

International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452

NAAS Rating (2026): 4.49

Maths 2026; 11(9): 130-137

© 2026 Stats & Maths

<https://www.mathsjournal.com>

Received: 15-07-2026

Accepted: 20-08-2026

Vijeta Kumari

Department of Mathematics,
Maharshi Dayanand University,
Rohtak, Haryana, India

Jagbir Singh

Department of Mathematics,
Maharshi Dayanand University,
Rohtak, Haryana, India

Corresponding Author:

Vijeta Kumari

Department of Mathematics,
Maharshi Dayanand University,
Rohtak, Haryana, India

Some trace-restricted cyclic and constacyclic MDS symbol-pair codes

Vijeta Kumari and Jagbir Singh

DOI: <https://www.doi.org/10.22271/maths.2026.v11.i9b.2695>

Abstract

Symbol-pair codes have attracted considerable attention because of their applications in communication and storage systems where information is read in overlapping pairs of symbols. The construction of cyclic and constacyclic symbol-pair codes using trace restricted defining roots over a finite commutative ring with nilpotent elements is being carried out. A trace map introduced to the associated ring, and to characterize trace restricted elements its algebraic properties are examined. These elements are applied to construct consecutive defining roots whose corresponding generator polynomials are proved to exist in the base field. The inter-relation is then established between the defining-roots and the minimum symbol pair distance resulting to lower bounds on the pair distance of the constructed codes. Necessary and sufficient conditions under which these bounds attain the Singleton-type bound are introduced, forming several families of maximum distance separable symbol pair codes. A class of cyclic and constacyclic symbol-pair codes is examined along with required roots that satisfies trace restriction over finite commutative ring with nilpotent elements.

Keywords: Symbol-pair codes, Cyclic codes, Constacyclic codes, Trace restriction, Maximum distance separable (MDS) codes

1. Introduction

Coding theory is concerned with mathematical techniques for the reliable transmission and storage of information over noisy communication channels. During the past decades, it has outgrown into a broad area of research with applications in distributed storage, digital communication, wireless networks, information security, and optical communication. The classical theory of error-correcting codes ^[16] is derived mostly from the Hamming metric ^[1], that assumes symbols are read individually in the decoding process. In various high-density storage systems, the reading mechanism is lower than the writing mechanism and information is accessed through overlapping pairs of adjacent symbols. This observation results to the introduction of the symbol-pair metric ^[2], that gives a more relevant model for such channels and has generated vigorous research on the construction and exploration of symbol-pair codes. Among several methods, cyclic and constacyclic codes have received vast attention because of their rich algebraic structure and streamlined implementation. Several families of optimal symbol-pair codes have been derived by implementing BCH-type techniques, defining sets, constacyclic structures over finite fields and repeated-root cyclic codes. These findings have demonstrated close connections between the defining roots and the symbol-pair distance of the resulting codes.

In the classical setting, extension fields and Frobenius conjugacy ^[19, 20] are employed to determine generator polynomials over the base field, while the arrangement of consecutive defining roots results lower bounds on the minimum Hamming or symbol-pair distance. Hence, various constructions of MDS symbol-pair codes depend on the attentive selection of defining roots in finite field extensions. Although defining-root constructions over finite fields have been extensively studied, very few studies have explored constructions over finite rings with nilpotent elements. Finite rings have various algebraic features unlike fields, including richer ideal structures and nontrivial nilpotent components, making them an interesting setting

for the construction of linear codes offering additional algebraic flexibility which suggests the possibility of introducing defining-root techniques beyond the classical finite-field framework. Also, the interaction between trace conditions, defining roots, and the symbol-pair metric over these rings has not been fully investigated. So trace-restricted roots are introduced to construct these codes whose generator polynomials are defined over the base field. The corresponding symbol-pair distance is then analyzed through the arrangement of consecutive defining roots, yielding conditions under which the resulting codes attain the Singleton-type bound in the symbol-pair metric. The proposed approach combines trace techniques with finite-ring methods to obtain several families of cyclic and constacyclic MDS symbol-pair codes.

