Rónyai Lajos előadása alapján írta: Sas Gábor és Vecsei Balázs

Az algebrai geometria a polinomokkal (egyenletekkel) definiált alakzatokkal foglalkozik. Ilyen alakzat például a körvonal, $V(x^2+y^2-r,\ L) \subseteq L^2,\ r \in L$.

1 Definíció (polinomokkal definiált alakzat). Legyen $f_1(\underline{x}), \ldots, f_m(\underline{x}) \in K[x_1, \ldots x_n],\ K \subset L$, ahol K test. Ekkor a polimokkal definiált alakzat a következő:

$$V(f_1, f_2, \ldots f_m, L) = \sum \underline{\alpha} = (\alpha_1, \ldots, \alpha_n),\ \alpha_i \in L,\ f_i(\underline{\alpha}) = 0$$

Cél: a véletlen kódoknál jobbat elérni. A véletlen kódokra jó eséllyel $R \geq 1 - \mathrm{H_q}(\delta)$ ($[n,k,d]_q$)-kód)), ahol

$\mathrm{H_q}$	az entrópiafüggvény	$R = \frac{k}{n}$	a sebesség
q	a jegyek száma	d	a minimális kódtávolság
$\delta = \frac{d}{n}$	a relatív távolság		

$\mathrm{H_q}(\delta) \approx \delta + O\left(\frac{1}{\log_2 q}\right)$. Itt az $O()$-ban rejlő konstans függ a δ-tól, tehát a közelítés akkor jó, ha δ fix és q nagy.

Viszony a Singleton-korláthoz:
$d \leq n - k + 1$
$\frac{d}{n} \leq \frac{n}{n} - \frac{k}{n} + \frac{1}{n}$
$\delta \leq 1 - R + \frac{1}{n} \Rightarrow R < 1 - \delta$

A véletlen kód tehát $O\left(\frac{1}{\log_2 q}\right)$ hibával közelít a Singleton korláthoz. (G)RS-kódoknál $d = n - k + 1$, , tehát $R = 1 - \delta + O\left(\frac{1}{q}\right)$ de n növelésével q-nak is nőnie kell, hiszen GRS-kódok csak $n \geq q$ esetén léteznek.

Algebrai geometriai kódokkal: elérhető tetszőleges q prímhatványra az $R = 1 - \delta - O\left(\frac{1}{\sqrt{q}}\right)$. Jobbak a véletlen kódoknál és szép struktúrájuk miatt hatékonyan konstruálhatók és dekodolhatók.

2 Állítás. Legyen K test, $0 \not\equiv f(x) \in K[x] \Rightarrow f$-nek $\leq \deg(f)$ darab gyöke van K-ban.

3 Állítás. Az $f(x_1, \ldots, x_n, t) \in K[x_1, \ldots x_n][t]$ polinomnak legfeljebb $\deg_t(f)$ darab $g(\underline{x})$ gyöke van $K[x_1, \ldots x_n]$-ben. Azaz legfeljebb $\deg_t(f)$ olyan $g(\underline{x}) = g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ n-változós polinom van, amelyre $f(\underline{x}, g(\underline{x})) = 0$.

4 Megjegyzés. $K[x_1, \ldots x_n][t]$ és $K[x_1, \ldots x_n, t]$ izomorfak.

Biz.: $K[x_1, \ldots, x_n] \subseteq K(x_1, \ldots, x_n) = l,\ f \in L[t],\ f$-nek $\leq \deg_t(f)$ gyöke van L-ben, így ennek részgyűrűiben is. □

5 Tétel. *Legyen* $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots x_n]$ $f \not\equiv 0$, *ekkor* f *nem tűnik el* $GF(q)^n$ *legalább* $\prod_{i=1}^{n}(q - \deg_{x_i}(f))$ *darab pontjában.*

Biz.: Indukció n szerint. $f(x_1)$nek legfeljebb $\deg_{x_1}(f)$ gyöke van.

Tegyük fel hogy $n > 1,\ f(\underline{x}) \in GF(q)[x_1, \ldots, x_{n-1}][x_n]$. Ekkor az előző állítás miatt legfeljebb $\deg_{x_n}(f)$ darab $\alpha \in GF(q)$ van, amelyre $f(x_1, \ldots, x_{n-1}, \alpha) = 0$, és ha α nem ilyen, (ezekből legalább $q - \deg_{x_n}(t)$ darab van), akkor $f_\alpha(x_1, \ldots, x_{n-1}) := f_\alpha(x_1, \ldots, x_{n-1}, \alpha),\ f_\alpha \not\equiv 0$.

