# The unsatisfiability threshold revisited

Alexis C. Kaporis [a,1,2] Lefteris M. Kirousis [a,1,2]
Yannis C. Stamatiou [a,b,1,3] Malvina Vamvakari [a,b,3] Michele Zito [c,4]

[a] *University of Patras, Department of Computer Engineering and Informatics, University Campus, GR-265 04 Patras, Greece.*
*e-mail: {kaporis,kirousis,stamatiu,mvamv}@ceid.upatras.gr.*

[b] *Computer Technology Institute, 61 Riga Feraiou Str., GR-262 21 Patras, Greece.*

[c] *Department of Computer Science, University of Liverpool, U.K.*
*e-mail: michele@csc.liv.ac.uk.*

**Abstract**

The problem of determining the unsatisfiability threshold for random 3-SAT formulas consists in determining the clause to variable ratio that marks the experimentally observed abrupt change from almost surely satisfiable formulas to almost surely unsatisfiable. Up to now, there have been rigorously established increasingly better lower and upper bounds to the actual threshold value. In this paper, we consider the problem of bounding the threshold value from above using methods that, we believe, are of interest on their own right. More specifically, we show how the method of *local maximum satisfying truth assignments* can be combined with results for the *occupancy problem* in schemes of random allocation of balls into bins in order to achieve an upper bound for the unsatisfiability threshold less than 4.571. In order to obtain this value, we establish a bound on the $q$-binomial coefficients (a generalization of the binomial coefficients). No such bound was previously known, despite the extensive literature on $q$-binomial coefficients. Finally, to prove our result we had to establish certain relations among the conditional probabilities of an event in various probabilistic models for random formulas. It turned out that these relations were considerably harder to prove than the corresponding ones for unconditional probabilities, which were previously known.

*Key words:* phase transition, complexity, satisfiability, probabilistic analysis.

[1] Research partially supported by the University of Patras - Research Committee, project C. Carathéodory . Also supported by Action PYTHAGORAS I of the Operational Programme for Educational & Vocational Training II, with matching funds from the European Social Fund and the Greek Ministry of Education.
[2] Research partially supported by the Computer Technology Institute.
[3] Research supported by the Computer Technology Institute.
[4] Research supported by EPSRC grant GR/L/77089.

## 1 Introduction

Let $\phi$ be a random 3-SAT formula constructed by selecting uniformly and with replacement $m$ clauses from the set of all possible clauses with three literals over $n$ variables. We call this model for constructing random formulas the $G_{mm}$ model; the double $m$ in the subscript refers to the possibility of replacement. Also,let $G_m$ be the probabilistic model where repetition of clauses is not allowed and let $G_p$ be the model where each clause has independent probability $p$ to be included in the formula. More on the last two alternative models in Section 4. It has been observed experimentally that as the numbers $n, m$ of variables and clauses, respectively, tend to infinity, while the ratio $m/n$ remains equal to a constant $r$, the random formulas exhibit a threshold behavior: if $r > 4.2$ (approximately) then almost all random formulas are unsatisfiable while the opposite is true if $r < 4.2$. The constant $r$ is called the *density* of the formula. On the theoretical side, Friedgut [10] has proved that there exists a sequence $\gamma_n$ such that for any $\epsilon > 0$, if finally for all $n$, $r \leq \gamma_n - \epsilon$, then the probability of a random formula being satisfiable approaches 1, while if finally for all $n$, $r \geq \gamma_n + \epsilon$, then this probability approaches 0. It has not been rigorously proved that the sequence $\gamma_n$ converges. Thus, proving that a threshold value exists and if it actually exists finding its *exact* value is still a major problem in probability and complexity theory. Up to now, only upper and lower bounds have been rigorously established for the threshold value (formally, for the terms of the sequence $\gamma_n$, as a threshold may not exist). The best lower bound has been recently proved by D. Achlioptas and G. Sorkin in [1] and it is 3.26. Concerning the upper bound, Dubois et al. in [6] announced that they have obtained the value 4.506. After the submission of our paper, a full proof for this upper bound was provided by Dubois et al. in [7]. Previously, Janson et al. [12] had established the value 4.596.

In this paper, we address the upper bound question for the unsatisfiability threshold from a new perspective that combines the idea of *local maximum* satisfying truth assignments proposed by Kirousis et al. in [14] with the sharp probability estimates for the occupancy problem in schemes of random allocation of balls into bins given by Kamath et al. in [13] (for an excellent introduction to the occupancy problem see [8,17]). With this approach, we obtain as an upper bound the number 4.571. The last author, following a similar approach, gives in his Ph.D. thesis [23] a bound of 4.5793 but without resorting to $q$-binomial coefficients (a generalization of the binomial coefficients). To obtain the value of 4.571, we had to establish an upper bound to the $q$-binomial coefficients. Despite the extensive literature on $q$-binomial coefficients (see, e.g., [9,11,16]), no such bound was, to the best of our knowledge, known.

Also, to obtain our result we had to carry the computation of a conditional probability in $G_p$ . There are classical results (see e.g., [2]), supported by intuition, that relate the unconditional probabilities of an event in $G_p$ and $G_m$ , respectively.

It turned out that getting corresponding results for conditional probabilities was harder, and moreover intuition offered no reliable guidance in this case. Section 4 contains these results. We consider them as a non-trivial part of this work.

## 2 The method of local maxima

In this section, we will state briefly the methodology followed in [14] and state an inequality that bounds from above the probability that a random formula is satisfiable. This inequality will be the starting point of our considerations.

Let $\mathbf{S}$ be the class of all truth assignments to $n$ variables and $\mathbf{A}_n$ the (random) class of truth assignments that satisfy a random formula $\phi$. For a given $A \in \mathbf{S}$, a *single flip* $sf$ is the change in $A$ of exactly one specified FALSE value to TRUE. By $A^{sf}$ we denote the truth assignment that results from this change. We define as $\mathbf{A}_n^1 \subseteq \mathbf{A}_n$ the random class of truth assignments with the following two properties:

- $A \models \phi$,
- for every single flip $sf$, $A^{sf} \not\models \phi$.

A partial order can be defined on $\mathbf{S}$: a truth assignment $A$ is smaller than a truth assignment $A'$ iff there exists an $i$ such that both $A$ and $A'$ assign the same value to the variables $x_j$, for all $j < i$, while $A$ assigns FALSE to $x_i$ and $A'$ assigns TRUE to it. The random class $\mathbf{A}_n^1$ coincides with the set of satisfying truth assignments that are *local maxima* with respect to the partial order defined above, among satisfying truth assignments that differ in one bit.

A more restricted random class of truth assignments results from $\mathbf{A}_n^1$ if we extend the scope of locality in obtaining a local maximum. A *double flip* is the change of exactly two specified variables $x_i$ and $x_j$, with $i < j$, where $x_i$ is changed from FALSE to TRUE and $x_j$ from TRUE to FALSE. In analogy with single flips, by $A^{df}$ we denote the truth assignment that results from $A$ if we apply the double flip $df$. Let $\mathbf{A}_n^2$ be defined as the set of truth of assignments $A$ that have the following properties:

- $A \models \phi$,
- for all single flips $sf$, $A^{sf} \not\models \phi$,
- for all double flips $df$, $A^{df} \not\models \phi$.

