# 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 byggður á rökum sem hægt er að leiða frá þekktum staðhæfingum.

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 $\sqrt{2}errtmargliunnar$f(x) $= x^2 - 2$. Sem er ekki regla á borð við pýþagórasarregluna, heldur fremur einhverskonar staðhæfing að rót margliðunnar er þekkt.

Munurinn er semsagt þessi, grundvallarregla algebrunnar segir að sérhver margliða af stigi d hefur d-rætur. Þetta er regla sem þarfnast almennrar sannanar um réttmæti hennar. Staðhæfingin "$\sqrt{2}errtmargliunnar$f(x) $= x^2 - 2$ęr hinsvegar ekki beint regla, helur fremur staðhæfing...

Sannanirnar sem við skoðum í þessari ritgerð eru tól sem einstaklingar geta notað til að sanna þekkingu fyrir hvor öðrum, í þeim skilningi að annar veit svar við vandamáli og vill sanna svarið fyrir öðrum án þess að hinn þurfi að leysa vandamálið sjálfur.

Tökum dæmi.

**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,Ęmbla tekur annan boltann ǫg 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."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?

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 Ęr 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. Ég er svo hrifinn af grasi, 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. Ękki málið Ari minn. Ég held þá þeim rauða fyrir mig", segir Embla og tekur við græna boltanum og stingur í vasann sinn.

## 2 Gagnvirkar Sannanir (e. Interactive Proofs)

Eins og drepið var á í inngangínum fjalla sannanir þessarar ritgerðar um að sanna lausn á skilgreindu vandamáli. Í enn þrengri skilningi höfum við tvo einstaklinga þar sem annar vill sannfæra hinn að hann viti lausn á fyrirframskilgreindu vandamáli, sem getur t.d. verið lausn á Flakkandi Sölumannsvandamáli eða 3-litun á neti. Almennt gerum við ráð fyrir því að það sé erfitt/tímafrekt að reikna lausnina sjálfur en með því að eiga samskipti við þann sem kveðst vita lausn getum við á einfaldari máta sannað að þetta sé lausn heldur en að reikna það sjálf.

Eftirfarandi er skilgreining á Gagnvirkri Sönnun:

**Skilgreining 2.1.** *Gagnvirk sönnun* er samskiptaregla sem fullnægir eftirfarandi eiginleikum með "miklum líkum":

1. *Fullkomleiki* (e. completeness) ef 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*, $\mathcal{V}$) þar sem sannprófarinn er algrím sem keyrir í **versta** falli í líkindafræðilegum margliðu-tíma (e. probabilistic polynomial time) til að taka afstöðu gagnvart staðhæfingu sem sannarinn heldur fram.

Athugum að settar eru hömlur á hvers kynns algrím sannprófarinn getur verið, þ.e. hversu lengi hann má í versta falli keyra, en engar hömlur settar á sannarann.

Svo t.d. ef sannarinn þarf að keyra/framkvæma útreikninga sem eru $\mathrm{O}(2^n) fyririnntak(st$
$tma$.

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

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

**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 $r_0$ upphafs-realisation á r 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. Algengast er að líta á

$(\mathcal{P}, \mathcal{V}, x, r_0) = 0$ sem höfnun $\mathcal{V}$ á staðhæfingu, x, $\mathcal{P}$. Og eins á $(\mathcal{P}, \mathcal{V}, x, r_0) = 1$ sem samþykki $\mathcal{V}$ á staðhæfingu, x, $\mathcal{P}$

Innri slembileiki, þar sem Gagnvirk sönnun byggir á röð spurninga og svara á milli sannara og sannprófara er innbyggt í sannprófarana slembistærð r. Því í hverri umferð samskiptareglunnar þá getur sannprófarinn ákveðið hver næsta spurning skal vera. T.d. 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. Þar með getum við lýst Ara sem slembibreytu X þ.a. $P[A =$ "$SamiboltiogArisndisustuumfer$"$] = P[A =$ "$\c{E}kkiSamiboltiogArisndisustuumfer$"$] =$ 0.5. En ef við festum A sem "Sami bolti og Ari sýndi í síðustu umferð"þá erum við ekki lengur með slembiferli (?) heldur er umferðin orðin determinísk 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 sönnun 2.1. Þar eigum við eingöngu við að sannprófari getur verið eins viss og hann vill/krefst að sönnun sé rétt ef hann ítrar samskiptaregluna nógu oft. Skoðum eftirfarandi skilgreiningu:

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

1. *fullkomleiki.* 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 $\delta_f, \delta_l \leq 1/2$.

