# Lecture 5: Voting Polynomials

Scribe: Jing-Tang Keith Jang

February 3, 2005

In this lecture, we will talk more about representing Boolean functions as polynomials. In particular, we shall study the voting polynomial, which was proposed by Aspnes, Beigel, Furst, and Rudich[1]. The central idea is parity and approximation representations: how much can we lower the degree of the polynomial but still get the correct parity?

## 1 Voting Puzzles

**Puzzle 1** Suppose we have $n$ people, and everyone's forehead is labelled by a random bit in $\{0, 1\}$. For each person, he can see other people's foreheads but not his own. Then these $n$ people vote the parity and get the majority of the votes. No communications between them are allowed, and the votes are done in private. Our goal is to find an optimal strategy (must be deterministic) that gives them the right vote with high probability. Assume that there will be no tie.

**Strategy 1A** Look at the people around you. Take the majority you see, and assume that bit is also on your forehead and vote accordingly. If you see the same number of 0's and 1's, then cast a vote of 0.

**Analysis of 1A** In the case that the numbers of 0's and 1's differ by more than one, the majority bit each person sees is the same as the actual majority bit. So this strategy succeeds.

In the case where the number of 0's is exact one more than the number of 1's, the majority of the people will cast a vote of 0. So we still have a working strategy.

In the case where the number of 0's is exact one less than the number of 1's, the people with 0's on their foreheads will vote 1, and those with 1's on their foreheads will vote 0. The majority vote is 0, which is wrong. This failure happens in $\binom{n}{\frac{n}{2}}$ out of $2^n$ cases, so the probability of failure is

$$\begin{aligned}
\frac{\binom{n}{\frac{n}{2}}}{2^n} &= \frac{\frac{n!}{(\frac{n}{2})!(\frac{n}{2})!}}{2^n} \\
&\simeq \frac{\sqrt{2\pi n}(\frac{n}{e})^n}{2^n \cdot \sqrt{2\pi \frac{n}{2}}(\frac{n}{2e})^{\frac{n}{2}} \cdot \sqrt{2\pi \frac{n}{2}}(\frac{n}{2e})^{\frac{n}{2}}} \text{ by the Stirling formula} \\
&= \theta\left(\frac{1}{\sqrt{n}}\right).
\end{aligned}$$

So the strategy succeeds with a probability of $1 - \theta(\frac{1}{\sqrt{n}})$.

**Strategy 1B** Suppose that we have $n = 2^k - 1$ people for the moment. First we group the people in the increasing power of 2. So we have $k$ groups, and group $i$ has $2^i$ people, where $0 \leq i \leq k-1$. Furthermore, we divide the $i$th group ($i \geq 2$) into two smaller groups of the same size, the 0-half and the 1-half. Let $P_i$ denote the parity of the forehead bits in group $i$. Our strategy works as follows. For the people in group $i$, they check if there is a group $j$ with $j < i$ and $P_j = 0$. If there is such a group, then the 0-half in group $P_i$ vote 0 and the 1-half vote 1. If no such group exists, then the $i$th group will assume its own parity to be 0 and vote accordingly.

**Analysis of 1B** Suppose that we have $P_i = 0$ for some $i$. Let $i$ denote the lowest number such that $P_i = 0$. For any group $j < i$, each person voted incorrectly since he assumed the parity of his group to be 0. This accounts for $2^i - 1$ incorrect votes. However, there are $2^i$ correct votes from group $i$, so there is exact one more correct vote than incorrect votes in groups $0, \ldots, i$. For any group $j$ such that $j > i$, the votes in group $j$ cancel out. So the strategy works in this case.

On the other hand, if $P_i = 1$ for all $i$, then a group would cast incorrect votes after they have checked the parities of less-numbered groups. The probability for this failure is $\frac{1}{2^k} = \frac{1}{n+1}$. So the probability for this strategy to succeed is $1 - \frac{1}{n+1}$. This is better than our first strategy. Also note that this strategy is optimal, since the correct votes is only one more than the incorrect votes in the winning case, and everyone votes incorrectly in the losing case.