$\deg_{x_i}(f_\alpha) \leq \deg_{x_i}(f)$, így az indukciós feltevés szerint legalább $\prod_{i=1}^{n-1}(q - \deg_{x_i}(f_\alpha)) \geq \prod_{i=1}^{n-1}(q - \deg_{x_i}(f))$ pontban. Ezt szorozva a jó α-k számával következik az állítás. □

6 Megjegyzés. Ez a korlát éles minden n-re.

A GRS-kódok kétdimenziós általánosítása

7 Definíció ($B_{q,l}$ kódok). Legyen q prímhatvány, $0 < l < q$ egész. Az üzenetszavak: $(l+1) \times (l+1)$-es mátrixok $GF(q)$ felett, az üzenetjegy száma $(l+1)^2$.

Az $m = (m_{ij})_{i,j=0}^{l}$ üzenetszót vehetjük kétváltozós polinomnak is. $m \leftrightarrow M(x,y) := \sum_{i=0}^{l}\sum_{j=0}^{l} m_{ij}x^iy^j$ A $B_{q,l}$ kód m üzenetének a kódolt változata: $\langle M(\alpha,\beta)\rangle_{\alpha,\beta \in GF(q)}$. A $B_{q,l}$ kód paraméterei: $n = q^2$, a kiértékelő helyek száma, q a jegyhalmaz mérete.

Az előző tétel miatt $d \geq (q-l)^2$. Fordítva: $d \leq (q-l)^2$ mert alkalmas $f(x)g(y)$ alakú $M(x,y)$ egyenlőséget ad, tehát $d = (q-l)^2$.

Ha $M(x,y) \neq 0 \Rightarrow$ akkor a kódszó sem, tehát a kódoló leképezés az üzenetek halmazéból a kódszavak halmazába injektív. $k = (l+1)^2$. A $B_{q,l}$ kódok tehát $[q^2, (l+1)^2, (q-l)^2]_q$-kódok. A $GF(q^2)$ feletti GRS-kódok $[q^2, (l+1)^2, q^2 - (l+1)^2 + 1]_{q^2}$-kódok. A távolságok különbsége: $2l(q-l) - 2l$ a GRS-kódok javára, tehát a $B_{q,l}$ kódoknál használt kisebb jegyhalmaz ennyi veszteséget okoz a kódtávolságban.

$M(x,y)$ L-en $h(t) = M(u_1 + tv_1, u_2 + tv_2)$ $\deg(h(t)) \leq 2l$, ha ez eltűnik $2l+1$ helyen, akkor $h \equiv 0$

Az ilyen részhalmazokat célszerű elkerülni. Tehát olyan S halmazt választunk, mint behelyettesítési pontok halmazát, ami a kisfokú görbéket kevés pontban metszi.

8 Tétel (Bézout). *Legyen K test, $K \subset L$ és $f, g \in K[x,y]$, tegyük fel, hogy nincs közös osztójuk $\bar{K}[x,y]$-ban. Ekkor* $|V(f,L) \cup V(g,L)| \leq \deg(f)\deg(g)$. **(Nem bizonyítjuk.)** □

Ötlet: $GF(q)^k$ helyett egy **görbe** pontjait vesszük, mint helyettesítési halmazt.

9 Példa. $\mathbb{F} := GF(13)$, $q := 13$, $S := V(R) \subseteq \mathbb{F}^2$ $R(x,y) := y^2 - 2x(x-1)(x+1)$. Az üzenetszavak (-polinomok) legyenek: $\langle 1, x, x, x^2, x^3, y, xy \rangle$ lineáris kombinációi. Ezekből 13^6 darab van. $M(x,y)$ üzenetpolinom $\mapsto \langle M(\alpha,\beta) \rangle_{(\alpha,\beta)\in V(R)}$ kódszó.

