BCH ENCODER AND DECODER

Petr ČÍKA, Master Degree Programme (5)
Dept. of Telecommunications, FEEC, BUT
E-mail: xcikap00@stud.feec.vutbr.cz

Supervised by: Dr. Karel Němec

ABSTRACT

This project deals with a large class of error-correcting cyclic Bose, Chaudhuri and Hocquenghem (BCH) codes. BCH codes operate over algebraic structures called Galois Field. The aim of the project is to create a computer application which simulates encoding and decoding proccess by BCH (15,5) code step by step, that could serve as a teaching aid.

1 ÚVOD

Přenos dat v telekomunikačních kanálech se v současné době děje většinou pomocí diskrétního dvoustavového signálu (0, 1). Tyto data jsou před vysláním do kanálu zabezpečeny zabezpečovacím kódem. Zabezpečovací kódování spočívá v přidávání zabezpečovacích prvků k nezabezpečené zprávě podle pravidel, definujících použitý zabezpečovací kód. V tomto příspěvku bude podrobně rozebrán lineární blokový cyklický BCH kód, pracující pouze s binárními daty. V současné době se používá například v doporučení ITU-T H.261 jako standard pro kódování videa ve videokonferencích.

2 BCH KODÉR

BCH (n, k) kodér je obdobou cyklického kodéru. Je zadán vytvářecím mnohočlenem $G(x)$, jehož řád určuje počet zabezpečovacích prvků $r = (n - k)$. V kódové kombinaci délky n bitů má na prvních k místech prvky nezabezpečené zprávy a na zbývajících r místech zabezpečovací prvky. Zabezpečení BCH kódem se provádí pomocí rovnice

$$F(x) = Z(x) \cdot x^{(n-k)} + R(x) = M(x) \cdot G(x) + R(x) + R(x) = M(x) \cdot G(x), \qquad (1)$$

kde $Z(x)$ je mnohočlen bloku nezabezpečené zprávy, $G(x)$ je vytvářecí (generující) mnohočlen definující zabezpečovací kód, $M(x)$ je mnohočlen podílu, $R(x)$ je mnohočlen zbytku a $F(x)$ je mnohočlen zabezpečené zprávy. Více o kódování najdeme v [1], [2].

3 BCH DEKODÉR

BCH kód s minimální Hammingovou vzdáleností $(2t + 1)$ je schopen opravit t - násobné

chyby. Pokud tedy existuje vyslané slovo $F'(x)$ obsahující t nebo méně chyb, stačí najít chybové slovo $E(x)$. Potom je kódové slovo $F(x) = F'(x) - E(x)$. Chybové slovo získáme dekódováním $F'(x)$. Jednou z metod dekódování BCH kódu je maticová metoda skládající se ze tří fází dekódování. Kontrola správnosti, stanovení chybového mnohočlenu a oprava chyb.

Kontrola správnosti se provádí postupným dosazováním kořenů α vytvářecího mnohočlenu $G(x)$ do mnohočlenu přijaté zprávy. Takto vzniklé rovnice představují syndromové rovnice. Pro kořeny mnohočlenu $G(x)$ platí: $g(\alpha) = g(\alpha^2) = \ldots = g(\alpha^{2t}) = 0$. Při bezchybném přenosu pro kódové slovo $F(x) = c_0 + c_1x_1 \ldots + c_{n-1}x_{n-1}$ platí pro syndromové rovnice $s_1(\alpha) = s_2(\alpha^2) = \ldots = s_{2t}(\alpha^{2t}) = 0$. Při přijetí chybového slova vznikne soustava syndromových rovnic, díky které mohou proběhnou další fáze dekódování.

Stanovení chybového mnohočlenu je druhou fází dekódování. Lokátorem chyb se nazývá polynom

$$L(x) = l_0 + l_1x + l_2x^2 + \ldots l_px^p \ . \qquad (2)$$

Pro výpočet koeficientů $l_i\,(0 < i \le p)$ polynomu (2) musíme nejprve stanovit počet chyb. Ten stanovíme pomocí rovnice

$$\mathbf{M_q} = \begin{bmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ s_2 & s_1 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{2q-2} & s_{2q-1} & \ldots & \ldots & s_q & s_{q-1} \end{bmatrix}. \qquad (4)$$

Je-li determinant matice $\mathbf{M_q}$ $(q > p + 1)$ roven nule, a zároveň determinant matice $\mathbf{M_p}$ $(q = p)$ a $\mathbf{M_{p+1}}$ $(q = p + 1)$ je nenulový, potom p je skutečný počet chyb. Koeficienty lokátoru chyb l_i potom stanovíme vyřešením soustavy

$$\mathbf{M_q} \cdot \begin{bmatrix} l_1 \\ l_2 \\ \ldots \\ l_q \end{bmatrix} = \begin{bmatrix} s_1 \\ s_3 \\ \ldots \\ s_{2q-1} \end{bmatrix}, \qquad (5)$$

kde $q = p$. Koeficient $l_0 = 1$.

