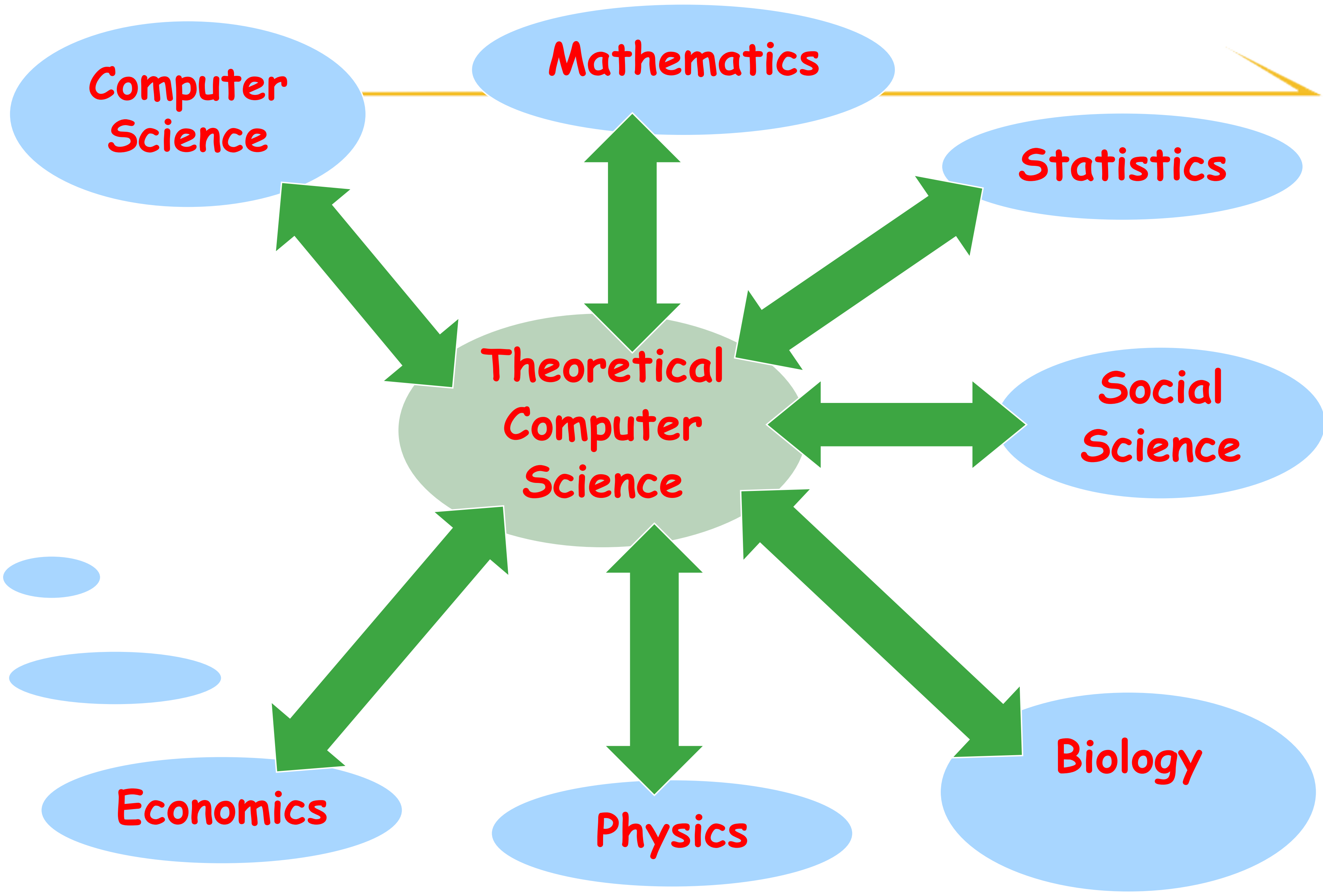
+ insights

Structure in TCS

Theoretical Computer Science

Avi Wigderson

IAS, Princeton


Computer Science
Mathematics
Statistics
Theoretical Computer Science
Social Science
Economics
Physics
Biology

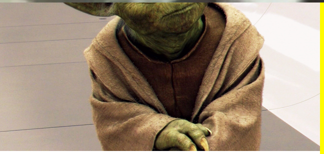
SIMONS INSTITUTE
FOR THE THEORY OF COMPUTING

CALVIN HALL

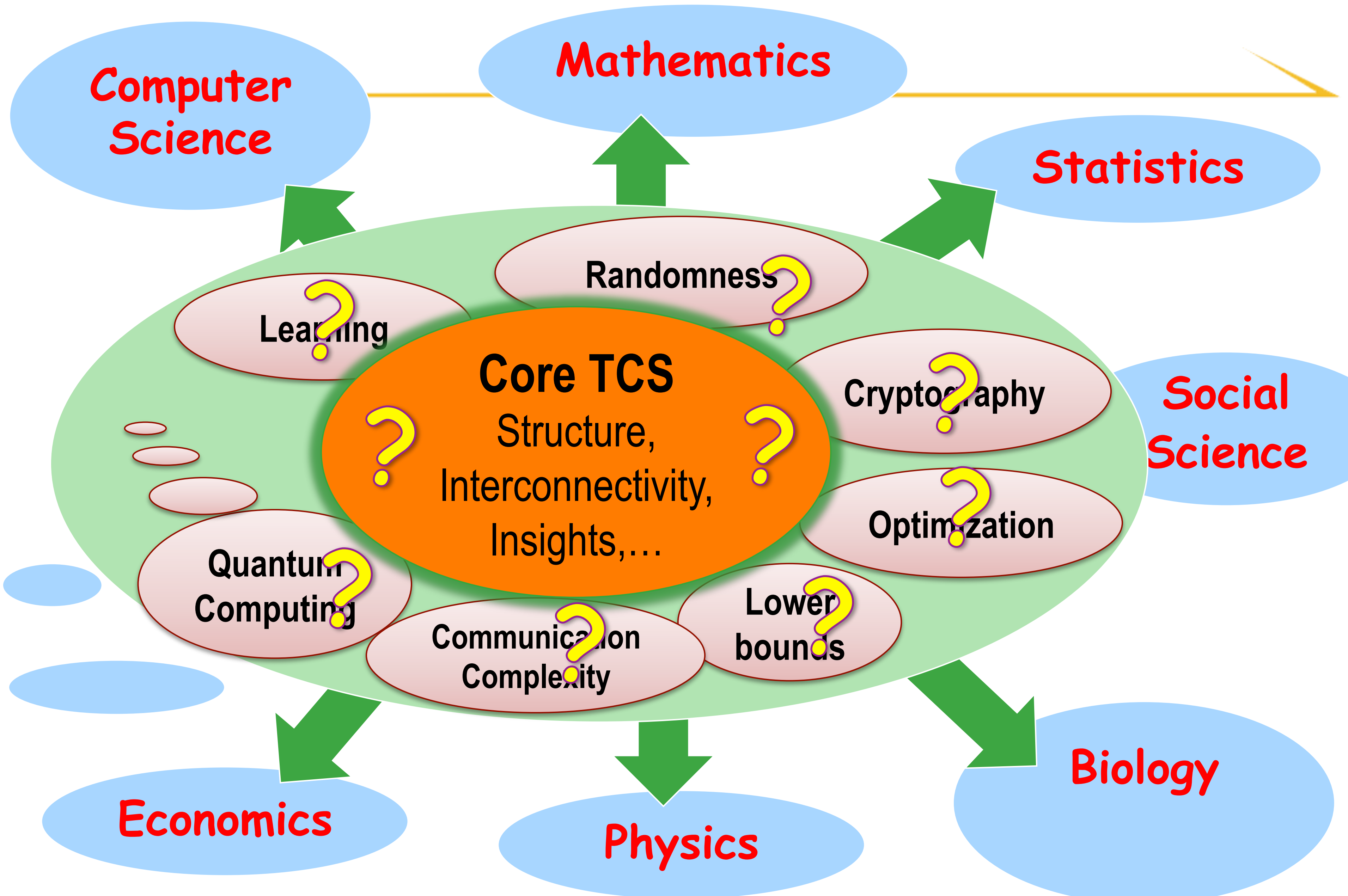
SIMONS INSTITUTE
FOR THE THEORY OF COMPUTING

