Sönnun án upplýsinga

Þórður Ágústsson

14. mars 2021

Útdráttur

Ágrip hér

1 Gagnvirkar Sannanir (e. Interactive Proofs)

Eins og drepið var á í inngangi 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 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 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 1.2. 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 1.3. 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. $P[A = "SamiboltiogArisndisustuumfer"] = P[A = Ekki Samiboltiog Arisndisustuumfer"] = 0.5$. 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 1.3.

Snúum okkur nú að setningunni '*Gagnvirk sönnun* er samskiptaregla sem fullnægir eftirfarandi eiginleikum með "miklum líkum" í skilgreiningu 1.1.

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 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.

1.1 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 1.5. (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. 1.5. 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 $1 - dv/|\mathbf{F}|$.

1.2 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.