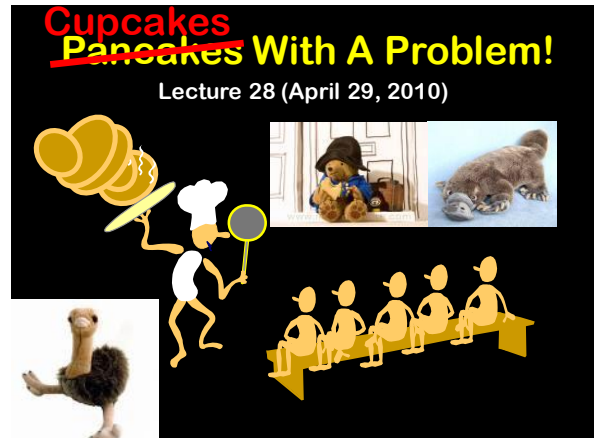


15-251

Great Theoretical Ideas in Computer Science



Announcements

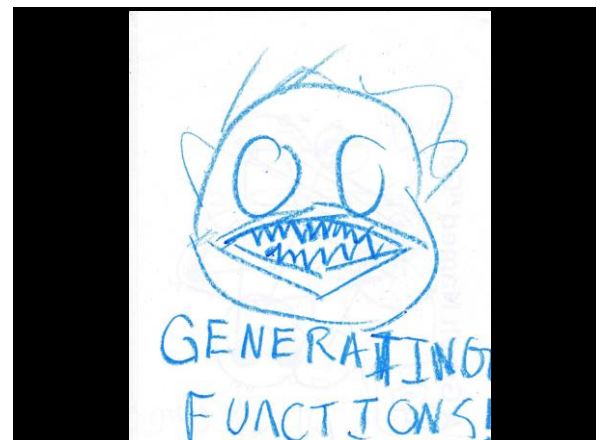
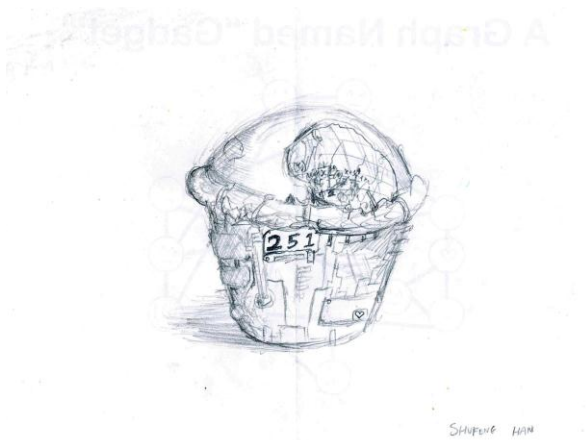
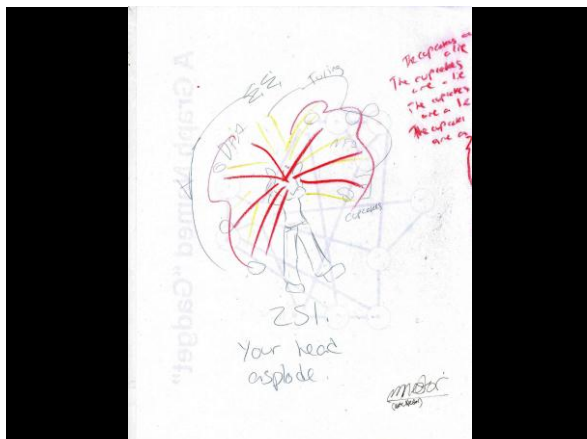
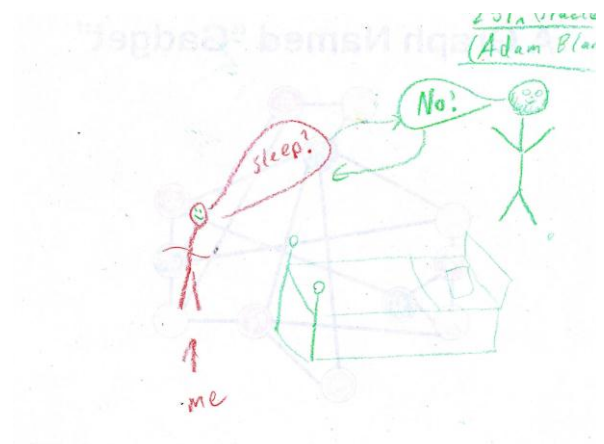
You are now eating manually.

Final Exam: Thursday May 6th 1:00pm – 4:00pm
The exam will be held in McConomy.

Review Session: Err...Dunno? This will be
posted.

We have some pictures...and stuffs...





