Elektrotehniški vestnik 70(1-2): 59–65, 2003
Electrotechnical Review, Ljubljana, Slovenija

Kodirni postopki na podlagi mrež

Rudolf Sušnik, Sašo Tomažič

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška c. 25, 1000 Ljubljana
E-pošta: rudolf.susnik@fe.uni-lj.si

Povzetek. Pomemben dejavnik pri kanalskem kodiranju so konstelacijski diagrami, ki ponazarjajo fizikalne lastnosti simbolov, ko ti postanejo električni impulzi. Gre za preoblikovanje nekega abstraktnega pojma v impulz s predpisano amplitudo in fazo. Učinkovitost prenosa je mogoče izboljšati s povečevanjem števila ortogonalnih nosilcev, oblikovanjem konstelacijskega diagrama kot celote in razporeditvijo simbolov oz. točk v diagramu. Razporeditev točk konstelacijskih diagramov najbolj razširjenih kodirnih postopkov ni posebej optimalna, zato iščemo boljše oblike od preprostega ekvidistančnega zlaganja simbolov v neodvisnih smereh. Ker simbol s prištetim šumom geometrijsko modeliramo s kroglo, problem kodiranja prevedemo na problem optimalnega zlaganja n-dimenzionalnih hiperkrogel. S povečevanjem števila dimenzij in optimizacijo konstelacijskega diagrama se želimo čim bolj približati Shannonovi meji kapacitete, žal pa hkrati s tem raste tudi zahtevnost izvedbe kodirnega postopka.

Ključne besede: večdimenzionalni kodirni postopki, grupe, mreže, optimalno zlaganje

Lattice based coding schemes

Extended abstract. Symbols in every channel coding scheme can be represented by constellations demonstrating their properties when applied to the physical channel. In the recent years, numerous researches have been made in the field of lattice codes. By using them one can achieve a few dB of the coding gain. Examples of such codes are the ones proposed to enhance the physical layer properties of wireless local area networks (IEEE 802.11).

Channel code preformances can be enhanced by adding orthogonal carriers, through constellation shaping or arranging constellation symbols. The problem of the coding gain has remained unsolved ever since the exact solution of the upper bound of the shaping gain.

In this paper, the idea of lattice based coding schemes is developed. The error probability depends on the closest symbol, thus forming the need for a constellation where each symbol would have as many as possible neighbors at the same distance. This problem is known and is termed "a sphere packing problem".

Despite of the convenient mathematical representation of lattices, the problem of decoding lattice codes still remains unsolved. Several universal decoding algorithms have been proposed without ultimate success, as they display computational inefficiency. Moreover, one is also familiar with several decoding algorithms for some well-known lattices attractive for applications. Such algorithms exploit the special structure of lattices, which is the key to efficient decoding.

Key words: lattice coding, goups, lattices, sphere packings, multi-dimensional codes

Prejet 8. maj, 2002
Odobren 10. december, 2002

1 Uvod

Teoretično zgornjo mejo kodirnih postopkov je že dolgo tega definiral Shannon, ker pa ni povedal, kako jo doseči, še vedno iščemo najboljši kodirni postopek.

Na učinkovitost prenosa vplivamo s številom ortogonalnih nosilcev, obliko konstelacijskega diagrama in razporeditvijo simbolov oz. točk v konstelacijskem diagramu. Z razporejanjem točk konstelacijskega diagrama pridobimo npr. na povprečni moči kodirnega postopka, z oblikovanjem pa vplivamo zlasti na razmerje med vršno in povprečno močjo (PAR, Peak to Average power Ratio).

Najbolj razširjeni kodirni postopki imajo neoptimalno razporeditev simbolov. Osnovna oblika je ekvidistančno nizanje simbolov v posameznih ortogonalnih smereh. V dvodimenzionalnem prostoru je ta oblika takšna, kot jo ima konstelacijski diagram modulacijskega postopka QAM (Quadrature Amplitude Modulation). V prostorih z več dimenzijami je izhodiščna oblika posplošitev opisane oblike.

Ker je verjetnost napake povezana z oddaljenostjo najbližjega simbola, ugotovimo da to ni optimalna oblika. Ob upoštevanju enakih oddaljenosti med točkami konstelacijskega diagrama v 2-D prostoru najdemo razporeditev, kjer ima vsak simbol šest sosedov. Struktura je ponovljiva v neskončnost in spominja na zgradbo čebeljih satov. Takšnim neskončnim strukturam rečemo mreže in jih matematično opišemo z grupami.

Raziskave o uporabi kod na podlagi mrež so se

obširneje začele v 80. letih prejšnjega stoletja [27], [28]. Področje je tesno povezano z matematiko, predvsem z algebro in teorijo števil. Med protagonisti apliciranja mrež na kodirne postopke lahko omenimo imena, kot so N. J. A. Sloane, J. H. Conway, G. D. Forney, W. Kassem, R. de Buda... Slednjega zasledimo tudi pri prvih praktičnih mikroprocesorskih izvedbah. Konec 80. let zasledimo modem na podlagi 24 – dimenzionalne mreže, ki deluje s hitrostjo prenosa 19.2 kbit/s [11]. V isti čas datira Forneyeva [30] ideja o uporabi Viterbijevega algoritma za kode na podlagi mrež. Ta ideja je dozorela v približno desetih letih [13]. V vmesnem času pa so se porajale ideje o optimizaciji kod za posebne oblike kanalov ([32], [35]), izpopolnjevanju dekodirnih postopkov ([8], [16], [20], [22], [31]) in tudi natančnejšem vrednotenju mrež ([36]). Kode na podlagi mrež so npr. predvidene tudi za uporabo v brezžičnih lokalnih omrežjih IEEE 802.11.

