Slovenská Technická Univerzita

Fakulta Elektrotechniky a Informatiky

Katedra Aplikovanej informatiky a výpočtovej techniky

Ilkovičova 3, 812 19 Bratislava 1

Marek Sýs

LATINSKÉ ŠTVORCE V KRYPTOGRAFII

dizertačná práca

Školiteľ: Prof. RNDr. Otokar Grošek, PhD.

Odbor: 9-1-9 Aplikovaná matematika

August 2009
Bratislava

Prehlásenie

Týmto prehlasujem, že predkladaná dizertačná práca je výsledkom mojej vlastnej práce a neobsahuje výsledky, ani čiastočné výsledky, iných ľudí mimo citovaných. Taktiež prehlasujem, že som použil len literatúru uvedenú zozname použitej literatúry.

Bratislava, August 10, 2009 Marek Sýs

Poďakovanie

Rád by som poďakoval Profesorovi Otokarovi Grošekovi za cenné pripomienky a rady, ktoré prispeli k skvalitneniu predloženej práce. Rovnako tak za jeho ochotu a trpezlivosť pri recenzovaní predošlých verzií. Tiež by som sa chcel poďakovať aj ostatným kolegom na Katedre KAIVT za rady a pomoc pri obstarávaní potrebnej literatúry.

Obsah

KAPITOLA 1

Zoznam symbolov

I_n	množina tvorená prvkami $1, 2, 3, \ldots, n$
$S(L)$	množina symbolov Latinského štvorca L
$Is(L)$	grupa autotopizmov Latinského štvorca L
$Is(L_1, L_2)$	množina izotopizmov Latinského štvorca L_1 na L_2
Ω_n	množina všetkých štvorcov rádu n
$\mathcal{L}_n$	množina všetkých štvorcov rádu n nad množinou symbolov I_n
$Sym(X)$	symetrická grupa prvkov množiny X
S_n	symetrická grupa prvkov I_n
I'_n	izotopizmy grupoidu s prvkami I_n
L_Q	množina l'avých translácií kvázigrupy Q
$C_n(g, h)$	množina prvkov $p \in S_n$, pre ktoré platí $pgp^{-1} = h$
$C_n(g, H)$	množina prvkov $p \in S_n$, pre ktoré platí $pgp^{-1} \in H$
$C_n(G, H)$	množina prvkov $p \in S_n$, pre ktoré platí $pGp^{-1} = H$
$\mathbb{Z}_n$	množina tried ekvivalencie modulo n
$\mathbb{F}_{p^r}$	konečné pole rádu p^r
$AUT(Q)$	grupa autotopizmov kvázigrupy Q
$Aut(G)$	grupa automorfizmov grupy G
$Hol(G)$	holomorf grupy G
$St_G(\alpha)$	stabilizátor prvku $\alpha \in X$ v akcii grupy G na množine X

KAPITOLA 2

Úvod

Použitie Latinských štvorcov, ako stavebných prvkov kryptografických systémov nemá dlhú tradíciu. Aj keď už skôr existovali kryptografické aplikácie využívajúce Latinské štvorce a kvázigrupy, ich použitie v nich bolo len okrajové. Začiatky použitia Latinských štvorcov v kryptografii sa dajú datovať zhruba do 90-tych rokov minulého storočia, keď bola navrhnutá bloková šifra IDEA [**34**]. V nej bol prvý krát použitý koncept neizotópnych kvázigrúp. Od toho času sa objavilo viacero prác dotýkajúcich sa kvázigrúp v súvislosti s kryptografiou. Teória S-boxov založených na kvázigrupách bola študovaná v prácach [**53**] a [**25**], v ktorých bol popísaný spôsob konštrukcie perfektne nelineárnych S-boxov s kompletne plochou diferenčnou tabuľkou.

V práci [**29**] popísal C. Koscielny metódu konštrukcie prúdových šifier postavených na kvázigrupách. E. Ochodková a V.Snášel v [**48**] navrhli ďalšie použitie kvázigrúp pri bezpečnom šifrovaní súborov. V [**39**] autori navrhli prúdovú šifru s takmer verejným kľúčom, kde sa šifrovanie a dešifrovanie konalo priamo v kvázigrúpách. V [**30**] bol uverejnený kryptosystém s verejným kľúčom postavenom na kvázigrupách. Ďalší široký prehľad použitia kvázigrúp v kryptografii možno vidieť v článku [**52**].

Ako najväčšieho prispievateľa k danej problematike možno pokladať D. Gligoroského, ktorého široké spektrum prác vyvrcholilo návrhom prúdovej šifry Edon80[**22**], ktorá je postavená výhradne na Latinských štvorcoch. Edon80 sa úspešne zúčastnil v súčasnosti už ukončeného projektu ECRYPT eSTREAM

[**19**], ktorý postavil prúdové šifry do centra pozornosti kryptologickej verejnosti. Jeho cieľom bolo odporučiť vybrané prúdové šifry pre štandardizáciu a zároveň výrazne podporiť výskum v tejto oblasti. Edon80 sa dostal do záverečnej tretej časti, kde však nakoniec neuspel. Akokoľvek už samotný fakt, že sa dostal do finálového výberu hovorí o potenciály Latinských štvorcov pre kryptografiu.

Z predchádzajúceho vidno, že Latinské štvorce si už v súčasnosti našli široké uplatnenie v kryptografii. Preto aj analýza ich vlastností tvorí významnú časť kryptoanalýzy, ako odvetvia kryptografie skúmajúcej bezpečnosť navrhovaných systémov. Základnou charakteristikou Latinských štvorcov je ich príslušnosť k takzvanej izotópnej triede. Jej prvky obsahujú štvorce, ktoré sa od seba líšia len prehodením riadkov, stĺpcov alebo symbolov. Sú teda určitým spôsobom podobné.

Práve takéto štvorce využíva prúdová šifra Edon 80. Na túto skutočnosť poukázala práca [**59**]. Analýza štvorcov Edonu80 prebiehala metódou úplného prehľadania, čo bolo možné len z toho dôvodu, že štvorce sú rozmeru 4×4. V súčasnosti však predložený návrh hašovacej funkcie EdonR [**23**] ako kandidáta na štandard SHA3 pracuje v kvázigrupách s rozmermi neporovnateľne väčšími.

Preto by bolo vhodné mať silný nástroj na posúdenie izotópnosti dvoch Latinských štvorcov. Tomuto tématu sa venovala už staršia Millerova práca [**43**], kde autor navrhol algoritmus so zložitosťou $O(n^{log_2 n})$. Autor vychádzal z Tarjanovho algoritmu [**57**] testujúceho izomorfnosť dvoch grúp.

Ako vidíme zložitosť algoritmu je už pre relatívne nízke n vysoká, preto tento nie je realizovateľný pri analýze štvorcov použitých v EdonR. Ďalšie algoritmy, ktoré hľadajú izotopizmy pracujú s grafovými reprezentáciami Latinských štvorcov. Tu sa hľadajú izomorfizmy silne regulárnych grafov. Ako ukazuje [**56**] zložitosť takýchto algoritmov je $O(n^{n^{1/3} log_2 n})$ a teda tieto sú vo všeobecnosti pomalšie ako Millerov algoritmus. Z toho dôvodu je nutné navrhnúť rýchlejší algoritmus testujúci izotópnosť.

Aj keď si už Latinské štvorce našli svoje miesto pri návrhu kryptografických systémov stále existujú oblasti, ktorých sa štvorce prakticky nedotkli. Jednou z takých oblastí je možnosť generovania podkľúčov blokových šifier, kde sa vyžaduje jednosmernosť návrhu. To dáva priestor na použitie štvorcov, keďže na tie sa dá nazerať ako tabuľku operácie kvázigrupy, v ktorej už riešenie dvoch polynomiálnych rovníc vyšších stupňov s viacerými premennými môže byť NP-ťažký problém [**49**],[**28**]. Predkladaná práca si preto kladie nasledujúce ciele:

(1) preskúmať možnosť rýchlejšieho posúdenia izotópnosti dvoch kvázigrúp.
(2) navrhnúť bezpečný algoritmus na generovanie podkľúčov s využitím Latinských štvorcov.

Práca je rozdelená na štyri hlavné kapitoly. V kapitole 3 popisujeme základné vlastnosti Latinských štvorcov a kvázigrúp. Ich úzke prepojenie a možné reprezentácie. Ďalej sa tu nachádza popis možných transformácií kvázigrúp a ich základné rozdelenia a v neposlednom rade je tu popísaná štruktúra kvázigrúp z pohľadu akcií symetrických grúp.

Kapitola 4 sa venuje návrhu nového algoritmu na hľadanie izotopií dvoch kvázigrúp. Ako vedľajší produkt možno klasifikovať algoritmus 4, ktorý nájde optimálne všetky prvky, ktoré konjugujú n prvkové množiny permutácií. Na základe návrhu algoritmu sú tu odvodené nové odhady maximálneho počtu izotopizmov kvázigrúp, ktoré výrazne upresňujú doposiaľ známe z [**13**]. V kapitole je prezentovaný univerzálny vzorec pre výpočet množstva autotopií konečných grúp vychádzajúci z konštrukcie algoritmu. Jedná sa o alternatívny vzorec k vzorcu z [**3**] a teda potvrdzuje korektnosť algoritmu.

Záver kapitoly je venovaný posúdeniu algoritmu a jeho porovnanie s už známymi algoritmami tohoto typu a odhad jeho zložitosti. Nachádzajú sa tu tiež výsledky experimentov, z ktorých možno usúdiť, že nová nutná podmienka izotópnosti kvázigrúp môže byť vhodným nástrojom pri zisťovaní izotópnosti veľkých kvázigrúp, kde už známe algoritmy nemajú uplatnenie.

V kapitole 5 sa zaoberáme perfektnou nelinearitou a balansovanosťou S-boxov. Uvádzame tu jednodnoduchý postup na skonštruovanie Latinských štvorcov ako funkcií s plochou diferenčnou tabuľkou vhodných pre použitie v návrhoch kryptosystémov. Tie sa následne používajú v kapitole 6, kde sa venujeme novému prístupu ku generovaniu podkľúčov blokových šifier prostredníctvom Latinských štvorcov. V kapitole sa nachádza podrobný návrh algoritmu a jeho analýza. Tento je následne otestovaný v reálnom prostredí s ohľadom na známe požiadavky na návrh kladené. V závere je na základe štatistických testov posúdená bezpečnosť návrhu.

KAPITOLA 3

Latinské štvorce a kvázigrupy

V tejto kapitole uvedieme niektoré známe fakty týkajúce sa Latinských štvorcov. Popíšeme v nej základnú štruktúru Latinských štvorcov, ich rozdelenia a možné transformácie.

Uvedieme tu tiež algebraický pohľad na Latinské štvorce prostredníctvom kvázigrúp, keďže Latinské štvorce a kvázigrupy spolu úzko súvisia.

3.1. Latinské štvorce

Pojem Latinský štvorec siaha hlboko do minulosti. Prvýkrát bol systematicky skúmaný Eulerom, ktorý ho definoval nasledovne:

DEFINÍCIA 3.1. [**13**] *Latinský štvorec L rozmeru n je tvorený tabuľkou rozmerov $n \times n$ nad n prvkovou množinou symbolov, pričom sa každý symbol nachádza v každom riadku a stĺpci práve raz.*

Prirodzené číslo n z definície 3.1 sa volá rozmer (rád) Latinského štvorca. Množinu všetkých Latinských štvorcov rádu n budeme podľa [**13**] označovať symbolom Ω_n. Množinu symbolov Latinského štvorca L budeme označovať $S(L)$. Symbol Latinského štvorca L, ktorý sa nachádza v jeho i-tom riadku a j-tom stĺpci budeme označovať symbolom l_{ij} prípadne $L(i, j)$. V súčasnosti sa bez ujmy na všeobecnosti definuje Latinský štvorec nad jednotnou množinou symbolov $I_n = \{1, 2, \ldots, n\}$ [**40**]. Množinu všetkých štvorcov nad I_n budeme v ďalšom texte označovať $\mathcal{L}_n$.

POZNÁMKA 3.2. Za množinu symbolov Latinských štvorcov sa berie fixná množina v prípade, keď sa jedná o počty štruktúr so štvorcami súvisiacich. Dôvod je zrejmý a síce, že

počet štvorcov nad ľubovoľnou množinou symbolov je nekonečný. Naproti tomu fixovaním množiny symbolov dostávame konečné číslo[**42**].

My sa budeme ďalej z rôznych dôvodov pridržiavať pôvodnej definície. Len v prípadoch z poznámky 3.2 budeme chápať Latinské štvorce nad jednotnou množinou symbolov.

3.1.1. Rozdelenie Latinských štvorcov. Tu si popíšeme základné rozdelenia Latinských štvorcov. Množina $\mathcal{L}_n$ nadobúda už pre malé n obrovské rozmery [**40**], čo prakticky znemožňuje pracovať s celou $\mathcal{L}_n$ ako takou. Z toho dôvodu sa táto množina delí na rôzne typy tried. Tie majú zväčša tú vlastnosť, že pomocou jediného Latinského štvorca danej triedy (zástupca triedy) možno použitím vhodných transformácií vygenerovať celú túto triedu.

3.1.1.1. *Izotopia.* Ako bolo spomenuté vyššie, existujú transformácie Latinských štvorcov, ktorých výsledkom je opäť Latinský štvorec. Medzi základné typy takýchto transformácií patria nasledovné:

- preusporiadanie riadkov
- preusporiadanie stĺpcov
- premenovanie symbolov

Tieto transformácie sa často využívajú pri vyšetrovaní vlastností prvkov Ω_n a tak štvorce, ktoré sú v uvedenom vzťahu (relácii), boli pomenované izotópne. Stalo sa tak zrejme z dôvodu, že izotópnosť a izomorfosť sú z algebraického hľadiska veľmi podobné pojmy ako možno vidieť z nasledujúcich definícií.

DEFINÍCIA 3.3. [**12**] *Hovoríme, že dva Latinské štvorce sú izotópne alebo ekvivalentné, ak preusporiadaním stĺpcov, riadkov a premenovaním symbolov jedného z nich možno získať druhý.*

DEFINÍCIA 3.4. [**12**] *Nech Latinské štvorce L a L' sú izotópne. Nech θ, ψ, φ sú bijekcie $\theta, \varphi : I_n \to I_n$ a $\psi : S(L) \to S(L')$ také, že*

$$\psi(L(\theta(i), \varphi(j))) = L'(i, j).$$

Potom usporiadanú trojicu (θ, φ, ψ) voláme izotopizmus Latinského štvorca L na L'. Ak sú štvorce L a L' totožné ($L(i,j) = L'(i,j)$ pre všetky $(i,j) \in I_n \times I_n$), tak izotopizmus medzi nimi voláme tiež autotopizmom.

Aplikáciu izotopizmu (θ, φ, ψ) na Latinský štvorec L budeme označovať symbolom $L^{(\theta,\varphi,\psi)}$.

POZNÁMKA 3.5. Izotopizmy možno podľa [**13**] prirodzene: skladať

$$\left(L^{(\alpha,\beta,\gamma)}\right)^{(\alpha_1,\beta_1,\gamma_1)} = L^{(\alpha_1\alpha,\beta_1\beta,\gamma_1\gamma)}$$

a invertovať

$$L^{(\alpha,\beta,\gamma)} = L_1 \leftrightarrow L_1^{(\alpha^{-1},\beta^{-1},\gamma^{-1})} = L.$$

Ako vidno z definície 3.4 možno s istou dávkou benevolencie povedať, že pojem izotópnosti zovšeobecňuje izomorfnosť. Názornejšie je to vidieť, keď sa pozeráme na Latinský štvorec prostredníctvom teórie kvázigrúp. Akokoľvek izotopia predstavuje dôležitú reláciu medzi štvorcami. Tá je dokonca reláciou ekvivalencie, ako možno vidieť z nasledujúcej vety.

VETA 3.6. [**13**] *Izotopia určuje reláciu ekvivalencie na množine Ω_n všetkých Latinských štvorcov rádu n.*

Veta hrá dôležitú rolu pri klasifikácii Latinských štvorcov. Plynie z nej, že relácia "izotopia" delí množinu Ω_n, rovnako ako $\mathcal{L}_n \subseteq \Omega_n$, na disjunktné triedy(množiny) izotópnych štvorcov.

DEFINÍCIA 3.7. [**13**] *Izotópna trieda pozostáva z Latinských štvorcov, ktoré sú navzájom izotópne (ekvivalentné).*

3.1.1.2. *Paratopia.* Ďalšou možnosťou, ako rozdeliť množiny Ω_n a $\mathcal{L}_n$ na disjunktné triedy, je použiť nasledovnú definíciu konjugovaných štvorcov.

DEFINÍCIA 3.8. [**12**] *Nech L je Latinský štvorec nad n prvkovou množinou symbolov E_3 a nech n prvkové množiny E_1, E_2 indexujú po rade riadky a stĺpce štvorca L. Nech*

$$\mathcal{T} = \{(x_1, x_2, x_3) : L(x_1, x_2) = x_3\}$$

pre $\{a, b, c\} = \{1, 2, 3\}$. *Potom konjugovaný (paratópny) štvorec* $L_{(a,b,c)}$ *ku štvorcu* L *je taký Latinský štvorec, ktorý má riadky, stĺpce a symboly indexované po rade množinami* E_a, E_b, E_c *a je definovaný vzťahom*

$$L_{(a,b,c)}(x_a, x_b) = x_c$$

pre všetky $(x_1, x_2, x_3) \in \mathcal{T}$.

Konjugovanosť a izotopia potom spolu určujú iný typ relácie Latinských štvorcov nazvaný paratopia.

DEFINÍCIA 3.9. [**42**] *Hovoríme, že dva Latinské štvorce* L, L' *sú paratópne, ak* L *je izotópny k ľubovoľnému konjugovanému štvorcu štvorca* L'.

Definícia 3.9 dáva do súvisu tie Latinské štvorce, ktoré možno transformovať medzi sebou prostredníctvom transformácií definujúcich izotopiu (permutácie riadkov, stĺpcov, premenovanie symbolov) a ďalšej špeciálnej transformácie.

Ta sa dá v skratke popísať nasledovne: Vezmime Latinský štvorec L nad množinou symbolov $S(L) = I_n$ a jeho ortogonálnu reprezentáciu.

POZNÁMKA 3.10. Ortogonálna reprezentácia Latinského štvorca L rádu n je množina tvorená n^2 usporiadanými trojicami tvaru $(i, j, L(i, j))$ pre $1 \leq i, j \leq n$.

Ak v tejto reprezentácii preusporiadame rovnakým spôsobom každú trojicu, dostávame ortogonálnu reprezentáciu Latinského štvorca L', ktorý je konjugovaný k L (definícia 3.8, kde $E_1 = E_2 = E_3 = I_n$).

PRÍKLAD 3.11. V tabuľke 3.11 môžeme vidieť Latinský štvorec L a k nemu konjugovaný $L_{(3,1,2)}$, ktorého ortogonálny zápis má tvar $(L(i, j), i, j)$ pre $(i, j) \in I_3 \times I_3$.

1	2	3
3	1	2
2	3	1

1	2	3
2	3	1
3	1	2

TABUĽKA 1. Konjugované štvorce L a L'.

Relácia paratopie je podobne ako izotopia reláciou ekvivalencie na množine Latinských štvorcov [**13**], a teda podľa nej možno Latinské štvorce rozdeliť na triedy ekvivalencie.

DEFINÍCIA 3.12. [**13**] *Množina Latinských štvorcov paratópnych k danému Latinskému štvorcu L sa volá hlavná trieda štvorca L.*

Z predchádzajúceho je zrejmé, že hlavná trieda pozostáva zo šiestich izotópnych tried. Tieto však nemusia byť nutne rôzne ako možno vidieť už v príklade 3.11, kde konjugované štvorce $L, L_{(3,1,2)}$ patria k tej istej izotópnej triede.

Veľmi dôležité postavenie medzi Latinskými štvorcami majú takzvané redukované Latinské štvorce.

DEFINÍCIA 3.13. [**12**] *Latinský štvorec L rádu n nad množinou symbolov $S(L) = \{1, 2, \ldots, n\}$ voláme redukovaný alebo v štandardnej forme, ak v prvom riadku a stĺpci sú symboly usporiadané prirodzeným spôsobom.*

Dôležitosť redukovaných štvorcov indukuje fakt, že obvykle sa zadaná úloha (zahŕňajúca Latinské štvorce) transformuje na úlohu, kde sa hľadajú redukované štvorce s požadovanou vlastnosťou. Riešenie pôvodnej úlohy potom možno odvodiť z nájdených redukovaných štvorcov za pomoci vhodných transformácií.

Ako typický príklad možno vziať úlohu generovania všetkých Latinských štvorcov z $\mathcal{L}_n$. Pri jej riešení sa nájdu všetky redukované štvorce rádu n a z nich potom možno pomocou preusporiadania riadkov a stĺpcov získať všetky prvky $\mathcal{L}_n$.

3.1.2. Akcie na množine Latinských štvorcov. V tomto odseku popíšeme vyššie definované pojmy (izotopia, paratopia, ...) pomocou akcií definovaných na Latinských štvorcoch. Toto bude prospešné pri jednoduchšom dokazovaní niektorých tvrdení.

3.1.2.1. *Akcie, orbity a stabilizátory.*

DEFINÍCIA 3.14. [**50**] *Nech G je grupa a X je neprázdna množina. Ľavou akciou grupy G na množine X voláme funkciu*

$$\alpha : G \times X \mapsto X$$

takú, že pre všetky $g_1, g_2 \in G$ a $x \in X$ platí:

- $\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$
- $\alpha(1_G, x) = x$.

V ďalšom texte budeme podľa obyčaje zapisovať $\alpha(g, x)$ ako $\alpha(g, x) = g.x$.Ako príklad často sa vyskytujúcej akcie možno vziať akciu grupy G na množine $X = G$ jej vlastných prvkov, ktorá je daná predpisom $x.g = g^{-1}xg$. Spomínaná akcia sa volá akcia konjugáciou a často sa využíva pri vyšetrovaní vlastností jednotlivých grúp. V práci budeme často používať špeciálnu akciu s názvom ľavá regulárna akcia grupy. Tá úzko súvisí s permutačnými reprezentáciami grúp.

DEFINÍCIA 3.15. [**50**] *Nech G je grupa a X je neprázdna množina. Potom homomorfizmus $\sigma : G \mapsto Sym(X)$ voláme permutačná reprezentácia grupy G na množine X.*

Úzku spojitosť medzi permutačnými reprezentáciami grupy a akciami na grupách potvrdzuje nasledujúca veta.

VETA 3.16. [**50**] *Nech G je grupa a X je neprázdna množina. Potom existuje bijekcia z množiny ľavých akcií G na X do množiny permutačných reprezentácií grupy G.*

Jej dôsledkom je známa Cayleyho veta o izomorfnosti grupy G a jej ľavej regulárnej reprezentácii.

DEFINÍCIA 3.17. [**50**] *Akcia grupy G na množine $X = G$ danú predpisom $x.g = xg$ voláme ľavá regulárna akcia grupy G. Zobrazenie $\lambda : G \mapsto Sym(G)$ dané predpisom $\lambda(g)(x) = gx$ voláme ľavá regulárna reprezentácia grupy G.*

VETA 3.18 (Cayleyho veta). [**50**] *Ľubovoľná grupa G je izomorfná s podgrupou $Sym(G)$ prostredníctvom priradenia $g \mapsto (x \mapsto gx)$ pre $x, g \in G$.*

Teraz popíšeme základné pojmy týkajúce sa akcií. Nech G je grupa a X neprázdna množina. Uvažujme ľavú akciu "." grupy G na množine X. Vezmime reláciu $\sim_G$ na množine X definovanú podľa pravidla $a \sim_g b$ práve vtedy, keď $g.a = b$ pre nejaké $g \in G$.

Dá sa ľahko ukázať, že relácia $\sim_G$ určuje reláciu ekvivalencie na množine X. V tejto súvislosti uvažujeme dva dôležité pojmy stabilizátor prvku a orbita prvku.

DEFINÍCIA 3.19. [**50**] *Stabilizátor $St_G(a)$ prvku $a \in X$ je podmnožina grupy G tvaru $St_G(a) = \{g.a = a | g \in G\}$. Teda $St_G(a)$ je tvorený všetkými prvkami grupy G, ktoré ponechávajú v akcii "." prvok a na mieste.*

Orbita prvku a je naopak množina tvaru $G.a = \{g.a | g \in G\}$. Teda orbita je tvorená všetkými obrazmi akcie "." na prvku a.

Najdôležitejšie fakty týkajúce sa akcií, orbít a stabilizátorov popisuje nasledujúca veta:

VETA 3.20. [**17**] *Majme akciu grupy G na množine X a $g_1, g_2 \in G$ a $\alpha, \beta \in X$. Potom :*

(1) *Dve orbity $G.\alpha$ a $G.\beta$ sú ako množiny zhodné alebo disjunktné. Teda tvoria rozklad X.*
(2) *Stabilizátor $St_G(\alpha)$ tvorí podgrupu grupy G a $St(\alpha) = gSt(\beta)g^{-1}$, ak $g_1.\alpha = \beta$. Naviac $g_1.\alpha = g_2.\alpha$ práve vtedy, keď $g_1 St_G(\alpha) = g_2 St_G(\alpha)$.*
(3) *Platí $|G.\alpha| = |G : St(\alpha)|$ pre všetky $\alpha \in X$. Ak G je konečná potom $|G.\alpha||St_G(\alpha)| = |G|$.*

POZNÁMKA 3.21. Pre grupu G a jej podgrupu H označuje $G : H$ triedy rozkladu grupy G podľa podgrupy H [**8**].

Už na začiatku sekcie 3.1 sme uviedli, že bez ujmy na všeobecnosti sa zvyčajne definujú Latinské štvorce nad jednotnou množinou symbolov. Teraz je vhodný čas ozrejmiť, čo vlastne toto "bez ujmy" znamená. Zamerajme sa na izotopizmy medzi Latinskými štvorcami rádu n. Uvažujme štvorce nad jednotnou množinou symbolov vo vzťahu k ľubovoľným prvkom Ω_n. Vezmime si dva izotópne Latinské štvorce $L_1, L_2 \in \Omega_n$ s $S(L_1) \neq S(L_2)$. Označme množinu ich izotopizmov L_1 na L_2 ako $Is(L_1, L_2)$.

Pýtame sa ako možno nájsť $Is(L_1, L_2)$, ak narábame len so štvorcami nad symbolovou množinou $S(L_1)$.

POZNÁMKA 3.22. Tu nemôžeme použiť akciu izotopizmov na Latinských štvorcoch, keďže izotopizmy Latinských štvorcov nad rôznymi symbolovými množinami nemožno vo všeobecnosti skladať. Tento nedostatok sa odstráni, keď uvažujeme štvorce s jednotnou množinou symbolov. K tomu koniec koncov v tomto odseku smerujeme.

