Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
Volume 7, dez. 2016
Edição ERMAC

Similaridade entre a estrutura algébrica associada a espaços projetivos e design combinatório via diagrama de Hasse

Similarity between the algebraic structure associated with projective space and combinatorial design via Hasse diagram

Leandro Bezerra de Lima
CPAq-UFMS /
FEEC-UNICAMP
leandro.lima@ufms.br

Reginaldo Palazzo Júnior
FEEC-UNICAMP
palazzo@dt.fee.unicamp.br

Resumo

Design combinatório é uma importante estrutura combinatória com elevado grau de regularidade, que está relacionada a existência e construção de conjuntos de cardinalidade finita. Codificação em espaço projetivo é uma área de pesquisa muito recente e tem como elemento um objeto matemático composto por todos os subespaços vetoriais de um dado espaço vetorial, chamado espaço projetivo. Munido da distância de subespaço, o espaço projetivo torna-se um espaço métrico e assim, pode-se definir códigos corretores de erros nesse espaço, onde as palavras códigos agora serão subespaços e a reunião desses subespaços forma o código de subespaço. Propomos apresentar algumas similaridades existentes entre alguns espaços projetivos e uma estrutura algébrica por meio do design combinatório, com intuito, de fornecer elementos que possam ser úteis para a elaboração e construção de algumas classes de códigos de subespaços.
Palavras-chave: Matemática Discreta, Design Combinatório, Espaço Projetivo, Códigos de Subespaço.

Abstract

Combinatorial design is an important combinatorial structure having a high degree of regularity and which is related to the existence and construction of systems of sets with finite cardinality. Projective space of order m over a finite field $\mathbb{F}_p$, denoted by $\mathbb{P}(\mathbb{F}_p^m)$, (note that $\mathbb{F}_{p^m}$ is isomorphic to $\mathbb{F}_p^m$), is the set of all the subspaces in the vector space $\mathbb{F}_p^m$. The projective space endowed with the subspace distance $d(X,Y) = dim(X) + dim(Y) - 2dim(X \cap Y)$ is a metric space. Hence, the subspace code $\mathscr{C}$ with parameters (n,M,d) in the projective space is a subset of $\mathbb{P}(\mathbb{F}_p^m)$ with cardinality M with a subspace distance at least d between any two codewords. In this paper we show the existing similarity between the Hasse diagram of an Abelian group consisting of the product of multiplicative finite Abelian groups $\mathbb{Z}_p^m$ and the Hasse diagram of the projective space $\mathbb{P}(\mathbb{F}_p^m)$, with the aim to provide the elements that may be useful in the identification and in the construction of good subspaces codes.
Keywords: Discrete Mathematics. Combinatorial Design. Subspace Code. Projective Space.

1 Introdução

Design combinatório é uma importante estrutura combinatorial com elevado grau de regularidade e que está relacionada à existência e construção de sistemas de conjuntos de cardinalidade finita [1]. Inicialmente, o objetivo era consolidar a teoria de modo matematicamente coerente, sem entretanto focar em questões de aplicações práticas. Devido à diversidade e relevância dos problemas com aplicações práticas a inclusão ocorreu de uma forma natural. Como um exemplo mencionamos a relação existente entre códigos corretores de erros em espaço de Hamming e design combinatório, onde as palavras-código de peso 3 do código de Hamming formam um sistema triplo de Steiner, [2, 3], assim como q-analogs de um código de peso constante no espaço de Hamming é um código na Grassmanniana do espaço projetivo, [4, 5]. Codificação em espaços projetivos é uma área de pesquisa recente e tem como elemento um objeto matemático composto por todos os subespaços vetoriais de um dado espaço vetorial, chamado *espaço projetivo*. Munido da distância de subespaço, o espaço projetivo torna-se um espaço métrico e assim, pode-se definir códigos corretores de erros nesse espaço, onde as palavras-código agora serão subespaços e a reunião desses subespaços forma o código de subespaço, [6]. Código de subespaço é uma alternativa para aplicações em controle de erros em codificação de rede (do inglês Network Coding), que adicionalmente à comutação possibilita que seja realizada a codificação em cada nó, ou seja, os dados na saída estão sujeitos à transformações bem definidas e pré-estabelecidas dos dados na entrada em cada nó, permitindo assim, um aumento na taxa de transmissão da informação pela rede, [6, 7]. Neste trabalho, o objetivo é evidenciar as similaridades existentes entre as estruturas algébrica e do design via o diagrama de Hasse com o objetivo de construir bons códigos de subespaços, [8, 9, 10, 11].