O dimenzijah in konstrukciji kodirnega postopka je Shannon dejal, da v neskončno dimenzionalnem prostoru razporeditev simbolov v konstelacijskem diagramu ni več pomembna. Ker pa imamo na voljo prostor končnega števila dimenzij in ker težimo k čim bolj učinkovitemu dekodiranju, lahko upamo le na približevanje zgornji teoretični meji.

2 Večdimenzionalni kodirni postopki

Uporaba večdimenzionalnih konstelacijskih diagramov je ugodna predvsem iz dveh razlogov:

- omogoča dodajanje redundance za prenos dodatnih (signalnih) podatkov,
- omogoča povečevanje razmerja signal/šum (SNR).

Najpreprostejše večnivojsko kodiranje v enodimenzionalnem prostoru je v obliki ekvidistančno razporejenih simbolov. Večdimenzionalen konstelacijski diagram dobimo s posplošitvijo enodimenzionalnega primera.

Opisana vrsta konstelacijskega diagrama je preprosta za implementacijo tako v oddajniku kot sprejemniku in je zaradi dobrih lastnosti dokaj razširjena v praksi. Poiskati pa želimo še učinkovitejše kodirne postopke, pri čemer bo merilo primerjava z opisanim osnovnim modelom. Pri iskanju novih konstelacijskih diagramov v prvi vrsti gledamo na kodno ojačenje (coding gain), ki pomeni prihranek moči, potrebne za prenos sporočila, v primerjavi s primerjanim kodirnim postopkom. V obeh primerih zahtevamo enako razmerje SNR, ki ga določa najkrajša razdalja med dvema sosednjima simboloma. Poleg razmerja SNR je merilo učinkovitosti kodirnih postopkov tudi razmerje med maksimalno in povprečno močjo (PAR – Peak to Average power Ratio), skalabilnost (možnost skaliranja) in tudi kompleksnost praktične realizacije postopka.

Primerjavo kodirnih postopkov lahko razdelimo na dva dela:

- kodno ojačenje (coding gain, γ_C) in
- oblikovno ojačenje (shaping gain, γ_S).

Pojma lahko obravnavamo povsem neodvisno, vendar je za smiselno primerjavo treba upoštevati oba hkrati. Da bi ju obravnavali neodvisno, morajo biti verjetnosti pojava posameznega simbola enake. Oblikovno ojačenje je do neke mere obrobnega pomena, ker poznamo najboljšo obliko (krogelne oblike) in njeno ojačenje, ki znaša 1.53dB. Z razporejanjem simbolov imamo bistveno večje težave, saj ne poznamo optimalne razporeditve.

Za povečevanje kodnega dobitka se uporabljajo različne razporeditve, ki so včasih optimirane tudi z vnaprejšnjim poznavanjem razmer na kanalu (Gaussov kanal, Rayleighjev kanal [15]). Običajno imamo opravka z nekim vzorcem, ki bi ga lahko ponavljali v neskončnost. V takih primerih govorimo o t. i. mrežah (lattice), ki so pravzaprav geometrijska predstavitev grup (vsebuje operacijo seštevanja).

Definiciji kodnega γ_C in oblikovnega γ_S ojačenja sta [5]:

$$\gamma_C(\Lambda) = \frac{d^2_{\min}(\Lambda)}{V(\Lambda)^{2/n}}, \tag{1}$$

$$\gamma_S(\Lambda) = \frac{V(R)^{2/n}}{6 \cdot P(R)}. \tag{2}$$

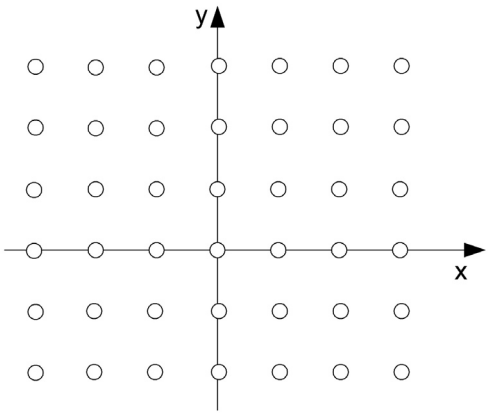
Λ pomeni razporeditev točk konstelacijskega diagrama oz. mrežo, R je prostor, ki ga zajema konstelacijski diagram in $V(R)$ njegova prostornina. Povprečna energija oz. moč kodirnega postopka je podana s $P(R)$, d_{min} pa pomeni najmanjšo razdaljo med točkami konstelacijskega diagrama.

3 Optimalno zlaganje, mreže in kodirni postopki

Izbiranje lege točk v konstelacijskem diagramu je načeloma poljubno, vendar je iz praktičnih razlogov (kodiranje in dekodiranje) preprostejša razdelitev točk, ki tvori neki vzorec. To pomeni, da imajo vse točke konstelacijskega diagrama enaka razmerja s svojimi sosedi (medsebojne razdalje). Osnova takšne porazdelitve je nekakšen vzorec, ki bi ga lahko ponavljali v neskončnost. Kadar imamo opravka s takšnimi vzorci, govorimo o mrežah (lattice) in kodiranju na podlagi mrež (lattice coding).