**Puzzle 2** Everything stays the same as the first puzzle, except that each voter can cast any finite number of votes. This is also called "Chicago voting".

**Strategy 2** We can use the same strategy as Strategy 1B, but with each person "simulates" one group. That is, a person looks at the parities of less-numbered people. If he finds someone with parity 0, then he casts no votes. Otherwise he assumes his own parity to be 0 and vote accordingly.

**Analysis of 2** The analysis is the same as the analysis for Strategy 1B, so the probability for the strategy to succeed is $1 - \frac{1}{2^n}$ since we have $n$ groups now. Also, this strategy is optimal by the same reason as before.

**Puzzle 3** Let $S$ be the set of $n$ random bits. Now we have $\binom{n}{k}$ voters, where $k$ is a fixed number, and each voter can only see a distinct subset of $S$ of size $k$. Each voter can cast a finite number of votes. Again, we wish to determine the parity.

Note that Puzzle 2 is a speical case of Puzzle 3 when $k = n - 1$. For a general $k$, Puzzle 3 is equivalent to the following question.

For a given $k$, how well can a degree $k$ polynomial's sign represent PARITY?

To see the equivalence, first suppose that we are given a voting strategy and each voter can see at most $k$ bits. Then we can construct a polynomial in those $k$ bits computing the net vote of each person. Here we adopt the convention that counting a vote for $b$ as $(-1)^b$. Then the total votes can be seen as a polynomial in all of the input bits with a degree at most $k$, and PARITY can be determined by taking the sign of the polynomial.

Conversely, given a polynomial with a degree at most $k$, we want to give a voting strategy for each voter. This can be done by summing up the terms in the polynomial that are accessible to each voter. For example, if a voter can see $b_1, \ldots, b_k$ random bits, then $b_1 b_2 b_3$ is accessible to him, while $b_2 b_k b_{k+1}$ is not.

Therefore there is an equivalence between a Boolean function (as in the voting strategy) and the sign of a polynomial. Observe that if $k$ is much less than $n$, we can then compute the voting strategy with a low-degree polynomial. This low-degree polynomial is exactly the notion of a voting polynomial. However, we are mostly interested in approximating PARITY using the voting polynomial, rather than computing the exact value of PARITY. A natural question to ask is the number of errors made by the polynomial when approximating PARITY. In the following section we shall give a tight bound.

# 2 Voting Polynomials

In this section we consider PARITY as a Boolean function from $\{1, -1\}^n$ to $\{1, -1\}$. In other words, the parity on $\{x_1, \ldots, x_n\}$ can be written as $\mathrm{PARITY} = \prod_{i=1}^{n} x_i$.

Before we give upper and lower bounds for the number of errors, we first introduce the following definition.

**Definition 1.** *We say that a polynomial $p$* ***weakly represents*** PARITY *if $p \neq 0$ (not the zero function) and for all $x$ such that $p(x) \neq 0$, we have* $\mathrm{SIGN}(p(x)) = \mathrm{PARITY}(x)$*. We call the least $k$ such that there exists a polynomial weakly representing* PARITY *as the* ***weak degree*** *of PARITY.*

**Lemma 2.1.** *The weak degree of* PARITY *is $n$.*

*Proof.* Let $p$ be the polynomial weakly representing PARITY. We claim that $p \cdot \mathrm{PARITY} > 0$, since the sum $\sum_x p(x) \cdot \mathrm{PARITY}(x)$ is nonnegative (they share the same sign) and at least one term in the sum must be positive, otherwise $p$ is the zero function. Since PARITY is orthogonal to all monomials with degrees less than $n$ (see last lecture), the degree of $p$ must be at least $n$, otherwise we would have $p \cdot \mathrm{PARITY} = 0$. $\square$

## 2.1 The Lower Bound

We now give the lower bound of mistakes made in approximating PARITY using a polynomial.

