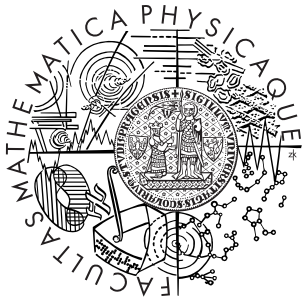
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Miroslav Štrupl

Náhodné procházky na grupách

Katedra algebry

Vedoucí bakalářské práce: Mgr. Pavel Příhoda, Ph.D.

Studijní program: Matematika

Obor: Obecná matematika

2010

Rád bych na tomto místě poděkoval vedoucímu práce za nabídnutí zajímavého tématu a ochotu věnovat mi čas na nezbytné konzultace a dále za vydatnou pomoc při dokončení práce.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 23.5.2010 Miroslav Štrupl

Obsah

Název práce: Náhodné procházky na grupách
Autor: Miroslav Štrupl
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Pavel Příhoda, Ph.D.
e-mail vedoucího: prihoda@karlin.mff.cuni.cz
Abstrakt: V první části práce jsou shrnuty některé pojmy z teorie pravděpodobnosti související s náhodnými procházkami, dále pojmy z teorie reprezentací konečných grup na konečně-dimenzionálních komplexních vektorových prostorech a je popsána Fourierova transformace na konečných grupách.

Druhá část je věnována samotnému řešení cvičení z předloženého textu [1]. Cvičení se týkají například souvislosti Markovových řetězců s dvojnásobně stochastickou maticí a náhodných procházek na symetrické grupě. Dále jsou rozebrány různé vlastnosti variační vzdálenosti dvou rozdělení včetně horních a dolních odhadů. Variační vzdálenost je dále používána k stanovení rychlosti konvergence náhodné procházky k rovnoměrnému rozdělení. Velká část cvičení je věnována náhodným procházkám na cyklických grupách, například stanovení dolní meze na rychlost konvergence, vyšetřování průběhu rozdělení. Poslední sada cvičení je věnována náhodné procházce na afinní grupě a souvisejícímu problému generování náhodných čísel.
Klíčová slova: náhodná procházka, reprezentace konečných grup, Fourierova transformace

Title: Random Walks on Groups
Author: Miroslav Štrupl
Department: Department of Algebra
Supervisor: Mgr. Pavel Příhoda, Ph.D.
Supervisor's e-mail address: prihoda@karlin.mff.cuni.cz
Abstract: In the first part some probability theory dealing with random walks is summarized, further representation theory of finite groups together with powerful tool of Fourier transform is described.

The second part is dedicated to solutions of exercises in the text [1]. First exercise is concerned with relation of Markov chains with doubly stochastic matrix and random walks on symmetric group. Further some properties of variation distance are explored including lower and upper bounds. The variation distance is then frequently used to access convergence speed of a random walk to the uniform distribution. Major part of exercises deals with random walks on a cyclic group, for e.g. lower bounds on convergence speed are assessed and some properties concerning shape of underlying distributions are investigated. The last set of exercises is dedicated to study of random walks on the affine groups and to the related problem of generating a random number.
Keywords: random walk, representation of finite groups, Fourier transform

Kapitola 1

Shrnutí pojmů použitých při řešení

V této části uvádím definice pojmů a lemmata, která v druhé části používám k řešení cvičení z [1]. Snaha je pokud možno uvést alespoň znění použitých vět s referencemi na důkazy, to se podařilo například u teorie reprezentací. Náhodná procházka na grupě není v [1] pořádně definována, a proto uvádím vlastní definici a dokazuji některé použité vlastnosti. To se může zdát trochu zbytečné (náhodná procházka na grupě je přímočarým zobecněním náhodné procházky na celých číslech uvedené v [4]). Na druhou stranu bez přesných definic nelze nic dokázat (a tedy vyřešit cvičení). Dále v lemmatech o náhodných procházkách na grupách jsou vidět zajímavé souvislosti teorie pravděpodobnosti, formálních polynomů a řad (konvoluce) a samozřejmě teorie grup. Například je ukázáno, že homomorfním obrazem náhodné procházky je opět náhodná procházka (lemma 4 II), dále souvislost "míry konvergence náhodné procházky" a jejího homomorfního obrazu (lemma 18).

1.1 Markovův proces v diskrétním čase, náhodná procházka na konečné grupě, konvoluce

$\mathbb{N} = \{1, 2, \ldots\}$ značím přirozená čísla, definuji $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Definice 1. *(Markovův proces v diskrétním čase [4], 2.1, Definice, str.15) Buď $(\Omega, \mathcal{A}, P)$ pravděpodobnostní prostor, $S \subset \mathbb{N}$ množina.* ***Markovovým procesem v diskrétním čase*** *nazveme posloupnost náhodných veličin $(X_k)_{k=0}^{\infty}$ s hodnotami v S, která splňuje tzv.* ***Markovovu vlastnost***

$$\forall k \in \mathbb{N}_0 \quad P(X_{k+1}|X_k, \ldots, X_0) = P(X_{k+1}|X_k), \quad \textit{má-li levá strana smysl.}^{1}$$

Prvky množiny S se nazývají stavy procesu a S množina stavů. ***Konečný Markovův proces*** *je Markovův proces s konečnou množinou stavů. Pravděpodobnosti*

$$P(X_{k+1}|X_k)$$

[1] Levá strana má smysl (podmíněná pravděpodobnost na levé straně je definována) pro $P(X_k, \ldots, X_0) > 0$. Tedy má-li smysl levá stana, má ho i paravá strana, protože $P(X_k, \ldots, X_0) > 0 \Rightarrow P(X_k) > 0$ a Markovova vlastnost vyžaduje, aby se pak obě strany rovnaly.

se nazývají ***pravděpodobnosti přechodu****. Markovův proces je* ***homogenní****, jsou-li pravděpodobnosti přechodu v čase k konstantní. Rozdělení*

$$P(X_0)$$

se nazývá ***iniciální rozdělení*** *Markovova procesu.*

Posloupnosti $(X_k)_{k=0}^{\infty}$ budu dále značit zkráceně (X_k). Dále budu pracovat s náhodnými veličinami, jejichž hodnoty budou mít význam prvků nějaké spočetné (většinou konečné) grupy G. Formálně správné by bylo zvolit nějaké očíslování prvků grupy (bijekci) $b : G \to S \subset \mathbb{N}$, náhodnou veličinu X definovat jako zobrazení do S a v případě, že budu chtít pracovat s prvky grupy použít $b^{-1} \circ X$, to ale zápis dosti znepřehledňuje. Proto bez újmy na obecnosti budu definovat náhodné veličiny přímo do G. Náhodné veličiny se pak definují jako měřitelná zobrazení do $(G, 2^G)$, obdobně jako v případě přirozených čísel, kde restrikce borelovské σ-algebry na $\mathbb{N}$ vede na diskrétní σ-algebru $2^{\mathbb{N}}$.

Definice 2. *Buď $(\Omega, \mathcal{A}, P)$ pravděpodobnostní prostor a G spočetná grupa. Posloupnost nezávislých identicky rozdělených náhodných veličin $D_k : \Omega \to G$, $k \in \mathbb{N}_0$, nazveme procesem přírůstku. Definujme náhodné veličiny $X_k : \Omega \to G$, $k \in \mathbb{N}_0$, $X_0 = e$ (tedy $P(\{X_0 = e\}) = 1$) a $X_k = D_{k-1}X_{k-1}$ pro $k \in \mathbb{N}$. Proces $(X_k)_{k=0}^{\infty}$ se pak nazývá náhodnou procházkou na grupě G generovanou $P(D_k)$.*

Předně členy posloupnosti (D_k) jsou identicky rozdělené a tedy $P(D_k)$ nezávisí na k, a jelikož $\mathrm{rng}(D_k) \subset G$, indukuje $P(D_k)$ pravděpodobnost na G způsobem $p(g) = P(\{D_k = g\})$, $g \in G$ (obraz míry). Naopak tato pravděpodobnost na G zřejmě určuje rozdělení celého procesu přírůstku a tím i náhodné procházky. Tedy v poslední větě definice lze psát i ... generovanou pravděpodobností $p(g)$, $g \in G$, na G. Pro snadnější zápis zavedeme pro náhodnou veličinu V s $\mathrm{rng}(V) \subset G$, kde G je nějaká spočetná grupa označení pro indukovanou pravděpodobnost na grupě $p_V(g) = P(\{V = g\})$, $g \in G$.

Lemma 1. *Buď $(\Omega, \mathcal{A}, P)$ pravděpodobnostní prostor a G spočetná grupa. (X_k) náhodná procházka na G generovaná pravděpodobností $p(g)$,$g \in G$. Pak (X_k) je homogenní Markovův proces s diskrétním časem, množinou stavů G, iniciálním rozdělením $X_0 = e$, a pravděpodobnostmi přechodu $P(X_{k+1} = h|X_k = g) = p(hg^{-1})$, $h, g \in G$.*

Důkaz: (jde o přímočarou úpravu důkazu pro náhodnou procházku na $\mathbb{Z}$ v [4], příklad 2.2, str.21) Hned z definice je jasné, že náhodná procházka (X_k) na G je proces se spočetnou množinou stavů a $X_0 = e$. Tedy zbývá ověřit Markovovu vlastnost, tvrzení o pravděpodobnosti přechodu (homogenita z tohoto tvrzení již plyne, neboť $p(g)$, $g \in G$ nezávisí na čase k). Z definice náhodné procházky platí $X_{k+1} = D_k X_k$ pro $k \in \mathbb{N}_0$ a $X_0 = e$. Tedy k realizaci procesu přírůstku (D_k) lze jednoznačně určit realizaci procesu náhodné procházky (X_k) a naopak. Z toho platí

$$\forall k \in \mathbb{N} \quad P(X_k = x_k, X_{k-1} = x_{k-1}, \ldots, X_1 = x_1, X_0 = x_0 = e) =$$
$$= P(D_{k-1} = x_k x_{k-1}^{-1}, \ldots, D_0 = x_1) = \prod_{i=0}^{k-1} P(D_i = x_{i+1} x_i^{-1}),$$

kde bylo použito nezávislosti náhodných veličin D_i z procesu přírůstku. Fixujme $k \in \mathbb{N}_0$. Z předchozího dostáváme

$$P(X_{k+1} = x_{k+1} | X_k = x_k, \ldots, X_0 = e) = \\ = \frac{P(X_{k+1} = x_{k+1}, X_k = x_k, \ldots, X_0 = e)}{P(X_k = x_k, \ldots, X_0 = e)} = P(D_k = x_{k+1}x_k^{-1}) = p(x_{k+1}x_k^{-1}).$$

Dále opět použitím nezávislosti náhodných veličin D_i z procesu přírůstku

$$P(X_{k+1} = x_{k+1}, X_k = x_k) = \\ = \sum_{d_{k-1}d_{k-2}\ldots d_0 = x_k} P(D_k = x_k x_{k-1}^{-1}, D_{k-1} = d_{k-1}, \ldots, D_0 = d_0) = \\ = P(D_k = x_{k+1}x_k^{-1}) \sum_{d_{k-1}d_{k-2}\ldots d_0 = x_k} P(D_{k-1} = d_{k-1}, \ldots, D_0 = d_0) = \\ = P(D_k = x_{k+1}x_k^{-1}) P(X_k = x_k).$$

Tedy

$$P(X_{k+1} = x_{k+1} | X_k = x_k) = \\ = \frac{P(X_{k+1} = x_{k+1}, X_k = x_k)}{P(X_k = x_k)} = P(D_k = x_{k+1}x_k^{-1}) = p(x_{k+1}x_k^{-1}).$$

Markovova vlastnost a tvrzení o pravděpodobnostech přechodu je tím dokázáno. □

Definice 3. *(konvoluce) Buď G spočetná grupa. Označme $L^1(G) = \{f : G \to \mathbb{R}; \sum_{g\in G} |f(g)| < \infty\}$ vektorový prostor všech funkcí definovaných na G jejichž součet absolutně konverguje. Pro $f \in L^1(G)$ definujme $\|f\| := \sum_{g\in G} |f(g)| < \infty$. Dále označme $\mathcal{P}(G) = \{f : G \to \mathbb{R}^+; \sum_{g\in G} f(g) = 1\} \subset L^1(G)$ pravděpodobnosti na G (přesněji $\mathcal{P}(G)$ jsou pravděpodobnostní míry na měřitelném prostoru $(G, 2^G)$). Speciálně označme δ_g, $g \in G$ pravděpodobnosti na G, které splňují $\delta_g(g) = 1$. Pro pravděpodobnost δ_e zaveďme zkrácené označení $\delta := \delta_e$. Speciálně pro konečnou G definujeme pravděpodobnost $U \in \mathcal{P}(G)$ tzv. rovnoměrné rozdělení předpisem $U(g) = 1/|G|$ pro $g \in G$. Nechť $f, q \in L^1(G)$, konvoluce $f * q : G \to \mathbb{R}$ je definována $(f * q)(g) = \sum_{h\in G} f(gh^{-1})q(h)$, $g \in G$.*

Lemma 2. *(vlastnosti konvoluce) Buď G spočetná grupa. Konvoluce $* : L^1(G) \times L^1(G) \to L^1(G)$ je korektně definovaná binární, asociativní, bilineární operace na $L^1(G)$. $< L^1(G), +, *, 0, \delta >$ je okruh, $< \mathcal{P}(G), *, \delta >$ jeho podmonoid a zobrazení $g \mapsto \delta_g$ je vnoření G do $\mathcal{P}(G)$.*

Důkaz: Nechť $f, q \in L^1(G)$, ověříme korektnost definice

$$\sum_{g\in G} |(f * q)(g)| = \sum_{g\in G} |\sum_{h\in G} f(gh^{-1})q(h)| \le \sum_{g\in G}\sum_{h\in G} |f(gh^{-1})||q(h)| = \\ = \sum_{h\in G}(\sum_{g\in G} |f(gh^{-1})|)|q(h)| = \sum_{h\in G} \|f\| \, |q(h)| = \|f\| \, \|g\| \le \infty.$$

Podobně se ověří, že konvoluce je rovněž binární operace na $\mathcal{P}(G)$, buďte $P, Q \in \mathcal{P}(G)$, pak $\sum_{g\in G}(P*Q)(g) = \sum_{h\in G}(\sum_{g\in G} P(gh^{-1}))Q(h) = \sum_{h\in G} 1Q(h) = 1$. Bilinearita (distributivita) je triviální. Ověříme asociativitu

$$\begin{aligned}[A*(B*C)](g) &= \sum_{x\in G} A(gx^{-1})(\sum_{z\in G} B(xz^{-1})C(z)) = \\ &= \sum_{z\in G}\sum_{x\in G} A(gx^{-1})B(xz^{-1})C(z) = \sum_{z\in G}\sum_{w\in G} A(gz^{-1}w^{-1})B(w)C(z) = \\ &= \sum_{z\in G}(\sum_{w\in G} A(gz^{-1}w^{-1})B(w))C(z) = [(A*B)*C](g).\end{aligned}$$

V prvém kroku jsem prohodil sumy, to lze např. ze zobecněného komutativního a asociativního zákona pro řady (uvažujeme zobecněnou řadu $\sum_{x,z\in G} A(gx^{-1})B(xz^{-1}C(z)))$ a pak jsem provedl substituci $x = wz$. Dokážeme tvrzení o vnoření, označme ho $\alpha : G \to \mathcal{P}(G)$, kde $\alpha(g) = \delta_g$, $g \in G$. Všimneme si, že z definice pro každé $g \in G$ platí $\delta_g(h) = 1$ pro $h = g$ a $\delta_g(h) = 0$ jinak. Ověříme, že α je prostý monoidový homomorfizmus. Jelikož G i $\mathcal{P}(G)$ jsou monoidy, stačí ověřit, že α je prosté (to je zřejmé), zobrazuje jednotkový prvek na jednotkový prvek (rovněž zřejmé) a pro libovolné $t \in G$ platí $(\alpha(g)\alpha(h))(t) = (\delta_g * \delta_h)(t) = \sum_{s\in G} \delta_g(ts^{-1})\delta_h(s) = \delta_{gh}(t) = (\alpha(gh))(t)$. Obraz při zobrazení α je tedy podmonoid. Abychom ukázali, že se jedná o grupu zbývá ověřit uzavřenost na inverzi, k tomu stačí ukázat, že $\alpha(g^{-1})$ je inverzní k $\alpha(g)$. Pro každé $g \in G$ platí $(\alpha(g^{-1}) * \alpha(g))(t) = \sum_{s\in G} \delta_{g^{-1}}(ts^{-1})\delta_g(s) = \sum_{s\in G} \delta_{g^{-1}}(ts^{-1})\delta_g(s) = \delta_e(t) = \delta(t)$. Obdobně se ukáže $\alpha(g) * \alpha(g^{-1}) = \delta$. Tedy α je prostý grupový homomorfizmus. □

Lemma 3. *Nechť G je spočetná grupa, $(\Omega, \mathcal{A}, P)$ pravděpodobnostní prostor.*

I. Buďte $X : \Omega \to G$, $Y : \Omega \to G$ nezávislé náhodné veličiny, definujme náhodnou veličinu $Z = XY$ (vzhledem k diskrétní σ-algebře na G se měřitelnost ověří triviálně). Pak platí $p_Z = p_X * p_Y$.

II. Buď $\varphi : G \to G'$ homomorfizmus do spočetné grupy G' definujme lineární zobrazení $\bar\varphi : L^1(G) \to L^1(G')$ předpisem $[\bar\varphi(f)](g') = \sum_{g\in\varphi^{-1}(\{g'\})} f(g)$, kde $\varphi^{-1}(\{M'\}) := \{g \in G; \varphi(g) \in M'\}$ pro libovolnou $M' \subset G'$ značí úplný vzor. Dále buď $V : \Omega \to G$ náhodná veličina, označme $V' = \varphi(V)$[2], pak platí $p_{V'} = \bar\varphi(p_V)$.

Důkaz: I. Pro každé $g \in G$ platí

$$\begin{aligned}p_z(g) = P(\{Z = g\}) &= P(\cup_{h\in G}\{X = gh^{-1}, Y = h\}) = \\ &= \sum_{h\in G} P(\{X = gh^{-1}, Y = h\}) = \sum_{h\in G} P(\{X = gh^{-1}\})P(\{Y = h\}) = \\ &= \sum_{h\in G} p_X(gh^{-1})p_Y(h) = p_X * p_Y(g).\end{aligned}$$

[2]Význam $\varphi(V)$ definuji $\varphi(V) := \varphi \circ V$. Toto značení jsem zavedl, protože značení s $\circ$ působí někdy dosti nepřehledně. Například pro grupu G a dvě náhodné veličiny X, Y s oborem hodnot v G a grupový homomorfizmus ψ s definičním oborem v G, platí $\psi \circ (XY) = (\psi \circ X)(\psi \circ Y)$. To samé v právě zavedeném značení vypadá $\psi(XY) = \psi(X)\psi(Y)$.

