Jelzéskódolás többszörös hozzáférésű VAGY csatornán

GYŐRI SÁNDOR

BME, Számítástudományi és Információelméleti Tanszék
gyori@szit.bme.hu

Reviewed

Kulcsszavak: többszörös hozzáférés, kombinatorika, kódkonstrukciók, becslési módszerek

A jelzéskódolást többszörös hozzáférésű VAGY csatornán vizsgáljuk, amikor az összes T közül legfeljebb M felhasználó aktív. Bemutatunk gyakorlati alkalmazási példákat. A matematikai probléma megegyezik az extremális kombinatorika M-fedésmentes halmazrendszerek témakörével. Alsó és felső korlátokat adunk az n(T,M) minimális kódszóhosszra, és néhány kódkonstrukciót is ismertetünk. A jelenleg ismert legjobb korlátok $1 \ll M \ll T$ esetén:

$$\frac{1}{2}\frac{M^2}{\log M}\log T \le n(T,M) \le \frac{1}{\ln 2} M^2 \log T,$$

tehát meglehetősen távol van egymástól az alsó és felső korlát. Ismertetünk néhány hatékony kódkonstrukciót.

1. Csatornamodell

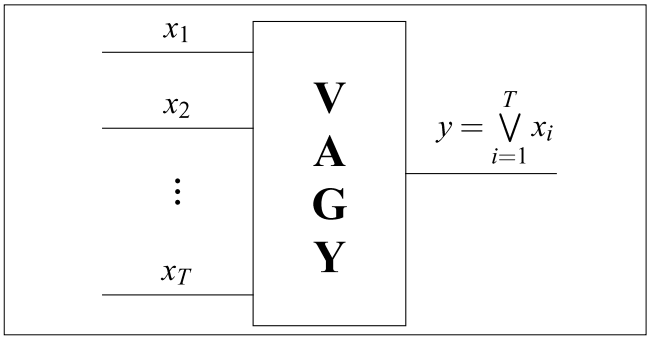
A *T*-felhasználós többszörös hozzáférésű VAGY csatorna – melyet először Cohen, Heller és Viterbi [6] vezetett be – bináris bemenetekkel (x_i, $1 \le i \le T$) és bináris kimenettel rendelkező determinisztikus csatorna, melynek kimenetén pontosan akkor jelenik meg 0, ha az összes bemenete 0. A csatorna kimenete tehát a bemenetek Boole-algebra szerinti összegeként adódik *(1. ábra)*:

$$y = \bigvee_{i=1}^{T} x_i = x_1 \vee x_2 \vee \cdots \vee x_T.$$

VAGY csatornaként modellezhető például egy olyan kommunikációs csatorna, amelyen a ki/bekapcsolás (OOK, On/Off Keying) modulációs eljárást alkalmazzuk, vagyis az 1-es bitnek megfeleltetünk egy jelalakot, míg a 0-s bitet a konstans 0 jelszint jelenti. Ekkor a demoduláció az a döntés, hogy az összes aktív felhasználó a 0 jelszintet adta-e a csatornába.

Egy többszörös hozzáférést lehetővé tevő kódnak általában három feladatot kell megoldania [16]:
- az aktív felhasználók azonosítása (detection, identification),
- kódszavaik szinkronizálása (synchronization),
- az üzenetek hibavédelme (decoding).

1. ábra Többszörös hozzáférésű VAGY csatorna



Folyamatosan aktív felhasználók esetén a maximális, egységnyi kihasználtság a legegyszerűbb módon, az időosztás segítségével is elérhető. Részleges felhasználói aktivitás esetén a hatékony kommunikáció megvalósítása nehéz és még korántsem megoldott probléma.

A továbbiakban a jelzéskódolás (signature coding) esetét fogjuk vizsgálni. Minden felhasználónak van egy saját *n*-bites kódszava, amelyet jelzésre használhat, viszont a csupa 0 kódszót (a konstans 0 jelszintet) használja, ha éppen nem aktív.

A kódolási probléma a következő: keressünk olyan kódot, amely garantálja, hogy ha a *T* felhasználó közül egyidejűleg legfeljebb *M* felhasználó akar jelezni (aktív), akkor a VAGY csatorna kimeneti vektorából egyértelműen meghatározható az aktív felhasználók halmaza. Az erőforrás hatékony kihasználása érdekében határozzuk meg azt a minimális kódszóhosszat, amely mellett a probléma még megoldható.

