Univerza v Ljubljani
Fakulteta za matematiko in fiziko

Matematika

Rok Erman

Dokazi brez razkritja znanja

Projekt

Ljubljana, 2008

Kazalo

Kazalo 3

1 Uvod 5

1.1 Dokazi, ki to niso 6

2 Zahteve 7

2.1 Osnovni protokol 8

3 Primeri 11

3.1 Otroški primer 11

3.2 Jama Ali Babe 12

3.3 Rubikova kocka 14

3.4 Sudoku 16

3.5 Hamiltonskost 19

3.6 Feige-Fiat-Shamir dokaz identitete 22

4 Interaktivni Turingovi stroji 25

4.0.1 Skupni izračuni dveh interaktivnih Turingovih strojev 26

4.0.2 Časovna zahtevnost interaktivnega Turingovega stroja 26

4.0.3 Časovna zahtevnost dokaza brez razkritja znanja 26

Literatura 26

Poglavje 1

Uvod

Velikokrat se srečamo s problemom, ko želimo nekomu nekaj dokazati, ne želimo pa, da s tem predamo svoje znanje naprej. Eden od možnih scenarijev je lahko razvoj nove kriptografske metode. Kupcu bi radi dokazali, da znamo bolje in hitreje kriptirati, ne bi pa mu radi pokazali kako, saj sicer zadeve ne bomo mogli prodati.

V vsakdanjem življenju pa smo pogosto soočeni s situacijo, ko nam nekdo pove skrivnost in se o tem pogovarjamo s tretjo osebo, ne vemo pa, če jo pozna tudi on. Tukaj mora eden drugemu dokazati, da pozna skrivnost ne da jo razkrije nato pa se lahko oba o njej prosto pogovarjata.

Dokazi brez razkritja znanja so kriptografski protokoli, z uporabo katerih lahko oseba A osebi B dokaže, da pozna določeno skrivnost ne da pri tem razkrila vsebino te skrivnosti osebi B ali morebitnim prisluškovalcem. Ključna lastnost dokazov brez razkritja znanja je ta, da se oseba B po tistem, ko je slišala dokaz osebe A, pred tretjimi osebami ne more izdajati, da pozna obravnavano skrivnost. Dokaze brez razkritja znanja se uporablja predvsem v računalniškem svetu. Seveda pa jih lahko zelo uspešno uporabljamo tudi v fizični obliki. Tako bomo videli nekaj primerov kako lahko nekomu v živo dokažemo veljavo neke trditve brez razkritja znanja. V ta namen bomo uporabljali kuverte, igralne karte, kartice z odstranljivim zaščitnim premazom in podobno.

Ves čas bomo za preverjevalca (verifier) uporabljali Viktorja in za dokazovalca (prover) Peggy, kot je to običajno v literaturi.

1.1 Dokazi, ki to niso

Preden nadaljujemo, je potrebno poudariti, da se dokaz brez razkritja znanja bistveno razlikuje od dokaza v ožjem matematičnem smislu in je po strukturi bližje dokazom, ki temeljijo na interakciji in interpretaciji ter jih ljudje uporabljajo pri vsakodnevni medsebojni komunikaciji. Striktni matematični dokazi so statični in formalni, saj so bodisi očitni, bodisi jih lahko izpeljemo iz že obstoječih dejstev z logičnim sklepanjem. Ljudje pa običajno uporabljamo dokaz v bolj intuitivnem smislu. Razliko med matematičnim dokazom in tem, kar delamo pri dokazih brez razkritja znanja, je lepo opisal Goldreich [4].

Poglavje 2

Zahteve

Dokaze brez razkritja znanja lahko opišemo kot kriptografske protokole, ki ustrezajo naslednjim lastnostim:

(a) *Preverjevalec se ne more iz protokola ničesar naučiti.* Osrednja ideja dokazov brez razkritja znanja je, da se med dokazom ne prenese nič znanja. Preverjevalec se iz protokola torej ne nauči ničesar, kar ne bi mogel izvedeti sam brez dokazovalca. Brez te lastnosti bi take protokole lahko imenovali kvečjemu dokazi z minimalnim razkritjem znanja.

(b) *Dokazovalec ne more prevarati preverjevalca (veljavnost).* Če Peggy skrivnosti ne pozna, bo lahko Viktorja prepričala le v primeru, ko bo imela neznansko srečo. Po večih korakih protokola se lahko verjetnost, da Viktor verjame lažnemu dokazu zmanjša na poljubno vrednost. Protokoli so tudi taki, da ko dokazovalec prvič ne poda pravilnega odgovora, Viktor ve, da Peggy skrivnosti ne pozna. Tako se verodostojnost dokaza z vsakim naslednjim korakom izboljšuje. Taki protokoli lahko delujejo tudi v primeru, če je verjetnost, da odgovor na Viktorjevo vprašanje uganemo, zelo velika. Takrat preprosto potrebujemo le več korakov za doseganje željene gotovosti. Z drugimi besedami, veljavnost zajema preverjevalčevo sposobnost, da se obvaruje pred tem, da ga dokazovalec prepriča o nepravilni trditvi (ne glede na to kaj dokazovalec stori, da bi to dosegel).