Lobby

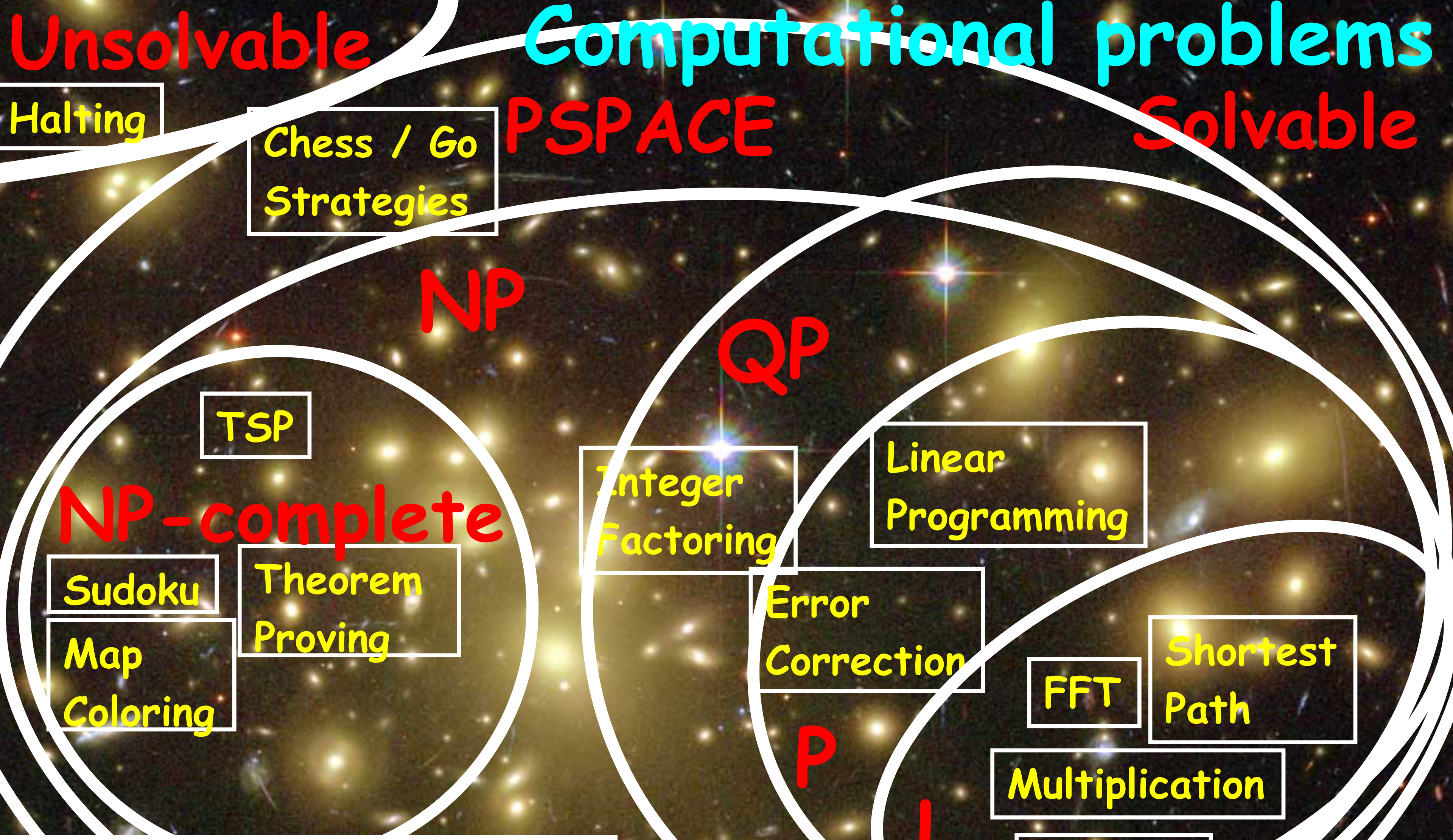
SIMONS INSTITUTE



SCIENCES … IS SOMETHING WE DO UNDERSTAND”
(AT LEAST FOR THE INFORMATION PROCESSES)



Computer Science
Mathematics
Statistics
Social Science
Biology
Physics
Economics
Randomness
Learning
Cryptography
Optimization
Lower bounds
Communication Complexity
Quantum Computing
Core TCS
Structure, Interconnectivity, Insights,…



1000s problems
Few complexity classes
Algorithms, Analysis,
Reductions, Completeness

Cryptographic problems:

-Privacy

-Resilience

Oblivious computation

Poker over telephone

Joint coin flipping

Secret Communication

Public-key encryption

Key exchange

Cryptomania

Commitment schemes

Trap-door Function

Private-key encryption

Minicrypt

One-way Function

Zero-knowledge proofs

Digital Signatures

Pseudorandom generation

1000s problems
Few complexity classes
Algorithms, Analysis
Reductions, Completeness

High level Structure in

- Optimization problems
- Approximation problems
- Cryptographic problems
- Probabilistic algorithms
- Lower bounds

Origins

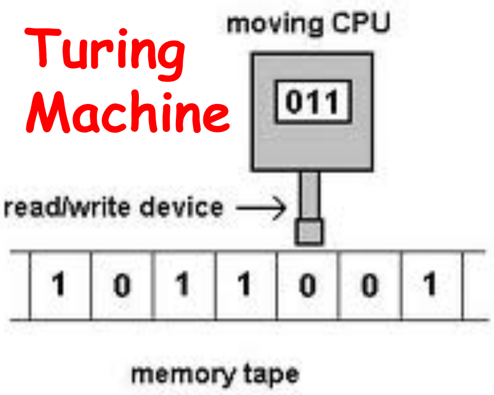
Birth of TCS

[Turing 1936]: "On computable numbers, with an application to the entscheidungsproblem"

Formal definition of computer & algorithm

The amazing power of a good theory

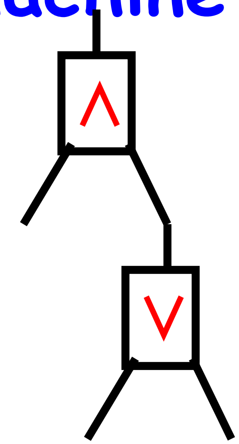
Turing Machine

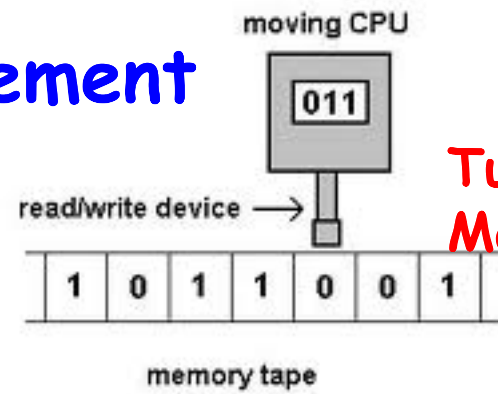


- Seed of the computer revolution
- The power of computing: Church-Turing Thesis
- The limits on of algorithms

