CPSC 664, Spring 2023 Scribe: Curtis McDonald
January 26, 2023 Lecturer: Tim Kunisky

Lecture 4: Random k-SAT II

1 Review of Random k-SAT Problem

Recall that we are studying the random k-SAT problem. In this setting, we have a random Boolean formula $F : \{0,1\}^n \to \{0,1\}$ acting on n Boolean input values $z_1, \cdots, z_n$. So we can think of the formula as the function F where given an entry $\boldsymbol{z}$ in the n-dimensional hypercube, F returns true or false for that $\boldsymbol{z}$ vector. The Boolean formula is composed of m clauses, each depending on k of the input z_i values. A single clause is a "or" ($\vee$) product of k possibly negated z_i values,

$$C_j = ((\neg)z_{i_{j,1}} \vee \cdots \vee (\neg)z_{i_{j,k}}) \tag{1}$$

where $\{i_{j,1}, \cdots, i_{j,k}\} \subset \{1, \cdots, n\}$ is a size-k selection of indices which appear in the clause. The overall F function is then the "and" ($\wedge$) product of these m clauses,

$$F(z) = C_1(z) \wedge \cdots \wedge C_m(z) \tag{2}$$

The function F is constructed randomly in uniform choice of subsets $\{i_{j,1}, \cdots, i_{j,k}\}$ for each clause and uniform choice of negations within each clause (i.e., do we use $z_{i_{j,1}}$ or $\neg z_{i_{j,1}}$ in the clause). The question is, for a given F, does there exist an element of the hypercube z such that $F(z) = 1$. In other words, does there exist a set of truth assignments for the z_i which satisfy F and evaluate to 1 or true. If so, F is said to be *satisfiable*; if not, F is said to be *unsatisfiable*.

The relationship depends on the relative sizes of m (the number of clauses) and n (the number of boolean inputs to the formula). Say $m = \alpha n$. The conjecture is that for each value of k, there is a threshold $\alpha^* = \alpha(^*k)$ such that

- If $\alpha > \alpha^*$, then F is unsatisfiable w.h.p.
- If $\alpha < \alpha^*$, then F is satisfiable w.h.p.

2 $k = 2$ Simple Case

As we will later see, the threshold for $k = 3$ based on current research and empirical simulation appears to be about $\alpha^*(3) \approx 4.26$. But first, we look at the simpler case of $k = 2$ where much of the complexity is reduced.

The $k = 2$ case is easier to study since each clause is of the form $((\neg x) \vee (\neg)y)$ for binary variables x and y. For such a clause to be true, say the clause $(\neg x \vee y)$, is equivalent to

1. If x is true, then $\neg x$ is false, so y must be true.

2. If y is false, then $\neg x$ must be true, or equivalently x must be false.

Thus x and y must share the same truth value in such a clause in order for the clause to be true. More generally, a 2-SAT instance corresponds to a graph of implications between the variables z_i and their negations which show which variables must be true when others are true. The function F is satisfiable if and only if there are no cycles in this graph that include z_i and $\neg z_i$ for some i.

We can analyze the 2-SAT problem by studying this graph structure. It turns out, in a phase transition similar to the emergence of a giant component in an Erdős-Rényi random graph, that the critical value is $\alpha^*(2) = 1$ This "implication graph" representation also shows that 2-SAT can be solved in polynomial time and, unlike k-SAT for $k \geq 3$ (assuming $\mathsf{P} \neq \mathsf{NP}$), belongs to the complexity class P.

3 $k = 3$ First Moment Method Initial Analysis

Note that going forward, we will use the notation $x \in \{0,1\}^n$ and not z as the input variable to the function F.

