What is the satisfiability threshold of random balanced Boolean expressions?

Naomi Lindenstrauss[1] and Michel Talagrand[2]

Abstract

We consider the model of random Boolean expressions based on balanced binary trees with 2^N leaves, to which are randomly attributed one of k_N Boolean variables or their negations. We prove that if for every $c > 0$ it holds that $k_N \exp(-c\sqrt{N}) \to 0$ then asymptotically with high probability the Boolean expression is either a tautology or an antitautology. Our methods are based on the study of a certain binary operation on the set of probability measures on $\{0,1\}^I$ for a finite set I.

1 Introduction

A Boolean variable is a Boolean expression. The negation of a Boolean variable is a Boolean expression. If A and B are Boolean expressions, then $\mathrm{and}(A,B)$ and $\mathrm{or}(A,B)$ are Boolean expressions. We find it convenient to think of a Boolean variable as taking the values 0 (=false) or 1 (=true). The negation of a Boolean variable x then takes the value $1-x$. When the Boolean variables in a Boolean expression are assigned values, this Boolean expression is assigned a value $\in \{0,1\}$, by the rules $\mathrm{and}(a,b) = ab$ and $\mathrm{or}(a,b) = a+b-ab$ for $a,b \in \{0,1\}$. Thus a Boolean expression of at most k Boolean variables defines a function on $\{0,1\}^k$. The Boolean expression is called a *tautology* if this function is identically equal to 1; an *antitautology* if this function is identically zero; and it is said to be *satisfiable* if it is not an antitautology, that is, if it is not identically 0. It is helpful to picture a Boolean expression as a binary tree such that a connective "and" or "or" is attached to each internal node of the tree, and such that to each leaf of the tree is attached either a Boolean variable or its negation.

It is natural to wonder what is a "typical" Boolean expression, and for this it is natural to introduce models of "random Boolean expressions", a kind of consideration that goes back to at least [L-S]. Such a model involves a random binary tree,

[1]The Hebrew University of Jerusalem, naomi.lind@gmail.com
[2]Paris, France, michel.talagrand@gmail.com

a random choice of the "and" and "or" connectives at the internal nodes of the tree and a random choice of the variables/negation of variables at the leaves of the tree. The most natural choice for the connectives is to choose independently at each of the internal nodes of the tree "and" and "or" respectively with probabilities p and $1-p$, where $0 < p < 1$ is a given parameter. The most interesting (and difficult) case is $p = 1/2$, to which most of the paper is devoted, the case $p \neq 1/2$ being considered in the last section. The most natural choice of the variables is to assign at random one of k given Boolean variables or their negation at each leaf of the tree. On the other hand there are several natural choices for the notions of random tree. The most popular are the Catalan model (where every binary tree with N leaves is given an equal weight, and which is studied among other papers in [G-M]) and the Galton-Watson model. Other models have also been considered such as in [C-G-M]. A large part of the existing literature focuses on the case where the number of Boolean variables remains fixed and where the size of the tree increases, and pretty complete results exist in this direction.

We will consider the model of random Boolean expressions where the underlying tree is the balanced binary tree where each branch has length N, so that there are 2^N leaves.[3] To make absolutely clear what is our model, and to prepare the reader for the basic construction introduced in Section 3.2, we provide an alternate description. The model depends on two integers N and k. Here k is the number of different Boolean variables, and the number N is called the *order* of the Boolean expression. A random Boolean expression of order $N = 0$ is just a one of the k Boolean variables or its negation, all $2k$ choices having equal probability. Having defined what is a random Boolean expression of order $N-1$, we define a random Boolean expression of order N as follows. First we define the connective "rand" to be either "and" with probability p or "or", with probability $1-p$. Consider then probabilistically independent random Boolean expressions A, B of order $N-1$, that are also probabilistically independent of the connective rand. The random Boolean expression of order N is then $\mathrm{rand}(A, B)$.

Until further notice we assume that $p = 1/2$. We use synthetic notation and denote simply by $\mathsf{P}(\mathit{tautology})$ the probability that the random Boolean expression of order N and k variables is a tautology (here, as often, the notation does not indicate the values of N and k when they are clear from the context). Since $p = 1/2$, by symmetry we have

$$\mathsf{P}(\mathit{tautology}) = \mathsf{P}(\mathit{antitautology}) \ . \tag{1.1}$$

The quantity

$$\mathsf{P}(\mathit{constant}) = \mathsf{P}(\mathit{tautology}) + \mathsf{P}(\mathit{antitautology}) \tag{1.2}$$

[3]There does not seem to be many papers in the literature studying balanced trees. One of the earliest such papers is [F-G-G] , which studies a slightly different model.

is the probability that the function computed by the Boolean formula is a constant. We expect that for large values of N and generic values of k the quantity $\mathsf{P}(\textit{constant})$ will be either close to zero or close to 1, and the difficult problem is to determine which of the two possibilities occurs for given values of N and k. For example it follows from a more general result proved in [B-M] that when k is fixed and $N \to \infty$ the quantity (1.2) goes to 1.

In view of the result of [B-M] it is natural to consider the case where $k = k_N$ goes to infinity with N. We expect that if k_N goes to infinity too slowly, we will have $\mathsf{P}(\textit{constant}) \to 1$ while if it goes to infinity fast enough then $\mathsf{P}(\textit{constant}) \to 0$.

Theorem 1.1 *Consider the model where the binary tree underlying the Boolean expression is the balanced binary tree with 2^N leaves, and where for each leaf we choose at random among k_N different Boolean variables or their negations. Then:*
(a) If for every $c > 0$ it holds that $k_N \exp(-c\sqrt{N}) \to 0$, then $\mathsf{P}(\textit{constant}) \to 1$.
(b) For a certain numerical constant d if it holds that $k_N \exp(-d\sqrt{N}) \to \infty$, then $\mathsf{P}(\textit{constant}) \to 0$.

The weakness of this result is the considerable gap between the rate $\exp(o(\sqrt{N}))$ of (a) and the rate $\exp(d\sqrt{N})$ of (b).

Problem 1.2 *What happens when $k_N \exp(-c\sqrt{N}) \to 1$ where $c > 0$ is very small? And where is the true threshold?*

More precisely, based on what often happens (as e.g. in the famous k-SAT problem, see [CO-P]), we expect that there exists a sequence (r_N) such that if $k_N/r_N \to 0$, then as $N \to \infty$, we have $\mathsf{P}(\textit{constant}) \to 1$, whereas if $k_N/r_N \to \infty$, then, as $N \to \infty$, we have $\mathsf{P}(\textit{constant}) \to 0$. Our methods are powerless to make progress in this direction, but it seems reasonable to believe that this is a very difficult problem.

The main contribution of the present paper is the technique by which we obtain (a). This technique is far more efficient than the moment computations that have been used in the literature. (The result obtained by these moment computations would require k_N not to grow faster than $\log N$ in (a).)

2 Proof of Theorem 1.1, (b)

If we are lucky enough that the binary tree underlying the random Boolean expression has a branch with "or" at every node, the expression is very easy to satisfy, by assigning the correct value to the Boolean variable corresponding to the leaf at the end of the branch. Unfortunately it is well known that the probability p_N that such a

branch exists in a binary tree of height N goes to zero as $N \to \infty$. This is rather obvious if one notices the recurrence relation $p_{N+1} = (1/2)(1-(1-p_N)^2) = p_N-(1/2)p_N^2$, so that the sequence (p_N) decreases to 0.

