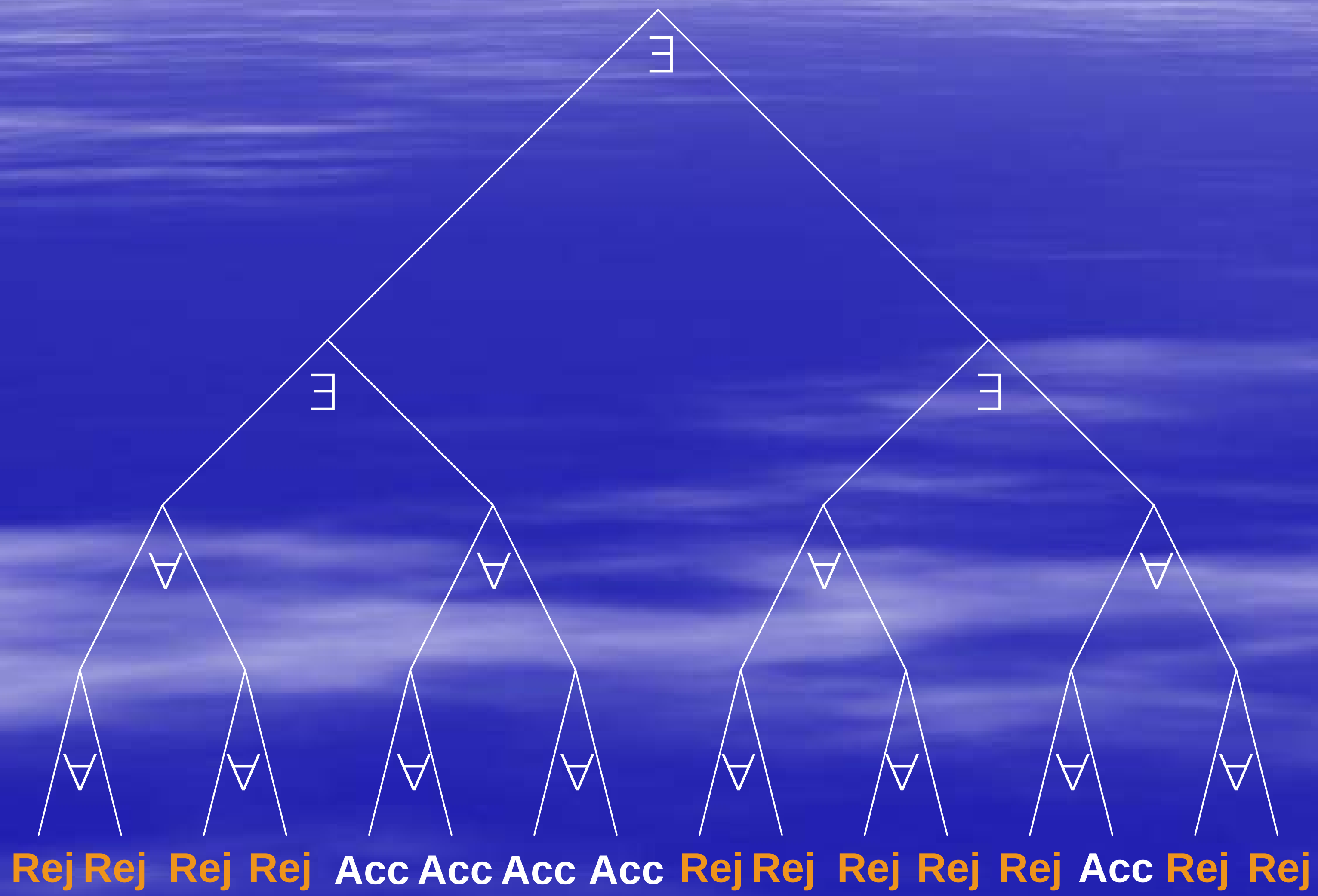


Other Alternating Models

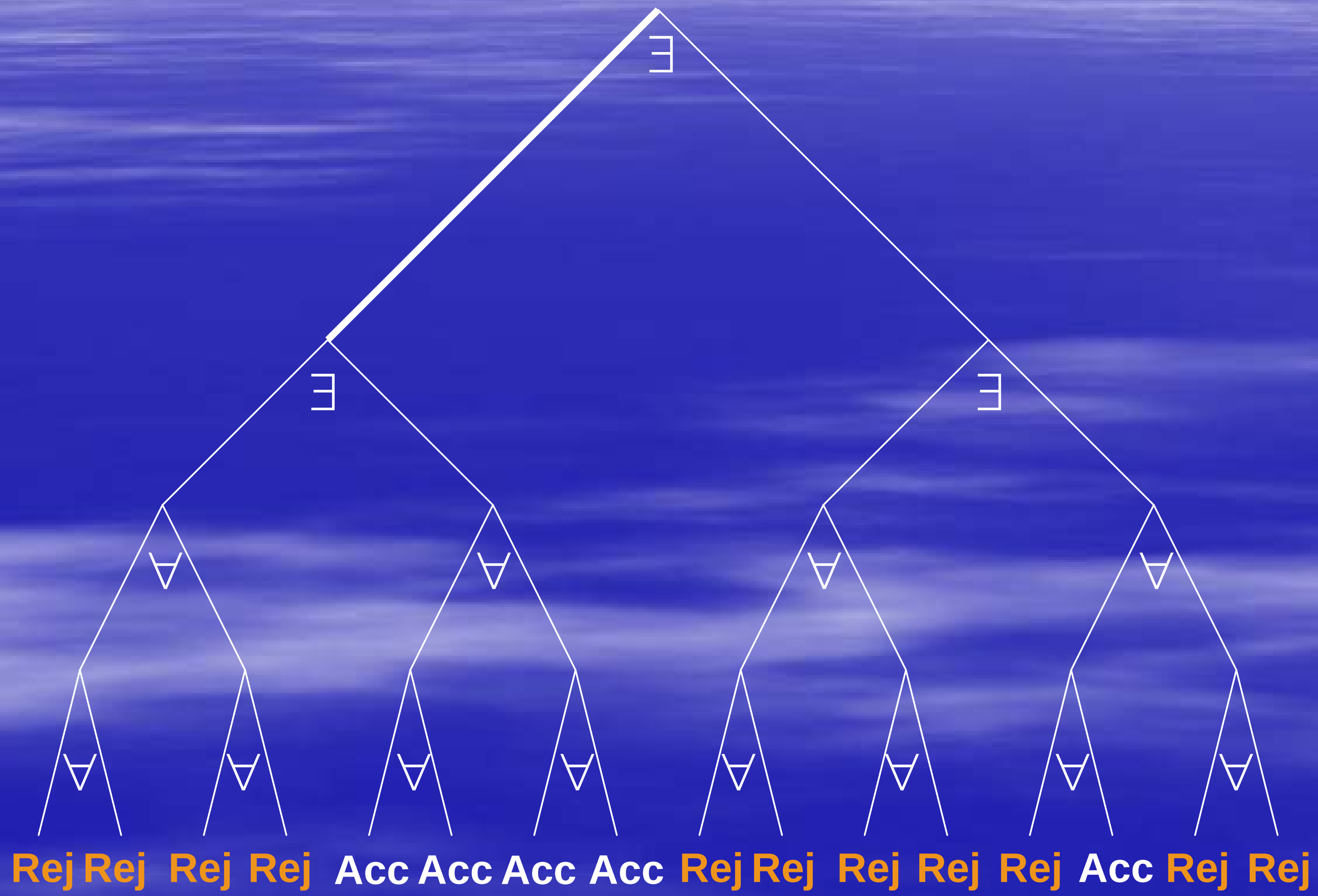
Chandra-Kozen-Stockmeyer 1981

- Log-Space Hierarchy
  – Collapses to NL (Immerman-Szelepcsényi ’88)
- Alternating Finite State Automaton
  – Same power as DFA but doubly exponential blowup in states.
- Alternating Push-Down Automaton
  – Accepts exactly E=DTIME($2^{O(n)}$)
  – Strictly stronger than PDAs
  – Inclusion due to Ladner-Lipton-Stockmeyer ’78

