Neperiodična binarna zaporedja z dobrimi avtokorelacijskimi lastnostmi: nizke vrednosti stranskih režnjev

Janez Brest, Borko Bošković

Laboratorij za računalniške arhitekture in jezike,
Inštitut za računalništvo,
Fakulteta za elektrotehniko, računalništvo in informatiko,
Univerza v Mariboru,
Koroška cesta 46, 2000 Maribor, Slovenija
E-pošta: janez.brest@um.si, borko.boskovic@um.si

Aperiodic Binary Sequences with Good Autocorrelation Properties: Low Peak Side-lobe Levels Values

In this short review paper, aperiodic binary sequences with good autocorrelation properties are presented. The Peak Side-Lobe Level (PSL) value of a binary sequence should be as small as possible. Algorithms for tackling this optimization problem have difficulties when searching for long binary sequences with low PSL values due to the huge search space. Our main focus is an analysis of the best-known results in the literature for aperiodic binary sequences of selected lengths.

1 Uvod

Binarna zaporedja z dobrimi avtokorelacijskimi lastnostmi so zelo uporabna v praksi. Srečamo jih v fiziki, kemiji, digitalnih komunikacijah, procesiranju signalov in kriptografiji. Iskanje binarnih zaporedij glede na definirane kriterije je znan in precej dobro preučen problem. V literaturi znani metriki sta najvišji nivo stranskega režnja (Peak Sidelobe Level, PSL) [17] in MF (Merit factor) [16].

V splošnem ločimo dve vrsti avtokorelacij in sicer:

- periodične in
- aperiodične ali neperiodične.

V tem članku se bomo omejili le na aperiodični problem binarnih zaporedij in na metriko najvišjega stranskega režnja. Bralec, ki želi izvedeti več o drugi metriki (merit factor) in nedavnih rezultatih, je napoten na literaturo: [4, 6, 10].

Pri danem binarnem zaporedju S:

$$S = (s_0, s_1, \ldots, s_{L-1}), \tag{1}$$

kjer L označuje dolžino binarnega zaporedja, imajo elementi $s_i, i \in \{0, L-1\}$ vrednost $+1$ ali -1.

Aperiodična avtokorelacijska funkcija binarnega zaporedja S pri zamiku k je definirana kot:

$$C_k(S) = \sum_{i=0}^{L-k-1} s_i s_{i+k}, \quad \text{za } k = -(L-1), \ldots, -1, 0, 1, \ldots, L-1. \tag{2}$$

Metrika, s katero opišemo kvaliteto binarnega zaporedja, je najvišji nivo stranskega režnja, PSL, in je definirana [18]:

$$PSL(S) = \max_{k=1}^{L-1} |C_k(S)|. \tag{3}$$

Cilj je poiskati binarna zaporedja, ki imajo minimalno vrednost PSL. C_0 imenujemo *glavni reženj*, ostali $(C_k, k = 1, 2, ..., L-1)$ pa predstavljajo *stranske režnje*. Stranski režnji so simetrični, kar lahko vidimo tudi v enačbi (2), in se pojavijo na obeh straneh ob glavnem režnju.

Nadaljevanje članka je sledeče. V 2. poglavju prikažemo izračun vrednosti na primeru kratkega aperiodičnega binarnega zaporedja. V 3. poglavju opravimo pregled najnovejše literature na področju iskanja aperiodičnih binarnih zaporedij z nizkimi avtokorelacijskimi lastnostmi in podamo pregled najboljših znanih binarnih zaporedij z nizkimi vrednostmi PSL glede na dolžino zaporedij. V 4. poglavju opravimo analizo rasti najboljših vrednosti PSL za zaporedja izbranih dolžin do velikosti približno 2000. Sledi zaključno poglavje, kjer izpostavimo smernice za nadaljnje raziskave.