The following notion offers a generalization of the idea of a branch with "or" at every node.

Definition 2.1 *A subset C of a "and" and "or" tree satisfies property $\mathcal{D}$ if the following occur:*

- *It contains the root.*
- *When it contains an "and" inner node it contains both children.*
- *When it contains an "or" inner node it contains at least one child.*

The following lemma is basically obvious by induction over N.

Lemma 2.2 *Assume that there exists a subset C of the binary tree with property $\mathcal{D}$ such that to each leaf in C corresponds a different Boolean variable.*[4] *Then the Boolean expression is satisfiable.*

Let us set $a = \pi^2/3$. Then it is proved in [A-C] (in a somewhat different language) that as $N \to \infty$ the probability that there exists a set with property $\mathcal{D}$ and at most $\exp(\sqrt{aN})$ leaves goes to 1. As a consequence of this result and of Lemma 2.2, a random Boolean expression will be satisfiable with probability close to 1 provided k_N is large enough that with probability close to 1, the Boolean variables assigned to a given set of $Q_N = \lfloor \exp(\sqrt{aN}) \rfloor$ leaves are all different. This probability is $(1 - 1/k_N)(1 - 2/k_N) \dots (1 - (Q_N - 1)/k_N)$. Using that $(1 - x) \geq \exp(-2x)$ for $x \leq 1/2$, it is elementary that this probability goes to 1 when $k_N/Q_N^2 \to \infty$, so that then the random Boolean expression will be satisfiable with probability $\to 1$ i.e. $\mathsf{P}(\textit{antitautology}) \to 0$. By symmetry $\mathsf{P}(\textit{tautology}) \to 0$ so that $\mathsf{P}(\textit{constant}) \to 0$.

In summary if $k_N \exp(-2\sqrt{aN}) \to \infty$, then $\mathsf{P}(\textit{constant}) \to 0$ as $N \to \infty$ and (b) of Theorem 1.1 is proved.

3 Measure Theory

3.1 Introduction

To approach Theorem 1.1 (a) we think of the set of assignments of the Boolean variables that satisfy the random Boolean expression as a random subset of the set of all assignments. It is then natural to be interested in the law of this random

[4] Here a Boolean variable and its negation are considered as the same variable.

subset. To be more specific, the set of all assignments of the k Boolean variables can be thought of as $\{0,1\}^k$. It will be fruitful to *forget* about the special structure of this set and to think of it as simply a finite set I. Given such a set I, we identify the set of subsets of I with $\{0,1\}^I$ in the usual manner: a point $t=(t_i)_{i\in I}\in\{0,1\}^I$ is identified with the set $\{i\in I; t_i=1\}$. For example, if $I=\{a,b\}$ the set $\{0,1\}^I$ has four elements $\{0,0\},\{0,1\},\{1,0\},\{1,1\}$ corresponding to the subsets $\emptyset,\{b\},\{a\},\{a,b\}$ of I. The set of all assignments of the k Boolean variables that satisfy the random Boolean expression is then a random subset of I, that is a random point of $\{0,1\}^I$. It is natural to consider the law of this set, a certain probability measure on $\{0,1\}^I$.

3.2 Basic definitions

In the next two pages or so, we provide some natural definitions pertaining to probability measures on $\{0,1\}^I$. After stating these we relate these definitions to our original problem. One should keep in mind that, for a probability measure μ on $\{0,1\}^I$, it makes sense to write $\mu(H)$ when $H\subset\{0,1\}^I$ is a *collection* of subsets of I . In particular when $A\subset I$, A is a *point* of $\{0,1\}^I$ and what makes sense is $\mu(\{A\})$, the measure of the collection of subsets of I consisting of A only (but $\mu(B)$ does not make sense for $B\subset I$).

Definition 3.1 *Given two measures μ and μ' (that need not be probabilities or even positive) on $\{0,1\}^I$ we denote by $T^{\cap}(\mu,\mu')$ the image of $\mu\otimes\mu'$ under the map $(A,B)\mapsto A\cap B$ from $\{0,1\}^I\times\{0,1\}^I$ to $\{0,1\}^I$. We denote by $T^{\cup}(\mu,\mu')$ the image of $\mu\otimes\mu'$ under the map $(A,B)\mapsto A\cup B$ from $\{0,1\}^I\times\{0,1\}^I$ to $\{0,1\}^I$. Finally we define*

$$T(\mu,\mu')=\frac{1}{2}\big(T^{\cup}(\mu,\mu')+T^{\cap}(\mu,\mu')\big)\ . \tag{3.1}$$

It is obvious from the definition that $T^{\cap}(\mu,\mu')$ and $T^{\cup}(\mu,\mu')$ are bilinear functions of (μ,μ'). It is only to state this property that we consider measures that need not be positive. From now on, all measures are positive.

Definition 3.2 *We denote $\mathcal{M}$ the set of probability measures μ on $\{0,1\}^I$ such that*

$$\forall i\in I\ ,\ \mu(\{A\subset I\ ;\ i\in A\})=\frac{1}{2}\ .$$

Lemma 3.3 *If $\mu,\mu'\in\mathcal{M}$ then $T(\mu,\mu')\in\mathcal{M}$.*

Proof. Because for $i\in I$ we have

$$\begin{aligned}T^{\cap}(\mu,\mu')(\{C;i\in C\})&=\mu\otimes\mu'(\{(A,B)\ ;\ i\in A\cap B\})\\&=\mu\otimes\mu'(\{(A,B)\ ;\ i\in A, i\in B\})=\mu(\{A;i\in A\})\mu'(\{B;i\in B\})=1/4\ ,\end{aligned}$$

and similary $T^{\cup}(\mu,\mu')(\{C; i \in C\}) = 3/4$. $\square$

Definition 3.4 *Given a probability measure $\mu \in \mathcal{M}$, for $N \geq 0$ we define recursively $\mu^N \in \mathcal{M}$ by $\mu^0 = \mu$ and $\mu^{N+1} = T(\mu^N, \mu^N)$.*

The following "symmetry" property is nearly obvious.

Lemma 3.5 *For $\mu \in \mathcal{M}$ denote by $S(\mu)$ the image of μ under that map $A \mapsto I \setminus A$. Then $S(\mu) \in \mathcal{M}$ and for each N we have $S(\mu)^N = S(\mu^N)$.*

We denote by $|I|$ the cardinality of a finite set I. Our main result is as follows. It will be proved in Section 5.

Theorem 3.6 *There exists a numerical constant $L \geq 6$ with the following property. For any $\mu \in \mathcal{M}$, any integer $N \geq 0$ and any $0 < \beta < 1/2$ such that $\beta\sqrt{N} \geq L$ then we have for any $\alpha > 0$*

$$\mu^N(\{A \subset I; |A| < \alpha\,|I|\}) \geq (1/2 - \beta)\Big(1 - \frac{1}{\alpha \exp(\exp(\beta\sqrt{N}/6))}\Big)\,. \tag{3.2}$$

In particular, taking $\alpha = 1/|I|$ we obtain that for $\beta\sqrt{N} \geq L$ we have

$$\mu^N(\{\emptyset\}) \geq (1/2 - \beta)\Big(1 - \frac{|I|}{\exp(\exp(\beta\sqrt{N}/6))}\Big)\,. \tag{3.3}$$

The following definition will help us to state a striking consequence of this result.