10 Állítás. A kódhossz $n = 19$: $S = \{(0,0), (\pm 1, 0), (2, \pm 5), (3, \pm 3), (4, \pm 4), (6, \pm 2), (7, \pm 3), (9, \pm 6), (10, \pm 2), (11, \pm 1)\}$□

11 Állítás. Legyen $M = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + b_0 y + b_1 xy$ egy nem $\equiv 0$ üzenet szó, $a_i, b_i \in \mathbb{F}$. Ekkor $| V(M) \cap V(R) | \leq 6$.

Hf: Egyenlőseg lehetséges

Biz.:

1. $R(x,y)$ irred. $\bar{\mathbb{F}}[x,y]$ -ban. Tegyük fel indirekte, hogy $R = F_1 F_2$, $\deg F_i > 0$. Az nem lehet, hogy valamelyik F_i -re $\deg_y F_i = 2$, mert ekkor volna $y^2 f(x)$ alakú tag R -ben. Tehát $F_1 = y - f_1(x)$ és $F_2 = y - f_2(x)$. De R -ben nincs olyan tag, amely elsőfokú y-ban, így $F_1 F_2 = y^2 - (f_1(x) + f_2(x))y + f_1(x) f_2(x)$ miatt $f_1 = -f_2$, azaz $R = y^2 - f_1^2(x)$ alakú, ami képtelenség, hiszen $(2(x-1)x(x+1)$ -nek nincs (nem triviális) többszörös osztója.

2. R, M- nek nincs (nem triv.) közös osztója. Ha volna, az csak R lehetne, de $R \nmid M$.

3. $M(x,y) + \frac{a_3}{2} R(x,y) =: H(x,y)$ -nak sincs közös osztója R -rel, mert különben M -nek és R-nek is volna. (Itt az x^3 tagot vontuk le.)

4. $V(M) \cap V(R) = V(H) \cap V(R) \Rightarrow$ elég az állítást M helyett H -ra bizonyítani. Mivel $\deg R = 3$, $\deg H \leq 2$, Bézout tétele szerint a metszet elemszáma $\leq 2 * 3 = 6$.

□

12 Következmény. A dimenzió $k = 6$, a kódtávolság $d = 13$. Így egy $[19, 6, 13]_{13}$ kódot kaptunk. (A megfelelő GRS-kód paraméterei: $[19, 6, 14]_q$, $q \geq 19$, tehát a távolságban 1-et vesztettünk, de az ábécé kisebb.)

Biz.: A kódtávolság (a linearitás miatt a legkisebb nem nulla súly) 19-6=13 az állítás és a feladat alapján. Ugyancsak az állításból következik, hogy a kódolás hűséges: $M \not\equiv 0$, akkor a belőle képzett kódszó sem 0 (≤ 6 zérus-koordinátája lehet). Mivel az üzenetttér 6 dimenziós, ugyanekkora lesz tehát a kód is. □

Általános konstrukció (AG-Kódok): , $\mathbb{F} = GF(q)$

- Vesszünk alkalmas $P_1, \ldots, P_{m-1} \in \mathbb{F}[x_1, \ldots, x_m]$ polinomokat (m-1 egyenlet kell egy görbe leírásához, ha dim=m).
- $S = V(f_1, f_2, \ldots, f_{m-1}, \mathbb{F})$
- Választunk olyan $U \subseteq \mathbb{F}[x_1, \ldots, x_m]$ polinom-alteret, melynek elemei nem tűnnek el sok S-beli helyen.
- Üzenetek: U
- Kódszavak: $< M(\underline{\alpha}) >_{\underline{\alpha} \in S}$, $\quad M \in U$

A nehézség: nagy $| S |$ és jó U együttes biztosítása.

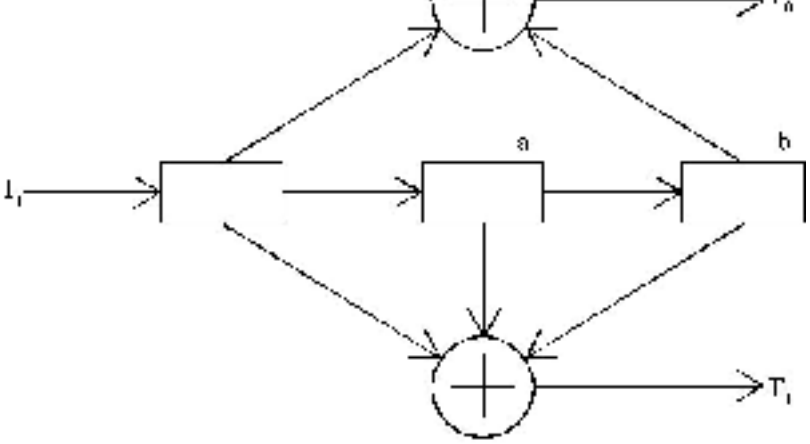
13 Tétel. Nagyon jó AG-kódok vannak: *Legyen q és δ rögzített ($\delta < 1 - \frac{1}{\sqrt{q}-1}$). Ekkor végtelen sok n -re létezik olyan AG-kód n, δ paraméterekkel $GF(q)$ felett, amelyre*

