Sönnun án upplýsinga

Þórður Ágústsson

11. apríl 2021

Útdráttur

Þessi ritgerð fjallar um gagnvirkar sannanir með áherslu [1] á sannanir án upplýsinga. Gerð verður grein fyrir skilgreiningu á gagnvirkum sönnunum og upplýsandi dæmi skoðuð. Einnig sýnum við hvað gerir dæmin að gagnvirkum sönnunum að tilsjón skilgreiningar. Eiginleikinn „án upplýsinga" er síðan kynntur til leiks og formlegar skilgreiningar sem leiða til eiginleikans ræddar. Bæði verða skoðaðar samskiptareglan um strjála logran og þrílitun nets og sýnt afhverju þær eru „án upplýsinga". Að lokum verður farið yfir sannanir án gagnvirkni og leiða til að breyta gagnvirkum sönnunum í sönnunum án gagnvirkni. Hagnýtingar verða ræddar fyrir samskiptareglur þessarar ritgerðar í lok hvers kafla.

1 Inngangur

Sannanir eru margskonar. Þær hefðbundnu sem maður kynnist í stærðfræðinámi eru byggðar á samfelldri röksemdarfærslu. Staðhæfing A er gefin og sönnunin leiðir lesandann frá þekktum staðreyndum yfir í staðhæfingu A. Sönnunin er þá gild ef vegurinn sem hún stikar, milli þekktra staðhæfinga yfir í A, er þráðbeinn og holulaus. Þesskonar sannanir eru t.d. sannanir á Pýþagórasarreglunni, grundvallarreglu algebrunnar og margar fleiri.

Þær sannanir sem við munum skoða í þessari ritgerð eru ekki af þessu almenna tagi. Þær krefjast þess að við víkkum skilning okkar á orðinu "sönnun". Einfalt er að hugsa sér að "sönnun" þurfi ekki eingöngu að eiga við reglur í stærðfræði, heldur einnig getum við hugsað okkur að "sönnun" eigi t.d. við sönnun á að $\sqrt{2}$ sé rót margliðunnar $f(x) = x^2 - 2$ eða að rætur margliðunnar $f(x) = x^{10} + 3 * x^2 + x + 73$ séu þekktar. Þetta eru ekki reglur, sem þarf að sanna, á borð við pýþagórasarregluna, heldur fremur einhverskonar staðhæfingar um þekkingu sem krefjast öðruvísi útleiðinga til að sýna að þær séu "sannar".

Til samanburðar segir grundvallarregla algebrunnar að sérhver margliða af stigi d hefur d-rætur (í $\mathbb{C}$). Þetta er regla sem þarfnast almennrar röksemdarfærslu um réttmæti hennar. Staðhæfingin "$\sqrt{2}$ er rót margliðunnar $f(x) = x^2 - 2$" er hinsvegar ekki beint regla, heldur fremur staðhæfing um þekkta lausn á vandamáli.

Sannanir þessarar ritgerðar munu fjalla um þessar hinsegin tegundir af sönnunum, þ.e. sönnun á staðhæfingu um þekkingu. Þær eru tól sem hægt er að nota til að sanna þekkingu á lausn á vandamáli, í þeim skilningi að ef einhver veit svar við vandamáli og vill sanna að svarið sé lausn fyrir öðrum án þess að aðrir þurfi að verja tíma í að leysa vandamálið sjálfir þá getur hann það með eins miklum líkum og hann vill. (Betur verður farið í orðalagið "eins miklum líkum og hann vill" seinna í ritgerðinni)

Við munum sjá að þessar sannanir nota samskipti milli þess sem segist vita lausn á vandamálinu og þess sem hann vill sannfæra um lausnina, eða sannfæra að hann viti lausn án þess að gefa upp lausnina. Við munum einnig veita slembileika samskiptanna athygli, þar sem slembi-eiginleiki sannananna er það sem gerir þær trúverðugar.

Ein tegund af svona sönnunum, sem hefur fengið mikla athygli síðustu ár, er sönnun án upplýsinga. Þær eru mikilvægur undirflokkur sannana sem hafa hagnýtt gildi í raunheimum og mun umræða þessarar ritgerðar að mestu fjalla um þær.

Eftirfarandi er sögudæmi sem sýnir kjarna sannana án upplýsinga (og gagnvirkra sannana) og verður mikið notað seinna í ritgerðinni til að, vonandi, auka skilning lesanda á efninu.

Litblindi vinurinn.

Ari og Embla sitja við borð. Á borðinu liggja tveir boltar. Annar rauður en hinn grænn. Að öðru leyti eru boltarnir algjörlega eins. Ari tekur upp boltana og segir við Emblu

"Afhverju komstu með þessa bolta?"

"Ahh, ég hugsaði bara að þú vildir kannski bolta, en vissi ekki hvaða lit þú vildir svo ég tók þá báða svo þú gætir valið" svarar Embla. Ari hlær.

"Hvað, ertu að reyna stríða mér? Þessir boltar eru alveg eins?" Segir Ari og starir á boltana til skiptis.

”Ha? Nei? Þessi er rauður,” Embla lyftir öðrum boltanum upp ”og hinn er grænn... Ari, ertu nokkuð litblindur?”.

Ari er forviða. Hann trúir þessu ekki. Heldur enn að Embla sé að bulla í honum.

”Neeee, þú ert að ljúga. Hlýtur að vera.”

Nú er Embla tiltölulega vel að sér í gagnvirkum sönnunum og segir því við Ara

”Það væri bara kjánalegt að ljúga að einhverju svona. Ég skal sanna þetta fyrir þér.”

Hvernig sannar Embla fyrir Ara að boltarnir séu mismunandi á litinn?

Gagnvirk sönnun fyrir mismunandi bolta

1. Embla lætur Ara halda á báðum boltunum og segir honum að setja þá undir borð eða fyrir aftan bak þannig að Embla getur ekki séð þá.

2. Ari sýnir annan boltann með því að setja hann upp á borðið en heldur hinum földum fyrir Emblu. Eftir að Embla hefur séð boltann setur Ari hann aftur undir borðið.

3. Ari velur annan boltann til að sýna Emblu (hér getur hann valið sama bolta og hann sýndi í skrefi 2 eða hinn) og setur upp á borðið. Þegar Embla hefur séð boltann spyr Ari hana

   ”Er þetta sami bolti og ég sýndi þér í skrefi 2?”

   Embla, verandi *ekki* litblind, á auðvelt með að svara hvort boltinn sé sá sami eða ekki þar sem liturinn auðkennir boltana. Hún svarar því hvort hann skipti um bolta eða ekki.

4. Endurtökum skref 2 og 3 þar til Ari er orðinn sáttur með að boltarnir séu mismunandi, og þar sem það eina sem er mismunandi við þá er liturinn hlýtur Embla að vera segja satt.

”Jæja, þú virðist hafa haft rétt fyrir þér. Skil ekki hvernig ég gat efast um þig,” segir Ari.

”Þú ert heiðarleg. Uppáhalds Marvel-ofurhetjan mín er Hulk, svo ég þigg græna boltann.” Segir ari glaður í bragði, þótt hann hafi haft rangt fyrir sér, og heldur fram báðum boltunum svo Embla geti tekið til sín þann rauða.

