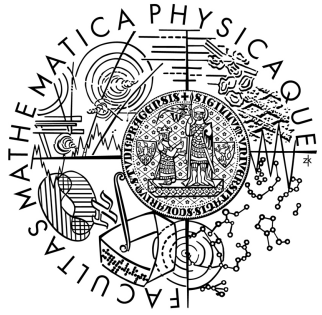
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Jana Kučerová

Řešení soustav diferenčních rovnic pro sčítání a booleovské operace

Katedra algebry

Vedoucí diplomové práce: Doc. RNDr. Jiří Tůma, DrSc.
Studijní program: Matematika
Studijní obor: Matematické metody informační bezpečnosti

2008

Na tomto místě bych ráda poděkovala vedoucímu mojí diplomové práce panu Doc. RNDr. Jiřímu Tůmovi, DrSc. za jeho cenné rady a připomínky a obětavou pomoc při psaní této práce.

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

V Praze dne 6. 8. 2008 Jana Kučerová

Obsah

Název práce: Řešení soustav diferenčních rovnic pro sčítání a booleovské operace
Autor: Jana Kučerová
Katedra (ústav): Katedra algebry
Vedoucí diplomové práce: Doc. RNDr. Jiří Tůma,DrSc.
e-mail vedoucího: tuma@karlin.mff.cuni.cz

Abstrakt: Předložená práce se věnuje řešení soustav diferenčních rovnic typu $(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma$, kde neznámé x, y i parametry α, β, γ jsou prvky stejné množiny X a $+$, $\oplus$ jsou grupové operace na množině X. V kapitole 2 zavedeme pojem *grupový pár*, popíšeme některé vlastnosti a vzájemné vztahy různých grupových párů. Kapitola 3 se zabývá řešením soustav diferenčních rovnic, kterým je věnována práce [1]. V kapitole 4 zadefinujeme grupový pár se speciální vzájemnou polohou příslušných grup, zavedeme pojem *přechodová funkce*, která popisuje vzájemný vztah operací $+$ a $\oplus$, a poté se zaměříme na řešení soustav diferenčních rovnic v tomto grupovém páru.

Klíčová slova: diferenční rovnice, grupový pár, přechodová funkce

Title: Solving systems of differential equations for addition and Boolean operations
Author: Jana Kučerová
Department: Department of Algebra
Supervisor: Doc. RNDr. Jiří Tůma,DrSc.
Supervisor's e-mail address: tuma@karlin.mff.cuni.cz

Abstract: The main topic of the present work is solving systems of differential equations of the type $(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma$, where both unknowns x, y and parameters α, β, γ are members of a set X, and $+$ and $\oplus$ are group operations on the set X. In chapter 2, we establish the term *group pair*, describe some properties and relationships between different group pairs. In chapter 3, we deal with solving systems of differential equations of addition, which is discussed in paper [1]. In chapter 4, we define a group pair, the groups of which are of special alignment, introduce the term *transition function* which describes alignment of the operations $+$ and $\oplus$, and then focus on solving systems of differential equations in such group pair.

Keywords: differential equation, group pair, transition function

Kapitola 1

Úvod

Paul a Preneel studovali řešení soustav rovnic typu

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma,$$

kde parametry α, β, γ i neznámé x, y jsou prvky množiny $\mathbf{2}^n$ a kde $+$ je operace sčítání modulo 2^n a $\oplus$ je operace xor. Nalezli algoritmus, který v případě řešitelnosti této soustavy najde jedno její řešení s polynomiální časovou složitostí.

Cílem této práce je zobecnit výsledky publikované v článku Paula a Preneela na obecnější grupy. Ukazuje se, že i u obecnějších abelovských grup se speciální vzájemnou polohou je použitelný mírně upravený algoritmus Paula a Preneela.

V této práci nejprve zadefinujeme pojem *grupový pár* a některé speciální typy grupových párů. Dále popíšeme různé vlastnosti grupových párů a některé vzájemné vztahy mezi grupovými páry. Poté se zaměříme na řešení soustav diferenčních rovnic v tzv. *standardním abelovském* grupovém páru, kterým se ve své práci zabývali Paul a Preneel. V poslední kapitole zobecníme algoritmus uvedený v článku [1] na algoritmus řešící soustavy diferenčních rovnic v tzv. *hustých abelovských* grupových párech. Tento zobecněný algoritmus však není obecně polynomiální. Proto na závěr zformulujeme podmínky na některé vlastnosti grupového páru, při jejichž splnění už zobecněný algoritmus bude polynomiální.

Kapitola 2

Grupové páry

Označení 2.1. Pro $n \in \mathbb{N}$ označme

$$\mathbf{2}^n = \{(a_{n-1}, \ldots, a_0) |\ a_j \in \{0,1\}, j = 0, \ldots, n-1\}.$$

Na množině $\mathbf{2}^n$ budeme uvažovat dvě grupy

$$C_2^n = (\mathbf{2}^n, \oplus), \text{ kde } \oplus \text{ značí operaci bitový xor,}$$

$$C_{2^n} = (\mathbf{2}^n, +), \text{ kde } + \text{ značí operaci sčítání modulo } 2^n.$$

Definice 2.2. Dvojici grup (G, H) na stejné množině X nazýváme *grupovým párem* na množině X.

Jsou-li grupy G a H abelovské, nazýváme pár (G, H) *abelovským grupovým párem.*

Binární grupový pár je dvojice grup (G, H) na množině X mohutnosti 2^n taková, že G je izomorfní s C_2^n a H je izomorfní s C_{2^n}.

Dvojici grup (C_2^n, C_{2^n}) nazýváme *standardním grupovým párem* na množině $\mathbf{2}^n$.

2.1 Podgrupy a rozkladové třídy

Poznámka 2.3. Grupa C_{2^n} je cyklická. Jedním z jejích možných generátorů je prvek $(0, \ldots, 0, 1)$. Jejími podgrupami jsou právě všechny grupy

$$D_{2^i} = \{(a_{n-1}, \ldots, a_0)\} \subseteq \mathbf{2}^n$$

takové, že $a_j = 0$ pro $j = 0, \ldots, i-1$, kde $i = 0, \ldots, n$. Zřejmě $\{0\} = D_{2^n} \subset D_{2^{n-1}} \subset \ldots \subset D_{2^1} \subset D_{2^0} = \mathbf{2}^n$.

Pro všechna $i = 0, \ldots, n$ jsou podgrupy D_{2^i} grupy C_{2^n} kanonicky[1] izomorfní s grupami $C_{2^{n-i}}$.

Všimněme si také, že každá podgrupa D_{2^i} grupy C_{2^n} je uzavřená rovněž na operaci $\oplus$, proto podmnožina D_{2^i} s operací $\oplus$ je také podgrupou C_2^n.

Tvrzení 2.4. *Dva prvky $x = (x_{n-1}, \ldots, x_0), y = (y_{n-1}, \ldots, y_0) \in \mathbf{2}^n$ jsou ekvivalentní modulo D_{2^i} v grupě C_{2^n}, právě když jsou ekvivalentní modulo D_{2^i} v grupě C_2^n. Jinými slovy, $x - y \in D_{2^i}$, právě když $x \oplus y \in D_{2^i}$.*

Důkaz. Nejprve ukážeme platnost následující ekvivalence

$$x - y \in D_{2^i} \Leftrightarrow (x_k = y_k \text{ pro } k = 0, \ldots, i-1). \tag{2.1}$$

Je-li $x - y \in D_{2^i}$, pak $x - y = ((x-y)_{n-1}, \ldots, (x-y)_i, 0, \ldots, 0)$. Protože $(x - y) + y = x$, je $x_k = y_k$ pro $k = 0, \ldots, i-1$. Je-li naopak $x_k = y_k$ pro $k = 0, \ldots, i-1$, je $x-y = ((x-y)_{n-1}, \ldots, (x-y)_i, 0, \ldots, 0) \in D_{2^i}$.

Nyní dokážeme tvrzení. Jsou-li prvky $x, y \in \mathbf{2}^n$ ekvivalentní modulo D_{2^i} v C_{2^n}, znamená to, že $x - y \in D_{2^i}$. Tedy $x_k = y_k$ pro $k = 0, \ldots, i-1$, a tedy $x \oplus y \in D_{2^i}$.

Předpokládejme naopak, že x a y jsou ekvivalentní modulo D_{2^i} v C_2^n, neboli že se shodují jejich hodnoty na indexech $0, \ldots, i-1$. Pak ale podle (2.1) je $x - y \in D_{2^i}$. □

Tvrzení 2.4 má řadu důsledků: Každá rozkladová třída C_{2^n}/D_{2^i} je rozkladovou třídou C_2^n/D_{2^i} a naopak. Jejich faktorové grupy jsou na stejné množině rozkladových tříd. Proto můžeme mluvit o rovnosti rozkladových tříd i faktorových grup.

V následujících kapitolách budeme hovořit o *řešení modulo podgrupa*. Nyní tento termín objasníme. Mějme algebru $A = (X, +, \oplus)$ a kongruenci π algebry A. Buďte $t(x_1, \ldots, x_k, \alpha_1, \ldots, \alpha_l)$ a $u(y_1, \ldots, y_p, \beta_1, \ldots, \beta_q)$ termy v algebře A s proměnnými $x_1, \ldots, x_k, y_1, \ldots, y_p$ a konstantami $\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_q$. Symbolem $[\alpha]_\pi$ označujeme rozkladovou třídu A/π, jejímž prvkem je prvek $\alpha \in X$. Termy $t(x_1, \ldots, x_k, [\alpha_1]_\pi, \ldots, [\alpha_l]_\pi)$ a $u(y_1, \ldots, y_p, [\beta_1]_\pi, \ldots, [\beta_q]_\pi)$ jsou termy v A/π. Řekneme, že prvky $a_1, \ldots, a_k, b_1, \ldots, b_p$ jsou řešením rovnice $t(x_1, \ldots, x_k, \alpha_1, \ldots, \alpha_l) = u(y_1, \ldots, y_p, \beta_1, \ldots, \beta_q) \pmod{\pi}$, právě když $t([a_1]_\pi, \ldots, [a_k]_\pi, [\alpha_1]_\pi, \ldots, [\alpha_l]_\pi) = u([b_1]_\pi, \ldots, [b_p]_\pi, [\beta_1]_\pi, \ldots, [\beta_q]_\pi)$ v A/π.

Rozklad na podgrupy je kongruence. Proto, budeme-li mluvit o řešení modulo podgrupa, budeme tím myslet řešení modulo příslušná kongruence.

[1] Kanonickým izomorfismem zde myslíme bijekci $g : D_{2^i} \to C_{2^{n-i}}$, která prvku $x = (x_{n-1}, \ldots, x_i, 0 \ldots, 0) \in D_{2^i}$ přiřadí prvek $(x_{n-1}, \ldots, x_i) \in C_{2^{n-i}}$

2.2 Přirozený systém reprezentantů

Někdy je výhodnější pracovat místo rozkladových tříd se systémy jejich reprezentantů. Z tvrzení 2.4 plyne, že systémy reprezentantů rozkladových tříd C_{2^n}/D_{2^i} se shodují se systémy reprezentantů rozkladových tříd C_2^n/D_{2^i}. Budeme pracovat s konkrétním systémem reprezentatů, který nazveme *přirozeným.*

Přirozeným reprezentantem prvku $x = (x_{n-1}, \ldots, x_0) \in \mathbf{2}^n$ v rozkladové třídě C_{2^n}/D_{2^i}, kde $i = 1, \ldots, n$, je prvek

$$r_i(x) = (0, \ldots, 0, x_{i-1}, \ldots, x_0) \in \mathbf{2}^n.$$

Protože každá rozkladová třída C_{2^n}/D_{2^i} je také rozkladovou třídou C_2^n/D_{2^i}, hovoříme o *společném systému přirozených reprezentantů* rozkladových tříd standardního grupového páru (C_2^n, C_{2^n}). Tento systém reprezentantů značíme

$$\mathcal{R}(C_{2^n}/D_{2^i}).$$

Pro každé $i = 1, \ldots, n$ lze každý prvek $x \in \mathbf{2}^n$ jednoznačně zapsat jako

$$x = r_i(x) + s_i(x),$$

kde $r_i(x) \in \mathcal{R}(C_{2^n}/D_{2^i})$ a $s_i(x) \in D_{2^i}$.

Řekneme, že dva prvky $x, y \in \mathbf{2}^n$ jsou si rovny modulo podgrupa D_{2^i}, právě když leží ve stejné rozkladové třídě C_{2^n}/D_{2^i}, tedy právě když se rovnají jejich přirozené reprezentanty $r_i(x) = r_i(y)$.

2.3 Izomorfismus grupových párů

Definice 2.5. Říkáme, že grupový pár (G_1, H_1) na konečné množině X_1 je *izomorfní* s grupovým párem (G_2, H_2) na množině X_2, pokud existuje bijekce $h : X_1 \to X_2$ taková, že h je izomorfismus $G_1 \to G_2$ a zároveň izomorfismus $H_1 \to H_2$.

Poznámka 2.6. Každou grupu G izomorfní s C_2^n lze považovat za aditivní grupu aritmetického vektorového prostoru dimenze n nad dvouprvkovým tělesem $\{0, 1\}$ s (jediným možným způsobem definovanou) operací násobení prvky z tělesa:

$$0x = (0, \ldots, 0) \in \mathbf{2}^n,$$

$$1x = x$$

pro každé $x \in G$. Kdykoliv budeme mluvit o bázi G, budeme tím myslet bázi příslušného vektorového prostoru.

Věta 2.7. *Binární grupový pár (G, H) na množině X mohutnosti 2^n je izomorfní se standardním grupovým párem (C_2^n, C_{2^n}) na $\mathbf{2}^n$, právě když každá podgrupa grupy H je uzavřená také na operaci grupy G.*

Důkaz. Operaci grupy G označíme $\oplus$ a operaci grupy H označíme $+$.

Předpokládejme, že každá podgrupa grupy H je uzavřená na operaci $\oplus$. Zvolme libovolný izomorfismus $h : H \to C_{2^n}$. Chceme ukázat, že h je také izomorfismem grup G a C_2^n. K tomu stačí ukázat, že existuje báze grupy G, která se pomocí h zobrazí na bázi grupy C_2^n.

V grupě H zavedeme následující označení:

$$t \cdot x = \underbrace{x + \cdots + x}_{t-\text{krát}}, \quad x \in H, t \in \mathbb{N}.$$

Uvažme bázi

$$\begin{aligned} e_0 &= (0, 0, \ldots, 0, 0, 1), \\ e_1 &= (0, 0, \ldots, 0, 1, 0), \\ e_2 &= (0, 0, \ldots, 1, 0, 0), \\ &\vdots \\ e_{n-1} &= (1, 0, \ldots, 0, 0, 0) \end{aligned}$$

grupy C_2^n. V grupě H existuje prvek x_0 takový, že $h : x_0 \mapsto e_0$. Protože h je izomorfizmus, je také

$$\begin{aligned} h : \quad 2 \cdot x_0 &\mapsto e_1, \\ 4 \cdot x_0 &\mapsto e_2, \\ &\vdots \\ 2^{n-1} \cdot x_0 &\mapsto e_{n-1}. \end{aligned}$$

Ukážeme, že množina $x_0, 2 \cdot x_0, \ldots, 2^{n-1} \cdot x_0$ je báze grupy G. Protože tato množina má n prvků, stačí ukázat její lineární nezávislost, tedy že pro každé $k = 0, \ldots, n-2$ platí, že prvek $2^k \cdot x_0$ neleží v lineárním obalu prvků $2^{k+1} \cdot x_0, \ldots, 2^{n-1} \cdot x_0$. To je ekvivalentní tomu, že prvek $2^k \cdot x_0$ neleží v podgrupě grupy G generované prvky $2^{k+1} \cdot x_0, \ldots, 2^{n-1} \cdot x_0$. Pro $k = n-1$ tvrzení platí, neboť obrazem prvku $2^{n-1} \cdot x_0$ při izomorfismu h je nenulový prvek e_{n-1}, a tedy prvek $2^{n-1} \cdot x_0$ je rovněž nenulový.

Nechť tedy $0 \leq k < n-1$. Protože h je izomorfismus a prvek $h(2^k \cdot x_0) = e_k \notin D_{2^{k+1}}$ neleží v podgrupě grupy C_{2^n} generované prvky $e_{k+1}, \ldots, e_{n-1} \in D_{2^{k+1}}$, tak také prvek $2^k \cdot x_0$ neleží v podgrupě K grupy H generované prvky $2^{k+1} \cdot x_0, \ldots, 2^{n-1} \cdot x_0$. Protože K je podgrupa grupy H, je vzhledem k předpokladu věty uzavřená na operaci $\oplus$, čili podgrupa grupy G generovaná prvky $2^{k+1} \cdot x_0, \ldots, 2^{n-1} \cdot x_0$ je částí K, a tedy neobsahuje prvek $2^k \cdot x_0$.

Opačná implikace plyne z konce poznámky 2.3. □

Poznámka 2.8. V předchozím důkazu bylo třeba ukázat, že pokud je každá podgrupa grupy H uzavřená i na operaci grupy G, pak existuje izomorfismus $h : G \to C_2^n$, který je také izomorfismem $H \to C_{2^n}$. Ukázali jsme však silnější tvrzení, totiž že takovýmto izomorfismem je libovolný izomorfismus $h : H \to C_{2^n}$.

Kapitola 3

Soustavy diferenčních rovnic

Nechť (C_2^n, C_{2^n}) je standardní grupový pár. Naším cílem je řešit soustavu rovnic

$$(x \oplus \alpha[k]) + (y \oplus \beta[k]) = (x + y) \oplus \gamma[k], \tag{3.1}$$

s neznámými $x, y \in \mathbf{2}^n$ a parametry $\alpha[k], \beta[k], \gamma[k] \in \mathbf{2}^n$, $k = 1, \ldots, m$. K tomu stačí umět najít všechna řešení rovnice typu

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma. \tag{3.2}$$

Množinu řešení soustavy (3.1) pak získáme jako průnik množin řešení jednotlivých rovnic soustavy.

Rovnici (3.2) budeme řešit tak, že indukcí podle i najdeme všechna řešení této rovnice modulo D_{2^i} pro $i = 1, \ldots, n$. Tak nakonec dostaneme všechna řešení modulo D_{2^n}, tedy řešení původní rovnice (3.2).

3.1 Řešení modulo D_{2^1}

Tvrzení 3.1. *Nutnou a postačující podmínkou pro řešitelnost rovnice (3.2) modulo D_{2^1} je $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$. Řešením modulo D_{2^1} je pak libovolná dvojice $x, y \in \mathbf{2}^n$.*

Důkaz. Hledáme-li řešení

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma \pmod{D_{2^1}}, \tag{3.3}$$

hledáme taková $x, y \in \mathbf{2}^n$, pro která se shodují přirozené reprezentanty $r_1((x \oplus \alpha) + (y \oplus \beta))$ a $r_1((x + y) \oplus \gamma)$.

Všimněme si, že pro libovolná $u, v \in \mathbf{2}^n$ je

$$u + v = u \oplus v \pmod{D_{2^1}}. \tag{3.4}$$

Z toho plyne, že $r_1((x \oplus \alpha) + (y \oplus \beta)) = (0, \ldots, 0, x_0 \oplus \alpha_0 \oplus y_0 \oplus \beta_0)$ a $r_1((x+y) \oplus \gamma) = (0, \ldots, 0, x_0 \oplus y_0 \oplus \gamma_0)$. Rovnice (3.3) je tedy řešitelná, právě když

$$x_0 \oplus \alpha_0 \oplus y_0 \oplus \beta_0 = x_0 \oplus y_0 \oplus \gamma_0,$$

což je ekvivalentní

$$\alpha_0 \oplus \beta_0 = \gamma_0.$$

Tato rovnost nezávisí na x, y, proto je v případě její platnosti řešením rovnice (3.3) libovolná dvojice $x, y \in \mathbf{2}^n$. □

3.2 Indukční krok

Než ukážeme obecný indukční krok, tedy jak lze ze znalosti řešení rovnice (3.2) modulo D_{2^i} získat její řešení modulo $D_{2^{i+1}}$, uvedeme, jak lze nalézt řešení modulo D_{2^2} za předpokladu, že rovnice (3.2) je řešitelná modulo D_{2^1}. Později uvidíme, že tento krok je speciální případ obecného indukčního kroku.

