Setting 2 variables at a time yields a new lower bound for random 3-SAT

[Extended Abstract]

Dimitris Achlioptas
Microsoft Research
One Microsoft Way
Redmond, WA 98052
optas@microsoft.com

ABSTRACT

Let X be a set of n Boolean variables and denote by $C(X)$ the set of all 3-clauses over X, i.e. the set of all $8\binom{n}{3}$ possible disjunctions of three distinct, non-complementary literals from variables in X. Let $F(n,m)$ be a random 3-SAT formula formed by selecting, with replacement, m clauses uniformly at random from $C(X)$ and taking their conjunction. The *satisfiability threshold conjecture* asserts that there exists a constant r_3 such that as $n \to \infty$, $F(n, rn)$ is satisfiable with probability that tends to 1 if $r < r_3$, but unsatisfiable with probability that tends to 1 if $r > r_3$. Experimental evidence suggests $r_3 \approx 4.2$.

We prove $r_3 > 3.145$ improving over the previous best lower bound $r_3 > 3.003$ due to Frieze and Suen. For this, we introduce a satisfiability heuristic that works iteratively, permanently setting the value of a pair of variables in each round. The framework we develop for the analysis of our heuristic allows us to also derive most previous lower bounds for random 3-SAT in a uniform manner and with little effort.

1. INTRODUCTION

The question "Are *typical* instances of satisfiability *hard*?" gave the original motivation for studying random(ly chosen) satisfiability (instances). While "hard" here is vis-à-vis the problem's NP-completeness, quantifying "typical" is a hard problem in itself. Considering random formulas allows one to sidestep this thorny issue.

An early result [21] on the performance of the Davis-Putnam (DP) algorithm [11; 10] on random formulas suggested that satisfiability is easy on average. As Franco and Paull [17] pointed out, though, the distribution of instances in [21] is so greatly dominated by easily satisfiable instances that if one tries truth assignments completely at random, the expected number of trials before finding a satisfying one is O(1).

STOC 2000 Portland Oregon USA

Franco and Paull [17], further, considered the performance of the DP algorithm on random instances of k-SAT. More precisely, let $F_k(n,m)$ denote a random formula in Conjunctive Normal Form with m clauses over n Boolean variables, where the clauses are chosen uniformly, independently and with replacement among all $2^k\binom{n}{k}$ non-trivial clauses of length k, i.e. clauses with k distinct, non-complementary literals. They showed that for all $k \geq 3$ and every constant $r > 0$, with probability $1 - o(1)$, the DP algorithm takes an *exponential* number of steps to report the satisfying truth assignments of $F_k(n, rn)$, i.e. either to report all (cylinders of) solutions, or that no solutions exist.

In a seminal paper, extending the ground-breaking result of Haken [22] on the worst-case complexity of resolution, Chvátal and Szemerédi [7] used $F_k(n, rn)$ to provide examples of formulas that are hard to prove unsatisfiable with *any* resolution-type strategy (such as the DP algorithm). In particular, they showed that for all $k \geq 3$, if $r2^{-k} > 0.7$ then there exists $\epsilon = \epsilon(k,r) > 0$ such that with probability $1 - o(1)$, $F_k(n, rn)$ is unsatisfiable but every resolution proof of this fact must generate at least $(1+\epsilon)^n$ clauses.

In [37], Selman, Mitchell and Levesque gave extensive experimental evidence suggesting that for $k \geq 3$ there is a range of the clauses-to-variables ratio, r, within which it seems hard even to *decide* if a randomly chosen k-SAT instance is satisfiable or not (as opposed to finding all satisfying truth assignments or giving a proof of unsatisfiability). For example, for $k = 3$ their experiments draw the following remarkable picture. For $r < 4$, a satisfying truth assignment can be easily found for almost all formulas; for $r > 4.5$, almost all formulas are unsatisfiable; for $r \approx 4.2$, a satisfying truth assignment can be found for roughly half the formulas and around this point the computational effort to find a satisfying truth assignment, whenever one exists, is maximized. Let

$$S_k(n,r) = \Pr[F_k(n,rn) \text{ is satisfiable}] \ .$$

In [6], the following possibility was put forward and has since become a folklore conjecture.

Satisfiability Threshold Conjecture *For each $k \geq 2$, there exists a constant r_k such that for any $\epsilon > 0$,*

$$\lim_{n\to\infty} S_k(n, r_k - \epsilon) = 1, \quad \textit{and} \quad \lim_{n\to\infty} S_k(n, r_k + \epsilon) = 0 \ .$$

This conjecture, which motivates our work, has attracted attention in computer science, mathematics and, more recently, mathematical physics [30; 31; 33; 32]. We introduce a new algorithmic approach to this problem and use it to prove

THEOREM 1. *For all $r \leq 3.145$, $F_3(n, rn)$ is satisfiable with probability $1 - o(1)$.*

For the connections of random formulas to proof complexity and computational hardness we refer the interested reader to the excellent surveys by Beame and Pitassi [2] and Cook and Mitchell [9], respectively. The rest of the paper is organized as follows. In Section 2 we summarize most known results regarding the conjecture. In Section 3 we give a more detailed account of our contribution and its relationship to past work. In Section 4 we present the preliminaries for the analysis and the main tools that we use. In Section 5 we prove our main result. We give some concluding remarks in Section 6.

2. SUMMARY OF KNOWN RESULTS

Let us say that a sequence of events $\mathcal{E}_n$ occurs *with high probability* (w.h.p.) if $\lim_{n\to\infty} \Pr[\mathcal{E}_n] = 1$ and *with positive probability* if $\liminf_{n\to\infty} \Pr[\mathcal{E}_n] > 0$. By $X \stackrel{D}{=} Y$ we will denote that the random variable X is distributed as Y. Throughout the paper we will omit floors and ceilings when this does not result in confusion.
While we adopt the $F_k(n, m)$ model throughout the paper it is worth noting that the results described below, along with our Theorem 1, hold in all standard models for random k-SAT, e.g. when clause replacement is not allowed and/or when each k-clause is formed by selecting k literals uniformly at random with replacement.

2.1 Random 2-SAT

For $k = 2$, Chvátal and Reed [6], Goerdt [20] and Fernandez de la Vega [15] independently proved the conjecture, in fact determining $r_2 = 1$. It is important to recall that 2-SAT being solvable in polynomial time [8] means that we have a *simple* characterization of unsatisfiable 2-SAT formulas. Indeed, both [6] and [20] make full use of this characterization as they proceed by focusing on the emergence of the "most likely" unsatisfiable subformulas in $F_2(n, rn)$. Also using this characterization, Bollobás et al. [3] recently completely determined the "scaling window" for random 2-SAT, showing that the transition from satisfiability to unsatisfiability occurs for $m = n + \lambda n^{2/3}$ as λ goes from $-\infty$ to $+\infty$. We will use a lemma that follows immediately from their results (and with a bit of work also from [20]).

LEMMA 1. *Let F be a random formula formed by taking the conjunction of $F_2(n, rn)$ and $F_1(n, q)$ (over the same n variables). For any constant $r < 1$, if $q = \text{polylog}(n)$ then F is satisfiable w.h.p.*

2.2 Random 3-SAT

For $k \geq 3$, much less progress has been made. Neither the value, nor even the existence of r_k has been established. A big step towards the latter was made by Friedgut [18].

THEOREM 2 ([18]). *For every $k \geq 2$, there exists a sequence $r_k(n)$ such that for any $\epsilon > 0$,*

$$\lim_{n\to\infty} S_k(n, r_k(n) - \epsilon) = 1, \quad \textit{and} \quad \lim_{n\to\infty} S_k(n, r_k(n) + \epsilon) = 0 \; .$$

The following immediate corollary of Theorem 2 is very useful, as it allows one to establish $r_k \geq r^*$ only by showing that $F_k(n, r^* n)$ is satisfiable with positive probability.

