1 Matice pro výpočet lineárních rekurencí (20 bodů)

Na úvod si ve stručnosti popišme, jak počítat Fibonacciho čísla pomocí umocňování matic; ve větších podrobnostech popsáno na konci kapitoly 3.1 textu Povídání o Lineární algebře. Nechť f_n je n-té Fibonacciho číslo, definováno takto:

$$f_0 = 0, \qquad f_1 = 1, \qquad f_{n+2} = f_{n+1} + f_n.$$

Uvažme matici A a vynásobme jí zprava vektorem obsahující dvě po sobě jdoucí Fibonacciho čísla:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} f_{k+1} \\ f_k \end{pmatrix} = \begin{pmatrix} f_k + f_{k+1} \\ f_{k+1} \end{pmatrix} = \begin{pmatrix} f_{k+2} \\ f_{k+1} \end{pmatrix},$$

tedy násobením A se posouváme v posloupnosti Fibonacciho čísel o jedna doprava. Proto platí, že

$$\underbrace{A \cdot A \cdots A}_{n\text{-krát}} \cdot \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = A^n \cdot \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = \begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix},$$

kde první rovnost platí díky asociativitě. Navíc A^n umíme spočítat v čase $\mathcal{O}(\log n)$.[1]

Zkusíme výše uvedený postup zobecnit. Máme nějakou obecnou zadanou lineární rekurentní posloupnost. První členy x_0 až x_{k-1} jsou předepsány. Každý další člen je lineární kombinace k předcházejících členů, tedy platí

$$x_{n+k} = c_{k-1}x_{n+k-1} + c_{k-2}x_{n+k-2} + \cdots + c_1 x_{n+1} + c_0 x_n$$

pro pevné koeficienty c_0 až c_{k-1}.

Příklad. Posloupnost může mít třeba určené první tři členy $x_0 = 1$, $x_1 = 2$, $x_2 = 3$ a další členy jsou určeny předpisem $x_{n+3} = x_{n+2} - x_{n+1} + 3x_n$. Začátek posloupnosti vypadá takto:

$$(1, 2, 3, 4, 7, 12, 17, 26, 45, \ldots).$$

Úloha 1.1. Zobecněte postup výpočtu pro obecnou lineární rekurenci. Pro zadané k a koeficienty $c_0, \ldots, c_{k-1}$ popište, jak se matice A zkonstruuje. Pochopitelně také dokážte, že má požadované vlastnosti. Tím pochopíte, jak jsme matici A pro Fibonacciho čísla získali.

Nápověda. Zkuste nejprve uvažovat posloupnosti pro $k = 2$, tedy posloupnosti, které závisí pouze na dvou předcházejících členech.

Poznámka. Matice A je zajímavá, i když nechceme zkonstruovat rychlý algoritmus, neboť z ní lze vydolovat vzorec pro n-tý člen lineární rekurence. K tomu se budou hodit vlastní čísla matice A. Ta nám umožní převést matici do Jordanova tvaru, ve kterém bude vzorec přímo vidět; viz úloha 4.

2 Permutační matice (25 bodů)

Permutace již známe z diskrétní matematiky. Permutace π je bijektivní zobrazení $\pi : X \to X$, tedy různým prvkům z X přiřazujeme různé prvky. Intuitivně je permutace pouze nějaké přeuspořádání prvků v X. Nás budou zajímat permutace množiny $X = \{1, 2, \ldots, n\}$.

Pro permutaci π je permutační matice P_π čtvercová matice $n \times n$ daná předpisem:

$$(P_\pi)_{ij} = \begin{cases} 1 & \text{pro } \pi(i) = j, \\ 0 & \text{jinak.} \end{cases}$$

[1] Využijeme půlení, neboť $a^n = \left(a^{\frac{n}{2}}\right)^2$. Pokud tento algoritmus neznáte, zkuste si rozmyslet detaily.

Tedy je to nula-jedničková matice, která má v každém řádku přesně jednu jedničku na pozici $(i, \pi(i))$.

Příklad. Ukážeme si dva příklady. Pro $n = 5$ mějme permutace π a σ dané následujícím předpisem (v druhém řádku je zapsáno, kam se čísla zobrazují):

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \qquad \text{a} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

Tyto permutace mají permutační matice P_π a P_σ (s vynechanými nulami):

$$P_\pi = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ 1 & & & & \\ & & & & 1 \\ & & & 1 & \end{pmatrix} \qquad \text{a} \qquad P_\sigma = \begin{pmatrix} & & 1 & & \\ 1 & & & & \\ & 1 & & & \\ & & & & 1 \\ & & & 1 & \end{pmatrix}.$$

Pro permutační matice vyřešte následující:

Úloha 2.1. Proč se permutačním maticím říká permutační? Uvažte, co permutační matice provádí s maticí A (pochopitelně správné velikosti), pokud ji násobí zleva či zprava.

Úloha 2.2. Permutační matice stejné velikosti lze násobit. Pro libovolné n-prvkové permutace π a σ má $P_\pi P_\sigma$ smysl. Ukažte, že součin permutačních matic je opět permutační matice a objevte, v jakém je vztahu k permutacím π a σ.

Úloha 2.3. Permutační matice mají plnou hodnost, $\mathrm{rank} P_\pi = n$. Tedy vždy existuje inverzní matice. Zjistěte pro libovolnou permutaci π, jak vypadá inverzní matice P_π^{-1}.

Úloha 2.4. Ukažte, že pro libovolnou permutační matici P_π existuje mocnina $k \geq 1$, že $P_\pi^k = I_n$. Jaká je nejmenší možná hodnota k?

3 Matice Pascalova trojúhelníku (20 bodů)

Část Pascalova trojúhelníku můžeme zapsat do matice $n \times n$ třemi způsoby: L_n je dolní trojúhelníková matice, U_n je horní trojúhelníková a S_n má zapsaný Pascalův trojúhelník po diagonálách. Formálně, pokud číslujeme prvky matice od 0 do $n-1$:

$$(L_n)_{i,j} = \binom{i}{j}, \qquad (U_n)_{i,j} = \binom{j}{i}, \qquad (S_n)_{i,j} = \binom{i+j}{i},$$

kde pochopitelně $\binom{i}{j} = 0$ pro nesmyslné hodnoty $j > i$.