Definition 3.7 *We say that a probability measure μ on $\{0,1\}^I$* concentrates *if $\mu(\{\emptyset\}) + \mu(\{I\}) \geq 3/4$. We define $N(\mu)$ as the smallest integer for which μ^N concentrates.*

The choice of the value $3/4$ is pretty much arbitrary. If we think of μ as the law of a random subset of I, μ concentrates if and only if with probability $\geq 3/4$ the random set is either $\emptyset$ or I. In the sequel, all logarithms are natural.

Proposition 3.8 *There exists a numerical constant L' such that for any $\mu \in \mathcal{M}$ we have $N(\mu) \leq L'(\log\log|I|)^2$ when $|I| \geq 10$.*

Proof. Assume that

$$N \geq 4L^2(\log\log|I|)^2/\beta^2\,. \tag{3.4}$$

Then $\beta\sqrt{N}/L \geq 2\log\log|I|$ and

$$\exp(\beta\sqrt{N}/6) \geq \exp(\beta\sqrt{N}/L) \geq \exp(2\log\log|I|) = (\log|I|)^2 \geq 2\log|I|$$

where we have used in the last inequality that $\log|I| \geq 2$ since $|I| \geq 10$. Therefore

$$\exp(\exp(\beta\sqrt{N}/6)) \geq |I|^2$$

and

$$\frac{|I|}{\exp(\exp(\beta\sqrt{N}/6))} \leq \frac{1}{|I|} \leq \frac{1}{10} \ .$$

Taking $\beta = 1/12$ in (3.3) we then have $\mu^N(\{\emptyset\}) \geq (5/12)(9/10) = 3/8$. Similarly, according to Lemma 3.5 we have $\mu^N(\{I\}) \geq 3/8$. We have proved that $N \geq 4(12)^2L^2(\log\log|I|)^2 \Rightarrow N \geq N(\mu)$. Since $L^2(\log\log|I|)^2 \geq 1$ because $L \geq 6$ and $|I| \geq 10$ it follows that $N(\mu) \leq L'(\log\log|I|)^2$ where $L' = 5(12L)^2$. □

Problem 3.9 *Relate the structure of μ and the number $N(\mu)$.*

It is part of the problem to find a relevant characteristic of μ.

3.3 Link with satisfiability

Let us go back to the case where $I = \{0,1\}^k$, the set of assignments of the k Boolean variables. For $1 \leq \ell \leq k$ and $\epsilon \in \{0,1\}$ consider the subsets V_ℓ^ϵ of I given by

$$V_\ell^\epsilon = \left\{\sigma = (\sigma_a)_{a\leq k} \in \{0,1\}^k \ ; \ \sigma_\ell = \epsilon\right\} \ .$$

Let us denote by $\tilde{\mu}$ the probability measure on $\{0,1\}^I$ that gives mass $1/(2k)$ to each $V_\ell^\epsilon \in \{0,1\}^I$ for $1 \leq \ell \leq k$ and $\epsilon \in \{0,1\}$. Define inductively the measure μ^N by $\mu^0 = \tilde{\mu}$ and $\mu^{N+1} = T(\mu^N, \mu^N)$. The following is basically obvious (using induction over N for the second statement).

Lemma 3.10 *(a) When the random Boolean formula consists of a single Boolean variable (or its negation), the law of the set of assignments that satisfy this formula is $\tilde{\mu}$.*
(b) When the random Boolean formula is of order N, the law of the set of assignments that satisfy this formula is μ^N.

The following is an obvious consequence of (b): when the Boolean formula is of order N then

$$\mathsf{P}(\textit{antitautology}) = \mu^N(\{\emptyset\}) \ ; \ \mathsf{P}(\textit{tautology}) = \mu^N(\{I\}) \ . \tag{3.5}$$

This should make it obvious that Problem 1.2 is closely connected to the problem of determining the smallest integer $N(\tilde{\mu})$ at which μ^N concentrates. Proposition 3.8

yields $N(\tilde{\mu}) \leq L'(\log\log|I|)^2 \leq L'(\log k)^2$. We unfortunately have no improvement to offer on this general bound using the special structure of our situation.

Proof of Theorem 1.1 (a). Combining (3.5) and (3.3), and using that $|I| = |\{0,1\}^{k_N}| = 2^{k_N}$ we obtain that for any $\beta < 1/2$ and N large enough

$$\mathsf{P}(\textit{tautology}) = \mathsf{P}(\textit{antitautology}) \geq (1/2-\beta)(1-2^{k_N}\exp(-\exp(\beta\sqrt{N}/6)) \; .$$

Under the condition that $k_N/\exp(c\sqrt{N}) \to 0$ for any $c > 0$, the right-hand side has a limit $1/2-\beta$, and since $\beta > 0$ is arbitrary, this proves that $\mathsf{P}(\textit{constant}) \to 1$. $\square$

More generally, the meaning of (3.2) is striking: with probability near $1/2$, only a very small proportion of all assignments of the variables satisfy the boolean formula. (Similarly, according to Lemma 3.5, with probability near $1/2$, an overwhelming proportion of all assignments of the variables satisfy the Boolean formula.) Of course, when there are M possible assignments and the proportion of assignments that satisfy the Boolean formula is $< 1/M$ this means that no assignment satisfies it and it is an antitautology.

4 A first decomposition result

For a positive measure ν on $\{0,1\}^I$ we denote by $|\nu|$ its total mass. Thus

$$|T^{\cap}(\nu,\nu')| = |\nu||\nu'| \; ; \; |T^{\cup}(\nu,\nu')| = |\nu||\nu'| \; . \tag{4.1}$$

Let us note the following simple, yet crucial fact.

Lemma 4.1 *For each $i \in I$ we have*

$$T^{\cap}(\nu,\nu')(\{A \subset I; i \in A\}) = \nu(\{A \subset I; i \in A\})\nu'(\{A \subset I; i \in A\}) \; . \tag{4.2}$$

$$T^{\cup}(\nu,\nu')(\{A \subset I; i \in A\}) \leq \nu(\{A \subset I; i \in A\})|\nu'| + |\nu|\nu'(\{A \subset I; i \in A\}) \; . \tag{4.3}$$

Proof. To prove (4.2) we write

$$\begin{aligned} T^{\cap}(\nu,\nu')(\{C \subset I; i \in C\}) &= \nu \otimes \nu'(\{(A,B) \in \{0,1\}^I \times \{0,1\}^I; i \in A \cap B\}) \\ &= \nu \otimes \nu'(\{(A,B) \in \{0,1\}^I \times \{0,1\}^I; i \in A, i \in B\}) \\ &= \nu(\{A \subset I; i \in A\})\nu'(\{A \subset I; i \in A\}) \; . \end{aligned} \tag{4.4}$$