COROLLARY 1. *If for a given r, $\liminf_{n\to\infty} S_k(n, r) > 0$ then for any $\epsilon > 0$, $\lim_{n\to\infty} S_k(n, r - \epsilon) = 1$.*

Franco and Paull [17] gave the first upper bound for r_3, by observing that the expected number of satisfying truth assignments of $F_3(n, rn)$, $(2(7/8)^r)^n$, is $o(1)$ when $r > r^* = 5.191\ldots$ Since then, and especially in recent years, there has been steady progress in terms of improving this bound. In [4], Broder, Frieze and Upfal were the first to point out that this bound is not tight and showed $r_3 < r^* - 10^{-7}$. Indeed, shortly afterwards El-Maftouhi and Fernandez de la Vega [14] proved $r_3 < 5.08$ and, independently, Kamath et al. [24] proved $r_3 < 4.758$. Later, Kirousis et al. [26] improved the bound even further to $r_3 < 4.601$, by using a much more direct and simple argument than [14; 24]. Independently, Dubois and Boufkhad [12], using a method similar to [26], obtained $r_3 < 4.64$. By improving upon an estimate in [26], Janson, Stamatiou and Vamvakari [23] showed $r_3 < 4.596$. Finally, very recently, Dubois, Boufkhad and Mandler [13] announced $r_3 < 4.506$.
Unlike upper bounds, that come from probabilistic counting arguments, all lower bounds for r_3 are algorithmic. Also unlike upper bounds, there has been no progress in terms of bounding r_3 from below since the work of Frieze and Suen [19]. An early analysis of a satisfiability heuristic on $F_3(n, rn)$ was given by Chao and Franco [5] who showed that the UNIT CLAUSE (UC) algorithm has positive probability of finding a satisfying truth assignment for $r < 8/3 = 2.66..$ and, when combined with a "majority" rule, for $r < 2.9$. Note that since these algorithms succeed only with positive probability, instead of w.h.p., this did not imply $r_3 \geq 2.9$.
The first lower bound for r_3 follows by a result of Franco [16], who considered the *pure literal* heuristic on $F_3(n, rn)$. This heuristic satisfies a literal only if its complement does not appear in the formula, thus only making "safe" steps. Franco showed that for $r < 1$, w.h.p. the pure literal heuristic eventually sets all the variables, implying $r_3 \geq 1$ (although the notion of r_k did not exist at the time). After $r_2 = 1$ was established, making $r_3 \geq 1$ trivial, the next lower bound, $r_3 \geq 1.63$, was given by Broder, Frieze and Upfal [4] who proved that the pure literal heuristic w.h.p. sets all the variables for $r \leq 1.63$ (and for $r > 1.7$ w.h.p. it does not).
The last lower bound for r_3 prior to this work was given by Frieze and Suen [19]. They considered two generalizations of UC, called SC and GUC respectively, and determined their exact probability of success on $F_3(n, rn)$. In particular, they showed that for $r < 3.003..$, both heuristics succeed with positive probability. Moreover, they proved that a modified version of GUC, which performs a very limited form of backtracking, succeeds w.h.p. for such r, thus yielding the best known lower bound for r_3 prior to this work.

3. A NEW APPROACH

In this paper we improve the lower bound for random 3-SAT to $r_3 > 3.145$. For this, we introduce a new satisfiability heuristic and a framework to analyze its performance. The main novelty of our heuristic is that, unlike all algorithms analyzed thus far, it often sets *two* variables "at a time". In particular, with the exception of the pure literal heuristic, all the algorithms discussed in the previous section proceed in rounds of the following type: at the beginning of each round precisely one literal ℓ is set to 1 with literals corresponding to unit-clauses always having highest priority (unit-clause propagation); the clauses containing ℓ are removed; each i-clause c containing $\bar{\ell}$ "shrinks" and becomes an $(i-1)$-clause; failure occurs iff a 0-clause is ever generated. Writing u.a.r. for uniformly at random, we can schematically describe all these algorithms as follows:

```
While there exist unset variables
    if there exist unit-clauses
        then pick a unit-clause ℓ u.a.r. and satisfy it
        else select a literal ℓ and satisfy it
```

The different algorithms implement select as follows.

- UC: Pick ℓ u.a.r. among all literals corresponding to unset variables.
- UC with majority: Pick an unset variable v u.a.r. Pick the literal $\ell \in \{v, \bar{v}\}$ which appears in most remaining 3-clauses (break ties u.a.r.).
- SC: If no 2-clauses remain, pick ℓ u.a.r. among all literals corresponding to unset variables. Else, pick a 2-clause $c = (\ell_1 \vee \ell_2)$ u.a.r. and pick $\ell \in \{\ell_1, \ell_2\}$ u.a.r.
- GUC: Among all remaining clauses of shortest length, pick u.a.r. a clause $c = (\ell_1 \vee \cdots \vee \ell_j)$. Pick $\ell \in \{\ell_1, \ldots, \ell_j\}$ u.a.r.

For a literal ℓ, let $\mathrm{v}(\ell)$ denote its underlying variable. Our heuristic, called TT for "Two at a Time", can be described in this scheme as

```
While there exist unset variables
    if there exist unit-clauses
        then pick a unit-clause ℓ u.a.r. and satisfy it
        else if there exists a 2-clause c = (ℓ1 ∨ ℓ2)
            then gently-satisfy(ℓ1, ℓ2)
            else pick an unset variable u.a.r.
                and assign it 0/1 u.a.r.
```

gently-satisfy(ℓ_1, ℓ_2): Among all three assignments to $\mathrm{v}(\ell_1) \neq \mathrm{v}(\ell_2)$ satisfying $c = (\ell_1 \vee \ell_2)$, pick the one which causes the fewest number of 3-clauses to become 2-clauses (break ties u.a.r.).

The framework we develop for the analysis of TT allows us to also recover the bounds corresponding to UC, UC with majority, SC and GUC in a uniform and rather simple manner. This uniformity and simplicity is mostly the result of employing a number of powerful tools developed by others. For example, Lemma 1 allows us to run each algorithm not until all variables are set, but until the remaining clauses form an "easy-to-satisfy" formula. This way we avoid having to analyze the, rather messy, last phases in the execution of each algorithm. Similarly, by Corollary 1 the fact that an algorithm succeeds with positive probability will suffice to yield a lower bound for r_3. Thus, we can avoid a backtracking similar to that in [19]. Finally, the central tool for our analysis is a theorem of Wormald [38] that will allow us to approximate with sufficient accuracy the number of remaining 2- and 3-clauses at the end of each round. The applicability of this theorem in our context is not obvious and rests on a *lazy-server* lemma that we prove which is of independent interest.

In this extended abstract, due to space limitations, we only derive our main result $r_3 > 3.145$. The derivation of the other bounds follows along similar, if simpler, lines.

4. PRELIMINARIES

There are several natural ways to implement TT into a specific procedure to be analyzed. Unfortunately, most of them lead to some subtle technical complications (which we will not discuss here). The most easily analyzed implementation (mTT) is described below. At first glance, it may appear to differ significantly from TT, but in fact the differences are superficial and only aimed at simplifying the analysis.

The algorithm runs in rounds, where precisely two variables are assigned a permanent value in each round. After t rounds, $\mathcal{C}_i(t)$ denotes the set of remaining i-clauses, $\mathcal{V}(t)$ the set of unset variables, and $\mathcal{L}(t)$ the set of literals corresponding to unset variables. Thus, $|\mathcal{L}(t)| = 2|\mathcal{V}(t)| = 2(n-2t)$, while we denote $C_i(t) = |\mathcal{C}_i(t)|$. For technical reasons, it will be useful to occasionally perform just-satisfy instead of gently-satisfy.

just-satisfy(ℓ_1, ℓ_2): Pick u.a.r one of the three value assignments satisfying $(\ell_1 \vee \ell_2)$ and assign it to $\mathrm{v}(\ell_1), \mathrm{v}(\ell_2)$.

The random variables $W(0), W(1), \ldots$ and $E(0), E(1), \ldots$ appearing in the description of mTT are Bernoulli random variables with densities $w(t)$ and $e(t)$, respectively. For now it will suffice to say that $w(t) = \phi(t/n, C_2(t)/n, C_3(t)/n)$ and $e(t) = \psi(t/n, C_2(t)/n, C_3(t)/n)$ for some functions ϕ, ψ to be specified in the course of the analysis. Note that mTT keeps running even after a contradiction (0-clause) has been generated. Naturally, if for some t_b we have $\mathcal{C}_0(t_b) \neq \emptyset$ then $\mathcal{C}_0(t) \neq \emptyset$ for all $t \geq t_b$.

mTT

```
For t = 0 ... ⌊n/2⌋
{Determine W(t) and E(t);
 if (W(t) = 0 ∧ C2(t) ≠ ∅)
    then {
          pick (ℓ1 ∨ ℓ2) ∈ C2(t) u.a.r.;
          if E(t) = 0
             then gently-satisfy(ℓ1, ℓ2)
             else just-satisfy (ℓ1, ℓ2)
         }
    else repeat twice {
          if there exist unit-clauses
             then pick a unit-clause ℓ u.a.r. and satisfy it
             else pick an unset variable u.a.r.
                  and assign it 0/1 u.a.r.
                  }
}
```

Two key points to keep in mind are: i) we will pick $e(t)$ so small that we almost never perform just-satisfy, and ii) we will pick $w(t)$ to be barely greater than the rate at which 1-clauses are generated.

