Homework 6

Computer Science Theory for the Information Age

致远 12 级 ACM 班　　刘爽　　5112409048

June 17, 2013

1. Modify the proof that every monotone peroperty has a threshold for $G(n, p)$ to apply to the 3-CNF satisfiability problem

   Solution:

   Let's call the 3-CNF model $B(n, m)$.

   We define an increasing property of $B(n, m)$ as follows:

   > Q is an increasing property of B if when a 3-CNF B has the property any 3-CNF obtained by adding clauses to B must also have the property.

   First we will proof the following lemma:

   > If Q is an increasing property and $0 \le m_1 \le m_2 \le 1$, then the probability that $B(n, m1)$ has property Q is less than or equal to the probability that $B(n, m2)$ has property Q.

   Notice we could generate $B(n, m_2)$ in this way: First we generate $B(n, m_1)$, then we generate a set $B(n, m_2 - m_1)$ and take the intersection of them to get $B(n, m_2)$. If $B(n, m_1)$ has the property Q, $B(n, m_2)$ must has it too.

   Next we will prove

   > Every increasing property of $B(n, m)$ has a threshold at $m(n)$, where for each n, $m(n)$ is the minimum real number a for which the probability that $B(n, a)$ has the property Q is $\frac{1}{2}$.

Suppose $m_0(n)$ is any function such that

$$\lim_{n\to\infty} \frac{m_0(n)}{m(n)} = 0$$

We will show that almost surely $B(n, m_0)$ does not have property Q. Suppose this is false. Then, the probability that $B(n, m_0)$ has the property Q does not converge to zero. By the definition of limit, there must be a positive real number ϵ for which the probability that $B(n, m_0)$ has property Q is at least ϵ on an infinite set I of n.

Here we define the m-fold replication of B be the intersection of m copies of $B(n, m)$.

Let $k = \lceil (1/\epsilon) \rceil$. Let 3-CNF H be the m-fold replication of $B(n, m_0)$. Since from the m-fold method we have

$$Prob\big(B(n, km) \text{ does not have Q}\big) \leq \Big(Prob\big(B(n, m) \text{ does not have Q}\big)\Big)^k$$

Then the probability that H does not have Q is at most $(1-\epsilon)^m \leq e^{-1} \leq 1/2$ for all $n \in I$. So for these n, since $m(n)$ is the minimum real number a for which the probability that $B(n, a)$ has property Q is $1/2$, $km_0 \geq m(n)$. This implies that $\frac{m_0(n)}{m(n)}$ is at leat $1/k$ infinitely often contradicting the hypothesis that $\lim_{n\to\infty} \frac{m_0(n)}{m(n)} = 0$. A symmetric argument shows that for any $m_1(n)$ such that $\frac{m(n)}{m_1(n)} \to 0$, $B(n, m_1)$ almost surely has property Q.

2. Verify that the sum of r rank-one matrices $\sum_{i=1}^{r} \sigma_i u_i v_i^T$ can be written as UDV^T, where the u_i are the columns of U and v_i are the columns of V. To do this, first verify that for any two matrices P and Q, we have

$$PQ^T = \sum_i p_i q_i^T$$

where p_i is the i^{th} column of P and q_i is the i^{th} column of Q.

Proof:

First we will prove

$$PQ^T = \sum_i p_i q_i^T$$

Let $A = PQ^T$

Then

$$a_{ij} = \sum_{k=1}^{r} p_{ik} q_{jk}$$

Let $B = \sum_i p_i q_i^T$

Then

$$\begin{aligned} b_{ij} &= \sum_{k=1}^{r} \{p_k q_k^T\}_{ij} \\ &= \sum_{k=1}^{r} p_{ik} q_{jk} \\ &= a_{ij} \end{aligned}$$

Do some tiny modification, we can complete our proof.

Let $A = UDV^T$

Then

$$a_{ij} = \sum_{k=1}^{r} u_{ik} d_{kk} v_{jk}$$

Let $B = \sum_i \sigma_i u_i v_i^T$

Then

$$\begin{aligned} b_{ij} &= \sum_{k=1}^{r} \{\sigma_k u_k v_k^T\}_{ij} \\ &= \sum_{k=1}^{r} u_{ik} d_{kk} v_{jk} \\ &= a_{ij} \end{aligned}$$

Thus $UDV^T = \sum_{i=1}^{r} \sigma_i u_i v_i^T$

$\square$