SIMULÁCIA VLASTNOSTÍ RS KÓDOV PRE PRENOSOVÉ SYSTÉMY SÚVISIACE S BEZPEČNOSŤOU V PROGRAMOVOM PROSTREDÍ MATLAB

Ing. Mária Franeková, PhD.
Katedra riadiacich a informačných systémov
Elektrotechnická fakulta
Žilinská univerzita v Žiline

Abstrakt

Príspevok sa zameriava na opis možnosti použitia samoopravnýych Reed-Solomonových kódov v uzatvorených a otvorených prenosových systémoch definovaných normami EN 50159. Na účely simulácie vlastností RS (n,k,t) kódov ako aj Galoisových polí je v príspevku použité programové prostredie Matlab s podporou Communications Toolboxu.

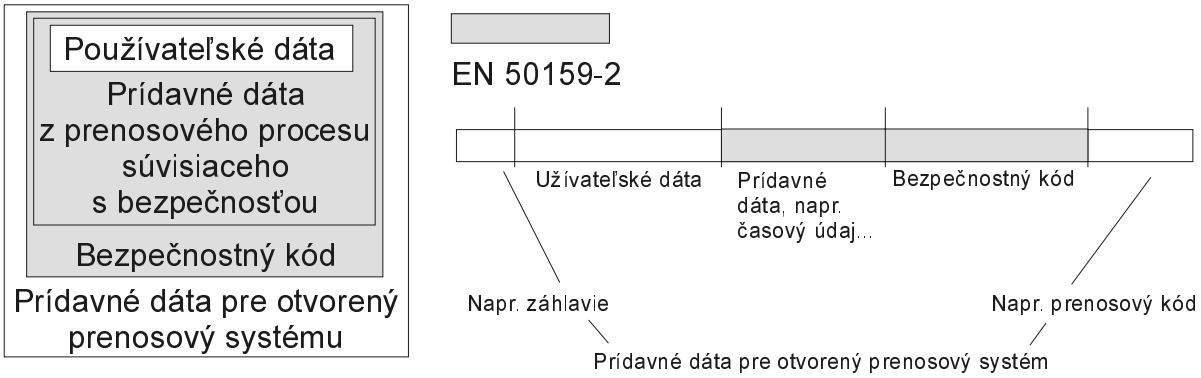
ÚVOD

Bezpečnostné požiadavky elementov komunikačného systému závisia od toho v akých aplikáciách je tento systém používaný. Ak ide o prenos veľmi citlivých dát, napr. pre potreby dopravného procesu (v rámci železničnej alebo leteckej dopravy), výber jeho častí je špecifikovaný normami [1],[2]. Takýto prenos dostáva v normách prívlastok - prenos súvisiaci s bezpečnosťou (z ang. *safety – related transmission*).

Pri prenose dát medzi zabezpečovacími systémami sú definované dve triedy systémov. Prvá trieda – uzatvorené prenosové systémy [3], zahrňuje také systémy, kde je určitá kontrola nad systémom, sú známe jeho charakteristiky a počet komunikujúcich účastníkov. Druhá trieda - otvorené prenosové systémy [4] zahrňuje všetky systémy, ktorých charakteristiky sú neznáme, alebo čiastočne známe a hrozí narušenie správ aj z vonkajšieho prostredia (napr. cez Internet, dátovú sieť…).

U oboch prenosových systémov je podľa [3] a [4] odporúčané na zabezpečenie prenosu proti vplyvu šumového prostredia použiť kódy len s detekčnými vlastnosťami. Pri výbere vhodného bezpečnostného kódu (v teórii kódovania sa skôr označuje pojmom kanálový kód - *Channel Coding*), sa berú sa do úvahy špecifiká a priority prenosu, akými je obmedzená časová platnosť vysielaných dát, spoľahlivosť a bezpečnosť prenosu s garantovanou pravdepodobnosťou chyby [5]. Pre zvolený (n,k) kód je potrebné realizovať podrobnú analýzu z pohľadu výpočtu pravdepodobnosti nedetegovanej chyby kódového

slova. Umiestnenie bezpečnostného kódu pre prenos dát súvisiaceho bezpečnosťou pre otvorený prenosový systém je znázornené na obr. 1.



