



UNIVERZITET U NOVOM SADU  
FAKULTET TEHNIČKIH NAUKA

**Paraunitarna reprezentacija  
komplementarnih sekvenci**

DOKTORSKA DISERTACIJA

Mr Srđan Budišin

Mentor: prof. dr Miodrag Temerinac

Novi Sad, juna 2012. godine

**UNIVERZITET U NOVOM SADU**  
**FAKULTET TEHNIČKIH NAUKA**

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj, RBR:	
Identifikacioni broj, IBR:	
Tip dokumentacije, TD:	Monografska dokumentacija
Tip zapisa, TZ:	Tekstualni štampani materijal
Vrsta rada, VR:	Doktorat
Ime i prezime autora, AU:	Srđan Budišin
Mentor MN: Komentor	Dr Miodrag Temerinac, redovni profesor Dr Aleksa Zejak, naučni savetnik
Naslov rada, NR:	Paraunitarna reprezentacija komplementarnih sekvenci
Jezik publikacije, JP:	srpski
Jezik izvoda, JI:	srpski / engleski
Zemlja publikovanja, ZP:	Republika Srbija
Uže geografsko područje, UGP:	Vojvodina
Godina, GO:	2012
Izdavač, IZ:	autorski reprint
Mesto i adresa, MA:	Novi Sad, Trg Dositeja Obradovića 6
Fizički opis rada, FO:	7 poglavlja / 130 stranica / 23 slike / 11 tabela / 77 referenci
Naučna oblast, NO:	Elektrotehnika i računarstvo
Naučna disciplina, ND:	Računarske komunikacije i radari
Predmetna odrednica, ključne reči, PO:	Paraunitarne matrice, komplementarne sekvence, efikasni korelator, PSK, QAM, OFDM
UDK	
Čuva se u, ČU:	Biblioteci Fakulteta tehničkih nauka, u Novom Sadu
Važna napomena, VN:	
Izvod, IZ:	U ovoj disertaciji je data opšta kanonična forma, bazirana na paraunitarnim matricama, u kojoj mogu da se predstavje svi do sada poznati i nepoznati parovi komplementarnih sekvenci. U toj kanoničnoj formi se mogu predstaviti binarne, polifazne (unimodularne) i QAM sekvence ali i sve druge kompleksne sekvence. Teorija je potkrepljena brojnim primerima iz gore navedenih familija sekvenci.
Datum prihvatanja teme od strane NN veća, DP:	
Datum odbrane, DO:	
Članovi komisije, KO:	<b>predsednik:</b> dr Vladimir Kovačević, profesor emeritus, FTN, Novi Sad <b>član:</b> dr Branislav Todorović, viši naučni saradnik, Institut RT-RK Novi Sad <b>član-komentor:</b> dr Aleksa Zejak, naučni savetnik, Institut RT-RK Novi Sad <b>član:</b> dr Bojan Zrnić, vanr.profesor, Vojna akademija, Beograd <b>član-mentor:</b> dr Miodrag Temerinac, dr, redovni profesor, FTN, Novi Sad

**University of Novi Sad**  
**Faculty of Technical Sciences**  
Key-word documentation

Accession number, ANO:	
Identification number, INO:	
Document type, DT:	Monograph documentation
Record type, TR:	Textual printed material
Thesis type, CC:	PhD Thesis
Author, AU:	Srđan Budišin
Mentor, MN: Comentor	Miodrag Temerinac, PhD Aleksa Zejak, PhD
Title, TI:	Paraunitary representation of complementary sequences
Language of the text, LT:	Serbian
Language of the abstract, LA:	Serbian / English
Country of publication, CP:	Republic of Serbia
Locality of publication, LP:	Vojvodina
Publication year, PY:	2012
Publisher, PU:	Author's reprint
Address, PP:	Novi Sad, Trg Dositeja Obradovića 6
Physical description, PD:	7 chapters / 130 pages / 23 figures / 11 tables / 77 references
Scientific field, SF:	Electronics and computers
Scientific discipline, SD:	Computer communications and radar
Subject, Key words, SKW:	Paraunitary matrices, complementary sequences, efficient correlator, PSK, QAM, OFDM
UC	
Holding library, HD:	Public library of Faculty of Technical Sciences, Novi Sad
Note, N	
Abstract, AB	In this thesis, a general canonic form for representing any complementary pair of sequences is proposed. This canonic form is based on paraunitary matrices and can be applied to any known or still unknown complementary pairs. Numerous examples of the application of this theory to binary, QPSK and QAM sequences are given including standard, non-standard and kernel cases.
Accepted by Science Board on, AS:	
Defense date, DE:	
Thesis Defense Committee, DB:	<b>President:</b> Vladimir Kovačević, PhD, professor emeritus, FTN, Novi Sad <b>Member:</b> Branislav Todorović, PhD Senior Research Fellow, Institut RT-RK Novi Sad <b>Member-comentor:</b> Aleksa Zejak, PhD, Principal Research Fellow, Institut RT-RK Novi Sad <b>Member:</b> Bojan Zrnić, PhD, Associate Professor, Military academy, Beograd <b>Member-mentor:</b> Miodrag Temerinac, PhD, Full Professor, FTN, Novi Sad

---

# Sadržaj

<b>Zahvalnica</b> .....	1
<b>Spisak slika</b> .....	2
<b>Spisak tabela</b> .....	4
<b>Lista skraćenica</b> .....	5
<b>Lista promjenljivih</b> .....	7
<b>Rezime</b> .....	9
<b>Abstract</b> .....	11
<b>1. Uvod</b> .....	13
1.1. Istorijat istraživanja komplementarnih sekvenci .....	14
1.1.1. Golejevi binarni komplementarni parovi .....	15
1.1.2. Komplementarni skupovi .....	16
1.1.3. Polifazne komplementarne sekvence .....	16
1.1.4. Višedimenzionalne komplementarne sekvence .....	17
1.1.5. Komplementarnost spektra.....	17
1.1.6. Nestandardne komplementarne sekvence .....	18
1.1.7. Veza s Rid-Milerovim kodovima.....	18
1.1.8. QAM komplementarne sekvence .....	19
1.2. Oblasti primene .....	19
1.2.1. Optika (Multislit spectrometry).....	19
1.2.2. Kompresija impulsa u radarima .....	19
1.2.3. WiFi standard – IEEE 802.11b .....	20
1.2.4. 3G mobilna telefonija – UMTS standard .....	21
1.2.5. WiMax standard – IEEE 102.16 .....	21
1.2.6. OFDM .....	21
1.2.7. Ostale primene.....	22
1.3. Prednosti komplementarnih sekvenci .....	22
1.4. Značaj komplementarnih sekvenci .....	23
1.5. Banke filtera i paraunitarne matrice.....	26
1.6. Struktura disertacije .....	27
<b>2. Notacija, terminologija i definicije</b> .....	28
2.1. Matematička notacija i terminologija .....	28
2.1.1. Unitarne matrice i transformacije.....	28
2.1.2. Z transformacija .....	29
2.1.3. Matrični polinomi.....	30

---

2.1.4.	Matrični proizvodi.....	32
2.1.5.	Permutacije i permutaciona matrica.....	32
2.1.6.	Bitska reprezentacija brojeva.....	33
2.1.7.	Volšove matrice i Volšove sekvence.....	34
2.2.	<b>Sekvence.....</b>	<b>35</b>
2.2.1.	Predstavljanje sekvenci pomoću Z transformacije.....	35
2.2.2.	Matrično predstavljanje parova i skupova sekvenci.....	36
2.2.3.	Autokorelaciona funkcija sekvence.....	37
2.2.4.	Faktor dobrote.....	37
2.2.5.	Furijeova transformacija sekvence.....	38
2.3.	<b>Komplementarne sekvence.....</b>	<b>39</b>
2.3.1.	Definicija komplementarnih sekvenci.....	39
2.3.2.	Uslov komplementarnosti u matričnom obliku.....	40
2.3.3.	Spektralne osobine.....	40
2.4.	<b>Paraunitarne matrice.....</b>	<b>42</b>
2.4.1.	Definicija.....	42
2.4.2.	Veza s komplementarnim sekvencama.....	42
<b>3.</b>	<b>Osobine binarnih komplementarnih sekvenci.....</b>	<b>45</b>
3.1.	Dužina sekvenci.....	45
3.2.	Broj različitih sekvenci zadate dužine.....	46
3.3.	Autokorelacione osobine.....	47
3.4.	Faktor dobrote.....	51
3.5.	Spektralne osobine.....	52
3.6.	Hamingova rastojanja.....	55
3.7.	Linearna složenost.....	55
3.8.	Generatori sekvenci.....	56
3.9.	Korelatori sekvenci.....	56
<b>4.</b>	<b>Poznati algoritmi.....</b>	<b>58</b>
4.1.	Standardni nerekurzivni algoritmi.....	59
4.2.	Standardni rekurzivni algoritam.....	60
4.3.	Višenivoske komplementarne sekvence.....	64
4.4.	Efikasni korelator komplementarnih sekvenci.....	65
4.5.	Varijacije standardnog algoritma.....	66
<b>5.</b>	<b>Paraunitarna dekompozicija i reprezentacija.....</b>	<b>68</b>
5.1.	Faktorizacija paraunitarnih matrica.....	69
5.2.	Algoritam dekompozicije.....	73
5.3.	Kanonična forma.....	75

5.4.	Kompaktna kanonična forma .....	76
5.5.	Dvokanalni paraunitarni filtri .....	78
5.6.	Dvokanalni komunikacioni sistem.....	81
5.7.	Ostali rekurzivni algoritmi .....	83
5.7.1.	Osobine generišućih matrica i omega vektora .....	83
5.7.2.	Algoritam nadovezivanja (concatenation) .....	85
5.7.3.	Algoritam učešljavanja (interleaving).....	85
5.7.4.	Nadovezivanje blokova (block concatenation) .....	86
5.7.5.	Učešljavanje blokova (block interleaving).....	87
5.7.6.	Turinov kompozitni algoritam za binarne sekvence .....	88
5.7.7.	Fazni pomak jedne od dve sekvence u paru.....	90
5.7.8.	Frekvencijski pomak obe sekvence.....	91
5.8.	Efikasnost generatora-korelatora .....	92
<b>6.</b>	<b>Primeri .....</b>	<b>93</b>
6.1.	Binarne sekvence .....	93
6.1.1.	Standardne.....	94
6.1.2.	Nestandardne.....	95
6.1.3.	Kerneli.....	95
6.1.3.1.	Kernel 10.....	95
6.1.3.2.	Kernel 20.....	98
6.1.3.3.	Kernel 26.....	99
6.2.	PSK sekvence.....	99
6.2.1.	Standardne.....	99
6.2.2.	Nestandardne.....	100
6.2.3.	Kerneli.....	100
6.2.3.1.	Kernel 3.....	101
6.2.3.2.	Kernel 5.....	102
6.2.3.3.	Kernel 10.....	102
6.2.3.4.	Kernel 11.....	102
6.2.3.5.	Kernel 13.....	103
6.2.3.6.	Kerneli 20 i 26 .....	103
6.3.	QAM sekvence.....	103
6.3.1.	Standardne.....	104
6.3.1.1.	16-QAM sekvence .....	104
6.3.1.2.	64-QAM sekvence .....	111
6.3.2.	Nestandardne sekvence .....	114
6.3.3.	Kerneli.....	115
<b>7.</b>	<b>Zaključak .....</b>	<b>118</b>
	<b>Literatura.....</b>	<b>119</b>

# Zahvalnica

Najpre izražavam zahvalnost svom prvom i dugogodišnjem direktoru dr Draganu Kosanoviću koji me je kao tek diplomirani inženjera primio u Institut za primenjenu fiziku i tako mi omogućio da se bavim najnaprednijim oblastima iz radarstva i telekomunikacija.

Zahvaljujem dr Aleksandaru Nešiću koji mi je pružio priliku da postavim koncepciju radara IR-10 na bazi kompresije impulsa te da se bavim mnogim drugim naprednim oblastima.

Zahvaljujem kolegi dr Branislavu Popoviću koji mi je prvi ukazao na fantastične osobine komplementarnih sekvenci i koji me je, bez obira na moju kategoričnu tvrdnju da je postojanje takvih sekvenci nemoguće, razuverio i zainteresovao me da pročitam Golejev fundamentalni rad. Upravo tada se rodilo moje oduševljenje komplementarnim sekvencama koje traje i danas.

Moja zahvalnost dugogodišnjem prijatelju dr Zoranu Miljaniću koji me je posle pauze od 20 godina vratio u struku i stoga je posredno zaslužan za objavljivanje nekoliko novijih radova iz oblasti sekvenci.

Hvala dr Aleksi Zejaku koji mi je dao veliku moralnu podršku kada sam mu rekao da posle 20 godina hoću da objavim rad i kazao mu kako razmišljam o tome da pišem doktorat a na kraju i zato što je predložio da mi bude mentor na izradi doktorata i što me je nesebično podržavao i usmeravao na tom putu.

Zahvaljujem dr Predragu Spasojeviću s kojim sam sarađivao na svim svojim radovima nastalim posle pauze od 20 godina. Uz to što me je podržavao, njegov doprinos u tim radovima je značajan. Napominjem da je povezivanje teorije komplementarnih sekvenci i teorije paraunitarnih matrica rezultat njegove inicijative i zajedničkog teorijskog rada.

## Spisak slika

Sl. 1. Citiranje Golejevog rada iz 1961. po decenijama.....	24
Sl. 2. Citiranje autorovih značajnijih radova po godinama.....	26
Sl. 3. Autokorelacione funkcije komplementarnog para .....	40
Sl. 4. Broj različitih sekvenci u funkciji dužine sekvenci.....	47
Sl. 5. Autokorelaciona funkcija komplementarnog para dužine 128 s velikim autokorelacionim pikom koji iznosi 39 (amplituda glavnog loba se ne vidi na slici a iznosi 128).....	50
Sl. 6. Autokorelaciona funkcija komplementarnog para dužine 128 s malim autokorelacionim pikom koji iznosi 8 (amplituda glavnog loba se ne vidi na slici a iznosi 128).....	50
Sl. 7. Faktor dobrote za Golejeve sekvence dužine 4 do 256 određen numerički .....	52
Sl. 8. Spektar prve sekvence iz komplementarnog para .....	54
Sl. 9. Spektar druge sekvence iz komplementarnog para .....	54
Sl. 10. Spektar PN sekvence .....	54
Sl. 11. Spektar Golejeve sekvence dužine 512 .....	54
Sl. 12. Spektar PN sekvence dužine 511.....	55
Sl. 13. Generator Golejeve sekvence direktnom metodom – prikazan je slučaj osnovne permutacije.....	59
Sl. 14. Blok šematski prikaz rekurzivnog algoritma za generisanje polifaznih sekvenci. 62	
Sl. 15. Blok šema algoritma za generisanje višenivoskih komplementarnih sekvenci. ....	65
Sl. 16. Kanonična forma .....	76
Sl. 17. Kompaktna kanonična forma.....	77
Sl. 18. Opšti oblik dvokanalnog generišućeg filtera.....	79

## Spisak slika

---

Sl. 19. Kanonična forma generišuće matrice .....	80
Sl. 20. Korelišuća matrica.....	81
Sl. 21. Dvokanalni primopredajni system.....	82
Sl. 22. Broj različitih 4-PSK I 16-QAM sekvenci zavisi od dužine sekvenci .....	109
Sl. 23. Primer složenosti izraza koji se koriste u radovima gde je primenjena direktna metoda.....	112
Sl. 24. Broj sekvenci generisanih pomoću predloženog algoritma i algoritma [Chang 2010] kao funkcija dužine sekvenci.....	114

# Spisak tabela

Tab. 1. Citiranje Golejevog rada iz 1961. po decenijama.....	24
Tab. 2. Rezultati pretraživanja po ključnim rečima u Google Scholaru .....	24
Tab. 3. Citiranje značajnijih autorovih radova po godinama.....	25
Tab. 4. Broj Golejevih sekvenci i PN sekvenci za različite dužine .....	46
Tab. 5. Maksimalni autokorelacioni pikovi i srednja kvadratna vrednost (RMS) lobova za najbolje i najgore primerke Golejevih i PN sekvenci .....	49
Tab. 6. PAPR za PN sekvence u zavisnosti od dužine .....	53
Tab. 7 . Svih šest mogućih permutacija $PB_n$ za $N=3$ .....	67
Tab. 8. Proces generisanja komplementarnog para dužine 10 (prvi kernel).....	98
Tab. 9. Q matrice, broj generisanih sekvenci, P i PAPR .....	107
Tab. 10. Nestandardne sekvence, vrednosti omega vektora i snage sekvenci $P_a$ i $P_b$ ....	115
Tab. 11. Omega vektori za sekvence iz [Huang 11] .....	116

## Lista skraćenica

2U2I – dvoulazni-dvoizlazni  
3G – 3rd generation (mobile telecommunications)  
CDMA – Code division multiple access  
DC – direct current  
DFT – Discrete Fourier transform  
FFT – Fast Fourier transform  
FIR – Finite impulse response  
FWT – Fast Walsh transform  
GUIDAR – guided radar  
IEEE – Institute of Electrical and Electronics Engineers  
IFFT – Inverse Fast Fourier transform  
IIR – Infinite impulse response  
IRE – Institute of Radio Engineers  
GDJ – Golay-Davis-Jedwab  
LTE – Long Term Evolution  
MC-CDMA – Multi-carrier code division multiple access  
OFDM – Orthogonal frequency-division multiplexing  
PAPR – Peak-to-Average Power Ratio  
PN (sekvence) – PseudoNoise  
PONS – Prometheus orthonormal sets  
PSK – Phase-shift keying  
QAM – Quadrature amplitude modulation  
RACH – Random Access Channel  
RMS – Root mean square  
TDD – Time-division duplex  
UMTS – Universal Mobile Telecommunications System  
XOR – eXclusive or

## **Lista skracenica**

---

WCDMA – Wideband Code Division Multiple Access

WIFI – wireless local area network

WIMAX – Worldwide Interoperability for Microwave Access

## Lista promenljivih

- $a(n), b(n)$  – komplementarni par sekvenci  
 $b_m(k)$  – m-ti bit broja  $k$  (unipolarna verzija)  
 $B_m(k)$  – m-ti bit broja  $k$  (bipolarna verzija)  
 $C, S$  – komponente unitarne matrice veličine  $2 \times 2$   
 $C(Z^{-1}), S(Z^{-1})$  – komponente paraunitarne matrice veličine  $2 \times 2$   
 $C_{x,y}(k)$  – međukorelacija sekvenci  $x$  i  $y$   
 $D_k$  – celobrojno kašnjenje u rekurzivnom algoritmu  
 $D_{Hamming}$  – Hamingovo rastojanje  
 $\mathbf{D}(Z^{-1})$  – paraunitarna matrica jediničnog kašnjenja  
 $E_x$  – energija sekvence  $x$   
 $F_x$  – faktor dobrote sekvence  $x$   
 $\mathcal{F}_x(f)$  – Furijeova transformacija sekvence  $x$   
 $F_x(k)$  – diskretna Furijeova transformacija sekvence  $x$   
 $H(Z^{-1})$  – prenosna funkcija filtera  
 $\mathbf{I}_N$  – jedinična matrice veličine  $N \times N$   
 $L$  – dužina sekvence  
 $\mathcal{M}(Z^{-1}), \mathcal{M}_G(Z^{-1})$  – generišuća matrica komplementarnog para  
 $\mathcal{M}_C(Z^{-1})$  – korelišuća matrica komplementarnog para  
 $\mathcal{M}_{CC}(Z^{-1})$  – kauzalna korelišuća matrica komplementarnog para  
 $\mathbf{M}_k(Z^{-1})$  – paraunitarna matrica koja generiše duži polifazni komplementarni par iz kraćeg  
 $N$  – broj iteracija u rekurzivnom algoritmu koji određuje dužinu sekvence  $L = 2^N$   
 $P$  – snaga sekvence  
 $P(n)$  – permutacija  
 $\mathbf{P}(Z^{-1})$  – paraunitarna matrica  
 $Q_k$  – realni parametar multilevel algoritma

## Lista promenljivih

---

- $R_x(k)$  – autokorelaciona funkcija sekvence  $x$   
 $\mathcal{R}_x(Z^{-1})$  – Z transformacija autokorelacione funkcije sekvence  $x$   
 $S(k)$  – položaj k-tog nenultog elementa u  $\Omega$  spektru  
 $S_x(f)$  – spektralna gustina snage sekvence  $x$   
 $U$  – unitarna matrica  
 $U_{\Omega_k}$  – unitarna matrica u paraunitarnoj faktorizaciji  
 $U_n$  – unitarna matrica koja je faktor  $V_n(Z^{-1})$  matrice  
 $v$  – matrica-kolona (vector-kolona)  $M \times 1$  s jediničnom normom korišćena u paraunitarnoj faktorizaciji  
 $V_n(Z^{-1})$  – faktori u početnom obliku paraunitarne faktorizacije  
 $V_{\Omega_k}(Z^{-1})$  – faktori generišuće matrice  
 $x(n)$  – sekvenca u vremenskom domenu  
 $X(Z^{-1})$  – Z transformacija sekvence  $x$   
 $\mathbf{x}(Z^{-1})$  – vector-kolona koja predstavlja komplementarni par ili skup  
 $\mathbf{x}_{AB}(Z^{-1})$  – vector-kolona koja predstavlja komplementarni par  $[a, b]$   
 $Z$  – kompleksna promenljiva u Z transformaciji  
 $\mathbf{W}^{(K)}$  – Volšova matrica veličine  $2^K \times 2^K$   
 $w_k(m)$  – k-ta Volšova funkcija  
 $W_k$  – unimodularna kompleksna konstanta  
 $\mathbf{W}_k$  – unitarna matrica koja je prvi faktor  $\mathbf{M}_k(Z^{-1})$  matrice  
 $\delta(k)$  – diskretni Dirakov delta impuls ili Hronekerova funkcija  
 $\Phi_n$  – koeficijent koji definiše  $\Phi_n$  matricu  
 $\Phi_n$  – kvazikomutativna matrica koja se pojavljuje u paraunitarnoj faktorizaciji  
 $\Omega_n$  – niz kompleksnih brojeva koji definiše  $\Omega_n$  matrice – omega vektor  
 $\Omega_n$  – unitarne matrice definisane kompleksnim brojevima  $\Omega_n$  koje se pojavljuju u završnoj formi paraunitarne faktorizacije

# Rezime

U ovoj disertaciji je data opšta kanonična forma, bazirana na paraunitarnim matricama, u kojoj mogu da se predstave svi do sada poznati i nepoznati parovi komplementarnih sekvenci. U toj kanoničnoj formi se mogu predstaviti binarne, polifazne (unimodularne) i QAM sekvence ali i sve druge kompleksne sekvence. Teorija je potkrepljena brojnim primerima iz gore navedenih familija sekvenci.

Prvo je dat detaljan pregled istorije komplementarnih sekvenci, njihovih osobina, primena i algoritama za njihovo generisanje. Zatim je pokazano da je uslov komplementarnosti sekvenci ekvivalentan uslovu koji polinomijalne matrice treba da ispune da bi bile paraunitarne. Time je stvorena mogućnost da se rezultati zrele i detaljno razrađene teorije filterskih banaka u kojoj je nastala teorija paraunitarnih matrica primene na teoriju komplementarnih sekvenci. Mi smo se bavili samo primenom paraunitarnih matrica veličine  $2 \times 2$  na teoriju komplementarnih parova. Na sličan način je moguće upotrebiti veće paraunitarne matrice da bi se razvila teorija komplementarnih skupova sekvenci.

Prvi korak u primeni paraunitarnih matrica na komplementarne sekvence bila je faktorizacija matrica veličine  $2 \times 2$ .

Drugi korak je bio da se razvije algoritam kojim se za proizvoljan komplementarni par određuju parametri paraunitarne faktorizacije. Na taj način je pokazano da je faktorizacija jednoznačna i da svakom komplementarnom paru odgovara samo jedna faktorizacija definisana kompleksnim vektorom koji smo nazvali omega vektor. Takođe je pokazano da se, polazeći od bilo kog omega vektora, može generisati komplementarni par, što znači da smo dobili algoritam koji može da generiše ma koji komplementarni par, bilo da postoji u literaturi ili ne postoji.

U trećem koraku je pokazano kako se, u slučaju kad omega vektor sadrži dosta nula, faktorizacija može napisati s manje faktora i tako se dobija kompaktna kanonična forma. Takođe je definisan stepen kompaktnosti.

U četvrtom koraku je pokazano kako se na osnovu kanonične forme može realizovati korelator (prilagođeni filter) i da kompaktna kanonična forma daje efikasan korelator.

## Rezime

---

Najzad je teorija primenjena na konkretne primere sledećih sekvenci: binarnih, QPSK (4-PSK) i 16-QAM i 64-QAM komplementarnih. Pri tome su dati primeri za standardne, nestandardne i komplementarne sekvence te za kernele.

# Abstract

In this thesis, a general canonic form for representing any complementary pair of sequences is introduced. This canonic form is based on paraunitary matrix representation and can be applied to any known or still unknown complementary pairs. Numerous examples of the application of this theory to known binary, QPSK and QAM sequences are given.

First we give a detailed overview of the history, properties, applications and algorithms related to complementary sequences. Next we show that the complementarity condition on the Z-transform matrix representation of a sequence pair is, in fact, a paraunitary matrix definition. Hence, we show that the study of complementary sequences is also a study of paraunitary matrices and vice versa. This allows us to borrow from the rich and mature theory of paraunitary matrices developed in the signal processing literature on filter-banks. In this thesis we only consider 2-by-2 paraunitary matrices and the corresponding complementary sequence pairs. In the future, we will study the relationship of larger paraunitary matrices and the complementary sequence sets.

Our theoretical contribution consists of several steps.

The first step was to find a unique factorization of 2-by-2 paraunitary matrices. We introduce a complex omega vector whose elements define the factors in the factorization.

In the second step, we describe an algorithm to calculate the omega vector for a given complementary pair. It is demonstrated that this calculation is unique and, hence, any complementary pair can be mapped to an omega vector and vice versa. In this way new complementary pairs can be constructed.

In the third step we show that, when the omega vector is sparse, the number of factors in the factorization can be reduced to the number of non-zero omega vector elements. We call this factorization the compact canonic form.

In the fourth step we introduce the paraunitary generating matrix and demonstrate that the correlating matrix [matched filter to complementary sequences] can be obtained by its transposition and conjugation. The correlating matrix is also compact when the

## Abstract

---

omega vector is sparse resulting in an efficient correlator. The efficiency of the correlator is also characterized in the general case.

Finally we verify the theory by applying it to many examples from binary, QPSK to QAM complementary sequences. For each family, examples from standard, non-standard and kernel complementary sequences are given.

# 1. Uvod

Prva primena sekvenci u obradi signala je opisana u radarskoj tehnici, kada je otkrivena kompresija impulsa. Prve analogne sekvence su bili linearno-frekvencijski modulirani impulsi popularno nazvani čirp (chirp) signali; njihovo ime bi se moglo prevesti kao cvrkuti. Međutim takvi signali su realizovani u analognoj tehnici. S razvojem digitalne tehnike pojavljuju se prve digitalne (binarne) sekvence poznate kao Barkerove sekvence [Barker 53]. Barkerove sekvence postoje samo za dužine 2, 3, 4, 5, 7, 11 i 13. Bez obzira na male dužine, one su se dugo primenjivale u radarskoj tehnici pošto su to bile jedine sekvence čiji su bočni lobovi imali vrednost koja nije bila veća od jedinice.

S vremenom se pojavila potreba za dužim sekvencama, posebno kada je u vojnim komunikacionim uređajima počeo da se primenjuje prenos u proširenom spektru (Spread Spectrum). Osobine sekvenci za prenos u proširenom spektru trebalo je da ispunjavaju iste zahteve kao osobine sekvenci za kompresiju impulsa. Prva naširoko poznata i primenjivana familija sekvenci bile su PN (PseudoNoise) sekvence [Golomb 64] i [Golomb 67]. One su imale bočne lobove jednake  $-1$  samo ako se posmatraju kao perodične sekvence pa su u neku ruku bile slične Barkerovim sekvencama. Verovatno su PN sekvence doživele veliku popularnost u inženjerskoj zajednici najviše zahvaljujući knjizi koju je Golomb napisao 1967. godine iako se u matematičkoj literaturi takve sekvence spominju još 1931. godine.

Prvi rad Golej je objavio 1949. godine [Golay 49], ali u časopisu koji se bavi optikom. Tek 12 godina kasnije, 1961, Golej objavljuje u IRE Transactions on Information Theory svoj fundamentalni rad [Golay 61] o binarnim komplementarnim sekvencama, no on biva dugo neprimećen (u šezdesetim godinama je bio samo jednom citiran dok je Golombova knjiga koja je izašla 6 godina kasnije citirana 90 puta u istoj deceniji). Prošlo je skoro 40 godina dok komplementarne sekvence nisu postale naširoko prihvaćene.

Zanimljivo je napomenuti da se u matematičkoj literaturi od 1951. zna za specijalnu familiju binarnih komplementarnih sekvenci. Ona nosi naziv Rudin-Šapiroovi polinomi [Shapiro 51], [Rudin 59] (iako neki smatraju da se Rudinu neopravdano pripisuju zasluge). Dugo posle objavljivanja Golejevog rada nije uočena veza između te dve oblasti

a danas se ponekad u literaturi sreće naziv Golej-Rudin-Šapiroove sekvence, odnosno polinomi. Ovi polinomi nisu ništa drugo nego  $Z$  transformacija odgovarajućih sekvenci. Više decenija posle objavljivanja Golejevog rada u matematičkoj literaturi se mogu naći radovi o Rudin-Šapiroovim polinomima u kojima se ne spominju Golejeve komplementarne sekvence iako one čine mnogo opštiju familiju sekvenci, odnosno polinoma.

Postoje i drugi radovi koji uvode sekvence za koje se kasnije pokazalo da su povezane s Golejevim sekvencama. Godine 1960. Velti je opisao kvaternarne sekvence pogodne za radarsku primenu [Wolti 60]. Turin je ubrzo pokazao [Turyn 63] vezu između Veltijevih sekvenci i Golejevih sekvenci. Kasnije se pojavljuju radovi o Hajzenberg-Vejlovim matricama (Heisenberg-Weil matrices) i o PONS (Prometheus Orthonormal Sets) sekvencama [An 05] koje su takođe tesno povezane s komplementarnim sekvencama i predstavljaju njihovo ponovno otkrivanje u novom kontekstu.

### 1.1. Istorijat istraživanja komplementarnih sekvenci

Iako je Golej [Golay 61] uveo pojam komplementarne sekvence za binarne parove, on je uopštavan na više načina. Pre svega alfabet je s binarnog proširen na više-fazni pa se dalje proširio na polje kompleksnih brojeva, bilo u diskretnoj formi kao što su M-QAM konstelacije ili u kontinualnoj formi kao što su, na primer, komplementarne Huffmanove sekvence [Budišin 90C]. Predmet ove disertacije su isključivo komplementarni parovi sekvenci, ali bez ikakvog ograničenja što se tiče alfabetu.

S druge strane, teorija komplementarnih sekvenci se proširuje na komplementarne skupove. U toj oblasti se dosta radilo ali još uvek ne postoji zaokružena teorija niti standardni algoritmi kakvi su poznati za komplementarne parove. Komplementarni skupovi nisu predmet ove disertacije.

Teorija takođe uvodi pojmove višedimenzionalnih komplementarnih sekvenci, periodičnih komplementarnih sekvenci i sl. ali za sada te varijante nisu izazvale veće interesovanje.

### 1.1.1. Golejevi binarni komplementarni parovi

Golej je u radu [Golay 61] opisao binarne parove komplementarnih sekvenci. On je dao direktnu konstrukciju binarnih parova za dužine jednake  $2^N$ . Takođe je istraživao postoje li komplementarni parovi za druge dužine i pokazao da njihova dužina sekvenci mora biti jednaka zbiru dva kvadrata. On je našao dva neekvivalentna para komplementarnih sekvenci dužine 10, a kasnije su numeričkim pretraživanjem pronađeni i po jedan par dužine 26 [Jaugegui 62] i 20 [Borwein 03]. Danas su to jedine dužine koje nisu stepen dvojke za koje je poznato da postoje binarni komplementarni parovi:

$$a_{10} = [+1, -1, -1, +1, +1, +1, +1, +1, 1, -1]$$

$$b_{10} = [+1, -1, -1, -1, +1, -1, +1, -1, -1, +1]$$

$$a'_{10} = [+1, -1, -1, +1, +1, +1, +1, +1, +1, -1]$$

$$b'_{10} = [+1, -1, -1, -1, +1, -1, +1, -1, -1, +1]$$

$$a_{20} = [+1, +1, +1, +1, -1, +1, -1, -1, -1, +1, +1, -1, -1, +1, +1, -1, -1, -1, +1]$$

$$b_{20} = [+1, +1, +1, +1, -1, +1, +1, +1, +1, +1, -1, -1, -1, +1, -1, +1, -1, +1, -1]$$

$$a_{26} = [+1, +1, +1, +1, -1, +1, +1, -1, -1, +, -1, +1, -1, +1, -1, -1, +1, +1, +1, -1, -1, +1, +1, +1]$$

$$b_{26} = [+1, +1, +1, +1, -1, +1, +1, -1, -1, +1, -1, +1, +1, +1, +1, -1, +1, -1, -1, -1, +1, +1, -1, -1, -1]$$

Golej [Golay 61] takođe navodi nekoliko rekurzivnih algoritama pomoću kojih se od kraćih komplementarnih sekvenci dobijaju duže. Najjednostavniji su algoritam za spajanje sekvenci i algoritam za učešljavanje sekvenci. Ipak Golej je ostavio otvoreno pitanje da li se primenom rekurzivnih algoritama na sekvence dobijene direktnom (nerekurzivnom) konstrukcijom dobijaju nove sekvence ili iste one koje se mogu dobiti samo primenom direktne konstrukcije. Takođe on nije odgovorio na pitanje koliko ima različitih komplementarnih sekvenci određene dužine. Primenom algoritama koje je formulisao Golej i kasnije Turin [Turyn 63] mogu se dobiti sekvence dužine  $2^n 10^m 26^k$ .

## 1.1.2. Komplementarni skupovi

Dalje uopštenje pojma komplementarnih sekvenci izvedeno je u [Tseng 72], gde je uveden pojam komplementarnih skupova. Skup sekvenci se naziva komplementarnim ako je zbir autokorelacionih funkcija sekvenci delta impuls. Uslov da sekvenca pripada komplementarnom skupu je manje strog od uslova da pripada komplementarnom paru. Komplementarni parovi se mogu smatrati specijalnim slučajem skupova od dve sekvence. Iako postoji dosta radova o komplementarnim skupovima, generalna konstrukcija do sada nije postavljena. Pošto komplementarni skupovi nisu predmet ove disertacije njima se nadalje nećemo baviti.

## 1.1.3. Polifazne komplementarne sekvence

U radovima [Sivaswamy 78] i [Frank 80] uvedene su polifazne komplementarne sekvence kao uopštenje binarnih komplementarnih sekvenci. Kod polifaznih sekvenci velika novina je bilo to što postoje sekvence za neparne dužine, recimo 3, 5, 11 i 13. Primeri takvih sekvenci su [Gibson 11]:

$$a_3 = [1, 1, -1]$$

$$b_3 = [1, i, 1]$$

$$a_5 = [1, 1, 1, -i, i]$$

$$b_5 = [1, i, -1, 1, -i]$$

$$a_{11} = [1, 1, 1, i, -1, 1, i, -i, i, 1, -1]$$

$$b_{11} = [1, i, -1, -1, -1, i, i, 1, -i, i, 1]$$

$$a_{13} = [1, 1, 1, i, -1, 1, 1, -i, 1, -1, 1, -i, i]$$

$$b_{13} = [1, i, -1, -1, -1, i, -1, 1, 1, -i, -1, 1, -i]$$

U radu [Budišin 90A] dat je opšti rekurzivni algoritam za generisanje polifaznih sekvenci dužine  $2^N$ . Taj algoritam takođe generiše sve Golejeve binarne sekvence dužine  $2^N$  kao specijalan slučaj.

Najzad, u radu [Davis 99] dat je opšti nerekurzivni algoritam za generisanje polifaznih sekvenci s konačnim alfabetom čiji su elementi kompleksni koreni jedinice.

### 1.1.4. Višedimenzionalne komplementarne sekvence

Komplementarne sekvence koje smo do sada spominjali jesu vektori koji zavise od jednog indeksa. Višedimenzionalne komplementarne sekvence jesu vektori koji zavise od više indeksa; njih su uveli Jedwab i Parker u [Jedwab 07] i dali im naziv Complementary Arrays. Pokazalo se da takav koncept značajan u razvoju teorije pošto je moguće predstaviti jednodimenzionalne sekvence dužine  $2^N$  kao preslikavanje N-dimenzionalnih sekvenci dužine 2. Neki drugi algoritmi za formiranje dužih sekvenci od kraćih takođe se mogu formulisati na taj način.

### 1.1.5. Komplementarnost spektra

Iako komplementarnost spektra direktno proističe iz komplementarnosti autokorelacione funkcije ona je prvi put uočen u [Budišin 87]. Kasnije [Popovic 91] opisuje primenu komplementarnih sekvenci u generisanju višetonskih signala s malim vršnim faktorom. U radu [Popovic 99A] takođe se predlaže primena komplementarnih sekvenci na MC-CDMA (Multi-carrier code division multiple access) koji je u stvari kombinacija sistema OFDM (Orthogonal frequency-division multiplexing) i CDMA (Code division multiple access). Direktna predlog da se komplementarne sekvence koriste u OFDM sistemima prvi put je iznet u [Davis 99].

Iz osobine spektralne komplementarnosti proističe i osobina svih sekvenci koje pripadaju nekom komplementarnog para, a to je da im je vršna snaga u spektru ograničena na dvaput srednju snagu spektra. U OFDM sistemima ta osobina se koristi tako što se komplementarne sekvence dovode na ulaz IFFT (Inverse Fast Fourier transform) bloka kako bi se na njegovom izlazu dobio signal ograničene vršne snage. To je veoma važna osobina koja se koristi da bi se postigla dobra efikasnost izlaznog pojačavača i ostvarila mala potrošnja uređaja baziranih na OFDM.

### 1.1.6. Nestandardne komplementarne sekvence

Standardne komplementarne sekvence dužine  $2^N$  dobijaju se pomoću opšteg algoritma koji generiše sekvence za proizvoljnu vrednost  $N$ . Kompjuterskim pretraživanjem se pokazalo da postoje sekvence dužine  $2^N$  koje se ne mogu dobiti opštim algoritmom. Prvi rad o tome [Li 05] koji je pokazao da postoje nestandardne 4-PSK (PSK – Phase-shift keying) sekvence dužine 16 izazvao je pravu pometnju među teoretičarima komplementarnih sekvenci. Stoga se pojavilo više radova u kojima se objašnjavala ta pojava. Drugi značajan rad [Fiedler 10] odnosi se na 6-PSK sekvence dužine 16 i privukao je mnogo manju pažnju. Sledeći rad o tome odnosi se na 16-QAM (QAM – Quadrature amplitude modulation) sekvence [Li 09] dužine 4 i pokazao je da postoji značajan broj nestandardnih sekvenci i da je on oko 60% broja standardnih sekvenci. Nažalost, broj 16-QAM sekvenci jako brzo raste s dužinom, tako da je praktično nemoguće pretražiti duže sekvence.

Stoga važi generalni utisak da pojava nestandardnih komplementarnih sekvenci nije izuzetak nego pravilo. Kako izgleda, može se očekivati da će se za dovoljno velike dužine sekvenci kad-tad otkriti neki skup nestandardnih sekvenci. Za sada nisu pronađene binarne nestandardne sekvence ali je veoma verovatno da one postoje za dovoljno veliku dužinu.

### 1.1.7. Veza s Rid-Milerovim kodovima

U radu [Davis 99] prvi put je otkrivena veza komplementarnih sekvenci s Rid-Milerovim (Reed-Muller) zaštitnim kodovima. U tom radu dat je algoritam za direktno generisanje komplementarnih sekvenci pomoću Bulovih funkcija. Drugi veoma značajan rad koji je razradio tu vezu i proširio je na komplementarne skupove sekvenci jeste [Paterson 00].

Postoje dva osnovna pristupa teoriji komplementarnih sekvenci. Prvi se zasniva na nerekurzivnom algoritmu (direktna metoda) i koristi Bulove funkcije. Drugi pristup se zasniva na rekurzivnom algoritmu u doveo je do predstavljanja sekvence pomoću paraunitarnih matrica. Upravo taj pristup mi ovde razrađujemo. Zbog toga ovde nećemo davati detalje prvog pristupa nego ćemo se posvetiti isključivo drugom pristupu.

Važno je znati da je prvi pristup omogućio otkrivanje veze Golejevih sekvenci s Rid-Milerovim kodovima. To je dalje dovelo do određivanja minimalnog Hamingovog rastojanja između svih standardnih Golejevih sekvenci određene dužine. I najzad, to je

omogućilo primenu efikasnih algoritama za dekodovanje Rid-Milerovih kodova na detektovanje Golejevih sekvenci.

### 1.1.8. QAM komplementarne sekvence

Po usvajanju OFDM prenosa kao najboljeg rešenja za mobilnu telefoniju javila se potreba za generisanjem što većeg broja različitih QAM komplementarnih sekvenci. Radovi koji su položili temelje te teorije jesu: [Roßing 01], [Chan 03], [Lee 06], [Li 08] i [Chang 10]. O ovim sekvencama će biti vie reči u poglavlju 6.

## 1.2. Oblasti primene

Zbog svojih izuzetnih osobina komplementarne sekvence su našle primenu u raznim oblastima tehnike i nauke.

### 1.2.1. Optika (Multislit spectrometry)

To je prva opisana oblast primene koju je naveo Golej [Golay 49] i [Golay 61]. Pošto se ova primena ne odnosi na oblast elektrotehnike nećemo je opisivati.

### 1.2.2. Kompresija impulsa u radarima

Ovo je prva oblast elektronike gde se pojavilo interesovanje za primenu komplementarnih sekvenci. Sivasvami (Sivaswamy) je među prvima razmatrao primenu komplementarnih sekvenci u radarima [Sivaswamy 78] i [Sivaswamy 82], od ostalih ranih autora vredno je pomenuti rad [Altes 82]. Nešto kasnije u Institutu za primenjenu

fiziku u Beogradu razvija se izviđački radar IR-10 koji koristi komplementarne sekvence. Konceptija kompresije impulsa ovog radara je objavljena 1987. godine [Budišin 87]. Značajno je da se u tom radu komplementarne sekvence pojavljuju u dve uloge. S jedne strane one bi-fazno modulišu predajni impuls a sa druge strane se koriste kao makrosekvence. Makrosekvencija određuje koja će od dve sekvence iz komplementarnog para u kom impulsu biti emitovana. Predloženo je da se komplementarne sekvence primenjuju kao makrosekvence, ne zbog osobine komplementarnosti ili zbog dobrih autokorelacionih osobina nego zbog dobrih spektralnih osobina. Tu je prvi put u literaturi objavljeno da komplementarne sekvence imaju osobinu komplementarnosti spektra i da im spektar snage nikad ne prelazi dvaput srednju vrednost.

U novijim radovima posebno težište se stavlja na primenu polarizovanog signala tako što se po svakoj od dve polarizacione ravni šalje jedna od dve sekvence iz komplementarnog para [Howard 06], [Howard 07], [Calderbank 06], [Searle 07] i [Searle 07A]

Golejeve sekvence su takođe predložene za primenu u sledećoj generaciji radarskih sistema za navođenje (GUIDAR – guided radar) [Harman 05].

