Microsoft

Computing in Science

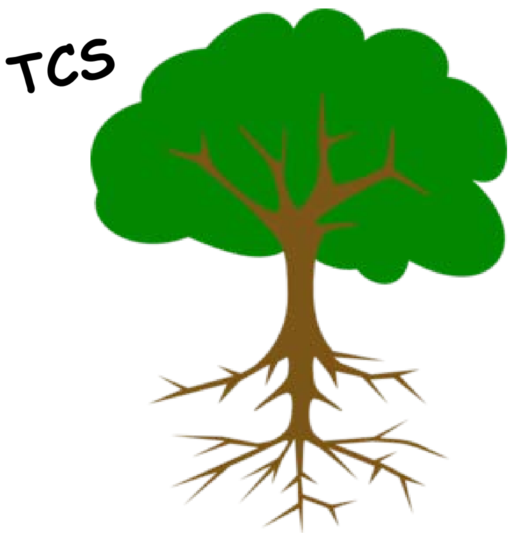
Microsoft Research Asia
FACULTY SUMMIT 2014
October 30-31
Beijing, China

Inter-disciplinarity: A View from Theoretical Computer Science

Andrew C. Yao
Institute of Interdisciplinary Information Sciences (IIIS)
Tsinghua University

*Some of the photos in this presentation are downloaded from the web.

The Story of
Theoretical Computer Science



Roots

A. Turing (Cook, Karp, Levin..): Model of Comp.

D. Knuth: Algorithms & data structures

A. Kolmogorov: Algorithmic information

P. Erdős: Combinatorics

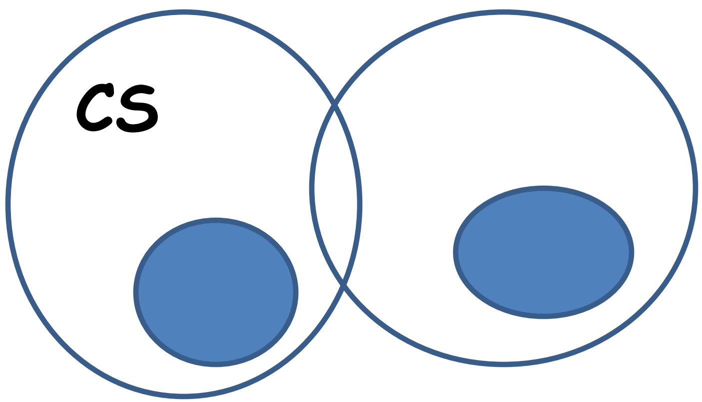
C. Shannon: Information theory

Modern Cryptography
Bio-informatics
Quantum computing
Economics & Games

Inter-disciplinarity

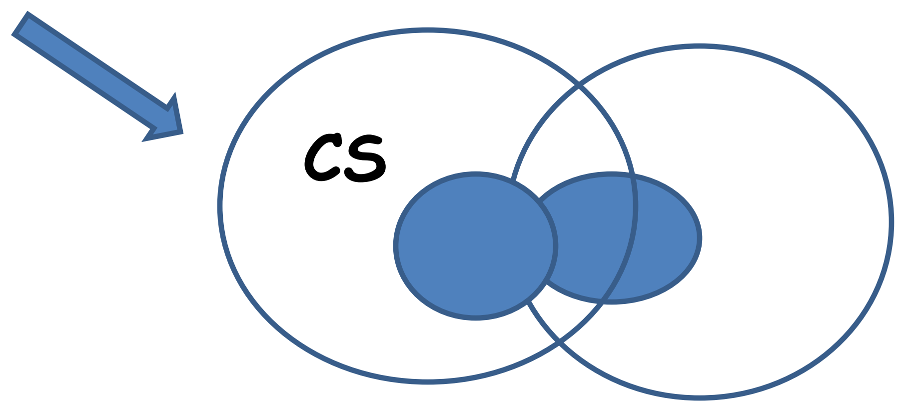
Computer Science → Physics, Biology, Engineering…

Numerical solutions
(Mathlab)



New trend:

Principled solutions,
core-core interactions



Some Examples

1. *CS + Economics :*
    - Auction -- Revenue maximization
2. *CS + Physics :*
    - Quantum Information – Super cloning
3. *CS + Math + Statistics + Physics + etc.*
    - Randomness – How to Certify?

