

EXACT LOCATION OF THE PHASE TRANSITION FOR RANDOM (1,2)-QSAT^{*,**}

NADIA CREIGNOU¹, HERVÉ DAUDÉ², UWE EGLY³
AND RAPHAËL ROSSIGNOL^{4,5}

Abstract. The QSAT problem is the quantified version of the SAT problem. We show the existence of a threshold effect for the phase transition associated with the satisfiability of random quantified boolean CNF formulas of the form $\forall X \exists Y \varphi(X, Y)$, where X has m variables, Y has n variables and each clause in φ has one literal from X and two from Y . For such formulas, we show that the threshold phenomenon is controlled by the ratio between the number of clauses and the number n of existential variables. Then we give the exact location of the associated critical ratio c^* : it is a decreasing function of α , where α is the limiting value of $m/\log(n)$ when n tends to infinity. Thus we give a precise location of the phase transition associated with a coNP-complete problem.

Mathematics Subject Classification. 68R01, 60C05, 05A16.

Keywords and phrases. Random quantified formulas, satisfiability, phase transition, sharp threshold.

* *Research supported by the Agence Nationale de la Recherche, ANR 2011 BS01 007 01, and by the Austrian Science Fund (FWF) under grant S11409-N23.*

** *Preliminary versions of this article appeared in [6] and [7].*

¹ Aix-Marseille Université, CNRS, LIF UMR 7279, 13288 Marseille, France.
creignou@lif.univ-mrs.fr

² Aix-Marseille Université, CNRS, I2M UMR 7373, 13453 Marseille, France.
daude@cmi.univ-mrs.fr

³ Institut für Informationssysteme 184/3, Technische Universität Wien, Favoritenstrasse 9-11 A-1040 Wien, Austria. uwe@kr.tuwien.ac.at

⁴ University Grenoble Alpes, IF, 38000 Grenoble, France.

⁵ CNRS, IF, 38000 Grenoble, France. raphael.rossignol@ujf-grenoble.fr

1. INTRODUCTION

A significant tool for SAT research has been the study of random instances. In the last decades, numerous experimental studies have provided strong evidence that the difficulty to solve large instances of k -SAT is tightly linked to a phase transition in the probability that a random instance is satisfiable (see *e.g.* [15]). As the clauses-to-variables ratio increases, the vast majority of formulas abruptly stop being satisfiable at a critical threshold point. The instances that are hard to solve seem to be located around this critical point. Determining the nature of the phase transition, locating it, determining a precise scaling window and gaining a better understanding of the structure of the space of solutions turn out to be challenging tasks, which have aroused a lot of interest and fruitful collaborations among different disciplines, namely combinatorics, probability, computer science and statistical physics.

Recently there has been a growth of interest in a powerful generalization of the Boolean satisfiability, namely the satisfiability of Quantified Boolean formulas, QBFs. Compared to the well-known propositional formulas, QBFs permit both universal and existential quantifiers over Boolean variables. Thus QBFs allow the modeling of problems having higher complexity than SAT, ranging in the polynomial hierarchy up to PSPACE. These problems include problems from the areas of verification, knowledge representation and logic (see, *e.g.* [10]). Models for generating random instances of QBF have been proposed [3, 12]. Problems for which one can combine practical experiments with theoretical studies are natural candidates for first investigations [5]. In this paper, we focus on a certain subclass of closed quantified Boolean formulas. We are interested in closed formulas in conjunctive normal form, (1,2)-QCNF, having two quantifier blocks. More precisely, we consider formulas of the type $\forall X \exists Y \varphi(X, Y)$, where X and Y denote distinct sets of variables, and $\varphi(X, Y)$ is a conjunction of 3-clauses, each of which containing exactly one universal literal and two existential ones. These formulas are closely linked to 2-CNF-formulas, whose random instances have been extensively studied in the literature (see, *e.g.* [2, 4, 8, 13, 17, 18]). However, the introduction of quantifiers increases the complexity (from linear time solvable [1] up to coNP-complete [11]) and requires additional parameters for the generation of random instances. The first one is the pair (m, n) that specifies the number of variables in each quantifier block, *i.e.* in X and Y . The second one is $L = \lfloor cn \rfloor$, the number of clauses. We shall study the probability that a formula drawn at random uniformly out of this set of formulas evaluates to true as n tends to infinity. We will denote by $\mathbb{P}_{m,c}(n)$ this probability. Thus, we are interested in

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

Let us recall that the transition from satisfiability to unsatisfiability for random 2-CNF formulas is sharp. Indeed, there is a *critical value* (or a *threshold*) of the ratio of the number of clauses to the number of variables, above which the likelihood of a random 2-CNF-formula being satisfiable vanishes as n tends to

infinity, and below which it goes to 1. Moreover, this critical value is known to be 1 (see [4, 13]).

For random (1,2)-QCNF-formulas, the transition from satisfiability to unsatisfiability depends on the number of universal variables. Indeed, on the one hand observe that, when there is only one universal variable *i.e.* when $m = 1$, a (1,2)-QCNF-formula with L clauses can be seen as the conjunction of two nearly independent 2-CNF-formulas (each of which corresponds to an assignment to the universal variable and has on average $L/2$ clauses). On the other hand, when m is large enough, a random (1,2)-QCNF-formula with $L = \lfloor cn \rfloor$ clauses has essentially distinct universal variables, and then behaves as an existential 2-CNF-formula.

Thus, in a first step, we prove that the transition between satisfiability and unsatisfiability for random (1,2)-QCNF-formulas occurs when c is between 1 and 2. Second, we identify a window for m in which the introduction of universal variables makes the critical ratio vary from 2 to 1. Our main contribution consists in proving that the logarithmic scale, $m = \lfloor \alpha \log n \rfloor$, is the right one in order to observe the evolution of the critical ratio associated to the (1,2)-QSAT phase transition. Indeed, we obtain the precise location of the critical ratio as a function of α :

Theorem 1.1. *For any real $\alpha > 0$, there exists $c^*(\alpha) \in [1, 2]$ such that:*

- if $c < c^*(\alpha)$, then $\mathbb{P}_{\lfloor \alpha \log n \rfloor, c}(n) \xrightarrow[n \rightarrow +\infty]{} 1$,
- if $c > c^*(\alpha)$, then $\mathbb{P}_{\lfloor \alpha \log n \rfloor, c}(n) \xrightarrow[n \rightarrow +\infty]{} 0$.

Let K be the binary entropy function: $K(x) = -x \log x - (1-x) \log(1-x)$ then, the critical ratio $c^*(\alpha)$ is given by

$$c^*(\alpha) = \begin{cases} 2 & \text{if } \alpha \leq 1 \\ \text{the unique root } c \in]1, 2[\text{ of } \alpha(1 - K(c/2)) = c/2 & \text{if } \alpha > 1 \end{cases}$$

Figure 1 makes the link between $c^*(\alpha)$ and the binary entropy function. Figure 2 shows the continuous evolution of the critical ratio $c^*(\alpha)$ as a function of α with $\lim_{\alpha \rightarrow 1^+} c^*(\alpha) = c^*(1) = 2$ and $\lim_{\alpha \rightarrow +\infty} c^*(\alpha) = 1$.

In addition we show (see Prop. 3.5) that at a sub-logarithmic scale for m , *i.e.* for $m \ll \log n$, the critical ratio is equal to 2, whereas for $m \gg \log n$, the critical ratio is equal to 1.

The paper is organized as follows. In Section 2 we present our combinatorial and probabilistic models. In Section 3 we give first estimates for the critical ratio of the phase transition. Section 4 is dedicated to the proof of our main result. In Section 4.1 we introduce specific substructures, namely pure bicycles and pure snakes, whose appearance is respectively necessary and sufficient to ensure falsity of a (1,2)-QCNF formula. In Sections 4.2 and 4.3 we prove lower and upper bounds for the critical ratio based respectively on the first and second moment method on the number of pure bicycles and pure snakes. The details of the proofs are postponed in the subsequent sections, Sections 5 and 6.

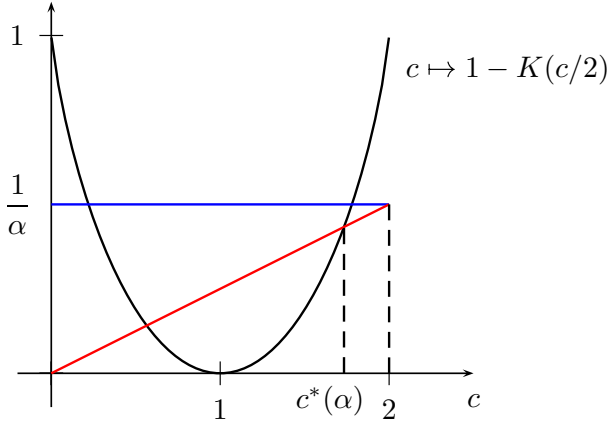


FIGURE 1. Location of the unique root of $\alpha(1 - K(c/2)) = c/2$.

