Codificação de Subespaço e Grupos n-Shot

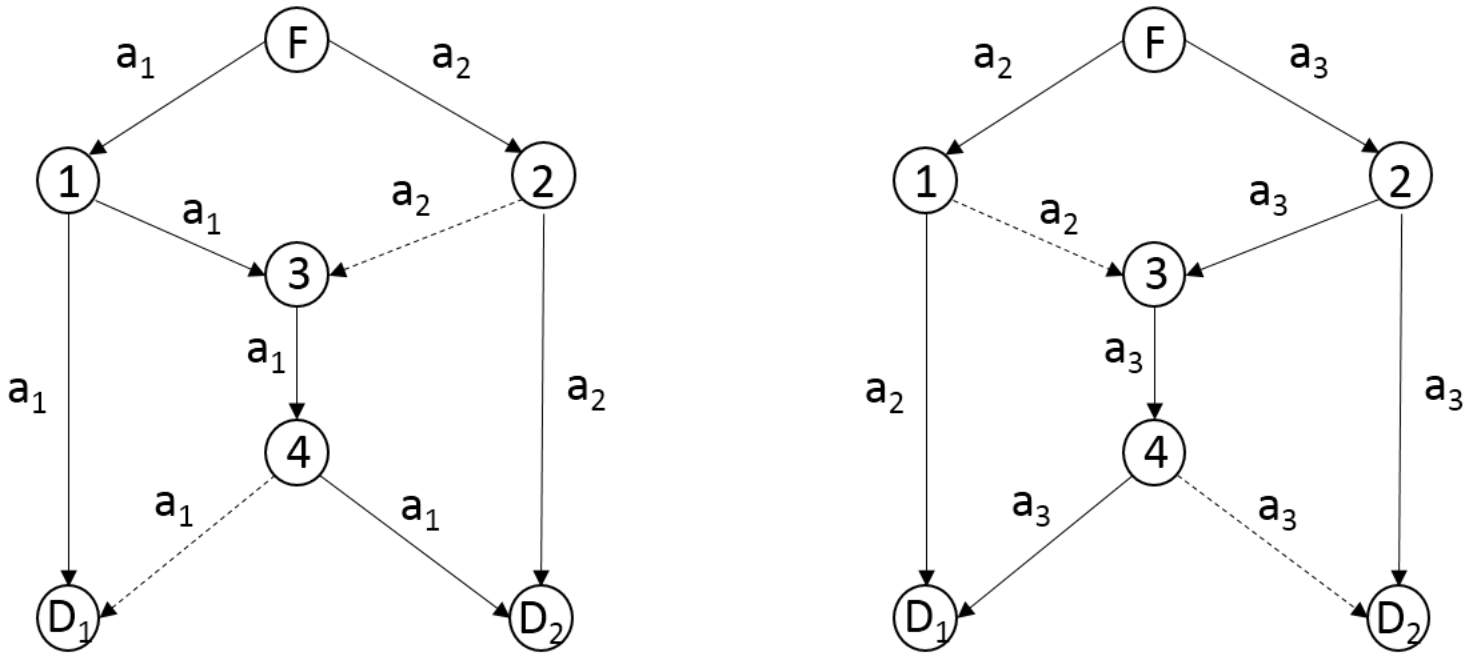
Leandro Bezerra de Lima - INMA / UFMS
(leandro.lima@ufms.br)

16 de junho de 2023

Sumário

Sumário

Motivação: Rede Borboleta

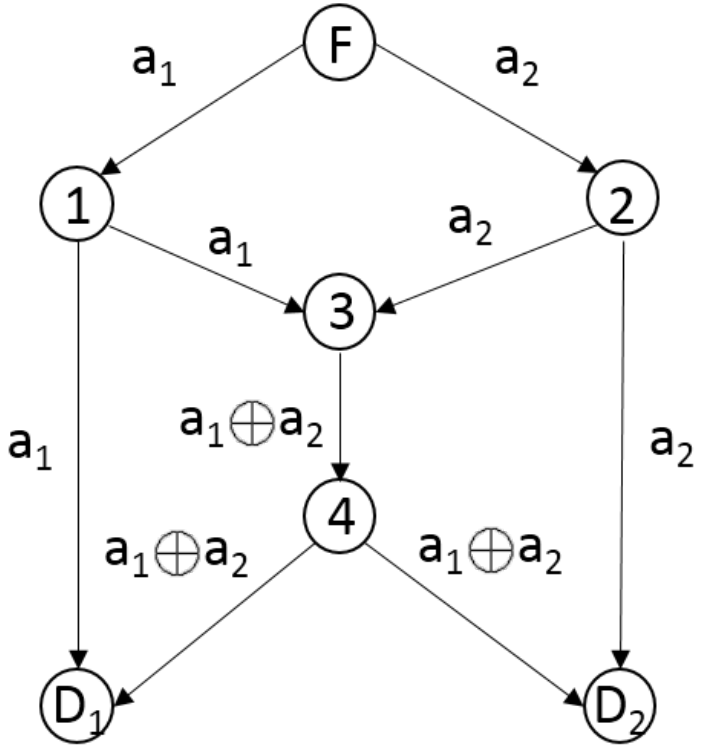


(a) Primeiro instante

(b) Segundo instante

Figura: Rede Borboleta Utilizando Roteamento

Motivação: Rede Borboleta



(a) Primeiro instante

Figura: Rede Borboleta Utilizando Codificação de Rede

Motivação: Codificação de Rede

Codificação de Rede - Roteamento. Permite replicar e selecionar caminhos para a informação trefegar na rede.

Codificação de Rede - Processador Digital. Permite realizar operações e processamento em cada nó.

Potencialidades:

- Ganhos em termos de taxa de informação.
- Simplificação de algoritmos de roteamento.
- Promissora para redes sem fio.
- Aplicações em redes de sensores, redes ópticas e distribuições de arquivos em redes.

Motivação: Trabalhos Anteriores

- **Linear network coding**. Li, R.; Yeung, R.W.; Cai, N. IEEE Transactions on Information Theory.2003
- **Network error correction, Part I: Basic concepts and upper bounds**. Yeung, R. W.; Cai, N. Communications in Information and Systems. 2006.
- **Coding for errors and erasures in random network coding**. Köetter, R.; Kschischang, F. IEEE Transactions on Information Theory. 2008.
- **Canais matriciais multiplicativos sobre corpos e anéis finitos com aplicações em codificação de rede**. NóBREGA, R. W. Tese de Doutorado UFSC.

Definição (D.Stinson)

*Seja $X \neq \emptyset$ um conjunto com v elementos e $B \neq \emptyset$ uma coleção de subconjuntos distintos de X com cardinalidade b. Definimos o par (X, B) por **t-design** com parâmetros (v, k, λ), onde $0 < k < v$ e $\lambda > 0$, e escreve (v, k, λ)-**desgin**, se:*

- *cada bloco de B contém exatamente k elementos;*
- *cada par de elementos distintos de X está contido em exatamente λ blocos.*

Observação (D.Stinson)

*Uma outra forma de denotar essa classe dos design é (v, k, λ)- **BIBD** (do Inglês, **B**alanced **I**ncomplete **B**lock **D**esign).*

Conceitos de Design Combinatório

Exemplo

Considere o conjunto $X = \{1, 2, 3, 4, 5, 6, 7\}$ *com* $B = \{123, 145, 167, 247, 256, 346, 357\}$. *O par* (X, B) *é um* $(7, 3, 1)$-*BIBD.*

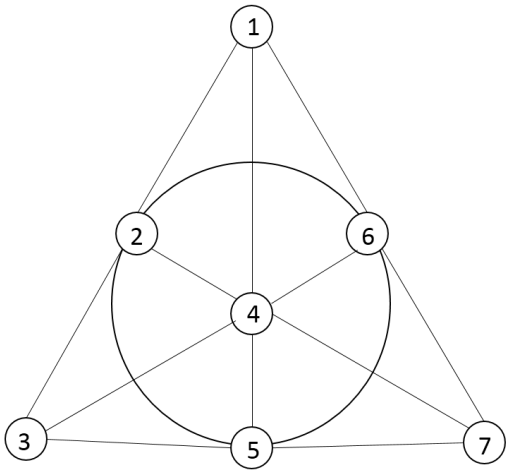


Figura: Plano de Fano

Definição (D.Stinson)

Um (v, k, λ)*-BIBD* (X, B) *diz-se* ***simétrico*** *se* $| X | = | B | = v = b$.

Exemplo

Seja $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D\}$ *e* $B = \{1234, 1567, 189A, 1BCD, 258B, 269D, 27AC, 359C, 36AB, 378D, 45AD, 468C, 479B\}$. *Assim o par* (X, B) *é um* $(13, 4, 1)$*-BIBD simétrico, onde* $b = v = 13$ *e* $r = k = 4$.

