GENEROVANIE HODNÔT POLYNOMICKEJ FUNKCIE

GENERATION OF THE VALUES OF THE POLYNOMIAL FUNCTION

A. Príkopová, L. Hargaš, D. Koniar

Katedra mechatroniky a elektroniky , Elektrotechnická fakulta ŽU v Žiline
Veľký diel, 010 26 Žilina, tel.: +421 41 1613, mail: anna.prikopova@fel.uniza.sk

Abstrakt Polynomické funkcie nad konečným telesom Galoisovým sú základom nového prístupu k riešeniu problematiky logického riadenia technologických procesov s využitím procesorových systémov. Predložený článok popisuje SW prostriedky pre vyčíslovanie polynomických funkcií.

Summary The polynomial functions of the Galois´ finit field make up the base of original access to the solution to area logic control of technological processes with of the exploitation μP systems. This article describes SW ways and means for determination of the polynomial function.

1. ÚVOD

V práci [1] bolo poukázané na možnosti nového prístupu k riešeniu problematiky konečných automatov pre logické riadenie s využitím μP radičov. Jedným z pozitívnych dôsledkov takéhoto prístupu sa ukázala možnosť využitia teoretických záverov na tvorbu jednotnej, univerzálnej programovej šablóny konečného automatu. Od takéhoto prístupu sa o.i. očakáva zníženie prácnosti návrhu konečného automatu a tiež zvýšenie čitateľnosti programového riešenia.

Ako možné riešenie takejto úlohy je v práci [2] predložená funkčná schéma konečného automatu založená na využití špeciálneho pojmu modernej algebry – polynomickej funkcie.

2. POLYNOMICKÁ FUNKCIA

Polynomickú funkciu je možné skonštruovať nad algebraickou štruktúrou, konečným telesom Galoisovým GF(p^q), ktorého prvkami sú polynomické formy konečného stupňa *q-1* s koeficientami s unitálneho podtelesa GF(p) celočíselných prvkov, zvyškov po delení celých čísel vhodným prvo-číselným modulom p. Inými slovami: Teleso GF(p^q) je konečným rozšírením unitálneho telesa GF(p), ktoré tvorí podteleso telesa GF(p^q), pričom toto roz-šírenie je generované vhodným prvkom z GF(p^q), ireducibilným polynómom stupňa q. Hovoríme že každé takéto konečné teleso GF(p^q) má konečnú prvočíselnú charakteristiku p, pričom ide o rozšíre-nie stupňa q, ktoré má rád $n = p^q$.

Zdôraznime, že v naznačenom prípade ide o špecifickú algebru, ktorá pracuje s polynomickými formami, teda prvkami sú polynomické formy tvaru

$$a_{q-1}.\varepsilon^{q-1} + a_{q-2}.\ \varepsilon^{q-2} + ... + a_2.\ \varepsilon^2 + a_1.\ \varepsilon + a_0, \qquad (1)$$

kde

- a_i celočíselné koeficienty z unitálneho telesa GF(p), t.j. z množiny {0 – p-1},
- ε neurčitá polynomickej formy.

Pri výpočtárskych operáciách ako operandy sú podľa árnosti operácií brané jednotlivé prvky, t.j. jedna, dve alebo viaceré polynomické formy z GF(p^q) a ako výsledok výpočtu je nová, výsledná polynomická forma z GF(2^q). Polynomické formy teda nevyčíslujeme, neurčujeme hodnoty polynómov nemá preto v tejto etape zmysel uvažovať o hodnotách neurčitej ε.

V uvádzanej algebraickej štruktúre polynomická funkcia definuje priradenie

$$\Psi = \Omega(\xi), \qquad (2)$$

kde

- ξ je neurčitá z telesa GF(p^q),
- Ω je funkčný predpis z telesa GF(p^q),
- Ψ je funkčná hodnota polynomickej funkcie, prislúchajúca argumentu ξ

Prvkami uvažovaného telesa sú polynomické formy, ktoré svojimi celočíselnými koeficientami definujú usporiadané q-tice prvkov. Pri voľbe charakteristiky $p = 2$ koeficienty polynomických foriem z GF(2^q) a teda i prvky usporiadaných q-tic sú čísla $0, 1 \in$ GF(2).

Dá sa ukázať, že obecné vyjadrenie polynomickej funkcie skonštruovanej nad definovaným telesom GF(2^q) má tvar

$$A_{n-1} \otimes \xi^{n-1} \oplus A_{n-2} \otimes \xi^{n-2} \oplus ..... \oplus A_1 \otimes \xi \oplus A_0 \qquad (3)$$

kde

- A_i koeficienty z GF(2^q) špecifikujúce konkrétnu polynomickú funkciu,
- n rád rozšírenia.