Obr. 1 Model reprezentácie správy v rámci prenosového systému súvisiaceho s bezpečnosťou

Pozn.: V rámci otvorených prenosových systémov je nutné sa venovať okrem návrhu bezpečnostného kódu aj voľbe kryptografických algoritmov. Problematika súvisiaca s kryptografickými mechanizmami nie je súčasťou tohoto príspevku.

Najviac používaným detekčným kódom v tejto oblasti je blokový systematický cyklický kód, ktorý pracuje na princípe CRC-r (*Cyclic Redundancy Check*), u ktorého je podstatné vybrať vhodný primitívny generujúci polynóm g(x) rádu *r*, pre danú dĺžku kódového slova *n* a chybovú štruktúru v kanáli [6].

V teórií kanálového kódovania však existuje množstvo efektívnych kódovacích a dekódovacích techník, ktoré síce patria do množiny samopravných kódov (tzv. techniky FEC *Forward Error Control*), ale pri dekódovaní sa dá jednoznačne vyčleniť časť súvisiaca s detekciou [7], [8], čo by umožnilo použiť FEC techniky v aplikáciách definovaných podľa [3] a [4].

Dekódovanie väčšiny lineárnych kódov sa zakladá na tzv. syndrómovej technike, kde na základe hodnoty syndrómu sa určí, či pri prenose v danom kódovom slove došlo resp. nedošlo k narušeniu informácie. V prípade polynomiálnych kódov (kód, ktorého charakteristiky sa dajú vyjadriť pomocou algebry mnohočlenov) existujú tri typy syndrómov [9]. Syndróm s(x) definovaný vzťahom (1), čo je prípad binárnych cyklických kódov:

$$s(x) = c'(x) \bmod g(x) \tag{1}$$

Kde:

$c'(x)$ je prijaté kódové slovo kódu , definovaného generačným polynómom g(x).

Pretože všetky kódové slová sú deliteľné generačným polynómom g(x), syndróm s(x) nezávisí od vyslaného kódového slova, ale len od chýb, ktoré vznikli pri prenose.

Druhý spôsob možno matematicky vyjadriť, ak generačný polynóm g(x) je súčinom viacerých ireducibilných polynómov $g_1(x)$, $g_2(x)$,…, $g_j(x)$ (2), potom sa syndrómy počítajú podľa (3):

$$g(x) = g_1(x)g_2(x)...g_j(x) \tag{2}$$

$$\begin{aligned} s_1(x) &= c'(x) \bmod g_1(x) \\ s_2(x) &= c'(x) \bmod g_2(x) \\ &... \\ s_j(x) &= c'(x) \bmod g_j(x) \end{aligned} \tag{3}$$

Tento spôsob výpočtu syndrómu používa množina zovšeobecnených Haminngových kódov Bose Chaudhuri Hocquenghemových BCH kódov.

Tretí spôsob definovania syndrómu spočíva v zavedení vektorov S_1, S_2, …, S_j. Potom sa syndrómy počítajú podľa (4), kde z_j je koreňom generujúceho polynómu g(x):

$$\begin{aligned} S_1 &= c'(z_1) \\ S_2 &= c'(z_2) \\ &... \\ S_j &= c'(z_j) \end{aligned} \tag{4}$$

Ide o prípad výpočtu syndrómu pre skupinu Reed- Solomonových kódov, ktorých vlastnosti sú uvedené v ďalšej kapitole.

1 VLASTNOSTI REED-SOLOMONOVÝCH KÓDOV VHODNÉ PRE PRENOSOVÉ SYSTÉMY SÚVISIACE S BEZPEČNOSŤOU

Požiadavky na bezpečnostný kód závisia od vlastností a architektúry použitého prenosového systému vzťahujúceho sa k bezpečnosti. Na bezpečnostný kód sú všeobecne kladené nasledujúce požiadavky:

- schopnosť detekcie systematických a náhodných chýb,
- aby pravdepodobnosť nedetegovanej chyby bola pod garantovanou hranicou,
- rýchlosť kódovacieho a dekódovacieho algoritmu (správa je platná len určitý čas),
- praktická realizácia algoritmu.