2 Zgled

Prikažimo izračun avtokorelacijskih funkcij na binarnem zaporedju s sedmimi elementi ($L = 7$):

$$S = (s_0, s_1, s_2, s_3, s_4, s_5, s_6).$$

S pomočjo enačbe (2) izračunamo avtokorelacijske funkcije C_k:

$$\begin{aligned}
C_1 &= s_0s_1 + s_1s_2 + s_2s_3 + s_3s_4 + s_4s_5 + s_5s_6,\\
C_2 &= s_0s_2 + s_1s_3 + s_2s_4 + s_3s_5 + s_4s_6,\\
C_3 &= s_0s_3 + s_1s_4 + s_2s_5 + s_3s_6,\\
C_4 &= s_0s_4 + s_1s_5 + s_2s_6,\\
C_5 &= s_0s_5 + s_1s_6,\\
C_6 &= s_0s_6.
\end{aligned}$$

Člen C_0 smo izpustili, saj ni vključen v enačbo (3). Omenimo, da ima vsak C_k natanko $L-k$ elementov. Za nekaj

primerov zaporedij za $L = 7$ izračunajmo vrednosti PSL:

$$\begin{aligned} S &= (1,1,1,1,1,1,1), & PSL &= 6; \\ S &= (-1,-1,-1,1,1,1,1), & PSL &= 4; \\ S &= (1,-1,1,1,1,1,1), & PSL &= 3; \\ S &= (1,1,1,-1,-1,1,-1), & PSL &= 1; \end{aligned}$$

Za zadnja dva primera zaporedij so avtokorelacijske funkcije prikazane na sliki 1. Zaporedje, kjer je $PSL = 1$, je tudi optimalno za dolžino 7 in je znano kot Barkerjevo zaporedje. Omenimo še, da je najdaljše binarno Barkerjevo zaporedje (zaporedja s $PSL = 1$) znano za $L = 13$.

Pri majhnih vrednostih L (kratka binarna zaporedja) lahko optimalno (minimalno) vrednost PSL izračunamo z *eksaktnim algoritmom*, s katerim izračunamo vrednost PSL za vse možne razvrstitve -1 in 1 v danem binarnem zaporedju. Vseh možnosti je 2^L, zato problem iskanja binarnih zaporedij z nizkimi avtokorelacijami spada med probleme z eksponentno časovno zahtevnostjo.

3 Pregled literature in znanih najboljših vrednosti PSL

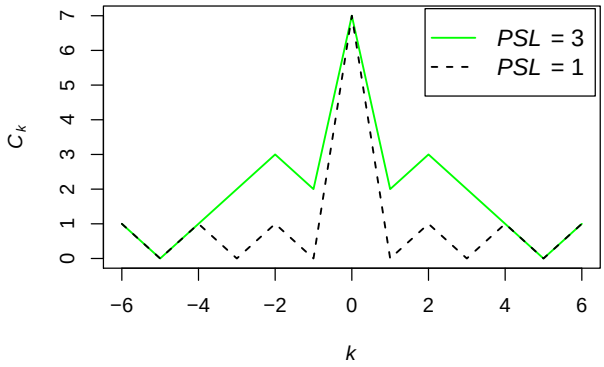
Ker je problem iskanja dolgih binarnih zaporedij eksponentne narave, se raziskovalci in znanstveniki lotevajo naslednjih možnosti pri reševanju problema iskanja zaporedij z dobrimi avtokorelacijskimi lastnostmi:

- konstrukcijske metode in
- hevristični algoritmi.

Konstrukcijske metode [7] omogočajo, da z dokaj preprostimi postopki načrtujemo binarna zaporedja, lahko tudi zelo dolga, to je za poljubno dolžino (nekatere konstrukcijske metode imajo omejitve, npr. možno jih je uporabiti le za dolžine $L = 2^n, n \in \mathbb{N}$), a imajo tako dobljena binarna zaporedja vrednosti PSL, ki so precej oddaljena od optimalnih vrednosti. Konstrukcijske metode poznamo že od leta 1950 [7].

