Satisfiability with Exponential Families

Dominik Scheder, Philipp Zumstein

ETH Zürich

SAT 2007

Problem Description (informal)

$$F = x_1 \wedge (x_2 \vee x_3) \wedge (\neg x_2 \vee \neg(x_5 \vee \neg x_4))$$

	00001	00010	00011			00110	00111
01000	01001		01011	01100	01101	01110	
	10001		10011	10100	10101	10110	10111
11000		11010	11011	11100	11101		11111

S_5

Assume: some of the assignments are forbidden

Question: Does there exists a satisfying assignment in S_5?

Problem Description (formal)

Satisfiability with the exponential family S

Fix: $S \subseteq \{0,1\}^*$ of exponential size

Given: $V = \{x_1, \ldots, x_n\}$ ordered variable set
F formula over V

Question: $\exists\, x \in S \cap \{0,1\}^n$: x satisfies F?
(we say that F is S-satisfiable)

S-SAT

complexity of the problem? NP-hard? polynomial?

Exponential Size

$S_n := S \cap \{0,1\}^n$ (levels of S)

Fact: If $|S_n|$ is polynomial in n, and S_n can be enumerated in polynomial time, then S-SAT is in P.

exponential size

$|S_n| = \Omega(\alpha^n)$ for some $\alpha > 1$

i.e. $|S_n| \geq \alpha^n$ for n large enough

weaker assumption allow also to have “holes”

e.g. $|S_{2k}|=2^{2k}$, $|S_{2k+1}|=0$

Examples

- $S = \{0,1\}^*$.
  Then the S-SAT problem is the normal SAT problem.

- $S = \{ x \in \{0,1\}^* : x_1 = 0 \}$.

Claim: S-SAT with this family is NP-hard.
Proof: We can reduce the SAT problem to S-SAT.
F formula over n variables
construct $F' = \text{switch}(F, x_1)$
x satisfy $F \Leftrightarrow \text{switch}(x, x_1)$ satisfy $\text{switch}(F, x_1)$
F is satisfiable $\Leftrightarrow F \vee F'$ is S-satisfiable.

- $S = \{ x \in \{0,1\}^* : |x|_1 \text{ is even}\}$.

- $S = \{ ww : w \in \{0,1\}^* \}$.

Main Results

Theorem 1: Suppose S $\subseteq \{0,1\}^*$ is exponential and context-free. Then S-SAT is NP-complete.

Theorem 2: If S-SAT is in P for some exponential S then SAT has polynomial circuits.

Theorem 3: There is an *exponential* S such that S-SAT is not NP-hard (provided P $\neq$ NP).

VC-dimension

$J \subseteq \{1,\ldots,n\}$ is **shattered** by S_n if the projection $S_n|_J = \{0,1\}^{|J|}$.
This means that the projection in these dimension is surjective,
i.e. for each $x \in \{0,1\}^{|J|}$ there is a $y \in S_{\mathbf{n}}$ with $x_i = y_i$ for $i \in J$.

Definition: $\dim_{VC}(S_n) = \max \{ |J| ; J \text{ is shattered by } S_n \}$
[Vapnik, Chervonenkis, 1971]

Lemma [Sauer, 1973]: Suppose $\dim_{VC}(S_n) \leq d$. Then
$|S_n| \leq \sum_{i=0}^{d} \text{binom}(n,i) \leq 2^{H(d/n)n}$.

Corollary: If $|S_n| \geq \alpha^n$ for some $\alpha>1$,
then $\dim_{VC}(S_n) \geq \delta n+1$ for some $\delta>0$.

VC-dimension: Example

	00001	00010	00011			00110	00111
01000	01001		01011	01100	01101	01110	
	10001		10011	10100	10101	10110	10111
11000		11010	11011	11100	11101		11111

