Sönnun án upplýsinga

Þórður Ágústsson

11. apríl 2021

1 Gagnvirk Sönnun án upplýsinga

Umfjöllunin í eftirfarandi kafla byggir á köflum 2-4 í lokaritgerð eftir Nihal R. Gowravaram sjá [?].

Sönnun án upplýsinga, skammstafað ZKP fyrir *Zero-Knowledge Proof*, er gagnvirk sönnun sem sannar fyrir sannprófara, $\mathcal{V}$, að sannari, $\mathcal{P}$, veit lausn við ákveðnu vandamáli án þess að gefa upp neinar upplýsingar um lausnina. Sönnun án upplýsinga gefur því hvorki upp sjálfa lausnina á vandamálinu né neinar upplýsingar sem gætu hjálpað öðrum að finna þessa ákveðnu lausn. Það eina sem sönnunin sýnir er að sannarinn viti rétta lausn.

Skilgreining 1.1. *Sönnun án upplýsinga* er gagnvirk sönnun sem hefur eftirfarandi eiginleika:

1. *Upplýsingaleysi* (*e. zero-knowledge*). Ef staðhæfingin er sönn mun enginn sannprófari læra neitt annað af sönnuninni heldur en að staðhæfingin er sönn.

Samskiptareglan sem Ari og Embla nota í inngangínum er gagnvirk sönnun án upplýsinga. Til að sýna það þurfum við leið til að tákna ferlið sem Ari og Embla ganga í gegnum þegar þau keyra samskiptaregluna. Við köllum samskipti Ara og Emblu fyrir eina keyrslu í gegnum samskiptaregluna *handrit* sönnunarinnar.

Skilgreining 1.2. Við köllum raðaðan lista af tölum/spurningum sem sendar eru á milli sannprófara $\mathcal{V}$ og sannara $\mathcal{P}$ í ákveðinni samskiptareglu fyrir inntakið x, *handrit* þessarar samskiptareglu fyrir inntakið x. Við táknum með $\text{View}_V(\mathcal{P}(x), \mathcal{V}(x))$ dreifinguna yfir möguleg handrit sem verða til við samskipti $\mathcal{P}$ og $\mathcal{V}$ á inntaki x fyrir ákveðna samskiptareglu ($\mathcal{P}$,$\mathcal{V}$).

Athugum að $\text{View}_{\mathcal{V}}$ táknar handrita-dreifinguna eins og hún er séð frá $\mathcal{V}$.

Í dæmisögunni í inngangínum gæti eitt handrit litið svona út:

$$\text{View}_{\text{Ari}}(\text{Embla}(x),\ \text{Ari}(x)) = [\mathcal{V}_{1_1}, \mathcal{P}_{1_1}, \mathcal{V}_{1_2}]$$

Þar sem inntakið er x ="Boltarnir eru mismunandi á litinn" og keyrslan í gegnum samskiptaregluna (hvernig Ari og Embla haga sér) $\mathcal{V}_1$ ="Sami bolti og í síðustu umferð", og $\mathcal{P}_1$ ="Já, þetta er sami bolti" og $\mathcal{V}_{1_2} = 1$, þ.e. Ari samþykkir staðhæfingu Emblu. Við sjáum að handritið lýsir nákvæmlega þeim ákvarðanatökum sem hafa áhrif á útkomuna í samskiptareglunni:

1. Ari sýnir Emblu sama bolta og í síðustu umferð => $\mathcal{V}_1$
2. Embla (sem er sannsögull sannari) svarar að þetta sé sami bolti og síðast => $\mathcal{P}_1$
3. Ari samþykkir svar Emblu og samþykkir því að boltarnir eru mismunandi og Embla veit muninn => $\mathcal{V}_{1_2} = 1$

Þessi skilgreining á handriti leyfir okkur að styrkja hvað við eigum við með að sönnun sé "án upplýsinga" í skilgreiningunni (1.1).

Skilgreining 1.3. Við segjum að gagnvirk sönnun, $(\mathcal{P}, \mathcal{V})$, sé sönnun án upplýsinga ef fyrir sérhvert margliðu-tíma sannprófara-algrím V' þá er til líkindafræðilegt margliðu-tíma algrím H' (kallað hermir, e. simulator) þannig að fyrir sérhverja sanna staðhæfingu, x, gildir að eftirfarandi slembistærðir hafa sömu dreifingu:

1. Dreifing handrita $\text{View}_{V'}(\mathcal{P}(x), \mathcal{V}'(x))$,
2. $H'(x)$.

Þessi skilgreining getur verið þung þegar hún er lesin fyrst. Sérstaklega því í flestum dæmum, og öllum sem við skoðum, er fullkomleika-villan = 0 og því er dreifingin fyrir $(\mathcal{P}, \mathcal{V}, x, r) \in \{0, 1\}$ þegar sannarinn er sannsögull $P((\mathcal{P}, \mathcal{V}, x, r) = 1) = 1$. En skilgreiningin tekur með dæmin þar sem $P((\mathcal{P}, \mathcal{V}, x, r) = 1) < 1$, og þau dæmi þar sem sannprófarinn þarf ekki að vera sannsögull.

