Electronic Colloquium on Computational Complexity, Report No. 176 (2013)

A Short Implicant of CNFs with Relatively Many Satisfying Assignments*

Daniel Kane
Department of Mathematics
Stanford University
Stanford CA 94305, USA
dankane@math.stanford.edu

Osamu Watanabe
Dept. of Math. and Comput. Sci.,
Tokyo Institute of Technology
Tokyo 152-8552, Japan
watanabe@is.titech.ac.jp

1 Introduction

We consider the following question:

> Consider any Boolean function $F(X_1, \ldots, X_N)$ that has relatively large number of satisfying assignments and that can be expressed by a CNF formula with relatively small (but superlinear) number of clauses. Then how many variables do we need to fix in order to satisfy F? In other words, what is the size of the shortest implicant of F?

To state our results precisely, we introduce some notation. Throughout this paper, let F be a given Boolean function over N variables, and we assume that it is given as a CNF formula with M clauses and that it has $P2^N$ satisfying assignments, where P will be referred as the *sat. assignment ratio* of F. Furthermore, we introduce two parameters[1] $\delta > 0$ and $\varepsilon > 0$, and consider the following situation: (i) $P \geq 2^{-N^\delta}$, and (ii) $M \leq N^{1+\varepsilon}$ For such a CNF formula F, we discuss the size of its implicant in terms of δ and ε. As our main result, we show that if $\delta + \varepsilon < 1$, then one can always find some "short" partial assignment on which F evaluates to 1 by fixing αN variables for some $\alpha > 0$; that is, F has an implicant of size $\leq \alpha N$. (In this paper, for any partial assignment, by its "size" we will mean the number of variables fixed by this assignment; we say that a partial assignment is *short* if it fixes at most αN variables for some constant $\alpha < 1$.)

If a function F has a short partial assignment, then it has many satisfying assignments. Our result shows that a certain converse relation holds provided that F is expressed as a CNF formula with a relatively small number of clauses. We believe that this structural property would be of some help for designing algorithms for CNF formulas. In fact, we derive, from our analysis, a deterministic algorithm that finds a short partial assignment in $\widetilde{O}(2^{N^\beta})$-time[2] for some $\beta < 1$ for

*This work was started from the discussion at the workshop on Computational Complexity at the Banff International Research Station for Mathematical Innovation and Discovery (BIRS), 2013. The first author is supported in part by an NSF postdoctoral research fellowship. The second author is supported in part by the ELC project (MEXT KAKENHI Grant No. 24106008).

[1]For simplicity, throughout this paper, we assume that these parameters are constants, and whenever necessary that N is sufficiently large w.r.t. these parameters.

[2]By $\widetilde{O}(t(N))$ we mean $O\left(t(N)(\log t(N))^{O(1)}\right)$.

ISSN 1433-8092

any CNF formula with $\delta + \varepsilon < 1$. (More precisely, we can show that $\beta \le 1 - \frac{(1-(\delta+\varepsilon))(1-\delta)}{4}$.) Clearly, this can be used as a subexponential-time algorithm for solving the CNF-SAT problem for any CNF formula with $\delta + \varepsilon < 1$.

Note that F needs to have many satisfying assignments so that F has a short implicant, which justifies a condition like (i) (with small δ). It seems that a condition like (ii) (with small ε) is also necessary. In particular, a DNF formula with a large number of terms can afford to have each term very long. To justify this intuition, we also show a lower bound for the above α in terms of δ and ε.

Hirsch [3] considered a similar problem for k-CNF formulas for any constant k. He considered k-CNF formulas with $P2^N$ assignments for any $P > 0$. It is shown that some deterministic algorithm finds, when such an F is given as an input, one of its satisfying assignments quite efficiently, for example, in linear-time when P can be regarded as a constant. As a corollary to this analysis, it is also proved that F always has a partial assignment of size $O(\log(1/P))$. Unfortunately, though, his argument does not seem to work for general CNF formulas (i.e., CNF formulas with no clause size restriction). In fact, Hirsch proved the existence of a general CNF formula that does not have a partial assignment of size $O(\sqrt{N})$ even though it has a large sat. assignment ratio, say, $P \ge 0.5$. It is then suggested that this difference between general CNF and k-CNF could be related to the difficulty of designing a subexponential-time algorithm for the CNF-SAT problem. We show here that even in the general case, if F satisfies our conditions (i) and (ii) with $\delta + \varepsilon < 1$, then it indeed has a somewhat short partial assignment, which can be found by some deterministic algorithm in subexponential-time.

For solving the general SAT problem, we have an obvious randomized algorithm that tries the satisfiability of an assignment chosen uniformly at random. Such an algorithm finds a satisfying assignment with probability $\ge 2^{-N^\delta}$ for any function with sat. assignment ratio $\ge 2^{-N^\delta}$. Then for the CNF-SAT problem, we may design a deterministic algorithm by applying some good pseudo random sequence generator (*prg* in short) against CNF formulas to this randomized algorithm. That is, an algorithm that tries to find a satisfying assignment among assignments generated by such a prg from all possible seeds. In order to ensure that this algorithm obtains some satisfying assignment for any CNF formula with sat. assignment ratio $\ge 2^{-N^\delta}$, we need to choose the seed length of the prg so that a generated pseudo random sequence (of length N) is $\gamma := O(2^{-N^\delta})$ close to the uniform distribution for any CNF formula (with, say, $N^{O(1)}$ clauses). For this application, the current best upper bound for the seed length is $\tilde{O}(\log(1/\gamma)^2)$ (ignoring minor factors for our discussion) due to the prg proposed by De et al. [2]. For this seed length, the running time of the simple deterministic algorithm becomes $\tilde{O}(2^{N^{2\delta}})$, which is subexponential if $\delta < 1/2$. This is incomparable with our algorithm's time bound $\widetilde{O}(2^{N^\beta})$ with $\beta = 1 - \frac{(1-(\delta+\varepsilon))(1-\delta)}{4}$. We should also mention that while the algorithm using prg is oblivious to the input, ours does not have this property.

2 Preliminaries

Throughout this paper, we will fix the usage of the following symbols: Let F be any Boolean function over N Boolean variables $X_1, \ldots, X_N$, where N is our main size parameter. We also use n to denote $\log_2 N$. We assume that F has $P2^N$ satisfying assignments where $P \ge 2^{-N^\delta}$, and that F is given as a CNF formula with $M \le N^{1+\varepsilon}$ clauses. In order to simply our discussion, we regard parameters δ and ε as constants; whenever necessary, we may assume that N is large enough for each choice of δ and ε. Symbols ρ and σ are used to denote partial assignments over $X_1, \ldots, X_N$. For any partial assignment ρ, by $\rho(X_i) = *$, for example, we mean that the partial assignment does not fix the value of X_i; let $F|\rho$ denote a function evaluated under partial assignment ρ. We use $\mathrm{Fix}(\rho)$ to denote the set of variables whose value is fixed by ρ.