For a set of Boolean variables V and an integer k let V_k denote the set of all $2^k \binom{|V|}{k}$ k-clauses on the variables of V (whose literals are non-complementary and distinct). For integers k, m let $D_k(V, m)$ denote the random set of k-clauses formed by selecting uniformly, independently and with replacement m members of V_k. A key property that mTT shares with TT and the other four algorithms discussed in Section 3 is that it maintains *uniform randomness*.

Claim 1 (Uniform randomness). *Assume that for a set V and every i, $C_i(0) \stackrel{D}{=} D_i(V, m_i)$. Then, for every i and every $t \geq 0$, conditional on $\mathcal{V}(t) = X$ and $C_i(t) = q$,*

$$C_i(t) \stackrel{D}{=} D_i(X, q) \ .$$

A formal proof of Claim 1, using the method of deferred decisions, is standard but tedious and we omit it in this extended abstract. The intuition behind the claim can be easily attained by considering the following setting. Imagine representing the input formula by using a row of i cards for each i-clause, each card bearing the name of one literal. Assume that originally all the cards are "face-down", i.e. the literal on each card is concealed and we never had an opportunity to see it. At the same time, assume that an intermediary knows precisely which literal is on each card. To interact with the intermediary we are allowed to either point at a card, or say the name of a variable. In response, if the card we point at carries literal ℓ, the intermediary reveals (flips) all the cards carrying $\ell, \bar{\ell}$. Similarly, if we announce variable v, the intermediary reveals all the cards carrying $v, \bar{v}$. Our claim now follows from observing that to run mTT, or any of the other algorithms, it suffices for us to keep track of $\mathcal{V}(t)$ and flip coins. Whenever we set a variable, we remove all the cards corresponding to dissatisfied literals and all the cards (some of them still concealed) corresponding to satisfied clauses. Thus, at the end of each round only "face-down" cards remain, containing only literals from $\mathcal{L}(t)$.

As we mentioned earlier, our main tool for the analysis of mTT will be the main theorem of [38] (stated as Theorem 3 in Appendix A for completeness). While the statement of the theorem is rather technical, the spirit of the theorem is that if a random process evolves "smoothly" in time, then w.h.p. it will remain very close to its "mean path" throughout its evolution. In particular, this mean path can be expressed as the solution of a system of differential equations associated with the process and thus it can either be recovered analytically, or bounded numerically. The idea of using differential equations to approximate discrete random processes goes back at least to Kurtz [27; 28]. It was first applied in the analysis of algorithms by Karp and Sipser [25].

The key idea which allows us to use Wormald's theorem, is that one can afford to take care of the 1-clauses in a "relaxed" way. That is, at the beginning of each round the algorithm flips a coin to decide if it will attempt to take care of 1-clauses, or not, in this round. This makes the expected change of C_2, C_3 in round t, independent of whether $\mathcal{C}_1(t) = \emptyset$ or not. Our "lazy-server" lemma then asserts that: if the rate at which the coin flips suggest taking care of 1-clauses is greater than the rate at which 1-clauses are generated, C_1 remains appropriately small throughout the algorithm's execution. As we will see, the (expected) rate at which 1-clauses are generated in round t is $C_2(t)/(n-2t) + \mathrm{o}(1)$. Thus, by keeping track of only $t, C_2(t)$, and $C_3(t)$ the algorithm can take $w(t)$ to be arbitrarily close to (but greater than) this rate. This keeps the algorithm safe without sacrificing its efficiency (we will define $w(t)$ more precisely later). The proof of Lemma 2 appears in Appendix B.

Lemma 2 (Lazy-server). *Let $F(0), F(1), \ldots$ be a sequence of random variables and denote $f(t) = \mathbf{E}(F(t))$. Let $W(0), W(1), \ldots$ be a sequence of independent Bernoulli random variables with density $w(t)$, i.e. $W(t) = 1$ with probability $w(t)$, and 0 otherwise. For a given integer $s > 0$, let $Q(0), Q(1), \ldots$ be the sequence of random variables defined by $Q(0) = 0$ and $Q(t+1) = \max(Q(t) - s \cdot W(t), 0) + F(t)$. Assume that there exist constants $a, b, c > 0$ such that for any fixed $j \geq i \geq 0$ and any $\delta > 0$,*

$$\Pr\left[\sum_{t=i}^{j} F(t) > (1+\delta) \sum_{t=i}^{j} f(t)\right] < \exp\left(-a\delta^b \left(\sum_{t=i}^{j} f(t)\right)^c\right).$$

Then, if for some $\epsilon, \lambda > 0$ and all $t \geq 0$, we have

$$(1-\epsilon)s \times w(t) > f(t) > \lambda \ , \tag{1}$$

there exist constants C and k depending on $a, b, c, s, \epsilon, \lambda$ such that for every $m \geq 1$,

$$\Pr\left[\max_{0 \leq t < m} Q(t) > \log^k m\right] = \mathrm{O}(m^{-2}) \tag{2}$$

$$\Pr\left[\sum_{t=0}^{m-1} Q(t) > Cm\right] = \mathrm{O}(m^{-2}) \ . \tag{3}$$

5. THE PROOF

Let $\epsilon = 10^{-6}$, $\zeta = 10^{-1}$ and $t_e = \lfloor 0.4n \rfloor$. Let $r^* = 3.1456$. To prove $r_3 > 3.145$ we will prove

Lemma 3. *Let F be a random formula resulting by taking the conjunction of $F_3(n, r^*n)$ and $F_2(n, \epsilon n)$. There exists a choice of ϕ, ψ and constants k, M such that if we run mTT on F for t_e rounds, each of the following holds w.h.p.*

$$C_1(t_e) \ < \ \log^k n \ , \tag{4}$$

$$\sum_{t=0}^{t_e} C_1(t) \ < \ Mn \ , \tag{5}$$

$$C_2(t_e) + C_3(t_e) \ < \ (1-\zeta)(n - 2t_e) \ . \tag{6}$$

Before proving Lemma 3 let us see how it implies Theorem 1.

Proof of Theorem 1. We will prove that F is satisfiable with positive probability, implying that $F_3(n, r^*n)$ is satisfiable with positive probability. By Corollary 1 this suffices. Let F_e be the random formula derived by: i) running mTT on F for t_e rounds, ii) removing any 0-clauses that might have been generated, and iii) removing precisely one randomly chosen literal from each remaining 3-clause. By uniform randomness, F_e is a conjunction of $F_2(n - 2t_e, C_2(t_e) + C_3(t_e))$ and $F_1(n - 2t_e, C_1(t_e))$, where $n - 2t_e = \Omega(n)$. Thus, by Lemma 1 and (4),(6) it follows that F_e is satisfiable w.h.p. Therefore, to prove that F is satisfiable with positive probability it suffices to prove that $\mathcal{C}_0(t_e) = \emptyset$ with positive probability. (Here, and elsewhere, we use that if an event A holds w.h.p. then for any event B, $\Pr[A \cap B] \geq \Pr[B] - \mathrm{o}(1)$.)

To bound $\Pr[\mathcal{C}_0(t_e) = \emptyset]$ from below, we first observe that the probability of a 0-clause being generated in a given round t is completely determined by $\mathcal{C}_2(t), \mathcal{C}_1(t)$ since each clause shrinks by at most one literal for each variable set. In particular, let x, y be the two variables set in round t. Then, for a 0-clause to be generated in that round either there must be a 2-clause in $\mathcal{C}_2(t)$ containing both x and y or at least one of x, y must be the underlying variable for a literal in $\mathcal{C}_1(t)$. Therefore, by uniform randomness, if $C_2(t) = q$ and $C_1(t) = s$ the probability that a 0-clause is not generated in round t is at least

$$\left(1 - \frac{1}{4\binom{n-2t}{2}}\right)^q \left(1 - \frac{1}{(n-2t)}\right)^s \ ,$$

which for $t \le t_e$ is bounded by $(1-6/n)^{s+20}$. Since w.h.p.

$$\sum_{t=0}^{t_e} C_1(t) < Mn \ ,$$

it follows that the probability of $\mathcal{C}_0(t_e) = \emptyset$ is at least

$$\left(1-\frac{6}{n}\right)^{(M+20)n} + \mathrm{o}(1) \ge e^{-6(M+20)} + \mathrm{o}(1) \ ,$$

which is bounded away from 0, as desired. □

To prove Lemma 3 we will trace the evolution of the random variables $C_i(t)$, $i = 2,3$, for $0 \le t \le t_e$. In particular, the lemma will follow from Lemma 4 below (this last proof appears in Appendix B). Let $\delta = 10^{-7}$, and recall the definition of ζ, t_e and F from Lemma 3. Also, recall that ϕ, ψ are the functions determining the density of $W(t), E(t)$ respectively.