Our starting point is the following inequality:

LEMMA 1 [14]

$$\Pr[\phi \text{ is satisfiable}] \leq \mathrm{E}[|\mathbf{A}_n^2|] =$$

$$\Pr[A \models \phi] \sum_{A \in \mathbf{S}} \left( \Pr[A \in \mathbf{A}_n^1 \mid A \models \phi] \cdot \Pr[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \right) =$$
$$(7/8)^{rn} \sum_{A \in \mathbf{S}} \left( \Pr[A \in \mathbf{A}_n^1 \mid A \models \phi] \cdot \Pr[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \right). \quad (1)$$

In order to find an upper bound for the unsatisfiability threshold, it suffices to find the smallest possible value for $r$ for which the right-hand side of (1) tends to 0. Given a random formula $\phi$ and a truth assignment $A$, the probability that all single flips of $A$ falsify the random formula $\phi$, i.e., $\Pr[A \in \mathbf{A}_n^1 \mid A \models \phi]$, is called the probability that the single flips of $A$ are *blocked*. Similarly, the $\Pr[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1]$ is called the conditional probability that the double flips are blocked. The conditional in this case refers to the event that the single flips of $A$ are blocked. In Section 3, we compute asymptotically the probability that the single flips are blocked. In Section 4, we introduce some machinery for translating the conditional probability that the double flips are blocked from the model $G_{mm}$ to the model $G_p$ (these models will formally defined in the same Section). In $G_p$ it is easier to handle the correlations between the events that each particular double flip is blocked. In Section 5, we establish an upper bound for the conditional probability that double flips are blocked (in $G_{mm}$). Finally, in Section 6, we compute an upper bound for the sum in (1). For that, we prove an asymptotic formula for the $q$-binomial coefficients. We then put everything together to establish the value 4.571.

## 3 Computation of the probability that the single flips are blocked

In this section, we will find an exact asymptotic expression for $\Pr[A \in \mathbf{A}_n^1 \mid A \models \phi]$ using a sharp estimate for the occupancy problem provided in [13]. The formula obtained in [14] was not exact. Such an exact expression was given by Dubois and Boufkhad [5] (who independently from [14] introduced the approach of single flips), but they used a different approach. Later, Zito in his thesis [23] also found an exact expression, with a method very similar to the one in this paper (he used the game of coupon collecting).

REMARK 1 *Notice that the conditional $A \models \phi$ is satisfied if we assume that the $m = rn$ clauses selected to form the formula are chosen from the $7\binom{n}{3}$ clauses that are satisfied by $A$. As in the sequel we will always work under the conditional $A \models \phi$, for a given truth assignment $A$, we assume for the rest of the paper that all events are conditional on $A \models \phi$ and that all clauses are selected from those that are satisfied by $A$. Also, for the rest of the paper, we will omit the conditional $A \models \phi$, unless its omitting may cause confusion. Actually, since we* a priori *assume that clauses are selected from the ones satisfied by $A$, the probabilities involved can be considered as unconditional. Notice that we cannot do the same if the conditional involved is that all single flips are blocked.*

Let $\phi$ be a formula considered as a multiset of $rn$ clauses. Given a set of clauses $\mathbf{B}$, the expression $\phi \cap \mathbf{B}$ has the meaning of set intersection with the additional requirement that a clause that appears in the intersection appears as many times as it appears in $\phi$.

Given a truth assignment $A$ and a variable $x$ such that $A(x) = \text{FALSE}$, the set of *blocking clauses* of $A$ for the variable $x$, denoted by $\mathbf{B}(A, x)$, is the set of clauses that have a unique literal that is satisfied by $A$ and this is $\neg x$. Obviously, the single flip of $A$ on $x$ falsifies a formula $\phi$ iff $\phi \cap \mathbf{B}(A, x) \neq \emptyset$. Let $\mathbf{B}_A$ be the set of blocking clauses of $A$ for all variables that are FALSE under $A$.

We partition the set of all formulas $\phi$ satisfiable by $A$ with respect the number $l, l = 0, \ldots, rn,$ of blocking clauses from $\mathbf{B}_A$ that are contained in $\phi$. Also we assume that $A$ has $k$ FALSE variables. Then we have:

$$\Pr[A \in \mathbf{A}_n^1\,] = \sum_{l=0}^{rn} \Big( \Pr[A \in \mathbf{A}_n^1 \mid |\phi \cap \mathbf{B}_A| = l] \cdot \Pr[|\phi \cap \mathbf{B}_A| = l\,] \Big)\,. \qquad (2)$$

To compute $\Pr[A \in \mathbf{A}_n^1 \mid |\phi \cap \mathbf{B}_A| = l]$, first observe that for every variable $x$ such that $A(x) = \text{FALSE}$ we have $|\mathbf{B}(A, x)| = \binom{n-1}{2}$. Therefore, for any $x$ such that $A(x) = \text{FALSE}$, a clause in $\mathbf{B}_A$ has uniform probability $\frac{\binom{n-1}{2}}{k\binom{n-1}{2}} = \frac{1}{k}$ to belong to $\mathbf{B}(A, x)$. Also, for every pair of distinct variables $x, y$ such that $A(x) = A(y) = \text{FALSE}$, we have $\mathbf{B}(A, x) \cap \mathbf{B}(A, y) = \emptyset$. Therefore, if we view each of the mutually disjoint subsets $\mathbf{B}(A, x)$ as a bin and each clause in $\mathbf{B}_A$ as a ball, the distribution of the clauses in $\mathbf{B}_A$ into the subsets $\mathbf{B}(A, x)$, where $x$ is FALSE under $A$, can be viewed as a uniform at random allocation of balls into bins. As a consequence, the event $A \in \mathbf{A}_n^1$, conditional on the event $|\phi \cap \mathbf{B}_A| = l$, is true iff after throwing $l$ balls uniformly at random into $k$ bins, as described above, none of the bins remains empty. This is an instance of the *occupancy problem*.

Before we continue, let us describe the notation for asymptotics that we will use. Given two functions $F$ and $G$ of $n$, $F \sim G$ denotes that $\lim_{n\to\infty} \frac{F(n)}{G(n)} = 1$ and $F \asymp G$ denotes that $\ln(F) \sim \ln(G)$.

The following theorem by Kamath et al. ([13]) gives a sharp estimate for the probability that $w$ bins remain empty:

**Theorem** 1 [13] *Let $W$ be the random variable that gives the number of empty bins after the placement, uniformly and independently, of $l$ balls into $k$ bins, where both $l$ and $k$ are constant multiples of $n$. Let $c = \frac{l}{k} \geq 1$. If we denote by $H(l, k, w)$ the probability that $W = w$ and if, in addition, $|w - \mathrm{E}[W]| = \Omega(k)$ then*

$$H(l, k, w) \asymp e^{-k(\int_0^{1-\frac{w}{k}} \ln(\frac{s_w - x}{1-x})dx - c\ln(s_w))},$$

*where $s_w$ is the solution of the equation*

$$w = k(1 - s_w(1 - e^{-c/s_w})). \tag{3}$$

For our purposes, since we require to have at least one blocking clause for each of the $k$ FALSE values of $A$, or equivalently no bin to remain empty, we set $w = 0$. Then we have:

$$|w - \mathrm{E}[W]| = |0 - k(1 - \frac{1}{k})^l| = \Omega(k).$$

Let now $k$, the number of FALSE values of $A$, be $\alpha n$ and $l$, the number of blocking clauses, be $\beta r n$, for some $\alpha, \beta \in [0, 1]$ such that $\beta \geq \frac{\alpha}{r}$. Then $c = \frac{\beta r}{\alpha}$. From (3) we get:

$$0 = k[1 - s_0(1 - \exp^{-\frac{c}{s_0}})] \Leftrightarrow \ln(s_0 - 1) = \ln(s_0) - \frac{c}{s_0}.$$

It can be verified that because of the above equality

$$s_0 = \frac{c}{c + \mathbf{W}(-c\exp(-c))},$$

where $\mathbf{W}$ is a special function known as Lambert **W** function (for details about this function see [4]). In addition it can be easily verified that:

$$\int_0^1 \ln(\frac{s_0 - x}{1 - x})dx = s_0 \ln(s_0) - s_0 \ln(s_0 - 1) + \ln(s_0 - 1) = c + \ln(s_0 - 1).$$

