T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DNA KODLARININ CEBİRSEL YAPISI

YÜKSEK LİSANS TEZİ

Elif Segah ÖZTAŞ

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Tez Danışmanı	**:**	**Doç. Dr. Mehmet ÖZEN**

Haziran 2009

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DNA KODLARININ CEBİRSEL YAPISI

YÜKSEK LİSANS TEZİ

Elif Segah ÖZTAŞ

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 19 / 06 /2009 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Doç. Dr. Mehmet ÖZEN	**Prof. Dr. İrfan ŞİAP**	**Yrd. Doç. Dr. Metin YAMAN**
Jüri Başkanı	**Üye**	**Üye**

TEŞEKKÜR

Tezin hazırlanma aşamasında bana her türlü desteği veren danışman hocam Sayın Doç. Dr. Mehmet ÖZEN'e ve hayatım boyunca maddi manevi desteklerini esirgemeyen aileme teşekkür ediyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

$\mathbb{Z}$	: Tamsayılar kümesi
F_q	: q elemanlı sonlu bir cisim
$V(n,q)$	: Elemanları F_q den alınan n-lilerin kümesi
der f	: f polinomunun derecesi
C	: Kodsözlerin bulunduğu küme
d(C)	: Hamming metriğine göre C kodunun minimum uzaklığı
[n,k,d]	: n uzunluğunda, k boyutlu, d minimum uzaklığında bir lineer kod
KTS	: Kendine ters sıralı (reciprocal)
KTSE	: Kendine ters sıralısına eş (self-reciprocal)
ST	: Sıralı terslenebilen (reversible)

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Lineer kodlar, devirli kodlar, DNA kodlar.

Üç bölüm halinde düzenlenen bu çalışmanın birinci bölümünde gerekli cebirsel tanımlar, teoremler ve lineer kodlarla ilgili bilgiler verilmektedir.

İkinci bölümde DNA kodları hakkındaki temel tanım ve teoremler verildi. Ayrıca GF(4) üzerinde oluşturulmuş DNA kodları örneklendirildi.

Üçüncü bölümde ise GF(16) da toplamsal sıralı terslenebilen, tamamlanan ve sıralı terslenebilen-tamamlanan devirli kodlar inşa edildi ve bazı örnekler verildi.

ALGEBRAIC STRUCTURE OF DNA CODES

SUMMARY

Keywords: Linear codes, cyclic codes, DNA codes.

This study consists of three chapters. First chapter includes algebraic definitions, theorems and some information for linear codes.

In the second chapter, definition, theorems and examples in GF(4) about DNA codes are introduced.

In the third chapter, additive reversible, complement and reversible complement cyclic codes in GF(16) are built and some examples are worked out.

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar

Tanım 1.1.1: $K \neq \emptyset$ kümesinin elemanlarından oluşan her sıralı ikiliye K de bir ve yalnız bir eleman karşılık getiren bir fonksiyona K üzerinde bir ikili işlem denir. Bu işlem $*$ sembolü ile gösterildiğinde;

$$\mathrm{K} \times \mathrm{K} \rightarrow \mathrm{K}$$
$$(\mathrm{a},\mathrm{b}) \rightarrow \mathrm{a} * \mathrm{b}$$

ile tanımlanır.

Tanım 1.1.2: G bir küme ve $*$, G de tanımlı bir ikili işlem olsun. Eğer aşağıdaki özellikler * işlemi tarafından sağlanıyorsa (G, $*$) ikilisine bir grup denir.

i. $\forall a,b,c \in$ G için $(a*b)*c = a*(b*c)$

ii. $\forall a \in$ G için $a*e = e*a = a$ olacak biçimde e$\in$ G vardır.(e etkisiz eleman)

iii. $a \in$ G için $a * a^{'} = a^{'} * a$=e olacak biçimde $a^{'} \in$ G vardır.($a^{'}$, a'nın tersidir)

Ayrıca, $\forall a,b,c \in$ G için $a*b = b*a$ sağlanıyorsa G ye bir değişmeli (abelyen) grup denir.

Tanım 1.1.3: G bir grup $0 \neq H \subset G$ olsun. Eğer H, G deki işleme göre bir grupsa H'a G nin alt grubu denir.

Tanım 1.1.4: G bir grup $0 \neq H \subset G$ olsun. H nin bir alt grup olması için gerek ve yeter şart

S1: $\forall a, b \in H$ için $a.b \in H$ olmalı.

S2: $\forall a \in H$ için $a^{-1} \in H$ olmalıdır.

Önerme 1.1.1: Bir grubun bir takım alt gruplarının arakesiti da bir alt gruptur [1].

Tanım 1.1 5: M, G grubunun bir alt kümesi olsun. M yi kapsayan G nin bütün alt gruplarının arakesitine M nin ürettiği alt grup denir $\langle M \rangle$ şeklinde gösterilir. $\langle M \rangle$ nin elemanlarına grubun üreteçleri denir. Eğer M sonlu bir küme ise G de sonlu bir gruptur.

Eğer $M = \{a\}$ şeklinde tek elemanlı bir küme ise G ye a ile üretilmiş devirli grup denir ve $G = \langle a \rangle$ şeklinde gösterilir.

Tanım 1.1.6: R$\neq \emptyset$ kümesi üzerinde tanımlı iki ikili işlem '+' ve '.' olsun. Aşağıdaki koşulları sağlayan (R,+,.) cebirsel yapısına bir halka denir.

R_1: (R,+) bir değişmeli gruptur.

R_2: $\forall a, b, c \in R$ için $a(bc) = (ab)c$ (çarpmaya göre birleşme özelliği)

R_3: $\forall a, b, c \in R$ için

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

(çarpmanın sağdan ve soldan toplama üzerinde dağılma özelliği).

Tanım 1.1.7: R ve R' iki halka olsun. ψ :R$\rightarrow R'$ fonksiyonu;

i. birebir ve örten,

ii. $\forall$ a,b$\in$R, ψ(a+b) = ψ(a) + ψ(b) ve ψ(a.b) = ψ(a). ψ(b) (Homomorfizma)

koşullarını sağlarsa, ψ ye R den R' ne bir izomorfizma denir ve R$\cong$ R' ile gösterilir.

Tanım 1.1.8: Bir halkada çarpma işlemi değişmeli ise bu halkaya değişmeli halka denir. Bir R halkasında $\forall$ x$\in$R için $1.x = x.1 = x$ olacak biçimde 1 elemanı varsa R ye birimli halka denir.

