Algebralliset menetelmät virheenkorjauskoodin tunnistamisessa

Jyrki Lahtonen, Anni Hakanen, Taneli Lehtilä, Toni Hotanen,
Teemu Pirttimäki, Antti Peltola

Turun yliopisto

MATINE-tutkimusseminaari, 16.11.2017

Johdanto

Tutkimusongelma: Virheenkorjauskoodin tunnistaminen havaitusta radiosignaalista.

- Oletuksenamme on, että radiosignaali on jo tulkittu biteiksi. Seuraavana askeleena signaalin käsittelyssä olisi kanavakoodauksen purkaminen.
- Olemme kehittäneet tunnistusalgoritmeja konvoluutiokoodien ja Reedin-Solomonin koodien tunnistamiseen binäärisyötteestä. Nämä ovat virheenkorjauskoodeja, joilla on paljon algebrallista rakennetta ja sen vuoksi tunnistettavissa pienehköstä datamäärästä.
- Tunnistusmenetelmät on implementoitu Matlab- ja Mathematica-ohjelmistoilla.

Konvoluutiokoodeista

Konvoluutiokoodit

- Virheenkorjauskoodi, jolla viesti koodataan muutaman bitin pätkissä.
- Kooderin rakenne ilmaistaan generaattorimatriisilla. Esimerkki:

$$G = \begin{pmatrix} 1+D & 1+D & 1 \\ 0 & D & 1+D \end{pmatrix}$$

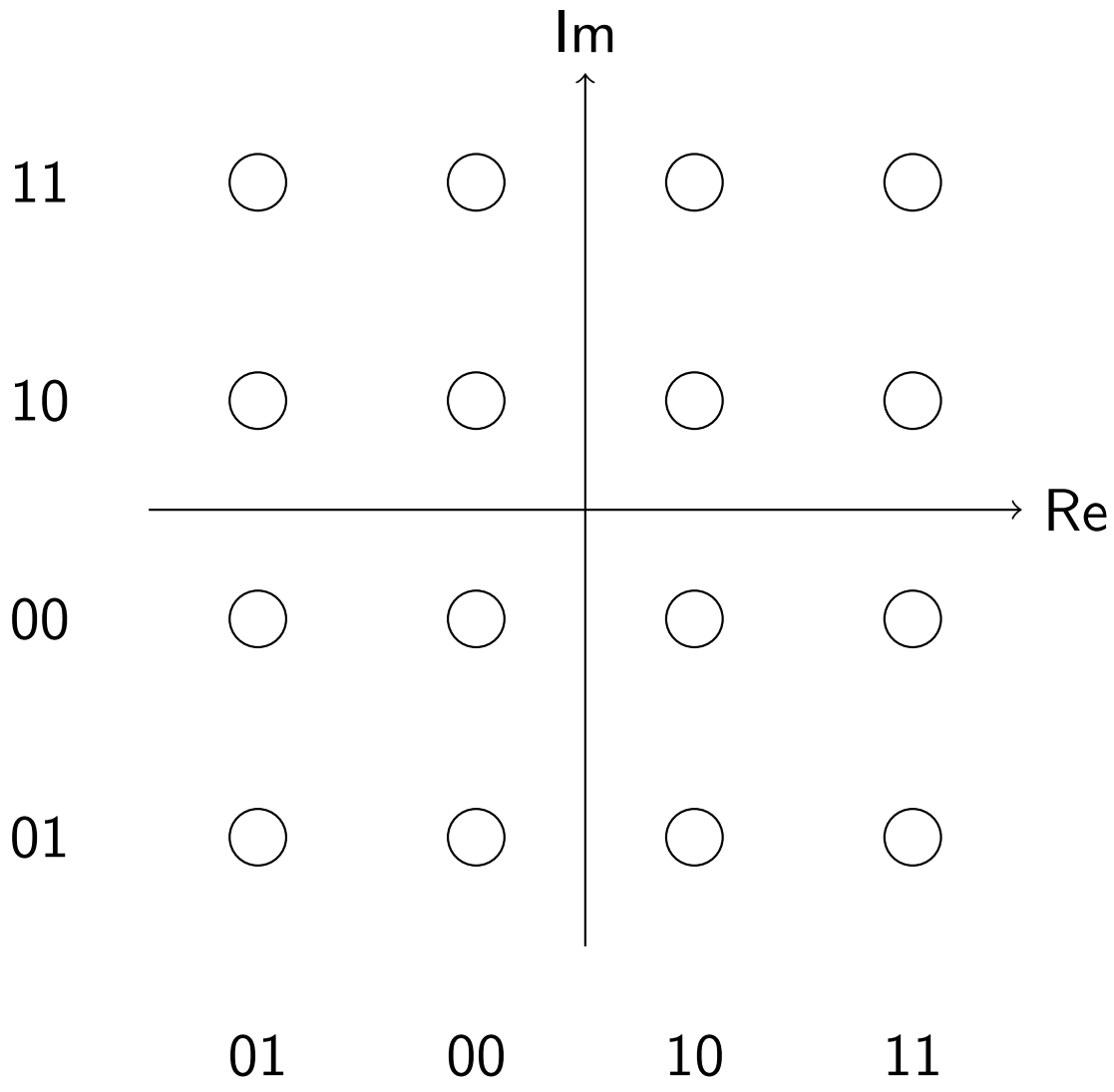
- Tärkeitä parametreja: generaattorimatriisin koko ja ulkoinen aste (koodauksen kompleksisuus), vapaa etäisyys (virheenkorjauskyky).