$$R > 1 - \delta - \frac{1}{\sqrt{q}-1} = 1 - \delta - O(\frac{1}{\sqrt{q}}).$$

- Első: Tsfasman - Vladut' - Zink, 1982.
- Jelenlegiek sokkal egyszerűbbek és explicitek.
- Garcia - Stichtenoth, 1995: (a kód generátor mátrixa $n^3(\log n)^{O(1)}$ időben konstruálható.
  A Garcia-Stichtenoth–görbe:
  - $q = r^2$, r prímhatvány $\quad \mathbb{F} = GF(q)$
  - változók $2m$ darab: $x_1, x_2, \ldots, x_m, y_1, \ldots, y_m$
  - befogadó tér: $\mathbb{F}^{2m}$
  - polinomok (egyenletek): $2m-1$ darab:
    $x_i^{r+1} = y_i^r + y_i \qquad (i = 1, \ldots, m)$
    $x_i x_{i+1} = y_i \qquad (i = 1, \ldots, m-1)$
  - $m = 1$ eset: síkgörbe: $x^{r+1} = y^r + y$, $GF(r^2)$ felett.
    (Ez az úgynevezett *Hermit-görbe*; r^3 pontja van.)
    (Az egyenletet másképp is lehet írni: baloldalon a norma szerepel, jobbon pedig a nyom, azaz Norma(x)=Nyom(y).)
    Görbe $\subseteq F^2$, $\mid F^2 \mid = r^4$

Jó könyv a témához: Algebraic function fields and codes; Stichenoth-tól

Főtétel (csak név): Rieman-Roch–tétel.



Konvolúciós kódok

Friedl Katalin és Rónyai Lajos előadása alapján írta: Balla Péter és Sas Gábor

tulajdonságok:

- nem blokk-kód
- folyamatos inputból folyamatos outputot generál
- kevésbé gazdag a matematikájuk
- néhány igen sikeres gyakorlati alkalmazásuk van, pl. bolygóközi kommunikáció)

példa: ($q = 2$): lásd ábra

- Az ábrában a téglalapok úgynevezett flip - flop-okat ábrázol (= 1 bites memóriacella.)
- Az összeadás a modulo 2 összeadást jelenti.
- Két darab shift-regisztert alkot (felső, alsó).
- I_0: input bitfolyam.
- T_0, T_1 két output bitfolyam.
- $t_0, t_1, \ldots$ időpillanatokban lép a szerkezet.
- A kezdetben a kódoló állapota adottnak kell hogy legyen, legtöbbször a és b kezdőállapota 0.

példa: Input: 0 0 0 1.
(Konvolúciós kódoknál szokásos az inputot jobbról balra felírni, azaz a mi példánkban $i_0 = 1$ és $i_1 = i_2 = i_3 = 0$.)

	inputbit	a	b	T_0	T_1
t_0	1	0	0	1	1
t_1	0	1	0	0	1
t_2	0	0	1	1	1
t_3	0	0	0	0	0

A kódoló T_0-t és T_1 -et összefésüli $\rightarrow$ 00 11 01 11

honnan (ab)	inputbit (I_0)	hova (ab)	outputbit (T_0, T_1)
00	0	00	00
00	1	10	11
01	0	00	11
01	1	10	00
10	0	01	01
10	1	11	10
11	0	01	10
11	1	11	01

Matematikai leírás: A bemenet legyen $i_0, i_1, \cdots \in GF(2)$. Felírhatunk egy formális hatványsort: $i_0 + i_1 x + i_2 x^2 + \cdots =: I_0(x)$. Véges bemenetre ez egy polinom. Ugyanigy felírható hatványsor a kimenet mindkét bitsorozatára, ezek lesznek $T_0(x)$ és $T_1(x)$.