1. Auction: Revenue maximization

Auctions

We have an item for sale.

<u>Problem</u>: *How much are the bidders willing to pay?*

We can ask them…

They will probably lie.

Auction design:

motivate the buyers to reveal their values.

Mechanism design

Auction theory is a sub-field of Mechanism Design.

We design the market.

"Economists as engineers"

Design an auction such that "*in equilibrium*" we get the results we want.

"Reverse Game Theory"

Goals

A seller (“auctioneer”) may have several goals.

Most common goals:

1. Maximize social welfare (efficiency)

   Give the item to the buyer that wants it the most
   (regardless of payments)

2. Maximize revenue (profit)

Two Auctions

'Sealed bid' auctions

1. 1^{st}-price/"pay-your-bid" auctions
2. 2^{nd}-price/Vickrey auctions

Nobel prize 1996

2^{nd}-Price Auction

2^{st}-price auction

- Award the item to the highest-price bidder,
  but charging only the 2^{nd}-highest price.

But do bidders bid truthfully?

- The 2^{nd} price auction for selling a single item is a truthful mechanism that maximizes social welfare (total utility of all bidders).
- Can this be achieved in revenue maximization ?

Revenue Maximization

- A single seller wants to sell k different items to N buyers, who each holds independently distributed values $F_1, \ldots, F_k$ for the k items.

- k=1 case: Myerson's classical work in 1981 (Nobel prize 2007)

- k>1 case: problem still open even for N=1.
  - simple mechanisms: selling the items *separately*, or selling them as *single bundle*.

Review: Selling One Item (k=1)

- A seller has 1 item to sell to a single buyer.
- Seller has partial knowledge of the buyer's interest in the item, as captured by a prior distribution *F*.
- How does the seller maximize (expected) revenue?

- Revenue with price p is: $p(1-F(p))$
  - ➔ Ask for the price that maximizes this expression

Selling Two items (k=2)

- Two items, One buyer
- Distribution on values for the two items is given
  - Simple case: IID

Sure, just sell each item optimally…

<u>Example</u>: item values are IID uniformly on {1,2}

<u>Selling Separately</u>: optimal revenue = 1

Price=1 ➔ Pr[buy]=1 ➔ Revenue=1

Price=2 ➔ Pr[buy]=1/2 ➔ Revenue=1

<u>Selling as Bundle</u>: you can get revenue > 2!

Price bundle at 3 ➔ Pr[buy]=3/4 ➔ Revenue = 2.25

Much More Complex!

- IID Uniform on {0,1}

  Selling each item separately is better than bundling

- IID uniform on {1, 2, 3}

  Buy any single item for \$2 or both for \$3

- IID uniform on [0,1] Manelli&Vincent 2006

  Buy any single item for \$X or both for \$Y

- IID on {1,2,4} with probabilities {1/6,1/2,1/3} Hart&Reny 2011

  Buy 50%-lottery for single item for \$1, or buy both surely for \$4

Maximum Revenue

REV(X) = max revenue from selling items of set X.

REV(X, Y) = max revenue from selling both sets X & Y.

Question: Is it possible that *REV(X, Y) >> REV(X) + REV(Y)* ?

Theorem [Hart, Nisan 2012] $REV(X,Y) \le 2(REV(X) + REV(Y))$ for independent X, Y.

Proof is surprisingly non-trivial.

Theorem [HN]

$$SREV(F_1 \times \cdots \times F_k) \ge \frac{c}{(\log k)^2} REV(F_1 \times \cdots \times F_k);$$

$$BREV(F_1 \times \cdots \times F_k) \ge \frac{c}{a \log k} REV(F_1 \times \cdots \times F_k) \quad \text{for identical } F_i.$$

Theorem [Li, Yao 2013]

$$SREV(F_1 \times \cdots \times F_k) \ge \frac{c}{\log k} REV(F_1 \times \cdots \times F_k);$$

$$BREV(F_1 \times \cdots \times F_k) \ge c\, REV(F_1 \times \cdots \times F_k) \quad \text{for identical } F_i.$$

Maximum Revenue (cont.)

