Homework 21

Joe Baker, Brett Schreiber, Brian Knotten

March 14, 2018

35

Determining whether a given set S is a certain size can be proven using a AM proof system with a constant number of steps as follows:

The trick is that Arthur will randomly generate a finite number of hash functions. Let $h_i(x) = r_i$ denote a given hash function and its resultant string. Let n be the number of hash functions Arthur generates. Along with these hash functions, Arthur will generate n random strings.

In the first round, Arthur sends over the n hash functions and n strings. If S is in fact a sufficiently large set, then Merlin should be able to find a certain number of strings x in S that resolve to a portion of the n random strings. Merlin is powerful enough to try every string in S against each of the n hash functions. Let this number of strings be m such that $m < n$. If S is not a large enough set to produce m correct strings, then Merlin tries to lie to Arthur by sending over meaningless strings that don't resolve any of the hash functions or are not in S. Merlin passes these m strings back to Arthur.

Arthur can then check these m strings and resolve that in fact there are at least m strings in the language or not. At this point Arthur can verify or falsify that S is sufficiently large.

The trick is to find clever values of m and n such that they can be satisfied if S is sufficiently large (that is, twice as large as the lower bound).