Megjegyzés Előbbi példában $T_0(x) = (1 + x^2)I_0(x)$ és $T_1(x) = (1 + x + x^2)I_0(x)$.

T_0 és T_1 összefésülése Páros helyekre T_0-belieket rakjuk, $T_0(x^2)$ pont ez; a páratlan helyekre pedig $xT_1(x^2)$ kerül. E kettő összege az összefésült kimenet: $T(x) := T_0(x^2) + xT_1(x^2)$.

Generálópolinom Legyen $G_0 := 1 + x^2$ és $G_1 := 1 + x + x^2$. Ekkor a kimenet igy irható:

$$T(x) = G_0(x^2)I_0(x^2) + xG_1(x^2)I_0(x^2) = I_0(x^2)(G_0(x^2) + xG_1(x^2))$$

Az $I(x) = I_0(x^2)$ s a $G(x) = G_0(x^2) + xG_1(x)$ jelölésekkel:

$$T(x) = G(x)I(x).$$

$G(x)$-et (vagy alkalmanként $G_0(x)$-et és $G_1(x)$-et) a kód generátorpolinomjának (-jainek) nevezik.

Definició Terjedési távolság: egy bemeneti bit hány kimeneti bitre hat.

Megjegyzés Előbbi példában ez 6, ugyanis 3 lépésen keresztül van az összeadóban egy bit. Igaz, hogy a 2. lépésben a 2. cella T_0-t nem befolyásolja, de definiálhatnánk ilyen szigorúan is. A kényelmes algebrai kezeléshez a terjedési távolságra vegyünk $\deg G(x) + 1$-et.
A fenti $G_0(x)$ és $G_1(x)$ másodfokú, x^2-et helyettesítve már negyedfokú, de egyik tagnak van még egy x-es szorzója, így $\deg G(x) = 5$. Ehhez egyet adva megkapjuk a 6-ot.

Definició Memóriaigény: hány korábbi inputbitet kell megjegyezni - hány cella van.

Definició Szabad távolság $:= min_{I(x)} \quad w(T_(x))$, ahol w a szokásos (Hamming-) súlyfüggvény, a nemnulla bitek száma.

Példa Legyen $i_0 = 1, i_1 = i_2 = \cdots = 0$. Erre a bemenetre a kódsorozat súlya 5, így a konvolúciós kódra a szabad távolság ≤ 5. Formálisan: $T(x) = G(x)I(x)$, $I(x) = 1$-re $T(x) = G(x)$ és így $w(T(x)) = w(G(x)) = 5$.

Megjegyzés A példában a kódsebesség $\frac{1}{2}$, mert 1 inputbithez 2 outputbitet rendel.

1/n sebességű kód $I_0(x)$ a bemenet és n darab kimeneti bitsorozatunk van: $T_0(x), \ldots, T_{n-1}(x)$. $T_i(x) = G_i(x)I_0(x)$. Az összefésült kimenet: $T(x) = \sum_{i=0}^{n-1} x^i G_i(x^n)$. $I(x) := I_0(x^n)$, $G(x) := \sum_{i=0}^{n-1} x^i G_i(x^n)$, $T(x) = G(x)I(x)$.

Definició Katasztrófális kódolás: valamely végtelen súlyú $I(x)$-re $T(x)$ véges súlyú.
Ez azért nagy gond, mert ha a kimeneten pont ezek a bitek romlanak el, akkor a csupa 0 kimenetet fogjuk látni, s ebből arra következtetünk, hogy a bemenet is csupa 0 volt $\rightarrow$ végtelen nagy dekodoló hiba.

Példa $G_0 := 1 + x^2$ $G_1 := 1 + x$ Ekkor a konvolúciós kódoló a csupa 1 bemenetre a következőt adja: $111000\ldots$. Ez katasztrófális kódolás, mert elég az első három helyen hibázni.

Tétel $(G_0, G_1, \ldots, G_{n-1}) = 1 \Longrightarrow$ a megfelelő kódolás nem katasztrófális.

$$\sum_{i=0}^{n-1} a_i(x^n)T_i(x^n) = \sum_{i=0}^{n-1} a_i(x^n)G_i(x_n)I_0(x^n) = \left(\sum_{i=0}^{n-1} a_i(x^n)G_i(x^n)\right) I_0(x^n) = I_0(x^n) = I(x)$$

Tehát a kimeneten kapott kódszó egyértelműen meghatározza a bemenetet, sőt, ha $T(x)$ véges súlyú lett, akkor $I(x)$ is véges súlyú volt (tehát a kódolás nem katasztrofális).