Příklad. Například pro $n = 5$ vypadají matice takto (s vynechanými nulami):

$$L_5 = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix}, \qquad U_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ & 1 & 2 & 3 & 4 \\ & & 1 & 3 & 6 \\ & & & 1 & 4 \\ & & & & 1 \end{pmatrix}, \qquad S_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{pmatrix}.$$

Úloha 3.1. Jak bude vypadat součin $L_5 U_5$?

Úloha 3.2. Zobecněte získaný výsledek a popište součin $L_n U_n$. Pochopitelně pokud odvodíte obecný vztah, nemusíte řešit předchozí úlohu.

Nápověda. Zkuste objevit co nejvíc důkazů. Lze si součin rozepsat formálně pomocí definice součinu a vzpomenout si na sumy kombinačních čísel. Další možné řešení je provést Gaussovu eliminaci vzniklé matice $L_n U_n$ a udělat její LDU dekompozici. Co budou asi matice L a U? Za každý různý důkaz budou další body (různost posuzuje cvičící :)).

4 Mocniny Jordanovy matice (20 bodů)

Jordanova matice je *bloková diagonální matice* složená z čtvercových bloků umístěných podél diagonály, které se nazývají *Jordanovy buňky*. Jordanova buňka J_λ je matice, která má na diagonále hodnotu λ, nad diagonálou proužek jedniček a zbytek matice je nulový, příklad Jordanovy buňky 5×5 je na obrázku vlevo. Jordanova matice je složena z bloků umístěných na diagonálu, a každý blok je jedna Jordanova buňka. Příklad Jordanovy matice je na obrázku vpravo.

$$J_\lambda = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \qquad J = \begin{pmatrix} J_{\lambda_1} & & & \\ & J_{\lambda_2} & & \\ & & J_{\lambda_3} & \\ & & & J_{\lambda_4} \end{pmatrix}$$

Jordanova věta je jeden z fundamentálních výsledků lineární algebry a říká následující:

Věta (Jordanova normální forma)**.** *Pro každou čtvercovou matici A existuje regulární matice S a Jordanova matice J, že*

$$A = SJS^{-1}.$$

Například pro matici A pro výpočet Fibonacciho čísel z prvního úkolu (či konce kapitoly 3.1 textu Povídání o lineární algebře) dostáváme následující na první pohled odpudivou Jordanovu normální formu:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \frac{1-\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \\ & \frac{1-\sqrt{5}}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{\sqrt{5}} & \frac{\sqrt{5}+1}{2\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{\sqrt{5}-1}{2\sqrt{5}} \end{pmatrix} = SJS^{-1}.$$

Je velice užitečné umět pro matici A spočítat její k-tou mocninu A^k, s tím jsme se už setkali v prvním úkolu pro výše uvedenou A. Přesně v takové situaci se hodí Jordanova věta, která umožňuje A^k přesně určit. Platí totiž:

$$A^k = SJS^{-1}SJS^{1-} \cdots SJS^{-1} = SJ^kS^{-1}.$$

Tedy v případě k-té mocniny stačí umocňovat pouze Jordanovu matici. Například můžete zkusit z výše uvedeného rozkladu vyvodit vzorec pro k-té Fibonacciho číslo

$$f_k = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^k.$$

Cílem této úlohy je zjistit, jak vypadá k-tá mocnina Jordanovy matice. To lze samozřejmě spočítat přímo z definice maticového násobení, i když postup je to trochu pracný. Ukážeme si trikový výpočet založený na binomické větě. Pro začátek jedna ze základních vlastností blokových diagonálních matic:

Úloha 4.1. Předpokládejme, že umíme umocňovat Jordanovy buňky, tedy známe J_λ^k. Určete J^k v závislosti na J_λ^k.

4.1 Binomická věta

Binomická věta z kombinatoriky je následující identita, která platí pro všechna reálná čísla a a b a přirozená čísla k:

$$(a+b)^k = \binom{n}{0}a^0b^n + \binom{n}{1}a^1b^{n-1} + \binom{n}{2}a^2b^{n-2} + \cdots + \binom{n}{n-1}a^{n-1}b^1 + \binom{n}{n}a^nb^0.$$

Přesně v této podobě však binomická věta pro matice fungovat nemůže, totiž například:

$$(A+B)(A+B) = A(A+B) + B(A+B) = A^2 + AB + BA + B^2.$$

Protože součin matic obecně nekomutuje, neplatí obecně rovnost $(A+B)^2 = A^2 + 2AB + B^2$. Pokud se však $AB = BA$, binomická věta platí. Speciálně jsme ukázali na cvičeních, že αI_n komutuje s libovolnou maticí A.

Úloha 4.2. Čemu se rovná $(A + \alpha I_n)^k$?

4.2 Mocnina Jordanovy buňky

Zbývá vyřešit, jak vypadá k-tá mocnina Jordanovy buňky J_λ^k. To uděláme ve dvou krocích:

Úloha 4.3. Jak vypadá k-tá mocnina J_0^k?

Nápověda. Tady stačí postupovat z definice násobení, ale výsledek vyjde velice hezky.

Úloha 4.4. Jak vypadá k-tá mocnina J_λ^k?

Nápověda. Využijte binomickou větu.

5 Matice s vzorem šachovnice (25 bodů)

Na cvičení jsme dokázali, že třídy $\mathcal{U}$ horních trojúhelníkových matic, $\mathcal{L}$ dolních trojúhelníkových matic a $\mathcal{D}$ diagonálních matic jsou uzavřené na sčítání, násobení a inverze (pochopitelně pouze pokud inverze existují). Tedy například pro $A, B \in \mathcal{U}$ platí $A + B \in \mathcal{U}$, $AB \in \mathcal{U}$ a $A^{-1} \in \mathcal{U}$, pokud operace dávají smysl.

