Neodlučivost u matematici

N. Ikodinović

ikodinovic@matf.bg.ac.rs

26. 12. 2017.

Pregled predavanja

Problem zaustavljanja

Halting problem

Skup $H = \{(e,x) \mid \varphi_e(x)\downarrow\}$ nije rekurzivan.

Dokaz primenom teoreme rekurzije.

Ako je $\chi_H(e,x) = \begin{cases} 1, & (e,x) \in H, \\ 0, & (e,x) \notin H. \end{cases}$ rekurzivna, onda je

$f(e,x) = \begin{cases} \uparrow, & \chi_H(e,x) = 1, \\ 0, & \chi_H(e,x) = 0. \end{cases}$ parcijalno rekurzivna.

Prema teoremi rekurzije postoji e_0 da je $\varphi_{e_0}(x) \simeq f(e_0,x)$.

- Ako $(e_0,x) \in H$, tada $f(e_0,x)\uparrow$ (prema definiciji funkcije f), a samim tim i $\varphi_{e_0}(x)\uparrow$, što znači da $(e_0,x) \notin H$. Kontradikcija.
- Ako $(e_0,x) \notin H$, tada $f(e_0,x)\downarrow 0$ (prema definiciji funkcije f), a samim tim i $\varphi_{e_0}(x)\downarrow 0$, što znači da $(e_0,x) \in H$. Kontradikcija.

Dakle, skup H ne može biti rekurzivan.

Problem zaustavljanja

Halting problem

Skup $H = \{(e,x) \mid \varphi_e(x)\downarrow\}$ nije rekurzivan.

Primenu teoreme rekurzije ilustrujemo i sledećom konstrukcijom.
Ako je $\mathbb{H}$ RM-program koji izračunava χ_H (i samim tim se zaustavlja za svaki ulaz (e,x)), do kontradikcije dolazimo konstrukcijom sledećeg programa:

$\mathbb{D}$ =za ulaz x :

1. Odredi (primenom teoreme rekurzije)
   sopstveni kod $\lceil\mathbb{D}\rceil$
2. Pozovi $\mathbb{H}$ za ulaz $(\lceil\mathbb{D}\rceil, x)$
3. Ako $\mathbb{H}$ kaže $(\lceil\mathbb{D}\rceil, x) \in H$, onda divergiraj;
   a ako $\mathbb{H}$ kaže $(\lceil\mathbb{D}\rceil, x) \notin H$, onda vrati izlaz 0.

Rajsova teorema

Definicija

Skup $A \subseteq \mathbb{N}$ je ekstenzionalan ako za sve $a, e \in \mathbb{N}$:

$$\text{iz } a \in A \text{ i } \varphi_e = \varphi_a \text{ sledi } e \in A.$$

Skup $A \subseteq \mathbb{N}$ je netrivijalan ako je $A \neq \emptyset$ i $A \neq \mathbb{N}$; u suprotnom je trivijalan.

Rajsova teorema

Svaki netrivijalan ekstenzionalan skup nije rekurzivan.

Rajsova teorema

Rajsova teorema

Svaki netrivijalan ekstenzionalan skup nije rekurzivan.

Dokaz. Neka je $A \subseteq \mathbb{N}$ netrivijalan ekstenzionalan skup; $a \in A$ i $b \in \mathbb{N} \setminus A$. Pretpostavimo da je A rekurzivan skup. Tada je funkcija

$$f(e,x) = \begin{cases} \varphi_b(x), & e \in A, \\ \varphi_a(x), & e \notin A, \end{cases}$$

parcijalno rekurzivna. Prema teoremi rekurzije, postoji $e_0 \in \mathbb{N}$ takav da je $\varphi_{e_0}(x) \simeq f(e_0,x)$, $x \in \mathbb{N}$.

- Ako $e_0 \in A$, onda je $\varphi_{e_0} = \varphi_b$, a kako je A ekstenzionalan i $b \notin A$, sledi da $e_0 \notin A$. Kontradikcija.
- Ako $e_0 \notin A$, onda je $\varphi_{e_0} = \varphi_a$, a kako je A ekstenzionalan i $a \in A$, sledi da $e_0 \in A$. Kontradikcija.

Dakle, A nije rekurzivan skup.

Rajsova teorema

Rajsova teorema

Svaki netrivijalan ekstenzionalan skup nije rekurzivan.

Posledica

Neka je $\mathcal{A}$ bilo koji skup unarnih parcijalno rekurzivnih funkcija. Skup $I(\mathcal{A}) = \{e \mid \varphi_e \in \mathcal{A}\}$ je rekurzivan akko je $\mathcal{A}$ trivijalan skup, tj. $\mathcal{A} = \emptyset$ ili $\mathcal{A}$ sadrži sve unarne parcijalno rekurzivne funkcije.

Problem reči

- Σ – alfabet;
- Σ-pravilo: $u \to v$, $u, v \in \Sigma^*$.
- Σ-proces – konačan skup Σ-pravila.
  Ako je $\mathcal{P}$ neki Σ-proces i $w, w' \in \Sigma^*$, tada $w \to_{\mathcal{P}} w'$ znači da se iz w može izvesti reč w' primenom pravila iz $\mathcal{P}$ konačan broj puta.

Problem reči

Da li postoji algoritam koji za zadati Σ-proces $\mathcal{P}$ i reči $w, w' \in \Sigma$ ispituje (odlučuje) da li $w \to_{\mathcal{P}}^* w'$ ili $w \not\to_{\mathcal{P}}^* w'$?

Konstruisaćemo Σ-proces $\mathcal{P}$ i izabrati jednu reč w' tako da ne postoji algoritam koji za zadatu reč w ispituje da $w \to_{\mathcal{P}}^* w'$ ili $w \not\to_{\mathcal{P}}^* w'$.

Problem reči

Neka je $\mathbb{P}$: $I_1, \ldots, I_N$ program u standarnoj formi koji izračunava funkciju $x \mapsto \Phi_U(x, x)$; $M = \|\mathbb{P}\| + 1$.
Biramo alfabet Σ pogodan za opisivanje izvršavanja programa $\mathbb{P}$:

$$\Sigma = \{b, a, r_1, \ldots, r_M, p_1, \ldots, p_N, p_{N+1}, q_1, \ldots, q_N, e_1, \ldots, e_N\}.$$

konfiguracija | | | | | | reča nad Σ

i	r_1	r_2	$\cdots$	r_M	$\mapsto$	$bp_i r_1 a^{r_1} r_2 a^{r_2} \cdots r_M a^{r_M}$

Specijalno, početnoj konfiguraciji za ulaz $x \in \mathbb{N}$ odgovara reč $w_x = bp_1 r_1 a^x r_2 r_3 \cdots r_{M-1} r_M$.

Σ-proces $\mathcal{P}$ konstruišemo tako što za svaku instrukciju I_i, $1 \leqslant i \leqslant N$, dodajemo Σ-pravila kojima se simulira izvršavanje te instrukcije.

Problem reči

Ako je I_i instrukcija $R_k^+ \mid \ell$, onda dodajemo pravila:

$$\left.\begin{array}{l} p_i r_j \to r_j p_i, 1 \leqslant j < k, \\ p_i a \to a p_i, \end{array}\right\}$$

Ako je $k > 1$ dodajemo najpre pravila pomoću kojih se iz neke reči koja opisuje konfiguraciju izvodi reč u kojoj je simbol p_i postavljen ispred r_k; naravno, ako je $k = 1$, onda je već p_i već postavljeno ispred r_1.

$$p_i r_k \to q_i r_k a,$$

Dodajemo pravilo koje odgovara povećavanju sadržaja registra R_k za 1. Uvodjenje slova q_i (umesto p_i) označava činjenicu da je izvršena akcija na registru R_k koju nalaže instrukcija I_i.

$$\left.\begin{array}{l} r_j q_i \to q_i r_j, 1 \leqslant j < k, \\ a q_i \to q_i a, \end{array}\right\}$$

Vraćamo (samo ako je $k > 1$) slovo q_i do slova b.

$$b q_i \to b p_\ell.$$

Menjamo q_i slovom p_ℓ.