II. Buď V, V' jako výše pro indukovaná rozdělení na G, G' platí

$$p_{V'}(g') = P(V' = g') = P(\varphi(V) = g') = P(\{V = g; \varphi(g) = g'\}) = \\ = \sum_{g \in G, \varphi(g) = g'} P(V = g) = \sum_{g \in G, \varphi(g) = g'} p_V(g) = [\bar{\varphi}(p_V)](g').$$

□

Lemma 4. *Nechť G je spočetná grupa, $(\Omega, \mathcal{A}, P)$ pravděpodobnostní prostor a (X_k) náhodná procházka na G generovaná pravděpodobností p na G. Pak platí:*

I. Pro každé $g \in G$ platí $P(X_k = g) = p^{*k}(g)$, kde $p^{*k}(g) := (p * p^{*(k-1)})(g)$ pro $k > 0$ a $p^{*0}(g) := \delta$.

II. Buď G' spočetná grupa a $\varphi : G \to G'$ homomorfizmus. Definujme lineární zobrazení $\bar{\varphi} : L^1(G) \to L^1(G')$ předpisem $[\bar{\varphi}(f)](g') = \sum_{g \in \varphi^{-1}(\{g'\})} f(g)$. Pro $k \in \mathbb{N}_0$ definujme náhodné veličiny $Y_k = \varphi(X_k)$, $C_k = \varphi(D_k)$ (G' i G uvažuji jako měřitelné prostory vybavené diskrétní σ-algebrou a tedy jakékoli zobrazení z G do G' je měřitelné a definice je tudíž korektní). Pak (Y_k) je náhodná procházka na G' generovaná pravděpodobností $q = \bar{\varphi}(p)$ a pro $k \in \mathbb{N}_0$ platí $Y_{k+1} = C_k Y_k$, $p_{C_k} = q$, $q^{*k} = p_{Y_k} = \bar{\varphi}(p_{X_k}) = \bar{\varphi}(p^{*k})$.

Důkaz: I. Budeme postupovat indukcí podle k. Předně z definice náhodné procházky $P(X_0) = \delta$. Nechť tvrzení platí pro $k \in \mathbb{N}_0$, ukážeme, že platí pro $k+1$ (použijeme indukční předpoklad a lemma 1)

$$P(X_{k+1} = g) = \sum_{h \in G} P(X_{k+1} = g, X_k = h) = \\ = \sum_{h \in G} P(X_{k+1} = g | X_k = h) P(X_k = h) = \sum_{h \in G} p(gh^{-1}) p^{*k}(h) = p^{*(k+1)}(g).$$

Jiný důkaz (rovněž indukcí) dává předchozí lemma a rozepsání X_{k+1} pomocí procesu přírůstku. II. Použijeme, že $\mathrm{rng}(D_k), \mathrm{rng}(X_k) \subset G$ a že φ je homomorfizmus grup

$$Y_{k+1} = \varphi(X_{k+1}) = \varphi(D_k X_k) = \varphi(D_k)\varphi(X_k) = C_k Y_k, Y_0 = \varphi(X_0) = \varphi(e) = e.$$

Použitím předchozího lemmatu 3 II dostáváme

$$p_{C_k} = \bar{\varphi}(p_{D_k}) = \bar{\varphi}(p)$$

Tedy C_k jsou identicky rozložené, jejich nezávislost plyne z nezávislosti D_k a $C_k = \varphi(D_k)$. Jde tedy o náhodnou procházku na G' generovanou $q := \bar{\varphi}(p)$. Dále dostáváme

$$p_{C_k} = \bar{\varphi}(p) = q, p_{Y_k} = q^{*k}, q^{*k} = p_{Y_k} = \bar{\varphi}(p_{X_k}) = \bar{\varphi}(p^{*k}).$$

□

1.2 Konečně dimenzionální lineární reprezentace konečných grup na $\mathbb{C}$

Dále uvedená definice je souhrn definic z [1] kapitola 2 případně z [2] kapitola 1.

Definice 4. *I. Buď V vektorový prostor nad tělesem komplexních čísel $\mathbb{C}$. Lineární* ***reprezentace*** *grupy G na vektorovém prostoru V je homomorfizmus $\rho : G \to \mathrm{GL}(V)$, kde $\mathrm{GL}(V)$ označuje grupu automorfizmů V. Reprezentace ρ je tedy akcí grupy G na V. Dimenze reprezentace je definována jako $\dim V$. Místo lineární reprezentace budu psát stručněji reprezentace.*

II. Buď $\rho : G \to \mathrm{GL}(V)$ reprezentace. Nechť dále V' je vektorový podprostor V invariantní (stabilní) vzhledem k akci ρ, pak $\rho' : G \to \mathrm{GL}(V')$ definované $\rho'(g) = \rho(g)|V'$, $g \in G$ je ***podreprezentace*** *reprezentace ρ. ρ' je* ***vlastní podreprezentace*** *ρ právě tehdy, když V' je vlastní podprostor V ($V' \neq V$, $V' \neq 0$). Reprezentace je* ***ireducibilní*** *pokud nemá žádné vlastní podreprezentace.*

III. Reprezentace $\rho_1 : G \to \mathrm{GL}(V_1)$, $\rho_2 : G \to \mathrm{GL}(V_2)$, jsou ***izomorfní*** *(ekvivalentní) právě tehdy, když existuje izomorfizmus $\phi : V_1 \to V_2$ takový, že pro každé $g \in G$ platí $\rho_1 = \phi^{-1}\rho_2\phi$.*

IV. ***Direktní součet reprezentací*** *$\rho_1 : G \to \mathrm{GL}(V_1)$ $\rho_2 : G \to \mathrm{GL}(V_2)$ je reprezentace $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}(V_1 \oplus V_2)$, definovaná $\rho_1 \oplus \rho_2(g)(v_1, v_2) = (\rho_1(g)(v_1), \rho_2(g)(v_2))$, $(v_1, v_2) \in V_1 \oplus V_2$.*

V. Buď Ω, $|\Omega| = N \in \mathbb{N}$ konečná množina $\alpha : G \to S(\Omega)$ akce grupy G na Ω ($S(\Omega)$ označuje grupu permutací na Ω). Vezměme $V = \mathbb{C}^N$ vektorový prostor aritmetických vektorů. Ztotožněme prvky Ω bijekcí $e : \Omega \to \{e_1, \ldots, e_N\}$ s prvky standardní báze V. Definujme zobrazení $\rho : G \to \mathrm{GL}(V)$ pro každé $g \in G$, $\omega \in \Omega$ předpisem $\rho(g)(e(\omega)) = e(\alpha(g)(\omega))$ ($\rho(g)$ je takto definováno na bázi a jednoznačně se rozšíří na homomorfizmus), pak ρ je reprezentace G. Reprezentace tohoto typu se nazývají ***permutační reprezentace****.*

VI. ***Regulární reprezentace*** *konečné grupy G je permutační reprezentace pro $\Omega = G$ a akci levými translacemi.*

VII. Reprezentace $\rho : G \to \mathrm{GL}(V)$ je ***triviální*** *pokud každému prvku grupy G přiřazuje identitu id_V (má triviální obraz).*

Lemma 5. *([1], kap.2B, Theorem 1, str.8) Buď G konečná grupa, V vektorový prostor, $\rho : G \to \mathrm{GL}(V)$ reprezentace. Buď $(.,.)$ skalární součin invariantní vůči akci ρ a $\rho_1 : G \to \mathrm{GL}(W)$ podreprezentace ρ, pak $\rho_2 : G \to \mathrm{GL}(W^\perp)$, kde $W^\perp$ je ortogonální doplněk W ve V vzhledem k $(.,.)$, je rovněž podreprezentace ρ. Platí tedy $\rho = \rho_1 \oplus \rho_2$.*

Jestliže existuje na V skalární součin $< ., . >$ (např. pro konečnou dimenzi lze vzít vždy standardní) lze položit $(u, v) := \sum_{g \in G} < \rho(g)(u), \rho(g)(v) >$, $(.,.)$ ($(.,.)$je pak invariantní). Dále u permutačních reprezentací je přímo standardní skalární součin invariantní.

Lemma 6. *([2], Theorem 2, str.7 a [2], Corollary 1, str.16) Buď G konečná grupa, V konečně dimenzionální vektorový prostor a $\rho : G \to \mathrm{GL}(V)$ reprezentace. Pak*

existují reprezentace $\rho_1, \rho_2, \ldots, \rho_N$, $N \in \mathbb{N}$ ireducibilní reprezentace grupy G tak, že

$$\rho = \rho_1 \oplus \rho_2 \oplus \ldots \oplus \rho_N,$$

kde rozklad je určen jednoznačně až na pořadí a izomorfizmus členů.

1.3 Charakter reprezentace a skalární součin charakterů na konečné grupě

Následující definice je opět souhrn definic z [1] kapitola 2 případně z [2] kapitola 2.

Definice 5. *I.* ***Maticová reprezentace*** *ρ_M grupy G dimenze $n \in \mathbb{N}$ je homomorfizmus $\rho_M : G \to \mathrm{GL}_n(\mathbb{C})$, kde $\mathrm{GL}_n(\mathbb{C})$ je grupa invertibilních matic o rozměru $n \times n$ nad tělesem $\mathbb{C}$.* ***Maticová reprezentace je unitární*** *pokud jsou matice z obrazu ρ_M unitární.* ***Charakter maticové reprezentace*** *$\chi_{\rho_M} : G \to \mathbb{C}$ definujeme $\chi_{\rho_M}(g) = \mathrm{tr}\rho_M(g)$.*

II. Každé reprezentaci $\rho : G \to \mathrm{GL}(\mathbb{C}^n)$ dokážeme přiřadit ***příslušnou maticovou reprezentaci*** *$\rho_M : G \to \mathrm{GL}_n(\mathbb{C})$ složením ρ a izomorfizmu, který lineárnímu zobrazení na $\mathbb{C}^n$ přiřadí jeho matici ve standardní bázi. Toto přiřazení je bijekce. Je-li ρ_M příslušná ρ, nazveme rovněž ρ příslušnou k ρ_M. Pomocí příslušné reprezentace můžeme pojmy zavedené pro reprezentace rozšířit i na maticové reprezentace a naopak. Například řekneme, že maticová reprezentace ρ_M je izomorfní s reprezentací ρ jestliže příslušná reprezentace k ρ_M je izomorfní s ρ.* ***Charakter reprezentace*** *definujeme jako charakter nějaké izomorfní maticové reprezentace.*

III. Buď G konečná grupa pro $\alpha, \beta : G \to \mathbb{C}$ definujeme skalární součin

$$(f|g) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)},$$

kde $\overline{z}$ pro $z \in \mathbb{C}$ značí komplexně sdružené číslo k z.

Poznámka 1. Charakter reprezentace $\rho : G \to \mathrm{GL}(V)$ je korektně definován, protože izomorfní maticová reprezentace existuje. Lze ji vytvořit tak, že fixujeme nějakou bázi V a automorfizmy z $\mathrm{GL}(V)$ ztotožníme s jejich maticemi ve fixované bázi. Jednoznačnost pak plyne z cykličnosti stopy. Z té také plyne, že izomorfní reprezentace mají stejný charakter. Obecněji cykličnost stopy umožňuje pojem stopy zobecnit na lineární zobrazení na nějakém konečně dimenzionálním vektorovém prostoru. Spousta důležitých pojmů je definována případně určena pomocí stopy matice (charakter, inverze Fourierovy transformace), proto se pro zavedení těchto pojmů používá maticových reprezentací. Ale není to nutné, zobecníme-li stopu naznačeným způsobem na lineární zobrazení. Proto se dále v definicích neomezuji na maticové reprezentace. Při řešení úloh naopak preferuji maticové reprezentace (například výpočet charakteru).

Buď $\rho_M : G \to \mathrm{GL}_n(\mathbb{C})$ maticová reprezentace, ta je vždy konečně dimenzionální a tedy vždy (jak již bylo zmíněno) existuje na $\mathbb{C}^n$ skalární součin $(.,.)$ invariantní

vůči akci ρ_M. V $\mathbb{C}^n$ zvolíme takovou bázi, ve které má bilineární forma příslušná $(.,.)$ jednotkovou matici. Přechodem k této bázi (složením ρ_M s příslušným automorfizmem GL_n) získáme unitární maticovou reprezentaci, která je izomorfní s původní reprezentací.

Ještě uvedu nějaké příklady unitárních reprezentací. Pro libovolnou permutační reprezentaci (homomorfizmus do $\mathrm{GL}(\mathbb{C}^n)$) je příslušná maticová reprezentace $\rho_M : G \to \mathrm{GL}_n(\mathbb{C})$ unitární (obraz ρ_M obsahuje pouze permutační matice). Reprezentace cyklické grupy, které napočítáme dále v lemmatu 9 budou rovněž unitární.

Nyní shrnu některé výsledky o skalárních součinech charakterů, čerpal jsem z [1], [2], [3].

Lemma 7. *Buď G konečná grupa. Všechny reprezentace se předpokládají konečně dimenzionální.*

I. ([2], Theorem 4, str.16) Nechť ρ je reprezentace grupy G s charakterem χ_ρ, buď $\rho = \rho_1 \oplus \rho_2 \oplus \ldots \oplus \rho_N, N \in \mathbb{N}$ její ireducibilní rozklad. Buď μ ireducibilní reprezentace grupy G s charakterem χ_μ, pak je počet ρ_n izomorfních s μ je roven $(\chi_\rho|\chi_\mu)$

II. ([2], Corollary 2 of Theorem 4, str.16) Dvě reprezentace grupy G se stejným charakterem jsou izomorfní.

III. ([2], Theorem 5, str.17) χ_ρ je charakter ireducibilní reprezentace ρ grupy G, právě tehdy, když $(\chi_\rho|\chi_\rho) = 1$

IV. ([1], kap.2C, Proposition 5, str.12) Označme ρ regulární reprezentaci grupy G. (a) Buď $g \in G$. Pro charakter regulární reprezentace platí $\chi_\rho(g) = |G|$ pro $g = e$, $\chi_\rho(g) = 0$ jinak. (b) Každá ireducibilní reprezentace je v regulární reprezentaci zahrnuta s násobností rovnou její dimenzi, což dává $\chi_\rho(g) = \sum_{\mu \text{ ired. rep. } G} d_\mu \chi_\mu(g)$ pro $g \in G$, dále $(\chi_\rho|\chi_\rho) = |G| = \sum_{\mu \text{ ired. rep. } G} d_\mu^2$, kde d_μ je dimenze ireducibilní reprezentace μ.

1.4 Fourierova transformace na konečných grupách

Definice 6. *([1], uvedeno na, str.7) Buď G konečná grupa, $f : G \to \mathbb{C}$ funkce a ρ reprezentace grupy G. Fourierova transformace $\hat{f}$ funkce f v reprezentaci ρ je definována $\hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g)$*

Lemma 8. *Buď G konečná grupa.*

I. ([1], kap.2B, exercise 1, str.7) Buďte $f, g : G \to \mathbb{C}$ funkce a ρ reprezentace grupy G, pak platí $\widehat{f * g} = \hat{f}\hat{g}$.

II. (Věta o inverzní Fourierově transformaci, [1], kap.2C, str.13) Buď $f : G \to \mathbb{C}$ funkce a ρ_n, $n = 1, \ldots, N$, $N \in \mathbb{N}$ všechny (neizomorfní) ireducibilní reprezentace G. Označme d_n dimenzi reprezentace ρ_n, $n = 1, \ldots, N$, pak pro každé $s \in G$ platí

$$f(s) = \frac{1}{|G|} \sum_{n=1}^{N} d_n \mathrm{tr}(\rho_n(s^{-1})\hat{f}(\rho_n)).$$

III. (Plancherelova formule, [1], kap.2C, str.13) Buď $f, g : G \to \mathbb{C}$ funkce a ρ_n, $n = 1, \ldots, N$, $N \in \mathbb{N}$ všechny (neizomorfní) ireducibilní reprezentace G. Označme d_n dimenzi reprezentace ρ_n, $n = 1, \ldots, N$, pak pro každé $s \in G$ platí

$$\sum_{s\in G} f(s^{-1})g(s) = \frac{1}{|G|}\sum_{n=1}^{N} d_n \mathrm{tr}(\hat{f}(\rho_n)\hat{g}(\rho_n)).$$

Speciálně pro f, g reálné funkce a ρ_n, $n = 1, \ldots, N$ navíc maticové unitární platí

$$\sum_{s\in G} f(s)g(s) = \frac{1}{|G|}\sum_{n=1}^{N} d_n \mathrm{tr}(\hat{g}(\rho_n)\hat{f}^H(\rho_n)),$$

kde A^H značí hermitovskou transpozici komplexní matice A.

IV. ([1], kap.2B, exercise 7, str.15) Konvoluce dvou třídových funkcí na G (třídová funkce je konstantní na třídách konjugace) je opět třídová funkce.

V. ([1], kap.2B, Theorem 7, str.15) Počet ireducibilních reprezentací je roven počtu tříd konjugace.

VI. Buď G konečná grupa, pro Fourierův obraz rovnoměrného rozdělení platí $\hat{U}(\rho) = \mathrm{id}$ pro ρ triviální, $\hat{U}(\rho) = 0$ pro ρ ireducibilní netriviální,

Důkaz: (pro cvičení nejsou v [1] důkazy uvedeny, proto je uvádím zde)

I. Buď ρ libovolná reprezentace grupy G, pak platí

$$\widehat{f * g}(\rho) = \sum_{t\in G}(f * g)(t)\rho(t) = \sum_{t\in G}\sum_{s\in G} f(ts^{-1})g(s)\rho(t) =$$
$$= \sum_{t\in G}\sum_{s\in G} f(ts^{-1})g(s)\rho(ts^{-1})\rho(s) = \sum_{s\in G} g(s)(\sum_{t\in G} f(ts^{-1})\rho(ts^{-1}))\rho(s) =$$
$$= \sum_{s\in G} g(s)\hat{f}(\rho)\rho(s) = \hat{f}(\rho)\hat{g}(\rho).$$

II. Důkaz věty o inverzní Fourierově transformaci je převzat z [1] a uvádím ho pouze pro úplnost a také proto, že je velmi krátký. Obě stany jsou lineární v f, rovnost tedy stačí ověřit na bázových prvcích δ_t, $t \in G$. Položme tedy $f = \delta_t$, pak $\hat{f}(\rho_n) = \rho_n(t)$ a pravá stana má tvar

$$\frac{1}{|G|}\sum_{n=1}^{N} d_n \mathrm{tr}(\rho_n(s^{-1}t)) = \frac{1}{|G|}\chi_\rho(s^{-1}t) = \delta_t(s),$$

kde ρ označuje regulární reprezentaci G. Bylo použito vlastností charakteru regulární reprezentace z lemmatu 7 IV. U Plancherelovy formule se postupuje obdobně, obě strany rovnosti jsou lineární v f, stačí tedy ověřovat pouze pro $f = \delta_t$. Dosazením za f do rovnosti získáme vztah pro inverzní Fourierovu transformaci, který byl již dokázán.