**Theorem 2.1.** *In approximating* PARITY *over $n$ variables, any polynomial with a degree $k$ must make at least*

$$T = \sum_{i=0}^{\lfloor \frac{n-k-1}{2} \rfloor} \binom{n}{i}$$

*mistakes.*

*Proof.* Suppose that there is a polynomial $p$ with a degree $k$ that makes fewer than $T$ mistakes in approximating PARITY. Let $S$ be the set of inputs where $p$ makes errors. More specifically, let

$$S = \{x \in \{1, -1\}^n : \mathrm{SIGN}(p(x)) \neq \mathrm{PARITY}(x)\}.$$

Now we want to construct a polynomial $q$ that is zero on $S$, and $q$ is not the zero function. We do so by writing a system of linear equations to interpolate $S$. Observe that $T$ equals the number of monomials in $q$ if the degree of $q$ is $\lfloor \frac{n-k-1}{2} \rfloor$. So our goal is to obtain the coefficients of the polynomial $q$ of degree $\lfloor \frac{n-k-1}{2} \rfloor$ (there are $T$ such coefficients in total). Also note that the linear system satisfies the folowing properties.

- The number of equations is $|S|$, since only points in $S$ are used.
- The number of variables is
$$T = \sum_{i=0}^{\lfloor \frac{n-k-1}{2} \rfloor} \binom{n}{i},$$
since each unknown coefficient corresponds to a monomial in $q$.
- This is a homogeneous linear system, since $q$ is zero on $S$.

Since $p$ makes less errors than $T$, we have $|S| < T$. In other words, we have a homogeneous linear system with more variables than equations. So there exists a nontrivial solution. That is, such a polynomial $q$ exists.

Now consider the polynomial $q^2p$. We know that $q^2p$ is not a zero function since none of $q$ and $p$ is. For any $x \in S$, we have $(q^2p)(x) = 0$. For any $x \notin S$, we have $(q^2p)(x) \neq 0$ and $\mathrm{SIGN}((q^2p)(x)) = \mathrm{SIGN}(p(x)) = \mathrm{PARITY}(x)$, since $p$ does not make mistakes outside $S$. So $q^2p$ weakly represents parity. However, the degree of $q^2p$ is
$$\lfloor \frac{n-k-1}{2} \rfloor \cdot 2 + k \leq n - k - 1 + k = n - 1 < n.$$
This is a contradiction because Lemma 2.1 tells us that the weak degree of PARITY is $n$. $\square$

## 2.2 The Upper Bound

Theorem 2.1 gives us the lower bound for the number of mistakes if we try to approximate PARITY using a polynomial. It turned out that the upper bound is the same as the lower bound. Before we prove that the lower bound is indeed tight, we first give a voting polynomial that approximates PARITY.

Let $s = \sum_{i=1}^{n} \frac{1-x_i}{2}$. Since $x_i \in \{-1, 1\}$, $s$ counts the number of $-1$'s in the input. Note that $s$ is binomially distributed. Then we have
$$\mathrm{PARITY}(x) = \prod_{i=1}^{n} x_i = (-1)^s.$$

Here is the polynomial that achieves the lower bound,
$$p(s) = (-1)^{\lfloor \frac{n-k}{2} \rfloor} \prod_{i=0}^{k-1} \left( \lfloor \frac{n-k}{2} \rfloor + i + \frac{1}{2} - s \right).$$

Note that $p(s)$ is of degree $k$ when we expand $p$ over $x_1, \ldots, x_n$.

We now give the upper bound for the mistakes made by this polynomial.