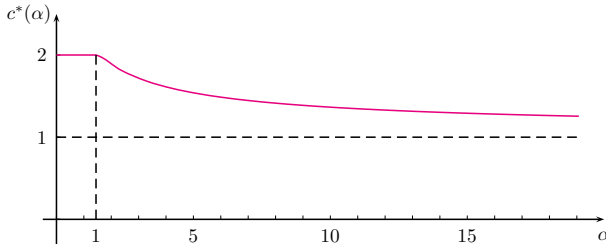


FIGURE 2. Evolution of the critical ratio value.

2. COMBINATORICS AND PROBABILISTIC MODEL

2.1. (1,2)-QCNF FORMULAS

A *literal* l is a propositional variable p or its negation \bar{p} . Literals are said to be *strictly distinct* when their corresponding variables are pairwise different. A *clause* is a finite disjunction of strictly distinct literals. A formula is in *conjunctive normal form* (CNF) if it is a conjunction of clauses. A formula is in k -CNF, if any clause consists of exactly k literals. Here we are interested in quantified propositional formulas of the form

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

where $X = \{x_1, \dots, x_m\}$, and $Y = \{y_1, \dots, y_n\}$, and $\varphi(X, Y)$ is a 3-CNF formula, with exactly one universal and two existential literals in each clause. We denote by $\Omega_{n,m}$ the set of all such formulas that we call (1,2)-QCNFs. These formulas can be considered as quantified extended 2-CNF formulas. Indeed, deleting the only universal literal in each clause and removing the \forall -quantifiers, which then concern variables that do not occur any more in the formula, result in a closed existentially

quantified conjunction of binary clauses. The number of clauses in F (which is also the number of clauses in φ) is denoted by $|F|$ (resp., $|\varphi|$). Given a (1,2)-QCNF-formula $F = \forall X \exists Y \varphi(X, Y)$, we call *subformula of F* any (1,2)-QCNF-formula $F' = \forall X \exists Y \varphi'(X, Y)$, where φ' seen as a set of clauses verifies $\varphi' \subseteq \varphi$.

A *truth assignment* for the universal (resp. existential) variables, X (resp. Y) is a Boolean function $I : X \rightarrow \{0, 1\}$ (resp. $Y \rightarrow \{0, 1\}$), which can be extended to literals by $I(\bar{x}) = 1 - I(x)$.

A (1,2)-QCNF formula is *true* (or *satisfiable*) if for every assignment to the variables X , there exists an assignment to the variables Y such that φ is true under this assignment. We denote by (1,2)-QSAT the property for a (1,2)-QCNF formula to be true. Note that the worst-case complexity of deciding whether a (1,2)-QCNF formula is true is known, it is coNP-complete (see [11]).

To any (1,2)-QCNF formula F , we can associate two existential formulas, which will be useful in the forthcoming analysis.

Definition 2.1. For any (1,2)-QCNF-formula F , let us denote by:

- F_Y , the existential 2-CNF formula obtained from F in removing the universal literal in each clause of F and then deleting the universal quantifiers.
- F_t , the 2-CNF formula obtained from F in setting all the universal variables to *true*, simplifying the resulting clauses with respect to truth constants and omitting all quantifiers.

Clearly we have

Lemma 2.2.

- $F_Y \in 2\text{-SAT} \implies F \in (1,2)\text{-QSAT}$.
- $F \in (1,2)\text{-QSAT} \implies F_t \in 2\text{-SAT}$.

2.2. PROBABILISTIC, MODEL

We consider formulas built on m universal variables, $\{x_1, \dots, x_m\}$, and n existential variables $\{y_1, \dots, y_n\}$. Thus the number of different (1,2)-clauses we can construct is a function of n and m :

$$N = N_m(n) = m \binom{n}{2} 2^3 = 8m \binom{n}{2} = 4mn(n-1).$$

We consider random formulas obtained by taking each one of the N possible clauses independently from the others with probability $p \in]0, 1[$, we call $\mathcal{F}_{n,m,p}$ this set of formulas. Thus, given a (1,2)-QCNF formula $F \in \{0, 1\}^{N_m}$ we have

$$\mu_{p,n,m}(F) = p^{|F|} (1-p)^{N_m - |F|}.$$

We denote by $\mu_{p,n,m}((1,2)\text{-QSAT})$ the probability that a random formula in this model evaluates to true. This model relates to the well-know model for random

2-CNFs as follows. Let ϕ be a 2-CNF formula over n variables $\{y_1, \dots, y_n\}$, $\phi \in \{0, 1\}^{4\binom{n}{2}}$, we set

$$\mu_{p,n,1/2}(\phi) = p^{|\phi|}(1-p)^{4\binom{n}{2}-|\phi|}.$$

We denote by $\mu_{p,n,1/2}(2\text{-SAT})$ the probability that a random 2-CNF formula in this model is satisfiable.

The mean of the number of clauses that occur in a random (1,2)-QCNF formula is $N \cdot p$. Therefore, for all $c > 0$, $\mathbb{E}_{p,n,m}(|F|) = cn$ if and only if $p = \frac{L}{4mn(n-1)}$. It is well known, see for instance [14], Sections 1.4 and 1.5, that this model and the model alluded to in the introduction – in which $L = \lfloor cn \rfloor$ distinct clauses are picked uniformly at random among all the N possible choices – are asymptotically equivalent, provided $p = \frac{L}{4mn(n-1)}$.

As a consequence we set

$$\mathbb{P}_{m,c}(n) = \mu_{\frac{c}{4m(n-1)},n,m}((1,2)\text{-QSAT}),$$

and

$$\mathbb{P}_{1/2,c}(n) = \mu_{\frac{c}{2(n-1)},n,\frac{1}{2}}(2\text{-SAT}).$$

We are interested in studying $\lim_{n \rightarrow +\infty} \mathbb{P}_{m,c}(n)$ as a function of the parameters m and c , where m is a positive, integer-valued function of n . As (1,2)-QSAT is a decreasing property, $\mathbb{P}_{m,c}(n)$ is a decreasing function of c . Any value of c such that $\mathbb{P}_{m,c}(n) \rightarrow 1$ (resp. such that $\mathbb{P}_{m,c}(n) \rightarrow 0$) makes precise the location of the transition between SATisfiability and UNSATisfiability.

3. FIRST ESTIMATES OF THE (1,2)-QSAT PHASE TRANSITION

The phase transition for 2-SAT is well-known:

Theorem 3.1. ([4])

- $\forall c > 1, \mathbb{P}_{1/2,c}(n) = o(1)$.
- $\forall c < 1, \mathbb{P}_{1/2,c}(n) = 1 - o(1)$.

Thus there is a threshold effect for 2-SAT with an associated critical ratio $c = 1$. Our goal is to show that such an effect exists for (1,2)-QSAT with an associated ratio that depends on m , the number of universal variables. For such m , any value of c such that $\mathbb{P}_{m,c}(n) \rightarrow 1$ (resp. such that $\mathbb{P}_{m,c}(n) \rightarrow 0$) will provide a lower (resp. upper) bound for the critical ratio associated to the satisfiability of random (1,2)-QCNF formulas. We first prove that for any m this critical ratio is between 1 and 2.

Proposition 3.2.

- For all m , for all $c > 2, \mathbb{P}_{m,c}(n) = o(1)$.
- For all m , for all $c < 1, \mathbb{P}_{m,c}(n) = 1 - o(1)$.

Proof. Let F be a random (1,2)-QCNF formula, F_Y and F_t being the two associated 2-CNF formulas as defined in Definition 2.1.

