CMPUT 675: Computational Complexity Theory **Winter 2019**

Lecture 18 (Mar 14th): **Cryptography** & **Spectral Graph Theory**

Lecturer: Zachary Friggstad *Scribe: Gao Yue*

18.1 Goldreich-Levin '89

In the last lecture, we have introduced Goldreich-Levin Theorem, and gave a short proof of it, in this lecture, the proof of why the Goldreich/Levin algorithm works will be revised.

Recall that we would like to successfully invert f(x) for $x \in \{0,1\}^n$ such that $\mathop{\mathbf{Pr}}_r[A(f(x), r) = x \circ r] \geq \frac{1}{2} + \frac{1}{2n^c}$. Here we provide such an algorithm :

Algorithm 1 Algorithm Recovering 'good' x Given y=f(x)

Input: y, which is equal to $f(x)$ for an unknown x.
Output: $\overline{x}$ such that $f(\overline{x}) = f(x)$ (or nothing, if it fails).

$m \leftarrow 200 \cdot n^{2c+1}$ (Could also be other polynomials of degree $\geq 2c+1$)
$k \leftarrow$ number of bits to write m
- Sample $s_0, ..., s_{k-1} \sim \{0,1\}^n$
- Form $r_j = \sum_{i \in T_j} s_i (\text{mod } 2)$ for $\forall 1 \leq j \leq m$, note that r_j are independent
- 'Guess' $x \circ s_i$ for $\forall 1 \leq i \leq k-1$
- For each i, let $y_j = \sum_{i \in T_j} x \circ s_j$, note that for the right guess, this is $x \circ r_j$
- Let $y_j^{'} = A(f(x), r_j \circ e_i)$

for each $i, 1 \leq i \leq n$ **do**
  $\overline{x_i} \leftarrow$ majority of $y_j, y_j^{'}$ $_{1 \leq j \leq m}$
end for
if $\overline{x} = y$ **then**
  output $\overline{x}$
end if

In the algorithm, T_j is the set of bit positions i such that bit i of j is 1. By 'guess', we mean that all $2^k \leq 2m$ possibilities for the different values of all $x \circ s_i$ should be enumerated and the rest of the algorithm should run for each guess, breaking only if an iteration successfully inverts $f(x)$ (i.e. $f(\overline{x}) = f(x)$).

We will show that the algorithm would successfully invert a x such that $\mathop{\mathbf{Pr}}_r[A(f(x), r) = x \circ r] \geq \frac{1}{2} + \frac{1}{2n^c}$ with high probability.

Claim 1 $\forall 1 \leq i \leq n$, $\boldsymbol{Pr}[\overline{x_i} \neq x_i] \leq \frac{1}{50 \cdot n}$.
(Note that 50 can be any other constant if we change m in the algorithm)

Proof. Note that $x \circ r_j = x \circ \left(\sum_{i \in T_j} s_i\right)$ is known when we guess all $x \circ s_i$ properly. So $\overline{x}_i \neq x_i$ only if the majority of j's have $A(y, r_j \oplus e^i) \neq (r_j \oplus e^i) \circ x$.

Fix i, let $Y_j \in \{0,1\}$ be the random vector such that

$$Y_j = \begin{cases} 1 & if A(y, r_j \oplus e^i) = (r_j \oplus e^i) \circ x \\ 0 & if A(y, r_j \oplus e^i) \neq (r_j \oplus e^i) \circ x \end{cases}$$

Then for $Y = \sum_{j=1}^{m} Y_j$, $\mathbb{E}[Y] \geq \frac{m}{2} + \frac{m}{2 \cdot n^c}$ since the probability of successfully inverting x is $\geq \frac{1}{2} + \frac{1}{2n^c}$,

$$\begin{aligned} Var[Y] &= \sum_{j=1}^{m} Var[Y_j] \qquad \text{because } r_j \text{ are pairwise independent} && (18.1) \\ &\leq m \qquad \text{as } Y_j \in \{0,1\}, \forall j && (18.2) \end{aligned}$$