We Had Some Lectures

1. Pancakes with a Problem
2. Inductive Reasoning
3. Ancient Wisdom: Unary and Binary
4. Counting I
5. Counting II
6. Counting III
7. Recurrences with Generating Functions
8. ~~Recurrences and Continued Fractions~~
9. Games I
10. Probability I
11. Probability II
12. ~~Random Walks~~
13. Linearity of Expectation
14. Probabilistic Method
15. Markov's Inequality
16. Union Bound
17. Number Theory
18. Cryptography and RSA
19. ~~Grade school: how to add and multiply~~
20. Algebraic Structures I
21. Algebraic Structures II
22. Lagrange's Theorem
23. ~~Cosets~~
24. Cyclic Group
25. Permutation Group
26. Cayley's Theorem
27. Graphs I: Trees and Planar Graphs
28. Graphs II: Matchings, Tours, and More
29. Adjacency Matrix
30. Minimum Spanning Tree
31. Kruskal's Algorithm
32. Travelling Salesman Problem
33. ~~The Traveling Salesman Problem~~
34. Automata: DFAs and Regular Languages
35. Turing Machines
36. ~~Social Networks~~
37. Cantor's Legacy: Infinity and Diagonalization
38. Turing's Legacy: The Limits of Computation
39. Gödel's Legacy: Formal Logic/Incompleteness
40. Definition of Axiom, Inference Rule
41. Propositional Calculus
42. Formation Rules
43. ~~Truth Concept~~
44. ~~Resolution Inference Rule~~
45. Induction on Proofs
46. Definitions of Consistency
47. Definition of Completeness
48. Definition of Soundness
49. Gödel Numbering
50. ~~Diagonal Lemma~~
51. ~~Proof of Gödel's First Theorem~~
52. Statement of Gödel's Theorems
53. ~~Arithmetical Hierarchy~~
54. Efficient Reductions Between Problems
55. Complexity Theory: P vs NP

Contest

You are now eating manually.

First person to finish his or her cupcake gets 1% extra credit on the final!

Zero Knowledge Proofs

I have a 3-coloring of a graph...

But Dmitriy is being mean to me...

So, I'm like... "I bet I can convince you that I have a three-coloring without letting you know what it is!"

How Should We Vote?

Subtitle: A failure of Theory

Lecture 28 (April 29, 2010)

Part 1: The System is Broken

Proof: The 2000 election.

Presidential candidate	Vote total	%	Party
George W. Bush (W)	2,912,790	48.847	Republican
Al Gore	2,912,253	48.838	Democratic
Ralph Nader	97,421	1.634	Green
Patrick J. Buchanan	17,484	0.293	Reform
Harry Browne	16,415	0.275	Libertarian
John Hagelin	2,281	0.038	Natural Law/Reform
Howard Phillips	1,378	0.023	Constitution
Other	3,028	0.051	—
Total	5,963,110		

Source: 2000 official presidential general election results [\[1\]](#)

QED. (There are many other examples)

The system we use (called plurality voting, where each voter selects one candidate) doesn't work well for 3 or more candidates.

Clearly the "wrong" candidate often wins.

By "wrong" I mean there is a losing candidate who would make more people happier than the winner. (We'll get to defining this more precisely later.)

Little known tangential fact:

Actually, Gore won the election, as shown in a full statewide recount down by a consortium of newspapers.

<http://www.nytimes.com/2001/11/12/politics/recount/12ASSE.html>

Part 2: Ranked Ballots

Nicolas de Caritat,
marquis de Condorcet,
1743 to 1794



He studied the concept of ranked ballots – having the voters rank all the candidates

Concorcet's Analysis

For each pair of candidates, decide who is preferable. (i.e. wins in more of the rank orderings)

In these matchups, if there's one candidate who beats all, he/she is the clear winner.

This candidate is called the **Condorcet Winner**

Example. Three candidates B, G, and N.

1000	B > G > N
500	G > B > N
500	G > N > B
10	N > G > B
1	N > B > G

Total of 2111 votes.

B > G	1001	G > B	1010
B > N	1500	N > B	511
G > N	2000	N > G	11

G is the Condorcet winner

Concorcet's Paradox

1	A > B > C
1	B > C > A
1	C > A > B

So we have $A > B$, $B > C$ and $C > A$

There might not be a Condorcet winner.

Proposed Solutions

Dozens of solutions have been proposed.

Two of them are:

Borda Counting
Instant Runoff Voting (IRV)

Borda Counting

There are n candidates.

Assign a score by each voter to each candidate. n to the best, $n-1$ to the next and so on down to 1 for the least.

Now compute the candidate with the highest total.

Instant Runoff Voting (IRV)

There are n candidates.

Repeat until there's just one candidate left:

Find the candidate with the least #1 rankings.

Delete that candidate from all ballots.

Borda and IRV are better than plurality, but is there a really good system?