Þar sem skilgreiningin kynnir til sögunnar algrím sem við köllum *Herma*, sem eru mikilvægir í umræðunni sem á eftir að koma, tökum við smá umræðu um þá.

1.1 Hermar

Þessi kafli er byggður á umfjöllun um herma í kafla 2.1 í ritgerð eftir Gerardo I. Simari, sjá [?].

Hermir er, eins og orðið gefur til kynna, aðferð/algrím sem býr til *handrit* af samskiptareglu án þess að hafa samskipti við sannarann (m.ö.o. þá hermir algrímið eftir raunverulegum samskiptum milli sannara og sannprófara).

Óformlega þýðir það að til sé hermir fyrir ákveðna samskiptareglu að $\mathcal{V}$ lærir ekkert frekar um lausn vandamálsins nema að $\mathcal{P}$ veit lausn á vandamálinu. Þetta getum við séð með því að athuga að ef $\mathcal{P}$ veit lausnina á vandamálinu þá ef $\mathcal{V}$ vill finna lausnina, og er alveg sama í raun hvort $\mathcal{P}$ veit lausnin eða ekki, græðir $\mathcal{V}$ ekkert á því að keyra samskiptaregluna við $\mathcal{P}$ því $\mathcal{V}$ gæti allt eins keyrt herminn og fengið jafnmikið af upplýsingum þaðan, því handritið frá herminum og handritið frá samskiptum við sannarann eru óaðgreinanleg.

Skilgreining 1.4. Fall, með staðhæfingu x sem inntak, sem býr til fölsk *handrit* (án samskipta við sannara) sem eru óaðgreinanleg (fallið hefur sömu dreifingu) frá handriti af gildri sönnun milli sannsöguls sannara og einhvers sannprófara köllum við *hermi*.

Skoðum skilgreininguna á hermi í samhengi við litblinda vininn í inngangínum. Er sú sönnun, sönnun án upplýsinga? Það virðist vera því augljóslega eru einu upplýsingarnar sem Ari hefur í lok sönnunarinnar að boltarnir eru mismunandi á litinn. Hann veit til dæmis ekki hvor þeirra er rauður og hvor er grænn sem gerði Emblu kleift að taka græna boltann og skilja Ara eftir með þann rauða án þess að Ari kæmist að því. En í sambandi við skilgreininguna, hvernig getum við notað hana til að sýna fram á að litblindi vinurinn er sönnun án upplýsinga? Við þurfum að sýna að við getum "hermt" eftir gildri sönnun án þess að hafa aðgang að Emblu, þ.e. aðgang að einhverjum sem veit muninn á boltunum. Skilgreinum herminn H' svona:

1. Ari velur annaðhvort $\mathcal{V}_{1_1}$ = "Ari setur fram sama bolta og í síðustu umferð" eða $\mathcal{V}_{1_1}$ = "Ari setur fram annan bolta frá því í síðustu umferð" og spyr "Er þetta sami bolti og ég sýndi þér í skrefi 2".
2. H' velur annaðhvort $\mathcal{P}_{1_1}$ ="Já, þetta er sami bolti" eða $\mathcal{P}_{1_1}$ ="Nei, þetta er ekki sami bolti" með jöfnum líkum.
3. Ef Ari samþykkir svar hermisins spýtir hermirinn út $[\mathcal{V}_{1_1}, \mathcal{P}_{1_1}, 1]$ fyrir gildin sem voru skilgreind í skrefum 1-2. Annars spólar hermirinn til baka aftur í skref 1.

Hér erum við að túlka 1 sem játun við spurningu Ara ”Er þetta sami bolti og ég sýndi þér í síðustu umferð” og 0 sem neitun við sömu spurningu. Athugum að hér höfum við því skilgreint fall sem hagar sér alveg eins og handrit Ara og Emblu án þess að fá upplýsingar frá Emblu, eingöngu með því að nota upplýsingar sem Ari hefur. Þetta fall mun alltaf sannfæra Ara um að fallið sjái mun á boltunum, eins og Embla gerir. Því er fallið gildur hermir.

Þessi hermir, H’, svipar til þess að Ari leikur samskiptaregluna við sjálfan sig. Þar sem handrit leiksins fer fram á sama veg og ef Ari léki leikinn við sannsöglan sannara þá samkvæmt skilgreiningunni er samskiptaregla mismunandi bolta samskiptaregla án upplýsinga (óformlega).

Við getum einnig litið á herminn sem upptöku af leiknum milli Emblu og Ara. Upptakan sjálf ætti ekki að sannfæra neinn litblindan einstakling sem horfir á hana að boltarnir séu mismunandi á litinn því Embla og Ari gætu hafa ákveðið fyrirfram spurningarnar sem Ari myndi spyrja Emblu og þannig reynt að plata þá sem horfa á upptökuna að boltarnir séu mismunandi á litinni. Hinsvegar þá er upptakan alveg eins og upptaka af samskiptareglunni milli þeirra ef þau eru ekki lygin. Því er upptakan hermir.