A kódosztásos többszörös hozzáférésű (CDMA) rendszerekben a felhasználók általában csak egy-egy kommunikációs ciklus idejére kapnak kódot (session code), tehát itt nincs azonosítási feladat. Esetünkben viszont minden felhasználó előre megkapja az alkalmazandó kódot, amely a rendszer teljes élettartama alatt állandó.

1.1. UD és ZFD kódok

Az UD és ZFD kódokat a VAGY csatornán való kommunikációhoz Kautz és Singleton [14] vezették be.

1. definíció (UD kód)

T darab n hosszú kódszóból álló kód M-edrendben egyértelműen dekódolható (Uniquely Decipherable, UD(T,M,n)), ha a legfeljebb M kódszóból álló összegek mind különbözőek.

Formálisan ez azt jelenti, hogy egy $C = \{\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_T\}$ kód UD(T,M,n) tulajdonságú, ha bármely $A,B \subset \{1,2,...,T\}$ halmazra, melyekre igaz, hogy $|A| \le M, |B| \le M, A \ne B$, teljesül az alábbi

$$\bigvee_{i\in A} \mathbf{x}_i \neq \bigvee_{j\in B} \mathbf{x}_j.$$

(Bináris vektorok összegén a koordinátánkénti Boole-összegek vektorát értjük.)

Példa: dokumentumkereső rendszer. Egy könyvtári nyilvántartásban a dokumentumokról (könyvek, folyóiratok stb.) különböző tulajdonságokat tárolnak. A keresés ezek alapján történik, vagyis el kell döntenünk, hogy egy adott dokumentum rendelkezik-e egy tulajdonsággal.

A vizsgálat megkönnyítésére a dokumentumok fejrészében hatékonyan szeretnénk tárolni jellemző tulajdonságaikat. Amennyiben a lehetséges tulajdonságok száma T és egy adott dokumentum ezekből legfeljebb M-mel rendelkezhet, a szükséges információ egy bináris vektorba kódolható, melynek hossza legalább

$$n = \log \sum_{m=0}^{M} \binom{T}{m} \simeq M \log T,$$

hiszen bármely, legfeljebb M tulajdonság együttesét meg kell tudnunk különböztetni.

Amennyiben a dokumentumok és tulajdonságaik bővülhetnek, akkor az ezeket leíró bináris vektort célszerű UD kódként előállítani, mivel egy újabb tulajdonság esetén csak az annak megfelelő kódszó VAGY kapcsolatát kell vennünk a régi Boole-összeggel. Legyen $\mathbf{x}_i$ az i-edik tulajdonsághoz rendelt bináris vektor. Ekkor az $i_1,...,i_m (m \le M)$ tulajdonságokkal rendelkező dokumentum leíró vektora az alábbi Boole-összegként adódik:

$$\mathbf{y} = \bigvee_{j\in\{i_1,...,i_m\}} \mathbf{x}_j.$$

Így UD(T,M,n) kód alkalmazásával a leíró vektorból meg tudjuk határozni, hogy a dokumentum mely tulajdonságokkal rendelkezik [14 és 5].

Az UD tulajdonság egyrészt nehezen ellenőrizhető, másrészt a dekódolás során kimerítő keresést igényel a legfeljebb M kódszóból álló összegvektorok halmazában. Ezek kiküszöbölésére bevezetünk egy könnyebben kezelhető tulajdonságot.

Azt mondjuk, hogy két, n hosszúságú bináris vektor közül $\mathbf{z} = (z_1,...,z_n)$ fedi $\mathbf{y} = (y_1,...,y_n)$ vektort, ha

$$\mathbf{z} \ge \mathbf{y},$$

vagyis $z_i \ge y_i$ ($i = 1,2,...,n$).

Az előző példában a leíró vektor kódolása egyszerű és gyors volt. Szeretnénk egy hasonlóan egyszerű dekódoló eljárást is. Vegyük észre, hogy tetszőleges $j \in \{i_1, i_2,...,i_m\}$-re

$$\mathbf{y} \ge \mathbf{x}_j.$$

Ez az UD kódok egy speciális esetéhez vezet.

2. definíció (ZFD kód)

T darab n hosszú kódszóból álló kód M-edrendben ZFD tulajdonságú (Zero False Drop, ZFD(T,M,n)), ha a legfeljebb M kódszóból álló összegek kizárólag az őket alkotó vektorokat fedik.