Athgum að í skilgreiningunni hér að ofan er gildið $\delta_f, \delta_l \leq 1/2$ valið af handahófi. Aukalega þá er fullkomleika-villan í öllum sönnunum sem við skoðum 0.

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 Embla þurfa 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 0.5*0.5 = 0.25 þ.e. Ari getur verið 75% viss um að Embla sé að segja satt, og ef hann framkvæmir 10 umferðir þá getur hann verið $1 - (0.5)^{10}$ þ.e. uþb. 99.9% viss.

## 2.1 Summu athugun

Dæmi um gagnvirka sönnun er summu-athugunar samskiptareglan. Sú reglan er oft notuð til að sýna fram á að til sé gagnvirk sönnun á einhverju ákveðnu vandamáli. Samskiptareglan 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 $\mathbf{F}$.

Síðan höfum við $\mathcal{P}$, sannara, sem segist vita gildið H á summunni fyrir gefna v-víða margliðu. Summu athugun snýst þá um hvernig sannarinn getur sannað fyrir sannprófara að H sé rétt gildi summunnar.

Einföld sönnun á þessari staðhæfingu $\mathcal{P}$ væri auðvitað að reikna bara 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 $O(2^v)$ aðgerðir. Svo ef $v \geq 100$ mun útreikningurinn taka of langan tíma til að sannprófa. Því snúum við okkur að summu athugun.

Til að finna lausn á þessu vandamáli minnkum það niður í einfaldara mál. Gerum ráð fyrir að v=3. Þá er:

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

$\mathcal{P}$ sendir stærðina H á $\mathcal{V}$. Athugum að nú tekur það $\mathcal{V}$ amk $2^3 = 8$ aðgerðir til að athuga hvort H sé rétt stærð, ef $\mathcal{V}$ einfaldlega reiknar summuna. Hinsvegar ef $\mathcal{P}$ sendir ekki bara H heldur einnig 1-víðu margliðuna:

$$g_1(X_1) := \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} g(X_1, b_2, b_3)$$

Þá getur $\mathcal{V}$ athugað $g_1(0) + g_1(1) = H$, athugum að ef $\mathcal{P}$ er sannsögull þá mun þetta vera jafngilt. En það er ekki nóg til að $\mathcal{V}$ getur verið viss um að H sé rétt, því $\mathcal{P}$ getur verið að reyna að plata $\mathcal{V}$ og gæti því sent ranga margliðu $g_1$ sem passar við H-ið sem hann er að reyna sannfæra $\mathcal{V}$ um að sé rétt H. Táknum með $s_1$ þá margliðu sem $\mathcal{P}$ sendir ef hann er sannsögull.

Því auðvitað eru til aðrar margliður $g_1 \neq s_1$ en samt þ.a. $s_1(0) + s_1(1) = g_1(0) + g_1(1)$. Svo við getum ekki 100% treyst því að $g_1$ sé rétt, en það að $g_1(0) + g_1(1) = H$ geta verið rök in favor of treysta $\mathcal{P}$, og til að breyta þeim í sterkari rök er gert á eftirfarandi máta.

Við veljum $r_1 \in \mathbf{F}$ af handahófi og sendum á $\mathcal{P}$ og biðjum hann að senda okkur til baka aðra margliðu:

$$g_2(X_2) := \sum_{b_3 \in \{0,1\}} g(r_1, X_2, b_3)$$

Við getum þá athugað hvort $g_1(r_1) = g_2(0) + g_2(1)$ og þetta eru sterkari rök heldur en að $g_1(0) + g_1(1) = H$ því $\mathcal{P}$ vissi ekki fyrirfram hvaða tölu $r_1$ hann fengi senda frá $\mathcal{V}$. Það að velja af handahófi $r_1$ og senda á $\mathcal{P}$ *eftir* að $\mathcal{P}$ sendir á $\mathcal{V}$ $g_1$ veldur því að hann getur ekki sent hvaða $g_1$ sem er nema hann viti um $g_2$ þ.a. $g_2(0) + g_2(1) = g_1(r_1)$.