Technology
Computer Revolution

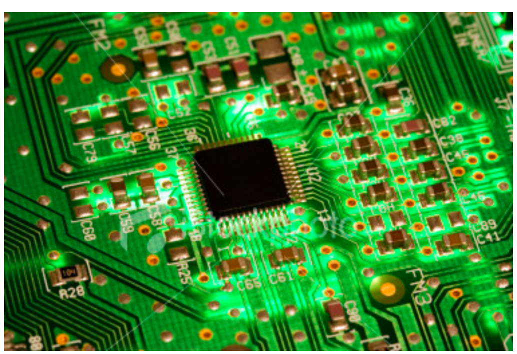
A Turing machine is easy to implement

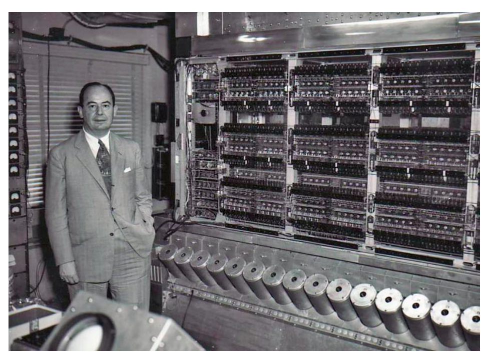




Turing
Machine

Simple
Local





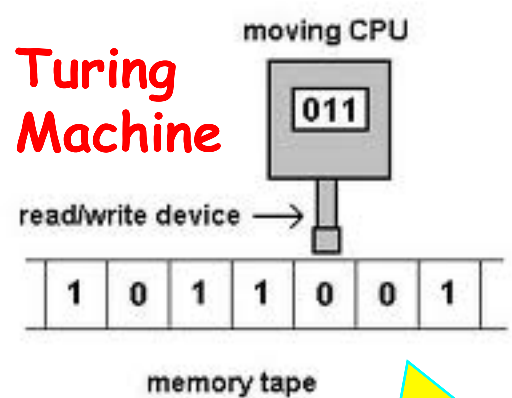
Science
Church-Turing Thesis

Turing machine can emulate any computation!

Computation: every process which is a sequence of *simple*, *local* steps. on

bits in computers
neurons in the brain
atoms in matter
cells in living tissue
individuals in populations

Turing Machine



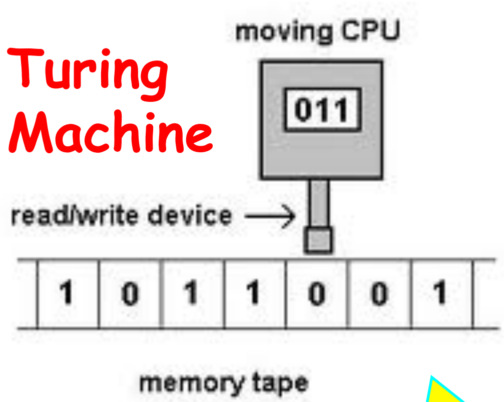
Simple
Local

Math
Theory

A Turing machine is a formal model
- basic step
- basic memory unit

Can prove theorems:
- analyze algorithms
- prove limits

Turing Machine



Simple
Local

Limits of computation

Unsolvable

CS [Turing]: Given a computer program, does it always halt?

Logic[Turing]: Given a statement, is it provable

Math [Mattiasevich]: Given an equation, does it have integer solutions?

Biology [Conway]: Given A rule for an epidemic, will it spread or die?

Solvable

I' m late

When?

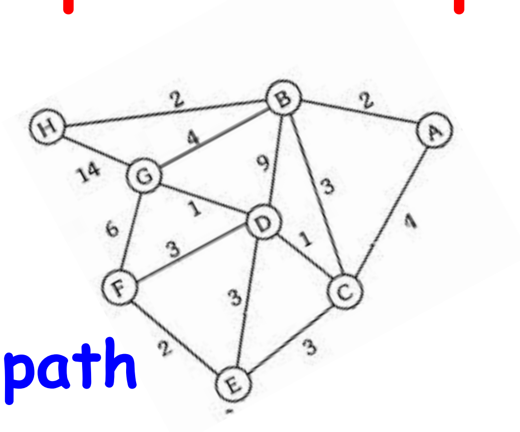
Computational Complexity Theory

Structure in decision, search, optimization problems

+ crash course on complexity & Classical reductions

Easy and Hard Problems

asymptotic complexity of functions



2-COL

Shortest path

2-SAT $(\underline{x}_2 \vee x_4)\ (x_5 \vee x_n)$…

Multiplication 23x67 = ?

poly(n) steps algorithm

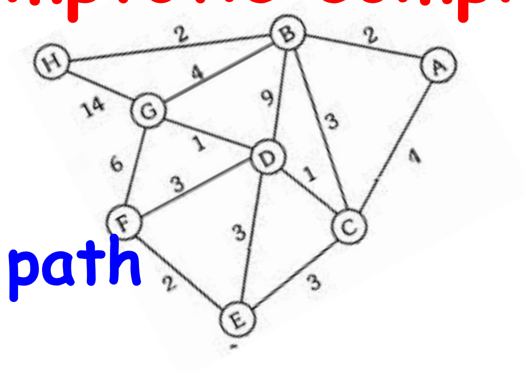
EASY P – Polynomial time

Asymptotics +
Worst case analysis
- Forward looking
- Reveal structure!

Robust
to model
variants

Easy and Hard Problems

asymptotic complexity of functions

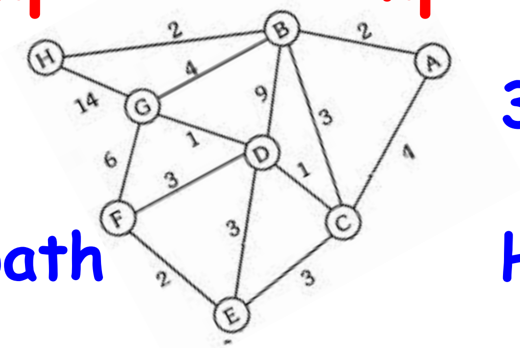


2-COL	3-COL
Shortest path	Hamilton path
2-SAT $(\underline{x}_2 \vee x_4)\ (x_5 \vee x_n)$…	3-SAT $(\underline{x}_1 \vee \underline{x}_2 \vee x_4)(x_5 \vee x_3 \vee x_n)$…
Multiplication 23x67 = ?	Factoring 1541 = ? x ?
poly(n) steps algorithm	best known alg exp(n) steps
EASY P – Polynomial time	HARD? we don't know!

P Polynomial – Possible, Practical, Pheasable
E Exponential – Extremely hard, Eempossible

