Sönnun án upplýsinga

Þórður Ágústsson

14. mars 2021

Útdráttur

Ágrip hér

1 Inngangur

Sannanir eru margskonar. Þær hefðbundnu sem maður hugsar um í stærðfræðinámi eru byggðar á röksemdarfærslu þar sem staðhæfing A er gefin og sönnunin leiðir lesandann frá þekktum staðreyndum (sannaðar áður eða "axioms") 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 etc. (KOMA MEÐ DÆMI UM SÖNNUN, I.E. REGLU OG SANNA HANA EH EAZY)

Þær sannanir sem við munum skoða í þessari ritgerð eru ekki af þessu almenna tagi. Þær krefjast þess að við víkkum skilgreiningu okkar á "sönnun". Einfalt er að hugsa sér að orðið "sönnun" á ekki eingöngu við reglur í stærðfræði, heldur einnig getur maður sannað staðhæfingu eins og $\sqrt{2}$ er rót margliðunnar $f(x) = x^2 - 2$. Sem er ekki regla á borð við pýþagórasarregluna, heldur fremur einhverskonar staðhæfing að rót margliðunnar er þekkt.

Til dæmis segir grundvallarregla algebrunnar að sérhver margliða af stigi d hefur d-rætur (í $\mathcal{C}$). 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, helur fremur staðhæfing um þekkta lausn á vandamáli. Sannanirnar sem við skoðum í þessari ritgerð eru líkari seinni tegundinni. Þær eru tól sem einstaklingar geta notað til að sanna þekkingu á lausn á vandamáli fyrir öðrum, í þeim skilningi að einn veit svar við vandamáli og vill sanna að svarið sé lausn fyrir öðrum án þess að hinn þurfi að leysa vandamálið sjálfur.

Ein tegund af þesskonar sönnunum er sönnun án upplýsinga. Þær eru mikilvægur undirflokkur af sönnunum sem hafa hagnýtt gildi í raunheimum.

Eftirfarandi er sögudæmi sem sýnir kjarna sannana án upplýsinga.

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?"

"Hugsaði að þú vildir kannski bolta, en vissi ekki hvaða lit þú vildir svo tók bara 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 tekur annan boltann "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. Hlítur 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 litaðir?

Skilgreining 1.1. 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 sér ekki boltana.

2. Síðan setur Ari annan boltann upp á borðið en heldur hinum földum. Og setur boltann síðan aftur undir borð.

3. Ari velur síðan annan boltann aftur (hér getur hann valið sama bolta og hann sýndi fyrst eða valið hinn) og setur upp á borðið og spyr Emblu "Er þetta sami bolti og ég sýndi þér fyrst?".

   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&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 afhverju ég efaðist 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 græna boltann og stingur í töskuna sína.

2 Gagnvirkar Sannanir (e. Interactive Proofs)

Eins og drepið var á í inngangínum fjalla sannanir þessarar ritgerðar um að sanna að gefin lausn á fyrirfram-skilgreindu vandamáli er 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 $g^x = v(\mod p)$ (sjá kafla 2.1), þrílitun á neti (kafli 2.2), 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 dæmi væri óþarfi að nota gagnvirka sönnun til að sanna að $x = \sqrt{2}$ sé rót á fallinu $f(x) = x^2 - 2$, því auðvelt/fljótlegt er að sannfæra þann sem skilur veldisvísa $x = \sqrt{2}$ er rót fallsins einungis með beinum reikningi $f(\sqrt{2}) = (\sqrt{2})^2 - 2 = 2 - 2 = 0$.

Eftirfarandi er skilgreining á Gagnvirkri Sönnun:

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 kynns algrím sannprófarinn getur verið, þ.e. hversu lengi hann má í versta falli keyra þ.a. þegar $\mathcal{V}$ er keyrt í samskiptareglunni á inntaki (staðhæfingu) x, þá tekur það $\mathcal{V}$ í versta falli $O(|x|^k)$ margar aðgerðir áður en $\mathcal{V}$ stöðvast. En engar hömlur eru settar á keyrslutíma sannaranns.

Svo t.d. 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 á meðan sannprófarinn þarf að keyra í margliðu-tíma til að reglan sé *Gagnvirk Sönnun*.

