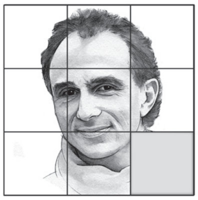

DOI:10.1145/2670917

Dennis Shasha

Upstart Puzzles

Proving without Teaching/ Teaching without Proving

Amazing Sand Counter claims to know the number of grains in the bucket just by looking at it. Do you believe him?

PETER WINKLER'S MATHEMATICALLY elegant, often whimsical puzzles have been a joy to read and wrestle with. My columns now embark on a different path. Each will come in two parts: one quite doable, for which I will provide a solution, the other an "upstart," or insolent variant, I do not know how to solve and that will be an open problem for the community. Here we go.

"Zero knowledge" proofs entail interaction between someone (the Prover) asserting a statement and someone else (the Verifier) determining whether it is true. The proofs give zero knowledge to the Verifier, as the Verifier gains no knowledge other than that the statement is true, either absolutely or beyond a reasonable doubt.[1] The statement in question is normally of a mathematical nature, but, in this case, it resembles, well, child's play.

Imagine the charming gentleman in the figure calls himself the Amazing Sand Counter. He says if he sees a bucket of sand, he will know how many grains are in it, though he will not tell you the number. Your task is to determine whether he is telling the truth beyond a reasonable doubt. Here are the rules of engagement: You may send him out of the room, put a tent over yourself and the bucket, and add or remove a few grains from/to the bucket. He will answer any question that will not give you information about the total number of grains in the bucket. This is the easy part. Try solving it before reading on.

Solution. Send him out of the room, cover yourself with a tent, take a few grains you count, put them in your pocket, remove the tent, invite him to return to the room, and ask him how many grains you have removed. Do this as many times as you like. If Amazing passes many such tests, then you know beyond a reasonable doubt he knows how many grains are in the bucket (assuming no X-ray vision), because the only information he has is that he is able to look at the bucket. In the meantime, you still have not learned any more than you might by simply counting the number of grains you added or removed.

Upstart, or open-problem, variant. Suppose Amazing says there are N grains. You do not necessarily believe him. Your task is to design a protocol that determines whether he is telling the truth. That protocol should take less than $O(\text{sqrt}(N))$ time. Here are the operations you are allowed (all taking $O(1)$ time): counting a single grain; dividing the bucket into approximately equal portions (the grains may have different shapes and weights so you can approximate divisions only by two); and asking a question of Amazing whose answer may or may not be true. You have many buckets at your disposal. You win if, in less than $O(\text{sqrt}(N))$ time, you determine he is telling the truth or catch him lying (even once) with probability at least ½. Otherwise, he wins.

Reference

1. Goldwasser, S., Micali, S., and Rackoff, C. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing 18*, 1 (Feb. 1989), 186–208.

All are invited to submit solutions and prospective upstart-style puzzles for future columns to upstartpuzzles@cacm.acm.org

Dennis Shasha (dennisshasha@yahoo.com) is a professor of computer science in the Computer Science Department of the Courant Institute of New York University, New York.

COLLAGE BY ANDRIJ BORYS ASSOCIATES/SHUTTERSTOCK