Athugum að ef $g_1 \neq s_1$ þá eru í mesta falli til d stök $x \in \mathbf{F}$ þar sem $g_1(x) = s_1(x)$

$G(x) =$

Athugum nú að ef $\mathcal{P}$, í staðinn fyrir að reikna H myndi reikna:

$$H_1 := \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(b_1, b_2, \ldots, b_v)$$

Og senda til $\mathcal{V}$ $H_1$ og margliðuna:

$$H_1 := \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} \cdots \sum_{b_v \in \{0,1\}} g(b_1, b_2, \ldots, b_v)$$

Reglan fer á þennan veg:

$\mathcal{P}$ sendir H og

**Skilgreining 2.5.** Skilgreining á summu athugunar samskiptareglu.

Sýna fram á að Summu Athugun sé gagnvirk sönnun.

## 2.2 Preliminaries

(Schwartz Zippel Lemma)

**Hjálparsetning 2.6.** *Látum* $\mathbf{F}$ *vera eitthvert svið og látum* $g :\longrightarrow \mathbf{F}^m \longrightarrow \mathbf{F}$ *vera margliðu af stigi í mesta lagi* $d$ *sem er ekki alstaðar núll. Þá gildir á sérhverju endanlegu mengi* $S \subset \mathbf{F}$*:*

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

*Þ.e. ef* $x$ *er valið af handahófi 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* $S^m$

**Skilgreining 2.7.** Fjölbreytu-margliða g er marglínuleg ef stig margliðunnar í sérhverri breytu er í mesta lagi 1.

**Hjálparsetning 2.8.** *Sérhvert fall* $f : \{0,1\}^v \longrightarrow \mathbf{F}$ *hefur eina og aðeins eina marglínulega útvíkkun yfir* $\mathbf{F}$*, hér eftir notum við* $\tilde{f}$ *fyrir þessa útvíkkun.*

### 2.2.1 Telja þríhyrninga í neti

Hvernig við getum notað summu athugun til að telja þríhyrninga í neti, með hjálp sannara sem veit fjölda þríhyrninga í netinu.

### 2.2.2 Algrím Freivalds og Fylkjamargföldun

...

# 3 Sönnun án upplýsinga

Byrjum á skilgreiningunni.

**Skilgreining 3.1.** *Sönnun án upplýsinga* er gagnvirk sönnun sem hefur eftirfarandi eiginleika:

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

Meira abstract / strangari skilgreining:

**Skilgreining 3.2.** Við segjum að $(\mathcal{P}, \mathcal{V})$ sé sönnun án upplýsinga ef fyrir sérhvern margliðu-tíma sannprófara-algrím $V'$ þá er til líkindafræðilegt margliðutíma algrím $S'$ (kallað hermir, e. simulator) þannig að fyrir sérhverja sanna staðhæfingu ($x \in \mathcal{L}$) gildir að eftirfarandi slembistærðir hafa sömu dreifingu:

1. Úttakið $(\mathcal{P}, \mathcal{V}, x, r) \in \{0, 1\}$, þar sem r er slembistærð,
2. Úttakið $S'(x) \in \{0, 1\}$.

Þessi skilgreining er vel óljós þegar hún er lesin í fyrsta sinn. 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 er ekki sannsögull.

Skoðum nú skilgreininguna í samhengi með Litblinda vininn dæmið í innganginum. 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. 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. $P(r = "Arisetur framsamaboltaogsustuumfer") = 0.5$ og $P(r = "Arisetur framhinnboltannfrvsustuumfer") = 0.5$ og skilgreinum $S'$ þ.a. $S'("Arisetur framsamaboltaogsustuumfer") = 1$ og $S'("Arisetur framhin$ 0. Hér erum við að túlka 1 sem játun við spurningu Ara Ęr þetta sami bolti og ég sýndi þér í síðustu umferðǫg 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.

Þetta fall svipar til þess að Ari leikur samskiptaregluna við sjálfan sig. Þar sem leikurinn fer fram á sama veg og ef hann léki leikinn við Emblu (sem gefið er að er sannsögul) þá samkvæmt skilgreiningunni er litblindi vinurinn samskiptareglan gagnvirk sönnun án upplýsinga.