Mrežo točk si najlaže predstavljamo geometrijsko (slika 1). Manj nazorno, vendar še laže kot geometrijsko, mrežo predstavimo kot grupo. Grupo predstavimo z množico in operacijo. V gornjem primeru imamo množico točk (dvodimenzionalni krajevni vektorji) in operacijo seštevanja. S seštevanjem krajevnih vektorjev poljubnih točk mreže dobimo neko drugo točko mreže, ki je še vedno članica naše množice.

Da bi dobili konkretnejšo podobo mreže na sliki 1, privzemimo, da je razdalja med točkami po osi x ali y celoštevilska vrednost. Iz tega sledi, da imajo točke celoštevilske (pozitivne in negativne) koordinate. Mrežo s celoštevilskimi elementi označimo z Z^n, kjer pomeni n prostorsko dimenzijo mreže v n – dimenzionalnem evklidskem prostoru (R^n). V primeru na sliki 1 gre za mrežo Z^2.



Slika 1. Mreža Z^2 Figure 1. Lattice Z^2

Po definiciji [2] opišemo mrežo Λ takole:

$$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + ... + \lambda_m \cdot v_m; \quad \lambda_1, \lambda_2, ..., \lambda_m \in Z. \quad (3)$$

Množica vektorjev $\{v_1, v_2, ..., v_m\}$ tvori bazo mreže, m pa pomeni dimenzijo oz. rang mreže. Kadar velja $m = n$ (n – dimenzija prostora), imamo opravka z mrežo polnega ranga (full-ranked lattice).

Mrežo lahko zapišemo tudi s pomočjo generatorske matrike (generator matrix), ki jo tvorijo bazni vektorji $\{v_1, v_2, ..., v_m\}$:

$$M = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} = \begin{bmatrix} v_{11} \cdots v_{1n} \\ \vdots \\ v_{m1} \cdots v_{mn} \end{bmatrix}. \quad (4)$$

V gornjem zapisu pomeni m dimenzijo mreže in n dimenzijo prostora (v_{xx} so koordinate vektorjev v posameznih dimenzijah). Kadar se dve mreži razlikujeta le v faktorju skaliranja in rotacije, imamo opravka z ekvivalentnima mrežama.

Prostor okoli točk mreže lahko razdelimo na take dele, da vsaki točki pripada enaka količina prostora. V kodirnem postopku s trdim odločanjem meje posameznih elementarnih prostorov pomenijo meje med simboli. Prostor, ki pripada eni točki, imenujemo Voronojevo območje (Voronoi cell). Točko mreže Λ v prostoru R^n označimo z s_i in definiramo Voronojevo območje $v(s_i)$ [2].

V literaturi najdemo za osnovni delec prostora tudi poimenovanje elementarni paralelotop (paralelotop je n-dimenzionalna posplošitev paralelepipeda, ki je ime za prizmo z osnovno ploskvijo v obliki paralelograma). Večkrat nas zanima prostornina tega prostora, ki je pri mreži polnega ranga enaka absolutni vrednosti determinante generatorske matrike. Prostornina je neodvisna od baze mreže, kar pa ne velja za obliko elementarnega paralelotopa. Prostornino osnovnega delca prostora mreže Λ ($|\det(M)|$) označimo tudi kot $d(\Lambda)$ ali *vol*(Λ).

Za mreže z nepopolnim rangom m ($m < n$, n – dimenzija prostora) prostornine ne moremo izračunati s pomočjo determinante generatorske matrike. To lahko storimo z uporabo Gram–Schmidtove ortogonalizacije in dobimo Gramovo matriko (A – Gramova matrika, M – generatorska matrika mreže Λ):

$$A = M \cdot M^T. \quad (5)$$

Pokazati je mogoče [2] splošno veljavnost enačbe:

$$d(\Lambda) = \sqrt{\det(A)}. \quad (6)$$

In za skalirane primere (konstanta skaliranja je c):

$$d(c \cdot \Lambda) = c^n \cdot d(\Lambda). \quad (7)$$

Ker je mreža poljubna urejena struktura, si lahko zamislimo veliko različnih mrež z različnimi lastnostmi oz. različnimi generatorskimi matrikami. Zato imajo mreže tudi svoja imena. V večini primerov gre za mreže, ki jih lahko posplošimo v n dimenzij (npr. Z^n, A_n, D_n, E_n). To pomeni, da oblika mreže, ki jo dobimo s posplošitvijo iz n v n+1 dimenzionalen prostor, v n dimenzijah ostane nespremenjena. Večkrat imajo enake mreže različna imena, npr. $\Lambda_2 = A_2$, $F_4 = D_4$, nekatere mreže pa se imenujejo po svojih iznajditeljih, npr. Leechova mreža, mreže Barnes-Wall itd. Obsežen katalog mrež in njihovih lastnosti najdemo v [9].

