Jadakoodid. Formalisatsioon

Algsed võrrandid

$$c_i^{(1)} = a_i + a_{i-2} \qquad c_i^{(2)} = a_i + a_{i-1} + a_{i-2}$$

Formaalsete ridadega antud võrrandid

$$c^{(1)}(x) = (1 + x^2)a(x)$$
$$c^{(2)}(x) = (1 + x + x^2)a(x)$$
$$a(x)(1 + x^2 \;\; 1 + x + x^2) = (c^{(1)}(x)\; c^{(2)}(x)) = C(x)$$

Fikseerime nüüd edaspidiseks ringi $\mathbb{F}_2[x]$.

Definitsioon 1

(n,k)-jadakoodiks mäluga M nimetatakse hulka $C \subseteq (\mathbb{F}_2[x])^n$, kus $k \leq n$ ja

$$C = \left\{ A(x)G(x) \mid A(x)^T \in (\mathbb{F}_2[x])^k \right\},$$

kus sisendite hulk $A(x)$ on järgmisel kujul $A(x) = (a^{(1)}(x) \;\; a^{(2)}(x) \ldots a^{(k)}(x))$ ja generaatormaatriks $G \in Mat_{k,n}(\mathbb{F}_2[x])$ iga elemendi aste $\deg g_{ij}(x) \leq M$ ning koodsõnadeks on reavektori $C(x) = A(x)G$ vastavate x astmete kordajatest $c_k^{(i)}$ moodustatud reavektoreid $(c_k^{(1)} \;\; c_k^{(2)} \ldots c_k^{(n)})$.

Jadakoodid. Omadused

Definitsioon 2

(n,k)-jadakoodi generaatormaatriksiga G nimetatakse pööratavaks, kui leidub polünomiaalsete elementidega maatriks H nii, et $GH^T = I_k$.

Teoreem 1 Generaatormaatriksi dekompositsioon

(n,k)-jadakoodi generaatormaatriks G on viidav kujule $G = U\Delta V$, kus U on $k \times k$, Δ on $k \times n$ ja V on $n \times n$ maatriksid. Kusjuures kõik maatriksite U,V ja Δ elemendid on polünoomid. Maatriks Δ on diagonaalsel kujul st. $\Delta_{i,i} = \delta_i$ ning $\Delta_{i,j} = 0$. Maatriksid U ja V on regulaarsed, kusjuures $\det U = \det V = 1$.

Märkus 1 : *Liikmeid δ_i nimetatakse generaatormaatriksi invariantseteks teguriteks.*

Märkus 2 : *Kehtib omadus $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_k$.*

Märkus 3 : *Kui γ_i on suurim ühistegur i-ndat jätku miinorite determinantidest, siis $\delta_i = \gamma_i / \gamma_{i-1}$.*

Järeldus 1.1 Koodi pööratavus

Kood on pööratav siis ja ainult siis, kui $\delta_1 = \delta_2 = \cdots = \delta_k = 1$.

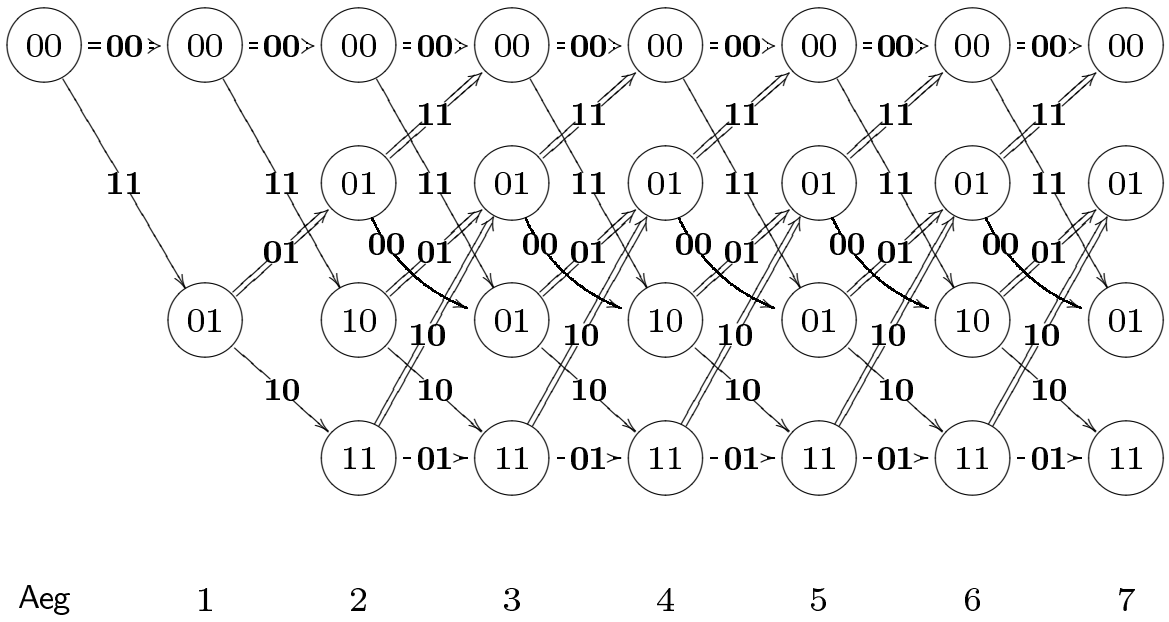
Jadakoodid. Võres

Definitsioon 3

Me ütleme, et (n,k)-jadakood on katastrofaalne, kui lõpmatu sisendjada(st. leidub lõpmata arv nullist erinevaid sisendbitte) kodeeritakse lõplikuks väljundjadaks.

