Tijana Jakšić i Pavle Tepavčević

Problemi merenja novčića

U ovom radu smo postavili i rešili modifikaciju Šapavalovljevog problema merenja novčića. Problem je generalizovan na n *novčića od kojih je* f *falično i merenja se sprovode digitalnom vagom umesto terazijama. Osim toga, nalazimo potreban broj merenja pomoću terazija za utvrđivanje da li faličnih novčića ima tačno* m*, za neko unapred zadato* m.

Uvod

Problemi merenja novčića su većini matematičara poznati još od prvog susreta sa matematikom. Prvi ovakav problem postavio je Grosman 1945. godine, i on je glasio (Grossman 1945):

> Dato je 12 novčića, od kojih je barem 11 iste težine. Kako nakon 3 merenja terazijama utvrditi koji je novčić faličan, da li je lakši ili teži, ili utvrditi da ne postoji (to jest da su svi iste težine)?

Ovaj problem je u matematičkom svetu odmah postao klasika i danas postoje brojne generalizacije i varijacije na temu problema merenja novčića. U radu Gaja i Novakovskog nalazi temeljan pregled rezultata postignutih na ovu temu do 1995. godine, kada je rad objavljen (Guy i Nowakowski 1995).

Novi problem merenja novčića se pojavio 2007. godine na Šestom međunarodnom matematičkom turniru „Kolmogorov” (Kolmogorov 2007). Ovaj problem je ubrzo postao popularan zato što je prvi koji se ne bavi otkrivanjem identiteta faličnih novčića, nego njegovim očuvanjem, uz otkrivanje broja falsifikata. Problem postavlja pitanje kako otkriti drugoj osobi broj faličnih novčića bez otkrivanja njihovog identiteta koristeći terazije.

Glavni deo našeg rada jeste definisanje modifikacije originalnog problema iz 2007. godine, tako da se za merenja koristi digitalna vaga umesto terazija, i postavljamo pitanje koliko je najmanje potrebno merenja da bi se drugoj osobi otkrio broj faličnih novčića. Takođe nalazimo po-

Tijana Jakšić (2001), Pančevo, učenica 4. razreda Gimnazije „Uroš Predić” u Pančevu

Pavle Tepavčević (2002) Novi Sad, učenik 3. razreda Gimnazije „Jovan Jovanović Zmaj” u Novom Sadu

MENTOR: Branislav Šobot, student Prirodno-matematičkog fakulteta Univerziteta u Novom Sadu

treban broj merenja pomoću terazija za utvrđivanje da li faličnih novčiča ima tačno m, za neko unapred zadato m.

U radu ukupan broj novčića označavamo sa n dok ukupan broj faličnih novčića označavamo sa f. Masu ispravnog i faličnog novčića smo označili sa m_r i m_f, respektivno, dok smo njihovu razliku označili sa Δm. Sa n_i i f_i smo označili ukupan broj novčića koji se nalazi na vagi i ukupan broj faličnih novčića koji se nalazi na vagi u i-tom merenju, respektivno. Neka je M_i masa koju pokazuje digitalna vaga u i-tom merenju, a M_i' masa koju bi pokazivala digitalna vaga da se u i-tom merenju nalaze samo ispravni novčići. Njihovu razliku smo označili sa Δm_i.

Metod

Šapavalovljev problem

Problem koji je Aleksandar Šapavalov postavio 2007. godine glasi:

> Dato je 80 novčića, od kojih je 3 falično. Osobi A je poznat identitet svakog novčića. Osoba B ne zna da li imaju 2 ili 3 falična novčića. Kako osoba A pomoću terazija, i bez otkrivanja identiteta novčića, može da ubedi osobu B da se u skupu nalaze tačno 3 falična?

Osvrnimo se na to zašto je ovaj problem toliko poseban. Prvi problemi merenja novčića su se pojavili oko 1945. i bavili su se tačnim identifikovanjem jednog faličnog novčića u gomili. Kasnije su se javljale generalizacije kao pronalaženje više faličnih novčića, identifikovanje novčića kada je prisutno više različitih težina i slični problemi.

Svi ovi problemi imaju za cilj otkrivanje identiteta novčića u što manje koraka. Šapavalovljev problem je prvi problem koji se bavi očuvanjem informacija, ne njihovim otkrivanjem.

Asimptotsko ponašanje potrebnog broja merenja terazijama

U radu (Diaco 2016) se pronalazi donja granica potrebnog broja merenja terazijama za utvrđivanje da li je f umnožak nekog unapred zadatog broja m.

