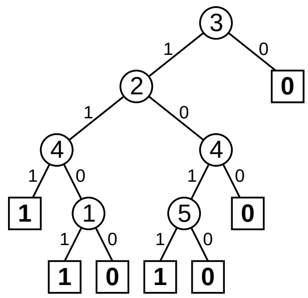
6 Evasiveness of Boolean Functions (February 13, 18, and 20)

6.1 String, Graph, and Digraph Properties

Recall from last time that a *string property* is a boolean function of the form $F : \{0,1\}^n \to \{0,1\}$. A string property is *evasive* if its deterministic decision tree complexity is exactly n, or in other words, if any algorithm that computes the function F must evaluate every input bit in the worst case. In this lecture, we'll develop some general tools for proving evasiveness.

As a simple example, consider the property "three 1s in a row". This property is trivially evasive when $n = 3$, and it is not hard to prove by brute force that it is also evasive when $n = 4$. When $n = 5$, however, the three-consecutive-1s property is *not* evasive, as there is an algorithm that examines at most four input bits:



In the homework, you'll be asked to prove that the three-consecutive-1s property is evasive if and only if $n \bmod 4 = 0$ or 3. We'll develop the necessary tools to prove the lower bound in this lecture.[1]

Most of this lecture will be concerned with *graph properties*, which are a special case of string properties. A graph property is a function of the form $F : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$, where the input bits represent the entries in the adjacency matrix of an undirected graph. We will make the additional assumption that *graph properties are unchanged by any permutation of the vertices.* In other words, we are concerned with properties of unlabeled graphs (connectivity, planarity, hamiltonicity) as opposed to properties of labeled graphs (vertex 17 has degree 42). After all, labeled graph properties are just properties of $\binom{n}{2}$-bit strings.

A graph property is *evasive* if its deterministic decision tree complexity is exactly $\binom{n}{2}$. In the last lecture, we used an adversary argument to prove that connectivity is an evasive graph property. In fact, almost every interesting graph property is evasive: acyclicity, planarity, bipartiteness, hamiltonicity, k-colorability, emptiness, and so forth. In fact, the only properties that are obviously not evasive are trivial: "Is this a graph?" and "Is this a flying pig named Rocco von Finkelstein?". More formally, we say that s graph property is *nontrivial* if at least one graph has the property and at least one graph does not. A graph property is *monotone* if either (1) every subgraph of a graph with the property also has the property, or (2) every supergraph of a graph with the property also has the property.

We can similarly define a *digraph property* as any function of the form $F : \{0,1\}^{n(n-1)} \to \{0,1\}$, where the input consists of the adjacency matrix of a directed graph, that is invariant under permutations of the vertices. A digraph property is evasive if its deterministic decision tree complexity is $n(n-1)$.

For example, let's define a *sink* to be a vertex with in-degree $n-1$ and out-degree 0.

Theorem 1. *The digraph property "having a sink" is not evasive.*

[1] For the $n-1$ upper bound in the non-evasive case, you're on your own!

Proof: We can locate a sink, if it exists, by probing only $O(n)$ bits, using the following algorithm. Observe that if (u, v) is an edge in the input graph, then u cannot be a sink, but it (u, v) is not an edge, then v cannot be a sink. Thus, by probing $n-1$ edges, we can narrow the set of possible sinks down to a single vertex. Once we've done this, we can confirm that this vertex is a sink by checking that its $n-1$ incoming edges are all present and its $n-1$ outgoing edges are all absent. Crudely, we probe at most $3n-3$ edges in the worst case. □

The following conjecture has been open for decades:

Conjecture 2 (Aanderaa-Karp-Rosenberg). *Every nontrivial monotone (di)graph property is evasive.*

The sink example shows that monotonicity is necessary for the conjecture in the case of directed graphs. A somewhat more complicated example ('scorpions') shows that there are nontrivial, non-monotone, non-evasive properties of undirected graphs as well.

6.2 Simple Properties of (Non)Evasive Functions

Given a string/graph/digraph property $F : \{0,1\}^n \to \{0,1\}$, define $F^{-1}(0) = \{x \mid F(x) = 0\}$ and $F^{-1}(1) = \{x \mid F(x) = 1\}$.

