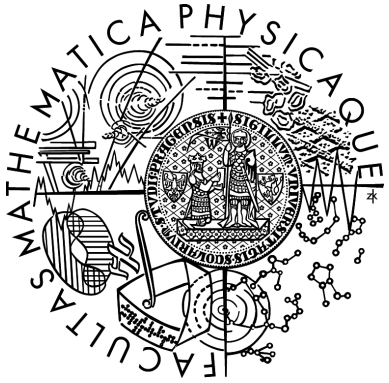
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Ivo Machek

Kvazigrupy, jednosměrné funkce a hašování

Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Aleš Drápal, CSc., DSc.
Studijní program: Matematické metody informační bezpečnosti

Děkuji prof. RNDr. Aleši Drápalovi, CSc., DSc. za cenné rady, náměty, jazykovou úpravu a hodiny konzultací a seminářů, kterými přispěl k napsání této diplomové práce. Dále děkuji svým rodičům, protože bez jejich lásky a podpory by tato práce nemohla vzniknout.

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

V Praze dne 17. dubna 2009 Ivo Machek

Obsah

Název práce: Kvazigrupy, jednosměrné funkce a hašování
Autor: Ivo Machek
Katedra: Katedra algebry
Vedoucí diplomové práce: prof. RNDr. Aleš Drápal, CSc., DSc.
E-mail vedoucího: drapal@karlin.mff.cuni.cz

Abstrakt: V první části této práce jsme se zabývali složitostí řešení nelineárních kvazigrupových rovnic pro různé třídy kvazigrup. Zvláště jsme se pak zabývali přenesením principu centrálních kvazigrup na bloky kongruence. Ukázali jsme, že tyto kvazigrupy splňují podmínku beztvarosti a proto jsme získali protipříklad k hypotéze, kterou předložil D. Gligoroski. V druhé části této práce jsme aplikovali předchozí výsledky na konkrétní kvazigrupy typu Edon-R-I,II a odvodili jsme složitost příslušného algoritmu pro invertování hašovací funkce Edon-R.

Klíčová slova: kvazigrupa, jednosměrná funkce, hašovací funkce Edon-R.

Title: Quasigroups, one-way functions and hash mappings
Author: Ivo Machek
Department: Department of algebra
Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc.
Supervisor's e-mail address: drapal@karlin.mff.cuni.cz

Abstract: In the first part of this work we study the complexity of solving nonlinear quasigroup equations for different classes of quasigroups. In particular we study the application of principle of central quasigroups on the blocks of congruence. We show that these quasigroups can be shapeless and therefore we gain counterexample to the hypothesis which was stated by D. Gligoroski. In the second part of this work we apply previous results on the concrete quasigroups of the type Edon-R-I,II and we deduce the complexity of the corresponding algorithm for inverting the hash function Edon-R.

Keywords: quasigroup, one-way function, hash function Edon-R.

Úvod

Hašovací funkce patří mezi nejdůležitější kryptografická primitiva. Jejich definičním oborem jsou libovolně dlouhé zprávy, které jsou převáděny do množiny zpráv pevné délky. Výstup hašovací funkce se nazývá otisk či haš zprávy. Hlavním využitím hašovacích funkcí je jejich součást při návrhu protokolů pro digitální podpis. Hlavní motivací této práce je hašovací funkce Edon-R, kterou navrhnul D. Gligoroski. Její návrh je založen na kvazigrupách velkých řádů.

Celkovou strukturu práce bychom mohli rozdělit do dvou bloků. V prvním bloku se zabýváme vlastností kvazigrupy nazvanou beztvarost, kterou definoval D. Gligoroski ve svých článcích. První kapitola se zabývá některými obecnými vlastnostmi především abelovských grup. Tyto poznatky následně uplatníme v kapitole 4 o centrálních kvazigrupách. Kapitola 2 nás krátce seznámí s kvazigrupami a v kapitole 3 zformalizujeme pojem kvazigrupové funkce a zformulujeme definici beztvaré kvazigrupy, která je základním stavebním kamenem pro vytvoření domnívaně jednosměrné funkce R_1. V kapitole 4 definujeme centrální kvazigrupy a uděláme jejich rozbor vzhledem k vlastnosti beztvarosti. V kapitole 5 definujeme kvazigrupy odvozené od centrálních kvazigrup, které budou sloužit jako protipříklad k hypotéze z kapitoly 3. Kapitola 6 potom rozebírá všechny doposud definované třídy kvazigrup z pohledu řešení nelinárních kvazigrupových rovnic.

Druhý blok této práce se zaměřuje na aplikace výsledků kapitol prvního bloku na hašovací funkci Edon-R. V kapitole 7 definujeme kvazigrupy typu Edon-R-I,II, které byly v návrzích této funkce použity. V kapitolách 8 a 9 budeme analyzovat tyto kvazigrupy obecně z pohledu řešení kvazigrupových rovnic. V kapitole 10 definujeme již hašovací funkci Edon-R a v poslední kapitole aplikujeme výsledek z kapitoly 9 na konkrétní parametry této funkce.

Kapitola 1

Grupy

V této kapitole se budeme věnovat poznatkům z teorie grup, které dále využijeme v kapitolách o kvazigrupách. Úvodní partie vycházejí především z učebnice Teorie grup - základní aspekty od Aleše Drápala [4], proto podrobnější úvod do následujících témat lze nalézt zde.

Definice 1.1. Množina G spolu s binární operací $\cdot$, unární operací $^{-1}$ a nulární operací 1 se nazývá *grupa*, jestliže operace $\cdot$ je asociativní ($x\cdot(y\cdot z) = (x\cdot y)\cdot z$ pro všechna $x, y, z \in G$), 1 je neutrální prvek ($1\cdot x = x = x\cdot 1$ pro všechna $x \in G$) a prvky x^{-1} jsou inverzní vůči prvkům x ($x\cdot x^{-1} = 1 = x^{-1}\cdot x$ pro všechna $x \in G$).

V případu multiplikativní notace grupové operace budeme symbol $\cdot$ vynechávat a budeme psát xy místo $x \cdot y$. Je-li grupová operace komutativní, potom budeme G nazývat abelovskou grupou a budeme používat aditivní notaci $(G, +)$. Protože hlavní aplikace této kapitoly se vztahuje na abelovské grupy, tak uvedeme několik základních poznatků.

Je-li G abelovská grupa a p prvočíslo, pak $G_{(p)} = \{a \in G : p^n a = 0 \text{ pro nějaké } n \geq 1\}$ se nazývá *p-primární komponenta* grupy G a platí, že $G_{(p)}$ je podgrupou G. Jestliže $G = G_{(p)}$, pak grupu G budeme nazývat *p-grupou*. Je zřejmé, že $G_{(p)}$ je p-grupa pro všechna $p \in \mathbb{P}$.

Tvrzení 1.2. *Nechť G je abelovská grupa, jejíž všechny prvky jsou konečného řádu. Potom $G = \bigoplus_{p\in\mathbb{P}} G_{(p)}$, kde $\mathbb{P}$ značí množinu všech prvočísel.*

Tvrzení 1.3. *Nechť G je konečná abelovská p-grupa. Potom G je možno vyjádřit jako direktní sumu cyklických grup. Tedy pro $l \in \mathbb{N}$ a $k_i \in \mathbb{N}$ takové,*

že $1 \leq k_1 \leq \ldots \leq k_l$ *platí*

$$G \cong \bigoplus_{i=1}^{l} \mathbb{Z}_{p^{k_i}}.$$

Nechť V je vektorový prostor nad tělesem $\mathbb{F}$. Potom grupu automorfismů prostoru V budeme značit $\mathrm{GL}(V)$. Jestliže V je konečné dimenze v a $\mathbb{F}$ je konečné těleso řádu q, tak budeme používat značení $\mathrm{GL}(v, q)$. Každý automorfismus vektorového prostoru konečné dimenze můžeme ztotožnit s prvkem maticového okruhu, který budeme značit $\mathrm{M}_v(\mathbb{F}_q)$.

Konečnou abelovskou p-grupu G, ve které řád každého netriviálního prvku je roven p, nazveme *elementární abelovskou* grupou. Je-li řád G roven p^v, pak tuto grupu ztotožníme s vektorovým prostorem dimenze v nad tělesem $\mathbb{Z}_p$ a odtud dostáváme, že grupa $\mathrm{Aut}(G)$ je izomorfní grupě $\mathrm{GL}(v, p)$.

Tvrzení 1.4. *Nechť q je mocnina prvočísla a $v \geq 1$. Potom platí*

$$|\mathrm{GL}(v, q)| = (q^v - 1) \cdot (q^v - q) \cdot \ldots \cdot (q^v - q^{v-1}).$$

Tvrzení 1.5. *Nechť $(G, +)$ je elementární abelovská p-grupa a nechť $\varphi \in \mathrm{Aut}(G)$. Potom*

$$|\varphi| < |G|.$$

Důkaz. Elementární abelovskou p-grupu ztotožníme s vektorovým prostorem V nad tělesem $\mathbb{Z}_p$, jeho konečnou dimenzi označíme v. Na vektorovém prostoru definujeme strukturu $\mathbb{Z}_p[x]$-modulu následujícím způsobem. Nechť $f = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}_p[x]$ a nechť $u \in V$. Potom

$$fu = \sum_{i=0}^{m} a_i \varphi^i(u).$$

Nechť $m_\varphi \in \mathbb{Z}_p[x]$ je minimální polynom automorfismu φ, tedy monický polynom nejmenšího stupně s vlastností $m_\varphi u = 0$ pro všechna $u \in V$. Pro charakteristický polynom $g \in \mathbb{Z}_p[x]$ automorfismu φ vyplývá z Hamilton-Cayleyho věty (například [2]), že $g(\varphi) = 0$ a proto $gu = 0$ pro všechna $u \in V$. Každý polynom s touto vlastností musí být dělitelný minimálním polynomem m_φ a proto $\deg m_\varphi \leq \deg g = v$. Následující podmínky jsou zřejmě ekvivalentní:

1. řád φ dělí n,

2. $\varphi^n(u) = u$ pro všechna $u \in V$,
3. $(x^n - 1)V = 0$,
4. $m_\varphi | x^n - 1$.

Nechť $m_\varphi = f_1 \cdot \ldots \cdot f_r$ je rozklad na ireducibilní polynomy. Nechť f_i je libovolný ireducibilní faktor m_φ. Rozkladové nadtěleso $\mathbb{Z}_p$ dané tímto polynomem je $\mathbb{F}_{p^{\deg(f_i)}}$. Řád každého kořenu f_i tedy dělí $p^{\deg(f_i)} - 1$. Odtud plyne, že pro každý kořen θ polynomu m_φ je $\theta^k = 1$, kde

$$k = \prod_{i=1}^{r} (p^{\deg(f_i)} - 1) < p^{\sum_{i=1}^{r} \deg(f_i)} \leq p^v.$$

Protože každý kořen polynomu $m_\varphi \in \mathbb{Z}_p[x]$ je zároveň kořenem polynomu $x^k - 1 \in \mathbb{Z}_p[x]$, tak $m_\varphi | (x^k - 1)$ a proto řád φ dělí k. □

Poznámka 1.6. V článku [10] od V. Horoševského je ukázáno, že tvrzení 1.5 platí pro všechny grupy (ne jen pro elementární abelovské). Důkaz je ale rozsáhlý a nebudeme toto zobecnění v naší práci potřebovat.

Značení. Nechť G je grupa a $\varphi \in \mathrm{Aut}(G)$. Označíme $\mathrm{Fix}(\varphi) = \{x \in G \mid \varphi(x) = x\} \leq G$.

Tvrzení 1.7. *Nechť $(G, +)$ je elementární abelovská p-grupa a nechť $\varphi \in \mathrm{Aut}(G)$. Potom*

$$|\varphi| \leq \frac{|G|}{|\mathrm{Fix}(\varphi)|}.$$

Důkaz. Jestliže $|\mathrm{Fix}(\varphi)| = 1$ potom důkaz plyne z tvrzení 1.5. Nechť tedy $|\mathrm{Fix}(\varphi)| > 1$. Budeme dokazovat indukcí podle hodnoty n, kde $|G| = p^n$. Jestliže $n = 0$ nebo $n = 1$, pak tvrzení zřejmě platí. Nechť platí pro $n - 1$. Označme $r = |\varphi|$ a $d = |\bar{\varphi}|$, kde $\bar{\varphi} \in \mathrm{Aut}(G/\mathrm{Fix}(\varphi))$ je automorfismus indukovaný φ tak, že pro všechna $x \in G$

$$\bar{\varphi}(x + \mathrm{Fix}(\varphi)) = \varphi(x) + \mathrm{Fix}(\varphi).$$

Uvažujme pro spor, že

$$r > \frac{|G|}{|\mathrm{Fix}(\varphi)|}. \tag{1.1}$$

Dle tvrzení 1.5 je řád automorfismu menší než řád grupy a proto $d < r$. Z definice automorfismu $\bar{\varphi}$ zřejmě dostáváme, že d dělí r. Pro každé $x \in G$

existuje $u \in \mathrm{Fix}(\varphi)$ takové, že $\varphi^d(x) = x + u$, odkud dostáváme, že $\varphi^{pd}(x) = (\varphi^d)^p(x) = x + pu = x$ a proto $pd = r$. Jako přímý důsledek získáváme následující nerovnost:

$$\frac{|G|}{p|\mathrm{Fix}(\varphi)|} < \frac{r}{p} = d \leq \frac{|G/\mathrm{Fix}(\varphi)|}{|\mathrm{Fix}(\bar{\varphi})|},$$

kde ostrá nerovnost plyne z (1.1) a neostrá z indukčního předpokladu. Porovnáním levé a pravé strany a zkrácením dostáváme, že $|\mathrm{Fix}(\bar{\varphi})| < p$, což je ekvivalentní s $|\mathrm{Fix}(\bar{\varphi})| = 1$.

Grupu G ztotožníme s vektorovým prostorem nad tělesem $\mathbb{Z}_p$ a podgrupu $\mathrm{Fix}(\varphi)$ s jeho podprostorem. Nechť $G = \mathrm{Fix}(\varphi) \oplus H$ pro nějaký podprostor H. Potom každému prvku $x \in G$ umíme jednoznačně přiřadit dvojici (u, h), kde $u \in \mathrm{Fix}(\varphi)$, $h \in H$ a $x = u \oplus h$. Použijeme-li tento zápis pro φ, tak dostáváme

$$\varphi((u, h)) = (u + \mu(h), \psi(h)),$$

kde $\mu : H \to \mathrm{Fix}(\varphi)$ je homomorfismus a $\psi \in \mathrm{Aut}(H)$ odpovídá $\bar{\varphi} \in \mathrm{Aut}(G/\mathrm{Fix}(\varphi))$. Proto $|\psi| = d$ a $|\mathrm{Fix}(\psi)| = 1$. Snadno odvodíme, že

$$\varphi^i((u, h)) = (u + \sum_{j=0}^{i-1} \mu(\psi^j(h)), \psi^i(h)).$$

Dosadíme-li za i hodnotu d, pak dostáváme, že $\psi^d(h) = h$ a

$$\sum_{j=0}^{d-1} \mu(\psi^j(h)) = \mu(\sum_{j=0}^{d-1} \psi^j(h)) = \mu(0) = 0,$$

neboť $\psi(\sum_{j=0}^{d-1} \psi^j) = \sum_{j=1}^{d} \psi^j = \sum_{j=0}^{d-1} \psi^j$ a tedy $\mathrm{Im}(\sum_{j=0}^{d-1} \psi^j) \subseteq \mathrm{Fix}(\psi) = \{0\}$. Pro všechna $u \in \mathrm{Fix}(\varphi)$, $h \in H$ dostáváme, že $\varphi^d((u, h)) = (u, h)$ a tedy $d = r$, což je spor, neboť z předpokladu plyne, že $d < r$. □

Nyní přistoupíme k další základní látce z teorie grup, kterou využijeme v následujících kapitolách. Nechť Ω je množina. Symbolem $S(\Omega)$ budeme značit *symetrickou grupu*, tedy grupu všech bijektivních zobrazení na Ω. *Působením* grupy P na Ω budeme rozumět každý homomorfismus $\varphi : P \to S(\Omega)$. Místo značení $\varphi(x)(\omega)$ budeme používat značení $x(\omega)$, přičemž z kontextu bude zřejmé o jaké působení grupy P jde. *Permutační grupou* budeme rozumět každou podgrupu symetrické grupy $S(\Omega)$. Každou permutační grupu

$P \leq S(\Omega)$ můžeme tedy ztotožnit s působením $i : P \to S(\Omega)$ grupy P na množině Ω, kde $i(x) = x$ pro všechna $x \in P$. Proto všechny termíny používané pro působení grupy na množině budeme analogicky používat i pro permutační grupy.

Nechť P působí na množině Ω. Řekneme, že toto působení je *tranzitivní*, jestliže pro všechna $\omega_1, \omega_2 \in \Omega$ existuje $x \in P$ takové, že $x(\omega_1) = \omega_2$. O množině $\Gamma \subseteq \Omega$ řekneme, že je to *blok* akce P na Ω, jestliže Γ je neprázdná a pro všechna $x \in P$ platí $x(\Gamma) = \Gamma$ nebo $x(\Gamma) \cap \Gamma = \emptyset$.

Lemma 1.8. *Nechť grupa P působí na Ω. Je-li Γ blok této akce, potom $x(\Gamma)$ je blokem pro každé $x \in P$. Je-li navíc toto působení tranzitivní, tak $\{x(\Gamma) : x \in P\}$ tvoří rozklad Ω.*

Je-li $(G, \cdot)$ grupa a $x \in G$, pak zobrazení $L_x, R_x \in S(G)$ definované vztahy $L_x(y) = xy$ a $R_x(y) = yx$ se nazývají *levou a pravou translací* určenou prvkem x. Permutační grupu na množině G, která je generována levými a pravými translacemi nazveme *multiplikativní grupou* G a značíme ji symbolem $\mathrm{Mlt}(G)$. Protože pro všechna $x, y \in G$ existuje $z = xy^{-1} \in G$ takové, že $x = L_z(y)$, tak $\mathrm{Mlt}(G)$ je tranzitivní permutační grupa.

Lemma 1.9. *Nechť Γ je blok působení $\mathrm{Mlt}(G)$ na G. Potom*

(1) *$B = \{\varphi(\Gamma) : \varphi \in \mathrm{Mlt}(G)\}$ je rozkladem grupy G,*
(2) *existuje $\Gamma_1 \in B$ taková, že Γ_1 je normální podgrupa G a*
(3) *rozklad G modulo Γ_1 je shodný s B.*

Důkaz. Bod (1) plyne přímo z lemma 1.8. Nechť $\Gamma_1 \in B$ obsahuje neutrální prvek 1. Pak díky vlastnosti bloku platí pro všechna $x \in \Gamma_1$, že $L_x(\Gamma_1) = \Gamma_1$. Naopak jestliže $x \notin \Gamma_1$, tak $L_x(\Gamma_1) \cap \Gamma_1 = \emptyset$. Jsou-li $x, y \in \Gamma_1$, tak $L_{xy}(\Gamma_1) = L_x L_y(\Gamma_1) = \Gamma_1$, $L_{x^{-1}}(\Gamma_1) = L_{x^{-1}} L_x(\Gamma_1) = \Gamma_1$ a $L_1(\Gamma_1) = \Gamma_1$. Proto je Γ_1 podgrupa G. Je zřejmé, že $B = \{L_x(\Gamma_1) : x \in G\} = \{R_x(\Gamma_1) : x \in G\}$ a proto ze shodnosti levých a pravých rozkladů grupy G modulo Γ_1 plyne, že Γ_1 je normální. □

Definice 1.10. Nechť $(G, \cdot)$ je grupa. *Holomorfem* grupy G se rozumí semidirektní součin grupy G s grupou $\mathrm{Aut}(G)$ všech automorfismů na G při použití identického homomorfismu $\mathrm{Aut}(G) \to \mathrm{Aut}(G)$. Holomorf lze ztotožnit s permutační grupou na G tvořenou zobrazeními $L_x\varphi$, kde $x \in G$ a $\varphi \in \mathrm{Aut}(G)$. Tuto permutační grupu budeme značit $\mathrm{Hol}(G)$. Příslušný izomorfismus je tvaru $(x, \varphi) \mapsto L_x\varphi$, takže v $\mathrm{Hol}(G)$ platí

$$\begin{aligned} (L_x\beta)(L_y\alpha) &= L_{x\beta(y)}\beta\alpha, \\ (L_x\varphi)^{-1} &= L_{\varphi^{-1}(x^{-1})}\varphi^{-1}. \end{aligned} \tag{1.2}$$

Lemma 1.11. *Nechť $i \in \mathbb{N}$ a $L_x\varphi \in \mathrm{Hol}(G)$. Potom $(L_x\varphi)^i = L_a\varphi^i$, kde $a = \prod_{j=0}^{i-1} \varphi^j(x)$.*

Důkaz. Budeme postupovat indukcí. Pro $i = 1$ je tvrzení zřejmé. Nechť platí pro $i-1$. Potom $(L_x\varphi)^i = (L_x\varphi)(L_x\varphi)^{i-1} = (L_x\varphi)(L_{\prod_{j=0}^{i-2}\varphi^j(x)}\varphi^{i-1}) = L_{\prod_{j=0}^{i-1}\varphi^j(x)}\varphi^i$ dle (1.2). □

Důsledek 1.12. *Řád automorfismu φ dělí řád prvku $L_x\varphi$.*

Důkaz. $(L_x\varphi)^r = L_a\varphi^r = \mathrm{id}$, právě když $a = 1$ a zároveň r dělí $|\varphi|$. □

Pro účely této práce by bylo potřebné znát řády zobrazení $L_x\varphi$, zejména pak nejmenší společný násobek n_φ všech $\{L_x\varphi : x \in G\}$, kde $\varphi \in \mathrm{Aut}(G)$. Je možné, že $n_\varphi \leq |G|$ pro každé $\varphi \in \mathrm{Aut}(G)$ a každou grupu G. Obecný důkaz se nám nepodařilo nalézt. Uvedeme nejdříve lemma 1.13, kde toto tvrzení platí za dodatečných podmínek na φ pro všechny grupy. Následně potom ukážeme, že nerovnost $n_\varphi \leq |G|$ platí pro všechny abelovské grupy.

Lemma 1.13. *Nechť G je grupa a $\varphi \in \mathrm{Aut}(G)$. Je-li $|\mathrm{Fix}(\varphi)| = 1$, pak*

$$n_\varphi = |\varphi|.$$

Důkaz. Budeme vycházet z rovnosti: $L_a\varphi L_{a^{-1}} = L_{a\varphi(a^{-1})}\varphi$. Zobrazení $\mu_\varphi : G \to G$, definované vztahem $\mu_\varphi(a) = a\varphi(a^{-1})$, je bijekce množiny G, neboť $(a\varphi(a^{-1}) = b\varphi(b^{-1})) \Rightarrow (b^{-1}a \in \mathrm{Fix}(\varphi)) \Rightarrow (a = b)$. Proto pro každé $x \in G$ existuje $y = \mu_\varphi^{-1}(x)$ takové, že $L_x\varphi = L_y\varphi L_{y^{-1}}$. Obecně platí, že konjugované prvky mají stejný řád a proto dostáváme, že $|L_x\varphi| = |L_y\varphi L_{y^{-1}}| = |\varphi|$ pro všechna $x \in G$. □

Věta 1.14. *Nechť $(G, +)$ je elementární abelovská p-grupa a nechť $\varphi \in \mathrm{Aut}(G)$. Je-li $|\mathrm{Fix}(\varphi)| > 1$, pak*

$$n_\varphi \leq |G|.$$

Důkaz. Označme $r = |\varphi|$ a $L_a\gamma = (L_x\varphi)^r$. Potom $\gamma = \mathrm{id}$ a platí, že $a \in \mathrm{Fix}(\varphi)$, neboť

$$\varphi(a) = \varphi(\sum_{i=0}^{r-1} \varphi^i(x)) = \sum_{i=1}^{r} \varphi^i(x) = \sum_{i=0}^{r-1} \varphi^i(x) = a.$$

Proto dostáváme $(L_a\gamma)^p = L_{pa}\gamma^p = \mathrm{id}$ a tedy

$$n_\varphi \leq pr \leq p\frac{|G|}{|\mathrm{Fix}(\varphi)|} \leq |G|,$$

využitím tvrzení 1.7 a předpokladu $|\mathrm{Fix}(\varphi)| \geq p$. □

Důsledek 1.15. *Nechť $(G,+)$ je elementární abelovská p-grupa a nechť $\varphi \in \mathrm{Aut}(G)$. Potom*

$$n_\varphi \leq |G|.$$

Důkaz. Tvrzení dostáváme spojením lemma 1.13 a věty 1.14. □

Lemma 1.16. *Nechť $(G,+)$ je abelovská grupa. Nechť $H \leq G$ a nechť $\varphi \in \mathrm{Aut}(G)$ indukuje na G/H identitu ($\bar{\varphi} = \mathrm{id}_{G/H}$). Označme $\varphi_1 = \varphi \restriction H \in \mathrm{Aut}(H)$. Označme $n_{\varphi,H} = \mathrm{NSN}\{|L_x\varphi| : x \in H\}$. Potom $n_{\varphi,H} = n_{\varphi_1}$.*

Důkaz. Jelikož $n_{\varphi_1} = \mathrm{NSN}\{|L_x\varphi_1| : x \in H\}$, tak $n_{\varphi,H} \geq n_{\varphi_1}$. Pro všechna $D \in G/H$ je D φ-invariantní. Označme $\varphi_D = \varphi \restriction D$. Nechť $x \in H$. Potom $L_x\varphi_D$ je permutací množiny D. Jestliže $u \in D$, pak zobrazení $L_u^{-1}(L_x\varphi_D)L_u$ je permutací množiny H a platí, že $L_u^{-1}(L_x\varphi_D)L_u = L_{-u+x+\varphi(u)}\varphi_1$. Protože $\varphi(u) - u \in H$, tak existuje $y \in H$ takové, že $L_u^{-1}(L_x\varphi_D)L_u = L_y\varphi_1$. Odtud plyne, že $(L_x\varphi_D)^{n_{\varphi_1}} = \mathrm{id}_D$ a tedy $n_{\varphi,H} \leq n_{\varphi_1}$. □

Věta 1.17. *Nechť $(G,+)$ je konečná abelovská p-grupa a nechť $\varphi \in \mathrm{Aut}(G)$. Potom*

$$n_\varphi \leq |G|.$$

Důkaz. Dle tvrzení 1.3 můžeme každou abelovskou p-grupu vyjádřit jako součin cyklických grup řádů p^{k_i}, kde $k_i \in \mathbb{N}$ jsou taková, že $k_1 \leq k_2 \leq \ldots \leq k_l$. Důkaz budeme provádět indukcí podle hodnoty k_l. Nepřímo tedy podle p^{k_l} exponentu G. Jestliže $k_l = 0$, tak G je triviální. Jestliže $k_l = 1$, tak G je elementární abelovská p-grupa a důkaz vyplývá z důsledku 1.15.