In this paper, we use symbols α and β for some constants w.r.t. N, which are defined by some other technical parameters chosen for δ and ε. On the other hand, the symbol c is used to denote some constants independent from N, δ, and ε. In order to simplify our notation, we write, e.g, $O(N)$ or $\Omega(N)$ when constant factors are not essential. We simply write log for $\log_2$ and ln for $\log_{\mathrm{e}}$. Let$c_0 = \log_2 \mathrm{e}$. When necessary, we write e^x and 2^x as $\exp(x)$ and $\exp_2(x)$ respectively for showing the exponent clearly.

We recall some common approximations that will be used several places in this paper. Note that for any integer $k \geq 1$, we have

$$\left(1 - \frac{1}{k}\right)^k \;\leq\; \mathrm{e}^{-1} \;\leq\; \left(1 - \frac{1}{k+1}\right)^k.$$

Since we will consider very large k, we ignore the difference between k and $k+1$, and we will simply approximate $(1-1/k)^k$ by e^{-1}.

We introduce some notation and state our results formally.

Let $\mathrm{sat}(F)$ denote the set of satisfying assignments of F. Then the *satisfying assignment ratio* of F is defined by

$$\mathrm{sat.ratio}(F) \;=\; \frac{\|\mathrm{sat}(F)\|}{2^N}.$$

We generalize this notion for partial assignments. Consider any partial assignment ρ over $X_1, ..., X_N$, and for any set $U \subseteq \{0,1\}^N$, by $U|\rho$ we denote the set of assignments in U that are consistent with ρ. For example, $\mathrm{sat}(F)|\rho$ is the set of satisfying assignments of F consistent with ρ, which is nothing but $\mathrm{sat}(F|\rho)$. Then the *satisfying assignment ratio* of F w.r.t. ρ (denoted as $\mathrm{sat.ratio}(F,\rho)$) is defined by

$$\mathrm{sat.ratio}(F,\rho) \;=\; \frac{\|\mathrm{sat}(F)|\rho\|}{\|\{0,1\}^N|\rho\|}.$$

Theorem 1. *For any $\delta, \varepsilon > 0$ such that $\delta + \varepsilon < 1$, let F be any CNF formula such that (i) its sat. assignment ratio P satisfies $P \geq \exp_2(-N^\delta)$, and (ii) it consists of $M \leq N^{1+\varepsilon}$ clauses. Then it has some partial assignment $\widehat{\rho}$ satisfying*

$$F|\widehat{\rho} = 1 \quad \text{and} \quad \|\mathrm{Fix}(\widehat{\rho})\| \leq \alpha N, \tag{1}$$

where α is defined by

$$\alpha \;=\; 1 - \frac{1-(\delta+\varepsilon)}{c} \tag{2}$$

with some constant $c \geq 1$.

We also have an algorithmic version of Theorem 1. In particular, this algorithm can be used to solve certain CNF-SAT instances.

Theorem 2. *There exists a deterministic algorithm such that for any parameters δ and ε, and for any CNF formula F satisfying (i) and (ii) of Theorem 1 w.r.t. δ and ε, it runs in $\widetilde{O}(2^{N^\beta})$-time for some $\beta < 1$ and yields some partial assignment $\widehat{\rho}$ satisfying*

$$F|\widehat{\rho} = 1 \quad \text{and} \quad \|\mathrm{Fix}(\widehat{\rho})\| \leq \alpha N,$$

where α *is defined by*

$$\alpha \;=\; \max\left(1 - \frac{1-(\delta+\varepsilon)}{c_1},\, 1 - c_2^{1/(1-\delta)}\right)$$

with some constants $c_1 \geq 1$ *and* $c_2 < 1$.

Remark. *We can show that the above time bound holds for any* β *such that* $\beta \leq 1 - \frac{1-(\delta+\varepsilon)(1-\delta)}{2(2-\delta)}$. *This bound for* β *can be further reduced to* $1 - \frac{1-(\delta+\varepsilon)}{c_3}$ *for some constant* c_3 *for a simpler task of finding a satisfying assignment*

We also give the following lower bound result.

Theorem 3. *For any parameters* δ *and* ε, $0 < \delta < 1$ *and* $0 < \varepsilon$, *consider* α *satisfying*

$$\alpha \;<\; \frac{\varepsilon}{1+\varepsilon-\delta}. \tag{3}$$

Then we have some Boolean function F *such that (i)* F *has sat. assignment ratio* $\geq \exp_2(-N^\delta)$, *(ii)* F *has a CNF formula with at most* $N^{1+\varepsilon}$ *clauses, and (iii) it has no partial assignment* ρ *such that*

$$F|\rho = 1 \quad \text{and} \quad \|\mathrm{Fix}(\rho)\| \leq \alpha N.$$

3 Upper bound proof

In this section we give a proof of Theorem 1, showing an upper bound on the size of "short" partial assignments. Throughout this section, for any $\delta, \varepsilon > 0$ such that $\delta + \varepsilon < 1$ holds, we consider sufficiently large N and fix any F satisfying (i) and (ii) of the theorem w.r.t. δ and ε.

For our analysis, we make use of the following version of Lovász Local Lemma.

Lemma 1. *Let* $\mathcal{E}$ *be a family of events, and for any* $E \in \mathcal{E}$, *let* $\Gamma(E)$ *be the set of events of* $\mathcal{E}$ *that may* not *be independent from* E*; in other words,* $\mathcal{E} - \Gamma(E)$ *is the set of events independent from* E. *For each* $E \in \mathcal{E}$, *define* $x(E) \in (0,1)$ *so that*

$$\Pr[\,E\,] \;\leq\; x(E) \prod_{E' \in \Gamma(E)} (1 - x(E')). \tag{4}$$

Then we have

$$\Pr\left[\bigwedge_{E\in\mathcal{E}} \overline{E}\right] \;\geq\; \prod_{E\in\mathcal{E}} (1 - x(E)), \tag{5}$$

where $\overline{E}$ *is the event that* E *does not hold.*

In the following, we will refer the above mapping x as an *LLL mapping.*

Let us first see our proof outline. The goal is to define some partial assignment $\widehat{\rho}$ satisfying the theorem. For this, we first define a sequence of partial assignments $\sigma_1, \sigma_2, \ldots, \sigma_T$; then with one more partial assignment ρ_0, we define $\widehat{\rho}$ by $\rho_0 \circ \sigma_T \circ \cdots \circ \sigma_1$. We will use Local Lovász Lemma for analyzing ρ_0; the sequence $\sigma_1, \sigma_2, \ldots, \sigma_T$ is used to have $F|(\sigma_T \circ \cdots \circ \sigma_1)$ satisfy conditions needed for the lemma. Intuitively, by each partial assignment σ_t, we would like to eliminate either a "short clause" or a "popular literal"; for eliminating a short clause C, we define σ_t to assign *some* values to the all variables appearing in C, and for eliminating a popular literal, we define σ_t to assign *some* value to the literal. By choosing appropriate values for each σ_t, we can guarantee that this process is terminated by assigning values to at most sublinear number of variables.

In our analysis, we will introduce some parameters. Parameters a_1, a_2, a_3, b_1 in $(0,1)$ are chosen appropriately and regarded as constants w.r.t. N. Intuitively, a_1, a_2, and a_3 are chosen close to 0, while b_1 is chosen close to 1.