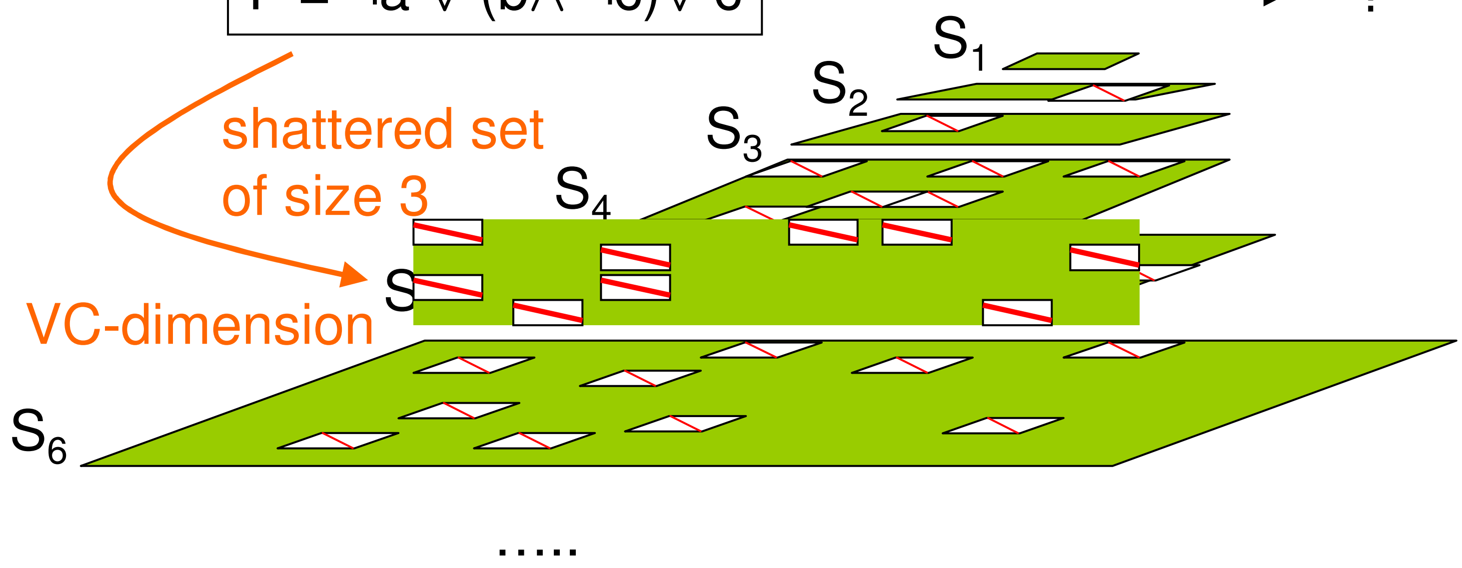
{1,2,3} is a shattered set

VC-dimension and S-SAT

Theorem: S $\subseteq \{0,1\}^*$ exponential family and suppose we can compute in polynomial time a linear size shattered index set J. Then S-SAT is NP-hard.

Proof: SAT ⇝ S-SAT

$F = \neg a \vee (b \wedge \neg c) \vee c$ → ?



VC-dimension and S-SAT

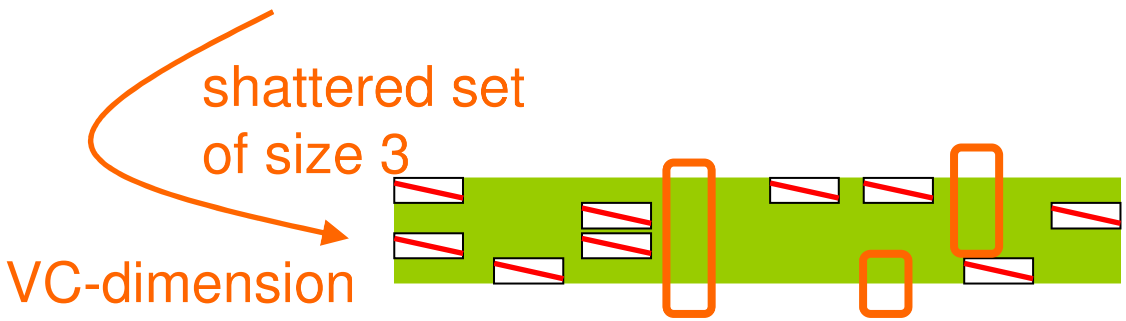
Theorem: $S \subseteq \{0,1\}^*$ exponential family and suppose we can compute in polynomial time a linear size shattered index set J. Then S-SAT is NP-hard.

Proof: SAT ⇝ S-SAT

$F = \neg a \vee (b \wedge \neg c) \vee c$ ⟶ ?