V dalším textu budeme symbolem $\mathbf{u}^i$ značit prvek

$$\mathbf{u}^i = (u^i_{n-1}, \ldots, u^i_i, 0, \ldots, 0) \in D_{2^i}.$$

Pro každou dvojici prvků $a, b \in \mathbf{2}^n$ platí pro součet jejich přirozených reprezentantů rovnost $r_i(a) + r_i(b) = r_i(r_i(a) + r_i(b)) + s_i(r_i(a) + r_i(b))$. Je $r_i(r_i(a) + r_i(b)) = r_i(a + b)$, neboť prvek a leží ve stejné rozkladové třídě C_{2^n}/D_{2^i} jako jeho reprezentant $r_i(a)$ a prvek b leží ve stejné rozkladové třídě C_{2^n}/D_{2^i} jako jeho reprezentant $r_i(b)$, a proto jsou reprezentanty rozkladových tříd C_{2^n}/D_{2^i}, ve kterých leží součty $a + b$ a $r_i(a) + r_i(b)$, stejné. Protože každá rozkladová třída C_{2^n}/D_{2^i} je také rozkladovou třídou C^n_2/D_{2^i}, je také $r_i(r_i(a) \oplus r_i(b)) = r_i(a \oplus b)$. Prvek $s_i(r_i(a)+r_i(b)) \in D_{2^i}$ nazýváme *přenosem z i-té souřadnice* při modulárním sčítání.

Lemma 3.2. *Pro každou dvojici $a, b \in \mathbf{2}^n$ a každé $i = 0, \ldots, n-1$ platí $r_{i+1}(a+b) = (0, \ldots, 0, a_i \oplus b_i \oplus e^i_i, a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1}, \ldots, a_1 \oplus b_1 \oplus e^1_1, a_0 \oplus b_0)$, kde $\mathbf{e}^k = (e^k_{n-1}, \ldots, e^k_k, 0, \ldots, 0) \in D_{2^k}$, $k = 1, \ldots, i$, je přenos[1] při (modulárním) sčítání z $(k-1)$-ní pozice.*

[1] V případě standardního grupového páru může být nenulový přenos pouze z i-té na $(i+1)$-ní pozici. Tedy hodnoty e^k_l pro $l \neq k$ jsou nulové. V následující kapitole ukážeme, že toto obecně neplatí.

Důkaz. Lemma dokážeme indukcí podle i. Z rovnosti (3.4) plyne, že $r_1(a+b) = (0,\ldots,0,a_0 \oplus b_0)$. Pro $i = 0$ tedy tvrzení platí.

Všimněme si, že pro každé $i = 1,\ldots,n-1$ a každou dvojici $a, b \in \mathbf{2}^n$ je $r_i(a) + r_i(b) = r_i(a+b) + \mathbf{e}^i$, $\mathbf{e}^i \in D_{2^i}$, což pro $i = 1$ znamená $(0,\ldots,0,a_0) + (0,\ldots,0,b_0) = (0,\ldots,0,a_0 \oplus b_0) + (e^1_{n-1},\ldots,e^1_1,0)$. Proto

$$\begin{aligned}
r_2(a) + r_2(b) &= (0,\ldots,0,a_1,a_0) + (0,\ldots,0,b_1,b_0) = \\
&= (0,\ldots,0,a_1,0) + (0,\ldots,0,b_1,0) + \\
&+ (0,\ldots,0,a_0 \oplus b_0) + (e^1_{n-1},\ldots,e^1_1,0) = \\
&= (0,\ldots,0,a_1 \oplus b_1 \oplus e^1_1,0) + (0,\ldots,0,a_0 \oplus b_0) + \\
&+ (e^2_{n-1},\ldots,e^2_2,0,0) = \\
&= (0,\ldots,0,a_1 \oplus b_1 \oplus e^1_1,a_0 \oplus b_0) + (e^2_{n-1},\ldots,e^2_2,0,0),
\end{aligned}$$

z čehož plyne $r_2(a+b) = (0,\ldots,0,a_1 \oplus b_1 \oplus e^1_1, a_0 \oplus b_0)$.

Předpokládejme, že $r_i(a+b) = (0,\ldots,0,a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1},\ldots,a_0 \oplus b_0)$ a ukažme, že $r_{i+1}(a+b) = (0,\ldots,0,a_i \oplus b_i \oplus e^i_i, a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1},\ldots,a_0 \oplus b_0)$, kde $i = 2,\ldots,n-1$.

Je

$$\begin{aligned}
r_{i+1}(a) + r_{i+1}(b) &= \\
&= (0,\ldots,0,a_i,a_{i-1},\ldots,a_0) + (0,\ldots,0,b_i,b_{i-1},\ldots,b_0) = \\
&= (0,\ldots,0,a_i,0,\ldots,0) + (0,\ldots,0,b_i,0,\ldots,0) + \\
&+ (0,\ldots,0,a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1},\ldots,a_0 \oplus b_0) + \\
&+ (e^i_{n-1},\ldots,e^i_i,0,\ldots,0) = (0,\ldots,0,a_i \oplus b_i \oplus e^i_i,0,\ldots,0) + \\
&+ (0,\ldots,0,a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1},\ldots,a_0 \oplus b_0) + \\
&+ (e^{i+1}_{n-1},\ldots,e^{i+1}_{i+1},0,\ldots,0) = \\
&= (0,\ldots,0,a_i \oplus b_i \oplus e^i_i, a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1},\ldots,a_0 \oplus b_0) + \\
&+ (e^{i+1}_{n-1},\ldots,e^{i+1}_{i+1},0,\ldots,0).
\end{aligned}$$

A protože je $r_{i+1}(a) + r_{i+1}(b) = r_{i+1}(a+b) + \mathbf{e}^{i+1}$, platí $r_{i+1}(a+b) = (0,\ldots,0,a_i \oplus b_i \oplus e^i_i, a_{i-1} \oplus b_{i-1} \oplus e^{i-1}_{i-1},\ldots,a_0 \oplus b_0)$. □

Tvrzení 3.3. *Je-li rovnice (3.2) řešitelná modulo D_{2^1}, pak je řešitelná modulo D_{2^2}, právě když $\alpha_1, \beta_1, \gamma_1, \alpha_0, \beta_0$ splňují jednu z podmínek uvedených v tabulce 3.1. Je-li splněná některá z těchto podmínek, pak jsou řešením takové dvojice $x, y \in \mathbf{2}^n$, jejichž hodnoty x_0, y_0 jsou v tabulce 3.1 na stejných řádcích jako hodnoty $\alpha_1 \oplus \beta_1 \oplus \gamma_1, \alpha_0, \beta_0$[2]. V případě, že*

[2]Význam sloupce d^1_1 v tabulce 3.1 ozřejmíme později.

$\alpha_1 \oplus \beta_1 \oplus \gamma_1, \alpha_0, \beta_0$ nabývají hodnot, které nejsou uvedeny v tabulce 3.1, nemá rovnice (3.2) řešení modulo D_{2^2}, a tedy nemá řešení.

Tabulka 3.1: Hodnoty x_0, y_0 vyhovující rovnici (3.5) při znalosti $\alpha_0, \beta_0, \alpha_1, \beta_1, \gamma_1$; hodnoty d_1^1 jsou pouze pomocné a jsou jednoznačně určitelné z hodnot x_0, y_0

$\alpha_1 \oplus \beta_1 \oplus \gamma_1$	α_0	β_0	x_0	y_0	d_1^1
0	0	0	0	0	0
0	0	0	0	1	0
0	0	0	1	0	0
0	0	0	1	1	1
0	0	1	0	0	0
0	0	1	0	1	0
0	1	0	0	0	0
0	1	0	1	0	0
0	1	1	0	1	0
0	1	1	1	0	0
1	0	1	1	0	0
1	0	1	1	1	1
1	1	0	0	1	0
1	1	0	1	1	1
1	1	1	0	0	0
1	1	1	1	1	1

Důkaz. Předpokládejme, že rovnice (3.3) je řešitelná a hledejme $x, y \in \mathbf{2}^n$ taková, že platí

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma \pmod{D_{2^2}}. \tag{3.5}$$

Podle lemmatu 3.2 je přirozený reprezentant $r_2((x \oplus \alpha) + (y \oplus \beta))$ výrazu $(x \oplus \alpha) + (y \oplus \beta)$ roven $(0, \ldots, 0, x_1 \oplus \alpha_1 \oplus y_1 \oplus \beta_1 \oplus c_1^1, x_0 \oplus \alpha_0 \oplus y_0 \oplus \beta_0)$, kde $r_1(x \oplus \alpha) + r_1(y \oplus \beta) = r_1((x \oplus \alpha) + (y \oplus \beta)) + \mathbf{c}^1$. Podobně spočítáme $r_2((x + y) \oplus \gamma) = (0, \ldots, 0, x_1 \oplus y_1 \oplus \gamma_1 \oplus d_1^1, x_0 \oplus y_0 \oplus \gamma_0)$, kde $r_1(x) + r_1(y) = r_1(x + y) + \mathbf{d}^1$, a tedy $(r_1(x) + r_1(y)) \oplus r_1(\gamma) = (r_1(x + y) + \mathbf{d}^1) \oplus r_1(\gamma) = r_1(x + y) \oplus r_1(\gamma) + \mathbf{d}^1 = r_1((x + y) \oplus \gamma) + \mathbf{d}^1$, neboť $\mathbf{d}^1 \in D_{2^1}$.

Existuje-li řešení rovnice (3.3), pak řešením rovnice (3.5) jsou právě všechny dvojice $x, y \in \mathbf{2}^n$ takové, že

$$x_1 \oplus \alpha_1 \oplus y_1 \oplus \beta_1 \oplus c_1^1 = x_1 \oplus y_1 \oplus \gamma_1 \oplus d_1^1,$$

neboli

$$c_1^1 \oplus d_1^1 = \alpha_1 \oplus \beta_1 \oplus \gamma_1. \tag{3.6}$$

Snadno ověříme, že

- $c_1^1 = 0 \Leftrightarrow (\alpha_0 = x_0 \vee \beta_0 = y_0)$,
- $c_1^1 = 1 \Leftrightarrow (\alpha_0 \neq x_0 \wedge \beta_0 \neq y_0)$,
- $d_1^1 = 0 \Leftrightarrow (x_0 = 0 \vee y_0 = 0)$,
- $d_1^1 = 1 \Leftrightarrow (x_0 = 1 \wedge y_0 = 1)$.

Řešme nyní rovnici (3.6). Mohou nastat dva případy:

1. Je-li $\alpha_1 \oplus \beta_1 \oplus \gamma_1 = 0$, pak $c_1^1 \oplus d_1^1 = 0$. Zde opět rozlišíme dva případy:
   (a) $c_1^1 = 0 \ \wedge \ d_1^1 = 0$
   Díky pozorování za rovnicí (3.6) vidíme, že rovnici (3.5) v takovém případě vyhovují hodnoty $x_0, y_0, \alpha_0, \beta_0$ uvedené v tabulce 3.2.
   (b) $c_1^1 = 1 \ \wedge \ d_1^1 = 1$
   Hodnoty $x_0, y_0, \alpha_0, \beta_0$ vyhovující rovnici (3.5) v tomto případě jsou uvedeny v tabulce 3.3
2. Je-li $\alpha_1 \oplus \beta_1 \oplus \gamma_1 = 1$, neboli $c_1^1 \oplus d_1^1 = 1$, pak buď
   (a) $c_1^1 = 0 \ \wedge \ d_1^1 = 1$
   nebo
   (b) $c_1^1 = 1 \ \wedge \ d_1^1 = 0$.
   Hodnoty $x_0, y_0, \alpha_0, \beta_0$ vyhovující rovnici (3.5) v případech 2a, resp. 2b, jsou uvedeny v tabulkách 3.5, resp. 3.4.

Tabulka 3.1 je shrnutím tabulek 3.2, 3.3, 3.4 a 3.5. □

Tabulka 3.2: Hodnoty $x_0, y_0, \alpha_0, \beta_0$ vyhovující rovnici (3.5) v případě, že $c_1^1 = 0 \wedge d_1^1 = 0$

x_0	y_0	α_0	β_0
0	0	0	0
0	0	0	1
0	0	1	0
0	1	0	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	0	1	1

Tabulka 3.3: Hodnoty $x_0, y_0, \alpha_0, \beta_0$ vyhovující rovnici (3.5) v případě, že $c_1^1 = 1 \wedge d_1^1 = 1$

x_0	y_0	α_0	β_0
1	1	0	0

Tabulka 3.4: Hodnoty $x_0, y_0, \alpha_0, \beta_0$ vyhovující rovnici (3.5) v případě, že $c_1^1 = 0 \wedge d_1^1 = 1$

x_0	y_0	α_0	β_0
1	1	0	1
1	1	1	0
1	1	1	1

Tabulka 3.5: Hodnoty $x_0, y_0, \alpha_0, \beta_0$ vyhovující rovnici (3.5) v případě, že $c_1^1 = 1 \wedge d_1^1 = 0$

x_0	y_0	α_0	β_0
0	0	1	1
0	1	1	0
1	0	0	1

Nyní ukážeme obecný indukční krok. Předpokládejme, že známe množinu řešení rovnice (3.2) modulo D_{2^i}, kde $i = 2, \ldots, n-1$. Potřebujeme zjistit, která z těchto řešení vyhovují také rovnici

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma \pmod{D_{2^{i+1}}}. \tag{3.7}$$

Budeme postupovat podobně jako při hledání řešení modulo D_{2^2} za předpokladu řešitelnosti modulo D_{2^1}, avšak s tím rozdílem, že $\mathbf{c}^i, \mathbf{d}^i$, kde $i = 2, \ldots, n-1$, nezávisí pouze na $\alpha_{i-1}, \beta_{i-1}, x_{i-1}, y_{i-1}$, jako to bylo u $i = 1$, ale také na $\mathbf{c}^{i-1}, \mathbf{d}^{i-1}$.

Tvrzení 3.4. *Je-li rovnice (3.2) řešitelná modulo D_{2^i}, kde $i = 1, \ldots, n-1$, pak je řešitelná modulo $D_{2^{i+1}}$, právě když $\alpha_i, \beta_i, \gamma_i, \alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}$, splňují jednu z podmínek uvedených v tabulce 3.6. Pokud je některá z těchto podmínek splněná, pak jsou řešením takové dvojice $x, y \in \mathbf{2}^n$, pro které jsou hodnoty $d_{i-1}^{i-1}, x_{i-1}, y_{i-1}$ v tabulce 3.6 na řádcích s hodnotami $\alpha_i \oplus \beta_i \oplus \gamma_i, \alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}$. V případě, že $\alpha_i \oplus \beta_i \oplus \gamma_i, \alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}$ nabývají hodnot, které nejsou uvedeny v tabulce 3.6, nemá rovnice (3.2) řešení modulo $D_{2^{i+1}}$, a tedy nemá řešení.*

Tabulka 3.6: Hodnoty $d_{i-1}^{i-1}, x_{i-1}, y_{i-1}$ vyhovující rovnici (3.7) při znalosti $\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}, \alpha_i, \beta_i, \gamma_i$; hodnoty d_i^i jsou pouze pomocné a jsou jednoznačně určitelné z hodnot $d_{i-1}^{i-1}, x_{i-1}, y_{i-1}$

$\alpha_i \oplus \beta_i \oplus \gamma_i$	α_{i-1}	β_{i-1}	γ_{i-1}	d_{i-1}^{i-1}	x_{i-1}	y_{i-1}	d_i^i
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0
0	0	0	0	0	1	0	0
0	0	0	0	0	1	1	1
0	0	0	0	1	0	0	0
0	0	0	0	1	0	1	1
0	0	0	0	1	1	0	1
0	0	0	0	1	1	1	1
0	0	0	1	0	0	0	0
0	0	0	1	0	1	1	1
0	0	0	1	1	0	0	0
0	0	0	1	1	1	1	1

Pokračování na následující straně

Tabulka 3.6 – pokračování

$\alpha_i \oplus \beta_i \oplus \gamma_i$	α_{i-1}	β_{i-1}	γ_{i-1}	d_{i-1}^{i-1}	x_{i-1}	y_{i-1}	d_i^i
0	0	1	0	0	0	1	0
0	0	1	0	0	1	1	1
0	0	1	0	1	0	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	0
0	0	1	1	0	0	1	0
0	0	1	1	1	1	0	1
0	0	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	1	0	0	0	1	1	1
0	1	0	0	1	0	0	0
0	1	0	0	1	0	1	1
0	1	0	1	0	0	0	0
0	1	0	1	0	1	0	0
0	1	0	1	1	0	1	1
0	1	0	1	1	1	1	1
0	1	1	0	0	0	1	0
0	1	1	0	0	1	0	0
0	1	1	0	1	0	1	1
0	1	1	0	1	1	0	1
1	0	0	1	0	0	1	0
1	0	0	1	0	1	0	0
1	0	0	1	1	0	1	1
1	0	0	1	1	1	0	1
1	0	1	0	0	0	0	0
1	0	1	0	0	1	0	0
1	0	1	0	1	0	1	1
1	0	1	0	1	1	1	1
1	0	1	1	0	1	0	0
1	0	1	1	0	1	1	1
1	0	1	1	1	0	0	0
1	0	1	1	1	0	1	1

Pokračování na následující straně

Tabulka 3.6 – pokračování

$\alpha_i \oplus \beta_i \oplus \gamma_i$	α_{i-1}	β_{i-1}	γ_{i-1}	d_{i-1}^{i-1}	x_{i-1}	y_{i-1}	d_i^i
1	1	0	0	0	0	0	0
1	1	0	0	0	0	1	0
1	1	0	0	1	1	0	1
1	1	0	0	1	1	1	1
1	1	0	1	0	0	1	0
1	1	0	1	0	1	1	1
1	1	0	1	1	0	0	0
1	1	0	1	1	1	0	1
1	1	1	0	0	0	0	0
1	1	1	0	0	1	1	1
1	1	1	0	1	0	0	0
1	1	1	0	1	1	1	1
1	1	1	1	0	0	0	0
1	1	1	1	0	0	1	0
1	1	1	1	0	1	0	0
1	1	1	1	0	1	1	1
1	1	1	1	1	0	0	0
1	1	1	1	1	0	1	1
1	1	1	1	1	1	0	1
1	1	1	1	1	1	1	1

Důkaz. Předpokládejme, že rovnice (3.2) je řešitelná modulo D_{2^i}. Z lematu 3.2 plyne, že reprezentanty $r_{i+1}((x \oplus \alpha) + (y \oplus \beta))$, $r_{i+1}((x+y) \oplus \gamma)$ jsou tvaru:

$$\begin{aligned} r_{i+1}((x \oplus \alpha) + (y \oplus \beta)) &= (0, \ldots, 0, x_i \oplus \alpha_i \oplus y_i \oplus \beta_i \oplus c_i^i, \ldots, \\ &\quad x_1 \oplus \alpha_1 \oplus y_1 \oplus \beta_1 \oplus c_1^1, x_0 \oplus \alpha_0 \oplus y_0 \oplus \beta_0), \end{aligned} \tag{3.8}$$

$$\begin{aligned} r_{i+1}((x+y) \oplus \gamma) &= (0, \ldots, 0, x_i \oplus y_i \oplus \gamma_i \oplus d_i^i, \ldots, x_1 \oplus y_1 \oplus \gamma_1 \oplus d_1^1, \\ &\quad x_0 \oplus y_0 \oplus \gamma_0). \end{aligned} \tag{3.9}$$

Dvojice $x, y \in \mathbf{2}^n$ je řešením rovnice (3.7), právě když se shodují reprezenanty (3.8), (3.9) příslušné této dvojici, což je právě tehdy, když je splněna rovnost

$$x_i \oplus \alpha_i \oplus y_i \oplus \beta_i \oplus c_i^i = x_i \oplus y_i \oplus \gamma_i \oplus d_i^i,$$

čili

$$c_i^i \oplus d_i^i = \alpha_i \oplus \beta_i \oplus \gamma_i.$$

Platí

- $c_i^i = 0 \Leftrightarrow (x_{i-1} \oplus \alpha_{i-1} = 0 \wedge y_{i-1} \oplus \beta_{i-1} = 0 \wedge c_{i-1}^{i-1} = 0) \vee$
  $(x_{i-1} \oplus \alpha_{i-1} = 0 \wedge y_{i-1} \oplus \beta_{i-1} = 0 \wedge c_{i-1}^{i-1} = 1) \vee$
  $(x_{i-1} \oplus \alpha_{i-1} = 0 \wedge y_{i-1} \oplus \beta_{i-1} = 1 \wedge c_{i-1}^{i-1} = 0) \vee$
  $(x_{i-1} \oplus \alpha_{i-1} = 1 \wedge y_{i-1} \oplus \beta_{i-1} = 0 \wedge c_{i-1}^{i-1} = 0),$
- $c_i^i = 1 \Leftrightarrow (x_{i-1} \oplus \alpha_{i-1} = 0 \wedge y_{i-1} \oplus \beta_{i-1} = 1 \wedge c_{i-1}^{i-1} = 1) \vee$
  $(x_{i-1} \oplus \alpha_{i-1} = 1 \wedge y_{i-1} \oplus \beta_{i-1} = 0 \wedge c_{i-1}^{i-1} = 1) \vee$
  $(x_{i-1} \oplus \alpha_{i-1} = 1 \wedge y_{i-1} \oplus \beta_{i-1} = 1 \wedge c_{i-1}^{i-1} = 0) \vee$
  $(x_{i-1} \oplus \alpha_{i-1} = 1 \wedge y_{i-1} \oplus \beta_{i-1} = 1 \wedge c_{i-1}^{i-1} = 1),$
- $d_i^i = 0 \Leftrightarrow (x_{i-1} = 0 \wedge y_{i-1} = 0 \wedge d_{i-1}^{i-1} = 0) \vee$
  $(x_{i-1} = 0 \wedge y_{i-1} = 0 \wedge d_{i-1}^{i-1} = 1) \vee$
  $(x_{i-1} = 0 \wedge y_{i-1} = 1 \wedge d_{i-1}^{i-1} = 0) \vee$
  $(x_{i-1} = 1 \wedge y_{i-1} = 0 \wedge d_{i-1}^{i-1} = 0),$
- $d_i^i = 1 \Leftrightarrow (x_{i-1} = 0 \wedge y_{i-1} = 1 \wedge d_{i-1}^{i-1} = 1) \vee$
  $(x_{i-1} = 1 \wedge y_{i-1} = 0 \wedge d_{i-1}^{i-1} = 1) \vee$
  $(x_{i-1} = 1 \wedge y_{i-1} = 1 \wedge d_{i-1}^{i-1} = 0) \vee$
  $(x_{i-1} = 1 \wedge y_{i-1} = 1 \wedge d_{i-1}^{i-1} = 1).$

Z těchto údajů[3] získáme tabulku 3.6.