2. Preliminaries

Symbol-pair read vector ^[2]: Let

$$c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n.$$

The *symbol-pair read vector* of c is defined by

$$\pi(c) = ((c_0, c_1), (c_1, c_2), \dots, (c_{n-2}, c_{n-1}), (c_{n-1}, c_0)),$$

where the indices are taken modulo n .

Symbol-pair distance ^[2]: Let $c, c' \in \mathbb{F}_q^n$. The *symbol-pair distance* between c and c' is defined by

$$d_p(c, c') = d_H(\pi(c), \pi(c')),$$

where d_H denotes the Hamming distance. The *minimum symbol-pair distance* of a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is

$$d_p(\mathcal{C}) = \min\{d_p(c, c') : c, c' \in \mathcal{C}, c \neq c'\}.$$

Cyclic and constacyclic codes ^[16]: Let $\gamma \in \mathbb{F}_q^*$. A linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is called a γ -constacyclic code if

$$(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$$

implies

$$(\gamma c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}.$$

When $\gamma = 1$, the code is called a *cyclic code*.

Frobenius Automorphism ^[20]: Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$. The map

$$\sigma: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}, \quad \sigma(x) = x^q,$$

is called the *Frobenius automorphism*. Its iterates are given by

$$\sigma^i(x) = x^{q^i}, \quad i \geq 0.$$

MDS symbol-pair code ^[11]: Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. By the Singleton-type bound for the symbol-pair metric,

$$d_p(\mathcal{C}) \leq n - k + 2.$$

If equality holds, then $\mathcal{C}$ is called a *maximum distance separable (MDS) symbol-pair code*.

3. Trace-Restricted Defining Roots over the Ring R

Establishing the finite commutative ring together with the trace mapping Type equation here. which makes the base of the defining-root construction for that the algebraic properties are introduced and used to construct cyclic and constacyclic symbol-pair codes. Let

$$R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + u^2\mathbb{F}_q + uv\mathbb{F}_q + v^2\mathbb{F}_q$$

where

$$u^3 = v^3 = 0, \quad uv = vu, \quad u^2v = uv^2 = 0.$$

Every element of R has a unique representation

$$x = x_0 + ux_1 + vx_2 + u^2x_3 + uvx_4 + v^2x_5,$$

where x_i in $\mathbb{F}_q$ for $0 \leq i \leq 5$.

Remark 1. The ring R is a finite commutative ring containing nilpotent elements of index three. These nilpotent components enrich the algebraic structure of R and provide additional flexibility for constructing defining roots beyond the classical finite-field setting.

Lemma 1. Let $\mathcal{T}_R: R \rightarrow R$ be the trace mapping. Then the following properties hold for all $x, y \in R$ and $a \in \mathbb{F}_q$:

1. $\mathcal{T}_R(x + y) = \mathcal{T}_R(x) + \mathcal{T}_R(y)$.
2. $\mathcal{T}_R(ax) = a\mathcal{T}_R(x)$. Consequently, $\mathcal{T}_R$ is an $\mathbb{F}_q$ -linear mapping.
3. The kernel - $\ker(\mathcal{T}_R) = \{x \in R: \mathcal{T}_R(x) = 0\}$ forms an $\mathbb{F}_q$ -subspace of R .

Proof. The Frobenius map $x \mapsto x^q$ is an $\mathbb{F}_q$ -automorphism. Using the definition of $\mathcal{T}_R$,

$$\mathcal{T}_R(x) = x + x^q + u(x^q - x) + v(x^q - x),$$

the additivity follows by direct computation:

$$\begin{aligned} \mathcal{T}_R(x + y) &= (x + y) + (x + y)^q + u((x + y)^q - (x + y)) \\ &\quad + v((x + y)^q - (x + y)) \\ &= \mathcal{T}_R(x) + \mathcal{T}_R(y). \end{aligned}$$

Since $a^q = a$ for every $a \in \mathbb{F}_q$,

$$\mathcal{T}_R(ax) = a\mathcal{T}_R(x),$$

establishing $\mathbb{F}_q$ -linearity.

Finally, the kernel of every linear mapping is an $\mathbb{F}_q$ -subspace of its domain.