We begin our precise argument by introducing ℓ defined by

$$\ell \;=\; b_1 \log\left(\frac{N}{-\log P}\right).$$

Here $b_1 \in [0,1)$ is a constant close to 1, whose value will be defined later. Then from our assumptions on N and P, we have

$$2^\ell \;=\; \left(\frac{N}{-\log P}\right)^{b_1} \;=\; \exp_2\bigl(b_1(1-\delta)n\bigr).$$

The *size* of C (denoted as $|C|$) is simply the number of literals in the clause. We say that a clause C is *short* if C contains at most ℓ literals, that is, $|C| \le \ell$. We say that a literal is *popular* if it appears in $L := N^{(1-a_1)(1-\delta)}$ $(= \exp_2\bigl((1-a_1)(1-\delta)n\bigr))$ clauses, where $a_1 > 0$ is some constant close to 0, whose value will be determined later.

We present our procedure for picking σ_t below in Figure 1. We iterate this procedure until the stopping condition $(*)$ holds. We show that the number of iterations is bounded by $O(N^{\beta_1})$ for some $\beta_1 < 1$. Since at most $O(\log N)$ variables are assigned by each σ_t, the number of variables fixed by $\overline{\sigma}_T := \sigma_T \circ \cdots \circ \sigma_1$ is $N^{\beta_1 + o(1)}$. Note that it may be possible that $(*)$ holds with empty F_t, that is, with all clauses being removed. This means that $\sigma_t \circ \cdots \circ \sigma_1$ satisfies F, and in this case, we use $\sigma_t \circ \cdots \circ \sigma_1$ as $\widehat{\rho}$, which clearly satisfies the theorem.

procedure for σ_t (where $t \ge 1$)
// assume that $\sigma_1, \ldots, \sigma_{t-1}$ have been defined, and
// let $\overline{\sigma}_{t-1}$ and F_{t-1} denote respectively $\sigma_{t-1} \circ \cdots \circ \sigma_1$ and $F|\overline{\sigma}_{t-1}$.
  if (F_{t-1} has no popular variable) and (F_{t-1} has no short clause) — $(*)$
    then stop and output the obtained sequence as $\sigma_1, \ldots, \sigma_T$;
  Case I: (if F_{t-1} has a short clause)
    $C =$ (any) one of the short clauses;
    $\sigma_t =$ a satisfying assignment σ of C maximizing sat.ratio(F_{t-1}, σ);
    // $\sigma_t(X) = *$ for all variables X not in C;
  Case II: (if F_{t-1} has no short clause and F_{t-1} has a popular literal)
    $Y_i =$ (any) one of the popular literal (either X_i or $\overline{X_i}$) in F_{t-1};
    if sat.ratio$(F_{t-1}, (Y_i := 0)) \ge (1 + 2^{-\ell-2}) \cdot$ sat.ratio(F_{t-1})
      then $\sigma_t = (Y_i := 0)$; **else** $\sigma_t = (Y_i := 1)$;

Figure 1: Procedure for defining σ_t

Before stating our formal analysis, let us give some intuitive reasoning for our choice of ℓ and L and why $(*)$ holds within sublinear number of iterations.

We first argue that Case I does not occur many times. For this, we consider the sat. assignment ratio sat.ratio$(F, \overline{\sigma})$ of F w.r.t. a so-far-defined partial assignment $\overline{\sigma}$. Let C be a short clause that is chosen at Case I of some tth iteration. Note that out of all possible $2^{|C|}$ assignments of C,

$2^{|C|}-1$ of them satisfy C. Then by defining σ_t to be one of such assignments satisfying C, the sat. assignment ratio $\mathrm{sat.ratio}(F, \sigma_t \circ \overline{\sigma})$ is increased from $\mathrm{sat.ratio}(F, \overline{\sigma})$ by a factor of $2^{|C|}/(2^{|C|}-1) \ge 2^{\ell}/(2^{\ell}-1)$ $(= (1-2^{-\ell})^{-1})$. Since the sat. assignment ratio is initially $P \ge \exp_2(-\delta n)$ and it is at most 1, we can bound the number of iterations where Case I occurs. As we will see below it is bounded by $N^{b_1+(1-b_1)\delta}$ from our choice of ℓ, and this bound is sublinear if $b_1 < 1$.

Next consider Case II. Let Y_i be one of the popular literals chosen at Case II of some tth iteration. Since it appears in L clauses in the current F_{t-1}, by a partial assignment "$Y_i := 1$" we can satisfy at least L clauses of F_{t-1} (and hence remove them from F_{t-1}). Clearly this does not occur more than M/L times, where $M/L = N^{(1+\varepsilon)-(1-a_1)(1-\delta)} = N^{(1-a_1)\delta+\varepsilon}$, which is sublinear if $a_1 > 0$. Here we need to be a bit careful. There may be many satisfying assignments that assigns 0 to Y_i, and we may lose many satisfying assignments by using the positive assignment "$Y_i := 1$" for the tth partial assignment σ_t. In order to avoid this situation, we first check whether the negative assignment "$Y_i := 0$" improves the sat. assignment ratio similar to Case I and use this assignment for σ_t if such a situation occurs (and use the positive assignment for σ_t if otherwise). Following the same argument as Case I, we can give a similar upper bound for the number of situations where negative assignments are used.

Now we state this idea formally.

Lemma 2. *The number T of iterations of the above procedure needed until $(*)$ holds for F_T is bounded by $O(N^{\beta_1})$ where $\beta_1 = \max\bigl(b_1 + (1-b_1)\delta, a_1 + (1-a_1)\delta + \varepsilon\bigr)$, which is less than 1 by choosing $a_1 > 0$ sufficiently small and $b_1 < 1$ (since we assume that $\delta + \varepsilon < 1$).*

Proof. In order to measure the progress made by each iteration, we introduce the following potential function for a given partial assignment $\overline{\sigma}$ of F. Below by $|F'|$ we denote the number of clauses in F'.

$$\Phi(\overline{\sigma}) \;=\; 2^{\ell} \log\left(\mathrm{sat.ratio}(F, \overline{\sigma})^{-1}\right) + \bigl|(F|\overline{\sigma})\bigr| \cdot L^{-1}.$$

Clearly, Φ must be nonnegative for any partial assignment. We show that each σ_t decreases Φ by constant whereas its initial value is $2N^{\beta_1}$, thereby proving our upper bound for T.

First estimate the initial potential, that is, $\Phi(\overline{\sigma}_0)$ for the null partial assignment $\overline{\sigma}_0$. Noting that $\mathrm{sat.ratio}(F, \overline{\sigma}_0) = P$ and $\bigl|(F|\overline{\sigma}_0)\bigr|$ $(= |F|) = M$, we have

$$\begin{aligned}\Phi(\overline{\sigma}_0) \;&=\; 2^{\ell}\,(-\log P) + M \cdot L^{-1} \;=\; N^{b_1}\,(-\log P)^{1-b_1} + N^{1+\varepsilon} N^{-(1-a_1)(1-\delta)} \\ &=\; N^{b_1} N^{(1-b_1)\delta} + N^{1+\varepsilon-(1-a_1)(1-\delta)} \;=\; N^{b_1+(1-b_1)\delta} + N^{a_1+(1-a_1)\delta+\varepsilon}.\end{aligned}$$

This is bounded by $2N^{\beta_1}$ with

$$\beta_1 \;=\; \max\bigl(\, b_1 + (1-b_1)\delta, a_1 + (1-a_1)\delta + \varepsilon \,\bigr) \;<\; 1. \tag{6}$$

Later (at the end of our analysis for the theorem) we will choose $a_1 > 0$ sufficiently small and $b_1 < 1$ so that the above bound for β_1 holds, which is possible since we assume that $\delta + \varepsilon < 1$.