2 Design Combinatório

Definição 1 *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) como sendo um* ***t-design*** *com parâmetros (v,k,λ), onde $0 < k < v$ e $\lambda > 0$, e denotado por (v,k,λ)-**design**, se:*

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

Observação 2 *Outra notação para a classe dos design da Definição 1 que aparece na literatura é (v,k,λ)- **BIBD** (do Inglês, Balanced Incomplete Block Design).*

Exemplo 1 *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, ver Fig. 1.*

Proposição 3 *Se (X,B) é um (v,k,λ)-BIBD, então cada elemento de X pertence a r blocos, onde:*

$$bk = rv \quad e \quad r(k-1) = \lambda(v-1). \tag{1}$$

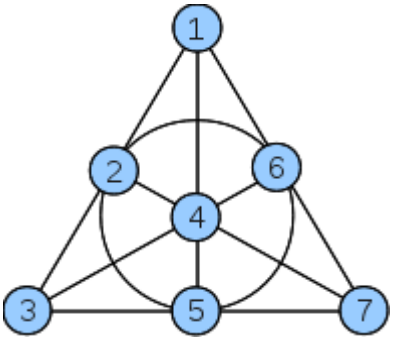


Figura 1: Plano de Fano

Observação 4 *Na literatura também encontra-se a seguinte notação para esta classe de design* (v,b,r,k,λ)***-BIBD**, [1].*

Apresentamos a seguir um resultado mais geral, válido para qualquer t-design.

Proposição 5 *Se* (X,B) *é um* t*-design com parâmetros* (v,k,λ)*, com* $0<t<k<v$ *e* $\lambda>0$*, então o número de blocos* b *é dado por:*

$$b\binom{k}{t}=\lambda\binom{v}{t}. \tag{2}$$

Definição 6 *Um* t*-design* (X,B) *denotado por* (v,k,λ)*-BIBD é dito* ***simétrico*** *se* $|X|=|B|=v=b$*.*

Observação 7 *Da equação (1) e da Definição 6, pode-se concluir que se um* (v,k,λ)*-BIBD é simétrico, então* $k=r$*.*

Exemplo 2 *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 8 *Um* t*-design com parâmetros* $(v,k,1)$ *é definido como sendo um* ***sistema de Steiner*** *e é denotado por* $S(t,v,k)$*.*

Um caso particular de sistemas de Steiner são os sistemas triplo de Steiner com $k=3$.

Definição 9 *Definimos um* ***sistema triplo de Steiner*** *de ordem* v *e denotamos por* $STS(v)$ *como sendo um sistema de Steiner com parâmetros* $S(2,v,3)$*.*

Observação 10 *Um sistema triplo de Steiner* $STS(v)$ *é um* $(v,3,1)$*-BIBD.*

Uma condição necessária para a existência de um sistema triplo de Steiner é apresentada através da seguinte proposição.

Proposição 11 *Uma condição necessária para que exista um sistema triplo de Steiner de ordem v, com* $v \geq 3$*, é que* $v \equiv 1 \ mod \ 6$ *ou* $v \equiv 3 \ mod \ 6$*.*

3 Espaços Projetivos e Códigos de Subespaço

Considerando que todo espaço vetorial de dimensão m sobre um corpo finito $\mathbb{F}_q$ é isomorfo a $\mathbb{F}_q^m$ apresentamos a seguir algumas definições importantes.