Similarly to how we analyzed the number partitioning problem, we are interested in the event $\{\exists x : F(x) = 1\}$. To study the probability that such an event will occur, we look at the size of the set of values which would satisfy this event,

$$Z = \#\{x \in \{0,1\}^n : F(x) = 1\}.$$

Note that Z is a random variable depending on the random assignments that construct F. The expectation of Z is

$$\begin{aligned}\mathbb{E}[Z] &= \sum_x \mathbb{P}[x \text{ satisfies } F] \\ &= \sum_x \prod_{j=1}^m \mathbb{P}[x \text{ satisfies } C_j] \\ &= \sum_x \mathbb{P}[x \text{ satisfies } C_1]^m,\end{aligned}$$

the last step following since each clause is chosen i.i.d. Then, using negation

$$\begin{aligned}P(x \text{ satisfies } C_1) &= 1 - \mathbb{P}[x \text{ not satisfies } C_1] \\ &= 1 - \frac{1}{8} \\ &= \frac{7}{8}.\end{aligned}$$

Here we use that clause C_j is the or of possibly negated $z_{i_{j,1}}, z_{i_{j,2}}, z_{i_{j,3}}$, so each has to be the wrong value with $\frac{1}{2}$ probability, so $\frac{1}{8}$ is probability of not satisfying this clause. So the sum becomes

$$\mathbb{E}[Z] = 2^n \left(\frac{7}{8}\right)^m = 2^n \left(\frac{7}{8}\right)^{\alpha n} = \left(2\left(\frac{7}{8}\right)^{\alpha}\right)^n.$$

The inner expression equaals 1 when $\alpha = \frac{\log(\frac{1}{2})}{\log \frac{7}{8}} \approx 5.19$, which we will call $\alpha^{(1)} \approx 5.19$, our first estimate for $\alpha^*(3)$. This leads to the following.

Proposition 3.1. *If $\alpha > \alpha^{(1)} \approx 5.19$, then w.h.p. F is unsatisfiable.*

This follows by the same Markov's inequality argument we have seen before.

Therefore, $\alpha^*(3)$, the conjectured threshold which divides satisfiablity and unsatisfiability for $k = 3$, if it exists, would have to be less than or equal to this value $\alpha^*(3) \leq \alpha^{(1)}$.

However, numerical experiments lead us to believe that $\alpha^*(3) \approx 4.26$. So there is some "gap" in our argument. What went wrong?

4 $k = 3$ First Moment Method Improved Analysis

In a nutshell, Z was not the best random variable to which to apply the first moment method. There is a better choice of counting variable which we apply the first moment method to and get a tighter bound on the threshold.

Note that by conditional probability

$$\mathbb{E}[Z] = \mathbb{E}[Z \mid F \text{ is satisfiable}] \cdot \mathbb{P}[F \text{ is satisfiable}].$$

If, say, $\alpha = 5$, we have that $\alpha^* = 4.26 < \alpha < \alpha^{(1)}$, thus we think F should be unsatisfiable w.h.p. (since $\alpha > \alpha^*$) but for $\alpha = 5$ the above expectation is not going to 0, it is going to infinity. So the above analysis would not conclude that F is unsatisfiable.

The issue is that while $\mathbb{P}[F \text{ is satisfiable}]$ may be small, $EE[Z \mid F \text{ is satisfiable}]$ maybe be large, forcing the overall expectation to diverge,, even if the probability is going to 0. So, we want a random variable which is smaller than Z to better track when the probability is going to zero and not to unintentionally bring up the expectation.

The main idea is to only count "special" or "canonical" satisfying x that exist whenever F is satisfiable.

Definition 4.1. *x satisfying F is **locally maximal** if all neighbors $x' = x$ with one 0 flipped to a 1 are not satisfying. That is, whenever we have:*

$$\begin{aligned} x &= 0 \quad 1 \quad \boldsymbol{0} \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \\ x' &= 0 \quad 1 \quad \boldsymbol{1} \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \end{aligned}$$

where x is satisfying, then x' must not be satisfying.

Basically, x is a satisfying vector which has more 1's than any immediate neighbors which are also satisfying.

We then consider

$$Y = \#\{x : x \text{ satisfies } F \text{ and } x \text{ is locally maximal}\}$$

Proposition 4.2. *If F is satisfiable, then there exists a locally maximal x that satisfies x.*

Proof. If F is satisfiable, there is one x which satisfies F. Take that x and go through the 0 values and try to flip them to 1 to get a new $'$. If this new x' still satisfies F, then set $x = x^{prime}$ and repeat this process. Eventually, we will get to an x which is all 1, or none of the remaining 0's can be flipped to a 1 while still satisfying F. Thus we terminate at a locally maximal satisfying x. $\square$

The set which Y counts is a subset of the set that Z counted, thus $Y \leq Z$.