□

Srovnáme-li tabulky 3.1 a 3.6, vidíme, že hledání řešení rovnice (3.2) modulo D_{2^2} za předpokladu její řešitelnosti modulo D_{2^1} je speciální případ obecného indukčního kroku. Pokud bychom z tabulky 3.6 vybrali právě ty řádky, na kterých je $\alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1} = 0$ a $d_{i-1}^{i-1} = 0$ a položili $i = 1$, získali bychom tabulku 3.1.

Vynecháme-li z tabulky 3.6 sloupce $\alpha_i \oplus \beta_i \oplus \gamma_i$ a d_i^i, dosadíme-li $i = n$ a řádky vzniklé tabulky vhodně přeuspořádáme, zjistíme, že (v případě, že rovnice (3.2) je řešitelná) dvojice x_{n-1}, y_{n-1} může nabývat libovolných hodnot bez ohledu na hodnoty $\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1}, d_{n-1}^{n-1}$.

Z tabulky 3.6 je zřejmé, že pro pevně daná $\alpha_i, \beta_i, \gamma_i, \alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}$

[3]Chceme, aby tabulka 3.6 ukazovala závislost x_{i-1}, y_{i-1}, d_{i-1}^{i-1} na α_{i-1}, β_{i-1}, γ_{i-1}, α_i, β_i, γ_i. K tomu využijeme rovnosti $c_i^i \oplus d_i^i = \alpha_i \oplus \beta_i \oplus \gamma_i$. Také víme, že $c_{i-1}^{i-1} \oplus d_{i-1}^{i-1} = \alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1}$, a ze znalosti $\alpha_{i-1}, \beta_{i-1}$ spočteme γ_{i-1}.

platí pro velikosti množin řešení následující rovnost

$$\begin{aligned}&\#\{\alpha_i \oplus \beta_i \oplus \gamma_i, \alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}, d_{i-1}^{i-1}, x_{i-1}, y_{i-1}, d_i^i| \\ &\quad d_{i-1}^{i-1} = 0; x_{i-1}, y_{i-1}, d_i^i \in \{0,1\}\} = \\ &\quad = \#\{\alpha_i \oplus \beta_i \oplus \gamma_i, \alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}, d_{i-1}^{i-1}, x_{i-1}, y_{i-1}, d_i^i| \\ &\quad d_{i-1}^{i-1} = 1; x_{i-1}, y_{i-1}, d_i^i \in \{0,1\}\}\end{aligned} \tag{3.10}$$

pro každé $i = 1, \ldots, n-1$. Tuto velikost nazveme pro účely následujícího odstavce *počtem řešení dané rovnice na i-tém bitu*. Protože hodnota d_i^i nezávisí na $\alpha_j, \beta_j, \gamma_j, j = 0, \ldots, n-1$, ale pouze na $x_{i-1}, y_{i-1}, d_{i-1}^{i-1}$, platí rovnost pro velikost množin trojic $(d_{i-1}^{i-1} = 0, x_{i-1}, y_{i-1})$ a $(d_{i-1}^{i-1} = 1, x_{i-1}, y_{i-1})$, které vyhovují soustavě (3.1) modulo D_{2^i}.

Počet dvojic (x_{i-1}, y_{i-1}), které vyhovují soustavě (3.1) modulo D_{2^i}, tedy nezávisí na hodnotě d_{i-1}^{i-1}, ale pouze na hodnotách $\alpha_i, \beta_i, \gamma_i, \alpha_{i-1}, \beta_{i-1}$, γ_{i-1}, proto je počet řešení soustavy (3.1) roven součinu počtů řešení na jednotlivých bitech.

3.3 Algoritmus

Nyní popíšeme algoritmus na hledání všech řešení soustavy (3.1).

Algoritmus 3.5.
Vstup: Keoficienty $\alpha_i[k], \beta_i[k], \gamma_i[k], i = 0, \ldots, n-1, k = 1, \ldots, m$.
Výstup: Množina všech dvojic $x = (x_{n-1}, \ldots, x_0), y = (y_{n-1}, \ldots, y_0)$, které jsou řešením soustavy (3.1) s koeficienty ze vstupu.
Postup:

1. Pro $k = 1, \ldots, m$:
2. Ověř, jestli $\alpha_0[k] \oplus \beta_0[k] \oplus \gamma_0[k] = 0$.
3. Pokud tato rovnost neplatí, pak soustava (3.1) nemá řešení. Konec.
4. Pro $k = 1, \ldots, m$:
5. Polož $d_0^0[k] = 0$.
6. Pro $i = 2, \ldots, n$:
7. Pro $k = 1, \ldots, m$:

8. V tabulce 3.6 najdi množinu všech řešení k-té rovnice soustavy (3.1) modulo D_{2^i}, tj. množinu čtveřic $(d_{i-1}^{i-1}, x_{i-1}, y_{i-1}, d_i^i)$[4], které vyhovují dané rovnici modulo D_{2^i}.

9. Pokud takové řešení neexistuje, pak soustava (3.1) nemá řešení. Konec.

10. Urči průnik množin řešení jednotlivých rovnic modulo D_{2^i}.

11. Zkombinuj výsledky[5], x_{n-1}, y_{n-1} libovolné.

Věta 3.6. *Nalezení jednoho řešení soustavy (3.1) pomocí algoritmu 3.5 má časovou složitost polynomiální vzhledem k mn, kde m je počet rovnic soustavy (3.1). Nemá-li soustava (3.1) řešení, pak tuto skutečnost zjistíme také v čase $\mathcal{O}(mn)$.*

Důkaz. Rozeberme časovou složitost jednotlivých kroků algoritmu. Kroky 2. a 3. mají konstantní časovou složitost, takže kroky 1.–3. mají složitost $\mathcal{O}(m)$. Kroky 4.–5. mají také časovou složitost $\mathcal{O}(m)$. Krok 8. má konstantní časovou složitost, neboť hledání řešení v tabulce 3.6 má složitost logaritmickou vzhledem k počtu řádků tabulky, který je konstantní. Krok 9. má také konstantní složitost. Průnik m množin, z nichž každá má velikost maximálně l, lze nalézt v $\mathcal{O}(ml^2)$. V našem případě je $l = 4$. Složitost kroku 10. je tedy opět v $\mathcal{O}(m)$. Kroky 6.–10. mají tedy složitost $\mathcal{O}(mn)$.

Pokud ukončíme krok 11. po nalezení prvního řešení, získáme tak jedno řešení soustavy (3.1) v čase $\mathcal{O}(n)$.

Celková časová složitost takto upraveného algoritmu je tedy v $\mathcal{O}(mn)$.

Nemá-li soustava (3.1) řešení, zjistíme to v průběhu kroků 1. - 10. algoritmu 3.5, tedy v čase $\mathcal{O}(mn)$. □

Poznámka 3.7. Počet všech řešení soustavy (3.1) může být exponenciální vzhledem k n (je v $\mathcal{O}(4^n)$). Proto nalezení všech řešení soustavy (3.1) obecně není polynomiální vzhledem k mn.

[4]Hodnota d_i^i není součástí řešení. Je to pomocná hodnota, kterou využijeme v kroku 11.

[5]Principem prohledávání do hloubky, a to tak, aby hodnota d_{i-1}^{i-1} získaná při hledání řešení soustavy modulo D_{2^i} byla shodná s hodnotou d_{i-1}^{i-1}, která je součástí řešení modulo $D_{2^{i+1}}$.

Tabulka 3.6 (bez sloupce d_i^i) odpovídá tabulce 1 z článku [1]. Tabulka 3.6 je však jednorozměrná, zatímco tabulka 1 z článku je dvourozměrná. Hodnoty $\alpha_i, \beta_i, \tilde{\gamma}_i, x_i, y_i, c_i$ z tabulky z článku odpovídají pořadě hodnotám $\alpha_{i-1}, \beta_{i-1}, \alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1}, x_{i-1}, y_{i-1}, d_{i-1}^{i-1}$ z tabulky 3.6. Hodnoty $\tilde{\gamma}_{i+1}$ uvedené „uvnitř“ tabulky 1 z článku odpovídají hodnotám $\alpha_i \oplus \beta_i \oplus \gamma_i$ v tabulce 3.6.

Kapitola 4

Abelovské grupové páry

V této kapitole budeme zkoumat, za jakých podmínek je soustava (3.1) řešitelná v abelovském grupovém páru (G, H) (viz definici 2.2) na množině X mohutnosti 2^n.

V předchozí kapitole, která se týkala článku [1], jsme používali indexaci podgrup a souřadnic, která korespondovala s indexací použitou v tomto článku. V této kapitole budeme používat „obrácenou“ indexaci, jak uvidíme v následujícícm odstavci.

Na množině X budeme uvažovat algebru $(X, 0, +, \oplus)$. Grupy G, H definujeme následovně: $G = (X, 0, \oplus)$ a $H = (X, 0, +)$. V celé kapitole budeme předpokládat, že $\iota_X = \pi_0 \subset \pi_1 \subset \cdots \subset \pi_n = X \times X$ je posloupnost kongruencí algebry $(X, 0, +, \oplus)$. Pro $i = 0, \ldots, n$ označme symbolem X_i třídu kongruence π_i, která obsahuje prvek 0. Grupy G a H mají společný neutrální prvek 0, proto $(X_i, 0, \oplus)$ je podgrupa G a $(X_i, 0, +)$ je podgrupa H a π_i je rozklad G/X_i a H/X_i pro každé $i = 0, \ldots, n$. Odtud plyne, že $\{0\} = X_0 \subset X_1 \subset \cdots \subset X_n = X$. Z Lagrangeovy věty a ze skutečností, že mohutnost množiny X je 2^n a inkluze mezi X_{i-1} a X_i jsou ostré pro všechna $i = 1, \ldots, n$, plyne, že X_{i-1} má index 2 v X_i pro $i = 1, \ldots, n$.

Definice 4.1. Abelovský grupový pár $(G = (X, 0, \oplus), H = (X, 0, +))$ na množině X mohutnosti 2^n takový, že existuje maximální řetízek kongruencí $\iota_X = \pi_0 \subset \pi_1 \subset \cdots \subset \pi_n = X \times X$ algebry $(X, 0, +, \oplus)$, nazýváme *hustým abelovským grupovým párem* na množině X.

Pro každé $i = 1, \ldots, n$ zvolme $e_i \in X_i \setminus X_{i-1}$. Takové prvky existují, protože X_{i-1} má index 2 v X_i pro $i = 1, \ldots, n$. Pro každé $i = 1, \ldots, n-1$ platí, že prvek e_{i+1} neleží v podalgebře X_i algebry X, která obsahuje prvky $e_1, \ldots, e_i$. Tuto posloupnost nazveme *bází grupového páru* (G, H) a označíme $E_X = (e_1, e_2, \ldots, e_n)$.

Lemma 4.2. *Každý prvek $x \in X$ lze jednoznačně zapsat jako $x = \sum_{j=1}^{n} x_j e_j = \bigoplus_{j=1}^{n} y_j e_j$, kde $x_j, y_j \in \{0,1\}$ pro $j = 1, \ldots, n$.*

Důkaz. Lemma dokážeme pouze pro operaci $+$. Pro operaci $\oplus$ by byl důkaz obdobný.

Nejprve dokážeme existenci vyjádření $x = \sum_{j=1}^{n} x_j e_j$, $x_j \in \{0,1\}, j = 1, \ldots, n$. Indukcí podle i ukážeme, že každé $x \in X_i$ lze zapsat jako $x = \sum_{j=1}^{i} x_j e_j$, kde $x_j \in \{0,1\}$, $j = 1, \ldots, i$. Nechť $i = 1$. Množina X_1 obsahuje pouze dva prvky $0 = 0 \cdot e_1$ a $e_1 = 1 \cdot e_1$. Nechť tedy $i = 1, \ldots, n-1$. Předpokládejme, že každé $x' \in X_i$ lze zapsat jako $x' = \sum_{j=1}^{i} x_j e_j$, kde $x_j \in \{0,1\}$, $j = 1, \ldots, i$. Nechť $x \in X_{i+1}$. Pak buď $x \in X_i$ nebo $x \in X_{i+1} \setminus X_i$. V prvním případě je $x = x' = x' + 0 \cdot e_{i+1}$ pro nějaké $x' \in X_i$. Ve druhém případě $x = x' + 1 \cdot e_{i+1}$. Je tedy $x = \sum_{j=1}^{i+1} x_j e_j$, $x_j \in \{0,1\}$, $j = 1, \ldots, i+1$, pro každé $x \in X_{i+1}$.

Zbývá dokázat jednoznačnost vyjádření $x = \sum_{j=1}^{n} x_j e_j$. Nechť jsou $\sum_{j=1}^{n} x_j e_j$ a $\sum_{j=1}^{n} x'_j e_j$ dvě různá vyjádření prvku $x \in X$. Označme $k = \max\{j; x_j \neq x'_j\}$. Je $0 = \sum_{j=1}^{n} x_j e_j - \sum_{j=1}^{n} x'_j e_j = \sum_{j=1}^{k} x''_j e_j$, kde $x''_j \in \{-1, 0, 1\}$, $j = 1, \ldots, k$. Je tedy $0 = \sum_{j=1}^{k} x''_j e_j \in X_k \setminus X_{k-1}$, což je spor se skutečností, že $0 \in X_0 \subset X_{k-1}$. □

Poznámka 4.3. Kdykoliv budeme v dalším textu hovořit o vyjádření prvku $x \in X$ pomocí operace $+$ nebo o jeho vyjádření pomocí operace $\oplus$, budeme tím myslet jeho vyjádření z lemmatu 4.2, tedy $x = \sum_{j=1}^{n} x_j e_j$, kde $x_j \in \{0,1\}$ pro $j = 1, \ldots, n$, nebo $x = \bigoplus_{j=1}^{n} y_j e_j$, kde $y_j \in \{0,1\}$ pro $j = 1, \ldots, n$.

Definice 4.4. Nechť $x \in X$ má následující vyjádření pomocí operací $+$ a $\oplus$: $x = \sum_{j=1}^{n} x_j e_j = \bigoplus_{j=1}^{n} y_j e_j$. Uspořádanou n-tici $(x_1, x_2, \ldots, x_n)$ nazýváme *souřadnice prvku x vzhledem k bázi E_X příslušné operaci $+$*, uspořádanou n-tici $(y_1, y_2, \ldots, y_n)$ nazýváme *souřadnice prvku x vzhledem k bázi E_X příslušné operaci $\oplus$*.

Nyní definujeme pojem důležitý pro hledání řešení soustav diferenčních rovnic v hustém abelovském grupovém páru (G, H).

Definice 4.5. *Váha* w je funkce $w : X \to \{0, \ldots, n\}$, která každému prvku $x \in X$ přiřadí následující hodnotu:

$$w(x) = \text{nejmenší } j \text{ takové, že } x \in X_j.$$

Hodnotu $w(x)$ nazýváme *váhou prvku x*.

Předchozí definice je korektní, protože každý prvek $x \in X$ je prvkem $X_n = X$ a pro podgrupy platí $X_0 \subset X_1 \subset \cdots \subset X_n$.

Lemma 4.6. *Pro každý prvek $e_i \in E_X$ platí $w(e_i+e_i) < i$ a $w(e_i \oplus e_i) < i$.*

Důkaz. Toto lemma opět stačí dokázat pro jednu z operací, neboť pro druhou operaci by byl důkaz obdobný. Dokážeme je pro operaci $+$.

Z volby prvků báze E_X plyne, že $w(e_i + e_i) \leq i$.

Předpokládejme, že $w(e_i + e_i) = i$, neboli $e_i + e_i \in X_i \setminus X_{i-1}$. Prvek e_i+e_i pak můžeme vyjádřit jako $e_i+e_i = e_i+h_{i-1}$, kde $h_{i-1} \in X_{i-1}$. Proto $e_i = h_{i-1}$, a tedy $e_i \in X_{i-1}$, což je spor s volbou prvků báze E_X. □

Důsledek 4.7. *Pro každé dva prvky $x, y \in X$ platí*

(i) $w(x) = w(y) \Rightarrow (w(x + y) < w(x) \wedge w(x \oplus y) < w(x))$,

(ii) $w(x) > w(y) \Rightarrow (w(x + y) = w(x) \wedge w(x \oplus y) = w(x))$.

Tedy $\forall x, y \in X : \; w(x + y) \leq \max\{w(x), w(y)\}, w(x \oplus y) \leq \max\{w(x), w(y)\}$.

Důkaz. Podobně jako předchozí lemma dokážeme toto tvrzení pouze pro operaci $+$. Buďte $(x_1, \ldots, x_n)$ a $(y_1, \ldots, y_n)$ souřadnice prvků x a y vzhledem k bázi E_X příslušné operaci $+$.

(i) Označme $i = w(x) = w(y)$. Je $x, y \in X_i \setminus X_{i-1}$, tedy

$$x = e_i + h_x, \quad h_x \in X_{i-1},$$

$$y = e_i + h_y, \quad h_y \in X_{i-1}.$$

Proto $x+y = (e_i+e_i)+h_x+h_y$, kde $(e_i+e_i) \in X_{i-1}$ podle lemmatu 4.6. Tedy $x + y \in X_{i-1}$, a proto $w(x + y) < i$.

(ii) Označme opět $i = w(x)$ a $j = w(y)$. Je $x \in X_i \setminus X_{i-1}$ a $y \in X_j \setminus X_{j-1}$. Protože $i > j$, je $X_j \subseteq X_{i-1}$. Tedy $y \in X_{i-1}$. A protože $x = e_i + h_x$, kde $h_x \in X_{i-1}$, dostáváme $x + y = e_i + h_x + y$, kde $(h_x + y) \in X_{i-1}$, tedy $x + y \in X_i \setminus X_{i-1}$.

□

Z důsledku 4.7 snadno plyne, že pro každé $x \in X$ platí

$$w(-x) = w(\ominus x) = w(x). \tag{4.1}$$

Podobně jako v 2. kapitole zavedeme pro každé $i = 0, \ldots, n-1$ *přirozený systém reprezentantů* rozkladových tříd X/X_i příslušný operaci $\oplus$, který značíme

$$\mathcal{R}^{\oplus}(X/X_i).$$

Přirozeným reprezentantem prvku $x = \bigoplus_{j=1}^{n} x_j e_j \in X$ příslušným operaci $\oplus$ v rozkladové třídě X/X_i je prvek

$$r_{i+1}^{\oplus}(x) = \bigoplus_{j=i+1}^{n} x_j e_j \in X \setminus X_i. \tag{4.2}$$

Nejprve je třeba ukázat, že jde opravdu o systém reprezentantů X/X_i. Množina $\mathcal{R}^{\oplus}(X/X_i)$ má 2^{n-i} prvků, proto stačí ukázat, že dva různé prvky této množiny leží v různých třídách X/X_i. Předpokládejme, že dva různé reprezentanty $r_{i+1}^{\oplus}(x) = \bigoplus_{j=i+1}^{n} x_j e_j$, $r_{i+1}^{\oplus}(y) = \bigoplus_{j=i+1}^{n} y_j e_j$ leží ve stejné rozkladové třídě X/X_i. Prvky $r_{i+1}^{\oplus}(x)$ a $r_{i+1}^{\oplus}(y)$ jsou tedy kongruentní modulo X_i, a tedy jejich rozdíl leží v X_i, $0 \neq r_{i+1}^{\oplus}(x) \ominus r_{i+1}^{\oplus}(y) \in X_i$. Označme $z = r_{i+1}^{\oplus}(x) \ominus r_{i+1}^{\oplus}(y) = \bigoplus_{j=1}^{i} z_j e_j$. Je $r_{i+1}^{\oplus}(x) = z \oplus r_{i+1}^{\oplus}(y) = \bigoplus_{j=1}^{n} t_j e_j$, kde $t_j = z_j$ pro $j = 1, \ldots, i$ a $t_j = y_j$ pro $j = i+1, \ldots, n$. Prvek $\bigoplus_{j=1}^{n} t_j e_j$ ale není prvkem $X \setminus X_i$, což je spor s vyjádřením (4.2).