Definição 12 *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* $\mathscr{G}(\mathbb{F}_q^m, k)$*.*

Observação 13 *Note que:*

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

Definição 14 *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 15 *A* ***cardinalidade de uma Grassmanniana*** *de* $\mathbb{P}(\mathbb{F}_q^m)$ *com dimensão k é*

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

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

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

Definição 16 *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,* $\mathscr{G}(\mathbb{F}_q^m, k) = \{V \in \mathbb{P}(\mathbb{F}_q^m) : dimV = k\}$*, ou seja, todas as suas palavras-código possuem a mesma dimensão, será chamado* ***código de subespaço de dimensão constante****. Denotamos por d a distância mínima do código* $\mathscr{C}$*.*

Definição 17 *A* ***distância de subespaço*** *entre U e V é definida como:*

$$d(U,V) = dim(U) + dim(V) - 2dim(U \cap V), \tag{3}$$

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

Definição 18 *Os* ***parâmetros*** *de um código* $\mathscr{C} \subset \mathbb{P}(\mathbb{F}_q^m)$ *são denotados por* (m, M, d) *onde n é a dimensão do espaço projetivo, M é a cardinalidade do código e d a distância mínima do código. Se o código* $\mathscr{C}$ *está em uma Grassmanniana de dimensão k o parâmetro é do tipo* (m, M, d, k)*.*

Exemplo 3 *Seja o espaço vetorial $\mathbb{F}_2^3$. Um exemplo interessante de código na Grassmanniana é o código simplex $\mathscr{C}_2 = \{S_1, S_2, S_3\}$ com parâmetro $(n, M, d, k) = (3, 3, 2, 2)$, cujas palavras-código, ou seja, os subespaços vetoriais são $S_1 = \{000, 011, 100, 111\}, S_2 = \{000, 010, 101, 111\}, S_3 = \{000, 001, 110, 111\}$.*

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

Diagrama de Hasse é uma ferramenta matemática que representa graficamente qualquer conjunto finito parcialmente ordenado. No nosso contexto, é possivel construir o diagrama de Hasse, visto que o espaço projetivo $\mathbb{P}(F_q^n)$ com a seguinte relação de ordem $\preceq$, em que $V_1 \preceq V_2$ se, e somente se, V_1 é subespaço de V_2, é parcialmente ordenado. Dois subespaços estão conectados se, e somente se, V_1 é subespaço de V_2 e $dimV_2 = dimV_1 + 1$ ou vice-versa. Logo, a partir do diagrama de Hasse, podemos interpretar a distância entre dois subespaços V_1, V_2 de $\mathbb{P}(F_q^n)$ como o caminho de menor distância, geodésica, ligando V_1 e V_2.

Lema 19 *Sejam U e V subespaços de um espaço vetorial de dimensão n. Então a distância é máxima, isto é, $d_s(U,V) = n$, se, e somente se,*

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

4 Relações entre Design Combinatório e Espaços Projetivos

Apresentamos alguns exemplos de design combinatório que descrevem as conexões de algumas classes de espaços projetivos.

Exemplo 4 *O design $(7,3,1)$-BIBD ou $STS(7)$, conhecido como plano de Fano, descreve as conexões do espaço projetivo $\mathbb{P}(\mathbb{F}_2^3)$, ver Fig. 4.*

Exemplo 5 *O design $(13,4,1)$-BIBD descreve as conexões do espaço projetivo $\mathbb{P}(\mathbb{F}_3^3)$.*

Teorema 20 *Seja $q \geq 2$ uma potência de primo e $d \geq 2$ um inteiro. Então existe um design simétrico:*

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) - BIBD.$$

Corolário 21 *Para cada potência de primo $q \geq 2$ e $d = 2$, existe um $(q^2+q+1, q+1, 1)$-BIBD simétrico, isto é, um plano projetivo de ordem q.*

Exemplo 6 *Existe um (31,6,1)-BIBD simétrico (plano projetivo de ordem 5) e um (57,8,1)-BIBD simétrico (plano projetivo de ordem 7) cada descrevendo, respectivamente, os espaços projetivos $\mathbb{P}(\mathbb{F}_5^3)$ e $\mathbb{P}(\mathbb{F}_7^3)$.*

Exemplo 7 *O design* $(15,3,1)$*-BIBD que é um* $STS(15)$*, ou seja, um sistema de Steiner de ordem 15 descreve as conexões entre os subespaços de dimensão* 1 *e dimensão* 2 *do espaço projetivo* $\mathbb{P}(\mathbb{F}_2^4)$.

