princeton u. sp'02 cos 598B: algorithms and complexity

Lecture 13: Topological Non-Constructive Methods

Lecturer: *Sanjeev Arora* Scribe:*Nir Ailon & Iannis Tourlakis*

In this lecture we will present the Borsuk-Ulam theorem and present two applications of it.

1 The Borsuk-Ulam Theorem

Let S^n denote the boundary of the $n+1$ dimensional unit ball $B^{n+1} \subseteq \mathcal{R}^{n+1}$. Note that although S^n lives in $n+1$ dimensional space, its surface is an n-dimensional manifold.

Theorem 1 (Borsuk-Ulam)
For every continuous map $f : S^n \to \mathcal{R}^n$, there exists $x \in S^n$ such that $f(x) = f(-x)$.

(Note that the points x and $-x$ on the sphere are called *antipodal points*.)

Example 1 Suppose we have a map from S^2 to $\mathcal{R}^2$ (i.e., we can think of the map as "squishing" a balloon onto the floor). Then the Borsuk-Ulam theorem says there are two antipodal points on the balloon that will be "one on top of the other" in this mapping.

Example 2 Suppose each point on the earth maps continuously to a temperature-pressure pair. Then there are two antipodal points on the earth with the same temperature and pressure.

The following celebrated theorem is implied by the Borsuk-Ulam Theorem.

Theorem 2 (Brouwer's Fixed-Point Theorem)
If $f : B^n \to B^n$ is continuous, then there exists $x \in B^n$ such that $f(x) = x$.

The following statements are all equivalent to the Borsuk-Ulam theorem.

1. For every antipodal continuous function $f : S^n \to \mathcal{R}^n$ (i.e., $f(-x) = -f(x)$) there exists $x \in S^n$ such that $f(x) = 0$. (The Borsuk-Ulam theorem trivially implies this; to see the converse, assume that f is any continuous function and consider the function g defined by $g(y) = f(y) - f(-y)$. Then g is antipodal and so, $g(x) = 0$ for some x. But then for the same x, $f(x) = f(-x)$.)

2. (Lyusternik and Shnirel'man, 1930). We say that $F_1, \ldots, F_k$ is a cover of S^n if $\cup F_i = S^n$. Then for every cover $F_1, \ldots, F_{n+1}$ of S^n where the F_i's are closed sets, there exists a point $x \in S^n$ such that $x, -x \in F_i$ for some i. We show why the Borsuk-Ulam theorem implies this statement and leave the converse as an exercise: Assume we have a closed cover $F_1, \ldots, F_{n+1}$ of S^n. Define a function $f : S^n \to \mathcal{R}^n$ by $f(x) = (d(x, F_1), \ldots, d(x, F_n))$. By the Borsuk-Ulam theorem, there exists y such that $f(y) = f(-y)$. There are two cases. Either there exists a coordinate i such that $f_i(y) = f_i(-y) = 0$ in which case we are done (by the fact that F_i is closed, and hence $y, -y \in F_i$); otherwise, neither y nor $-y$ are in $\cup_{i=1}^n F_i$ and hence, must both be covered by F_{n+1}.
Fact: This theorem is true even if we assume that each F_i is either open or closed.

2 Knesser's Conjecture

Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. We will use the notation $\binom{[n]}{k}$ to mean "all subsets of $[n]$ of size k".

DEFINITION 1 *The* Knesser graph $G_{n,k} = (V, E)$ *has* $V = \binom{[n]}{k}$ *and* $E = \{(F_1, F_2) : F_1 \cap F_2 = \emptyset\}$.

What is the chromatic number $\chi(G_{n,k})$ for the Knesser graph? Knesser observed that $\chi(G_{n,k}) \leq n - 2k + 2$, as we shall also shortly see, and conjectured that $\chi(G_{n,k}) = n - 2k + 2$.

First, note that $\chi(G_{n,k}) \leq n - 2k + 2$ is an *NP-style* statement: if true, it has a short witness, namely, a colouring using no more than $n - 2k + 2$ colours: Let the colour of $F \in V$ be $\min(F \cup \{n - 2k + 2\})$. To see that this works, assume first that two different sets F_1, F_2 have the same colour $i < n - 2k + 2$. Then $i \in F_1 \cap F_2$, and hence $(F_1, F_2) \notin E$. If on the other hand F_1, F_2 both have colour $n - 2k + 2$, then $F_1, F_2 \subseteq \{n - 2k + 2, n - 2k + 3, \ldots, n\}$ which is a set of size $2k - 1$. Hence, F_1, F_2 must have a non-empty intersection, and hence $(F_1, F_2) \notin E$.

