U N I V E R Z I T E T U B E O G R A D U

PRIRODNO-MATEMATIČKI FAKULTET

Ranko L. Šćepanović

O LINEARNOJ SLOŽENOSTI RASPOZNAVANJA NEKIH KLASA OBLIKA

— doktorska disertacija —

Beograd, 1985. god.

Број: _____

Датум: _____

SADRŽAJ

U V O D

Teorija složenosti je dio matematičke kibernetike tijesno povezan s problemom sinteze upravljačkih sistema. Interesovanje za nju raste sa sve većom primjenom elektronskih računskih mašina. Za mnoge zadatke važne u praksi još nijesu nadjeni realno ostvarljivi algoritmi. Postoje li za dati zadatak brzi algoritmi ili on ima urodjenu složenost - to je osnovno pitanje teorije složenosti.

Kod izučavanja složenosti važno je izabrati pogodan jezik na kojem će se opisivati algoritmi. Postojeći programski jezici su pogodni pri razradi gotovih algoritama, dok su veoma nepogodni pri dokazivanju nepostojanja (ekonomičnih) algoritama. Zato se teorija složenosti i bavi prostim modelima algoritama koji olakšavaju njihovu analizu. Takvi modeli su, na primjer, disjunktivne normalne forme, Boole-ove formule, sheme od funkcionalnih elemenata, automati, Turing-ove mašine i tome slično.

Funkcionisanje blokova elektronskih računskih mašina i drugih uredjaja koji obradjuju diskretne informacije, opisuje se Boole-ovim funkcijama. Isto tako možemo reći da svaki program savremenih računara izračunava vrijednosti sistema Boole-ovih funkcija. Zato su još 30-ih godina ovog vijeka inženjeri počeli da izučavaju Boole-ove modele, tj. modele koji izračunavaju vrijednosti Boole-ovih funkcija (u daljem tekstu govorićemo prosto da izračunavaju Boole-ove funkcije). Tu spadaju Boole-ove formule, kontaktne sheme, sheme od funkcionalnih elemenata, logičke mreže itd. Boole-ovi modeli su krajnje prosti što olakšava njihov opis i dozvoljava, za razliku od složenijih modela, precizne formula-

cije problema teorije složenosti. Zbog toga je teorija složenosti Boole-ovih modela i najrazvijeniji dio teorije složenosti. Većina osnovnih rezultata teorije složenosti može se izložiti na jeziku Boole-ovih modela, što im daje osobit značaj u toj teoriji.

Za sve nabrojane modele možemo reći da su to objekti konstruisani po odredjenim sintaksičkim pravilima i služe za izračunavanje funkcija. Takve objekte nazovimo shemama. Uredjen par (S,f), gdje je S shema a f funkcija koju ona izračunava (realizuje), nazvaćemo upravljačkim sistemom(strogu definiciju upravljačkog sistema i osnovne zadatke teorije upravljačkih sistema dao je S.V.Jablonski u [4]). Na taj način, sa svakim skupom upravljačkih sistema se, na prirodan način, vezuje skup $\mathcal{Y}$ njihovih shema i skup $\mathcal{F}$ njihovih funkcija. Jedan od osnovnih zadataka teorije upravljačkih sistema je zadatak sinteze: za datu funkciju $f \in \mathcal{F}$ naći shemu $S \in \mathcal{Y}$ koja je realizuje. Ovaj zadatak, kao po pravilu, nema jedinstveno rješenje. Zato se on dalje precizira.

Za većinu zadataka nije važno samo sastaviti program ili izvršiti neku konstrukciju, nego i uraditi to što je moguće ekonomičnije. Pojam ekonomičnosti se može odrediti uvodjenjem raznih mjera složenosti (zavisno od problema koji se rješava).

Tako na primjer, pri rješavanju problema ekonomične konstrukcije pojedinih blokova elektronskih računskih mašina, prirodno se nameću, kao mjere složenosti, broj elemenata u shemi, broj simbola promjenljivih u formuli, broj kontakta u kontaktnoj shemi, broj konjunkcija u disjunktivnoj normalnoj formi i tome slično. Razumna mjera složenosti bi bila i dubina sheme, tj. maksimalna dužina puta koji predje signal od ulaza do izlaza iz she-

me. Ima interesa izučavati i broj elemenata sheme koji se istovremeno nadju u aktivnom stanju u toku izračunavanja.

Pri teorijskom izučavanju brzine izvršavanja programa, prirodna mjera složenosti bi bio broj elementarnih koraka iz kojih se sastoji algoritam, npr. Turing-ova mašina. Druge mjere složenosti bi bile dužina programa (npr. broj komandi), veličina memorije koju koristi program (radna memorija), vrijeme izračunavanja pri paralelnim izračunavanjima i tome slično.

Raznorodne mjere složenosti nijesu medjusobno nezavisne. Tako na primjer, očigledno je postojanje veze izmedju vremena izvršavanja programa i potrebne radne memorije, izmedju broja elemenata u shemi i njene dubine itd. Manje očigledna, no dokazana je tijesna veza izmedju vremena i veličine memorije potrebne za izvršavanje programa,s jedne strane i broja elemenata u shemi od funkcionalnih elemenata s druge strane (vidi [33], [34], [35]). Poslednja veza ima principijelan značaj, jer govori da su sheme,od funkcionalnih elemenata pogodne za izučavanje kako prostornih (shemnih), tako i programskih (računskih, mašinskih) mjera složenosti.

Uvodjenjem mjere složenosti, tj. funkcionala L(S) na skupu shema S iz date klase upravljačkih sistema, zadatak sinteze se precizira: za datu funkciju $f \in \mathcal{F}$ naći shemu $S \in \mathcal{S}$ koja je realizuje, takvu da je L(S) minimalno ("minimalnu shemu"). Tu minimalnu vrijednost ćemo označiti sa L(f).

Osnovna poteškoća koja ostavlja trag na svu problematiku teorije složenosti je praktična nerješivost zadatka konstrukcije minimalnih shema. Tu se ne radi o algoritamskoj nerješivosti, jer postoji trivijalni algoritam konstrukcije mini-

malnih shema zasnovan na pretraživanju svih shema odredjene složenosti. Medjutim, primjena tog algoritma je praktično nemoguća čak i za mali broj promjenljivih (n=6,7), zbog astronomskog vremena potrebnog za njegovo izvršavanje. Čak ni primjena najbržih računara skoro da ne povećava mogućnosti algoritma. Svi pokušaji da se nadju efektivniji algoritmi zasad nijesu dali rezultat . S.V.Jablonski je izrazio hipotezu (i dobio prve rezultate koji je opravdavaju; detaljnije o tome vidi u [7]) da je trivijalni algoritam "potpunog pretraživanja" u tim zadacima neophodan [5]. Zbog toga se zadatak sinteze mora dalje precizirati. Postoji nekoliko prilaza.

Jedan od takvih prilaza je asimptotski i pripada C.Shannon-u [1], [2]. Uslov minimalnosti se zamjenjuje uslovom "skoro minimalnosti": traži se shema čija je složenost asimptotski jednaka minimalnoj shemi. Osim toga, razmatra se zadatak sinteze za cijelu klasu funkcija (npr. za klasu $\mathcal{P}_2^n$ Boole-ovih funkcija od n promjenljivih). Tačnija postavka zadatka bi se sastojala u sledećem. Neka je $L(n)=\max L(f)$, gdje se maksimum uzima po svim funkcijama $f(x_1,\ldots,x_n)$ iz $\mathcal{P}_2^n$. Funkcija L(n) je dobila naziv Shannon-ova funkcija. Treba naći algoritam po kojem se za svaku funkciju $f(x_1,\ldots,x_n)$ konstruiše shema S koja realizuje tu funkciju, takva da je $L(S) \leqslant L(n)$.

Prve rezultate u tom pravcu je dobio C.Shannon [1], [2]. On je dao algoritam sinteze kontaktnih shema reda optimalnog algoritma (tj. optimalan s tačnošću do multiplikativne konstante) i dobio ocjene:

$$\frac{2^n}{n} \leqslant L(n) \leqslant \frac{2^{n+2}}{n} .$$

Asimptotski najbolji algoritam je konstruisao O.B.Lupanov i time je dobijena asimptotika Shannon-ove funkcije [10], [13]:

$$L(n)\sim\frac{2^n}{n}\ .$$

O.B.Lupanov je takodje dao asimptotski najbolje algoritme sinteze formula i shema od funkcionalnih elemenata u proizvoljnoj konačnoj bazi [11], [12]. Asimptotike Shannon-ovih funkcija u tim slučajevima su

$$L(n)\sim\rho\frac{2^n}{\log n}\quad\text{i}\quad L(n)\sim\rho\frac{2^n}{n}\ ,$$

gdje je ρ - konstanta koja se lako odredjuje za datu bazu.

Na osnovu tih metoda kasnije su se pojavili analogni asimptotski rezultati i za druge klase upravljačkih sistema. Izmedju njih izdvojimo rad V.A.Kuzmina [21] u kojem je dobijena asimptotika Shannon-ove funkcije za složenost realizacije Booleovih funkcija normalnim algoritmima i Turing-ovim mašinama i pokazana zavisnost te asimptotike od broja slova korišćene azbuke.

Rezultati asimptotske teorije pokazuju da ponašanje Shannon-ove funkcije slabo zavisi od klase upravljačkih sistema. Osim toga, oni govore i da skoro sve funkcije iz $\mathcal{P}_2^n$ imaju skoro jednaku složenost, asimptotski jednaku složenosti najsloženije funkcije i zato su praktično nedostupne. Ova pojava nosi naziv efekat Shannon-a. Zbog toga je važno izdvojiti klase funkcija koje mogu biti realizovane prostije od većine funkcija i naći metode sinteze shema za njih. Primjeri takvih klasa su poznati još iz perioda prvih radova iz sinteze. Zatim je S.V.Jablonski [5], [6] konstruisao i izučio neprekidnu familiju klasa funkcija zatvorenih u odnosu na smjene konstanti i permutacije promjen-

ljivih. Svaku takvu klasu karakteriše neki brojni parametar σ koji odražava broj elemenata klase ($0 \leqslant \sigma \leqslant 1$). Za klase kod kojih je $\sigma \neq 0$, S.V.Jablonski je konstruisao asimptotski najbolje metode sinteze i dobio asimptotike Shannon-ovih funkcija.

Poslije toga, O.B.Lupanov je predložio jedan opšti pristup sintezi shema - princip lokalnog kodiranja [14]. On omogućuje da se po opisu klase funkcija (pridržavajući se nekih specijalnih uslova) konstruiše asimptotski najbolji metod sinteze shema za funkcije posmatrane klase. Korišćenjem tog principa pokazalo se mogućim,na jedan jedini način, dobiti metode sinteze shema za poznate klase funkcija, a takodje i metode sinteze za mnoge nove klase funkcija. Asimptotika složenosti shema za funkcije iz tih klasa odredjena je brojem M_n funkcija $f(x_1,\ldots,x_n)$ u klasi i ima oblik

$$\varphi \frac{\log M_n}{\log \log M_n} .$$

Ova funkcija može uzimati vrijednosti od veličina bliskih n, do $2^n/n$. Princip lokalnog kodiranja je naročito pogodan za primjenu na dovoljno bogatim klasama upravljačkih sistema (sheme od funkcionalnih elemenata, automati, algoritmi).

Kao što je već rečeno,većina Boole-ovih funkcija ima vrlo veliku složenost shemne realizacije. Dokaz te činjenice nije efektivan: proizilazi iz odnosa broja elemenata skupa svih Boole-ovih funkcija i broja elemenata skupa shema (iz date klase upravljačkih sistema) odredjene složenosti. Prvu "efektivnu" nelinearnu donju ocjenu dobila je B.A.Subotovskaja za složenost realizacije linearne funkcije od n promjenljivih formulama nad bazom $\{\&,\vee,-\}$ [16]. Ta ocjena ima oblik $C \cdot n^{3/2}$. V.M. Hrapčenko je povisio tu

cjenu do n^2 i time je ustanovljen red složenosti linearne funkcije u klasi formula [17]. On je predložio i jedan opšti metod obijanja kvadratnih donjih ocjena složenosti formula u bazi &, V, -}. Donje ocjene bliske kvadratnim u "jačim" klasama upravljačkih sistema (formule nad proizvoljnom bazom, kontaktne sheme) obio je E.I. Nečiporuk [18]. U "slabijim" klasama upravljačkih istema (formule i sheme od funkcionalnih elemenata nad funkcionalno nekompletnim bazama) dobijene su donje ocjene reda n^c, dje je c proizvoljna konstanta [19], [20], [39].

Do danas nije dobijena nijedna nelinearna donja ocjena loženosti Boole-ovih funkcija u klasi shema od funkcionalnih lemenata nad kompletnom bazom. S obzirom na eksponencijalnu loženost većine Boole-ovih funkcija, problem povišenja donjih cjena složenosti predstavlja snažan stimulans razvitku teorije loženosti.

Predmet ove disertacije, s aspekta teorije složenosti, ripada navedenom problemu izdvajanja klasa Boole-ovih funkcija oje mogu biti realizovane prostije nego većina funkcija. Konretno, ovdje su opisane neke klase Boole-ovih funkcija i za njih okazana linearna složenost realizacije, tj. najmanja moguća.

S druge strane, te Boole-ove funkcije linearne složenoti su veoma značajne jer modeliraju mnoge situacije koje se poavljuju u praksi. Posmatra se binarni ekran dimenzije m x n i kup O stanja ekrana (tj. skup Boole-ovih matrica tipa m x n) oja nastaju pomjeranjem nadesno ravne figure prikazane na ekrau kada se on nalazi u stanju $M=\|\alpha_{ij}\|_m^n$. Skup O smo nazvali $D_{m,n}^M$ oblikom. Definisali smo Boole-ovu funkciju $f_o(x_1,\ldots,x_{m\cdot n})$ d $m\cdot n$ promjenljivih tako da je $f_o(\alpha_1,\ldots,\alpha_{m\,.\,n})=1$ akko niz

$\alpha_1,\ldots,\alpha_{mn}$ obrazuju vrste neke matrice $M' \in O$, poredjane slijeva nadesno jedna do druge. Posmatra se realizacija Boole-ovih funkcija shemama od funkcionalnih elemenata i kaže se da shema S raspoznaje oblik O ako ona realizuje funkciju f_0 .Složenost realizacije funkcije f_0 nazvali smo složenošću raspoznavanja oblika O . Složenošću raspoznavanja klase oblika nazvali smo maksimalnu od složenosti raspoznavanja oblika iz te klase. U disertaciji su opisane neke klase $PD^M_{m,n}$ oblika i za njih dokazana linearna složenost raspoznavanja. Pri nekom ograničenju na dimenzije ekrana m i n dokazana je linearna složenost raspoznavanja svih $PD^M_{m,n}$ oblika.

U I glavi disertacije data je precizna formulacija problema, definisan je pojam shema od funkcionalnih elemenata i navedeni su osnovni poznati rezultati složenosti realizacije Boolevih funkcija shemama od funkcionalnih elemenata, na koje smo se kasnije,nekoliko puta, pozivali. Na kraju glave je data nelinearna gornja ocjena složenosti raspoznavanja klase svih $PD^M_{m,n}$ oblika.

U II glavi disertacije, pri ograničenju $n \leqslant C \cdot \log m$ na dimenzije ekrana, dokazana je linearna složenost raspoznavanja klase svih $PD^M_{m,n}$ oblika. Dat je univerzalan (za sve $PD^M_{m,n}$ oblike), reda optimalnog, metod sinteze shema od funkcionalnih elemenata za raspoznavanje $PD^M_{m,n}$ oblika.

III glava disertacije, u slučaju kada je $n \gg \log m$, pokazuje svu ozbiljnost i težinu postavljenog problema. S jedne strane, metod iz druge glave daje nelinearnu gornju ocjenu složenosti. S druge strane, broj elemenata skupa svih $PD^M_{m,n}$ oblika nije dovoljan za primjenu bilo kog poznatog rezultata asimptotske

teorije složenosti, pa i principa lokalnog kodiranja O.B.Lupanova, primjenom kojeg su, kao što smo već rekli, konstruisani asimptotski najbolji metodi sinteze shema za sve poznate klase Boole-ovih funkcija. Osim toga, na putu nalaženja univerzalnog metoda sinteze shema za raspoznavanje $PD^M_{m,n}$ oblika, prirodno se pojavljuje operator pomjeranja T_n, koji pomjera nadesno proizvoljan niz dužine n za proizvoljan broj mjesta. O.B. Lupanov je u [14] dao nelinearnu gornju ocjenu složenosti realizacije operatora T_n, $L(T_n) \leqslant C \cdot n \cdot \log n$, i izrekao hipotezu da je operator T_n nelinearan. Zbog principijelnih teškoća oko povećanja donjih ocjena, koje smo već pomenuli, ta hipoteza do danas nije dokazana. Isto tako, nikome nije pošlo za rukom da pronadje metod bolji od metoda O.B.Lupanova i snizi gore navedenu nelinearnu ocjenu.

Sve to govori da, u slučaju $n \gg \log m$, treba odustati od traženja univerzalnog metoda sinteze shema od funkcionalnih elemenata koji bi dao linearnu složenost raspoznavanja klase svih $PD^M_{m,n}$ oblika. Treba ići putem izdvajanja podklasa klase svih $PD^M_{m,n}$ oblika i za njih naći metode sinteze shema linearne složenosti.

Na taj način, od operatora pomjeranja O.B.Lupanova prirodno dolazimo do klase operatora T^{α}_n, $\alpha=(\alpha_0,\ldots,\alpha_{n-1})$, $\alpha_i \in \{0,1\}$, $i=0,\ldots,n-1$, svaki od kojih pomjera nadesno fiksirani niz za proizvoljan broj mjesta. Tako sebi otvaramo put da izdvajanjem podskupova skupa svih nizova α dužine n iskoristimo svojstva nizova iz tih podskupova i konstruišemo metode sinteze shema koji bi snizili, u prvom redu nelinearnu ocjenu složenosti O.B. Lupanova operatora pomjeranja T^{α}_n odredjenih nizovima sa tim svojstvi-

ma, a zatim i nelinearnu ocjenu složenosti raspoznavanja odgovarajućih klasa $PD^{M}_{m,n}$ oblika. U III glavi disertacije su upravo opisani podskupovi skupa svih nizova, a time i klase $PD^{M}_{m,n}$ oblika i za njih dati metodi koji snižavaju pomenute nelinearne ocjene složenosti do linearnih, tj. do najmanjih mogućih. Na taj način, svi ti opisani metodi su reda optimalnih.

Time problem složenosti raspoznavanja $PD^{M}_{m,n}$ oblika, u slučaju $n \gg \log m$, nije u potpunosti zatvoren. Opisanim metodima i izloženom tehnikom su izdvojeni $PD^{M}_{m,n}$ oblici linearne složenosti raspoznavanja kao i operatori pomjeranja T^{α}_{n} linearne složenosti realizacije shemama od funkcionalnih elemenata. Ostala je klasa oblika, odnosno operatora pomjeranja T^{α}_{n}, nad kojom stoji sjenka nelinearnosti, no dokaz te činjenice zahtijeva nove prodore teorije. Stanje stvari u teoriji složenosti je takvo, da kod mnogih matematičara koji se bave ovim problemima raste pesimizam da se u bliskoj budućnosti neće dobiti nelinearna donja ocjena složenosti realizacije individualne Boole-ove funkcije shemama od funkcionalnih elemenata nad kompletnom bazom.

Većina rezultata navedenih u disertaciji je sadržana u [37], [38], [39] i [40].

Glava I. OSNOVNI POJMOVI I FORMULACIJA PROBLEMA

1.1. Definicija $K_{m,n}$ oblika

Posmatrajmo rešetku R=N x N u ravni, tj. skup tačaka sa koordinatama (i,j), gdje su $i,j \in N$ (N - skup prirodnih brojeva). Ekranom $E_{m,n}$ tipa m x n, $m,n \in N$, nazvaćemo sledeći podskup rešetke R: $E_{m,n}=\{(i,j) \mid i \leqslant m, j \leqslant n\}$. Smatraćemo da svaka tačka (i,j) ekrana $E_{m,n}$ može da se nadje u jednom od dva stanja: 0 ili 1. Stanjem M (binarnog) ekrana $E_{m,n}$ nazvaćemo Boole-ovu matricu $M=\|\alpha_{ij}\|_m^n$ $(1 \leqslant i \leqslant m, \quad 1 \leqslant j \leqslant m)$, gdje je α_{ij} stanje tačke ekrana sa koordinatama (i,j). Neka se ekran $E_{m,n}$ nalazi u stanju M. Skup tačaka ekrana koje se nalaze u stanju 1 nazvaćemo (ravnom) figurom odredjenom stanjem M ekrana.

Označimo sa K skup nekih kretanja u ravni i sa M proizvoljno stanje ekrana $E_{m,n}$. Skup stanja ekrana $E_{m,n}$ koja nastaju svim superpozicijama kretanja iz datog skupa K figure odredjene stanjem M ekrana, nazovimo $K^M_{m,n}$ oblikom. Klasu svih $K^M_{m,n}$ oblika označimo sa $K_{m,n}$. Ponekad ćemo, radi prostijeg označavanja, a kada to ne bude bitno, proizvoljan $K^M_{m,n}$ oblik takodje označavati sa $K_{m,n}$.

1.2. Raspoznavanje $K_{m,n}$ oblika - svodjenje na realizaciju Boole-ovih funkcija

Označimo sa B_n skup svih nizova $(\alpha_0,\ldots,\alpha_{n-1})$ dužine n, gdje je $\alpha_i \in \{0,1\}$, i=0,1,...,n-1. Preslikavanje F skupa B_n

u skup B_m ćemo zvati (Boole-ovim) (n,m)-operatorom. Operatorom ćemo nazivati (n,m)-operator za neko n i m. Svaki (n,m)-operator F možemo posmatrati kao uredjen sistem m Boole-ovih funkcija od n promjenljivih. Specijalno, (n,1)-operatori predstavljaju Boole-ove funkcije od n promjenljivih.

Neka je O proizvoljan $K_{m,n}$ oblik. Svakom stanju (matrici) $M=\left|\left|\alpha_{i,j}\right|\right|_m^n$ oblika O pridružimo niz $\tilde{\alpha}_M \in B_{mn}$:

$$\tilde{\alpha}_M=(\alpha_{11},\ldots,\alpha_{1n},\alpha_{21},\ldots,\alpha_{2n},\ldots,\alpha_{m1},\ldots,\alpha_{mn}) .$$

Tada svakom $K_{m,n}$ obliku O pridružimo Boole-ovu funkciju $f_o(x_1,\ldots,x_{mn})$, takvu da je $f_o(\alpha_1,\ldots,\alpha_{mn})=1$ akko je niz $(\alpha_1,\ldots,\alpha_{mn})$ dužine $m\cdot n$ pridružen bilo kom stanju M oblika O.

Govorićemo da neki objekat raspoznaje oblik O ako on izračunava vrijednosti (realizuje) funkcije f_o.