Problem reči

Ako je I_i instrukcija $R_k^- \mid \ell_0, \ell_1$, onda dodajemo pravila:

$p_i r_j \to r_j p_i, 1 \leqslant j < k,$

$p_i a \to a p_i.$

$\left.\begin{array}{l} p_i r_k a \to q_i r_k, \\ p_i r_k r_{k+1} \to e_i r_k r_{k+1}, \end{array}\right\}$ Dodajemo pravilo koje odgovara akciji na registru R_k: ako u R_k nije upisana nula, onda se sadržaj umanjuje za 1, i ta akcija se pamti slovom q_i; a ako je u R_k upisana nula, onda se sadržaj ne menja, i taj slučaj se pamti slovom e_i.

$r_j q_i \to q_i r_j, 1 \leqslant j < k,$

$a q_i \to q_i a,$

$r_j e_i \to e_i r_j, 1 \leqslant j < k,$

$a e_i \to e_i a,$

$b q_i \to b p_{\ell_1},$

$b e_i \to b p_{\ell_0}.$

Problem reči

Najzad, dodajemo pravila

$$p_{N+1}r_i \to p_{N+1}, p_{N+1}a \to p_{N+1},$$

kojima se reč, koja odgovara završnoj konfiguraciji (ako se ona uopšte dostiže) izračunavanja $\mathbb{P}(x)$, transformiše u bp_{N+1}.

Za svaki prirodan broj x važi:

$$w_x \to_{\mathcal{P}}^* bp_{N+1} \text{ akko } \Phi_U(x,x)\downarrow, \text{odn. } w_x \to_{\mathcal{P}}^* bp_{N+1} \text{ akko } x \in K.$$

Budući da skup K nije rekurzivan, ne postoji algoritam koji se traži u problemu reči.

Problem valjanosti

Logički simboli

- *Promenljive*: $\mathrm{Var} = x, y, z, x_1, \ldots$
- *Veznici*: $\neg, \wedge (\vee, \rightarrow, \leftrightarrow)$
- *Kvantifikatori*: $\forall$, $\exists$
- *Pomoćni znaci*: $)$, $($

Nelogički simboli

- *Relacijski simboli*: Rel
- *Operacijski simboli*: Fun

– $\mathrm{Rel} \cap \mathrm{Fun} = \emptyset$, $\mathcal{L} = \mathrm{Rel} \cup \mathrm{Fun}$

– $\mathbf{ar} : \mathrm{Rel} \cup \mathrm{Fun} \rightarrow \mathbb{N}$

– $p \in \mathrm{Rel}$, $\mathrm{ar}(p) = 0$
iskazno slovo

– $c \in \mathrm{Fun}$, $\mathrm{ar}(f) = 0$
simbol konstante

Problem valjanosti

Da li postoji algoritam koji za zadatu $\mathcal{L}$-rečenicu σ ispituje (odlučuje) da li je σ valjana (tačna u svim modelima) ili nije, tj. postoji model u kojem nije tačna?

Problem valjanosti

Neka je $\mathbb{P}$: $I_1, \ldots, I_N$ program u standarnoj formi koji izračunava funkciju $x \mapsto \Phi_U(x,x)$; $M = \|\mathbb{P}\| + 1$.
Biramo $\mathcal{L}$ tako da $\mathcal{L}$-rečenice budu pogodne za opisivanje izvršavanja RM-programa $\mathbb{P}$:

- jedan simbol konstante $\underline{0}$,
- unarni operacijski simbol $'$ i
- $d+1$-arni relacijski simbol R.

Za svako $n \in \mathbb{N}$, term $\underline{0}\overbrace{'\cdots'}^{n \text{ puta}}$ (tzv. *numeral*) označićemo $\underline{n}$.
Za svaku instrukciju $\mathbb{I}_i$ programa $\mathbb{P}$ sastavićemo rečenicu σ_i koja izražava značenje te instrukcije.

Problem valjanosti

Ako je I_i instrukcija $R_k^+ \mid \ell$, onda je σ_i rečenica

$$\forall x_1 \ldots \forall x_d (R(\underline{i}, x_1, \ldots, x_k, \ldots, x_d) \Rightarrow R(\underline{\ell}, x_1, \ldots, x_k', \ldots, x_d)).$$

Ako je I_i instrukcija $R_k^- \mid \ell_0, \ell_1$, onda je σ_i rečenica

$$\begin{aligned}\forall x_1 \ldots \forall x_d (R(\underline{i}, x_1, \ldots, \underline{0}, \ldots, x_d) \Rightarrow R(\underline{\ell_0}, x_1, \ldots, \underline{0}, \ldots, x_d) \wedge \\ \wedge\ R(\underline{i}, x_1, \ldots, x_k', \ldots, x_d) \Rightarrow R(\underline{\ell_1}, x_1, \ldots, x_k, \ldots, x_d)).\end{aligned}$$

σ_0 je rečenica $\forall x \forall y ((x' = y' \Rightarrow x = y) \wedge x' \neq \underline{0})$.

Za $n \in \mathbb{N}$ neka je σ_n rečenica:

$$\sigma_0 \wedge \sigma_1 \wedge \cdots \wedge \sigma_N \wedge R(\underline{1}, \underline{n}, \underline{0}, \ldots, \underline{0}) \Rightarrow \exists x_1 \cdots \exists x_d R(\underline{N+1}, x_1, \ldots, x_d).$$

Za svaki prirodan broj n važi:

$$\mathbb{P}(n)\downarrow \text{ akko } \models \sigma_n, \text{ odn. } n \in K \text{ akko } \models \sigma_n.$$

Rešivost Diofantovih jednačina

10. Hilbertov problem

Da li postoji algoritam koji za svaki polinom $P(x_1, \ldots, x_k)$, čiji su koeficijenti prirodni brojevi, odlučuje da li jednačina $P(x_1, \ldots, x_k) = 0$ ima rešenja u $\mathbb{N}^k$ ili nema?

Definicija

Skup $A \subseteq \mathbb{N}^k$ je diofantovski ukoliko postoji polinom $P(x_1, \ldots, x_k, y_1, \ldots, y_m)$ takav da je

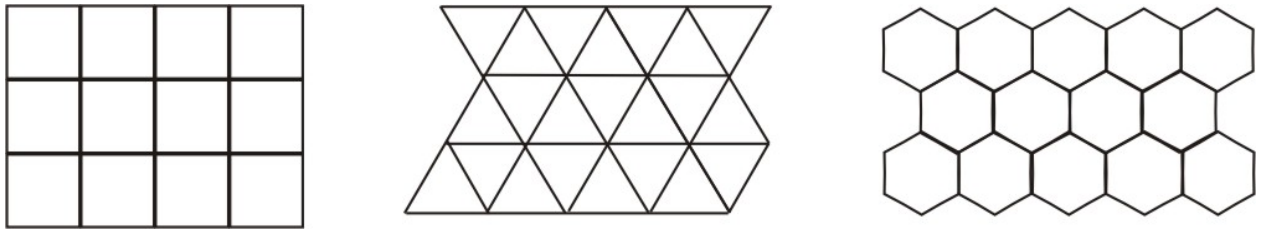
$$A = \{\vec{x} \in \mathbb{N}^k \mid \exists y_1 \ldots y_m \, P(\vec{x}, \vec{y}) = 0.\}$$

Matijasevičeva teorema

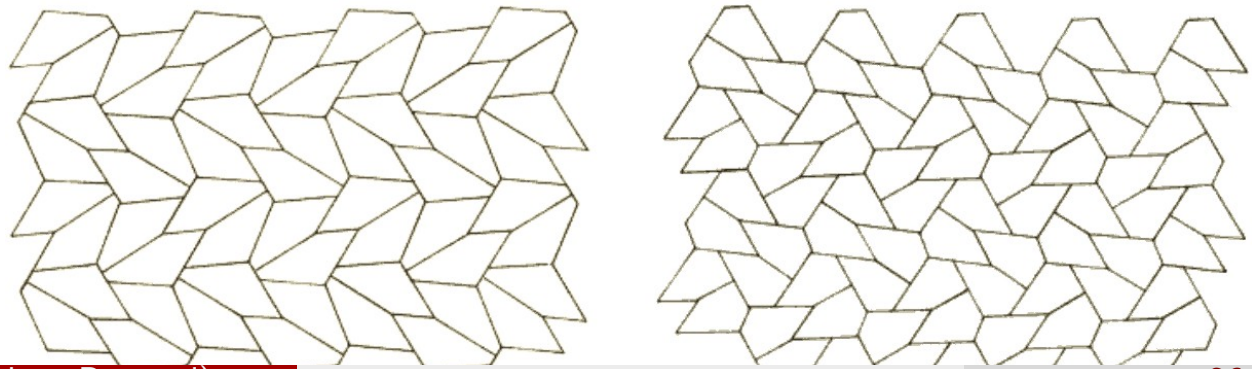
Svaki rekurzivno nabrojiv skup je diofantovski.