”Ekki málið Ari minn. Ég held þá þeim rauða fyrir mig”, segir Embla áður en hún tekur græna boltann og stingur í töskuna sína.

2 Gagnvirkar Sannanir (e. Interactive Proofs)

Umfjöllun í þessum kafla er byggð á kafla 3 úr óútgefinni bók um sannanir eftir Justin thaler, sjá [5].

Eins og drepið var á í innganginum fjalla sannanir þessarar ritgerðar um sannanir á að gefin lausn á fyrirfram-skilgreindu vandamáli sé í raun og veru lausn.

Í enn þrengri skilningi, þá höfum við tvo einstaklinga A og B þar sem A heldur fram lausn x á vandamáli H og vill sannfæra B að x sé raunveruleg lausn á þessu vandamáli. Gagnvirk sönnun er þá samskiptaregla milli A og B sem gerir A kleift að sannfæra B um lausnina, ef hún er raunverulega lausn á vandamálinu.

Þetta fyrirfram skilgreinda vandamál getur verið af ýmsum toga. Það getur t.d. verið lausn x á strjála logranum $g^x = v \pmod p$ (sjá kafla 3.6), þrílitun á neti (kafli 3.3), rót margliðu eða ótal mörg fleiri vandamál.

Almennt eru gagnvirkar sannanir notaðar þegar tímafrekt er að reikna/finna lausnina sjálfur með beinum útreikningum og þær þá notaðar í staðinn til að staðfesta að gefin lausn sé raunveruleg lausn á vandamálinu. Til dæmis væri óþarfi að nota gagnvirka sönnun til að sanna að $x = \sqrt{2}$ sé rót á fallinu $f(x) = x^2 - 2$, því auðvelt er að sannfæra þann sem skilur veldisvísa að $x = \sqrt{2}$ er rót fallsins einungis með beinum reikningi $f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 2 - 2 = 0$, sem tekur stuttan tíma.

Skilgreining 2.1. *Gagnvirk sönnun* er samskiptaregla $(\mathcal{P}, \mathcal{V})$, þar sem $\mathcal{P}$ og $\mathcal{V}$ eru algrím þ.a. $\mathcal{V}$ keyrir í líkindafræðilegum margliðu-tíma (e. probabilistic polynomial time), sem fullnægir eftirfarandi eiginleikum með "miklum líkum":

1. *Fullkomleiki* (e. completeness), að sérhver sönn staðhæfing hefur sannfærandi sönnun um réttmæti hennar.

2. *Lögmæti* (e. soundness), ef *engin* ósönn staðhæfing hefur sannfærandi sönnun um réttmæti hennar.

Hefð er fyrir því að tákna samskiptaregluna, í skilgreiningu 2.1, með $(\mathcal{P}, \mathcal{V})$ og kalla aðilana sem nota regluna í samskiptum *sannari* (e. *prover*, $\mathcal{P}$) og *sannprófari* (e. *verifier*, $\mathcal{V}$).

Athugum að settar eru hömlur á hvers konar algrím sannprófarinn getur verið, hversu lengi það má í versta falli keyra á inntaki x áður en það stöðvar. Það þýðir að þegar $\mathcal{V}$ er keyrt í gagnvirkri sönnun á inntaki (staðhæfingu) x, þá

tekur það $\mathcal{V}$ í versta falli $O(|x|^k)$ margar aðgerðir áður en $\mathcal{V}$ stöðvast. Engar hömlur eru hinsvegar settar á keyrslutíma sannaranns. Við höfum því þá tiltölulega óeðlilegu staðreynd að ef sannarinn þarf að keyra/framkvæma útreikninga sem eru $O(2^n)$ fyrir inntak (staðhæfingu) af stærð n í samskiptareglunni til að sanna fyrir sannprófaranum staðhæfinguna þá er samskiptareglan samt sem áður *Gagnvirk sönnun*, ef við gerum ráð fyrir að sannprófarinn keyrir í versta falli í margliðu-tíma.

Þessi staðreynd skilgreiningarinnar virðist óeðlileg í augum þess sem ímyndar sér notagildi þesskonar sannana. Hvernig notagildi getur *Gagnvirk sönnun* haft ef sannarinn þarf að framkvæma $O(2^n)$ útreikninga, sem í flestum vandamálum eru svo ógurlega margir reikningar að engin tölva getur klárað þá á skikkanlegum tíma? Það eru gildar vangaveltur og svarið er einfalt, skilgreiningin hefur aðeins áhuga á tímanum sem samskiptaregla krefur sannprófarann um. Ef nota á samskiptaregluna í raunveruleikanum þá getur maður allt eins valið eina af þeim sönnunum sem krefur sannarann ekki um kripplandi marga útreikninga. Oft, í fræðunum, gerum við bara ráð fyrir að sannarinn hefur umráð yfir mun öflugri tölvum en sannprófarinn (og raunveruleikinn ef það þarf). En það er ekki alltaf nauðsynlegt.

Skilgreining 2.1 setur okkur því þær hömlur að sannprófarinn verður að geta keyrt útreikningana í samskiptareglunni "hratt".

Annar hlutur skilgreiningarinnar sem er óljós er hvernig við eigum að skilja frasann "með miklum líkum", en hann er nátengdur slembi-eiginleika sannananna. Við munum brátt átta okkur betur á mikilvægi slembileika í *Gagnvirkum sönnunum* en fyrst skulum við skoða hvaðan hann á upptök sín. Við höfum séð slembileikann að verki í dæmisögunni um litblinda vininn í inngangínum þar sem í hverri umferð hefur Ari val um hvorn boltann hann vill sýna Emblu. Athugum að það er algjörlega undir Ara komið í hvaða röð hann velur boltana. Val Ara, að minnsta kosti í augum Emblu, er slembibreyta. Við segjum "að minnsta kosti" því Ari getur haft vel-ákveðna strategíu á því hvernig hann velur boltana en strategían getur líka verið byggð á handahófskenndu vali með einhverja dreifingu (t.d. með því að kasta krónu). Við sjáum að í báðum tilvikum er valið á boltunum slembibreyta í augum Emblu. Við köllum það sem stjórnar vali Ara í hverri umferð *innri slembileika* hans.

Skilgreining 2.2. *Innri slembileiki* algríms $\mathcal{V}$ er slembibreyta (-vigur) með einhverja skilyrta dreifingu sem $\mathcal{V}$ skilgreinir.

Athugum að innri slembileikinn getur táknað slembibreytu skilgreinda af dreifingu sem sannarinn veit ekkert um. Hinsvegar má sannarinn alveg vita hver

dreifingin er á meðan hún er ekki löggeng (e. deterministic). Ef hann veit dreifinguna hefur það ekki áhrif á gildi sönnuninarinnar ef gert er ráð fyrir að sannprófarinn veit að sannarinn veit dreifinguna. Þá getur sannprófarinn einfaldlega ákveðið að leika fleiri lotur í samskiptareglunni, ef dreifingin er ekki jafndreifð, til að núlla út vitneskju sannarans á dreifingunni. Við munum skilja betur hvernig þetta virkar seinna.

