MTH 995-003: Intro to CS and Big Data Spring 2014

Lecture 26 — April 03, 2014

Inst. Mark Iwen *Scribe: Ashwini Maurya*

1 Homework

This set of homework is due by **Thursday, April 17**.

Problem Set-up: Fix $\omega \in [N] = \{0, 1, 2, \ldots, N-1\} - \{0\}$, consider the random variable

$$X_l := e^{\frac{2\pi i u_l w}{N}}$$

where u_l is uniformaly chosen from $[N]$, $\forall \;\; l \in [m]$.

Q1. Prove that

$$E\Big[\frac{1}{m} Re\{X_l\}\Big] = E\Big[\frac{1}{m} Im\{X_l\}\Big] = 0$$

Q2. Use theorem 2 from lecture 11 (Bernstein's Inequality/theorem) twice to show that:

$$P\left[\frac{1}{m}\left|\sum_{l\in[m]} X_l\right| \geq \mu\right] \leq \frac{p}{N-1}$$

whenever $m \geq \frac{8 \;\ln\left(\frac{4(n-1)}{p}\right)}{\mu^2}$.

Q3. Let $A \in \mathbb{C}^{m\times N}$ be defined as

$$A_{l,w'} := \frac{e^{\frac{2\pi i u_l w'}{N}}}{\sqrt{m}}; \qquad for \;\; l \;\in [m] \; and \; w' \in [N]$$

a) Show that the columns of A are ℓ_2-normalized.

b) Then show that $\mu(A) < \epsilon$, with probability at least $1-p$, whenever $m \geq \frac{8 \;\ln\left(\frac{4(N-1)}{p}\right)}{\epsilon^2}$

Q4. **a)** How large does m have to be before $\epsilon_k(A) < \epsilon$ is implied by the coherence?

(*Hint: Refer to Lecture 25*)

b) Going back to *BOS*(Bounded Orthonormal Set), how much larger is m than it is to be?

Q5. Do *Problem 5.1* on page 129 of the book.

Note: Consider subgaussian random matrices $A \in \mathbb{R}^{m\times N}$. Note that since each entry is a random subgaussian and therefore unstructured. To store the all matrix entries to a precision of 2^{-s} takes total $O(mNs)$ bits. Consider the $Q.3$ matrix, It can be stored using $O(m\log(N))$-bits. Also the value of m from $Q.4$ is not too large in terms of μ.

2 Deterministic Constructions

In **today's lecture**, we would like to develop binary matrices $\{0,1\}^{m\times N}$ with both small m and *small* coherence. One of the main advantages of these matrices is that they will also be very compact to store (requiring very few bits to remember). The entries of these matrices will also always be either 0 or 1, which will give them useful combinatorial properties.

Definition 1. *Let $K, \alpha \in N$. Let $A \in \{0,1\}^{m\times N}$, where $m \leq N$, is (K,α)-coherent if both:*

a) *Every column of A has at least K $1's$.*

b) *Every pair of columns of A, $\vec{a_j}$ & $\vec{a_l} \in \{0,1\}^N$, $j \neq l$, have*

$$< \vec{a_j}, \vec{a_l} > \leq \alpha$$

Let $\tilde{A}$ be A with its columns ℓ_2-normalized. We have

$$\mu(\tilde{A}) \leq \frac{\alpha}{K}$$

Below we give two examples of (K,α)-coherent matrices.

Rapid Review

A finite field, F, of prime order P is essentially $\mathbb{Z}_P$, or, $[P] := \{0,\ldots,P-1\}$ with multiplication, division, addition, and subtraction. That is, for $a, b \in [P]$

$$a \pm b = (a \pm b) \bmod P, \qquad ab = (ab) \bmod P,$$
$$\frac{a}{b} = c \in [P] \text{ such that } bc = a \bmod P.$$

The field, F, behaves a lot like $\mathbb{Q} \subset \mathbb{R}$ with respect to algebraic solutions of simple polynomial equations.

Example 1 (See [1])**.** *Let $P \in [N]$ be a prime number. Let F be the finite field of order P.*

Let

$$\theta_j(X) := j_0 + j_1 X + j_2 X^2 + \cdots + j_{\lceil \log_P N\rceil - 1} X^{\lceil \log_P N\rceil - 1} \qquad \forall j \in [N].$$

where $j_0, j_1, ..., j_{\lceil \log_P N \rceil - 1}$ *are digits of* j *base* P*, i.e.,*

$$j = j_0 + j_1 P + j_2 P^2 + \cdots + j_{\lceil \log_P N \rceil - 1} P^{\lceil \log_P N \rceil - 1}.$$

Create $A = (\vec{a_1}, \vec{a_2}, ..., \vec{a_N}) \in \{0,1\}^{m \times N}$, $m = P^2$*, by letting*

$$(\vec{a_j})_{l+bP} = \begin{cases} 1 & \text{if } \theta_j(b) = l \\ 0 & \text{otherwise.} \end{cases}$$

So, if we split $\vec{a}_j$ *into* P *blocks of length* P*, each block will contain exactly one '*1*'.*