Tanım 1.1.9: R birimli bir halka olsun. m$\in$R nin, R de tersi varsa m ye R nin bir tersinir (birimsel) elemanı denir.

Tanım 1.1.10: R değişmeli, birimli bir halka ve $\forall$ m$\in$R-{0} elemanı tersinir ise R ye bir cisim denir.

Tanım 1.1.11: R bir halka ve S $\subseteq$R olsun. S, R deki işlemlere göre bir halka ise S ye R nin bir alt halkası denir.

Tanım 1.1.12: $a,b \in R$ için a $\neq 0$ ve b $\neq 0$ olduğunda $ab = 0$ oluyorsa, a ve b ye R nin sıfır bölenleri denir. Eğer $\forall$ $a,b \in R$ için $ab = 0$ iken $a = 0$ veya $b = 0$ ise R ye sıfır bölensiz halka denir.

Teorem 1.1.1: $\mathbb{Z}_n$ halkasının sıfır bölenleri n ile aralarında asal olmayan elemanlardır [1].

Tanım 1.1.13: Bir R halkasında $\forall$ $a \in R$ için $na = 0$ sağlayan pozitif n tamsayılarının en küçüğüne halkanın karakteristiği denir ve $kar(R) = n$ ile gösterilir. Eğer böyle bir n tamsayısı yoksa R ye sıfır karakteristikli halka denir.

Tanım 1.1.14: R bir halka ve $\varnothing \neq$ I $\subseteq$R olsun. I alt kümesi

i. $\forall$ a,b$\in$I için a-b$\in$I
ii. $\forall$ a$\in$I ve $\forall$ r$\in$R için ra$\in$I veya ar$\in$I

özelliklerini sağlıyorsa I ya R nin bir ideali denir.

Tanım 1.1.15: Bir eleman tarafından üretilen ideallere temel idealler denir.

Tanım 1.1.16: R değişmeli ve birimli bir halka ve M de R nin (1) den farklı bir ideali olsun. R nin, M yi kapsayan M ve R den başka hiçbir ideali yoksa, M ye R nin bir maksimal ideali denir.

Önerme 1.1.2: Birimli ve değişmeli bir R halkasında [2]

M maksimal idealdir $\Leftrightarrow$ R/M cisimdir.

Tanım 1.1.17: R bir halka, x bir bilinmeyen ve $a_0, a_1, a_2, ..., a_n$ ler R nin elemanları olmak üzere,

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

şeklindeki bir ifadeye R den katsayılı bir polinom denir. R den katsayılı tüm polinomların kümesi R[x] ile gösterilir.

Önerme1.1.3: R bir halka ise R[x] de bir halkadır [2].

Önerme1.1.4: F bir cisim ve $f \in F[x],\ \mathrm{der} f \geq 1$ olsun. $(f) = f(x)F[x]$ temel ideali için $F[x]/(f)$ bölüm halkasının tam temsilciler sistemi $\mathrm{der}\, r < \mathrm{der} f$ olan $r \in F[x]$ polinomları şeklinde alınabilir [1].

Tanım 1.1.18: $(f(x), h(x)) = 1$ ise $f(x)$ ve $h(x)$ aralarında asaldır.

Tanım 1.1.19: $f(x) \in$ F[x] olsun. $f(x)$ polinomu F[x] içinde pozitif dereceli polinomların çarpımı olarak yazılabilirse $f(x)$, F[x]de çarpanlarına ayrılabilir denir.

$$f(x) = p(x)g(x)...s(x)$$

biçiminde ise $p(x), g(x),..., s(x)$ polinomlarına çarpan, $f(x) = p(x)g(x)...s(x)$ ifadesine de $f(x)$ polinomunun F[x] de çarpanlara ayrılışı denir.

Tanım 1.1.20: Bir cisim üzerinde tanımlanmış bir polinom çarpanlarına ayrılamıyorsa bu polinom indirgenemezdir.

Teorem 1.1.2: F[x] içindeki pozitif dereceli her polinomun bir indirgenemez çarpanlara ayrılışı vardır [1].

Teorem 1.1.3: $p(x), f(x),\ g(x) \in$ F[x] ve $p(x)$, F[x] de indirgenemez olsun. Buna göre,

$$p\ (x) \mid f(x).g(x)\ \ p(x) \mid f(x)\ veya\ p(x) \mid g(x)$$

dir [1].

Teorem 1.1.4: F[x] de bir $\langle p(x) \rangle \neq 0$ idealinin maksimal olması için gerek ve yeter şart p(x) in F üzerinde indirgenemez olmasıdır [1].

1.2. Lineer Kodlar

Tanım 1.2.1: $A = \{a_1,..., a_q\}$ sonlu bir küme olsun. Bu kümeye alfabe denir. A^n ise A kümesinden alınan n-lileri temsil etsin ve A^n in herhangi bir C alt kümesine q-lu blok kodu denir. C nin sözlerine kodsöz denir. Eğer $C \subset A^n$ nın M tane elemanı varsa, C'ye n uzunluğunda, M kodsözler (vektörler) elemanlı bir kod denir ve C ye kısaca (n,M)- kodu denir.

Tanım 1.2.2: x ve y aynı uzunlukta, aynı alfabe üzerinde tanımlanmış n-liler olsun. x ve y nin farklı bileşenlerinin sayısına Hamming uzaklığı denir ve $d(x, y)$ ile gösterilir. Yani, $x = (x_1, x_2,..., x_n)$ ve $y = (y_1, y_2,..., y_n)$ ise

$$d(x,y) = |\{i \mid x_i \neq y_i\}|$$

olur.

$$d(C) = \min_{c,d \in C, c \neq d} d(c,d)$$

ye de kodun minimum uzaklığı denir.

n uzunluğunda, M eleman sayısına sahip ve minimum uzaklığı d olan bir kod kısaca (n, M, d) - kodu ile gösterilir.

Teorem 1.2.1: A^n, A alfabesinden meydana gelen n-lilerin kümesi olsun. Hamming uzaklığı aşağıdaki özelliklere sahiptir. Her bir $x, y, z \in A^n$ için,

1. $d(x,y) \geq 0$ ve $d(x,y) = 0 \Leftrightarrow x = y$
2. $d(x,y) = d(y,x)$
3. $d(x,y) \leq d(x,z) + d(z,y)$

(A^n, d) ikilisi bir metrik uzaydır [3].