Lemma 3. *If $|F^{-1}(0)|$ is odd, then F is evasive.*

Proof: Let v be an arbitrary node in an arbitrary boolean decision tree T. If the depth of v is d, then exactly 2^{n-d} of the possible inputs lead to v. In particular, any node whose depth is at most $n-1$ is reached by an even number of possible inputs. Each input reaches exactly one leaf. Thus, if $|F^{-1}(0)|$ is odd, there must be a leaf that is reached by a single input x with $F(x) = 0$; this leaf has depth n. □

Say that a bit string is *even* if it contains an even number of 1s, and *odd* otherwise.

Lemma 4. *If F is not evasive, then exactly half the strings in $F^{-1}(0)$ are even.*

Proof: This is just a refinement of the previous proof. Let v be an arbitrary node with depth $d < n$. The inputs that reach v have d bits in common, and the remaining $n-d$ bits can take on all 2^{n-d} possible values. Thus, exactly half of the inputs that reach v contain an even number of 1s. Summing over all 0-leaves gives the result. □

Theorem 5. *The string property "at least k 1s" is evasive if and only if $1 \le k \le n$.*

Proof: Let F_k denote the property "at least k 1s". By Lemma 3, if F_k is not evasive, we have

$$\sum_{x \in F^{-1}(0)} (-1)^{\#1(x)} = 0.$$

We can rewrite this sum in terms of binomial coefficients as follows:

$$\sum_{x \in F^{-1}(0)} (-1)^{\#1(x)} = \sum_{i=0}^{k-1} (-1)^i \binom{n}{i} = (-1)^{k-1} \binom{n-1}{k-1}$$

If $1 \le k \le n$, this binomial coefficient is nonzero, so F_k must be evasive. On the other hand, if $k \le 0$ or $k > n$, the property F_k is trivial. □

Corollary 6. *Every nontrivial monotone property of* 3*-vertex graphs is evasive.*

Proof: There are exactly four isomorphism classes of 3-vertex graphs: the empty graph, three graphs with one edge, three graphs with two edges, and the complete graph. Thus, the only nontrivial monotone graph properties are "at least k edges" and "at most $3 - k$ edges", for some $k \in \{1, 2, 3\}$. The result follows immediately from the previous theorem.[2] □

Neither Lemma 3 nor Lemma 4 is a *necessary* condition for evasiveness.

6.3 Permutation Groups

Let $[n]$ denote the set of positive integers $\{1, 2, \ldots, n\}$. A *permutation* is a one-to-one and onto function $\pi : [n] \to [n]$. Permutations can be composed (as functions) and inverted (as functions). The set of all permutations of $[n]$ form a group under composition, called the *symmetric group* S_n, with the trivial permutation as the identity element. In general, a set of permutations that is closed under inverses and composition is called a *permutation group.*

We say that a function $F : \{0,1\}^n \to \{0,1\}$ is *invariant* under a permutation $\pi \in S_n$ if

$$F(x_1, x_2, \ldots, x_n) = F(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

for all bit strings $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$. It is trivial to check that the set of permutations under which F is invariant form a permutation group.

Recall that a graph property must be invariant under relabellings of the vertices, or equivalently, under any permutation of the edges that is induced by a permutation of the vertices. Given any permutation $\pi : [n] \to [n]$, we can define the permutation $\pi' : \binom{[n]}{2} \to \binom{[n]}{2}$ over the set of unordered pairs in $[n]$ as follows:

$$\pi'\{i, j\} = \{\pi(i), \pi(j)\}$$

The set $\{\pi' \mid \pi \in S_n\}$ is a permutation group called the *pair group.*

We say that a permutation group Γ is *transitive* if for any pair of ground elements i and j, there is a permutation $\pi \in \Gamma$ such that $\pi(i) = j$. It is easy to verify that the pair group is transitive. The Aanderaa-Karp-Rosenberg conjecture is actually a special case of the following more general hypothesis.

Conjecture 7. *Every nontrivial monotone string property that is invariant under a transitive permutation group is evasive.*

The nontrivial monotone string properties that are invariant under the full symmetric group are precisely the "at least k 1s" properties that we proved evasive in Theorem 5 (and their complements).

6.4 The Rivest-Vuillemin Theorem

For the special case where n is the power of a prime number, Conjecture 2 was proved by Ron Rivest and ?? Vuillemin. In fact, they proved the following slightly stronger result.