Pomôžeme si nasledujúcou lemou.

LEMA 3.23. *Pre ľubovoľné dva Latinské štvorce z danej izotópnej triedy je počet ich izotopizmov rovnaký.*

DÔKAZ. Majme izotópne štvorce L_1, L_2, L_3. Označme symbolom $Is(L_i, L_j)$ množinu všetkých izotopizmov štvorcov L_i, L_j pre $i, j \in I_3$. Vezmime si štvorce L_{i_1}, L_{i_2} a izotopizmus $\sigma \in Is(L_{i_1}, L_{i_2})$. Majme ľubovoľný izotopizmus $\delta \in Is(L_{i_2}, L_{i_3})$. Z poznámky 3.5 plynie, že $\delta\sigma \in Is(L_{i_1}, L_{i_3})$. Naviac je zrejmé, že pre rôzne δ dostávame rôzne izotopizmy $\delta\sigma$. Preto platí

$$|Is(L_{i_1}, L_{i_2})| \leq |Is(L_{i_2}, L_{i_3})|.$$

Toto platí pre ľubovoľný výber i_1, i_2, i_3 a teda mohutnosť množiny $Is(L_{i_1}, L_{i_2})$ je pre ľubovoľný výber $i_1, i_2 \in I_3$ rovnaká. □

Dôkaz lemy nám dáva návod ako skonštruovať zo znalosti $Is(L_1, L_2)$ a jediného izotopizmu medzi štvorcami L_2, L_3 množinu $Is(L_1, L_3)$.

Vezmime teraz Latinský štvorec L_3 izotópny s L_2 prostredníctvom izotopizmu $\sigma = (id, id, \psi)$ ($L_2^{(id,id,\psi)} = L_3$), kde $\psi : S(L_2) \mapsto S(L_3)$ je ľubovoľná bijekcia a id predstavuje identickú permutáciu na I_n. Z dôkazu lemy a zo skladania izotopizmov (poznámka 3.5) máme $Is(L_1, L_2) = (id, id, \psi)Is(L_1, L_3)$.

Ako vidíme, pri hľadaní izotopizmov štvorcov sa stačí zamerať len na štvorce nad rovnakou množinou symbolov.

Vezmime si teraz Latinské štvorce $\mathcal{L}_n$ nad množinou symbolov I_n a grupu $G = S_n \times S_n \times S_n = S_n^3$ s operáciou skladania permutácií po zložkách. Majme akciu grupy G na množine Latinských štvorcov $\mathcal{L}_n$ definovanú predpisom $(\theta, \varphi, \psi).L = L^{(\theta,\varphi,\psi)}$. Táto je zjavne dobre definovaná (poznámka 3.5).

Izotópna trieda Latinského štvorca L podľa definície 3.7 je potom zhodná s orbitou $S_n^3.L$ v tejto akcii. Stabilizátor $St_{S_n^3}(L)$, ktorý budeme označovať symbolom $Is(L)$, je tvorený izotopizmami, ktoré zachovávajú štvorec L.

POZNÁMKA 3.24. Stabilizátor $Is(L)$ tvorí grupu nazývanú aj autotópna grupa. Jej prvky voláme autotopizmy.

Všeobecnejšie, $\sigma \in S_n^3$ je izotopizmom štvorca L na L', ak platí $\sigma.L = L'$. Vezmime si teraz grupu S_3. Vezmime akciu tejto grupy na množine Latinských štvorcov definovanú ako $\tau.L = L_{(\tau(1)\tau(2)\tau(3))}$ pre $\tau \in S_3$. Permutácia τ teda určuje, ktorý zo 6 konjugovaných štvorcov k L bude výsledný štvorec $\tau.L$.

POZNÁMKA 3.25. Štvorec $L_{(\tau(1)\tau(2)\tau(3))}$ budeme skrátene zapisovať ako L_τ.

Zložením predchádzajúcich dvoch akcií možno zadefinovať novú akciu grupy $S_n^3 \times S_3$ na množine Latinských štvorcov $\mathcal{L}(n)$ definovanú vzťahom $(\theta, \psi, \varphi, \tau).L = L_\tau^{(\theta,\psi,\varphi)}$. Orbita štvorca L v tejto akcii potom predstavuje hlavnú triedu štvorca L. Naopak, stabilizátor Latinského štvorca L, ktorý budeme označovať podľa [**42**] $Par(L)$, je grupa vyjadrená ako $Par(L) = \{\sigma \in S_n^3 \times S_3 | \sigma.L = L\}$.

POZNÁMKA 3.26. Grupa $Par(L)$ sa tiež nazýva autoparatópna grupa štvorca L a jej prvky sú autotoparatopizmy.

Z predchádzajúceho je vidieť, že niektoré základné pojmy týkajúce sa Latinských štvorcov sa dajú popísať pomocou akcií na množine $\mathcal{L}(n)$. Naviac pomocou nich možno jednoduchým spôsobom dokázať nasledujúcu vetu.

VETA 3.27. *Ak L a L' sú izotópne, potom aj k nim konjugované štvorce L_τ, L'_τ pre ľubovoľné $\tau \in I_3$ sú izotópne.*

DÔKAZ. Vezmime spomínanú akciu grupy $S_n^3 \times S_3$ na množine Latinských štvorcov s $S(L) = I_n$. Majme izotopizmus (θ, φ, ψ) štvorca L na L'. Platí teda $(\theta, \varphi, \psi, id).L = L'$. Z toho vyplýva $L_\tau^{(\theta,\psi,\varphi)} = (\theta, \varphi, \psi, \tau).L = (id, id, id, \tau)L' = L'_\tau$, čo dokazuje vetu. □

3.2. Kvázigrupy

V dnešnej dobe sa pozeráme na Latinský štvorec cez algebraickú teóriu grúp a jej zovšeobecnenia. Tie viedli k zavedeniu pojmu kvázigrupa. Kvázigrupa sa definuje nasledovne:

DEFINÍCIA 3.28. [**13**] *Množina Q s binárnou operáciou $*$ tvorí kvázigrupu $(Q, *)$, ak pre l'ubovol'né prvky $a, b \in Q$ majú rovnice*

$$a * x = b,$$

$$y * a = b$$

jednoznačné riešenie.

Kvázigrupa je, ako už samotný názov napovedá, úzko spätá s pojmom grupa. Porovnaním definície 3.28 kvázigrupy a grupy [**7**] je možné nazerať na kvázigrupu ako na grupu ochudobnenú o asociativitu.

3.2.1. Rozdelenie kvázigrúp. Podobne ako pri Latinských štvorcov, aj nad kvázigrupami sú definované relácie, ktoré dávajú do súvisu "podobné" kvázigrupy. Základnou reláciou medzi kvázigrupami je relácia izotopie. Nasledujúca definícia hovorí o tom, kedy sú dve kvázigrupy izotópne.

DEFINÍCIA 3.29. [**13**] *Nech $(Q_1, *_1), (Q_2, *_2)$ sú dve kvázigrupy a nech pre bijektívne zobrazenia $\theta, \varphi, \psi : Q_1 \to Q_2$ platí*

$$\theta(x) *_2 \varphi(y) = \psi(x *_1 y)$$

pre l'ubovol'né $x, y \in Q_1$. Potom hovoríme, že kvázigrupy $(Q_1, *_1), (Q_2, *_2)$ sú izotópne. Usporiadanú trojicu (θ, φ, ψ) voláme izotopizmus kvázigrupy $(Q_1, *_1)$ na $(Q_2, *_2)$.

Relácia izotopie kvázigrúp určuje, podobne ako pre Latinské štvorce reláciu ekvivalencie [**13**].

Ďalším nemenej dôležitým pojmom v teórii kvázigrúp je konjugovanosť kvázigrúp.

DEFINÍCIA 3.30. [**12**] *Nech $(Q, *)$ je kvázigrupa. Vezmime šest' binárnych operácií $*_{(1,2,3)}, *_{(1,3,2)}, *_{(2,1,3)}, *_{(2,3,1)}, *_{(3,1,2)},$*

$*_{(3,2,1)}$ *nad* Q *definovaných nasledovne: rovnosť* $a * b = c$ *platí práve vtedy, keď*

$$a *_{(1,2,3)} b = c, a *_{(1,3,2)} c = b, b *_{(2,1,3)} a = c,$$

$$b *_{(2,3,1)} c = a, c *_{(3,1,2)} a = b, c *_{(3,2,1)} b = a$$

Hovoríme, že kvázigrupy $(Q, *_{(i,j,k)})$, *kde* $\{i, j, k\} = \{1, 2, 3\}$ *sú konjugované s kvázigrupou*$(Q, *)$.

POZNÁMKA 3.31. Treba poznamenať, že všetky kvázigrupy $(Q, *_{(i,j,k)})$ sú konjugované aj navzájom a teda relácia "byť konjugovaný" je reláciou ekvivalencie na množine kvázigrúp.

3.2.2. Základné vlastnosti kvázigrúp. Teraz popíšeme základné vlastnosti kvázigrúp a izotopizmov medzi nimi.

Ako sme mohli vidieť vyššie, pri kvázigrupách sa používajú rovnaké pojmy ako pri Latinských štvorcoch. Dokonca aj ich definície a správanie sa sú takmer rovnaké. To dáva tušiť úzku previazanosť Latinských štvorcov a kvázigrúp. Túto skutočnosť potvrdzuje nasledujúca veta.

VETA 3.32. [**13**] *Multiplikatívna tabuľka ľubovoľnej kvázigrupy tvorí Latinský štvorec.*

Podľa nej možno teda na Latinský štvorec nazerať ako na Cayleyho tabuľku nejakej kvázigrupy. Z toho vyplýva, že narábať s kvázigrupou v podstate znamená narábať s Latinským štvorcom ako jej tabuľkou operácie. Preto možno pojmy a úvahy týkajúce sa Latinských štvorcov preniesť do prostredia kvázigrúp bez straty významu. Pre izotopizmy to teda znamená, že tieto možno skladať a invertovať podľa poznámky 3.5. To sa dá koniec koncov nahliadnuť aj priamo z definície 3.4.

Rovnako ako pri Latinských štvorcoch sa pri hľadaní izotopizmov stačí zamerať na kvázigrupy nad fixnou množinou prvkov. Platí tu podobná úvaha ako pri Latinských štvorcoch. V prípade kvázigrúp stačí nahradiť Latinské štvorce L_i, kvázigrupami $(Q_i, *_i)$ pre $i \in I_3$. A namiesto izotopizmu (id, id, ψ) štvorca L_2 na L_3 treba vziať izotopizmus (ψ, ψ, ψ) kvázigrupy $(Q_2, *_2)$ na $(Q_1, *_3)$, kde bijekcia $\varphi : Q_2 \mapsto Q_3$ je opäť ľubovoľná. Keďže lema 3.23 platí aj pre izotopizmy kvázigrúp,

platí aj zvyšok úvahy a teda stačí sa zaoberať len kvázigrupami nad fixnou množinou prvkov Q.

Pre kvázigrupy platia nasledovné dôležité vety, ktoré dopĺňajú a rozširujú tvrdenia pre Latinské štvorce. Tvrdenia sú prevzané z [**13**] a popisujú vlastnosti izotopizmov kvázigrúp ako špeciálneho prípadu grupoidov.

DEFINÍCIA 3.33. *Množina S tvorí grupoid s ohľadom k binárnej operácii $*$, ak ku každému usporiadanému páru a, b prvkov z S je jednoznačne pridružený prvok $a * b$.*

VETA 3.34. [**13**] *Množina všetkých izotopizmov grupoidu rádu n tvorí grupu I'_n rádu $(n!)^3$.*

DÔSLEDOK 3.35. [**13**] *Platí $I'_n \cong S_n \times S_n \times S_n$.*

DÔSLEDOK 3.36. [**13**] *Množina všetkých izotopizmov kvázigrupy rádu n tvorí grupu rádu $(n!)^3$.*

DEFINÍCIA 3.37. [**13**] *Ak trojica (θ, φ, ψ) predstavuje izotopizmus kvázigrupy $(G, *)$ na ňu samotnú, potom izotopizmus (θ, φ, ψ) voláme autotopizmus kvázigrupy G. Ak autotopizmus je zároveň izomorfizmom ($\theta = \varphi = \psi$) potom ho tiež voláme automorfizmus kvázigrupy $(G, *)$.*

POZNÁMKA 3.38. V ďalšom budeme označovať grupu autotopizmov kvázigrupy Q symbolom $AUT(Q)$. Pri používaní $AUT(Q)$ si však treba dať pozor na možnú zámenu s označením automorfizmov kvázigrupy $Aut(Q)$.

VETA 3.39. [**13**] *Množina všetkých autotopizmov kvázigrupy Q rádu n tvorí podgrupu grupy I'_n.*

DÔSLEDOK 3.40. [**13**] *Rád grupy $AUT(G)$ autotopizmov kvázigrupy Q delí $(n!)^3$.*

VETA 3.41. [**13**] *Ak sú dve kvázigrupy G_1 a G_2 izotópne potom platí $AUT(G_1) \cong AUT(G_2)$.*

VETA 3.42. [**13**] *Dve zložky autotopizmu kvázigrupy jednoznačne určujú tretiu zložku.*

DÔSLEDOK 3.43. [**13**] *Rád grupy autotopizmov kvázigrupy je nanajvýš $(n!)^2$.*

DÔSLEDOK 3.44. [**13**] *Každá zložka hlavného autotopizmu určuje tento jednoznačne.*

DEFINÍCIA 3.45. [**13**] *Hlavný autotopizmus kvázigrupy je autotopizmus tvaru* (θ, φ, id)*, kde* id *predstavuje identickú permutáciu.*

DÔSLEDOK 3.46. [**13**] *Rád grupy hlavných autotopizmov kvázigrupy je nanajvýš* $n!$.

Uvedené tvrdenia sa účelovo dotýkajú len grupy autotopizmov kvázigrúp. Je to z toho dôvodu, že autotopizmy danej kvázigrupy tvoria grupu, zatiaľčo pri kvázigrupách s rôznymi množinami prvkov to pravda nie je.

Treba však poznamenať, že tvrdenia dotýkajúce sa počtov izotopizmov medzi ľubovoľnými kvázigrupami rovnakého rádu platia všeobecne. To plynie z lemy 3.23 pre kvázigrupy.

Rovnako platí pre ľubovoľné dve kvázigrupy aj veta 3.42.

VETA 3.47. *Dve zložky izotopizmu dvoch kvázigrúp určujú tretiu zložku izotopizmu jednoznačne.*

KAPITOLA 4

Algoritmus na hľadanie izotopií

V tejto kapitole sa venujeme návrhu nového algoritmu na hľadanie izotopií dvoch kvázigrúp. Ako vedľajší produkt návrhu možno klasifikovať algoritmus, ktorý nájde prvky, ktoré konjugujú n prvkové množiny permutácií. Na základe návrhu algoritmu sú neskôr odvodené odhady maximálneho počtu izotopizmov kvázigrúp, ktoré upresňujú doposiaľ známu hornú hranicu $nn!$ [**13**]. V kapitole je tiež prezentovaný univerzálny vzorec pre výpočet množstva autotopií konečných grúp, ktorý je ekvivalentom vzorca z [**3**].

POZNÁMKA 4.1. Budeme predpokladať, že kvázigrupy, ktorých izotopizmy hľadáme majú rovnakú množinu prvkov Q.

Hľadáme teda izotopie medzi kvázigrupami $Q_1 = (Q, *_1)$, $Q_2 = (Q, *_2)$, ktoré sú tvorené rovnakými prvkami. Pri algoritmoch budeme naviac predpokladať, že kvázigrupy majú množinu prvkov $Q = I_n$.

Chceme prezentovať algoritmus, ktorý nájde všetky izotopizmy medzi dvoma kvázigrupami.Dokáže teda tiež rozhodnúť, či sú dané dve kvázigrupy izotópne.

4.1. Reprezentácia kvázigrupy

Algoritmus používa na reprezentáciu kvázigrupy $(Q, *)$ rádu n množinu L_Q permutácií zo symetrickej grupy $Sym(Q)$. Množina L_Q pozostáva z n rôznych ľavých translácií $L_{q_i}, q_i \in Q$ kvázigrupy $(Q, *)$.

DEFINÍCIA 4.2. [**13**] *Ľavá translácia prvkom $x \in Q$ kvázigrupy $(Q, *)$ je zobrazenie $L_x : Q \to Q$ definované vzťahom $L_x(y) = x * y$. Pravá translácia R_x rovnakým prvkom má vyjadrenie $R_x(y) = y * x$.*

POZNÁMKA 4.3. Poznamenajme, že prvky L_Q predstavujú permutácie na množine Q a teda $L_Q \subseteq Sym(Q)$. Ďalej treba poznamenať, že zápis kvázigrupy pomocou jej translácií je jednoznačný. Čiže množina L_Q definuje operáciu na kvázigrupe jednoznačne.

POZNÁMKA 4.4. V literatúre je izomorfizmus λ grupy $(G, *)$ do množiny jej ľavých translácií L_G známy ako ľavá regulárna reprezentácia [**50**]. Množina L_G je preto "ekvivalentom" grupy G v symetrickej grupe $Sym(G)$. Pri kvázigrupách však toto všeobecne neplatí, a teda nemožno hovoriť o množine L_Q ako o izomorfnom obraze kvázigrupy Q.

V nasledujúcom príklade možno vidieť kvázigrupu Q a jej množinu translácií L_Q.

PRÍKLAD 4.5. V tabuľke 1 možno vidieť Cayleyho tabuľku kvázigrupy $(Q, *)$ a k nej prislúchajúcu množinu L_Q.

*	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

L_Q
$L_{\mathbf{1}} = \binom{1234}{1234}$
$L_{\mathbf{2}} = \binom{1234}{2341}$
$L_{\mathbf{3}} = \binom{1234}{3412}$
$L_{\mathbf{4}} = \binom{1234}{4123}$

TABUĽKA 1. Cayleyho tabuľka kvázigrupy Q a množina L_Q

Dôvod prečo algoritmus používa množinu translácií L_Q kvázigrupy je ten, že pomocou nej sa dá izotopia kvázigrúp jednoducho popísať pomocou skladania permutácií a rovností množín. Takto je možné narábať s kvázigrupou ako s podmnožinou grupy $Sym(Q)$. Môžeme teda využívať asociatívnosť "prostredia".

V zhode s poznámkou 3.5 sa budeme pridržiavať nasledujúceho zápisu skladania permutácií:

DEFINÍCIA 4.6. *Pre permutácie α, β množiny X definujeme ich zloženie $\alpha \circ \beta$ vzťahom*

$$(\alpha \circ \beta)(x) = \alpha(\beta(x))$$

pre každé $x \in X$.

Pre zjednodušenie budeme namiesto $\alpha \circ \beta$ písať len $\alpha\beta$.

4.2. Izotopia a množina L_Q

Spôsob akým sa dá izotopia kvázigrúp vyjadriť pomocou ľavých translácií naznačuje séria troch nasledujúcich liem. Tie popisujú v akom vzťahu sú množiny ľavých translácií L_{Q_1}, L_{Q_2} izotópnych kvázigrúp Q_1, Q_2.

LEMA 4.7. *Nech pre kvázigrupy* $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ *a pre ľubovoľné* $x, y \in Q$ *platí:*

$$x *_2 y = \psi(x *_1 y)$$

pre nejaké $\psi \in Sym(Q)$. *Potom pre množiny ľavých translácií* L_{Q_1}, L_{Q_2} *platí vzťah:*

$$L_{Q_2} = \psi L_{Q_1}.$$

DÔKAZ. Vezmime si ľubovoľný prvok x množiny Q. Pýtame sa, ako vyzerá ľavá translácia L_x^2 prvkom x v kvázigrupe Q_2. Z definície ľavej translácie máme $L_x^2(y) = x *_2 y$, čo možno pomocou predpokladov lemy prepísať ako $x *_2 y = \psi(L_x^1(y))$. Tu predstavuje L_x^1 ľavú transláciu prvkom x v kvázigrupe Q_1. Pre všetky $y \in Q$ platí $L_x^2(y) = \psi(L_x^1(y))$. Keďže L_x^1, L_x^2, ψ sú permutácie z $Sym(Q)$, platí pre ľubovoľné $x \in Q$ rovnosť

$$L_x^2 = \psi L_x^1.$$

Z toho už priamo dostávame $L_{Q_2} = \psi L_{Q_1}$.

□

V leme 4.7 rovnako ako v celom ďalšom texte rozumieme pod súčinom CD podmnožín C, D multiplikatívnej grupy $(G, .)$ (a teda aj prvku a množiny) množinu

$$C.D = \{cd | c \in C, d \in D\}.$$

LEMA 4.8. *Nech pre kvázigrupy* $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ *a pre ľubovoľné* $x, y \in Q$ *platí*

$$x *_2 \varphi(y) = x *_1 y \tag{1}$$

pre nejaké $\varphi \in Sym(Q)$. Potom pre množiny ľavých translácií L_{Q_1}, L_{Q_2} platí vzťah

$$L_{Q_2} = L_{Q_1}\varphi^{-1}.$$

DÔKAZ. Túto lemu dokážeme obdobným spôsobom ako lemu 4.7. Majme ľubovoľný fixný prvok x množiny Q. Pýtame sa ako vyzerá ľavá translácia L_x^2 kvázigrupy Q_2 vo vzťahu k L_x^1. Prepísaním rovnice (1) do translácií dostávame rovnosť $L_x^2(\varphi(y)) = L_x^1(y)$ platnú pre ľubovoľné $y \in Q$. Teda $L_x^2\varphi = L_x^1$. To je ekvivalentné s

$$L_x^2 = L_x^1\varphi^{-1}.$$

Vzhľadom na to, že uvedené platí pre ľubovoľné $x \in Q$, možno pre L_{Q_2}, L_{Q_1} písať $L_{Q_2} = L_{Q_1}\varphi^{-1}$. □

LEMA 4.9. *Pre kvázigrupy $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ platí*

$$L_{Q_2} = L_{Q_1}$$

práve vtedy, keď existuje $\theta \in Sym(Q)$ také, že

$$\theta(x) *_2 y = x *_1 y \tag{2}$$

pre všetky $x, y \in Q$.

DÔKAZ. Najskôr dokážeme nutnú podmienku. Nech platí $L_{Q_2} = L_{Q_1}$. Pre ľubovoľné $x_2 \in Q$ teda existuje $x_1 \in Q$ také, že $L_{x_2}^2 = L_{x_1}^1$. Vezmime zobrazenie $\theta : Q \mapsto Q$, také, že pre ľubovoľné $x \in Q$ platí $L_{\theta(x)}^2 = L_x^1$. Teda ľavá translácia prvkom x v kvázigrupe Q_1 a ľavá translácia prvkom $\theta(x)$ v kvázigrupe Q_2 určujú zhodnú permutáciu. Keďže sú všetky prvky množiny L_{Q_1} rôzne ako permutácie (rovnako aj L_{Q_2}), tvorí zobrazenie θ permutáciu množiny Q. Preto $\theta \in Sym(Q)$. Použitím definície ľavej translácie možno prepísať $L_{\theta(x)}^2 = L_x^1$ do tvaru $\theta(x) *_2 y = x *_1 y$. To platí pre všetky y a teda dokazuje nutnú podmienku.

Postačujúca podmienka: Nech platí rovnica (2) pre ľubovoľné $x, y \in Q$ a $\theta \in Sym(Q)$. Rovnica sa dá prepísať pomocou ľavých translácií ako $L_{\theta(x)}^2 = L_x^1$. Keďže θ je permutáciou na Q, tak skutočne platí $L_{Q_1} = L_{Q_2}$. □

Na základe predchádzajúcich liem 4.7,4.8,4.9 vieme odvodiť vzťah medzi transláciami izotópnych kvázigrúp.

VETA 4.10. *Nech trojica (θ, φ, ψ) tvorí izotopizmus kvázigrupy $Q_1 = (Q, *_1)$ na $Q_2 = (Q, *_2)$. Potom pre množiny ľavých translácií L_{Q_1}, L_{Q_2} platí*

$$L_{Q_2} = \psi L_{Q_1} \varphi^{-1}. \tag{3}$$

DÔKAZ. Z liem 4.7,4.8,4.9 priamo vyplýva, že pre izotópne kvázigrupy Q_1, Q_2 a ich izotopizmus (θ, φ, ψ) platí vzťah $L_{Q_2} = \psi L_{Q_1} \varphi^{-1}$. □

Z vety 4.10 je zrejmé, že existencia permutácií φ, ψ spĺňajúcich rovnosť (3) je nutnou podmienku izotopie kvázigrúp Q_1, Q_2. Ako si teraz ukážeme je táto podmienka zároveň postačujúca.

VETA 4.11. *Nech $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ sú kvázigrupy. Potom pre každú dvojicu permutácií $\varphi, \psi \in Sym(Q)$, ktorá spĺňa rovnicu (3), existuje izotopizmus (θ, φ, ψ) kvázigrupy Q_1 na Q_2 pre nejaké $\theta \in Sym(Q)$.*

DÔKAZ. Vezmime si kvázigrupu $Q_3 = (Q, *_3)$ izotópnu s Q_1 prostredníctvom izotopizmu (id, φ, ψ). Platí

$$x *_3 \varphi(y) = \psi(x *_1 y).$$

Z vety 4.10 máme pre translácie vzťah $L_{Q_3} = \psi L_{Q_1} \varphi^{-1}$. Využitím rovnice (3) možno písať $L_{Q_3} = L_{Q_2}$. Z lemy 4.9 vyplýva, že Q_3, Q_2 sú izotópne a existuje izotopizmus Q_3 na Q_2 tvaru (θ, id, id).

Keďže (id, φ, ψ) určuje izotopizmus Q_1 na Q_3 a (θ, id, id) určuje izotopizmus Q_3 na Q_2, tak (θ, φ, ψ) určuje izotopizmus Q_1 na Q_2 pre nejaké $\theta \in Sym(Q)$. Tým je veta dokázaná. □

Veta 4.11 nehovorí len o tom, v akom vzťahu sú translácie izotópnych kvázigrúp, dáva tiež návod ako možno nájsť príslušný izotopizmus. Pre kvázigrupy Q_1, Q_2 stačí vziať všetky možné kombinácie permutácií $\varphi, \psi \in Sym(Q)$ a testovať, či príslušné množiny $\varphi^{-1} L_{Q_1} \psi, L_{Q_2}$ sú zhodné. Ak také φ, ψ nájdeme, tak vieme okamžite určiť ich izotopizmus.