Tanım 1.2.3: $V(n,q)$, q elemanlı sonlu bir cisim olan F_q üzerinde tanımlanmış n uzunluğundaki vektör uzayı olsun. Eğer C kodu bir $V(n,q)$ vektör uzayın alt uzayı ise ($C \subset V(n,q)$) C koduna bir lineer kod denir. Eğer C nin $V(n,q)$ üzerindeki boyutu k ise C ye bir [n,k] kodu denir. C nin minimum mesafesi d ise C koduna bir [n,k,d] lineer kodu denir.

Teorem 1.2.2: C bir [n,k,d]- kodu ise C kodu tam t hata düzelten olması için gerek ve yeter koşul $d = 2t + 1$ veya $d = 2t + 2$ olacak şekilde bir $t \in \mathbb{Z}$ olmasıdır. C koduna t-hata düzelten kod denir [3].

Kodun minimum uzaklığı kodun hata düzeltme kabiliyetini vermektedir.

Bütün lineer kodlar $0 = (0...0)$ şeklinde gösterilen sıfır kodsözünü içerir. Ayrıca q-lı bir [n,k]-lineer kodun eleman sayısı M ve hızı R aşağıdaki gibidir:

$$M = q^k, R = \frac{k}{n}.$$

Tanım 1.2.4: Bir $c \in V(n,q)$ vektörünün, $w(c)$ ile gösterilen (Hamming) ağırlığı o vektörün sıfırdan farklı olan bileşenlerinin sayısına eşittir. Bir C kodunun minimum ağırlığı w(C) o kodun sıfırdan farklı vektörlerin, ağırlıklarının en küçüğüdür.

Lineer kodların önemli bir özelliği ise $d(C) = w(C)$ olmasıdır. Yani lineer bir kodun minimum uzaklığı minimum ağırlığa eşittir.

Tanım 1.2.5: C, n uzunluğunda bir kod olsun. C kodunda ağırlığı i olan kod sözlerin sayısı A_i olsun, yani

$$A_i = |\{c \mid w(c) = i, c \in C\}|$$

olmak üzere,

$$W_c(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)} = \sum_{i=1}^{n} A_i x^{n-i} y^i$$

polinomuna C kodunun Hamming ağırlık sayacı denir.

1.2.1. Lineer kodun üreteç matrisi

Bir lineer kod bir vektör uzay olduğundan, lineer kod vektör uzayın tabanı kullanılarak tanımlanabilir.

Tanım 1.2.1.1: C bir [n,k] kodu olsun. Satırları C nin bir tabanı olan k x n tipindeki D matrisine C kodunun üreteç matrisi denir.

Tanım 1.2.1.2: n uzunluğunda bir kodsöz oluşturulurken, k uzunluğundaki orijinal mesaja $n-k$ uzunluğunda kontrol biti eklenir. Böyle kodsözler sistematik şekildedir.

Teorem 1.2.1.1: C bir lineer [n,k] kodu olsun. Herhangi bir k koordinat yerleri verilsin, bu yerler üzerinde C ye denk olan sistematik bir kod vardır [3].

G=($I_k \,|$ A) formundaki G matrisine C kodunun standart form matrisi denir. Burada I_k , k boyutlu birim matristir.

1.2.2. Lineer kodun duali

$V(n,q)$ bir vektör uzay ve $u=\left(u_1,u_2,...,u_n\right), v=\left(v_1,v_2,...,v_n\right)\in V(n,q)$ olmak üzere u ile v nin iç çarpımı;

$$<u,v>=u_1v_1+...+u_nv_n$$

şeklinde tanımlanır.

Tanım 1.2.2.1: C bir [n,k] lineer kodu olsun.

$$C^{\perp}=\left\{x\in V(n,q):<x,c>=0\,,\forall c\in C\right\}$$

kümesine C nin dual kodu denir.

Teorem 1.2.2.1:

1) $G=(I_k \mid A)$ matrisi C kodu için bir üreteç matrisi ise

$$C^{\perp}=\left\{x\in V(n,q):<x,c>=0\,,\forall c\in C\right\}$$

olur [3].

2) Bir lineer [n,k] kodunun duali olan $C^{\perp}$ kodu da bir [n,n-k] lineer koddur.

3) Her lineer C kodu için $(C^{\perp})^{\perp} = C$ olur.

Eğer C [n,k] lineer kodunun üreteç matrisi k x n boyutlu G matrisinin standart formu G=($I_k \mid A$) ise $C^{\perp}$ in üreteç matrisi H=(- $A^T \mid I_{n-k}$) olur. H matrisine C kodun kontrol (parity check) matrisi de denir.

1.3. Sonlu Cisimler

Bu bölümde sonlu cisimlerle ilgili temel öğelere yer verilmektedir. DNA kodlarında kullanılan yapıların elemanları sonlu cisimlerden alınabilmektedir.

Teorem 1.3.1: F sonlu bir cisim ise F nin karakteristiği bir asal sayıdır. Eğer F nin karakteristiği p ise n bir pozitif sayı olmak üzere F nin p^n tane elmanı vardır [3].

Bu sonlu cisme aynı zamanda Galois cismi denir ve $q = p^n$ elemanlı bir Galois cismi $GF(p^n)$ ya da F_q ile gösterilir.

Tanım 1.3.1: p(x) polinomunun katsayıları $GF(q)$ nin elemanlarından oluşsun. $p(x)$ polinomunun katsayısı $GF(q)$ nin uygun bir elemanı ile çarpılarak $p(x)$ polinomunun baş katsayısı 1 yapılabilir. Bu durumda, $p(x)$ polinomuna monik polinom denir.

Tanım 1.3.2: Cismin tanımından $F^* = F - \{0\}$ çarpma işlemine göre bir gruptur. $|F| = q$ ise $|F^*| = q-1$ dir. ayrıca F^* bir grup olduğundan

$$\alpha \in F^* \Rightarrow \alpha^{q-1} = 1$$

yada

$$\alpha \in F \Rightarrow \alpha^q = \alpha.$$

Diğer bir deyişle, F cisminin her elemanı $f_q(x) = x^q - x$ polinomunun bir köküdür. Bu polinomun en fazla q tane kökü vardır.

F cisminin sıfırdan farklı elemanlarının kümesi olan F^* bir devirli gruptur.

