YARI DEVİRLİ KODLAR

Nilgün Külhan, İrfan Şiap

Özet - **Lineer kodlar ailesinin içinden olan devirli kodlar cebirsel olarak zengin bir yapıya sahip olduklarından önem arz ederler. Ancak daha büyük uzunluklarda hata düzeltme kabiliyetleri zayıflamaktadır. Bunun aksine, yarı devirli kodlar devirli kodların bir doğal genellemesi olmasına rağmen büyük uzunluklarda çok iyi bir performans sergilemekte ve bir çok yeni kod bu aileden keşfedilmektedir. Bu çalışmamızda yarı devirli kodların cebirsel yapıları, özellikleri incelenecek ve BCH tipinde bir alt sınır verilecektir.**

Anahtar Kelimeler – lineer kod, devirli kod, yarı devirli kod, BCH – sınırı.

Abstract- **Cyclic codes which are a family of linear codes have a rich algebraic structure. However, their error correction capability for larger lenghts is weak. On the contrary, although quasi cyclic codes are a natural generalization of cyclic codes in larger lengths they perform better than cyclic codes and many (record breaking) new codes are found from this family. In this survey, we investigate the structure, properties of quasi cyclic codes and give a BCH-type bound for quasi cyclic codes.**

Keywords – linear code, cyclic code, quasi cyclc code, BCH – bound.

I. GİRİŞ

Bilgi çağında yaşadığımız bu günlerde bilginin transferi (cep telefonları, internet, bankacılık, vs.) ya da depolanması (CD, vs.) aşamasında meydana gelebilecek bilgi zedelenmelerini koruma ve düzeltme amacıyla kodlama kullanılmaktadır.

N.Külhan; Adapazarı Atatürk Lisesi, Adapazarı, Sakarya
İ.Şiap; Gaziantep Üniversitesi, Adıyaman Eğitim Fakültesi, Adıyaman. e-mail : isiap@gantep.edu.tr

Bu anlamda kullanılan kodlar içinde lineer kodlar önemli bir yer tutmaktadır. Bu çalışmada, lineer kodlar ailesinin zengin cebirsel yapısına sahip ve bu ailenin bir alt kümesi olan yarı devirli kodlar ailesi incelenecektir. İkinci ve üçüncü bölümlerde sırasıyla lineer ve devirli kodlar ile ilgili temel tanım ve teoremler verilecektir. Üçüncü bölümde ise yarı devirli kodlar ailesi tanımlanacaktır. Bu kod ailesi ile ilgili örnekler verilip teoremler ispatlanacaktır. Birinci ve ikinci bölümde geçen tanım, teorem ile ilgili daha geniş bilgi için [1] kitabından faydalanılabilir.

II. LİNEER KODLAR

t pozitif bir tamsayı ve p bir asal sayı olsun. F_q, karakteristiği p olan $q = p^t$ elemanlı sonlu bir cisim olsun. F_q cismini kısaca F ile gösterelim. F^n, F-vektör uzayının bileşen bileşene toplama ve skaler ile çarpma işlemlerine göre herhangi bir alt vektör uzayına n uzunluğunda bir ***lineer kod*** denir. C alt vektör uzayının (yani kodun) boyutu k olduğunda C ye kısaca bir $[n,k]$-kod denir. Bu durumda C nin eleman sayısı q^k olur. F^n nin elemanlarına ***söz***, C nin elemanlarına ise ***kodsöz*** denir. $x, y \in F^n$ vektörlerinin karşılıklı bileşenlerinin farklı oldukları yerlerinin sayısına x ve y vektörlerinin ***Hamming uzaklığı*** denir ve $d(x,y)$ ile gösterilir.

$d : A^n x\ A^n \rightarrow []$

ve $d(x,y) = \left|\{i \mid x_i \neq y_i, \quad 1 \leq i \leq n\}\right|$ olmak üzere, (A^n, d) ikilisi bir metriktir.