Pro každé $i = 0, \ldots, n-1$ lze každý prvek $x \in X$ jednoznačně zapsat jako součet

$$x = r_{i+1}^{\oplus}(x) \oplus s_{i+1}^{\oplus}(x),$$

kde $r_{i+1}^{\oplus}(x) \in \mathcal{R}^{\oplus}(X/X_i), s_{i+1}^{\oplus}(x) \in X_i$.

Dále pro každé $i, j = 0, \ldots, n-1$, $i > j$ zavedeme přirozený systém reprezentantů rozkladových tříd X_i/X_j následovně:

$$\mathcal{R}^{\oplus}(X_i/X_j) := \mathcal{R}^{\oplus}(X/X_j) \cap X_i.$$

Řekneme, že dva prvky $x, y \in X$ jsou si rovny modulo podalgebra $X_i = (X_i, 0, +, \oplus)$, právě když leží ve stejné rozkladové třídě X podle X_i.

Podobně jako v případě standardního grupového páru (viz str. 12) platí pro $i = 1, \ldots, n$ a pro libovolné dva prvky $a, b \in X$ následující rovnost

$$r_i^{\oplus}(a) \oplus r_i^{\oplus}(b) = r_i^{\oplus}(a \oplus b) \oplus s_i^{\oplus}(r_i^{\oplus}(a) \oplus r_i^{\oplus}(b)), \tag{4.3}$$

kde $s_i^{\oplus}(r_i^{\oplus}(a) \oplus r_i^{\oplus}(b)) \in X_{i-1}$. Prvek $s_i^{\oplus}(r_i^{\oplus}(a) \oplus r_i^{\oplus}(b))$ nazveme *přenosem z i-té souřadnice* při operaci $\oplus$.

Dále zavedeme pro každé $i = 0, \ldots, n-1$ *přirozený systém reprezentantů* rozkladových tříd X/X_i příslušný operaci $+$, který značíme

$$\mathcal{R}^{+}(X/X_i).$$

Přirozeným reprezentantem prvku $x = \sum_{j=1}^{n} y_j e_j \in X$ příslušným operaci $+$ v rozkladové třídě X/X_i je prvek

$$r_{i+1}^{+}(x) = \sum_{j=i+1}^{n} y_j e_j \in X \setminus X_i. \tag{4.4}$$

Přirozený systém reprezentantů $\mathcal{R}^{+}(X/X_i)$ má obdobné vlastnosti jako přirozený systém reprezentantů $\mathcal{R}^{\oplus}(X/X_i)$.

Pro každé $i = 0, \ldots, n-1$ lze každý prvek $x \in X$ jednoznačně zapsat jako součet

$$x = r_{i+1}^{+}(x) + s_{i+1}^{+}(x),$$

kde $r_{i+1}^{+}(x) \in \mathcal{R}^{+}(X/X_i), s_{i+1}^{+}(x) \in X_i$.

Pro operaci $+$ platí také následující obdoda rovnosti (4.3):

$$r_i^{+}(a) + r_i^{+}(b) = r_i^{+}(a+b) + s_i^{+}(r_i^{+}(a) + r_i^{+}(b)), \tag{4.5}$$

kde $s_i^{+}(r_i^{+}(a)+r_i^{+}(b)) \in X_{i-1}$. Prvek $s_i^{+}(r_i^{+}(a)+r_i^{+}(b))$ nazveme *přenosem z i-té souřadnice* při operaci $+$.

Protože pro každé $i \in \{1, \ldots, n\}$ množina $\mathcal{R}^{\oplus}(X_i/X_{i-1})$ obsahuje pouze dva prvky 0 a e_i, platí následující lemma.

Lemma 4.8. *Nechť $i \in \{1, \ldots, n\}$. Pro každé dva prvky $u, v \in \mathcal{R}^{\oplus}(X_i/X_{i-1})$ platí $r_i^{\oplus}(u+v) = r_i^{\oplus}(u \oplus v)$, neboli $u + v = u \oplus v \pmod{X_{i-1}}$.*

4.1 Vyjádření operace $+$ pomocí operace $\oplus$

K hledání řešení soustav diferenčních rovnic v hustém abelovském grupovém páru $((X, 0, +), (X, 0, \oplus))$ je třeba umět vyjádřit jednu operaci pomocí druhé. Operace $+$ a $\oplus$ jsou z tohoto hlediska rovnocenné. Protože však v případě standardního grupového páru převádíme operaci $+$ na operaci $\oplus$, použijeme tento přístup i v případě obecnějšího hustého abelovského grupového páru.

Vyjádření operace $+$ pomocí operace $\oplus$ na množinách X_i, $i = 1, \ldots, n$, získáme indukcí podle i. Pro $i = 1, 2$ je situace jednoduchá. Podmnožina X_1 množiny X obsahuje pouze dva prvky: 0 a e_1. Je $w(e_1 + e_1) = w(e_1 \oplus e_1) = 0$, a tedy $e_1 + e_1 = e_1 \oplus e_1 = 0$.

Množina X_2 je čtyřprvková, $X_2 = \{0, e_1, e_2, e_1 + e_2\} = \{0, e_1, e_2, e_1 \oplus e_2\}$. Podle lemmatu 4.2 o jednoznačnosti vyjádření je $e_1 + e_2 = e_1 \oplus e_2$. Pro úplný popis operací $+$ a $\oplus$ v množině X_2 zbývá ukázat, jak mohou vypadat prvky $e_2 + e_2$ a $e_2 \oplus e_2$. Vzhledem k tomu, že je (podle lemmatu 4.6) $w(e_2 + e_2) < 2$ a $w(e_2 \oplus e_2) < 2$, musí být $e_2 + e_2, e_2 \oplus e_2 \in X_1$, a tedy

buď $e_2 + e_2 = 0$ nebo $e_2 + e_2 = e_1$, podobně $e_2 \oplus e_2 = 0$ nebo $e_2 \oplus e_2 = e_1$. Ve všech případech v X_2 tedy umíme vyjádřit operaci $+$ pomocí operace $\oplus$.

Indukční krok je následující: Předpokládejme, že pro všechny dvojice $x', y' \in X_i$ známe vyjádření $x' + y' = \sum_{j=1}^{i} z_j e_j = \bigoplus_{j=1}^{i} z'_j e_j$. V následujícím lemmatu ukážeme, že stačí umět vyjádřit pomocí operace $\oplus$ součet $e_{i+1} + x \in X_{i+1}$ pro všechna $x \in X_i$ a dále součet $e_{i+1} + e_{i+1} \in X_i$, a odtud pak odvodíme vyjádření pomocí operace $\oplus$ pro součet $x + y$ libovolné dvojice prvků $x, y \in X_{i+1}$.

Lemma 4.9. *Nechť je známé vyjádření prvků $x' + y'$, $x' + e_{i+1}$ a $e_{i+1} + e_{i+1}$ pomocí operace $\oplus$ pro každé $x', y' \in X_i$. Potom umíme vyjádřit pomocí operace $\oplus$ i součet $x + y$ pro libovolnou dvojici $x, y \in X_{i+1}$.*

Důkaz. Je $x = x' + x_{i+1}e_{i+1}$, $y = y' + y_{i+1}e_{i+1}$, kde $x', y' \in X_i$. Součet $x + y$ určíme následovně:

$$\begin{aligned} x + y &= (x' + x_{i+1}e_{i+1}) + (y' + y_{i+1}e_{i+1}) = \\ &= x' + y' + (x_{i+1}e_{i+1} + y_{i+1}e_{i+1}), \end{aligned}$$

kde $x' + y' \in X_i$, tedy tento součet umíme vyjádřit pomocí operace $\oplus$. Pro $x_{i+1}e_{i+1} + y_{i+1}e_{i+1}$ mohou nastat dva případy: Pokud je $x_{i+1} = y_{i+1}$, pak $x_{i+1}e_{i+1} + y_{i+1}e_{i+1} \in X_i$, tedy součet $x + y$ je prvkem X_i, a proto jej umíme vyjádřit pomocí operace $\oplus$. Je-li $x_{i+1} \neq y_{i+1}$, pak $x_{i+1}e_{i+1} + y_{i+1}e_{i+1} = e_{i+1}$, tedy prvek $x + y$ je součtem prvku množiny X_i a prvku e_{i+1}, který podle předpokladu umíme také vyjádřit pomocí operace $\oplus$. □

Zbývá určit vyjádření součtu $x' + e_{i+1}, x' \in X_i$. Ukážeme, že stačí znát vyjádření tohoto součtu pouze pro některé prvky $x \in X_i$, z nichž již odvodíme toto vyjádření pro zbylé prvky množiny X_i, a tedy i vyjádření součtu $x + y$ libovolných dvou prvků $x, y \in X_i$.

K tomuto účelu zavedeme pojem *přechodová funkce*.

Definice 4.10. Nechť $i \in \{0, \ldots, n-1\}$. *Přechodovou funkcí* od množiny X_i k množině X_{i+1} nazveme funkci

$$f_i : X_i \to X_i,$$

pro kterou platí

$$x + e_{i+1} = f_i(x) \oplus e_{i+1}$$

pro každé $x \in X_i$.

Tvrzení 4.11. *Pro každé $i = 0, \ldots, n-1$ je funkce f_i permutace na množině X_i, a tedy bijekce.*

Důkaz. Zřejmě stačí ukázat, že jde o prostou funkci. Zvolme libovolné $i \in \{0, \ldots, n-1\}$. Nechť $f_i(x) = f_i(y)$ pro $x, y \in X_i$. Pak

$$x + e_{i+1} = f_i(x) \oplus e_{i+1},$$

$$y + e_{i+1} = f_i(x) \oplus e_{i+1}.$$

Odtud plyne, že $x + e_{i+1} = y + e_{i+1}$, a tedy $x = y$. □

Ukážeme, že ne každá bijekce $X_i \to X_i$ je přechodovou funkcí a poté najdeme *minimální množinu* $m(X_i)$ prvků množiny X_i, která jednoznačně určuje přechodovou funkci f_i v tom smyslu, že známe-li vyjádření hodnot $f_i(y)$ pomocí operace $\oplus$ pro všechna $y \in m(X_i)$, pak známe vyjádření hodnot $f_i(x)$ pomocí operace $\oplus$ pro všechna $x \in X_i$.

Předně si uvědomme, že pro každé $x \in X$ a každé $i = 0, \ldots, n$ platí důležitá rovnost

$$x + X_i = x \oplus X_i, \tag{4.6}$$

která plyne z toho, že X_i je třída kongruence π_i.

Přímým důsledkem rovnosti (4.6) je rovnost

$$x + e_1 = x \oplus e_1, \tag{4.7}$$

která platí pro všechna $x \in X$. Je totiž $x + \{0, e_1\} = x + X_1 = x \oplus X_1 = x \oplus \{0, e_1\}$, a tedy $\{x, x + e_1\} = \{x, x \oplus e_1\}$. Z lemmatu 4.2 o jednoznačnosti vyjádření pak plyne rovnost (4.7).

Rovnost (4.7) platí pro všechna $x \in X$, a tedy speciálně pro prvky e_i, $i = 2, \ldots, n$. Proto platí

$$f_i(e_1) = e_1, \quad i = 2, \ldots, n. \tag{4.8}$$

Z rovnosti (4.7) plyne také další důležitá rovnost:

$$f_i(e_1 \oplus x) = e_1 \oplus f_i(x), \quad x \in X, i = 2, \ldots, n. \tag{4.9}$$

Je totiž $f_i(e_1 \oplus x) \oplus e_{i+1} = (e_1 \oplus x) + e_{i+1} \overset{(4.7)}{=} (e_1 + x) + e_{i+1} = e_1 + (x + e_{i+1}) \overset{(4.7)}{=} e_1 \oplus (x + e_{i+1}) = e_1 \oplus f_i(x) \oplus e_{i+1}$.

Z definice přechodové funkce a z rovnosti (4.6) plyne, že pro každé $j = 0, \ldots, i$ platí následující rovnost

$$X_j + e_{i+1} = X_j \oplus e_{i+1}, \tag{4.10}$$

neboli

$$f_i(X_j) = X_j. \tag{4.11}$$

Přechodové funkce mají několik důležitých vlastností, které dokážeme v následujícím lemmatu.

Lemma 4.12. *Pro každé $i = 0, \ldots, n-1$ platí*

$$f_i(0) = 0. \tag{4.12}$$

Pro každé $i, j = 0, \ldots, n-1$, $j < i$ platí

$$x \sim_{\pi_j} y \Leftrightarrow f_i(x) \sim_{\pi_j} f_i(y), \quad \forall x, y \in X_i. \tag{4.13}$$

Důkaz. Pro každé $i = 0, \ldots, n-1$ platí $0 + e_{i+1} = e_{i+1} = 0 \oplus e_{i+1}$, a tedy $f_i(0) = 0$.

Nechť $i \in \{1, \ldots, n-1\}$ a $0 \leq j < i$. Buďte dále $x, y \in X_i$ takové, že $x \sim_{\pi_j} y$. Pak

$$e_{i+1} \oplus f_i(x) = e_{i+1} + x \sim_{\pi_j} e_{i+1} + y = e_{i+1} \oplus f_i(y),$$

neboť π_i je kongruence algebry $(X, 0, \oplus, +)$. Odtud plyne, že $e_{i+1} \oplus f_i(x) \sim_{\pi_j} e_{i+1} \oplus f_i(y)$, a tedy $f_i(x) \sim_{\pi_j} f_i(y)$.

Opačnou implikaci dokážeme podobně. Nechť pro $i \in \{1, \ldots, n-1\}$, $0 \leq j < i$ a $x, y \in X_i$ je $f_i(x) \sim_{\pi_j} f_i(y)$. Potom

$$e_{i+1} + x = e_{i+1} \oplus f_i(x) \sim_{\pi_j} e_{i+1} \oplus f_i(y) = e_{i+1} + y,$$

a tedy $x \sim_{\pi_j} y$. □

Lemma 4.13. *Pro každé $j = 1, \ldots, i$ platí $f_i(X_{j-1} \oplus e_j) = X_{j-1} \oplus e_j$.*

Důkaz. K důkazu tohoto lemmatu použijeme předchozí lemma 4.12.

Mějme prvek $x \in X_{j-1} \oplus e_j$. Pak $x \sim_{\pi_{j-1}} e_j$, což je podle podmínky (4.13) ekvivalentní $f_i(x) \sim_{\pi_{j-1}} f_i(e_j)$. Dokážeme-li, že $f_i(e_j) \sim_{\pi_{j-1}} e_j$, pak bude $f_i(x) \sim_{\pi_{j-1}} e_j$, a tedy $f_i(x) \in X_{j-1} \oplus e_j$.

Pro prvek e_j platí $e_j \sim_{\pi_j} 0$, a proto $f_i(e_j) \sim_{\pi_j} f_i(0) = 0$. Je tedy $f_i(e_j) \in X_j$. Podle rovnosti (4.11) je $f_i(X_{j-1}) = X_{j-1}$. A protože f_i je prostá funkce, musí být $f_i(e_j) \notin X_{j-1}$, a proto $f_i(e_j) \sim_{\pi_{j-1}} e_j$.

Je tedy $f_i(x) \in X_{j-1} \oplus e_j$, a proto $f_i(X_{j-1} \oplus e_j) \subseteq X_{j-1} \oplus e_j$. Protože však funkce f_i je prostá, platí dokazovaná rovnost. □

Lemma 4.14. *Pro každé $j = 1, \ldots, i$ je buď*

$f_i(X_{j-1} \oplus e_{j+1}) = X_{j-1} \oplus e_{j+1}$,
$f_i(X_{j-1} \oplus e_j \oplus e_{j+1}) = X_{j-1} \oplus e_j \oplus e_{j+1}$

nebo

$f_i(X_{j-1} \oplus e_{j+1}) = X_{j-1} \oplus e_j \oplus e_{j+1}$,
$f_i(X_{j-1} \oplus e_j \oplus e_{j+1}) = X_{j-1} \oplus e_{j+1}$.

Důkaz. Zvolme libovolný prvek $x \in X_{j-1} \oplus e_{j+1}$. Podobně jako v důkazu předchozího lemmatu 4.13 bychom ukázali, že $f_i(x) \in X_{j+1}$ a $f_i(x) \notin X_j$. Je tedy $f_i(x) \in X_{j+1} \setminus X_j$. Podobně lze ukázat, že pro libovolné $x' \in X_{j-1} \oplus e_j \oplus e_{j+1}$ je $f_i(x') \in X_{j+1} \setminus X_j$.

Množina X_{j+1} je disjunktním sjednocením čtyř tříd kongruence π_{j-1}, $X_{j+1} = X_{j-1} \,\dot\cup\, (X_{j-1} \oplus e_j) \,\dot\cup\, (X_{j-1} \oplus e_{j+1}) \,\dot\cup\, (X_{j-1} \oplus e_j \oplus e_{j+1})$, kde $X_j = X_{j-1} \,\dot\cup\, (X_{j-1} \oplus e_j)$. Proto je

$$X_{j+1} \setminus X_j = (X_{j-1} \oplus e_{j+1}) \,\dot\cup\, (X_{j-1} \oplus e_j \oplus e_{j+1}). \tag{4.14}$$

Protože $x \in X_{j-1} \oplus e_{j+1}$, platí pro libovolný prvek $y \in X_{j-1} \oplus e_{j+1}$ ekvivalence $x \sim_{\pi_{j-1}} y$. Podle lemmatu 4.12 je tedy $f(x) \sim_{\pi_{j-1}} f(y)$. Předpokládejme, že $f_i(x) \in X_{j-1} \oplus e_{j+1}$. Pak $f_i(y) \sim_{\pi_{j-1}} f_i(x) \sim_{\pi_{j-1}} e_{j+1}$, a tedy $f_i(y) \in X_{j-1} \oplus e_{j+1}$.

Z prostoty přechodové funkce f_i potom plyne, že $f_i(X_{j-1} \oplus e_{j+1}) = X_{j-1} \oplus e_{j+1}$ a podle rovnosti (4.14) je tedy také $f_i(X_{j-1} \oplus e_j \oplus e_{j+1}) = X_{j-1} \oplus e_j \oplus e_{j+1}$.

Podobně lze ukázat druhou možnost. □

Ukážeme, že obdoba lemmatu 4.14 platí pro všechny množiny, které nejsou tvaru X_j, $j = 0, \ldots, n$.

Lemma 4.15. *Nechť $i, j \in \{1, \ldots, n-1\}$, $j < i$, a nechť je*

$$f_i(X_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_j \oplus \bigoplus_{k=j+1}^{i} x'_k e_k,$$

kde $x_k, x'_k \in \{0,1\}, k = j+1, \ldots, i$, a $\exists l, l' \in \{j+1, \ldots, i\} : x_l = x'_{l'} = 1$.

Pak buď

$f_i(X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x'_k e_k,$

$f_i(X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x'_k e_k,$

nebo

$f_i(X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x'_k e_k,$

$f_i(X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x'_k e_k.$

Důkaz. Tento důkaz bude podobný předchozímu důkazu.

Pro množinu $X_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k$ platí

$$X_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k = (X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k) \,\dot\cup\, (X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k). \tag{4.15}$$

Zvolme libovolný prvek $x \in X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k$. Pro libovolný prvek $y \in X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k$ platí $x \sim_{\pi_{j-1}} y$, a tedy podle lemmatu 4.12 je $f(x) \sim_{\pi_{j-1}} f(y)$.

Předpokládejme, že $f_i(x) \in X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k$. Pak $f_i(y) \sim_{\pi_{j-1}} f_i(x) \sim_{\pi_{j-1}} \bigoplus_{k=j+1}^{i} x_k e_k$, a tedy $f_i(y) \in X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k$.

Opět z prostoty přechodové funkce f_i potom plyne, že $f_i(X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_{j-1} \oplus \bigoplus_{k=j+1}^{i} x'_k e_k$. A podle rovnosti (4.15) je tedy $f_i(X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x_k e_k) = X_{j-1} \oplus e_j \oplus \bigoplus_{k=j+1}^{i} x'_k e_k$, kde jsme opět využili fakt, že f_i je prostá funkce.

Druhou možnost lze dokázat obdobně. □

K ilustraci chování funkce f_i slouží obrázek 4.2.