Aftur að litblinda vininum. Gerum ráð fyrir að strategía Ara sé að velja bolta alltaf af handahófi. Þá getum við lýst valinu hans sem slembibreytu A með þekkta dreifingu $P[A = \text{"Sami bolti og Ari sýndi í síðustu umferð"}] = P[A = \text{"Ekki Sami bolti og Ari sýndi í síðustu umferð"}] = 0.5$. Nú, ef við skilyrðum A þannig að í fyrstu lotu er $A =$ "Sami bolti og Ari sýndi í síðustu umferð" þá er restin af umferðinni í samskiptareglunni orðin löggeng (e. deterministic) og við getum fundið út hver niðurstaða samskiptareglunnar verður.

Við lok sérhverrar lotu ákveður sannprófarinn, $\mathcal{V}$, hvort sannarinn, $\mathcal{P}$, svaraði spurningum þessarar lotu eins og sá sem er að segja satt eða hvort hann er að ljúga. $\mathcal{V}$ ákveður síðan annaðhvort að samþykkja staðhæfinguna, fyrir þessa lotu, eða hafna henni, hætta samskiptareglunni og slíta öllum vinaböndum við $\mathcal{P}$ sem er lúalegur ljúgari. Við köllum þessa ákvörðun *úttak* samskiptareglunnar.

Skilgreining 2.3. Látum $(\mathcal{P}, \mathcal{V})$ vera Gagnvirka sönnun. Látum x tákna inntak samskiptareglunnar (þ.e. staðhæfinguna, sem $\mathcal{P}$ heldur fram að sé lausn á fyrirframskilgreindu vandamáli) og látum r vera innri slembileika $\mathcal{V}$ og látum r_0 tákna tölu sem tekin er úr dreifingu r þegar samskipti $\mathcal{P}$ og $\mathcal{V}$ hefjast (r_0 er fasti ákvarðaður af dreifingu r). Við táknum þá með

$$(\mathcal{P}, \mathcal{V}, x, r_0) \in \{0, 1\}$$

niðurstöðu samskiptareglunnar og köllum *úttak* hennar.

Hefð er fyrir því að líta á $(\mathcal{P}, \mathcal{V}, x, r_0) = 0$ sem höfnun $\mathcal{V}$ á inntaki (staðhæfingu), x, eftir eina umferð af samskiptareglunni og eins á $(\mathcal{P}, \mathcal{V}, x, r_0) = 1$ sem samþykki $\mathcal{V}$ á staðhæfingu, x.

Nú förum við alveg að geta útskýrt nægjanlega hvernig ber að skilja "með miklum líkum" úr skilgreiningu 2.1.

Við sjáum að í hverri lotu í samskiptareglunni milli Ara og Emblu eru 50% líkur á því að óheiðarleg Embla (Embla sem heldur því fram að boltarnir séu mismunandi á litinn en þeir eru í raun alveg eins) nái að sannfæra Ara um að boltarnir séu mismunandi, þ.e. þegar Ari spyr hvort hann skipti um bolta eða

ekki þá veit Embla ekki svarið og því er það besta sem hún getur gert til að plata Ara að giska. Því eru helmingslíkur á að hún giski á rétt svar við spurningu Ara. Hinsvegar ef Embla er heiðarleg þá mun hún í hverri umferð, með líkunum 100%, geta svarað Ara rétt hvort hann skipti um bolta eða ekki. Þessar líkur kallast "lögmætis-villa" (50%), og "fullkomleika-villa" (0%, þ.e. líkurnar á að ná ekki að sannfæra sannprófara um sanna staðhæfingu), í þessari röð.

Skilgreining 2.4. *Gagnvirk sönnun* $(\mathcal{P}, \mathcal{V})$ er sögð hafa fullkomleika-villu (e. completeness-error) δ_f og lögmætis-villu (e. soundness-error) δ_ℓ ef eftirfarandi gildir:

1. *fullkomleiki*. Gerum ráð fyrir að sannari $\mathcal{P}$ sé heiðarlegur. Fyrir sérhvert inntak x og slembibreytu r gildir:

$$P[(\mathcal{P}, \mathcal{V}, x, r) = 1] \geq 1 - \delta_f$$

2. *Lögmæti*. Fyrir sérhvert inntak x, slembibreytu r og sérhverja löggengna (e. deterministic) sönnunar aðferð $\mathcal{P}'$ þá gildir ef sannarinn sendir *ósanna* staðhæfingu x til sannprófarans:

$$P[(\mathcal{P}', \mathcal{V}, x, r) = 1] \leq \delta_\ell$$

Við segjum að gagnvirk sönnun $(\mathcal{P}, \mathcal{V})$ sé *gild* ef $\delta_f, \delta_\ell \leq 1/2$.

Athugum að í skilgreiningunni hér að ofan er gildið $\delta_f, \delta_\ell \leq 1/2$ valið af handahófi. Ennfremur þá gæti lögmætisvillan allt eins verið 0.99 bara á meðan hún er <1 þá er sönnunin gild.

Skoðum þessa skilgreiningu í ljósi samskiptareglunnar fyrir mismunandi bolta (1):

1. **Fullkomleika-villa**. Gerum ráð fyrir Embla sé að segja satt þá mun hún í hverri umferð svara áskorun Ara rétt (þ.e. segja rétt til um hvort hann skipti um bolta). Svo þar er fullkomleika-villan 0.

2. **Lögmætis-villa**. Nú gerum ráð fyrir að Embla sé að ljúga að Ara og boltarnir eru í raun eins á litinn. Þá í hverri umferð mun besta strategía Emblu vera að giska á hvort Ari skipti um bolta. Svo líkurnar á að hún giski á rétt, og plati Ara í þeirri umferð, eru 0.5 í hverri umferð og því er lögmætisvillan 0.5 .

Við sjáum að ef við höfum samskiptareglu sem uppfyllir þessum skilyrðum þá getur sannprófarinn ítrað regluna þar til hann er orðinn nægjanlega viss um að sannprófarinn sé að segja satt. Til dæmis, ef Embla er að ljúga að Ara, þá ef hann ákveður að framkvæma 2 umferðir af samskiptareglunni fyrir mismunandi bolta (1) eru líkurnar á því að Embla nái að sannfæra Ara um að boltarnir séu mismunandi á litinn (þótt þeir séu það ekki) $0.5 \cdot 0.5 = 0.25$ þ.e. Ari getur verið 75% viss um að Embla sé að segja satt ef hún svarar rétt í tvær umferðir af reglunni í röð, og ef hann framkvæmir 10 umferðir þá getur hann verið $1 - (0.5)^{10}$, um það bil 99.9% viss að hún sé að segja satt ef hún svarar rétt í öllum umferðunum. Hér sjáum við að ef sannprófarinn (Embla) veit dreifinguna á slembibreytu Ara (þ.e. hvernig hann velur boltana) þá er reglan samt gild, gefið að dreifingin er ekki föst/löggengin, og að sannarinn getur "núllað út" áhrifin að Embla viti dreifinguna með því að leika fleiri umferðir af reglunni. Hann getur það eingöngu ef valið hans byggir raunverulega á handahófskenndu vali byggðri á slembibreytu. Auðvitað er reglan ekki gild ef Ari hefur löggengna strategíu sem Embla veit. Hinsvegar er mikilvægt að Ari viti að Embla viti dreifinguna til að Ari getur reiknað út hversu margar umferðir hann skal leika af samskiptareglunni til að fá líkurnar á svindli undir það gildi sem hann vill.