For any 2-CNF formula ϕ we have

$$\mu_{p,n,m}(F_Y = \phi) = (1 - (1 - p)^{2m})^{|\phi|} (1 - p)^{N_m - 2m|\phi|} = \mu_{1-(1-p)^{2m},n,1/2}(\phi).$$

According to Lemma 2.2 we get

$$\mu_{p,n,m}(F \in (1,2)\text{-QSAT}) \geq \mu_{p,n,m}(F_Y \in \text{SAT}) \geq \mu_{1-(1-p)^{2m},n,1/2}(2\text{-SAT}).$$

If $N_m \cdot p = cn$, i.e. $4mn(n-1)p = cn$, then $4\binom{n}{2}(1 - (1-p)^{2m}) \sim cn$ since $1 - (1-p)^{2m} \sim 2mp$. Thus, if $c < 1$, then according to Proposition 3.1,

$$\mu_{1-(1-p)^{2m},n,1/2}(2\text{-SAT}) = 1 - o(1),$$

and hence $\mu_{p,n,m}(F \in (1,2)\text{-QSAT}) = 1 - o(1)$. This proves that for all $c < 1$, $\mathbb{P}_{m,c}(n) = 1 - o(1)$.

Now observe that

$$\mu_{p,n,m}(F_t = \phi) = (1 - (1 - p)^m)^{|\phi|} (1 - p)^{N_m/2 - m|\phi|} = \mu_{1-(1-p)^m,n,1/2}(\phi).$$

According to Lemma 2.2 we get

$$\mu_{p,n,m}(F \in (1,2)\text{-QSAT}) \leq \mu_{p,n,m}(F_t \in \text{SAT}) \leq \mu_{1-(1-p)^m,n,1/2}(2\text{-SAT}).$$

If $N_m \cdot p = cn$, i.e. $4mn(n-1)p = cn$, then $4\binom{n}{2}(1 - (1-p)^m) \sim \frac{c}{2}n$. Thus, if $c > 2$, then according to Proposition 3.1, $\mu_{1-(1-p)^m,n,1/2}(2\text{-SAT}) = o(1)$, and hence $\mu_{p,n,m}(F \in (1,2)\text{-QSAT}) = o(1)$. This proves that for all $c > 2$, $\mathbb{P}_{m,c}(n) = o(1)$. \square

Thus, we can define:

- $c_m^+ = \inf\{c > 0 \text{ such that } \mathbb{P}_{m(n),c}(n) = o(1)\}$.
- $c_m^- = \sup\{c > 0 \text{ such that } \mathbb{P}_{m(n),c}(n) = 1 - o(1)\}$.

With this notation we get as a corollary of Proposition 3.2

Corollary 3.3. $1 \leq c_m^- \leq c_m^+ \leq 2$.

Our main task is to measure the influence of introducing universal variables on the location of the transition. The first step is to show that the more we introduce universal variables, the less the associated critical ratio is.

Proposition 3.4. *If $m_1 \ll m_2$ then $c_{m_1}^+ \geq c_{m_2}^+$, and $c_{m_1}^- \geq c_{m_2}^-$.*

Proof. Let $q = m_2 \operatorname{div} m_1$ and $r = m_2 \bmod m_1$, i.e. $m_2 = qm_1 + r$. Note that if $m_1 \ll m_2$, then $r \ll m_2$. From a formula $F \in \Omega_{n,m_2}$, we construct a formula $\tilde{F} \in \Omega_{n,m_1}$ as follows: we replace in F all x_i 's by $x_{((i-1) \bmod m_1)+1}$ for $i \leq qm_1$,

and we delete all clauses that contain some x_i for $i > qm_1$. Observe that $F \in (1,2)\text{-QSAT} \implies \tilde{F} \in (1,2)\text{-QSAT}$, therefore

$$\mu_{n,m_2,p}(F \in (1,2)\text{-QSAT}) \leq \mu_{n,m_2,p}(F \text{ s.t. } \tilde{F} = F_0, F_0 \in \Omega_{n,m_1}, F_0 \in (1,2)\text{-QSAT}).$$

Observe that

$$\mu_{n,m_2,p}(F \text{ s.t. } \tilde{F} = F_0) = (1 - (1-p)^q)^{|F_0|} (1-p)^{qN_{m_1} - q|F_0|} = \mu_{n,m_1,1-(1-p)^q}(F_0).$$

Therefore

$$\mu_{n,m_2,p}((1,2)\text{-QSAT}) \leq \mu_{n,m_1,1-(1-p)^q}((1,2)\text{-QSAT}). \quad (3.1)$$

Observe that $N_{m_1}(1 - (1-p)^q) \sim N_{m_1}qp$. But, $\frac{qN_{m_1}}{N_{m_2}} = \frac{qm_1}{m_2} = 1 - \frac{r}{m_2} \sim 1$ since $r \ll m_2$. Thus, $N_{m_1}(1 - (1-p)^q) \sim N_{m_2}p$. Hence if $N_{m_2}p = cn$, then $N_{m_1}(1 - (1-p)^q) \sim cn$. From this and (3.1) we can deduce, as in the proof of Proposition 3.2 that $c_{m_1}^+ \geq c_{m_2}^+$, and $c_{m_1}^- \geq c_{m_2}^-$. \square

Observe that Theorem 1.1, together with the fact that $\lim_{\alpha \rightarrow 0^+} c^*(\alpha) = 2$ and $\lim_{\alpha \rightarrow +\infty} c^*(\alpha) = 1$, and Proposition 3.4 give the following proposition.

Proposition 3.5. *Let $m = m(n)$ be a sequence of positive integers.*

- *If $m \ll \log n$, then $c_m^+ = c_m^- = 2$.*
- *If $m \gg \log n$, then $c_m^- = c_m^+ = 1$.*

Notice that Proposition 3.5 together with Theorem 1.1 provide a complete description of the evolution of the critical ratio associated to the phase transition of (1,2)-QSAT.

4. PROOF OF THEOREM 1.1

4.1. PURE QUANTIFIED FORMULAS

In our analysis pure quantified formulas, which are defined below, will play a central role.

Definition 4.1. 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.

Proposition 4.2. *Let F be a pure (1,2)-QCNF-formula, then*

$$F \in (1,2)\text{-QSAT} \iff F_Y \in 2\text{-SAT}.$$

Moreover, we have the following.

Proposition 4.3. *A (1,2)-QCNF-formula is false if and only if it contains a false pure subformula.*

Proof. Suppose that the (1,2)-QCNF-formula $F = \forall X \exists Y \varphi(X, Y)$ is false. Then, there is an assignment I to the universal variables X such that for all assignment to the existential variables Y , φ evaluates to false. Consider the subformula of F obtained in keeping only the clauses for which the universal literal is assigned 0 by I , and deleting the other ones. This subformula is pure (it cannot contain both a clause with a universal variable x and another with \bar{x} since either x or \bar{x} is assigned 1 by I), and is false by the choice of I . The converse direction is obvious. \square

In order to investigate the phase transition of random 2-SAT formulas, Chvátal and Reed [4] identified appropriate witnesses for unsatisfiability. They showed that every unsatisfiable formula contains a *bicycle* and that every *snake* is an unsatisfiable formula. In the context of quantified formulas, let us define pure versions of these specific structures.

Definition 4.4. A pure *snake* of length $s + 1 \geq 4$, with $s + 1 = 2t$, is a set of $s + 1$ clauses C_0, \dots, C_s which have the following structure: there is a sequence of s strictly distinct existential literals w_1, \dots, w_s , and a pure sequence of $s + 1$ universal literals v_0, \dots, v_s such that, for every $0 \leq r \leq s$, $C_r = (v_r \vee \overline{w_r} \vee w_{r+1})$ with $w_0 = w_{s+1} = \overline{w_t}$.

Definition 4.5. A *pure bicycle* of length $s + 1 \geq 3$, is a set of $s + 1$ clauses C_0, \dots, C_s which have the following structure: there is a sequence of s strictly distinct existential literals w_1, \dots, w_s , and a pure sequence of $s + 1$ universal literals v_0, \dots, v_s such that, for $0 < r < s$, $C_r = (v_r \vee \overline{w_r} \vee w_{r+1})$, $C_0 = (v_0 \vee u \vee w_1)$ and $C_s = (v_s \vee \overline{w_s} \vee v)$ with literals u and v chosen from $w_1, \dots, w_s, \overline{w_1}, \dots, \overline{w_s}$ with $(u, v) \neq (\overline{w_s}, w_1)$.

From [4] and Proposition 4.2 we get the following proposition.

Proposition 4.6.

- Every (1,2)-QCNF-formula that contains a pure snake is false.
- Every (1,2)-QCNF-formula that is false, contains a pure bicycle.

4.2. A LOWER BOUND FOR THE CRITICAL RATIO

From now on we will concentrate on the case where $m = \lfloor \alpha \log n \rfloor$ with $\alpha > 0$.

We obtain a lower bound for the satisfiability threshold by applying the first moment method to pure bicycles.