Consider first Case I of the above procedure for defining σ_t and analyze the difference between $\Phi(\overline{\sigma}_t)$ and $\Phi(\overline{\sigma}_{t-1})$. Let C be the short clause satisfied by σ_t. We first estimate the sum of $\mathrm{sat.ratio}(F, \sigma \circ \overline{\sigma}_{t-1})$ over all satisfying assignments σ of C, which we write by $\Sigma_{\sigma:\mathrm{sat}.C}\, \mathrm{sat.ratio}(F, \sigma \circ \overline{\sigma}_{t-1})$. From the definition of the satisfying assignment ratio, we have

$$\Sigma_{\sigma:\mathrm{sat}.C}\ \mathrm{sat.ratio}(F, \sigma \circ \overline{\sigma}_{t-1}) \;=\; \frac{\Sigma_{\sigma:\mathrm{sat}.C}\ \|\mathrm{sat}(F|\overline{\sigma}_{t-1} \circ \sigma)\|}{\|\{0,1\}^N|\overline{\sigma}_{t-1} \circ \sigma\|}.$$

Note here that

$$\Sigma_{\sigma:\text{sat}.C}\ \|\text{sat}(F|\overline{\sigma}_{t-1}\circ\sigma)\| \ = \ \|\text{sat}(F|\overline{\sigma}_{t-1})\|,$$

and

$$\|\{0,1\}^N|\overline{\sigma}_{t-1}\circ\sigma\| \ = \ \Sigma_{\sigma:\text{sat}.C}\ 2^{-|C|}\|\{0,1\}^N|\overline{\sigma}_{t-1}\|.$$

Hence, we have

$$\begin{aligned}\Sigma_{\sigma:\text{sat}.C}\ \text{sat.ratio}(F,\sigma\circ\overline{\sigma}_{t-1}) \ &= \ \frac{\|\text{sat}(F|\overline{\sigma}_{t-1})\|}{\Sigma_{\sigma:\text{sat}.C}\ 2^{-|C|}\|\{0,1\}^N|\overline{\sigma}_{t-1}\|}\\ &= \ 2^{|C|}\Sigma_{\sigma:\text{sat}.C}\ \frac{\|\text{sat}(F|\overline{\sigma}_{t-1})\|}{\|\{0,1\}^N|\overline{\sigma}_{t-1}\|} \ = \ 2^{|C|}\Sigma_{\sigma:\text{sat}.C}\ \text{sat.ratio}(F,\overline{\sigma}_{t-1}).\end{aligned}$$

Note that there are $2^{|C|}-1$ satisfying assignments for C. Thus, the above estimation shows that $\text{sat.ratio}(F,\sigma\circ\overline{\sigma}_{t-1})$ on average is $2^{|C|}/(2^{|C|}-1)\times\text{sat.ratio}(F,\overline{\sigma}_{t-1})$. Since we choose for σ_t an assignment maximizing the ratio, we have

$$\text{sat.ratio}(F,\sigma_t\circ\overline{\sigma}_{t-1}) \ \geq \ \frac{2^{|C|}}{2^{|C|}-1}\cdot\text{sat.ratio}(F,\overline{\sigma}_{t-1}) \ \geq \ \frac{1}{1-2^{-\ell}}\cdot\text{sat.ratio}(F,\overline{\sigma}_{t-1}),$$

since $|C|\leq\ell$ because C is a short clause.

Then $2^\ell\log(\text{sat.ratio}(F,\overline{\sigma}_{t-1})^{-1})$, the first term of $\Phi(\overline{\sigma}_{t-1})$, gets decreased at least by $\log_2 \mathrm{e}>1$ because

$$\begin{aligned}2^\ell\log\left(\text{sat.ratio}(F,\sigma_t\circ\overline{\sigma}_{t-1})^{-1}\right) \ &\leq \ 2^\ell\log\left(\left(1-2^{-\ell}\right)\text{sat.ratio}(F,\overline{\sigma}_{t-1})^{-1}\right)\\ &= \ \log\left(1-2^{-\ell}\right)^{2^\ell}+2^\ell\log\left(\text{sat.ratio}(F,\overline{\sigma}_{t-1})^{-1}\right).\end{aligned}$$

Thus, we have $\Phi(\sigma_t\circ\overline{\sigma}_{t-1})\leq\Phi(\overline{\sigma}_{t-1})-1$.

Consider next Case II. In this case, we want to assign Y_i positively (i.e., to use the assignment $Y_i:=1$) to satisfy at least L clauses. But in order to avoid the situation where too many satisfying assignments are lost by this assignment, we first check whether the satisfying assignment ratio gets increased by assigning Y_i negatively. If the ratio is increased by a factor of $(1+2^{-\ell-2})$, then we simply use this negative assignment for σ_t, by which the Φ value gets decreased by at least $1/4$, since

$$2^\ell\log\left(1+\frac{1}{2^{\ell+2}}\right) \ \approx \ \frac{1}{4}\log\mathrm{e} \ \geq \ \frac{1}{4}.$$

Otherwise, the ratio would not get decreased more than $(1-2^{-\ell-2})$ times by assigning Y_i positively, which means that the increment of the first term of the Φ value is at most $(\log\mathrm{e})/4<1$. On the other hand, by assigning Y_i positively, we can satisfy (and hence eliminate) at least L clauses from F_{t-1}, by which the Φ value is decreased by at least 1. Thus, we have $\Phi(\sigma_t\circ\overline{\sigma}_{t-1})\leq\Phi(\overline{\sigma}_{t-1})-\Omega(1)$, and from this the lemma is proved. □

Now we may assume that some partial assignment $\overline{\sigma}$ is chosen such that (i) it assigns at most $N^{\beta_1+o(1)}$ variables for some $\beta_1<1$, and (ii) $F|\overline{\sigma}$ has no popular variable nor short clause. We may also assume that the value of $F|\overline{\sigma}$ is not yet fixed and there are some clauses remained in $F|\overline{\sigma}$. For this $F|\overline{\sigma}$, we define our last partial assignment ρ_0 via Lovász Local Lemma.

Let a_2 be a parameter in $(0,1)$ that is sufficiently small; again a_2 will be determined at the end of our analysis. For defining our ρ_0, we consider a standard random partial assignment ρ that is defined by

$$\rho(X_i) \;=\; \begin{cases} 0, & \text{with prob. } (1-a_2)/2, \\ 1, & \text{with prob. } (1-a_2)/2, \text{ and} \\ *, & \text{with prob. } a_2 \end{cases}$$

for each $X_i \notin \mathrm{Fix}(\overline{\sigma})$. We would like to find some ρ that still keeps $\Omega(N)$ variables unassigned and yet $F|\rho \circ \overline{\sigma} = 1$. If such ρ exists, then we use it for ρ_0 and define $\widehat{\rho} = \rho_0 \circ \overline{\sigma}$.