Við höfum því þær hömlur að sannprófarinn verður að geta keyrt útreikningana í samskiptareglunni "hratt", í einhverjum skilningi.

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

Innri slembileikinn getur því verið skilgreindur af dreifingu sem er óþekkt frá sannaranum séð. Fyrir framhaldið getur verið gott að líta á Innri slembileikann sem upphafsdreifingu Markov-Keðju.

Skilgreining 2.3. Látum $(\mathcal{P}, \mathcal{V})$ vera Gagnvirka sönnun. Látum x tákna staðhæfinguna sem $\mathcal{P}$ heldur fram og látum r vera innri slembileika $\mathcal{V}$ og látum r_0 tákna tölu sem tekin er úr dreifingu r af handahófi þegar samskipti $\mathcal{P}$ og $\mathcal{V}$ hefjast (þ.e. r_0 er fasti ákvarðaður af dreifingu r). Við táknum þá $(\mathcal{P}, \mathcal{V}, x, r_0) \in \{0, 1\}$ sem 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 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.

Innri slembileiki, þar sem Gagnvirk sönnun byggir á röð spurninga og svara á milli sannara og sannprófara er innbyggt í sannprófarann slembistærð r. Því í hverri umferð samskiptareglunnar þá getur sannprófarinn ákveðið hver næsta spurning skal vera. Sem veldur að í augum sannaranns $\mathcal{P}$ geta spurningarnar verið túlkaðar sem slembibreytur.

Við sjáum þetta vel í dæminu um litblinda vininn. Þar er Embla sannarinn og Ari sannprófarinn. Í hverri umferð þá sýnir Ari Emblu annan boltann, og það er algjörlega undir Ara komið að ákveða hvorn boltann hann sýnir Emblu. Hann getur sýnt henni alltaf sama boltann. Alltaf skipst á. Eða valið bolta algjörlega af handahófi.

Ef strategía Ara er að velja bolta af handahófi getum við lýst honum sem slembibreytu A þ.a. $P[A = "SamiboltiogArisndisustuumfer"] = P[A = Ękki Samiboltiog Arisndisustuumfer"] = 0.5$. En ef við festum A sem "Sami bolti og Ari sýndi í síðustu umferð"þá er restin af umferðinni í samskiptareglunni orðin löggeng (deterministic) og við getum því skilgreint úttakið/fallið í skilgreiningunni hér að ofan 2.3.

Snúum okkur nú að setningunni '*Gagnvirk sönnun* er samskiptaregla sem fullnægir eftirfarandi eiginleikum með "miklum líkum“ í skilgreiningu 2.1.

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 sannsögull. Fyrir sérhverja staðhæfingu x og slembibreytu r gildir:

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

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

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

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

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

Í litblindi Vinurinn dæminu þá höfum við:

1. 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. 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 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 viss um að sannprófarinn sé að segja satt. T.d. Ef Embla er að ljúga að Ara þá ef hann ákveður að framkvæma 2 umferðir af bolta-samskiptareglunni þá eru líkurnar á því að Embla nái að sannfæra Ara um það boltarnir eru mismunandi á litinn (þótt þeir séu það ekki) 0.5*0.5 = 0.25 þ.e. Ari getur verið 75% viss um að Embla sé að segja satt ef hún svara rétt í tvær umferðir í röð, og ef hann framkvæmir 10 umferðir þá getur hann verið $1 - (0.5)^{10}$ þ.e. uþb. 99.9% viss að hún sé að segja satt ef hún svarar rétt í öllum umferðunum.

Við sjáum í þessu dæmi kjarnann hvernig Gagnvirkar sannanir virka. Sannprófarinn gefur sannaranum í hverri umferð áskorun og ef sannaranum tekst að svara/ljúka áskoruninn þá minnka líkurnar á að hún sé að ljúga og sönnunin styrkist. Við getum aldrei verið 100% viss um staðhæfinguna en við getum komist eins nálægt því og við viljum með því einu að framkvæma fleiri umferðir af samskiptareglunni.

2.1 Summu athugun

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 (þ.e. v-víð margliða, e. v-variate polynomial) og skilgreind yfir eitthvað (vanalega endanlegt) svið $\mathbf{F}$.

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 getum $\mathcal{P}$ 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, en við gerum hér ráð fyrir að hún er of stór fyrir sannprófaran 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. 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.

