Randomness and Computation

or, “Randomized Algorithms”

Mary Cryan

School of Informatics
University of Edinburgh

The probabilistic method

> *The* Probabilistic Method *is a nonconstructive method of proof, primarily used in combinatorics and pioneered by Paul Erdős, for proving the existence of a desired kind of mathematical object. It works by showing that if we randomly choose objects from a specified class,* the probability *that the result has the desired property is greater than zero. This is enough to tell us that there must be* at least one *object with the desired property in the class.*
>
> *Note that although this approach uses probability, the result (that some object with the property exists) will be definite, not "in probability".*

Slightly different theme to the rest of the results in this course, as we are concerned with showing *existence* (rather than constructing the object). However, sometimes we can derandomize/construct.

Max Cuts in Graphs

Of interest is the Max Cut of a given graph (as well as "Min"):

> *Given an* undirected, unweighted *graph* $G = (V, E)$ *with* $|V| = n$, $|E| = m$, *compute a "max cut"; that is, a partition of* E *into two non-empty sets* S, $V \setminus S$, *such that the following quantity is* maximized*:*

$$\{e = (u, v) : u \in S, v \in V \setminus S\}$$

Well-known as one of the classical NP-complete problems. So we believe there is no *polynomial-time* algorithm to compute this exactly (not in $\Theta(n^2 m)$, not in $\Theta(m^5 n^9)$ etc).

We will show that every graph $G = (V, E)$ has a cut of size *at least* $|E|/2$.

Max Cuts in Graphs

Consider the following Algorithm:

Algorithm RANDOMCUT($G = (V, E)$)

1. $S \leftarrow \emptyset$
2. **for** every $v \in V$ in fixed order **do**
3. Draw a value b uniformly from $\{0, 1\}$.
4. **if** $(b = 1)$ **then**
5. $S \leftarrow S \cup \{v\}$
6. **return** S, $V \setminus S$

We are going to analyse this algorithm and show that C_S (the number of edges between S and $V \setminus S$) has *expected size* at least $|E|/2$.

Max Cuts in Graphs

Theorem (6.3)

For any given graph $G = (V, E)$*, there is* some *cut* $(S, V \setminus S)$ *such that* $|C_S| \geq |E|/2$.

Proof.

We show that the *expected* cardinality of C_S, $\mathrm{E}[|C_S|]$ is at least $|E|/2$ when S is a random subset of V. We can write

$$E[|C_S|] = \frac{1}{2^n} \sum_{S:S\subset V} \sum_{e=(u,v)\in E} \mathbb{I}_{|\{u,v\}\cap S|=1}.$$

Switching summations,

$$E[|C_S|] = \sum_{e=(u,v)\in E} \frac{1}{2^n} \sum_{S:S\subset V} \mathbb{I}_{|\{u,v\}\cap S|=1}.$$

For every $e \in E$, it has 4 options wrt a randomly generated S: $u, v \in S$, $u \in S, v \notin S$, $u \notin S, v \in S$, and $u \notin S, v \notin S$. Probability $1/4$ each.

Max Cuts in Graphs

Proof cont.

Hence, for a fixed $e \in E$,

$$\frac{1}{2^n} \sum_{S : S \subset V} \mathbb{I}_{|\{u,v\} \cap S| = 1} = \frac{2}{4} = \frac{1}{2}.$$

Hence, summing over all $e \in E$,

$$E[|C_S|] = \sum_{e=(u,v) \in E} \frac{1}{2} = \frac{|E|}{2},$$

as claimed.

Now switch back to thinking of this as the expectation over random S. If the *expected* size is $|E|/2$, then *certainly* there is at least one cut of at least that size.

□

Probabilistic Method

- We did not analyse the probability that RANDOMCUT gives a good (high cardinality) cut, and are not going to do that yet.
- Can *de-randomise* the algorithm using conditional probabilities.
- The proof that every graph has a cut of cardinality $\geq |E|/2$ is a very very simple example of *the probabilistic method*.
- With the probabilistic method, we use randomness and the laws of expectation to prove that certain structures must exist.
- More later in the course.

De-randomization

We derandomize via “conditional expectation”.

Our concern is the value of $|C_S|$, and the expected value of this quantity will change throughout the algorithm (as vertices get added to S or $V \setminus S$).