Teoreem 2

(n,k)-jadakood on katastrofaalne parajasti siis, kui tegur $\gamma_k = \delta_1\delta_2\cdots\delta_k$ *pole* x *aste.*



Joonis 1: Eespool vaadatud (2,1)-jadakoodi võres

Jadakoodid. Kaugus

Definitsioon 4

Kahe (kood)sõna $u(x) = (u^{(1)}(x), u^{(2)}(x), \ldots, u^{(n)}(x))$ *ja* $v(x) = (v^{(1)}(x), v^{(2)}(x), \ldots, v^{(n)}(x))$ *vaheline (vaba)kaugus* $d(u, v)$ *on defineeritud*

$$d(u,v) = \left|\left\{(i,j) \mid u_j^{(i)} \neq v_j^{(i)},\ i = 1,2,\ldots,n\ j \in \mathbb{N}\right\}\right|.$$

Definitsioon 5

(n,k)-jadakoodi C *kaugus* d_{free} *on defineeritud*

$$d_{free} = \min\{d(u,v) \mid u, v \in C \text{ ja } u \neq v\}.$$

Märkus : *Jadakoodi lineaarsusest saame, et*

$$d_{free} = \min\{d(u,0) \mid u \in C \setminus \{0\}\}$$

Märkus : *Kui jadakood pole katastrofaalne, siis realiseerib kauguse* d_{free} *üks tee jadakoodi võreses, mis algab seisust 0 ja lõpeb seisus 0.*

Vitebi-dekodeerimisalgoritm

Lemma 1

Olgu $v(x)$ vastuvõetud sõnum, siis serva e kaal $w(e)$ jadakoodi võreses on servale e vastava väljundi Hammingi kaugus vastavast koodsõnast. Vastaku ajahetkele i võrese tipp s_i, siis vähima kaaluga tee p_{s_i} on leitav rekursiivselt ning

$$w(p_{s_i}) = \min_{s_{i-1}}\{w(p_{s_{i-1}}) + w(e), \text{ kus } e \text{ ühendab tippu } s_{i-1} \text{ ja } s_i\}.$$

Märkus : *Seda tähelepanekut kasutavat algoritmi nimetatakse Vitebi-dekodeerimisalgoritmiks algoritmiks. Algoritmi keerukus sõltub kahest asjast:*

- *koodri võimalikkude sisendseisude arvust, mis on 2^{Mk}, kus M koodri mälu ja k sisendkanalite arv;*
- *võrreldavate teede pikkusest l (mahuline keerukus).*

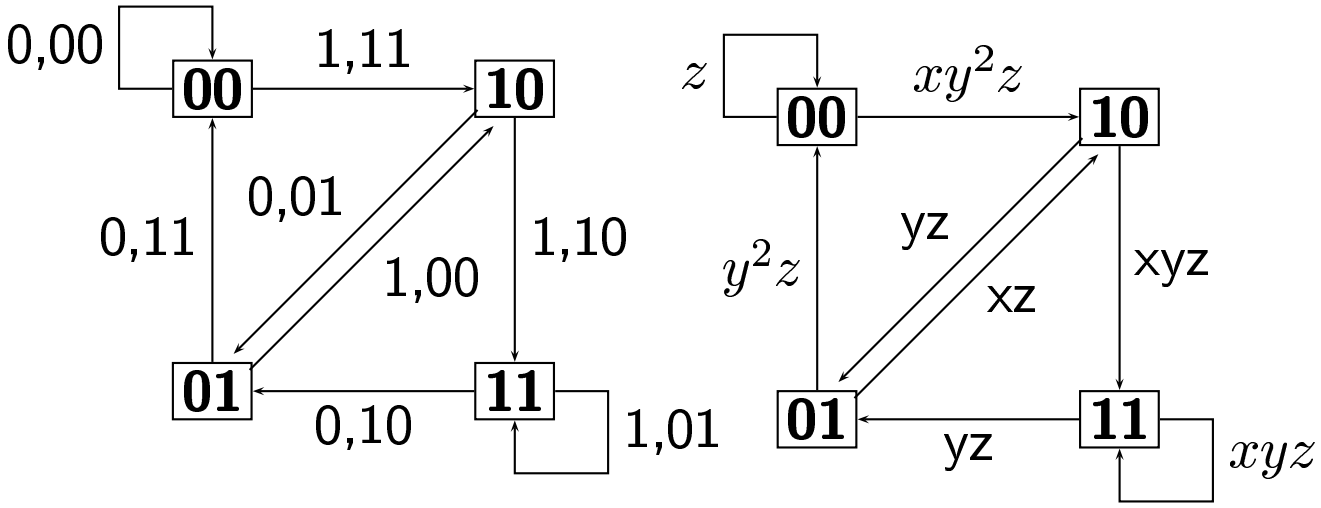
Üldiselt on ajaline keerukus $O(2^{(M+1)k})$ ning mahuline keerukus $O(2^{(M+1)l}l)$.

