Advanced Graph Algorithms Jan-Apr 2014

Lecture 27 — May 11, 2014

Lecturer: Saket Saurabh *Scribe: Prafullkumar P Tale*

1 Introduction

Recall the randomized algorithm we used in lecture number 22.

Input: Two nxn matrices A and B over $0, 1$
Output: Witness matrix W for the Boolean matrix $C = AB$
$W \leftarrow -AB$
for $t \leftarrow 0$ **to** $\log n$ **do**
  $r \leftarrow 2^t$
  repeat
    Choose Random $R \subseteq \{1, \ldots, n\}$ with $|R| = r$
    Compute A^R and B^R
    $Z \leftarrow A^R B^R$
    forall the *(i, j)* **do**
      if $W_{ij} < 0$ *and* Z_{ij} *is witness* **then**
        $W_{ij} \leftarrow Z_{ij}$
      end
    end
  until $\lceil 3.77 \log n \rceil$ *times*;
  forall the *(i, j)* **do**
    if $W_{ij} < 0$ **then**
      find witness W_{ij} by brute force
    end
  end
end

Algorithm 1: Algorithms to compute Witness Matrix

Like the above algorithm, every randomized algorithms can be viewed as a two-stage procedure in which first a *sample point/set* is chosen at random (in this case R) and next a deterministic procedure is applied to it. In the generic case the sample point is an arbitrary string of specific length (say n), the sample space consists of the set of all 2^n strings, and *choosing a sample at random* amounts to taking the outcome of n consecutive unbiased coin tosses. However, as observed by M. Luby , in many cases the algorithm behaves as well when the sample is chosen from a much smaller sample space. If points in the smaller sample space can be compactly represented and generated then this yields a saving in the number of coin tosses required for the procedure.

The construction of small sample spaces which have some randomness properties is of major theoretical and practical importance. A typical property is that the probability distribution, induced on every k bit locations in a string randomly selected in the sample space, should be uniform. Such a sample space is called k-wise independent. Loosely speaking, the probability distribution induced

on every k bit locations in the sample string is not uniform but statistically close to it then we call it, almost k-wise independent.

In his paper[Lub86], Luky developed a general technique which converts a probability space with a large sample space where events are mutually independent to a new probability space with a very small sample space where events are pairwise independent. Alon, Babai and Itai [ABI86] presented an efficient construction of k-wise independent sample spaces of size approximately $n^{k/2}$. This result is very close to best possible, in view of the lower bound of presented in this paper [CGH$^+$85]. This fact led Naor and Naor to introduce the notion of *almost k-wise independent* sample spaces [NN93]. Today, we will present three alternative construction of sample spaces which was presented in this paper [AGHP90].

First we will see some basic definitions followed by three constructions of smaller sample space. We will tie all the results together with the theorem.

2 Preliminaries

A sample space which is contained in $\{0,1\}^n$ will be sub-indexed by n. The super-index will usually represent an upper bound on the logarithm (to base 2) of the cardinality of the sample space. Hence, S_n^m denotes a sample space of $\leq 2^m$ strings each of length n.

2.1 Definitions

Definition 1 (k-wise Independence)**.** *A sample space S_n is k-wise independent if when $X = x_1 \dots x_n$ is chosen uniformly from S_n then for any k positions $i_1 < i_2 < \cdots < i_k$ and any k-bit string α, we have*

$$Pr[x_{i1}x_{i2}\dots x_{ik} = \alpha] = 2^{-k}$$

Definition 2 (Almost k-wise Independence in max norm)**.** *Let S_n be sample space and $X = x_1 \dots x_n$ be chosen uniformly from S_n. S_n is (ϵ, k) independent in max norm if for any k positions $i_1 < i_2 < \cdots < i_k$ and any k-bit string α, we have*

$$|Pr[x_{i1}x_{i2}\dots x_{ik} = \alpha] - 2^{-k}| \leq \epsilon$$

Definition 3 (Almost k-wise Independence in L_1 norm(Statistical closeness))**.** *Let S_n be sample space and $X = x_1 \dots x_n$ be chosen uniformly from S_n. S_n is ϵ-away in L_1 norm if for any k positions $i_1 < i_2 < \cdots < i_k$ we have*

$$\sum_{a \in \{0,1\}^k} |Pr[x_{i1}x_{i2}\dots x_{ik} = \alpha] - 2^{-k}| \leq \epsilon$$

If S_n is (ϵ, k)-independent in max norm then it is at most $2^k\epsilon$-away in L_1 form from k-wise independence, whereas if S_n is ϵ-away in $L1$ norm from k-independence then it is (ϵ, k)-independent in max norm.