More specifically, block k *will have its* 1 *non-zero entry located at* $\theta_j(k)$*. Thus, we have*

$$\vec{a_j} = \begin{pmatrix} 0 & \\ \vdots & \\ 1 & \Leftarrow (\text{in entry } \theta_j(0)) \\ \vdots & \\ 0 & \\ 0 & \\ \vdots & \\ 1 & \Leftarrow (\text{in entry } \theta_j(1)) \\ \vdots & \\ 0 & \\ \vdots & \\ \vdots & \\ 0 & \\ \vdots & \\ 1 & \Leftarrow (\text{in entry } \theta_j(P-1)) \\ \vdots & \\ 0 & \end{pmatrix}.$$

Note that:

- *Every single column of* A *has exactly* P *1's.*
- $< a_j, a_l >$ *for* $\neq j$ *is # of elements of* $b \in [P]$ *with* $\theta_j(b) = \theta_l(b)$*. This equality happens only if* $(\theta_j - \theta_l)(b) = 0$*. Since* $\theta_j - \theta_l$ *is a polynomial of degree at most* $\lceil \log_P N \rceil - 1$*. Thus,* $\theta_j - \theta_l$ *can have at most* $\lceil \log_P N \rceil - 1$ *zeroes. Therefore,* $< a_j, a_l > \leq \alpha := \lceil \log_P N \rceil - 1$ *works as a coherence bound.*
- A *is therefore* $\left(P, \lfloor \frac{\ln N}{\ln P} \rfloor\right)$*-coherent. This implies that* $\mu(A)$ *is like* $O(\frac{\ln N}{P \ln P})$ *after normalizing its columns. Since* $m = P^2$ *we can see that this is pretty good...*
- *It can be stored in only* $O(\log N)$ *bits!*

Example 2 (A Fourier-friendly (K, α)-coherent matrix)**.** *Let* $p_0 = 1$, $p_1 = 2$ *,*$p_2 = 3, p_3 = 5 \cdots$ *where* $p_l = l^{th}$ *prime. Choose some* $q, K \in [N]$ *and consider* $p_q, ..., p_{q+K-1}$*, setting* $m = \sum_{l \in [K]} p_{q+l}$*.*

Define $A \in \{0,1\}^{m \times N}$ *by*

$$A_{(l,h),j} = \begin{cases} 1 & \text{if } j = h \bmod (p_{q+l}) \\ 0 & \text{otherwise.} \end{cases}$$

here $l \in [K]$ *and* $h \in [P_{q+l}]$. *For example, if* $p_q = 2$ *and* $p_{q+1} = 3$, *we have*

$$A = \begin{pmatrix} 0 \bmod 2 & 1 & 0 & 1 & 0 & 1 & 0 \cdots \\ 1 \bmod 2 & 0 & 1 & 0 & 1 & 0 & 1 \cdots \\ 0 \bmod 3 & 1 & 0 & 0 & 1 & 0 & 0 \cdots \\ 1 \bmod 3 & 0 & 1 & 0 & 0 & 1 & 0 \cdots \\ 2 \bmod 3 & 0 & 0 & 1 & 0 & 0 & 1 \cdots \end{pmatrix}.$$

Every columns has exactly K $1's$.

- $< a_j, a_l >=$ *# of primes* $\tilde{p} \in \{p_q, p_{q+1}, \cdots, p_{q+K-1}\}$ *with* $l \equiv j \bmod \tilde{p}$
- *If* $j \neq l$ *then # of* $\tilde{p}'s$ *can be at most be* α *where*

$$\alpha = \min\left\{c \in [K] \middle| p_q p_{q+1} \cdots p_{q+c} \geq N\right\}$$

$$\implies \alpha \leq \lfloor \tfrac{\ln N}{\ln P} \rfloor \text{ by the Chinese Remainder Theorem.}$$

This matrix is "Fourier friendly", because for $\tilde{N} = \prod_{l \in [K]} p_{q+l}$, *the periodic extension of* A, $\tilde{A} \in \{0,1\}^{m \times \tilde{N}}$ *where*

$$\tilde{A}_{(l,h),j} = \begin{cases} 1 & \text{if } j = h \bmod (p_{q+l}) \\ 0 & \text{otherwise.} \end{cases}$$

- $\tilde{A}$ *is Fourier friendly because* $\tilde{A}F_{\tilde{N}} \in \mathbb{C}^{m \times \tilde{\mathbb{N}}}$ *is very sparse, where* $F_{\tilde{N}} \in \mathbb{C}^{\tilde{N} \times \tilde{N}}$ *is a Discrete Fourier Transform matrix.*

Homework

Q.6 a) Show that the (l,h)-row of $\tilde{A}F_{\tilde{N}}$ has exactly p_{q+l} non-zero entries in it.

b) Show that only m columns of $\tilde{A}F_{\tilde{N}}$ have non-zero entries in them.

References

[1] Ronald A. DeVore. Deterministic constructions of compressed sensing matrices. Journal of Complexity, 2007.