

Sąsūkų kodai

2010

Tiesiniai registrai ir daugianarių daugyba	2
Daugyba naudojantis registrų sistema	3
Daugyba naudojantis registrais	4
Patobulinta sistema	5
Kaip supinti du srautus į vieną?	6
Sisteminis kodavimas	7
Sąsūkų kodas	8
Dar vienas pavyzdys	9
Sąsūkų kodo vaizdavimas būsenų diagrama	10
Grotelių diagrama	11
Keliai būsenų diagramoje	12
Kodavimas	13
Srauto iškraipymai	14
Viterbi algoritmas	15
Viterbi algoritmas	16

Tiesiniai registrai ir daugianarių daugyba

Generatorius

$$g(x) = 1 + x + x^2,$$

daugianaris iš informacinių bitų:

$$u(x) = u_0 + u_1x + u_2x^2 + \dots + u_nx^n, \quad u_i \in \mathbb{F}_2.$$

Jų sandauga yra daugianaris $v(x) = v_0 + v_1x + \dots + v_nx^n + v_{n+1}x^{n+1} + v_{n+2}x^{n+2}$.

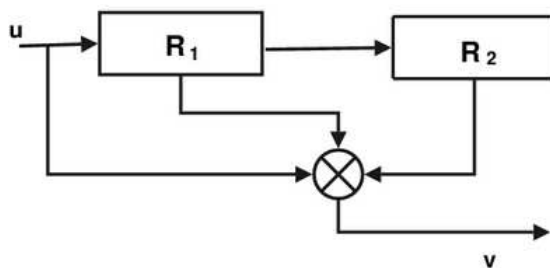
Koeficientai randami taip:

$$v_k = u_k + u_{k-1} + u_{k-2}, \quad k = 2, 3, \dots, n.$$

Kad ši lygybė tiktų ir $v_0, v_1, v_{n+1}, v_{n+2}$ reikia susitarti, kad $u_{-2} = u_{-1} = u_{n+1} = u_{n+2} = 0$. $v(x)$ koeficientai gaunami „susukant“ į vieną tris $u(x)$ koeficientus.

2 / 16

Daugyba naudojantis registų sistema



Visus daugianario $v(x)$ koeficientus generuos šis paprastas įrenginys, jeigu į jį įvesime $u_0u_1 \dots u_n00$. Taigi šis paprastas tiesinių registų įrenginys atlieka daugianarių daugybą!

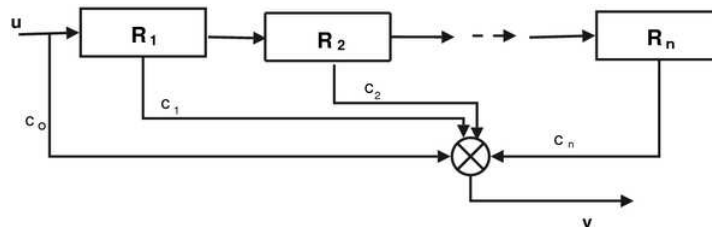
3 / 16

Daugyba naudojantis registras

Kaip sukonstruoti tiesinių registrų sistemą, kuri daugianarius daugintų iš

$$g(x) = c_0 + c_1x + \dots + c_nx^n, \quad c_n \neq 0?$$

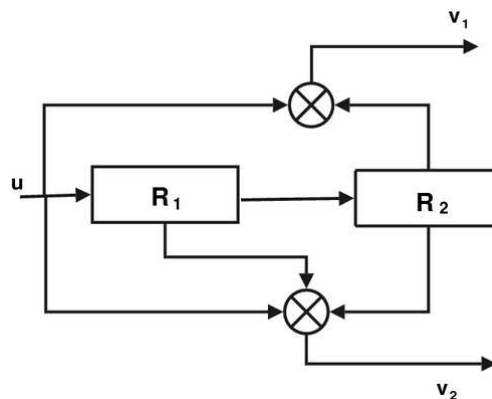
Sprendimas paprastas:



Kiekvienam įvesties bitui u_i sukuriamas išvesties bitas v_i .