$|F^*| = q-1$ ve α ise F^* ın mertebesi d olan bir elemanı olsun. Böylece $d \mid (q-1)$ dır. α tarafından üretilen devirli alt grup:

$$\langle \alpha \rangle = \{1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{d-1}\}$$

burada $\langle \alpha \rangle$ nın her bir elemanın mertebesi d'yi böler. O zaman $\langle \alpha \rangle$ nın tüm kökleri $x^d - 1$ polinomunun kökleridir. Bu polinomun F de en fazla d tane farklı kökü olabilir. O halde $x^d - 1$ in tüm kökleri kümesi $\langle \alpha \rangle$ dır.

Tanım 1.3.3: F_q^* u devirli üreten her hangi bir F_q^* elemanına F_q nun bir ilkel (primitif) elemanı denir.

Sonlu bir cismi temsil etmede şu iki yol kullanılır: Bunlardan birinde, $p(x)$ indirgenemez bir polinom olmak üzere $F[x]/p(x)$ bölüm halkası kullanılır. İkincisi ise F_q^* in bir devirli grup olması nedeniyle, F_q un tüm elemanlarını, bir ilkel elemanın kuvveti olarak temsil edilmesidir. Cisimleri birinci ifade yolu ile oluşturulan kodlar, ikinci ve üçüncü bölümde kullanılmaktadır.

$p(x), F_q[x]$ üzerinde indirgenemeyen bir polinom olduğunda

$$K = F(x)/(p(x))$$

bölüm halkası bir cisimdir. $p(x)$ in derecesi d ise $K = F_{q^d}$ olur. F_{q^d} cismi çarpma ve toplama işleminin modülo p(x) e göre yapıldığı polinomlar cümlesi ile temsil edilebilir:

$$F_{q^d} = \frac{F(x)}{(p(x))} = \{r(x) + (p(x)) \mid \deg(r(x) < d\}.$$

Örnek 1.3.1: Sekiz elemanlı bir cisim oluşturulsun.

$p(x) = x^3 + x + 1$ polinomu $F_2[x]$ cismi üzerinde indirgenemez bir polinomdur.

$$F_2[x] \big/ x^3 + x + 1$$

bir cisim olur.

$\alpha \in F$ ve $p(a) = 0$ ise

$$\alpha^3 + \alpha + 1 = 0$$

dir.

$$\begin{array}{ll} \alpha^0 = 1 & \alpha^4 = \alpha + \alpha^2 \\ \alpha = \alpha & \alpha^5 = \alpha^2 + \alpha^3 = \alpha^2 + \alpha + 1 \\ \alpha^2 = \alpha^2 & \alpha^6 = \alpha^3 + \alpha^2 + \alpha = 1 + \alpha^2 \\ \alpha^3 = 1 + \alpha & \alpha^7 = 1 \end{array}$$

cismimiz şu şekilde gösterilir:

$$GF(8) = F_{2^3} = F_8 = \{0, 1, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}.$$

1.4. Devirli Kodlar

Tanım 1.4.1: $V(n,q)$, bileşenleri F_q cisminden olan, n-lilerden oluşan vektör uzayıdır.

Tanım 1.4.2: $C \subset V(n,q)$ lineer kodu için, eğer

$$c_0c_1...c_{n-1} \in C \text{ iken } c_{n-1}c_0c_1...c_{n-2} \in C$$

oluyorsa bu lineer koda bir devirli kod denir.

F_q üzerinde derecesi en fazla n-1 olan polinomlar ile $V(n,q)$ vektör uzayı arasında bir izomorfizma kurulabilir. $R_n = F_q[x]/\langle x^n - 1\rangle$ olmak üzere

$$\Phi : V(n,q) \to R_n$$

$$\Phi((c_0, c_1, ..., c_{n-1})) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$$

şeklinde tanımlanan Φ fonksiyonu $V(n,q)$ ile R_n arasında bir izomorfizmadır.
Eğer C

$$R_n = \frac{F_q[x]}{\langle x^n - 1\rangle}$$

halkasının bir ideali ise C bir devirli kod olur.

R_n, F_q üzerinde derecesi n den küçük olan tüm polinomların kümesidir. R_n de toplama polinomların toplamı ve çarpma da polinomların çarpımıdır. Tüm işlemler $x^n - 1$ kalanına göre olacaktır. Eğer

$$c_0c_1...c_{n-1} \to c_{n-1}c_0c_1...c_{n-2}$$

devirli öteleme (shift) altında C lineer kodu kapalı ise devirli koddur. Bu durumda ise C bütün sağ ötelemeler altında kapalıdır. Yani

$$c_0c_1...c_{n-1} \to c_k...c_{n-1}c_0c_1...c_{k-1}$$

olur. Bu sağ ötelemesi uygulanırken son terim başa gelir.

1.4.1. Devirli kodun üreteç polinomu

Teorem 1.4.1.1: C, R_n de bir ideal olsun. Bu durumda C, n uzunluğunda bir devirli kod olur [3].

1) C de derecesi minimum olan tek bir monik polinom $(g(x))$ vardır. Bu polinom $\mathrm{C} = \langle g(x) \rangle$ şeklinde C yi üretir ve bu polinoma C nin üreteç polinomu denir.

2) Üreteç polinomu olan $g(x)$, x^n -1 i böler.

3) Eğer $\mathrm{der}(g(x)) = r$ ise C'nin boyutu n - r olur. Yani

$$C = \langle g(x) \rangle = \{r(x)g(x): \ \mathrm{der}(r(x)) < n - r\}$$

dir.

4) Eğer $g(x) = g_0 + g_1x + \cdots + g_rx^r$ ise bu durumda $g_0 \neq 0$ ve C nin üreteç matrisi

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{pmatrix}$$

olur.

1.4.2. Devirli kodun kontrol polinomu

Eğer $g(x)$ polinomu R_n de bir [n,n-r] devirli kodunun üreteç polinomu ise $g(x)$, x^n -1 i böler. Yani

$$x^n\text{-}1 = g(x)h(x)$$

olur. Burada $h(x)$ derecesi n-r olan bir polinomdur ve bu polinoma C nin kontrol polinomu denir.

Teorem 1.4.2.1: $h(x)$, R_n de C devirli kodunun kontrol polinomu olsun.

1) C kodu;

$$C = \{\, p(x) \in R_n :\ p(x)h(x) \equiv 0 \mod x^n - 1 \}$$

şeklinde tanımlanır.