Nyní již můžeme určit minimální množinu $m(X_i)$ množiny X_i. Obraz množiny X_1 je určen jednoznačně. V každé další rozkladové třídě podle X_1 je třeba zvolit obraz jednoho z jejích prvků, obraz druhého prvku pak bude určen jednoznačně. Minimální množina $m(X_i)$ má tedy $2^{i-1} - 1$ prvků. Množinu $m(X_i)$ lze zkonstruovat například takto: Definujme $m_i(X_j)$ minimální množinu množiny X_j, na které je třeba znát hodnoty $f_i(x')$, $x' \in m_i(X_j)$, abychom znali hodnotu $f_i(x)$ pro všechna $x \in X_j$. Jistě je $m_i(X_2) = \{e_2\}$ a dále pro $j = 3, \ldots, i$

$$m_i(X_j) = m_i(X_{j-1}) \cup \big((\{0\} \cup m_i(X_{j-1})) \oplus e_j\big).$$

Pak $m(X_i) = m_i(X_i)$ je minimální množina X_i. Je tedy $m_i(X_3) = \{e_2, e_3, e_2 \oplus e_3\}$, $m_i(X_4) = \{e_2, e_3, e_2 \oplus e_3, e_4, e_2 \oplus e_4, e_3 \oplus e_4, e_2 \oplus e_3 \oplus e_4\}$ atd. Tedy $m_i(X_j)$ je množina všech nenulových „pozitivních lieárních kombinací“ prvků $\{e_2, \ldots, e_j\}$ v $(X_j, 0, \oplus)$, neboli $m_i(X_j) = \{\bigoplus_{k=2}^{j} x_k e_k; x_k \in \{0, 1\}$ pro $k = 2, \ldots, j\} \setminus \{0\}$.

Právě popsaný způsob konstrukce minimální množiny je jedním z několika možných. Ve zbytku této kapitoly budeme pod pojmem *minimální množina množiny* X_i rozumět množinu $m(X_i) = \{\bigoplus_{k=2}^{j} x_k e_k; x_k \in \{0, 1\}, k = 2, \ldots, j\} \setminus \{0\}$.

Z minimální množiny $m(X_i)$ můžeme zkonstruovat přechodovou funkci f_i následujícím algoritmem 4.16, jehož správnost plyne z lemmat 4.12 a 4.13 a rovnosti (4.9).

Algoritmus 4.16.
Vstup: Minimální množina $m(X_i)$ množiny X_i.
Výstup: Hodnoty přechodové funkce f_i na všech prvcích množiny X_i.
Postup:

1. Pro $j = 1, \ldots, i$:

2. Polož $Z = m(X_j) \setminus m(X_{j-1})$.

3. Dokud $Z \neq \emptyset$:

4. Zvol $x \in Z$.

5. Zvol $f_i(x)$ tak, aby

   - $f_i(x) \sim_{\pi_{j-1}} e_j$,
   - $f_i(x) \not\sim_{\pi_1} f_i(y), \quad \forall y \in m(X_j) \setminus m(X_{j-1}) \setminus Z$,
   - $x \sim_{\pi_k} y \Rightarrow f_i(x) \sim_{\pi_k} f_i(y)$,
     $\forall k = 0, \dots i-1,\ y \in m(X_j) \setminus m(X_{j-1}) \setminus Z$.

6. Polož $f_i(e_1 \oplus x) = f_i(x) \oplus e_1$.

7. Polož $Z = Z \setminus \{x\}$.

Každá přechodová funkce f_i od X_i k X_{i+1} spolu s vyjádřením prvků $e_{i+1} + e_{i+1}$ a $e_{i+1} \oplus e_{i+1}$ pomocí operace $\oplus$ určuje jeden *typ přechodu* od X_i k X_{i+1}. V následující podkapitole popíšeme, jak lze v závislosti na typu přechodu od X_i k X_{i+1} zkonstruovat tabulku pro rozšíření řešení soustavy diferenčních rovnic modulo X_{i+1} na její řešení modulo X_i.

Známe-li soubor přechodových funkcí f_i a prvky $e_i + e_i$, $e_i \oplus e_i$, $i = 2, \dots, n-1$, dokážeme převést souřadnice libovolného prvku $x \in X$ vzhledem k bázi E_X příslušné operaci $\oplus$ na souřadnice tohoto prvku vzhledem k bázi E_X příslušné operaci $+$ (viz definici 4.4), a to následujícím algoritmem:

Algoritmus 4.17.
Vstup: Vyjádření prvku $x \in X$ pomocí operace $\oplus$.
Výstup: Vyjádření prvku x pomocí operace $+$.
Postup:

1. Pro $i = 1, \dots, n$:

2. Polož $x'_i = 0$.

3. Polož $z = x$.

4. Dokud $w(z) > 0$:

5. Polož $x'_{w(z)} = 1$.

6. Polož $z = z - e_{w(z)}$.

7. `Vrať` $x = \sum_{i=1}^{n} x'_i e_i$.

Známe-li přechodovou funkci f_i a prvky $e_i + e_i$, $e_i \oplus e_i$ pro $i \in \{2, \ldots, n-1\}$, dokážeme v polynomiálním čase najít prvek $-e_i$. Proto má algoritmus 4.17 polynomiální časovou složitost.

Tvrzení 4.18. *Nechť $(X, 0, \oplus)$ je abelovská grupa na množině X mohutnosti 2^n a π_i, $i = 0, \ldots, n$ jsou takové kongruence grupy $(X, 0, \oplus)$, že $\iota_X = \pi_0 \subset \pi_1 \subset \cdots \subset \pi_n = X \times X$. Pro každé $i = 0, \ldots, n$ označme symbolem X_i třídu kongruence π_i, která obsahuje prvek 0 a pro každé $j = 1, \ldots, n$ zvolme prvek $e_j \in X_j \setminus X_{j-1}$. Nechť dále $f_i : X_i \to X_i$, $i = 0, \ldots, n-1$, je soubor funkcí, pro které platí*

$$f_i(0) = 0 \quad \forall i = 0, \ldots, n-1,$$

$$x \sim_{\pi_j} y \Leftrightarrow f_i(x) \sim_{\pi_j} f_i(y) \quad \forall x, y \in X_i; i, j = 0, \ldots, n-1, j < i.$$

Předpokládejme dále, že $g(i)$ je prvek X_{i-1} pro každé $i = 1, \ldots, n$.

Potom existuje právě jeden hustý abelovský grupový pár $(X, 0, \oplus)$, $(X, 0, +)$ takový, že f_{i-1} jsou přechodové funkce tohoto grupového páru a $e_i + e_i = g(i)$ pro každé $i = 1, \ldots, n$.

Důkaz. Operaci $+$ definujeme na každé množině X_i, $i = 1, \ldots, n$, indukcí podle i.

Pro $i = 1$ je $X_i = \{0, e_1\}$. A protože $e_1 + e_1 = g(1) \in X_0$, je $e_1 + e_1 = 0$, a tedy také $-e_1 = e_1$. Tím máme definovanou abelovskou grupu $(X_1, 0, +)$.

Předpokládejme, že máme definovanou abelovskou grupu $(X_i, 0, +)$. Chceme ji rozšířit na abelovskou grupu $(X_{i+1}, 0, +)$.

Zvolme tedy $x, y \in X_{i+1}$. Součet $x + y$ definujeme následovně:

- Je-li $x, y \in X_i$, máme součet $x + y$ definovaný podle indukčního předpokladu.
- Je-li $x \in X_i$ a $y \in X_{i+1} \setminus X_i$, je $y = y' \oplus e_{i+1}$, kde $y' \in X_i$. V tomto případě definujeme $y + x = x + y = f_i(x + f_i^{-1}(y')) \oplus e_{i+1}$.
- A nakonec, jsou-li $x, y \in X_{i+1} \setminus X_i$, je $x = x' \oplus e_{i+1}$ a $y = y' \oplus e_{i+1}$ pro nějaká $x', y' \in X_i$. Pak definujeme $x+y = f_i^{-1}(x') + f_i^{-1}(y') + g(i+1)$. Všechny sčítance na pravé straně předchozí rovnosti leží v X_i, kde je operace $+$ již definovaná, proto je tato definice korektní. Navíc X_i je komutativní grupa, takže $x + y = y + x$.

Máme tedy na X_{i+1} komutativní binární operaci s neutralním prvkem 0.

K dokončení důkazu, že $(X_{i+1}, 0, +)$ je abelovská grupa, zbývá dokázat, že operace $+$ je asociativní v množině X_{i+1} a že ke každému prvku $x \in X_{i+1}$ existuje inverzní prvek $-x \in X_{i+1}$ vzhledem k operaci $+$.

Dokažme tedy asociativitu operace $+$ v množině X_{i+1}, tedy, že pro libovolná $x, y, z \in X_{i+1}$ platí

$$(x + y) + z = x + (y + z). \tag{4.16}$$

Díky komutativitě operace $+$ na množině X_{i+1} stačí dokázat rovnost (4.16) rozborem následujících čtyř případů:

- Je-li $x, y, z \in X_i$, pak rovnost (4.16) platí podle indukčního předpokladu.
- Je-li $x, y \in X_i$ a $z \in X_{i+1} \setminus X_i$, pak $z = z' \oplus e_{i+1}$ pro nějaké $z' \in X_i$. Z definice operace $+$ na množině X_{i+1} a její asociativity na množině X_i plyne

$$\begin{aligned}(x + y) + z &= (x + y) + (z' \oplus e_{i+1}) = \\ &= f_i\big((x + y) + f_i^{-1}(z')\big) \oplus e_{i+1} = \\ &= f_i\big(x + (y + f_i^{-1}(z'))\big) \oplus e_{i+1} = \\ &= x + (y + f_i^{-1}(z') + e_{i+1}) = x + (y + z),\end{aligned}$$

  neboť $x, y, f_i^{-1}(z') \in X_i$.
- Pro $x \in X_i$ a $y, z \in X_{i+1} \setminus X_i$ je $y = y' \oplus e_{i+1}$, $z = z' \oplus e_{i+1}$, kde $y', z' \in X_i$. Opět podle definice operace $+$ platí

$$\begin{aligned}(x + y) + z &= (f_i(x + f_i^{-1}(y')) \oplus e_{i+1}) + (z' \oplus e_{i+1}) = \\ &= f_i^{-1}\big(f_i(x + f_i^{-1}(y'))\big) + f_i^{-1}(z') + g(i + 1) = \\ &= x + f_i^{-1}(y') + f_i^{-1}(z') + g(i + 1) = \\ &= x + (f_i^{-1}(y') + f_i^{-1}(z') + g(i + 1)) = x + (y + z),\end{aligned}$$

  kde jsme využili komutativitu operace $+$ v X_{i+1} a její asociativitu v X_i a skutečnost, že $x, f_i^{-1}(y'), f_i^{-1}(z'), g(i + 1) \in X_i$.
- Konečně, jsou-li $x, y, z \in X_{i+1} \setminus X_i$, pak opět z definice operace $+$ na množině X_{i+1}, její asociativity na množině X_i a komutativity na množině X_{i+1} plyne

$$\begin{aligned}(x + y) + z &= (f_i^{-1}(x') + f_i^{-1}(y') + g(i + 1)) + z = \\ &= f_i\big((f_i^{-1}(x') + f_i^{-1}(y') + g(i + 1)) + f_i^{-1}(z')\big) \oplus e_{i+1} = \\ &= f_i\big(f_i^{-1}(x') + (f_i^{-1}(y') + f_i^{-1}(z') + g(i + 1))\big) \oplus e_{i+1} = \\ &= f_i\big(f_i^{-1}(x') + (y + z)\big) \oplus e_{i+1} = x + (y + z),\end{aligned}$$

neboť $f_i^{-1}(x'), f_i^{-1}(y'), f_i^{-1}(z'), g(i+1) \in X_i$.

Nyní dokážeme, že pro každý prvek $x \in X_{i+1}$ existuje v množině X_{i+1} prvek k němu inverzní vzhledem k operaci $+$.

Je-li $x \in X_i$, pak k němu existuje inverzní prvek vzhledem k operaci $+$ v $X_i \subset X_{i+1}$ podle indukčního předpokladu.

Je-li $x \in X_{i+1} \setminus X_i$, pak je $x = x' \oplus e_{i+1}$ pro nějaké $x' \in X_i$. K prvku x je inverzní prvek $z = z' \oplus e_{i+1}$, kde $z' = f_i(-f_i^{-1}(x') - g(i+1))$. Oba prvky v závorce jsou z X_i, takže známe prvky k nim opačné. Přímým výpočtem ověříme, že $x + z = 0$. Je totiž

$$\begin{aligned} x + z &= (x' \oplus e_{i+1}) + (z' \oplus e_{i+1}) = \\ &= (x' \oplus e_{i+1}) + \big(f_i(-f_i^{-1}(x') - g(i+1)\big) \oplus e_{i+1}) = \\ &= f_i^{-1}(x') + (f_i^{-1}(x') - g(i+1)) + g(i+1) = 0. \end{aligned}$$

Tím je definována grupa $(X_{i+1}, 0, +)$, a tedy ukončen indukční krok v její definici.

Zbývá tedy dokázat, že π_i, $i = 0, \ldots, n$, jsou společné kongruence grupového páru $(X, 0, \oplus)$, $(X, 0, +)$. To uděláme opět indukcí podle i. A to tak, že dokážeme, že pro každé $i = 1, \ldots, n$ platí, že pro každé $0 \leq j \leq i$ je $\pi_j \cap (X_i \times X_i)$ společná kongruence grupového páru $(X, 0, \oplus)$, $(X, 0, +)$.

Nechť $i = 1$. Potřebujeme dokázat, že pro každou dvojici $(x, y) \in X_1 \times X_1$ platí

$$(x, y) \in \pi_1 \Rightarrow x - y \in X_1$$

a

$$(x, y) \in \pi_0 \Rightarrow x - y \in X_0.$$

To je však snadné, neboť x i $-y$ jsou prvky X_1, a tedy jejich součet je také prvkem X_1. Je-li $(x, y) \in \pi_0$, znamená to, že $x \ominus y \in X_0$. Pak nutně $x = y = 0$ nebo $x = y = e_1$. Pro oba případy je $x - y = 0 \in X_0$.

Předpokládejme, že pro $i \in \{1, \ldots, n-1\}$ platí, že pro každé $0 \leq j \leq i$ je $\pi_j \cap (X_i \times X_i)$ společná kongruence grupového páru $(X, 0, \oplus)$, $(X, 0, +)$. Dokažme, že také pro $i+1$ platí, že pro každé $0 \leq j \leq i+1$ je $\pi_j \cap (X_{i+1} \times X_{i+1})$ společná kongruence grupového páru $(X, 0, \oplus)$, $(X, 0, +)$.

Pro $j = i + 1$ je třeba dokázat, že pro každé $(x, y) \in X_{i+1} \times X_{i+1}$ platí $(x, y) \in \pi_{i+1} \Rightarrow x - y \in X_{i+1}$. Protože však $x, -y \in X_{i+1}$, je také $x - y \in X_{i+1}$.

Je-li $j \leq i$ a $x, y \in X_{i+1}, (x, y) \in \pi_j$, pak je třeba dokázat, že $x - y \in X_j$. Z předpokladu $(x, y) \in \pi_j$ plyne, že $x \ominus y \in X_j \subseteq X_i$. To znamená,

že buď $x, y \in X_i$, a pak $x - y \in X_j$ podle indukčního předpokladu, nebo $x = x' \oplus e_{i+1}$ a $y = y' \oplus e_{i+1}$, kde $x', y' \in X_i$. Z předpokladu $x \ominus y \in X_j$ plyne, že $x' \ominus y' \in X_j$, a tedy $(x', y') \in \pi_j$ podle indukčního předpokladu a $(f_i^{-1}(x'), f_i^{-1}(y')) \in \pi_j$ podle druhého předpokladu o funkci f_j, a tedy také $f_i^{-1}(x') - f_i^{-1}(y') \in X_j$.

Ukážeme-li, že $x - y = f_i^{-1}(x') - f_i^{-1}(y')$, bude $x - y \in X_j$, a tedy budeme mít dokázáno, že π_j je společná kongruence grupového páru $(X_{i+1}, 0, \oplus), (X_{i+1}, 0, +)$.

Podle definice sčítání a opačného prvku v X_{i+1} je

$$\begin{aligned} x - y &= (x' \oplus e_{i+1}) - (y' \oplus e_{i+1}) = \\ &= (x' \oplus e_{i+1}) + f_i\big(- f_i^{-1}(y') - g(i+1)\big) \oplus e_{i+1} = \\ &= f_i^{-1}(x') + f_i^{-1}\big(f_i(-f_i^{-1}(y') - g(i+1))\big) + g(i+1) = \\ &= f_i^{-1}(x') - f_i^{-1}(y'). \end{aligned}$$

Dokázali jsme tedy, že $(X, 0, \oplus), (X, 0, +)$ je hustý abelovský grupový pár.

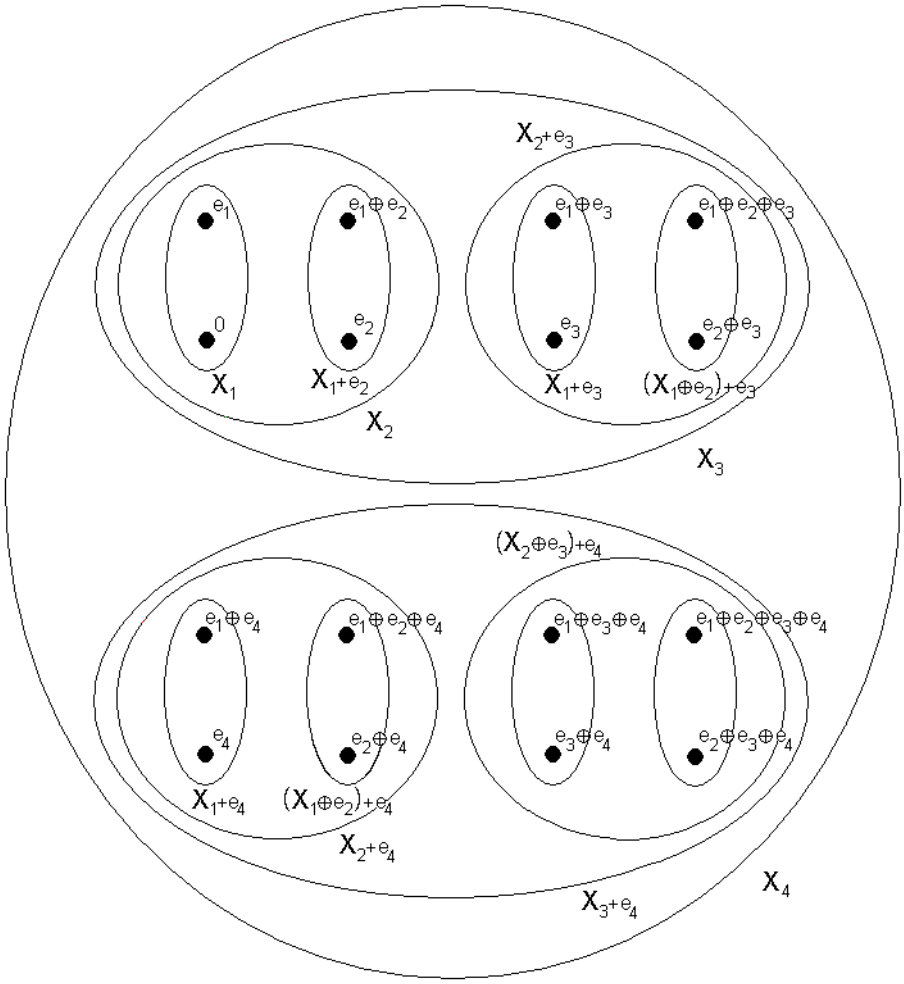
Z definice sčítání prvků $x \in X_i$ a $y \in X_{i+1} \setminus X_i$ a prvního předpokladu o funkci f_i plyne, že

$$\begin{aligned} x + e_{i+1} = x + (0 \oplus e_{i+1}) &= f_i(x + f_i^{-1}(0)) \oplus e_{i+1} = \\ &= f_i(x + 0) \oplus e_{i+1} = f_i(x) \oplus e_{i+1}. \end{aligned}$$

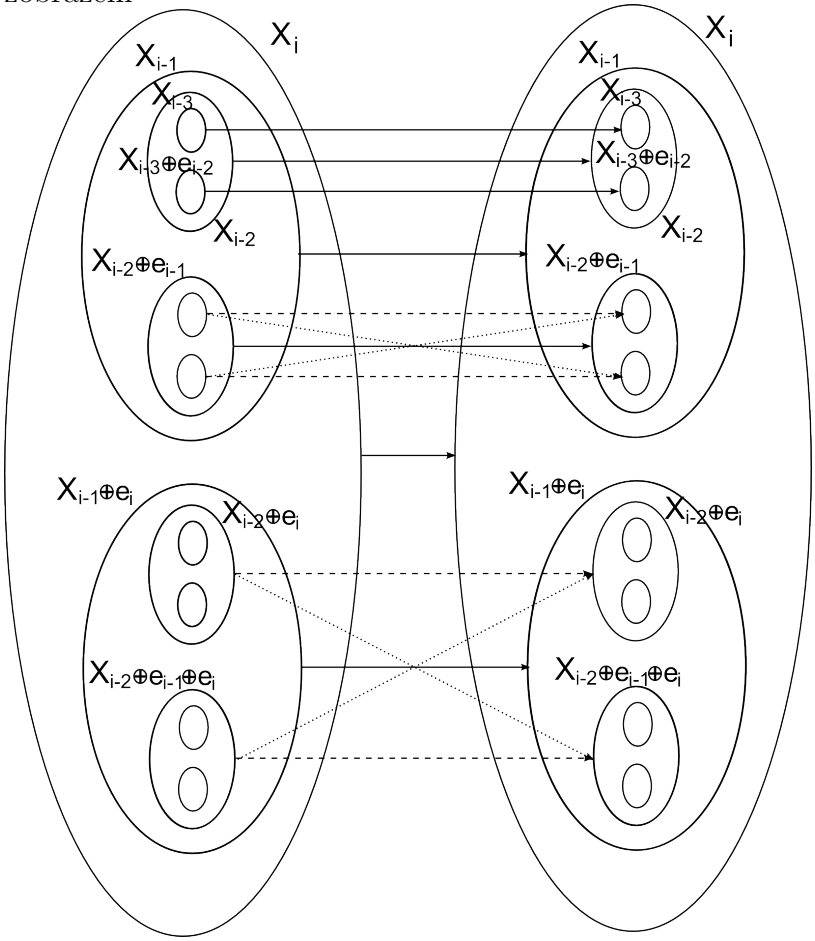
Odtud plyne, že f_i, $i = 0, \ldots, n-1$ jsou přechodové funkce hustého abelovského grupového páru $(X, 0, \oplus), (X, 0, +)$.