3.1 Problem optimalnega zlaganja

V matematiki je že dolgo poznan problem optimalnega zlaganja, ki govori o zlaganju enakih poljubnodimenzionalnih krogel. Cilj naloge oz. rešitev problema je čim večje število krogel v danem prostoru. S kroglami prostora ne moremo povsem zapolniti, zato odstotek zapolnjenosti prostora označimo z gostoto zlaganja – Δ (packing density).

Med rešitvami problema optimalnega zlaganja je tudi t. i. mrežno zlaganje (lattice packing), kjer za osnovo vzamemo mrežo (lattice) polnega ranga in v točke mreže postavimo krogle z enakim polmerom. Ker so med točkami mreže enake razdalje d_{min}, lahko v te točke namestimo krogle s polmerom $\rho = {}^{d_{\min}}/_{2}$. Krogle se dotikajo, vendar se ne prekrivajo. Krogla polmera ρ je hkrati tudi največja, Voronojevemu območju včrtana

krogla. Gostoto zlaganja (Δ) definiramo s kvocientom prostornine ene krogle in prostornino Voronojevega območja.

Pomemben pojem je tudi število dotikov (kissing number), ki pove, s koliko drugimi kroglami se dotika poljubna krogla. Na splošno je število dotikov različno za vsako kroglo, kadar pa imamo opravka z mrežnim zlaganjem, je to število enako za vsako točko (kroglo) mreže.

Tabelo najgostejših poznanih rešitev na podlagi mrež najdemo v [9].

3.2 Kodiranje in optimalno zlaganje

Za preslikavo med simboli in električnimi signali služi konstelacijski diagram, ki vsakemu simbolu priredi točko oz. vektor x v prostoru poljubne dimenzije. Evklidska norma vektorja x pomeni energijo prenašanega signala.

Pri prenosu prek kanala se signalu x prišteje šum η, tako da mora sprejemnik pravo vrednost izluščiti iz vsote $y = x + \eta$. Denimo, da imamo kodirni postopek z naborom $\{s_1, s_2, ...s_M\}$, Voronojevo območje okoli poljubne točke označimo z $\upsilon\left(s_k\right)$. V primeru, ko je bil oddan signal s_k, lahko sprejemnik pravilno dekodira simbol, če vrednost signala na vhodu v sprejemnik leži znotraj Voronojevega območja $\upsilon\left(s_k\right)$. Verjetnost, da se to res zgodi, je:

$$P = \frac{1}{(\sigma \cdot \sqrt{2\pi})^n} \int\limits_{\upsilon(s_k)} e^{-\frac{\|x\|^2}{2\sigma^2}} dx. \tag{8}$$

Kadar konstelacijski diagram gradimo na podlagi mrež, govorimo o mrežnih konstelacijah (lattice constellation). Zapišimo še verjetnost napake (e – error):

$$P(e) = 1 - P. \tag{9}$$

Ta enačba velja za neskončno število točk konstelacijskega diagrama ($M \rightarrow \infty$), česar pa v praksi seveda nikoli ne srečamo. Do napake pride zaradi točk, ki ležijo na robu konstelacijskega diagrama, njim pripadajoča Voronojeva območja pa so v nekaterih smereh neomejena. Kljub temu je enačba dober približek za kodiranje s primerno velikim naborom simbolov, saj postajajo s povečevanjem števila simbolov robni efekti zanemarljivi.

Za kodiranje na podlagi N-dimenzionalne mreže z determinanto $d(\Lambda)$ in uporabi Gaussovega kanala s standardno deviacijo σ definiramo razmerje signal/šum [15]:

$$SNR_{dB} = 10 \cdot \log \frac{\left[d(\Lambda)\right]^{2/N}}{4 \cdot \sigma^2}. \tag{10}$$

Glavna težava pri ocenjevanju mrežnih konstelacij je zapleteno računanje verjetnosti napake $P(e)$. Opravka imamo z integriranjem po prostorih, ki jih je težko opisati. Zato uporabimo približke, uporabne le za primerna razmerja SNR. V teh enačbah predpostavljamo enako verjetnost pojava kateregakoli simbola in konstelacijski diagram s takšnim številom točk, da smemo zanemariti robne efekte.

Pri relativno velikih razmerjih SNR in enakih razdaljah med točkami velja, da je približna verjetnost napake [2]:

$$P(e) \approx \frac{\tau}{2} \cdot erfc\left(\frac{\rho}{\sigma \cdot \sqrt{2}}\right). \tag{11}$$

Za izračun po zgornji formuli moramo poznati število dotikov τ in polmer krogel ρ, ki jih zlagamo.

SNR lahko zapišemo preprosteje tudi, če imamo nabor z ustrezno velikim številom simbolov M in znano največjo moč kodirnega postopka C^2 [2]:

$$SNR_{dB}^{'} = 10 \cdot \log \frac{{}^{C^2}/_N}{2 \cdot \sigma^2 \cdot M^{2/N}}. \tag{12}$$

Od tod sledi nov zapis verjetnosti napake [2]:

$$P\left(e\right) \approx \frac{\tau}{2} \cdot erfc\left(\sqrt{\Delta^{2/n} \cdot n \cdot SNR_{dB}^{'}}\right). \tag{13}$$

Kodni dobitek (coding gain) definiramo glede na razporeditevZ^n. Pri visokih razmerjih SNR velja [2]:

$$\gamma_C\left(\Lambda\right) = \frac{d_{\min}^2}{\sqrt[n]{d\left(\Lambda\right)^2}} = 4 \cdot \sqrt[n]{\delta}. \tag{14}$$

Tabela 1 prikazuje kodne dobitke za nekaj kodirnih postopkov na podlagi mrež.