Gray-koodit

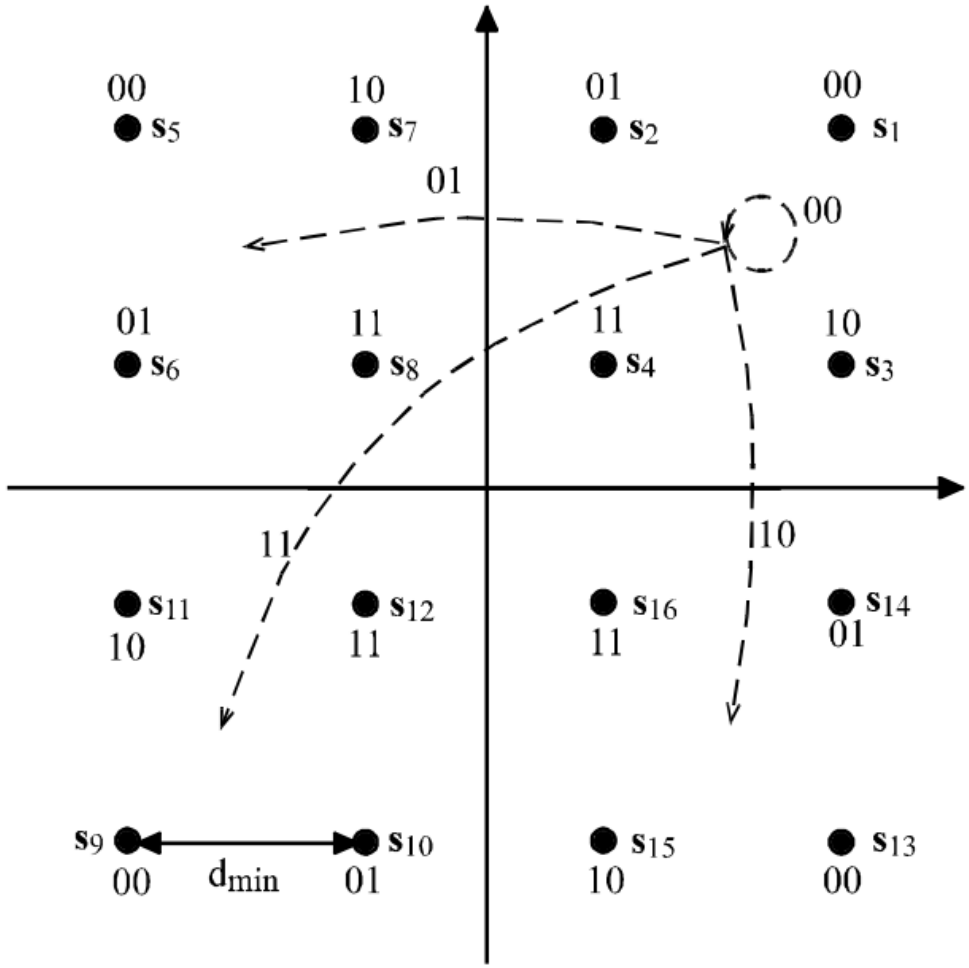
- Kiinnitetään koodisanojen pituus n.
- Järjestetään kaikki n pituiset koodisanat siten, että seuraava sana eroaa edellisestä yhden bitin kohdalla.
- Esimerkiksi kun $n = 2$, eräs Gray-koodi on