(c) *Preverjevalec ne more pravarati dokazovalca.* Viktor iz protokola ne more pridobiti nobene dodatne informacije, tudi če se protokola ne drži. Viktor se lahko le prepriča, da Peggy res pozna skrivnost. Kasneje bomo videli, da dokazovalec vedno poda le eno od mnogih rešitev za nek problem, nikdar pa vseh, s čimer bi dovolil preverjevalcu, da sam spozna skrivnost.

(d) *Preverjevalec se ne more izdajati za dokazovalca tretji osebi.* Ker se ne prenese nobene informacije iz Peggy na Viktorja, se Viktor ne more izdajati kot dokazovalec tretji osebi. Prav tako ne more Viktor posneti pogovora med njim in Peggy in ga uporabiti kot dokaz. Posnetek bi izgledal natanko tak, kot ponarejen posnetek, kjer se preverjevalec in dokazovalec vnaprej zmenita, katera vprašanja bo preverjevalec postavil. Pri večini teh protokolov je možen napad vmesnega človeka, ki pošilja sporočila med dokazovalcem in preverjevalcem. Tak napad pa k sreči napadalcu prav nič ne pomaga, saj deluje le kot snemalec pogovora.

(e) *Viktorja lahko prepričamo o katerikoli resnični trditvi.* To lastnost imenujemo polnost (completeness) in v bistvu zajema sposobnost dokazovalca, da preverjevalca prepriča o resničnosti poljubne resnične trditve, ki spada v vnaprej določeno množico resničnih trditev.

Več o navedenih lastnostih je mogoče prebrati v [2].

2.1 Osnovni protokol

Peggy in Victorja lahko obravnavamo kot verjetnostna algoritma. Vsak od njiju lahko izvaja izračune, ki jih vidi le on sam in vsak ima lasten skriven generator naključnih števil. Na začetku imata oba nek vnos podatkov x. Cilj interaktivnega dokaza je Victorja prepričati, da x ima neko lastnost. Interaktiven dokaz je protokol oblike izziv-odgovor in je sestavljen iz določenega števila krogov oziroma ponovitev. V vsakem krogu Peggy in Victor izmenično delata naslednje:

- sprejmi sporočilo

- izračunaj potreben odgovor
- pošlji sporočilo

Tipičen krog je sestavljen iz izziva, ki ga pošlje Victor in Peggyjinega odgovora. Na koncu dokaza Victor sprejme ali zavrne dokaz, glede na to ali je Peggy uspešno odgovarjala na njegove izzive.

Poglavje 3

Primeri

V vseh primerih dokazov brez razkritja znanja, ki jih bomo navedli, bosta nastopali dve osebi: dokazovalka Peggy in preverjevalec Victor. Peggy bo poznala neko skrivnost in bo želela o tem prepričati Victorja ne da bi mu jo izdala. Victor bo Peggy zastavljal vrsto vprašanj, s katerimi bo poskušal ugotoviti, ali Peggy res pozna skrivnost.

3.1 Otroški primer

V osemdesetih letih je pri otrocih postala zelo priljubljena knjiga Where's Waldo. V njej so bile narisane slike z veliko ljudmi, kot jo vidite spodaj. Na sliki je bilo potrebno najti Walda, ki je bil bolj ali manj dobro skrit ali preoblečen. Otroci so potem gledali te slike in iskali Walda.

Predpostavimo sedaj da majhna Peggy in Viktor gledata to knjigo. Peggy trdi, da je Walda našla, a noče Viktorju pokazati, kje ga vidi. Viktor ji ne verjame, saj po dolgem iskanju Walda še vedno ni našel. Peggy bi seveda rada, da ji Viktor verjame. Kako lahko rešita nastali problem?

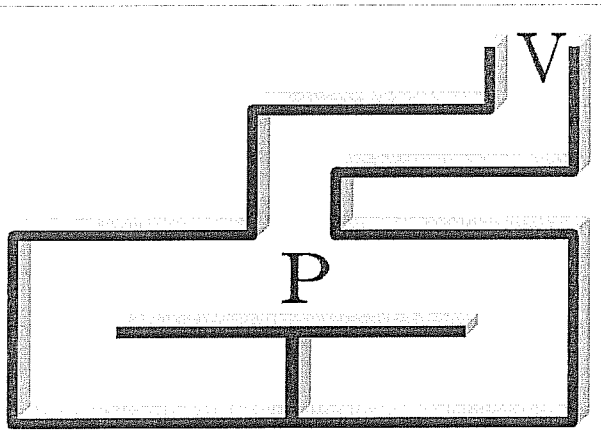
Preprosta rešitev je:

Peggy iz lepenke izreže pravokotnik z vsaj podvojenimi merami odprte knjige. Na sredini izreže pravokotnik velikosti Walda in ga prekrije. Knjigo nese za lepenko nastavi Walda v okence in ga odkrije Viktorju. Sedaj Viktor mora verjeti Peggy, sam pa ne ve ničesar novega o lokaciji Walda.