$d(C) = \min_{x,y \in C, x \neq y} d(x,y)$ sayısına C kodun ***minimum uzaklığı*** denir. F cismi üzerinde tanımlı olan

n uzunluğunda, k boyutlu, ve minimum uzaklığı d olan

Bir kodsözdeki sıfırdan farklı bileşenlerin sayısına ise o kodsözün ***Hamming ağırlığı*** yada kısaca kodsözün ***ağırlığı*** denir. İki kodsöz arasındaki Hamming uzaklığı ise bu kodsözlerin farklarının Hamming ağırlığına eşittir. C deki kodsözlerin sıfırdan farklı en küçük ağırlığına **C** nin ***Hamming ağırlığı*** denir ve kısaca $w(C)$ ile gösterilir. Diğer yandan, C deki sıfırdan farklı en küçük Hamming uzaklığına ise C nin ***minimum uzaklığı*** denir ve $d(C)$ ile gösterilir. Lineer kodlarda $d(C) = w(C)$ dir. Lineer kodların vektör uzayları olması dışında Hamming uzaklığı yardımıyla kodun hata düzeltme kabiliyeti hakkında bilgi ediniriz. Hamming minimum uzaklığı bilmenin faydası aşağıdaki teorem ile görülür:

Teorem II.1: [1] C lineer kodun uzunluğu n ve minimum uzaklığı $d = 2t+1$ veya $d = 2t$ olsun. Bu durumlarda C kodu tam t hata düzeltir.

Tanım II.1. C, $[n,k]$ bir lineer kod olsun. Satırları C nin bazından oluşan $k \times n$ tipindeki matrise C nin ***üreteç matrisi*** denir.

Eğer bir C kodunun bileşenlerine bir permütasyon uygulanarak D kodu elde ediliyorsa C kodu ile D kodu birbirine ***denktir*** denir. Dikkat edilirse C ile D nin üç temel parametreleri n, k, ve d aynıdır ve kodlama anlamında farklı yapılar değildirler.

II. DEVİRLİ KODLAR

$(n,q)=1$ olsun. $R_n = F_q[x]/\langle x^n - 1\rangle$ bir temel ideal halkasıdır.

$$\psi : V(n,q) \rightarrow R_n$$

$$\psi((c_0, c_1, \ldots, c_{n-1})) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \quad \ldots.(III.1)$$

ise ψ, $V(n,q)$ ile R_n arasında bir F_q-vektör uzayı izomorfizmasıdır.

Tanım III.1: C lineer bir kod olsun. Eğer herhangi bir $(c_0, c_1, \ldots, c_{n-1}) \in C$ için $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ ise $C \subset V(n,q)$'ye bir ***devirli kod*** denir. Yani, C devirli kodun herhangi bir kodsözü devresel olarak 1 bileşen sağa doğru ötelendiğinde yine kodun içine düşerse bu lineer koda devirli kod denir. C devirli kodu $\psi(C)$ ile özdeşlendiğinde R_n'nin bir ideali olduğu görülür.

bir C kodu kısaca $[n,k,d]_q$ - kodu olarak gösterilir.

R_n bir temel ideal halkası olduğundan, C devirli kodunu üreten bir $f(x)$ polinomu vardır, yani $C = \langle f(x)\rangle$, ayrıca $f(x) \mid (x^n - 1)$ [1].

ÖnermeIII.1:[1]
$f(x) = a_0 + a_1 x + \ldots + a_r x^r$, $a_r = 1$ ve $f(x)$ fonksiyonu $x^n - 1$'i tam bölsün. $C = \langle f(x)\rangle$, R_n'nin bir ideali olarak $f(x)$'in ürettiği devirli lineer kod olan C'nin boyutu $n - r = k$'dır ve üreteç matrisi,

$$G = \begin{bmatrix} 0 & \cdots & 0 & a_0 & \ldots & a_r \\ 0 & \cdots & a_0 & \ldots & a_r & 0 \\ \vdots & & & & & \vdots \\ a_0 & \cdots & a_r & 0 & \ldots & 0 \end{bmatrix}_{k \times n}$$

şeklindedir.

Yukarıdaki Teorem II.1 de görüldüğü gibi kodun minimum uzaklığını bilmek çok önemlidir. Devirli kodlarda minimum uzaklık için bir alt sınır verme imkanı vardır. Bu alt sınıra BCH sınırı denir.