Alternation as a Game

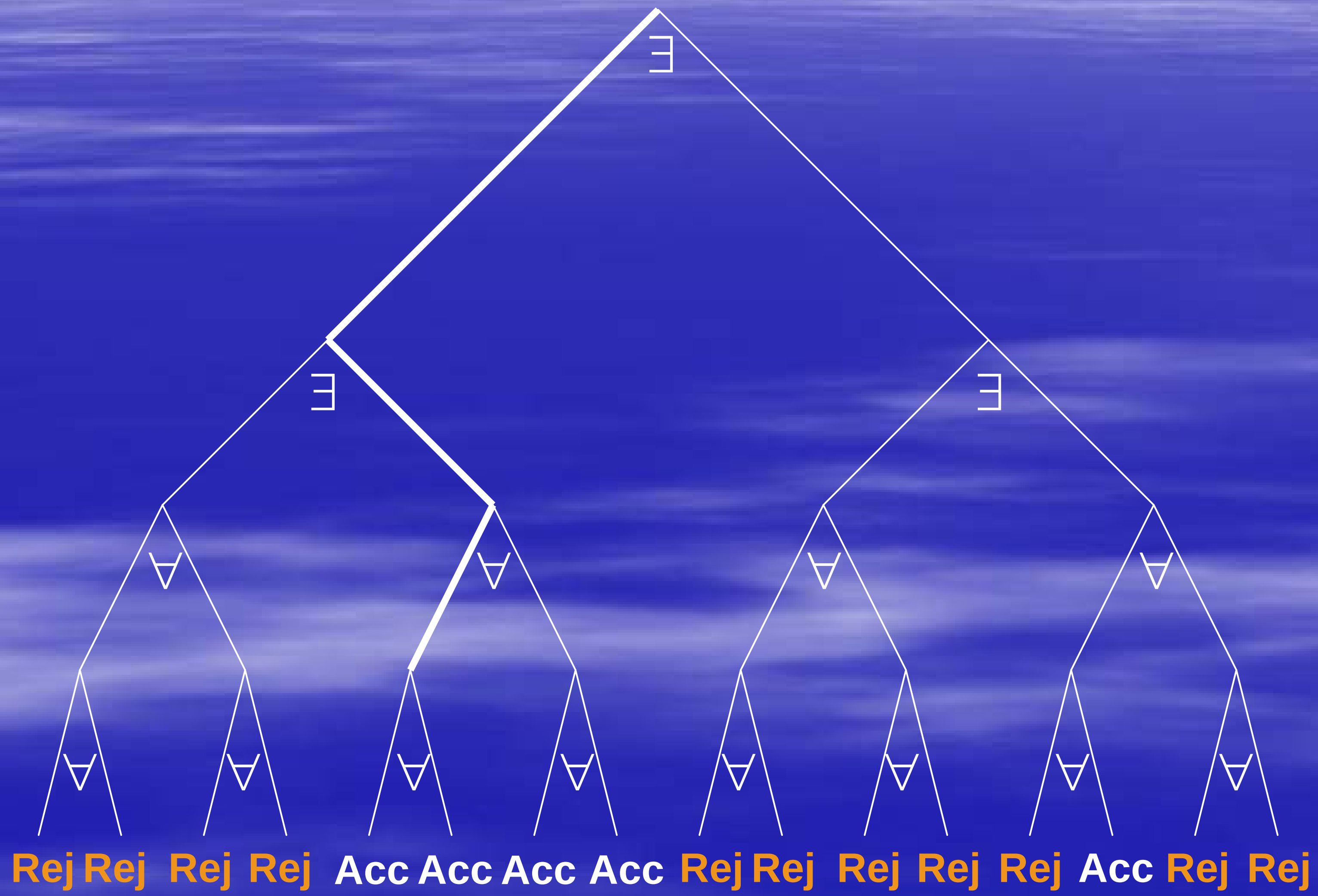


Alternation as a Game

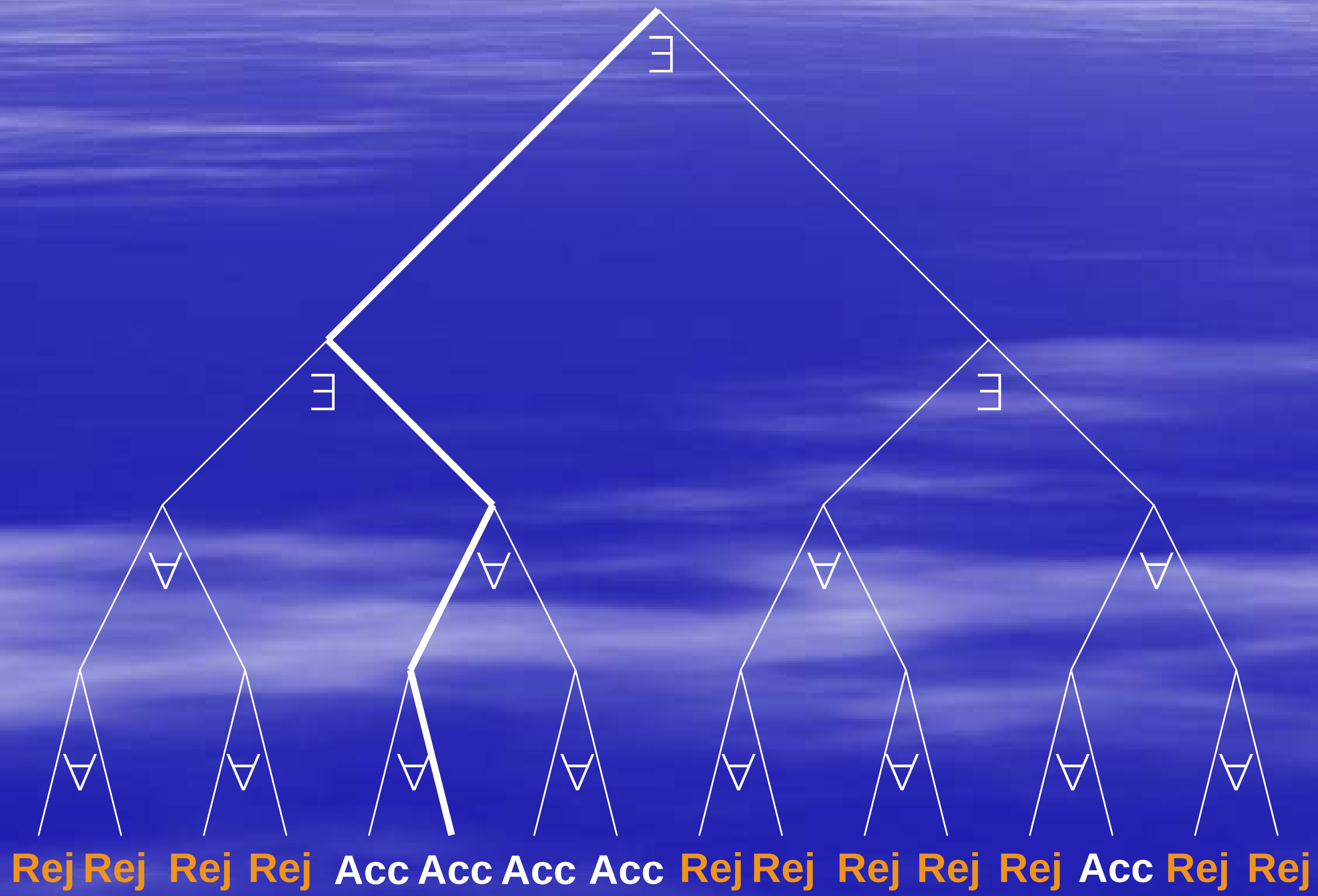


Alternation as a Game

Alternation as a Game



Alternation as a Game

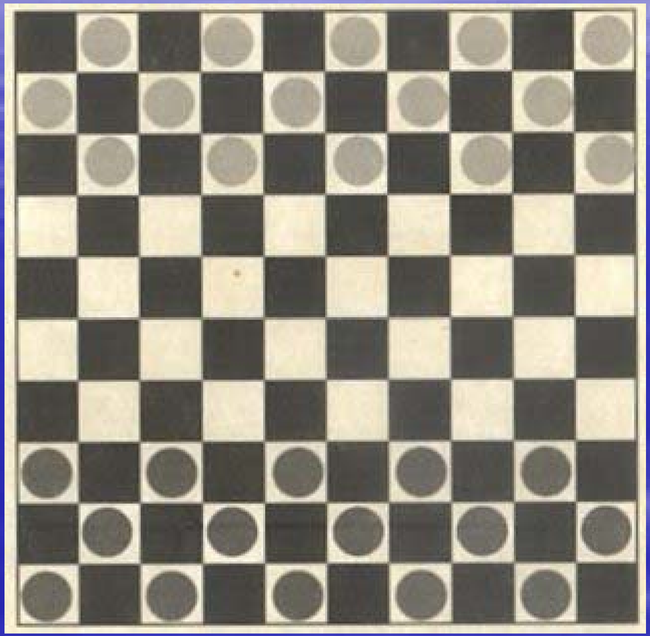


Complete Sets Via Games

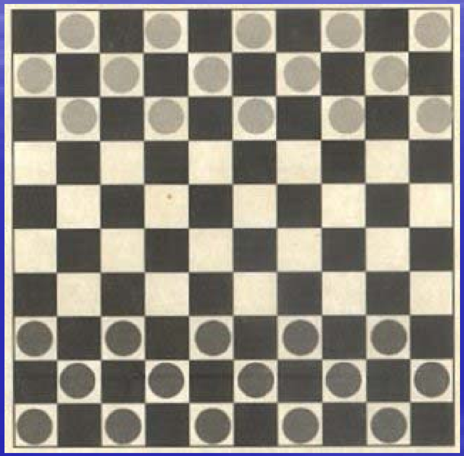
- Stockmeyer-Chandra 1979
- Can use problems based on games to get completeness results for PSPACE and EXP.
- Create a combinatorial game that is EXP-complete and thus not decidable in P.
- First complete sets for PSPACE and EXP not based on machines or logic.