Note that for all i,

$$\begin{aligned} \mathbf{Pr}[\overline{x_i} \neq x_i] &\leq \mathbf{Pr}[Y \leq \frac{m}{2}] && (18.3) \\ &\leq \mathbf{Pr}[Y \leq \mathbb{E}[Y] - \frac{m}{2 \cdot n^c}] && (18.4) \\ &\leq \mathbf{Pr}[|Y - \mathbb{E}[Y]| \leq \frac{\sqrt{m}}{2 \cdot n^c} \cdot \sqrt{m}] && (18.5) \\ &\leq \mathbf{Pr}[|Y - \mathbb{E}[Y]| \leq \frac{\sqrt{m}}{2 \cdot n^c} \cdot \sqrt{Var[Y]}] && (18.6) \\ &\leq \frac{4 \cdot n^{2c}}{m} && (18.7) \\ &= \frac{4 \cdot n^{2c}}{200 \cdot n^{2c+1}} && (18.8) \\ &= \frac{1}{50n} && (18.9) \end{aligned}$$

■

So by the union bound, $\mathbf{Pr}[\exists i, \overline{x_i} \neq x_i] \leq \sum_{i=1}^{n} \frac{1}{50n} = \frac{1}{50}$. The algorithm successfully finds $\overline{x}$ such that $f(\overline{x}) = y$ with probability $\geq \frac{49}{50}$. (Note that this probability can be other constant or even $1 - 1/\text{poly}(n)$ if we change m in the algorithm).

Claim 2 *If f is a one-way permutation, then for all polynomial $\ell(n)$, $G(x,r) = (r, f^{\ell(n)}(x) \circ r, f^{\ell(n)-1}(x) \circ r, f^{\ell(n)-2}(x) \circ r, ..., f(x) \circ r)$ is a pseudorandom generator with stretch $\ell(2n) + 2n$ taking inputs $x, r \in \{0,1\}^n$.*

Proof. By Yao's Lemma, it sufficies to show that G is unpredictable, i.e., there is no algorithm B that has: $\mathbf{Pr}_{\substack{x,r \sim \{0,1\}^n \\ i \sim [l(n)]}}[B(1^n, i, r, f^l(x) \circ r, ..., f^{i+1}(x) \circ r) = f^i(x) \circ r] \geq \frac{1}{2} + \frac{1}{n^d}$ for some d.

We prove by contradiction, suppose such B exists, then we can define an algorithm $B^{'}$ to predict $x \circ r$ given y = f(x) and r.

Algorithm 2 Algorithm $B^{'}$ to predict $x \circ r$ given $y = f(x), r$

- Sample $i \sim [l]$
- Output $B(1^n, i, r, f^{l-i-1}(y) \circ r, ..., f(y) \circ r, y \circ r)$

Note that for a random i, for $x, r \sim \{0,1\}^n$, the distribution over $f^{l-i-1}(y) \circ r, ..., y \circ r$ is the same as the distribution over $f^l(x^{'}) \circ r, ..., f^{i+1}(x^{'}) \circ r$.

If we sample $x^{'}, r \sim \{0,1\}^n$, set $x = f^i(x^{'})$, then B can predict $f^i(x^{'}) \circ r$ with probability $\geq \frac{1}{2} + \frac{1}{n^d}$, so equivalently $B^{'}$ can predict $x \circ r$ given y=f(x) with probability $\geq \frac{1}{2} + \frac{1}{n^d}$, contradicting Goldreich-Levin Theorem. ■

18.2 Spectral Graph Theory

We are now entering the "topics" half of the class, having covered most of the core material in the first part of the textbook. Our first topic is the use and construction of expander graphs.

18.2.1 A Quick Review of Linear Algebra

The results we review are standard from an intermediate undergraduate course on linear algebra. A couple are proven here just for clarity and to get us "warmed up" to these sorts of arguments. 1. For a matrix A, λ is an eigenvalue of A if $Ax = \lambda x$ for some $x \neq 0$.

2. If A is a symmetric real matrix, then
(a) All eigenvalues of A are real.
(b) The multiplicity of an eigenvalue as a root of the characteristic polynomial $\det(A - x \cdot I)$ equals the dimension of its *eigenspace* $\{x : Ax = \lambda x\}$.
(c) The total multiplicity of all eigenvalues is n.
(d) $\langle x, x^{'} \rangle = 0$ if $x, x^{'}$ are eigenvectors of A for different eigenvalues.

proof: Since $x, x^{'}$ are eigenvectors of A for different eigenvalues, then there exists $\lambda, \lambda^{'}$ such that

$\lambda \neq \lambda^{'}$; $Ax = \lambda x$; $Ax^{'} = \lambda^{'} x^{'}$

Hence $\lambda \cdot \langle x, x^{'} \rangle = \langle Ax, x^{'} \rangle = \langle x, Ax^{'} \rangle = \langle x, x^{'} \rangle \cdot \lambda^{'}$

Since $\lambda \neq \lambda^{'}$, then $\langle x, x^{'} \rangle = 0$.