Teorem (BCH sınırı) III.2: [1] $C = \langle f(x)\rangle \subset R^n$ devirli bir kod ve $f(x) \mid (x^n - 1)$ olsun. $f(x)$ polinomunun parçalanış cismi F_{q^s} olsun. F_{q^s} cismini üreten ve birimin n. ilkel kökü w olsun. w nin $f(x)$ in kök olan en çok sayıdaki ardışık kuvvetlerinin sayısı a olsun. Bu durumda

$$d(C) \geq a + 1$$

olur.

III. YARI DEVİRLİ KODLAR

n uzunluğundaki bir kod içinde 1 bileşen ötelemesi ile invaryant kalan lineer koda devirli kod demiştik. Bunun doğal bir genellemesi ise l $(1 \leq l \leq n)$ ötelemesi altında invaryant kalan (değişmeyen) kodlardır.

Tanım IV.1: l $(1 \leq l \leq n)$ devirsel ötelemesi altında invaryant kalan koda l-yarı devirli (l-Quasi-cyclic) ya

da kısaca l-QC kod denir. n ile l aralarında asal olduklarında l-QC kodu devirli bir kod olur. Bu durum ilginç olmadığından $n = ml$ alınır. Ayrıca bu bölümün tamamında m ile q sayılarının aralarında asal oldukları kabul edilecektir.

Yarı devirli kodlar üzerinde yapılan çalışmalar son zamanlarda yoğunlaşmıştır. Bunun başlıca sebeplerinden bazıları şunlardır:

1. Yarı devirli kodlar devirli kodların doğal bir genelleştirilmesi olduğundan cebirsel yapıları zengindir [2],[3],[4],[5],[9] ve [13].
2. Asimptotik (çok büyük uzunluklarda) olarak iyidirler [14],
3. Bazı önemli kodların yapıları yarı devirli kodlar gibi ya da bunlara denktir [1] ve [13],
4. Son zamanlarda yapılan araştırmalarda en iyi parametrelere sahip lineer kodlar yarı devirli kodlar ailesinden elde edilmiştir [6], [7], [10], [11], ve [12].

Yukarıda saydığımız sebepler bu kod ailesini yeterince ilginç kılmaktadır.

Tanım IV.2: $\begin{bmatrix} c_0 & c_1 & \cdots & c_m \\ c_m & c_0 & \cdots & c_{m-1} \\ \vdots & & & \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix}$ tipindeki matrislere **devresel** (circulant) **matris** denir.

Yarı devirli (QC) kod ailesinin üreteç matrislerinin yapısı [5] makalesinde şu aşağıdaki önemli teorem ile vermiştir:

Teorem IV.1: [5] C, n uzunluğunda bir l-QC kodu olsun.

$$G_{ij} = \begin{bmatrix} g_0^{ij} & g_1^{ij} & \cdots & g_{m-1}^{ij} \\ g_{m-1}^{ij} & g_0^{ij} & \cdots & g_{m-2}^{ij} \\ \vdots & & & \\ g_1^{ij} & g_2^{ij} & \cdots & g_0^{ij} \end{bmatrix}, 1 \le i \le k, 1 \le j \le l$$

$m \times m$ tipinde devresel alt matrisler olmak üzere C kodu, üreteç matrisi

$$G = \begin{bmatrix} G_{11} & G_{12} & \cdots & G_{1l} \\ G_{21} & G_{21} & \cdots & G_{2l} \\ \vdots & & & \\ G_{k1} & G_{k2} & \cdots & G_{kl} \end{bmatrix}_{mk \times n} \quad \ldots\ldots\ldots \text{(IV.1)}$$

şeklinde olan bir koda denktir.

Yukarıdaki Teorem yardımıyla l-QC kodlarının üreteç matrisleri (IV.1) şeklinde olduğunu kabul edebiliriz.

