École Polytechnique Fédérale de Lausanne
Prof. Eisenbrand
Assistant: Manuel Aprile

October 28, 2016

**Combinatorial Optimization** (Fall 2016)

# Assignment 5

Deadline: November 4 10:00, into the right box in front of MA C1 563.

Exercises marked with a $\star$ can be handed in for bonus points.

## Problem 1

In class we saw that we can decide whether a graph $G$ has a perfect matching or not looking at the determinant of the Tutte matrix $A_G$, which is a polynomial with variables $x_e, e \in E(G)$. In this exercise we will see a randomized approach to check whether a polynomial is identically 0 or not. This algorithm would then allow us to decide whether $G$ has a perfect matching or not.

1. Prove the following (Schwartz-Zippel Lemma): let $p$ be a polynomial in variables $x_1, \dots, x_n$ of total degree $d$. Assume $p$ is not identically 0, and let $S \subset \mathbb{R}$ be any finite set. If $y_1, \dots, y_n$ are chosen independently and uniformly at random from $S$, then:

$$\Pr[p(y_1, \dots, y_n) = 0] \leq \frac{d}{|S|}$$

   *Hint: use induction on $n$.*

2. Use part 1. to derive a randomized algorithm that takes a polynomial $p$ as an input and returns $p \equiv 0$ or $p \not\equiv 0$. The algorithm should have one-sided error: if it returns $p \not\equiv 0$, then it is correct; if it returns $p \equiv 0$, then the probability that $p \not\equiv 0$ can be made arbitrarily small.

**Solution:**

1. The proof is by induction on $n$. If $n = 1$, $p(x_1)$ has at most $d$ roots. Therefore $\mathbb{P}(p(x_1^*) = 0) \leq \frac{d}{|S|}$.

   Suppose $n > 1$. We write $p$ as a polynomial in $x_n$, with coefficients in $\mathbb{R}[x_1, \dots, x_{n-1}]$:

$$p(x_1, \dots, x_n) = \sum_{i=0}^{k} q_i(x_1, \dots, x_{n-1}) x_n^i$$

   with $k \leq d, q_k \not\equiv 0$. Let $E_1$ be the event that $p(y_1, \dots, y_n) = 0$, and $E_2$ be the event that $q_k(y_1, \dots, y_{n-1}) = 0$. Note that since $q_k$ has degree at most $d - k$, by induction $\mathbb{P}(E_2) \leq \frac{d-k}{|S|}$. Now:

$$\mathbb{P}(E_1) = \mathbb{P}(E_1 \wedge E_2) + \mathbb{P}(E_1 \wedge \neg E_2) \leq \mathbb{P}(E_2) + \mathbb{P}(E_1 \wedge \neg E_2) \leq$$

$$\frac{d-k}{|S|} + \mathbb{P}(E_1 | \neg E_2) \cdot \mathbb{P}(\neg E_2) \leq \frac{d-k}{|S|} + \mathbb{P}(E_1 | \neg E_2) \leq \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}$$

   where in the last inequality we have used the fact that, if $\neg E_2$ holds, the coefficient of $x_n^k$ is not zero, hence $p$ is a polynomial of degree $k$ in $x_n$.

2. The algorithm chooses any $S$ such that $|S| \geq 2\deg(p)$, then samples $M$ points independently and uniformly at random from $S^n$, and evaluates $p$ in those points. If for one of these points $y$ $p(y) \neq 0$, then it returns $p \not\equiv 0$ (note that in this case the answer is correct). If for all the sampled points $p$ evaluates to 0, then the algorithm returns $p \equiv 0$. We now argue that the probability of error is small. Thanks to part 1, if $p \not\equiv 0$, the probability that a random point from $S$ is a root of $f$ is less than $1/2$. Hence, the probability that this happens for each of the $M$ points is at most $\frac{1}{2^M}$, which can be made arbitrarily small.

**Problem 2** ($\star$)

1. Prove that if $M_1$ and $M_2$ are matchings of $G$ and $|M_2| > |M_1|$ then there exists at least $|M_2| - |M_1|$ vertex-disjoint $M_1$-augmenting paths.

2. Prove that if $M$ is a matching of $G$ that is not maximum cardinality then there exists a maximum cardinality matching $M^*$ such that every vertex covered by $M$ is also covered by $M^*$. *Hint: use part 1.*

**Solution:**

1. Consider $M_1 \Delta M_2$. This is the union of alternating paths and even cycles. For each component $H$ of $M_1 \Delta M_2$ if $|E(H) \cap M_2| > |E(H) \cap M_1|$ then $H$ is an $M_1$-augmenting path and $|E(H) \cap M_2| = |E(H) \cap M_1| + 1$. Hence we must have at least $|M_2| - |M_1|$ such augmenting paths. And since each of them is a component in $M_1 \Delta M_2$ they must be vertex disjoint.

2. Let $M$ be a matching of $G$ and suppose that $M$ is not maximum cardinality. Let $M^*$ be a maximum cardinality matching. Then since $|M^*| > |M|$ by part $(i)$ we can find an $M$-augmenting path. Flipping the edges of $M$ along this path we obtain a matching $M'$ where $|M'| = |M| + 1$ and $M'$ covers every vertex that $M$ covers. We then repeat this process until $|M'| = |M^*|$.

**Problem 3** ($\star$)

Suppose you are given an oracle that given a graph $G$, tells you whether $G$ has a perfect matching or not. Show how to use this oracle to determine the maximum cardinality matching of a graph $G(V, E)$.
*Hint: you should modify the graph at each call of the oracle. The total number of calls should be at most $|V| + |E|$.*

**Solution:**
For $k = 0, \ldots, n = |V|$, let $G + k$ be the graph obtained by adding to $G$ $k$ dummy vertices joint to all the vertices of $G$. Since a matching has an even number of nodes, in what follows we only consider values of $k$ of the same parity as $n$. Notice that $G + k$ has a perfect matching if and only if $G$ has a matching of size $\frac{n-k}{2}$. We call the oracle on $G + k$, starting with $k = 0$ (or 1, depending on the parity of $n$) and increasing it, until $G + k$ has a perfect matching. For the minimum such $k$, we know that there is a matching $M$ of size $\frac{n-k}{2}$ and it has maximum cardinality. Now to find such a matching, we remove one edge $e \in E$ from $G + k$ at time and we ask the oracle if this graph has a perfect matching: if it doesn't, then $e \in M$, and we can delete $e$ and its endpoints and continue. If it does, then $e \notin M$ and we delete just $e$ and continue. In this way we will find $M$. The total number of calls is at most $k + |E| \leq n + |E|$.