Preverimo zahteve za dokaze brez razkritja znanja:

- V tem najpreprostejšem primeru je že osnovna predpostavka o nerazkritju znanja zelo vprašljiva. Viktor lahko iz Waldove okolice sklepa, kje ga lahko najde. Prav tako vidi kako je oblečen. Pri izvedbi protokola mora Peggy biti zelo previdna, da niti malo ne nakaže na katerem delu slike se skriva Waldo.
- Da Peggy res ve kje je Waldo je tukaj očitno, če privzamemo, da nima neke druge slike Walda.
- Viktor lahko prevara Peggy na mnogo načinov. lahko ji iztrga lepenko iz rok ali pa ko vidi Walda hitro počečka po njem in ga kasneje z lahkoto najde.
- Viktor se ob dobri izvedbi protokola ne more pretvarjati tretji osebi, da pozna Waldovo lokacijo, a kot smo videli zgoraj lahko pridobi nekaj informacije o skrivnosti.
- Polnost je izpolnjena, saj lahko Peggy Walda pokaže pa naj se nahaja kjerkoli na sliki.

3.2 Jama Ali Babe



Slika 3.1: Jama Ali Babe

Oglejmo si primer krožne različice jame Ali Babe [5]. Kot je razvidno iz slike, se jama takoj za vhodom razcepi v dva tunela, na stiku katerih se nahajajo vrata,

ki jih je mogoče odpreti z geslom. Peggy pozna geslo in želi prepričati Victorja, da ga res pozna, ne želi pa, da Victor izve geslo. Dokaza brez razkritja znanja se lotita tako, da Peggy sama vstopi v jamo in se nato odpravi v naključno izbrani tunel. Nato vstopi v jamo Victor, ki si naključno izbere enega od obeh tunelov in o izbiri obvesti Peggy, ki mora sedaj priti iz izbranega tunela. Če Peggy res pozna geslo, bo lahko vedno zadostila tej zahtevi, saj ima možnost z geslom odpreti vrata, ki povezujejo tunela. Če se je Peggy zlagala in v resnici ne pozna gesla, se v polovici primerov ne bo mogla k vhodu vrniti iz pravega tunela in jo bo Victor zalotil pri laži. Večkrat ko se bo Peggy vrnila iz pravega tunela, bolj bo lahko Victor prepričan o tem, da dejansko pozna geslo. Če bosta postopek ponovila 10-krat in bo Peggy vsakič prišla iz pravega tunela, bo verjetnost, da Peggy ne pozna gesla le $1/2^{10} = 1/1024$. Opisani primer dobro ilustrira obe ključni lastnosti dokazov brez razkritja znanja. Victorju med postopkom dokazovanja, ki ga je izvajala Peggy, ni uspelo izvedeti njenega gesla, hkrati pa on s pomočjo njenega dokaza ne more prepričati drugih oseb, da tudi on pozna geslo.

Preverimo zahteve za dokaze brez razkritja znanja:

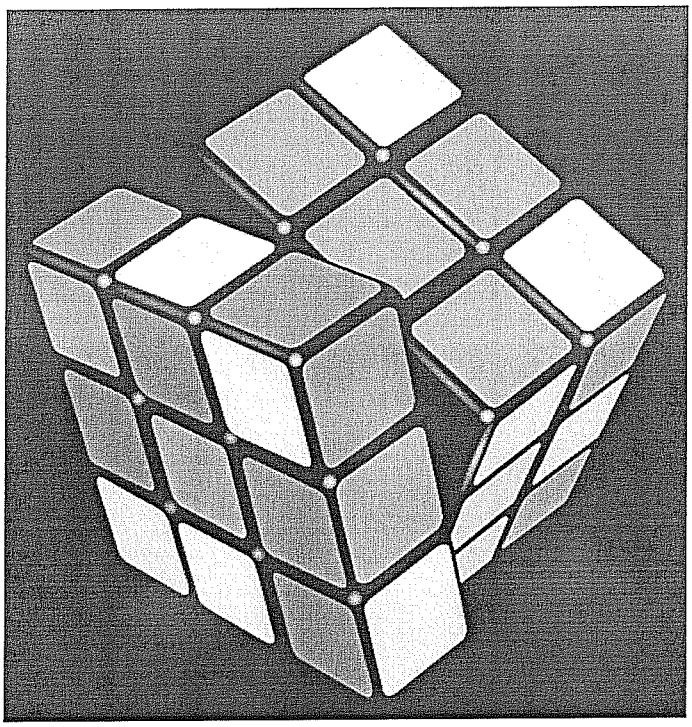
- Tukaj je zahteva o nerazkritju znanja izpolnjena, če Viktor ne more slišati Peggy, ko izreče geslo.

- Da Peggy pozna geslo lahko, kot smo rekli trdimo samo z neko verjetnostjo. A ta verjetnost je lahko poljubno večja od verjetnosti, da nam zaradi ustrezne ureditve atomov v telesu uspe pasti skozi (celo) betonsko ploščo.

- Viktor lahko spet prevara Peggy, če je recimo možno, da se ji neopaženo približa in tako sliši geslo.

- Viktor se lahko le s poljubno majhno verjetnostjo pretvarja, da pozna geslo.

- Polnost je izpolnjena saj je edina stvar, ki jo dokazujemo en bit informacije - ali Peggy pozna geslo ali ne.



