tcs math

some mathematics & computation

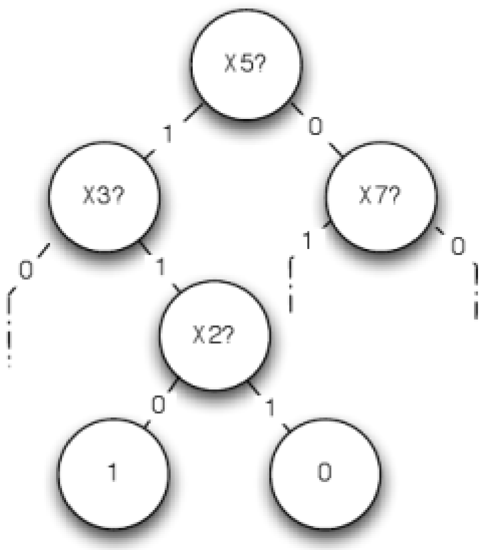
Lecture 7: The evasiveness conjecture

OCTOBER 23, 2008OCTOBER 23, 2008 ~ JAMES

Continuing our look at some toplogical methods, today we'll see the evasiveness conjecture in decision tree complexity. In the next lecture, we'll see how we can sometimes analyze the complexity using fixed point theorems (http://en.wikipedia.org/wiki/Lefschetz_fixed-point_theorem), and their generalizations (like the Hopf index formula (http://en.wikipedia.org/wiki/Poincare-Hopf_theorem)), following the work of Kahn, Saks, and Sturtevant (http://www.cs.washington.edu/homes/jrl/tocmath08/evasive.pdf). These two lectures are co-blogged with Elisa Celis, with a lot of input from (http://arxiv.org/pdf/cs/0205031v1) (http://en.wikipedia.org/wiki/Topological_combinatorics)Lovasz's lecture notes (http://arxiv.org/pdf/cs/0205031v1).

Decision tree complexity and evasiveness

Consider a boolean function $f : \{0,1\}^n \to \{0,1\}$ on n bits. We define the *decision tree complexity* of f as follows. Given an unknown input $x \in \{0,1\}^n$, you are allowed to ask about the values of various bits of x, e.g. $x_{17}, x_{34}, x_3, \ldots$. Your goal is to compute $f(x)$ using as few questions as possible, and your questions can be adaptive, depending on answers to previous questions. The complexity of such a strategy is the maximum number of questions asked for any $x \in \{0,1\}^n$. The decision tree complexity, written $D(f)$, is the minimum complexity of any strategy that computes f. (There are many other interesting models of decision complexity, see e.g. this survey (http://homepages.cwi.nl/~rdewolf/publ/qc/dectree.ps).)



(https://tcsmath.files.wordpress.com/2008/10/dtree.png)

Clearly $D(f) \le n$, because we can trivially query all the bits of x, and then output f(x). A function f is called *evasive* if this upper bound is met, i.e. $D(f) = n$. As an example, consider the parity function $\mathsf{PARITY}(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$, where $\oplus$ is addition modulo 2. Clearly PARITY is evasive because after $n-1$ bits of x are asked about, the setting of the final bit determines the value of f.

For a more general example, consider any $f : \{0,1\}^n \to \{0,1\}$ such that $\#\{x : f(x) = 1\}$ is odd. In this case, for every $i = 1, 2, \ldots, n$, exactly one of $f|_{x_i=0}$ or $f|_{x_i=1}$ has the same property that the number of inputs resulting in a 1 is odd. (These two functions are the natural restriction of f to functions on n-1 bits, which results from fixing the value of the ith bit.) Thus an adversary could keep answering questions "x_i?" so that the restricted function retains this property. Since the number of inputs yielding a 1 is always odd, the restricted function always takes both possible values, implying that f is evasive–the advesary ensures that the value cannot be determined until all n possible questions are asked.