**Theorem 2.2.** *The polynomial $p(s)$ defined above makes at most*

$$\sum_{i=0}^{\lfloor\frac{n-k}{2}\rfloor}\binom{n}{i}$$

*mistakes.*

*Proof.* Suppose that $s=\lfloor\frac{n-k}{2}\rfloor$. Then we have

$$p(s)=(-1)^s\prod_{i=0}^{k-1}\left(i+\frac{1}{2}\right).$$

Since we only care about the sign of $p(s)$, $p(s)$ has the same sign as PARITY in this case.

Suppose that we have $\lfloor\frac{n-k}{2}\rfloor<s\leq\lfloor\frac{n-k}{2}\rfloor+k$. Let $d=s-\lfloor\frac{n-k}{2}\rfloor$, then we have

$$\begin{aligned}
p(s) &= (-1)^{\lfloor\frac{n-k}{2}\rfloor}\prod_{i=0}^{k-1}\left(i+\frac{1}{2}-d\right)\\
&= (-1)^{\lfloor\frac{n-k}{2}\rfloor+d}\prod_{i=0}^{d-1}\left(d-i-\frac{1}{2}\right)\prod_{i=d}^{k-1}\left(i+\frac{1}{2}-d\right)\\
&= (-1)^{s}\prod_{i=0}^{d-1}\left(d-i-\frac{1}{2}\right)\prod_{i=d}^{k-1}\left(i+\frac{1}{2}-d\right).
\end{aligned}$$

It follows that

$$\mathrm{SIGN}(p(s))=(-1)^s=\mathrm{PARITY}(s),$$

since we have

$$\prod_{i=0}^{d-1}\left(d-i-\frac{1}{2}\right)\prod_{i=d}^{k-1}\left(i+\frac{1}{2}-d\right)>0,\text{ where }1\leq d\leq k.$$

So our polynomial $p(s)$ gives us the correct sign when $\lfloor\frac{n-k}{2}\rfloor\leq s\leq\lfloor\frac{n-k}{2}\rfloor+k$.

We now want to give the number of $x$ such that $\mathrm{SIGN}(p(x))\neq\mathrm{PARITY}(x)$, i.e. $\mathrm{SIGN}(p(x))\neq(-1)^s$. We first note that, if $s=\lfloor\frac{n-k}{2}\rfloor+k+2t$ or $s=\lfloor\frac{n-k}{2}\rfloor-2t$, then $\mathrm{SIGN}(p(s))=(-1)^s$. This can be seen from

$$\begin{aligned}
& s=\lfloor\frac{n-k}{2}\rfloor+k+2t\\
\Rightarrow\quad & p(s)=(-1)^{\lfloor\frac{n-k}{2}\rfloor}\prod_{i=0}^{k-1}\left(i+\frac{1}{2}-k-2t\right)=(-1)^{\lfloor\frac{n-k}{2}\rfloor}(-1)^k\prod_{i=0}^{k-1}\left(-i-\frac{1}{2}+k+2t\right),\\
& \text{where }\left(-i-\frac{1}{2}+k+2t\right)>0\text{ for all }0\leq i\leq k-1\\
\Rightarrow\quad & \mathrm{SIGN}(p(s))=(-1)^{\lfloor\frac{n-k}{2}\rfloor+k}=(-1)^s,
\end{aligned}$$

and

$$
\begin{aligned}
& s = \lfloor \frac{n-k}{2} \rfloor - 2t \\
\Rightarrow \quad & p(s) = (-1)^{\lfloor \frac{n-k}{2} \rfloor} \prod_{i=0}^{k-1} \left( i + \frac{1}{2} + 2t \right), \text{ where } \left( i + \frac{1}{2} + 2t \right) > 0 \text{ for all } 0 \leq i \leq k-1 \\
\Rightarrow \quad & \mathrm{SIGN}(p(s)) = (-1)^{\lfloor \frac{n-k}{2} \rfloor} = (-1)^s.
\end{aligned}
$$