(e) More generally, we can pick an orthonormal basis of eigenvectors. That is, writing $\lambda_1, \lambda_2, ..., \lambda_n$ as all eigenvalues that can pick eigenvectors $x^1, ..., x^n$ such that
i. $Ax^i = \lambda_i \cdot x^i$
ii.

$$\langle x^i, x^j \rangle = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

18.2.2 Random Walks

In this section, we'll mainly talk about d-regular graph and properties of eigenvalues of its random walk matrix.

Consider the undirected graph shown in figure 18.1, imagine that you are standing at any vertex, if there are k edges incident to that vertex, assume the probability that you are going to move along any of those k edges are all $\frac{1}{k}$.
Then an random walk matrix A can be defined as : $A_{ij} = \mathbf{Pr}[\text{A step from } v_i \text{ moves to } v_j], \forall 1 \leq i, j \leq n$. This is just the adjacency matrix normalized so all rows sum to 1. e.g., the random walk matrix for the graph 18.1 is

$$\begin{bmatrix} 1/3 & 1/3 & 1/3 & 0 \\ 1/3 & 1/3 & 0 & 1/3 \\ 1/3 & 0 & 0 & 2/3 \\ 0 & 1/3 & 2/3 & 0 \end{bmatrix}$$

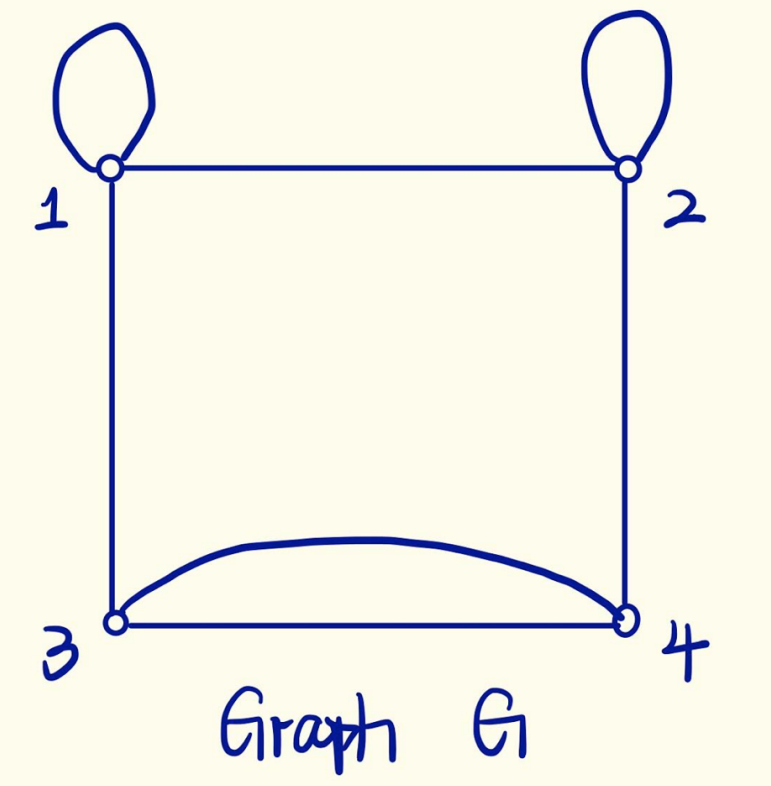

Figure 18.1: A 3-regular graph

Definition 1 (d-regular graph) *A graph G is a d-regular graph if all nodes in G are endpoints of exactly d edges.*

We consider graphs with loops: a loop contributes exactly 1 to the degree of the node even though we often draw it with two endpoints touching the node. So graph 18.1 is a 3-regular graph.

If an undirected graph is d-regular, then its random walk matrix must be symmetric. This is simply because the random walk matrix A is then $\frac{1}{d}$ times the adjacency matrix and the adjacency matrix of an undirected graph is symmetric.

We now explore basic properties of the random walk matrix A as they related to the structure of the graph G.

Claim 3 *Let $p \in [0,1]^{|V|}$ be such that $\sum_{v=1}^{|V|} p_v = 1$ (a probability distribution over V). Then $A^k \cdot p$ is the probability distribution over V after sampling $u \sim p$ and taking a random walk of length k starting from u.*

Proof. Just from the definitions. ■

Claim 4 *Suppose A is a random walk matrix of a d-regular graph, then $|\lambda| \leq 1$ for $\forall$ eigenvalues λ of A*

Proof. Pick any eigenvalue λ of A, then there is some $x \neq 0$ that $Ax = \lambda \cdot x$.

