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

i

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.

Alternative idea for 37.a.1:
Merlin will construct a function $s(x)$ as follows:

$$
\begin{aligned}
s(x) &= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}(x+y+(1-z)) * ((1-x)+(1-y)+z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}x(1-x)+y(1-x)+(1-z)(1-x)+x(1-y)+y(1-y)+(1-z)(1-y)+xz+yz+z(1-z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}x-x^2+y-xy+1-z-x+xz+x-xy+y-y^2+1-y-z+zy+xz+yz+z-z^2 \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}x-x+x-x^2+y-y+y-xy-xy-z-z+z+xz+xz-y^2+2zy-z^2+1+1 \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}x-x^2+y-2xy-z+2xz-y^2+2zy-z^2+2 \\
&= \Pi_{y=0}^{1}(x-x^2+y-2xy-(0)+2x(0)-y^2+2(0)y-(0)^2+2)+(x-x^2+y-2xy-(1)+2x(1)-y^2+2(1)y-(1)^2+2) \\
&= \Pi_{y=0}^{1}(x-x^2+y-2xy-y^2+2)+(x-x^2+y-2xy-1+2x-y^2+2y-1+2) \\
&= \Pi_{y=0}^{1}3x-2x^2+4y-4xy-2y^2+2 \\
&= (3x-2x^2+4(0)-4x(0)-2(0)^2+2) * (3x-2x^2+4(1)-4x(1)-2(1)^2+2) \\
&= (-2x^2+3x+2) * (-2x^2-x+4) \\
&= (-2x^2+3x+2) * (-2x^2-x+4) \\
&= 4x^4-4x^3-15x^2+10x+8
\end{aligned}
$$

$$
\begin{aligned}
S &= s(0)+s(1) \\
&= (4(0)^4-4(0)^3-15(0)^2+10(0)+8)+(4(1)^4-4(1)^3-15(1)^2+10(1)+8) \\
&= 8+4-4-15+10+8 \\
&= 11
\end{aligned}
$$

ii

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

iii

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

b

i

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

$$
\begin{aligned}
s(x) &= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}(x+y+(1-z)) * ((1-x)+(1-y)+z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}x(1-x)+y(1-x)+(1-z)(1-x)+x(1-y)+y(1-y)+(1-z)(1-y)+xz+yz+z(1-z) \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}x-x+y-xy+1-z-x+xz+x-xy+y-y+1-y-z+yz+xz+yz+z-z \\
&= \Pi_{y=0}^{1}\Sigma_{z=0}^{1}2xz-2xy+2-2z+2yz \\
&= \Pi_{y=0}^{1}(2x(0)-2xy+2-2(0)+2y(0))+(2x(1)-2xy+2-2(1)+2y(1)) \\
&= \Pi_{y=0}^{1}-2xy+2+2x-2xy+2y \\
&= \Pi_{y=0}^{1}-4xy+2+2x+2y \\
&= (-4x(0)+2+2x+2(0)) * (-4x(1)+2+2x+2(1)) \\
&= (2+2x) * (-2x+4) \\
&= -4x+4x+8 \\
&= 8
\end{aligned}
$$

$$
\begin{aligned}
S &= s(0) + s(1) \\
&= 8 + 8 \\
&= 16
\end{aligned}
$$

ii

After receiving $r = 1/3$, Merlin will construct a linearized function $g(y)$ as follows:

$$
\begin{aligned}
g(y) &= \Sigma_{z=0}^{1}((1/3) + y + (1 - z)) * ((1 - (1/3)) + (1 - y) + z) \\
&= \Sigma_{z=0}^{1} - y + 2yz + y/3 - z - z/3 + 20/9 \\
&= \Sigma_{z=0}^{1} - 2y/3 + 2yz - 4z/3 + 20/9 \\
&= (-2y/3 + 2y(0) - 4(0)/3 + 20/9) + (-2y/3 + 2y(1) - 4(1)/3 + 20/9) \\
&= (-2y/3 + 20/9) + (-2y/3 + 2y - 4/3 + 20/9) \\
&= (2y)/3 + 28/9
\end{aligned}
$$

iii