LECTURE 3: SATISFIABILITY

SATISFIABILITY

Definition:

A compound proposition is **satisfiable** if it can be made true by assigning appropriate values to its **variables**.

Examples: Are these satisfiable?

$$p \lor \neg p$$

$$p \land \neg p$$

$$(p \lor \neg q) \land (q \lor \neg r) \land (r \lor \neg p)$$

$$(p \land q \land r) \land (p \land r \to \neg q)$$

SATISFIABILITY

Definition:

A compound proposition is **satisfiable** if it can be made true by assigning appropriate values to its **variables**.

Examples: Are these satisfiable?

$p \vee \neg p$ Yes (tautology)

$p \wedge \neg p$

$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$

$(p \wedge q \wedge r) \wedge (p \wedge r \rightarrow \neg q)$

SATISFIABILITY

Definition:

A compound proposition is **satisfiable** if it can be made true by assigning appropriate values to its **variables**.

Examples: Are these satisfiable?

$p \vee \neg p$	Yes (tautology)
$p \wedge \neg p$	No (contradiction)
$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$	
$(p \wedge q \wedge r) \wedge (p \wedge r \rightarrow \neg q)$	

SATISFIABILITY

Definition:

A compound proposition is **satisfiable** if it can be made true by assigning appropriate values to its **variables**.

Examples: Are these satisfiable?

$p \vee \neg p$	Yes (tautology)
$p \wedge \neg p$	No (contradiction)
$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$	Yes
$(p \wedge q \wedge r) \wedge (p \wedge r \rightarrow \neg q)$	

SATISFIABILITY

Definition:

A compound proposition is **satisfiable** if it can be made true by assigning appropriate values to its **variables**.

Examples: Are these satisfiable?

$p \vee \neg p$	Yes (tautology)
$p \wedge \neg p$	No (contradiction)
$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$	Yes
$(p \wedge q \wedge r) \wedge (p \wedge r \rightarrow \neg q)$	No

SAT SOLVERS

Definition:

The **SAT** problem is the problem of determining whether a compound proposition is satisfiable. If so, truth assignments that satisfy the compound proposition are called the **solution**.

SAT problems are HARD!

- NP Complete
- No efficient algorithm for ALL problems
- Truth table: 1000 variables = $2^{1000} > 10^{300}$ rows
- SAT solvers exists that can solve problems with many unknowns

REDUCTIONS TO SAT

Many problems can be mapped into a SAT problem

- Fact: Any "decidability" problem reduces to SAT
- SAT solvers can solve almost anything

Real-World:

- Register allocation
- Traveling salesman (delivery routing)
- Packing problems (knapsack)
- Cryptography
- Verifying digital cirtcuits
- FPGS layout
- Candy Crush Saga

Examples we'll look at:

- System Specification
- Logic puzzles
- Sudoku

SYSTEM SPECIFICATION

Logical requirements that a system must satisfy:

- Written before coding begins
- Unit tests build to verify system specifications

"If a message is stored in buffer, it is transmitted"

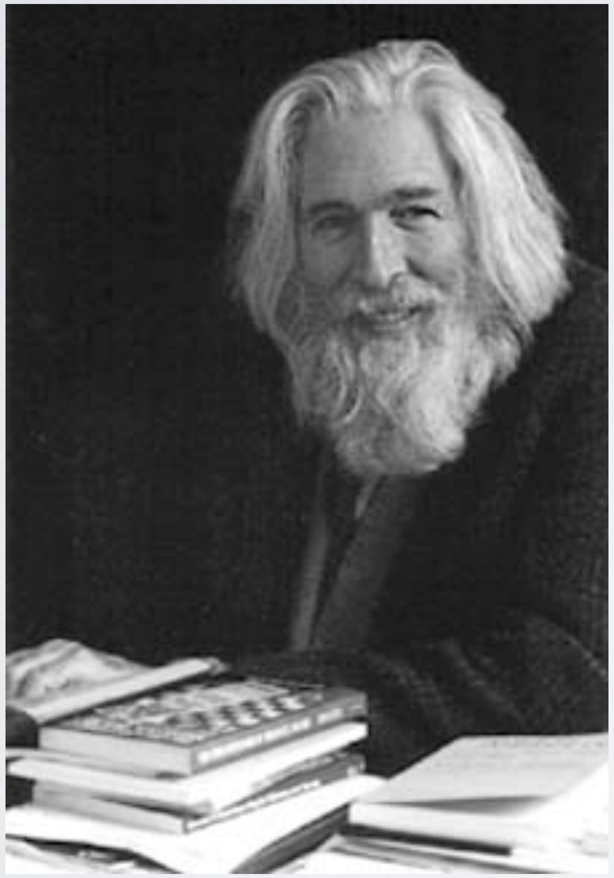
"A message is stored in the buffer"

Definition:

Specifications are **consistent** if they can be satisfied simultaneously.
Otherwise, they are **inconsistent**.

"The message is not transmitted"

LOGIC PUZZLES



Raymond Smullyan

His Fault

- Word Puzzles that reduce to SAT problems
- Big part of LSAT

Knights: Always tell the truth
Knaves: Compulsive liars

FAMOUS PUZZLE:

You go to an island and meet A and B.
A says: "**B is a knight**"
B says: "**The two of us are of opposite types**"

Convert to SAT:

p: A is a knight
q: B is a knight

Do on Board

APPLICATION: THE LABYRINTH

Hypothetical Situation

You're Jennifer Connelly and you're in the 1986 film "The Labyrinth" with David Bowie. You're walking through a maze trying to find your little brother that David Bowie has kidnapped, and for some reason David Bowie is wearing leggings and a dance belt. You come to a fork in the road with two strange creatures. They tell you one path leads to death and one leads to freedom. One creature is a knight and the other is a knave. **You ask A: "what would B say if I asked him which way to freedom?" A responds "left." Which way should you go?**

SUDOKU

Rules:

- Every column has every digit 1-9
- Every row has every digit 1-9
- Every block has every digit 1-9
- Every square has 1 digit

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Define simple propositions

$p_{r,c,n}$ The box at row r and column c contains n

There are 9x9x9=729 variables

Idea: Embed into SAT

Cook up a compound proposition that is true only for solutions

LOGIC RULES

Every row has every digit:

$$\bigwedge_{r=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{c=1}^{9} p_{r,c,n}$$

Every col has every digit:

$$\bigwedge_{c=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{r=1}^{9} p_{r,c,n}$$

Every block has every digit:

$$\bigwedge_{R=0}^{2} \bigwedge_{C=0}^{2} \bigwedge_{n=0}^{9} \bigvee_{r=1}^{3} \bigvee_{c=1}^{3} p_{3R+r,3C+c,n}$$

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

LOGIC RULES

Every cell has at most one number:

$$\bigwedge_{r,c,n\neq n'} p_{r,c,n} \rightarrow \neg p_{r,c,n'}$$

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Every "given" cell is already fixed:

$$p_{1,1,5} = T$$

$$p_{1,2,3} = T$$

$$\vdots$$

Q: Do we need to assert that every cell has a number?