Hér höfum við skilninginn sem "með miklum líkum" í skilgreiningu 2.1 á við. Það á við að $\mathcal{V}$ getur verið eins nálægt 100% viss um að $\mathcal{P}$ sé að segja satt og $\mathcal{V}$ vill. Þannig að *fullkomleika* getur verið náð með eins nálægt 100% líkum og $\mathcal{V}$ vill. Eins fáum við *lögmæti* "með miklum líkum" þannig að líkurnar á því að óheiðarlegur sannari nái að sannfæra $\mathcal{V}$ um ósanna staðhæfingu er hægt að ná niður í eins nálægt 0% og $\mathcal{V}$ vill. Þessir eiginleikar nást almennt með því að ítra gagnvirku sönnunina nógu oft svo að skilyrði $\mathcal{V}$ á hve viss hann vill vera að $\mathcal{P}$ sé ekki að ljúga er náð.

Við sjáum á skilgreiningunni 2.1 og dæminu um litblinda vininn kjarnann sem lætur gagnvirkar sannanir virka. Sannprófarinn gefur sannaranum í hverri umferð óvænta áskorun og ef sannaranum tekst að svara/ljúka áskoruninni á fullnægjandi máta þá minnka líkurnar á að því í augum sannprófaranns að sannarinn sé að ljúga og sönnunin styrkist. Með Gagnvirkum sönnunum getum við ekki verið 100% viss um staðhæfingu (hvort hún er sönn eða fölsk) en við getum komist eins nálægt því og við viljum með því einu að framkvæma fleiri umferðir af samskiptareglunni.

2.1 Summu athugun

Útlistunin á summu athugun er byggð á umfjöllun í kafla 4.1 í bók Justin Thalers um sannanir, sjá [5].

Við skulum taka eitt sértækt dæmi sem er mikið notað í fræðunum um gagnvirkar sannanir sem og í flækjufræðum (e. complexity theory). Gagnvirka sönnunin sem við skoðum kallast summu-athugun (e. sum-check) og snýst um eftirfarandi summu:

$$H := \sum_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(b_1, b_2, \ldots, b_v),$$

þar sem g er margliða með v-breytum (v-víð margliða, e. v-variate polynomial) og skilgreind yfir eitthvað (vanalega endanlegt) svið $\mathbb{F}$.

Samskiptareglan felst síðan í því að sanna að talan H sé raunverulega summan sem skilgreind er hægra megin.

Við höfum $\mathcal{P}$, sannara, sem segist vita gildið H á summunni fyrir gefna v-víða margliðu. Hvernig getur $\mathcal{P}$ sannað þá staðhæfingu fyrir $\mathcal{V}$.

Einföld sönnun á þessari staðhæfingu $\mathcal{P}$ væri auðvitað fyrir $\mathcal{V}$ bara að reikna summuna sjálfur, sem er auðvelt þegar v er lítil stærð, og bera saman við staðhæfðu summuna frá $\mathcal{P}$. Hinsvegar, þá gerum við hér ráð fyrir að summan sé of stór (innihaldi of marga liði, 2^v) fyrir sannprófarann til að reikna á skikkanlegum tíma. Því eins og vitað er tekur almennur útreikningur á $H \sim O(2^v)$ aðgerðir. Svo ef $v \geq 100$ mun útreikningurinn taka of langan tíma til að sannprófa á þennan einfalda máta. Því snúum við okkur að summu-athugun sem gerir $\mathcal{P}$ kleift að sanna staðhæfinguna fyrir $\mathcal{V}$ án þess að $\mathcal{V}$ þurfi að framkvæma alla þessa reikninga.

Samskiptaregla fyrir Summu Athugun

1. Í upphafi samskiptareglunnar sendir $\mathcal{P}$ töluna C_1 á $\mathcal{V}$ og staðhæfir að $C_1 = H$. Eftir það hefjast umferðirnar.

2. Í fyrstu umferð sendir $\mathcal{P}$ margliðuna $g_1(X_1)$ sem hann staðhæfir að jafngildir einvíðu margliðunni:

$$s_1(X_1) = \sum_{b_2 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(X_1, b_2, \ldots, b_v)$$

3. $\mathcal{V}$ athugar hvort

$$C_1 = g_1(1) + g_1(0)$$

og hvort g_1 sé einvíð margliða af stigi í mesta lagi $\deg_1(g)$ (þar sem $\deg_i(g)$ táknar stig breytu X_i í g), og hafnar ef einhver þessara athugana er röng.

4. $\mathcal{V}$ velur $r_1 \in \mathbb{F}$ af handahófi og sendir á $\mathcal{P}$

5. í lotu i, $1 < i < v$ sendir $\mathcal{P}$ á $\mathcal{V}$ margliðu $g_i(X_i)$ sem hann staðhæfir að sé jöfn einvíðu margliðunni:

$$s_i(X_i) = \sum_{b_{i+1}\in\{0,1\}} \sum_{b_{i+2}\in\{0,1\}} \cdots \sum_{b_v\in\{0,1\}} g(r_1, r_2, \ldots, r_{i-1}, X_i, b_{i+1}, \ldots, b_v)$$

6. $\mathcal{V}$ athugar hvort g_i sé einvíð margliða af stigi í mesta lagi $\deg_i(g)$ og að $g_i(1) + g_i(0) = g_{i-1}(r_{i-1})$ og hafnar staðhæfingunni ef þetta gildir ekki.

7. $\mathcal{V}$ velur $r_i \in \mathbb{F}$ af handahófi og sendir á $\mathcal{P}$

8. Í lotu v þá sendir $\mathcal{P}$ á $\mathcal{V}$ margliðuna $g_v(X_v)$ sem hann staðhæfir að jafngildir einvíðu margliðunni:

$$s_v(X_v) = g(r_1, r_2, \ldots, r_{v-1}, X_v)$$

9. Eins og áður athugar $\mathcal{V}$ hvort g_v er einvíð margliða af stigi í mesta lagi $\deg_v g$ og hvort $g_v(1) + g_v(0) = g_{v-1}(r_{v-1})$, og hafnar ef þetta gildir ekki.

10. Að lokum, ef $\mathcal{P}$ hefur staðist öll fyrirframgreind próf þá velur $\mathcal{V}$ af handahófi $r_v \in \mathbb{F}$ og athugar hvort $g_v(r_v) = g(r_1, r_2, \ldots, r_{v-1}, r_v)$ og hafnar ef þetta gildir ekki.