Popločavanje ravni

Poznato je da se ravan može *popločati*, tj. pokriti bez preklapanja i praznina, kvadratima, jednakostraničnim trouglovima i pravilnim šestouglovima, a da se ne može popločati, na primer, pravilnim petouglovima.

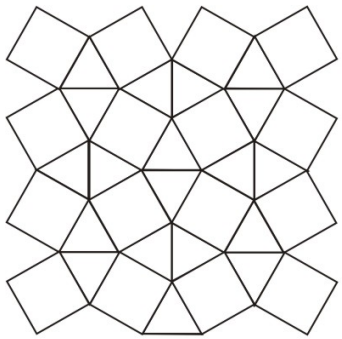
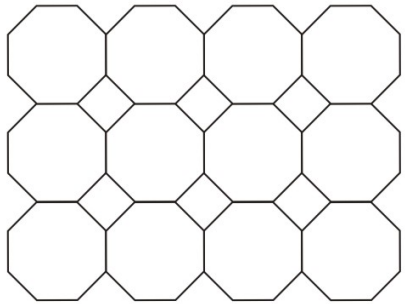
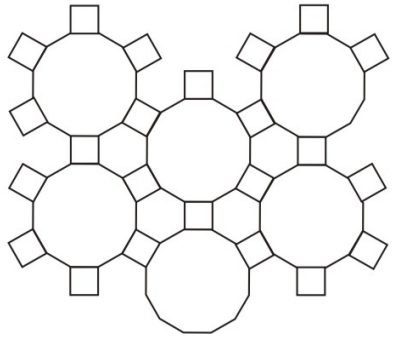


Mnogi drugi oblici mogu popločati ravan, kao, na primer, svaki od nepravilnih petouglova prikazanih na narednoj slici.



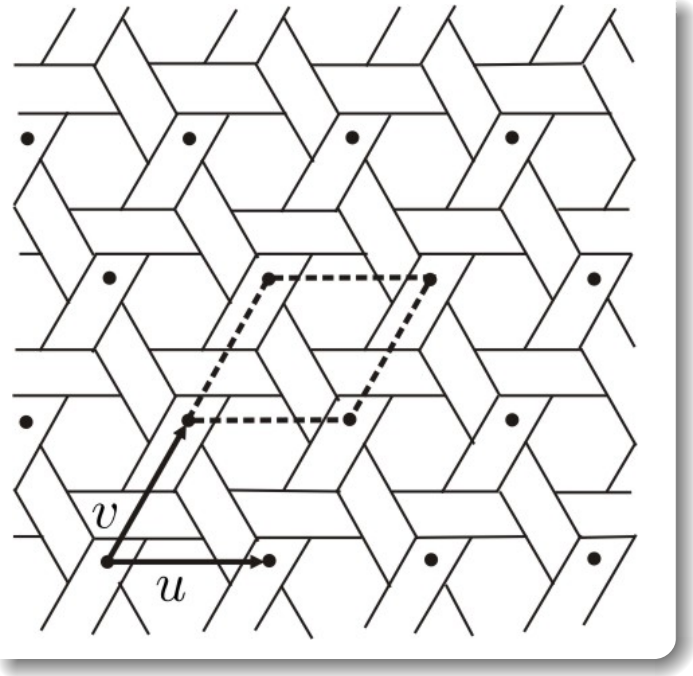
Popločavanje ravni

Razmatranje popločavanja ravni prilično se komplikuje povećavanjem broja oblika.

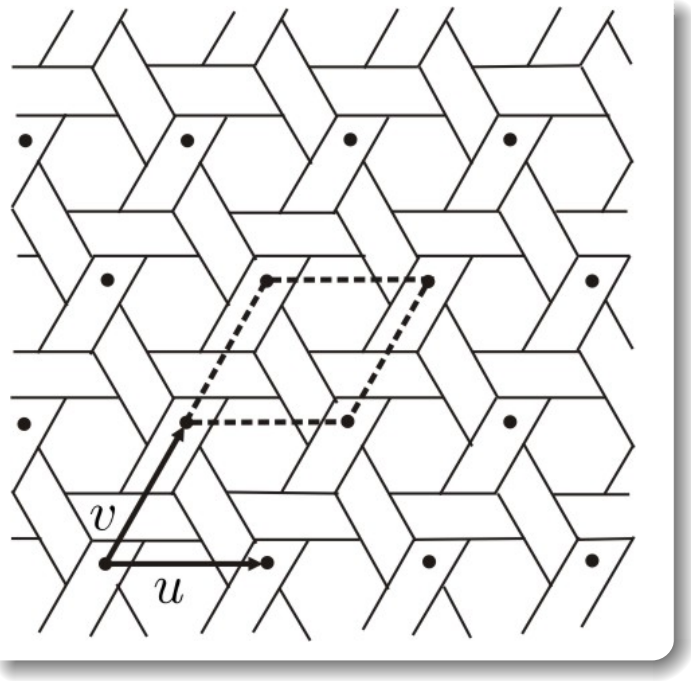
Popločavanje ravni

Sva popločavanja ravni prikazana na prethodnim slikama su *periodična*. Grubo govoreći, to znači da postoje bar dva različita pravca u popločanoj ravni i na svakom od njih beskonačno mnogo tačaka iz kojih možemo posmatrati popločanu ravan a da ono što vidimo bude jedan te isti šablon, odnosno da nam popločana ravan izgleda potpuno isto kada je posmatramo iz bilo koje od pomenutih tačaka.



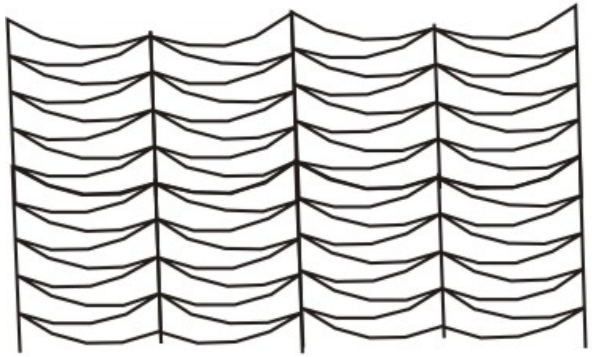
Popločavanje ravni

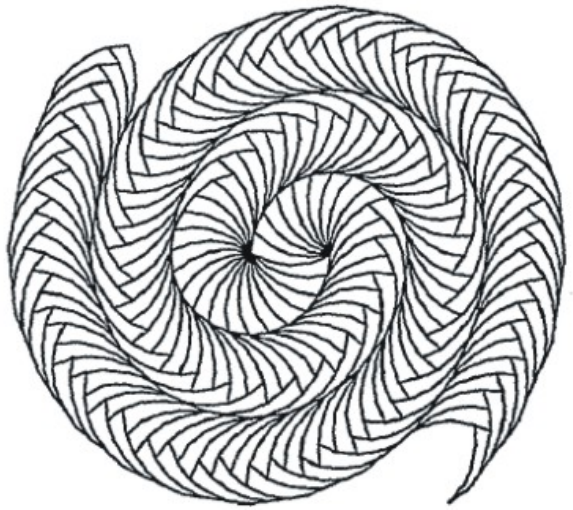
Matematičkim jezikom, popločavanje je periodično ako postoje dve nezavisne translacije ravni koje uočeno popločavanje prevode u sebe. Za svako periodično popločavanje ravni postoji tzv. *paralelogram perioda* odredjen vektorima translacija koje to popločavanje prevode u sebe.



