Homework 22

Joe Baker, Brett Schreiber, Brian Knotten

March 16, 2018

36

In an MAM protocol, Arthur makes the wrong decision on the first round with probablility $\frac{1}{3}$. But this probability can be as low as $\frac{1}{4^m}$, where m is the number of bits that Merlin sends over. For proving some strings, Merlin may only need to send over 1 bit of information (like when proving an instance of GRAPH-NON-ISO). But Merlin can send m bits instead as a proof against m different tests. (In GRAPH-NON-ISO, Arthur sends over m relabeled graphs, each randomly corresponding to either G_0 or G_1, to which Merlin responds with m bits where the ith bit of m corresponds to the ith graph that Arthur sent over). So Arthur has up to m proofs to check against, giving him m opportunities to reject, whereas before he may have only had just one. This lowers the probability of a wrong decision in GRAPH-NON-ISO from $\frac{1}{2}$ to $\frac{1}{2^m}$.

37

a

1

Since the assignment of $x = 1, y = 0/1, z = 1$ will satisfy this boolean formula, Merlin will send true answers for each function and integer. In the first step, Merlin will send the function $s(x)$ which is derived from an integer S which is 1 iff the Boolean Formula $\exists x \forall y \exists z (x \vee y \vee \overline{z}) \wedge (\overline{x} \vee \overline{y} \vee z)$ is true.

$$\begin{aligned} y \vee \overline{z} &\to (1-y)(1-(1-z)) = 1 - z(1-y) \\ x \vee y \vee \overline{z} &\to 1-(1-x)(1-(1-z(1-y))) = 1-(1-x)(1-y)z \\ \overline{y} \vee z &\to 1-(1-(1-y))(1-z) = 1-y(1-z) \\ \overline{x} \vee \overline{y} \vee z &\to 1-(1-(1-x))(1-(1-y(1-z))) = 1-xy(1-z) \end{aligned}$$

Using this, and changing $\exists \to \Sigma$, $\forall \to \Pi$, then S is:

$$S(x) = \Sigma^1_{x=0}\Pi^1_{y=0}\Sigma^1_{z=0}(1-(1-x)(1-y)z)(1-xy(1-z)) = 1$$

$S = 1$ since Merlin knows the formula is satisfiable. Merlin will send

$$s(x) = \Pi^1_{y=0}\Sigma^1_{z=0}(1-(1-x)(1-y)z)(1-xy(1-z))$$

Additionally Merlin will return the integer 1 since he knows there is a true answer.

2

$$s(x) = \Sigma^1_{z=0}(1-(1-x)(1-y)z)(1-xy(1-z))$$

3

Arthur will check that $s''(1/3) = s'(0) * s'(1)$.

b

1

Merlin will construct a linearized function $s(x)$ as follows:

$$\begin{aligned}
s(x) &= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}(1-(1-x)(1-y)z)(1-xy(1-z)) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - z(1-x)(1-y) - xy(1-z) + xyz(1-x)(1-y)(1-z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - (z-xz)(1-y) - xy + xyz + (xyz-xyz)(1-y)(1-z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - (z-xz)(1-y) - xy + xyz + (0)(1-y)(1-z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - (z-xz)(1-y) - xy + xyz \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - (z-xz) - y(z-zx) - xy + xyz \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - z + xz - yz + xyz - xy + xyz \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}1 - z + xz - yz - xy + 2xyz
\end{aligned}$$

2

3