V této úloze chceme zjistit, jestli něco podobného platí pro dvě třídy matic $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ se šachovnicovým vzorem. Nejprve definujme tyto třídy. Čtvercová matice A patří do $\check{\mathcal{S}}_\ell$, právě když $(A)_{i,j} = 0$, kdykoliv $i + j$ je liché. Podobně čtvercová matice B patří do $\check{\mathcal{S}}_s$, právě když $(B)_{i,j} = 0$, kdykoliv $i + j$ je sudé. Na ostatní políčka matic neklademe žádné předpoklady, tedy například nulová matice patří do obou tříd.

Příklad. Několik příkladů těchto matic (s vynechanými nulami mimo šachovnicový vzor):

$$\underbrace{\begin{pmatrix} 1 & \\ & 2 \end{pmatrix}, \begin{pmatrix} 0 & & 1 \\ & 5 & \\ 0 & & 2 \end{pmatrix}, \begin{pmatrix} 1 & & 0 & \\ & 3 & & 17 \\ 0 & & \frac{1}{2} & \\ & 1 & & 0 \end{pmatrix}}_{\in \check{\mathcal{S}}_\ell} \quad \text{a} \quad \underbrace{\begin{pmatrix} & 1 \\ 2 & \end{pmatrix}, \begin{pmatrix} & 1 & \\ 3 & & 2 \\ & 0 & \end{pmatrix}, \begin{pmatrix} & 4 & & 0 \\ 4 & & 2 & \\ & 2 & & 7 \\ 0 & & 7 & \end{pmatrix}}_{\in \check{\mathcal{S}}_s}.$$

Úloha 5.1. Rozhodněte, zda jsou třídy $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ uzavřené na součet.

Úloha 5.2. Rozhodněte, zda jsou třídy $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ uzavřené na součin? Jsou součiny matic z těchto tříd v nějakém dalším vztahu; třeba pro AB, pokud $A \in \check{\mathcal{S}}_\ell$ a $B \in \check{\mathcal{S}}_s$?

Úloha 5.3. Rozhodněte, zda jsou třídy $\check{\mathcal{S}}_\ell$ a $\check{\mathcal{S}}_s$ uzavřené na inverze (opět s předpokladem, že pro A inverzní matice A^{-1} existuje)? Lze pro některé rozměry s jistotou říct, že matice není invertovatelná?

Nápověda. Inverze se počítá pomocí Gaussovy eliminace, která převede tvar $(A \mid I_n)$ na tvar $(I_n \mid A^{-1})$. Nelze nějak vhodně využít vlastností šachovnicového vzoru?

6 Dedekindovy řezy (30 bodů)

V této úloze se pokusíme seznámit s *Dedekindovými řezy*, pomocí nichž zavedeme reálná čísla. Tuto konstrukci vymyslel a publikoval Dedekind v roce 1872. Poznamenejme, že ve stejném roce Cantor publikoval alternativní zavedení reálných čísel jako limit Cauchyovských posloupností.

Samotnou konstrukci neprovedeme do nejmenších detailů, ostatně to by formálně zabralo několik stránek. Naším cílem bude poznat, jak tyto řezy fungují a proč mají vlastnosti, které po reálných čísel požadujeme. Tou nejklíčovější vlastností bude existence suprema každé neprázdné shora omezené množiny.

Na začátku máme uspořádané těleso racionálních čísel $\mathbb{Q}$, které splňuje následující vlastnosti: Sčítání a násobení je komutativní, asociativní, existují inverzní prvky a operace jsou svázané distributivitou, navíc máme definované lineární uspořádání (tedy tranzitivní antisymetrickou relaci). Budeme chtít toto těleso rozšířit, tedy vytvořit těleso reálných čísel $\mathbb{R}$ rozšiřující $\mathbb{Q}$, které bude splňovat velice silný axiom o supremu. Další veledůležitou vlastností racionálních čísel, kterou budeme potřebovat, je, že jsou *husté*, tedy že mezi každými dvěma racionálními čísly je jedno další. Formálně: Pokud $a, b \in \mathbb{Q}$ a $a < b$, potom existuje $c \in \mathbb{Q}$, že $a < c < b$.

6.1 Definice řezu

Budeme chtít využít faktu, že reálných čísel je přesně tolik, kolik je podmnožin racionálních čísel. Tedy reálná čísla budeme reprezentovat jako podmnožiny racionálních čísel. Ovšem ne ledajaké podmnožiny, budeme uvažovat pouze podmnožiny, které jsou *řezy*.

Řez α je podmnožina $\mathbb{Q}$, která splňuje tři podmínky:

1. α je neprázdná a rozdílná od celého $\mathbb{Q}$,
2. pokud $p \in \alpha$, $q \in \mathbb{Q}$ a $q < p$, potom i $q \in \alpha$,
3. pokud $p \in \alpha$, potom existuje r, že $p < r$ a $r \in \alpha$.

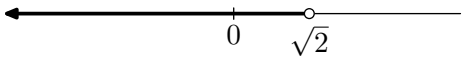
První podmínka říká, že řez je netriviální podmnožina. Druhá říká, že řez obsahuje s každým reálným číslem i všechna menší. Třetí naopak říká, že řez neobsahuje největší racionální číslo.

V dalším textu budeme řeckými písmeny $\alpha, \beta, \gamma, \ldots$ označovat řezy a normálními písmeny racionální čísla.

Úloha 6.1. Pro lepší seznámení s řezy dokažte:

1. Pokud $p \in \alpha$ a $q \notin \alpha$, potom $p < q$,
2. Pokud $r \notin \alpha$ a $r < s$, potom i $s \notin \alpha$.

Pan Dedekind nebyl cukrář, a tedy řezy se nejmenují řezy podle cukrárny. Tento název dostaly, neboť odpovídají rozříznutí reálné osy na dvě části. Reálné číslo r je reprezentováno tak, že vezmeme reálnou osu a rozřízneme ji v bodě r na dvě části. Řez reprezentující r jsou potom všechna racionální čísla menší než r. Například řez, který bude reprezentovat $\sqrt{2}$ bude množina všech racionálních čísel q menších než $\sqrt{2}$ (tedy to jsou buď čísla záporná nebo ty, že $q^2 < 2$). Tento řez je naznačen tučně na obrázku.