LEMMA 4. *There exists a choice of ϕ, ψ such that if we run* mTT *on F for t_e rounds, then each of the following holds w.h.p.*

- *For all $0 \le t \le t_e$, $C_2(t) < 2(1-\delta)w(t)(n-2t)$.*
- *$C_2(t_e) + C_3(t_e) < (1-\zeta)(n-2t_e)$.*

Proof of Lemma 4. We will apply Theorem 3 for random variables C_2, C_3 taking $m = n$ and $C = r^*$ (as $C_i(t) \le r^* n$ for all t). Thus, $\mathbf{H}(t) = \langle \vec{C}(0), \ldots, \vec{C}(t) \rangle$, where $\vec{C}(t) = (C_2(t), C_3(t))$. With foresight, we take the domain D to be

$$D = \{(y_1, y_2, y_3) : 0 \le y_1 \le 0.41, y_2 \ge \epsilon/2, y_3 \ge \epsilon/2\} \ .$$

We will first determine the differential equation for C_3 and then for C_2.

• A clause leaves $\mathcal{C}_3(t)$ during round t iff it contains at least one of the variables set in round t. Hence, by uniform randomness, we see that conditional on $\mathbf{H}(t)$,

$$C_3(t+1) = C_3(t) - X \ ,$$

where $X \stackrel{\mathcal{D}}{=} \mathrm{Bin}(C_3(t), p_3(t))$ and

$$p_3(t) \equiv \frac{2 \times 8\binom{n-2t-2}{2} + 8\binom{n-2t-2}{1}}{8\binom{n-2t}{3}} = \frac{6}{n-2t} + \mathrm{o}(1/n) \ .$$

Thus, $\mathbf{E}(C_3(t+1) - C_3(t) \mid \mathbf{H}(t)) = -6C_3(t)/(n-2t) + \mathrm{o}(1)$. Moreover, applying the Chernoff bound to X implies that condition (ii) of Theorem 3 is satisfied immediately for C_3. Finally, if $f_3(y_1, y_2, y_3) = -6y_3/(1-2y_1)$, then

$$\mathbf{E}(C_3(t+1) - C_3(t) \mid \mathbf{H}(t)) = f_3(t/n, C_2(t)/n, C_3(t)/n) + \mathrm{o}(1).$$

It is clear that f_3 is continuous and satisfies a Lipschitz condition on D (since $y_1 \le 0.41$). Thus, the differential equation and initial condition corresponding to C_3 are

$$\frac{dz_3}{ds} = -\frac{6z_3}{1-2s} \ , \quad z_3(0) = r^* \ . \tag{7}$$

Solving (7), yields

$$z_3(s) = r^*(1-2s)^3 \ .$$

• Unlike the case for C_3, the expected change of C_2 in round t clearly depends on the values of $W(t), E(t)$.

($*$) If $W(t) = 1$ then, analogously to $\mathcal{C}_3$, each clause leaves $\mathcal{C}_2(t)$ during round t iff it contains at least one of the variables set in that round. Moreover, by uniform randomness, each clause in $\mathcal{C}_3(t)$ containing precisely one of the two variables set in round t, ends up in $\mathcal{C}_2(t+1)$ with probability 1/2. Therefore, letting

$$p_2(t) \equiv \frac{2 \times 4\binom{n-2t-2}{1} + 4\binom{n-2t-2}{0}}{4\binom{n-2t}{2}} = \frac{4}{n-2t} + \mathrm{o}(1/n) \ ,$$

$$p_{32}(t) \equiv \frac{1}{2}\,\frac{2 \times 8\binom{n-2t-2}{2}}{8\binom{n-2t}{3}} = \frac{3}{n-2t} + \mathrm{o}(1/n) \ ,$$

we see that conditional on $\mathbf{H}(t)$ and $W(t) = 1$,

$$C_2(t+1) = C_2(t) - X + Y \ ,$$

where $X \stackrel{\mathcal{D}}{=} \mathrm{Bin}(C_2(t), p_2(t))$ and $Y \stackrel{\mathcal{D}}{=} \mathrm{Bin}(C_3(t), p_{32}(t))$.

($*$) If $W(t) = 0$ we note that $(t/n, C_2(t)/n, C_3(t)/n) \in D$ implies $C_2(t)/n > \epsilon/3 > 0$ and therefore that there certainly exists $c = (\ell_1 \vee \ell_2) \in \mathcal{C}_2(t)$ to pick and either gently-satisfy or just-satisfy[1]. Moreover, every clause in $\mathcal{C}_2(t)$ other than c leaves $\mathcal{C}_2(t)$ during round t iff it contains at least one of $\mathrm{v}(\ell_1), \mathrm{v}(\ell_2)$. Therefore, the number of 2-clauses leaving $\mathcal{C}_2(t)$ during round t when $W(t) = 0$, is $T+1$, where $T \stackrel{\mathcal{D}}{=} \mathrm{Bin}(C_2(t)-1, p_2(t))$.

Before we proceed to analyze the distribution of the number of 3-clauses leaving $\mathcal{C}_3(t)$ and entering $\mathcal{C}_2(t+1)$ when $W(t) = 0$, let us observe that this number is bounded by the number, Z, of 3-clauses in $\mathcal{C}_3(t)$ containing precisely one of $\mathrm{v}(\ell_1), \mathrm{v}(\ell_2)$. Since $Z \stackrel{\mathcal{D}}{=} \mathrm{Bin}(C_3(t), 2p_{32}(t))$, by applying the Chernoff bound for each of X, Y, T, Z, we see that condition (ii) of Theorem 3 is satisfied for C_2 when $W(t) = 0$, independently of the value of $E(t)$.

Let U denote the random variable equal to the number of 3-clauses leaving $\mathcal{C}_3(t)$ and entering $\mathcal{C}_2(t+1)$ in round t. If $W(t) = 0$ and $E(t) = 1$ then U behaves identically to the case $W(t) = 1$. To see this, note that in order to just-satisfy($\ell_1 \vee \ell_2$) the algorithm does not consider any clauses in $\mathcal{C}_3(t)$ and, therefore, the claim follows by the uniform randomness of c.

To determine the distribution of U when $W(t) = E(t) = 0$ let $\mathcal{E}(t, \ell_1, \ell_2)$ be the set of all clauses in $\mathcal{C}_3(t)$ containing exactly one of $\ell_1, \bar{\ell}_1, \ell_2, \bar{\ell}_2$ (since a clause containing two of these literals either gets satisfied or ends up in $\mathcal{C}_1(t+1)$). Moreover, let X_1, X_2, X_3, X_4 be the random variables corresponding to the number of clauses in $\mathcal{E}(t, \ell_1, \ell_2)$ containing $\ell_1, \bar{\ell}_1, \ell_2, \bar{\ell}_2$, respectively. Finally, let us define the function $\mathrm{sb} : \mathbb{R}^4 \to \mathbb{R}$, by

$$\begin{aligned}\mathrm{sb}(w_1, w_2, w_3, w_4) = \min(&\min(w_1, w_2) + \max(w_3, w_4),\\ &\max(w_1, w_2) + \min(w_3, w_4)) \ .\end{aligned}$$

Thus, $\mathrm{sb}(X_1, X_2, X_3, X_4)$ is the number of 3-clauses that will leave $\mathcal{C}_3(t)$ to enter $\mathcal{C}_2(t+1)$ if we need to assign the "second best" value assignment to $\mathrm{v}(\ell_1), \mathrm{v}(\ell_2)$ in executing

[1]This is precisely the reason for which we add ϵn 2-clauses to the input formula: while initially (and for a long time) the rate at which 2-clauses are generated is substantially greater than the rate at which they disappear, if $\mathcal{C}_2(0) = \emptyset$ then it is possible that in the first polylog(n) rounds, $\mathcal{C}_2(t) = \emptyset$ occurs a number of times; the extra $\Omega(n)$ 2-clauses provide a "cushion" guaranteeing that w.h.p. this does not happen.

gently-satisfy. Note now that the probability of this last event is precisely 1/4 (independently of everything else). This is because the "best possible" value assignment for $v(\ell_1), v(\ell_2)$ is a function only of clauses in $C_3(t)$ and therefore, by uniform randomness, that assignment fails to satisfy $c \in C_2(t)$ with probability 1/4. Hence, conditional on $\mathbf{H}(t)$ and $W(t) = E(t) = 0$, the expected value of U is

$$\begin{aligned}&\frac{3}{4} \times \mathbf{E}(\min(X_1, X_2) + \min(X_3, X_4))\\ &+\frac{1}{4} \times \mathbf{E}(\mathrm{sb}(X_1, X_2, X_3, X_4)) \ .\end{aligned} \tag{8}$$