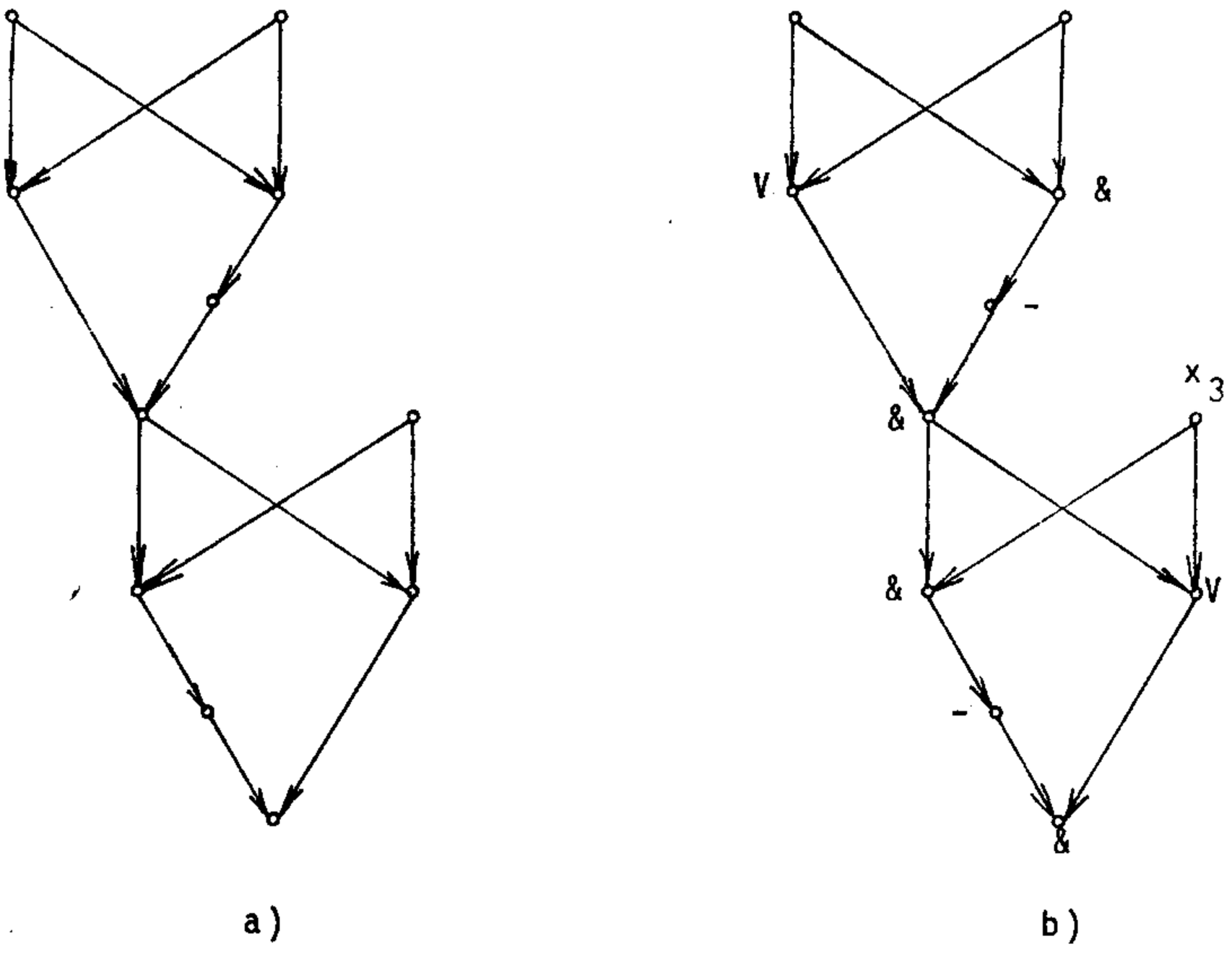
Mi ćemo se baviti realizacijom Boole-ovih funkcija u klasi shema od funkcionalnih elemenata, tc stoga i prelazimo na definiciju te klase upravljačkih sistema.

1.3. S h e m e o d f u n k c i o n a l n i h e l e m e n a t a

Neka je B proizvoljan skup Boole-ovih funkcija. Nazvaćemo ga bazom (naziv baza je ostao iz navike, iako skup B ne mora biti kompletan u funkcionalnom smislu). Da bismo izbjegli suvišne glomaznosti i neopravdan formalizam, definisaćemo sheme iz funkcionalnih elemenata nad bazom $B_0=\{\&,\vee,-\}$. Odatle će biti jasno kako se definicija prenosi na slučaj proizvoljne baze.

Neka je G - proizvoljan konačan orijentisan graf bez kontura (tj. koji ne sadrži orijentisanih ciklusa), takav da mu

u svaki čvor ulaze ne više od dvije grane. Primjer takvog grafa dat je na sl. 1a (primijetimo da u tom grafu postoje ciklusi ali ne postoje orijentisani ciklusi, tj. konture). Čvorovi grafa G u koje ne ulazi ni jedna grana, nazivaju se ulaznim čvorovima ili polovima. Ostali čvorovi grafa nazivaju se unutrašnjim. Neke čvorove grafa označimo kao izlazne. Dobijeni graf naziva se mrežom.



a) b)

S1.1.

Lema 1.3.1. [22] Konačan orijentisan graf bez kontura sadrži barem jedan čvor bez ulaznih grana i barem jedan čvor bez izlaznih grana.

Posledica ovog tvrdjenja je da svaka mreža sadrži polove.

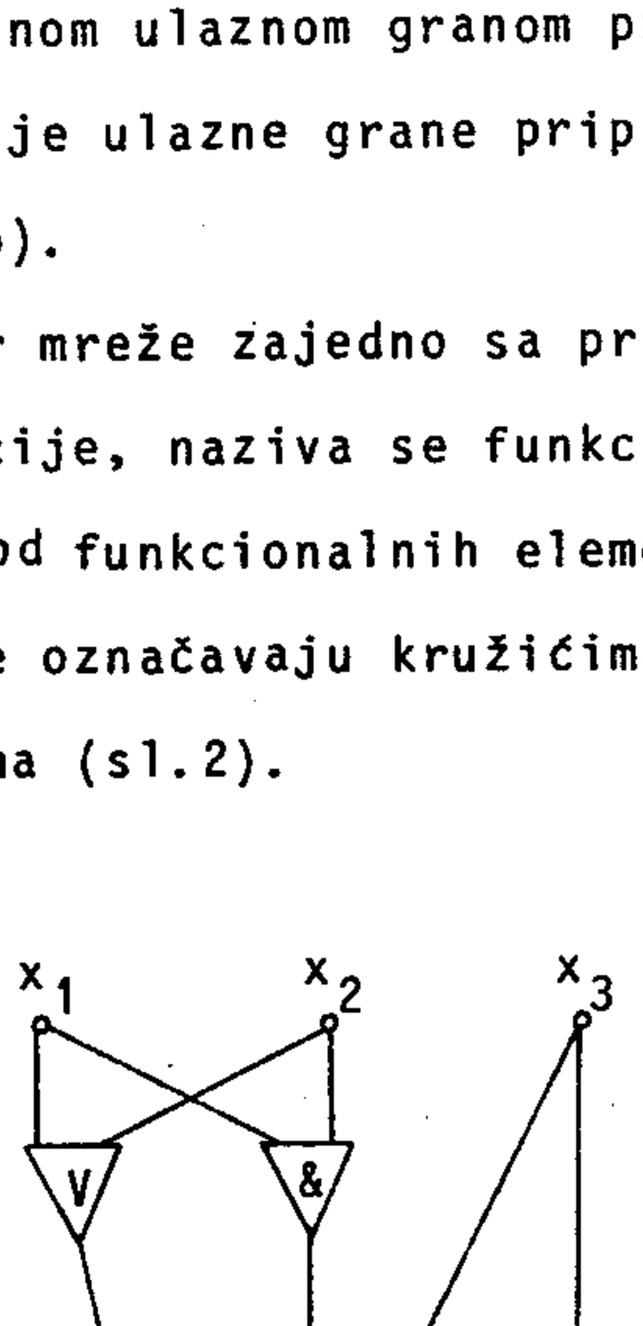
Pripišimo sada svakom čvoru mreže jedan od simbola promjenljivih $x_1,\ldots,x_n$ ili Boole-ovih funkcija iz baze $B_o=\{\&,V,-\}$, na sledeći način:

1. Svakom polu pripišimo jedan od simbola promjenljivih $x_1,\ldots,x_n$.

2. Čvoru sa jednom ulaznom granom pripišimo simbol -.

3. Čvoru sa dvije ulazne grane pripišimo jedan od simbola & ili V (vidi sl. 1b).

Unutrašnji čvor mreže zajedno sa pripisanim mu na opisani način simbolom funkcije, naziva se funkcionalnim elementom, a dobijena mreža shemom od funkcionalnih elemenata (nad bazom B_o). Ponekad se polovi sheme označavaju kružićima, a elementi trouglovima ili pravougaonicima (sl.2).



Sl. 2.

Pridružimo sada svakom čvoru sheme neku Boole-ovu funkciju na sledeći način. Svakom polu kome smo pripisali simbol x_i pridružimo funkciju $p_i(x_1,\ldots,x_n)=x_i$. Neka u čvor a ulaze grane iz čvorova b i c, kojima smo već pridružili funkcije $f_b(x_1,\ldots,x_n)$ i $f_c(x_1,\ldots,x_n)$. Ako smo čvoru a pripisali simbol & (V) tada mu pridružimo funkciju f_b & f_c (f_b V f_c). Ako u čvor a ulazi samo jedna grana, recimo iz čvora b, tada mu pridružimo funkciju $\bar{f}_b$.

Reći ćemo da se u čvoru a sheme S od funkcionalnih elemenata realizuje (izračunava) Boole-ovafunkcija koju smo mu na opisani način pridružili. Na taj način, svakom čvoru sheme možemo naći funkciju koja se u njemu realizuje. To je veoma korisno pri analizi shema, npr. pri dokazivanju donjih ocjena složenosti. Kada se ispituje makroponašanje shema (tj. kada se shema posmatra kao crna kutija sa ulazima i izlazima) od interesa su samo funkcije koje se realizuju u izlaznim čvorovima sheme (govoriće-mo,i na izlazima sheme). Neka su izlazni čvorovi sheme S uredjeni na neki način: $v_1,v_2,\ldots,v_m$. Kazaćemo da shema S realizuje Boole-ov (n,m)-operator $F=(f_1,\ldots,f_m)$ ako se funkcija f_i realizuje u izlaznom čvoru v_i sheme (na i-tom izlazu sheme), i=1,...,m.

1.4. S h a n n o n - o v e f u n k c i j e. N e k i p o z n a t i r e z u l t a t i

Neka je S shema od funkcionalnih elemenata nad bazom B. Složenost $L^B(S)$ sheme S definišimo kao broj elemenata u njoj, a složenost $L^B(F)$ (Boole-ovog) operatora F kao najmanju od složenosti shema koje realizuju taj operator. Neka je $\mathcal{F}$ konačan skup operatora. Označimo sa $L^B(\mathcal{F})=\max_{F\in\mathcal{F}} L^B(F)$. Funkcije $L^B(S)$, $L^B(F)$

i $L^{B}(\mathcal{F})$ se nazivaju Shannon-ovim funkcijama.

Lema 1.4.1. [22] Ako se funkcije iz baze B' mogu predstaviti u bazi B'', tada je

$$L^{B'}(F) = O(L^{B''}(F)).$$

Posledica 1.4.1. Ukoliko su baze B' i B'' kompletni sistemi Boole-ovih funkcija, tada je

$$L^{B'}(F) \asymp L^{B''}(F).$$

Primjedba 1.4.1. Uzimajući u obzir prethodnu posledicu i to da ćemo se ovdje baviti samo redom veličine Shannon-ovih funkcija zaključujemo da svi rezultati koje ćemo izložiti i dokazati uzimajući za bazu $B_0=\{\&,\vee,-\}$ ostaju tačni i u slučaju proizvoljne kompletne baze.

Dalje ćemo, radi prostijeg označavanja, ispuštajući gornji indeks u Shannon-ovim funkcijama podrazumijevati da se radi o bazi $B_0=\{\&,\vee,-\}$. Navedimo sada neke poznate rezultate.

U slučaju kada je $\mathcal{F}=\mathcal{P}_2^n$ - skup svih Boole-ovih funkcija od n promjenljivih, uobičajeno je $L(\mathcal{P}_2^n)$ označavati sa $L(n)$. Sledeća teorema pripada O.B.Lupanovu.

Teorema 1.4.1. [13] Skoro sve Boole-ove funkcije (tj. sve osim $o(2^{2^n})$) imaju složenost realizacije u klasi shema od funkcionalnih elemenata asimptotski jednaku L(n), gdje je

$$L(n) \sim \frac{2^n}{n}.$$

Neka je $\mathcal{F}=(\mathcal{F}_1,\mathcal{F}_2,\ldots,\mathcal{F}_n,\ldots)$ - niz klasa operatora pri čemu se $\mathcal{F}_n$ sastoji iz (n,m_n)-operatora (ne mora svih!). Neka je $M(\mathcal{F}_n)$ - broj operatora u klasi $\mathcal{F}_n$, $H(\mathcal{F}_n)=\log M(\mathcal{F}_n)$ i

$$J(\mathcal{F}_n) = \frac{H(\mathcal{F}_n)}{\log H(\mathcal{F}_n)}.$$

Teorema 1.4.2. [14] Neka

$$\frac{n + m_n}{J(\mathcal{F}_n)} \to 0 \quad (n \to \infty).$$

Tada

$$L(\mathcal{F}_n) \gtrsim J(\mathcal{F}_n) .$$

Označimo sa $\mathcal{F}^{n,m}$ klasu svih (n,m)-operatora.

Teorema 1.4.3. [14]

$$L(\mathcal{F}^{n,m}) \asymp \frac{m \cdot 2^n}{n+\log m} + m.$$

1.5. Precizna formulacija problema. Klasa $PD_{m,n}$ oblika - gruba gornja ocjena

Kao što smo nagovijestili u paragrafu 1.2, bavićemo se raspoznavanjem $K_{m,n}$ oblika u klasi shema od funkcionalnih elemenata.Reći ćemo da shema S (od funkcionalnih elemenata) raspoznaje $K_{m,n}$ oblik O ako ona realizuje Boole-ovu funkciju f_O (pridruženu obliku O na način opisan u paragrafu 1.2). Složenost funkcije f_O, tj. veličinu $L(f_O)$ zvaćemo složenošću raspoznavanja oblika O, i označavati sa L(O). Složenost $L(\mathcal{O})$ raspoznavanja klase oblika $\mathcal{O}$ definišemo kao obično: $L(\mathcal{O}) = \max_{O \in \mathcal{O}} L(O)$.

Predmet izučavanja ove disertacije je složenost raspoznavanja $K_{m,n}$ oblika gdje se skup K kretanja u ravni sastoji iz kretanja PD - pomjeranja nadesno za jedinicu. U daljem tekstu ćemo ih nazivati $PD_{m,n}$ oblicima. Formalno, $PD^M_{m,n}$ oblik je skup stanja M_i ekrana $E_{m,n}$, i=0,1,...,n-1, gdje je $M_0=M=\|\alpha_{ij}\|^n_m$, a

$$M_i = \begin{Vmatrix} 0 & \dots & 0 & \alpha_{11} & \cdots & \alpha_{1,n-i} \\ 0 & \dots & 0 & \alpha_{21} & \cdots & \alpha_{2,n-i} \\ & \vdots & & & \vdots & \\ 0 & \dots & 0 & \alpha_{m1} & \cdots & \alpha_{m,n-i} \end{Vmatrix}, \quad i=1,\dots,n-1.$$

Stanje M ćemo nazivati osnovnim stanjem $PD^M_{m,n}$ oblika. Kao i u paragrafu 1.1 sa $PD_{m,n}$ ćemo označiti klasu svih $PD^M_{m,n}$ oblika kao i proizvoljan $PD^M_{m,n}$ oblik kada ne bude važno ukazati na njegovo osnovno stanje.

Napomena 1.5.1. Nema principijelnih problema da se u disertaciji navedeni ili analogni rezultati, tehnikom koja će biti demonstrirana, dokažu i za klase oblika odredjene pomjeranjem ulijevo, gore, dolje i cikličnim pomjeranjem, pa ih stoga, i ujedno da ne bi slabili pažnju čitaoca, izostavljamo.

Lema 1.5.1. Neka su M_1 i M_2 matrice tipa m x n. Ako je $M_1 \neq M_2$, tada je $PD^{M_1}_{m,n} \neq PD^{M_2}_{m,n}$.

Dokaz. Neka su $M_1 = \|\alpha_{ij}\|^n_m$, $M_2 = \|\beta_{ij}\|^n_m$. Kako je $M_1 \neq M_2$, to postoje i, j takvi da je $\alpha_{ij} \neq \beta_{ij}$. Neka je $j_o = \min_{\alpha_{ij} \neq \beta_{ij}} j$ i, radi odredjenosti, $\alpha_{ij_o}=1$, $\beta_{ij_o}=0$. Tada očigledno $M_1 \notin PD^{M_2}_{m,n}$, čime je lema dokazana.

Posledica 1.5.1. Broj elemenata klase $PD_{m,n}$ je jednak $2^{m \cdot n}$.

U daljem tekstu, sve asimptotske jednakosti i nejednakosti podrazumijevaju da $n \to \infty$, a simboli C (sa indeksima, primovima itd.) označavaju neke konstante.

Lema 1.5.2.

$$m \cdot n \lesssim L(PD_{m,n}) \lesssim m \cdot n^2 .$$

Dokaz. Donja ocjena je trivijalna, jer je broj ulaza

sheme jednak m·n.

Gornja ocjena. Za bilo koji $PD_{m,n}$ oblik 0 funkcija f_o je jednaka jedinici na ne više od n nizova dužine m·n. Stoga je potrebno najviše n uporedjivanja ulaznog niza dužine m·n sa nizovima $\tilde{\alpha}_{M_i}$, i=0,1,...,n-1, otkuda i sleduje tvrdjenje leme (očigledno je za uporedjivanje dva niza dužine k dovoljno C·k elemenata).

U uvodu smo već rekli da su primjenom principa lokalnog kodiranja O.B.Lupanova [14] , nadjeni asimptotski najbolji metodi sinteze shema od funkcionalnih elemenata za skoro sve poznate klase Boole-ovih operatora. Donje ocjene u tim asimptotikama su rezultat primjene teoreme 1.4.2. U slučaju klase $PD_{m,n}$ oblika odnosno skupa Boole-ovih funkcija pridruženih oblicima iz te klase, imajući u vidu posledicu 1.5.1, dobijamo da, ili je nemoguće primijeniti pomenutu teoremu 1.4.2 ili ona daje slabiju donju ocjenu od trivijalne (navedene u lemi 1.5.2). Zbog nedostatka drugih (efektivnih) metoda za povišenje donjih ocjena složenosti do nelinearnih (u klasi shema od funkcionalnih elemenata) zaključujemo da metode sinteze shema,reda asimptotski optimalnih metoda, možemo dobiti samo ako izdvojimo klase $PD_{m,n}$ oblika i za njih nadjemo metode linearne složenosti. Upravo to i jeste cilj ove disertacije: opisati $PD_{m,n}$ oblike linearne složenosti raspoznavanja.

Glava II. LINEARNA SLOŽENOST RASPOZNAVANJA SVIH $PD_{m,n}$ OBLIKA NA "IZDUŽENIM" EKRANIMA

2.1. F o r m u l a c i j a t e o r e m e

U ovoj glavi ćemo dokazati da je složenost raspoznavanja bilo kog $PD_{m,n}$ oblika, ako dimenzije ekrana zadovoljavaju uslov $n \leqslant C \cdot \log m$, linearna. Drugim riječima, dokazaćemo sledeću teoremu.

Teorema 2.1.1. [38] Neka je $n \leqslant C \cdot \log m$. Tada je

$$L(PD_{m,n}) \asymp m \cdot n \ .$$

2.2. N e k i s p e c i j a l n i o p e r a t o r i

Prije nego što dokažemo formulisanu teoremu, definisaćemo neke, za dokaz potrebne operatore i dati ocjene njihove složenosti.

Neka je $\tilde{\alpha} = (\alpha_0, \ldots, \alpha_{n-1}) \in B_n$. Označimo sa $|\tilde{\alpha}|$ broj $\sum_{i=0}^{n-1} \alpha_i 2^i$ i sa $\|\tilde{\alpha}\|$ broj jedinica u nizu $\tilde{\alpha}$.

1^o Operator oduzimanja R_n. To je $(2n,n)$-operator. On na osnovu razreda dva n - cifrena broja odredjuje n razreda njihove razlike:

$$R_n(\tilde{x},\tilde{y}) = \tilde{z} \ , \quad \text{gdje je} \quad |\tilde{z}| = |\tilde{x}| - |\tilde{y}| \ .$$

Lema 2.2.1. $L(R_n) \leqslant C_r \cdot n$.

Dokaz lako proizilazi iz "školskog" algoritma za oduzimanje brojeva.

2^o Operator množenja U_n. To je $(2n,2n)$-operator koji na osnovu razreda dva n - cifrena broja odredjuje 2n razreda njiho-

/og proizvoda:

$$U_n(\tilde{x},\tilde{y}) = \tilde{z} \ , \quad \text{gdje je} \quad |\tilde{z}| = |\tilde{x}| \cdot |\tilde{y}| \ .$$

Lema 2.2.2. $L(U_n) \leqslant C_u \cdot n^2$.

Dokaz lako proizilazi iz običnog "školskog" algoritma za nnoženje brojeva. (U stvari, za realizaciju tog operatora treba nnogo manje elemenata, no nas zadovoljava i ova gruba ocjena!).

3^o Operator poredjenja S_n. To je (2n,1)-operator. On upo-redjuje dva n - cifrena broja:

$$S_n(\tilde{x},\tilde{y}) = \begin{cases} 1, & \text{ako je} \quad |\tilde{x}| \geqslant |\tilde{y}| \\ 0, & \text{ako je} \quad |\tilde{x}| < |\tilde{y}| \ . \end{cases}$$

Lema 2.2.3. [14] $L(S_n) \leqslant C_s \cdot n$.

4^o Operator jednakosti E_n. To je (2n,1)-operator koji ıstanovljava jednakost dva n - cifrena broja:

$$E_n(\tilde{x},\tilde{y}) = \begin{cases} 1, & \text{ako je} \quad |\tilde{x}| = |\tilde{y}| \\ 0, & \text{ako je} \quad |\tilde{x}| \neq |\tilde{y}| \ . \end{cases}$$

ıčigledno važi:

Lema 2.2.4. $L(E_n) \leqslant C_e \cdot n$.

5^o Operator N_n. To je (n,]log(n+1)[)-operator. On po-izu $\tilde{x}$ izračunava niz $\tilde{y}$ koji predstavlja binaran zapis broja je-inica u $\tilde{x}$, tj. $|\tilde{y}| = x_o + \ldots + x_{n-1}$ (suma nije po mod 2, nego obi-na!).

Lema 2.2.5. [14] $L(N_n) \leqslant C_n \cdot n$.