Definição (D.Stinson)

Um **design balanceado aos pares - PBD** *é um design* (X, B)*, tal que cada par de pontos distintos de* X *está contido em exatamente* λ *blocos, onde* λ *é um inteiro positivo. Além disso,* (X, B) *é um* **design balanceado aos pares regular - PBD Regular** *se todos os pontos* $x \in X$ *ocorrem exatamente em* r *blocos* $B_{i's} \in B$*, em que* r *é um inteiro positivo.*

Conceitos de Conjuntos Parcialmente Ordenados

Definição (S. Roman)

Seja P um conjunto não vazio. Dizemos que uma relação binária é um ***ordem parcial*** *em P, normalmente denotada por "$\leq$", se possui as seguintes propriedades:*

- *$a \leq a$, para todo $a \in P$ (reflexiva);*
- *Se $a, b \in P$ são tais que $a \leq b$ e $b \leq a$, então $a = b$ (anti-simétrica);*
- *Se $a, b, c \in P$ são tais que $a \leq b$ e $b \leq c$, então $a \leq c$ (transitiva).*

Observação

Neste contexto, dizemos que $(P, \leq)$ é um conjunto parcialmente ordenado. Podemos dizer ainda que se $a \leq b$ então a precede b, e que a e b são comparavéis. Dizemos ainda que b é um sucessor de a se $a < b$ e se não existe $x \in P$ tal que $a < x < b$.

Conceitos de Conjuntos Parcialmente Ordenados

Definição (S. Roman)

Seja "$\leq$" uma ordem parcial em P. Se $a \leq b$ ou $b \leq a$, para quaisquer $a, b \in P$, dizemos que "$\leq$" é uma ***ordem total*** *e que P é um* ***conjunto totalmente ordenado***.

Exemplo

Sendo G um grupo, o conjunto dos subgrupos de G, munido da relação de inclusão, é um conjunto parcialmente ordenado, normalmente denotado por $R(G)$.

Conceitos de Conjuntos Parcialmente Ordenados

Diagrama de Hasse é uma ferramenta matemática que representa graficamente qualquer conjunto finito parcialmente ordenado. O diagrama de Hasse é construido da seguinte forma:

- Os elementos do conjunto são representados por pequenos círculos (ponto);
- Se $a \leq b$, então o círculo que representa b fica a direita do circulo que representa a;
- Se b é sucessor de a, então o círculo que representa a é conectado ao círculo que representa b por um segmento de reta.

Conceitos de Conjuntos Parcialmente Ordenados

Definição (S. Roman)

Sejam P e Q dois conjuntos parcialmente ordenados. Dizemos que uma aplicação $\varphi : P \to Q$ é:

- ***isótona**, se para $a, b \in P$ tais que $a \leq b$ tivermos $\varphi(a) \leq \varphi(b)$.*
- ***antítona**, se para $a, b \in P$ tais que $a \leq b$ tivermos $\varphi(b) \leq \varphi(a)$.*

Definição (S. Roman)

*Um **isomorfismo de conjuntos ordenados** é definido como sendo uma aplicação bijetiva isótona com aplicação inversa isótona. Se existe um isomorfismo $\varphi : P \to Q$ dizemos que P e Q são conjuntos isomorfos, e denotamos por $P \simeq Q$.*

Conceitos de Conjuntos Parcialmente Ordenados

Observação

Se $\varphi : P \to Q$ é um isomorfismo de conjuntos ordenados e $x, y \in P$ são elementos distintos, então:

$$x < y \leftrightarrow \varphi(x) < \varphi(y)$$

Portanto, todas as relações hierárquicas entre elementos são preservadas por isomorfismo, portanto possuem o mesmo diagrama de Hasse. A recíproca é verdadeira, ou seja, conjuntos parcialmente ordenados que possuem mesmo diagrama de Hasse são isomorfos.

Definição (S. Roman)

Sejam P um conjunto parcialmente ordenado e $B \subseteq P$ um subconjunto limitado superiormente, ou seja, que possui cota superior em P. Um elemento $b \in P$ será chamado ***supremo*** *do conjunto B, quando b é a menor das cotas superiores de B em P, isto é:*

1. *Para todo $x \in B$, tem-se $x \leq b$;*
2. *Se $c \in P$ é talque $x \leq c$ para todo $x \in B$, então $b \leq c$.*

Definição (S. Roman)

Sejam P um conjunto parcialmente ordenado e $A \subseteq P$ um subconjunto limitado inferiormente, ou seja, que possui cota inferior em P. Um elemento $a \in P$ será chamado ***ínfimo*** *do conjunto A, quando a é a maior das cotas inferiores de A em P, isto é:*

1. *Para todo $y \in A$, tem-se $a \leq y$;*
2. *Se $c \in P$ é tal que $c \leq y$ para todo $y \in a$, então $b \leq c$.*

Conceitos de Conjuntos Parcialmente Ordenados

Definição (S. Roman)

Um conjunto parcialmente ordenado será dito um ***reticulado*** *se nele existirem o supremo e o ínfimo de qualquer par de seus elementos.*

Exemplo

Para todo grupo G, temos que $R(G)$ é um reticulado. De fato, dados dois subgrupos $H, N \leq G$, lembre que $H \cap N$ é o maior subgrupo contido em ambos. Além disso, claramente $H \subseteq \langle H \cup N \rangle$ e $N \subseteq \langle H \cup N \rangle$. Tomando, agora K subgrupo de G tal que $H \subseteq K$ e $N \subseteq K$, temos que $H \cup N \subseteq K$ e assim $\langle H \cup N \rangle \subseteq K$.

Conceitos de Conjuntos Parcialmente Ordenados

Exemplo

O conjunto de todos os subespaços de um espaço vetorial, parcialmente ordenado pela inclusão, é um reticulado. Observe que o ínfimo de dois subespaços W_1 e W_2 é a sua interseção. Veja também que se W_3 é um subespaço tal que $W_1, W_2 \subseteq W_3$, então $W_1 + W_2 \subseteq W_3$, onde:

$$W_1 + W_2 = \{w_1 + w_2; w_i \in W_i\}.$$

Assim, $W_1 + W_2$ é o supremo, ou seja, o menor subespaço que contém ambos.

Códigos Geometricamente Uniformes

Definição (G. D. Forney Jr.)

*Um conjunto de sinais S é **geometricamente uniforme** se dado dois pontos quaisquer $s, s' \in S$ existe uma isometria u tal que:*

- $u(s) = s'$
- $u(S) = S$.

Exemplo

Uma constelação de sinais binária unidimensional $S = \{-1, 1\}$ é geometricamente uniforme. Basta observarmos que o grupo de simetrias $\Gamma(S) = V = \{e, v\}$, onde e indica a identidade e v indica uma reflexão em torno da origem, satisfaz

$$v(1) = -1, \quad v(-1) = 1 \quad e \quad v(S) = S$$

Códigos Geometricamente Uniformes

Teorema (G. D. Forney Jr.)

O produto cartesiano de conjunto de sinais geometricamente uniforme é um conjunto de sinais geometricamente uniforme.

Observação

Uma observação interessante é que, se considerarmos a composição de isometrias para cada entrada separadamente, temos que o conjunto $S = \{-1, 1, \cdots, -1, 1\}$ *ainda será uma constelação de sinais, cujo grupo gerador é* V^n *com* 2^n *elementos e é isomorfo a* $\mathbb{Z}_2^n$.

Espaços Projetivos e Códigos de Subespaços

Definição (R. Koetter and F. Kschischang, A. Khaleghi, D. Silva, and F.R. Kschischang)

*O **espaço projetivo** é definido como o conjunto de todos os subespaços vetoriais de $\mathbb{F}_q^m$ e é denotado por $\mathbb{P}(\mathbb{F}_q^m)$. Além disso, o conjunto de todos os subespaços com uma dada dimensão k é denominado **Grassmanniana** e denotado por $\mathcal{G}(\mathbb{F}_q^m, k)$.*

Observação

Note que:

$$\mathbb{P}(\mathbb{F}_q^m) = \bigcup_{k=0}^{m} \mathcal{G}(\mathbb{F}_q^m, k).$$

Definição (R. Koetter and F. Kschischang)

*O **número de subespaços vetoriais** de $\mathbb{P}(\mathbb{F}_q^m)$ com dimensão k é dado por*

$$\binom{m}{k}_q = \prod_{i=0}^{k-1} \frac{q^m - q^i}{q^k - q^i}.$$

Definição (R. Koetter and F. Kschischang)

*A **cardinalidade de uma Grassmanniana** de $\mathbb{P}(\mathbb{F}_q^m)$ com dimensão k é*

$$\mid \mathcal{G}(\mathbb{F}_q^m, k) \mid = \binom{m}{k}_q.$$

*e a **cardinalidade do espaço projetivo** de $\mathbb{P}(\mathbb{F}_q^m)$ é*

$$\mid \mathbb{P}(\mathbb{F}_q^m) \mid = \sum_{k=0}^{m} \binom{m}{k}_q.$$

Espaços Projetivos e Códigos de Subespaços

Definição (R. Koetter and F. Kschischang, A. Khaleghi, D. Silva, and F.R. Kschischang)

*A **distância de subespaço** entre U e V é definida como:*

$$d(U,V) = dim(U) + dim(V) - 2dim(U \cap V), \tag{1}$$

onde $+$ e $\cap$ representam, respectivamente, a soma e a interseção de subespaços.

Teorema

$(\mathbb{P}(\mathbb{F}_q^m), d)$ é um espaço métrico.