Jednoznačnost tohoto grupového páru plyne z jeho konstrukce. □

Obrázek 4.1: Rozkladové třídy X_4 podle X_1, X_2 a X_3



Obrázek 4.2: Přechodová funkce. Plné šipky znázorňují jednoznačnost zobrazení funkcí f_i, přerušované šipky znázorňují alternativní možnosti zobrazení



4.2 Řešení soustav diferenčních rovnic v hustém abelovském grupovém páru

Nyní přistoupíme k řešení soustavy rovnic

$$(x \oplus \alpha[k]) + (y \oplus \beta[k]) = (x + y) \oplus \gamma[k], \tag{4.17}$$

s neznámými $x, y \in X$ a parametry $\alpha[k], \beta[k], \gamma[k] \in X$, $k = 1, \ldots, m$, v hustém abelovském grupovém páru $(X, 0, \oplus)$, $(X, 0, +)$. Stejně jako v kapitole 3 nejprve najdeme všechna řešení rovnice typu

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma \tag{4.18}$$

a následně určíme množinu řešení soustavy (4.17) jako průnik množin řešení jednotlivých rovnic soustavy.

V celé kapitole budeme předpokládat znalost vyjádření prvků α, β a γ pomocí operace $\oplus$, znalost souboru přechodových funkcí f_i a prvků $e_{i+1} \oplus e_{i+1}$, $e_{i+1} + e_{i+1}$ pro $i = 0, \ldots, n-1$.

Při znalosti vyjádření daného prvku pomocí operace $\oplus$ a souboru přechodových funkcí f_i a prvků $e_{i+1} \oplus e_{i+1}$, $e_{i+1} + e_{i+1}$ pro $i = 0, \ldots, n-1$ lze v čase polynomiálním vzhledem k n určit vyjádření tohoto prvku pomocí operace $+$. Naopak, při znalosti přechodových funkcí f_i a prvků $e_{i+1} \oplus e_{i+1}$, $e_{i+1} + e_{i+1}$ pro $i = 0, \ldots, n-1$ a vyjádření daného prvku pomocí operace $+$ lze v polynomiálním čase (vzhledem k n) určit vyjádření tohoto prvku pomocí operace $\oplus$. Proto budeme převod mezi vyjádřením pomocí operace $\oplus$ a vyjádřením pomocí operace $+$ nebo naopak považovat za jeden krok algoritmu na nalezení všech řešení soustavy (4.17).

Při hledání řešení rovnice (4.18) budeme opět postupovat indukcí, stejně jako v předchozí kapitole.

Než zformulujeme obdobu tvrzení 3.1 pro hustý abelovský grupový pár, dokážeme ještě pomocné lemma.

Označení 4.19. Symbolem $*$ označíme běžnou operaci xor na množině $\{0, 1\}$.

Lemma 4.20. *Buď $i \in \{1, \ldots, n\}$. Pro libovolnou množinu $Y = \{x^1, x^2, \ldots, x^k\}, x_i \in \{0, 1\}$ pro $i = 1, \ldots, k$, $k \in \mathbb{N}$, platí*

$$x^1 e_i \oplus x^2 e_i \oplus \cdots \oplus x^k e_i = (x^1 * x^2 * \cdots * x^k) e_i \oplus u \tag{4.19}$$

a

$$x^1 e_i + x^2 e_i + \cdots + x^k e_i = (x^1 * x^2 * \cdots * x^k) e_i \oplus v, \tag{4.20}$$

kde $u, v \in X_{i-1}$.

Důkaz. Dokážeme pouze rovnost (4.19), neboť důkaz rovnosti (4.20) je obdobný. Důkaz provedeme indukcí podle počtu nenulových členů množiny Y, který si označíme j. Bez újmy na obecnosti můžeme předpokládat, že $x^1 = \cdots = x^j = 1$ a $x^{j+1} = \ldots = x^k = 0$. Je tedy $x^1e_i \oplus \cdots \oplus x^ke_i = x^1e_i \oplus \cdots \oplus x^je_i$.

Pro $j = 0, 1$ je rovnost (4.19) zřejmá.

Pro $j = 2$ položíme $u = e_i \oplus e_i \in X_{i-1}$. Pak je $x^1e_i \oplus x^2e_i \oplus \cdots \oplus x^ke_i = e_i \oplus e_i = (1 * 1)e_i \oplus u = u$. Rovnost (4.19) tedy platí i pro $j = 2$.

Předpokládejme, že rovnost (4.19) platí pro $j \in \{0, \ldots, k-1\}$ a dokažme, že platí také pro $j+1$. Je tedy $x^1e_i \oplus \cdots \oplus x^ke_i = x^1e_i \oplus \cdots \oplus x^je_i = (j \bmod 2)e_i \oplus u'$, $u' \in X_{i-1}$.

Je-li j sudé, pak položíme $u = u'$. Podle předpokladu je $x^1e_i \oplus x^2e_i \oplus \cdots \oplus x^je_i \oplus e_i = (j \bmod 2)e_i \oplus u' \oplus e_i = e_i \oplus u' = ((j+1) \bmod 2)e_i \oplus u' = ((j+1) \bmod 2)e_i \oplus u$.

Pro j liché položíme $u = u' \oplus e_i \oplus e_i$. Máme $x^1e_i \oplus x^2e_i \oplus \cdots \oplus x^je_i \oplus e_i = (j \bmod 2)e_i \oplus u' \oplus e_i = e_i \oplus u' \oplus e_i = u = ((j+1) \bmod 2)e_i \oplus u$.

Rovnost (4.19) tedy platí i pro $j+1$ nenulových členů množiny Y. □

Nyní dokážeme obdobu tvrzení 3.1 pro hustý abelovský grupový pár.

V celém následujícím textu budeme předpokládat, že prvky $\alpha, \beta, \gamma, x, y$ mají následující vyjádření pomocí operace $\oplus$: $\alpha = \bigoplus_{j=1}^{n} \alpha_j e_j, \beta = \bigoplus_{j=1}^{n} \beta_j e_j, \gamma = \bigoplus_{j=1}^{n} \gamma_j e_j, x = \bigoplus_{j=1}^{n} x_j e_j, y = \bigoplus_{j=1}^{n} y_j e_j$.

Tvrzení 4.21. *Nutnou a postačující podmínkou pro řešitelnost rovnice (4.18) modulo X_{n-1} je $\alpha_n * \beta_n * \gamma_n = 0$. Řešením modulo X_{n-1} je pak libovolná dvojice $x, y \in X$.*

Důkaz. Množina X/X_{n-1} je dvouprvková, proto

$$u + v = u \oplus v \pmod{X_{n-1}} \quad \forall u, v \in X. \tag{4.21}$$

Je tedy

$$x \oplus \alpha \oplus y \oplus \beta = (x \oplus \alpha) + (y \oplus \beta) = ((x+y) \oplus \gamma) = x \oplus y \oplus \gamma \pmod{X_{n-1}}.$$

To znamená, že pro řešitelnost rovnice (4.18) je třeba, aby se rovnaly přirozené reprezentanty $r_n^{\oplus}(x \oplus \alpha \oplus y \oplus \beta)$ a $r_n^{\oplus}(x \oplus y \oplus \gamma)$.

Z lemmatu 4.20 plyne, že $r_n^{\oplus}(x \oplus \alpha \oplus y \oplus \beta) = (x_n * \alpha_n * y_n * \beta_n)e_n$, neboť $r_n^{\oplus}(x \oplus \alpha \oplus y \oplus \beta) = r_n^{\oplus}(r_n^{\oplus}(x) \oplus r_n^{\oplus}(\alpha) \oplus r_n^{\oplus}(y) \oplus r_n^{\oplus}(\beta)) = r_n^{\oplus}(x_ne_n \oplus \alpha_ne_n \oplus y_ne_n \oplus \beta_ne_n) = (x_n * \alpha_n * y_n * \beta_n)e_n$. Podobně lze ukázat, že $r_n^{\oplus}(x \oplus y \oplus \gamma) = (x_n * y_n * \gamma_n)e_n$.

Rovnice (4.18) je tedy řešitelná modulo X_{n-1}, právě když

$$x_n * \alpha_n * y_n * \beta_n = x_n * y_n * \gamma_n,$$

což je ekvivalentní

$$\alpha_n * \beta_n * \gamma_n = 0.$$

Protože tato rovnost nezávisí na x, y, je v případě její platnosti řešením rovnice (4.18) modulo X_{n-1} libovolná dvojice $x, y \in X$. □

Nyní dokážeme několik pomocných lemmat a poté popíšeme indukční krok algoritmu na nalezení všech řešení soustavy (4.17).

Lemma 4.22. *Pro libovolné dva prvky* $x = \bigoplus_{k=1}^{n} x_k e_k$, $y = \bigoplus_{k=1}^{n} y_k e_k \in X$ *platí*

$$x \oplus y = \bigoplus_{k=1}^{n} (x_k * y_k * c_k^k) e_k, \tag{4.22}$$

kde $\mathbf{c}^k = \bigoplus_{j=1}^{k} c_j^k e_j \in X_k$, $k = 1, \ldots, n-1$, *je přenos z* $(k+1)$*-ní souřadnice při sčítání* $x \oplus y$. *Definujeme* $\mathbf{c}^n = 0$.

Důkaz. Lemma dokážeme s využitím lemmatu 4.20. Je

$$\begin{aligned}
x \oplus y &= (x_n e_n \oplus \cdots \oplus x_1 e_1) \oplus (y_n e_n \oplus \cdots \oplus y_1 e_1) = \\
&= (x_n e_n \oplus y_n e_n) \oplus (x_{n-1} e_{n-1} \oplus y_{n-1} e_{n-1}) \oplus \cdots \oplus (x_1 e_1 \oplus y_1 e_1) \overset{4.20}{=} \\
&= (x_n * y_n) e_n \oplus \mathbf{c}^{n-1} \oplus (x_{n-1} e_{n-1} \oplus y_{n-1} e_{n-1}) \oplus \cdots \oplus \\
&\oplus (x_1 e_1 \oplus y_1 e_1) \overset{4.20}{=} (x_n * y_n) e_n \oplus (x_{n-1} * y_{n-1} * c_{n-1}^{n-1}) e_{n-1} \oplus \mathbf{c}^{n-2} \oplus \\
&\oplus (x_{n-2} e_{n-2} \oplus y_{n-2} e_{n-2}) \oplus \cdots \oplus (x_1 e_1 \oplus y_1 e_1) \overset{4.20}{=} \cdots \overset{4.20}{=} \\
&= \bigoplus_{k=1}^{n} (x_k * y_k * c_k^k) e_k.
\end{aligned}$$

Z předchozího výpočtu, definice přirozeného reprezentantu (4.2) a přenosu (4.3) plyne, že $\mathbf{c}^k$ je je přenos z $(k+1)$-ní souřadnice při sčítání $x \oplus y$ pro každé $k = 1, \ldots, n-1$. □

Obdobné lemma dokážeme i pro operaci $+$.

Lemma 4.23. *Pro libovolné dva prvky* $x = \sum_{k=1}^{n} x_k e_k$, $y = \sum_{k=1}^{n} y_k e_k \in X$ *platí*

$$x + y = \sum_{k=1}^{n} (x_k * y_k * d_k^k) e_k, \tag{4.23}$$

kde $\mathbf{d}^k = \sum_{j=1}^{k} d_j^k e_j \in X_k$, $k = 1, \ldots, n-1$. *Definujeme* $\mathbf{d}^n = 0$.

Důkaz. Toto lemma dokážeme, podobně jako předchozí lemma, s využitím lemmatu 4.20. Je

$$\begin{aligned}
x+y &= (x_n e_n + \cdots + x_1 e_1) + (y_n e_n + \cdots + y_1 e_1) = \\
&= (x_n e_n + y_n e_n) + (x_{n-1} e_{n-1} + y_{n-1} e_{n-1}) + \cdots + (x_1 e_1 + y_1 e_1) \overset{4.20}{=} \\
&= (x_n * y_n) e_n + \mathbf{d}^{n-1} + (x_{n-1} e_{n-1} + y_{n-1} e_{n-1}) + \cdots + \\
&+ (x_1 e_1 + y_1 e_1) \overset{4.20}{=} (x_n * y_n) e_n + (x_{n-1} * y_{n-1} * d_{n-1}^{n-1} e_{n-1}) + \mathbf{d}^{n-2} + \\
&+ (x_{n-1} e_{n-1} + y_{n-1} e_{n-1}) + \cdots + (x_1 e_1 + y_1 e_1) \overset{4.20}{=} \cdots \overset{4.20}{=} \\
&= \sum_{k=1}^{n} (x_k * y_k * d_k^k) e_k.
\end{aligned}$$

□

Z definice přenosu (4.5) a reprezentantu (4.4) plyne, že prvek $\mathbf{d}^k$ z předchozího lemmatu je přenos z $(k+1)$-ní souřadnice při sčítání $x+y$.

Nyní dokážeme užitečné lemma s velmi důležitým důsledkem.

Lemma 4.24. *Pro každé $x \in X$ a každé $i = 1, \ldots n$ platí*

$$w((x \oplus e_i) - x) = i \tag{4.24}$$

a

$$w((x + e_i) \ominus x) = i. \tag{4.25}$$

Důkaz. Dokážeme pouze rovnost (4.24). Důkaz rovnosti (4.25) je obdobný.

Zvolme libovolný prvek $x \in X$. Protože π_i je kongruence algebry $(X, 0, \oplus, +)$, platí:

$$e_i \not\sim_{\pi_{i-1}} 0 \Rightarrow x \oplus e_i \not\sim_{\pi_{i-1}} x \Rightarrow (x \oplus e_i) - x \not\sim_{\pi_{i-1}} x - x = 0.$$

Je tedy $(x \oplus e_i) - x \notin X_{i-1}$, a tedy $w((x \oplus e_i) - x) \geq i$.

Zároveň však $e_i \sim_{\pi_i} 0$, a tedy $x \oplus e_i \sim_{\pi_i} x$, což je ekvivalentní $(x \oplus e_i) - x \in X_i$. To znamená, že $w((x \oplus e_i) - x) \leq i$. Dokázali jsme tedy, že je $w((x \oplus e_i) - x) = i$. □

Důsledek 4.25. *Nechť $x = \bigoplus_{k=1}^{n} x_k e_k = \sum_{k=1}^{n} x'_k e_k$ jsou vyjádření prvku x pomocí operací $\oplus$ a $+$. Nechť dále $i \in \{1, \ldots, n\}$. Potom pro $x + e_i = \bigoplus_{k=1}^{n} t_k e_k$ a $x \oplus e_i = \sum_{k=1}^{n} z_k e_k$ platí*

$$t_k = x_k, z_k = x'_k \text{ pro } k = i+1, \ldots, n, \tag{4.26}$$

$$t_i \neq x_i, z_i \neq x'_i. \tag{4.27}$$

Důkaz. Tento důsledek dokážeme opět pouze pro koeficienty z_k, $k = i, \ldots, n$, neboť pro koeficienty t_k, $k = i, \ldots n$, by byl důkaz obdobný.

Kdyby existoval index $j \in \{i+1, \ldots, n\}$ takový, že $z_j \neq x'_j$, bylo by $w((x \oplus e_i) - x) = j > i$, což by byl spor s předchozím lemmatem. Podmínka (4.26) je tedy dokázaná.

Kdyby $z_i = x'_i$, pak by (kvůli podmínce (4.26)) bylo $w((x \oplus e_i) - x) < i$. To je opět spor s lemmatem 4.24, a tedy platí i podmínka (4.27). □

Protože v dalším textu budeme pracovat střídavě s vyjádřením prvků pomocí operace $+$ a pomocí operace $\oplus$, zavedeme následující označení.

Označení 4.26. Pro libovolný prvek $x \in X$ a $i = 1, \ldots, n$ označíme i-tý koeficient vyjádření prvku x pomocí operace $\oplus$ symbolem $(x)_i^{\oplus}$ a symbolem $(x)_i^{+}$ označíme i-tý koeficient vyjádření prvku x pomocí operace $+$.

Poznámka 4.27. Všimněme si, že pro každý prvek $x \in X$ a každé $i \in \{1, \ldots, n\}$ je $(r_i^{+}(x))_i^{+} = (x)_i^{+}$ a $(r_i^{\oplus}(x))_i^{\oplus} = (x)_i^{\oplus}$.

Lemma 4.28. *Pro libovolné dva prvky* $x = \sum_{k=1}^{n} x_k e_k$, $y = \sum_{k=1}^{n} y_k e_k \in X$ *a libovolné* $i \in \{1, \ldots, n\}$ *platí*

$$r_i^{+}(x) + r_i^{+}(y) = r_i^{+}(x+y) + \mathbf{d}^{i-1}, \tag{4.28}$$

kde $\mathbf{d}^{i-1} = \sum_{j=1}^{i-1} d_j^k e_j \in X_{i-1}$, $k = 1, \ldots, n-1$, *a kde definujeme* $\mathbf{d}^n = 0$. *Pro každé* $i = 1, \ldots n$ *je*

$$(x+y)_i^{+} = x_i * y_i * d_i^i. \tag{4.29}$$

Důkaz. Toto lemma dokážeme podobně jako lemma 4.23. Je

$$\begin{aligned}
r_i^{+}(x) + r_i^{+}(y) &= (x_n e_n + \cdots + x_i e_i) + (y_n e_n + \cdots + y_i e_i) = \\
&= (x_n e_n + y_n e_n) + (x_{n-1} e_{n-1} + y_{n-1} e_{n-1}) + \cdots + (x_i e_i + y_i e_i) \overset{4.20}{=} \\
&= (x_n * y_n) e_n + \mathbf{d}^{n-1} + (x_{n-1} e_{n-1} + y_{n-1} e_{n-1}) + \cdots + \qquad (4.30) \\
&+ (x_i e_i + y_i e_i) \overset{4.20}{=} (x_n * y_n) e_n + (x_{n-1} * y_{n-1} * d_{n-1}^{n-1} e_{n-1}) + \\
&+ \mathbf{d}^{n-2} + (x_{n-1} e_{n-1} + y_{n-1} e_{n-1}) + \cdots + (x_i e_i + y_i e_i) \overset{4.20}{=} \cdots \overset{4.20}{=} \\
&= \sum_{k=i}^{n} (x_k * y_k * d_k^k) e_k + \mathbf{d}^{i-1}.
\end{aligned}$$

A protože z lemmatu 4.23 plyne, že $r_i^{+}(x+y) = \sum_{k=i}^{n} (x_k * y_k * d_k^k) e_k$, je důkaz rovnosti (4.28) u konce.

Rovnost (4.29) plyne z rovnosti (4.28) a posledního řádku vyjádření (4.30). □

Lemma 4.29. *Nechť x je libovolný prvek množiny X. Pak pro každé $i = 1, \ldots, n$ platí*

$$(r_i^+(x))_j^\oplus = (x)_j^\oplus \quad \forall j = i, \ldots, n, \tag{4.31}$$

$$(r_i^\oplus(x))_j^+ = (x)_j^+ \quad \forall j = i, \ldots, n. \tag{4.32}$$

Důkaz. Také u tohoto lemmatu dokážeme pouze rovnost (4.31), neboť rovnost (4.32) by se dokazovala obdobně.