Checkers

Generalized Checkers



Generalized Checkers

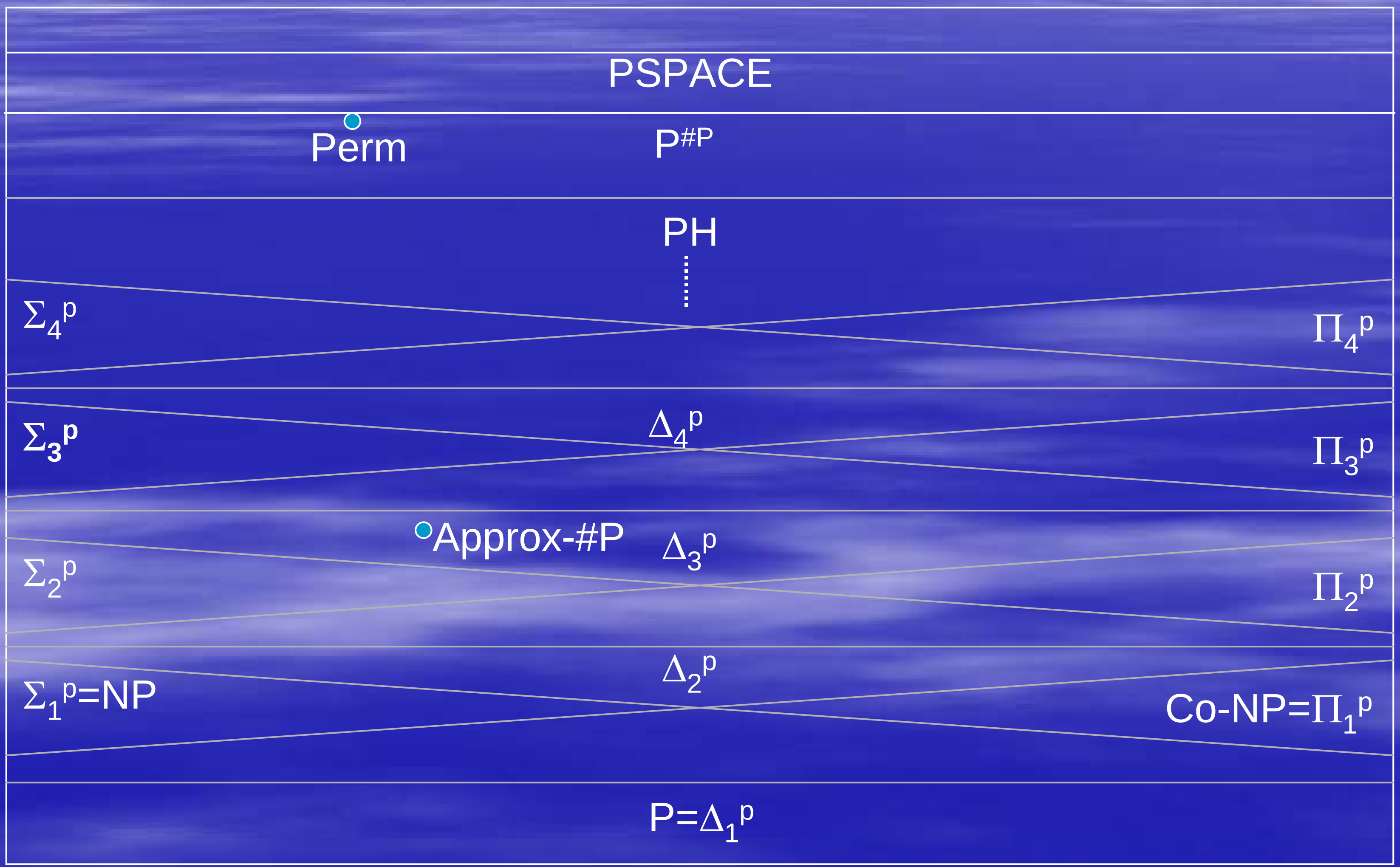


- PSPACE-hard
  - Fraenkel et al. 1978
- EXP-complete
  - Robson 1984

Approximate Couting

- #P – Valiant 1979
  - Functions that count solutions of NP problems.
  - Permanent is #P-complete
- Stockmeyer 1985 building on Sipser 1983
  - Can approximate any #P function f in polytime with an oracle for Σ_2^p.
- Toda 1991
  - Every language in PH reducible to #P

Complexity of #P



Legacy of Larry Stockmeyer

- Circuit Complexity
- Infinite Hierarchy Conjecture
- Probabilistic Computation
- Interactive Proof Systems

Circuit Complexity

- Baker-Gill-Solovay ’75: Relativization Paper
  - Open: Is PH infinite relative to an oracle?
- Sipser ’83: Strong lower bounds on depth d circuits simulating depth d+1 circuits.
- Yao ’85: “Separating the Polynomial-Time Hierarchy by Oracles”
- Led to future circuit results by Håstad, Razborov, Smolensky and many others.

Infinite Hierarchy Conjecture

- Is the Polynomial-Time Hierarchy Infinite?
- Best Evidence: Yao's result shows alternating log-time hierarchy infinite.
- Many complexity results
  - If PROP then the polynomial-time hierarchy collapses.
  - If PH is infinite then NOT PROP.
- Gives evidence for NOT PROP.