POZNÁMKA 4.12. Permutáciu $\theta \in Sym(Q)$, ktorá určuje tretiu zložku izotopizmu, možno nájsť jednoduchým porovnaním $\psi L_{Q_1}\varphi^{-1}$ a L_{Q_2}. Teda $\theta(q_i) = q_j$, ak pre transláciu $L^2_{q_j} \in Sym(Q)$ prvkom q_j v kvázigrupe Q_2 platí $\psi L^1_{q_i}\varphi^{-1} = L^2_{q_j}$. Permutácia $L^1_{q_i}$ tu predstavuje transláciu prvkom q_i v kvázigrupe Q_1.

V opačnom prípade samozrejme kvázigrupy Q_1, Q_2 izotópne nie sú. Takýto spôsob hľadania izotopií má však vysokú zložitosť, keďže možných párov φ, ψ je $(n!)^2$. To znamená, že nie je príliš vhodný pre praktické použitie a je teda nutná jeho úprava. Hlavnou myšlienkou, ktorá vedie k rýchlejšiemu algoritmu je upraviť pôvodný tak, aby namiesto dvoch voľných premenných φ, ψ vystupovala vo vyjadrení L_{Q_2} len jedna. Potrebujeme teda nejakým spôsobom eliminovať vo vyjadrení L_{Q_2} buď φ alebo ψ. Problém však je, že nepoznáme ani jedno z nich. Vieme však, že množina translácií L_{Q_2} má pre izotópne kvázigrupy Q_1, Q_2 tvar $L_{Q_2} = \psi L_{Q_1}\varphi^{-1}$.

POZNÁMKA 4.13. V ďalšom texte prepokladáme, že trojica (θ, φ, ψ) tvorí izotopizmus kvázigrupy Q_1 na Q_2.

Na elimináciu ψ z L_{Q_2} stačí vziať nejakú permutáciu $p_2 \in L_{Q_2}$ a sprava ňou prenásobiť všetky prvky L_{Q_2}. Dostávame tak ďalšiu množinu permutácií

$$L'_{Q_2} = L_{Q_2}p_2^{-1}. \tag{4}$$

Keďže $p_2 \in L_{Q_2}$ a $L_{Q_2} = \psi L_{Q_1}\varphi^{-1}$ tak existuje $p_1 \in L_{Q_1}$ taká, že platí:

$$p_2 = \psi p_1 \varphi^{-1}. \tag{5}$$

Spojením rovníc (4) a (5) možno vyjadriť L'_{Q_2} pomocou L_{Q_1} ako:

$$L'_{Q_2} = L_{Q_2}p_2^{-1} = \psi L_{Q_1}\varphi^{-1}(\psi p_1 \varphi^{-1})^{-1}. \tag{6}$$

To je ekvivalentné rovnici

$$L'_{Q_2} = \psi L_{Q_1}\varphi^{-1}(\varphi p_1^{-1}\psi^{-1}) = \psi L_{Q_1}p_1^{-1}\psi^{-1}, \tag{7}$$

v ktorej už permutácia φ nevystupuje.

O tom ako sa dá táto konštrukcia použiť na testovanie izotópnosti Latinských štvorcov hovorí nasledujúca veta.

VETA 4.14. *Majme kvázigrupy* $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ *a ľubovoľné* $p_2 \in L_{Q_2}$. *Kvázigrupy* Q_1, Q_2 *sú izotópne práve vtedy, keď existujú permutácie* $p_1 \in L_{Q_1}, p \in Sym(Q)$ *také, že platí*

$$L_{Q_2} p_2^{-1} = p L_{Q_1} p_1^{-1} p^{-1}. \tag{8}$$

DÔKAZ. Vezmime izotópne kvázigrupy Q_1, Q_2. Z vety 4.10 vyplýva $L_{Q_2} = \psi L_{Q_1} \varphi^{-1}$ pre nejaké $\varphi^{-1}, \psi \in Sym(Q)$. Platí teda $L_{Q_2} p_2^{-1} = p L_{Q_1} p_1^{-1} p^{-1}$ pre ľubovoľné $p_2 \in L_{Q_2}$ a $p_1 = \psi^{-1} p_2 \varphi, p = \psi$.

Opačná implikácia zrejme platí, keďže rovnosť

$$L_{Q_2} p_2^{-1} = p L_{Q_1} p_1^{-1} p^{-1}$$

je ekvivalentná rovnosti

$$L_{Q_2} = p^{-1} L_{Q_1} p_1^{-1} p^{-1} p_2.$$

Sú teda splnené predpoklady vety 4.11, čo zaručuje izotópnosť kvázigrúp Q_1, Q_2. □

DÔSLEDOK 4.15. *Ak sú kvázigrupy* $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ *izotópne, tak existuje bijekcia* $\tau : L_{Q_1} \to L_{Q_2}$ *taká, že pre nejaké* $p \in Sym(Q)$ *platí*

$$L_{Q_2}(\tau(p_1))^{-1} = p L_{Q_1} p_1^{-1} p^{-1}. \tag{9}$$

DÔKAZ. Vezmime zobrazenie τ dané predpisom $\tau(p_1) = \psi p_1 \varphi^{-1}$, kde (θ, φ, ψ) určuje nejaký izotopizmus kvázigrupy Q_1 na Q_2. Z vety 4.14 vyplýva bijektívnosť zobrazenia τ. Využitím rovnice $L_{Q_2} = \psi L_{Q_1} \varphi^{-1}$ a faktu $p_2 = \psi p_1 \varphi^{-1}$ dostávame

$$L_{Q_2}(\tau(p_1))^{-1} = L_{Q_2} p_2^{-1} = \psi L_{Q_1} \varphi^{-1} (\psi p_1 \varphi^{-1})^{-1} = \psi L_{Q_1} p_1^{-1} \psi^{-1}.$$

Za p potom stačí vziať permutáciu ψ. □

DÔSLEDOK 4.16. *Ak sú kvázigrupy* $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ *izotópne, tak existuje izotopizmus* $(\theta, p_2^{-1} p p_1, p)$, *kde* θ *je nejaká permutácia z* $Sym(Q)$ *a permutácie* p, p_1, p_2 *sú práve tie, ktoré vystupujú v rovnici (8)* .

DÔKAZ. Priamo vyplýva z viet 4.11 a 4.14. □

DÔSLEDOK 4.17. *Majme izotópne kvázigrupy* $Q_1 = (Q, *_1)$, $Q_2 = (Q, *_2)$. *Vezmime l'ubovoľné* $p_2 \in L_{Q_2}$. *Potom počet izotopizmov medzi kvázigrupami* Q_1, Q_2 *je zhodný s počtom rôznych dvojíc* $(p, p_1) \in Sym(Q) \times L_{Q_1}$ *spĺňajúcich rovnosť (8).*

DÔKAZ. Vezmime dôsledok 4.16 vety 4.14. Z neho vieme, že každý izotopizmus má pre l'ubovoľné fixné $p_2 \in L_{Q_2}$ a vhodné $p_1 \in L_{Q_1}, p \in Sym(Q)$ tvar $(\theta, p_2^{-1}pp_1, p)$. Z vety 3.47 máme, že izotopizmus dvoch kvázigrúp je určený jednoznačne dvoma zložkami. Stačí nám teda ukázať, že každá z dvojíc tvaru $(p_2^{-1}pp_1, p)$ je jedinečná.

Pokračujeme sporom. Predpokladajme, že máme permutácie $p, p' \in Sym(Q)$ a $p_1, p_1' \in L_{Q_1}$, pre ktoré platí

$$(p, p_1) \neq (p', p_1').$$

Nech sú obe zložky indukovaného izotopizmu zhodné t.j. $p = p'$, $p_2^{-1}pp_1 = p_2^{-1}p'p_1'$. Z toho ale plynie rovnosť $p_1 = p_1'$ a teda máme spor s tým, že dvojice $(p, p_1), (p', p_1')$ sú rôzne. Preto každý vhodný pár p, p_1 určuje pre fixné $p_2 \in L_{Q_2}$ jedinečný izotopizmus. □

Veta 4.14 umožňuje nájsť izotopie dvoch kvázigrúp Q_1, Q_2 oveľa efektívnejšie. Stačí hľadať pre pevne zvolenú permutáciu $p_2 \in L_{Q_2}$ permutácie $p_1 \in L_{Q_1}, p \in Sym(Q)$ tak, aby bolo splnené $L_{Q_2}p_2^{-1} = pL_{Q_1}p_1^{-1}p^{-1}$.

Pseudokód základného algoritmu na hľadanie izotopií medzi kvázigrupami Q_1, Q_2 možno vidieť v algoritme 1:

ALGORITMUS 1.

VSTUP: *Kvázigrupy* Q_1, Q_2 *rádu* n

VÝSTUP: *Množina izotopizmov* $Is(Q_1, Q_2)$

---

(1) *Zvoľ si l'ubovoľnú permutáciu* $p_2 \in L_{Q_2}$.

(2) *Vezmi v cykle každú permutáciu* $p_1 \in L_{Q_1}$ *urob pre ňu nasledovné*

  (2.1) *generuj postupne v cykle všetky permutácie* p *z* $Sym(Q)$.

  (2.2) *Ak pre nejaké* p *platí* $L_{Q_2}p_2^{-1} = pL_{Q_1}p_1^{-1}p^{-1}$, *nastav* $\psi = p$, $\varphi = p_2^{-1}pp_1$.

  (2.3) *Nájdi* θ *porovnaním* L_{Q_2} *a* $\psi L_{Q_1}\varphi^{-1}$. *(poznámka 4.12)*

(2.4) *Ulož do* $Is(Q_1, Q_2)$ *trojicu* (θ, φ, ψ).
(3) *Vráť* $Is(Q_1, Q_2)$.

4.3. Optimalizácia algoritmu

Ako môžeme vidieť vyššie nájdenie izotopizmu dvoch kvázigrúp Q_1, Q_2 s množinou prvkov I_n je ekvivalentné nájdeniu permutácie $p \in S_n$, pre ktorú platí $pAp^{-1} = B$. Množiny permutácií $A, B \subseteq S_n$ boli získané "normovaním" translácií L_{Q_1}, L_{Q_1} kvázigrúp Q_1, Q_2. Vyvstáva teda otázka, ako sa dá efektívnym spôsobom nájsť príslušné p, prípadne všetky také p. Ďalší postup ako efektívne hľadať p vychádza z faktu, že množiny permutácií A, B sú konjugované. To umožní, ako si neskôr ukážeme, významne zredukovať počty možných kandidátov na permutáciu p.

Pri definovaní konjugovaných množín sa vychádza z nasledujúcej definície.

DEFINÍCIA 4.18. *Nech G je grupa a nech $a, b \in G$ sú nejaké jej dva prvky. Hovoríme, že a, b sú konjugované, ak existuje $c \in G$ také, že platí $cac^{-1} = b$.*

Konjugovanosť množín sa potom definuje obdobne.

DEFINÍCIA 4.19. *Nech G je grupa a nech $A, B \subseteq G$ sú nejaké jej dve podmnožiny. Hovoríme, že množiny A, B sú konjugované, ak existuje $c \in G$ také, že platí $cAc^{-1} = B$.*

Vlastnosti konjugovaných prvkov a množín možno najlepšie popísať pomocou akcie konjugácia.

DEFINÍCIA 4.20. *Nech G je multiplikatívna grupa. Akciu konjugáciou definujeme ako zobrazenie $\alpha : G \times G \to G$ s predpisom $\alpha(g, m) = gmg^{-1}$. Hovoríme, že výsledok vznikol ako konjugácia prvku m prvkom g.*

Podobne ako pri prvkoch môžeme definovať akciu konjugáciou na množinách.

DEFINÍCIA 4.21. *Nech G je multiplikatívna grupa. Nech 2^G predstavuje systém podmnožín množiny G. Akciu konjugáciou $\alpha : G \times 2^G \to 2^G$ na tomto systéme definujeme predpisom $\alpha(g, M) = gMg^{-1}$, kde $M \in 2^G$.*

My pracujeme s permutáciami z S_n a teda pre grupu G a množinu M platí $G = S_n, M \in 2^{S_n}$.

Z definície 4.21 plynie, že dve množiny permutácií sú konjugované, ak sa nachádzajú v rovnakej orbite tejto akcie. Preto relácia "byť konjugovaný" predstavuje reláciu ekvivalencie na systéme 2^{S_n}. Nás špeciálne zaujímajú orbity n prvkových množín permutácií, ktoré tvoria translácie kvázigrúp rádu n. Ukážme si teraz, čo musia spĺňať konjugované množiny permutácií.

4.3.1. Konjugované permutácie a cykly. Začneme s popisom vlastností konjugovaných permutácií.

DEFINÍCIA 4.22. [**9**] *Permutácia p je cyklická (tvorí cyklus), ak sa dá zapísať ako*

$$p = \begin{pmatrix} s_1 & s_2 & \dots & s_{n-1} & s_n \\ s_2 & s_3 & \dots & s_n & s_1 \end{pmatrix}.$$

Cyklickú permutáciu p budeme d'alej zapisovať podľa obyčaje ako $p = (s_1 s_2 \dots s_{n-1} s_n)$.

Vychádzme z nasledujúcich viet:

VETA 4.23. [**8**] *Každá permutácia σ konečnej množiny X je súčinom $\lambda_1 \lambda_2 \dots \lambda_k$ disjunktných cyklických permutácií λ_i, z ktorých každá má dĺžku aspoň dva. Ak odhliadneme od poradia cyklov, má permutácia σ len jeden takýto rozklad.*

VETA 4.24. [**8**] *Ak $\lambda \in S_n$ je cyklus dĺžky m, potom aj cyklus $\tau\lambda\tau^{-1}$ konjugovaný s λ má dĺžku m.*

Cyklus alebo cyklická permutácia sa definuje nasledovne:

Z viet 4.23 a 4.24 je zrejmé, že cykly konjugovaných permutácií si svojou dĺžkou zodpovedajú. To tvorí nutnú podmienku konjugovanosti dvoch permutácií, ktorá je zároveň postačujúca (lema 4.26). Najskôr si však zadefinujme pojem "typ permutácie", ktorý hovorí o jej rozklade na cykly.

DEFINÍCIA 4.25. [**6**] *Nech p je n-permutácia (permutácia n prvkovej množiny), ktorá má práve a_i cyklov dĺžky i pre každé $i \in I_n$. Potom hovoríme, že p je typu $(a_1, a_2, \dots, a_n)$.*

Uvedieme aj dôkaz lemy 4.26, keďže dáva návod na konštrukciu permutácie, ktorá konjuguje dve dané permutácie.

LEMA 4.26. [**6**] *Prvky $g, h \in S_n$ sú v S_n konjugované práve vtedy, keď sú rovnakého typu.*

DÔKAZ. Dokážme najskôr nutnú podmienku. Predpokladajme, že permutácie g, h sú konjugované, t.j. $pgp^{-1} = h$ pre $p \in S_n$. Nech $(b_1 \dots b_k)$ je cyklus permutácie g. Potom platí $g^i(b_1) = b_{i+1}$ pre všetky $i \in I_k$ a $g^k(b_1) = b_1$. Z rovnosti $h = pgp^{-1}$ máme $h^i = pg^ip^{-1}$. Teda $h^i(x) = pg^ip^{-1}(x)$. Pre x také, že $p(x) = b_1$, máme $pg^ip^{-1}(x) = p^{-1}(g^i(b_1)) = p^{-1}(b_{i+1})$ pre $i \in I_{k-1}$ a $pg^kp^{-1}(x) = p^{-1}(b_1)$. Prenásobením zľava permutáciou p a sprava p^{-1} sa zobrazí cyklus $(b_1 \dots b_k)$ na cyklus $(p^{-1}(b_1)p^{-1}(b_2) \dots p^{-1}(b_k))$.

Preto permutácia p určuje bijekciu k-cyklov permutácií g, h pre všetky k. Platí teda nutná podmienka.

Postačujúca podmienka sa dokáže nasledovne. Predpokladajme, že permutácie g, h sú rovnakého typu. Skonštruujme permutáciu p aby platilo $pgp^{-1} = h$. Ak $(b_1b_2 \dots b_k)$ je cyklus g a $(c_1c_2 \dots c_k)$ je cyklus permutácie h, potom z predchádzajúceho máme, že musíme zvoliť p tak, aby $p^{-1}(b_i) = c_i$ pre $i \in I_k$. Poznáme teda obrazy k prvkov b_i pre $i \in I_k$ permutácie p^{-1}. Na nájdenie celej p^{-1}, a teda aj p, potom stačí aplikovať rovnaký postup na zvyšné cykly. □

Pomocou lemy možno ľahko nájsť všetky p s požadovanou vlastnosťou. Stačí aplikovať postup z dôkazu lemy s tým rozdielom, že namiesto cyklu $(c_1c_2 \dots c_k)$ vezmeme každý k-cyklus permutácie h a rekurzívne tento postup zopakujeme.

Máme teda algoritmus, ktorý pre dané konjugované permutácie $g, h \in S_n$ (permutácie rovnakého typu) nájde všetky $p \in S_n$, pre ktoré platí $pgp^{-1} = h$.

Ďalej budeme symbolom $C_n(g, h)$ označovať množinu takýchto p. Podobne budeme označovať množinu všetkých p, ktoré konjugujú množiny $G, H \subseteq S_n$ a síce:

$$C_n(G, H) = \{p | p \in S_n, pGp^{-1} = H\}.$$

Algoritmus, ktorý nájde množinu $C_n(g,h)$ má nasledovný tvar:

ALGORITMUS 2.
VSTUP: *Permutácie* $g, h \in S_n$
VÝSTUP: *Množina* $C_n(g,h)$

---

(1) *Nastav* $C_n(g,h)$ *na prázdnu množinu.*
(2) *Rozlož permutácie z* g, h *na disjunktné cykly* $g = \lambda_1 \dots \lambda_l$ *a* $h = \delta_1 \dots \delta_l$
(3) *Zafixuj l'ubovol'né* $\{s_1, \dots, s_l\}$ *také, že* s_i *sa nachádza v cykle* λ_i *pre všetky* $i \in I_l$.
(4) *Nájdi všetky permutácie* $P_j \in S_l$ *také, že cykly* $\lambda_i, \delta_{P_j(i)}$ *majú rovnaké dĺžky. Ak také* P_j *neexistuje, ukonči algoritmus a vrát'* $C_n(g,h) = \emptyset$.
(5) *Pre každé z nájdených permutácií* P_j *rob nasledovné:*
  (5.1) *Zvol' l'ubovol'né* $\{s'_1, \dots, s'_l\}$ *také, že* s'_i *sa nachádza v cykle* $\delta_{P_j(i)}$ *pre všetky* $i \in I_l$.
  (5.2) *Nastav* $p^{-1}(s_i) = s'_i$ *pre všetky* $i \in I_l$.
  (5.3) *Dopočítaj obrazy zvyšných prvkov permutácie* p^{-1} *podl'a vzt'ahu* $p^{-1}(g^k(s_i)) = h^k(s'_i)$.
  (5.4) *Ulož* p *do* $C_n(G,H)$.

V príklade 4.27 môžeme vidieť aplikáciu algoritmu 2.

PRÍKLAD 4.27. Majme permutácie $g = \binom{1234567}{2143675}$ $h = \binom{1234567}{6472153}$, ktoré majú nasledovný cyklový zápis :

$$g = (12)(567)(34)$$
$$h = (24)(37)(165)$$

Máme teda cykly $\lambda_1 = (567), \lambda_2 = (12), \lambda_3 = (34)$ a $\delta_1 = (165), \delta_2 = (24), \delta_3 = (37)$. Existujú dve párovania $P_1, P_2 \in S_3$, ktoré spájajú cykly $\lambda_i, \delta_{P(i)}$ rovnakej dĺžky. Majú tvar $P_1 = \binom{123}{123}, P_2 = \binom{123}{132}$.

Vezmime si P_1. Vezmime symboly $(s_1, s_2, s_3) = (1, 5, 3)$. Pre výber $(s'_1, s'_2, s'_3) = (2, 1, 3)$ dostávame permutáciu

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 7 & 1 & 6 & 5 \end{pmatrix}.$$

Zvyšné permutácie z $C_n(g,h)$ sa získajú ďalšími voľbami symbolov s'_1, s'_2, s'_3.

Z algoritmu 2 je zrejmé, že mohutnosť ním získanej množiny permutácií je určená počtom možných párovaní $P \in S_l$ a počtom rôznych výberov symbolov s'_i z cyklov h. Rôznych výberov je zjavne $\prod_{i=1}^{n} i^{a_i}$ pre každú P_j, a g, h typu $(a_1, \ldots, a_n)$. Spolu s párovaniami P_j, ktorých je zrejme $\prod_{j=1}^{n} a_i!$, tak získame $\prod_{i=1}^{n} a_i! i^{a_i}$ permutácií. Tieto sú všetky rôzne, keďže zhodnosť dvoch permutácií by znamenala rovnaké P_j a rovnaký výber symbolov s'_i. Preto algoritmus má ako svoj výstup skutočne množinu $C_n(g,h)$. Korektnosť uvedenej konštrukcie podporuje dôsledok 4.29 vety 4.28.

VETA 4.28. [**6**] *Počet permutácií z S_n typu $(a_1, \ldots, a_n)$ je*

$$\frac{n!}{\prod_{i=1}^{n} a_i! i^{a_i}}.$$

DÔSLEDOK 4.29. *Nech g, h sú permutácie typu $(a_1, \ldots, a_n)$. Potom pre mohutnosť množiny $C_n(g,h)$ platí*

$$|C_n(g,h)| = |St_{S_n}(g)| = \prod_{i=1}^{n} a_i! i^{a_i}.$$

DÔKAZ. Vezmime akciu konjugáciou v grupe S_n. Vezmime si z vety 3.20 bod 2. Teda $g_1.\alpha = g_2.\alpha$ práve vtedy, keď $g_1 St_G(\alpha) = g_2 St_G(\alpha)$. To ale znamená $g_2^{-1} g_1 \in St_G(\alpha)$. Počet rôznych g_i takých, že $g_i.\alpha = g_1.\alpha$ je preto rovný mohutnosti stabilizátora $St_G(\alpha)$. Prepísaním uvedeného máme $|C_n(g,h)| = |St_{S_n}(g)|$.

Z vety 3.20 tiež vyplýva $|S_n| = |St_{S_n}(g)||g.S_n|$. Z vety 4.28 vyplýva $|g.S_n| = \frac{n!}{\prod_{i=1}^{n} a_i! i^{a_i}}$ a teda platí aj rovnosť $|C_n(g,h)| = \prod_{i=1}^{n} a_i! i^{a_i}$. □

4.3.2. Algoritmy na hľadanie $C_n(G,H)$. V tejto sekcii si ukážeme ako hľadať množinu permutácií $C_n(G,H) \subseteq S_n$. Začnime s nutnou podmienkou. Podobne ako pri permutáciach zadefinujme typ množiny permutácií.

DEFINÍCIA 4.30. *Hovoríme, že množina permutácií $G \subset S_n$ je typu $(n_1, \ldots, n_l) \times (A_1, A_2, \ldots, A_l)$, ak G obsahuje práve n_i permutácií typu $A_i = (a_{i,1}, \ldots, a_{i,n})$. Pre typy permutácií A_i predpokladáme ich lexikografické usporiadanie tj. pre A_i, A_{i+1} platí $a_{i,j} = a_{i+1,j}$ pre všetky $j < k$ a $a_{i,k} \geq a_{i+1,k}$.*

Môžeme vysloviť podobnú vetu ako pri permutáciach.

LEMA 4.31. *Ak sú množiny $G, H \subseteq S_n$ v S_n konjugované, potom sú rovnakého typu.*

DÔKAZ. Priamo vyplýva z definície 4.30 a lemy 4.26. □

Opačná implikácia, ako tomu bolo v leme 4.26, však neplatí ako možno vidieť na nasledujúcom príklade.

PRÍKLAD 4.32. Majme nasledujúce množiny $G, H \subseteq S_4$ permutácií zapísané cyklovou notáciou $G = \{(1234), (13)\}$, $H = \{(1234), (12)\}$. Predpokladajme, že permutácia $p \in S_4$ ich konjuguje. To by ale znamenalo, že $p^{-1}(1) = 1, p^{-1}(3) = 2$ alebo $p^{-1}(1) = 2, p^{-1}(3) = 1$. Pre $p^{-1}(1) = 1$ by sme zo štvorcyklov mali $p^{-1} = id$, prípadne pre voľbu $p^{-1}(1) = 2$ dostávame $p^{-1} = (1234)^2$. To je však v spore s obrazom $p^{-1}(3)$ pre dvojcykly a teda neexistuje p s požadovanou vlastnosťou.

Akokoľvek nutnou podmienkou konjugovanosti množín permutácií G, H je zhodnosť ich typov. Vyvstáva prirodzená otázka ako možno nájsť $C_n(G, H)$. Jedna z možností je vziať fixnú permutáciu $g \in G$ a všetky $h_i \in H$ rovnakého typu ako g. Na získanie $C_n(G, H)$, stačí nájsť množinu kandidátov $C_n(g, H) = \bigcup C_n(g, h_i)$ pre $h_i \in H$ a otestovať, pre ktoré permutácie $p \in C_n(g, H)$ platí $pGp^{-1} = H$. Symbolom $C_n(g, H)$ budeme ďalej označovať množinu permutácií $p \in S_n$, pre ktoré platí $pgp^{-1} \in H$.

POZNÁMKA 4.33. Tento postup možno optimalizovať výberom permutácie $g \in G$. Samozrejme g treba vybrať tak, aby množina kandidátov $C_n(g, H)$ bola čo najmenšia. Mohutnosť množiny $C_n(g, H)$ možno pre permutáciu g typu A_i vypočítať zo vzorca $|C_n(g, H)| = n_i \prod_{j=1}^{n} a_{i,j}! j^{a_{i,j}}$.

Na základe vzorca z poznámky 4.33 možno na nájdenie $C_n(G,H)$ použiť algoritmus s nasledovným pseudokódom:

ALGORITMUS 3.
VSTUP: *Množiny* $G, H \subseteq S_n$
VÝSTUP: *Množina* $C_n(G,H)$

---

(1) *Zisti typ* $(n_1,\ldots,n_l)\times(A_1,A_2,\ldots,A_l),(m_1,\ldots,m_l)\times(B_1,B_2,\ldots,B_k)$ *množín* G,H. *Ak sú zhodné t.j.* $k=l, n_i=m_i, A_i=B_i$ *pre všetky* $i\in I_l$ *pokračuj inak skonči.*
(2) *Nájdi* $j\in I_l$ *tak, aby* $n_i\prod_{j=1}^{n} a_{i,j}!j^{a_{i,j}}$ *bolo najmenšie.*
(3) *Vezmi l'ubovol'nú permutáciu* g *typu* A_j *a množinu všetkých permutácií* $H_g\subseteq H$ *typu* A_j.
(4) *Skonštruuj pomocou algoritmu 2 množinu kandidátov* $C_n(g,H)=\cup_{h\in H_g}C_n(g,h)$.
(5) *Pre každú permutáciu* p *z* $C_n(g,H)$ *otestuj rovnosť množín* pGp^{-1} *a* H. *Ak je splnená vlož* p *do* $C_n(G,H)$.
(6) *Vráť* $C_n(G,H)$.

