

Phase transition for the satisfiability of Random (Quantified) formulas

Nadia Creignou

LIF, Aix-Marseille Université

Microsoft Research, Cambridge, Tractability Workshop 2010

Outline

1 Satisfiability of random CNF-formulas

- Random models
- Nature of the transition
- Location of the transition
- 3-SAT and 2-SAT

2 Quantified satisfiability problems

- QSAT
- (1,2)-QSAT
- Experimental results

Outline

1 Satisfiability of random CNF-formulas

- Random models
- Nature of the transition
- Location of the transition
- 3-SAT and 2-SAT

2 Quantified satisfiability problems

- QSAT
- (1,2)-QSAT
- Experimental results

Phase transition

- Transition from SAT to UNSAT for random formulas when the number of clauses increases.
- Asymptotical results : the number of variables tends to infinity

Random models for k-CNF-formulas

n variables, $N = 2^k \binom{n}{k}$ clauses.

- Choose L clauses independently and uniformly among all the possible ones
 $Pr_{n,cn}(3\text{-SAT})$: probability that such a random 3-CNF formula over n variables with $L = cn$ clauses is satisfiable.
- Choose each of the clauses independently with probability $p(n)$,
 $Pr_{n,p}(3\text{-SAT})$

When $p(n) \cdot N \sim cn$, the two models are equivalent

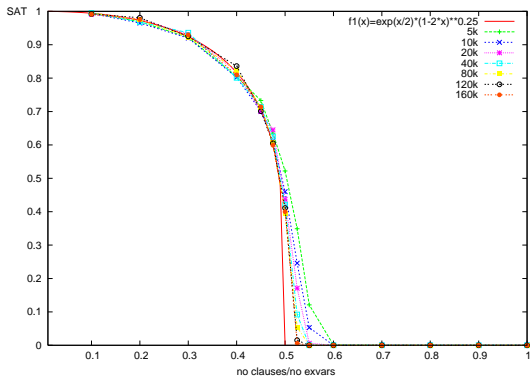
We study

$$\lim_{n \rightarrow +\infty} Pr_{n,cn}(3\text{-SAT}) = \varphi(c)$$

as a function of the parameter c

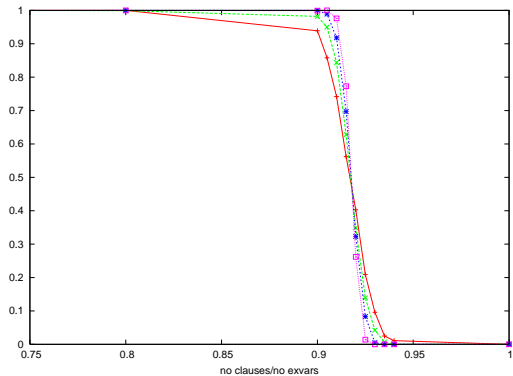
Example of transition : 2-XOR-SAT

$$\varphi(c) = \exp(c/2)(1 - 2c)^{1/4}$$



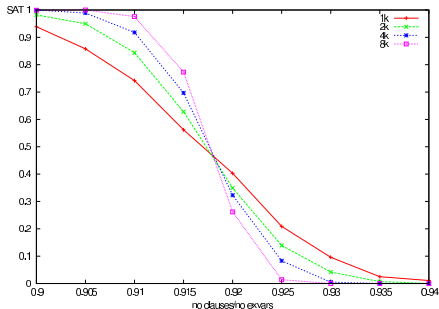
Another example : 3-XOR-SAT

“degenerated” $\varphi(c)$



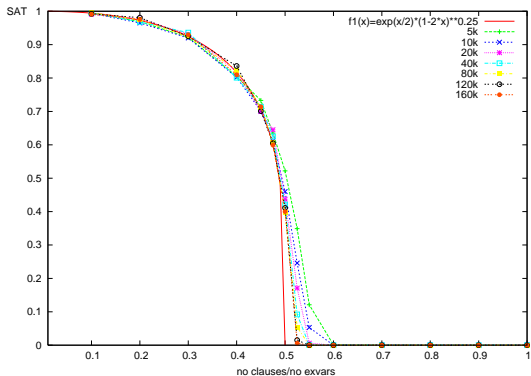
The transition seen through a magnifying glass