Popločavanje ravni

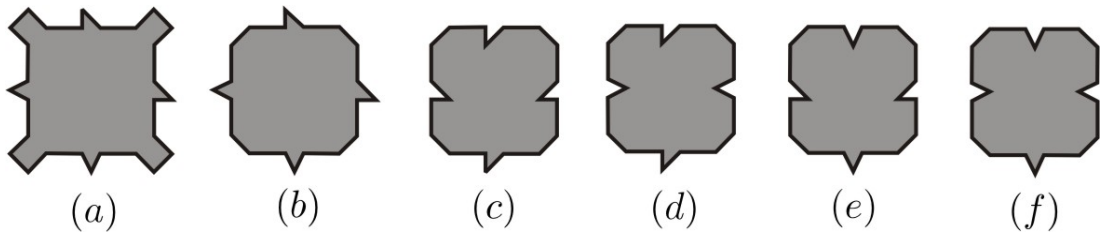
Postoje pločice kojima se ravan može popločavati i periodično i neperiodično.





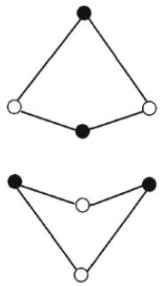
Popločavanje ravni

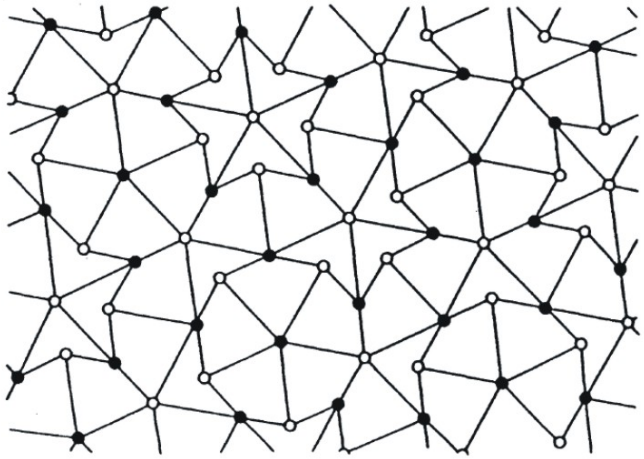
Postoji li konačan skup dozvoljenih oblika koji se mogu redjati samo neperiodično? Postoji – Robinsonov aperiodičan skup pločica.



Popločavanje ravni

Postoji još aperiodičnih skupova pločica: Penrouzove pločice – zmaj i strelica.





Popločavanje ravni

Kako i zašto su otkriveni aperiodični skupovi pločica?

Hao Vang je 1961. godine formulisao je problem: Postoji li postupak za rešavanje problema popločavanja, tj. postoji li neki algoritam kojim se može utvrditi da li dati skup mnogougaonih pločica može popločati ravan?

Dokazao je da će ovakav algoritam postojati ako se dokaže da svaki skup pločica koji popločava ravan zaparavo je popločava periodično.
(U to vreme se verovalo da aperiodični skupovi pločica ne postoje).

M. R. Robinson, *Undecidability and nonperiodicity for tilings of the plane*, Invent. Math. 12, 1971.

Neodlučivost problema popločavanja ravni

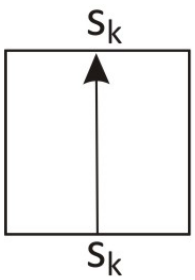
Suštinska ideja dokaza neodlučivosti problema popločavanja ravni jeste simulacija Tjuringovih mašina pomoću pločica. Sama simulacija je zanimljiva sama po sebi jer omogućava da pakovanje pločica zamišljamo kao model izračunljivosti.

Simuliraćemo rad proizvoljne Tjuringove mašine na praznoj traci jer: ne postoji algoritam koji odlučuje da li se proizvoljna Tjuringova mašina zaustavlja ako započne rad na praznoj traci.

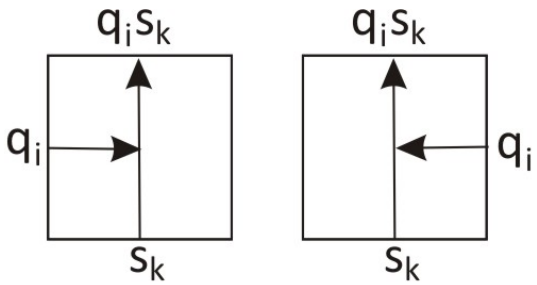
Umesto opšteg problema popločavanja ravni razmatraćemo tzv. *problem popločavanja ravni sa početnim zahtevima*.

Neodlučivost problema popločavanja ravni

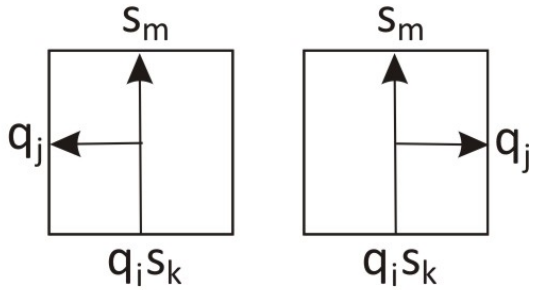
Za simulaciju rada Tjuringovih mašina na praznoj traci koristicemo sledeće pločice.



