Sönnun án upplýsinga

Þórður Ágústsson

11. apríl 2021

Útdráttur

Ágrip hér

1 Gagnvirkar Sannanir (e. Interactive Proofs)

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

Eins og drepið var á í inngangínum 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 **??**), þrílitun á neti (kafli **??**), 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 1.1. *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 1.1, 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 1.1 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 sannan-

anna. 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 innganginum 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 1.2. *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 1.3. 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 1.1.

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 1.4. *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. **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 (**??**) 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 1.1 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 1.1 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.

1.1 Summu athugun

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

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 1.5. 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 $1 - dv/|\mathbb{F}|$.

1.1.1 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.

1.2 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 [**?**] eða kafla 2.2 í [**?**]) 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 [**?**].