6^o Operator $\tilde{H}_n$. To je (n,n)-operator, koji transformiše vaki niz oblika

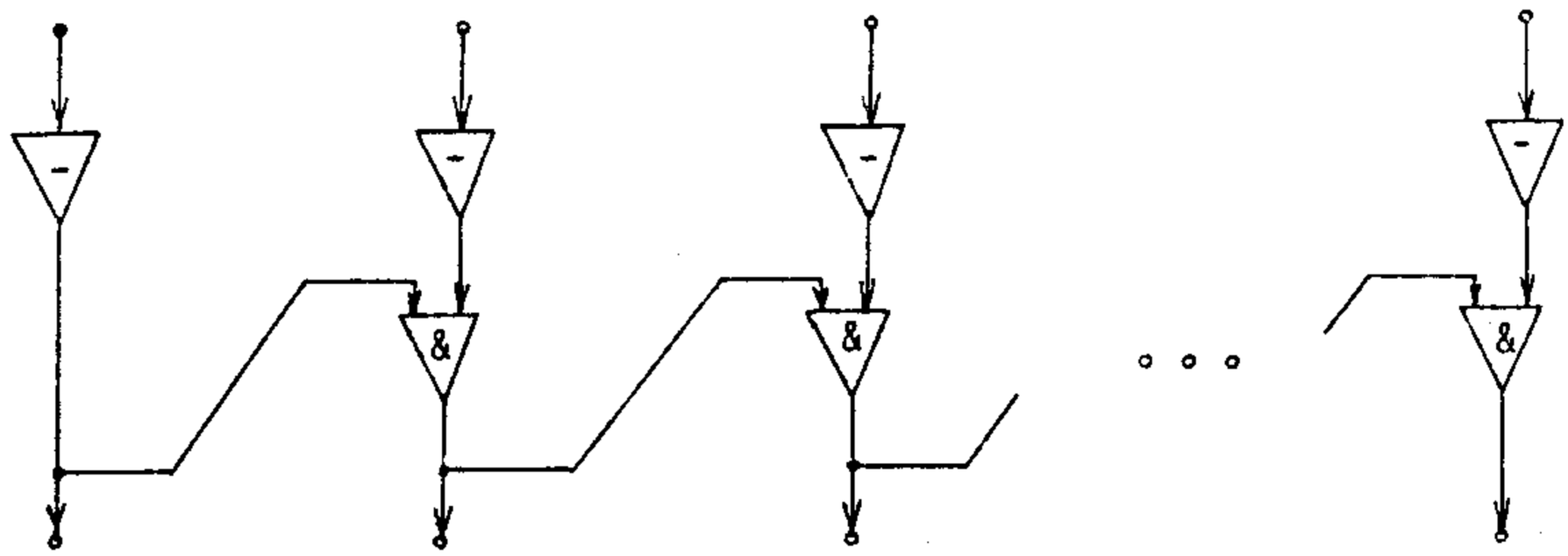
$$(0, \ldots, 0, 1, \sigma_1, \ldots, \sigma_k)$$

niz

$$(1, \ldots, 1, 0, 0, \ldots, 0) \ .$$

Lema 2.2.6. $L(\widetilde{H}_n) \leqslant C_h \cdot n$.

Ova ocjena je očigledna (vidi sl. 3).



Sl.3.

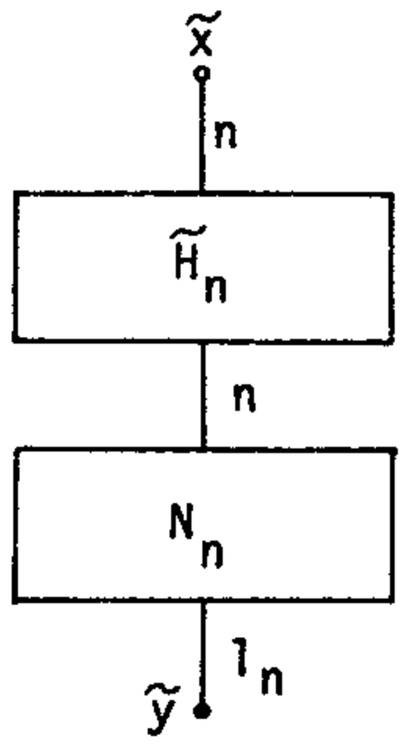
U daljem tekstu ćemo veličinu $]\log(n+1)[$ označavati sa l_n.

7^o Operator P_n. To je (n, l_n)-operator. On niz $\widetilde{x}$ transformiše u niz $\widetilde{y}$, koji predstavlja binaran zapis broja nula u nizu $\widetilde{x}$ do prve slijeva jedinice, tj.

$$|\widetilde{y}| = \begin{cases} k , & \text{ako je } x_0=x_1=\ldots=x_{k-1}=0 , \ x_k=1 \\ n , & \text{ako je } x_0=x_1=\ldots=x_{n-1}=0 \end{cases}$$

Lema 2.2.7. $L(P_n) \leqslant C_p \cdot n$.

Dokaz slijedi iz lema 2.2.5 i 2.2.6 (vidi sl.4).



Sl.4.

8^{o} Operator pomjeranja T_n. To je $(n+l_n,n)$-operator, koji proizvoljan niz $\tilde{x}$ pomjera nadesno za $|\tilde{y}|$ mjesta. Formalno, operator T_n transformiše nizove $\tilde{x}=(x_o,\ldots,x_{n-1})$ i $\tilde{y}=(y_o,\ldots,y_{l_n-1})$ u niz $\tilde{z}=(0,\ldots,0,x_o,\ldots,x_{n-|\tilde{y}|-1})$. Označimo ga sa $\tilde{x}\overrightarrow{|\tilde{y}|}$.

Lema 2.2.8. [14] $L(T_n) \leqslant C_t \cdot n \cdot \log n$.

2.3. D o k a z t e o r e m e

Donja ocjena je trivijalna, jer je broj ulaza sheme jednak $m \cdot n$.

Gornja ocjena. Neka je $M=\|\alpha_{ij}\|_m^n$ proizvoljna nenula matrica (inače je dokaz trivijalan). Označimo sa i_o i j_o sledeće indekse: $j_o=\min\limits_{\alpha_{ij}=1} j$, a i_o bilo koji indeks koji zadovoljava jednakost $\alpha_{i_o j_o}=1$. Neka je $\tilde{\beta}=(\beta_o,\ldots,\beta_{l_n-1})$ binaran zapis broja j_o-1, a $\tilde{\gamma}=(\gamma_o,\ldots,\gamma_{l_n-1})$ binaran zapis broja l_n (suvišne stari-je razrede u nizu $\tilde{\gamma}$ ispunimo nulama).

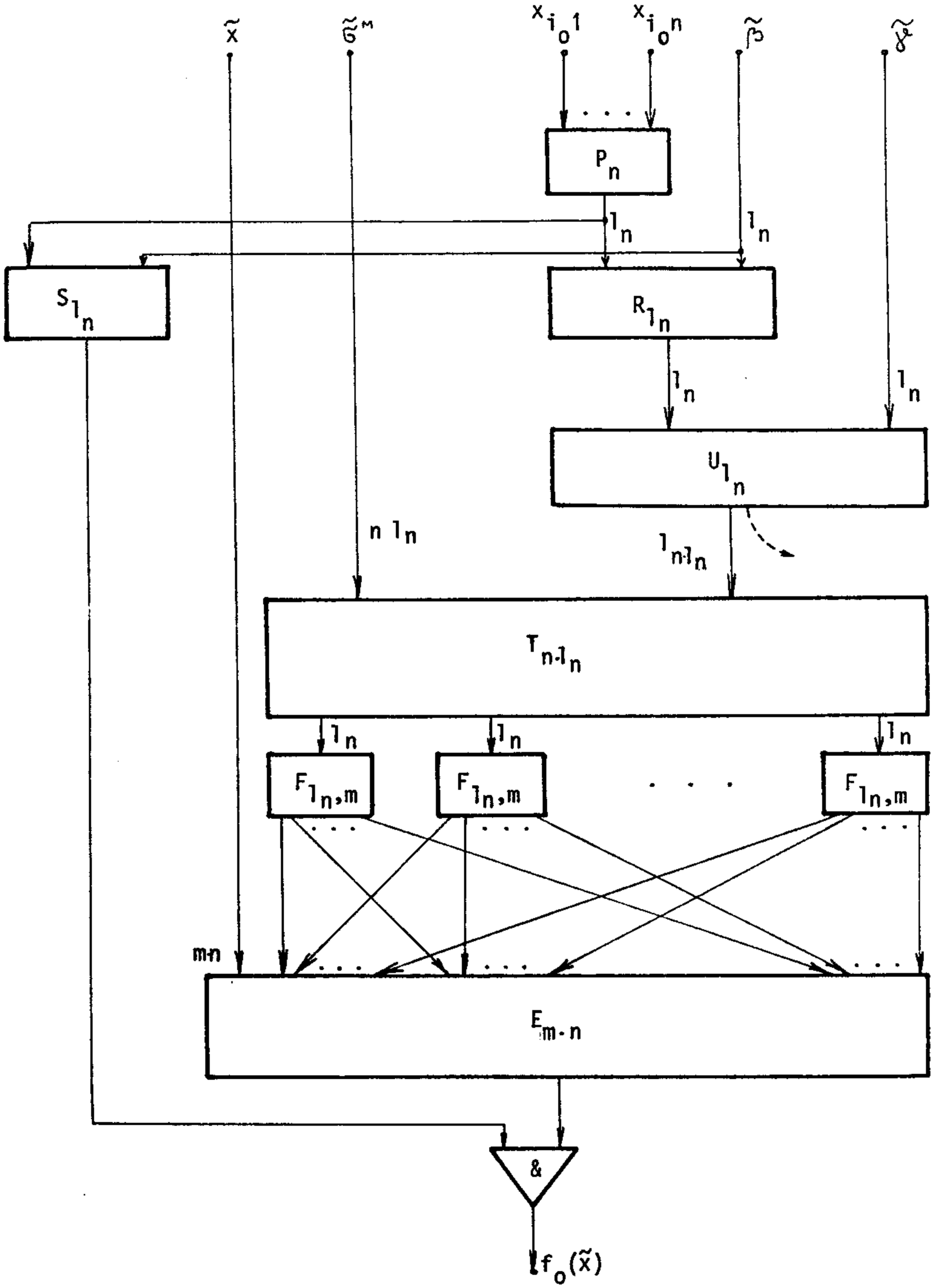
Uočimo sve različite kolone matrice M. Kako ih ima nc više od n, zakodirajmo ih nizovima dužine l_n tako da različitim kolonama odgovaraju različiti kodovi i nula koloni nula kod. Označimo sa $\tilde{\sigma}^M$ sledeći niz dužine $n \cdot l_n$:

$$\tilde{\sigma}^M=(\sigma_{11},\ldots,\sigma_{1l_n},\sigma_{21},\ldots,\sigma_{2l_n},\ldots,\sigma_{n1},\ldots,\sigma_{nl_n}),$$

gdje je $(\sigma_{i1},\ldots,\sigma_{il_n})$ kod i-te kolone matrice M, $i=1,2,\ldots,n$.

Označimo sa $O\,PD^M_{mn}$ oblik, odredjen matricom M. Shema od funkcionalnih elemenata koja realizuje funkciju f_o, konstruiše se saglasno sledećem algoritmu (vidi sl.5):

1) Neka je $\tilde{x}=(x_{11},\ldots,x_{1n},\ldots,x_{m1},\ldots,x_{mn})$ ulazni niz. Dovedimo $x_{i_o1},\ldots,x_{i_on}$ na ulaze sheme koja realizuje operator P_n. $L(P_n) \leqslant C_p \cdot n$ (lema 2.2.7).


x̃
σ̃ᵐ
x_{i_o}1
x_{i_o}n
β̃
α̃
P_n
1_n
1_n
S_{1_n}
R_{1_n}
1_n
1_n
U_{1_n}
n 1_n
1_{n-1_n}
T_{n-1_n}
1_n
1_n
1_n
F_{1_n,m}
F_{1_n,m}
F_{1_n,m}
m·n
E_{m·n}
&
f_o(x̃)

S1.5.

2) Izlazni niz sheme P_n i niz $\tilde{\beta}$ (koji je moguće realizovati sa složenošću $C \cdot \log n$) se dovode na ulaze sheme R_{l_n}, koja izračunava njihovu razliku, tj. veličinu pomjeraja. $L(R_{l_n}) \leqslant C'_r \cdot \log n$ (lema 2.2.1).

3) Izlazni niz sheme R_{l_n} i niz $\tilde{\gamma}$ (koji je moguće realizovati sa složenošću $C \cdot \log n$) dovode se na ulaze sheme U_{l_n}. $L(U_{l_n}) \leqslant C'_u \cdot \log^2 n$ (lema 2.2.2).

4) Niz $\tilde{\omega}^M$ (koji je moguće realizovati sa složenošću $C \cdot n \cdot \log n$) i mladjih $l_{n \cdot l_n}$ razreda izlaznog niza sheme U_{l_n} dovode se na ulaze sheme $T_{n \cdot l_n}$. $L(T_{n \cdot l_n}) \leqslant C'_t \cdot n \cdot \log^2 n$ (lema 2.2.8).

5) Izlaze sheme $T_{n \cdot l_n}$ razbijmo slijeva nadesno na n grupa po l_n izlaza u svakoj, i svaku grupu izlaza dovedimo na ulaze po jedne od n shema $F_{l_n,m}$, svaka od kojih po ulaznom nizu dužine l_n - kodu kolone matrice M, odredjuje samo kolonu - niz dužine m na nizovima koji nijesu iskorišćeni pri kodiranju, ona daje proizvoljne vrijednosti). Na taj način, svaka od tih n shema $F_{l_n,m}$ realizuje neki (l_n,m)-operator (koji zavisi od matrice M i načina kodiranja). Složenost tog operatora nije veća od složenosti najsloženijeg (l_n,m)-operatora, tj. od veličine

$$C' \cdot \left(\frac{m \cdot 2^{l_n}}{\log m + l_n} + m \right)$$

vidi teoremu 1.4.3). Dakle, složenost n shema $F_{l_n,m}$, pri uslovu teoreme $n \leqslant C \cdot \log m$, nije veća od

$$C' \cdot n \cdot \left(\frac{m \cdot 2^{l_n}}{\log m + l_n} + m \right) \leqslant C'_o \cdot m \cdot n \ .$$

6) Izlaze n shema $F_{l_n,m}$, na kojima se realizuje matrica pomjerena za veličinu odredjenu ulaznim nizom $\tilde{x}$, pregrupišimo

tako da dobijemo niz pridružen toj matrici. Tako pregrupisane izlaze dovedimo zajedno sa nizom $\tilde{x}$ na ulaze sheme E_{mn}, koja ih sravnjuje. $L(E_{mn}) \leqslant C_e \cdot m \cdot n$ (lema 2.2.4).

7) Najzad se izlazna vrijednost sheme E_{mn} množi sa izlaznom vrijednošću sheme poredjenja S_{1_n}, koja uporedjuje izlazni niz sheme P_n sa nizom $\tilde{\beta}$. $L(S_{1_n}) \leqslant C'_s \cdot \log n$ (lema2.2.3).

Na taj način, sumirajući sve te složenosti, dobijamo da je za $n \leqslant C \cdot \log m$, $L(f_o) \leqslant C_o \cdot m \cdot n$, za bilo koji $PD_{m,n}$ oblik O.

Teorema je dokazana.

Glava III. RASPOZNAVANJE $PD_{m,n}$ OBLIKA I OPERATORI POMJERANJA

3.1. Operator pomjeranja - tačni- ja gornja ocjena. Hipoteza Ľupanova

Metod sinteze shema iz glave II u slučaju kada dimenzije m i n ekrana $E_{m,n}$ ne zadovoljavaju uslov $n \leqslant C \cdot \log m$, daje nelinearnu gornju ocjenu složenosti raspoznavanja klase svih $PD_{m,n}$ oblika. Nije teško vidjeti da taj metod za bilo koje m i n daje sledeću ocjenu:

Teorema 3.1.1.

$$L(PD_{m,n}) \lesssim \frac{m \cdot n^2}{\log n} .$$

Vidimo da je ta ocjena mnogo bolja od grube gornje ocjene date u lemi 1.5.2.

Opisaćemo sada jedan drugi metod sinteze koji za klasu svih $PD_{m,n}$ oblika, u slučaju kada nije ispunjeno $n \leqslant C \cdot \log m$, daje asimptotski bolju i od te, ocjenu složenosti raspoznavanja.

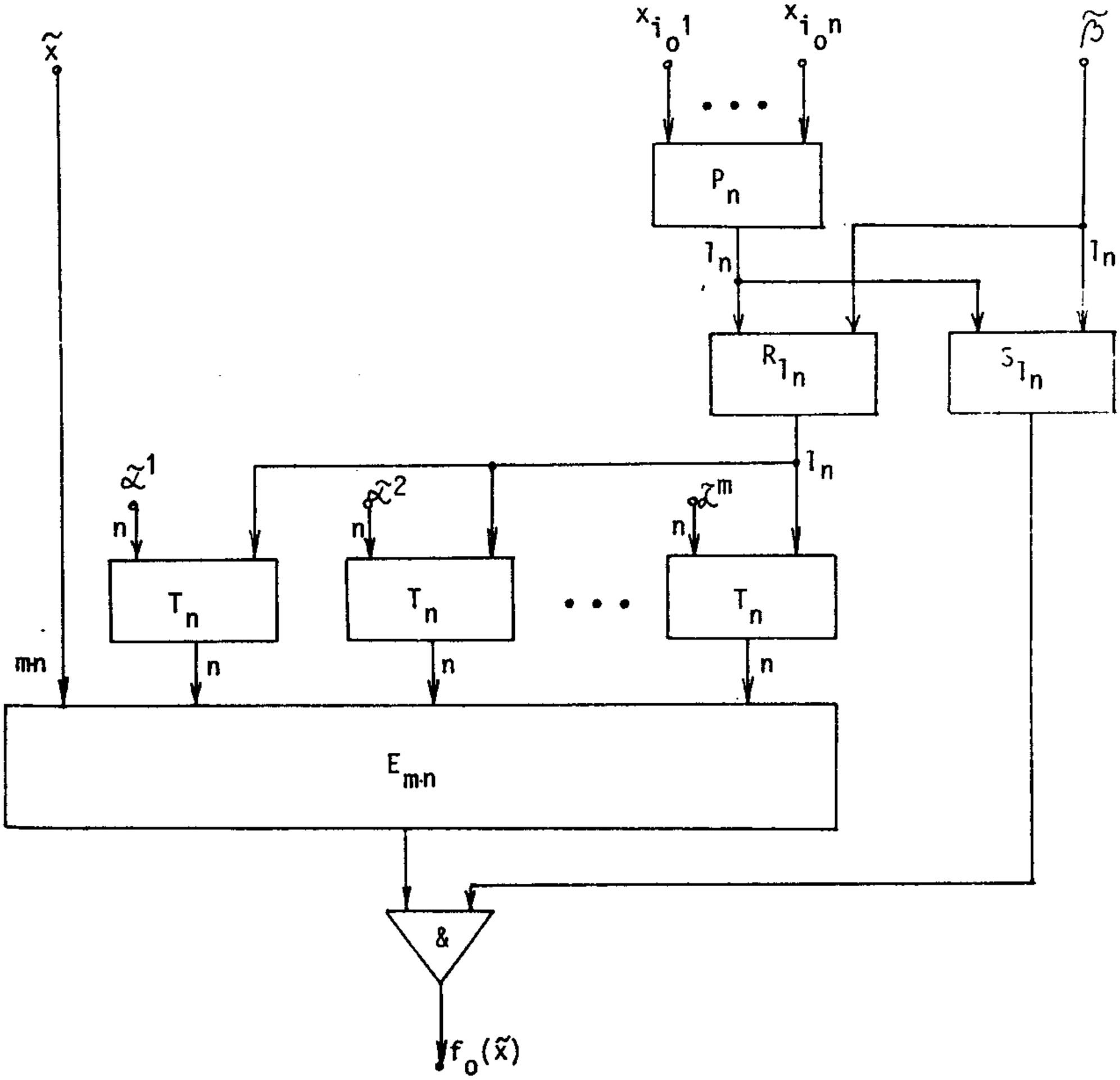
Teorema 3.1.2.

$$L(PD_{m,n}) \lesssim m \cdot n \cdot \log n ,$$

Dokaz. Posmatrajmo proizvoljan $PD^M_{m,n}$ oblik O, gdje je $M = \|\alpha_{ij}\|^n_m$ nenula matrica (inače je dokaz trivijalan). Kao i u dokazu teoreme 2.1.1 označimo sa i_o i j_o sledeće indekse: $j_o = \min\limits_{\alpha_{ij}=1} j$, a i_o bilo koji indeks koji zadovoljava jednakost $\alpha_{i_o j_o} = 1$. Označimo sa $\tilde{\beta} = (\beta_0, \ldots, \beta_{l_n - 1})$ binaran zapis broja $j_o - 1$. Neka je $\tilde{\alpha}^i = (\alpha_{i1}, \ldots, \alpha_{in})$, $i = 1, \ldots, m$. Shema koja raspoznaje posmatrani $PD^M_{m,n}$ oblik konstruiše se prema sledećem algoritmu (vidi sl.6):

1) Neka je $\tilde{x}=(x_{11},\ldots,x_{1n},\ldots,x_{m1},\ldots,x_{mn})$ ulazni niz. Dovedimo $x_{i_o1},\ldots,x_{i_on}$ na ulaze sheme koja realizuje operator P_n. $L(P_n) \leqslant C_p \cdot n$ (lema 2.2.7).

2) Izlazni niz sheme P_n i niz $\tilde{\beta}$ (koji je moguće realizovati sa složenošću $C \cdot \log n$) dovodimo na ulaze sheme R_{1_n} koja izračunava njihovu razliku, tj. veličinu pomjeraja. $L(R_{1_n}) \leqslant C'_r \cdot \log n$ (lema 2.2.1).



S1.6.

3) Izlaze sheme R_{1_n} dovedimo na II grupu ulaza svake od m shema koje realizuju operator pomjeranja T_n. Neka su te sheme uredjene na neki način. Na I grupu ulaza i-te sheme dovedimo niz $\mathcal{X}^i$, i=1,...,m (sve nizove $\mathcal{X}^i$ možemo realizovati sa složenošću $C \cdot m \cdot n$). $L(T_n) \leqslant C_t \cdot n \cdot \log n$ (lema 2.2.8), pa je složenost m takvih shema $\leqslant C_t \cdot m \cdot n \cdot \log n$.

4) Ulazni niz $\tilde{x}$ i izlazne nizove m shema koje realizuju operator T_n, uzete onim redom kako su sheme uredjene, dovedimo na ulaze sheme $E_{m \cdot n}$ koja ih sravnjuje. $L(E_{m \cdot n}) \leqslant C_e \cdot m \cdot n$ (lema 2.2.4).

5) Izlazna vrijednost sheme $E_{m \cdot n}$ se množi sa izlaznom vrijednošću sheme poredjenja S_{1_n}, koja ispituje da li je veličina pomjeraja veća ili jednaka od veličine j_o-1. $L(S_{1_n}) \leqslant C'_s \cdot \log n$ (lema 2.2.3).

Na taj način, sumirajući sve navedene složenosti, dobijamo $L(PD^M_{m,n}) \leqslant C'' \cdot m \cdot n \cdot \log n$, za bilo koji $PD^M_{m,n}$ oblik.

Teorema je dokazana.

Hipoteza Lupanova. Analizom opisane sheme zaključujemo da joj glavni dio složenosti dolazi upravo od shema koje realizuju operator pomjeranja T_n. Gornju nelinearnu ocjenu njegove složenosti, $L(T_n) \leqslant C_t \cdot n \cdot \log n$, navedenu u paragrafu 2.2 (lema 2.2.8), dao je O.B.Lupanov [14]. Do danas nikome nije pošlo za rukom da je snizi. Čak šta više, O.B.Lupanov je izrazio hipotezu da operator pomjeranja T_n ima nelinearnu složenost. Zbog principijelnih problema oko dokazivanja donjih ocjena složenosti individualnih funkcija, ta hipoteza do danas nije dokazana.