Með skilgreiningunni á hermum getum við einfaldað skilgreininguna á sönnun án upplýsinga, skilgr. 1.3

Skilgreining 1.5. *Sönnun án upplýsinga* er gagnvirk sönnun þar sem til er hermir.

Til umhugsunar: Ef sannprófari hefur undir höndunum Hermi, hvað fær hann útúr samskiptum við heiðarlegan sannara? Þessi spurning hljómar kannski óeðlilega en athugið að hermirinn getur búið til handrit af samskiptunum. Handrit sem er óaðgreinanlegt frá handriti sem verður til við raunveruleg samskipti við heiðarlegan sannara. Nú, ef í hvert skipti sem maður ætlar að tala við annan mann væri vél sem prentaði út handrit af samræðunum áður en þær ættu sér stað, hver væri tilgangurinn í að tala við manninn? Maður veit núþegar hvað hann mun segja. Þannig hvaða upplýsingar fær maður af því að tala við hann?

Þetta er hugsunin á bakvið skilgreininguna „án upplýsinga”. Það að til sé hermir þýðir að maður veit fyrirfram hvernig samræður við heiðarlegan sannara munu fara. Svo að einu upplýsingarnar sem þú færð á raunverulegum samskiptum eru hvort sannarinn hagar sér eins og handritið frá herminum spáir. Ef hann hagar sér ekki á þann veg þá hefurðu lært að hann er óheiðarlegur. En ekkert annað sem þú vissir ekki núþegar frá því að lesa handrit frá herminum.

1.2 Strjáll logri

Eftirfarandi umfjöllun er að miklu leiti byggð á kafla 1.2.3 og 2.2 úr ritgerð Nihal R. Gowravaram, sjá [?].

Nú skulum við taka fyrir dæmi um samskiptareglu sem er gagnvirk sönnun án upplýsinga.

Í dulritun er vandamálið með strjála lograng oft notað í hinum ýmsu samskiptareglum. Það vandamál er notað því lausn á vandamálinu er talið erfitt að finna en auðvelt að athuga hvort tilgreind lausn sé lausn.

Skilgreining 1.6. (Strjáll logri) Gerum ráð fyrir að p sé (stór) prímtala og látum g tákna spönnuð (e. generator) margföldunargrúpunnar sem inniheldur heiltölurnar modulo p (án 0 auðvitað). Strjáli lograinn af heiltölunni v með tilliti til g er það x sem uppfyllir:

$$g^x = v \pmod{p}$$

Nú, þegar maður veit ekki töluna x en veit v og g þá er það talið mjög erfitt vandamál að finna x. Svipað erfitt og að ítra sig í gegnum allar mögulegar heiltölur mod p. Við getum nýtt okkur það í samskiptareglu þar sem sannarinn veit lausn x á strjála logranum af v.

Samskiptaregla strjála lograns

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, reiknar $h = g^r \pmod{p}$ og sendir h til $\mathcal{V}$.
2. $\mathcal{V}$ velur $b \in \{0, 1\}$ af handahófi og sendir til baka á $\mathcal{P}$.
3. $\mathcal{P}$ reiknar $a = r + bx \pmod{p}$ og sendir á $\mathcal{V}$
4. $\mathcal{V}$ athugar hvort $g^a = hv^b \pmod{p}$, og ef þetta gildir þá samþykkir hann staðhæfingu $\mathcal{P}$ (amk fyrir þessa umferð) en hafnar annars (og lýkur þá reglunni með höfnun)
5. Ítra skref 1-4 þar til $\mathcal{V}$ er sannfærður eða hann hafnar.

Við getum enn á ný séð af þessari samskiptareglu, summu-athugun og reglunni fyrir litblinda vininn, að slembileiki er lykillinn á bakvið traustið sem gagnvirkar sannanir veita. Slembileikinn gerir $\mathcal{V}$ kleift að grípa óheiðarlegan

sannara í lygi. Í öllum þessum samskiptareglum er því mikilvægt að sannarinn viti ekki fyrirfram hvaða spurningar/tölur hann fær sendar frá sannprófaranum. Ef hann veit þær þá getur hann búið til strategíu og náð að blekkja sannprófarann. Við sjáum það í dæminu hjá Ara og Emblu, ef Embla veit alltaf hvort Ari skiptir um bolta eða ekki (t.d. ef hún er með myndavél undir borðinu) þá getur hún auðveldlega platað Ara til að halda að tveir eins boltar séu mismunandi.