To determine the expectations in (8) we first note that while the random variables X_i are identically distributed, they are not independent; e.g. if $X_1 = C_3(t)$ then $X_2 = 0$. Yet, since the number of appearances of each literal is, asymptotically, distributed as a Poisson random variable with constant mean, it is intuitively clear that as long as both t and $C_3(t)$ are $\Omega(n)$, the dependence between the X_i is minuscule. In particular, let $p^* = \frac{3}{2(n-2t)}$ denote the probability that a clause in $C_3(t)$ contains a given literal. Now, let $X'_1, \ldots, X'_4$ be i.i.d. random variables with $X'_i \stackrel{D}{=} \mathrm{Bin}(C_3(t), p^*)$. It is not hard to prove that for $(t/n, C_2(t)/n, C_3(t)/n) \in D$, the quantity in (8) equals

$$\begin{aligned}&\frac{3}{4} \times 2\,\mathbf{E}(\min(X'_1, X'_2))\\ &+\frac{1}{4} \times \mathbf{E}(\mathrm{sb}(X'_1, X'_2, X'_3, X'_4)) + \mathrm{o}(1) \ .\end{aligned} \tag{9}$$

To handle the expectations in (9) we use the following lemma (its proof appears in Appendix C).

LEMMA 5. *Let $S_1, \ldots, S_4$ be i.i.d. random variables with $S_i \stackrel{D}{=} \mathrm{Bin}(N,p)$, where $Np = \lambda + \mathrm{o}(1)$ for some constant $\lambda > 0$ (asymptotically in N). Let $Y = \min(S_1, S_2)$, and $Z = \mathrm{sb}(S_1, S_2, S_3, S_4)$.*

(a) There exist functions $g, h : \mathbb{R} \to \mathbb{R}$ such that $\mathbf{E}(Y) = g(\lambda) + \mathrm{o}(1)$ and $\mathbf{E}(Z) = h(\lambda) + \mathrm{o}(1)$.

(b) Let functions γ, χ be as defined in Appendix C. Then γ, χ are continuous, satisfy a Lipschitz condition in $[0, \infty)$, and for all $\lambda > 0$,

$$g(\lambda) < \gamma(\lambda) \le \lambda \quad \textit{and} \quad h(\lambda) < \chi(\lambda) \le 2\lambda \ .$$

Recall that $\mathbf{E}(X'_i) = 3C_3(t)/(2(n-2t))$. Therefore, from (a) of Lemma 5 we get $\mathbf{E}(U \mid \mathbf{H}(t) \cap W(t) = E(t) = 0) = f_U(t/n, C_2(t)/n, C_3(t)/n) + \mathrm{o}(1)$, where

$$f_U(y_1, y_2, y_3) = \frac{3}{2} g\left(\frac{3y_3}{2(1-2y_1)}\right) + \frac{1}{4} h\left(\frac{3y_3}{2(1-2y_1)}\right) \ .$$

Thus, combining our estimates for the different cases we get $\mathbf{E}(C_2(t+1) - C_2(t) \mid \mathbf{H}(t)) = f_2(t/n, C_2(t)/n, C_3(t)/n) + \mathrm{o}(1)$, where [writing $\phi(y_1, y_2, y_3)$ as ϕ and $\psi(y_1, y_2, y_3)$ as ψ]

$$\begin{aligned}f_2(y_1, y_2, y_3) = &\\ &\phi \times \frac{3y_3}{1-2y_1}\\ &+ (1-\phi) \times \left(\psi \frac{3y_3}{1-2y_1} + (1-\psi) f_U(y_1, y_2, y_3) - 1\right)\\ &- \frac{4y_2}{1-2y_1} \ .\end{aligned}$$

Let $\xi = \xi(y_1, y_3) \equiv \frac{3y_3}{2(1-2y_1)}$. For γ, χ as in Lemma 5, we define ψ by

$$\psi(y_1, y_2, y_3) = \frac{\frac{3}{2}\gamma(\xi) + \frac{1}{4}\chi(\xi) - f_U(y_1, y_2, y_3)}{\xi - f_U(y_1, y_2, y_3)} \tag{10}$$

so that [again writing $\phi(y_1, y_2, y_3)$ as ϕ] f_2 simplifies to

$$\begin{aligned}f_2(y_1, y_2, y_3) = &\\ &\phi \times \frac{3y_3}{1-2y_1}\\ &+ (1-\phi) \times \left(\frac{3}{2}\gamma\left(\frac{3y_3}{2(1-2y_1)}\right) + \frac{1}{4}\chi\left(\frac{3y_3}{2(1-2y_1)}\right) - 1\right)\\ &- \frac{4y_2}{1-2y_1} \ .\end{aligned}$$

Note that our choice of ψ above is valid since, by Lemma 5, both enumerator and denominator in (10) are strictly positive, and the former is no greater than the latter.

Regarding the choice of ϕ, it is not hard to see that the rate at which 1-clauses are generated is $2C_2(t)/(n-2t) + \mathrm{o}(1)$ for all t (we show this in the proof of Lemma 3). Thus, as one might guess, we choose ϕ so that for some arbitrarily small $\theta > 0$, (and as long as $C_2(t)/(n-2t) < 1$)

$$2 \cdot \phi(t/n, C_2(t)/n, C_3(t)/n) = (1+\theta)\frac{2C_2(t)}{n-2t} \ .$$

Hence, for some (small) θ to be specified, we define

$$\phi(y_1, y_2, y_3) = \min\left(\frac{(1+\theta)y_2}{1-2y_1}, 1\right) \ .$$

With this choice of ϕ and recalling that $z_3(s) = r^*(1-2s)^3$, we let $\tau_\theta(s, z_2) \equiv \min\left(\frac{(1+\theta)z_2}{1-2s}, 1\right)$ and $\nu(s) \equiv 3r^*(1-2s)^2$. The differential equation and initial condition corresponding to C_2 are thus

$$\begin{aligned}\frac{dz_2}{ds} = \ &\tau_\theta(s, z_2) \times \nu(s)\\ &+ (1 - \tau_\theta(s, z_2)) \times \left(\frac{3}{2}\gamma\left(\frac{\nu(s)}{2}\right) + \frac{1}{4}\chi\left(\frac{\nu(s)}{2}\right) - 1\right)\\ &- \frac{4z_2}{1-2s} \ ,\end{aligned}$$

$$z_2(0) = \epsilon \ .$$

It is easy to verify that for $s \in [0,1)$ and $z_2 \in [0, \infty)$, dz_2/ds is continuous and satisfies a Lipschitz condition (therefore satisfying the condition of Theorem 3 on D).

Taking $\theta = 10^{-5}$, we solved the above differential equation numerically, using two different methods. The first one, easy to use but without guaranteed results, was by employing the numerical option in the `dsolve` function in Maple [36]. The second method was by using the *interval arithmetic* differential equation solver in [35]. The latter, partitions the domain of s in intervals and returns *guaranteed*, i.e. provable, upper and lower bounds for the value of z_2 in each interval. (Maple remained inside those bounds out to six decimal digits.)
The lower bounds calculated using interval arithmetic give that indeed for all $s \in [0, 0.41]$, $z_2(s) > 0.9\epsilon$ and thus that

z_2 does not leave the domain for $s \le 0.41$. (For z_3 this follows immediately from the fact that z_3 is decreasing and $z_3(0.41) = 0.018.. > \epsilon/2$.) The upper bounds calculated for z_2 yield that indeed for all $s \in [0, 0.41]$, $z_2(s)/(1-2s) < (1-\delta)/(1+\theta)$ and therefore that indeed with our choice of ϕ, ψ w.h.p.

$$\frac{C_2(t)}{n-2t} < 2(1-\delta)w(t) \ , \quad \text{for all } 0 \le t \le t_e \ .$$

Finally, the upper bound $z_2(0.4) < 0.13$ along with $z_3(0.4) = 0.025..$ imply that w.h.p.

$$C_2(t_e) + C_3(t_e) < (1-\zeta)(n-2t_e) \ .$$

□

6. DISCUSSION

More than two variables: In setting two variables at a time, our algorithm exploits the correlation implicit in the fact that the two variables chosen appear in the same 2-clause. It is not hard to see that since the underlying 2-SAT formula is sparse, picking at random any constant number $q > 1$ of 2-clauses would not yield further progress: the q 2-clauses and the corresponding 3-clauses involved, w.h.p. will have no variables in common; thus, the decisions for each pair of variables would be independent of the choices made for the other pairs.