By the same Markov's inequality argument as before, if $\mathbb{E}[Y] \to 0$, then w.h.p. there does not exist a locally maximal satisfying x, and so by the Proposition w.h.p. F is unsatisfiable.

So we study the expected value of Y,

$$\mathbb{E}[Y] = \sum_x \mathbb{P}[x \text{ satisfies } F \text{ and } x \text{ is locally maximal}]$$

Claim 1. *If x is locally maximal, and some $x_i = 0$ for some i, then there must exist some "blocking" clause $C = C(i)$ that is false under x' where we flip x_i and leave the rest the same.*

This blocking clause must be of the form

$$C = (\neg x_i) \vee (\cdots) \vee (\cdots)$$

where the first term is true under x, and the other terms are false under x. Thus if we tried to flip x_i this first term would become false, the rest are false, and thus clause would be false and we do not satisfy F anymore.

We then have

$$\begin{aligned} &\mathbb{P}[x \text{ satisfies } F \text{ and } x \text{ is locally maximal}] \\ =&\mathbb{P}[x \text{ satisfies } F] \cdot \mathbb{P}[x \text{ locally maximal} \mid x \text{ satisfies } F]. \end{aligned}$$

We already determined the marginal probability $PP[x \text{ satisfies } F] = (\frac{7}{8})^m$ before, thus this conditional probability term can only decrease the joint probability (we are multiplying by a term between 0 and 1) and thus we will have a reduced probability and thus a reduced overall expectation.

We now calculate

$$\begin{aligned} &\mathbb{P}[x \text{ locally maximal} \mid x \text{ satisfies } F] \\ =&\mathbb{P}[\text{there exists a blocking clause in F for every index i where } x_i = 0 \mid x \text{ satisfies } F] \end{aligned}$$

By the above structure of blocking clauses, each clause can only block at most one index i, and so it is reasonable to believe that each i with $x_i = 0$ getting blocked by some clause are negatively correlated events. Based on this intuition, we claim (without further justification) that

$$\begin{aligned} &\mathbb{P}[\text{there exists a blocking clause in F for every index i where } x_i = 0 \mid x \text{ satisfies } F] \\ &\leq \prod_{i:x_i=0} \mathbb{P}[\text{there exists a clause in F blocking index } i \mid x \text{ satisfies } F] \\ &= \prod_{i:x_i=0} (1 - \mathbb{P}[C \text{ does not block } i \mid x \text{ satisfies } C]^m), \end{aligned}$$

in the last step again using that the clauses are i.i.d.

We now study $P(\text{C does not block i}|x \text{ satisfies } C)$. By Bayes's rule,

$$\begin{aligned}\mathbb{P}[C \text{ does not block } i \mid x \text{ satisfies } C] &= 1 - \frac{\#\{C : C \text{ blocks } i, x \text{ satisfies } C\}}{\#\{C : x \text{ satisfies } C\}} \\ &= 1 - \frac{\binom{n}{2}}{\frac{7}{8} \cdot 2^3 \binom{n}{3}}\end{aligned}$$

Putting all this together, we have

$$\begin{aligned}\mathbb{P}[x \text{ satisfies } F \text{ and } x \text{ is locally maximal}) &\leq \left(\frac{7}{8}\right)^m \left(\prod_{i:x_i=0} \left(1 - \left(1 - \frac{\binom{n}{2}}{7\binom{n}{3}}\right)^m\right)\right) \\ &= \left(\frac{7}{8}\right)^m \left(1 - \left(1 - \frac{\binom{n}{2}}{7\binom{n}{3}}\right)^m\right)^{\#\{i:x_i=0\}}\end{aligned}$$