Thus,

$$H(l, k, 0) \asymp \exp\left[-k(c + \ln(s_0 - 1) - c\ln(s_0))\right].$$

Therefore:

$$\begin{aligned}\Pr[A \in \mathbf{A}_n^1 \mid |\phi \cap \mathbf{B}_A| = l] &= H(k, l, 0) \\ &\asymp \exp\left[-k(c + \ln(s_0 - 1) - c\ln(s_0))\right].\end{aligned} \tag{4}$$

Now to compute $\Pr[|\phi \cap \mathbf{B}_A| = l\ ]$, i.e. the second probability appearing in the right-hand side of (2), we consider the sequence of clause selections for $\phi$, drawn from the set of all clauses satisfied by $A$, as a sequence of $m = rn$ Bernoulli trials. Success occurs whenever a clause belongs to $\mathbf{B}_A$, i.e. it is a blocking clause. The probability of this event is equal to $\frac{k\binom{n-1}{2}}{7\binom{n}{3}} = \frac{3k}{7n} = \frac{3\alpha}{7}$. We have the following asymptotic expansion of a Binomial distribution with constant probability of success:

$$\begin{aligned}\Pr[|\phi \cap \mathbf{B}_A| = l\ |] &= \binom{rn}{l}\left(\frac{3k}{7n}\right)^l\left(1 - \frac{3k}{7n}\right)^{rn-l} \\ &\asymp \left[\frac{(3\alpha)^\beta(7 - 3\alpha)^{(1-\beta)}}{7\beta^\beta(1 - \beta)^{(1-\beta)}}\right]^{rn},\end{aligned} \tag{5}$$

where we used $\binom{rn}{l} \asymp \left[ (\frac{rn}{l})^{\frac{l}{rn}} (\frac{rn}{rn-l})^{(1-\frac{l}{rn})} \right]^{rn}$. Let now $E(\alpha, \beta, r)$ be given by

$$\exp\left[-\alpha(c + \ln(s_0 - 1) - c \ln s_0)\right] \left( \frac{(3\alpha)^{\beta}(7-3\alpha)^{1-\beta}}{7\beta^{\beta}(1-\beta)^{1-\beta}} \right)^{r}. \tag{6}$$

Combining (2), (4), (5) and (6), we obtain the following (recall that $\alpha = \frac{k}{n}$ and $\beta = \frac{l}{rn}$):

**Theorem** 2

$$\Pr[A \in \mathbf{A}_n^1] \asymp \sum_{l=k}^{rn} \left(E(\alpha, \beta, r)\right)^n. \tag{7}$$

REMARK 2 *The bound of the expectation* $\mathrm{E}[|\mathbf{A}_n^2|]$ *given in (1) contains factors that are exponential in* $n$ *functions. Therefore, to find the value of* $r$ *for which this bound has limit zero, we may ignore polynomial and inverse polynomial factors. In other words, we work within the scope of the "*$\asymp$*" asymptotics. In the sequel, sometimes we will omit to explicitly mention that an equality or inequality between probabilities holds within a rational (i.e., fraction of polynomials) factor. Especially if the fact that this assumption is made is obvious from the context.*

## 4 Probability models for random formulas

Fix a truth assignment $A$. Recall that we consider random formulas with $m = rn$ clauses that are uniformly at random and with replacement drawn from the set of $7\binom{n}{3}$ clauses satisfied by $A$. We call this model of random formulas the $G_{mm}$ model (the double $m$ in the subscript is to remind that replacement is allowed). There are alternatives to this model:

- Select the $m = rn$ clauses of $\phi$, drawing each clause uniformly and independently from the set of clauses satisfied by $A$ *without* replacement (model $G_m$).
- Each of the clauses that are satisfied by $A$ is independently chosen with probability $p(n)$ for inclusion in $\phi$ (model $G_p$).

A random formula in $G_p$ has variable length, while in $G_{mm}$ and $G_m$ it has fixed length equal to $m = rn$. Notice that if $p = \frac{rn}{7\binom{n}{3}} \sim (6r)/(7n^2)$, the expected length of a random formula in $G_p$ is $m = rn$. Unless otherwise specified, we assume in the sequel that whenever the model $G_p$ is examined, $p \sim (6r)/(7n^2)$. The probability of an event $Q$ concerning a random formula $\phi$ generated according to model $G_m$ , $G_{mm}$ or $G_p$ is denoted by $\Pr_m[\phi \in Q], \Pr_{mm}[\phi \in Q]$ and $\Pr_p[\phi \in Q]$, respectively.

Notice that the probabilities in (1) are all in $G_{mm}$, since the model we considered until now allows clause repetitions when forming a formula.

In [14] both the probability to block all single flips and the conditional probability to block all double flips where computed in $G_p$ . To show that this is legitimate, it was first observed in [14] that the product of these two probabilities is equal to the unconditional probability that all flips (single and double) are blocked. Then it was shown, by a fairly easy argument, that the transition from $G_{mm}$ to $G_p$ can be legitimately performed for such an unconditional probability. Finally, the later probability was again factored into the product of the probability that all single flips are blocked with the conditional probability that all double flips are blocked, and each factor was computed separately (in $G_p$).

However, the probability in $G_p$ of an event that refers to the blocking of flips is in general larger than the corresponding probability in $G_{mm}$ by an exponential factor. So, the model change pays the price of getting a slightly larger upper bound to the threshold. In the previous chapter we computed exactly (within a rational factor) the probability that the single flips are blocked. Unfortunately, we were not able to do the same for the conditional probability that the double flips are blocked. This makes necessary to resort again to the model $G_p$ . However, to retain the advantageous computation of the probability for the single flips in $G_{mm}$ , the transition from one model to the other for double flips has to be performed for the conditional probability. That this transition of a *conditional* probability can be legitimately performed (although again at some price) is the object of this Section.

We start with the easy part. We first establish the legitimacy of changing model from $G_{mm}$ to $G_m$ , for a conditional probability. Actually we show that these two models are equivalent, within a rational factor, for the events that interest us.

Let P be the event that $\phi$ has no two clauses identical and let $\bar{P}$ its complement. Then, because the order of the number of all possible clauses is $\Theta(n^3)$ and the order of the number of the clauses contained in $\phi$ is $\Theta(n)$, $\lim_{n\to\infty} \Pr_{mm}[\bar{P}] = 0$.

Now let $Q_1$ and $Q_2$ be two arbitrary events such that the following two conditions, which we call *regularity* conditions hold:

- For some $\epsilon > 0$ and finally for all $n$, $\ln(\Pr_m[Q_2|Q_1]) < -\epsilon$, i.e. $\Pr_m[Q_2|Q_1]$ is bounded away from 1.
- $\lim_{n\to\infty} \Pr_{mm}[\bar{P}|Q_1, Q_2] = \lim_{n\to\infty} \Pr_{mm}[\bar{P}|Q_1] = 0$.

Under the above regularity conditions, we have that:

$$\Pr_m[Q_2|Q_1] \asymp \Pr_{mm}[Q_2|Q_1]. \tag{8}$$

Indeed,

$$\Pr_m[Q_2\,|Q_1] = \Pr_{mm}[Q_2\,|Q_1, P] = \frac{\Pr_{mm}[Q_2\,|Q_1] - \Pr_{mm}[Q_2 \wedge \bar{P}\,|Q_1]}{1 - \Pr_{mm}[\bar{P}\,|Q_1]}$$
$$= \Pr_{mm}[Q_2\,|Q_1]\frac{1 - \Pr_{mm}[\bar{P}\,|Q_2, Q_1]}{1 - \Pr_{mm}[\bar{P}\,|Q_1]}.$$

Now first taking logarithms, then dividing both sides with $\ln(\Pr_m[Q_2|Q_1])$ and finally letting $n \to \infty$, we get the required (the regularity conditions are needed in the computation of the limits). This concludes the proof that $G_{mm}$ and $G_m$ are equivalent.