For an example of a *non-evasive* property, think of a point $x \in \{0,1\}^{\binom{N}{2}}$ as speciying a directed graph on N vertices, where there is exactly one directed edges connecting every pair of vertices, and x specifies the direction of this edge (this is called a tournament (http://en.wikipedia.org/wiki/Tournament_(graph_theory))). Thinking of the vertices as players, a directed edge from u to v means that u defeats v. Now $f(x) = 1$ if the digraph specified by x has one vertex that defeats everyone else. What is $D(f)$?

Well, first we can conduct a single elimination tournament, where vertex 1 plays vertex 2, and the winner players vertex 3, and the winner of that players vertex 4, etc. At the end, there is only one remaining vertex i that remains undefeated. Now asking $N-2$ more questions, we can determine whether i indeeds defeats everyone else. The total number of questions was $(N-1)+(N-2) = 2N-3$, hence $D(f) \le 2N-3 \ll \binom{N}{2}$, implying that f is not evasive.

Montone graph properties and the evasiveness conjecture

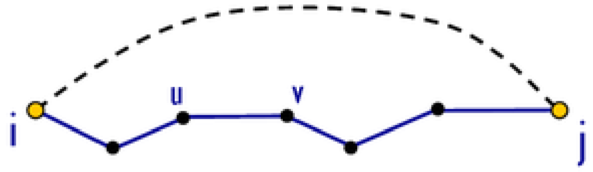
Let $m = \binom{N}{2}$. In general, we can encode an arbitrary *undirected* N-vertex graph as an element $G \in \{0,1\}^m$. A function $f : \{0,1\}^m \to \{0,1\}$ is called a *graph property* if relabeling the vertices of G doesn't affect the value of $f(G)$. The function f is *monotone* if the value of the function can never change from 1 to 0 when flipping one of the input bits from 0 to 1. In the setting of graph properties, this corresponds to those which are maintained under addition of edges to the graph, e.g. $f(G) =$ "is G connected?" or $f(G) =$ "does G have a k-clique?"

Evasiveness Conjecture (Aanderaa-Karp-Rosenberg): Every non-trivial monotone graph property is evasive.

Here, non-trivial means that $f(\bar{0}) \neq f(\bar{1})$, where $\bar{0}$ and $\bar{1}$ denote the all-zeros and all-ones strings, respectively.

For example, consider the example $f(G) =$ "is G connected?" The adversary is simple: When asked about a possible edge $\{i,j\}$, she answers NO unless this answer would imply that the graph is disconnected. In other words, she answers NO unless she has answered NO already for all edges across a cut $(S, \bar{S})$ except for $\{i,j\}$, in which case she has to answer YES.

Now, suppose there is a strategy which figures out the connectivity of G without asking a question about some edge $\{i,j\}$. In this case, the conclusion must be that $f(G) = \text{ YES}$ because the adversary always maintains that by answering everything in the future YES, she could force the graph to be connected. In this case, the edges answered YES have to form a spanning tree of G (otherwise by answering all unasked questions NO, the graph would become disconnected). Consider a path P from i to j in this YES spanning tree. Let $\{u,v\}$ be the edge of P which was asked about last. Clearly the adversary answered YES for $\{u,v\}$, but this contradicts the advesary's strategy. Since $\{i,j\}$ has not been asked yet, the adversary is safe to answer NO for $\{u,v\}$, and still later by answering YES on $\{i,j\}$, she could force the graph to be connected. Thus no such strategy exists, and connectivity is evasive.



(https://tcsmath.files.wordpress.com/2008/10/connect1.png)

A natural generalization of the evasiveness conjecture is to general monotone functions which are invariant under a group acting (http://en.wikipedia.org/wiki/Orbit_(group_theory)#Orbits_and_stabilizers) transitively (http://en.wikipedia.org/wiki/Group_action#Types_of_actions) on the coordinates. For a permutation $\pi \in S_n$, let π act on $\{0,1\}^n$ via $\pi(x_1, \ldots, x_n) = (x_{\pi(1)}, \ldots, x_{\pi(n)})$. We say that $f : \{0,1\}^n \to \{0,1\}$ is invariant under π if $f(x) = f(\pi x)$ for every $x \in \{0,1\}^n$. Let $\mathsf{Sym}(f)$ be the group of all permutations under which f is invariant. We will say that f is *weakly symmetric* if $\mathsf{Sym}(f)$ acts transitively on $\{1, 2, \ldots, n\}$.