IV. Buďte f, g třídové funkce na grupě G, pro každé $a, b \in G$ platí

$$(f * g)(aba^{-1}) = \sum_{s\in G} f(aba^{-1}s^{-1})g(s) =$$
$$= \sum_{s\in G} f(ba^{-1}s^{-1}a)g(a^{-1}sa) = \sum_{s\in G} f(b(a^{-1}sa)^{-1})g(a^{-1}sa) = (f * g)(b).$$

VI. Buď nejprve ρ triviální, dostáváme $\hat{U}(\rho) = \sum_{g\in G} U(g)\rho(g) = \sum_{g\in G} \mathrm{id}/|G| = \mathrm{id}$.

Dále buď ρ netriviální ireducibilní reprezentace, vezměme ρ_M nějakou izomorfní maticovou unitární reprezentaci. Použijeme verzi Plancherelovy formule pro reálné funkce $f = g = U$ a unitární reprezentace

$$\frac{1}{|G|} = \sum_{s\in G} U^2(s) = \frac{1}{|G|}\sum_{n=1}^{N} d_n \mathrm{tr}(\hat{U}(\rho_n)\hat{U}^H(\rho_n)) = \frac{1}{|G|} + \frac{1}{|G|} d_\rho \sum_{\rho}^{*} \mathrm{tr}(\hat{U}(\rho)\hat{U}^H(\rho)).$$

Suma $\sum_\rho^*$ jde přes všechny (až na izomorfizmus) netriviální ireducibilní unitární reprezentace grupy G, dostáváme

$$0 = \sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{U}(\rho)\hat{U}^H(\rho)).$$

Z tvaru matice $\hat{U}(\rho)\hat{U}^H(\rho)$ je vidět, že je hermitovská a positivně semidefinitní, má tedy nezáporná vlastní čísla $\lambda_{\rho,1}, \ldots, \lambda_{\rho,N_\rho}$ a platí

$$\mathrm{tr}(\hat{U}(\rho)\hat{U}^H(\rho)) = \lambda_{\rho,1} + \ldots + \lambda_{\rho,N_\rho} \geq 0.$$

Členy v součtu $0 = \sum_\rho^* \ldots$ jsou nezáporné a tedy nutně všechny nulové. Všechna vlastní čísla musí být pak rovněž nulová a matice $\hat{U}(\rho)\hat{U}^H(\rho) = 0$. Z toho pak rovněž $\hat{U}(\rho) = 0$ ($\hat{U}(\rho)\hat{U}^H(\rho)$ si lze představit jako matici kvadratické formy, která by pro nenulové $\hat{U}(\rho)$ byla netriviální). Dostáváme $\hat{U}(\rho) = 0$ pro libovolnou netriviální ireducibilní unitární maticovou reprezentaci ρ. Konečně buď ρ' libovolná netriviální ireducibilní reprezentace, pak je ale izomorfní nějaké netriviální ireducibilní unitární maticové reprezentaci ρ a $\hat{U}(\rho') = 0$ je tedy rovněž nulová (rozepíšeme $\hat{U}(\rho')$ pomocí definice Fourierovy transformace, dále pomocí reprezentace příslušné k ρ). □

1.5 Ireducibilní reprezentace konečné cyklické grupy

Lemma 9. *Konečná cyklická grupa $\mathbb{Z}_n$ má právě n neizomorfních ireducibilních reprezentací, příslušné maticové reprezentace jsou tvaru $\rho_m : \mathbb{Z}_n \to \mathbb{C}$, $\rho_m(l) = \mathrm{e}^{\jmath\frac{2\pi}{n}ml}$, $m = 0, \ldots, n-1$. Uvedené maticové reprezentace jsou zřejmě unitární a jednodimenzionální.*

Poznamenejme, že diskrétní Fourierova transformace používaná v číslicovém zpracování signálů (téměř každý signálový procesor zahrnuje nějaké prostředky usnadňující implementaci této transformace počínaje adresními módy až po koprocesory) je totožná s Fourierovou transformací na uvedených reprezentacích.

Důkaz: Buď $m \in \{0, \ldots, n-1\}$ libovolné. Ověříme, že ρ_m je homomorfizmus

$$\rho_m(k \oplus l) = \rho_m(k + l + cn) = \mathrm{e}^{\jmath \frac{2\pi}{n} m(k+l+cn)} = \mathrm{e}^{\jmath \frac{2\pi}{n} mk} \mathrm{e}^{\jmath \frac{2\pi}{n} ml} = \rho_m(k)\rho_m(l).$$

Grupovou operaci na $\mathbb{Z}_n$ jsem označil $\oplus$ a v druhém kroku ji namodeloval $+$ na $\mathbb{C}$, $c \in \{0, -1\}$. Jelikož izomorfní reprezentace mají stejné charaktery, stačí ukázat, že se charaktery liší. Vezmeme charaktery pro $l = 1$, reprezentací k $m, m' \in \{0, \ldots, n-1\}, m \neq m'$ dostáváme

$$\frac{\chi_{\rho_m}(1)}{\chi_{\rho'_m}(1)} = \frac{\mathrm{e}^{\jmath \frac{2\pi}{n} m}}{\mathrm{e}^{\jmath \frac{2\pi}{n} m'}} = \mathrm{e}^{\jmath \frac{2\pi}{n}(m-m')} \neq 1,$$

protože $0 < |m - m'| < n$. Charaktery se liší, máme tedy n neizomorfních ireducibilních (ρ_m jsou jednodimenzionální) reprezentací. Další neizomorfní ireducibilní reprezentace již neexistuje, jinak bychom dostali spor s $|\mathbb{Z}_n| = \sum_{\rho \text{ ired. rep. } \mathbb{Z}_n} d_\rho^2 = n$. (viz. lemma 7 IV(b)).

□

Kapitola 2

Řešená cvičení

Řešení je vždy provedeno formou důkazu, někdy je ale původní zadání poněkud nejednoznačné nebo nepřesné, nebo se mi nepodařilo dokázat vše, proto je občas připojena poznámka, která vysvětluje, co přesně dokazuji nebo je rovnou formulováno lemma.

Cvičení 1. ([1], exercise 1, str.20) (I.) Nechť p je pravděpodobnost na symetrické grupě S_n. Náhodnou procházku generovanou p si představujte jako výsledek opakovaného míchání balíčku n karet. Pro permutaci π, nechť $L(\pi) = \pi(1)$. Hodnoty L udávají pozici 1. karty počátečního pořadí ve výsledku. Ukažte, že náhodná procházka indukuje Markovův řetězec pro L. Ukažte, že matice přechodu tohoto řetězce je dvojnásobně stochastická. (II.) Naopak ukažte, že pro každou dvojnásobně stochastickou matici existuje pravděpodobnost p na S_n, která se hodí k dané matici pro L.

Poznámka 2. Co se týče druhé části, podařilo se mi ukázat pouze existenci funkce p, která se hodí k dané dvojnásobně stochastické matici. Nepodařilo se mi zatím ukázat, že existuje i nezáporné řešení (pravděpodobnost).

Důkaz: (Řešení cvičení 1, část II je vyřešena pouze částečně) I. Náhodnou procházku na S_n generovanou p označím (X_k) a odpovídající proces přírůstku (D_k). (L_k) označím proces $L(X_k)$ (náhodná veličina $L(X_k)$ zobrazuje do $\{1, \dots, n\}$ a $l_0 = 1$), ukážu, že (L_k) má Markovovu vlastnost. Označme $G_{ij} := \{\pi \in S_n; j = \pi(i)\}$. Pro každé $k \in \mathbb{N}$ platí (opět použijeme nezávislost procesu přírůstku)

$$P(L_k = l_k, L_{k-1} = l_{k-1}, \dots, L_0 = l_0) =$$
$$= P(D_{k-1} \in G_{l_{k-1},l_k}, \dots, D_0 \in G_{l_0,l_1}) = \prod_{i=0}^{k-1} P(D_i \in G_{l_i,l_{i+1}}),$$

což ihned dává (pro $k \in \mathbb{N}_0$)

$$P(L_{k+1} = l_k | L_k = l_k, \dots, L_0 = l_0) =$$
$$= \frac{P(L_{k+1} = l_{k+1}, L_k = l_k, \dots, L_0 = l_0)}{P(L_k = l_k, \dots, L_0 = l_0)} = P(D_k \in G_{l_k,l_{k+1}}) = p(G_{l_k,l_{k+1}}).$$

Dále platí (pro $k \in \mathbb{N}_0$)

$$P(L_{k+1} = l_k | L_k = l_k) = P(D_k \in G_{l_k, l_{k+1}}).$$

Tím je dokázána Markovova vlastnost a homogenita pro (L_k). Zbývá ukázat, že matice přechodu pro (L_k) je dvojnásobně stochastická (součet pravděpodobností v libovolném řádku je 1 a totéž platí pro sloupce). Jelikož $p(S_n) = 1$ (p je pravděpodobnost na S_n), stačí ukázat, že $\{G_{i,j}; j = 1, \ldots, n\}$ a $\{G_{i,j}; i = 1, \ldots, n\}$ jsou rozklady S_n, to je ale hned vidět z definice množin $G_{i,j}$. Zvolme libovolnou permutaci $\pi \in S_n$, zřejmě $\pi \in G_{i,\pi(i)}$ a rovněž $\pi \in G_{\pi^{-1}(j),j}$, tedy oba soubory množin jsou pokrytí. Disjunktnost množin v prvém resp. druhém souboru plyne z toho, že permutace jsou zobrazení resp. prostá zobrazení.

II. Označme $M = [m_{ij}]$ danou dvojnásobně stochastickou matici

$$\forall i \in \{1, \ldots, n\} \ \sum_{j=1}^{n} m_{ij} = 1, \quad \forall j \in \{1, \ldots, n\} \ \sum_{i=1}^{n} m_{ij} = 1. \tag{2.1}$$

Za předpokladu, že požadované p existuje musí z I. platit

$$p(G_{i,j}) = m_{ij} \text{ pro } i, j \in \{1, \ldots, n\}, \quad p(S_n) = 1, \quad p(g) \geq 0, \text{ pro } g \in S_n.$$

Zde se budu zabývat pouze řešitelností soustavy bez nerovností $p(g) \geq 0$, $g \in S_n$. Existenci nezáporného řešení se mi zatím nepodařilo stanovit. Jedná se o soustavu $n^2 + 1$ rovnic pro $n!$ neznámých $p(g)$, $g \in S_n$. Ale díky omezením (2.1) na m_{ij}, zjistíme, že pro každý řádkový index i je rovnice k indexu (i, n) ekvivalentní lineární kombinací rovnic k indexům (i, j), $j < n$

$$\sum_{j=1}^{n} p(G_{i,j}) = \sum_{j=1}^{n} m_{ij} = 1, \quad p(G_{i,n}) = 1 - \sum_{j=1}^{n-1} p(G_{i,j}) = 1 - \sum_{j=1}^{n-1} m_{ij} = m_{in}$$

můžeme ji tedy vynechat. Podobně plyne, že lze vynechat i rovnosti k indexům (n, j), $j < n$. Zbývá tedy $(n-1)^2$ rovnic k indexům $i, j \in \{1, \ldots, n-1\}$ a rovnice $p(S_n) = 1$. Ukážeme, že matice soustavy má plnou řádkovou hodnost $((n-1)^2 + 1)$ a má tedy podle Frobeniovy věty řešení. Sloupcový vektor $\mathbf{a}_g$ matice soustavy k neznámé $p(g)$, $g \in G$ má tvar

$$\mathbf{a}_g^T = [a_{g,(1,1)}, \ldots, a_{g,(i,j)}, \ldots, a_{g,(n-1,n-1)}, a_g],$$

kde $a_{g,(i,j)} = \chi_{G_{i,j}}(g)$ pro $i, j \in \{1, \ldots, n-1\}$ a $a_g = \chi_G(g) = 1$. χ_A jsem označil charakteristickou funkci množiny A. Stačí ukázat, že lineární obal sloupců matice soustavy, označme ho V, obsahuje $(n-1)^2 + 1$ nezávislých vektorů. Není potřeba uvažovat všechny sloupce, stačí vzít vektory k transpozicím (u, n) pro $u < n$, identitu id a vektory k trojcyklům (u, v, n), $u, v < n$, $u \neq v$. Označme $\mathbf{e}_{(i,j)}$ vektor, který má jednotku pouze na indexu (i, j) a ostatní složky nulové. Protože $\mathbf{e}_{(u,u)} = \mathbf{a}_{\mathrm{id}} - \mathbf{a}_{(u,n)}$ pro $u < n$, platí $\mathbf{e}_{(u,u)} \in V$, pro $u < n$. Dále pro $u, v < n$, $u \neq v$ platí $\mathbf{e}_{(u,v)} \in \left\langle \{\mathbf{a}_{(u,v,n)}, \mathbf{a}_{\mathrm{id}}, \mathbf{e}_{(t,t)} (\text{pro } t < n)\} \right\rangle$ ($\langle A \rangle$ značí lineární obal množiny A), tedy $\mathbf{e}_{(u,v)} \in V$ pro $u, v < n$. Dále $\mathbf{a}_{\mathrm{id}} \notin \left\langle \{\mathbf{e}_{(u,v)}; u, v < n\} \right\rangle$, neboť $a_{\mathrm{id}} = 1$. Tedy $\{\mathbf{e}_{(u,v)}; u, v < n\} \cup \{\mathbf{a}_{\mathrm{id}}\}$ je hledaná $(n-1)^2+1$ prvková lineárně nezávislá podmnožina V. Soustava má řešení a p hledaných vlastností existuje. □

2.1 Variační vzdálenost

Definice 7. *Nechť G je konečná grupa. $p, q \in \mathcal{P}(G)$ pravděpodobnosti na G. Variační vzdálenost mezi p a q je definována*

$$\|p - q\| = \max_{A \subset G} |p(A) - q(A)|.$$

Cvičení 2. ([1], kap.3B, exercise 2, str.21) Dokažte

$$\|p - q\| = \frac{1}{2} \sum_{s \in G} |p(s) - q(s)| = \frac{1}{2} \max_{\|f\| \leq 1} |p(f) - q(f)|,$$

kde v posledním výrazu $f : G \to \mathbb{R}$ s $|f(s)| \leq 1$ a $p(f) := \sum_{s \in G} p(s) f(s) = \mathrm{E}_p[f]$. Také dokažte platnost následující interpretace (Paul Switzer): Při jednom pozorování, pocházejícího z p nebo q se stejnou pravděpodobností $1/2$ máte rozhodnout z kterého z rozdělení p, q pozorování pochází. Pravděpodobnost úspěchu je $\frac{1}{2} + \frac{1}{2} \|p - q\|$.

Poznámka 3. K tomu, abych dokázal platnost posledního tvrzení o interpretaci je třeba zadání trochu upřesnit. Předně jevy "pozorování pochází z p" a "pozorování pochází z q" považuji za disjunktní. Dále je třeba fixovat způsob rozhodování. Předpokládám, že pro pozorování $s \in G$ rozhodneme v případě $p(s) \geq q(s)$ (tedy $s \in B$) pro rozdělení p v případě $p(s) < q(s)$ ($s \in G \setminus B$) pro rozdělení q.

Nejprve dokážeme jednu z dalších možností, jak variační vzdálenost počítat.

Lemma 10. *Buď G konečná grupa. p, q pravděpodobnosti na G. Definujme funkci $\alpha : 2^G \to \mathbb{R}$ předpisem $\alpha(M) := p(M) - q(M)$, $M \subset G$. Funkce α je znaménková míra. Buď B podmnožina G, pak platí:*

B maximalizuje α, B je největší taková $\iff$

$$\iff B = \{s \in G; \alpha(\{s\}) \geq 0\} \iff G \setminus B = \{s \in G; \alpha(\{s\}) < 0\}.$$

Buď $B = \{s \in G; \alpha(\{s\}) \geq 0\}$, pak platí $\alpha(G \setminus B) = -\alpha(B)$, $\|p - q\| = \alpha(B)$.

Důkaz: Že α je znaménková míra je zřejmé. Dále nechť $B \subset G$ maximalizuje funkci α a je největší taková. Pro $s \in B$ platí $\alpha(\{s\}) \geq 0$, jinak by $\alpha(B \setminus \{s\}) > \alpha(B)$, což je spor s volbou B. Pro $s \in G \setminus B$ platí $\alpha(\{s\}) < 0$ jinak by $\alpha(B \cup \{s\}) \geq \alpha(B)$, což je opět spor s volbou B.

Označme $\eta = \alpha(B) \geq 0$. Z definice α platí $\alpha(G) = 0$, což dává $0 = \alpha(G) = \alpha(B) + \alpha(G \setminus B)$ a tedy $\alpha(G \setminus B) = -\alpha(B) = -\eta$. Vezměme naopak libovolnou množinu A minimalizující α. Zřejmě $(G \setminus B) \subset A$, protože jinak pro libovolné $s \in G \setminus B, s \notin A$ platí $\alpha(A \cup \{s\}) < \alpha(A)$, což je spor s volbou A. Množinu A lze tedy rozložit na $A = (G \setminus B) \cup (B \cap A)$, z toho $\alpha(A) = \alpha(G \setminus B) + \alpha(B \cap A)$, kde $\alpha(B \cap A) \geq 0$ a tedy $\alpha(A) \geq \alpha(G \setminus B) = -\eta$. Dostáváme $\|p - q\| = \max_{A \subset G} |\alpha(A)| = \eta$, kde η je míra α libovolné množiny maximalizující α (např. B). □

Důkaz: (řešení cvičení 2) Označme α znaménkovou míru $\alpha : 2^G \to \mathbb{R}$ definovanou předpisem $\alpha(M) := p(M) - q(M)$,$M \subset G$ a $B = \{s \in G; \alpha(\{s\}) \geq 0\} \subset G$, označme $\eta = \alpha(B)$ pak z lemmatu 10 dostáváme $G \setminus B = \{s \in G; \alpha(\{s\}) < 0\}$, $\alpha(G \setminus B) = -\eta$, $\|p - q\| = \eta$. Dokážeme prvou rovnost

$$\frac{1}{2}\sum_{s\in G}|p(s)-q(s)| = \frac{1}{2}(\sum_{s\in B}|p(s)-q(s)| + \sum_{s\in G\setminus B}|p(s)-q(s)|) =$$
$$= \frac{1}{2}(\sum_{s\in B} p(s)-q(s) - \sum_{s\in G\setminus B} p(s)-q(s)) = \frac{1}{2}(\alpha(B) - \alpha(G\setminus B)) = \eta = \|p-q\|.$$

Nyní k druhé rovnosti. Definujme $f_B(s) := 1$ pro $s \in B$ a $f_B(s) := -1$ pro $s \in G \setminus B$. Volba $f := f_B$ hned dává $\|p - q\| = \eta \leq \frac{1}{2}\max_{\|f\|\leq 1}|p(f) - q(f)|$. Ukážeme druhou nerovnost. Buď f libovolná funkce na G s $\|f\| \leq 1$. Pro každé $s \in G$ platí $-1 \leq f(s) \leq 1$. Pro $s \in B$ platí $p(\{s\}) - q(\{s\}) = \alpha(\{s\}) \geq 0$ a pro $s \in G \setminus B$ naopak $p(\{s\}) - q(\{s\}) = \alpha(\{s\}) \leq 0$. Dostáváme odhady pro $f(s)\alpha(\{s\})$

$$-\alpha(\{s\}) \leq f(s)\alpha(\{s\}) \leq \alpha(\{s\}) \text{ pro } s \in B,$$
$$\alpha(\{s\}) \leq f(s)\alpha(\{s\}) \leq -\alpha(\{s\}) \text{ pro } s \in G \setminus B.$$

Rozepíšeme

$$p(f) - q(f) = \sum_{s\in G} f(s)(p(s)-q(s)) = \sum_{s\in G} f(s)\alpha(\{s\}).$$

Uplatněním odhadů pro $f(s)\alpha(\{s\})$ dostáváme

$$-2\eta = -\sum_{s\in B}\alpha(\{s\}) + \sum_{s\in G\setminus B}\alpha(\{s\}) \leq p(f)-q(f) \leq \sum_{s\in B}\alpha(\{s\}) - \sum_{s\in G\setminus B}\alpha(\{s\}) = 2\eta.$$

Dostáváme druhou nerovnost $\|p - q\| = \eta \geq \frac{1}{2}\max_{\|f\|\leq 1}|p(f) - q(f)|$.

