Diszkrét matematika 2.C szakirány

8. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2017. tavasz

Véges testek

Tekintsük valamely p prímre a $\mathbb{Z}_p$ testet, továbbá egy $f(x) \in \mathbb{Z}_p[x]$ felbonthatatlan főpolinomot. Vezessük be a $g(x) \equiv h(x) \pmod{f(x)}$, ha $f(x)|g(x) - h(x)$ relációt.
Ez ekvivalenciareláció, ezért meghatároz egy osztályozást $\mathbb{Z}_p[x]$-en.

Minden osztálynak van $deg(f)$-nél alacsonyabb fokú reprezentánsa (Miért?), és ha $deg(g), deg(h) < deg(f)$, továbbá g és h ugyanabban az osztályban van, akkor egyenlőek (Miért?). Tehát $deg(f) = n$ esetén bijekciót létesíthetünk az n-nél kisebb fokú polinomok és az osztályok között, így p^n darab osztály van.

Az osztályok között értelmezhetjük a természetes módon a műveleteket. Ezeket végezhetjük az n-nél alacsonyabb fokú reprezentánsokkal: ha a szorzat foka nem kisebb, mint n, akkor az $f(x)$-szel vett osztási maradékot vesszük.

Véges testek

$f \not| g$ esetén a bővített euklideszi algoritmus alapján
$d(x) = u(x)f(x) + v(x)g(x)$.
Mivel $f(x)$ felbonthatatlan, ezért $d(x) = d$ konstans polinom, így $\frac{v(x)}{d}$ multiplikatív inverze lesz $g(x)$-nek.

Tétel (NB)

Az ekvivalenciaosztályok halmaza a rajta értelmezett összeadással és szorzással testet alkot.

Megjegyzés

Tetszőleges p prím és n pozitív egész esetén létezik p^n elemű test, mert létezik n-ed fokú felbonthatatlan polinom $\mathbb{Z}_p$-ben.

Megjegyzés

Véges test elemszáma prímhatvány, továbbá az azonos elemszámú testek izomorfak.

Véges testek

Példa

Tekintsük az $x^2 + 1 \in \mathbb{Z}_3[x]$ felbonthatatlan polinomot (Miért az?). A legfeljebb elsőfokú polinomok: $0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$.
Az összeadás műveleti táblája:

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

Például:

$$2x + 2 + 2x + 1 = 4x + 3 \overset{\mathbb{Z}_3}{=} x$$

Véges testek

Példa folyt.

·	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Például:

$$(2x+2)(2x+1) = 4x^2 + 6x + 2 \overset{\mathbb{Z}_3}{=} x^2 + 2 = (x^2+1) + 1$$

Feladat: Legyen $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$. Mik lesznek a $z^2 + 1 \in \mathbb{F}_9[z]$ polinom gyökei?

A kommunikáció során információt hordozó adatokat viszünk át egy csatornán keresztül az információforrástól, az adótól az információ címzettjéhez, a vevőhöz.

A kommunikáció vázlatos ábrája

Megjegyzés

Az információ átvitele térben és időben történik. Egyes esetekben az egyik, más esetekben a másik dimenzió a domináns (pl. telefonálás; információ rögzítése adathordozóra, majd későbbi visszaolvasása).

Definíció

Az információ új ismeret. Shannon nyomán az általa megszüntetett bizonytalansággal mérjük.

Definíció

Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki. Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \ldots, a_k$.
Ha az a_j üzenet m_j-szer fordul elő, akkor azt mondjuk, hogy a gyakorisága m_j, relatív gyakorisága pedig $p_j = \frac{m_j}{n} > 0$.
A $p_1, p_2, \ldots, p_k$ szám k-ast az üzenetek eloszlásának nevezzük ($\sum_{j=1}^{k} p_j = 1$).
Az a_j üzenet egyedi információtartalma $I_j = -\log_r p_j$, ahol r egy 1-nél nagyobb valós szám, ami az információ egységét határozza meg. Ha $r = 2$, akkor az információ egysége a bit.
Az üzenetforrás által kibocsátott üzenetek átlagos információtartalma, vagyis $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$ a forrás entrópiája. Ez csak az üzenetek eloszlásától függ, a tartalmuktól nem.
Egy k tagú eloszlásnak olyan pozitív valós számokból álló $p_1, p_2, \ldots, p_k$ sorozatot nevezünk, amelyre $\sum_{j=1}^{k} p_j = 1$. Ennek az eloszlásnak az entrópiája $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$.