Állítás A példabeli kód szabad távolsága 5.

Bizonyítás Már kijött, hogy a szabad távolsága legfeljebb 5, most belátjuk, hogy legalább 5. $(G_0, G_1) = 1 \Longrightarrow I(x)$ véges súlyú, emiatt $I(x)$ polinom. Tekintsük a kódolóhoz tartozó véges automatát! A $[0,0]$ állapotból indulok, ebből az állapotból biztosan kilépek, mert $I(x) \not\equiv 0$. Mivel $I(x)$ véges súlyú, valamelyik bittől kezdve csupa 0-át kapok. Tehát a $[0,0]$ állapotba kell visszaérnem. Számoljuk össze, egy ilyen séta alatt hány 1-es jelenik meg a kimeneten! A $[0,0]$ állapot elhagyásakor kapok 2 darabot. A $[0,0]$-ba való utolsó lépés csak a $[0,1]$ állapotból történhet, ez pedig szintén 2 darab 1-es megjelenésével jár. Most már csak az a kérdés, hogy miként lehet eljutni $[1,0]$-ból $[0,1]$-be. A rövid úton menve 1 darab 1-es keletkezik; a hosszabbikon legalább 2. Összeadva, legkevesebb 5 darab 1-es keletkezik a kimeneten.

Megjegyzés Az automata állapotait és átmeneteit egy irányított gráf csúcsainak tekintve, ha az élekre a keletkező 1-esek számát írjuk, akkor az előbb ezen a gráfon kerestünk legrövidebb kört. Tudtuk, melyik állapotból indulunk, s hogy melyikbe érkezünk. Végtelen súlyú bemenetre mindenféle végtelen séták között kéne meghatároznunk a minimumot.

$\frac{k}{n}$ sebességű konvolúciós kódok: $I_0(x), \ldots, I_{k-1}(x)$ input, $T_0(x), \ldots, T_{n-1}(x)$ output sorozatok:

$$T_j(x) = \sum_{i=0}^{k-1} G_{ij}(x)I_i(x)$$

Most a kódot egy mátrix írja le: $G(x) = (G_{ij}(x))$ $i = 0, \ldots, k-1$ $j = 0, \ldots, n-1$

H legyen a $GF(2)[x]$ hatványsorok hányadosteste. Ebben formális Laurent-sorok vannak: $\sum_{i=s}^{\infty} a_i x^i$ $s \in \mathrm{Z}$

Egy lépésben k darab inputbitbol kapunk n darab outputbitet. Összességében k darab Laurent-sorból kapunk n darab Laurent-sort, azaz a kódoló elvileg tekinthető $H^k \mapsto H^n$ blokk-kódolónak.

$\frac{k}{n}$ sebességű konvolúviós kód k-dimenziós altere H^n-nek. Ennek van bázisa $GF(2)[x]^n$-ből - nevezetesen G sorai.

Az analógia a blokk-kódokkal azonban nem nagyon gyümölcsöző a konvolúciós kódok elemzése szempontjából.

Konvolúciós dekódolók: Alapötlet: Valamely rögzített $l > 0$ számra T első l bitjéből következtetünk I első bitjére (lehet benne hiba!), majd T-nek az elsőt követő l darab bitjéből I második bitjére, stb...

Viterbi-algoritmus: Maximum-likelihood alapú döntés. A döntéshez szükséges valószínűségeket a PERT-módszerhez hasonló dinamikus programozási eljárással számítjuk ki. Elvileg az üzenet első uk bitjének a meghatározásához 2^{uk} valószínűséget kéne nyilvántartani, azonban – a csatornamodellhez (hibaeloszláshoz) alkalmasan tervezett kódoló esetén – jó eséllyel minden lépésben elegendő csak 2^{vk} lehetőséggel dolgozni (és a további munkához megtartani), ahol v általában a kódoló memóriájának 2-3-szorosa. (A fenti sémában megfogalmazva lényegében $l \approx v\frac{n}{k}$.