$F' = \neg x_1 \vee (x_2 \wedge \neg x_3) \vee x_3$

$V = \{ x_1, x_2, x_3, x_4, x_5 \}$



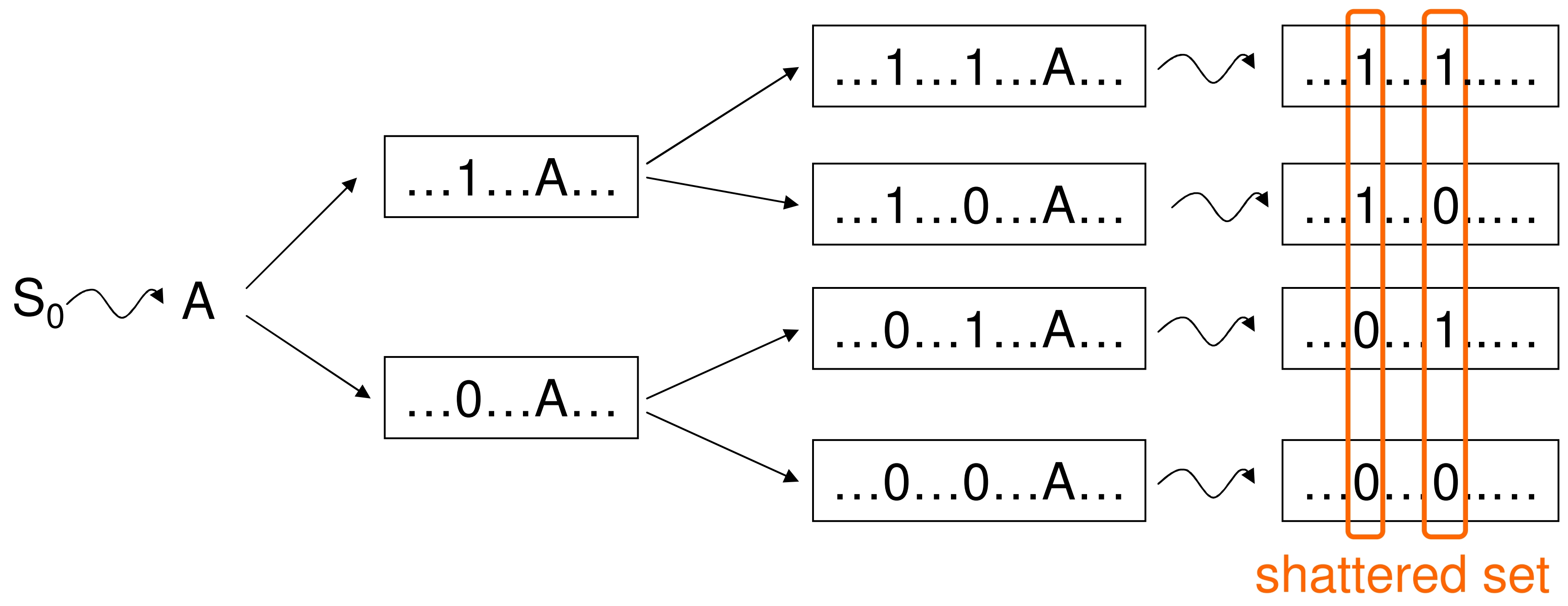
{1,2,3} is shattered set

F is satisfiable ⇔ F' is S-satisfiable
polynomial reduction

Exponential Context-free Languages

Theorem 1: Suppose $S \subseteq \{0,1\}^*$ is exponential and context-free.
Then S-SAT is NP-complete.