Eins með strjála logrann. Ef $\mathcal{P}$ veit hvort $\mathcal{V}$ mun senda honum $b = 0$ eða $b = 1$ þá getur hann alltaf sannfært $\mathcal{V}$ um að hann veit lausnina x þótt hann veit hana ekki. Sjáum hvernig hann gerir það. Gerum ráð fyrir að sannarinn veit hvort sannprófarinn muni, í skrefi 2, senda $b = 0$ eða $b = 1$. Strategían hans væri þá eftirfarandi. Gerum ráð fyrir að $\mathcal{P}$ veit ekki lausnina x á strjála logranum. Ef $\mathcal{P}$ veit fyrirfram, þ.e. áður en umferðin hefst, að $\mathcal{V}$ mun senda $b = 0$ þá getur hann hagað sér alveg eins og er útlistað í skrefum 1-4 í samskiptareglunni. Því þegar kemur í skrefi 4 að $\mathcal{V}$ athugar jöfnuna mun hann samþykkja svör $\mathcal{P}$ sem gild. Ef $\mathcal{P}$ veit að $b = 1$, í skrefi 2, þá getur $\mathcal{P}$ valið að senda $h = g^s v^{-1}$ fyrir eitthvað handahófskennt $0 \leq s < p$ í skrefi 1 og síðan sent $a = s$ í skrefi 3 því þá fær $\mathcal{V}$ að $hv^b = hv^1 = g^s v^{-1} v = g^s = g^a$ og samþykkir svar $\mathcal{P}$ og staðhæfinguna að hann veit lausnina x á strála logranum af v, þótt hann veit hana ekki.

Við sjáum því að sannprófarinn grunar ekkert ef sannarinn veit fyrirfram hvort sannprófarinn velur $b = 0$ eða $b = 1$. Því er mikilvægt að halda valinu á b földu fyrir $\mathcal{P}$ þar til hann er búinn að senda h-ið á $\mathcal{V}$ í skrefi 1.

Samskiptareglan virkar hinsvegar því sannarinn velur *fyrst* r og reiknar $h = g^r \pmod p$ og sendir til $\mathcal{V}$ áður en sannprófarinn sýnir val sitt á b. $\mathcal{P}$ er því búinn að festa val sitt og getur ekki breytt því án þess að $\mathcal{V}$ komist að því og þá væntanlega í framhaldi af því hafnað staðhæfingu $\mathcal{P}$ um að hann viti x.

Athugum nú hvort þessi samskiptaregla fullnægir skilyrðunum um Gagnvirka sönnun.

Fullkomleiki

Athugum að ef sannarinn er sannsögull þá veit hann gildið x þ.a. sannprófarinn mun reikna í 4. skrefi $g^a = g^{r+bx} = g^r g^{bx} = hv^b$ þ.a. fullkomleika-villan er 0. (þ.e. $P((\mathcal{P}, \mathcal{V}, x, b) = 1) = 1$)

Lögmæti

Lögmæti er aðeins flóknara að sanna heldur en fullkomleikann. Gerum ráð fyrir að $\mathcal{P}$ veit ekki gildið x sem hann segist vita. Nú getur tvennt gerst:

1. $\mathcal{V}$ sendir $b = 0$ í skrefi 2

Nú þar sem $b = 0$ þá vitum við að $\mathcal{V}$, í skrefi 4, mun athuga hvort $g^a = h \pmod p$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda gildi (h, a) sem uppfylla $g^a = h \pmod p$, sem er jafngilt því að senda lausnina a við strjála logranum af h. Því sjáum við að $\mathcal{P}$ þarf að vita lausn á strjála logranum af h til að sannfæra $\mathcal{V}$ í samskiptareglunni, ef $\mathcal{V}$ velur $b = 0$. Svo, ef $\mathcal{P}$ veit ekki lausnina á strjála logranum af h (þ.e. ef hann fylgir ekki samskiptareglunni) þá er það jafn-erfitt að finna a sem uppfyllir skrefi 4 og að leysa strjála logrann af v, þ.e. finna sjálft x-ið, lausnina á strjála logranum af v, sem hann veit ekki.

2. $\mathcal{V}$ sendir b = 1 í skrefi 2

Nú í skrefi 4 mun $\mathcal{V}$ athuga hvort $g^a = hv \pmod p$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda $(h, a) => g^a = hv \pmod p$ sem þýðir að $\mathcal{P}$ veit lausnina a á strjála logranum af hv. Athugum að hér getur óheiðarlegur $\mathcal{P}$ verið sniðugur og sent $(h, a) = (g^r v^{-1}, r)$, fyrir handahófskennt r. Ef hann gerir það þá í skrefi 4 mun $\mathcal{V}$ reikna $g^a = g^r = g^r v^{-1} v = hv$ og því trúa staðhæfingum $\mathcal{P}$. Hinsvegar ef hann reynir þetta, að vera sniðugur, þá mun hann ekki geta svarað rétt ef $\mathcal{V}$ velur $b = 0$ í skrefi 2.

Með þessar upplýsingar í höndunum getum við séð tvær mögulegar strategíur fyrir $\mathcal{P}$ sem veit ekki lausnina x við strjála logranum af v:

$\mathcal{P}$ fylgir skrefi 1 í samskiptareglunni

Nú getum við séð útfrá útlistuninni hér að ofan að ef $\mathcal{V}$ velur $b = 0$ í skrefi 2 þá er $\mathcal{P}$ í góðum málum og sendir bara það r sem hann valdi til baka (þ.e. $a = r$) og $\mathcal{V}$ mun auðvitað samþykkja það þar sem $\mathcal{P}$ fylgdi samskiptareglunni.