When $Q_1$ and $Q_2$ are the events $A \in \mathbf{A}_n^1$ and $A \in \mathbf{A}_n^2$, respectively, then the first regularity condition is satisfied, as, according to the bound we compute in Section 5 (Relation (17)), $\Pr_m[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1]$ is exponentially small. Also, the second regularity condition is true for this particular choice of $Q_2$ and $Q_1$. Indeed both these events and their conjunction are negatively correlated with $\bar{P}$, so $\Pr_{mm}[\bar{P}|Q_1] \leq \Pr_{mm}[\bar{P}] \to 0$ and similarly for $\Pr_{mm}[\bar{P}|Q_1, Q_2]$. To prove the negative correlation claim for, say, $Q_1$ and $\bar{P}$, observe that the correlation claim is equivalent to $\Pr_{mm}[Q_1|P] \geq \Pr_{mm}[Q_1]$, which in turn is equivalent to $\Pr_m[Q_1] \geq \Pr_{mm}[Q_1]$. This last inequality is intuitively obvious (under the assumption that $A \models \phi$), because the probability to get blocking clauses for all FALSE values of the satisfying truth assignment $A$ increases when the clauses of the formula are assumed to be different. For a formal proof of this for general increasing and reducible properties (like $Q_1$ and $Q_2$), we refer to [15].

We come now to the relation between $G_m$ and $G_p$ . Bollobás in [2] proves that for an arbitrary event $Q$, $\Pr_p[Q] \geq \Pr_m[Q]$ (within a polynomial factor—but in general $\Pr_p[Q]$ may be exponentially larger than $\Pr_m[Q]$) if $p$ and $m$ are related so that the expected length of a formula in $G_p$ is $m$. In our case, this means that $m = rn$ and $p = (6r)/(7n^2)$. To get the analogous result for a conditional probability, assume that we have a probability value $p'$ not necessarily equal to $(6r)/(7n^2)$, but equal to $(6r')/(7n^2)$ for an $r'$ different, in general, from the value of the upper bound $r$ we are trying to compute. The value of $m$ is considered fixed and equal to $rn$. We then proceed as in [2]:

$$\begin{aligned}
&\Pr_{p'}[A \in \mathbf{A}_n^2\,|A \in \mathbf{A}_n^1] = \\
&\sum_{i=0}^{7\binom{n}{3}} \left(\Pr_{p'}[|\phi| = i\,|A \in \mathbf{A}_n^1] \cdot \Pr_{p'}[A \in \mathbf{A}_n^2\,|A \in \mathbf{A}_n^1, |\phi| = i]\right) = \\
&\sum_{i=0}^{7\binom{n}{3}} \left(\Pr_{p'}[|\phi| = i\,|A \in \mathbf{A}_n^1] \cdot \Pr_i[A \in \mathbf{A}_n^2\,|A \in \mathbf{A}_n^1]\right) \geq \\
&\Pr_{p'}[|\phi| = m\,|A \in \mathbf{A}_n^1] \cdot \Pr_m[A \in \mathbf{A}_n^2\,|A \in \mathbf{A}_n^1].
\end{aligned} \tag{9}$$

Above, the probabilities with subscript $p'$ are in the variable formula-length model, while all other probabilities are in the fixed formula-length model without repetitions. We now claim that for every given truth assignment $A$, there exists appropriate choice of $p' < p$ (or equivalently a choice of an $r' < r$), such that $\Pr_{p'}[|\phi| = rn \mid A \in \mathbf{A}_n^1] = 1$ (within a rational factor). The required value of $p'$ is (as it is intuitively expected) that for which the expectation of the length of the random formula conditional on the event $A \in \mathbf{A}_n^1$, i.e. conditional on the event that the single flips are blocked, in the model $G_{p'}$, is $m = rn$. Intuitively it is expected that this value of $p'$ is smaller than $(6r)/(7n^2)$, because the conditional that the single flips are blocked forces some clauses into the formula. This argument is formalized in Appendix A, where we actually prove that $r$ and $r'$ are related by the equality:

$$r = r' \left( \frac{3\alpha}{7(e^{3r'/7)} + 1)} + 1 \right), \tag{10}$$

where $\alpha n$ is the number of variables that are false under $A$.

Therefore we have that

**Theorem** 3 *For $r = m/n$, there is an $r' < r$ implicitly defined by the relation (10) above such that:*

$$\Pr_m[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \leq \Pr_{p'}[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1], \tag{11}$$

*where $p = (6r)/(7n^2)$, $m = rn$ and $p' = (6r')/(7n^2)$.*

NB Although we could not show that:

$$\Pr_m[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \leq \Pr_p[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1],$$

for $m = rn$ and $p = (6r)/(7n^2)$, still Theorem 3 above is sufficient to carry on our proof. Also, although $p' < p$ the previous relation does not immediately follow from (11), nor is it supported by intuition that

$$\Pr_{p'}[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \leq \Pr_p[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1],$$

because the probabilities involved are conditional; actually we conjecture that the last two relations are wrong for certain values of $r$.

## 5 Computation of an upper bound for the conditional probability that the double flips are blocked

By the first part of the previous Section,

$$\Pr_{mm}[A \in \mathbf{A}_n^2 \,|A \in \mathbf{A}_n^1] \asymp \Pr_m[A \in \mathbf{A}_n^2 \,|A \in \mathbf{A}_n^1]. \tag{12}$$

Now in [14], the following functions of $r$ were introduced:

$$\begin{aligned} u(r) &= e^{-r/7}, \\ z(r) &= -\frac{6u^6 \ln(1/u)}{1-u^3} - \frac{18u^9 \ln^2(1/u)}{(1-u^3)^2} \cdot \frac{\mathbf{W}\left(-\frac{6u^6 \ln(1/u)}{1-u^3}\right)}{\frac{6u^6 \ln(1/u)}{1-u^3}}, \end{aligned} \tag{13}$$

$$Y_n(r) = 1 + z(r)\frac{1}{n} + o\left(\frac{1}{n}\right) \tag{14}$$

and was proved that for *any* $r \in [3,5]$ and for $p = (6r)/(7n^2)$:

$$\Pr_p[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \leq (Y_n(r))^{df(A)}, \tag{15}$$

where $df(A)$ is the number of double flips of $A$.

It is easy to check analytically (or, for the non-purist, using Maple) that $z(r) < 0$ at least in the interval $[3,5]$ and that $z(r)$ is an *increasing* function of $r$ at least in the interval $[3.5,5]$. Also, from Relation (10) it follows that for any $r \in [4,5]$ and for any $A$, $(0.9)r < r' < r$. Therefore, if $r$ is in the interval $[4,5]$ then $r'$ is in the interval $[3.5,5]$ (all these numerical values are far from being the best possible, yet are sufficient for our purposes). So from the monotonicity of $z(r)$ in $[3.5,5]$ and from the definition of $Y_n(r)$ (Relation (14)) we get that for any $r \in [4,5]$, for sufficiently large $n$ and for $r'$ as is implicitly defined by (10),

$$0 < Y_n(r') < Y_n(r) < 1. \tag{16}$$

Using now Relation (11), Relation (15) applied to $r'$ and $p' = (6r')/(7n^2)$, and finally Relation (16), we get that for any $r \in [4,5]$:

$$\Pr_m[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \leq (Y_n(r))^{df(A)}, \tag{17}$$

therefore, by Relation (12) we get:

$$\Pr_{mm}[A \in \mathbf{A}_n^2 \mid A \in \mathbf{A}_n^1] \leq (Y_n(r))^{df(A)}, \tag{18}$$

where $m = rn$ and $p = (6r)/(7n^2)$. Therefore,

$$\begin{aligned}\Pr[\phi \text{ is satisfiable}] &\leq \mathrm{E}[|\mathbf{A}_n^2|] \\ &\leq (7/8)^{rn} \sum\nolimits_{A \in \mathbf{S}} \left( \Pr_{mm}[A \in \mathbf{A}_n^1] \cdot (Y_n(r))^{df(A)} \right). \end{aligned} \tag{19}$$

In the next Section, we will bound the above sum.

