O Problema da Cobertura Curta Sobre Anéis

Irene Naomi Nakaoka,
UEM - Departamento de Matemática,
87020-900, Maringá, PR
E-mail: innakaoka@uem.br,

Otávio José Neto Tinoco Neves dos Santos
UEMS - Unidade de Nova Andradina
79750-000, Nova Andradina, MS
E-mail: ojneto@uems.br.

Resumo: Dado um anel comutativo com unidade A, o número $c(A, n, R)$ é definido como sendo a mínima cardinalidade dos conjuntos H de A^n que satisfazem a seguinte propriedade: qualquer elemento de A^n difere no máximo R coordenadas de um múltiplo de um elemento de H. Neste trabalho os números $c(\mathbb{Z}_m, n, 0)$ são determinados, para todos inteiros $m, n \geq 2$. Também são apresentados limitantes superiores para $c(A, n, R)$, quando $A = \mathbb{Z}_q$ ou $A = \mathbb{Z}_q^m$. Além disso os números $c(A, n, R)$ serão relacionados com conjuntos livres de produto, desta relação obtemos um limitante superior para $c(\mathbb{Z}_q, 3, 1)$, quando q é potência de um primo p.
Palavras-chave: problema de cobertura, conjuntos livre de produto, ações de grupo, anéis finitos

1 Introdução

Seja V_q^n o conjunto de todas as n-uplas de elementos de um conjunto finito de cardinalidade q, estas n-uplas são também chamadas de *vetores* ou *palavras*. A *distância de Hamming* entre duas palavras $u = (u_1, \cdots, u_n)$ e $v = (v_1, \cdots, v_n)$ de V_q^n é definida por $d(u, v) = |\{i : u_i \neq v_i\}|$. A *bola* de centro v e raio R corresponde ao conjunto $B(v, R) = \{u \in V_q^n : d(u, v) \leq R\}$. Um subconjunto $C \subset V_q^n$ é uma *R-cobertura* de V_q^n, se para todo $v \in V_q^n$ existe uma palavra $c \in C$ tal que $v \in B(c, R)$. A mínima cardinalidade de uma R-cobertura de V_q^n é denotada por $K_q(n, R)$. Os números $K_q(n, R)$ são bastante conhecidos, o problema extremal de determinar valores ou pelo menos limitantes para estes números é conhecido como problema da cobertura e é um importante tópico da teoria combinatória dos códigos. (Veja [1], para mais detalhes).

Recentemente, em [2], foi proposta a seguinte variante para o problema da cobertura. Seja $\mathbb{F}_q$ um corpo finito com q elementos, definimos $c(\mathbb{F}_q, n, R)$ como a mínima cardinalidade de um subconjunto $H \subset \mathbb{F}_q^n$ com a propriedade que, para toda palavra $v \in \mathbb{F}_q^n$, existem $\alpha \in \mathbb{F}_q$ e $h \in H$ tais que $v \in B(\alpha h, R)$. Os melhores limitantes conhecidos para $c(\mathbb{F}_q, n, R)$ são

$$\left\lceil \frac{q+1}{2} \right\rceil \leq c(\mathbb{F}_q, 3, 1) \leq \frac{3(q+4)}{4}, \tag{1}$$

que foram obtidos em [2] e [3] usando, entre outras ferramentas, ações de grupos e uma relação entre estas coberturas e conjuntos livre de produto.

Neste trabalho, estendemos a variante c, da função k como segue. Estaremos considerando sempre A como sendo um anel comutativo com unidade 1. Para um elemento $h \in A^n$, seja

$$E(h, R) = \bigcup_{\alpha \in A} B(\alpha h, R).$$

Se $S \subset A^n$, dizemos que o subconjunto H de A^n é uma *R-cobertura curta* de S quando $S \subset \cup_{h\in H} E(h, R)$. Definimos $c(A, n, R)$ como sendo a mínima cardinalidade de uma R-cobertura curta de A^n.

O problema clássico da cobertura é um conceito puramente combinatório, depende apenas do número de elementos do espaço. Entretanto os números $c(A, n, R)$ não dependem apenas da cardinalidade do anel A, mas também da sua estrutura algébrica, isto é, os números $c(A_1, n.R)$ e $c(A_2, n.R)$ podem ser diferentes mesmo quando $|A_1| = |A_2|$. Por exemplo, em [4] foi mostrado que $c(\mathbb{Z}_4, 3, 1) = 4$ e $c(\mathbb{Z}_2 \times \mathbb{Z}_2, 3, 1) = 3$. A seguir mostraremos que existe uma relação entre os números $c(A, n, R)$ e uma classe especial dos números $K_q(n, R)$ e, como consequência desta relação, obteremos um limitante inferior para $c(A, 3, 1)$.