Důkaz rovnosti (4.31) provedeme indukcí podle i. Protože $r_1^+(x) = x$, je

$$(r_1^+(x))_j^\oplus = (x)_j^\oplus \quad \forall j = 1, \ldots, n.$$

Indukční krok je následující: Nechť $i \in \{1, \ldots, n-1\}$. Předpokládejme, že platí

$$(r_i^+(x))_l^\oplus = (x)_l^\oplus \quad \forall l = i, \ldots, n \tag{4.33}$$

a dokažme, že

$$(r_{i+1}^+(x))_j^\oplus = (x)_j^\oplus \quad \forall j = i+1, \ldots, n. \tag{4.34}$$

Platí

$$r_i^+(x) = r_{i+1}^+(x) + \varepsilon_i e_i. \tag{4.35}$$

Je-li $\varepsilon_i = 0$, pak $r_i^+(x) = r_{i+1}^+(x)$, a tedy podle indukčního předpokladu (4.33) je $(r_{i+1}^+(x))_j^\oplus = (r_i^+(x))_j^\oplus \overset{(4.33)}{=} (x)_j^\oplus$ pro každé $j = i, \ldots, n$.

Pro $\varepsilon_i = 1$ máme $r_i^+(x) = r_{i+1}^+(x) + e_i$, a tedy podle indukčního předpokladu (4.33), rovnosti (4.35) a důsledku 4.25 je

$$(r_{i+1}^+(x))_j^\oplus \overset{4.25}{=} (r_{i+1}^+(x) + e_i)_j^\oplus \overset{(4.35)}{=} (r_i^+(x))_j^\oplus \overset{(4.33)}{=} (x)_j^\oplus, \tag{4.36}$$

což platí pro všechna $j = i+1, \ldots, n$, neboť první rovnost platí pro všechna $j' = i+1, \ldots, n$, prostřední rovnost platí pro všechna $l' = 1, \ldots, n$ a poslední rovnost platí pro všechna $l = i, \ldots, n$. □

Lemma 4.30. *Nechť $x \in X$ je libovolný prvek množiny X. Pak pro každé $i = 1, \ldots, n$ platí*

$$(r_i^+(x))_i^\oplus = (x)_i^\oplus \tag{4.37}$$

a

$$(r_i^\oplus(x))_i^+ = (x)_i^+ \tag{4.38}$$

a pro každé $k = 1, \ldots, n-1$ platí

$$(x)_k^\oplus = (x)_k^+ * (r_{k+1}^+(x))_k^\oplus \tag{4.39}$$

a

$$(x)_k^+ = (x)_k^\oplus * (r_{k+1}^\oplus(x))_k^+. \tag{4.40}$$

Důkaz. Zde opět stačí dokázat rovnosti (4.37) a (4.39), neboť důkaz rovností (4.38) a (4.40) by byl obdobný.

Rovnost (4.37) je speciálním případem vztahu (4.31) pro $j = i$.

K důkazu rovnosti (4.39) stejně jako v předchozím důkazu použijeme následující vyjádření prvku $r_k^+(x)$:

$$r_k^+(x) = r_{k+1}^+(x) + \varepsilon_k e_k. \tag{4.41}$$

Je-li $\varepsilon_k = 0$, pak $r_k^+(x) = r_{k+1}^+(x)$ a z rovnosti (4.37) plyne, že $(x)_k^\oplus = (r_k^+(x))_k^\oplus = (r_{k+1}^+(x))_k^\oplus = 0 * (r_{k+1}^+(x))_k^\oplus = (x)_k^+ * (r_{k+1}^+(x))_k^\oplus$, neboť $(x)_k^+ = \varepsilon_k = 0$. Pro $\varepsilon_k = 0$ tedy platí rovnost (4.39).

Pro $\varepsilon_k = 1$ plyne z důsledku 4.25 a rovností (4.37) a (4.41), že

$$(x)_k^\oplus \overset{(4.37)}{=} (r_k^+(x))_k^\oplus \overset{(4.41)}{=} (r_{k+1}^+(x) + e_k)_k^\oplus \overset{4.25}{=} (r_{k+1}^+(x))_k^\oplus * 1,$$

což dokazuje rovnost (4.39) pro $(x)_k^+ = \varepsilon_k = 1$. □

Označení 4.31. Ve zbylém textu budeme pro každé $i = 1, \ldots, n-1$ označovat symbolem $\mathbf{b}^i$ prvek $\mathbf{b}^i = \bigoplus_{k=1}^i b_k^i e_k$ takový, že

$$x \oplus \alpha = r_{i+1}^\oplus(x \oplus \alpha) \oplus \mathbf{b}^i,$$

kde $r_{i+1}^\oplus(x \oplus \alpha) \in \mathcal{R}^\oplus(X/X_i)$ je přirozený reprezentant prvku $x \oplus \alpha$ v rozkladové třídě X/X_i příslušný operaci $\oplus$.

Dále budeme symbolem $\mathbf{c}^i$ označovat prvek $\mathbf{c}^i = \bigoplus_{k=1}^i c_k^i e_k$ takový, že

$$y \oplus \beta = r_{i+1}^\oplus(y \oplus \beta) \oplus \mathbf{c}^i,$$

kde $r_{i+1}^\oplus(y \oplus \beta) \in \mathcal{R}^\oplus(X/X_i)$ je přirozený reprezentant prvku $y \oplus \beta$ v rozkladové třídě X/X_i příslušný operaci $\oplus$.

Symbolem $\mathbf{d}^i$ budeme označovat takový prvek $\mathbf{d}^i = \sum_{k=1}^i d_k^i e_k \in X_i$, pro který platí

$$x + y = r_{i+1}^+(x + y) + \mathbf{d}^i,$$

kde $r_{i+1}^+(x+y) \in \mathcal{R}^+(X/X_i)$ je přirozený reprezentant prvku $x+y$ v rozkladové třídě X/X_i příslušný operaci $+$.

Symbolem $\mathbf{g}^i$ budeme označovat takový prvek $\mathbf{g}^i = \sum_{k=1}^i g_k^i e_k \in X_i$, pro který platí

$$(x \oplus \alpha) + (y \oplus \beta) = r_{i+1}^+((x \oplus \alpha) + (y \oplus \beta)) + \mathbf{g}^i,$$

kde $r_{i+1}^+((x \oplus \alpha) + (y \oplus \beta)) \in \mathcal{R}^+(X/X_i)$ je přirozený reprezentant prvku $(x \oplus \alpha) + (y \oplus \beta)$ v rozkladové třídě X/X_i příslušný operaci $+$.

Konečně symbolem $\mathbf{h}^i$ budeme označovat prvek $\mathbf{h}^i = \bigoplus_{k=1}^{i} h_k^i e_k \in X_i$, pro který platí

$$(x+y) \oplus \gamma = r_{i+1}^{\oplus}((x+y) \oplus \gamma) \oplus \mathbf{h}^i,$$

kde $r_{i+1}^{\oplus}((x+y) \oplus \gamma) \in \mathcal{R}^{\oplus}(X/X_i)$ je přirozený reprezentant prvku $(x+y) \oplus \gamma$ v rozkladové třídě X/X_i příslušný operaci $\oplus$.

Definujeme $\mathbf{b}^n = 0$, $\mathbf{c}^n = 0$, $\mathbf{d}^n = 0$, $\mathbf{g}^n = 0$ a $\mathbf{h}^n = 0$.

Tvrzení 4.32. *Pro libovolné $i \in \{1, \ldots, n-1\}$ je*

$$r_i^{\oplus}((x \oplus \alpha) + (y \oplus \beta)) = r_{i+1}^{\oplus}((x \oplus \alpha) + (y \oplus \beta)) \oplus \lambda_i e_i, \tag{4.42}$$

kde

$$\begin{aligned} \lambda_i = x_i * \alpha_i * b_i^i * (r_{i+1}^{\oplus}(x \oplus \alpha))_i^+ * y_i * \beta_i * c_i^i * \\ * (r_{i+1}^{\oplus}(y \oplus \beta))_i^+ * g_i^i * (r_{i+1}^{+}((x \oplus \alpha) + (y \oplus \beta)))_i^{\oplus}. \end{aligned} \tag{4.43}$$

Důkaz. Z definice přirozeného reprezentantu plyne, že

$$r_i^{\oplus}((x \oplus \alpha) + (y \oplus \beta)) = r_{i+1}^{\oplus}((x \oplus \alpha) + (y \oplus \beta)) \oplus \lambda_i e_i, \quad \lambda_i \in \{0, 1\}.$$

Chceme tedy najít hodnotu koeficientu λ_i.

Označme si $p = x \oplus \alpha$ a $q = y \oplus \beta$. Nechť $p = \sum_{k=1}^{n} p_k e_k$ a $q = \sum_{k=1}^{n} q_k e_k$ jsou vyjádření prvků p, q pomocí operace $+$.

Nejprve ukážeme, že

$$\lambda_i = p_i * q_i * g_i^i * (r_{i+1}^{+}(p+q))_i^{\oplus}. \tag{4.44}$$

Podle lemmatu 4.28 je $r_i^+(p+q) = r_{i+1}^+(p+q) + (p_i * q_i * g_i^i)e_i$, a tedy (podle poznámky 4.27) $(p+q)_i^+ = (r_i^+(p+q))_i^+ = p_i * q_i * g_i^i$.

K dokončení důkazu rovnosti (4.44) zbývá dokázat, že

$$\lambda_i = (p+q)_i^+ * (r_{i+1}^+(p+q))_i^{\oplus}. \tag{4.45}$$

Nechť $r_{i+1}^+(p+q) = \bigoplus_{k=1}^{n} \sigma_i e_i$ a $r_i^+(p+q) = \bigoplus_{k=1}^{n} \varphi_i e_i$ jsou vyjádření prvků $r_{i+1}^+(p+q)$ a $r_i^+(p+q)$ pomocí operace $\oplus$. Protože $r_i^+(p+q) = r_{i+1}^+(p+q) + (p+q)_i^+ e_i$, je podle důsledku 4.25

- $\varphi_k = \sigma_k$ pro $k = 1, \ldots, n$, pokud $(p+q)_i^+ = 0$,
- $\varphi_k = \sigma_k$ pro $k = i+1, \ldots, n$ a $\varphi_i \neq \sigma_i$, pokud $(p+q)_i^+ = 1$.

To znamená, že $\varphi_i = \sigma_i * (p+q)_i^+$. A protože je $\sigma_i = (r_{i+1}^+(p+q))_i^\oplus$, stačí ukázat, že $\lambda_i = \varphi_i$, a důkaz rovnosti (4.44) bude hotov. Rovnost $\lambda_i = \varphi_i$ však plyne z lemmatu 4.30, neboť $\lambda_i = (p+q)_i^\oplus$ a $\varphi_i = (r_i^+(p+q))_i^\oplus$.

Ukážeme-li, že

$$p_i = x_i * \alpha_i * b_i^i * (r_{i+1}^\oplus(x \oplus \alpha))_i^+ \tag{4.46}$$

a

$$q_i = y_i * \beta_i * c_i^i * (r_{i+1}^\oplus(y \oplus \beta))_i^+, \tag{4.47}$$

bude tvrzení dokázáno.

Dokážeme pouze rovnost (4.46), neboť rovnost (4.47) lze dokázat analogicky. Důkaz rovnosti (4.46) bude podobný důkazu rovnosti (4.44).

Z definice přirozeného reprezentantu (4.2) a lemmatu 4.22 plyne, že $r_i^\oplus(p) = r_i^\oplus(x \oplus \alpha) = r_{i+1}^\oplus(x \oplus \alpha) \oplus (x_i * \alpha_i * b_i^i)e_i$, a tedy $(p)_i^\oplus = (x \oplus \alpha)_i^\oplus = x_i * \alpha_i * b_i^i$.

Podívejme se nyní na vyjádření reprezentantů $r_{i+1}^\oplus(x \oplus \alpha)$ a $r_i^\oplus(x \oplus \alpha)$ pomocí operace $+$. Označme $r_{i+1}^\oplus(x \oplus \alpha) = \sum_{k=1}^n \eta_i e_i$ a $r_i^\oplus(x \oplus \alpha) = \sum_{k=1}^n \omega_i e_i$. Podle důsledku 4.25 je

- $\omega_k = \eta_k$ pro $k = 1, \ldots, n$, pokud $(x \oplus \alpha)_i^\oplus = 0$,
- $\omega_k = \eta_k$ pro $k = i+1, \ldots, n$ a $\omega_i \neq \eta_i$, pokud $(x \oplus \alpha)_i^\oplus = 1$.

To znamená, že $\omega_i = \eta_i * (x \oplus \alpha)_i^\oplus$. A protože je $p_i = (x \oplus \alpha)_i^+$ a $\omega_i = (r_i^\oplus(x \oplus \alpha))_i^+$, plyne z lemmatu 4.30, že $p_i = \omega_i = \eta_i * (x \oplus \alpha)_i^\oplus = (r_{i+1}^\oplus(x \oplus \alpha))_i^+ * (x \oplus \alpha)_i^\oplus$, neboť $\eta_i = (r_{i+1}^\oplus(x \oplus \alpha))_i^+$.

Rovnost (4.46) je tedy dokázána, neboť (jak jsme již dříve ukázali) je $(x \oplus \alpha)_i^\oplus = x_i * \alpha_i * b_i^i$. □

Důkaz následujícího tvrzení je velmi podobný důkazu tvrzení 4.32, proto uvedeme pouze náznak důkazu.

Tvrzení 4.33. *Pro libovolné $i \in \{1, \ldots, n-1\}$ je*

$$r_i^\oplus((x+y) \oplus \gamma) = r_{i+1}^\oplus((x+y) \oplus \gamma) \oplus \kappa_i e_i, \tag{4.48}$$

kde

$$\kappa_i = (x)_i^+ * (y)_i^+ * d_i^i * (r_{i+1}^+(x+y))_i^\oplus * \gamma_i * h_i^i. \tag{4.49}$$

Náznak důkazu. Označme si $z = x + y = \bigoplus_{k=1}^n z_k e_k$ a $w = z \oplus \gamma = \bigoplus_{k=1}^n w_k e_k$. Podobně jako v předchozím tvrzení lze dokázat, že

$$z_i = (x)_i^+ * (y)_i^+ * d_i^i * (r_{i+1}^+(x+y))_i^\oplus \tag{4.50}$$

a

$$\kappa_i = w_i = (z)_i^\oplus * (\gamma)_i^\oplus * h_i^i, \tag{4.51}$$

kde $(z)_i^\oplus = z_i$ a $(\gamma)_i^\oplus = \gamma_i$. □

Nyní zformulujeme tvrzení, které v sobě zahrnuje kombinaci předchozích tvrzení 4.32 a 4.33.

Tvrzení 4.34. *Předpokládejme, že $x, y \in X$ jsou řešením rovnice (4.18) modulo X_i. Potom jsou prvky $x, y \in X$ řešením rovnice (4.18) modulo X_{i-1}, právě když*

$$\begin{aligned}\alpha_i * \beta_i * \gamma_i = (r_{i+1}^{\oplus}(x))_i^+ * (r_{i+1}^{\oplus}(y))_i^+ * (r_{i+1}^+(x+y))_i^{\oplus} * \\ * (r_{i+1}^{\oplus}(x \oplus \alpha))_i^+ * (r_{i+1}^{\oplus}(y \oplus \beta))_i^+ * \\ * (r_{i+1}^+((x \oplus \alpha) + (y \oplus \beta)))_i^{\oplus} * b_i^i * c_i^i * d_i^i * g_i^i * h_i^i.\end{aligned} \tag{4.52}$$

Důkaz. Prvky $x, y \in X$ jsou řešením rovnice (4.18) modulo X_{i-1}, právě když prvek $(x \oplus \alpha) + (y \oplus \beta)$ leží ve stejné rozkladové třídě X podle X_{i-1} jako prvek $(x+y) \oplus \gamma$, tedy právě když se rovnají přirozené reprezentanty $r_i^{\oplus}((x \oplus \alpha) + (y \oplus \beta))$ a $r_i^{\oplus}((x+y) \oplus \gamma)$. Podle tvrzení 4.32 a 4.33 tato rovnost nastává, právě když

$$\begin{aligned}x_i * \alpha_i * b_i^i * (r_{i+1}^{\oplus}(x \oplus \alpha))_i^+ * y_i * \beta_i * c_i^i * \\ * (r_{i+1}^{\oplus}(y \oplus \beta))_i^+ * g_i^i * (r_{i+1}^+((x \oplus \alpha) + (y \oplus \beta)))_i^{\oplus} = \\ = (x)_i^+ * (y)_i^+ * d_i^i * (r_{i+1}^+(x+y))_i^{\oplus} * \gamma_i * h_i^i,\end{aligned}$$

neboť podle předpokladu je $r_{i+1}^{\oplus}((x \oplus \alpha) + (y \oplus \beta)) = r_{i+1}^{\oplus}((x+y) \oplus \gamma)$.

Podle rovnosti (4.40) z lemmatu 4.30 je

$$(x)_i^+ = x_i * (r_{i+1}^{\oplus}(x))_i^+$$

a

$$(y)_i^+ = y_i * (r_{i+1}^{\oplus}(y))_i^+.$$

Z tohoto vyjádření získame po jednoduché úpravě dokazovanou rovnost (4.52). □

Označení 4.35. Ve zbývajícím textu budeme označovat symbolem $\circ$ běžné sčítání v množině přirozených čísel. Symbolem $\cdot$ označíme běžné násobení v množině přirozených čísel. A konečně celočíselné dělení čísla a číslem b označíme $a \operatorname{div} b$.

Ve vyjádření hodnoty $\alpha_i * \beta_i * \gamma_i$ pomocí rovnosti (4.52) se objevují hodnoty $(r_{i+1}^{\oplus}(x))_i^+$, $(r_{i+1}^{\oplus}(y))_i^+$, $(r_{i+1}^+(x+y))_i^{\oplus}$, $(r_{i+1}^{\oplus}(x \oplus \alpha))_i^+$, $(r_{i+1}^{\oplus}(y \oplus \beta))_i^+$ a $(r_{i+1}^+((x \oplus \alpha) + (y \oplus \beta)))_i^{\oplus}$, které jsou nezávislé na hodnotách x_{i+1}, y_{i+1}, α_{i+1}, β_{i+1}, γ_{i+1}, a hodnoty b_i^i, c_i^i, d_i^i, g_i^i a h_i^i, které na hodnotách x_{i+1}, y_{i+1}, α_{i+1}, β_{i+1}, γ_{i+1} závisí.