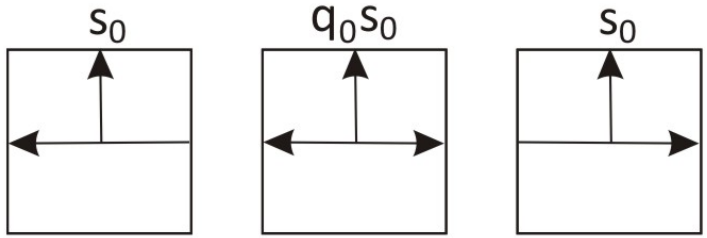
Плочица
симбол



Плочице
везе



Плочице
акције



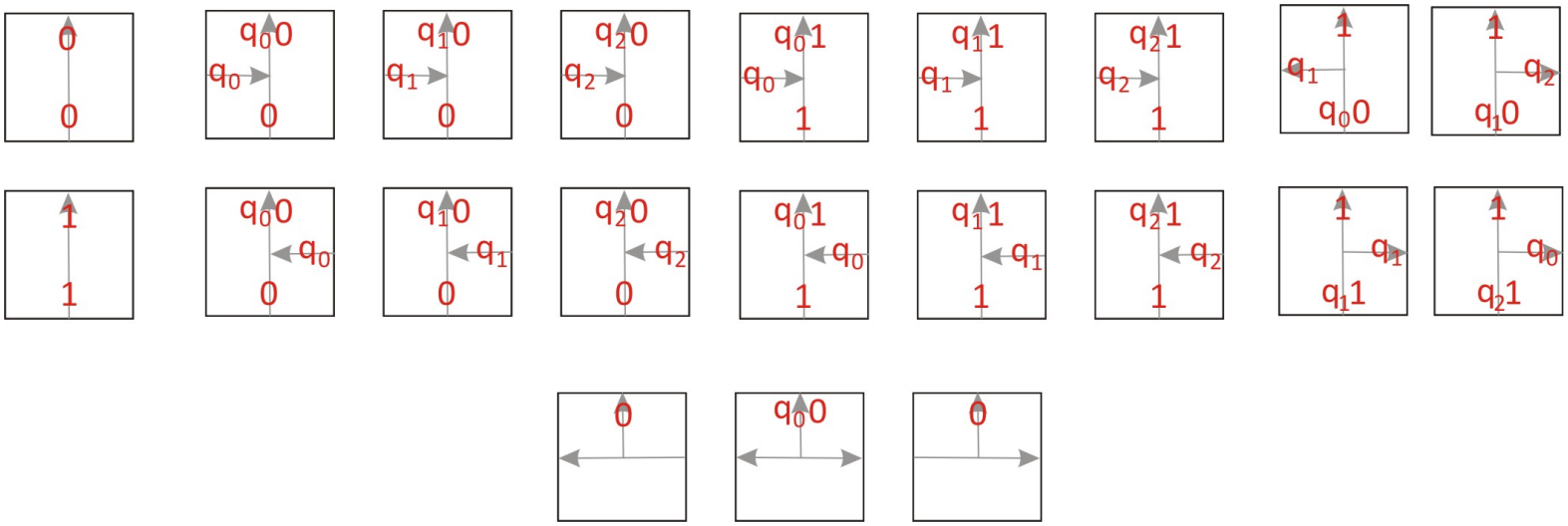
Почетне плочице

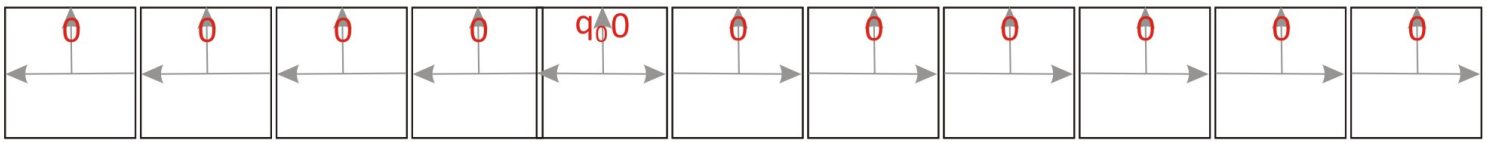
Neodlučivost problema popločavanja ravni

ZADATAK 23. Ispitati rad na praznoj traci Tjuringove mašine date sa:

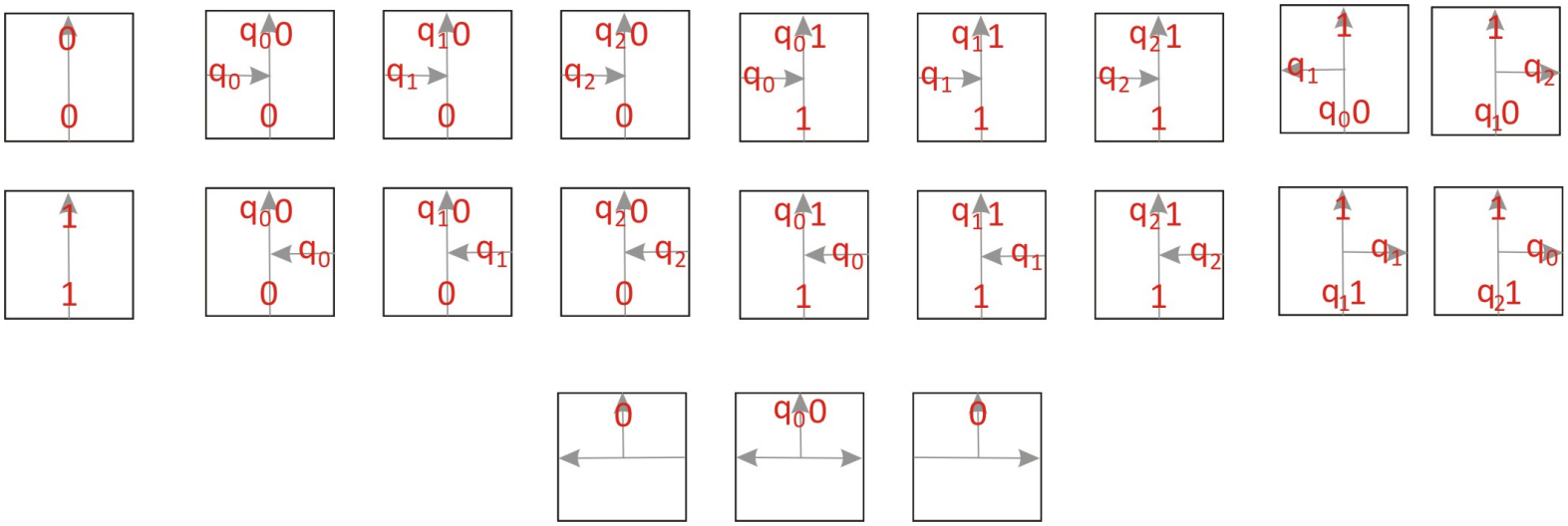
$$q_0 01 \mathrm{L} q_1,\ q_1 01 \mathrm{R} q_2,\ q_1 11 \mathrm{R} q_1,\ q_2 11 \mathrm{R} q_0.$$

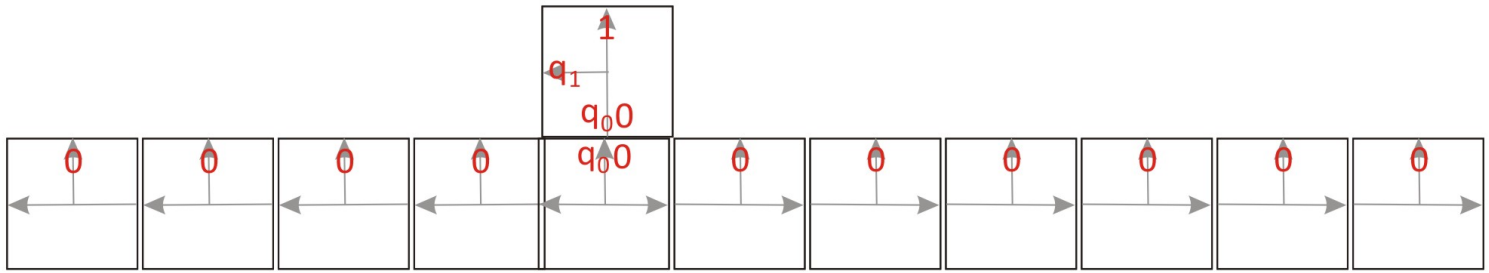
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