2 Limitante Inferior

Como é usual, a cardinalidade de um conjunto X será denotada por $|X|$. Uma R-cobertura curta de cardinalidade mínima será chamada de *R-cobertura curta mínima*.

Proposição 1. *[4].* $K_{|A|}(n, R) \leq (|A| - 1)\, c(A, n, R) + 1$.

Kalbfleish e Stanton mostraram em [5] que $K_q(3, 1) = \lceil q^2/2 \rceil$. Aplicando a proposição anterior obtemos.

Corolário 2. *[4]. Para todo anel comutativo com unidade A,* $c(A, 3, 1) \geq \lceil (|A| + 1)/2 \rceil$

O limitante inferior dado no Corolário 2 é bastante útil, por exemplo, dele segue que $c(\mathbb{Z}_{2p}, 3, 1) \geq p + 1$.

3 O Caso $R = 0$

É fácil verificar que $K_q(n, 0) = q^n$. Se $\mathbb{F}_q$ é um corpo com q elementos e H é uma 0-cobertura curta mínima de $\mathbb{F}_q^n$, então $\mathbb{F}_q H = \mathbb{F}_q^n$, isto implica que $|H| = \dfrac{q^n - 1}{q - 1}$, ou seja, $c(\mathbb{F}_q, n, 0) = \dfrac{q^n - 1}{q - 1}$. Contudo, uma 0-cobertura curta de $\mathbb{Z}_q$ tem mais elementos. Como mostra o seguinte resultado.

Teorema 3. *Sejam $p_1, p_2, \ldots, p_s$ primos distintos. Se $m = q_1 q_2 \cdots q_s$, aqui $q_j = p_j^{r_j}$ com $r_j > 0$ para todo $1 \leq j \leq s$, então*

$$c(\mathbb{Z}_m, n, 0) = \prod_{j=1}^{s} \left(\frac{p_j^n - 1}{p_j - 1} \right) \left(\frac{q_j}{p_j} \right)^{n-1}.$$

4 O Caso $R > 0$

Por ser um problema recente, pouco se sabe sobre os números $c(A, n, R)$. O próximo teorema fornece um limitante superior para $c(A, n, R)$ em função de $c(A, n, 0)$, que é conhecido quando $A = \mathbb{Z}_m$.

Proposição 4. *Para todo anel comutativo com unidade A e para todos inteiros positivos n e R tais que $R < n$, $c(A, n, R) \leq c(A, n - R, 0)$.*

Demonstração. Seja H uma 0-cobertura curta de A^{n-R}. Então o conjunto

$$K = \{(h_1, h_2, \ldots, k_{n-R}, 0, 0, \ldots, 0) \in A^n : (h_1, h_2, \ldots, k_{n-R}) \in H\}$$

é uma R-cobertura curta de A^n.

Corolário 5. *Sejam $p_1, p_2, \ldots, p_s$ primos distintos. Se $m = q_1 q_2 \cdots q_s$, aqui $q_j = p_j^{r_j}$ com $r_j > 0$ para todo $1 \leq j \leq s$, então*

$$c(\mathbb{Z}_m, n, R) \leq \prod_{j=1}^{s} \left(\frac{p_j^{n-R} - 1}{p_j - 1} \right) \left(\frac{q_j}{p_j} \right)^{n-R-1}.$$

A seguir o limitante dado no corolário acima será melhorado para $R = 1$ e um caso especial de n.

Proposição 6. *Sejam $p, p_1, p_2, \ldots, p_s$ primos distintos. Se $t = q_1 q_2 \cdots q_s$, aqui $q_j = p_j^{r_j}$ com $r_j > 0$ para todo $1 \leq j \leq s$ e $n = (p^r - 1)/(p - 1)$, então*

$$c(\mathbb{Z}_{pt}, n, 1) \leq \frac{p^{n-r} - 1}{p - 1} \prod_{j=1}^{s} \left(\frac{p_j^{n-1} - 1}{p_j - 1} \right) \left(\frac{q_j}{p_j} \right)^{n-2}.$$

Corolário 7. *[4]. Se p é um primo ímpar, então $c(\mathbb{Z}_{2p}, 3, 1) = p + 1$.*

Observamos que, nas condições da Proposição 6, diminuímos o limitante superior de $c(\mathbb{Z}_{pt}, n, 1)$ dado no Corolário 5 em $p^{p-1} \prod_{j=1}^{s} \left(\frac{p_j^{n-1} - 1}{p_j - 1} \right) \left(\frac{q_j}{p_j} \right)^{n-2}$ elementos.