Lovász proved Knesser's conjecture in 1978 using the Borsuk-Ulam theorem. Note that he had to prove a *coNP-style statement*, that $\chi(G_{n,k}) > n - 2k + 1$. Lovász's proof was simplified by many people, and the simplest version is from 2002 due to J. Greene (an undergrad at the time!):
PROOF: Let $d = n - 2k + 1$. We want to show that $\chi(G_{n,k}) > d$. Let $X \subseteq S^d$ be any n points in "general position" (by "general position" we mean that at most d points from X lie on any hyperplane passing through the origin). We identify X with $[n]$. Suppose we have a valid colouring of $G_{n,k}$ using d colours. For a point $x \in S^n$, let $H(x)$ denote the open hemisphere of points y such that $y \cdot x > 0$. Define a cover $A_1, \ldots, A_{d+1}$ of S^d as follows: For $i = 1, \ldots, d$, let $A_i = \{x : \exists F \in \binom{X}{k}$ with colour i such that $F \subseteq H(x)\}$. Let $A_{d+1} = S^d \setminus \cup_{i=1}^{d} A_i$.

By the Lyusternik-Shnirel'man version of the Borsuk-Ulam theorem, there exist $x \in S^d$, $i \in [d + 1]$ such that $x, -x \in A_i$. We will now derive a contradiction.

Case 1: $i \leq d$. Then both $H(x)$ and $H(-x)$ contain sets F_1 and F_2, respectively, both of colour i. But since $H(x)$ and $H(-x)$ are disjoint, F_1 and F_2 are disjoint, and hence, they cannot have the same colour (since there is an edge between them).

Case 2: $i = d + 1$. Hence, $x, -x \in A_{d+1}$. Therefore, $H(x)$ contains at most $k - 1$ points from X (otherwise, it would contain some F with colour $j \leq d$ and x would belong to A_j and not to A_{d+1}). Similarly, $H(-x)$ must also contain at most $k - 1$ points from X. Hence $S^n \setminus (H(x) \cup H(-x))$, which is contained in the hyperplane $y \cdot x = 0$, contains at least $n - 2k + 2 = d + 1$ points, a contradiction to the fact that the points in X are in "general position". □

Note that to find points in general position one may draw n points from S^n uniformly and independently at random. With probability 1 this will succeed. A deterministic way to pick the points is to use the so-called moment generating curve. This curve is defined as $\{(t^0, t^1, \ldots, t^d) : t \in \mathcal{R}^+\}$. It is easy to see that no d distinct points from the curve together with the zero point are on the same hyperplane (otherwise, we would have $d + 1$ distinct solutions to the equation $\sum_{i=0}^{d} c_i t^i = 0$). By normalizing the d distinct points we get d points in S^{d-1} with the required properties.

3 Nash Equilibria

Let A and B be payoff matrices of size $n \times m$. This means that when player 1 plays strategy i and player 2 plays strategy j, then players 1 and 2 get payoffs A_{ij} and B_{ij}, respectively. A *mixed strategy* is a pair of vectors $p \in (\mathcal{R}^+)^n, q \in (\mathcal{R}^+)^m$ such that $\sum p_i = \sum q_j = 1$ (i.e., they are probability distributions). The expected payoffs are $p^T Aq$ and $p^T Bq$ for players 1 and 2, respectively.

A *Nash equilibrium* is a mixed strategy (p, q) such that for every p', $p'^T Aq \leq p^T Aq$ and for every q', $p^T Aq' \leq p^T Aq$. This means that no player has an incentive to change his strategy, assuming the other player plays according to the Nash equilibrium.

Theorem 3 (Nash)
For all payoff matrices A and B, there exists a Nash equilibrium.

Note that there is no known polynomial time algorithm for finding the Nash equilibrium. It is easy, however, to verify that a mixed strategy is a Nash equilibrium using an LP.
Proof:[Sketch] Consider the space of all mixed strategies, that is, all vectors with $n+m$ non-negative coordinates such that the first n sum to 1 and the last m sum to 1. This space is homeomorphic to B^{n+m-2}. Each vector is mapped to a "close neighbor" $(p+\epsilon, q+\epsilon')$ which gives the highest increases to the payoffs of p and q. This map is defined continuously and so by Brouwer's theorem it has a fixed point. That is, it has a mixed strategy (p, q) such that no small change of p or q improves the payoffs. $\Box$

4 Nonconstructive profos, NP statements, and coNP statements

In mathematics, *nonconstructive proofs* refer to proofs that use techniques like axiom of choice. For us, this term refers to proofs of statements that cannot be verified in any obvious way in polynomial time. To prove circuit lowerbounds, we need to show something like "Every short circuit for 3SAT fails to compute 3SAT," which has the flavor of a coNP statement. (Recall that in the context of Natural Proofs, the "input" to the proof is the truth table for 3SAT, which has length $N = 2^n$. Enumerating over all circuits of size n^k (say) is a conondeterministic computation that runs in $\log^k N$ time.) In fact, Rudich extended the notion of Natural proofs to *NP-natural proofs* and showed that "NP-style reasoning" probably will not suffice to prove circuit lowerbounds.

In general, complexity lowerbounds seem to involve coNP statements (we'll see some examples in the context of communication complexity soon).

Unfortunately, there are not too many examples of coNP statements proved in discrete mathematics. This makes the Lovász-Kneser theorem special. (Actually there is a sub area in graph theory that consists of many similar statements proved using fixed point theorem.) It is much more common to find NP-style statements proved using nonconstructive methods. Next time Noga Alon will talk about some of them.