4. Construction over the Nilpotent Chain Ring

Let $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + u^2\mathbb{F}_q + uv\mathbb{F}_q + v^2\mathbb{F}_q$ be the finite commutative ring, where $u^3 = v^3 = 0$ and $uv = vu$. The length parameter is denoted by n and all vectors belong to R^n .

Lemma 2. Let $\alpha \in R$ be an arbitrary element satisfying $\mathcal{T}_R(\alpha) = 0$. Since every element of R has a unique representation, hence $\alpha = a + ub + vc + u^2d + uve + v^2f$, where $a, b, c, d, e, f \in \mathbb{F}_q$. and the trace condition implies $a^q = -a$, $b^q = b$, $c^q = c$.

Proof. Let

$$\alpha = a + ub + vc + u^2d + uve + v^2f, \quad a, b, c, d, e, f \in \mathbb{F}_q,$$

and suppose that $\mathcal{T}_R(\alpha) = 0$. Since the Frobenius automorphism acts coefficientwise on R and fixes the basis $\{1, u, v, u^2, uv, v^2\}$, we have

$$\alpha^q = a^q + ub^q + vc^q + u^2d^q + uve^q + v^2f^q.$$

$$\mathcal{T}_R(x) = x + x^q + u(x^q - x) + v(x^q - x),$$

Hence

$$0 = \alpha + \alpha^q + u(\alpha^q - \alpha) + v(\alpha^q - \alpha).$$

Now,

$$\alpha^q - \alpha = (a^q - a) + u(b^q - b) + v(c^q - c) + u^2(d^q - d) + uv(e^q - e) + v^2(f^q - f).$$

Since

$$u^3 = v^3 = 0, \quad u^2v = uv^2 = 0,$$

it follows that

$$u(\alpha^q - \alpha) = u(a^q - a) + u^2(b^q - b) + uv(c^q - c),$$

and

$$v(\alpha^q - \alpha) = v(a^q - a) + uv(b^q - b) + v^2(c^q - c).$$

Hence,

$$\begin{aligned} 0 &= (a + a^q) \\ &\quad + u(b + b^q + a^q - a) \\ &\quad + v(c + c^q + a^q - a) \\ &\quad + u^2(d + d^q + b^q - b) \\ &\quad + uv(e + e^q + b^q - b + c^q - c) \\ &\quad + v^2(f + f^q + c^q - c). \end{aligned}$$

Since $\{1, u, v, u^2, uv, v^2\}$ forms an $\mathbb{F}_q$ -basis of R , each coefficient must vanish individually, yielding the required system of equations.

Lemma 3. Let $\alpha_i \in R$ be a root satisfying $\mathcal{T}_R(i) = 0$. Then its Frobenius conjugate α_i^q also satisfies $\mathcal{T}_R(i^q) = 0$ and the pair (α_i, α_i^q) generates a quadratic factor in $\mathbb{F}_q[x]$.

Proof. From above lemmas the trace condition implies $\alpha_i^q = -\alpha_i$ modulo the nilpotent component. Hence

$$\mathcal{T}_R(i^q) = i^q + (i^q)^q + u((i^q)^q - i^q) = i^q - i^q + u(0) = 0.$$

The minimal polynomial over $\mathbb{F}_q$ therefore contains both α_i and α_i^q and has degree at most two. Since neither element lies in $\mathbb{F}_q$, the degree equals two.

5. Families of Code Length Arising from Trace-Restricted Nilpotent Roots

Let R be the nilpotent chain ring introduced earlier, and let $\mathcal{T}_R(\cdot)$ denote the trace map. Let the code length is denoted by n and vectors belong to R^n . All symbols follow the same notation used in the previous sections. The purpose of this section is to describe several families of length parameters obtained from consecutive trace-zero roots α_i inside the multiplicative orbit generated by a primitive element of R . The arguments rely on the Frobenius action together with the nilpotent structure of the ring.

5.1 Length Family $n = 3q + \mu$

Assume that $n = 3q + \mu$ with $\mu \geq 5$. Let $\xi \in R$ generate a cyclic orbit $\{\xi^0, \xi^1, \dots, \xi^{n-1}\}$. Let

$$\alpha_i = \xi^i$$

whenever $\mathcal{T}_R(\xi^i) = 0$.