Let \mathcal{B}_s be the set of all pure bicycles of length $s + 1$. We define the random variables B_s and B over the set of formulas $\mathcal{F}_{n,m,p}$ as $B_s(F) = \sum_{b \in \mathcal{B}_s} 1_{[b \subseteq F]}$ and $B = \sum_{s+1 \geq 3} B_s$.

The following inequality is an immediate consequence of Proposition 4.6.

$$1 - \mathbb{P}_{m,c}(n) \leq \Pr(B \geq 1) \leq \mathbb{E}_{m,c}(B). \quad (4.1)$$

We will soon understand that it is always sufficient to evaluate moments up to a polylogarithmic factor in n . Thus, when a_n and b_n are two quantities depending on n we shall use the following notation:

$$a_n \lesssim b_n,$$

when there is a positive constant τ such that for every n large enough,

$$a_n \leq (\ln n)^\tau b_n.$$

and we shall write $a_n \equiv b_n$ if $a_n \lesssim b_n$ and $b_n \lesssim a_n$. Furthermore, when the quantities a_n and b_n depend on some extra parameters β and γ restricted to some space \mathcal{D} (as in Prop. 5.6) the constant τ above will be implicitly understood as uniform over all choices of the parameters in \mathcal{D} .

For all $\alpha > 1$, let $c^*(\alpha)$ denotes the unique root in $]1, 2[$ of $\alpha(1 - K(c/2)) = c/2$, which is also the unique root in $]1, 2[$ of $H(c) = \frac{1}{\alpha}$, where

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

Proposition 4.7. *Let $m = \lfloor \alpha \log n \rfloor$ with $\alpha > 0$. For all $c \in]1, 2[$,*

- $\sum_{s \geq \frac{2m}{\log(2/c)}} \mathbb{E}_{m,c}(B_s) = o(1)$,
- if $\alpha \leq 1$, then $\mathbb{E}_{m,c}(B) = o(1)$,
- if $\alpha > 1$, then $\mathbb{E}_{m,c}(B) = n^{\alpha H(c) - 1} + o(1)$.

The proof of this proposition is given in Section 5. As a corollary we get:

Corollary 4.8. *Let $m = \lfloor \alpha \log n \rfloor$, then*

- If $\alpha \leq 1$, then $c^-(m) = c^+(m) = 2$.
- If $\alpha > 1$, then $c^-(m) \geq c^*(\alpha)$.

Proof. The first item follows from the second item of the above proposition together with (4.1). For the second one, observe that $\alpha H(c) - 1 < 0$ when $c < c^*(\alpha)$. \square

4.3. AN UPPER BOUND FOR THE CRITICAL RATIO

The upper bound is obtained by the second moment method applied to pure snakes.

Let \mathcal{X}_s be the set of all pure snakes of length $s + 1$ and $\mathcal{X}_{s,k}$ be the set of all pure snakes of length $s + 1$ with k strictly distinct universal literals. We define the

associated random variables X_s and $X_{s,k}$ over the set of formulas $\mathcal{F}_{n,m,p}$ as in the previous section. Thus, $X_s = \sum_k X_{s,k}$.

By the second moment bound and Proposition 4.6 we get for every s :

$$1 - \mathbb{P}_{m,c}(n) \geq 1 - \Pr(X_s = 0) \geq \frac{\mathbb{E}(X_s)^2}{\mathbb{E}(X_s^2)}. \quad (4.2)$$

We first obtain the following concentration result.

Proposition 4.9. *For all $c \in]1, 2[$ and all $\alpha > 1$ such that $\alpha H(c) - 1 > 0$, if $\widehat{s} = \lfloor \frac{-2\alpha \ln(2-c)}{c} \ln n \rfloor$, then*

$$\frac{\mathbb{E}(X_{\widehat{s}})^2}{\mathbb{E}(X_{\widehat{s}}^2)} = 1 - o(1).$$

The proof of this proposition is given in Section 6.

From (4.2), we get the following.

Corollary 4.10. *If $m = \lfloor \alpha \log n \rfloor$ with $\alpha > 1$, then $c^+(m) \leq c^*(\alpha)$.*

Corollaries 4.8 and 4.10 prove our main result, Theorem 1.1.

5. PROOF OF PROPOSITION 4.7

The proof will be decomposed into three propositions, each of them corresponding to one of the items of the proposition.

We shall drop the subscript m, c in the expectations to lighten the notation.

Since $\mathbb{E}(B_s) = p^{s+1} |\mathcal{B}_s|$, and thus $\mathbb{E}(B) = \sum_{s+1 \geq 3} p^{s+1} |\mathcal{B}_s|$ it is clear that the proof requires estimations of $|\mathcal{B}_s|$. We introduce $\mathcal{B}_{s,k}$ the set of pure bicycles of length $s+1$ with k distinct universal variables, and denote by $B_{s,k}$ the associated random variable. Thus, $B_s = \sum_k B_{s,k}$.

Let us first state a useful combinatorial lemma.

Lemma 5.1.

$$|\mathcal{B}_s| = ((2s-1)^2 - 1)(n)_s 2^s d(m, s+1),$$

with

$$d(m, s+1) = \sum_{k=1}^{\min(m, s+1)} \binom{m}{k} \cdot 2^k \cdot \mathcal{S}(s+1, k) \cdot k!,$$

where $\mathcal{S}(s+1, k)$ are Stirling numbers of the second kind. Moreover,

$$d(m, s+1) \leq 2^{\min\{m, s+1\}} m^{s+1}.$$

Proof. The enumeration of bicycles of size $s+1$ is similar to the one made in [4], here in addition we have to enumerate the pure sequence of $s+1$ universal literals. Therefore we make a case distinction according to k the number of distinct universal variables that occur, hence considering $\mathcal{B}_{s,k}$. Let us recall that $\mathcal{S}(m, k) \cdot k!$

is the number of applications from a set of m elements onto a set of k elements. A pure sequence of literals of length $s + 1$ is obtained by exactly one sequence of choices of the following choosing process.

- (1) Choose the number k of different variables occurring in the sequence.
- (2) Choose the k variables.
- (3) For each such variable, choose whether it occurs positively or negatively.
- (4) Choose their places in the sequence.

This gives

$$|\mathcal{B}_{s,k}| = [(2(s-1))^2 - 1](n)_s 2^s \binom{m}{k} \cdot 2^k \cdot \mathcal{S}(s+1, k),$$

and the expression for $|\mathcal{B}_s|$ follows in summing over all possible k .

Observe that $d(m, s+1)$ is bounded from above by $2^{\min\{m, s+1\}}$ times the number of applications from $\{1, \dots, s+1\}$ to $\{1, \dots, m\}$. Therefore,

$$d(m, s+1) \leq 2^{\min\{m, s+1\}} m^{s+1}. \quad \square$$

The following proposition deals with the first item of Proposition 4.7.

Proposition 5.2. *For all $c \in]1, 2[$ and all m ,*
$$\sum_{s \geq \frac{2m}{\log(2/c)}} \mathbb{E}_{m,c}(B_s) = o(1).$$

Proof. According to Lemma 5.1,

$$\mathbb{E}(B_s) = ((2s-1)^2 - 1)(n)_s 2^s d(m, s+1) p^{s+1}, \text{ where } p = \frac{c}{4mn}.$$

Since $0 < \log(2/c) < 1$ for $1 < c < 2$, if $s \geq \frac{2m}{\log(2/c)}$ we have $m \leq \frac{s}{2} \log(2/c) \leq s/2$, and thus $d(m, s+1) \leq 2^m m^{s+1}$. Hence

$$\begin{aligned} \mathbb{E}(B_s) &\leq \frac{c}{n} \left(\frac{c}{2}\right)^s s^2 2^m. \\ \sum_{s \geq \frac{2m}{\log(2/c)}} \mathbb{E}(B_s) &\leq \frac{c}{n} 2^m \sum_{s \geq \frac{2m}{\log(2/c)}} s^2 \left(\frac{c}{2}\right)^s \\ &\leq \frac{c 2^m}{n} \left(\frac{2m}{\log(2/c)}\right)^2 \frac{(c/2)^{\frac{2m}{\log(2/c)}}}{(1-c/2)^3} \\ &\lesssim \frac{m^2 2^m}{n} (c/2)^{\frac{2m}{\log(2/c)}} \\ &\lesssim \frac{m^2 2^m}{n} \exp(-2m \ln 2) \\ &\lesssim \frac{m^2 2^{-m}}{n} = o(1). \quad \square \end{aligned}$$