## 3.1 Strjáll Logri

Í dulritun er vandamálið með strjála lograns oft notað í hinum ýmsu samskiptareglum. Það grundvallast á því að lausn á vandamálinu er talið erfitt að leysa. Skilgreinum:

**Skilgreining 3.3.** 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, og reglunni fyrir litblinda vininn, að þáttaka slembileika er það sem gerir okkur kleift að treysta á niðurstöðu þessara regla. Slembileikinn gerir okkur kleift að grípa sannarann í lygi ef hann er ekki að segja satt. Ef sannarinn vissi fyrirfram hvaða gildi sannprófarinn mun senda á hann þá mun hann geta planað fyrirfram hvað hann mun gera. Eins og 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 svindlað.

Eins með strjála logrann. 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. En ef hann veit að b=1 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 því mun sannprófarinn ekkert gruna EF sannarinn veit fyrirfram hvort sannprófarinn velur $b = 0$ eða $b = 1$.

En samskiptareglan virkar því sannprófarinn velur FYRST $r$ og reiknar $h = g^r (\bmod p)$ og sendir til $\mathcal{V}$ og því getur hann ekki verið svona sniðugur, því hann veit ekki hvort sannprófarinn mun velja $b = 0$ (þ.e. velja að biðja $\mathcal{P}$ um að senda sér töluna r sem hann valdi í skrefi 1) eða $b = 1$ (þ.e. velja að biðja $\mathcal{P}$ um að senda sér a sem mun sannfæra $\mathcal{V}$ að $\mathcal{P}$ viti lausn á strjála logranum).

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 $g^a = g^{r+bx} = g^r g^{bx} = hv^b$ og þ.a. fullkomleikavillan er 0. þ.e. $P((\mathcal{P}, \mathcal{V}, x, b) = 1) = 1$.

**Lögmæti**

Gerum nú 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 mun $\mathcal{V}$ í skrefi 4 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. lausn 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 hann auðvitað gerir ef hann fylgir samskiptareglunni.

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

Nú í skrefi 4 mun $\mathcal{V}$ athuga hvort $g^a = hv (\bmod p)$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda $(h, a) => g^a = hv (\bmod p)$ sem þýðir að $\mathcal{P}$ veit lausn, a, á strjála logranum af hv. Athugum að hér getur lyginn $\mathcal{P}$ 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 $\mathcal{P}$.

Með þessar upplýsingar í hönd getum við séð tvær niðurstöður:

**$\mathcal{P}$ 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 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 $g^a = hv(\ \mathrm{mod} p)$ sem krefst þess af okkur að senda til baka lausn a á stjrála logarithmanum af hv. En þar sem $\mathcal{P}$ veit aðeins lausnina r fyrir strjála logarithmann 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. Þ.e. 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. $g^a = hv(\ \mathrm{mod}\ p)$ er c « p. Við fáum því að líkurnar á að $\mathcal{P}$ nái að plata $\mathcal{V}$ er:

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

**$\mathcal{P}$ fylgir ekki skrefi 1 og velur því r þar sem hann hann veit ekki**

## 3.2 Sigma Samskiptareglur

**Skilgreining 3.4.** Skilgreina Sigma Samskiptareglur

### 3.2.1 Strjáll logri - Samskiptaregla

**Skilgreining 3.5.** Skilgreina Samskiptaregluna

### 3.3 Notagildi

Fjárhagsreglugerðir / Kjarnorku-afvopnun / Rafmyntir etc.

Eitthvað um Interactive Proofs, byrjunina á þeim og hvernig Zero-Knowledge sannanir eru tengdar Interactive Proofs.

Dæmi um Zero-Knowledge "sönnun", þ.e. Ali Baba, Krukkurnar, Spilastokkurinn, Litblindi Vinurinn, Erum við í sama skattþrepi etc.

Smá um að Zero-knowledge proofs eru eitthvað aðeins annað heldur en týpískar stærðfræðilegar sannanir, þær eru helst notaðar til að sanna staðreyndir sem er erfitt að sanna en hafa mögulega ekkert dýpra gildi heldur en þær eru sannar. Ekki eins og Grundvallar Lögmál Algebrunnar, sem hefur eitthvað meira að segja heldur en þær staðreyndir sem eru sannaðar með Interactívum sönnunum.