$$\{00,\ 10,\ 11,\ 01\}.$$

M-QAM

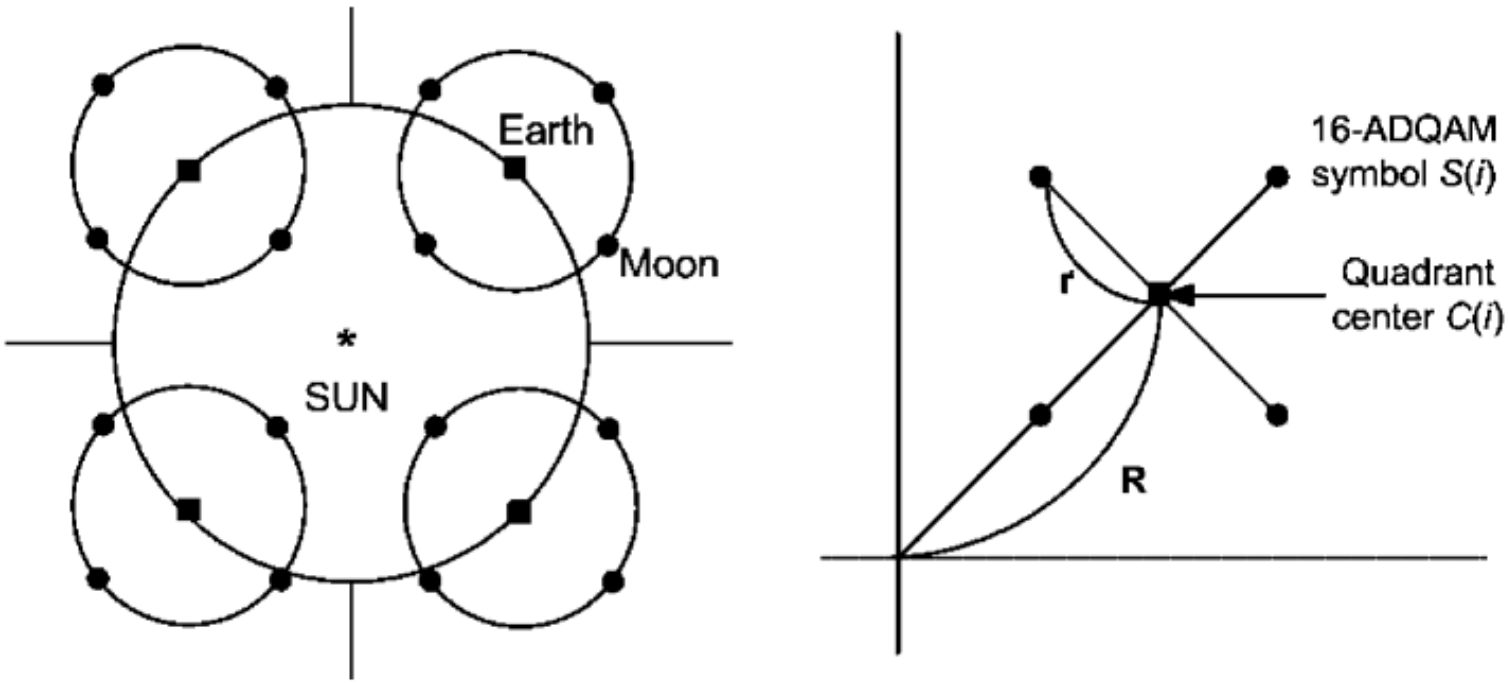


DQAM



Lähde: Weber, W. J., "Differential encoding formultiple amplitude and phase shift keying systems," *IEEE Trans. Comms.*, vol. 26, no. 3, Mar. 1978, pp. 385–391. Copyright © 1978 IEEE.

ADQAM



Lähde: Hwang J, Chiu Y, Liao C. "Angle differential-QAM scheme for resolving phase ambiguity in continuous transmission system". *Int. J. Communication Systems*, 2008. 21(6):631–641. Copyright © 2007 John Wiley & Sons, Ltd.

Muunnokset & siirtymät

- Gray-koodista toiseen voidaan siirtyä bittien permutoinnin ja vakiovektorin lisäämisen avulla.
- Kun saatu signaali on muunnettu binääriseksi jonkin QAM-mallin ja Gray-koodin mukaan, käytetty Gray-koodi voidaan vaihtaa toiseen permutoimalla bittejä ja lisäämällä vakiovektori.
- Väärä Gray-koodi sekoittaa viestin rakennetta. Väärin tulkittu viesti on kuitenkin jonkin konvoluutiokooderin ulostulo. Tällaiselle kooderille saadaan generaattorimatriisi muokkaamalla alkuperäisen koodin generaattorimatriisia.