It is easy to see that ρ assigns $*$ to approximately $a_2 N'$ variables with high probability, where N' is the number of variables of $F|\overline{\sigma}$. Recall that $N' \geq N - N^{\beta_1 + o(1)}$; then the following claim holds.

Claim 1. *With probability $1 - 2^{-\Omega(N)}$, the random partial assignment ρ assigns $*$ to more than $(a_2/2)N$ variables.*

Thus, we set $\alpha = 1 - a_2/2$; then the theorem follows from the following lemma, which shows that with some positive probability there exists ρ with $F|\rho\circ\overline{\sigma} = 1$ among those satisfying the above claim. We can simply use one of them for ρ_0 to define our target $\widehat{\rho} = \rho_0 \circ \overline{\sigma}$. (The bound (2) for α will be given after the proof of the lemma by determining our technical parameters.)

Lemma 3. *For some $\beta_2 > 0$, we have*

$$\Pr_{\rho}\left[\, F|\rho \circ \overline{\sigma} = 1 \,\right] \;\geq\; \exp\left(-2^{(1-\beta_2)n}\right) \;=\; \exp\left(-N^{(1-\beta_2)}\right).$$

Proof. Let $\mathcal{C}$ be the set of clauses of $F|\overline{\sigma}$. For each clause $C \in \mathcal{C}$, let E_C be the event that ρ does not satisfy C, i.e., $C|\rho \neq 1$. Then $\Pr[\, \wedge_{C\in\mathcal{C}} \overline{E_C} \,]$ is the probability that $F|\widehat{\rho} = 1$, i.e., the probability that we would like to bound.

Here we use Lovász Local Lemma to estimate this probability. In the following analysis, we introduce symbols u, v, w to simplify expressions and also for later reference. First we define an LLL mapping x for Lovász Local Lemma. In order to define $x(E_C)$ for each $C \in \mathcal{C}$ appropriately, we note that

$$\begin{aligned} \Pr[\, E_C \,] \;&=\; \left(\frac{1+a_2}{2}\right)^{|C|} \;=\; 2^{-|C|} \cdot (1+a_2)^{a_2^{-1} \cdot p|C|} \\ &\approx\; 2^{-|C|} \cdot \mathrm{e}^{-a_2|C|} \;=\; 2^{-|C|(1-c_0 a_2)} \;=\; 2^{-u|C|}, \end{aligned} \tag{7}$$

where $c_0 = \log \mathrm{e}$ and $u = 1 - c_0 a_2$. We then introduce a parameter $a_3 > 0$ and define $x(E_C)$ for each $C \in \mathcal{C}$ by

$$x(E_C) \;=\; 2^{-u|C|} \cdot 2^{a_3 u|C|} \;=\; 2^{-(1-a_3)u|C|} \;=\; 2^{-v|C|},$$

where we let $v = (1-a_3)u \in (0,1)$.

We show that the condition (4) of Lovász Local Lemma is satisfied. First note that $E_{C'} \in \Gamma(E_C)$ if and only if C' shares some variable with C; thus,

$$\|\Gamma(E_C)\| \;\leq\; L \cdot |C| \;=\; 2^{(1-a_1)(1-\delta)n}|C|$$

because there is no popular variable. Thus, we have

$$\begin{aligned}
\prod_{E_{C'}\in\Gamma(E_C)} (1 - x(E_{C'})) &= \prod_{E_{C'}\in\Gamma(E_C)} \left(1 - 2^{-v|C'|}\right) \;\geq\; \prod_{E_{C'}\in\Gamma(E_C)} \left(1 - 2^{-v\ell}\right) \\
&\geq \left(1 - 2^{-v\ell}\right)^{\|\Gamma(E_C)\|} \;\geq\; \left(1 - 2^{-v\ell}\right)^{2^{v\ell}\left(2^{-v\ell}\cdot L\cdot|C|\right)} \\
&\approx \exp\left(-2^{-v\ell}\cdot L\cdot|C|\right) \;=\; \exp\left(-2^{-v\ell}\cdot 2^{(1-a_1)(1-\delta)n}\cdot|C|\right) \\
&= \exp\left(-2^{\left(-vb_1(1-\delta)n+(1-a_1)(1-\delta)n\right)}\cdot|C|\right) \\
&= \exp\left(-2^{\left((1-a_1)-vb_1\right)(1-\delta)n}\cdot|C|\right) \;=\; \exp_2\left(-c_0 2^{w(1-\delta)n}\cdot|C|\right),
\end{aligned}$$

where $w = (1-a_1) - vb_1$. Hence, we have

$$x(E_C)\prod_{E_{C'}\in\Gamma(E_C)} (1 - x(E_{C'})) \;\geq\; \exp_2\bigl(-u|C| + (a_3 - c_0 2^{w(1-\delta)n}/u)u|C|\bigr). \tag{8}$$

Now for condition (4), we will define our parameters so that

$$w \;=\; (1-a_1) - vb_1 \;=\; (1-a_1) - (1-a_3)(1-c_0a_2)b_1 \;<\; 0 \tag{9}$$

holds; then then we have

$$c_0 2^{w(1-\delta)n}/y \;<\; a_3$$

for sufficiently large n, and this implies (7) < (8); that is, (4) holds for our mapping.

Then by Lovász Local Lemma (5) we have

$$\begin{aligned}
\Pr\left[\bigwedge_{C\in\mathcal{C}} \overline{E_C}\right] &\geq \prod_{C\in\mathcal{C}}(1 - x(E_C)) \;=\; \prod_{C\in\mathcal{C}}(1 - 2^{-v|C|}) \\
&= \left(1 - 2^{-v\ell}\right)^M \;=\; \left(1 - 2^{-v\ell}\right)^{2^{v\ell}\cdot M\cdot 2^{-v\ell}} \\
&\approx \exp\left(-M\cdot 2^{-v\ell}\right) \;=\; \exp\left(-2^{(1+\varepsilon)n}\cdot 2^{-v\ell}\right) \\
&= \exp\left(-2^{(1+\varepsilon)n}\cdot 2^{-vb_1(1-\delta)n}\right) \;=\; \exp\left(-2^{\left(1-(vb_1-(vb_1\delta+\varepsilon))\right)n}\right) \\
&> \exp\left(-2^{\left(1-(vb_1-(\delta+\varepsilon))\right)n}\right).
\end{aligned}$$

By our choice of parameters (explained later), we may assume that

$$vb_1 - (\delta+\varepsilon) \;>\; 0. \tag{10}$$

Thus, the lemma holds with $\beta_2 = vb_1 - (\delta+\varepsilon) > 0$. □

To conclude our proof, we determine our technical parameters a_1, a_2, a_3, and b_1. Recall that these values are chosen to satisfy the following inequalities: (6), (9), and (10). Let $\Delta = 1 - (\delta+\varepsilon)$, which is positive by our assumption. Let d be any positive number such that $2d << 1-\delta$; for simplicity, we let $d=(1-\delta)/4$. Define a by

$$a \;=\; \frac{(1+2d)\Delta}{2-\delta} \;\;\bigl(<\;\Delta\bigr).$$

Then we define a_1, a_2, a_3, and b_1 as follows:

$$a_1 \;=\; a, \quad a_2 \;=\; \frac{d\Delta}{c_0(\varepsilon+a)}, \quad a_3 \;=\; \frac{d\Delta}{2-\delta}, \quad \text{and} \quad b_1 \;=\; \frac{\varepsilon+a}{1-\delta}.$$