Proposição 8. *Se q é a potência de um primo p, então*

$$c(\mathbb{Z}_q^m, n, 1) \leq c(\mathbb{Z}_q, n, 1) \left[\left(\frac{p^{n-1} - 1}{p - 1} \right) \left(\frac{q}{p} \right)^{n-2} \right]^{m-1}.$$

Em particular, se $n = (p^r - 1)/(p - 1)$, então

$$c(\mathbb{Z}_p^m, n, 1) \leq \frac{(p^{n-r} - 1)(p^{n-1} - 1)^{m-1}}{(p - 1)^m}.$$

5 Cobertura Curta, Ações e Conjuntos Livres de Produto

Como é usual, $U(A)$ é o grupo das unidades de A. Considere o produto direto $S_n \times U(A)$, onde S_n denota o grupo simétrico de grau n. Para $\varphi \in S_n$, $\lambda \in U(A)$, e $v = (v_1, v_2, \ldots, v_n) \in A^n$, definimos a ação de $S_n \times U(A)$ sobre o conjunto A^n colocando

$$v^{(\varphi,\lambda)} = \left(\lambda v_{(1)\varphi^{-1}}, \lambda v_{(2)\varphi^{-1}}, \ldots, \lambda v_{(n)\varphi^{-1}} \right). \tag{2}$$

Para $\varphi \in S_n$ e $\lambda \in A$ escrevemos $\varphi\lambda$ ao invés de (φ, λ); portanto $v^{\varphi\lambda} = v^{(\varphi,\lambda)}$, $v^{\varphi} = v^{(\varphi,1)}$, e $v^{\lambda} = v^{(1,\lambda)}$. Quando um grupo G age sobre um conjunto X, denotamos a órbita de v por $v^G = \{v^g : g \in G\}$. Se Y é um subconjunto de X e H é um subconjunto de G, Y^H denota o conjunto $\{y^h : y \in Y \text{ and } h \in H\}$.

O próximo resultado estabelece um método para decidir quando um candidato H é realmente uma R-cobertura curta de A^n

Teorema 9. *[4]. Seja B um subconjunto de A^n invariante pela ação de $S_n \times U(A)$. Se L é um subconjunto de A^n invariante pela ação de S_n tal que cada órbita da ação de $S_n \times U(A)$ sobre B contém um elemento v tal que $d(v, \alpha h) \leq R$, para algum $\alpha \in A$ e algum $h \in H$, então L é uma R-cobertura curta de B.*

A seguir apresentaremos uma conexão, baseada numa construção feita em [3], entre coberturas curtas e conjuntos livres de produto. Esta conexão será útil para obtermos um limitante

superior para $c(\mathbb{Z}_q, 3, 1)$, quando q é potência de primo. Nossa abordagem consiste em determinar uma 1-cobertura curta para o seguinte subconjunto de A^3

$$\mathcal{U}(A) = \{(x, y, z) : x, y, z \in U(A) \text{ and } x, y, z \text{ são dois a dois distintos}\}.$$

O próximo passo é encontrar uma 1-cobertura curta para o complemento de $\mathcal{U}(A)$ em A^3.

Começamos observando que $\mathcal{U}(A)$ é invariante pela ação do produto direto $S_3 \times U(A)$. Consequentemente, esta ação sobre A^3 induz de maneira natural uma ação sobre $\mathcal{U}(A)$.

Um subconjunto X de um grupo multiplicativo G é chamado de livre de produto em G, se $ab \notin X$ para todos $a, b \in X$.

