Diszkrét matematika III.

Véges testek kódoláselméleti alkalmazása

2009. május 15-16.

Véges testek.

Definíció: primitív polinom.

Legyen p prímszám, n természetes szám és $f \in \mathbb{Z}_p[x]$ n-edfokú irreducibilis polinom. Az f polinom **primitív**, ha az $\alpha = x + (f) \in \mathbb{Z}_p[x]/(f)$ elem hatványai a $\mathrm{GF}(p^n) = \mathbb{Z}_p[x]/(f)$ test valamennyi a zéruselemtől különböző elemét előállítják.

Véges testek.

Definíció: primitív polinom.

Legyen p prímszám, n természetes szám és $f \in \mathbb{Z}_p[x]$ n-edfokú irreducibilis polinom. Az f polinom **primitív**, ha az $\alpha = x + (f) \in \mathbb{Z}_p[x]/(f)$ elem hatványai a $\mathrm{GF}(p^n) = \mathbb{Z}_p[x]/(f)$ test valamennyi a zéruselemtől különböző elemét előállítják.

Tétel.

Tetszőleges véges test esetén van primitív polinom.

Véges testek.

Példa.

Legyen $p = 2$, $n = 3$ és $f = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Az f polinom irreducibilis, mivel nincs gyöke $\mathbb{Z}_2$-ben. Legyen $\alpha = x + (f) \in \mathbb{Z}_2[x]/(f) = \mathrm{GF}(2^3)$. Ekkor

$$\alpha^1 = x + (f), \qquad \alpha^2 = x^2 + (f),$$
$$\alpha^3 = x^3 + (f) = (x^2 + 1) + (f), \quad \alpha^4 = x^4 + (f) = (x^2 + x + 1) + (f),$$
$$\alpha^5 = x^5 + (f) = (x + 1) + (f), \quad \alpha^6 = x^6 + (f) = (x^2 + x) + (f),$$
$$\alpha^7 = x^7 + (f) = 1 + (f).$$

Azaz f primitív polinom.

Véges testek.

Definíció: primitív elem.

Legyen p prímszám, n természetes szám. A p^n-elemű $\mathrm{GF}(p^n)$ test β elemét **primitív**nek nevezzük, ha a β elem hatványai a $\mathrm{GF}(p^n) \setminus \{0\}$ halmaz valamennyi elemét előállítják.

Véges testek.

Definíció: primitív elem.

Legyen p prímszám, n természetes szám. A p^n-elemű $\mathrm{GF}(p^n)$ test β elemét **primitív**nek nevezzük, ha a β elem hatványai a $\mathrm{GF}(p^n) \setminus \{0\}$ halmaz valamennyi elemét előállítják.

Példa.

Legyen $p = 2$, $n = 4$ és $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$. Az f polinom irreducibilis $\mathbb{Z}_2[x]$-ben. Legyen $\beta = (x^2 + x + 1) + (f) \in \mathrm{GF}(2^4)$. Ekkor $\beta^3 = (x^6 + x^5 + x^3 + x + 1) + (f) = 1 + (f)$, azaz β nem primitív elem.

Véges testek.

Definíció: primitív elem.

Legyen p prímszám, n természetes szám. A p^n-elemű $\mathrm{GF}(p^n)$ test β elemét **primitív**nek nevezzük, ha a β elem hatványai a $\mathrm{GF}(p^n) \setminus \{0\}$ halmaz valamennyi elemét előállítják.

Példa.

Legyen $p = 2$, $n = 4$ és $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$. Az f polinom irreducibilis $\mathbb{Z}_2[x]$-ben. Legyen $\beta = (x^2 + x + 1) + (f) \in \mathrm{GF}(2^4)$. Ekkor $\beta^3 = (x^6 + x^5 + x^3 + x + 1) + (f) = 1 + (f)$, azaz β nem primitív elem.

Tétel.

Minen véges testben van primitív elem.

Véges testek.

Definíció: primitív polinom.

Legyen p prímszám, n természetes szám, $\beta \in \mathrm{GF}(p^n)$. Azt a legalacsonyabb fokú $\mathbb{Z}_p[x]$-beli főpolinomot, amelynek β gyöke, a β elem **minimálpolinomjának** nevezzük.

Véges testek.

Definíció: primitív polinom.

Legyen p prímszám, n természetes szám, $\beta \in \mathrm{GF}(p^n)$. Azt a legalacsonyabb fokú $\mathbb{Z}_p[x]$-beli főpolinomot, amelynek β gyöke, a β elem **minimálpolinomjának** nevezzük.

Tétel.

Legyen p prímszám, n természetes szám és $\beta \in \mathrm{GF}(p^n)$.

Véges testek.

Definíció: primitív polinom.

Legyen p prímszám, n természetes szám, $\beta \in \mathrm{GF}(p^n)$. Azt a legalacsonyabb fokú $\mathbb{Z}_p[x]$-beli főpolinomot, amelynek β gyöke, a β elem **minimálpolinomjának** nevezzük.

Tétel.

Legyen p prímszám, n természetes szám és $\beta \in \mathrm{GF}(p^n)$.