Hevristični algoritmi prav tako ne zagotavljajo, da bi vedno našli binarna zaporedna z najmanjšimi možnimi (optimalnimi) vrednostmi – lahko pa uspejo najti solidne rešitve. Tudi s hevrističnimi algoritmi se lahko lotimo iskanja zaporedij, ki so nekoliko daljša. Hevristične algoritme lahko dalje razdelimo v dve skupini. Prvi med postopkom iskanja uporabljajo le eno rešitev (npr. simulirano ohlajanje) in jo postopoma poskušajo izboljševati, drugi pa so populacijski algoritmi, ki med preiskovanjem uporabljajo več rešitev, ki jim rečemo populacija. Primeri populacijskih algoritmov so: evolucijski algoritmi, algoritmi za optimizacijo z roji delcev itd. Pri iskanju binarnih zaporedij so učinkoviti tudi hevristični algoritmi, ki uporabljajo le eno rešitev in vključujejo mehanizem ponovnih zagonov (restartov) [5]. Uporabo hevrističnih algoritmov za iskanje binarnim zaporedij z nizkimi vrednostmi stranskih režnjev najdemo v [6, 12].

Barkerjeva zaporedja so splošno znana zaporedja, ki imajo odlične aperiodične avtokorelacijske lastnosti, vendar je velikost najdaljšega poznanega Barkerjevega zaporedja enaka 13, kar pa je ponavadi premalo za uporabo v praktičnih aplikacijah.



Slika 1: Primera avtokorelacijskih funkcij s $PSL = 3$ in $PSL = 1$ za binarni zaporedji dolžine $L = 7$.

K.U. Schmidt [24] je predlagal konstrukcijsko metodo za aperiodična binarna zaporedja z vrednostmi PSL, ki niso višja od $\sqrt{L \ln(2L)}$ in njihove vrednosti PSL bi naj rastle z redom $\sqrt{L \ln(\ln L)}$, vendar slednje ni dokazano.

Obstaja precej konstrukcijskih metod, a nobena od njih ne zagotavlja, da bi generirana binarna zaporedja imela najnižjo možno vrednost PSL [12].

Precej računskega napora je bilo vloženega v iskanje binarnih zaporedij z nizkimi vrednostmi PSL [19, 22, 24]. Dandanes so najboljše znane vrednosti PSL (ki bi naj bile tudi optimalne) za binarna zaporedja dolžine $86 \leq L \leq 105$ objavljene v [22].

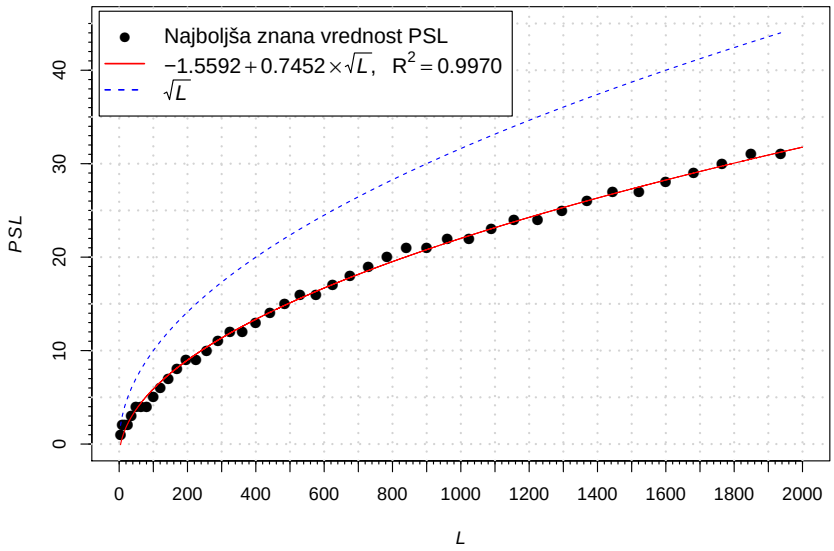
Za daljša zaporedja so poznane le najboljše znane vrednosti (ang. best-known results) in pregled literature naredimo glede na dolžino zaporedij:

- rezultate za zaporedja $106 \leq L \leq 300$ najdemo v [6, 12, 13],
- za izbrane dolžine na intervalu $301 < L \lessapprox 4000$ v prispevkih [6, 7, 8, 9, 13, 15, 21, 23, 25],
- za nekatere dolžine L od 4000 do 8191 v prispevkih [2, 3] in
- za najdaljše (tudi do dolžine 10^6) lahko najdemo v literaturi: [6, 7, 11, 20].