Í raun eru interactive sannanir ekki tól til að sanna eitthvað óþekkt heldur fremur tól sem Sannari ("prover") getur notað til að sanna fyrir Verifier að staðreynd sem Sannarin veit er sönn án þess að Verifier-inn þurfi að kunna að sanna staðreyndina sjálfa. Þannig í rauninni eru Interactífar sannanir tól fyrir þá lötu í heiminum sem nenna ekki að lesa yfir sönnun og læra hvernig hann getur sjálfur sýnt fram á þessa staðreynd heldur fremur bara spyrja Proverinn hnitmiðaðra spurninga til að sannfæra sjálfan sig um að staðreyndin sé sönn.

+ Pælingar um í hvað gagnvirkar sannanir eru notaðar fræðilega (complexity theory) og hvernig þær eru notað í praktís (cryptography etc).

# 4 Gagnvirkar Sannanir (e. Interactive Proofs)

**Skilgreining 4.1.** Eftirfarandi eru skilgreiningar á eiginleikum samskiptaregla sem gerðar eru til að sanna staðhæfingar:

1. *Fullkomleiki* (e. completeness) er sá eiginleiki að sérhver sönn staðhæfing skal hafa sannfærandi sönnun um réttmæti hennar.

2. *Lögmæti* (e. soundness) er sá eiginleiki að engin ósönn staðhæfing skal hafa sannfærandi sönnun um réttmæti hennar.

SKILGREINA TUNGUMÁL?? **BÆTA:**

**Skilgreining 4.2.** *Gagnvirk sönnun* er samskiptaregla milli tveggja aðila sem fullnægir báðum eiginleikunum í skilgreiningu 2.1 með "miklum líkum". Hefð er fyrir því að tákna samskiptaregluna með $(\mathcal{P}, \mathcal{V})$ og kalla aðilana *sannari* (e. *prover*, $\mathcal{P}$) og *sannprófari* (e. *verifier*, $\mathcal{V}$) þar sem sannprófarinn er algrím sem keyrir í versta falli í líkindafræðilegum margliðu-tíma (e. probabilistic polynomial time) til að sannfæra sig um staðhæfingu sem sannarinn heldur fram. (i.e. sannfæra sig um að ákveðið inntak er í tungumáli $\mathcal{L}$ sleppa?)

Athugum að settar eru hömlur á hvers kynns algrím sannprófarinn getur verið en engar hömlur settar á sannarann. Svo t.d. getur sannarinn keyrt í veldisvísistíma og á meðan sannprófarinn keyrir í margliðutíma þá eru samskiptareglurnar sem sannarinn og sannprófarinn vinna eftir *gagnvirk sönnun*.

Við munum tákna $(\mathcal{P}, \mathcal{V}, x, r) \in \{0, 1\}$ sem úttakið frá sannprófaranum þegar sannarinn staðhæfir x og r er innri slembileiki (e. inner randomness) sannprófarans. Hér getum við hugsað að úttakið $(\mathcal{P}, \mathcal{V}, x, r) = 0$ sé höfnun sannprófarans á x, staðhæfingu sannprófarans. Og svipað með 1.

Innri slembileiki, þar sem sannprófarinn getur keyrt algrím sem byggir á slembistærð X þurfum við að "festa"gildið á slembistærðinni í X=r til að geta skilgreint hvað gerist...

Hvað meinum við þegar við segjum að eiginleikar skilgreiningar 2.1 er fullnægt með "miklum líkum"? Þar meinum við:

**Skilgreining 4.3.** *Gagnvirk sönnun* $(\mathcal{P}, \mathcal{V})$ er sögð hafa fullkomleika-villu (e. completeness-error) $\delta_f$ og lögmætis-villu (e. soundness-error) $\delta_l$ ef eftirfarandi gildir:

1. *fullkomleiki.* Fyrir sérhverja staðhæfingu x gildir:

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

2. *Lögmæti.* Fyrir sérhverja staðhæfingu x 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 $\delta_f, \delta_l \leq 1/3$.

Athgum að í skilgreiningunni hér að ofan er gildið $\delta_f, \delta_l \leq 1/3$ valið af handahófi, í raun á meðan $\delta_f, \delta_l < 1/2$ hefur sérhver gagnvirk sönnun eitthvert gildi.

Aukalega athugum við að ef við höfum samskiptareglu sem uppfyllir skilyrðunum í skilgreiningu 2.3 þá getur sannprófarinn sannað staðhæfingu fyrir sjálfan sig með eins mikilli nákvæmni og hann vill með því að ítra samskiptaregluna þar til hann er orðinn sáttu með líkurnar á að staðhæfingin er sönn.