Para uma família $\mathcal{P} = \{(x_1, y_1), ..., (x_k, y_k)\}$ de elementos de $G \times G$, colocamos

$$\Delta_{\mathcal{P}} = \{1\} \cup \bigcup_{i=1}^{k} \Delta_{(x_i, y_i)}$$

onde $\Delta_{(x,y)} = \{x, y, x^{-1}, y^{-1}, xy^{-1}, yx^{-1}\}$. Observamos que $\Delta_{\mathcal{P}}$ é um conjunto inverso, isto é, $\Delta_{\mathcal{P}} = (\Delta_{\mathcal{P}})^{-1} = \{x^{-1} \,|x \, \in \Delta_{\mathcal{P}}\}$.

Teorema 10. *[4]. Seja $\mathcal{P} = \{(x_1, x_2), \dots (x_k, y_k)\}$ uma coleção de pares de elementos de $U(A)$. Se o complemento de $\Delta_{\mathcal{P}}$ em $U(A)$ é livre de produto, então o conjunto*

$$H = \bigcup_{i=1}^{k} (1, x_i, y_i)^{S_3}$$

é uma 1-cobertura curta de $\mathcal{U}(A)$.

Demonstração. Pelo Teorema 9 basta verificar que a união $\bigcup\{E(h, 1) : h \in H\}$ contém um representante de cada órbita da ação de $G = S_3 \times U(A)$ sobre $\mathcal{U}(A)$. Observamos que cada órbita contém um elemento da forma $(1, a, b)$ com $a \in \Delta_{\mathcal{P}} \setminus \{1\}$. De fato, para todos $(x, y, z) \in \mathcal{U}(A)$ temos que $(x, y, z)^G = (1, x^{-1}y, x^{-1}z)^G = (1, x^{-1}z, x^{-1}y)$, com $x^{-1}y \neq 1$ e $x^{-1}z \neq 1$. Assim, se $x^{-1}y \in \Delta_{\mathcal{P}}$ ou $x^{-1}z \in \Delta_{\mathcal{P}}$ nada temos à demonstrar. Por outro lado, se $x^{-1}y, x^{-1}z \in \mathcal{U}(A) \setminus \Delta_{\mathcal{P}}$, então $(x^{-1}y)^{-1} \in \mathcal{U}(A) \setminus \Delta_{\mathcal{P}}$, pois $\Delta_{\mathcal{P}}$ é um conjunto inverso, e sendo $\mathcal{U}(A) \setminus \Delta_{\mathcal{P}}$ livre de produto, obtemos que $y^{-1}z = (x^{-1}y)^{-1}(x^{-1}z) \in \Delta_{\mathcal{P}}$. Nossa observação segue do fato que $(1, x^{-1}y, x^{-1}z)^G = (y^{-1}x, 1, y^{-1}z)^G = (1, y^{-1}x, y^{-1}z)^G$.

Seja O o conjunto das órbitas e seja $(1, a, b) \in O$, com $a \in \Delta_{\mathcal{P}} \setminus \{1\}$. Então a pertence ao conjunto $\{x_i, y_i, x_i^{-1}, y_i^{-1}, x_i^{-1}y_i, y_i x_i^{-1}\}$, para algum $i, 1 \leq i \leq k$. Temos seis casos para analizar:
• se $a = x_i$, então $(1, a, b) = (1, x_i, y_i) + (b - y_i)(0, 0, 1)$;
• se $a = x_i^{-1}$, então $(1, a, b) = x_i^{-1}(x_i, 1, y_i) + (b - x_i^{-1}y_i)(0, 0, 1)$;
• se $a = x_i^{-1}y_i$, então $(1, a, b) = x_i^{-1}(x_i, y_i, 1) + (b - x_i^{-1})(0, 0, 1)$.

Os outros três casos são similares a um dos casos acima. Portanto, em qualquer um dos casos, $(1, a, b) \in \bigcup\{E(h, 1) : h \in H\}$ e o resultado segue pelo Teorema 9.

Aplicaremos o Teorema 10 para obtermos uma 1-cobertura curta de $\mathcal{U}(\mathbb{Z}_q)$, quando q é potência de primo. Denotamos o complemento de S em $U(\mathbb{Z}_q)$ por $\overline{S}$.