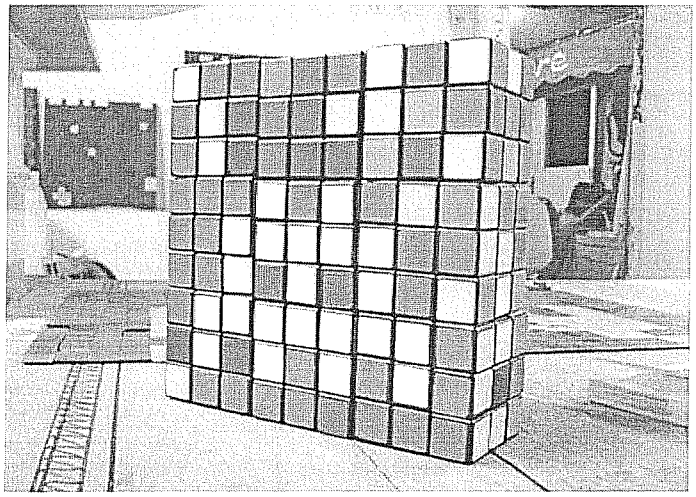
Slika 3.2: Rubikova kocka

3.3 Rubikova kocka

Bolj zapleten primer protokola dokazovanja brez razkritja znanja lahko ponazorimo s pomočjo Rubikove kocke. Predpostavimo, da Peggy zna razrešiti Rubikovo kocko in želi o svoji sposobnsoti prepričati Victorja, noče pa mu pokazati, kako se kocko razreši. Victor pokaže Peggy zmešano Rubikovo kocko A in želi videti dokaz, da jo Peggy zna razrešiti. Peggy nato pokaže Victorju novo zmešano Rubikovo kocko B. Victor mora sedaj izbrati med dvema možnostima:

- od Peggy lahko zahteva, da mu pokaže, kako iz pozicije, v kateri je zmešana kocka B, priti do pozicije zmešane kocke A,
- od Peggy lahko zahteva, da mu pokaže, kako razrešiti kocko B.

Če Peggy ve, kako iz pozicije kocke A priti do pozicije kocke B in nato iz te pozicije do rešitve, lahko uspešno odgovori na obe zahtevi. Če Peggy ne zna razrešiti Rubikove kocke, bi lahko izbrala kocko B na tak način, da bi lahko izpolnila eno od Victorjevih zahtev, ne pa obeh. Večkrat ko Peggy in Victor opravita opisani postopek, bolj je



Slika 3.3: Večja rubikova kocka

lahko Victor prepričan, da Peggy res zna razrešiti Rubikovo kocko. Pri ponavljanju postopka je ključno, da si Peggy izbere vsakič drugo pozicijo zmešane kocke B. Če bi si dvakrat izbrala enako, bi ji Victor lahko postavil obe zahtevi in s tem dobil informacijo o tem, kako rezrešiti kocko A.

Tako Jama Ali Babe kot Rubikova kocka sta primera, pri katerih je rezultat postopka dokazovanja dokaz o znanju. Poznamo pa tudi sorodne protokole, pri katerih je rezultat dokazovanja dokaz o identiteti. V teh primerih protokol zagotavlja, da se nobena tretja oseba ne bi mogla izdajati za Peggy ali Victorja.

Ali so izpolnjene zahteve za dokaze brez razkritja znanja?

- Zahteva o nerazkritju znanja bo izpolnjena, če Viktor ne more videti Peggy, ko preureja kocko.
- Da Peggy zna rešiti kocko lahko trdimo samo s poljubno veliko verjetnostjo.
- Viktor lahko prevara Peggy, če ji lahko vmes ukrade kocko ali kako posname preurejanje.
- Viktorju bo uspelo tretji osebi dokazati, da zna rešiti kocko s poljubno majhno verjetnostjo.
- Polnost je izpolnjena, kot zgoraj.

3.4 Sudoku

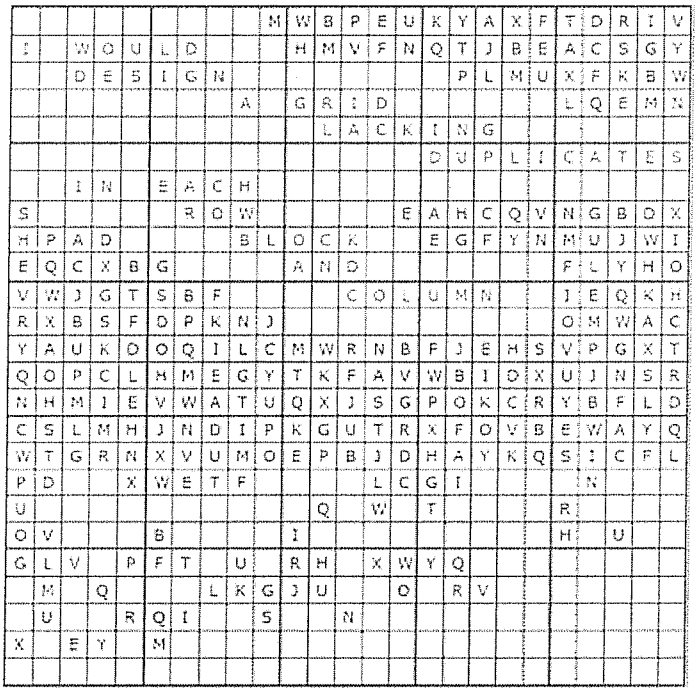
		1						
		2		3				4
			5			6		7
5			1	4				
	7						2	
				7	8			9
8		7			9			
4				6		3		
						5		