11. Ef $\mathcal{P}$ stóðst allar loturnar þá samþykkir $\mathcal{V}$ staðhæfinguna og ályktar að $C_1 = H$.

Tökum fyrst einfalt dæmi af notkun summu-athugunar áður en við skoðum hvað veldur því að samskiptareglan uppfyllir fullkomleika og lögmæti.

Dæmi 2.5. Látum $\mathbb{F}$ vera heiltölurnar modulo 13. Látum $g(X_1, X_2, X_3) = X_1X_2X_3 + 2X_2X_1^2 + 5X_3$. Við höfum þá summuna

$$H := \sum_{b_1\in\{0,1\}} \sum_{b_2\in\{0,1\}} \sum_{b_3\in\{0,1\}} g(b_1, b_2, b_3) = 25 \equiv 12 \pmod{13}$$

Í upphafi samskiptareglunnar sendir sannarinn,$\mathcal{P}$, heiltöluna $C_1 = 12$ á $\mathcal{V}$ sem hann staðhæfir að jafngildir H (sem það gerir hér).

Lota 1: $\mathcal{P}$ sendir á $\mathcal{V}$ margliðuna $g_1(X_1)$ sem hann heldur fram að jafngildir $s_1(X_1)$ (sjá samskiptaregluna fyrir skilgreiningu á s_i margliðunum):

$$g_1(X_1) = \sum_{b_2\in\{0,1\}} \sum_{b_3\in\{0,1\}} g(X_1, b_2, b_3) = 5+2X_1^2+5+2X_1^2+X_1 = 10+X_1+4X_1^2$$

$\mathcal{V}$ athugar bæði $\deg(g_1) = 2 \leq \deg_1(g) = 2$ og að:

$$g_1(0) + g_1(1) = 10 + 10 + 1 + 4 = 25 \equiv 12 \pmod{13}$$

$\mathcal{P}$ stóðst þessar fyrstu athuganir svo að $\mathcal{V}$ velur $r_1 = 7 \in \mathbb{F}$ af handahófi og sendir á $\mathcal{P}$.

Lota 2: $\mathcal{P}$ reiknar margliðuna:

$$g_2(X_2) = \sum_{b_3\in\{0,1\}} g(r_1, X_2, b_3) = 98X_2+7X_2+98X_2+5 = 5+203X_2 \equiv 5+8X_2 \pmod{13}$$

og sendir á $\mathcal{V}$. $\mathcal{V}$ athugar að $\deg(g_2) = 1 \leq \deg_2(g) = 1$ og reiknar

$$g_2(0) + g_2(1) = 5 + 5 + 8 = 18 \equiv 5 \pmod{13}$$

og

$$g_1(r_1) = 10 + 7 + 4 \cdot 7^2 = 213 \equiv 5 \pmod{13}$$

þ.a. $g_2(0) + g_2(1) = g_1(r_1)$ svo að $\mathcal{V}$ velur $r_2 = 3 \in \mathbb{F}$ af handahófi og sendir á $\mathcal{P}$

Lota 3: $\mathcal{P}$ reiknar margliðuna:

$$g_3(X_3) = g(r_1, r_2, X_3) = g(7, 3, X_3) = 21X_3+294+5X_3 \equiv 8+0X_3 \pmod{13}$$

og sendir á $\mathcal{V}$ sem athugar hvort $\deg(g_3) = 0 \leq \deg_3(g) = 1$ og reiknar:

$$g_3(0) + g_3(1) = 8 + 8 = 16 \equiv 3 \pmod{13}$$

og

$$g_2(r_2) = g_2(3) = 5 + 8 \cdot 3 = 29 \equiv 3 \pmod{13}$$

þ.a. $g_3(0) + g_3(1) = g_2(r_2)$. Að lokum velur $\mathcal{V}$ $r_3 = 7 \in \mathbb{F}$ af handahófi og reiknar, sjálfur:

$$g_3(r_3) = g_3(7) = 8$$

og

$$g(7, 3, 7) = 7 \cdot 3 \cdot 7 + 2 \cdot 3 \cdot 7^2 + 5 \cdot 7 = 476 \equiv 8 \pmod{13}$$

þ.e. $g_3(r_3) = g(r_1, r_2, r_3)$ og því, fylgjandi samskiptareglunni, samþykkir $\mathcal{V}$ staðhæfingu $\mathcal{P}$ að $C_1 = H$. □

Eftir þetta lýsandi dæmi á samskiptareglunni skulum við skoða hvað gerir hana að gagnvirkri sönnun.

Athugum að samskiptareglan felur í sér, í hverri lotu i, að $\mathcal{P}$ sendir einvíða margliðu g_i á $\mathcal{V}$ sem sannarinn staðhæfir að jafngildir s_i, $s_i(r) = g_i(r), \forall r \in \mathbb{F}$. Nú ef $\mathcal{P}$ er óheiðarlegur þá veit hann ekki hver margliðan s_i er og verður því að giska á hana. Giskið hans verður margliðan g_i. Nú vitum við að sérhverjar tvær *mismunandi* margliður af stigi d geta í *mesta* lagi verið jafngildar í d punktum $r \in \mathbb{F}$ og ef þær taka sama gildi í fleirum fáum við að margliðurnar eru ein og sama margliðan. Svo ef við höfum margliðu $g_i \neq s_i$ þá gildir:

$$P_{r \in_R \mathbb{F}}[s_i(r) = g_i(r)] \leq d/|\mathbb{F}|$$

Þar sem við notum $r \in_R \mathbb{F}$ til að tákna að gildið $r \in \mathbb{F}$ er valið af handahófi (með jafndreifingu).

Sem felur í sér þá fullyrðingu að líkurnar á að margliðan sem $\mathcal{P}$ velur í umferð i taki sama gildi og s_i í handahófskenndu gildi $r \in \mathbb{F}$ eru minni en eða jafnar $d/|\mathbb{F}|$, og þar sem í flestum tilfellum er $d << |\mathbb{F}|$ eru þetta óverulegar líkur.

Sönnum nú, óformlega, að samskiptareglan sé *Gagnvirk sönnun.*

Fullkomleiki

Athugum að ef $\mathcal{P}$ er sannsögull þá mun samskiptareglan leiða til þess að $\mathcal{V}$ samþykkir staðhæfinguna með líkunum 1. Því $\mathcal{P}$ mun alltaf geta sent $g_i = s_i$ í sérhverri umferð i.

Lögmæti

Hér viljum við sýna að ef $\mathcal{P}$ er ósannsögull, þ.e. $C_1 \neq H$, að þá eru líkurnar á að $\mathcal{P}$ nái að plata $\mathcal{V} < 1$.

Notum þrepun á fjölda breyta í fallinu g.

Gerum ráð fyrir að $v = 1$, þ.e. g er einvíð margliða af stigi d. Þá sendir $\mathcal{P}$ í byrjun C_1 sem hann staðhæfir að sé jafngilt

$$H = g(0) + g(1)$$

Og margliðuna $g_1(X_1)$ sem hann staðhæfir að jafngildir:

$$s_1(X_1) = g(X_1)$$

Athugum að ef $s_1 \neq g_1$ þá gildir þar sem þetta eru mismunandi einvíðar margliður af stigi í mesta lagi $\deg_1(g) = d$ að þær geta í mesta lagi tekið sama gildi í d mismunandi gildum í $\mathbb{F}$ þ.a.

$$P_{r_1 \in_R \mathbb{F}}[s_1(r_1) = g_1(r_1)] \leq d/|\mathbb{F}|$$

skv. umræðunni okkar að ofan þ.a. líkurnar á að $\mathcal{V}$ hafni staðhæfingu $\mathcal{P}$ eru $1 - d/|\mathbb{F}| < 1$.