## 6 Asymptotics

In the sequel, we establish an asymptotic upper bound for the $q$-binomial coefficients that will help us to estimate the summation in (19).

Let $sf(A) = k = \alpha n$ denote the number of FALSE values assigned by the truth assignment $A$, i.e. the number of single flips of $A$. Recall that $df(A)$ denotes the number of double flips of $A$. For notational convenience, let $z = z(r)$ and $Y = Y_n(r)$. Let also:

$$X(sf(A)) = \Pr_{mm}[A \in \mathbf{A}_n^1 \,|]. \tag{20}$$

Therefore, using (20), Inequality (19) may be written as follows:

$$\Pr_{mm}[\phi \text{ is satisfiable}] \leq (7/8)^{rn} \sum\nolimits_{A \in \mathbf{S}} X(sf(A)) Y^{df(A)}. \tag{21}$$

Furthermore the following equality can be derived (see [14]) by induction on $n$:

$$\sum\nolimits_{A \in \mathbf{S}} X(sf(A)) Y^{df(A)} = \sum_{k=0}^{n} \binom{n}{k}_Y X(k), \tag{22}$$

where $\binom{n}{k}_q$ denotes the $q$-*binomial* or *Gaussian* coefficients (see [11]). From Relations (21) and (22) and Theorem 2, we obtain the following:

$$\Pr_{mm}[\phi \text{ is satisfiable}] \leq \left(\frac{7}{8}\right)^{rn} \sum_{k=0}^{n} \sum_{l=k}^{rn} \binom{n}{k}_Y (E(\alpha, \beta, r))^n. \tag{23}$$

We will now consider an arbitrary term of the double sum that appears in (23) and examine for which values of $r$ it converges to 0. If we find a condition on $r$ that forces all such terms to converge to 0, then the whole sum will converge to 0 since it contains polynomially many terms, all of which vanish exponentially fast. This technique, made known to us by D. Achlioptas, avoids the problem of finding a closed-form upper bound for the sum itself. However, in order to handle an arbitrary

term, we need an upper bound for the $q$-binomial coefficients. To establish such a bound we need the following standard result:

LEMMA 2 [19] *Let $f(z) = \sum_{i=0}^{\infty} f_i z^i$ be the generating function for the sequence $f_i$, $i \geq 0$. Then if $f(z)$ is analytic in $|z| < R$ and if $f_i \geq 0$ for all $i \geq 0$, then for any $t$, $0 < t < R$, and any $n \geq 0$, it holds that $f_n \leq t^{-n} f(t)$.*

Using this lemma, we can prove the following:

**Theorem** 4 *Let $\binom{n}{\alpha n}_q$ denote the q-binomial coefficients for $\alpha, q \in (0,1)$. Then the following inequality holds:*

$$\binom{n}{\alpha n}_q \leq 2q^{-\binom{\alpha n}{2}} x_0^{-\alpha n} e^{\frac{1}{\ln q}[\mathrm{dilog}(1+x_0) - \mathrm{dilog}(1+x_0 q^{n-1})]}, \tag{24}$$

*where $x_0 = \frac{1-q^{\alpha n}}{q^{\alpha n} - q^{n-1}}$ and $\mathrm{dilog}(x) = \int_1^x \frac{\ln t}{1-t} dt$.*

Proof. For the ordinary generating function of $q^{\binom{i}{2}}\binom{n}{i}_q$ the following holds [3, p. 118]:

$$\begin{aligned}\sum_{i=0}^{n} q^{\binom{i}{2}} \binom{n}{i}_q x^i &= \prod_{i=1}^{n} (1 + xq^{i-1}) = e^{\sum_{i=1}^{n} \ln(1+xq^{i-1})} \\ &= (1+x) e^{\sum_{i=2}^{n} \ln(1+xq^{i-1})}.\end{aligned}$$

Since $\ln(1 + xq^{i-1})$ is decreasing in $i$,

$$\begin{aligned}\sum_{i=0}^{n} q^{\binom{i}{2}} \binom{n}{i}_q x^i &\leq (1+x) e^{\int_1^n \ln(1+xq^{i-1}) di} \\ &= (1+x) e^{\frac{1}{\ln q}[\mathrm{dilog}(1+x) - \mathrm{dilog}(1+xq^{n-1})]}.\end{aligned}$$

Applying Lemma 2, we have that for all $x \in (0,1)$

$$q^{\binom{i}{2}} \binom{n}{i}_q \leq x^{-i} (1+x) e^{\frac{1}{\ln q}[\mathrm{dilog}(1+x) - \mathrm{dilog}(1+xq^{n-1})]}. \tag{25}$$

The above inequality holds for any value of $x \in (0,1)$. Therefore, we may optimize it by choosing the value $x_0 = \frac{1-q^i}{q^i - q^{n-1}}$ that minimizes the expression on the right-hand side of (25). The required inequality is then obtained by setting $i = \alpha n$. ■

Setting $q = Y = 1 + z/n$ in (24) and using the approximation $\ln(1 + z/n) \sim z/n$, as $n \to \infty$, the following can be derived:

$$\binom{n}{\alpha n}_q \leq 2\left[\left(\frac{1}{x_0}\right)^{\alpha} \cdot e^{-\frac{\alpha^2 z}{2} + \frac{1}{z}[\mathrm{dilog}(1+x_0) - \mathrm{dilog}(1+x_0 e^z)]}\right]^n, \tag{26}$$

where $x_0 = \frac{1-e^{\alpha z}}{e^{\alpha z} - e^z}$, which is expedient in the proof of the following:

**Theorem** 5 *An arbitrary term of the double sum in (23) is asymptotically (ignoring polynomial multiplicative factors) bounded from above by the following expression $F$ raised to $n$:*

$$F = \exp\left[-\alpha(c + \ln(s_0 - 1) - c\ln s_0)\right]\left(\frac{(3\alpha)^{\beta}(7-3\alpha)^{1-\beta}}{8\beta^{\beta}(1-\beta)^{1-\beta}}\right)^r \times \frac{e^{-\frac{\alpha^2 z}{2} + \frac{1}{z}[\mathrm{dilog}(1+x_0) - \mathrm{dilog}(1+x_0 e^z)]}}{{x_0}^{\alpha}},$$

*where, $\alpha = \frac{k}{n}$, $\beta = \frac{l}{rn}$, $x_0 = \frac{1-e^{\alpha z}}{e^{\alpha z} - e^z}$, $z$ as given in (13) and $s_0 = \frac{c}{c + \mathbf{W}(-ce^{-c})}$, with $c = r\frac{\beta}{\alpha}$.*

An immediate consequence of this result is that *any* value of $r$ for which $F$ is smaller than 1 for all $\alpha, \beta$ in the domain $\mathbf{D} = \{\alpha, \beta \in [0,1] \text{ and } \beta r \geq \alpha\}$ is an upper bound for the unsatisfiability threshold. In other words, any value of $r$ for which the maximum of the function $\ln(F)$ over $\mathbf{D}$ is negative is an upper bound for the threshold.