Nechť $k_l > 1$ a nechť tvrzení platí pro všechny menší hodnoty k_l. Nechť $j \in \{1,\ldots,l\}$ je největší takové, že $k_{l-j+1} = k_l$. Definujme podgrupu $H \leq G$, $H = \{g \in G : |g| < p^{k_l}\}$. Snadno se ukáže, že H je izomorfní sumě

$$\mathbb{Z}_{p^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_{l-j}}} \oplus \mathbb{Z}_{p^{k_{l-j+1}-1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_l-1}}.$$

Faktorgrupa G/H je izomorfní abelovské elementární grupě $\bigoplus_{i=1}^{j} \mathbb{Z}_p$. Protože automorfismy zachovávají řád prvků, tak $\varphi(H) = H$. Proto můžeme definovat $\bar{\varphi} \in \mathrm{Aut}(G/H)$ předpisem $\bar{\varphi}(x+H) = \varphi(x) + H$. Z důsledku 1.15 plyne, že existuje $n_{\bar{\varphi}} \leq |G/H|$ takové, že

$$(L_{(x+H)}\bar{\varphi})^{n_{\bar{\varphi}}} = \mathrm{id}_{G/H}. \tag{1.3}$$

Označme $L_a\gamma = (L_x\varphi)^{n_{\bar{\varphi}}}$. Z (1.3) plyne, že $\gamma = \varphi^{n_{\bar{\varphi}}}$ indukuje identitu na G/H a

$$\sum_{j=0}^{n_{\bar{\varphi}}-1} \bar{\varphi}^j(x+H) = H \Rightarrow \sum_{j=0}^{n_{\bar{\varphi}}-1} \varphi^j(x) + H = H \Rightarrow a + H = H \Rightarrow a \in H.$$

Proto dle lemma 1.16 platí, že $(L_a\gamma)^{n_{\gamma_1}} = (L_x\varphi)^{n_{\gamma_1} n_{\bar{\varphi}}} = \mathrm{id}$, kde $\gamma_1 = \gamma \restriction H$. Z indukčního předpokladu plyne, že $n_{\gamma_1} \leq |H|$ a následně dostáváme $n_\varphi = n_{\bar{\varphi}} n_{\gamma_1} \leq |G/H||H| = |G|$. □

Věta 1.18. *Nechť $(G,+)$ je konečná abelovská grupa a nechť $\varphi \in \mathrm{Aut}(G)$. Potom*

$$n_\varphi \leq |G|.$$

Důkaz. Dle tvrzení 1.2 můžeme každou konečně generovanou abelovskou grupu vyjádřit jako direktní sumu abelovských p-grup: $G \cong \bigoplus_{p\in\mathbb{P}} G_{(p)}$. Protože uvažujeme G konečnou, tak i $G_{(p)}$ jsou konečné. Obecně platí, že mají-li grupy H a K nesoudělné řády, pak $\mathrm{Aut}(H \times K) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Proto platí, že

$$\mathrm{Aut}(G) \cong \bigoplus_{p\in\mathbb{P}} \mathrm{Aut}(G_p).$$

Jelikož G je konečná, označme $G_{p_1}, \ldots, G_{p_l}$ netriviální G_p v rozvoji G. Potom na každý prvek $L_x\varphi \in \mathrm{Hol}(G)$ můžeme pohlížet jako na l-tici $(L_{x_1}\varphi_1, \ldots, L_{x_l}\varphi_l)$, kde $x_i \in G_{p_i}$ a $\varphi_i \in \mathrm{Aut}(G_{p_i})$. Odtud snadno plyne, že $n_\varphi = \mathrm{NSN}(n_{\varphi_1}, \ldots, n_{\varphi_l}) \leq \prod_{i=1}^{l} n_{\varphi_i} \leq \prod |G_{p_i}| = |G|$. □

Kapitola 2

Kvazigrupy

Definice 2.1. Množina Q spolu s binární operací $*$ se nazývá *kvazigrupa*, jestliže pro všechna $a, b \in Q$ mají rovnice

$$x * a = b \text{ a } a * y = b$$

jednoznačná řešení $x = b/a$ a $y = a\backslash b$. Řekneme, že kvazigrupa je *lupa*, jestliže obsahuje neutrální prvek $e \in Q$ ($e * a = a = a * e$ pro všechna $a \in Q$).

Je-li Q konečná řádu n, potom Caleyho (multiplikativní) tabulka Q tvoří latinský čtverec $n \times n$ - to jest čtverec vyplněný čísly z množiny $\{1, \ldots, n\}$ tak, že v každém řádku a sloupci se žádné dvě čísla neopakují. V celé práci budeme uvažovat pouze konečné kvazigrupy. Některá tvrzení ovšem platí i pro nekonečný případ, ale nebudeme se jím zabývat. Každá grupa je zřejmě kvazigrupou. Opačný případ je charakterizován následujícím lemmatem.

Lemma 2.2. *Nechť $(Q, *)$ je kvazigrupa. Jestliže $*$ je asociativní, potom lze dodefinovat unární operaci $^{-1}$ a $e \in Q$ tak, že $(Q, *, ^{-1}, e)$ je grupa.*

Důkaz. Nechť $q \in Q$. Potom existují $a, b \in Q$ takové, že $q * a = q = b * q$. Ukážeme, že $a = b = e$ je jednotkovým prvkem Q. Pro všechna $p \in Q$ existují $p_1, p_2 \in Q$ takové, že $q * p_1 = p = p_2 * q$. Odtud plyne $p * a = (p_2 * q) * a = p_2 * (q * a) = p_2 * q = p$ a podobně $b * p = p$. Rovnost vyplývá přímo z $a = a * b = b$.

Pro každé q existují $c, d \in Q$ takové, že $q * c = e = d * q$. Chceme ukázat, že $c = d = q^{-1}$, což platí z $c = e * c = (d * q) * c = d * (q * c) = d * e = d$. □

Stejně jako v grupách definuje v kvazigrupách levé a pravé translace. Pro odlišení je budeme značit symboly λ_x pro levou translaci určenou prvkem $x \in Q$ a ρ_x pro pravou translaci určenou prvkem $x \in Q$. Stejně tak definujeme $\mathrm{Mlt}(Q)$ multiplikativní grupu Q jako podgrupu $S(Q)$ generovanou levými a pravými translacemi kvazigrupy Q.

Definice 2.3. Nechť $(Q, *)$ je kvazigrupa. Definujeme *řád levých translací* $n_{Q,\lambda}$ a *řád pravých translací* $n_{Q,\rho}$ předpisy

$$\begin{aligned} n_{Q,\lambda} &= \mathrm{NSN}(|\lambda_x| : x \in Q), \\ n_{Q,\rho} &= \mathrm{NSN}(|\rho_x| : x \in Q). \end{aligned}$$

Definice 2.4. *Kongruencí* kvazigrupy $(Q, *)$ budeme rozumět ekvivalenci na množině Q, která je slučitelná s operacemi $*$, $/$ a $\backslash$, což znamená, že je-li $x \sim y$ a $u \sim v$, pak

$$x * u \sim y * v,\ x/u \sim y/v \text{ a } x\backslash u \sim y\backslash v.$$

Poznámka 2.5. Důkaz toho, že ekvivalence $\sim$ je kongruencí Q můžeme rozložit na důkaz jednodušších tvrzení. Konkrétně $x * u \sim y * v$ pro všechna $x \sim y$, $u \sim v$ je ekvivalentní tomu, že $x * u \sim y * u$ a $u * x \sim u * y$ pro všechna $x \sim y$ a $u \in Q$. Tato ekvivalence plyne přímo ze vztahů $x * u \sim y * u \sim y * v$ a $u * x \sim u * y \sim v * y$. Analogické rozložení důkazu můžeme provést i pro operace $/, \backslash$. Je-li Q konečná, pak v následujícím lemma ukážeme, že dokonce stačí důkaz provést jen pro jednu z těchto operací.

Lemma 2.6. *Nechť $(Q, *)$ je konečná kvazigrupa. Jestliže ekvivalence $\sim$ je slučitelná s operací $*$, pak je slučitelná i s operacemi $/$ a $\backslash$.*

Důkaz. Nechť $u \in Q$ je libovolné. Potom pro všechna $i \in \mathbb{N}$ z $x \sim y$ plyne, že $\rho_x^i(u) \sim \rho_y^i(u)$. Nechť $m = |\rho_x|$ a $n = |\rho_y|$, nechť $d = \mathrm{NSN}(m, n)$. Potom platí, že $\rho_x^{d-1}(u) = u/x$ a $\rho_y^{d-1}(u) = u/y$. Odtud dostáváme, že $x \sim y$ implikuje $u/x \sim u/y$. Nechť $d = |\rho_u|$. Potom $\rho_u^{d-1}(x) = x/u$ a $\rho_u^{d-1}(y) = y/u$. Odtud plyne, že $x \sim y$ implikuje $x/u \sim y/u$. A tedy dle poznamky 2.5 platí, že $\sim$ je slučitelná s operací $/$. Důkaz pro operaci $\backslash$ bychom provedli analogicky s levou translací. □

Tvrzení 2.7. *Nechť $(Q, *)$ je kvazigrupa.*

(1) *Je-li $\sim$ kongruence Q, pak libovolný blok $\Gamma \subseteq Q$ modulo $\sim$ je blokem působení permutační grupy $\mathrm{Mlt}(Q)$ a rozklad Q modulo $\sim$ je roven rozkladu $\{\varphi(\Gamma) : \varphi \in \mathrm{Mlt}(Q)\}$.*

(2) *Libovolný blok* $\Gamma \subseteq Q$ *permutační grupy* $\mathrm{Mlt}(Q)$ *indukuje kongruenci kvazigrupy* Q *tvaru: pro všechna* $x, y \in Q$ *platí* $x \sim y$*, právě když existuje* $\varphi \in \mathrm{Mlt}(Q)$ *takové, že* $x, y \in \varphi(\Gamma)$.

Důkaz. (1) Díky slučitelnosti kongruence $\sim$ s operacemi $*, /, \backslash$ převádí libovolné zobrazení $\varphi \in \mathrm{Mlt}(Q)$ blok Γ na blok $\varphi(\Gamma)$. Proto vždy buď $\Gamma \cap \varphi(\Gamma) = \emptyset$ nebo $\Gamma = \varphi(\Gamma)$. Díky tranzitivitě $\mathrm{Mlt}(Q)$ je $\{\varphi(\Gamma) : \varphi \in \mathrm{Mlt}(Q)\}$ rozklad Q a je zřejmé, že je shodný s rozkladem Q modulo $\sim$.

(2) Slučitelnost s operacemi $*, /, \backslash$ budeme dokazovat dle poznámky 2.5. Jsou-li $x, y \in \Gamma$ a $u \in Q$, pak dostáváme

$$x * u = \rho_u(x) \quad \sim \quad \rho_u(y) = y * u, \tag{2.1}$$
$$u * x = \lambda_u(x) \quad \sim \quad \lambda_u(y) = u * y, \tag{2.2}$$
$$x/u = \rho_u^{-1}(x) \quad \sim \quad \rho_u^{-1}(y) = y/u, \tag{2.3}$$
$$u\backslash x = \lambda_u^{-1}(x) \quad \sim \quad \lambda_u^{-1}(y) = u\backslash y. \tag{2.4}$$

Zbývá dokázat, že $u/x \sim u/y$ a $x\backslash u \sim y\backslash u$. Nechť $v \in Q$ je libovolné. Z $x \sim y$ máme dle (2.1) $v * x \sim v * y$ a odtud $v = (v * x)/x \sim (v * y)/x$ využitím (2.3). Dosadíme-li $v = u/y$ dostáváme: $u/y \sim ((u/y) * y)/x = u/x$. Druhá ekvivalence se dokáže analogickým způsobem. □

Definice 2.8. Nechť $(Q, *)$ je kvazigrupa s kongruencí σ. *Faktorkvazigrupa* $Q/_\sigma$ je definována na rozkladových třídách kongruence σ tak, že $P_1 * P_2 = P_3$, právě když $x * y \in P_3$ pro $x \in P_1$ a $y \in P_2$ (ze slučitelnosti s operací $*$ plyne, že $x * y \in P_3$ pro všechna $x \in P_1$, $y \in P_2$, právě když $x * y \in P_3$ pro alespoň jedny $x \in P_1$, $y \in P_2$).

Značení. Nechť $(Q, *)$ je kvazigrupa s kongruencí σ. Protože budeme v následujících kapitolách často pracovat s hodnotou velikosti bloku Q modulo σ, tak zavedeme pro tuto hodnotu zjednodušené značení $\kappa_\sigma = \frac{|Q|}{|Q/_\sigma|}$.

Lemma 2.9. *Nechť* $(Q, *)$ *je kvazigrupa s kongruencí* σ*. Přirozená projekce* $\pi : Q \to Q/_\sigma$ *je homomorfismem kvazigrup.*

Důkaz. Důkaz vyplývá přímo z definice 2.8. □

Definice 2.10. Kvazigrupy $(Q_1, *_1)$, $(Q_2, *_2)$ nazveme *isotopní*, jestliže existují bijekce $\alpha, \beta, \gamma : Q_1 \to Q_2$ takové, že pro všechna $x, y \in Q_1$

$$\alpha(x) *_2 \beta(y) = \gamma(x *_1 y).$$

Trojice (α, β, γ) se nazývá *isotopismus* kvazigrup Q_1 a Q_2.

Kapitola 3

Kvazigrupové funkce a rovnice

Nechť $(Q, *)$ je kvazigrupa. Uvažujme absolutně volnou algebru termů A nad množinou $Q \cup \{x_1, \ldots, x_v\}$ s binárními operacemi $\circ, //, \backslash\backslash$. Na této algebře definujeme přepisovací pravidla:

1. $p \circ q \to p * q$, $p//q \to p/q$ a $p\backslash\backslash q \to p \backslash q$, kde se předpokládá, že $p, q \in Q$ (pravá strana relace $\to$ je tedy prvek Q) a
2. $(t_1 \circ t_2)//t_2 \to t_1$, $t_2\backslash\backslash(t_2 \circ t_1) \to t_1$, $t_2 \circ (t_2\backslash\backslash t_1) \to t_1$, $(t_1//t_2) \circ t_2$, $(t_2//t_1)\backslash\backslash t_2 \to t_1$, $t_2//(t_1\backslash\backslash t_2) \to t_1$ pro všechny prvky $t_1, t_2 \in A$.

Podobnou metodou jako u konstrukce volné kvazigrupy lze i zde ukázat, že daný přepisovací systém je konfluentní. Pokud na A definujeme ekvivalenci $\sim$ jako nejmenší ekvivalenci, která obsahuje relaci $\to$, tak v každé třídě $\sim$ je právě jeden terminální prvek přepisovacího systému. Ekvivalence $\sim$ je zřejmě kongruence a $A/_\sim$ je kvazigrupa, která obsahuje Q jako svou podkvazigrupu. Kvazigrupu $A/_\sim$ budeme značit $Q(x_1, \ldots, x_v)$. Je to rozšíření Q vzniklé přidáním volných proměnných $x_1, \ldots, x_v$. Prvky $Q(x_1, \ldots, x_v)$ lze ztotožnit s terminálovými prvky uvedeného přepisovacího systému. Vidíme, že jde vlastně o formalizaci pojmu kvazigrupového termu v proměnných $x_1, \ldots, x_v$. Operace $\circ, //, \backslash\backslash$ vztažené na kvazigrupu $Q(x_1, \ldots, x_v)$ přeznačíme přirozeně na $*, /, \backslash$.

Příklad. Nechť $t_1, t_2, t_3 \in Q(x_1, x_2, x_3)$ jsou dány předpisy: $t_1 \equiv x_1 * x_2$, $t_2 = x_1 * x_3$ a $t_3 = (x_1 * x_2)\backslash x_3$. Potom zřejmě platí: $t_1 * t_3 \equiv x_3$ a $t_2 * t_3 \equiv (x_1 * x_3) * ((x_1 * x_2)\backslash x_3)$.

Definice 3.1. Pro každé $f \in Q(x_1, \ldots, x_v)$ definujeme *množinu* Ω_f *podtermů* f tak, že je-li $f \in Q \cup \{x_1, \ldots, x_v\}$, pak $\Omega_f = \{f\}$ a pokud existují

$f_1, f_2 \in Q(x_1, \ldots, x_v)$ takové, že $f = f_1 * f_2$, $f = f_1/f_2$ nebo $f = f_1 \backslash f_2$, pak $\Omega_f = \{f\} \cup \Omega_{f_1} \cup \Omega_{f_2}$.

Nechť $t \in Q(x_1, \ldots, x_v)$ a $\bar{a} = (a_1, \ldots, a_v) \in Q^n$. Potom výraz $t(\bar{a})$ představuje dosazení jednotlivých hodnot a_i za proměnné x_i. Na každý term $t \in Q(x_1, \ldots, x_v)$ můžeme tedy pohlížet jako na kvazigrupovou funkci $f : Q^v \to Q$ danou předpisem $f(\bar{a}) = t(\bar{a})$ pro všechna $\bar{a} \in Q^v$. Kvazigrupu Q nazveme *primální*, jestliže pro každou funkci $f : Q^v \to Q$ existuje term $t \in Q(x_1, \ldots, x_v)$ takový, že $f(\bar{a}) = t(\bar{a})$ pro všechna $\bar{a} \in Q^v$. Jestliže je kvazigrupa primální, pak tedy umíme vyjádřit každou kvazigrupovou funkci $f : Q^v \to Q$ pomocí termového zápisu.

Na uspořádanou dvojici $\langle t_1, t_2 \rangle$, kde $t_1, t_2 \in Q(x_1, \ldots, x_v)$, budeme pohlížet jako na kvazigrupovou rovnici, jejíž levou stranu tvoří term t_1 a pravou stranu term t_2. Pro zpřehlednění budeme pro vyjádření množiny všech takových rovnic používat zápis:

$$\mathcal{E}_v = Q(x_1, \ldots, x_v) \times Q(x_1, \ldots, x_v).$$

Jestliže kvazigrupa Q obsahuje kongruenci σ, pak přirozenou projekci $\pi : Q \to Q/_\sigma$ můžeme díky slučitelnosti s kvazigrupovými operacemi rozšířit na množinu $Q(x_1, \ldots, x_v)$. Každou rovnici $\langle f_1, f_2 \rangle \in \mathcal{E}_v$ pak převedeme do kvazigrupy $Q/_\sigma$ pomocí přirozené projekce:

$$\pi(\langle f_1, f_2 \rangle) = \langle \pi(f_1), \pi(f_2) \rangle.$$

Definice 3.2. Nechť $v \in \mathbb{N}$. Nechť $(Q, *)$ je kvazigrupa a $m \in Q$. Definujeme kvazigrupovou funkci $\lambda_m : Q^v \to Q^v$, $\lambda_m \equiv (\lambda_{m,1}, \lambda_{m,2}, \ldots, \lambda_{m,v})$, kde $\lambda_{m,i} \in Q(x_1, \ldots, x_v)$ jsou dány předpisem

$$\begin{aligned} \lambda_{m,1}((a_1, \ldots, a_v)) &= m * a_1, \\ \lambda_{m,i}((a_1, \ldots, a_v)) &= \lambda_{m,i-1}(a_1, \ldots, a_v) * a_i \end{aligned}$$

pro $1 < i \leq v$. Pomocí funkce λ_m následně definujeme kvazigrupovou funkci $R_1 : Q^v \to Q^v$:

$$R_1((a_1, a_2, \ldots, a_v)) = \lambda_{a_1}(\lambda_{a_2}(\ldots(\lambda_{a_v}((a_1, a_2, \ldots, a_v))))).$$

Příklad. Uvažujme funkci R_1 s konstantou $v = 3$. Nechť $(b_1, b_2, b_3) \in \mathrm{Im}(R_1)$. Potom nalezení vzoru k (b_1, b_2, b_3) je ekvivalentní vyřešení následující soustavy kvazigrupových rovnic s neznámými x_1, x_2, x_3:

$$\begin{aligned} b_1 &= x_1 * (x_2 * (x_3 * x_1)) \\ b_2 &= (x_2 * (x_3 * x_1)) * ((x_3 * x_1) * x_2) \\ b_3 &= ((x_3 * x_1) * x_2) * x_3. \end{aligned} \tag{3.1}$$

		a_1	a_2	a_3	a_4	$\dots$	a_v
	$*$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$\dots$	$a_{0,v}$
a_v	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$\dots$	$a_{1,v}$
a_{v-1}	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$\dots$	$a_{2,v}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_1	$a_{v,0}$	$a_{v,1}$	$a_{v,2}$	$a_{v,2}$	$a_{v,3}$	$\dots$	$a_{v,v}$
		b_1	b_2	b_3	b_4	$\dots$	b_v

Tabulka 3.1: Schéma počítání funkce $R_1((a_1, \dots, a_v)) = (b_1, \dots, b_v)$, kde hodnoty v tabulce mají následující význam: pro všechna $i > 0$ platí, že $a_{0,i} = a_i$, $a_{i,0} = a_{v-i+1}$, $a_{v,i} = b_i$ a $\lambda_{a_{i,0}}((a_{i-1,1}, \dots, a_{i-1,v}) = (a_{i,1}, \dots, a_{i,v}))$. Odtud pro všechna $i, j > 0$ platí $a_{i,j} = a_{i-1,j} * a_{i,j-1}$.

V obecném případě bychom převedli invertování funkce R_1 na vyřešení v kvazigrupových rovnic o v neznámých.

Definice 3.3. Řekneme, že funkce $f : \mathbb{N} \to \mathbb{R}$ je *zanedbatelná*, jestliže pro všechna $k \in \mathbb{N}$ existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $n > n_0$ je $f(n) < \frac{1}{n^k}$.

Definice 3.4. Řekneme, že funkce $f : \{0,1\}^* \to \{0,1\}^*$ je *jednosměrná*, jestliže f je polynomiálně vyčíslitelná a pro každý pravděpodobnostní polynomiální algoritmus M platí, že funkce $p : \mathbb{N} \to \mathbb{R}$ je zanedbatelná:

$$p(v) = \Pr_{x \in \{0,1\}^v}(M(f(x)) \in f^{-1}(f(x))).$$

V této práci bychom chtěli rozebrat složitost invertování funkce R_1. Dopředu můžeme prozradit, že je-li $v = 3$, tak funkce $R_1 : Q^3 \to Q^3$ tvoří základ jedné varianty hašovací funkce Edon-R. Existují dvě možnosti, jak na tuto složitost pohlížet. Buď zafixujeme $v = 3$ a budeme počítat konkrétní počet elementárních kroků, který potřebujeme k invertování R_1. Nebo zvolíme obecnější model a budeme počítat složitost invertování R_1 v závislosti na parametru v. V této práci budeme rozebírat tento obecnější model. Naším cílem bude najít takové podmínky na kvazigrupu Q, za kterých by funkce R_1 mohla být jednosměrná. Základní definicí, z které budeme vycházet, je definice beztvaré kvazigrupy [6] - to jest kvazigrupy, která by neměla mít žádné matematické vlastnosti, které by mohly sloužit k snížení složitosti pro vyřešení nelineárních kvazigrupových rovnic (například (3.1)).

Definice 3.5. Kvazigrupu $(Q, *)$ nazveme *beztvarou*, jestliže platí následující podmínky:

1. $(Q, *)$ není komutativní,
2. $(Q, *)$ neobsahuje levou ani pravou jednotku,
3. $(Q, *)$ neobsahuje vlastní podkvazigrupu,
4. pro řády translací Q platí: $n_{Q,\lambda}, n_{Q,\rho} \geq 2|Q|$.

Poznámka 3.6. Z definice 3.5 snadno vyplývá, že v beztvaré kvazigrupě operace $*$ není asociativní, neboť dle lemma 2.2 je každá asociativní kvazigrupa grupou a ta obsahuje jednotku.

Hypotéza 3.7. *V beztvaré kvazigrupě* $(Q, *)$ *je funkce* $R_1 : Q^v \to Q^v$ *jednosměrná.*

Kapitola 4

Centrální kvazigrupy

Definice 4.1. Nechť $(G,+)$ je abelovská grupa. Kvazigrupu $(Q,*)$ nazveme *centrální* nad G, jestliže existují $\alpha,\beta \in \mathrm{Aut}(G)$ a $c \in G$ takové, že

$$x * y = \alpha(x) + \beta(y) + c. \tag{4.1}$$

Pro operace / a \ získáme jednoduchým odvozením ze vztahu (4.1) následující vyjádření:

$$\begin{aligned} x/y &= \alpha^{-1}(x) - \alpha^{-1}\beta(y) - \alpha^{-1}(c), \\ y\backslash x &= \beta^{-1}(x) - \beta^{-1}\alpha(y) - \beta^{-1}(c). \end{aligned}$$

Lemma 4.2. *Nechť $(Q,*)$ je centrální kvazigrupa. Potom*

$$\mathrm{Mlt}(Q) = \langle \mathrm{Mlt}(G), \alpha, \beta \rangle.$$

Důkaz. Dosazením definice centrální kvazigrupy do λ_x a ρ_x získáme

$$\begin{aligned} \lambda_x(y) &= x * y = \alpha(x) + \beta(y) + c = L_{\alpha(x)+c}\beta(y), \\ \rho_x(y) &= y * x = \alpha(y) + \beta(x) + c = L_{\beta(x)+c}\alpha(y) \end{aligned}$$

a tedy $\lambda_x = L_{\alpha(x)+c}\beta$ a $\rho_x = L_{\beta(x)+c}\alpha$. Jelikož zobrazení $x \mapsto \alpha(x) + c$ a $x \mapsto \beta(x) + c$ jsou permutace, tak existují $x, y \in Q$ takové, že $\lambda_x = L_0\alpha = \alpha$, $\rho_y = L_0\beta = \beta$. Dostáváme tedy $\langle \alpha, \beta \rangle \subseteq \mathrm{Mlt}(Q)$. Protože jistě $\alpha^{-1} \in \langle \alpha, \beta \rangle$, tak pro všechna $x \in G$ dostáváme $L_x = (L_x\alpha)\alpha^{-1} \in \mathrm{Mlt}(Q)$ a protože $R_x = L_x$ díky komutativitě operace $+$, tak $\mathrm{Mlt}(G) \subseteq \mathrm{Mlt}(Q)$. Na druhou stranu pro všechna $L_x\alpha, L_y\beta \in \mathrm{Mlt}(Q)$ jistě platí, že $L_x\alpha, L_y\beta \in \langle \mathrm{Mlt}(G), \alpha, \beta \rangle$ a proto $\mathrm{Mlt}(Q) = \langle \mathrm{Mlt}(G), \alpha, \beta \rangle$. □

V této kapitole budeme rozebírat centrální kvazigrupy vzhledem k podmínkám na beztvarost z definice 3.5. Charakteristika vzhledem k prvním dvěma podmínkám je triviální. Charakteristiku vzhledem ke třetí podmínce pojmeme více obecněji zapojením pojmu kongruence. Z odvozených podmínek bude zřejmé, že je snadné zkonstruovat centrální kvazigrupu vyhovující bodům 1 až 3 definice 3.5, ale jak ukážeme ve větě 4.9, tak žádná centrální kvazigrupa nesplňuje bod 4. Proto centrální kvazigrupy nejsou beztvaré.

Lemma 4.3. *Centrální kvazigrupa $(Q, *)$ je komutativní, právě když $\alpha = \beta$.*

Důkaz. Q je komutativní, právě když pro všechna $x, y \in Q$ je $x * y = y * x$ a to je, právě když $\alpha(x) + \beta(y) + c = \alpha(y) + \beta(x) + c$ a to je, právě když $\alpha(x - y) = \beta(x - y)$. Tedy Q je komutativní, právě když $\alpha = \beta$. □

Lemma 4.4. *Centrální kvazigrupa $(Q, *)$ obsahuje levou jednotku $e \in Q$, právě když $\alpha(e) = -c$ a zároveň β je identita na G. Podobně Q obsahuje pravou jednotku $f \in Q$, právě když $\beta(f) = -c$ a zároveň α je identita na G.*

Důkaz. Prvek $e \in Q$ je levá jednotka, právě když pro všechna $y \in Q$ je $e * y = y$ a to je, právě když $\alpha(e) + \beta(y) + c = y$. Volbou $y = 0$ dostáváme $\alpha(e) = -c$ a odtud $\beta = \mathrm{id}_G$. Analogicky pro pravou jednotku. □

Tvrzení 4.5. *Nechť $(Q, *)$ je centrální kvazigrupa nad grupou $(G, +)$. Potom existuje bijekce z množiny všech kongruencí Q do množiny všech α, β-invariantních podgrup P grupy G taková, že rozklad G modulo P je shodný s rozkladem Q modulo $\sim$, kde P je obraz $\sim$ v této bijekci.*

Důkaz. Jestliže Q obsahuje kongruenci $\sim$, pak dle tvrzení 2.7 rozklad Q modulo $\sim$ je rozkladem na bloky působení $\mathrm{Mlt}(Q)$ na Q. Jelikož dle lemma 4.2 platí $\mathrm{Mlt}(G) \subseteq \mathrm{Mlt}(Q)$, tak dle lemma 1.9 existuje $P \leq G$ taková, že Q modulo $\sim$ je shodný s rozkladem G modulo P. Protože dle lemma 4.2 také $\langle \alpha, \beta \rangle \subseteq \mathrm{Mlt}(Q)$ a protože $0 \in P$, tak $\alpha(P) = \beta(P) = P$ díky vlastnosti bloku působení.

