Nullteadmusprotokollid

Helger Lipmaa

Küberneetika AS; http://www.cyber.ee

helger@cyber.ee; http://home.cyber.ee/helger

30. november 1998. a.

Küsimuse tõstatus

Olgu L — mingi keel (ülesannete klass). Kuidas tõestada, et $x \in L$, nii et muud teadmust peale selle, et $x \in L$, ei paljastuks?

Kasutusalad:

1. krüptograafiliste protokollide juures saaks tõestada, et osapool järgib protokolli,

2. identimised (inimene teab parooli),

3. jne jne

Interaktiivsed Turingi masin

Interaktiivne Turingi masin (ITM) on TM

- ainult-loetava sisendlindi,
- ainult-loetava juhuarvude lindi,
- loetav-kirjutatav töölindi,
- ainult-loetava suhtluslindi,
- ainult-kirjutatava suhtluslindi ja
- ainult-kirjutatava väljundlindiga.

Juhuarvude lindil on loenduv arv bitte (*mündivisked*), seda linti saab skaneerida vaid vasakult paremale. TM *viskab münti* $\iff$ ta loeb oma juhuarvude lindilt järgmise biti.

Ainult-kirjutatava suhtluslindi sisuks on masina poolt edastatud bitid. Ainult-loetava suhtluslindi sisuks on masina poolt vastu võetud bitid.

Interaktiivne protokoll

Interaktiivne protokoll on sama sisendlinti jagav ITM-ide järjestatud paar (P, V), kus V ainult-kirjutatav suhtluslint on P ainult-loetav suhtluslint ja vastupidi. Masinad aktiveeruvad kordamööda, esimesena on aktiivne V.

Aktiivse faasi ajal teostab masin teatava (sisemise) arvutuse, mis sõltub tema lintide sisust, kirjutab mingi teate oma ainult-kirjutatavale suhtluslindile ning deaktiveerub masin. Seejärel aktiveerub teine masin. Protokoll loetakse lõppenuks, kui kirjutatav teade on tühistring. Masin V *aktsepteerib* (*lükkab tagasi*) sisendi, lõpetades protokolli seisundis Accept (Reject). Masina i-ndaks teateks on teade, mida vastav masin kirjutab i-ndal sammul.

P on arvutuslikult piiramatu TM. Masina V *arvutusajaks* nimetatakse V poolt aktiivsetel faasidel teostatud arvutuste kestuste summat, V arvutusaeg on piiratud polünoomiga sisendi pikkusest.

Interaktiivne tõestussüsteem

Ütleme, et keelel L on *interaktiivne tõestussüsteem*, kui leidub selline ITM V, nii et

1. $\exists$ ITM P, nii et (P, V) on IP ning $\forall x \in L$, $|x|$ piisavalt suur, on sündmuse "V aktsepteerib" tõenäosus $> 2/3$ (tõenäosus üle V ja P mündivisete).

2. $\forall$ ITM P, nii et (P, V) on IP ning $\forall x \notin L$, $|x|$ piisavalt suur, on sündmuse "V aktsepteerib" tõenäosus $< 1/3$ (tõenäosus üle V ja P mündivisete).

Teises tingimuses on vaja nõuda, et "$\forall$ ITM P." Paari (P, V), mille korral I tingimus on tõene, nim keele L *interaktiivseks tõestuseks*. Olgu **IP** nende keelte hulk, millel leiduvad interaktiivsed tõestused.

Triviaalselt **NP** $\subseteq$ **IP**.

Näide arvuteooriast

Olgu $\mathbb{Z}_n^* = \{0 < x \leq n : (x, n) = 1\}$. Olgu $\mathrm{QR}(n) := \{(x, n) : x \in \mathbb{Z}_n^* \wedge \exists y. y^2 \equiv x \mod n\}$ ning $\mathrm{QNR}(n) := \mathbb{Z}_n^* \setminus \mathrm{QR}$. Näitame, et $\mathrm{QNR}(n) \in$ **IP**. Protokoll on järgmine. Sisendi (x, n) korral

$V \to P$: V saadab P-le korteeži $(w_1, \ldots, w_k)$, kus $k = |n|$ ning

$$w_i = \begin{cases} z_i^2 \mod n \ , & b_i = 1 \ , \\ x \cdot z_i^2 \mod n \ , & b_i = 0 \ , \end{cases}$$

kus $z_i \in \mathbb{Z}_n^*$ ja $b_i \in \{0, 1\}$ on V poolt juhuslikult valitud.