Iz dokaza prethodne teoreme zaključujemo da je možemo preformulisati na sledeći način:

Teorema 3.1.3.

$$L(PD_{m,n}) \lesssim m \cdot L(T_n) .$$

Dakle, svako sniženje gornje ocjene složenosti operatora pomjeranja T_n, snizuje gornju ocjenu složenosti raspoznavanja klase svih $PD_{m,n}$ oblika.

Iako nije jasna neophodnost operatora T_n u našem problemu raspoznavanja $PD_{m,n}$ oblika, on se tu, ipak, javlja na prirodan način, pa nas hipoteza Lupanova upućuje na odustajanje od traženja univerzalnog metoda za raspoznavanje svih $PD_{m,n}$ oblika. Ako se ograničimo na neku podklasu $PD^{\mathcal{M}}_{m,n}$ klase $PD_{m,n}$, $PD^{\mathcal{M}}_{m,n}=\{PD^{M}_{m,n} \mid M \in \mathcal{M}\}$ gdje je $\mathcal{M}$ neki skup Boole-ovih matrica tipa m x n, iz dokaza prethodne teoreme zaključujemo da nama nije neophodan operator T_n, već neki njegovi podoperatori $T^{\tilde{\alpha}}_n$, $\tilde{\alpha} \in A \subseteq B_n$, gdje je A skup vrsta matrica $M \in \mathcal{M}$, svaki od kojih pomjera nadesno konkretan niz $\tilde{\alpha}$ za proizvoljan broj mjesta. Formalnije, operator $T^{\tilde{\alpha}}_n$, $\tilde{\alpha} \in B_n$ je (l_n,n)-operator koji transformiše niz $\tilde{y}=(y_0,\ldots,y_{l_n-1})$ u niz $\tilde{\alpha}^{\rightarrow}_{|\tilde{y}|}=(0,\ldots,0,\alpha_0,\ldots,\alpha_{n-|\tilde{y}|-1})$.

Na taj način, dolazimo do još preciznije preformulacije teoreme 3.1.2:

Teorema 3.1.4. Za svaki $PD^{M}_{m,n}$ oblik važi

$$L(PD^{M}_{m,n}) \lesssim \sum_{i=1}^{m} L(T^{\tilde{\alpha}^i}_n),$$

gdje je $\tilde{\alpha}^i$ - i-ta vrsta matrice M.

Time smo, naš problem opisivanja klasa $PD_{m,n}$ oblika linearne složenosti raspoznavanja sveli na problem opisivanja skupova $A \subseteq B_n$ takvih da je za svako $\tilde{\alpha} \in A$, $L(T^{\tilde{\alpha}}_n) \asymp n$. Ideja je da, koristeći svojstva nizova $\tilde{\alpha} \in A$, konstruišemo metode sinteze shema linearne složenosti koje realizuju operatore $T^{\tilde{\alpha}}_n$, $\tilde{\alpha} \in A$, i time snizimo do minimalne nelinearnu ocjenu složenosti operatora T_n,

koja važi i za operatore $T_n^{\tilde{\alpha}}$. U narednim paragrafima ćemo to i učiniti.

Na kraju ovog paragrafa dokažimo jednu lemu na koju ćemo se kasnije često pozivati.

Kazaćemo da je niz $\tilde{x}=(x_0,\ldots,x_{n-1})\in B_n$ član po član suma po mod 2 nizova $\tilde{y}=(y_0,\ldots,y_{n-1})\in B_n$ i $\tilde{z}=(z_0,\ldots,z_{n-1})\in B_n$ ako je $x_i=y_i \oplus z_i$, $i=0,\ldots,n-1$. U tom slučaju ćemo pisati $\tilde{x}=\tilde{y}\oplus\tilde{z}$. Analogno se definiše član po član suma nizova $\tilde{y}^i$, $i=1,\ldots,l$. Označavaćemo je sa $\bigoplus_{i=1}^{l}\tilde{y}^i$.

Lema 3.1.1. Ako je niz $\tilde{x}\in B_n$ član po član suma po mod 2 nizova $\tilde{y}^i$, $i=1,\ldots,C$ i $L(T_n^{\tilde{y}^i})\asymp n$ za $i=1,\ldots,C$, tada je $L(T_n^{\tilde{x}})\asymp n$.

Dokaz proizilazi iz činjenice da $\tilde{x}=\bigoplus_{i=1}^{c}\tilde{y}^i$ povlači $\tilde{x}_{|\vec{z}|}=\bigoplus_{i=1}^{c}\tilde{y}^i_{|\tilde{z}|}$, gdje je $\tilde{z}$ ulazni niz operatora $T_n^{\tilde{x}}$.

3.2. N e k i s p e c i j a l n i o p e r a t o r i
(n a s t a v a k p a r a g r a f a 2.2)

Osim operatora definisanih u paragrafu 2.2 nadalje će se više puta koristiti još neki operatori, te ocjenama njihove složenosti i posvećujemo ovaj paragraf.

1^o Operator K_n ("dešifrator"). To je $(n,2^n)$-operator koji proizvoljan niz $\tilde{x}=(x_0,\ldots,x_{n-1})$ transformiše u niz $\tilde{y}=(y_0,\ldots,y_{2^n-1})$ takav, da

$$y_i=\begin{cases}1, & \text{ako je } i=|\tilde{x}|\\ 0, & \text{ako je } i\neq|\tilde{x}|\end{cases}.$$

Dobro je poznata sledeća ocjena:

Lema 3.2.1. $L(K_n)\leqslant C_k\cdot 2^n$.

2^o Operator Q_n (u nekom smislu inverzan operatoru K_n). To je $(2^n, n+1)$-operator. On niz $\tilde{e}_i=(0,\ldots,0,\underset{i}{1},0,\ldots,0)$, $i=0,\ldots,2^n-1$,

dužine 2^n transformiše u binaran zapis indeksa razreda u kojem leži jedinica, nula niz transformiše u niz $(0,\ldots,0,1)$, a na ostalim nizovima može biti proizvoljan.

Lema 3.2.2. [14] $L(Q_n) \leqslant C_q \cdot 2^n$.

3^o Operatori dijeljenja D_n^k odredjeni prirodnim brojem k, $1 \leqslant k < 2^n$. Pri fiksiranom k, D_n^k je $(n,2n)$-operator, koji niz $\tilde{x}$ dužine n transformiše u dva niza: niz $\tilde{y}$ dužine n takav da je $\tilde{y} = \left[\frac{|\tilde{x}|}{k}\right]$ i niz $\tilde{z}$ dužine n takav da je $|\tilde{z}| = |\tilde{x}| - |\tilde{y}| \cdot k$.

Lema 3.2.3. Za svako k, $1 \leqslant k < 2^n$,

$$L(D_n^k) \leqslant C_d \cdot 2^n .$$

Dokaz trivijalan (iz teoreme 1.4.3).

4^o Operator H_n. To je (n,n)-operator koji svaki niz oblika

$$(0,\ldots,0,1,0,\ldots,0)$$

transformiše u niz

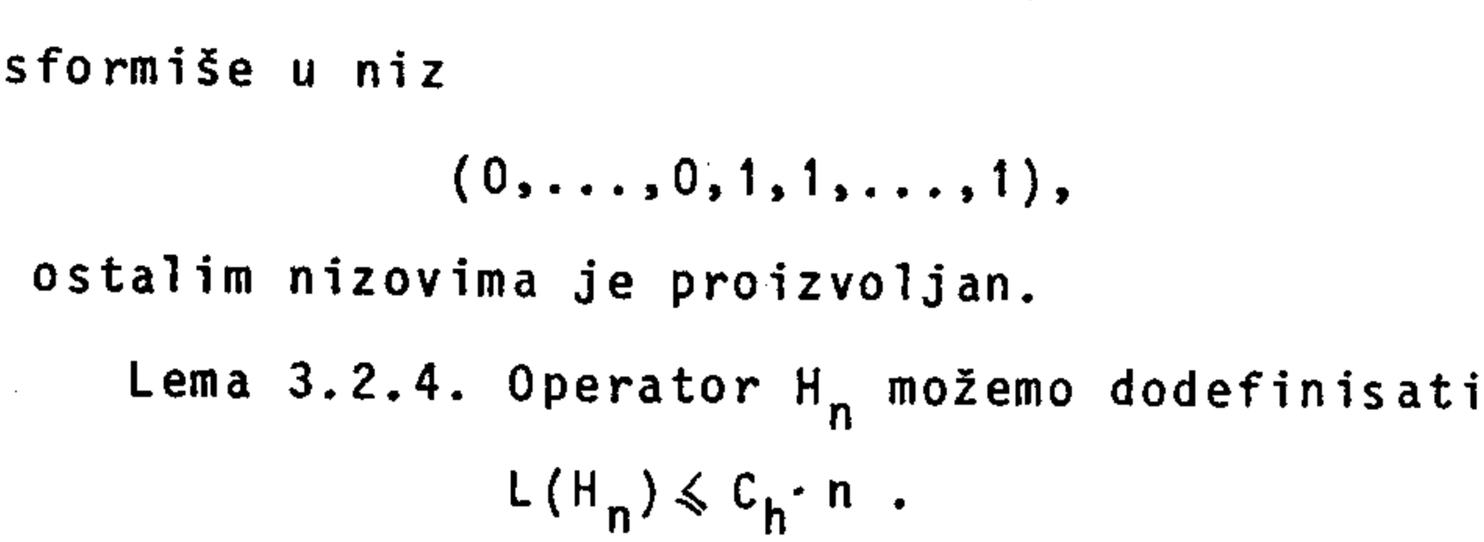
$$(0,\ldots,0,1,1,\ldots,1),$$

a na ostalim nizovima je proizvoljan.

Lema 3.2.4. Operator H_n možemo dodefinisati tako da je

$$L(H_n) \leqslant C_h \cdot n .$$

Dokaz je očigledan (vidi sl.7).



Sl.7.

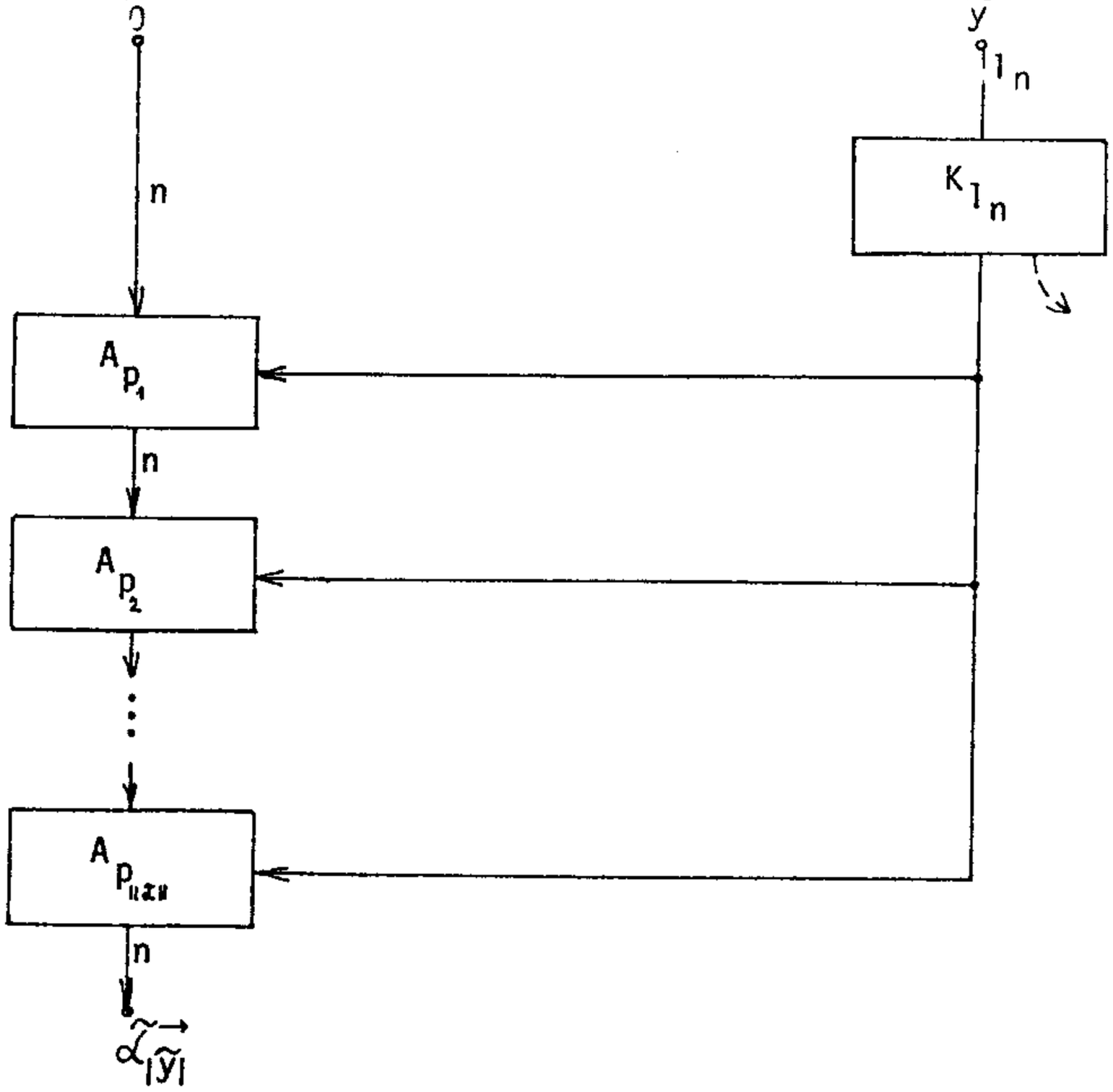
5^{o} Operatori ograničenog pomjeranja $M_n^{\tilde{\alpha}}$, $\tilde{\alpha} \in B_n$. Za dati niz $\tilde{\alpha}$, $M_n^{\tilde{\alpha}}$ je (l_n, n)-operator koji proizvoljan niz $\tilde{y}$ dužine l_n transformiše u niz $\tilde{\alpha}_{|\tilde{y}|}^{\rightarrow}$, ako je $|\tilde{y}| < C \cdot \frac{n}{\|\tilde{\alpha}\|}$, i u nula niz u ostalim slučajevima.

Lema 3.2.5. Za svako $\tilde{\alpha} \in B_n$

$$L(M_n^{\tilde{\alpha}}) \leqslant C_m n.$$

Dokaz. Neka je $\tilde{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ proizvoljan nenula niz (inače je dokaz trivijalan). Označimo sa p_i, $i=1,2,\ldots,\|\tilde{\alpha}\|$ indekse članova niza $\tilde{\alpha}$ jednakih jedinici. Shema koja realizuje operator $M_n^{\tilde{\alpha}}$ konstruiše se saglasno sledećem algoritmu (vidi sl.8):

1) Ulazni niz $\tilde{y} = (y_0, \ldots, y_{l_n - 1})$ dovedimo na ulaze dešifratora K_{l_n}. $L(K_{l_n}) \leqslant C'_k \cdot n$ (lema 3.2.1).



Sl.8.

2) Prvih $C\frac{n}{\|\tilde{\alpha}\|}$ članova izlaznog niza dešifratora (ili on čitav ako je $\|\tilde{\alpha}\| \leqslant C$) dovedimo na II grupu ulaza shema A_{p_i}, $i=1,\ldots,\|\tilde{\alpha}\|$, gdje shema A_{p_i} pomjera i-tu jedinicu niza $\tilde{\alpha}$ za $|\tilde{y}|$ mjesta. Na I grupu ulaza sheme A_{p_1} dovedimo nula niz dužine n, a na prvu grupu ulaza sheme A_{p_i}, $i>1$ (ukoliko postoji, tj. ukoliko je $\|\tilde{\alpha}\|>1$) dovedimo izlazni niz sheme $A_{p_{i-1}}$ (tj. niz kod koga su prvih (i-1) jedinica već postavljene na mjesto odredjeno veličinom pomjeraja $|\tilde{y}|$). Formalno, shema A_p, $0 \leqslant p \leqslant n-1$ realizuje $(n+C\frac{n}{\|\tilde{\alpha}\|}, n)$-operator, koji nizove $\tilde{u}=(u_0,\ldots,u_{n-1})$ (to je I grupa ulaza sheme) i $\tilde{v}=(v_0,\ldots,v_{C\frac{n}{\|\tilde{\alpha}\|}-1})$ (to je II grupa ulaza sheme), transformiše u niz $z=(z_0,\ldots,z_{n-1})$ odredjen sledećom relacijom:

$$z_i=\begin{cases} u_i \vee v_{i-p}, & p \leqslant i < \min\left\{n, C\frac{n}{\|\tilde{\alpha}\|}+p\right\} \\ u_i, & \text{u ostalim slučajevima.} \end{cases}$$

Očigledno je, za svako i, $L(A_{p_i}) \leqslant C\frac{n}{\|\tilde{\alpha}\|}$.

Na taj način, $L(M_n^{\tilde{\alpha}}) \leqslant C'_k \cdot n + C\cdot\frac{n}{\|\tilde{\alpha}\|}\cdot\|\tilde{\alpha}\| \leqslant C_m \cdot n$.

Lema je dokazana.

6^o Operatori $B^i_{n,k}$, $i=0,1,\ldots,\left]\frac{n}{k}\right[-1$. Pri fiksiranom $k \in N$, za svako i, $i \in \left\{0,1,\ldots,\left]\frac{n}{k}\right[-1\right\}$, $B^i_{n,k}$ je $(n+2k+1,n)$-operator koji nizove $\tilde{x}=(x_0,\ldots,x_{n-1})$, $\tilde{y}=(y_0,\ldots,y_{2k-1})$ i $\tilde{z}=(z_0)$ transformiše u niz $\tilde{v}=(v_0,\ldots,v_{n-1})$ saglasno sledećoj relaciji:

$$v_j=\begin{cases} x_j \vee y_{j-2k} \,\&\, z_0, & ik \leqslant j < \min\{(i+2)k, n\} \\ x_j, & \text{u ostalim slučajevima.} \end{cases}$$

Očigledno važi:

Lema 3.2.6. Za svako $k \in N$ i svako $i \in \left\{0,1,\ldots,\left]\frac{n}{k}\right[-1\right\}$

$$L(B^i_{n,k}) \leqslant C_b \cdot k.$$

7^o Operator I_n. To je $(2n,n)$-operator, koji nizove $\tilde{x}=(x_0,\ldots,x_{n-1})$

i $\tilde{y}=(y_0,\ldots,y_{n-1})$ član po član množi, tj. transformiše u niz $\tilde{z}=(z_0,\ldots,z_{n-1})$ gdje je $z_i=x_i \,\&\, y_i$, $i=0,\ldots,n-1$. Očigledno važi:

Lema 3.2.7. $L(I_n) \leqslant C_i \cdot n$.

8^o Operator $\sum_n$. To je $(2n,n)$-operator koji nizove $\tilde{x}=(x_0,\ldots,x_{n-1})$ i $\tilde{y}=(y_0,\ldots,y_{n-1})$ član po član sumira, tj. transformiše u niz $\tilde{z}=(z_0,\ldots,z_{n-1})$ gdje je $z_i=x_i \vee y_i$, $i=0,\ldots,n-1$. Očigledno važi:

Lema 3.2.8. $L(\sum_n) \leqslant C_g \cdot n$.

3.3. P e r i o d i č n i n i z o v i

Za niz $\tilde{x}=(x_0,\ldots,x_{n-1})$ reći ćemo da je periodičan slijeva nadesno sa periodom $\tilde{y}=(y_0,\ldots,y_{k-1})$ dužine k, ako je

$$\tilde{x}=(y_0,\ldots,y_{k-1},y_0,\ldots,y_{k-1},\ldots,y_0,\ldots,y_{k-1},y_0,\ldots,y_{n-\left[\frac{n}{k}\right]\cdot k-1}) ,$$

gdje se niz $\tilde{y}=(y_0,\ldots,y_{k-1})$ ponavlja $\left[\frac{n}{k}\right]$ puta. Za niz $\tilde{x}=(x_0,\ldots,x_{n-1})$ reći ćemo da je periodičan sdesna nalijevo sa periodom $\tilde{y}=(y_0,\ldots,y_{k-1})$ dužine k, ako je niz $\tilde{x}^{-1}=(x_{n-1},x_{n-2},\ldots,x_1,x_0)$ periodičan slijeva nadesno sa periodom $\tilde{y}=(y_0,\ldots,y_{k-1})$.

Teorema 3.3.1. Ako je $\tilde{\alpha} \in B_n$ periodičan niz slijeva nadesno sa periodom dužine k, $k \leqslant C_1 \cdot \frac{n}{\log n}$, onda je

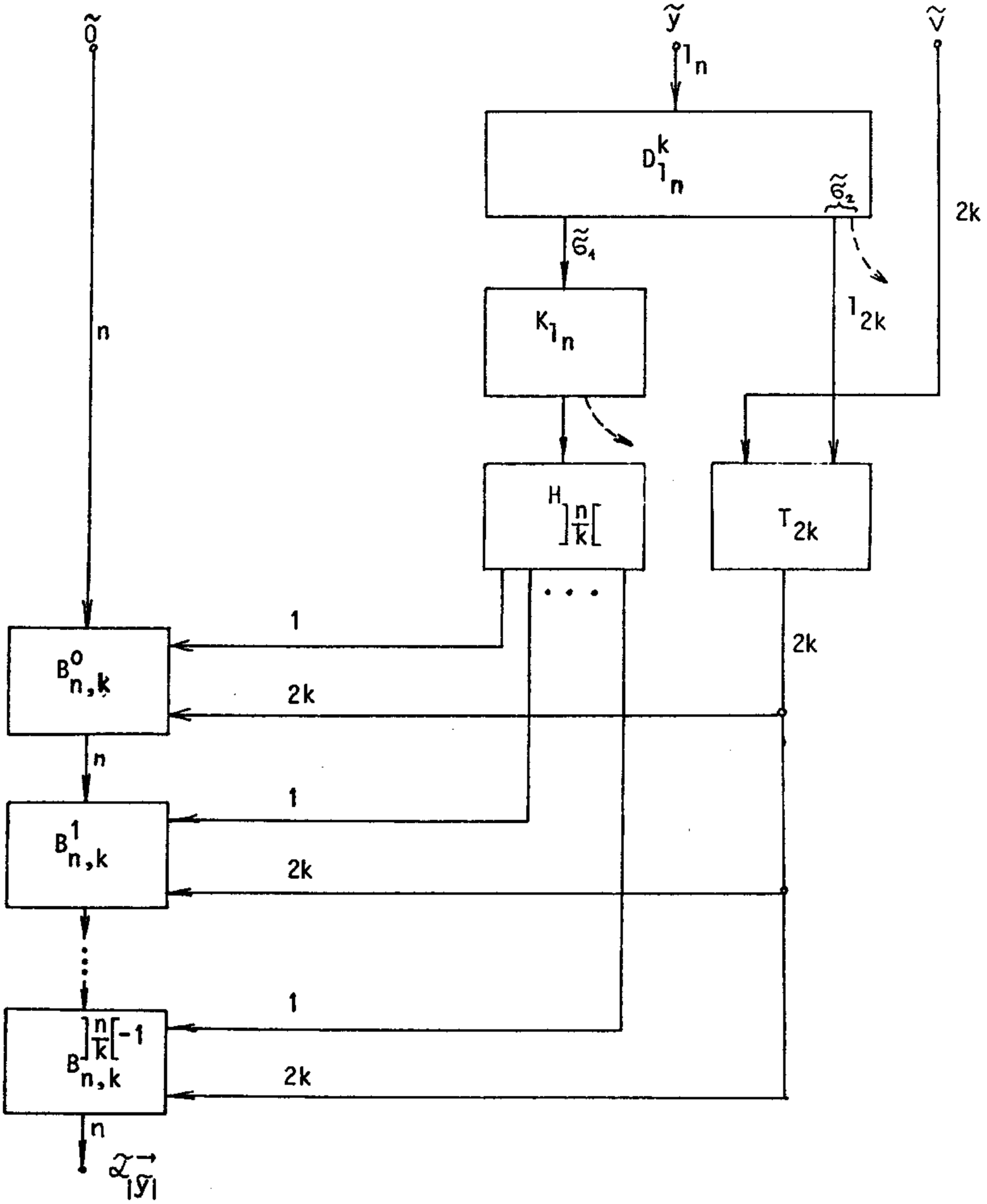
$$L(T_n^{\tilde{\alpha}}) \asymp n .$$

Dokaz. Neka je $\tilde{\alpha}=(\alpha_0,\ldots,\alpha_{n-1})$ periodičan niz slijeva nadesno sa periodom $\tilde{\sigma}=(\sigma_0,\ldots,\sigma_{k-1})$, gdje je $k \leqslant C_1 \frac{n}{\log n}$. Neka je $\tilde{v}=(\sigma_0,\ldots,\sigma_{k-1},0,\ldots,0)$, gdje je broj nula jednak k. Shema za operator $T_n^{\tilde{\alpha}}$ se konstruiše saglasno sledećem algoritmu (vidi sl.9):

1) Niz $\tilde{y}=(y_0,\ldots,y_{1_n-1})$ kojim se zadaje veličina pomjeraja, dovodi se na ulaze sheme $D_{1_n}^k$ koja odredjuje nizove $\tilde{\sigma}_1$ i $\tilde{\sigma}_2$ - bina-

rne zapise brojeva $\left[\frac{|\tilde{y}|}{k}\right]$ i $|\tilde{y}| - \left[\frac{|\tilde{y}|}{k}\right] \cdot k$. $L(D^k_{1_n}) \leqslant C'_d \cdot n$ (lema 3.2.3).