Proposition 5.3. *If $\alpha \leq 1$, then for all $c \in]1, 2[$, $\mathbb{E}_{m,c}(B) = o(1)$.*

Proof. If $m \leq s + 1$, then $d(m, s + 1) \leq 2^m m^{s+1}$ and

$$\begin{aligned} \mathbb{E}(B_s) &\leq ((2s - 1)^2 - 1)(n)_s 2^s 2^m m^{s+1} \frac{c^{s+1}}{4^{s+1} m^{s+1} n^{s+1}} \\ &\leq \frac{2^m c s^2}{n} \left(\frac{c}{2}\right)^s. \end{aligned}$$

Thus,

$$\sum_{m \leq s+1} \mathbb{E}(B_s) \leq \frac{2^m c}{n} \sum_{s \geq m-1} s^2 \left(\frac{c}{2}\right)^s.$$

Standard computations when $0 < x < 1$ and $r \geq 2$, show that

$$\sum_{s=r}^{\infty} s^2 x^s \leq r^2 \frac{x^r}{(1-x)^3}.$$

Hence we get

$$\begin{aligned} \sum_{s \geq m-1} \mathbb{E}_{m,c}(B_s) &\leq \frac{c 2^m}{n} (m-1)^2 \frac{\left(\frac{c}{2}\right)^{m-1}}{(1-c/2)^3}, \text{ for } 0 < c < 2, \text{ and } m \geq 3 \\ &\leq \frac{2c^m}{n} (m-1)^2 \frac{1}{(1-c/2)^3}. \end{aligned} \quad (5.1)$$

If $m > s + 1$, then $d(m, s + 1) \leq 2^{s+1} m^{s+1}$ and

$$\mathbb{E}(B_s) \leq 4s^2 (n)_s 2^s 2^{s+1} m^{s+1} \frac{c^{s+1}}{4^{s+1} m^{s+1} n^{s+1}} \leq \frac{2s^2}{n} c^{s+1}.$$

Hence we get

$$\begin{aligned} \sum_{s \leq m-2} \mathbb{E}_{m,c}(B_s) &\leq \frac{2c}{n} \sum_{s \leq m-2} s^2 c^s \\ &\leq \frac{m^2 2c}{n} \sum_{s \leq m-2} c^s \\ &\leq \frac{2cm^3 \max(c^m, 1)}{n}. \end{aligned} \quad (5.2)$$

Now, for $m \leq \log(n)$, observe that since $\frac{c^m}{n} = \exp(m \ln c - \ln n)$, we have $m \ln c \leq \frac{\ln c}{\ln 2} \ln n$. Thus,

$$\frac{c^m}{n} \leq \exp\left(\ln n \left[\frac{\ln c}{\ln 2} - 1\right]\right) \leq n^{\rho(c)},$$

where $\rho(c) = \frac{\ln c}{\ln 2} - 1$. But, $\rho(c) < 0$ for $c < 2$, therefore according to (5.2) on the one hand we get

$$\sum_{s \leq m-2} \mathbb{E}(B_s) \lesssim n^{\rho(c)}. \quad (5.3)$$

On the other hand, according to (5.1) we get

$$\sum_{s \geq m-1} \mathbb{E}(B_s) \lesssim n^{\rho(c)} \text{ if } c \geq 1 \quad \text{and} \quad \sum_{s \geq m-1} \mathbb{E}(B_s) \lesssim n^{-1} \text{ if } c \leq 1. \quad (5.4)$$

Therefore, from (5.4) and (5.3) we get

$$\sum_s \mathbb{E}(B_s) = o(1) \text{ for } 0 < c < 2. \quad \square$$

The function g defined in the following will play an important role in our analysis.

Definition 5.4. Let $c \in]1, 2[$. For any $\alpha > 0$ let \mathcal{D}_α be the following domain

$$\mathcal{D}_\alpha = \{(\beta, \gamma) \mid 0 < \beta \leq \alpha \text{ and } \beta \leq \gamma\},$$

and $g_{\alpha,c}$ defined over \mathcal{D} by

$$g_{\alpha,c}(\beta, \gamma) = \ln \left[\frac{1}{e} \left(\frac{c\gamma}{2ex_0\alpha} \right)^\gamma \cdot \frac{\alpha^\alpha}{\beta^\beta(\alpha-\beta)^{\alpha-\beta}} \cdot 2^\beta \cdot (e^{x_0} - 1)^\beta \right], \quad (5.5)$$

with $1 - e^{-x_0} = \frac{\beta}{\gamma} x_0$ and $g_{\alpha,c}(\beta, \beta) = \ln \left[\frac{1}{e} \left(\frac{c}{e\alpha} \right)^\beta \cdot \frac{\alpha^\alpha}{(\alpha-\beta)^{\alpha-\beta}} \right]$.

Notice that $g_{\alpha,c}$ is continuously differentiable on the interior of \mathcal{D}_α , and thus, when (β, γ) belongs to the interior of \mathcal{D}_α ,

$$n^{g_{\alpha,c}(\beta+O(1/\log n), \gamma+O(1/\log n))} \equiv n^{g_{\alpha,c}(\beta, \gamma)}. \quad (5.6)$$

It turns out that the function $g_{\alpha,c}$ has a unique global maximum on \mathcal{D}_α , whose value is $\alpha H(c) - 1$.

Lemma 5.5. *The function $g_{\alpha,c}$ defined by (5.5) has a global maximum on \mathcal{D}_α , given by its unique stationarity point in the interior of \mathcal{D}_α . More precisely*

$$\max_{\mathcal{D}_\alpha} g_{\alpha,c}(\beta, \gamma) = g_{\alpha,c}(\hat{\beta}(\alpha, c), \hat{\gamma}(\alpha, c)) = \alpha H(c) - 1 \quad (5.7)$$

with $\hat{\beta} = \frac{2\alpha(c-1)}{c}$, $\hat{\gamma} = \frac{-2\alpha \ln(2-c)}{c}$, $H(c) = \ln c + \left(\frac{2}{c} - 1 \right) \ln(2-c)$.

Moreover, for any domain $V_\alpha \subset \mathcal{D}_\alpha$ such that $(\hat{\beta}, \hat{\gamma}) \notin \overline{V_\alpha}$, there exists $\delta > 0$ such that

$$\max_{V_\alpha} g_{\alpha,c}(\beta, \gamma) \leq \alpha H(c) - 1 - \delta. \quad (5.8)$$

Proof. See the appendix. \square

We have $\mathbb{E}(B) = \sum_{s+1 \geq 3} \sum_{k=1}^{\min(m, s+1)} \mathbb{E}(B_{s,k}) = \sum_{s+1 \geq 3} \mathbb{E}(B_s)$ and from the first item of Proposition 4.7 we get $\mathbb{E}(B) = \sum_{3 \leq s+1 \leq \frac{2m}{\log(2/c)}} \mathbb{E}(B_s) + o(1)$. Thus the last item of Proposition 4.7 is a direct consequence of the following

Proposition 5.6. *Let $c \in]1, 2[$, $\alpha > 0$ and $(\beta, \gamma) \in \mathcal{D}_\alpha$. If $s = \gamma \ln n + O(1)$ and $k = \beta \ln n + O(1)$, then*

- $\mathbb{E}(B_{s,k}) \equiv n^{g_{\alpha,c}(\beta,\gamma)}$,
- $\mathbb{E}(B_s) \lesssim n^{\alpha H(c)-1}$.

Moreover, if $\hat{s} = \hat{\gamma} \ln n + O(1)$ and $\hat{k} = \hat{\beta} \ln n + O(1)$, with $\hat{\beta} = \frac{2\alpha(c-1)}{c}$ and $\hat{\gamma} = \frac{-2\alpha \ln(2-c)}{c}$, then,

- $\mathbb{E}(B_{\hat{s},\hat{k}}) \equiv n^{g_{\alpha,c}(\hat{\beta},\hat{\gamma})} \equiv n^{\alpha H(c)-1}$,
- there exists $\delta > 0$ such that for $s < \hat{s}/2$, $\mathbb{E}(B_s) \leq n^{\alpha H(c)-1-\delta}$.