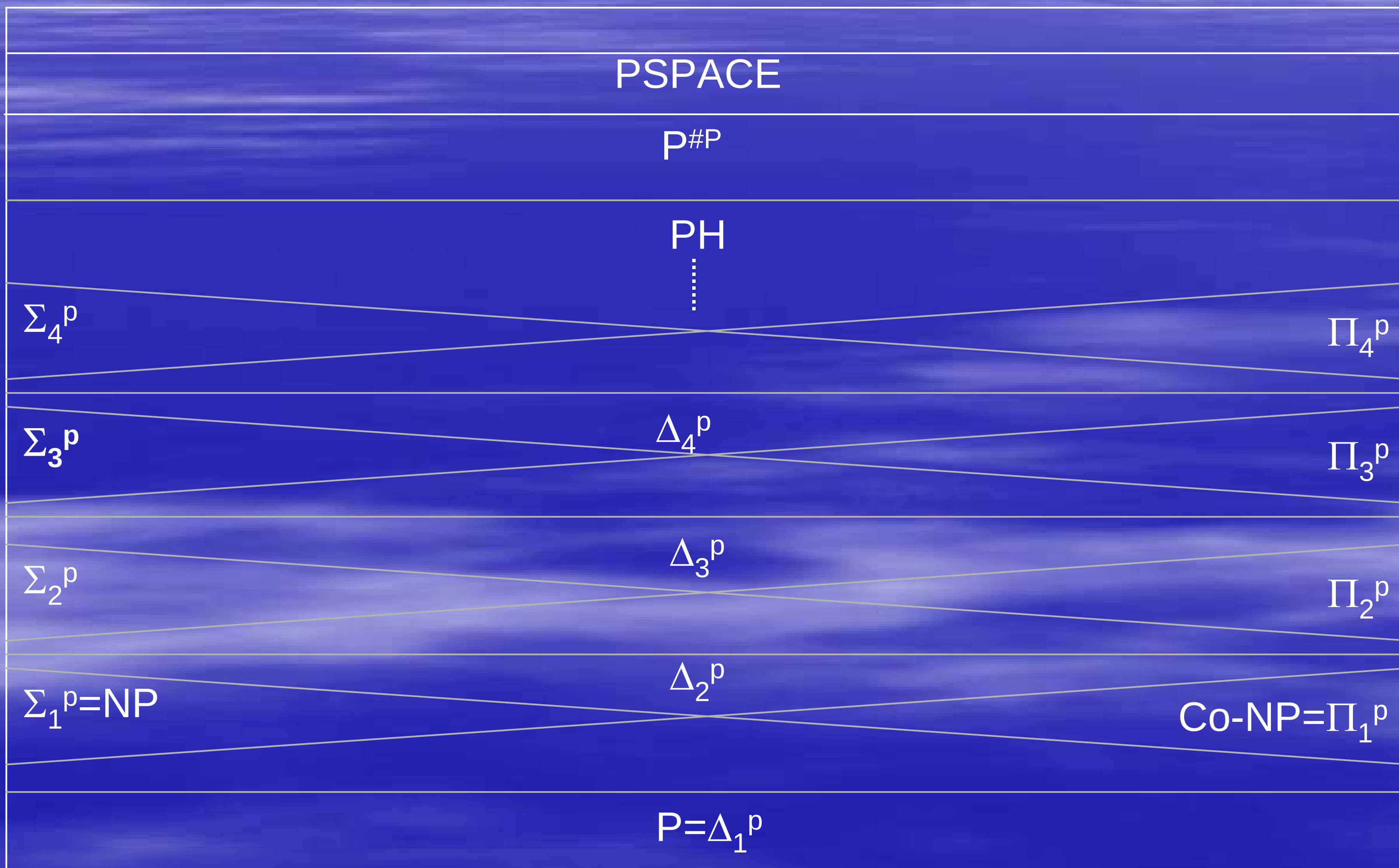
If Hierarchy is Infinite …

- SAT does not have small circuits.
  - Karp-Lipton 1980
- Graph isomorphism is not NP-complete.
  - Goldreich-Micali-Wigderson 1991
  - Goldwasser-Sipser 1989
  - Boppana-Håstad-Zachos 1987