Skup novčića se može predstaviti $\{0, 1\}$-vektorom $x \in \{0, 1\}^n$. Potrebno je numerisati novčiće brojevima od 1 do n, a i-toj koordinati vektora, x_i, dodeliti vrednost po pravilu da je $x_i = 1$ ako je i-ti novčić ispravan, a $x_i = 0$ inače.

Takođe, osobinu koju ispitujemo na skupu novčića možemo predstaviti funkcijom. Ako želimo da odredimo koliko ima falsifikata u datom skupu novčića, funkcija će imati oblik $f : \{0,1\}^n \to \mathbb{N}$, to jest vektoru koji predstavlja novčiće će dodeliti prirodan broj, broj falsifikata u skupu. Kodomen funkcije zavisi od osobine koja se ispituje. Dalje, uvedimo definiciju osetljivosti funkcije, koju je Purdi postavio u (Purdy 2011).

Definicija 1. Neka $f:\{0,1\}^n \to \mathbb{N}$, i neka . Za $1 \le i \le n$, neka je x^i vektor x sa i-tom koordiatom zamenjenom (dakle ako se na i-tom mestu u vektoru x nalazila jedinica onda se na i-tom mestu u vektoru x^i nalazi nula i obrnuto). Osetljivost funkcije f u tački x, u oznaci $\sigma_x(f)$, je broj takvih $1 \le i \le n$, gde važi $f(x^i) \ne f(x)$. Prosečna osetljivost funkcije f, u oznaci $\alpha(f)$, je $\frac{\sum \sigma_x(f)}{2^n}$.

Primer 2. Želimo da proverimo da li u skupu ima falsifikata. Definišimo funkciju $f:\{0,1\}^n \to \mathbb{N}$ na sledeći način:

$$f(x) = \begin{cases} 1, & \text{ako postoji nula u vektoru } x \\ 0, & \text{inače} \end{cases}.$$

Posmatrajmo kada se može desiti $f(x^i) \ne f(x)$. Očigledno ako je broj nula u vektoru x dva ili više onda će se nakon promene neke koordinate tog vektora opet u njemu nalaziti bar jedna nula pa će samim tim funkcija ostati nepromenjena. Ako se u vektoru x nalazi tačno jedna nula, recimo da se nalazi na mestu a, onda će važiti $x(x^i) = 1 = f(x)$, za $i \ne a$ i $f(x^a) = 0 = f(x)$. Dakle za svaki vektor x sa tačno jednom nulom postoji tačno jedno i takvo da važi $f(x) \ne f(x^i)$. Drugim rečima osetljivost funkcije f u tački x je $\sigma_x(f) = 1$. Ovakvih vektora x ima n.

Ako se u vektoru x ne nalazi ni jedna nula, onda uvek važi $f(x^i) \ne f(x)$, jer se u vektoru x^i uvek nalazi tačno jedna nula, pa je $\sigma_x(f) = n$. Postoji samo jedan vektor x koji nema ni jednu nulu u sebi.

Sada možemo izračunati prosečnu osetljivost funkcije f:

$$\alpha(f) = \frac{\sum \sigma_x(f)}{2^n} = \frac{0+0+\ldots+1\cdot n + n\cdot 1}{2^n} = \frac{n}{2^{n-1}}.$$

Definicija 3. $\Omega\big(f(n)\big)$ je skup svih funkcija g takvih da postoji $M \in \mathbb{R}$ i postoji x_0 tako da za svako $x \ge x_0$ važi $|g(x)| \ge M \cdot f(x)$. Iako je $\Omega\big(f(n)\big)$ skup, često se zapisuje $g(n) = \Omega\big(f(n)\big)$ umesto $g(n) \in \Omega\big(f(n)\big)$.

Teorema 4 je jedan od rezultata Purdijevog rada (Purdy 2011). Ona određuje asimptotsko ponašanje potrebnog broja merenja za određivanje neke osobine skupa novčića preko prosečne osetljivosti funkcije koja opisuje traženu osobinu.

Pre navođenja teoreme potrebno je napomenuti da je *slepi algoritam* svaki algoritam čiji tok ne zavisi od osobina podataka, odnosno koraci algoritma su poznati pre početka izvršavanja i nezavisni od ulaznih parametra i međurešenja. Suprotno tome, postoje *prilagodljivi algoritmi* kod kojih postoje koraci koji se izvršavaju samo ako je prethodno međurešenje određene vrednosti.

Teorema 4. Neka je svojstvo skupa novčića koje se ispituje predstavljeno funkcijom $f:\{0,1\}^n \to \mathbb{R}$. Svaki slepi algoritam merenja novčića za utvrđivanje f mora upotrebiti $\Omega\left(\alpha(f)/\sqrt{n}\right)$ merenja, gde je $\alpha(f)$ prosečna osetljivost funkcije f.