Theorem 8 (Rivest-Vuillemin). *If n is a prime power, $F : \{0,1\}^n \to \{0,1\}$ is invariant under a transitive permutation group, and $F(0, 0, \ldots, 0) \neq F(1, 1, \ldots, 1)$, then F is evasive.*

[2] This was overkill. It's easy to prove this result directly from Lemma 2.

We will prove this theorem using Lemma 4, but first we need to develop a few more facts about permutations. Every permutation $\pi : [n] \to [n]$ on the input coordinates induces a permutation $\hat{\pi} : \{0,1\}^n \to \{0,1\}^n$ on the set of possible input strings:

$$\hat{\pi}(x_1, x_2, \ldots, x_n) = (x_{\pi(1)}, x_{\pi(1)}, \ldots, x_{\pi(n)})$$

Let Γ be the permutation group under which F is invariant, and let $G = \{\hat{\pi} \mid \pi \in \Gamma\}$ be the induced permutation group of input vectors. We define the *orbit* of a string x (under G) to be the set of images of x under permutations in G:

$$\text{orbit}(x) = \{\hat{\pi}(x) \mid \hat{\pi} \in G\}$$

Note that if $y \in \text{orbit}(x)$, then $x \in \text{orbit}(y)$, and thus $\text{orbit}(x) = \text{orbit}(y)$.

For example, if F is a graph property, then Γ is the pair group, each input x represents a labeled graph, and $\text{orbit}(x)$ is the set of all labeled graphs isomorphic to x (or equivalently, the underlying unlabeled graph).

Every input string in an orbit obviously has the same number of 1s. In particular, the constant strings $\vec{0} = (0, 0, \ldots, 0)$ and $\vec{1} = (1, 1, \ldots, 1)$ have singleton orbits: $\text{orbit}(\vec{0}) = \{\vec{0}\}$ and $\text{orbit}(\vec{1}) = \{\vec{1}\}$. Also, the function F is constant over any orbit; that is, $F(x) = F(y)$ for any $y \in \text{orbit}(x)$.

Proof of Theorem 8: Let $n = p^e$ for some prime p. I claim that for any string x except $\vec{0}$ or $\vec{1}$, the size of the orbit of x is a multiple of p. The orbit of x clearly has more than one element in this case. We can trivially write

$$\sum_{y \in \text{orbit}(x)} \#1(y) = \sum_{y \in \text{orbit}(x)} \sum_{i=1}^{n} y_i = \sum_{i=1}^{n} \sum_{y \in \text{orbit}(x)} y_i.$$

Since Γ is transitive, there must be a permutation $\pi \in \Gamma$ such that $\pi(i) = 1$. Thus the inner summation does not actually depend on i.

$$\sum_{y \in \text{orbit}(x)} \#1(y) = n \sum_{y \in \text{orbit}(x)} y_1.$$

Since all bit strings in the orbit have the same number of 1s, we have

$$\sum_{y \in \text{orbit}(x)} \#1(y) = |\text{orbit}(x)| \cdot \#1(x).$$

Thus, $|\text{orbit}(x)| \cdot \#1(x)$ is a multiple of $n = p^e$. Since $\#1(x)$ is not a multiple of n, this implies that $|\text{orbit}(x)|$ is a multiple of p.

Lemma 4 implies that F is evasive if

$$\Sigma = \sum_{x \in F^{-1}(0)} (-1)^{\#1(x)} \neq 0.$$

If $F(x) = 0$, then the orbit of x contributes

$$\sum_{y \in \text{orbit}(x)} (-1)^{\#1(x)} = |\text{orbit}(x)| \cdot (-1)^{\#1(x)}$$

to this summation, since all bit strings in $\text{orbit}(x)$ have the same number of 1s. Except for the cases $x = \vec{0}$ and $x = \vec{1}$, this is a multiple of p. Since exactly one of the strings $\vec{0}$ and $\vec{1}$ is in $F^{-1}(0)$, the sum Σ is either one more or one less than a multiple of p. In either case, $\Sigma \neq 0$, so F must be evasive. $\square$

6.5 Nontrivial Monotone Graph Properties are Weakly Evasive

The Rivest-Vuillemin Theorem is not immediately useful for graph properties, since $\binom{n}{2}$ is only a power of a prime when $n = 2$ or $n = 3$. However, by combining this theorem with the Little Birdie Principle, we can prove a *weak* form of the Aanderaa-Karp-Rosenberg conjecture.