2) Eğer $h(x) = h_0 + h_1 x + \cdots + h_{n-r} x^{n-r}$ ise bu durumda C'nin kontrol matrisi

$$H = \begin{pmatrix} h_{n-r} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & h_0 & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & h_0 \end{pmatrix}$$

olur.

3) C nin diki olan $C^{\perp}$ kodunun boyutu r dir ve C devirlidir. $C^{\perp}$ devirli kodunun üreteç polinomu ise

$$h^{\perp} = h_0^{-1} x^{n-r} h(x^{-1}) = h_0^{-1}(h_0 x^{n-r} + h_1 x^{n-r-1} + \cdots + h_{n-r})$$

şeklindedir [3].

Lineer kodlar ve devirli kodlar ile ilgili daha detaylı bilgi için [4]'e bakılabilir.

BÖLÜM 2. DNA KODLARI

DNA hesaplamaları 1994 te Leonard Adleman'ın, test tüpündeki DNA moleküllerinin işlenmesinde, Hamilton yolu gibi zor sayısal problemleri çözmesiyle başlamıştır [5]. Çünkü tipik test tüpündeki büyük DNA moleküllerinin sayısı ile DNA esaslı herhangi bir sayısal metot arasında büyük bir paralellik olduğu görülür. Bu paralellik DNA nın kimyasal yapısına uygun koşullarla sınırlandırılır.

DNA (deoksiribo nükleik asit) A (adenin), G(guanin), C(sitozin) ve T(timin) denilen, dört bazın farklı şekillerde birleşmesiyle oluşur. Çift sarmal şeklinde bir yapısı vardır. Bu sarmal yapı karşılıklı gelen ve üzerinde A,G,C,T bazları bulunan iki zincirden oluşur.

n uzunluğundaki bir DNA zinciri için mümkün olan olasılık 4^n kadardır.1 gr DNA da 2.1 x 10^{21} tane bazdan oluşur. Her baz iki bit olarak kodlanır. Dolayısıyla 1 gr DNA için 4.2 x 10^{21} tane bit olduğu söylenebilir. Ama günümüz teknolojileri en fazla 10^9 adet bit barındırabiliyor.

[6] ve [7] de DNA kodları, minimum uzaklığı d olan Hamming koşulu, sıralı terslenebilen-tamamlanan (reversible-complement) koşulu, sıralı terslenebilen (ST) koşulu, sabit GC-miktarı (fixed GC-content) şeklinde dört farklı koşul ele alınmıştır. GC-miktar koşulu benzer erime sıcaklıklarını elde etmek için kullanılır [7]. Çünkü DNA da A ile T arasında iki, G ile C arasında üç hidrojen bağı bulunmaktadır. Dolayısıyla, içerisinde G ya da C bazı bulunan DNA ları ayırmak için yüksek erime sıcaklıklarına ihtiyaç duyulmaktadır. [8] de ise bazı sonlu halkalarda, devirli kodlar, dual tamamlanan devirli kodlar, tamamlanan devirli kodlar da incelenmekte ve kodların DNA yapısıyla benzer yapıda olduğu ifade edilmektedir. [9] da ise devirli DNA kodların nasıl üretildiği verilmektedir. [10] da DNA kod yapıları için GF(4) te devirli kodlar kullanılmakta ama yazar çalışmasını sadece lineer sıralı terslenebilen

(ST) devirli kodlarla sınırlandırmaktadır.

GF(4) te belirtilen toplamsal devirli (additive cyclic) ve ST-tamamlanan (reversible-complement) kod yapılarının, DNA kodların yapısı için yapılan açıklama ve örnekler bu bölümde verilmektedir.

2.1. Temel Bilgiler

DNA, {A, T, G, C} harflerinin sıralanmasıyla tanımlanan bir zincirden oluşmaktadır. Burada n uzunluğundaki sıralı bir DNA kodunun kodsöz kümesi $u_i \in \{A, C, T, G\}$ olmak üzere $(u_0, u_1 \ldots u_{n-1})$ şeklinde tanımlanır. {A, T, G, C} kodlarını $\overline{w} = w^2, w^2 + w + 1 = 0$ (dolayısıyla $w^2 = w + 1$) olmak üzere $GF(4) = \{0, 1, w, w^2\}$ ile $A \to 0, G \to \overline{w}, C \to w$ ve $T \to 1$ olacak şekilde eşleştirebilir. ([8] de ise şu şekilde bir eşleştirme uygulanmıştır: $A \to 0, G \to 1, C \to u$ ve $T \to 1 + u$).

Watson-Crick tamamlayıcısı (complement) DNA zincirinde karşılıklı gelen bazları tanımlar ve $A^c = T, T^c = A, C^c = G, G^c = C$ şeklinde ifade edilir. Her bir $u = (u_0, u_1, \ldots, u_{n-1})$ kodsözü için u nun sıralı tersi (reverse) $u^r = (u_{n-1}, u_{n-2}, \ldots u_0)$, u nun tamamlayıcısı (complement) $u^c = (u_0^c, u_1^c, \ldots, u_{n-1}^c)$ ve ST-tamamlayıcısı $u^{rc} = (u_{n-1}^c, \ldots, u_0^c)$ şeklinde gösterilir.

u' ve u'' kodsözleri arasındaki Hamming uzaklığı $d(u', u'')$ şeklinde gösterilir. n uzunluğunda, k boyutlu, GF(4) deki C(n, 2^k) toplamsal kodu $GF(4)^n$ in toplamsal bir alt grubudur. Eğer C k boyutlu $GF(4)^n$ ve sıfır olmayan minimum Hamming uzaklığı d ise bu koda “lineer” kod denir ve C[n,k,d] ile gösterilir. GF(4) teki C lineer koduna, eğer $(u_0, \ldots, u_{n-1}) \in C$ ve $(u_{n-1}, u_0, \ldots, u_{n-2}) \in C$ şeklindeki eşleme sağlanıyorsa, devirli (cyclic) kod denir. Her bir $(u_0, \ldots, u_{n-1})$ kodsözü $u(x) = u_0 + u_1 x + \ldots + u_{n-1} x^{n-1}$ şeklinde bir polinom ile eşleştirilir. Bu durumda devirli kodlar $GF(4)[x]/(x^n - 1)$ halkasında idealdirler.