Na druhou stranu je-li $P \leq G$ α, β-invariantní podgrupa G, pak G modulo P indukuje rozklad na bloky působení $\mathrm{Mlt}(Q) = \langle \mathrm{Mlt}(G), \alpha, \beta \rangle$, neboť všechna generující zobrazení zachovávají bloky tohoto rozkladu: $L_y(x+P) = (x + y) + P$, $\alpha(x + P) = \alpha(x) + P$ a $\beta(x + P) = \beta(x) + P$. Dle tvrzení 2.7 tedy dostáváme požadovanou kongruenci. □

Lemma 4.6. *Nechť $(Q, *)$ je centrální kvazigrupa s kongruencí σ. Potom kvazigrupa $Q/_\sigma$ je také centrální kvazigrupa.*

Důkaz. Existence kongruence implikuje dle tvrzení 4.5 existenci $P \leq G$ takové, že rozklad Q modulo σ je shodný s rozkladem G modulo P. Jelikož také $\alpha(P) = \beta(P) = P$, tak můžeme definovat $\bar{\alpha}, \bar{\beta} \in \mathrm{Aut}(G/P)$ předpisy $\bar{\alpha}(x+P) = \alpha(x)+P$ a $\bar{\beta}(x+P) = \beta(x)+P$. Pro všechna $x+P, y+P \in G/P$ platí, že

$$(x+P) * (y+P) = \bar{\alpha}(x+P) + \bar{\beta}(y+P) + (c+P). \quad \square$$

Tvrzení 4.7. *Nechť $(Q, *)$ je centrální kvazigrupa. Potom $Q_1 \subseteq Q$ je podkvazigrupa Q, právě když existuje α, β-invariantní podgrupa P grupy G a zároveň existuje $x \in G$ takové, že $x * x \in x + P = Q_1$.*

Důkaz. Položme $Q_1 = \{q_1, \ldots, q_l\}$ a $P = \{x - y : x, y \in Q_1\}$. Dokážeme, že P je α-invariantní podgrupa G. Platí:

$$\begin{aligned} \alpha(q_1) + \beta(Q_1) + c &= Q_1, \\ \alpha(q_2) + (\alpha(q_1) - \alpha(q_1)) + \beta(Q_1) + c &= Q_1, \\ \alpha(q_2) - \alpha(q_1) + (\alpha(q_1) + \beta(Q_1) + c) &= Q_1, \\ \alpha(q_2 - q_1) + Q_1 &= Q_1. \end{aligned}$$

Analogicky dojdeme k tomu, že $\alpha(q_j - q_1) + Q_1 = Q_1$ pro všechna $1 \leq j \leq l$. Zafixujeme-li j, potom existuje $\pi_j \in S_l$ taková, že $\alpha(q_j - q_1) + q_r = q_{\pi_j(r)}$ pro všechna $1 \leq r \leq l$. Z tohoto důvodu můžeme psát

$$\begin{aligned} \alpha(q_1 - q_1) &= q_{\pi_1(1)} - q_1 = q_{\pi_1(2)} - q_2 = \ldots = q_{\pi_1(l)} - q_l, \\ \alpha(q_2 - q_1) &= q_{\pi_2(1)} - q_1 = q_{\pi_2(2)} - q_2 = \ldots = q_{\pi_2(l)} - q_l, \\ &\vdots \\ \alpha(q_l - q_1) &= q_{\pi_l(1)} - q_1 = q_{\pi_l(2)} - q_2 = \ldots = q_{\pi_l(l)} - q_l. \end{aligned}$$

Díky tomu, že $\alpha \in \mathrm{Aut}(G)$, tak pro všechna $j \neq j'$ a $1 \leq i \leq l$ platí $\pi_j(i) \neq \pi_{j'}(i)$, tudíž $P = \{q_i - q_1 \,|\, 1 \leq i \leq l\}$ a $|P| = |Q_1|$. Dále dostáváme $Q_1 = q_1 + P$ a $\alpha(P) = P$. Nyní stačí dokázat, že P je podgrupa G:

$$\begin{aligned} (q_i - q_1) + (q_j - q_1) &= (q_i - q_1) + (q_{\pi_x(i)} - q_i) = q_{\pi_x(i)} - q_1 \\ -(q_i - q_1) &= q_1 - q_i = q_{\pi_y(1)} - q_1 \\ 0 &= q_1 - q_1 \end{aligned}$$

Na druhou stranu je-li $P \leq G$ α, β-invariantní podgrupa a $x * x \in x + P = Q_1$, potom pro všechna $x + p_1, x + p_2 \in Q_1$ platí:

$$(x + p_1) * (x + p_2) = \alpha(x) + \beta(x) + c + \alpha(p_1) + \beta(p_2) \in x + P = Q_1. \quad \square$$

Důsledek 4.8. *Nechť $(Q, *)$ je centrální kvazigrupa. Obsahuje-li Q podkvazigrupu Q_1, pak tato kvazigrupa indukuje kongruenci σ takovou, že jeden z bloků Q modulo σ je shodný s Q_1.*

Důkaz. Důkaz vyplývá přímo ze spojením tvrzení 4.5 a 4.7. □

Věta 4.9. *Nechť $(Q, *)$ je centrální kvazigrupa. Potom*

$$n_{Q,\lambda}, n_{Q,\rho} \leq |Q|.$$

Důkaz. Jelikož $x * y = \alpha(x) + \beta(y) + c$, tak $\lambda_x = L_{\alpha(x)+c}\beta$ a $\rho_x = L_{\beta(x)+c}\alpha$. Díky tomu, že zobrazení $x \mapsto \alpha(x)+c$ a $x \mapsto \beta(x)+c$ jsou permutace G, tak použijeme-li značení z kapitoly 1, dostáváme $n_{Q,\lambda} = n_\beta$ a $n_{Q,\rho} = n_\alpha$. Tvrzení potom plyne z věty 1.18. □

Kapitola 5

Po částech centrální kvazigrupy

V této kapitole zavedeme definici po částech centrální kvazigrupy, která má zabudován princip centrálních kvazigrup zvlášť pro jednotlivé dvojice bloků kongruence. Ukážeme, že taková kvazigrupa ale celkově centrální není a proto ztrácí část regularity v nich obsažené. Na základě po částech centrálních kvazigrup definujeme rekurzivně centrální kvazigrupy. Ukážeme, že v této třídě kvazigrup jsme schopni nalézt takové kvazigrupy, které splňují podmínky definice 3.5 (zvláště pak bod 4) a tedy jsou beztvaré. Zároveň jsou ale zkonstruovány na základě principu centrálních kvazigrup, což nám umožní efektivní řešení rovnic.

Ve větě 4.9 jsme představili horní mez na řády levých a pravých translací v centrálních kvazigrupách. O to samé se budeme snažit pro všechny třídy kvazigrup, které budeme uvažovat v této kapitole. Pro vyjádření této meze v obecných kvazigrupách zavedeme následující značení.

Definice 5.1. Nechť $n \in \mathbb{N}$. Potom definujeme

$$\psi(n) = \prod_{p^{k_l} \leq n < p^{k_l+1},\, p \in \mathbb{P}} p^{k_l}.$$

Lemma 5.2. *Pro všechna $a, b > 1$ platí, že $\psi(a)\psi(b) < \psi(ab)$.*

Důkaz. Je-li $p^{k_a} \leq a$ a $p^{k_b} \leq b$, pak jistě $p^{k_a} p^{k_b} \leq ab$ a proto $\psi(a)\psi(b) \leq \psi(ab)$. Bertrandův postulát říká, že pro všechna $n \geq 2$ existuje $p \in \mathbb{P}$ takové, že $n < p < 2n$. Proto existuje p takové, že $a, b < p < ab$ a tedy $\psi(a)\psi(b) < \psi(ab)$. □

Řád každé permutace je dán nejmenším společným násobkem délek cyklů z cyklického rozkladu permutace. Působí-li permutace φ na množině B, pak

délka každého cyklu je menší nebo rovna $|B|$ a proto $|\varphi|$ musí dělit $\psi(|B|)$. Aplikujeme-li tento fakt na levé translace kvazigrupy Q, pak zřejmě dostáváme, že $|\lambda_x|$ dělí $\psi(|Q|)$. Jelikož řád levých translací Q je nejmenším společným násobkem řádů λ_x, tak platí, že $n_{Q,\lambda}$ dělí $\psi(|Q|)$ a tedy

$$n_{Q,\lambda} \leq \psi(|Q|). \tag{5.1}$$

Získali jsme horní mez na řády levých translací pro obecné kvazigrupy. V této kapitole dále definujeme postupně konkrétnější třídy kvazigrup a s tímto postupem bude tato mez klesat.

Nechť kvazigrupa Q obsahuje vlastní kongruenci σ. V souladu s definicí 2.3 označíme $n_{Q/\sigma,\lambda}$ jako řád levých translací faktorkvazigrupy Q/σ. Nechť $x \in Q$ a nechť $k > 0$ je nejmenší takové, že $\sigma(\lambda_x^k(y), y)$ pro všechna $y \in Q$. Potom k je zřejmě řád $\lambda_{[x]_\sigma}$ v Q/σ. Díky slučitelnosti kongruence s kvazigrupovými operacemi zřejmě platí, že $\sigma(\lambda_x^{k+i}(y), \lambda_x^i(y))$ pro všechna $y \in Q$ a $i \in \mathbb{N}$. Protože kongruence jsou tranzitivní, tak dostáváme, že $\sigma(\lambda_x^j(y), y)$ pro všechna $y \in Q$, právě když $j = ik$ pro nějaké $i \in \mathbb{N}$. Protože $\sigma(\lambda_x^{|\lambda_x|}(y) = y, y)$ pro všechna $y \in Q$, tak k dělí $|\lambda_x|$. Dostáváme tedy, že $|\lambda_{[x]_\sigma}|$ dělí $|\lambda_x|$ a proto $n_{Q/\sigma,\lambda}$ dělí $n_{Q,\lambda}$. Definujeme pomocné zobrazení $\Lambda_x : Q \to Q$ předpisem pro všechna $y \in Q$:

$$\Lambda_x(y) = \lambda_x^{n_{Q/\sigma,\lambda}}(y).$$

Označíme $n_{Q,\lambda,\sigma}$ jako nejmenší společný násobek řádů zobrazení $\{\Lambda_x : x \in Q\}$. Přirozenou spojitost těchto definovaných hodnot zformulujeme v následujícím lemmatu.

Lemma 5.3. *Nechť $(Q, *)$ je kvazigrupa s kongruencí σ. Potom*

$$n_{Q,\lambda} = n_{Q/\sigma,\lambda} \cdot n_{Q,\lambda,\sigma}.$$

Důkaz. Nerovnost $n_{Q,\lambda} \leq n_{Q/\sigma,\lambda} \cdot n_{Q,\lambda,\sigma}$ vyplývá z definice, neboť jistě pro všechna $x \in Q$:

$$\lambda_x^{n_{Q/\sigma,\lambda} \cdot n_{Q,\lambda,\sigma}} = \left(\lambda_x^{n_{Q/\sigma,\lambda}}\right)^{n_{Q,\lambda,\sigma}} = \Lambda_x^{n_{Q,\lambda,\sigma}} = \mathrm{id}.$$

Na druhou stranu nechť p^{k_1} dělí $n_{Q/\sigma,\lambda}$ a nechť p^{k_2} dělí $n_{Q,\lambda,\sigma}$. Potom existuje $x \in Q$ takové, že p^{k_2} dělí řád $\Lambda_x = \lambda_x^{\left(\frac{n_{Q/\sigma,\lambda}}{p^{k_1}}\right)p^{k_1}}$. Odtud dostáváme, že $p^{k_1+k_2}$ dělí řád $\lambda_x^{\left(\frac{n_{Q/\sigma,\lambda}}{p^{k_1}}\right)}$ a proto $p^{k_1+k_2}$ dělí řád λ_x. Protože $p \in \mathbb{P}$ volíme libovolně, tak dostáváme $n_{Q,\lambda} \geq n_{Q/\sigma,\lambda} \cdot n_{Q,\lambda,\sigma}$. □

Protože pro všechna $y \in Q$: $\sigma(\Lambda_x(y), y)$, tak každý blok Q modulo σ je Λ_x-invariantní. Proto délka každého cyklu v cyklickém rozkladu permutace Λ_x je menší nebo rovna velikosti bloku. Proto $|\Lambda_x|$ dělí $\psi(\kappa_\sigma)$ a proto také $n_{Q,\lambda,\sigma}$ dělí $\psi(\kappa_\sigma)$. Dostáváme tedy

$$n_{Q,\lambda} \leq \psi\left(|Q/_\sigma|\right) \cdot \psi(\kappa_\sigma) < \psi(|Q|), \tag{5.2}$$

kde neostrá nerovnost vyplývá z lemma 5.3 a ostrá nerovnost vyplývá z lemma 5.2. Tudíž přítomností kongruence v kvazigrupě jsme získali ostře nižší horní mez na řády levých translací. Nyní přistoupíme k zavedení principu centrálních kvazigrup na jednotlivé bloky kongruence.

Definice 5.4. Nechť $(G, \odot)$ je grupa a $(H, +)$ je abelovská podgrupa G. Zvolme pevně $b_i \in G$ tak, že $\{b_i \odot H : 1 \leq i \leq k\}$ je levý rozklad G modulo H. Nechť kvazigrupa $(Q, *)$ obsahuje kongruenci σ takovou, že rozklad Q modulo σ je shodný s levým rozkladem G modulo H. Potom Q nazveme *po částech centrální* nad grupami G a H, jestliže pro $1 \leq i, j \leq k$ existují $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ a $c_{i,j} \in H$ takové, že pro $(b_i \odot H) * (b_j \odot H) = b_l \odot H$ a všechna $x, y \in H$:

$$(b_i \odot x) * (b_j \odot y) = b_l \odot (\alpha_{i,j}(x) + \beta_{i,j}(y) + c_{i,j}).$$

Poznámka 5.5. Grupa $(G, \odot)$ je použita v definici 5.4 pouze jako nosná množina kvazigrupy. Každý prvek z Q vyjádříme jednoznačně jako $b_i \odot h$ pro nějaké $1 \leq i \leq k$ a $h \in H$. Operace $\odot$ a $+$ mají v definici odlišný význam a proto jsme zvolili různé symboly. V dalším textu budeme často pro obě operace používat symbol jeden.

Lemma 5.6. *Nechť $(Q, *)$ a $(Q', *')$ jsou po částech centrální kvazigrupy nad grupami G a H definované pomocí stejných $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$, $c_{i,j} \in H$. Nechť zvolené množiny reprezentantů $\{b_i\}_{i=1}^k$ a $\{b'_i\}_{i=1}^k$ bloků G modulo H jsou pro kvazigrupy Q a Q' libovolné. Potom kvazigrupy Q a Q' jsou izomorfní.*

Důkaz. Izomorfismus $\varphi : Q \to Q'$ je dán přirozeným předpisem $\varphi(b_i \odot x) = (b'_i \odot x)$, neboť

$$\begin{aligned}
\varphi((b_i \odot x) * (b_j \odot y)) &= \varphi(b_l \odot (\alpha_{i,j}(x) + \beta_{i,j}(y) + c_{i,j})) \\
&= b'_l \odot (\alpha_{i,j}(x) + \beta_{i,j}(y) + c_{i,j}) \\
&= (b'_i \odot x) * (b'_j \odot y) \\
&= \varphi(b_i \odot x) * \varphi(b_j \odot y). \qquad \square
\end{aligned}$$

Každá centrální kvazigrupa $(Q, *)$ nad grupou $(G, +)$ je po částech centrální nad grupami G a G, neboť dle lemma 5.6 můžeme volit reprezentant jediného bloku G/G roven 0 a tedy parametry po částech centrální kvazigrupy zvolíme přímo $\alpha_{1,1} = \alpha$, $\beta_{1,1} = \beta$ a $c_{1,1} = c$:

$$0 + (\alpha_{1,1}(x) + \beta_{1,1}(y) + c_{1,1}) = \alpha(x) + \beta(y) + c.$$

V následujícím lemma ukážeme, že jestliže Q obsahuje vlastní kongruenci, pak na Q můžeme pohlížet jako na po částech centrální kvazigrupu působící na této kongruenci.

Lemma 5.7. *Nechť $(Q, *)$ je centrální kvazigrupa nad grupou $(G, +)$ s kongruencí σ. Potom existuje H podgrupa G taková, že Q je po částech centrální nad G a H a rozklad Q modulo σ je shodný s rozkladem G modulo H.*

Důkaz. Dle tvrzení 4.5 existuje H podgrupa G taková, že rozklad Q modulo σ je shodný s rozkladem G modulo H. Ukážeme, že na Q lze pohlížet jako na po částech centrální kvazigrupu nad grupami G a H. Je-li $\{b_i\}_{i=1}^{k}$ množina reprezentantů bloků modulo H, pak pro všechna $1 \leq i, j \leq k$ položíme $\alpha_{i,j} = \alpha \restriction H$, $\beta_{i,j} = \beta \restriction H$ a pro $(b_i + H) * (b_j + H) = b_l + H$ položíme $c_{i,j} = \alpha(b_i) + \beta(b_j) + c - b_l \in H$. Díky tomu, že operace $+$ je komutativní z definice centrální kvazigrupy, tak dostáváme:

$$\begin{aligned}
(b_i + x) * (b_j + y) &= \alpha(b_i + x) + \beta(b_j + y) + c \\
&= \alpha(b_i) + \alpha(x) + \beta(b_j) + \beta(y) + c + b_l - b_l \\
&= b_l + (\alpha(x) + \beta(y) + (\alpha(b_i) + \beta(b_j) + c - b_l)) \\
&= b_l + (\alpha_{i,j}(x) + \beta_{i,j}(y) + c_{i,j}).
\end{aligned}$$

Tedy kvazigrupa $(Q, *)$ je shodná s po částech centrální kvazigrupou nad G a H definovanou parametry $\alpha_{i,j}$, $\beta_{i,j} \in \mathrm{Aut}(H)$ a $c_{i,j} \in H$. □

Značení. V následujícím příkladu i ve všech dalších budeme uvažovat vektory z vektorového prostoru $\mathbb{Z}_2^n$ ve sloupcové notaci. Tedy například $c = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = (1\,0\,1)^T \in \mathbb{Z}_2^3$.

Příklad. Při konstrukci konkrétního příkladu po částech centrální kvazigrupy vyjdeme z centrální kvazigrupy s vlastní kongruencí. Dle lemma 5.7 je tato kvazigrupa po částech centrální. Tuto kvazigrupu následně použijeme jako šablonu pro konstrukci po částech centrální kvazigrupy, která ale

		β							
	$*_1$	0	1	2	3	4	5	6	7
α	0	0	1	3	2	4	5	7	6
	1	1	0	2	3	5	4	6	7
	2	2	3	1	0	6	7	5	4
	3	3	2	0	1	7	6	4	5
	4	7	6	4	5	3	2	0	1
	5	6	7	5	4	2	3	1	0
	6	5	4	6	7	1	0	2	3
	7	4	5	7	6	0	1	3	2

		β_1				β_2			
	$*_2$	0	1	2	3	4	5	6	7
α_1	0	0	1	3	2	4	6	5	7
	1	1	0	2	3	5	7	4	6
	2	2	3	1	0	6	4	7	5
	3	3	2	0	1	7	5	6	4
α_2	4	4	5	7	6	0	2	1	3
	5	7	6	4	5	3	1	2	0
	6	6	7	5	4	2	0	3	1
	7	5	4	6	7	1	3	0	2

Tabulka 5.1: V levé tabulce je centrální kvazigrupa Q_1 definovaná pomocí $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_2^3)$, v pravé pak po částech centrální kvazigrupa Q_2 definovaná pomocí $\alpha_1 = \alpha_{1,i}$, $\alpha_2 = \alpha_{2,i}$, $\beta_1 = \beta_{i,1}$ a $\beta_2 = \beta_{i,2}$, kde $\alpha_i, \beta_i \in \mathrm{Aut}(H)$, $H \simeq \mathbb{Z}_2^2$.

již nebude centrální. Dosáhneme toho pouhou změnou některých parametrů $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ a $c_{i,j} \in H$.

Nechť $(Q_1, *_1)$ je centrální kvazigrupa nad grupou $G = (\mathbb{Z}_2^3, \oplus)$ definovaná pomocí automorfismů $\alpha, \beta \in \mathrm{Aut}(G)$ indukovaných maticemi $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ a prvkem $c = (0\,0\,0)^T$. Snadno se přesvědčíme, že podgrupa

$$H = \langle (0\,1\,0)^T, (0\,0\,1)^T \rangle \subset \mathbb{Z}_2^3$$

je α, β-invariantní a proto dle tvrzení 4.5 kvazigrupa Q_1 obsahuje kongruenci σ takovou, že rozklad Q_1 modulo σ je shodný s rozkladem G modulo H. Pevně zvolíme reprezentanty $b_1 = (0\,0\,0)^T$ a $b_2 = (1\,0\,0)^T$ obou dvou bloků G modulo H. Kvazigrupa Q_1 je po částech centrální nad grupami G a H, kde příslušné automorfismy $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ vzniknou jako restrikce α, β na podgrupu H a kde snadno dopočítáme prvky $c_{1,1} = c_{1,2} = (0\,0\,0)^T$ a $c_{2,1} = c_{2,2} = (0\,1\,1)^T$.

Nyní na základě této šablony definujeme po částech centrální kvazigrupu $(Q_2, *_2)$. Podgrupa H je izomorfní $(\mathbb{Z}_2^2, \oplus)$, kde příslušný izomorfismus je dán: $(x_1, x_2, x_3) \mapsto (x_2, x_3)$. Definujeme tedy $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ pomocí příslušných matic automorfismů $A_{i,j}, B_{i,j} \in \mathrm{M}_2(\mathbb{Z}_2)$. Abychom zdůraznili korespondenci s Q_1, tak pro dvojici bloků $(b_1 \oplus H, b_1 \oplus H)$ zachováme původní automorfismy (samozřejmě v restrikci na H):

$$A_1 \;=\; A_{1,1} = A_{1,2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{aligned} A_2 &= A_{2,1} = A_{2,2} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \\ B_1 &= B_{1,1} = B_{2,1} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \\ B_2 &= B_{1,2} = B_{2,2} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right). \end{aligned}$$

Pro jednoduchost položíme $c_{i,j} = (0\,0\,0)^T \in H$ pro $1 \leq i, j \leq 2$. Potom Caleyho tabulky kvazigrup Q_1 a Q_2 můžeme nalézt v tabulce 5.1, kde bijekce $\varphi : \mathbb{Z}_2^3 \to \mathbb{Z}_8$ je dána standartně převodem z binární do desítkové soustavy.

Řád levých translací v po částech centrální kvazigrupách: Tento problém bychom podobně jako v centrálních kvazigrupách chtěli převést na počítání řádů prvků holomorfu grupy. Protože zobrazení λ_x nezachovávají jednotlivé bloky modulo H, tak nejsme schopni jednoduše vyjádřit λ_x^i jako prvek holomorfu H. Proto využijeme zobrazení Λ_x, které už jednotlivé bloky modulo H zachovávají. Odvodíme přesnou formuli pro zobrazení Λ_x, která se ale bude lišit pro jednotlivé dvojice bloků.

Bez újmy na obecnosti zvolme pevně $B_1, B_2 \in G/H$. Nechť $b_1 \in B_1$, $b_2 \in B_2$ jsou jejich reprezentanti. Označme $r = n_{Q/\sigma,\lambda}$. Definujeme posloupnost $1 \leq j_0, \ldots, j_r \leq k$ tak, aby vyjadřovala jednotlivé bloky do nichž padne prvek z bloku B_2 působíme-li na něj levou translací určenou prvkem z bloku B_1. Tedy tak, aby $\lambda_{b_1}^i(b_2) \in B_{j_i}$. Zřejmě platí: $j_0 = j_r = 2$. Jestliže $x, y \in H$, pak dosazením definice po částech centrální kvazigrupy dostáváme

$$\begin{aligned} \lambda_{b_1 \odot x}(b_2 \odot y) &= b_{j_1} \odot (\alpha_{1,2}(x) + \beta_{1,2}(y) + c_{1,2}), \\ \lambda_{b_1 \odot x}^2(b_2 \odot y) &= b_{j_2} \odot (\alpha_{1,j_1}(x) + \beta_{1,j_1}(\alpha_{1,2}(x) + \beta_{1,2}(y) + c_{1,2}) + c_{1,j_1}) \\ &= b_{j_2} \odot ((\alpha_{1,j_1} + \beta_{1,j_1}\alpha_{1,2})(x) + (\beta_{1,j_1}\beta_{1,2})(y) + \\ &\qquad + \beta_{1,j_1}(c_{1,2}) + c_{1,j_1}), \\ &\vdots \\ \Lambda_{b_1 \odot x}(b_2 \odot y) &= b_2 \odot (\zeta_{1,2}(x) + \eta_{1,2}(y) + d_{1,2}) \\ &= b_2 \odot (L_{(\zeta_{1,2}(x)+d_{1,2})}\eta_{1,2}(y)), \end{aligned}$$

kde $\zeta_{1,2} \in \mathrm{End}(H)$, $\eta_{1,2} \in \mathrm{Aut}(H)$ a $d_{1,2} \in H$ jsou definovány předpisy

$$\zeta_{1,2} = \sum_{i=0}^{r-1} \beta_{1,j_{r-1}} \circ \ldots \circ \beta_{1,j_{i+1}} \circ \alpha_{1,j_i}, \tag{5.3}$$

$$\eta_{1,2} = \beta_{1,j_{r-1}} \circ \ldots \circ \beta_{1,j_1} \circ \beta_{1,2}, \tag{5.4}$$

$$d_{1,2} = \sum_{i=0}^{r-1} \beta_{1,j_{r-1}}(\ldots(\beta_{1,j_{i+1}}(c_{1,j_i}))). \tag{5.5}$$

Analogicky bychom definovali $\zeta_{i,j}, \eta_{i,j}$ a $d_{i,j}$ pro všechny dvojice bloků $B_i, B_j \in G/H$. Pro všechna $1 \leq i \leq k$ a $x \in H$ zřejmě dostáváme

$$|\Lambda_{(b_i \odot x)}| = \mathrm{NSN}(|L_{\zeta_{i,j}(x)+d_{i,j}} \eta_{i,j}| : 1 \leq j \leq k). \tag{5.6}$$

Tvrzení 5.8. *Nechť $(Q, *)$ je po částech centrální kvazigrupa nad grupami G a H. Potom*

$$\mathrm{NSN}(|\eta_{i,j}| : 1 \leq i, j \leq k) \leq n_{Q,\lambda,\sigma} \leq |H| \cdot |\mathrm{Aut}(H)|.$$

Důkaz. Dolní mez plyne přímo z faktu, že $|\varphi|$ dělí $|L_x \varphi|$. Horní mez plyne z faktu, že $\mathrm{Hol}(H)$ je semidirektním součinem H a $\mathrm{Aut}(H)$. Tudíž řád každého prvku $\mathrm{Hol}(H)$ dělí $|H| \cdot |\mathrm{Aut}(H)|$. □

Dosazením výsledků z tvrzení 5.8 do vztahu z lemma 5.3 získáme horní mez na řády translací v po částách centrálních kvazigrupách:

$$\begin{aligned} n_{Q,\lambda} &\leq n_{Q/\sigma,\lambda} \cdot n_{Q,\lambda,\sigma} \leq \\ &\leq \psi(|Q/\sigma|) \cdot |H| \cdot |\mathrm{Aut}(H)|. \end{aligned} \tag{5.7}$$

Definice 5.9. Posloupnost kongruencí $\{\sigma_i\}_{i=0}^{l}$ kvazigrupy Q nazveme *filtrací*, jestliže platí

$$Q \times Q = \sigma_0 \supset \sigma_1 \supset \ldots \supset \sigma_l = \mathrm{id}_Q.$$

Značení. Nechť $\sigma_1 \supset \sigma_2$ jsou kongruence kvazigrupy Q. Definujeme relaci $\sigma_1' \subset Q/_{\sigma_2} \times Q/_{\sigma_2}$ předpisem: $\sigma_1'([x]_{\sigma_2}, [y]_{\sigma_2})$, právě když $\sigma_1(x, y)$. Potom σ_1' je zřejmě kongruence $Q/_{\sigma_2}$. Kongruenci σ_1 tedy můžeme vnímat jako kongruenci Q nebo $Q/_{\sigma_2}$. Dále nebudeme používat notaci σ_1' a z kontextu vždy poznáme k jaké kvazigrupě se kongruence σ_1 vztahuje.