- Babaioff et al [2014]
  max{SREV, BREV} >c REV ($F_1, \ldots, F_k$)

- Yao [SODA 2015]
  Study the general n,k case.
  Th. REV under Bayesian and Dominant-
  Strategy are equivalent up to constant factor

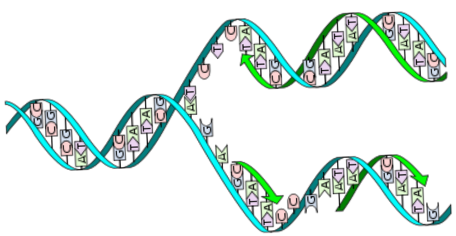
Hart, Nisan: Economist/Comp Scientist team
EC2012 Cross-discipline conference
Li, Yao [PNAS 2013]
Results are of interest to both fields

2. Quantum Information: Super-cloning

Replicating information

Replicating information has diverse applications:
information science, technology, biology, art, etc.

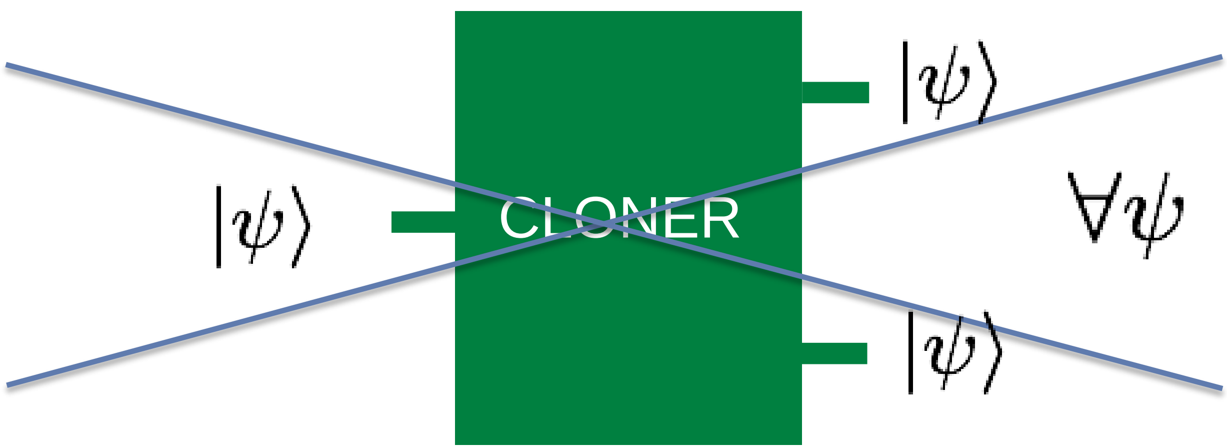
ANDY WARHOL



Can we invent microscopic copying machines that replicate
atoms, molecules, etc ?

Copying at the quantum scale: the no-go theorem

No-cloning theorem (Wootters and Zurek, Dieks)	No physical process can take as input a quantum system in an arbitrary state $\|\psi\rangle$ and produce as output two identical systems, each of them in the same state $\|\psi\rangle$



✓ Basis for the security of quantum cryptography.

Beyond the no-cloning theorem

- approximate cloning (copies are not perfect)
- probabilistic cloning (replication sometimes fails)

Q: Many special cases have been studied –
Is it possible to find general rules?

Q: Probabilistic processes often have nearly perfect cloning performances --
What are the ultimate limits?

The ultimate quantum limits

A replication process transforms N copies into $N + \delta N$ copies:

$$\delta N = O(N^\alpha) \qquad \alpha = \text{“replication rate”}$$

The replication is reliable if the copies are perfect for large N.

Theorem: For a set of states with continuous symmetry, reliable replication requires

- $\alpha < 1$ for deterministic processes (“standard quantum limit)
- $\alpha < 2$ for probabilistic processes (“Heisenberg limit”)

Chiribella, Yang, Yao [Nature Communications 2013]

SQL $\longrightarrow$ negligible number of extra-copies

HL $\longrightarrow$ large number (e.g duplication with almost no error)

Link with Computer Science

- *Cloning of photons can be modeled as a computational geometry problem in high-dimensional Hilbert space.*

- Also akin to the generation of almost-identical quantum keys for a group of users.