Espaços Projetivos e Códigos de Subespaços

Definição (R. Koetter and F. Kschischang, A. Khaleghi, D. Silva, and F.R. Kschischang)

*Um **código de subespaço** é um conjunto não vazio de $\mathbb{P}(\mathbb{F}_q^m)$. No caso em que o código de subespaço está contido em uma Grassmanniana de ordem k, $\mathcal{G}(\mathbb{F}_q^m, k) = \{V \in \mathbb{P}(\mathbb{F}_q^m) : dimV = k\}$, ou seja, todas as suas palavras códigos possuem a mesma dimensão, ele será chamado **código de subespaço de dimensão constante**. Denotamos por d a distância mínima do código $\mathcal{C}$.*

Definição (R. Koetter and F. Kschischang, A. Khaleghi, D. Silva, and F.R. Kschischang)

*A **cardinalidade** do código $\mathcal{C}$ é dada por $\mid \mathcal{C} \mid = M$ e a **taxa do código** é definida por $R(\mathcal{C}) = \frac{log|\mathcal{C}|}{m}$ ou $R(\mathcal{C}) = \frac{logM}{m}$ medida em unidades de informação por uso de canal de subespaço, onde q é a base do logaritmo.*

Definição (R. Koetter and F. Kschischang)

*A **distância mínima** do código $\mathcal{C}$ é definida como:*

$$d = d(\mathcal{C}) = min\{d(U, V),\ U,\ V \in \mathcal{C},\ U \neq V\}.$$

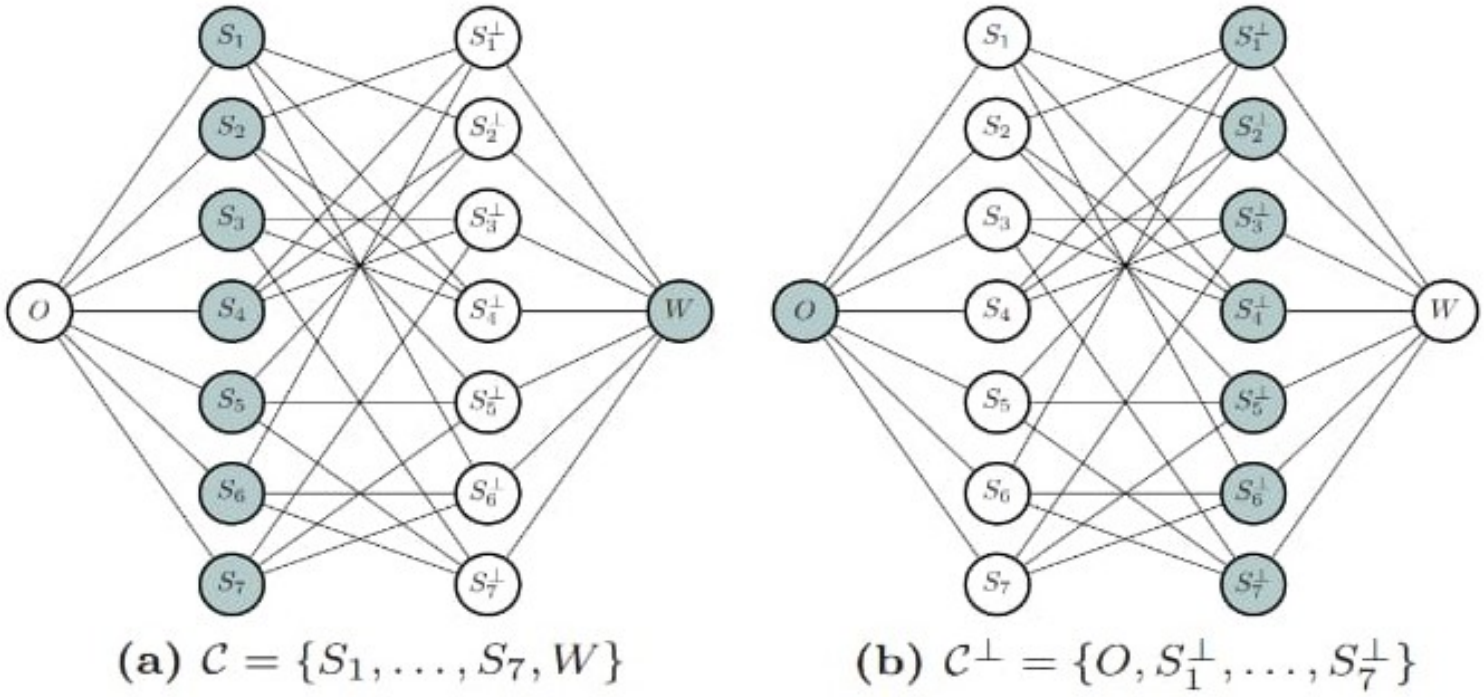
Definição

*Seja (m, M, d) os **parâmetros** do código $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)$, onde m é a dimensão do espaço projetivo, M é a cardinalidade do código e d a distância mínima do código. Se o código $\mathcal{C}$ está em uma Grassmanniana de dimensão k os parâmetros são (m, M, d, k).*

Espaços Projetivos e Códigos de Subespaços

Uma forma de interpretar a distância de subespaço é por meio do diagrama de Hasse.

- Neste contexto, é possível construir o diagrama de Hasse, visto que o espaço projetivo $\mathbb{P}(F_q^m)$ com a seguinte relação de ordem $\preceq$, em que $S_1 \preceq S_2$ se, e somente se, S_1 é subespaço de S_2, é parcialmente ordenado.
- Dois subespaços estão conectados, se e somente se, S_1 é subespaço de S_2 e $dim S_2 = dim S_1 + 1$ ou vice-versa. Logo, a partir do diagrama de Hasse, podemos interpretar a distância entre dois subespaços S_1, S_2 de $\mathbb{P}(F_q^m)$ como o caminho de menor distância ligando S_1 e S_2 (geodésica).



(a) $\mathcal{C} = \{S_1, \ldots, S_7, W\}$ **(b)** $\mathcal{C}^\perp = \{O, S_1^\perp, \ldots, S_7^\perp\}$

Exemplos de Códigos de Subespaços Nóbrega.R. W. e Uchôa-Filho, B. F.

Espaços Projetivos e Códigos de Subespaços

Exemplo

Seja o espaço vetorial $\mathbb{F}_2^3$. *Um exemplo interessante de código na Grassmanniana é o código simplex* $\mathcal{C}_2 = \{S^3, S^5, S^6\}$ *com parâmetros* $(n, M, d, k) = (3, 3, 2, 2)$, *cujas palavras-código, ou seja, os subespaços vetoriais são* $S^3 = \{000, 011, 100, 111\}$, $S^5 = \{000, 010, 101, 111\}$, $S^6 = \{000, 001, 110, 111\}$. *Observe que os subespaços* S_1, S_2, S_3 *tem dimensão 2 e a intersecção entre quaisquer dois deles é o subespaço* $S_7 = \{000, 111\}$. *Assim, a distância é dada por:*

$$d(S_i, S_j) = dim(S_i) + dim(S_j) - 2.dim(S_i \cap S_j) = 2 + 2 - 2.1 = 4 - 2 = 2,$$

para quaisquer $i, j \in \{1, 2, 3\}$ *com* $i \neq j$.

$$
\begin{array}{lcllcl}
O & = & \{000\} & W & = & \{000, 001, \ldots, 110, 111\} \\
S_1 & = & \{000, 001\} & S_1^{\perp} & = & \{000, 010, 100, 110\} \\
S_2 & = & \{000, 010\} & S_2^{\perp} & = & \{000, 001, 100, 101\} \\
S_3 & = & \{000, 011\} & S_3^{\perp} & = & \{000, 011, 100, 111\} \\
S_4 & = & \{000, 100\} & S_4^{\perp} & = & \{000, 001, 010, 011\} \\
S_5 & = & \{000, 101\} & S_5^{\perp} & = & \{000, 010, 101, 111\} \\
S_6 & = & \{000, 110\} & S_6^{\perp} & = & \{000, 001, 110, 111\} \\
S_7 & = & \{000, 111\} & S_7^{\perp} & = & \{000, 011, 101, 110\}
\end{array}
$$