Dokážeme poslední tvrzení o interpretaci variační vzdálenosti. Označme H_p resp. H_q disjunktní jevy "pozorování pochází z p" resp. "pozorování pochází z q". Označím S náhodnou veličinu mající význam pozorování. Víme $P(H_p) = P(H_q) = 1/2$ a dále $P(S = s|H_p) = p(s)$, $P(S = s|H_q) = q(s)$. Platí

$$P(\text{"správné rozhodnutí"}) = P(S \in B, H_p) + P(S \in G \setminus B, H_q) =$$
$$= \sum_{s\in B} P(S=s,H_p) + \sum_{s\in G\setminus B} P(S=s,H_q) =$$
$$= \sum_{s\in B} P(S=s|H_p)P(H_p) + \sum_{s\in G\setminus B} P(S=s|H_q)P(H_q) =$$
$$= \frac{1}{2}(1 - q(G) + \sum_{s\in B} p(s) + \sum_{s\in G\setminus B} q(s)) =$$
$$= \frac{1}{2} + \frac{1}{2}(\sum_{s\in B} p(s) - q(s)) = \frac{1}{2} + \frac{1}{2}\eta = \frac{1}{2} + \frac{1}{2}\|p-q\|.$$

□

Cvičení 3. ([1], kap.3B, exercise 3, str.22) Ukažte, že když U je rovnoměrné a $h : G \to G$ je bijekce, pak

$$\|p - U\| = \left\|ph^{-1} - U\right\|, \text{kde } ph^{-1}(A) = p(h^{-1}(A)).$$

Důkaz: Použijeme, že h je permutace (G je konečná, jinak by nebyla variační vzdálenost vůbec definovaná) a tedy $Uh^{-1}(s) = 1/|G| = U(s)$, dostáváme

$$\left\|ph^{-1} - U\right\| = \frac{1}{2}\sum_{s\in G} |p(h^{-1}(s)) - U(s)| =$$
$$= \frac{1}{2}\sum_{s\in G} |p(h^{-1}(s)) - U(h^{-1}(s))| = \frac{1}{2}\sum_{g\in G} |p(g) - U(g)| = \|p - U\|.$$

□

Cvičení 4. ([1], kap.3B, exercise 4, str.22) Buď $G = S_n$. (a) Nechť p je definovaná "karta 1 je navrchu, zbytek je náhodný". Tedy $p(\pi) = 0$ pro $\pi(1) \neq 1$ a $p(\pi) = 1/(n-1)!$ jinak. Jaká je $\|p - U\|$? (b) Nechť p je definovaná "karta 1 je náhodně rozložena na fixní množině A pozic, všechny ostatní karty jsou rozloženy náhodně". Jaká je $\|p - U\|$?

Poznámka 4. Jak je naznačeno v bodě (a) náhodným rozložením je myšleno rovnoměrné. V bodě (b) se tedy nejspíš jedná o rozdělení $p(\pi) = (1/|A|)(1/(n-1)!)$ pro $\pi(1) \in A$, $p(\pi) = 0$ jinak.

Řešení: (cvičení 4) Z lemmatu 10 dostáváme $\|p - q\| = p(B) - q(B)$, kde $B = \{s \in G; p(s) - q(s) \geq 0\}$, kde nyní $G = S_n$ a $q = U$.

(a) Zde má množina B tvar $B = \{\pi \in S_n; \pi(1) = 1\}$, tedy

$$\|p - U\| = p(B) - U(B) = (n-1)!(\frac{1}{(n-1)!} - \frac{1}{n!}) = 1 - \frac{1}{n}.$$

(b) Zde má množina B tvar $B = \{\pi \in S_n; \pi(1) \in A\}$, tedy

$$\|p - U\| = p(B) - U(B) = |A|(n-1)!(\frac{1}{|A|(n-1)!} - \frac{1}{n!}) = 1 - \frac{|A|}{n}.$$

□

Nyní uvedu lemma o horní mezi na variační vzdálenost, kterého se často v [1] využívá a rovněž zde se na něj budu při řešení příkladů často odvolávat.

Lemma 11. *(Lemma o horní mezi, [1], kap.3B, str.24) Nechť q je pravděpodobnost na konečné grupě G. Pak*

$$\|q - U\|^2 \leq \frac{1}{4}\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{q}(\rho)\hat{q}^H(\rho)),$$

kde $\sum_\rho^*$ značí součet přes všechny netriviální ireducibilní reprezentace ρ grupy G. Dále reprezentace v $\sum_\rho^*$ se předpokládají unitární.

K unitárním reprezentaci lze vždy přejít podle poznámky 1. Reprezentace $\mathbb{Z}_n$ odvozené v lemmatu 9 jsou unitární. Každá maticová permutační reprezentace je rovněž unitární.

Cvičení 5. ([1], kap.3B, exercise 5, str.24) S notací lemmatu o horní mezi, ukažte

$$\|q-U\| \geq \frac{1}{2|G|}\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{q}(\rho)\hat{q}^H(\rho)).$$

Rovněž ukažte

$$\|q-U\|^2 \geq \frac{1}{4|G|}\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{q}(\rho)\hat{q}^H(\rho)).$$

Důkaz: Nejprve určíme Fourierovu transformaci funkce $q-U$ na ireducibilních reprezentacích. Na triviální reprezentaci ρ_t mají všechny pravděpodobnosti p na G Fourierovu transformaci jednotkovou, jak je snadno vidět $\hat{p}(\rho_t) = \sum_{s\in G} p(s)\rho_t(s) = \sum_{s\in G} p(s)1 = 1$. Tedy $\widehat{q-U}(\rho_t) = 0$. Na libovolné netriviální ireducibilní reprezentaci ρ je z lemmatu 8 VI $\widehat{U}(\rho) = 0$ a tedy $\widehat{q-U}(\rho_t) = \hat{q}$.

Použitím cvičení 2, $|q(s)-U(s)| \leq 1$ pro $s \in G$, a Plancherelovy formule pro reálné funkce a unitární reprezentace viz. lemma 8 III, dostáváme

$$\|q-U\| = \frac{1}{2}\sum_{s\in G}|q(s)-U(s)| \geq \frac{1}{2}\sum_{s\in G}|q(s)-U(s)|^2 = \frac{1}{2|G|}\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{q}(\rho)\hat{q}^H(\rho)),$$

obdobně postupujeme i u druhé nerovnosti

$$\|q-U\|^2 = \frac{1}{4}(\sum_{s\in G}|q(s)-U(s)|)^2 \geq \frac{1}{4}\sum_{s\in G}|q(s)-U(s)|^2 = \frac{1}{4|G|}\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{q}(\rho)\hat{q}^H(\rho)).$$

□

Cvičení 6. ([1], kap.3B, exercise 6, str.25) Nechť G je konečná grupa. Definujme pravděpodobnost p na G

$$p(e) = 1-\frac{\epsilon}{2}, \quad p(s) = \frac{\epsilon}{2(|G|-1)} \text{ pro } s \neq e,\ 0 \leq \epsilon \leq 2.$$

Ukažte, že

$$p^{*k}(e) = \frac{1}{|G|} + \frac{|G|-1}{|G|}(1-\frac{\epsilon}{2}\frac{|G|}{|G|-1})^k,$$
$$p^{*k}(s) = \frac{1}{|G|} - \frac{1}{|G|}(1-\frac{\epsilon}{2}\frac{|G|}{|G|-1})^k \text{ pro } s \neq e,$$
$$\left\|p^{*k}-U\right\| = \frac{|G|-1}{|G|}|1-\frac{\epsilon}{2}\frac{|G|}{|G|-1}|^k,$$
$$\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{p}^k(\rho)\hat{p}^{kH}(\rho)) = (|G|-1)(1-\frac{\epsilon}{2}\frac{|G|}{|G|-1})^{2k}.$$

Poznámka 5. Zadání má smysl pouze pro $|G| \geq 2$ (budu to tedy při důkazu předpokládat). Tento příklad má sloužit jako příklad, kdy lemma o horní mezi nedává příliš dobrý odhad a skutečně poměr odhadu variační vzdálenosti ze zmíněného lemmatu a skutečné variační vzdálenosti pro právě řešený příklad může být dosti vysoký

$$\frac{\frac{1}{4}\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{p}^k(\rho)\hat{p}^{kH}(\rho))}{\|p^{*k} - U\|^2} = \frac{|G|^2}{4(|G|-1)}.$$

Důkaz: Co se týče reprezentací G budu při důkazu pracovat pouze s unitárními ireducibilními maticovými reprezentacemi. Nejjednodušší je asi převést výpočet do obrazové oblasti Fourierovy transformace. Rozepíšeme p jako lineární kombinaci pravděpodobností δ a U

$$p = \alpha\delta + \beta U, \quad \alpha := 1 - \frac{\epsilon}{2}\frac{|G|}{|G|-1}, \quad \beta := \frac{\epsilon}{2}\frac{|G|}{|G|-1}.$$

Z lemmatu 8 VI víme, že Fourierova transformace pravděpodobnosti U má tvar $\hat{U}(\rho) = 1$ pro ρ triviální, $\hat{U}(\rho) = 0$ pro ρ netriviální (ireducibilní). Dále budeme potřebovat ještě Fourierovu transformaci pravděpodobnosti δ. Z definice snadno zjistíme $\hat{\delta}(\rho) = \sum_{g\in G}\delta(g)\rho(g) = \rho(e) = E$, kde ρ značí jakoukoli reprezentaci a E jednotkovou matici rozměru $d_\rho \times d_\rho$ (d_ρ značím dimenzi reprezentace ρ).

Nyní přejdeme k Fourierovu obrazu $\hat{p} = \alpha\hat{\delta} + \beta\hat{U}$. Ze znalosti $\hat{\delta}$ a $\hat{U}$ dostáváme $\hat{p}(\rho) = (\alpha+\beta)$ pro ρ triviální a $\hat{p}(\rho) = \alpha E$ pro ρ netriviální. Jelikož konvoluce přejde ve Fourierově obrazu na součin dostáváme $\widehat{p^{*k}} = \hat{p}^k$, což dává

$$\widehat{p^{*k}}(\rho) = (\alpha+\beta)^k \text{ pro } \rho \text{ triviální a } \widehat{p^{*k}}(\rho) = (\alpha)^k E \text{ pro } \rho \text{ netriviální.}$$

To lze zapsat jako lineární kombinaci obrazů k pravděpodobnostem δ a ρ

$$\widehat{p^{*k}} = ((\alpha+\beta)^k - \alpha^k)\hat{U} + \alpha^k\hat{\delta}.$$

Použitím prostoty Fourierovy transformace (jakožto zobrazení z $G^{\mathbb{C}}$ do množiny $\{\hat{f}|R_G; f \in G^{\mathbb{C}}\}$, kde R_G jsem označil množinu všech ireducibilních reprezentací grupy G), která plyne přímo z věty o inverzní Fourierově transformaci viz. lemma 8 II, dostáváme

$$p^{*k} = \alpha^k\delta + ((\alpha+\beta)^k - \alpha^k)U.$$

Rozepsáním po prvcích (všimneme si, že $\alpha + \beta = 1$) dostáváme dokazovaný tvar p^{*k}

$$p^{*k}(e) = \frac{1}{|G|} + \frac{|G|-1}{|G|}\alpha^k,$$
$$p^{*k}(s) = \frac{1}{|G|} - \frac{1}{|G|}\alpha^k, \text{ pro } s \in G, s \neq e.$$

Variační vzdálenost určíme nejjednodušeji z lemmatu 10, kde $B = \{e\}$ pro $\alpha^k > 0$ a $G \setminus B = \{e\}$ pro $\alpha^k < 0$ v obou případech dostáváme

$$\left\|p^{*k} - U\right\| = |p^{*k}(e) - U(e)| = \frac{|G|-1}{|G|}|\alpha|^k.$$

Pro $\alpha^k = 0$ je tento výsledek rovněž použitelný, neboť $p^{*k} = U$ a tedy $\left\|p^{*k} - U\right\| = 0$. Pro výraz z lemmatu 11 o horní mezi dostáváme

$$\sum_{\rho}^{*} d_\rho \mathrm{tr}(\hat{p}^k(\rho)\hat{p}^{kH}(\rho)) = \sum_{\rho}^{*} d_\rho \mathrm{tr}(\alpha^k E(\alpha^k E)^*) = \sum_{\rho}^{*} d_\rho^2 \alpha^{2k} = (|G| - 1)\alpha^{2k},$$

kde jsem použil lemmatu 7 IV(b) ($|G| = \sum_\rho d_\rho^2$, kde se sčítá přes všechny ireducibilní reprezentace) a že triviální reprezentace je ireducibilní reprezentace dimenze jedna. Tím je vše požadované dokázáno. □

2.2 Náhodná procházka na $\mathbb{Z}_q$

Cvičení 7 až 10 se týkají náhodné procházky na $\mathbb{Z}_q$ (aditivní grupa celých čísel modulo q) a následujícího tvrzení

Lemma 12. *([1], kap.3C, Theorem 2, str.25) Nechť $\mathbb{Z}_q$ značí aditivní grupu celých čísel modulo q. Definujme $p(-1) = p(1) = 1/2$, $p(j) = 0$ jinak (pravděpodobnost na $\mathbb{Z}_q$). Pak pro $k \geq q^2$, pro q liché větší než 7 platí*

$$\left\|p^{*k} - U\right\| \leq \mathrm{e}^{-\alpha k/q^2}$$

pro $\alpha = \pi^2/2$. Dále pro $q \geq 7$ a jakékoli k platí

$$\left\|p^{*k} - U\right\| \geq \frac{1}{2}\mathrm{e}^{-\alpha k/q^2 - \beta k/q^4},$$

kde $\alpha = \pi^2/2$, $\beta = \pi^4/11$.

Důkaz: (Důkaz je převzat z [1].) Označme $\rho_m(l) = \exp(\jmath 2\pi ml/q)$ pro $m, l \in \mathbb{Z}_q$ ireducibilní unitární reprezentace grupy $\mathbb{Z}_q$ z lemmatu 9. Fourierova transformace pravděpodobnosti p má tvar

$$\hat{p}(\rho_m) = \frac{1}{2}(\mathrm{e}^{\jmath\frac{2\pi m}{q}} + \mathrm{e}^{-\jmath\frac{2\pi m}{q}}) = \cos(\frac{2\pi m}{q}).$$

Z lemmatu o horní mezi 11 dostáváme

$$\left\|p^{*k} - U\right\| \leq \frac{1}{4}\sum_{m=1}^{q-1}\cos(\frac{2\pi m}{q})^{2k} = \frac{1}{2}\sum_{m=1}^{(q-1)/2}\cos(\frac{2\pi m}{q})^{2k} = \frac{1}{2}\sum_{m=1}^{(q-1)/2}\cos(\frac{\pi m}{q})^{2k}.$$

V posledním kroku bylo použito $|\cos(2\pi m/q)| = |\cos(\pi - 2\pi m/q)| = |\cos(\pi(q - 2m)/q)|$, kde $q - 2m$ je liché a tedy členy pro $m > q/4$ v předposlední sumě jsou právě ty členy v poslední sumě s lichým indexem m. Odhadneme kosinus shora

$$\cos x \leq \mathrm{e}^{-\frac{x^2}{2}} \text{ pro } x \in [0, \frac{\pi}{2}].$$

K ověření tohoto faktu zřejmě stačí ukázat, že $h(x) := \ln(\exp(x^2/2)\cos x) < 0$ pro $x \in [0, \pi/2]$. Na uvedeném intervalu platí $h'(x) = x - \tan x \leq 0$ a tedy $h(x) \leq h(0) = 0$. Použijeme získaný odhad kosinu a odhadneme poslední sumu

$$\left\|p^{*k} - U\right\| \leq \frac{1}{2} \sum_{m=1}^{(q-1)/2} \mathrm{e}^{-\frac{\pi^2 m^2 k}{q^2}} =$$

$$= \frac{1}{2}\mathrm{e}^{-\frac{\pi^2 k}{q^2}} \sum_{m=1}^{(q-1)/2} \mathrm{e}^{-\frac{\pi^2 (m^2-1) k}{q^2}} \leq \frac{1}{2}\mathrm{e}^{-\frac{\pi^2 k}{q^2}} \sum_{m=0}^{(q-1)/2} \mathrm{e}^{-\frac{\pi^2 3mk}{q^2}} = \frac{1}{2}\frac{\mathrm{e}^{-\frac{\pi^2 k}{q^2}}}{1 - \mathrm{e}^{-3\frac{\pi^2 k}{q^2}}},$$

kde bylo použito faktu $3m \leq ((m+1)^2 - 1)$ pro $m \in \mathbb{N}_0$ (stačí srovnat členy k indexům m resp. $m+1$ neboť odpovídající sumy sčítají od $m = 0$ resp. od $m = 1$). Odhadnutím jmenovatele jedničkou, což lze pro $k \geq q^2$, neboť jmenovatel je pak menší než jedna, získáváme horní mez v lemmatu.

K dolnímu odhadu použijeme funkci $f := \cos(2\pi ml/q)$ s $m = (q-1)/2$, která je omezená jedničkou a má nulovou střední hodnotu při rovnoměrném rozdělení $\mathrm{E}_U[f] = 0$. Použitím symetrie p dostáváme

$$\mathrm{E}_{p^{*k}}[f] = \sum_{l=0}^{q-1} p^{*k}(l)\cos(\frac{2\pi}{q}ml) =$$

$$= \frac{1}{2}\sum_{l=0}^{q-1} p^{*k}(l)(\mathrm{e}^{\jmath\frac{2\pi}{q}ml} + \mathrm{e}^{-\jmath\frac{2\pi}{q}ml}) = \widehat{p^{*k}}(\rho_m) = \cos(\frac{2\pi m}{q})^k = (-1)^k\cos(\frac{\pi}{q})^k.$$

Použitím cvičení 2 dostáváme

$$\left\|p^{*k} - U\right\| = \frac{1}{2}\max_{\|g\|\leq 1} |\mathrm{E}_{p^{*k}}[g] - \mathrm{E}_U[g]| = |\mathrm{E}_{p^{*k}}[f] - \mathrm{E}_U[f]| \geq |\cos(\frac{\pi}{q})^k|.$$

Je-li $x \leq 1/2$, $\cos x \geq \exp(-x^2/2 - x^4/11)$, což dává dokazovaný tvar dolní meze pro $q \geq 7$. □

V poznámce [1] zmiňuje další dva možné přístupy k získání dolní meze na $\left\|p^{*k} - U\right\|$. Uvedu pouze jeden

Poznámka 6. ([1], kap.3C, remark 3, approach 2, str.27): Uvažujte náhodnou procházku na celých číslech s kroky ± 1 s pravděpodobností 1/2. Nechť S_k je částečný součet. Proces z lemmatu 12 je $S_n \pmod q$. Použitím centrální limitní věty (pro k malá oproti q^2) má S_k pouze malou šanci se dostat mimo $\{j; |j| \leq q/4\}$. To se dá upřesnit použitím Berry-Esséenovy věty.