Definice 5.10. Kvazigrupu $(Q, *)$ nazveme *rekurzivně centrální* nad grupami $\{G_i\}_{i=1}^{l}$ a $\{H_i\}_{i=1}^{l}$, jestliže obsahuje filtraci $\{\sigma_i\}_{i=0}^{l}$ takovou, že pro všechna $1 \leq i \leq l$:

1. kvazigrupa $Q/_{\sigma_i}$ je po částech centrální nad grupami G_i a H_i,
2. rozklad $Q/_{\sigma_i}$ modulo σ_{i-1} je shodný s rozkladem G_i modulo H_i.

Poznámka 5.11. Nechť $\sigma_1 \supset \sigma_2$ jsou kongruence Q. Nechť $Q/_{\sigma_2}$ je po částech centrální nad grupami G a H. Nechť rozklad $Q/_{\sigma_2}$ modulo σ_1 je

shodný s rozkladem G modulo H. Vnímáme-li σ_1 jako kongruenci $Q/_{\sigma_2}$, pak $|H| = \kappa_{\sigma_1}$. Vnímáme-li σ_1 jako kongruenci Q, pak

$$|H| = \frac{|Q/_{\sigma_2}|}{|Q/_{\sigma_1}|} = \frac{\frac{|Q|}{|Q/_{\sigma_1}|}}{\frac{|Q|}{|Q/_{\sigma_2}|}} = \frac{\kappa_{\sigma_1}}{\kappa_{\sigma_2}}.$$

Když budeme v rekurzivně centrální kvazigrupě uvažovat velikost bloku kongruence nebo velikost H, budeme vždy vnímat všechny σ_i jako kongruence Q. Proto dle poznámky 5.11 dostáváme pro všechna $1 \leq i \leq k$:

$$|G_i| = |Q/_{\sigma_i}| \text{ a } |H_i| = \frac{\kappa_{\sigma_{i-1}}}{\kappa_{\sigma_i}}. \tag{5.8}$$

Jelikož $\sigma_0 = Q \times Q$, tak $\kappa_{\sigma_0} = |Q|$ a dostáváme:

$$|H_1| = \frac{|Q|}{\kappa_{\sigma_1}} = |Q/_{\sigma_1}| = |G_1|.$$

Proto je kvazigrupa $Q/_{\sigma_1}$ centrální nad abelovskou grupou $G_1 = H_1$. Je snadné nahlédnout, že každá centrální kvazigrupa nad grupou G je rekurzivně centrální nad grupami $G_1 = G$ a $H_1 = G$, kde příslušná filtrace je tvaru $Q \times Q = \sigma_0 \supset \sigma_1 = \mathrm{id}_Q$. Dokonce, je-li Q centrální kvazigrupa nad grupou G, která obsahuje vlastní kongruenci σ, pak dle lemma 5.7 existuje grupa H taková, že Q je po částech centrální nad G a H a rozklad Q modulo σ je shodný s rozkladem G modulo H. Dle lemma 4.6 je $Q/_{\sigma}$ centrální kvazigrupa nad G/H a proto na Q můžeme pohlížet jako na rekurzivně centrální kvazigrupu nad grupami $G_1 = G/H$, $G_2 = G$ a $H_1 = G/H$, $H_2 = H$, přičemž příslušná filtrace je tvaru $Q \times Q = \sigma_0 \supset \sigma_1 = \sigma \supset \sigma_2 = \mathrm{id}_Q$. Na druhou stranu rekurzivně centrální kvazigrupy nejsou zobecněním po částech centrálních kvazigrup (i když je používají ve své definici), neboť je-li Q po částech centrální nad G a H ($|H| < |G|$) a σ příslušná kongruence, tak uvažujeme-li přirozenou filtraci $Q \times Q = \sigma_0 \supset \sigma_1 = \sigma \supset \sigma_2 = \mathrm{id}_Q$, dostáváme, že sice $Q = Q/_{\sigma_2}$ je po částech centrální nad G a H, ale obecně kvazigrupa $Q/_{\sigma_1}$ není po částech centrální.

Poznámka 5.12. Ze vztahu (5.8) vyplývá jednoduché pozorování

$$\prod_{i=1}^{l} |H_i| = \prod_{i=1}^{l} \frac{\kappa_{\sigma_{i-1}}}{\kappa_{\sigma_i}} = \frac{\kappa_{\sigma_0}}{\kappa_{\sigma_l}} = \frac{|Q|}{1} = |Q|. \tag{5.9}$$

Tvrzení 5.13. *Nechť $(Q,*)$ je rekurzivně centrální kvazigrupa nad grupami $\{G_i\}_{i=1}^l$ a $\{H_i\}_{i=1}^l$. Nechť $\{\sigma_i\}_{i=0}^l$ je příslušná filtrace. Potom*

$$n_{Q,\lambda} = \prod_{i=1}^{l} n_{Q/_{\sigma_i},\lambda,\sigma_{i-1}}.$$

Důkaz. Budeme dokazovat indukcí dle hodnoty l. Jestliže $l = 1$, tak snadno dostáváme:

$$n_{Q/_{\sigma_1},\lambda,\sigma_0} = n_{Q/_{\sigma_1},\lambda} = n_{Q,\lambda}.$$

Nechť $l > 1$ a nechť tvrzení platí pro všechny menší hodnoty. Z lemma 5.3 plyne, že

$$n_{Q,\lambda} = n_{Q/_{\sigma_l},\lambda} = n_{Q/_{\sigma_{l-1}},\lambda} \cdot n_{Q/_{\sigma_l},\lambda,\sigma_{l-1}}. \tag{5.10}$$

Zřejmě platí, že kvazigrupa $Q/_{\sigma_{l-1}}$ je rekurzivně centrální nad grupami $\{G_i\}_{i=1}^{l-1}$ a $\{H_i\}_{i=1}^{l-1}$, kde příslušná filtrace je $\{\sigma_i\}_{i=0}^{l-1}$. Z indukčího předpokladu tedy máme $n_{Q/_{\sigma_{l-1}},\lambda} = \prod_{j=1}^{l-1} n_{Q/_{\sigma_i},\lambda,\sigma_{i-1}}$ a tvrzení získáme dosazením do (5.10). □

Důsledek 5.14. *Nechť $(Q,*)$ je rekurzivně centrální kvazigrupa nad grupami $\{G_i\}_{i=1}^l$ a $\{H_i\}_{i=1}^l$. Potom*

$$n_{Q,\lambda} \leq |H_1| \cdot \prod_{i=2}^{l} |H_i| \cdot |\mathrm{Aut}(H_i)|.$$

Příklad. Nyní představíme konkrétní příklad rekurzivně centrální kvazigrupy, která bude beztvará. Nechť G je grupa a H její vlastní abelovská podgrupa. Budeme uvažovat dvě úrovně (tedy $l = 2$) rekurzivně centrální kvazigrupy. Nejdříve definujeme centrální kvazigrupu $Q/_{\sigma_1}$ nad grupou $G_1 = H_1 = G/H$. Ve druhé fázi konstrukce ztotožníme prvky $Q/_{\sigma_1}$ s bloky kvazigrupy $Q = Q/_{\sigma_2}$ modulo kongruenci σ_1. Kvazigrupu $Q/_{\sigma_2}$ definujeme tak, aby byla po částech centrální nad grupami $G_2 = G$ a $H_2 = H$.

Konkrétní nosné množiny, se kterými budeme pracovat, jsou $G = (\mathbb{Z}_2^7, \oplus)$ a $H \cong (\mathbb{Z}_2^5, \oplus)$, $H \leq G$. Zřejmě platí, že $G/H \cong (\mathbb{Z}_2^2, \oplus)$. Parametry centrální kvazigrupy $Q/_{\sigma_1}$ zvolíme tak, aby neobsahovala vlastní podkvazigrupu, protože jinak by tato podkvazigrupa indukovala podkvazigrupu celé Q. Vyhovujícími parametry jsou například $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ a $c = (0\,1)^T$. Potom Caleyho tabulka $Q/_{\sigma_1}$ má následující tvar (opět používáme standartní bijekci $\varphi : \mathbb{Z}_2^2 \to \mathbb{Z}_4$):

$*$	0	1	2	3
0	1	0	2	3
1	2	3	1	0
2	3	2	0	1
3	0	1	3	2

Z tabulky vyčteme, že $|\lambda_1| = 4$ a proto $n_{Q/_{\sigma_1},\lambda} = 4$, neboť dle věty 4.9 je toto nejvyšší možný řád levých translací centrálních kvazigrup. Analogicky dostáváme, že $|\rho_0| = 4$ a proto $n_{Q/_{\sigma_1},\rho} = 4$. Prvky kvazigrupy $Q/_{\sigma_1}$ představují jednotlivé bloky Q modulo σ_1. Na těchto blocích vystavíme po částech centrální kvazigrupu. Nechť

$$H = \langle (0\,0\,0\,0\,0\,0\,1), (0\,0\,0\,0\,0\,1\,0), (0\,0\,0\,0\,1\,0\,0), (0\,0\,0\,1\,0\,0\,0), (0\,0\,1\,0\,0\,0\,0)\rangle \subset G.$$

Vybereme reprezentanty G modulo H:

$$\begin{aligned} b_1 &= (0\,0\,0\,0\,0\,0\,0), \\ b_2 &= (0\,1\,0\,0\,0\,0\,0), \\ b_3 &= (1\,0\,0\,0\,0\,0\,0), \\ b_4 &= (1\,1\,0\,0\,0\,0\,0). \end{aligned}$$

Uvažujme prozatím pro všechna $1 \leq i, j \leq 4$ obecné $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ a položme dopředu $c_{i,j} = 0$. Z multiplikativní tabulky kvazigrupy $Q/_{\sigma_1}$ dostáváme: $[b_1]_{\sigma_1} * [b_3]_{\sigma_1} = [b_3]_{\sigma_1}$ a $[b_1]_{\sigma_1} * [b_4]_{\sigma_1} = [b_4]_{\sigma_1}$. Bloky $(b_3 \oplus H)$ a $(b_4 \oplus H)$ jsou tedy zřejmě pro všechna $x \in H$ $\lambda_{b_1 \oplus x}$-invariantní. Dosazením do vzorců (5.3), (5.4) a (5.5), které jsme odvodili v této kapitole, získáváme pro všechna $x, y \in H$:

$$\begin{aligned} \Lambda_{b_1\oplus x}(b_3 \oplus y) &= b_3 \oplus (L_{\bigoplus_{i=0}^{3} \beta_{1,3}^i \alpha_{1,3}(x)} \beta_{1,3}^4(y)), \\ \Lambda_{b_1\oplus x}(b_4 \oplus y) &= b_4 \oplus (L_{\bigoplus_{i=0}^{3} \beta_{1,4}^i \alpha_{1,4}(x)} \beta_{1,4}^4(y)). \end{aligned}$$

Zřejmě platí, že $|\beta_{1,3}^4|$ a $|\beta_{1,4}^4|$ dělí $|\Lambda_{b_1\oplus x}|$. Volbou vhodných parametrů $\beta_{1,3}, \beta_{1,4} \in \mathrm{Aut}(H)$ jistě dosáhneme toho, že $|\Lambda_{b_1\oplus x}| > |H|$. Konkrétní kandidáty definujeme pomocí jejich matic automorfismů $B_{1,3}, B_{1,4} \in \mathrm{M}_5(\mathbb{Z}_2)$:

$$B_{1,3} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \; B_{1,4} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Snadno se přesvědčíme, že $|\beta_{1,3}| = 5$ a $|\beta_{1,4}| = 31$. Odkud plyne, že $|\beta_{1,3}^4| = 5$ a $|\beta_{1,4}^4| = 31$. Odkud plyne, že 155 dělí $n_{Q/_{\sigma_2},\lambda,\sigma_1}$. A proto tedy:

$$n_{Q,\lambda} = n_{Q/_{\sigma_1},\lambda,\sigma_0} \cdot n_{Q/_{\sigma_2},\lambda,\sigma_1} \geq 4 \cdot 155 = 620 > 2 \cdot 2^7 = 2|Q|.$$

Protože platí $[b_1]_{\sigma_1} * [b_2]_{\sigma_1} = [b_1]_{\sigma_1}$ a $[b_3]_{\sigma_1} * [b_2]_{\sigma_1} = [b_3]_{\sigma_1}$, tak bloky $(b_1 \oplus H)$ a $(b_3 \oplus H)$ jsou pro všechna $x \in H$ $\rho_{b_2 \oplus x}$-invariantní. Tudíž stejným postupem a volbou $A_{1,2} = B_{1,3}$, $A_{3,2} = B_{1,4}$ dosáhneme toho, že

$$n_{Q,\rho} \geq 620 > 2 \cdot 2^7 = 2|Q|.$$

Dodefinováním dalších parametrů $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ bychom jistě byli schopni sestrojit kvazigrupu s vyšším řádem levých i pravých translací, ale to nebylo naším cílem. Z konkrétního tvaru kvazigrupy $Q/_{\sigma_1}$, kterou jsme definovali celou, snadno nahlédneme, že Q neobsahuje žádnou jednotku a Q není komutativní. Tudíž rekurzivně centrální kvazigrupa Q je beztvará.

Kapitola 6

Složitost řešení rovnic

V této kapitole budeme rozebírat složitost řešení kvazigrupových rovnic pro jednotlivé typy kvazigrup, které jsme doposud definovali. Je-li Q obecná kvazigrupa, pak jediná metoda, kterou můžeme využít k vyřešení libovolné soustavy, je prohledávání hrubou silou - tedy vyzkoušení všech možných řešení. Základní třídou kvazigrup, v kterých umíme řešit rovnice efektivně, jsou centrální kvazigrupy nad abelovskými elemetnárními grupami. Tento princip následně přeneseme i napočástech centrální a rekurzivně centrální kvazigrupy nad abelovskými elementárními grupami.

Centrální kvazigrupy: Nechť $(Q, *)$ je centrální kvazigrupa nad abelovskou grupou $(G, +)$ definovaná pomocí $\alpha, \beta \in \mathrm{Aut}(G)$ a $c \in G$. Označíme q jako exponent grupy G. Potom pro každý term $f \in Q(x_1, \ldots, x_v)$ definujeme zobrazení

$$\begin{aligned} \mu : Q(x_1, \ldots, x_v) &\rightarrow \mathbb{Z}_q[\alpha, \beta](x_1, \ldots, x_v), \\ \nu : Q(x_1, \ldots, x_v) &\rightarrow G, \end{aligned}$$

které vyjadřují substituci definice centrální kvazigrupy za operace $*, /$ a $\backslash$. Přičemž zobrazení μ představuje nekonstantní část výsledného vyjádření a ν konstantní část. Formální předpis těchto zobrazení nebudeme definovat, ale postup je přímočarý a využívá toho, že α, β jsou homomorfismy, a toho, že grupová operace je komutativní.

Příklad. Uvažujme term $f_1 \in Q(x_1, x_2)$ tvaru $(x_1 * x_2) * x_1$. Dosazením definice centrální kvazigrupy za operaci $*$ získáme předpis $\alpha(\alpha(x_1) + \beta(x_2) + c) + \beta(x_1) + c$. Roznásobením a úpravou dostáváme $\nu(f) = \alpha(c) + c$ a

$$\mu(f) = (\alpha^2 + \beta)(x_1) + (\alpha\beta)(x_2).$$

Příklad. Uvažujme term $f_2 \in Q(x_1, x_2)$ tvaru $(x_1 * x_2)/x_1$. Dosazením definice centrální kvazigrupy za operace $*$ a $/$ získáme předpis $\alpha^{-1}(\alpha(x_1) + \beta(x_2)+c)-\alpha^{-1}\beta(x_1)-\alpha^{-1}(c)$. Roznásobením a úpravou dostáváme $\nu(f) = 0$ a

$$\mu(f) \quad = \quad (\mathrm{id} - \alpha^{-1}\beta)(x_1) + (\alpha^{-1}\beta)(x_2).$$

Centrální kvazigrupy nad elementárními abelovskými grupami: Je-li G elementární abelovská grupa řádu p^m, pak okruh $\mathbb{Z}_p[\alpha, \beta]$ lze chápat jako podokruh maticového okruhu $\mathrm{M}_m(\mathbb{Z}_p)$. Proto po roznásobení a úpravě lze každý prvek z okruhu $\mathbb{Z}_p[\alpha, \beta](x_1, \ldots, x_v)$ zapsat ve standartním tvaru

$$A_1 \cdot x_1 + A_2 \cdot x_2 + \ldots + A_v \cdot x_v,$$

kde $A_i \in \mathrm{M}_m(\mathbb{Z}_p)$. Matici $M \in \mathbb{Z}_p^{m \times mv}$ definovanou předpisem

$$M = (A_1, \ldots, A_v)$$

nazveme *maticí indukovanou termem* f. Nechť $\mathcal{E} = \langle f_1, f_2 \rangle \in \mathcal{E}_v$. Nechť $M_1, M_2 \in \mathbb{Z}_p^{m \times mv}$ jsou matice indukované termy f_1 a f_2. Poté matici $M = M_1 - M_2$ nazveme *maticí indukovanou rovnicí* $\mathcal{E}$. Prvky $\nu(f_1), \nu(f_2) \in G$ ztotožníme s příslušnými prvky vektorového prostoru $\mathbb{Z}_p^m$ a definujeme zobrazení $\nu : \mathcal{E}_v \to \mathbb{Z}_p^m$ předpisem $\nu(\mathcal{E}) = \nu(f_2) - \nu(f_1)$. Potom každé řešení $(x_1, \ldots, x_v) \in Q^v$ kvazigrupové rovnice $\mathcal{E}$ odpovídá řešení $x = (x_1, \ldots, x_v)^T \in \mathbb{Z}_p^{mv}$ soustavy lineárních rovnic nad tělesem $\mathbb{Z}_p$:

$$M \cdot x = \nu(\mathcal{E}). \tag{6.1}$$

Nechť $\mathcal{E} = (\langle f_{1,1}, f_{1,2} \rangle, \ldots, \langle f_{1,1}, f_{1,2} \rangle) \in \mathcal{E}_v^r$. Nechť $M_1, \ldots, M_r \in \mathbb{Z}_p^{m \times mv}$ jsou matice indukované jednotlivými rovnicemi $\langle f_{i,1}, f_{i,2} \rangle \in \mathcal{E}_v$ soustavy $\mathcal{E}$. Potom matici $M \in \mathbb{Z}_p^{mr \times mv}$ definovanou předpisem

$$M = \begin{pmatrix} M_1 \\ \vdots \\ M_r \end{pmatrix}$$

nazveme *maticí indukovanou soustavou* $\mathcal{E}$. Definujeme zobrazení $\nu : \mathcal{E}_v^r \to \mathbb{Z}_p^{rm}$ předpisem $\nu(\mathcal{E}) = (\nu(\langle f_{1,1}, f_{1,2} \rangle), \ldots, \nu(\langle f_{1,1}, f_{1,2} \rangle))^T$ a dostáváme, že každé řešení $(x_1, \ldots, x_v) \in Q^v$ soustavy $\mathcal{E}$ odpovídá řešení $x = (x_1, \ldots, x_v)^T \in \mathbb{Z}_p^{mv}$ soustavy lineárních rovnic nad $\mathbb{Z}_p$:

$$M \cdot x = \nu(\mathcal{E}). \tag{6.2}$$

Protože lineární rovnice nad tělesy umíme řešit efektivně, tak umíme řešit efektivně i kvazigrupové rovnice v centrálních kvazigrupách nad abelovskými elementárními grupami.

Tvrzení 6.1. *Nechť $(Q, *)$ je centrální kvazigrupa řádu p^n nad abelovskou elementární grupou $(G, +)$. Potom počet elementárních operací (dělení, násobení, sčítání a odčítání v tělese $\mathbb{Z}_p$) potřebných k nalezení vzoru k danému obrazu funkce $R_1 : Q^v \to Q^v$ je $O(n^3v^3)$.*

Důkaz. Invertování funkce R_1 je ekvivalentní vyřešení v kvazigrupových rovnic o v neznámých. Tento problém umíme převést na vyřešení soustavy nv lineárních rovnic o nv neznámých nad tělesem $\mathbb{Z}_p$. Tuto soustavu umíme vyřešit Gaussovou eliminací, jež má kubickou složitost. □

Obecná kvazigrupa s kongruencí σ: Nechť $\mathcal{E} \in \mathcal{E}_v^r$ je soustava rovnic v Q. Označme $K \subseteq Q^v$ množinu řešení soustavy $\mathcal{E}$ a označme $K_\sigma \subseteq (Q/_\sigma)^v$ množinu řešení soustavy $\pi(\mathcal{E})$. Ze slučitelnosti kvazigrupových operací s přirozenou projekcí dostáváme, že

$$\pi(K) \subseteq K_\sigma.$$

Rovnost ale obecně nenastává. Existence kongruence nám dovolí definovat lepší algoritmus než je prohledávání přes všechna možná řešení. Nejdříve použijeme prohledávání hrubou silou na soustavu $\pi(\mathcal{E})$ a získáme množinu řešení K_σ. Toto řešení představuje částečnou informaci o řešení původní soustavy. Tudíž se v druhém kroku při prohledávání hrubou silou kvazigrupy Q omezíme pouze na množinu

$$\pi^{-1}(K_\sigma) \subseteq Q^v.$$

Po částech centrální kvazigrupa: Nechť Q je po částech centrální kvazigrupa nad grupami G a H, kde příslušná kongruence je σ. Algoritmus na vyřešení soustavy $\mathcal{E} \in \mathcal{E}_v^r$ zůstane v prvním kroku stejný jako pro obecnou kvazigrupu s kongruencí σ. Vyřešíme hrubou silou rovnici $\pi(\mathcal{E})$ a získáme množinu K_σ. V druhém kroku budeme postupně probírat všechna řešení $[z]_\sigma \in K_\sigma$ a budeme hledat řešení $x \in Q^v$ soustavy $\mathcal{E}$ takové, že $\sigma(x, z)$. To, že známe v-tici bloků $[z]_\sigma$, do které patří řešení, je zásadní pro využití principu centrálních kvazigrup. Postupovat budeme analogicky jako pro centrální kvazigrupy s tou změnou, že při každé substituci definice po částech

centrální kvazigrupy za operace $*, /, \backslash$ musíme rozhodnout na základě příslušných kongruenčních tříd jaké automorfismy $\alpha_{i,j}, \beta_{i,j} \in \mathrm{Aut}(H)$ a prvek $c_{i,j} \in H$ použít. Opět tudíž pro každé $[z]_\sigma$ definujeme zobrazení

$$\begin{aligned} \mu : Q(x_1, \ldots, x_v) &\to \mathbb{Z}_q[\{\alpha_{i,j}\}, \{\beta_{i,j}\}](x_1, \ldots, x_v), \\ \nu : Q(x_1, \ldots, x_v) &\to H. \end{aligned}$$

které vyjadřují substituci definice po částech centrální kvazigrupy za operace $*, /$ a $\backslash$. Je-li H elementární abelovská grupa řádu p^m, pak analogicky jako pro centrální kvazigrupy každé soustavě rovnic z $\mathcal{E}_v^r$ přiřadíme v závislosti na $[z]_\sigma$ matici indukovanou soustavou a stejně tak příslušné zobrazení $\nu : \mathcal{E}_v^r \to \mathbb{Z}_p^{rm}$. Vyřešení libovolné soustavy poté převedeme na vyřešení lineární soustavy rovnic tvaru (6.2).

Složitost tohoto algoritmu zůstává stále exponenciálně závislá na v, neboť množinu řešení $K_\sigma \subseteq Q/_\sigma$ jsme spočítali hrubým prohledáváním.

Příklad. Nechť $\mathcal{E} = \langle f_1, f_2 \rangle \in \mathcal{E}_1^1$ je dána předpisy $f_1 \equiv (x * x) * x$ a $f_2 \equiv x$. Uvažujme po částech centrální kvazigrupu Q_2 nad grupami G a H, kterou jsme definovali v tabulce 5.1 a příslušném příkladu. V prvním kroku vyzkoušíme oba dva prvky $G/H \cong \mathbb{Z}_2$ a zjistíme, že rovnice $\pi(\mathcal{E})$ má množinu řešení

$$K_\sigma = Q/_\sigma = \{[0]_\sigma, [4]_\sigma\}.$$

Budeme uvažovat zvlášť volby $z = 0$ a $z = 4$. V obou případech vynecháme člen $c_{i,j} \in H$, protože je z definice Q_2 roven 0. Nechť $z = 0$. Potom pro všechna $h \in H = \langle (0\,1\,0)^T, (0\,1\,0)^T \rangle$ dostáváme (při použití standartní bijekcí $\mathbb{Z}_2^3 \to \mathbb{Z}_8$) následující úpravu

$$\begin{aligned} ((0 \oplus h) * (0 \oplus h)) * (0 \oplus h) &= 0 \oplus h \\ (0 \oplus (\alpha_1(h) \oplus \beta_1(h))) * (0 \oplus h) &= 0 \oplus h \\ 0 \oplus (\alpha_1(\alpha_1(h) \oplus \beta_1(h)) \oplus \beta_1(h)) &= 0 \oplus h \\ (\alpha_1^2 \oplus \alpha_1\beta_1 \oplus \beta_1)(h) &= h \\ (\alpha_1^2 \oplus \alpha_1\beta_1 \oplus \beta_1 \oplus \mathrm{id})(h) &= 0. \end{aligned} \tag{6.3}$$

Nechť $z = 4$. Potom pro všechna $h \in H = \langle (0\,1\,0)^T, (0\,1\,0)^T \rangle$ dostáváme

$$\begin{aligned} ((4 \oplus h) * (4 \oplus h)) * (4 \oplus h) &= 4 \oplus h \\ (0 \oplus (\alpha_2(h) \oplus \beta_2(h))) * (4 \oplus h) &= 4 \oplus h \end{aligned}$$

$$\begin{aligned} 4 \oplus (\alpha_1(\alpha_2(h) \oplus \beta_2(h)) \oplus \beta_2(h)) &= 4 \oplus h \\ (\alpha_1\alpha_2 \oplus \alpha_1\beta_2 \oplus \beta_2)(h) &= h \\ (\alpha_1\alpha_2 \oplus \alpha_1\beta_2 \oplus \beta_2 \oplus \mathrm{id})(h) &= 0. \end{aligned} \tag{6.4}$$

Po dosazení příslušných matic za automorfismy získáme pro $z = 0$ a $z = 4$ různé matice indukované soustavou $\mathcal{E}$:

$$M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Ze vztahů (6.3) a (6.4) nahlédneme, že pro oba dva případy také platí $\nu(\mathcal{E}) = 0$ a proto řešení příslušných soustav jsou $K_0 = \langle (0\,1), (1\,0) \rangle$ pro volbu $z = 0$ a $K_4 = \langle (1\,0) \rangle$ pro volbu $z = 4$. Tudíž celkové řešení získáme aplikováním izomorfismu $\mathbb{Z}_2^2 \to H$:

$$\begin{aligned} K &= \{(0\,0\,0) \oplus \langle (0\,0\,1), (0\,1\,0) \rangle, (1\,0\,0) \oplus \langle (0\,1\,0) \rangle\}, \\ K &= \{0, 1, 2, 3, 4, 6\}. \end{aligned}$$

O správnosti výsledku se můžeme přesvědčit díky jednoduchosti rovnice přímo dosazením do multiplikativní tabulky kvazigrupy Q_2.

Rekurzivně centrální kvazigrupy: Nechť $(Q, *)$ je rekurzivně centrální kvazigrupa nad $\{G_i\}_{i=1}^{l}$ a $\{H_i\}_{i=1}^{l}$, kde $\{\sigma_i\}_{i=0}^{l}$ je příslušná filtrace. Nechť H_i jsou elementární abelovské grupy. Nechť $\mathcal{E} \in \mathcal{E}_v^r$. Algoritmus na řešení soustavy $\mathcal{E}$ rozdělíme přirozeně do l kroků, přičemž budeme postupovat od prvního k l-tému. Zobrazení $\pi_i : Q \to Q/_{\sigma_i}$ bude značit přirozenou projekci kvazigrupy Q do faktorkvazigrupy $Q/_{\sigma_i}$.