Our random algorithm considered the vertices in fixed order. Let $x_1, x_2, \ldots, x_k, \ldots$ be the choices for the variables ($x_i = 1$ means that v_i is added to S, otherwise it's added to $V \setminus S$).

Our derandomization will construct a specific cut (again defined by $x_1, \ldots, x_k, \ldots$) of size $\geq \frac{|E|}{2}$ by making decisions for the vertices one-by-one. At each step we will ensure we choose x_{k+1} so that

$$\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_{k+1}}] \geq \mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}].$$

Derandomization cont'd.

Suppose we have considered $v_1, \ldots, v_k$ so far, and we have taken decisions $x_1, \ldots, x_k$ for these vertices.

Suppose (induction hypothesis) we know that
$\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}] \geq \mathrm{E}[|\mathrm{C_S}|$.

Let $A = \{v_i \mid x_i = 1, i \leq k\}$, $B = \{v_i \mid x_i = 0, i \leq k\}$.

Think about the (random) process for adding v_{k+1} (picture).
There are two choices for x_{k+1}, of equal probability.
Hence

$$\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}] = \frac{\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}, \mathrm{x_{k+1}} = 1] + \mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}, \mathrm{x_{k+1}} = 0]}{2}.$$

So one of these expectations is at least as good as $\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}]$, which (by induction) is at least as good as $\mathrm{E}[|\mathrm{C_S}|] = \frac{|\mathrm{E}|}{2}$.

Derandomization cont'd.

How do we decide which of $\mathrm{E}[|C_S| \mid x_1, \ldots, x_k, x_{k+1} = 1]$, $\mathrm{E}[|C_S| \mid x_1, \ldots, x_k, x_{k+1} = 0]$ is larger?

- If $x_{k+1} = 1$ (ie, v_{k+1} goes into A), then we add 1 to $|C_S|$ for every $(v_i, v_{k+1}) \in E$ with $v_i \in B$ (and $i \leq k$, obviously).
- If $x_{k+1} = 0$ (ie, v_{k+1} goes into B), then we add 1 to $|C_S|$ for every $(v_i, v_{k+1}) \in E$ with $v_i \in A$ (and $i \leq k$, obviously).
- For every v_i with $i > k+1$, we add $\frac{1}{2}$ to $\mathrm{E}[|C_S| \mid x_1, \ldots, x_k]$ *regardless* of whether v_{k+1} gets added to A or B.

So the *difference* of conditional expectations satisfies

$$\begin{aligned} & \mathrm{E}[|C_S| \mid x_1, \ldots, x_k, x_{k+1} = 1] - \mathrm{E}[|C_S| \mid x_1, \ldots, x_k, x_{k+1} = 0] \\ = \quad & |\{(v_i, v_{k+1}) \in E, v_i \in B, i \leq k\}| - |\{(v_i, v_{k+1}) \in E, v_i \in A, i \leq k\}| \end{aligned}$$

Derandomization cont'd.

How do we decide which of $\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}, \mathrm{x_{k+1}} = 1]$, $\mathrm{E}[|\mathrm{C_S}| \mid \mathrm{x_1}, \ldots, \mathrm{x_k}, \mathrm{x_{k+1}} = 0]$ is larger?

We can easily compute $|\{(v_i, v_{k+1}) \in E, v_i \in B, i \leq k\}|$ and $|\{(v_i, v_{k+1}) \in E, v_i \in A, i \leq k\}|$ by examining the graph and the cut so far $((A, B))$.

If $|\{(v_i, v_{k+1}) \in E, v_i \in B, i \leq k\}|$ is larger than $|\{(v_i, v_{k+1}) \in E, v_i \in A, i \leq k\}|$, we set $x_{k+1} = 1$, else we set $x_{k+1} = 1$.

By Induction, we construct a cut guaranteed to be as large as $\mathrm{E}[|\mathrm{C_S}|] = \frac{|\mathrm{E}|}{2}$.

Base case?

References

Today's topic is from Sections 6.2, 6.3 of the book. We will return to the probabilistic method, and derandomization, in a couple of weeks.

TCS "cheat sheet" is always useful
`http://www.tug.org/texshowcase/cheat.pdf`

We will start work on Chernoff Bounds next week. It's a good idea to look at the early sections of Chapter 4.