Easy and Hard Problems

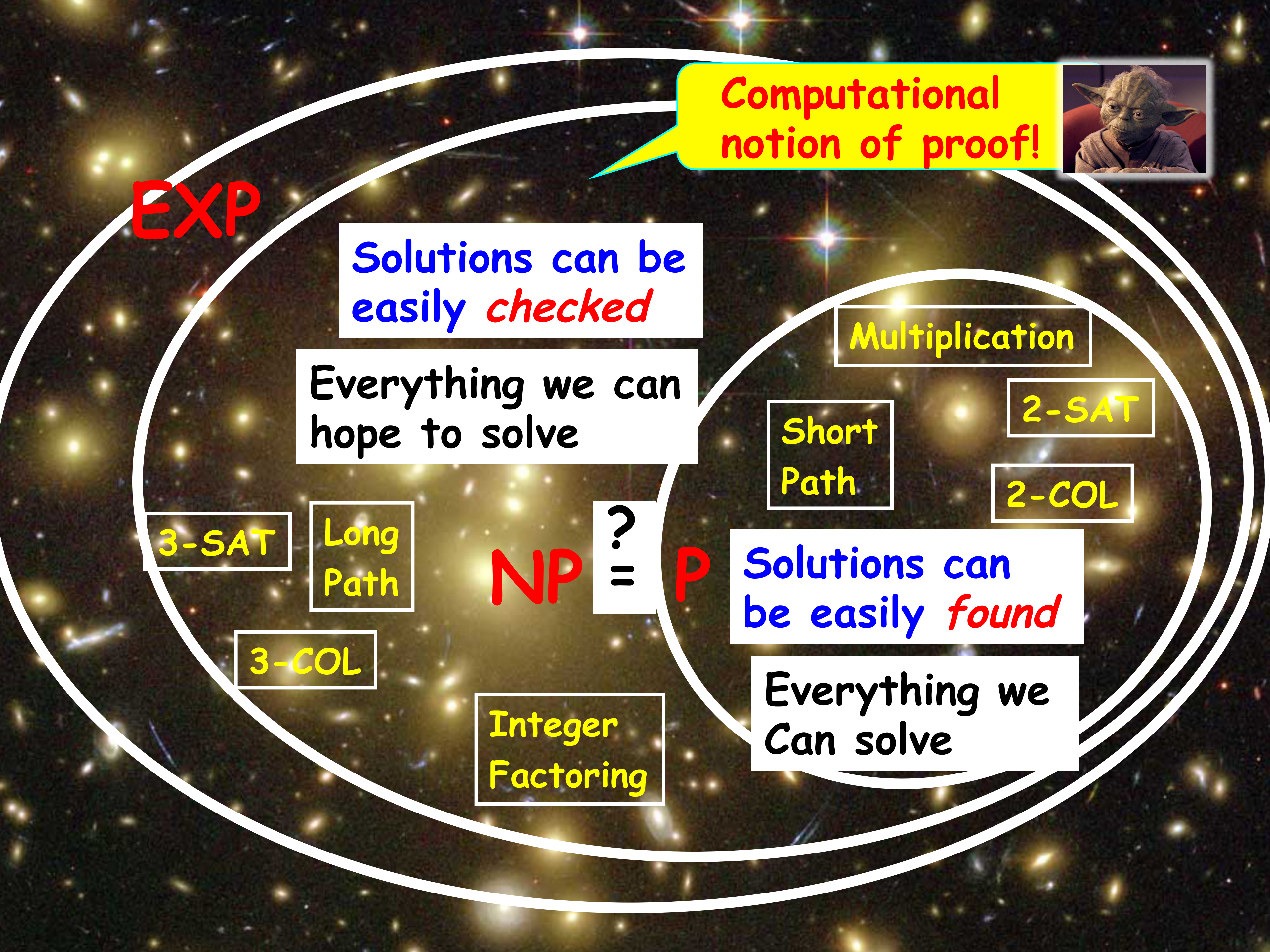
asymptotic complexity of functions



2-COL	3-COL
Shortest path	Hamilton path
2-SAT $(\underline{x}_2 \vee x_4)\ (x_5 \vee x_n)\ldots$	3-SAT $(\underline{x}_1 \vee \underline{x}_2 \vee x_4)(x_5 \vee x_3 \vee x_n)\ldots$
Multiplication 23x67 = ?	Factoring 1541 = ? x ?
poly(n) steps algorithm	best known alg exp(n) steps
EASY P - Polynomial time	HARD? we don't know!

Thm: If 3-COL is Easy then Factoring & 3-SAT are Easy

Something unites all problems we have seen so far


Computational notion of proof!
EXP
Solutions can be easily checked
Everything we can hope to solve
Multiplication
2-SAT
Short Path
2-COL
3-SAT
Long Path
NP ?= P
Solutions can be easily found
3-COL
Integer Factoring
Everything we Can solve

Miracle! One problem captures whole class!

NP-complete problems

[Cook, Levin'71] 3-SAT easy → P=NP

[Karp'72] 3-COL easy → 3-SAT easy

21 problems, network, logic, scheduling…

['00] Thousands across math & sciences

If one is easy, all are.

If one is hard, all are.

A universal phenomena

Why prove NP-completeness results?

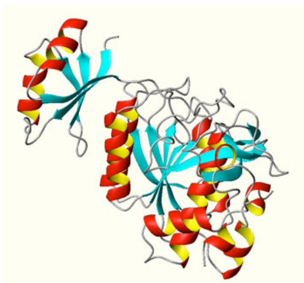
Programmers/CS – Hardness certificate

Mathematicians – Structural nastiness

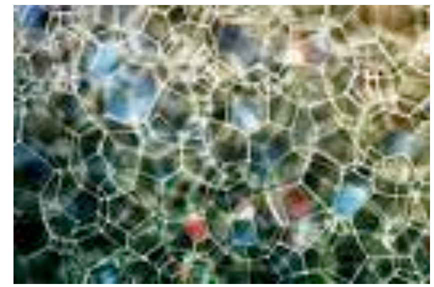
Scientists – Model validation / sanity check

NP-complete problems that "nature solves"

Biology: Minimum energy Protein Folding



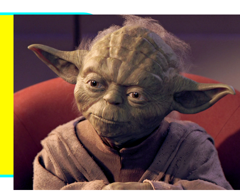
Physics: Minimum surface area Foam



Possibilities:

model is wrong or inputs are special or P=NP

Use P≠NP as a law of nature!



Add nature to laptop
Random, Quantum,…

Why are there so many?