To prove (4.3) we note that

$$T^{\cup}(\nu,\nu')(\{C \subset I; i \in C\}) = \nu \otimes \nu'(\{(A,B) \in \{0,1\}^I \times \{0,1\}^I; i \in A \cup B\})$$

is at most

$$\nu\otimes\nu'(\{(A,B)\in\{0,1\}^I\times\{0,1\}^I; i\in A\})+\nu\otimes\nu'(\{(A,B)\in\{0,1\}^I\times\{0,1\}^I; i\in B\})$$

and that this quantity equals the right-hand side of (4.3). □

Proposition 4.2 *Consider $\mu\in\mathcal{M}$. Assume that we have a decomposition $\mu=\nu+\nu'$ where ν and ν' are positive measures. Then there is a decomposition*

$$T(\mu,\mu)=\lambda+\lambda' \tag{4.5}$$

such that $|\lambda|=|\nu|$ and for each $i\in I$ we have

$$\lambda(\{C\subset I; i\in C\})\le\frac{1}{2}(1+2|\nu|)\nu(\{C\subset I; i\in C\})\ . \tag{4.6}$$

Proof. We define the positive measure λ by

$$2\lambda=T^{\cap}(\nu,\nu)+T^{\cap}(\nu,\nu')+T^{\cap}(\nu',\nu)+T^{\cup}(\nu,\nu)\ . \tag{4.7}$$

(It is true but not helpful that $T^{\cap}(\nu,\nu')=T^{\cap}(\nu',\nu)$.) We note that $|\mu|=1=|\nu|+|\nu'|$ so that

$$2|\lambda|=|\nu|^2+2|\nu||\nu'|+|\nu|^2=2|\nu|(|\nu|+|\nu'|)=2|\nu|$$

and thus $|\lambda|=|\nu|$. Furthermore it is obvious from (3.1) that (4.5) holds for λ' such that

$$2\lambda'=T^{\cap}(\nu',\nu')+T^{\cup}(\nu,\nu')+T^{\cup}(\nu',\nu)+T^{\cup}(\nu',\nu')\ .$$

Next, thinking of i as fixed once and for all, let $\alpha=\nu(\{C\subset I; i\in C\})$ and $\alpha'=\nu'(\{C\subset I; i\in C\})$. Since $\mu\in\mathcal{M}$ we have $1/2=\mu(\{C\subset I; i\in C\})=\alpha+\alpha'$ so that

$$\alpha'=\frac{1}{2}-\alpha\ . \tag{4.8}$$

The idea behind the choice (4.7) is that for each of the pieces θ of this sum we can use (4.2) and (4.3) to control $\theta(\{C\subset I; i\in C\})$, and it follows from these relations that

$$2\lambda(\{C\subset I; i\in C\})\le\alpha^2+2\alpha\alpha'+2\alpha|\nu|$$

and using (4.8) we obtain

$$2\lambda(\{C\subset I; i\in C\})\le\alpha^2+2\alpha(1/2-\alpha)+2\alpha|\nu|\le\alpha(1+2|\nu|)\ .$$

□

Corollary 4.3 *Consider a measure $\mu \in \mathcal{M}$. Define recursively $\mu^0 = \mu$ and $\mu^{N+1} = T(\mu^N, \mu^N)$. Consider any $0 < \beta < 1/2$. Then we can write*

$$\mu^N = \lambda_N + \lambda'_N \; . \tag{4.9}$$

where λ_N and λ'_N are positive measures with $|\lambda_N| = 1/2 - \beta$ and

$$\forall i \in I \; , \; \lambda_N(\{C \subset I; i \in C\}) \leq \exp(-\beta N)|\lambda_N| \; . \tag{4.10}$$

Proof. The proof is by induction over N. For $N = 0$ it suffices to take $\lambda_0 = (1/2 - \beta)\mu$. For the induction step from N to $N+1$ we use Proposition 4.2 and $(1 + 2|\lambda_N|)/2 = 1 - \beta \leq \exp(-\beta)$. □

5 Proof of Theorem 3.6

Let us start with an elementary fact.

Lemma 5.1 *Consider an integer $q \geq 2$. Consider numbers $(a_\ell)_{1 \leq \ell \leq q}$ with $a_\ell \geq 0$ and $\sum_{1 \leq \ell \leq q} a_\ell \leq 1$. We define $a_{1,\ell} = a_\ell$. For $N \geq 1$ and $1 \leq s \leq q$ we define $a_{N,s}$ by the formulas*

$$a_{N+1,1} = a_{N,1} - \frac{a_{N,1}^2}{2} \; ,$$

$$1 < s < q \Rightarrow a_{N+1,s} = a_{N,s} + \frac{a_{N,s-1}^2}{2} - \frac{a_{N,s}^2}{2}$$

$$a_{N+1,q} = a_{N,q} + \frac{a_{N,q-1}^2}{2} \; .$$

Then for each $1 \leq s \leq q-1$ and each $N \geq 1$ we have

$$a_{N,s} \leq \frac{2s}{N} \; . \tag{5.1}$$

Proof. The proof is going to be a double induction. The important fact is the trivial inequality

$$\frac{1}{N} - \frac{1}{N^2} \leq \frac{1}{N+1} \; . \tag{5.2}$$

Let us first observe that it is obvious to prove by induction that $\sum_{1 \leq s \leq q} a_{N,s} = \sum_{1 \leq s \leq q} a_\ell \leq 1$ and that $a_{N,s} \geq 0$.

Let us first prove that (5.1) holds for $s = 1$. For $N \leq 2$ this is because $a_{N,1} \leq 1 \leq 2/N$. For $N \geq 2$ we proceed by induction over N, using that $2/N \leq 1$ and that

the function $x - x^2/2$ is increasing for $x \leq 1$. The induction step is immediate from (5.2).

Let us now assume that (5.1) had been proved for a given $s < q-1$ and all N. We then prove that it holds for $s+1$ and all N. For $N \leq 2(s+1)$ this is obvious since $a_{s+1,N} \leq 1$. For $N \geq 2(s+1)$ we proceed by induction over N, using again that the function $x - x^2/2$ is increasing for $x \leq 1$ and that $2(s+1)/N \leq 1$. We have

$$a_{N+1,s+1} = a_{N,s+1} + \frac{a_{N,s}^2}{2} - \frac{a_{N,s+1}^2}{2} \leq \frac{2(s+1)}{N} + \frac{2s^2}{N^2} - \frac{2(s+1)^2}{N^2},$$

and since $2s^2 - 2(s+1)^2 \leq -2(s+1)$ the right-hand side is $\leq 2(s+1)/(N+1)$ by (5.2). □

Let us explain right away how we will use this.

Corollary 5.2 *We have*

$$a_{N,q} \geq \sum_{1 \leq \ell \leq q} a_\ell - q^2/N \; . \tag{5.3}$$

Proof. As we already observed we have $\sum_{1 \leq \ell \leq q} a_{N,\ell} = \sum_{1 \leq \ell \leq q} a_\ell$, and by (5.1) we have $\sum_{1 \leq \ell < q} a_{N,\ell} \leq \sum_{1 \leq \ell < q} 2\ell/N = q(q-1)/N \leq q^2/N$. □

Let us now introduce some notation. Given a number $0 < a < 1$, for $\ell \geq 0$ we define $H(a,\ell)$ as follows: $H(a,0) = 1$, $H(a,1) = a$ and $H(a,\ell+1) = H(a,\ell)^2$, so that for $\ell \geq 1$ we have $H(a,\ell) = a^{2^{\ell-1}}$.

Let us now state our main technical construction.