Formálisan ez azt jelenti, hogy ha valamely k-ra

$$\mathbf{y} \ge \mathbf{x}_k.$$

akkor

$$\mathbf{x}_k = \mathbf{x}_{i_j}$$

valamely i_j -re. A dokumentumkereső rendszer példájában tehát ZFD tulajdonság esetén egy $\mathbf{y}$ leíró vektorral rendelkező dokumentum pontosan akkor rendelkezik a k tulajdonsággal, ha

$$\mathbf{y} \ge \mathbf{x}_k.$$

Ez valóban gyors dekódolást tesz lehetővé, hiszen a tulajdonságok számának függvényében lineáris időben végrehajtható, míg csupán az UD tulajdonság alapján történő dekódolás során az összes lehetséges kombinációt meg kellene vizsgálnunk.

A ZFD tulajdonságot egy dekódolási szabállyal definiáltuk, ezért a ZFD(T,M,n) kód egyben UD(T,M,n) is. Mennyit vesztünk azzal, hogy ha UD kód helyett ZFD-t használunk?

1. tétel (Kautz és Singleton [14])

Egy UD(T,M,n) kód ZFD($T,M-1,n$) tulajdonságú, és egy ZFD(T,M,n) kód UD(T,M,n) tulajdonságú.

Bizonyítás

1. Legyen a C kód UD(T,M,n). Ha C nem lenne ZFD ($T,M-1,n$) tulajdonságú, akkor lennének olyan $\mathbf{x}_M \notin \{\mathbf{x}_1,...,\mathbf{x}_{M-1}\}$ kódszavai, hogy

   $$\mathbf{x}_M \le \mathbf{x}_1 \vee \mathbf{x}_2 \vee \cdots \vee \mathbf{x}_{M-1},$$

   vagyis

   $$\mathbf{x}_1 \vee \mathbf{x}_2 \vee \cdots \vee \mathbf{x}_{M-1} \vee \mathbf{x}_M = \mathbf{x}_1 \vee \mathbf{x}_2 \vee \cdots \vee \mathbf{x}_{M-1},$$

   ami ellentmond annak, hogy C UD(T,M,n).

2. Tegyük fel, hogy a C kód ZFD(T,M,n), de nem UD(T,M,n).
   Ekkor léteznek olyan $\{\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_K\} \ne \{\mathbf{y}_1,\mathbf{y}_2,...,\mathbf{y}_L\}$, $K,L \le M$ kódszóhalmazok, amelyekre

   $$\mathbf{x}_1 \vee \mathbf{x}_2 \vee \cdots \vee \mathbf{x}_K = \mathbf{y}_1 \vee \mathbf{y}_2 \vee \cdots \vee \mathbf{y}_L.$$

   Mivel a két halmaz nem egyenlő, létezik egy olyan kódszó, amely csak az egyikben van benne. Legyen ez $\mathbf{x}_i$, amely tehát nincs benne az $\{\mathbf{y}_1,\mathbf{y}_2,...,\mathbf{y}_L\}$ halmazban, ugyanakkor

   $$\mathbf{x}_i \le \mathbf{y}_1 \vee \mathbf{y}_2 \vee \cdots \vee \mathbf{y}_L,$$

   ami ellentmond a feltételezésünknek. ■

Jelölje $n_{ZFD}(T,M)$ és $n_{UD}(T,M)$ a ZFD(T,M) illetve az UD(T,M) kód minimális hosszát.

1. következmény

A ZFD és UD tulajdonságú kódosztályok között az alábbi tartalmazási kapcsolat áll fenn:

$$ZFD(T,M,n) \subseteq UD(T,M,n) \subseteq ZFD(T,M-1,n) \subseteq \cdots,$$

a minimális kódszóhosszakra pedig:

$$n_{ZFD}(T,M) \geq n_{UD}(T,M) \geq n_{ZFD}(T,M-1) \geq \cdots .$$

Példa: jelzéskódolás. Tekintsünk egy *T*-felhasználós többszörös hozzáférésű VAGY csatornát, ahol minden felhasználó rendelkezik egy *n* hosszúságú bináris vektorral (kódszóval). Ha egy felhasználó aktív, elküldi a saját kódszavát, ellenkező esetben a csupa 0 kódszót adja a csatorna bemenetére.

A VAGY csatorna kimenetéből, vagyis az aktív felhasználók kódszavainak Boole-összegéből meg kell tudnunk állapítani, hogy mely felhasználók voltak aktívak. Amennyiben egyidejűleg legfeljebb *M* felhasználó lehet csak aktív, úgy egy UD(*T,M,n*) kóddal megoldható a probléma, illetve az egyszerű dekódolhatóság érdekében használhatunk ZFD(*T,M,n*) kódot is.

Példa: riasztás. Fűzzünk fel *T* darab tűzjelző készüléket egy közös vezetékre. Amikor egy készülék jelezni kíván, OOK modulációval elküldi a kódszavát a vezetéken. Ha az egyidejű jelzések száma nem haladhatja meg az *M*-et, akkor az aktív állomások azonosíthatók a vezetéken megjelenő jelből.