Útlistun á samskiptareglunni.

Samskiptaregla fyrir Summu Athugun

1. Í upphafi samskipareglunnar sendir $\mathcal{P}$ C_1 á $\mathcal{V}$ og staðhæfir að $C_1 = H$, og þá 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 i í g), og hafnar ef einhver þessara prófa er röng.

4. $\mathcal{V}$ velur $r_1 \in \mathbf{F}$ 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. Í lotu v þá sendir $\mathcal{P}$ á $\mathcal{V}$ margliðuna $g_v(X_v)$ sem hann staðhæfir að jafngildir einvíðu margliðunni:

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

8. 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.

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

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

Tökum fyrst einfalt dæmi áður en við skoðum hvað veldur því að samskiptareglan uppfylli fullkomleika og lögmæti.

Dæmi Látum $\mathbf{F}$ vera heilturnar modulo 13. Látum $g(X_1, X_2, X_3) = X_1X_2X_3 + 2X_2X_1^2 + 5X_3$ þ.a.

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

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

Lota 1 Síðan sendir $\mathcal{P}$ margliðuna

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

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

$$g_1(0) + g_1(1) = 10 + 10 + 1 + 4 = 25(\text{ mod } 13) = 12 = C_1$$

$\mathcal{V}$ velur $r_1 = 7 \in \mathbf{F}$ af handahófi og sendir á $\mathcal{P}$.

Lota 2

$\mathcal{P}$ reiknar margliðuna:

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

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

$$g_2(0) + g_2(1) = 5 + 5 + 8 = 18 \equiv 5$$

og

$$g_1(r_1) = 10 + 7 + 4 * 7^2 = 213 \equiv 5$$

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

Lota 3

$\mathcal{P}$ reiknar margliðuna:

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

og sendir á $\mathcal{V}$.

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

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

og

$$g_2(r_2) = g_2(3) = 5 + 8 * 3 = 293(\text{ mod } 13)$$

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

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

og

$$g(7, 3, 7) = 7 * 3 * 7 + 2 * 3 * 7^2 + 5 * 7 = 476 \equiv 8(\text{ mod } 13)$$

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

Eftir þetta dæmi skulum við nú skoða hvað gerir þessa samskiptareglu að gagnvirkri sönnun.

Til þess þá þurfum við eftirfarandi niðurstöðu, athugum að heildarstig er hámarks stig af liðunum í margliðu. T.d. ef við höfum margliðu $g(x_1, x_2) = 3x_1^3x_2 + 4x_2^5$ þá er liðurinn $3x_1^3x_2$ af stigi 4 og $4x_2^5$ af stigi 5 svo heildarstig margliðunnar er 5.

Hjálparsetning 2.5. (Schwartz Zippel Lemma). *Látum* $\mathbf{F}$ *vera eitthvert svið og látum* $g : \mathbf{F}^m \longrightarrow \mathbf{F}$ *vera margvíða margliðu af heildarstigi (e. total degree) í mesta lagi d sem er ekki alstaðar núll. Þá gildir á sérhverju endanlegu mengi* $S \subset \mathbf{F}$*:*

$$P_{x \in_R S^m}[g(x) = 0] \leq d/|S| \tag{1}$$

Þ.e. ef x er valið af handahófi (táknað $\in_R$*) úr* S^m *þá eru líkurnar á að g(x) = 0 í mesta lagi* $d/|S|$*. Ennfremur gildir að fyrir sérhverjar tvær mismunandi margliður af stigi í mesta lagi d að þær taka sama gildi í mesta lagi* $d/|S|$ *hlutfalli af punktum úr* S^m

Sönnun: Við sönnum lemmuna með þrepun. Ef m=1 (þ.e. margliðan er einvíð) þá fáum við skv deilingarreikniritinu (eða skv. grundvallar reglu algebrunnar) að g hefur í mesta lagi d rætur í $\mathbf{F}$ og því er ójafnan rétt fyrir m=1.