Λ	$\gamma_C(\Lambda)$ /dB
A_2	0.62
D_4	1.50
E_6	2.21
E_8	3.01
K_{12}	3.63
Λ_{16}	4.51
Λ_{24}	6.02

Tabela 1. Kodni dobitki v primerjavi z Z^n
Table 1. Coding gains of some lattices compared to Z^n

3.3 Dekodirni postopki

Kodirni postopki s konstelacijskimi diagrami na podlagi mrež teoretično izkazujejo dobre rezultate, De Buda [14] je dokazal, da se asimptotično približujejo Shannonovi meji.

Glavni problem je učinkovit dekodirni postopek, ki je za zdaj ovira za večjo razširjenost. Poznanih je več univerzalnih dekodirnih postopkov, ki delujejo na principu

iskanja najbližje točke konstelacijskega diagrama (closest point search), a so žal časovno potratni. Poleg tega je poznanih nekaj učinkovitih algoritmov za posebne primere, kot npr. za mreže A_n, D_n in Leechovo mrežo Λ_{24}. Algoritmi za omenjene mreže izkoriščajo specifične lastnosti posameznih mrež in so v tem pogledu optimizirani.

Druga vrsta dekodirnih algoritmov za splošne primere uporablja Viterbijev dekodirni postopek. Tak pristop je mogoč pri mrežah s končnim številom elementov, pri čemer mrežo predstavimo z mrežnim diagramom (trellis diagram).

3.4 Univerzalni dekodirni postopki

Z univerzalnim dekodirnim postopkom je mogoče dekodirati poljubno kodo. Obširen pregled univerzalnih dekodirnih postopkov najdemo v [8], manjši del pa tudi v [15].

Sprejeti vektor, ki ga želimo dekodirati, označimo z x, konstelacijski diagram oz. mrežo, ki jo sestavljajo vektorji u_{ij}, pa z Λ. Problema se lotimo tako, da mrežo premaknemo za sprejeti vektor in rešujemo naslednji problem:

$$\min_{u\in\Lambda} \|x-u\| = \min_{w\in z-\Lambda} \|w\| .$$

S translacijo smo dobili navidezno novo izhodišče mreže, ki mu iščemo najbližjo točko. Območje iskanja omejimo na hiperkroglo s polmerom R, ki je nekoliko večji od polovice razdalje med dvema sosednjima točkama, saj pri optimalnem zlaganju vedno ostane med kroglami nekaj prostora praznega.

Ker polmera R večkrat ne poznamo, lahko uporabimo Rogerjevo zgornjo mejo [15]:

$$R \le \left(\frac{d(\Lambda)}{V_n} \left(n \cdot \ln d + n \cdot \ln(\ln n) + 5 \cdot n \right) \right)^{1/n}, \tag{15}$$

kjer V_n pomeni prostornino enotske n– dimenzionalne hiperkrogle.

Nadaljnji postopek je iskanje točke znotraj hiperkrogle, ki je najbližja izhodišču. Nekatere izvedbe tega postopka uporabljajo tudi strategijo spreminjanja polmera R, in sicer tako, da bodisi povečujejo bodisi zmanjšujejo polmer hiperkrogle toliko časa, da se v njeni notranjosti ne nahaja samo ena točka.

Velja ocena [31], da zahtevnost dekodiranja raste eksponento s kodnim ojačenjem (γ_C) in dimenzijo mreže (n).

3.5 Dekodiranje z Viterbijevim algoritmom

Viterbijev dekodirni algoritem najlaže opišemo z mrežnimi diagrami (trellis diagrams). Pojem mrežnega diagrama, ki na splošno služi za opisovanje Markovskih procesov [3], ni neposredno povezan s konstelacijskimi diagrami na podlagi mrež.

Kot je v [30] dokazal Forney, lahko tudi kode na podlagi mrež predstavimo z mrežnimi diagrami in za dekodiranje uporabimo Viterbijev algoritem. Podrobnejše meje računskih zahtevnosti takih postopkov so predstavljene v [13] in [37] – [39].

Za mero kompleksnosti mrežnega diagrama uporabimo število poti N v mrežnem diagramu, kar je posledica dejstva, da je število poti mrežnega diagrama kode na podlagi mreže odvisno od permutiranja koordinat [13] kodirnega postopka. Mrežni diagram kode Λ imenujemo minimalni, če minimizira vrednost $N(\Lambda)$.

Meje zahtevnosti lahko izrazimo v odvisnosti od baze mreže B (ki je osnova za kodo), njene prostorske dimenzije (n), kodnega ojačenja (γ_C) in dolžine najkrajšega baznega vektorja (λ). V praktičnih primerih se skoraj vedno uporabljajo mreže z enakimi dolžinami baznih vektorjev, saj je dokazano [31], da mreže s tako lastnostjo pomenijo najgostejše zlaganje. Te mreže se imenujejo tudi ESM (Equal Successive Minima). Omenjena baza B je povezana z redukcijo baze mreže (lattice base reduction), ki na splošno neortogonalne bazne vektorje mreže transformira v paroma ortogonalne vektorje. Tudi dolžina najkrajšega baznega vektorja λ izhaja iz transformirane baze. Poznanih je več postopkov redukcije (Hermite, Minkowski, Korkin – Zolotarev itn.), eden izmed najučinkovitejših pa je Korkin – Zolotarev [31], ki se tudi najpogosteje pojavlja pri obravnavi kod na podlagi mrež.