We have to change the scale

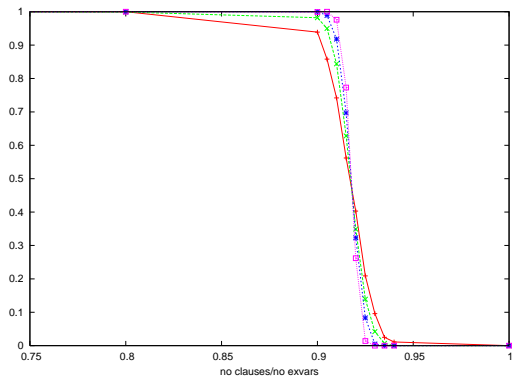


$$\lim_{n \rightarrow +\infty} Pr_{n, 0.918n + c\sqrt{n}}(3\text{-XOR-SAT}) = \varphi(c)?$$

2-XOR-SAT : Coarse



3-XOR-SAT : sharp



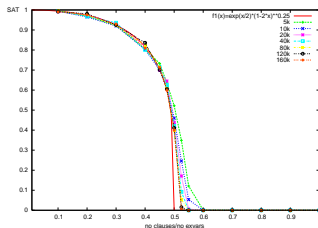
Critical ratio estimated to $c_{3\text{-XOR-SAT}} = 0.918$.

Sharp or Coarse Transition

Define L_ε by $P_{n,L_\varepsilon}(\text{SAT}) = \varepsilon$.

- Scaling window : $L_\varepsilon(\text{SAT}) - L_{1-\varepsilon}(\text{SAT})$
- Sharp transition if for all ε , $\frac{L_\varepsilon(\text{SAT}) - L_{1-\varepsilon}(\text{SAT})}{L_{1/2}(\text{SAT})} \rightarrow 0$
- Coarse (or smooth) transition otherwise.

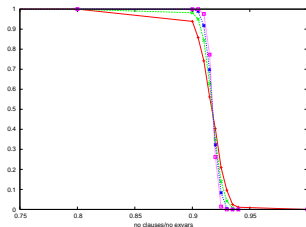
Scaling window for 2-XOR-SAT : Coarse



$$\text{for } n = 5000, \frac{L_{0.2}(\text{SAT}) - L_{0.8}(\text{SAT})}{L_{1/2}(\text{SAT})} = \frac{0.54n - 0.4n}{0.5n} = 0.28$$

$$\text{for } n = 160000, \frac{L_{0.2}(\text{SAT}) - L_{0.8}(\text{SAT})}{L_{1/2}(\text{SAT})} = \frac{0.52n - 0.4n}{0.5n} = 0.24$$

Scaling window for 3-XOR-SAT : sharp

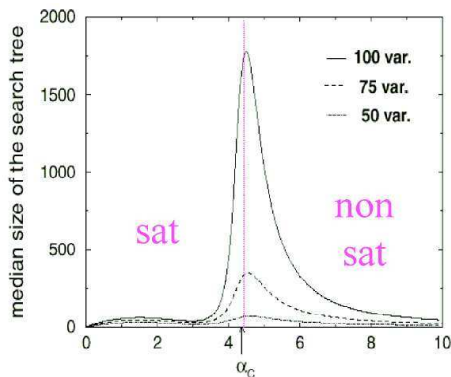


$$\text{for } n = 5000, \frac{L_{0.2}(\text{SAT}) - L_{0.8}(\text{SAT})}{L_{1/2}(\text{SAT})} = \frac{0.093n - 0.91n}{0.918n} = 0.0218$$

$$\text{for } n = 20000, \frac{L_{0.2}(\text{SAT}) - L_{0.8}(\text{SAT})}{L_{1/2}(\text{SAT})} = \frac{0.92n - 0.915n}{0.918n} = 0.005$$

Hard instances

3-SAT has a sharp transition with a critical ratio estimated at 4.25



Random instances are useful to evaluate the performance of SAT solvers : hard instances are at the threshold The now well-known “easy-hard-easy” pattern.

Friedgut and Bourgain's criterion

If the satisfiability property has a coarse threshold, then either :

- C1 **There are “small/simple” minimal unsatisfiable formulas.**
Typically : this is not the case for k -SAT since for any minimal UNSAT formula $|var(F)| < |F|$ (Aharoni, Linial 1985)
- C2 **There are small satisfiable formulas that are boosters for unsatisfiability** (i.e., such that conditioning on the appearance of such a formula as a subformula increases significantly the probability of unsatisfiability).