Proof. We need to obtain sharp estimates on expression $|\mathcal{B}_{s,k}| = [(2(s-1))^2 - 1](n)_s 2^s \binom{m}{k} \cdot 2^k \cdot \mathcal{S}(s+1, k)$. First, if $1 \leq b \leq a$, we shall use the following well-known inequalities for binomial coefficients:

$$\sqrt{\frac{1}{a}} \left(\frac{a}{b}\right)^b \cdot \left(\frac{a}{a-b}\right)^{a-b} \leq \binom{a}{b} \leq \left(\frac{a}{b}\right)^b \cdot \left(\frac{a}{a-b}\right)^{a-b}. \quad (5.9)$$

Then, from the uniform asymptotics obtained in [16], one gets the following uniform bounds for Stirling numbers of the second kind. There exist universal constants $K > 0$ and $K' > 0$ such that, for every $1 \leq b \leq a$, the following inequalities hold:

$$K \sqrt{\frac{b}{a}} \left(\frac{e^{x_0} - 1}{x_0}\right)^b \left(\frac{a}{e}\right)^a x_0^{b-a} \leq b! \mathcal{S}(a, b) \leq K' \sqrt{b} \left(\frac{e^{x_0} - 1}{x_0}\right)^b \left(\frac{a}{e}\right)^a x_0^{b-a} \quad (5.10)$$

where $x_0 > 0$ is a function of b/a defined implicitly for $b < a$ by $1 - e^{-x_0} = \frac{b}{a} x_0$, and for $a = b$ by $x_0 = 0$. The conventions are that $0^0 = 1$ and $\frac{e^0 - 1}{0} = 1$.

By using these precise results, already used in [9] and [5], it appears that the behaviour of $\mathbb{E}(B_{s,k})$ is governed by a continuous function of several real variables. Combining $\mathbb{E}(\mathcal{B}_{s,k}) = p^{s+1} [(2(s-1))^2 - 1](n)_s 2^s \binom{m}{k} \cdot 2^k \cdot \mathcal{S}(s+1, k)$ with (5.9) and (5.10) we obtain that there exist $A > 0$ and $B > 0$ such that for every $c > 0$, for every positive integers n, m, s and k such that $k \leq \min(m, s+1)$:

$$\frac{A(n)_s \sqrt{k}}{n \sqrt{m(s+1)}} n^{g_{\frac{m}{\ln n}, c}(\frac{k}{\ln n}, \frac{s+1}{\ln n})} \leq \mathbb{E}(B_{s,k}) \leq B \sqrt{m} n^{g_{\frac{m}{\ln n}, c}(\frac{k}{\ln n}, \frac{s+1}{\ln n})}. \quad (5.11)$$

Thus we get $\mathbb{E}(B_{s,k}) \equiv n^{g_{\alpha,c}(\beta,\gamma)}$ from (5.6). All the following assertions in Proposition 5.6 then directly follow from (5.7) and (5.8) in Lemma 5.5, the inequality $k \leq s+1$ being used for the assertions on $\mathbb{E}(B_s)$. \square

6. PROOF OF PROPOSITION 4.9

For every $1 \leq i \leq s$, let $N_{m,s}(i)$ denote the number of pure snakes B of length $s+1$ such that A_0 and B share exactly i clauses, A_0 being a given pure snake of length $s+1$. Then, we have:

$$\frac{\mathbb{E}(X_s)^2}{\mathbb{E}(X_s^2)} \geq \frac{1}{1 + \frac{1 + \sum_{i=1}^s N_{m,s}(i)p^{s+1-i}}{\mathbb{E}_{m,c}(X_s)}}. \quad (6.1)$$

We have to prove that

- $\sum_{i=1}^{\hat{s}} N_{m,s}(i)p^{\hat{s}+1-i} = o(\mathbb{E}_{m,c}(X_{\hat{s}}))$,
- $\mathbb{E}_{m,c}(X_{\hat{s}}) \longrightarrow +\infty$

Observe that $|\mathcal{B}_s| = |\mathcal{X}_s|[(2(s-1))^2 - 1]$, therefore

$$\mathbb{E}(X_{\hat{s}}) \equiv n^{\alpha H(c)-1}. \quad (6.2)$$

Notably, when $\alpha H(c) - 1 > 0$, $\mathbb{E}(X_{\hat{s}})$ goes to infinity.

The crucial point is to improve the enumeration on snakes made in [4]. In the next lemma we consider snakes, ignoring the universal variables. The required upper bounds for the number of pure snakes is then easy to deduce.

Lemma 6.1. *Let A_0 be a given snake of length $s+1 = 2t$ and for every $1 \leq i \leq s$, let $N_s(i)$ be the number of snakes B of length $s+1$ such that A_0 and B share exactly i clauses. Then, if $2t$ is less than $1/2n^{1/3}$:*

$$N_s(i) \leq \begin{cases} 4 \frac{(s+1)^3}{n} (n)_{s-i} 2^{s-i} & \text{for } 1 \leq i \leq t-1 \\ 4(s+1)^3 (n)_{s-i} 2^{s-i} & \text{for } t \leq i \leq 2t-1. \end{cases} \quad (6.3)$$

With this lemma (which is proved below) we are in a position to prove Proposition 4.9. Observe that for every s

$$N_{m,s}(i) \leq N_s(i)d(m, s+1-i). \quad (6.4)$$

Therefore in using Lemma 6.1 we obtain with $s+1 = 2t$:

$$\begin{aligned} \sum_{i=1}^{\hat{t}-1} N_{m,\hat{s}}(i)p^{\hat{s}+1-i} &\lesssim \frac{1}{n} \sum_{i=1}^{\hat{t}-1} (n)_{\hat{s}-i} 2^{\hat{s}-i} d(m, \hat{s}+1-i) p^{\hat{s}+1-i} \\ &\lesssim \frac{1}{n} \sum_{i=1}^{\hat{t}-1} \mathbb{E}(X_{\hat{s}+1-i}) \\ &\lesssim n^{\alpha H(c)-2} \text{ (from (6.2)).} \end{aligned}$$

Now,

$$\begin{aligned} \sum_{i=\hat{t}}^{2\hat{t}-1} N_{m,\hat{s}}(i)p^{\hat{s}+1-i} &\lesssim \sum_{i \geq \hat{t}} \mathbb{E}(X_{\hat{s}+1-i}) \\ &\lesssim \max_{i \geq \hat{t}} \mathbb{E}(X_{\hat{s}+1-i}) \\ &\lesssim \max_{s \leq \hat{s}/2} \mathbb{E}(X_s). \end{aligned}$$

Since $\mathbb{E}(X_s) \equiv \mathbb{E}(B_s)$, we deduce from Proposition 5.6, that for $s \leq \hat{s}/2$, $\mathbb{E}(X_s) \leq \max_{s \leq \hat{s}/2} \mathbb{E}(B_s) \lesssim n^{\alpha H(c)-1-\delta}$ for some $\delta > 0$, thus:

$$\sum_{i=1}^{\hat{s}} N_{m,s}(i)p^{\hat{s}+1-i} \lesssim n^{\alpha H(c)-2} + n^{\alpha H(c)-1-\delta} = o(\mathbb{E}_{m,c}(X_{\hat{s}})).$$

Plugging this asymptotic and (6.2) into the second moment bound (6.1) leads to Proposition 4.9.

Proof of Lemma 6.1. Given a literal w , let $|w|$ denote its underlying variable. Observe that a snake of length $s+1 = 2t$ contains s distinct existential variables. Moreover, every existential variable $|w_i|$ appearing in a snake occurs exactly twice (once positively and once negatively), except for $|w_0|$ which occurs four times (twice positively and twice negatively). This special variable will be called the *double point* of the snake. A snake can be described by a (circular) sequence of existential literals $w_0, w_1, \dots, w_s(w_0)$ (with $w_0 = \overline{w_t}$).

The enumeration made in [4] is not good enough for us: indeed, Chvátal and Reed lose a factor n when $i \geq t$, and while this is unimportant for them, this factor will be crucial for us. Therefore we need to reproduce below, more carefully, their analysis.

Let A_0 be a given snake of length $s+1 = 2t$. $N_s(2t) = 1$, so we shall focus on $i \leq 2t-1$. Then, $N_s(i)$ can be decomposed as

$$N_s(i) = \sum_{j \geq i+1} N_s(i, j)$$

where $N_s(i, j)$ is the number of snakes B of length $s+1$ such that A_0 and B share exactly i clauses and j variables. Now we are looking for upper bounds on the $N_s(i, j)$.

Let us note that the intersection of A_0 and B can be read on the (circular) sequence of literals $w_0, w_1, \dots, w_t, \dots, w_s(w_0)$, where $w_t = \overline{w_0}$. In order to get i clauses and j variables in common, one has to choose $k = (j-i)$ blocks of consecutive literals in this sequence. We make a case distinction according to whether the two snakes A_0 and B have the same double point or not.

