Sönnun án upplýsinga

Þórður Ágústsson

14. mars 2021

1 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 1.1. *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 1.2. 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 1.3. 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.

1.1 Hermar

Óformlega þýðir það að til sé Hermir fyrir ákveðna samskiptareglu að $\mathcal{V}$ lærir ekkert frekar um að $\mathcal{P}$ viti lausn á vandamálinu heldur en það, að $\mathcal{P}$ veit lausn á vandamálinu. Þetta getum við séð með því að athuga að ef $\mathcal{P}$ veit lausnina á vandamálinu þá mun $\mathcal{V}$ ekkert græða á því að keyra samskipta regluna nema það að $\mathcal{V}$ veit þá að $\mathcal{P}$ veit lausnina, því ef

Skoðum skilgreininguna í samhengi með Litblinda vininn dæmið 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. 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.

1.2 Strjáll Logri

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

leysa. Skilgreinum:

Skilgreining 1.4. 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:

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

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 $h = g^r (\mod p)$ 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 $a = r + bx (\mod p)$ og sendir á $\mathcal{V}$
4. $\mathcal{V}$ athugar hvort $g^a = hv^b (\mod p)$, 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 $h = g^r(\mod p)$ 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 $g^a = h(\mod p)$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda $(h, a) => g^a = h(\mod p)$, 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 $g^a = hv(\mod p)$ svo til að plata $\mathcal{V}$ þarf $\mathcal{P}$ að senda $(h, a) => g^a = hv(\mod p)$ sem þýðir að $\mathcal{P}$ veit 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 (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 $g^a = hv(\mod p)$ sem krefst þess af okkur að senda til baka lausn a á stjrála logariþmanum 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 (því lausn á strjála logranum er í NP, ?). 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 c « p. Við fáum því að líkurnar á að $\mathcal{P}$ nái að plata $\mathcal{V}$ eru:

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

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

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 eru $\frac{c}{p}$ 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 $h = g^s v^{-1}(\bmod p)$ 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 $\mathcal{V}$:

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

Og samþykkir þá 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 viti þessar ákveðnu upplýsingar (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 consistently rétt. 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 bæti 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.

Mikilvægi slembibreytunnar er því mikilvæg. Athugum ennfremur að ekki er nauðsynlegt að b sé slembibreyta í augum $\mathcal{V}$, heldur eingöngu að $\mathcal{P}$ sjái breytuna sem slembibreytu sem hann veit ekki dreifinguna á.

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 einhvern sannprófara-algrím, sem er ekki endilega sannsögull, með slembileika r. Við ætlum að útbúa hermi H' þ.a. fyrir sérhverja staðhæfingu x gildir að eftirfarandi slembibreytur

1. ($\mathcal{P}$, $\mathcal{V}$, x, r)
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, handahófskennt veldi t af spönnuðinum g^t. Þ.e. 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 handahófskennt hér eigum við uniformly random) og því með sömu dreifingu og r-ið valið af $\mathcal{P}$ sem veldur því að h-in hafa sömu handahófskenndu 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 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) og hegðar sér eins og raunveruleg samskipti milli $\mathcal{P}$ og $\mathcal{V}$.

Strjáli Logrinn - samskiptareglan er því Gagnvirk sönnun án upplýsinga. Hún getur því verið notuð t.d. til að útbúa vegabréfskerfi þar sem eigandi vegabréfsins þarf aldrei að sýna vegabréfið sitt (hvorki sem plaintext né dulkóða það fyrst) til að sanna að hann sé sá sem hann segist vera.

Strjáli Logrinn er dæmi um Σ-samskiptareglu.

1.3 Þrílitað net

Þrílitun nets er vandamál í netafræði. Vandamálið er:

Gefið er net G = (V,E) er hægt að lita sérhvern hnút v með einum lit af þremur, setjum $c \in \{\text{rauður, grænn, blár}\}$, þannig að engin tenging/vegur (e. edge) e tengir tvo hnúta af sama lit.

Þetta vandamál er í menginu NP-Complete, þ.e. mengi þeirra vandamála sem hægt er að sannprófa í margliðutíma en ekki leysa í margliðutíma (i.e. tekur meiri tíma eða slembi-margliðutíma). Því ef manni er gefin 3-litun á tilteknu neti G þá getur maður athugað alla hnúta sem eru tengdir þannig í versta falli tekur það $\binom{|V|}{2} \approx |V|^2$.

Samskiptareglan fyrir þrílitun nets

Gerum ráð fyrir að Agnes vill sannfæra Emil um að hún veit um þrílitun, {rauður, grænn, blár}, á tilteknu neti G = (V,E).

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 svo öruggara væri að leika $|E|^2$ lotur til að vera tiltölulega vel viss um að hún sé ekki að ljúga.

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 lyginn 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)).

ATH: $(1 - \frac{1}{n})^{kn} < \frac{1}{2^k}$.

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 úttakið úr herminum (LÍKLEGA ÆTTIR AÐ LÁTA ÚTTAKIÐ VERA TRANSCRIPT/History FYRIR EINA LOTU!) hefur sömu dreifingu og úttak samskiptareglunnar milli heiðarlegs $\mathcal{P}$ og einhvers $\mathcal{V}$ því hnútarnir 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.

1.4 Smá flækjufræði

Skilgreining 1.5. P er flokkur af ákvörðunar-vandamálum sem eru leysanleg með algrími sem keyrir í margliðutíma

Skilgreining 1.6. NP er flokkur af ákvörðunar-vandamálum sem eru leysanleg með brigðgengnu (non-deterministic) algrími sem keyrir í margliðutíma. (https://cs.stackexchange.com/questions/1243/what-is-meant-by-solvable-by-non-deterministic-algorithm-in-polynomial-time)

Þar sem brigðgengin algrím þýðir í einföldu máli að algrímið tekur ákvarðanir í hverju skrefi ekki eingöngu útfrá inntakinu. Þ.a. það keyrir í slembirými og þegar við segjum að þesskonar algrím keyrir í margliðutíma er átt við að EF þegar algrímið keyrir á ákveðnu inntaki algrímið gerir 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 1.7. 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 $\in$ NP-fullkomið (HEIMILD!) fáum við þá niðurstöðu að $NP \subseteq ZKP$

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