Primena komplementarnih sekvenci u nepolarizovanim radarima je obrađena u [Pezeshki 08].

### 1.2.3. WiFi standard – IEEE 802.11b

WiFi standard iz 1999 [IEEE 802.11b] uvodi Complementary Code Keying [van Nee 96], [Shao 04] da bi prenosio podatke brzinom od 11 Mbs u lokalnoj bežičnoj mreži u opsegu oko 2,4 GHz. U ovom standardu korišćene su skraćene Golejeve sekvence. Golejeve sekvence su izabrane zbog dobrih spektralnih osobina pošto im vršna snaga ne prelazi srednju snagu za više od 3 dB. Međutim, pri skraćivanju sekvenci vršna snaga ponekad prelazi srednju snagu i za više od 6 dB. Na prijemu se koristi brza Volšova transformacija FWT (Fast Walsh transform) i RAKE prijemnik.

Ipak, uređaji po WiFi standardu su verovatno do sada najmasovnije proizvedeni uređaji koji koriste komplementarne sekvence.

### 1.2.4. 3G mobilna telefonija – UMTS standard

Usvajanje komplementarnih sekvenci za RACH (Random Access Channel) preambulu [ERICSSON 99] u UMTS (Universal Mobile Telecommunications System) standardu rezultat je nekoliko radova autora iz Instituta za primenjenu fiziku iz Beograda. Godine 1991. je objavljen rad [Budišin 91] gde je prvi put prezentiran efikasni korelator za komplementarne sekvence. Rad je ostao prilično nezapažen u telekomunikacionoj zajednici pošto je težište rada bilo na radarskoj primeni. Godine 1999. dr Branislav Popović objavljuje rad [Popović 99] gde iznosi neka objašnjenja algoritma ali predlaže da se primeni u RACH bloku 3G (3rd generation) standarda. Popović tada radi u Eriksonu, u grupi za standardizaciju, i njegov veoma zapažen rad doprinosi da komplementarne sekvence i efikasni korelator uđu u standard za 3G telefoniju.

Pored toga, u varijanti 3G standarda namenjenoj kineskom tržištu takođe se koriste komplementarne sekvence i to na tri mesta. To je UMTS WCDMA (Wideband Code Division Multiple Access) TDD (Time-division duplex) standard [Rudolf 01] i [Chitrapu 04]. U ovoj varijanti 3G standarda komplementarne sekvence se koriste u sledećim ulogama: preambula u RACH bloku, sekvenca za sinhronizaciju i kao referentni signal.

### 1.2.5. WiMax standard – IEEE 102.16

Dalja evolucija WiFi standarda dovela je do WiMax standarda [IEEE 802.16]. Taj standard se često spominje kao 4G standard i zamišljeno je da konkuriše LTE (Long Term Evolution) standardu mobilne telefonije. Kao LTE standard, i WiMax je baziran na OFDM-u.

Komplementarne sekvence se koriste u WiMax standardu kao pilot sekvence za određivanje karakteristike kanala. Ove sekvence dužina 109, 433, 865 i 1729 dobijene su skraćivanjem Golejevih binarnih sekvenci dužina 128, 512, 1024 i 2.048.

### 1.2.6. OFDM

Problem vršnog faktora koji je poznat pod skraćenicom PAPR (Peak-to-Average Power Ratio) još uvek nije zadovoljavajuće rešen u novim sistemima na bazi OFDM

modulacije kao što su LTE i WiMax. Jedna od varijanti rešenja koja se intenzivno istražuje jeste primena komplementarnih sekvenci i to posebno QAM komplementarnih sekvenci.

Prvi rad gde su objavljene dobre spektralne osobine komplementarnih sekvenci nastao je u Institutu za primenjenu fiziku [Budišin 87] ali je taj doprinos ostao neprimećen. Sledeći važan rad objavljuje Branislav Popović [Popovic 91] i on je citiran 159 puta. Zatim sledi [Popovic 99A] koji je citiran 139 puta. Konačni zamajac primeni komplementarnih sekvenci u OFDM sistemima daju Davis i Jedwab u [Davis 99] u radu koji je citiran 562 puta.

Posle toga se pojavljuju mnogi predlozi za generisanje QAM komplementarnih sekvenci u cilju povećanja broja različitih sekvenci i povećanja brzine prenosa. Najznačajniji radovi su: [Roßing 01], [Chong 03], [Lee 06], [Li 08] i [Chang 10].

### 1.2.7. Ostale primene

- Ultrazvuk – [Diaz 99], [Hernandez 03] i [Alvareza 06],
- Akustika [Foster 1986],
- Magnetno snimanje [Braun 98]
- Estimacija kanala [Spasojević 01] i [Wang 07]
- Testiranje elektronskih sistema [Ghani 10]

## 1.3. Prednosti komplementarnih sekvenci

Najšire korišćene i najpoznatije binarne sekvence su svakako PN sekvence (pseudo-noise sequences), takođe poznate pod nazivima: m-sekvence (m-sequences), sekvence maksimalne dužine (maximal length sequences) i sekvence generisane pomoću šift registara (shift register sequences) [Golomb 64] i [Golomb 67]. U poređenju s njima, binarne komplementarne sekvence, često nazvane Golejeve sekvence, imaju niz prednosti:

Teorija komplementarnih sekvenci se zasniva na matematici u polju realnih brojeva dok se teorija PN sekvenci zasniva na konačnim poljima Galoa, a ona je inženjerima znatno manje poznata.

Dužina sekvenci u najbrojnijoj potfamiliji Golejevih sekvenci je  $2^N$  dok PN sekvence imaju dužinu  $2^N - 1$ . Pored toga Golejeve sekvence postoje i za mnoge druge dužine dok su PN sekvence ograničene isključivo na dužine  $2^N - 1$ .

Broj različitih Golejevih sekvenci je mnogostruko veći od broja PN sekvenci.

Autokorelacione osobine su slične kod obe familije iako dosta Golejevih sekvenci imaju manje lobove od PN sekvenci [Budišin 92].

Golejeve sekvence imaju ograničen spektar snage na dvaput srednju snagu. PN sekvence mogu da imaju mnogo veće spektralne vrhove.

Golejeve sekvence se mogu uopštiti na polifazne sekvence [Budišin 90A] kojih ima ne-prebrojivo mnogo. One mogu da imaju dužinu  $2^N$  ali i mnoge druge dužine uključujući 3, 5 itd. Polifazne PN sekvence postoje samo sa  $p$  faza gde je  $p$  prost broj i njihova dužina je  $p^N - 1$ .

PN sekvence dužine  $2^N - 1$  imaju linearnu kompleksnost jednaku  $N$  dok Golejeve sekvence imaju linearnu kompleksnost koja se približava  $2^N$ . To ih čini pogodnijim za kriptografske primene od PN sekvenci.

Za generisanje Golejevih sekvenci dužine  $2^N$  koristi se brojač dužine  $N$  praćen veoma jednostavnom logičkom mrežom. PN sekvence se generišu pomoću pomeračkog registra dužine  $N$  s nekoliko povratnih sprega u obliku XOR kola. U suštini, ova dva generatora su veoma slična po složenosti.

Korelator binarnih Golejevih sekvenci [Budišin 91] jeste digitalni filter s  $N$  blokova od koji svaki sadrži samo sabirač i oduzimač. Korelator PN sekvenci može da se efikasno implementira pomoću brze Volšove transformacije koja takođe ima složenost  $N$  ali nju je mnogo komplikovanije implementirati [Budišin 89].

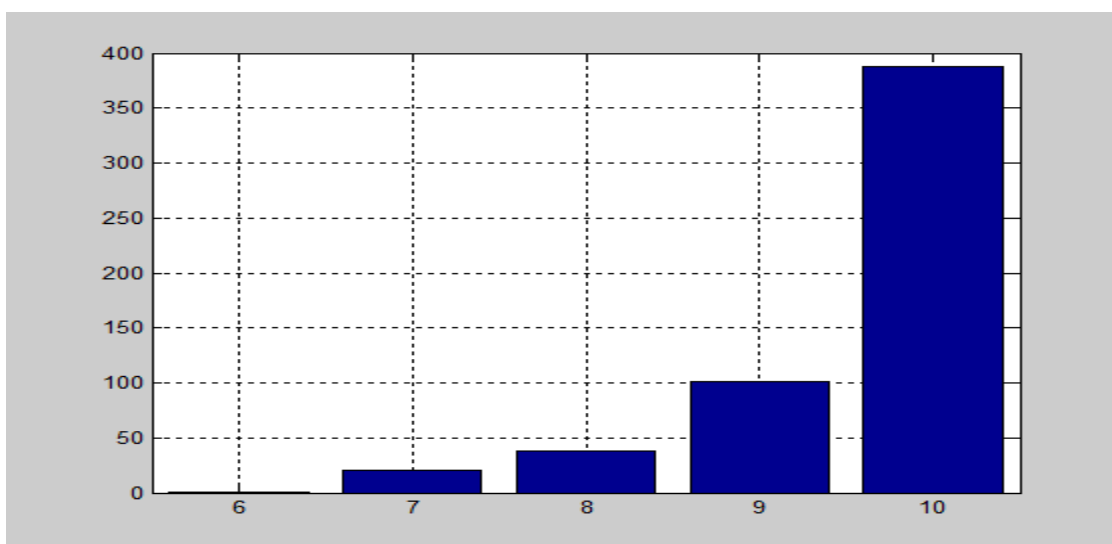
## 1.4. Značaj komplementarnih sekvenci

Od pojave Golejevog rada [Golay 61] interesovanje za komplementarne sekvence je raslo polako ali uporno. Da bismo prikazali kvantitativnu meru tog interesovanja koristili smo nekoliko pokazatelja. Kao prvi pokazatelj je koršćen podatak o citiranosti Golejevog rada po decenijama na osnovu podataka s veb-sajta Google Scholar. Podaci su navedeni u Tab. 1.

Tab. 1. Citiranje Golejevog rada iz 1961. po decenijama

Decenija	1961.-1970.	1971.-1980.	1981.-1990.	1991.-2000.	2001.-2010.
Broj citata	1	21	38	101	388

Taj rast je grafički prikazan na Sl. 1 gde su na X osi označene decenije, pri čemu broj 6 označava šestu deceniju XX veka od 1961. do 1970. a broj 10 prvu deceniju XXI veka od 2001. do 2010.



Sl. 1. Citiranje Golejevog rada iz 1961. po decenijama

Da bismo proučili koliko su koje oblasti doprinele u tom rastu interesovanja, ponovo smo koristili pretraživanje u Google Scholar-u. Ti podaci su mnogo manje pouzdani od podataka o citiranosti pošto su mnogi radovi više puta navedeni a ponekad se desi da Google Scholar na zadate ključne reči prikaže i radove koji se ne odnose na oblast koja nas zanima. Ipak, verujemo da je tih slučajeva malo i da dobijeni podaci daju dobru indikaciju o trendovima. Rezultati su prikazani u Tab. 2.

Tab. 2. Rezultati pretraživanja po ključnim rečima u Google Scholaru

Ključne reči / Decenija	1961.-1970	1971.-1980	1981.-1990	1991.-2000	2001...-2010
Golay Complementary	83	191	352	981	3.589
Golay Complementary radar	20	36	64	92	281
Golay Complementary CDMA	0	0	0	61	388
Golay Complementary OFDM	0	0	0	69	636

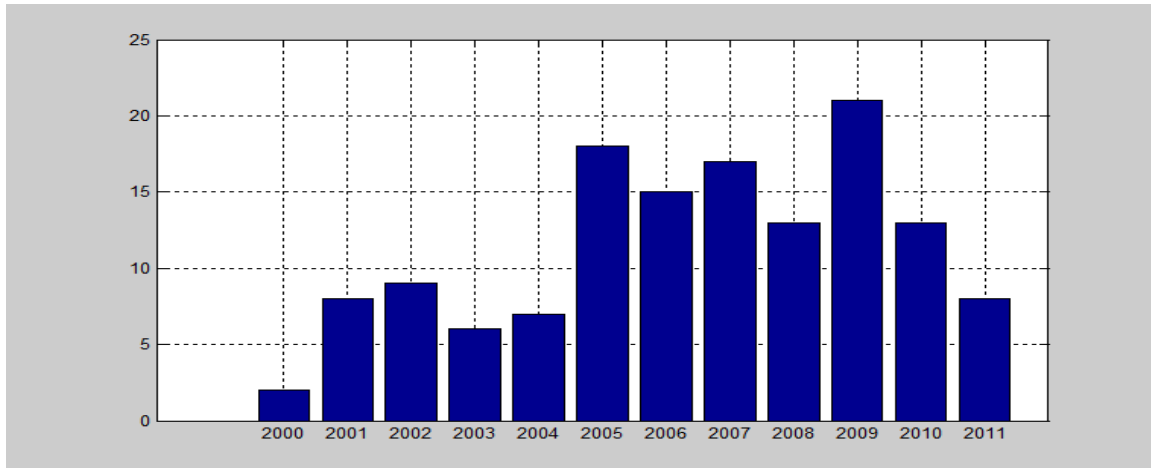
U prvoj koloni su date ključne reči korišćene u pretraživanju. Od 3 analizirane oblasti vidi se da je radarska oblast zastupljena od samog početka, dok CDMA i OFDM počinju da budu značajne tek od poslednje decenije prošlog veka. Takođe se može uočiti i to da OFDM preuzima primat u prošloj deceniji, a to se zbiva pre svega zato što OFDM postaje standardna modulacija za mobilnu telefoniju četvrte generacije.

Podatke o citiranosti radova autora ove disertacije koji su nastali u periodu od 1986. do 1991. godine prikazujemo u Tab. 3. Što je zanimljivo, od 147 citata samo se 10 javlja devedesetih godina, svi ostali su iz perioda posle 2000. godine – više od 20 godina posle njihovog objavljivanja.

Tab. 3. Citiranje značajnijih autorovih radova po godinama

Decenija	90-te	00	01	02	03	04	05	06	07	08	09	10	11
Designing radar signals using complementary sequences [Budišin 87]		1					1	3	2	1		1	
New complementary pairs of sequences [Budišin 90A]	7	1	2	3	2	4	8	7	4	4	9	5	1
New multilevel complementary pairs of sequences [Budišin 90B]	1		1	1	1				1			2	1
Efficient pulse compressor for Golay complementary sequences [Budišin 91]	2		4	4	2	1	8	5	7	6	8	4	5
Golay complementary sequences are superior to PN sequences [Budišin 92]			1	1	1	2	1		3	2	4	1	1
TOTAL	10	2	8	9	6	7	18	15	17	13	21	13	8

Poseban kuriozitet jeste to da je rad „Designing radar signals using complementary sequences”, koji je se bavi čisto radarskom problematikom, citiran isključivo posle 2000. godine i to uglavnom 20 godina otkako je objavljen. Broj citata po godinama je prikazan na Sl. 2.



Sl. 2. Citiranje autorovih značajnijih radova po godinama

## 1.5. Banke filtera i paraunitarne matrice

Teorija o bankama filtera (Filter Banks) [Vaidyanathan 93] veoma je značajna u oblasti digitalnih filtera. Nastala je na osnovu potrebe da se signal razloži na niz uskopojasnih signala koja se javlja u raznim primenama. Ova teorija je doživela pravi procvat s primenom u kompresiji signala i to naročito muzičkih i video signala (izraz kompresija u ovom slučaju nema direktnu vezu sa izrazom kompresija impulsa iz radarske tehnike). Iz ove teorije nastaje druga veoma popularna teorija o talasićima (wavelets).

Sama teorija o bankama filtera koja se razvijala preko polifaznih filterskih banaka i filterskih banaka za savršenu rekonstrukciju dovodi do matematičkog pojma paraunitarnih matrica.

Veza između filterskih banaka i komplementarnih sekvenci je ranije spomenuta u nekim radovima. Tako se u dva rada istoga autora [Phoong 03] i [Phoong 05] konstatuje da se paraunitarne matrice s binarnim koeficijentima mogu dobiti pomoću Golejevih sekvenci, ali se ne predlažu nikakvi zaključci o primeni na analizu i sintezu komplementarnih sekvenci. Zanimljivo je da se u tim radovima koristi termin „Lapped Hadamrd Transform Matrix“ koji je sinonim za paraunitarne matrice. Treći rad o tome je [Candan 06], gde autor primenjuje teoriju polifaznih filterskih banaka na generisanje komplementarnih sekvenci i detaljnije razrađuje algoritam za generisanje

komplementarnog skupa od 4 sekvence. Autor se ne bavi primenom teorije na komplementarne parove.

## 1.6. Struktura disertacije

Ova disertacija je podeljena na sedam poglavlja.

U uvodnom poglavlju je dat istorijat razvoja teorije komplementarnih sekvenci, pregled najvažnijih primena, prednosti komplementarnih sekvenci, njihov značaj u literaturi i najzad pregled literature o paraunitanim matricama.

U drugom poglavlju je data notacija, terminologija i osnovne definicije koje su nam potrebne za iznošenje teorijskih rezultata.

U trećem poglavlju su detaljno analizirane osobine binarnih komplementarnih sekvenci i upoređene s najprihvaćenijim PN sekvencama i pokazano je da komplementarne sekvence, po mnogim karakteristikama, imaju bolje osobine od PN sekvenci.

U četvrtom poglavlju je dat pregled poznatih algoritama za generisanje i korelisanje komplementarnih sekvenci.

U petom poglavlju je prikazan osnovni doprinos disertacije. Polazeći od ekvivalentnosti uslova komplementarnosti sekvenci i definicije paraunitarnih matrica, izvedena je faktorizaciju paraunitarnih matrica i pokazano da se pomoću nje može prikazati proizvoljni komplementarni par. Zatim je pokazano da se parametri te reprezentacije mogu izračunati za proizvoljan komplementarni par, čime je dokazano da je ta reprezentacija univerzalna i jedinstvena, to jest, da važi za bilo koji par.

U šestom poglavlju dati su brojni primeri koji ilustruju paraunitarnu dekompoziciju i reprezentaciju.

Zaključak je u sedmom poglavlju.

## 2. Notacija, terminologija i definicije

U ovom poglavlju navodimo osnovno o korišćenim matematičkim pojmovima, teoriji sekvenci generalno i posebno o teoriji komplementarnih sekvenci.

### 2.1. Matematička notacija i terminologija

Gde god je moguće koristili smo sledeće konvencije:

- Velikim slovima iz skupa  $[K, L, M, N, \dots]$  označavamo celobrojne konstante
- Malim slovima iz skupa  $[k, l, m, n, \dots]$  označavamo celobrojne promenljive
- Ostalim velikim slovima označavamo realne ili kompleksne konstante
- Ostalim malim slovima označavamo realne ili kompleksne promenljive (izuzetak je promenljiva  $Z$  koja se pojavljuje u  $Z$  transformaciji i koja se tradicionalno označava velikim slovom)
- Masnim velikim slovima označavamo matrice, na primer  $\mathbf{Y}$
- Masnim malim slovima označavamo vektore, na primer  $\mathbf{x}$

#### 2.1.1. Unitarne matrice i transformacije

Ortogonalni vektori se definišu kao vektori čiji je skalarni proizvod jednak nuli.

Ortogonalne matrice jesu matrice s realnim elementima čije su sve kolone (odnosno vrste) međusobno ortogonalne. Unitarne matrice su generalizacija pojma ortogonalnih matrica na matrice s kompleksnim elementima. One zadovoljavaju uslove:

$$\mathbf{U}^H \cdot \mathbf{U} = \mathbf{I}_N \quad (1)$$

gde  $(\cdot)^H = ((\cdot)^*)^T = ((\cdot)^T)^* = (\cdot)^{*T}$  označava Hermitov operator (kompleksno konjugovanje i transponovanje).

Transponovana unitarna matrica ostaje unitarna.

Kompleksno konjugovana unitarna matrica ostaje unitarna.

Množenje bilo koje vrste ili kolone unitarne matrice s jediničnim kompleksnim brojem daje unitarnu matricu.

Permutacijom vrsta i kolona unitarne matrice dobija se unitarna matrica.

Opšti oblik unitarne matrice veličine  $2 \times 2$  je [Murnaghan 62]:

$$\mathbf{U} = \begin{bmatrix} C & S \\ -S^* & C^* \end{bmatrix} \quad (2)$$

gde  $(\cdot)^*$  označava kompleksno konjugovanje a  $|C|^2 + |S|^2 = 1$ . Ovo je ujedno i matični oblik kvaterniona.

Invertovana unitarna matrica veličine  $2 \times 2$  je:

$$\mathbf{U}^{-1} = \mathbf{U}^H = \begin{bmatrix} C^* & -S \\ S^* & C \end{bmatrix} \quad (3)$$

Proizvod dve unitarne matrice je unitarna matrica Tako za matrice veličine  $2 \times 2$  imamo:

$$\begin{aligned} \mathbf{U}_1 \cdot \mathbf{U}_2 &= \begin{bmatrix} C_1 & S_1 \\ -S_1^* & C_1^* \end{bmatrix} \begin{bmatrix} C_2 & S_2 \\ -S_2^* & C_2^* \end{bmatrix} = \begin{bmatrix} C_1 C_2 - S_1 S_2^* & C_1 S_2 + S_1 C_2^* \\ -S_1^* C_2 - C_1^* S_2^* & C_1^* C_2^* - S_1^* S_2 \end{bmatrix} \\ &= \begin{bmatrix} (C_1 C_2 - S_1 S_2^*) & (C_1 S_2 + S_1 C_2^*) \\ -(C_1 S_2 + S_1 C_2^*)^* & (C_1 C_2 - S_1 S_2^*)^* \end{bmatrix} = \begin{bmatrix} C_3 & S_3 \\ -S_3^* & C_3^* \end{bmatrix} = \mathbf{U}_3 \end{aligned} \quad (4)$$

Gde je  $C_3 = (C_1 C_2 - S_1 S_2^*)$  a  $S_3 = (C_1 S_2 + S_1 C_2^*)$

Poznati primeri unitarnih matrica su Volšove matrice, DFT (Discrete Fourier transform) matrice i permutacione matrice. Inače, svakoj unitarnoj matrici može se pridružiti ortogonalna transformacija definisana množenjem s tom unitarnom matricom. Inverzna transformacija se definiše množenjem s Hermitovom matricom dobijenom od te unitarne matrice. Tako su definisane npr. Volšova transformacija i DFT transformacija.

## 2.1.2. Z transformacija

U oblasti digitalne obrade signala često se koristi Z transformacija koja se za signal  $x(n)$  definiše kao:

$$X(Z^{-1}) = \sum_{n=-\infty}^{+\infty} x(n)Z^{-n} \quad (5)$$

Matematički naziv ovakvog izraza glasi beskonačan Loranov polinom. Ukoliko je signal  $x(n)$  kauzalan, onda indeks  $n$  ide od 0 do beskonačnosti pa se  $Z$  transformacija svodi na običan beskonačni polinom po  $Z^{-1}$ . Ukoliko je signal  $x(n)$  konačnog trajanja, onda se njegova  $Z$  transformacija svodi na običan polinom po  $Z^{-1}$ .

$Z$  transformacija se koristi i za predstavljanje impulsnog odziva diskretnog filtera (često nazvanog digitalni filter). Kako je impulсни odziv kauzalnog filtera uvek kauzalan, njegova  $Z$  transformacija je običan filter. Ako je impulсни odziv konačan, takav filter se zove FIR (Finite Impulse Response) filter. Ukoliko je beskonačan, zove se IIR (Infinite impulse response) filter. IIR filteri se najčešće predstavljaju kao racionalna funkcija, odnosno kao količnik dva polinoma.  $Z$  transformacija impulsnog odziva filtera naziva se prenosna funkcija filtera.

Ako je prenosna funkcija filtera  $H(Z^{-1})$  i  $Z$  transformacija ulaznog signala  $X(Z^{-1})$  onda se  $Z$  transformacija izlaznog signala  $y(n)$  može dobiti kao:

$$Y(Z^{-1}) = H(Z^{-1}) \cdot X(Z^{-1}) \quad (6)$$

### 2.1.3. Matrični polinomi

Ukoliko imamo matricu čiji su elementi polinomi po  $Z^{-k}$  takođe je možemo predstaviti i kao polinom čiji su koeficijenti matrice.

$$\begin{aligned}
 \mathbf{P}(Z) &= \begin{bmatrix} \sum_{k=0}^{N-1} p_{11}^{(k)} Z^{-k} & \sum_{k=0}^{N-1} p_{12}^{(k)} Z^{-k} & \dots & \sum_{k=0}^{N-1} p_{1M}^{(k)} Z^{-k} \\ \sum_{k=0}^{N-1} p_{21}^{(k)} Z^{-k} & \sum_{k=0}^{N-1} p_{22}^{(k)} Z^{-k} & \dots & \sum_{k=0}^{N-1} p_{2M}^{(k)} Z^{-k} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \sum_{k=0}^{N-1} p_{M1}^{(k)} Z^{-k} & \sum_{k=0}^{N-1} p_{M2}^{(k)} Z^{-k} & \dots & \sum_{k=0}^{N-1} p_{MM}^{(k)} Z^{-k} \end{bmatrix} \\
 &= \sum_{k=0}^{N-1} \begin{bmatrix} p_{11}^{(k)} & p_{12}^{(k)} & \dots & p_{1M}^{(k)} \\ p_{21}^{(k)} & p_{22}^{(k)} & \dots & p_{2M}^{(k)} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ p_{M1}^{(k)} & p_{M2}^{(k)} & \dots & p_{MM}^{(k)} \end{bmatrix} Z^{-k}
 \end{aligned} \tag{7}$$

Zato ovakve matrice zovemo matrični polinomi ali možemo ih zvati i polinomijalne matrice pošto se mogu prikazati i u obliku matrica čiji su elementi polinomi. Mi ćemo u ovoj disertaciji isključivo koristiti matrice  $2 \times 2$  i  $2 \times 2$  koje imaju oblik:

$$\mathbf{P}(Z) = \begin{bmatrix} \sum_{k=0}^{N-1} p_{11}^{(k)} Z^{-k} & \sum_{k=0}^{N-1} p_{12}^{(k)} Z^{-k} \\ \sum_{k=0}^{N-1} p_{21}^{(k)} Z^{-k} & \sum_{k=0}^{N-1} p_{22}^{(k)} Z^{-k} \end{bmatrix} = \sum_{k=0}^{N-1} \begin{bmatrix} p_{11}^{(k)} & p_{12}^{(k)} \\ p_{21}^{(k)} & p_{22}^{(k)} \end{bmatrix} Z^{-k} \tag{8}$$

odnosno:

$$\mathbf{P}(Z) = \begin{bmatrix} \sum_{k=0}^{N-1} p_{11}^{(k)} Z^{-k} \\ \sum_{k=0}^{N-1} p_{21}^{(k)} Z^{-k} \end{bmatrix} = \sum_{k=0}^{N-1} \begin{bmatrix} p_{11}^{(k)} \\ p_{21}^{(k)} \end{bmatrix} Z^{-k} \tag{9}$$

## 2.1.4. Matrični proizvodi

U daljem tekstu često ćemo koristiti proizvode matrica sledećeg oblika:

$$\prod_{k=N}^1 \mathbf{A}_k(Z^{-1}) = \mathbf{A}_N(Z^{-1}) \cdot \mathbf{A}_{n-1}(Z^{-1}) \dots \mathbf{A}_2(Z^{-1}) \cdot \mathbf{A}_1(Z^{-1}) \quad (10)$$

Kako matrično množenje nije komutativno, u ovom proizvodu je bitno da rastući indeksi dolaze s leve strane, odnosno da je proizvod definisan rekurzijom:

$$\prod_{k=N}^1 \mathbf{A}_k(Z^{-1}) = \mathbf{A}_N(Z^{-1}) \cdot \left\{ \prod_{k=N-1}^1 \mathbf{A}_k(Z^{-1}) \right\} \quad (11)$$

## 2.1.5. Permutacije i permutaciona matrica

Pod permutacijom podrazumevamo svako jednoznačno preslikavanje skupa  $S = \{0, 1, 2, \dots, n-1\}$  na samog sebe. To znači da je preslikavanje 1-na-1. Svako takvo preslikavanje prikazaćemo nizom  $[P(0), P(1), P(2), \dots, P(n-1)]$ . Skup tih preslikavanja čini grupu, evo zašto:

Postoji "proizvod" preslikavanja  $P(n) = P_1(P_2(n))$  pri čemu množenje permutacija nije komutativno. Označavaćemo ga s  $P_1 \times P_2$ . U opštem slučaju  $P_1 \times P_2 \neq P_2 \times P_1$ .

Postoji neutralni element:  $P_e = [0, 1, 2, \dots, n-1]$  i on ima osobinu da je  $P_e \times P = P \times P_e = P$ .

Postoji inverzni element  $P^{-1} \times P = P \times P^{-1} = P_e$ .

Broj različitih permutacija je  $n! = 1 \cdot 2 \cdot \dots \cdot n = \prod_{k=1}^n k$ .

**Primer:** sve moguće permutacije dužine 3 jesu:  $[0, 1, 2]$ ,  $[0, 2, 1]$ ,  $[1, 0, 2]$ ,  $[1, 2, 0]$ ,  $[2, 0, 1]$ ,  $[2, 1, 0]$  i ima ih ukupno 6.

Neutralni element je  $P_e = [0, 1, 2]$ .

Svako permutaciji možemo jednoznačno pridružiti permutacionu matricu. Jediničnoj permutaciji (neutralni element) odgovara jedinična matrica. Generalno, permutaciji  $P$  odgovara matrica  $\mathbf{P}$  koja ima jedinice na indeksima  $P_{k+1, P(k)+1} = 1$  dok su svi ostali elementi jednaki nula. Dakle, imamo preslikavanja:

$$\begin{aligned}
 [0, 1, 2] &\Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; [0, 2, 1] \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}; [1, 0, 2] \Rightarrow \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \\
 [1, 2, 0] &\Rightarrow \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}; [2, 0, 1] \Rightarrow \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}; [2, 1, 0] \Rightarrow \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}
 \end{aligned}$$

Najvažnija osobina ovog preslikavanja jeste to što množenju permutacija odgovara množenje permutacionih matrica, neutralni element je jedinična matrica a inverznoj permutaciji odgovara inverzna matrica.

### 2.1.6. Bitska reprezentacija brojeva

Svaki broj možemo predstaviti u binarnom obliku. Za brojeve od 0 do  $2^n - 1$  dovoljno je  $n$  bita za jedinstveno predstavljanje. Neka je  $l$ -ti bit broja  $k$  dat sa  $b_l(k)$  i tada možemo da pišemo:

$$k = \sum_{l=0}^{n-1} b_l(k) 2^l \quad (12)$$

$b_0(k)$  možemo izračunati kao ostatak deljenja sa 2:  $b_0(k) = k \bmod 2$ . Na sličan način možemo izračunati i ostale bitove. Na primer  $b_1(k) = (k - b_0(k))/2 \bmod 2$  ili generalno:

$$b_m(k) = \left( k - \sum_{l=0}^{m-1} b_l(k) 2^l \right) / 2^m \bmod 2 \quad (13)$$

Kako su izrazi  $b_m(k)$  funkcije od  $k$ , uobičajeno je da ih zovemo Bulove funkcije. Ovako definisane Bulove funkcije daju vrednosti 0 i 1 pa ćemo ih još zvati i unipolarne Bulove funkcije. Često su potrebne Bulove funkcije koje uzimaju vrednosti +1 i -1 i njih ćemo zvati Bulove binarne funkcije; dobijamo ih pomoću:

$$B_m(k) = 2b_m(k) - 1 \quad (14)$$

Treba naglasiti da logička operacija XOR primenjena na unipolarne binarne funkcije  $a(k)$  a  $b(k)$  odgovara operaciji množenja u slučaju bipolarnih funkcija:  $a(k) \text{ XOR } b(k) \Leftrightarrow A(k) \cdot B(k)$ . Takođe treba uočiti da logička operacija OR u slučaju unipolarnih binarnih funkcija može da se izrazi kao operacija množenja nad unipolarnim funkcijama:  $a(k) \text{ OR } b(k) \Leftrightarrow a(k) \cdot b(k)$ . Ovo važi za sve binarne funkcije pa i za Bulove.

## 2.1.7. Volšove matrice i Volšove sekvence

Volšove (Walsh) matrice spadaju u širu klasu Hadamardovih matrica koje imaju osobinu da su im elementi samo +1 i -1 i da su ortogonalne. Hadamardove matrice su kvadratne matrice i poznato je da postoje za dimenzije  $2 \times 2$  i za dimenzije koje su umnožak od 4. Ekvivalentne Hadamardove matrice se definišu kao matrice koje se dobijaju permutacijom kolona ili vrsta ili množenjem bilo koje vrste ili kolone sa -1. Neekvivalentne matrice su one koje se ne mogu dobiti pomoću ovih transformacija. Nije poznato koliko ima neekvivalentnih Hadamardovih matrica za proizvoljnu dužinu. Takođe se definišu i generalizovane Hadamardove matrice; njihovi su elementi kompleksni brojevi čiji je moduo jednak jedan.

Volšove matrice su Hadamardove matrice dimenzije  $2^n$  s veoma jednostavnom konstrukcijom. Naime, polazeći od matrice dimenzije jedan:  $W^{(0)} = [1]$  konstruišemo dvaput veće matrice pomoću rekurzivnog algoritma:

$$W^{(K+1)} = \begin{bmatrix} W^{(K)} & W^{(K)} \\ W^{(K)} & -W^{(K)} \end{bmatrix} \quad (15)$$

Primeri Volšovih matrica veličine 2 i 4:

$$W^{(1)} = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}; W^{(2)} = \begin{bmatrix} W^{(1)} & W^{(1)} \\ W^{(1)} & -W^{(1)} \end{bmatrix} = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix} \quad (16)$$

Pojedinačne vrste Volšove matrice često se definišu kao Volšove funkcije ili Volšove sekvence. Za njih ćemo koristiti notaciju  $w_k(m)$  gde indeks k odgovara indeksu vrste matrice, dok m odgovara indeksu kolone matrice. Tako za dimenziju 4 imamo sledeće Volšove funkcije:

$$w_0(n) = [+1, +1, +1, +1],$$

$$w_1(n) = [+1, -1, +1, -1],$$

$$w_2(n) = [+1, +1, -1, -1],$$

$$w_3(n) = [+1, -1, -1, +1],$$

Volšove funkcije mogu se izraziti direktno, pomoću bipolarnih Bulovih funkcija:

$$w_k(m) = \sum_{l=0}^{n-1} B_l(k)B_l(m) \quad (17)$$

## 2.2. Sekvence

Sekvenca  $x(n)$  definiše se kao preslikavanje skupa celih brojeva  $\mathbf{Z}$  na skup kompleksnih brojeva  $\mathbf{C}$ . Ukoliko je  $x(n) = 0$  za svako  $0 \leq n$  i  $n \leq L - 1$  kaže se da je sekvenca konačna a u protivnom je beskonačna. Zbog toga konačnu sekvencu možemo predstaviti kao konačni vektor  $(x(0), x(1), \dots, x(L - 1))$ .

Pored podele na konačne i beskonačne, korisna je i podela na osnovu toga kom podskupu kompleksnih brojeva (alfabetu - konstelaciji) pripadaju elementi sekvence. Tako definišemo:

Binarne sekvence: uzimaju vrednosti is skupa  $\{-1, +1\}$ .

Polifazne sekvence u užem smislu: vrednosti su stepeni nekog korena jedinice  $e^{2\pi ik/M}$  gde su  $k$  i  $M$  prirodni brojevi. Njih ćemo još zvati M-PSK (Phase Shift Keying) sekvence.

Polifazne sekvence u širem smislu: vrednosti su unimodularni kompleksni brojevi oblika  $e^{\varphi i}$  gde je  $\varphi$  realan broj između 0 i  $2\pi$ .

Višenivoske sekvence: vrednosti pripadaju skupu realnih brojeva  $\mathbb{R}$  (u širem smislu) ili skupu celih brojeva  $\mathbb{Z}$  (u užem smislu). Specijalan slučaj ovih sekvenci su ternarne sekvence.

QAM (Quadrature Amplitude Modulation) sekvence. Poznati primeri su 16-QAM i 64-QAM sekvence koje se koriste u sistemima četvrte generacije mobilne telefonije kao što su WiMax i LTE.

### 2.2.1. Predstavljanje sekvenci pomoću Z transformacije

Za konačne sekvence ova definicija se svodi na:

$$X(Z^{-1}) = \sum_{n=0}^{N-1} x(n)Z^{-n} \quad (18)$$

PRIMER: Neka je sekvenca  $x = [1, 0, -1, 0, 0, 1, 0, 0, 0, -1]$ . Njena Z transformacija je:

$$X(Z^{-1}) = 1 - Z^{-2} + Z^{-5} - Z^{-9}$$

Zapažamo da je sekvenca dužine 10 dok je Z transformacija polinom stepena 9 a to je zato što stepeni polinoma počinju od nule. Takođe treba uočiti da je u ovom slučaju Z

transformacija mnogo kompaktnija reprezentacija sekvence pošto se članovi s koeficijentom 0 ne pojavljuju u polinomu.

Tako, na primer, sekvenca  $x = [0, 1, 0]$  je predstavljena sa  $X(Z^{-1}) = Z^{-1}$  koji je polinom prvog stepena, što odgovara sekvenci dužine 2. Naime, ista  $Z$  transformacija se dobija za sekvencu dužine 2:  $x = [0, 1]$ . O ovome treba voditi računa kada se zaključuje o dužini sekvence na osnovu njene  $Z$  transformacije. Dodavanjem nula s desne strane sekvence neće se povećati stepen pridruženog polinoma. Međutim dodavanje nula s leve strane sekvence (na početku) nema isti efekat, što znači da te nule povećavaju stepen polinoma. O ovoj specifičnosti posebno ćemo voditi računa kada budemo razmatrali polinomijalne matrice i njima pridružene sekvence. Tako recimo matrica-vrsta  $[1 + Z^{-2} \quad 1 - Z^{-1}]$  je matrični polinom stepena 2 pošto se može napisati kao  $[1 \quad 1] + [0 \quad -1]Z^{-1} + [1 \quad 0]Z^{-2}$  iako prvi polinom odgovara sekvenci dužine 3 a drugi sekvenci dužine 2.

## 2.2.2. Matrično predstavljanje parova i skupova sekvenci

Kako se komplementarne sekvence najčešće generišu kao parovi ili skupovi, radi kompaktnije notacije mi ćemo parove sekvenci predstavljati kao vektor njihovih  $Z$  transformacija. Tako ćemo par sekvenci  $x_1(n)$  i  $x_2(n)$  predstavljati preko vektor-kolone:

$$\mathbf{x}(Z^{-1}) = \begin{bmatrix} X_1(Z^{-1}) \\ X_2(Z^{-1}) \end{bmatrix} \quad (19)$$

Mi smo ovde izabrali da koristimo vektor-kolonu iako smo takođe mogli koristiti i vektor-vrstu. Glavna prednost ovakvog matričnog predstavljanja leži u sledećoj činjenici. Ukoliko su dva para  $(x_1(n), x_2(n))$  i  $(y_1(n), y_2(n))$  povezana linearnom relacijom (što je čest slučaj u algoritmima za generisanje sekvenci):

$$\begin{aligned} y_1(n) &= a_{11}x_1(n) + a_{12}x_2(n) \\ y_2(n) &= a_{21}x_1(n) + a_{22}x_2(n) \end{aligned} \quad (20)$$

onda takvu relaciju možemo predstaviti u matričnom obliku kao:

$$\mathbf{y}(Z^{-1}) = \mathbf{A} \cdot \mathbf{x}(Z^{-1}) \quad (21)$$

gde je  $\mathbf{A}(Z^{-1}) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

U slučaju skupova sekvenci  $\mathbf{x}(Z^{-1})$  i  $\mathbf{y}(Z^{-1})$  mogu da budu vektori dužine  $M$  a  $\mathbf{A}(Z^{-1})$  je kvadratna matrica veličine  $M \times M$ . Strogo govoreći,  $\mathbf{x}(Z^{-1})$  i  $\mathbf{y}(Z^{-1})$  nisu obični skupovi sekvenci (iako se taj termin uvek koristi kada je reč o komplementarnim sekvencama) nego su uređeni skupovi sekvenci ili nizovi sekvenci (ovaj izraz nećemo koristiti pošto može izazvati konfuziju jer su reči nizovi i sekvence u suštini sinonimi).

Ipak, svakom uređenom skupu možemo pridružiti običan skup, s tim što obrnuto preslikavanje nije jednoznačno. Takođe treba imati u vidu da ni sam izraz skupovi sekvenci nije precizan pošto se neke sekvence mogu ponavljati, pa matematički precizan izraz za takvu strukturu glasi multi-skupovi (Multi-Sets).

### 2.2.3. Autokorelaciona funkcija sekvence

Aperiodična međukorelaciona funkcija  $C_{x,y}(k)$  za dve beskonačne sekvence definiše se kao:

$$C_{x,y}(k) = \sum_{n=-\infty}^{\infty} x^*(n) y(n+k) \quad (22)$$

odnosno za konačne sekvence dužine  $N$  kao:

$$C_{x,y}(k) = \begin{cases} \sum_{n=0}^{N-1-k} x^*(n) y(n+k), & \text{za } -N+1 \leq k \leq 0 \\ \sum_{n=k}^{N-1} x^*(n) y(n+k), & \text{za } 0 \leq k < N-1 \\ 0, & \text{za ostale vrednosti} \end{cases} \quad (23)$$

Autokorelaciona funkcija  $R_x(k)$  definiše se kao međukorelaciona funkcija sekvence sa samom sobom. Dakle:

$$R_x(k) = C_{x,x}(k) \quad (24)$$

$Z$  transformacija autokorelacione funkcije jednaka je:

$$\mathcal{R}_x(Z^{-1}) = \sum_{k=-\infty}^{\infty} R_x(k) Z^{-k} = X^*(Z^{-1}) \cdot X(Z) \quad (25)$$

### 2.2.4. Faktor dobrote

Golej [Golay 77] definisao je faktor dobrote (Merit Factor) sekvence  $x$  kao:

$$F_x = \frac{N^2}{2 \cdot \sum_{k=1}^{N-1} |R_x(k)|^2} \quad (26)$$

Sušтина ove definicije pokazuje da je faktor dobrote mera ravnoće spektra. Za potpuno ravan spektar faktor dobrote bio bi beskonačan. Ekvivalentna definicija u spektralnom domenu prema [Parker 04] glasi:

$$F_x = \frac{N^2}{\int_0^{2\pi} (|X(e^{i\varphi})|^2 - N)^2 dt} \quad (27)$$

gde je  $X(Z^{-1})$  Z transformacija sekvence “ $x$ ”.

Golej postavlja hipotezu da je za bilo koju sekvencu dužu od 13:

$$\limsup_{n \rightarrow \infty} F_x = 12,32$$

pretpostavljajući da se za veliko N lobovi autokorelacione funkcije mogu posmatrati kao nezavisne slučajne varijable.

## 2.2.5. Furijeova transformacija sekvence

Furijeova transformacija (FT) sekvence  $x(n)$  definiše se kao vrednost njene Z transformacije na jediničnom krugu. Drugim rečima, jednaka je njenoj Z transformaciji za  $Z = e^{2\pi if}$ .

$$\mathcal{F}_x(f) = FT\{x(n)\} = X(Z^{-1})|_{Z=e^{2\pi ik/N}} = \sum_{n=0}^{N-1} x(n) e^{2\pi if} \quad (28)$$

Diskretna Furijeova transformacija se definiše kao Furijeova transformacija sekvence u N ekvidistantnih tačaka, znači za  $Z = e^{2\pi ik/N}$ . Dakle:

$$F_x(k) = DFT\{x(n)\} = \sum_{n=0}^{N-1} x(n) e^{2\pi i kn/N} = \mathcal{F}_x(k/N) \quad (29)$$

što znači, jednaka je vrednosti Furijeove transformacije u diskretnim tačkama.