Naznačené algebraické operácie „ ⊕ “ a „ ⊗ “ sú operácie súčtu a súčinu v telese GF(2^q) nad polynomickými prvkami z tohto telesa a mocnina

$$\xi^i = \underbrace{\xi \otimes \xi \otimes .... \otimes \xi}_{\text{i - krát}} \qquad (4)$$

Základným predpokladom praktického využitia naznačeného prístupu je implementácia výpočtových operácií v telese GF(2^q) nad polynomickými prvkami z tohoto telesa, ale tiež efektívny algoritmus generovania hodnôt polynomickej funkcie.

Riešenie prvej úlohy, totiž implementácia výpočtových operácií v telese GF(2^q) nad polynomickými prvkami z tohoto telesa je dokumentované v práci [3], kde na báze podrobnej špecifikácie algebraickej štruktúry sú definované požadované algebraické operácie, ale najmä je poukázané na vhodnú reprezentáciu prvkov telesa pre aplikáciu v procesorovom systéme. V súvislosti s definíciou uveďme najskôr zavedenie aditívnej operácie $\oplus$ z GF(2^q), totiž súčet dvoch polynomických foriem

$$\sum a_i.\varepsilon^i \oplus \sum b_i.\varepsilon^i = \sum c_i.\varepsilon^i \qquad (5)$$

kde výsledkom súčtu dvoch ľubovolných prvkov z GF(2^q) je opäť polynomická forma z GF(2^q), pre ktorú platí

$$c_i \equiv a_i + b_i \qquad \text{mod } 2, \qquad (6)$$

pričom $a_i, b_i, c_i \in$ GF(2).

Ľahko sa dá overiť, že nulovým prvkom v GF(2^q) je polynomická forma s $a_i = 0$ pre všetky $i \in \{0 \div q - 1\}$. Rovnako ľahko sa dá overiť, že ku každému prvku ξ z GF(2^q) existuje opačný prvok $-\xi$ z GF(2^q) taký, že platí

$$\xi \oplus (-\xi) = 0. \qquad (7)$$

Analogicky je zavedená multiplikatívna operácia $\otimes$ z GF(2^q), totiž súčin dvoch polynomických foriem

$$\sum a_i.\varepsilon^i \otimes \sum b_i.\varepsilon^i = \sum c_i.\varepsilon^i \qquad (8)$$

Násobenie prebieha ako obvyklé násobenie dvoch polynómov s koeficientami z GF(2), pričom získaný výsledok musí byť delený zvoleným ireducibilným polynómom, aby výsledná polynomická forma spadala do GF(2^q). Jednoducho zavedieme jednotkový prvok v GF(2^q) ako polynomickú formu s $a_i = 0$ pre všetky $i \in \{1 \div q - 1\}$ s výnimkou $a_0 = 1$.

Pre výpočtové operácie sa dá overiť platnosť zákona komutatívneho, asociatívneho i distributívneho. Z tohoto hľadiska teda ide o obvyklú algebraickú štruktúru.

Dôležitým krokom, umožňujúcim bezproblémové praktické využitie je riešenie reprezentácie prvkov telesa pre aplikáciu v procesorovom systéme. Zavedenie prvkov uvažovaného algebraického systému udáva vzťah (1). Použitý zápis najmä v súvislosti s využitím procesorových systémov je však nevhodný. Pri zachovaní všetkých relevantných informácií je možné symboliku zodpovedajúcim spôsobom upraviť. V prvom rade je zrejmé, že v rámci daného telesa GF(2^q) je štruktúra polynomických foriem podľa vzťahu (1) pevná, nemenná. Je totiž stupeň rozšírenia q zadaný pevný parameter, ktorý udáva pevnú dĺžku polynomických foriem i rozsah exponentov neurčitej polynomickej formy. Za týchto okolností sa jednotlivé prvky vzájomne líšia iba hodnotami koeficientov pri jednotlivých mocninách neurčitej polynomickej formy. Je preto možné každý prvok telesa jednoznačne určiť usporiadanou q-ticou koeficientov

$$a_{q-1}, a_{q-2}, \ldots\ldots a_2, a_1, a_0, \qquad (9)$$

nadobúdajúcich iba hodnoty 0, 1. Z praktického hľadiska je takýto spôsob reprezentácie prvkov telesa mimoriadne vhodný práve pre aplikácie v procesorových systémoch. Z hľadiska teoretického tento krok môžeme označiť ako bijekciu množiny prvkov podľa (1) na zodpovedajúcu množinu q-bitových slov v pamäti procesora.