Gerum ráð fyrir að ójafnan er gild fyrir m-1 breytur. Skrifum g:

$$g(x_1, ..., x_m) = x_1^k c_k(x_2, ..., x_m) + x_1^{k-1} c_{k-1}(x_2, ..., x_m) + ... + c_0(x_2, ..., x_m)$$

þ.e. sem margliðu í x_1 þar sem við gerum ráð fyrir að $c_k(x_2, ..., x_m)$ er margliða sem er ekki alstaðar 0. Nú skv þrepunarforsendu vitum við að:

$$P_{x \in_R S^{m-1}}[c_k(x) = 0] \leq (d - k)/|S|$$

Látum $(r_1, r_2, ..., r_m) = x \in_R S^m$. Nú ef $c_k(r_2, ..., r_m) \neq 0$ þá er $g(x_1, r_2, ..., r_m)$ ekki alstaðar 0. Við vitum aukalega, þar sem $g(x_1, r_2, ..., r_m)$ er einvíð margliða af stigi, að:

$$P_{x_1 \in_R S}[g(x_1, r_2, ..., r_m) = 0] \leq k/|S|$$

Þá gildir ef $g(r_1, r_2, ..., r_m) = 0$ að annaðhvort er $c_k(r_2, ..., r_m) = 0$ eða einvíða margliðan $g(x_1, r_2, ..., r_m)$ er núll þegar $x_1 = r_1$. Fyrri möguleikinn hefur líkurnar $\leq (d-k)/|S|$ og sá seinni hefur líkurnar $\leq p \cdot k/|S|$ þar sem p<1 eru líkurnar á því að $c_k(r_2, ..., r_m) \neq 0$. Við fáum því:

$$P_{x\in_R S^m}[g(x)=0] \leq (d-k)/|S| + p\cdot k/|S| \leq (d-k)/|S| + k/|S| = d/|S|$$

□

Með þessari hjálparsetningu getum við sýnt að Summu athugun er gagnvirk sönnun.

Fullkomleiki

Athugum að ef $\mathcal{P}$ er sannsögull þá mun samskiptareglan leiða til þess að $\mathcal{V}$ samþykkir staðhæfinguna með líkunum 1.

Lögmæti

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

Notum þrepum. 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

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

Skv. 2.5. þ.a. líkurnar á að $\mathcal{V}$ hafni staðhæfingu $\mathcal{P}$ eru $1 - d/|\mathbf{F}| < 1$.

Nú ef g er v-1 víð margliða gerum við ráð fyrir að líkurnar á að $\mathcal{V}$ hafni falskri staðhæfingu $C_1 = H$ séu að minnsta kosti $1 - d(v-1)/|\mathbf{F}|$.

Látum nú

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

Og að $\mathcal{P}$ sendir og margliðu $g_1 \neq s_1$ í fyrstu lotu samskiptareglunnar. Nú eins og áður eru líkurnar á að $g_1(r_1) = s_1(r_1)$ fyrir handahófskennt r_1 í mesta lagi $d/|\mathbf{F}|$. Nú með skilyrtum atburði $g_1(r_1) \neq s_1(r_1)$ þá þarf $\mathcal{P}$ að reyna sanna að $g_1(r_1) = \sum_{b_2\in\{0,1\}} \sum_{b_3\in\{0,1\}} \cdots \sum_{b_v\in\{0,1\}} g(r_1, b_2, \ldots, b_v)$, og þar sem $g(r_1, b_2, \ldots, b_v)$ 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 $1-d(v-1)/|\mathbf{F}|$ skv þrepunarforsendu. Sem veldur að $\mathcal{V}$ mun ekki hafna rangri staðhæfingu $C_1 = H$ eru

$$P_{r_1 \in_R \mathbf{F}}[s_1(r_1) = g_1(r_1)] + \sum_{i=2}^{v} P_{r_i \in_R \mathbf{F}}[s_i(r_i) = g_i(r_i)]$$

$$= P_{r_1 \in_R \mathbf{F}}[s_1(r_1) = g_1(r_1)] + P[\mathcal{V} \text{ hafnar staðhæfingu } \mathcal{P} \text{ í einhverri lotu } 1 < j \leq v]$$

$$\leq d/|\mathbf{F}| + d(v-1)/|\mathbf{F}| = dv/|\mathbf{F}|$$

þ.e. höfum lögmætisvillu upp á $dv/|\mathbf{F}|$ svo á meðan $d, v << \mathbf{F}$ þá er lögmæti uppfyllt.