Proposition 5.3 *Consider $\mu \in \mathcal{M}$, an integer $q \geq 2$ and a number $0 < a < 1$. Assume that we have a decomposition*

$$\mu = \sum_{0 \leq \ell \leq q} \nu_\ell \tag{5.4}$$

where ν_ℓ is a positive measure with the following property:

$$\forall \ell \leq q \; , \; \forall i \in I \; , \; \nu_\ell(\{A \subset I; i \in A\}) \leq H(a,\ell)|\nu_\ell| \; . \tag{5.5}$$

Then we have a decomposition

$$T(\mu,\mu) = \sum_{0 \leq \ell \leq q} \lambda_\ell \tag{5.6}$$

where the λ_ℓ are positive measures that satisfy the following property

$$\forall \ell \leq q \; , \; \forall i \in I \; , \; \lambda_\ell(\{A \subset I; i \in A\}) \leq 2H(a,\ell)|\lambda_\ell| \; . \tag{5.7}$$

Moreover we have

$$|\lambda_0| = |\nu_0| \; ; \; |\lambda_1| = |\nu_1| - |\nu_1|^2/2 \; ; \; |\lambda_q| = |\nu_q| + |\nu_{q-1}|^2/2 \tag{5.8}$$

and for $1 < s < q$ *we have*

$$|\lambda_s| = |\nu_s| + |\nu_{s-1}|^2/2 - |\nu_s|^2/2 \; . \tag{5.9}$$

Proof. We have

$$2T(\mu,\mu) = \sum_{0\le\ell,\ell'\le q} T^{\cap}(\nu_\ell,\nu_{\ell'}) + \sum_{0\le\ell,\ell'\le q} T^{\cup}(\nu_\ell,\nu_{\ell'}) \; , \tag{5.10}$$

and we are going to define each of the measures $2\lambda_\ell$ as a sum of a suitable subset of these $2(q+1)^2$ terms, using each term exactly once. The difficulty is to satisfy the condition (5.7). The larger ℓ, the more stringent is this definition. For $\ell = 0$, this condition is the easiest to satisfy, and each of the terms in the right-hand side of (5.10) satisfies it. For this reason we will define λ_0 last, as the sum of all the terms that we cannot handle otherwise. We define

$$2\lambda_1 = T^{\cap}(\nu_1,\nu_0)+T^{\cap}(\nu_0,\nu_1)+T^{\cup}(\nu_1,\nu_1)+\sum_{2\le\ell\le q} T^{\cup}(\nu_\ell,\nu_1)+\sum_{2\le\ell\le q} T^{\cup}(\nu_1,\nu_\ell) \; . \tag{5.11}$$

Thus

$$2|\lambda_1| = 2|\nu_1||\nu_0| + |\nu_1|^2 + 2|\nu_1| \sum_{2\le\ell\le q} |\nu_\ell| = 2|\nu_1|\Big(\sum_{0\le\ell\le q} |\nu_\ell|\Big) - |\nu_1|^2 = 2|\nu_1| - |\nu_1|^2 \; .$$

Now (5.11) exhibits λ_1 as a sum $\sum_n \lambda_{1,n}$, so that to proves (5.7) for $\ell = 1$ it suffices to use Lemma 4.1 and (5.5) to show that for each of these pieces we have $\lambda_{1,n}(\{A \subset I; i \in A\}) \le 2a|\lambda_{1,n}|$. For example, we have

$$\begin{aligned} T^{\cap}(\nu_1,\nu_0)(\{A \subset I; i \in A\}) &= \nu_1(\{A \subset I; i \in A)\nu_0(\{A \subset I; i \in A\}) \\ &\le a|\nu_1||\nu_0| = a|T^{\cap}(\nu_1,\nu_0)| \; . \end{aligned}$$

and

$$T^{\cup}(\nu_1,\nu_1)(\{A \subset I; i \in A\}) \le 2\nu_1(\{A \subset I; i \in A\})|\nu_1| \le 2a|\nu_1|^2 = 2a|T^{\cup}(\nu_1,\nu_1)| \; .$$

Now we define

$$2\lambda_q = T^{\cap}(\nu_q,\nu_q)+\sum_{0\le\ell\le q-1} T^{\cap}(\nu_q,\nu_\ell)+\sum_{0\le\ell\le q-1} T^{\cap}(\nu_\ell,\nu_q)+T^{\cup}(\nu_q,\nu_q)+T^{\cap}(\nu_{q-1},\nu_{q-1}) \; , \tag{5.12}$$

so that

$$2|\lambda_q| = |\nu_q|^2 + 2|\nu_q| \sum_{0\le\ell\le q-1} |\nu_\ell| + |\nu_q|^2 + |\nu_{q-1}|^2$$
$$= 2|\nu_q| \sum_{0\le\ell\le q} |\nu_\ell| + |\nu_{q-1}|^2 = 2|\nu_q| + |\nu_{q-1}|^2.$$

Since (5.12) exhibits λ_q as a sum $\sum_n \lambda_{q,n}$, to prove that (5.7) holds for $\ell = q$ it suffices to prove that for each n we have $\lambda_{q,n}(\{A \subset I; i \in A\}) \le 2H(a,q)|\lambda_{q,n}|$. For all the terms but the last one this is a consequence of Lemma 4.1 and (5.5). For the last term, we use that $H(a,q-1)^2 = H(a,q)$, so that

$$T^\cap(\nu_{q-1},\nu_{q-1})(\{A \subset I; i \in A\}) = \nu_{q-1}(\{A \subset I; i \in A\})^2$$
$$\le H(a,q-1)^2|\nu_{q-1}|^2 = H(a,q)|T^\cap(\nu_{q-1},\nu_{q-1})| \ .$$

For $1 < s < q$ we define (see the figure below)

$$2\lambda_s = \sum_{0\le\ell<s} T^\cap(\nu_s,\nu_\ell) + \sum_{0\le\ell<s} T^\cap(\nu_\ell,\nu_s) + T^\cup(\nu_s,\nu_s)$$
$$+ \sum_{s<\ell\le q} T^\cup(\nu_s,\nu_\ell) + \sum_{s<\ell\le q} T^\cup(\nu_\ell,\nu_s) + T^\cap(\nu_{s-1},\nu_{s-1}) \ , \quad (5.13)$$

so that

$$2|\lambda_s| = 2|\nu_s| \sum_{0\le\ell<s} |\nu_\ell| + |\nu_s|^2 + 2|\nu_s| \sum_{s<\ell\le q} |\nu_\ell| + |\nu_{s-1}|^2$$
$$= 2|\nu_s| \sum_{0\le\ell\le q} |\nu_\ell| - |\nu_s|^2 + |\nu_{s-1}|^2 = 2|\nu_s| - |\nu_s|^2 + |\nu_{s-1}|^2 \ . \quad (5.14)$$