Rezultati

Šapavalovljev problem sa digitalnom vagom

U ovom odeljku definišemo našu modifikaciju Šapavalovljevog problema koja koristi digitalnu vagu i pronalazimo potreban broj merenja da se taj problem reši. Koristeći vagu s terazijama, moguće je odabrati dva različita skupa novčića i uporediti ih, odnosno saznati koji je skup teži ili saznati da su jednaki. Kada kažemo da merimo digitalnom vagom, biramo jedan skup novčića i dobijamo tačnu informaciju o njegovoj masi.

Sledi modifikacija Šapavalovljevog problema definisana u ovom radu:

> Dato je n naizgled identičnih novčića, od kojih je f falično, pri čemu je $0 < f < n$. Svi ispravni novčići su međusobno iste mase i svi falični su međusobno iste mase, ali su falični lakši od ispravnih. Osobi A je poznat identitet svakog novčića. Osoba B zna masu ispravnog novčića, ali ne zna ni njihove identitete ni broj faličnih. Koliko je merenja potrebno da osoba A pomoću digitalne vage, bez otkrivanja identiteta novčića, ubedi osobu B da u skupu ima tačno f faličnih?

Teorema 5. Osoba A ne može u jednom merenju ubediti osobu B u broj faličnih novčića, bez otkrivanja identiteta faličnih novčića.

Dokaz.

Posmatrajmo slučajeve:

1. Svi novčići učestvuju u merenju

Na vagi će biti očitana masa lakša od $m_r \cdot n$, gde je m_r masa ispravnog novčića. Kako osobi B nije poznata masa faličnog novčića, onda su mogući parovi:

$$(f, m_f) \in \left\{ \left(1,\ M-(n-1)m_r\right), \left(2, \frac{M-(n-1)m_r}{2}\right), \ldots, \left(n-1, \frac{M-(n-(n-1))m_r}{n-1}\right) \right\}$$

gde je M masa koju pokazuje vaga u prvom, odnosno ovde jedinom merenju.

2. Ne učestvuju svi novčići u merenju

Ponovo nije moguće jednoznačno utvrditi broj faličnih novčića, zato što svaki neizmeren novčić može i da bude ispravan i da bude faličan.

Dakle, osoba A ne može ubediti osobu B u broj faličnih novčića u jednom merenju. $\square$

Dokaz prethodne teoreme je sličan ovome i u slučaju kada su falični novčići teži od ispravnih.

Teorema 6. Osoba A može ubediti osobu B u broj faličnih novčića bez otkrivanja njihovog identiteta u dva merenja za $2 < f < n-1$.

Dokaz. Ukupan broj novčića postavljen u prvom, odnosno u drugom merenju obeležavamo sa n_1, odnosno n_2. Na prvo merenje je potrebno staviti $f-1$ faličnih i 1 ispravan novčić. To je ukupno $n_1 = f-1+1 = f$ novčića prisutnih u prvom merenju. Masa koju vaga pokazuje biće obeležena sa M_1. Na drugo merenje potrebno je staviti sve ostale novčiće. Masa koju vaga pokazuje biće obeležena sa M_2. Kako osoba B zna masu ispravnog novčića, poznato mu je koliku bi masu pokazivala vaga u prvom i drugom merenju da su na vagu bili postavljeni isključivo ispravni novčići. Označimo te mase M_1' i M_2', respektivno. Primetimo da je $M_1' = m_r \cdot n_1$ i $M_1' = m_r \cdot n_2$, gde je m_r masa ispravnog novčića, a n_1 i n_2 brojevi novčića u prvom, odnosno drugom merenju. Neka su:

$$\Delta M_1 = M_1' - M_1,$$

$$\Delta M_2 = M_2' - M_2.$$

Neka je f_1 broj faličnih novčića u prvom merenju, a f_2 u drugom. Primetimo da je $f_1 + f_2$ jer smo svaki novčić merili tačno jednom. Odavde je osobi B poznato da važi $\Delta M_1 = \Delta m \cdot f_1$ i $\Delta M_2 = \Delta m \cdot f_2$, gde je Δm razlika mase jednog ispravnog i jednog faličnog novčića. Deljenjem ΔM_1 i ΔM_2 se dobija racionalan broj, zato što se Δm skrati, a f_1 i f_2 su prirodni brojevi:

$$\frac{\Delta M_1}{\Delta M_2} = \frac{\Delta m \cdot f_1}{\Delta m \cdot f_2} = \frac{f_1}{f_2}.$$