Tunnistus & valinta

- Menetelmä konvoluutiokoodin generaattorimatriisin tunnistamiseen binäärisestä viestistä on jo olemassa.
- Väärällä Gray-koodilla saatu generaattorimatriisi on kuitenkin pääsääntöisesti suurempi kuin alkuperäinen.
- Oikea generaattorimatriisi ja Gray-koodi voidaan tunnistaa käymällä kaikki vaihtoehdot läpi ja valitsemalla koodi, jolla on parhaat ominaisuudet (oletamme, että viestin lähettäjä käyttää hyvää kanavakoodausta).

Reedin-Solomonin koodeista

RS-koodin määrittely

- RS-koodit määritellään käyttäen aakkostona äärellistä kuntaa $\mathbb{F}_q$.
- Usein käytössä on esimerkiksi 256-alkioinen kunta $\mathbb{F}_{2^8}$, jolloin koodisanojen symbolit voidaan esittää 8 bitillä.
- RS-koodit voidaan määritellä useilla tavoilla. Eräs tavallinen tapa on määritellä RS-koodi C, jonka pituus on $n < 256$ ja dimensio k, joukkona

$$C = \{m(x)g(x) \mid m(x) \in \mathbb{F}_{2^8}[x], \deg(m(x)) < k\},$$

missä $g(x) \in \mathbb{F}_{2^8}[x]$ on RS-koodin *generaattoripolynomi*, $\deg(g(x)) = n - k$.

RS-koodien tunnistaminen

RS-koodi siis määräytyy käytetystä äärellisestä kunnasta, koodin pituudesta n, dimensiosta k sekä koodin generaattoripolynomista $g(x)$.

- Tavoitteena on ensinnäkin kyetä tunnistamaan, onko bittijono tuotettu RS-koodilla, ja jos on, niin lisäksi pystyä tunnistamaan siitä kyseiset koodin määräävät parametrit.
- Olemme käsitelleet sekä tilannetta, jossa jo tunnemme tavan muuttaa binääriset koodiviestit kunnan alkioiksi, että tapausta, jossa ei ole tiedossa, miten tämä muunnos tehdään.
- Molempiin tilanteisiin on kehitetty luotettavia tunnistusmenetelmiä.

RS-koodien tunnistaminen

- Helpommassa tapauksessa, kun bittikombinaatiot on jo osattu tulkita äärellisen kunnan alkioiksi, RS-koodin tunnistaminen pystytään tekemään yleensä jo yhdenkin havaitun koodisanan perusteella tarkastelemalla sen nollakohtia. Nollakohdista voidaan päätellä koodin generaattoripolynomi.
- Bittikombinaatioiden tulkitseminen oikein äärellisen kunnan alkioiksi, esimerkiksi tavun muuntaminen kunnan $\mathbb{F}_{2^8}$ alkioksi, onkin huomattavasti haastavampi tehtävä.
- Tämä muunnos voitaisiin periaatteessa tehdä hyvin useilla eri tavoilla, mutta järkeviä vaihtoehtoja on kuitenkin rajoitetusti. Mielellään tämä pitäisi pystyä havaitsemaan datasta.

RS-koodien tunnistaminen

Ongelman ratkaisemiseen on implementoitu kaksi erilaista tunnistusalgoritmia. Molemmat näistä menetelmistä perustuvat RS-koodin sykliseen rakenteeseen ja hyödyntävät sitä hieman eri tavoin.

- Esimerkiksi kunnan $\mathbb{F}_{2^8}$ yli määritellyn k-dimensioisen RS-koodin tunnistamiseksi tarvitaan havainto noin $8k$ koodilohkosta.
- RS-koodien syklisyyden vuoksi jokaisesta havaitusta koodilohkosta pystytään kuitenkin tuottamaan k kappaletta koodin sanoja, joten dataa tarvitaan käytännössä noin 8 koodisanan verran.
- Koodin parametrit pystytään selvittämään etsimällä binääriselle RS-koodille systemaattinen generaattorimatriisi tai vaihtoehtoisesti niin sanotuilla Gröbnerin kannoilla polynomialgebraa käyttäen.

RS-koodien tunnistaminen

- Kehitetyillä tunnistusalgoritmeilla pystytään luotettavasti erottamaan, onko bittijono sattumanvaraisesti generoitu vaiko tuotettu jollain RS-koodilla.
- Koodilohkojen pituus pystytään usein saamaan selville, vaikka ne sisältäisivät joitain bittivirheitä, mutta kaikkien RS-koodin parametrien tunnistamiseksi havaitun datan tulee kuitenkin olla täysin virheetöntä.
- Koodin tunnistamiseen liittyy myös monikäsitteisyyttä, jonka merkitystä on tutkittu.
- Erityisestikin bittiyhdistelmien kuvaus kunnan alkioiksi voidaan tehdä tietyillä eri tavoilla ja onnistua silti tunnistamaan koodin parametrit oikein.