Hinsvegar ef $\mathcal{V}$ velur $b = 1$ þá vitum við að $\mathcal{V}$ mun athuga hvort $g^a = hv \pmod p$, í skrefi 4, sem krefst þess af $\mathcal{P}$ að senda til baka lausn a á stjrála logranum af hv. En þar sem $\mathcal{P}$ veit aðeins lausnina r fyrir strjála logrann af h en ekki fyrir v þá er jafn erfitt fyrir $\mathcal{P}$ að finna lausnina fyrir hv og það er fyrir hann að finna sjálft x. Og þar sem sú lausn er mjög erfið að finna þá er það besta sem $\mathcal{P}$ getur gert er að giska á lausn. Ef við gerum ráð fyrir því að p sé mjög stór tala þá gildir að fjöldi heiltalna $a < p$ þ.a. $g^a = hv \pmod p$ er fasti $c << p$. Við fáum því að líkurnar á að $\mathcal{P}$ nái að plata $\mathcal{V}$ eru:

$$P(b = 0) + P(b = 1)(g^a = hv \pmod p) = \frac{1}{2} + \frac{1}{2} \cdot (\frac{c}{p}) \approx 0.5$$

$\mathcal{P}$ fylgir ekki skrefi 1 og sendir h til $\mathcal{V}$ sem hann veit ekki strjála logrann af

Í þessu tilviki er $\mathcal{P}$ aðeins í vondum málum ef $\mathcal{V}$ velur $b = 0$ í skrefi 2, því ef $b = 0$ þarf $\mathcal{P}$ að senda til baka lausnina r á strjála logranum af h sem hann veit ekki. Því getur hann aðeins giskað og eins og í tilvikinu hér að ofan eru líkurnar á að hann giski á $a = r$ sem $\mathcal{V}$ mun samþykkja $\frac{c}{p}$ þar sem $c << p$.

Hinsvegar ef $\mathcal{V}$ velur $b = 1$ þá getur $\mathcal{P}$ notfært sér að hann veit lykilinn v. $\mathcal{P}$ getur í lotu 1 sent $h = g^s v^{-1} \pmod p$ á $\mathcal{V}$, fyrir einhverja tölu $0 \leq s < p$. Athugum að þá ef $\mathcal{V}$ velur b=1 getur $\mathcal{P}$ sent tilbaka $a = s$ og þá í skrefi 4 prófar $\mathcal{V}$:

$$g^a = g^s = g^s(v^{-1}v) = (g^s v^{-1})v = hv(\bmod p)$$

Og samþykkir það svar og dregur þá ályktun að $\mathcal{P}$ hlýtur að vita lausnina x. Athugum að ef $\mathcal{P}$ notar þessa strategíu þá eru líkurnar á að hann nái að plata $\mathcal{V}$ í einni umferð þær sömu og í fyrra tilvikinu:

$$\frac{1}{2} + \frac{1}{2}\frac{c}{p} \approx \frac{1}{2}$$

Lögmætisvillan er því $\delta_\ell \approx 1/2$.

Samskiptareglan er því gagnvirk sönnun með fullkomleikavillu 0 og lögmætisvillu 1/2. □

Við sjáum enn og aftur að sannanir án upplýsinga grundvallast í þessum lotubundnu samskiptum milli $\mathcal{P}$ og $\mathcal{V}$ þar sem í hverri lotu gefur sannprófarinn sannaranum tækifæri til að sanna að hann raunverulega veit þessar ákveðnu upplýsingar (t.d. gildið x í strjála logranum, litirnir á boltunum í litblinda vininum) með því að leggja fyrir hann áskorun/spurningu sem aðeins sá sem veit upplýsingarnar á að geta svarað rétt í hverri lotu, hversu margar sem þær eru.

Við sjáum í strjála logranum að reglan er hönnuð á þann veg að ef $\mathcal{P}$ er lyginn einstaklingur þá mun hann, ef hann er sniðugur, aðeins geta leyst aðra áskorunina sem $\mathcal{V}$ sendir á hann í sérhverri umferð. Ef $\mathcal{V}$ velur $b = 0$, þá er það jafngilt því að $\mathcal{V}$ biður $\mathcal{P}$ að leysa strjála logrann fyrir h-ið sem $\mathcal{P}$ sendir í skrefi 1. Sú spurning/áskorun veldur því að $\mathcal{P}$ getur ekki svindlað á því hvernig hann velur h-ið, án þess að eiga á hættu að $\mathcal{V}$ biðji um staðfestingu á að h-ið sé valið á réttan máta og þannig nappað $\mathcal{P}$ í lygi. Eins ef $b = 1$, þá er það jafngilt því að $\mathcal{V}$ biður $\mathcal{P}$ að leysa strjála logrann af v (þ.e. að $\mathcal{P}$ veit lausnina x), án þess að gefa upp sjálfa lausnina.