Kada osoba B dobije nesvodljiv razlomak (nazovimo ga $\frac{r}{s}$), ona još uvek ne zna da su f_1 i f_2 bili uzajamno prosti, to jest da li važi $f_1 = r$ i $f_2 = s$. Pretpostavimo da f_1 i f_2 nisu uzajamno prosti. Tada $\text{NZD}(f_1, f_2) > 1$. Onda bi se u prvom merenju nalazilo barem $2r$ novčića. Nama je poznato da je osoba B za r dobila $f - 1$, kao i da se na prvom merenju nalazilo ukupno $n_1 = f$ novčića. Pošto je $2 \cdot (f - 1) > f$ za $f > 2$, osoba B zaključuje da je $r = f_1$, $s = f_2$, i $f = f_1 + f_2$. Pri ovoj proceduri se nije otkrio identitet ni jednog novčića. Dakle, koristeći ovu strategiju osoba A može ubediti osobu B u broj faličnih novčića bez otkrivanja njihovog identiteta u dva merenja za $2 < f < n - 1$. □

Kako teorema 5 pokazuje da nije moguće pokazati broj faličnih novčića u jednom merenju, dva zaista jeste najmanji broj merenja potreban da se osoba B ubedi u broj faličnih novčića.

Teorema 6 se slično dokazuje i u slučaju da su falični novčići teži od ispravnih.

Strategija ne funkcioniše za $f \in \{1, 2, n - 1\}$. Ako je $f = 1$ onda osoba B neće moći da izračuna količnik $\frac{\Delta M_1}{\Delta M_2}$ jer je u drugom merenju dobijena masa bila jednaka očekivanoj, to jest $\Delta M_2 = 0$. S druge strane, osoba B će se dvoumiti da li se u prvom merenju nalazi 1 ili 2 falična novčića, pa su moguće sledeće trojke:

$$(f_1, f_2, m_f) \in \left\{ (1, 0, M_1 - m_r), (2, 0, \frac{M_1}{2}) \right\}.$$

Ako je $f = 2$ onda osoba B neće moći da zaključi da li je $f = 2$ ili $f = 4$, jer su moguće trojke:

$$(f_1, f_2, m_f) \in \left\{(1,1,M_1 - m_r),(2,2,\frac{M_1}{2})\right\}.$$

Ako je $f = n-1$ onda će se u drugom merenju nalaziti samo falični novčići, što znači da će, nakon postupka opisanog u teoremi 6, osoba B zaključiti da je $f_2 = n-2 = n_2$ a time bi se otkrio identitet tih $n-2$ novčića, što nije dozvoljeno.

Modifikovani Šapavalovljev problem sa digitalnom vagom

U ovom odeljku takođe nalazimo donju granicu broja merenja u kojoj osoba A može ubediti osobu B u broj faličnih novčića bez otkrivanja njihovog identiteta pomoću digitalne vage, ali ovog puta osoba B ne zna ni masu faličnog, ni masu ispravnog novčića. Tako formulacija problema treba da glasi:

> Dato je n naizgled identičnih novčića, od kojih je njih f falično ($0 < f < n$). Svi ispravni novčići su međusobno iste mase, kao što su i svi falični novčići su međusobno iste mase, ali su falični lakši od ispravnih. Osobi A je poznat identitet svakog novčića. Osoba B ne zna ni masu ispravnog novčića, ni njihove identitete ni broj faličnih. Koliko je merenja osobi A potrebno da pomoću digitalne vage, bez otkrivanja identiteta faličnih novčića, ubedi osobu B da u skupu ima tačno f faličnih novčića?

Teorema 7. Osoba A može ubediti osobu B da ima f faličnih novčića u 3 merenja ako osobi B nije poznata masa ispravnog ili masa faličnog novčića, za $2 < f < n-1$.

Dokaz. U prvom merenju postavimo jedan ispravan novčić. U drugom merenju postavimo $f-1$ faličan i jedan ispravan novčić. Nakon prvog merenja osoba B neće moći da zaključi da li je meren ispravan ili faličan novčić. Nakon drugog merenja će primetiti da važi $M_1 \cdot n_2 > M_2$ (M_1 je masa koju vaga pokazuje masa u prvom merenju, M_2 masa u drugom, a n_2 broj novčića u drugom merenju). Ovo je moguće jedino ako je novčić meren u prvom merenju ispravan. Na treće merenje treba postaviti sve novčiće koji nisu učestvovali u drugom. Ovako je osoba B dobila sve informacije kao i u teoremi 6 i na isti način može da dođe do informacije o broju faličnih novčića. □

U ovoj konstrukciji osoba B je odredila falične novčiće na osnovu toga što su oni lakši od ispravnih. Ako želimo možemo definisati falične novčiće kao one teže i na analogan način bismo konstruisali tri merenja pomoću kojih osoba A može ubediti osobu B u broj faličnih novčića.