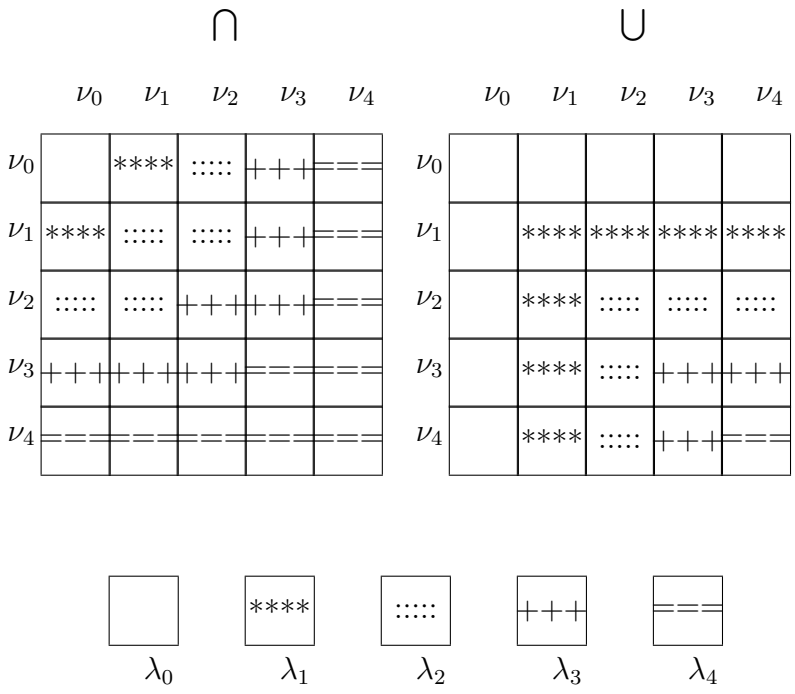

Figure: Attribution of the terms when $q = 4$

The proof of (5.7) when $1 < s < q$ is identical to the proof in the case $s = q$. Next we define λ_0 as the sum of the terms that have not appeared in one of the λ_s for $1 \leq s \leq q$. Even though this formula is irrelevant, the reader can check that

$$\lambda_0 = T^{\cap}(\nu_0, \nu_0) + T^{\cup}(\nu_0, \nu_0) + \sum_{1 \leq \ell \leq q} T^{\cup}(\nu_0, \nu_\ell) + \sum_{1 \leq \ell \leq q} T^{\cup}(\nu_\ell, \nu_0) \ .$$

Finally, we show that each term of the type $T^{\cap}(\nu_\ell, \nu_{\ell'})$ or $T^{\cup}(\nu_\ell, \nu_{\ell'})$ appears in exactly one the formulas for λ_s, $0 \leq s \leq q$. For the terms $T^{\cup}(\nu_\ell, \nu_{\ell'})$ this is obvious as they appear in the formula for $\lambda_{\min(\ell,\ell')}$ (and only this formula). A term $T^{\cap}(\nu_\ell, \nu_\ell)$ appears in λ_0 if $\ell = 0$, in λ_q if $\ell = q$ and in $\lambda_{\ell+1}$ if $0 < \ell < q$ (and only there). Finally a term $T^{\cap}(\nu_\ell, \nu_{\ell'})$ for $\ell \neq \ell'$ appears in $\lambda_{\max(\ell,\ell')}$ (and only there). □

Let us now explain what we have gained by performing this construction. For $\ell \geq 1$ we obviously have $2H(a, \ell) \leq H(2a, \ell)$. Also, since $H(2a, 0) = 1$ we deduce from (5.7) that

$$\forall \ell \leq q \ , \ \forall i \in I \ , \ \lambda_\ell(\{A \subset I; i \in A\}) \leq H(2a, \ell)|\lambda_\ell| \ . \tag{5.15}$$

That is, at the cost of replacing a by $2a$, $T(\mu,\mu)$ has a decomposition similar to (5.4) but we have shifted a little bit of mass to λ_q. In (5.3) we estimated how the mass has shifted by repeating the operation N times. More formally, we have the following.

Proposition 5.4 *Consider $\mu \in \mathcal{M}$. Consider an integer $P \geq 1$ and an integer $q \geq 2$. Assume that we have a decomposition $\mu = \nu + \nu'$ with the property that*

$$\forall i \in I \ , \ \nu(\{A \subset I; i \in A\}) \leq 2^{-P}|\nu| \ . \tag{5.16}$$

Then we have a decomposition $\mu^P = \eta + \eta'$ with $|\eta| \geq |\nu| - q^2/P$ and

$$\forall i \in I \ , \ \eta(\{A \subset I, i \in A\}) \leq 2^{-2^{q-1}}|\eta| \ . \tag{5.17}$$

This statement is useful when 2^q is much larger than P but q^2 is much smaller than P.

Proof. For $1 \leq \ell \leq q$ define the numbers a_ℓ by $a_1 = |\nu_1|$ and $a_\ell = 0$ otherwise. For $N \geq 1$ consider the numbers $a_{N,\ell}$ defined by the induction relations of Lemma 5.1. We prove by induction over N that for $1 \leq N \leq P$ there exists a decomposition $\mu^N = \sum_{0 \leq \ell \leq q} \lambda_{N,\ell}$ such that for $1 \leq \ell \leq q$ we have $|\lambda_{N,\ell}| = a_{N,\ell}$, while

$$\forall \ell \leq q \ , \ \forall i \in I \ , \ \lambda_{N,\ell}(\{A \subset I; i \in A\}) \leq H(2^{N-P-1}, \ell)|\lambda_{N,\ell}| \ . \tag{5.18}$$

For $N = 1$ we set $\lambda_{1,1} = \nu_1$, $\lambda_{1,\ell} = 0$ for $1 < \ell \leq q$ and $\lambda_0^1 = \nu_0$. Then (5.18) holds because it holds trivially for $1 < \ell \leq q$ while for $\ell = 1$ it holds by (5.16) since $H(a,1) = a$. For the induction step from N to $N+1$ we simply apply Proposition 5.3. For $N = P$ we obtain a decomposition $\mu^N = \sum_{0 \leq \ell \leq q} \lambda_{P,\ell}$ with $|\lambda_{P,q}| \geq |\nu_1| - q^2/N$ and

$$\forall \ell \leq q \ , \ \forall i \in I \ , \ \lambda_{P,\ell}(\{A \subset I, i \in A\}) \leq H(2^{-1}, \ell)|\lambda_{P,\ell}| \ .$$

We then set $\eta = \lambda_{P,q}$ and $\eta' = \sum_{0 \leq \ell \leq q-1} \lambda_{P,\ell}$, using also that $H(2^{-1}, q) = 2^{-2^{q-1}}$. □

Proof of Theorem 3.6. The idea is to use first Corollary 4.3 in order to produce the condition (5.16) and to be able to use Proposition 5.4. Let us fix $\beta < 1/2$ and consider an integer $q \geq 2$ with $N \geq 9q^2/\beta^2$. Consider the smallest integer P such that $P \geq 2q^2/\beta$, so that $P \leq 3q^2/\beta \leq 3q^2/\beta^2 \leq N/3$. Let $N' = N - P$ so that $\beta N' \geq \beta N - \beta P \geq 9q^2/\beta - 3q^2/\beta \geq 6q^2/\beta \geq 2P$.