4 / 16

Patobulinta sistema



Dabar įvesties bitų žodžiui u sistema sukuria du išvesties žodžius v_1 ir v_2 , t.y. kiekvienam įvesties daugianariui $u(x)$ sukuriami du daugianariai:

$$\begin{aligned} v_1(x) &= u(x)g_1(x), & g_1(x) &= 1 + x^2 \\ v_2(x) &= u(x)g_2(x), & g_2(x) &= 1 + x + x^2. \end{aligned}$$

5 / 16

Kaip supinti du srautus į vieną?

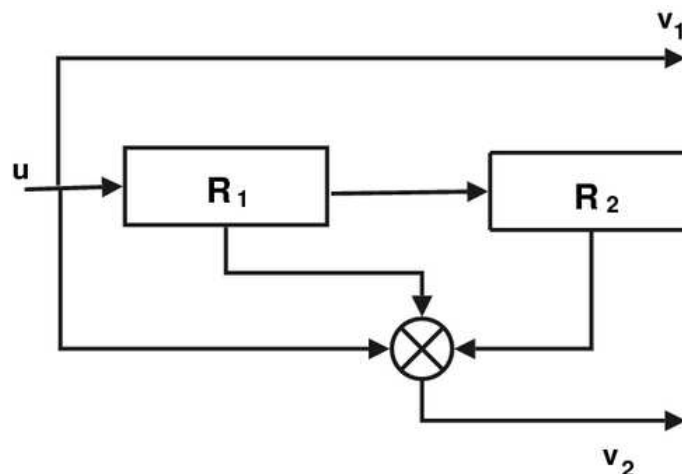
Norėtume „supinti“ abu išvesties srautus į vieną, pavyzdžiui, padaryti taip, kad kiekvieną srauto v_1 bitą sektų atitinkamas v_2 bitas.

Tokį supintą srautą galima užrašyti daugianariu, kurio koeficientai prie lyginių laipsnių yra skolinti iš $v_1(x)$, o prie nelyginių – iš $v_2(x)$. Tokį daugianarį paprasta sudaryti:

$$\begin{aligned}v(x) &= v_1(x^2) + xv_2(x^2) = u(x^2)(g_1(x^2) + xg_2(x^2)) \\v(x) &= u(x^2)(1 + x + x^3 + x^4 + x^5).\end{aligned}$$

6 / 16

Sisteminis kodavimas



Šios schemos sukurtas srautas v_1 – tiesiog įvesties srauto kopija. Šitaip koduojant į duomenų srautą tiesiog įterpiami simboliai, reikalingi klaidoms taisyti.

7 / 16

Sąsūkų kodas

$$u(x) \mapsto \langle v_1(x), v_2(x) \rangle, \text{ arba } u(x) \mapsto v(x),$$

čia

$$v_1(x) = u(x)g_1(x), \quad g_1(x) = 1 + x^2$$

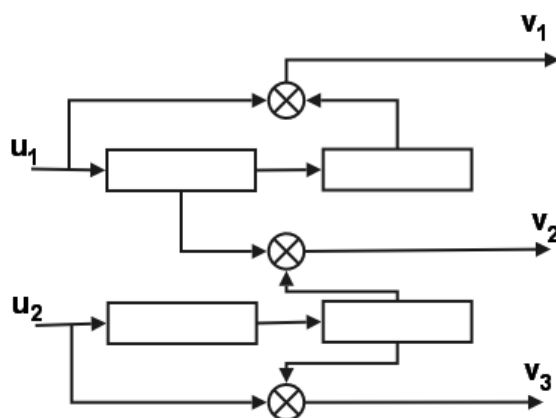
$$v_2(x) = u(x)g_2(x), \quad g_2(x) = 1 + x + x^2$$

$$v(x) = u(x^2)g(x), \quad g(x) = 1 + x + x^3 + x^4 + x^5.$$

Registų sistema (arba daugianarių atitikties) apibrėžia sąsūkų kodą su parametrais $(k, m, n) = (1, 2, 2)$. k – viename žingsnyje į sistemą įvedamų bitų skaičius, m – sistemos registų skaičius, n – viename žingsnyje išvedamų bitų skaičius. Santykį k/n vadinsime sąsūkų kodo koeficientu. Taigi mūsų sistema apibrėžia sąsūkų kodą su koeficientu $1/2$.