$P \to V$: P saadab V-le korteeži $(c_1, \ldots, c_k)$, kus

$$c_i = \begin{cases} 1 \ , & w_i \in \mathrm{QR}(n) \ , \\ 0 \ , & w_i \notin \mathrm{QR}(n) \ . \end{cases}$$

Kui $b_i = c_i$, $\forall i$, aktsepteerib V sisendi (st loeb, et $(x, n) \in \mathrm{QNR}$).

Esimese näite korrektsus

Kui $(x, n) \in$ QNR, siis $w_i \in$ QR$(n) \iff b_i = 1$. Seega suudab kõikvõimas P alati leida, kas $w_i \in$ QR(n) või mitte, ning seega leida kõik b_i väärtused korrektselt (ning seega V aktsepteerib tõenäosusega 1).

Kui $(x, n) \in$ QR, siis on w_i juhuslikult valitud ruutjääk $\bmod n$ sõltumatult b_i väärtusest. Seega on sel juhul tõenäosus, et P leiab sellise c_i, et $c_i = b_i$, ülimalt $1/2$ suvalise i jaoks ning seega aktsepteerib V tõenäosusega $\leq \left(\frac{1}{2}\right)^k$.

Näide graafiteooriast

Graafid G_1 ja G_2 on *isomorfsed* kui leidub selline bijektsioon $\pi : V(G_1) \to V(G_2)$, et $(v, w) \in E(G_1) \iff (\pi(v), \pi(w)) \in E(G_2)$. Vastasel juhul graafid G_1 ja G_2 ei ole isomorfsed. Olgu

$$\text{GNI} := \{(G_1, G_2) : G_1 \text{ ja } G_2 \text{ ei ole isomorfsed}\} .$$

Keelele GNI ei ole teada lühikesi **NP**-tõestusi (st ei ole teada, kas GNI $\in$ **NP**). Interaktiivne tõestus sisendil (G_1, G_2) seisneb järgnevate sammude itereerimisest $i = 1, \ldots, i = k$ jaoks:

$V \to P$: V valib juhuslikult $\alpha_i \in \{1, 2\}$, genereerib juhuslikult graafiga G_{α_i} isomorfse graafi G' ning saadab selle P-le.

$P \to V$: P saadab V-le arvu β_i.

V aktsepteerib kui $\beta_i = \alpha_i$, $\forall 1 \leq i \leq k$.

Teise näite põhjendus

Kui $(G_1, G_2) \in$ GNI, suudab P eristada graafi G_1 isomorfseid koopiaid graafi G_2 isomorfsetest koopiatest ning seega V aktsepteerib tõenäosusega 1.

Kui $(G_1, G_2) \notin$ GNI, on graafi G_1 isomorfne koopia alati ka graafi G_2 isomorfne koopia (ning vastupidi). Seega on tõenäosus, et $\beta_i = \alpha_i$, ülimalt $1/2$. Tõenäosus, et $\beta_i = \alpha_i$, $\forall$i, on $\leq \left(\frac{1}{2}\right)^k$.

Nullteadmus

Vaatleme järgnevalt, kui palju “teadmust” tuleb edastada selleks, et veenda polünomiaalselt piiratud verifitseerijat propositsiooni tõesuses. Kõigepealt, mis on “teadmus?”

Kõigi kehtestatavate lausearvutusvalemite keel SAT (**NP**-täielik). Loomulik on järgmine tõestus: sisendvalemi ϕ korral edastab P $\mathcal{V}$-le väärtustuse $\vec{x}$, $\phi(\vec{x}) = \top$. Fakti $\phi(\vec{x}) = \top$ saab verifitseerida polünomiaalses ajas.