Devirli kodlara benzer şekilde (IV.1) matrisindeki her satıra (III.1) deki ψ dönüşümü yardımıyla aşağıdaki gibi bir polinom vektörü karşılık getirilsin. $\overline{g}_{ij} = (g_0^{ij}, g_1^{ij}, \ldots, g_{m-1}^{ij})$ olmak üzere $1 \le i \le k$ için

$$\left[\overline{g}_{i1}, \ldots, \overline{g}_{il}\right] \xrightarrow{\Phi} \left(\psi(\overline{g}_{i1}), \ldots, \psi(\overline{g}_{il})\right)$$

şeklinde bir Φ dönüşümü tanımlansın.

Teorem IV.2: $\Phi(C)$ kümesi $\left(F_q / \left(x^m - 1\right)\right)^l$ modülünün bir F_q-alt modülüdür. Φ dönüşümü ise C kodundan $\Phi(C)$ modülüne birebir ve örten olan bir F_q-modül homomorfizmasıdır.

İspat: $\Phi(C)$ kümesi $\left(F_q / \left(x^m - 1\right)\right)^l$ modülünün bir F_q-alt modülü olduğu açıktır.

$$\Phi\left(\left(\overline{g}_{i1}, \ldots, \overline{g}_{il}\right) + \left(\overline{g}_{j1}, \ldots, \overline{g}_{jl}\right)\right)$$
$$= \Phi\left(\overline{g}_{i1} + \overline{g}_{j1}, \ldots, \overline{g}_{il} + \overline{g}_{jl}\right)$$
$$= \left(\psi\left(\overline{g}_{i1} + \overline{g}_{j1}\right), \ldots, \psi\left(\overline{g}_{il} + \overline{g}_{jl}\right)\right)$$

ve ψ toplamsal olduğundan Φ toplamsaldır.

Diğer yandan, $\lambda \in F_q$ olsun,

$$\Phi\left(\lambda\left(\overline{g}_{i1}, \ldots, \overline{g}_{il}\right)\right) = \Phi\left(\lambda\overline{g}_{i1}, \ldots, \lambda\overline{g}_{il}\right)$$
$$= \left(\psi\left(\lambda\overline{g}_{i1}\right), \ldots, \psi\left(\lambda\overline{g}_{il}\right)\right)$$
$$= \left(\lambda\psi\left(\overline{g}_{i1}\right), \ldots, \lambda\psi\left(\overline{g}_{il}\right)\right)$$
$$= \lambda\left(\psi\left(\overline{g}_{i1}\right), \ldots, \psi\left(\overline{g}_{il}\right)\right) = \lambda\Phi\left(\overline{g}_{i1}, \ldots, \overline{g}_{il}\right)$$

bulunur. $\text{Çek}(\Phi) = \{(0, 0, \ldots..0)\}$ olduğundan Φ birebirdir. Örten olduğu ise tanımdan görülmektedir. Dolayısıyla, Φ örten ve birebir olan bir F_q- modül homomorfizmasıdır.

Yukarıdaki önerme yardımıyla l-QC kodları $\left(F_q / \left(x^m - 1\right)\right)^l$ modülünün birer alt modülü olarak düşünebiliriz. Bu yaklaşım yardımıyla, yarı devirli kodların yapıları hakkında daha çok bilgi edinilebilir. $\left(F_q / \left(x^m - 1\right)\right)^l$ nin s tane elemanı tarafından üretilen bir C koduna *s üreteçli bir l-QC kod* denir. Burada s C kodunun boyutuna eşit olmayabilir. Aşağıda verilecek olan teoremler Gröbner bazları yardımıyla [3] ve [4] tarafından ispatlanmıştır. Ancak, [8] de aşağıdaki gibi daha temel bir yaklaşımla teoremlerin ispatı verilmiştir. Ayrıca, Teorem IV.4 ün II. ve III. kısımları yazarlar tarafından verilmiş ve ispatlanmıştır.