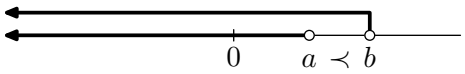
Abychom pomocí řezů vytvořili uspořádané těleso reálných čísel, budeme muset udělat čtyři věci:

1. Zadefinovat na řezech uspořádání,
2. zadefinovat operaci sčítání,
3. zadefinovat operaci násobení a
4. ukázat, že v sobě obsahují racionální čísla jako podtěleso.

Pokud bychom chtěli definici ověřit do všech detailů, museli bychom ukázat, že splňuje všechny axiomy uspořádaného tělesa. Takový důkaz by byl moc pracný, a proto ověříme jenom některé axiomy. I tak získáme dobrý náhled do toho, jak řezy fungují, díky čemuž by dokázání ostatních vlastností už nebylo obtížné.

6.2 Uspořádání na řezech

Na řezech nadefinujeme uspořádání zcela přirozeně. Řezy uspořádáme inkluzí, tedy $\alpha \prec \beta$, pokud $\alpha \subsetneq \beta$.



Úloha 6.2. Dokažte, že pro každé dva řezy nastane právě jedna z možností $\alpha \prec \beta$, $\alpha = \beta$ nebo $\alpha \succ \beta$.

Úloha 6.3. Dokažte, že je uspořádání tranzitivní: Pro každé tři řezy α, β, γ platí, že $\alpha \prec \beta$ a $\beta \prec \gamma$ implikuje $\alpha \prec \gamma$.

Úloha 6.4. Ukažte, že platí axiom o supremu. Tedy ukažte, že pro libovolnou neprázdnou shora omezenou podmnožinu řezů M existuje $\sup(M)$, nejmenší horní závora množiny M.

Nápověda. Uvažte množinu všech horních závor, každá z nich je řez. Definujte $\sup(M)$ jako průnik všech horních závor. Budete muset ukázat, že $\sup(M)$ je řez a že neexistuje žádná menší horní závora.

6.3 Sčítání řezů

Pro dva řezy α a β definujeme sčítání takto:

$$\alpha \oplus \beta = \{x + y \mid x \in \alpha, y \in \beta\}.$$

Pokud chceme něco dokázat o sčítáni řezů, potřebujeme využít vlastností sčítání v racionálních číslech. Jak by se dalo čekat, struktura racionálních čísel se přenese i na řezy.

Úloha 6.5. Dokažte, že sčítání $\oplus$ je komutativní a asociativní.

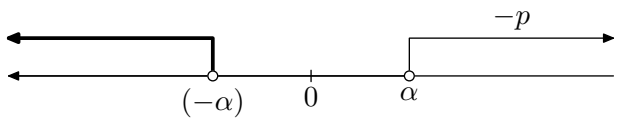
Neutrální prvek $0^\star$ definujeme jako množinu všech záporných racionálních čísel.[2]

Úloha 6.6. Dokažte, že $0^\star$ je skutečně neutrální prvek vůči operaci $\oplus$, tedy $\alpha \oplus 0^\star = \alpha$ pro každý řez α.

Definovat inverzní prvek bude maličko komplikovanější. Nechť α je libovolný řez. Definujme

$$(-\alpha) = \{p \mid p \in \mathbb{Q} \text{ a } \exists r > 0, \text{ že } -r - p \notin \alpha\}.$$

Jinými slovy, p leží v $(-\alpha)$, pokud nějaké racionální číslo menší než $-p$ neleží v α. Následující obrázek ilustruje definici. Množina všech $-p$ z definice odpovídá všem „větším racionálním číslům“ než těm obsažených v řezu α. Množina $(-\alpha)$ obsahuje racionální čísla k nim opačná.



Korektnost definice dokážeme ve dvou krocích:

Úloha 6.7. Dokažte, že pro každý řez α je množina $(-\alpha)$ řez, tedy splňuje podmínky (1) až (3) z definice řezu.

Úloha 6.8. Dokažte pro každý řez α, že $(-\alpha)$ je skutečně inverzní prvek ke sčítání, tedy $\alpha + (-\alpha) = 0^\star$.

[2] Značíme s hvězdičkou, abychom odlišili od neutrálního prvku $0 \in \mathbb{Q}$.

6.4 Násobení řezů

Definovat násobení je kvůli znaménku maličko složitější než definovat sčítání. Omezíme se proto nejprve jenom na kladné řezy. Nechť $\alpha \succ 0^\star$ a $\beta \succ 0^\star$, potom definujeme

$$\alpha \odot \beta = \{p \mid \exists r \in \alpha, \exists s \in \beta, \text{ že } r \geq 0 \text{ a } p < rs\}.$$

Úloha 6.9. Ukažte, že pro libovolné dva řezy $\alpha \succ 0^\star$ a $\beta \succ 0^\star$ je $\alpha \odot \beta$ řez.

Podobně jako výše, lze snadno ukázat, že násobení splňuje všechny axiomy tělesa. Jako neutrální prvek $1^\star$ se použije množině všech racionálních čísel menších než jedna. Pro $\alpha \succ 0^\star$ se definuje inverzní prvek jako

$$\alpha^{-1} = \left\{p \mid p \leq 0 \text{ nebo } \exists r > 0, \text{ že } \tfrac{1}{p} - r \notin \alpha\right\}.$$

Protože však důkaz by byl hodně podobný výše uvedeným důkazům pro sčítání, detaily si zde odpustíme.

Dodefinovat násobení pro všechny řezy je jednoduché. Pro libovolný řez α platí, že $\alpha \odot 0^\star = 0^\star \odot \alpha = 0^\star$. Dále definujeme

$$\alpha \odot \beta = \begin{cases} -((-\alpha) \odot \beta), & \text{pokud } \alpha \prec 0^\star \text{ a } \beta \succ 0^\star, \\ (-\alpha) \odot (-\beta), & \text{pokud } \alpha \prec 0^\star \text{ a } \beta \prec 0^\star, \\ -(\alpha \odot (-\beta)), & \text{pokud } \alpha \succ 0^\star \text{ a } \beta \prec 0^\star, \\ \alpha \odot \beta, & \text{jinak platí původní definice.} \end{cases}$$

Inverzní prvky se dodefinují podobně, pro $\alpha \prec 0^\star$ definujeme $\alpha^{-1} = (-((-\alpha)^{-1}))$. Opět vynecháme detaily důkazů, že násobení splňuje axiomy tělesa.