3. Certifying Randomness

Randomness

February 14, 2012 (The New York Times)

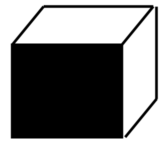
Researchers found that a fraction of RSA public keys in a database *-- 27,000 out of 7 million – have not been randomly generated.*

That is, it would be possible for someone to figure out the secret prime numbers behind the public keys, and to decode sensitive online communications.

Certifiable Source of Randomness

black box

F



x: 001011 → F → *F(x): 1001100101…*

- *Statistics based :*
  - *e.g., congruential random number generator*
- *Complexity-theory based:*
  - *e.g.* X^2 *(mod n) generator (1980's)*
- *Quantum-theory based:*
  - *e.g. using the CHSH test (Bell inequalities) as generator (2010)*

Device-Independent Quantum Cryptography

Make quantum cryptography work even using untrusted quantum apparatus.

- *Mayers, Yao [FOCS 1998]*
  - *Raised the concept*
- *Reichardt, Unger, Vazirani [Nature 2013]*
  - *Used quantum-based certification, made key progress in realizing DIQ*

Conclusions

- Sciences share:

  Methodology – observe phenomena,
  develop theories, testing them, etc

  Math/Algorithms – probability, complexity,
  approximations

- Common abstraction in different embodiment:

  e.g. *Many-body Systems*

- Universal topics:

  e.g. *Randomness, Information*

CALVIN HALL (central Berkeley campus)

Anatomy of the Program

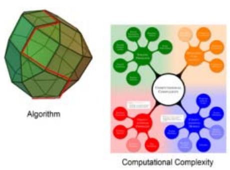
- Approx 35 long-term participants, including:
  - 3-4 program organizers
  - 6-10 visiting faculty
  - 6-10 postdocs
  - 10-20 visiting and local graduate students
- Additional influx of approx 35 people for each of 3 week-long workshops
- Introductory intensive "getting-on-same-page" course
- Reunion workshop one year after program

SIMONS INSTITUTE
FOR THE THEORY OF COMPUTING

Institute for Interdisciplinary Information Sciences (IIIS)

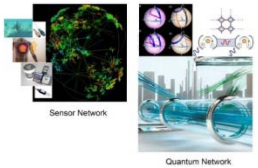
Established 4 years ago, 3 faculty → now 20

◆ Computer Science



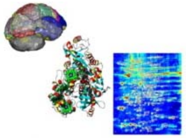
Theory

Security



Network Science

Machine Learning



Bio-informatics

Systems

Smart Grids

Comp Economics

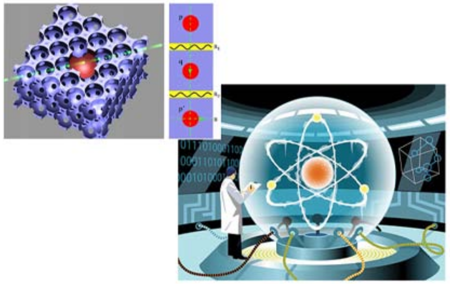
Natural Lang

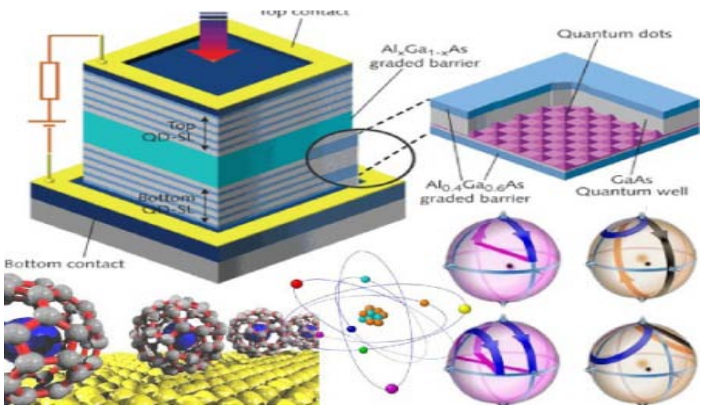
◆ Physics

Quantum info

Many-body physics

Complex systems





Center for Quantum Information of IIIS

New Building for IIIS, Tsinghua

Microsoft

Computing in Science

Microsoft Research Asia
FACULTY SUMMIT 2014
October 30-31
Beijing, China

Thanks