1. V prvním kroku vyřešíme soustavu $\pi_1(\mathcal{E})$. Protože $Q/_{\sigma_1}$ je centrální kvazigrupa nad grupou H_1, tak umíme tuto soustavu vyřešit efektivně. Jako výstup prvního kroku algoritmu předáme množinu všech řešení soustavy $\pi_1(\mathcal{E})$, kterou označíme K_{σ_1}.
2. V i-tém kroku vyřešíme soustavu $\pi_i(\mathcal{E})$. Kvazigrupa $Q/_{\sigma_i}$ je po částech centrální nad grupami G_i a H_i, kde příslušná kongruence je σ_{i-1}. Protože řešení soustavy $\pi_{i-1}(\mathcal{E})$ jsme dostali na vstupu jako výstup $(i-1)$-ního kroku algoritmu, tak pro každé $[z]_{\sigma_{i-1}} \in K_{\sigma_{i-1}}$ umíme vyřešit soustavu $\pi_i(\mathcal{E})$ efektivně. Výstupem i-tého kroku algoritmu je množina K_{σ_i}, která vznikne sjednocením všech množin řešení soustav $\pi_i(\mathcal{E})$ příslušných jednotlivým $[z]_{\sigma_{i-1}} \in K_{\sigma_{i-1}}$.

3. Jelikož $Q/_{\sigma_l} = Q$, tak množina $K_{\sigma_l} \subseteq Q^v$ tvoří množinu všech řešení soustavy $\mathcal{E}$.

Schéma tohoto algoritmu si představíme jako strom (typ grafu) jehož hloubka je $l+1$. Kořenem tohoto stromu je triviální řešení soustavy $\pi_0(\mathcal{E})$. Každý vrchol i-té úrovně tohoto stromu ztotožníme s jedním řešením soustavy $\pi_i(\mathcal{E})$ a jeho potomky ztotožníme s řešeními soustavy $\pi_{i+1}(\mathcal{E})$, která odpovídají řešení $\pi_i(\mathcal{E})$ dané tímto vrcholem. Všechny vrcholy l-té úrovně tohoto stromu odpovídají všem řešením soustavy $\mathcal{E}$. Základní algoritmus, který jsme představili, odpovídá prohledávání tohoto stromu do šířky a má tu vlastnost, že vždy najde všechna řešení. Kdybychom chtěli nalézt pouze jedno řešení, tak použijeme prohledávání do hloubky. Abychom se vyhnuli obtížnému počítání průměrné složitosti těchto algoritmů, definujeme algoritmus jednodušší, který vychází z prohledávání do hloubky a je definován dodatečnými pravidly:

1. V i-tém kroku algoritmu zvolíme náhodně jedno řešení z množinu K_{σ_i} a to předáme jako výstup i-tého kroku.
2. Jestliže pro nějaké $i \in \{1, \ldots, l\}$ je $K_{\sigma_i} = \emptyset$, pak algoritmus skončí neúspěchem.

Tedy v každém vrcholu stromu, do kterého se dostaneme, vybereme náhodně jednoho potomka, kterým budeme v algoritmu pokračovat. Jestliže se takto dostaneme do vrcholu, který není na l-té úrovni a který nemá žádné potomky, pak algoritmus skončí neúspěchem.

Složitost tohoto algoritmu je rovna součtu složitostí jednotlivých kroků (každý se v algoritmu objeví nejvýšše jednou). Je-li $|H_i| = p_i^{m_i}$ a $\mathcal{E} \in \mathcal{E}_v^v$, pak v i-tém kroku umíme převést soustavu $\pi_i(\mathcal{E})$ na soustavu vm_i lineárních rovnic o vm_i neznámých nad $\mathbb{Z}_{p_i}$, která je určena maticí indukovanou soustavou $\pi_i(\mathcal{E})$ a vektorem pravé strany $\nu(\pi_i(\mathcal{E}))$. Celková složitost algoritmu je tedy rovna nejvýšše

$$\tau(v) = \sum_{i=1}^{l} O(m_i^3 v^3).$$

Nyní se budeme věnovat průměrné úspěšnosti. Zvolme pevné $1 \leq i \leq l$ představující krok algoritmu. Budeme předpokládat, že jestliže soustava $\mathcal{E}$ byla vybrána z množiny $\mathcal{E}_v^v$ náhodně, pak hodnost matice M indukované soustavou $\pi_i(\mathcal{E})$ pro příslušné $[z]_{\sigma_{i-1}} \in K_{\sigma_{i-1}}$ je náhodná veličina, která

má stejné rozdělení jako náhodná veličina, která vyjadřuje hodnost matice vybrané z množiny všech prvků $\mathbb{Z}_{p_i}^{vm_i \times vm_i}$. Jestliže hodnost matice M je rovna vm_i (plná hodnost), pak soustava bude mít pro libovolnou pravou stranu právě jedno řešení. Počet všech matic, které mají plnou hodnost je $(p^{vm_i}-1)\cdot(p^{vm_i}-p)\cdot\ldots\cdot(p^{vm_i}-p^{vm_i-1})$. Proto pravděpodobnost, že náhodně zvolená matice bude mít plnou hodnost je rovna

$$p(v, m_i) = \frac{(p^{vm_i}-1)\cdot(p^{vm_i}-p)\cdot\ldots\cdot(p^{vm_i}-p^{vm_i-1})}{p^{(vm_i)^2}}. \tag{6.5}$$

Pravděpodobnost nalezení alespoň jednoho řešení soustavy $\pi_i(\mathcal{E})$ pro příslušné $[z]_{\sigma_{i-1}} \in K_{\sigma_{i-1}}$ je zřejmě vyšší než $p(v, m_i)$, ale pro zjednodušení výpočtu budeme pracovat s touto dolní mezí.

Poznámka 6.2. Bez důkazu uvádíme, že výraz (6.5) se rovná q-Pochhammerovu číslu $(\frac{1}{p}, \frac{1}{p})_{vm_i}$ (viz. [1]) a platí, že pro všechna $p \in \mathbb{P}$:

$$\lim_{v\to\infty} p(v, m_i) = \left(\frac{1}{p}, \frac{1}{p}\right)_{\infty} \in (0, 1).$$

Z poznámky 6.2 vyplývá, že $p(v, m_i)$ není zanedbatelná funkce v proměnné v. Odtud dostáváme, že minimální úspěšnost celého algoritmu $\prod_{i=1}^{l} p(v, m_i)$ také není zanedbatelná funkce.

Shrnutí: Za předpokladu, že se soustavy $\mathcal{E} \in \mathcal{E}_v^v$, které získáme při invertování funkce R_1, chovají pro parametr v jdoucí do nekonečna náhodně vzhledem k hodnosti matice indukované soustavou, pak předchozí algoritmus dává návod, jak funkci R_1 efektivně invertovat. Jelikož z kapitoly 5 víme, že rekurzivně centrální kvazigrupy nejsou obecně beztvaré, tak dostáváme protipříklad k hypotéze 3.7. Přirozeným rozšířením definice beztvaré kvazigrupy, která by vyloučila rekurzivně centrální případ i jiné možnosti jak zjednodušit danou soustavu rovnic, je přidání podmínky na neexistinci vlastní kongrunce.

Kapitola 7

Definice kvazigrupy velkého řádu

Každá kvazigrupa je definována svou multiplikativní tabulkou. Pro práci s konkrétní kvazigrupou by nám proto stačilo tuto tabulku uchovávat. To lze ovšem jen pro kvazigrupy "malých"řádů, neboť velikost multiplikativní tabulky je $|Q|^2$. Existuje řada způsobů, jak kvazigrupy „velkých“ řádů zkonstruovat. Jedním z těchto způsobů je kvazigrupa isotopní grupě. V našem případě budeme uvažovat abelovské grupy řádu 2^n. Abychom s kvazigrupovými operacemi mohli efektivně pracovat, tak isotopní permutace $\alpha, \beta, \gamma : \{0,1\}^n \to \{0,1\}^n$ i jejich inverzy musí být definovány pomocí efektivního algoritmu. Narozdíl od definice 2.10 isotopní kvazigrupy zaměníme permutaci γ za permutaci γ^{-1}, což je zřejmě ekvivalentní, a budeme pracovat s kvazigrupovou operací ve tvaru

$$x * y = \gamma(\alpha(x) + \beta(y)).$$

V této kapitole definujeme konkrétní permutace použité v návrhu hašovací funkce Edon-R.

Než přistoupíme k samotné definici, tak představíme různé reprezentace prvku kvazigrupy. Nechť $Q = \{0,1\}^n$ a nechť $n = mw$ pro $m, n, w \in \mathbb{N}$. Základem je reprezentace pomocí binárního vektoru $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$. Od ní odvodíme další dvě reprezentace a to pouze přerovnáním jednotlivých bitů. Nechť $x_{i,j} = x_{(j-1)w+i}$ pro $1 \leq i \leq w$, $1 \leq j \leq m$. Definujeme

$$\begin{aligned} X_j &= (x_{1,j}, \ldots, x_{w,j}) \in \mathbb{Z}_2^w, \\ \bar{x}_i &= (x_{i,1}, \ldots, x_{i,m})^T \in \mathbb{Z}_2^m \end{aligned}$$

a prvek x budeme reprezentovat jako

$$x = (X_1, \ldots, X_m)^T, \tag{7.1}$$

	$\bar{x}_1$	$\bar{x}_2$	$\dots$	$\bar{x}_i$	$\dots$	$\bar{x}_w$
X_1	$x_{1,1}$	$x_{1,2}$	$\dots$	$x_{1,i}$	$\dots$	$x_{1,w}$
X_2	$x_{2,1}$	$x_{2,2}$	$\dots$	$x_{2,i}$	$\dots$	$x_{2,w}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
X_m	$x_{m,1}$	$x_{m,2}$	$\dots$	$x_{m,i}$	$\dots$	$x_{m,w}$

Tabulka 7.1: Schéma reprezentace prvku $x \in \mathbb{Z}_2^n$.

$$x \quad = \quad (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_w). \tag{7.2}$$

Tyto reprezentace jsou znázorněny v tabulce 7.1. Motivací pro reprezentaci ve tvaru (7.1) je hašovací funkce Edon-R, která pracuje s prvkem $x \in Q$ uloženým v m w-bitových registrech. V konkrétním návrhu konstanta w nabývá hodnot 32 nebo 64. Forma (7.2) je na druhou stranu vhodnější pro naši analýzu. Poslední reprezentace, kterou budeme používat, využívá standartní bijekci $\varphi : \mathbb{Z}_2^w \to \mathbb{Z}_{2^w}$ převodu z binární do desítkové soustavy

$$\varphi((x_1, \dots, x_w)) = \sum_{i=1}^{w} x_i \cdot 2^{w-i}.$$

Na $x \in Q$ můžeme tedy pohlížet jako na $(X_1, \dots, X_m)^T \in \mathbb{Z}_{2^w}^m$. Všechny konverze mezi těmito reprezentacemi jsou přímočaré a při následujících definicích se jimi už nebudeme zabývat.

Značení. Grupovou operaci na cyklické grupě $\mathbb{Z}_{2^w}$ budeme značit $+$, grupovou operaci na elementární abelovské grupě $\mathbb{Z}_2^i$ budeme značit $\oplus$ pro libovolné $i \in \mathbb{N}$. Grupovou operaci na součinu cyklických grup $\mathbb{Z}_{2^w}^m$ budeme značit $+_m$.

Nyní definujeme dílčí permutace $\mathbf{AddM}_X, \mathbf{AddX}_X, \mathbf{RotL}_X : \{0,1\}^n \to \{0,1\}^n$. Tyto permutace byly navrženy tak, aby jejich implementace v počítači byla co nejrychlejší. Z tohoto důvodu se velikost registru volí $w = 32$ nebo $w = 64$ a jediné operace, které se s registry provádějí je binární sčítání ($\mathbf{AddX}_X$), sčítání modulo 2^w ($\mathbf{AddM}_X$) a rotace registru ($\mathbf{RotL}_X$). Permutace $\alpha, \beta : \{0,1\}^n \to \{0,1\}^n$ z definice isotopní kvazigrupy vzniknou složením kombinací těchto permutací a budou se lišit pouze v hodnotách parametrů X. Permutace $\gamma : \{0,1\}^n \to \{0,1\}^n$ pouze permutuje jednotlivá slova $\gamma((X_1, \dots, X_m)^T) = (X_{\pi(1)}, \dots, X_{\pi(m)})^T$. Jak uvidíme dále, tuto permutaci můžeme z návrhu v principu vypustit.

1. Permutaci $\mathbf{AddX}_B : (\mathbb{Z}_2^w)^m \to (\mathbb{Z}_2^w)^m$ nazveme *binární sčítání slov*. Je-li $B \in \mathbb{Z}_2^{m\times m}$ regulární matice nad tělesem $\mathbb{Z}_2$, pak pro $1 \leq i \leq m$ definujeme $T_i \subseteq \{1, \ldots, m\}$ jako množinu, jejíž vektor incidence je shodný s i-tým řádkem matice B. Pak $(Y_1, \ldots, Y_m)^T = \mathbf{AddX}_B((X_1, \ldots, X_m)^T)$, právě když

$$Y_i = \bigoplus_{j \in T_i} X_j.$$

   Ekvivalentní a přímočařejší definicí, která ale nezdůrazňuje práci se slovy (registry), je definice pomocí formy $x = (\bar{x}_1, \ldots, \bar{x}_w)$. Je-li $y = \mathbf{AddX}_B(x)$, pak dostáváme

$$\bar{y}_i = \Big(\bigoplus_{j \in T_1} x_{i,j}, \bigoplus_{j \in T_2} x_{i,j}, \ldots, \bigoplus_{j \in T_m} x_{i,j} \Big)^T = B \cdot \bar{x}_i$$

   a proto platí

$$\mathbf{AddX}_B((\bar{x}_1, \ldots, \bar{x}_w)) = (B \cdot \bar{x}_1, \ldots, B \cdot \bar{x}_w). \tag{7.3}$$

   Z tohoto vyjádření je zřejmé, že $\mathbf{AddX}_B$ je automorfismus grupy $(\mathbb{Z}_2^n, \oplus)$, neboť obě podmínky $\mathbf{AddX}_B(x \oplus y) = \mathbf{AddX}_B(x) \oplus \mathbf{AddX}_B(y)$ a $\mathbf{AddX}_B(0) = 0$ jsou splněny.

2. Permutaci $\mathbf{AddM}_{A,d} : \mathbb{Z}_{2^w}^m \to \mathbb{Z}_{2^w}^m$ nazveme *modulární sčítání slov*. Nechť $A \in \mathbb{Z}_{2^w}^{m\times m}$ je regulární matice nad okruhem $\mathbb{Z}_{2^w}$ a $d \in \mathbb{Z}_{2^w}^m$. Potom definujeme

$$\mathbf{AddM}_{A,d}((X_1, \ldots, X_m)^T) = A \cdot (X_1, \ldots, X_m)^T +_m d.$$

   Abychom se vyhnuli násobení v okruhu $\mathbb{Z}_{2^w}$ jakožto relativně výpočetně pomalé operaci, tak výběr hodnot prvků matice A omezíme na množinu $\{0, 1\} \subseteq \mathbb{Z}_{2^w}$. Za této dodatečné podmínky pak pro $1 \leq i \leq m$ definujeme $S_i \subseteq \{1, \ldots, m\}$ jako množinu, jejíž vektor incidence je shodný s i-tým řádkem matice A. Potom $\mathbf{AddM}_{A,d}((X_1, \ldots, X_m)^T) = (Y_1, \ldots, Y_m)^T$, právě když

$$Y_i = \sum_{j \in S_i} X_j + D_i. \tag{7.4}$$

   Zvolíme-li $d = 0$, pak $\mathbf{AddM}_{A,0}$ je zřejmě automorfismem $(\mathbb{Z}_{2^w}^m, +_m)$. Nyní přistoupíme k vyjádření $\mathbf{AddM}_{A,d}$ ve formě $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_w)$. Nejdříve

ale musíme odvodit, jak sčítání modulo 2^w zapsat pomocí binárního sčítání $\oplus$. Nechť $X, Y \in \mathbb{Z}_{2^w}$ a nechť $(x_1, \ldots, x_w)$, $(y_1, \ldots, y_w)$ jsou jejich příslušné binární rozvoje. Definujeme $C = (c_1, \ldots, c_w)$ *přenosové bity* modulárního sčítání X a Y předpisem $c_w = 0$ a pro $1 \leq i \leq w-1$

$$c_i = c_{i+1}x_{i+1} \oplus c_{i+1}y_{i+1} \oplus x_{i+1}y_{i+1}.$$

Potom platí

$$X + Y = X \oplus Y \oplus C.$$

Důležitý je fakt, že bit c_i záleží pouze na bitech x_j a y_j pro $i < j \leq w$. Jesliže $S \subseteq \{1, \ldots, m\}$ je libovolná a $D = (d_1, \ldots, d_w) \in \mathbb{Z}_{2^w}$, pak opět existuje $C \in \mathbb{Z}_2^w$ takové, že

$$\sum_{j \in S} X_j + D = \bigoplus_{j \in S} X_j \oplus D \oplus C, \tag{7.5}$$

kde $c_w = 0$ a bit c_i závisí pouze na bitech $x_{j,k}$ a d_j pro $k \in S$ a $i < j \leq w$. Přesnou podobu přenosových bitů již nebudeme do detailu rozebírat, vystačíme pouze s uvedenou vlastností jednotlivých c_i. Využitím tohoto principu dosáhneme oddělení lineární a nelineární části permutace $\mathbf{AddM}_{A,d}$. Substitujeme-li (7.5) do všech souřadnic (7.4) definice $\mathbf{AddM}_{A,d}$, tak z každého slova Y_i získáme přenosové bity C_i. Položíme-li $c = (C_1, \ldots, C_m)$, potom platí, že $\bar{c}_w = 0$ a $\bar{c}_i$ závisí pouze na $\bar{x}_j$ a $\bar{d}_j$ pro $i < j \leq w$. Celkový tvar permutace $\mathbf{AddM}_{A,d}$ je poté

$$\mathbf{AddM}_{A,d}((\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_w)) = (A \cdot \bar{x}_1 \oplus \bar{d}_1 \oplus \bar{c}_1, \ldots, A \cdot \bar{x}_w \oplus \bar{d}_w \oplus \bar{c}_w).$$

3. Permutaci $\mathbf{RotL}_r : (\mathbb{Z}_2^w)^m \to (\mathbb{Z}_2^w)^m$ nazveme *levou rotací slov*. Nechť $X = (x_1, \ldots, x_w) \in \mathbb{Z}_2^w$ a nechť $r \in \mathbb{Z}_w$. Potom definujeme $Y = [X]_r$, právě když $y_i = x_{((i+r-1) \bmod w)+1}$ pro všechna $1 \leq i \leq w$. Pro ilustraci uvádíme

$$[X]_r = (x_{1+r}, \ldots, x_w, x_1, \ldots, x_r).$$

Je-li $r = (r_1, \ldots, r_m) \in \mathbb{Z}_w^m$, pak

$$\mathbf{RotL}_r((X_1, \ldots, X_m)^T) = ([X_1]_{r_1}, \ldots, [X_m]_{r_m})^T.$$

Permutace $\mathbf{RotL}_r$ je automorfismus grupy $(\mathbb{Z}_2^n, \oplus)$, neboť zřejmě platí $[X \oplus Y]_r = [X]_r \oplus [Y]_r$. Naopak zřejmě neplatí, že $\mathbf{RotL}_r$ je automorfismus $(\mathbb{Z}_{2^w}^m, +_m)$.

Značení. Nechť $X = (x_1, \ldots, x_w)$. Nechť $Y = [X]_r$. Potom pro všechna $1 \leq i \leq w$ platí $y_i = x_{((i+r-1) \bmod w)+1}$. Abychom se vyhnuli tomuto pracného zápisu, tak budeme dál uvažovat v indexu sčítání prováděné vždy podle tohoto vzorce a zapisovat ho budeme ve tvaru: $y_i = x_{i+r}$.

Definice 7.1. Nechť $m, n, w \in \mathbb{N}$ jsou taková, že $mw = n$. Kvazigrupu $(Q, *)$ nazveme *typu Edon-R-I*, právě když je isotopní grupě $(\mathbb{Z}_2^n, \oplus)$ a pro isotopní permutace α, β, γ platí: $\gamma = \mathrm{id}$ a existují regulární matice $A_\alpha, A_\beta \in \mathbb{Z}_{2^w}^{m \times m}$, $B_\alpha, B_\beta \in \mathbb{Z}_2^{m \times m}$ a $r_\alpha, r_\beta, s_\alpha, s_\beta \in \mathbb{Z}_w^m$ takové, že

$$\begin{aligned} \alpha &= \mathbf{RotL}_{s_\alpha} \circ \mathbf{AddX}_{B_\alpha} \circ \mathbf{RotL}_{r_\alpha} \circ \mathbf{AddM}_{A_\alpha,0}, \\ \beta &= \mathbf{RotL}_{s_\beta} \circ \mathbf{AddX}_{B_\beta} \circ \mathbf{RotL}_{r_\beta} \circ \mathbf{AddM}_{A_\beta,0}. \end{aligned}$$

Definice 7.2. Nechť $m, n, w \in \mathbb{N}$ jsou taková, že $mw = n$. Kvazigrupu $(Q, *)$ nazveme *typu Edon-R-II*, právě když je isotopní grupě $(\mathbb{Z}_{2^w}^m, +_m)$ a pro isotopní permutace α, β, γ platí: $\gamma = \mathrm{id}$ a existují regulární matice $A_\alpha, A_\beta \in \mathbb{Z}_{2^w}^{m \times m}$, $B_\alpha, B_\beta \in \mathbb{Z}_2^{m \times m}$, $d_\alpha, d_\beta \in \mathbb{Z}_{2^w}^m$ a $r_\alpha, r_\beta \in \mathbb{Z}_w^m$ takové, že

$$\begin{aligned} \alpha &= \mathbf{AddX}_{B_\alpha} \circ \mathbf{RotL}_{r_\alpha} \circ \mathbf{AddM}_{A_\alpha,d}, \\ \beta &= \mathbf{AddX}_{B_\beta} \circ \mathbf{RotL}_{r_\beta} \circ \mathbf{AddM}_{A_\beta,d}. \end{aligned}$$

Poznámka 7.3. Protože $\gamma(x \oplus y) = \gamma(x) \oplus \gamma(y)$, $\gamma(x +_m y) = \gamma(x) +_m \gamma(y)$ a pro všechna $r \in \mathbb{Z}_w^m$, $B \in \mathbb{Z}_2^{m \times m}$ zřejmě existují $r' \in \mathbb{Z}_w^m$, $B' \in \mathbb{Z}_2^{m \times m}$ takové, že

$$\begin{aligned} \gamma \circ \mathbf{RotL}_r &= \mathbf{RotL}_{r'}, \\ \gamma \circ \mathbf{AddX}_B &= \mathbf{AddX}_{B'}, \end{aligned}$$

tak původní návrhy od D. Gligoroskeho [7] a [8], které obsahovaly permutaci γ jsou s našemi definicemi kvazigrup typu Edon-R-I,II, které γ neobsahují, ekvivalentní.

Konkrétní hodnoty parametrů permutací $\mathbf{AddM}_X, \mathbf{AddX}_X, \mathbf{RotL}_X$ nebudeme v této práci rozebírat a chování kvazigrup typu Edon-R-I,II budeme řešit obecně. Nicméně ilustrujeme zde zajímavý způsob, jakým Gligoroski odvodil matice A a B. Protože se jednotlivá řešení mírně liší pro různé volby m, tak princip ilustrujeme na konkrétním příkladu, kdy $m = 8$. Nechť L je latinský čtverec řádu $m = 8$. Matice A_α, B_α pro permutaci α odvodíme

ze čtverce L tak, že ho rozdělíme na dvě části v poměru $5:3$.

$$L = \left(\begin{array}{cccccccc} 3 & 2 & 8 & 7 & 4 & 5 & 1 & 6 \\ 5 & 4 & 3 & 6 & 1 & 8 & 2 & 7 \\ 8 & 1 & 2 & 5 & 7 & 3 & 6 & 4 \\ 7 & 8 & 1 & 2 & 5 & 6 & 4 & 3 \\ 2 & 5 & 7 & 4 & 6 & 1 & 3 & 8 \\ \hline 1 & 7 & 6 & 3 & 2 & 4 & 8 & 5 \\ 6 & 3 & 4 & 1 & 8 & 7 & 5 & 2 \\ 4 & 6 & 5 & 8 & 3 & 2 & 7 & 1 \end{array}\right)$$

Uvažujeme-li sloupce horní části tohoto čtverce jako podmnožiny $\{1, \ldots, m\}$, potom řádky matice A_α jsou vektory incidence těchto množin. Analogicky řádky matice B_α jsou vektory incidence sloupců dolní části čtverce L.

$$A_\alpha = \left(\begin{array}{cccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right) \quad B_\alpha = \left(\begin{array}{cccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right)$$

Je zajímavé, že ne pro každý latinský čtverec tato metoda dává regulární matice A_α, B_α. Ale volbu tohoto čtverce autor nespecifikuje, stejně jako konkrétní hodnoty rotačních vektorů.

Kapitola 8

Analýza kvazigrup typu Edon-R-I,II - část 1

V této kapitole se budeme zabývat vlivem jednotlivých permutací $\mathbf{AddM}_X$, $\mathbf{AddX}_X$ a $\mathbf{RotL}_X$ na řešitelnost rovnic v kvazigrupách typu Edon-R-I,II. Jako prostředek nám budou sloužit kvazigrupy, které vzniknou vynecháním některých z těchto permutací. Z analýzy těchto kvazigrup budeme schopni odvodit jakou vlastnost vynechaná dílčí permutace přináší do celkové kvazigrupové operace. Jako nástroj pro charakterizaci těchto neúplných kvazigrup nám budou sloužit pojmy, které jsme definovali v předchozích kapitolách. Celé kvazigrupy typu Edon-R-I,II jsou naopak natolik složité, že se těmito pojmy charakterizovat nedají, což je základní předpoklad k tomu, aby mohly být pokládány za kryptograficky bezpečné z pohledu hašovací funkce Edon-R.

Permutace $\mathbf{AddX}_X$ a $\mathbf{RotL}_X$ jsou automorfismy grupy $(\mathbb{Z}_2^n, \oplus)$. Proto, jestliže z kvazigrupy typu Edon-R-I vypustíme permutaci $\mathbf{AddM}_X$, získáme centrální kvazigrupu nad elementární abelovskou grupou $(\mathbb{Z}_2^n, \oplus)$. Z kapitoly 6 umíme v centrálních kvazigrupách nad elementárními grupami řešit rovnice efektivně. V kvazigrupě typu Edon-R-II je permutace $\mathbf{AddM}_{A,0}$ automorfismem grupy $(\mathbb{Z}_{2^w}^m, +_m)$ a zřejmě platí, že $\mathbf{AddM}_{A,d} = L_d\mathbf{AddM}_{A,0}$. Proto, jestliže vypustíme permutace $\mathbf{AddX}_X$ a $\mathbf{RotL}_X$, získáme centrální kvazigrupu nad grupou $(\mathbb{Z}_{2^w}^m, +_m)$. Z definice permutace $\mathbf{AddM}_{A,d}$ snadno nahlédneme, že potom každou kvazigrupovou soustavu rovnic můžeme převést na soustavu rovnic v grupě $\mathbb{Z}_{2^w}$.