Jestliže jsou známy všechny potřebné koeficienty lokátoru $L(x)$, proběhne poslední fáze dekódování. Postupným dosazováním prvků Galoisova tělesa $\alpha^0, \alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{-(n-1)}$ do lokátoru chyb se určí jeho kořeny. Bity na i-tém místě přenášené zprávy se invertují právě tehdy, když $l(\alpha^{-i}) = 0$. Více o dekódování najdeme v [2].

4 SOFTWAROVÁ APLIKACE PRO KODEK BCH (15, 5) KÓDU

Softwarová aplikace navržená pro kodek BCH (15, 5) kódu vyobrazená na Obr.1 ukazuje jednotlivé fáze kódování a dekódování zmíněným kódem. Data určená ke kódování se mohou zadávat buď ve tvaru znaků ASCII kódu, nebo v binární podobě (tj. posloupnost nul a jedniček). Podle formátu vstupních dat se volí tlačítko ke kódování.

Při kódování znaků ASCII se zpráva nejprve rozdělí do bloků po osmi bitech, které definují jednotlivé znaky ASCII kódu, a poté se celá bitová posloupnost rozdělí pětic bytů. Pokud není celkový počet bitů beze zbytku dělitelný pěti, doplní se na konec zprávy nulové

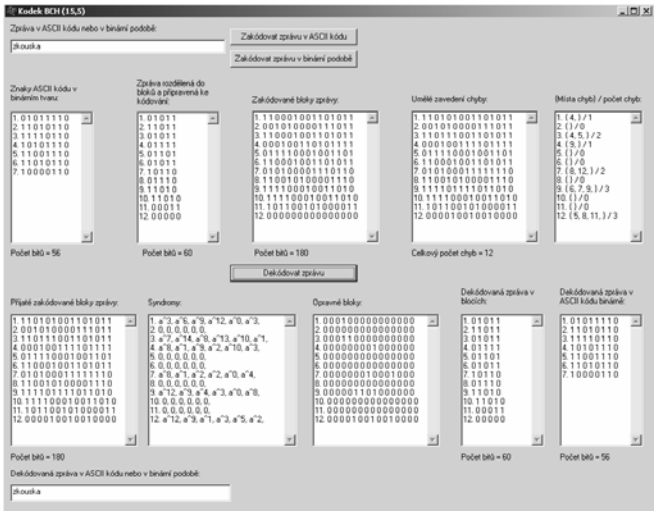
bity tak, aby celkový počet bitů byl beze zbytku dělitelný číslem 5.

Při zadávání dat v binární podobě se data ihned rozdělí do bloků po pěti bytech. Pokud celkový počet bitů není beze zbytku dělitelný pěti, doplní se zpráva opět nulovými bity tak jak tomu bylo zadávání znaků ASCII.

Po přípravě dat ke kódování nastává samotný proces kódování metodou popsanou v kapitole 2. Po úspěšném zakódování lze v okně "Umělé zavedení chyby:" přepsat jednotlivé bity zabezpečených bloků a tím zavést chyby do přenášené zprávy.

Při dekódování se používá maticová metoda popsaná v kapitole 3 V okně "{Místa chyb} / počet chyb:" se zobrazí pozice a počty chyb v jednotlivých blocích přenášené zprávy zadané před dekódováním. Dále se zobrazí syndromy pro jednotlivé bloky a pozice chyb nalezených při dekódování. Ty, jak je podle Obr.1 patrné, odpovídají chybám, které byla zadány před dekódováním. To znamená, že dekódováni proběhlo úspěšně.

Po dekódování se ze zprávy odstraní nadbytečné nulové bity. Pokud byla kódovaná zpráva zadána v ASCII kódu, rozdělí se tato zpráva zpět na osmice bitů, které se přeloží do znaků ASCII a zobrazí se na výstupu. Pokud byla zadávaná data v binární podobě, zobrazí se na výstupu posloupnost binárních dat.



Obr. 1: *Aplikace s jednotlivými fázemi kódování a dekódování BCH (15, 5) kódem*

5 ZÁVĚR

Na základě teoretického rozboru kodéru a dekodéru BCH kódu v kapitole 2 a 3 byla naprogramována aplikace v jazyku C++, která vyobrazuje jednotlivé fáze kódování a dekódování BCH (15, 5) kódem schopným opravit až 3 chyby v jednom bloku. Aplikace by měla sloužit jako učební pomůcka ke snazšímu pochopení problematiky týkající se těchto kódů.

LITERATURA

[1] Němec, K.: Datové komunikace, Brno, VUTIUM 2000, ISBN 80-214-1652-1

[2] Adámek, J.: Kódování a teorie informace, Praha, ČVUT 1991, ISBN 80-01-00661-1