Označme si hodnotu $(r^{\oplus}_{i+1}(x))^+_i * (r^{\oplus}_{i+1}(y))^+_i * (r^+_{i+1}(x+y))^{\oplus}_i * (r^{\oplus}_{i+1}(x \oplus \alpha))^+_i * (r^{\oplus}_{i+1}(y \oplus \beta))^+_i * (r^+_{i+1}((x \oplus \alpha) + (y \oplus \beta)))^{\oplus}_i$ symbolem δ_i. Pak můžeme rovnost (4.52) zapsat následovně:

$$\alpha_i * \beta_i * \gamma_i = \delta_i * b^i_i * c^i_i * d^i_i * g^i_i * h^i_i. \tag{4.53}$$

Pro hodnoty b^i_i, c^i_i, d^i_i, g^i_i a h^i_i zřejmě platí

$$\begin{aligned}
b^i_i &= b^{i+1}_i * \big((x_{i+1} \circ \alpha_{i+1} \circ b^{i+1}_{i+1}) \operatorname{div} 2\big) \cdot (e_{i+1} \oplus e_{i+1})^{\oplus}_i, \\
c^i_i &= c^{i+1}_i * \big((y_{i+1} \circ \beta_{i+1} \circ c^{i+1}_{i+1}) \operatorname{div} 2\big) \cdot (e_{i+1} \oplus e_{i+1})^{\oplus}_i, \\
d^i_i &= d^{i+1}_i * \big(((x)^+_{i+1} \circ (y)^+_{i+1} \circ d^{i+1}_{i+1}) \operatorname{div} 2\big) \cdot (e_{i+1} + e_{i+1})^+_i, \\
g^i_i &= g^{i+1}_i * \big(((x \oplus \alpha)^+_{i+1} \circ (y \oplus \beta)^+_{i+1} \circ g^{i+1}_{i+1}) \operatorname{div} 2\big) \cdot (e_{i+1} + e_{i+1})^+_i, \\
h^i_i &= h^{i+1}_i * \big(((x+y)^{\oplus}_{i+1} \circ \gamma_{i+1} \circ h^{i+1}_{i+1}) \operatorname{div} 2\big) \cdot (e_{i+1} \oplus e_{i+1})^{\oplus}_i.
\end{aligned}$$

Je tedy

$$\begin{aligned}
b^i_i * c^i_i * d^i_i * g^i_i * h^i_i = {} & b^{i+1}_i * c^{i+1}_i * d^{i+1}_i * g^{i+1}_i * h^{i+1}_i * \\
& * \big[\big((x_{i+1} \circ \alpha_{i+1} \circ b^{i+1}_{i+1}) \operatorname{div} 2\big) * \big((y_{i+1} \circ \beta_{i+1} \circ c^{i+1}_{i+1}) \operatorname{div} 2\big) * \\
& * \big(((x+y)^{\oplus}_{i+1} \circ \gamma_{i+1} \circ h^{i+1}_{i+1}) \operatorname{div} 2\big)\big] \cdot (e_{i+1} \oplus e_{i+1})^{\oplus}_i * \\
& * \big[\big(((x)^+_{i+1} \circ (y)^+_{i+1} \circ d^{i+1}_{i+1}) \operatorname{div} 2\big) * \\
& * \big(((x \oplus \alpha)^+_{i+1} \circ (y \oplus \beta)^+_{i+1} \circ g^{i+1}_{i+1}) \operatorname{div} 2\big)\big] \cdot (e_{i+1} + e_{i+1})^+_i,
\end{aligned} \tag{4.54}$$

kde

$(x)^+_{i+1} \overset{(4.40)}{=} x_{i+1} * (r^{\oplus}_{i+2}(x))^+_{i+1}$,

$(y)^+_{i+1} \overset{(4.40)}{=} y_{i+1} * (r^{\oplus}_{i+2}(y))^+_{i+1}$,

$(x \oplus \alpha)^+_{i+1} \overset{(4.46)}{=} x_{i+1} * \alpha_{i+1} * b^{i+1}_{i+i} * (r^{\oplus}_{i+2}(x \oplus \alpha))^+_{i+1}$,

$(y \oplus \beta)^+_{i+1} \overset{(4.47)}{=} y_{i+1} * \beta_{i+1} * c^{i+1}_{i+i} * (r^{\oplus}_{i+2}(y \oplus \beta))^+_{i+1}$

a

$$\begin{aligned}
(x+y)^{\oplus}_{i+1} &\overset{(4.39)}{=} (x+y)^+_{i+1} * (r^+_{i+2}(x+y))^{\oplus}_{i+1} \overset{(4.50)}{=} \\
&= (x)^+_{i+1} * (y)^+_{i+1} * d^{i+1}_{i+1} * (r^+_{i+2}(x+y))^{\oplus}_{i+1} \overset{(4.40)}{=} \\
&= x_{i+1} * (r^{\oplus}_{i+2}(x))^+_{i+1} * y_{i+1} * (r^{\oplus}_{i+2}(y))^+_{i+1} * d^{i+1}_{i+1} * (r^+_{i+2}(x+y))^{\oplus}_{i+1}.
\end{aligned}$$

Hodnoty b^{i+1}_i, c^{i+1}_i, d^{i+1}_i, g^{i+1}_i, h^{i+1}_i nezávisí na hodnotách x_{i+1}, y_{i+1}, α_{i+1}, β_{i+1}, γ_{i+1}, proto je můžeme spolu s hodnotou δ_i „sloučit“ do jediné proměnné, kterou označíme ψ_i a definujeme

$$\psi_i = \delta_i * b^{i+1}_i * c^{i+1}_i * d^{i+1}_i * g^{i+1}_i * h^{i+1}_i.$$

Při označení

$$\tau_i = \big((x_{i+1} \circ \alpha_{i+1} \circ b_{i+1}^{i+1}) \operatorname{div} 2\big) * \big((y_{i+1} \circ \beta_{i+1} \circ c_{i+1}^{i+1}) \operatorname{div} 2\big) * \\ * \big(((x+y)_{i+1}^{\oplus} \circ \gamma_{i+1} \circ h_{i+1}^{i+1}) \operatorname{div} 2\big)$$

a

$$\vartheta_i = \big(((x)_{i+1}^{+} \circ (y)_{i+1}^{+} \circ d_{i+1}^{i+1}) \operatorname{div} 2\big) * \\ * \big(((x \oplus \alpha)_{i+1}^{+} \circ (y \oplus \beta)_{i+1}^{+} \circ g_{i+1}^{i+1}) \operatorname{div} 2\big)$$

tedy platí

$$\alpha_i * \beta_i * \gamma_i = \psi_i * \tau_i \cdot (e_{i+1} \oplus e_{i+1})_i^{\oplus} * \vartheta_i \cdot (e_{i+1} + e_{i+1})_i^{+}.$$

Hodnota $\alpha_i * \beta_i * \gamma_i$ tedy závisí na hodnotách $\psi_i, x_{i+1}, y_{i+1}, \alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}, b_{i+1}^{i+1}, c_{i+1}^{i+1}, d_{i+1}^{i+1}, g_{i+1}^{i+1}, h_{i+1}^{i+1}, (r_{i+2}^{\oplus}(x))_{i+1}^{+}, (r_{i+2}^{\oplus}(y))_{i+1}^{+}, (r_{i+2}^{+}(x+y))_{i+1}^{\oplus}, (r_{i+2}^{\oplus}(x \oplus \alpha))_{i+1}^{+}, (r_{i+2}^{\oplus}(y \oplus \beta))_{i+1}^{+}, (e_{i+1} \oplus e_{i+1})_i^{\oplus}$ a $(e_{i+1} + e_{i+1})_i^{+}$.

Tuto závislost popisují tabulky na přiloženém CD. Každé uspořádané desetici $\Lambda_{i+1} = \big(b_{i+1}^{i+1}, c_{i+1}^{i+1}, g_{i+1}^{i+1}, h_{i+1}^{i+1}, (r_{i+2}^{\oplus}(x))_{i+1}^{+}, (r_{i+2}^{\oplus}(y))_{i+1}^{+}, (r_{i+2}^{+}(x+y))_{i+1}^{\oplus}, (r_{i+2}^{\oplus}(x \oplus \alpha))_{i+1}^{+}, (r_{i+2}^{\oplus}(y \oplus \beta))_{i+1}^{+}, \psi_i\big)$ přísluší jedna tabulka.

Na průsečíku řádku a sloupce určených hodnotami $x_{i+1}, y_{i+1}, d_{i+1}^{i+1}, \alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}$ nalezneme uspořádanou čtveřici $(\mu_1, \mu_2, \mu_3, \mu_4)$, kde

- μ_1 je hodnota výrazu $\alpha_i * \beta_i * \gamma_i$ pro $(e_{i+1} \oplus e_{i+1})_i^{\oplus} = 0$ a $(e_{i+1} + e_{i+1})_i^{+} = 0$,
- μ_2 je hodnota výrazu $\alpha_i * \beta_i * \gamma_i$ pro $(e_{i+1} \oplus e_{i+1})_i^{\oplus} = 0$ a $(e_{i+1} + e_{i+1})_i^{+} = 1$,
- μ_3 je hodnota výrazu $\alpha_i * \beta_i * \gamma_i$ pro $(e_{i+1} \oplus e_{i+1})_i^{\oplus} = 1$ a $(e_{i+1} + e_{i+1})_i^{+} = 0$,
- μ_4 je hodnota výrazu $\alpha_i * \beta_i * \gamma_i$ pro $(e_{i+1} \oplus e_{i+1})_i^{\oplus} = 1$ a $(e_{i+1} + e_{i+1})_i^{+} = 1$.

4.3 Algoritmus

Nyní přistoupíme k hledání řešení rovnice typu (4.18). Prvky $\mathbf{d}^i$, $i = 1, \ldots, n-1$, závisí pouze na prvcích x, y, $(e_{i+1} + e_{i+1})$, $(e_{i+1} \oplus e_{i+1})$ a na přechodových funkcích, nikoliv na prvcích α, β, γ. Proto je, stejně jako v případě standardního grupového páru, hodnota d_{i+1}^{i+1} součástí řešení.

Ze zadání známe hodnoty α_{i+1}, β_{i+1}, γ_{i+1}, $\alpha_i * \beta_i * \gamma_i$ a $(e_{i+1} \oplus e_{i+1})_i^{\oplus}$, $(e_{i+1} + e_{i+1})_i^{+}$. Hodnoty $x_{i+1}, y_{i+1}, d_{i+1}^{i+1}$, které spolu se zadanými hodnotami splňují rovnost (4.52), nazýváme *řešením rovnice (4.18) na* $(i+1)$*-ní pozici*. Dvojici (x_{i+1}, y_{i+1}), pro kterou je $x_{i+1}, y_{i+1}, d_{i+1}^{i+1}$ řešením rovnice (4.18) na $(i+1)$-ní pozici, nazýváme *řešením rovnice (4.18) na* $(i+1)$*-ní pozici příslušným hodnotě* d_{i+1}^{i+1}.

K hledání řešení na $(i+1)$-ní pozici můžeme použít přiložené tabulky. V každé z nich ve sloupci určeném hodnotami $\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}$ najdeme sloupeček určený hodnotami $(e_{i+1} \oplus e_{i+1})_i^{\oplus}$, $(e_{i+1} + e_{i+1})_i^{+}$. Řádky, na kterých se v tomto sloupečku vyskytuje hodnota $\alpha_i * \beta_i * \gamma_i$, určují trojice $(x_{i+1}, y_{i+1}, d_{i+1}^{i+1})$, které jsou řešením rovnice (4.18) na $(i+1)$-ní pozici příslušným dané desetici Λ_{i+1}.

Jak vidíme v přiložených tabulkách, řešení rovnice (4.18) na $(i+1)$-ní pozici v některých případech existuje pouze pro jediné ψ_i. Např. pro $(e_{i+1} \oplus e_{i+1})_i^{\oplus} = 0$, $(e_{i+1} + e_{i+1})_i^{+} = 0$ existuje řešení pouze v případě, že $\alpha_i * \beta_i * \gamma_i = \psi_i$.

To způsobuje, že hledání jednoho řešení rovnice (4.18) pomocí algoritmu Paula a Preneela zobecněného na husté abelovské grupové páry nemůže být obecně polynomiální. Může se totiž stát, že některé řešení rovnice (4.18) modulo X_i nepůjde „prodloužit“ na řešení modulo X_{i-1}, ale zjistíme to až v okamžiku, kdy známe Λ_{i+1}, a tedy ψ_i.

Nyní popíšeme algoritmus na nalezení všech řešení soustavy (4.17). Krok 9. upřesníme v komentáři za algoritmem.

Algoritmus 4.36.
Vstup: Souřadnice prvků $\alpha[k]$, $\beta[k]$, $\gamma[k]$ vzhledem k bázi E_X příslušné operaci $\oplus$ pro $k = 1, \ldots, m$, soubor přechodových funkcí f_i a prvky $e_i \oplus e_i, e_i + e_i \in X_{i-1}$ pro $i = 0, \ldots, n-1$.
Výstup: Množina všech dvojic $x = \bigoplus_{j=1}^{n} x_j e_j, y = \bigoplus_{j=1}^{n} y_j e_j \in X$ které jsou řešením soustavy (4.17) s koeficienty ze vstupu.
Postup:

1. Pro $k = 1, \ldots, m$:
2. Ověř, jestli $\alpha_n[k] * \beta_n[k] * \gamma_n[k] = 0$.
3. Pokud tato rovnost neplatí, pak soustava (4.17) nemá řešení. Konec.
4. Pro $k = 1, \ldots, m$:
5. Polož $\mathbf{b}^0[k] = 0$, $\mathbf{c}^0[k] = 0$, $\mathbf{d}^0[k] = 0$, $\mathbf{g}^0[k] = 0$, $\mathbf{h}^0[k] = 0$.

6. Pro $k = 1, \ldots, m$:

7. Pro $i = n-1, \ldots, 0$:

8. V každé z přiložených tabulek najdi množinu všech trojic $(x_{i+1}, y_{i+1}, d_{i+1}^{i+1})$, pro které je na místě určeném hodnotami α_{i+1}, β_{i+1}, γ_{i+1}, x_{i+1}, y_{i+1}, d_{i+1}^{i+1}, $(e_{i+1} \oplus e_{i+1})_i^{\oplus}$, $(e_{i+1} + e_{i+1})_i^{+}$ daná hodnota $\alpha_i * \beta_i * \gamma_i$.

9. Principem prohledávání do hloubky najdi všechna řešení k-té rovnice soustavy (4.17).

10. Urči průnik množin řešení jednotlivých rovnic soustavy.

Popišme 9. krok algoritmu 4.36. Množiny řešení jednotlivých rovnic budeme hledat „prodlužováním“ řešení modulo X_i na řešení modulo X_{i-1}, kde $i = 0, \ldots, n-1$. Ve druhém kroku algoritmu jsme zjistili, že každá rovnice soustavy (4.17) je řešitelná modulo X_{n-1} (jinak by algoritmus ukončil výpočet ve 3. kroku a nedostal by se na 9. krok).

Jak lze snadno ověřit, je vždy $\Lambda_n = (0,0,0,0,0,0,0,0,0,0)$. Proto při prodlužování řešení rovnice (4.18) modulo X_{n-1} na její řešení modulo X_{n-2} používáme vždy tabulku 1. Z 8. kroku algoritmu známe množinu všech trojic (x_n, y_n, d_n^n), které jsou v tabulce 1 řešením dané rovnice na n-té pozici. Z nich vybereme ty, ve kterých je $d_n^n = 0$, protože je $\mathbf{d}^n = 0$. Z takto získané množiny vybereme libovolný prvek (x_n, y_n), který je řešením dané rovnice na n-té pozici příslušným hodnotě $d_n^n = 0$. Odtud určíme hodnoty $b_{n-1}^{n-1}, c_{n-1}^{n-1}, d_{n-1}^{n-1}, g_{n-1}^{n-1}, h_{n-1}^{n-1}, (r_n^{\oplus}(x))_{n-1}^{+}, (r_n^{\oplus}(y))_{n-1}^{+}, (r_n^{+}(x+y))_{n-1}^{\oplus}, (r_n^{\oplus}(x \oplus \alpha))_{n-1}^{+}, (r_n^{\oplus}(y \oplus \beta))_{n-1}^{+}, \psi_{n-2}$, čímž získáme Λ_{n-1} a d_{n-1}^{n-1}.

Podobně postupujeme také při prodlužování řešení dané rovnice modulo X_i na její řešení modulo X_{i-1} pro $i = 0, \ldots, n-2$. Hodnoty d_{i+1}^{i+1} a Λ_{i+1} nám určí množinu jejích řešení na $(i+1)$-ní pozici příslušné hodnotě d_{i+1}^{i+1}. Z ní vybereme jeden prvek, s jehož pomocí spočteme Λ_i a d_i^i.

Rozeberme nyní časovou složitost jednotlivých kroků algoritmu 4.36. Kroky 2. a 3. mají konstantní časovou složitost, takže kroky 1.–3. mají složitost $\mathcal{O}(m)$. Kroky 4.–5. mají také časovou složitost $\mathcal{O}(m)$. Krok 8. má konstantní časovou složitost, neboť velikost přiložených tabulek je konstantní. V kroku 9. se při každém prodlužování řešení rovnice (4.18) modulo X_i na její řešení modulo X_{i-1} provádí několik převodů vyjádření prvku pomocí operace $+$ na jeho vyjádření pomocí operace $\oplus$ nebo naopak, což má časovou složitost polynomiální v n. Krok 9. má proto časovou složitost $\mathcal{O}(p(n)4^n)$, kde $p(n)$ je polynom v n. Kroky 6. - 9. mají tedy časovou složitost $\mathcal{O}(m \cdot 4^n)$. Složitost kroku 10. je v $\mathcal{O}(m \cdot 4^{2n})$,

neboť průnik m množin, z nichž každá má velikost maximálně l, lze nalézt v $\mathcal{O}(ml^2)$. V tomto případě je $l = 4^n$.

Algoritmus 4.36 má tedy časovou složitost $\mathcal{O}(m \cdot 4^{2n})$. Obecně je tedy z hlediska časové složitosti výhodnější k nalezení všech řešení soustavy (4.17) vyzkoušet všech 4^n možností řešení, neboť tento postup má časovou složitost $\mathcal{O}(m \cdot p(n) \cdot 4^n)$, neboť i zde je třeba převádět vyjádření prvku pomocí operce $+$ na jeho vyjádření pomocí operace $\oplus$ nebo opačně.

Při splnění určitých podmínek ovšem algoritmus 4.36 na nalezení všech řešení soustavy (4.17) najde jedno řešení rovnice (4.18) v polynomiálním čase. Jaké jsou tyto podmínky?

Předpokládejme, že známe prvky $\alpha = \bigoplus_{k=1}^{n} \alpha_k e_k$, $\beta = \bigoplus_{k=1}^{n} \beta_k e_k$, $\gamma = \bigoplus_{k=1}^{n} \gamma_k e_k$ a dále pro každé $i = 1, \ldots, n$ přechodovou funkci f_{i-1} a prvky $(e_i + e_i)$, $(e_i \oplus e_i)$. K tomu, aby algoritmus 4.36 nalezl v polynomiálním čase jedno řešení rovnice (4.18), je třeba, aby pro každé $i = 1, \ldots, n$, pro každou hodnotu $\alpha_{i-1} * \beta_{i-1} * \gamma_{i-1}$ a pro každou dvojici Λ_i, $\widetilde{\Lambda}_i$, které se liší pouze v jedné položce, buď ani v jedné z tabulek příslušných Λ_i a $\widetilde{\Lambda}_i$ neexistovalo žádné řešení určené hodnotami $(e_i + e_i)^+_{i-1}$, $(e_i \oplus e_i)^{\oplus}_{i-1}$, nebo aby v tabulce příslušné Λ_i existovala taková dvě řešení $(x_{i,1}, y_{i,1}, d^i_{i,1})$, $(x_{i,2}, y_{i,2}, d^i_{i,2})$, pro která $d^i_{i,1} \neq d^i_{i,2}$, a aby zároveň v tabulce příslušné $\widetilde{\Lambda}_i$ existovala taková dvě řešení $(\widetilde{x}_{i,1}, \widetilde{y}_{i,1}, \widetilde{d}^i_{i,1})$, $(\widetilde{x}_{i,2}, \widetilde{y}_{i,2}, \widetilde{d}^i_{i,2})$, pro která $\widetilde{d}^i_{i,1} \neq \widetilde{d}^i_{i,2}$.

Je-li splněna první část podmínky, tedy neexistence daného řešení ani v jedné tabulce, pak v případě, že rovnice (4.18) nemá řešení, zjistíme to v první fázi algoritmu 4.36 (kroky 1. - 8.), která má polynomiální časovou složitost. Podmínka existence dvou řešení na i-té pozici s různými hodnotami $d^i_{i,1} \neq d^i_{i,2}$ a $\widetilde{d}^i_{i,1} \neq \widetilde{d}^i_{i,2}$ zajišťuje, že v případě řešitelnosti rovnice (4.18) lze její řešení modulo X_{i+1} vždy prodloužit na její řešení modulo X_i.

V případě standardního grupového páru je pro každé $i = 0, \ldots, n-1$ přechodová funkce f_i identita na X_i. Dále pro všechna $x \in X$ a $i = 1, \ldots, n-1$ platí $(r^+_{i+1}(x))^{\oplus}_i = 0$ a $(r^{\oplus}_{i+1}(x))^+_i = 0$, $b^{i+1}_i = c^{i+1}_i = d^{i+1}_i = g^{i+1}_i = h^{i+1}_i = 0$. A také pro každé $i = 1, \ldots, n$ je $\mathbf{b}^i = \mathbf{c}^i = \mathbf{h}^i = 0$ a $(e_i + e_i)^+_{i-1} = 1$, $(e_i \oplus e_i)^{\oplus}_{i-1} = 0$. Proto je pro standardní grupový pár vždy $\psi_i = 0$ a $\Lambda_{i+1} = (0, 0, g^{i+1}_{i+1}, 0, 0, 0, 0, 0, 0, 0)$.

Pro standardní grupový pár jsou tedy relevantní pouze tabulky 1 a 129. V nich z každého sloupce příslušejícího trojici $(\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1})$ vybíráme 2. sloupeček, neboť ten přísluší případům, kdy $(e_{i+1} + e_{i+1})^+_i = 1$, $(e_{i+1} \oplus e_{i+1})^{\oplus}_i = 0$.

Ve standardním grupovém páru navíc platí podmínka, že $\alpha_i * \beta_i * \gamma_i = d^i_i * g^i_i$. Proto z vybraných sloupečků uvažujeme pouze ty položky, jejichž

příslušné hodnoty α_i, β_i, γ_i, d_i^i, g_i^i splňují tuto podmínku.

Ve standardním grupovém páru jsou tedy splněny podmínky, při kterých algoritmus 4.36 najde jedno řešení rovnice (4.18) v polynomiálním čase.

Literatura

[1] Paul S., Preneel B., *Solving Systems of Differential Equations of Addittion*, Information Security and Privacy, Lecture Notes in Computer Science 3574, Springer-Verlag, Berlin, 2005, ISBN 978-3-540-26547-4