Példa: bejelentkezés. Tekintsünk egy mobil távközlési rendszert, amelyben sok, viszonylag ritkán aktív felhasználó akar korlátozott számú csatornán keresztül kapcsolatot teremteni. Az adáshoz a felhasználóknak be kell jelentkezniük a rendszerbe. Ehhez elküldik az egyedi kódszavukat a bázisállomásnak egy VAGY csatornán keresztül, amelynek kimenetéből a bázisállomás megállapítja, hogy mely felhasználók aktívak, és mindegyikhez dedikált csatornát rendel, amelyen már ütközés nélkül kommunikálhatnak.

Napjainkban a mobil távközlőhálózatok a bejelentkezéshez véletlen hozzáférést használnak visszacsatolással. Ez a módszer kiváltható a VAGY csatornán alkalmazott jelzéskódolással, s így megtakarítható a visszacsatolások feldolgozása.

Példa: mérésadatgyűjtés. A fogyasztók elektromosenergia-felhasználását szeretnénk automatikusan összegyűjteni. Az elektromos hálózat használható többszörös hozzáférésű VAGY csatornaként. Minden fogyasztásmérő órához egyedi kódszót rendelünk, amelyet az mindig elküld a közös csatornán keresztül egy-egy egység, például 1 kWh elfogyasztása után.

Példa: csomagküldés ütközéses csatornán. A réselt ALOHA modellhez hasonlóan tekintsük a többszörös hozzáférésű ütközéses csatornát azzal a lényegi különbséggel, hogy nincs visszacsatolás, azaz az adó nem értesül arról, hogy a csomagja ütközött-e vagy sem.

Mindegyik adó rendelkezik egy egyedi kódszóval (protokoll sorozattal), az *i*-edik az $\mathbf{x}_i$-vel, és amennyiben az *i*-edik adónak van elküldendő csomagja, úgy azt az $\mathbf{x}_i$ 1-eseinek helyén ismételve elküldi, remélve azt, hogy a csomag legalább egyszer sikeresen átmegy. *T* felhasználó esetén, amelyek közül egyidejűleg legfeljebb *M* aktív, ZFD(*T,M*−1,*n*) kód alkalmazásával ez teljesíthető, vagyis minden $\mathbf{x}_i$ protokoll sorozatnak lesz olyan 1-ese, amelyet a másik *M*−1 protokoll sorozat nem fed le.

1.2. Kapcsolat a halmazrendszerekkel

A ZFD problémát többen és sokszor vizsgálták extremális halmazrendszerek kapcsán. Legyen *U* egy *n*-elemű alaphalmaz. $\binom{U}{k}$ módon jelöljük az *U* halmaz *k*-elemű részhalmazainak halmazát ($0 \leq k \leq n$), míg 2^U pedig *U* hatványhalmazát jelenti:

$$(2^U = \bigcup_{k=0}^{n} \binom{U}{k})$$

Az *U* halmaz részhalmazainak egy $\mathcal{F}$ rendszere a hatványhalmaz egy részhalmaza ($\mathcal{F} \subseteq 2^U$).

3. definíció
(Fedésmentes halmazrendszer, [10 és 11])
Az $\mathcal{F}$ halmazrendszer M-fedésmentes, ha

$$F_0 \not\subseteq F_1 \cup \cdots \cup F_M$$

fennáll minden különböző $F_0,F_1,...,F_M \in \mathcal{F}$ halmazra.

Keressük az $\mathcal{F} \subseteq 2^U$ *M*-fedésmentes halmazrendszer maximális *T* méretét, ha $|U| = n$. Ez a probléma megegyezik a ZFD kódok minimális hosszának meghatározásával.

A paraméterek megfeleltetése a következő. Legyen $U = \{1,2,...,n\}$, és egy $F \in \mathcal{F}$ halmazhoz rendeljük az $\mathbf{x}_F$ bináris kódszót, amelynek *i*-edik pozícióján pontosan akkor áll 1-es, ha $i \in F$.

A halmazrendszer *T* számossága játssza a lehetséges felhasználók számának szerepét, az *M*-fedésmentes tulajdonság felel meg az *M*-edrendű ZFD tulajdonságnak és az *U* alaphalmaz *n* mérete pedig a kódszóhossznak.

2. ZFD kódok minimális hosszára vonatkozó korlátok

Ebben a szakaszban korlátokat adunk a ZFD(*T,M*) kód minimális hosszára.