Pick $v = \arg\max_u x_u$, then

$$\begin{aligned} |\lambda| \cdot |x_u| &= |\lambda \cdot x_u| && (18.10)\\ &= |(A \cdot x)_u| && (18.11)\\ &= |\sum_v A_{uv} \cdot x_v| && (18.12)\\ &\leq \sum_v A_{uv} \cdot |x_v| && (18.13)\\ &\leq |x_u| \cdot \sum_v A_{uv} && (18.14)\\ &= |x_u| && (18.15) \end{aligned}$$

Note that $x_u \neq 0$, so $|\lambda| \leq 1$. ■

Claim 5 *For the random walk matrix A of a d-regular graph, multiplicity of 1 as an eigenvalue equals to number of connected components in graph.*

Proof.

1. multiplicity of 1 as an eigenvalue $\geq$ number of connected components :

   Let $C \subseteq V$ be a connected component, let

   $$x_v^C = \begin{cases} 1 & v \in C \\ 0 & v \notin C \end{cases}$$

   In the graph shown in figure 18.2, there are two connected components, BLUE and RED, then by definition,

   $$A = \begin{pmatrix} 0 & 1/2 & 1/2 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 1/2 & 1/2 & 0 \end{pmatrix} \quad x^{BLUE} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad x^{RED} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

   Then for any connected component C,

   $$Ax^C = \begin{pmatrix} a_1 \circ x^C \\ a_2 \circ x^C \\ \cdots \\ a_n \circ x^C \end{pmatrix}.$$

   Where a_i is the i-th row-vector of A (recalling A is symmetric). Note that for all i, $a_i \circ x^C = \sum_{v=1}^n a_{iv} \cdot x_v^C = \sum_{v \in C} a_{iv} = x_i^C$ (Since C is a connected component, if i is in C, then the total probability of stepping from i to $v \in C$ is 1; If i is not in C, the probability of stepping from i to $v \in C$ is 0).
   Hence $Ax^C = x^C$ for any connected components C, so the multiplicity of 1 as an eigenvalue $\geq$ number of connected components.

2. number of connected components = multiplicity of 1 as an eigenvalue :

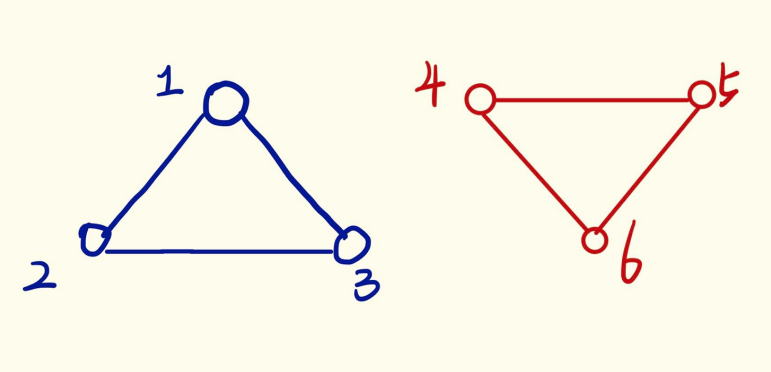

Figure 18.2: Connected Components BLUE and RED

Let x be such that $Ax = x$. We claim for u, v in the same component that $x_u = x_v$. To see this, consider a component C and pick $v = \arg\max_{u \in C} |x_u|$. If $x_v = 0$ there is nothing to show, otherwise

$$\begin{aligned} |x_v| &= |(A \cdot x)_v| && (18.16)\\ &= |\sum_u A_{uv} \cdot x_u| && (18.17)\\ &\leq \sum_u A_{uv} \cdot |x_u| && (18.18)\\ &\leq |x_v| \cdot \sum_v A_{uv} && (18.19)\\ &= |x_v| && (18.20) \end{aligned}$$

So (18.17) = (18.18) = (18.19), then $|x_u| = |x_v|$ for every neighbour u of v for the second bound to hold with equality. But then the first bound holds with equality only if $x_u = x_v$ (without absolute values). Then by induction on the distance of a node u from v, every u in the same component as v has $x_u = x_v$.