Teorema 7 pokazuje da je moguće pokazati broj faličnih novčića u modifikovanom Šapavalovljevom problemu u 3 merenja. Sada je potrebno proveriti da li je moguće to uraditi u 2 merenja. Time se bavi teorema 11.

Definicija 8. Gustina *i*-tog merenja obeležena je sa ξ_i i definišemo je kao $\xi_i = \frac{M_i}{n_i}$, gde je M_i masa *i*-tog merenja i n_i broj novčića u *i*-tom merenju.

Lema 9. Ako dva merenja imaju istu gustinu, onda važi $\frac{f_1}{n_1} = \frac{f_2}{n_2}$.

Dokaz. Lema sledi iz sledećeg niza jednakosti:

$$\xi_1 = \xi_2$$

$$\frac{M_1}{n_1} = \frac{M_2}{n_2}$$

$$\frac{m_r \cdot (n_1 - f_1) + m_f \cdot f_1}{n_1} = \frac{m_r \cdot (n_2 - f_2) + m_f \cdot f_2}{n_2}$$

$$n_2 \cdot \left(m_r \cdot (n_1 - f_1) + m_f \cdot f_1 \right) = n_1 \cdot \left(m_r \cdot (n_2 - f_2) + m_f \cdot f_2 \right)$$

$$n_1 \cdot n_2 \cdot m_r - m_r \cdot n_2 \cdot f_1 + m_f \cdot f_1 \cdot n_2 = n_1 \cdot n_2 \cdot m_r - m_r \cdot n_1 \cdot f_2 + m_f \cdot f_2 \cdot n_1$$

$$n_2 \cdot f_1 \cdot (m_f - m_r) = n_1 \cdot f_2 \cdot (m_f - m_r)$$

$$n_2 \cdot f_1 = n_1 \cdot f_2$$

$$\frac{f_1}{n_1} = \frac{f_2}{n_2}.$$

□

Lema 10. Ako važi $\xi_1 < \xi_2$ onda mora važiti $\frac{f_1}{n_1} > \frac{f_2}{n_2}$.

Dokaz prethodne leme je analogan dokazu leme 9.

Teorema 11. Nije moguće ubediti osobu B u broj faličnih novčića u 2 merenja ako osobi B nije poznata masa ispravnog ili masa faličnog novčića ako $f > 0$.

Dokaz. Pretpostavimo da je osoba A napravila samo dva merenja. Posmatrajmo slučajeve:

1. Brojevi novčića u oba merenja su jednaki, odnosno $n_1 = n_2$

a) Jednake su i gustine merenja $\xi_1 = \xi_2$.

Onda važi $f_1 = f_2$, ali f_1, odnosno f_2 mogu biti bilo koji brojevi od 0 do $n_1 - 1$ to jest $n_2 - 1$. Kako je masa koju pokazuje vaga u prvom merenju veća od mase koju bi pokazivala das u se na njoj nalazili samo falični novčići, imamo: $n_1 m_f < M_1 \Rightarrow m_f < \frac{M_1}{n_1}$. Dokažimo da se osoba B dvoumi ako je $m_f < \frac{M_1}{n_1 + 1}$.

Važe jednakosti: $M_1 = f_1 m_f + (n_1 - f_1) m_r$ i $M_2 = f_2 m_f + (n_2 - f_{21}) m_r$ što je ekvivalentno sa $M_1 = f_1 m_f + (n_1 - f_1) m_r$, jer je druga jednakost umnožak prve. Možemo izraziti m_r preko f_1, f_2 i m_f, odnosno preko f_1, f_2 i $M_1 n_1$. Dakle moguće su četvorke:

$$(f_1, f_2, m_r, m_f) \in \left\{ \left(0, 0, \frac{M_1}{n_1 + 1}, \frac{M_1}{n_1}\right), \left(1, 1, \frac{M_1}{n_1 + 1}, \frac{M_1 n_1}{(n_1 - 1)(n_1 + 1)}\right), \ldots, \right.$$

$$\left. \left(n_1 - 1, n_1 - 1, \frac{M_1}{n_1 + 1}, M_1 \frac{n_1 + 1 - (n_1 - 1)}{\big(n_1 - (n_1 - 1)\big)(n_1 + 1)}\right) \right\}.$$

b) Gustine merenja nisu jednake. Bez umanjenja opštosti recimo da je $\xi_1 > \xi_2$, tj. $f_1 < f_2$.