We finally claim that for any value of $r$, the expression $\ln(F)$ is an upwards convex function of $\alpha, \beta$ over the domain $\mathbf{D}$. For a proof of this claim see Appendix B.

Since for any fixed $r$, $\ln(F)$ is upwards convex and continuously differentiable, there is a unique point in $\mathbf{D}$ where $\ln(F)$ attains its maximum, and this point can be computed by setting the partial derivatives of $\ln(F)$ equal to 0. Due to the complicated form of the expression $\ln(F)$, we maximized it numerically over $\mathbf{D}$ for $r = 4.571$ using a Maple [18] implementation of *Downhill Simplex*. This implementation is based on the method and the code described in [20] and it is freely distributed by F.J. Wright in his Web page [22]. Guided by the plot of $\ln(F)$ given by Maple, we chose as a starting set of values for downhill simplex $\alpha = 0.42$ and $\beta = 0.21$. We set the accuracy and the scale parameters equal to $10^{-50}$. In addition, we set the *Digits* parameter of Maple (accuracy of floating point numbers) equal to 100. We ran downhill simplex and it returned as the maximum value of $\ln(F)$ over $\mathbf{D}$ the number $-0.0000884$. We then computed all the partial derivatives of $\ln(F)$ at the point of $\mathbf{D}$ where $\ln(F)$ takes the value $-0.0000884$. They were found to be numerically equal to 0. As a final check, we generated 30000 random points close

to the point of $\mathbf{D}$ where $\ln(F)$ takes the value $-0.0000884$ and we confirmed that at all these points, the value of $\ln(F)$ is not greater than $-0.0000884$. All these considerations show that the maximum of $\ln(F)$ over $\mathbf{D}$ is negative for $r = 4.571$. (For larger values of $r$, the downhill simplex returns a positive maximum.) Thus, the value $r = 4.571$ is established as an upper bound to the unsatisfiability threshold.

## References


[1] D. Achlioptas and G. B. Sorkin, "Optimal Myopic Algorithms for Random 3-SAT" in: *Proc. 41st Annual Symposium on Foundations of Computer Science (FOCS)*, pp 590–600, 2000.

[2] B. Bollobás, *Random Graphs*, Academic Press, London, 1985.

[3] L. Comtet, *Advanced Combinatorics; The Art of Finite and Infinite Expansions*, D. Reidel, 1974.

[4] R.M. Corless, G.H. Gonnet, D.E.G. Hare, D.J. Jeffrey, and D.E. Knuth, "On the Lambert **W** function," *Advances in Computational Mathematics* 5, pp. 329–359, 1996.

[5] O. Dubois and Y. Boufkhad, "A general upper bound for the satisfiability threshold of random $r$-SAT," *J. of Algorithms* 24, pp 395–420, 1997.

[6] O. Dubois, Y. Boufkhad, and J. Mandler, "Typical random 3-SAT formulae and the satisfiability threshold," in: *Proc. 11th Symposium on Discrete Algorithms (SODA)*, pp 126–127, 2000.

[7] O. Dubois, Y. Boufkhad, and J. Mandler, "Typical random 3-SAT formulae and the satisfiability threshold," Electronic Colloquium on Computational Complexity Report TR03-007, Jan 28, 2003.

[8] W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. 1, 3rd ed., 1968.

[9] N.J. Fine, *Basic Hypergeometric Series and Applications*, Mathematical Surveys and Monographs, Number 27, 1980.

[10] E. Friedgut, appendix by J. Bourgain, "Sharp thresholds of graph properties, and the $k$-sat problem," *J. Amer. Math. Soc.* 12, pp 1017–1054, 1999.

[11] G. Gasper and M. Rahman, *Basic Hypergeometric Series*, Encyclopedia of Mathematics and its Applications, vol 35, Cambridge University Press, 1990.

[12] S. Janson, Y.C. Stamatiou, and M. Vamvakari, "Bounding the unsatisfiability threshold of random 3-SAT," *Random Structures and Algorithms* 17, pp 108–116, 2000.

[13] A. Kamath, R. Motwani, K. Palem, and P. Spirakis, "Tail bounds for the occupancy and the satisfiability threshold conjecture," *Random Structures and Algorithms* 7, pp 59–80, 1995.

[14] L.M. Kirousis, E. Kranakis, D. Krizanc, and Y.C. Stamatiou, “Approximating the unsatisfiability threshold of random formulas,” *Random Structures and Algorithms* 12, pp 253–269, 1998.

[15] L.M. Kirousis and Y.C. Stamatiou, *An inequality for reducible, increasing properties of randomly generated words*, Technical Report TR-96.10.34, Computer Technology Institute, University of Patras, Patras Greece, 1996.

[16] D.E. Knuth, *Fundamental Algorithms*, The Art of Computer Programming, 2nd ed., Addison-Wesley, 1973.

[17] V.F. Kolchin, *Random Mappings*, Translation series in Mathematics and Engineering, Optimization Software Inc., 1986.

[18] M.B. Monagan, K.O. Geddes, K.M. Heal, G. Labahn, and S.M. Vorkoetter, *Programming Guide*, Maple V Release 5, Springer-Verlag, 1998.

[19] A.M. Odlyzko, “Asymptotic Enumeration Methods,” in: R.L. Graham, M. Grötschel, and L. Lovász, eds. *Handbook of Combinatorics*, Chapter 22, pp. 1063–1229, Elsevier, 1995.

[20] W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery, *Numerical Recipes in C: The Art of Scientific Computing*, 2nd ed., Cambridge University Press, 1993.

[21] A.E. Taylor and W.R Mann, *Advanced Calculus*, 3rd ed., John Wiley & Sons, 1983.

[22] F.J. Wright: `http://centaur.maths.qmw.ac.uk/Computer_Algebra/`. A Maple (V-5) implementation of *Downhill Simplex* based on code given in [20].

[23] M. Zito, Randomised Techniques in Combinatorial Algorithmics, PhD Thesis, Department of Computer Science, University of Warwick, November 1999.

## Appendix A

Proof of Theorem 3. We first show that there exists $p' = (6r')/(7n^2) < p = (6r)/(7n^2)$, such that:

$$\mathrm{E}_{p'}[|\phi| \mid A \in \mathbf{A}_n^1] = rn.$$

Fix $A$ (containing $\alpha n$ FALSE values). As we have seen in Section 3, the blocking clauses of $A$ have cardinality $\alpha n\binom{n-1}{2}$. We call the remaining $7\binom{n}{3} - \alpha n\binom{n-1}{2}$ clauses *non-blocking*. We shall now compute $\mathrm{E}_{p'}[|\phi| \mid A \in \mathbf{A}_n^1]$, as if the value of $p'$ (or equivalently $r'$) was known. We work in the model $G_{p'}$. For a non-blocking clause $c$, the event that it is contained in the random formula is independent from the event $A \in \mathbf{A}_n^1$. This is so because we work in a model where for each clause it is independently decided to be included in the formula and moreover the conditional $A \in \mathbf{A}_n^1$ does not involve non-blocking clauses. So the expected number of non-blocking clauses in $\phi$, conditional on $A \in \mathbf{A}_n^1$, equals:

$$\left(7\binom{n}{3} - \alpha n\binom{n-1}{2}\right)\frac{6r'}{7n^2} \sim \frac{7-3\alpha}{7}r'n \tag{27}$$

An arbitrary blocking clause $c$ has probability to be selected that equals:

$$\mathrm{Pr}_{p'}[c \in \phi \mid A \in \mathbf{A}_n^1] = \frac{\mathrm{Pr}_{p'}[c \in \phi]\mathrm{Pr}_{p'}[A \in \mathbf{A}_n^1 \mid c \in \phi]}{\mathrm{Pr}_{p'}[A \in \mathbf{A}_n^1]}. \tag{28}$$