Spodnja meja zahtevnosti mrežnega diagrama za kode na podlagi mrež je izpeljana v [37].

$$N(\Lambda, B) \ge \gamma_C^{n/2} \tag{16}$$

Kodirni postopki oz. mreže, katerih mrežni diagrami dosegajo spodnjo mejo, se imenujejo ekstremni (trellis – extremal).

Natančnejši dokaz zgornje meje najdemo v [13].

$$N(\Lambda, B) \le \lambda^{n(n-1)} \tag{17}$$

4 Lastnosti nekaterih mrež in njihova uporabnost

V tabeli 2 so zbrani najpomembnejši podatki (determinanta, polmer krogel in število dotikov) nekaterih najpomembnejših mrež, ki se največkrat pojavljajo praktičnih primerih.

Pri načrtovanju komunikacijskega kanala nas zanima predvsem verjetnost napake pri prenosu sporočila, ki je, kot vidimo v enačbi (18), povezana z razmerjem SNR. Kodno ojačenje je predvsem orientacijska vrednost, saj bi tako velik prihranek moči dosegli pri izredno majhni

verjetnosti napake. V nadaljevanju prikazujemo primer optimizacije kodirnega postopka v dvodimenzionalnem prostoru. Rezultat je graf (slika 2), ki prikazuje dobitek razmerja SNR pri uporabi kodirnega postopka na podlagi mreže A_2 in verjetnosti napake 10^{-7}.

Λ	$d(\Lambda)$	ρ	τ
$\boldsymbol{Z}^n$	1	$1/2$	$2n$
A_n (n≥2)	$\sqrt{n+1}$	$1/\sqrt{2}$	$n(n+1)$
D_n (n≥3)	2	$1/\sqrt{2}$	$2n(n-1)$
E_8	1	$1/\sqrt{2}$	240
E_7	16	1	126
E_6	$\sqrt{3}$	$1/\sqrt{2}$	72
K_{12}	27	1	756
Λ_{16}	16	1	4320
Λ_{24}	1	1	196560

Tabela 2. Značilni parametri nekaterih mrež
Table 2. Some lattice properties

4.1 Optimizacija kodirnega postopka v 2-D

Zanima nas razmerje SNR, ki nam bo omogočilo komunikacijo z zahtevano verjetnostjo napake. Za naš primer si izberimo verjetnost napake 10^{-7}, kar je npr. standardna vrednost za ISDN.

Z uporabo enačb (11) in (14) izračunamo potrebno razmerje SNR za kodirni postopek na podlagi mreže Z^2:

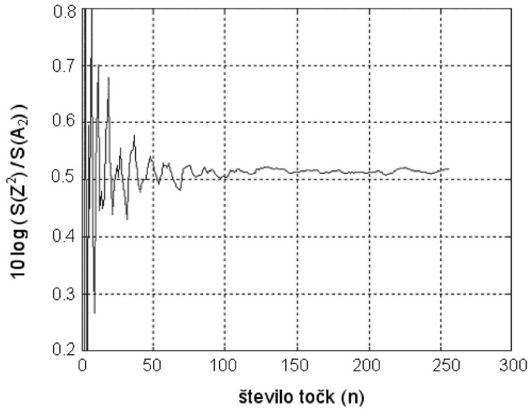
$$SNR_{dB}(Z^2) \approx 14.7dB.$$

Z uporabo istih enačb in upoštevanjem parametrov mreže A_2 izračunamo še:

$$SNR_{dB}(A_2) \approx 14.2dB.$$

Primerjava vrednosti SNR da razliko 0.5dB. To pomeni, da pri zahtevani verjetnosti napake 10^{-7} in uporabi konstelacije A_2 na enakem kanalu prihranimo 0.5dB pri potrebni povprečni moči oddajnika.

Graf na sliki 2 prikazuje razmere za poljubno število točk konstelacijskega diagrama. Vidimo, da se z večanjem števila simbolov čedalje bolj približujemo dobitku 0.5dB, skokovito obnašanje pri majhnem številu simbolov je predvsem posledica oblike konstelacijskega diagrama, ki je npr. pri n= 7 optimalna za mrežo A_2. Vrednost dobitka je odvisna tudi od oblike konstelacijskega diagrama, ki je predvsem pri majhnem številu simbolov lahko izrazito neugodna. Pri prikazanih rezultatih je bilo oblikovanje izvedeno z minimiziranjem energije konstelacijskega diagrama za posamezno število simbolov.