- Boolean hierarchy is infinite.
  - Kadin 1988

Boolean Hierarchy

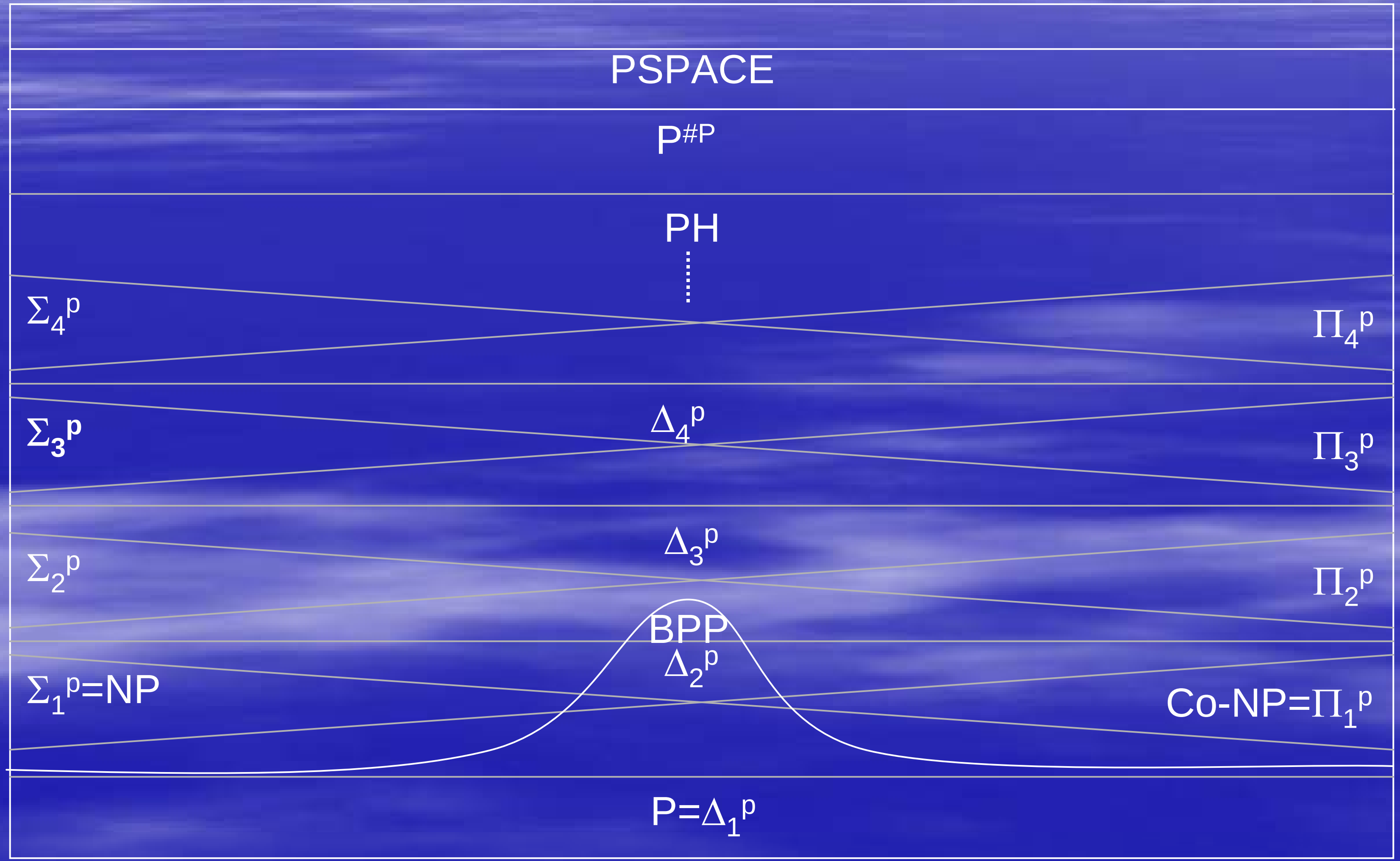
- BH_1 = NP
- BH_{k+1} = { B-C | B in NP and C in BH_k}
- { (G,k) | Max clique of G has size k} in BH_2
- Kadin: If $BH_k=BH_{k+1}$ then $PH=\Sigma_3^p$.