Proto je důležité, aby definice kvazigrupové operace obsahovala jak komponentu, která bude lineární nad $(\mathbb{Z}_2^n, \oplus)$, tak komponentu, která bude li-

neární nad $(\mathbb{Z}_{2^w}^m, +_m)$. Přirozeným adeptem, který tento princip splňuje, je kvazigrupa, ve které vynecháme všechny rotace $\mathbf{RotL}_X$, ale ponecháme obě permutace $\mathbf{AddM}_X$ a $\mathbf{AddX}_X$. V obou typech Edon-R-I,II probíhá analýza stejným způsobem a proto se budeme zabývat jen kvazigrupami typu Edon-R-I a rozšíření pro druhý typ uvedeme na konci v poznámce 8.4. Pro celou kapitolu označíme tuto kvazigrupu $(Q, *)$ a platí tedy

$$x * y = \alpha(x) \oplus \beta(y) = \mathbf{AddX}_{B_\alpha}(\mathbf{AddM}_{A_{\alpha,0}}(x)) \oplus \mathbf{AddX}_{B_\beta}(\mathbf{AddM}_{A_{\beta,0}}(y)).$$

V této kapitole budeme pracovat výlučne s reprezentací prvku $x \in Q$ tvaru $(\bar{x}_1, \ldots, \bar{x}_w)$. V předchozí kapitole jsme vyjádření pro permutace $\mathbf{AddM}_{A,0}$ a $\mathbf{AddX}_B$ odvodili:

$$\begin{aligned} \mathbf{AddM}_{A,0}((\bar{x}_1, \ldots, \bar{x}_w)) &= (A \cdot \bar{x}_1 \oplus \bar{c}_1, \ldots, A \cdot \bar{x}_w \oplus \bar{c}_w), \\ \mathbf{AddX}_B((\bar{x}_1, \ldots, \bar{x}_w)) &= (B \cdot \bar{x}_1, \ldots, B \cdot \bar{x}_w), \end{aligned}$$

kde $\bar{c}_i$ závisí pouze na $\bar{x}_j$ pro $i < j \leq w$. Složením těchto permutací dostáváme

$$\begin{aligned} \alpha((\bar{x}_1, \ldots, \bar{x}_w)) &= \mathbf{AddX}_{B_\alpha}(\mathbf{AddM}_{A_{\alpha,0}}((\bar{x}_1, \ldots, \bar{x}_w))) \\ &= (B_\alpha A_\alpha \cdot \bar{x}_1 \oplus B_\alpha \cdot \bar{c}_1, \ldots, B_\alpha A_\alpha \cdot \bar{x}_w \oplus B_\alpha \cdot \bar{c}_w) \\ &= (B_\alpha A_\alpha \cdot \bar{x}_1, \ldots, B_\alpha A_\alpha \cdot \bar{x}_w) \oplus (B_\alpha \cdot \bar{c}_1, \ldots, B_\alpha \cdot \bar{c}_w). \end{aligned}$$

Definice 8.1. Nechť $0 \leq i \leq w$. Definujeme relaci σ_i na množině Q:

$$\sigma_i((\bar{x}_1, \ldots, \bar{x}_w), (\bar{y}_1, \ldots, \bar{y}_w)) \iff \bar{x}_j = \bar{y}_j \text{ pro všechna } w - i < j \leq w.$$

Tvrzení 8.2. *Relace σ_i je kongruence kvazigrupy $(Q, *)$.*

Důkaz. $\sigma_i(x * v, y * v)$, právě když pro všechna $w - i < j \leq w$

$$\begin{aligned} (\overline{x * v})_j &= (\overline{y * v})_j \\ (\overline{\alpha(x) \oplus \beta(v)})_j &= (\overline{\alpha(y) \oplus \beta(v)})_j \\ \overline{\alpha(x)}_j \oplus \overline{\beta(v)}_j &= \overline{\alpha(y)}_j \oplus \overline{\beta(v)}_j \\ \overline{\alpha(x)}_j &= \overline{\alpha(y)}_j \\ B_\alpha A_\alpha \cdot \bar{x}_j \oplus B_\alpha \cdot \bar{t}_j &= B_\alpha A_\alpha \cdot \bar{y}_j \oplus B_\alpha \cdot \bar{u}_j, \end{aligned}$$

kde $t, u \in (\mathbb{Z}_2^m)^w$ jsou příslušné přenosové bity permutace $\mathbf{AddM}_X$ (z důvodu nepřehlednosti po přidání dalšího indexu jsme nepoužili pro přenosové bity jednotné označení c). Z $\bar{t}_w = \bar{u}_w (= 0)$ plyne

$$\begin{aligned} B_\alpha A_\alpha \cdot \bar{x}_w &= B_\alpha A_\alpha \cdot \bar{y}_w \\ \bar{x}_w &= \bar{y}_w. \end{aligned}$$

Protože $\bar{t}_{w-1}$ je funkce proměnné $\bar{x}_w$ a $\bar{u}_{w-1}$ je stejnou funkcí proměnné $\bar{y}_w$, tak $\bar{t}_{w-1} = \bar{u}_{w-1}$. Použitím indukčního principu snadno dostáváme, že $\bar{x}_j = \bar{y}_j$ pro všechna $w - i < j \leq w$, což je ekvivaletní s $\sigma_i(x, y)$. Analogicky dostaneme, že $\sigma_i(x, y)$, právě když $\sigma_i(v * x, v * y)$ a proto dle lemma 2.6 je σ_i kongruence $(Q, *)$. □

Je zřejmé, že $\sigma_0 = Q \times Q$, $\sigma_w = \mathrm{id}_Q$ a $\sigma_{i-1} \supset \sigma_i$, proto kvazigrupa Q obsahuje filtraci $\{\sigma_i\}_{i=0}^{w}$. Abychom mohli s kvazigrupou $Q/_{\sigma_i}$ přehledněji pracovat, tak přeznačíme její prvky pomocí isomorfismu $\varphi_i : Q/_{\sigma_i} \to Q_i$, kde Q_i je kvazigrupa definovaná stejnými parametry jako kvazigrupa Q až na délku slova, která je rovna i. Následující předpis dává požadovaný isomorfismus

$$\varphi_i([(\bar{x}_1, \ldots, \bar{x}_{w-i}, \bar{x}_{w-i+1}, \ldots, \bar{x}_w)]_{\sigma_i}) = (\bar{x}_{w-i+1}, \ldots, \bar{x}_w).$$

Prvky Q_i budeme přirozeně reprezentovat ve tvaru $(\bar{x}_1, \ldots, \bar{x}_i)$. Definujeme kongruenci kvazigrupy Q_i předpisem: pro všechna $x, y \in Q_i$ $\sigma(x, y)$, právě když $\bar{x}_j = \bar{y}_j$ pro všechna $1 < j \leq i$. Je snadné nahlédnout, že kongruence σ odpovídá kongruenci σ_{i-1} kvazigrupy $Q/_{\sigma_i}$, nebo-li pro všechna $x, y \in Q_i$ $\sigma(x, y)$, právě když $\sigma_{i-1}(\varphi_i^{-1}(x), \varphi_i^{-1}(y))$. Zafixujme nyní množinu reprezentantů bloků kvazigrupy Q_i modulo σ:

$$\{(0, \bar{x}_2, \ldots, \bar{x}_i) : \bar{x}_j \in \mathbb{Z}_2^m\}.$$

Nechť $H_i = \{(\bar{h}, 0, \ldots, 0) : \bar{h} \in \mathbb{Z}_2^m\}$ je podgrupa $(G_i, \oplus) = ((\mathbb{Z}_2^m)^i, \oplus)$. Potom rozklad G_i modulo H_i je shodný s rozkladem Q_i modulo σ. Nechť $x = (0, \bar{x}_2, \ldots, \bar{x}_i)$, $y = (0, \bar{y}_2, \ldots, \bar{y}_i)$, $z = (0, \bar{z}_2, \ldots, \bar{z}_i)$ jsou takové, že $[x]_\sigma * [y]_\sigma = [z]_\sigma$. Pro každé $g = (\bar{g}_1, 0, \ldots, 0), h = (\bar{h}_1, 0, \ldots, 0) \in H_i$ platí $[x \oplus g]_\sigma = [x]_\sigma$ a $[y \oplus h]_\sigma = [y]_\sigma$. Proto dostáváme

$$[(x \oplus g) * (y \oplus h)]_\sigma = [x \oplus g]_\sigma * [y \oplus h]_\sigma = [z]_\sigma.$$

Pro každé $g, h \in H_i$ tedy existuje $f = (\bar{f}_1, 0, \ldots, 0) \in H_i$ takové, že $(x \oplus g) * (y \oplus h) = z \oplus f$. Dosadíme-li do tohoto vztahu definice isotopních operací α, β kvazigrupy Q, tak získáme

$$\bar{f}_1 = (B_\alpha A_\alpha \cdot \bar{g}_1 \oplus B_\alpha \cdot \bar{t}_1) \oplus (B_\beta A_\beta \cdot \bar{h}_1 \oplus B_\beta \cdot \bar{u}_1), \tag{8.1}$$

kde $\bar{t}_1$,$\bar{u}_1 \in \mathbb{Z}_2^m$ jsou vektory přenosových bitů permutací $\mathbf{AddM}_{A_\alpha,0}$ a $\mathbf{AddM}_{A_\beta,0}$. Tyto hodnoty závisejí pouze na $x, y \in Q_i$, proto je hodnota $\bar{c}_{x,y} = B_\alpha \cdot \bar{t}_1 \oplus B_\beta \cdot \bar{u}_1$ jednoznačným adeptem na konstantní člen v definici po

částech centrálních kvazigrup. Označíme-li α_i automorfismus H_i definovaný předpisem $(\bar{h}, 0, \ldots, 0) \mapsto (B_\alpha A_\alpha \cdot \bar{h}, 0, \ldots, 0)$, β_i automorfismus H_i definovaný předpisem $(\bar{h}, 0, \ldots, 0) \mapsto (B_\beta A_\beta \cdot \bar{h}, 0, \ldots, 0)$ a $c_{x,y} = (\bar{c}_{x,y}, 0, \ldots, 0)$, potom platí, že pro všechny $h, g \in H_i$:

$$(x \oplus g) * (y \oplus h) = z \oplus (\alpha_i(g) \oplus \beta_i(h) \oplus c_{x,y}). \tag{8.2}$$

Proto kvazigrupa Q_i je po částech centrální nad grupami G_i a H_i. Použitím isomorfismu $\varphi : Q/_{\sigma_i} \to Q_i$ přímo dostáváme, že kvazigrupa $Q/_{\sigma_i}$ je po částech centrální nad grupami $\varphi_i^{-1}(G_i)$ a $\varphi_i^{-1}(H_i)$, kde příslušná kongruence je rovna σ_{i-1}. Jako důsledek tohoto rozboru dostáváme následující tvrzení, které je přímou aplikací definice 5.10.

Tvrzení 8.3. *Kvazigrupa $(Q, *)$ je rekurzivně centrální nad abelovskými elementárními grupami $\{\varphi_i^{-1}(G_i)\}_{i=1}^w$ a $\{\varphi_i^{-1}(H_i)\}_{i=1}^w$, kde příslušná filtrace je tvaru $\{\sigma_i\}_{i=0}^w$. Dále pro všechna $1 \leq i \leq w$ platí, že $\varphi_i^{-1}(G_i) \cong (\mathbb{Z}_2^m)^i$ a $\varphi_i^{-1}(H_i) \cong \mathbb{Z}_2^m$.*

Poznámka 8.4. Jak jsme již předeslali na začátku, analogický rozbor můžeme provést pro kvazigrupy typu Edon-R-II. V tomto případě se vyskytuje navíc přičítání konstanty d v permutaci $\mathbf{AddM}_{A,d}$, která se projeví v každém kroku v konečné definici $\bar{c}_{x,y}$, nicméně samotný princip nijak neporuší. Dále musíme navíc započítat fakt, že kvazigrupa je isotopní grupě $(\mathbb{Z}_{2^w}^m, +_m)$ a tedy z tohoto finálního sčítání dostáváme další přenosové bity $v \in (\mathbb{Z}_2^m)^w$, nicméně opět na tyto přenosové bity můžeme použít stejný princip. Uvažujme kvazigrupu $Q_i \cong Q/_{\sigma_i}$. Potom Q_i je po částech centrální nad grupami G_i a H_i. Automorfismy $\alpha_i, \beta_i \in \mathrm{Aut}(H_i)$ získáme stejným způsobem jako pro kvazigrupy typu Edon-R-I. Konstantní člen $c_{x,y} = (\bar{c}_{x,y}, 0, \ldots, 0) \in H_i$ definujeme pro každé dva reprezentanty $x, y \in Q_i$ bloků modulo σ předpisem:

$$\bar{c}_{x,y} = B_\alpha \cdot (\bar{t}_1 \oplus \bar{d}_1) \oplus B_\beta \cdot (\bar{u}_1 \oplus \bar{d}_1) \oplus \bar{v}_1,$$

kde pro jednodušší zápis předpokládáme, že $d = d_\alpha = d_\beta$. Hodnoty $\bar{u}_1, \bar{t}_1, \bar{v}_1 \in \mathbb{Z}_2^m$ závisí pouze na hodnotách $\bar{x}_j, \bar{y}_j, \bar{d}_j \in \mathbb{Z}_2^m$ pro $1 < j \leq i$.

Poznámka 8.5. Nechť $1 \leq i \leq w$ je pevné. Z definice automorfismů $\alpha_i, \beta_i \in \mathrm{Aut}(H_i)$ je zřejmé, že tyto automorfismy nezávisí na jednotlivých dvojicích bloků kongruence (jak je to obecně definováno v po částech centrálních kvazigrupách). Jednotlivé dvojice bloků odlišuje pouze parametr

$c_{x,y} \in H_i$. Proto je-li $\mathcal{E} \in \mathcal{E}_v^r$ nad kvazigrupou Q_i, pak matice indukovaná soustavou $\mathcal{E}$ nezávisí na řešení $[z]_\sigma$ rovnice $\pi(\mathcal{E})$. Dále pro všechna $1 \leq i \leq w$ platí, že $H_i \cong \mathbb{Z}_2^m$ a $\alpha_i, \beta_i \in \mathrm{Aut}(H_i)$ jsou zřejmě v grupě $\mathbb{Z}_2^m$ indukovány maticemi $B_\alpha A_\alpha, B_\beta A_\beta \in \mathrm{M}_m(\mathbb{Z}_2)$. Proto matice M_i indukované soustavami $\pi_i(\mathcal{E})$ jsou pro všechna $1 \leq i \leq w$ totožné.

Algoritmus pro řešení soustav: Nyní se pokusíme o volnější rozbor algoritmu pro řešení rovnic v rekurzivně centrální kvazigrupě (kapitola 5), který aplikujeme na kvazigrupy typu Edon-R-I s vypuštěnými rotacemi. Pro snadnější notaci předpokládejme, že $\mathcal{E} \in \mathcal{E}_1^1$. Algoritmus pro řešení rovnic v rekurzivně centrálních kvazigrupách pracuje v w krocích, které odpovídají postupnému řešení pro jednotlivé souřadnice. V prvním kroku rovnou sestavíme soustavu lineárních rovnic nad $\mathbb{Z}_2$ pro neznámou $\bar{x}_w \in \mathbb{Z}_2^m$, neboť žádné přenosové bity tuto souřadnici neovlyvňují.

$$M \cdot \bar{x}_w = \nu(\pi_1(\mathcal{E}))$$

Ze znalosti $\bar{x}_w$ umíme dopočítat všechny vektory přenosových bitů $\bar{c}_{w-1}$, které jsou dány působením permutace **AddM** na w-tou souřadnici. Pomocí indukčního principu snadno nahlédneme, že v i-tém kroku algoritmu sestavíme soustavu lineárních rovnic nad $\mathbb{Z}_2$ pro neznámou $\bar{x}_{w-i+1} \in \mathbb{Z}_2^m$, neboť přenosové bity $\bar{c}_{w-i+1} \in \mathbb{Z}_2^m$ jsme získali v předchozím kroku.

$$M \cdot \bar{x}_{w-i+1} = \nu(\pi_i(\mathcal{E}))$$

Protože matice M je pro všechny kroky stejná, tak schéma v podobě stromu, které určuje průběh algoritmu je jednodušší než pro obecný případ rekurzivně centrální kvazigrupy. Základním pozorováním je, že hodnost matice M jednoznačně určuje, kolik potomků každý vrchol může mít. Konkrétně je-li $M \in \mathbb{Z}_2^{m \times m}$ matice hodnosti h, pak každý vrchol má s pravděpobností 2^{h-m} právě 2^{m-h} potomků a s pravděpodobností $1 - 2^{h-m}$ právě žádného potomka. Nejjednodušší situace nastává, jestliže M má plnou hodnost. Potom je schéma algoritmu vždy pouze cestou a algoritmus vždy uspěje a vždy bude mít právě jedno řešení.

Značení. Jelikož v i-tém kroku algoritmu pracujeme s $(w - i + 1)$-ní souřadnicí, tak kvůly přehlednosti v indexování budeme v následující kapitole vždy pro obecný krok algoritmu pracovat v notaci: $(w-i+1)$-ní krok a i-tá souřadnice.

Shrnutí: Vypustíme-li z kvazigrupy typu Edon-R-I,II rotace, tak dostáváme rekurzivně centrální kvazigrupu nad abelovskými elementárními grupami. V kapitole 6 jsme ukázali efektivní algoritmus pro řešení rovnic v těchto kvazigrupách. Odtud plyne, že rotace mají stěžejní roli při rušení algebraické sktruktury rekurzivně centrálních kvazigrup.

Kapitola 9

Analýza kvazigrup typu Edon-R-I,II - část 2

Tato kapitola se bude věnovat algoritmu na řešení rovnic v kvazigrupách typu Edon-R-I,II. V minulé kapitole jsme ukázali, že vypuštěním permutací $\mathbf{RotL}_r$ získáme rekurzivně centrální kvazigrupu, proto budeme vycházet z algoritmu pro řešení rovnic v rekurzivně centrálních kvazigrupách. Protože přítomnost rotací nám tento algoritmus znemožňuje, tak rotace nahradíme binárním přičítáním konstanty, kterou ovšem neznáme a proto budeme přes tyto konstanty prohledávat. Protože z tohoto pohledu je typ Edon-R-II jednodušší, jelikož obsahuje jen jednu rotaci, tak se zaměříme v popisu na něj. V závěru kapitoly odvodíme složitost tohoto algoritmu v závislosti na parametrech rotací r_α, r_β a parametrech příslušné řešené rovnice, pro jejichž definici zavedeme následující značení.

Nechť $f \in Q(x_1, \ldots, x_v)$. Definujeme $\Omega_{\alpha,f} \subset Q(x_1, \ldots, x_v)$ *množinu nekonstantních levých podtermů* f a $\Omega_{\beta,f} \subset Q(x_1, \ldots, x_v)$ *množinu nekonstantních pravých podtermů* f:

$$\begin{aligned} \Omega_{\alpha,f} &= \{t \in \Omega_f : t \notin Q \text{ a existují } t_1, t_2 \in \Omega_f \text{ takové, že } t * t_1 = t_2\}, \\ \Omega_{\beta,f} &= \{t \in \Omega_f : t \notin Q \text{ a existují } t_1, t_2 \in \Omega_f \text{ takové, že } t_1 * t = t_2\}. \end{aligned}$$

Je-li Q isotopní kvazigrupa, pak množina $\Omega_{\alpha,f}$ představuje nekonstantní podtermy termu f, na které se při substituci definice isotopní kvazigrupy uplatní permutace α. Proto touto množinou budeme indexovat ta místa algoritmu, kde budeme nahrazovat rotaci $\mathbf{RotL}_{r_\alpha}$ za přičítání konstanty. Nechť $\mathcal{E} = \langle f_1, f_2 \rangle \in \mathcal{E}_v$, pak definujeme množiny nekonstantních levých a pravých

podtermů rovnice $\mathcal{E}$ předpisy

$$\begin{aligned}\Omega_{\alpha,\mathcal{E}} &= \Omega_{\alpha,f_1} \cup \Omega_{\alpha,f_2},\\ \Omega_{\beta,\mathcal{E}} &= \Omega_{\beta,f_1} \cup \Omega_{\beta,f_2}.\end{aligned}$$

Pro soustavy rovnic $\mathcal{E} \in \mathcal{E}_v^r$ definujeme množiny $\Omega_{\alpha,\mathcal{E}}$ (respektive $\Omega_{\beta,\mathcal{E}}$) jako sjednocení množin $\Omega_{\alpha,\mathcal{E}}$ (respektive $\Omega_{\beta,\mathcal{E}}$) jednotlivých rovnic soustavy. V celé této kapitole budeme pracovat se soustavami $\mathcal{E} \in \mathcal{E}_v^r$ takovými, že každá neznámá x_i je v této soustavě uplatněna. Nebo-li pro všechna $1 \leq i \leq v$ platí, že $x_i \in \Omega_{\alpha,\mathcal{E}}$ nebo $x_i \in \Omega_{\beta,\mathcal{E}}$. Dále budeme předpokládat, že každá z r rovnic soustavy obsahuje alespoň jeden term, který není prvkem žádné jiné rovnice. Za těchto předpokladů dostáváme jednoduché nerovnosti:

$$v \leq |\Omega_{\alpha,\mathcal{E}}| + |\Omega_{\beta,\mathcal{E}}|, \tag{9.1}$$

$$r \leq |\Omega_{\alpha,\mathcal{E}}| + |\Omega_{\beta,\mathcal{E}}|. \tag{9.2}$$

Příklad. Nechť $\mathcal{E} = \langle f_1, f_2 \rangle \in \mathcal{E}_3$, kde $f_1 \equiv (c{*}x_2){*}(x_3{*}c)$ a $f_2 \equiv x_1{*}(x_2{*}c)$. Potom

$$\begin{aligned}\Omega_{\alpha,\mathcal{E}} &= \{x_1, x_2, x_3, c * x_2\},\\ \Omega_{\beta,\mathcal{E}} &= \{x_2, x_3 * c, x_2 * c\}.\end{aligned}$$

Nyní zavedeme značení potřebná pro popis předeslaného algoritmu. Nechť $\mathcal{E} \in \mathcal{E}_v^r$. Kvůly složitému indexování označíme $\mathbf{X}$ množinu neznámých, $|\mathbf{X}| = v$. Nebudeme explicitně předpokládat, že její prvky jsou x_i, ale budeme se na ně obecně odvolávat vztahem $x \in \mathbf{X}$. Nechť $z \in Q^v$ je libovolné pevně zvolené řešení soustavy $\mathcal{E}$. Každému termu $t \in \Omega_{\alpha,\mathcal{E}}$ přiřadíme prvek $y_\alpha(t) \in \{0,1\}^n$ a každému termu $u \in \Omega_{\beta,\mathcal{E}}$ přiřadíme prvek $y_\beta(u) \in \{0,1\}^n$:

$$\begin{aligned}y_\alpha(t) &= \mathbf{AddM}_{A_\alpha,d_\alpha}(t(z)),\\ y_\beta(u) &= \mathbf{AddM}_{A_\beta,d_\beta}(u(z)).\end{aligned} \tag{9.3}$$

Dále pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ a $u \in \Omega_{\beta,\mathcal{E}}$ definujeme prvky $\Delta_\alpha(t), \Delta_\beta(t) \in \{0,1\}^n$ předpisy:

$$\begin{aligned}\Delta_\alpha(t) &= \mathbf{RotL}_{r_\alpha}(y_\alpha(t)) \oplus y_\alpha(t),\\ \Delta_\beta(u) &= \mathbf{RotL}_{r_\beta}(y_\beta(u)) \oplus y_\beta(u).\end{aligned} \tag{9.4}$$

Hodnoty $\Delta_\alpha(t)$ a $\Delta_\beta(u)$ byly zřejmě definovány tak, aby představovali příslušné konstanty, jejichž přičtením nahradíme permutaci $\mathbf{RotL}_r$, jestliže chceme nalézt řešení $z \in Q^v$. Než začneme s definicí samotného algoritmu, tak definujeme některé pojmy (definice 9.1), jejichž smysl ale objasníme až při popisu algoritmu.

Značení. Protože pro permutace α a β je situace ve všech směrech symetrická, tak většinu detailů v této kapitole budeme rozebírat pouze pro permutaci α a nebudeme permutaci β explicitně jmenovat. Nicméně každé takové tvrzení má přirozenou analogii i pro permutaci β.

Definice 9.1. Nechť $r_\alpha, r_\beta \in \mathbb{Z}_w^m$ jsou parametry rotací kvazigrupy $(Q, *)$ typu Edon-R-II. Potom definujeme množiny $\mathcal{A}_j^{(k)}, \mathcal{B}_j^{(k)} \subseteq \{1, \ldots, w\}$ pro $1 \leq k \leq w$ a $1 \leq j \leq m$ následujícími rekurzivními předpisy:

$$\mathcal{A}_j^{(w)} = \mathcal{B}_j^{(w)} = \emptyset$$

Jestliže $k + r_\alpha[j] > w$ (respektive $k + r_\beta[j] > w$), pak

$$\mathcal{A}_j^{(k-1)} = \mathcal{A}_j^{(k)} \cup \{k + r_\alpha[j] - w\}, \tag{9.5}$$

$$\mathcal{B}_j^{(k-1)} = \mathcal{B}_j^{(k)} \cup \{k + r_\beta[j] - w\}. \tag{9.6}$$

Jestliže $k + r_\alpha[j] \leq w$ (respektive $k + r_\beta[j] \leq w$]), pak

$$\mathcal{A}_j^{(k-1)} = \mathcal{A}_j^{(k)}, \tag{9.7}$$

$$\mathcal{B}_j^{(k-1)} = \mathcal{B}_j^{(k)}. \tag{9.8}$$

Lemma 9.2. *Pro všechna $1 \leq k \leq w$ a $1 \leq j \leq m$ platí, že $k \in \mathcal{A}_j^{(k)}$, právě když $k \leq r_\alpha[j]$.*

Důkaz. Jestliže $k + r_\alpha[j] > w$, pak

$$\mathcal{A}_j^{(k)} = \{k + 1 + r_\alpha[j] - w, \ldots, r_\alpha[j]\}. \tag{9.9}$$

Jestliže $k + r_\alpha[j] \leq w$, pak

$$\mathcal{A}_j^{(k)} = \{1, \ldots, r_\alpha[j]\}.$$

Proto k dokončení důkazu stačí ukázat, že $k + 1 + r_\alpha[j] - w \leq k$, což ale dostaneme přímo z faktu, že $r_\alpha[j] \leq w - 1$ z definice parametrů rotace. □

Lemma 9.3. *Jestliže $r_\alpha[j] = 0$, pak pro všechna $1 \leq k \leq w$ je $\mathcal{A}_j^{(k)} = \emptyset$.*

Důkaz. Zřejmě pro žádné k není splněna podmínka $k + r_\alpha[j] > w$ a proto v žádném kroku nedojde k zvětšení množiny. □

Algortimus pro řešení rovnic v kvazigrupě typu Edon-R

Nechť $\mathcal{E} \in \mathcal{E}_v^r$. Nechť $z \in Q^v$ je řešení $\mathcal{E}$. Předpokládejme, že známe hodnoty $\Delta_\alpha(t)$ a $\Delta_\beta(u)$ pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ a $u \in \Omega_{\beta,\mathcal{E}}$. Tyto hodnoty závisí na hodnotě z. Předpokládejme, že neznáme samotné z. Potom pro jeho nalezení bychom mohli použít analogii algoritmu definovaného v minulé kapitole, neboť bychom pouze každou rotaci nahradili přičtením příslušného prvku $\Delta_\alpha(t)$ nebo $\Delta_\beta(u)$, což by do algoritmu přidalo pouze další konstanty a nijak by to neovlivnilo jeho řešitelnost. Problémem zůstává, že hodnoty $\Delta_\alpha(t)$ a $\Delta_\beta(u)$ neznáme a proto definujeme algoritmus, který bude využívat algoritmus pro řešení rovnic v rekurzivně centrálních kvazigrupách a který bude zároveň prohledávat přes hodnoty $\Delta_\alpha(t)$ a $\Delta_\beta(u)$. Výstupem algoritmu poté budou tyto hodnoty a řešení $z \in Q^v$ soustavy $\mathcal{E}$, které bude těmto hodnotám odpovídat.