Teorem IV.3: C kodu $\{g_1(x), g_2(x), \ldots, g_s(x)\}$ kümesi tarafından üretilen s üreteçli $n = ml$ uzunluğunda bir l-QC kod ve $g_j(x) = (g_{j1}(x), g_{j2}(x), \ldots, g_{jl}(x))$ olsun. Bu durumda, $1 \le i \le l$ ve $1 \le j \le s$ için

$$g_{ji}(x) = f_{ji}(x) g_i(x), \; g_i(x) \mid (x^m - 1)$$

$$\left(f_{ij}(x), \frac{x^m - 1}{g_i(x)}\right) = 1 \text{ ve}$$

$$f_{ij}(x), g_i(x) \in F_q(x)/(x^m - 1)$$

İspat: C kodunun ilk m bloğundan (ilk m koordinata kısıtlanışı) elde edilen vektörler m uzunluğunda bir devirli kodun elemanlarıdır. III bölümden, bu devirli kod $F_q(x)/(x^m - 1)$ in bir ideali olduğundan $g_1(x)$ tarafından üretilir. Benzer şekilde ikinci m ve sırasıyla l. m blokları birer devirli kod üretir. Dolayısıyla, istenen sonuç elde edilmiş olur.

Teorem IV.4: $i = 1, 2, \ldots, l$ için $g_i(x) \mid (x^m - 1)$ ve

$$\left(f_i(x), \frac{x^m - 1}{g_i(x)}\right) = 1 \text{ olsun. } C \text{ kodu}$$

$$(f_1(x)g_1(x), f_2(x)g_2(x), \ldots, f_l(x)g_l(x))$$

elemanı tarafından üretilen tek üreteçli $n = ml$ uzunluğunda bir l-QC kod olsun. Bu durumda,

I) $\text{boy}(C) = m - \deg(\text{ebob}(g_1(x), \ldots, g_l(x)))$

Birimin m. ilkel kökü w olmak üzere w nin $g_i(x)$ in kökü olan en çok sayıdaki ardışık kuvvetlerinin sayısı a_i, $h_i(x) = \dfrac{x^m - 1}{g_i(x)}$

ve $G(x) = (f_1(x)g_1(x), \ldots, f_l(x)g_l(x))$ olsun.

II) $\mu = \min_{i=1}^{n} \{\deg(h_i(x))\}$ olmak üzere

$$\{G(x), xG(x), \ldots, x^{\mu-1}G(x)\}$$

tarafından üretilen C' kodun F deki boyutu μ ve minimum uzaklığı

$$d(C') \ge \sum_{i=1}^{l} (a_i + 1)$$

eşitsizliğini sağlar.

III) $\lambda = \max_{i=1}^{n} \{\deg(h_i(x))\}$ olmak üzere

$$\{G(x), xG(x), \ldots, x^{\lambda-1}G(x)\}$$

tarafından üretilen C'' kodun F deki boyutu λ ve minimum uzaklığı

$$d(C'') \ge \min_{i=1}^{l} \{a_i + 1\}$$

eşitsizliğini sağlar.

İspat: I) $F_q[x]$'te

$$\text{EKOK}(h_1(x), h_2(x), \ldots, h_l(x)) = H(x)$$

olsun. Her $i = 1, 2, \ldots, l$ için $(x^m - 1) \mid H(x)g_i(x)$ olur. Diğer yandan ise herhangi bir $p(x)$ ve $\deg(p(x)) < \deg(H(x))$ için $(x^m - 1) \nmid p(x)g_i(x)$. Yani,

$$p(x)(f_1(x)g_1(x), \ldots, f_l(x)g_l(x)) \neq 0.$$

Dolayısıyla,

$$\text{boy}(C) = \deg(H(x)) =$$

$$= m - \deg(\text{ebob}(g_1(x), g_2(x), \ldots, g_l(x)))$$

II) C kodunu ilk m koordinatı m uzunluğunda devirli bir kod olduğunu biliyoruz. Bu devirli kodun minimum ağırlığı Teorem III.2 ye göre en az $a_1 + 1$ dir. Benzer şekilde 2. m, 3.m, ..., l. m bloklarından elde edilen devirli kodların minimum uzaklıklar en az sırasıyla $a_2 + 1, \ldots, a_l + 1$ dir. C' kodu C nin bir alt kodu ve m bloklarından en az biri daima sıfırdan farklı olacağından istenen sonuç elde edilir.

III) C'' kodu yine C nin bir alt kodu ve sıfırdan farklı herhangi bir elemanın her bir m. bloku sıfırdan farklı olacağından Teorem III.2 e göre m. blokların her birinin Hamming ağırlığı en az $a_i + 1$ olacaktır.