V naznačenom zložkovom vyjadrení je okrem znalosti hodnoty každého koeficienta dôležitá explicitná informácia o jeho pozícii v slove, t.j. určenie, pri ktorej mocnine neurčitej polynomickej formy stojí. Toto rieši obvyklý poziční zápis čísla v dvojkovej sústave

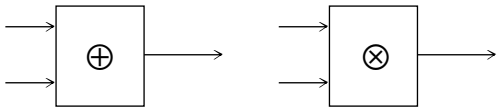
$$a_{q-1}.2^{q-1} + a_{q-2}.2^{q-2} + \ldots\ldots + a_1.2^1 + a_0.2^0 \qquad (10)$$

Vyčíslením váhového vyjadrenia každej zložky skonvertujeme dvojkové číslo podľa (10) na nezáporné celé číslo vo zvolenej číselnej sústave, obvykle desiatkovej, čím obdržíme tzv. dekadický ekvivalent, ktorý pri správnej interpretácii môže tvoriť jednoduchú a jedno-jednoznačnú reprezentáciu prvku z GF(2^q). Totiž, každý konkrétny prvok z GF(2^q) možno naznačeným spôsobom jednoznačne previesť na prislúchajúci dekadický ekvivalent a naopak, každý takýto dekadický ekvivalent možno jednoznačne zapísať v tvare (10), z ktorého možno extrahovať q-ticu koeficientov, dovolujúcu pôvodný zápis prvku v tvare (1). Naznačená úvaha dovoľuje deklarovať prvky telesa GF(p^q) ako jednoduchý, integrálny dátový typ. Pre takýto prípad je nutné interpretovať výpočty na operácie nad integrálnymi typmi.

Na základe predchádzajúcich poznatkov môžeme zhrnúť, že [**A**, $\oplus$, $\otimes$, 0, 1], kde **A** = {0, 1, 2, 3, ...q-1} je množina celých čísel, je celočíselný algebraický systém. Binárne operácie súčtu a súčinu v celočíselnej (ekvivalentovej) reprezentácii prvkov sú osobitými aritmetickými operáciami nad vybranými celými číslami. Realizácia týchto operácií vyplýva z definičných polynomických vzťahov (5) a (8).

Praktickému využívaniu popisovanej algebry okrem zložitosti definície bráni najmä výpočtárska náročnosť, čo v súčasnosti možno eliminovať imple-

mentáciou operácií do programového vybavenia počítačov obvyklou užívateľskou definíciou funkcie.



a) *b)*

Obr. 1. Znázornenie realizácie súčtu a súčinu v GF(2^q).

Fig. 1. Representation of the realisation of the addition and multiplication in GF(2^q).

Názorná predstava o realizácii základných binárnych operácií je vytvorená na obr. 1 a, b, kde bloky $\oplus$ a $\otimes$ reprezentujú programové procedúry typu funkcie dvoch premenných ξ_1, ξ_2 z GF(2^q). Fungovanie týchto procedúr možno – s prihliadnutím na použitú reprezentáciu prvkov telesa GF(2^q) – sformulovať do nasledujúcich algoritmov:

a. *Algoritmus súčtu.* Po prevzatí oboch sčítancov musí v prvom rade prebehnúť konverzia ich jednoduchej celočíselnej reprezentácie do usporiadaných q-tíc koeficientov $a_{q-1}, a_{q-2}, ... a_2, a_1, a_0$, resp. $b_{q-1}, b_{q-2}, ... b_2, b_1, b_0$. Na tomto základe možno realizovať súčet v zmysle uvádzaného vzťahu (5), resp. (6). Po získaní q-tice koeficientov výslednej polynomickej formy túto spätnou konverziou prevedieme na výsledok celočíselného typu.

b. *Algoritmus súčinu.* Analogicky aj v tomto prípade musí prvotne prebehnúť konverzia jednoduchej celočíselnej reprezentácie vstupných parametrov do usporiadaných q-tíc koeficientov $a_{q-1}, a_{q-2}, ... a_2, a_1, a_0$, resp. $b_{q-1}, b_{q-2}, ... b_2, b_1, b_0$. Na tomto základe možno realizovať súčin operandov po bitových zložkách, s rešpektovaním pravidiel algebry modulo 2. Po jeho výpočte sa určí zvyšok po delení príslušným ireducibilným polynómom. Po získaní koeficientov výslednej polynomickej formy túto spätnou konverziou prevedieme na výsledok celočíselného typu.

Pre efektívne vyčíslovanie polynomických funkcií podľa vzťahu (3) je účelné základné binárne operácie doplniť unárnou operáciou umocňovania. Algoritmus tejto operácie v zmysle definície (4) v plnej miere využíva operáciu súčinu.

Naznačené algoritmy v prostredí VBA pre Excell realizujú funkcie

PolySucet(ξ_1 As Long, ξ_2 As Long, q As Integer)
PolySucin(ξ_1 As Long, ξ_2 As Long, q As Integer)
PolyMocnina(ξ As Long, e As Integer, q As Integer).