Teorema 11. *[4]. Seja $q = p^r$ a potência de um primo p, com $q > 9$.*

(i) *Se p é ímpar, então existe uma 1-cobertura curta de $\mathcal{U}(\mathbb{Z}_q)$ com pelo menos $9n/16 + 9/4$ elementos, aqui $n = p^{r-1}(p-1)$*

(ii) *Se $p = 2$ e $r \geq 5$, então existe uma 1-cobertura curta de $\mathcal{U}(\mathbb{Z}_q)$ com $9 \cdot 2^{r-5}$*

Demonstração. Para o caso $p = 2$ e $r \geq 5$, observamos que o grupo multiplicativo $U(\mathbb{Z}_q) = \{1, 3, 5, \dots, q-1\}$ é gerado por -1 e 5 e isomorfo ao grupo $\mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}}$, como mostra o Teorema

5.44 [6]. Além disso, a ordem de 5 em $U(\mathbb{Z}_q)$ é $m = 2^{r-2}$. Seja K o subgrupo de $U(\mathbb{Z}_q)$ gerado por 5. Usando a expansão binomial de $5^i = (1+4)^i$ obtemos

$$K = \{1, 5, 5^2, \ldots, 5^{m-1}\} = \{x \in U(\mathbb{Z}_q) \,|\, x \equiv 1 (\mathrm{mod}\, 4)\}.$$

É fácil verificar que $\overline{K} = \{x \in U(\mathbb{Z}_q) \,|\, x \equiv 3 (\mathrm{mod}\, 4)\}$ é livre de produto em $U(\mathbb{Z}_q)$. Agora, basta determinar uma família $\mathcal{P}$ tal que $\overline{\Delta_\mathcal{P}} \subset \overline{K}$. Se $r = 5$ definimos $\mathcal{P} = \left\{\left(5, 5^3\right), \left(5^4, 5^4\right)\right\}$ e se $r > 5$,

$$\begin{aligned}\mathcal{P} &= \left\{\left(5, 5^{m/2-1}\right), \left(5^3, 5^{m/2-3}\right), \ldots, \left(5^{m/4-1}, 5^{m/2-(m/4-1)}\right)\right\} \\ &\cup \left\{\left(5^4, 5^8\right), \left(5^{12}, 5^{16}\right), \ldots, \left(5^{4(m/8-1)}, 5^{4(m/8)}\right)\right\}.\end{aligned}$$

Se $r = 5$, temos que $\Delta_\mathcal{P} = K$. Se $r > 5$, não é difícil checar que $\{1, 5, 5^2, \ldots, 5^{m/2}\} \subset \Delta_\mathcal{P}$ e como $\Delta_\mathcal{P}$ é um conjunto inverso, segue que $K \subset \Delta_\mathcal{P}$. Assim, em qualquer um dos casos, temos que $\overline{\Delta_\mathcal{P}} \subset \overline{K}$, logo $\overline{\Delta_\mathcal{P}}$ é livre de produto em $U(\mathbb{Z}_q)$. Portanto, $\mathcal{P}$ induz uma 1-cobertura curta em $\mathcal{U}(\mathbb{Z}_q)$, contendo $9 \cdot 2^{r-5}$ elementos.

Agora, suponhamos que p seja um primo ímpar. Observamos que $U(\mathbb{Z}_q)$ é um grupo cíclico de ordem $n = p^{r-1}(p-1)$. Seja ξ um gerador deste grupo. Como o conjunto $\left\{\xi^1, \xi^3, \ldots, \xi^{n-1}\right\}$ é livre de produto em $U(\mathbb{Z}_q)$ é suficiente encontrarmos uma coleção $\mathcal{P}$ tal que

$$\left\{1, \xi^2, \xi^4, \ldots, \xi^{n-2}\right\} \subset \Delta_\mathcal{P}. \tag{3}$$

Dado um inteiro par k, seja

$$\mathcal{A}(k) = \left\{\left(\xi^2, \xi^{4k-2}\right), \left(\xi^6, \xi^{4k-6}\right), \ldots, \left(\xi^{2k-2}, \xi^{2k+2}\right)\right\}.$$

Se $k/2$ é par, colocamos

$$\mathcal{B}(k) = \left\{\left(\xi^8, \xi^{16}\right), \left(\xi^{24}, \xi^{32}\right), \ldots, \left(\xi^{8(k/2-1)}, \xi^{8(k/2)}\right)\right\},$$

caso contrário, fazemos

$$\mathcal{B}(k) = \left\{\left(\xi^8, \xi^{16}\right), \left(\xi^{24}, \xi^{32}\right), \ldots, \left(\xi^{8(k/2-2)}, \xi^{8(k/2-1)}\right)\right\} \cup \left\{\left(\xi^{8(k/2)}, \xi^{8(k/2)}\right)\right\}.$$