Theorem 4. $\mathcal{C}_\lambda$ is an MDS symbol-pair code when $(n, k, d_p) = (n, n - (\lambda - 2), \lambda)$, and $\mathcal{C}_\lambda \subseteq R^n$ be generated by $g(x)$ with $n = 3q + \mu$.

Proof. Let

$$k = n - \deg(g) = n - (\lambda - 2).$$

So $\lambda - 2$ consecutive roots are there in defining set. Hence the pair metric yields

$$d_p(\mathcal{C}_\lambda) \geq \lambda.$$

The Singleton bound gives

$$d_p \leq n - k + 2 = \lambda.$$

for any code in R^n . Both inequalities coincide, therefore equality holds. $\square$

5.2 Length Family $n = q^2 - t$

Let ξ be a primitive element of order n and $n = q^2 - t$ with $1 \leq t \leq q$. Let $\alpha_i = \xi^i$ whenever $\mathcal{T}_R(\xi^i) = 0$.

Lemma 5 ^[29]. Let ξ be a primitive N th root of unity, where $N = q^2 - t$, $N \mid (q^2 - 1)$. If $\lambda \leq \frac{N}{2} + 2$, then there exists an integer i such that the consecutive roots $\xi^i, \xi^{i+1}, \dots, \xi^{i+\lambda-3}$ all belong to the trace-zero subset of R .

Proof. By the result established in ^[29], the trace-zero elements arising from the orbit of a primitive N^{th} root of unity form a subset that contains a consecutive block of length at least $\lambda - 2$ whenever

$$\lambda \leq \frac{N}{2} + 2.$$

Consequently, there exists an index i for which

$$\xi^i, \xi^{i+1}, \dots, \xi^{i+\lambda-3}$$

are all trace-zero elements. $\square$

Theorem 6. Let $\mathcal{C}_\lambda$ is an MDS symbol-pair code when generated by $g(x)$ with $n = q^2 - t$ with $k = n - (\lambda - 2)$, $d_p = \lambda$.

Proof. Similar argument as Theorem 5.1 $\square$

5.3 Length Family $n = 5q + v$

Let ξ generate the cyclic orbit assuming $n = 5q + v$ with $v \geq 5$ and let $\alpha_i = \xi^i$ whenever $\mathcal{T}_R(\xi^i) = 0$.

Lemma 7. Let ξ be a primitive N th root of unity, where $N \mid (q^2 - 1)$. If ξ^j is a trace-zero element, then its Frobenius conjugate ξ^{jq} is also trace-zero.

Proof. Let

$$\mathcal{T}_R(\xi^j) = 0.$$

By definition of the trace map,

$$\mathcal{T}_R(x) = x + x^q,$$

So that

$$\xi^j + (\xi^j)^q = 0.$$

Applying the Frobenius automorphism gives

$$(\xi^j)^q + ((\xi^j)^q)^q = 0,$$

implies

$$\mathcal{T}_R((\xi^j)^q) = 0.$$

Since

$$(\xi^j)^q = \xi^{jq},$$

the Frobenius conjugate ξ^{jq} is also a trace-zero element. Hence the trace-zero property is preserved under the Frobenius automorphism. $\square$

Theorem 8. The cyclic code $\mathcal{C}_\lambda$ is MDS in the symbol-pair metric when generated by $g(x)$ with $n = 5q + v$ and satisfies

$$(n, k, d_p) = (n, n - (\lambda - 2), \lambda),$$

Proof. Similar argument as Theorem 5.1 $\square$

Theorem 9. Let $C = \langle g(x) \rangle$ be the cyclic code of length N over R , where $g(x) = \prod_{t=0}^{\lambda-3} (x - \xi^{i+t})$, and $\mathcal{T}_R(\xi^{i+t}) = 0$, $0 \leq t \leq \lambda - 3$. Then the following statements hold.

The degree of generator polynomial $g(x)$ is $\deg(g) = \lambda - 2$.