Slika 2. Dobitek kodirne sheme na podlagi mreže A_2
Figure 2. A_2 lattice coding gain

5 Sklep

Teoretična zgornja meja dobitka, ki ga pridobimo z oblikovanjem konstelacijskega diagrama, je znana, kot so poznani tudi postopki oz. oblike, ki so primerne tako s stališča praktične realizacije kot s stališča ugodnega dobitka. Problem razporeditve simbolov oz. točk konstelacijskega diagrama je teže rešljiv. Glede na to, da na verjetnost napake pri sprejemu najbolj vplivajo sosednji simboli, je zanimiva ideja iskanje čim bolj goste razporeditve. Ta problem je v matematiki znan pod imenom zlaganje krogel (sphere packing). Optimalna rešitev tega problema je znana le za enodimenzionalni in dvodimenzionalni prostor, za prostore več dimenzij pa so znani le bolj ali manj dobri približki. Vse te rešitve imajo zanimivo in uporabno lastnost – vzorec zlaganja se ponavlja v neskončnost in jih zato matematično preprosto opišemo z mrežami.

Težava kodirnih postopkov na podlagi grup je zlasti zahtevna realizacija dekodirnega postopka. Univerzalni dekodirni algoritmi so uporabni, vendar pa tudi potratni. Optimalne rešitve so pogojene z upoštevanjem specifičnih lastnosti mrež.

Za današnje razmere je praktična uporaba kodirnih postopkov na podlagi mrež omejena s težavami pri implementaciji. Kljub teoretično boljšim lastnostim, kot jih imajo danes najbolj razširjene kode, se kode na podlagi mrež redko pojavljajo, saj ne preveč izrazitega dobitka (še) ni moč upravičiti s kompleksnostjo izvedbe. Ob morebitni iznajdbi učinkovitega univerzalnega dekodirnega postopka pa bi se razmere utegnile spremeniti.

6 Literatura

[1] T. M. Thompson, *From error-correcting codes through sphere packings to simple groups*, Mathematical Association of America, 1983.

[2] J. H. Conway, N. J. A. Sloane, *Sphere packings, Lattices and groups*, Springer-Verlag, 1988.

[3] E. A. Lee, D. G. Messerschmitt, *Digital Communications*, Kluwer Academic, 1990.

[4] A. J. Viterbi, J. K. Omura, *Principles of Digital Communication and Coding*, McGraw – Hill, 1979.

[5] G. D. Forney, L. F. Wei, Multidimensional Constellations – Part I: Introduction, Figures of Merit, and Generalized Cross Constellations, *Select. Areas in Comm., IEEE Journal on*, vol 7, no. 6, str. 877 – 892, 1989.

[6] S. Neumann, *Coding theory and its application to the study of sphere-packing*, University of Göteborg, 1998.

[7] G. D. Forney, Multidimensional Constellations – Part II: Voronoi Constellations, *Select. Areas in Comm., IEEE Journal on*, vol. 7, no. 6, str. 941 – 958, 1989.

[8] E. Agrell, T. Eriksson, A. Vardy, K. Zeger, Closest Point Search in Lattices, *IEEE Trans. on Inf. Theory*, vol. 48, no. 8, str. 2201 – 2214, 2002.

[9] G. Nebe, N. J. A. Sloane, *A Catalogue of Lattices*, http://www.research.att.com/∼njas/lattices, 2002.

[10] N. Wang, J. D. Gibson, Leech lattice coding and modulation for IEEE 802.11a WLAN, *BroadBand Comm. for the Internet Era Symposium digest, IEEE Emerging Techn. Symposium on*, str. 38 – 42, 2001.

[11] G. R. Lang, F. M. Longstaff, A Leech lattice modem, *Select. Areas in Comm.*, IEEE Journal on , vol. 7, no. 6, str. 968 – 973, 1989.

[12] A. G. Burr, J. A. Sheppard, Hardware architectures for lattice decoders, *DSP Application in Comm. Systems, IEEE Colloquium on*, str. 8/1 – 8/6, 1993.

[13] A. H. Banihashemi, I. F. Blake, Trellis Complexity and Minimal Trellis Diagrams of Lattices, *IEEE Trans. on Inf. Theory*, vol 44, no. 5, str. 1829 – 1847, 1989.

[14] R. de Buda, Some optimal codes have structure, *Select. Areas in Comm., IEEE Journal on* , vol. 7, no. 6, str. 893 – 899, 1989.

[15] E. Viterbo, *Computational methods for analysis and design of lattice constellations*, Politecnico of Torino, februar 1995.

[16] G. D. Forney, A bounded distance-decoding algorithm for the Leech lattice with generalizations, *IEEE Trans. on Inf. Theory*, vol. 35, no. 4, str. 1152 – 1187, 1989.

[17] A.G. Burr, R. W. Taylor, Architectures and algorithms for decoding multi-dimensional lattice codes, *Multi- Dimensional Signal Processing, IEEE Colloquium on*, str. 3/1 - 3/4, 1989.

[18] M. O. Damen, K. Abed-Meraim, M. S. Lemdani, Further results on the sphere decoder, *Inf. Theory, IEEE International Symposium on, Proceedings*, str. 333, 2001.

[19] M. O. Damen, A. Chkeif, J. C. Belfiore, Lattice code decoder for space-time codes, *IEEE Comm. Letters*, vol. 4, no. 5, str. 161 – 163, 2000.

[20] E. Viterbo, J. Bouros, A universal lattice code decoder for fading channels, *IEEE Trans. on Inf. Theory*, vol. 45, no. 5, str. 1639 – 1642, 1999.

[21] V. Tarokh, A. Vardy, K. Zeger, Universal bound on the performance of lattice codes, *IEEE Trans. on Inf. Theory*, vol. 45, no.2, str. 670 – 681, 1999.