Cvičení 7. ([1], kap.3C, exercise 7, str.27) Napište opravdový důkaz pro jeden z přístupů uvedených v poznámce 6. Ukažte, že $\left\|p^{*k} - U\right\| \to 1$ pro $n = c(q)q^2$, $c(q) \to 0$.

Jak je zmíněno bude potřeba Berry-Esséenova věta.

Lemma 13. *(Berry-Esséenova Věta [5], kap.XVI.5, Theorem 1, str.542) Nechť $X_1, X_2, ...,$ jsou nezávislé identicky rozložené náhodné proměnné s $\mathrm{E}[X_1] = 0$, $\mathrm{E}[X_1^2] = \sigma^2 > 0$, a $\mathrm{E}[|X_1|^3] = \rho < \infty$. Definujme $Y_n = (X_1 + X_2 + \cdots + X_n)/(\sigma\sqrt{n})$. Označme F_n distribuční funkci pro Y_n, a ϕ distribuční funkci k standardnímu normálnímu rozdělení. Pak pro všechna x a n platí*

$$|F_n(x) - \phi(x)| < \frac{C\rho}{\sigma^3\sqrt{n}},$$

kde $C = 3$.

Hodnota konstanty C byla postupně zmenšována, wikipedie uvádí nejnovější referenci [7], kde byla stanovena hodnota této konstanty $C = 0.7056$. Zde budu používat hodnotu $C = 0.80$. Dokážeme následující.

Lemma 14. *(Řešení ke cvičení 7) Nechť $p(-1) = p(1) = 1/2$, $p(j) = 0$ jinak je pravděpodobnost na $\mathbb{Z}_q$, pro q liché (stejné jako ve lemmatu 12). Označme $\bar{p}$ pravděpodobnost rozšiřující p na $\mathbb{Z}$. Buď (S_k) náhodná procházka na $\mathbb{Z}$ generovaná pravděpodobností $\bar{p}$ (stejně jako v poznámce 6). Označme G_k distribuční funkci k S_k a ϕ distribuční funkci k standardnímu normálnímu rozdělení. C nechť má stejný význam jako v Berry-Esséenově větě (lemma 13). Buď x libovolné takové, že $0 < x \leq 1/2$ a $xq \notin \mathbb{Z}$. Pak platí:*
I.

$$\left\|p^{*k} - U\right\| \geq (\sum_{n\in\mathbb{Z}} G_k(xq + 2nq) - G_k(-xq + 2nq)) - x - \frac{1}{q},$$
$$\left\|p^{*k} - U\right\| \geq 2\phi(\frac{xq}{\sqrt{k}}) - 1 - x - \frac{1}{q} - \frac{2C}{\sqrt{k}},$$
$$\left\|p^{*k} - U\right\| \geq 2(\phi(\frac{xq}{\sqrt{k}}) + \phi(\frac{xq+2q}{\sqrt{k}}) - \phi(\frac{-xq+2q}{\sqrt{k}})) - 1 - x - \frac{1}{q} - \frac{6C}{\sqrt{k}}.$$

II. Nechť $q > 10^5$, pak platí

$$\left\|p^{*q^2} - U\right\| \geq 0.0041.$$

III. Buď c funkcí q splňující $c(q) \to 0+ \wedge q\sqrt{c(q)} \to \infty$ pro $q \to \infty$ a $q^2c \in \mathbb{N}_0$. Definujme $k = q^2c$, pak

$$\left\|p^{*k} - U\right\| \to 1 \quad \textit{pro } q \to \infty.$$

Poznámka 7. Nedostatkem odhadů obdržených v bodě I. (2. a 3. nerovnost) je jednak výskyt distribuční funkce ϕ standardního normálního rozdělení, a dále odhad chyby aproximace G_k pomocí ϕ (členy s C), který vyžaduje poměrně velké množství kroků k, aby byl dostatečně malý.

Na druhou stranu mohou tyto odhady dávat i lepší dolní mez než odhady z lemmatu 12, což je demonstrováno v bodě II. (odhad z lemmatu 12 dává pouze 0.0036).

V bodě III. byl přidán předpoklad $q\sqrt{c(q)} \to \infty$, pro $q \to \infty$, který je nutný k omezení chyby aproximace z Berry-Esséenovy věty, jinak tato chyba diverguje a činí tak aproximaci nepoužitelnou. S touto úpravou má úloha stále smysl, neboť c předepsaných vlastností stále existují např. $c(q) = 1/q$.

Důkaz: I. Buď $0 < x \leq 1/2$, $xq \notin \mathbb{Z}$, k sudé definujme množinu $M_x = \{2i \in \mathbb{Z}_q; i \in \mathbb{Z}, 0 \leq 2i < xq\} \cup \{q - 2i \in \mathbb{Z}_q; i \in \mathbb{Z}, 0 < 2i < xq\}$. Pak platí

$$\begin{aligned}\left\|p^{*k} - U\right\| \geq p^{*k}(M_x) - U(M_x) = P(S_k \in \cup_{n\in\mathbb{Z}}\{2i + 2nq; |2i| < xq\}) - U(M_x) = \\ = (\sum_{n\in\mathbb{Z}} G_k(xq + 2nq) - G_k(-xq + 2nq)) - U(M_x) \geq \\ \geq (\sum_{n\in\mathbb{Z}} G_k(xq + 2nq) - G_k(-xq + 2nq)) - x - \frac{1}{q}.\end{aligned}$$

Analogicky lze postupovat pro k liché. Tím je dokázán první odhad v I. Druhý resp. třetí odhad dostaneme tím, že z sumy (s kladnými členy) vezmeme pouze členy pro $n = 0$ resp. $n = -1, 0, 1$ a použijeme aproximaci z Berry-Esséenovy věty (členů nelze vzít příliš mnoho, neboť tím celková chyba aproximace rychle roste - pro l členů má velikost $2l/\sqrt{k}$). V Berry-Esséenově větě položíme $Y_k\sigma\sqrt{k} = S_k$, pak (X_k) z věty má význam procesu přírůstku a jednotlivé X_k mají tedy rozdělení $\bar{p}$, snadno ověříme $\mathrm{E}[X_1] = 1/2(1 - 1) = 0$, $\mathrm{E}[X_1^2] = \sigma^2 = 1/2(1 + 1) = 1$, a $\mathrm{E}[|X_1|^3] = \rho = 1/2(1 + 1) = 1 < \infty$. Postup uvádím pouze pro druhý odhad (třetí se konstruuje obdobně)

$$\begin{aligned}(\sum_{n\in\mathbb{Z}} G_k(xq + 2nq) - G_k(-xq + 2nq)) - x - \frac{1}{q} \geq G_k(xq) - G_k(-xq) - x - \frac{1}{q} \geq \\ \geq \phi(\frac{xq}{\sqrt{k}}) - \phi(-\frac{xq}{\sqrt{k}}) - x - \frac{1}{q} - \frac{2C}{\sqrt{k}} \geq 2\phi(\frac{xq}{\sqrt{k}}) - 1 - x - \frac{1}{q} - \frac{2C}{\sqrt{k}}.\end{aligned}$$

II. Využijeme třetího odhadu z I. a dosadíme počet kroků $k = q^2$ a $x = 1/2$ (tedy $xq \notin \mathbb{Z}$). Pro takové velké k je nutné se omezit, jak je uvedeno v předpokladu na dostatečně velká $q > 10^5$ (aby chyba aproximace z Berry-Esséenovy věty byla přijatelná). Použijeme $C = 0.8$

$$\left\|p^{*q^2} - U\right\| \geq 2(\phi(0.5) + \phi(2.5) - \phi(1.5)) - 1 - 0.5 - 10^{-5} - 6 \cdot 0.8 \cdot 10^{-5} = 0.0041,$$

kde jsem použil hodnoty kvantilů $\phi(0.5) = 0.6915$, $\phi(1.5) = 0.9332$, $\phi(2.5) = 0.9938$ z [6].

III. Mějme c splňující předpoklady a nechť $k = q^2c$. Jelikož platí $0 < \sqrt{y}|\ln(y)| \to 0+$ pro $y \to 0+$, existuje y_0 tak že pro všechna $0 < y < y_0$ je $0 < \sqrt{y}|\ln(y)| < 1/2$. Dále z $c(q) \to 0 \wedge q\sqrt{c(q)} \to \infty$ pro $q \to \infty$ plyne existence q_0 takového, že pro každé $q > q_0$, $0 < c(q) < y_0$. Definujme $x(q) := \sqrt{c(q)}|\ln(c(q))|$ pro $q > q_0$, pak dostáváme $0 < x(q) < 1/2$. V případě, že pro nějaké q nastává $x(q)q \in \mathbb{Z}$ zvolíme nějaké $\theta_q \in (0.9, 1)$ tak, aby $\theta_q\sqrt{c(q)}|\ln(c(q))|q \notin \mathbb{Z}$ a předefinujeme $x(q) := \theta_q\sqrt{c(q)}|\ln(c(q))|$.

Nyní již $x(q)$ splňuje předpoklady bodu I. a lze tedy použít druhý odhad

$$\left\|p^{*k} - U\right\| \geq 2\phi(\frac{xq}{\sqrt{k}}) - 1 - x - \frac{1}{q} - \frac{2C}{\sqrt{k}}.$$

Definujme $z = \theta\sqrt{c(q)}|\ln(c(q))|$. Stačí ukázat, že pro libovolné $\theta \in (0.9, 1]$ a

$$B(q) := 2\phi(\frac{zq}{\sqrt{k}}) - 1 - z - \frac{1}{q} - \frac{2C}{\sqrt{k}}$$

platí $B(q) \to 1$. Zvolme tedy libovolné $\theta \in (0.9, 1]$. Dostáváme

$$\lim_{q\to\infty} \phi(\frac{zq}{\sqrt{k}}) = \lim_{q\to\infty} \phi(\theta|\ln(c(q))|) = 1,$$

kde bylo použito věty o limitě složené funkce jednak pro $-\ln(u) \to \infty$, $u \to 0$ (pro vnitřní funkci $0 < c(q) \to 0$, $q \to \infty$) a jednak pro $\phi(v) \to 1-$, $v \to \infty$. Dále

$$\lim_{q\to\infty} z = \theta \lim_{q\to\infty} \sqrt{c(q)}|\ln(c(q))| = 0.$$

Opět se použije věta o limitě složené funkce pro vnější funkci $\sqrt{u}|\ln(u)| \to 0$, $u \to 0$ a vnitřní funkci $0 < c(q) \to 0$, $q \to \infty$. Dále se využije předpokladu $\sqrt{k} = q\sqrt{c(q)} \to \infty$ pro $p \to \infty$

$$\lim_{q\to\infty} \frac{2C}{\sqrt{k}} = 0.$$

Věta o součtu limit pak dává požadované. □

Cvičení 9. ([1], kap.3C, exercise 9, str.28) Dokažte, že konvoluce symetrických unimodálních rozdělení na $\mathbb{Z}_n$ je opět symetrické unimodální rozdělení.

Před vlastním důkazem nejprve upřesním intuitivně jasné pojmy symetrie a unimodalita na $\mathbb{Z}_n$.

Definice 8. *Buď $f \in L^1(\mathbb{Z}_n)$. f má v $k_0 \in \mathbb{Z}_n$ ostré lokální maximum právě tehdy, když $f(k_0 - 1) \leq f(k_0) \wedge f(k_0 + 1) \leq f(k_0)$.*

Dále f je symetrická kolem 0 právě tehdy, když pro všechna $k \in \mathbb{Z}_n$, $0 \leq k \leq n/2$ platí $f(k) = f(-k)$. Dále f je symetrická kolem k_0 právě tehdy, když $f(k - k_0)$ je symetrická kolem 0.

Intervalem na $\mathbb{Z}_n$ rozumím obraz intervalu J na $\mathbb{Z}$ s $|J| \leq n$ při zobrazení $\phi = b \circ \pi$, kde $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ je kanonická projekce a b je kanonický izomorfizmus $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Uspořádaný interval $\phi(J)^{\leq}$ na $\mathbb{Z}_n$ je interval $\phi(J)$ na $\mathbb{Z}_n$ s uspořádáním převzatým ze $\mathbb{Z}$, tedy pro $a, b \in \phi(J)^{\leq}$ je $a \leq b \iff \phi^{-1}(a) \leq \phi^{-1}(b)$ (podobně pro ostré uspořádání). Z podmínky $|J| \leq n$ se snadno ověří prostota $\phi|J$ a tedy i korektnost definice. Pro každé $a \in \phi(J)^{\leq}$ definujeme $|a| = |\phi^{-1}(a)|$.

f je neklesající resp. nerostoucí na (uspořádaném) intervalu $\phi(J)^{\leq} \in \mathbb{Z}_n$ právě tehdy, když pro všechna $a, b \in \phi(J)^{\leq}$ platí $a \leq b \Rightarrow f(a) \leq f(b)$ resp. $a \leq b \Rightarrow f(a) \geq f(b)$

f je symetrická (ostře) unimodální právě tehdy, když existuje k_0 tak, že f je symetrická kolem k_0 (,má ostré lokální maximum v k_0) a je nerostoucí na $\phi([k_0, k_0 + n/2])^{\leq}$.

Lemma 15. *Buďte $f, g \in L^1(\mathbb{Z}_n)$.*

I. Nechť f, g jsou symetrické unimodální, pak $f * g$ je symetrická unimodální.

II. Nechť f, g jsou symetrické ostře unimodální, pak $f * g$ je symetrická ostře unimodální.

Důkaz: I. Buď $2 \leq n \in \mathbb{Z}_n$ sudé (pro lichá n se důkaz liší pouze málo). Buďte $f, g \in L^1(\mathbb{Z}_n)$ symetrické unimodální. Bez újmy na obecnosti nechť je k_0 v definici symetrické unimodální funkce u obou funkcí nulové. Jinak by stačilo vzít $f'(k) := f(k - k_0)$, $g'(k) := g(k - l_0)$. Protože konvoluce s δ_{k_0} (viz. definice 3) realizuje pouze posunutí o k_0 a $f' * g' = f * \delta_{k_0} * g * \delta_{l_0} = f * g * \delta_{k_0+l_0}$ (kde jsme použili komutativitu konvoluce pro abelovské grupy a faktu, že $m \mapsto \delta_m$ pro $m \in \mathbb{Z}_n$ je grupový homomorfizmus - viz. lemma 2), dostáváme $f' * g'$ je je pouze posunutou verzí konvoluce původních funkcí $(f' * g')(k) = (f * g)(k - k_0 - l_0)$. Posuv však na symetrii případně unimodalitě nic nezmění.

Ukážeme, že $h = f * g$ je opět symetrická unimodální (s $k_0 = 0$). Nejprve ukážeme symetrii kolem 0. Vezměme libovolné $k \in \phi([0, n/2])$, pak platí

$$h(-k) = (f * g)(-k) =$$
$$= \sum_{l=-n/2+1}^{n/2} f(-k-l)g(l) = \sum_{l=-n/2+1}^{n/2} f(k+l)g(-l) = \sum_{u=-n/2}^{n/2-1} f(k-u)g(u) = h(k),$$

kde byla použita symetrie f, g kolem 0 (a substituce $u = -l$).

Nyní budeme dokazovat tvrzení o monotonii. Víme (z předpokladu), že f i g jsou nerostoucí na $\phi([0, n/2])^{\leq}$ a neklesající na $\phi([-n/2, 0])^{\leq}$ (symetrie f, g). Stačí ukázat $h(k) \geq h(k + 1)$ pro $k \in \phi([0, n/2 - 1])^{\leq}$. Zvolme jedno $k \in \phi([0, n/2 - 1])^{\leq}$, nerovnost je ekvivalentní (použijeme symetrii g)

$$0 \leq h(k)-h(k+1) = \sum_{l=-n/2}^{n/2-1} f(l)(g(k-l)-g(k-l+1)) = \sum_{l=-n/2}^{n/2-1} f(l)(g(l-k)-g(l-k-1)). \tag{2.2}$$

Ve zbytku zavedu absolutní hodnotu a uspořádání na $\mathbb{Z}_n$ podle $I = \phi([-n/2, n/2 - 1])^{\leq}$ (meze u l v sumě). Podle toho, pro jaká $l \in I$ padne $l - k$ do $\phi([1, n/2])$ resp. do $\phi([-n/2 + 1, 0])$, rozložíme I na dvě množiny A_1 resp. A_2

$$\begin{aligned} A_1 &:= \{l \in I; l - k \in \phi([1, n/2])\} = \phi([k + 1, n/2 + k]) = \\ &= \phi([-n/2, -n/2 + k]) \cup \phi([k + 1, n/2 - 1]), \\ A_2 &:= \{l \in I; l - k \in \phi([-n/2 + 1, 0])\} = \phi([-n/2 + k + 1, +k]). \end{aligned}$$

Pro $l \in A_1$ je zřejmě rozdíl v sumě $g(l - k) - g(l - k - 1) \leq 0$ v důsledku toho, že g je na intervalu $\phi([1, n/2])^{\leq}$ nerostoucí podle předpokladu. Obdobně pro $l \in A_2$ je $g(l - k) - g(l - k - 1) \geq 0$ v důsledku toho, že g je na $\phi([-n/2 + 1, 0])^{\leq}$ neklesající. Označme $\Delta(l) := g(l - k) - g(l - k - 1)$. Ze symetrie g je jasné, že zvolíme-li libovolné $l_2 \in A_2$, pak existuje $l_1 \in A_1$ tak, že $\Delta(l_2) = -\Delta(l_1)$. Přesněji existuje bijekce $\theta : A_2 \to A_1$ taková, že

$$\Delta(l) = -\Delta(\theta(l)).$$

Přepíšeme výraz v (2.2) s použitím uvedené vlastnosti

$$h(k)-h(k+1)=\sum_{l=-n/2}^{n/2-1} f(l)\Delta(l)=\sum_{l\in A_1} f(l)\Delta(l)+\sum_{l\in A_2} f(l)\Delta(l)=$$
$$=\sum_{l\in A_2} f(\theta(l))\Delta(\theta(l))+\sum_{l\in A_2} f(l)\Delta(l)=\sum_{l\in A_2}(f(\theta(l))\Delta(\theta(l))+f(l)\Delta(l))=$$
$$=\sum_{l\in A_2}(f(\theta(l))(-\Delta(l))+f(l)\Delta(l))=\sum_{l\in A_2}(f(l)-f(\theta(l)))\Delta(l).$$

Jelikož $\Delta(l)\geq 0$ stačí dokázat

$$f(l)-f(\theta(l))\geq 0.$$

Z toho, že f je nerostoucí "napravo" od 0, neklesající "nalevo" od 0 a symetrická stačí ukázat, že $\theta(l)$ je "dál" od 0 než l. Přesněji stačí ukázat, že

$$|\theta(l)|\geq |l|, \tag{2.3}$$

kde absolutní hodnotu případně uspořádání vztahujeme k $I=\phi([-n/2,n/2-1])^{\leq}$. K tomu budeme potřebovat konkrétní tvar bijekce θ. Zobrazení (zrcadlení)

$$\theta(l):=l+2(k-l)+1=-l+2k+1$$

splňuje všechny podmínky kladené na θ, neboť je to bijekce A_2 na A_1 a (použijeme symetrii g)

$$\Delta(\theta(l))=g(\theta(l)-k)-g(\theta(l)-k-1)=$$
$$=g(-l+k+1)-g(-l+k)=g(l-k-1)-g(l-k)=-\Delta(l).$$

Mějme tedy $l\in A_2=\phi([-n/2+k+1,+k])$, abychom mohli uplatnit absolutní hodnotu $|\theta(l)|$ potřebujeme najít $(\phi|[-n/2,n/2-1])^{-1}(\theta(l))$, tedy hodnotu z $[-n/2,n/2-1]$ jež je rovna $\theta(l)$ až na násobek n. To je právě ta hodnota $\theta(l)+mn$, $m\in\mathbb{Z}$, která je nejblíž 0. Vezmeme $-l+2k+1\geq 0$ a $-l+2k+1-n\leq 0$ (ostatní jsou dál). Stačí ukázat $-l+2k+1-n\leq |l|\leq -l+2k+1$. Pro $l<0$ dostáváme

$$-l+2k+1-n\ \leq\ -l\ \leq\ -l+2k+1\quad\Longleftrightarrow\quad 2k+1-n\ \leq\ 0\ \leq\ 2k+1.$$

Obě poslední nerovnosti jsou splněny z definice k. Pro $l\geq 0$ dostáváme

$$-l+2k+1-n\leq l\leq -l+2k+1\iff$$
$$\iff 2k+1-n\leq 2l\leq 2k+1\iff k+1/2-n/2\leq l\leq k+1/2,$$

což platí z $l\in A_2=\phi([-n/2+k+1,k])$. Tím je (2.3) a tedy požadované tvrzení o monotonii h dokázáno.