Spektralna gustina snage se definiše kao kvadrat modula Furijeove transformacije:

$$S_x(f) = |\mathcal{F}_x(f)|^2 = |FT\{x(n)\}|^2 \quad (30)$$

Furijeova transformacija autokorelacione funkcije jednaka je Z transformaciji na jediničnom krugu, to jest za  $Z = e^{2\pi if}$ :

$$\begin{aligned} FT\{R_x(k)\} &= \mathcal{R}_x(e^{2\pi if}) = X^*(e^{2\pi if}) \cdot X(e^{2\pi if}) = |X(e^{2\pi if})|^2 \\ &= |FT\{x(k)\}|^2 = |\mathcal{F}_x(f)|^2 = S_x(f) \end{aligned} \quad (31)$$

Dakle, Furijeova transformacija autokorelacione funkcije jednaka je spektralnoj gustini snage.

## 2.3. Komplementarne sekvence

### 2.3.1. Definicija komplementarnih sekvenci

Komplementarni par sekvenci je definisan kao par sekvenci koje imaju osobinu da je zbir njihovih autokorelacionih funkcija delta impuls. Ako par komplementarnih sekvenci obeležimo s  $a(n)$  i  $b(n)$  onda je definicija komplementarnosti:

$$R_a(k) + R_b(k) = C^2 \cdot \delta(k) = (R_a(0) + R_b(0)) \cdot \delta(k) = (E_a + E_b) \cdot \delta(k) \quad (32)$$

Znači da  $C^2 = E_a + E_b = R_a(0) + R_b(0)$  predstavlja zbir energija pojedinačnih sekvenci u paru. U slučaju da obe sekvence imaju istu energiju  $E_a = E_b = E$  (kao što je slučaj s binarnim, polifaznim i standardnim QAM sekvencama) onda dobijamo:  $C^2 = 2E$ . Ponekad je umesto ukupne energije zgodnije koristiti srednju snagu koja je jednaka energiji po simbolu:  $P = E/L$  odnosno  $E = P \cdot L$ , pa dobijamo

$$C^2 = 2 \cdot P \cdot L \quad (33)$$

U Z domenu definicija komplementarnosti glasi:

$$R_a(Z^{-1}) + R_b(Z^{-1}) = A^*(Z) \cdot A(Z^{-1}) + B^*(Z) \cdot B(Z^{-1}) = C^2 = 2 \cdot P \cdot L \quad (34)$$

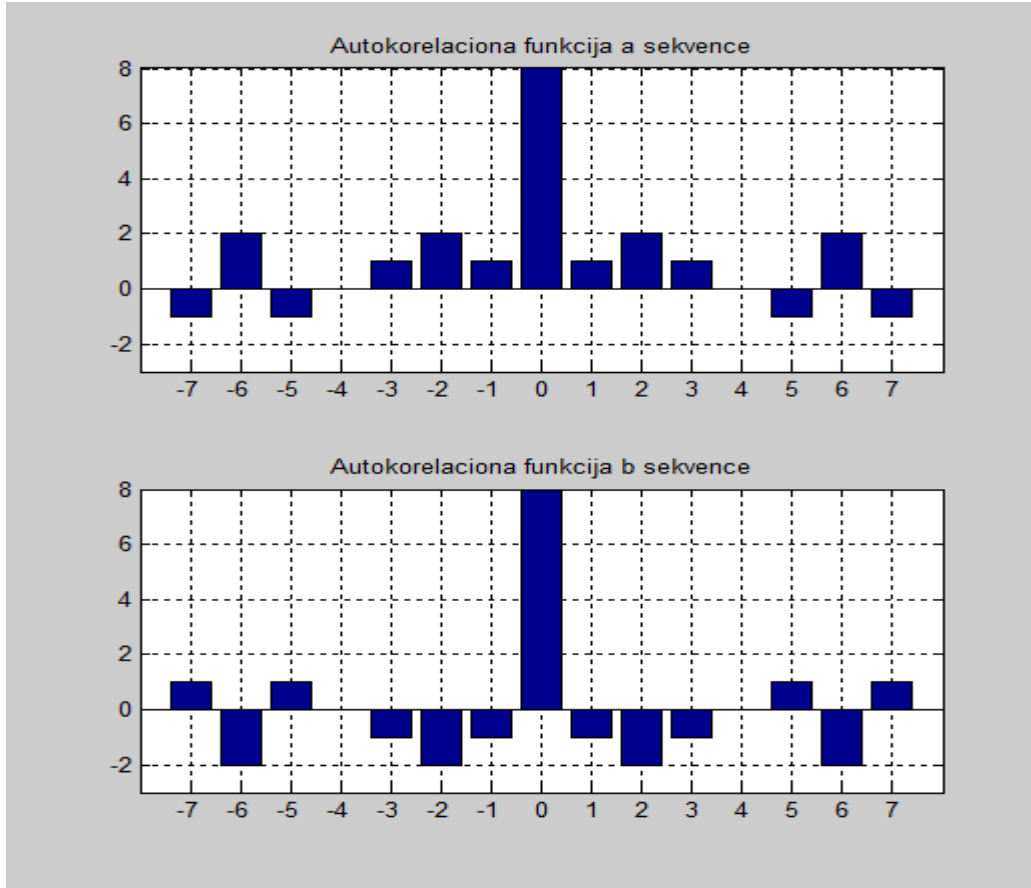
dok u Furijeovom domenu ona glasi:

$$S_a(f) + S_b(f) = 2 \cdot P \cdot L \quad (35)$$

Definicija komplementarnosti (32) može se uopštiti na skupove od M sekvenci  $x_m(n)$  za  $m = 1, \dots, M$  i tada glasi:

$$\sum_{m=0}^{M-1} R_{x_m}(k) = C^2 \cdot \delta(k) \quad (36)$$

Primer autokorelacionih funkcija komplementarnog para sekvenci  $[a, b]$  prikazan je na Sl. 3.



Sl. 3. Autokorelacione funkcije komplementarnog para

### 2.3.2. Uslov komplementarnosti u matričnom obliku

Z transformacija zbira autokorelacionih funkcija komplementarnog skupa može se izraziti kao:

$$\mathbf{x}^H(Z) \mathbf{x}(Z^{-1}) = C^2 = 2E \quad (37)$$

gde je  $(\cdot)^H$  Hermitov operator (konjugacija i transponovanje matrice).

### 2.3.3. Spektralne osobine

Ukoliko u prethodnoj jednačini zamenimo Z sa  $Z = e^{2\pi i f}$  dobijamo uslov:

$$[X_1^*(e^{-2\pi if}), X_2^*(e^{-2\pi if}), \dots, X_N^*(e^{-2\pi if})][X_1(e^{-2\pi if}), X_2(e^{-2\pi if}), \dots, X_N(e^{-2\pi if})]^1 = C^2$$

$$\sum_{k=1}^N |x_k(e^{-2\pi if})|^2 = \sum_{k=1}^N S_{X_k}(f) = C^2 \quad (38)$$

U slučaju para sekvenci  $[a, b]$  ovaj izraz postaje:

$$S_a(f) + S_b(f) = C^2 \quad (39)$$

Kako su spektralne gustine snaga pozitivne funkcije iz uslova  $S_b(f) \geq 0$ , to dobijamo:

$$S_a(f) \leq C^2 \quad (40)$$

Ukoliko obe sekvence imaju istu energiju, što je, recimo, slučaj kod binarnih i polifaznih sekvenci, onda imamo:

$$\overline{S_a(f)} = \overline{S_b(f)} = C^2/2 \quad (41)$$

što najzad daje:

$$S_a(f) \leq 2 \cdot \overline{S_a(f)} \quad (42)$$

Za odnos vršne i srednje snage PAPR (peak to average power ratio) dobijamo:

$$PAPR = \max_f(S_a(f))/\overline{S_a(f)} \leq 2 \quad (43)$$

Naravno, isto važi i za  $b$  sekvencu. Na sličan način za skup od  $N$  sekvenci dobijamo:

$$S_{X_k} \leq C^2 \quad (44)$$

$$\sum_{k=1}^N \overline{S_{X_k}(f)} = N \cdot \overline{S_{X_k}(f)} \cdot C^2 \quad (45)$$

Odakle sledi:

$$\overline{S_{X_k}(f)} = C^2/N \quad (46)$$

pa je PAPR za bilo koju sekvencu iz skupa:

$$PAPR = \max_f(S_{X_k}(f))/\overline{S_{X_k}(f)} \leq N \quad (47)$$

Naravno, ako snage sekvenci nisu međusobno jednake ali su poznate, na sličan način možemo izračunati PAPR za svaku pojedinačnu sekvencu iz skupa.

## 2.4. Paraunitarne matrice

Paraunitarne matrice su uvedene kao generalizacija unitarnih matrica u teoriji filterskih banaka.

### 2.4.1. Definicija

Uvešćemo notaciju za tilda operaciju:

$$\mathbf{P}(\widetilde{Z^{-1}}) = \mathbf{P}^H(Z) = \{\mathbf{P}^*(Z)\}^T \quad (48)$$

gde  $(.)^H = ((.)^T)^*$  označava Hermitovo transponovanje matrica (transponovanje i konjugovanje). Paraunitarne matrice su polinomske matrice po  $Z^{-1}$  veličine  $M \times M$  definisane sledećom relacijom:

$$\mathbf{P}(\widetilde{Z^{-1}}) \cdot \mathbf{P}(Z^{-1}) = \mathbf{I}_M \quad (49)$$

gde je  $\mathbf{I}_M$  jedinična matrica veličine  $M \times M$ .

Paraunitarne matrice možemo posmatrati kao uopštavanje pojma unitarne matrice (koji je definisan za konstantne kompleksne matrice) na matrice koje su funkcija kompleksne promenljive  $Z^{-1}$ . U tom kontekstu može se reći da je paraunitarna svaka matrica koja je funkcija od  $Z^{-1}$  i koja je unitarna za svako  $Z^{-1}$  koje se nalazi na jediničnom krugu.

### 2.4.2. Veza s komplementarnim sekvencama

Takođe se mogu definisati i paraunitarne matrice-kolone  $\mathbf{x}(Z^{-1})$  veličine  $M \times 1$ :

$$\mathbf{x}(\widetilde{Z^{-1}}) \cdot \mathbf{x}(Z^{-1}) = 1 \quad (50)$$

Prethodna jednačina se svodi na uslov:

$$\mathbf{x}^H(Z) \cdot \mathbf{x}(Z^{-1}) = 1 \quad (51)$$

koji je identičan kao uslov komplementarnosti za komplementarne sekvence (37). Takođe se pokazuje da je svaku paraunitarnu matricu-kolonu  $\mathbf{x}(Z^{-1})$  moguće prikazati pomoću kvadratne paraunitarne matrice  $\mathbf{X}(Z^{-1})$  na sledeći način:

$$\mathbf{x}(Z^{-1}) = \mathbf{X}(Z^{-1}) \cdot \mathbf{h} \quad (52)$$

gde je  $\mathbf{h}$  bilo kakva matrica-kolona. Ovda treba napomenuti da se uslov paraunitarnosti kao i uslov unitarnosti mogu formulisati striktno i manje striktno. U striktnoj definiciji s desne strane definišuće jednačine biće jedinična matrica dok će u manje striktnoj definiciji ta jedinična matrica biti pomnožena realnom pozitivnom konstantom. Mi ćemo uglavnom koristiti manje striktnu definiciju.

Ova analogija uslova paraunitarnosti matrica-kolona i uslova komplementarnosti osnova je za primenu bogate teorije paraunitarnih matrica, nastale u oblasti filterskih banaka [Vaidyanathan 93], na teoriju komplementarnih sekvenci.

Osobine paraunitarnih matrica

Primena tilda operacije na paraunitarnu matricu daje paraunitarnu matricu.

Transponovanje paraunitarne matrice daje paraunitarnu matricu.

Konjugovanje paraunitarne matrice daje paraunitarnu matricu.

Opšti oblik paraunitarne matrice stepena  $N$  i veličine  $2 \times 2$  jeste:

$$\mathbf{P}(Z^{-1}) = \begin{bmatrix} C(Z^{-1}) & S(Z^{-1}) \\ -S^{*R}(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} = \begin{bmatrix} C(Z^{-1}) & S(Z^{-1}) \\ -Z^{-N}S^*(Z) & Z^{-N}C^*(Z) \end{bmatrix} \quad (53)$$

gde  $(\cdot)^R$  označava revertovanje polinoma.

On se može pisati i u transponovanom obliku:

$$\mathbf{P}'(Z^{-1}) = \begin{bmatrix} C(Z^{-1}) & -S^{*R}(Z^{-1}) \\ S(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} = \begin{bmatrix} C(Z^{-1}) & -Z^{-N}S^*(Z) \\ S(Z^{-1}) & Z^{-N}C^*(Z) \end{bmatrix} \quad (54)$$

Invertovana paraunitarna matrica je:

$$\mathbf{P}^{-1}(Z^{-1}) = \tilde{\mathbf{P}}(Z^{-1}) = \begin{bmatrix} C^*(Z) & -Z^N S(Z^{-1}) \\ S^*(Z) & Z^N C(Z^{-1}) \end{bmatrix} \quad (55)$$

i ona je nekauzalna matrica. Od nje se može dobiti kauzalna matrica kada se pomnoži s kašnjenjem  $Z^{-N}$ :

$$Z^{-N} \cdot \mathbf{P}^{-1}(Z^{-1}) = \begin{bmatrix} C^*(Z)Z^{-N} & -S(Z^{-1}) \\ S^*(Z)Z^{-N} & C(Z^{-1}) \end{bmatrix} = \begin{bmatrix} C^{*R}(Z^{-1}) & -S(Z^{-1}) \\ S^{*R}(Z^{-1}) & C(Z^{-1}) \end{bmatrix} \quad (56)$$

Tu matricu ćemo zvati kauzalna inverzna matrica matrice  $\mathbf{P}$ . Proizvod paraunitarne matrice i njene kauzalno-inverzne matrice je jedinična matrica pomerena u vremenu (zakašnjena):

$$\begin{aligned} \begin{bmatrix} C(Z^{-1}) & S(Z^{-1}) \\ -S^{*R}(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} \begin{bmatrix} C^{*R}(Z^{-1}) & -S(Z^{-1}) \\ S^{*R}(Z^{-1}) & C(Z^{-1}) \end{bmatrix} &= \begin{bmatrix} Z^{-N} & 0 \\ 0 & Z^{-N} \end{bmatrix} == \\ &= Z^{-N} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = Z^{-N} \cdot \mathbf{I}_2. \end{aligned} \quad (57)$$

Proizvod dve paraunitarne matrice je paraunitarna matrica:

$$\begin{aligned} \mathbf{P}_1(Z^{-1}) \cdot \mathbf{P}_1(Z^{-1}) &= \begin{bmatrix} C_1 & S_1 \\ -S_1^{*R} & C_1^{*R} \end{bmatrix} \cdot \begin{bmatrix} C_2 & S_2 \\ -S_2^{*R} & C_2^{*R} \end{bmatrix} = \\ &= \begin{bmatrix} C_1 C_2 - S_1 S_2^{*R} & C_1 S_2 + S_1 C_2^{*R} \\ -S_1^{*R} C_2 - C_1^{*R} S_2^{*R} & C_1^{*R} C_2^{*R} - S_1^{*R} S_2 \end{bmatrix} = \begin{bmatrix} (C_1 C_2 - S_1 S_2^{*R}) & (C_1 S_2 + S_1 C_2^{*R}) \\ -(C_1 S_2 + S_1 C_2^{*R})^{*R} & (C_1 C_2 - S_1 S_2^{*R})^{*R} \end{bmatrix} \end{aligned} \quad (58)$$

Stepen paraunitarne matrice se definiše kao stepen polinoma koji se dobija kada se izračuna determinanta paraunitarne matrice. Naravno, važi osobina da je stepen proizvoda dve paraunitarne matrice jednak zbiru stepeni pojedinačnih matrica u proizvodu.

Paraunitarne matrice mogu da se interpretiraju kao banke filtera s N ulaza i N izlaza. Množenje matrica odgovara kaskadi filtera. Znači, paraunitarna matrica veličine  $2 \times 2$  odgovara dvoulazno dvoizlaznom filteru.

Množenje paraunitarne matrice s desne strane sa  $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$  (ili sa  $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ ) odgovara korišćenju samo gornjeg (ili donjeg) izlaza filtera tako da dobijamo dvoulazno jednoizlazni filter.

Množenje paraunitarne matrice s leve strane sa  $[1 \ 1]$  odgovara dovođenju istog signala na oba ulaza filtera tako da dobijamo jednoulazni dvoizlazni filter. Sličan efekat se dobija množenjem s leve strane sa  $[1 \ 0]$  ili  $[0 \ 1]$ .

## 3. Osobine binarnih komplementarnih sekvenci

Pod standardnim binarnim komplementarnim (Golejevim) sekvencama podrazumevaćemo binarne sekvence dužine  $2^N$  čiju je konstrukciju dao Golej u svom radu [Golay 61]. Interesantno je da se u vrlo malo radova obrađuju autokorelacione osobine ovih sekvenci kao individualnih sekvenci. U literaturi su ove sekvence mahom analizirane kao parovi, tako da su veoma retko proučavane kao pojedinačne sekvence. Iako su binarne Golejeve sekvence samo veoma specijalan slučaj šire familije komplementarnih sekvenci, čak ni one nisu detaljno proučene a kamoli cela familija. Utoliko pre nedostaje literatura o osobinama polifaznih sekvenci, skupova komplementarnih sekvenci i naravno QAM komplementarnih sekvenci. Osobine nestandardnih sekvenci, kernela i sekvenci dobijenih njihovom kombinacijom potpuno su neistražene. Zato ćemo se mi ovde pozabaviti samo osobinama binarnih sekvenci, s nadom da će neko uskoro proučiti i ostale familije. Rezultati koje ćemo prikazati uglavnom potiču iz [Budišin 92] uz manje dopune.

### 3.1. Dužina sekvenci

Dužina standardnih Golejevih sekvenci je  $2^N$  dok je dužina PN sekvenci manja za jedan i jednaka je  $2^N - 1$ . Zbog prirode broja koji određuje njihovu dužinu, Golejeve sekvence su pogodnije za implementaciju digitalnih elektronskih sklopova. U radarskim i komunikacionim sistemima je uobičajeno da se blokovi definišu kao umnošci nekog osnovnog takta s brojem koji je stepen dvojke. Tako se obično pojednostavljuje

implementacija osnovnih algoritama za obradu signala. Očigledan primer je FFT (Fast Fourier Transform) blok koji je prirodno definisan za takve dužine. Tako se, na primer, za rešavanje PAPR problema u OFDM sistemima sekvenca dovodi na FFT-IFFT blok pa su Golejeve sekvence u toj primeni mnogo pogodnije od drugih sekvenci. Čak i ostale standardne komplementarne sekvence u višim konstelacijama (M-PSK 16-QAM, 64-QAM) imaju dužinu  $2^N$ .

### 3.2. Broj različitih sekvenci zadate dužine

Broj binarnih Golejevih sekvenci izražava se veoma jednostavnom formulom:  $N! 2^N / 2$ . Faktor  $N!$  jednak je broju permutacija koje se koriste pri generisanju dok faktor  $2^N$  potiče od broja Volšovih funkcija.

Tab. 4. Broj Golejevih sekvenci i PN sekvenci za različite dužine

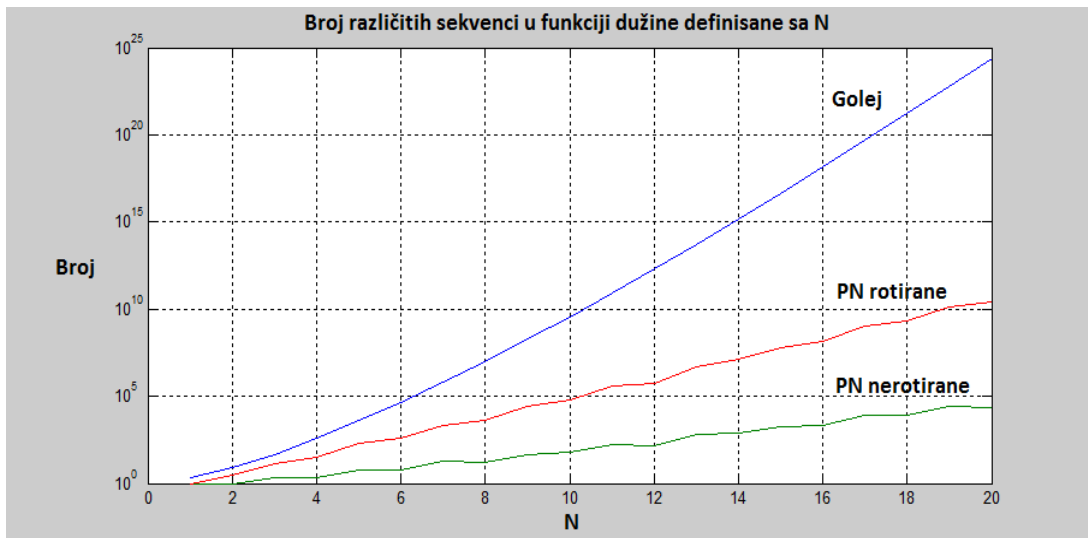
N	Dužina Golej	Dužina PN	Broj Golejevih sekvenci	Broj PN sekvenci	Broj rotiranih PN sekvenci
2	4	3	8	1	3
3	8	7	48	2	14
4	16	15	384	2	30
5	32	31	3.840	6	186
6	64	63	46.080	6	378
7	128	127	645.120	18	2.286
8	256	255	10.321.920	16	4.080
9	512	511	185.794.560	48	24.528
10	1.024	1.023	3.715.891.200	60	61,380
11	2.048	2.047	81.749.606.400	176	360.272
12	4.096	4.095	1.961.990.553.600	144	589.680
13	8.192	8.191	51.011.754.393.600	630	5.160.330
14	16.384	16.383	1.428.329.123.020.800	756	12.385.548
15	32.768	32.767	42.849.873.690.624.000	1.800	58.980.600

S druge strane, broj različitih PN sekvenci zavisi od broja generišućih polinoma u konačnom polju Galoa. Za određivanje tih polinoma neophodno je veoma sofisticirano poznavanje polja Galoa. Broj različitih PN sekvenci, ne računajući ciklične rotacije, jednak je  $\varphi(2^N - 1)/N$ ;  $\varphi(\cdot)$  se naziva Ojlerova totient funkcija i definisana je kao broj

prirodnih brojeva manjih od  $N$  i uzajamno prostih s  $N$ . Ne postoji analitički izraz kojim se ova funkcija može predstaviti kao što, recimo, ne postoji analitički izraz za  $N$ -ti prost broj. Ako bi se u obzir uzele i ciklično rotirane PN sekvence, ukupan broj bi iznosio:

$$\varphi(2^N - 1) \cdot (2^N - 1)/N$$

Iz podataka u Tab. 4 uočavamo da je broj Golejevih sekvenci veći od broja PN sekvenci za svaku dužinu  $i$  i to čak i kada se računaju sve ciklično pomerene PN sekvence (što je za mnoge primene neprihvatljivo). Za dugačke sekvence, na primer za dužinu 1023/1024, komplementarnih sekvenci ima drastično više nego PN sekvenci. Generalni trendovi rasta broja sekvenci prikazani su na Sl. 4.



Sl. 4. Broj različitih sekvenci u funkciji dužine sekvenci

### 3.3. Autokorelacione osobine

Mehanizam koji garantuje ograničene bočne lobove i kod Golejevih sekvenci i kod PN sekvenci sličan je. Prvo treba napomenuti da su Golejeve sekvence definisane kao aperiodične sekvence pošto je uslov komplementarnosti formulisan pomoću aperiodičnih autokorelacionih funkcija. S druge strane, PN sekvence su definisane kao periodične sekvence i jedna od najznačajnijih osobina im je da njihova periodična autokorelaciona

funkcija ima lobove jednake -1. Manje je poznato da se ova osobina može formulisati preko aperiodične autokorelacione funkcije kao:

$$R_{PN}(k) + R_{PN}(L - k) = -1 \quad (59)$$

Kada ovaj izraz uporedimo sa uslovom komplementarnosti za Golejeve sekvence vidimo analogiju:

$$R_a(k) + R_b(k) = 0 \quad (60)$$

Treba uočiti ovo: kada  $N$  raste odnos bočnog loba (koji je -1) i glavnog loba (koji ima vrednost  $2^N - 1$ ) teži nuli i to veoma brzo. Zato gornju jednačinu možemo pisati:

$$R_{PN}(k) + R_{PN}(L - k) \sim 0 \quad (61)$$

Ovaj uslov možemo zvati uslov komplementarnosti PN sekvenci.

Na prvi pogled nije jasno kako uslov komplementarnosti autokorelacione funkcije garantuje male bočne lobove. To ćemo objasniti na slučaju komplementarnih sekvenci. Podsetimo se da je Furijeova transformacija autokorelacione funkcije jednaka spektralnoj gustini snage. Takođe se podsetimo i toga da spektar snage ne može biti veći od dvostruke vrednosti srednje snage. Pošto je Furijeova transformacija linearna funkcija, možemo autokorelacionu funkciju posmatrati kao zbir centralnog loba koji ima oblik delta impulsa i bočnih lobova čiji je oblik nepoznat. U spektralnom domenu delta impuls koji predstavlja glavni lob preslikava se u konstantnu - DC (direct current) komponentu spektra a to je srednja vrednost spektra i označićemo je sa  $E$ . Bočni lobovi se preslikavaju u varijabilni deo spektra koji se dodaje na  $E$ . Međutim, ta varijabilna komponenta je ograničena na opseg vrednosti od  $-E$  do  $+E$ , zato što je spektar uvek pozitivan a maksimalna vrednost ne može da pređe  $2E$ . Kada bi varijabilna komponenta imala samo vrednosti  $\pm E$  bez međuvrednosti, njena snaga bi bila  $E^2$ . DC komponenta koja ima konstantnu vrednost  $E$  takođe ima snagu  $E^2$ . Znači, možemo zaključiti da ukupna snaga varijabilnog dela spektra, koji potiče od bočnih lobova, ne može biti veća od snage DC komponente u spektru. Kako je spektar kontinualna funkcija, sigurno je nemoguće da će varijabilna komponenta imati skokovite promene od  $-E$  do  $+E$  i obrnuto. Pre se može očekivati da će te promene ličiti na sinusoidalnu funkciju. Ako bismo koristili model sinusoide koja ima amplitudu  $E$ , onda bi njena srednja snaga bila  $E^2/2$ . Sledi da bi snaga varijabilnog dela spektra bila dvaput manja od snage DC komponente spektra.

Po Parsevalovoj teoremi, snaga bočnih lobova autokorelacione funkcije ne može biti veća od snage glavnog loba (model kada varijabilni deo spektra uzima vrednosti  $\pm E$ ) a verovatno je bolja aproksimacija da je jednaka polovini snage glavnog loba (sinusoidalni model). Pošto je amplituda glavnog loba  $2^N$  onda je njegova snaga  $4^N$ . Snaga bočnih lobova je po drugom modelu  $4^N/2$ . Nas zanima srednja snaga bočnih lobova koju dobijamo kada ukupnu snagu podelimo s brojem bočnih lobova pa dobijamo:  $(4^N/2)/(2 \cdot 2^N) = 2^N/4$ . Iz ove vrednosti možemo izračunati srednju amplitudu bočnih lobova i ona iznosi:  $\sqrt{2^N/4} = 2^{N/2}/2 = \sqrt{L}/2$  gde je  $L$  dužina sekvence.

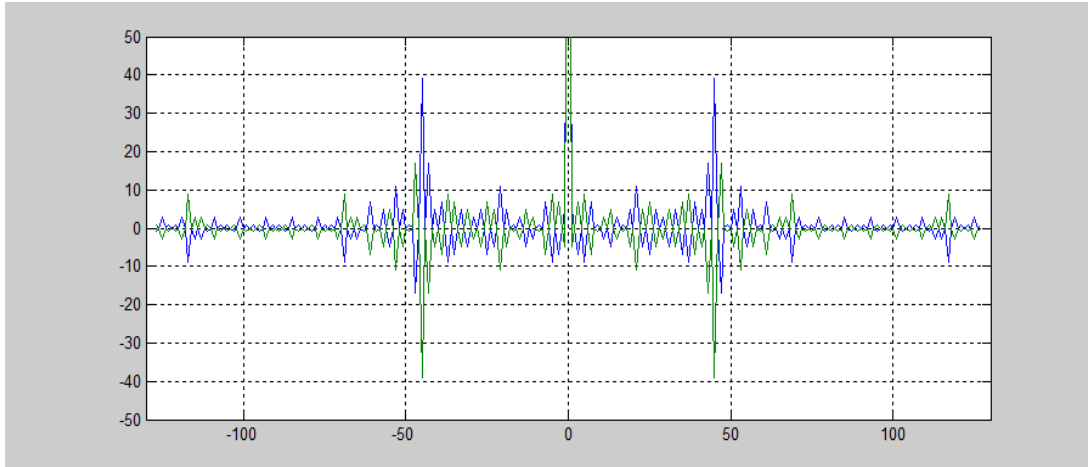
Međutim, za sekvence je često važan podatak kolika je vršna vrednost bočnih lobova. Kako bočni lobovi sigurno nisu međusobno jednaki, moramo zaključiti da će oni pouzdano biti znatno veći od njihove srednje vrednosti. Ali može se očekivati kako će biti sačuvan opšti trend da veličina bočnih lobova raste s kvadratnim korenom dok glavni lob raste linearno s dužinom sekvenci. Poređenje srednje kvadratne vrednosti lobova i vršne vrednosti lobova prikazano je u Tab. 5.

Tab. 5. Maksimalni autokorelacioni pikovi i srednja kvadratna vrednost (RMS) lobova za najbolje i najgore primerke Golejevih i PN sekvenci

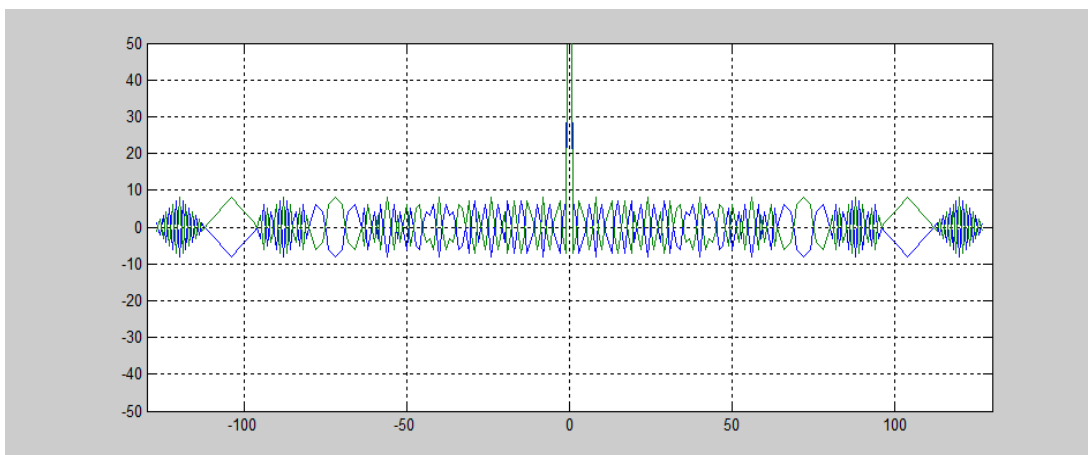
N	Dužina		Autokorelacioni pikovi				RMS vrednost bočnih lobova			
	Golej	PN	Min. Golej	Min. PN	Maks. Golej	Maks. PN	Min. Golej	Min. PN	Maks. Golej	Maks. PN
2	4	3	1	1	1	2	0,82	0,70	0,82	1,58
3	8	7	2	1	3	3	1,31	0,70	1,31	1,78
4	16	15	3	3	5	5	1,26	1,39	1,93	2,25
5	32	31	4	4	11	7	1,90	1,74	2,78	2,92
6	64	63	6	6	21	11	2,57	2,01	3,87	3,94
7	128	127	8	8	39	16	3,82	3,90	5,26	5,39
8	256	255	12	13	<b>73</b>	22	5,35	5,91	7,53	7,19

Iz navedenog izvodimo sledeće zaključke:

- Kada poredimo najbolje sekvence u pogledu najvećeg pika, obe familije su jednake sem za dužine 8/7 gde su bolje PN sekvence i dužine 256/255 gde su bolje Golejeve sekvence.
- Kada poredimo najgore sekvence u pogledu najvećeg pika, PN sekvence imaju ubedljivo bolje rezultate. Recimo, za dužinu 256/255 najgora Golejeva sekvenca ima lob (veličine **73**) koji je 28,5% od glavnog loba dok je to kod PN sekvence (22) 8,6%. Međutim, ovaj podatak treba posmatrati u svetlu činjenice da Golejevih sekvenci imamo drastično više tako da je moguće ove loše sekvence izbaciti i dalje dobiti veliki skup Golejevih sekvenci sa niskim lobovima. Sa druge strane ova činjenica može da objasni zašto Golejeve sekvence nisu postigle popularnije (što je sasvim neopravdano) – zato što su prve analize bile površne, naime, analiziran je samo mali podskup svih Golejevih sekvenci, i pokazale su da Golejeve sekvence imaju velike lobove.
- Kada poredimo RMS (Root mean square) vrednosti lobova vidimo da nijedna familija nije značajno bolja. Najveće razlike su u okviru 25%. Još je interesantno uočiti da su najbolje i najgore Golejeve sekvence u pogledu RMS vrednosti uglavnom u odnosu  $\sqrt{2}$ : 2.



Sl. 5. Autokorelaciona funkcija komplementarnog para dužine 128 s velikim autokorelacionim pikom koji iznosi 39 (amplituda glavnog loba se ne vidi na slici a iznosi 128)



Sl. 6. Autokorelaciona funkcija komplementarnog para dužine 128 s malim autokorelacionim pikom koji iznosi 8 (amplituda glavnog loba se ne vidi na slici a iznosi 128)

### 3.4. Faktor dobrote

Golej [Golay 77] je definisao faktor dobrote (Merit Factor) kao:

$$F_a = \frac{N^2}{2 \cdot \sum_{k=1}^{N-1} |R_a(k)|^2} \quad (62)$$

Sušтина ove definicije pokazuje kako je faktor dobrote mera ravnoće spektra. Za potpuno ravan spektar, faktor dobrote bio bi beskonačan. Ekvivalentna definicija u spektralnom domenu prema [Parker 04] glasi:

$$F_a = \frac{N^2}{\int_0^{2\pi} (|A(e^{i\varphi})|^2 - N)^2 dt} \quad (63)$$

gde je  $A(Z^{-1})$  Z transformacija od "a".

Najveći faktor dobrote ima Barkerova sekvenca dužine 13 i on iznosi 14,08. Sledeća sekvenca je Barkerova sekvenca dužine 11 s faktorom dobrote 12,1. Za sekvence do dužine 117 najveći poznat faktor dobrote je 9.56 (pronađen sistematskim pretraživanjem).

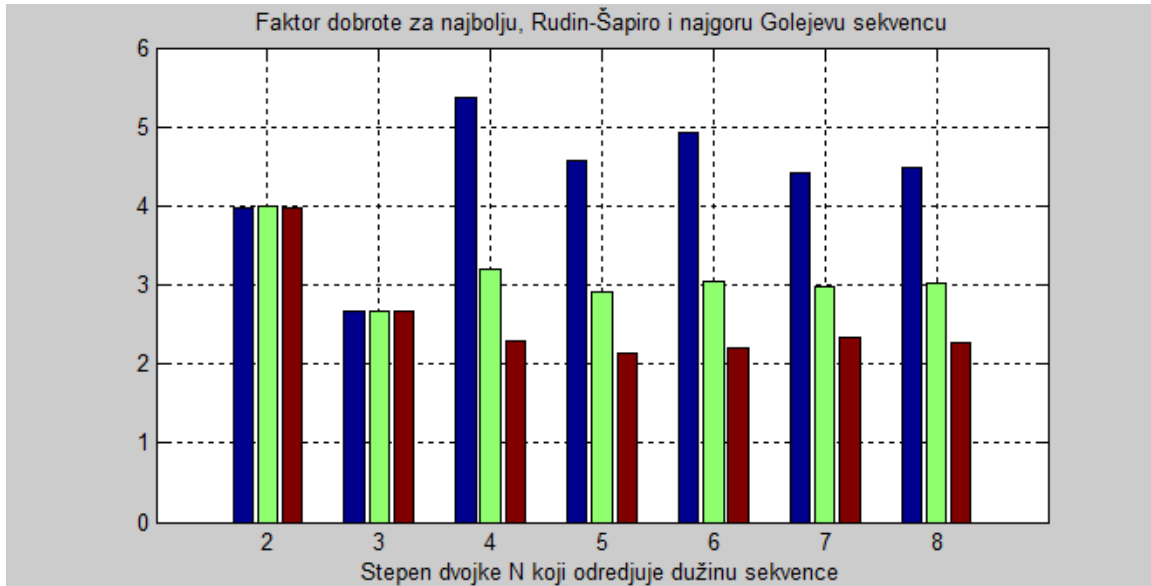
Familija sekvenci koja postoji za proizvoljno velike dužine s velikim faktorom dobrote jesu rotirane Ležandrove sekvence i njihov asimptotski faktor dobrote je 6, a on se postiže kada se sekvenca rotira za četvrtinu svoje dužine.

Sledeća beskonačna familija sa asimptotski dobrim merit faktorom koji je jednak 3 jesu Golejeve sekvence. Naime, za Rudi-Šapiroovu konstrukciju koja odgovara Golejevima sekvencama generisanim pomoću jedinične permutacije, postoji analitički izraz za merit faktor i on za sekvence dužine  $2^N$  iznosi:

$$F_a = \frac{3}{1 - (-0,5)^N} \quad (64)$$

Merit factor za Golejeve sekvence je moguće izračunati kada znamo srednju kvadratnu vrednost lobova koja je data u Tab. 5. Na osnovu tih vrednosti određen je factor dobrote prikazan na

Sl. 7. Može se postaviti hipoteza da najbolji factor dobrote teži ka vrednosti  $3\sqrt{2}$  a najgori ka  $3\sqrt{2}/2$ .



Sl. 7. Faktor dobrote za Golejeve sekvence dužine 4 do 256 određen numerički

Bilo bi interesantno da se ova hipoteza teorijski dokaže pošto bi tada Golejeve sekvence bile drugoplasirana beskonačna familija sekvenci sa velikim asimptotskim faktorom dobrote odmah posle rotiranih Ležandrovih sekvenci. Rotirane Ležandrove sekvence imaju factor dobrote 6 dok bi za Golejeve on bio 4,24 što je bolje od, do sada, poznatog rezultata za Rudin-Šapiro konstrukciju Golejevih sekvenci za koju on iznosi 3.

Kako PN sekvence imaju slične srednje kvadratne vrednosti bočnih lobova zaključujemo da će imati i slične vrednosti za factor dobrote.

### 3.5. Spektralne osobine

Ranije smo videli da je vršni faktor spektra komplementarnih sekvenci ograničen sa 2. Tu maksimalnu vrednost dostiže većina sekvenci, ako ne egzaktno, onda joj se veoma približava. Kod većine sekvenci to odstupanje nije veće od 0,1%. Zbog toga nema svrhe pretraživati komplementarne sekvence da bi se našle one bolje u pogledu vršne vrednosti spektra.

U prethodnom poglavlju pokazali smo da postoji veza između srednje kvadratne vrednosti promenljivog dela spektra i srednje kvadratne vrednosti bočnih lobova.

Pokazali smo i to da srednja kvadratna vrednost promenljivog dela spektra ne može biti veća od kvadrata DC komponente. Procenili smo da bi ona mogla biti jednaka polovini te vrednosti.

Periodična autokorelaciona funkcija PN sekvenci je dvonivoska pa je i DFT dvonivoski. To bi značilo da je spektar ravan, izuzev nulte komponente koja je značajno manja. Međutim, zna se da DFT, po definiciji, računa spektar periodičnog signala. Kako se u praksi PN sekvence uvek koriste kao aperiodične, valja izračunati aperiodični spektar. To se može uraditi na dva načina:

Dodaje se veći broj nula (mnogo više od dužine sekvence) i računa se DFT.

Računa se Furijeova transformacija kao kontinualna funkcija od ugaone frekvencije  $\omega$ .

Tako izračunat spektar aperiodične PN sekvence ne pokazuje samo to da spektar nije konstantan već i to da vršna vrednost često premašuje dvaput srednju vrednost i to često za značajan faktor. U Tab. 6. prikazan je vršni faktor PAPR za najbolje i najlošije PN sekvence do dužine 1023. Kako su sekvence analizirane kao aperiodične, generisane su sekvence koje odgovaraju svim primitivnim polinomima kao i svi ciklični pomaci sekvenci.

Tab. 6. PAPR za PN sekvence u zavisnosti od dužine

N	Dužina sekvence	PAPR najbolje sekvence	PAPR najgore sekvence
2	3	1,67	3,00
3	7	1,38	3,57
4	15	2,03	3,48
5	31	1,96	5,45
6	63	2,14	4,83
7	127	2,42	5,12
8	255	2,80	5,96
9	511	2,94	6,56
10	1023	3,09	6,42

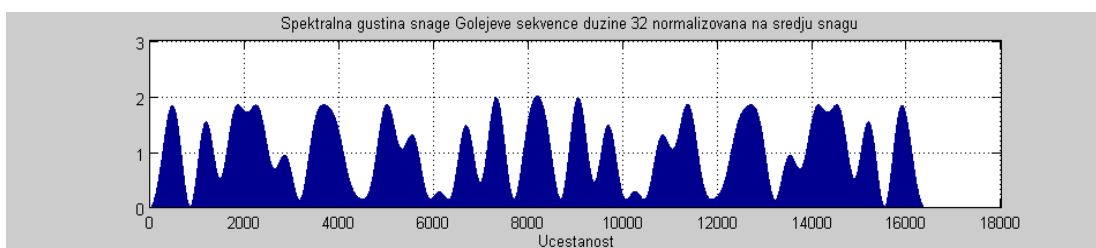
Zapažamo da za dužine veće od 31 ne postoje PN sekvence čiji je PAPR manji od 2 i da za dužinu 511 PAPR za neke sekvence dostiže čak vrednost 6.56. Na Sl. 8, Sl. 9 i Sl. 10 prikazani su spektri Golejeve sekvence dužine 32:

[1,-1,-1,-1,-1,1,-1,-1,-1,1,1,1,-1,1,-1,-1,-1,1,1,1,-1,1,1,-1,1,1,-1,1,-1,-1]

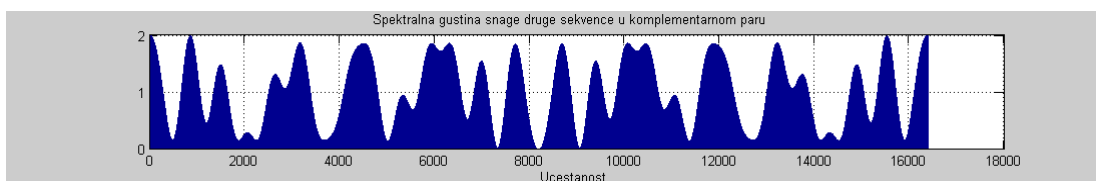
i PN sekvence dužine 31:

[1,-1,-1,-1,1,-1,1,1,1,1,-1,1,1,-1,-1,1,1,1,-1,-1,-1,1,1,-1,1,-1,1,-1,-1].