A legegyszerűbb alsó korlátot annak felismerésével kapjuk, hogy a legfeljebb *M* kódszóból álló összegvektoroknak különbözniük kell egymástól, vagyis számuk nem haladhatja meg az *n*-bites bináris vektorok számát:

$$\sum_{k=0}^{M} \binom{T}{k} \leq 2^n$$

Felhasználva, hogy $\sum_{k=0}^{M} \binom{T}{k} \simeq T^M$ kapjuk a következő korlátot:

$$n_{\mathrm{ZFD}}(T,M) \geq M \log T.$$

Bassalygo alábbi eredménye jellegében eltér a szokásos korlátoktól, azonban támpontot ad arra vonatkozólag, hogy milyen esetekben érdemes az időosztásnál hatékonyabb kódolást keresnünk.

2. tétel (Bassalygo-korlát, [8,9,1])

$$n_{ZFD}(M,T) \geq \min\left\{\frac{(M+1)(M+2)}{2}, T\right\}$$

A tételből következik, hogy ha $\sqrt{2}T < M < T$, akkor $n_{\text{ZFD}}(T,M) = T$, vagyis ha M értéke ebben a tartományban van, akkor egyetlen ZFD(T,M) kód sem lehet jobb az időosztásnál.

3. tétel [8,9,11,15]

A ZFD(T,M) kód minimális hosszára jelenleg ismert legjobb alsó korlát, $T \to \infty$, $M \to \infty$ és $M \ll T$ esetén:

$$n_{ZFD}(T,M) \geq k \frac{M^2}{\log M}(1+o(1))\log T$$

ahol a k konstans értéke [8] szerint 1/2*, [11] szerint* 1/4*, [15] alapján pedig* 1/8*.*

A és Zeisel [3] a véletlen kódválasztás technikájával adott felső korlátot a minimális kódszóhosszra.

4. tétel [3]

Rögzített M és $T \to \infty$ esetén

$$n_{ZFD}(T,M) \leq K(M)M^2(1+o(1))\log T,$$

ahol $K(M) \leq 1.5112$.

Amennyiben $M \to \infty$ is teljesül,

$$\limsup_{M\to\infty} K(M) = \frac{1}{\ln 2} \approx 1.4427$$

Bizonyítás

Tekintsünk egy véletlenszerűen választott kódot az 1,2,...,L ($L \geq M$) ábécé felett. A kódszavak hossza n/L, és az egyes szimbólumokat egymástól függetlenül egyenletes eloszlás szerint sorsoljuk. Ebből a kódból készítünk egy bináris C kódot úgy, hogy minden szimbólumot L hosszúságú, 1 súlyú bináris sorozattal helyettesítünk az alábbi leképezés szerint:

$$\begin{aligned} &1 \Rightarrow 0\ldots001\\ &2 \Rightarrow 0\ldots010\\ &\ldots\\ &L \Rightarrow 1\ldots000 \end{aligned}$$

Ekkor a C kód n hosszúságú, bináris kódszavakból áll. A C kód nem teljesíti a ZFD tulajdonságot, amennyiben ki tudunk választani a T darab kódszó közül M-et úgy, hogy minden L hosszú szegmensben legalább egynek olyan pozíción van az 1-es bitje, amely megegyezik egy tőlük függetlenül választott (M+1)-edik kódszóéval.

$$\begin{aligned} \mathbf{P}_{(C\text{ nem ZFD})} &\leq \binom{T}{M}(T-M)\left(1-\left(1-\frac{1}{L}\right)^M\right)^{\frac{n}{L}} \leq \\ &\leq \exp\left((M+1)\ln T + \frac{n}{L}\ln\left(1-\left(1-\frac{1}{L}\right)^M\right)\right) \end{aligned}$$

Azt kell belátnunk, hogy ez a valószínűség 1-nél kisebb, mert ekkor létezik M-edrendű ZFD kód. Ehhez az exponenciális függvény argumentumának kell 0-nál kisebbnek lennie:

$$(M+1)\ln T + \frac{n}{L}\ln\left(1-\left(1-\frac{1}{L}\right)^M\right) < 0$$

Ebből a kódszóhosszat kifejezve kapjuk, hogy

$$\frac{(M+1)L\log T}{-\log\left(1-\left(1-\frac{1}{L}\right)^M\right)} < n_{\text{véletlen}}$$

vagyis a kódszóhosszat ennél nagyobbra választva létezik M-edrendű ZFD kód, tehát a minimális kódszóhossz ennél nem nagyobb:

$$n_{\text{ZFD}}(T,M) \leq \frac{(M+1)L\log T}{-\log\left(1-\left(1-\frac{1}{L}\right)^M\right)}.$$