Generalized Evasiveness Conjecture: If f is a non-trivial, monotone, weakly symmetric function, then f is evasive.

Clearly this generalizes the previous conjecture because every graph property is invariant under permutations of the vertices (which induces a transitive action on the edges).

A proof when n is prime

We'll end this lecture with a proof of the generalized conjecture which holds when n is prime. The proof will hint at the topological connections coming up in the next lecture.

First, we generalize the proof that f is evasive when $\#\{x : f(x) = 1\}$ is odd. For $x \in \{0,1\}^n$, let $|x|$ denote the hamming weight of x, i.e. the number of 1's in x, and for $f : \{0,1\}^n \to \{0,1\}$, define

$$\mu(f) = \sum_{x : f(x)=1} (-1)^{|x|}.$$

Topologically-minded readers will recognize this as some kind of Euler characteristic (http://en.wikipedia.org/wiki/Euler_characteristic), and this connection will bear out in the next lecture. We claim that if $\mu(f) \neq 0$, then f is evasive. To see this, note that $\mu(f) = \mu(f|_{x_i=0}) - \mu(f|_{x_i=1})$. Hence if $\mu(f) \neq 0$, then one of $\mu(f|_{x_i=0})$ or $\mu(f|_{x_i=1})$ is non-zero, so an adversary can keep answering so that the restriction has $\mu(\cdot) \neq 0$. Finally, notice that if $\mu(f) \neq 0$, then f must take both values 0 and 1, so the adversary can maintain this until all n questions are asked.

Theorem: Suppose n is prime. If $f : \{0,1\}^n \to \{0,1\}$ is monotone, non-trivial, and weakly symmetric, then f is evasive.

Proof: We'll show that $\mu(f) \neq 0$. First, we argue that $\mathsf{Sym}(f)$ contains a cyclic permutation. Write $\mathsf{Sym}(f) = U_1 \cup U_2 \cup \cdots \cup U_n$, where $U_i = \{\pi \in \mathsf{Sym}(f) : \pi(1) = i\}$. By transitivity, we have $|U_1| = |U_2| = \cdots = |U_n|$, hence n divides $|\mathsf{Sym}(f)|$. Now since n is prime, by Cauchy's theorem (http://en.wikipedia.org/wiki/Cauchy%27s_theorem_(group_theory)) there is an element $\sigma \in \mathsf{Sym}(f)$ or order n (i.e. an n-cycle).

Since f is non-trivial, we know that $f(\bar{0}) = 0$ and $f(\bar{1}) = 1$. For any $x \in \{0,1\}^n$ with $x \notin \{\bar{0}, \bar{1}\}$, it is clear that all n elements $x, \sigma x, \sigma^2 x, \ldots, \sigma^{n-1} x$ are distinct, since n is prime. But f is invariant under σ, thus the set $\{x : f(x) = 1\}$ partitions into equivalence classes $S_1, S_2, \ldots, S_k, \{\bar{1}\}$, where $|S_i| = n$ for every i. But this immediately implies that $\mu(f) \equiv 1 \pmod{n}$, which gives $\mu(f) \neq 0$.

POSTED IN CSE 599S, LECTURE, MATH
DECISION TREE COMPLEXITY EVASIVENESS

3 thoughts on "Lecture 7: The evasiveness conjecture"

1. **Amit C**
   SAYS:
   OCTOBER 23, 2008 AT 11:30 AM
   This is by far my favourite use of "higher" mathematics to TCS. You might want to see this paper for some extensions to the Kahn-Saks-Sturtevant work: http://www.cs.dartmouth.edu/~ac/Pubs/sicomp-evasive.pdf.

2. Pingback: Property Testing Lecture 3 « Expanders, Property Testing and the PCP theorem
3. **nils**
   SAYS:

DECEMBER 1, 2008 AT 12:59 PM
I have not seen one new post in weeks.
Is this blog still active?

BLOG AT WORDPRESS.COM.