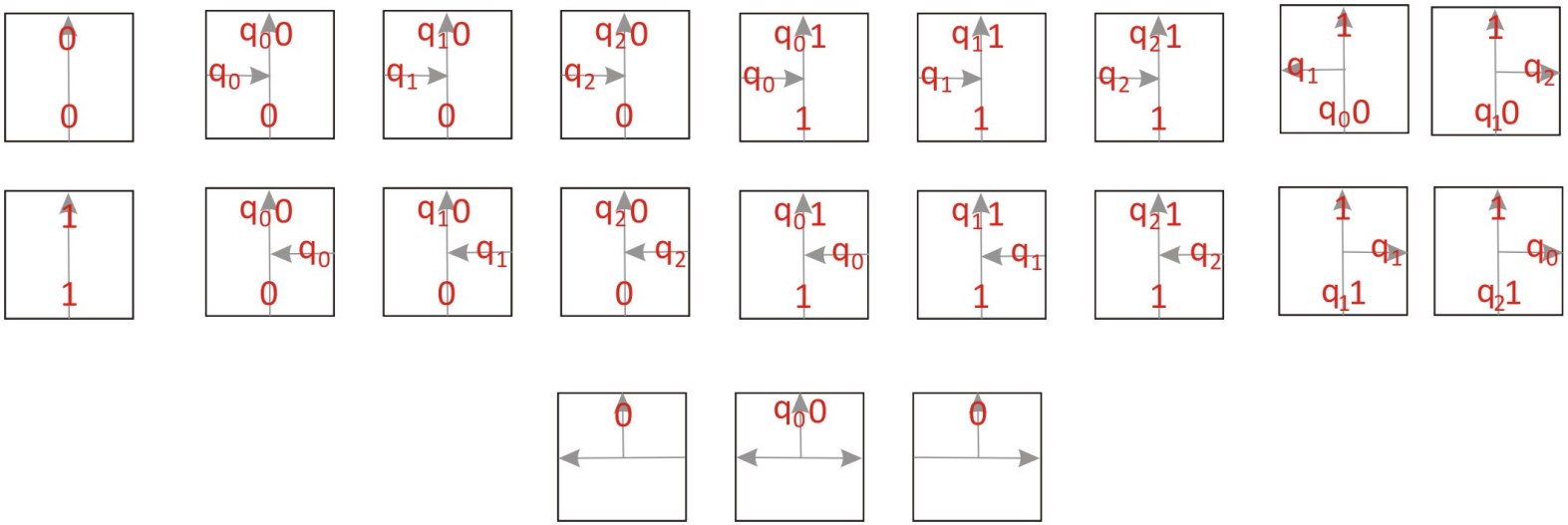


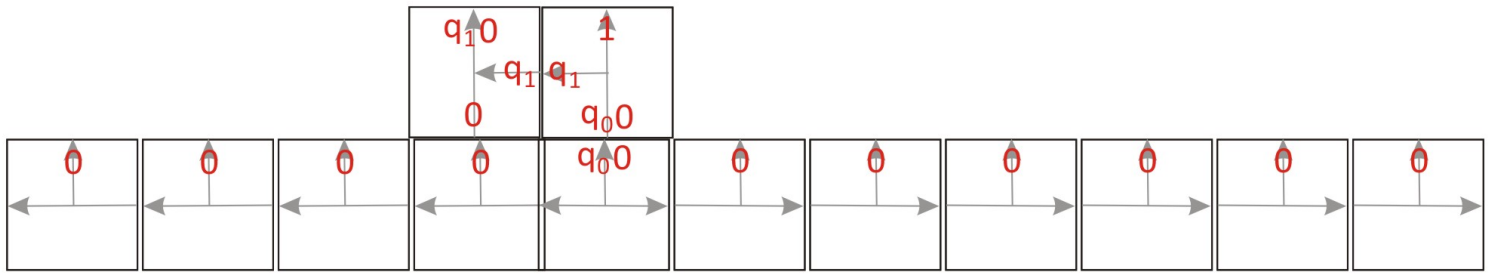
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



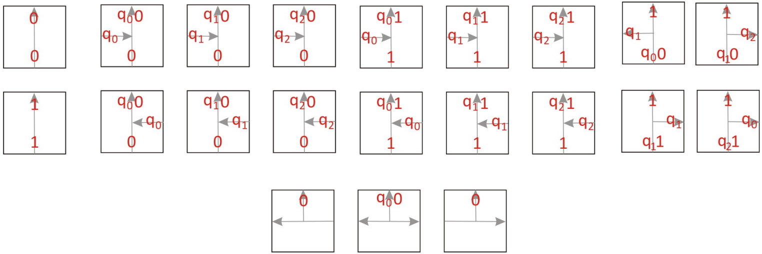


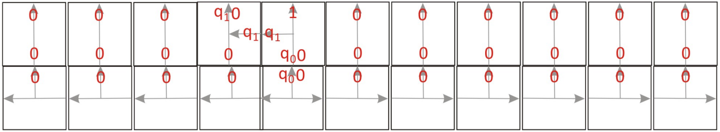
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



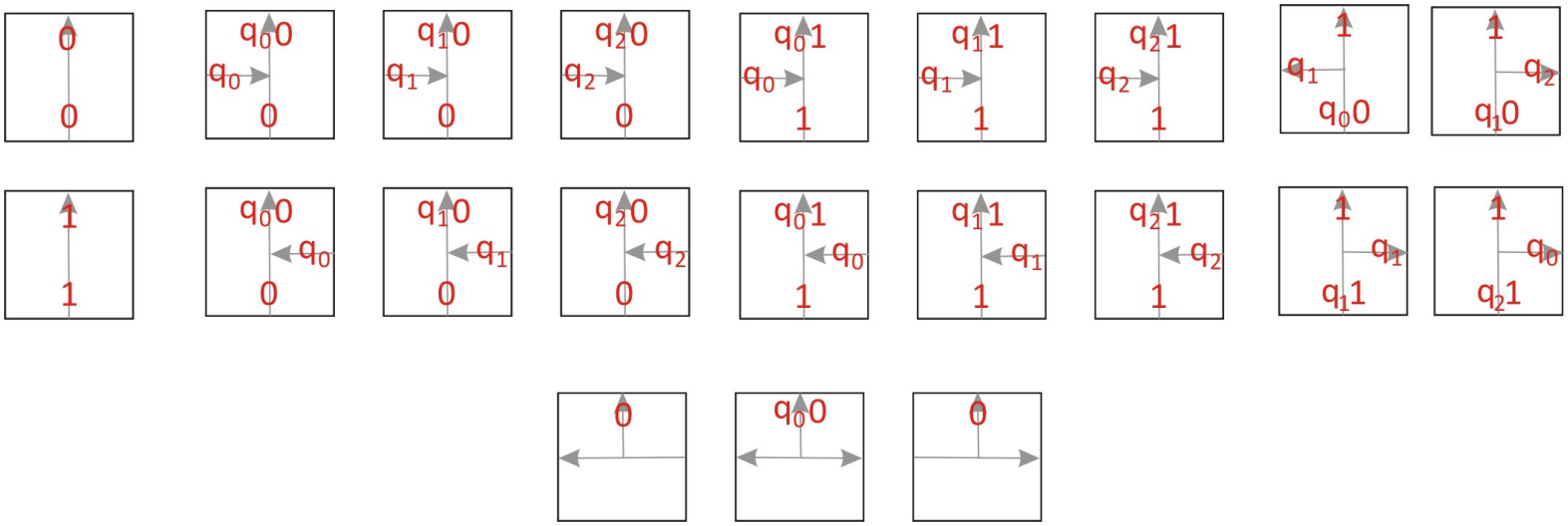


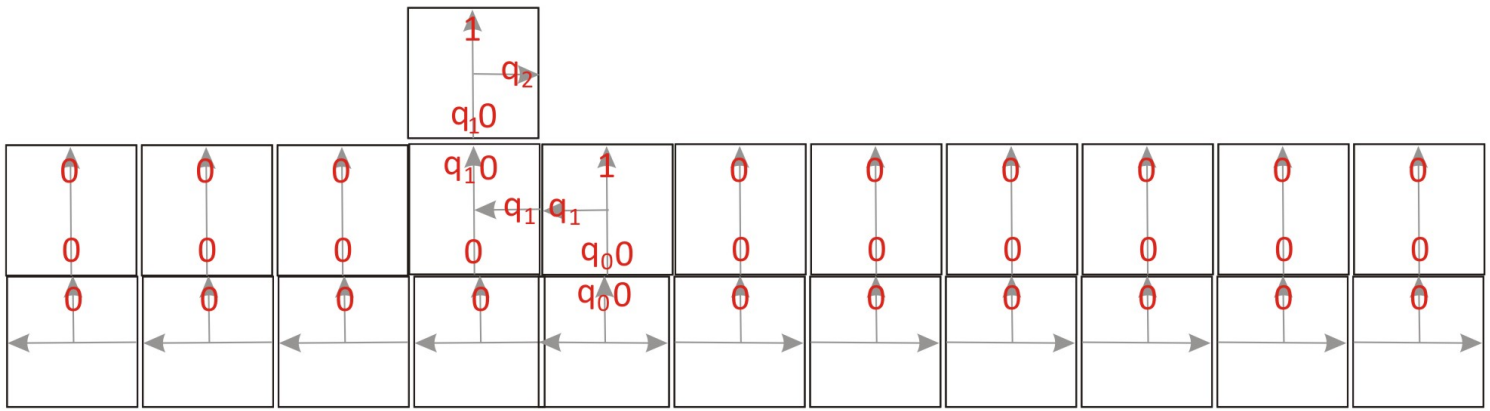
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