Subespaços do Espaço projetivo $\mathbb{P}(\mathbb{F}_2^3)$

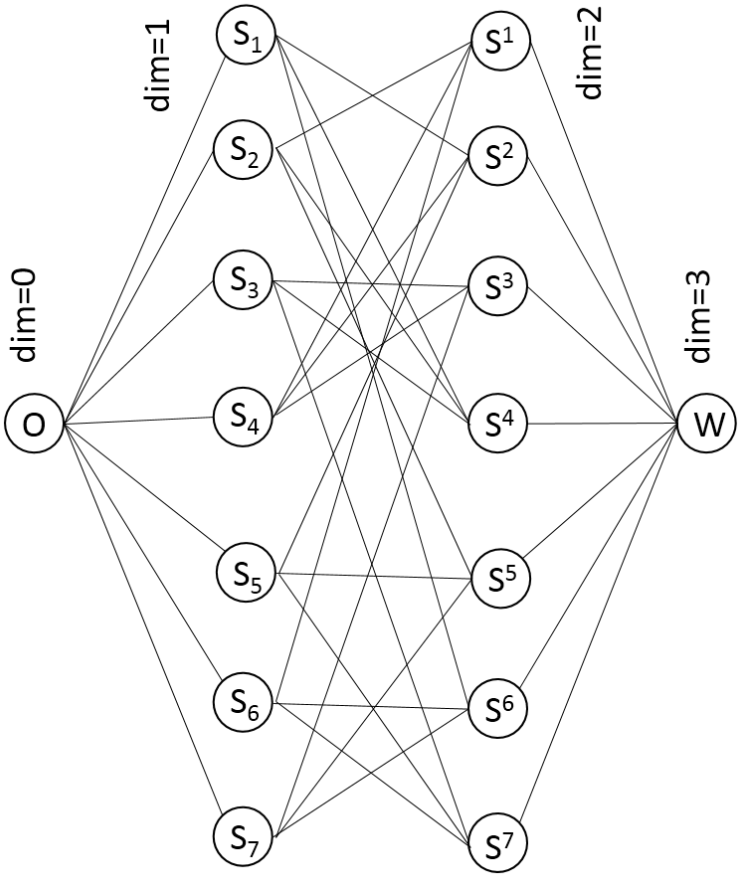


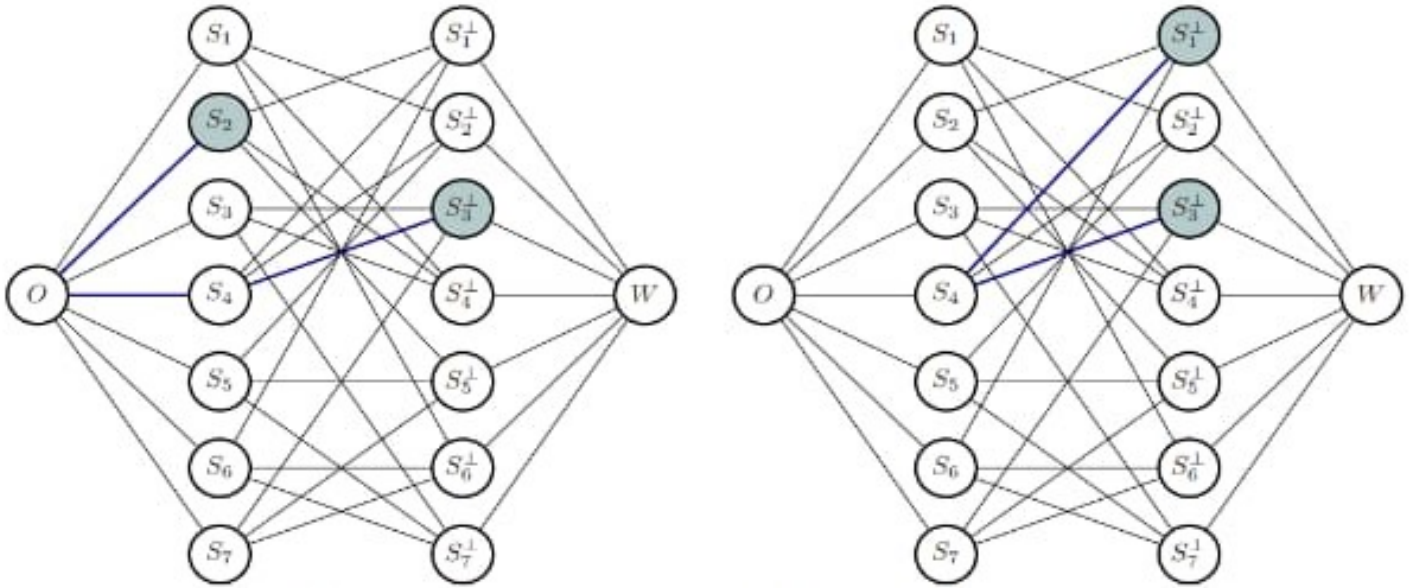
Figura: Diagrama de Hasse do Espaço projetivo $\mathbb{P}(\mathbb{F}_2^3)$

Espaços Projetivos e Códigos de Subespaços

Lema (R. Koetter and F. Kschischang, A. Khaleghi, D. Silva, and F.R. Kschischang)

Sejam U e V subespaços de um espaço vetorial de dimensão m. Então a distância é máxima, isto é, $d(U,V) = m$, se, e somente se,

1. *Os subespaços U e V se intersectam em um subespaço de dimensão 0;*
2. $dim(U) + dim(V) = m$.



(a) De S_2 a $S_3^\perp$; comprimento 3. **(b)** De $S_1^\perp$ a $S_3^\perp$; comprimento 2.

Nóbrega.R. W. e Uchôa-Filho, B. F.

Espaços Projetivos e Códigos de Subespaços

Exemplo

Considere os subespaços S_1, S_2, S_3, S_4 elementos da Grassmanniana $\mathcal{G}(F_2^4, 2)$, dados por:

$$S_1 = \{0000, 1000, 0100, 1100\} \quad S_2 = \{0000, 0010, 0001, 0011\}$$

$$S_3 = \{0000, 1000, 0010, 1010\} \quad S_4 = \{0000, 0100, 0010, 0110\}$$

A distância de subespaço entre S_1 e S_2 é dada por:

$$d_s(S_1, S_2) = dimS_1 + dimS_2 - 2dim(S_1 \cap S_2) = 2 + 2 - 0 = 4$$

Já a distância de subespaço entre S_1 e S_3 é dada por:

$$d_s(S_1, S_3) = dimS_1 + dimS_3 - 2dim(S_1 \cap S_3) = 2 + 2 - 2.1 = 2$$

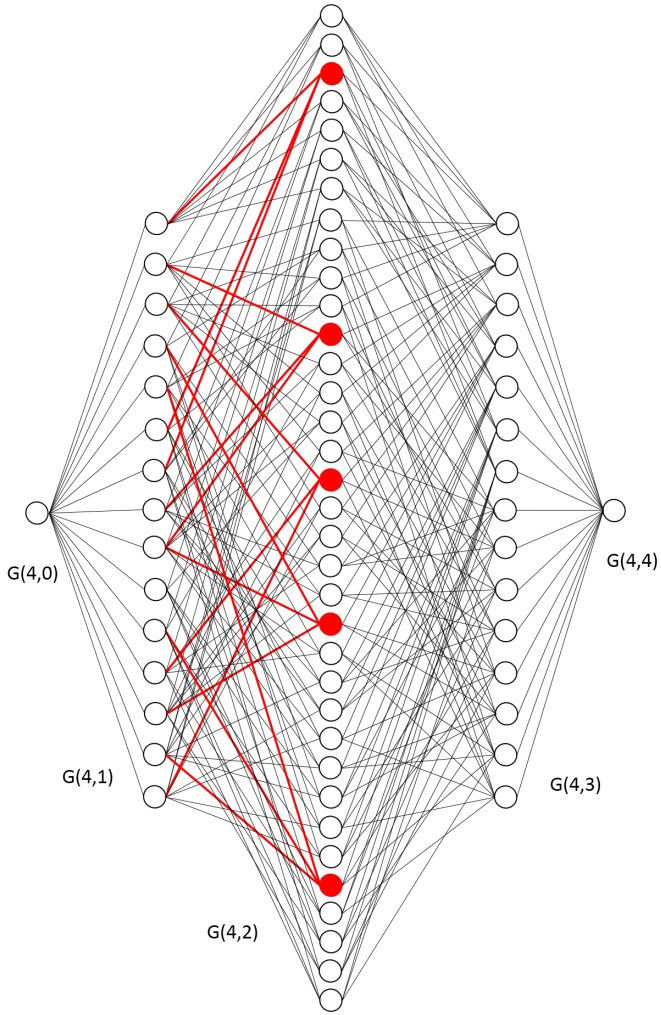


Figura: Espaço projetivo $\mathbb{P}(F_2^4)$

Um problema não trivial, assim como no caso clássico (códigos no hipercubo de Hamming) é encontrar o maior tamanho possível de um código de subespaço dados os parâmetros q e m e fixada uma distância miníma d. Sugestão: **http://subspacecodes.uni-bayreuth.de/table/2**

$$A_q(m,d) = max\{\mid \mathcal{C} \mid : \mathcal{C} \subseteq \mathbb{P}(F_q^m), d(\mathcal{C}) = d\} \tag{2}$$

Exemplo

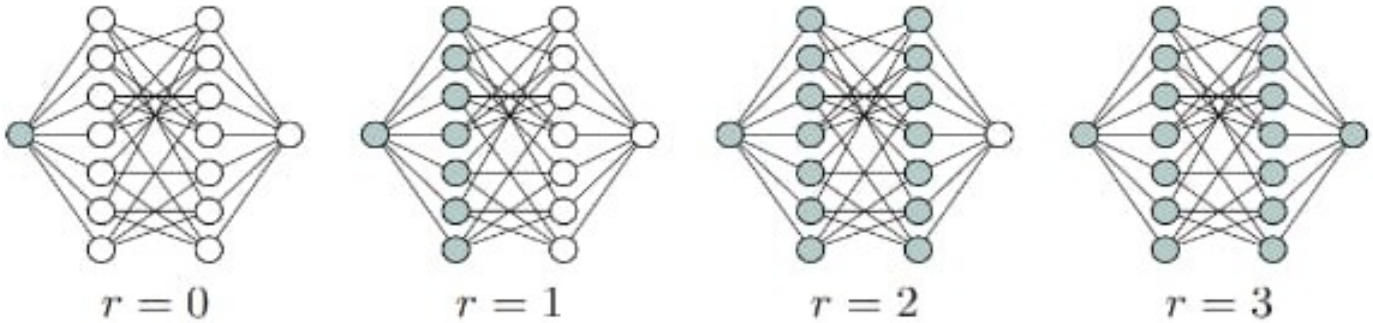
*A **esfera** de centro V_0 e raio r é dada por*

$$\beta_{(q,m)}(V_0, r) = \{V \in \mathbb{P}(F_q^m) : d(V, V_0) \leq r\} \tag{3}$$