Note that, for k fixed and n large,

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \approx \frac{n^k}{k!},$$

and therefore

$$\frac{\binom{n}{2}}{7\binom{n}{3}} \approx \frac{3}{7n}.$$

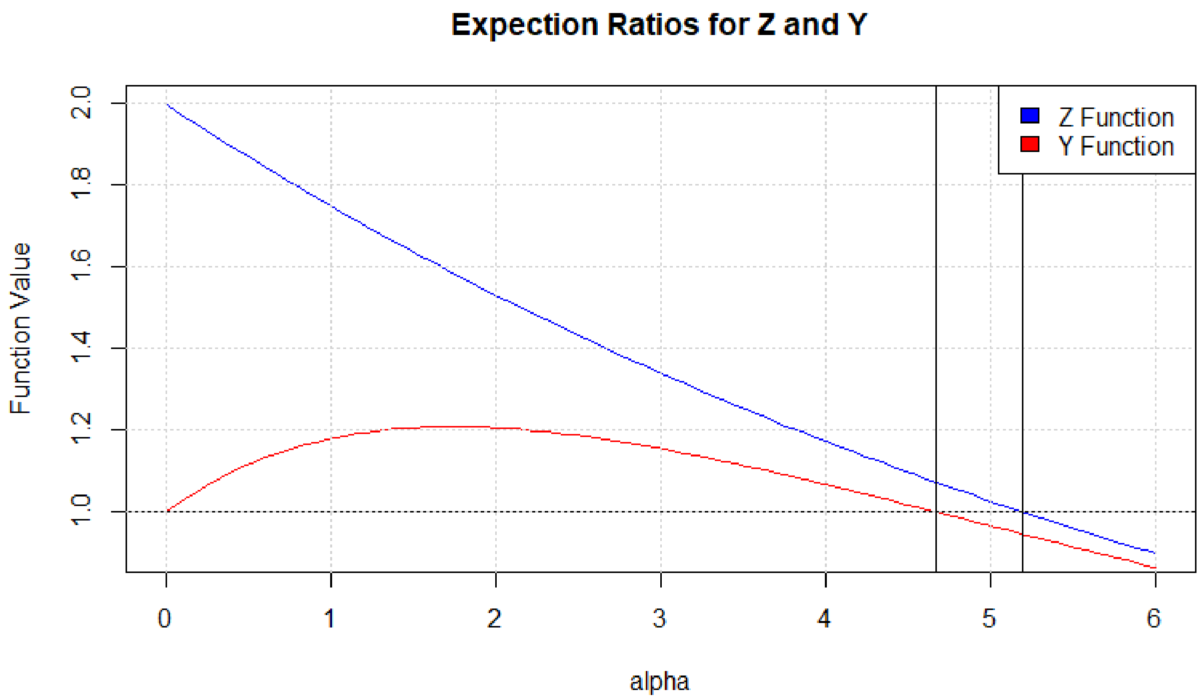
Plugging this in, the above simplifies to

$$\left(\frac{7}{8}\right)^m \left(1 - \left(1 - \frac{\binom{n}{2}}{7\binom{n}{3}}\right)^m\right)^{\#\{i:x_i=0\}} \approx \left(\frac{7}{8}\right)^m \left(1 - e^{-\frac{3}{7}\alpha}\right)^{\#\{i:x_i=0\}}.$$

We sum over all x, and, using that the above quantity depends only on the number of 0's in x, we may reduce and use the binomial theorem,

$$\begin{aligned}\mathbb{E}[Y] &\leq \sum_{f=0}^{n} \binom{n}{f} \left(\frac{7}{8}\right)^m \left(1 - e^{-\frac{3}{7}\alpha}\right)^f \\ &= \left(\frac{7}{8}\right)^{\alpha n} (2 - e^{-\frac{3}{7}\alpha})^n = \left[\left(\frac{7}{8}\right)^{\alpha} (2 - e^{-\frac{3}{7}\alpha})\right]^n.\end{aligned}$$

As in the first calculation, we are interested in the α for which the inner quantity equals 1. Before, this quantity was $2\left(\frac{7}{8}\right)^{\alpha}$, while now we an additional additive term of $e^{-\frac{3}{7}\alpha}$, which will decrease this quantity and make it equal 1 for a smaller α. It turns out that this value is approximately $\alpha^{(2)} \approx 4.67 < 5.19 = \alpha^{(1)}$, so this adjustment indeed improves the first moment method.


Expection Ratios for Z and Y
Z Function
Y Function
Function Value
2.0
1.8
1.6
1.4
1.2
1.0
0
1
2
3
4
5
6
alpha