[Karp '72] If 3-COL easy then 3-SAT easy

Locality of computation

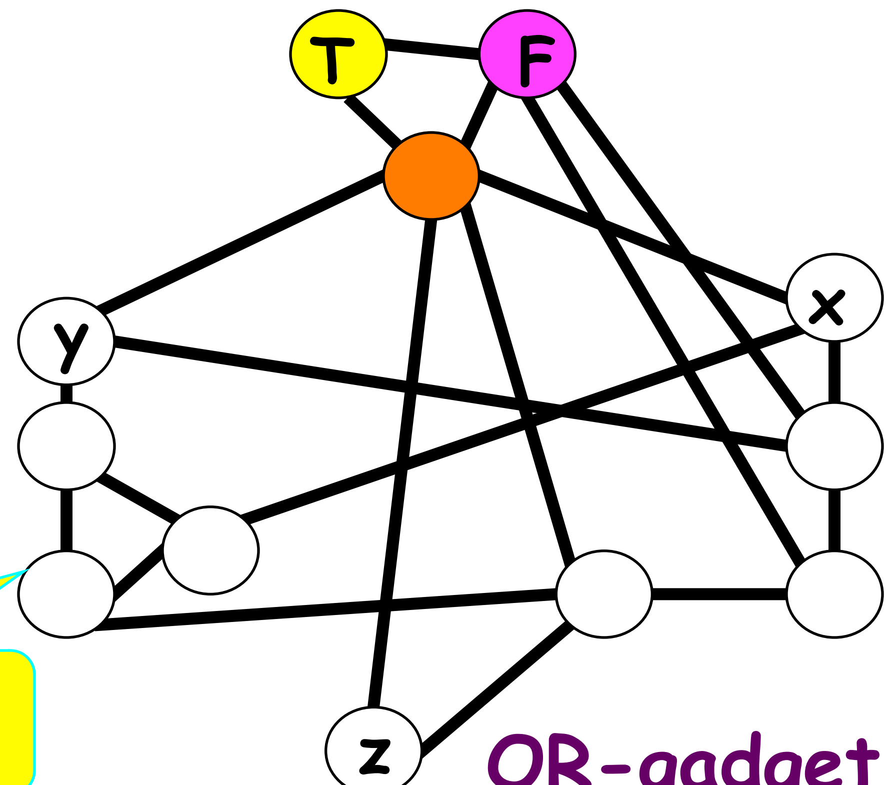
efficient algorithm

formula → graph

x ∨ y

satisfying ↔ legal

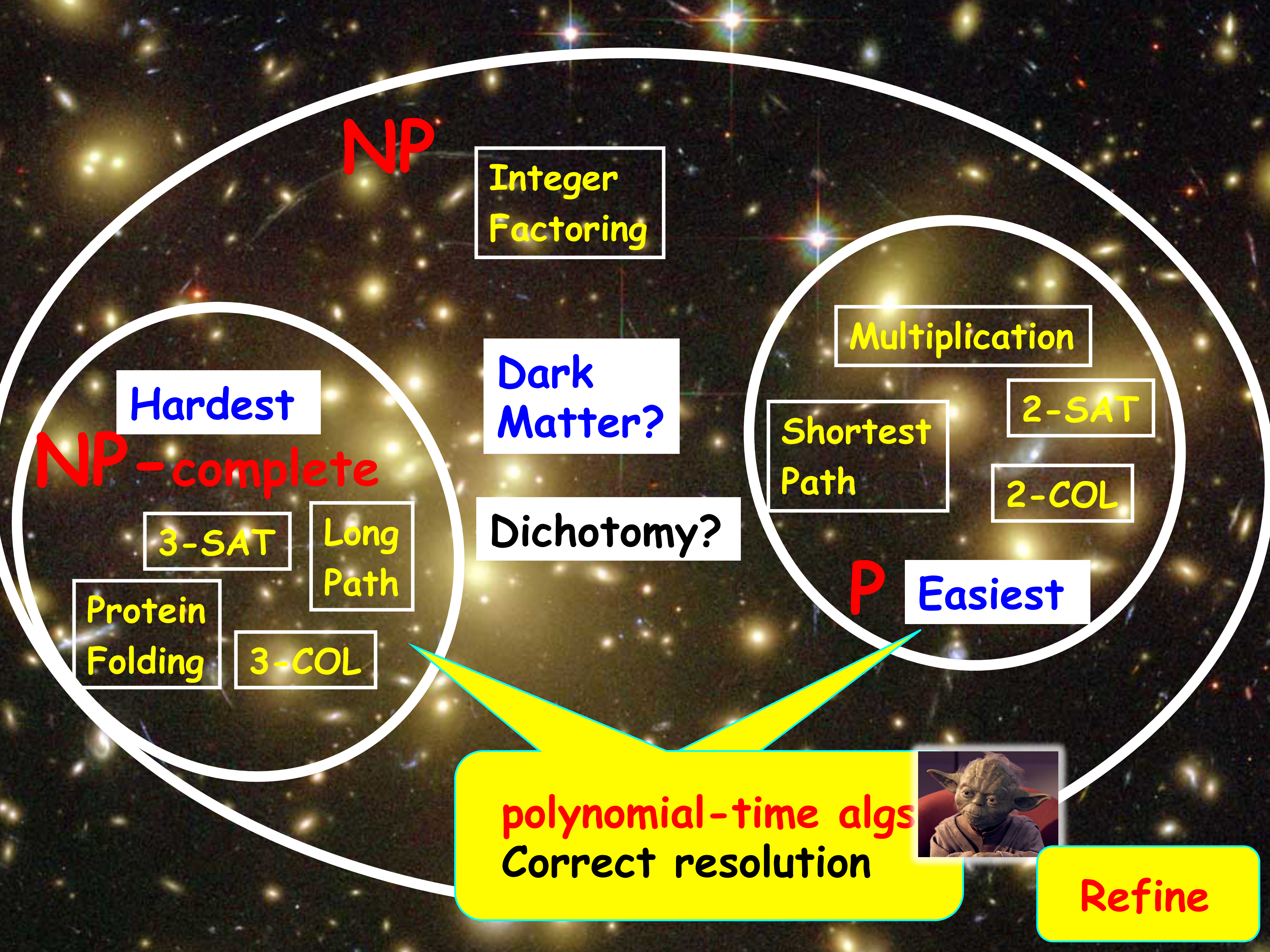
assignment coloring



Claim: In every legal 3-coloring, z = x ∨ y

OR-gadget

Many structures encode computation


NP
Integer Factoring
Multiplication
Hardest
NP-complete
Dark Matter?
2-SAT
Shortest Path
2-COL
3-SAT
Long Path
Dichotomy?
Protein Folding
3-COL
P
Easiest
polynomial-time algs
Correct resolution
Refine

Structure in approximation problems

(+ sophisticated reductions)

The mystery of approximation

1970s: Essentially all optimization problems are either in P or are NP-complete

Hard problems don't go away...

How well can we approximate the optimum?

3-SAT:	$\leq$ 8/7	Set Cover:	$\leq$ log n
TSP:	$\leq$ 3/2	3-COL:	$\leq n^{.4}$
Vertex Cover:	$\leq$ 2	Clique:	$\leq n/\log^2 n$

Are these good? Do better? Theory??