Uvedené požiadavky z množiny detekčných kanálových kódov spĺňajú binárne cyklické kódy, ktoré dokážu detegovať náhodné zhluky chýb odpovedajúce stupni generujúcemu polynómu r so zvyškovou chybovosťou 2^{-r}. Zhluky chýb veľkých dĺžok dokážu detegovať a následne korigovať aj algoritmy nebinárnych (znakových) Reed-Solomonových kódov (ďalej RS kódy), ktoré v porovnaní s binárnymi kódmi sa vyznačujú vyššou rýchlosťou kódovania a

dekódovania (závisí od konkrétnej implementácie), pretože majú dobre prepracované dekódovacie techniky [97].

RS (n,k,t) kódy patria medzi systematické, lineárne, blokové kódy, u ktorých pri kódovaní každý blok dĺžky k je delený do m – bitových symbolov. Ich objaviteľmi sú Irving Reed a Gustave Solomon a ich vlastnosti sú podporované matematickými základmi Galoisovej algebry, objavenej matematikom Evariste Galoisom. RS dekodér je schopný opraviť $(n-k)/2$, alebo t symbolov. Ide o efektívny algoritmus, ktorý má schopnosť korekcie zhlukov chýb veľkých dĺžok, u ktorého sa z celkového dekódovacieho algoritmu dá jednoducho vyčleniť detekčná časť kódu a je ho možno použiť pre aplikácie definované normami [3] a [4].

V súčasnosti existuje niekoľko modifikácii RS kódov, používaných :

- v pamäťových médiách (ochrana hard diskov a kompaktných diskov),
- v bezdrôtovej komunikácií (mobilné telefóny, mikrovlnové linky),
- v satelitnej komunikácií,
- v širokopásmových modemoch.

RS kódy používajú aritmetiku Galoisových polí a sú definované v ľubovoľnom konečnom Galoisovom poli GF(q)=GF(p^m) s generačným polynómom g(x):

$$g(x) = (x - z^{j})(x - z^{j+1})...(x - z^{j+2t-1}) \tag{5}$$

Kde:

q je mocnina prvočísla p^m , alebo počet prvkov Galoisového poľa,

j je celé nezáporné číslo (v praxi sa najčastejšie volí j=0, alebo j=1)

z je primitívny prvok GF(q).

Teória Galoisových polí s definovanými pravidlami sčítania a násobenia je podrobne spracovaná napr. [10], [11]. V tab. 1 je uvedený príklad Galoisového poľa GF (2^3), pozostávajúceho z 8 prvkov {0, z^0, z^1, z^2, z^3, z^4, z^5, z^6}. Polynomický tvar nad primitívnym poľom GF(2) sa získa ako zvyšok delenia v aritmetike mod2 s ireducibilným polynómom p(x) stupňa m, čo v prípade poľa GF (2^3) je $p(x)=z^3+z+1$. V tab. 1 v poslednom stĺpci je uvedený aj binárny tvar nad GF (2).

Pre dekódovanie RS kódov sa používa syndrómová metóda dekódovania, pričom syndrómy pre tento typ kódov sú definované vzťahom (4). Úlohou dekódovania je nájsť chybové slovo e(x) na základe prijatého slova c'(x), pričom e(x) má nenulové koeficienty len na miestach, ktoré zodpovedajú pozícií chýb. Ak nastane t chýb platí:

$$S_k = \sum_{i=1}^{t} Y_i X_i^{\,k} \tag{6}$$

Kde:

k nadobúda hodnoty k = 0, 1, …,2t-1,

X_i označuje lokátor i-tej chyby,

Y_i označuje hodnotu chyby.

Tab. 1 Konečné Galoisove pole GF (2^3)

Prvky poľa	Polynóm nad GF (2)	Binárny tvar nad GF (2)
0	0	000
z^0	1	001
z^1	x	010
z^2	x^2	100
z^3	x + 1	011
z^4	x^2 + x	110
z^5	x^2 + x + 1	111
z^6	x^2 + 1	101

Proces dekódovania originálneho samoopravného RS kódov možno zhrnúť do nasledujúcich bodov:

1. výpočet syndrómov S_k,
2. nájdenie polynómov lokátorov chýb σ(x),
3. nájdenie koreňov lokátorov σ(x) – lokátory X_i,
4. výpočet hodnôt Y_i a následná korekcia chyby.