Slika 3.4: Klasičen sudkou

Nekoliko bolj matematičen primer dokaza brez razkritja znanja lahko predstavimo s pomočjo sudokuja [6]. Primer sudokuja, ki ga bomo obravnavali, sestavlja mreža 9×9 celic, ki je razdeljena na podmreže velikosti 3×3. Nekatere od celic že imajo vpisana števila od 1 do 9. Naš cilj je tudi v vse ostale celice vpisati števila od 1 do 9 tako, da se bo vsako od števil v vsakem stolpcu, vrstici ali podmreži pojavilo natanko enkrat.

Predpostavimo, da Peggy pozna rešitev danega sudokuja in želi o tem prepričati Victorja, pri tem pa mu noče izdati nobene informacije, ki bi mu lahko pomagala, da sam pride do rešitve. V nadaljevanju bomo opisali protokol, s katerim lahko to doseže.

Še prej velja omeniti, da v splošnem problem reševanja sudokuja po kompleksnosti sodi v razred NP (glej [8]). Znano je, da za vse NP probleme obstajajo dokazi brez razkritja znanja (glej [3]). Do dokaza brez razkritja znanja za sudoku bi lahko prišli tako, da bi najprej problem sudokuja prevedli na enega od NP problemov, za katere poznamo poznamo algoritem dokaza brez razkritja znanja (npr.



Slika 3.5: Abecedni sudoku 25×25

3-obarvljivost), toda rajši bomo navedli kar direkten algoritem, ki ga je lažje implementirati.

Preprost algoritem je sledeč. Peggy izbere permutacijo $\pi \in S_9$ in jo uporabi na svoji rešitvi sudokuja. Očitno je, da bo dobljena razpredelnica še vedno sudoku. Sedaj Peggy zaklene vsako polje permutirane rešitve najprej z Viktorjevim javnim ključem nato pa še svojim zasebnim. Viktor nato izbere eno izmed možnosti:

- izbere enega od stolpcev
- izbere eno od vrstic
- izbere eno od 3×3 polj
- rad bi videl permutirano verzijo originalnega problema.

Če izbere eno izmed prvih treh možnosti Peggy odklene izbrana polja in Viktor preveri ali ustrezajo pogojem sudokuja. Torej če so v danem stolpcu, vrstici ali 3×3 polju vsa števila različna. V zadnjem primeru pa preveri, če so dobljena polja dejansko permutirane začetne vrednosti. Če dobljena polja ne ustrezajo zahtevam,

Viktor dokaz takoj zavrne. V danem koraku dokaza bo Viktor odkril napako vsaj z verjetnostjo $\frac{1}{28}$ (če ima Peggy napako v rešitvi samo na enem mestu, sicer bo ta verjetnost večja). Da bi dosegli željeno verjetnost p s katero lahko trdimo, da Peggy pozna rešitev enostavno izvedemo n korakov, da velja $1 - \frac{27}{28}^n > p$. Omeniti velja, da moram Peggy pri algoritmu paziti, da ne izbere dvakrat iste permutacije, saj s tem lahko preda nekaj informacije o rešitvi.

Na zgoraj opisan način lahko dokažemo količinsko zelo omejeno informacijo. Zelo lahko pa je to shemo razširiti na posplošen sudoku. Ta ima dimenzije $n \times n$, kjer je $n = k^2$ za nek naraven k. Njegova podpolja so velikosti $k \times k$ in vanj vpisujemo števila od 1 do n. Še vedno velja, da se morajo števila v posamezni vrstici, stolpcu ali $k \times k$ polju paroma razlikovati. S tem lahko z uporabo sudokuja dokažemo poljubno trditev. Potrebno jo je le predhodno zakodirati v rešitev nekega sudokuja.

Poglejmo si še primer izvedbe podobnega algoritma v fizični obliki. Tukaj je veliko težje zakleniti polja v neke škatle in jih predati Victorju, saj ne moremo biti gotovi, da jih Viktor ne bo mogel odpreti. Zato sta Moran in Naor [9] predlagala, da se v fizičnem svetu osredotočimo na zaščito, ki zagotavla, da bomo možno odprtje odkrili. Tak primer so zapečatene kuverte in scratch off kartice (kartice s premazom, ki ga je potrebno odstraniti, da vidimo napisano pod njim).

- Peggy položi na vsako polje tri zapečatene kuverte. Na polja kjer so v začetnem problemu že vnesena števila položi tri že odprte kuverte s pravilno vrednostjo v njih.

- Za vsako vrstico, stolpec in $k \times k$ polje si Viktor naključno izbere eno izmed treh kuvert na izbranih poljih.

- Peggy tako izbrane vrstice, stolpce in $k \times k$ polja zbere na $3n$ kupčkov in vsakega posebej dobro zmeša. Tako premešane vrne Viktorju.

