ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institute of Theoretical Computer Science
Mohsen Ghaffari, Angelika Steger, David Steurer, Emo Welzl, Peter Widmayer

Solution 1

You might notice that there is a very short direct proof of Lemma 1 in (c). Even though (a) and (b) are longer than (c) the main point is not just proving Lemma 1 but that of practicing the manipulation of systems of inequalities and seeing that the statement is simply one of many instantiations of Farkas lemma.

(a) The constrains can be interpreted as flow conservation constraints so that for every arc $e = (u, v)$ the variable x_e describes the amount of flow from u to v. Then for $v \in V \setminus \{s, t\}$ the constraint

$$\sum_{e \in \delta(v)^+} x_e - \sum_{e \in \delta(v)^-} x_e = 0$$

is saying that the amount of flow incoming to v is the same as the amount of flow going out from v. For s the corresponding constraint is saying that there is more outgoing flow than incoming flow, i.e., s is a source of flow, and for t the constraints dictate that t is a sink because there is more incoming flow than outgoing flow. It is possible to argue using this flow interpretation but we do not do the proof in such a way.

If there is a directed s-t path P, we can set $x_e = 1$ for every arc e on the path P and $x_e = 0$ for every arc not on P. It is then easy to see that this constitutes a solution to the system by considering separately constraints corresponding to the vertices that are internal vertices on the path P, the endpoints s, t of P and the vertices not on P.

To show the other direction let $\hat{x} \in \mathbb{R}^A$ be a solution to the system given in the exercise description and assume that among all solutions $\hat{x}$ minimizes the total weight $\mathbf{1}^T\hat{x}$. Let $D' = (V, A')$ be a subgraph of D so that A' contains exactly those arcs from A that have positive weight in $\hat{x}$. Observe that D' is acyclic as otherwise we could reduce the weight on all edges of a cycle by some small amount $w > 0$ which would result in a feasible solution with smaller total weight than $\hat{x}$, a contradiction. The weight w can be taken to be the minimum weight of any arc on the cycle.

By considering the constraints we observe that s has at least one outgoing arc in D' and t has at least one incoming arc in D'. Any vertex $v \in V \setminus \{s, t\}$ that is adjacent to an arc in D' is adjacent to at least one outgoing and at least one incoming arc. From these properties and from the acyclicity of D' it then follows that if we start

a directed walk from s in D' we will necessarily reach t eventually which proves the existence of an s-t path since D' is a subgraph of D.

(b) Let us write the equality constrains in a matrix form $\mathbf{Bx} = \mathbf{b}$ where $\mathbf{B} \in \mathbb{R}^{V \times A}$, and $\mathbf{b} \in \mathbb{R}^{V}$. Then for every vertex $v \in V$ and every arc $e = (u, w) \in A$ we have that

$$\mathbf{B}_{v,e} = \begin{cases} 1 & \text{if } u = v \\ -1 & \text{if } w = v \\ 0 & \text{otherwise.} \end{cases} \quad \text{and} \quad \mathbf{b}_v = \begin{cases} 0 & \text{if } v \in V \setminus \{s, t\} \\ 1 & \text{if } v = s \\ -1 & \text{if } v = t. \end{cases}$$

In other words, $\mathbf{B}$ is a matrix whose rows are indexed by the vertices V and whose columns are indexed by the arcs A. In the column corresponding to the arc $e = (u, w)$ there is a 1 at the row corresponding to u and a -1 at the row corresponding to w and remaining entries in the column are 0.

Using Farkas lemma II from the lecture notes we know that exactly one of the two systems $\{\mathbf{Bx} = \mathbf{b}, \mathbf{x} \geq \mathbf{0}\}$ and $\{\mathbf{B}^T\mathbf{y} \geq 0, \mathbf{b}^T\mathbf{y} < 0\}$ has a solution. To prove Lemma 1 we therefore have to show that the second system has a solution if and only if there exists a strong s-t cut. We can write out the second system as

$$\begin{aligned} \forall e = (u, w) \in A: \quad & \mathbf{y}_u - \mathbf{y}_w \geq 0 \text{ and} \\ & \mathbf{y}_s - \mathbf{y}_t < 0. \end{aligned} \tag{1}$$

Assume first that S is a strong s-t cut. Then by setting $y_v = 0$ for $v \in S$ and $y_v = 1$ for $v \in V \setminus S$ satisfies the constraints in (1) in particular because the constraints corresponding to the arcs in the cut $C(S)$ are satisfied due to the strong s-t cut property, the constraints corresponding to edges within S and $V \setminus S$ hold with equality and for the last constraint we have $\mathbf{y}_s - \mathbf{y}_t = 0 - 1 = -1 < 0$ as it should.