GF(4) te ki bir C kodunun tam Hamming ağırlık sayacı aşağıdaki gibi gösterilir:

$n_a(c)$, c kodsözündeki a bileşenlerinin sayısını belirtir.

$$CWE_C(x,y,z,t)=\sum_{c\in C} x^{n_0(c)} y^{n_1(c)} z^{n_w(c)} t^{n_{\overline{w}}(c)}$$

GF(4) te ki bir C kodunun GC-ağırlık sayacı, C deki $\{0,1\}$ ve $\{w,w^2\}$ in sayısını hesaplayan bir polinom oluşturur. Yani, 0 ve 1 ler x olarak , w ve w^2 ler y olarak sayılmaktadır.

$$GCW_C(x,y)=CWE_C(x,x,y,y)$$

şeklinde gösterilir.

Tanım 2.1.1 F bir cisim, $F_q \subset F_{q^r}=F$ ise

$$tr=tr_{q^r|q}:F\rightarrow F_q$$

olacak şekilde iz (trace) fonksiyonu aşağıdaki gibi tanımlanır.

$$tr(x)=x+x^q+x^{q^2}+\ldots+x^{q^{r-1}}$$

Dolayısıyla $GF(4)$ için kullanılacak iz fonksiyonu aşağıdaki gibidir [11].

$$Tr:GF(4)\rightarrow GF(2) \text{ olmak üzere}$$

$$Tr(x)=x+x^2$$

olur.

$$Tr(0)=Tr(1)=0 \text{ ve } Tr(w)=Tr(\overline{w})=1$$

olur. Birbirinin tamlayıcısı olan bazların iz fonksiyonu sonuçları aynıdır.

$p_r \neq 0$ için her bir $p(x) = p_0 + p_1 x + \ldots + p_r x^r$ polinomunun kendine ters sıralısı (KTS, reciprocal) $p^*(x) = x^r p(1/x) = p_r + p_{r-1} x + \ldots + p_0 x^r$ olarak tanımlanır. Şunu belirtelim ki, $\deg p^*(x) \leq \deg p(x)$ ve $p_0 \neq 0$ ise, $p(x)$ ve $p^*(x)$ genellikle aynı dereceye sahiptiler. Eğer $p(x) = p^*(x)$ ise p(x) e kendine ters sıralısına eş (KTSE, self-reciprocal) denir.

Tanım 2.1.2: C, GF(4) te, n uzunluğunda bir lineer kod olsun. Her $u \in C$ için $u^r \in C$ ise C sıralı-terslenebilen (reversible) denir.

Tanım 2.1.3: C, GF(4) de, n uzunluğunda bir lineer koddur. Her $u \in C$ için $u^c \in C$ ise C ye tamamlanan (complemet) dır denir.

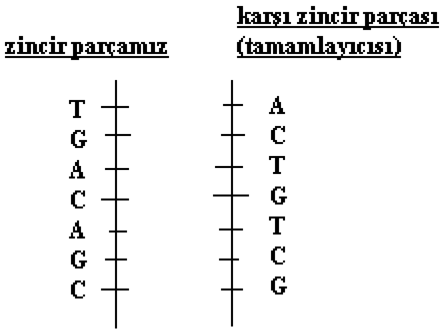
Tanım 2.1.4: Minimum uzaklığı d olan C lineer (toplamsal) kodu,

(1) C devirli ise,
(2) C sıralı-terslenebilen (reversible) ise,
(3) C tamamlanan (complement) ise

C ye ST-tamamlanan (reversible-complement) devirli kod denir.

Örnek 2.1.1: Bu örnekte bir DNA zincir parçasının yukarıdaki tanımlara göre nasıl ifade edildiği gösterilmektedir.

TGACAGC DNA parçasının bir zinciri olsun .
Bu zincirin tamamlayıcısı, yani karşı zinciri Şekil 2.1 deki gibidir.



Şekil 2.1. Bir DNA zincir parçası ve karşı zinciri

Yani, TGACAGC nin tamamlayıcısı ACTGTCG olur. Bu seçilen DNA parçası $GF(4)=\{0,1,w,w^2\}$ elemanları ile ifade edilerek yazılırsa TGACAGC $(1,w^2,0,w,0,w^2,w)$ kodsözü şeklinde gösterilir. Eğer $u=(1,w^2,0,w,0,w^2,w)$ denilirse, u kodsözünün tamamlayıcısı $u^c=(0,w,1,w^2,1,w,w^2)$ şeklinde gösterilir. $u^c=(0,w,1,w^2,1,w,w^2)$ kodsözü ACTGTCG e karşılık gelen kodsözdür.

TGACAGC nin sıralı tersi CGACAGT olur ve $u^r=(w,w^2,0,w,0,w^2,1)$ kodsözü şeklinde ifade edilir.
TGACAGC nin ST-tamamlayıcısı GCTGTCA olur ve $u^{rc}=(w^2,w,0,c,0,w^2,1)$ şeklinde ifade edilir.

TGACAGC polinom şeklinde gösterilirse, $u=(1,w^2,0,w,0,w^2,w)$ olduğundan, $u(x)=1+w^2x+wx^3+w^2x^5+wx^6$ olur.

Teorem 2.1.1: C, GF(4) te $(n,2^k)$ toplamsal devirli kod olsun. $C=\langle wp(x)+q(x),r(x)\rangle$ şeklindedir. p(x), r(x) ikili (binary, katsayıları $\mathbb{Z}_2$ den oluşan) polinomdurlar ve bunlar (x^n-1) (mod 2) i böler. r(x) $q(x)(x^n-1)/p(x)(\bmod 2)$ yi böler ve $k=2n-\deg p-\deg r$ dir [12].

İspat: İz fonksiyonu göz önünde bulundurularak $Tr : C \to \mathbb{Z}_2[x] \big/ x^n - 1$ eşleştirmesi kullanılır. Bu eşlemede kodun ikili devirli kısmını üreten $\langle r(x) \rangle$ tektir ve $r(x)$ $x^n - 1$ i böler. Kodun bu eşleşmeye göre görüntüsünü üreten $\langle p(x) \rangle$ dir. Orijinal kod $r(x)$ ve $p(x)$ in bazı ters görüntüleriyle, $wp(x) + q(x)$ gibi, üretilir. Eğer $r(x)$ $q(x)(x^n - 1)/p(x)$ i bölmez ise $((x^n - 1)/p(x))(wp(x) + q(x))$ C nin ikili vektörleri olan $\langle r(x) \rangle$ içinde olmaz. Bu bir çelişkidir.

