Randomness and Computation

or, “Randomized Algorithms”

Heng Guo

(Based on slides by M. Cryan)

Max-Cut

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-Cut

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 Bernoulli$(1/2)$ random variable b .
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.

Consider the random S drawn by RandomCut. We show that the *expected* cardinality of C_S, $\mathrm{E}[|C_S|]$ is $|E|/2$ when S is a random subset of V.

Let I_e be the indicator variable of whether e is in C_S or not. There are 4 possibilities for $e = (u, v)$:

$$u, v \in S; \quad u \in S, v \notin S; \quad u \notin S, v \in S; \quad u, v \notin S.$$

Notice that 2 out of the 4 cases lead to $e \in C_S$. Thus,

$$\mathrm{E}[I_e] = \frac{1}{2}.$$

□

Max Cuts in Graphs

Proof cont.

Hence, summing over all $e \in E$ and by linearity of expectation,

$$E[|C_S|] = \sum_{e \in E} \mathrm{E}[I_e] = \frac{|E|}{2}.$$

If the *expected* size is $|E|/2$, then *certainly* there is at least one cut of at least that size. $\square$

The probabilistic method

- 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.

The probabilistic method

The (basic) probabilistic method:

- Draw a random object;
- The probability of the random object satisfying certain property is strictly positive;
- The desired object must exist!

This is a non-constructive method of proving the existence of combinatorial objects, pioneered by Paul Erdős.

Although this approach uses probability, the result (that some object with the property exists) will be definite, not "in probability".

It only tells us that some object exists, but in many cases, we can find / construct the object efficiently as well.

More later in the second half of the course.

De-randomization

- We did not analyse the probability that RandomCut gives a good (high cardinality) cut, and are not going to do that.
- Can *de-randomize* the algorithm using conditional probabilities.

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 $\overline{S}$).

Our random algorithm considered the vertices in fixed order. Let $X_1, \ldots,$ X_n be the indicator random variables ($X_i = 1$ means that v_i is added to S, otherwise it’s added to $\overline{S}$).

Our derandomization will construct a specific cut (defined by $X_1, \ldots, X_n$) 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

$$\mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_{k+1} = x_{k+1}] \geq \mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_k = x_k].$$

Derandomization cont'd.

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

Suppose (induction hypothesis) we know that

$$\mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_k = x_k] \geq \mathrm{E}[|C_S|].$$

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

$$\begin{aligned} & \mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_k = x_k] \\ = \; & \frac{\mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_k = x_k, X_{k+1} = 1]}{2} \\ & + \frac{\mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_k = x_k, X_{k+1} = 0]}{2}. \end{aligned}$$

So one of these expectations is at least as good as $\mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_k = x_k]$, which (by induction) is at least as good as $\mathrm{E}[|C_S|] = \frac{|E|}{2}$.

Derandomization cont'd.

How do we decide the value of X_{k+1}?

We want to compute the conditional expectation

$$Z_i := \mathrm{E}[|C_S| \mid X_1 = x_1, \ldots, X_{k+1} = i].$$

Recall the linearity of conditional expectation, and $|C_S| = \sum_{e \in E} I_e$. We just need to compute

$$Z_{i,e} := \mathrm{E}[I_e \mid X_1 = x_1, \ldots, X_{k+1} = i]$$

for each $e \in E$, and $Z_i = \sum_{e \in E} Z_{i,e}$.

Derandomization cont'd.

$$Z_{i,e} = \mathrm{E}[I_e \mid X_1 = x_1, \ldots, X_{k+1} = i]$$

There are three possibilities of the two endpoints of e:

- Both have been determined — the conditional expectation is 0 or 1;
- One of them is determined — the conditional expectation is $1/2$;
- None of them is determined — the conditional expectation is $1/2$.

Moreover, these values are easy to compute. Thus we can compute $Z_{i,e}$ for each e, and sum them up to get the desired Z_i.

Then we compare Z_0 and Z_1 and choose the larger.

Derandomization cont'd.

To decide X_{k+1}, all we care actually is if $Z_1 - Z_0 \geq 0$, and

$$Z_1 - Z_0 = \sum_{e \in E} Z_{1,e} - Z_{0,e}.$$

Back to the possibilities for e:

- If neither endpoints of e is v_{k+1}, $Z_{1,e} = Z_{0,e}$;
- If one endpoint of e is v_{k+1} and the other end is not determined, then $Z_{1,e} = Z_{0,e} = \frac{1}{2}$.
- If one endpoint of e is v_{k+1} and the other end is determined, then $Z_{1,e} \neq Z_{0,e}$.

Thus we only need to care about the last case.

Derandomization cont'd.

For $i = 0, 1$, let $A_i := \{v_j \mid i \in [k],\ X_j = i,\ (v_j, v_{k+1}) \in E\}$.
Namely $A_{0/1}$ is the set of neighbours of v_{k+1} that are in S or $\overline{S}$.

Each vertex in A_1 contributes 1 to Z_0,
and each vertex in A_0 contributes 1 to Z_1.

Thus, $Z_1 - Z_0 = |A_0| - |A_1|$.

What is the de-randomized algorithm?

From the first vertex to the last, assign the current vertex to S or $\overline{S}$ so as to maximize the current cut value.

What is the de-randomized algorithm?

From the first vertex to the last, assign the current vertex to S or $\overline{S}$ so as to maximize the current cut value.

This is just the familiar greedy algorithm!

What is the de-randomized algorithm?

From the first vertex to the last, assign the current vertex to S or $\overline{S}$ so as to maximize the current cut value.

This is just the familiar greedy algorithm!

More generally, the greedy algorithm is guaranteed to be better than the expectation when all choices are random.

Reference and reading

Today's topic is from Sections 6.2, 6.3 of the book. We will return to the probabilistic method, and derandomisation, after the reading week.

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

Goemans-Williamson algorithm

The best approximation ratio for Max-cut is ≈ 0.878, due to Goemans and Williamson (1995). Improving upon this ratio would disprove major conjectures in computational complexity!

Max-cut is equivalent to a quadratic integer program:

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} 1 - x_u x_v \\ \text{subject to} \quad & \forall v \in V,\ x_v \in \{+1, -1\}. \end{aligned}$$

We cannot solve this efficiently. Instead, we can solve a relaxation

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} 1 - \langle \vec{x}_u, \vec{x}_v \rangle \\ \text{subject to} \quad & \forall v \in V,\ \|\vec{x}_v\|_2 = 1 \\ & \forall v \in V,\ \vec{x}_v \in \mathbb{R}^n. \end{aligned}$$

Goemans-Williamson algorithm

Solving

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} 1 - \langle \vec{x}_u, \vec{x}_v \rangle \\ \text{subject to} \quad & \forall v \in V,\ \|\vec{x}_v\|_2 = 1 \\ & \forall v \in V,\ \vec{x}_v \in \mathbb{R}^n. \end{aligned}$$

gives us a collection of vectors on the unit sphere. The final step is to choose a random hyperplane through the origin that cuts the sphere in half!

The approximation ratio is at least

$$\min_{0\le\theta\le\pi} \frac{\theta/\pi}{(1-\cos\theta)/2} \approx 0.878.$$