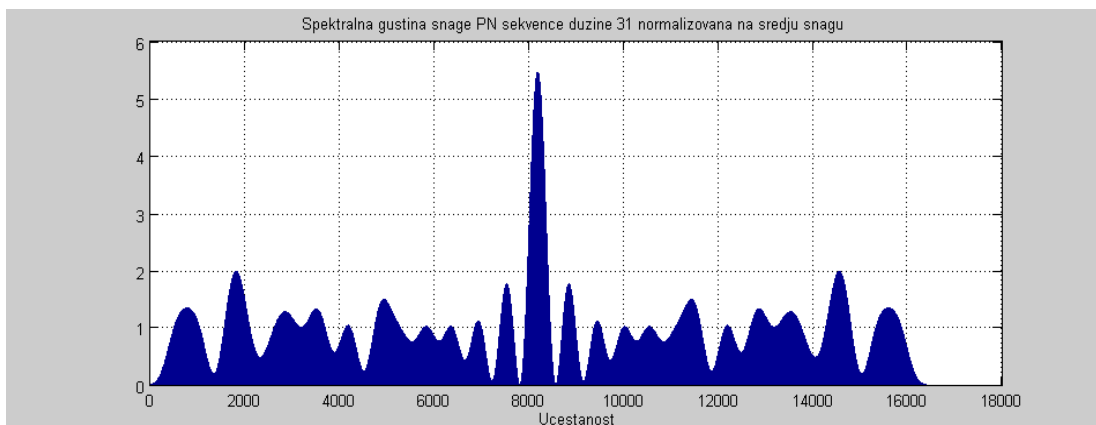
Sl. 11 i Sl. 12 prikazuju spektre sekvenci dužine 512, odnosno 511.



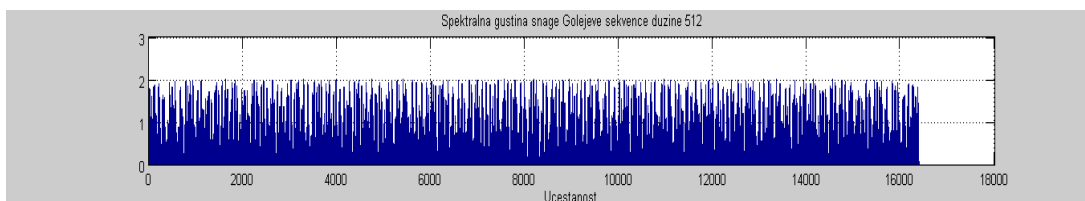
Sl. 8. Spektar prve sekvence iz komplementarnog para



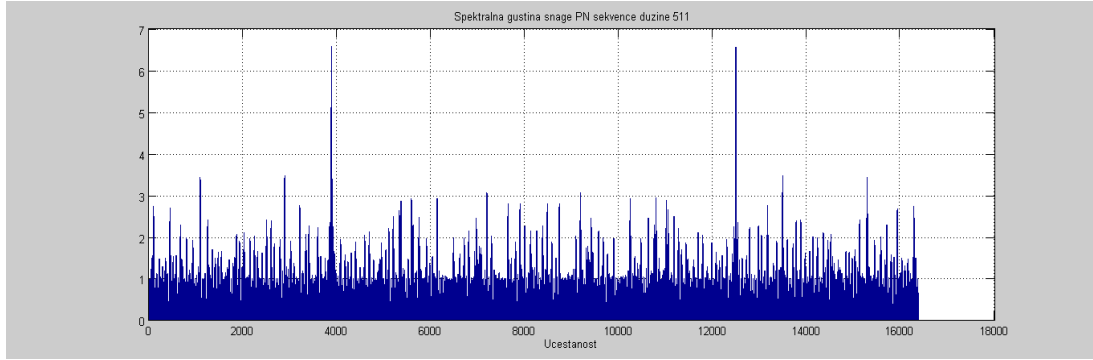
Sl. 9. Spektar druge sekvence iz komplementarnog para



Sl. 10. Spektar PN sekvence



Sl. 11. Spektar Golejeve sekvence dužine 512



Sl. 12. Spektar PN sekvence dužine 511

### 3.6. Hamingova rastojanja

U radu [Davis 99] pokazano je da je za Golejeve binarne sekvence minimalno Hamingovo rastojanje definisano izrazom  $D_{\text{Ham}} > 2^n/4$ .

Naime, sekvence generisane jednom permutacijom razlikuju se samo po Volšovoj funkciji koja množi jednu osnovnu sekvencu. Tada su međusobna rastojanja jednaka  $D_{\text{Ham}} = 2^n/2$ , odnosno međukorelacija je nula. Između sekvenci generisanih različitim permutacijama (što odgovara različitim kosetima Rid-Milerovih kodova) važi  $D_{\text{Ham}} > 2^n/4$ . Prevedeno na međukorelaciju to se svodi na  $C = 2^n/2$ . Kako je autokorelacioni pik  $2^n$  to znači da je relativna međukorelacija  $C_R < 50\%$ .

### 3.7. Linearna složenost

Linearna složenost sekvenci je naročito značajna za kriptografiju. Ona se definiše kao dužina najkraćeg pomeračkog registra s linearnim povratnim spregama koji može da generiše datu sekvencu. U radu [Karkkainen 1994] analizirana je linearna složenost Golejevih sekvenci. Korišćene su sekvence generisane polazeći od kernela dužine 2, 10 i 26. Autor je koristio Berlekamp-Masijev algoritam i pokazao da je linearna složenost Golejevih sekvenci između 0,75 i 0,98 puta dužina sekvenci. To je veoma povoljan

rezultat budući da je složenost PN sekvenci logaritam za osnovu dva od dužine sekvence a to je znatno manje od dužine sekvence i brzo opada sa povećanjem dužine.

S druge strane, u radu [Parker 00] postavljena je hipoteza da Golejeve sekvence imaju optimalan Hadamardov i Nega-Hadamardov vršni faktor. Takođe je konstatovano da Golejeve sekvence pripadaju familiji Bent i familiji Nega-Bent za dužine  $2^N$  gde je  $N \neq 2 \pmod{3}$ . Bent sekvence su veoma značajne u kriptografiji pošto su najudaljenije od sekvenci generisanih linearnim generatorom.

### 3.8. Generatori sekvenci

Bilo koji element bilo koje Golejeve sekvence može se lako izračunati softverski ili generisati hardverski. Da bi se generisala PN sekvenca, prvo treba odrediti generišući polinom kao primitivni polinom u polju Galoa a za to valja imati znanja iz apstraktne algebre; taj zadatak ne može se lako softverski realizovati a posebno je nepraktično realizovati ga hardverski.

Golejeve sekvence mogu da se generišu nerekurzivnim algoritmom ali i rekurzivnim. Ipak, nerekurzivni algoritam se mnogo jednostavnije implementira u slučaju binarnih sekvenci, pošto su neophodni samo brojači i logička kola.

### 3.9. Korelatori sekvenci

Algoritam za brzu Golejevu korelaciju objavljen je prvi put u [Budišin 91]. Autor se u radu prvenstveno bavi primenom u kompresiji radarskih impulsa, pa rad nije bio zapažen. Međutim, u radu [Popović 99] predložena je primena brzog korelatora u mobilnoj telefoniji i to je privuklo pažnju telekomunikacione zajednice. Od tada je objavljeno mnogo radova u kojima se detaljnije razmatra implementacija brzog korelatora i na komplementarne parove i na komplementarne skupove od više od dve sekvence ali i na sekvence izvedene iz komplementarnih sekvenci; uzmimo za primer [Pérez 10].

Osnovna karakteristika efikasnog korelatora jeste to da se on, za binarne sekvence dužine  $2^N$ , sastoji od  $N$  kaskadnih blokova koji sadrže samo liniju za kašnjenje i jedan sabirač i jedan oduzimač. Svaki blok kompleksnih (polifaznih) komplementarnih sekvenci sadrži i jedan kompleksni množač (njega nema u slučaju da se sekvence binarne). Još je važno imati u vidu da efikasni korelator istovremeno koreliše ulazni signal s obe komplementarne sekvence koje čine komplementarni par što predstavlja dodatnu uštedu u hardveru ako su obe korelacije potrebne.

S druge strane, moguće je realizovati i efikasni korelator za PN sekvence [Budišin 89]. Taj korelator se svodi na blok za permutovanje ulaznih simbola, blok za brzu Volšovu transformaciju (FWT – Fast Walsh Transform) i blok za permutovanje izlaznih simbola. Sam FWT blok ima strukturu sličnu FFT algoritmu s tim što su svi koeficijenti samo  $\pm 1$ . Ipak, sam FFT/FWT algoritam nije jednostavan i postoji mnogo njegovih podvarijanti: Radix-2, Radix-4, in place, decimation in time, decimation in frequency i sl.

## 4. Poznati algoritmi

Poznati algoritmi za generisanje sekvenci dužine  $2^N$  dele se na rekurzivne i nerekurzivne algoritme (direktne metode). Osnovni nerekurzivni algoritam dao je Golej [Golay 61] i do sada nisu poznate binarne sekvence dužine  $2^N$  koje se ne mogu generisati tim algoritmom.

Golej je u istom radu dao i nekoliko rekurzivnih algoritama, ali nije analizirao odnos rekurzivnih i nerekurzivnih algoritama. Prva kompletno rekurzivna konstrukcija binarnih komplementarnih sekvenci je data u [Budišin 90A]. Međutim, u tom radu nisu generisane samo binarne sekvence nego i polifazne tako da je tu prvi put rekurzivnim algoritmom generisana šira klasa sekvenci nego tada poznatim nerekurzivnim algoritmom.

Nešto kasnije, u [Davis 99] navedena je direktna metoda za generisanje polifaznih sekvenci i ona postaje opšte prihvaćena; sekvence generisane tom metodom navode se kao GDJ (Golay-Davis-Jedwab) sekvence. Ta nerekurzivna metoda je postala toliko značajna zato što su autori pokazali ekvivalentnost GDJ sekvenci i Rid-Milerovih kodova. Ali ona generiše samo sekvence s konačnim alfabetom čiji su elementi stepena primitivnog korena jedinice dok je rekurzivna metoda iz [Budišin 90A] opštija i generiše pored sekvenci s konačnim alfabetom i sekvence s beskonačnim alfabetom.

Ubrzo posle rada [Budišin 90A] pojavljuje se i rad sa sličnim algoritmom [Budišin 90B] s tim što sekvence nisu ograničene da po modulu budu jednake jedinici nego u opštem slučaju mogu biti višenivoske.

Dalji radovi o QAM komplementarnim sekvencama isključivo su se zasnivali na direktnoj metodi i koristili metodologiju uvedenu u [Davis 99] pa je izgledalo da nerekurzivna metoda definitivno preovlađuje. Mi ovde zasnivamo celu teoriju na rekurzivnim metodama za koje se pokazalo da su direktno povezane s paraunitarnim matricama iz teorije banaka filtera (Filter Banks). Zato ćemo od direktnih metoda opisati samo prvobitnu Golejevu metodu.

## 4.1. Standardni nerekurzivni algoritmi

Opšti nerekurzivni algoritam za binarne sekvence dao je Golej [Golay 61].

Neka je P permutacija N brojeva i neka je  $b_l(k)$  Bulova funkcija. Unipolarne sekvence:

$$a(k) = \left\{ \sum_{l=1}^{N-1} b_{P(l-1)}(k) b_{P(l)}(k) \right\} \text{ mod } 2$$

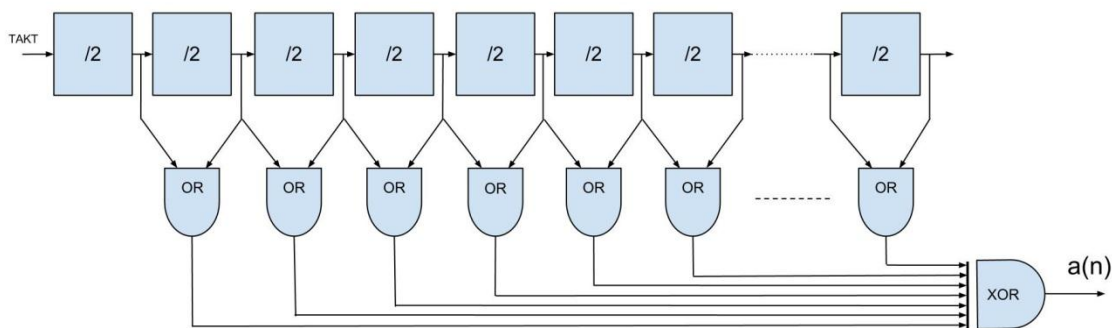
$$b(k) = \left\{ \sum_{l=1}^{N-1} b_{P(l-1)}(k) b_{P(l)}(k) + b_{P(0)}(k) \right\} \text{ mod } 2 \quad (65)$$

čine komplementarni par. Takođe sekvence:

$$a(k) = \left\{ \sum_{l=1}^{N-1} b_{P(l-1)}(k) b_{P(l)}(k) \right\} \text{ mod } 2$$

$$b(k) = \left\{ \sum_{l=1}^{N-1} b_{P(l-1)}(k) b_{P(l)}(k) + b_{P(N-1)}(k) \right\} \text{ mod } 2 \quad (66)$$

čine komplementarni par. Golej dokazuje da par ostaje komplementaran ako obe sekvence (u bipolarnom obliku što odgovara XOR operaciji u unipolarnom obliku) iz para pomnožimo s Volšovom sekvencom. Takođe treba uočiti da je drugi sabirak u izrazu za  $b(k)$  Volšova sekvenca.



Sl. 13. Generator Golejeve sekvence direktnom metodom – prikazan je slučaj osnovne permutacije

Na Sl. 13. ilustriran je generator Golejeve sekvence za osnovnu permutaciju i osnovnu Volšovu funkciju. Generator se svodi na jedan  $N$  stepeni binarni brojač (delitelj) praćen s  $N - 1$  OR kola čiji ulazi idu na  $N - 1$  ulazno XOR kolo. U slučaju da permutacija nije osnovna, samo se drugačije povezuju ulazi u OR kola. Kada Volšova funkcija nije osnovna neki izlazi iz brojača se povezuju na ulaze XOR kola, što znači da u najsloženijem slučaju XOR kolo treba da ima dvaput više ulaza nego u prikazanom slučaju.

U [Paterson 00] pokazano je da ova metoda generiše iste sekvence kao rekurzivna metoda iz [Budišin 90A].

## 4.2. Standardni rekurzivni algoritam

Rekurzivni algoritam kojim se duplira dužina sekvenci zasniva se na sledećim transformacijama koje zadržavaju komplementarnost. Pretpostavimo da je par sekvenci  $a(n)$  i  $b(n)$  komplementaran:

Pomeranje jedne ili obe sekvence u vremenu. Ovo je, u stvari, osobina koja zadržava vrednost autokorelacione funkcije pojedinačnih sekvenci pa samim tim i komplementarnost para. Znači, sekvence  $a(n - k_a)$  i  $b(n - k_b)$  su komplementarne ili formulisano u  $Z$  domenu  $A(Z^{-1}) \cdot Z^{-k_a}$  i  $B(Z^{-1}) \cdot Z^{-k_b}$  predstavljaju komplementarni par.

Fazni pomak jedne ili obe sekvence. Ovo je takođe osobina koja zadržava vrednost autokorelacione funkcije pojedinačnih sekvenci pa samim tim i komplementarnost para. Znači, sekvence  $a(n) \cdot e^{i\alpha}$  i  $b(n) \cdot e^{i\beta}$  su komplementarne odnosno u  $Z$  domenu  $A(Z^{-1}) \cdot e^{i\alpha}$  i  $(Z^{-1}) \cdot e^{i\beta}$ .

Novi par sekvenci koji se dobija kao zbir i razlika početnog para takođe je komplementaran. Dakle, sekvence  $a(n) + b(n)$  i  $a(n) - b(n)$  su komplementarne sekvence, odnosno  $A(Z^{-1}) + B(Z^{-1})$  i  $A(Z^{-1}) - B(Z^{-1})$ . Ovo ćemo dokazati pomoću jednačine (25):

$$\begin{aligned} \mathcal{R}_{a+b}(Z^{-1}) + \mathcal{R}_{a-b}(Z^{-1}) &= \\ \{A(Z) + B(Z)\}\{A^*(Z^{-1}) + B^*(Z^{-1})\} + \{A(Z) - B(Z)\}\{A^*(Z^{-1}) - B^*(Z^{-1})\} &= \\ 2A(Z)A^*(Z^{-1}) + 2B(Z)B^*(Z^{-1}) = 2\{\mathcal{R}_a(Z) + \mathcal{R}_b(Z)\} = 2C & \quad (67) \end{aligned}$$

Ova transformacija suštinski generiše kvalitativno nove komplementarne sekvence. Na bazi ove 3 osnovne transformacije, u radu [Budišin 90A] dat je opšti rekurzivni algoritam koji generiše sve binarne sekvence dužine  $2^n$  iz Golejevog rada

[Golay 61] i polifazne sekvence iste dužine. Neka su početne sekvence dužine 1 date sa  $a_0(n) = b_0(n) = [1]$ . Tada duže sekvence dobijamo sledećom rekurzijom:

$$\begin{aligned} a_{k+1}(n) &= a_k(n) + W_k \cdot b_k(n - D_k) \\ b_{k+1}(n) &= a_k(n) - W_k \cdot b_k(n - D_k) \end{aligned} \quad (68)$$

gde su  $W_k$  unimodularni koeficijenti, kašnjenja su:  $D_k = 2^{P_k}$ ,  $P_k$  je permutacija brojeva  $\{0, 1, \dots, N - 1\}$  a  $N$  je broj rekurzija. Treba izabrati ovakave vrednosti za  $D_k$  jer se tako dobijaju polifazne ili binarne sekvence. Ako to ne postavljamo za uslov onda se mogu uzimati proizvoljne vrednosti za  $D_k$  koeficijente i generisane sekvence i dalje će biti komplementarne. Pri tome treba imati u vidu da je dužina generisanih sekvenci posle poslednje rekurzije jednaka zbiru svih  $D_k$  koeficijenata plus 1 te da se za neki izbor  $D_k$  koeficijenata, u sekvenci mogu pojaviti praznine, to jest – elementi sekvence koji su jednaki nuli. Kada je  $D_k = 2^{P_k}$  dobijaju se najduže sekvence bez praznina čija je dužina  $2^N$ . Tada se sabiranje i oduzimanje u (68) uvek vrši s jednim sabirkom koji je jednak nuli, a to znači da u praktičnoj implementaciji uopšte ne treba sabirati i oduzimati. Kada je dužina veća od  $2^N$  obavezno će se pojaviti praznine. Kada je dužina manja od  $2^N$  obavezno nastaju preklapanja, što znači da će u (68) ponekad oba sabirka biti različita od nule, pa će rezultat sabiranja biti po modulu veći od 1 (ipak postoje slučajevi kada se sabiraju brojevi čiji je moduo jednak 1 a i zbir je jednak 1 ali oni su retki). Treba imati u vidu da izbor dužine sekvenci ne garantuje odsustvo praznina i preklapanja. On je samo preuslov, a njihovo odustvo garantuje samo pravilan izbor kašnjenja  $D_k$ .

Formulisano u domenu  $Z$  transformacije, rekurzija postaje:

$$\begin{aligned} A_{k+1}(Z^{-1}) &= A_k(Z^{-1}) + W_k \cdot B_k(Z^{-1}) \cdot Z^{-D_k} \\ B_{k+1}(Z^{-1}) &= A_k(Z^{-1}) - W_k \cdot B_k(Z^{-1}) \cdot Z^{-D_k} \end{aligned} \quad (69)$$

i najzad u matičnom obliku:

$$\mathbf{x}_{k+1}(Z^{-1}) = \begin{bmatrix} 1 & W_k \cdot Z^{-D_k} \\ 1 & -W_k \cdot Z^{-D_k} \end{bmatrix} \cdot \mathbf{x}_k(Z) = \mathbf{M}_k(Z^{-1}) \cdot \mathbf{x}_k(Z^{-1}) \quad (70)$$

gde je  $\mathbf{x}_k(Z^{-1}) = \begin{bmatrix} A_k(Z^{-1}) \\ B_k(Z^{-1}) \end{bmatrix}$ , a:

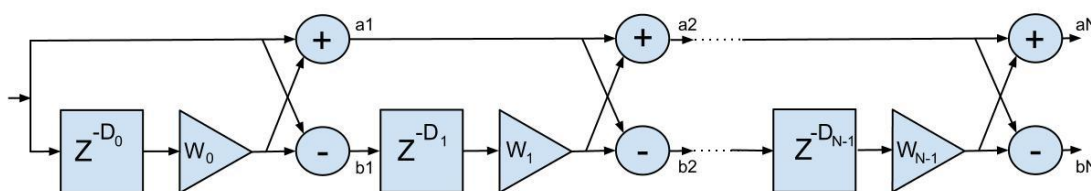
$$\begin{aligned} \mathbf{M}_k(Z^{-1}) &= \begin{bmatrix} 1 & W_k Z^{-D_k} \\ 1 & -W_k Z^{-D_k} \end{bmatrix} = \begin{bmatrix} 1 & W_k \\ 1 & -W_k \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_k} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_k \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_k} \end{bmatrix} \end{aligned} \quad (71)$$

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_{N-1}Z^{-D_{N-1}} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_{N-2}Z^{-D_{N-2}} \end{bmatrix} \cdot \\ &\quad \dots \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_0Z^{-D_0} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned} \quad (72)$$

ili u eksplicitnoj formi:

$$\mathbf{x}_N(Z^{-1}) = \prod_{k=N-1}^0 \left\{ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & W_k Z^{-D_k} \end{bmatrix} \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \prod_{k=N-1}^0 \left\{ \begin{bmatrix} 1 & W_k Z^{-D_k} \\ 1 & -W_k Z^{-D_k} \end{bmatrix} \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (73)$$

Ovaj algoritam možemo prikazati blok šematski kao na Sl. 14:



Sl. 14. Blok šematski prikaz rekurzivnog algoritma za generisanje polifaznih sekvenci

$$\begin{aligned} \mathbf{M}_k(Z^{-1}) &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_k \cdot Z^{-D_k} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix} \cdot W_k \cdot Z^{-D_k} \\ &= \mathbf{A} + \mathbf{B} \cdot W_k \cdot Z^{-D_k} \end{aligned} \quad (74)$$

gde su  $\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$  i  $\mathbf{B} = \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}$ .  $\mathbf{M}_k$  je matrični binom (polinom s dva člana) stepena  $D_k$ . Sada možemo napisati i nerekurzivni – eksplicitni izraz za komplementarne sekvence pomoću binoma iz (74):

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) &= \prod_{k=N-1}^0 \left\{ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & W_k Z^{-D_k} \end{bmatrix} \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \left\{ \prod_{k=N-1}^0 (\mathbf{A} + \mathbf{B} \cdot W_k \cdot Z^{-D_k}) \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned} \quad (75)$$

Na kraju ćemo pokazati alternativnu formu ovog algoritma koja će nam biti korisna kasnije. Polazeći od (71) i (72) možemo pisati:

$$\begin{aligned}
 \mathbf{x}_N(Z^{-1}) &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_{N-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_{N-1}} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_{N-2} \end{bmatrix} \\
 &\cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_{N-2}} \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\
 &\cdot \begin{bmatrix} 1 & 0 \\ 0 & W_0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_0} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} =
 \end{aligned} \tag{76}$$

$$\begin{aligned}
 \mathbf{x}_N(Z^{-1}) &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_{N-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_{N-1}} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_{N-2} \end{bmatrix} \\
 &\cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_{N-2}} \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -W_0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_1} \end{bmatrix} \\
 &\cdot \begin{bmatrix} 1 & 0 \\ 0 & -W_0^* \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_0} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}
 \end{aligned} \tag{77}$$

Ovde smo levo od faktora  $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  na krajnje desnoj strani ubacili matricu:  $\begin{bmatrix} 1 & 0 \\ 0 & -W_0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -W_0^* \end{bmatrix}$  koja je jednaka jediničnoj matrici. Zatim smo zamenili mesta matricama  $\begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_1} \end{bmatrix}$  i  $\begin{bmatrix} 1 & 0 \\ 0 & -W_0 \end{bmatrix}$  pošto su dijagonalne matrice komutativne. Onda matricu  $\begin{bmatrix} 1 & 0 \\ 0 & -W_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -W_0 \end{bmatrix}$  možemo pisati kao  $\begin{bmatrix} 1 & 0 \\ 0 & W_1 W_0 \end{bmatrix}$  koju možemo označiti kao  $\begin{bmatrix} 1 & 0 \\ 0 & w_1 \end{bmatrix}$  i nastaviti proces. Dobili smo novu matricu:

$$\begin{aligned}
 \begin{bmatrix} 1 & 0 \\ 0 & -W_0^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W_0 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & -W_0^* \end{bmatrix} \cdot \begin{bmatrix} 1 & W_0 \\ 1 & -W_0 \end{bmatrix} = \begin{bmatrix} 1 & W_0 \\ -W_0^* & 1 \end{bmatrix} \\
 &= \begin{bmatrix} 1 & -w_0 \\ w_0^* & 1 \end{bmatrix}
 \end{aligned} \tag{78}$$

Na taj način jednačina (76) dobija oblik:

$$\begin{aligned}
 \mathbf{x}_N(Z^{-1}) &= \begin{bmatrix} 1 & -w_{N-1} \\ w_{N-1}^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_{N-1}} \end{bmatrix} \cdot \begin{bmatrix} 1 & -w_{N-2} \\ w_{N-2}^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_{N-2}} \end{bmatrix} \cdot \dots \\
 &\quad \cdot \begin{bmatrix} 1 & -w_1 \\ w_1^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -w_0 \\ w_0^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_0} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
 &= \prod_{k=N-1}^0 \left\{ \begin{bmatrix} 1 & -w_k \\ w_k^* & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_k} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}
 \end{aligned} \tag{79}$$

gde je  $w_0 = -W_0$ ,  $w_1 = -W_1 \cdot W_0$  itd. Kako su  $w_k$  koeficijenti unimodularni kao i  $W_k$  koeficijenti, mi ćemo ubuduće u gornjoj formuli koristiti  $W_k$  umesto  $w_k$ . Takođe treba napomenuti da je u izrazu (79) s krajnje leve strane ispušten jedan faktor oblika  $\begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix}$  ali on nije bitan pošto samo menja fazu  $b$  sekvence a to se svodi na problem normalizacije.

### 4.3. Višenivoske komplementarne sekvence

Drugi za nas važan rekurzivni algoritam dat je u [Budišin 90B] i glasi:

$$\begin{aligned}
 A_{k+1}(Z^{-1}) &= A_k(Z^{-1}) - Q_k \cdot B_k(Z^{-1}) \cdot Z^{-D_k} \\
 B_{k+1}(Z^{-1}) &= Q_k \cdot A_k(Z^{-1}) + B_k(Z^{-1}) \cdot Z^{-D_k}
 \end{aligned} \tag{80}$$

gde je  $Q_k$  realan broj, i može biti prikazan u matričnom obliku:

$$\mathbf{x}_{k+1}(Z^{-1}) = \begin{bmatrix} 1 & -Q_k \cdot Z^{-D_k} \\ Q_k & Z^{-D_k} \end{bmatrix} \mathbf{x}_k(Z) = \mathbf{M}_k(Z^{-1}) \cdot \mathbf{x}_k(Z^{-1}) \tag{81}$$

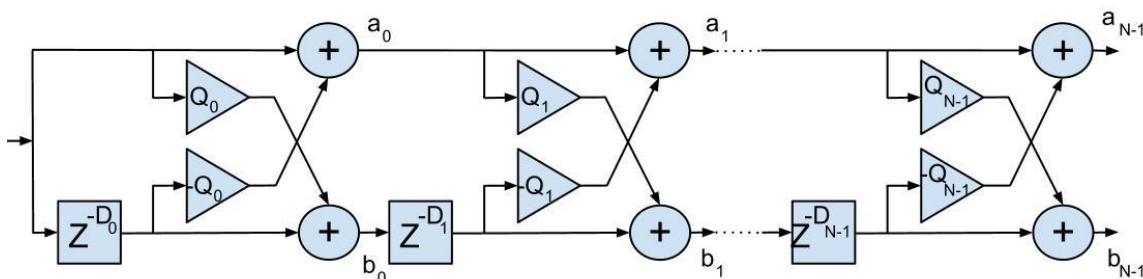
gde je  $\mathbf{x}_k(Z^{-1}) = \begin{bmatrix} A_k(Z^{-1}) \\ B_k(Z^{-1}) \end{bmatrix}$ , a

$$\begin{aligned}
 \mathbf{M}_k(Z^{-1}) &= \begin{bmatrix} 1 & -Q_k \cdot Z^{-D_k} \\ Q_k & Z^{-D_k} \end{bmatrix} = \begin{bmatrix} 1 & -Q_k \\ Q_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_k} \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot Q_k \cdot Z^{-D_k} = \mathbf{C} + \mathbf{D} \cdot Q_k \cdot Z^{-D_k}
 \end{aligned} \tag{82}$$

gde su  $\mathbf{C} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  i  $\mathbf{D} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ . Ovo je matrični binom (polinom s dva člana) stepena  $D_k$ . Koristeći ove relacije možemo napisati i nerekurzivni izraz za komplementarne sekvence kao:

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) = \begin{bmatrix} A_N(Z) \\ B_N(Z) \end{bmatrix} &= \left\{ \prod_{k=N-1}^0 (\mathbf{C} + \mathbf{D} \cdot Q_k \cdot Z^{-D_k}) \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \prod_{k=N-1}^0 \left\{ \begin{bmatrix} 1 & -Q_k \\ Q_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-D_k} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned} \quad (83)$$

Ovaj algoritam se može blok šematski prikazati kao na Sl. 15. Na ulaz se dovodi delta impuls.



Sl. 15. Blok šema algoritma za generisanje višenivoskih komplementarnih sekvenci.

## 4.4. Efikasni korelator komplementarnih sekvenci

U radu [Budišin 91] prvi put je opisan efikasni korelator komplementarnih sekvenci. Za razliku od standardne realizacije korelatora koji zahteva  $N$  operacija, efikasni korelator zahteva  $\log_2(N)$  operacija. To je ista veličina uštede kao kada se umesto DFT algoritma koristi FFT algoritam. Međutim, za razliku od FFT algoritma struktura efikasnog korelatora je veoma jednostavna i uniformna.

Sam korelator je prikazan na Sl. 14 s tim što on predstavlja prilagođeni filter na revertovane i konjugovane sekvence pošto se korelacija svodi na konvoluciju s revertovanom i konjugovanom sekvencom. Blok šema korelatora prilagođenog na sekvence generisane pomoću blok šeme sa Sl. 14 prikazana je u [Popović 99]; slična je blok šemi sa Sl. 14 s tim što se element za kašnjenje nalazi u drugoj grani a  $W$  koeficijenti su konjugovani.

Ovde treba primetiti da je na blok šemi na Sl. 14 prikazan jednoulazni dvoizlazni sklop. Mi ćemo u sledećem poglavlju prikazati opštiju blok šemu generatora/korelatora

koji je dvoulazni i dvoizlazni. Takođe ćemo pokazati da je sklop sa Sl. 14 samo specijalan slučaj tog opštijeg generatora/korelatora.

## 4.5. Varijacije standardnog algoritma

Sada navodimo razne varijante generisanja binarnih komplementarnih sekvenci. Premda ćemo obraditi i polifazne sekvence, usredsredićemo se na generisanje binarnih sekvenci. Pre nego što izložimo algoritme, navešćemo nekoliko osobina komplementarnih sekvenci. Gornji algoritam (70) generiše sekvence čiji je prvi element uvek jednak +1. Sekvence čiji je prvi element jednak -1 mogu se dobiti od prethodnih sekvenci množenjem sa -1.

Sekvenca  $a(n)$  dobijena pomoću permutacije  $P$  i sekvenca dobijena pomoću revertovane permutacije jednake su. Takođe, parovi sekvenci  $[a, b]$  i  $[a', b']$  koji su dobijeni pomoću revertovanih permutacija su takve da su  $a$  i  $a'$  jednake a  $b$  i  $b'$  su međusobno revertovane.

Za komplementarni par  $a(k)$  i  $b(k)$  važi relacija  $b(k) = a(k) \cdot w_{P(0)}(k)$  ili  $b'(k) = a(k) \cdot w_{P(n-1)}(k)$ . Kako sekvence  $b(k)$  i  $b'(k)$  nisu jednake a očigledno imaju istu autokorelacionu funkciju, zaključujemo da su one međusobno revertovane. Znači, ako znamo jednu komplementarnu sekvencu, njena revertovana sekvenca se dobija pomoću izraza:

$$a^R(k) = a^R(k) \cdot w_{P(0)}(k) \cdot w_{P(n-1)}(k). \quad (84)$$

Takođe možemo zaključiti: ako je  $[a, b]$  komplementarni par, komplementarni su parovi  $[a, b^R]$ ,  $[a^R, b]$  i  $[a^R, b^R]$ . Postoji još 12 komplementarnih parova koji se dobijaju tako što se prva ili druga ili obe sekvence invertuju (pomnože sa -1); onda se dobija 16 komplementarnih parova koji odgovaraju jednom osnovnom paru:

$$\begin{aligned} & [a, b], [a, b^R], [a^R, b], [a^R, b^R] \\ & [-a, b], [-a, b^R], [-a^R, b], [-a^R, b^R] \\ & [a, -b], [a, -b^R], [a^R, -b], [a^R, -b^R] \\ & [-a, -b], [-a, -b^R], [-a^R, -b], [-a^R, -b^R] \end{aligned}$$

Ako se komplementarna sekvenca/par  $[a, b]$  generiše pomoću jedinične (70) permutacije  $P_0 = [0, 1, \dots, n-1]$ , onda se sekvenca/par generisan pomoću proizvoljne permutacije  $P$  dobija pomoću izraza:  $a'(n) = a(P_B(n))$  gde je  $P_B$  permutacija bita.  $P_B$  je permutacija brojeva  $[0, 1, \dots, 2^n - 1]$  koja se dobija iz permutacije  $P$  na sledeći način:

$$P_B(n) = \sum_{k=0}^{N-1} b_{P(k)}(n) \cdot 2^k \quad (85)$$

gde  $b_k(n)$  označava k-ti bit broja n. Primer permutacija  $P_B(n)$  naveden je u Tab. 7.

Tab. 7 . Svih šest mogućih permutacija  $P_B(n)$  za N=3

n	Bitovi broja n			Permutacija brojeva (0,1,2) P(k)					
	$b_2(n)$	$b_1(n)$	$b_0(n)$	(0,1,2)	(0,2,1)	(1,0,2)	(1,2,0)	(2,0,1)	(2,1,0)
0	0	0	0	0	0	0	0	0	0
1	0	0	1	1	1	2	4	2	4
2	0	1	0	2	4	1	1	4	2
3	0	1	1	3	5	3	5	6	6
4	1	0	0	4	2	4	2	1	1
5	1	0	1	5	3	6	6	3	5
6	1	1	0	6	6	5	3	5	3
7	1	1	1	7	7	7	7	7	7

U slučaju binarnih sekvenci, ako je komplementarna sekvenca  $a(k)$  dobijena pomoću parametara  $W_k = 1$ , onda se sekvenca  $a'(k)$  dobija uz korišćenje proizvoljnih parametara  $W_k$  tako što se  $a(k)$  sekvenca pomnoži odgovarajućom Volšovom funkcijom. Naime:

$$a'(n) = a(n) \cdot w_k(n) \quad (86)$$

gde je  $w_k(n)$  Volšova funkcija a

$$k = \sum_{l=0}^{n-1} \frac{(W_l + 1)}{2} 2^l \quad (87)$$

pri čemu  $(W_l + 1)/2$  predstavlja unipolarnu verziju koeficijenata  $W_l$ .

Pomoću ove dve formule (86) i (87) mogu se sve binarne komplementarne sekvence određene dužine generisati iz samo jedne osnovne sekvence. Ta osnovna sekvenca može biti generisana sa osnovnom permutacijom i s  $W_l$  koeficijentima jednakim jedan, ali i ne mora. Čak se može poći od bilo koje Golejeve sekvence i množenjem sa svim Volšovim funkcijama i permutovanjem sa svim  $P_B(n)$  permutacijama dobiće se sve moguće Golejeve sekvence. Jedino što u tom slučaju treba posebno voditi računa o numeraciji sekvenci pošto je ona sasvim drugčija nego u slučaju kada se koristi osnovna sekvenca.

## 5. Paraunitarna dekompozicija i reprezentacija

U ovoj glavi nalazi se osnovni doprinos disertacije. Ranije smo videli da se komplementarni par (skup) sekvenci može predstaviti kao paraunitarna matrica-kolona (vektor) odnosno kao proizvod kvadratne paraunitarne matrice i unitarne matrice kolone. Ovde ćemo izvesti jednačine za faktorisanje paraunitarnih matrica u opštem obliku, čime se pokazuje kako se proizvoljan komplementarni par može generisati rekursivnim algoritmom.

Prvo je prikazano kako izgleda faktorizacija paraunitarne matrice veličine  $2 \times 2$  u opštem obliku. Zatim sledi objašnjenje kako se proizvoljni komplementarni par može predstaviti pomoću paraunitarnih matrica i pokazano je da je to ekvivalentno rekursivnom algoritmu za generisanje komplementarnih sekvenci. Najzad navodimo algoritam za određivanje parametara paraunitarne matrice ako je dat bilo koji komplementarni par, čime je definisan rekursivni algoritam za generisanje proizvoljnog komplementarnog para sekvenci. Time je dokazano da se sve sekvence generisane direktnom metodom mogu generisati i rekursivnom metodom. Obrnuto ne važi, što znači da je rekursivna metoda opštija od direktne (nerekursivne) metode.

Na osnovu faktorizacije paraunitarnih matrica izvedena je kanonična forma u kojoj se može predstaviti bilo koji komplementarni par. Definisan je omega vektor koji potpuno određuje komplementarni par. Neke komplementarne sekvence imaju mnogo nula u omega vektoru. U tom slučaju kanonična forma se može modifikovati tako da proizvod matrica koji je definiše ima manje članova i takvu formu zovemo kompaktna kanonična forma. Zanimljivo je zapažanje da se svaki komplementarni par može predstaviti u obliku kompaktne kanonične forme, što znači da je ona isto toliko opšta kao standardna kanonična forma.

Najzad, za sekvence za koje je kompaktna kanonična forma stvarno kompaktna (omega vektor sadrži dosta nula) definiše se stepen efikasnosti generatora/korelatora

pošto se on tada može realizovati s manje operacija nego kada se koristi standardna kanonična forma. Takva implementacija korelatora je poznata kao efikasni korelator.

## 5.1. Faktorizacija paraunitarnih matrica

Ovde ćemo primeniti opšti rezultat iz teorije filterskih banaka i paraunitarnih matrica proizvoljne veličine [Vaidyanathan 93] na paraunitarne matrice veličine  $2 \times 2$  koje su korisne za predstavljanje komplementarnih parova sekvenci. Napominjemo da ovo izvođenje može biti putokaz za proširivanje naše teorije na skupove komplementarnih sekvenci.

Polazeći od glave 14 iz knjige dr Vajdjanatana [Vaidyanathan 93] prvo ćemo izložiti algoritam dekompozicije paraunitarnih matrica veličine  $M \times M$ . Najpre se definišu osnovni blokovi  $V(Z^{-1})$ :

$$\mathbf{V}(Z^{-1}) = \mathbf{I} - \mathbf{v} \cdot \mathbf{v}^H + \mathbf{v} \cdot \mathbf{v}^H \cdot Z^{-1} \quad (88)$$

gde je  $\mathbf{v}$  matrica-kolona (vector-kolona) veličine  $M \times 1$  s jediničnom normom:

$$\mathbf{v}^H \cdot \mathbf{v} = 1 \quad (89)$$

Bilo koja paraunitarna matrica  $\mathbf{P}(Z^{-1})$  veličine  $M \times M$  stepena  $N - 1$  po  $Z^{-1}$  može se faktorisati na sledeći način kao što je dokazano u [Vaidyanathan 93]:

$$\mathbf{P}(Z^{-1}) = \mathbf{V}_{N-1}(Z^{-1}) \cdot \mathbf{V}_{N-2}(Z^{-1}) \cdot \dots \cdot \mathbf{V}_1(Z^{-1}) \cdot \mathbf{P}_0 \quad (90)$$

gde je  $\mathbf{P}_0$  unitarna matrica veličine  $M \times M$ .

Ista faktorizacija je moguća ako je  $\mathbf{p}(Z^{-1})$  paraunitarna matrica veličine  $M \times 1$  ali se u tom slučaju  $\mathbf{P}_0$  zamenjuje matricu-kolonom veličine  $M \times 1$ . Tada možemo da pišemo:

$$\mathbf{p}(Z^{-1}) = \mathbf{V}_{N-1}(Z^{-1}) \cdot \mathbf{V}_{N-2}(Z^{-1}) \cdot \dots \cdot \mathbf{V}_1(Z^{-1}) \cdot \mathbf{p}_0 \quad (91)$$

gde  $\mathbf{p}(Z^{-1})$  i  $\mathbf{p}_0$  označavaju matricu-kolonu (vector-kolonu).

Kako je par komplementarnih sekvenci prikazan paraunitarnom matricom oblika  $2 \times 1$  mi ćemo gornji opšti rezultat primeniti na taj specijalan slučaj. Tako za  $M = 2$  možemo predstaviti  $\mathbf{x}_N(Z^{-1})$  kao:

$$\mathbf{x}_N(Z^{-1}) = \mathbf{V}_{N-1}(Z^{-1}) \cdot \mathbf{V}_{N-1}(Z^{-1}) \cdot \dots \cdot \mathbf{V}_1(Z^{-1}) \cdot \mathbf{p}_0 \quad (92)$$

gde je  $\mathbf{V}_n(Z^{-1})$  paraunitarna matrica oblika  $2 \times 2$  stepena 1 po  $Z^{-1}$  data sa (89). Koristeći jednačinu (14.1.5) iz knjige [Vaidyanathan 93] dobijamo:

$$\mathbf{V}_n(Z^{-1}) \cdot \mathbf{U}_n = \mathbf{U}_n \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \quad (93)$$

gde je  $\mathbf{U}_n$  unitarna matrica i tako možemo pisati:

$$\mathbf{V}_n(Z^{-1}) = \mathbf{U}_n \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \mathbf{U}_n^H = \mathbf{U}_n \cdot \mathbf{D} \cdot \mathbf{U}_n^H \quad (94)$$

Ubacujući ovaj izraz u (92) dobijamo:

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) &= \mathbf{U}_{N-1} \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{U}_{N-1}^H \cdot \mathbf{U}_{N-2} \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{U}_{N-2}^H \cdot \dots \cdot \mathbf{U}_1 \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{U}_1^H \\ &\quad \cdot \mathbf{h}_0 \\ \mathbf{x}_N(Z^{-1}) &= \mathbf{W}_{N-1} \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{W}_{N-2} \cdot \mathbf{D}(Z^{-1}) \dots \cdot \mathbf{W}_n \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{W}_{n-1} \cdot \dots \\ &\quad \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{W}_1 \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{W}_0 \cdot \mathbf{h}_0 \\ &= \left\{ \prod_{n=N-1}^1 \mathbf{W}_n \cdot \mathbf{D}(Z^{-1}) \right\} \cdot \mathbf{W}_0 \cdot \mathbf{h}_0 \end{aligned} \quad (95)$$

gde je  $\mathbf{D}(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix}$ ,  $\mathbf{W}_{N-1} = \mathbf{U}_{N-1}$ ,  $\mathbf{W}_n = \mathbf{U}_{n+1}^H \cdot \mathbf{U}_n$ ,  $\mathbf{W} = \mathbf{U}_1^H$ . Pošto su  $\mathbf{U}_n$  unitarne matrice, napominjemo da su i  $\mathbf{U}_n^H$  unitarne matrice, pa je i proizvod dve unitarne matrice takođe unitarna matrica:  $\mathbf{W}_n = \mathbf{U}_{n+1}^H \cdot \mathbf{U}_n$ .