## 4.1 Preliminaries

(Schwartz Zippel Lemma)

**Hjálparsetning 4.4.** *Látum* $\mathbf{F}$ *vera eitthvert svið og látum* $g :\longrightarrow \mathbf{F}^m \longrightarrow \mathbf{F}$ *vera margliðu af stigi í mesta lagi* $d$ *sem er ekki alstaðar núll. Þá gildir á sérhverju endanlegu mengi* $S \subset \mathbf{F}$*:*

$$P_{x \in S^m}[g(x) = 0] \leq d/|S| \tag{2}$$

*Þ.e. ef* x *er valið af handahófi 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* $S^m$

**Skilgreining 4.5.** Fjölbreytu-margliða g er marglínuleg ef stig margliðunnar í sérhverri breytu er í mesta lagi 1.

**Hjálparsetning 4.6.** *Sérhvert fall* $f : \{0,1\}^v \longrightarrow \mathbf{F}$ *hefur eina og aðeins eina marglínulega útvíkkun yfir* $\mathbf{F}$*, hér eftir notum við* $\tilde{f}$ *fyrir þessa útvíkkun.*

## 4.2 Summu athugun

Dæmi um gagnvirka sönnun er summu-athugunar samskiptareglan.

**Skilgreining 4.7.** Skilgreining á summu athugunar samskiptareglu.

Sýna fram á að Summu Athugun sé gagnvirk sönnun.

### 4.2.1 Telja þríhyrninga í neti

Hvernig við getum notað summu athugun til að telja þríhyrninga í neti, með hjálp sannara sem veit fjölda þríhyrninga í netinu.

### 4.2.2 Algrím Freivalds og Fylkjamargföldun

...

# 5 Sönnun án upplýsinga

Dæmi ? Ali baba etc.?

**Skilgreining 5.1.** *Sönnun án upplýsinga* er gagnvirk sönnun sem hefur eftirfarandi eiginleika:

1. *Upplýsingaleysi* (. *zero-knowledge* (**Betri þýðingu vinsamlegast!**). Ef staðhæfingin er sönn mun enginn sannprófari læra neitt meira eftir sönnunina heldur en að staðhæfingin er sönn.

Meira abstract / strangari skilgreining:

**Skilgreining 5.2.** Við segjum að $(\mathcal{P}, \mathcal{V})$ sé sönnun án upplýsinga ef fyrir sérhvern margliðu-tíma sannprófara-strategíu $V'$ þá er til líkindafræðilegt margliðu-tíma algrím $S'$ (kallað hermir, e. simulator) þannig að fyrir sérhverja sanna staðhæfingu ($x \in \mathcal{L}$) gildir að eftirfarandi slembistærðir eru (í einhverjum skilningi, skilgreina betur!) óaðgreinanlegar:

1. Úttakið $(\mathcal{P}, \mathcal{V}, x, X)$, þar sem X er slembistærð,
2. Úttakið $S'(x)$.

**Skilgreining 5.3.** SKILGREINA "óaðgreinanlegar"í skilgreiningu 3.2 hér að ofan.

**Skilgreining 5.4.** SKILGREINA Skuldbingingarkerfi e. commitment schemes.

NOTAGILDI SKULBINDINGARKERFA???

## 5.1 Sigma Samskiptareglur

**Skilgreining 5.5.** Skilgreina Sigma Samskiptareglur

### 5.1.1 Strjáll logri - Samskiptaregla

**Skilgreining 5.6.** Skilgreina Samskiptaregluna

## 5.2 Notagildi

Fjárhagsreglugerðir / Kjarnorku-afvopnun / Rafmyntir etc.

# 6 zk-Snark, Non-interactive Protocols

MÖGULEGA SLEPPA.

Skilgreining + Public coin vs Private Coin.

To be written.

# 7 Gagnvirkar sannanir og flækjufræði

MÖGULEGA SLEPPA.

**Setning 7.1.** *Látum $\mathcal{L} \in \mathbf{NP}$. Þá, ef við notum skuldbindingarkerfi, er til gagnvirk sönnun án upplýsinga sem sannar að $x \in \mathcal{L}$*

**Setning 7.2.** *Öll vandamál sem hægt er að sanna með gagnvirkri sönnun er hægt að sanna án upplýsinga.*

**Setning 7.3.** ***IP*** $=$ ***PSPACE***.

To be written.

# 8 Samantekt

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