(a) A β elemnek van minimálpolinomja, amely legfeljebb n-edfokú és egyértelműen meghatározott.

Véges testek.

Definíció: primitív polinom.

Legyen p prímszám, n természetes szám, $\beta \in \mathrm{GF}(p^n)$. Azt a legalacsonyabb fokú $\mathbb{Z}_p[x]$-beli főpolinomot, amelynek β gyöke, a β elem **minimálpolinomjának** nevezzük.

Tétel.

Legyen p prímszám, n természetes szám és $\beta \in \mathrm{GF}(p^n)$.

(a) A β elemnek van minimálpolinomja, amely legfeljebb n-edfokú és egyértelműen meghatározott.

(b) Ha $m \in \mathbb{Z}_p[x]$ a β elem minimálpolinomja és a $g \in \mathbb{Z}_p[x]$ polinomnak β gyöke, akkor $m \mid g$.

Véges testek.

Példa.

Legyen $p = 3$, $n = 4$ és $f = x^4 + x^2 + x + 1$. Ekkor f irreducibilis $\mathbb{Z}_3$ felett, így $K = \mathbb{Z}_3[x]/(f)$ test. Legyen $\beta = (x^2 + x + 1) + (f)$, és jelölje m a β elem minmálpolinomját. Ekkor $m^* < 4$. Legyen $a_0, \ldots, a_3 \in \mathbb{Z}_3$ és $\gamma = a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 + \beta^4$. Ekkor

$$\gamma = (2a_2 + 1)x^3 + (a_1 + 2a_2)x^2 + (a_2 + a_1 + a_3)x + a_0 + 2 + a_1 + 2a_3.$$

Így $\gamma = 0 + (f)$ pontosan akkor teljesül, ha $2a_2 + 1 = a_1 + 2a_2 = a_2 + a_1 + a_3 = a_0 + 2 + a_1 + 2a_3 = 0$. Azaz $a_0 = a_1 = a_2 = a_3 = 1$, és így $m(\beta) = 0$, ahol $m = x^4 + x^3 + x^2 + x + 1$. Mivel m irreducibilis, ezért m a β elem minimálpolinomja.

Véges testek.

Tétel (A BCH kódok alaptétele).

Legyen p prímszám, d és n pedig olyan természetes számok, amelyekre $1 < d < p^n$ teljesül. Legyen α primitív elem a $\mathrm{GF}(p^n)$ testben, és legyen $g_i \in \mathbb{Z}_p[x]$ az α^i elem minimálpolinomja ($i = 1, 2, \ldots, d-1$). Jelölje g a $g_1, \ldots, g_{d-1}$ polinomok legkisebb közös többszörösét. Ekkor g bármely 0-tól különböző $(p^n - 1)$-nél kisebb fokú $\mathbb{Z}_p[x]$-beli többszörösében legalább d darab együttható különbözik 0-tól.

BCH kódok.

Definíció: BCH kódolás.

Legyenek d és n olyan természetes számok, amelyekre $1 < d < 2^n$ teljesül. Legyen f egy n-edfokú primitív polinom $\mathbb{Z}_2$ felett, $\alpha = x + (f)$. Legyen $g_i \in \mathbb{Z}_p[x]$ az α^i elem minimálpolinomja $(i = 1, 2, \ldots, d-1)$. Jelölje g a $g_1, \ldots, g_{d-1}$ polinomok legkisebb közös többszörösét. Legyenek M és N olyan természetes számok, hogy $g^* < M < 2^{n-1}$ és $N = M - g^*$. Ekkor az $E\colon \{0,1\}^N \to \{0,1\}^M,\ u \mapsto ug$ kódolást a d **minimális távolsághoz tervezett BCH kódolásnak nevezzük**.

A BCH kódolást Bose és Chaudhury, illetve Hocquenghem fedezte fel 1960-ban.

BCH kódok.

Definíció: BCH kódolás.

Legyenek d és n olyan természetes számok, amelyekre $1 < d < 2^n$ teljesül. Legyen f egy n-edfokú primitív polinom $\mathbb{Z}_2$ felett, $\alpha = x + (f)$. Legyen $g_i \in \mathbb{Z}_p[x]$ az α^i elem minimálpolinomja $(i = 1, 2, \ldots, d-1)$. Jelölje g a $g_1, \ldots, g_{d-1}$ polinomok legkisebb közös többszörösét. Legyenek M és N olyan természetes számok, hogy $g^* < M < 2^{n-1}$ és $N = M - g^*$. Ekkor az $E\colon \{0,1\}^N \to \{0,1\}^M,\ u \mapsto ug$ kódolást a d **minimális távolsághoz tervezett BCH kódolásnak nevezzük**.

A BCH kódolást Bose és Chaudhury, illetve Hocquenghem fedezte fel 1960-ban.

Tétel.

A d minimális távolsághoz tervezett BCH kódolás lineáris, és a kódszavak közötti minimális távolság d.

BCH kódok.

Tétel.

Ha d páratlan, akkor a BCH kódolás definíciójában szereplő g polinom foka legfeljebb $n(d-1)/2$.