Örnek 2.1.2:

$$\begin{aligned} C_1 = \{&000, 1ww^2, w^2 1w, ww^2 1, 1w^2 w, w1w^2, w^2 w1, 011, \\ &101, 110, w^2 0w^2, w^2 w^2 0, 0w^2 w^2, ww0, 0ww, w0w\} \end{aligned}$$

şeklindeki 3 uzunluğundaki bir kodun $r(x), p(x), q(x)$ aşağıdaki şekildedir.

$$\text{Tr: } C_1 \to C_2$$

$$Tr(x) = x + x^2$$

olmak üzere C_1 kodun Tr(x) fonksiyonu altındaki görüntüsü Tablo 2.1 deki gibidir.

Tablo 2.1. Kodun iz fonksiyon karşılığı

$$
\begin{gathered}
000 \rightarrow 000 \\
1ww^2 \rightarrow 011 \\
w^2 1w \rightarrow 101 \\
ww^2 1 \rightarrow 110 \\
1w^2 w \rightarrow 011 \\
w1w^2 \rightarrow 101 \\
w^2 w1 \rightarrow 110 \\
011 \rightarrow 000 \\
101 \rightarrow 000 \\
110 \rightarrow 000 \\
w^2 0w^2 \rightarrow 101 \\
w^2 w^2 0 \rightarrow 110 \\
0w^2 w^2 \rightarrow 011 \\
ww0 \rightarrow 110 \\
0ww \rightarrow 011 \\
w0w \rightarrow 101.
\end{gathered}
$$

Burada C_1 kodunun ikili (110,011,101,000) kısmını üreten $r(x)$ dir. Dolayısıyla $r(x) = 1 + x$ olur. $Tr(C_1) = C_2$ yi üreten ise $p(x) = 1 + x$ dir.

$$
\begin{aligned}
1 + wx + w^2x^2 &= 1 + wx + (w+1)x^2 \\
&= 1 + wx + wx^2 + x^2 \\
&= w(x + x^2) + x + x^2
\end{aligned}
$$

$$
\begin{aligned}
&\Rightarrow x^2[w(x + x^2) + x + x^2] \\
&\Rightarrow w(\underbrace{1 + x}_{p(x)}) + \underbrace{x + x^2}_{q(x)}
\end{aligned}
$$

$$
\begin{aligned}
&\text{der}\, p = 1 \\
&\text{der}\, q = 2 \\
&\quad k = 2n - \text{der}\, p - \text{der}\, r \\
&\quad\ = 2.3 - 1 - 1 \\
&\quad\ = 4.
\end{aligned}
$$

$p(x), r(x)$ ve $q(x)$ polinomları Teorem 2.1.1 deki özellikleri taşımaktadır.

Örnek 2.1.3: $C = \langle wp(x) + q(x), r(x) \rangle$ de $p(x) = 1, r(x) = 1 + x^2 + x^3 + x^4$ ve $q(x) = 1 + x^2 + x^3$ şeklinde olduğunda aşağıdaki kodsözler üretilir. $p(x), r(x)$ ve $q(x)$ polinomları Teorem 2.1.1 i sağlamaktadır. Bu kodun elemanları olan kodsözler aşağıda verilmiştir.

(0, 0, 0, 0, 0), (w, 0, 1, 1, 0), (0, w, 0, 1, 1),
(1, 0, w, 0, 1), (1, 1, 0, w, 0), (0, 1, 1, 0, w),
(w, w, 1, 0, 1), (w^2, 0, w^2, 1, 1), (w^2, 1, 1, w^2, 0),
(w, 1, 0, 1, w), (1, w, w, 1, 0) (1, w^2, 0, w^2, 1),
(0, w^2, 1, 1, w^2), (0, 1, w, w, 1), (1, 1, w^2, 0, w^2),
(1, 0, 1, w, w), (w^2, w, w^2, 0, 0), (w^2, w^2, 1, w, 1),
(w, w^2, 0, 0, w^2), (w, 1, w^2, w^2, 1), (w^2, 1, w, 1, w^2),
(w^2, 0, 0, w^2, w), (0, w^2, w, w^2, 0), (1, w^2, w^2, 1, w),

(1, w, 1, w^2, w^2), (0, 0, w^2, w, w^2), (w, w^2, w^2, w, 0),
(w^2, w^2, w, 0, w), (w^2, w, 0, w, w^2), (w, 0, w, w^2, w^2),
(0, w, w^2, w^2, w), (w, w, w, w, w), (1, 1, 1, 1, 1),
(w^2, 1, 0, 0, 1), (1, w^2, 1, 0, 0), (0, 1, w^2, 1, 0),
(0, 0, 1, w^2, 1), (1, 0, 0, 1, w^2), (w^2, w^2, 0, 1, 0),
(w, 1, w, 0, 0), (w, 0, 0, w, 1), (w^2, 0, 1, 0, w^2),
(0, w^2, w^2, 0, 1), (0, w, 1, w, 0), (1, w, 0, 0, w),
(1, 0, w^2, w^2, 0), (0, 0, w, 1, w), (0, 1, 0, w^2, w^2),
(w, w^2, w, 1, 1), (w, w, 0, w^2, 0), (w^2, w, 1, 1, w),
(w^2, 0, w, w, 0), (w, 0, w^2, 0, w), (w, 1, 1, w, w^2),
(1, w, w^2, w, 1), (0, w, w, 0, w^2), (0, w^2, 0, w, w),
(1, 1, w, w^2, w), (w^2, w, w, w^2, 1), (w, w, w^2, 1, w^2),
(w, w^2, 1, w^2, w), (w^2, 1, w^2, w, w), (1, w^2, w, w, w^2) ,
(w^2, w^2, w^2, w^2, w^2)

$f_1(x), f_2(x) \in F_2[x] / (x^n - 1)$ ve herhangi iki polinom olmak üzere;

$$C = \langle wp(x) + q(x), r(x) \rangle \text{ olduğundan}$$

$$c(x) = [wp(x) + q(x)] f_1(x) + r(x) f_2(x) \text{ olur.}$$

Eğer $p(x) = 0$ ise $q(x) = 0$ ve $k = n - \operatorname{der} r$ olur. Benzer şekilde, eğer $r(x) = 0$ ise $k = n - \operatorname{der} p$ olur.

Teorem 2.1.2: Farz edelim ki $C = \langle r(x) \rangle$ şeklinde $GF(4)$ te lineer devirli bir kod olsun. C nin ST olması için gerek ve yeter koşul $r(x)$ polinomunun KTSE olmasıdır [13].