Úloha 6.10. Ukažte, že pro libovolné dva řezy α a β je $\alpha \odot \beta$ řez.

Tím je odvození téměř dokončeno. Víme, že takto sestrojené řezy tvoří uspořádané těleso, které má supremum pro libovolnou neprázdnou shora omezenou množinu.

6.5 Vnoření racionálních čísel

Zbývá dokázat, že vzniklé těleso obsahuje racionální čísla jako podtěleso. Pro racionální číslo r uvažujme množinu $r^\star$ definovanou takto:

$$r^\star = \{p \mid p \in \mathbb{Q}, p < r\}.$$

Úloha 6.11. Pro libovolné racionální číslo r platí, že $r^\star$ je řez.

Úloha 6.12. Sčítání řezů reprezentujících racionální čísla odpovídá sčítání racionálních čísel, tedy pro libovolná dvě racionální čísla r a s je $r^\star \oplus s^\star = (r+s)^\star$.

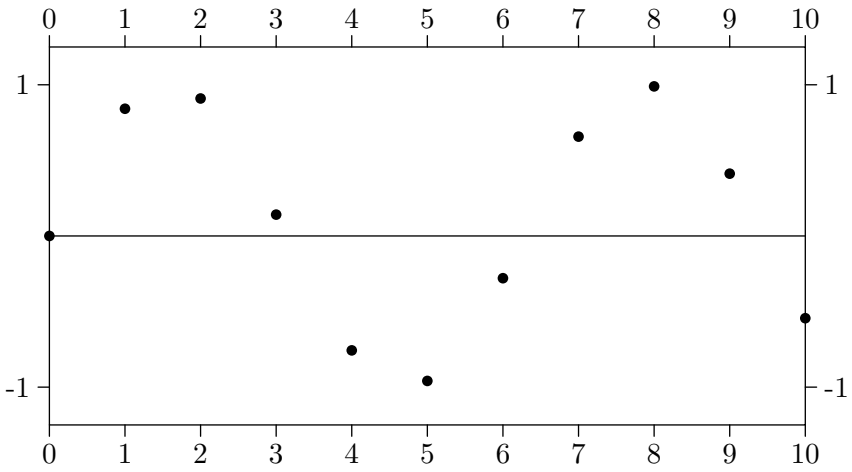
Podobně lze dokázat, že pro libovolná dvě racionální čísla r a s platí, že $r^\star \odot s^\star = (rs)^\star$ a $r^\star \prec s^\star$, právě když $r < s$. Z toho vyplývá, že každé racionální číslo r můžeme zidentifikovat s řezem $r^\star$.

6.6 Shrnutí

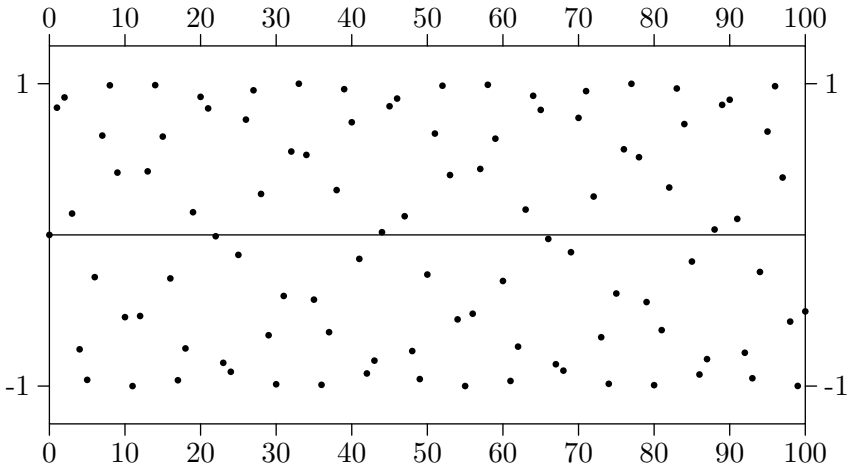
V této úloze jsme popsali, jak pomocí Dedekinových řezů zkonstruovat z uspořádaného tělesa $(\mathbb{Q}, +, \cdot, <)$ jiné uspořádané těleso $(\mathbb{R}, \oplus, \odot, \prec)$ splňující axiom o supremu. Navíc jsme ukázali, že lze těleso $\mathbb{Q}$ vnořit do nově zkonstruovaného tělesa $\mathbb{R}$.

7 Jen jeden sinus? (25 bodů)

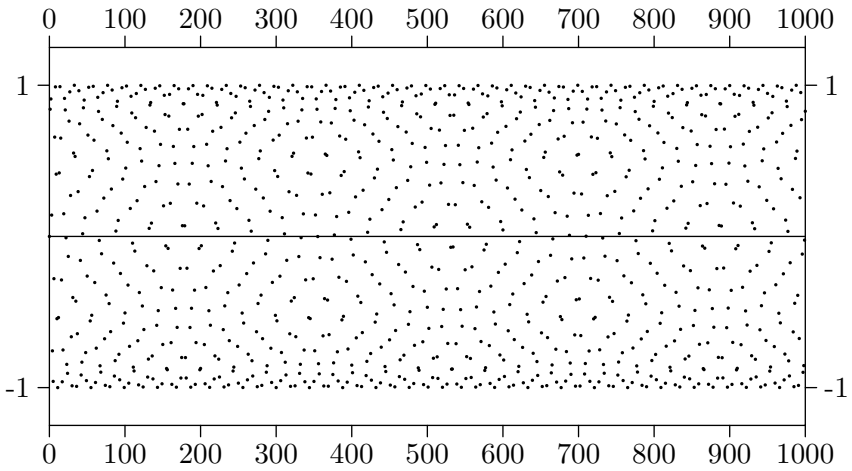
Čtenář určitě dobře zná křivku funkce $\sin x$. V této úloze se zaměříme na posloupnost $\{\sin n\}_{n=0}^{\infty}$ a její počáteční úsek. Ukážeme si, že změna měřítka může mít velký vliv. Prvních deset členů posloupnosti vypadá přesně tak, jak čtenář očekává.