Aszimptótikusan az alábbi felső határt kapjuk:

$$n_{ZFD}(T,M) \leq K(M)M^2(1+o(1))\log T$$

ahol

$$K(M) = \min_{M\leq L} \frac{\ln 2}{-\frac{M+1}{L}\ln\left(1-\left(1-\frac{1}{L}\right)^M\right)}$$

Válasszuk meg a szegmenshosszt $L = \left\lfloor \frac{M+1}{\ln 2} \right\rfloor$ értékre, és alkalmazzuk az $M \leq L$ esetén fennálló

$\left(1-\frac{1}{L}\right)^M \geq \exp\left(-\frac{M+1}{L}\right)$ egyenlőtlenséget.

Így kapjuk, hogy

$$K(M) \leq \frac{\ln 2}{-\alpha\ln(1-e^{-\alpha})} \leq \frac{\ln 2}{-\ln(1-e^{-1})} \approx 1.5112$$

ahol $\alpha = \frac{M+1}{\left\lfloor \frac{M+1}{\ln 2} \right\rfloor}$.

Ha $M \to \infty$, akkor $\alpha \to \ln 2$, így

$$\limsup_{M\to\infty} K(M) = \frac{\ln 2}{-\ln 2\ln(1-e^{-\ln 2})} = \frac{1}{\ln 2} \approx 1.4427$$

s ezzel beláttuk a tételt. ■

A minimális kódszóhosszra kapunk felső korlátot abban az esetben is, ha a 4. tételtől eltérően nem konstans súlyú kódszavakkal dolgozunk, hanem a kódszavakban szereplő 1-es bitek száma binomiális eloszlás szerinti.

5. tétel (Dyachkov és Rykov [9])

$1 \ll M \ll T$ *és* $T \to \infty$ *esetén*

$n_{ZFD}(T,M) \leq e\ln 2M(M+1)\log T \approx$
$1.884M^2(1+o(1))\log T.$

Bizonyítás

Tekintsünk egy n hosszú kódszavakból álló véletlenszerűen választott bináris kódot. A kódszavak bitjeit egymástól függetlenül sorsoljuk: p valószínűséggel 1-est, 1 – p valószínűséggel pedig 0-t. Így egy kódszóban lévő 1-esek száma binomiális eloszlást követ. A C kód nem ZFD tulajdonságú, amennyiben ki tudunk választani a T darab kódszó közül M-et úgy, hogy minden olyan pozíción, ahol egy tőlük függetlenül választott (M+1)-edik kódszó 1-est tartalmaz, az M közül legalább egynek szintén van 1-ese.

$$\begin{aligned} &\mathbf{P}(C\text{ nem ZFD})\\ &\leq \sum_{k=0}^{n} \mathbf{P}(\text{minden 1-es fedett} \mid \text{1-esek száma} = \\ &\qquad = k)\mathbf{P}(\text{1-esek száma} = k) \leq \end{aligned}$$

$$\leq \sum_{k=0}^{n} \binom{T}{M} (T-M) \left(1-(1-p)^M\right)^k \binom{n}{k} p^k (1-p)^{n-k} =$$

$$= \binom{T}{M} (T-M) \sum_{k=0}^{N} \binom{n}{k} \left(p\left(1-(1-p)^M\right)\right)^k (1-p)^{n-k} =$$

$$= \binom{T}{M} (T-M) \left(p\left(1-(1-p)^M\right)+1-p\right)^n =$$

$$= \binom{T}{M} (T-M) \left(1-p(1-p)^M\right)^n .$$

Ez a kifejezés a minimumát $p = \frac{1}{M+1}$ esetén veszi fel, és itt az értéke

$$\begin{aligned}
&\mathbf{P}(C \text{ nem ZFD}) \\
&\leq \binom{T}{M} (T-M) \left(1-\frac{1}{M+1}\left(1-\frac{1}{M+1}\right)^M\right)^n \leq \\
&\leq \binom{T}{M} (T-M) \left(1-\frac{\mathrm{e}^{-1}}{M+1}\right)^n \leq \\
&\leq \binom{T}{M} (T-M) \mathrm{e}^{-\frac{n}{M+1}\mathrm{e}^{-1}} \leq \\
&\leq T^M \mathrm{e}^{-\frac{n}{M+1}\mathrm{e}^{-1}} = \\
&= \mathrm{e}^{M\ln 2 \log T - \frac{n}{M+1}\mathrm{e}^{-1}} < \\
&< 1.
\end{aligned}$$

Mindkét oldal logaritmusát véve kapjuk

$$M \ln 2 \log T - \tfrac{n}{M+1}\mathrm{e}^{-1}$$

és ebből

$$\mathrm{e}\ \ln 2 M(M+1)\ \log T < n_{\text{véletlen}},$$

vagyis a kódszóhosszat ennél nagyobbra választva létezik M-edrendű ZFD kód, tehát a minimális kódszóhossz ennél nem nagyobb:

$$n_{\text{ZFD}}(T,M) \leq \mathrm{e}\ \ln 2 M(M+1)\ \log T. \qquad \blacksquare$$

3. Kódkonstrukciók

ZFD kódok létrehozására Kautz és Singleton [14] konstans súlyú módszert javasolt.