Hrubý nástin algoritmu: Opět budeme pracovat po souřadnicích, tedy od w-té souřadnice, která představuje nejméně důležité bity, k první souřadnici, která představuje nejdůležitější bity jednotlivých slov prvků kvazigrupy Q. Hodnoty $\Delta_\alpha(t)$ a $\Delta_\beta(u)$ nebudeme volit celé, ale během prohledávání algoritmu budeme postupně volit jejich souřadnice. Nechť $1 \leq k \leq w$. Potom v $(w-k+1)$-ním kroku budeme volit $\overline{\Delta_\alpha(t)}_k$ a $\overline{\Delta_\beta(u)}_k$ pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ a $u \in \Omega_{\beta,\mathcal{E}}$. Pomocí těchto hodnot budeme schopni zformulovat rovnice pro k-tou souřadnici na stejném principu jako jsme to udělali v algoritmu pro kvazigrupu bez rotací v kapitole 8. Následně získáme řešení $\bar{x}_k$ pro všechna $x \in \mathbf{X}$ a provedeme kontrolu, zda-li všechny zvolené a vypočítané hodnoty odpovídají hodnotám, které jsme získali z předchozích kroků (tento postup vysvětlíme v bodech 4 a 5 algoritmu). Pokud bychom chtěli opět pracovat se schématem algoritmu v podobě stromu, tak do kořene umístíme nulovou informaci (triviální řešení rovnice $\pi_0(\mathcal{E})$ v případě kvazigrupy z minulé kapitoly) a každý vrchol $(w-k+1)$-ní úrovně ztotožníme s nějakým řešením soustavy pro k-tou souřadnici, které je představováno hodnotami $\{\bar{x}_k\}_{x\in\mathbf{X}}$, $\{\overline{\Delta_\alpha(t)}_k\}_{t\in\Omega_{\alpha,\mathcal{E}}}$ a $\{\overline{\Delta_\beta(u)}_k\}_{u\in\Omega_{\beta,\mathcal{E}}}$. Každý potomek tohoto vrcholu potom představuje řešení rovnice pro $(k-1)$-ní souřadnici, která odpovídá přenosovým bitům určených daným vrcholem. Opět všechny vrcholy w-té úrovně představují řešení soustavy $\mathcal{E}$ a pro nalezení jednoho řešení budeme používat algoritmus prohledávání stromu do hloubky.

Nyní představíme v několika bodech kostru algoritmu pro jeden konkrétní $(\mathbf{w-k+1})$-ní krok algoritmu. K detailům se dostaneme v poznámkách, které následují po tomto popisu a v kterých odvodíme složitost algoritmu.

1. Jako vstup dostáváme částečně známé hodnoty neznámých $\{x\}_{x\in\mathbf{X}}$, $\{y_\alpha(t)\}_{t\in\Omega_{\alpha,\mathcal{E}}}$ a $\{y_\beta(u)\}_{u\in\Omega_{\beta,\mathcal{E}}}$. Jako konstanty dostáváme všechny vektory přenosových bitů, které vyvstali z $(w-k)$-tého kroku algoritmu. Konkrétně pro každé $x \in \mathbf{X}$ dostáváme hodnoty

   $$\bar{x}_{k+1}, \ldots, \bar{x}_w,$$

   které odpovídají řešení rovnice $\pi_{w-k}(\mathcal{E})$ algoritmu pro rekurzivně centrální kvazigrupy. Stejně tak pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ dostáváme hodnoty

   $$\overline{y_\alpha(t)}_{k+1}, \ldots, \overline{y_\alpha(t)}_w.$$

   Navíc ale známe i další bity neznámých $y_\alpha(t)$. Pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ a pro všechna $i \leq k$ známe bit $\overline{y_\alpha(t)}_i[j]$, právě když $i \in \mathcal{A}_j^{(k)}$. Množiny $\mathcal{A}_1^{(k)}, \ldots, \mathcal{A}_m^{(k)}$ tedy tvoří šablonu pro „nestandartní“ známé bity neznámých $y_\alpha(t)$ na vstupu do $(w-k+1)$-ního kroku algoritmu. Jak jsme tuto informaci získali objasníme v bodu 5. Grafické znázornění této částečné informace najdeme v tabulce 9.1.

2. Druhým bodem algoritmu je zvolení hodnot $\overline{\Delta_\alpha(t)}_k, \overline{\Delta_\beta(u)}_k \in \mathbb{Z}_2^m$ pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ a $u \in \Omega_{\beta,\mathcal{E}}$. Pro zjednodušení algoritmu budeme předpokládat, že tato volba je náhodná, ačkoli v poznámce 9.7 ukážeme, že tyto hodnoty budeme volit postupně z množiny řešení určité soustavy lineárních rovnic nad $\mathbb{Z}_2$. Jediná vyjímka v náhodné volbě $\overline{\Delta_\alpha(t)}_k, \overline{\Delta_\beta(u)}_k$, kterou v tomto stadiu popisu algoritmu uděláme, se vyskytne, jestliže pro nějaké $1 \leq j \leq m$ je $r_\alpha[j] = 0$. Pak permutace $\mathbf{RotL}_{r_\alpha}$ je v restrikci na j-té slovo identita. Proto jistě pro všechna $1 \leq i \leq w$ a pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$:

   $$\overline{\mathbf{RotL}_{r_\alpha}(y_\alpha(t))}_i[j] = \overline{y_\alpha(t)}_i[j].$$

   Proto $\overline{\Delta_\alpha(t)}_k[j] = 0$. V detailnější analýze (poznámka 9.5) ukážeme jaká další omezení pro volbu $\overline{\Delta_\alpha(t)}_k, \overline{\Delta_\beta(u)}_k$ musíme dodržet.

3. Pokud v permutaci $\alpha = \mathbf{AddX}_{B_\alpha} \circ \mathbf{RotL}_{r_\alpha} \circ \mathbf{AddM}_{A_\alpha,d}$ nahradíme rotaci $\mathbf{RotL}_{r_\alpha}$ přičtením konstanty Δ_α ($\alpha = \mathbf{AddX}_{B_\alpha} \circ L_{\Delta_\alpha} \circ \mathbf{AddM}_{A_\alpha,d}$), pak po přenesení do naší reprezentace získáváme předpis:

   $$\alpha((\bar{x}_1, \ldots, \bar{x}_w)) \;=\; (B_\alpha A_\alpha \cdot \bar{x}_1, \ldots, B_\alpha A_\alpha \cdot \bar{x}_k, \ldots, B_\alpha A_\alpha \cdot \bar{x}_w) \oplus$$

x	$\bar{x}_1$	$\bar{x}_2$	$\bar{x}_3$	$\bar{x}_4$	$\bar{x}_5$	$\bar{x}_6$	$\bar{x}_7$	$\bar{x}_8$
X_1	-	-	-	-	-	-	-	O
X_2	-	-	-	-	-	-	-	O
X_3	-	-	-	-	-	-	-	O
X_4	-	-	-	-	-	-	-	O

y_α	$\bar{y}_1$	$\bar{y}_2$	$\bar{y}_3$	$\bar{y}_4$	$\bar{y}_5$	$\bar{y}_6$	$\bar{y}_7$	$\bar{y}_8$
Y_1	O	-	-	-	-	-	-	O
Y_2	-	O	-	-	-	-	-	O
Y_3	-	-	-	O	-	-	-	O
Y_4	-	-	-	-	-	-	-	O

y_β	$\bar{y}_1$	$\bar{y}_2$	$\bar{y}_3$	$\bar{y}_4$	$\bar{y}_5$	$\bar{y}_6$	$\bar{y}_7$	$\bar{y}_8$
Y_1	-	O	-	-	-	-	-	O
Y_2	-	O	-	-	-	-	-	O
Y_3	-	-	-	-	O	-	-	O
Y_4	-	-	-	-	-	-	O	O

Tabulka 9.1: Ilustrační příklad. Tabulky částečné informace o neznámých x, $y_\alpha(t)$ a $y_\beta(u)$ na vstupu do 2. kroku algoritmu. Symbol "-"značí neznámý bit a symbol "O"značí známý bit. Parametry kvazigrupy jsou $m = 4$, $w = 8$ a $r_\alpha = (1, 2, 4, 0)$ a $r_\beta = (2, 2, 5, 7)$.

$$\begin{aligned}&\oplus(B_\alpha \cdot (\bar{d}_1 \oplus \bar{c}_1), \ldots, B_\alpha \cdot (\bar{d}_k \oplus \bar{c}_k), \ldots \\ &\qquad \ldots, B_\alpha \cdot (\bar{d}_w \oplus \bar{c}_w)) \oplus \\ &\oplus(B_\alpha \cdot (\overline{\Delta_\alpha})_1, \ldots, B_\alpha \cdot (\overline{\Delta_\alpha})_k, \ldots, B_\alpha \cdot (\overline{\Delta_\alpha})_w).\end{aligned}$$

Pro úspěšné sestavení soustavy lineárních rovnic, která bude odpovídat k-té souřadnici, tedy známe všechny potřebné hodnoty a tudíž umíme sestavit soustavu (9.10) lineárních rovnic nad $\mathbb{Z}_2$ pro neznámou $x \in \mathbb{Z}_2^{mv}$, která představuje vektor uspořádaných hodnot $\{\bar{x}_k\}_{x \in \mathbf{X}}$:

$$M \cdot x = \nu(\mathcal{E}). \tag{9.10}$$

Matici $M \in \mathbb{Z}^{rm \times vm}$ nazveme maticí indukovanou soustavou $\mathcal{E}$ a tato matice se neliší od matice indukované soustavou $\mathcal{E}$, pokud uvažujeme kvazigrupu bez rotací definovanou v kapitole 8. Proto také pro všechny kroky $1 \leq k \leq w$ je matice M totožná. Symbol $\nu(\mathcal{E})$ představuje stejný princip oddělení konstantní a nekonstantní části jako při substituci definice po částech centrální kvazigrupy. Toto zobrazení dále rozdělíme na část, která závisí jen na hodnotách $\overline{\Delta_\alpha(t)}_k$, $\overline{\Delta_\beta(u)}_k$ a na část, která na nich závislá není:

$$\nu(\mathcal{E}) = \nu_c(\mathcal{E}) \oplus \nu_\Delta\left(\mathcal{E}, \{\overline{\Delta(t)}_k\}_{t \in \Omega_{\alpha,\mathcal{E}}}, \{\overline{\Delta(u)}_k\}_{u \in \Omega_{\beta,\mathcal{E}}}\right). \tag{9.11}$$

Zobrazení $\nu_c(\mathcal{E})$ závisí jen na vektorech přenosových bitů souřadnice k (ty odpovídají konstantním členům po částech centrálních kvazigrup z kapitoly 8) a na všech konstantách přítomných v soustavě $\mathcal{E}$ v projekci na k-tou souřadnici.

4. Tento bod algoritmu nazveme *kontrolou bitů před rotací*. Pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ spočítáme hodnoty $\overline{y_\alpha(t)}_k$. To můžeme udělat, protože v předchozím bodu jsme spočítali $\{\bar{x}_k\}_{x\in\mathbf{X}}$ z nichž jsou tyto hodnoty odvozeny. Protože některé bity z hodnot $\overline{y_\alpha(t)}_k$ jsme mohli získat na vstupu algoritmu (bod 1), tak musíme zkontrolovat, jestli jsou tyto bity shodné s hodnotami spočítanými v tomto kroku. Pozice, kde budeme muset tuto kontrolu provést, jsou charakterizovány množinami $\mathcal{A}_j^{(k)}$ (bod 1). Konkrétně platí, že bit $\overline{y_\alpha(t)}_k[j]$ jsme dostali na vstupu $(w-k+1)$-ního kroku, právě když $k \in \mathcal{A}_j^{(k)}$. V prvním kroku algoritmu tato kontrola odpadá, neboť $\mathcal{A}_j^{(w)} = \emptyset$.

   (a) Jestliže se některé bity právě vypočítaných hodnot $\overline{y_\alpha(t)}_k$ neshodují s odpovídajícími bity, které jsme dostali na vstupu, pak se vrátíme zpět na bod 2 a zvolíme nové hodnoty $\overline{\Delta_\alpha(t)}_k$ a $\overline{\Delta_\beta(u)}_k$.

   (b) Jestliže se všechny kontrolované bity v tomto i následujícím bodu shodují, pak z tohoto bodu předáme do dalšího kroku hodnoty $\overline{y_\alpha(t)}_k$ jako známé.

5. Tento bod algoritmu nazveme *kontrolou bitů po rotaci*. Pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ vypočítáme ze vztahu (9.4) hodnoty:

$$\overline{\mathbf{RotL}_{r_\alpha}(y_\alpha(t))}_k \;=\; \overline{y_\alpha(t)}_k \oplus \overline{\Delta_\alpha(t)}_k.$$

   Z definice rotace určují hodnoty $(\overline{\mathbf{RotL}_{r_\alpha}(y_\alpha(t))})_k$ bity neznámých $y_\alpha(t)$ na těchto pozicích pro $1 \le j \le m$:

$$\overline{y_\alpha(t)}_{(k+r_\alpha[j])}[j] \;=\; \overline{\mathbf{RotL}_{r_\alpha}(y_\alpha(t))}_k[j].$$

   Opět některé z těchto bitů jsme mohli získat na vstupu jako známé bity a proto je musíme porovnat s právě vypočítanými hodnotami. Jestliže

$$k < k + r_\alpha[j] \le w,$$

x	$\bar{x}_1$	$\bar{x}_2$	$\bar{x}_3$	$\bar{x}_4$	$\bar{x}_5$	$\bar{x}_6$	$\bar{x}_7$	$\bar{x}_8$
X_1	-	-	-	-	-	-	O	O
X_2	-	-	-	-	-	-	O	O
X_3	-	-	-	-	-	-	O	O
X_4	-	-	-	-	-	-	O	O

y_α	$\bar{y}_1$	$\bar{y}_2$	$\bar{y}_3$	$\bar{y}_4$	$\bar{y}_5$	$\bar{y}_6$	$\bar{y}_7$	$\bar{y}_8$
Y_1	O	-	-	-	-	-	O	X
Y_2	O	O	-	-	-	-	O	O
Y_3	-	-	O	O	-	-	O	O
Y_4	-	-	-	-	-	-	O	O

y_β	$\bar{y}_1$	$\bar{y}_2$	$\bar{y}_3$	$\bar{y}_4$	$\bar{y}_5$	$\bar{y}_6$	$\bar{y}_7$	$\bar{y}_8$
Y_1	O	O	-	-	-	-	O	O
Y_2	O	O	-	-	-	-	O	O
Y_3	-	-	-	O	O	-	O	O
Y_4	-	-	-	-	-	O	X	O

Tabulka 9.2: Ilustrační příklad. Tabulky částečné informace o neznámých x, $y_\alpha(t)$ a $y_\beta(u)$ na výstupu z 2. kroku. Symboly "X"značí ty pozice, na kterých jsme provedli kontrolu shody bitů. Parametry kvazigrupy jsou $m = 4$, $w = 8$ a $r_\alpha = (1, 2, 4, 0)$ a $r_\beta = (2, 2, 5, 7)$.

pak bit $\overline{y_\alpha(t)}_{(k+r_\alpha[j])}[j]$ známe, neboť na vstupu $(w-k+1)$-ního kroku jsme obdrželi:

$$\overline{y_\alpha(t)}_{k+1}, \ldots, \overline{y_\alpha(t)}_{w}.$$

Na druhou stranu jestliže $k + r_\alpha[j] > w$, pak bit $\overline{y_\alpha(t)}_{(k+r_\alpha[j])}[j]$ neznáme, protože

$$(k + r_\alpha[j] - w) \notin \mathcal{A}_j^{(k)}$$

dle vyjádření množiny $\mathcal{A}_j^{(k)}$ tvaru (9.9).

(a) Jestliže se některé právě vypočítané bity $\overline{y_\alpha(t)}_{k+r_\alpha[j]}[j]$ neshodují s odpovídajícími bity, které jsem dostali na vstupu, pak se vrátíme zpět na bod 2 a zvolíme nové hodnoty $\overline{\Delta_\alpha(t)}_k$ a $\overline{\Delta_\beta(u)}_k$.

(b) Jestliže se všechny kontrolované bity v tomto i předcházejícím bodu shodují a $k + r_\alpha[j] > w$, pak z tohoto bodu předáváme do dalšího kroku bity $\overline{y_\alpha(t)}_{k+r_\alpha[j]}[j]$ jako známé. Odtud zřejmě plyne motivace pro definice množin $\mathcal{A}_j^{(k)}$, neboť pro $k + r_\alpha[j] > w$ jsme definovali

$$\mathcal{A}_j^{(k-1)} = \mathcal{A}_j^{(k)} \cup \{k + r_\alpha[j] - w\}.$$

6. Všechny bity neznámých $\{x\}_{x\in\mathbf{X}}$, $\{\overline{y_\alpha(t)}\}_{t\in\Omega_{\alpha,\mathcal{E}}}$ a $\{\overline{y_\beta(u)}\}_{u\in\Omega_{\beta,\mathcal{E}}}$, které jsme spočítali v tomto kroku předáme do dalšího kroku jako známe bity (pro grafický náhled tabulka 9.2). Dále z hodnot $\{\bar{x}_k\}_{x\in\mathbf{X}}$ spočítáme všechny přenosové bity, které vyvstali z výpočtů pro k-tou souřadnici. Tyto hodnoty budeme v následujícím kroku považovat za konstantní a odpovídají konstantním členům po částech centrální kvazigrupy z kapitoly 8.

Poznámka 9.4. Označme rovnice z nichž se skládá soustava $\mathcal{E}\in\mathcal{E}_v^r$ standartně předpisem

$$\mathcal{E}=(\langle f_{1,1},f_{1,2}\rangle,\ldots,\langle f_{r,1},f_{r,2}\rangle).$$

Zobrazení ν_Δ ze vztahu (9.11) vyjádříme stejně jako celé zobrazení ν po složkách, které odpovídají jednotlivým rovnicím soustavy:

$$\nu_\Delta(\mathcal{E})=(\nu_\Delta(\langle f_{1,1},f_{1,2}\rangle),\ldots,\nu_\Delta(\langle f_{r,1},f_{r,2}\rangle)).$$

Díky tomu, že zobrazení ν_Δ závisí pouze na hodnotách $\overline{\Delta_\alpha(t)}_k$ a $\overline{\Delta_\beta(u)}_k$, tak ze substituce definice kvazigrupy typu Edon-R-II za operace $*$, $/$ a $\setminus$ vyplývá, že na každou z těchto složek můžeme pohlížet jako na prvek okruhu

$$\mathbb{Z}_2[A_\alpha,B_\alpha,A_\beta,B_\beta](\{\overline{\Delta_\alpha(t)}_k\}_{t\in\Omega_{\alpha,\mathcal{E}}},\{\overline{\Delta_\beta(u)}_k\}_{u\in\Omega_{\beta,\mathcal{E}}}).$$

Dále budeme používat standartní zápis tvaru:

$$\nu_\Delta(\langle f_{i,1},f_{i,2}\rangle)=\bigoplus_{t\in\Omega_{\alpha,\mathcal{E}}}A_{t,i}\cdot\overline{\Delta_\alpha(t)}_k\oplus\bigoplus_{u\in\Omega_{\beta,\mathcal{E}}}B_{u,i}\cdot\overline{\Delta_\beta(u)}_k,\tag{9.12}$$

kde $A_{t,i},B_{u,i}\in\mathbb{Z}_2^{m\times m}$ jsou matice, na které můžeme pohlížet jako na prvky maticového okruhu $\mathbb{Z}_2[A_\alpha,B_\alpha,A_\beta,B_\beta]\subseteq\mathrm{M}_m(\mathbb{Z}_2)$. Jestliže se term $t\in\Omega_{\alpha,\mathcal{E}}$ vyskytuje jako levý podterm termů $f_{i,1}$ a $f_{i,2}$ pouze jednou, pak matice $A_{t,i}$ je zřejmě regulární, protože vznikne pouze vynásobením kombinace regulárních matic $A_\alpha,B_\alpha,A_\beta,B_\beta$. Stejně tak, jestliže se term u vyskytuje jako pravý podterm termů $f_{i,1}$ a $f_{i,2}$ pouze jednou, tak matice $B_{u,i}$ je regulární.

Poznámka 9.5. V bodu 2 jsme uvedli omezení na výběr hodnot $\overline{\Delta_\alpha(t)}_k$ a $\overline{\Delta_\beta(u)}_k$, jestliže pro nějaké $1\leq j\leq m$ je $r_\alpha[j]=0$ nebo $r_\beta[j]=0$. Pro jednoduchost jsme dále předpokládali náhodný výběr těchto hodnot. Nyní představíme další omezení, která na tyto hodnoty uplatníme. Jestliže pro nějaké $1\leq j\leq m$ platí

$$k\leq\min(r_\alpha[j],w-r_\alpha[j]),$$

pak dle lemma 9.2 dostáváme, že $k \in \mathcal{A}_j^{(k)}$ a zároveň $k + r_\alpha[j] \leq w$. Proto na vstupu do $(w-k+1)$-ního kroku algoritmu dostáváme pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$ oba dva bity $\overline{y_\alpha(t)}_k[j]$ a $\overline{y_\alpha(t)}_{(k+r_\alpha[j])}[j]$. Tyto dva bity nám jednoznačně určují hodnotu:

$$\overline{\Delta_\alpha(t)}_k[j] = \overline{y_\alpha(t)}_k[j] \oplus \overline{y_\alpha(t)}_{(k+r_\alpha[j])}[j]. \tag{9.13}$$

Lemma 9.6. *Nechť $M \in \mathbb{Z}_2^{r\times v}$. Nechť $b \in \mathbb{Z}_2^r$. Potom při náhodné volbě vektoru b jako vektoru pravé strany soustavy $(M|b)$ je průměrná velikost množiny řešení této soustavy rovna 2^{v-r}.*

Poznámka 9.7. Předpoklad, že hodnoty $\overline{\Delta_\alpha(t)}_k$ a $\overline{\Delta_\beta(u)}_k$ volíme v každém kroku náhodně, jsme udělali proto, abychom základní kostru algoritmu zjednodušili. Každá podmínka na omezení této volby představuje nějakou soustavu lineárních rovnic nad $\mathbb{Z}_2$, kde za neznámé považujeme hodnoty $\{\overline{\Delta_\alpha(t)}_k[j] : r_\alpha[j] \neq 0\}$, $\{\overline{\Delta_\beta(u)}_k[j] : r_\beta[j] \neq 0\}$ a $\{\bar{x}_k\}_{x\in\mathbf{X}}$. Nyní představíme výčet těchto omezujících lineárních rovnic. Každá z nich bude pracovat nad celkovým počtem neznámých:

$$vm + |\Omega_{\alpha,\mathcal{E}}|m_\alpha + |\Omega_{\beta,\mathcal{E}}|m_\beta.$$

1. Základním požadavkem, který tyto nezmámé hodnoty musí splňovat, je rovnice (9.10). Do této rovnice dosadíme nejdříve vyjádření (9.11) a následně člen $\nu_\Delta(\mathcal{E})$ rozepíšeme pro každou rovnici soustavy zvlášť ve tvaru (9.12). Dostáváme tedy soustavu rm lineárních rovnic nad $\mathbb{Z}_2$.

2. Dalším požadavkem, který tyto neznáme hodnoty musí splňovat, jsou rovnice (9.13). Tyto rovnice získáme, právě když $k \leq \min(r_\alpha[j], w - r_\alpha[j])$. Pro každé takové $1 \leq j \leq m$ získáme tedy dalším $|\Omega_{\alpha,\mathcal{E}}|$ lineárních rovnic nad $\mathbb{Z}_2$ (v tomto případě získáme přímo hodnotu proměnné $\overline{\Delta_\alpha(t)}_k[j]$).

3. Posledním požadavkem, který tyto hodnoty musí splňovat, je shoda bitů před a po rotaci, kterou jsme v algoritmu prováděli v bodech 4 a 5. Ze substituce definice kvazigrupy typu Edon-R-II za operace $*, /$ a $\backslash$ zřejmě plyne, že každou hodnotu $\overline{y_\alpha(t)}_k$ umíme vyjádřit ve tvaru

$$\overline{y_\alpha(t)}_k = \bigoplus_{x\in\mathbf{X}} C_x \cdot \bar{x}_k \oplus \bigoplus_{t\in\Omega_{\alpha,\mathcal{E}}} A_t \cdot \overline{\Delta_\alpha(t)}_k \oplus \bigoplus_{u\in\Omega_{\beta,\mathcal{E}}} B_u \cdot \overline{\Delta_\beta(u)}_k \oplus c,$$

   kde $C_x, A_t, B_u \in \mathbb{Z}_2[A_\alpha, B_\alpha, A_\beta, B_\beta] \subseteq \mathrm{M}_m(\mathbb{Z}_2)$ a $c \in \mathbb{Z}_2^m$. Lineární rovnice získané ztohoto vztahu rozdělíme do tří případů, kdy bit $\overline{y_\alpha(t)}_k[j]$ musíme zkontrolovat jen před rotací, jen po rotaci a před i po rotaci:

(a) **Kontrola jen před rotací:** $k \in \mathcal{A}_j^{(k)}$ a zároveň $k + r_\alpha[j] > w$. Na vstupu $(w-k+1)$-ního kroku dostáváme pouze bit $\overline{y_\alpha(t)}_k[j]$. V bodě 4 algoritmu musíme tento bit zkontrolovat pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$. Tato kontrola nám tedy pro každé příslušné $1 \leq j \leq m$ dává dalších $|\Omega_{\alpha,\mathcal{E}}|$ lineárních rovnic nad $\mathbb{Z}_2$.

(b) **Kontrola jen po rotací:** $k < k + r_\alpha[j] \leq w$ a zároveň $k \notin \mathcal{A}_j^{(k)}$. Na vstupu $(w-k+1)$-ního kroku dostáváme pouze bit $\overline{y_\alpha(t)}_{k+r_\alpha[j]}[j]$. V bodě 5 algoritmu musíme tento bit zkontrolovat pro všechny termy $t \in \Omega_{\alpha,\mathcal{E}}$. Jelikož

$$\overline{y_\alpha(t)}_{k+r_\alpha[j]}[j] = \overline{\Delta_\alpha(t)}_k[j] \oplus \overline{y_\alpha(t)}_{k[j]}[j], \tag{9.14}$$

tak tato kontrola nám také pro každé příslušné $1 \leq j \leq m$ dává $|\Omega_{\alpha,\mathcal{E}}|$ lineárních rovnic nad $\mathbb{Z}_2$.

(c) **Kontrola před i po rotací:** $k \in \mathcal{A}_j^{(k)}$ a zároveň $k < k + r_\alpha \leq w$. Na vstupu $(w-k+1)$-ního kroku dostáváme oba dva bity $\overline{y_\alpha(t)}_k[j]$ a $\overline{y_\alpha(t)}_{k+r_\alpha[j]}[j]$. Jejich vzájemný vztah je dán rovnicí (9.14), kterou jsme již ale zahrnuli v bodu 2 tohoto výčtu. Proto dostáváme opět pouze $|\Omega_{\alpha,\mathcal{E}}|$ lineárních rovnic nad $\mathbb{Z}_2$ daných bez újmy na obecnosti kontrolou před rotací, neboť rovnice z kontroly po rotaci bychom odvodili spojením s rovnicí (9.14).

Protože podmínka $k \in \mathcal{A}_j^{(k)}$ je ekvivalentní podmínce $k \leq r_\alpha[j]$, tak v $(w-k+1)$-ním kroku budeme muset provést kontrolu bitu $\overline{y_\alpha(t)}_k[j]$ nebo bitu $\overline{y_\alpha(t)}_{k+r_\alpha[j]}[j]$, právě když

$$(r_\alpha[j] \neq 0) \wedge (k \leq \max(r_\alpha[j], w - r_\alpha[j])). \tag{9.15}$$

Pro každé $1 \leq j \leq m$, které splňuje (9.15), pak dostáváme $|\Omega_{\alpha,\mathcal{E}}|$ lineárních rovnic nad $\mathbb{Z}_2$, neboť pro všechny tři případy (a),(b),(c), které mohou nastat, je situace stejná.