5 Estrutura Algébrica para uma Classe de Espaços Projetivos

Apresentamos uma similaridade ou compatibilização de espaço projetivo com uma estrutura algébrica através do diagrama de Hasse.

Considere um grupo multiplicativo C_p, onde p é um número primo, isto é, $C_p = (\{1,2,3,....,p-1\}, \odot_p)$, com $\odot_p$ representando o produto módulo p.

Exemplo 8 *Note a similaridade, via os correspondentes diagramas de Hasse, entre o espaço projetivo* $\mathbb{P}(\mathbb{F}_2^2)$ *e o grupo* $G = C_2 \times C_2$ *de ordem 4, onde* $\times$ *denota o produto direto, como ilustrado nas Fig. 2 e Fig. 3.*

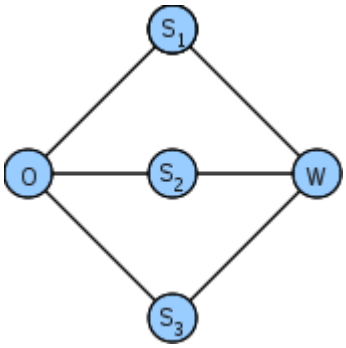


Figura 2: Espaço projetivo $\mathbb{P}(\mathbb{F}_2^2)$

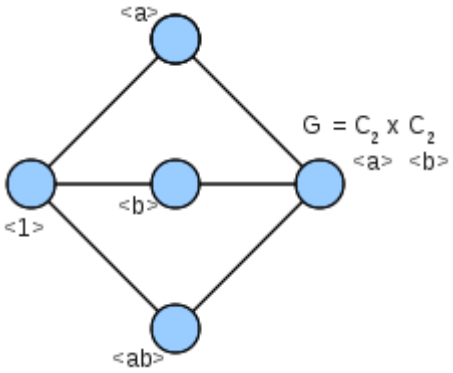
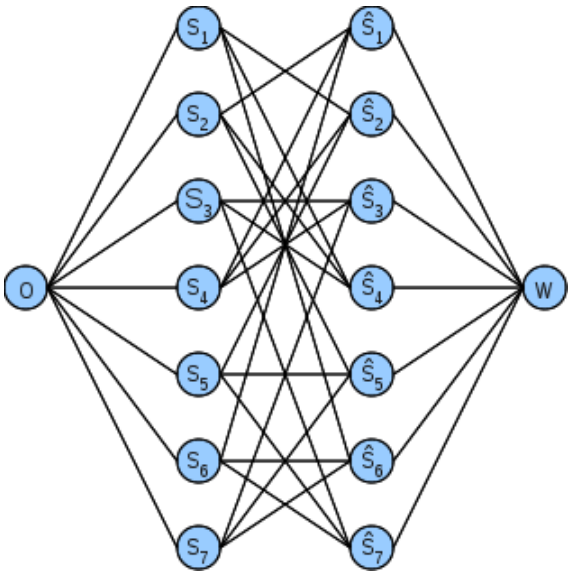


Figura 3: Estrutura algébrica $C_2 \times C_2$

Exemplo 9 *Novamente, note a similaridade, via os correspondentes diagramas de Hasse, entre o espaço projetivo* $\mathbb{P}(\mathbb{F}_2^3)$ *e o grupo* $G = C_2 \times C_2 \times C_2$ *de ordem 8, Fig. 4 e Fig. 5.*