We show that with these parameters, inequalities (6), (9), and (10) are satisfied. First consider (6). Note that $b_1+(1-b_1)\delta = \delta + b_1(1-\delta) = \delta+\varepsilon+a$, and that $a_1+(1-a_1)\delta+\varepsilon \le \delta+\varepsilon+a$. Thus, we have

$$\beta_1 \;=\; \max\bigl(\, b_1+(1-b_1)\delta, a_1+(1-a_1)\delta+\varepsilon \,\bigr) \;=\; \delta+\varepsilon+a.$$

On the other hand, we have

$$\delta+\varepsilon+a \;=\; 1-\frac{(1-(\delta+\varepsilon))(1-\delta-2d)}{2-\delta} \;=\; 1-\frac{(1-(\delta+\varepsilon))(1-\delta)}{2(2-\delta)} \;<\; 1, \qquad (11)$$

and (6) is proved.

In order to show (9), we compare $(1-a_1)/(b_1(1-a_3))$ and $1-c_0a_2$. By using $a_3<a_1$, we have

$$\frac{1-a_1}{b_1(1-a_3)} \;=\; \frac{1-a_1}{b_1}\left(1+\frac{a_3}{1-a_3}\right) \;<\; \frac{1-a_1+a_3}{b_1}.$$

Then (9), that is, $(1-a_1)/(b_1(1-a_3)) < 1-c_0a_2$ follows from $(1-a_1+a_3)/b_1 < 1-c_0a_2$, which is shown by substituting our defined values to these parameters. Also (10) is immediate from (9) because we have $vb_1 > 1-a_1 > 1-\Delta = \delta+\varepsilon$.

Finally, we show the bound (2) for α. Recall that we defined $\alpha = 1-a_2/2$. Then (2) with $c=8c_0$ follows from

$$a_2 \;=\; \frac{d\Delta}{c_0(\varepsilon+a)} \;=\; \frac{(1-\delta)(\delta+\varepsilon)}{4c_0(\varepsilon+a)} \;=\; \frac{(\varepsilon+\Delta)(\delta+\varepsilon)}{4c_0(\varepsilon+a)} \;\le\; \frac{\delta+\varepsilon}{4c_0}.$$

4 Algorithmic version

In this section we give a proof of Theorem 2, showing an algorithmic way to define a short partial assignment.

The key tool is to use an algorithmic version of Lovász Local Lemma, which has been improved greatly [4, 5, 1]. Our idea is simple. We show some subexponential-time deterministic algorithm that reduces our task to the CNF-SAT problem and use an algorithmic version of Lovász Local Lemma. Here we use the version[3] reported in [1].

We specify our target problem and state their lemma in a slightly simpler way. Note that in the algorithmic version of Lovász Local Lemma one should consider all CNF formulas (more precisely,

[3]In their paper, as a typical application of the lemma, an efficient deterministic algorithm is shown for k-CNF formulas with no variable appearing in many clauses. This may be used in our situation; but here we go back to the original lemma to confirm that our parameter choice works.

all CNF formulas satisfying certain conditions) instead of considering some single CNF formula as we did in the previous section. For any N', let $\mathcal{F}_{N'}$ be the set of CNF formulas F' over N' Boolean variables with at most $(N')^2$ clauses. Let $\mathcal{F} = \cup_{N'} \mathcal{F}_{N'}$. We use a mapping x considered in Lemma 1, which can be defined for each formula. Consider any $F' \in \mathcal{F}$. Let $\mathcal{C}$ denote the set of its clauses. Consider a random assignment to its N' variables, and for each $C \in \mathcal{C}$, let E_C denote an event that C becomes false by the assignment. Our goal (and the task of our algorithm) is to find an assignment avoiding E_C for all $C \in \mathcal{C}$, that is, to find a satisfying assignment for a given $F' in \mathcal{F}$. Let $\Gamma(E_C)$ be the set of events $E_{C'}$ such that C' shares some variable with C. In the lemma we consider an LLL mapping x (for this F'); by using this x, we also define $x'(E_C)$ by

$$x'(E_C) \; = \; x(E_C) \prod_{E_{C'} \in \Gamma(E_C)} (1 - x(E_{C'})).$$

Now we state the following algorithmic version of Lovász Local Lemma [1].

Lemma 4. *For any $\epsilon > 0$ and $d_2 > 0$, there exists a deterministic algorithm that, for any given $F' \in \mathcal{F}_{N'}$, runs in time $(N')^{cd_1 d_2 (1/\epsilon)}$ and yields some satisfying assignment of F' if we can define some mapping x for F' that satisfies*

$$\Pr[\, E_C \,] \; \le \; x'(E_C)^{1+\epsilon}, \quad x(E_C) \; < \; 1/2, \quad \text{and} \quad x'(E_C) \; \ge \; N^{-d_2} \tag{12}$$

for all $C \in \mathcal{C}$.

We propose our deterministic algorithm and show that it indeed satisfies the requirement of the theorem. Below we explain the execution of the algorithm on any given CNF formula F satisfying the condition of the theorem. We use the same set of parameters with almost the same values as previous section; these values will be justified at the end of this section. Our deterministic algorithm starts with executing the procedure of Figure 1 for sufficient number of times for obtaining a partial assignment $\overline{\sigma}$. Note that the procedure is executed deterministically in a brute force way. That is, instead of choosing each σ_t appropriately, we try all possibilities and consider all possible $\overline{\sigma}$'s that can be obtained by iterating the procedure for at most $2N^{\beta_1}$ times, where $2N^{\beta_1}$ is the bound given in the proof of Lemma 2. Then as Lemma 2 guarantees that there should be some $\overline{\sigma}$ that satisfies the target condition $(*)$ of Figure 1; that is, $F|\overline{\sigma}$ has no short clause nor popular variable. Since we can easily check this condition, choose any such $\overline{\sigma}$. It is easy to check that the time needed to compute this part is bounded by

$$\left(\max\left\{ 2^{\ell}, 2 \right\} + N^{O(1)} \right)^{O(N^{\beta_1})} \; \le \; \exp_2\left((cb_1(1-\delta)\log N) \cdot N^{\beta_1} \right) \; \le \; \widetilde{O}\left(2^{N^{\beta_1}} \right).$$

For this $F|\overline{\sigma}$, we consider a random assignment ρ' that is similar to ρ used in the previous section. With a parameter a_2, this ρ' assigns $*$ independently to each variable with probability a_2 (and leave it unassigned otherwise). Since every clause of $F|\overline{\sigma}$ has at least ℓ literals (where $\log \ell = b_1(1-\delta)\log N$), we have the following claim by Chernoff bound and the union bound. (The proof will be stated later.)

