Stanford University	**Spring 2016**
Math 233: Non-constructive methods in combinatorics	**Instructor: Jan Vondrák**
Lecture date: May 11, 2016	**Scribe: Scott Mutchnik**

Lecture 14. Real-rooted Polynomials

We turn to discussing problems whose solution relies on controlling the roots of certain polynomials. Ultimately we seek to present the proof of the Kadison-Singer conjecture. We are especially interested in *real-rooted* polynomials (real polynomials all of whose roots are real), and their complex-variable generalization known as *stable* polynomials.

14.1. Bernoulli variables and real-rooted polynomials

We begin by studying real-rooted polynomials. Consider the following example.

Let $X = \sum_{i=1}^{n} X_i$ where the X_i are independent Bernoulli random variables equal to 1 with probability $b_i \in [0,1]$ and 0 with probability $1 - b_i$. Furthermore, let $p_k = \Pr[X = k]$. The distribution of X should be roughly Gaussian as $n \to \infty$. Here, we shall show that $(p_k)_{k=0}^{n}$ is log-concave (that is, $p_k^2 \geq p_{k-1}p_{k+1}$ for $1 \geq k \geq n-1$) and thus unimodal. How do we prove this? Define

$$P(x) = \mathbb{E}[x^X] = \sum_{k=0}^{n} p_k x^k.$$

By studying $P(x)$ we gain information about the p_k, and thus the distribution of X.

Lemma 10.1 *P(x) is real-rooted.*

Proof: We have that for $0 \leq k \leq n$, p_k is the summation, over $S \subseteq [n]$ of size k, of the probability that exactly the X_i for $i \in S$ are equal to 1, which is $b^S(1-b)^{[n]\setminus S}$ (where $b^S = \prod_{i \in S} b_i$, and $(1-b)^S$ and later $(bx)^S$ are defined similarly). So,

$$P(x) = \sum_{i=0}^{n} p_k x^k = \sum_{i=0}^{n} \sum_{\substack{S \subseteq [n] \\ |S|=k}} (bx)^S (1-b)^{[n]\setminus S} = \prod_{i=1}^{n} (b_i x + (1-b_i)) = \prod_{i=1}^{n} b_i \prod_{j=1}^{n} \left(x + \frac{1-b_j}{b_j} \right).$$

We see that $\lambda_i = \frac{b_i - 1}{b_i}$ is a root of $P(x)$ for $1 \leq i \leq n$, and so P has n real roots (including multiplicities). □

The real-rootedness of P implies the following classical inequalities.

Theorem 10.2 (Newton's Inequalities): *If* $P(x) = \sum_{k=0}^{n} p_k x^k$ *is real-rooted,* $p_k \geq 0$*, then*

$$\left(\frac{p_k}{\binom{n}{k}} \right)^2 \geq \frac{p_{k-1}}{\binom{n}{k-1}} \frac{p_{k+1}}{\binom{n}{k+1}}$$

for $1 \leq k \leq n-1$.

We postpone the proof for a bit and see first what implications this has.

Corollary 10.3 *If $P(x) = \sum_{k=0}^{n} p_k x^k$ is real-rooted, $p_k \geq 0$, then $(p_k)_{k=0}^{n}$ is log-concave.*

Proof: By Theorem 10.2, for $1 \leq k \leq n-1$, $(\frac{p_k}{\binom{n}{k}})^2 \geq \frac{p_{k-1}}{\binom{n}{k-1}} \frac{p_{k+1}}{\binom{n}{k+1}}$, so $p_k^2 \geq \frac{\binom{n}{k}^2}{\binom{n}{k-1}\binom{n}{k+1}} p_{k-1}p_{k+1}$. We have $\frac{\binom{n}{k}^2}{\binom{n}{k-1}\binom{n}{k+1}} = \frac{\binom{n}{k}}{\binom{n}{k-1}} \frac{\binom{n}{k}}{\binom{n}{k+1}} = \frac{n-k+1}{k} \frac{k+1}{n-k} = \frac{n-k+1}{n-k} \frac{k+1}{k} = (1 + \frac{1}{n+k})(1 + \frac{1}{k}) > 1$, so $p_k^2 > p_{k-1}p_{k+1}$. □

Corollary 10.4 *Let $X = \sum_{i=1}^{n} X_i$ where the X_i are independent Bernoulli random variables equal to 1 with probability $b_i \in [0,1]$ and 0 with probability $1 - b_i$, and $p_k = \Pr[X = k]$. Then $(p_k)_{k=0}^{n}$ is log-concave.*

Proof: Same as above. □

To prove Theorem 10.2 we begin by observing some basic properties of real-rooted polynomials that allow new real-rooted polynomials to be obtained from old ones; we will also introduce the concept of interlacing polynomials, though this concept is not necessary for the proof.