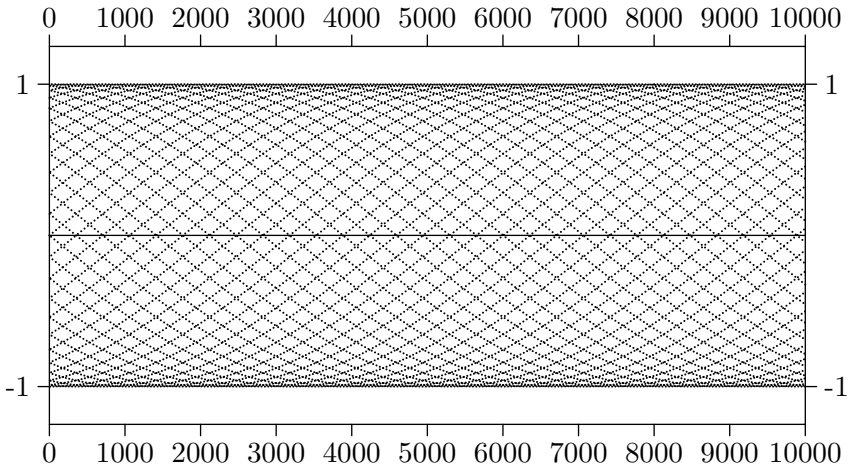


Pro prvních sto členů vypadá obrázek mnohem chaotičtěji. Ostatně to dává smysl, protože jsme hodnoty desetkrát více nahustili vedle sebe, tedy jednotlivé obloučky funkce $\sin x$ začnou splývat.



Zkusíme tedy zobrazit prvních tisíc a prvních deset tisíc členů, což vytvoří dva různé překvapivé vzory. Pro tisíc členů dostáváme jakýsi vzor šestiúhelníků. Ty vidíme kvůli našemu vnímání, které spojuje nesouvisející věci. Pro deset tisíc však dostáváme ještě překvapivější vzor, který vůbec nevypadá jako posloupnost; vidíme řadu sinusovek položených přes sebe.





Možná je překvapivé, že se obrázky pro tisíc a deset tisíc bodů tolik liší. Zkuste se však na obrázek pro tisíc bodů podívat ze strany a uvidíte posunuté sinusovky.

Úloha 7.1. Vaším úkolem je poslední obrázek pochopit a vysvětlit. Proč na obrázku vidíme přes sebe položené sinusovky? Kolik těch sinusovek je a jakou mají periodu? Proč obrázek vypadá symetricky kolem osy x?

Nápověda. Co víte o aproximaci čísla π? Můžete k analyzování posloupnosti používat libovolný matematický software a zkusit lépe pochopit, jak se hodnoty posloupnosti $\{\sin n\}_{n=1}^{\infty}$ chovají.

8 Konečná tělesa existují jen pro mocniny prvočísla (40 bodů)

V této úloze si ukážeme část z důkazu následující algebraické věty.

Věta. *Konečné těleso $\mathbb{F}$ řádu $ř$ existuje, právě když $ř$ je mocnina prvočísla p^k.*

Dokonce platí, že konečně těleso daného řádu je určeno jednoznačně (až na přejmenování prvků, kterému se odborně říká *isomorfismus*). Tato věta tedy opodstatňuje označení $\mathbb{GF}(p^k)$, neboť těleso řádu p^k je jednoznačně určené. V důkazu ukážeme, že každé takové těleso je vysoce symetrický objekt, který v sobě skrývá vektorový prostor. To je poměrně překvapivé, neboť v definici tělesa se vektorové prostory vůbec nevyskytují a naopak ty se definují pomocí těles.

Co o tělesech už známe ...

V samotném důkazu můžeme použít *pouze axiomy tělesa* a jejich důsledky! Připomeňme si, co říkají axiomy tělesa:

- Těleso je struktura s dvěma operacemi – sčítáním a násobením.
- Těleso obsahuje dva speciální prvky, neutrální prvek na sčítání (budeme značit 0) a neutrální prvek na násobení (značíme 1).
- Z hlediska sčítání se těleso chová jako grupa – máme inverzní prvky a neutrální prvek.
- Z hlediska násobení se těleso bez 0 chová jako grupa – opět máme inverze a neutrální prvek.
- Navíc operace sčítání a násobení jsou dohromady svázané distributivitou.

Z axiomů lze odvodit i další vlastnosti těles, některé jsme již viděli.

- Neutrální prvky 0 a 1 a inverze pro obě operace jsou určeny jednoznačně. Ostatně to platí obecně i v grupách.
- Libovolný násobek 0 je zase nula: $a \cdot 0 = 0$.

- Pokud $a + b = a + c$, potom $b = c$.
- Podobně pro násobení a $a \neq 0$, pokud $a \cdot b = a \cdot c$, potom $b = c$.
- Neexistují dvě nenulová čísla a a b, že $a \cdot b = 0$.

$\mathbb{Z}_p$ je podtěleso $\mathbb{F}$

Na rozjezd vyřešíme tělesa s prvočíselnou velikostí. Uvažujme strukturu $\mathbb{Z}_k$ tvořenou čísly $0, \ldots, k-1$ a operacemi sčítaní a násobení definovanými jako zbytek po celočíselném sčítání a násobení.

Příklad. Například pro $\mathbb{Z}_4$ a prvky $a = 2$ a $b = 3$ dostaneme, že $a + b = 1$ a $a \cdot b = 2$, neboť přesně takové zbytky mají čísla 5 a 6 po dělení 4.

Úloha 8.1. Dokažte, že $\mathbb{Z}_p$ je těleso, právě když p je prvočíslo.