First consider the case where the number of vertices is a power of two.

Theorem 9. *Let $n = 2^k$. Every nontrivial monotone graph property of n-vertex graphs has deterministic decision tree complexity at least $n^2/4$.*

Proof: Let $F : \{0,1\}^n \to \{0,1\}$ be a nontrivial monotone graph property. For any integer j, let G_j be the graph consisting of $n/2^j$ disjoint copies of the clique K_{2^j}. In particular, G_0 is the empty graph on n vertices, and G_k is the complete graph on n vertices. Without loss of generality, assume that $F(G_0) = 1$ and $F(G_k) = 1$. By monotonicity, there is a unique index j—which we know—such that $F(G_j) = 1$ but $F(G_{j+1}) = 0$.

Now suppose a little birdie tells us that each the induced subgraph of vertices 1 through $n/2$ consists of $n/2^{j+1}$ disjoint copies of K_{2^j}, as does the induced subgraph of vertices $n/2+1$ through n. Now only $n^2/4$ of the $\binom{n}{2}$ input bits actually matter, namely pairs i, j where $i \le n/2$ and $j > n/2$. Let $F' : \{0,1\}^{n^2/4} \to \{0,1\}$ denote the induced (bipartite graph) property on these bits.

Since n is a power of two, $n^2/4$ is a power of a prime. $F'(\vec{0}) \ne F'(\vec{1})$, since $F'(\vec{0}) = F(G_j) = 1$ and $F'(\vec{1}) = F(G_{j+1} + \text{some edges}) = 0$. Finally, F' is invariant under a transitive automorphism group induced by the vertex permutations that leave the little birdie information fixed.

Thus, by the Rivest-Vuillemin theorem, F' is evasive. Finally, the Little Birdie Principle implies that $D(F) \ge D(F') = n^2/4$. □

Let $m(n)$ denote the minimum complexity of any nontrivial monotone graph property on graphs with n vertices. The previous theorem implies that $m(2^k) = 4^{k-1}$; the AKR conjecture is that $m(n) = \binom{n}{2}$.

Theorem 10. $m(n) \ge \min\{m(n-1), 2n^2/9\}$

Proof: Let $F : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be any nontrivial monotone property on n-vertex graphs, where $F(\vec{0}) = 1$. (That is, the empty graph has property F.) To prove the theorem, we need to show that $D(F) \ge \min\{m(n-1), 2n^2/9\}$.

We define two *restrictions* of F as follows: F_+ is the restriction of F to graphs where one vertex has degree $n-1$, and F_- is the restriction of F to graphs where one vertex has degree zero. Each of these functions is actually a monotone property of the remaining $(n-1)$-vertex graph. The Little Birdie Principle implies immediately that $D(F) \ge \max\{D(F_+), D(F_-)\}$.

This observation does not make the theorem trivial; either F_+ or F_- could be trivial properties. Let G_+ be a star graph with n vertices, where one vertex has degree $n-1$ and all other vertices have degree 1. F_+ is a restriction of F to supergraphs of G_+; thus, if $F(G_+) = 0$, then by monotonicity, $F_+ \equiv 0$. Similarly, let G_- be a clique on $n-1$ vertex plus an isolated vertex of degree zero. F_- is a restriction to subgraphs of G_-, so if $F(G_-) = 1$, then $F_- \equiv 1$. If either F_+ or F_- is nontrivial, then $\max\{D(F_+), D(F_-)\} \ge m(n-1)$, and the lemma is proved. However, if both restrictions are trivial (for example, if F is "disconnectedness"), we have to consider a third case.

Suppose both F_+ and F_- are trivial, so $F(G^+) = 0$ and $F(G^-) = 1$. Let p be a prime number between $n/3$ and $2n/3$, which must exist by Erdős's Non-Fields-Medal Proof.[3] We define a new restriction $F_\times$ of F to graphs where the induced subgraph on the vertices $L = \{1, 2, \ldots, p\}$ is empty, and the induced subgraph on the remaining vertices $R = \{p+1, p+2, \ldots, n\}$ is complete. $F_\times$ is a monotone property of $p \times (n-p)$ bipartite graphs. The Little Birdie Principle implies that $D(F) \geq D(F_\times)$.