Máme teda algoritmus, ktorý nájde $C_n(G,H)$ pre l'ubovoľné množiny $G,H\subset S_n$. Tento môžeme použiť v algoritme 1 namiesto kroku 2.2.

Zložitosť algoritmu závisí na mohutnosti množiny $C_n(G,H)$. Tá môže nadobúdať v prípade, že prvky G a H obsahujú permutácie zložené len z dvojcyklov hodnotu $n(n/2)!2^{n/2}$. Takýto algoritmus má teda v porovnaní s algoritmom z [**43**] rádovo vyššiu zložitosť.

Z toho je zrejmé, že pri množinách permutácií $G=L_{Q_1}p_1^{-1}$, $H=L_{Q_2}p_2^{-1}$ možno nájsť permutáciu p, ktorá ich konjuguje oveľa rýchlejšie. Prvky množín G,H uvedeného tvaru majú určitú špeciálnu štruktúru, ktorá sa dá pri hľadaní $C_n(G,H)$ použiť. Jedná sa konkrétne o to, že pre rôzne $\pi_1,\pi_2\in G$ nemá permutácia $\pi_1^{-1}\pi_2$ fixný bod.

POZNÁMKA 4.34. Permutácia p z $Sym(X)$ má fixný bod práve vtedy, keď pre nejaké $x\in X$ platí rovnosť $p(x)=x$.

Inými slovami túto vlastnosť permutácií z G popisuje nasledujúca lema.

LEMA 4.35. *Nech $(Q, *)$ je kvázigrupa a p je ľubovoľná permutácia z L_Q. Potom pre ľubovoľné π_1, π_2 z množiny permutácií $L_Q p^{-1}$ platí $\pi_1(q) \neq \pi_2(q)$ pre každé $q \in Q$.*

DÔKAZ. Lemu dokážeme sporom. Majme $\pi_1(q), \pi_2(q) \in L_Q p^{-1}$. Na to aby sme dokázali $\pi_1(q) \neq \pi_2(q)$ stačí ukázať platnosť $\pi_1'(q) \neq \pi_2'(q)$ pre ľubovoľné rôzne $\pi_1'\pi_2' \in L_Q$.

Nech $\pi_1' \neq p_2'$ predstavujú translácie prvkami q_1, q_2 a nech $\pi_1'(q) = \pi_2'(q)$ pre nejaké $q \in Q$. Potom ale $q_1 * q = q_2 * q$. Priamo z definície 3.28 máme $q_1 = q_2$ a $\pi_1' = \pi_2'$, čo je v spore s predpokladom. Tým je lema dokázaná. □

Ako možno využiť túto špeciálnu vlastnosť prvkov G, H ? Treba si uvedomiť, že pri hľadaní $C_n(G, H)$ najprv nájdeme jednotlivé $C_n(g, h)$ pre fixné $g \in G$ a potom otestujeme, ktoré z prvkov konjugujú G, H. Postup teda závisí len na jedinej permutácii g. Pomocou nej sa skonštruuje množina $C_n(g, H)$, ktorá sa následne "filtruje." Problémom je, že táto množina môže byť príliš veľká. Možnosť ako získať menšiu množinu kandidátov je použiť aj iné permutácie $g_i \in G$ a to nasledovným spôsobom:

Bez ujmy na všeobecnosti predpokladajme, že permutácia $p \in C_n(G, H)$ konjuguje permutácie $g_i \in G, h_i \in H$ pre všetky $i \in I_n$ t.j.

$$p \in C_n(g_i, h_i)$$

pre všetky i. Platí teda:

$$p \in \bigcap_{i=1}^{n} C_n(g_i, h_i).$$

Predpokladajme teraz $p^{-1}(1) = s_1$. Z algoritmu 2 vyplýva $p^{-1}(g_i^j(1)) = h_i^j(s_1)$ pre ľubovoľné $i \in I_n, j \in \mathbb{N}$. Môžeme teda získať aj obrazy ďalších prvkov prostredníctvom permutácie p^{-1}. Na tie potom možno ďalej uplatniť rovnaký postup. Dá sa ukázať, že uvedeným postupom získame celú p. Ľahko sa to nahliadne z toho, že množiny G, H sú tvaru $G = L_{Q_1} p_1^{-1}, H = L_{Q_2} p_2^{-1}$ a teda pre každé $j \in I_n$ existuje permutácia $g_i \in G$ taká, že $g(1) = j$.

Pre názornosť si ukážme ako možno skonštruovať hľadanú permutáciu.

PRÍKLAD 4.36. Majme množiny G, H tvaru

$$G = \{g_1, g_2, g_3, g_4\} = \{id, (12)(34), (13)(24), (1423)\}$$

$$H = \{h_1, h_2, h_3, h_4\} = \{id, (13)(42), (14)(23), (1234)\}.$$

Hľadáme $p \in S_4$ aby $pg_ip^{-1} = h_i$ pre všetky $i \in I_4$. Nech $p^{-1}(1) = 2$. Z g_2, h_2 potom máme $p^{-1}(2) = 4$. Ďalej z g_3, h_3 máme $p^{-1}(3) = 3$ a z g_4, h_4 $p^{-1}(4) = 3$. Tu nastáva spor a teda voľba $p^{-1}(1) = 2$ nie je vhodná.

Vezmime teraz $p^{-1}(1) = 1$. Z cyklov permutácií g_i, h_i obsahujúcich 1 postupne dostávame $p^{-1}(2) = 3$, $p^{-1}(3) = 4$ a $p^{-1}(4) = 2$. Permutácia p^{-1} má teda tvar $p^{-1} = \binom{1234}{1342}$. Skúškou správnosti sa jednoducho zistí, že platí $pg_ip^{-1} = h_i$ pre všetky $i \in I_k$.

Z príkladu 4.36 vidíme, že obraz $p^{-1}(j)$ nejakého prvku $j \in I_k$ možno získať z viacerých dvojíc g_i, h_i. Ide tu teda o akúsi redundanciu informácií a teda zrejme stačí vziať menej párov g_i, h_i na skonštruovanie celej p^{-1}. Otázkou je koľko dvojíc stačí, aby sme z voľby $p^{-1}(1) = s_1$ našli celú p.

Z predchádzajúcich úvah je zrejmé, že stačí nájsť také $G' = \{\overline{g_1}, \ldots, \overline{g_k}\} \subseteq G$, že uzáver prvku 1 podľa funkcií z G' tvorí celú I_n.

POZNÁMKA 4.37. Pod uzáverom prvku $s \in S$ podľa funkcií $f_1, \ldots, f_m : S \mapsto S$ máme na mysli množinu $S' \subseteq S$, pre ktorú $f_i(S') = S'$ pre všetky $i \in I_m$ a $s \in S'$.

Prvky G' teda možno v určitom zmysle chápať ako generátory množiny G. Uvedené sa dá názornejšie popísať pomocou grafovej reprezentácie permutácií.

Uvažujme grafy G_{g_i} nad n vrcholmi vytvorené z permutácií g_i. Vrcholy V sú po rade označené symbolmy $1, \ldots, n$. Vrcholy j, k sú v G_{g_i} spojené hranou, ak permutácia g_i obsahuje cyklus tvaru $(\ldots j \ldots k \ldots)$. Potom je zrejmé, že pre každé G' tvorí zjednotenie grafov $G_{\overline{g_1}}, \ldots, G_{\overline{g_k}}$ súvislý graf na n vrcholoch. To je zároveň postačujúce, aby G' generovalo G.

Nech množina G' "generuje" G. Na nájdenie $p \in C_n(G,H)$ stačí zvoliť nejaké $h_i \in H$ ku každému $\overline{g_i}, i \in I_k$. Správnou voľbou s_1 ($p^{-1}(1) = s_1$) potom možno dopočítať celú p. Samozrejme tu tiež platí, že vybraná množina permutácií h_i tvorí generátor množiny H. Máme teda algoritmus, ktorý pre dve množiny permutácií $G = L_{Q_1}p_1^{-1}, H = L_{Q_2}p_2^{-1}$ nájde $C_n(G,H)$.

Tu môžeme vidieť jeho pseudokód:

ALGORITMUS 4.
VSTUP: *Množiny* $G, H \subseteq S_n$
VÝSTUP: *Množina* $C_n(G,H)$

---

(1) *Rozlož permutácie* $g_i \in G$ *na cykly a nájdi najmenšiu množinu* $G' = \{\overline{g_1}, \ldots, \overline{g_m}\}$ *generujúcu* G.
(2) *Rozlož na cykly permutácie* $h_i \in H$.
(3) *Pre každú množinu* H' *s* m *permutáciami* $\overline{h_1}, \ldots, \overline{h_m}$ *takými, že* H' *je rovnakého typu ako* G' *a* H' *generuje* H *rob nasledovné:*
  (3.1) *Pre každé* $P_j \in I_m$*, pre ktoré sú* $\overline{g_i}$ *a* $\overline{h_{P_j(i)}}$ *rovnakého typu, zvoľ každé* $s_i \in I_n$ *ako* $p^{-1}(1) = s_i$ *a dopočítaj* p.
  (3.2) *Ak platí rovnosť* $pGp^{-1} = H$ *ulož* p *do* $C_n(G,H)$.
(4) *Vráť* $C_n(G,H)$.

4.4. Algoritmus - zhrnutie

Teraz môžeme popísať výsledný algoritmus vyhodnocujúci izotópnosť kvázigrúp Q_1, Q_2.

Začneme s nutnými podmienkami, ktoré ako uvidíme z reálnych experimentov rapídne urýchlia rozhodovací proces.

4.4.1. Nutné podmienky izotópnosti. Vychádzame z dôsledku 4.15 vety 4.14. Tento dôsledok možno interpretovať tak, že pre izotópne kvázigrupy Q_1, Q_2 existuje bijekcia $\tau : L_{Q_2} \mapsto L_{Q_1}$, pre ktorú sú množiny permutácií $L_{Q_1}(\tau(p_2))^{-1}$, $L_{Q_2}(p_2^{-1})$ konjugované. Existuje teda párovanie medzi n prvkovými množinami tvaru $L_{Q_1}p_1^{-1}, L_{Q_2}p_2^{-1}$ pre $p_1 \in L_{Q_1}, p_2 \in L_{Q_2}$, ktoré "spája" množiny permutácií rovnakého typu.

Uvedené sa dá preformulovať nasledovne:
Nech $L_{Q_1} = \{g_1, \ldots, g_n\}, L_{Q_2} = \{h_1, \ldots, h_n\}$. Označme $L_{Q_1} g_i^{-1}$ symbolom $L^i_{Q_1}$ a obdobne $L_{Q_2} h_i^{-1} = L^i_{Q_2}$ pre $i \in I_n$. Potom z dôsledku 4.15 plynie, že pre izotópne kvázigrupy Q_1, Q_2 existuje permutácia $P \in S_n$ taká, že množiny $L^i_{Q_1}, L^{P(i)}_{Q_1}$ sú rovnakého typu. Teda pre izotópne kvázigrupy sú počty množín $L^i_{Q_1}$,$L^i_{Q_2}$ ľubovoľného typu zhodné.

Túto podmienku ešte možno zosilniť použitím kvázigrupovej verzie vety 3.27.

VETA 4.38. *Ak kvázigrupy $(Q, *)$ a $(Q, .)$ sú izotópne, potom aj k nim konjugované kvázigrupy $(Q, *_{i,j,k})$,$(Q, .{}_{i,j,k})$ pre $\{i, j, k\} = \{1, 2, 3\}$ sú izotópne.*

Z vety vyplýva, že pre každú dvojicu $(Q, *_{(i,j,k)}), (Q, .{}_{(i,j,k)})$ musí existovať spomínaná permutácia P. Ako ukazuje dôsledok 4.39 vety 4.39 stačí testovať len 3 dvojice.

VETA 4.39. *Nech $Q = (Q, *)$ je kvázigrupa. Pre konjugované $Q_1 = (Q, *_{(i,j,k)}), Q_2 = (Q, *_{(i,k,j)})$ kvázigrupy ku Q platí $L_{Q_1} = \{q^{-1} | q \in L_{Q_2}\}$.*

DÔKAZ. Vetu dokážeme najskôr pre $(i, j, k) = (1, 2, 3)$. Vezmime si ľubovoľné prvky $a, b \in Q$. Vezmime prvok c, pre ktorý platí $a * b = c$ v kvázigrupe Q. Z definície 3.30 máme

$$a *_{(1,2,3)} b = c, a *_{(1,3,2)} c = b.$$

Prepísaním do translácií kvázigrupy Q_1 máme $L^{Q_1}_a(b) = c$. Pri kvázigrupe Q_2 máme naopak $L^{Q_2}_a(c) = b$. Zloženie permutácií $L^{Q_1}_a, L^{Q_2}_a$ je identická permutácia, keďže pre ľubovoľné $b \in Q$ platí

$$L^{Q_2}_a(L^{Q_1}_a(b)) = b.$$

Teda $L^{Q_1}_a, L^{Q_2}_a$ sú navzájom inverzné permutácie. Toto platí pre ľubovoľné $a \in Q$ a teda množiny L_{Q_1}, L_{Q_2} obsahujú navzájom inverzné permutácie.

Rovnakým spôsobom sa to dokáže aj pre ostatné trojice (i, j, k). □

DÔSLEDOK 4.40. *Nech $Q = (Q, *)$ je kvázigrupa rádu n. Pre konjugované $Q_1 = (Q, *_{i,j,k}), Q_2 = (Q, *_{i,k,j})$ kvázigrupy*

ku Q existuje $P \in S_n$ také, že množiny $L^i_{Q_1}, L^{P(i)}_{Q_2}$ sú rovnakého typu.

DÔKAZ. Z vety 4.39 máme, že množiny L_{Q_1}, L_{Q_2} obsahujú navzájom inverzné permutácie. Bez ujmy na všeobecnosti prepokladajme, že príslušné inverzné permutácie sú v množinách L_{Q_1}, L_{Q_2} usporiadané v rovnakom poradí. Z rovnosti $g_i^{-1} = h_i$ vyplýva, že množiny $L_{Q_1}g_i^{-1}, L_{Q_2}h_i^{-1}$ tiež obsahujú navzájom inverzné permutácie. Keďže inverzné permutácie majú rovnakú cyklovú štruktúru, sú tiež rovnakého typu(veta 4.24). Z vety 4.39 máme, že množiny $L^i_{Q_1}, L^i_{Q_2}$ majú rovnaký počet permutácií daného typu. Sú teda rovnakého typu. □

Ako vidíme z dôsledku 4.40 pri testovaní nutnej podmienky stačí hľadať len tri permutácie. Pre ostatné konjugované kvázigrupy, už permutácie P budú existovať. Zahrnutím silnejšej nutnej podmienky dostávame výsledný algoritmus pre nájdenie izotopizmov dvoch kvázigrúp nasledovného tvaru:

ALGORITMUS 5.
VSTUP: *Kvázigrupy G, H rádu n.*
VÝSTUP: *Množina ich izotopizmov $Is(G, H)$.*

---

(1) *Skonštruuj konjugované kvázigrupy $G_1 = G = G_{(1,2,3)}, G_2 = G_{(2,1,3)}, G_3 = G_{(3,1,2)}$ a $H_1 = G = H_{(1,2,3)}, H_2 = H_{(2,1,3)}, H_3 = H_{(3,1,2)}$.*
(2) *Nájdi permutácie $P_1, P_2, P_3 \in S_n$, pre ktoré množiny $L^i_{G_j}$ a $L^{P_j(i)}_{H_j}$ sú rovnakého typu pre všetky $i, j \in I_n \times I_3$. Ak taká trojica neexistuje ukonči algoritmus a vráť $Is(G, H) = \emptyset$.*
(3) *Pre každé $j \in I_n$, pre ktoré L^1_G, L^j_H sú rovnakého typu rob nasledovné:*
  (3.1) *Algoritmom 4 nájdi množiny $C_n(L^1_G, L^j_H)$.*
  (3.2) *Nastav pre každé $p \in C_n(L^1_G, L^j_H)$ dve zložky izotopizmu $\varphi = h_j^{-1}pg_1, \psi = p$. Nájdi tretiu zložku θ a ulož do $Is(G, H)$ izotopizmus (θ, φ, ψ).*
(4) *Vráť $Is(G, H)$.*

---

	rád kvázigrupy		
	6	7	8
Veľkosť skupiny	počet skupín		
1	10	69	7288
2	6	203	788761
3		1	94
4		18	17982
5			18
6		1	1851
7		1	
8		1	505
9			1
10			183
12			76
13			1
14			40
16			14
18			9
20			5
22			4
24			3
34			1

TABUĽKA 2. Početností skupín pre slabšiu podmienku

4.5. Experimenty

Testovali sme obe verzie nutnej podmienky(slabšiu aj silnejšiu) na zástupcoch všetkých izotópnych tried Latinských štvorcov (kvázigrúp) rádov $6, 7, 8$. Tie boli získané zo stránky [**10**].

Keďže obe nutné podmienky rozlišujú štvorce na základe typov k nim priradených permutácií, je jasné, že množina zástupcov izotópnych tried sa rozpadne na skupiny (triedy). Prvky v rámci triedy prejdú testom nutnej podmienky ako potencionálne izotópne, prvky z rôznych tried naopak.

V tabuľke 2 možno vidieť počty jednotlivých skupín v závislosti od ich veľkosti pre rády $n = 6, 7, 8$ pre slabšiu nutnú podmienku.

	rád kvázigrupy		
	6	7	8
Veľkosť skupiny	počet skupín		
1	20	554	1675442
2	1	5	411
3			1

TABUĽKA 3. Početností skupín pre silnejšiu podmienku

Pre silnú verziu nutnej podmienky dostávame tabuľku 3. Tá sa dá interpretovať nasledovne. Majme zástupcov $L_i, i \in I_{22}$ rôznych izotópnych tried štvorcov rádu 6. Vezmime silnejšiu verziu nutnej podmienky a aplikujeme ju na každý pár štvorcov L_i, L_j pre $i, j \in I_{22}$. Z tabuľky 3 plynie, že pre jediný pár $L_i, L_j, i \neq j$ nedokáže nutná podmienka rozlíšiť ich neizotópnosť. Pri ráde 7 je takýchto párov 5. Pri ráde 8 už ich je 411. Naviac tu existuje jedna trojica zástupcov L_i, L_j, L_k, ktoré sú nerozlíšiteľné navzájom(každý s každým). Teda počet všetkých možných dvojíc, ktoré prejdú testom nutnej podmienky a sú neizotópne je $411.\binom{2}{2} + 1.\binom{3}{2} = 414$

Ako môžeme vidieť z tabuliek 3 a 2 ani jedna z nutných podmienok nedokáže rozlíšiť úplne neizotópne štvorce. Avšak percentuálna šanca, že príslušné Latinské štvorce, ktoré prejdú testom silnejšej nutnej podmienky a nie sú izotópne je minimálna. Pre rád 6 má jej úspešnosť hodnotu $1 - 1.\binom{22}{2} = 1 - 0.0043$. Pri ráde 7 sa dá jej úspešnosť vyjadriť ako $1 - 5.\binom{2}{2}/\binom{564}{2} = 1 - 3.15 * 10^{-5}$. Pri ráde 8 dostávame približne $1 - 3.0 * 10^{-10}$.

4.6. Zložitosť algoritmu a jeho porovnanie s Millerovým algoritmom

V tejto sekcii sa budeme venovať Millerovmu algoritmu [**43**] testujúceho izotópnosť dvoch kvázigrúp a jeho porovnaniu s naším algoritmom z hľadiska zložitosti a praktickej výkonnosti.

Millerov algoritmus je zovšeobecnením Tarjanovho algoritmu [**57**] na testovanie izomorfnosti dvoch grúp. Ten vychádza

z pozorovania, že grupy rádu n majú maximálny počet generátorov rovný $\log_2 n$ a teda ich izomorfnosť je rozhodnuteľná so zložistosťou $O(n^{\log_2 n+O(1)})$.

Miller ukázal, že toto dá zovšeobecniť aj na prípad kvázigrúp. V kvázigrupách sa dá množina generátorov popísať pomocou alternatívnej definície kvázigrupy:

DEFINÍCIA 4.41. *Množina Q spolu s binárnou operáciou $*$ tvorí kvázigrupu $(Q, *)$, ak pre ľubovoľné prvky $a, b \in Q$ majú rovnice*

$$a * b = x \tag{10}$$

$$a * x = b \tag{11}$$

$$x * a = b \tag{12}$$

jediné riešenie.

Vezmime si teraz funkcie f_1, f_2, f_3 také, že $f_1(a, b) = x$ ak platí rovnosť (10). Rovnako tak nech $f_2(a, b) = x, f_3(a, b) = x$ ak platia po rade rovnosti (11),(12).

Hovoríme, že prvky generujú kvázigrupu Q, ak ich uzáver podľa funkcií f_1, f_2, f_3 tvorí celú množinu Q. Miller ukázal, že množina takto definovaných generátorov kvázigrupy je mohutnosti nanajvýš $\log_2 n$.

LEMA 4.42. [**43**] *Kvázigrupa rádu n je generovaná množinou s maximálne $\log_2 n$ prvkami.*

Platí teda nasledujúca veta.

VETA 4.43. [**43**] *Izomorfnosť kvázigrúp je rozhodnuteľná so zložitosťou $O(n^{\log_2 n+O(1)})$.*

Ako dôkaz vety skonštruoval Miller nasledujúci algoritmus s uvedenou zložitosťou:

ALGORITMUS 6.
VSTUP: *Kvázigrupy Q_1, Q_2 rádu n.*
VÝSTUP: *Izomorfnosť Q_1 a Q_2.*

(1) *Nájdi množinu generátorov$\{a_1, \ldots, a_m\}$ kvázigrupy Q_1 obsahujúcu maximálne $\log_2 n$ prvkov.*
(2) *Pre každú m prvkovú množinu $\{b_1, \ldots, b_m\} \subset Q_2$ otestuj, či zobrazenie tvaru $\phi(a_i) = b_i$ pre $i \in I_m$ je dobre definovaný izomorfizmus Q_1 na Q_2.*
(3) *Ak sa v predchádzajúcom kroku našiel izomorfizmus, tak kvázigrupy sú izotópne. V opačnom prípade izotópne nie sú.*

V ňom fakticky len nahradil generátory grupy z Tarjanovho algoritmu generátormi kvázigrupy.

Tento algoritmus potom Miller použil s malou úpravou aj pri testovaní izotópnosti dvoch kvázigrúp.

Vezmime si teraz izotópne Latinské štvorce L, L_1 prostredníctvom izotopizmu (θ, φ, ψ) teda $L_1 = L^{(\theta,\varphi,\psi)}$.

Ako ukazuje lema 4.44 možno úlohu nájdenia izotopizmu dvoch štvorcov L, L_1 previesť na úlohu nájdenia izomorfizmu medzi štvorcami L_2, L_1 v redukovanom tvare. Tu predstavuje redukovaný štvorec L_2 štvorec izotópny k L prostredníctvom izotopizmu $(\theta_1, \varphi_1, \psi_1)$, teda $L_2 = L^{(\theta_1,\varphi_1,\psi_1)}$. Permutácia θ_1 predstavuje cyklickú permutáciu $(1\theta^{-1}(1))$.

LEMA 4.44. [**43**] *Pre dva izotópne normované Latinské štvorce L a L_1 sú štvorce $L_2 = L_1^{(\theta_1,\varphi_1,\psi_1)}$ a L_1 izomorfné.*

Z lemy vyplýva, že na otestovanie izotópnosti štvorcov L, L_1 (kvázigrúp) stačí vziať všetky redukované štvorce L_2 izotópne k L a hľadať izomorfizmus medzi L_2 a L_1. Keďže počet takýchto L_2 je n^2, dostávame nasledujúcu vetu:

VETA 4.45. [**43**] *Izotópnosť Latinských štvorcov je rozhodnuteľná so zložitosťou $O(n^{\log_2 n + O(1)})$.*

4.6.1. Porovnanie Millerovho a nášho algoritmu. Z hľadiska zložitosti je pre náš algoritmus (algoritmus 5) určujúcim faktorom krok 3.1, kde sa hľadá množina $C_n(L_G, L_H)$.

Pri algoritme 3 hľadajúcom $C_n(G, H)$ zas veľkosť množiny G', ktorá generuje G. Teraz ukážeme, čo platí pre veľkosť G'. Máme množinu G s n permutáciami. Pýtame sa aká je mohutnosť najmenšej $L_{G'}$, ktorá generuje (v našom zmysle) $L_G \subseteq S_n$. O množine L_G vieme, že pre rôzne permutácie $L_{g_i}, L_{g_j} \in L_G$ platí $L_{g_i}(x) \neq L_{g_j}(x)$ pre ľubovoľné $x \in I_n$ a $|L_G| = n$.

Teraz si pomôžeme dôkazom lemy 4.42. V ňom Miller ukázal, že každá podkvázigrupa H kvázigrupy G má maximálne $|G|/2$ prvkov, čo už samotné stačí na dôkaz lemy. Nám teda stačí ukázať, že uzáver prvku 1 podľa ľubovoľnej množiny $L_{G'}$ tvorí podkvázigrupu kvázigrupy G. Majme teda uzáver H prvku 1 prostredníctvom permutácií z $L_{G'}$. Pre každé $L_g \in G'$ a ľubovoľné $x \in H$ platí $L_g(x) \in H$, čo sa dá prepísať ako $g * H = H$ a teda H musí byť nutne podkvázigrupa G.

Preto mohutnosť generujúcej množiny v našom zmysle je maximálne $\log_2 n$.

Platí teda $|G'| \leq |\log_2 n|$. Pre algoritmus 4 to znamená, že k fixným permutáciam $\overline{g}_i$ možno vybrať permutácie $h_i \in H$ maximálne $n^{log_2 n}$ spôsobmi. Pre voľbu s_1 máme n možností a teda zložitosť algoritmu 4 je $O(n^{log_2 n + O(1)})$. To je smerodajné aj pre zložitosť algoritmu 5, keďže ďalšie jeho kroky sú polynomiálnej zložitosti stupňa 3.

Ako vidíme náš algoritmus a Millerov má rovnakú teoretickú zložitosť. S predpokladom, že nutná podmienka dokáže rozlíšiť väčšinu neizotópnych kvázigrúp rovnako ako v testovaných prípadoch je náš algoritmus výrazne rýchlejší.