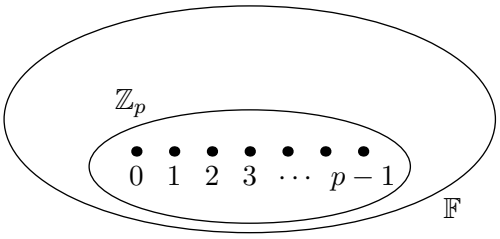
Nápověda. Pokud p není prvočíslo, není těžké nalézt dvojici, která porušuje poslední vlastnost. Pro prvočísla to se sčítáním bude docela jednoduché. Je však třeba pro každý prvek a ukázat, že násobení tímto prvkem je prosté, tedy že neexistuje dvě rozdílná čísla b a c, aby $a \cdot b = a \cdot c$.

Charakteristika tělesa je nejmenší přirozené číslo k takové, že součet k jedniček $1+1+\cdots+1 = 0$, případně 0, pokud takové k neexistuje (třeba reálná čísla).

Úloha 8.2. Dokažte, že pro každé konečné těleso $\mathbb{F}$ je jeho charakteristika nějaké prvočíslo p.

Nápověda. Ukažte nejprve, že charakteristika je nenulová. Poté zkuste dokazovat sporem. Kdyby charakteristika nebyla prvočíselná, co by bylo špatně?

Označme součet k jedniček pomocí k. V tělese tedy máme prvky $0, \ldots, p-1$. O dalších prvcích zatím nic nevíme.



Úloha 8.3. Ukažte, že prvky $0, \ldots, p-1$ tvoří podtěleso totožné $\mathbb{Z}_p$.

Cože? Těleso je vektorový prostor?

Nyní využijeme získané znalosti o tělesech a dokončíme důkaz překvapivým úskokem, však posuďte sami.

Úloha 8.4. Dokažte, že každé konečné těleso $\mathbb{F}$ charakteristiky p je vektorový prostor $\mathbb{V}$ nad tělesem $\mathbb{Z}_p$. Operace $\mathbb{V}$ definujeme takto: sčítání vektorů odpovídá sčítání v tělese a skalární násobení násobením v tělese (protože $\mathbb{Z}_p$ je podtěleso $\mathbb{F}$, lze to takto definovat).

Nápověda. K tomu potřebujeme dokázat, že vzniklá struktura splňuje všechny axiomy vektorového prostoru. Neplyne to snadno z toho, že $\mathbb{F}$ je těleso?

Víme, že vektorové prostory tvoří silně předurčenou strukturu, pojďme toho tedy využít. Vektorový prostor $\mathbb{V}$ má totiž konečnou dimenzi k. Podle Steinitzovy věty víme, že existuje nějaká báze $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Sice vůbec netušíme, jak vypadá, ale to nebudeme potřebovat – stačí vědět, že existuje.

Bude se hodit ještě jedno obecné tvrzení o bázích a lineárních kombinacích.

Úloha 8.5. Dokažte, že pokud $\mathbf{b}_1, \ldots, \mathbf{b}_k$ je báze vektorového prostoru, potom její různé lineární kombinace definují různé vektory. Tedy dokažte, že $\sum_{i=1}^{k} \alpha_i \mathbf{b}_i = \sum_{i=1}^{k} \bar{\alpha}_i \mathbf{b}_i$ implikuje, že $\alpha_i = \bar{\alpha}_i$.

Dokončení důkazu

A na závěr složme oba poznatky dohromady.

Úloha 8.6. Dokažte, že každé konečné těleso $\mathbb{F}$ má p^k prvků.

Nápověda. Kolik rozdílných lineárních kombinací vektorů $\mathbf{b}_1, \ldots, \mathbf{b}_k$ existuje?

Tím jsme ukázali neexistenci konečného tělesa velikosti, která není mocnina prvočísla. Také vám přijde trik hezký? Pokud jste se dostali až sem (a případně všechna tvrzení po cestě dokázali), máte můj obdiv (a zasloužíte si své body :)).

9 Hadamardovy matice dají nejvíce! (30 bodů)

V této úloze se budeme zabývat speciálními čtvercovými maticemi, které se nazývají Hadamardovy. Mají překvapivě zajímavou kombinatorickou strukturu a používají se například v teorii samoopravných kódu nebo ve statistice. Jeden ze základních otevřených problémů je, pro které velikosti vůbec existují. Ukážeme si konstrukci pro velikosti ve tvaru 2^k a také překvapivou souvislost Hadamardových matic s determinantem.

Definice. Matice $H \in \{-1, 1\}^{n \times n}$ se nazývá *Hadamardova*, pokud platí

$$HH^\mathsf{T} = H^\mathsf{T}H = nI_n.$$

Tedy Hadamardova matice je tvořená ± 1 a má ortogonální řádky a sloupce.

Například Hadamardova matice řádu dva vypadá takto: $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Nejprve vypozorujme:

Úloha 9.1. Nechť H je Hadamardova matice $n \times n$. Potom $n = 1, 2$ nebo je dělitelné čtyřmi.

Nápověda. Nejprve zkuste dokázat dělitelnost dvěma (s výjimkou $n = 1$). Pokud H je Hadamardova matice, můžeme s ní provádět určité úpravy, které „hadamardovost“ zachovávají.

Základní hypotéza Hadamardových matic říká, že Hadamardova matice existuje pro každé $n = 4k$. Je známo pouze několik různých konstrukcí, z nichž dostaneme Hadamardovy matice pouze pro některé řády.[3] Ukážeme si Sylvesterovu konstrukci pro $n = 2^k$. Pokud vymyslíte či nastudujete nějakou jinou konstrukci a naučíte mě ji, můžete dostat bonusové body.

Úloha 9.2. Dokažte, že existuje Hadamardova matice H_n velikosti $n \times n$ pro každé $n = 2^k$.