Na výpočet zložitosti jednotlivých krokov dekódovania RS kódov pomocou syndrómovej metódy boli robené rôzne štúdie [12]. Voľba zvolenej metódy závisí od dĺžky kódu, spôsobu realizácie (HW, SW), požiadavky na rýchlosť dekódovania a iné. Výpočet rovnice σ(x) možno realizovať napr. Gausovou eliminačnou metódou, Gausovou Jordanovou redukciou, Wonogradovým algoritmom, alebo Berlekampovým - Masseyho algoritmom (posledný uvedený sa odporúča, ak počet chýb t >5.) Tretí krok možno riešiť pomocou Chienovho algoritmu, štvrtý sa dá realizovať najlepšie pomocou Forneyho algoritmu.

Ak by sme z dekódovacie algoritmu vyčlenili len časť odpovedajúcu detekcii chyby z uvedeného postupu vypočítať len prvý krok – syndrómy S_k, čím sa originálny dekódovací

algoritmus značne urýchli. Syndrómy pre jednotlivé generujúce korene možno vypočítať podľa (7) , pričom výpočet sa dá urýchliť úpravou podľa (8).

$$S_k = c'(z^k) = c(z^k) + e(z^k) \tag{7}$$

pre k=0,1,…,2t-1.

$$S_k = (...(c'_{n-1} z^k + c'_{n-2}) z^k + ... + c'_1) z^k + c'_0 \tag{8}$$

Ak po výpočte hodnoty všetkých syndrómov S_k nenulové, pri prenose došlo k chybe a správu netreba akceptovať, prípadne požiadať o jej opakovanie. V opačnom prípade bola správa prijatá bezchybne.

2 SIMULÁCIA VLASTNOSTÍ RS KÓDOV V PROGRAMOVOM PROSTREDÍ MATLAB A COMMUNICATIONS TOOLBOX

Pri výbere vhodného RS (n,k,t) kódu a na overenie jeho vlastností pre dané prenosové prostredie možno použiť programové prostredie Matlab s podporou knižníc Communications Toolbox (využíva implementované M súbory), alebo Communications Blockset v spojení so Simulinkom (využíva knižnicu MDL funkčných blokov) [13]. V tomto prostredí možno simulovať algoritmus kodéra/dekódera samostatne, alebo po ich zapojení do prenosového reťazca s definovaným modelom komunikačného šumového kanála. Simuláciu prenosu pomocou RS kódov je výhodné sledovať v tomto prostredí aj z dôvodu kompletnej, dobre prepracovanej podpory pre aritmetiku s Galoisovými poliami, s ktorou je teória RS kódov zviazaná. Aj keď väčšina MDL funkčných blokov z knižnice Communications Blockset má svoj ekvivalent v knižnici M súborov Communications Toolboxu, táto skutočnosť neplatí pre oblasť Galoisových polí, ktoré sú podporované len Communications Toolboxom. Preto je pre detailnejšie sledovanie uvedenej problematiky výhodnejšie realizovať simuláciu prenosu prostredníctvom M súborov. Pri tvorbe programu je potrebné správne definovať parametre v používaných M funkciách, pretože spôsob práce so znakovými RS kódmi je odlišný od klasických binárnych kódov. Na príkladoch budú uvedené špecifiká zadávania parametrov v niektorých funkciách súvisiacich s aritmetikou Galoisových a polí a procesom kódovania a dekódovania RS kódov. Výsledky budú konfrontované s teoretickými vedomosťami uvedenými v predchádzajúcej kapitole.

Communications Toolbox poskytuje podporu funkcií pre primitívne, ako aj pre rozšírené Galoisove pole $GF(q=p^m)$, (primitívne, ak q = 1 a m = 1, rozšírené ak m > 1). Výpis všetkých funkcií možno nájsť v príručke [13], alebo na www stránkach mathwork [14].

Pre potreby samoopravných techník kódovania pomocou BCH a RS kódov knižnica ponúka zúženú množinu funkcií len nad Galoisovým poľom GF (2^m). Aby algoritmus kódovania a dekódovania bol vykonávaný efektívne dĺžka kódového slova *n* musí spĺňať rovnosť $n=2^m-1$ a redundancia r = n-k, by mala byť nepárne číslo.