Backtracking: It is not hard to show that TT can be modified to incorporate a limited form of backtracking (that proposed in [19]), so that it succeeds with w.h.p. for all $r \le 3.145$.

A question on (2+p)-SAT: In [33; 34], using the non-rigorous "replica method" of statistical physics, it was suggested that there exists $c > 0$ such that for any $\epsilon > 0$, a conjunction of $F_2(n, (1-\epsilon)n)$ and $F_3(n, cn)$ (on the same n variables) is w.h.p. satisfiable; moreover, it was proposed that if c_3 is the greatest such c, then $c_3 \approx 0.71...$ While the proposition $c_3 > 0$ is perhaps counterintuitive, in [1] it was shown that indeed $2/3 \le c_3 \le 2.21$. One of the benefits of analyzing satisfiability algorithms using our framework is a very simple proof of this lower bound for c_3. In particular, one can show that all the algorithms considered in [5; 19], along with TT, succeed with positive probability on a conjunction of $F_2(n, (1-\epsilon)n)$ and $F_3(n, cn)$, for any $\epsilon > 0$ and $c \le 2/3$ (and this probability can be suitably boosted to $1 - o(1)$). Yet, also using our methods, one can show that replacing 2/3 by any greater constant causes each of these algorithms to fail w.h.p.

Determining whether $c_3 = 2/3$ is a very interesting open problem on its own, with significant implications for the replica method. Moreover, any improvement over $c_3 \ge 2/3$ would immediately yield an improved lower bound for r_3.

7. ACKNOWLEDGEMENTS

I want to thank Luc Devroye, Alan Frieze, Jeong Han Kim, Heikki Mannila, Michael Molloy, Ned Nedialkov and Boris Pittel for numerous helpful suggestions. Special thanks to Lefteris Kirousis for many illuminating conversations, one of which led to the lazy-server lemma.

Work supported in part by a Postoctoral Fellowship from the National Science and Engineering Council of Canada.

APPENDIX

A. APPENDIX

In the statement of Theorem 3, below, asymptotics denoted by o and O, are for $n \to \infty$ but uniform over all other variables. In particular, "uniformly" refers to the convergence implicit in the o() terms. For a random variable X, we say $X = o(f(n))$ *always* if $\max\{x \mid \Pr[X = x] \neq 0\} = o(f(n))$. We say that a function f satisfies a *Lipschitz condition* on $D \subseteq \mathbb{R}^j$ if there exists a constant $L > 0$ such that $|f(u_1, \ldots, u_j) - f(v_1, \ldots, v_j)| \le L \sum_{i=1}^{j} |u_i - v_i|$, for all $(u_1, \ldots, u_j)$ and $(v_1, \ldots, v_j)$ in D.

THEOREM 3 ([38]). *Let $Y_i(0), Y_i(1), \ldots, Y_i(t), \ldots$ be a sequence of real-valued random variables, $1 \le i \le k$ for some fixed k, such that for all i, t, n, $|Y_i(t)| \le Cn$ for some constant C. Let $\mathbf{H}(t)$ be the history of the sequence, i.e. the matrix $\langle \vec{Y}(0), \ldots, \vec{Y}(t) \rangle$, where $\vec{Y}(t) = (Y_1(t), \ldots, Y_k(t))$. Define the set I to be*

$$\{(y_1, \ldots, y_k) : \Pr[\vec{Y}(0) = (y_1 n, \ldots, y_k n)] \neq 0 \text{ for some } n\} \ .$$

Let D be some bounded connected open set containing the intersection of $\{(s, y_1, \ldots, y_k) : s \ge 0\}$ with a neighborhood[2] *of $\{(0, y_1, \ldots, y_k) : (y_1, \ldots, y_k) \in I\}$.*

Let $f_i : \mathbb{R}^{k+1} \to \mathbb{R}$, $1 \le i \le k$, and suppose that for some $m = m(n)$,

(i) for all i and uniformly over all $t < m$,

$$\mathbf{E}\left(Y_i(t+1) - Y_i(t) | \mathbf{H}(t)\right) = f_i(t/n, Y_0(t)/n, \ldots, Y_k(t)/n) + o(1) \ , \ \textit{always};$$

(ii) for all i and uniformly over all $t < m$,

$$\Pr\left[|Y_i(t+1) - Y_i(t)| > n^{1/5} \middle| \mathbf{H}(t) \right] = o(n^{-3}) \ , \ \textit{always};$$

(iii) for each i, the function f_i is continuous and satisfies a Lipschitz condition on D.

Then

(a) for $(0, \hat{z}^{(0)}, \ldots, \hat{z}^{(k)}) \in D$ the system of differential equations

$$\frac{dz_i}{ds} = f_i(s, z_0, \ldots, z_k), \qquad 1 \le i \le k$$

has a unique solution in D for $z_i : \mathbb{R} \to \mathbb{R}$ passing through $z_i(0) = \hat{z}^{(i)}$, $1 \le i \le k$, and which extends to points arbitrarily close to the boundary of D;

(b) almost surely

$$Y_i(t) = z_i(t/n) \cdot n + o(n) \ ,$$

uniformly for $0 \le t \le \min\{\sigma n, m\}$ and for each i, where $z_i(s)$ is the solution in (a) with $\hat{z}^{(i)} = Y_i(0)/n$, and $\sigma = \sigma(n)$ is the supremum of those s to which the solution can be extended.

Note: The theorem remains valid if the reference to "always" in (i),(ii) is replaced by the restriction to the event $(t/n, Y_0(t)/n, \ldots, Y_k(t)/n) \in D$.

[2] That is, after taking a ball around the set I, we require D to contain the part of the ball in the halfspace corresponding to $s = t/n \ge 0$.

B. APPENDIX

Proof of Lemma 2. Let us say that Q *returns* at step t, if $Q(t) < s$ and $Q(t-1) \geq s$; let us say that Q *departs* at step t, if $Q(t) \geq s$ and $Q(t-1) < s$. For $j \geq 0$, let $B_j = t_j^r - t_j^d$, where $t_j^r, t_j^d > 0$ are the steps corresponding to the jth return and the jth departure, respectively. For $t \geq 0$, let $h^r(t) = \min\{j : t_j^r \geq t\}$, i.e. the index of the first return occurring no earlier than t.

We first observe that for any values (realizations) $b_0, b_1, \ldots$ of the random variables B_j,

$$\sum_{t=0}^{m-1} Q(t) \leq \sum_{j=0}^{h^r(m-1)} \frac{1}{2} b_j(s(b_j+1)-2) \leq s \cdot \sum_{j=0}^{h^r(m-1)} b_j^2 ,$$

since Q decreases by at most s in each step and, therefore, cannot exceed $s(b_j+1)-2$ between t_j^d and t_j^r (the "worst case" occurs when Q "shoots up" from below s and then continually drops).

For each $i = 0, \ldots, s-1$ and $t = 0, 1, \ldots$, let us define two sequences of random variables $W_t^i(z), F_t^i(z)$, $z \geq 0$, by $W_t^i(z) \overset{D}{=} W(t+z)$ and $F_t^i(z) \overset{D}{=} F(t+z)$. Now, for each $i = 0, \ldots, s-1$ and $t = 0, 1, \ldots$, we define the sequence of random variables $D_t^i(z)$, as follows: $D_t^i(0) = i$ and $D_t^i(z+1) = \max\left(D_t^i(z) - s \cdot W_t^i(z), 0\right) + F_t^i(z)$. Finally, let $b_t^i = \min\{z > t : D_t^i(z) < s\}$. If we now consider for each sequence D_t^i its subsequence from $z = 0$ to $z = b_t^i$ we see that Q is realized by some concatenation of these subsequences. Therefore,

$$\sum_{t=0}^{m-1} Q(t) \leq s \cdot \sum_{i=0}^{s-1} \sum_{t=0}^{m-1} (b_t^i)^2 \equiv s \cdot Z .$$

To get a handle on the distribution of Z we will bound $\Pr[b_t^i \geq x]$ for each i, t and integer $x \geq 0$. For this, we first observe that if for some $l > 0$,

$$\sum_{z=0}^{l} F_t^i(z) < s \cdot \sum_{z=0}^{l} W_t^i(z) \tag{11}$$

then there exists $0 < z \leq l$ such that $D_t^i(z) < s$. So, for a fixed l, the probability that (11) does not hold is bounded by

$$\begin{aligned} &\Pr\left[\sum_{z=0}^{l} F_t^i(z) > (1+\epsilon/3)\sum_{z=0}^{l} f(t+z)\right] \\ &+ \Pr\left[\sum_{z=0}^{l} W_t^i(z) < (1-\epsilon/3)\sum_{z=0}^{l} w(t+z)\right] , \end{aligned} \tag{12}$$

since if neither of the events in (12) occurs, then (1) implies that (11) holds.