Nápověda. Zkuste objevit induktivní konstrukci, která vytvoří H_{2n} nějakým způsobem z matice H_n. Také můžete využít Kroneckerův součin matic, který se definuje takto: Nechť A je matice $m \times n$ a B je matice $p \times q$. Kroneckerův součin $A \otimes B$ je matice $mp \times nq$ tvořená $m \times n$ bloky velikosti $p \times q$ tak, že blok na souřadnicích (i, j) je matice $a_{i,j}B$. Jestliže A a B jsou Hadamardovy matice, jak vypadá $A \otimes B$? Příklad součinu $A \otimes B$:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & \\ 2 & -1 \end{pmatrix}, \qquad \text{potom} \qquad A \otimes B = \left(\begin{array}{cc|cc|cc} 1 & & 2 & & 3 & \\ 2 & -1 & 4 & -2 & 6 & -3 \\ \hline 4 & & 5 & & 6 & \\ 8 & -4 & 10 & -5 & 12 & -6 \end{array}\right).$$

Na závěr dokažme, že Hadamardovy matice jsou extremální matice pro následující větu. Objevil ji sám Hadamard v roce 1893, čímž započal zkoumání Hadamardových matic.

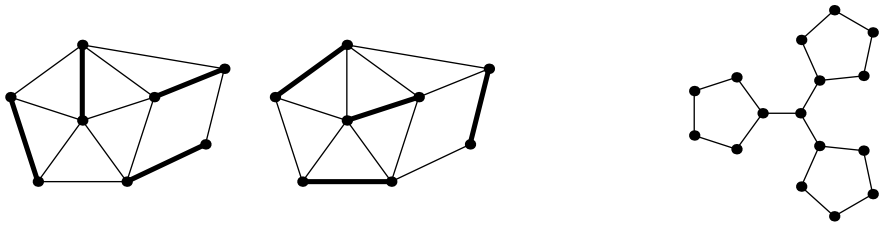
Úloha 9.3. Mějme matici A velikosti $n \times n$, že $|a_{i,j}| \leq 1$ ve všech pozicích (i, j). Potom platí $|\det(A)| \leq n^{n/2}$ a rovnosti se nabývá právě tehdy, když A je Hadamardova matice.

Nápověda. Využijte toho, že absolutní hodnota determinantu odpovídá objemu rovnoběžnostěnu určeného řádky matice. Pokud máme rovnoběžnostěn určený vektory $\mathbf{x}_{(1)}, \ldots, \mathbf{x}_{(n)}$, jaký je jeho maximální objem v závislosti na normách $\|\mathbf{x}_{(1)}\|, \ldots, \|\mathbf{x}_{(n)}\|$? A kdy se tohoto maxima přesně nabývá?

[3] Otevřené řády do dvou tisíc jsou 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948 a 1964. Například matice řádu 428 byla zkonstruována teprve nedávno, v IPM v Tehránu v roce 2005.

10 Determinují determinanty perfektní párování? (25 bodů)

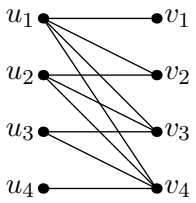
V této úloze si ukážeme jednu kombinatorickou aplikaci determinantů. *Párování* P je množina hran, které nesdílejí koncové vrcholy. Tedy žádný vrchol grafu je incidenční s nejvýše jednou hranou z P. Párování je *perfektní*, pokud obsahuje $\frac{n}{2}$ hran, kde n je počet vrcholů grafu; tedy každý vrchol je spárovaný s nějakým jiným. Pochopitelně ne každý graf obsahuje perfektní párovaní. Minimálně musí být počet vrcholů sudý, aby vůbec perfektní párování mohlo existovat. Na obrázku jsou pro graf vlevo vyznačena dvě různá perfektní párování, pro graf vpravo žádné perfektní párování neexistuje. (Proč?)



Pro jednoduchost se v této úloze zaměříme na bipartitní grafy. Mějme bipartitní graf G s dvěma partitami $U = \{u_1, \ldots, u_m\}$ a $V = \{v_1, \ldots, v_n\}$. Ten lze popsat incidenční matici partit I_G velikosti $m \times n$ takovou, že

$$(I_G)_{i,j} = \begin{cases} 1, & \text{pokud } u_i v_j \in E(G), \\ 0, & \text{pokud } u_i v_j \notin E(G). \end{cases}$$

Například pro níže uvedený graf G dostaneme následující matici I_G:



$$I_G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}$$

Aby perfektní párování vůbec mohlo existovat, musí platit $|U| = |V|$, tedy matice I_G musí být čtvercová. Vaším úkolem je zjistit, jaký je vztah mezi $\det(I_G)$ a existencí perfektního párování.

Úloha 10.1. Dokažte, že pokud $\det(I_G) \neq 0$, graf G má nutně perfektní párování.

Úloha 10.2. Rozhodněte a zdůvodněte, zda platí i obrácená implikace: Pokud G obsahuje perfektní párování, potom $\det(I_G) \neq 0$. Je nějaký vztah mezi hodnotou determinantu a počtem různých perfektních párování?

Poznámka. Výše uvedený vztah lze zobecnit i na nebipartitní grafy, i když je to maličko komplikovanější a souvisí to s počtem cyklických pokrytí grafu. Přesný počet perfektních párování bipartitního grafu je roven *permanentu* $\operatorname{perm}(I_G)$, což je „determinant bez znaménka“:

$$\operatorname{perm}(A) = \sum_{\pi \in S_n} \prod_{i=1}^{n} a_{i,\pi(i)}.$$

Určit počet perfektních párování i pro bipartitní graf (a tedy i výpočet permanentu matic obsahujících pouze nuly a jedničky) je #P-úplný problém, což znamená, že pro to (pravděpodobně) neexistuje polynomiální algoritmus.[4] Zatímco determinant můžeme spočítat efektivně, drobná změna v definici na permanent způsobí, že se tato formule efektivně určit nedá.

[4] Třída #P obsahuje počítací verze problémů z NP. Například problém existence hamiltonovské kružnice patří do NP a příslušný problém určení počtu různých hamiltonovských kružnic patří do #P. Pochopitelně každý problém z #P je alespoň tak těžký jako příslušný rozhodovací problém v NP. Problém je #P-úplný, pokud je to nejtěžší problém v #P.