Dokažimo da je moguće da se B dvoumi kada je $f_2 = n_2$, to jest kada su svi novčići u lakšoj gomili falični. Tada f_1 može biti bilo koji broj iz skupa $\{0, 1, \ldots, n_1 - 1\}$, pa f nije jednoznačno određeno. Moguće su sledeće četvorke:

$$(f_1, f_2, m_r, m_f) \in \left\{ \left(0, n_2, \frac{M_2}{n_2}, \frac{M_1}{n_1}\right), \left(1, n_2, \frac{M_2}{n_2}, \frac{M_1 - \frac{M_2}{n_2}}{n_1 - 1}\right), \right.$$

$$\left. \left(2, n_2, \frac{M_2}{n_2}, \frac{M_1 - \frac{2}{n_2} M_2}{n_1 - 2}\right), \ldots, \left(n_1 - 1, n_2, \frac{M_2}{n_2}, \frac{M_1 - \frac{n_1 - 1}{n_2} M_2}{n_1 - (n_1 - 1)}\right) \right\},$$

to znači da je $m_r > 0$ pa ova konstrukcija ima smisla.

2. Brojevi novčića u prvom i u drugom merenju nisu jednaki, bez umanjenja opštosti recimo da važi $n_1 < n_2$.

a) Važi $\xi_1 < \xi_2$, to jest $\frac{f_1}{n_1} > \frac{f_2}{n_2}$. Dokažimo da je moguće da se osoba B dvoumi kada važi $n_1 = f_1$, to jest kada su svi novčići u gomili manje gustine falični. Tada $f_2 \in \{0, 1, \ldots, n_2 - 1\}$, pa broj faličnih novčića nije jednoznačno određen. Moguće su sledeće četvorke:

$$(f_1, f_2, m_f, m_r) \in \left\{ \left(n_1, 0, \frac{M_1}{n_1}, \frac{M_2}{n_2}\right), \left(n_1, 1, \frac{M_1}{n_1}, \frac{M_2 - \frac{1}{n_1} M_1}{n_2 - 1}\right), \right.$$

$$\left. \left(n_1, 2, \frac{M_1}{n_1}, \frac{M_2 - \frac{2}{n_1} M_1}{n_2 - 2}\right), \ldots, \left(n_1, n_2 - 1, \frac{M_1}{n_1}, \frac{M_2 - \frac{n_2 - 1}{n_1} M_1}{n_2 - (n_2 - 1)}\right) \right\}.$$

Kako $\xi_2 > \xi_1 \Rightarrow \frac{M_2}{n_2} > \frac{M_1}{n_1} \Rightarrow M_2 > \frac{n_2}{n_1} M_1 > \frac{n_2 - 1}{n_1} M_1 > \frac{n_2 - 2}{n_1} M_1 > \ldots$

$\ldots > \frac{1}{n_1} M_1$, pa je $m_r > 0$, što znači da ova kontrukcija ima smisla.

b) Ako važi $\xi_1 > \xi_2$, to znači da $\frac{f_1}{n_1} < \frac{f_2}{n_2}$ odakle sledi da je moguće da važi $f_2 = n_2$ i $f_1 \in \{0, 1, \ldots, n_1 - 1\}$, pa broj faličnih novčića nije jednoznačno određen. Dakle moguće su četvorke:

$$(f_1, f_2, m_f, m_r) \in \left\{ \left(0, n_2, \frac{M_2}{n_2}, \frac{M_1}{n_1}\right), \left(1, n_2, \frac{M_2}{n_2}, \frac{M_1 - \frac{1}{n_2} M_2}{n_1 - 1}\right), \ldots, \right.$$

$$\left. \left(n_1 - 1, n_2, \frac{M_2}{n_2}, \frac{M_1 - \frac{n_1 - 1}{n_2} M_2}{n_1 - (n_1 - 1)}\right) \right\}.$$

Kako $\xi_1 > \xi_2 \Rightarrow \frac{M_1}{n_1} > \frac{M_2}{n_2} \Rightarrow M_1 > \frac{n_1}{n_2} M_2 > \frac{n_1 - 1}{n_2} M_2 > \ldots > \frac{0}{n_2} M_2$, pa je $m_r > 0$, što znači da ova kontrukcija ima smisla.

c) Ako važi $\xi_1 = \xi_2$:

Prvi slučaj: $\mathrm{NZD}(n_1, n_2) > 1$. Iz Leme 9 znamo da važi $\frac{f_1}{n_1} = \frac{f_2}{n_2}$.

Moguće je da $(f_1, f_2) = (0, 0)$, i moguće je da $(f_1, f_2) = \left(\frac{n_1}{\mathrm{NZD}(n_1, n_2)}, \frac{n_2}{\mathrm{NZD}(n_1, n_2)}\right)$. Ponovo, broj faličnih novčića nije jednoznačno određen.