Na zobrazenie prvkov Galoisového poľa GF(q) možno použiť funkciu **gftuple.** Ak by sme chceli zobraziť prvky Gaoisového poľa definované v tab. 1 je potrebné zadať:

```
m=3;p=2;
[tp,idx]=gftuple([-1:p^m-2]'m,p)
```

Po vykonaní príkazu sa v premennej `tp` nachádzajú prvky GF(2^3) nad GF (2) v binárnom formáte. Pričom váha jednotlivých koeficientov je opačná v porovnaní s tab. 1. V premennej `idx` sú jednotlivé prvky poľa, pričom znak –Inf (nekonečno) odpovedá znaku 0 a ostatné prvky sú uvedené v exponenciálnom tvare t. j. exponent 0 predstavuje prvok z^0 , exponent 1 odpovedá znaku z ,…, exponent 6 odpovedá znaku z^6 .

Okrem exponenciálneho formátu, možno na reprezentáciu elementov Galoisoveho poľa použiť aj polynomický formát, kde váha jednotlivých elementov je v súlade s formátom funkcií súvisiacich s mnohočlenmi (od najnižšej mocniny po najvyššiu).

Na výpočet generačného polynómu definovaného vzťahom (5) možno v Communications Toolboxe použiť funkciu **rspoly.**

Ako príklad uveďme generačný generačný polynóm RS kódu (7,3) pre m=3, p=2, zároveň s výpočtom počtu korigovaných chýb t.

```
[pg,t]=rspoly(7,3)
```

Výsledkom príkazu je riadkový vektor `pg`, ktorý reprezentuje koeficienty generačného polynómu (od najvyššej mocniny, pričom každý koeficient je element GF(2^3) uvedený v exponenciálnom formáte.

```
pg =      3     1     0     3     0
```

Výsledný tvar generačného polynómu potom v súlade so vzťahom (5) je

$g(x) = z^3x^0 + z^1x + z^0x^2 + z^3x^3 + z^0x^4$

Počet korigovaných symbolov daného kódu je uložený v premennej *t* a odpovedá teoretickým vedomostiam z úvodnej kapitoly t = (n-k)/2=2 symboly, alebo 6 bitov (1 symbol je daný 3 bitmi).

Na kódovanie a dekódovanie RS kódov možno použiť niekoľko funkcií, ktoré sa odlišujú rýchlosťou výpočtu, počtom zobrazovaných parametrov a zvoleným formátom. Správu a kódové slovo možno reprezentovať troch formátoch:

- binárny formát ,
- decimálny formát,
- exponenciálny formát.

V simulovanom programe možno použiť funkcie na konverziu medzi jednotlivými zvolenými formátmi. Pri spracovaní kódových slov väčších dĺžok je z dôvodu rýchlosti výhodné použiť binárny formát, pretože funkcie vnútorne pracujú v tomto formáte .

Pre potreby kódovania/dekódovania RS kódov možno použiť funkcie tzv. nižšej úrovne **encode**, alebo vyššej úrovne **rsenco** a **rsencode**. Funkcia **rsenco** pracuje so všetkými uvedenými formátmi, kým funkcia **rsencode** len v exponenciálnom formáte.
Ako príklad uveďme krátky program pre už uvedený RS kód (7,3) na zakódovanie a dekódovanie správy (pre lepšiu názornosť binárnej forme).

```
m=3;
n=2^m-1;
k=3;
pg=rspoly(7,3);
msg=[100;110;010];
code=rsenco(msg,n,k,'binary',pg)
```

Výsledkom premennej code je 21 bitová zakódovaná hodnota v tvare

```
  Columns 1 through 12

     0     1     1     0     0     1     1     1     0     0
1     1

  Columns 13 through 21

     0     0     0     0     0     0     0     0     0
```

Pre zaujímavosť uveďme, že Communications Toolbox má implementovanú aj funkciu **rsencof** na kódovanie ASCII znakov pomocou RS kódu (127, 117)

Ekvivalentne ku všetkým kódovacím funkciám existujú inverzné funkcie na dekódovanie. Dekódovací postup používa rovnaké procedúry jako pre BCH kódy a je v súlade z postupom častí uvádzaným v teoretickej časti. Toolbox podporuje aj niektoré dielčie funkcie z dekódovacieho algoritmu napr. na nájdenie lokátora chýb σ(x), možno použiť funkciu **errlocp**.