Za sada nećemo određivati vrednosti matrica  $\mathbf{W}_n$ . Umesto toga navodimo opšti oblik tih unitarnih matrica [Murnaghan 62]:

$$\mathbf{W}_n = \begin{bmatrix} C_n & S_n \\ -S_n^* & C_n^* \end{bmatrix} \quad (96)$$

Da bi matrica bila striktno unitarna kompleksni brojevi  $C_n$  i  $S_n$  treba da ispunjavaju uslov da je  $[C_n]^2 + [S_n]^2 = 1$  odnosno  $|\mathbf{W}_n| = 1$ . Međutim, mi nećemo insistirati na striktnoj unitarnosti tako da u tom slučaju ova dva parametra mogu da imaju proizvoljne vrednosti.

Vidimo da  $\mathbf{W}_n$  matrica zavisi od 2 kompleksna parametra. Čak i kada bi oveli normalizaciju tako da matrica postane striktno unitarna, samo bi ukinuli jedan realni stepen slobode tako da bi još uvek ostala tri slobodna realna parametra. Međutim, u daljem izvođenju mi ćemo pokazati da se broj slobodnih parametara može svesti na jedan kompleksni broj. Matricu  $\mathbf{W}_n$  možemo prikazati kao:

$$\begin{aligned} \mathbf{W}_n &= \begin{bmatrix} C_n & S_n \\ -S_n^* & C_n^* \end{bmatrix} = \begin{bmatrix} C_n & 0 \\ 0 & C_n^* \end{bmatrix} \begin{bmatrix} 1 & S_n/C_n \\ -S_n^*/C_n^* & 1 \end{bmatrix} = \begin{bmatrix} C_n & 0 \\ 0 & C_n^* \end{bmatrix} \begin{bmatrix} 1 & \Phi_n \\ -\Phi_n^* & 1 \end{bmatrix} \\ &= \mathbf{C}_n \cdot \Phi_n \end{aligned} \quad (97)$$

gde je:  $\Phi_n = S_n/C_n$ ,  $\mathbf{C}_n = \begin{bmatrix} C_n & 0 \\ 0 & C_n^* \end{bmatrix}$ ,  $\Phi_n = \begin{bmatrix} 1 & \Phi_n \\ -\Phi_n^* & 1 \end{bmatrix}$ . Obratimo pažnju na to da je  $\mathbf{C}_n$  dijagonalna matrica. U slučaju da su  $C_n$  realne vrednosti,  $\mathbf{C}_n$  bi se mogla prikazati kao  $\mathbf{C}_n = C_n \cdot \mathbf{I}$  i onda bi se sve te matrice mogle izvući ispred proizvoda koji predstavlja

paraunitarnu matricu. Nažalost, u kompleksnom slučaju to nije moguće izvesti direktno. Ipak, zahvaljujući nekim osobinama matrica mi ćemo uspjeti da postignemo sličan efekat.

Sada se vraćamo na opšti oblik paraunitarne matrice-kolone:

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) &= \mathbf{C}_{N-1} \cdot \boldsymbol{\Phi}_{N-1} \cdot \mathbf{D}(Z^{-1}) \cdot \dots \cdot \mathbf{C}_n \cdot \boldsymbol{\Phi}_n \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{C}_{n-1} \cdot \boldsymbol{\Phi}_{n-1} \cdot \dots \\ &\quad \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{C}_0 \cdot \boldsymbol{\Phi}_0 \end{aligned} \quad (98)$$

Prvo uočavamo da su  $\mathbf{D}(Z^{-1})$  i  $\mathbf{C}_n$  dijagonalne matrice pa da zato komutiraju. Zatim ćemo iskoristiti sledeću osobinu  $\boldsymbol{\Phi}$  i  $\mathbf{C}_n$  matrica:

$$\begin{aligned} \boldsymbol{\Phi} \cdot \mathbf{C}_n &= \begin{bmatrix} 1 & \boldsymbol{\Phi} \\ -\boldsymbol{\Phi}^* & 1 \end{bmatrix} \begin{bmatrix} \mathbf{C}_n & 0 \\ 0 & \mathbf{C}_n^* \end{bmatrix} = \begin{bmatrix} \mathbf{C}_n & \mathbf{C}_n^* \boldsymbol{\Phi} \\ -\mathbf{C}_n \boldsymbol{\Phi}^* & \mathbf{C}_n^* \end{bmatrix} = \\ &= \begin{bmatrix} \mathbf{C}_n & 0 \\ 0 & \mathbf{C}_n^* \end{bmatrix} \begin{bmatrix} 1 & \boldsymbol{\Phi} \frac{\mathbf{C}_n^*}{\mathbf{C}_n} \\ -\boldsymbol{\Phi}^* \frac{\mathbf{C}_n}{\mathbf{C}_n^*} & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{C}_n & 0 \\ 0 & \mathbf{C}_n^* \end{bmatrix} \begin{bmatrix} 1 & \boldsymbol{\Phi}' \\ -\boldsymbol{\Phi}'^* & 1 \end{bmatrix} = \mathbf{C}_n \cdot \boldsymbol{\Phi}' \end{aligned} \quad (99)$$

gde je  $\boldsymbol{\Phi}' = \boldsymbol{\Phi} \cdot \mathbf{C}_n^* / \mathbf{C}_n$  and  $\boldsymbol{\Phi}' = \begin{bmatrix} 1 & \boldsymbol{\Phi}' \\ -\boldsymbol{\Phi}'^* & 1 \end{bmatrix}$ .

Osobinu  $\boldsymbol{\Phi} \cdot \mathbf{C}_n = \mathbf{C}_n \cdot \boldsymbol{\Phi}'$  zvaćemo kvazikomutativnost. Kvazikomutativnost se razlikuje od prave komutativnosti po tome što kvazikomutativnost modifikuje  $\boldsymbol{\Phi}$  matricu kada matrice zamene svoja mesta. Pri tome nova  $\boldsymbol{\Phi}'$  matrica ima isti oblik kao prvobitna  $\boldsymbol{\Phi}$  matrica ali one nisu identične kao što bi bilo u slučaju komutativnosti. Moglo bi se to kazati i ovako:  $\mathbf{C}$  matrica “pri prolasku kroz  $\boldsymbol{\Phi}$  matricu” modifikuje  $\boldsymbol{\Phi}$  matricu. Ali kada  $\mathbf{C}_n$  matrica “prolazi kroz  $\mathbf{D}$  matricu” nju ne modifikuje pošto su one strogo komutativne. Dakle, svaka  $\mathbf{C}_n$  matrica može da prođe kroz sve matrice u proizvodu i da se pojavi na krajnje levoj strani proizvoda. Što je još važnije, sve  $\mathbf{C}_n$  matrice će se naći na levoj strani proizvoda jedna pored druge i pošto su sve dijagonalne, njihov proizvod će takođe biti dijagonalna matrica istog oblika i nju ćemo označiti sa  $\mathbf{C}$ . Matrice  $\boldsymbol{\Phi}'$  će biti rezultat prolaska većeg broj  $\mathbf{C}_n$  matrica kroz njih, tako da je komplikovano naći eksplicitni izraz za njih (u opštem obliku). Ali nama to nije ni potrebno pošto znamo da sve te matrice imaju isti opšti oblik. Zato nećemo ni pokušavati da nađemo opšti izraz nego ćemo rezultujuće  $\boldsymbol{\Phi}_n'$  matrice označiti sa:  $\boldsymbol{\Omega}_n$ . Tako možemo pisati:

$$\mathbf{x}_N(Z^{-1}) = \mathbf{C} \cdot \boldsymbol{\Omega}_{N-1} \cdot \mathbf{D}(Z^{-1}) \cdot \dots \cdot \boldsymbol{\Omega}_n \cdot \mathbf{D}(Z^{-1}) \cdot \boldsymbol{\Omega}_{n-1} \cdot \dots \cdot \mathbf{D}(Z^{-1}) \cdot \boldsymbol{\Omega}_0 \cdot \mathbf{h}_0 \quad (100)$$

gde je:  $\boldsymbol{\Omega}_n = \begin{bmatrix} 1 & \boldsymbol{\Omega}_n \\ -\boldsymbol{\Omega}_n^* & 1 \end{bmatrix}$ ;  $\mathbf{C} = \mathbf{C}_{N-1} \cdot \mathbf{C}_{N-2} \cdot \dots \cdot \mathbf{C}_0$  pa dobijamo:

$$\begin{aligned}
 \mathbf{x}_N(Z^{-1}) &= \begin{bmatrix} C & 0 \\ 0 & C^* \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_{N-1} \\ -\Omega_{N-1}^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & \Omega_n \\ -\Omega_n^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \\
 &\quad \cdot \begin{bmatrix} 1 & \Omega_{n-1} \\ -\Omega_{n-1}^* & 1 \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_0 \\ -\Omega_0^* & 1 \end{bmatrix} \cdot \mathbf{h}_0 \\
 &= \mathbf{C} \cdot \left\{ \prod_{n=N-1}^1 \boldsymbol{\Omega}_n \cdot \mathbf{D}(Z^{-1}) \right\} \cdot \boldsymbol{\Omega}_0 \cdot \mathbf{h}_0 \tag{101}
 \end{aligned}$$

Na prvi pogled dobili smo izraz koji je praktično identičnog oblika kao (95). No suštinska razlika je to što u izrazu (95)  $\mathbf{W}_n$  matrice zavise od 2 kompleksna broja, odnosno od 4 realna broja. Čak i posle normalizacije ostaju 3 kompleksna broja koji definišu matricu  $\mathbf{W}_n$ . Međutim,  $\boldsymbol{\Omega}_n$  matrice zavise samo od jednog kompleksnog broja, odnosno od dva realna broja. To znači da u izrazu (95) postoje redundantni podaci koji su ovde otklonjeni. U sledećim odeljcima videćemo da u ovom konačnom izrazu nikakva redundansa više ne postoji.

Iako je iz dosadašnjeg razmatranja verovatno jasno da je faktorizovana paraunitarna matrica ekvivalentna rekurzivnom algoritmu, pokazaćemo to i formalno. Polazeći od izraza (101) možemo pisati:

$$\begin{aligned}
 \mathbf{x}_N(Z^{-1}) &= \mathbf{C} \cdot \left\{ \prod_{n=N-1}^1 \boldsymbol{\Omega}_n \cdot \mathbf{D}(Z^{-1}) \right\} \cdot \boldsymbol{\Omega}_0 \cdot \mathbf{h}_0 \\
 &= \boldsymbol{\Omega}_{N-1} \cdot \mathbf{D}(Z^{-1}) \cdot \left[ \mathbf{C} \cdot \left\{ \prod_{n=N-1}^1 \boldsymbol{\Omega}_n \cdot \mathbf{D}(Z^{-1}) \right\} \cdot \boldsymbol{\Omega}_0 \cdot \mathbf{h}_0 \right] \\
 &= \{\boldsymbol{\Omega}_{N-1} \cdot \mathbf{D}(Z^{-1})\} \cdot \mathbf{x}_{N-1}(Z^{-1}) \tag{102}
 \end{aligned}$$

Ili u razvijenom obliku:

$$\begin{bmatrix} A_n(Z^{-1}) \\ B_n(Z^{-1}) \end{bmatrix} = \begin{bmatrix} 1 & \Omega_{n-1} \\ -\Omega_{n-1}^* & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} A_{n-1}(Z^{-1}) \\ B_{n-1}(Z^{-1}) \end{bmatrix} \tag{103}$$

odnosno:

$$\begin{aligned}
 A_n(Z^{-1}) &= A_{n-1}(Z^{-1}) + \Omega_{n-1} \cdot Z^{-1} \cdot B_{n-1}(Z^{-1}) \\
 B_n(Z^{-1}) &= -\Omega_{n-1}^* \cdot A_{n-1}(Z^{-1}) + Z^{-1} \cdot B_{n-1}(Z^{-1}) \tag{104}
 \end{aligned}$$

ili u vremenskom domenu:

$$\begin{aligned}
 a_n(k) &= a_{n-1}(k) + \Omega_{n-1} \cdot b_{n-1}(k-1) \\
 b_n(k) &= -\Omega_{n-1}^* \cdot a_{n-1}(k) + b_{n-1}(k-1) \tag{105}
 \end{aligned}$$

Takođe treba uočiti da se ovaj rekurzivni algoritam može dobiti pomoću ranije poznatih rekurzivnih algoritama. Iz rada [Budišin 90A] poznato nam je korišćenje unitarne matrice:

$\begin{bmatrix} 1 & 0 \\ 0 & W \end{bmatrix}$  ( $|W| = 1$ ) u rekurzivnom algoritmu. U radu [Budišin 90B] korišćena je unitarna matrica  $\begin{bmatrix} 1 & Q \\ -Q & 1 \end{bmatrix}$  ( $Q$  – realan broj) pomoću koje se vrši rekurzija. Sada formirajmo matricu  $\begin{bmatrix} 1 & 0 \\ 0 & W^* \end{bmatrix} \cdot \begin{bmatrix} 1 & Q \\ -Q & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W \end{bmatrix}$  koja je takođe unitarna matrica pošto je proizvod 3 unitarne matrice i dobijamo matricu:

$$\begin{bmatrix} 1 & 0 \\ 0 & W^* \end{bmatrix} \cdot \begin{bmatrix} 1 & Q \\ -Q & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & W \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & W^* \end{bmatrix} \cdot \begin{bmatrix} 1 & Q \cdot W \\ -Q & W \end{bmatrix} = \begin{bmatrix} 1 & Q \cdot W \\ -Q \cdot W^* & 1 \end{bmatrix} \quad (106)$$

koja tačno odgovara omega matrici za  $\Omega = Q \cdot W$  odnosno  $Q = |\Omega|$  i  $W = \Omega/|\Omega|$ .

## 5.2. Algoritam dekompozicije

Algoritam dekompozicije komplementarnog para omogućava da na jedinstven način izvršimo dekompoziciju i da pomoću parametara dekompozicije na jedinstven način definišemo algoritam za generisanje komplementarnih sekvenci. Ovaj algoritam nije ograničen na binarne i polifazne sekvence ali je primenjiv na njih, i one predstavljaju najvažniji primer primene algoritma dekompozicije.

U prethodnom poglavlju videli smo kako se proizvoljne sekvence mogu generisati primenjivanjem rekurzivnog algoritma da bi od kraćih sekvenci konstruisali duže. Sada ćemo taj isti rekurzivni algoritam koristiti unazad da bismo izvršili dekompoziciju proizvoljnog para. Pođimo od proizvoljnog komplementarnog para:  $\begin{bmatrix} A_N(Z^{-1}) \\ B_N(Z^{-1}) \end{bmatrix}$  dužine  $N$  i primenimo rekurziju:

$$\begin{bmatrix} 1 & \Omega_{N-1} \\ -\Omega_{N-1}^* & 1 \end{bmatrix} \cdot \begin{bmatrix} A_N(Z^{-1}) \\ B_N(Z^{-1}) \end{bmatrix} = \begin{bmatrix} A_N(Z^{-1}) + \Omega_{N-1} \cdot B_N(Z^{-1}) \\ -\Omega_{N-1}^* \cdot A_N(Z^{-1}) + B_N(Z^{-1}) \end{bmatrix} \quad (107)$$

Cilj nam je da skratimo ove dve sekvence bar za 1. To postizemo ako polinom  $A_N(Z^{-1}) + \Omega_{N-1} \cdot B_N(Z^{-1})$  sadrži samo stepene po  $Z^{-1}$  do  $(N - 2)$ -og stepena, odnosno kada učinimo da koeficijent uz  $Z^{N-1}$  bude nula. Kako obe sekvence moraju biti iste dužine, logično je pretpostaviti da to isto treba uraditi s drugim polinomom  $-\Omega_{N-1}^* \cdot A_N(Z^{-1}) + B_N(Z^{-1})$ . Nažalost, to nije moguće istovremeno uraditi ali se taj polinom može skratiti s leve strane, odnosno može se postaviti uslov da slobodni član polinoma bude 0. Te uslove u vremenskom domenu možemo pisati:

$$\begin{aligned} a(N-1) + \Omega_{N-1} \cdot b(N-1) &= 0 \\ -\Omega_{N-1}^* \cdot a(0) + b(0) &= 0 \end{aligned} \quad (108)$$

ili:

$$\begin{aligned} \Omega_{N-1} &= -a(N-1)/b(N-1) \\ \Omega_{N-1}^* &= b(0)/a(0) \end{aligned} \quad (109)$$

Na prvi pogleda izgleda da smo dobili dva različita izraza za  $\Omega_{N-1}$  i da oba uslova ne mogu biti istovremeno ispunjena. Međutim kada postavimo uslov da ova izraza budu međusobno jednaka dobijamo:

$$\begin{aligned} a(N-1)/b(N-1) &= -b^*(0)/a^*(0) \\ a(N-1)a^*(0) + b(N-1)b^*(0) &= 0 \end{aligned} \quad (110)$$

a to je tačno uslov komplementarnosti za  $a$  i  $b$  sekvence.

Sada kada se sekvenca  $a$  nalazi na položaju od 0 do  $N-2$  a sekvencu  $b$  na položaju od 1 do  $N-1$  samo još treba da pomerimo sekvencu  $b$  za jedno mesto ulevo što odgovara množenju sa  $Z$  u domenu  $Z$  transformacije. Tako se novi par sekvenci skraćenih za jedan simbol dobija množenjem s matricom:  $\begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix}$ . Kompletan algoritam sada izgleda ovako:

$$\begin{bmatrix} A_{N-1}(Z^{-1}) \\ B_{N-1}(Z^{-1}) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \begin{bmatrix} 1 & \Omega_{N-1} \\ -\Omega_{N-1}^* & 1 \end{bmatrix} \begin{bmatrix} A_N(Z^{-1}) \\ B_N(Z^{-1}) \end{bmatrix} \quad (111)$$

Iterativnom primenom ovog algoritma dolazimo do:

$$\begin{bmatrix} A_0 \\ B_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_1 \\ -\Omega_1^* & 1 \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_{N-1} \\ -\Omega_{N-1}^* & 1 \end{bmatrix} \cdot \mathbf{x}_N(Z^{-1}) \quad (112)$$

Ako uradimo još jednu iteraciju dobijamo:

$$\begin{aligned} C \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 1 & \Omega_0 \\ -\Omega_0^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_1 \\ -\Omega_1^* & 1 \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_{N-2} \\ -\Omega_{N-2}^* & 1 \end{bmatrix} \\ &\cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_{N-1} \\ -\Omega_{N-1}^* & 1 \end{bmatrix} \cdot \mathbf{x}_N(Z^{-1}) \end{aligned} \quad (113)$$

Ovaj algoritam pokazuje da za svaki zadati par komplementarnih sekvenci, možemo na jedinstven način izračunati parametre dekompozicije  $[\Omega_0, \Omega_1, \dots, \Omega_{N-1}]$ . Ovaj niz kompleksnih brojeva zvaćemo omega vektor komplementarnog para. Zapažamo da postoji jednoznačno preslikavanje koje svakom kompleksnom paru (pogodno normalizovanom) dodeljuje jedan omega vektor, ali i svakom omega vektoru dodeljuje jedan jedinstven komplementarni par sekvenci (defnisan do tačnosti na normalizacionu konstantu  $C$ ). Važna je činjenica da se kao omega vektor može koristiti bilo koji niz kompleksnih brojeva.

### 5.3. Kanonična forma

Ako rešimo jednačinu (113) po  $\mathbf{x}_N(Z^{-1})$  i koristimo osobine matrica:

$$\begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} i \begin{bmatrix} 1 & \Omega \\ -\Omega^* & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -\Omega \\ \Omega^* & 1 \end{bmatrix} (1 + |\Omega|^2)^{-1} \quad (114)$$

dobijamo:

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) = K & \begin{bmatrix} 1 & -\Omega_{N-1} \\ \Omega_{N-1}^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-2} \\ \Omega_{N-2}^* & 1 \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & -\Omega_1 \\ \Omega_1^* & 1 \end{bmatrix} \\ & \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_0 \\ \Omega_0^* & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned} \quad (115)$$

gde je  $K$  kompleksna multiplikativna konstanta jednaka proizvodu  $C$  i svih članova oblika:  $(1 + |\Omega|^2)^{-1}$  odnosno:

$$K = C \cdot \prod_{k=0}^{N-1} (1 + |\Omega_k|^2)^{-1} \quad (116)$$

Bez umanjnja opštosti možemo pretpostaviti da je  $K = 1$  pošto  $K$  samo određuje fazu i amplitudu sekvenci a to nije ključna osobina komplementarnog para.

Koristeći notaciju:

$$\mathbf{U}_\Omega = \begin{bmatrix} 1 & -\Omega \\ \Omega^* & 1 \end{bmatrix}, \mathbf{D} = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} i \mathbf{V}_\Omega(Z^{-1}) = \mathbf{U}_\Omega \cdot \mathbf{D}(Z^{-1}) = \begin{bmatrix} 1 & -\Omega \cdot Z^{-1} \\ \Omega^* & Z^{-1} \end{bmatrix}$$

možemo da pišemo:

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) &= \mathbf{U}_{\Omega_{N-1}} \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{U}_{\Omega_{N-2}} \cdot \mathbf{D}(Z^{-1}) \cdot \dots \cdot \mathbf{U}_{\Omega_1} \cdot \mathbf{D}(Z^{-1}) \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \left\{ \prod_{k=N-1}^1 \mathbf{V}_{\Omega_k}(Z^{-1}) \right\} \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \prod_{k=N-1}^1 \{ \mathbf{U}_{\Omega_k} \cdot \mathbf{D}(Z^{-1}) \} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned} \quad (117)$$

$$\mathbf{x}_N(Z^{-1}) = \prod_{k=N-1}^1 \left\{ \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (118)$$

ili

$$\mathbf{x}_N(Z^{-1}) = \mathcal{M}_N(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (119)$$

gde je:

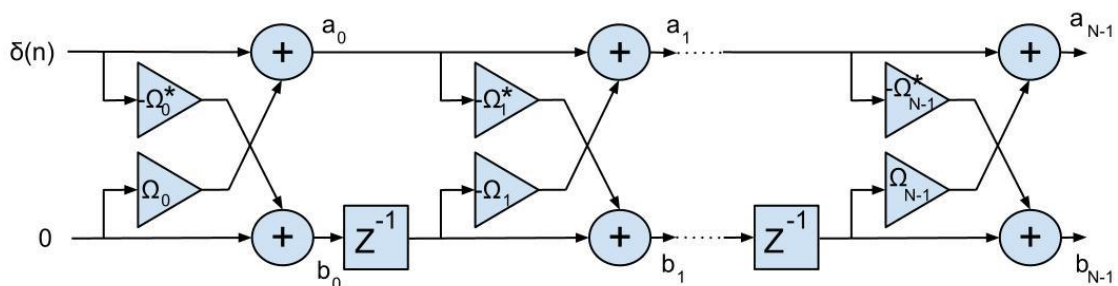
$$\begin{aligned}
 \mathcal{M}_N(Z^{-1}) &= \left\{ \prod_{k=N-1}^1 \mathbf{V}_{\Omega_k}(Z^{-1}) \right\} \cdot \mathbf{U}_{\Omega_0} = \prod_{k=N-1}^1 \{ \mathbf{U}_{\Omega_k} \cdot \mathbf{D}(Z^{-1}) \} \cdot \mathbf{U}_{\Omega_0} \\
 &= \prod_{k=N-1}^1 \left\{ \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix}
 \end{aligned} \tag{120}$$

generišuća matrica komplementarnog para.

Jasno je da generišuća matrica zadovoljava rekurzivnu jednačinu:

$$\mathcal{M}_{n+1}(Z^{-1}) = \begin{bmatrix} 1 & -\Omega_n^* \\ \Omega_n & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \mathcal{M}_n(Z^{-1}) \tag{121}$$

Kanonična forma se može predstaviti blok šematski kao na Sl. 16.



Sl. 16. Kanonična forma

## 5.4. Kompaktna kanonična forma

U mnogim slučajevima koji su zanimljivi u praksi, na primer kod Golejevih binarnih sekvenci, standardnih polifaznih sekvenci, standardnih 16-QAM sekvenci itd., veliki broj omega koeficijenata je nula. Matematički rečeno, omega vektor je redak. Tada se može napisati gornji proizvod s mnogo manje faktora i tako se dobija mnogo kompaktnija forma. Recimo, kod Golejevih binarnih sekvenci i kod standardnih polifaznih sekvenci dužine  $2^N$  taj proizvod ima samo  $N$  članova umesto  $2^N$ .

U stvari, ako je neki od  $\Omega_k$  jednak nuli, onda je  $\mathbf{U}_{\Omega_k} = \begin{bmatrix} 1 & -\Omega_k \\ \Omega_k^* & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}$ .

Tada je  $\mathbf{D} \cdot \mathbf{U}_{\Omega_k} \cdot \mathbf{D} = \mathbf{D} \cdot \mathbf{I} \cdot \mathbf{D} = \mathbf{D}^2$ . Isto tako ako je niz uzastopnih omega vrednosti nula:

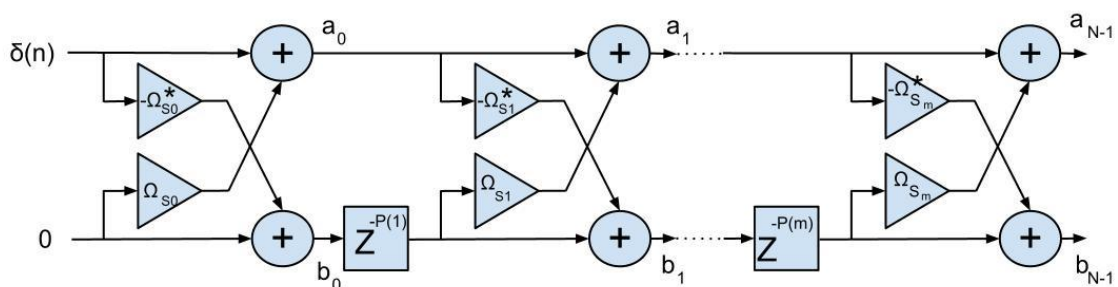
$\Omega_k, \Omega_{k+1}, \dots, \Omega_{k+N-1} = 0$  dobijamo:

$$\begin{aligned} \mathbf{D} \cdot \mathbf{U}_{\Omega_k} \cdot \mathbf{D} \cdot \mathbf{U}_{\Omega_{k+1}} \cdot \mathbf{D} \cdot \dots \cdot \mathbf{D} \cdot \mathbf{U}_{\Omega_{k+N-1}} \cdot \mathbf{D} &= \mathbf{D} \cdot \mathbf{I} \cdot \mathbf{D} \cdot \mathbf{I} \cdot \dots \cdot \mathbf{D} \cdot \mathbf{I} \cdot \mathbf{I} \cdot \mathbf{D} \\ &= \mathbf{D}^{N+1} \end{aligned} \quad (122)$$

Na osnovu toga možemo napisati:

$$\begin{aligned} \mathbf{x}_N(Z^{-1}) &= \mathbf{U}_{\Omega_{S(m)}} \cdot \mathbf{D}^{P(m)} \cdot \dots \cdot \mathbf{U}_{\Omega_{S(1)}} \cdot \mathbf{D}^{P(1)} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \left\{ \prod_{k=m}^1 \mathbf{v}_{\Omega_{S(k)}}(Z^{-P(k)}) \right\} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \left\{ \prod_{k=m}^1 \mathbf{U}_{\Omega_{S(k)}} \cdot \mathbf{D}(Z^{-P(k)}) \right\} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \left\{ \prod_{k=m}^1 \begin{bmatrix} 1 & -\Omega_{S(k)}^* \\ \Omega_{S(k)} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-P(k)} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -\Omega_{S(0)}^* \\ \Omega_{S(0)} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned} \quad (123)$$

gde  $S(k)$  označava položaj  $k$ -tog nenultog elementa u  $\Omega$  spektru a  $P(m)$  je broj nultih omega vrednosti između dva nenulta elementa:  $P(m) = S(m) - S(m-1)$ . Prvi i poslednji element u omega spektru moraju biti nenulte vrednosti inače dužina sekvence ne bi bila jednaka  $N$  nego manja, tako da mora biti  $S(0) = 1$  i  $S(m) = N$ . Takođe uočavamo i ovo: ako je za svako “ $k$ ”  $P(k) = 1$  izraz (123) se svodi na (117) i ta dva izraza su potpuno ekvivalentna. Drugim rečima, izraz (123) je isto toliko opšti kao izraz (117). Jedino se razlikuju po tome što izraz (123) ima manje faktora nego izraz (117) ako je omega vektor redak. Međutim ako omega vector nije redak oba izraza imaju identičan broj factor  $I$  izgledaju identično. Kompaktna kanonična forma se može prikazati blok šematski kao na Sl. 17.



Sl. 17. Kompaktna kanonična forma

Tipičan primer algoritma u kompaktnoj kanoničnoj formi jeste rekurzivni algoritam za generisanje binarnih i polifaznih komplementarnih sekvenci iz [Budišin 90A] dat jednačinom (70).

## 5.5. Dvokanalni paraunitarni filtri

Generišuća matrica  $\mathcal{M}(Z^{-1})$  iz (120) opisuje dvoulazno-dvoizlazni FIR filter. Iako je do sada jasno da je  $\mathcal{M}(Z^{-1})$  paraunitarna matrica, mi ćemo prvo izvesti njene. Prvo ćemo dokazati sledeću teoremu:

TEOREMA: Ako je:

$$\mathbf{x}_n = \begin{bmatrix} A_n(Z^{-1}) \\ B_n(Z^{-1}) \end{bmatrix} = \mathcal{M}_n(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (124)$$

pri čemu je  $\mathbf{x}_n$  komplementarni par a  $\mathcal{M}_n(Z^{-1})$  paraunitarna matrica onda je:

$$\begin{aligned} \mathcal{M}_n &= \begin{bmatrix} \mathcal{M}_{11}(Z^{-1}) & \mathcal{M}_{12}(Z^{-1}) \\ \mathcal{M}_{21}(Z^{-1}) & \mathcal{M}_{22}(Z^{-1}) \end{bmatrix} = \begin{bmatrix} A_n(Z^{-1}) & -B_n^{*R}(Z^{-1}) \\ B_n(Z^{-1}) & A_n^{*R}(Z^{-1}) \end{bmatrix} \\ &= \begin{bmatrix} A_n(Z^{-1}) & -Z^{-N+1}B_n^*(Z) \\ B_n(Z^{-1}) & Z^{-N+1}A_n^*(Z) \end{bmatrix} \end{aligned} \quad (125)$$

Za dokaz ćemo koristiti matematičku indukciju. Prvo ćemo dokazati teoremu za  $N = 1$  a zatim i to da iz pretpostavke da važi za  $n$  sledi da važi za  $n+1$ . Očigledno je da na osnovu (120) važi:

$$\mathcal{M}_1(Z^{-1}) = \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \quad (126)$$

što je oblika

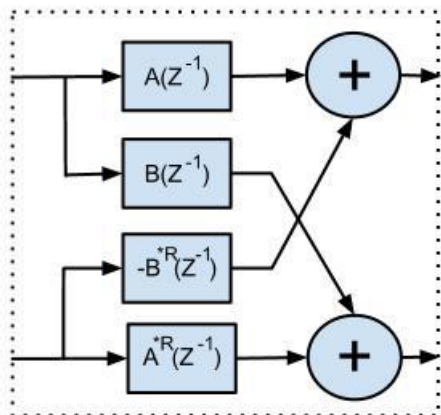
$$\mathcal{M}_1 = \begin{bmatrix} A_1 & -B_1^{*R} \\ B_1 & A_1^{*R} \end{bmatrix} \quad (127)$$

za  $A_1 = 1$  i  $B_1 = \Omega_0$

Sada dokažimo da  $\mathcal{M}_{n+1}$  ima oblik (115) ako  $\mathcal{M}_n$  ima taj oblik:

$$\begin{aligned} \mathcal{M}_{n+1}(Z^{-1}) &= \begin{bmatrix} 1 & -\Omega_n^* \\ \Omega_n & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \mathcal{M}_n(Z^{-1}) \\ &= \begin{bmatrix} 1 & -\Omega_n^* \\ \Omega_n & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} A_n(Z^{-1}) & -B_n^{*R}(Z^{-1}) \\ B_n(Z^{-1}) & A_n^{*R}(Z^{-1}) \end{bmatrix} \\ &= \begin{bmatrix} 1 & -\Omega_n^* \cdot Z^{-1} \\ \Omega_n & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} A_n(Z^{-1}) & -Z^{-N+1}B_n^*(Z) \\ B_n(Z^{-1}) & Z^{-N+1}A_n^*(Z) \end{bmatrix} \\ &= \begin{bmatrix} A_n(Z^{-1}) - \Omega_n^* \cdot Z^{-1}B_n(Z^{-1}) & -(Z^{-N+1}B_n^*(Z) + \Omega_n^* \cdot Z^{-N}A_n^*(Z)) \\ \Omega_n A_n(Z^{-1}) + Z^{-1}B_n(Z^{-1}) & Z^{-N}A_n^*(Z) - \Omega_n Z^{-N+1}B_n^*(Z) \end{bmatrix} \\ &= \begin{bmatrix} A_n(Z^{-1}) - \Omega_n^* \cdot Z^{-1}B_n(Z^{-1}) & -\{\Omega_n A_n(Z^{-1}) + Z^{-1}B_n(Z^{-1})\}^{*R} \\ \Omega_n A_n(Z^{-1}) + Z^{-1}B_n(Z^{-1}) & \{A_n(Z^{-1}) - \Omega_n^* \cdot Z^{-1}B_n(Z^{-1})\}^{*R} \end{bmatrix} \end{aligned} \quad (128)$$

Time je dokazivanje završeno. Blok šematski prikaz generišuće matrice nalazi se na Sl. 18.



Sl. 18. Opšti oblik dvokanalnog generišućeg filtera

Zatim ćemo pokazati sledeću osobinu. Ako je  $\mathcal{M}_G(Z^{-1})$  matični polinom stepena  $N - 1$ :

$$\mathcal{M}_G(Z^{-1}) = \begin{bmatrix} A(Z^{-1}) & -B^{*R}(Z^{-1}) \\ B(Z^{-1}) & A^{*R}(Z^{-1}) \end{bmatrix} = \begin{bmatrix} A(Z^{-1}) & -Z^{-N+1}B^*(Z) \\ B(Z^{-1}) & Z^{-N+1}A^*(Z) \end{bmatrix} \quad (129)$$

a definišemo matricu  $\mathcal{M}_C(Z^{-1})$  kao:

$$\begin{aligned} \mathcal{M}_C(Z^{-1}) &= \widetilde{\mathcal{M}}_G(Z^{-1}) = \mathcal{M}_G^{T^*}(Z) = \begin{bmatrix} A^*(Z) & B^*(Z) \\ -B^R(Z) & A^R(Z) \end{bmatrix} \\ &= \begin{bmatrix} A^*(Z) & B^*(Z) \\ -Z^N B(Z^{-1}) & Z^N A(Z^{-1}) \end{bmatrix} \end{aligned} \quad (130)$$

onda je

$$\begin{aligned} \mathcal{M}_G(Z^{-1}) \cdot \mathcal{M}_C(Z^{-1}) &= \begin{bmatrix} A(Z^{-1}) & -Z^{-N}B^*(Z) \\ B(Z^{-1}) & Z^{-N}A^*(Z) \end{bmatrix} \cdot \begin{bmatrix} A^*(Z) & B^*(Z) \\ -Z^N B(Z^{-1}) & Z^N A(Z^{-1}) \end{bmatrix} \\ &= \begin{bmatrix} A(Z^{-1})A^*(Z) + B(Z^{-1})B^*(Z) & A(Z^{-1})B^*(Z) - B^*(Z)A(Z^{-1}) \\ B(Z^{-1})A^*(Z) - A^*(Z)B(Z^{-1}) & A(Z^{-1})A^*(Z) + B(Z^{-1})B^*(Z) \end{bmatrix} = C^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= C^2 \mathbf{I} \end{aligned} \quad (131)$$

Matricu  $\mathcal{M}_G(Z^{-1})$  zovemo generišuća matrica a  $\mathcal{M}_C(Z^{-1})$  komprimujuća ili korelišuća matrica. Ukoliko se obe matrice normalizuju na  $C$ , onda su striktno inverzne. Međutim, matrica  $\mathcal{M}_C(Z^{-1})$  ne odgovara kauzalnom FIR filteru, pa da bismo dobili kauzalni filter formiramo matricu:

$$\begin{aligned} \mathcal{M}_{CC}(Z^{-1}) &= \mathcal{M}_C(Z^{-1}) \cdot Z^{-N+1} = \begin{bmatrix} Z^{-N+1} \cdot A^*(Z) & Z^{-N+1} \cdot B^*(Z) \\ -B(Z^{-1}) & A(Z^{-1}) \end{bmatrix} \\ &= \begin{bmatrix} A^{*R}(Z^{-1}) & B^{*R}(Z^{-1}) \\ -B(Z^{-1}) & A(Z^{-1}) \end{bmatrix} \end{aligned} \quad (132)$$

Ova osobina generišućeg i komprimujućeg FIR filtera protivreči inženjerskoj logici. Mi smo navikli da inverzni filter FIR filtera može biti samo IIR filter – naime u teoriji jednoulazno- jednoizlaznih filtera, FIR filteri imaju samo nule u prenosnoj funkciji i da bi se te nule poništile potrebni su nam polovi koji postoje samo u IIR filterima. Očigledno, u teoriji dvoulazno-dvoizlaznih (2U2I) filtera ta osobina ne važi pošto koeficijenti filtera nisu kompleksni brojevi nego matrice. Glavna razlika između matrice i realnih koeficijenata jeste to što za prve ne važi zakon komutativnosti. Upravo zbog toga što u teoriji 2U2I filtera ne važi komutativnost, ona je mnogo bogatija od teorije standardnih filtera.

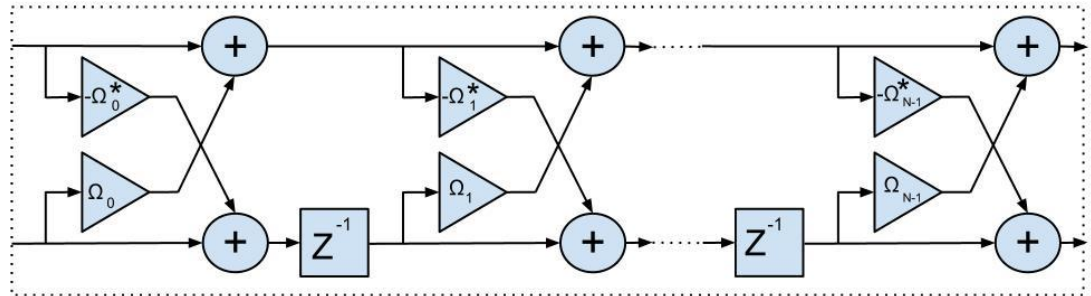
Pogledajmo sada kako izgleda korelišuća matrica kada je generišuća matrica data u kanoničnoj formi:

$$\mathcal{M}_G(Z^{-1}) = \prod_{k=N-1}^1 \left\{ \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \quad (133)$$

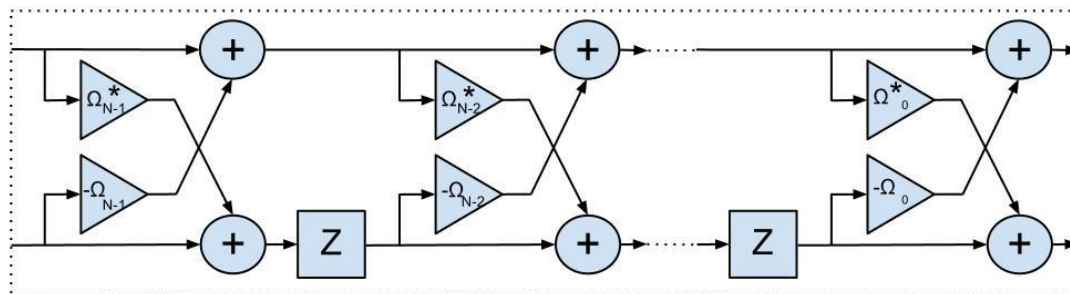
$$\begin{aligned} \mathcal{M}_C(Z^{-1}) &= \mathcal{M}_G^{T^*}(Z) = \begin{bmatrix} 1 & \Omega_0^* \\ -\Omega_0 & 1 \end{bmatrix} \cdot \prod_{k=1}^{N-1} \left\{ \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & \Omega_k^* \\ -\Omega_k & 1 \end{bmatrix} \right\} \\ &= \prod_{k=0}^{N-2} \left\{ \begin{bmatrix} 1 & \Omega_k^* \\ -\Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & \Omega_{N-1}^* \\ -\Omega_{N-1} & 1 \end{bmatrix} \end{aligned} \quad (134)$$

$$\begin{aligned} \mathcal{M}_{CC}(Z^{-1}) &= \mathcal{M}_C(Z^{-1}) \cdot Z^{-N+1} \\ &= \prod_{k=0}^{N-2} \left\{ \begin{bmatrix} 1 & \Omega_k^* \\ -\Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} Z^{-1} & 0 \\ 0 & 1 \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & \Omega_{N-1}^* \\ -\Omega_{N-1} & 1 \end{bmatrix} \end{aligned} \quad (135)$$

Generišuća i korelišuća matrica prikazane su na slikama Sl. 19 i Sl. 20.



Sl. 19. Kanonična forma generišuće matrice



Sl. 20. Korelišuća matrica

U svetlu teorije paraunitarnih matrica možemo uočiti da su  $\mathcal{M}_G(Z^{-1})$  i  $\mathcal{M}_C(Z^{-1})$  inverzne paraunitarne matrice i da se mogu dobiti jedna iz druge primenom tilda operatora. Ovo pokazuje koliko se izvođenje pojednostavljuje kada se koristi teorija paraunitarnih matrica.

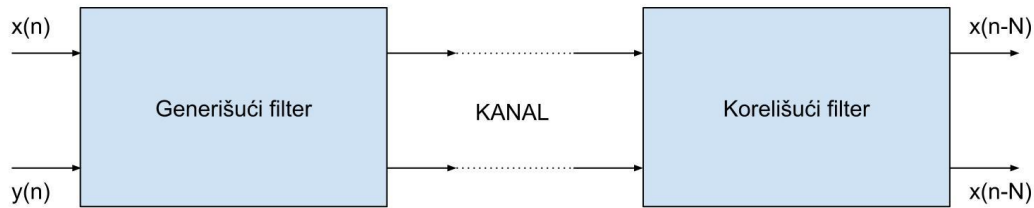
Najzad treba napomenuti da se u generišućoj matrici pojavljuju sva 4 moguća para komplementarnih sekvenci vezanih za jednu Golejevu sekvencu – A i B, A revertovano i B revertovano, A i B revertovano, A revertovano i B. Tako možemo dobiti sledeće parove:

$$\begin{aligned} \mathcal{M}(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} A(Z^{-1}) \\ B(Z^{-1}) \end{bmatrix} \\ \mathcal{M}(Z^{-1}) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} &= \begin{bmatrix} -B^{*R}(Z^{-1}) \\ A^{*R}(Z^{-1}) \end{bmatrix} \\ \mathcal{M}(Z^{-1})^T \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} A(Z^{-1}) \\ -B^{*R}(Z^{-1}) \end{bmatrix} \\ \mathcal{M}(Z^{-1})^T \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} &= \begin{bmatrix} B(Z^{-1}) \\ A^{*R}(Z^{-1}) \end{bmatrix} \end{aligned}$$

## 5.6. Dvokanalni komunikacioni sistem

U prethodnom odeljku videli smo da generišuća matrica i kauzalna korelišuća matrica poništavaju jedna drugu. Odnosno, ako kaskadiramo dva takva bloka rezultat su isti signali koje imamo na ulazu u prvi blok samo pomereni u vremenu (zakašnjeni). To nam daje mogućnost da prvi blok stavimo na predajnu stranu a drugi blok na prijemnu. Rezultat bi bio idealan prenos u proširenom spektru bez ikakvih korelacionih bočnih

lobova koji se inače uvek javljaju u jednokanalnim sistemima za prenos u proširenom spektru. Ili u slučaju primene u radarima to bi bila idealna kompresija impulse bez ikakvih bočnih lobova. Takav sistem je prikazan na Sl. 21.