Dakle moguće su četvorke:

$$(f_1, f_2, m_f, m_r) \in \left\{ \left(0, 0, \frac{M_1}{2n_1}, \frac{M_1}{n_1}\right), \right.$$

$$\left. \left(\frac{n_1}{\mathrm{NZD}(n_1, n_2)}, \frac{n_2}{\mathrm{NZD}(n_1, n_2)}, \frac{M_2}{2n_1}, \frac{M_1 - \frac{1}{\mathrm{NZD}(n_1, n_2)} M_1}{n_1 - \frac{n_1}{\mathrm{NZD}(n_1, n_2)}}\right) \right\}.$$

Kako je $\mathrm{NZD}(n_1, n_2) > 1 \Rightarrow M_1 > \frac{n_1}{2n_1 \mathrm{NZD}(n_1, n_2)} M_1$ i

$n_1 > \frac{n_1}{\mathrm{NZD}(n_1, n_2)}$, što znači da je $m_r > 0$, pa ova kontrukcija ima smisla.

Drugi slučaj: $\mathrm{NZD}(n_1, n_2) = 1$.

Iz Leme 9 znamo da važi $\frac{f_1}{n_1} = \frac{f_2}{n_2} \Rightarrow f_1 n_2 = f_2 n_1$. Kako n_1 deli desnu stranu jednakosti onda deli i levu, a kako je NZD(n_1, n_2) = 1, to znači da $n_1 | f_1$. S obzirom na to da $f_1 \le n_1$, to znači da $f_1 = 0 \vee f_1 = n_1$. Ako je $f_1 = n_1$ odatle bi sledelo da je $f_2 = n_2$ pa bi onda svi novčići bili falični, što nije moguće. Podsetimo se da smo još u definiciji problema naglasili $0 \le f < n$. Dakle $f_1 = 0$, što znači da je $f_2 = 0$, što i jeste jedina mogućnost.

Dakle, jedino u slučaju $f = 0$ osoba A može ubediti osobu B u broj faličnih novčića i to ako u prvom merenju postavi jedan novčić, a u rugom sve ostale. □

Ova teorema se slično dokazuje i u slučaju kada su falični novčići teži od ispravnih jer je jedina suštinska razlika izmedju faličnih i ispravnih novčića (naravno osim njihove mase) ta da se ne sme otkriti identitet faličnog, a sme ispravnog novčića, a to nigde nije iskorišćeno u ovom dokazu.

Teorema 5 tvrdi da osoba A ne može ubediti osobu B u broj faličnih novčića u jednom merenju ako osoba B zna masu ispravnog novčića. To znači da osoba A sigurno neće moći da ubedi osobu B u broj faličnih novčića u jednom merenju ako osoba B ne zna masu ispravnog novčića. Iz ovoga, teoreme 7 i teoreme 11 vidimo da najmanji broj merenja potreban osobi A da ubedi osobu B u broj faličnih novčića, kada osoba B ne zna ni masu ispravnog ni faličnog novčića, iznosi tačno 3.

Asimptotsko ponašanje potrebnog broja merenja terazijama za utvrđivanje da li je broj faličnih novčića jednak nekom unapred zadatom broju

U ovom odeljku se bavimo utvrđivanjem donje granice potrebnog broja merenja terazijama za utvrđivanje da li je broj faličnih novčića, f, jednak nekom unapred zadatom broju m.

Koristeći ranije navedenu definiciju osetljivosti, Purdijev glavni (Purdy 2011) rezultat, i definisanjem odgovarajuće funkcije možemo doći do donje granice broja merenja koje nam je potrebno da bismo, uz pomoć terazija, utvrdili da li ima tačno m faličnih novčića.

Definicija 12. Neka je $f_m : \{0, 1\}^n \to \{0, 1\}$ funkcija koja daje 1 ako je broj jedinica u vektoru jednak m, a 0 u suprotnom.

Teorema 13. Funkcija $f_m : \{0, 1\}^n \to \{0, 1\}$ ima prosečnu osetljivost

$$\alpha(f_m) = \binom{n}{m} \cdot \frac{n}{2^{n-1}}.$$

Dokaz. Za sve brojeve faličnih novčića koji su manji od $m-1$ važi $\sigma_x(f) = 0$ jer je uvek $f(x) = f(x^i) = 0$, isto važi i za sve koji su veći od $m+1$.