Otvorenou otázkou teda zostáva akú úspešnosť má nutná podmienka pre väčšie kvázigrupy. Ak by bola táto úspešnosť porovnateľná s prípadmi $n = 7, 8$ dostali by sme veľmi výkonný pravdepodobnostný algoritmus na zistenie izotópnosti.

Zložitosť testovania nutnej podmienky sa odvodí nasledovne: Zistenie typu permutácie je zložitosti $O(n)$. Pre každú z n množín $L^i_{Q_1}$ sa zistí typ každej z jej n permutácií. Zistenie typov všetkých $L^i_{Q_1}$ je teda zložitosti $O(n^3)$. Porovnanie typov $L^i_{Q_1}$ a $L^j_{Q_2}$ má zložitosť $O(n^2)$ a teda testovanie nutnej podmienky izotopie kvázigrúp má zložitosť $O(n^3)$.

4.7. Výsledky

V tomto odseku popíšeme niekoľko zaujímavých výsledkov, ktoré vyplývajú z predchádzajúcich konštrukcií algoritmu. Upresníme odhad z [**51**] pre maximálny počet autotopizmov kvázigrúp (Latinských štvorcov) daného rozmeru. Ukážeme tu tiež ako vyzerajú autotopizmy grúp a zároveň tu uvedieme vzorec pre výpočet $|AUT(G)|$. Ako uvidíme na záver, vzorec pre výpočet $|AUT(G)|$ je ekvivalentný vzorcu z [**3**]. Táto skutočnosť teda potvrdzuje korektnosť konštrukcie prezentovaného algoritmu na hľadanie izotopií kvázigrúp.

4.7.1. Odhad počtu autotopizmov kvázigrúp. Začneme so zlepšením odhadu autotopizmov kvázigrúp. Už Sade v článku [**51**] z roku 1968 dokázal, že pre štvorec L rádu n sa dá mohutnosť množiny jeho autotopizmov ($AUT(L)$) ohraničiť číslom $n(n!)$. Sade odvodil uvedenú hornú hranicu za pomoci takzvaných fundamentálych autotopizmov. Ukázal, že každý autotopizmus ľubovoľnej kvázigrupy Q sa dá zapísať ako zloženie fundamentálneho autotopizmu a automorfizmu špeciálnej kvázigrupy izotópnej s Q.

My budeme pri určení presnejšej hornej hranice používať odhady plynúce z konštrukcie algoritmu 5.

Vychádzame z dôsledku 4.17. Hľadáme pre L_Q a fixné $p_2 \in L_Q$ také dvojice $(p_1, p) \in L_Q \times Sym(Q)$, že platí $L_Q p_2^{-1} = pL_Q p_1^{-1} p^{-1}$. Ak označíme $L_Q p_2^{-1} = G, L_Q p_1^{-1} = H$, potom platí:

$$p \in C_n(G, H) \subset \bigcap_{g_i \in G} C_n(g_i, H).$$

Nech n_i označuje počet permutácií $h \in H$ rovnakého typu ako permutácia $g_i \in G$. Potom mohutnosť $C_n(g_i, H)$ sa dá podľa dôsledku 4.29 ohraničiť číslom $n_i|St_{Sym(Q)}(g_i)|$. Toto číslo je maximálne vtedy, ak všetky permutácie $h_i \in H$ (okrem identickej permutácie) sú rovnakého typu a mohutnosť ich stabilizátora $St_{S_n}(g_i)$ je maximálna.

Hľadáme teda permutáciu z S_n s maximálnym stabilizátorom. Začneme s tým, že cyklová štruktúra takej permutácie sa musí skladať len z dvoj a trojcyklov.

LEMA 4.46. *Vezmime akciu konjugáciou na grupe S_n. Nech permutácia $p \in S_n$ obsahuje cyklus dĺžky aspoň štyri. Potom existuje permutácia $p' \in S_n$ taká, že jej stabilizátor v tejto akcii má väčšiu mohutnosť t.j. $|St_{S_n}(p)| < |St_{S_n}(p')|$.*

DÔKAZ. Lemu dokážeme priamo. Vezmime permutáciu $p \in S_n$, ktorá je typu $(a_1, a_2, \ldots, a_n)$. Podľa predpokladov lemy sa v nej nachádza cyklus dĺžky aspoň 4. To znamená, že pre nejaké $4 \leq k \leq n$ je a_k nenulové. Vezmime teraz permutáciu p', ktorá vznikne z p tak, že v nej rozložíme každý z cyklov dĺžky k na dva cykly dĺžky 2 a $k-2$. Chceme ukázať, že permutácia p' má väčší stabilizátor.

Priamo z konštrukcie vieme, že p' je typu $(b_1, b_2, \ldots, b_n)$, kde a_i, b_i sú až na členy b_{k-2}, b_k, b_2 rovnaké.

Pre tieto platí $b_{k-2} = a_{k-2} + a_k$, $b_k = 0$, $b_2 = a_2 + a_k$.

Ukážme, že skutočne platí $|St_{S_n}(p)| < |St_{S_n}(p')|$. Z dôsledku 4.29 môžeme pre mohutnosť stabilizátora $|St_{S_n}(p)|$ písať $|St_{S_n}(p)| = \prod a_i! i^{a_i}$. Pre podiel $|St_{S_n}(p')|/|St_{S_n}(p)|$ máme

$$\begin{aligned}
|St_{S_n}(p')|/|St_{S_n}(p)| &= \prod b_i! i^{b_i} / \prod a_i! i^{a_i} \\
&= \frac{(a_2 + a_k)! 2^{(a_2+a_k)} . (a_{k-2} + a_k)! (k-2)^{(a_{k-2}+a_k)}}{(a_2)! 2^{a_2} . (a_{k-2})! (k-2)^{a_{k-2}} . a_k! k^{a_k}} \\
&= a_k! \binom{a_2 + a_k}{a_2} \binom{a_{k-2} + a_k}{a_{k-2}} \left[\frac{2(k-2)}{k}\right]^{a_k}.
\end{aligned} \tag{13}$$

Keďže sme predpokladali, že a_k je nenulové, sú obe kombinačné čísla vystupujúce v rovnici 13 väčšie ako jedna. Navyše $\frac{2(k-2)}{k} \geq 1$ a teda platí $|St_{S_n}(p')| > |St_{S_n}(p)|$.

□

Z lemy 4.46 plynie, že pri hľadaní permutácie s najväčším stabilizátorom stačí uvažovať len permutácie zložené z dvoj a trojcyklov. Ako si ukážeme v nasledujúcej leme permutácia má maximálny stabilizátor, keď obsahuje maximálny počet, alebo naopak minimálny počet dvojcyklov.

LEMA 4.47. *Z permutácií $p_i \in S_n$, ktoré sú zložené z cyklov dĺžky dva a tri má maximálny stabilizátor permutácia p_i, ktorá obsahuje maximálny, alebo naopak minimálny počet dvojcyklov.*

DÔKAZ. Vezmime si permutáciu typu $(0, a_2, a_3, 0, \ldots)$ a diskrétnu funkciu

$$f(a_2, a_3) = a_2!2_2^a.a_3!3_3^a,$$

ktorá určuje mohutnosť jej stabilizátora. Pre n samozrejme platí $n = 2a_2+3a_3$. Jedná sa teda o funkciu s jediným parametrom a_2. Pre väčšiu názornosť budeme niekde chápať funkciu f, ako funkciu s dvoma parametrami a_2, a_3.

Na to aby sme dokázali lemu stačí ukázať, že funkcia f nenadobúda žiadne lokálne maximum vo vnútornom bode. Teda pre žiadne $a_2 \in \mathbb{N}$ a $a_{2min} < a_2 < a_{2max}$, kde symboly a_{2min}, a_{2max} označujú minimálne resp. maximálne prípustné hodnoty a_2.

Funkcia f nadobúda v bode a_2 lokálne maximum, keď hodnota funkcie v susedných (prípustných) bodoch je menšia ako $f(a_2)$.

Susedné body pre a_2 sú $a_2' = a_2 + 3$ a $\bar{a}_2 = a_2 - 3$. V nich nadobúda funkcia f hodnoty

$$f(a_2') = (a_2 + 3)!2^{a_2+3}(a_3 - 2)!3^{a_3-2},$$
$$f(\bar{a}_2) = (a_2 - 3)!2^{a_2-3}(a_3 + 2)!3^{a_3+2}.$$

Vezmime teraz podiely funkčných hodnôt vo vnútornom bode a_2 a jeho susedoch. Pre ne platí nasledovné:

$$f(a_2)/f(a_2') = \frac{a_2!2^{a_2}a_3!3^{a_3}}{(a_2 + 3)!2^{a_2+3}(a_3 - 2)!3^{a_3-2}} = \frac{9a_3(a_3 - 1)}{8(a_2 + 1)(a_2 + 2)(a_2 + 3)}$$

$$f(a_2)/f(\bar{a}_2) = \frac{a_2!2^{a_2}a_3!3^{a_3}}{(a_2 - 3)!2^{a_2-3}(a_3 + 2)!3^{a_3+2}} = \frac{8a_2(a_2 - 1)(a_2 - 2)}{9(a_3 + 1)(a_3 + 2)}.$$

Funkcia f nadobúda v a_2 lokálne maximum, keď oba podiely sú väčšie ako 1. Ich súčinom dostaneme výraz

$$\frac{f(a_2)f(a_2)}{f(a_2')f(\bar{a}_2)} = \frac{9a_3(a_3-1)8a_2(a_2-1)(a_2-2)}{8(a_2+1)(a_2+2)(a_2+3)9(a_3+1)(a_3+2)}.$$

Tento výraz je evidentne menší ako 1 a teda $f(a_2) < f(a_2')$, alebo $f(a_2) < f(\bar{a}_2)$.

Z toho teda vyplýva jednoznačný záver, že funkcia f môže nadobudnúť maximum len v krajných bodoch. Teda tam, kde je a_2 maximálne respektíve minimálne. To dokazuje lemu.

□

Teraz ukážeme, pre ktoré z dvoch hodnôt a_{2min}, a_{2max} je stabilizátor najmohutnejší.

VETA 4.48. *Majme permutácie z množiny S_n, kde $n \geq 5$ zložené z dvoj a trojcyklov. Mohutnosť ich stabilizátora v akcii konjugácie $|St_{S_n}(p)|$ s výnimkou $n = 9$ je maximálna, ak obsahuje maximálny možný počet dvojcyklov. Pre $n = 9$ je naopak stabilizátor maximálny, ak príslušná permutácia sa skladá len z trojcyklov.*

DÔKAZ. Z lemy 4.47 vyplýva, že stačí uvažovať len permutácie zložené z dvoj a troj cyklov, pričom počet dvojcyklov je maximálny alebo naopak minimálny. Vetu dokážeme matematickou indukciou vzhľadom na veľkosť n. Chceme dokázať indukčný predpoklad: Ak platí nerovnosť $f(a_{2min}) < f(a_{2max})$ pre n, potom platí aj pre $n+6$. Pre permutácie z S_{n+6} sa dajú ich hodnoty a'_{2min}, a'_{2max} vyjadriť ako $a'_{2min} = a_{2min}, a'_{2max} = a_{2max} + 3$.

Pre podiely $f(a'_{2min})/f(a_{2min})$ a $f(a'_{2min})/f(a_{2max})$ dostávame nasledovné :

$$\begin{aligned} f(a'_{2min})/f(a_{2min}) &= \frac{a'_{2min}!2^{a'_{2min}}a'_3!3^{a'_3}}{a_{2min}!2^{a_{2min}}a_3!3^{a_3}} \\ &= 9(a_3+1)(a_3+2) \end{aligned} \tag{14}$$

$$f(a'_{2max})/f(a_{2max}) = \frac{a'_{2max}!2^{a'_{2max}}a'_3!3^{a'_3}}{a_{2max}!2^{a_{2max}}a_3!3^{a_3}}$$
$$= 8(a_{2max}+3)(a_{2max}+2)(a_{2max}+1) \qquad (15)$$

Pre $a_{2max} > a_3$ a $n > 9$ dostávame z rovníc (14),(15)

$$f(a'_{2min})/f(a_{2min}) < f(a'_{2max})/f(a_{2max}).$$

Z toho plynie

$$f(a_{2max})f(a'_{2min}) < f(a_{2min})f(a'_{2max}).$$

Keďže $f(a_{2max}) > f(a_{2min})$, tak platí $f(a'_{2max}) > f(a'_{2min})$ a teda platí indukčný predpoklad.

Teraz už stačí ukázať platnosť $f(a_{2max}) > f(a_{2min})$ pre 6 po sebe idúcich hodnôt n. Pre a_{2min}, a_{2max} a $n = \{5, \ldots, 16\}$ dostávame hodnoty mohutností stabilizátotov, ktorých prehľad možno vidieť v nasledujúcich tabuľkách.

n	5	6	7	8	9	10
a_{2min}, a_3	(1,1)	(0,2)	(2,1)	(1,2)	(0,3)	(2,2)
$f(a_{2min})$	6	18	24	36	162	144
n	11	12	13	14	15	16
a_{2min}, a_3	(1,3)	(0,4)	(2,3)	(1,4)	(0,5)	(2,4)
$f(a_{2min})$	324	1944	1296	3888	29160	15552

n	5	6	7	8	9	10
a_{2max}, a_3	(1,1)	(3,0)	(2,1)	(4,0)	(3,1)	(5,0)
$f(a_{2max})$	6	48	24	384	144	3840
n	11	12	13	14	15	16
a_{2max}, a_3	(4,1)	(6,0)	(5,1)	(7,0)	(6,1)	(8,0)
$f(a_{2max})$	1152	23040	11520	645120	138240	$> 10^7$

Z tabuliek je vidno, že pre $n \in \{10, \ldots, 16\}$ platí nerovnosť $f(a_{2min}) < f(a_{2max})$. Využitím indukcie dostávame platnosť vety pre všetky $n > 9$. Z tabuliek ďalej vyplýva, že veta platí pre všetky $n > 4$ okrem $n = 9$. Tým je veta dokázaná. □

DÔSLEDOK 4.49. *Majme l'ubovoľnú kvázigrupu Q rádu $n > 5$. Pre n párne možno pre mohutnosť množiny jej autotopizmov písať*

$$|AUT(Q)| \leq n(n-1)(n/2)!2^{n/2}.$$

Pre každé nepárne n okrem $n = 9$ sa dá $|AUT(Q)|$ ohraničiť ako

$$|Aut(Q)| \leq n(n-1)3((n-3)/2)!2^{(n-3)/2}.$$

Pre $n = 9$ platí $|Aut(Q)| \leq 9(9-1)3!3^3 = 11664$.

DÔKAZ. Majme l'ubovoľné fixné p_{2Q}. Počet autotopizmov Q je daný počtom dvojíc $(p_1, p) \in L_Q \times Sym(Q)$, pre ktoré platí $L_Q p_2^{-1} = pL_Q p_1^{-1} p^{-1}$(dôsledok 4.17). Voliť p_1 možno n spôsobmi. Pre $G = L_Q p_2^{-1}$ a $H = L_Q p_1^{-1}$ je $p \in C_n(G, H)$. Z úvah na začiatku sekcie (4.7.1) máme,

$$C_n(G, H) \leq \sum_{i=1}^{n} n_i St_{Sym(Q)}(g_i),$$

kde n_i predstavuje počet permutácií z H rovnakého typu ako g_i. Keďže H obsahuje identickú permutáciu platí $n_i \leq n-1$. A teda $|AUT(Q)| \leq n(n-1)|St_{Sym(Q)}(g_i)|$ pre l'ubovoľné $g_i \in G$. To už spolu s vetou 4.48 dokazuje dôsledok. □

4.7.2. Autotopizmy grúp. V tejto sekcii sa budeme zaoberať autotopizmami grúp, ich konštrukciou a odhadmi počtu. Dokážeme tu alternatívny vzorec pre výpočet počtu autotopií kvázigrúp.

Majme grupu $(G, *)$ rádu n. Pýtame sa ako vyzerajú autotopizmy tejto grupy. Z dôsledku 4.17 máme, že každý autotopizmus je pre l'ubovoľné fixné $p_1 \in L_G$ určený jednoznačne permutáciami $p_2 \in L_G, p \in Sym(G)$ spĺňajúcimi vzťah

$$L_G p_1^{-1} = pL_G p_2^{-1} p^{-1}.$$

Z Cayleyho vety (veta 3.18) máme, že grupa $(G, *)$ je izomorfná s L_G, keďže L_g tvorí práve priradenie $g \mapsto (x \mapsto gx)$ zo znenia vety.

Máme teda grupu L_G, ktorá je izomorfným obrazom grupy G v symetrickej grupe $Sym(G)$.

Z toho ale vyplýva, že $L_G p_i^{-1} = L_G$ pre l'ubovol'né $p_i \in L_G$. Teda nájdenie izotopizmu sa nám zredukovalo na nájdenie takých permutácií p, pre ktoré

$$L_G = pL_G p^{-1}.$$

Dostávame sa tak k normalizátoru množiny L_G.

DEFINÍCIA 4.50. *Nech X je podmnožina grupy G. Potom normalizátor X v grupe G je množina*

$$N_G(X) = \{g | g \in G, gXg^{-1} = X\}.$$

Normalizátor l'avej regulárnej reprezentácie grupy $(G, *)$ v $Sym(G)$ sa tiež nazýva holomorf grupy G a označuje sa $Hol(G.)$ Platí preň nasledujúca veta.

VETA 4.51. *Nech G je grupa a L_G jej regulárna reprezentácia v $Sym(G)$. Potom pre holomorf grupy G platí*

$$Hol(G) = Aut(G)L_G.$$

Z nej už možno odvodiť počet autotopizmov grupy.

DÔSLEDOK 4.52. *Autotopizmy grupy G sú tvaru $(\theta, p, p_2^{-1} p p_1)$, pre l'ubovol'né $p_1, p_2 \in L_G$, $p \in Aut(G)L_G$ a nejaké $\theta \in Sym(G)$.*

DÔKAZ. Priamo z vety 4.51 a dôsledku 4.16. □

DÔSLEDOK 4.53. *Pre mohutnosť grupy $AUT(G)$ autotopizmov grupy G platí*

$$|AUT(G)| = n^2 |Aut(G)|.$$

DÔKAZ. Priamo z vety 4.51 a dôsledku 4.17. □

KAPITOLA 5

Latinské štvorce a S- boxy

V tejto kapitole ukážeme konštrukciu Latinských štvorcov s dobrými kryptografickými vlastnosťami. Začneme s konštrukciou perfektných nelineárnych funkcií.

5.1. Konštrukcia perfektných nelineárnych funkcií

Z hľadiska kryptoanalýzy je potrebné, aby funkcie $f : Z_2^n \mapsto Z_2^m$ (S-boxy), používané pri konštrukciách šifier, spĺňali dve základné kritériá: balansovanosť a perfektnú nelinearitu. Je známe, že S-boxy nemôžu súčasne spĺňať obe kritériá. Z toho dôvodu možno skonštruovať len S- boxy, ktoré spĺňajú úplne len jedno z kritérií. Keďže stupeň nelinearity S-boxov použitých v šifre je určujúcou hodnotou kvality šifry, je vhodné uprednostniť kritérium perfektnej nelinearity pred balansovanosťou. Je potrebné však, aby perfektne nelineárny S-box bol "dostatočne balansovaný".

Ako ukázala Nybergová v [**47**], tohoto je možné dosiahnuť len v prípade, keď je $n \geq 2m$. V článku sa pri konštrukcii takýchto S-boxov používajú takzvané "bent" funkcie, čo sú z hľadiska balansovanosti jemne vychýlené funkcie. V článku [**26**] zovšeobecnili autori perfektnú nelineárnosť na grupoidy. To im umožnilo skonštruovať perfektne nelineárnu funkciu s úplne plochou diferenčnou tabuľkou.

Našou snahou je ukázať na základe tohoto článku jednoduchú konštrukciu kvalitných Latinských štvorcov pre kryptografické aplikácie.

5.1.1. Perfektná nelinearita a balansovanosť. Diferenciálna kryptoanalýza využíva pri analýze S-boxov takzvanú diferenčnú tabuľku [**27**]. Táto tabuľka udáva počet diferencií výstupov (stĺpce) v závislosti od diferencií vstupných (riadky) hodnôt S-boxu. Diferenčná tabuľka je smerodajná pri určovaní

nelinearity danej funkcie a z toho dôvodu aj vhodnosti príslušného S-boxu pre konštrukciu šifry.

PRÍKLAD 5.1. V tabuľke 1 možno vidieť funkciu $f : Z_2^2 \mapsto Z_2$ a jej diferenčnú tabuľku. Riadky diferenčnej tabuľky určujú diferenciu vstupu, stĺpce diferenciu výstupu. Bunky sú vyplnené hodnotami početností vstupných diferencií v závislosti od výstupných diferencií.

i	$f(i)$
0	1
1	1
2	1
3	0

$\triangle i / \triangle f(i)$	0	1
0	4	0
1	2	2
2	2	2
3	2	2

TABUĽKA 1. Funkcia f a jej diferenčná tabuľka

Táto tabuľka popisuje perfektne nelineárnu funkciu (pozri nižšie).

Ak je nejaká hodnota diferenčnej tabuľky dostatočne vychýlená od strednej hodnoty, možno spravidla cez takýto nekvalitný S-box zrealizovať útok na šifru. Ideálny stav je teda, keď je celá diferenčná tabuľka vyplnená jednou hodnotou a je teda kompletne "plochá". Takúto funkciu (S-box) popisuje nasledujúca definícia.

DEFINÍCIA 5.2. [**47**] *Funkcia $f : Z_q^n \mapsto Z_q$ je perfektne nelineárna(PN), ak pre každé nenulové $w \in Z_q^n$ dosahuje diferencia*

$$f(w + x) - f(x)$$

každú z hodnôt $k \in Z_q$ práve q^{n-1} krát.

POZNÁMKA 5.3. Pod operáciou "$-$" máme na mysli inverznú operáciu k sčítaniu v príslušnom okruhu.

Zovšeobecnenie perfektnej nelinearity na funkcie s oborom hodnôt Z_q^m uvádza definícia 5.4.

DEFINÍCIA 5.4. [**47**] *Funkcia $f : Z_q^n \mapsto Z_q^m$ je perfektne nelineárna, ak pre každé nenulové $w \in Z_q^n$ dosahuje diferencia*

$$f(w + x) - f(x)$$

každú z hodnôt $k \in Z_q$ práve q^{n-m} krát.

Analyzujme teraz funkcie $f : Z_2^n \mapsto \mathbb{Z}_2^m$ z hľadiska perfektnej nelinearity. Predpokladajme, že pracujeme s funkciou $f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$. Uvažujme diferenčnú tabuľku funkcie. Keďže platí

$$f(i \oplus x) \oplus f(x) = f(i \oplus (i \oplus x)) \oplus f(i \oplus x),$$

tak hodnoty v diferenčnej tabuľke sú buď nulové, alebo prinajmenšom majú hodnotu dva.

POZNÁMKA 5.5. V ďalšom texte budeme symbolom $\oplus$ označovať XOR operáciu.

Keďže tabuľka má rozmery $2^n \times 2^n$ bude "najplochejšia" (hodnoty buniek budú v úzkom intervale) tabuľka, ktorú možno získať taká tabuľka, kde bunky majú hodnoty dva alebo nula.

Je zrejmé, že počty 0 a 2 sú v takomto prípade pre každý riadok 2^{n-1} (viď poznámka 5.6).

POZNÁMKA 5.6. V diferenčnej tabuľke funkcie $f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^m$ má suma hodnôt cez ľubovoľný riadok veľkosť 2^n.

Samozrejme pri vstupnej diferencii 0 sa nachádza v riadku na nultej pozícii hodnota 2^n a zvyšok sú nuly. To platí všeobecne takže, keď budeme hovoriť o riadkoch diferenčnej tabuľky funkcií $f : Z_2^n \mapsto Z_2^m$ máme na mysli riadky $1, 2, \ldots, 2^n - 1$.

Teda perfektnú nelinearitu nemožno dosiahnuť pri funkciách, kde definičný obor a obor hodnôt je tvorený rovnakou grupou $\mathbb{Z}_2^n$.

Ako je to však pri rôznych oboroch?

Pre všeobecný prípad, kde $f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^m$ je teoreticky možné podľa predchádzajúcej úvahy dosiahnuť stav, kde všetky hodnoty každého z riadkov sú zhodné a to už v prípade $n = m + 1$. Tu by príslušná hodnota každej bunky bola 2. Zvyšovaním parametra n by iba narastala hodnota výplne diferenčnej tabuľky na 2^{n-m}. Ako však ukázala Nybergová toto je prakticky možné len pre $n \geq 2m$.

Perfektná nelinearita sa dá tiež popísať pomocou balansovanosti. Tá charakterizuje funkcie, ktorých funkčné hodnoty

sa vyskytujú s rovnakou početnosťou a pokrývajú celý obor hodnôt. Balansovanosť popisujú nasledujúce dve definície.

DEFINÍCIA 5.7. [**47**] *Funkcia $g : Z_q^n \mapsto Z_q$ je balansovaná, ak platí :*

$$\sum_{x \in Z_q^n} g(x) = q^{n-1}.$$

DEFINÍCIA 5.8. [**47**] *Funkcia $g : Z_q^n \mapsto Z_q^m$ je balansovaná, ak pre každé $c \in Z_q^m$ je $c.g(x)$ balansovaná funkcia.*

Tu aj v d'alšom texte budeme pod operáciou . mať na mysli skalárny súčin vektorov c a $g(x)$.

S využitím balansovanosti potom stačí, keď sa použije "derivát" $D_w f : Z_q^n \mapsto Z_q^m$ funkcie f tvaru

$$D_w f(x) = f(x + w) - f(x).$$

Funkcia f je potom perfektne nelineárna, ak $D_w f$ je balansovaná pre všetky $w \in Z_q^m$. Toto potvrdzuje nasledujúca veta.

VETA 5.9. [**47**] *Funkcia $f : Z_q^n \mapsto Z_q^m$ je perfektne nelineárna práve vtedy, keď pre každé nenulové $c \in Z_q^m$ je funkcia $g(x) = c.f(x)$ perfektne nelineárna v zmysle definície 5.2.*

5.2. Zovšeobecnená perfektná nelinearita

Teraz sa zameriame na všeobecnejší prípad perfektnej nelinerity, ktorý umožní pristúpiť ku konštrukcii perfektných nelineárnych funkcií cez Latinské štvorce. Pojmy "perfektná nelinearita" a "balansovanosť" možno rozšíriť na funkcie, ktorých definičný obor je grupoid [**26**]. Stačí, ak sa v definíciach 5.7,5.8 nahradí grupa $\mathbb{Z}_2^n$ grupoidom.