In order to prove that the transition is sharp, then you have to prove that both $\neg C1$ and $\neg C2$ hold.

Nature of the transition for generalized satisfiability

Formulas can be seen as hypergraphs.

Theorem (Creignou, Daudé 2009)

If every tree-formula and every unicyclic formulas are satisfiable ($\neg C1$), then the satisfiability property has a sharp threshold .

Typical coarse transition : 1-SAT and 2-XOR-SAT.

Critical ratio

In the case of a sharp transition at the scale $L(n) = cn$, it can happen that there is a critical ratio c^* such that :

- $Pr_{n,cn}(\text{SAT}) \xrightarrow[n \rightarrow +\infty]{} 1$ for $c < c^*$, and
- $Pr_{n,cn}(\text{SAT}) \xrightarrow[n \rightarrow +\infty]{} 0$ for $c > c^*$

Friedgut and Bourgain's criterion does not prove the existence of such a critical ratio.

Some results ...

Problem	Scale	Nature	critical ratio	complexity
3-SAT	$L = \theta(n)$	Sharp	$3.52 \leq c_{3\text{-SAT}} \leq 4.4898$	NP-complete
2-SAT	$L = \theta(n)$	Sharp	$c_{2\text{-SAT}} = 1$	P
3-XOR-SAT	$L = \theta(n)$	Sharp	$c_{3\text{-XOR-SAT}} \sim 0.918$	P
2-XOR-SAT	$L = \theta(n)$	Coarse		P
3-NAE-SAT	$L = \theta(n)$	Sharp	$1.5 \leq c_{3\text{-NAE-SAT}} \leq 2.20$	NP-complete

First moment method for an upper bound

Let I be a truth assignment, and X_I be the r.v. such that

$$X_I(F) = 1 \text{ iff } I \models F$$

Let

$$X = \sum_I X_I$$

$$Pr_{n,cn}(3\text{-SAT}) = Pr_{n,cn}(X \geq 1) \leq E(X) \text{ (Markov inequality)}$$

$$E(X) = \sum_I E(X_I) = 2^n \left(\frac{7 \binom{n}{3}}{8 \binom{n}{3}} \right)^L$$

When $L = cn$, we get

$$Pr_{n,cn}(3\text{-SAT}) \xrightarrow{n \rightarrow +\infty} 0, \text{ when } 2 \left(\frac{7}{8} \right)^c < 1,$$

i.e., when $c > \ln 2 / \ln(8/7) \sim 5.19$.

Improvement of the first moment method

Consider satisfiability certificates that are less numerous.

(Dubois, Boufkhad 1996)

Consider locally maximal satisfying assignments only.

Upper bounds for well-known problems

Nom	$c^\#$	c^*
3-SAT	5.19089	4.64248
3-NAE-SAT	2.40942	2.19573
3-XOR-SAT	1.	0.95662
1-in-3-SAT	0.706695	0.61493

(Creignou, Daudé, Dubois, 2007)

Second moment method for a lower bound

Let X_I be the r.v. such that $X_I(F) = 1$ iff $I \models F$, and

$$X = \sum_I X_I$$

$$Pr_{n,cn}(3\text{-SAT}) = Pr_{n,cn}(X \geq 1) = Pr_{n,cn}(X > 0) \geq \frac{(E(X))^2}{E(X^2)}.$$

(Cauchy-Schwarz inequality)

$$\frac{(E_{n,c \cdot n}(X))^2}{E_{n,c \cdot n}(X^2)} \sim 1 \Rightarrow P_{n,c \cdot n}(\text{SAT}) \rightarrow 1.$$

if you know that the transition is sharp, and that $\frac{(E_{n,c \cdot n}(X))^2}{E_{n,c \cdot n}(X^2)} = \Omega(1)$,
then $c^* < c$

Second moment method for a lower bound

Let X_I be the r.v. such that $X_I(F) = 1$ iff $I \models F$, and

$$X = \sum_I X_I$$

$$Pr_{n,cn}(3\text{-SAT}) = Pr_{n,cn}(X \geq 1) = Pr_{n,cn}(X > 0) \geq \frac{(E(X))^2}{E(X^2)}.$$