Nebolo možné uviesť všetky funkcie podporujúce problematiku RS kódov a opísať skúsenosti pri simulácií ich vlastností. Treba však skonštatovať, že programová simulácia s ich využitím môže uľahčiť prácu dizajnera prenosových systémov (aj prenosových systémov súvisiacich s bezpečnosťou).

ZÁVER

Samoopravné techniky bezpečnostných RS kódov so syndrómovou technikou dekódovania sú efektívnymi algoritmami pre korekciu, ako aj detekciu systematických zhlukov chýb, vyskytujúcich sa v kanáli. Po oddelení korekčnej časti algoritmu ich možno použiť na ochranu dát súvisiacich s bezpečnosťou, v súlade s normami [3], [4]. Pri výbere vhodného (n,k,t) RS kódu, ako aj na otestovanie jeho korekčných vlastností je výhodné použiť programové prostredie Matlab s Communications toolboxom. Softvérová implementácia RS kódov sa v literatúre uvádza ako časovo náročnejšia a pre potreby rýchleho prenosu je odporúčaná viac implementácia na báze hardvérovej Pre praktickú realizáciu sa odporúča počet znakov m voliť m=3, alebo m=8. V prípade výskytu náhodných chýb v kombinácii so systematickými zhlukmi veľkých dĺžok možno RS kódy kombinovať s konvolučnými kódmi v tzv. kombinovanom kódovacom systéme.

LITERATÚRA

[1] Kunhart, M.: Design of Interlocking RAMS Parameters, 11. Medz. konferencia ŽU v Žiline, Veda, vzdelávanie a spoločnosť, 17.-19.9.2003, s.141-144

[2] Lazar, T., Kvasnica, P.: Paradigm of decentralised system control operating speed and temperature of the aircraft engine output gasses, zborník XXXV. Jarní medzinárodní konferenci Modelovaní a simulace systémů MOSIS' 03, 23. až 25. apríla 2003. Brno, Česká republika

[3] ČSN EN 50159-1 Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracovaní dat, Část 1: Komunikace v uzavřených přenosových zabezpečovacích systémech., ČTN, april 2002

[4] ČSN EN 50159-2 Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracovaní dat, Část 2: Komunikace v otvořených přenosových zabezpečovacích systémech, ČTN, máj 2002

[5] Janota, A., Rástočný, K., Tomašov, P., Zahradník, J.: System with Defined Level of Safety, IFAC Workshop on PDS 2000, Ostrava, február, 2000, ČR, s. 237-241

[6] Franeková, M.: Modelovanie komunikačných systémov v programovom prostredí Matlab, Communications Toolbox a Simulink, skriptá ŽU v Žiline, 2003

[7] Adámek, J.: Kódovaní a teorie informace, ČVUT, Praha, 1991

[8] Clarc, C. C., Cain, J. B.: Error –Correcting for Digital Communications, Plenum Press, New York, 1988

[9] Farkaš, P.: Kódovanie a modulácie, STU, Bratislava, 1993

[10] Blahut, Richard E. : Theory and Practice of Error Control Codes. Reading, Mass.: Addison-Wesley, 1983.

[11] Lang, Serge.: Algebra. Third Edition. Reading, Mass.: Addison-Wesley, 1993.

[12] Farkaš, P.: Complexity of Software Realization of Decoders of some Reed-Solomon Codes,

Elektrotechnický časopis 3/92, s. 81-86

[13] Matlab Communications Toolbox, User's Guide, version 2, The Math Work, 1997

[14] http://www.mathworks.co.uk/…k_r12pl/help/toolbox/comm/tutorl120.shtm

Ing. Mária Franeková, PhD.
KRIS, Elektrotechnická fakulta
Žilinská univerzita
Veľký diel, blok NF
Slovensko
Tel.: +421-041-5133346
Email: maria.franekova@fel.utc.sk