1 Brief Introduction to Second Moment Method

In previous lecture, we presented a lower bound for threshold of satisfiability problem by unit clause propagation algorithm. In this lecture, we use the second moment method to give another, and better lower bound for K-SAT problem. We recall the basic setting below.

Let $P_N(k, \alpha)$ be the probability that a random formula from $\text{SAT}_N(k, M = \alpha N)$ ensemble is SAT. We try to find a lower bound of $\alpha$, such that $P_N(k, \alpha) \to 0$ as $N \to \infty$.

At first, let’s go over the main ideas of second moment method. Given a nonnegative function $U$, which is defined in the space of all K-SAT formulas, satisfying $U(\psi) = 0$ if $\psi$ is not SAT. Then,

$$P[\psi \text{ is SAT}] \geq P[U(\psi) > 0] \geq \frac{\mathbb{E}^2[U(\psi)]}{\mathbb{E}[U^2(\psi)]},$$

by Cauchy-Shwarz inequality. So, we try to pick up some function $U$ whose moments can be evaluated efficiently, and give us a meaningful bound as well.

Remark 1 It is an art to pick up $U$. For example, if we take $U(\psi) = \#$ of satisfying assignments, it will give us nothing but a zero lower bound.

Here, we take

$$U(\psi) = \sum_{x \in \{0,1\}^N} \prod_{a=1}^M \omega(x, a),$$

in which

$$\omega(x, a) = \begin{cases} 0, & \text{if } C_a(x) = 0; \\ \lambda^r(x,a), & \text{if } C_a(x) = 1, r(x,a) = \# \text{ of variables in } x \text{ satisfying } C_a. \end{cases}$$

Now, we try to computer the first and second moment of $U(\psi)$. 

9-1
2 Computation of First Moment

By the definition of $U$,

\[
E[U(\psi)] = E\left[ \sum_{x \in \{0,1\}^N} \prod_{a=1}^{M} \omega(x, a) \right]
\]

\[
= \sum_{x \in \{0,1\}^N} E\left[ \prod_{a=1}^{M} \omega(x, a) \right]
\]

\[
= 2^N E[\omega(x, a)]^M
\]

Last equality holds since the clauses in a formula are chosen independently (with repetition).

Since

\[
E[\omega(x, a)] = 2^{-k} \sum_{r=1}^{k} \binom{n}{k} \lambda^r
\]

\[
= 2^{-k}[(1 + \lambda)^k - 1]
\]

We conclude:

Claim 2 $\frac{\log E[U(\psi)]}{N} = \log 2 - \alpha k \log 2 + \alpha \log[(1 + \lambda)^k - 1] \equiv h_1(\lambda, \alpha)$.

3 Computation of Second Moment

The second moment calculations are typically more involved:
\[ \mathbb{E}[U^2(\psi)] = \sum_{x,y \in \{0,1\}^N} \mathbb{E}\left[ \prod_{a=1}^M \omega(x,a) \prod_{a=1}^M \omega(y,a) \right] \]

\[ = \sum_{x,y \in \{0,1\}^N} \{ \mathbb{E}[\omega(x,a)\omega(y,a)] \}^M \]

(let \( L = d_H(x,y) \) Hamming distance)

\[ = \sum_{x \in \{0,1\}^N} \sum_{L=0}^N \sum_{y:d_H(y,x)=L} \mathbb{E}\{ [\omega(x,a)\omega(y,a)] \}^M \]

\[ = 2^N \sum_{L=0}^N \binom{N}{L} (g(N,L))^M, \]  \hspace{1cm} (1)

where

\[ g(N,L) = 2^{-k} \sum_{u,v \neq 0}^N \lambda^{w(u)} \lambda^{w(v)} (\frac{L}{N})^{d(u,v)} (1 - \frac{L}{N})^{k-d(u,v)}. \]

Here, \( w(u) \) denotes \# of 1’s in \( u \). (1) is true because

**Claim 3** If \( d_H(x,y) = L \), then \( \mathbb{E}[\omega(x,a)\omega(y,a)] = g(N,L) \).

**Proof:** Denote \( u \) as \((u_1,u_2,\ldots,u_k)\), and let \( u_i = 1 \) if and only if the \( i \)th position of \( a \) is satisfied by \( x \), i.e., the \( i \)th variable in \( a \) and the counterpart in \( x \) have the same sigh. And similarly define \( v \). Now we fix \( u, v \) and then count the number of corresponding clauses. We give a brief case by case analysis. If \( u_i = v_i \), then the \( i \)th variable of \( a \) can be and only be picked up from those for which \( x \) and \( y \) have the same value; if \( u_i \neq v_i \), then the \( i \)th variable of \( a \) can be and only be picked up from those for which \( x \) and \( y \) have different values. And in both cases, the sigh of the variable has one and only one choice. Summing over all possible choices of \( u \) and \( v \), we get the equality in the claim. \( \square \)