Nú ef g er $(v-1)$-víð margliða, af heildarstigi d, gerum við ráð fyrir að líkurnar á að $\mathcal{V}$ hafni falskri staðhæfingu, $C_1 \neq H$, séu að minnsta kosti $1-d(v-1)/|\mathbb{F}|$. Við rifjum upp að:

$$s_1(X_1) = \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(X_1, b_2, \ldots, b_v).$$

Nú sendir $\mathcal{P}$ margliðu $g_1 \neq s_1$ í fyrstu lotu samskiptareglunnar. Eins og áður eru líkurnar á að $g_1(r_1) = s_1(r_1)$ fyrir handahófskennt r_1 í mesta lagi $d/|\mathbb{F}|$. Þannig að með skilyrtum atburði $g_1(r_1) \neq s_1(r_1)$ þá þarf $\mathcal{P}$ að reyna sanna að

$$C_2 = g_1(r_1) = \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(r_1, b_2, \ldots, b_v)$$

og þar sem $g(r_1, X_2, \ldots, X_v)$ er v-1 víð margliða af heildargráðu d eru líkurnar á því að $\mathcal{V}$ hafni staðhæfingunni

$$g_1(r_1) = \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(r_1, b_2, \ldots, b_v)$$

í einhverri af lotum 2 til v að minnsta kosti $1 - d(v-1)/|\mathbb{F}|$ skv þrepunarforsendu. Það veldur því að líkurnar á að $\mathcal{V}$ samþykki ranga staðhæfingu $C_1 = H$, þar sem raunverulega $C_1 \neq H$, eru

$$P_{r_1 \in_R \mathbb{F}}[s_1(r_1) = g_1(r_1)] +$$

$$P[\mathcal{V} \text{ samþykkir staðhæfinguna } s_1(r_1) := g_1(r_1) \mid s_1(r_1) \neq g_1(r_1)]$$
$$\leq d/|\mathbb{F}| + d(v-1)/|\mathbb{F}| = dv/|\mathbb{F}|.$$

Athugum að í summunni hér að ofan þá þarf óheiðarlegur sannari aðeins að hitta á eitt gildi r_i þ.a. $s_i(r_i) = g_i(r_i)$ en ekki í sérhverri lotu, þess vegna eru líkurnar summaðar en ekki margfaldaðar saman.

Við höfum því sýnt að summu-athugun hefur lögmætisvillu upp á $dv/|\mathbb{F}|$, þar sem d er hæsta stig margliðunnar og v er fjöldi breyta, svo á meðan $d \cdot v < \mathbb{F}$ þá er lögmæti uppfyllt.

Út frá þessu sjáum við að summu-athugun er gagnvirk sönnun því hún uppfyllir bæði fullkomleika með líkum 1 og lögmæti með líkum $1 - dv/|\mathbb{F}|$.

2.1.1 Umræða um Summu Athugun

Summu-athugun er tiltölulega einföld gagnvirk sönnun. Hún sýnir einnig hve öflugar gagnvirkar sannanir geta verið. Því það tekur $\mathcal{V}$ aðeins $O(v +$ [Fjöldi aðgerða til að reikna gildið á g í einum punkti í $\mathbb{F}^v$]) í staðinn fyrir $O(2^v)$ ef hann reiknar summuna beint. Hinsvegar tekur það sannarann um $O(2^v \cdot$[Fjöldi aðgerða til að reikna gildið á g í einum punkti í $\mathbb{F}^v$]) sem er auðvitað alltof tímafrekt til notkunar í raunheimum, fyrir flest vandamál. Hinsvegar er summu-athugun gott verkfæri til að sýna að til séu *Gagnvirkar sannanir* á ákveðnum vandamálum, því oft er hægt að minnka (e. reduce) vandamál niður í að reikna svona margliðusummu. Vandamál sem hægt er að minnka niður í útreikning á margliðusummu eru t.d. að telja þríhyrninga í neti og margföldun fylkja og því eru til *Gagnvirkar sannanir* fyrir bæði þessi vandamál.

2.2 Umræða um hagnýtingar

Hagnýtingar á gagnvirkum sönnunum eru mögulegar alls staðar þar sem tveir aðilar þurfa að treysta á hvorn. Þar koma gagnvirkar sannanir að notum til að útrýma þörfinni á trausti.

Til dæmis er oft hagur í að fá aðra tölvu til að framkvæma útreikninga sem manns eigin tölva er hæg að framkvæma. Gefum okkur að við þurfum að reikna útkomu-fylkið C sem fæst með því að margfalda fylkin A og B, $C = AB$. Það getur verið tímafrekt á fartölvu fyrir mjög stór fylki og því gæti maður viljað útvista verkefninu til ofurtölvu út í heimi. Við látum hana fá fylkin A og B og hún sendir innan skamms til baka fylkið C. En hvernig getum við verið viss um að ofurtölvan reiknaði raunverulega fylkið C, og ennfremur hvort það var rétt reiknað? Þar koma sannanir til bjargar. Ein einföld útfærsla á sönnun fyrir þetta verk kallast *Algrím Freivalds* (sjá [7] eða kafla 2.2 í [5]) og krefst af sannprófaranum að reikna ABx fyrir einhvern vigur x og bera saman við Cx, hafna ef mismunandi en samþykkja annars. Athugum að það tekur aðeins $O(n^2)$ útreikninga að reikna $x_1 = Bx$ og eins aðeins $O(n^2)$ að reikna Ax_1 og C_x svo útreikningarnir ABx og Cx eru aðeins $O(n^2)$ fyrir sannprófarann. Á meðan tekur það, fyrir venjuleg algrím (til eru hraðari), $O(n^3)$ að reikna $C = AB$. Við sjáum því að með þessari gagnvirku sönnun þarf sannprófarinn að framkvæma verulega færri útreikninga heldur en ef hann þyrfti að reikna $C = AB$ sjálfur.

Dæmið um Freivald hér að ofan er aðeins ætlað til einfaldra útskýringa á mögulegri hagnýtingu sannana. Hinsvegar er algrím Freivalds ekki beint gagnvirk sönnun (því sannarinn sendir bara lausnina á sannprófarann, engin fleiri samskipti verða milli þeirra). Til eru gagnvirkar sannanir fyrir fylkjamargföldun og ein þeirra byggir á *summu-athugun.*. Sjá kafla 4.4 í [5].

3 Gagnvirk Sönnun án upplýsinga

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

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 3.1. *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 3.2. 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 (3.1).

Skilgreining 3.3. 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.

3.1 Hermar

Þessi kafli er byggður á umfjöllun um herma í kafla 2.1 í ritgerð eftir Gerardo I. Simari, sjá [4].