Seja k o quociente da divisão de n por 8. Como n é par, temos que $n = 8k + r$, com $r = 0, 2, 4$ ou 6. Definimos

$\mathcal{P} = \mathcal{A}(k) \cup \mathcal{B}(k)$, se $r = 0$ ou 2 e k é par;
$\mathcal{P} = \mathcal{A}(k-1) \cup \mathcal{B}(k-1) \cup \left\{\left(\xi^{4k-2}, \xi^{4k}\right)\right\}$, se $r = 0$ ou 2 e k é ímpar;
$\mathcal{P} = \mathcal{A}(k) \cup \mathcal{B}(k) \cup \left\{\left(\xi^{4k+2}, \xi^{4k+2}\right)\right\}$, se $r = 4$ ou 6 e k é par
$\mathcal{P} = \mathcal{A}(k-1) \cup \mathcal{B}(k-1) \cup \left\{\left(\xi^{4k-2}, \xi^{4k}\right), \left(\xi^{4k+2}, \xi^{4k+2}\right)\right\}$, se $r = 4$ ou 6 e k é ímpar.

Não é difícil mostrar que, em qualquer caso, $\mathcal{P}$ satisfaz a inclusão (3) e que, portanto, $\overline{\Delta_\mathcal{P}}$ é livre de produto. Assim, pelo Teorema 10, em qualquer caso, $\mathcal{P}$ induz uma 1-cobertura curta de $\mathcal{U}(\mathbb{Z}_q)$. Uma simples contagem mostra que cada cobertura contém no máximo $9n/16 + 9/4$ elementos.

A seguir, completaremos a 1-cobertura curta de $\mathcal{U}(\mathbb{Z}_q)$, obtida no teorema anterior, a uma 1-cobertura curta de $\mathbb{Z}_q^3$ obtendo um limitante superior para $c(\mathbb{Z}_q, 3, 1)$.

Teorema 12. *[4]. Seja $q = p^r$ a potência de um primo p.*

(i) *Se $p \neq 2$ e $q > 9$, então* $c(\mathbb{Z}_q, 3, 1) \leq \dfrac{9}{16} q \left(1 + \dfrac{23}{9p}\right) + \dfrac{13}{4}$.

(ii) *Se $p = 2$ e $r \geq 5$, então* $c(\mathbb{Z}_q, 3, 1) \leq \dfrac{41}{32} q + 1$.

Demonstração. Definimos o conjunto K, colocando $K = \emptyset$, se $r = 1$, caso contrário, colocamos $K = \{(1, ip, 1), (ip, 1, ip) : i = 1, 2, \cdots, p^{n-1} - 1\}$. Se H é uma 1-cobertura curta de $\mathcal{U}(\mathbb{Z}_q)$, então $L = H \cup (1, 1, 0)^{S_3} \cup K$ é uma 1-cobertura curta de $\mathbb{Z}_q^3$ e o resultado segue usando o teorema anterior e uma simples contagem.

Segue do Teorema 12 que se p é um primo ímpar, então $c(\mathbb{Z}_p, 3, 1) \leq 9p/16 + 75/16$. Para $p \geq 23$, este resultado melhora o limitante superior dado em (1).

Agradecimentos

Agradecemos a E. L. Monte Carmelo pelas sugestões durante o desenvolvimento desta pesquisa.

Este trabalho foi parcialmente financiado pelo CNPq - Processo 480506/2007-8

Referências Bibliográficas:

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, "Covering Codes", North-Holland Publishing, Amsterdam, 1997.

[2] E.L. Monte Carmelo, I.N. Nakaoka, and J.R. Gerônimo, A, Covering problem on finite spaces and rook domains, *Int. J. Appl. Math*, 20 (2007), 875-886.

[3] E.L. Monte Carmelo and I.N. Nakaoka, Short coverings in tridimensional spaces arising from sum-free sets, *Europ. J. Combin.*, 29 (2008), 227-233.

[4] I.N. Nakaoka and O.J.N.T.N Santos, A Covering problem over rings and product-free sets, *Int. J. Appl. Math.*, 21 (2008) 339-351.

[5] J.G. Kalbfleish, and R.G. Stanton, A combinatorial problem in matching, J. London Math. Soc., 44, (1969), 60-64.

[6] J.J. Rotman, "An Introduction to the Theory of Groups", Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, (1995).