Vitebi-dekodeerimisalgoritm

Märkus : *Kui on tarvis dekodeerida vaid osa sisendkanalitest, siis võib keerukus oluliselt langeda.*

Märkus : *Kui vaadelda binaarse sümmetrilise kanali asemel Gaussi kanalit, siis algoritm ei muutu oluliselt. Ainus erinevus on selles, et servade kaal arvutatakse vastavalt* $\|\cdot\|_2$ *suhtes.*

Võrese teede loend



Joonis 2: Jadakoodri seisundite graaf

Teeme nüüd anname igale servale $(m, c^{(1)}c^{(2)})$ kaalu $x^m y^{c^{(1)}+c^{(2)}} z$, mis lubab taastada sisendi kaalu, väljundi kaalu ning teepikkuse(z aste). Seega on suvalisele teele $\mathcal{P}$ seisundigraafis anda kaal $w(\mathcal{P})$ kui servade kaalu korrutis.

Definitsioon 6

Seisundi graafi fundamentaalteeks ninetatakse positiivse pikkusega teed, mis algab seisust s ja lõpeb seisus 0, ilma et oleks vahepeal läbinud seisu 0. Viimane tingimus tähendab ühtlasi ka seda, et tee $0 \to 0$ pole fundamentaalne.

Võrese teede loend

Definitsioon 7

Fundamentaalteede loendiks $A_s(x, y, z)$, mis vastab koodri seisule s nimetatakse järgmist summat

$$A_s(x, y, z) = \sum_{\mathcal{P} \text{ on fundamentaaltee } s \to 0} w(\mathcal{P}) \qquad (1)$$

Meie (2,1)-jadakoodi korral saame lihtsad seosed

$$\begin{aligned}
A_{00}(x, y, z) &= xy^2zA_{10}(x, y, z) \\
A_{01}(x, y, z) &= y^2z + xzA_{10}(x, y, z) \\
A_{10}(x, y, z) &= yzA_{01}(x, y, z) + xyzA_{11}(xyz) \\
A_{11}(x, y, z) &= yzA_{01}(x, y, z) + xyzA_{11}(x, y, z)
\end{aligned}$$

Siit saab LVS lahendada ning saame

$$A_{00}(x, y, z) = \frac{xy^5z^3}{1 - xyz(1 + z)} = xy^5z^3(1+xyz(1+z)+\cdots)$$

Esimese vea tõenäosus

Olgu $Pr^e(\mathcal{P}, 0)$ tõenäosus, et nullidele vastav sisend dekodeeritakse teele $\mathcal{P}$ vastavaks sisendiks. Siis esimese vea tõenäosus on ülalt hinnatav

$$P \leq \sum_{\mathcal{P} \text{ on fundamentaalne tee algusega } 0} Pr^e(\mathcal{P}, 0)$$

Et

$$Pr^e(\mathcal{P}, 0) = \sum_{k \geq \lceil w/2 \rceil} \binom{w}{k} p^k (1-p)^{w-k}$$

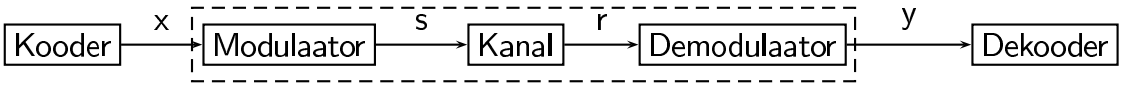
$$Pr^e(\mathcal{P}, 0) \leq (2\sqrt{p(1-p)})^w$$

Teoreem 3

Dekoodri esimese vea tõenäosus Pr_1 on hinnatav jadakoodi fundamentaalteede loendi abil

$$Pr_1 \leq A_0(1, 2\sqrt{p(1-p)}, 1)$$

Reaalsed kanalid ning modulatsiooni parandamine



Joonis 3: Reaalne sidekanal

Kui kasutada koos signaali moduleerimist ja kodeerimist võib saada parema tulemuse. Tõenäosusjaotus Gaussi kanalis annab

$$Pr(r \mid s) = \frac{1}{\sqrt{2\pi}} e^{-|r-s|^2/2\sigma^2},$$

mis tähendab, et mida suurem on $|r-s|^2$ kaugus, seda tõenäolisemalt eristatakse lained s ja r. Kasutades jadakoodrit võib vähendades korraga saadetava info mahtu vähendada kanali müra, kusjuures saadakse parem tulemus kui lihtsal infomahu vähendamisel.