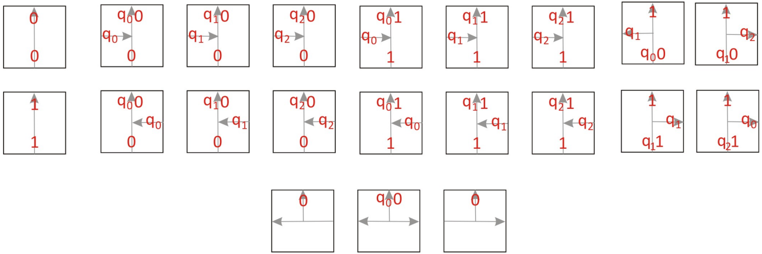


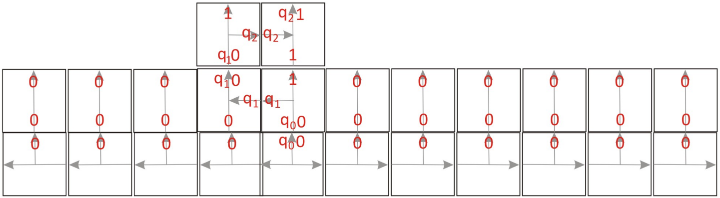
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



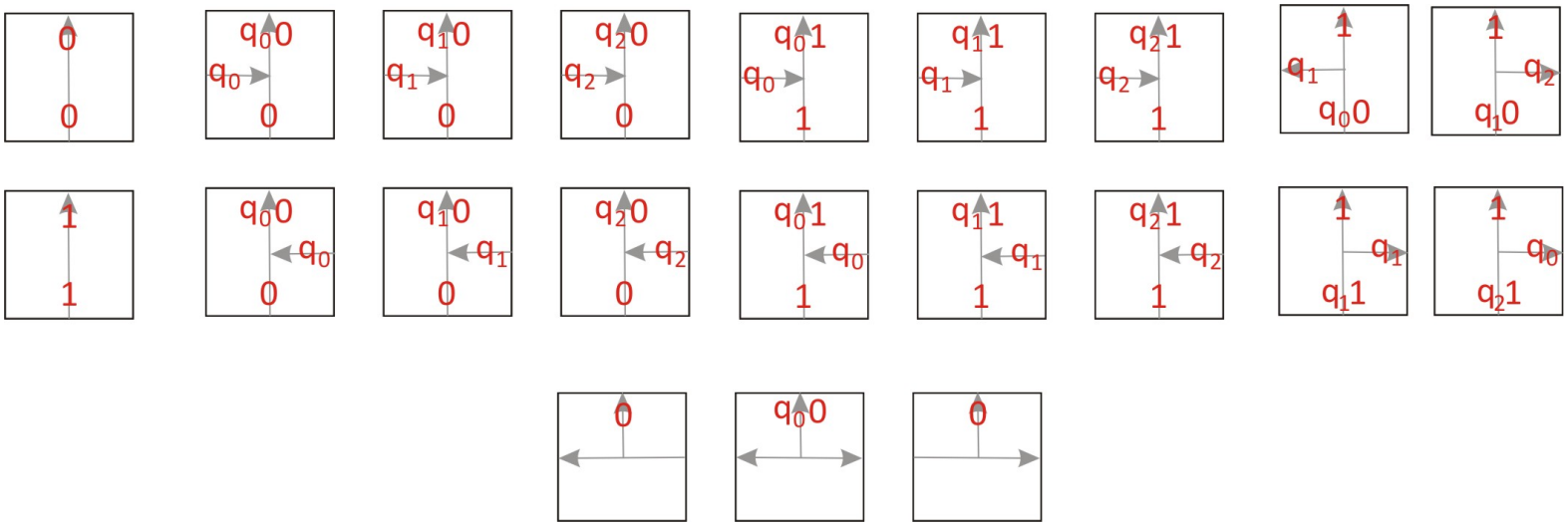


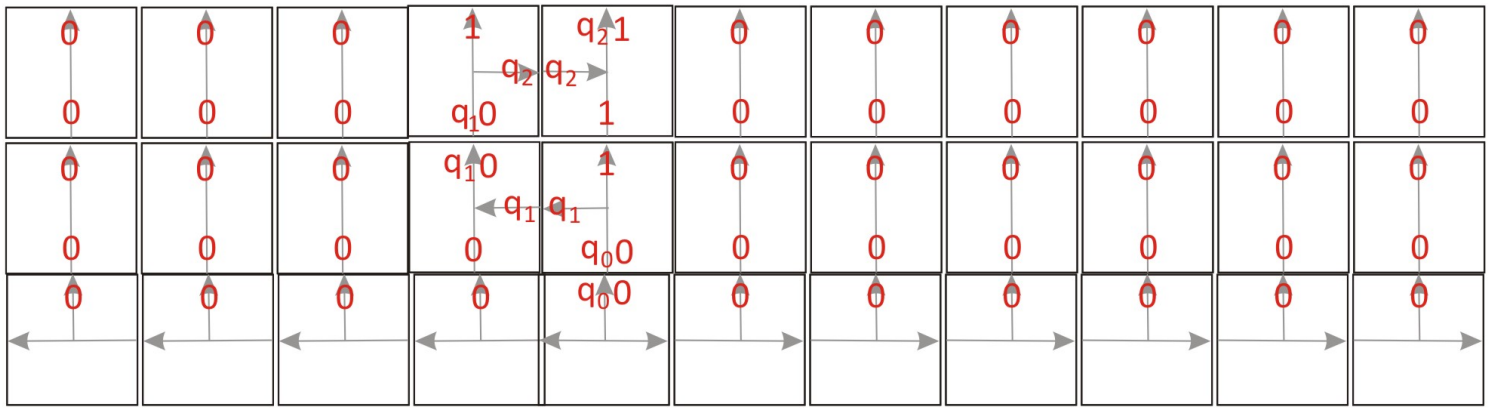
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