Við sjáum að bæði þessi tilviki, $b = 0$ og $b = 1$, eru mikilvæg í samskiptareglunni og ennfremur að það er mikilvægt að $\mathcal{P}$ viti ekki hvort gildið verður valið

þegar hann reiknar h-ið. Því ef hann veit hvora áskorunina $\mathcal{V}$ mun senda á hann þá mun hann alltaf geta svindlað og sannfært $\mathcal{V}$ að hann veit lausnina x þótt hann veit hana ekki.

Slembileiki samskiptareglunnar er því grundvallaratriðið sem gerir hana að sönnun. Athugum ennfremur að ekki er nauðsynlegt að b sé slembibreyta í augum $\mathcal{V}$, heldur eingöngu að $\mathcal{P}$ sjái breytuna sem slembibreytu.

Án upplýsinga

Hérna flækjast málin. Til að sýna fram á að samskiptareglan er *án upplýsinga* þurfum við að smíða hermi sem hermir eftir samskiptum við raun-sannara.

Látum V' vera eitthvert sannprófara-algrím, sem er ekki endilega sannsögult, með innri slembileika r. Við ætlum að útbúa hermi H' þ.a. fyrir sérhverja staðhæfingu x gildir að eftirfarandi slembibreytur hafa sömu dreifingu.

1. $\text{View}_V(\mathcal{P}(x), \mathcal{V}(x))$
2. $H'(x)$

Látum herminn virka á eftirfarandi máta:

1. Velur $b \in \{0, 1\}$ og $0 \leq r < p$ af handahófi.
2. Sendir $h = g^r v^{-b}$ á V'
3. Lætur $b' \in \{0, 1\}$ vera svar V' við h-inu í skrefi 2. Ef $b' \neq b$ spólar hermirinn aftur í skref 1.
4. $b = b'$. Sendir $a = r$ á V'.
5. Lætur úttakið vera úttak V' við $a = r$, þ.e. 0 ef V' hafnar en 1 ef V' samþykkir.

Athugum eftirfarandi:

1. Dreifing h valin af H' og h valin af sannsöglum $\mathcal{P}$ er sú sama.
2. $P[b' = b] \geq 0.5$
3. Skilyrt að $b = b'$ og gildinu h sem H' reiknar í skrefi 2 þá er gildið á a-inu sem H' sendir í skrefi 4 það "sama" og gildið sem $\mathcal{P}$ sendir þegar $\mathcal{P}$ sendir fyrst h og fær svarið b' frá V'.

1)

Athugum að h-ið er, bæði hjá $\mathcal{P}$ og herminum, handhófskennt veldi t af spönnuðinum, þ.e. g^t. Hjá herminum er $h = g^r v^{-b} = g^{r-bx}$ en athugum að $-bx$ er annaðhvort 0 eða $-x$, og hvort sem er þá er $r - bx$ handahófskennd tala (alltaf þegar við tölum um handhófskennt hér eigum við við handhófskennt með jafndreifingu (e. uniformly random) og því með sömu dreifingu og r-ið valið af heiðarlegum $\mathcal{P}$ sem veldur því að h-in hafa sömu handhófskenndu dreifinguna.

2)

Athugum að þar sem h-in hafa sömu dreifingu þá fær V' engar upplýsingar um hvernig h-ið var valið og því eru 50% líkur á að b-ið sem Hermirinn velur í skrefi 1 sé eins og b', þ.e. $P[b' = b] = 0.5$.

3)

Athugum að a-ið sem $\mathcal{P}$ velur í samskiptareglunni er strjáli logrinn af h-inu ef $b = 0$ og strjáli logrinn af hv ef $b = 1$. Eins er

$$g^r = hv^{b'}$$

og $a = r'$ í Herminum. Þ.a. a-ið í Herminum er strjáli logrinn af h þegar $b' = 0$ en strjáli logrinn af hv þegar $b' = 1$. Þar sem sami logrinn er reiknaður þegar $b' = b$ fáum við að gildið a er það "sama" bæði fyrir Herminn og $\mathcal{P}$. Hér meinum við með því "sama" að a er lausn á "sama" vandamáli, annaðhvort lausn á strjála logranum af h eða af hv. Þar sem ekki er öruggt að h-in séu þau sömu, bara að þau hafi sömu dreifingu, en athugum að ef h-in eru þau sömu þá verða a-in þau sömu bæði hjá Herminum og $\mathcal{P}$.

Með 1-3) sjáum við að skv. 1) er dreifing h sú sama fyrir H' og $\mathcal{P}$. 2-3) gefa síðan, skilyrt með gildinu á h, að b-bitinn er sá sami bæði hjá H' og $\mathcal{P}$ og því sama a-ið (ef þeir gáfu sama h-ið).