Útfrá þessu sjáum við að Summu Athugun er gagnvirk sönnun því hún uppfyllir bæði fullkomleika með líkum 1 og lögmæti með líkum $1 - dv/|\mathbf{F}|$.

2.2 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 $\mathbf{F}^v$]) 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 $\mathbf{F}^v$]) sem er auðvitað alltof tímafrekt til notkunar í raunheimum, fyrir flest vandamál. Hinsvegar er summu athugun gott verkfæri til að sýna að tiltekin vandamál hafi Gagnvirkar Sannanir, því oft er hægt að minnka (e. reduce) vandamál niður í að reikna svona margliðusummu, vandamál eins og að telja þríhyrninga í neti, margföldun fylkja og útreikningur á reiknings-tré/rás (Arithmetic circuit) geta öll verið minnkuð niður í að meta gildi á margliðusummu og því eru til Gagnvirkar sannanir fyrir þau öll.

3 Gagnvirk Sönnun án upplýsinga

Sönnun án upplýsinga er gagnvirk sönnun sem sannar fyrir sannprófaranum $\mathcal{V}$ að $\mathcal{P}$ veit svar við ákveðnu vandamáli án þess að gefa upp hvert svarið er og þannig að eftir sönnunina hefur sannprófarinn ekki öðlast neinar frekari upplýsingar sem geta verið nýttar til að finna svarið fljótar en ella.

Við skilgreinum þess konar sannanir

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.

Við höfum þrengri skilgreiningu á sönnun án upplýsinga sem við getum nýtt til að sanna að samskiptareglur skoðaðar seinna eru án upplýsinga. Fyrst þurfum við skilgreiningu á handriti sannana.

Skilgreining 3.2. Við köllum raðaða listann 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 handrit sem verða til við samskipti $\mathcal{P}$ og $\mathcal{V}$ á inntaki x fyrir ákveðna samskiptareglu.

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 S' (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. $S'(x)$.

Þessi skilgreining er vel óljós við fyrstu yfirferð. 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 tökum við smá umræðu um þá.

3.1 Hermar

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 lausn eða ekki, græðir $\mathcal{V}$ ekkert á því að keyra samskiptaregluna því hann gæti allt eins keyrt herminn og fengið jafn mikið af upplýsingum þaðan.

Skilgreining 3.4. Fall sem býr til fölsk handrit (án samskipta við sannara) sem eru óaðskiljanleg (fallið hefur sömu dreifingu) og handrit af gildri sönnun milli sannsöguls sannara og einhvers sannprófara köllum við *Hermir*.

Skoðum skilgreininguna á hermi í samhengi með Litblinda vininn í inngangi-num. Er sú sönnun, sönnun án upplýsinga? Það virðist vera því athugum að einu upplýsingarnar sem Ari hefur í lok sönnunarinnar er að boltarnir eru mismunandi á litinn, hann til dæmis veit ekki hvor þeirra er rauður og hvor er grænn sem gerði Emblu kleift að velja græna boltann án þess að Ari kemst að því. En í sambandi við skilgreininguna, hvernig getum við notað hana til að sýna fram á að litblindi vinurinn er sönnun án upplýsinga?

Látum r vera slembibreytu þ.a.

$$P(r = \text{ "Ari setur fram sama bolta og í síðustu umferð)}$$
$$= P(r = \text{ "Ari setur fram annan boltann frá því í síðustu umferð)} = 0.5$$

og skilgreinum S' þ.a. $S'(\text{ "Ari setur fram sama bolta og í síðustu umferð)} = 1$ og $S'(\text{ "Ari setur fram annan boltann frá því í síðustu umferð)} = 0$. Hér er-um 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 Embla án þess að fá upplýsingar frá Emblu, eingöngu með því að nota upplýsingar sem Ari hefur. Og þetta fall mun alltaf sannfæra Ara um að fallið sjái mun á boltunum, eins og Embla gerir. Því er fallið gildur hermir.

Þessi hermir, S', 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 sannar þá samkvæmt skilgreiningunni er litblindi vinurinn sam-skiptaregla án upplýsinga.

Við getum einnig litið á hermi sem upptöku af leiknum milli Emblu og Ara. Upptakan sjálf ætti ekki að sannfæra neinn litblindan einstakling sem horfir á hana að boltarnir sé 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.