The graph represented by $\vec{1}$ is a supergraph of G_+, so $F_\times(\vec{1}) = 0$, and the graph represented by $\vec{0}$ is a subgraph of G_-, so $F_\times(\vec{0}) = 1$. Thus, $F_\times$ is nontrivial. Also, $F_\times$ is invariant under the group Γ of edge permutations induced by permutations of the vertex set L. (Note that this group is *not* transitive!)

To complete the proof, we show that $F_\times$ is evasive, using roughly the same argument as the proof of the Rivest-Vuillemin theorem.

For any vertex $x \in R$, let $C(x)$ denote the graph consisting of edges between x and every vertex in L. Consider a *nonempty* bipartite graph $A \subseteq L \times R$, such that $F_\times(A) = 1$. This graph must contain a vertex $x \in R$ such that $|A \cap C(x)| = q$, where $1 \leq q \leq p-1$. (If $x \in R$ were connected to every vertex in L, then monotonicity would imply that $F_\times(A) = 0$.) For any graph B in the orbit of A, we have $|A \cap C(x)| = q$, since the permutation group Γ leaves x fixed. Thus,

$$\sum_{B \in \text{orbit}(A)} |B \cap C(x)| = q|\text{orbit}(A)|.$$

On the other hand, since the permutation group Γ is transitive over the vertices in L, every edge of $C(x)$ appears equally often in the sum $\sum_{B \in \text{orbit}(A)} |B \cap C(x)|$. Thus, $q|\text{orbit}(A)|$ must be a multiple of p; since $q < p$, this implies that $|\text{orbit}(A)|$ is a multiple of p.

Lemma 4 implies that $F_\times$ is evasive if

$$\Sigma = \sum_{A \in F_\times^{-1}(1)} (-1)^{\#1(A)} \neq 0,$$

where $\#1(A)$ is the number of edges in A. The orbit of any graph $A \in F_\times^{-1}(1)$ contributes

$$\sum_{B \in \text{orbit}(A)} (-1)^{\#1(A)} = |\text{orbit}(A)| \cdot (-1)^{\#1(A)}$$

to Σ, since all graphs in orbit(A) have the same number of edges. Except when $A = \vec{0}$, this contribution is a multiple of p. Thus, since $F(\vec{0}) = 1$, the sum Σ is one more than a multiple of p and so must be nonzero. Lemma 4 now implies that $F_\times$ is evasive, and our proof is complete. □

Corollary 11. *Every nontrivial monotone graph property of n-vertex graphs has deterministic decision tree complexity $\Omega(n^2)$.*

[3]The short version of this story is that someone else won the Fields Medal (the equivalent of the Nobel Prize in mathematics) for independently discovering Erdős's proof from the Book[4] that there is at least one prime number between any integer and its double. By the time people realized the significance of Erdős's later work in combinatorics, he was too old; only mathematicians under 40 are eligible for the Fields Medal. *Good Will Hunting* notwithstanding, no combinatorialist has ever won the Fields Medal; combinatorics isn't considered "real" math.

[4]Erdős believed that the Supreme Fascist (God) holds a Book in which the simplest, most elegant proofs of every mathematical result are written; a few very lucky mathematicians are granted a peek at the Book before they are born, and then spend their lives trying to remember what they saw. Most mathematicians believe in the Book[5], even if they don't believe in the S.F.

[5]Unfortunately for Erdős, Gödel discovered a Book proof that the Book is either incomplete or inconsistent!

6.6 Simplicial Complexes...

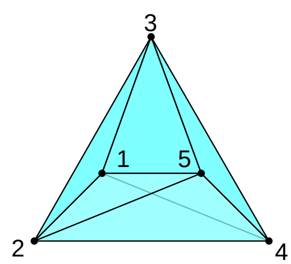
The strongest attacks on the AKR conjecture use tools from discrete topology: simplicial complexes, collapsibility, Euler characteristics, fixed points, etc. I won't have time to cover these results in their full glory, but in this last lecture on evasiveness, I want to describe at least the basic connections between evasiveness and topology. For more details, see Lovász and Young's "Lectures on Evasiveness of Graph Properties".