Definition 10.5 *Let $Q(x)$ be a degree-$(n-1)$ real-rooted polynomial with (not necessarily distinct) roots $\mu_{n-1} \leq \ldots \leq \mu_1$ and $P(x)$ a degree-n real-rooted polynomial with roots $\lambda_n \leq \ldots \leq \lambda_1$. Then the roots of $Q(x)$ **interlace** those of $P(x)$ if $\lambda_n \leq \mu_{n-1} \leq \lambda_{n-1} \leq \ldots \leq \lambda_2 \leq \mu_1 \leq \lambda_1$.*

We make two observations about real-rooted polynomials.

(1) *If $P(x)$ is real-rooted then so is $P'(x)$, and the roots of $P'(x)$ interlace those of $P(x)$.*
To see this, let $\lambda_n \leq \ldots \leq \lambda_1$ be the roots of $P(x)$. If $\lambda_{k+1} > \lambda_k$ are consecutive distinct roots of $P(x)$, then $P(x)$ attains a critical point at some μ_k with $\lambda_{k+1} > \mu_k > \lambda_k$ at which $P'(x) = 0$. If $\lambda_{k+l} = \ldots = \lambda_k$ is an l-tuple root of $P(x)$, then it is also an $l-1$-tuple root of $P'(x)$, and considering these $l-1$ roots of $P'(x)$ as $\mu_{k+l-1} = \ldots = \mu_k$ with $\lambda_{k+l} = \mu_{k+l-1} = \lambda_{k+l-1} \ldots = \mu_k = \lambda_n$ (so perhaps as "infinitesimally close" interlacing roots) we have then accounted for $n-1$ real roots of the consequently real-rooted polynomial $P'(x)$, which interlace the roots of $P(x)$.

(2) *If $P(x) = \sum_{k=0}^{n} p_k x^k$ is a real-rooted polynomial of degree n, then $x^n P(\frac{1}{x}) = \sum_{k=0}^{n} p_{n-k} x^k$ (which is $P(x)$ with the coefficients in reverse order) is a real-rooted polynomial of degree at most n with roots the inverses of the nonzero roots of $P(x)$.*
This is because if $P(x) = \prod_{i=1}^{n}(x - \lambda_i)$ then $x^n P(\frac{1}{x}) = x^n \prod_{i=1}^{n}(\frac{1}{x} - \lambda_i) = \prod_{i=1}^{n}(1 - \lambda_i x)$, which is clearly real-rooted with roots the inverses of the nonzero λ_i. Note that if some of the λ_i are zero then $x^n P(\frac{1}{x})$ has a lower degree than $P(x)$.

Now to show Newton's inequalities for the coefficients p_{k-1}, p_k, p_{k+1} of $P(x)$ we will seek to extract a real-rooted polynomial from $P(x)$ with only these three coefficients, and obtain information about these coefficients from the real-rootedness of this polynomial.

Proof: Let $1 \leq k \leq n-1$. Then differentiating $P(x)$ $k-1$ times, we obtain

$$Q(x) = P^{(k-1)}(x) = (k-1)!p_{k-1} + k!p_k x + \frac{(k+1)!}{2} p_{k+1} x^2 + \ldots + x^{n-k+1}$$

which is real-rooted as we argued above. Note that $(k-1)!p_{k-1}$, $k!p_k x$ and $\frac{(k+1)!}{2}p_{k+1}x^2$ come from $p_{k-1}x^{k-1}$, $p_k x^k$ and $p_{k+1}x^{k+1}$ respectively; the other coefficients of $Q(x)$ are of no interest here. Now reversing the coefficients of $Q(x)$:

$$R(x) = x^{n-k+1}Q\left(\frac{1}{x}\right) = (k-1)!p_{k-1}x^{n-k+1} + k!p_k x^{n-k} + \frac{(k+1)!}{2}p_{k+1}x^{n-k-1} + \ldots + 1$$

is real-rooted again. Differentiating $n-k-1$ times, we obtain

$$R^{(n-k-1)}(x) = \frac{(n-k-1)!}{2}(k-1)!p_{k-1}x^2 + (n-k)!k!p_k x + (n-k-1)!\frac{(k+1)!}{2}p_{k+1}.$$

This is a real-rooted quadratic, so its discriminant is nonnegative:

$$((n-k)!k!p_k)^2 - 4\left(\frac{(n-k-1)!}{2}(k-1)!p_{k-1}\right)\left((n-k-1)!\frac{(k+1)!}{2}p_{k+1}\right) \geq 0.$$

Dividing by $n!^2$, we get

$$\left(\frac{p_k}{\binom{n}{k}}\right)^2 \geq \frac{p_{k-1}}{\binom{n}{k-1}}\frac{p_{k+1}}{\binom{n}{k+1}}.$$

□

Furthermore, the real-rooted polynomials with nonnegative coefficients are, essentially, exactly those given by independent Bernoulli variables. That is, we have the following converse to Lemma 10.1.

