Technická zpráva 2018

Pseudonáhodné posloupnosti v radionavigačních systémech

Algoritmy generátorů

Autor: Petr BOJDA
Adresa: Morávka 575, okr. Frýdek-Místek
Dne: 20. prosince 2018
Verze dokumentu: 1.0

1 Úvod

Hlavní cíl zprávy

Zpráva vzniká na podnět výzkumného týmu Katedry Leteckých elektrotechnických systémů k podpoře výzkumného úkolu v oblasti terestriálních navigačních systémů s rozprostřeným spektrem. Cílem je nalézt vhodnou strukturu a parametry signálu tak, aby co nejlépe vyhověl požadavkům na celkový systém. Tato práce, vzniklá v průběhu roku 2018, se zabývá analýzou pseudonáhodných posloupností, čili kódů PRN, které v systémech s rozprostřeným spektrem plní dvě úlohy. Jednak zajišťují jednoznačnost při výběru zdroje signálu v přijímači (tzv. CDMA - Code Division Multiple Access) a potom plní úlohu tzv. časoměrného kódu. Obě hlediska je potřeba při návrhu systému zohlednit a přizpůsobit jim volbu kódu. Zpracovaná práce se těmito otázkami zabývá.

Použité prostředky

Zpráva vznikla jako komentovaný popis a dokumentace návrhu generátorů kódů, jejich simulace, analýzy a implementace. Cílovou platformou je SDR, a veškeré kroky směřují k nalezení efektivního způsobu realizace bloků generátorů kódu pomocí vhodných softwarových modulů. Veškeré softwarové nástroje a prostředky použité při zpracování této zprávy jsou v kategorii "Open-Source Software License", zejména BSD licence v případě simulačních nástrojů a GNU GPL v případě implementačních nástrojů. Textová část je editována v systému Latex. Jednotlivé práce byly odvedeny na počítačích s operačním systémem Linux, distribuce Ubuntu. Nebyly použity žádné softwarové nástroje podléhající komerční licenci.

K simulacím je využit systém knihoven v jazyce Python, zejména pak knihovny NumPy, Matplotlib a SciPy nainstalovaných v rámci balíku Anaconda 4.3.24. Tyto nástroje umožnily jednak ověření konceptu generování kódů a také analýzu jejich vlastností. Následné implementace generátorů kódů byly uskutečněny pomocí software GNU Radio a to ve verzi 3.7.10.1.

S využitím funkcí těchto knihoven byly vytvořeny soubory funkcí vypočítávajících korelační koeficient v časové i kmitočtové oblasti. Jak bylo uvedeno výše, všechny simulace jsou psány v programovacím jazyce Python.

2 Generátory pseudonáhodných posloupností

Pseudonáhodné posloupnosti (PRS - Pseudo Random Sequence) jsou základním stavebním prvkem systému a rozprostřeným spektrem typu DSSS (Direct Sequence Spread Spectrum). Plní následující role:

Role pseudonáhodných posloupností v systému s rozprostřeným spektrem

- Rozprostření spektra přenášeného signálu
- Výběr požadovaného signálu v přijímači a potlačení rušení a šumu
- Sesynchronizování kopie signálu generované v přijímači se signálem přijímaným

2.1 Druhy pseudonáhodných posloupností

Pro rozdělení pseudonáhodných posloupností by se jistě našlo více různých kritérií. Zde zvolené kritérium [1] [2] souvisí s charakterem použití posloupnosti v radionavigačním systému k měření času. Obecně všechny pseudonáhodné posloupnosti mají jednu ze základních charakteristik - svou *délku*. Tedy počet bitů obsažených v posloupnosti, zde značené N. Záleží pak na způsobu tvorby vysílaného signálu, jestli se bude posloupnost generovat periodicky nebo jen jednorázově. To potom ovlivňuje charakter autokorelační funkce C_{xx}. Pokud je posloupnost generována opakovaně, pracuje tento systém s korelační funkcí *periodickou*, naopak při jednorázovém vyslání posloupnosti jde o systém s *aperiodickou* korelační funkcí.

Jak již bylo řečeno, systémy s periodickou korelační funkcí pracují tak, že průběh pseudonáhodné posloupnosti se při vysílání periodicky v čase opakuje. Tudíž i jejich korelační funkce vykazuje periodický charakter s postupně se opakujícími maximy. Hlavní využití je v komunikačních systémech typu CDMA. Tímto způsobem se využívají zejména následující posloupnosti:

Posloupnosti využívané s periodickou korelační funkcí

- posloupnost maximální délky (MSL - Maximum Length Sequence, m-sequence)
- Goldovy posloupnosti
- odvozené Goldovy posloupnosti (Gold like sequences)
- Kasamiho posloupnosti