Kui väärtustuse $\vec{x}$ leidmine nõuaks $\mathcal{V}$-lt rohkem kui polünomiaalset aega (mis kehtib, kui **P** $\neq$ **NP**), ütleme, et $\mathcal{V}$ on saanud protokolli jooksul *lisateadmust*. Täpsemalt, keele L interaktiivne tõestussüsteem on *nullteadmus*-, kui järgmine lause on tõene. Juhul $\mathrm{x} \in \mathrm{L}$ kehtib: mistahes väärtuse, mida $\mathcal{V}$ suudab polünomiaalses ajas arvutada pärast protokolli lõppu, suudaks ta arvutada polünomiaalses ajas ilma P-ga suhtlemata, kasutades stohhastilist polünomiaalset Turingi masinat.

Definitsioonid

Olgu (P, V) — interaktiivne protokoll. P ja V fikseeritud mündivisete järjestuse korral on view_{pv} P ning V vahel edastatud teadete jada konkateneeritud V poolt visatud müntidega (seega, view_{pv} on juhuslik suurus, üle P ja V mündivisete p ja v). Olgu h — verifitseerija privaatsisend, kus $|h|$ on polünomiaalne ühise sisendi pikkuse suhtes.

Ütleme, et (P, V) on keele L *perfektne nullteadmustõestus*, kui leidub stohhastiline polünomiaalne Turingi masin M, nii et $\forall x \in L$, $\forall a > 0$, $\forall h, |h| < |x|^a$, on juhuslikud suurused $M_r(x, h)$ ning $\mathrm{view}_{pv}(x)$ sama jaotusega (kus $M_r(x, h)$ jaotus on üle M-i mündivisete r sisendil (x, h)).

Statistiline nullteadmus

Ütleme, et (P, V) on keele L *statistiline nullteadmus-tõestus*, kui leidub stohhastiline polünomiaalne Turingi masin M, nii et $\forall x \in L$, $\forall a > 0$, $\forall h$, $|h| < |x|^a$,

$$\sum_{\alpha} |\operatorname{Prob}_r(M_r(x, h) = \alpha) - \operatorname{Prob}_{p,v}(\operatorname{view}_{pv}(x) = \alpha)| < \frac{1}{|x|^c} \ ,$$

kõigi konstantide $c > 0$ ning piisavalt suure $|x|$ jaoks.

Intuitiivselt: piiramatu arvutusvõimsusega vaatleja ei suuda eristada hulkasid $S_1 := \{M_r(x, h) : r\}$ ning $S_2 := \{v_{pv} : p, v\}$, kui talle on antud vaid polünomiaalne arv sisendeid kummastki hulgast.

Arvutuslik nullteadmus

Ütleme, et (P, V) on keele L *arvutuslik nullteadmus-tõestus*, kui leidub stohhastiline polünomiaalne Turingi masin M, nii et $\forall$ polünomiaalse suurusega skeemipere $C := \{C_{|\alpha|}\}$, $\forall$ konstantide $a, d > 0$, $\forall x \in L$, $|x|$ piisavalt suur, $\forall h$, $|h| < |x|^a$,

$$\frac{1}{|x|^d} > |\,\mathrm{Prob}(C_{|x|}(\alpha) = 1 : \alpha \in_R M_r(x,h)) - \mathrm{Prob}(C_{|x|}(\alpha) = 1 : \alpha \in_R \mathrm{view}_{pv}(x))|$$

kõigi konstantide $c > 0$ ning piisavalt suure $|x|$ jaoks.

Intuitiivselt: stohhastilises polünomiaalses ajas töötav vaatleja ei suuda eristada hulkasid $S_1 := \{M_r(x,h) : r\}$ ning $S_2 := \{v_{pv} : p, v\}$, kui talle on antud vaid polünomiaalne arv sisendeid kummastki hulgast.

Nullteadmustõestussüsteemid

Ütleme, et keelel L on *(arvutuslik/statistiline/perfektne)-nullteadmustõestussüsteem*, kui

1. $\exists$ keele L interaktiivne tõestussüsteem (P, V);

2. $\forall$ interaktiivse Turingu masina V' korral on interaktiivne protokoll (P, V') on keele L (arvutuslik/statistiline/perfektne)-nullteadmusprotokoll.

Olgu **KC[0]** selliste keelte hulk, millel leiduvad arvutuslikud nullteadmustõestussüsteemid.

Ühesuunaliste kujutuste leidumisest järeldub **NP** $\subseteq$ **KC[0]**

T1: Kui leidub (mitte-uniformses) polünomiaalses ajas eristatamatu krüptoskeem, siis **NP** $\subseteq$ **KC[0]**. T2: Kui leiduvad ühesuunalised kujutused, siis leiduvad (mitte-uniformses) polünomiaalses ajas eristatamatud krüptoskeemid.