In [14] it was shown that:

$$\mathrm{Pr}_{p'}[A \in \mathbf{A}_n^1] \sim (1 - e^{-\frac{3r'}{7}})^{\alpha n}. \tag{29}$$

Since each blocking clause $c$ forces exactly one single flip of $A$ to falsify $\phi$ and since there are totally $\alpha n$ single flips we obtain:

$$\mathrm{Pr}_{p'}[A \in \mathbf{A}_n^1 \mid c \in \phi] \sim (1 - e^{-\frac{3r'}{7}})^{\alpha n - 1}. \tag{30}$$

From (29) and (30), Equation (28) becomes:

$$\mathrm{Pr}_{p'}[c \in \phi \mid A \in \mathbf{A}_n^1] \sim \frac{6r'}{7n^2}(1 - e^{-\frac{3r'}{7}})^{-1}. \tag{31}$$

So the expected number of blocking clauses in $\phi$, conditional on $A \in \mathbf{A}_n^1$, is:

$$\alpha n\binom{n-1}{2}\mathrm{Pr}_{p'}[c \in \phi \mid A \in \mathbf{A}_n^1] \sim \frac{3\alpha}{7}(1 - e^{-\frac{3r'}{7}})^{-1}r'n. \tag{32}$$

From (27) and (32) we conclude:

$$\mathrm{E}_{p'}[|\phi| \mid A \in \mathbf{A}_n^1] \sim \left(1 + \frac{3\alpha}{7(e^{3r'/7} - 1)}\right) r'n. \tag{33}$$

We want to find $r'$ such that for $p' = (6r')/7n^2), \mathrm{E}_{p'}[|\phi| \mid A \in \mathbf{A}_n^1] = rn$. By (33), $r'$ must satisfy:

$$r = r'\left(\frac{3\alpha}{7(e^{3r'/7} - 1)} + 1\right). \tag{34}$$

It is easy to see that the last relation uniquely defines $r' < r$.

Next we show that for $p' = (6r')/(7n^2)$, where $r'$ is implicitly given by (34), we have that $\Pr_{p'}[|\phi| = rn \ \ |A \in \mathbf{A}_n^1] \asymp 1$. By the remarks preceding the statement of Theorem 3, this will complete its proof. The basic idea to show this is the following: it suffices to show that the probability distribution of $|\phi|$ in $G_{p'}$ is, in some sense, sharply concentrated on its mean. To show the later it suffices to show that $\Pr_{p'}[|\phi| = i \ \ |A \in \mathbf{A}_n^1] \asymp 1$, where $i$ is a variable, can be expressed as an exponential function in $n$ whose base is a function of $i$ *with a unique maximum*. As this maximum then has to be 1, in order to have that the polynomially many possible values for $i$ have probabilities that add up to 1, and as all other bases have to be less than 1, the sharp concentration follows. Actually, we will prove that $\Pr_{p'}[|\phi| = i \ \ |A \in \mathbf{A}_n^1] \asymp 1$ is not an exponential function, but a sum of exponential functions instead. This does not change the essence of our argument. We formalize this argument below.

Fix $r'$ (recall that $A$ is also fixed and has $k = \alpha n$ FALSE values). Let $\gamma > 0$ be a parameter and let $i = \gamma n$. We start by computing $\Pr_{p'}[|\phi| = i \ |A \in \mathbf{A}_n^1]$:

$$\begin{aligned}
&\Pr_{p'}[|\phi| = i \ |A \in \mathbf{A}_n^1] \\
&= \frac{\Pr_{p'}[|\phi| = i \ \wedge A \in \mathbf{A}_n^1]\Pr_{p'}[|\phi| = i]}{\Pr_{p'}[|\phi| = i]\Pr_{p'}[A \in \mathbf{A}_n^1]} \\
&= \frac{\Pr_{p'}[A \in \mathbf{A}_n^1 \mid |\phi| = i]\Pr_{p'}[|\phi| = i]}{\Pr_{p'}[A \in \mathbf{A}_n^1]} \\
&= \frac{\Pr_{i}[A \in \mathbf{A}_n^1]\Pr_{p'}[|\phi| = i]}{\Pr_{p'}[A \in \mathbf{A}_n^1]}
\end{aligned} \tag{35}$$

The probabilities with subscript $p'$ are in the variable formula-length model, while the ones with subscript $i$ are in the fixed formula-length model without repetitions. It is easy to see that for some function $G_1(\gamma)$, such that $\ln(G_1(\gamma))$ is upwards convex, $\Pr_{p'}[|\phi| = i] \sim (G_1(\gamma))^n$ . Also, for some constant $C$ (depending on $r'$ and

$A$), $\Pr_{p'}[A \in \mathbf{A}_n^1] \sim C^n$ (see Relation (29) above). Finally, by Theorem 2 and from the equivalence of the models $G_{mm}$ and $G_m$ that we established in Section 4, we conclude that if we let $G_2(\beta, \gamma) = E(\alpha, \beta, \gamma)$ ($\alpha$ is fixed), then:

$$\Pr_i[A \in \mathbf{A}_n^1] \asymp \sum_{l=k}^{i} (G_2(\beta, \gamma))^n ,$$

where $\gamma = i/n$, $\beta = l/i$ and $\alpha = k/n$. By directly computing its Hessian, as we do in the next Appendix for the function $\ln(E(r, \alpha, \beta)$, but in terms of the variables $\alpha$ and $\beta$, we can show that $\ln(G_2(\beta, \gamma))$ is upwards convex. Also, obviously there is a large enough constant $M$ such that

$$\sum_{i=0}^{Mn} \Pr_{p'}[|\phi| = i \,|A \in \mathbf{A}_n^1] \sim 1.$$

Putting everything together, we conclude that there is a function $G(\beta, \gamma)$, where $\ln(G(\beta, \gamma))$ is upwards convex and such that:

$$\sum_{i=0}^{Mn} \Pr_{p'}[|\phi| = i \,|A \in \mathbf{A}_n^1] \asymp \sum_{i=0}^{Mn} \sum_{l=k}^{i} (G(\beta, \gamma))^n \asymp 1.$$

We can immediately conclude that there are values of $\beta$ and $\gamma$ such that $G(\beta, \gamma) = 1$ (otherwise we would have that polynomially many functions that are exponentially zero sum up to 1). But because $\ln(G)$ is convex, $G$ has a unique maximum, so the values of $\beta$ and $\gamma$ are unique. Therefore there is a unique $\gamma = i/n$ such that

$$\Pr_{p'}[|\phi| = i \,|A \in \mathbf{A}_n^1] \asymp \sum_{l=k}^{i} (G(\beta, \gamma))^n \asymp 1.$$

But then we should have $\gamma = r$, otherwise we would contradict the fact that

$$\mathrm{E}_{p'}[|\phi| \mid A \in \mathbf{A}_n^1] \sim rn.$$

■

**Appendix B**

We establish the upwards convexity of $\ln(F)$ for a any fixed $r$ over the domain $\mathbf{D} = \{\alpha, \beta \in [0, 1] \text{ and } \frac{\beta r}{\alpha} \geq 1\}$.

$$\begin{aligned}\ln(F) = &- \alpha(c + \ln(s_0 - 1) - c \ln s_0) \\ &- \beta r \ln \beta - (1 - \beta) r \ln(1 - \beta) + \beta r \ln(3\alpha) - r \ln 8 + r(1 - \beta) \ln(7 - 3\alpha)\end{aligned}$$

$$+\alpha \ln \frac{1}{x_0} - \alpha^2 \frac{z}{2} + \frac{1}{z}[\mathrm{dilog}(1+x_0) - \mathrm{dilog}(1+x_0 e^z)].$$