Now, using the fact that both $w(t), f(t)$ are bounded away from 0 for all t, along with the given tail bound for $\sum F(t)$, and the Chernoff bound for $\sum W(t)$, we get that there exist $\eta, \zeta > 0$ depending on $a, b, c, s, \epsilon, \lambda$ such that for all i, t

$$\Pr[b_t^i \geq x] < \exp(-\eta x^{\zeta}) . \tag{13}$$

Thus, Z is the sum of sm independent random variables $R_0, \ldots, R_{sm-1}$ (where $R_{st+i} = (b_t^i)^2$) such that for every integer $x \geq 0$, $\Pr[R_j \geq x^2] \leq \exp(-\eta x^{\zeta})$. Hence, $\mathbf{E}[R_j]$ is bounded by a constant:

$$\mathbf{E}[R_j] = \sum_{y=0}^{\infty} \Pr[R_j > y] \leq \sum_{y=0}^{\infty} \exp(-\eta(\lfloor\sqrt{y}\rfloor)^{\zeta}) < K(\eta, s, \zeta) .$$

Let $k = \lceil 3/\zeta \rceil$ and write $K \equiv K(\eta, s, \zeta)$. To conclude the proof we let

$$R_j' = \begin{cases} R_j & \text{if } R_j \leq \log^k m, \\ 0 & \text{if } R_j > \log^k m. \end{cases}$$

and

$$Z' = \sum_{j=0}^{sm-1} R_j' .$$

We first observe that $\Pr[Z \neq Z'] \leq sm \Pr[R_j \neq R_j'] = \mathrm{O}(m^{-2})$ (we take $\mathrm{O}(m^{-2})$ as it is sufficient for our purposes). This immediately proves our claim in (2). Moreover, $\mathbf{E}[Z'] \leq \mathbf{E}[Z] \leq Km$. Thus, for $L = L(a, b, c, s, \epsilon, \lambda) = 2K$ we get

$$\begin{aligned} \Pr[Z > Lm] &\leq \Pr[Z' > 2Km] + \mathrm{O}(m^{-2}) \\ &\leq \Pr[Z' - \mathbf{E}(Z') > Km] + \mathrm{O}(m^{-2}) . \end{aligned} \tag{14}$$

To bound the probability in (14) we consider the martingale sequence formed by the random variables $T_0, T_1, \ldots, T_{sm-1}$ where $T_0 = \mathbf{E}(Z')/\log^k m$ and T_{j+1} is $1/\log^k m$ times the conditional expectation of Z' given the values of $R_0', \ldots, R_j'$. Applying Azuma's inequality, yields

$$\Pr[Z' - \mathbf{E}(Z') > Km] < 2\exp\left(-\frac{K^2 m}{2(\log m)^{\frac{3}{\zeta}}}\right) = \mathrm{O}(m^{-2}) ,$$

and, thus, taking $C = sL$ yields (3). □

Proof of Lemma 3. Since, by Lemma 4, (6) holds w.h.p. it will suffice to prove that each of (4) and (5) hold w.h.p. Let $\mathit{flow}_1(t)$ be the random variable equal to the number of clauses that shrink to length 1 during round t. Then, $C_1(0) = 0$ and it is easy to see that for all $t \geq 0$,

$$C_1(t+1) \leq \max(C_1(t) - 2 \cdot W(t), 0) + \mathit{flow}_1(t) . \tag{15}$$

Let $G(t)$ be defined by $G(0) = 0$ and $G(t+1) = \max(G(t) - 2 \cdot W(t), 0) + \mathit{flow}_1(t)$, for $t \geq 0$. An easy induction shows that $G(t) \geq C_1(t)$ for all t. Now, let

$$\begin{aligned} p_{21}(t) &= \frac{4\binom{n-2t-2}{1}}{4\binom{n-2t}{2}} = \frac{2}{n-2t} + \mathrm{o}(1) , \\ p_{31}(t) &= \frac{2\binom{n-2t-2}{1}}{8\binom{n-2t}{3}} = \frac{3}{2(n-2t)^2} + \mathrm{o}(1) . \end{aligned}$$

By uniform randomness it follows that $\mathit{flow}_1(t) = \mathit{flow}_{21}(t) + \mathit{flow}_{31}(t)$, where

$$\begin{aligned} \mathit{flow}_{21}(t) &\overset{D}{=} \mathrm{Bin}(X(t), p_{21}(t)) , \\ \mathit{flow}_{31}(t) &\overset{D}{=} \mathrm{Bin}(C_3(t), p_{31}(t)) , \end{aligned}$$

and $X(t)$ is either $C_2(t)$ or $C_2(t) - 1$.

Using the above facts and Lemma 4 it is straightforward to construct, via a simple coupling, a random variable $Q(t)$ which i) satisfies the conditions of Lemma 2 by construction, and such that ii) w.h.p. $C_1(t) \leq Q(t)$ for all $0 \leq t \leq t_e$. The lemma then follows by applying Lemma 2 for Q and using the fact that if events A and B each hold w.h.p. then so does the event $A \cap B$. □

C. APPENDIX

Definition of function γ: γ is the *piecewise linear* function defined by $\gamma(0) = 0$, $\gamma(1) = 0.476223$ $\gamma(3/2) = 0.840260$, $\gamma(2) = 1.228495$, $\gamma(5/2) = 1.631218$, $\gamma(3) = 2.043874$, $\gamma(7/2) = 2.463906$, $\gamma(4) = 2.889703$, $\gamma(9/2) = 3.320170$, $\gamma(5) = 3.754520$, $\gamma(6) = 6$; $\gamma(\lambda) = \lambda$, for $\lambda \geq 6$.
Definition of function χ: to define χ let $z(\lambda) = \frac{1}{100}(2\lambda^2 + 174\lambda - 22)$. Then, for $\lambda \in [0, 1/2]$, $\chi(\lambda) = 2\lambda$; for $\lambda \in [1/2, 1]$, $\chi(\lambda) = 2(z(1) - 1)\lambda + 2 - z(1)$; for $\lambda \in [1, 5]$, $\chi(\lambda) = z(\lambda)$; for $\lambda \in [5, 6]$, $\chi(\lambda) = (12 - z(5))\lambda + 6z(5) - 60$; $\chi(\lambda) = 2\lambda$, for $\lambda \geq 6$.

Proof of Lemma 5.
a) Using the standard approximation of the Binomial random variable with the corresponding Poisson random variable it is easy to show that

$$\begin{aligned} \mathbf{E}(Y) &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} e^{-2\lambda}\frac{\lambda^{i+j}}{i!j!}\min(i,j) + \mathrm{o}(1) \\ &\equiv g(\lambda) + \mathrm{o}(1) \ , \end{aligned}$$

and

$$\begin{aligned} \mathbf{E}(Z) &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{\infty}\sum_{l=0}^{\infty} e^{-4\lambda}\frac{\lambda^{i+j+k+l}}{i!j!k!l!}\mathrm{sb}(i,j,k,l) + \mathrm{o}(1) \\ &\equiv h(\lambda) + \mathrm{o}(1) \ . \end{aligned}$$

b) The fact that γ, χ are continuous and satisfy a Lipschitz condition on $[0, \infty)$ is trivial to verify by inspection. Similarly, for the facts $\gamma(\lambda) \leq \lambda$ and $\chi(\lambda) \leq 2\lambda$, for all $\lambda \geq 0$. From the fact that the inequalities $\min(i,j) \leq (i+j)/2$ and $\mathrm{sb}(i,j,k,l) \leq (i+j+k+l)/2$ are strict for certain i, j we get that for all $\lambda > 0$, $g(\lambda) < \lambda$ and $h(\lambda) < 2\lambda$. This yields that for $\lambda > 6$, $g(\lambda) < \gamma(\lambda)$ and $h(\lambda) < \chi(\lambda)$. Therefore, we are left to prove $g(\lambda) < \gamma(\lambda)$ and $h(\lambda) < \chi(\lambda)$, for $\lambda \in (0, 6]$.