[Hastad'01] $8/7-\varepsilon$ is NP-complete for 3-SAT

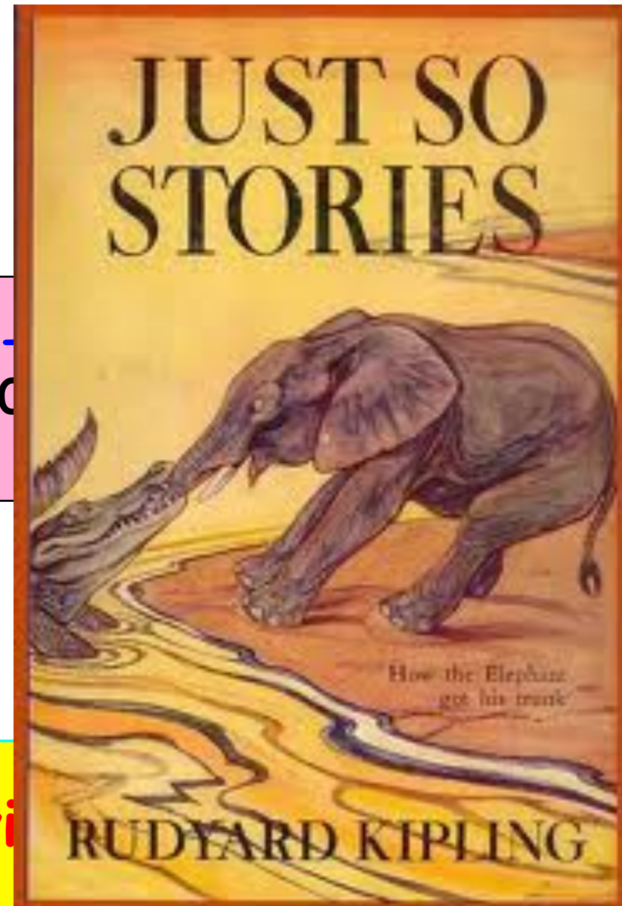
2010 2000 1990 1980 1970

3-SAT is
8/7-ε hard

Decade

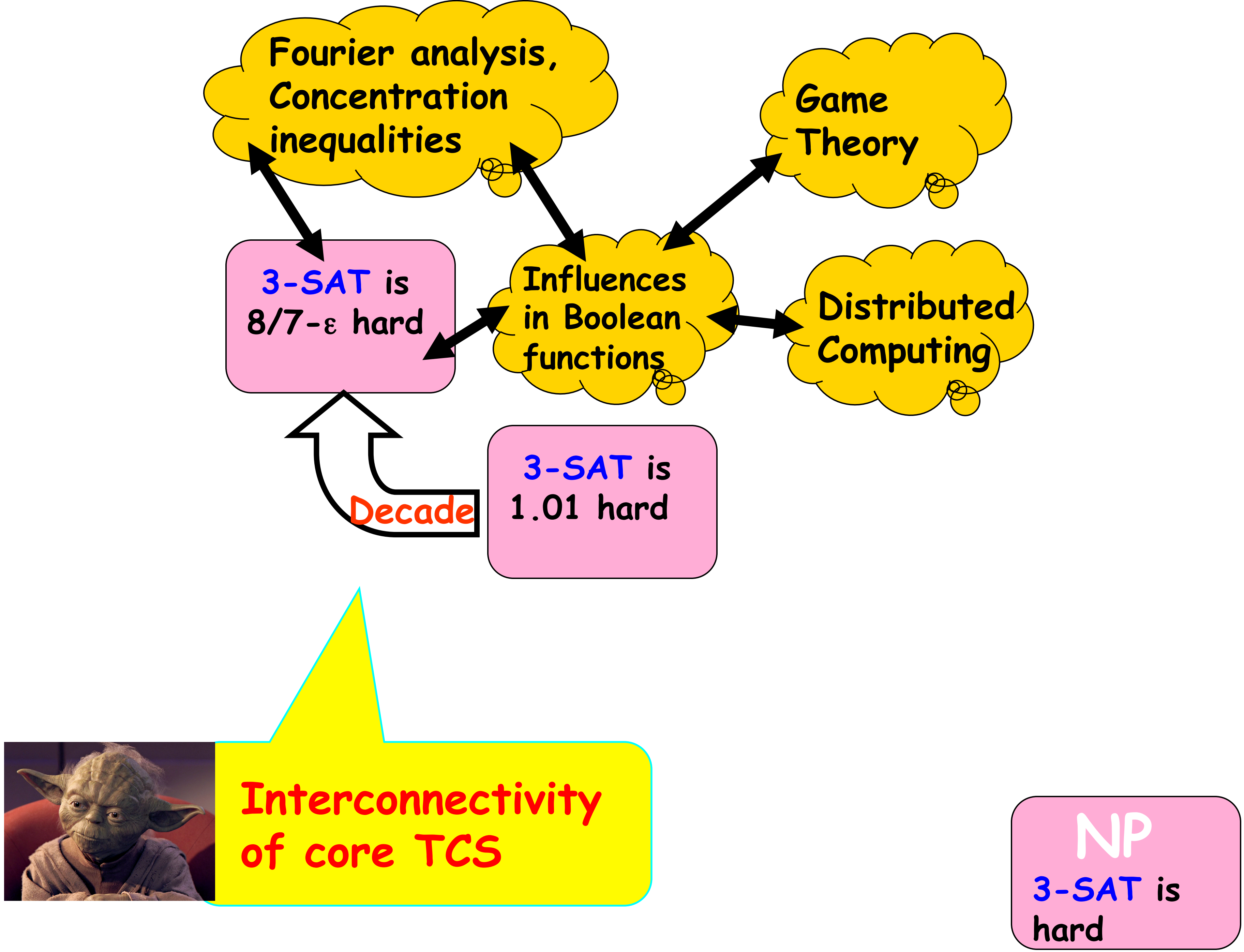
3-
1.0

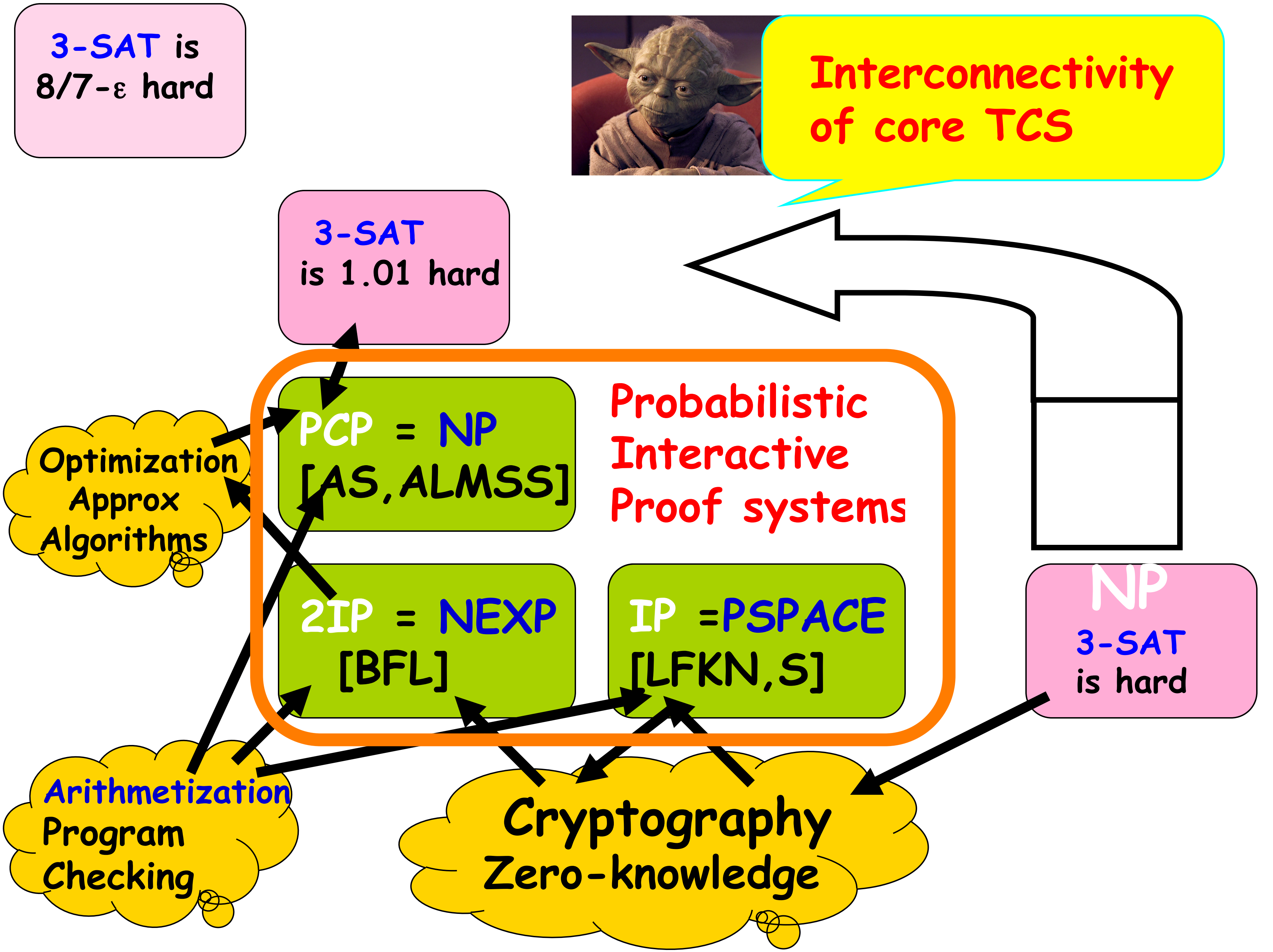
es



NP
3-SAT is
hard

Interconnectivi
of core TCS


Fourier analysis, Concentration inequalities
Game Theory
3-SAT is 8/7-ε hard
Influences in Boolean functions
Distributed Computing
Decade
3-SAT is 1.01 hard
Interconnectivity of core TCS
NP
3-SAT is hard



3-SAT is 8/7-ε hard
Interconnectivity of core TCS
3-SAT is 1.01 hard
PCP = NP [AS,ALMSS]
Probabilistic Interactive Proof systems
Optimization Approx Algorithms
2IP = NEXP [BFL]
IP =PSPACE [LFKN,S]
NP 3-SAT is hard
Arithmetization Program Checking
Cryptography Zero-knowledge

The last decade

By 2000s: Exact approx ratios for many problems

3-SAT = 8/7

3-XOR = 2

Set Cover = log n

… …

Where do these numbers come from?