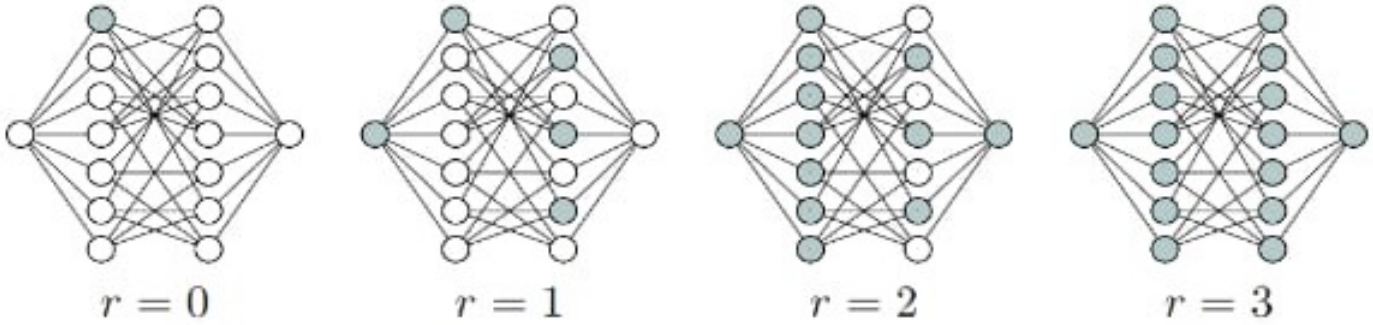
*e o **volume** dessa esfera é definido por*

$$Vol_{(q,m)}(V_0, r) = \mid \beta_{(q,m)}(V_0, r) \mid, \tag{4}$$

isto é, o número de pontos nela situados.



(a) Esferas centradas em O.



(b) Esferas centradas em S_1.

Nóbrega.R. W. e Uchôa-Filho, B. F.

Observar que o espaço projetivo com a distância de subespaço não é um espaço métrico regular.

Definição (R. Nóbrega and B. Uchôa-Filho)

*A **n-ésima extensão** do espaço projetivo $\mathbb{P}(\mathbb{F}_q^m)$ denotada por $\mathbb{P}(\mathbb{F}_q^m)^n$, é o n-ésimo produto cartesiano do espaço projetivo. Dessa forma, elementos de $\mathbb{P}(\mathbb{F}_q^m)^n$ são n-uplas tendo como componentes subespaços do espaço projetivo original $\mathbb{P}(\mathbb{F}_q^m)$.*

Definição (R. Nóbrega and B. Uchôa-Filho)

*A **distância (de subespaço estendida)** entre dois elementos $\boldsymbol{U} = (U_1, U_2, \cdots, U_n)$ e $\boldsymbol{V} = (V_1, V_2, \cdots, V_n)$ do espaço projetivo estendido $\mathbb{P}(\mathbb{F}_q^m)^n$ é definida como:*

$$d(\boldsymbol{U}, \boldsymbol{V}) = \sum_{i=1}^{n} d(U_i, V_i), \tag{5}$$

onde $d(U_i, V_i) = dim(U_i) + dim(V_i) - 2dim(U_i \cap V_i)$ para $i \in \{1, 2, \cdots, n\}$. Tem-se $1 \leq d(\boldsymbol{U}, \boldsymbol{V}) \leq m.n.$

Espaços Projetivos Estendidos e Códigos de Subespaços n-shot

Teorema

$(\mathbb{P}(\mathbb{F}_q^m)^n, d)$ *é um espaço métrico.*

Definição (R. Nóbrega and B. Uchôa-Filho)

Um ***código de bloco de subespaços*** *é um subconjunto não vazio* $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ *denominado* ***código de subespaço n-shot****.*

Definição

A ***cardinalidade do código*** $\mathcal{C}$ *é dada por* $|\mathcal{C}| = M^n$ *e a* ***taxa do código*** *é definida por* $R(\mathcal{C}) = \frac{log|\mathcal{C}|}{m.n}$ *ou* $R(\mathcal{C}) = \frac{logM^n}{m.n}$ *medida em unidades de informação por uso de canal de subespaço, onde q é a base do logaritmo.*

Espaços Projetivos Estendidos e Códigos de Subespaços n-shot

Definição

*A **distância mínima** do código $\mathcal{C}$ é definida como:*

$$d = d(\mathcal{C}) = min\{d(\boldsymbol{U}, \boldsymbol{V}),\ \boldsymbol{U},\ \boldsymbol{V} \in \mathcal{C},\ \boldsymbol{U} \neq \boldsymbol{V}\},$$

onde $1 \leq d(\mathcal{C}) \leq m.n$ *e* $0 \leq R(\mathcal{C}) \leq 1$.

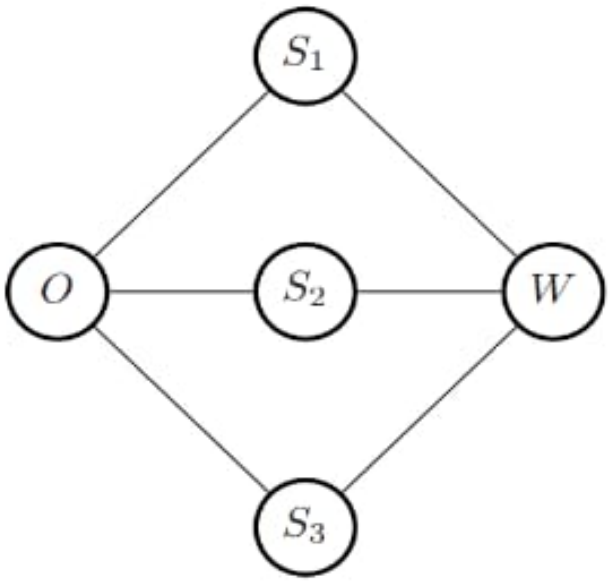
Definição

*Os **parâmetros** do código de subepaço n-shot* $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ *é denotado por* $(m.n, M^n, d)$ *onde* $m.n$ *é a dimensão do espaço projetivo,* M^n *é a cardinalidade do código e* d *a distância mínima do código. Se o código* $\mathcal{C}$ *está em uma Grassmanniana de dimensão* $k.n$ *os parâmetros do código são* $(m.n, M^n, d, k.n)$.

Motivação

Exemplo

Suponhamos que se queira um código de subespaço n-shot utilizando o espaço projetivo $\mathbb{P}(\mathbb{F}_2^2)$.



$$O = \{00\}$$

$$S_1 = \{00, 01\}$$

$$S_2 = \{00, 10\}$$

$$S_3 = \{00, 11\}$$

$$W = \{00, 01, 10, 11\}$$

Exemplo

Uma primeira possibilidade é simplesmente estender o melhor código de $\mathbb{P}(\mathbb{F}_2^2)$ *com distância d=2, que é* $\mathcal{C} = \{S_1, S_2, S_3\}$ *Fazendo isto temos:* $\mathcal{C}_1 = \mathcal{C} \times \mathcal{C} = \{S_1, S_2, S_3\} \times \{S_1, S_2, S_3\} = \{S_1S_1, S_1S_2, \cdots, S_3S_3\}$, *com* $\mid \mathcal{C} \mid = 9$. *Uma outra possibilidade seria olhar para o mapeamento bijetivo entre* $\{O, S_1, S_2, S_3, W\}$ *e* $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ *e para o código clássico ótimo de comprimento 2 sobre* $\mathbb{Z}_5$ *com distância mínima de Hamming 2 que é o código de repetição* $\mathcal{H}_2 = \{00, 11, 22, 33, 44\}$ *que mapeado de volta fica* $\mathcal{C}_2 = \{OO, S_1S_1, S_2S_2, S_3S_3, WW\}$ *com* $\mid \mathcal{C}_2 \mid = 5$.

Observação

1) Essa segunda possibilidade desconsiderou a estrutura de subespaço por trás de $\mathbb{P}(\mathbb{F}_2^2)$ *e fez uso apenas de codificação clássica.*

2) É necessário projetar códigos nos espaço métrico $\mathbb{P}(\mathbb{F}_2^2)^2$ *pois leva em consideração tanto a estrutura de subespaço quanto a evolução temporal.*