- $N_s^a(i, j)$ denotes the number of snakes B of length $s+1$ such that A_0 and B share exactly i clauses and j variables, and have the same double point $|w_0|$,

- $N_s^b(i, j)$ denotes the number of snakes B of length $s + 1$ such that A_0 and B share exactly i clauses and j variables, and do not have the same double point.

Thus $N_s(i, j) = N_s^a(i, j) + N_s^b(i, j)$.

Let us first consider $N_s^a(i, j)$. Observe that in the special case when $j = i + 1$ (only one block), and A_0 and B have the same double point, then i is necessarily equal to or larger than t . This is crucial to get a good bound, and is the idea behind the definition of a snake. Therefore,

$$\text{for } 1 \leq i \leq t - 1, \quad N_s^a(i, i + 1) = 0. \quad (6.5)$$

In the general case, to count $N_s^a(i, j)$ we perform the following sequence of choices:

- (1) the intersection $A_0 \cap B$ such that it has i clauses and j variables, *i.e.*, $k = (j - i)$ blocks of consecutive literals in the sequence of literals describing A_0 ,
- (2) the sequence of strictly distinct existential literals that are in $B \setminus (A_0 \cap B)$,
- (3) the places of the k blocks of $A_0 \cap B$ among the literals chosen in (2).

Step (1). To build the intersection $A_0 \cap B$, we choose $2k$ literals in the sequence representing A_0 . They represent the first and last literals of the k blocks of $A_0 \cap B$. The first literal is chosen after or at ω_0 . To define completely the intersection, we need to know whether this first literal is the beginning or the end of a block, so we get at most $2 \binom{s+1}{2k} \leq (s+1)^{2k}$ possible choices.

Step (2). Notice that $|w_0|$ is the double point of B . So, it remains only to choose a sequence of $s - (j - 1)$ strictly distinct literals. Thus, we have at most $(n)_{s+1-j} 2^{s+1-j}$ possible choices.

Step (3). We need to choose how the k blocks will be plugged among the “remaining literals” chosen in Step (2). This leads to at most $(s+1)^k$ possible choices.

Thus, since $k = j - i$ we obtain that for $1 \leq i \leq 2t - 1$, $j \geq i + 1$

$$\begin{aligned} N^a(i, j) &\leq (s+1)^{3k} (n)_{s+1-j} 2^{s+1-j}, \\ &\leq (s+1)^3 \left(\frac{(s+1)^3}{n-s} \right)^{j-i-1} (n)_{s-i} 2^{s-i}. \end{aligned}$$

Recalling (6.5), we obtain for $i \leq t - 1$,

$$\sum_{j=i+1}^{2t} N_s^a(i, j) \leq (s+1)^3 \left[\sum_{h=1}^{2t-i-1} \left(\frac{(s+1)^3}{n-s} \right)^h \right] (n)_{s-i} 2^{s-i}. \quad (6.6)$$

When $i \geq t$, we only have:

$$\sum_{j=i+1}^{2t} N_s^a(i, j) \leq (s+1)^3 \left[\sum_{h=0}^{2t-i-1} \left(\frac{(s+1)^3}{n-s} \right)^h \right] (n)_{s-i} 2^{s-i}. \quad (6.7)$$

The enumeration of $N^b(i, j)$ differs from the one of $N^a(i, j)$ only at Step (2). Indeed, when B does not have $|w_0|$ as a double point, at Step (2) we have first to

choose a sequence of $s - j$ strictly distinct literals (thus having determined the s variables occurring in B), and then choose one of these s variables as the double point. Hence, we have at most $s(n)_{s-j}2^{s-j}$ choices. Thus, we get for $1 \leq i \leq 2t - 1$ and $j \geq i + 1$

$$N^b(i, j) \leq s \left(\frac{(s+1)^3}{n-s} \right)^{j-i} (n)_{s-i} 2^{s-i},$$

whence

$$\sum_{j=i+1}^{2t} N^b(i, j) \leq s \left[\sum_{h=1}^{2t-i} \left(\frac{(s+1)^3}{n-s} \right)^h \right] (n)_{s-i} 2^{s-i}. \quad (6.8)$$

From (6.4), (6.6) and (6.8), we get, for $1 \leq i \leq t - 1$

$$N_s(i) \leq 2(s+1)^3 \left[\sum_{h=1}^{2t} \left(\frac{(s+1)^3}{n-s} \right)^h \right] (n)_{s-i} 2^{s-i}$$

and from (6.4), (6.7) and (6.8), we get, for $t \leq i \leq 2t - 1$

$$N_s(i) \leq 2(s+1)^3 \left[\sum_{h=0}^{2t} \left(\frac{(s+1)^3}{n-s} \right)^h \right] (n)_{s-i} 2^{s-i}.$$

Now, when $2t \leq (1/2)n^{1/3}$, we have, for $h \leq 2t$:

$$\left(\frac{n}{n-s} \right)^h \leq e^{\frac{4t^2}{n-2t}} \leq e,$$

and

$$\begin{aligned} \sum_{h=1}^{2t} \left(\frac{(s+1)^3}{n-s} \right)^h &\leq e \frac{(s+1)^3}{n} \sum_{h=0}^{+\infty} \left(\frac{(s+1)^3}{n} \right)^h \\ &\leq e \frac{(s+1)^3}{n(1-1/8)}. \end{aligned}$$

Similarly,

$$\sum_{h=0}^{2t} \left(\frac{(s+1)^3}{n-s} \right)^h \leq 4e.$$

This concludes the proof. \square

7. CONCLUSION

We have studied a natural and expressive quantified problem, (1,2)-QSAT. We have proved the existence of a sharp phase transition from satisfiability to unsatisfiability for (1,2)-QCNF-formulas and we have given the exact location of the

threshold. The obtained results have several interesting features. The parameter m , which is the number of universal variables, controls the worst-case computational complexity of the problem (which is ranging from linear time solvable to coNP-complete), as well as the typical behavior of random instances. When m is small enough, namely when $m \ll \log n$, there is a sharp threshold at $c = 2$. On the other side, when m is large enough, namely when $m \gg \log n$, there is a sharp threshold at $c = 1$. More importantly, an original regime is observed when $m = \lfloor \alpha \log n \rfloor$. Using counting arguments on pure bicycles, which are the seed of unsatisfiability, and on pure snakes, which are special minimally false formulas, we got respectively a lower and an upper bound for the threshold. It appears that these two bounds, which are based on an analytical analysis of involved combinatorial expressions, coincide thus giving the exact location of the critical ratio as a function of α . Let us emphasize that this was a priori unexpected. It suggests that (1,2)-QSAT is a satisfiability problem that is worth studying by combinatorial means. Such problems are not so common and not so easy to identify. Therefore an important feature of our work is to reveal an expressive satisfiability problem (it is coNP-complete) which could be a testbed for developing innovative combinatorial (enumerative) methods for the study of phase transitions.

A. PROOF OF LEMMA 5.5

Let us recall that for any $1 < c < 2$ and $\alpha > 0$, we consider the domain $\mathcal{D}_\alpha = \{(\beta, \gamma) \mid 0 < \beta \leq \alpha \text{ and } \beta \leq \gamma\}$ for the function $g_{\alpha,c}$ given from (5.5) by

$$g_{\alpha,c}(\beta, \gamma) = -1 + \alpha \ln \alpha - (\alpha - \beta) \ln(\alpha - \beta) + \gamma \ln \left[\frac{c\gamma}{2ex_0\alpha} \right] + \beta \ln \left[\frac{2(e^{x_0} - 1)}{\beta} \right] \quad (\text{A.1})$$

and

$$g_{\alpha,c}(\beta, \beta) = -1 + \alpha \ln \alpha - (\alpha - \beta) \ln(\alpha - \beta) + \beta \ln \left[\frac{c}{e\alpha} \right]$$

with x_0 defined implicitly when $0 < \beta < \gamma$ by

$$1 - e^{-x_0} = \frac{\beta}{\gamma} x_0. \quad (\text{A.2})$$

In the sequel, we shall write g for $g_{\alpha,c}$ and \mathcal{D} for \mathcal{D}_α . We want to prove that g has a strict and global maximum on \mathcal{D} which is equal to $\alpha H(c) - 1$ with $H(c) = \ln c + \left(\frac{2}{c} - 1\right) \ln(2 - c)$. This follows from the following claim:

Claim A.1. For any $1 < c < 2$ and $\alpha > 0$,

- (1) for every fixed β with $0 < \beta \leq \alpha$, the function $\gamma \mapsto g(\beta, \gamma)$ is strictly concave on $[\beta, +\infty[$ with a strict maximum at $\gamma_\beta = \frac{2\alpha}{c} \ln \left(\frac{2\alpha}{2\alpha - \beta c} \right)$,

- (2) the function $\beta \mapsto g(\beta, \gamma_\beta)$ is strictly concave on $]0, \alpha]$ with a maximum at $\hat{\beta} = \frac{2\alpha(c-1)}{c}$, then with $\hat{\gamma} := \gamma_{\hat{\beta}} = \frac{-2\alpha \ln(2-c)}{c}$, $g(\hat{\beta}, \hat{\gamma}) = \alpha H(c) - 1$.