Sl. 21. Dvokanalni primopredajni system

Nažalost, u realnim sistemima teško se primenjuje ovakav prenos jer ne postoje dva identična kanala. To je praktično nemoguće u radarskim primenama gde je priroda problema takva da se ne može izvršiti sinhronizacija kao u komunikacionim kanalima. Potencijalno, ovakav prenos može se primeniti kada se koriste dve polarizacioni ravni antene ali i tu postoji problem zbog nejednakih refleksionih osobina ciljeva u dve različite polarizacione ravni i zbog međupolarizacije.

Nešto je bolja situacija u komunikacionim sistemima pošto kod njih može da se izvrši sinhronizacija (vremenska, frekvencijska, polarizaciona). Naročito je zanimljiva primena u MIMO sistemima, naročito u sistemima s dve antene (2I2O). Tu se već standardno primenjuje Alamutijev algoritam koji koristi matrice istog oblika kao naše omega matrice. U svakom slučaju, pod uslovom da je ostvarena sinhronizacija između prijemnika i predajnika, dva kanala prenosa mogu da se obezbede na jedan od sledećih načina:

- koriste se dve polarizacione ravni
- koriste se dve antene na prijemu i na predaji: MIMO
- koristi se frekvencijski multipleks
- koristi se vremenski multipleks.

## 5.7. Ostali rekurzivni algoritmi

Golej pored direktnog algoritma (nerekurzivnog) daje i nekoliko rekurzivnih algoritama koji se mogu primeniti i na sekvence čije dužine nisu stepeni dvojke. Navodimo te algoritme formulisane u matricnoj notaciji. Za svaki dajemo generišuću matricu i određujemo omega vektor. Međutim pre navođenja samih algoritama dajemo neke osobine specijalnih generišućih matrica i njihovih omega vektora koje će biti korisne za formulisanje tih algoritama u matičnom obliku.

### 5.7.1. Osobine generišućih matrica i omega vektora

Pre nego što damo ove konkretne algoritme dajemo nekoliko važnih osobina generišuće matrice odnosno omega vektora.

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & -\Omega_1^* \\ \Omega_1 & 1 \end{bmatrix}$  omega vektor je očigledno  $\Omega = [\Omega_1]$  (vektor dužine 1).
- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}$  omega vektor je  $\Omega = [0]$
- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} C & -S^* \\ S & C^* \end{bmatrix} = \begin{bmatrix} 1 & -S^*/C^* \\ S/C & 1 \end{bmatrix} \begin{bmatrix} C & 0 \\ 0 & C^* \end{bmatrix}$ . Pa komplementarni par možemo pisati kao:

$$\mathbf{y}(Z^{-1}) = \begin{bmatrix} 1 & -S^*/C^* \\ S/C & 1 \end{bmatrix} \begin{bmatrix} C & 0 \\ 0 & C^* \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = C \begin{bmatrix} 1 & -S^*/C^* \\ S/C & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

Odakle dobijamo da je:  $\Omega = [S/C]$

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$  na osnovu predhodne tačke  $\Omega = [S/C] = [1/0] = [\infty]$
- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & -\Omega_1^* \\ \Omega_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -\Omega_2^* \\ \Omega_2 & 1 \end{bmatrix} = \begin{bmatrix} 1 - \Omega_1^* \Omega_2 & -\Omega_1^* - \Omega_2^* \\ \Omega_1 + \Omega_2 & 1 - \Omega_1 \Omega_2^* \end{bmatrix}$  koristeći rezultat iz predhodne tačke dobijamo:

$$\Omega = [S/C] = \left[ \frac{\Omega_1 + \Omega_2}{1 - \Omega_1^* \Omega_2} \right]$$

- Ako se nova matrica dobija decimacijom matrice:

$$\mathcal{M}(Z^{-1}) = \mathcal{M}_1(Z^{-K})$$

Pri čemu je stepen matrice  $\mathcal{M}_1$  jednak N. onda je omega vektor dat sa:

$$\Omega = \left[ \underbrace{\Omega_0^{(1)}, 0, \dots, 0}_{K-1}, \underbrace{\Omega_1^{(1)}, 0, \dots, 0}_{K-1}, \dots, \underbrace{0, \dots, 0}_{K-1}, \underbrace{\Omega_{N-1}^{(1)}, 0, \dots, 0}_{K-1} \right]$$

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  omega vektor je

$$\Omega = [0, 0]$$

- Za  $\mathcal{M}(Z^{-1}) = \mathcal{M}_1(Z^{-1}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix}$  omega vektor je:

$$\Omega = [0, \Omega_0^{(1)}, \Omega_1^{(1)}, \dots, \Omega_{N-2}^{(1)}, \Omega_{N-1}^{(1)}]$$

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \mathcal{M}_1(Z^{-1})$  omega vektor je:

$$\Omega = [\Omega_0^{(1)}, \Omega_1^{(1)}, \dots, \Omega_{N-2}^{(1)}, \Omega_{N-1}^{(1)}, 0]$$

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-2} \end{bmatrix}$  omega vektor je  $\Omega = [0, 0, 0]$

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z^{-K} \end{bmatrix}$  omega vektor je  $\Omega = \left[ \underbrace{0, 0, \dots, 0, 0}_{K+1} \right]$

- Problem određivanja omega vektora kada je generišuće matrice je u opštem slučaju složen:

$$\mathcal{M}(Z^{-1}) = \mathcal{M}_1(Z^{-1}) \cdot \mathcal{M}_2(Z^{-1})$$

Razlog tome leži u činjenici da kanonična forma generišuće matrice počinje i završava sa omega matricom pa množenjem dve generišuće matrice u sredini proizvoda dobijamo proizvod dve omega matrice koji, kao što smo videli u predhodnoj tački, nije omega matrica. Zbog toga ćemo se zadovoljiti određivanjem jednog specijalnog slučaja proizvoda:

- $\mathcal{M}(Z^{-1}) = \mathcal{M}_1(Z^{-1}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-K} \end{bmatrix} \cdot \mathcal{M}_2(Z^{-1})$ . U ovom slučaju matrica  $\begin{bmatrix} 1 & 0 \\ 0 & Z^{-K} \end{bmatrix}$  razdvaja poslednju omega matricu matrice  $\mathcal{M}_1(Z^{-1})$  od prve omega matrice matrice  $\mathcal{M}_2(Z^{-1})$  pa se ne pojavljuje njihov proizvod. Omega vektor ima oblik:

$$\Omega = \left[ \Omega_0^{(2)}, \Omega_1^{(2)}, \dots, \Omega_{N-2}^{(2)}, \Omega_{N-1}^{(2)}, \underbrace{0, 0, \dots, 0, 0}_K, \Omega_0^{(1)}, \Omega_1^{(1)}, \dots, \Omega_{M-2}^{(1)}, \Omega_{M-1}^{(1)}, \right]$$

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} 0 & -Z^{-1} \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  pa je omega vektor  $\Omega = [0, \infty]$ . Ovde treba imati u vidu da je ova beskonačnost posledica usvojene normalizacije unitarnih matrica. Naime za omega matrice usvojena normalizacija je  $C = 1$  što je bilo pogodno za jednostavnije predstavljanje binarnih i polifaznih sekvenci. Opštija normalizacija, koju smo već spominjali ranije, se bazira na  $|C|^2 + |S|^2 = 1$ , u kom slučaju bi se izbegle beskonačnosti.

- Za  $\mathcal{M}(Z^{-1}) = \begin{bmatrix} Z^{-1} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$  pa je omega vektor  $\Omega = [\infty, \infty]$

### 5.7.2. Algoritam nadovezivanja (concatenation)

Ovaj algoritam se svodi na dodavanje elemenata druge sekvence iza elemenata prve sekvence. Za par sekvenci  $\mathbf{x}(Z^{-1})$  dužine  $N$ , novi par  $\mathbf{y}(Z^{-1})$  dobija se pomoću:

$$\mathbf{y}(Z^{-1}) = \begin{bmatrix} 1 & -Z^{-N} \\ 1 & Z^{-N} \end{bmatrix} \mathbf{x}(Z^{-1}) \quad (136)$$

Ako  $\mathbf{x}(Z^{-1})$  prikažemo u kanoničnoj formi:

$$\mathbf{x}(Z^{-1}) = \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}_{\mathbf{x}(Z^{-1})} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (137)$$

tada je:

$$\begin{aligned} \mathcal{M}_{\mathbf{y}(Z^{-1})} &= \begin{bmatrix} 1 & -Z^{-N} \\ 1 & Z^{-N} \end{bmatrix} \cdot \mathcal{M}_{\mathbf{x}(Z^{-1})} \\ \mathcal{M}_{\mathbf{y}(Z^{-1})} &= \left\{ \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix}^{N-1} \\ &\quad \cdot \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \mathbf{U}_{\Omega_0} \end{aligned} \quad (138)$$

Znači, ako je omega vektor  $\mathbf{x}(Z^{-1})$  komplementarnog para:  $[\Omega_0, \Omega_1, \dots, \Omega_N]$  onda je omega vektor  $\mathbf{y}(Z^{-1})$  komplementarnog para jednak:

$$\left[ \Omega_0, \Omega_1, \dots, \Omega_{N-1}, \underbrace{0, \dots, 0}_{N-1}, -1 \right]$$

### 5.7.3. Algoritam učešljavanja (interleaving)

Po ovom algoritmu, nove sekvence se formiraju naizмениčnim učešljavanjem elemenata  $a$  i  $b$  sekvence. Dakle:

$$\mathbf{y}(Z^{-1}) = \begin{bmatrix} 1 & -Z^{-1} \\ 1 & Z^{-1} \end{bmatrix} \cdot \mathbf{x}(Z^{-2}) \quad (139)$$

Ako  $\mathbf{x}(Z^{-1})$  ima opšti oblik:

$$\mathbf{x}(Z^{-1}) = \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}_{\mathbf{x}(Z^{-1})} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (140)$$

s omega vektorom  $[\Omega_0, \Omega_1, \dots, \Omega_{N-1}]$  onda  $\mathbf{x}(Z^{-2})$  ima opšti oblik:

$$\begin{aligned} \mathbf{x}(Z^{-2}) &= \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \mathcal{M}_{\mathbf{x}}(Z^{-2}) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned} \quad (141)$$

a s omega vektorom:  $[\Omega_0, 0, \Omega_1, 0, \dots, \Omega_{N-2}, 0, \Omega_{N-1}]$ . Komplementarni par  $\mathbf{y}(Z^{-1})$  ima oblik

$$\mathbf{y}(Z^{-1}) = \begin{bmatrix} 1 & Z^{-1} \\ 1 & -Z^{-1} \end{bmatrix} \cdot \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \mathbf{U}_{\Omega_0} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (142)$$

pa je njegov omega vektor:  $[\Omega_0, 0, \Omega_1, 0, \dots, 0, \Omega_{N-1}, -1]$ .

#### 5.7.4. Nadovezivanje blokova (block concatenation)

Golej takođe daje 2 algoritma koji od dva komplementarna para dužine M i N generišu par dužine 2MN. Polazimo od dva para komplementarnih sekvenci:

$$\begin{aligned} \mathbf{x}_{AB}(Z^{-1}) &= \left\{ \prod_{k=M}^1 \begin{bmatrix} 1 & -\Omega_k^{(AB)*} \\ \Omega_k^{(AB)} & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \mathbf{U}_{\Omega_0}^{(AB)} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}_{AB}(Z^{-1}) \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ \mathbf{x}_{CD}(Z^{-1}) &= \left\{ \prod_{k=N}^1 \begin{bmatrix} 1 & -\Omega_k^{(CD)*} \\ \Omega_k^{(CD)} & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \mathbf{U}_{\Omega_0}^{(CD)} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}_{CD}(Z^{-1}) \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned} \quad (143)$$

$$\begin{aligned} \mathcal{M}_{AB}(Z^{-1}) &= \begin{bmatrix} A(Z^{-1}) & -B^{*R}(Z^{-1}) \\ B(Z^{-1}) & A^{*R}(Z^{-1}) \end{bmatrix} \\ \mathcal{M}_{CD}(Z^{-1}) &= \begin{bmatrix} C(Z^{-1}) & -D^{*R}(Z^{-1}) \\ D(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} \end{aligned} \quad (144)$$

Iz [Parker 04] preuzimamo izraz za ovaj algoritam:

$$\mathbf{y}(Z^{-1}) = \begin{bmatrix} A(Z^{-N}) \cdot C(Z^{-1}) - B^R(Z^{-N}) \cdot D(Z^{-1}) \cdot Z^{-MN} \\ B(Z^{-N}) \cdot C(Z^{-1}) + A^R(Z^{-N}) \cdot D(Z^{-1}) \cdot Z^{-MN} \end{bmatrix} \quad (145)$$

Pokazaćemo da se generišuća matrica može napisati u obliku:

$$\begin{aligned}
 \mathcal{M}_y(Z^{-1}) &= \mathcal{M}_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-NM} \end{bmatrix} \cdot \mathcal{M}_{CD}(Z^{-1}) \\
 &= \begin{bmatrix} A(Z^{-N}) & -B^{*R}(Z^{-N}) \\ B(Z^{-N}) & A^{*R}(Z^{-N}) \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-NM} \end{bmatrix} \cdot \begin{bmatrix} C(Z^{-1}) & -D^{*R}(Z^{-1}) \\ D(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} \\
 &= \begin{bmatrix} A(Z^{-N}) & -B^{*R}(Z^{-N}) \cdot Z^{-NM} \\ B(Z^{-N}) & A^{*R}(Z^{-N}) \cdot Z^{-NM} \end{bmatrix} \cdot \begin{bmatrix} C(Z^{-1}) & -D^{*R}(Z^{-1}) \\ D(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} \\
 &= \begin{bmatrix} A(Z^{-N})C(Z^{-1}) - B^{*R}(Z^{-N})D(Z^{-1})Z^{-NM} & -A(Z^{-N})D^{*R}(Z^{-1}) - B^{*R}(Z^{-N})C^{*R}(Z^{-1})Z^{-NM} \\ B(Z^{-N})C(Z^{-1}) + A^{*R}(Z^{-N})D(Z^{-1})Z^{-NM} & -B(Z^{-N})D^{*R}(Z^{-1}) + A^{*R}(Z^{-N})C^{*R}(Z^{-1})Z^{-NM} \end{bmatrix}
 \end{aligned} \tag{146}$$

$$\mathbf{y}(Z^{-1}) = \mathcal{M}_y(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} A(Z^{-N})C(Z^{-1}) - B^{*R}(Z^{-N})D(Z^{-1})Z^{-NM} \\ B(Z^{-N})C(Z^{-1}) + A^{*R}(Z^{-N})D(Z^{-1})Z^{-NM} \end{bmatrix} \tag{147}$$

pa je omega vektor jednak:

$$\left[ \Omega_0^{(AB)}, \underbrace{0, \dots, 0}_{N-1}, \Omega_1^{(AB)}, \underbrace{0, \dots, 0}_{N-1}, \dots, \Omega_{M-1}^{(AB)}, \underbrace{0, \dots, 0}_{NM-1}, \Omega_0^{(CD)}, \Omega_1^{(CD)}, \dots, \Omega_{N-1}^{(CD)} \right]$$

### 5.7.5. Učešljanje blokova (block interleaving)

Ovaj algoritam je dat izrazom [Parker 04]:

$$\mathbf{y}(Z^{-1}) = \begin{bmatrix} A(Z^{-2N}) \cdot C(Z^{-2}) - B^R(Z^{-2N}) \cdot D(Z^{-2}) \cdot Z^{-1} \\ B(Z^{-2N}) \cdot C(Z^{-2}) + A^R(Z^{-2N}) \cdot D(Z^{-2}) \cdot Z^{-1} \end{bmatrix} \tag{148}$$

Na sličan način generišića matrica se dobija:

$$\begin{aligned}
 \mathcal{M}_y(Z^{-1}) &= \mathcal{M}_{AB}(Z^{-2N}) \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \mathcal{M}_{CD}(Z^{-2}) \\
 \mathcal{M}_y(Z^{-1}) &= \begin{bmatrix} A(Z^{-2N}) & -B^{*R}(Z^{-2N}) \\ B(Z^{-2N}) & A^{*R}(Z^{-2N}) \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} C(Z^{-2}) & -D^{*R}(Z^{-2}) \\ D(Z^{-2}) & C^{*R}(Z^{-2}) \end{bmatrix}
 \end{aligned} \tag{149}$$

pa je omega vektor jednak:

$$\left[ \Omega_0^{(AB)}, \underbrace{0, \dots, 0}_{2N-1}, \Omega_1^{(AB)}, \underbrace{0, \dots, 0}_{2N-1}, \dots, \Omega_{M-1}^{(AB)}, \Omega_0^{(CD)}, 0, \Omega_1^{(CD)}, 0, \dots, 0, \Omega_{N-1}^{(CD)} \right]$$

## 5.7.6. Turinov kompozitni algoritam za binarne sekvence

Turin [Turyn 63] je sačinio mnogo praktičniji i značajniji algoritam koji omogućava da se na osnovu dva komplementarna para generiše par dužine  $NM$ . Nažalost, taj algoritam se odnosi samo na binarne sekvence, tačnije  $[C D]$  par treba da bude binaran. Zahvaljujući Turinovom algoritmu moguće je konstruisati binarne sekvence dužine  $2^n 10^k 26^l$ . Kao ilustraciju značaja tog algoritma navodimo da se pomoću njega mogu konstruisati parovi dužine 100 dok Golejev algoritam ne dopušta tu mogućnost, naime, Golejev algoritam omogućava konstruisanje samo sekvenci dužine 200.

Iz [Parker 04] Turinov algoritam može da se napiše kao:

$$\begin{aligned} & \mathbf{y}(Z^{-1}) \\ &= \begin{bmatrix} A(Z^{-N}) \cdot \frac{C(Z^{-1}) + D(Z^{-1})}{2} + Z^{-N(M-1)} \cdot B(Z) \cdot \frac{C(Z^{-1}) - D(Z^{-1})}{2} \\ B(Z^{-N}) \cdot \frac{C(Z^{-1}) + D(Z^{-1})}{2} - Z^{-N(M-1)} \cdot A(Z) \cdot \frac{C(Z^{-1}) - D(Z^{-1})}{2} \end{bmatrix} \end{aligned} \quad (150)$$

$$\begin{aligned} & \mathbf{y}(Z^{-1}) \\ &= \begin{bmatrix} A(Z^{-N}) \cdot \frac{C(Z^{-1}) + D(Z^{-1})}{2} + Z^{-MN} \cdot B^R(Z) \cdot \frac{C(Z^{-1}) - D(Z^{-1})}{2} \\ B(Z^{-N}) \cdot \frac{C(Z^{-1}) + D(Z^{-1})}{2} - Z^{-MN} \cdot A^R(Z) \cdot \frac{C(Z^{-1}) - D(Z^{-1})}{2} \end{bmatrix} \end{aligned} \quad (151)$$

Na sličan način generišića matrica se dobija:

$$\begin{aligned} & \mathcal{M}_{\mathbf{y}}(Z^{-1}) = \mathcal{M}_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} \cdot \mathcal{M}_{CD}(Z^{-1}) \\ & \mathcal{M}_{\mathbf{y}}(Z^{-1}) = \frac{1}{2} \begin{bmatrix} A(Z^{-N}) & -B^{*R}(Z^{-N}) \\ B(Z^{-N}) & A^{*R}(Z^{-N}) \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} C(Z^{-1}) & -D^{*R}(Z^{-1}) \\ D(Z^{-1}) & C^{*R}(Z^{-1}) \end{bmatrix} \end{aligned} \quad (152)$$

Jednostavniji izraz se dobija kada se genrišuće matrice napišu kao:

$$\begin{aligned} & \mathcal{M}_{AB}(Z^{-N}) = \mathcal{M}'_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \\ & \mathcal{M}_{CD}(Z^{-1}) = \mathcal{M}'_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \end{aligned} \quad (153)$$

Tada komplementarni par ima oblik:

$$\begin{aligned} & \mathbf{y}(Z^{-1}) = \mathcal{M}'_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} \cdot \mathcal{M}'_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ & = \mathcal{M}'_{AB}(Z^{-N}) \cdot \mathcal{M}'_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned} \quad (154)$$

Zato što:  $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix} = I$  i  $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ . Ostaje još da se odrede matrice  $\mathcal{M}'_{AB}(Z^{-N})$  i  $\mathcal{M}'_{CD}(Z^{-N})$ . Iz (153) dobijamo:

$$\begin{aligned} \mathcal{M}'_{AB}(Z^{-N}) &= \mathcal{M}_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{-1} = \frac{1}{2} \cdot \mathcal{M}_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \\ \mathcal{M}'_{CD}(Z^{-1}) &= \mathcal{M}_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{-1} = \frac{1}{2} \cdot \mathcal{M}_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \end{aligned} \quad (155)$$

Veoma je značajno kako se predstavljaju početne sekvence:

$$\begin{aligned} \mathbf{y}_{AB}(Z^{-1}) &= \mathcal{M}_{AB}(Z^{-N}) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}'_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}'_{AB}(Z^{-N}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ \mathbf{y}_{CD}(Z^{-1}) &= \mathcal{M}_{CD}(Z^{-1}) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}'_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathcal{M}'_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned} \quad (156)$$

Možemo prepoznati da je ovo generišuća formula iz [Budišin 90B] data jednačinom (79) pa ćemo generišuće matrice  $\mathcal{M}'_{AB}$  i  $\mathcal{M}'_{CD}(Z^{-1})$  zvati „binarne generišuće matrice“ da bi ih razlikovali od standardnih generišućih matrica.

Turinov algoritam je izuzetno značajan zato što se može veoma jednostavno primeniti na proizvoljan broj komplementarnih parova. Samo se dodaju nove matrice u gornji proizvod. Ovo ćemo ilustrovati primerom s 3 komplementarna para. Taj primer je osnova za konstruisanje binarnih sekvenci dužine  $2^k \cdot 10^m \cdot 26^n$ . Svakako treba imati u vidu da će u ovom slučaju proizvod imati  $k + m + n$  članova.

$$\mathbf{y}(Z^{-1}) = \mathcal{M}'_{AB}(Z^{-NM}) \cdot \mathcal{M}'_{CD}(Z^{-N}) \cdot \mathcal{M}'_{EF}(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (157)$$

#### PRIMER

Neka je  $\mathcal{M}_{AB}(Z^{-N}) = \mathcal{M}_{CD}(Z^{-1}) = \begin{bmatrix} 1 + Z^{-1} & -1 + Z^{-1} \\ 1 - Z^{-1} & 1 + Z^{-1} \end{bmatrix}$ . Tada je:

$$\begin{aligned} \mathcal{M}_y(Z^{-1}) &= \frac{1}{2} \cdot \begin{bmatrix} 1 + Z^{-2} & -1 + Z^{-2} \\ 1 - Z^{-2} & 1 + Z^{-2} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 + Z^{-1} & -1 + Z^{-1} \\ 1 - Z^{-1} & 1 + Z^{-1} \end{bmatrix} \\ &= \begin{bmatrix} 1 & Z^{-2} \\ -Z^{-2} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 + Z^{-1} & -1 + Z^{-1} \\ 1 - Z^{-1} & 1 + Z^{-1} \end{bmatrix} \\ &= \begin{bmatrix} 1 + Z^{-1} + Z^{-2} - Z^{-3} & -1 + Z^{-1} + Z^{-2} + Z^{-3} \\ 1 - Z^{-1} - Z^{-2} - Z^{-3} & 1 + Z^{-1} + Z^{-2} - Z^{-3} \end{bmatrix} \\ \mathbf{y}(Z^{-1}) &= \mathcal{M}_y(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 + Z^{-1} + Z^{-2} - Z^{-3} \\ 1 - Z^{-1} - Z^{-2} - Z^{-3} \end{bmatrix} \end{aligned}$$

što daje komplementarni par sekvenci  $[1 \ 1 \ 1 \ -1]$  i  $[1 \ -1 \ -1 \ -1]$ . Isti rezultat možemo dobiti koristeći binarne generišuće matrice:

$$\mathcal{M}'_{AB}(Z^{-N}) = \frac{1}{2} \cdot \begin{bmatrix} 1 + Z^{-1} & -1 + Z^{-1} \\ 1 - Z^{-1} & 1 + Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & Z^{-1} \\ -Z^{-1} & 1 \end{bmatrix}$$

Pa je prema (154):

$$\begin{aligned}
 \mathbf{y}(Z^{-1}) &= \mathcal{M}'_{AB}(Z^{-2}) \cdot \mathcal{M}'_{CD}(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & Z^{-2} \\ -Z^{-2} & 1 \end{bmatrix} \begin{bmatrix} 1 & Z^{-1} \\ -Z^{-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\
 &= \begin{bmatrix} 1 - Z^{-3} & Z^{-1} + Z^{-2} \\ -Z^{-1} - Z^{-2} & 1 - Z^{-3} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 - Z^{-3} + Z^{-1} + Z^{-2} \\ -Z^{-1} - Z^{-2} + 1 - Z^{-3} \end{bmatrix} \\
 &= \begin{bmatrix} 1 + Z^{-1} + Z^{-2} - Z^{-3} \\ 1 - Z^{-1} - Z^{-2} - Z^{-3} \end{bmatrix}
 \end{aligned}$$

Što je isti rezultat koji smo predhodno dobili.

Valja još primetiti da se binarna generišuća matrica  $\mathcal{M}'_y(Z^{-1}) = \mathcal{M}'_{AB}(Z^{-2}) \cdot \mathcal{M}'_{CD}(Z^{-1})$  može koristiti i kao standardna generišuća matrica ali ona tada ne generiše binarne nego ternarne sekvence!

### 5.7.7. Fazni pomak jedne od dve sekvence u paru

Neka je nova generišuća matrica prikazana:

$$\mathcal{M}_y(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \mathcal{M}_x(Z^{-1}) \quad (158)$$

gde je  $|w| = 1$ . Ako pođemo od kanonične forme:

$$\mathcal{M}_x(Z^{-1}) = \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \quad (159)$$

dobijamo:

$$\begin{aligned}
 \mathcal{M}_y(Z^{-1}) &= \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -\Omega_k^* \\ \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \\
 &= \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-1}^* \\ \Omega_{N-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-2}^* \\ \Omega_{N-2} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \dots \\
 &\quad \cdot \begin{bmatrix} 1 & -\Omega_1^* \\ \Omega_1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \quad (160) \\
 &= \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-1}^* \\ \Omega_{N-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-2}^* \\ \Omega_{N-2} & 1 \end{bmatrix} \\
 &\quad \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & -\Omega_1^* \\ \Omega_1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \\
 &\quad \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \quad (161)
 \end{aligned}$$

$$\begin{aligned}
 &= \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-1}^* \\ \Omega_{N-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_{N-2}^* \\ \Omega_{N-2} & 1 \end{bmatrix} \\
 &\quad \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \dots \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_1^* \\ \Omega_1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \\
 &\quad \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 & -\Omega_0^* \\ \Omega_0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w^* \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix}
 \end{aligned} \tag{162}$$

$$\begin{aligned}
 &= \begin{bmatrix} 1 & -w^* \cdot \Omega_{N-1}^* \\ w \cdot \Omega_{N-1} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -w^* \cdot \Omega_{N-2}^* \\ w \cdot \Omega_{N-2} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \dots \\
 &\quad \cdot \begin{bmatrix} 1 & -w^* \cdot \Omega_1^* \\ w \cdot \Omega_1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -w^* \cdot \Omega_0^* \\ w \cdot \Omega_0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix}
 \end{aligned} \tag{163}$$

$$= \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -w^* \cdot \Omega_k^* \\ w \cdot \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -w^* \cdot \Omega_0^* \\ w \cdot \Omega_0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \tag{164}$$

Znači, dobili smo omega vektor jednak:

$$[w\Omega_0, w\Omega_1, \dots, w\Omega_{N-2}, w\Omega_{N-1}]$$

Kada računamo komplementarni par:

$$\begin{aligned}
 &\mathbf{y}(Z^{-1}) = \mathcal{M}_y(Z^{-1}) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \\
 &= \left\{ \prod_{k=N-1}^1 \begin{bmatrix} 1 & -w^* \cdot \Omega_k^* \\ w \cdot \Omega_k & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 & -w^* \cdot \Omega_0^* \\ w \cdot \Omega_0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}
 \end{aligned} \tag{165}$$

poslednja matrica  $\begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix}$  nestaje pošto je:  $\begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ .

### 5.7.8. Frekvencijski pomak obe sekvence

Ukoliko obe sekvence frekvencijski pomerimo za  $\omega$  na sledeći način:

$$\begin{aligned}
 a'(n) &= a(n) \cdot e^{i\omega n} \\
 b'(n) &= b(n) \cdot e^{i\omega n}
 \end{aligned} \tag{166}$$

čime se ne narušava komplementarnost, novi par ima omega vektor jednak:

$$[\Omega_0, \Omega_1 e^{i\omega}, \Omega_2 e^{i2\omega}, \dots, \Omega_{N-2} e^{i(N-2)\omega}, \Omega_{N-1} e^{i(N-1)\omega}]$$

## 5.8. Efikasnost generatora-korelatora

Prvi efikasni generator-korelator za binarne i polifazne komplementarne sekvence prikazan je u [Budišin 92]. Kako on ima  $N$  faktora u kompaktnoj kanoničnoj reprezentaciji a  $2^N$  faktora u standardnoj kanoničnoj formi, stepen efikasnosti možemo definisati kao odnos ta dva broja. Stepen kompaktnosti kompaktno kanonične forme bio bi definisan kao broj faktora u kompaktnoj formi podeljen s dužinom sekvence. Stepen efikasnosti bio bi definisan kao recipročna vrednost stepena kompaktnosti. Na primer, za efikasni korelator iz [Budišin 92] stepen efikasnosti bio bi  $2^N/N$  dok je kompaktnost data s  $N/2^N$ .

Generalno, efikasnost bilo kog para sekvenci definiše se kao odnos broja faktora u kanoničnoj formi i broja faktora u kompaktnoj kanoničnoj formi. Na osnovu ranije korišćenih oznaka varijabli efikasnost je:

$$\varepsilon = \frac{N}{m} \tag{167}$$

## 6. Primeri

Primere smo podelili prema korišćenim modulacijama u digitalnim komunikacionim sistemima na: BPSK, M-PSK i QAM. Svim ovim tipovima sekvenci zajednička je odlika to što je za svaku poznat takozvani standardni algoritam za koji se očekivalo da će generisati sve komplementarne parove dužine  $2^N$ . U stvari, tako se mislilo do pojave rada [Li 05] u kome je, za 4-PSK sekvence dužine 16, pokazano da postoje sekvence koje se ne mogu dobiti standardnim algoritmom. Takve sekvence su dobijene sistematskim računarskim pretraživanjem i nazivaju se nestandardne komplementarne sekvence. Do sada su pronađene i publikovane 4-PSK, 6-PSK i 16-QAM nestandardne komplementarne sekvence. Samo za binarne sekvence danas nisu poznate nestandardne sekvence.

Pored standardnih i nestandardnih sekvenci, koje su dužine  $2^N$ , postoje i sekvence drugih dužina koje se ne mogu konstruisati nekom rekurzivnom metodom iz kraćih sekvenci. Takve sekvence nazivamo kerneli (kernels). One su dobijene računarskim pretraživanjem. Kerneli nisu značajni samo po tome što je dokazano da postoje nego i po tome što se pomoću njih mogu konstruisati komplementarni parovi različitih kompozitnih dužina. Tako za binarne sekvence, koristeći Turinov algoritam, mogu da se konstruišu sekvence dužine  $2^N 10^M 26^L$ . Za ostale sekvence, pomoću Golejevog algoritma za konstruisanje sekvenci kompozitnih dužina, moguće je konstruisati sekvence dužine  $2 \cdot N \cdot M$  iz kernela dužine  $N$  i  $M$ . Ovaj algoritam može se još jednom ponoviti da se konstruišu sekvence dužine  $4 \cdot N \cdot M \cdot L$  iz 3 kernela dužina  $N$ ,  $M$  i  $L$  itd.

### 6.1. Binarne sekvence

U slučaju binarnih sekvenci standardne sekvence se mogu dobiti Golejevom direktnom metodom ili pomoću [Budišin 90A] kad se uzme da su  $W$  koeficijenti  $\pm 1$ .

Takvih sekvenci ima  $N! \cdot 2^N$ . Kerneli postoje za dužinu 10 (2 para) i 26 (1 par). Pored toga, pomoću rekurzivnih algoritama mogu se dobiti sekvence dužine 20 iz kernela dužine 10. Međutim, pokazalo se da postoje parovi sekvenci dužine 20 koji se ne mogu dobiti na ovaj način. Oni se isto smatraju kernelima. Pronađen je jedan kernel dužine 20.

### 6.1.1. Standardne

Kako se standardne binarne komplementarne sekvence po algoritmu [Budišin 90A] već generišu pomoću paraunitarne generišuće matrice, ovde nije potrebno posebno dokazivati da se može izvršiti dekompozicija na N faktora. Zato ćemo samo ilustrovati proces dekompozicije na jednoj standardnoj binarnoj sekvenci. Treba uočiti da je matrica korišćena u [Budišin 90A] različita od omega matrice. Međutim ta razlika je minorna i u proizvodu koji odgovara kanoničnoj formi može se jedna matrica transformisati u drugu.

Binarni par sekvenci iz [Golay 61]:

$$a = [+1, +1, +1, +1, +1, -1, -1, +1]$$

$$b = [+1, -1, +1, -1, +1, +1, -1, -1]$$

Dekompozicija izgleda ovako:

$$\mathbf{X}_8(Z^{-1}) = \begin{bmatrix} 1+Z^{-1}+Z^{-2}+Z^{-3}+Z^{-4} - Z^{-5}-Z^{-6}+Z^{-7} \\ 1-Z^{-1}+Z^{-2}-Z^{-3}+Z^{-4} + Z^{-5}-Z^{-6}-Z^{-7} \end{bmatrix}; \Omega_7 = -\frac{a_8(7)}{b_8(7)} = 1$$

$$\mathbf{X}_7(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \mathbf{X}_8 = 2 \begin{bmatrix} 1+Z^{-2}+Z^{-4}-Z^{-6} \\ -1-Z^{-2}+Z^{-4}-Z^{-6} \end{bmatrix}, \Omega_6 = -1;$$

$$\mathbf{X}_6(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \mathbf{X}_7 = 4 \begin{bmatrix} 1+Z^{-2} \\ Z^{-3}-Z^{-5} \end{bmatrix}; \Omega_5 = 0;$$

$$\mathbf{X}_5(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \mathbf{X}_6 = 4 \begin{bmatrix} 1+Z^{-2} \\ Z^{-2}-Z^{-4} \end{bmatrix}; \Omega_4 = 0;$$

$$\mathbf{X}_4(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \mathbf{X}_5 = 4 \begin{bmatrix} 1+Z^{-2} \\ Z^{-1}-Z^{-3} \end{bmatrix}; \Omega_3 = 0;$$

$$\mathbf{X}_3(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \mathbf{X}_4 = 4 \begin{bmatrix} 1+Z^{-2} \\ 1-Z^{-2} \end{bmatrix}; \Omega_2 = 1;$$

$$\mathbf{X}_2(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \mathbf{X}_3 = 8 \begin{bmatrix} 1 \\ -Z^{-1} \end{bmatrix}; \Omega_1 = 0;$$

$$\mathbf{X}_1(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \mathbf{X}_2 = 8 \begin{bmatrix} 1 \\ -1 \end{bmatrix}; \Omega_0 = 1;$$

$$\mathbf{X}_0(Z^{-1}) = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \mathbf{X}_1 = 16 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Omega vektor  $[\Omega_0, \Omega_2, \dots, \Omega_7] = [1, 0, 1, 0, 0, 0, -1, 1]$  je redak, kanonična forma izgleda ovako:

$$X_{10} = U_1 \cdot D \cdot U_{-1} \cdot D \cdot U_0 \cdot D \cdot U_0 \cdot D \cdot U_0 \cdot D \cdot U_1 \cdot D \cdot U_0 \cdot D \cdot U_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Kompaktna kanonična forma je:

$$X_{10} = U_1 \cdot D^1 \cdot U_{-1} \cdot D^4 \cdot U_1 \cdot D^2 \cdot U_{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$X_{10} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-4} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-2} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$X_{10} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-4} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-2} \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Prepoznaje se da je to kompaktna kanonična forma s parametrima:

$$[P(1), P(2), P(3)] = [2, 4, 1] \text{ i } [S(1), S(2), S(3)] = [3, 7, 8]$$

## 6.1.2. Nestandardne

Do danas jos nisu pronađene nestandardne binarne sekvence. Kako su one pronađene u 4-PSK, 6-PSK i 16-QAM familijama logično je očekivati da postoje i u binarnoj verziji. Ovo je jedno od nerešenih pitanja u teoriji komplementarnih sekvenci. Postoje dva načina pretraživanja koja bi mogla dovesti do pronalaženja nestandardnih binarnih sekvenci:

Sistematsko pretraživanje svih binarnih sekvenci i provera da li svi pronađeni komplementarni parovi pripadaju familiji standardnih sekvenci. Ovaj pristup ne može dati rezultate za sekvence mnogo duže od 32, bez obzira na to što su računari sve moćniji, pošto broj slučajeva koje treba pretražiti raste kao  $2^{2^N}$ .

Drugi pristup je pretraživanje standardnih komplementarnih sekvenci i pronalaženje ukrštenih autokorelacionih funkcija. Drugim rečima, valja naći dva komplementarna para sa istim autokorelacionim funkcijama. Broj komplementarnih sekvenci koje treba pretražiti raste sa  $N! 2^N$ , pa je ovaj pristup mnogo brži od prethodnog pristupa.

## 6.1.3. Kerneli

### 6.1.3.1. Kernel 10

Golej je u svom radu [Golay 61] dao dva kernela dužine 10. Prvi Golejev kernel dužine 10 je:

$$a_1 = [+1, -1, -1, +1, +1, +1, +1, +1, +1, -1]$$

$$b_1 = [+1, -1, -1, -1, +1, -1, +1, -1, -1, +1]$$

Drugi Golejev par dužine 10 je:

$$a_1 = [+1, -1, +1, -1, +1, +1, +1, +1, -1, -1]$$

$$b_1 = [+1, +1, +1, +1, -1, +1, +1, -1, -1, +1]$$

Ovako se dekomponuje prvi par:

$$X_{10}(Z^{-1}) = \begin{bmatrix} 1-Z^{-1}-Z^{-2}+Z^{-3}+Z^{-4}+Z^{-5}+Z^{-6}+Z^{-7}+Z^{-8}-Z^{-9} \\ 1-Z^{-1}-Z^{-2}-Z^{-3}+Z^{-4}-Z^{-5}+Z^{-6}-Z^{-7}-Z^{-8}+Z^{-9} \end{bmatrix}; \Omega_9 = \frac{b_0(9)}{a_0(9)} = 1$$

$$X_9 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot X_{10} = 2 \begin{bmatrix} 1-Z^{-1}-Z^{-2}+Z^{-4}+Z^{-6} \\ -Z^{-2}-Z^{-4}-Z^{-6}-Z^{-7}+Z^{-8} \end{bmatrix}, \Omega_8 = 0;$$

$$X_8 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot X_9 = 2 \begin{bmatrix} 1-Z^{-1}-Z^{-2}+Z^{-4}+Z^{-6} \\ -Z^{-1}-Z^{-3}-Z^{-5}-Z^{-6}+Z^{-7} \end{bmatrix}, \Omega_7 = 0;$$

$$X_7 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot X_8 = 2 \begin{bmatrix} 1-Z^{-1}-Z^{-2}+Z^{-4}+Z^{-6} \\ -1-Z^{-2}-Z^{-4}-Z^{-5}+Z^{-6} \end{bmatrix}, \Omega_6 = -1$$

$$X_6 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot X_7 = 2 \begin{bmatrix} 2-Z^{-1}+2Z^{-4}+Z^{-5} \\ -1-2Z^{-1}-Z^{-4}+2Z^{-5} \end{bmatrix}; \Omega_5 = -0.5$$

$$X_5 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -0.5 \\ 0.5 & 1 \end{bmatrix} \cdot X_6 = \begin{bmatrix} 5+5Z^{-4} \\ -5+5Z^{-4} \end{bmatrix}; \Omega_4 = -1$$

$$X_4 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot X_5 = \begin{bmatrix} 10 \\ 10Z^{-3} \end{bmatrix}; \Omega_3 = 0;$$

$$X_3 = X_4 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot X_5 = \begin{bmatrix} 10 \\ 10Z^{-3} \end{bmatrix}; \Omega_2 = 0$$

$$X_2 = X_3 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot X_5 = \begin{bmatrix} 10 \\ 10Z^{-3} \end{bmatrix}; \Omega_1 = 0$$

$$X_1 = X_2 = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot X_5 = \begin{bmatrix} 10 \\ 10Z^{-3} \end{bmatrix}; \Omega_0 = 1;$$

$$X_0 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot X_1 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 10 \end{bmatrix} = 20 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Omega vektor je:

$$[\Omega_1, \Omega_2, \dots, \Omega_{10}] = [1, 0, 0, 0, -1, -0.5, -1, 0, 0, 1]$$

a kanonična forma izgleda ovako:

$$X_{10} = U_1 \cdot D \cdot U_0 \cdot D \cdot U_0 \cdot D \cdot U_{-1} \cdot D \cdot U_{-0.5} \cdot D \cdot U_{-1} \cdot D \cdot U_0 \cdot D \cdot U_0 \cdot D \cdot U_0 \cdot D \cdot U_1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$X_{10} = U_1 \cdot D \cdot I \cdot D \cdot I \cdot D \cdot U_{-1} \cdot D \cdot U_{-0.5} \cdot D \cdot U_{-1} \cdot D \cdot I \cdot D \cdot I \cdot D \cdot I \cdot D \cdot U_1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$X_{10} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \\ \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0.5 \\ -0.5 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$\mathbf{X}_{10} = \begin{bmatrix} 1 & -Z^{-1} \\ 1 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & Z^{-1} \\ -1 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0.5Z^{-1} \\ -0.5 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & Z^{-1} \\ -1 & Z^{-1} \end{bmatrix} \\ \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Kompaktna kanonična forma je:

$$\mathbf{X}_{10} = \mathbf{U}_1 \cdot \mathbf{D}^3 \cdot \mathbf{U}_{-1} \cdot \mathbf{D} \cdot \mathbf{U}_{-0.5} \cdot \mathbf{D} \cdot \mathbf{U}_{-1} \cdot \mathbf{D}^4 \cdot \mathbf{U}_1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \\ = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-3} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0.5 \\ -0.5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-4} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \\ \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\mathbf{X}_{10} = \begin{bmatrix} 1 & -Z^{-3} \\ 1 & Z^{-3} \end{bmatrix} \begin{bmatrix} 1 & Z^{-1} \\ -1 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0.5Z^{-1} \\ -0.5 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & Z^{-4} \\ -1 & Z^{-4} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\mathbf{X}_{10} = \begin{bmatrix} 1 & -Z^{-3} \\ 1 & Z^{-3} \end{bmatrix} \begin{bmatrix} 1 & Z^{-1} \\ -1 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0.5Z^{-1} \\ -0.5 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & Z^{-4} \\ -1 & Z^{-4} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Alternativno, ovaj izraz se može napisati u obliku:

$$\mathbf{X}_{10} = \begin{bmatrix} 1 & Z^{-3} \\ 1 & -Z^{-3} \end{bmatrix} \cdot \begin{bmatrix} 1 & -Z^{-1} \\ 1 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & -0.5 \cdot Z^{-1} \\ 0.5 & Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & Z^{-4} \\ 1 & -Z^{-4} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (168)$$

koji je u skladu s notacijom korišćenom u [Budišin 90A] i [Budišin 11]

Pogledamo li 4 individualne matrice u proizvodu uočavamo da su prva, druga i četvrta matrica istog oblika kao matrice koje se koriste u [Budišin 90A] dok se samo treća matrica razlikuje. Međutim, ona je specifična samo po tome što sadrži koeficijent 0,5 koji se u digitalnoj implementaciji u aritmetici s fiksnim zarezom može ostvariti prostim pomeranjem bita za jedno mesto udesno; kako pri tome nisu neophodna dodatna logična kola, ne povećava se cena elektronskog kola. Proces generisanja komplementarnog para dužine 10 prikazan je u Tab. 8.