8 / 16

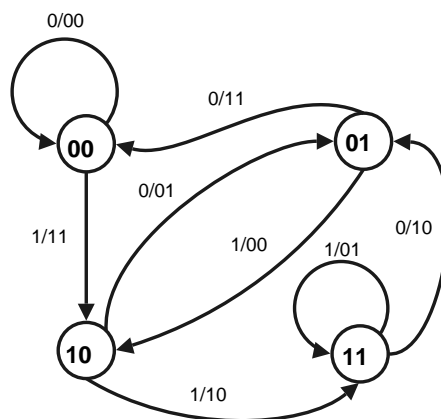
Dar vienas pavyzdys



Į brėžinyje pavaizduotą registų sistemą kiekviename žingsnyje paduodami du bitai, o išvedami trys. Taigi tokio kodo koeficientas yra $2/3$.

9 / 16

Sąsūkų kodo vaizdavimas būsenų diagrama

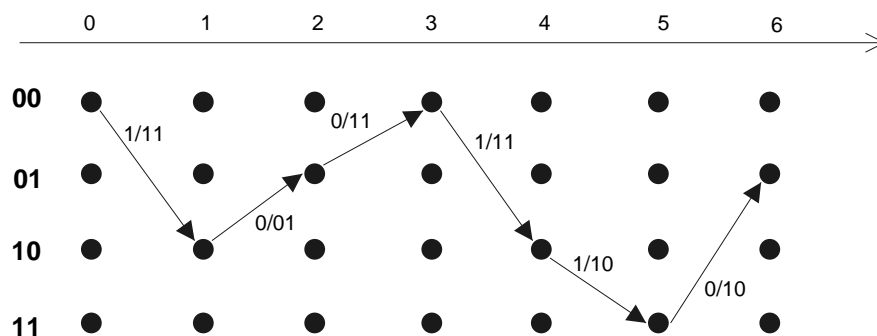


Koduojant pagal pateiktą diagramą

$$u = 10011010 \dots \mapsto 1101001110100001 \dots = v.$$

10 / 16

Grotelių diagrama



Jeigu briauna veda į viršų – įvesties bitas lygus nuliui. Jeigu žemyn – vienetas. Yra du atvejai, kai briaunos lygiagrečios laiko ašiai: kai iš 00 grįžtama į 00 ir iš 11 į 11. Pirmuoju atveju įvesties bitas nulis, antruoju – vienetas.

11 / 16

Keliai būsenų diagramoje

Kiekvienas kodavimo eigą atitinkantis kelias prasideda nuo nulinės būsenos. Mūsų pavyzdyje yra iš viso $4 \times 4 \times \dots \times 4 = 4^m$ kelių, vedančių iš pradinės būsenos į kurią nors m -ojo žingsnio būseną. Tačiau ne visi keliai atitinka kokių nors srautų kodavimo eigą. „Tikrų“ kodavimo kelių yra tik 2^m .

12 / 16

Kodavimas

Tarkime, kodavimui naudojamas tas sąsukų kodas, kurį nagrinėjome anksčiau.

Bus koduojama po r srauto bitų, po to dar bus įvedami du nuliniai bitai, kad sistema sugrįžtų į būseną 00. Taigi iš tiesų į sistemą bus įvedami žodžiai $u_0 u_1 \dots u_{r-1} 00$.

Po $r + 2$ žingsnių sistema sugrįš į pradinę padėtį ir vėl bus koduojama iš naujo.

Jeigu sistemoje būtų s atminties registrai, tada prie koduojamo bloko reiktų pridėti iš viso s nulių.