From the above calculations, it can be easily observed that $p(s)$ gives us incorret signs only when $s = \lfloor \frac{n-k}{2} \rfloor + k + 2t + 1$ and $s = \lfloor \frac{n-k}{2} \rfloor - 2t - 1$. Since $s$ is binomially distributed, the number of input $x$ that $p$ gives incorrect signs is

$$
W = \sum_{t \geq 0} \binom{n}{\lfloor \frac{n-k}{2} \rfloor + k + 2t + 1} + \sum_{t \geq 0} \binom{n}{\lfloor \frac{n-k}{2} \rfloor - 2t - 1},
$$

where the two sums correspond to the right tail and the left tail outside the region $\lfloor \frac{n-k}{2} \rfloor \leq s \leq \lfloor \frac{n-k}{2} \rfloor + k$, respectively. We then have two cases.

**Case 1: $(\mathbf{n} - \mathbf{k})$ is odd.** We then have

$$
\begin{aligned}
W &= \sum_{t \geq 0} \binom{n}{\frac{n+k+1}{2} + 2t} + \sum_{t \geq 0} \binom{n}{\frac{n-k-1}{2} - 2t - 1} \\
&= \sum_{t \geq 0} \binom{n}{\frac{n-k-1}{2} - 2t} + \sum_{t \geq 0} \binom{n}{\frac{n-k-1}{2} - (2t+1)}, \text{ by } \binom{n}{i} = \binom{n}{n-i} \\
&= \sum_{t \geq 0} \binom{n}{\frac{n-k-1}{2} - t}, \text{ since they fill the gap between them} \\
&= \sum_{t=0}^{\frac{n-k-1}{2}} \binom{n}{t}, \text{ by a change of variables.}
\end{aligned}
$$

So the upper bound and the lower bound on $p$'s mistakes are the same.

**Case 2: $(\mathbf{n}-\mathbf{k})$ is even.** We then have

$$\begin{aligned}
W &= \sum_{t\geq 0}\binom{n}{\frac{n+k}{2}+2t+1}+\sum_{t\geq 0}\binom{n}{\frac{n-k}{2}-2t-1} \\
&= 2\sum_{t\geq 0}\binom{n}{\frac{n-k}{2}-2t-1}, \text{ by symmetry} \\
&= 2\sum_{t\geq 0}\binom{n-1}{\frac{n-k}{2}-2t-1}+2\sum_{t\geq 0}\binom{n-1}{\frac{n-k}{2}-2t-2}, \\
&\quad \text{by the Pascal's triangle identity: } \binom{n}{i}=\binom{n-1}{i}+\binom{n-1}{i-1} \\
&= 2\sum_{t\geq 0}\binom{n-1}{\frac{n-k}{2}-t-1}, \text{ since they fill the gap between them again} \\
&= 2\sum_{t=0}^{\frac{n-k}{2}-1}\binom{n-1}{t}, \text{ by a change of variables.}
\end{aligned}$$

So $W$ is twice the lower bound on the number of mistakes any polynomial of degree $k$ would make on $(n-1)$ bits. We now claim that $W$ is the lower bound on the number of mistakes that any polynomial of degree $k$ would make on $n$ bits. Suppose that there is a polynomial $r$ with degree $k$ and $r$ makes fewer errors than $W$ on $n$ bits. Then we could pick any input bit $x_i$ and fix its value. The polynomial thus obtained has a degree $k$, but makes even fewer mistakes than our lower bound, $\sum_{t=0}^{\frac{n-k}{2}-1}\binom{n-1}{t}$, which is impossible. Therefore $p$ also approximates PARITY optimally in this case. $\square$

Since $p$ gives us the optimal approximation for PARITY, we can use $p$ as the voting strategy for Puzzle 3.

# References


[1] James Aspnes, Richard Beigel, Merrick L. Furst, and Steven Rudich. The expressive power of voting polynomials. In Proceedings of the 23rd ACM Symposium on Theory of Computation, pages 402–409. Association for Computing Machinery, 1991.