II. Opět stačí předpokládat že f i g mají maxima v 0. Z toho, že f je symetrická ostře unimodální plyne existence $0<a\in\mathbb{R}$, že $f-a\delta$ je symetrická unimodální.

Podobně existuje $0 < b \in \mathbb{R}$, že $g - b\delta$ je symetrická unimodální. Pak platí (použijeme bilinearitu konvoluce a a že δ je jednotkový prvek vzhledem ke konvoluci viz. lemma 2)

$$h = f * g = (f - a\delta + a\delta) * (g - b\delta + b\delta) = (f - a\delta) * (g - b\delta) + b(f - a\delta) + a(g - b\delta) + ab\delta.$$

Prvý člen je podle I. symetrický unimodální druhý a třetí rovněž (vše kolem 0), součet je tedy rovněž symetrický unimodální (součet nerostoucích na intervalu je nerostoucí, součet symetrických zůstává symetrický). Poslední (čtvrtý) příspěvek k součtu pak garantuje existenci ostrého lokálního maxima v 0. □

Cvičení 10. ([1], kap.3C, exercise 10, str.28) Nechť n je liché. Uvažujte náhodnou procházku na $\mathbb{Z}_n$ generovanou $p(1) = p(-1) = 1/2$. Dokažte, že po sudém počtu kroků, bude mít 0 největší pravděpodobnost. Obecněji ukažte, že je procházka monotónní ve smyslu $p^{*2k}(j) \geq p^{*2k}(j + 2i)$, kde $0 \leq j \leq j + 2i \leq n/2$.

Důkaz: Označme $G \cong H \cong \mathbb{Z}_n$ izomorfní kopie $\mathbb{Z}_n$. Buď (X_k) náhodná procházka na G generovaná p. Nejprve ukážeme, že (Y_k), kde $Y_k := X_{2k}$ je náhodná procházka na G generovaná p^{*2}. Buď (D_k) proces přírůstku pro (X_k). Definuji $C_k := D_{2k+1}D_{2k}$, jelikož jsou D_k, $k \in \mathbb{N}_0$ nezávislé jsou i C_k, $k \in \mathbb{N}_0$ nezávislé. Abychom získali rozdělení $C_k = D_{2k+1}D_{2k}$, všimneme si, že D_{2k+1} a D_{2k} jsou nezávisle identicky rozložené s p, tedy rozdělení C_k je z lemmatu 3 I dáno konvolucí $p_{C_k} = p_{D_{2k+1}} * p_{D_{2k}} = p * p = p^{*2}$, tedy C_k, $k \in \mathbb{N}_0$ jsou identicky nezávisle rozložené s pravděpodobností p^{*2}. Pro (Y_k) dostáváme $Y_0 = X_0 = e$ a pro $k \in \mathbb{N}_0$ platí $Y_{k+1} = X_{2k+2} = D_{2k+1}X_{2k+1} = D_{2k+1}D_{2k}X_{2k} = C_kY_k$. Tedy (Y_k) je náhodná procházka na G generovaná p^{*2}. p^{*2} má tvar $p^{*2}(0) = 1/2$, $p^{*2}(-2) = p^{*2}(2) = 1/4$.

Definujme homomorfizmus z $\alpha : H \to G$ předpisem $\alpha(k) = 2k$. Jelikož n je liché, snadno se ukáže, že $\ker \alpha = 0$ a tedy α je prosté. Jelikož G i H mají stejný a konečný počet prvků, jde o izomorfismus. Všimneme si, že prvky $0 \leq k \leq n/2$ (v první polovině) se prvky H zobrazují na sudé prvky G, a prvky $n/2 \leq k \leq n$ (v druhé polovině) se zobrazují na liché prvky G.

Nyní použijeme lemma 4 II a pomocí izomorfizmu α^{-1} přejdeme od (Y_k) k náhodné procházce $Z_k := \alpha^{-1}Y_k$, $k \in \mathbb{N}_0$ na H generované rozdělením $q = \alpha^{-1}(p)$, $q(0) = 1/2$, $q(-1) = q(1) = 1/4$. q je ale symetrické ostře unimodální. Z cvičení 9 indukcí plyne, že $p_{Z_k} = q^{*k}$ je symetrické ostře unimodální pro každé $k \in \mathbb{N}_0$. Jelikož $Y_k = \alpha(Z_k)$, $k \in \mathbb{N}_0$ platí (opět z lemmatu 4 II) $p^{*2k} = p_{Y_k} = \bar{\alpha}(p_{Z_k}) = \bar{\alpha}(q^{*k})$, což dává tvrzení o maximu pravděpodobnosti v 0 po sudém počtu kroků a tvrzení o monotonii $p^{*2k}(2j) \geq p^{*2k}(2j + 2i)$, kde $0 \leq 2j \leq 2j + 2i \leq n$, případně $p^{*2k}(2j+1) \leq p^{*2k}(2j+1+2i)$, kde $0 \leq 2j+1 \leq 2j+1+2i \leq n$ (což je trochu něco jiného než v zadání). □

Cvičení 11 se týká náhodné procházky na $\mathbb{Z}_q$ s náhodným multiplikátorem definované ([1], kap.3C example 3, str.30) jako proces $(X_k), k \in \mathbb{N}_0$ s $\mathrm{rng}(X_k) \in \mathbb{Z}_q$, kde $X_0 = 0$, $X_n = 2X_{n-1} + \epsilon_n$ a ϵ_n jsou identicky nezávisle rozložené s pravděpodobností $P(\epsilon_n = 0) = P(\epsilon_n = -1) = P(\epsilon_n = 1) = 1/3$. Dále pak "vzdálenosti" dvou pravděpodobností p, p' na cyklické grupě $\mathbb{Z}_q$ definované

$$D(p, p') := \sup_J |p(J) - p'(J)|$$

kde supremum jde přes všechny intervaly na $\mathbb{Z}_q$ (interval na $\mathbb{Z}_q$ je definován v definici 8). Pro tuto vzdálenost byl uveden následující horní odhad

Lemma 16. *([1], kap.3C, str.33)*

$$D(p,p') \leq \frac{1}{\sqrt{2}} \sum_{j=1}^{q-1} \frac{|\hat{p}(\rho_j) - \hat{p'}(\rho_j)|}{j^*},$$

kde $j^* := \min(j, q-j)$*, kde* ρ_j *jsou ireducibilní reprezentace z lemmatu 9.*

Cvičení 11. ([1], kap.3C, exercise 11, str.34) Buďte $p_n, n \in \mathbb{N}_0$ pravděpodobnosti na $\mathbb{Z}_q$, q liché, definované $p_n := p_{X_n}$ ($p_n(j) = P(\{X_n = j\}, j \in Z_q)$, kde X_n je proces náhodné procházky s náhodným multiplikátorem definovaný výše ([1], kap.3C example 3, str.30). S použitím lemmatu 16 ukažte, že existují konstanty a, b tak, že pro každé q liché

$$D(p_n, U) \leq a\mathrm{e}^{-bn/\ln q}.$$

Podařilo se mi ukázat následující.

Lemma 17.

$$D(p_n, U) \leq 2^{\frac{3}{2}} t \mathrm{e}^{-\lfloor \frac{n}{t} \rfloor \ln 3},$$

pro q *tvaru* $q = 2^t - 1$*,* $t \in \mathbb{N}$*, kde* $\lfloor a \rfloor$ *označuje dolní celou část* $a \in \mathbb{R}$*.*

To je o něco horší s ohledem na $\log_2(q) \doteq t$ před exponenciálou a omezení na q. Důkaz je v podstatě upravená verze důkazu Věty 4 z [1], kap.3C, str.30.

Důkaz: Abychom mohli použít odhadu z lemmatu 16, je potřeba nejprve určit Fourierovy obrazy $\hat{p}_n(\rho_j)$ a $\hat{U}(\rho_j)$ ($0 \leq j < q$ indexuje ireducibilní reprezentace $\rho_j(k) = \exp(-\jmath 2\pi jk/q)$). Z lemmatu 8 VI víme, že $\hat{U}$ je nulové na netriviálních reprezentacích $\hat{U}(j) = 0$, pro $0 < j$ (s ohledem na tvar dolní meze nás zajímají pouze netriviální ireducibilní reprezentace). Dále rozepíšeme rekurzi pro $X_n = 2^{n-1}\epsilon_1 + \ldots + 2\epsilon_{n-1} + \epsilon_n$. Nejprve stanovíme obraz libovolného členu v součtu. Zřejmě

$$p_{2^a\epsilon_l}(-2^a) = p_{2^a\epsilon_l}(0) = p_{2^a\epsilon_l}(2^a) = 1/3.$$

Tedy

$$\hat{p}_{2^a\epsilon_l}(\rho_j) = \sum_{k=0}^{q-1} p_{2^a\epsilon_l}(k)\rho_j(k) = \frac{1}{3} + \frac{2}{3}\cos\frac{2\pi 2^a j}{q}.$$

Protože součet nezávislých náhodných veličin vede na konvoluci příslušných pravděpodobností na grupě (viz. lemma 3 I) a konvoluce přejde ve Fourierově transformaci na součin obrazů (viz. lemma 8 I), dostáváme

$$\hat{p}_n(\rho_j) = \prod_{a=0}^{n-1}(\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi 2^a j}{q})).$$

Protože budeme potřebovat odhadnout $|\hat{p}_n(\rho_j)|$, bude se nám hodit odhad

$$|\frac{1}{3}+\frac{2}{3}\cos(2\pi x)| \le h(x) := \begin{cases} \frac{1}{3} \text{ pro } x \in [\frac{1}{4},\frac{3}{4}), \\ 1 \text{ jinak.} \end{cases}$$

Máme tedy

$$|\hat{p}_n(\rho_j)| \le \prod_{a=0}^{n-1} h(\{\frac{2^a j}{q}\}),$$

kde $\{x\}$ označuje zlomkovou část x ($\{x\} = x - \lfloor x \rfloor$, kde $\lfloor x \rfloor$ označuje dolní celou část x). Buď $\{x\} = .\alpha_1\alpha_2\alpha_3\ldots$ binární rozvoj zlomkové části x, pak

$$h(x) = \begin{cases} \frac{1}{3} \text{ pro } \alpha_1 \neq \alpha_2, \\ 1 \text{ pro } \alpha_1 = \alpha_2. \end{cases}$$

Nechť $A(x,n)$ označuje počet alternací v prvních n binárních číslicích x (váhy 2^{-1} až 2^{-n}) $A(x,n) := |\{1 \le i < n : \alpha_i \neq \alpha_{i+1}\}|$. Dostáváme

$$\prod_{a=0}^{n-1} h(\{\frac{2^a j}{q}\}) \le 3^{-A(\frac{j}{q},n)}.$$

Pro q tvaru $q = 2^t - 1$ se binární rozvoj j/q periodicky opakuje s periodou t. Definujme $r = \lfloor n/t \rfloor$, pak platí $n \ge rt$, $A(j/q,n) \ge rA(j/q,t)$. Použijeme horní mez z lemmatu 16 dosadíme za Fourierovy obrazy a použijeme uvedené odhady

$$\begin{aligned} D(p_n,U) &\le \frac{1}{\sqrt{2}}\sum_{j=1}^{q-1}\frac{|\hat{p}_n(\rho_j)-\hat{U}(\rho_j)|}{j^*} = \frac{1}{\sqrt{2}}\sum_{j=1}^{q-1}\frac{|\hat{p}_n(\rho_j)|}{j^*} \le \\ &\le \frac{1}{\sqrt{2}}\sum_{j=1}^{q-1}\frac{\prod_{a=0}^{n-1}h(\{\frac{2^a j}{q}\})}{j^*} \le \frac{1}{\sqrt{2}}\sum_{j=1}^{q-1}\frac{3^{-A(\frac{j}{q},n)}}{j^*} \le \frac{1}{\sqrt{2}}\sum_{j=1}^{q-1}3^{-A(\frac{j}{q},n)} \le \\ &\le \sqrt{2}\sum_{k=1}^{t}\binom{t}{k}3^{-kr} = \sqrt{2}((1+3^{-r})^t - 1) \le \sqrt{2}(\mathrm{e}^{3^{-r}t}-1), \end{aligned}$$

kde v posledních krocích bylo použito $j^* \ge 1$, $|\{j; A(j/q,t) = k\}| \le 2\binom{t}{k}$ a $1 + x \le \exp(x)$. Abychom dostali odhad v požadovaném tvaru (exponenciála), použijeme odhad $\exp(x) - 1 \le cx$, kde $0 \le x \le x_0$ a $c \ge c_0 := (\exp(x_0)-1)/x_0$ (exponenciála je konvexní, tak ji na intervalu $[0,x_0]$ odhadneme shora sečnou), kde v našem případě $x = 3^{-r}t$. Podíváme se, pro jaká r (případně n) lze odhad použít, tedy kdy $x_0 \ge x = 3^{-r}t$. To nastává pro $r \ge (\ln t - \ln x_0)/\ln 3 =: r_0$ (tedy pro $n \ge \lceil r_0 \rceil t$) [1]. Např pro $x_0 := 1$ dostáváme $c_0 = \mathrm{e} - 1 < 2 =: c$ a $r_0 = \ln t/\ln 3$. Odhad pak vypadá

$$D(p_n,U) \le \sqrt{2}(\mathrm{e}^{3^{-r}t}-1) \le \sqrt{2}23^{-r}t = 2^{\frac{3}{2}}t\mathrm{e}^{-r\ln 3} = 2^{\frac{3}{2}}t\mathrm{e}^{-\lfloor\frac{n}{t}\rfloor\ln 3},$$

[1] Symbolem $\lceil a \rceil$ označuji horní celou část $a \in \mathbb{R}$

což je klesající funkce v r (rovněž v n). Posledním výrazem v r lze rovněž definovat funkci v reálné proměnné r, která je rozšířením původní funkce v $r \in \mathbb{N}_0$. Toto rozšíření je rovněž klesající a jeho hodnota v $r = r_0$ je $2^{\frac{3}{2}} \geq 1$. Jelikož variační vzdálenost je shora omezená jedničkou, a protože

$$\|p - p'\| = \sup_{M \subset \mathbb{Z}_q} |p(M) - p'(M)| \geq \sup_{J \text{ interval v } \mathbb{Z}_q} |p(J) - p'(J)| = D(p, p')$$

dostáváme, že $D(p_n, U)$ je rovněž omezená jednotkou. Takže omezení na $r \geq r_0$ případně na $n \geq \lceil r_0 \rceil t$ je zbytečné. □

Odhad exponenciály sečnou se může zdát dosti hrubý, avšak pro $n \to \infty$ a tedy $x \to 0+$ je tento odhad pouze c-krát větší (bylo použito $c = 2$), jak plyne z

$$\lim_{x \to 0+} \frac{cx}{\mathrm{e}^x - 1} = c.$$

Konstantu c (spolu s x_0) je možné volit menší (lepší horní mez), pak se ale samozřejmě zvýší n_0. Odhad $1 < j^*$ se zdá rovněž dosti hrubý. Problém je, jak možná j omezit pomocí počtu alternací k. Podařilo se mi ukázat, že je-li u $\{j/q\}$ počet alternací k platí

$$j^* \geq \frac{2^{k+1} - 1}{3}.$$

Například chceme-li j omezit zdola pro lichý počet alternací k v prvních t místech binárního rozvoje $\{j/q\}$, nejmenšímu možnému j odpovídá zmíněný binární rozvoj tvaru 00000101 (pouze příklad pro $t = 8$, $k = 3$). Jedničky v rozvoji mají váhu $2^{k-1-t}, 2^{k-3-t}, \ldots, 2^{-t}$ součet dává zmíněnou mez, podobně se provede omezení shora a pro sudé počty alternací k. Ale použitím tohoto odhadu se mi nepodařilo nějak výrazně horní mez zlepšit.

2.3 Náhodná procházka na afinní grupě A_q

Cvičení 13. (Náhodná procházka na afinní grupě A_q, [1], kap.3C, example 4, str.34) Buď q prvočíslo. Náhodná čísla jsou často generována rekurzivním schématem $X_k = aX_{k-1} + b(\mod q)$. Tato posloupnost cvičení umožňuje odhadnout rychlost konvergence, když a i b jsou náhodné. Transformace $x \mapsto ax + b$ s $a \neq 0(\mod q)$ označíme $T_{a,b}(x)$. Množina takových transformací tvoří konečnou grupu A_q. Označme (a, b) prvek A_q odpovídající $T_{a,b}$. Součin je $(a, b)(c, d) = (ac, ad + b)$, identita je $(1, 0)$ a $(a, b)^{-1} = (a^{-1}, -ba^{-1})$. Tato grupa má $q(q - 1)$ prvků. Podgrupy $\{(1, b)\} \cong \mathbb{Z}_q$ a $\{(a, 0)\} \cong \mathbb{Z}_q^*$ jsou užitečné.