2) Niz $\tilde{v}$ (koji je moguće realizovati sa složenošću $C \cdot k$) i prvih 1_{2k} članova niza $\tilde{G}_2$ dovode se na ulaze sheme T_{2k} koja pomjera niz $\tilde{v}$ za $|\tilde{G}_2|$ mjesta. $L(T_{2k}) \leqslant C_t \cdot 2k \cdot \log 2k$ (lema 2.2.8).



S1.9.

3) Niz $\widetilde{\sigma}_1$ dovedimo na ulaze dešifratora K_{l_n}. $L(K_{l_n}) \leqslant C'_k \cdot n$ (lema 3.2.1).

4) Prvih $\left]\frac{n}{k}\right[$ članova izlaznog niza dešifratora K_{l_n} dovedimo na ulaze sheme $H_{\left]\frac{n}{k}\right[}$. $L(H_{\left]\frac{n}{k}\right[}) \leqslant C'_h \cdot \frac{n}{k}$ (lema 3.2.4). Izlazni niz sheme $H_{\left]\frac{n}{k}\right[}$ označimo sa $\widetilde{\beta}=(\beta_0,\ldots,\beta_{\left]\frac{n}{k}\right[-1})$.

5) Nula niz dužine n, izlaze sheme T_{2k} i i prvi izlaz sheme $H_{\left]\frac{n}{k}\right[}$ (izlaz na kojem se realizuje β_0) dovedimo na ulaze sheme $B^0_{n,k}$, a za $i=1,2,\ldots,\left]\frac{n}{k}\right[-1$ izlaze sheme $B^{i-1}_{n,k}$, izlaze sheme T_{2k} i izlaz sheme $H_{\left]\frac{n}{k}\right[}$ na kojem se realizuje β_i, dovedimo na ulaze sheme $B^i_{n,k}$. Iz leme 3.2.6 sleduje da je za svako $i=0,1,\ldots,\left]\frac{n}{k}\right[-1$, $L(B^i_{n,k}) \leqslant C_b \cdot k$.

Na izlazima sheme $B^r_{n,k}$, $r=\left]\frac{n}{k}\right[-1$, dobili smo niz $\widetilde{\alpha_{\widetilde{y}_1}}$. Na taj način, $L(T^{\widetilde{\alpha}}_n) \leqslant C'_1 \cdot n$. Kako operator $T^{\widetilde{\alpha}}_n$ nema fiktivnih promjenljivih, dobijamo da je $L(T^{\widetilde{\alpha}}_n) \asymp n$, čime je teorema dokazana.

Posledica 3.3.1. Ako je $\widetilde{\alpha} \in B_n$ periodičan niz sdesna nalijevo sa periodom dužine k, $k \leqslant C_2 \cdot \frac{n}{\log n}$, onda je

$$L(T^{\widetilde{\alpha}}_n) \asymp n .$$

Dokaz. Ako je niz $\widetilde{\alpha}$ periodičan sdesna nalijevo sa periodom $\widetilde{y}=(y_0,\ldots,y_{k-1})$, onda je on periodičan i slijeva nadesno sa periodom $\widetilde{y}'=(y_{n-\left[\frac{n}{k}\right]\cdot k-1}, y_{n-\left[\frac{n}{k}\right]\cdot k-2},\ldots,y_1,y_0,y_{k-1},\ldots,y_{n-\left[\frac{n}{k}\right]\cdot k})$ iste dužine, te iz teoreme 3.3.1 i slijedi gornje tvrdjenje.

3.4. N i z o v i s a n e v e l i k i m b r o j e m j e d i n i c a.

U ovom paragrafu ćemo prvo dokazati četiri važne teoreme, a zatim pomoću njih i teoremu o linearnoj realizaciji klase

operatora $T_n^{\tilde{\alpha}}$, odredjenih skupom nizova $\tilde{\alpha}$ koji imaju ne više od $C_3 \cdot \frac{\log n}{\log \log n}$ jedinica [37].

Teorema 3.4.1. Neka je niz $\tilde{\alpha} \in B_n$ takav da izmedju svake dvije susjedne jedinice sadrži barem (k-1) nula, gdje je $k \geqslant C_4 \cdot \log n \cdot \log \log n$. Tada je,

$$L(T_n^{\tilde{\alpha}}) \asymp n.$$

Dokaz. Uvedimo oznake: $k_1 = [\log k]$, $k' = 2^{k_1}$, $\tilde{\gamma} = (\gamma_0, \ldots, \gamma_{l_n - 1})$ - binaran zapis broja (k_1+1) i $\tilde{y} = (y_0, \ldots, y_{l_n - 1})$ - niz kojim se zadaje veličina pomjeraja. Shema koja realizuje operator $T_n^{\tilde{\alpha}}$, gdje je $\tilde{\alpha} \in B_n$ niz koji zadovoljava uslov teoreme, konstruiše se saglasno sledećem algoritmu (vidi sl. 10):

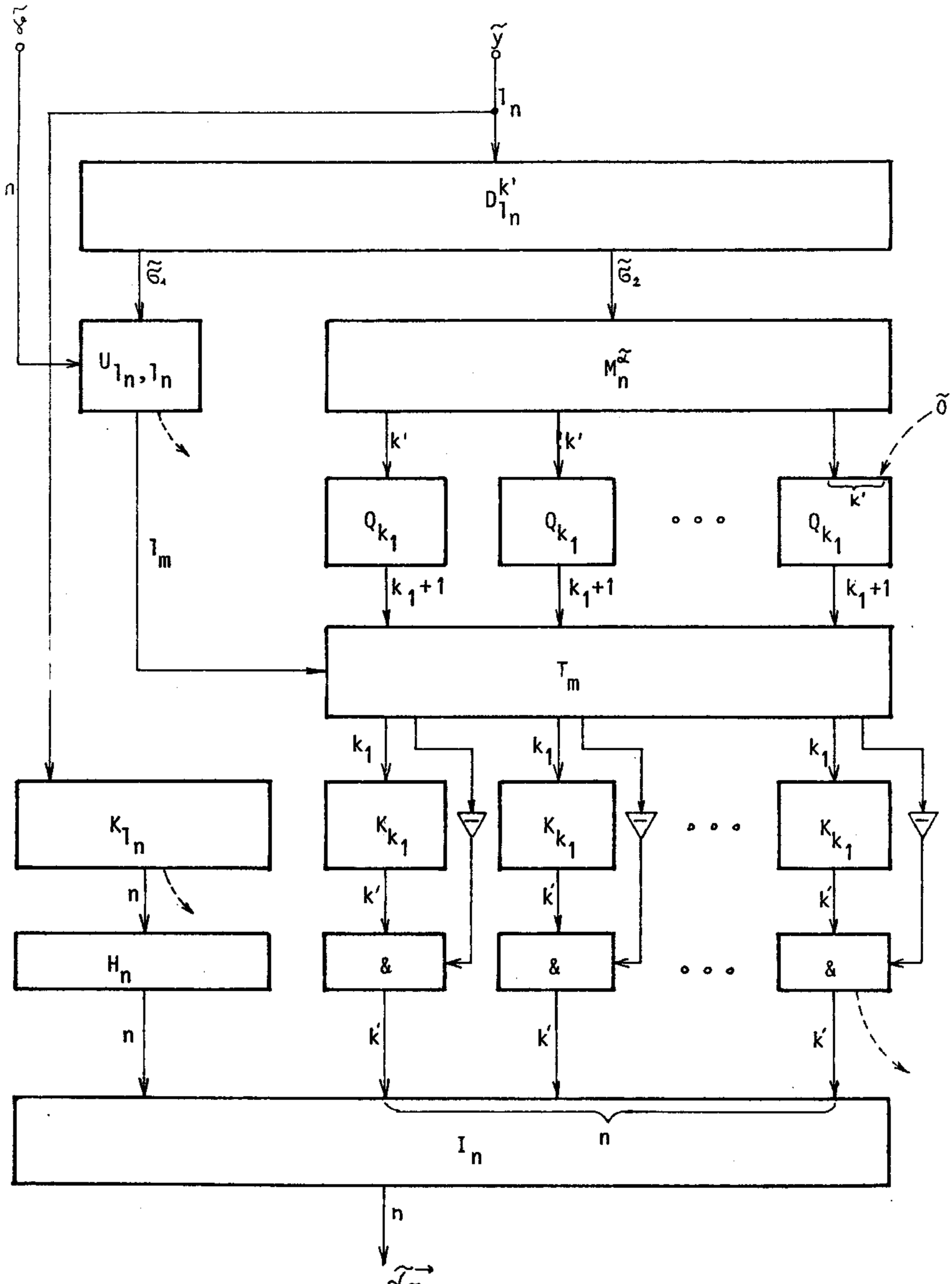
1) Ulazni niz $\tilde{y}$ se dovodi na ulaze sheme $D_{l_n}^{k'}$ koja ga transformiše u nizove $\tilde{\sigma}_1$ i $\tilde{\sigma}_2$ - binarne zapise brojeva $\left[\frac{|\tilde{y}|}{k'}\right]$ i $|\tilde{y}| - \left[\frac{|\tilde{y}|}{k'}\right] \cdot k'$. $L(D_{l_n}^{k'}) \leqslant C'_d \cdot n$ (lema 3.2.3).

2) Niz $\tilde{\sigma}_2$ se dovodi na ulaze sheme $M_n^{\tilde{\alpha}}$, koja pomjera niz $\tilde{\alpha}$ za $|\tilde{\sigma}_2|$ mjesta, $|\tilde{\sigma}_2| < k' \leqslant k \leqslant C \cdot \frac{n}{\|\tilde{\alpha}\|}$. $L(M_n^{\tilde{\alpha}}) \leqslant C_m \cdot n$ (lema 3.2.5).

3) Nizovi $\tilde{\sigma}_1$ i $\tilde{\gamma}$ dovode se na ulaze sheme U_{l_n, l_n}, koja ih množi. $L(U_{l_n, l_n}) \leqslant C'_u \cdot \log^2 n$ (lema 2.2.2).

4) Izlaze sheme $M_n^{\tilde{\alpha}}$ razbijmo slijeva nadesno na $\left]\frac{n}{k'}\right[$ grupa, po k′ izlaza u svakoj (osim, možda, u poslednjoj) i dovedimo ih na ulaze $\left]\frac{n}{k'}\right[$ "kodera" Q_{k_1} (poslednjem "koderu" na preostale slobodne ulaze dovedimo nule!). $L(Q_{k_1}) \leqslant C_q \cdot k'$ (lema 3.2.2).

5) Objedinjujući slijeva nadesno izlaze tih "kodera" (ima ih $m = \left]\frac{n}{k'}\right[(k_1+1))$ dovedimo ih zajedno sa l_m prvih slijeva izlaza sheme U_{l_n, l_n} na ulaze sheme koja realizuje operator T_m, tj. koji pomjera zakodirani niz dobijen na izlazima "kodera" Q_{k_1} za


α_1
$\tilde{y}$
l_n
n
$D^{k'}_{l_n}$
$\tilde{\sigma}_1$
$\tilde{\sigma}_2$
U_{l_n,l_n}
$M^{\tilde{\alpha}}_n$
$\tilde{\sigma}$
k'
k'
k'
Q_{k_1}
Q_{k_1}
Q_{k_1}
l_m
k_1+1
k_1+1
k_1+1
T_m
k_1
k_1
k_1
K_{l_n}
K_{k_1}
K_{k_1}
K_{k_1}
n
k'
k'
k'
H_n
&
&
&
n
k'
k'
k'
I_n
n
n
$\tilde{\alpha}_{|\tilde{y}|}$

Sl. 10.

$\left[\frac{|\tilde{y}|}{k'}\right](k_1+1)$ mjesta nadesno. $L(T_m) \lesssim C_t' \cdot \frac{n}{k'} \cdot k_1 \cdot \log n$ (lema 2.2.8).

6) Izlaze sheme T_m razbijmo slijeva nadesno na $\left]\frac{n}{k'}\right[$ grupa, po (k_1+1) u svakoj. Iz svake grupe, lijevih k_1 izlaza dovedimo na ulaze po jednog dešifratora K_{k_1} i niz dobijen na njegovim izlazima član po član pomnožimo sa poslednjim izlazom u grupi. Označimo sa $\tilde{\beta}$ niz dužine n koji se dobija na lijevih n od $\left]\frac{n}{k'}\right[\cdot k'$, na taj način dobijenih izlaza. $L(K_{k_1}) \lesssim C_k \cdot k'$ (lema 3.2.1).

7) Niz $\tilde{y}$ dovedimo na ulaze dešifratora K_{1_n}. $L(K_{1_n}) \lesssim C_k' \cdot 2^n$ (lema 3.2.1).

8) Izlaze dešifratora K_{1_n} dovedimo na ulaze sheme H_n. $L(H_n) \lesssim C_h n$ (lema 3.2.4).

9) Niz realizovan na izlazima sheme H_n, pomoću sheme operatora I_n, član po član se množi sa nizom $\tilde{\beta}$ dobijenim u koraku 6. $L(I_n) \lesssim C_i \cdot n$ (lema 3.2.7).

Na taj način, imajući u vidu da je $k \geqslant C_4 \cdot \log n \cdot \log \log n$, sleduje da je $L(T_n^{\tilde{\alpha}}) \lesssim C_5 \cdot n$, odnosno $L(T_n^{\tilde{\alpha}}) \asymp n$.

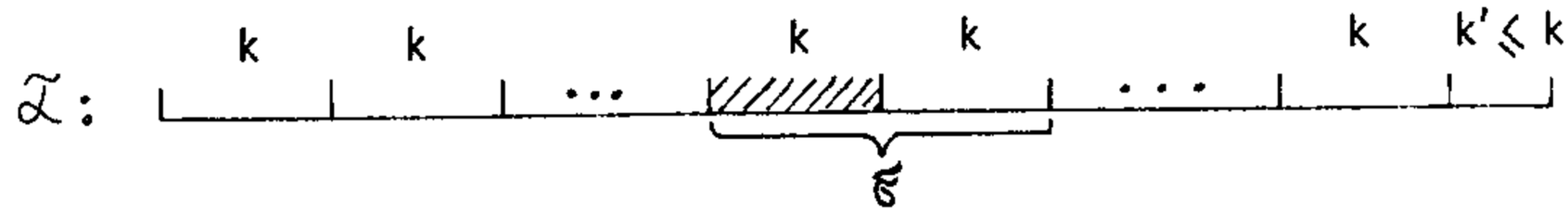
Teorema je dokazana.

Uvedimo jedan pojam. Svaki podniz $(\alpha_i, \alpha_{i+1}, \ldots, \alpha_{i+s})$, niza $\tilde{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ zvaćemo parčetom. Parče ćemo nazivati praznim parčetom ako su mu svi članovi jednaki 0, a nepraznim u suprotnom slučaju.

Teorema 3.4.2. Neka niz $\tilde{\alpha} \in B_n$ zadovoljava sledeći uslov: ako ga, slijeva nadesno, razbijemo na parčad dužine k, $k \lesssim \frac{n}{\log n}$, njegove jedinice se nalaze u ne više od C_6 parčadi. Tada je

$$L(T_n^{\tilde{\alpha}}) \asymp n .$$

Dokaz. Iz leme 3.1.1 sleduje da možemo pretpostaviti da niz $\tilde{\alpha}$ sadrži samo jedno neprazno parče dužine k. Od tog parčeta i praznog parčeta iste dužine, obrazujmo niz $\tilde{\sigma}$ dužine 2k (sl.11).



Sl.11.

Označimo sa $\tilde{y}$ niz kojim se zadaje veličina pomjeraja, sa $\tilde{v}$ niz dužine $]\frac{n}{k}[$, gdje je $v_i=1$ akko je i-to parče niza $\tilde{\alpha}$ neprazno (ima se u vidu da su parčad numerisana slijeva nadesno brojevima $i=0,1,\ldots,]\frac{n}{k}[-1$).

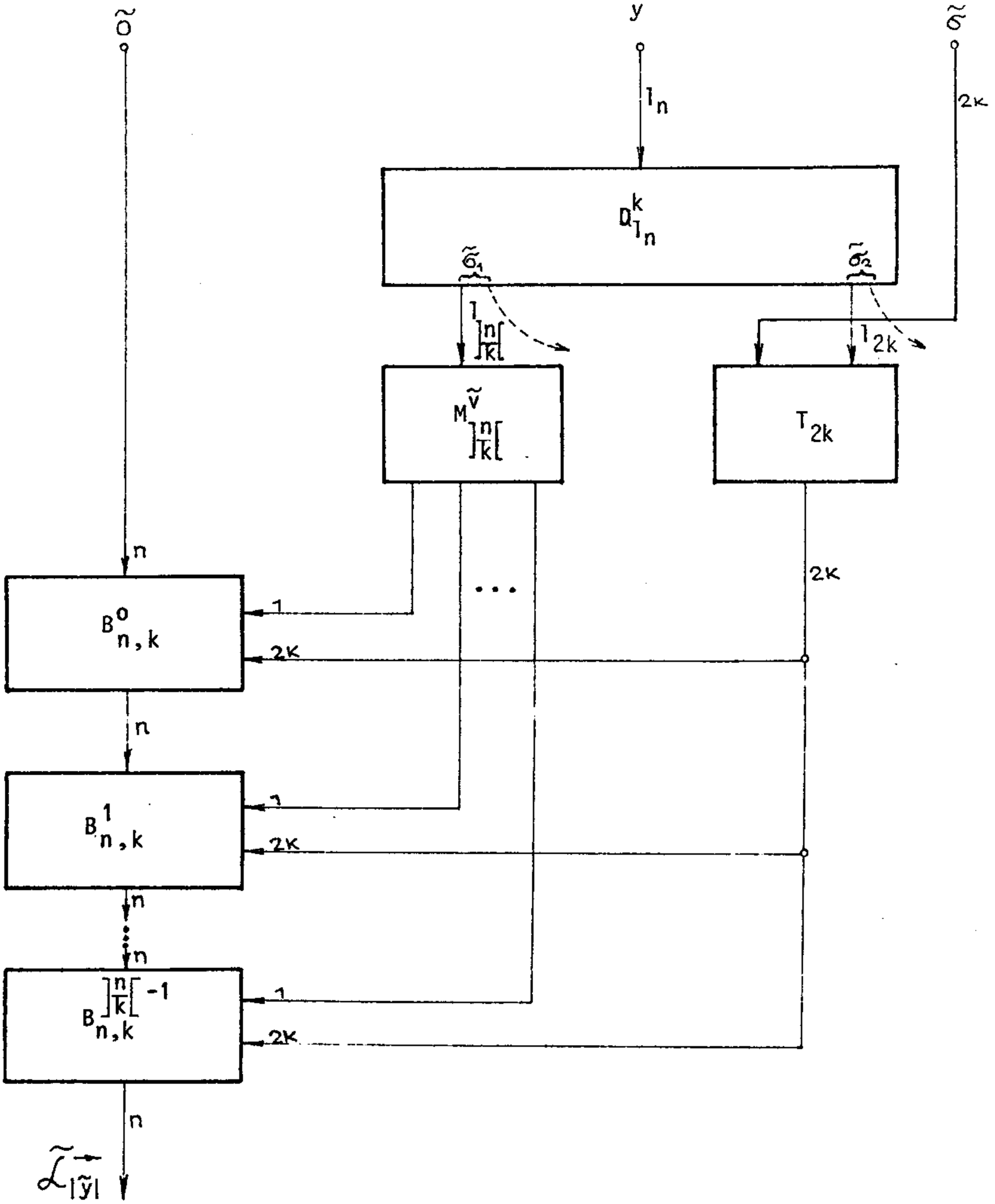
Shema operatora $T^{\tilde{v}}_n$ konstruiše se saglasno sledećem algoritmu (vidi sl.12):

1) Ulazni niz $\tilde{y}$ dovodimo na ulaze sheme $D^k_{l_n}$ koja ga transformiše u nizove $\tilde{\sigma}_1$ i $\tilde{\sigma}_2$ - binarne zapise brojeva $\left[\frac{|\tilde{y}|}{k}\right]$ i $|\tilde{y}| - \left[\frac{|\tilde{y}|}{k}\right]\cdot k$. $L(D^k_{l_n}) \leqslant C'_d\cdot n$ (lema 3.2.3).

2) Niz $\tilde{\sigma}$ i prvih l_{2k} članova niza $\tilde{\sigma}_2$ dovodimo na ulaze sheme koja realizuje operator T_{2k}, tj. koja pomjera niz $\tilde{\sigma}$ za $|\tilde{\sigma}_2|$ mjesta nadesno. $L(T_{2k}) \leqslant C_t\cdot 2k\cdot\log 2k$ (lema 2.2.8).

3) Neka je $m=]\frac{n}{k}[$. Prvih l_m članova niza $\tilde{\sigma}_1$ dovode se na ulaze sheme $M^{\tilde{v}}_m$ koja pomjera niz $\tilde{v}$ za $|\tilde{\sigma}_1|$ mjesta nadesno. Označimo sa $\tilde{\delta}=(\delta_0,\ldots,\delta_{m-1})$ izlazni niz sheme $M^{\tilde{v}}_m$. $L(M^{\tilde{v}}_m)\leqslant C'_m\cdot\frac{n}{k}$ (lema 3.2.5).

4) Pomoću m shema operatora $B^i_{n,k}$, $i=0,1,\ldots,m-1$, "posta-



Sl.12.

vimo" niz realizovan na izlazu sheme T_{2k} na mjesto koje odgovara veličini pomjeraja (ono je ukazano položajem jedinice u

nizu $\widetilde{\delta}$). $L(B^i_{n,k}) \leqslant C_b \cdot k$, $i=0,1,\ldots,m-1$ (lema 4.2.6).

