Diszkrét matematika 2.C szakirány

10. előadás

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

Komputeralgebra Tanszék

2016. ősz

Betűnkénti kódolás

Kódfa

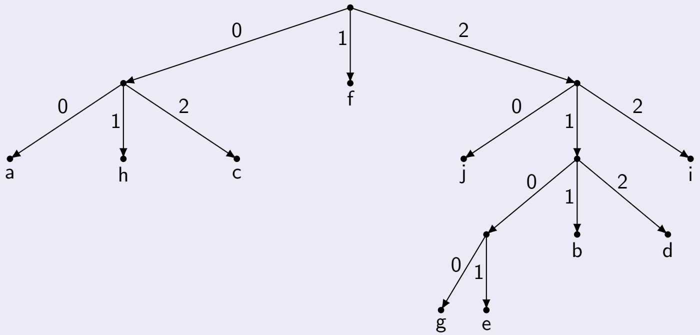
A betűnkénti kódolás szemléltethető egy címkézett irányított fával.
Legyen $\varphi : A \to B^*$ egy betűnkénti kódolás, és tekintsük $\mathrm{rng}(\varphi)$ prefixeinek halmazát. Ez a halmaz részbenrendezett a ,,prefixe'' relációra. Vegyük ennek a Hasse-diagramját. Így egy irányított fát kapunk, aminek a gyökere az üres szó, és minden szó a hosszának megfelelő szinten van.
A fa éleit címkézzük úgy B elemeivel, hogy ha $\beta = \alpha b$ valamely $b \in B$-re, akkor az α-ból β-ba vezető él címkéje legyen b.
A kódfa csúcsait is megcímkézhetjük: az $a \in A$ kódjának megfelelő csúcs címkéje legyen $a \in A$; azon csúcs címkéje, amely nincsen $\mathrm{rng}(\varphi)$-ben, legyen ,,üres''.

Megjegyzés

Az előbbi konstrukció meg is fordítható. Tekintsünk egy véges, élcímkézett irányított fát, ahol az élcímkék halmaza B, az egy csúcsból kiinduló élek mind különböző címkéjűek, továbbá az A véges ábécének a csúcsokra való leképezését, amelynél minden levél előáll képként.
Az $a \in A$ betű kódja legyen az a szó, amelyet úgy kapunk, hogy a gyökértől az a-nak megfelelő csúcsig haladó irányított út mentén összeolvassuk az élek címkéit.

Kódfa

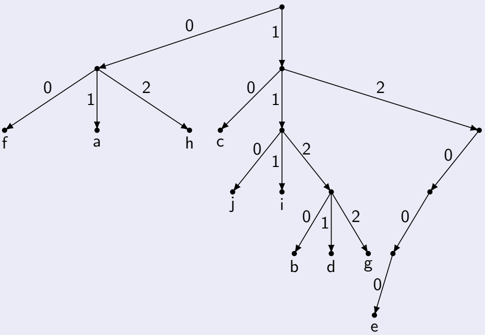
Példa



A Huffman-kódos példában szereplő kódhoz tartozó kódfa.
$\varphi(a)=$00, $\varphi(b)=$211, $\varphi(c)=$02, $\varphi(d)=$212, $\varphi(e)=$2101, $\varphi(f)=$1, $\varphi(g)=$2100, $\varphi(h)=$01, $\varphi(i)=$22, $\varphi(j)=$20.
A kódszavak prefixeinek halmaza:
$\{\lambda, 1, 00, 0, 01, 02, 20, 2, 22, 211, 21, 212, 2100, 210, 2101\}$

Kódfa

Példa



A Shannon-kódos példában szereplő kódhoz tartozó kódfa.
$\varphi(a)=$01, $\varphi(b)=$1120, $\varphi(c)=$10, $\varphi(d)=$1121, $\varphi(e)=$12000, $\varphi(f)=$00, $\varphi(g)=$1122, $\varphi(h)=$02, $\varphi(i)=$111, $\varphi(j)=$110.
A kódszavak prefixeinek halmaza:
$\{\lambda, 01, 0, 1120, 112, 11, 1, 10, 1121, 12000, 1200, 120, 12, 00, 1122, 02, 111, 110\}$

Hibakorlátozó kódolás

Példa (ISBN (International Standard Book Number) kódolása)

Legyen $d_1, d_2, \ldots, d_n$ decimális számjegyek egy sorozata ($n \leq 10$). Egészítsük ki a sorozatot egy $n+1$-edik számjeggyel, amelynek értéke

$$d_{n+1} = \sum_{j=1}^{n} j \cdot d_j \mod 11,$$

ha az nem 10, különben d_{n+1} legyen X.
Ha valamelyik számjegyet elírjuk, akkor az összefüggés nem teljesülhet: d_{n+1} elírása esetén ez nyilvánvaló, $j \leq n$-re d_j helyett d_j'-t írva pedig az összeg $j(d_j' - d_j)$-vel nőtt, ami nem lehet 11-gyel osztható (Miért?).
Azt is észrevesszük, ha $j < n$ esetén d_j-t és d_{j+1}-et felcseréljük:
az összeg $jd_{j+1} + (j+1)d_j - jd_j - (j+1)d_{j+1} = d_j - d_{j+1}$-gyel nő, ami csak akkor lehet 11-gyel osztható, ha $d_j = d_{j+1}$.