Definition 4 (Quadratic residue)**.** *An integer q is called a quadratic residue modulo n if if there exists an integer x such that $x^2 \equiv q \pmod{n}$. Otherwise, q is called a quadratic non-residue modulo n.*

The Quadratic Residue or Character is also denoted by $\chi_p(x)$. One of the property we will use is $\chi_p(xy) = \chi_p(x)\chi_p(y)$.

Definition 5 (Galois Field)**.** *Galois field is a field that contains a finite number of elements.*

$GF(p)$ is the Galois field of p elements with addition modulo p operation.

2.2 Linear Test

Let $(\alpha, \beta)_2$ denote the inner-product mod 2 of the binary vectors α and β i.e. $(\alpha_1, \alpha_2 \ldots \alpha_n, \beta_i \ldots \beta_n)_2 = \sum \alpha_i \beta_i \bmod 2$.

A 0-1 random variable X is called ϵ-biased if $|Pr[X = 0] - Pr[X = 1]| \leq \epsilon$.

Let S_n be a sample space and $X = x_1 \ldots x_n$ be chosen uniformly from S_n. The sample space S_n is said to be ϵ-biased with respect to linear tests if for every $\alpha = \alpha_1 \ldots \alpha_n \in \{0,1\}^n - \{0\}^n$ the random variable $(\alpha, X)_2$ is ϵ-biased.

The sample space S_n is said to be ϵ-biased with respect to linear tests of size at most k if for every $\alpha = \alpha_1 \ldots \alpha_n \in \{0,1\}^n - \{0\}^n$ such that at most k of the α_i are one, the random variable $(\alpha, X)_2$ is ϵ-biased.

2.3 Lemmas

Lemma 6 (Vazirani)**.** *Let $S_n \subset \{0,1\}^n$ be a sample space that is ϵ-biased with respect to linear tests. Then, for every k, the sample space S_n is $((1 - 2^{-k})\epsilon, k)$-independent (in max norm), and $(2^k - 1)^{1/2}\epsilon$-away (in L_1 norm) from k-wise independence.*

In the applications of the lemma we will use the bounds ϵ and $2^{k/2}\epsilon$ respectively, since the difference is minimal.

Using the construction in [ABI86] we get:

Lemma 7 (Naor and Naor)**.** *Let $k < n$ be an odd integer and $N \leq 2^{\frac{2(n-1)}{(k-1)}} - 1$. Let $S_n^m \subseteq \{0,1\}^n$ be a sample space of cardinality 2^m that is ϵ-biased with respect to linear tests. One can construct $R_N^m \subseteq \{0,1\}^N$ of cardinality 2^m such that R_N^m is a sample space (ϵ, k)-independent (in max norm), and $2^{k/2}\epsilon$ -away (in L_1 norm) from k-wise independence.*

Hence, an (ϵ, k)-independent sample space on N bits can be constructed using $\mathcal{O}(loglogN + logk + log\frac{1}{\epsilon})$ random bits instead of $\mathcal{O}(logN + logk + log\frac{1}{\epsilon})$ random bits.

In view of lemma 7, the main part of the paper deals merely with the construction of small sample spaces which have small bias with respect to linear tests.

Theorem 8 (Weil)**.** *Let p be an odd prime. Let $f(t)$ be a polynomial over $GF(p)$ which is not the square of another polynomial and has precisely n distinct zeros. Then,*

$$\Big| \sum_{x \in GF(p)} \chi_p(f(x)) \Big| \leq (n-1)\sqrt{p}$$

3 Construction

The i^{th} bit in the j^{th} sample string, in our sample space, will be $\chi_p(i+j)$. A translation from sequences to $\{0,1\}$ sequences can be easily effected.