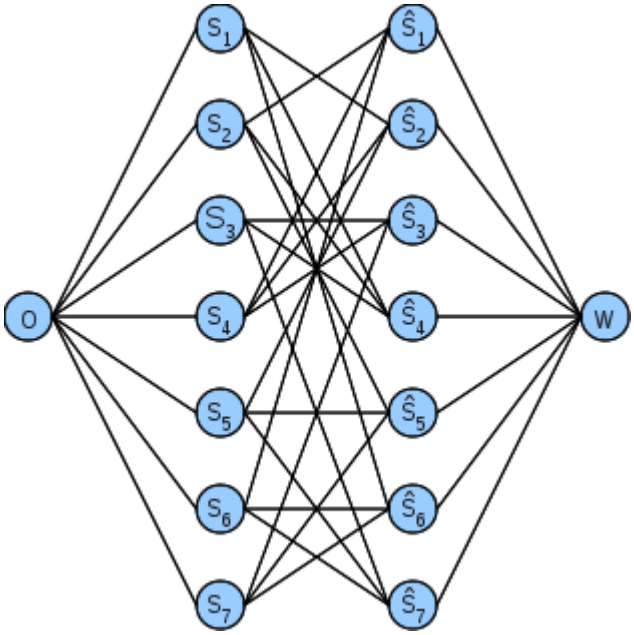


Figura 4: Espaço projetivo $\mathbb{P}(\mathbb{F}_2^3)$

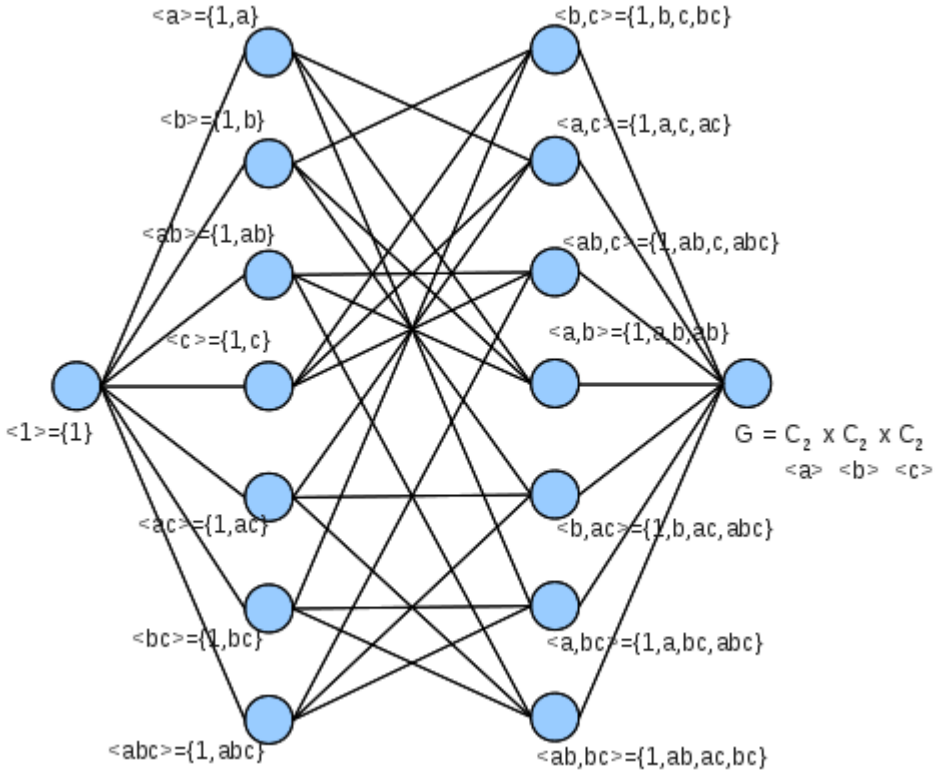


Figura 5: Estrutura algébrica $C_2 \times C_2 \times C_2$

Exemplo 10 *Note a similaridade, via os correspondentes diagramas de Hasse, entre o espaço projetivo* $\mathbb{P}(\mathbb{F}_3^2)$ *e o grupo* $G = C_3 \times C_3$ *de ordem 9, similar ao exemplo 8.*

Exemplo 11 *Note a similaridade, via os correspondentes diagramas de Hasse, entre o espaço projetivo* $\mathbb{P}(\mathbb{F}_3^3)$ *e o grupo* $G = C_3 \times C_3 \times C_3$ *de ordem 27, por meio do design* $(13,4,1)$*-BIBD .*