Claim 2. *With probability $1 - N^{-\Omega(1)}$, the random partial assignment ρ' satisfies the following $(**)$: it assigns $*$ to more than $(a_2/2)N$ variables and it assigns $*$ to at most $|C|/2$ variables at each clause C of $F|\overline{\sigma}$.*

We deterministically obtain for ρ' one of such partial assignments satisfying (**). This is possible in polynomial-time in N by the standard method of using conditional probabilities. For the obtained ρ', we remove all variables from $F|\overline{\sigma}$ that are assigned $*$ by ρ'. Note that even after this each clause has at least $\ell' := \ell/2$ literals. Then we define F' by keeping only the first ℓ' literals for each clause (where we may use any order of literals in each clause). The crucial points are: (a) any satisfying assignment of F' is extended naturally (by using $\overline{\sigma}$ and ρ') to a partial assignment $\widehat{\rho}$ for F satisfying the condition of the theorem, and (b) all clauses of F' is of size ℓ' and F' has no popular variables. By using (b) we show below that Lemma 4 can be used to show some polynomial-time deterministic algorithm for finding a satisfying assignment for F'; then by (a) we use this satisfying assignment to define a partial assignment satisfying the theorem. This is the execution of our deterministic algorithm. It is easy to see that the total running time of this algorithm is bounded by $\widetilde{O}(2^{N^{\beta_1}})$.

Below after stating a technical lemma and the proof of Claim 2, we conclude our proof by justifying the choice of our technical parameter values.

Lemma 5. *For the above F', we can define an LLL mapping satisfying the condition (12) of Lemma 4.*

Proof. We use the analysis given in the proof of Lemma 3. Consider the first condition of (12). Note that

$$\Pr\big[\,E_C\,\big] \;=\; 2^{-|C|},$$

and hence (7) holds with $u = 1$. This is only the difference, and the other part of the analysis works as before. Thus, from (8) we have

$$x'(E_C) \;\geq\; \exp_2\big(-|C| + (a_3 - c_0 2^{w(1-\delta)n})|C|\,\big),$$

where we may assume that $a_3 - c_0 2^{w(1-\delta)n} \geq \epsilon$ for some constant $\epsilon > 0$ for any sufficiently large n ($= \log N$). Therefore, the first condition of (12) is satisfied because

$$\Pr\big[\,E_C\,\big] \;=\; 2^{-|C|} \;<\; 2^{-(1+\epsilon)(1-\epsilon)|C|} \;=\; \Big(2^{-|C|+\epsilon|C|}\Big)^{1+\epsilon} \;\leq\; x'(E_C)^{1+\epsilon}.$$

For the second and the third conditions (12), we note that $|C| = \ell' = \ell/2 = b_1(1-\delta)n/2$ holds for all clauses C. Then it is easy to see that the second condition holds and the third one holds with $d_2 = 1$. □

Proof of Claim 2. The first condition of (**) was analyzed by Claim 1; thus, we consider here only the second condition.

Consider any clause C of $F|\overline{\sigma}$, and let Z be the number of literals that gets $*$ by our random partial assignment. Then its expectation μ is $a_2|C|$, which is much smaller than $|C|/2$. Thus, by Chernoff bound, we can bound the probability that Z exceeds $|C|/2$ by

$$\begin{aligned}
\Pr\left[\,Z > \frac{|C|}{2}\,\right] &= \Pr\big[\,Z > (1+\eta)a_2|C|\,\big] \;=\; \Pr\big[\,Z > (1+\eta)\mu\,\big] \\
&\leq \left(\frac{\mathrm{e}}{(1+\eta)^{1+\eta}}\right)^{\mu} \;=\; \big(2a_2\mathrm{e}\big)^{\frac{1}{2a_2}a_2|C|} \times \mathrm{e}^{-\mu} \\
&\leq \big(2a_2\mathrm{e}\big)^{|C|} \;\leq\; \big(2a_2\mathrm{e}\big)^{\ell} \;=\; \big(2a_2\mathrm{e}\big)^{b_1(1-\delta)n}, \qquad (13)
\end{aligned}$$

where we let $\eta = (2a_2)^{-1} - 1$ so that it satisfies $(1+\eta)a_2 = 1/2$.

It is easy to check that $b_1 \geq 1/2$ holds for the value of b_1 defined in the proof of Lemma 5. Thus, we may choose some constant $c_2 < 1$ of Theorem 2 so that

$$a_2 \;\leq\; c_2^{1/(1-\delta)} \quad\Longleftrightarrow\quad a_2^{b_1(1-\delta)} \;\leq\; 2^{-3}(2\mathrm{e})^{-1}$$

holds. Then this implies

$$(2a_2\mathrm{e})^{b_1(1-\delta)} \;\leq\; 2^{-3},$$

and hence, (13) is at most $2^{-3n} = N^{-3}$. Since there are at most N^2 clauses, the lemma follows by the union bound. □

We can use the same parameter values except for a_2. For a_2, we add one more condition $a_2 \leq c_2^{1/(1-\delta)}$ in the above; but it is easy to check that this new condition (which may lower the choice of a_2) does not affect the choice of the other parameters. (Note that we can use the constant c of Theorem 1 for c_1.) In particular, we can choose a_1 and b_1 so that the bound (6) for β_1 holds. Therefore, we have Theorem 2.

5 A lower bound

We move on to the proof of Theorem 3. The idea is relatively easy. For any $\varepsilon \geq 0$ and $\delta \in [0,1]$, consider α satisfying (3) of Theorem 3. Let Π be the set of partial assignments fixing values of αN variables. Our goal is to show F that satisfies the conditions (i) and (ii) of the theorem *and* that is satisfied by no $\rho \in \Pi$.

We define F randomly as the conjunction of $N^{1+\varepsilon}$ random clauses chosen independently. Roughly speaking, each clause is a disjunction of approximately s randomly chosen literals. The parameter s is chosen large enough to guarantee that each clause is satisfiable with a certain probability so that F's sat. assignment ratio exceeds $\Gamma := \exp_2(-N^{\delta})$ with probability larger than some γ. On the other hand, we keep s small enough so that each clause is satisfied with relatively small probability by fixing values of at most αN variables, thereby ensuring that $F|\rho = 1$ for some partial assignments $\rho \in \Pi$ with probability $< \gamma$. Then with the probabilistic argument, we can show the existence of our target Boolean formula F.

To explain this idea in detail, we only have to give a precise method to define a random clause. For a given parameter s that will be defined later, our random clause C is defined as the disjunction of literals that are selected independently with probability s/N. The following claim holds under this method of generating random clauses.

Claim 3. *For any assignment* $\mathbf{a} \in \{0,1\}^N$ *and any partial assignment* $\rho \in \Pi$*, we have*

$$\Pr_C[\,C(\mathbf{a}) = 0\,] \;\approx\; \mathrm{e}^{-s}, \quad \text{and} \quad \Pr_C[\,C|\rho \neq 1\,] \;\approx\; \mathrm{e}^{-s\alpha}.$$

Proof. Consider any $\rho \in \Pi$, and let $I_{\rho,+}$ (resp., $I_{\rho,-}$) be the set of indecies i such that $\rho(X_i) = 1$ (resp., $\rho(X_i) = 0$). A random clause C is not satisfied by ρ (i.e., $C|\rho \neq 1$ holds) if and only if X_i is not chosen for all $i \in I_{\rho,+}$ *and* $\overline{X_i}$ is not chosen for all $i \in I_{\rho,-}$. Thus, we have

$$\Pr_C[\,C|\rho \neq 1\,] \;=\; \left(1 - \frac{s}{N}\right)^{\alpha N} \;\approx\; \mathrm{e}^{-s\alpha}.$$

□

Here we fix s by

$$s \;=\; (1+\varepsilon-\delta)\ln N + 1,$$

from which we have

$$\mathrm{e}^{-s}N^{1+\varepsilon} \;=\; N^{\delta}/\mathrm{e}. \tag{14}$$

Note also that $0 < s/N < 1$; hence, we can use s/N as a parameter for our random selection. We define our random formula F by the conjunction of $N^{1+\varepsilon}$ clauses randomly defined as above independently. Then we have the following two claims, from which the existence of our desired F follows immediately.