- Viktor sedaj odpre kuverte in preveri, ali so v vsakem kupčku sama različna števila.

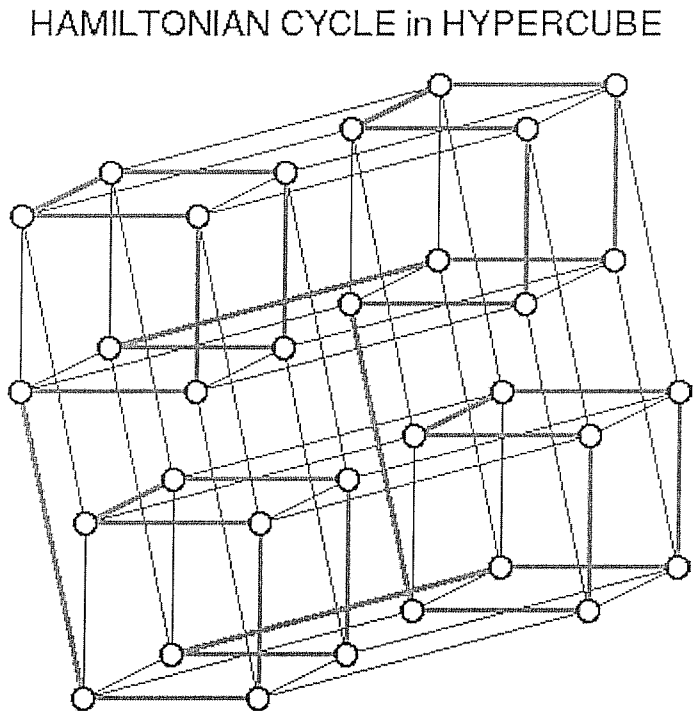
Trditev 3.4.1 *Tukaj je verjetnost, da sprejmemo napačen dokaz največ* $\frac{1}{3}$.

Dokaz. Predpostavimo, da Peggy ne pozna rešitve za dan sudoku. Potem jo ob Viktor vedno razkrinkal, če bo postavila na vsako polje tri kuverte z isto vrednostjo. Edini način, da ga lahko prevara je, da na neko polje postavi kuverte z različnimi vrednostmi. Naj bo to polje a. To pomeni, da mora biti vsaj ena vrednost y različna od ostalih. Predpostavimo, da je Viktor za vsa ostala polja že dodelil kuverte stolpcem, vrsticam in $k \times k$ poljem. Potreben pogoj, da lahko Peggy Viktorja prevara je, da glede na izbire kuvert za stolpce, vrstice in $k \times k$ polja, obstaja eno izmed teh, ki potrebuje y, da zapolni svoj seznam števil $\{1, 2, \ldots, n\}$. Verjetnost, da sedaj dodeli kuverto z vrednostjo y vrstici, stolpcu ali podpolju, ki ga potrebuje, je enaka $1/3$. □

- Zahteva o nerazkritju znanja je izpolnjena, če pri računalniški izvedbi zaupamo kriptografiji z javnimi ključi, v realnem primeru pa moramo zaupati, da se ne da odpreti kuvert, brez da bi se to opazilo.
- Da Peggy pozna rešitev je še enkrat dokazano le z veliko verjetnostjo.
- Viktor ob dobri izvedbi protokola ne more prevarati Peggy.
- Viktor lahko le z zelo majhno verjetnostjo dokaže, da pozna rešitev pred tretjo osebo.
- Polnost je izpolnjena za precej "velik"jezik. Poljubno število lahko zakodiramo v rešitev posplošenega sudokuja in tako dokažemo poljubno dolgo končno trditev.

3.5 Hamiltonskost

Do še enega matematičnega primera dokaza brez razkritja znanja lahko pridemo pri ugotavljanju hamiltonske lastnosti grafov. Pokazati, da je graf hamiltonski je v splošnem NP-poln problem. Denimo, da Peggy ve, da je graf G hamiltonski in celo pozna hamiltonski cikel C v njem. O tem svojem znanju želi prepričati Victorja, noče pa, da bi lahko Viktor na osnovi njenega dokaza kaj lažje sam poiskal hamiltonski cikel v grafu G.



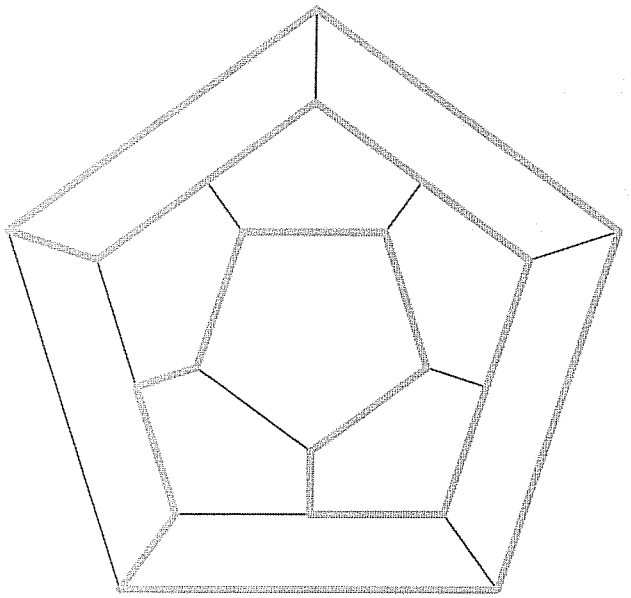
Slika 3.6: hamiltonski cikel v hiperkocki

Peggy dokaz začne tako, da si izbere avtomorfizem π grafa G. Izbrani avtomorfizem uporabi na grafu G in dobi graf $H = \pi(G)$, ki ga potem pošlje Viktorju. Viktor ima sedaj na voljo dve možnosti:

- od Peggy lahko zahteva, da mu pokaže hamiltonski cikel v grafu H,
- od Peggy lahko zahteva, da mu izda avtomorfizem π.