Definície zostávajú v pôvodnom znení rovnako ako všetky tvrdenia, ktoré zostávajú v platnosti ($\mathbb{Z}_2^n$ sa nahradí grupoidom S, $0 \in \mathbb{Z}_2^n$ sa nahradí ľavou jednotkou grupoidu). Nepatrný rozdiel medzi funkciami s definičným oborom Z_2^n a grupoidom charakterizuje veta 5.10.

VETA 5.10. [**26**] *Funkcia $g : S \mapsto \mathbb{Z}_2^m$ je balansovaná práve vtedy, keď $|S| = 2^m l$ a pre každé $k \in \mathbb{Z}_2^m$ platí: $|A_k| = |S|/2^m$.*

Množina A_k z vety 5.10 má tvar $A_k = \{i : g(i) = k\}$, kde k je desiatkový rozvoj binárneho vektora k.

Veta je rigoróznym potvrdením faktu, že obrazy balansovanej funkcie $g : S \mapsto \mathbb{Z}_2^m$ pokrývajú celý obor hodnôt a jednotlivé obrazy $y \in \mathbb{Z}_2^m$ sú rovnako početné.

Nad grupoidom sa definuje obdoba perfektnej nelinearity - všeobecná perfektná nelinearita.

DEFINÍCIA 5.11. [**26**] *Funkcia $f : S \mapsto \mathbb{Z}_2^m$ je všeobecne perfektne nelineárna (VPN), ak pre každé $i \in S$ rôzne od l'avej jednotky je $D_i f : S \mapsto \mathbb{Z}_2^m$ balansovaná funkcia.*

Platí obdoba vety 5.9.

VETA 5.12. [**26**] *Funkcia $f : S \mapsto \mathbb{Z}_2^m$ je VPN práve vtedy, keď pre každé $c \in \mathbb{Z}_2^m \setminus 0$ je funkcia $c.(D_i f) : S \mapsto \mathbb{Z}_2$ balansovaná.*

Na rozdiel od PN umožňuje koncept VPN funkcií skonštruovanie funkcie, ktorá je balansovaná (viď [**26**]) a má kompletne plochú diferenčnú tabuľku. V ňom autori ukázali, ako skonštruovať funkciu $f : S \mapsto \mathbb{Z}_2^n$, ktorá je VPN a balansovaná pre sprava jednoduchý grupoid $(S, *)$ s 2^n prvkami.

POZNÁMKA 5.13. Ak pre grupoid $(S, *)$ platí $a * S = S$ pre každé $a \in S$, potom S voláme sprava jednoduchý.

Budeme sledovať spomínanú konštrukciu uvedenú v [**26**], keďže táto je kľúčová pre naše účely.Nech $S = \{0, \ldots, 2^n - 1\}$ a funkcia $f : S \mapsto \mathbb{Z}_2^n$ má predpis $f(x) = x_b$, kde x_b predstavuje binárny rozvoj čísla x. Našou úlohou je teraz zadefinovať operáciu $*$ na grupoide tak, aby f bola VPN (balansovaná už je).

POZNÁMKA 5.14. Skonštruovanie bijektívnej VPN funkcie $f : S \mapsto \mathbb{Z}_2^n$ pre daný grupoid $(S, *_1)$ je ekvivalentné zadefinovaniu operácie $*_2$, aby bijektívna funkcia $F : S \mapsto \mathbb{Z}_2^n$ bola VPN. Plynie to z faktu, že F, f sú bijekcie a teda stačí vhodne premenovať symboly. Nech teda f je VPN. Potom aby F bola VPN na grupoide $(S, *_2)$ stačí vziať

$$i_1 *_2 i_2 = F^{-1}(f(i_1)) *_1 F^{-1}(f(i_2)).$$

Aby f bola VPN, musí byť funkcia

$$D_i f(x) = (i * x)_b \oplus x_b$$

pre každé $i \in S$ balansovaná (definícia 5.11). Je zrejmé, že to nastane v prípade, keď $D_i f(x)$ predstavuje bijekciu.

Na druhej strane, ak je $D_i f(x)$ bijekcia, potom aj $i * x$ musí tvoriť pre fixné i permutáciu s $Sym(S)$. Hľadáme teda permutáciu $\alpha \in Sym(S)$, pre ktorú platí $\alpha(x) = i * x$ a bijekciu $\beta : S \mapsto \mathbb{Z}_2^n$ takú, že $\beta(x) = D_i f(x) = (i * x)_b \oplus x_b$ pre $x \in S$.

Pre zjednodušenie zápisu stotožnime množinu S s množinou $\mathbb{Z}_2^n$.

Teda nech $i \in S$ predstavuje prvok i_b v $\mathbb{Z}_2^n$. Potom hovoríme o dvoch permutáciách α, β na $\mathbb{Z}_2^n$ s vlastnosťou

$$\beta(x) = \alpha(x) \oplus x$$

pre $x \in \mathbb{Z}_2^n$. Hovoríme vlastne o úplnom zobrazení grupy (kvázigrupy) $(\mathbb{Z}_2^n, \oplus)$.

DEFINÍCIA 5.15. [**13**] *Úplné zobrazenie kvázigrupy $(Q, *)$ je bijektívne zobrazenie $\theta : Q \mapsto Q$ také, že zobrazenie $\eta : Q \mapsto Q$ dané predpisom $\eta(x) = x * \theta(x)$ je tiež bijekcia.*

Úplné zobrazenie sa dá pomocou Latinských štvorcov popísať transverzálou.

DEFINÍCIA 5.16. [**13**] *Transverzála Latinského štvorca rádu n je tvorená n bunkami, pričom sa v každom riadku a každom stĺpci nachádza práve jedna z nich. Naviac žiadne dve bunky transverzály neobsahujú rovnaký symbol.*

Transverzála je ekvivalentom úplného zobrazenia v Latinskom štvorci. Teda, ak máme úplné zobrazenie θ kvázigrupy Q a Latinský štvorec L predstavujúci jeho Cayleyho tabuľku, potom bunky tvaru $L(x, \theta(x))$ tvoria transverzálu L. Teda existuje jednoznačný vzťah medzi úplnými zobrazeniami kvázigrupy a transverzálami jej Cayleyho tabuľky.

Fakt, že grupa $(\mathbb{Z}_2^n, \oplus)$ má skutočne úplné zobrazenie možno nahliadnuť z vety 5.17.

VETA 5.17. [**26**] *Nech G je Ábelovská grupa s prvkami $a_1, a_2, \ldots, a_N$ a nech L je jej Cayleyho tabuľka. Potom L obsahuje transverzálu práve vtedy, keď*

$$\prod_{i=1}^{N} a_i = e,$$

kde e predstavuje neutrálny prvok grupy G.

Môžeme teda zadefinovať operáciu $*$ tak, aby $f : S \mapsto \mathbb{Z}_2^n$ s predpisom $f(x) = x_b$ bola balansovaná a VPN na grupoide $(S, *)$. Operáciu možno zadefinovať nasledovne

$$i * j = \theta(j) \oplus j$$

pre všetky $i \in S$. Táto však z hľadiska kryptografie nie je vhodná. Ideálnejšie by bolo, aby $(S, *)$ tvorilo kvázigrupu. To možno docieliť tak, že nájdeme úplné zobrazenia $\theta_1, \theta_2, \ldots, \theta_n$, pre ktoré platí: $\theta_i(x) \neq \theta_j(x)$ pre ľubovoľné $i \neq j$ a $x \in S$. Ak sa na tieto úplné zobrazenia pozrieme cez transverzály zistíme, určujú rozklad Cayleyho tabuľky $(\mathbb{Z}_2^n, \oplus)$. Ako vyzerajú takéto úplné zobrazenia možno nahliadnuť z dôkazu vety 5.18, ktorá zároveň potvrdzuje, že $\theta_1, \theta_2, \ldots, \theta_n$ skutočne existujú.

VETA 5.18. [**13**] *Ak Cayleyho tabuľka L Ábelovskej grupy $(G, *)$ rádu N obsahuje transverzálu, potom L možno rozložiť do N disjunktných transverzál.*

Z vety 5.18 a jej dôkazu [**13**] plynie, že $\theta_2, \theta_3, \ldots, \theta_n$ sú v rozklade jednoznačne určené a majú tvar $\theta_i(x) = \theta(x) \oplus i_b$.

Definovaním operácie na grupoide S ako

$$i * j = \theta_i(j) \oplus j$$

dostávame $(S, *)$ ako kvázigrupu, na ktorej je funkcia f VPN.

POZNÁMKA 5.19. S využitím úplných zobrazení θ_i možno definovať aj ďalšie kvázigrupy, na ktorých je f VPN. Stačí, keď sa v Cayleyho tabuľke kvázigrupy ľubovoľne spermutujú riadky.

Z predchádzajúceho vyplýva, že na nájdenie funkcie $f : Q \mapsto \mathbb{Z}_2^n$ s plochou diferenčnou tabuľkou stačí nájsť transverzály Cayleyho tabuľky grupy $(\mathbb{Z}_2^n, \oplus)$.

5.2.1. Transverzály $\mathbb{Z}_{p^r}$. V tomto odseku si popíšeme ako nájsť transverzály štvorcov Cayleyho tabuliek grupy $(\mathbb{Z}_{p^r}, +)$, kde p^r je mocnina prvočísla p. Tento prípad zahŕňa aj transverzály Latinských štvorcov odvodených z aditívnej grupy $\mathbb{Z}_2^n$.

Začneme s konceptom ortogonálnych Latinských štvorcov.

DEFINÍCIA 5.20. [**13**] *Dva Latinské štvorce $L_1 = \{a_{ij}\}$,$L_2 = \{b_{ij}\}$ sú ortogonálne, ak sa každý usporiadaný pár symbolov (a_{ij}, b_{ij}) nachádza práve raz medzi všetkými pármi (a_{ij}, b_{ij}) pre $i, j \in I_n$.*

Ortogonálne štvorce majú úzku súvislosť s transverzálami. Predpokladajme, že máme ortogonálne štvorce L_1, L_2 a transverzálu štvorca L_1.

Potom z definície 5.20 je zrejmé, že bunky z L_2, zodpovedajúce transverzále v L_1 musia obsahovať navzájom rôzne symboly. Teda ak chceme nájsť transverzálu v štvorci L stačí, ak nájdeme k nemu ortogonálny štvorec L'. Potom už len stačí nájsť n buniek v L' (v každom riadku a stĺpci práve jednu), ktoré obsahujú rovnaký symbol a bunky s rovnakými súradnicami tvoria v L transverzálu.

PRÍKLAD 5.21. V tabuľke 5.21 možno vidieť ortogonálne štvorce L_1, L_2.

L_1				
	0	**1**	2	3
	1	0	3	**2**
	2	3	**0**	1
	3	2	1	0

L_2				
	3	**2**	1	0
	1	0	3	**2**
	0	1	**2**	3
	2	3	0	1

TABUĽKA 2. Ortogonálne štvorce

Zo zvýraznených štyroch buniek v štvorci L_2 sa nachádza každá bunka práve v jednom riadku a stĺpci a obsahujú rovnaký symbol 2. Teda zodpovedajúce bunky v L_1 tvoria transverzálu. Keďže L_1 tvorí Cayleyho tabuľku komutatívnej grupy $(\mathbb{Z}_2^2, \oplus)$, tak ďalšie transverzály sú v tvare $L(x, \theta(x) \oplus c)$ pre ľubovoľnú konštantu $c \in \mathbb{Z}_2^2$. Tieto transverzály sú ako sme už skôr povedali disjunktné.

Zostáva nám teda nájsť ortogonálne štvorce ku Cayleyho tabuľke grupy $\mathbb{Z}_p^r$.

Pomožeme si vetou z [**13**], ktorá dáva univerzálny návod na skoštruovanie množiny dokonca $p^r - 1$ navzájom ortogonálnych štvorcov.

VETA 5.22. [**13**] *Označme prvky konečného poľa F_{p^r} symbolmi $\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = x, \alpha_3 = x^3, \ldots, \alpha_{p^r-1} = x^{p^{r-2}}$, kde x označuje generátor multiplikatívnej grupy $F_{p^r}^*$ poľa. Platí $\alpha_i\alpha_j = \alpha_t$, kde $t = (i-1) + (j-1) + 1 = i + j - 1 \mod p^r - 1$ pre všetky nenulové i, j. Skonštruovať kompletnú množinu ortogonálnych štvorcov $L_1, L_2, \ldots, L_{p^r-1}$ možno nasledujúcou voľbou prvkov:*

(1) *prvky nultého riadku a nultého stĺpca štvorca L_1 sú v prirodzenom poradí, teda $L_1(i, 0) = \alpha_i, L_1(0, j) = \alpha_j$ pre $i, j \in \{0, 1, \ldots, p^r - 1\}$.*

(2) *prvky prvého riadku štvorca L_1 sa získajú podľa pravidla $L_1(1, j) = \alpha_1 + \alpha_j$.*

(3) *prvky zvyšných riadkov L_1 sa získajú podľa pravidla*

$$\begin{aligned} L_1(i+1, j+1) \quad &= 0 \quad pre \;\; L(i,j) = 0, \\ &= \alpha_{s+1} \quad pre \;\; L(i,j) = \alpha_s, 0 < s < p^r - 1 \\ &= \alpha_1 \quad pre \;\; L(i,j) = \alpha_{p^r-1} \end{aligned}$$

(4) *Zvyšné štvorce $L_2, \ldots, L_{p^r-1}$ majú s L_1 rovnaký prvý stĺpec a zvyšné sa cyklicky permutujú. Teda v L_2 je druhý stĺpec zhodný s tretím v L_1, tretí so štvrtým atď.*

Problémom uvedenej konštrukcie je, že z daných $p^r - 1$ štvorcov ani jeden nemusí tvoriť Cayleyho tabuľku grupy $\mathbb{Z}_p^r$. Avšak plynie z nej, že získané štvorce sú všetky izotópne s aditívnou grupou poľa F_{p_r} a tak možno použiť nasledujúcu vetu.

VETA 5.23. [**13**] *Ak sú Latinské štvorce L_1, L_2 ortogonálne, potom sú ortogonálne aj štvorce $L_1^{(\theta,\varphi,\psi)}, L_2^{(\theta,\varphi,\psi)}$.*

Majme navzájom ortogonálne štvorce $L_1, L_2, \ldots, L_{p^r-1}$. Nech L predstavuje Cayleyho tabuľku aditívnej grupy poľa F_{p^r}. Snažíme sa nájsť ortogonálne štvorce k L. S využitím vety 5.23

stačí nájsť izotopizmus δ z L_i na L. Jeho aplikáciou na všetky štvorce L_j dostávame množinu navzájom ortogonálnych štvorcov L_j^δ, pre $j \in I_{p^r-1}$. Jeden z nich už je daný L, konkrétne $L_i^\delta = L$.

Pri hľadaní ďalších štvorcov ortogonálnych k L_1 možno postupovať podobným spôsobom. Majme dva ortogonálne Latinské štvorce L_1, L_2. Predpokladajme, že chceme nájsť ďalšie L_i, ktoré sú ortogonálne k L_1. Môžeme znovu využiť vetu 5.23. Stačí, keď nájdeme autotopizmus δ štvorca L_1 a aplikujeme ho na L_2.

5.3. Záver

V predchádzajúcich sekciách sme ukázali ako možno skonštruovať perfektne nelineárnu funkciu $f : S \mapsto Z_2^n$ ($|S| = 2^n$) s úplne plochou diferenčnou tabuľkou. Túto funkciu charakterizuje Latinský štvorec L rádu 2^n, ktorý je zložený z disjunktných transverzál Cayleyho tabuľky grupy $(\mathbb{Z}_2^n, \oplus)$. Keďže funkcia f má ideálne kryptografické vlastnosti, má ich aj Latinský štvorec L. Tieto štvorce teda možno použiť pri konštrukcii návrhov kryptografických aplikácií. Tomu sa venujeme v nasledujúcej kapitole.

KAPITOLA 6

Generovanie podkľúčov s využitím Latinských štvorcov

V tejto kapitole popíšeme algoritmus na automatické generovanie podkľúčov (AGP) postavený na Latinských štvorcoch.

Algoritmus je možné využiť v blokových šifrách, ktoré sa skladajú z viacerých kôl. Spracovanie bloku dát v každom kole je prevedené jedinou funkciou. Táto je však parametrizovaná, pričom príslušný tajný parameter i-teho kola je tvorený i-tym podkľúčom. Podkľúče sa generujú pomocou AGP z jediného tajného parametra šifry - tajného kľúča.

Na AGP sa môžeme pozerať ako na zobrazenie κ, ktoré zobrazí kľúč na reťazec podkľúčov. Pre šifru s r kolami možno κ formálne zapísať

$$\kappa : K \rightarrow Q, \tag{16}$$

kde K tvorí kľúč a $Q = K^{(1)}||K^{(2)}||...||K^{(r)}$ je zreťazenie (symbol $||$) jednotlivých podkľúčov.

V skutočnosti musíme skúmať dve zreťazenia:

$$Q^{(e)} = K^{(e,1)}||K^{(e,2)}|| \ldots ||K^{(e,r)},$$

kde $e = \begin{cases} 0 \text{ - pre šifrovanie} \\ 1 \text{ - pre dešifrovanie} \end{cases}$. Pri E/D podobných šifrách (rovnako sa šifruje a dešifruje) samozrejme $Q^{(0)}$ a $Q^{(1)}$ spolu úzko súvisia.

6.1. Známe požiadavky na podkľúče

Keďže podkľúče (rovnako ako kľúč a AGP) určujú jednoznačne spôsob šifrovania je nutné, aby potencionálny útočník mal pri ich získavaní, čo najviac sťaženú úlohu. Túto situáciu sa snažia vystihnúť odporúčania z Crypto'96 [**33**], kde sa vyžaduje platnosť nasledujúcich princípov:

(1) Všetky bity $Q^{(e)}$ musia byť nezávislé a rovnomerne rozdelené.
(2) Všetky bity $Q^{(e)}$ musia byť štatisticky nezávislé od niekoľkých susedných bitov.
(3) Počet núl a jednotiek v $K^{(e,i)}$ musí byť približne rovnaký.
(4) Počet možných rôznych vygenerovaných zreťazení a kľúčov musí byť (v ideálnom prípade) rovnaký, t.j.

$$|K| \approx \left|Q^{(e)}\right| .$$

Všeobecný postup ako to overiť neexistuje. Cieľom je aspoň odhadnúť možnosť kolízie, t.j. či je možné z dvoch rôznych kľúčov (s tým istým AGP) vygenerovať tie isté podkľúče.

Ako upozornil už Biham [**4**] treba mať tiež na zreteli, že jednoduché AGP niekedy vykazujú závislosti medzi podkľúčmi a to sa dá využiť pri útoku na šifru. Nezávislosť bitov podkľúčov tiež zabezpečí odolnosť voči útokom, kedy je (sub)kľúč čiastočne známy.

6.1.1. Požiadavky kladené na návrh AGP. Pri dĺžke bloku n_b a počte kôl r potrebujeme $n_b(r+1)$ bitov, ak predpokladáme pre- a post-whitening. Pri návrhu musíme zvážiť, či sa generované podkľúče majú používať on-line, t.j. paralelne s rozvojom šifrového algoritmu, alebo je možné ich najprv vygenerovať v chránenej časti pamäte a potom využívať. V prvom prípade je výhodné (ale nie nevyhnutné), aby sa algoritmus AGP odvodil od samotného šifrového algoritmu. Uľahčuje to totiž taktovanie algoritmu. V druhom prípade musíme voliť kompromis medzi rýchlosťou a bezpečnosťou. Vzhľadom na požiadavku premenlivosti dĺžky kľúča je dobré, ak AGP má vlastnosť modularity t.j. je nezávislý na veľkosti bloku.

O zhrnutie požiadaviek sa pokúšalo viacero autorov. Napríklad Knudsen ([**32**] 1993)uvádza tieto požiadavky:

- Funkcia κ nesmie vykazovať kolízie a mala by byť jednocestná.To zabezpečuje, že nemožno vypočítať jej inverziu.

- Medzi všetkými bitmi podkľúčov a K musí byť minimálna závislosť. (Zlé príklady: DES, GOST, AES [**4**])
- Jednoduchá implementovateľnosť. Je vhodné, aby funkcia κ bola (čiastočne) totožná so šifrovacím algoritmom. A aby jej časovanie κ bolo totožné s kolami algoritmu.

6.1.2. Testovanie nezávislosti bitov generovaných algoritmom AGP. V praxi je možné testovanie nezávislosti jednotlivých bitov Q generovaných algoritmom AGP ako aj testovanie závislosti konkrétneho bitu od niekoľkých susedných bitov. Problémom pri testovaní je samozrejme malý rozsah náhodného výberu, ktorý ako sme už uviedli je $n_b(r+1)$. Pre $n_b = 128, r = 10$ to reprezentuje len 1408 bitov. Takže nie je možné použiť napríklad spektrálny test. Podrobnejšie sa tieto princípy premietnu v dvoch testoch uvedených nižšie.

6.1.2.1. *Testovanie nezávislosti susedných bitov.* Na štatistické testovanie nezávislosti susedných bitov podkľúčov použijeme známy postup s využitím kontingenčných tabuliek.

Z kľúča K vygenerujeme pomocou AGP $Q^{(e)}$ a skúmame i-ty a j-ty bit postupnosti. Sledujeme početnosti výskytu dvojíc 0 a 1 bez prekrytia:

$i \backslash j$	0	1	
0	n_{00}	n_{01}	$n_{0\cdot}$
1	n_{10}	n_{11}	$n_{1\cdot}$
	$n_{\cdot 0}$	$n_{\cdot 1}$	n

Pravdepodobnosti výskytu 0 na mieste i-teho a j-teho bitu sú približne:

$$P(i=0) \approx \frac{n_{0\cdot}}{n}$$

$$P(j=0) \approx \frac{n_{\cdot 0}}{n}$$

Pravdepodobnosti v tabuľke majú byť nezávislé. Preto pre $i, j = 0, 1$ má platiť:

$$\left(\frac{n_{i\cdot}}{n} \cdot \frac{n_{\cdot j}}{n} - \frac{n_{ij}}{n}\right) \to 0$$

Test s jedným stupňom voľnosti má tvar:

$$\chi_1{}^2 = \sum_{i\in\{0,1\}} \sum_{j\in\{0,1\}} \frac{\left(n_{ij} - \frac{n_{i\cdot}\cdot n_{\cdot j}}{n}\right)^2}{\frac{n_{i\cdot}\cdot n_{\cdot j}}{n}}$$

Ak pri zvolenej hladine významnosti α je $\chi^2 > \chi_1{}^2(\alpha)$, hypotézu zamietame, čiže AGP "nie je dobrý". Kritické hodnoty pre $\chi_1^2(\alpha)$ možno nájsť v [**1**] a sú nasledovné:

$\alpha(\%)$	$99,9$	$99,5$	$99,0$	$97,5$	$5,0$	$2,5$	$1,0$	$0,5$
$\chi_1^2(\alpha)$	$0,000$	$0,000$	$0,000$	$0,001$	$3,84$	$5,02$	$6,63$	$7,88$

6.1.2.2. *Testovanie nezávislosti konkrétneho bitu od susedných bitov.* Nezávislosť bitu od susedných bitov môžeme určiť pomocou korelačného koeficientu ρ. Vo všeobecnosti je ho možné určiť pre 2 rôzne náhodné premenné X, Y ako

$$\rho = \frac{cov(X,Y)}{\sqrt{var(X)\cdot var(Y)}} \in < -1, 1 > .$$

Pre ρ=0 hovoríme o nekorelovaných náhodných premenných. Pre normálne a alternatívne rozdelenie znamená ρ=0, že X, Y sú nezávislé. Naopak, pri $|\rho|$=1 sú X, Y lineárne závislé.

Ak X, Y sú náhodné vektory, môžeme zaviesť maticu **W**, ktorá vyzerá nasledovne:

$$\mathbf{W} = \begin{pmatrix} var(X) & cov(X,Y) \\ cov(Y,X) & var(Y) \end{pmatrix}$$

Ak determinant matice **W** označíme $|\mathbf{W}|$, môžeme určiť závislosť X, Y zo vzťahu:

$$\frac{|\mathbf{W}|}{var(X)\cdot var(Y)} = 1 - \rho^2 \qquad (17)$$

V prípade, že hodnota výrazu z rovnice (17) je 0, sú X, Y lineárne závislé; ak 1, sú X, Y nezávislé.

Ak teraz potrebujeme vyšetriť (ne)závislosť konkrétneho bitu od susedných bitov, definujeme maticu **V**, kde Y je n-bitový vektor pozostávajúci z náhodných premenných Y_i priradených jednotlivým bitom. Pre prvky **V** platí: $\mathbf{V} = (v_{ij})$, $v_{ij} = cov(Y_i, Y_j)$.

Bit, ktorého štatistickú nezávislosť sledujeme, reprezentujeme náhodnou premennou X. Platí $cov(X,Y) = cov(Y,X)^T$, kde $cov(X,Y)$ je vektor so zložkami $cov(X,Y_i)$. Podobne ako v prípade s jednoduchou náhodnou premennou Y sa použije matica $\mathbf{W}$ s rozmermi $(n+1) \times (n+1)$. Jej prvky sú:

$$\begin{array}{rcll} w_{11} & = & var(X), & \\ w_{1i} & = & cov(X, Y_{i-1}), & \text{pre } i = 2,3,...n+1; \\ w_{i1} & = & cov(Y_{i-1}, X), & \text{pre } i = 2,3,...n+1; \\ w_{ij} & = & v_{i-1,j-1}, & \text{pre } i = 2,3,...n+1, j = 2,3,...n+1. \end{array}$$

Vzorec pre výpočet výrazu ρ^2 možno nájsť v [**1**] a má tvar:

$$\rho^2 = \frac{cov(X,Y) \cdot \mathbf{V}^{-1} \cdot cov(Y,X)}{var(X)}.$$

6.2. Softvérový návrh

Tento odsek obsahuje podklady pre implementáciu novej metódy AGP postavenej na Latinských štvorcoch.

