Problem exchange weekend

June 2, 2011

The bunkbed conjecture (EA)

Let G be an undirected graph. Construct another graph G' as follows. For each vertex x in G, we have two vertices x_0 and x_1 in G'. Vertices with subscript 0 form the 'lower layer', the other the 'upper layer'. Add an edge (x_i, y_i) in G' (observe x_i and y_i are from the same layer!) for each edge (x, y) in G. For some arbitrarily chosen subset T of nodes of G, add an edge between x_0 and x_1 for each $x \in T$ and contract it (that is, identify x_0 and x_1. The new vertex is still called x_0 or x_1 for convenience).

We now choose an edge subset F of G' uniformly at random. The bunkbed conjecture is: for any vertices x, y in G, we have
$P(F$ contains a path from x_0 to $y_0) \geq P(F$ contains a path from x_0 to $y_1)$, for any choice of T.

This problem has received some attention (first posed in 1985) but no real progress has been made towards the general case.

Voting in circles (EA)

warning: soft question

Suppose we want to decide in a democratic way (by some definition) whether (i) build a statue of a cat (ii) build a statue of a dog (iii) build no statue.

A common way to decide this is to let voters give a number from $[0, 1]$ where 0 represents strongly wishing for building the cat statue, 0.5 no statue, 1 dog statue, compute the average of the votes and let the location of the average decide in some justified manner. This presupposes (iii) is a middle option of (i) and (ii), perhaps using the theory of cat-lovers and dog-lovers being disjoint. However *it is possible* that you simply like statues, and think (iii) is a worst option of the three.

The natural solution, then, would be to allow voters to cast their votes on S^1, the circle, rather than $[0, 1]$, and let you cast your vote between (i) and (ii), far from (iii). The new problem that arises is: what to do with the data? There are at least two approaches: either put up reasonable criteria a 'choice function' should have, or just propose a mathematical model and analyse it. The latter will be done here.

Specifically, we imagine the three choices to be three equally spaced marks on S^1, and let $x_1, \ldots, x_n$ be the votes given. One model that reduces to the take-the-mean model if all votes lie on the arc from (i) to (ii) going through

(iii), is: let the 'vote of society' be any $x^* \in S^1$ such that

$$\sum_{i=1}^{n} \mathrm{dist}(x_i, x^*)^2$$

is minimized among all choices of x^*.

A yet more natural model, reducing to the median in the $[0,1]$ case, is: let the vote of society be any $x^* \in S^1$ such that

$$\sum_{i=1}^{n} \mathrm{dist}(x_i, x^*)$$

is minimized among all choices of x^*.

Here $\mathrm{dist}(p,q)$ is the length of the shortest arc, clockwise or counter-clockwise, from $p \in S^1$ to $q \in S^1$. For definiteness, S^1 has perimeter 1.

Comment: When electing a best candidate, as opposed to electing a distribution of seats in a parliament, there are some good reasons for using the median rather than averages (and to consider the elements of $[0,1]$ to be nothing more than elements of a totally ordered set). As far as I know, there is no good reason to use the average at all (compared to some other number lying inside the range of numbers).

Questions (refer to the generalized median)

Is there a nice characterisation of the minima? (They can easily be computed in $O(n)$ time where n is the number of voters. The question is whether there is any nice expression for their location. If this question was asked for $[0,1]$ rather than S^1, then $\frac{x_1+\cdots+x_n}{n}$ would be an answer.)

Are there other natural solutions to the original problem?

How should multiple minima be interpreted?

How likely are multiple minima? (common sense says they are quite common (but concentrated), a quantitative solution to this question is to prefer)

Characterize the sets of votes giving the same output.

Miscellaneous problems (EA)

(some of unassessed difficulty)

Problem: Any number not a power of two can be represented as the sum of two or more consecutive positive integers. What can be said about sums of squares of consecutive positive integers?

Problem (from Jonas Karlsson): For a fixed n, consider the set $S = \{k :$ there is no graph on n vertices with exactly k triangles$\}$. Calculate $\min S$ as a function of n. Known: The answer is $\binom{n}{3} - O(n^2)$ (probably a poor bound).

Problem (threshold cryptography): Given some data, say a bit string of length l, we would like to send data to n servers, possibly different data to each server, such that

- the data stored at any k servers together determine the original data uniquely.
- the data stored at any $k-1$ servers together give no (or essentially no) information about the original data.

There are many solutions to this, of varying space and time performances. An easy case is $k = n$ where we can send random l bit strings to $n-1$ of the servers and send s to the remaining one, where s is the bitwise xor of these random strings and the original message. The idea that any k points on a degree $k-1$ polynomial curve determine the polynomial leads in a natural way to a solution using so-called Reed-Solomon codes (certain error-correcting codes). The idea that any k vectors out of n randomly chosen vectors in $\mathbb{R}^k$ (in an actual application this should probably be replaced by a vector space over a finite field instead) are linearly independent similarly leads to another kind of error-correcting-codes solution. **Soft question:** Provide other examples of mathematical concepts for which statements like "any k out of n taken from X determine [some data], but no $k-1$ do" can be made, and try to come up with a threshold cryptography scheme based on them.

Interesting illumination problems by Joseph O'Rourke:
Problem: Put a radial light source in the origin. Is it possible to trap light from escaping to infinity using a finite number of reflecting disjoint closed line segments?
Problem: Given any polygon with reflecting sides, is there necessarily a point P inside the polygon such that any other point in the polygon 'sees' P (think of a polygonal hall of mirrors)?
In one version, we have absorbing corners. In another we have small circular corners. Both versions are unsolved. There exist non-illuminable non-polygonal regions in the plane.