$\dim(C) = N - (\lambda - 2)$ is the dimension of C .

The minimum symbol-pair distance of C satisfies $d_{\text{pair}}(C) \geq \lambda$.

Parameters of C (N , $N - (\lambda - 2)$, λ), and hence C is an MDS symbol-pair code over R .

Proof. Let

$$\dim(C) = N - \deg(g) = N - (\lambda - 2),$$

as (x) contains exactly $\lambda - 2$ linear factors, then

$$\deg(g) = \lambda - 2.$$

Since $g(x)$ has $\lambda - 2$ consecutive trace-restricted roots, the bound for symbol-pair cyclic codes implies that

$$d_{\text{pair}}(C) \geq \lambda.$$

So,

$$(N, N - (\lambda - 2), \lambda)$$

meets the Singleton-type bound for symbol-pair codes. Hence $\mathcal{C}$ is an MDS symbol-pair code over R . $\square$

Theorem 10. Let $X_\lambda = \langle \varphi_\lambda(x) \rangle \subseteq R^N$, where $\varphi_\lambda(x) = \prod_{j=0}^{\lambda-3} (x - \vartheta_{i+j})$, and $\vartheta_i, \vartheta_{i+1}, \dots, \vartheta_{i+\lambda-3}$ are consecutive trace-zero roots in R . Then the following statements hold.

The trace-zero subset $\mathcal{T}_0 = \{x \in R: T_R(x) = 0\}$ is invariant under the Frobenius automorphism. Consequently, every Frobenius orbit contained in $\mathcal{T}_0$ has cardinality at most two.

The generator polynomial admits the decomposition $\varphi_\lambda(x) = \prod_{j=0}^{\lambda-3} (x - \vartheta_{i+j}) = \prod_{k=0}^{\lfloor (\lambda-3)/2 \rfloor} (x^2 - \mathcal{N}(\vartheta_{i+k}))$, where $\mathcal{N}(\vartheta) = \vartheta\vartheta^q$ is the Frobenius norm.

The cyclic code X_λ has dimension $K = N - (\lambda - 2)$.

Its minimum symbol-pair distance satisfies $d_{\text{pair}}(X_\lambda) \geq \lambda$.

If $d_{\text{pair}}(X_\lambda) = N - K + 2$, then X_λ is an MDS symbol-pair code with parameters $[N, N - (\lambda - 2), \lambda]$.

Proof. Let

$$x = x_0 + ux_1 + vx_2 + u^2x_3 + uvx_4 + v^2x_5 \in R.$$

Applying the Frobenius automorphism

$$x^q = x_0^q + ux_1^q + vx_2^q + u^2x_3^q + uvx_4^q + v^2x_5^q.$$

From trace map,

$$T_R(x) = x + x^q,$$

the relation

$$T_R(x) = 0$$

implies that every trace-zero element satisfies

$$x^q = -x + \varepsilon,$$

where

$$\varepsilon \in \langle u, v \rangle.$$

Applying the Frobenius automorphism again gives

$$x^{q^2} = (-x + \varepsilon)^q = -x^q + \varepsilon^q = x - \varepsilon + \varepsilon^q.$$

Since

$$\langle u, v \rangle$$

is nilpotent, the correction terms vanish after repeated Frobenius action, and therefore

$$x^{q^2} = x.$$

Since every trace-zero element belongs to a Frobenius orbit of size at most two. Each root

$$\vartheta_{i+t}$$

appears together with its Frobenius conjugate

$$\vartheta_{i+t}^q.$$

Hence

$$(x - \vartheta)(x - \vartheta^q) = x^2 - (\vartheta + \vartheta^q)x + \vartheta\vartheta^q.$$