We use Corollary 4.3 (with $\beta/2$ instead of β) to obtain that we can write

$$\mu^{N'} = \nu + \nu'$$

with $|\nu| = 1/2 - \beta/2$ and

$$\forall i \in I \ , \ \nu(\{A \subset I; i \in A\}) \leq \exp(-\beta N'/2)|\nu| \ .$$

Also, $\exp(-\beta N'/2) \leq \exp(-P) \leq 2^{-P}$. We may then apply Proposition 5.4 to $\mu^{N'}$ to obtain a decomposition $\mu^N = (\mu^{N'})^P = \eta + \eta'$ with $|\eta| \geq |\nu_1| - q^2/P = 1/2 - \beta/2 - q^2/P \geq 1/2 - \beta$ and (5.17) holds. Now, using (5.17) in the last line we then have

$$\int |A| \mathrm{d}\eta(A) = \int \sum_{i \in I} 1_A(i) \mathrm{d}\eta(A) = \sum_{i \in I} \int 1_A(i) \mathrm{d}\eta(A)$$
$$= \sum_{i \in I} \eta(\{C \subset I; i \in C\}) \leq |I| \, 2^{-2^{q-1}} |\eta|$$

so that by Markov's inequality

$$\eta(\{A \subset I \ ; \ |A| \geq \alpha \, |I|\}) \leq \frac{1}{\alpha} 2^{-2^{q-1}} |\eta|$$

and thus

$$\mu^N(\{A \subset I \ ; \ |A| < \alpha \, |I|\}) \geq (1 - \frac{1}{\alpha} \, 2^{-2^{q-1}})|\eta| = (1 - \frac{1}{\alpha} \, 2^{-2^{q-1}})(1/2 - \beta) \ . \quad (5.19)$$

To prove Theorem 3.6, we may assume that $\beta^2 N \geq 36$. We will apply (5.19) to a suitable value of q to prove (3.2). We consider the largest integer q with $9q^2 \leq \beta^2 N$, so that $9(q+1)^2 > N\beta^2$ and thus $q - 1 > \beta\sqrt{N}/3 - 2$. Also, since $9 \times 2^2 \leq \beta^2 N$ we have $q \geq 2$. Now, since $\mathrm{e} < 4$ there exists a constant L such that for $\beta\sqrt{N} \geq L$ we have $2^{\beta\sqrt{N}/3-2} = 4^{\beta\sqrt{N}/6-1} \geq 2\exp(\beta\sqrt{N}/6)$. Then $2^{q-1} \geq 2^{\beta\sqrt{N}/3-2} \geq 2\exp(\beta\sqrt{N}/6)$ and thus $2^{-2^{q-1}} \leq \exp(-\exp(\beta\sqrt{N}/6))$. We have proved that (5.19) implies (3.2). □

6 The Asymmetric Case

We now investigate the case where at each internal node of the tree we chose independently the connectives "and" or "or" but we chose "and" with probability $p > 1/2$ and "or" with probability $1 - p$. We will prove that Boolean expressions have a very strong tendency to be antitautologies. (Of course if $p < 1/2$ they have a very strong tendency to be tautologies.) It is known[5] that for $p > 1/2$ there is a constant $c > 0$, depending on p only, such that if $2^{k_N} \exp(-cN) \to 0$ then $\mathsf{P}(\textit{antitautology}) \to 1$. Our main result is much stronger.

[5]This is actually a simple consequence of Lemma 6.4 below.

Theorem 6.1 *If $p > 1/2$ there exists a constant $c > 0$ depending on p only such that if $k_N \exp(-cN) \to 0$ then $\mathsf{P}(\textit{antitautology}) \to 1$.*

We will deduce this result from a theorem proved in the abstract setting of Section 3, replacing 3.1 by

$$T(\mu, \mu') = pT^{\cap}(\mu, \mu') + (1-p)T^{\cup}(\mu, \mu') \; . \tag{6.1}$$

Theorem 6.2 *There is a constant K and a constant $\alpha < 1$ both depending on $p > 1/2$ only with the following property. Consider a measure $\mu^0 \in \mathcal{M}$ and define recursively $\mu^{N+1} = T(\mu^N, \mu^N)$. Then for $N \geq K \log\log(3|I|)$ we have*

$$\mu^N(\{\emptyset\}) \geq 1 - \alpha^N \; . \tag{6.2}$$

The main point of this theorem is that (6.2) holds for rather small values of N.[6] Let us start with some simple facts.

Lemma 6.3 *The quantity $a_N = \mu^N(\{A \subset I; i \in A\})$ is independent of i and satisfies the relations $a_0 = 1/2$ and*

$$a_{N+1} = 2(1-p)a_N + (2p-1)a_N^2 \; . \tag{6.3}$$

Proof. The fact that $a_0 = 1/2$ is a consequence of the definition of $\mathcal{M}$ and of the fact that $\mu^0 \in \mathcal{M}$. Furthermore (6.3) is a consequence of the relations

$$T^{\cap}(\mu^N, \mu^N)(\{A \subset I; i \in A\}) = a_N^2 \; ; \; T^{\cup}(\mu^N, \mu^N)(\{A \subset I; i \in A\}) = 2a_N - a_N^2 \; .$$

□

Lemma 6.4 *For each N we have $a_N \leq (3/2 - p)^N/2$.*

Proof From (6.3) it is immediate by induction over N that $a_N \leq 1/2$. We then deduce from (6.3) that $a_{N+1} \leq a_N(2(1-p) + (2p-1)/2) = a_N(3/2 - p)$. □

Proposition 6.5 *Given $p > 1/2$ there exists a number $\rho < 1$ depending only on p with the following property. Assume that for a certain number $a > 0$ we have a decomposition $\mu = \nu + \nu'$ with the following properties:*

$$|\nu| \geq 1/4 \; , \tag{6.4}$$

[6] A referee pointed out that it is possible by refining Lemma 6.4 to show that we have $\mu^N(\{\emptyset\}) \geq 1 - C|I|(2-2p)^N$ for a constant C depending on p only. This improves upon (6.2) for large values of N.

$$\forall i \in I \ , \ \nu(\{A \subset I; i \in A\}) \leq a \ . \tag{6.5}$$

Then we have a decomposition $\mu^N = \lambda + \lambda'$ *with* $|\lambda| \geq 1 - \rho^N$ *and*

$$\forall i \in I \ , \ \lambda(\{A \subset I; i \in A\}) \leq 2^N a \ . \tag{6.6}$$

In particular there exists an integer $q = q(p)$ *depending on* p *only such that there is a decomposition* $\mu^{q(p)} = \lambda + \lambda'$ *with* $|\lambda| \geq 3/4$ *and*

$$\forall i \in I \ , \ \lambda(\{A \subset I; i \in A\}) \leq 2^{q(p)} a \ . \tag{6.7}$$

It will follow from the next two results.

Lemma 6.6 *Given* $p > 1/2$ *there exists* $\rho < 1$ *depending on* p *only with the following property. Consider a sequence* (a_N) *with* $a_0 \geq 1/4$ *and* $a_{N+1} = 2pa_N + (1-2p)a_N^2$. *Then* $a_N \geq 1 - \rho^N$.

Proof. This is basically obvious once one draws the graph of the function $f(x) = 2px + (1-2p)x$. For a formal proof, it is obvious inductively that $a_N \leq a_{N+1} \leq 1$. Setting $b_N = 1 - a_N$ we obtain that $0 \leq b_N \leq 3/4$ and that $b_{N+1} = (2-2p)b_N + (2p-1)b_N^2 \leq \rho b_N$ where $\rho = 2 - 2p + 3(2p-1)/4 < 1$. Thus $b_N \leq \rho^N$. □

Lemma 6.7 *Assume that we have a decomposition* $\mu = \nu + \nu'$ *such that (6.5) holds. Then we have a decomposition* $T(\mu, \mu) = \eta + \eta'$ *such that* $|\eta| = 2p|\nu| + (1-2p)|\nu|^2$ *and*

$$\forall i \in I \ , \ \eta(\{A \subset I; i \in A\}) \leq 2a \ . \tag{6.8}$$

Proof. Define

$$\eta = pT^{\cap}(\nu, \nu) + pT^{\cap}(\nu, \nu') + pT^{\cap}(\nu', \nu) + (1-p)T^{\cup}(\nu, \nu) \ ,$$

so that $|\eta| = p(|\nu|^2 + 2|\nu||\nu'|) + (1-p)|\nu|^2 = 2p|\nu| + (1-2p)|\nu|^2$ since $|\nu'| = 1 - |\nu|$, while (6.8) follows from (4.3) since $p(|\nu| + 2|\nu'|) + 2(1-p)|\nu| \leq 2$. □

Proof of Proposition 6.5. Apply recursively N times Lemma 6.7 and use Lemma 6.6. □

We recall the integer $q(p)$ of Proposition 6.5.