So x is constant across any connected component meaning it can be represented as a linear combination of all eigenvectors of the form x^C for the various connected components C. That is, the eigenspace for eigenvalue 1 has $\{x^C : C \text{ a component of } G\}$ as a basis. Hence number of connected components = multiplicity of 1 as an eigenvalue.

■

Claim 6 *Let G be a connected, d-regular graph with random walk matrix A, then -1 is an eigenvalue if and only if G is bipartite.*

Proof.

- G is bipartite ⇒ -1 is an eigenvalue :
  Let $L, R \subset V$ be the two parts, then define a vector x s.t.

$$x_v = \begin{cases} 1 & v \in R \\ -1 & v \in L \end{cases}$$

Then for all $1 \leq i \leq n$, $(Ax)_i = a_i \circ x = \sum_{v=1}^{n} a_{iv} \cdot x_v = \sum_{v \in R} a_{iv} - \sum_{v \in L} a_{iv} = -x_i$ (Since if $i \in R$, $a_{iv} = 0$ for all $v \in R$, and $a_{iv} = 1$ for some $v \in L$, so $\sum_{v \in R} a_{iv} - \sum_{v \in L} a_{iv} = -1 = -x_i$; For the case $i \in L$, similar).

- -1 is an eigenvalue $\Rightarrow$ G is bipartite :
  Suppose there is some vector $x \neq 0$ such that $Ax = -x$. We verify that $L = \{v : x_v \leq 0\}, R = \{r : x_r > 0\}$ is a bipartition. Let v have the largest value $|x_v|$. By negating x if necessary $x_v > 0$ as well. One one hand
  $$-x_v = (Ax)_v = \sum_u A_{uv} x_u.$$
  On the other hand, $x_v = \sum_u A_{uv} x_v$, so $\sum_u A_{uv} x_u = \sum_u A_{uv} \cdot (-x_v)$. We know $x_u \geq -x_v$ by our choice of v. If any neighbour u of v has $x_u > -x_v$ then equality in this sum could not hold as all entries of A are nonnegative and $A_{uv} > 0$ for a neighbour u of v. So every neighbour u of v has $x_u = -x_v$. Continuing in this way, we see that any node u with distance i from v has $x_u = (-1)^i \cdot x_v$. Then essentially the same argument also shows for every edge uw that $x_u = -x_w$. So L and R is a bipartition: no edge has both endpoints in one set.

■

Corollary 1 *Let G be connected, nonbipartite, d-regular graph with eigenvalues $\lambda_1, ..., \lambda_n$ such that $|\lambda_1| \geq |\lambda_2| \geq ... \geq |\lambda_n|$. Then $\lambda_1 = 1$ and $|\lambda_2| < 1$.*

Proof. Since G only has 1 connected component, by **Claim 4**, multiplicity of 1 as eigenvalue is 1. Since G is not bipartite, by **Claim 5**, -1 is not an eigenvalue. Then by **Claim 3**, $\lambda_1 = 1$ and $|\lambda_2| < 1$ ■

18.2.3 Rayleigh Quotient

Before we introduce Cheegers' Inequality, we'll first introduce arguments based on Rayleigh Quotients which will be used a couple of times in the lectures.

Claim 7 *If A is a symmetric real matrix, $\lambda_1, ..., \lambda_n$ are eigenvalues of A such that $|\lambda_1| \geq |\lambda_2| \geq ... \geq |\lambda_n|$, then for $\forall x \in \mathbb{R}^n$, that is orthogonal to the eigenspaces of $\lambda_1, \ldots, \lambda_k$, we have $|\langle Ax, x \rangle| \leq |\lambda_{k+1}| \cdot ||x||^2$, i.e, the Rayleigh Quotient $R(A, x) \leq |\lambda_{k+1}|$*

Proof. Let $y_1, \ldots, y_n$ be an orthonormal collection of vectors where y_i is an eigenvector for λ_1. Write $x = \sum_{j=k+1}^{n} \alpha_j \cdot y_j$ (we can do that because x is orthogonal to eigenspaces for λ_i, $i \leq k$). Then

$$\begin{aligned}
|\langle Ax, x \rangle| &= |\langle A \cdot \sum_j \alpha_j \cdot y_j, \sum_j \alpha_j \cdot y_j \rangle| && (18.21)\\
&= |\sum_{j,j'} \alpha_j \alpha_{j'} \cdot \langle A y_j, y_{j'} \rangle| && (18.22)\\
&= |\sum_{j,j'} \alpha_j \alpha_{j'} \cdot \langle \lambda_j y_j, y_{j'} \rangle| && (18.23)\\
&= |\sum_j \lambda_j \alpha_j^2| && (18.24)\\
&\leq \sum_j |\lambda_{k+1}| \cdot \alpha_j^2 && (18.25)\\
&= |\lambda_{k+1}| \cdot ||x||^2 && (18.26)
\end{aligned}$$

The final bound follows because $||x||^2 = \sum_j \alpha_j^2$. ■

18.2.4 Cheegers' Inequality

Cheegers' inequality relates the spectral gap to edge expansion, we'll first introduce the notation of edge expansion.

