Homework 22

Austin Frownfelter Matthew Bialecki

March 16, 2018

1 Problem 36

Show that MAM is a subset of AM.

Consider an MAM protocol. The soundness error for this protocol is $\leq \frac{1}{3}$. Merlin sends a message, π, to Arthur, who then flips a coin to decide whether x $\in$ L. The probability Arthur accepts if x $\notin$ L is $\leq \frac{1}{3}$. By using the known error reduction technique, Arthur can flip $m+1$ coins and decide if any of them would make him reject. The probability Merlin fools Arthur is $\leq \frac{1}{3^{m+1}}$.

Consider switching the protocol such that Arthur sends his random coin flips to Merlin before Merlin sends his message. Merlin can choose up to m different messages to send. For any given π Merlin chooses, the probability it will fool Arthur is $\leq \frac{1}{3^{m+1}}$. By using the union bound, the probability Merlin can choose a π which fools Arthur for all of his coin flips is $\leq \frac{1}{3}$. Therefore, this new AMM protocol is still sound.

Since an AMM protocol is equivalent to an AM protocol where both M messages are sent at once, this MAM protocol can be converted into an AM protocol. Therefore, MAM $\subseteq$ AM.

2 Problem 37

2.1 Part a

First consider the protocol without linearization.

2.1.1 i

What is the integer S and polynomial s(x) that Merlin sends in the first round?

S = 2.

$s(x) = \Pi_{y=0}^{1} \Sigma_{z=0}^{1} P(x, y, z)$

$= \Sigma_{z=0}^{1} P(x, 0, z) * P(x, 1, z)$

$= P(x,0,0) * P(x,1,0) + P(x,0,1) * P(x,1,1)$

$= ((1-(1-x)*1*0)*(1-x*0*1))*((1-(1-x)*0*0)*(1-(1-x)*1*1)) + ((1-(1-x)*1*1)*(1-x*0*0))*((1-(1-x)*0*1)*(1-(1-x)*1*0))$

$= (1*1)*(1*(1-(1-x))) + ((1-(1-x))*1)*(1*1)$

$= (1)*(x) + (x)*1$

$= 2x$

2.1.2 ii

What is the polynomial that Merlin sends in his second message to Arthur?

$s(r) = \Pi_{y=0}^{1}\Sigma_{z=0}^{1} P(r,y,z)$

$q(y) = \Sigma_{z=0}^{1} P(r,y,z)$

$= P(r,y,0) + P(r,y,1)$

$= (1-(1-r)*(1-y)*0)*(1-r*y*1) + (1-(1-r)*(1-y)*1)*(1-r*y*0)$

$= (1)*(1-r*y) + (1-(1-r)*(1-y))*(1)$

$= (1-r*y) + (1-(1-r)*(1-y))$

$= (1-\frac{1}{3}*y) + (1-(1-\frac{1}{3})*(1-y))$

$= 1-\frac{1}{3}*y + (1-\frac{2}{3}*(1-y))$

$= 1-\frac{1}{3}*y + (1-\frac{2}{3}+\frac{2}{3}y)$

$= \frac{1}{3}y + \frac{4}{3}$

2.1.3 iii

Arthur checks this second polynomial to see if it has some property, what property is this?

Whether $q(0) * q(1) = s(r)$ (if not, reject; otherwise continue)

2.2 Part b

Now consider the protocol with linearization.

2.2.1 i

What is the integer S and polynomial s(x) that Merlin sends in the first round?

S = 2.

$s(x) = \Pi_{y=0}^{1} \Sigma_{z=0}^{1} P(x, y, z)$

$= \Sigma_{z=0}^{1} P(x, 0, z) * P(x, 1, z)$

$= P(x, 0, 0) * P(x, 1, 0) + P(x, 0, 1) * P(x, 1, 1)$

$= ((1-(1-x)*1*0)*(1-x*0*1))*((1-(1-x)*0*0)*(1-(1-x)*1*1))+ ((1-(1-x)*1*1)*(1-x*0*0))*((1-(1-x)*0*1)*(1-(1-x)*1*0))$

$= (1*1)*(1*(1-(1-x))) + ((1-(1-x))*1)*(1*1)$

$= (1)*(x) + (x)*1$

$= 2x$

$= x$

2.2.2 ii

What is the polynomial that Merlin sends in his second message to Arthur?

$s(r) = \Pi_{y=0}^{1} \Sigma_{z=0}^{1} P(r, y, z)$

$q(y) = \Sigma_{z=0}^{1} P(r, y, z)$

$= P(r, y, 0) + P(r, y, 1)$

$= (1-(1-r)*(1-y)*0)*(1-r*y*1)+(1-(1-r)*(1-y)*1)*(1-r*y*0)$

$= (1)*(1-r*y) + (1-(1-r)*(1-y))*(1)$

$= (1-r*y) + (1-(1-r)*(1-y))$

$= (1-\frac{1}{3}*y) + (1-(1-\frac{1}{3})*(1-y))$

$= 1-y+(1-(1-y))$

$= 1-y+y$

$= 1$

2.2.3 iii

Arthur checks this second polynomial to see if it has some property, what property is this?

Whether $q(0) * q(1) = s(r)$ (if not, reject; otherwise continue)