Poznámka 9.8. Definujeme pomocné zobrazení $\varphi_\alpha : \mathbb{Z} \to \mathbb{Z}$, které udává počet lineárních rovnic nad $\mathbb{Z}_2$ pro jeden term $t \in \Omega_{\alpha,\mathcal{E}}$, které jsme schopni sestavit v $(w-k+1)$-ním kroku algoritmu. Rovnice, které jsme odvodili pro každý term, se nacházejí v bodech 2 a 3 poznámky 9.7, odkud dostáváme:

$$\begin{aligned} \varphi_\alpha(k) &= |\{j : k \leq \min(r_\alpha[j], w - r_\alpha[j])\}| \\ &\quad + |\{j : k \leq \max(r_\alpha[j], w - r_\alpha[j]) \wedge r_\alpha[j] \neq 0\}|. \end{aligned}$$

Definujeme další pomocné zobrazení $\varphi : \mathbb{Z} \to \mathbb{Z}$, které představuje celkový počet všech lineárních rovnic nad $\mathbb{Z}_2$, které získáme v $(w-k+1)$-ním kroku. Opět předpis získáme přímo z rozboru uvedeného v poznámce 9.7:

$$\varphi(k) = rm + |\Omega_{\alpha,\mathcal{E}}|\varphi_\alpha(k) + |\Omega_{\beta,\mathcal{E}}|\varphi_\beta(k).$$

Označme příslušnou soustavu $\varphi(k)$ lineárních rovnic nad $\mathbb{Z}_2$: $(N_k|b)$. Matice N_k nad $\mathbb{Z}_2$ jsou typu $(\varphi(k), vm + |\Omega_{\alpha,\mathcal{E}}|m_\alpha + |\Omega_{\beta,\mathcal{E}}|m_\beta)$. Z jejich definice zřejmě plyne, že jsou pro $1 \leq k \leq w$ pevné a nemění se pro různé volby v předchozích krocích. Předpokládejme, že pro pevné $1 \leq k \leq w$ vektor b pravé strany nabývá všech možných hodnot z množiny $\mathbb{Z}_2^{\varphi(k)}$ se stejnou pravděpodobností. Potom označíme-li

$$\begin{aligned}\psi(k) &= vm + |\Omega_{\alpha,\mathcal{E}}|m_\alpha + |\Omega_{\beta,\mathcal{E}}|m_\beta - \varphi(k)\\ &= vm - rm + |\Omega_{\alpha,\mathcal{E}}|(m_\alpha - \varphi_\alpha(k)) + |\Omega_{\beta,\mathcal{E}}|(m_\beta - \varphi_\beta(k)),\end{aligned}$$

tak dle lemma 9.6 v $(w-k+1)$-kroku algoritmu získáváme v průměru $2^{\psi(k)}$ různých kombinací hodnot $\{\bar{x}_k\}_{x\in\mathbf{x}}$, $\{\overline{\Delta_\alpha(t)}_k\}_{t\in\Omega_{\alpha,\mathcal{E}}}$ a $\{\overline{\Delta_\beta(u)}_k\}_{u\in\Omega_{\beta,\mathcal{E}}}$, přes které musíme prohledávat. Pokud tento výsledek přeneseme do schématu algoritmu popsaného stromem, tak to znamená, že každý vrchol $(w-k+1)$-ní úrovně má v průměru $2^{\psi(k)}$ potomků.

Poznámka 9.9. Dosazením do definic zobrazení φ_α z poznámky 9.8 snadno získáme $\varphi_\alpha(1) = 2m_\alpha$, $\varphi_\alpha(w) = 0$ a

$$\begin{aligned}\varphi_\alpha\left(\left\lfloor\frac{w}{2}\right\rfloor\right) &= \left|\left\{j : \left\lfloor\frac{w}{2}\right\rfloor \leq \min(r_\alpha[j], w - r_\alpha[j])\right\}\right| + m_\alpha,\\ \varphi_\alpha\left(\left\lfloor\frac{w}{2}\right\rfloor + 1\right) &= 0 + \left|\left\{j : \left\lfloor\frac{w}{2}\right\rfloor + 1 \leq \max(r_\alpha[j], w - r_\alpha[j]) \wedge r_\alpha[j] \neq 0\right\}\right|.\end{aligned}$$

Zřejmě pak dostáváme, že $\varphi_\alpha\left(\left\lfloor\frac{w}{2}\right\rfloor\right) \geq m_\alpha \geq \varphi_\alpha\left(\left\lfloor\frac{w}{2}\right\rfloor + 1\right)$. Dále budeme uvažovat pro jednoduchost jen soustavy v rovnic o v neznámých, čímž podstatně zjednodušíme předpis pro zobrazení ψ. Dosazením výsledků pro zobrazení φ_α získáváme:

$$\begin{aligned}\psi(1) &= -m_\alpha|\Omega_{\alpha,\mathcal{E}}| - m_\beta|\Omega_{\beta,\mathcal{E}}|,\\ \psi\left(\left\lfloor\frac{w}{2}\right\rfloor\right) &\leq 0,\\ \psi\left(\left\lfloor\frac{w}{2} + 1\right\rfloor\right) &\geq 0,\\ \psi(w) &= m_\alpha|\Omega_{\alpha,\mathcal{E}}| + m_\beta|\Omega_{\beta,\mathcal{E}}|.\end{aligned}$$

Poznámka 9.10 (Složitost-speciální případ)**.** Pro snažší odhad složitosti algoritmu zformulujeme předpoklad, který nemusí být vždy splněn, ale který nám umožní dojít k výsledku podobnou cestou jako v algoritmu pro rekurzivně centrální kvazigrupy.

Předpoklad: Nechť matice N_k pro $\left\lfloor \frac{w}{2} \right\rfloor < k$ mají všechny řádky lineárně nezávislé a nechť matice N_k pro $k \leq \left\lfloor \frac{w}{2} \right\rfloor$ mají plnou hodnost.

Tyto předpoklady nejsou ve sporu s celkovým typem těchto matic, protože z předchozích výsledků pro zobrazení φ je zřejmé, že pro $\left\lfloor \frac{w}{2} \right\rfloor < k$ je počet řádků $\varphi(k)$ menší nebo roven počtu sloupců a pro pro $k \leq \left\lfloor \frac{w}{2} \right\rfloor$ je počet řádků $\varphi(k)$ větší nebo roven počtu sloupců.

Za těchto předpokladů při postupu stromem schématu algoritmu má každý vrchol $(w-k+1)$-ní úrovně pro $\left\lfloor \frac{w}{2} \right\rfloor < k$ alespoň jednoho potomka a každý vrchol pro $k \leq \left\lfloor \frac{w}{2} \right\rfloor$ nejvýšše jednoho potomka. Algoritmus prohledávání stromu definujeme na stejném principu jako zjednodušený algoritmus pro rekurzivně centrální kvazigrupy. Tedy při nenalezení žádného řešení v libovolném kroku ohlásíme neúspěch. Je-li $k \leq \left\lfloor \frac{w}{2} \right\rfloor$, pak $\psi(k) \leq 0$ a proto z předpokladu dostáváme, že průměrná úspěšnost v tomto kroku je $2^{\psi(k)}$. Potom pravděpodobnost, že tento algoritmus uspěje, je zřejmě rovna

$$\iota = \prod_{k=1}^{\lfloor \frac{w}{2} \rfloor} 2^{\psi(k)}. \tag{9.16}$$

Pro jednodušší vyjádření celkové úspěšnosti použijeme následující vzorec:

$$\begin{aligned} \sum_{k=1}^{\lfloor \frac{w}{2} \rfloor} m_\alpha - \varphi_\alpha(k) &= \sum_{k=1}^{\lfloor \frac{w}{2} \rfloor} -|\{j : k \leq \min(r_\alpha[j], w - r_\alpha[j])\}| \\ &= -\sum_{j=1}^{m} \min(r_\alpha[j], w - r_\alpha[j]). \end{aligned}$$

Označíme-li poté

$$\Omega = -\sum_{j=1}^{m} |\Omega_{\alpha,\mathcal{E}}| \min(r_\alpha[j], w - r_\alpha[j]) + |\Omega_{\beta,\mathcal{E}}| \min(r_\beta[j], w - r_\beta[j]), \tag{9.17}$$

pak $\iota = 2^\Omega$. Položíme-li za základní jednotku složitosti jeden běh tohoto zjednodušeného algoritmu, pak složitost vyřešení soustavy $\mathcal{E}$ je v průměru rovna

$$\tau = 2^{-\Omega}.$$

Poznámka 9.11 (Složitost-obecný případ)**.** Nechť $1 \leq F \leq w$. Potom průměrný počet vrcholů F-té úrovně stromu odpovídajícímu schématu algoritmu je

$$\prod_{k=w-F+1}^{w} 2^{\psi(k)}.$$

Z předchozí poznámky dostáváme, že nejvíce vrcholů má zřejmě úroveň, která odpovídá $(\lfloor \frac{w}{2} \rfloor + 1)$-ní souřadnici. Proto celkový počet všech vrcholů stromu je menší než

$$1 + w \prod_{k=\lfloor \frac{w}{2} \rfloor + 1}^{w} 2^{\psi(k)}.$$

Celkovou složitost našeho algoritmu potom můžeme ztotožnit s celkovým počtem všech vrcholů. Snadno se ukáže, že toto číslo umíme opět vyjádřit pomocí Ω a platí, že

$$\tau \leq 1 + w2^{-\Omega}.$$

Kapitola 10

Hašovací funkce Edon-R

Jak jsme již předeslali, hašovací funkce Edon-R má dvě konkrétní varianty. Hlavním autorem těchto návrhů je Danilo Gligoroski. První návrh, z kterého jsme vycházeli nejčastěji, pochází z článku [7] a vychází z obecného náhledu na práci s kvazigrupovými řetězci ([5]) a z obecné definice nekonečné třídy funkcí $R_1 : Q^v \to Q^v$ ([6]), kterou jsme definovali v kapitole 3. V těchto článcích ([5],[6]) nenajdeme konkrétní podobu kvazigrupy, ale pouze schémata využívající kvazigrupy s určitými vlastnostmi (například beztvarost). Konkrétní parametry nalezneme až v článku [7], kde je definována kvazigrupa typu Edon-R-I. Druhá varianta hašovací funkce Edon-R je přepracovanou verzí první varianty a byla přijata do soutěže o nový standart kryptografického hašovacího algoritmu SHA-3 [8]. Tento návrh využívá kvazigrupy typu Edon-R-II, ale hlavní rozdíl mezi variantami je v struktuře kompresní funkce.

Obě varianty Edonu-R jsou navrženy dle Merkle-Damgardovy konstrukce iterovaných hašovacích funkcí [3]. Obě také deklarují odolnost vůči generickým útokům na multikolize [11], protože používají řetězící hodnoty, jejichž velikost je dvakrát větší než velikost výsledného haše, což je dle [13] za předpokladu správného návrhu kompresní funkce postačující podmínka. Kompresní funkce obou variant jsou založeny na kvazigrupových operacích, ale mají odlišnou strukturu. Obě varianty jsou definovány pro základní délky otisku zprávy $n = 256, 512$. Než se pustíme do popisu kompresních funkcí, tak nejdříve zavedeme příslušné zpracování zprávy.

1. Varianta [7]: Nechť $m \in \{0,1\}^*$ je zpráva délky $l \leq 2^{128}$. Zprávu m doplníme dle standartního Merkle-Damgardova zesílení tak, aby délka doplněné zprávy $m' \in \{0,1\}^*$ byla násobkem n a posledních 128 bitů, aby reprezentovalo délku zprávy. Zprávu m' poté rozdělíme na n-bitové

bloky $m^{(i)}$:

$$m' = m^{(1)}||m^{(2)}||\dots||m^{(N)}.$$

2. Varianta [8]: Nechť $m \in \{0,1\}^*$ je zpráva délky $l \leq 2^{64}$. Zprávu m doplníme dle standartního Merkle-Damgardova zesílení tak, aby délka doplněné zprávy $m' \in \{0,1\}^*$ byla násobkem $2n$ a posledních 64 bitů, aby reprezentovalo délku zprávy. Zprávu m' poté rozdělíme na dvojice n-bitových bloků $(m_0^{(i)}, m_1^{(i)})$:

$$m' = (m_0^{(1)}||m_1^{(1)})||(m_0^{(2)}||m_1^{(2)})||\dots||(m_0^{(N)}||m_1^{(N)}).$$

Nyní přistoupíme k popisu kompresní funkce:

1. Varianta [7]: Řetězící hodnoty, které jsou výstupem i-tého kroku iterace, budeme značit $h_0^{(i)}, h_1^{(i)} \in \{0,1\}^n$. Hodnoty $h_0^{(0)}, h_1^{(0)} \in \{0,1\}^n$ jsou konstanty, které jsou definovány ve specifikaci algoritmu. Odvození hodnot $h_0^{(i)}, h_1^{(i)} \in \{0,1\}^n$ probíhá pomocí následujícího předpisu:

$$R_1((h_0^{(i-1)}, h_1^{(i-1)}, m^{(i)})) = (b^{(i)}, h_0^{(i)}, h_1^{(i)}),$$

kde hodnoty $b^{(i)}$ dále nevyužijeme. Výsledný otisk zprávy m je poté dán vztahem

$$\mathbf{Edon-R}(m) = h_1^{(N)}.$$

2. Varianta [8]: Řetězící hodnoty, které jsou výstupem i-tého kroku iterace, budeme opět značit $h_0^{(i)}, h_1^{(i)} \in \{0,1\}^n$. Hodnoty $h_0^{(0)}, h_1^{(0)} \in \{0,1\}^n$ jsou konstanty, které jsou definovány ve specifikaci algoritmu. Předpis pro kompresní funkci v této variantě už není tak přímočarý a nevyužívá pouze kvazigrupové operace, takže nejde čistě o kvazigrupovou funkci. Definujeme zobrazení $\hat{(\,)} : \{0,1\}^n \to \{0,1\}^n$ předpisem: je-li $x = (X_1, X_2, \dots, X_m)$, pak $\hat{x} = (X_m, \dots, X_2, X_1)$. Kompresní funkci poté definujeme tabulkou 10.1 a označíme ji $R_2 : Q^4 \to Q^2$. Potom platí, že $R_2((h_0^{(i-1)}, h_1^{(i-1)}, m_0^{(i)}, m_1^{(i)})) = (h_0^{(i)}, h_1^{(i)})$. Výsledný otisk zprávy m je poté opět dán vztahem

$$\mathbf{Edon-R}(m) = h_0^{(N)}.$$

R_2	$m_0^{(i)}$	$m_1^{(i)}$
$\hat{m}_1^{(i)}$	$t_1^{(i)}$	$t_2^{(i)}$
$h_0^{(i-1)}$	$t_3^{(i)}$	$t_4^{(i)}$
$h_1^{(i-1)}$	$t_5^{(i)}$	$t_6^{(i)}$
$\hat{m}_0^{(i)}$	$h_1^{(i)}$	$h_0^{(i)}$

$\Leftarrow$

$t_1^{(i)} = \hat{m}_1^{(i)} * m_0^{(i)}$	$t_2^{(i)} = t_1^{(i)} * m_1^{(i)}$
$t_3^{(i)} = h_0^{(i-1)} * t_1^{(i)}$	$t_4^{(i)} = t_3^{(i)} * t_2^{(i)}$
$t_5^{(i)} = t_3^{(i)} * h_1^{(i-1)}$	$t_6^{(i)} = t_4^{(i)} * t_5^{(i)}$
$h_1^{(i)} = \hat{m}_0^{(i)} * t_5^{(i)}$	$h_0^{(i)} = h_1^{(i)} * t_6^{(i)}$

Tabulka 10.1: Schéma kompresní funkce $R_2 : Q^4 \to Q^2$.

V obou kompresních funkcích se používá kvazigrupa jejíž řád je roven 2^n, kde n je velikost výsledného otisku zprávy. Ve variantě [7] je použita kvazigrupa typu Edon-R-I a ve variantě [8] je použita kvazigrupa typu Edon-R-II. Na všechny hodnoty $m^{(i)}, h^{(i)}$ a $t^{(i)}$ pohlížíme v popisu kompresní funkce jako na prvky příslušné kvazigrupy. Konkrétní předpisy daných kvazigrup je možné nalézt ve specifikacích algoritmů.

Kapitola 11

Útok na nalezení vzoru Edonu-R

V této kapitole se budeme věnovat pouze variantě hašovací funkci Edon-R, která byla navržena do soutěže na SHA-3 [8]. Budeme tedy pracovat s kvazigrupami typu Edon-R-II. Útok, který představíme má za úkol k dané hodnotě otisku $h \in \{0,1\}^n$ spočítat její vzor. Budeme vycházet z principu, který je popsán v [12], ale stěžejní část našeho příspěvku pracuje na jiném principu. Tento útok patří do kategorie "Meet-In-The-Middle"(MITM) útoků.

Budeme předpokládat, že zpráva m doplněná na násobek $2n$, má délku $6n$ bitů, i když útok je snadno rozšiřitelný na libovolnou větší délku zprávy. Označme její bloky standartně

$$m' = (m_0^{(1)}||m_1^{(1)})||(m_0^{(2)}||m_1^{(2)})||(m_0^{(3)}||m_1^{(3)}).$$

Potom zřejmě $h = h_0^{(3)}$ spolu s inicializačními prvky $h_0^{(0)}$, $h_1^{(0)}$ jsou jediné vstupní hodnoty algoritmu. Následující popis rozdělíme do tří kroků a rozbor složitosti provedeme až na závěr.

1. Protože blok zprávy $m_1^{(3)}$ obsahuje padding, tak při jeho volbě nemáme úplnou volnost, což bychom potřebovali pro náš algoritmus. Proto ohnisko MITM útoku přesuneme o jednu pozici zpátky. Blok $m_1^{(3)}$ libovolně zvolíme, tak aby posledních 65 bitů tvořilo správný padding. Z daných hodnot $h_0^{(3)}, m_1^{(3)} \in \{0,1\}^n$ a z libovolně zvolených hodnot $m_0^{(3)}, h_1^{(3)}$ dopočítáme jednoznačně určená $h_0^{(2)}, h_1^{(2)}$ taková, že

$$R_2((h_0^{(2)}, h_1^{(2)}, m_0^{(3)}, m_1^{(3)})) = (h_0^{(3)}, h_1^{(3)}).$$

Existence a jednoznačnost těchto hodnot snadno nahlédneme přímo z definující tabulky 10.1 funkce R_2 tak, že budeme postupně počítat jednoznačně určené hodnoty: $t_1^{(3)}, t_2^{(3)}, t_5^{(3)}, t_6^{(3)}, t_4^{(3)}, t_3^{(3)}$ a $h_0^{(2)}, h_1^{(2)}$.

2. Nyní popíšeme *krok vpřed* v MITM útoku, který budeme provádět na hodnotě $h_0^{(1)}$. Bez újmy na obecnosti položme $h_1^{(1)} = 0$ (mohli bychom zvolit libovolnou jinou konstantu). Zvolme libovolné $m_0^{(1)}$. Z daných hodnot $h_0^{(0)}, h_1^{(0)}, m_0^{(1)}, h_1^{(1)}$ dopočítáme jednoznačně určená $m_1^{(1)}, h_0^{(1)}$ taková, že

$$R_2((h_0^{(0)}, h_1^{(0)}, m_0^{(1)}, m_1^{(1)})) = (h_0^{(1)}, h_1^{(1)}).$$

Existence a jednoznačnost těchto hodnot snadno opět nahlédneme přímo z definující tabulky 10.1 tak, že budeme postupně počítat jednoznačně určené hodnoty: $t_5^{(1)}, t_3^{(1)}, t_1^{(1)}, m_1^{(1)}, t_2^{(1)}, t_4^{(1)}, t_6^{(1)}$ a $h_0^{(1)}$.

3. Nyní popíšeme *krok zpět* v MITM útoku. Máme dány hodnoty $h_0^{(2)}, h_1^{(2)}$ a $h_1^{(1)} = 0$. Naším úkolem bude nalézt hodnoty $h_0^{(1)}$ a $m_0^{(2)}, m_1^{(2)}$ takové, že

$$R_2((h_0^{(1)}, h_1^{(1)}, m_0^{(2)}, m_1^{(2)})) = (h_0^{(2)}, h_1^{(2)}).$$

Pokud by se hodnoty $h_0^{(1)}$ spočítané při kroku vpřed i vzad rovnali, potom bychom našli hledaný vzor. Tato část algoritmu je výpočetně nejnáročnější, protože nelze provést přímo jako první dva kroky. V prví fázi nejdříve zvolíme libovolné $m_0^{(2)}$ a spočítáme postupně jednoznačně určené hodnoty: $t_5^{(2)}, t_6^{(2)}, t_3^{(2)}, t_4^{(2)}, t_2^{(2)}$. V druhé fázi využijeme algoritmus pro řešení rovnic v kvazigrupách typu Edon-R definovaný v kapitole 9 a vyřešíme rovnici s neznámou $m_1^{(2)}$:

$$(\hat{m}_1^{(2)} * m_0^{(2)}) * m_1^{(2)} = t_2^{(2)}. \tag{11.1}$$

Ve třetí fázi dopočítáme postupně jednoznačně určené hodnoty: $t_1^{(2)}, t_3^{(2)}$ a $h_0^{(1)}$.

Protože v kroku zpět MITM útoku musíme vyřešit rovnici (11.1), tak tento krok je výpočetně náročnější než krok vpřed MITM útoku. Označme jako jednotku složitosti spočítání jedné hodnoty $h_0^{(1)}$ kroku vpřed. Dle průběhu kroku vpřed můžeme jistě tuto jednotku ztotožnit s jedním během kompresní funkce, jakožto jednotkou, která se používá pro porovnání s jinými útoky. Označme t složitost kroku zpět vyjádřenou pomocí těchto základních jednotek. Základní struktura MITM útoku vzhledem k složitosti je následující:

1. Různými volbami hodnoty $m_0^{(2)}$ vygenerujeme množinu $T \subseteq \{0,1\}^n \times \{0,1\}^n$ příslušných dvojic hodnot $(m_0^{(2)}, h_0^{(1)})$, které odpovídají kroku zpět. Časová složitost tohoto kroku je zřejmě $t|T|$ a paměťová složitost je zřejmě $2|T|$ uložených hodnot z množiny $\{0,1\}^n$.

2. Různými volbami hodnoty $m_0^{(1)}$ spočítáme hodnotu $h_0^{(1)}$ pomocí kroku vpřed MITM útoku. Po $\frac{2^n}{|T|}$ volbách s vysokou pravděpodobností nalezneme takové $h_0^{(1)}$, které leží v množině T, a tudíž jsme uspěli v nalezení vzoru k danému otisku. Časová složitost tohoto kroku je zřejmě $\frac{2^n}{|T|}$. Paměťové nároky nemá tento krok žádné.

Průměrná celková časová složitost algoritmu je součtem částečných složitostí a tedy je rovna

$$\tau = t|T| + \frac{2^n}{|T|}. \tag{11.2}$$

Průměrná celková paměťová složitost algoritmu je zřejmě rovna

$$\upsilon = 2|T|. \tag{11.3}$$

Aplikace na konkrétní parametry Edonu-R
Nyní budeme uvažovat konkrétní parametry kvazigrupy, která je uvedena ve specifikaci [8]. Budeme se zabývat variantami pro $n = 256$ a $n = 512$. Z parametrů kvazigrupy a obecného vzorce pro složitost (9.16) odvodíme hodnotu t, která značí o kolik je krok zpět algoritmu MITM pomalejší než krok vpřed. Konkrétní hodnoty rotačních vektorů pro $n = 256$ jsou

$$\begin{aligned} r_\alpha &= (0, 4, 8, 13, 17, 22, 24, 29), \\ r_\beta &= (0, 5, 9, 11, 15, 20, 25, 27) \end{aligned}$$

a konkrétní hodnoty rotačních vektorů pro $n = 512$ jsou

$$\begin{aligned} r_\alpha &= (0, 5, 15, 22, 31, 40, 50, 59), \\ r_\beta &= (0, 10, 19, 29, 36, 44, 48, 55). \end{aligned}$$

Označíme-li $\mathcal{E} \in \mathcal{E}_1^1$ jako rovnici (11.1). Pak zřejmě platí

$$\begin{aligned} \Omega_{\alpha,\mathcal{E}} &= \{\hat{m}_1^{(2)}, \hat{m}_1^{(2)} * m_0^{(2)}\}, \\ \Omega_{\beta,\mathcal{E}} &= \{m_1^{(2)}\}. \end{aligned}$$

Využitím vzorce (9.17) získáme $t_{256} = 2^{186}$ pro $n = 256$ a $t_{512} = 2^{363}$ pro $n = 512$, neboť jeden běh zjednodušeného algoritmu z kapitoly 9 ztotožníme s jedním během kroku vpřed MITM útoku. Abychom minimalizovali celkovou časovou složitost algoritmu, tak zvolíme $|T_{256}| = 2^{35}$ a $|T_{512}| = 2^{75}$. Využitím (11.2) dostáváme

$$\begin{aligned} \tau_{256} &= 2^{222}, \\ \tau_{512} &= 2^{438} \end{aligned}$$

potřebných časových jednotek. Paměťová složitost je $\upsilon_{256} = 2^{36}$ uložených hodnot z $\{0,1\}^{256}$ a $\upsilon_{512} = 2^{75}$ uložených hodnot z $\{0,1\}^{512}$.

Poznámka 11.1. S neznámou $\hat{m}_1^{(2)}$ můžeme pracovat na stejném principu jako s neznámou $m_1^{(2)}$, protože permutaci slov můžeme jednodušše zabudovat do permutace $\mathbf{AddM}_{A,d}$ změnou matice A.

Poznámka 11.2. Shodu konkrétních matic N_k s předpokladem z kapitoly 9 jsme neprováděli, ale pro vzorec obecné složitosti bychom dostali podobné výsledky, které by neměly vliv na princip útoku.

Shrnutí: Ačkoli tento výsledek neznamená prolomení hašovací funkce Edon-R, protože neplatí, že $\tau_{256}\upsilon_{256} < 2^{256}$ nebo $\tau_{512}\upsilon_{512} < 2^{512}$, tak možnost této záměny časové a paměťové složitosti (time-memory trade-off) je přirozenou slabinou[1] hašovací funkce.

[1] pro stávající standart SHA-2 nejsou žádné útoky tohoto typu známé

Závěr

Základním cílem první části této práci byl rozbor řešitelnosti kvazigrupových rovnic v beztvarých kvazigrupách. Ukázali jsme, že hypotéza o jednosměrnosti funkce R_1 je nepřesná a navrhli jsme rozšíření definice beztvaré kvazigrupy o podmínku na neexistenci kongruence. V druhé části práce jsme se věnovali konkrétnímu návrhu hašovací funkce Edon-R a speciálně kvazigrupám definovaným v tomto návrhu. Představili jsme algoritmus na řešení kvazigrupových rovnic, který je pro rovnice, které nejsou příliš velké, efektivnější než algoritmus hrubého prohledávání. Tento algoritmus jsme následně aplikovali na konkrétní rovnice, které vyplývají z tvaru kompresní funkce Edon-R. Hodnoty paměťové a časové složitosti představeného útoku sice nesplňují požadavky na prolomení hašovací funkce, ale jistě představují slabinu. Proto naši kryptoanalýzu můžeme považovat částečně za úspěšnou.

Literatura

[1] G. E. Andrews: *Special functions*, Cambridge University Press, 1999.

[2] L. Bican: *Lineární algebra a geometrie*, Academia, Praha, 2000.

[3] I. Damgard: *A Design Principle for Hash Functions.* In Advances in Cryptology - CRYPTO '89 Proceedings, Lecture Notes in Computer Science Vol. 435, G. Brassard, ed, Springer-Verlag, 1989, pp. 416-427.

[4] A. Drápal: *Teorie grup: základní aspekty*, Karolinum, Praha, 2000.

[5] D. Gligoroski *Candidate One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations*, Cryptology ePrint Archive, Report 2005/352, 2005. http://eprint.iacr.org/.

[6] D. Gligoroski, S. Markovski, L. Kocarev: *Edon-R, An infinite family of cryptographic hash functions*, Second NIST Cryptographic Hash Workshop, University of California - Santa Barbara, 2006.

[7] D. Gligoroski, S. J. Knapskog: *Edon-R(256,384,512)-An efficient implementation of Edon-R family of cryptographic hash functions*, Comment.Math.Univ.Carolin., 49,2:219–239, 2008.

[8] D. Gligoroski, R.S. Odegard, M. Mihova, S.J. Knapskog, L. Kocarev, A. Drapal: *Cryptographic Hash Function EDON-R*, October 2008, SHA-3 submission.

[9] O. Goldreich: *Foundations of Cryptography*, Cambridge University Press 2001.

[10] M. V. Horoševskii: *On automorphisms of finite groups*, Math. USSR Sb. 22 584-594 (1974).

[11] A. Joux: *Multicollisions in iterated hash functions. Aplication to cascaded constructions.*, CRYPTO 2004, 306-316.

[12] D. Khovratovich, I. Nikolić, R.-P. Weinmann: *Cryptanalysis of Edon-R.* Available online, 2008.

[13] S. Lucks: *Design principles for iterated hsh functions*, Cryptology ePrint Archive, Report 2004/253, 2004. http://eprint.iacr.org/.