Če Peggy zna poiskati hamiltonski cikel v grafu G, potem bo lahko izpolnila obe Viktorjevi zahtevi. Če temu ni tako, pa bo lahko izpolnila kvečjemu eno od njih. Večkrat ko bosta ponovila postopek, bolj bo lahko Viktor prepričan, da Peggy res pozna hamiltonski cikel v grafu G. Opisani dokaz pa je zares smiseln le v primeru, ko ima graf G dovolj vozlišč in dovolj veliko grupo avtomorfizmov. Peggy namreč ne sme dvakrat uporabiti istega avtomorfizma π grafa G, saj bi tako lahko Viktorju predala celotno informacijo o hamiltonskem ciklu v grafu.

Opisani dokaz bi v praksi lahko izvedli tudi tako, da bi Peggy graf G narisala na prozorno folijo, vozlišča pa označila z velikimi krogi. Nato bi vzela velik pokončno stoječ kos lepenke in vanj izrezala luknjo, ki bi bila po velikosti nekoliko manjša



Slika 3.7: Hamiltonski cikel v dodekaedru

od posameznega vozilišča. Peggy bi najprej Viktorju pokazala graf G, tako da bi si ta zapomnil število vozlišč $N = |V(G)|$. Nato bi stopila za lepenko in eno od vozlišč grafa centrirala na luknjo v njej. Viktor bi stal na drugi strani lepenke in bi s poljubno izbrano barvo v centrirano vozlišče napisal številko 1. Nato bi Peggy foljo z grafom premaknila tako, da bi bila luknja centrirana na naslednje vozlišče v hamiltonskem ciklu, pri tem pa bo pazila, da bo luknja med premikom ves čas centrirana na povezavi med vozliščema. Viktor bo nato novo vozlišče pobarval. Peggy bo sedaj zarotirala folijo z grafom za naključno izbran kot in jo premaknila v naslednje vozlišče. Postopek bo ponavljala toliko časa, dokler ne bo prišla nazaj v vozlišče, označeno z 1. Viktor bo lahko s precejšnjo gotovostjo verjel, da mu Peggy res pokazala hamiltonski cikel, če bo poleg prvega obarval še $N - 1$ vozlišč in ga Peggy ne bo nikoli zapeljala v že pobarvano vozlišče.

Zahteve:

- Zahteva o nerazkritju znanja je izpolnjena, če verjamemo, da je problem izomorfizma grafa zelo težak.

- Da Peggy pozna rešitev je dokazano le z veliko verjetnostjo.

- Za Viktorja bo v računalniški različici nemogoče prevarati Peggy, če ne more rešiti problema izomorfizma. V realni različici pa si lahko seveda pomaga z nasiljem ali kakšnimi vohunskimi pripomočki.
- Viktor se lahko pred tretjo osebo pretvarja, da pozna rešitev le če po nesreči odkrije hamiltonski cikel, kar pa pomeni, da potem pozna rešitev.
- Podobno, kot v prejšnjem primeru lahko v Hamiltonski cikel zakodiramo poljubno število in tako dokažemo poljubno trditev.

Ta primer lahko zelo preprosto prevedemo na poljuben težak problem v teoriji grafov namesto Hamiltoskosti. Lahko bi recimo uporabili 3-obarvljivost, $L(2,1)$-barvanje ali karkoli podobnega.

3.6 Feige-Fiat-Shamir dokaz identitete

Ta primer bo od obravnavanih najbolj matematičen in strikten. Najprej je potrebno opraviti predhodne izračune:

Neodvisna oseba zgenerira naključen modul n (512-1024 bitov), ki je produkt dveh velikih praštevil. Nato zgenerira še zasebni in javni ključ za Peggy tako, da izbere število v, ki je kvadratni ostanek $\mod n$ (npr. $x^2 \equiv v \mod n$ ima rešitev in $v^{-1} \mod n$ ne obstaja). To število v je javni ključ. Zasebni ključ je potem njamanjši s za katerega velja $s = \sqrt{\frac{1}{v} \mod n}$.

Identifikacijski protokol je sledeč:

- Peggy izbere naključen r, kjer $r|n$. Nato izračuna $x = r^2 \mod n$ in x pošlje Victorju.
- Victor pošlje Peggy naključen bit b.
- Če je $b = 0$ Peggy pošlje Victorju r, če je $b = 1$ pa mu pošlje $y = r \cdot s \mod n$
- Če je $b = 0$ Victor preveri, da velja $x \equiv r^2 \mod n$, kar dokazuje, da Peggy pozna $\sqrt{x}$. Če je $b = 1$ pa preveri, da je $x \equiv y^2 \cdot v \mod n$, kar dokazuje, da Peggy pozna $\sqrt{\frac{x}{v}}$.