Dolayısıyla, sıfırdan farklı olan bir kodsözün ağırlığı blokların ağırlıklarının toplamlarından fazladır.

Dikkat edildiğinde yukarıdaki teorem ile herhangi bir yarı devirli C kod için çok iyi bir alt sınır elde etme imkanı yoktur. Ancak, yarı devirli kodlar arasında özel bir aile için durum daha farklıdır:

Sonuç IV.1: $i = 1, 2, .., l$ için $g(x) \mid (x^m - 1)$ ve

$$\left(f_i(x), \frac{x^m - 1}{g(x)}\right) = 1 \text{ olsun. } C \text{ kodu}$$

$$(f_1(x)g(x), f_2(x)g(x), \ldots, f_l(x)g(x))$$

elemanı tarafından üreteçli $n = ml$ uzunluğunda bir l-QC kod olsun. Bu durumda,

I) $\text{boy}(C) = m - \deg(g(x))$ ve

II) birimin m. ilkel kökü w olmak üzere w nin $g(x)$ in kökü olan en çok sayıdaki ardışık kuvvetlerinin sayısı a ise

$$d(C) \geq l(a+1).$$

İspat: I) Yukarıdaki teoremde $l = 1$ alınırsa sonuca ulaşılır.

II) İlk m. blok ve diğer m. blokların hepsi $g(x)$ tarafından üretilen devirli kodlardır. C deki herhangi bir kodsözün sıfır olması için gerek ve yeter koşul her bir m. koordinatın sıfır olmasıdır. Dolayısıyla, sıfırdan farklı bir kodsözün her bir m. koordinatı sıfıra eşit değildir ve BCH alt sınırdan her bir m. blokun ağırlığı en az $a+1$ dir. Toplam l blok olduğundan C de sıfırdan farklı herhangi bir elemanın ağırlığı en az $l(a+1)$ dir.

Yukarıdaki Sonuç IV.1 i bir örnek üzerine uygulanışı görelim:

Örnek: $m = 28$ ve l=2 olsun. $n = 56$ uzunluğunda ve $k = 15$ boyutunda F_3 cismi üzerinde bir QC kod oluşturalım. $g(x) \mid x^{28} - 1$, $\deg(g(x)) = 13$ olacak şekilde bir $C = \langle (g(x), f_2(x)g(x)) \rangle$ QC kodu bulalım. 3 ün modülo 28 e göre çarpımsal mertebesi 6 olduğundan $x^{28} - 1$ polinomun K parçalanış cisminin F_3 üzerindeki boyutu 6 dır. $x^6 + x + 2$ polinomu F_3 üzerinde ilkel olduğundan, K parçalanış cismini $K = F_3[x]/(x^6 + x + 2)$ olarak alabiliriz. $cl_m(a)$ ile a nin devresel (cyclotomic) kalan sınıfını gösterelim:

$cl(1) = \{1,3,9,19,25,27\}$,

$cl(2) = \{2,6,10,18,22\}$,

$cl(4) = \{4,8,12,16,20,24\}$,

$cl(5) = \{5,11,13,15,17,23\}$, $cl(7) = \{7,21\}$ ve

$cl(14) = \{14\}$ bulunur.

$x^{28} - 1$ polinomunu bölen ve derecesi 13 e eşit olan $cl(1), cl(2), cl(4)$ ve $cl(5)$ içinden herhangi ikisi ile birlikte $cl(14)$ ten meydana gelen bir $g(x)$ polinomu oluşturalım. Bunun için tam 6 seçenek vardır. Bunların arasından birimin 28. ilkel kökü w nun kuvvetleri olan devresel kalan sınıflardan en yüksek ardışıklığı $T = cl(4) \cup cl(5) \cup cl(14)$ seçiminden elde edilir. Dolayısıyla,

$$g(x) = \prod_{i \in T} (x - w^i)$$

$$= x^{13} + x^{11} + 2x^{10} + x^8 + x^5 + 2x^3 + x^2 + 1$$

polinomu seçildiğinde, $g(x)$ in kökleri arasında w^i, $11 \leq i \leq 17$ da vardır. Yani, $g(x)$ in ardışık 7 tane kökü vardır.

