جامعة الموصل
كلية علوم الحاسوب والرياضيات

القيود حول اصغر مسافة للشفرات الخطية على GF(q) والشفرات – MDS على GF(37)

رسالة تقدمت بها

فردوس نجيب عبدالله الراوي

إلى
مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
وهي جزء من متطلبات نيل شهادة الماجستير علوم
في الرياضيات / بحتة

بإشراف
الاستاذ المساعد
الدكتورة ندى ياسين قاسم يحيى

1442هـ 2020 م

المستخلص

من اهم التطبيقات الهندسة الجبرية في المستوي الاسقاطي $PG(2,q)$ نظرية التشفير والشفرات – MDS ذات بعد $n = 3,5$ وشفرة تصحيح الاخطاء_e .

تعرف الشفرة الخطية _$[k,n,d]_q$ بانها نظام ثلاثية طولها k وبعده n مع وجود اقصر مسافة بين الشفرات $d = k-n$ معرفة على حقل كالوا $GF(q)$. ان علاقة الشفرة الخطية بالقوس –(K,n) والمجموعة القالبية – (ℓ,t) هي علاقة وجود .

من الاهداف الرئيسية لهذه الرسالة دراسة نظرية التشفير وتطبيق النتائج على عدم وجود الشفرات الخطية _$[k,n,d]$ و تحديد الشفرات – MDS وشفرات تصحيح الاخطاء_e

قمنا بإثبات عدم وجود الاقواس لقيم n=26,…46 في المستوي الاسقاطي $PG(2,47)$ مع الشفرات الخطية غير الموجودة وحصلنا على مبرهنتين جديدتين

اثبات القيد الاعلى الجديد لقيم n=32,…,58 في $PG(2,59)$ وحصلنا على مبرهنة جديدة .

وكذلك استطعنا تحسين احدى المعلمات k,n,d للشفرة الخطية التي هي عبارة عن فضاء جزئي ذي ابعاد n للفضاء المتجه k ذو الابعاد $V(k,q)$ مع عدم وجود متجه صفري له وزن على الاقل d بالنسبة للقيم المعطاة للاثنين والثابت q , وكدلك تصحيح الاخطاء للشفرة ذي الحد الادنى للمسافة 2e+1 على الاقل وحصلنا المبرهنة جديدة على شفرة –MDS لان مجموع $V(C)$=0 عندما n=3 وعند تطبيقها على البعد n=5 اصبحت المجموع =1 وبذلك حصلنا مبرهنة جديدة هي شفرة – $AMDS$ وبينا ان الاقواس لها تطبيقات في نظرية التشفير وكل قوس يمكن تفسيرها على انه شفره خطية.

UNIVERSITY OF MOSUL
COLLEGE OF COMPUTER SCIENCES
AND MATHEMATICS

Bounds On Minimum Distance for Linear Codes over GF(q) and MDS - Codes over GF(37)

A Thesis Submitted By

Fardos Najeeb Abdullah Al-Rawi

To

**The Council of the College of
Computer Sciences and Mathematics
University of Mosul
In a Partial Fulfillment of Requirements
For the Degree of Master of Science
In**

Mathematics/Pure

Supervised by

Assistant professor

Dr.Nada Yassen kasm Yahya

2020 A.D. **1441 A.H.**

Abstract

One of the most important applications of algebraic geometry at the projection plane *PG(2,q)* is the theory of coding and *MDS*- codes with $n = 3,5$ dimension and error correction code.

The linear code- $[k,n,d]_q$ is defined as a triple system with a length of k and after it n with the minimum distance between the codes $d = k\text{-}n$ defined by *GF(q)* field. The relationship of the linear code to the arc - *(K,n)* and the blocking set - (ℓ,t) is an existential relationship.

One of the main objectives of this thesis is to study coding theory and apply the results to the absence of linear codes _ $[k,n,d]_q$ and identification of *MDS*- codes and error correction codes

We demonstrated the absence of parentheses for the values of $n = 26, \ldots., 46$ in the projection plane *PG* (2,47) with non-existent linear codes and obtained the two new theorems and the new upper bound of the values of $n = 32,\ldots, 58$ in *PG* (2,59) and we got the new theorem

Also, we were able to improve one of the parameters k, n, d for the linear code, which is a subspace with dimensions n for the vector space k with dimensions *V(k, q)* with no zero vector having a weight of at least d in relation to the given values of the two and the constant q, as well as Correcting the errors for the code with the minimum distance of at least $2e + 1$ and we got the new theorem on the *MDS*- code because the sum of $\nabla(C) = 0$ when $n = 3$ and when applied to the dimension $n = 5$ the sum becomes = 1 and thus we got the new theorem It is the *AMDS*- code, indicating that parentheses have applications in coding theory, and each arc can be interpreted as a linear code.