Sketch of a Proof: There exists a non-terminal A with derivations



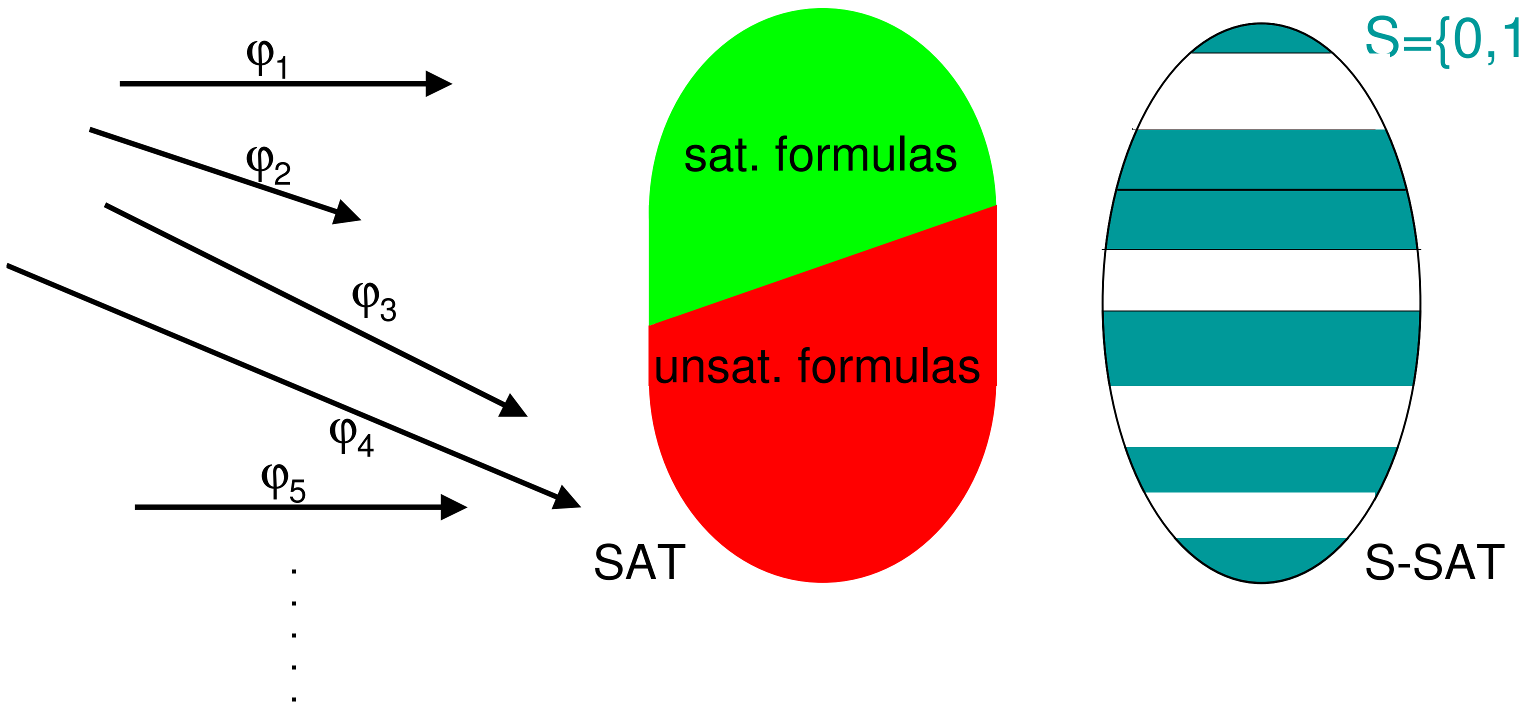
S-SAT which is not NP-hard

Construction:

let $\varphi_1, \varphi_2, \varphi_3, \ldots$ be a sequence of all possible polynomial reductions (countable many)

(i) there are arbitrarily big formulas with satisfiable preimages

(ii) „destroy a level“ for each reduction and „let the next one be full“ and continue then on the next level → definition of S



$S = \{0,1\}^* - \{0,1\}^{n_1}$
$- \{0,1\}^{n_2}$
$- \ldots$

S-SAT which is not NP-hard

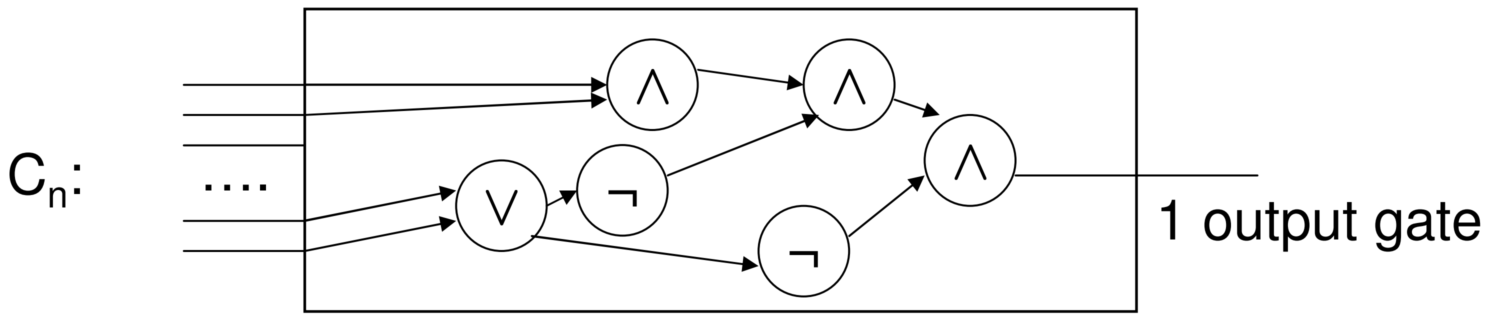
So we have seen the following

Theorem 3: There exists an exponential S (with some holes) for which S-SAT is not NP-hard (provided NP $\neq$ P).

With some more work we can also delete the holes.

S-SAT and Polynomial Circuits

Circuit family $\mathcal{C} = (C_1, C_2, \ldots)$



$\mathcal{C}$ decides a language $L \subseteq \{0,1\}^*$.

If the size of C_n grows polynomially in n then $\mathcal{C}$ is called to be a polynomial circuit family. Furthermore if we have an algorithm which computes C_n and runs in polynomial time then we say that L has uniform polynomial circuits.

S-SAT and Polynomial Circuits

Theorem 2: If S-SAT is in P for some exponential S, then SAT has polynomial circuits.

Sketch of Proof: there are shattered index sets of linear size with these sets we can reduce SAT to S-SAT this give us the (not necessarily uniform) polynomial circuits for SAT.

Karp, Lipton: If SAT has polynomial circuits, then the polynomial hierarchy would collapse to its second level!

Summary and Questions

- S-SAT for exponential families is NP-hard if we know some structure about S, namely if we can compute a shattered set of linear size in each dimension in polynomial time
- For context-free languages S we have enough structure to prove that it is NP-hard.
- There are construction which shows that S-SAT can also be not NP-hard for exponential S.

- What about other classes of assignments?
- What about other hardness results?

Thank you!