Sönnun án upplýsinga

Þórður Ágústsson

17. febrúar 2021

Útdráttur

Ágrip hér

1 Inngangur

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).

2 Gagnvirkar Sannanir (e. Interactive Proofs)

Skilgreining 2.1. 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 2.2. *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 2.3. *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.* 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.

2.1 Preliminaries

(Schwartz Zippel Lemma)

Hjálparsetning 2.4. *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* $S \subset \mathbf{F}$*:*

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

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

Hjálparsetning 2.6. *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.*

2.2 Summu athugun

Dæmi um gagnvirka sönnun er summu-athugunar samskiptareglan.

Skilgreining 2.7. Skilgreining á summu athugunar samskiptareglu.

Sýna fram á að Summu Athugun sé gagnvirk sönnun.

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

Dæmi ? Ali baba etc.?

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 meira eftir sönnunina 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-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 3.3. SKILGREINA "óaðgreinanlegar"í skilgreiningu 3.2 hér að ofan.

Skilgreining 3.4. SKILGREINA Skuldbingingarkerfi e. commitment schemes.

NOTAGILDI SKULBINDINGARKERFA???

3.1 Sigma Samskiptareglur

Skilgreining 3.5. Skilgreina Sigma Samskiptareglur

3.1.1 Strjáll logri - Samskiptaregla

Skilgreining 3.6. Skilgreina Samskiptaregluna

3.2 Notagildi

Fjárhagsreglugerðir / Kjarnorku-afvopnun / Rafmyntir etc.

4 zk-Snark, Non-interactive Protocols

MÖGULEGA SLEPPA.

Skilgreining + Public coin vs Private Coin.

To be written.

5 Gagnvirkar sannanir og flækjufræði

MÖGULEGA SLEPPA.

Setning 5.1. *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 5.2. *Öll vandamál sem hægt er að sanna með gagnvirkri sönnun er hægt að sanna án upplýsinga.*

Setning 5.3. ***IP*** $=$ ***PSPACE***.

To be written.

6 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