(1) Nalezněte q různých tříd konjugace. Vysvětlete, proč míry konstantní na třídách konjugace nejsou příliš zajímavé.

(2) Z části (1) existuje q různých (neekvivalentních) ireducibilních reprezentací; $q-1$ z nich je jednodimenzionálních daných volbou charakteru χ_i podgrupy $\mathbb{Z}_q^*$ a definováním $\rho_i(a, b) = \chi_i(a)$. Ukažte, že jsou to neekvivalentní ireducibilní

reprezentace. Ukažte, že je zde ještě jedna ireducibilní reprezentace ρ dimenze $q-1$. Použijte [2], kap.2 exercise 2.6, str.17 ke konstrukci této reprezentace s uvážením akce A_q na $\mathbb{Z}_q$. Explicitní volbou báze ukažte, že

$$\begin{aligned}\chi_\rho(1,0) &= q-1\\ \chi_\rho(1,b) &= -1 \qquad ,b\neq 0,\\ \chi_\rho(a,b) &= 0 \qquad\quad ,a\neq 1.\end{aligned}$$

(3) Nechť ρ^+ resp. ρ^* jsou restrikce ρ z části (2) na $\mathbb{Z}_q$ resp. $\mathbb{Z}_q^*$. Použitím charakteru ρ a skalárního součinu ukažte, že ρ^* je regulární reprezentace $\mathbb{Z}_q^*$ a ρ^+ obsahuje všechny netriviální ireducibilní reprezentace $\mathbb{Z}_q$ právě jednou.

(4) Nechť p^+ je pravděpodobnost na $\mathbb{Z}_q$ a p^* je pravděpodobnost na $\mathbb{Z}_q^*$. Nechť χ_i^+ a χ_i^* jsou charaktery $\mathbb{Z}_q$ a $\mathbb{Z}_q^*$. Nechť $p(a,b)=p^*(a)\cdot p^+(b)$. Ukažte

- **(a)** $\hat{p}(\rho)=\hat{p}^+(\rho^+)\hat{p}^*(\rho^*)$.
- **(b)** Vlastní čísla matice $\hat{p}^*(\rho^*)$ je $q-1$ čísel $\hat{p}^*(\chi_i^*)$, vlastní čísla $\hat{p}^+(\rho^+)$ je $q-1$ čísel $\hat{p}^+(\chi_i^+)$, pro χ_i^+ netriviální.

(5) Nechť q je liché prvočíslo takové, že 2 je generátor $\mathbb{Z}_q^*$. Uvažujte náhodnou procházku na A_q, začínající v 0 a je založena na p^* a p^+, kde $p^*(1)=p^*(2)=p^*((q+1)/2)=\frac{1}{3}$ a $p^+(0)=p^+(1)=p^+(-1)=\frac{1}{3}$. Ukažte, že $k=c(q)q^2\log q$, kde $c(q)\to\infty$, pro $q\to\infty$ je dostačující pro konvergenci k rovnoměrnému rozdělení. Užijte tohoto výsledku k argumentaci, že $T_{X_k}(0)$ se blíží rovnoměrnému rozdělení na $\mathbb{Z}_q$ pro uvedený počet kroků. Jeden možný postup využívá následujícího faktu. Nechť $\tau(A)$ je spektrální poloměr matice A. Nechť A,B jsou diagonalizovatelné matice, pak $\tau(AB)\leq\tau(A)\tau(B)$.

(6) Ukažte uvažujíce pouze první souřadnici (a,b) že $k=cq^2$ kroků není dostačující pro fixní c.

Poznámka 8. Zadání opět trochu upřesním, X_0 neuvažuji libovolné, ale fixuji $X_0=0$. Pravděpodobnost výběru invertibilní afinní transformace považuji za konstantní v k.

Důkaz: Jenom shrneme že A_q, kde q je prvočíslo, je grupa prvků tvaru (a,b), kde $a\in\mathbb{Z}_q^* \iff a\in\{1,\dots,q-1\}$ a $b\in\mathbb{Z}_q$. Prvky (a,b) grupy je možné ztotožnit s invertibilními afinními transformacemi $T_{a,b}$ na $\mathbb{Z}_q$ s operací skládání, odpovídající grupová operace, tvar inverzního prvku a jednotkového prvku byl popsán v zadání.

(1) Zvolme libovolný prvek $(c,d)\in A_q$ a proveďme konjugaci nějakým prvkem $(a,b)\in A_q$. Výsledek je $(a,b)(c,d)(a,b)^{-1}=(ac,ad+b)(a^{-1},-ba^{-1})=(aca^{-1},-bc+ad+b)=(aca^{-1},-bc+ad+b)=(c,b(1-c)+ad)$, definujme-li $h:=b(1-c)+ad$, pak platí

$$(a,b)(c,d)(a,b)^{-1}=(c,h),\quad h=b(1-c)+ad.$$

Vidíme, že prvá složka (c,d) zůstává konjugací vždy zachována, tedy prvky s různými prvými složkami budou ležet v různých třídách konjugace, otázka je, zda ekvivalence

podle prvé složky dává třídy konjugace. Mějme $(c,d) \in A_q$ a $h \in \mathbb{Z}_q$ libovolné a ověřme, zda (c,d) a (c,h) jsou ve vztahu konjugace, tedy zda existuje $(a,b) \in A_q$ tak, že platí $h = b(1-c) + ad$. Omezme se nejprve na $c \neq 1$, pak stačí volit $a := 1$ a dostáváme řešení $b = (h-d)(1-c)^{-1}$ ($(1-c)$ je invertibilní). V případě $c = 1$ dostáváme jednoprvkovou třídu konjugace odpovídající jednotkovému prvku $(1,0)$ a pro $d \neq 0$ stačí položit $a = hd^{-1}$ (b lze volit libovolně). Dostáváme tedy q tříd konjugace. Pro $c \in \mathbb{Z}_q^* \setminus \{1\}$ dostáváme $q-2$ tříd tvaru $\{(c,d); d \in \mathbb{Z}_q\}$. Pro $c = 1$ dostáváme dvě třídy, jednak třídu odpovídající jednotkovému prvku $\{(1,0)\}$ a jednak třídu $\{(1,d); d \in \mathbb{Z}_q \setminus \{0\}\}$.

Označme (X_k) proces s $\mathrm{rng}(X_k) \in \mathbb{Z}_q$ popsaný v zadání jako rekurzivní schéma pro generování náhodných čísel $X_{k+1} = a_k X_k + b_k$ pro $k \in \mathbb{N}_0$, $X_0 = 0$. Invertibilní afinní transformaci T_{a_k,b_k} ztotožníme s prvkem $T_k := (a_k, b_k) \in A_q$, $X_{k+1} = T_{a_k,b_k} X_k = T_k X_k$. Pravděpodobnost výběru invertibilní afinní transformace je konstantní v k a odpovídá nějaké pravděpodobnosti $p = p_{T_k}$ na A_q. Označme $(Y_k) = (A_k, B_k)$ náhodnou procházku na A_q s procesem přírůstku (T_k). $Y_{k+1} = T_k Y_k, Y_0 = (1,0)$. Ta je generována pravděpodobností p, což dává $p_{Y_k} = p^{*k}$. Platí

$$X_{k+1} = T_k X_k = Y_k X_0 = Y_k 0.$$

Tedy pro každé $l \in \mathbb{Z}_q$ platí

$$\begin{aligned} p_{X_{k+1}}(l) &= P(X_{k+1} = l) = \\ &= P(Y_k 0 = l) = P(A_k 0 + B_k = l) = p_{B_k}(l) = \sum_{a \in \mathbb{Z}_q^*} p_{Y_k}(a,l) = \sum_{a \in \mathbb{Z}_q^*} p^{*k}(a,l). \end{aligned}$$

Nechť je p třídová funkce (konstantní na třídách konjugace). Jelikož konvoluce třídových funkcí je opět třídová funkce (viz. lemma 8 IV) je p^{*k} opět třídová funkce (indukcí). Označme c_a,$a \in \mathbb{Z}_q^*$ resp. $c_{(1,0)}$ konstanty, takové, že

$$\begin{aligned} p^{*k}(a,b) &= c_a, \quad \text{pro } a \in \mathbb{Z}_q^*, a \neq 0, b \in \mathbb{Z}_q, \\ p^{*k}(1,b) &= c_1, \quad \text{pro } b \in \mathbb{Z}_q, b \neq 0, \\ p^{*k}(1,0) &= c_{(1,0)} + c_1. \end{aligned}$$

Ze vztahu pro $p_{X_{k+1}}$ pak plyne

$$p_{X_{k+1}}(b) = \sum_{a \in \mathbb{Z}_q^*} p^{*k}(a,b) = c_{(1,0)}\delta(b) + \sum_{a \in \mathbb{Z}_q^*} c_a,$$

že $p_{X_{k+1}}$ má tvar lineární kombinace δ a rovnoměrného rozdělení, v čase se mohou měnit pouze koeficienty této lineární kombinace.

V případě, že $c_{(1,0)} = 0$ dostáváme pouze rovnoměrné rozdělení. Není těžké ukázat, že má-li p $c_{(1,0)}$ nulové platí to i pro p^{*k}, tedy že p_{X_k} je stále rovnoměrné. Abychom to ukázali, definujme $\delta_{a_0}(a,b) = 1$ pro $a = a_0$, $\delta_{a_0}(a,b) = 0$ jinak. Předpokládáme, že p má tvar lineární kombinace δ_{a_0}, $a_0 \in \mathbb{Z}_q^*$, máme ukázat, že p^{*k} je rovněž taková. Postupujeme indukcí podle k. Pro $k = 0$ tvrzení platí. V indukčním kroku stačí z bilinearity konvoluce ukázat, že

$$\delta_{a_0} * \delta_{a_1} = \delta_{a_0 a_1},$$

což lze rozepsáním $\delta_a = \sum_{b\in\mathbb{Z}_q} \delta_{(a,b)}$ a použitím $\delta_{(a,b)}\delta_{(a',b')} = \delta_{(a,b)(a',b')} = \delta_{(aa',ab'+b)}$. Zřejmě proces (X_k), kde rozdělení p_{X_k} v prvém kroku přejde na rovnoměrné a dále se nemění, není příliš zajímavý. Případ obecnější třídovou funkcí p, $c_{(1,0)} \neq 0$ jsou p_{X_k} trochu bohatší, ale jak bylo popsáno ne o moc.

(2) Definujme zobrazení $\varphi : A_q \to \mathbb{Z}_q^*$ předpisem $\varphi : (a,b) \mapsto a$. Ověříme, že jde o homomorfizmus $\varphi((a,b)(c,d)) = \varphi((ac, ad+b)) = ac = \varphi((a,b))\varphi((c,d))$. Víme, že $\mathbb{Z}_q^*$ je $q-1$ prvková cyklická grupa vzhledem k násobení. Označme g nějaký její generátor pak $\mathbb{Z}_q^* = \{g^k; k = 0,\ldots,q-2\}$. Některé reprezentace A_q tedy obdržíme složením φ se známými reprezentacemi cyklické grupy $\mathbb{Z}_q^*$, výsledné reprezentace označíme $\rho_m((g^k,b)) = \exp(\jmath 2\pi mk/(q-1))$, $m,k \in \{0,\ldots,q-2\}$. Jedná se zřejmě o $q-1$ neekvivalentních (různé charaktery), ireducibilních (jsou jednodimenzionální) reprezentací. Víme, že počet ireducibilních reprezentací je roven počtu tříd konjugace a ten je q z bodu (1). Zbývá tedy najít poslední ireducibilní reprezentaci ρ, její dimenzi lze určit z vlastností regulární reprezentace, neboť platí (viz. lemma 7 IV(b))

$$q(q-1) = |A_q| = \sum_{\mu \text{ ired. rep. } A_q} d_\mu^2,$$

kde d_μ označuje dimenzi ireducibilní reprezentace μ. Pro dimenzi ρ tedy dostáváme $d_\rho^2 = q(q-1) - (q-1)1^2 = (q-1)^2$, tedy $d_\rho = (q-1)$. Jak je naznačeno v zadání, ke konstrukci ρ stačí uvažovat definující permutační reprezentaci A_q (akci A_q na $\mathbb{Z}_q$). Uvažujme tedy q dimenzionální vektorový prostor $V = \mathbf{C}^q$ aritmetických vektorů. Prvku $k \in \mathbb{Z}_q$ nechť odpovídá prvek standardní báze e_k. Prvku $(a,b) \in A_q$ pak odpovídá invertibilní homomorfizmus na V, který má v popsané bázi $e_0,\ldots,e_{q-1}$ permutační matici - budeme pracovat s maticovou reprezentací. Označme tuto reprezentaci $\mu : A_q \to \mathrm{GL}_q$. Víme, že charakter je třídová funkce (je konstantní na třídě konjugace), dále u permutační reprezentace je charakter dán počtem pevných bodů. K určení charakteru prvku $(a,b) \in A_q$ stačí stanovit počet řešení $x = T_{a,b}(x) = ax+b$, $x \in \mathbb{Z}_q$. Pro jednotkový prvek $(1,0)$ jsou všechna x řešením, tedy $\chi_\mu(a,b) = q$. Pro $(1,b)$, $b \neq 0$ neexistuje žádné řešení $\chi_\mu(1,b) = 0$ a konečně pro (a,b), $a \in \mathbb{Z}_q^* \setminus \{1\}$ dostáváme právě jedno řešení $x = b(1-a)^{-1}$, tedy $\chi_\mu(a,b) = 1$. Dále permutační reprezentace vždy obsahuje triviální reprezentaci $\mu_t : G \to V_t := \langle e_0 + \ldots + e_{q-1}\rangle \leq V$, která vznikne restrikcí zobrazení $\mu(a,b) : V \to V$ na jednodimenzionální podprostor V_t ($\langle A\rangle$ značí lineární obal množiny A). Protože standardní skalární součin na V je invariantní vůči akci μ grupy A_q ($\mu(a,b)$ permutují pouze složky vektorů z V -platí pro každou permutační reprezentaci), je podle lemmatu 5 zobrazení $\rho : G \to V_t^\perp$, kde $V_t^\perp$ je ortogonální doplněk k V_t a $\rho(a,b) := \mu(a,b)|V_t^\perp$ ($(a,b) \in A_q$), podreprezentací μ. To, že ρ je hledaná ireducibilní reprezentace, je třeba teprve ověřit. Předně dimenze $d_\rho = d_\mu - d_{\mu_t} = q-1$ souhlasí. Pro charakter ρ platí $\chi_\mu = \chi_\rho + \chi_t$ (charakter direktního součtu reprezentací), dostáváme

$$\begin{aligned}
&\chi_\rho(1,0) = q-1,\\
&\chi_\rho(1,b) = -1, \text{ pro } b \in \mathbb{Z}_q \setminus \{0\},\\
&\chi_\rho(a,b) = 0, \text{ pro } a \in \mathbb{Z}_q^* \setminus \{1\}, b \in \mathbb{Z}_q.
\end{aligned}$$

Ireducibilitu ověříme pomocí skalárního součinu

$$(\chi_\rho|\chi_\rho) = \frac{1}{|A_q|}\sum_{(a,b)\in A_q}|\chi_\rho(a,b)|^2 =$$

$$= \frac{1}{q(q-1)}(1\times(q-1)^2+(q-1)\times(-1)^2+(q-2)q\times 0^2) = \frac{(q-1)^2+(q-1)}{q(q-1)} = 1.$$

Tedy ρ je zbývající $q-1$ dimenzionální ireducibilní reprezentace.

(3) Grupa $\mathbb{Z}_q$ je vnořena do A_q prostřednictvím monomorfizmu $b\mapsto(1,b)$, dále grupa $\mathbb{Z}_q^*$ je vnořena do A_q prostřednictvím monomorfizmu $a\mapsto(a,0)$. Dále ztotožníme $\mathbb{Z}_q$ a $\mathbb{Z}_q^*$ s jejich obrazy v popsaných vnořeních $\mathbb{Z}_q = \{(1,b); b\in\mathbb{Z}_q\}\leq A_q$, $\mathbb{Z}_q^* = \{(a,0); a\in\mathbb{Z}_q^*\}\leq A_q$. Označme $\rho^+ := \rho|\mathbb{Z}_q$ a $\rho^* := \rho|\mathbb{Z}_q^*$ restrikce ρ na příslušné podgrupy. Víme, že reprezentace jsou ekvivalentní právě tehdy, když mají stejné charaktery (viz. lemma 7 II). Dále víme, že regulární reprezentace $\mathbb{Z}_q^*$, označme ji α, má charakter $\chi_\alpha(1) = q-1$, pro $\chi_\alpha(a) = 0$ pro $a\neq 1$. Stačí tedy ukázat, že ρ^* má stejný charakter. Z vypočtených charakterů pro ρ v bodě (2) dostáváme $\chi_{\rho^*}(1,0) = \chi_\rho(1,0) = q-1$ a $\chi_{\rho^*}(a,0) = \chi_\rho(a,0) = 0$ pro $a\neq 1$. Tedy ρ^* je ekvivalentní s regulární reprezentací $\mathbb{Z}_q^*$.

Označme $\alpha_m(b) = \exp(\jmath 2\pi mb/q)$, $m,b\in\mathbb{Z}_q, m$ ireducibilní reprezentace $\mathbb{Z}_q$. Abychom ukázali, že ρ^+ obsahuje každou ireducibilní netriviální reprezentaci $\mathbb{Z}_q$ právě jednou, stačí z lemmatu 7 I ukázat, že $(\chi_{\rho^+}|\chi_{\alpha_m}) = 1$ pro $m\neq 0$

$$(\chi_{\rho^+}|\chi_{\alpha_m}) = \frac{1}{|\mathbb{Z}_q|}\sum_{b=0}^{q-1}\chi_{\rho^+}(1,b)\overline{\chi_{\alpha_m}(b)} = \frac{1}{q}(\chi_\rho(1,0)\overline{\chi_{\alpha_m}(0)} + \sum_{b=1}^{q-1}\chi_\rho(1,b)\overline{\chi_{\alpha_m}(b)}) =$$

$$= \frac{1}{q}((q-1) - \sum_{b=1}^{q-1}\mathrm{e}^{-\jmath\frac{2\pi}{q}mb}) = \frac{1}{q}((q-1) - (\frac{1-\mathrm{e}^{-\jmath\frac{2\pi}{q}mq}}{1-\mathrm{e}^{-\jmath\frac{2\pi}{q}m}} - 1)) = 1.$$

(4) Nechť p^+ je pravděpodobnost na $\mathbb{Z}_q$ a p^* pravděpodobnost p^+ na $\mathbb{Z}_q^*$, pak $p(a,b) := p^*(a)p^+(b)$ je pravděpodobnost na A_q.