Megjegyzés

2007 óta 13 jegyű.
A személyi számnál is használják.

Hibakorlátozó kódolás

Példa (Paritásbites kód)

Egy n hosszú 0-1 sorozatot egészítsünk ki egy $n+1$-edik bittel, ami legyen 1, ha a sorozatban páratlan sok 1-es van, különben pedig legyen 0. Ha egy bit megváltozik, akkor észleljük a hibát.

Példa (Kétdimenziós paritásellenőrzés)

$$\begin{array}{ccccc|c}
b_{0,0} & \cdots & b_{0,j} & \cdots & b_{0,n-1} & b_{0,n} \\
\vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\
b_{i,0} & \cdots & b_{i,j} & \cdots & b_{i,n-1} & b_{i,n} \\
\vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\
b_{m-1,0} & \cdots & b_{m-1,j} & \cdots & b_{m-1,n-1} & b_{m-1,n} \\
\hline
b_{m,0} & \cdots & b_{m,j} & \cdots & b_{m,n-1} & b_{m,n}
\end{array}$$

Oszlopok és sorok végén paritásbit. Ha megváltozik egy bit, akkor a sor és az oszlop végén jelez az ellenőrző bit, ez alapján tudjuk javítani a hibát. Ha két bit változik meg, akkor észleljük a hibát, de nem tudjuk javítani.

Hibakorlátozó kódolás

Definíció

Egy kód t-hibajelző, ha minden olyan esetben jelez, ha az elküldött és megkapott szó legfeljebb t helyen tér el.
Egy kód pontosan t-hibajelző, ha t-hibajelző, de van olyan $t+1$-hiba, amit nem jelez.

Példa

- ISBN - 1-hibajelző
- paritásbites kód - 1-hibajelző
- kétdimenziós paritásellenőrzés - 2-hibajelző

Hiba javításának módjai

ARQ (Automatic Retransmission Request) - újraküldés,
FEC (Forward Error Correction) - javítható, pl.: kétdimenziós paritásell.

Hibakorlátozó kódolás

Definíció

Legyen A véges ábécé, továbbá $u, v \in A^n$. Ekkor u és v Hamming-távolsága alatt az azonos pozícióban lévő különböző betűk számát értjük:

$$d(u, v) = |\{i : 1 \leq i \leq n \wedge u_i \neq v_i\}|.$$

Példa

$$\begin{array}{ccccc} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ \hline \neq & \neq & = & \neq & \neq \end{array} \qquad \begin{array}{cccc} A & L & M & A \\ A & N & N & A \\ \hline = & \neq & \neq & = \end{array}$$

$d(01110,10101)=4$ $\qquad$ $d(ALMA,ANNA)=2$

Hibakorlátozó kódolás

Állítás

A Hamming-távolság rendelkezik a távolság szokásos tulajdonságaival, vagyis tetszőleges u, v, w-re

1) $d(u, v) \geq 0$;
2) $d(u, v) = 0 \iff u = v$;
3) $d(u, v) = d(v, u)$ (szimmetria);
4) $d(u, v) \leq d(u, w) + d(w, v)$ (háromszög-egyenlőtlenség).

Bizonyítás

1), 2) és 3) nyilvánvaló.
4) Ha u és v eltér valamelyik pozicióban, akkor ott u és w, illetve w és v közül legalább az egyik pár különbözik.

Hibakorlátozó kódolás

Definíció

A K **kód távolsága** ($d(K)$) a különböző kódszópárok távolságainak a minimuma.

Példa (*)

$$\begin{array}{lllll}
(0,0)\mapsto (0,0,0,0,0) & & & & \\
 & 3 & & & \\
(0,1)\mapsto (0,1,1,1,0) & & 3 & & \\
 & 4 & & & 4 \\
(1,0)\mapsto (1,0,1,0,1) & & & 3 & \\
 & 3 & & & \\
(1,1)\mapsto (1,1,0,1,1) & & & &
\end{array}$$

A kód távolsága 3.

Felmerül a kérdés, hogy vajon mi lehetett a kódszó, ha a (0,1,0,0,0) szót kapjuk.

Hibakorlátozó kódolás

Definíció

Minimális távolságú dekódolás esetén egy adott szóhoz azt a kódszót rendeljük, amelyik hozzá a legközelebb van. Több ilyen szó esetén kiválasztunk ezek közül egyet, és az adott szóhoz mindig azt rendeljük.

Megjegyzés

A dekódolás két részre bontható: a hibajavításnál megpróbáljuk meghatározni, hogy mi volt az elküldött kódszó, majd visszaállítjuk az üzenetet. Mivel az utóbbi egyértelmű, ezért hibajavító kódok dekódolásán legtöbbször csak a hibajavítást értjük.