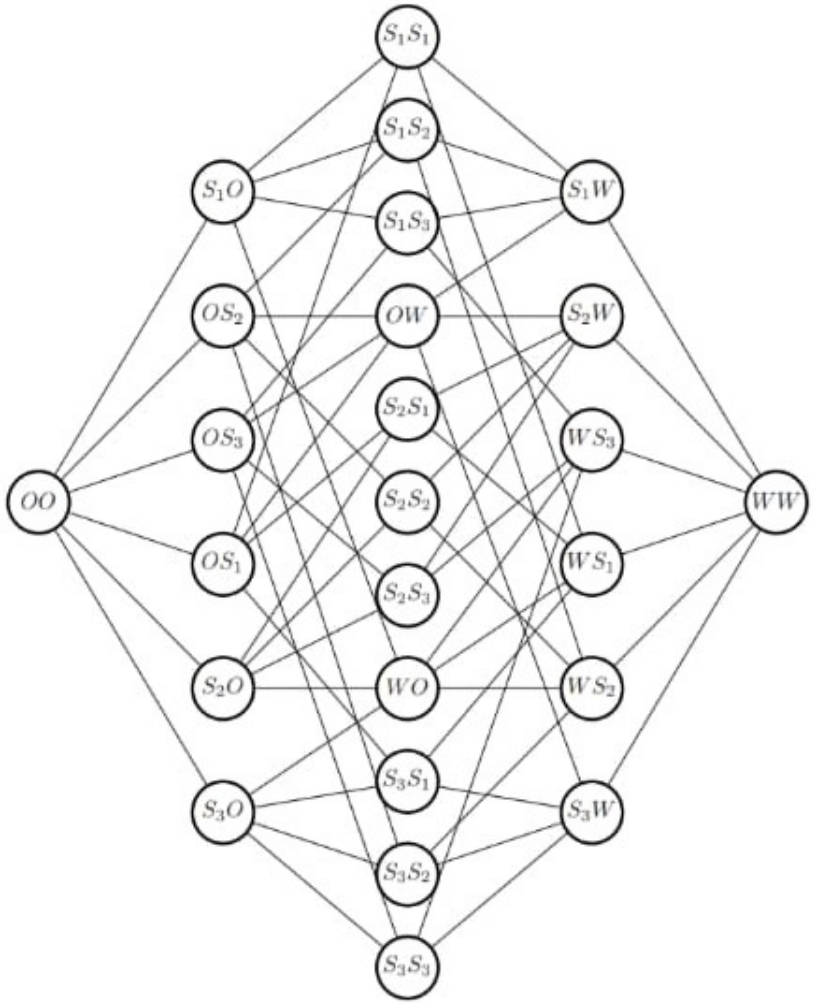


Figura: Subespaços de $\mathbb{P}(\mathbb{F}_2^2)^2$

Mapeamento por Mapeamentos de Conjuntos

Dado um conjunto $\mathbf{S}$, um particionamento L- nível de $\mathbf{S}$ é definido como uma sequência de $L+1$ partições $\Gamma_0, \cdots, \Gamma_L$ tal que:

- a partição do nível 0 consiste no conjunto $\mathbf{S}$ completo, isto é, $\Gamma_0 = \{\mathbf{S}\}$.
- a partição Γ_l é um refinamento da partição Γ_{l-1}, para $l = 1, \cdots, L$.
- a partição do nível L consiste nos subconjuntos unitários de $\mathbf{S}$, isto é, $\Gamma_L = \{\{s\} : s \in \mathbf{S}\}$.

Definição (G. Ungerboeck)

*Dado um conjunto $\boldsymbol{S}$, uma **partição** de $\boldsymbol{S}$ consiste em uma coleção $\Gamma = \{\boldsymbol{S}_1, \cdots, \boldsymbol{S}_p\}$ de p subconjuntos não vazios de $\boldsymbol{S}$ tais que:*

- *a união de todos os elementos da partição é igual ao conjunto $\boldsymbol{S}$: $\boldsymbol{S}_1 \cup \cdots \cup \boldsymbol{S}_p = \boldsymbol{S}$.*
- *a interseção de quaisquer dois elementos da partição é vazia: $\boldsymbol{S}_i \cap \boldsymbol{S}_j = \oslash$, $i \neq j$.*

Definição (R. Calderbank)

*A **distância de subespaço intrasubset** do nível l é definida por*

$$d_s^{(l)} = min\{d_s(\mathcal{X}) : \mathcal{X} \in \Gamma_l\}$$

para $l = 0, \cdots, L$. Tem-se sempre $d_s^{(0)} = d_s(\boldsymbol{S})$ e $d_s^{(L)} = \infty$.

Observação

*A construção multinível pode ser aninhada, ou seja, cada nó pai do nível anterior tem o mesmo número de nó filhos, do nível posterior, então tais níveis devem ser "protegidos"por códigos clássicos de comprimento n sobre $\mathbb{Z}_2$, chamados **códigos componentes** e denotados por H_l, com distâncias (de Hamming) mínimas $d_H^{(l)} = d_H(H_l)$ ou não aninhada, no caso do exemplo abaixo. Logo, a distância mínima do código de subespaço projetado é limitada inferiormente por:*

$$d_S(C) \geq min\{d_S^{(l-1)}.\ d_H^{(l)} : 1 \leq l \leq L'\}$$

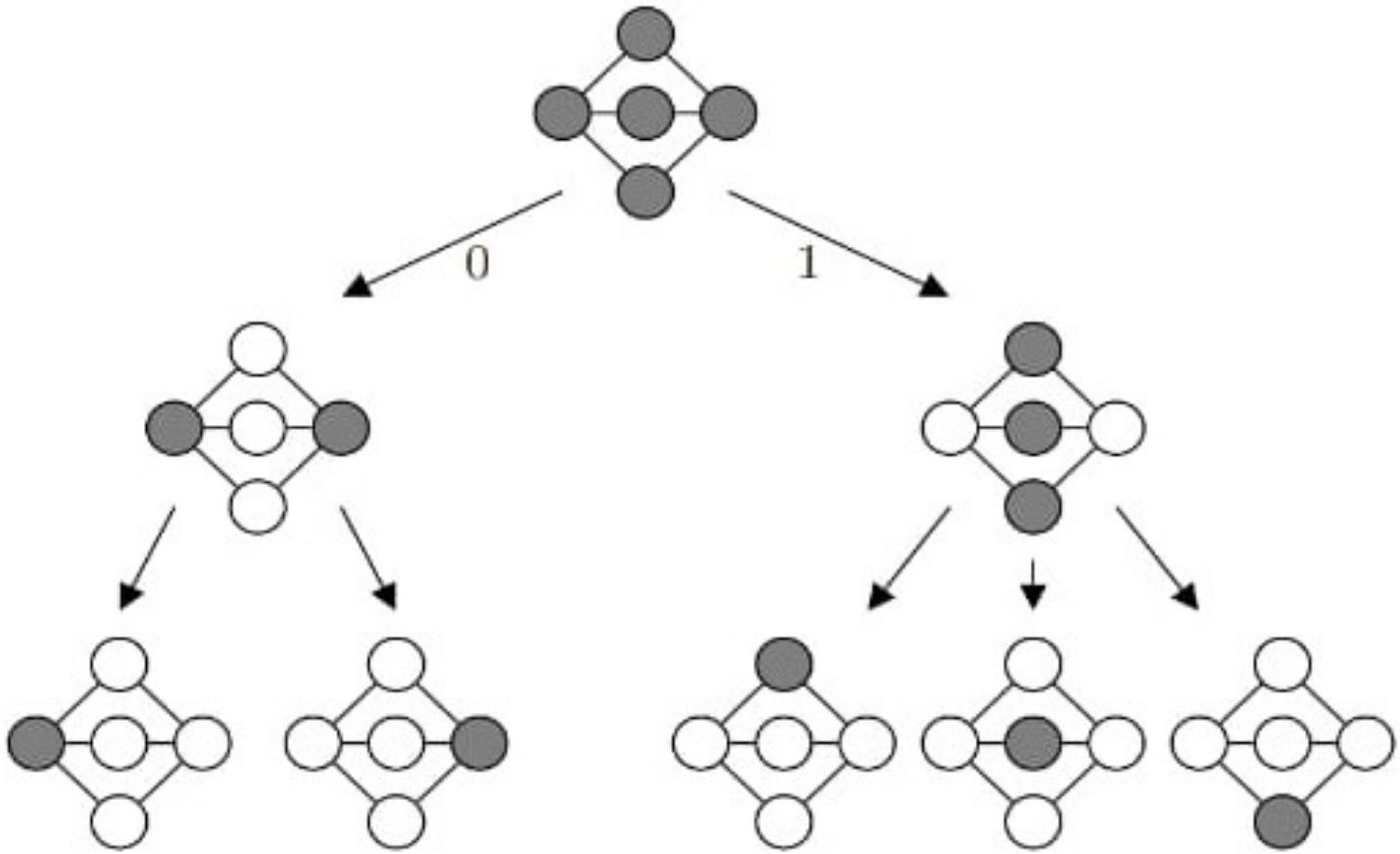


Figura: Particionamento de $\mathbb{P}(\mathbb{F}_2^2)$: Nóbrega.R. W. e Uchôa-Filho, B. F.

$$\begin{aligned} \mathcal{C}_3 &= \{O, W\} \times \{O, W\} \cup \\ &\quad \{S_1, S_2, S_3\} \times \{S_1, S_2, S_3\} \\ &= \{OO, OW, WO, WW, \\ &\quad S_1S_1, S_1S_2, \ldots, S_3S_2, S_3S_3\}, \end{aligned}$$

Código construído com o código de repetição {00,11}

Observação

Cabe observar que no caso da codificação clássica, a extensão $(\mathbb{Z}_q^m)^n$ *é equivalente a* $(\mathbb{Z}_q^{mn})$*, no sentido em que existe uma isometria entre esses dois espaços métricos. Esse fato, no entanto, não ocorre na codificação de subespaço, contudo, a n-ésima extensão de um espaço projetivo* $\mathbb{P}(\mathbb{F}_q^m)^n$*, ainda pode ser vista como um "subconjunto"do espaço projetivo maior* $\mathbb{P}(\mathbb{F}_q^{mn})$*.*

Códigos de Subespaços n-shot Geometricamente Uniforme

Definição

Um ***código de subespaço n-shot $\mathcal{C}$ é geometricamente uniforme*** *se dado quaisquer dois vetores de subespaços $\boldsymbol{U}, \boldsymbol{V} \in \mathcal{C}$ existe uma isometria I tal que:*

- $I(\boldsymbol{U}) = \boldsymbol{V}$
- $I(\mathcal{C}) = \mathcal{C}$

Códigos de Subespaços n-shot Geometricamente Uniforme

Lema

A transformação,

$$T_{ij} : \boldsymbol{\mathcal{C}} = \overbrace{\mathcal{C} \times \mathcal{C} \times \cdots \times \mathcal{C}}^{n-vezes} \subseteq \mathbb{P}(\mathbb{F}_q^m)^n \to \boldsymbol{\mathcal{C}} = \overbrace{\mathcal{C} \times \mathcal{C} \times \cdots \times \mathcal{C}}^{n-vezes} \subseteq \mathbb{P}(\mathbb{F}_q^m)^n,$$

onde o código de subespaço $\boldsymbol{\mathcal{C}}$ é o produto cartesiano n-vezes do código de subespaço $\mathcal{C}$, definida por:

$$\begin{cases} T_{ij}(\boldsymbol{U}_i) = \boldsymbol{U}_j \\ T_{ji}(\boldsymbol{U}_j) = \boldsymbol{U}_i \\ T_{ij}(\boldsymbol{U}_k) = \boldsymbol{U}_k \quad k \neq i, j \end{cases} \tag{6}$$

é uma isometria para quaiquer $i, j \in \{1, \cdots, n\}$.