[Khot] Conjecture
Linear equations are hard

[Raghavendra '08]
A single, universal algorithm achieves optimal approx ratio for all constraint satisfaction problems

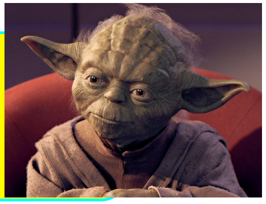
Decade

3-SAT is 8/7-ε hard

3-SAT is 1.01 hard

Convex programming
Analysis, Geometry

complete algorithm



NP
3-SAT
Is hard

Structure in cryptographic problems

Complexity-based

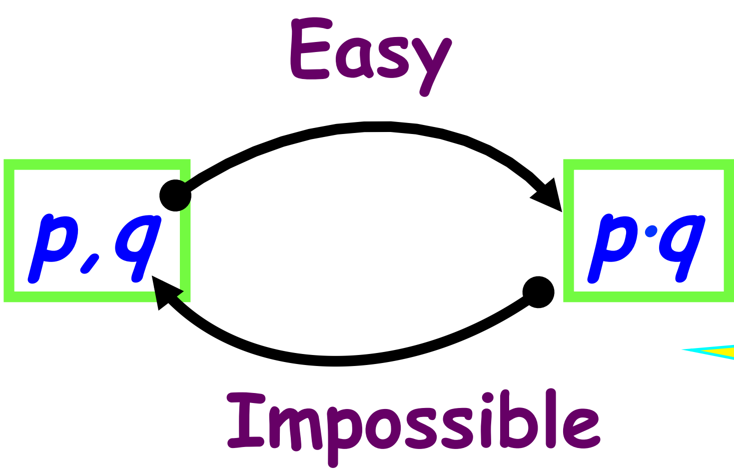
Cryptography

Predated the Internet & E-commerce

Enabled the Internet & E-commerce

- Parties can only solve easy problems
- Factoring is hard

Asymptotic view allows setting parameters



Information Theory
vs.
Complexity Theory

Secret communication
Public-key encryption
E-commerce security

Diffie-Hellman, Merkle '76
Rivest-Shamir-Adleman '77
Goldwasser-Micali '81

Alice

E_A

you

I want to purchase "War and Peace". My credit card number is

E_B(1111 2222 3333 4444)

Bob

amazon.com and you're done.

E_B

E_C

New reduction!

New standard

[DH,M,RSA] fficient recovery of x rom E_B(x)

[GM] Efficien distinguishing E_B(x) random

➔ Factoring is easy

Thm: Factoring hard ➔ secret communication

Ask the impossible

What else can be done?

- Digital signatures
- Secret exchange
- Oblivious Transfer
- Commitments
- Digital cash
- Coin Flipping

[GMR '85] Zero-Knowledge proofs

- ....

Different settings & privacy constraints

Different reductions to Factoring

- **Everything!!**

(in 2 steps)

A unified reduction

Eliminating bad guys

Bad guys

Malicious behavior

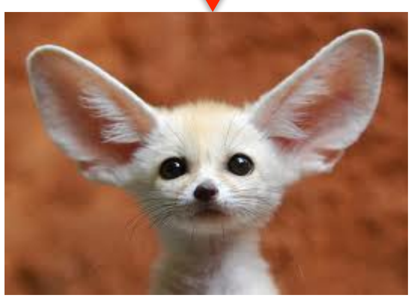
Fault-tolerance

GMW '86

Zero-Knowledge Compiler

New, complete primitive

Good guys

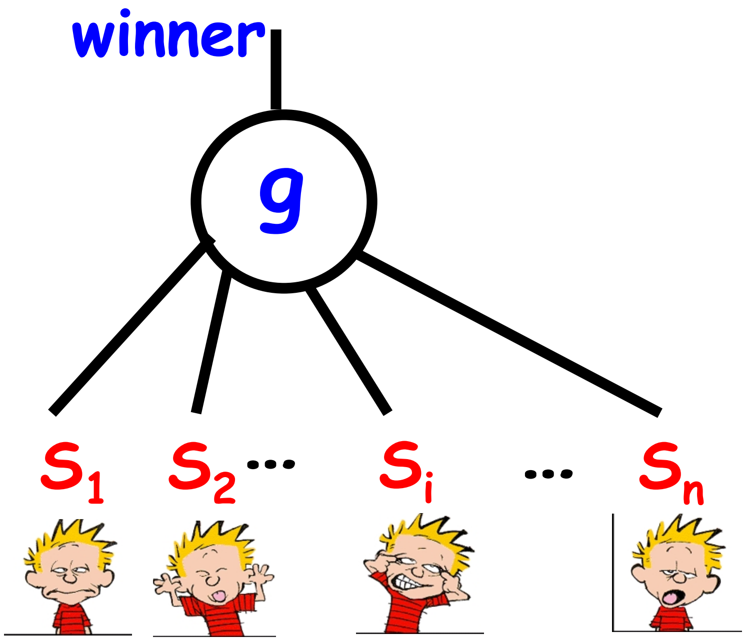


Honest But curious

Privacy / Secrecy

Dealing with good guys

Elections for honest players



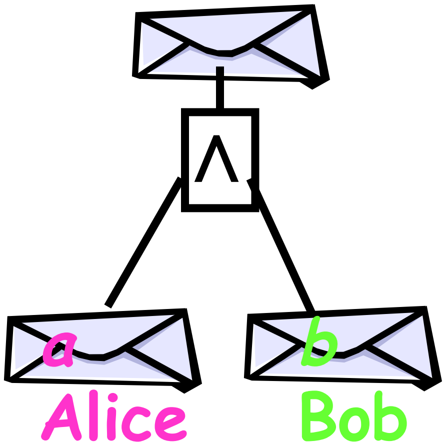
$$S_i = \begin{cases} 0 & \text{Democrats} \\ 1 & \text{Republicans} \end{cases}$$