For a d-regular graph G, define $\lambda(G) = |\lambda_2|$, where $\lambda_1, ..., \lambda_n$ s.t. $|\lambda_1| \geq |\lambda_2| \geq ... \geq |\lambda_n|$ are eigenvalues of the random walk matrix of G. Let $S \subset V$, $|S| \leq \frac{n}{2}$, the *sparsity* of the cut S is $\frac{|\delta(S)|}{|S|}$, where $\delta(S)$ is the number of edges exiting S. Let the edge expansion $h(G) = \min_{S \subset V, |S| \leq \frac{n}{2}} \frac{|\delta(S)|}{|S|}$, i.e, h(G) is a cut of minimal sparsity.

Cheegers' inequality includes a lower bound and upper bound for edge expansion based on $\lambda(G)$, we will introduce and prove the easier part (lower bound) of Cheegers' Inequality.

Theorem 1 *Easier Part of Cheegers' Inequality*
$h(G) \geq \frac{d}{2} \cdot (1 - \lambda(G))$

Proof. Let $S \subset V$, $|S| \leq \frac{n}{2}$ have $h(G) = \frac{|\delta(S)|}{|S|}$.
Let vector x be such that

$$x_u = \begin{cases} -|V - S| & u \in S \\ |S| & u \notin S \end{cases}$$

Note that $x \perp \mathbf{1}$, where $\mathbf{1} = (\frac{1}{n}, ..., \frac{1}{n})$ (since $\sum_u x_u = -|V - S| \cdot |S| + |S| \cdot |V - S| = 0$), so $\langle Ax, x \rangle \leq \lambda(G) \cdot ||x||^2$ by property of Rayleigh Quotient (**claim 6**).
Let $z = \sum_{u,v} A_{u,v} \cdot (x_u - x_v)^2$, then we have

1. $z = \frac{2}{d} \cdot |\delta(S)| \cdot (-|V - S| - |S|)^2 = 2 \cdot |\delta(S)| \cdot n^2/d$.
   The first equality can be seen because any u, v pair with $\notin \delta(S)$ has its corresponding term cancel so the sum is really just twice the sum of $(|S| + |V - S|)^2$ over all edges in $\delta(S)$, divided by d.
2. $$\begin{aligned} z &= \sum_{u,v} A_{u,v} \cdot x_u^2 + \sum_{u,v} A_{u,v} \cdot x_v^2 - 2\sum_{u,v} A_{u,v} x_u x_v && (18.27) \\ &= ||x||^2 + ||x||^2 - 2 \cdot \langle Ax, x \rangle && (18.28) \\ &\geq 2 \cdot ||x||^2 - 2 \cdot \lambda(G) \cdot ||x||^2 && (18.29) \end{aligned}$$
   The second equality can be seen by, say, noting $\sum_{u,v} A_{u,v} x_u^2 = \sum_u x_u^2 \sum_v A_{u,v} = \sum_u x_u^2 = ||x||^2$ and the bound follows from a Rayleigh quotient noting x is orthogonal to the all-1 vector.

It is also easy to see $||x||^2 = |S| \cdot |V - S| \cdot n$. So combine 1 and 2, we have

$$\begin{aligned} \frac{2}{d} \cdot |\delta(S)| \cdot n^2 &\geq (1 - \lambda(G) \cdot |S| \cdot |V - S| \cdot n && (18.30) \\ \frac{|\delta(S)|}{|S|} &\geq d(1 - \lambda(G)) \cdot \frac{|V - S|}{n} && (18.31) \\ &\geq \frac{d}{2} \cdot (1 - \lambda(G)) && (18.32) \end{aligned}$$

where we have used $|V - S| \geq n/2$. ■

References

AB09 S.Arora and B.Barak, Computational Complexity: A Modern Approach, *Cambridge University Press,New York, NY, USA*, 2009, pp. 126–151.