Proposition 6.8 *Assume that for some integer* $\ell \geq 0$ *we have a decomposition* $\mu = \nu + \nu'$ *where* $|\nu| \geq 1/4$ *and*

$$\forall i \in I \ , \ \nu(\{A \subset I; i \in A\}) \leq 2^{-(2^\ell + 2)q(p)} \ . \tag{6.9}$$

Then there is a decomposition $\mu^{q(p)+1} = \theta + \theta'$ *such that* $|\theta| \geq 1/4$ *and*

$$\forall i \in I \ , \ \theta(\{A \subset I; i \in A\}) \leq 2^{-(2^{\ell+1} + 2)q(p)} \ . \tag{6.10}$$

Proof. We use Proposition 6.5 with $a = 2^{-(2^\ell+2)q(p)}$ to obtain a decomposition $\mu^{q(p)} = \lambda + \lambda'$ with $|\lambda| \geq 3/4$ and

$$\forall i \in I \ , \ \lambda(\{A \subset I; i \in A\}) \leq 2^{-(2^\ell+1)q(p)} \ . \tag{6.11}$$

We then set $\theta = pT^{\cap}(\lambda, \lambda)$, so that $|\theta| = p|\lambda|^2 \geq p(3/4)^2 \geq 9/32 \geq 1/4$. We then use (4.2) to deduce (6.10) from (6.11). □

Let us now fix $p > 1/2$ once and for all. According to Lemma 6.4 there exists N_0 depending on p only such that $\mu^{N_0}(\{A \subset I; i \in A\}) \leq 2^{-(2^0+2)q(p)}$ for each $i \in I$. For $\ell \geq 0$ we set $N_\ell = N_0 + \ell(q(p)+1)$.

The following elementary lemma deserves no proof.

Lemma 6.9 *There exists a constant K^* depending on p only such that the following occur for any integer N, denoting by ℓ_0 the largest integer ℓ with $N_\ell \leq N/2$:*

$$N \geq K^* \log\log 3 \Rightarrow \ell_0 \geq N/(3q(p)) \ , \tag{6.12}$$

$$N \geq K^* \log\log 3 \Rightarrow 2N - 2^{N/(3q(p))} \leq -2^{N/(4q(p))} \ , \tag{6.13}$$

$$N \geq K^* \log\log(3|I|) \Rightarrow |I| 2^{-2^{N/(4q(p))}} \leq 1 \ . \tag{6.14}$$

Proof of Theorem 6.2. We first show by induction over $\ell \geq 0$ that we have a decomposition $\mu^{N_\ell} = \theta + \theta'$ where $|\theta| \geq 1/4$ and $|\theta|$ satisfies $\theta(\{A \subset I; i \in A\}) \leq 2^{-(2^\ell+2)q(p)}$ for each $i \in I$. For $\ell = 0$ this holds by the choice of N_0 and the induction step is performed by Proposition 6.8. Consider two integers ℓ and s. Then, applying Proposition 6.5 (with s instead of N) to μ^{N_ℓ} we obtain a decomposition $\mu^{s+N_\ell} = (\mu^{N_\ell})^s = \gamma + \gamma'$ with $|\gamma| \geq 1 - \rho^s$ and

$$\forall i \in I \ , \ \gamma(\{A \subset I; i \in A\}) \leq 2^{s-(2^\ell+1)q(p)} \ , \tag{6.15}$$

so that

$$\mu^{s+N_\ell}(\{\emptyset\}) \geq \gamma(\{\emptyset\}) \geq |\gamma| - |I| 2^{s-(2^\ell+2)q(p)} \geq 1 - \rho^s - |I| 2^{s-(2^{\ell_0}+2)q(p)} \ . \tag{6.16}$$

Consider now $N \geq K^* \log\log(3|I|)$. Recall from Lemma 6.9 the largest integer ℓ_0 such $N_{\ell_0} \leq N/2$. Then by (6.12) we have $\ell_0 \geq N/(3q(p))$. Take $s = N - N_{\ell_0}$ so that $N/2 \leq s \leq N$ and $\rho^s \leq \rho^{N/2}$. Also, using in turn (6.13) and (6.14) we get

$$|I| 2^{s-(2^{\ell_0}+2)q(p)} \leq 2^{-N} |I| 2^{2N - 2^{N/(3q(p))}} \leq 2^{-N} |I| 2^{-2^{N/(4q(p))}} \leq 2^{-N} \ .$$

The right-hand side of (6.16) is then $\geq 1 - \rho^{N/2} - 2^{-N}$. Assuming without loss of generality that $\rho > 1/4$ this is $\geq 1 - 2\rho^{N/2} = 1 - \rho_N^N$ for $\rho_N = 2^{1/N}\rho^{1/2}$, and $\rho_N < 1$ for N large enough. □

Proof of Theorem 6.1. Proceeding as in Section 3.3 it is a consequence of Theorem 6.2.

Acknowledgment. The authors are grateful to J.F. Le Gall and N. Curien, who introduced them to the paper [A-C]. This played a crucial role in the present project.

References

[A-C] Auffinger, A; Cable, D. Pemantle min-plus binary tree. Manuscript, 2017. https://arxiv.org/abs/1709.07849

[B-M] Broutin, N; Mailler, C. And/or trees: a local limit point of view. Random Structures & Algorithms 53 (2018), no. 1, 15–58.

[C-G-M] Chauvin, B.; Gardy, D.; Mailler, C. A sprouting tree model for random Boolean functions. Random Structures & Algorithms 47 (2015), no. 4, 635–662.

[CO-P] Coja-Oghlan, A; Panagiotou, K. The asymptotic k-SAT threshold. Advances in Mathematics 288, (2016), 985–10.

[F-G-G] Fournier, H; Gardy, D; Genitrini, A. Balanced And/Or trees and linear threshold functions. In 5th SIAMWorkshop on Analytic and Combinatorics (ANALCO), 2009, 51–57.

[G] Gardy, D. Random Boolean expressions. Computational logic and applications, CLA '05, 1–35, Discrete Math. Theor. Comput. Sci. Proc., AF, Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2006.

[G-M] Genitrini, A; Mailler, C. Generalized and Quotient Models for Random And/Or Trees and Application to Satisfiability. Algorithmica 76(4)(2016): 1106–1138.

[G-W] Gardy, D; Woods, A. And/or tree probabilities of Boolean functions. 2005 International Conference on Analysis of Algorithms, 139–146, Discrete Math. Theor. Comput. Sci. Proc., AD, Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2005.

[L-S] Lefmann, H; Savický, P. Some typical properties of large AND/OR Boolean formulas. Random Structures & Algorithms 10 (1997), no. 3, 337–351.