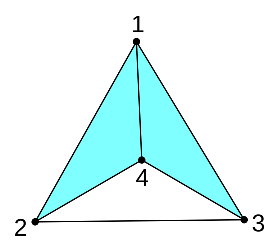
An *(abstract) simplicial complex* is a nonempty collection Δ of sets that is closed under taking subsets; that is, if $A \in \Delta$ and $B \subset A$, then $B \in \Delta$. In particular, every simplicial complex contains the empty set as a member, and the intersection of any two sets is another set in the complex. The elements of the sets in Δ (not the elements of Δ itself!) are called the *vertices* of the complex. We will consider only finite simplicial complexes.[6] As a matter of convenience, we will identify the vertices of any complex with the integers from 1 to n.

Any simplicial complex Δ can be realized as a *geometric* simplicial complex $\overline{\Delta}$ in $\mathbb{R}^n$ as follows. We identify each vertex i with the point e_i at unit distance from the origin on the ith coordinate axis. The convex hull of any subset of vertices is a *simplex*—a point, segment, triangle, tetrahedron, and so on. For each set $A \in \Delta$, the the geometric complex $\overline{\Delta}$ contains the simplex $\overline{A}$ whose vertices are the points corresponding to the elements of A. It is easy to verify that any two simplices in $\overline{\Delta}$ intersect only at a common boundary face, which is also a simplex in $\overline{\Delta}$; specifically, we have $\overline{A} \cap \overline{B} = \overline{A \cap B}$ for any pair of sets $A, B \in \Delta$.

All our arguments will deal directly with abstract complexes, but in the interest of intuition, we will adopt terminology from the geometric setting. Thus, the sets in any simplicial complex Δ are called *simplices*, and the subsets of any simplex are called its *faces*. If A is a face of B, we also say that B is a *co-face* of A. A simplex is *maximal* if it has no proper co-faces. The *dimension* of a simplex A is $|A| - 1$; in particular, the empty set has dimension -1.

A nonempty simplex $A \in \Delta$ is *free* if it has exactly one maximal proper co-face, that is, if there is exactly one maximal simplex that contains A as a face. We can *collapse* any free simplex by removing it and all its cofaces from the complex. Finally, a simplicial complex Δ is *collapsible* if there is a sequence of collapses that reduces Δ to a single point. Collapsible complexes have no interesting topology like loops or bubbles.[7] In particular, a complex consisting of a single simplex and its faces is always collapsible.





Left: A collapsible simplicial complex, consisting of a tetrahedron, three triangles, and their faces.
Right: A noncollapsible simplicial complex consisting of two triangles, an edge, and their faces.

[6]So we will ignore all sorts of interesting examples, like the set of open intervals on the real line, or the set of all finite sets of integers. Too bad.

[7]Readers familiar with topology should recognize that every (geometric realization of a) collapsible complex is *contractible*: it can be continuously deformed to a single point. The converse is not true, however; there are contractible but non-collapsible complexes.

6.7 ...are Monotone Boolean Functions!

For any simplicial complex Δ with n vertices, we can define a boolean function $F_\Delta : \{0,1\}^n \to \{0,1\}$ such that $F_\Delta(x_1, x_2, \ldots, x_n) = 1$ if and only if the set $\{i \mid x_i = 1\}$ is an element of Δ. The definition of simplicial complex implies that this function is monotone. We say that the complex Δ is *evasive* if the corresponding function F_Δ is evasive.

Conversely, let $F : \{0,1\}^n \to \{0,1\}$ be any monotone boolean function, where $F(\vec{0}) = 1$. We can define a set of subsets of $[n]$ as follows:

$$\Delta_F = \{\{i \mid x_i = 1\} \mid F(x_1, x_2, \ldots, x_n) = 1\}.$$

It is trivial to check that since F is monotone, then Δ_F is an abstract simplicial complex! Moreover, the previous construction recovers the original function: $F_{\Delta_F} = F$. For monotone functions where $F(\vec{0}) = 0$, we can define $\Delta_F = \Delta_{1-F}$. Thus, we have a two-to-one correspondence between monotone boolean functions and simplicial complexes. We say that a monotone boolean function F is *collapsible* if the corresponding simplicial complex Δ_F is collapsible.

Notice that Δ_F consists of a simplex with n vertices (and its faces) if and only if F is trivial.