V oboch prípadoch ide o programové procedúry s návratovou hodnotou, ktorá je celočíselnou reprezentáciou výsledku. Ako vstupné parametre sú prirodzene požadované dva operandy ξ_1, ξ_2, resp. jeden operand ξ a to v celočíselnej reprezentácii. Naviac je požadovaný exponent e a stupeň rozšírenia q, ktorý konkretizuje teleso GF(2^q).

Špecifikácia nulárnych a unárnych operácií ako je vyznačenie nulových a jednotkových prvkov je triviálna, opačné a reciproké prvky pre zamýšľané úlohy nie sú nutné. Je preto, s prihliadnutím na platnosť zákonov komutatívneho, asociatívneho a distributívneho rozsah implementácie algebraických operácií pre prácu s polynomickými formami v prostredí PC pre požadované aplikácie postačiteľný.

Existencia vyššieuvedených základných algebraických operácií s polynomickými prvkami z GF(2^q) umožňuje vyčíslovanie polynomických funkcií, ktoré spočíva v nasledujúcich krokoch:

-Prevzatie aktuálnej hodnoty neurčitej ξ z telesa GF(2^q), ktorá reprezentuje vstupnú hodnotu pre polynomickú funkciu.
-Prevzatá hodnota je postupne umocňovaná až do stupňa $n-1$, kde $n = 2^q$ je rád rozšírenia unitálneho telesa. V zmysle definície ľubovolnej i-tej mocniny je zrejmé, že získané výsledky sú opäť hodnoty z GF(2^q).
-Každá i-tá mocnina, $i \in \langle 0 \div n-1 \rangle$ () je násobená príslušným koeficientom z množiny $\{A_{n-1}, A_{n-2}, ... A_1, A_0\}$ špecifikujúcej konkrétnu polynomickú funkciu. V zmysle definície ľubovolného súčinu je zrejmé, že získané výsledky sú opäť hodnoty z GF(2^q).
-Jednotlivé súčiny vytvárajú súčet. V zmysle definície súčtu je zrejmé, že získané výsledky sú opäť hodnoty z GF(2^q).
-Hodnota výsledného súčtu z čiastkových sčítancov v počte n je celočíselnou hodnotou polynomickej funkcie.

Popísaný algoritmus možno jednoducho realizovať pomocou funkcie

PolyFn(ξ As Long, q As Integer) As Long.

Tejto funkcii treba v inicializačnej fáze poskytnúť n-ticu ($n = 2^q$) koeficientov $A_0, A_1, ... A_{n-2}, A_{n-1}$ špecifikujúcich konkrétnu polynomickú funkciu. Následne jej môže byť poskytnutá hodnota neurčitej ξ, spolu s explicitne vyjadreným stupňom rozšírenia q.

V súlade s upraveným definičným vzťahom

$$(...((A_0 \oplus A_1 \otimes \xi) \oplus A_2 \otimes \xi^2) \oplus ....) \qquad (11)$$

je do vynulovaného pomocného sumačného akumulátora funkciou *PolySucet* pripočítaný koeficient A_0. Ďalej je volaním funkcie *PolySucin* vytvorený súčin hodnoty neurčitej ξ a koeficienta A_1. Získaný výsledok je funkciou *PolySucet* pripočítaný do sumačného akumulátora. V nasledujúcom kroku funkcia *PolyMocnina* vytvorí druhú mocninu hodnoty neurčitej ξ, ktorá je následne funkciou *PolySucin* násobená koeficientom A_2 a takto pripočítaná funkciou *PolySucet* do sumačného akumulátora.

Výpočet pokračuje striedavým volaním funkcií vytvárajúcim mocniny hodnoty neurčitej ξ, ich súčiny s prislúchajúcimi koeficientami špecifikujúcimi konkrétnu polynomickú funkciu až do získania vý-

sledného súčtu v sumačnom akumulátore. Tento je vrátený ako celočíselná reprezentácia hodnoty polynomickej funkcie.

3. ZÁVER

Polynomické funkcie nad konečným Galoisovým telesom sú základom nového pohľadu na riešenie problematiky logického riadenia technologických procesov. Praktické využívanie popisovanej zložitej algebry s výpočtárskou náročnosťou je v súčasnosti umožnené implementáciou príslušných operácií do programového vybavenia počítačov.

LITERATÚRA

[1] PRÍKOPOVÁ, A.: *Syntéza algoritmov pre sekvenčné obvody s detekciou porúch*. Dizertačná práca. Žilinská univerzita v Žiline, Elektrotechnická fakulta, 6/2006.

[2] PRÍKOPOVÁ, A., PALKOVÁ, Z.: *Univerzálna programová šablóna konečného automatu – teoretická báza*. AT&P journal 8/2006.

[3] PRÍKOPOVÁ, A., PALKOVÁ, Z.: *Implementácia algebraických operácií konečného telesa Galoisovho*. AT&P journal 8/2006.