(Cauchy-Schwarz inequality)

$$\frac{(E_{n,c \cdot n}(X))^2}{E_{n,c \cdot n}(X^2)} \sim 1 \Rightarrow P_{n,c \cdot n}(\text{SAT}) \longrightarrow 1.$$

if you know that the transition is sharp, and that $\frac{(E_{n,c \cdot n}(X))^2}{E_{n,c \cdot n}(X^2)} = \Omega(1)$,
then $c^* < c$

Some lower bounds obtained via the second moment method

- For 3-XOR-SAT we obtain the lower bound : $c_{3\text{-XOR}} \geq 0.889$
- For 3-NAE-SAT we obtain the lower bound : $c_{3\text{-NAE-SAT}} \geq 1.5$
- This method does not work for 3-SAT. However in using

$$Pr_{n,L}(3\text{-SAT}) \leq Pr_{n,L}(3\text{-NAE-SAT})$$

we get that $c_{3\text{-SAT}} \geq 1.5$.

Another method for lower bounds

Analysis of algorithms : choose your favorite algorithm, and try to prove that for some fixed c , it almost surely finds a solution for any formula with cn clauses. Then $c^* > c$.

$$c_{3\text{-SAT}} > 3.52 \text{ (Kaporis, Kirousis, Lalas 2003)}$$

2-SAT

There is a combinatorial characterization of unsatisfiability
“a formula is unsatisfiable iff its implication graph has a strongly connected component that contains both x and $\neg x$ for some variable x ”

- Every 2-CNF-formula that contains a *snake* is unsatisfiable
- Every unsatisfiable formula contains a pure *bicycle*

First moment method and second moment method applied respectively on bicycles and snakes provide resp. lower and upper bounds for the 2-SAT property, and they coincide, $c_{2\text{-SAT}} = 1$!

A threshold phenomenon for 3-SAT

$Pr_{n,cn}(3\text{-SAT})$: probability that a 3-CNF formula over n variables with cn clauses is satisfiable

- The transition from satisfiability to unsatisfiability is sharp (Friedgut, 1998)
- The critical ratio is *estimated* at around 4.25
- Only lower and upper bounds have been established

$$Pr_{n,c \cdot n}(3\text{-SAT}) \rightarrow 1 \text{ for } c \leq 3.52$$

(Kaporis, Kirousis, Lalas, 2003) use the analysis of algorithms

$$Pr_{n,c \cdot n}(3\text{-SAT}) \rightarrow 0 \text{ for } c \geq 4.4898$$

(Diaz, Kirousis, Mitsche, Pérez, 2009)

previously 4.506 (Dubois, Boufkhad, Mandler, 2000)

A threshold phenomenon for 2-SAT

- The transition for 2-SAT is sharp and the critical ratio is 1 (Chvatal & Reed, Goerdts, 1992)
They use first and second moment methods
- The scaling window is known (Bollobàs *et al.*, 2001)
- The probability of satisfiability of a random 2-CNF at the critical ratio $c = 1$ has been experimentally estimated to

$$Pr_{n,n}(2\text{-SAT}) \sim 0.9$$

(Deroulers, Monasson 2006)

What makes the difference (a posteriori) ?

- **There is a simple combinatorial characterization of unsatisfiable 2-CNF formulas :**
 - ▶ 2-SAT is in P
 - ▶ A linear time algorithm allows simulations at a very high scale
 - ▶ For the threshold, one can focus on the emergence of the most likely unsatisfiable formulas in random formulas
- **Such a characterization is missing for 3-CNF formulas :**
 - ▶ 3-SAT is NP-complete.
 - ▶ Simulations are therefore hard to run
 - ▶ For the threshold, no focus on typical unsatisfiable formulas is known

Outline

1 Satisfiability of random CNF-formulas

- Random models
- Nature of the transition
- Location of the transition
- 3-SAT and 2-SAT

2 Quantified satisfiability problems

- QSAT
- (1,2)-QSAT
- Experimental results

QSAT

Input : φ a closed formula of the form $Q_1x_1 Q_2x_2 \dots Q_nx_n \varphi$, where Q_1, \dots, Q_n are arbitrary quantifiers and φ is a CNF-formula

Question : Is φ true ?