- Ipatovovy posloupnosti
- Huffmanovy posloupnosti

Posloupnosti využívané s aperiodickou korelační funkcí

Systémy s aperiodickou korelační funkcí používají signál, v němž se pseudonáhodná posloupnost neopakuje, ba co víc, nebývá ani celá vygenerovaná. V signálu se často vysílá pouze její část. Tyto typy systémů využívají signál DSSS výhradně k synchronizaci a měření času. Posloupnosti využívané v těchto systémech jsou hlavně

- Williardovy kódy
- Barkerovy kódy
- Neuman-Hoffmanovy kódy
- Frankovy kódy
- Zadovovy-Chu kódy

2.2 Způsob generování pseudonáhodné posloupnosti

Algoritmy používané ke generování pseudonáhodných posloupností jsou s výhodou popisovány pomocí polynomů s binárními koeficienty. Hardwarová realizace generujících polynomů pak využívá struktury posuvných registrů s vyvedenými zpětnými vazbami (SSRG - Simple Shift Register Generator). Dále je důležité zmínit, že se využívají výhradně *lineární* registry [1]. Pojem linearity se tady odkazuje na tvar stavového diagramu, kdy je žádoucí, aby každému jednomu ze stavů registru předcházel zase jen jeden jediný stav. Tedy stavový diagram je tvořen "řetězem"stavů – jeden za druhým – bez větvení. Respektive, jde o propojení stavů do kruhu, kdy se z posledního stavu dostává registr opět do stavu prvního.

2.2.1 Použitý matematický aparát

Před popisem jednotlivých algoritmů generátorů je užitečné definovat základní pojmy a předestřít matematický aparát, který bude v popisu použit [1]. Zejména zde bude prostor věnován aritmetice Galoisových (konečných) polí a aritmetice polynomů, [1].

[1] Omlouvám se čtenáři za s největší pravděpodobností nepřesnou českou terminologii. Prezentovaný a zúžený výklad potřebných matematických pojmů čerpá převážně z anglicky psaných zdrojů a literatury. Nebyla provedena patřičná jazyková korektura ani ověřena správnost zde uváděných pojmů v českém jazyce.

Galoisovy pole

Galoisovo pole je zjednodušeně definovat jako množinu prvků konečného počtu. Počet prvků pole je q. Aby pole mohlo být označeno za Galoisovo, musí pro ně platit následujících devět podmínek:
Nechť a, b a c jsou prvky pole $\mathcal{G}$. Potom

i Pro všechny $a, b \in \mathcal{G}$ jsou definovány dvě základní operace mezi prvky pole, a sice *sčítání* $a + b$ a *násobení* $a \cdot b$.

ii Všechny operace mezi prvky pole jsou uzavřené: $a, b \in \mathcal{G} \Rightarrow a \circ b = c \in \mathcal{G}$.

iii Existuje nulový prvek (angl. *additive identity element*) 0: $a \in \mathcal{G} : a + 0 = a$.

iv Existuje jednotkový prvek (angl. *multiplicative identity element*) 0: $a \in \mathcal{G} : 1 \cdot a = a$.

v Existuje záporný prvek (angl. *additive inverse element*) $(-a)$: $a \in \mathcal{G} : a + (-a) = 0$. Tento prvek umožňuje odečítání.

vi Existuje prvek s opačnou hodnotou (angl. *multiplicative inverse element*) (a^{-1}): $a \in \mathcal{G} : a \cdot a^{-1} = 1$. Tento prvek umožňuje opraci dělení.

vii Platí asociativní zákon: $a, b, c \in \mathcal{G} : a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$

viii Platí komutativní zákon: $a, b \in \mathcal{G} : a + b = b + a, a \cdot b = b \cdot a$

ix Platí distributivní zákon: $a, b, c \in \mathcal{G} : a \cdot (b + c) = a \cdot b + a \cdot c$

Další podmínka se vztahuje k počtu prvků q. Aby pole bylo považováno za Galoisovo, pro q musí platit:

$$q = p^m, \tag{1}$$

kde p je prvočíslo (angl. *prime*) a m je kladné celé číslo (angl. *positive integer*). Galoisovy pole se potom značí: $\mathbf{GF}(q)$ z angl. *Galoise Field*. Příklady polí: $\mathbf{GF}(11)$, $\mathbf{GF}(81) =$

Výklad vychází z matematické disciplíny či oboru *Teorie grup* podle Évariste Galoise nebo *Modulární aritmetiky* podle Karla Friedricha Gausse. Dělení popisovaných objektů na grupy, cyklické grupy a pole, potažmo konečná neboli Galoisova pole nemusí být plně v souladu s českou odbornou terminologií a vychází z překladu anglických pojmů "*Groups*", "*Rings*"a "*Fields*", resp. "*Galoise Fields*"neboli "*Finite Fields*".