Elections: g = Majority

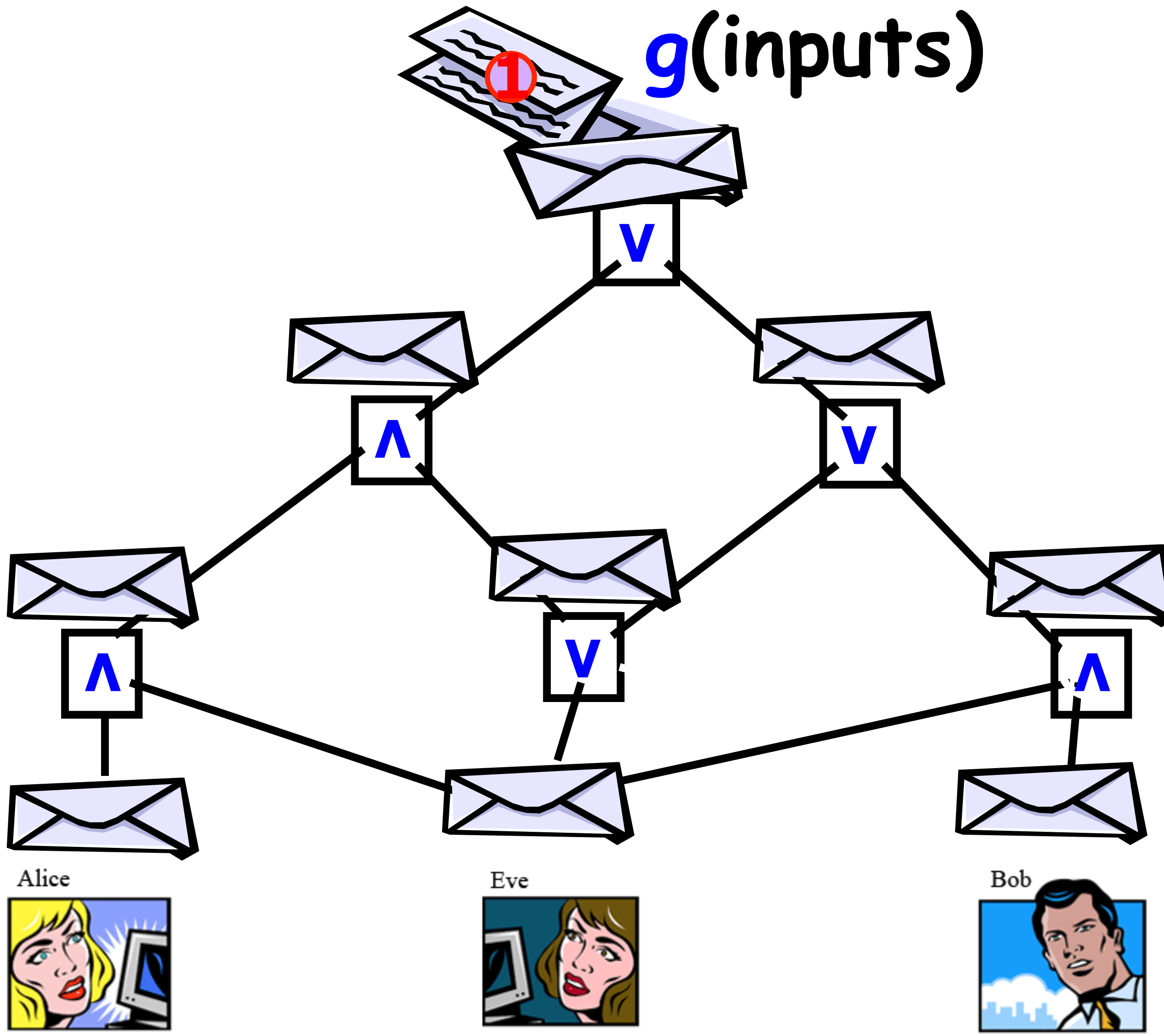
- All players learn $g(S_1, S_2, \ldots, S_n)$
- No subset learns anything more

Yao '86
GMW '87

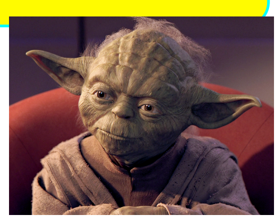
Oblivious computation with secret inputs



AND - complete problem



Locality



Secret communication is universal
in the complexity-theoretic model

[Yao '86, GMW '87]:

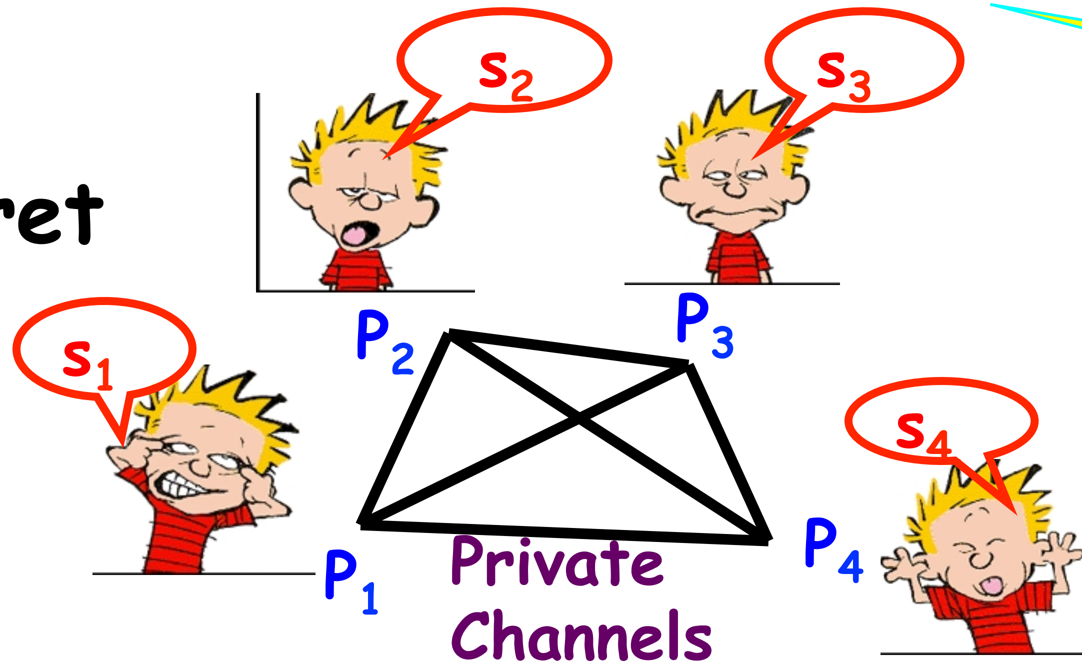
Every task can be performed*
privately & securely

*if at most 1/2 of the players misbehave.

Secret communication is universal
in the information-theoretic model

Analogy!

s_i secret



[BenOr-Goldwasser-Wigderson '90]: Every task can be performed* privately&securely

*if at most 1/3 of the players misbehave.

Structure in randomness

The power of randomness

- ~~Primality Testing~~ Agrawal-Kayal-Saxena'06
- Approximating the volume of convex bodies
- Computing large Fourier coefficients
- Testing polynomial identities
- Factoring polynomials over finite fields
- Approximating satisfiability of DNFs
- ……

Have probabilistic algorithms of polynomial time
Best known deterministic algs are exponential

Is this power real??
Where is the perfect randomness coming from??

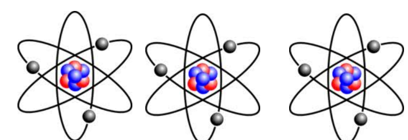
The Weakness of randomness

Approximating the volume
Computing large Fourier coefficients
Testing polynomial identities
Factoring polynomials over finite fields
Approximating satisfiability of DNFs
……

Have probabilistic algorithms of polynomial time

Best known deterministic algs are exponential

Is this power real??
Where is the perfect randomness coming from??

Only imperfect randomness in the world 
Thm[B,SV,NZ,……,GUV] Imperfect randomness suffices!
Randomness Extraction theory

The world is deterministic
Thm[BM,Y,……NW,IW] “P ≠ NP” suffices!!
Hardness vs. Randomness

Lower bounds?

Introspection - why we fail

- To prove general lower bounds, e.g. P ≠ NP

60's T
70's [B
80's C
90's [R
00's C
10's [A

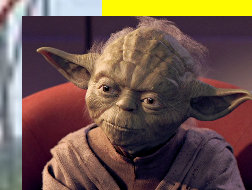
- To ss

Bl

All le

- Proo
- Inde
- Whi

ion



Open

P = NP? Can creativity be automated ?

P = BPP? Does randomness help ?

P = BQP? Does quantumness help ?

Is factoring hard? Is Internet security real?

Is multiplication harder than addition?

TCS education challenges

Algorithms are the language of the future

K-12 education: major addition to math

- Efficiency is basic human instinct
- More fun – algorithmic problems in games, puzzles,…
- Foster improvement & encouragement
- Highlight conceptual and intellectual sides

Undergrad, Grad: increase numbers

- Growing draw on TCS experts outside the field
- Growing need at the core

General public: Make Turing a household name

Thanks!