- QSAT is PSPACE-complete (ranges over the full polynomial hierarchy depending on the number of quantifier alternations)
- QSAT allows the modelling of various problems (games, model checking, verification, ...)
- QSAT is a monotone property.

QSAT and random instances

- Is there a phase transition for QSAT ?
- What is a "good" probabilistic Model ?
- Is there an easy-hard-easy pattern for random instances ?

(Cadoli et al. 97, Gent and Walsh 99, Chen and Interian 05)

QSAT with one alternation

$$\forall X \exists Y \varphi(X, Y)$$

Deciding the truth value of such a formula is at the second level of the polynomial hierarchy

$$\Pi_2\text{P} = \text{coNP}^{\text{NP}}$$

QSAT only one alternation and k -CNF formulas

$$\forall X \exists Y \varphi(X, Y), \text{ where } \varphi \text{ is } k\text{-CNF}$$

To obtain a random model in which the transition can be observed one has to fix the number u of **universal** variables and the number e of **existential** variables that occur in each clause ($u + e = k$).

(1,2)-QSAT

A **(1,2)-QCNF-formula** is a closed quantified formula of the following type

$$\forall X \exists Y \varphi(X, Y)$$

- X and Y denote distinct sets of variables,
- $\varphi(X, Y)$ is a 3-CNF-formula such that each clause contains exactly 1 variable from X and exactly 2 variables from Y .
- (1,2)-QSAT the property for an (1,2)-QCNF-formula of being true.

An example for a (1,2)-QCNF-formula

- Let $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2, y_3\}$
- $\forall x_1 \forall x_2 \exists y_1 \exists y_2 \exists y_3 (x_1 \vee \bar{y}_1 \vee y_2) \wedge (\bar{x}_2 \vee y_2 \vee y_3) \wedge (\bar{x}_1 \vee \bar{y}_1 \vee \bar{y}_3)$

(1,2)-QSAT and its complexity

Let m be the number of **universal** variables, and n be the number of **existential** variables

- If m is constant, (1,2)-QSAT is solvable in **linear time**
- If $m = \alpha \lceil \log n \rceil$, (1,2)-QSAT is solvable in **polynomial time**
- If $m = n$, then (1,2)-QSAT is **coNP-complete**
(Flögel, Karpinski and Kleine Büning, 1990)

A combinatorial characterization of the truth of a (1,2)-QCNF-formula

A (multi-)set of literals is *pure* if it does not contain both a variable x and its negation \bar{x} .

By extension, we call a (1,2)-QCNF-formula, $F = \forall X \exists Y \varphi(X, Y)$, *pure* if the set of universal literals occurring in φ is pure.

Theorem

A (1,2)-QCNF-formula is false if and only if it contains a false pure subformula (equivalent to a 2-CNF formula).

The interest of (1,2)-QSAT (a priori)

- It is a quantified problem
- Its complexity interpolates between linear and coNP-complete, depending on m , the number of universal variables
- There is a “simple” combinatorial characterization of unsatisfiable (1,2)-QCNF formulas

(1,2)-QCNF((m,n),L)-formulas

- m is the number of universal variables, $\{x_1, \dots, x_m\}$
- n is the number of existential variables, $\{y_1, \dots, y_n\}$
- Random formulas $\forall X \exists Y \varphi(X, Y)$ are obtained by choosing uniformly independently and with replacement L clauses among the $N = 2^3 \binom{m}{1} \binom{n}{2}$ possible clauses.

(1,2)-QSAT and its parameters

- There are 3 parameters to characterize formulas
 - ▶ m is the number of universal variables, $m = m(n)$
 - ▶ n is the number of existential variables
 - ▶ $L = cn$ is the number of clauses
- We are interested in the probability that a randomly chosen formula is true

$$\mathbb{P}_{m,c}(n)$$

- We study

$$\lim_{n \rightarrow +\infty} \mathbb{P}_{m,c}(n)$$

as a function of the parameters m and c

(1,2)-QSAT and its parameters

- There are 3 parameters to characterize formulas
 - ▶ m is the number of universal variables, $m = m(n)$
 - ▶ n is the number of existential variables
 - ▶ $L = cn$ is the number of clauses
- We are interested in the probability that a randomly chosen formula is true