Definíció

Legyen $I \subset \mathbb{R}$ egy intervallum. Az $f : I \to \mathbb{R}$ függvényt konvexnek nevezzük, ha bármely $x_1, x_2 \in I$ és $0 \leq t \leq 1$ esetén

$$f\left(tx_1 + (1-t)x_2\right) \leq tf(x_1) + (1-t)f(x_2).$$

f szigorúan konvex, ha egyenlőség csak $t = 0$ vagy $t = 1$ esetén lehetséges.

Lemma (Jensen-egyenlőtlenség, NB)

Legyen $p_1, p_2, \ldots, p_k$ egy eloszlás, $f : I \to \mathbb{R}$ pedig egy szigorúan konvex függvény az $I \subset \mathbb{R}$ intervallumon. Ekkor $q_1, q_2, \ldots, q_k \in I$ esetén

$$f\left(\sum_{j=1}^{k} p_j q_j\right) \leq \sum_{j=1}^{k} p_j f(q_j),$$

és egyenlőség pontosan akkor áll fenn, ha $q_1 = q_2 = \ldots = q_k$.

Tétel

Bármilyen eloszláshoz tartozó entrópiára

$$H_r(p_1, p_2, \ldots, p_k) \leq \log_r k,$$

és egyenlőség pontosan akkor teljesül, ha $p_1 = p_2 = \ldots = p_k = \frac{1}{k}$.

Bizonyítás

$r > 1$ esetén a $-\log_r(x)$ függvény szigorúan konvex, ezért használhatjuk a lemmát $q_j = \frac{1}{p_j}$ választással:

$$-H_r(p_1, p_2, \ldots, p_k) = \sum_{j=1}^{k} p_j \log_r p_j =$$

$$= \sum_{j=1}^{k} p_j \left(-\log_r \frac{1}{p_j}\right) \geq -\log_r \left(\sum_{j=1}^{k} p_j \frac{1}{p_j}\right) = -\log_r k.$$

Definíció

A kódolás alatt a legáltalánosabb értelemben az üzenetek halmazának egy másik halmazba való leképezését értjük.
Ha a leképezés injektív, akkor azt mondjuk, hogy a kódolás felbontható, egyértelműen dekódolható, vagy veszteségmentes, egyébként veszteségesnek nevezzük, mert információvesztéssel jár.

Betűnkénti kódolás

A betűnkénti kódolás során az üzenetet meghatározott módon egymáshoz átfedés nélkül csatlakozó részekre bontjuk, egy-egy ilyen részt egy szótár alapján kódolunk, és az így kapott kódokat az eredeti sorrendnek megfelelően egymáshoz láncoljuk.
Az általánosság csorbítása nélkül feltehetjük, hogy a szótár alapján kódolandó elemi üzenetek egy A ábécé (a kódolandó ábécé) betűi, és egy-egy ilyen betű kódja egy másik (az előbbitől nem feltétlenül különböző) B ábécé (kódoló ábécé vagy kódábécé) betűivel felírt szó, vagyis ezen ábécéből vett betűk véges sorozata, a sorozat elemeit egyszerűen egymás mellé írva. Az ábécékről feltesszük, hogy nem-üresek és végesek.

Definíció

Az A ábécé betűivel felírható összes (legalább egy betűt tartalmazó) szó halmazát A^+ jelöli, míg az egyetlen betűt sem tartalmazó üres szóval (jele: $\emptyset$ vagy λ) kibővített halmazt A^*.

Betűnkénti kódolás

Definíció

A betűnkénti kódolást egy $\varphi : A \to B^*$ leképezés határozza meg, amelyet természetes módon terjesztünk ki egy $\psi : A^* \to B^*$ leképezéssé: $a_1 a_2 \dots a_n = \alpha \in A^*$ esetén $\psi(\alpha) = \varphi(a_1)\varphi(a_2)\dots\varphi(a_n)$.
$\mathrm{rng}(\psi)$-t kódnak nevezzük, elemei a kódszavak.