Na taj način,

$$L(T_n) \leqslant C'_d \cdot n + C_t \cdot 2k \cdot \log 2k + C'_m \cdot \frac{n}{k} + \frac{n}{k} \cdot C'_b \cdot k \leqslant C_7 \cdot n .$$

Imajući u vidu donju trivijalnu ocjenu, dobijamo

$$L(T^{\widetilde{\alpha}}_n) \asymp n .$$

Teorema je dokazana.

Teorema 3.4.3. Neka niz $\widetilde{\alpha} \in B_n$ ispunjava sledeći uslov: moguće ga je razbiti slijeva nadesno na parčad dužine k (dužina poslednjeg parčeta može biti $\leqslant k$), $k \geqslant C_8 \cdot \log n \cdot \log \log n$, tako da izmedju svaka dva susjedna neprazna parčeta, praznih parčadi ima više nego jedinica u desnom od ta dva neprazna parčeta. Tada je

$$L(T^{\widetilde{\alpha}}_n) \asymp n .$$

Dokaz. Neka niz $\widetilde{\alpha}$ zadovoljava uslov teoreme. Transformisaćemo ga pomjeranjem njegovih jedinica tako da dobijemo niz $\widetilde{\beta}$ koji zadovoljava uslov teoreme 3.4.1, njega s linearnom složenošću pomjeriti, i onda, transformacijama inverznim početnim, ustanoviti pomjereni niz $\widetilde{\alpha}$. Opišimo sada to detaljno.

Posmatrajmo proizvoljno neprazno parče u nizu $\widetilde{\alpha}$. Označimo sa l broj jedinica u njemu. Prema uslovu teoreme, lijevo od tog parčeta postoji barem (l+1)-no prazno parče. Jedinice iz nepraznog parčeta razmjestimo po tim praznim parčadima na sledeći način: poslednju jedinicu, gledano slijeva nadesno, pomjerimo ulijevo za k mjesta, predposlednju za 2k mjesta itd., l-tu za $l \cdot k$ mjesta. Ako to uradimo sa svakim nepraznim parčetom niza $\widetilde{\alpha}$, dobićemo niz $\widetilde{\beta}$ o kojem smo govorili na početku dokaza.

Razbijmo tako dobijeni niz $\tilde{\beta}$ slijeva nadesno na parčad dužine k. Nije teško vidjeti da niz $\tilde{\beta}$ ima sledeća svojstva:

1) Svako njegovo parče sadrži najviše jednu jedinicu.

2) Broj nula izmedju dvije susjedne jedinice u nizu je $>k$.

3) Susjedne jedinice u nizu $\tilde{\beta}$ koje potiču od susjednih jedinica koje se nalaze u jednom parčetu niza $\tilde{\alpha}$, leže u susjednim parčadima niza $\tilde{\beta}$.

4) Susjedne jedinice u nizu $\tilde{\beta}$ koje potiču od susjednih jedinica koje se nalaze u raznim parčadima niza $\tilde{\alpha}$, leže u parčadima niza $\tilde{\beta}$ izmedju kojih postoje barem dva prazna parčeta.

Zbog jednoznačnosti dekodiranja, "produžimo" niz $\tilde{\beta}$ nadesno praznim parčetom dužine $(\left]\frac{n}{k}\right[+1)\cdot k-n$. Dobijeni niz označimo sa $\tilde{\beta}'$. Sada možemo preći na opis algoritma, saglasno kojem ćemo i konstruisati shemu operatora $T_n^{\tilde{\alpha}}$ (vidi sl.14):

1) Niz $\tilde{y}$ kojim se zadaje veličina pomjeraja dovodi se na ulaze sheme koja realizuje operator $T_m^{\tilde{\beta}'}$, $m=(\left]\frac{n}{k}\right[+1)\cdot k$. Kako niz $\tilde{\beta}'$ zadovoljava uslov teoreme 3.4.1, to je $L(T_m^{\tilde{\beta}'})\leqslant C_5'\cdot n$.

2) Izlaze te sheme razbijmo, slijeva nadesno, na $\left]\frac{n}{k}\right[+1$ zonu, po k izlaza u svakoj. Označimo sa $\tilde{\nu}_i$ niz koji se realizuje u i-toj zoni, $i=1,2,\ldots,\left]\frac{n}{k}\right[+1$. Nizovi $\tilde{\nu}_i$, $i=1,2,\ldots,\left]\frac{n}{k}\right[+1$, dovode se na isto toliko disjunktivnih shema V_i koje utvrdjuju prisustvo jedinice u i-toj zoni, tj. izračunavaju signale (funkcije) $t_i=\bigvee_{j=o}^{k-1}\nu_{ij}$. Očigledno, za svako i, $L(V_i)\leqslant k$.

3) Na osnovu signala t_j, $j=1,\ldots,\left]\frac{n}{k}\right[+1$, sheme R^i, $i=1,\ldots,\left]\frac{n}{k}\right[$ izračunavaju signale r_i, gdje je $r_i=0$ u slučaju da

jedinicu iz i-te zone treba prenijeti u lijevo parče sakupljača (vidi korak 5 i sl.14), i r_i=1 kada tu jedinicu treba prenijeti u desno parče sakupljača (u slučaju kada su jedinice iz nepraznog parčeta niza $\tilde{\alpha}$ poslije pomjeranja djelimično prekrile dva parčeta dužine k). Nije teško provjeriti da mora biti:

$$r_1=0$$

$$r_{i+1}=\bar{r}_i t_i \bar{t}_{i+1} t_{i+2} \vee r_i t_{i+1}, \quad i=1,2,\ldots, \left]\frac{n}{k}\right[-1 .$$

Na taj način, $L(R^i) \leqslant C_{11}$ za svako i.

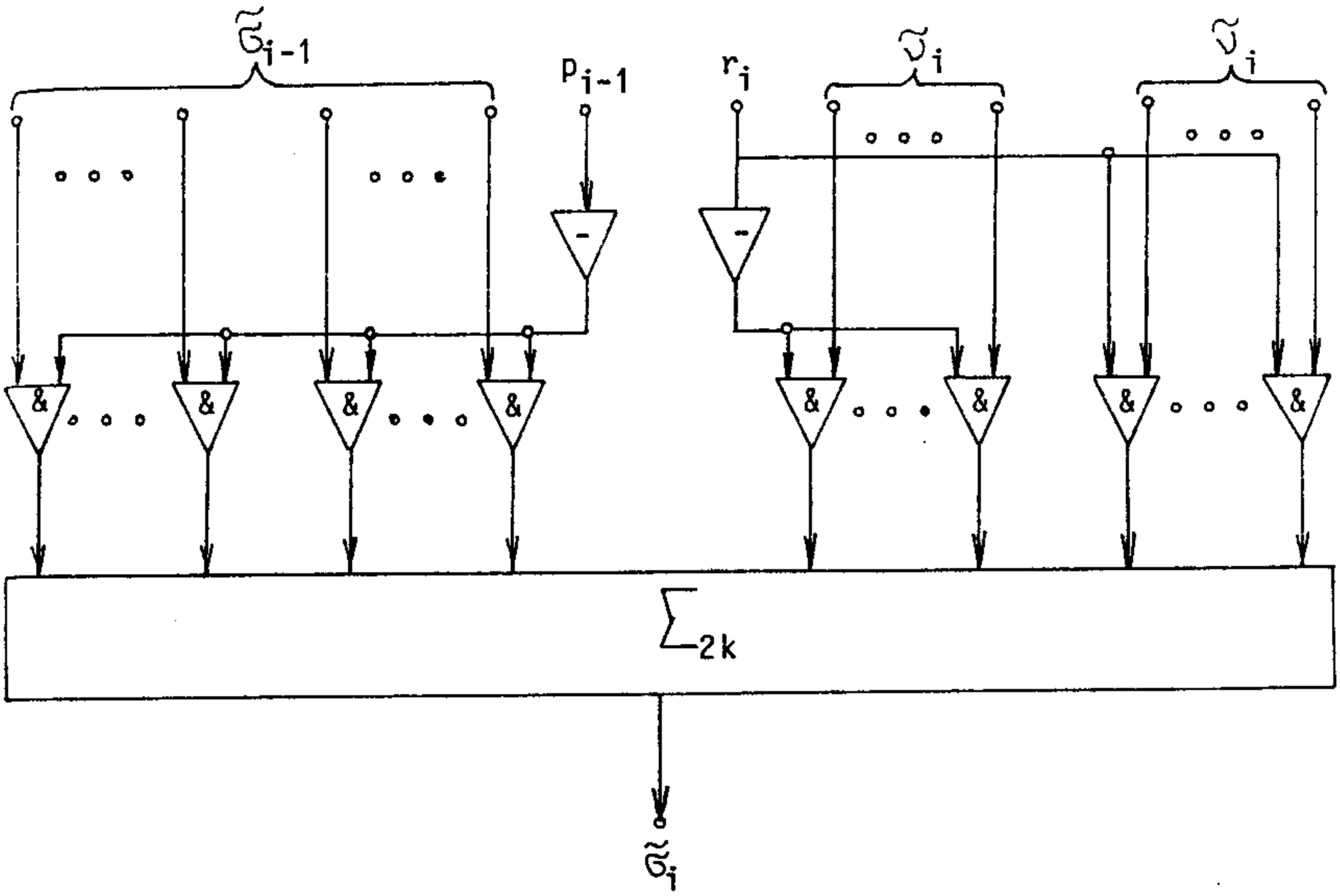
4) Na osnovu signala t_1, $1=1,2,\ldots,\left]\frac{n}{k}\right[+1$ i r_j $j=1,\ldots,\left]\frac{n}{k}\right[$ sheme P^i, $i=1,\ldots,\left]\frac{n}{k}\right[$ izračunavaju signale p_i, gdje je p_i=1 kada u i-to i (i+1)-vo parče niza koji formiramo polazeći od nula niza dužine m, treba postaviti sakupljač (zato što smo jedinice koje smo sakupljali "vratili" na mjesto odredjeno pomjerajem niza $\tilde{\alpha}$) i p_i=0 u ostalim slučajevima. Nije teško provjeriti da mora biti:

$$p_i = \bar{t}_i \bar{t}_{i+1} \vee t_i \bar{t}_{i+1} r_i , \quad i=1,\ldots, \left]\frac{n}{k}\right[,$$

odakle i sleduje ocjena $L(P^i) \leqslant C_{12}$, za svako i.

5) Za svako i, $i=1,\ldots,\left]\frac{n}{k}\right[$ konstruiše se shema W_i koja odredjuje niz $\tilde{\sigma}_i$ dužine 2k, tj. sakupljač. Detaljnije, shema W_i zavisno od vrijednosti signala r_i, propušta jedinicu iz i-te zone (niza $\tilde{\upsilon}_i$) u lijevo ili desno parče niza $\tilde{\sigma}_{i-1}$, pomnoženog prethodno, član po član sa p_{i-1} (vidi sl.13). Za $\tilde{\sigma}_0$ se uzima nula niz dužine 2k,i p_0=1. Očigledno je,

$$L(W_i) \leqslant C'_W \cdot k + L(\sum_{2k}) \leqslant C_W \cdot k .$$

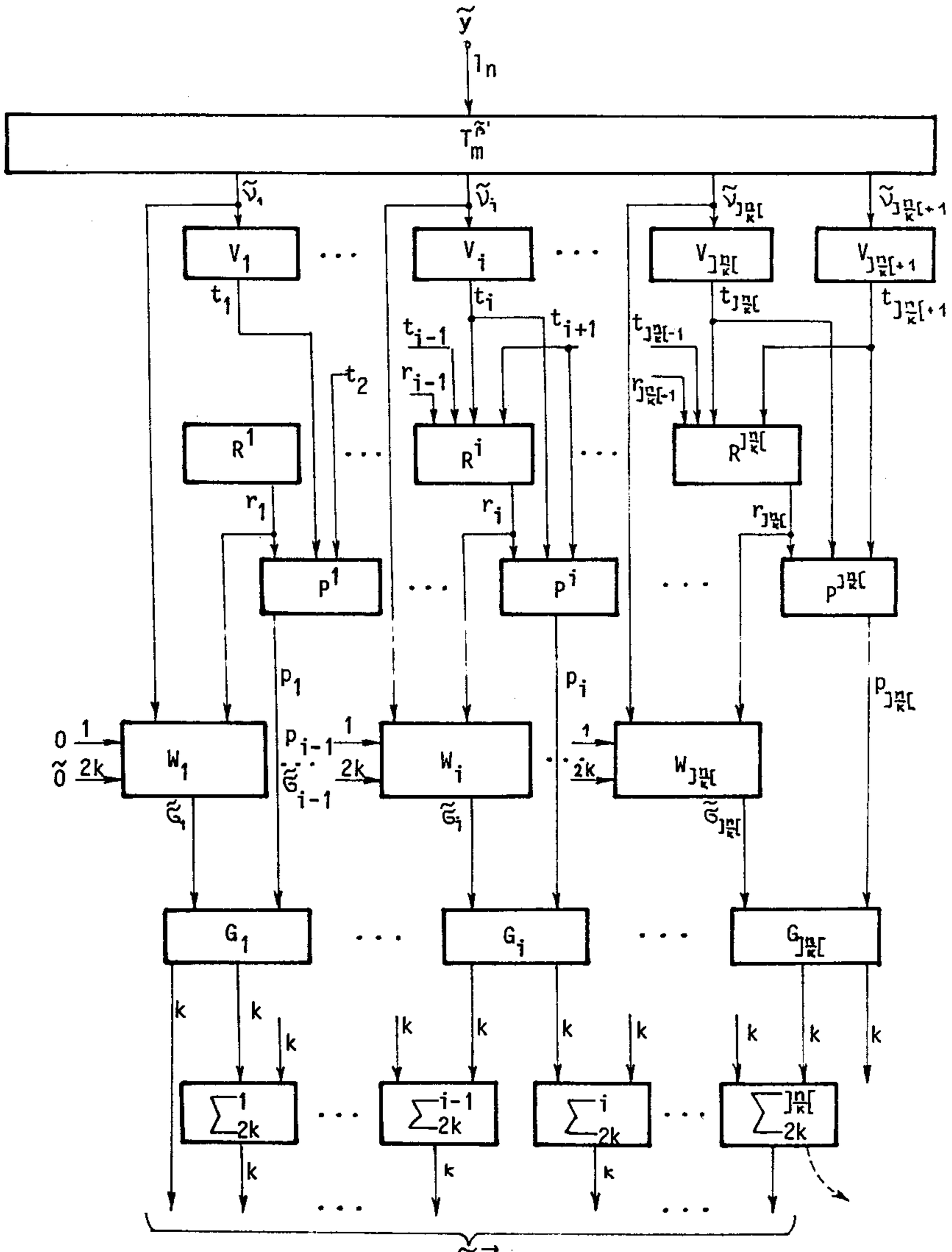


Sl.13.

6) Za svako i, niz $\tilde{\sigma}_i$ množi se član po član sa p_i pomoću $]\frac{n}{k}[$shema G_i. Očigledno je $L(G_i) \leqslant C_{13} \cdot k$, za svako $i=1,\ldots,]\frac{n}{k}[$.

7) Označimo sa $\tilde{\sigma}'_i$ nizove koji se dobijaju na izlazima shema G_i, $i=1,\ldots,]\frac{n}{k}[-1$. Pomoću $]\frac{n}{k}[-1$ shema $\sum_{2k}^{i}$ koje realizuju operator $\sum_{2k}$, sumiraćemo član po član desno parče niza $\tilde{\sigma}'_i$ s lijevim parčetom niza $\tilde{\sigma}'_{i+1}$. Iz leme 3.2.8 dobijamo da je za svako i, $i=1,\ldots,]\frac{n}{k}[-1$, $L(\sum_{2k}^{i}) \leqslant C_g k$.

Objedinjujući, slijeva nadesno lijevih k izlaza sheme G_1 sa izlazima shema $\sum_{2k}^{i}$, $i=1,\ldots,]\frac{n}{k}[-2$ i prvih $n-(]\frac{n}{k}[-1)k$ izlaza sheme $\sum_{2k}^{m_1}$, $m_1 =]\frac{n}{k}[-1$, dobijamo na tim objedinjenim izlazima niz $\tilde{\alpha}_{|\vec{\tilde{y}}|}$.


$\tilde{y}$
l_n
$T_m^{\tilde{n}'}$
$\tilde{v}_1$
$\tilde{v}_i$
$\tilde{v}_{]\frac{n}{k}[}$
$\tilde{v}_{]\frac{n}{k}[+1}$
V_1
V_i
$V_{]\frac{n}{k}[}$
$V_{]\frac{n}{k}[+1}$
t_1
t_i
t_{i-1}
t_{i+1}
$t_{]\frac{n}{k}[}$
$t_{]\frac{n}{k}[+1}$
$t_{]\frac{n}{k}[-1}$
t_2
r_{i-1}
$r_{]\frac{n}{k}[-1}$
R^1
R^i
$R^{]\frac{n}{k}[}$
r_1
r_i
$r_{]\frac{n}{k}[}$
P^1
P^i
$P^{]\frac{n}{k}[}$
p_1
p_i
$p_{]\frac{n}{k}[}$
0 1
$\tilde{0}$ 2k
W_1
W_i
$W_{]\frac{n}{k}[}$
p_{i-1}
$\tilde{G}_{i-1}$
$\tilde{G}_1$
$\tilde{G}_i$
$\tilde{G}_{]\frac{n}{k}[}$
G_1
G_i
$G_{]\frac{n}{k}[}$
k
$\sum_{2k}^{1}$
$\sum_{2k}^{i-1}$
$\sum_{2k}^{i}$
$\sum_{2k}^{]\frac{n}{k}[}$
$\tilde{\mathcal{L}}_{|\tilde{y}|}$

S1.14.

Na taj način, sumirajući navedene složenosti svih algoritamskih koraka dobijamo $L(T_n^{\tilde{\alpha}}) \leqslant C_{20} \cdot n$ odnosno $L(T_n) \asymp n$.

Teorema je dokazana.

Teorema 3.4.4. Svaki niz $\tilde{\alpha} \in B_n$, $\|\tilde{\alpha}\| = k$, možemo razložiti na, član po član sumu po mod 2 dva niza: jedan od njih zadovoljava uslov teoreme 3.4.3, a kod drugog je broj članova izmedju prve i poslednje jedinice $< k^k \cdot M$, gdje je $M = \log n \cdot \log\log n$.

Dokaz. Razbijmo jedinice u nizu $\tilde{\alpha}$ na grupe tako da izmedju susjednih jedinica svake grupe bude manje od M nula, a izmedju susjednih jedinica raznih grupa bude $\geqslant M$ nula. Očigledno je broj grupa $\leqslant k$. Posmatrajmo parčad niza $\tilde{\alpha}$ minimalne dužine koja sadrže po jednu i samo jednu od dobijenih grupa jedinica. Označimo sa D_1 dužinu najdužeg od tih parčadi. Sada ćemo navesti algoritam kojim ćemo objedinjavati "kraća" parčad u "duža".

1) Uočimo poslednju (gledano slijeva nadesno) jedinicu u nizu $\tilde{\alpha}$ i stavimo i=1.

2) Posmatrajmo parče niza $\tilde{\alpha}$ dužine D_i koje sadrži tu jedinicu i D_i-1 član niza lijevo od nje. Označimo sa p broj jedinica u tom parčetu, a sa r dužinu maksimalnog susjednog praznog parčeta niza koje se nalazi lijevo od posmatranog parčeta. Ispituje se da li je $r \geqslant (p+1)\, D_i$? Ako je nejednakost ispunjena prelazimo na korak 3, ako nije, na korak 4.

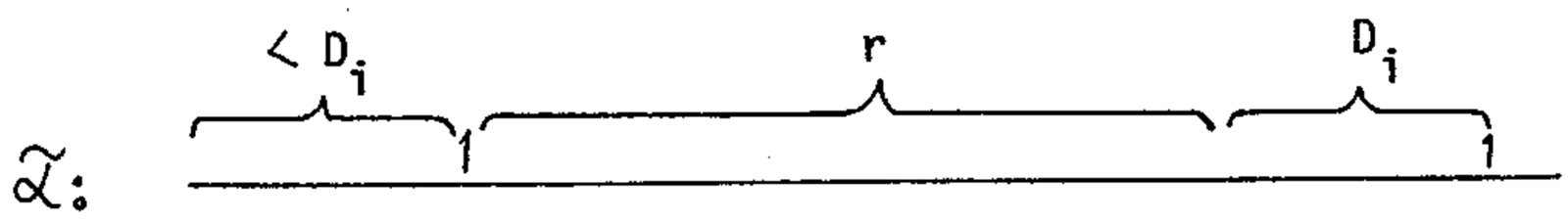
3) Imamo dvije mogućnosti:

a) ako postoji još jedinica lijevo od posmatranog parčeta, uočimo prvu od njih (sdesna nalijevo) i predjimo na korak 2;

b) ako lijevo nema više jedinica, algoritam se zaustavlja i očigledno niz $\tilde{\alpha}$ zadovoljava uslov teoreme 3.4.3.

4) Nejednakost $r \geqslant (p+1)\cdot D_i$ neće biti ispunjena u jednom od sledeća dva slučaja:

a) postoji jedinica u nizu $\tilde{\alpha}$ lijevo od posmatranog parčeta zbog koje je $r < (p+1)\cdot D_i$. U tom slučaju, produžimo posmatrano parče ulijevo dok ne uključimo u njega (staro) parče u kojem se nalazi ta jedinica (vidi sl.15).



Sl.15.

Označimo dužinu, tako dobijenog (novog) parčeta sa D_{i+1}. Očigledno je,

$$D_{i+1} < D_i + r + D_i < (p+3)\cdot D_i .$$

Vratimo se opet poslednjoj (gledano slijeva nadesno) jedinici u nizu $\tilde{\alpha}$, no već sa novim D_i (i je za jedinicu veće) i prelazimo na korak 2;

b) ne postoji jedinica lijevo od posmatranog parčeta. Algoritam se zaustavlja.

Na taj način, algoritam se zaustavlja ili poslije koraka 3b i niz $\tilde{\alpha}$ zadovoljava uslov teoreme 3.4.3, ili poslije koraka 4b kada niz $\tilde{\alpha}$ možemo razložiti na član po član sumu po mod 2 nizova od kojih jedan zadovoljava uslov teoreme 3.4.3 (to je parče niza $\tilde{\alpha}$ od jedinice, ne uključujući je, kod koje je narušeno

ispunjenje uslova $r \geqslant (p+1)\cdot D_i$, pa do kraja niza $\tilde{\alpha}$, produženo nalijevo nulama do ukupne dužine n), a kod drugog je broj članova izmedju krajnjih jedinica $< D_j$, za neko j. Nije teško uočiti, da se pri svakom ispunjenju koraka 4a algoritma broj posmatranih parčadi u nizu $\tilde{\alpha}$ smanjuje barem za 1. Slijedi, $j < k$. Kako je,

$$D_{i+1} < (p+3)\cdot D_i \quad , \quad D_1 < k\cdot M$$

dobijamo

$$D_j < k^k \cdot M \ , \quad \text{za svako } j.$$

Teorema je dokazana.