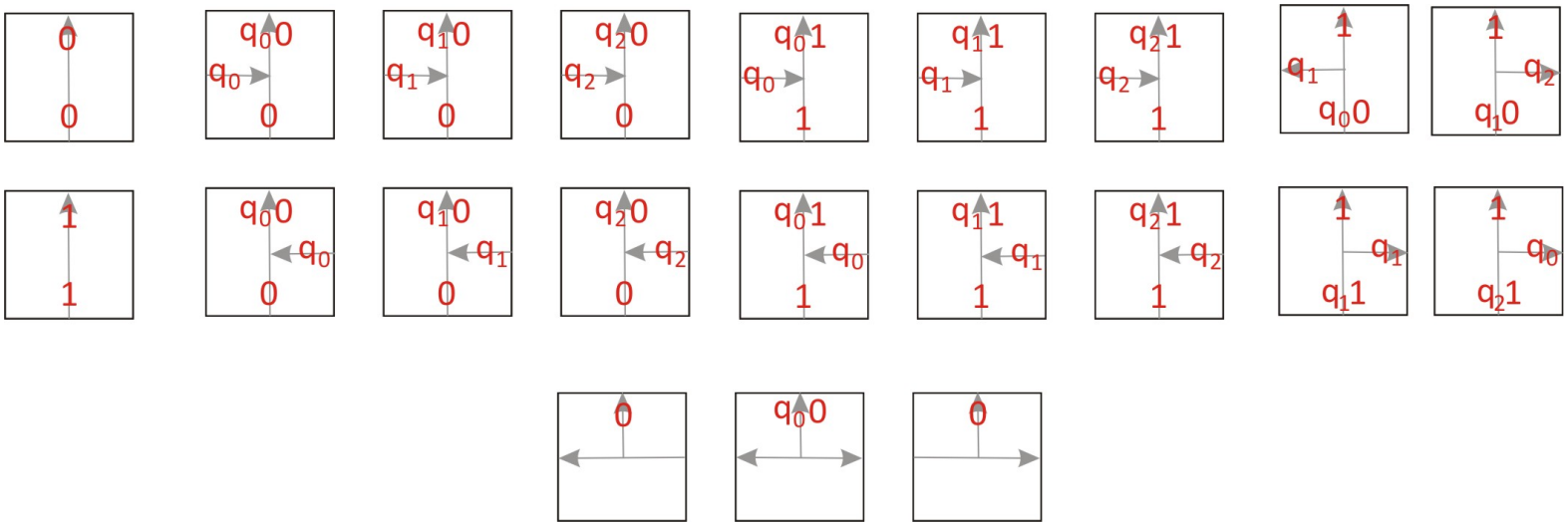


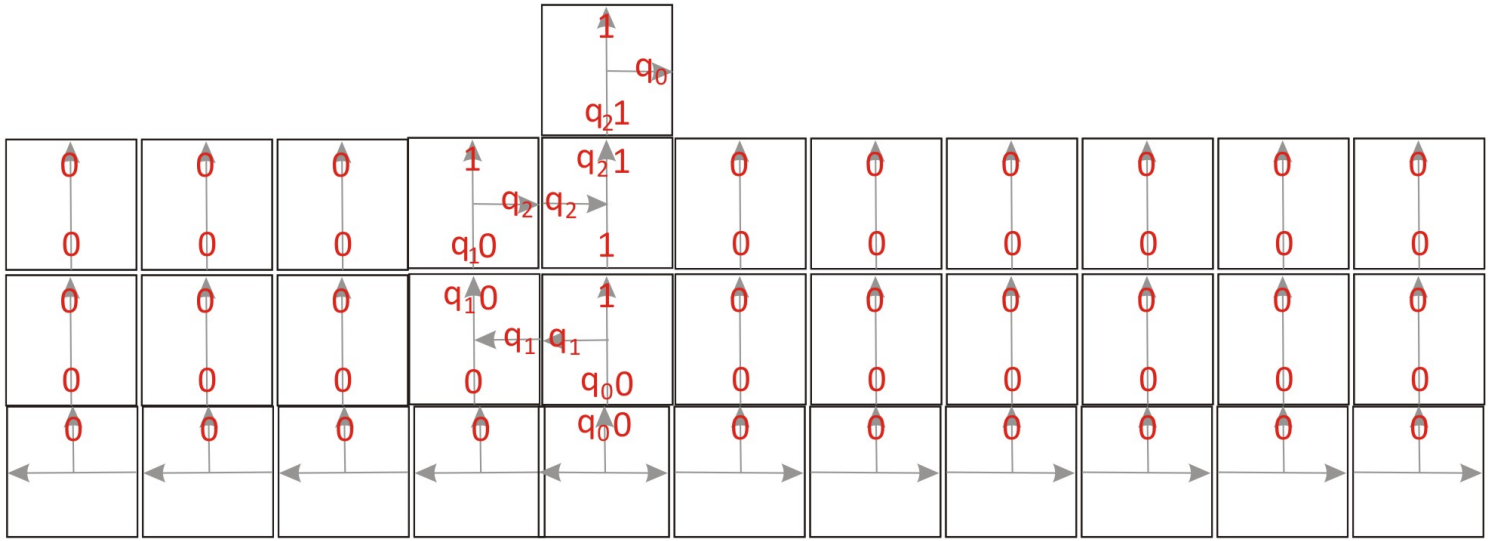
Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



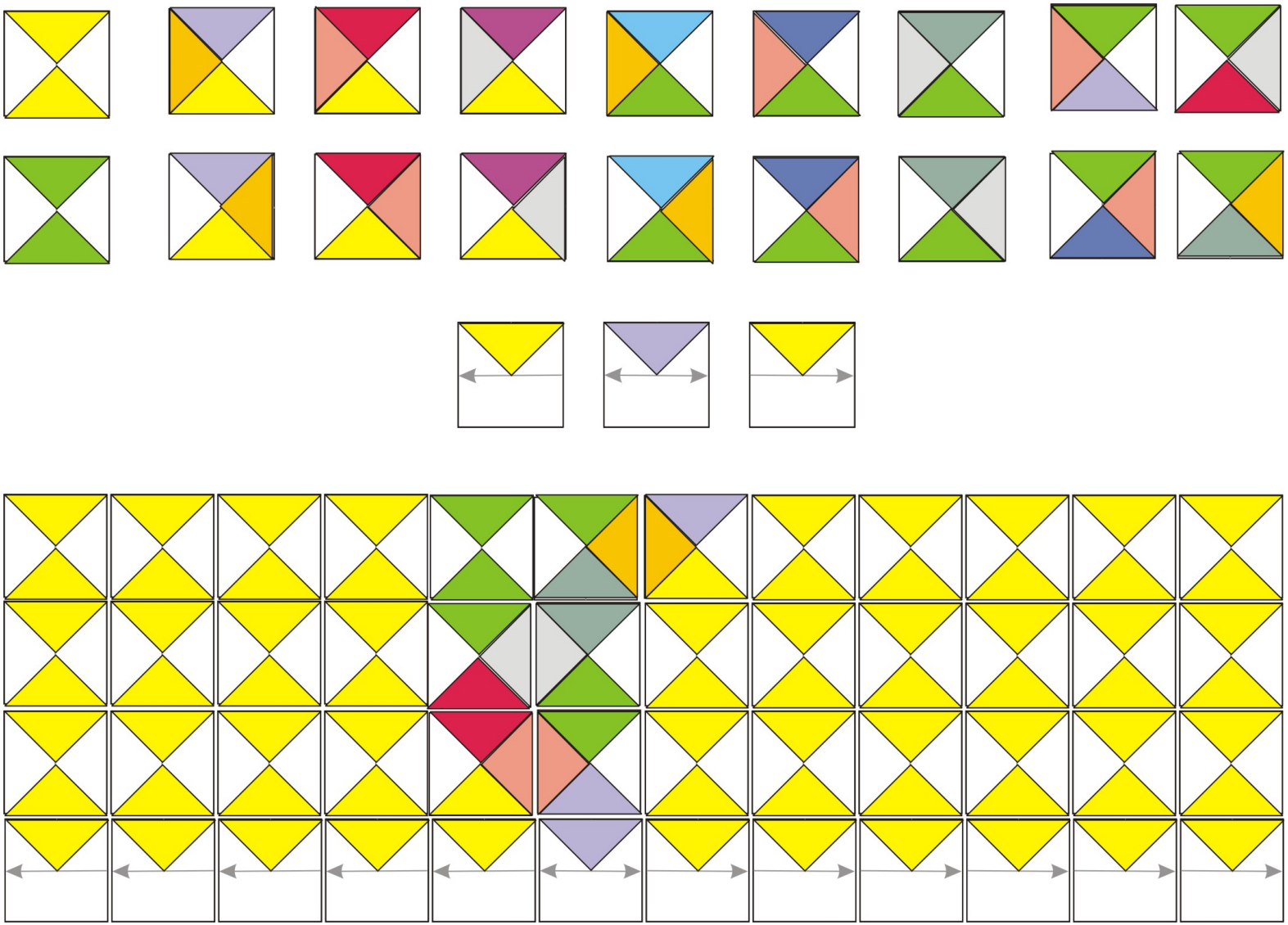


Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$





Primer $q_0 01 \mathrm{L} q_1$, $q_1 01 \mathrm{R} q_2$, $q_1 11 \mathrm{R} q_1$, $q_2 11 \mathrm{R} q_0$



Neodlučivost problema popločavanja ravni

Označimo sa $\langle T \rangle$ skup pločica odredjenih Tjuringovom mašinom T.
NAPOMENA. $\langle T \rangle$ je konačan skup pločica.

Tjuringova mašina T se ne zaustavlja na praznoj traci
akko
pločicama iz $\langle T \rangle$ je moguće prekriti poluravan sa odgovarajućom prvom vrstom.