Egy kód maximális átlapolásának (maximum overlap) vagy keresztkorrelációjának (cross-correlation) hívjuk azon pozíciók számát, amelyeken két tetszőlegesen választott kódszó közül mindkettőben 1-es áll.

1. lemma [14]

Legyen w_{min} a C kód kódszavainak minimális súlya. Ha a kódszavak közötti maximális átlapolás c, akkor a C kód ZFD tulajdonságú legalább M_0-adrendben, ahol

$$M_0 = \left\lfloor \frac{w_{min}-1}{c} \right\rfloor .$$

Ha minden c elemű szimbólumegyüttes a C kód legalább két kódszavában szerepel, akkor a kód rendje pontosan M_0.

Bizonyítás

A C kód rendelkezik a ZFD tulajdonsággal M_0-adrendben, ugyanis minden kódszó súlya legalább $w_{\min} \geq M_0 c+1$, így egyetlen kódszót sem tud tőle különböző M_0 darab másik kódszó Boole-összege lefedni, hiszen mindegyikkel csak legfeljebb c pozíción lapol át.

Ha minden c elemű szimbólumegyüttes legalább két kódszóban szerepel, akkor bármely legfeljebb $(M_0+1)c$ súlyú kódszóhoz található M_0+1 másik kódszó, amelyek összege fedi azt. Így C nem lehet ZFD tulajdonságú M_0+1-edrendben. ■

6. tétel [14 és 10]

Legyen C_Q egy (n_Q,k) paraméterű és d_Q kódtávolságú GF(Q) feletti kód (Q prímhatvány). Helyettesítsük a Q-áris szimbólumokat Q-hosszú 1-súlyú bináris sorozatokkal a következő módon:

$$\begin{aligned}
0 &\Rightarrow 0\ldots001 \\
1 &\Rightarrow 0\ldots010 \\
&\ldots \\
Q-1 &\Rightarrow 1\ldots000
\end{aligned}$$

Az így kapott konkatenált C kód $T = Q^k$ kódszót tartalmaz, melyek hossza $n=Qn_Q$, és legalább M-edrendben ZFD tulajdonságú, ahol

$$M \geq \left\lfloor \frac{n_Q-1}{n_Q-d_Q} \right\rfloor .$$

Bizonyítás

Nyilvánvalóan $T = |C| = |C_Q| = Q^k$, $n = Qn_Q$. A bináris kód Hamming-távolsága a Q-áris távolság kétszerese: $d=2d_Q$, és minden kódszó $w=n_Q$ súlyú. A bináris kód maximális átlapolása

$$c = w - \frac{d}{2} = n_Q - d_Q,$$

melyből az 1. lemma miatt következik az állítás. ■

Vizsgáljuk meg a Kautz–Singleton-konstrukció néhány speciális esetét!

Reed–Solomon kód [2, 10, 17]

Legyen C_Q egy maximális, $n_Q=Q-1$ hosszú Reed–Solomon-kód. A C konkatenált kódnak $T=Q^k$ kódszava van, s mindegyiknek $w=n_Q=Q-1$ súlya.

Mivel a Reed–Solomon-kód maximális távolságú, így $d_Q=n_Q-k+1$ (lásd Györfi, Győri és Vajda [13]), amiből

$$c = n_Q - (n_Q - k + 1) = k - 1.$$

Egy maximális távolságú kódban bármely k szimbólum lehet üzenet, így minden $c = k-1$ elemű szimbólumegyüttes pontosan Q-szor ismétlődik a bináris kódban. Az 1. lemmából következően a ZFD tulajdonság rendje pontosan

$$M = \left\lfloor \frac{w-1}{c} \right\rfloor = \left\lfloor \frac{Q-2}{k-1} \right\rfloor .$$

Felhasználva, hogy $k = \frac{\log T}{\log Q}$ kapjuk az alábbi egyenlőtlenséget:

$$\frac{\log T}{\log Q} \leq \frac{Q-2}{M} + 1.$$

Ha adott *T,M*, és egy minimális hosszúságú kódot szeretnénk előállítani a Kautz–Singleton-konstrukcióval, akkor meg kell keresnünk ennek az egyenlőtlenségnek eleget tevő legkisebb (prímhatvány) *Q* értéket, s ekkor a kódszóhossz $n = Qn_Q = Q(Q-1)$.