$$f_2(x) = x^5 + x^7 + 2x^8 + 2x^{10} + x^{12} + x^{13}$$

olarak aldığımızda $\left(f_2(x), \frac{x^{28} - 1}{g(x)} \right) = 1$ olur ve $(g, f_2 g)$ tarafından üretilen kodun minimum uzaklığı Sonuç IV.1 den dolayı en az 16 olur. Gerçekte, [7] de gösterildiği gibi bu kodun esas minimum uzaklığı 23 tür ve bu parametrelere bağlı bilinen en iyi lineer kodtur.

Sonuç olarak yarı devirli kodların cebirsel yapıları çok zengin ve bilinmeyen yönleri çoktur. $s = 1$ için çalışmalar [2] de yapılmıştır. $s \geq 1$ için ise [3] ve [4] Gröbner baz yaklaşımı ile yarı devirli kodların yapıları anlaşılmaya çalışılmıştır. Ancak, $s > 1$ üreteçli yarı devirli kodların yapıları hakkında olgunlaşmış bir teori yoktur. Son zamanlarda [13] de yarı devirli kodların cebirsel yapıları incelenmiş ve bu kod ailesinin dualleri hakkında bilgi verilmiştir.

KAYNAKLAR

[1] F.J. MacWilliams and N.J. Sloane, *The Theory of Error Correcting Codes*, North Holland Pub. Co., 1977.

[2] G.E. Seguin and G. Drolet, *The Theory of 1-Generator Quasy-Cyclic Codes*, preprint 1990.

[3] K. Lally and P. Fitzpatrick, *Construction and Classification of Quasy-Cyclic Codes*, WCC 99, Workshop on Coding Theory and Cryptography, January, p.11-14, Paris.

[4] K. Lally and P. Fitzpatrick, *Algebraic Structure of Quasy-Cyclic Codes*, Discr. Appl. Math. Vol. 111, p. 157-175, 2001.

[5] Koshy Thomas, *Polynomial Approach to Quasy-Cyclic Codes*, Bul. Cal. Math. Soc.,69, p. 51-59, 1977.

[6] Nuh Aydın and İrfan Siap, *New Quasi-Cyclic Codes over GF(5)*, Appl. Math. Letters, 15, p. 833-836, 2002.

[7] İrfan Siap, Nuh Aydın and Dijen K. Ray-Chaudhuri, *New Ternary Quasi-Cyclic Codes with Better Minimum Distances*, IEEE Trans. Inform. Theory, vol 46, No. 4, p. 1554-1558, July 2000.

[8] İrfan Şiap, Generalized r-fold Weight Enumerators for Linear Codes and New Linear Codes with Improved Minimum Distances, Phd. Thesis, The Ohio State University, Columbus, December 1999.

[9] J. Conan and G. Seguin, *Structural Properties and Numeration of Quasi-Cyclic Codes*, AAECC, vol.4, p. 25-39, 1993.

[10]P.P. Greenough and R. Hill, *Optimal Ternary and Quasi-Cyclic Codes*, Des. Codes and Cryptogr., vol 2. P. 81-91, 1992.

[11]R.N. Daskalov, T.A. Gulliver and E. Metodieva, *New Good Quasi-Cyclic Ternary and Quaternary Linear Codes*, IEEE Trans. Inform. Theory, vol. 43, p. 1647-1650, Sept. 1997.

[12]S.E. Taraves, V.K. Bhargava and S.G.S. Shiva, *Some Best Rate* $p/(p+1)$ *Quasi-Cyclic Codes*, IEEE Trans. Inform. Theory, vol IT 20, p.133-135, Jan. 1974.

[13]San Ling and Patrick Sole, *On the Algebraic Structure of Quasi-Cyclic Codes I: Finite Fields*, IEEE Trans. Inform. Theory, vol. 47, No. 7, p.2751-2759, November 2001.

[14]T. Kasami, *A Gilbert-Varshamov Bound for Quasi-Cyclic Codes of Rate 1/2*, IEEE Trans. Inform. Theory, vol IT 20, p.679-680, Sept. 1974.