Uvedimo oznake:

$$V_{n,k} = \{\tilde{\alpha} \mid \tilde{\alpha} \in B_n \ , \ \|\tilde{\alpha}\| = k\} \ , \quad \mathcal{T}_A = \{T_n^{\tilde{\alpha}} \mid \tilde{\alpha} \in A \subseteq B_n\}.$$

Teorema 3.4.5. Za svako k, $k \leqslant C_{45}\cdot \frac{\log n}{\log \log n}$,

$$L(\mathcal{T}_{V_{n,k}}) \asymp n \ .$$

Dokaz. Neka je $T_n^{\tilde{\alpha}} \in \mathcal{T}_{V_{n,k}}$ i $k \leqslant C_{45}\cdot \frac{\log n}{\log \log n}$. Imajući u vidu lemu 3.1.1 možemo pretpostaviti da je $k \leqslant \frac{\log n}{\log \log n}$. Otuda je

$$k^k \cdot M < C_{46} \frac{n}{\log n} \ .$$

Primjenom teoreme 3.4.4, a zatim teorema 3.4.3 i 3.4.2, dobijamo tvrdjenje teoreme 3.4.5.

3.5. N a j s l o ž e n i j i n i z o v i

Dolazimo do momenta kada je prirodno postaviti sledeće suštinsko pitanje: kakva svojstva imaju operatori $T_n^{\tilde{\alpha}}$ koji ne zadovoljavaju uslove prethodnih teorema, odnosno za koje se tehnikom i metodima izloženim u prethodnim paragrafima ne može dokaza-

ti linearna složenost. Nije teško vidjeti da su to neperiodični nizovi sa približno jednakim brojem nula i jedinica. Jednom skupu takvih nizova, a naime, u intuitivnom smislu možemo reći najsloženijih, posvećujemo ovaj paragraf i dokazujemo linearnu složenost operatora T_n^{α} definisanih tim nizovima. Radi prostijeg označavanja, u ovom paragrafu ćemo, umjesto nizova dužine n posmatrati nizove dužine 2^n, n=1,2,... . Napominjem da time ne činimo nikakvo suštinsko ograničenje jer nas ovdje interesuje samo red složenosti. (Shema operatora odredjenog nizom čija dužina nije stepen dvojke, dobija se odbacivanjem odredjenog broja izlaza u shemi operatora odredjenog nizom dužine 2^n i, eventualno, primjenom leme 3.1.1).

40-ih godina ovog vijeka I.K.Postumus je, vezano za jedan problem u teoriji informacija,definisao tzv. P_n-cikluse kao nizove nula i jedinica dužine 2^n koji, ako se rasporede po krugu zadovoljavaju sledeći uslov: svih 2^n mogućih uredjenih n-torki nula i jedinica koje obrazuju n uzastopnih članova niza su medjusobno različite. Tako na primjer, P_3-ciklus 00010111 sadrži sve moguće uredjene trojke (00010111, 00101110 itd. posmatraju se kao jedan isti ciklus!).

Za n=1,2,3,4 svi P_n-ciklusi se mogu lako naći. Postoji samo jedan P_1-ciklus, a naime 01, jedan P_2-ciklus 0011, dva P_3-ciklusa 00010111 i 11101000 i šesnaest P_4-ciklusa. Postumus je našao da je broj P_5-ciklusa jednak 2048, i na taj način, za n=1,2,3,4,5 dobio sledeće brojeve P_n-ciklusa:

$$1 , 1 , 2 , 2^4 , 2^{11} ,$$

zbog čega je i dao hipotezu da je broj P_n-ciklusa jednak

$$2^{2^{n-1}-n} .$$

Tačnost hipoteze je dokazao de Bruijn N.G. [24].

P'_n-ciklusom nazvaćemo niz dužine 2^n-1 koji se dobija iz P_n-ciklusa izbacivanjem jedne od n uzastopnih nula. Dakle, P'_n-ciklus sadrži sve uredjene n-torke kao parčad dužine n, izuzimajući n-torku sastavljenu samo od nula.

Primjedba 3.5.1. Jasno je da jedan P_n (P'_n)-ciklus odredjuje 2^n (2^n-1) nizova iz B_{2^n} (B_{2^n-1}). Za svaki od njih ćemo govoriti da predstavlja P_n (P'_n)-ciklus.

Prije nego što opišemo jednu klasu P_n-ciklusa koja odredjuje operatore pomjeranja linearne složenosti, napomenućemo, ukratko, neka svojstva konačnih polja (detaljnije vidjeti u [23], [31], [32]).

Neka je $B_1=\{0,1\}$. Struktura $(B_1,\oplus,\cdot)$ u odnosu na operacije $\oplus$ - sabiranje po mod 2 i $\cdot$ - množenje (konjunkcija) čini polje reda 2 (redom polja se naziva broj elemenata polja).

Označimo sa $R_2(x)$ skup polinoma od promjenljive x nad poljem $(B_1,\oplus,\cdot)$. Poznato je da za svaki prirodan broj n u $R_2(x)$ postoji nesvodljiv polinom $f(x)=x^n+C_{n-1}x^{n-1}+\ldots+C_1x+1$, tj. polinom kojeg je nemoguće predstaviti kao proizvod dva polinoma iz $R_2(x)$ stepeni većih od nule. Uočimo podskup $R_2^n(x)$ polinoma iz $R_2(x)$ čiji je stepen manji od n. Očigledno, $R_2^n(x)$ se sastoji iz 2^n polinoma. Sumom polinoma $a(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ i $b(x)=b_0+b_1x+\ldots+b_{n-1}x^{n-1}$ nazvaćemo polinom $c(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$, gdje je $c_i = a_i \oplus b_i$, $i=0,\ldots n-1$, a proizvodom - ostatak pri dijeljenju polinoma $a(x)\cdot b(x)$ sa $f(x)$. Koristeći nesvodljivost polinoma $f(x)$ može se pokazati da skup $R_2^n(x)$ polinoma stepena manjeg od n čini polje reda 2^n u odnosu na ove dvije operacije.

Lema 3.5.1. [23] Sva konačna polja istog reda su izomorfna.

Konstruisano polje reda 2^n se obično označava sa $GF(2^n)$ (Galois Field).Saglasno tome, polje $(B_1,\oplus,\cdot)$ se označava sa GF(2). Na taj način, izbor odredjenog nesvodljivog polinoma stepana n radi konstrukcije polja $GF(2^n)$ vezan je samo za numeraciju elemenata polja.

Lema 3.5.2. [23] Konačno polje je vektorski prostor nad bilo kojim svojim podpoljem.

Na taj način, polje $GF(2^n)$ polinoma stepena manjeg od n je vektorski prostor dimenzije n nad poljem GF(2).

Jedno od najvažnijih specifičnih svojstava konačnih polja koje ih i razlikuje od beskonačnih je sadržano u sledećem tvrdjenju.

Lema 3.5.3. [23] Neka je F konačno polje reda q i F^* skup svih q-1 nenula elemenata polja F. F^* je ciklična multiplikativna grupa reda q-1.

Neka je α generatorni elemenat ciklične grupe $GF^*(2^n)$. Elemenat α polja $GF(2^n)$ naziva se primitivnim, ako je njegov red jednak 2^n-1 (red elementa a multiplikativne grupe je minimalno r takvo da je $a^r=1$). Dakle, svako konačno polje sadrži primitivni elemenat.

Neka je $\varphi(n)$ funkcija Euler-a definisana za svaki prirodan broj n kao broj brojeva manjih od n koji su uzajamno prosti sa n. Nije teško pokazati da je

$$\varphi(n) = n\cdot\prod_{p\mid n}(1-\frac{1}{p}),$$

gdje p prolazi skupom prostih djelilaca broja n.

Lema 3.5.4. 23 Broj primitivnih elemenata polja $GF(2^n)$ jednak je $\varphi(2^n-1)$.

S obzirom da svaki elemenat polja $GF(2^n)$ zadovoljava jednačinu

$$X^{2^n} - X = 0 ,$$

to se za svaki elemenat α tog polja definiše minimalan polinom $m_\alpha(x)$ - to je normiran polinom (s najstarijim koeficijentom jednakim 1) s koeficijentima iz GF(2) najmanjeg mogućeg stepena takav da je $m_\alpha(\alpha) = 0$. Nije teško pokazati da je stepen minimalnog polinoma primitivnog elementa polja $GF(2^n)$ jednak n. Takav polinom se naziva primitivnim.

Lema 3.5.5. Neka je f(x) primitivan polinom stepena n i neka je $GF(2^n)$ konačno polje polinoma stepena manjeg od n nastalo sječenjem prstena svih polinoma $R_2(x)$ sa f(x) (na gore opisani način). Tada je elemenat $\alpha = x$ primitivni elemenat polja $GF(2^n)$.

Dakle, nenula elementi polja $GF(2^n)$ obrazuju multiplikativnu cikličnu grupu, pri čemu, ako se u svojstvu nesvodljivog polinoma f(x) uzme primitivan polinom, tada su svi nenula elementi polja stepeni elementa $\alpha = x$.

Označimo sa $\mathcal{L}_f$ niz $(\alpha_0, \ldots, \alpha_{2^n-2})$, gdje je α_i slobodan član polinoma koji se dobija kao ostatak pri dijeljenju polinoma x^i sa primitivnim polinomom f(x) stepena n, $i=0,\ldots,2^n-2$.

Teorema 3.5.1. Niz $\tilde{\mathcal{L}}_f$, gdje je f primitivan polinom stepena n, predstavlja P_n' - ciklus.

Dokaz. Neka je $f(x)=x^n+C_{n-1}x^{n-1}+\ldots+C_1x+C_0$ primitivan polinom stepena n i neka je

$$D^i_{n-1}\cdot x^{n-1} + D^i_{n-2}\cdot x^{n-2} + \ldots + D^i_1\cdot x + D^i_0$$

ostatak pri dijeljenju polinoma x^i sa $f(x)$. Iz algoritma dijeljenja polinoma dobijamo sledeće relacije:

$$D_{n-j}^{i+1} = D_{n-1}^{i} \cdot C_{n-j} + D_{n-j-1}^{i} \ , \ j=1,2,\ldots,n-1$$

i

$$D_{o}^{i+1} = D_{n-1}^{i} \cdot C_{o} \ .$$

Otuda sleduje, za svako k,

$$D_{n-j}^{k+n} = \sum_{i=1}^{n-j+1} D_{n-1}^{k+n-i} \cdot C_{n-j+1-i}$$

$$= \sum_{i=1}^{n-j+1} D_{o}^{k+n-i+1} \cdot C_{n-j+1-i} \ , \ j=1,2,\ldots,n \ , \tag{1}$$

gdje sve gornje indekse treba uzeti po mod (2^n-1).

Pretpostavimo da niz D_o^o, D_o^1, ... , $D_o^{2^n-2}$ ne predstavlja P_n' - ciklus. To znači da postoje l i m, $l \neq m$, takvi da je

$$D_{o}^{l+i} = D_{o}^{m+i} \ , \ i=1,2,\ldots,n.$$

Otuda i iz relacije (1) sleduje da je

$$D_{n-j}^{l+n} = D_{n-j}^{n+m} \ , \quad j=1,2,\ldots,n.$$

Dakle, ostaci pri dijeljenju polinoma x^{l+n} i x^{m+n} sa $f(x)$, $l \neq m$, su jednaki, što je nemoguće zbog leme 3.5.5.

Teorema je dokazana.

Označimo sa $\mathcal{Z}_f^k$, $k=0,1,\ldots,2^n-2$ niz $\mathcal{Z}_f$ ciklično pomjeren nalijevo za k mjesta. Nije teško uočiti da je $\mathcal{Z}_i^k$ - i-ti član niza $\mathcal{Z}_f^k$, slobodan član ostatka pri dijeljenju polinoma x^{i+k} sa primitivnim polinomom $f(x)$, $i=0,1,\ldots,2^n-2$. Dakle, $\mathcal{Z}_f = \mathcal{Z}_f^o$. Svi nizovi $\mathcal{Z}_f^k$, $k=0,1,\ldots,2^n-2$, pri fiksiranom primitivnom polinomu $f(x)$ stepena n, predstavljaju jedan isti P_n'-ciklus.

Teorema 3.5.2. [40] Za svaki primitivan polinom f(x) stepena n i svako k, $k=0,1,\ldots,2^n-2$,

$$L(T^{\mathcal{L}_f^k}_{2^n-1}) \asymp 2^n .$$

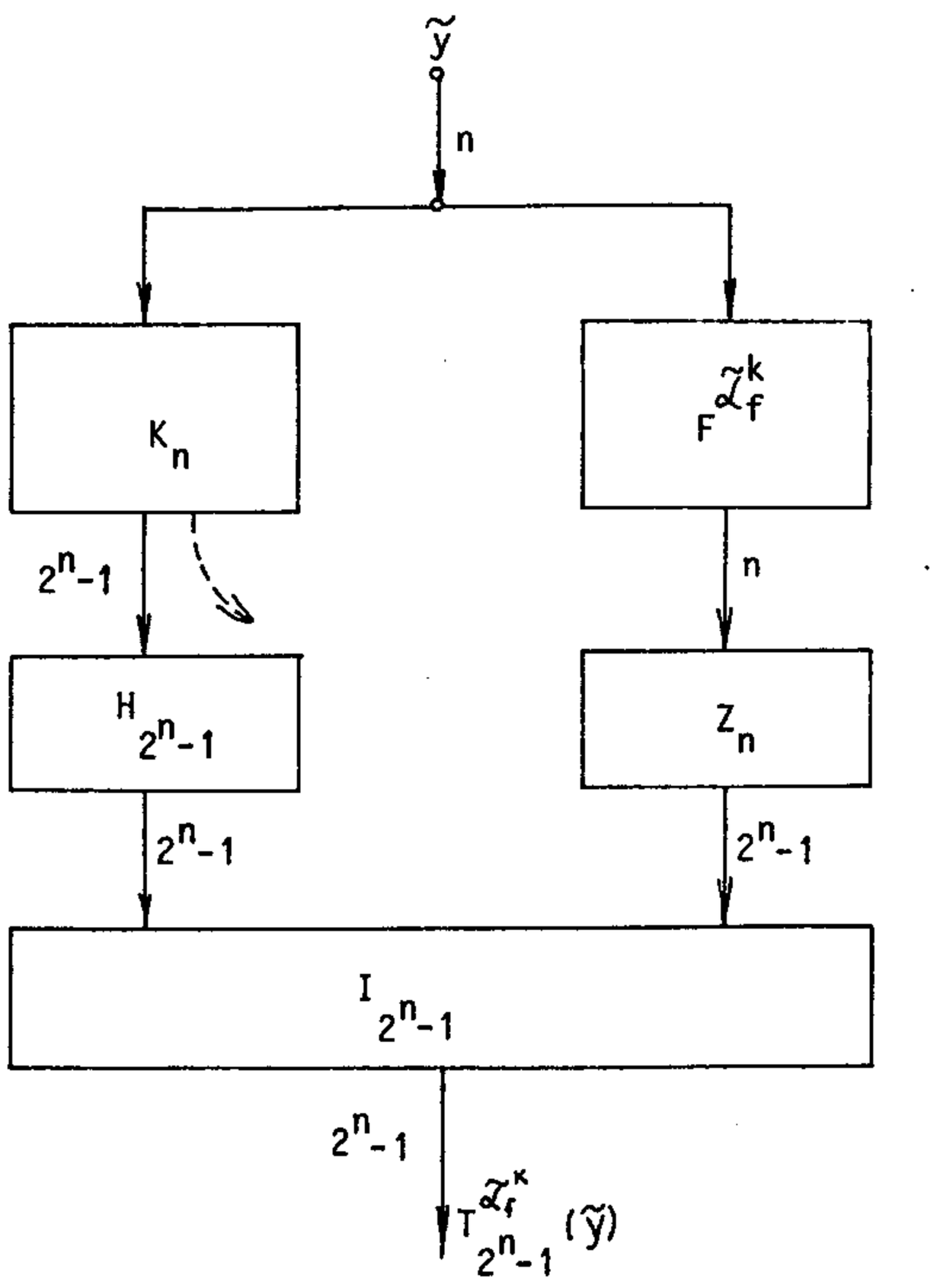
Dokaz. Primijetimo da svaki polinom iz $R_2^n(x)$ koji ima k nenula koeficijenata možemo predstaviti kao sumu dva polinoma iz $R_2^n(x)$ koji imaju manje od k nenula koeficijenata. Na taj način, imajući polinome $1,x,x^2,\ldots,x^{n-1}$, sumirajući po dva od njih dobijamo sve polinome iz $R_2^n(x)$ sa po dva nenula koeficijenta, zatim, sumirajući po dva od tih i polaznih možemo dobiti sve polinome iz $R_2^n(x)$ sa po tri nenula koeficijenta itd., dobijamo sve polinome iz $R_2^n(x)$, koristeći za svaki samo po jedno sumiranje.

Saglasno tom algoritmu konstruišimo shemu Z_n sa n ulaza $x_0,\ldots,x_{n-1}$ i 2^n-1 izlaza $y_0,\ldots,y_{2^n-2}$, takvu da je $y_i=x_i$, $i=0,\ldots,n-1$, a za $k>n$ $y_k=y_j \oplus y_1$, ukoliko smo, saglasno opisanom algoritmu polinom koji se dobija pri dijeljenju x^k sa primitivnim polinomom f(x) stepena n izrazili kao sumu polinoma koji se dobijaju kao ostaci pri dijeljenju polinoma x^j i x^1 sa f(x). Na taj način, $L(Z_n) \leqslant C_z 2^n$.

Zahvaljujući cikličnosti multiplikativne grupe svih nenula polinoma iz $R_2^n(x)$, zaključujemo da shema Z_n ne zavisi od cikličnog pomjeraja, tj. ako umjesto $1,x,\ldots,x^{n-1}$ imamo $x^i,x^{i+1},\ldots,x^{i+n-1}$, gdje je $i \in \{1,\ldots,2^{n-2}\}$, i svi eksponenti se uzimaju po mod (2^n-1), gore opisana shema sukcesivnog izražavanja polinoma iz $R_2^n(x)$ strukturno ostaje nepromijenjena. Na taj način, imajući prvih n članova pomjerenog niza $\mathcal{L}_f^k$, opisana shema će pravilno izračunavati ostale članove pomjerenog niza. Opi-

šimo sada detaljnije algoritam konstrukcije sheme koja realizuje operator $T^{\tilde{\alpha}_f^k}_{2^n-1}$ za bilo koje $k \in \{0,1,\ldots,2^n-2\}$ i bilo koji primitivan polinom f(x) stepena n (vidi sl.16).

1) Ulazni niz $\tilde{y}$ dužine n dovodimo na ulaze sheme $F^{\tilde{\alpha}_f^k}$ koja odredjuje prvih n članova ciklično pomjerenog nadesno za veličinu $|\tilde{y}|$ niza $\tilde{\alpha}_f^k$. Složenost operatora koji realizuje shema nije veća od složenosti najsloženijeg (n,n)-operatora (teorema 1.4.3), te je $L(F^{\tilde{\alpha}_f^k}) \leqslant C \cdot 2^n$.



Sl.16.

2) Izlaze sheme $F^{\alpha_f^x}$ dovedimo na ulaze sheme Z_n, koja odredjuje niz α_f^k ciklično pomjeren nadesno za $|\tilde{y}|$ mjesta. Malo-prije smo pokazali, da je $L(Z_n) \leqslant C_z 2^n$.

3) Niz $\tilde{y}$ dovedimo i na ulaze dešifratora K_n. $L(K_n) \leqslant C_k \cdot 2^n$ (lema 3.2.1).

4) Izlaze dešifratora, izuzimajući poslednji, gledano slijeva nadesno, dovedimo na ulaze sheme koja realizuje operator H_{2^n-1}. $L(H_{2^n-1}) \leqslant C_h \cdot 2^n$ (lema 3.2.4).

5) Pomoću sheme I_{2^n-1} pomnožimo član po član izlazne nizove shema H_{2^n-1} i Z_n. Iz leme 3.2.7 imamo, $L(I_{2^n-1}) \leqslant C_i \cdot 2^n$.

Na izlazima sheme I_{2^n-1} dobijamo niz $\tilde{\alpha}_f^k$ pomjeren nadesno za $|\tilde{y}|$ mjesta.

Na taj način, sumirajući navedene složenosti, dobijamo da je

$$L(T^{\alpha_f^k}_{2^n-1}) \leqslant C_{55} \cdot 2^n ,$$

čime je, imajući u vidu donju trivijalnu ocjenu složenosti, dokaz teoreme završen.

Kao što smo vidjeli, opisani nizovi koji predstavljaju P'_n-cikluse ne sadrže n uzastopnih nula. S druge strane, možemo ih dobiti izbacivanjem jedne od n uzastopnih nula nizova koji predstavljaju odgovarajuće P_n-cikluse. Sledeća teorema, formulisana opštije, govori o linearnoj realizaciji operatora pomjeranja odredjenih nizovima koji predstavljaju P_n-cikluse, od kojih se, izbacivanjem jedne od n uzastopnih nula dobijaju gore opisani P'_n-ciklusi.

Teorema 3.5.3. Neka je $\tilde{\alpha}=(\alpha_0,\ldots,\alpha_{n-1})$ niz dužine n i $\tilde{\alpha}_{-i}=(\alpha_0,\ldots,\alpha_{i-1},\alpha_{i+1},\ldots,\alpha_{n-1})$ niz dužine n-1, dobijen iz niza $\tilde{\alpha}$ izbacivanjem člana α_i. Ako je

$$L(T_{n-1}^{\tilde{\alpha}_{-i}}) \asymp n ,$$

tada je

$$L(T_n^{\tilde{\alpha}}) \asymp n .$$

Dokaz. Uvedimo sledeće nizove: $\tilde{\delta}^i_{\alpha_i}=(0,\ldots,0,\alpha_i,0,\ldots,0)$ dužine n , gdje je α_i na i-tom mjestu u nizu i $\tilde{\gamma}^i=(0,\ldots,0,1,0,\ldots,0)$ dužine n-1, gdje je 1 takodje na i-tom mjestu u nizu. Shema operatora $T_n^{\tilde{\alpha}}$ konstruiše se saglasno sledećem algoritmu (vidi sl.17):

1) Ulazni niz $\tilde{y}$ dužine l_n (tačnije, prvih l_{n-1} članova niza $\tilde{y}$), kojim se zadaje veličina pomjeraja dovodimo na ulaze dvije sheme: sheme koja realizuje operator $T_{n-1}^{\tilde{\alpha}_{-i}}$ i sheme $M_{n-1}^{\tilde{\gamma}^i}$ koja pomjera niz $\tilde{\gamma}^i$. Iz pretpostavke teoreme imamo da je $L(T_{n-1}^{\tilde{\alpha}_{-i}}) \leqslant C_{\alpha_i} n$, a iz leme 3.2.5, $L(M_{n-1}^{\tilde{\gamma}^i}) \leqslant C_m \cdot n$.

2) Ulazni niz $\tilde{y}$ dovodimo i na ulaze sheme $M_n^{\tilde{\delta}^i_{\alpha_i}}$, koja pomjera nadesno niz $\tilde{\delta}^i_{\alpha_i}$ za veličinu $|\tilde{y}|$. $L(M_n^{\tilde{\delta}^i_{\alpha_i}}) \leqslant C_m \cdot n$ (lema 3.2.5).