The sample space $B_n^{\log(p)}$ consists of p strings each of length n. Let $x \in \{0,1,\ldots,p-1\}$ and $i \in \{0,1,\ldots,n-1\}$. x^{th} string is given by $r(x) = r_0(x)r_1(x)\ldots r_{n-1}(x)$.

$$r_i(x) = \begin{cases} 1 & \text{if } \chi_p(x+i) = 0 \\ (1-\chi_p(x+i))/2 & \text{otherwise} \end{cases}$$

Hence, the size of the sample space $B_n^{\log(p)}$ is exactly p.

Proposition 9. *The sample space $B_n^{\log(p)}$ is $\left(\frac{n-1}{\sqrt{p}} + \frac{n}{p}\right)$-biased with respect to linear tests.*

Proof. We need to prove that for any nonzero α the random variable $(\alpha, r)_2$ is $\left(\frac{n-1}{\sqrt{p}} + \frac{n}{p}\right)$-biased when $r(x)$ is selected uniformly in $B_n^{\log(p)}$. The bias of $(\alpha, r)_2$ equals the expectation of $(-1)^{(\alpha,r)_2}$ taken over all possible $r(x)$. Hence the bias is

$$\begin{aligned} &= \frac{1}{p}\Big|\sum_{x\in GF(p)} (-1)^{(\alpha,r(x))_2}\Big| \\ &= \frac{1}{p}\Big|\sum_{x\in GF(p)} (-1)^{\sum_{i=0}^{n-1}\alpha_i r_i(x)}\Big| \\ &= \frac{1}{p}\Big|\sum_{x\in GF(p)} (-1)^{\alpha_0 r_0(x)} \times (-1)^{\alpha_1 r_1(x)} \times \cdots \times (-1)^{\alpha_{n-1} r_{n-1}(x)}\Big| \end{aligned}$$

When $\chi_p(x+i)$ is not equal to zero, $\chi_p(x+i) = (-1)^{r_i(x)}$. Also, $\chi_p(x+i)$ is zero at most n number of times.

$$\begin{aligned} &\leq \frac{1}{p}\Big|\sum_{x\in GF(p)} \chi_p(x+0)^{\alpha_0}\chi_p(x+1)^{\alpha_1}\ldots\chi_p(x+i)^{\alpha_{n-1}}\Big| + \frac{n}{p} \\ &\leq \frac{1}{p}\Big|\sum_{x\in GF(p)} \chi_p\Big(\prod_{i=0}^{n-1}(x+i)^{\alpha_i}\Big)\Big| + \frac{n}{p} \end{aligned}$$

Consider the function $f(x) = \prod_{i=0}^{n-1}(x+i)^{\alpha_i}$, it can't be written as square of any other polynomial and it has exactly $n'(\leq n)$, roots. Hence by Weil's theorem (8),

$$\text{Bias of } (\alpha, r(x))_2 \leq \frac{(n-1)}{\sqrt{p}} + \frac{n}{p}$$

□

Using Vazirani's lemma (6), we can see that $B_n^{\log p}$ is almost k-wise independent.

References

[ABI86] Noga Alon, László Babai, and Alon Itai. A fast and simple randomized parallel algorithm for the maximal independent set problem. *Journal of algorithms*, 7(4):567–583, 1986.

[AGHP90] Noga Alon, Oded Goldreich, Johan Hastad, and René Peralta. Simple construction of almost k-wise independent random variables. In *Foundations of Computer Science, 1990. Proceedings., 31st Annual Symposium on*, pages 544–553. IEEE, 1990.

[CGH+85] Benny Chor, Oded Goldreich, Johan Hasted, Joel Freidmann, Steven Rudich, and Roman Smolensky. The bit extraction problem or t-resilient functions. In *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pages 396–407. IEEE, 1985.

[Lub86] Michael Luby. A simple parallel algorithm for the maximal independent set problem. *SIAM journal on computing*, 15(4):1036–1053, 1986.

[NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM journal on computing*, 22(4):838–856, 1993.