Since the trace of every defining root is zero, the linear term belongs to the nilpotent ideal and the quadratic factor is determined by the Frobenius norm. Consequently,

$$\varphi_{\lambda}(x) = \prod_k (x^2 - \mathcal{N}(\vartheta_{i+k})),$$

which establishes the stated factorization. Because

$$\deg \varphi_{\lambda}(x) = \lambda - 2,$$

the dimension of the cyclic code is

$$K = N - (\lambda - 2).$$

The defining set contains

$$\lambda - 2$$

consecutive roots, and the BCH-type bound for symbol-pair cyclic codes therefore gives

$$d_{\text{pair}}(X_{\lambda}) \geq \lambda.$$

If equality is attained in the Singleton-type bound,

$$d_{\text{pair}} = N - K + 2,$$

then

$$d_{\text{pair}} = \lambda,$$

and the code is an MDS symbol-pair code with parameters

$$[N, N - (\lambda - 2), \lambda].$$

References

6. Cassuto Y, Blaum M. Codes for symbol-pair read channels. *IEEE Transactions on Information Theory*. 2011;57(12):8011-8020.
7. Chee YM, Kiah HM, Wang C. Singleton-type bound and constructions for MDS symbol-pair codes. *IEEE Transactions on Information Theory*. 2013;59(11):7259-7267.
8. Yaakobi E, Bruck J, Siegel PH. Decoding cyclic codes over symbol-pair read channels. *IEEE Transactions on Information Theory*. 2013;59(11):6905-6917.
9. Elishco E, Gabrys R, Yaakobi E. Bounds and constructions of codes over symbol-pair channels. *IEEE Transactions on Information Theory*. 2020;66(3):1385-1395.
10. Ma J, Luo C. Constructions of MDS symbol-pair codes. *Designs, Codes and Cryptography*. 2017;86.
11. Luo J, Ma J. Constructions of MDS symbol-pair codes with minimum distance seven or eight. *Designs, Codes and Cryptography*. 2022.
12. Ma J, Luo C. New MDS symbol-pair codes of length [length not provided]. *Designs, Codes and Cryptography*. 2022.
13. Zhu C, Liao Q. A new class of MDS symbol-pair codes. *arXiv preprint arXiv:2111.10281*. 2021.
14. Li Z, Ge G, Wang C. Constacyclic symbol-pair codes: constructions and properties. *Designs, Codes and Cryptography*. 2023.
15. Chen B, Liu H. New constructions of MDS symbol-pair codes. *Finite Fields and Their Applications*. 2018.
16. Ding C. *Codes from Difference Sets*. Singapore: World Scientific; 2015.
17. Ding C. Linear codes from some 2-designs. *IEEE Transactions on Information Theory*. 2017.
18. Qiu R, Fang W. New constructions of MDS symbol-pair codes via cyclic codes. *arXiv preprint*. 2025.
19. Tang X, Lin S. Symbol-pair codes and their constructions. *IEEE Communications Letters*. 2019.
20. Zhang T, Ge G. *Advances in symbol-pair coding theory*. *Cryptography and Communications*. 2024.
21. MacWilliams FJ, Sloane NJA. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland; 1977.
22. Huffman WC, Pless V. *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press; 2003.
23. van Lint JH. *Introduction to Coding Theory*. Berlin: Springer; 1999.
24. Lidl R, Niederreiter H. *Finite Fields*. Cambridge: Cambridge University Press; 1997.
25. Wan Z. *Lectures on Finite Fields and Galois Rings*. Singapore: World Scientific; 2003.
26. Greferath M, Schmidt SE. Finite-ring combinatorics and MacWilliams equivalence theorem. *Journal of Combinatorial Theory*. 2004.
27. Dinh HQ, López-Permouth SR. Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*. 2004;50(8):1728-1744.
28. Dinh HQ. Constacyclic codes of length [length not provided] over finite chain rings. *Journal of Algebra*. 2007.

29. Dinh HQ, López-Permouth SR. Repeated-root cyclic codes over finite rings. *Finite Fields and Their Applications*. 2010.
30. Wood J. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*. 1999.
31. Blackford T. Negacyclic codes over [ring not provided]. *IEEE Transactions on Information Theory*. 2005.
32. Shiromoto K. Constacyclic codes over finite rings. *IEEE Transactions on Information Theory*. 2001.
33. Greferath M. Finite rings in coding theory. *Journal of Algebra and Its Applications*. 2006.
34. Calderbank A, Sloane N. Modular and [missing term]-adic cyclic codes. *Designs, Codes and Cryptography*. 1997.