Podemos generalizar os exemplos anteriores, associando o design $(q^2+q+1, q+1, 1)$-BIBD simétrico, q-primo com o espaço projetivo $\mathbb{P}(\mathbb{F}_q^3)$ e uma estrutura algébrica $G = C_p \times C_p \times C_p$ de ordem p^3, possuindo subgrupos de ordem p^2, ordem p e ordem 1 que descrevem a mesma estrutura combinatória que o espaço projetivo $\mathbb{P}(\mathbb{F}_q^3)$. O número de subgrupos de ordem p^2 é dado por:

$$\binom{3}{2}_p = \prod_{i=0}^{k-1} \frac{p^3 - p^i}{p^2 - p^i} = \frac{p^3-1}{p^2-1}\frac{p^3-p}{p^2-p} = p^2 + p + 1,$$

enquanto que a quantidade de subgrupos de ordem p é dada por:

$$\binom{3}{1}_p = \prod_{i=0}^{k-1} \frac{p^3 - p^i}{p - p^i} = \frac{p^3-1}{p-1} = p^2 + p + 1.$$

Note que para $p = 2$ o número de subgrupos cujas ordens são 2 e 4, é igual a 7, ver Exemplo 9. Para $p = 3$, o número de subgrupos cujas ordens são 3 e 9 é igual a 13, ver Exemplo 11.

6 Conclusões

Neste artigo apresentamos por meio de vários exemplos, similaridade existente entre uma classe de espaços projetivos do tipo $\mathbb{P}(\mathbb{F}_q^3)$ e uma estrutura algébrica $G = C_p \times C_p \times C_p$ com $p = q$ primos. Tal similaridade ficou evidenciada por meio do diagrama de Hasse das duas estruturas. Acreditamos que evidenciar tal similaridade seja útil para a elaboração e construção de bons códigos de subespaço.

Referências

[1] STINSON, D. R. **Combinatorial designs:** constructions and analysis. New York: Springer, 2004.

[2] ETZION, T.; SILBERSTEIN, N. Error correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. **IEEE Transactions on Information Theory**, vol. 55, n.7, p. 2909-2919, Jul. 2009.

[3] KOETTER, R.; KSCHISCHANG, F. R. Coding for errors and erasures in random network coding. **IEEE Transactions on Information Theory**, v. 54, n.8, p. 3579-3591, Aug. 2008.

[4] BRAUN, M. et al. Existence of q-analogs of Steiner systems. Forum of Mathematics, Pi, Los Angeles, v.4, e7, 2016. Disponível em <https://www.cambridge.org/core/journals/forum-of-mathematics-pi/article/existence-of-q-analogs-of-steiner-systems/CCA4E791C28A449903101CF467CBB0D3> Acesso em: 10/09/2016.

[5] ETZION, T.; VARDY, A. Error correcting codes in projective space. In INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY, 2008, Toronto. **Proceendings ISIT** Toronto, Canadá, 2008. p. 871-875.

[6] KLALEGHI, A.; SILVA, D.; KSCHISCHANG, F. R. Subspace codes. **Lecture Notes in Computer Science**, v. 5921, p. 1-21, 2009.

[7] AHLSWEDE, R. et al. Network information flow, **IEEE Transactions On Information Theory**, vol. 46,n.º4, p. 1204-1216, Jul. 2000.

[8] COSTA, C.H.A. **Automorfismos de grupos abelianos finitos**. 2014. 64 f. Dissertação (Mestrado em Matemática) - Programa de Pós-Graduação em Matemática, Universidade Federal de Visçosa, Viçosa/MG, 2014.

[9] GUERREIRO, M. Group algebras and coding theory. **São Paulo J. Math. Sci.** v.10, n. 2, p. 346-371, 2016.

[10] MIYAMOTO, G. A. **Códigos de subespaço geometricamente uniformes**, 2015. 48 f. Dissertação (Mestrado em Engenharia Elétrica) - Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, 2015.

[11] NÓBREGA, R. W.; UCHÔA-FILHO, B. F. Multishot codes for network coding: bounds and a multilevel construction. In: INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY,2009, Seoul. **Proceedings ISIT**, Seoul, South Korea, 2009. p. 428-432.