Claim 4.

$$\Pr_F\left[\,\text{sat.ratio}(F) \ge \Gamma\,\right] \;\ge\; \exp_2\left(-N^{\delta}\right). \tag{15}$$

Proof. Consider any assignment $\mathbf{a} \in \{0,1\}^N$. From Claim 3 and from the definition of random formula F, it follows

$$\Pr_F[\,F(\mathbf{a})=1\,] \;\approx\; \left(1-\mathrm{e}^{-s}\right)^{N^{1+\varepsilon}} \;\approx\; \exp\left(-\mathrm{e}^{-s}N^{1+\varepsilon}\right) \;=\; \exp\left(-N^{\delta}/\mathrm{e}\right),$$

where the last expression is from (14). Let Γ' denote $\exp(-N^{\delta}/\mathrm{e})$. Note that $\Gamma' >> \Gamma = \exp_2(-N^{\delta})$; in particular, we have $\Gamma' > 2\Gamma$.

Now we use the standard averaging argument. Note first that

$$\begin{aligned}
\mathrm{Exp}_F\left[\,\text{sat.ratio}(F)\,\right] \;&=\; \mathrm{Exp}_F\left[2^{-N}\sum_{\mathbf{a}} F(\mathbf{a})\right]\\
&=\; 2^{-N}\sum_{\mathbf{a}} \mathrm{Exp}_F\left[\,F(\mathbf{a})\,\right]\\
&=\; 2^{-N}\sum_{\mathbf{a}} \Pr_F\left[\,F(\mathbf{a})=1\,\right] \;\approx\; \Gamma'
\end{aligned}$$

On the other hand, letting $p = \Pr_F[\,\text{sat.ratio}(F) < \Gamma\,]$, we have

$$\mathrm{Exp}_F\left[\,\text{sat.ratio}(F)\,\right] \;<\; p\cdot\Gamma + (1-p)\cdot 1 \;=\; 1-p(1-\Gamma).$$

Then from the above two (in)equalities, we have $\Gamma' < 1-p(1-\Gamma)$, from which

$$p \;<\; \frac{1-\Gamma'}{1-\Gamma} \;=\; 1-\frac{\Gamma'-\Gamma}{1-\Gamma} \;<\; 1-\Gamma$$

since $\Gamma' > 2\Gamma$ and $1-\Gamma < 1$. This proves the claim. $\square$

Claim 5.

$$\Pr_F\left[\,\exists \rho \in \Pi\left[\,F|\rho = 1\,\right]\,\right] \;\le\; \left(\frac{2}{\mathrm{e}}\right)^{N} \;<<\; \Gamma. \tag{16}$$

Proof. Consider any partial assignment $\rho \in \Pi$. Again from Claim 3 and from the definition of random formula F, it follows

$$\Pr_F[\,F|\rho=1\,] \;\approx\; \left(1-\mathrm{e}^{-s\alpha}\right)^{M} \;\approx\; \exp\left(-\mathrm{e}^{-s\alpha}M\right) \;=\; \exp\left(-\left(\frac{N^{\delta-(1+\varepsilon)}}{\mathrm{e}}\right)^{\alpha} N^{1+\varepsilon}\right).$$

We will analyze below the last expression and show that it is at most $\exp(-2N)$; then the claim follows from the union bound because there are at most 3^N partial assignments.

We show that the argument of the above expression $\exp(\cdots)$ is at most $-2N$; to see this, consider

$$\ln\left(\left(\frac{N^{\delta-(1+\varepsilon)}}{\mathrm{e}}\right)^{\alpha} N^{1+\varepsilon} \right) \;=\; \big((1+\varepsilon) - \alpha(1+\varepsilon-\delta)\big)\ln N - \alpha. \tag{17}$$

Here note that there is some $a > 0$ with which

$$\alpha \;=\; \frac{\varepsilon - a}{1+\varepsilon-\delta}$$

holds; this follows from the assumption (3) and the fact that $1+\varepsilon-\delta > 0$. Then we can restate (17) by

$$(17) \;=\; (1+a)\ln N - \alpha \;=\; \ln N + a\ln N - \alpha,$$

and, noting that $\alpha \le 1$, this can be bounded below by $\ln N + \ln 2 = \ln(2N)$ for sufficiently large N. This gives our desired bound. □

From this lower bound, we know, for any F with N^d clauses, the size of a partial assignment ρ satisfying F must be at least $1 - 1/d$ that goes to 1 with $d \to \infty$. But it does not exclude the possibility that any N^d-size CNF formula has some satisfying partial assignment of size $\alpha_d N$ for some $\alpha_d < 1$ if it has sat. assignment ratio greater than, say, $> 1/2$. On the other hand, it is easy to see that our upper bound approach works only for CNF formulas with $N^{1+\varepsilon}$ clauses for some $\varepsilon < 1$ (no matter how we choose the technical parameters). Note first that b_1 must be smaller than 1 in order to bound the number of iterations of defining $\overline{\sigma}$ by $O(N^{\beta_1})$ for some $\beta_1 < 1$ (see (6)). Then from (9) we need $a_1 > 0$, which means that the threshold L for "being popular" is sublinear in N. Then again for bounding the number of iterations (based on the bound $M/L = N^{1+\varepsilon}/L$), we need the condition $\varepsilon < 1$. It is an interesting open problem to determine whether this $\varepsilon < 1$ bound is essential.

References

[1] K. Chandrasekaran, N. Goyal, and B. Haeupler, Deterministic algorithms for the Lovász Local Lemma, in *Proc. of the 21st Annual ACM-SIAM Sympos. on Discrete Algorithms* (SODA'10), SIAM, 992–1004, 2010.

[2] A. De, O. Etesami, L. Trevisan, and M. Tulsiani, Improved pseudo-random generators for depth 2 circuits, in *Proc. the 14th. International Workshop on Randomization and Computation*, (APPROX-RANDOM'10), Lecture Notes in Computer Science 6302, 504–517, 2010.

[3] E. Hirsch, A fast deterministic algorithm for formulas that have many satisfying assignments, *Logic Journal of the IGPL*, 6(1): 59–71, 1998.

[4] R. Moser, A constructive proof of the Lovász local lemma, in *Proc. of the 41st Annual ACM Sympos. on Theory of Computing* (STOC'09), 343–350, 2009.

[5] R. Moser and G. Tardos, A constructive proof of the general Lovász local lemma, *J. ACM*, 57(2), 2010.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de