V zadnjem času je bilo objavljenih precej člankov o binarnih zaporedjih in zanimivo je, da v teh člankih lahko zasledimo precejšnje izboljšanje eksperimentalnih rezultatov, ki niso le odraz povečane zmogljivosti računalniških sistemov.

4 Rast najboljših znanih vrednosti PSL

Pri binarnih zaporedjih raziskovalce in znanstvenike zanima (asimptotična) odvisnost vrednosti PSL od njihove dolžine. Kot zanimivost povejmo, da matematični dokazi potekajo v smeri preučevanja ne le izbranih razredov zaporedij, ampak vseh binarnih zaporedij. V literaturi zasledimo, da je rast vrednosti PSL *skoraj vseh binarnih*



Slika 2: Rast vrednosti PSL glede na dolžino binarnih zaporedij (L) za $L = m^2, 4 \leq m \leq 44, m \in \mathbb{N}$.

zaporedij dolžine L:

$$\Theta(\sqrt{L \ln L}). \tag{4}$$

Matematični dokaz najdemo v [1], v [14, 18] pa najdemo eksperimentalni dokaz, ki temelji na računalniških poskusih. Izraz skoraj vseh uporabljamo, saj obstajajo razredi binarnih zaporedij, ki odstopajo od enačbe (4), npr. binarna zaporedja, kjer imajo vsi elementi vrednost +1.

Prav tako zanimivo vprašanje se glasi: kako je z rastjo najboljših znanih vrednosti PSL v odvisnosti od njihove dolžine? Preden nadaljujemo, opozorimo na dve zadevi: v enačbi (4) nastopajo skoraj vsa binarna zaporedja (v tem primeru govorimo o rasti povprečnih vrednosti) in da so optimalne vrednosti PSL znane za $L \leq 105$. V nadaljevanju bomo na slednje vprašanje odgovorili za izbrane dolžine binarnih zaporedij do velikosti približno 2000. Za omenjene dolžine so se v zadnjem času v literaturi pojavili algoritmi, ki dokaj uspešno rešujejo problem iskanja binarnih zaporedij z dobrimi avtokorelacijskimi lastnostmi.

Slika 2 prikazuje aproksimacijo trenutno znanih najboljših vrednosti PSL aperiodičnih binarnih zaporedij, ki imajo dolžino:

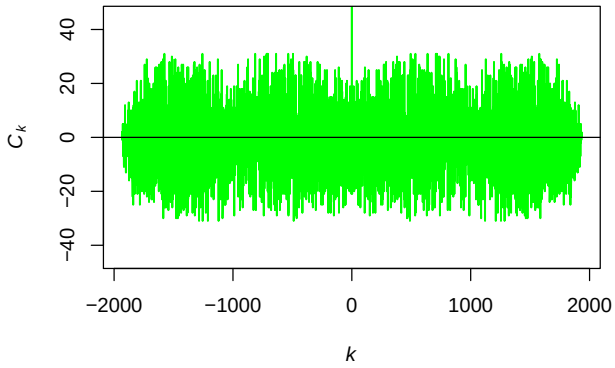
$$L = m^2,\ m \in \{4, 5, \cdots, 44\} \tag{5}$$

in jo primerja z rastjo $\sqrt{L}$. Torej izbrane vrednosti L so 16, 25, 36, ..., 1936 in za njih velja, da je $m^2 < 2000$. Dobljene vrednosti PSL najdemo v literaturi: [13] ter [6] (dodali smo še nekaj izračunanih vrednosti naših zadnjih raziskav). Opazimo lahko, da je $\sqrt{L}$ (na sliki 2 označeno z modro barvo) precej višje, kot je aproksimacija najboljših znanih vrednosti PSL (na sliki označeno z rdečo barvo). Omenjena aproksimacija sledi krivulji, ki jo prikazuje enačba (6):