Códigos de Subespaços n-shot Geometricamente Uniforme

Definição (J. Rotman)

Se G é um p-grupo Abeliano para algum primo p, então G é chamado ***grupo p-primário****.*

Teorema (J. Rotman)

*(**Decomposição Primária**) Cada grupo Abeliano finito G é uma soma direta de grupos p-primários.*

Teorema (J. Rotman)

Cada grupo Abeliano finito G é uma soma direta de grupos cíclicos.

Exemplo

Neste exemplo iremos considerar a construção dos códigos de subespaço 1-shot, 2-shot e 3-shot geometricamente uniforme. Considere o espaço projetivo $\mathbb{P}(\mathbb{F}_2^2)$.

- *O código de subespaço 1-shot* $\mathcal{C}_1^{(1)}$ *é especificado por* $\mathcal{C}_1^{(1)} = \{S_1, S_2\}$, *onde* $S_1 = \{00, 10\}$ *e* $S_2 = \{00, 01\}$. *Sejam* $P_0 = [1 \quad 0]$ *a matriz geradora de* S_1 *e* $P_1 = [0 \quad 1]$ *a matriz geradora de* S_2. *Existe um subgrupo Abeliano, neste caso, um subgrupo cíclico* Q_1, *dado por:*

$$Q_1 = \left\{ Q_1^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, Q_2^{(1)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\},$$

do grupo das permutações que age transitivamente nas palavras-código de $\mathcal{C}_1^{(1)}$, *onde* $Q_j^{(i)}$ *são elementos do grupo para j variando dentro da cardinalidade do código e i associado à n-ésima extensão do código, ou seja:*

Exemplo

$$P_0.Q_1^{(1)} = P_0 \qquad [1 \quad 0].\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = [1 \quad 0]$$

e

$$P_0.Q_2^{(1)} = P_1 \qquad [1 \quad 0].\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = [0 \quad 1].$$

ou

$$P_1.Q_1^{(1)} = P_0 \qquad [0 \quad 1].\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = [0 \quad 1]$$

e

$$P_1.Q_2^{(1)} = P_1 \qquad [0 \quad 1].\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = [1 \quad 0].$$

Portanto, $\mathcal{C}_1^{(1)}$ *é um código de subespaço 1-shot geometricamente uniforme com parâmetros* $(m, M, d, k) = (2, 2, 2, 1)$*, cuja taxa do código é* $R(\mathcal{C}_1^{(1)}) = \frac{log_2 2^1}{2 \cdot 1} = \frac{1}{2} = 0,5.$

Exemplo

- *A extensão do código* $\mathcal{C}_1^{(1)}$ *para o caso código de subespaço 2-shot* $\boldsymbol{\mathcal{C}}_1^{(2)}$, *é*
$\boldsymbol{\mathcal{C}}_1^{(2)} = \mathcal{C}_1^{(1)} \times \mathcal{C}_1^{(1)} = \{S_1, S_2\} \times \{S_1, S_2\} = \{S_1S_1, S_1S_2, S_2S_1, S_2S_2\}$
onde:

$$S_1S_1 = \{0000, 0010, 1000, 1010\} = \langle 0010, 1000 \rangle,$$
$$S_1S_2 = \{0000, 0001, 1000, 1001\} = \langle 0001, 1000 \rangle,$$
$$S_2S_1 = \{0000, 0010, 0100, 0110\} = \langle 0010, 0100 \rangle,$$
$$S_2S_2 = \{0000, 0001, 0100, 0101\} = \langle 0001, 0100 \rangle.$$

onde $\langle e_1, e_2, \cdots, e_k \rangle$ *denota os geradores canônicos do subespaço. As matrizes* P_0, P_1, P_2, P_3 *são matrizes compostas pelos geradores nas linhas, dos respectivos subespaços acima, isto é,*
$P_0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ *gera* S_1S_1, $P_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ *gera* S_1S_2.

Exemplo

$P_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ *gera* S_2S_1. $P_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ *gera* S_2S_2.

Obtemos os seguintes elementos de um subgrupo Abeliano do grupo das permutações, da seguinte maneira:

$$Q_1^{(2)} = Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)},$$
$$Q_2^{(2)} = Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)},$$
$$Q_3^{(2)} = Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)},$$
$$Q_4^{(2)} = Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)}.$$

Tal que: $P_iQ_1^{(2)} = P_i$, $P_iQ_2^{(2)} = P_{(i+1)mod\ 4}$, $P_iQ_3^{(2)} = P_{(i+2)mod\ 4}$, $P_iQ_4^{(2)} = P_{(i+3)mod\ 4}$ *para qualquer* $i \in \{0, 1, 2, 3\}$, *onde a representação matricial de* Q_2 *é dada por:*

Exemplo

$$Q_2 = \left\{ Q_1^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, Q_2^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \right.$$

$$\left. Q_3^{(2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, Q_4^{(2)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right\}.$$

Assim, como cada elemento do grupo Q_2 age transitivamente nos elementos do código de subespaço 2-shot $\mathcal{C}_1^{(2)}$ temos que $\mathcal{C}_1^{(2)}$ é um código de subespaço 2-shot geometricamente uniforme com parâmetros $(m.n, M^n, d, k.n) = (4, 4, 2, 2)$, onde a taxa do código $R(\mathcal{C}_1^{(2)}) = \frac{log_2 4^2}{4 \cdot 2} = \frac{log_2 2^4}{8} = \frac{1}{2} = 0,5.$

Exemplo

- *Para o caso do código de subespaço 3-shot* $\mathcal{C}_1^{(3)}$*, temos:*

$$\begin{aligned}\mathcal{C}_1^{(3)} &= \{S_1, S_2\} \times \{S_1, S_2\} \times \{S_1, S_2\} \\ &= \{S_1S_1S_1, S_1S_1S_2, S_1S_2S_1, S_1S_2S_2, S_2S_1S_1, S_2S_1S_2, S_2S_2S_1, S_2S_2S_2\}\end{aligned}$$

$$\begin{aligned}S_1S_1S_1 &= \langle 000010, 001000, 100000\rangle, \\ S_1S_1S_2 &= \langle 000001, 001000, 100000\rangle, \\ S_1S_2S_1 &= \langle 000010, 000100, 100000\rangle, \\ S_1S_2S_2 &= \langle 000001, 000100, 100000\rangle, \\ S_2S_1S_1 &= \langle 000010, 001000, 010000\rangle, \\ S_2S_1S_2 &= \langle 000001, 001000, 010000\rangle, \\ S_2S_2S_1 &= \langle 000010, 000100, 010000\rangle, \\ S_2S_2S_2 &= \langle 000001, 000100, 010000\rangle.\end{aligned}$$

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \cdots, P_7 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

$$\begin{aligned}
Q_1^{(3)} &= Q_1^{(1)} \times Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)} \oplus Q_1^{(1)}, \\
Q_2^{(3)} &= Q_1^{(1)} \times Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)} \oplus Q_2^{(1)}, \\
Q_3^{(3)} &= Q_1^{(1)} \times Q_2^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)} \oplus Q_1^{(1)}, \\
Q_4^{(3)} &= Q_1^{(1)} \times Q_2^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)} \oplus Q_2^{(1)}, \\
Q_5^{(3)} &= Q_2^{(1)} \times Q_1^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)} \oplus Q_1^{(1)}, \\
Q_6^{(3)} &= Q_2^{(1)} \times Q_1^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)} \oplus Q_2^{(1)}, \\
Q_7^{(3)} &= Q_2^{(1)} \times Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)} \oplus Q_1^{(1)}, \\
Q_8^{(3)} &= Q_2^{(1)} \times Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)} \oplus Q_2^{(1)}.
\end{aligned}$$

Exemplo

Os elementos do grupo Q_3 agem transitivamente nos elementos do código $\mathcal{C}_1^{(3)}$ da seguinte maneira:

- $P_i Q_1^{(3)} = P_i$,
- $P_i Q_2^{(3)} = P_{(i+1) mod\ 8}$
- $P_i Q_3^{(3)} = P_{(i+2) mod\ 8}$
- $P_i Q_4^{(3)} = P_{(i+3) mod\ 8}$
- $P_i Q_5^{(3)} = P_{(i+4) mod\ 8}$
- $P_i Q_6^{(3)} = P_{(i+5) mod\ 8}$
- $P_i Q_7^{(3)} = P_{(i+6) mod\ 8}$
- $P_i Q_8^{(3)} = P_{(i+7) mod\ 8}$

para qualquer $i \in \{0, \cdots, 7\}$. $\mathcal{C}_1^{(3)}$ é um código de subespaço 3-shot geometricamente uniforme: $(m.n, M^n, d, k.n) = (6, 8, 2, 3)$.