Með skilgreiningunni á Hermum getum við einfalda skilgreininguna á sönnun án upplýsinga, 3.3

Skilgreining 3.5. *Sönnun án upplýsinga* er gagnvirk sönnun þar sem til er hermir.

3.2 Strjáll Logri

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

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:

$$g^x = v \ (\bmod p)$$

Nú, þegar maður veit ekki töluna x en veit v og g þá er það talið vera erfitt að finna x. Þ.e. svipað erfitt og að ítra sig í gegnum allar mögulegar tölur mod p. Við getum nýtt okkur það í eftirfarandi samskiptareglu:

Samskiptaregla strjála lograns

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, reiknar $h = g^r (\bmod p)$ 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 $a = r + bx (\bmod p)$ og sendir á $\mathcal{V}$
4. $\mathcal{V}$ athugar hvort $g^a = hv^b (\bmod p)$, 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 séð af þessari samskiptareglu, Summu athugun og reglunni fyrir litblinda vininn, að slembileiki veldur að sannprófari getur treyst staðhæfingu sannarans ef hann nær að svara spurningum samskiptareglanna.

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 planað hver svör hans verða og með góðum árangri náð að blekkja sannprófarann. Við sjáum það í dæminu hjá Ara og Emblu, ef Embla vissi alltaf hvort Ari skiptir um bolta eða ekki (t.d. ef hún er með myndavél undir borðinu) þá gæti 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 viti x þótt hann viti það ekki.

Strategían hans væri þá eftirfarandi. Gerum ráð fyrir að $\mathcal{P}$ viti ekki lausnina x á strjála logranum. Þá 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 skref 4 að $\mathcal{V}$ athugar jöfnuna mun hann samþykkja svör $\mathcal{P}$.

Og ef $\mathcal{P}$ veit að b=1, í skrefir 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 samþykkja svar $\mathcal{P}$ og staðhæfinguna að hann veit x, þótt hann viti það ekki.

Við sjáum því að sannprófarinn ekkert gruna 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 $\mathcal{V}$ h-ið í skrefi 1.

Samskiptareglan virkar hinsvegar því sannprófarinn velur FYRST r og reiknar $h = g^r (\bmod p)$ og sendir til $\mathcal{V}$. Hann 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 uppfyllir 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 en fullkomleikinn. Gerum ráð fyrir að $\mathcal{P}$ viti ekki gildið x sem hann segist vita. Nú getur tvennt gerst:

$\mathcal{V}$ sendir b = 0 í skrefi 2

Nú þar sem b=0 þá vitum við að $\mathcal{V}$, í skrefi 4, mun athuga hvort $g^a = h (\bmod p)$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda $(h, a) => g^a = h (\bmod p)$, þ.e. 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. Sem ef hann veit það ekki núþegar (þ.e. ef hann fylgir ekki samskiptareglunni) þá er það jafnerfitt að leysa og að finna sjálft x-ið sem hann

veit ekki.

$\mathcal{V}$ sendir b = 1 í skrefi 2

Nú í skrefi 4 mun $\mathcal{V}$ athuga hvort $g^a = hv(\mod p)$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda $(h, a) => g^a = hv(\mod p)$ 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. Athugum að 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 $\mathcal{P}$. 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 hönd getum við séð tvær niðurstöður á strategíu $\mathcal{P}$ sem veit ekki lausnina x við strjála logranum:

$\mathcal{P}$ 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 $g^a = hv(\mod p)$, 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 talinn MJÖG erfið að finna þá er það besta sem $\mathcal{P}$ getur gert er að giska á lausn. Og ef við gerum ráð fyrir því að p sé mjög stór tala þá gildir að fjöldi heiltala a < p þ.a. $g^a = hv(\mod p)$ er fasti c « p. Við fáum því að líkurnar á að $\mathcal{P}$ nái að plata $\mathcal{V}$ eru:

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

$\mathcal{P}$ fylgir ekki skrefi 1 og sendir h til $\mathcal{V}$ sem hann veit ekki lausn r á $h = g^r(\mod p)$