Vse zahteve za dokaze brez razkritja znanja so tukaj najbolje izpolnjene. Če se želi tretja oseba izdajati za Peggy lahko izbere tak r, da bo lahko odgovorila na Viktorjevo vprašanje, če ta pošlje bit 1 ali 0, ne more pa se pripraviti na oba primera hkrati. Torej se bo izdala z verjetnostjo 1/2 v vsakem krogu. Viktor se prav tako ne more pretvarjati, da pozna Peggyjina števila, saj bo naključen bit, ki mu ga pošlje nov preverjevalec le v polovici primerov enak kot bit, ki ga je prej Viktor poslal Peggy.

Peggy mora pri tem protokoli paziti, da nikoli ne uporabi istega r dvakrat. Če bi to storila, bi lahko Viktor poslal oba bita in tako prejel oba odgovora. Potem bi lahko, če zbere veiko takih parov poskušal nekoga drugega prepričati, da je Peggy.

Poglavje 4

Interaktivni Turingovi stroji

Interaktiven Turingov stroj [3] je deterministično Turingov stroj s šestimi trakovi. Ti trakovi so:

- vnosni trak (samo branje)
- naključen trak (samo branje)
- delovni trak (branje in pisanje)
- pisalni komunikacijski trak
- bralni komunikacijski trak
- izhodni trak (samo branje)

Niz znakov na vnosnem traku je osnovni vnos za problem (input). Vsebina komunikacijskih trakov so sporočila, ki si jih stroja izmenjata. Neskončno vsebino naključnih trakov si lahko predstavljamo kot izid neskončnega števila metov pravičnega kovanca. Izhod je niz znakov, ki ga najdemo na izhodnem traku po tem, ko se stroja ustavita.

Kompleksnost Turingovega stroja se meri glede na vhodne podatke. Za Turingov stroj M rečemo, da je polinomski, če obstaja tak polinom p, da je število korakov, ki jih Turingov stroj M izvede na vhodnem podatku x največ $p(|x|)$ ne glede na vsebino naključnega komunikacijskega traku.

4.0.1 Skupni izračuni dveh interaktivnih Turingovih strojev

Za dva interaktivna Turingova stroja pravimo, da sta povezana, če se ujemata v vnosnem traku in je pisalni komunikacijski trak prvega enak bralnemu komunikacijskemu traku drugega (in obratno). Ostali trakovi (naključni, delovni izhodni) so lahko različni.

Skupen izračun povezanega para interaktivnih Turingovih strojev na skupnem vnosu x je zaporedje parov. Vsak par je sestavljen iz lokalne konfiguracije obeh strojev. V vsakem paru takih lokalnih konfiguracij je aktiven natanko eden od obeh strojev.

Če se v postopku izračuna ustavi eden od povezanih interaktivnih Turingovih strojev, pravimo, da sta se zaustavila oba.

4.0.2 Časovna zahtevnost interaktivnega Turingovega stroja

Interaktiven Turingov stroj A ima časovno zahtevnost $t : \mathbb{N} \to \mathbb{N}$, če za vsak interaktiven Turingov stroj B in vsak niz x velja naslednje: stroj A, ki v povezavi s strojem B deluje na skupnem vnosu x, se vsakič (neodvisno od vsebine naključnih trakov stroja A in B) zaustavi v največ $t(|x|)$ korakih.

4.0.3 Časovna zahtevnost dokaza brez razkritja znanja

Literatura

[1] P. van Oorschot, A. Menezes, S. Vanstone: Handbook of applied cryptography, (1996).

[2] H. Aronsson: Zero knowledge protocols and small systems.

[3] O. Goldreich, S. Micali, A. Wigderson: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems, Journal of the ACM, **38(3)** (1991), 691–729.

[4] O. Goldreich: Foundations of cryptography (Fragments of a book), Weizman institute of science (1995).

OdedGoldreich,SilvioMicaliandAviWigderson, ProofsthatYieldNothingButtheirValidity [9] andaMethodologyofCryptographicProtocolDesign,J.oftheACM38,1991,pp.691729.

[5] J. Quisquater, Myriam Quisquater, Muriel Quisquater, Michaa"el Quisquater, L. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, S. Guillou, T. Berson: How to explain zero-knowledge protocols to your children, Lecture notes in computer science **435** (1989), 20–24.

[6] R. Gradwohl, M. Naor, B. Pinkas, G. N. Rothblum: Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles, Proc. of Fun with Algorithms 2007, LNCS **4475** (2007), Springer-Verlag, 166–182.

[7] D. Stinson, Cryptography: Theory and practice, Third edition, (2006).

[8] T. Yato: Complexity and completeness of finding another solution and its application to puzzles, Master thesis, Univ. of Tokyo, Dept. of Information Science, Jan 2003.

[9] T. Moran, M. Naor: Basing cryptographic protocols on tamper-evident seals, Proceedings of the 32nd International Colloquium on Automata, Languages and Programming(ICALP) (2005).