To show that γ strictly bounds g from above we will use the following fact (due to Diaconis, see p. 293 in [29]): if $W_1, \ldots, W_k$ are i.i.d. Poisson random variables with mean λ, and $\phi : \mathbb{R}^k \to \mathbb{R}$ is a convex function, then $\mathbf{E}(\phi(W_1, \ldots, W_k))$ is a convex function of λ. Since min is convex, it follows that g is bounded from above by any piecewise linear function defined by upper bounds for values of g. To get such bounds, we use that for any $u \geq 0$,

$$\begin{aligned} g(\lambda) &\leq \lambda - \sum_{i=0}^{u}\sum_{j=0}^{u} e^{-2\lambda}\frac{\lambda^{i+j}}{i!j!}\left(\frac{i+j}{2} - \min(i,j)\right) \\ &\equiv \lambda - q_u(\lambda) \ . \end{aligned} \tag{16}$$

Now, q_u can be bounded numerically with *guaranteed* accuracy using interval arithmetic. For this, we used the function shake of Maple [36]. The values defining γ were derived by substituting the returned lower bound for q_{40} at each respective point to (16), dividing by $1 - 10^{-8}$, and rounding up.
For h matters are complicated by the fact that sb is not a convex function. Analogously to g, though, we note that for any $u \geq 0$, h is bounded by

$$\begin{aligned} 2\lambda &- \sum_{i=0}^{u}\sum_{j=0}^{u}\sum_{k=0}^{u}\sum_{l=0}^{u} e^{-4\lambda}\frac{\lambda^{i+j+k+l}}{i!j!k!l!}\frac{i+j+k+l}{2} \\ &+ \sum_{i=0}^{u}\sum_{j=0}^{u}\sum_{k=0}^{u}\sum_{l=0}^{u} e^{-4\lambda}\frac{\lambda^{i+j+k+l}}{i!j!k!l!}\mathrm{sb}(i,j,k,l) \\ &\equiv 2\lambda - h_u(\lambda) \ . \end{aligned}$$

By inspection, i.e. plotting, we observed that $z(\lambda)$ bounds $2\lambda - h_{15}(\lambda)$ from above in $[1/2, 6]$. To prove this we used interval arithmetic to bound the range of $z(\lambda) - 2\lambda + h_{15}(\lambda)$ from below for $\lambda \in [1/2, 6]$; we got a lower bound of 8.32603×10^{-7}. For $(0, 1/2]$ the fact $h(\lambda) < \chi(\lambda)$ follows from the fact $h(\lambda) < 2\lambda$ for all $\lambda > 0$ and the definition of χ. □

D. REFERENCES

[1] D. Achlioptas, L. M. Kirousis, E. Kranakis, and D. Krizanc. Rigorous results for random $(2+p)$-SAT. In *Proceedings of RALCOM 97 (Santorini, Greece)*, pages 1–13, 1997. Submitted to Theoret. Comput. Sci.

[2] P. Beame and T. Pitassi. Propositional proof complexity: past, present, and future. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (65):66–89, 1998.

[3] B. Bollobás, C. Borgs, J. Chayes, J. H. Kim, and D. B. Wilson. The scaling window of the 2-SAT transition. Manuscript, 1999.

[4] A. Z. Broder, A. M. Frieze, and E. Upfal. On the satisfiability and maximum satisfiability of random 3-CNF formulas. In *4th Annual ACM-SIAM Symposium on Discrete Algorithms (Austin, TX, 1993)*, pages 322–330. ACM, New York, 1993.

[5] M.-T. Chao and J. Franco. Probabilistic analysis of two heuristics for the 3-satisfiability problem. *SIAM J. Comput.*, 15(4):1106–1118, 1986.

[6] V. Chvátal and B. Reed. Mick gets some (the odds are on his side). In *33th Annual Symposium on Foundations of Computer Science (Pittsburgh, PA, 1992)*, pages 620–627. IEEE Comput. Soc. Press, Los Alamitos, CA, 1992.

[7] V. Chvátal and E. Szemerédi. Many hard examples for resolution. *J. Assoc. Comput. Mach.*, 35(4):759–768, 1988.

[8] S. A. Cook. The complexity of theorem-proving procedures. In *3rd Annual ACM Symposium on Theory of Computing (Shaker Heights, OH, 1971)*, pages 151–158. ACM, New York, 1971.

[9] S. A. Cook and D. G. Mitchell. Finding hard instances of the satisfiability problem: a survey. In *Satisfiability problem: theory and applications (Piscataway, NJ, 1996)*, pages 1–17. Amer. Math. Soc., Providence, RI, 1997.

[10] M. Davis, G. Logemann, and D. Loveland. A machine program for theorem-proving. *Comm. ACM*, 5:394–397, 1962.

[11] M. Davis and H. Putnam. A computing procedure for quantification theory. *J. Assoc. Comput. Mach.*, 7:201–215, 1960.

[12] O. Dubois and Y. Boufkhad. A general upper bound for the satisfiability threshold of random r-SAT formulae. *J. Algorithms*, 24(2):395–420, 1997.

[13] O. Dubois, Y. Boufkhad, and J. Mandler. Typical random 3-SAT formulae and the satisfiability threshold. In *11th Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000)*, pages 126–127. ACM, New York, 2000.

[14] A. El Maftouhi and W. Fernandez de la Vega. On random 3-SAT. *Combin. Probab. Comput.*, 4(3):189–195, 1995.

[15] W. Fernandez de la Vega. On random 2-SAT. 1992. Manuscript.

[16] J. Franco. Probabilistic analysis of the pure literal heuristic for the satisfiability problem. *Ann. Oper. Res.*, 1:273–289, 1984.

[17] J. Franco and M. Paull. Probabilistic analysis of the Davis–Putnam procedure for solving the satisfiability problem. *Discrete Appl. Math.*, 5(1):77–87, 1983.

[18] E. Friedgut. Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-SAT problem. *J. Amer. Math. Soc.*, 12:1017–1054, 1999.

[19] A. M. Frieze and S. Suen. Analysis of two simple heuristics on a random instance of k-SAT. *J. Algorithms*, 20(2):312–355, 1996.

[20] A. Goerdt. A threshold for unsatisfiability. *J. Comput. System Sci.*, 53(3):469–486, 1996.

[21] A. Goldberg. On the complexity of the satisfiability problem. In *4th Workshop on Automated Deduction (Austin, TX, 1979)*, pages 1–6, 1979.

[22] A. Haken. The intractability of resolution. *Theoret. Comput. Sci.*, 39(2-3):297–308, 1985.

[23] S. Janson, Y. C. Stamatiou, and M. Vamvakari. Bounding the unsatisfiability threshold of random 3-SAT. 1999. Submitted.

[24] A. Kamath, R. Motwani, K. Palem, and P. Spirakis. Tail bounds for occupancy and the satisfiability threshold conjecture. *Random Structures Algorithms*, 7(1):59–80, 1995.

[25] R. Karp and M. Sipser. Maximum matchings in sparse random graphs. In *22nd Annual Symposium on Foundations of Computer Science*, pages 364–375. IEEE Comput. Soc. Press, Los Alamitos, CA, 1981.

[26] L. M. Kirousis, E. Kranakis, D. Krizanc, and Y. Stamatiou. Approximating the unsatisfiability threshold of random formulas. *Random Structures Algorithms*, 12(3):253–269, 1998.

[27] T. G. Kurtz. Solutions of ordinary differential equations as limits of pure jump Markov processes. *J. Appl. Probability*, 7:49–58, 1970.

[28] T. G. Kurtz. *Approximation of population processes.* Society for Industrial and Applied Mathematics (SIAM), Philadelphia, Pa., 1981.

[29] A. W. Marshall and I. Olkin. *Inequalities: theory of majorization and its applications.* Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1979.

[30] R. Monasson and R. Zecchina. Entropy of the K-satisfiability problem. *Phys. Rev. Lett.*, 76(21):3881–3885, 1996.

[31] R. Monasson and R. Zecchina. Statistical mechanics of the random K-satisfiability model. *Phys. Rev. E (3)*, 56(2):1357–1370, 1997.

[32] R. Monasson and R. Zecchina. Tricritical points in random combinatorics: the $(2+p)$-SAT case. *J. Phys. A*, 1998. submitted.

[33] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, and L. Troyansky. Phase transition and search cost in the $(2+p)$-SAT problem. In *4th Workshop on Physics and Computation, (Boston, MA, 1996).*

[34] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, and L. Troyansky. Determining computational complexity from characteristic phase transitions. *Nature*, 400:133–137, 1999.

[35] N. Nedialkov. *Computing Rigorous Bounds on the Solution of an Initial Value Problem for an Ordinary Differential Equation.* Ph.D. Thesis, University of Toronto, 1999.

[36] D. Redfern. *The Maple Handbook: Maple V Release 3.* Springer Verlag, New York, third edition, 1994.

[37] B. Selman, D. G. Mitchell, and H. J. Levesque. Generating hard satisfiability problems. *Artificial Intelligence*, 81(1-2):17–29, 1996.

[38] N. C. Wormald. Differential equations for random processes and random graphs. *Ann. Appl. Probab.*, 5(4):1217–1235, 1995.