$$\alpha(f) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sigma_x(f_m) =$$

$$= \frac{1}{2^n} \cdot \left[\binom{n}{0} \cdot 0 + \binom{n}{m-2} \cdot 0 + \binom{n}{m-1} \cdot (n-m+1) + \binom{n}{m} \cdot n + \binom{n}{m+1} \cdot (m+1) + \right.$$

$$\left. + \binom{n}{m+2} \cdot 0 + \ \dots + \binom{n}{n} \cdot 0 \right] =$$

$$= \frac{1}{2^n} \cdot \left[\binom{n}{m-1} \cdot (n-m+1) + \binom{n}{m} \cdot n + \binom{n}{m+1} \cdot (m+1) \right] =$$

$$= \frac{1}{2^n} \cdot \left[\frac{n!}{(m-1)!(n-m+1)!} \cdot (n-m+1) + \frac{n!}{m!(n-m)!} \cdot n + \right.$$

$$\left. + \frac{n!}{(m+1)!(n-m-1)!} \cdot (m+1) \right] =$$

$$= \frac{1}{2^n} \cdot \left[\frac{n!}{(m-1)!(n-m)!} + \frac{n \cdot n!}{m!(n-m)!} + \frac{n!}{m!(n-m-1)!} \right] =$$

$$= \frac{1}{2^n} \cdot \left[\frac{m \cdot n!}{m!(n-m)!} + \frac{n \cdot n!}{m!(n-m)!} + \frac{(n-m) \cdot n!}{m!(n-m)!} \right] =$$

$$= \frac{n!}{m!(n-m)!} \cdot \frac{n+m+n-m}{2^n} \Rightarrow$$

$$\Rightarrow \alpha(f) = \binom{n}{m} \cdot \frac{2n}{2^n}.$$

□

Teorema 12. Ako je dat broj $m \in \mathbb{N}$, potrebno je barem $\Omega\left(\binom{n}{m} \cdot \frac{\sqrt{n}}{2^{n-1}}\right)$ merenja za utvrđivanje da li se u skupu novčića nalazi tačno m faličnih.

Dokaz. Iz teoreme 4 sledi da je potrebno barem $\Omega\left(\alpha(f) / \sqrt{n}\right)$ merenja, a iz teoreme 11 je poznato $\alpha(f) = \binom{n}{m} \cdot \frac{2n}{2^n}$. To znači da je potrebno bar $\Omega\left(\binom{n}{m} \cdot \frac{\sqrt{n}}{2^{n-1}}\right)$ merenja, što je i trebalo dokazati.

□

Zaključak

Iako je oblast problema merenja novčića popularna još od četrdesetih godina dvadesetog veka, još uvek se javljaju i rešavaju problemi u ovoj oblasti. U ovom radu smo postavili i rešili modifikaciju Šapavalovljevog problema iz 2007. godine. U prvoj modifikaciji dato je n novčića, od kojih je f falično. Osobi A su poznati identiteti svih novčića, a osobi B samo masa faličnog. Dokazali smo da je dva najmanji broj merenja dovoljan da osoba A otkrije osobi B koliko je faličnih novčića, ali ne i koji novčići su falični.

U drugoj modifikaciji osoba B ne zna ni masu ispravnog novčića. Dokazali smo da je tada potrebno tri merenja.

Oba slučaja su dokazana tako što je data konstrukcija merenja koju osoba A treba da obavi i dokaz da ne može sa manje merenja. Date konstrukcije rešavaju problem za $2 < f < n-1$.

Autori smatraju da je za slučajeve $f \in \{1, 2, n-1\}$ osoba A ne može otkriti osobi B koliko je f u istom broju merenja kao i za $2 < f < n-1$ bez otkrivanja identiteta faličnih novčića, ali to ostaje stvar koja tek treba da se dokaže.

Osim ovoga, pronašli smo asimptotsko ponašanje potrebnog broja merenja terazijama za utvrđivanje da li je broj faličnih novčića jednak nekom unapred zadatom broju m.

Literatura

Grossman H. D. 1945. The twelve-coin problem. *Scripta Mathematica*, **11**: 360.

Guy R. K., Nowakowski R. J. 1995. Coin-Weighing Problems. *The American Mathematical Monthly*, **102** (2): 164.

Kolmogorov 2007. Kolmogorov Math Tournaments. http://cdoosh.ru/kolm/kolm.html

Diaco N. 2016. Counting Counterfeit Coins: A New Coin Weighing Problem. arXiv preprint arXiv:1606.04170

Purdy E. 2011. Lower Bounds for Coin-Weighing Problems. *ACM Transactions on Computation Theory*, **2** (2): 1.

Tijana Jakšić and Pavle Tepavčević

Coin Weighing Problems

In this paper, we posed and solved a modification of the Shapovalov's coin weighing problem. The problem is generalized to n coins of which f is counterfeit. Measurements are performed using a digital scale instead of balance scales. We also found the necessary number of balance scale Measurements to determine if there is exactly m counterfeit coins, for a given m.