Proof. For the first point of this claim we compute, from (A.1) and (A.2), the partial derivatives of g with respect to γ . We get

$$\frac{\partial g}{\partial \gamma}(\beta, \gamma) = \ln\left(\frac{c\gamma}{2x_0\alpha}\right) \quad \text{and} \quad \frac{\partial^2 g}{\partial \gamma^2}(\beta, \gamma) = \frac{\gamma - \beta x_0}{\gamma(\gamma - \beta(x_0 + 1))}. \quad (\text{A.3})$$

With (A.2) we first observe that

$$\gamma - \beta x_0 = \gamma e^{-x_0} > 0. \quad (\text{A.4})$$

Then

$$\begin{aligned} \gamma - \beta(x_0 + 1) &= \gamma - \beta x_0 - \beta \\ &= \gamma e^{-x_0} - \beta \\ &= \gamma e^{-x_0} - \frac{\gamma(1 - e^{-x_0})}{x_0} \\ &= \frac{\gamma}{x_0}(x_0 e^{-x_0} - 1 + e^{-x_0}). \end{aligned}$$

Let $\varphi(x) = x e^{-x} - 1 + e^{-x}$. The function φ is decreasing with $\varphi(0) = 0$. Hence, $\varphi(x_0) < 0$ and

$$\gamma - \beta(x_0 + 1) < 0. \quad (\text{A.5})$$

From the second identity in (A.3), (A.4) and (A.5) we conclude that $\frac{\partial^2 g}{\partial \gamma^2}(\beta, \gamma) < 0$. The strict concavity of $\mapsto g(\beta, \gamma)$ follows. Then the first identity in (A.3) and (A.2) give the expected formula for the unique extremum, indeed we obtain

$$\gamma_\beta = \frac{2x_0\alpha}{c} = \frac{2\alpha}{c} \ln\left(\frac{2\alpha}{2\alpha - \beta c}\right) \quad \text{and} \quad e^{x_0} - 1 = \frac{\beta c}{2\alpha - \beta c}. \quad (\text{A.6})$$

For the second point of the claim, observe that with (A.1) we have:

$$g(\beta, \gamma) = -1 + \gamma \ln\left[\frac{c\gamma}{2x_0\alpha}\right] - \gamma + \alpha \ln \alpha - (\alpha - \beta) \ln(\alpha - \beta) + \beta \ln \frac{2(e^{x_0} - 1)}{\beta},$$

thus from (A.6) we obtain

$$g(\beta, \gamma_\beta) = -1 + \alpha K_c\left(\frac{\beta}{\alpha}\right) \quad (\text{A.7})$$

where for any $x \in]0, 1[$, $K_c(x) = x \ln c + \left(\frac{2}{c} - x\right) \ln\left(1 - \frac{cx}{2}\right) - (1-x) \ln(1-x)$. The function K_c is strictly concave on $]0, 1[$ and reaches its maximum at $x = \frac{2(c-1)}{c}$.

From (A.7) with $\frac{\hat{\beta}}{\alpha} = \frac{2(c-1)}{c}$ we get $\max_{\beta>0} g(\beta, \gamma_\beta) = -1 + \alpha K_c \left(\frac{\hat{\beta}}{\alpha} \right) = -1 + \alpha H(c)$. Then, with (A.6) we obtain $\gamma_{\hat{\beta}} = \frac{2\alpha}{c} \ln \left(\frac{2\alpha}{2\alpha - \hat{\beta}c} \right) = \frac{-2\alpha \ln(2-c)}{c} := \hat{\gamma}$.

At last, observe that $\frac{\partial g}{\partial \beta}(\beta, \gamma) = \ln \left(\frac{2(e^{x_0} - 1)(\alpha - \beta)}{\beta} \right)$, so $\hat{\beta}$ and $\hat{\gamma}$ give the coordinates of the unique stationarity point of g , that is the unique solution of $\frac{\partial g}{\partial \beta}(\beta, \gamma) = \frac{\partial g}{\partial \gamma}(\beta, \gamma) = 0$.

The last statement of the lemma follows then from the fact that $g_{\alpha,c}$ is continuous on the interior of \mathcal{D}_α . \square

Acknowledgements. We thank the reviewers for their very careful reading and valuable comments.

REFERENCES

- [1] B. Aspvall, M.F. Plass and R.E. Tarjan, A linear-time algorithm for testing the truth of certain quantified boolean formulas. *Inform. Process. Lett.* **8** (1979) 121–123.
- [2] B. Bollobás, C. Borgs, J.T. Chayes, J.H. Kim and D.B. Wilson, The scaling window of the 2-SAT transition. *Random Structures and Algorithms* **18** (2001) 201–256.
- [3] H. Chen and Y. Interian, A model for generating random quantified boolean formulas. In *Proc. of the 19th International Joint Conference on Artificial Intelligence (IJCAI 2005)* (2005) 66–71.
- [4] V. Chvátal and B. Reed, Mick gets some (the odds are on his side). In *Proc. of the 33rd Annual Symposium on Foundations of Computer Science (FOCS 92)* (1992) 620–627.
- [5] N. Creignou, H. Daudé and U. Egly, Phase transition for random quantified XOR-formulas. *J. Artif. Intell. Res.* **19** (2007) 1–18.
- [6] N. Creignou, H. Daudé, U. Egly and R. Rossignol, New results on the phase transition for random quantified Boolean formulas. *Proc. of the 11th International Conference on Theory and Applications of Satisfiability Testing (SAT 2008)*. In vol. 4996 of *Lect. Notes Comput. Sci.* (2008) 34–47.
- [7] N. Creignou, H. Daudé, U. Egly and R. Rossignol, (1,2)-QSAT: A good candidate for understanding phase transitions mechanisms. *Proc. of the 12th International Conference on Theory and Applications of Satisfiability Testing (SAT 2009)*. In vol. 5584 of *Lect. Notes Comput. Sci.* (2009) 363–376.
- [8] W. Fernandez de la Vega, Random 2-SAT: results and problems. *Theor. Comput. Sci.* **265** (2001) 131–146.
- [9] O. Dubois and Y. Bouffkhad, A general upper bound for the satisfiability threshold of random r -SAT formulae. *J. Algorithms* **24** (1997) 395–420.
- [10] U. Egly, T. Eiter, H. Tompits and S. Woltran, Solving Advanced Reasoning Tasks Using Quantified Boolean Formulas. In *Proc. of the 17th National Conference on Artificial Intelligence and the 12th Innovative Applications of Artificial Intelligence Conference (AAAI/IAAI 2000)*. AAAI Press / MIT Press (2000) 417–422.
- [11] A. Flögel, M. Karpinski and H. Kleine Büning, Subclasses of quantified Boolean formulas. In *Proceedings of the 4th Workshop on Computer Science Logic (CSL 90)* (1990) 145–155.
- [12] I.P. Gent and T. Walsh, Beyond NP: the QSAT phase transition. In *Proc. of AAAI-99* (1999).
- [13] A. Goerdt, A threshold for unsatisfiability. *J. Comput. Syst. Sci.* **53** (1996) 469–486.

- [14] S. Janson, T. Luczack and A. Rucinski, Random graphs. John Wiley (2000).
- [15] B. Selman, D. Mitchell and H.J. Levesque, Generating hard satisfiability problems. *Artif. Intell.* **81** (1996) 17–29.
- [16] N.M. Temme, Asymptotic estimates of Stirling numbers. *Stud. Appl. Math.* **89** (1993) 223–243.
- [17] Y. Verhoeven, Random 2-SAT and unsatisfiability. *Inform. Proc. Lett.* **72** (1999) 119–123.
- [18] D.B. Wilson, On the critical exponents of random k -SAT. *Random Struct. Algorithms* **21** (2002) 182–195.

Communicated by S. Perifel.

Received May 5, 2014. Accepted August 28, 2014.