$$0.7452\sqrt{L} - 1.5592 \tag{6}$$

Sama aproksimacija s kvadratnim polinomom se lepo ujema, saj je statistična vrednost $R^2 = 0.997$. Iz dobljenega pa žal ne moremo sklepati, kako je z rastjo najboljših binarnih zaporedij pri zelo velikih dolžinah, npr. $L > 10^6$, saj pri teh dolžinah postanejo tudi najboljši hevristični algoritmi časovno preveč zahtevni in seveda tudi premalo zmogljivi.

Matematični dokaz ali pa vsaj računalniški eksperimenti tako ostajajo odprti pri ugotavljanju rasti vrednosti PSL aperiodičnih binarnih zaporedij.



Slika 3: Primer avtokorelacijskih funkcij s $PSL = 31$ za binarno zaporedje dolžine $L = 1936$.

Na sliki 3 vidimo primer avtokorelacijskih funkcij za binarno zaporedje dolžine $L = 1936$ ($44^2 = 1936$).

Glavni reženj C_0 je na sliki odrezan. Stranski režnji so simetrični glede na glavni reženj.

5 Zaključek

V preglednem članku smo predstavili aperiodična binarna zaporedja z nizkimi avtokorelacijskimi vrednostmi, kjer smo se omejili na nizke vrednosti stranskih režnjev oziroma vrednost PSL.

Opravili smo pregled nedavnih prispevkov, kjer smo se fokusirali na iskanje neperiodičnih binarnih zaporedij z nizkimi vrednostmi PSL in trenutno znanimi najboljšimi rezultati za izbrane dolžine do velikosti približno 2000. Na omenjenem intervalu smo opravili aproksimacijo najboljših vrednosti. Dobljena aproksimacija sledi krivulji $0.7452\sqrt{L} - 1.5592$, ki je nižja (to je boljša) kot $\sqrt{L}$.

Hevristični algoritmi, ki jih zasledimo v literaturi, imajo težave pri reševanju iskanja aperiodičnih binarnih zaporedij z nizkimi vrednostmi PSL zaradi velikosti iskalnega prostora, ki se glede na dolžino zaporedja povečuje eksponentno.

Nadaljnje raziskave na tem področju lahko potekajo v smeri opravljanja eksperimentov za višje dolžine binarnih zaporedij z uporabo zmogljive računalniške strojne opreme, katere zmogljivost se povečuje iz dneva v dan.

Zahvala

J. Brest in B. Bošković priznavata financiranje prispevka s strani Javne agencije za raziskovalno dejavnost Republike Slovenije, raziskovalni program P2-0041 – Računalniški sistemi, metodologije in inteligentne storitve.

Literatura

[1] Noga Alon, Simon Litsyn, and Alexander Shpunt. Typical peak sidelobe level of binary sequences. *IEEE transactions on information theory*, 56(1):545–554, 2009.

[2] Arindam Bose. *Waveform Synthesis for Active Sensing with Emerging Applications*. PhD thesis, University of Illinois at Chicago, 2021.

[3] Arindam Bose and Mojtaba Soltanalian. Constructing binary sequences with good correlation properties: An efficient analytical-computational interplay. *IEEE Trans. Signal Process.*, 66(11):2998–3007, 2018.

[4] Borko Bošković and Janez Brest. Two-phase Optimization of Binary Sequences with Low Peak Sidelobe Level Value. *arXiv preprint arXiv:2107.09801*, 2021.

[5] Borko Bošković, Franc Brglez, and Janez Brest. Low-Autocorrelation Binary Sequences: On Improved Merit Factors and Runtime Predictions to Achieve Them. *Appl. Soft Comput.*, 56:262–285, 2017.

[6] Janez Brest and Borko Bošković. Low Autocorrelation Binary Sequences: Best-Known Peak Sidelobe Level Values. *IEEE Access*, 9:67713–67723, 2021.