Megjegyzés

Ha φ nem injektív, vagy az üres szó benne van az értékkészletében, akkor a kapott ψ kódolás nem injektív (Miért?), tehát nem felbontható, ezért betűnkénti kódolásnál feltesszük, hogy φ injektív, és B^+-ba képez.

Betűnkénti kódolás

Definíció

Tekintsünk egy A ábécét, és legyen $\alpha, \beta, \gamma \in A^*$. Ekkor α prefixe (előtagja), míg γ szuffixe (utótagja) $\alpha\gamma$-nak, β pedig infixe (belső tagja) $\alpha\beta\gamma$-nak.

Definíció

Prefixmentes halmaznak nevezzük szavak egy halmazát, ha nincs benne két különböző szó, hogy egyik a másik prefixe.

Definíció

Az üres szó és α prefixe, szuffixe és infixe is α-nak, ezeket α triviális prefixeinek, triviális szuffixeinek és triviális infixeinek nevezzük.

Definíció

α egy prefixét, szuffixét, illetve infixét valódi prefixnek, valódi szuffixnek, illetve valódi infixnek nevezzük, ha nem egyezik meg α-val.

Betűnkénti kódolás

Definíció

Tekintsük az injektív $\varphi : A \to B^+$ leképezést, illetve az általa meghatározott ψ betűnkénti kódolást.
Ha $\mathrm{rng}(\varphi)$ prefixmentes halmaz, akkor prefix kódról beszélünk.
Ha $\mathrm{rng}(\varphi)$ elemei azonos hosszúságúak, akkor egyenletes kódról, fix hosszúságú kódról, esetleg blokk-kódról beszélünk.
Vesszős kódról beszélünk, ha van egy olyan $\vartheta \in B^+$ szó (a vessző), amely minden kódszónak szuffixe, de egyetlen kódszó sem áll elő $\alpha\vartheta\beta$ alakban nem üres β szóval.

Állítás

Prefix kód felbontható.

Bizonyítás

Konstruktív: nézzük az eddig beérkezett szimbólumokból összeálló szót. Amint ez kiadja a kódolandó ábécé valamely betűjének a kódját, azonnal dekódolhatunk a megfelelő betűre, mert a folytatásával kapott jelsorozat egyetlen betűnek sem lehet a kódja.

Betűnkénti kódolás

Állítás

Egyenletes kód prefix (így nyilván felbontható is).

Bizonyítás

Mivel a kódszavak hossza azonos, ezért csak úgy lehet egy kódszó prefixe egy másiknak, ha megegyeznek.

Állítás

Vesszős kód prefix (így nyilván felbontható is).

Bizonyítás

A vessző egyértelműen jelzi egy kódszó végét, hiszen ha folytatva kódszót kapnánk, abban a vessző tiltott módon szerepelne.

Betűnkénti kódolás

Példák

Legyen $A = \{a,b,c\}$, $B = \{0,1\}$, $\varphi : A \to B^+$ pedig az alábbi módon definiált.

	1.	2.	3.	4.	5.	6.
$\varphi(a)$	01	1	01	0	00	01
$\varphi(b)$	1101	01	011	10	10	001
$\varphi(c)$	01	10	11	11	11	0001

1. $\varphi(a) = \varphi(c) \Longrightarrow \varphi$ nem injektív
2. $\psi(ab) = 101 = \psi(ca) \Longrightarrow$ nem felbontható
3. nem prefix, de felbontható
4. prefix
5. egyenletes
6. vesszős

Betűnkénti kódolás

Tétel (McMillan-egyenlőtlenség, NB)

Legyen $A = \{a_1, a_2, \ldots, a_n\}$ és B két ábécé, B elemeinek száma $r \geq 2$, és $\varphi : A \to B^+$ injektív leképezés.
Ha a φ által meghatározott betűnkénti kódolás felbontható, akkor $l_j = |\varphi(a_j)|$ jelöléssel

$$\sum_{j=1}^{n} r^{-l_j} \leq 1.$$

Tétel (McMillan-egyenlőtlenség ,,megfordítása", NB)

Az előző tétel jelöléseit használva, ha $l_1, l_2, \ldots, l_n$ olyan pozitív egész számok, hogy $\sum_{j=1}^{n} r^{-l_j} \leq 1$, akkor van az A-nak a B elemeivel való olyan felbontható (sőt prefix) kódolása, hogy az a_j betű kódjának hossza l_j.