[22] M. Ran, J. Snyders, Efficient decoding of the Gosset, Coxeter-Todd and the Barnes-Wall lattices, *Inf. Theory, IEEE International Symposium on, Proceedings*, str. 92, 1998.

[23] O. Amrani, Y. Beery, Bounded-distance decoding: algorithms, decision regions, and pseudo nearest neighbors, *IEEE Trans. on Inf. Theory*, vol. 44, no. 7, str. 3072 – 3082, 1998.

[24] R. Urbanke, B. Rimoldi, Lattice codes can achieve capacity on the AWGN channel, *IEEE Trans. on Inf. Theory*, vol. 44, no. 1, str. 273 – 278, 1998.

[25] H. A. Loeliger, Averaging bounds for lattices and linear codes, *IEEE Trans. on Inf. Theory*, vol. 43, no. 6, str. 1767 – 1773, 1997.

[26] J. H. Conway, N. J. A. Sloane, Fast quantizing and decoding algorithms for lattice quantizers and codes, *IEEE Trans. on Inf. Theory*, vol. IT-28, str. 227 – 232, 1982.

[27] N. J. A. Sloane, Tables of sphere packings and spherical codes, *IEEE Trans. on Inf. Theory*, vol. IT-27, str. 327 – 338, 1981.

[28] H. M. de Oliveira, G. Battail, A capacity theorem for lattice codes on Gaussian channels, *Telecommunications Symposium, ITS '90 Symposium Record., SBT/IEEE International*, str. 5 – 9, 1990.

[29] G. D. Forney, Jr., Coset codes. I. Introduction and geometrical classification, *IEEE Trans. on Inf. Theory*, vol. 34, no. 5, str. 1123 – 1151, 1988.

[30] G. D. Forney, Jr., Coset codes. II. Binary lattices and related codes, *IEEE Trans. on Inf. Theory*, vol. 34, no. 5, str. 1152 – 1187, 1988.

[31] A. H. Banihashemi, A. K. Khandani, On the Complexity of Decoding Lattices Using the Korkin-Zolotarev Reduced Basis, *IEEE Trans. on Inf. Theory*, vol. 44, no.1, str. 162 – 171, 1998.

[32] A. K. Khandani, P. Kabal, Optimization of a Lattice-Based Constellation for Signaling Over a Partial Response Channel, *IEEE Trans. on Communitations*, vol. 46, no. 7, str. 854 – 856, 1998.

[33] B. H. Banihashemi, A. K. Khandani, An Inequality on the Coding Gain of Densest Lattice Packings, *Designs, Codes and Cryptography*, vol. 14, str. 207 – 212, 1998.

[34] A. R. Calderbank, N. J. A. Sloane, New Trellis Codes Based on Lattices and Cosets, *IEEE Trans. on Inf. Theory*, vol. 33, no. 2, str. 177 – 195, 1987.

[35] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiore, Good Lattice Constellations for both Rayleigh Fading and Gaussian Channels, *IEEE Trans. on Inf. Theory*, vol. 42, no. 2, str. 502 – 518, 1996.

[36] E. Viterbo, E. Biglieri, Computing the Voronoi cell of a lattice: The diamond-cutting algorithm, *IEEE Trans. on Inf. Theory*, vol. 42, no. 1, str. 161 – 171, 1996.

[37] V. Tarokh, I. F. Blake, Trellis complexity versus the coding gain of lattices I, *IEEE Trans. on Inf. Theory*, vol. 42, no. 6, str. 1796 – 1807, 1996.

[38] V. Tarokh, I. F. Blake, Trellis complexity versus the coding gain of lattices II, *IEEE Trans. on Inf. Theory*, vol. 42, no. 6, str. 1808 – 1816, 1996.

[39] V. Tarokh, A. Vardy, Upper bounds on trellis complexity of lattices, *IEEE Trans. on Inf. Theory*, vol. 43, no. 4, str. 1294 – 1300, 1997.

[40] R. de Buda, The upper bound of a new near optimal code, *IEEE Trans. on Inf. Theory*, vol. IT-21, str. 441 – 445, 1975.

[41] I. N. Bronštejn, K. A. Semendjajev, G. Musiol, H. Muehlig, *Matematični priročnik*, Tehniška založba Slovenije, 1997.

Rudolf Sušnik je leta 2001 diplomiral na Fakulteti za elektrotehniko Univerze v Ljubljani s področja telekomunikacij. Zaposlen je kot mladi raziskovalec v Laboratoriju za komunikacijske naprave na Fakulteti za elektrotehniko, kjer je tudi študent podiplomskega študija elektrotehnike. Njegovo raziskovalno in razvojno delo je osredotočeno na komunikacijska omrežja.

Sašo Tomažič je diplomiral leta 1979, magistriral leta 1981 in doktoriral leta 1991 na Univerzi v Ljubljani, s področja telekomunikacij. Zaposlen je na Fakulteti za elektrotehniko v Ljubljani kot profesor in predstojnik Laboratorija za komunikacijske naprave in predstojnik Katedre za telekomunikacije. Je nacionalni koordinator za področje telekomunikacij na Ministrstvu za šolstvo, znanost in šport. Njegovo sedanje delo obsega raziskave na področju obdelave signalov, varnosti v telekomunikacijah, elektronskega poslovanja in porazdeljenih podatkovnih sistemov.