Tab. 8. Proces generisanja komplementarnog para dužine 10 (prvi kernel)

**Inicijalne sekvence:**  $a = [1], b = [1]$

$a$ sekvenca:	1	0	0	0	0	0	0	0	0	0
$b$ sekvenca:	1	0	0	0	0	0	0	0	0	0
pomerana $b$ sekvenca	0	0	0	0	1	0	0	0	0	0

**1. rekurzija:**  $A'(Z^{-1}) = A(Z^{-1}) + B(Z^{-1})Z^{-4}, B'(Z^{-1}) = A(Z^{-1}) - B(Z^{-1})Z^{-4}$

$a$ sekvenca:	1	0	0	0	1	0	0	0	0	0
$b$ sekvenca:	1	0	0	0	-1	0	0	0	0	0
pomerana $b$ sekvenca	0	1	0	0	0	-1	0	0	0	0

**2. rekurzija:**  $A'(Z^{-1}) = A(Z^{-1}) - 0,5B(Z^{-1})Z^{-1}, B'(Z^{-1}) = 0,5A(Z^{-1}) + B(Z^{-1})Z^{-1}$

$a$ sekvenca:	1	-0,5	0	0	1	0,5	0	0	0	0
$b$ sekvenca:	0,5	1	0	0	0,5	-1	0	0	0	0
pomerana $b$ sekvenca	0	0,5	1	0	0	0,5	-1	0	0	0

**3. rekurzija:**  $A'(Z^{-1}) = A(Z^{-1}) - B(Z^{-1})Z^{-1}, B'(Z^{-1}) = A(Z^{-1}) + B(Z^{-1})Z^{-1}$

$a$ sekvenca:	1	-1	-1	0	1	0	1	0	0	0
$b$ sekvenca:	1	0	1	0	1	1	-1	0	0	0
pomerana $b$ sekvenca	0	0	0	1	0	1	0	1	1	-1

**4. rekurzija:**  $A'(Z^{-1}) = A(Z^{-1}) + B(Z^{-1})Z^{-3}, B'(Z^{-1}) = A(Z^{-1}) - B(Z^{-1})Z^{-3}$

$a$ sekvenca:	1	-1	-1	1	1	1	1	1	1	-1
$b$ sekvenca:	1	-1	-1	-1	1	-1	1	-1	-1	1

Drugi kernel Golejevih sekvenci dužine 10 [Golay 61] može se prikazati na sličan način:

$$X'_{10} = \begin{bmatrix} 1 & Z^{-1} \\ 1 & -Z^{-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & Z^{-3} \\ 1 & -Z^{-3} \end{bmatrix} \cdot \begin{bmatrix} 1 & -0,5 \cdot Z^{-3} \\ 0,5 & Z^{-3} \end{bmatrix} \cdot \begin{bmatrix} 1 & Z^{-2} \\ 1 & -Z^{-2} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (169)$$

### 6.1.3.2. Kernel 20

$$a_{20} = [+1; +1; +1; +1; -1; +1; -1; -1; -1; +1; +1; -1; -1; +1; +1; -1; +1; -1; -1; +1]$$

$$b_{20} = [+1; +1; +1; +1; -1; +1; +1; +1; +1; +1; -1; -1; -1; +1; -1; +1; -1; +1; +1; -1]$$

Njegov omega vektor je:

$$[-1, 0, 0, 0, 0, 0, -1, 0, 0, 1/2, -2/5, 8/29, -3/181, 25/113, -10/37, 4/13, 1/5, -1/2, -1, 1]$$

Vidi se da u omega vektoru ima samo 7 nultih elemenata pa je efikasnost  $13/20 = 0,65$ . To je veoma loš odnos, naročito kada se poredi sa standardnim binarnim sekvencama dužine 16 i 32 kod kojih je taj odnos  $4/16 = 0,25$  i  $5/32 \sim 0,16$ . Situacija se posebno pogoršava pošto su omega koeficijenti složenog izgleda. Stoga je praktična implementacija veoma složena pošto postaju neophodni množači.

### 6.1.3.3. Kernel 26

$$a_{26} = [1; 1; 1; 1; -1; 1; 1; -1; -1; 1; -1; 1; -1; 1; -1; -1; 1; -1; 1; 1; 1; -1; -1; 1; 1; 1]$$

$$b_{26} = [1; 1; 1; 1; -1; 1; 1; -1; -1; 1; -1; 1; 1; 1; 1; -1; 1; -1; -1; -1; 1; 1; -1; -1; -1]$$

Omega vektor je:

$$[-1, 0, 0, +1, +1/2, -1/5, -4/13, -3/37, +81/106, +3/37, -4/13, +1/5, +1/2, +1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1]$$

On ima samo 13 nultih elemenata pa je efikasnost samo 2.

Takođe treba uočiti neobičnu simetriju-antisimetriju u omega vektoru od elementa 3 do elementa 13. Znači, imamo:

$$[+1, +1/2, -1/5, -4/13, -3/37, +81/106, +3/37, -4/13, +1/5, +1/2, +1]$$

Kada napišemo niz znakova koji govore koji elementi su simetrični a koji antisimetrični, počevši od prvog i poslednjeg pa idući ka sredini dobijamo: [+ , + , - , + , -]. Pri tome nismo uzeli u obzir centralni element veličine +81/106 koji je sam sebi simetričan.

## 6.2. PSK sekvence

Broj faza u M-PSK konstelaciji u principu može biti proizvoljan, međutim, zbog popularnosti QAM modulacija danas je najznačajnija četvorofazna familija (4-PSK). Treba istaći da se ta modulacija često naziva QPSK modulacija ili 4-QAM modulacija. Zato ćemo mi isključivo njih posmatrati.

### 6.2.1. Standardne

Standardne polifazne sekvence su prvi put opisane rekursivnim algoritmom [Budišin 90A]. U tom algoritmu skup mogućih faza nije diskretizovan nego može da uzme bilo koje vrednosti iz skupa  $[0, 2\pi)$ . Kasnije [Davis 99] daje nerekursivni algoritam za specijalan slučaj kada su faze koreni jedinice što odgovara M-PSK konstelaciji.

Kako smo već objasnili kad smo govorili o standardnim binarnim sekvencama koje se generišu pomoću algoritma iz [Budišin 90A], generator tih sekvenci je u obliku paraunitarnih matrica pa se ovde nećemo posebno baviti njime.

Daćemo samo jedan primer 4-faznih sekvenci dužine 16 da bi nam poslužio kao primer za poređenje sa primerom u sledećem odeljku koji se odnosi na nestandardne 4-fazne sekvence dužine 16.

$$a_{16} = [1; -i; 1; i; 1; -i; 1; i; i; 1; -i; 1; i; -1; i; 1]$$

$$b_{16} = [1; i; 1; -i; 1; i; 1; -i; i; -1; i; -1; -i; 1; i; 1]$$

Njegov omega vektor je:

$$[-1; 0; 0; 0; 1; 0; 0; 0; 0; 0; 0; 0; 0; i; 0; -i; -1]$$

Treba uočiti da postoji samo 6 nenulatih vrednosti i da su sve nenulte vrednosti po modulu jednake, a to znači da je za ovaj par moguće realizovati efikasan korelator što je potvrda od ranije poznate činjenice.

## 6.2.2. Nestandardne

Prve nestandardne 4-PSK sekvence dužine 16 navedene su u radu [Li 05]. U tom radu su navedene 1024 sekvence koje se ne mogu dobiti standardnom konstrukcijom. Jedan primer takvih sekvenci je:

$$a_{16} = [1; 1; 1; i; -i; -1; -i; i; 1; -1; -1; -i; i; -1; -i; i]$$

$$b_{16} = [1; -1; 1; -i; -i; 1; -i; -i; 1; 1; -1; i; i; 1; -i; -i]$$

Njihov omega vektor je:

$$[i; 0; -1/2-i/2; 0; 1/3; 0; -2/5-i/5; 0; -1/5+2i/5; 0; i/3; 0; -1/2+i/2; 0; 1; -1]$$

Zapažamo da je broj nenulatih vrednosti 9; kod standardnih polifaznih sekvenci njihov je 5. Takođe vidimo da veliki broj nenulatih elemenata ima vrednosti čiji modul nije 1.

Na osnovu ovoga možemo zaključiti da za ovakve parove sekvenci kompaktna kanonična forma ne daje efikasan korelator.

## 6.2.3. Kerneli

Prvo vidimo da za binarne sekvence svi kerneli imaju parne dužine. Međutim, za kvaternarne sekvence postoje kerneli dužine 3, 5, 11 i 13. I dalje ne postoje kerneli dužine 7 i 9. Treba naglasiti da se kernel 9 ne može dobiti Turinovim algoritmom  $3 \times 3$

pošto kerneli dužine 3 nisu binarni a Turinov algoritam se primenjuje samo na binarne sekvence.

U radu [Gibson 11] data su ova 4 kvaternarna kernela:

### 6.2.3.1. Kernel 3

$$a_3 = [+1; +1; -1]$$

$$b_3 = [+1; +i; +1]$$

Evo kako se dekomponuje ovaj kernel:

$$X_3(Z^{-1}) = \begin{bmatrix} 1 + Z^{-1} - Z^{-2} \\ 1 + i \cdot Z^{-1} + Z^{-2} \end{bmatrix}, \Omega_2 = -\frac{a_3(2)}{b_3(2)} = 1$$

$$X_2(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 + Z^{-1} - Z^{-2} \\ 1 + i \cdot Z^{-1} + Z^{-2} \end{bmatrix} = \begin{bmatrix} 2 + (1+i) \cdot Z^{-1} \\ (i-1) + 2 \cdot Z^{-1} \end{bmatrix}, \Omega_1 = -\frac{a_2(1)}{b_2(1)} = -\frac{1+i}{2}$$

$$X_1(Z^{-1}) = \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -(1+i)/2 \\ (1-i)/2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 + (1+i) \cdot Z^{-1} \\ (i-1) + 2 \cdot Z^{-1} \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix}, \Omega_0 = -\frac{a_1(0)}{b_1(0)} = \frac{3}{3} = 1$$

$$X_0(Z^{-1}) = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix} = 6 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Omega vektor je:

$$[\Omega_0, \Omega_1, \Omega_2] = [1, -\frac{1+i}{2}, 1]$$

a kompletna dekompozicija izgleda ovako:

$$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & -(1+i)/2 \\ (1-i)/2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 + Z^{-1} - Z^{-2} \\ 1 + i \cdot Z^{-1} + Z^{-2} \end{bmatrix} = 6 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Kanonična forma, koja je istovremeno i kompaktna kanonična forma, jeste:

$$X_3(Z^{-1}) = \begin{bmatrix} 1 + Z^{-1} - Z^{-2} \\ 1 + i \cdot Z^{-1} + Z^{-2} \end{bmatrix} = \begin{bmatrix} 1 & -Z^{-1} \\ 1 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & (1+i)Z^{-1}/2 \\ -(1-i)/2 & Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Vidimo da je efikasnost ovog kernela jednaka 1 što znači da se ne može očekivati nikakvo povećanje efikasnosti u odnosu na standardni algoritam.

### 6.2.3.2. Kernel 5

4-PSK kernel dužine 5 je:

$$a_5 = [+1; +1; +1; -i; +i]$$

$$b_5 = [+1; +i; -1; +1; -i]$$

Omega vektor ovog kernela je:

$$[-1, -1/2, -1/2 i, -1/3 i, -1/2, -1/2 i, +i]$$

Ovaj kernel se ne može iskoristiti za efikasni generator/korelator.

### 6.2.3.3. Kernel 10

Binarni kerneli dužine 10 mogu se posmatrati i kao polifazni kernel, kad se ima u vidu da binarni simboli  $\pm 1$  predstavljaju podskup polifaznih simbola. Pored tih trivijalnih slučajeva, frekencijskom modulacijom moguće je izvesti i čisto polifazni kernel 10 iz binarnog kernela. Tako, na primer, množenjem obe sekvence binarnog kernela 10 s kvaternarnom sekvencom:

$$[+1, +i, -1, -i, +1, +i, -1, -i, +1, +i]$$

dobijamo 4PSK kernel 10:

$$a_{10} = [+1, -i, +1, -i, +1, +i, -1, -i, 1, -i];$$

$$b_{10} = [+1, -i, +1, +i, +1, -i, -1, +i, -1, +i]$$

### 6.2.3.4. Kernel 11

$$a_{11} = [1; 1; 1; i; -1; 1; i; -i; i; 1; -1]$$

$$b_{11} = [1; i; -1; -1; -1; i; i; 1; -i; i; 1]$$

Omega vektor ovog kernela je:

$$[-1; (1-i)/2; i/3; -(1+i)/10; -9/17; 21/74(1-i); 9i/17; (1+i)/10; 1/3; (1-i)/2; -1]$$

### 6.2.3.5. Kernel 13

$$a_{13} = [1; 1; 1; i; -1; 1; 1; -i; 1; -1; 1; -i; i]$$

$$b_{13} = [1; i; -1; -1; -1; i; -1; 1; 1; -i; -1; 1; -i]$$

Omega vektor ovog kernela je:

$$[i; -(1+i)/2; 1/3; (-1+i)/10; 9/17i; -21/74(1+i); -21/157; 21/74(1-i); 9/17i; (1+i)/10; 1/3; (1-i)/2; -1]$$

### 6.2.3.6. Kerneli 20 i 26

Ovi binarni kerneli mogu se smatrati i polifaznim kernelima, kao što je objašnjeno u slučaju kernela 10. Takođe je moguće frekvencijski modulirati obe sekvence i tako se dobijaju čisto polifazni kerneli.

## 6.3. QAM sekvence

U modernim komunikacionim sistemima uveliko se koristi QAM modulacija. Najčešće korišćene varijante su 16-QAM i 64-QAM dok se razmatra i 256-QAM. Prednost ovih modulacija jeste što omogućavaju prenos većeg broja bita po simbolu i to 4 bita u slučaju 16-QAM, 6 bitova u slučaju 64-QAM i 8 bitova u slučaju 256-QAM.

Javilo se interesovanje za primenu komplementarnih sekvenci u QAM sistemima zato što se oni pre svega koriste u OFDM prenosu. Kako je poznato da je vršna snaga spektra komplementarnih sekvenci najviše 2, ova osobina je predložena za rešavanje problema vršne snage signala na izlazu iz predajnika (PAPR problem). Prve razmatrane komplementarne sekvence su bile binarne [Popovic 91] zatim 4-PSK [Davis 99]. Kod svih ovih sistema osnovni nerešeni problem jeste to što je protok bitova veoma mali kada se komplementarne sekvence koriste kao kodne reči. Naime, za dužine kodnih reči reda veličine 1024 iskoristivost kanala pada ispod 1%. Zato teoretičari uložili velike napore u povećanje broja sekvenci. Da bi se to postiglo, istraživane se komplementarne sekvence u višim QAM konstelacijama. Do sada je objavljeno više radova u kojima se generišu 16-QAM i 64-QAM komplementarne sekvence. Svi ti radovi su bili bazirani na direktnoj

metodi generisanja u kojoj se koriste Bulove funkcije. Mi ovde dajemo novo rešenje, zasnovano na paraunitarnim matricama.

### 6.3.1. Standardne

Na osnovu algoritma dekompozicije koji smo primenili na sekvence generisane direktnom metodom otkriveni su novi rekurzivni algoritmi za generisanje 16-QAM i 64-QAM komplementarnih sekvenci. U slučaju 16-QAM sekvenci novi rekurzivni algoritam generiše isti broj sekvenci kao i do sada poznati nerekurzivni algoritam dok je u slučaju 64-QAM sekvenci taj broj značajno povećan.

#### 6.3.1.1. 16-QAM sekvence

Za 16-QAM sekvence do sada je bio poznat nerekurzivni algoritam. Primenjujući naš algoritam dekompozicije postepeno smo otkrivali unutrašnju strukturu tih sekvenci i tako smo došli do opšteg rekurzivnog algoritma koji ovde prikazujemo.

Naše rešenje polazi od klasičnog rekurzivnog algoritma za generisanje polifaznih sekvenci koji je koje je primenjen na specijalan slučaj kada je broj faza 4, odnosno za 4-PSK sekvence. Modifikovali smo ovaj algoritam ubacujući jednu matricu (zvaćemo je Q matrica) koja transformiše 4-PSK signal u 16-QAM i dobili smo sve sekvence koje se mogu dobiti direktnom metodom ali mnogo jednostavnije i mnogo logičnije. Otkrivanje svih verzija Q matrice je bio poseban izazov. Osnovna alatka koju smo koristili u tom procesu bila je dekompozicija 16-QAM sekvenci generisanih direktnom metodom. Na taj način su otkrivene sve verzije Q matrica dok se nije dobio algoritam koji generiše sve poznate 16-QAM komplementarne sekvence.

Polazna osnova je bio algoritam za generisanje polifaznih komplementarnih sekvenci [Budišin 90A]:

$$\begin{aligned} \mathbf{x}_n^{(4PSK)}(Z^{-1}) &= \begin{bmatrix} 1 & w_n \\ 1 & -w_n \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-P_n} \end{bmatrix} \cdot \mathbf{x}_{n-1}^{(4PSK)}(Z^{-1}) \\ &= \mathbf{Y}_n(Z^{-1}) \cdot \mathbf{X}_{n-1}^{(4PSK)}(Z^{-1}) \end{aligned} \quad (170)$$

gde je  $n = 1, 2, \dots, N$ , dužina sekvence je:  $2^N$ , a  $[P_1, P_2, \dots, P_N]$  je bilo koja permutacija brojeva  $\{1, 2, 4, \dots, 2^{N-1}\}$ , zatim

$$\begin{aligned} \mathbf{Y}_n(Z^{-1}) &= \begin{bmatrix} 1 & w_n \\ 1 & -w_n \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-P_n} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w_n \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & Z^{-P_n} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & w_n \cdot Z^{-P_n} \end{bmatrix} \end{aligned} \quad (171)$$

a početni komplementarni par je:  $\mathbf{x}_0^{(4PSK)}(Z^{-1}) = \begin{bmatrix} w_0 \\ w_0 \end{bmatrix} = w_0 \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ . Pri tome je

$w_n \in \{e^{-im\pi/2} = i^m, m = 0, \dots, 3\}$  za  $n = 0, 1, 2, \dots, N$ .

Kako simetrične permutacije generišu identične  $a$  sekvence, mi nećemo koristiti simetrične permutacije da bismo generisali jedinstvene sekvence. To znači da je broj permutacija  $N!/2$  umesto  $N!$ .

Eksplisitni izraz za par komplementarnih 4-PSK sekvenci je:

$$\begin{aligned} \mathbf{x}_N^{(4PSK)}(Z^{-1}) &= \left\{ \prod_{k=N}^1 \mathbf{Y}_k(Z^{-1}) \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \\ &= \mathbf{Y}_N(Z^{-1}) \cdot \mathbf{Y}_{N-1}(Z^{-1}) \cdot \dots \cdot \mathbf{Y}_1(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \end{aligned} \quad (172)$$

Prema direktnoj konstrukciji iz [Davis 99] koja je ekvivalentna s [Budišin 90A] broj različitih 4-PSK sekvenci jeste:

$$M_{4PSK} = N!/2 \cdot 4^{(N+1)} \quad (173)$$

Prvi faktor  $N!$  jednak je broju permutacija. Drugi faktor u izrazu potiče od  $N + 1$  konstanti  $w_n$ , od kojih svaka ima jednu od 4 vrednosti faze.

Drugi relevantan algoritam je prikazan u [Roßing 01] i on koristi par 4-PSK sekvenci kao glavnu i sporednu koordinatu da bi se generisala 16-QAM sekvenca. Taj algoritam se može predstaviti jednačinom:

$$\mathbf{Q}^{(Rö\beta)} = \begin{bmatrix} 1 & q \\ -q & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} \quad (174)$$

Prepoznavamo da je ova matrica istog oblika kao matrica za generisanje višenivoskih sekvenci [Budišin 90B] ili, još opštije, ona je kao naša omega matrica. Mi ćemo u daljoj generalizaciji za  $\mathbf{Q}$  matricu koristiti opšti oblik omega matrice.

Kombinujući ovu jednačinu i jednačinu za 4-PSK sekvence Robingov algoritam postaje:

$$\mathbf{x}^{(16QAM)}(Z^{-1}) = \mathbf{Q}^{(Rö\beta)} \cdot \mathbf{x}^{(4PSK)}(Z^{-1}) \quad (175)$$

Broj različitih 16-QAM komplementarnih sekvenci koje se ovako generišu isti je kao broj 4-PSK sekvenci i iznosi  $M_{4PSK} = N!/2 \cdot 4^{N+1}$  pošto je preslikavanje jednoznačno. Najzad, par komplementarnih 4-PSK sekvenci  $\mathbf{x}^{(4PSK)}(Z^{-1})$  možemo zameniti s njegovim rekurzivnim izrazom:

$$\begin{aligned} \mathbf{X}_N^{(16QAM)}(Z^{-1}) &= \mathbf{Q}_N^{(R\delta\beta)} \cdot \left\{ \prod_{k=N}^1 \mathbf{Y}_k(Z^{-1}) \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \\ &= \mathbf{Q}_N^{(R\delta\beta)} \cdot \mathbf{Y}_N(Z^{-1}) \cdot \mathbf{Y}_{N-1}(Z^{-1}) \cdot \dots \cdot \mathbf{Y}_1(Z^{-1}) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \end{aligned} \quad (176)$$

Ovde treba uočiti suštinsku razliku između  $\mathbf{Q}$  matrice i  $\mathbf{Y}$ . S jedne strane,  $\mathbf{Y}$  matrica ne vrši rekombinovanje  $a$  i  $b$  sekvence zato što je pri sabiranju (u okviru množenja sa  $\mathbf{Y}$  matricom) jedan element ove dve sekvence uvek nula, tako da  $\mathbf{Y}$  matrica samo učešljava nenulte elemente komplementarnih sekvenci. S druge strane,  $\mathbf{Q}$  matrica direktno rekombinuje elemente dve sekvence tako što jednu sekvencu množi sa 2 a drugu sa 1 i na taj način proizvodi višenivoske sekvence čiji elementi pripadaju 16-QAM konstelaciji.

Novi algoritam, koji je direktna generalizacija gornjeg algoritma, uvodi dve novine:

Umesto  $\mathbf{Q}^{(R\delta\beta)}$  matrice koristi omega matrice koje zadovoljavaju uslov da mapiraju 4-PSK simbole u 16-QAM simbole.

$\mathbf{Q}$  matrica više ne mora biti na početku proizvoda (krajnje leva strana) nego bilo gde unutar proizvoda, pa čak i na krajnje desnoj strani proizvoda. Tako se dobija  $N+1$  položaj  $\mathbf{Q}$  matrice.

Računarskim pretraživanjem pronađeno je 14  $\mathbf{Q}$  matrica koje zadovoljavaju uslova mapiraju 4-PSK komplementarne sekvence u 16-QAM sekvence:  $\mathbf{Q}^{(1)}, \mathbf{Q}^{(2)}, \dots, \mathbf{Q}^{(14)}$ ; one su prikazane u Tab. 9. Prepoznamo da je matrica  $\mathbf{Q}^{(1)}$  u stvari  $\mathbf{Q}^{(R\delta\beta)}$ . Prvih 8 matrica su opšte, što znači da mapiraju bilo koji par 4-PSK simbola u par 16-QAM simbola. Četiri specijalne matrice  $\mathbf{Q}^{(9)}, \dots, \mathbf{Q}^{(12)}$  ne mapiraju proizvoljni par 4-PSK simbola u 16-QAM simbole nego samo one parove simbola iz komplementarnih parova. Najzad, dve trivijalne matrice:  $\mathbf{I}$  i  $3 \cdot \mathbf{I}$  mapiraju 4-PSK simbole u same sebe ili u 3 puta veće verzije. Naravno, ti simboli takođe pripadaju 16-QAM konstelaciji.

Korišćenjem tih 14 matrica broj različitih 16-QAM sekvenci se povećava 14 puta i to sa  $M_{4PSK} = N!/2 \cdot 4^{N+1}$  koje generiše Robingov algoritam na  $14 \cdot M_{4PSK}$ .

Tab. 9.  $\mathbf{Q}$  matrice, broj generisanih sekvenci,  $P$  i PAPR

$\mathbf{Q}$ matrica	Veličina	$P$	PAPR
$\mathbf{Q}^{(1)} \dots \mathbf{Q}^{(4)} = \begin{bmatrix} 1 & 2 \cdot u \\ -2 \cdot u^* & 1 \end{bmatrix}$ <p>gde je <math>u = e^{i(2k)\pi/4}, k = 0:3</math></p>	$4(N+1) \cdot M_{4PSK}$	5	2,0
$\mathbf{Q}^{(5)} \dots \mathbf{Q}^{(8)} = \begin{bmatrix} 1 & \sqrt{2} \cdot v \\ -\sqrt{2} \cdot v^* & 1 \end{bmatrix}$ <p>gde je <math>v = e^{i(2k+1)\pi/4}, k = 0:3</math></p>	$4(N+1) \cdot M_{4PSK}$	3	1,2
$\mathbf{Q}^{(9)} \dots \mathbf{Q}^{(12)} = \begin{bmatrix} 2+u & uv+v \\ -uv+v & 2-u \end{bmatrix}$ <p>gde je <math>u, v = \pm i</math></p>	$4(N+1) \cdot M_{4PSK}$	7	2,8
$\mathbf{Q}^{(13)} = \mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$M_{4PSK}$	1	0,4
$\mathbf{Q}^{(14)} = 3 \cdot \mathbf{I} = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$	$M_{4PSK}$	9	3,6

Druga značajna odlika novog algoritma jeste to da se  $\mathbf{Q}$  matrica može nalaziti bilo gde u proizvodu a ne samo s leve strane. To je moguće zahvaljujući činjenici da su matrice i  $\mathbf{Y}_k(Z^{-1})$  i  $\mathbf{Q}$  matrice unitarne tako da se njihovom primenom održava komplementarnost. Pored toga, kako  $\mathbf{Y}_k(Z^{-1})$  matrice samo učešljavaju sekvence, na mestu u proizvodu gde  $\mathbf{Q}$  matrica transformiše par 4-PSK sekvenci u 16-QAM par, sekvence ostaju 16-QAM i posle množenja sa ostatkom  $\mathbf{Y}_k(Z^{-1})$  matrica s leve strane od  $\mathbf{Q}$  matrice. Tako da je krajni rezultat celog proizvoda komplementarni par sekvenci koji pripada 16-QAM konstelaciji.

Formalno, novi algoritam možemo napisati u sledećem obliku:

$$\mathbf{x}_{N,m}^{(16QAM)}(Z^{-1}) = \left\{ \prod_{k=N}^{m+1} \mathbf{Y}_k(Z^{-1}) \right\} \cdot \mathbf{Q}_m^{(l)} \cdot \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z^{-1}) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \quad (177)$$

gde,  $l = 1, 2, \dots, 12$  određuje koja se  $\mathbf{Q}^{(l)}$  matrica koristi dok  $m = 0, 1, \dots, N$  određuje položaj u proizvodu te  $\mathbf{Q}_m^{(l)}$  matrice. Sada ćemo primerom ilustrovati kako se pri upotrebi trivijalnih  $\mathbf{Q}^{(13)}$  i  $\mathbf{Q}^{(14)}$  na različitim položajima u proizvodu ne dobijaju dodatni komplementarni parovi.

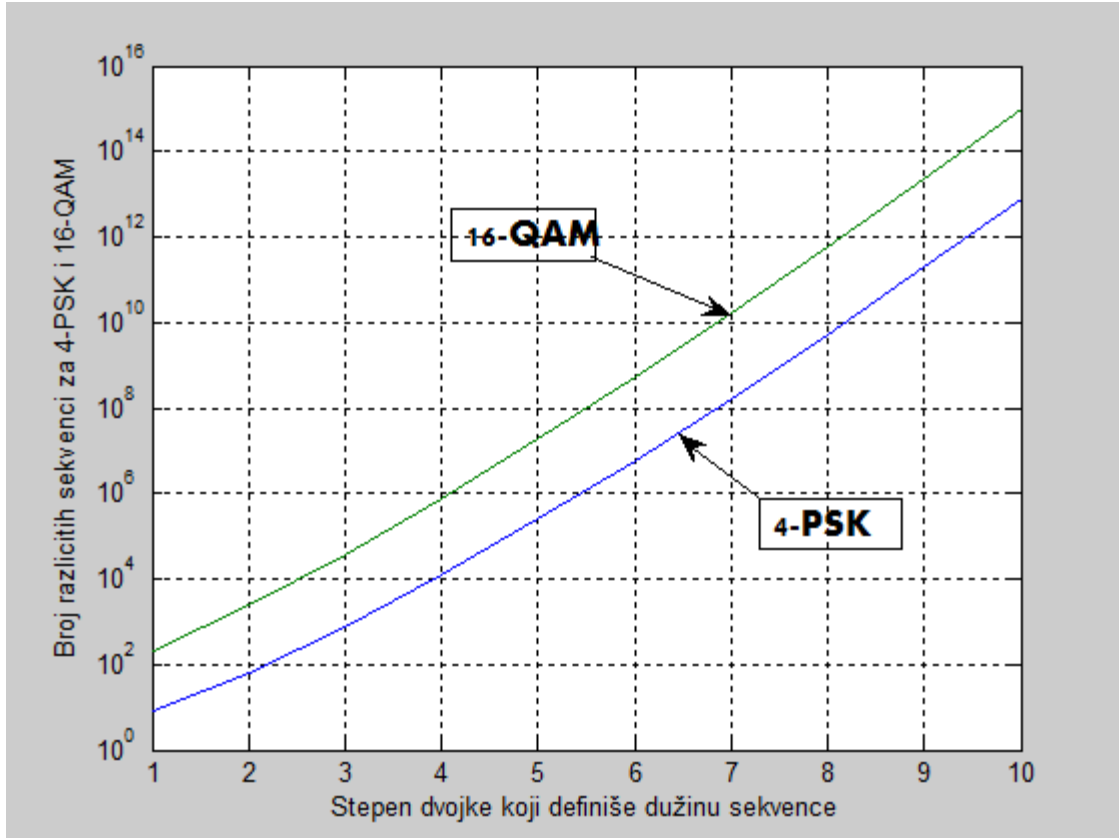
Na primer, ako  $\mathbf{Q}^{(13)} = \mathbf{I}$  ubacimo u (177), dobijamo:

$$\begin{aligned} \mathbf{x}_N^{(16QAM)} &= \left\{ \prod_{k=N}^{m+1} \mathbf{Y}_k(Z^{-1}) \right\} \cdot \mathbf{I} \cdot \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z^{-1}) \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \\ &= \left\{ \prod_{k=N}^1 \mathbf{Y}_k(Z^{-1}) \right\} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \end{aligned} \quad (178)$$

što je tačno izraz koji generiše 4-PSK komplementarne sekvence. Isto važi i za  $\mathbf{Q}^{(14)} = 3 \cdot \mathbf{I}$  osim što sekvenca tada ima 3 puta veću amplitudu.

Dakle, mi ćemo koristiti samo 12 netrivialnih  $\mathbf{Q}^{(l)}$  matrica u gornjim jednačinama a dodaćemo dva trivijalna slučaja. Postoji  $N+1$  lokacija u proizvodu gde može da se postavi  $\mathbf{Q}$  matrica tako da je ukupni broj sekvenci koje mogu da se generišu pomoću matrica  $\mathbf{Q}^{(1)}$  do  $\mathbf{Q}^{(12)}$  jednak:  $12 \cdot (N+1) \cdot N!/2 \cdot 4^{N+1}$ . Dve trivijalne matrice  $\mathbf{Q}^{(13)}$  i  $\mathbf{Q}^{(14)}$  generisaće isti skup različitih sekvenci bez obzira na položaj u proizvodu tih matrica tako da one generišu ukupno  $2N!/2 \cdot 4^{N+1}$  različitih sekvenci. Sledi da je ukupan broj različitih 16-QAM komplementarnih sekvenci jednak zbiru ta dva broja:  $M_{16QAM} = 12 \cdot (N+1) \cdot N!/2 \cdot 4^{N+1} + 2N!/2 \cdot 4^{N+1} = (14 + 12N) \cdot N!/2 \cdot 4^{N+1}$  što je identičan broj onom generisanom na osnovu algoritma poznatog iz literature. Ovaj izraz možemo jos napisati i kao:  $M_{16QAM} = (14 + 12N) \cdot N!/2 \cdot 4^{N+1} = (14 + 12N) M_{4PSK}$  gde je  $M_{4PSK} = N!/2 \cdot 4^{N+1}$  broj 4-PSK sekvenci.

Na Sl. 22 prikazano je kako broj različitih sekvenci zavisi od dužine generisanih sekvenci.



Sl. 22. Broj različitih 4-PSK I 16-QAM sekvenci zavisi od dužine sekvenci

*Primer:* Ilustrovaćemo novi algoritam jednostavnim primerom. Generisaćemo 16-QAM sekvence dužine 4 koristeći fiksirane  $\mathbf{Y}$  i  $\mathbf{Q}$  matrice a samo ćemo varirati položaj  $\mathbf{Q}$  matrice u proizvodu ( $m = 0,1,2$ ). Uzećemo vrednosti:  $w_0 = w_1 = w_2 = w = 1$ ,  $P = [1,2]$ , i  $\mathbf{Q} = \mathbf{Q}^{(1)}$  i tako dobijamo:

$$\mathbf{Y}_2(Z^{-1}) = \begin{bmatrix} 1 & w \\ 1 & -w \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Z^{-2} \end{bmatrix} = \begin{bmatrix} 1 & Z^{-2} \\ 1 & -Z^{-2} \end{bmatrix},$$

$$\mathbf{Y}_1(Z^{-1}) = \begin{bmatrix} 1 & Z^{-1} \\ 1 & -Z^{-1} \end{bmatrix} \quad (179)$$

Generisane sekvence su:

$$\mathbf{x}_{2,2}^{(16QAM)} = \mathbf{Q} \cdot \mathbf{Y}_2 \cdot \mathbf{Y}_1 = \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & Z^{-2} \\ 1 & -Z^{-2} \end{bmatrix} \begin{bmatrix} 1 & Z^{-1} \\ 1 & -Z^{-1} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 3 + 3Z^{-1} - Z^{-2} + Z^{-3} \\ -1 - Z^{-1} - 3Z^{-2} + 3Z^{-3} \end{bmatrix} \quad (180)$$

$$\begin{aligned} \mathbf{x}_{2,1}^{(16QAM)} &= \mathbf{Y}_2 \cdot \mathbf{Q} \cdot \mathbf{Y}_1 = \begin{bmatrix} 1 & Z^{-2} \\ 1 & -Z^{-2} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & Z^{-1} \\ 1 & -Z^{-1} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 3 - Z^{-1} - Z^{-2} - 3Z^{-3} \\ 3 - Z^{-1} + Z^{-2} + 3Z^{-3} \end{bmatrix} \end{aligned} \quad (181)$$

$$\begin{aligned} \mathbf{x}_{2,0}^{(16QAM)} &= \mathbf{Y}_2 \cdot \mathbf{Y}_1 \cdot \mathbf{Q} = \begin{bmatrix} 1 & Z^{-2} \\ 1 & -Z^{-2} \end{bmatrix} \begin{bmatrix} 1 & Z^{-1} \\ 1 & -Z^{-1} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 3 - Z^{-1} + 3Z^{-2} + Z^{-3} \\ 3 - Z^{-1} - 3Z^{-2} - Z^{-3} \end{bmatrix} \end{aligned} \quad (182)$$

ili u vremenskom domenu:

$$a_2 = [+3, +3, -1, +1]; a_1 = [+3, -1, -1, -3]; a_0 = [+3, -1, +3, +1] \quad (183)$$

Posmatrajući položaj elemenata sekvence s amplitudom 3, zaključujemo kako položaj  $\mathbf{Q}$  matrice utiče na generišuće sekvence i zašto proizvodi različite sekvence.

*Vršni faktor PAPR:* polazimo od računanja ukupne energije sekvenci u paru na osnovu izraza za uslov komplementarnosti u matičnom obliku (37) koristeći izraz za  $\mathbf{x}$  iz (177) i dobijamo:

$$\begin{aligned} 2E &= \mathbf{x}(Z)^H \mathbf{x}(Z^{-1}) \\ &= \left[ \left\{ \prod_{k=N}^{m+1} \mathbf{Y}_k(Z) \right\} \cdot \mathbf{Q}_m^{(l)} \cdot \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \right]^H \times \left[ \left\{ \prod_{k=N}^{m+1} \mathbf{Y}_k(Z) \right\} \cdot \mathbf{Q}_m^{(l)} \cdot \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z^{-1}) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right] \\ &= \begin{bmatrix} 1 \\ 1 \end{bmatrix}^H \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z) \right\}^H \left( \mathbf{Q}_m^{(l)} \right)^H \left\{ \prod_{k=m+1}^N (\mathbf{Y}_k(Z))^H \times \prod_{k=N}^{m+1} \mathbf{Y}_k(Z^{-1}) \right\} \mathbf{Q}_m^{(l)} \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z^{-1}) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{aligned} \quad (184)$$

Primenjujemo paraunitarnost:  $\tilde{\mathbf{Y}}_k(Z^{-1}) \cdot \mathbf{Y}_k(Z^{-1}) = \mathbf{Y}_k^H(Z) \cdot \mathbf{Y}_k(Z^{-1}) = 2 \cdot \mathbf{I}$  tako da dobijamo:

$$\prod_{k=m+1}^N (\mathbf{Y}_k(Z))^H \times \prod_{k=N}^{m+1} \mathbf{Y}_k(Z^{-1}) = 2^{N-m} \cdot \mathbf{I} \quad (185)$$

što daje:

$$2E = 2^{N-m} \begin{bmatrix} 1 \\ 1 \end{bmatrix}^H \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z) \right\}^H \cdot \left\{ \left( \mathbf{Q}_m^{(l)} \right)^H \cdot \mathbf{Q}_m^{(l)} \right\} \cdot \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z^{-1}) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (186)$$

Lako se pokazuje da je  $\left( \mathbf{Q}_m^{(l)} \right)^H \cdot \mathbf{Q}_m^{(l)} = K \cdot \mathbf{I}$  pošto su matrice  $\mathbf{Q}$  unitarne a  $K$  je konstanta koja zavisi od svake  $\mathbf{Q}$  matrice. Iz ovog izraza  $K$  je jednako:

$$K = \sqrt{|(\mathbf{Q}^{(L)})^H \cdot \mathbf{Q}^{(L)}|} \quad (187)$$

$$\begin{aligned} 2E &= 2^{N-m} \begin{bmatrix} 1 \\ 1 \end{bmatrix}^H \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z) \right\}^H \cdot K \cdot \mathbf{I} \cdot \left\{ \prod_{k=m}^1 \mathbf{Y}_k(Z^{-1}) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= K \cdot 2^{N-m} \begin{bmatrix} 1 \\ 1 \end{bmatrix}^H 2^m \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 2 \cdot K \cdot 2^N \end{aligned} \quad (188)$$

Najzad dobijamo izraz za energiju sekvence:  $E = K \cdot 2^N$ . Snaga sekvence jednaka je energiji podeljenoj s dužinom sekvence pa imamo:

$$P = E/2^N = K \quad (189)$$

U Tab. 9. su date vrednosti za snagu  $P$  za različite grupe  $\mathbf{Q}$  matrica. Primećuje se da najmanju snagu i najveću snagu imaju sekvence generisane pomoću trivijalnih  $\mathbf{Q}$  matrica. One imaju  $P = 1$  i  $P = 9$ . Ostale 3 grupe sekvenci imaju  $P = 3, 5$  i  $7$ .

Vršna snaga spektra PAPR svih komplementarnih sekvenci (u slučaju da obe sekvence imaju istu snagu) jeste 2. To, naravno, važi i za 16-QAM sekvence. Međutim, kod 16-QAM sekvenci zanima nas PAPR koji je malo drukčije definisan. Za razliku od PAPR definisanog za pojedinačne sekvence, ovde ćemo odrediti PAPR definisan kao vršna vrednost konkretne sekvence prema srednjoj vrednosti snage celog skupa sekvenci. Tako se za 16-QAM komplementarne sekvence dobija da je srednja snaga 5. Ako je za pojedinačnu 16-QAM sekvencu srednja snaga  $P$  onda je njena vršna snaga  $2P$  pa je PAPR koji nas interesuje:  $PAPR = 2P/5 = 0,4P$ . Vrednosti za PAPR su takođe navedene u Tab. 9. i potpuno se slažu s podacima iz tabele II u radu [Chan 03].

### 6.3.1.2. 64-QAM sekvence

Prateći logiku konstrukcije 16-QAM sekvenci pomoću paraunitarnih matrica, razvili smo i teoriju 64-QAM sekvenci. Da bi se shvatila složenost ove problematike koja je do sada obrađivana isključivo na bazi direktne konstrukcije zasnovane na primeni Bulovih funkcija, daćemo dva primera.

Kao prvo, u dva fundamentalna rada gde je sačinjena direktna konstrukcija 16-QAM sekvenci [Chan 03] i 64-QAM sekvenci [Lee 06] promakla je suštinska greška tako da generisane sekvence nisu bile komplementarne jedna drugoj. Greška je ispravljena tek nakon 5 godina od prvog rada, u radu drugog autora [Li 08]. To nam govori da grešku nisu uočili ni recenzenti a ni 21 autor koji su citirali rad.