The answer is "NO". Kenneth Arrow proved in 1950 that Democracy is impossible.

Things are hopeless. Forget about it.

Ok, calm down. What did he actually prove?

Say you have an election function F that takes as input the rank orderings of all the voters and outputs a rank ordering.

$F(v_1, v_2, v_3, \dots, v_n)$

(F is deterministic and not necessarily symmetrical on its inputs.)

It would be nice if F had the following properties:

1. (U) Unanimity If all votes have $A > B$ then the output has $A > B$.
2. (IIA) Independence of irrelevant alternatives: If we delete a candidate from the election, then the outcome is the same except with that candidate missing.

Arrow's Theorem:

Any voting function that handles 3 or more candidates and satisfies U and IIA is a dictatorship!

(A dictatorship I mean that there's one voter who dictates the entire outcome of the election.)

The proof is not too difficult.

Arrow won the Nobel Prize in economics primarily for this work.

This theorem derailed the entire field of social choice theory for the last 50 years, as we'll see.

Wait, you say.

We really only want to determine a winner. We don't need the election function to generate a full rank ordering. Surely we can do that.

Good point. But you're out of luck there too.

In the 1970s Gibbard and Satterthwaite proved this: There does not exist a winner selection algorithm satisfying these properties:

1. The system is not a dictatorship
2. If every voter ranks A on top, then A wins
3. It's deterministic
4. There are at least three candidates
5. It never pays for voters to lie. That is, if a voter V prefers A to B, then putting B before A in her vote cannot cause a better outcome from her point of view.

Part 3: Range Voting

What about the kind of voting we use all the time on the internet. Like at Amazon.com, or HotOrNot, or MRQE?

Every voter scores each candidate on a scale of, say 1 to 10. Then order the candidates by their average vote.

The idea is called **range voting**.

Let's think about the criteria listed in Arrow's theorem.

Does range voting satisfy unanimity?

Of course. If each voter scores A above B then A will have a higher average than B

Does range voting satisfy IIA?

Of course. If we delete one or more candidates from the election, then the rest stay the same.

Is range voting a dictatorship?

No. Duh.

RANGE VOTING DOES THE IMPOSSIBLE!

How does it do that?

We've changed the rules of the game laid out by Concordet, and followed by the entire field of social choice for 250 years.

We don't restrict voting to preference lists. We allow scores. This tiny change completely fixes these problems.

Oh, and what about the Gibbard Satterthwaite theorem?

Again, range voting does the "impossible".

It satisfies all the criteria at least for three person elections.

See: <http://www.rangevoting.org/GibbSat.html>

But is there a better way to analyze voting systems?

Enter Warren Smith in the late 1990s.

Smith applied a system called **Bayesian Regret** to the analysis of voting systems.

Oddly, this had never been applied to voting systems before.

Bayesian Regret Simulations

1. Each voter has a personal "utility" value for the election of each candidate
2. Now the voters vote, based both on their private utility values, and (if they are strategic voters) on their perception from "pre-election polls" (also generated artificially within the simulation, e.g. from a random subsample of "people") of how the other voters are going to act.
3. The election system E elects some winning candidate W.
4. The sum over all voters V of their utility for W, is the "achieved societal utility."
5. The sum over all voters V of their utility for X, *maximized* over all candidates X, is the "optimum societal utility" which would have been achieved if the election system had magically chosen the societally best candidate.
6. The difference between 5 and 4 is the "Bayesian Regret" of the election system. It is zero if $W=X$, or it could be positive if W and X differ.

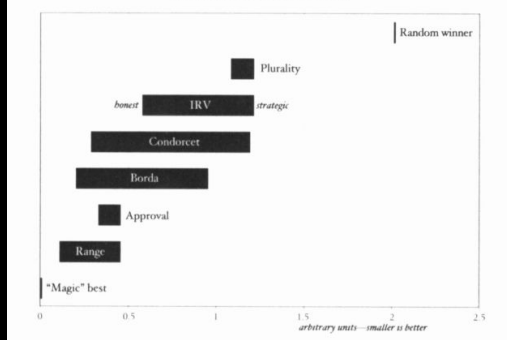
See <http://www.rangevoting.org/BayRegDum.html>

Warren Smith's Simulations

Smith simulated millions of election scenarios, adjusting the distribution of strategic voters, and the distributions of private utility values.

Range voting worked the best in *ALL* of the simulations.

Which Voting System Is Best?



The moral of the story

1. In theory we often make assumptions in order to prove theorems.

Be careful how you interpret and use the theorems. They can be misleading.

EG: Voting is impossible..

EG: Don't even bother to try to solve NP complete problems. It's hopeless.

2. Range Voting is the best voting system.

References

www.rangevoting.org

Gaming the Vote -- Why elections aren't fair, and what we can do about it
by William Poundstone, 2008