13 / 16

Srauto iškraipymai

Kiekvieną žodį $u_0 u_1 \dots u_{r-1} 00$ grotelių diagramoje atitinka kelias iš būsenos 00 į 00. Tokių kodavimo kelių yra 2^r . Į kanalą perduodamas $2(r + 2)$ ilgio žodis

$$\mathbf{v} = v_0^{(1)} v_0^{(2)} v_1^{(1)} v_1^{(2)} \dots v_{r+1}^{(1)} v_{r+1}^{(2)}.$$

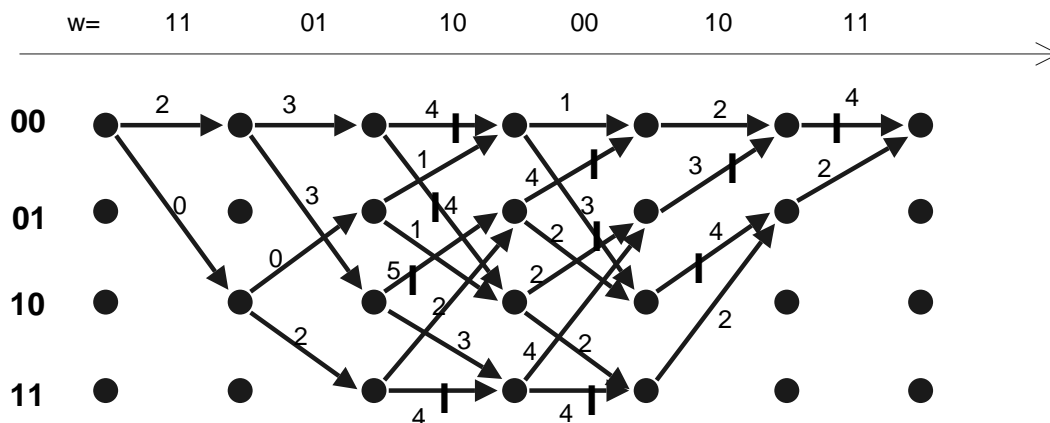
Kanalas yra simetrinis ir be atminties. Tada jis su vienodomis tikimybėmis iškraipo perduodamus simbolius ir gavėjas vietoje srauto \mathbf{v} gaus iškraipytą srautą

$$\mathbf{w} = w_0^{(1)} w_0^{(2)} w_1^{(1)} w_1^{(2)} \dots w_{r+1}^{(1)} w_{r+1}^{(2)}.$$

14 / 16

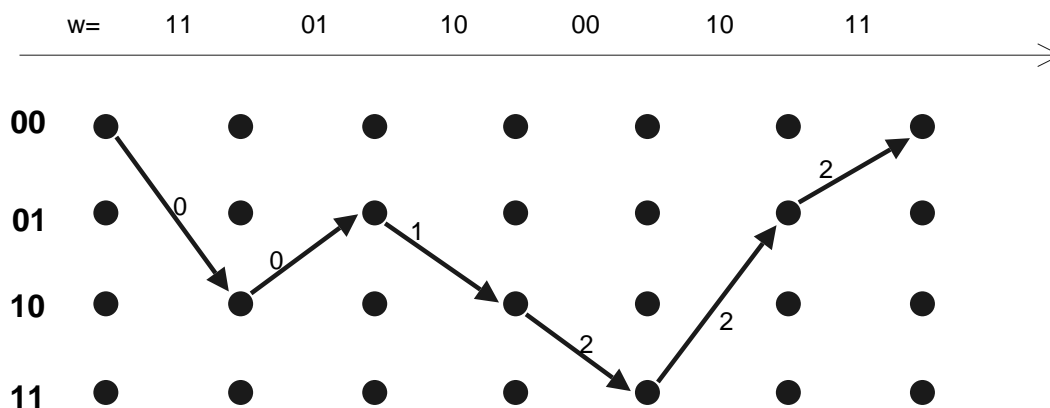
Viterbi algoritmas

Tarkime, iš kanalo gautas toks bitų srautas $w = 11\ 01\ 10\ 00\ 10\ 11$.
Ieškosime, kuris iš galimų srautų mažiausiai skiriasi nuo gautojo.



15 / 16

Viterbi algoritmas



O prisiminę, kad kryptis žemyn reiškia, kad buvo įvestas 1, aukštyn – 0, galime iškart atkurti ir pradinį, į sistemą įvestą žodį: $v = 101100$.

16 / 16