Da bismo shvatili kako je to moguće, pogledajmo na Sl. 23 ilustraciju složenosti matematičkih izraza koji se koriste u tim radovima:

$$\begin{aligned}
 C_C(u) + C_D(u) &= \sum_{i=0}^{n-u-1} \left[ r_1^2 \left\{ \xi^{A_i - A_{i+u}} + \xi^{B_i - B_{i+u}} \right\} \right. \\
 &\quad + r_2^2 \left\{ \xi^{a_i - a_{i+u}} + \xi^{b_i - b_{i+u}} \right\} + r_3^2 \left\{ \xi^{\alpha_i - \alpha_{i+u}} + \xi^{\beta_i - \beta_{i+u}} \right\} \\
 &\quad + r_1 r_2 \left\{ \xi^{A_i - a_{i+u}} + \xi^{a_i - A_{i+u}} + \xi^{B_i - b_{i+u}} + \xi^{b_i - B_{i+u}} \right\} \\
 &\quad + r_1 r_3 \left\{ \xi^{A_i - \alpha_{i+u}} + \xi^{\alpha_i - A_{i+u}} + \xi^{B_i - \beta_{i+u}} + \xi^{\beta_i - B_{i+u}} \right\} \\
 &\quad \left. + r_2 r_3 \left\{ \xi^{a_i - \alpha_{i+u}} + \xi^{\alpha_i - a_{i+u}} + \xi^{b_i - \beta_{i+u}} + \xi^{\beta_i - b_{i+u}} \right\} \right] \\
 &= \sum_{i=0}^{n-u-1} \left[ r_1 r_2 \left\{ \xi^{A_i - a_{i+u}} + \xi^{a_i - A_{i+u}} + \xi^{B_i - b_{i+u}} + \xi^{b_i - B_{i+u}} \right\} \right. \\
 &\quad + r_1 r_3 \left\{ \xi^{A_i - \alpha_{i+u}} + \xi^{\alpha_i - A_{i+u}} + \xi^{B_i - \beta_{i+u}} + \xi^{\beta_i - B_{i+u}} \right\} \\
 &\quad \left. + r_2 r_3 \left\{ \xi^{a_i - \alpha_{i+u}} + \xi^{\alpha_i - a_{i+u}} + \xi^{b_i - \beta_{i+u}} + \xi^{\beta_i - b_{i+u}} \right\} \right] \\
 &= r_1 r_2 \sum_{i=0}^{n-u-1} \left\{ \xi^{A_i - a_{i+u}} + \xi^{a_i - A_{i+u}} + \xi^{B_i - b_{i+u}} + \xi^{b_i - B_{i+u}} \right\} \\
 &= r_1 r_2 \sum_{i=0}^{n-u-1} \left[ \xi^{A_i - a_{i+u}} \left\{ \xi^{-s_{i+u}^{(1)}} + \xi^{s_i^{(1)}} \right\} + \xi^{a_i - A_{i+u}} \left\{ \xi^{-s_{i+u}^{(1)}} + \xi^{s_i^{(1)}} \right\} (-1)^{(i \pi(1) - (i+n) \pi(1))} \right] \\
 &= r_1 r_2 \sum_{i=0}^{n-u-1} \left[ \xi^{A_i - a_{i+u}} \left\{ \xi^{-s_{i+u}^{(1)}} + \xi^{s_i^{(1)}} \right\} \times \left\{ 1 + (-1)^{(i \pi(1) - (i+n) \pi(1))} \right\} \right].
 \end{aligned}$$

Sl. 23. Primer složenosti izraza koji se koriste u radovima gde je primenjena direktna metoda

Za razliku od njih mi koristimo pristup baziran na paraunitarnim matricama i naša konstrukcija je data sledećim izrazom:

$$\mathbf{x}_{N,m,n}^{(64QAM)}(Z^{-1}) = \left\{ \prod_{k=N}^{m+1} \mathbf{Y}_k(Z^{-1}) \right\} \cdot \mathbf{R}_m^{(l)} \cdot \left\{ \prod_{k=m}^{n+1} \mathbf{Y}_k(Z^{-1}) \right\} \cdot \mathbf{S}_n^{(l)} \cdot \left\{ \prod_{k=n}^1 \mathbf{Y}_k(Z^{-1}) \right\} \begin{bmatrix} 1 \\ 1 \end{bmatrix} w_0 \quad (190)$$

gde su  $\mathbf{R}_m^{(l)}$  i  $\mathbf{S}_n^{(l)}$  matrice oblika omega matrice koje tek treba odrediti. One imaju istu ulogu kao  $\mathbf{Q}$  matrica u konstrukciji 16-QAM sekvenci. Istraživanje mogućih  $\mathbf{R}$  i  $\mathbf{S}$  matrica pokazalo se kao prilično složen problem. Srećom, istraživanje PAPR problema kod 16-QAM matrica pokazalo se veoma korisno za pretraživanje  $\mathbf{R}$  i  $\mathbf{S}$  matrica. Naime, lako se pokazuje da i kod 64-QAM sekvenci snaga zavisi samo od  $\mathbf{R}$  i  $\mathbf{S}$  matrica i to tako da je  $P$  jednako proizvodu  $P_R$  i  $P_S$  gde  $P_R$  i  $P_S$  odgovaraju pojedinačnim  $\mathbf{R}$  i  $\mathbf{S}$  matricama. Iz toga sledi da je  $P = P_R \cdot P_S$ . Pošto su  $P$ -ovi celi neparni brojevi,  $\mathbf{R}$  i  $\mathbf{S}$  matrice mogu se pretraživati po vrednostima  $P$ -ova. Ukoliko je, na primer,  $P$  prost broj onda jedna od te dve matrice kojoj odgovara  $P = 1$  mora da bude trivijalna jedinična matrica.

Tako dolazimo do klasifikacije  $\mathbf{R}$  i  $\mathbf{S}$  matrica. Postoje 3 mogućnosti:

- Obe matrice su netrivialne i takve slučajeve ćemo zvati netrivialnim.
- Jedna matrica je netrivialna a druga trivijalna i takve slučajeve ćemo zvati polutrivialnim. Treba uočiti da se tada algoritam svodi na isti oblik kao algoritam za 16-QAM
- Obe matrice su trivijalne i taj slučaj ćemo zvati trivijalnim. Treba napomenuti da se tada algoritam generisanja svodi na algoritam za 4-PSK i da se matrice tada mogu zameniti konstantama. Dok su u slučaju 16-QAM te konstante uzimale samo dve vrednosti 1 i 3, sada mogu da uzmu 4 moguće vrednosti: 1, 3, 5 i 7.

Pokazalo se da postoje samo 3 netrivialna slučaja i to kada je

- $P = 3 \cdot 3 = 9$
- $P = 3 \cdot 5 = 15$
- $P = 5 \cdot 5 = 25$

Ti slučajevi generišu  $(18N(N + 1) + 4(N + 1)) \cdot M_{4PSK}$  različitih sekvenci. Mi ćemo u daljoj analizi posmatrati samo multiplikativni faktor  $18N(N + 1) + 4(N + 1)$ . Prvo treba uočiti da ovaj broj raste s kvadratom parametra  $N$ , za razliku od 16-QAM slučaja gde je multiplikativni faktor bio  $2 + 12(N + 1)$  što znači da je rastao linearno s  $N$ .

Polutrivialni slučajevi postoje za sve neparne vrednosti  $P$  od 3 do 43, izuzev vrednosti 35 i 41. Ukupan broj polutrivialnih sekvenci je  $228 \cdot (m + 1)$  (naravno, dat je samo multiplikator).

Na kraju treba dodati 4 trivijalna slučaja koje smo ranije već naveli.

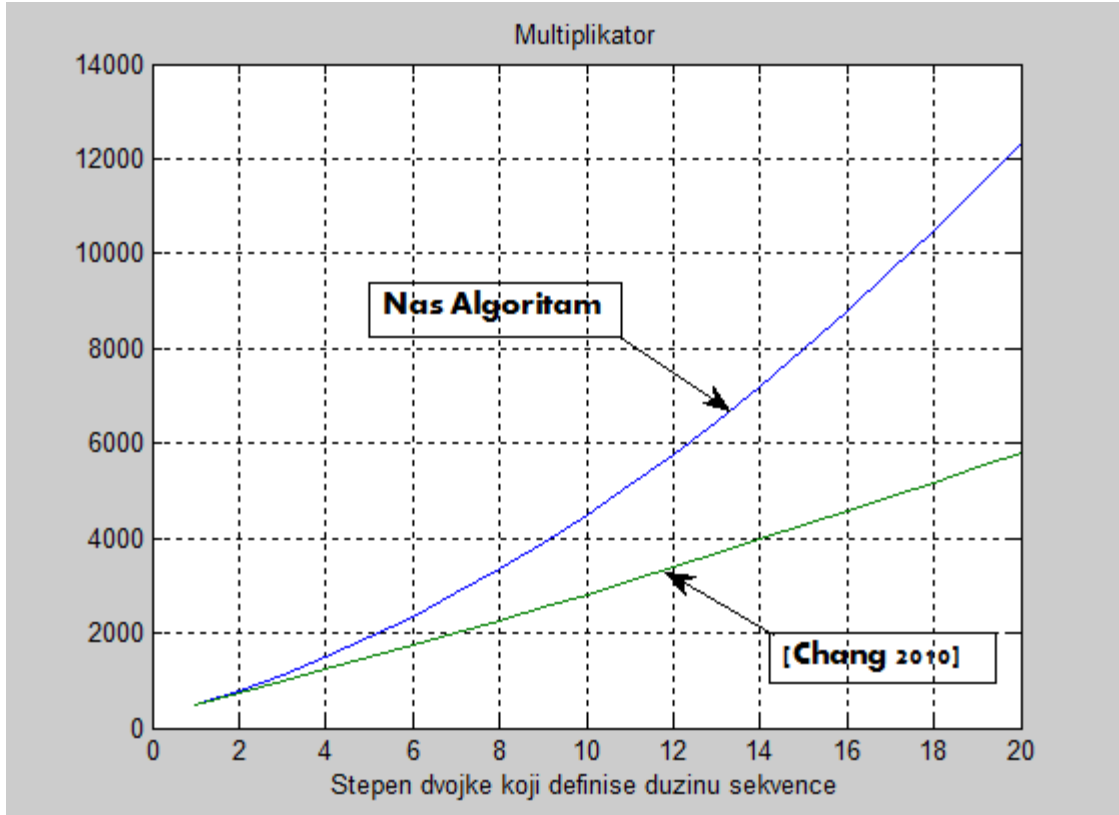
Kada se sve te sekvence saberu, dobija se ukupan broj:

$$M_{64QAM} = 18 \cdot N \cdot (N + 1) + 228 \cdot (N + 1) + 4 \quad (191)$$

Kada ovaj broj uporedimo s najboljim poznatim algoritmom baziranim na Bulovim funkcijama [Chang 10]:

$$M'_{64QAM} = 2 \cdot N \cdot (N + 1) + 236 \cdot (N + 1) + 4 \quad (192)$$

vidimo da naš algoritam generiše znatno više sekvenci. Ova dva multiplikatora broja sekvenci su prikazana na Sl. 24:



Sl. 24. Broj sekvenci generisanih pomoću predloženog algoritma i algoritma [Chang 2010] kao funkcija dužine sekvenci

### 6.3.2. Nestandardne sekvence

Prve nestandardne 16-QAM sekvence dužine 4 objavljene su u [Li 09]. Činjenica da su pronađene nestandardne sekvence za tako male dužine govori da se nestandardne sekvence veoma često javljaju u QAM konstelacijama i logično je očekivati da će njihova učestanost naglo rasti kako povećavamo konstelaciju i kako povećavamo dužinu sekvenci. Takođe je veoma indikativna činjenica da postoje 2.432 standardne Golejeve sekvence dužine 4 i 1.440 nestandardnih sekvenci, što je povećanje od 59%. U radu [Li 09] takođe je konstatovano da se ove sekvence mogu svesti na 13 osnovnih parova. Do sada nije istraženo postoji li unutrašnja struktura u tim parovima; da postoji, bilo bi nade da se te sekvence mogu konstruisati kakvim opštim algoritmom. Takođe je konstatovano da sekvence u 12 od tih 13 parova imaju različitu snagu. U Tab. 10 date su sekvence, vrednosti omega vektora i snage sekvenci  $P_a$  i  $P_b$ .

Tab. 10. Nestandardne sekvence, vrednosti omega vektora i snage sekvenci  $P_a$  i  $P_b$

	"a" sekvenca	"b" sekvenca	$\Omega(0)$	$\Omega(1)$	$\Omega(2)$	$\Omega(3)$	$P_a$	$P_b$
1	[A, A, A, A]	[A, B, -B, -A]	1	i	-i	-1	1	3
2	[A, A, -A, -A]	[A, -A, 3A, A]	-1	-1	1	-1	1	3
3	[A, A, iA, A]	[A, iA, -B, -A]	1	i	$(1-i)/2$	-1	1	2
4	[B, B, -B, -B']	[B, -B, -3A, B']	$(4-3i)/5$	$(-1-3i)/10$	1	-1	5	6
5	[A, A, -A, -iB]	[A, iA, B', iB]	$2-i$	$i/3$	$(1-i)/2$	-1	2	3
6	[B, -B, -A, B']	[B, iB, iB, -B']	$(-4+3i)/5$	$(-2-i)/5$	$(-1-i)/2$	-1	4	5
7	[A, A, -B, -iB]	[A', iB, -B, B]	-1	$(1+2i)/3$	$(-1+i)/2$	i	3	4
8	[A, -iB, -3A, -B]	[A, 3A, A', B]	$-1-2i$	i	$(-1-i)/2$	-1	5	4
9	[B, -A, -A, B']	[B, -3A, B, -B']	$(-4+3i)/5$	$(-7-i)/10$	$0.2-0.4i$	-1	3	6
10	[A, B, -B, B']	[B, -A, B, -A']	-i	$(1-i)/2$	$(-1+2i)/3$	$-1-2i$	4	3
11	[A, A, -3A, iB]	[A, 3A, -iB', -iB]	$-2+i$	$(1-i)/2$	-1	-1	4	5
12	[A, A, -iB', -A]	[A, -iB', 3A, A]	-1	-1	$1-i$	-1	2	4
13	[A, A, -iB', A]	[A, iB', A, -A]	1	-1	i	-1	2	2

Vrednosti A i B su definisane sa:  $A = 1 + i, B = (1 + 2i) \cdot A$ . Na osnovu Tab. 10 zaključujemo da se ne može uočiti velika pravilnost u vrednostima za omega vektor. Možda bi veća pravilnost mogla da se zapazi na dužim sekvencama ali takvo pretraživanje do sada nije urađeno.

### 6.3.3. Kerneli

Prvi opisani 16-QAM kerneli su dati u [Huang 11] za dužine 7, 9 i 15. Kerneli dužine 7 su dobijeni računarskim pretraživanjem i njih ima 79. Autori su uočili da se neki od tih kernela dobijaju učešljavanjem dva para dužine 3 i 4. Oni su prikazali opšti uslov pod kojim je takvo učešljavanje moguće i na osnovu toga su, učešljavajući sekvence dužine 4 i 5 odnosno 7 i 8, konstruisali kernele dužine 9 i 15. Kako kerneli dužine 9 i 15 nisu dobijeni sistematskim pretraživanjem njihov spisak nije kompletan. Zbog toga ćemo analizirati samo kernele dužine 7.

Iz Tab. 11. vidimo da određen broj sekvenci poseduje neku strukturu. Tome svedoče nule u Omega(3) i Omega(5) te mnogo unimodularnih koeficijenata. S druge strane, mnoge sekvence nemaju strukturu, a za to su dokaz veoma kompozitni koeficijenti.

Primeri

Tab. 11. Omega vektori za sekvence iz [Huang 11]

	$\Omega(0)$	$\Omega(1)$	$\Omega(2)$	$\Omega(3)$	$\Omega(4)$	$\Omega(5)$	$\Omega(6)$
1	$-2 - i$	0	$(1/2) + (1/2)i$	0	-1	$(1/2) - (1/2)i$	-1
2	$-2 + i$	$(1/2) - (1/2)i$	i	0	$(1/2) - (1/2)i$	0	-1
3	$2 + i$	$-(1/2) - (1/2)i$	i	0	$-(1/2) - (1/2)i$	0	-1
4	$(4/5) - (3/5)i$	$-(1/10) + (7/10)i$	$(2/5) + (1/5)i$	0	$(1/2) + (1/2)i$	0	-1
5	-i	$-(1/2) + (1/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
6	-i	$(1/2) + (1/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
7	-i	$-(3/2) + (1/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
8	-i	$(3/2) + (1/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
9	i	$-(3/2) - (1/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
10	i	$(3/2) - (1/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
11	$-(4/5) + (3/5)i$	$(1/10) - (7/10)i$	$-(2/5) - (1/5)i$	0	$(1/2) - (1/2)i$	0	-1
12	$-2 + i$	0	$(1/2) - (1/2)i$	0	-1	$(1/2) - (1/2)i$	-1
13	$(4/5) - (3/5)i$	$-(1/10) + (7/10)i$	$(2/5) + (1/5)i$	0	$-(1/2) - (1/2)i$	0	-1
14	$(4/5) - (3/5)i$	$-(1/10) + (7/10)i$	$(2/5) + (1/5)i$	0	$(1/2) - (1/2)i$	0	-1
15	-i	$-(3/2) + (3/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
16	-i	$(3/2)0 + (3/2)i$	i	0	$(1/2) + (1/2)i$	0	-1
17	$(4/5) - (3/5)i$	$-(7/10) - (1/10)i$	$(4/5) - (3/5)i$	0	$(1/10) + (3/10)i$	0	-1
18	$(4/5) - (3/5)i$	$-0.1 + (7/10)i$	$(4/5) - (3/5)i$	0	$(1/10) + (3/10)i$	0	-1
19	1	$-1 - i$	$(1/3) - (1/3)i$	$(1/2) + (1/2)i$	0	0	-1
20	-1	$(1/2) - (1/2)i$	$(1/3) - (2/3)i$	$(1/14) - (1/14)i$	$-(2/3) + (1/3)i$	$(1/2) - (1/2)i$	-1
21	1	$-(1/2) + (1/2)i$	$(1/3)$	$-(7/10) - (7/10)i$	$(1/3)i$	$(1/2) - (1/2)i$	-1
22	1	$(1/2) + (1/2)i$	i	$-(1/2) + (1/2)i$	$(1/3)$	$(1/2) + (1/2)i$	-1
23	1	$-(1/2) + (1/2)i$	$-(1/3)$	$(1/2) + (1/2)i$	i	$(1/2) - (1/2)i$	-1
24	1	$(1/2) - (1/2)i$	-1	$(1/2) - (1/2)i$	$(1/3)i$	$(1/2) + (1/2)i$	-1
25	1	$(1/2) + (1/2)i$	-1	$(1/2) + (1/2)i$	$(1/3)i$	$(1/2) - (1/2)i$	-1
26	-1	$(1/2) - (1/2)i$	$(1/3)i$	$-1 - i$	$(1/2) + (1/2)i$	0	-1
27	1	$-(1/2) + (1/2)i$	$(1/3)$	$(1/2) + (1/2)i$	i	$(1/2) - (1/2)i$	-1
28	1	$(1/2) - (1/2)i$	i	$-(1/2) - (1/2)i$	$-(1/3)$	$(1/2) - (1/2)i$	-1
29	1	$(1/2) - (1/2)i$	$(1/3)i$	$(1/2) + (1/2)i$	-1	$(1/2) - (1/2)i$	-1
30	1	$-(1/2) + (1/2)i$	1	$(1/2) + (1/2)i$	$(1/3)i$	$(1/2) - (1/2)i$	-1
31	1	$-(1/2) + (1/2)i$	-1	$(1/2) + (1/2)i$	$(1/3)i$	$(1/2) - (1/2)i$	-1
32	1	$(1/2) + (1/2)i$	$(1/3)i$	$(1/2) - (1/2)i$	-1	$(1/2) + (1/2)i$	-1
33	i	$-(1/2) - (1/2)i$	$(2/3) + (1/3)i$	$-(2/7) - (2/7)i$	$-(3/2) + (1/2)i$	0	-1
34	1	$-(1/2) + (1/2)i$	$(1/3)i$	$-(11/10) - (11/10)i$	$(1/3)$	$(1/2) - (1/2)i$	-1
35	1	$(1/2) - (1/2)i$	i	$-(1/6) - (1/6)i$	-1	$(1/2) - (1/2)i$	-1
36	1	$(1/2) - (1/2)i$	i	$(1/6) + (1/6)i$	-1	$(1/2) - (1/2)i$	-1
37	-1	$1 + i$	$-1 + (1/3)i$	$-(1/2) + (1/2)i$	0	0	-1
38	-1	$1 - i$	$-(1/3) - i$	$(1/2) + (1/2)i$	0	0	-1
39	$-1 - 2i$	$(1/3)i$	$(13/20) - (11/20)i$	$-(1/5) + (2/5)i$	$(1/3)i$	$-(1/2) + (1/2)i$	-1

## Primeri

40	$(3/5) + (4/5)i$	$-(3/10) + (1/10)i$	$(4/11) - (1/11)i$	$(1/3) - (1/3)i$	$-(1/2) + (1/2)i$	0	-1
41	-1	$1 - i$	$-1 - i$	$(1/2) + (1/2)i$	0	0	-1
42	$-(3/5) - (4/5)i$	$(7/10) + (1/10)i$	$(4/15) - (1/5)i$	$-(1/25) + (7/25)i$	$(7/10) + (1/10)i$	0	-1
43	-3	$(1/10) + (1/10)i$	$(19/17)i$	$(1/10) - (1/10)i$	$-(1/3)$	$(1/2) + (1/2)i$	-1
44	-1	$(1/10) + (1/10)i$	$(19/17)$	$-(1/10) + (1/10)i$	$(1/3)i$	$(1/2) + (1/2)i$	-1
45	-1	$i$	$(1/2)i$	$(1/5)$	$(1/2)i$	$i$	-1
46	1	-1	$-(1/2)$	$(1/5)i$	$-(1/2)$	-1	-1
47	-1	$(1/2) - (1/2)i$	$i$	$-(1/2) + (1/2)i$	$-(1/3)$	$(1/2) + (1/2)i$	-1
48	1	$(1/2) + (1/2)i$	$(1/3)i$	$-1 + i$	$(1/2) - (1/2)i$	0	-1
49	-1	$-(1/2) + (1/2)i$	$i$	$-(1/2) + (1/2)i$	$(1/3)$	$(1/2) + (1/2)i$	-1
50	-1	$-i$	$(1/2)i$	$(3/5) + 0.0i$	$(1/2)i$	$i$	-1
51	1	$-(1/2) - (1/2)i$	$(2/3) - (1/3)i$	$-(1/7) - (1/7)i$	$(3/2)0 + (1/2)i$	0	-1
52	$(3/5) + (4/5)i$	$-(3/10) + (1/10)i$	$-(2/11) + (1/11)i$	$(1/3) + (1/3)i$	$-(1/2) - (1/2)i$	0	-1
53	1	$-(1/2) - (1/2)i$	$(2/3) + (1/3)i$	$1 + i$	$-(1/2) - (1/2)i$	0	-1
54	-1	$-(1/2) + (1/2)i$	$(2/3) - (1/3)i$	$-(1/2) + (1/2)i$	-1	$(1/2) - (1/2)i$	-1
55	-1	$(1/2) - (1/2)i$	$-(1/3) - (2/3)i$	$-(1/2) + (1/2)i$	$i$	$(1/2) - (1/2)i$	-1
56	-1	$-(1/2) + (1/2)i$	$(2/3) - (1/3)i$	$-(1/2) + (1/2)i$	1	$-(1/2) + (1/2)i$	-1
57	1	$(1/2) + (1/2)i$	$-(2/3) + (1/3)i$	$1 + i$	$-(1/2) - (1/2)i$	0	-1
58	$-i$	1	$(1/4) - (1/4)i$	$(4/9) + (1/9)i$	$(1/7) + (2/14)i$	$(3/2)0 - (1/2)i$	-1
59	-1	$-(1/2) + (1/2)i$	$i$	$-(1/2) + (1/2)i$	$(1/3) - (2/3)i$	$-(1/2) + (1/2)i$	-1
60	$-1 - 2i$	$(1/3) + (1/3)i$	$(1/2) - (5/22)i$	$-(2/5) + (2/5)i$	$(1/3)i$	$(1/2) + (1/2)i$	-1
61	1	$-(1/2) + (1/2)i$	$-(2/3) + (1/3)i$	$-(1/2) + (1/2)i$	1	$-(1/2) - (1/2)i$	-1
62	1	$(1/2) - (1/2)i$	-1	$(1/2) - (1/2)i$	$(2/3) + (1/3)i$	$-(1/2) + (1/2)i$	-1
63	-1	$-(1/2) - (1/2)i$	$-(2/3) - (1/3)i$	$1 + i$	$-(1/2) - (1/2)i$	0	-1
64	-1	$(1/2) - (1/2)i$	$-(2/3) - (1/3)i$	$-(1/2) + (1/2)i$	1	$-(1/2) - (1/2)i$	-1
65	-1	$-i$	$-(1/2)$	1	$-(1/2)$	$i$	-1
66	-1	$(1/2) - (1/2)i$	$-(2/3) - (1/3)i$	$(1/7) + (5/7)i$	$(1/2) - (3/2)0i$	0	-1
67	$(3/5) + (4/5)i$	$(1/10) + (3/10)i$	$-(2/11) - (5/11)i$	$(1/3) + (1/3)i$	$-(1/2) - (1/2)i$	0	-1
68	-1	$(1/2) + (3/2)0i$	$-(5/7) - (4/7)i$	$(1/10) - (1/2)i$	$(1/3)i$	$-(1/2) + (1/2)i$	-1
69	1	$(1/2) - (1/2)i$	-1	$(1/2) + (1/2)i$	$i$	$(1/2) + (1/2)i$	-1
70	$-(3/5) - (4/5)i$	$-1 + (7/10)i$	$-(2/3) - (1/3)i$	$(1/70) - (1/10)i$	$(1/5) - (2/55)i$	$-(3/10) + (1/10)i$	-1
71	1	$(1/2) - (1/2)i$	$i$	$(1/2) - (1/2)i$	-1	$(1/2) - (1/2)i$	-1
72	-1	$(1/2) - (1/2)i$	$i$	$1 - i$	$-(1/2) - (1/2)i$	0	-1
73	$1 + 2i$	$(2/3)i$	$-(2/13) + (1/13)i$	$-(3/4) + (1/4)i$	1	0	-1
74	1	$(1/2) - (1/2)i$	$i$	$(1/2) - (1/2)i$	$-1 - (2/3)i$	$(1/2) + (1/2)i$	-1
75	$1 + 2i$	$(1/3) - (1/3)i$	$-1 + i$	$-(1/2) - (1/2)i$	0	0	-1
76	1	$(1/2) - (1/2)i$	$-2 + i$	$(1/3) - (1/3)i$	$-(1/2) - (1/2)i$	0	-1
77	$1 + 2i$	$-1 - i$	$-(1/3) + (1/3)i$	$(1/2) + (1/2)i$	0	0	-1
78	$-(3/5) - (4/5)i$	$-(1/10) + (7/10)i$	$-(2/5) - (1/5)i$	$-(1/3) - (1/3)i$	$(1/2) - (1/2)i$	0	-1
79	$-(3/5) - (4/5)i$	$-(1/10) + (7/10)i$	$-(2/5) - (1/5)i$	$(1/3) - (1/3)i$	$-(1/2) + (1/2)i$	0	-1

## 7. Zaključak

U ovoj disertaciji je data opšta kanonična forma u kojoj može da se predstavi proizvoljan komplementarni par sekvence. Pokazana je veza između komplementarnih sekvenci i paraunitarnih matrica. Uveden je pojam omega vektora; on se može izračunati za svaki komplementarni par. Takođe, za bilo koji omega vektor može da se izračuna komplementarni par. To znači da između komplementarnih parova sekvenci i omega vektora postoji preslikavanje 1-na-1.

Drugi značajan rezultat je kompaktna kanonična forma koja dovodi do realizacije efikasnog korelatora. Do sada je u literature naveden efikasni korelator za standardne binarne i polifazne sekvence. Sada se može naći za bilo koji par za koji je stepen kompaktnosti kanonične forme veliki. Direktnom primenom ove teorije izvedena je dekompozicija Golejevog binarnog kernela dužine 10 i konstruisan efikasni korelator za sekvence dužine  $2^M 10^N$ . Teorija je primenjena i za to da se nađe rekurzivni algoritam za 16-QAM i 64-QAM komplementarne sekvence.

Teorija je takođe primenjena na brojne kernele i nestandardne sekvence ali za sada se nije pokazalo da postoje takve sekvence za koje postoji efikasni korelator. Kernel 10 je za sada jedini izuzetak.

Dalji rad u ovom pravcu pre svega treba nastaviti na skupovima komplementarnih sekvenci. Ta oblast je posebno interesantna za rešavanje PAPR problema u OFDM sistemima.

Pored toga postoji nekoliko familija sekvenci koje nisu obuhvaćene ovom disertacijom a to su, recimo, ternarne komplementarne sekvence i Humanove komplementarne sekvence. Te familije mogu biti zanimljive za primenu u radarstvu ali i za neke druge primene.

## Literatura

[Altes 82] Altes, R.A.; "Radar/Sonar Signal Design for Bounded Doppler Shifts", IEEE Transactions on Aerospace and Electronic Systems, July 1982, Vol. AES-18, Issue:4

[Alvarez 06], Alvarez F J, Hernandez A, Urena J, etc. "Real-time implementation of an efficient correlator for complementary sets of four sequences applied to ultrasonic pulse compression systems" J. Microprocessors and Microsystems, 2006, 30(1): pp. 43-51.

[An 05] An M.; Byrnes J., Moran W.; Saffari B.; Shapiro H. S.; Tolimieri R.: "Pons, Reed-Muller Codes, and Group Algebras" Computational Noncommutative Algebra and Applications (2005) 136: 155-196, January 01, 2005

[Barker 53] Barker R.H.: "Group synchronizing of binary digital systems", Communication Theory (W. Jackson, ed.), Academic Press, New York, 1953, pp. 273-287.

[Borwein 03] Borwein P. B., Ferguson R. A., "A complete description of Golay pairs for lengths up to 100", Mathematics of Computation, Vol. 73, Issue 246, pp. 967-985, 2003

[Braun 98] Braun, V.: "Dipulse-response measurement of a magnetic recording channel using Golay complementary sequences", IEEE Transactions on Magnetics, Jan 1998, vol.: 34 Issue:1, pp. 309-316

[Budišin 87] S. Budišin, B. Popović, I. Inđin, "Designing radar signals using complementary sequences", International conference Radar 87, London, 1987.

[Budišin 89] S. Budišin, "Fast PN sequence correlation by using FWT", Proceedings of MELECON 89, Lisabon, April 1989.

[Budišin 90A] S. Budišin, "New complementary pairs of sequences", IEE Electronics Letters, Vol. 26, No. 13, June 1990, pp. 881-883.

[Budišin 90B] S. Budišin, "New multilevel complementary pairs of sequences", IEE Electronics Letters, Vol. 26, No. 22, Oct. 1990, pp. 1861-1863.

[Budišin 90C] S. Budišin, "Complementary Huffman sequences", IEE Electronics Letters, Vol. 26, No. 8, April 1990, pp. 533-534.

[Budišin 91] Budišin, S.Z.: "Efficient pulse compressor for Golay complementary sequences", Electronics Letters, 31 Jan. 1991, Volume: 27, Issue: 3, pp. 219- 220

[Budišin 92] S. Budišin, "Golay complementary sequences are superior to PN sequences", IEEE International Conference on Systems Engineering, Sept. 1992, pp. 101-104

[Budišin 11] S. Budišin, "Golay kernel 10 decomposition“, Electronics Letters, Vol. 47, No. 15, Jul. 2011, pp. 853-855.

[Calderbank 06] A. R. Calderbank, S. D. Howard, W. Moran, A. Pezeshki, and M. Zoltowski, "Instantaneous radar polarimetry with multiple dually-polarized antennas," in Conf. Rec. 40th Asilomar Conf. Signals, Systems and Computers, Pacific Grove, CA, Oct. 2006, pp. 757-761.

[Candan 06] Candan, C.: "Derivation of length extension formulas for complementary sets of sequences using orthogonal filterbanks", Electronics Letters, November 23 2006, Volume: 42 , Issue: 24, pp. 1427-1428

[Chan 03] Chan V.C., Venkataramani R., Tarokh V.: 'A new construction of 16-QAM Golay complementary sequences', IEEE Transactions on IT, 2003, Vol.: 49 Issue: 11, pp. 2953- 2959.

[Chang 10] C. Y.Chang, Y. Li and J. Hirata, "New 64-QAM Golay Complementary Sequences", IEEE Trans. Inf. Theory, vol.56, no.5, pp. 2479-2485, May 2010.

[Chitrapu 04] Chitrapu P.: "Wideband TDD – WCDMA for the Unpaired Spectrum", 2004, John Wiley & Sons Ltd.

[Chong 03] C. V.Chong, R. Venkataramani and V. Tarokh, "A New Construction of 16-QAM Golay Complementary Sequences", IEEE Trans. Inf. Theory, vol. 49, no. 11, pp. 2953-2959, Nov. 2003.

[Davis 99] Davis J.A., Jedwab J.: "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," IEEE Trans. Inform. Theory, Vol 45, No 7, pp 2397-2417, Nov 1999

[Diaz 99] V. Diaz, J. Urena, J. J. Garcia, M. Mazo, E. Bueno and A. Hernandez, "Using Golay complementary sequences for multi-mode ultrasonic operation", in Proc. 7th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA99), vol. 1, 1999, pp. 599-604.

[ERICSSON 99] ERICSSON, : 'New RACH preambles with low auto-correlation sidelobes and reduced detector complexity'. TSG-RAN Working Group 1 meeting No.3, TSGR1#3(99)205, Nynashamn, Sweden, 22-26 March 1999

[Fiedler 10] Fiedler F., Jedwab J. , and Wiebe A. : "A new source of seed pairs for Golay sequences of length 2m", J. Combin. Theory (A) 117 (2010), pp.589-597.

[Foster 1986] Foster, S. "Impulse response measurements using Golay codes," in IEEE, 1986, Conference on Acoustics, Speech, and Signal Processing (ICASSP), New York!, Vol. 2, pp. 929–932.

[Frank 80] Frank, R.: "Polyphase complementary codes", IEEE Transactions on Information Theory, Nov 1980, Volume: 26, Issue: 6, pp: 641- 647

[Ghani 10] Ghani F., Shafiza N., "Complementary Sequences in DSP Based Testing of Electronic Systems", International Journal of Engineering & Technology IJET-IJENS Vol:10 No:2 2010

[Gibson 2011b] Gibson R.G. , Jedwab J. , "Quaternary Golay sequence pairs II: odd length," Des. Codes Cryptogr. vol. 59 pp.147-157, 2011.

[Gibson 2011a] Gibson R.G., Jedwab J. , "Quaternary Golay sequence pairs I: even length," Des. Codes Cryptogr. vol. 59 pp.131-146, 2011.

[Golay 49] Golay M. J. E.: "Multislit spectroscopy". *J. Opt. Soc. Amer.* **39**: pp. 437-444.

[Golay 61] Golay M. J. E.: "Complementary series". *IRE Trans. Inform. Theory* **IT-7**: 82–87.

[Golay 62] Golay M. J. E.: "Note on Complementary series". Proc. IRE 50: 84.

[Golay 77] Golay M. J. E.: "Sieves for low autocorrelation binary sequences," IEEE Transactions on Information Theory, vol. IT-23, no. 1, pp. 43-51, Jan. 1977.

[Golomb 64] Golomb S. W. , Ed., "Digital Communications with Space Applications". Englewood Cliffs, NJ: Prentice-Hall, 1964.

[Golomb 67] Golomb S., "Shift Register Sequences", San Francisco, Holden-Day, 1967

[Harman 05] K. Harman and B. Hodgins, "Next generation of GUIDAR technology," IEEE Aerosp. Electron. Syst. Mag., vol. 20, no. 5, pp. 16-26, Mar. 2005.

[Hernandez 03] A. Hernandez, J. Urena, D. Hernanz, J. J. Garcia, M. Mazo, J. P. Derutin, J. Serot and S. Palazuelos, "Real-time implementation of an efficient Golay correlator (EGC) applied to ultrasonic sensorial systems", Microprocessors and Microsystems, no. 27, pp. 397-406, 2003.

[Howard 06] S. D. Howard, A. R. Calderbank, and W. Moran, "A simple polarization diversity technique for radar detection," in Proc. 2nd Int. Conf. Waveform Diversity and Design, Lihue, HI, Jan. 2006.

[Howard 07] S. D. Howard, A. R. Calderbank, and W. Moran, "A simple signal processing architecture for instantaneous radar polarimetry," IEEE Trans. Inf. Theory, vol. 53, no. 4, pp. 1282-1289, Apr. 2007.

[Huang 11] Huang Y-W, Li Y.: "16-QAM Golay complementary sequences with new sequence lengths", 2011 IEEE International Symposium on Information Theory Proceedings (ISIT), pp: 698-702

[IEEE 802.11b] IEEE 802.11b-1999, na WEB stranici:  
<http://standards.ieee.org/getieee802/download/802.11b-1999.pdf>

[IEEE 802.16] IEEE Std 802.16: IEEE standard for local and metropolitan area networks—Part 16, pp. 960-968, May 2009.

[Jaugogui 62] S. Jaugogui, "Complementary Sequences of Length 26," IEEE Trans. Inform. Theory, vol. it-8, no. 4, p. 323, July 1962

[Jedwab 07] Jedwab, J. Parker, M. G.: "Golay complementary array pairs", DESIGNS CODES AND CRYPTOGRAPHY 2007, VOL 44; NUMBER 1-3, pp: 209-216

[Karkkainen 94] H. A Karkkainen and P. A Leppanen, "Linear Equivalence of binary Golay Complementary Sequences", IEEE PIMRC94, pp755-759

[Lee 06] Lee, H., Golomb, S.W., "A new construction of 64-QAM golay complementary sequences", IEEE Transactions on Information Theory, April 2006, Volume: 52, Issue: 4, pp: 1663-1670

[Li 05] Li, Y., Chu, W. B.: "More Golay sequences", IEEE Transactions on Information Theory, March 2005, Volume: 51, Issue: 3, pp: 1141- 1145

[Li 08] Li Y,: 'Comments on "A New Construction of 16-QAM Golay Complementary Sequences" and Extension for 64-QAM Golay Sequences' IEEE Transactions on Information Theory, July 2008, Volume: 54, Issue: 7, pp: 3246-3251

[Li 09] Li Y., Huang Y-W.: "New QAM Golay complementary pairs with unequal sequence power", IISIT 2009. IEEE International Symposium on nformation Theory, 2009, pp: 433- 437

[Murnaghan 62] Murnaghan F. D.: "The Unitary and Rotation Groups". Washington, DC: Spartan Books, 1962.

[Parker 00] Parker M.G.: "Constabent Properties of Golay-Davis-Jedwab Sequences, ISIT2000, Sorrento, Italy, June 25-30, 2000

[Parker 04] Parker M. G., Paterson K. G., Tellambura C.: "Golay Complementary Sequences", January 19, 2004

[Paterson 00] Paterson, K.G.: "Generalized Reed-Muller codes and power control in OFDM modulation", IEEE Transactions on Information Theory, Jan 2000, Volume: 46, Issue: 1, pp: 104-120

[Pérez 10] Pérez, M.C., Ureña, J., De Marziani, C., Hernández, A., García, J.J., Álvarez, F.J.: "Very efficient correlator for loosely synchronised codes", Electronics Letters, August 5 2010, Volume: 46, Issue: 16, pp: 1127-1129

[Pezeshki 08] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, "Doppler resilient Golay complementary waveforms," IEEE Trans. Inf. Theory, vol. 54, pp. 4254-4266, Sep. 2008.

[Phoong 03] Phoong S. M., Lin Y. P.: "Lapped Hadamard transforms and filterbanks," in Proc. Int. Conf. Acoust. Speech, Signal Processing, Apr. 2003

[Phoong 05] Phoong S. M., Chang K. Y.: "Antipodal Paraunitary Matrices and their applications to OFDM Systems," IEEE Trans. Signal Process., vol. 53, no. 4, pp. 1374-1386, Apr. 2005

[Popovic 91] Popovic, B.M.: "Synthesis of power efficient multitone signals with flat amplitude spectrum", IEEE Transactions on Communications, Jul 1991, Volume: 39, Issue: 7, pp: 1031- 1033

[Popović 99] Popović, B. M.: "Efficient Golay correlator", Electronics Letters, 19 Aug 1999, Volume: 35, Issue: 17, pp: 1427-1428

[Popovic 99A] Popovic, B. M.: "Spreading sequences for multicarrier CDMA systems", IEEE Transactions on Communications, Jun 1999, Volume: 47, Issue: 6, pp: 918-926

[Roßing 01] C. Roßing and V. Tarokh, "A construction of OFDM 16-QAM sequences having low peak powers", IEEE Trans. Inf. Theory, vol.47, no. 5, pp.2091-2094, Nov. 2001.

[Rudin 59] Rudin, W., "Some Theorems on Fourier Coefficients", Proc. Amer. Math. Soc. 10 (1959), pp: 855-859

[Rudolf 01] Rudolf, M., Jechoux, B.: "Design of concatenated extended complementary sequences for inter-base station synchronization in WCDMA TDD mode", IEEE Global Telecommunications Conference, 2001. GLOBECOM '01, 2001, p: 674- 679

[Searle 07] S. J. Searle and S. D. Howard, "A novel polyphase code for sidelobe suppression," in Proc. Int. Waveform Diversity and Design Conf., Pisa, Italy, Jun. 2007, pp. 377-381.

[Searle 07A] S. J. Searle and S. D. Howard, "A novel nonlinear technique for sidelobe suppression in radar," in Proc. Int. Conf. Radar Systems, Edinburgh, U.K., Oct. 2007.

[Shao 04] Shao-bo Liu, Aiping Huang, Zhao-yang Zhang, and Zhijian Zhang, "Performance Analysis of CCK Modulation under Multipath Fading Channel", Proceedings of the 6th Nordic Signal Processing Symposium – NORSIG 2004, June 9-11, 2004, Espoo, Finland

[Shapiro 51] Shapiro H.S. , "Extremal Problems for Polynomials and Power Series", Sc.M. thesis, MIT, 1951

[Sivaswamy 78] Sivaswamy, R.: 'Digital and analog subcomplementary sequences for pulse compression', IEEE Trans., 1978, AES-14, pp. 343-350

[Sivaswamy 82] Sivaswamy, R.: 'Self-clutter cancellation and ambiguity properties of subcomplementary sequences', *ibid.*, 1982, AES-18, pp. 163-181

[Sivaswamy 78] Sivaswamy, R.: "Multiphase Complementary Codes", IEEE Transactions on Information Theory, Sep 1978, Volume: 24, Issue: 5, pp: 546- 552

[Spasojević 01] Spasojević P., Georghiades C. N.: "Complementary sequences for ISI channel estimation," IEEE Trans. Inform. Theory, vol. 47, pp. 1145-1152, Mar. 2001

[Tseng 72] Tseng C. C.: "Complementary sets of sequences", IEEE Transactions on Information Theory, , Sep 1972, Volume: 18, Issue: 5, pp: 644- 652

[Turyn 63] Turyn R., "Ambiguity Functions of Complementary Sequences", IEEE Transactions On Information Theory, Vol. IT-9, pp. 46-47, January 1963.

[Vaidyanathan 93] Vaidyanathan P. P.: "Multi-rate systems and filter banks", Prentice Hall, 1993

[van Nee 96] van Nee, R.D.J.: "OFDM codes for peak-to-average power reduction and error correction", Global Telecommunications Conference, 1996. GLOBECOM '96. 'Communications: The Key to Global Prosperity, Volume: 1 ,pp: 740- 744

[Wang 07] Wang S., Abdi A.: "MIMO ISI Channel Estimation Using Uncorrelated Golay Complementary Sets of Polyphase Sequences", IEEE Transactions on Vehicular Technology, Volume: 56 Issue:5, Sept. 2007

[Welti 60] Welti G. R., "Quaternary Codes for Pulsed Radar", IRE Transactions on Information Theory, Vol. IT-6, pp. 400-408, June 1960