T1 tõesustamiseks piisab ühe konkreetse **NP**-täieliku keele jaoks arvutusliku nullteadmussüsteemi näitamisest. Valime selleks keeleks keele 3COL — kolme värviga värvitavate graafide keele.

Keele 3COL nullteadmustõestus

P tahab V-d veenda, et G kromaatiline arv $\chi(G) \leq 3$, ilma 3-värvingut avalikustamata. Protokoll seisneb järgnevate sammude $|E|^2$-kordses itereerimises:

1. P valib juhusliku permutatsiooni π värvide vahel (näiteks $\pi(R) = B$, $\pi(B) = G$ ja $\pi(G) = R$).

2. P krüptib iga tipu v värvi $\pi(C(v))$, kasutades stohhastilist krüptoskeemi, erineva võtmega E_v iga tipu v jaoks. P avalikustab saadud krüptogrammid koos vastavusega, mis seob krüptogramme graafi G tippudega.

3. V valib juhuslikult graafi G serva $e = (v, w)$.

4. P avalikustab dekrüptimisvõtmed D_v ja D_w.

5. V leiab suurused $\pi(C(v))$ ning $\pi(C(w))$ ning verifitseerib, et need on erinevad.

Protokolli korrektsus

Kui $\chi(G) \leq 3$ ja P teab vastavat 3-värvingut, ei detekteeri V kunagi ebakorrektselt värvitud serva.

Kui $\chi(G) > 3$, siis $\pi(C(v)) = \pi(C(w))$ igal sammul tõenäosusega $\geq |E|^{-1}$. Pärast $|E|^2$ sammu on aktsepteerimise tõenäosus eksponentsiaalselt väike.

Kui $\chi(G) \leq 3$, on suhtluse tõmmis võrdne edastatud teadete konkatenatsiooniga. On võimalik tõestada (eeldades turvalise krüptoskeemi leidumist), et üle kõikide tõmmiste defineeritud tõenäosusjaotus on polünomiaalses ajas eristamatu kõikide V enese poolt (ilma P-ga suhtlemata) polünomiaalses ajas genereeritavate tõmmiste hulgast. Ehk: esitatud protokoll on arvutuslik nullteadmusprotokoll.

Rakendused kasutaja identimisel

Nullteadmusprotokollide abil saab kasutajaid identida. Idee: iga kasutaja salvestab üldkättesaadavasse nimistusse teoreemi, mille tõestust vaid tema üksi teab. Sisselogimisel käivitub kasutaja (P) ning masina (V) vahel nullteadmustõestus. Kui V aktsepteerib, garanteeritakse kasutajale ligipääs.

Isegi kui ründaja kuuleb nullteadmusprotokolli pealt, ei suuda ta sellest teha järeldusi, mis võimaldaksid autoriseerimata ligipääsu saavutamist. Kõige tuntum nullteadmusprotokoll kasutaja identimiseks on *Fiat-Shamiri protokoll*.

Fiat-Shamiri identimisprotokoll

Ühekordne seadistus. Usaldatav keskus T genereerib ja avalikustab mooduli $n = pq$, hoides algarvud p ja q salajased. Iga kasutaja P genereerib juhuslikult arvu $s \in \mathbb{Z}_n^*$ ning registreerib arvu v, $v = s^2 \mod n$, kui oma avaliku võtme.

Protokoll:

$P \to V$: P valib juhusliku arvu $r \in_R \mathbb{Z}_n \setminus \{0\}$, ja edastab V-le arvu $x := r^2 \mod n$.

$V \to P$: V valib juhuslikult biti $e \in_R \{0, 1\}$ ning edastab e P-le.

$P \to V$: P arvutab väärtuse $y = r$ (kui $e = 0$) või $y = rs \mod n$ (kui $e = 1$) ning saadab selle V-le.

V lükkab tõestuse tagasi, kui $y = 0$. Vastasel korral aktsepteerib V, kui $y^2 \equiv x \cdot v^e \mod n$ (kui $e = 0$, siis $y^2 \equiv xv^0$; kui $e = 1$, siis $y^2 \equiv xv^1$).