Við höfum því að útkoman, og handritið, mun vera sú sama fyrir bæði H' og samskiptin milli $\mathcal{V}$ og heiðarlegs $\mathcal{P}$. Ennfremur mun dreifingin á handritunum vera sú sama. Hermirinn okkar er því gildur-hermir sem keyrir í slembi-margliðutíma (því þar sem líkurnar á að $b =' b$ eru 0.5 mun hermirinn á endanum komast í loka skrefið og hætta keyrslu, í margliðutíma) og skilar handriti sem er óaðgreinanlegt frá raunverulegum samskiptum milli heiðarlegs $\mathcal{P}$ og $\mathcal{V}$.

Strjáli Logrinn - samskiptareglan er því *Gagnvirk sönnun án upplýsinga.*

Þessi samskiptaregla, annað en summu-athugun, hefur bein tengsl við raun-

heima að því leyti að hægt er að útfæra hana og nota sem lausn á ýmsum mögulegum vandamálum. Helsta, og augljóstasta, leiðin til að nota þessa samskiptareglu er í auðkenningu. Til dæmis getur maður notað hana til að útbúa vegabréfskerfi þar sem eigandi vegabréfsins þarf aldrei að sýna vegabréfið sitt (hvorki dulkóðað né sem hreinan texta) til að sanna að hann sé sá sem hann segist vera.

Strjáli logrinn er sérstakt dæmi af Σ-samskiptareglu. (sjá kafla 5.1.2 í [**?**] eða kafla 11 í [**?**])

1.3 Þrílitað net

Umfjöllun þessa kafla er byggð á kafla 4.2 úr ritgerð Nihal R. Gowravaram (sjá [**?**]) og kafla 3 í ritgerð Gerardo I. Simari (sjá [**?**]).

Þrílitun nets er vandamál í netafræði. Gefið er net $G = (V, E)$ og vandamálið snýst um hvort hægt er að lita sérhvern hnút v með einum lit af þremur, setjum $c \in \{\text{rauður, grænn, blár}\}$, þannig að enginn leggur (e. edge) e tengir tvo hnúta af sama lit.

Þetta vandamál er eitt af mörgum vandamálum í flokknum NP-fullkomið (e. NP-Complete), sem er flokkur vandamála sem hægt er að sannprófa í margliðutíma en ekki leysa í margliðutíma (þ.e. tekur meiri tíma eða slembi-margliðutíma). Erfitt er að finna lausn á stórum netum en ef manni er gefin þrílitun á tilteknu neti G þá getur maður athugað alla hnúta sem eru tengdir og í versta falli tekur það $\binom{|V|}{2} \approx |V|^2$.

Gerum ráð fyrir að Agnes vilji sannfæra Emil um að hún veit um þrílitun, $\{\text{rauður, grænn, blár}\}$, á tilteknu neti $G = (V, E)$.

Samskiptaregla fyrir þrílitun nets

Sérhver lota samskiptareglunnar fer á eftirfarandi veg:

1. Agnes umraðar litunum $\{\text{rauður, grænn, blár}\}$ og litar netið G, með nýju röðinni af litunum.

2. Agnes felur litunina (t.d. með því að líma límmiða yfir sérhvern hnút, eða með einhverskonar dulritun ef þau eiga í samskiptum yfir netið) og sýnir Emil netið.

3. Emil velur legg e af handahófi (og sendir til Agnesar)

4. Agnes fjarlægir límmiðana af hnútunum sem leggurinn tengir og sýnir Emil.

5. Emil athugar hvort hnútarnir eru mismunandi litaðir, samþykkir ef þeir eru það en hafnar annars.

Sýnum nú (óformlega) að þessi samskiptaregla er gagnvirk sönnun:

fullkomleiki

Nú ef Agnes veit þrílitun á grafinu þá mun hún augljóslega í hverri lotu sannfæra Emil, gefið að hún vilji það. Því nýja þrílitunin er eingöngu umröðun á þeirri gömlu og því gild þrílitun. Fullkomleika-villan er því 0.

Lögmæti

Gerum nú ráð fyrir að Agnes sé lygin og veit ekki um þrílitun á neti G og reynir því að plata Emil. Hún fylgir skrefi 1 en þrílitunin er alls ekki þrílitun á netinu (því Agnes veit ekki um þrílitun á netinu). Það þýðir að minnsta kosti að einn leggur $e \in E$ tengir hnúta sem eru eins litaðir. Líkurnar að hún nái ekki að plata Emil eru þá að minnsta kosti $\frac{1}{|E|} > 0$, Emil getur valið akkúrat þann legg sem tengir eins liti. Við höfum því að lögmætis-villan er í mesta lagi $1 - \frac{1}{|E|} < 1$ fyrir hverja lotu.