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 3.4. 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 innganginum. 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. 3.3

Skilgreining 3.5. *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.

3.2 Strjáll logri

Eftirfarandi umfjöllun er að miklu leiti byggð á kafla 1.2.3 og 2.2 úr ritgerð Nihal R. Gowravaram, sjá [2].

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 3.6. (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 logrinn 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 [2] eða kafla 11 í [5])

3.3 Þrílitað net

Umfjöllun þessa kafla er byggð á kafla 4.2 úr ritgerð Nihal R. Gowravaram (sjá [2]) og kafla 3 í ritgerð Gerardo I. Simari (sjá [4]).

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 [1])).

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.

3.4 Smá flækjufræði

Skilgreining 3.7. P er flokkur af ákvörðunar-vandamálum sem eru leysanleg með algrími sem keyrir í margliðutíma

Skilgreining 3.8. 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 3.9. 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 3.10. 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 [8]) 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.

4 ZKP án Gagnvirkni

Umfjöllun þessa kafla er byggð á kafla 4.7 úr óútgefinni bók eftir Justin Thaler, sjá [5], sem og wikipedia-grein um Fiat-shamir, sjá [6].

Nú höfum við séð nokkrar samskiptareglur sem hægt er að nota til að sanna hinar ýmsu staðhæfingar og í þeim öllum er grundvallaratriði að sannarinn gefur sannprófaranum færi á að spyrja sig spurninga/leggja fyrir sig áskoranir. Þetta er gagnvirknin í samskiptareglunni. Gagnvirknin er sjálf samskiptin milli sannarans og sannprófarans og er, eins og við höfum drepið svo oft að áður, mikilvægasti partur sannaninnar. Það að sannprófarinn geti spurt sannarann spurninga er það sem gerir *Gagnvirkar Sannanir* traustverðugar. Þrátt fyrir það spyr maður sig samt, er hægt að komast hjá samskiptunum. Er hægt að hafa sönnun án Gagnvirkni og afhverju ætti maður að vilja það?

Þrátt fyrir að gagnvirknin sé undirstaðan í gagnvirkum sönnunum hefur hún sína ókosti eins og t.d. að sannarinn þarf að sanna staðhæfinguna sína að nýju fyrir sérhvern nýjan einstakling. Það væri kúl, og hentugra, ef sannarinn gæti bara birt sönnun sína fyrir öllum og sannprófarar farið yfir sönnunina án þess að þurfa að eiga í óþarfa samskiptum við sannarann. En einnig án þess að þurfa að gefa upp á bátinn öryggið sem gagnvirkar sannanir veita.

Svo við viljum einhvernveginn losna við samskiptin milli sannarans og sannprófarans en samt halda lögmæti sönnunarinnar. Notum samskiptareglu strjála lograns og reynum að breyta henni í sönnun án gagnvirkni.

Við þurfum fyrsta skilgreiningu á véfrétt.

Skilgreining 4.1. Við skilgreinum *Véfrétt* sem eitthvað óþekkt algrím sem tekur við inntaki og gefur úttak til baka. *Handahófskennda-Véfrétt* skilgreinum við sem óþekkt algrím sem fyrir hver tvö mismunandi inntök, gefur tvö mismunandi handahófskennd úttök, en ef inntökin 2 eru eins þá eru úttök véfréttarinnar líka eins.

Minnum okkur aftur á samskiptareglu strjála lograns

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 sjáum að til að breyta þessari samskiptareglu í sönnun án gagnvirkni þurfum við að skipta út virkni sannprófarans í samskiptunum. Þannig að við þurfum að fá valið á b einhvern veginn öðruvísi heldur en frá $\mathcal{V}$.

Fyrsta, ógáfulega, pæling til að breyta reglunni í sönnun án gagnvirkni væri að leyfa $\mathcal{P}$ að velja b-ið sjálfur af handahófi. En við áttum okkur fljótt á skyssunni þar því það mun eingöngu virka ef við treystum $\mathcal{P}$ til að velja b-ið af handahófi (því auðvitað getur $\mathcal{P}$ valið b-ið þannig að það virki alltaf fyrir hann í hverri umferð), en þar sem við viljum ekki þurfa að treysta $\mathcal{P}$ þá gengur þessi lausn ekki.

Önnur, ógáfuleg, pæling væri að nota sameiginlega véfrétt, $\mathcal{O}$, þ.a. $\mathcal{P}$ sendir h úr skrefi 1 á véfréttina og véfréttin gefur handahófskennt svar tilbaka $\{0, 1\}$ (en samt sama svar ef $\mathcal{P}$ sendir sama h-ið aftur, svo þegar $\mathcal{V}$ fer yfir sönnunina getur hann athugað hvort þetta eru réttu gildin sem véfréttin gaf). Þessi hugmynd er ekki góð því $\mathcal{P}$ getur, áður en hann býr til sönnunina, fundið mismunandi $h = g^r \pmod{p}$ sem gefa 0 og mismunandi $h = g^r v^{-1} \pmod{p}$ sem gefa 1 og notað þau í sönnuninni sinni, þá veit hann gildin sem hann mun fá og mun því geta framleitt sannfærandi sönnun. Sem er samt ósönn.

Við komumst að þeirri niðurstöðu að til að geta breytt samskiptareglunni í sönnun án gagnvirkni þurfum við að breyta henni örlítið. Þá getum við notað svipaða hugsun og að ofan með handahófskenndu véfréttina.

4.1 Fiat-Shamir Ummyndun

Við sáum í kafla 2 að gagnvirkar sannanir styðja sig heilmikið við möguleika sannprófara á að koma sannara á óvart. Pælingin í Fiat-Shamir er að nýta sér það og skipta slembileika sannprófarans út fyrir slembileika heiðarlegs þriðja aðila (sem er almennt líkt sem hass-falli (e. hash-function) í hagnýtingum) sem bæði sannari og sannprófari hafa aðgang að.

Í Fiat-Shamir ummyndun þá gerum við ráð fyrir að sannarinn og sannprófarinn hafa aðgang að sömu handahófskenndu-véfréttinni. Síðan þegar sannarinn

$\mathcal{P}$ vill útbúa sönnunina þá framkvæmir hann samskiptaregluna eins og hann myndi gera við sannprófara nema í staðinn fyrir að hafa samskipti við sannprófarann hefur hann samskipti við véfréttina.

Uppfærð 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 $0 \leq b < p$ 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 $h = g^a v^{-b}$, 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.

Athugum að ef $\mathcal{P}$ er heiðarlegur þá er $g^a v^{-b} = g^{r+bx} g^{-bx} = g^r = h$ og því mun hann sannfæra $\mathcal{V}$ um staðhæfinguna. Sönnunin á því að uppfærða samskiptareglan er gagnvirk sönnun án upplýsinga fer fram á svipaðan máta og sönnunin í kaflanum á undan. Hérna getum við notað Fiat-Shamir ummyndun. Með Fiat Shamir verður sönnunin svona:

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, og reiknar $h = g^r \pmod{p}$.
2. $\mathcal{P}$ sendir h á handahófskenndu-véfréttina $\mathcal{O}$ og fær tilbaka $0 \leq b < p$.
3. $\mathcal{P}$ reiknar $a = r + bx \pmod{p}$ og geymir $(h, a)_i$ sem sönnunina á staðhæfingunni fyrir lotu i.
4. Ítra skref 1-3 þar til nógu mörg gildi $(h, a)_i$ eru tilbúin svo sönnunin sé með nægilega lága lögmætis-villu.
5. skila sönnuninni $\{(h, a)_1, (h, a)_2, ..., (h, a)_k\}$.