BCH kód [12]

Legyen C_Q egy maximális, $n_Q = Q^r - 1$ hosszú BCH-kód valamely $r \geq 2$-re. Ekkor a C konkatenált kódnak $T = |C_Q| = Q^{(k-1)r+1}$ kódszava van, melyek hossza $n = Qn_Q = Q(Q^r - 1)$, súlyuk pedig $w = n_Q = Q^r - 1$. C_Q minimális távolságára alsó becslést adhatunk [4]:

$$d_Q \geq Q^r - 1 - (k-1)Q^{r-1}.$$

Ekkor a C bináris kód ZFD tulajdonságának rendje legalább

$$\begin{aligned} M &\geq \frac{n_Q - 1}{n_Q - d_Q} \\ &\geq \frac{(Q^r - 1) - 1}{(Q^r - 1) - (Q^r - 1 - (k-1)Q^{r-1})} \\ &= \frac{Q^r - 2}{(k-1)Q^{r-1}} \\ &\simeq \frac{Q}{k-1}, \end{aligned}$$

ami hozzávetőleg megegyezik a Reed–Solomon-kód esetében kapott értéknek. A BCH-kód használatának előnye, hogy a lehetséges felhasználók számára még kis *r* érték esetén is hatalmas számot kapunk, bár az is igaz, hogy a minimális kódszóhossz szintén nagyobb a Reed–Solomon-kódéhoz képest.

A kódkonstrukciókról részletes tanulmány olvasható Dyachkov, Macula és Rykov [7] írásában.

Irodalom

[1] N. Q. A., Some coding problems of multiple-access communication systems. DSc dissertation, Hungarian Academy of Sciences, 1986.

[2] N. Q. A, L. Györfi, and J. L. Massey, Constructions of binary constantweight cyclic codes and cyclically permutable codes. Problems of Control and Information Theory, 38(3):940–949, 1992.

[3] N. Q. A and T. Zeisel, Bounds on constant weight binary superimposed codes. Problems of Control and Information Theory, 17(4):223–230, 1988.

[4] R. E. Blahut, Theory and Practice of Error Control Codes. Reading, MA: Addison-Wesley, 1984.

[5] R. T. Chien and W. D. Frazer, An application of coding theory to document retrieval. IEEE Transactions on Information Theory, 12(2):92–96, 1966.

[6] A. R. Cohen, J. A. Heller, and A. J. Viterbi, A new coding technique for asynchronous multiple access communication. IEEE Transactions on Communication Technology, 19:849–855, 1971.

[7] A. G. Dyachkov, A. J. Macula, and V. V. Rykov, New constructions of superimposed codes. IEEE Transactions on Information Theory, 46(1):284–290, 2000.

[8] A. G. Dyachkov and V. V. Rykov, Bounds on the length of disjunctive codes. Problemy Peredachi Informatsii, 18(3):7–13, 1982.

[9] A. G. Dyachkov and V. V. Rykov, A survey of superimposed code theory. Problems of Control and Information Theory, 12(4), 1983.

[10] P. Erdős, P. Frankl, and Z. Füredi, Families of finite sets in which no set is covered by the union of *r* others. Israel Journal of Mathematics, 51(1-2):79–89, 1985.

[11] Z. Füredi, On r-cover-free families. Journal of Combinatorial Theory, 73:172–173, 1996.

[12] L. Györfi and I. Vajda, Constructions of protocol sequences for multiple access collision channel without feedback. IEEE Transactions on Information Theory, 39(5):1762–1765, 1993.

[13] Györfi L., Győri S. és Vajda I., Információ- és kódelmélet. TypoTEX, Budapest, 2002.

[14] W. H. Kautz and R. C. Singleton, Nonrandom binary superimposed codes. IEEE Transactions on Information Theory, 10:363–377, October 1964.

[15] M. Ruszinkó, Note on the upper bound of the size of the *r*-cover-free families. Journal of Combinatorial Theory, 66(2):302–310, 1994.

[16] I. Vajda, Code constructions for code division multiple access channels. Journal on Communications, 45:2–9, 1994.

[17] V. A. Zinoviev, Cascade equal-weight codes and maximal packings. Problems of Control and Information Theory, 12(1):3–10, 1983.