To show the other direction assume that there exists a solution $\hat{\mathbf{y}}$ to (1). Define $S := \{v \in V \mid \hat{\mathbf{y}}_v \leq \hat{\mathbf{y}}_s\}$ as the set of vertices that are assigned a value at most $\hat{\mathbf{y}}_s$ in $\hat{\mathbf{y}}$. We claim that S is a strong s-t cut. Firstly, by definition $s \in S$ and by the second inequality of (1) we have $t \notin S$ so S is an s-t cut. Also from the definition of S we observe that for every $u \in S$ and every $w \in V \setminus S$ it holds that $\hat{\mathbf{y}}_u - \hat{\mathbf{y}}_w < 0$. Since $\hat{\mathbf{y}}$ is a solution to (1) this implies that there can be no arcs $(u, w) \in A$ with $u \in S, w \in V \setminus S$ and therefore S is a strong s-t cut. This concludes the proof.

(c) If there is a directed s-t path P, then there can not exist a strong s-t cut since for any set $S \subseteq V$ with $s \in S$ and $t \notin S$ there is at least one arc of P that goes from S to $V \setminus S$. If there is no directed s-t path, we let S be the set of all vertices reachable from S by a directed path. Then S is a strong s-t cut because no vertex of $V \setminus S$ is reachable from a vertex of S.

Solution 2

Assume that the matrix C is wrong in exactly the i-th row compared to the correct product AB. There is at least one error in this row but perhaps there is more than

one error. We define $D = AB - C$ and write $D = (d_{ij})$. This is a zero-matrix except in the i-th row there are some ones. We may assume that the $d_{ij} = 1$. Take a vector $x \in_{\text{u.a.r.}} \{0,1\}^n$ and compute the product Dx. Every entry but the i-th one is zero. We look at the i-th entry of this product and split this up

$$(Dx)_i = \sum_{k=1}^{n} d_{ik}x_k = \underbrace{\sum_{k=1,k\neq j}^{n} d_{ik}x_k}_{=:S} \quad + \quad d_{ij}x_j,$$

where the S is some number, either 0 or 1. The probability that we will detect the error is exactly the probability that $(Dx)_i = 1$. Let x_j be the last entry of x that we choose randomly. Then independent of the value of S we see that $(Dx)_i$ is 0 with probability $\frac{1}{2}$, and it is 1 with probability $\frac{1}{2}$. This means that the probability of detecting an error is exactly $\frac{1}{2}$.

REMARK: What we proved here is that indeed for any vectors $a, b \in GF(2)^n, a \neq b$ fixed and for $x \in_{\text{u.a.r.}} GF(2)^n$

$$\Pr[a^T x = b^T x] = \frac{1}{2},$$

where ^{T} stands for the transpose of a vector.

Solution 3

Let $i, j \in \{1..n\}$ be indices such that A_{ij} is nonzero. Consider the i-th entry $(Ax)_i$ of the matrix-vector product. It calculates as

$$(Ax)_i = \sum_{k\in\{1..n\}\setminus\{j\}}^{n} A_{ik}x_k + A_{ij}x_j.$$

Since the x_i are being chosen independently of one another, we may prescribe any order in which they are evaluated; let us evaluate x_j last. Once all terms in the sum are being fixed, then it takes a fixed real value s. At most one out of the possible choices for x_j can yield $A_{ij}x_j = -s$ and so the probability that this happens is at most $1/3$, yielding the claim.

Solution 4

Let $\{a_1, \ldots, a_d\} \subseteq S$ be a set of d elements. We define the polynomial $p(x_1, \ldots, x_n)$ as

$$p(x_1, \ldots, x_n) := (x_1 - a_1)(x_1 - a_2) \cdots (x_1 - a_d).$$

Note that the only variable occurring in this polynomial is x_1, and the degree of the polynomial is d.

This polynomial evaluates to zero if and only if $x_1 \in \{a_1, \ldots, a_d\}$. The other variables $x_2, \ldots, x_n$ can be set to arbitrary values in S. Therefore, the number of n-tuples $(r_1, \ldots, r_n) \in S^n$ with $p(r_1, \ldots, r_n) = 0$ is exactly

$$\underbrace{d}_{\text{choices for } r_1} \times \underbrace{|S|}_{\text{choices for } r_2} \times \cdots \times \underbrace{|S|}_{\text{choices for } r_n},$$

which is $d \cdot |S|^{n-1}$.