**A.** The expression $-\beta r \ln \beta - (1-\beta) r \ln(1-\beta) + \beta r \ln(3\alpha) - r \ln 8 + r(1-\beta)\ln(7-3\alpha)$ is an upwards convex function of $\alpha, \beta$. Indeed, the quadratic form of its Hessian (see e.g. [21]) computed at an arbitrary vector $(\alpha', \beta') \in \mathbf{R}^2$ is:

$$\begin{aligned}
&-(\alpha')^2 r \left[\frac{\beta}{\alpha^2} + \frac{9(1-\beta)}{(7-3\alpha)^2}\right] + 2\alpha'\beta' r \left[\frac{1}{\alpha} + \frac{3}{7-3\alpha}\right] - (\beta')^2 r \left[\frac{1}{\beta} + \frac{1}{1-\beta}\right] \\
&= -(\alpha')^2 r \left[\frac{\beta(7-3\alpha)^2 + 9(1-\beta)r}{\alpha^2(7-3\alpha)^2}\right] + 2\alpha'\beta' r \left[\frac{7}{\alpha(7-3\alpha)}\right] - (\beta')^2 r \left[\frac{1}{\beta(1-\beta)}\right] \\
&\leq -(\alpha')^2 r \left[\frac{\beta(7-3\alpha)^2 + 9(1-\beta)r}{\alpha^2(7-3\alpha)^2}\right] + 2\alpha'\beta' r \left[\frac{\sqrt{\beta(7-3\alpha)^2 + 9(1-\beta)\alpha^2}}{\alpha(7-3\alpha)\sqrt{\beta(1-\beta)}}\right] \\
&-(\beta')^2 r \left[\frac{1}{\beta(1-\beta)}\right] \\
&= -\left[\alpha' \sqrt{r\frac{\beta(7-3\alpha)^2 + 9(1-\beta)r}{\alpha^2(7-3\alpha)^2}} - \beta' \sqrt{r\frac{1}{\beta(1-\beta)}}\right]^2.
\end{aligned}$$

Therefore, the Hessian is negative semi-definite and so the function $-\beta r \ln \beta - (1-\beta) r \ln(1-\beta) + \beta r \ln(3\alpha) - r \ln 8 + r(1-\beta)\ln(7-3\alpha)$ is upwards convex.

**B.** The expression $\alpha \ln \frac{1}{x_0} - \alpha^2 \frac{z}{2} + \frac{1}{z}[\mathrm{dilog}(1+x_0) - \mathrm{dilog}(1+x_0 e^z)]$, where $x_0 = \frac{1-e^{\alpha z}}{e^{\alpha z} - e^z}$, $z < 0$, is an upwards convex function of $\alpha, \beta$. Indeed, first observe that it is actually a function of $\alpha$ alone since for fixed $r$, $z$ is constant (recall its definition in the beginning of Section 5) and $x_0$ depends only on $\alpha$. Therefore, the quadratic form of its Hessian computed at an arbitrary $(\alpha', \beta') \in \mathbf{R}^2$ is: $z\left[-\frac{(e^z-1)e^{\alpha z}}{(1-e^{\alpha z})(e^{\alpha z}-e^z)} - 1\right](\alpha')^2$. Since $z < 0$, in order to show that the last expression is non-positive it suffices to show that $\frac{(e^z-1)e^{\alpha z}}{(1-e^{\alpha z})(e^{\alpha z}-e^z)} < -1$. Since $(1-e^{\alpha z})(e^{\alpha z} - e^z) > 0$, it is sufficient to show that $(e^z - 1)e^{\alpha z} < -(1-e^{\alpha z})(e^{\alpha z} - e^z) \Leftrightarrow e^z - 2e^{\alpha z}e^z + (e^{\alpha z})^2 > 0$. But the last inequality holds, since $e^z - 2e^{\alpha z}e^z + (e^{\alpha z})^2 > (e^z)^2 - 2e^{\alpha z}e^z + (e^{\alpha z})^2 = (e^z - e^{\alpha z})^2 > 0$.

**C.** Finally, let us consider the expression $M = -\alpha(c + \ln(s_0 - 1) - c \ln s_0)$ as a function of $\alpha, \beta$. The quadratic form of its Hessian computed at an arbitrary vector $(\alpha', \beta') \in \mathbf{R}^2$ is:

$$\frac{\beta r e^{-\beta r/(\alpha s_0)}}{e^{-\beta r/(\alpha s_0)} - \alpha/(\beta r)} \left[\frac{\alpha'}{\alpha} - \frac{\beta'}{\beta}\right]^2. \tag{36}$$

We prove (36) by the following steps: Using that $\ln(s_0 - 1) = \ln s_0 - \frac{c}{s_0}$, $c = \frac{\beta r}{\alpha}$ and $s_0(1 - e^{-c/s_0}) = 1$, we first obtain:

$$M = -r\beta - \alpha \ln s_0 + \frac{r\beta}{s_0} + r\beta \ln s_0. \tag{37}$$

Setting in Expression (37), $s_0 = \frac{c}{x^*}$, where $x^*$ is an arbitrary positive variable, we then obtain:

$$M = -r\beta - \alpha \ln \frac{r\beta}{\alpha} + \alpha \ln x^* + \alpha x^* + r\beta \ln \frac{r\beta}{\alpha} - r\beta \ln x^*. \tag{38}$$

Notice now that:

$$s_0(1 - e^{-c/s_0}) = 1 \Leftrightarrow 1 - e^{-x^*} - \frac{\alpha}{r\beta} x^* = 0 \Leftrightarrow \frac{\alpha e^{x^*}}{e^{x^*} - 1} = \frac{r\beta}{x^*}. \tag{39}$$

Therefore the partial derivatives of Expression (38) are given by:

$$\frac{\partial M}{\partial \alpha} = x^* + \ln x^* + \ln \alpha - \frac{r\beta}{\alpha} - \ln r\beta, \qquad \frac{\partial M}{\partial \beta} = r \ln r\beta - r \ln \alpha - r \ln x^* \cdot$$

$$\frac{\partial^2 M}{\partial \alpha^2} = \frac{x^*+1}{x^*} \frac{\partial x^*}{\partial \alpha} + \frac{1}{\alpha} + \frac{r\beta}{\alpha^2}, \quad \frac{\partial^2 M}{\partial \beta^2} = -\frac{r}{x^*} \frac{\partial x^*}{\partial \beta} + \frac{r}{\beta}, \quad \frac{\partial^2 M}{\partial \alpha \partial \beta} = -\frac{r}{x^*} \frac{\partial x^*}{\partial \alpha} - \frac{r}{\alpha}.$$

We then use once more Expression (39) in order to obtain:

$$\frac{\partial x^*}{\partial \alpha} = \frac{x^*}{r\beta} \frac{1}{e^{-x^*} - \alpha/(r\beta)}, \qquad \frac{\partial x^*}{\partial \beta} = -\frac{\alpha x^*}{r\beta^2} \frac{1}{e^{-x^*} - \alpha/(r\beta)}.$$

Using the partial derivatives above, we conclude that (36) holds.

Now using (39) again, we observe that

$$e^{-\beta r/(\alpha s_0)} - \frac{\alpha}{\beta r} = e^{-x^*} - \frac{\alpha}{\beta r} = \frac{1 + x^* - e^{x^*}}{x^* e^{x^*}} < 0,$$

since $1 + x^* < e^{x^*}$. Therefore, expression (36) is non-positive and the proof of the upwards convexity of $\ln(F)$ over $\mathbf{D}$ is complete.