Códigos de Subespaços n-shot Geometricamente Uniforme

Definição

Seja $\mathcal{C} = \{S_1, S_2, \cdots, S_M\}$ *um código de subespaço 1-shot. Dizemos que* $\mathcal{C}$ *é um* ***código de subespaço 1-shot geometricamente uniforme*** *com parâmetros* (m, M, d, k) *para algum espaço projetivo* $\mathbb{P}(\mathbb{F}_2^m)$ *conveniente, se existe um subgrupo Abeliano* $Q_1 = \{Q_1^{(1)}, Q_2^{(1)}, \cdots, Q_M^{(1)}\}$ *tal que os elementos de* Q_1 *agem transitivamente sobre os subespaços de* $\mathcal{C}$*, representados pelas matrizes* $P_0, P_1, \cdots, P_M$*, ou seja,* $P_i Q_1 = P_i, P_i Q_2 = P_{(i+1) mod\ M}, \cdots, P_i Q_M = P_{(i+(M-1)) mod\ M}$.

Códigos de Subespaços n-shot Geometricamente Uniforme

Proposição

Seja a n-ésima extensão do código $\mathcal{C}$, dada por, $\boldsymbol{\mathcal{C}} = \mathcal{C} \times \mathcal{C} \times \cdots \times \mathcal{C}$ e a n-ésima extensão do espaço projetivo $\mathbb{P}(\mathbb{F}_q^m)$, como sendo, $\mathbb{P}(\mathbb{F}_q^m)^n$. O código $\boldsymbol{\mathcal{C}}$ é um ***código de subespaço n-shot geometricamente uniforme*** *em $\mathbb{P}(\mathbb{F}_q^m)^n$ com parâmetros $(m.n, M^n, d, k.n)$. Nestas condições, existe um subgrupo Abeliano $Q_n = \{Q_1^{(n)}, Q_2^{(n)}, \cdots, Q_{M^n}^{(n)}\}$, onde cada $Q_i^{(n)}$ para $i \in \{1, 2, \cdots, M^n\}$ é a soma direta de combinações de elementos de Q_1, que agem transitivamente nas matrizes geradoras $P_0, P_1, \cdots, P_{M^n}$, da seguinte forma*

$$P_i Q_1^{(n)} = P_i, P_i Q_2^{(n)} = P_{(i+1) mod\ M^n}, \cdots, P_i Q_{M^n}^{(n)} = P_{(i+(M^n-1)) mod\ M^n}.$$

Dados os resultados, há uma série de trabalhos futuros possíveis de se realizar, e listamos a seguir alguns deles.
Com respeito aos códigos de subespaços n-shot geometricamente uniformes:

- É importante analisar e realizar estudos sobre o conceito de códigos de subespaços n-shot geometricamente uniforme para corpos finitos $\mathbb{F}_p$, onde $p > 2$ primo.
- Também é importante analisar e realizar estudos sobre o conceito de códigos de subespaços n-shot geometricamente uniforme para outras estruturas algébricas, como exemplo, os anéis $\mathbb{Z}_q$, com q um inteiro positivo.
- É importante analisar e realizar estudos sobre o conceito de códigos de subespaços n-shot geometricamente uniforme para outras métricas, como as métricas da injeção e do posto.

Bibliografia


R.Ahlswede, N. Cai, R. Li,and R. Yeung, **Network Information Flow**, IEEE Transactions On Information Theory, vol. 46,n.º4, pp. 1204-1216, Jul. 2000.


M.Braun, T. Etzion and A. Vardy, **Linearity and complements in projective space**, Linear and Its Applications, vol.438, p. 57-70, 2013.


M. Braun, M. Kiermaier and A. Nakic, **On the automorphism group of a binary q-Analog of the Fano plane**, arxiv.org/1501.0779v1, Jan. 2015.


R. Calderbank, **Multilevel Codes and Multistage Decoding**, IEEE Transactions on Communications, vol.37, n.º3, pp.222-229, Mar. 1989.


C. Coulborn and J. Dinitz, **Handbook of Combinatorial Design**, Chapman Hall/CRC,2007.


H.H. Domingues e G. Iezzi, **Álgebra Moderna**, Atual Editora, 4ª Edição, São Paulo, 2003.


T. Etzion, **Problem on q-Analogs in Coding Theory**, arxiv.org/1305.6126v1, May. 2013.

Bibliografia


T.Etzion and N. Silberstein, **Error Correcting Codes in Projective Spaces via Rank Metric Codes and Ferrers Diagrams**, IEEE Transactions on Information Theory, vol. 55, n.º7, pp.2909-2919, Jul. 2009.


T. Etzion and A. Vardy, **Error Correcting Codes in Projective Space**, in Proceedings of the 2008 IEEE International Symposium on Information Theory - ISIT-08, pp. 871-875, Toronto, Canada, Jul. 2008.


G. D. Forney Jr., **Geometrically Uniform Codes**, IEEE Transactions on Information Theory, vol. 37, n.º5, pp. 1241-1260, Sep., 1991.


T. Etzion and L. Storme, **Galois Geometries and Coding Theory**, Designs, Codes and Cryptography, p. 311-350, 2016.


T. Etzion and N. Raviv, **Equidistant Codes in the Grassmannian**, Discrete Applied Mathematics, vol. 186, p. 187-197, 2015.


M. J. E. Golay, **Notes on Digital Coding**, Proceedings IEEE, vol. 27, 1949.


A. Khaleghi, D. Silva, and F.R. Kschischang, **Subspace Codes**, Lecture Notes in Computer Science, vol. 5921, pp. 1-21, 2009.

Bibliografia


D.M. Greenberger, H.M.S.A.; and A. Zeilinger, **Bell's Theorem without Inequalities**, Am. J. Phys. vol. 58, p 1131, 1990.


H. Imai and S.A. Hirakawa, **A new Coding Method Using Error-Correcting Codes**, IEEE Transactions on Information Theory, vol. 23, nº 3, 1977.


R. Koetter and F. Kschischang, **Coding for Errors and Erasures in Random Network Coding**, IEEE Transactions on Information Theory, vol. 54, n.º 8, pp. 3579-3591, Aug. 2008.


A. Kohnert and S.Kurz, **Construction of Large Constant Dimension Codes with a Prescribed Minimum Distance**, in Mathematical Methods in Computer Science, Lecture Notes in Computer Science, vol. 5393, pp. 31-42, Dec. 2008.


R. Li, W. Yeung and N. Cai, **Linear Network Coding**, IEEE Transactions on Information Theory, vol. 49, p. 371-381, 2003.


G.A.Miyamoto, **Códigos de Subespaço Geometricamente Uniformes**, Dissertação de Mestrado, FEEC - UNICAMP, Mar. 2015.

Bibliografia


R. Nóbrega and B. Uchôa-Filho, **Multishot Codes for Network Coding: Bounds and a Multilevel Construction**, in Proceedings of the 2009 IEEE International Symposium on Information Theory - ISIT-09, Seoul, South Korea, Jun. 2009.


W.C. Gazzoni, **Estudo do Emaranhamento Quântico com base na Teoria de Codificação Clássica**, Tese de Doutorado, FEEC-UNICAMO, 2008.


D.R. Stinson, **Combinatorial Designs: Constructions and Analysis**, Springer Verlag, New York, United States of America, 2004.


G. Ungerboeck, **Channel Coding with Multilevel/Phase Signls**, IEEE Transaction on Information Theory, vol. 28, n.º1, pp. 55-67, Jan. 1982.


R. W. Nobrega, **Canais Matriciais Multiplicativos sobre Corpos e Anéis Finitos com aplicações em Codificação de Rede**, Tese de Doutorado, Programa de Pós-Graduação em Engenharia Elétrica - UFSC, 2013.


M. Nielsen and I. Chuang, **Quantum Computation and Quantum Information**, Cambridge University Press, 2000.


S. Roman, **Lattices and Ordered Sets**, Springer Verlag, 2008.

Bibliografia


J. Rotman, **An Introduction to the Theory of Groups**, Springer Verlag, 1993.


R.W. Hamming **Error Detecting and Error Correcting Codes**, The Bell System Technical Journal, vol. 27, 1948.


F. MacWillians and N. Sloane, **The Theory of Error-Correcting Codes**, The Mathematical Association of America, vol. 21, 1983.


C.E. Shannon, **A Mathematical Theory of Comunication**, The Bell System Technical Journal, vol. 28, 1948.


D. Slepian, **Group Codes for the Gaussian Channel**, Bell Labs Thecnical Journal, vol. 47, p. 575-602, 1968.


Nóbrega, R. W. **Códigos de Subespaço aplicados a Codificação de Rede**. Dissertação de Mestrado - Programa de Pós-Graduação em Engenharia Elétrica - UFSC, 2009.

Obrigado pela Atenção!