Probabilistic Computation



Probabilistic Computation

Sipser-Gács-Lautemann 1983

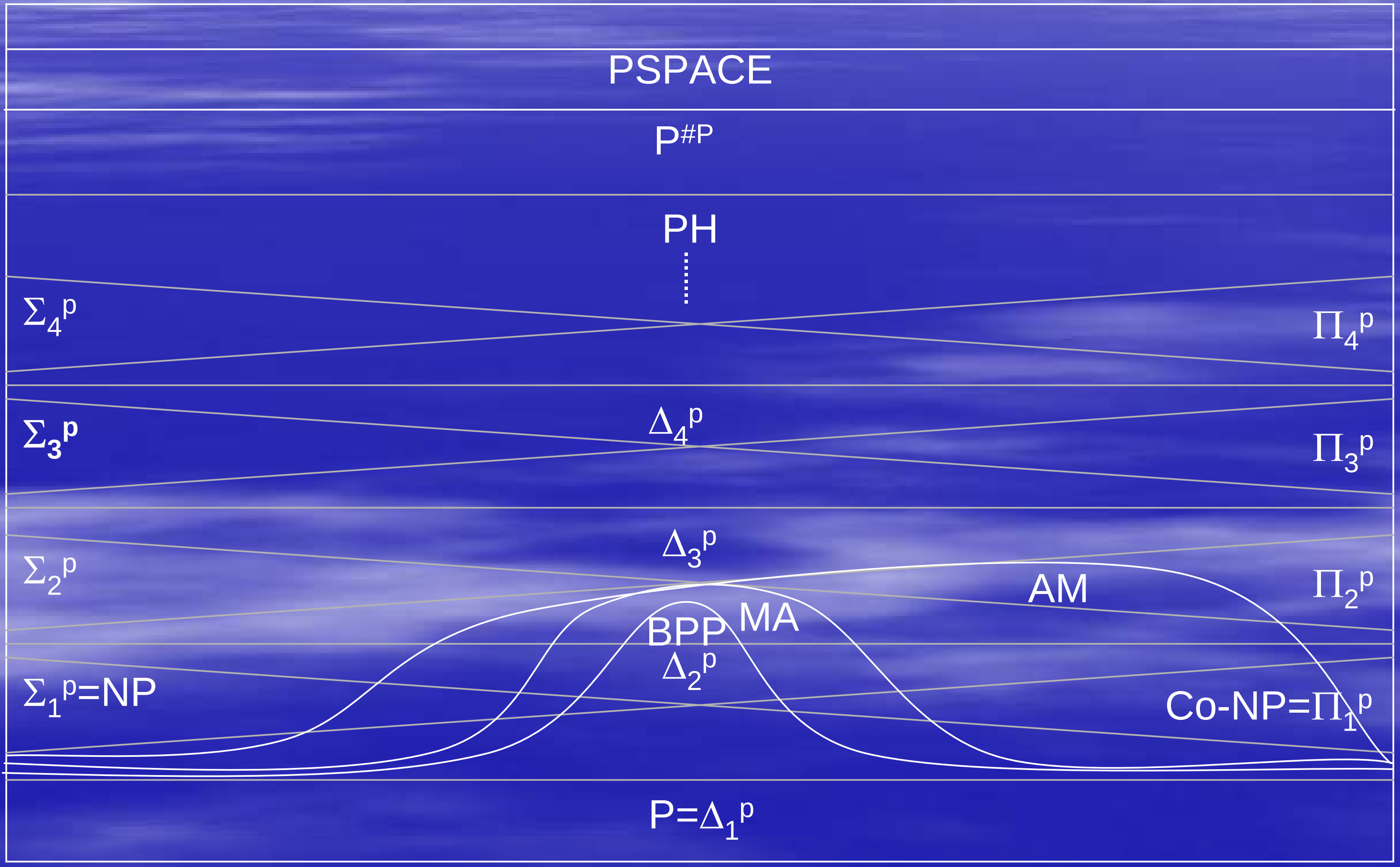


Interactive Proof Systems

- Papadimitriou 1985 – Alternation between nondeterministic and probabilistic players
- Interactive Proof Systems
  – Public Coin: Babai-Moran 1988
  – Private Coin: Goldwasser-Micali-Rackoff 1989
  – Equivalent: Goldwasser-Sipser 1989