Í þessu tilviki er $\mathcal{P}$ aðeins í vondum málum ef $\mathcal{V}$ velur $b = 0$ í skrefi 2, því ef b=0 þá 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. Þ.e. $\mathcal{P}$ getur í lotu 1 sent $h = g^s v^{-1}(\mod p)$ 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 $\mathcal{V}$:

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

Og samþykkir það svar og dregur þá ályktun að $\mathcal{P}$ hlítur 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:

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

Smá útskýring á mikilvægi slembibreytunnar b í samskiptareglunni hér að ofan:

Athugum 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 raunverlu viti þessar ákveðnu upplýsingar (t.d. x í strjála logranum, litirnir á boltunum í litblinda vininum) með því að setja 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 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. Eins ef b=1, þá er það jafngilt því að $\mathcal{V}$ biður $\mathcal{P}$ að leysa strjála logrann af v (þ.e. að $\mathcal{P}$ viti lausnina x).

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 viti x-ið þótt hann viti það 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 einhvert sannprófara-algrím, sem er ekki endilega sannsögult, með slembileika r. Við ætlum að útbúa hermi H' þ.a. fyrir sérhverja staðhæfingu x gildir að eftirfarandi slembibreytur

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

hafa sömu dreifingu.
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 $b' \neq b$ fer 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 "samaǫg 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 í jöfnum mæli (e. uniformly random) og því með sömu dreifingu og r-ið valið af $\mathcal{P}$ 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. Og því 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, 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 mun vera sú sama fyrir bæði H' og $\mathcal{P}$, og ennfremur mun dreifingin á handritunum vera sú sama. Hermirinn okkar er því gildur-hermir sem keyrir í slembi-margliðutíma (því líkurnar á að b='b eru 0.5 mun hermirinn á endanum komast í loka skrefið og enda 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 raunheima 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 dæmi um Σ-samskiptareglu. (Heimild? Ábending um meiri upplýsingar? Sleppa?)

3.3 Þrílitað net

Þrílitun nets er vandamál í netafræði. Gefið er net G = (V,E) og spurningin er, er hægt að lita sérhvern hnút v með einum lit af þremur, setjum $c \in$ {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), þ.e. mengi þeirra 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 vill sannfæra Emil um að hún veit um þrílitun, {rauður, grænn, blár}, á tilteknu neti G = (V,E).

Skilgreining 3.7. Samskiptaregla fyrir þrílitun nets
Sérhver lota samskiptareglunnar fer á eftirfarandi veg:

1. Agnes umraðar litunum {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 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). Sem þýðir að minnsta kosti að einn leggur $e \in E$ tengir hnúta sem eru eins litaðir. Þ.a. líkurnar að hún nái EKKI að plata Emil eru að minnsta kosti $\frac{1}{|E|} > 0$. Þ.e. lögmætis-villan er í mesta lagi $1 - \frac{1}{|E|} < 1$ fyrir hverja lotu.

Við höfum því að það er ALLS ekki nóg að leika aðeins 1 lotu til að sannfæra Emil með þessari samskiptareglu. Athugum að $(1 - \frac{1}{n})^n \xrightarrow{n \longrightarrow \infty} e^{-1} \approx 0.37$ þ.a. 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 óheiðarelgur 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 þau tilvik þegar lögmætisvillan er svona há. (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 heimild .... How to prove a theorem so no one else can claim it)).

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 sönnunin án upplýsinga.

3.4 Smá flækjufræði

Skilgreining 3.8. P er flokkur af ákvörðunar-vandamálum sem eru leysanleg með algrími sem keyrir í margliðutíma

Skilgreining 3.9. NP er flokkur af ákvörðunar-vandamálum sem eru leysanleg með brigðgengnu (non-deterministic) algrími sem keyrir í margliðutíma.

Þar sem 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 þegar algrímið keyrir á ákveðnu inntaki algrímið velur alltaf "rétta" aðgerð þá finnur algrímið lausn í margliðutíma.

Dæmi: Ef vandamálið er að ákvarða hvort að tala N sé *ekki* prímtala þá er 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) að leysa það vandamál 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 $x \in NP - fullkomi$ 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 fyrst yfir í vandamál x og síðan leysa það vandamál. Þetta er hið fræga P=NP vandamál. Almennt er talið að $P \neq NP$, en maður má láta sig dreyma.

