Cyklické algebry s delením a ich využitie v bezdrôtovej komunikácií

Juraj Pohanka

Katedra matematiky FJFI, ČVUT

Popis problematiky

- Teória kódovania sa zaoberá problématikou efektnívneho prenosu informácií cez kanály spôsobujúce rušenie.
- Jej úlohou je dizajn prenosového systému, ktorý je spoľahlivý, účinný a rýchly.
- Medzi jej aktuálne problémy patrí princípy a dizajn tzv. MIMO(Multiple Input Multiple Output) kanálov.

História problematiky

Princíp multi-anténového prenosu

- praktická aplikácia - Marconi,Tesla (1.dekáda 20.storočia)
- teoretický popis - Tarokh,Seshadri,Calderbank(1998)
- prvý STBC: Alamoutiho schéma - Alamouti(1999)

Modelovanie prenosového kanála

- N_t vysielajúcich antén
- N_r prijímajúcich antén
- $\vec{s}$ - vektor vysielaných signálov; $\vec{r}$ - vektor prijímaných signálov
- $\vec{\eta}$ - vektor šumu pre jednotlivé dvojice $s_i - r_i$
- H matice prenosu signálu(h_{ij}- prenos z i-tej vysielacej na j-tu prijímaciu anténu)
- $\vec{s} \in \mathbb{C}^{N_t}$; $\vec{r}, \vec{\eta} \in \mathbb{C}^{N_r}$; $H \in \mathbb{C}^{N_r, N_t}$

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{N_r} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1N_t} \\ h_{21} & h_{22} & \dots & h_{2N_t} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_r 1} & h_{N_r 2} & \dots & h_{N_r N_t} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{N_t} \end{pmatrix} + \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_{N_r} \end{pmatrix}$$

$$\vec{r} = H\vec{s} + \vec{\eta}$$

Modelovanie prenosového kanála

Signály sa budú vysielať diskrétne v čase. Každá anténa bude vysielať reťazec T komplexných čísel:

$$(\forall t \in \{1, .., T\})(\vec{r_t} = H\vec{s_t} + \vec{\eta_t})$$

$$(\vec{r_1}, \vec{r_2}, \ldots, \vec{r_T}) = H(\vec{s_1}, \vec{s_2}, \ldots, \vec{s_T}) + (\vec{\eta_1}, \vec{\eta_2}, \ldots, \vec{\eta_T})$$

$$R = H.S + W$$

$$R \in \mathbb{C}^{N_r \times T}$$

Predpokladáme kvázistatické kanály $\Longrightarrow$ koeficienty h_{ij} budú počas prenosu takmer konštantné.

Signálne konštalácie

Signálna konštalácia $S \subset \mathbb{C}$ je konečná podmnožina komplexných čísel.

Základné druhy signálnych konštalácií

- M-PSK : $S_M = \{\omega_M^j : j = 0, 1, ..M - 1\}$
- M-QAM : M bodov v mriežke $\mathbb{Z}[i]$ nachádzajúcich sa v okolí počiatku $\{a + bi$: a,b sú liché a $|a|, |b| < \sqrt{M}\}$
- HEX : určitá konečná podmnožina Eisensteinových čísel $Z[\omega_6]$

Základné pojmy

STBC(Space-Time Block Code)

je ľubovoľná konečná podmnožina $C \subset M_{N_t \times T}(\mathbb{C})$, kde N_t je počet vysielajúcich antén a T je dĺžka bloku.

STBC je nad signálnou konštaláciou S

ak každý prvok matíc v C je komplexná lineárna kombinácia prvkov z S.

STBC je úplne nad signálnou konštaláciou S

ak každý prvok matíc v C je prvok z S.

Kritérium hodnosti

$(\forall V, W \in C)(rank(V - W) = n)$. Ak kritérium platí pre C, hovoríme, že C je plne diverzné.

Kritérium determinantu

$$\Delta_{min}(C) = \min_{V,W \in C; V \neq W} |det(V - W)|$$

Daný minimálny determinant musí byť čo možno najväčší.

Kritéria pre efektívne STBC

Vedľajšie kritéria

Rýchlosť

Definujeme ju ako $\frac{1}{T} log_{|S|}|C|$. Vyjadruje, ako rýchlo sa informácia pri danom kóde prenáša.

Diverzita

Pre daný kanál máme pravdepodobnosť chyby danú vzťahom $K\rho^{-D}$,kde ρ je pomer signál-šumu a kde D je diverzita.

STBC pomocou algebier s delením

Algebra s delením

Je okruh s jednotkou v ktorom pre každý prvok existuje inverzný.

Nech S je naša signálna konštalácia a $F = \mathbb{Q}(S)$. Chceme aby $C \subseteq M_{n\times n}(F)$ spĺňalo kritérium hodnosti. Postačí nám nájsť algebru s delením D a okruhový homomorfizmus $\phi : D \to M_{n\times n}(F)$. Algebra s delením nemá žiadne vlastné netriviálne ideály $\implies ker\phi = 0 \implies \phi$je teda vnorenie

$$\phi : D \hookrightarrow M_{n\times n}(F)$$

Generická konštrukcia

Nech máme algebru s delením D a teleso $E \subseteq Z(D)$. Potom D je vektorový priestor nad E. Označme ho D_E. Potom D pôsobí na D_E pomocou násobenia z prava :
$(\forall d \in D)(\lambda_d : D_E \to D_E)$,$\lambda_d : x \to dx$ čo je lineárna transformácia: $(\forall e_1, e_2 \in E)(\forall x_1, x_2 \in D_E)$

$$\lambda_d(e_1x_1 + e_2x_2) = d(e_1x_1 + e_2x_2) = de_1x_1 + de_2x_2$$

$$= e_1dx_1 + e_2dx_2 = e_1\lambda_d(x_1) + e_2\lambda_d(x_2) \Longrightarrow \lambda_d \in End_E(D).$$

Generická konštrukcia

Zobrazenie $\Lambda : D \to End_E(D)$,$\Lambda : d \to \lambda_d$ je okruhový homomorfizmus $(\forall c, d \in D)(\forall x \in D_E)$:

$$(\lambda_c.\lambda_d)(x) = \lambda_c(\lambda_d(x)) = \lambda_c(dx) = cdx = \lambda_{cd}(x)$$

$$(\lambda_c + \lambda_d)(x) = \lambda_c(x) + \lambda_d(x) = cx + dx = (c + d)x = \lambda_{c+d}(x)$$

$End_E(D) \cong M_{n\times n}(E)$, čo znamená $\phi : D \xrightarrow{\Lambda} End_E(D) \xrightarrow{\cong} M_{n\times n}(E)$ kde $n = [D : E]$, v prípade pre F : $D \supseteq F = \mathbb{Q}(S)$ je $n = [D : F]$

STBC pomocou nekomutatívnych algebier s delením

Cyklické algebry s delením

Cyklická algebra s delením D nad telesom F je algebra s delením s centrom F a maximálnym podtelesom K takým, že K je Galoisovo nad F a $Gal(K/F)$ je cyklická

Nech D je cyklická algebra s delením nad F s indexom n($n^2 =$ [D:F]) s maximálnym podtelesom F. Nech σ je generátor Gal(K/F) tak, že rád σ je n. Potom je známe že existuje také $z \in D$ tak, že:

$$z^n = \delta, \delta \in F$$

$$kz = z\sigma(K), \forall k \in K$$

$$D = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K$$

Ďakujem za pozornosť