$$\mathbb{P}_{m,c}(n)$$

- We study

$$\lim_{n \rightarrow +\infty} \mathbb{P}_{m,c}(n)$$

as a function of the parameters m and c

Case 1 : m is small enough or big enough

- When m is small enough,

$$m \leq \frac{\log n}{\log 2},$$

there is a sharp threshold at $c = 2$

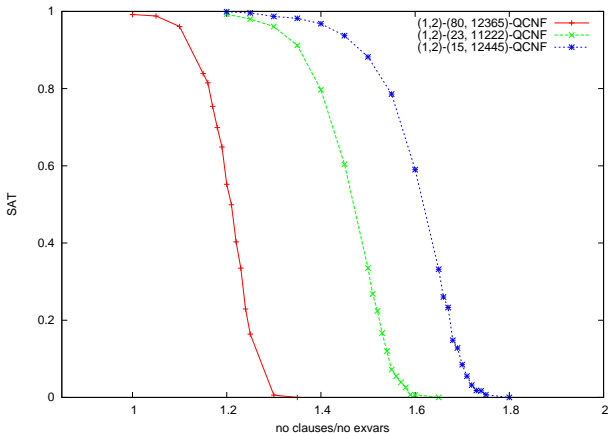
- When m is large enough,

$$m \gg \ln n,$$

there is a sharp threshold at $c = 1$

Case 2 : An intermediate regime when $m = \alpha \lceil \log n \rceil$

When $m = \alpha \lceil \log n \rceil$ the transition occurs for c between 1 and 2



The exact value of the threshold when $m = \lfloor \alpha \ln n \rfloor$

Let $a(\alpha)$ be the solution of the equation $\alpha \cdot H(c) = 1$, where

$$H(c) = \ln(c) + \left(\frac{2}{c} - 1\right) \ln(2 - c)$$

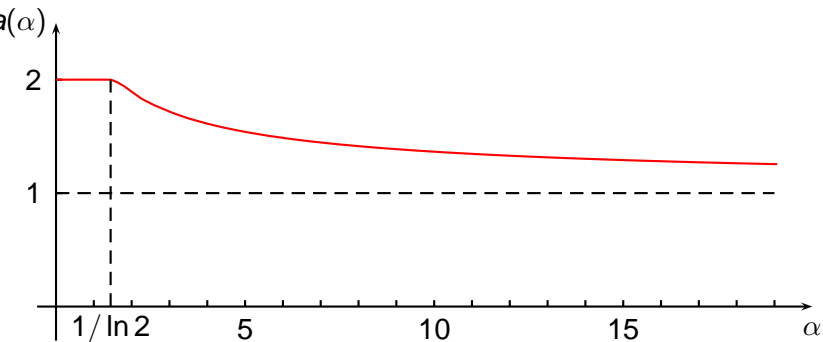
For any $\frac{1}{\ln 2} < \alpha$,

Theorem (Lower and upper bounds match, C. Daudé, Egly, Rossignol, 2009)

- if $c < a(\alpha)$, then $\mathbb{P}_{\lfloor \alpha \ln n \rfloor, c} \xrightarrow{n \rightarrow +\infty} 1$
- if $c > a(\alpha)$, then $\mathbb{P}_{\lfloor \alpha \ln n \rfloor, c} \xrightarrow{n \rightarrow +\infty} 0$.

The exact value of the threshold

We plot the evolution of the critical ratio as a function of α



Proof

- First moment method on the number of pure bicycles in a formula (every unsatisfiable formula contains a pure bicycle).