Lemma 10.6 *Let $P(x) = \sum_{k=0}^n p_k x^k$, $p_k \geq 0$ for $0 \leq k \leq n$, $p(1) = 1$ be a real-rooted polynomial. Then there are independent Bernoulli variables Z_i such that $p_k = \Pr[\sum_{i=1}^n Z_i = k]$ for $0 \leq k \leq n$.*

Proof: Since $P(x)$ is real-rooted, there are $\lambda_1, \ldots, \lambda_n$ and C such that $P(x) = C\prod_{i=1}^n(x+\lambda_i)$. Thus $P(1) = C\prod_{i=1}^n(1+\lambda_i)$ so $C = \frac{P(1)}{\prod_{i=1}^n(1+\lambda_i)} = \frac{1}{\prod_{i=1}^n(1+\lambda_i)}$ by assumption. Hence $P(x) = \prod_{i=1}^n(\frac{x+\lambda_i}{1+\lambda_i}) = \prod_{i=1}^n(\frac{x}{1+\lambda_i} + (1-\frac{1}{1+\lambda_i}))$. Since $\frac{1}{1+\lambda_i} \in [0,1]$ as $\lambda_i \geq 0$ (since $P(x)$ has nonnegative coefficeients, so no positive roots), we can choose Z_i for $1 \leq i \leq n$ to be equal to 1 with probability $\frac{1}{1+\lambda_i}$ and 0 with probability $1 - \frac{1}{1+\lambda_i}$, and the result follows from the computation done in the proof of Lemma 10.1. □

Relating real-rooted polynomials to independent Bernoulli variables can give us results about the polynomials themselves. For example, using the Chernoff bound we have the following:

Corollary 10.7 *Let $P(x)$ be as in Lemma 10.6, so there exist Z_i as in Lemma 10.6, and λ_i as in the proof of Lemma 10.6. Then for $\mu = \sum_{i=1}^n \frac{1}{1+\lambda_i} = \mathbb{E}[\sum_{i=1}^n Z_i]$, $0 < \varepsilon < 1$ we have*

$$\sum_{n \geq k > (1+\varepsilon)\mu} p_k = \Pr[\sum_{i=1}^n Z_i > (1+\varepsilon)\mu] < e^{-\varepsilon^2\mu/3},$$

$$\sum_{0 \leq k < (1+\varepsilon)\mu} p_k = \Pr[\sum_{i=1}^n Z_i < (1-\varepsilon)\mu] < e^{-\varepsilon^2\mu/2}.$$

14.2. Computability of real-rootedness

It turns out that it is computable in polynomial time whether a given polynomial is real-rooted.

Definition 10.8 *For a matrix $A \in \mathbb{C}^{m\times n}$, A^* denotes the matrix with entries $(A^*)_{ij} = \overline{A_{ji}}$ (transpose and complex conjugate). A matrix $H \in \mathbb{C}^{n\times n}$ is Hermitian if $H^* = H$.*

Definition 10.9 *Let $H \in \mathbb{C}^{n\times n}$ be a Hermitian matrix. Then H is* ***positive-semidefinite*** *if for all $\mathbf{x} \in \mathbb{C}^n$, $\mathbf{x}^* H \mathbf{x} \geq 0$.*

We state without proof the following theorem providing a computable criterion for real-rootedness.

Theorem 10.10 [Hermite-Sylvester]
Let $P(x) = \prod_{i=1}^n (x-\lambda_i)$, with $\lambda_i \in \mathbb{C}$. Then $P(x)$ is real-rooted if and only if $H = (m_{i+j-2})_{i,j=1}^n$ is positive-semidefinite, where $m_k = \sum_{i=1}^n \lambda_i^k$.

Let us write $P(x)$ in the form $P(x) = \sum_{k=0}^n (-1)^k e_k x^{n-k}$. It may seem that computing the m_k relies on determining the roots of $P(x)$, which is computationally hard. But in fact the m_k can be computed efficiently from *Newton's identities*:

$$m_k = (-1)^{k-1} k e_k + \sum_{i=1}^{k-1} (-1)^{k-1+i} e_{k-i} m_i.$$

Also, it can be checked in polynomial time whether a given matrix is *positive-semidefinite*. We conclude that it can be checked in polynomial time whether a given polynomial $P(x)$ is real-rooted.