Definíció

Egy kód t-hibajavító, ha minden olyan esetben helyesen javít, amikor egy elküldött szó legfeljebb t helyen változik meg.
Egy kód pontosan t-hibajavító, ha t-hibajavító, de van olyan $t+1$ hibával érkező szó, amit helytelenül javít, vagy nem javít.

Hibakorlátozó kódolás

Megjegyzés

Ha a kód távolsága d, akkor minimális távolságú dekódolással $t < \frac{d}{2}$ esetén t-hibajavító.

Példa

Az előző példában szereplő kód pontosan 1-hibajavító.
$(0,0,0,0,0) \rightsquigarrow (1,0,0,0,1) \longrightarrow (1,0,1,0,1)$

Példa (ismétléses kód)

a$\longmapsto$(a,a,a) $d = 3$ 1-hibajavító,
a$\longmapsto$(a,a,a,a,a) $d = 5$ 2-hibajavító.

Hibakorlátozó kódolás

Tétel (Singleton-korlát)

Ha $K \subset A^n$, $|A| = q$ és $d(K) = d$, akkor $|K| \leq q^{n-d+1}$.

Bizonyítás

Ha minden kódszóból elhagyunk $d-1$ betűt (ugyanazokból a pozíciókból), akkor az így kapott szavak még mindig különbözőek, és $n-d+1$ hosszúak. Az ilyen hosszú szavak száma szerepel az egyenlőtlenség jobb oldalán.

Definíció

Ha egy kódra a Singleton-korlát egyenlőséggel teljesül, akkor azt maximális távolságú szeparábilis kódnak (MDS-kód) nevezzük.

Példa

Az n-szeri ismétlés kódja. Ekkor $d = n$, és $|K| = q$.

Hibakorlátozó kódolás

Tétel (Hamming-korlát)

Ha $K \subset A^n$, $|A| = q$ és K t-hibajavító, akkor

$$|K| \sum_{j=0}^{t} \binom{n}{j} (q-1)^j \leq q^n.$$

Bizonyítás

Mivel a kód t-hibajavító, ezért bármely két kódszóra a tőlük legfeljebb t távolságra lévő szavak halmazai diszjunktak (Miért?). Egy kódszótól pontosan j távolságra lévő szavak száma $\binom{n}{j}(q-1)^j$ (Miért?), így egy kódszótól legfeljebb t távolságra lévő szavak száma $\sum_{j=0}^{t} \binom{n}{j}(q-1)^j$. A jobb oldalon az n hosszú szavak száma szerepel (Miért?).

Hibakorlátozó kódolás

Definíció

Ha egy kódra a Hamming-korlát egyenlőséggel teljesül, akkor azt perfekt kódnak nevezzük.

Példa

A (*) kód esetén $|K| = 4$, $n = 5$, $q = 2$ és $t = 1$.
B.O.$= 4\left(\binom{5}{0}(2-1)^0 + \binom{5}{1}(2-1)^1\right) = 4(1+5) = 24$,
J.O.$= 2^5 = 32$.
Nem perfekt kód.

A kód távolságának és hibajelző képességének kapcsolata

Tekintsünk egy kódot, aminek a távolsága d.

Ha egy elküldött kódszó legalább 1, de d-nél kevesebb helyen sérül, akkor az így kapott szó biztosan nem kódszó, mivel két kódszó legalább d helyen különbözik. Tehát legfeljebb $d-1$ hiba esetén a kód jelez.

A kódban van két olyan kódszó, amelyek távolsága d, és ha az egyiket küldik, és ez úgy változik meg, hogy éppen a másik érkezik meg, akkor d hiba történt, de nem vesszük észre. Tehát van olyan d hiba, amit a kód nem tud jelezni.
Ezáltal a kód pontosan $d-1$-hibajelző.

A kód távolságának és hibajavító képességének kapcsolata

Legyen a kód távolsága továbbra is d, és tegyük fel, hogy minimális távolságú dekódolást használunk.

$t < \frac{d}{2}$ hiba esetén biztosan jól javítunk, hiszen a háromszög-egyenlőtlenség miatt az eredetileg elküldött kódszótól különböző bármely kódszó biztosan $\frac{d}{2}$-nél több helyen tér el a vett szótól (Miért?).

Másrészt legyenek u és w olyan kódszavak, amelyek távolsága d, és legyen v az a szó, amit úgy kapunk u-ból, hogy a d pozícióból $t \geq \frac{d}{2}$ helyre a w megfelelő pozíciójában lévő betűt írjuk.
Ekkor v az u-tól t helyen, míg w-től $d - t \leq \frac{d}{2} \leq t$ helyen különbözik.
Ha a kód t-hibajavító lenne, akkor v-t egyrészt u-ra, másrészt w-re kellene javítania.
Ezáltal a kód pontosan $\left\lfloor \frac{d-1}{2} \right\rfloor$-hibajavító.