6.2.1. Návrh algoritmu. Algoritmus generovania bajtov pre podkľúče je znázornený na obr. 1.

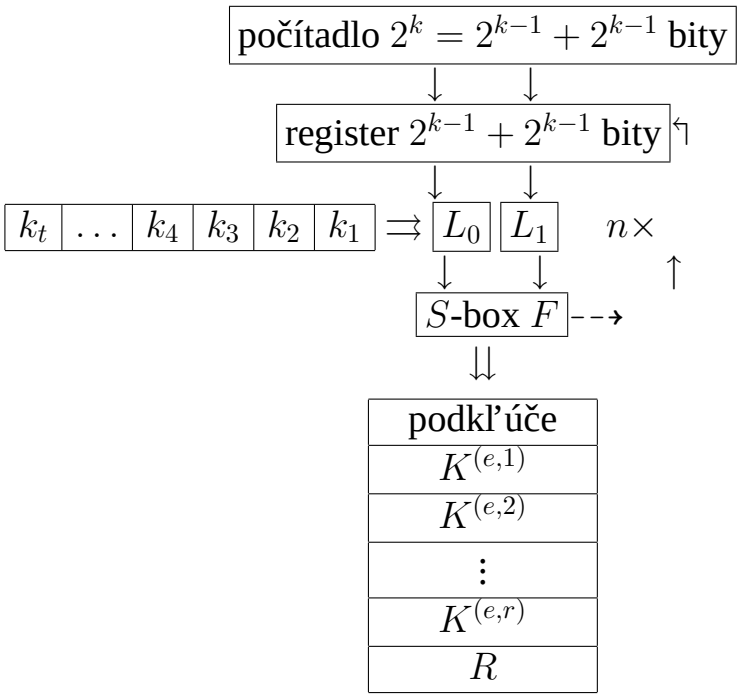
Hodnoty t sú pre rôzne dĺžky kľúčov a rozmery Latinských štvorcov $2^{2^{k-1}} \times 2^{2^{k-1}}$ nasledovné:

kľúč	t	$k=3$
128	2^{8-k}	$t = 32$
192	$2^{8-k} + 2^{7-k}$	$t = 48$
256	2^{9-k}	$t = 64$

Súčasťou generovania sú dva Latinské štvorce L_0, L_1 nad množinou symbolov $\{0, 1, \ldots, 2^{2^{k-1}} - 1\}$. Postup generovania reťazca subkľúčov $Q^{(e)}$ je nasledovný:

(1) Posledný kľúč $K^{(r+1)}$ je totožný s $K \oplus \bigoplus_{i=1}^{r} K^{(i)}$, ktorý sa paralelne počíta v osobitnom registri R. Ten je na začiatku naplnený kľúčom K.

(2) Do registra vstúpi posledných $2^k = 2^{k-1} + 2^{k-1}$ bitov z kľúča K, t.j binárna hodnota $k_t || k_{t-1}$.



OBRÁZOK 1. Algoritmus na generovanie podkľúčov.

(3) Prvé 2^{k-1} bity k_1 kľúča K sa vynásobia s pomocou L_0 s 2^{k-1} ľavými bitmi registra. Podobne, druhé 2^{k-1} bity k_2 kľúča K sa vynásobia s pomocou L_1 s 2^{k-1} pravými bitmi registra.
(4) Spojený výsledok (2^k bitov) vstupuje do bijektívneho S-boxu $F : \mathbb{Z}_2^k \to \mathbb{Z}_2^k$.
(5) Výstup je opäť vložený do registra a postup sa opakuje n- krát (napr. pokiaľ sa nepoužijú všetky bity kľúča, t.j. $n = t/2$).
(6) Výsledok, t.j. 2^k bitov, je prvých 2^k bitov prvého podkľúča.
(7) Následne do registra vstúpi binárna hodnota $k_t||k_{t-1}$ inkrementovaná o hodnotu registra a postup sa opakuje. Zvyšovanie hodnoty počítadla ako aj inkrementácia $k_t||k_{t-1} + h$ sú počítané $\mod 2^k$.
(8) Ak $t = 32$, potom je výsledkom reťazec s 11×128 bitmi. To znamená, že

$$Q^{(e)} = K^{(e,1)}||K^{(e,2)}|| \ldots ||K^{(e,10)}||R.$$

(9) Ak je $t = 48$ alebo $t = 64$, potom po vygenerovaní 10 subkľúčov sa kľúč K zamení s aktuálnou hodnotou registra R a algoritmus pokračuje ďalej. Výsledkom je reťazec

$$Q^{(e)} = K^{(e,1)}||K^{(e,2)}||\dots||K^{(e,12)}||R$$

resp.

$$Q^{(e)} = K^{(e,1)}||K^{(e,2)}||\dots||K^{(e,14)}||R.$$

6.3. Analýza návrhu algoritmu

V tejto časti sa venujeme posúdeniu základných stavebných prvkov návrhu algoritmu. Sú to S-box, voľba Latinského štvorca ako aj zdôvodnenie nezávislosti generovaných bitov podkľúčov.

6.3.1. Nezávislosť bitov podkľúčov. Návrh algoritmu AGP priamo zabezpečuje vzájomnú nezávislosť všetkých bitov podkľúčov za predpokladu, že kľúče K sú generované náhodne. Je tomu tak preto, lebo výstupy z L_0, L_1 sú nezávislé a náhodné.

6.3.2. Voľba Latinského štvorca. Ako sme ukázali v sekcii (5.2) Latinské štvorce s dobrými kryptografickými vlastnosťami možno skonštruovať pomocou transverzál Cayleyho tabuľky grupy $(\mathbb{Z}_2^n, \oplus)$.

6.3.3. Voľba S-boxu. Voľba S-boxu úzko súvisí s voľbou Latinských štvorcov. Aby sme mohli zvoliť pre dané štvorce dobrý S-box potrebujeme analyzovať ekvivalentnú schému, kde nahradíme štvorce L_0, L_1 rádu $2^{2^{k-1}}$ a S-box F jediným štvorcom L rádu 2^{2^k}. Tomuto sa venujeme obšírnejšie v sekcii (6.4).

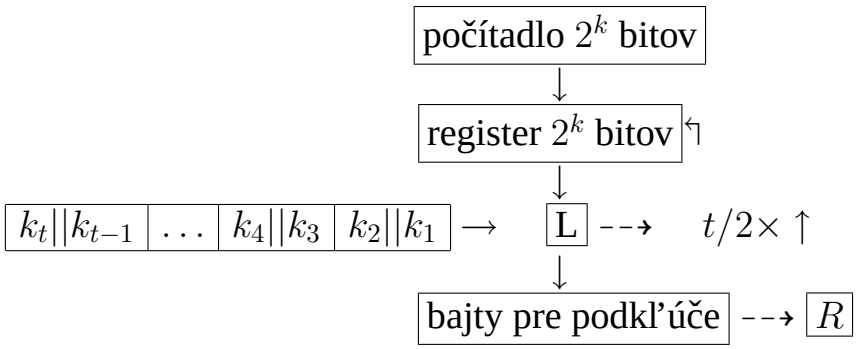
6.3.4. Pomerná rýchlosť implementácie. Vychádzajúc z hodnotenia použitého Mayom a kol.[**58**], kde kritériom je pomer počet kôl AGP/počet kôl AES na jeden blok, sú tieto hodnoty pre náš návrh nasledovné:

dĺžka kľúča	pomer AES	pomer May	náš návrh
128	1,60	3,30	25,6
192	2,04	3,25	48,0
256	2,24	3,21	73,1

Ako vidno, hodnoty v nami predloženom návrhu sú rádovo vyššie ako hodnoty AGP použitom v AES resp. Mayovým návrhom. Praktická realizácia nášho AGP by preto mala byť výrazne rýchlejšia. Ďalším pozitívom nášho návrhu je fakt, že sa v ňom fakticky nič nepočíta a hodnoty sa čítajú priamo z uložených tabuliek. To v praxi predstavuje výraznú časovú úsporu a ešte viac urýchľuje celkový beh AGP.

6.4. Analýza ekvivalentnej schémy

V tejto sekcii budeme analyzovať ekvivalentnú schému. Štvorce L_0, L_1 a S-box F nahradíme jediným štvorcom L nad množinou symbolov $\{0, 1, \ldots, 2^{2^k} - 1\}$. Grafické znázornenie takejto schémy možno vidieť na obrázku (2).



OBRÁZOK 2. Ekvivalentný algoritmus na generovanie podkľúčov

Analyzovať pôvodný návrh z obrázku (1) teda znamená analyzovať kryptografické vlastnosti štvorca L.

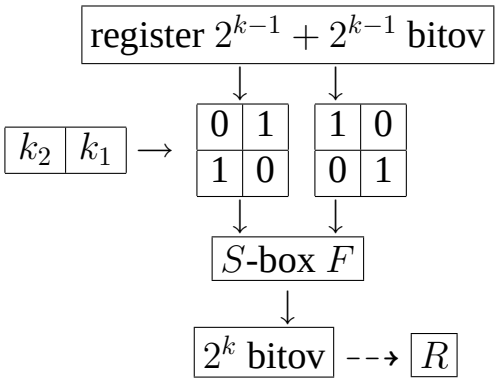
6.4.1. Vlastnosti a tvar štvorca L. Začnime malým príkladom.

PRÍKLAD 6.1. Predpokladajme, že máme schému z obrázku (3), kde $k = 1$ a kľúč je zložený len z dvoch častí k_1, k_2. Nech

S-box zapísaný ako permutácia F má tvar

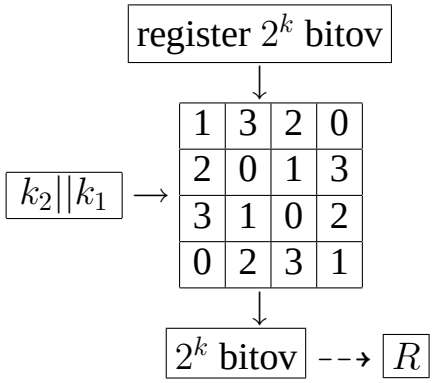
$$F = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}.$$

Potom schému z obrázku (3) je možné nahradiť ekvivalentnou



OBRÁZOK 3. Algoritmus na generovanie podkľúčov.

schémou z obrázku (4). Tu berieme ako vstup do štvorca L spojenie $k_2||k_1$ a k bitov registra.



OBRÁZOK 4. Algoritmus na generovanie podkľúčov.

Z príkladu vidíme, že štvorec L je v našom prípade opäť Latinský štvorec. Ako ukazuje nasledujúca veta, toto platí pre ľubovoľné L_0, L_1 a bijektívny S-box F.

VETA 6.2. *Štvorec L v obrázku 2 je Latinský štvorec.*

DÔKAZ. Vezmime si výstup z S-boxu F. Ten má pre prvky k_2, k_1 kľúča K a r_1, r_2 počítadla (registra) tvar:

$$F(L_0(k_1, r_1)||L_1(k_2, r_2)).$$

Platí teda $L(k_2||k_1, r_1||r_2) = F(L_0(k_1, r_1)||L_1(k_2, r_2))$. Aby sme ukázali, že L je Latinský štvorec stačí ak ukážeme, že platí $L(k_2||k_1, r_1||r_2) \neq L(k_2'||k_1', r_1||r_2)$ pre ľubovoľné $k_2||k_1 \neq k_2'||k_1'$ a $L(k_2||k_1, r_1||r_2) \neq L(k_2||k_1, r_1'||r_2')$ pre ľubovoľné $r_1||r_2 \neq r_1'||r_2'$. Ako sme už na začiatku povedali platí rovnosť

$$L(k_2'||k_1', r_1||r_2) = F(L_0(k_1', r_1)||L_1(k_2', r_2)).$$

Keďže L_0, L_1 sú Latinské štvorce, môžeme pre $k_2||k_1 \neq k_2'||k_1'$ okamžite písať

$$L_0(k_1, r_1)||L_1(k_2, r_2) \neq L_0(k_1', r_1)||L_1(k_2', r_2).$$

Aplikáciou bijektívneho S-boxu F na obe strany je nerovnosť zachovaná, a teda L má v riadku všetky symboly rôzne. Obdobne sa dokáže, že štvorec L má všetky symboly v stĺpci rôzne, a teda sa jedná o Latinský štvorec. □

Pýtame sa, ako vyzerá daný štvorec. Začnime s tým, ako vyzerá štvorec L', ktorým možno nahradiť štvorce L_0, L_1. Kvôli väčšej názornosti si pomôžeme "produktom" matíc, ktorý popisuje nasledovná definícia.

DEFINÍCIA 6.3. *Nech A je matica rozmerov $m \times m$ a B je matica rozmerov $n \times n$. Symbolom $A \odot B$ budeme označovať $nm \times nm$ maticu v blokovom tvare:*

$$A \odot B = \begin{array}{c|c|c} m.a_{00}.E_n + B & \dots & m.a_{0m-1}.E_n + B \\ \hline m.a_{10}.E_n + B & \dots & m.a_{1m-1}.E_n + B \\ \hline \vdots & & \vdots \\ \hline m.a_{n-10}.E_n + B & \dots & m.a_{n-1m-1}.E_n + B \end{array} \quad (18)$$

Tu chápeme pod symbolom E_n maticu rozmerov $n \times n$, v ktorej $e_{ij} = 1$ pre všetky $i, j \in I_n$.

Využitím definície 6.3 možno pre prvok $(ni_1 + i_2, nj_1 + j_2)$ matice $A \odot B$ písať

$$(A \odot B)(ni_1 + i_2, nj_1 + j_2) = mA(i_1, j_1) + B(i_2, j_2).$$

Vezmime si teraz štvorec L', ktorý substituuje štvorce L_0, L_1. Pre ten platí nasledovné

$$L'(k_2||k_1, r_1||r_2) = L_0(k_1, r_1)||L_1(k_2, r_2), \quad (19)$$

čo sa dá zapísať aj ako (tu je $m = n = 2^{2^{k-1}}$)

$$L'(2^{2^{k-1}}k_2 + k_1, 2^{2^{k-1}}r_1 + r_2) = 2^{2^{k-1}}L_0(\mathbf{k_1}, r_1) + L_1(\mathbf{k_2}, r_2). \tag{20}$$

To pripomína produkt štvorcov L_0, L_1, ktorý má v našom prípade vyjadrenie:

$$(L_0 \odot L_1)(2^{2^{k-1}}k_2 + k_1, 2^{2^{k-1}}r_1 + r_2) = 2^{2^{k-1}}L_0(\mathbf{k_2}, r_1) + L_1(\mathbf{k_1}, r_2). \tag{21}$$

Rozdiel medzi vzťahmi (20) a (21) je v premenných k_1, k_2 (zvýraznené boldom), ktoré sú navzájom "prehodené". To sa dá interpretovať tak, že vo štvorci L' sa nachádza príslušné číslo $2^{2^{k-1}}L_0(k_1, r_1) + L_1(k_2, r_2)$ v $2^{2^{k-1}}k_2 + k_1$-tom riadku, kdežto pri $\odot$-produkte je to v $2^{2^{k-1}}k_1 + k_2$-tom riadku. Teda štvorec L' vznikne z produktu $L_0 \odot L_1$ tak, že sa vymenia riadky $i||j$ a $j||i$ pre každé i, j. Aplikáciou S-boxu F na prvky tohoto štvorca nakoniec dostaneme finálny L, kde sa každý symbol s nahradí symbolom $F(s)$.

6.4.2. Kritéria pre štvorec L. Tu si ukážeme dopad kritérií zo sekcie (6.1) na štvorec L.

6.4.2.1. *Jednocestnosť návrhu.* Analyzujme schému z obrázka (2). Predpokladajme, že

(1) oponent zachytí hodnotu a;
(2) oponent zachytí hodnotu

$$y = k_n * (k_{n-1} * (\ldots (k_2 * (k_1 * a))) \ldots));$$

(3) pozná latinský štvorec L;

a položme si otázku, či je schopný vypočítať skutočnú hodnotu kľúča K, t.j. $k_n||k_{n-1}|| \ldots ||k_2||k_1$.

(1) Je zrejmé, že rovnica $k_1 * a = y$ má práve jedno riešenie.
(2) Rovnica $k_2 * (k_1 * a) = y$ má práve toľko riešení, koľko prvkov má Q, t.j. n. Ak zvolíme k_1 ľubovoľne, potom je už k_2 určené jednoznačne. Pretože prvky $k_1 a$ sú pre rôzne k_1 rôzne, budú rôzne aj riešenia k_2.
(3) Rovnica $k_3 * (k_2 * (k_1 * a)) = y$ má zrejme n^2 riešení. Tieto riešenia sú všetky rôzne (ako trojice), lebo ak $k_2 * (k_1 * a)$ sú rôzne, potom sú rôzne aj hodnoty k_3.

(4) Preto rovnica

$$k_t * (k_{t-1} * (\ldots (k_2 * (k_1 * a))) \ldots)) = y \qquad (22)$$

má n^{t-1} riešení.

Tieto všetky hodnoty reprezentujú v tomto prípade ekvivalentné kľúče. Všeobecne, nech $(Q, *)$ je konečná kvázigrupa, $|Q| = n$. Vezmime si ľavé translácie $L_k : Q \to Q$ kvázigrupy. Tieto tvoria permutácie množiny prvkov kvázigrupy a ich použitím možno rovnicu (22) prepísať na

$$L_{k_t} \circ L_{k_{t-1}} \ldots L_{k_2} \circ L_{k_1}(a) = y. \qquad (23)$$

Označme G najmenšiu grupu generovanú permutáciami L_1,$L_2, \ldots, L_n$. Keďže $G \subseteq S_n$, tak pre mohutnosť G máme $|G| \leq |S_n| = n!$ a naviac $|G||n!$. Riešenia rovnice (22) môžeme hľadať takto: zvolíme ľubovoľné $L_u \in G$ s vlastnosťou $L_u(a) = y$. Následne musíme nájsť všetky rozklady translácie $L_u \in G$ dĺžky t vytvorené len z prvkov $L_1, L_2, \ldots, L_n$. Z toho plynie, že docieliť jednocesnosť zobrazenia κ možno voľbou takej kvázigrupy, pre ktorú je obtiažne nájsť rozklady prvkov G do t translácií kvázigrupy. Z toho titulu teda kvázigrupa $(Q, *)$ nemôže byť grupou a samozrejme mohutnosť G by mala byť čo najväčšia. Ak by sme mali k dispozícii niekoľko zachytených párov (a, y), potom hľadáme také riešenie, ktoré vyhovuje všetkým rovniciam. V krajnom prípade, ak poznáme všetky páry (a, y), (poznáme permutáciu $p \in G$) potom nájdenie kľúča (ekvivalentných kľúčov) zodpovedá nájdeniu translácií $L_{k_n}, L_{k_{n-1}} \ldots L_{k_2}, L_{k_1}$, že platí

$$L_{k_n} \circ L_{k_{n-1}} \ldots L_{k_2} \circ L_{k_1} = p. \qquad (24)$$

Postup riešenia pre viaceré páry môžeme ilustrovať na nasledujúcom príklade.

PRÍKLAD 6.4. Uvažujme latinský štvorec daný tabuľkou

$(Q,*)$	1	2	3	4	5
1	2	5	4	3	1
2	4	2	1	5	3
3	5	1	3	2	4
4	1	3	2	4	5
5	3	4	5	1	2

a máme riešiť sústavu rovníc

$$\begin{aligned} k_2 * (k_1 * 1) &= 3 \\ k_2 * (k_1 * 2) &= 5 \end{aligned}$$

Prvá rovnica má zrejme 5 riešení, lebo pre dané u má rovnica $k_2 * u = 3$ práve jedno riešenie. Podobne druhá rovnica. My hľadáme spoločné riešenie pre obe rovnice. Všetky možné hodnoty translácií k_1 v bode 1 resp. 2 sa nachádzajú v stĺpcoch "1" a "2" latinského štvorca. Aby sme získali hodnoty $k_2 * (k_1 * a)$ pre rôzne k_2, musíme tieto stĺpce prenásobiť postupne s 1,2,3,4,5. V prvej schéme hľadáme hodnotu pravej strany prvej rovnice, t.j. 3 a v druhej 5.

k_2	$k_1 * 1 =$	2	4	5	1	3
1		5	**3**	1	2	4
2		2	5	3	4	1
3		1	2	4	5	3
4		**3**	4	5	1	2
5		4	1	2	**3**	5

k_2	$k_1 * 2 =$	5	2	1	3	4
1		1	**5**	2	4	3
2		3	2	4	1	5
3		4	1	5	3	2
4		**5**	3	1	2	4
5		2	4	3	**5**	1

Riešenia našej sústavy sú tie, kde sú hodnoty 3 a 5 na rovnakých pozíciách v oboch tabuľkách. Uvedené riešenia teda sú $(k_1, k_2) = (1, 2), (4, 1), (5, 4)$.

Z riešenia príkladu je zrejmé, že maximálny počet rovníc, ktoré sú "nezávislé", je totožný s počtom prvkov kvázigrupy. Ďalej, keby sme mali dlhší reťazec v sústave rovníc, t.j. napr.

$$\begin{aligned} k_3 * (k_2 * (k_1 * 1)) &= 3 \\ k_3 * (k_2 * (k_1 * 2)) &= 5, \end{aligned}$$

potom by sme museli každý riadok v posledných dvoch tabuľkách prenásobiť všetkými hodnotami $k_3 = 1, 2, ..., 5$ a opäť

hľadať miesta, kde sa na rovnakých pozíciách vyskytujú pravé strany 3 a 5. Ako možno vidieť, určiť kľúč zo zachytených párov (a, y) je vo všeobecnosti veľmi ťažká úloha. Teda možno prehlásiť, že uvedený návrh spĺňa pre vhodnú kvázigrupu podmienku jednocestnosti zobrazenia κ.

6.4.2.2. *Bezkolíznosť*. Nech L_Q označuje množinu ľavých translácií kvázigrupy $(Q, .)$. Z predchádzajúcich úvah plynie (s ohľadom na bezkolíznosť), že pre mohutnosti množín permutácií tvaru $(L_Q)^i$ pre $i \in \{1, \ldots, t\}$, by mal platiť vzťah

$$|(L_Q)^i| \approx |L_Q|^i.$$

Teda, že veľkosť množiny zreťazení podkľúčov je približne zhodná s množinou kľúčov. To možno zapísať nasledovne: $|Q^e| \approx (L_Q)^t$.

6.4.3. Evivalentnosť kľúčov. Teraz budeme analyzovať množiny $(L_Q)^i$, keďže tie majú priamy dopad na voľbu S-boxu.

Ako sme mohli vidieť skôr pracujeme so štvorcom L, ktorý vznikne z produktu $L_0 \odot L_1$, tak, že prehodíme riadky a následne nahradíme symboly s za $F(s)$.

Pomocou translácií kvázigrúp sa dá uvedené zapísať ako $L_Q = L_{Q'} \circ F$, kde Q', je kvázigrupa, ktorej Cayleyho tabuľka predstavuje štvorec L'.

6.4.3.1. *Množiny L_Q^i a ich vlastnosti*. Majme kvázigrupu Q rádu m a L_Q množinu jej ľavých translácií. Vzhľadom na to, že pri L_Q^i ide o násobenie komplexov, možno pre mohutnosti množín L_Q^i okamžite písať $|L_Q^i|.|Q| \geq |L_Q^{i+1}| \geq |L_Q^i|$. Rovnako je z neho zrejmé, že ich mohutnosť je ohraničená hodnotou $m!$.

Máme teda reťazec množín L_Q^i, pre ktorý platí

$$|L_Q^1| \leq |L_Q^2| \leq \ldots \leq |L_Q^{\mathbf{i}}| = |L_Q^{\mathbf{i}+1}| = \ldots. \qquad (25)$$

Index $\mathbf{i}$ predstavuje najmenší z indexov i, pre ktoré platí:

$$|L_Q^i| = |L_Q^{i+1}| = \ldots.$$

Zaujíma nás, ako závisia mohutnosti $|L_Q^i|$ od množiny L_Q. Pomôžeme si nasledujúcou vetou.

VETA 6.5. *Nech A predstavuje ľubovoľnú neprázdnu množinu permutácií z S_m. Pre reťazec množín $A_1, A_2, A_3, \ldots$, kde $A_i = A^i$ platí, že maximálna mohutnosť prvkov tohoto reťazca delí rád grupy $|S_m| = m!$.*

DÔKAZ. Nech $\mathbf{i}$ predstavuje najmenší index, od ktorého sú mohutnosti prvkov reťazca rovnaké. Platí teda $|A_{i+1}| = |A_{\mathbf{i}}|$ pre všetky $i \geq \mathbf{i}$. Vezmime si ľubovoľný prvok $a \in A$. Keďže platia vzťahy $|aA_{\mathbf{i}}| = |AA_{\mathbf{i}}|$ a $aA_{\mathbf{i}} \subseteq AA_{\mathbf{i}} = A_{\mathbf{i+1}}$, tak množinu $A_{\mathbf{i}+1}$ možno zapísať ako:

$$A_{\mathbf{i}+1} = aA_{\mathbf{i}}.$$

Pre každé $l > 1$ sa teda dá $A_{\mathbf{i}+l}$ zapísať nasledovne:

$$A_{\mathbf{i}+l} = a^l A_{\mathbf{i}}.$$

Najprv ukážme, že pre ľubovoľné $i, j \geq \mathbf{i}$ platí pre $A_i \cap A_j \neq \emptyset$ rovnosť $A_i = A_j$. Nech teda existuje b také, že $b \in A_i \cap A_j$. Potom ale platí $bA = AA_i \cap AA_j$ a $|bA| = |AA_i| = |AA_j|$. Z toho máme $bA = AA_i = AA_j$, čo možno tiež zapísať ako $bA = aA_i = aA_j$. Preto $A_i = A_j$.

Vezmime si teraz množinu permutácií $G = [A]$, kde pod symbolom $[A]$ máme na mysli obal množiny A. Ako je dobre známe, táto množina tvorí grupu, ktorej rád delí $m!$ [**7**].

Dá sa ľahko ukázať, že pre grupu G platí

$$G = \bigcup_{i=\mathbf{i}}^{\infty} A_i.$$

Ako sme ukázali vyššie, množiny A_i pre $i \geq \mathbf{i}$ sú buď identické alebo disjunktné, a teda tvoria rozklad množiny G. Z toho dôvodu $|A_{\mathbf{i}}| \mid |G|$ a tým je veta dokázaná. □

Priamou aplikáciou vety 6.5 na množinu L_Q možno pre $|L_Q^{\mathbf{i}}|$ odvodiť

$$|L_Q^{\mathbf{i}}| \mid m!.$$

To samozrejme neodpovedá na základnú otázku, aké sú mohutnosti množín L_Q^i.

Poskytuje to však určitú predstavu o maximálnom množstve neekvivalentných kľúčov. Akokoľvek, veta 6.5 spolu s jej dôkazom nám poskytuje aparát na skúmanie ekvivalentných kľúčov. To je, ako už bolo spomínané skôr, veľmi náročná úloha.

Preto, aby sme vedeli aspoň približne odhadnúť hodnoty $\mathbf{i}$ a $|L_Q^{\mathbf{i}}|$ je potrebné vykonať niekoľko testov pre malé rozmery štvorca L. Vytvorili sme preto testovací program, ktorý analyzuje AGP určené schémou z obrázku (2) z hľadiska priestoru ekvivalentných kľúčov.