Nú þar sem þrílitun nets er NP-fullkomið vandamál (HEIMILD!) fáum við þá niðurstöðu að $NP \subseteq ZKP$

Þ.e. öll vandamál í NP hafa sönnun án upplýsinga.

4 ZKP án Gagnvirkni

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, þ.e. gagnvirkni.

Það hefur sína ókosti eins og t.d. að sannarinn þarf að sanna staðhæfinguna sína að nýju fyrir sérhvern nýjan einstakling. Gott væri ef sannarinn gæti birt sönnun sína fyrir öllum og sannprófarar farið yfir sönnunina án þess að þurfa eiga í óþarfa samskiptum við sannarann.

Svo við viljum einhvernveginn losna við samskiptin við sannprófarann 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 óþekkt algrím sem tekur við inntaki og gefur úttak til baka. Handahófskennd-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.

Munum:
Samskiptaregla Strjála lograns

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, reiknar $h = g^r (\bmod p)$ 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 $a = r + bx (\bmod p)$ og sendir á $\mathcal{V}$
4. $\mathcal{V}$ athugar hvort $g^a = hv^b (\bmod p)$, 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 athugum að mikilvægið sem $\mathcal{V}$ kemur með í sönnunina er slembileikinn þar sem $b \in \{0, 1\}$ er valið af handahófi. 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 $\mathcal{P}$ að velja b-ið af handahófi, en þar sem við viljum ekki þurfa að treysta $\mathcal{P}$ þá gengur þessi lausn ekki.

Önnur, ógáfuleg, pæling væri að nota véfrétt þ.a. $\mathcal{P}$ sendir h úr skrefi 1 á véfréttina, $\mathcal{O}$, og véfréttin gefur handahófskennt tilbaka svar $\{0, 1\}$ (en samt sama svar ef $\mathcal{P}$ sendir sama h-ið aftur). Þessi hugmynd er ekki góð því $\mathcal{P}$ getur, áður en hann býr til sönnunina, fundið mismunandi $h = g^r (\mod p)$ sem gefa 0 og mismunandi $h = g^r v^{-1} (\mod p)$ 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 þurfum því að breyta samskiptareglunni örlítið, því við viljum nota Handahófskennda-véfrétt. Þá getum við notað svipaða hugsun og að ofan.

4.1 Fiat-Shamir Ummyndun

(ATH. eftirfarandi er veika útgáfan af Fiat-Shamir, sjá page 6 í main og wikiped heimild 8)

Við sáum í kafla 2 að gagnvirkar sannanir styðja sig heilmikið við möguleika sannprófara á að koma sannara á óvart / styðja sig við að í augum sannarans líta viðbrögð sannprófarans við svörum sannarans út eins og slembibreytur. Pælingin í Fiat-Shamir er að nýta sér það og skipta slembileika sannprófarans út fyrir slembileika þriðja aðila 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 $h = g^r (\mod p)$ 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 $a = r + bx (\mod p)$ 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. 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 $h = g^r (\mod p)$.

2. $\mathcal{P}$ sendir h á handahófskenndu-véfréttina $\mathcal{O}$ og fær tilbaka $0 \leq b < p$.

3. $\mathcal{P}$ reiknar $a = r + bx (\mod p)$ 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 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 $b \neq \mathcal{O}(h)$ þá hafnað 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.

Við sjáum að lykillinn bakvið þessa sönnun er að láta töluna sem véfréttin skilar vera háða svörum $\mathcal{P}$, og að svör véfréttarinnar eru handahófskennd og mismunandi fyrir mismunandi inntök.

Fiat-Shamir ummyndunin er því in general sú að hafa handahófskenndavéfrétt, 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 h í skrefi 1 í strjála logranum).

Þetta svipar til Bálkakeðju-líkansins 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.

Listi yfir heimildir er geymdur í skránni `bibtex.bib`. Auðveldasta leiðin til að bæta í hana er að finna heimildina á `http://ams.org/mathscinet`. Smella á *Select alternative format*, velja *Bibtex* og líma textann sem birtist í skrána.

Frekari leiðbeining um LaTeXmá finna í *The Not So Short Introduction to LaTeX*, `https://tobi.oetiker.ch/lshort/lshort.pdf`, og á `https://en.wikibooks.org/wiki/LaTeX`.

Heimildir