BCH-KÓDY

Otázky

1. Ktoré polynómy stupňa 1,2,3,4,5 a 6 sú primitívne?
2. Aká je charakteristika polí $GF(32)$, $GF(49)$, $GF(1024)$?
3. Ako resp. koľkými spôsobmi možno zostrojiť $GF(2^5)$?
4. Koľko generátorov existuje v $GF^*(2^k)$ pre $k = 1, 2, 3, 4, 5$?
5. Je Hammingov kód dĺžky 15 cyklický? Ak áno, nájdite jeho generujúci polynóm, ak nie, zdôvodnite.
6. BCH kódy opravujúce 2 chyby sú definované pre $r \geq 4$. Aký kód generuje polynóm $g(x) = m_\beta(x) \cdot m_{\beta^3}(x)$, ak $r = 3$?

Úlohy

1. Určte rády všetkých prvkov v $GF^*(2^k)$ pre $k = 1, 2, 3, 4, 5$.
2. Zostrojte $GF(2^k)$ pre:
   a) $k = 2$,
   b) $k = 3$, použijúc polynóm $h(x) = 1 + x + x^3$,
   c) $k = 3$, použijúc polynóm $h(x) = 1 + x^2 + x^3$,
   d) $k = 4$, použijúc polynóm $h(x) = 1 + x + x^4$,
   e) $k = 4$, použijúc polynóm $h(x) = 1 + x^3 + x^4$,
   f) $k = 5$, použijúc polynóm $h(x) = 1 + x^2 + x^5$.
   Ak je to možné, za generátor zvoľte $\beta = x$
   Návod: Pole $GF(2^k)$ získate faktorizáciou $B[x]$ podľa $h(x)$ (v úlohe "a)" si polynóm $h(x)$ zvoľte sami). Potom vyjadrite každý prvok $GF^*(2^k)$ ako mocninu β. Nezabudnite, že v $GF(2^k)$ platí $h(x) = 0$.
3. Nájdite minimálny polynóm každého prvku v $GF(2^k)$ pre nasledujúce k, ak pole $GF(2^k)$ bolo skonštruované pomocou ireducibilného polynómu $h(x)$:
   a) $k = 3,\ h(x) = 1 + x + x^3$,
   b) $k = 3,\ h(x) = 1 + x^2 + x^3$,
   c) $k = 4,\ h(x) = 1 + x + x^4$,
   d) $k = 4,\ h(x) = 1 + x^3 + x^4$,
   e) $k = 5,\ h(x) = 1 + x^2 + x^5$.
4. Nech $GF(2^3)$ je pole zostrojené pomocou polynómu $1 + x + x^3$.
   a) Ukážte, že polynóm $m_\beta(x) = 1 + x + x^3$ je generujúci polynóm cyklického Hammingovho kódu dĺžky 7.
   b) V tomto kóde dekódujte prijaté slovo 1101001.
5. Nech $GF(2^3)$ je pole zostrojené pomocou polynómu $1 + x + x^3$.
   a) Ukážte, že polynóm $m_{\beta^3}(x) = 1 + x^2 + x^3$ je generujúci polynóm cyklického Hammingovho kódu dĺžky 7.
   b) Nájdite kontrolnú maticu tohto kódu.
   c) V tomto kóde dekódujte prijaté slovo $x + x^2 + x^4$.
   d) Konfrontujte svoje výsledky s výsledkami pre reprezentáciu pomocou slov z B^7.
6. Zostrojte kontrolnú maticu pre cyklický Hammingov kód dĺžky 15.
7. a) Nájdite generujúci polynóm cyklického kódu dĺžky 15 tak, aby $1, \beta^7, \beta^5 \in GF(2^4)$ (pole zostrojené pomocou $1 + x + x^4$) boli jeho korene.

b) Nájdite kontrolnú maticu tohto kódu.

8. Pomocou výsledkov z tretej úlohy nájdite generujúci polynóm BCH kódu dĺžky n, ktorý opravuje 2 chyby, ak:
   a) $n = 15$ a pole vzniklo faktorizáciou $B[x]$ podľa $1 + x + x^4$,
   b) $n = 15$ a pole vzniklo faktorizáciou $B[x]$ podľa $1 + x^3 + x^4$,
   c) $n = 31$ a pole vzniklo faktorizáciou $B[x]$ podľa $1 + x^2 + x^5$.
9. Ukážte, že stĺpce kontrolnej matice kódu C_{15} sú lineárne nezávislé, a teda $dim\ C_{15} = 8$.
10. Pomocou kontrolnej matice kódu C_{15} ukážte, že $d = 5$.
11. Ukážte, že ak β je generátor $GF(2^r),\ r > 2$, tak

$$|\{\beta^{2^i} \mid 0 \leq i \leq r-1\}| = |\{(\beta^3)^{2^i} \mid 0 \leq i \leq r-1\}| = r,$$

    a preto $deg(m_\beta(x)) = deg(m_{\beta^3}(x)) = r$.
12. Určte, ktoré z nasledujúcich slov sú kódové slová v C_{15}, ak $g(x) = 1 + x^4 + x^6 + x^7 + x^8$:
    a) 01100 10110 00010, b) 00011 10100 00110,
    c) 01110 00000 10001, d) 11111 11111 11111.
13. Nájdite korene kvadratických polynómov v $GF(2^4)$:
    a) $x^2 + \beta^4 \cdot x + \beta^{13}$, b) $x^2 + \beta^7 \cdot x + \beta^2$,
    c) $x^2 + \beta^2 \cdot x + \beta^5$, d) $x^2 + \beta^6$,
    e) $x^2 + \beta^2 \cdot x$, f) $x^2 + x + \beta^8$.
14. Správy sú kódované v C_{15}. Ak je to možné, nájdite chybové polynómy prijatých slov w, ktorých syndrómy s_w sú:
    a) [0100, 0101], b) [1110, 1000],
    c) [1100, 1101], d) [0100, 0000],
    e) [0000, 0100], f) [1010, 0100],
    g) [0011, 1101], h) [0000, 0000].
15. Ak je to možné, dekódujte v kóde C_{15} prijaté slová:
    a) 11000 00000 00000, b) 00001 00001 00001,
    c) 01000 10101 00000, d) 11001 11001 11000,
    e) 11001 11001 00000, f) 11100 00000 00001,
    g) 10111 00000 00000, h) 10101 00101 10001,
    i) 01000 01000 00000, j) 01010 10010 11000,
    k) 11011 10111 01100, l) 10111 00000 01000,
    m) 11100 10110 00000, n) 00011 10100 00110.
16. Ak je to možné, dekódujte v kóde C_{31} prijaté slová:
    a) 00100 10110 11101 00101 10111 00000 0,
    b) 00100 10110 10101 01101 11000 11110 1,
    c) 10110 00100 00001 11000 00100 00001 0,
    d) 11011 10110 01000 10101 00101 10111 0.