The following lemma illustrates why we just went through this rewriting exercise:

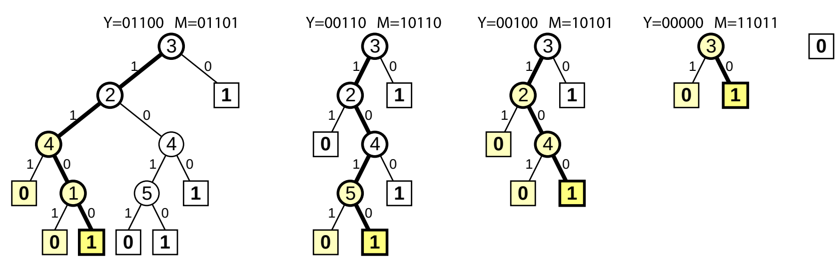
Lemma 12 (Kahn-Saks-Sturtvesant). *Any non-evasive monotone boolean function (or simplicial complex) is collapsible.*

Proof: Let F be a non-evasive boolean function with $F(\vec{0}) = 1$, let Δ be the corresponding simplicial complex, and let T be a boolean decision tree with depth less than n that computes F. By convention, if the bit queries at any node is 1, we branch to the left. The fact that F is monotone is equivalent to saying that the 1-leaves in T are exactly the leaves that are right children.

For any leaf ℓ in T, we define two bit strings: $Y(\ell)$ is the string with the *minimum* number of 1s that reaches ℓ, and $M(\ell)$ is the input with the *maximum* number of 1s that reaches ℓ. In other words, $Y(\ell)$ contains 1s only in positions where the algorithm *knows* there is a one, and $M(\ell)$ contains 0s only in positions where the algorithm *knows* there is a zero. Note that $Y(\ell) \neq M(\ell)$ if and only if the depth of ℓ is less than n. (These strings play exactly the same role as the graphs Y and M in the adversary argument for connectivity.)

We prove that Δ is collapsible by induction on the number of 1-leaves. If T has a single 1-leaf, the complex Δ is just a simplex, and the vertices of Δ are indicated by the string $M(\ell)$. As we noted earlier, every simplex is collapsible.

Otherwise, let ℓ be the leftmost 1-leaf in T. It is straightforward to prove that the simplex corresponding to $Y(\ell)$ is free in Δ; its unique coface is the simplex corresponding to $M(\ell)$. We can collapse the free simplex by changing ℓ to a 0-leaf and then shrinking any subtree with only 0-leaves to a single 0-leaf. The resulting tree T' computes a boolean function F', which is obviously non-evasive and easily seen to be monotone. Thus, by the inductive hypothesis, that the corresponding complex Δ' is collapsible, which implies that Δ is collapsible. $\square$



Collapsing the tree for the 5-bit property "no 111"

Finally, we can rephrase the Aanderaa-Karp-Rosenberg conjecture into topological terminology as follows. An *automorphism* of a simplicial complex is a bijection from the complex to itself. This is the equivalent of an invariant permutation; in fact, we can specify an automorphism by describing how it permutes the vertices. The set of automorphisms of a complex Δ form a group $\mathrm{Aut}(\Delta)$, which is called *vertex-transitive* if, for any vertices v and w, there is an automorphism in the group that maps v to w.

Conjecture 13 ("Aanderaa-Karp-Rosenberg"). *Any collapsible simplicial complex with a vertex-transitive automorphism group is a simplex.*[8]

The following weaker result can be proved using Brouwer's fixed point theorem—Every map from a contractible space to itself has a fixed point—and the fact that any fixed point of any automorphism of a simplicial complex is the center of mass of one of its faces.

Theorem 14 (¿Lovász?). *Let Δ be a collapsible simplicial complex. If $\mathrm{Aut}(\Delta)$ has a transitive subgroup Γ, which has a normal subgroup Γ' of size p^e for some prime p and positive integer e, such that the quotient group Γ/Γ' is cyclic, then Δ is a simplex.*

This theorem implies (with some effort) that if $n = p^e$, then any nontrivial monotone n-vertex graph property is evasive. This is the most general case of the Aanderaa-Karp-Rosenberg conjecture known to be true.

[8] My Berkeley course notes say "This conjecture is expected to be false." I have no idea why.