GF(3^4). Třeba pole **GF**(256) = **GF**(2^8) je používáno při popisu kryptoalgoritmu standardu AES (angl. *Advanced Encryption Standard*). Zvláštní pozornost bude dále v souvislosti s popisem generátorů binárních pseudonáhodných posloupností věnována poli **GF**(2^1), tedy poli binárnímu.

Aritmetika Galoisových polí

Aby operace s prvky Galoisových polí splňovaly výše uvedené podmínky, je nutné dodržet určité zásady jejich provádění.
Pro $a, b, c, d, e \in$ **GF**$(p) = \{0, 1, 2, \ldots p-1\}$ se operace definují následovně:

Sčítání (spolu s odečítáním) a násobení jsou počítány známým způsobem. Ovšem aby byla dodržena podmínka uzavřenosti (ii), jsou doplněny navíc operací modulo p.

I sčítání: $a + b \equiv c \mod p$

II odečítání: $a - b \equiv c \mod p$

III násobení: $a \cdot b \equiv c \mod p$

Dělení, nebo inverze podle (vi) je operace, jež zasluhuje zvláštní pozornost. Pro $a \in$ **GF**$(p) = \{0, 1, 2, \ldots p-1\}$ prvek a^{-1} musí splňovat podmínku:

$$a \cdot a^{-1} \equiv 1 \mod p, \tag{2}$$

Inverzní prvek a^{-1} je pak nalezen pomocí Euklidova algoritmu.

Aritmetika polynomů

Následuje popis operací prováděných nad polynomy. Nechť $f(x)$ je polynom řádu n jehož koeficienty jsou prvky binárního pole **GF**(2).

$$f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n, f_i \in \mathbf{GF}(2) \tag{3}$$

a polynom $g(x)$, což je polynom řádu m rovněž nad polem **GF**(2)

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_m x^m, g_i \in \mathbf{GF}(2) \tag{4}$$

přičemž platí $n > m$.

Potom operace nad těmito polynomy jsou definovány následovně:

I sčítání

$$\begin{aligned} f(x)+g(x) &= (f_0+g_0)+(f_1+g_1)x+(f_2+g_2)x^2+\ldots+(f_m+g_m)x^m \\ &\quad +(f_{m+1})x^{m+1}+\ldots+f_nx^n, \end{aligned} \tag{5}$$

II násobení

$$f(x)\cdot g(x)=a_0+a_1x+a_2x^2+\ldots+a_{n+m}x^{n+m}, \tag{6}$$

kde

$$\begin{aligned} a_0 &= f_0g_0 \\ a_1 &= f_0g_1+f_1g_0 \\ a_2 &= f_0g_2+f_1g_1+f_2g_0 \\ &\vdots \\ a_i &= f_0g_i+f_1g_{i-1}+f_2g_{i-2}+\ldots+f_ig_0 \\ &\vdots \\ a_{n+m} &= f_ng_m, \end{aligned}$$

III dělení, resp. inverze

$$\begin{aligned} \frac{f(x)}{g(x)} &= q(x)+\tfrac{r(x)}{g(x)}, \\ f(x) &= q(x)g(x)+r(x), \end{aligned} \tag{7}$$

přičemž $q(x)$ je nazýván *podílem*, angl. *quotient* a $r(x)$ *zbytkem*, angl. *reminder*. Podíl a zbytek jsou pak nalezeny pomocí rozšířeného Euklidova algoritmu.

Je nutno podotknout, že všechny dílčí operace sčítání a násobení s koeficienty polynomů jsou prováděny v souladu s pravidly platnými pro aritmetiku nad polem $\mathbf{GF}(2)$. To znamená, že jsou doplněny o modulo 2.

3 Analýza generovaných posloupností

generování posloupností - výpočetní náročnost - zobrazení auto a vzájemných korelačních funkcí - kmitočtová spektra

4 Implementace generátorů do GNU Radia

Zde budou doplněny postupy a algoritmy, tak jak byly napsány v jazyce C a implementovány coby samostatné bloky do GNU Rádia.

5 Výsledky implementací a jejich srovnání se simulacemi

Veškeré simulace byly vytvořeny v jazyce Python, variantě 3.5.2. s využitím nástrojů knihoven Matplotlib 1.5.3, NumPy 1.11.1 a SciPy 0.18.1, vše instalováno v rámci balíku Anaconda 4.2.0. Simulace byly napsány, vyzkoušeny a provozovány na počítači s operačním systémem Linux Ubuntu 16.04. ovaných vstupním vektorem t.

Reference

[1] J. Holmes, *Spread Spectrum Systems for GNSS and Wireless Communications*, ser. GNSS technology and applications series. Artech House, 2007, no. v. 45. [Online]. Available: https://books.google.cz/books?id=-AUfAQAAIAAJ

[2] N. Levanon and E. Mozeson, *Radar Signals*, ser. Wiley - IEEE. Wiley, 2004. [Online]. Available: https://books.google.cz/books?id=l_2lHI9fVHUC