Athugum nú að sérhver sannprófari getur lesið sönnunina $\{(h, a)_1, (h, a)_2, ..., (h, a)_k\}$ og athugað fyrir hverja lotu hvort að $h = g^a v^{-b}$, en ekki eingöngu það heldur líka hvort $b = \mathcal{O}(h)$ þar sem $\mathcal{O}(*)$ skilar tölunni sem handahófskennda-véfréttin skilar á inntaki h. Og ef $b \neq \mathcal{O}(h)$, í einhverri lotunni, þá hafnar $\mathcal{V}$ sönnuninni.

Athugum að í þessari útfærslu af samskiptareglu strjála lograns þá þarf $\mathcal{P}$ alltaf að vita lausn á strjála logranum af v til að svara $\mathcal{V}$ á réttan máta, nema þegar $b = 0$. Þannig var það ekki í upprunalegu skilgreiningunni.

Við sjáum að lykillinn bakvið þessa sönnun án gagnvirkni er að láta töluna sem véfréttin skilar vera háða svörum $\mathcal{P}$, og að svör véfréttarinnar eru handahófskennd og mismunandi fyrir mismunandi inntök. Það veldur því að óheiðarlegur $\mathcal{P}$ mun ekki geta áætlað fyrirfram hvernig hann muni geta klekkt á væntanlegum sannprófurum.

Fiat-Shamir ummyndunin er því sú almenna aðferð að skipa út sannprófaranum fyrir handahófskennda-véfrétt, sem sannarinn og allir sannprófarar hafa aðgang að, og láta sannarann nota véfréttina þannig að svör véfréttarinnar eru háð skuldbindingu sannaranns (t.d. skuldbindingu hans við töluna r og því h í skrefi 1 í strjála logranum).

Þetta svipar til Bálkakeðju-líkansins í rafmyntum þar sem sérhver bálki er háður hassinu á bálkunum á undan.

Handahófskenndar-véfréttir eru almennt útfærðar í praktís sem hass-föll, t.d. sha256 og sha3.

Þess ber að geta að Fiat-Shamir ummyndun er einungis ein aðferð til að breyta gagnvirkri sönnun í sönnun án gagnvirkni. Til eru fleiri.

4.2 Umræða um hagnýtingar á sönnunum án upplýsinga

Hagnýtingarnar eru margar. Nú þar sem sönnun án upplýsinga er gagnvirk sönnun vitum við, eins og kom fram í umræðunni um hagnýtingar á gagnvirkum sönnunum (2.2), að þær nýtast vel í að útrýma nauðsyn trausts á milli aðila. Eiginleikinn „án upplýsinga" er síðan hægt að nýta þar sem viðkæmar upplýsingar eru til staðar. Upplýsingar sem er nauðsynlegt að halda leyndum.

Augljós hagnýting er verndun lykilorða. Til dæmis getum við nýtt samskiptaregluna um strjála logrann (3.6) til að gera notanda kleyft að auðkenna sig án þess að gefa upp lykilorðið sitt. Þetta er tiltölulega lýsandi, og öflugt, dæmi. Athugum að með þessu kerfi þá er ekki nauðsynlegt fyrir notandann að senda lykilorðið sitt til (t.d.) bankans eða þess sem vill vera viss um að notandinn sé sá sem hann segist vera. Það eina sem bankinn hefur er v-ið í reglunni og þegar notandinn auðkennir sig svarar hann aðeins spurningum bankans í samræmi við samskiptaregluna. Nú er þessi samskiptaregla svo öflug að ekki er einu sinni nauðsynlegt að dulkóða skilaboðin. Því hlerari, sem reynir að stela mikilvægum upplýsingum, öðlast engar upplýsingar á því að fylgjast með samskiptunum (reglan er „án upplýsinga"). Hann getur ekki einu sinni verið viss um hvort samskiptin séu raunveruleg.

Fleiri mögulegar hagnýtingar eru í kjarnorkuafvopnun (sjá [9] og kafla 5.2 í [2]) og viðskipta-reglugerðum (sjá II-hluta ritgerðar Nihal R. Gowravaram, [2]).

ZKP-án gagnvirkni hafa einnig mikla möguleika á hagnýtingum. Mest vinna og þróun á ZKP-án gagnvirkni hefur verið gerð í rafmyntum eins og ZCash og Monero. Þar sem þær nota (meðal annars) zk-SNARKs (e. zero knowledge succint non-interactive *arguments* of knowledge, sjá [11]), sem er afbrigði af ZKP-án gagnvirkni, til að t.d. fela upphæðir í viðskiptum (e. transactions), reikningsnúmer (hver á hvaða „reikning") og hver raunverulega borgaði hvað. (fyrir Zcash sjá [10], og Monero sjá sérstaklega „Pedersen Commitment", „Stealth Address" og „Ring CT" á [3])

Heimildir

[1] M. Blum, *How to prove a theorem so no one else can claim it*, in Proceedings of the International Congress of Mathematicians, 1987, pp. 1444–1451.

[2] N. R. Gowravaram, *Zero knowledge proofs and applications to financial regulation*, 2018. Harvard University, Senior Thesis, https://dash.harvard.edu/handle/1/38811528/, sótt 11.04.2021.

[3] Monero-team, *Moneropedia*, 2021. https://www.getmonero.org/resources/moneropedia/, sótt 11.04.2021.

[4] G. I. Simari, *A primer on zero knowledge protocols*, 2002. Universidad Nacional del Sur, Paper.

[5] J. Thaler, *Proofs, Arguments, and Zero-Knowledge*, Óútgefið efni í eigu höfundar, 2021. http://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.html/, sótt 11.04.2021.

[6] Wikipedia, *Fiat-shamir heuristic*, 2021. https://en.wikipedia.org/wiki/Fiat%E2%80%93Shamir_heuristic/, sótt 11.04.2021.

[7] ——, *Freivalds algorithm*, 2021. https://en.wikipedia.org/wiki/Freivalds'_algorithm/, sótt 11.04.2021.

[8] ——, *Graph coloring*, 2021. https://en.wikipedia.org/wiki/Graph_coloring#Computational_complexity/, sótt 11.04.2021.

[9] ——, *Zero-knowledge proof*, 2021. https://en.wikipedia.org/wiki/Zero-knowledge_proof#Nuclear_disarmament/, sótt 11.04.2021.

[10] Zcash-team, *How it works*, 2021. https://z.cash/technology/, sótt 11.04.2021.

[11] ——, *What are zk-snarks?*, 2021. https://z.cash/technology/zksnarks/, sótt 11.04.2021.