Við sjáum að hér er alls-ekki nóg að leika aðeins 1 lotu til að sannfæra sannprófara, Emil, með þessari samskiptareglu. Athugum að $(1-\frac{1}{n})^n \to e^{-1} \approx 0.37$ þegar n stefnir á óendanlegt. Svo, ef við leikum $|E|$ lotur þá stefna líkurnar á að Agnes nái að plata Emil á 37% sem er tiltölulega hátt. Athugum hinsvegar að $(1 - \frac{1}{n})^{kn} < \frac{1}{2^k}$ svo ef við veljum $k = |E|$ fáum við að líkurnar á að Agnes nái að plata emil eftir k umferðir eru minni en $\frac{1}{2^k} = \frac{1}{2^{|E|}}$.

Hér sjáum við að þótt að lögmætis-villan er tiltölulega há (t.d. fyrir |E| = 100 er hún $1 - 1/100 = 0.99$, þ.e. 99% líkur á að óheiðarlegur sannari nái að plata sannprófara í einni lotu, þá er samskiptareglan samt sem áður gagnvirk sönnun. Það er bara nauðsynlegt að leika mun fleiri lotur í þeim tilvikum sem lögmætisvillan er svona há ($x^n \longrightarrow 0$ ef $|x| < 1$). (Athyglisvert er hinsvegar að til er samskiptaregla fyrir þrílitað net sem hefur lögmætisvillu 0.5, sem veldur að ekki þarf að leika jafnmargar lotur og í samskiptareglunni hér að ofan (sjá samskiptareglu „A zero-knowledge protocol for proving that a graph G is 3-colorable" í [**?**])).

Sýnum nú að samskiptareglan sé "án upplýsinga".

Án upplýsinga

Gerum ráð fyrir að við höfum sannprófara V'. Búum til hermi H' sem virkar svona:

1. Litum sérhvern hnút í netinu með einum lit úr {rauður, grænn, blár} af handahófi.
2. Felum litunina og sendum netið á V'. V' velur legg e.
3. Skoðum hnútana sem leggur e tengir, ef þeir eru einslitaðir förum aftur í skref 1.
4. (hnútarnir eru mislitaðir) Sýnum V' hnútana og látum úttakið vera niðurstöðu V' eftir að hafa séð hnútana, 1 ef V' samþykkir en 0 annars.

Athugum að handrit fyrir eitt inntak í Herminn hefur sömu dreifingu og handrit milli heiðarlegs $\mathcal{P}$ og einhvers $\mathcal{V}$ því litirnir á hnútunum sem hermirinn sýnir hafa sömu dreifingu og hnútarnir sem heiðarlegur $\mathcal{P}$ sýnir og því er úttakið frá herminum það sama og úr samskiptum $(\mathcal{P}, \mathcal{V})$. Því er samskiptareglan gagnvirk sönnun án upplýsinga.

1.4 Smá flækjufræði

Skilgreining 1.7. P er flokkur af ákvörðunar-vandamálum sem eru leysanleg með algrími sem keyrir í margliðutíma

Skilgreining 1.8. NP er flokkur af ákvörðunar-vandamálum sem eru leysanleg með brigðgengnu (non-deterministic) algrími sem keyrir í margliðutíma.

Brigðgengin algrím þýðir í einföldu máli að algrímið tekur ákvarðanir í hverju skrefi ekki eingöngu útfrá inntakinu. Það keyrir semsagt í slembirými og þegar við segjum að þesskonar algrím keyrir í margliðutíma er átt við að ef, fyrir ákveðið inntak, algrímið velur alltaf "rétta" aðgerð þegar það er keyrt þá finnur algrímið lausn í margliðutíma.

Dæmi 1.9. Ef vandamálið er að ákvarða hvort að tala N sé *ekki* prímtala þá framkvæmir algrímið þá aðgerð að athuga hvort til sé $n \leq \sqrt{N}$ þ.a. $N|n$, ef N er ekki prímtala þá finnur algrímið þá lausn í einu skrefi með því að gera "rétta" aðgerð þ.e. velja rétta tölu n þ.a. N | n.

Skilgreining 1.10. Við segjum að vandamál $x \in NP$ sé NP-fullkomið ef fyrir sérhvert vandamál $y \in NP$ er hægt að einfalda (e. reduce) lausnaraðferð þess vandamáls niður í að leysa x með margliðu-aukningu í tíma.

Skilgreiningin á NP-fullkomnun hér að ofan gefur til dæmis til kynna að ef til er algrím sem finnur lausn á vandamáli $x \in$ NP-fullkomið í margliðutíma þá hefur sérhvert vandamál $y \in NP$ lausn sem hægt er að finna í margliðutíma, þ.e. með því fyrst að einfalda (e. reduce) það niður í vandamál x og síðan leysa það vandamál.

Nú þar sem þrílitun nets er NP-fullkomið vandamál (sjá [**?**]) fáum við þá niðurstöðu að NP $\subseteq$ ZKP þ.e. öll vandamál í NP hafa sönnun án upplýsinga (ZKP).

Þessi niðurstaða hefur að minnsta kosti þær afleiðingar að til eru ógrynni vandamála sem eru talin erfið að leysa sem hægt er að nýta í samskiptareglur, gagnvirkar sannanir án upplýsinga og því miklir möguleikar á notagildi ZKP í raunheimum.