(a) Pro libovolný prvek $(a,b)\in A_q$ platí $(a,b) = (1,b)(a,0)$, kde zřejmě $(1,b)\in\mathbb{Z}_q$, $(a,0)\in\mathbb{Z}_q^*$. Vyjádříme $\hat{p}(\rho)$ a použijeme uvedenou vlastnost

$$\hat{p}(\rho) = \sum_{a\in\mathbb{Z}_q^*, b\in\mathbb{Z}_q} p(a,b)\rho((a,b)) =$$

$$= \sum_{a\in\mathbb{Z}_q^*, b\in\mathbb{Z}_q} p^*(a)p^+(b)\rho((1,b)(a,0)) = \sum_{a\in\mathbb{Z}_q^*, b\in\mathbb{Z}_q} p^*(a)p^+(b)\rho((1,b))\rho((a,0)) =$$

$$= \sum_{a\in\mathbb{Z}_q^*, b\in\mathbb{Z}_q} p^*(a)p^+(b)\rho^+((1,b))\rho^*((a,0)) = \hat{p}^+(\rho^+)\hat{p}^*(\rho^*).$$

(b) V bodě (3) jsme ukázali, že ρ^* je ekvivalentní regulární reprezentaci $\mathbb{Z}_q^*$ a tedy obsahuje právě všechny ireducibilní reprezentace cyklické $q-1$ prvkové grupy $\mathbb{Z}_q^*$. Označme tyto reprezentace $\rho_m(g^k) = \exp(\jmath 2\pi mk/q)$, $m,k\in\mathbb{Z}_{q-1}$ (g opět značí generátor $\mathbb{Z}_q^*$). Tedy uvažujeme-li příslušné maticové reprezentace, existuje regulární matice R rozměru $(q-1)\times(q-1)$ tak, že platí $R\rho^*(a,0)R^{-1} = \mathrm{diag}(\rho_0(a),\ldots,\rho_{q-2}(a)) =:$

$\rho'(a)$. Vlastní čísla se podobnostní transformací nemění, stačí tedy stanovit vlastní čísla $R\hat{p}^*(\rho^*)R^{-1}$

$$R\hat{p}^*(\rho^*)R^{-1} = \sum_{a\in\mathbb{Z}_q^*} p^*(a)R\rho^*(a,0))R^{-1} = \sum_{a\in\mathbb{Z}_q^*} p^*(a)\rho'(a) =$$
$$= \mathrm{diag}(\sum_{a\in\mathbb{Z}_q^*} p^*(a)\rho_0(a), \ldots, \sum_{a\in\mathbb{Z}_q^*} p^*(a)\rho_{q-2}(a)) = \mathrm{diag}(\hat{p}^*(\rho_0), \ldots, \hat{p}^*(\rho_{q-2})).$$

vlastní čísla $\hat{p}^*(\rho^*)$ jsou tedy $\hat{p}^*(\rho_0), \ldots, \hat{p}^*(\rho_{q-2})$. Protože ρ^+ obsahuje pro změnu všechny netriviální ireducibilní reprezentace $\mathbb{Z}_q$ označme je $\mu_m^+(b) = \exp(\jmath mb2\pi/q)$, $m, b \in \mathbb{Z}_q, m \neq 0$, obdobným způsobem dostaneme, že vlastní čísla $\hat{p}^+(\rho^+)$ jsou právě $\hat{p}^+(\mu_1^+), \ldots, \hat{p}^+(\mu_{q-1}^+)$.

(5) Nechť q je liché prvočíslo takové, že 2 je generátor $\mathbb{Z}_q^*$. Uvažujeme náhodnou procházku na A_q generovanou pravděpodobností p, kde $p(a,b) = p^*(a)p^+(b)$, $(a,b) \in A_q$ s $p^*(1) = p^*(2) = p^*((q+1)/2) = 1/3$ a $p^+(0) = p^+(1) = p^+(-1) = 1/3$. Variační vzdálenost p^{*k} od rovnoměrného rozdělení odhadneme použitím lemmatu 11 o horní mezi (bez újmy na obecnosti viz. poznámka 1 předpokládáme ρ maticovou unitární)

$$\left\|p^{*k} - U\right\|^2 \leq \frac{1}{4}(\sum_{m=1}^{q-2} 1\mathrm{tr}(\hat{p}^k(\rho_m)(\hat{p}^k(\rho_m))^H) + (q-1)\mathrm{tr}(\hat{p}^k(\rho)(\hat{p}^k(\rho))^H)) \leq$$
$$\leq \frac{1}{4}(\sum_{m=1}^{q-2} |\hat{p}^k(\rho_m)|^2 + (q-1)(q-1)\tau(\hat{p}(\rho))^{2k}),$$

kde $\tau(A)$ značí spektrální poloměr A. Nejprve určíme $\hat{p}^k(\rho_m)$ (ze zadání víme, že 2 generuje $\mathbb{Z}_q^*$)

$$\hat{p}(\rho_m) = \sum_{l=0}^{q-2}\sum_{b\in\mathbb{Z}_q} p(2^l,b)\mathrm{e}^{\jmath\frac{2\pi}{q-1}ml} = \sum_{l=0}^{q-2}\sum_{b\in\mathbb{Z}_q} p^*(2^l)p^+(b)\mathrm{e}^{\jmath\frac{2\pi}{q-1}ml} =$$
$$= \sum_{l=0}^{q-2} p^*(2^l)\mathrm{e}^{\jmath\frac{2\pi}{q-1}ml} = \frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q-1}m).$$

Sumu v horní mezi odhadneme maximálním členem ($m = 1, m = q-2$)

$$\sum_{m=1}^{q-2} |\hat{p}^k(\rho_m)|^2 \leq (q-2)(\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q-1}))^{2k}.$$

Jak bylo napovězeno v zadání, pro spektrální normu $\tau(\hat{p}(\rho))$ s využitím (4a) platí

$$\tau(\hat{p}(\rho)) = \tau(\hat{p}^+(\rho^+)\hat{p}^*(\rho^*)) \leq \tau(\hat{p}^+(\rho^+))\tau(\hat{p}^*(\rho^*)).$$

Zbývá určit spektrální poloměry matic $\hat{p}^+(\rho^+)$ a $\hat{p}^*(\rho^*)$. Vlastní čísla těchto matic jsme již určili v (4b). Vlastní čísla $\hat{p}^+(\rho^+)$ mají tvar

$$\hat{p}^+(\mu_m^+) = \sum_{b=0}^{q-1} p^+(b)\mu_m^+(b) = \sum_{b=0}^{q-1} p^+(b)\mathrm{e}^{\jmath\frac{2\pi}{q}mb} = \frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q}m),$$

kde $m = 1, \ldots, q-1$, pro spektrální poloměr tedy platí

$$\tau(\hat{p}^+(\rho^+)) = \frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q}).$$

Vlastní čísla $\hat{p}^*(\rho^*)$ mají tvar $\hat{p}^*(\rho_0), \ldots, \hat{p}^*(\rho_{q-2})$,

$$\hat{p}^*(\rho_m) = \sum_{l=0}^{q-2} p^*(2^l)\mu_m^*(2^l) = \sum_{l=0}^{q-2} p^*(2^l)\mathrm{e}^{\jmath\frac{2\pi}{q-1}ml} = \frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q-1}m),$$

kde $m = 0, \ldots, q-2$. Pro spektrální poloměr dostáváme

$$\tau(\hat{p}^*(\rho^*)) = 1.$$

Dosadíme do odhadu variační vzdálenosti

$$\begin{aligned}\left\|p^{*k} - U\right\|^2 &\leq \frac{1}{4}(\sum_{m=1}^{q-2} |\hat{p}^k(\rho_m)|^2 + (q-1)^2\tau(\hat{p}(\rho))^{2k}) \leq \\ &\leq \frac{1}{4}((q-2)(\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q-1}))^{2k} + (q-1)^2(\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q}))^{2k}) \leq \\ &\leq \frac{1}{2}(q-1)^2(\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q}))^{2k}.\end{aligned}$$

Použijeme odhad $\cos x$ na intervalu $x \in [0,1]$ založený na Taylorově řadě $\sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$. Absolutní hodnoty členů klesají monotónně k 0 ($x \in [0,1]$) a členy střídají znaménko. Libovolný částečný součet ke kladnému členu lze tedy použít jako horní odhad součtu (řada konverguje na $\mathbb{R}$). Zde vezmeme částečný součet k $n = 2$ (Dá se ukázat, že tento odhad platí pro všechna $x \in \mathbb{R}$, zde ale vystačíme s uvedenou verzí.)

$$\cos x \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}, \;\; x \in [0,1].$$

Odhad použijeme pro $1 \geq x = 2\pi/q$. To dává omezení na $q \geq 7$. Odhad dosadíme do horní meze na variační vzdálenost

$$\begin{aligned}\left\|p^{*k} - U\right\|^2 &\leq \frac{1}{2}(q-1)^2(\frac{1}{3}+\frac{2}{3}\cos(\frac{2\pi}{q}))^{2k} \leq \frac{1}{2}(q-1)^2(\frac{1}{3}+\frac{2}{3}(1-\frac{(\frac{2\pi}{q})^2}{2}+\frac{(\frac{2\pi}{q})^4}{24}))^{2k} = \\ &= \frac{1}{2}(q-1)^2(1 - \frac{2\pi^2}{q^2} + \frac{2\pi^4}{3q^4}))^{2k} \leq \frac{1}{2}(q-1)^2\mathrm{e}^{(-\frac{2\pi^2}{q^2}+\frac{2\pi^4}{3q^4})2k} \leq \frac{1}{2}(q-1)^2\mathrm{e}^{-\frac{2k\pi^2}{q^2}},\end{aligned}$$

kde v posledních krocích byl použit odhad $1 + x \leq \exp(x)$ a $-2\pi^2/q^2 + 2\pi^4/(3q^4) \leq -\pi^2/q^2$ pro $q \geq 2\pi/\sqrt{3}$. Dosazením do výsledného odhadu variační vzdálenosti za $k = c(q)q^2 \ln q$, kde $c(q) \to \infty$ (viz. zadání) dostáváme $\left\|p^{*k} - U\right\| \to 0$ pro $q \to \infty$.

Zbývá ukázat, že pro zadaný počet kroků $k = c(q)q^2 \ln q$, $\|p_{X_k} - U\| \to 0$ pro $q \to \infty$. Jelikož máme podobný výsledek pro $\left\|p^{*k} - U\right\|$ stačí ukázat, že $\|p_{X_k} - U\| \leq$

$\left\|p^{*k} - U\right\|$. Použijeme identitu odvozenou v bodě (2) $p_{X_k} = \sum_{a\in\mathbb{Z}_q^*} p^{*k}(a,b)$, vztah rovnoměrných rozdělení $U(b) = 1/q$ na $\mathbb{Z}_q$ a $U(a,b) = 1/(q(q-1))$ na $\mathbb{A}_q$

$$U(b) = \sum_{a\in\mathbb{Z}_q^*} U(a,b)$$

a definujeme zobrazení θ, které podmnožině $M \subset \mathbb{Z}_q$ přiřadí podmnožinu $M' \subset A_q$ předpisem $M' = \theta(M) := \{(a,b) \in A_q; a \in M\}$. Pro variační vzdálenosti dostáváme požadované

$$\|p_{X_k} - U\| = \sup_{M\subset\mathbb{Z}_q} p_{X_k}(M) - U(M) = \sup_{M\subset\mathbb{Z}_q} \sum_{b\in M} p_{X_k}(b) - \sum_{b\in M} U(b) =$$

$$= \sup_{M\subset\mathbb{Z}_q} \sum_{b\in M}\sum_{a\in\mathbb{Z}_q^*} p^{*k}(a,b) - \sum_{b\in M}\sum_{a\in\mathbb{Z}_q^*} U(a,b) = \sup_{M'\subset\mathbb{A}_q, M'=\theta(M), M\subset\mathbb{Z}_q} p_{X_k}(M') - U(M') \leq$$

$$\leq \sup_{M'\subset\mathbb{A}_q} p_{X_k}(M') - U(M') = \left\|p^{*k} - U\right\|.$$

□

Nyní dokážeme lemma, které dává do vztahu variační vzdálenost $\|p_{X_k} - U\|$ náhodné procházky (X_k) a jejího homomorfního obrazu.

Lemma 18. *Buď (X_k) náhodná procházka na konečné grupě G a $\varphi : G \to H$ homomorfizmus na H. Pak (Z_k), $Z_k = \varphi(X_k)$ je náhodná procházka na H a platí*

$$\|p_{X_k} - U\| \geq \|p_{Z_k} - U\|.$$

Tedy variační vzdálenost v obrazu lze použít jako dolní odhad pro variační vzdálenost v předmětu (tímto způsobem použijeme uvedené lemma při důkazu bodu (6)) a naopak.

Důkaz: Důkaz je obdobou toho, co bylo provedeno na závěr důkazu bodu (5), tam však nešlo o homomorfní obraz. Z lemmatu 4 II víme, že (Z_k) je náhodná procházka na H a pro každé $h \in H$ platí

$$p_{Z_k}(h) = \sum_{g\in\varphi^{-1}(h)} p_{X_k}(g).$$

Pro rovnoměrná rozdělení na G a H platí

$$U(h) = \frac{1}{|H|} = \frac{|\ker\varphi|}{|G|} = \sum_{g\in\varphi^{-1}(h)} U(g)$$

pro každé $h \in H$, neboť $U(g) = 1/|G|$ a $|\varphi^{-1}(h)| = |\ker\varphi|$. Pro variační vzdálenosti dostáváme

$$\|p_{Z_k} - U\| = \sup_{M\subset H} p_{Z_k}(M) - U(M) = \sup_{M\subset H} \sum_{h\in M} p_{Z_k}(h) - \sum_{h\in M} U(h) =$$

$$= \sup_{M\subset H} \sum_{h\in M}\sum_{g\in\varphi^{-1}(h)} p_{X_k}(g) - \sum_{h\in M}\sum_{g\in\varphi^{-1}(h)} U(g) = \sup_{M\subset H} \sum_{g\in\varphi^{-1}(M)} p_{X_k}(g) - \sum_{g\in\varphi^{-1}(M)} U(g) =$$

$$= \sup_{M\subset H} p_{X_k}(\varphi^{-1}(M)) - U(\varphi^{-1}(M)) \leq \sup_{M'\subset G} p_{X_k}(M') - U(M') = \|p_{X_k} - U\|.$$

□

Důkaz: (6) Využijeme homomorfizmu definovaného v bodě (2) $\varphi : A_q \to \mathbb{Z}_q^*$, kde $\varphi : (a, b) \mapsto a$. Podle právě dokázaného lemmatu 18 je proces (Z_k) definovaný $Z_k = \varphi(X_k)$ náhodná procházka na $\mathbb{Z}_q^*$ a platí

$$\|p_{X_k} - U\| \geq \|p_{Z_k} - U\| .$$

Tedy abychom zdola odhadli $\|p_{X_k} - U\|$ stačí zdola odhadnou $\|p_{Z_k} - U\|$. Víme, že náhodná procházka Z_k je z lemmatu 4 II generována pravděpodobnosti

$$t(a) = \sum_{(a',b)\in\varphi^{-1}(a)} p(a', b) = \sum_{b\in\mathbb{Z}_q} p(a, b) = \sum_{b\in\mathbb{Z}_q} p^*(a)p^+(b) = p^*(a),$$

(časté použití konvoluce činí zápis s $p^*(a)$ nečitelný, proto jsem tuto pravděpodobnost přeznačil), a že 2 generuje $\mathbb{Z}_q^*$.

$$\|p_{Z_k} - U\| = \left\|t^{*k} - U\right\| = \sup_{f,|f|\leq 1} \mathrm{E}_{t^{*k}}(f) - \mathrm{E}_U(f) \geq \mathrm{E}_{t^{*k}}(f) - \mathrm{E}_U(f),$$

kde pro f v posledním výrazu platí $|f| \leq 1$ na $\mathbb{Z}_q^*$. Podobně jako v [1] zvolíme $f(2^l) := \cos(2\pi/(q-1)l)$, což dává $\mathrm{E}_U(f) = 0$ a dosadíme

$$\|p_{Z_k} - U\| \geq \mathrm{E}_{t^{*k}}(f) = \sum_{l\in\mathbb{Z}_{q-1}} t^{*k}(2^l)\cos(\frac{2\pi}{q-1}l) =$$
$$= \frac{1}{2}\sum_{l\in\mathbb{Z}_{q-1}} t^{*k}(2^l)(\mathrm{e}^{\jmath\frac{2\pi}{q-1}l} + \mathrm{e}^{-\jmath\frac{2\pi}{q-1}l}) = \frac{1}{2}(\hat{t}^k(1) + \hat{t}^k(-1)),$$

kde

$$\hat{t}(1) = \sum_{l\in\mathbb{Z}_{q-1}} t(2^l)\mathrm{e}^{\jmath\frac{2\pi}{q-1}l} = \frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q-1}) = \hat{t}(-1)$$

jsou Fourierovy obrazy t v reprezentacích $2^l \mapsto \exp(\jmath 2\pi l/(q-1))$ a $2^l \mapsto \exp(-\jmath 2\pi l/(q-1))$. Dosazením za obrazy dostáváme

$$\|p_{Z_k} - U\| \geq (\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi}{q-1}))^k.$$

Podobně jako v bodě (5) použijeme odhad $\cos x \geq 1 - x^2/2$ pro $x \in [0, 1]$, kde $x := 2\pi/(q-1)$ (tentokrát zdola), což dává

$$\|p_{Z_k} - U\| \geq (1 - \frac{4\pi^2}{3(q-1)^2})^k$$

pro $q \geq 2\pi + 1$. Dále použijeme odhad $1 - y \geq \exp(-2y)$ pro $y \in [0, 1/2]$, kde $y := 4\pi^2/(3(q-1)^2)$, což dává

$$\|p_{Z_k} - U\| \geq \mathrm{e}^{-\frac{8\pi^2}{3(q-1)^2}k}$$

pro $q \geq \pi\sqrt{8/3} + 1$. Pro $k = cq^2$, kde c je konstanta na q dostáváme $\|p_{Z_k} - U\| \to \mathrm{e}^{-\frac{8\pi^2}{3}c} > 0$, $q \to \infty$ (pro $k = o(q^2)$, $q \to \infty$ pak dokonce $\|p_{Z_k} - U\| \to 1$ pro $q \to \infty$). Tedy $k = cq^2$, $q \to \infty$ kroků není dostatečných pro konvergenci k rovnoměrnému rozdělení jak pro Z_k tak pro X_k na A_q □

Literatura

[1] Diaconis P.: *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics, Hayward, California, 1988.

[2] Serre J. P.: *Linear Representations of Finite Groups*, Springer-Verlag, 1977.

[3] Sagan B. E.: *The Symmetric Group - Representations, Combinatorial Algorithms, and Symmetric Functions*, Springer-Verlag, 2001.

[4] Prášková Z., Lachout P.: *Základy náhodných procesů*, Karolinum, 1998.

[5] Feller W.: *An Introduction to Probability Theory and Its Applications*, Volume II, 1971.

[6] Dupač V., Hušková M.: *Pravděpodobnost a matematická statistika*, Karolinum, 2009.

[7] Shevtsova I. G.: *Sharpening of the upper bound of the absolute constant in the Berry-Esseen inequality*, Theory of Probability and its Applications **51** (2007) 549-553.