Now, we turn to the computation of \( g(N,L) \). For simplicity of notation, we let \( Z = \frac{L}{N} \). So,

\[ 2^k g(N,L) = \sum_{u,v \in \{0,1\}^k} \lambda^{w(u)+w(v)} Z^{d_H(u,v)} (1-Z)^{k-d_H(u,v)} \]

\[ -2 \sum_{u \in \{0,1\}^k} \lambda^{w(u)} Z^{w(u)} (1-Z)^{k-w(u)} + (1-Z)^k \]

\[ \equiv I_1 - 2I_2 + (1-Z)^k. \]  \hspace{1cm} (2)
By fixing the Hamming distance of \( u \) and \( v \) and summing over the number of 1’s in common positions, we get

\[
I_1 = \sum_{d=0}^{k} \binom{k}{d} 2^d Z^d (1 - Z)^{k-d} \sum_{r=0}^{k-d} \lambda^{r+d} \binom{k-d}{r}
\]
\[
= \sum_{d=0}^{k} \binom{k}{d} 2^d Z^d \lambda^{d} (1 - Z)^{k-d} (1 + \lambda^2)^{k-d}
\]
\[
= (2\lambda Z + (1 - Z)(1 + \lambda^2))^k. \tag{3}
\]

And fixing number of 1’s in \( u \) and then summing over, we get

\[
I_2 = \sum_{r=0}^{k} \binom{k}{r} \lambda^{r} Z^r (1 - Z)^{k-r}
\]
\[
= (\lambda Z + (1 - Z))^k. \tag{4}
\]

Combining (2), (3) and (4), we get

\[
2^k g(N, L) = (2\lambda Z + (1 - Z)(1 + \lambda^2))^k - 2(\lambda Z + (1 - Z))^k + (1 - Z)^k.
\]

Based on discussions above, we are ready to make a claim as follow:

**Claim 4** \( \log \mathbb{E}[U^2(\psi)] / N \approx \log 2 + \max_{0 \leq Z \leq 1} \{-Z \log Z - (1 - Z) \log (1 - Z) + \alpha \log f(Z, \lambda)\} - \alpha k \log 2 \equiv h_2(\lambda, \alpha, Z) \), in which \( f(Z, \lambda) = 2^k g(N, L) \).

**Proof:** Using Stirling formula for the factorials and note that the order of logarithm of sum depends mainly on the maximum term in the sum. \( \square \)

### 4 Comparisons of Two Moments and Conclusion

We summarize the remaining steps of the argument without detail.

- \( h_2(\lambda, \alpha, \frac{1}{2}) = 2h_1(\lambda, \alpha) \).
- Unless \( Z = \frac{1}{2} \) maximizes \( h_2(\lambda, \alpha, \frac{1}{2}) \), \( \mathbb{E}^2[|\psi|] / \mathbb{E}^2[|\psi|^2] \) is exponentially small when \( N \) goes to \( \infty \).
- \( Z = \frac{1}{2} \) being a maximizer implies that \( (1 + \lambda)^{k-1} = \frac{1}{1-\lambda} \).
• while $\lambda$ satisfying last equality and $\alpha < 2^k \log 2 - k - 5$, $Z = \frac{1}{2}$ is the maximizer and meanwhile,

$$\frac{E^2[U(\psi)]}{E[U^2(\psi)]} \approx \frac{\exp(2Nh_1(\lambda, \alpha))}{\exp(Nh_2(\lambda, \alpha, 1/2))} = \Omega(1).$$

From discussion above, now we can get the main conclusion in this lecture.

**Theorem 5** The lower bound of $\alpha$, in order that a random $\text{SAT}_N(K, M)$ formula is SAT with vanishing probability in the $N \to \infty$ limit, can be reached through second moment method as: $\alpha \geq 2^k \log 2 - k - 5$.

**Remark 6** Suppose $\alpha$ such that second moment works and $\exists Z < \frac{1}{2}$, s.t. $h_2(\lambda, \alpha, Z) < 0$, then there are clusters in the space of solutions. Formally, $\exists$ pair of solutions at distance $\frac{N}{2}$, and $\nexists$ pair of solutions at distance $ZN$. 