When $c < a(\alpha)$, there is no pure bicycle

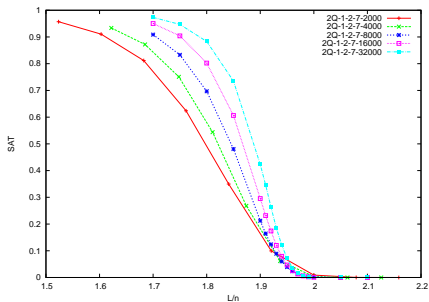
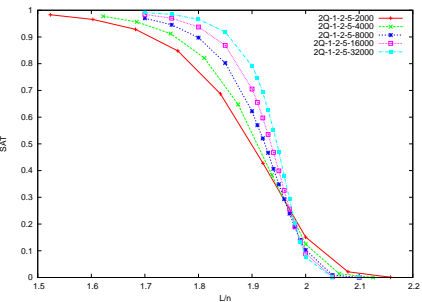
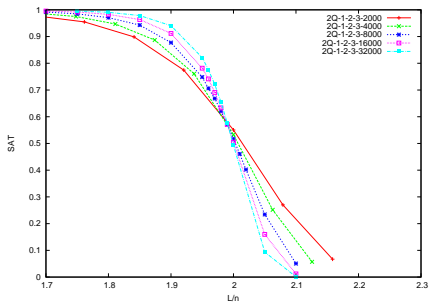
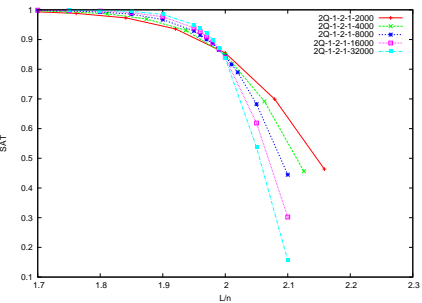
- Second moment method on the number of pure snakes (every formula that contains a snake is false).

When $c > a(\alpha)$, there is a pure snake

Protocol

- One experiment
 - ▶ Fix values for m (\forall -vars) and n (\exists -vars) and $c = L/n$
 - ▶ Generate at random (in drawing uniformly and independently) (1,2)-QCNF formulas for m , n and c
- For each value of c , a sample of 100,000 formulas was studied using the QBF solver QuBE (Giunchiglia et al., 2001), thus computing the truth value of each formula
- The proportion of true (or satisfiable) instances for each considered value of c was then plotted.
- Varying c results in a “satisfiability curve” for m and n

Curves for $m = 1, 3, 5, 7$ and various n

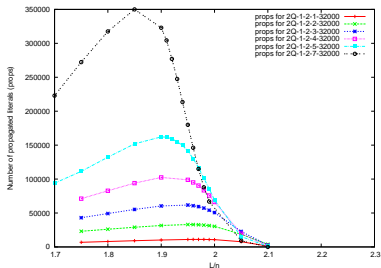
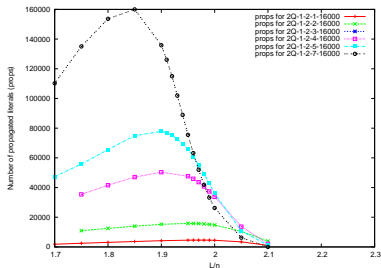


Limits of the experiments

- The critical value is difficult to estimate from the experiments as m increases for two reasons :
 - ▶ The probability of SAT for critical formulas vanishes to 0
 - ▶ The asymptotical regime is reached at a higher scale
- Therefore, simulations are valuable for having an intuition on the behavior of random instances
- But they are inappropriate to get reliable estimates of the critical ratio

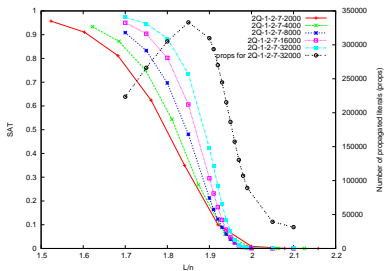
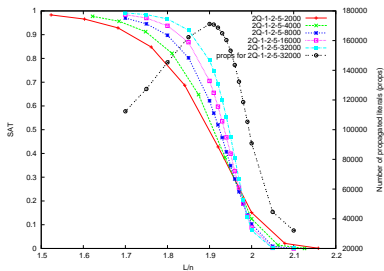
Computational effort

- Computational effort : number of propagations of literals per formula
- Where is the computational effort for deciding the truth value of a random formula maximized ?



Easy-hard-easy pattern

The peak in computational effort coincides with the phase transition



Conclusion

- (1,2)-QSAT has a sharp transition.
- When $m = \lfloor \alpha \ln n \rfloor$, we give the exact location of the threshold as a function of α , $a(\alpha)$
- The peak of the computational effort occurs within the phase transition, with an “easy-hard-easy” pattern.

Challenges

- Getting precise experimental results in order to estimate the critical ratio, or the width of the transition as in [Wilson-02](#) (much more computational power or new forms of simulation).
- Obtaining similar results (sharpness, lower and upper bounds) for a more elaborated quantified problem (Specialize Friedgut-Bourgain's criterion ? find some appropriate candidates for the first and second moment methods ? innovative ideas ?)