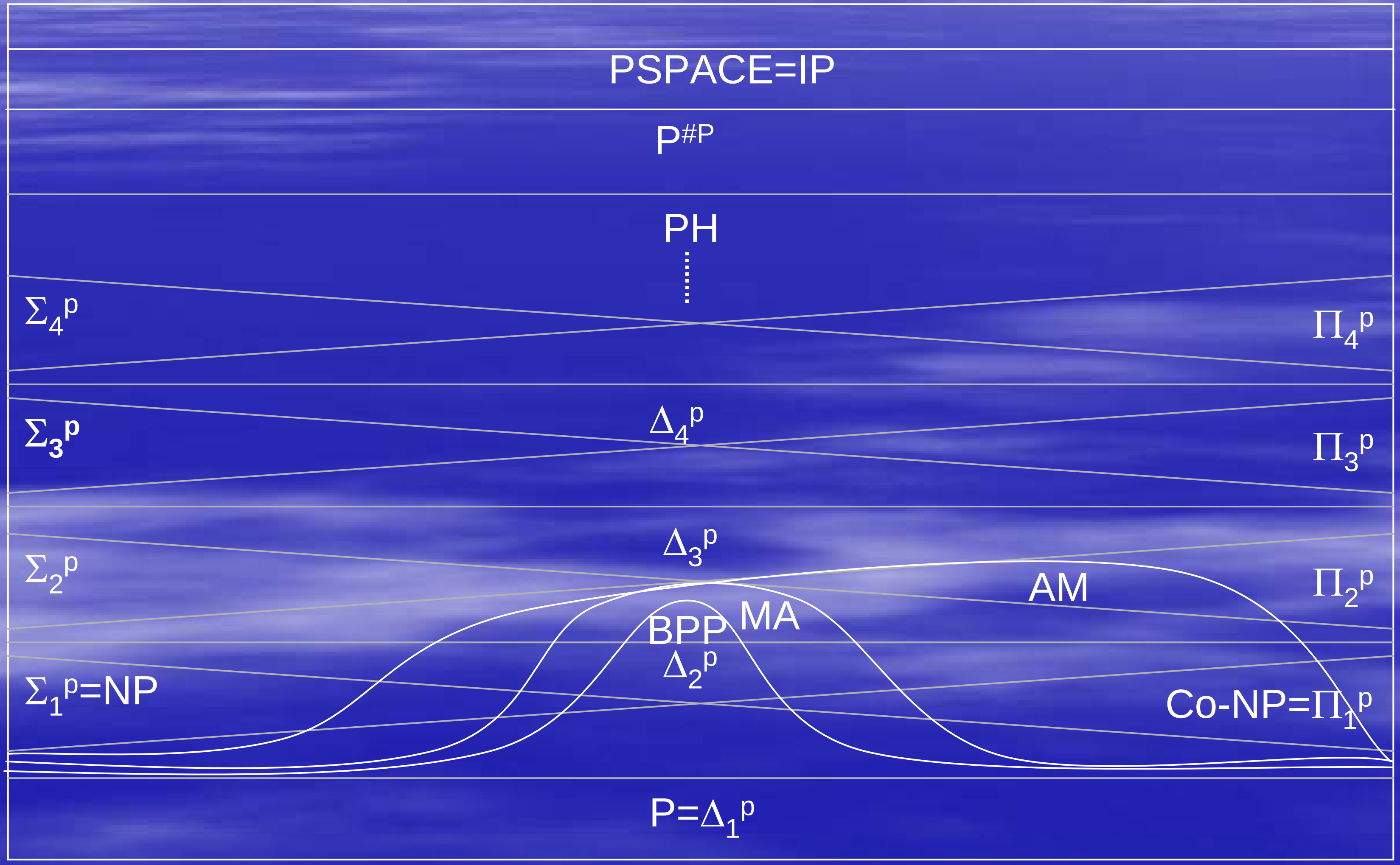
Interactive Proof Systems

Babai-Moran 1988



Interactive Proof Systems

LFKN, Shamir 1992



Interactive Proof Systems

- Hardness of Approximation
  - Feige-Goldwasser-Lovász-Safra-Szegedy 1996
- Probabilistically Checkable Proofs
  - NP in PCPs with O(log n) coins and constant number of queries.
  - Arora-Lund-Motwani-Sudan-Szegedy 1998
- Interactive Proofs with Finite State Verifiers
  - Dwork and Stockmeyer

Other Work

- Larry Stockmeyer contributed much more to complexity and important work in other areas including automata theory and parallel and distributed computing.
- Most Cited Article (CiteSeer):
  - Dwork, Lynch, and Stockmeyer, "Consensus in the presence of partial synchrony" JACM, 1988.

Conclusion

- What natural problems can’t we compute?
- Led to exciting work on polynomial-time hierarchy, alternation, approximation and much more.
- These idea affect much of computational complexity today and the legacy will continue for generations in the future.

Remembering

- Other members of our community that we have recently lost…

George Dantzig

Shimon Even

Seymour Ginsburg

Frank Harary

Leonid Khachiyan

Clemens Lautemann

Carl Smith

Larry Stockmeyer