[7] Yutao Chen and Ronghao Lin. Computationally Efficient Long Binary Sequence Designs with Low Autocorrelation Sidelobes. *IEEE Trans. Aerosp. Electron. Syst.*, 2021.

[8] Gregory E Coxson, Connie R Hill, and Jon C Russo. Adiabatic quantum computing for finding low-peak-sidelobe codes. In *2014 IEEE High Performance Extreme Computing Conference (HPEC)*, pages 1–6. IEEE, 2014.

[9] Gregory E Coxson, Jon C Russo, and Angeline Luther. Long Low-PSL Binary Codes by Multi-Thread Evolutionary Search. In *2020 IEEE International Radar Conference (RADAR)*, pages 256–261. IEEE, 2020.

[10] Miroslav Dimitrov. New classes of binary sequences with high merit factor. *arXiv preprint arXiv.2206.12070*, 2022.

[11] Miroslav Dimitrov. On the Aperiodic Autocorrelations of Rotated Binary Sequences. *IEEE Commun. Lett.*, Dec, 2020.

[12] Miroslav Dimitrov, Tsonka Baicheva, and Nikolay Nikolov. Hybrid Constructions of Binary Sequences With Low Autocorrelation Sidelobes. *IEEE Access*, 9:112400–112410, 2021.

[13] Miroslav Dimitrov, Tsonka Baitcheva, and Nikolay Nikolov. On the Generation of Long Binary Sequences With Record-Breaking PSL Values. *IEEE Signal Process. Lett.*, 27:1904–1908, 2020.

[14] Denis Dmitriev and Jonathan Jedwab. Bounds on the growth rate of the peak sidelobe level of binary sequences. *Advances in Mathematics of Communications*, 1(4):461, 2007.

[15] Anna Dzvonkovskaya and Hermann Rohling. Long binary phase codes with good autocorrelation properties. In *2008 International Radar Symposium*, pages 1–4. IEEE, 2008.

[16] M Golay. The merit factor of Legendre sequences (corresp.). *IEEE Transactions on Information Theory*, 29(6):934–936, 1983.

[17] Jonathan Jedwab et al. A survey of the merit factor problem for binary sequences. In *SETA*, pages 30–55. Springer, 2004.

[18] Jonathan Jedwab and Kayo Yoshida. The peak sidelobe level of families of binary sequences. *IEEE transactions on information theory*, 52(5):2247–2254, 2006.

[19] Anatolii N Leukhin and Egor N Potekhin. Optimal peak sidelobe level sequences up to length 74. In *2013 European Radar Conference*, pages 495–498. IEEE, 2013.

[20] Ronghao Lin, Mojtaba Soltanalian, Bo Tang, and Jian Li. Efficient Design of Binary Sequences With Low Autocorrelation Sidelobes. *IEEE Trans. Signal Process.*, 67(24):6397–6410, 2019.

[21] Wai Ho Mow, Ke-Lin Du, and Wei Hsiang Wu. New evolutionary search for long low autocorrelation binary sequences. *IEEE Trans. Aerosp. Electron. Syst.*, 51(1):290–303, 2015.

[22] Carroll J Nunn and Gregory E Coxson. Best-known autocorrelation peak sidelobe levels for binary codes of length 71 to 105. *IEEE Trans. Aerosp. Electron. Syst.*, 44(1), 2008.

[23] K Veerabhadra Rao and V Umapathi Reddy. Biphase sequence generation with low sidelobe autocorrelation function. *IEEE Trans. Aerosp. Electron. Syst.*, AES-22(2):128–133, 1986.

[24] Kai-Uwe Schmidt. Binary sequences with small peak sidelobe level. *IEEE Trans. Inf. Theory*, 58(4):2512–2515, 2012.

[25] Mingxing Zhang, Zhengchun Zhou, Meng Yang, Zilong Liu, and Yang Yang. A hybrid algorithm for the search of long binary sequences with low aperiodic autocorrelations. *Soft Computing*, 25(20):12725–12744, 2021.