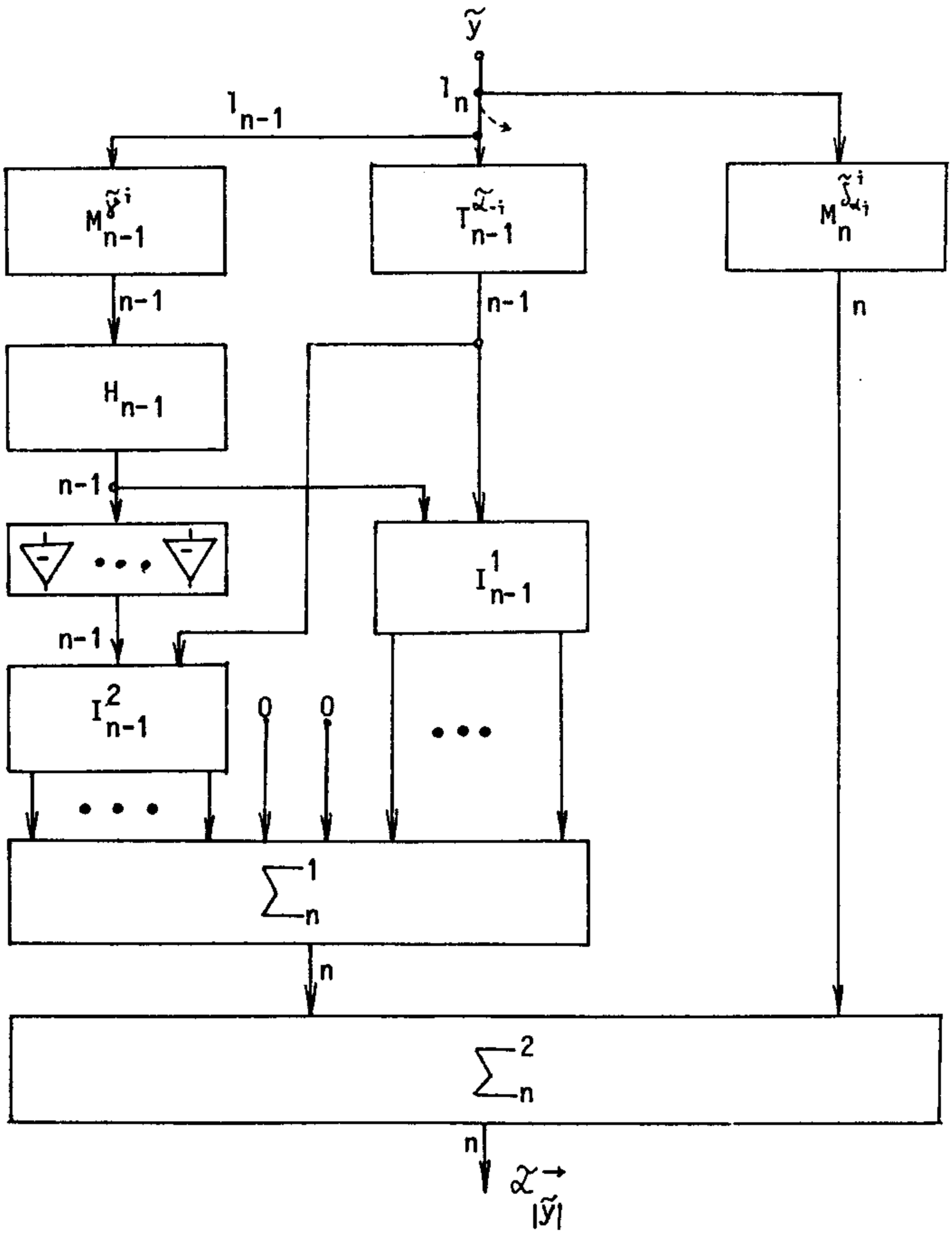
3) Izlazni niz sheme $M_{n-1}^{\tilde{\gamma}^i}$ dovodimo na ulaze sheme H_{n-1}. $L(H_{n-1}) \leqslant C_h \cdot n$ (lema 3.2.4).

4) Izlaze sheme H_{n-1} pomnožimo član po član sa izlazima sheme $T_{n-1}^{\tilde{\alpha}_{-i}}$ pomoću sheme I_{n-1}^1. $L(I_{n-1}^1) \leqslant C_i \cdot n$ (lema 3.2.7).

5) Izlaze iz sheme H_{n-1} dovodimo na ulaze (n-1)-og invertora, a izlaze invertora množimo član po član sa izlazima sheme $T_{n-1}^{\tilde{\alpha}_{-i}}$ pomoću sheme I_{n-1}^2. Očigledno, složenost ovog koraka ne pre-

lazi 2n.

6) Izlazima sheme I^1_{n-1} dodajmo s lijeve strane jedan ulaz na kojem se realizuje 0, a izlazima sheme I^2_{n-1} dodajmo s desne strane isto takav ulaz. Tako dobijena dva niza od po n ulaza dovedimo na ulaze sheme $\sum^1_n$ koja ih član po član sumira. $L(\sum^1_n) \leqslant C_g n$ (lema 3.2.8).



S1.17.

7) Izlaze sheme $\sum_n^1$ dovedimo zajedno sa izlazima sheme $M_n^{\delta_{\tilde{\alpha}_i}^{\alpha_i}}$ na ulaze sheme $\sum_n^2$ koja ih, član po član sumira, tj. umeće elemenat α_i niza $\tilde{\alpha}$ na svoje mjesto u pomjerenom nizu. Na izlazima sheme $\sum_n^2$ dobijamo niz $\tilde{\alpha}_{|\tilde{y}|}^{\rightarrow}$.

Na taj način, sumirajući navedene složenosti, i imajući u vidu donju trivijalnu ocjenu, dobijamo da je

$$L(T_n^{\tilde{\alpha}}) \asymp n .$$

3.6. O jednom drugom metodu raspoznavanja $PD_{m,n}$ oblika pomoću operatora pomjeranja

Iz teorema: 3.1.4, 3.3.1, 3.4.1, 3.4.2, 3.4.3, 3.4.5, 3.5.2, 3.5.3 i leme 3.1.1 sleduje sledeća teorema:

Teorema 3.6.1. Ako vrste matrice M zadovoljavaju uslove jedne od teorema 3.3.1, 3.4.1, 3.4.2, 3.4.3, 3.4.5, 3.5.2, ili su konačna član po član suma po mod 2 nizova koji zadovoljavaju uslove tih teorema, tada je

$$L(PD_{m,n}^M) \asymp m \cdot n .$$

Dosad smo, u ovoj glavi, raspoznavanje $PD_{m,n}^M$ oblika realizovali pomjeranjem svake vrste matrice M posebno. Medjutim, možemo umjesto da pomjeramo svaku vrstu posebno, pomjerati niz $\tilde{\sigma}_m$ dužine $m \cdot n$, koji je pridružen matrici M (vidi paragraf 1.2), i pri tome je potrebna veličina pomjeranja $\leqslant n$.

Teorema 3.6.2. Za svaki $PD_{m,n}^M$ oblik je

$$L(PD_{m,n}^M) \lesssim L(T_{m \cdot n}^{\tilde{\sigma}_m}) ,$$

gdje veličina pomjeraja $|\tilde{y}|$, tj. ulazna veličina operatora $T^{\tilde{\sigma}_M}_{m\cdot n}$ ne prelazi n.

Dokaz. Posmatrajmo proizvoljan $PD^M_{m,n}$ oblik O, gdje je $M=||\alpha_{ij}||^n_m$ nenula matrica (inače je dokaz trivijalan). Označimo sa i_o i j_o sledeće indekse: $j_o=\min\limits_{\alpha_{ij}=1} j$ i i_o bilo koji indeks koji zadovoljava jednakost $\alpha_{i_o j_o}=1$. Neka je $\tilde{\beta}=(\beta_0,\ldots,\beta_{l_n-1})$ binaran zapis broja j_o-1. Shema koja raspoznaje dati $PD^M_{m,n}$ oblik konstruiše se prema sledećem algoritmu (visi sl.18):

1) Neka je $\tilde{x}=(x_{11},\ldots,x_{1n},\ldots,x_{m1},\ldots,x_{mn})$ ulazni niz. Dovedimo $x_{i_o 1},\ldots,x_{i_o n}$ na ulaze sheme koja realizuje operator P_n. $L(P_n)\leqslant C_p\cdot n$ (lema 2.2.7).

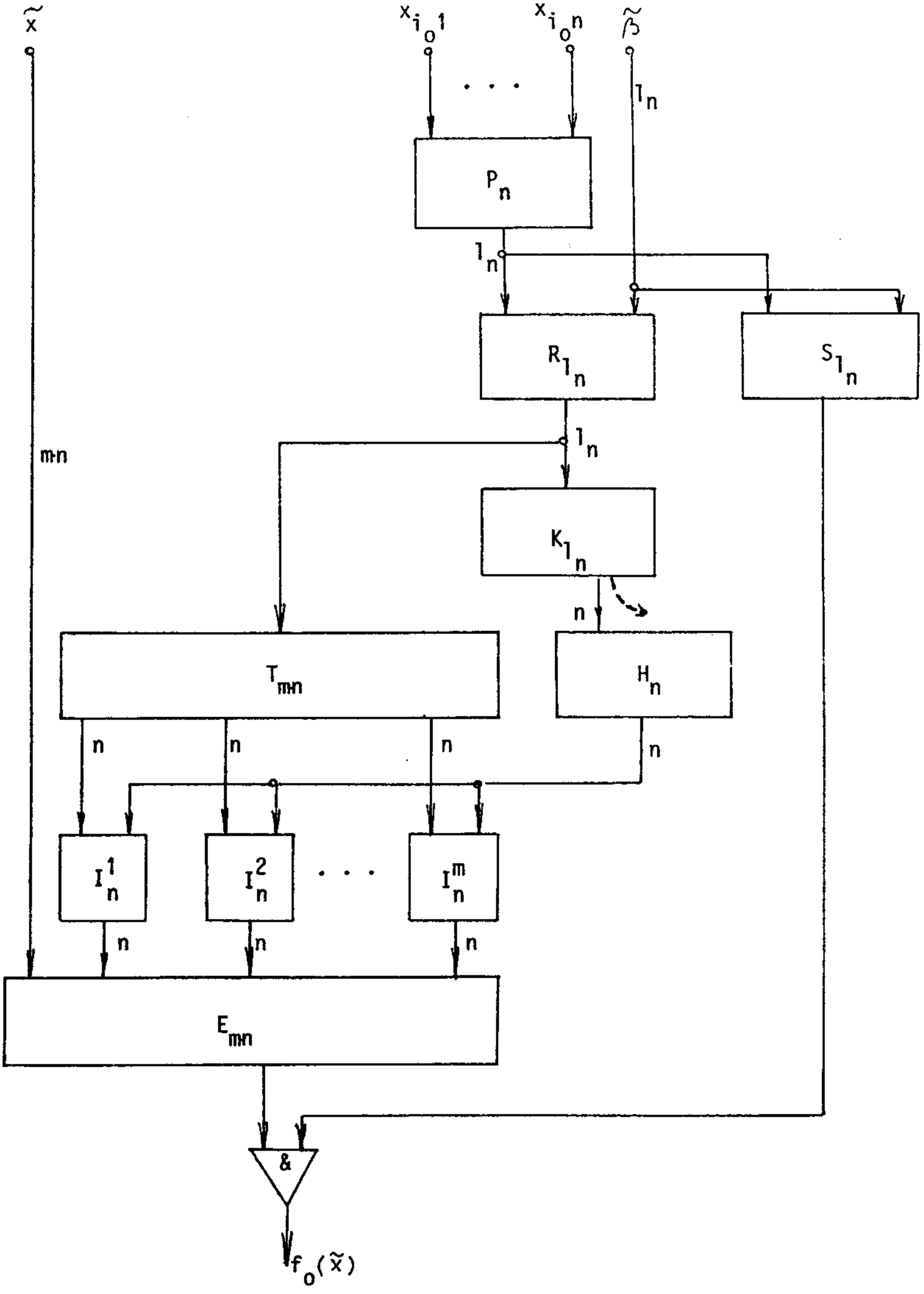
2) Izlazni niz sheme P_n i niz $\tilde{\beta}$ dovedimo na ulaze sheme R_{l_n} koja izračunava veličinu pomjeraja. $L(R_{l_n})\leqslant C'_r\cdot\log n$ (lema 2.2.1).

3) Izlazni niz sheme R_{l_n} dovedimo na ulaze dešifratora K_{l_n}. $L(K_{l_n})\leqslant C'_k\cdot n$ (lema 3.2.1).

4) Izlazni niz dešifratora dovedimo na ulaze sheme koja realizuje operator H_n. $L(H_n)\leqslant C_h\cdot n$ (lema 3.2.4).

5) Izlaze sheme R_{l_n} dovedimo na ulaze sheme koja realizuje operator $T^{\tilde{\sigma}_M}_{m\cdot n}$ sa složenošću $L(T^{\tilde{\sigma}_M}_{m\cdot n})$.

6) Izlaze sheme $T^{\tilde{\sigma}_M}_{m\cdot n}$ razbijmo slijeva nadesno na m grupa po n izlaza u svakoj i svaku grupu izlaza dovedimo na prvih n ulaza po jedne od m shema I^i_n koje ih član po član množe sa izlaznim nizom sheme H_n, $i=1,\ldots,m$. $L(I^i_n)\leqslant C_i\cdot n$, za svako i (lema 3.2.7).


$\tilde{x}$
$x_{i_0 1}$
$x_{i_0 n}$
$\tilde{\beta}$
l_n
P_n
l_n
R_{l_n}
S_{l_n}
l_n
m·n
K_{l_n}
n
T_{mn}
H_n
n
n
n
n
I_n^1
I_n^2
I_n^m
n
n
n
E_{mn}
&
$f_0(\tilde{x})$

S1.18.

7) Ulazni niz $\tilde{x}$ i izlazne nizove shema I_n^i, i=1,...,m, uzete tim redom, dovedimo na ulaze sheme $E_{m.n}$, koja ih sravnjuje. $L(E_{m.n}) \leqslant C_e \cdot m \cdot n$ (lema 2.2.4).

8) Izlazna vrijednost sheme $E_{m.n}$ se množi sa izlaznom vrijednošću sheme poredjenja S_{1_n} koja ispituje da li je veličina pomjeraja veća ili jednaka od veličine j_o-1. $L(S_{1_n}) \leqslant C'_s \cdot \log n$ (lema 2.2.3).

Na taj način,

$$L(PD^M_{m,n}) \leqslant C_{62} \cdot m \cdot n + L(T^{\tilde{\sigma}_M}_{m.n}) \lesssim L(T^{\tilde{\sigma}_M}_{m.n}) ,$$

jer je za svako $\tilde{\sigma}_M$,

$$L(T^{\tilde{\sigma}_M}_{m.n}) \geqslant m \cdot n .$$

Teorema je dokazana.

Posledica 3.6.1. Ako je $L(T^{\tilde{\sigma}_M}_{m.n}) \asymp m \cdot n$, tada je

$$L(PD^M_{m,n}) \asymp m \cdot n .$$

Na taj način dolazimo i do sledeće teoreme:

Teorema 3.6.3. Ako niz $\tilde{\sigma}_M$ zadovoljava uslove jedne od teorema 3.3.1, 3.4.1, 3.4.2, 3.4.3, 3.4.5, 3.5.2, ili je konačna član po član suma po mod 2 nizova koji zadovoljavaju uslove tih teorema, tada je

$$L(PD^M_{m,n}) \asymp m \cdot n .$$

Imajući u vidu da je za raspoznavanje $PD^M_{m,n}$ oblika dovoljno pomjeranje niza $\tilde{\sigma}_M$ za veličinu ne veću od n, koristeći ranije uvedene operatore ograničenog pomjeranja $M^{\tilde{\alpha}}_n$, dobijamo sledeću teoremu (vidi lemu 3.2.5):

Teorema 3.6.4. Za svaki $PD^{M}_{m,n}$ oblik takav da je $\|\tilde{\mathfrak{G}}_{M}\| \leqslant c_{64}m$ važi

$$L(PD^{M}_{m,n}) \asymp m \cdot n \ .$$

SPISAK SPECIJALNIH SIMBOLA

$\left.\begin{matrix}\oplus \\ \bigoplus\end{matrix}\right\}$ - znak sume po mod 2

$[a]$ - najveći cio broj, ne veći od a

$]a[$ - najmanji cio broj, ne manji od a

$\log a$ - logaritam za osnovu 2

& - simbol konjunkcije

V - simbol disjunkcije

$\neg$ - simbol negacije

$p|n$ - p dijeli n

$a_n \lesssim b_n$ - $\overline{\lim} \frac{a_n}{b_n} \leqslant 1$

$a_n \sim b_n$ - $\frac{a_n}{b_n} \to 1$

$\left.\begin{matrix}a_n \lesssim b_n \\ a_n = O(b_n)\end{matrix}\right\}$ - postoji pozitivna konstanta C takva da je $a_n \leqslant C \cdot b_n$, za dovoljno veliko n

$a_n \asymp b_n$ - $a_n \lesssim b_n$ i $b_n \lesssim a_n$

$\left.\begin{matrix}a_n = o(b_n) \\ b_n >> a_n\end{matrix}\right\}$ - $\frac{a_n}{b_n} \to 0$

LITERATURA

[1] Shannon C.E.,A symbolic analysis of relay and switching circuits, Trans. AIEE 57, 1938, 713-722. (Ruski prevod u zborniku: Šenon K.E.,Raboti po teorii informacii i kibernetike, M., IL, 1963, 9-45).

[2] Shannon C.E., The synthesis of two-terminal switching circuits, Bell Syst. Techn. J. 28,1,1949,59-98. (Ruski prevod u zborniku: Šenon K.E.,Raboti po teorii informacii i kibernetike, M., IL, 1963, 59-101).

[3] Jablonski S.V., Funkcionaljnije postrojenija v k - značnoj logike,Trudi matem. in-ta im. V.A. Stjeklova, 1958, t.51, 5-142.

[4] Jablonski S.V.,Asnovnije panjatija kibernetiki, Problemi kibernetiki, M., 1959, vip.2, 7-38.

[5] Jablonski S.V.,O algoritmičeskih trudnostjah sinteza minimaljnih kontaktnih shem, Problemi kibernetiki, M., 1959, vip.2, 75-121.

[6] Jablonski S.V.,O klasah funkcij algebri logiki, dopuskajuših prostuju shemnuju realizaciju, Uspehi matem. nauk 12, vip.6, 1957, 189-196.

[7] Jablonski S.V.,Obzor nekotorih rezuljtatov v oblasti diskretnoj matematiki, Vsesojuznaja konf. po problemam teoret. kibern. (Novosibirsk, junj 1969). Dokladi (plenarnije i sekcionije). Inform.materiali, 5(42). Naučnij savjet po kompleksnoj probljeme "Kibernetika". M., 1970, 5-15.

[8] Jablonski S.V.,Lupanov O.B.(redaktori), Diskretnaja matematika i matematičeskije vaprosi kibernetiki, t.1,"Nauka",M.,1974.

[9] Jablonski S.V.,Vvedenije v diskretnuju matematiku, "Nauka", M., 1979.

[10] Lupanov O.B., O sinteze kontaktnih shem, DAN SSSR, 1958, t. 119, 1, 23-26.

[11] Lupanov O.B.,Ob adnom metode sinteza shem, Izvestija vuzov, Radiofizika, 1958, t.1, 1, 120-140.

[12] Lupanov O.B.,O složnosti realizacii funkcij algebri logiki formulami, Problemi kibernetiki, M., 1960, vip.3, 61-80.

[13] Lupanov O.B.,O sinteze nekatorih klasov upravljajuših sistem, Problemi kibernetiki, M., 1963, vip.10, 63-97.

[14] Lupanov O.B.,Ob adnom padhode k sintezu upravljajuših sistem - principe lokaljnovo kodirovanija, Problemi kibernetiki, M., 1965, vip.14, 31-110.

[15] Lupanov O.B., Ob asimptotičeskih acjenkah složnosti upravljajuših sistem, Meždunarodn. kongres matematikov v Nice, 1970, M., 1972, 162-167.

[16] Subatovskaja B.A., O realizacii linejnih funkcij formulami v bazise V,&,-, DAN SSSR, 136,3(1961), 553-555.

[17] Hrapčenko V.M., O složnosti realizacii linejnoj funkciji v klase - shem, Matem. zametki, 9,1 (1971), 35-40.

[18] Nečiporuk E.I., Ob adnoj bulevskoj funkcii, DAN SSSR, 169, 4 (1966), 765-767.

[19] Nečiporuk E.I., O realizacii dizjunkcii i konjunkcii v nekatorih monotonih bazisah, Problemi kibernetiki, M., 1970, vip. 23, 291-293.

[20] Rohlina M.M., O shemah, povišajuših nadjožnost, Problemi kibernetiki, M., 1970, vip.23, 295-301.

[21] Kuzmin V.A.,Realizacija funkcij algebri logiki avtomatami, normaljnimi algoritmami i mašinami Tjuringa, Problemi kibernetiki, M., 1965, vip.13, 75-96.

[22] Nigmatulin R.G.,Složnost bulevih funkcij, Izdateljstvo Kazanskovo universiteta, 1983.

[23] Kasami T., Tokura N., Ivadari E., Inagaki Y., Teorija kodirovanija, prevod s japanskog, "Mir", M., 1978.

[24] de Bruijn N.G., A combinatorial problem, Proc. Kon. Ned. Akad. v. Wet., 49, 7(1946), 758-764.

[25] Mehlhorn K., Some remarks on Boolean sums, Acta Informatica 12 (1979), 371-375.

[26] Čandrasekharan K., Vvedenije v analitičeskuju teoriju čisel, "Mir", M., 1974.

[27] Čandrasekharan K., Arifmetičeskije funkcii, "Nauka", M.,1975.

[28] Kudrijavcev V.B., Aljošin S.V., Podkolzin A.S., Elementi teorii avtomatov, Izdateljstvo Moskovskovo universiteta,M.,1978.

[29] Kobrinskij N.E., Trahtenbhot B. A., Vvedenije v teoriju kanječnih avtomatov, M., Fizmatgiz, 1962.

[30] Ulig D., O sinteze samokorektirujušihsja shem iz funkcionaljnih elementov s malim čislom nadjožnih elementov, Matematičeskije zametki, M.,t.15, 6(1974), 937-944.

[31] Albert A.A., Fundamental concepts of higher algebra,Ch.V,1956.

[32] Gil A., Linejnije posledovateljnostnije mašini, "Nauka", M.,1974.

[33] Savage J.E., Computational work and time on finite machines, J. Ass. Comp. Mach., 1972, V.19, 660-674.

[34] Schnorr C.P., Lower bounds for the product of time and space requirements of Turing machine computations, Proc. of MFCS Higs Tatras, 1973, 153-163.

[35] Schnorr C.P., The network complexity and the Turing machine complexity of finite functions, Acta Informatica, 1976, V.7, 95-107.

[36] Šćepanović R.L., O složenosti raspoznajućih automata, magistarski rad, Beograd, 1980.

[37] Šćepanović R.L., O linejnoj složnosti realizacii nekatorih operatorov zdviga, primljen za štampu u "Zbornik rabot po matematičeskoj kibernetike", M., 1985.

[38] Šćepanović R.L., O linejnoj složnosti realizacii raspoznavanija nekatorovo klasa obrazov, predat za štampu u Publ. Inst.Math., Beograd.

[39] Šćepanović R.L., O nelinejnoj složnosti monotonoj realizacii adnavo semejstva bulevih sum, predat za štampu u Publ. Inst. Math., Beograd.

[40] Šćepanović R.L., O linejnoj složnosti realizacii samih složnih operatorov zdviga, u pripremi.