Analyzovali sme mohutnosti množín pre rády štvorcov 6 a 8. Štvorce boli vytvorené z Cayleyho tabuliek grúp $Z_2 \times Z_3$ a Z_2^3, na ktoré bola následne aplikovaná každá permutácia (S-box F) symbolov z S_6, S_8. V nasledujúcej tabuľke možno vidieť prehľad počtov Latinských štvorcov(izotópnych s $Z_2 \times Z_3$ prostredníctvom len symbolovej permutácie) v závislosti od hodnôt $|L_Q^i|$.

i / $\lvert L_Q^i \rvert$	6	18	24	36	108	120	372	528	552	612	648	714	720
$i = 5$	12	24	36	36	36	72	72	72	72	144	144		
$i = 6$	12	24	36	36		108	72	72				72	432
$i = 7$	12	24	36	36		108							504
$i = 8$	12	24	36	36		108							504

TABUĽKA 1. Počet štvorcov rádu 6 s danou hodnotou $|L_Q^i|$

Interpretácia tabuľky (1) je nasledovná: v prvom riadku sú uvedené hodnoty $|L_Q^i|$ získané úplným prehľadávaním. Zo všetkých možných 720 (=6!) latinských štvorcov odvodených z jedného štvorca s použitím riadkovej permutácie sa s rastúcou dĺžkou kľúča $i = 5, 6, 7, 8$ zvyšujú počty neekvivalentných kľúčov.

Pri obdobnom testovaní štvorca Z_2^3 sme zistili, že najvhodnejšie S-boxy F sú tie, pre ktoré je minimum rádov permutácií z $L_Q = F \circ L_{Z_2^3}$ najväčsie.

V nasledujúcej tabuľke možno vidieť mohutnosti množín L_Q^i pre rôzny výber permutácií F.

skupina	$\lvert L_Q^2\rvert$	$\lvert L_Q^3\rvert$	$\lvert L_Q^4\rvert$	$\lvert L_Q^5\rvert$	$\lvert L_Q^6\rvert$	$\lvert L_Q^7\rvert$	$\lvert L_Q^8\rvert$	$\lvert L_Q^9\rvert$
1.	8	8	8	8	8	8	8	8
2.	32	128	512	2048	6144	13824	19584	20160
3.	64	512	1152	1344	1344	1344	1344	1344
4.	64	456	2304	7344	13952	19776	20160	20160
5.	64	512	4096	13824	18816	20160	20160	20160

TABUĽKA 2. Mohutnosti množín pre rôzne voľby F.

Z uvedených experimentálnych údajov vyplýva, že hodnota $|L_Q^i|$ zrejme závisí len od rádu jednotlivých permutácií. Samozrejme nie v prípade, že L_Q tvorí grupu.

Konkrétne pre skupinu 5, kde mohutnosti množín $|L_Q^i|$ rastú najrýchlejšie sú rády jednotlivých permutácií nasledovné: $4, 5, 6, 6, 7, 7, 15, 15$. Možno teda vysloviť hypotézu, že po minimum m z rádov permutácií množiny L_Q narastá mohutnosť množiny neekvivalentných kľúčov ideálne. Teda $|L_Q^i| = n^i$ pre $i < m$.

6.4.4. Rovnomernosť rozdelenia hodnôt. Analyzujme teraz množiny L_Q^i s ohľadom na početnosť výskytu jednotlivých symbolov $\{0, 1, \ldots, m-1\}$ na jednotlivých pozíciach permutácií z L_Q^i.

Nech $L_Q^i(s, j)$ označuje početnosť symbolu s na j-tej pozícii (súradnici) v permutáciach z L_Q^i. Teda

$$L_Q^i(s, j) = |\{p \in L_Q^i : p(j) = s\}|.$$

Pre množinu L_Q "tvorenú riadkami" štvorca L možno pre $i = 1$ a ľubovoľné $s \in \{0, 1, \ldots, m-1\}$ okamžite písať $L_Q^1(s, j) = 1$. Hoci odvodiť hodnotu $|L_Q^i|$ je vo všeobecnosti zrejme obtiažne, určiť relatívne zastúpenie jednotlivých symbolov v L_Q^i je všeobecne možné.

Pomôžeme si nasledujúcou vetou.

VETA 6.6. *Nech množina $A = \{a_1, a_2, \ldots, a_m\}$ je tvorená m permutáciami z S_m, pre ktoré platí $a_i(s) \neq a_j(s)$ pre ľubovoľné $i \neq j$ a ľubovoľný symbol $s \in \{0, 1, \ldots, m-1\}$. Potom*

pre ľubovoľné $l \in \mathbb{N}$ *a* $s_1, s_2, p_1, p_2 \in \{0, 1, \ldots, m-1\}$ *platí*

$$A^l(s_1, p_1) = A^l(s_2, p_2).$$

DÔKAZ. Vetu dokážeme matematickou indukciou. Pre každé s, p jasne platí $A(s, p) = 1$. Dokážme platnosť indukčného kroku. Chceme dokázať implikáciu

$$A^l(s_1, p_1) = A^l(s_2, p_2) \Rightarrow A^{l+1}(s_1, p_1) = A^{l+1}(s_2, p_2).$$

Vezmime ľubovoľnú permutáciu $a \in A$. Tá zobrazuje symbol s na $a(s)$ a preto platí

$$aA^l(a(s), p) = A^l(s, p).$$

Toto zrejme platí pre ľubovoľné s, p. Pre $A^{l+1}(a(s), p)$ môžeme teda písať

$$\begin{aligned} A^{l+1}(s,p) = \sum_{i=1}^{m} a_i A^l(s,p) &= \sum_{i=1}^{m} a_i A^l(a_i(a_i^{-1}(s), p) \\ &= \sum_{i=1}^{m} A^l(a_i^{-1}(s), p). \end{aligned}$$

Využijúc predpoklad $A^l(s_1, p_1) = A^l(s_2, p_2)$ pre ľubovoľné s_1, s_2, p_1, p_2 môžeme písať $A^{l+1}(s, p) = \sum_{i=1}^{m} A^l(s, p)$, čo dokazuje vetu.

□

Veta potvrdzuje rovnomernosť výskytu jednotlivých symbolov v podkľúčoch a teda návrh spĺňa kritérium pre rovnomerné rozdelenie bitov (sekcia 6.1).

6.5. Experimenty

V tomto odseku popíšeme realizované experimenty, ktorými sa snažíme potvrdiť korektnosť nového AGP z hľadiska požiadaviek uvedených v odseku (6.1).

Testovali sme schému pre $k = 3$, so 128 bitovým kľúčom. Štvorce L_0, L_1 boli skonštruované pomocou transverzál Z_2^4 z kapitoly (5). Ich tvar možno vidieť v tabuľkách 3,4.

Ako S-box sme volili S-box z AES s posunom 111. Pre Latinský štvorec L rádu 256 ekvivalentnej schémy sme zistili,

0	10	7	13	11	1	12	6	4	14	3	9	15	5	8	2
1	11	6	12	10	0	13	7	5	15	2	8	14	4	9	3
2	8	5	15	9	3	14	4	6	12	1	11	13	7	10	0
3	9	4	14	8	2	15	5	7	13	0	10	12	6	11	1
4	14	3	9	15	5	8	2	0	10	7	13	11	1	12	6
5	15	2	8	14	4	9	3	1	11	6	12	10	0	13	7
6	12	1	11	13	7	10	0	2	8	5	15	9	3	14	4
7	13	0	10	12	6	11	1	3	9	4	14	8	2	15	5
8	2	15	5	3	9	4	14	12	6	11	1	7	13	0	10
9	3	14	4	2	8	5	15	13	7	10	0	6	12	1	11
10	0	13	7	1	11	6	12	14	4	9	3	5	15	2	8
11	1	12	6	0	10	7	13	15	5	8	2	4	14	3	9
12	6	11	1	7	13	0	10	8	2	15	5	3	9	4	14
13	7	10	0	6	12	1	11	9	3	14	4	2	8	5	15
14	4	9	3	5	15	2	8	10	0	13	7	1	11	6	12
15	5	8	2	4	14	3	9	11	1	12	6	0	10	7	13

TABUL'KA 3. Štvorec L_0.

0	7	1	6	8	15	9	14	3	4	2	5	11	12	10	13
1	6	0	7	9	14	8	15	2	5	3	4	10	13	11	12
2	5	3	4	10	13	11	12	1	6	0	7	9	14	8	15
3	4	2	5	11	12	10	13	0	7	1	6	8	15	9	14
4	3	5	2	12	11	13	10	7	0	6	1	15	8	14	9
5	2	4	3	13	10	12	11	6	1	7	0	14	9	15	8
6	1	7	0	14	9	15	8	5	2	4	3	13	10	12	11
7	0	6	1	15	8	14	9	4	3	5	2	12	11	13	10
8	15	9	14	0	7	1	6	11	12	10	13	3	4	2	5
9	14	8	15	1	6	0	7	10	13	11	12	2	5	3	4
10	13	11	12	2	5	3	4	9	14	8	15	1	6	0	7
11	12	10	13	3	4	2	5	8	15	9	14	0	7	1	6
12	11	13	10	4	3	5	2	15	8	14	9	7	0	6	1
13	10	12	11	5	2	4	3	14	9	15	8	6	1	7	0
14	9	15	8	6	1	7	0	13	10	12	11	5	2	4	3
15	8	14	9	7	0	6	1	12	11	13	10	4	3	5	2

TABUL'KA 4. Štvorec L_1.

že minimálna hodnota rádu odvodených permutácií z L_Q bola 250. To znamená, že počet ekvivalentných kľúčov, by mal byť pre $n < 250$ nulový. My máme v návrhu $n = t/2 = 16$ a teda môžeme prehlásiť, že návrh je z hľadiska ekvivalentných kľúčov vhodný. Pre testovanie nezávislosi bitov podkľúčov sme spustili 1000 krát AGP s náhodne voleným 128-bitovým kľúčom. Výsledky testov možno nájsť v nasledovnej sekcii.

6.5.1. Testovanie nezávislosti bitov. Prehľad tabuliek početnosti n_{00} pre prvých 12 bitov možno vidieť v tabuľke (5).

i/j	0	1	2	3	4	5	6	7	8	9	10	11
0	464	251	246	233	223	250	235	220	212	226	228	218
1	251	520	270	246	263	276	255	262	233	252	253	239
2	246	270	502	247	247	257	255	250	244	242	246	250
3	233	246	247	494	246	264	234	247	238	248	256	252
4	223	263	247	246	495	250	253	242	229	237	245	250
5	250	276	257	264	250	516	259	247	233	252	251	253
6	235	255	255	234	253	259	493	244	239	237	243	236
7	220	262	250	247	242	247	244	483	216	229	239	220
8	212	233	244	238	229	233	239	216	475	238	239	220
9	226	252	242	248	237	252	237	229	238	475	246	231
10	228	253	246	256	245	251	243	239	239	246	499	249
11	218	239	250	252	250	253	236	220	220	231	249	491

TABUĽKA 5. Početnosť párov nula-nula pre prvých 12 bitov.

bit	0	1	2	3	4	5	6	7	8	9	10	11
n_0	464	520	502	494	495	516	493	483	475	475	499	491

TABUĽKA 6. Početnosť výskytu núl pre prvých 12 bitov.

Prehľad hodnôt ${\chi_1}^2$ testu s jedným stupňom voľnosti pre prvých 12 bitov možno vidieť v tabuľke (7).

Pri zvolenej hladine významnosti $\alpha = 5\%$ sme zistili, že nadkritickú hodnotu 4 χ^2 testu dosahuje 25067 párov bitov podkľúčov. Ak sme brali do úvahy hladinu významnosti $\alpha = 1\%$, tak počet "silnejšie" závislých párov klesol na 8307. Tu má kritická hodnota veľkosť 7. Maximálna hodnota, ktorá presahuje hladinu významnosti, bola v našich experimentoch 27.

i/j	0	1	2	3	4	5	6	7	8	9	10	11
0	-	1	2	0	0	1	0	0	1	0	0	1
1	1	-	1	1	0	0	0	1	3	0	0	4
2	2	1	-	0	0	0	0	0	0	0	0	0
3	0	1	0	-	0	1	1	1	0	2	1	1
4	0	0	0	0	-	0	1	0	0	0	0	0
5	1	0	0	1	0	-	0	0	2	0	0	0
6	0	0	0	1	1	0	-	0	0	0	0	0
7	0	1	0	1	0	0	0	-	2	0	0	4
8	1	3	0	0	0	2	0	2	-	2	0	2
9	0	0	0	2	0	0	0	0	2	-	1	0
10	0	0	0	1	0	0	0	0	0	1	-	0
11	1	4	0	1	0	0	0	4	2	0	0	-

TABUL'KA 7. Hodnoty χ_1^2 pre prvých 12 bitov.

Ďalej sme analyzovali závislosti jednotlivých bitov podkľúčov od ich susedných 30 bitov pomocou korelačného koeficientu. Pre všetky bity podkľúčov sa hodnoty ρ pohybovali medzi hodnotami $\rho_{min} = 0.00948, \rho_{max} = 0.23811$. Tabuľka 8 udáva prehľad hodnôt korelačného koeficientu každého z prvých 12 bitov a ich 30 susedov.

bit	0	1	2	3	4	5
ρ	0.1660	0.1583	0.1543	0.1721	0.1711	0.1801
bit	6	7	8	9	10	11
ρ	0.1391	0.1614	0.1526	0.1523	0.1933	0.1469

TABUL'KA 8. Hodnoty ρ pre prvých 12 bitov.

6.5.2. Vyhodnotenie experimentov. V prípade nezávislosti bitov bol nový návrh AGP v celku úspešný. Z celkovo milióna možných párov bitov podľúčov presiahlo hladinu významnosti χ^2 testu len okolo 1.2% párov. Z toho silnejšie závislých bolo len 0.4% všetkých párov. Predpokladáme, že pri lepšom výbere Latinských štvorcov by mohli testom nezávislosti vyhovieť aj zvyšné bity. Navyše, jeden bit podkľúča bol z hľadiska

korelačného koeficientu dostatočne lineárne nezávislý od susedných 30 bitov. Počet ekvivalentných kľúčov sme sa snažili odhadnúť na zmenšenom modeli. Výsledky pre menšie štvorce naznačujú, že ich počet v plnom modeli môže dosiahnuť nulovú hodnotu a teda z tohoto pohľadu možno návrh AGP klasifikovať ako veľmi dobrý.

KAPITOLA 7

Záver

V kapitole 4 sme sa venovali návrhu nového algoritmu na nájdenie izotopizmov dvoch kvázigrúp.

Algoritmus vychádzal z konceptu konjugovaných množín permutácií a reprezentácii kvázigrúp prostredníctvom translácií. Tento prístup umožnil v sekcii 4.7.1 zlepšiť známe odhady maximálneho počtu autotopizmov kvázigrúp. Ako vedľajší produkt uvedenej konštrukcie možno klasifikovať algoritmus, ktorý nájde optimálnym spôsobom prvky, ktoré konjugujú n prvkové množiny permutácií. V sekcii 4.7.2 sme sa venovali autotopizmom grúp z hľadiska konštrukcie algoritmu. Na základe dokázaných tvrdení pri konštrukcii algoritmu sme tu potvrdili platnosť vzorca z [**3**] pre počet autotopizmov grúp.

V sekcii 4.6 sme porovnali známy Millerov a náš algoritmus z hľadiska zložitosti. Ukázali sme, že majú rovnakú zložitosť. Ako prínos nášho prístupu však možno považovať odvodenie novej nutnej podmienky izotopie, ktorá dosiahla v reálnych testoch pozoruhodné výsledky.

Tie boli prevedené v prostredí malých kvázigrúp rádov 6,7, 8, kde len veľmi mizivé percento neizotópnych kvázigrúp prešlo testom nutnej podmienky. Z uvedených výsledkov možno predpokladať podobnú úspešnosť aj pre väčšie rády, avšak toto by malo byť ešte podložené ďalšími testami. Tu vidíme ďalší priestor pre možný výskum, ktorého výsledkom by bol pravdepodobnostný algoritmus vyhodnocujúci izotópnosť dvoch kvázigrúp so zložitosťou $O(n^3)$.

V kapitole 5 sme sa zaoberali konštrukciou Latinských štvorcov vhodných pre kryptografické aplikácie. Popísali sme tu jednoduchú konštrukciu založenú na transverzálach štvorcov

grupy Z_2^n. Jej použitím sme skonštruovali Latinské štvorce rádu 16, ktoré boli neskôr použité pri novom návrhu algoritmu na generovanie podkľúčov blokových šifier.

Spomínanému návrhu AGP a jeho analýze sa venuje kapitola 6. AGP postavené rýdzo na Latinských štvorcoch sme analyzovali z hľadiska počtu neekvivaletných kľúčov, nezávislosti jednotlivých bitov podkľúčov a možnosti potencionálneho útočníka dopočítať kľúč zo znalosti niektorých podkľúčov. Návrh sme implementovali pre 128 bitový blokový šifrátor s počtom podkľúčov 11. Výsledky experimentov naznačujú, že navrhnuté AGP spĺňa požadované kritériá a teda Latinské štvorce možno úspešne použiť ako základ pre AGP.

Literatúra

[1] Anděl J.: Matematická statistika., SNTL/Alfa, Praha1978.

[2] Belousov, V.D.: Osnovi teorii kvazigrup i lup., (1967) Nauka, Moskva

[3] V.D. Belousov: Elements of quasigroup theory: a special course, Kishinev State University, Kishinev, 1981, (in Russian).

[4] Biham E.: New Types of Cryptanalytic Attacks using Related Keys. EUROCRYPT 93, LNCS 765, 1993, 398-409.

[5] Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J.: A Message Authentication Code Based on Latin Squares, Australian Conference on Information Security and Privacy (ACISP '97), Springer-Verlag, 1997, LNCS 1270, pp. 194-203.

[6] Bóna, M. Combinatorics of permutations. SIGACT News 39, 4 (Nov. 2008), 21-25.

[7] Birkhoff G., Mac Lane S.: Prehľad modernej algebry, Alfa, 1979(in Slovak)

[8] Birkhoff G., Mac Lane S.: Algebra, Alfa, Bratislava, 1973, 2. edition: 1978.(in Slovak)

[9] Carmichael R. D.: Introduction to the Theory of Groups of Finite Order Boston, Ginn and Co., 1937. 447 pp.

[10] `http://cs.anu.edu.au/ bdm/data/`

[11] Colbourn C. J., Dinitz J.H. , Mutually orthogonal latin squares: A brief survey of constructions, J. Stat. Plann. Infer. 95 (2001) 9–48.

[12] Colbourn C. J., Dinitz J.H. (eds.), The CRC Handbook of Combinatorial Designs. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996. 753 pp.

[13] Dénes, J., Keedwell, A.D.: Latin Squares and Their Applications, Academic Press, NY, 1974.

[14] J. Denes and A. Keedwell, Latin squares: New developments in the theory and applications, Annals of Discrete Mathematics, vol. 46, North Holland Publishing Company, 1991.

[15] Dvorský, J., Ochodková, E., Snášel, V.: Hash Function Based on Quasigroups ("Hashovací funkce založená na kvazigrupách"), *Proc. of Mikulášská kryptobesídka*, Praha, pp. 27-36, 2001 (in Czech).

[16] Dvorský, J., Ochodková, E., Snášel, V.: Hash Functions Based on Large Quasigroups, *Proc. of Velikonoční kryptologie*, Brno, pp. 1-8, 2002.

[17] Dixon J. D.,Mortimer B.: Permutation Groups. Number 163 in Graduate Texts in Mathematics. Springer-Verlag, 1996

[18] ECRYPT Project - European Network of Excellence in Cryptology, `http://www.ecrypt.eu.org`

[19] ECRYPT Stream Cipher Project, `http://www.ecrypt.eu.org/stream/` .

[20] E.N. Gilbert, Latin squares which contain no repeated digrams, SIAM Rev. 7 (1965)

[21] GOST, Gosudarstvennyi Standard 28147-89, Cryptographic Protection for Data Processing Systems," Government Committee of the USSR for Standards, 1989.

[22] Gligoroski, D., Markovski, S., Kocarev, L., Gusev, M.: Edon80, eSTREAM, ECRYPT Stream Cipher Project, Report 2005/007, 2005, `http://www.ecrypt.eu.org/stream`.

[23] Gligoroski D.,Odegard R. S.,Mihova M. Knapskog S. J.,Kocarev L., Drápal A. :Cryptographic Hash Function EDON-R http://people.item.ntnu.no/̃danilog/Hash/Edon-R/Supporting_Documentation/EdonRDocumentation.pdf
[24] Gligoroski, D., Markovski, S., Bakeva, V.: On Infinite Class of Strongly Collision Resistant Hash Functions "EDON-F" with Variable Length of Output, Proceedings of 1st International Conference On Mathematics and Informatics for Industry, April 2003, Thessaloniki, Greece.
[25] Grošek, O., Satko, L., Nemoga, K.: Ideal Difference Tables from an Algebraic Point of View, Cryptology and Information Security, Proceedings of VI RECSI, Teneriffe, Spain, September 2000, ammendment to CRIPTOLOGÍA y SEGURIDAD de la INFORMACIÓN, editors - P.Caballero-Gil and C.Hernández-Goya, RA-MA, Madrid, 2000, pp. 453-454.
[26] Grošek, O., Satko,L., Nemoga,K.: Generalized perfectly nonlinear functions. Tatra Mountains Math.Publ. 20 (2000), pp.121-131.
[27] Heys H.M. :A Tutorial on Linear and Differential Cryptanalysis http://www.engr.mun.ca/h̃oward/PAPERS/ldc_tutorial.pdf
[28] KALTOFEN, E.: Polynomial factorization: a success story. Proc. of the 2003 int. symp. on Symbolic and algebraic computation, 2003, s. 3 – 4.
[29] Koscielny, C.: A method of constructing quasigroup-based stream-ciphers. Appl. Math. and Comp. Sci. 6 (1996) 109–121.
[30] Koscielny C. and Mullen G.L. (1999): A quasigroup-based public-key cryptosystem.—Int. J. Appl. Math. Comp. Sci., Vol. 9, No. 4, pp. 955–963.
[31] A. G Kurosh: The theory of groups. Vol 1 Chelsea Pub. Co, 1960, 580pp
[32] L. Knudsen: Practically Secure Feistel Ciphers. 1st FSE, LNCS 809, 1993, 211-221.
[33] J. Kelsey, B. Schneier, D. Wagner: Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and TRIPLE-DES. CRYPTO 96, LNCS 1109, 1996, 237-251.
[34] Lai X., Massey J. L., A Proposal for a New Block Encryption Standard, EUROCRYPT 1990, pp389–404
[35] Laywine C., Mullen G. Discrete Mathematics Using Latin Squares Wiley, 1998
[36] Markovski, S., Gligoroski, D., Andova, S.: Using Quasigroups for One–One Secure Encoding, Proceedings of LIRA '97 – Novi Sad Yugoslavia.
[37] Markovski, S., Gligoroski, D., Bakeva, V.: Quasigroups and Hash Functions, Proceedings of the 6th International Conference on Discrete Mathematics and Applications, Bansko, Bulgaria, South-West University, Blagoevgrad, Bulgaria.
[38] Markovski, S., Gligoroski, D., Kocarev, L.: Unbiased Random Sequences from Quasigroup String Transformations, Proceedings of Fast Software Encryption 2005, LNCS 3557, Springer-Verlag, 2005, pp. 163-180.
[39] Markovski, S., Gligoroski, D., Stojcevska,B.: Secure two way on-line communication by using quasigroups enciphering with almost public key,Novi Sad J.Math. 30, No.2,2000,43-49
[40] Mckay B.D., Meynert A., Myrvold W., Small Latin squares, quasigroups and loops, J. Combin. Designs,2007,98–119
[41] McKay, B.D., Rogoyski, E.:Latin squares of order 10. Electronic J. Comb. 2 (1995)
[42] McKay B. D., Wanless I.M., On the number of Latin squares, Ann. Combin., 9 (2005) 335-344.
[43] Miller G. L. :On the nlog n isomorphism technique, Proc. 10th ACM Symp Thy. Conp. (1978), 51-58.
[44] NESSIE Project, http://www.cryptonessie.org.
[45] NIST: AES Initiative, http://www.nist.gov/aes
[46] H. W. Norton, The 7 x 7 squares, Ann. Eugenics, 9 (1939) 269–307.

[47] Nyberg K.: Perfect nonlinear s-boxes. Advances in Cryptology - EUROCRYPT'91, LNCS, vol. 547, Springer-Verlag, 1991

[48] Ochodková, E., Snášel, V.: Using Quasigroups for Secure Encoding of File System, Proceedings of the International Scientific NATO PfP/PWP Conference "Security and Information Protection 2001", May 9–11, 2001, Brno, Czech Republic, pp.175–181.

[49] PLAISTED, D. A.: Some polynomial and integer divisibility problems are NPhard. SIAM J. Comput. 7, 1978, s. 458 – 464.

[50] Robinson, Derek J. S. An Introduction to Abstract Algebra Berlin, New York (Walter de Gruyter) 2003

[51] Sade, A. Autotopies des quasigroupes et des systémes associatifs. Arch. Math.(Brno) 4 (1968),1-23. MR 42(1971)

[52] Shcherbacov V. On some known possible applications of quasigroups in cryptology. `www.karlin.mff.cuni.cz/ drapal/krypto.pdf`

[53] Satko, L., Grošek, O.: Extremal Generalized S-Boxes, Computing and Informatics, Vol. 22(2003), No.1, pp. 85-99.

[54] SÝS, M.: Isotopy Classes of Latin Squares. In: Journal of Electrical Engineering. - ISSN 1335- 3632. - Vol. 58, No. 7/s (2007), p. 97-99. (in English)

[55] Sýs, M.: Algoritmus na hľadanie množiny izotopov medzi Latinskými štvorcami. In: ITAT 2008: Informačné Technológie - Aplikácie a Teória : Zborník príspevkov prezentovaných na pracovnom seminári ITAT, Hrebienok, September 2008. S. 99-104

[56] Spielman, D. A. Faster isomorphism testing of strongly regular graphs. In Proceedings of the Twenty-Eighth Annual ACM Symposium on theory of Computing (Philadelphia, Pennsylvania, United States, May 22 - 24, 1996). STOC '96. ACM, New York, NY, 576-584.

[57] Miller's private communication with Tarjan.

[58] L. May, M. Henricksen, W. Millan, G. Carter, E. Dawson: Strengthening the Key Schedule of the AES. ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, Springer-Verlag, Berlin, 2002, pp. 226-240.

[59] VOJVODA, M., SÝS, M., JÓKAY, M.: A Note on Algebraic Properties of Quasigroups in Edon80. In: SASC 2007. The State of the Art of Stream Ciphers: Workshop. Bochum, Germany, 31.1.-1.2.2007. - Bochum: ECRYPT Network of Excelence in Cryptology, 2007. - p. 307-315. (in English)