Lemma 2.1.1: $f(x)$ ve $g(x)$ $GF(4)[x]$ teki herhangi iki polinom ve $\operatorname{der} f(x) \geq \operatorname{der} g(x)$ olsun [14].

1. $[f(x)g(x)]^* = f(x)^* g(x)^*$
2. $[f(x) + g(x)]^* = f(x)^* + x^{\operatorname{der} f - \operatorname{der} g} g(x)^*$

olur.

2.2. GF(4) Deki Sıralı Terslenebilen Tamamlanan Devirli Kodlar

GF(4) deki ST-tamamlanan devirli kodlar, aşağıdaki koşulları sağladığı için önemli kodlardır.

1) Hamming koşulu : x ve w herhangi iki kodsöz olduğunda $d(w, x) \geq d$ dir.
2) ST-tamamlanan koşulu : x ve w (w ve x eşit olabilir) herhangi iki kodsöz $d(w^c, x^r) \geq d$ olur.

Lemma 2.2.1: $GF(4)[x]/(x^n-1)$ de $g_1(x), g_2(x)$ ve $g_3(x)$ polinomları x^n-1 polinomunu bölen, sıfırdan farklı, polinomlar ve $x^n-1=g_1(x)g_2(x)g_3(x)$ ise aşağıdaki durumlar gerçeklenir [14].

1. Eğer $g_1(x)$ ve $g_2(x)$ KTSE ise $g_1(x)g_2(x)$ KTSE olur.
2. $g_1(x)$ ve $g_2(x)$ den sadece bir tanesi KTSE ise $g_1(x)g_2(x)$ KTSE değildir.
3. Eğer $g_1(x)$ ve $g_2(x)$ KTSE değilse $g_1(x)g_2(x)$ de KTSE olabilir.

İspat: $GF(4)[x]/(x^n-1)$ de $g_1(x), g_2(x)$ ve $g_3(x)$ x^n-1 i bölen, sıfırdan farklı, polinomlar olmak üzere $x^n-1=g_1(x)g_2(x)g_3(x)$ olsun.

1. Farz edelim ki $g_1(x)$ ve $g_2(x)$ KTSE olsun. $[g_1(x)g_2(x)]^*=g_1(x)^*g_2(x)^*=g_1(x)g_2(x)$ olduğu görülür.

2. $g_1(x)$ KTSE olsun ve $g_2(x)$ KTSE olmasın. Farz edelim ki $GF(4)[x]/x^n-1$ te $g_1(x)g_2(x)$ KTSE olsun.

$$
\begin{aligned}
g_1(x)g_2(x) &= [g_1(x)g_2(x)]^* \\
&= g_1(x)^* g_2(x)^* \\
&= g_1(x)g_2(x)^* \\
&\Rightarrow g_1[g_2-g_2^*]=0=x^n-1
\end{aligned}
$$

bu bir çelişkidir. Dolayısıyla $GF(4)[x]/x^n-1$ de $g_1(x)g_2(x)$ KTSE değildir.

3. $GF(4)$ te $g_1(x)=x+w^2$ ve $g_2(x)=x^2+x+w$ x^n-1 i böler. $g_1(x)$ ve $g_2(x)$ nin KTSE olmadığı aşikardır. Ayrıca $g_1(x)g_2(x)=x^3+x+wx^2+1$ olur ve bu da KTSE değildir. Bir diğer şekilde, $g_1(x)=x+w^2$ ve $g_2(x)=x+w$ olacak şekilde seçersek. $g_1(x)$ ve $g_2(x)$ KTSE değildir. Ama $g_1(x)g_2(x)=x^2+x+1$ KTSE olur.

Teorem 2.2.1: Farz edelim ki $C = \langle r(x) \rangle$, $GF(4)$ te toplamsal devirli bir kod olsun. C nin ST olması için gerek ve yeter koşul $r(x)$ polinomunun KTSE olmasıdır [14].

2.3. $n = 7$ Uzunluğunda Toplamsal Sıralı Terslenebilen -Tamamlanan Devirli Kodlar

Kodlar farklı uzunluklarda oluşturulabilmektedir.[14] te daha önce bilinen 9,11,13 uzunluğunda kodların, aynı Hamming uzaklığına sahip olacak şekilde, daha çok kodsöz üretildiği gösterilmektedir. [14] ve [15] te daha önce 7 uzunluğunda olan kodlardan en iyisi elde edildiği gösterilmektedir. Yazdığımız örneklerde 7 uzunluğunda kodlar kullanılmaktadır.

Şimdiye kadar, $GF(4)$ te 7 uzunluğunda 29 tane ST-tamamlanan kod bulunmaktadır. Bunlardan bazıları 180, 208 ([16]) ve en son 256 tane kodsöz içeren kod bulunmaktadır ([14],[15]). d=3 olan bu kodlardan 256 elemana sahip olarak bulunan kodlar aşağıdaki gibidir.

$$C_1 = \left\langle w + \left(x^4 + x^3\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$$
$$C_2 = \left\langle w + \left(x^4 + x^3 + 1\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$$
$$C_3 = \left\langle w + \left(x^5 + x^2\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$$
$$C_4 = \left\langle w + \left(x^5 + x^4 + x^3 + x^2\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$$
$$C_5 = \left\langle w + \left(x^5 + x^2 + 1\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$$
$$C_6 = \left\langle w + \left(x^5 + x^4 + x^3 + x^2 + x + 1\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$$

C_2, C_3, C_4, C_5 kodları, GC-miktarı ile, DNA kod yapısının en iyi terimlerini içermektedir. Tüm kodlar aynı GC-ağırlık sayacı fonksiyonu tarafından verilir.

$$GCW(x,y) = [70x^3y^4 + 14x^6y + 70x^4y^3 + 42x^5y^2 + 42x^2y^5 + 14xy^6 + 2x^7 + 2y^7]$$

C_2, C_4 ve C_5 aynı $CWE_C(x,y,z,t)$ e sahiptir, bunlar aşağıdaki gibidir:

$$CWE_C(x,y,z,t)=\begin{bmatrix} y^7+x^7+7x^2y^2z^3+7x^2z^2t^3+7y^2z^3t^2+7x^2z^3t^2 \\ +7y^2z^2t^3+7x^2yt^4+7xy^2z^4+7xy^4t^2+7x^4yz^2 \\ +7x^2y^3t^2+t^7+7x^3y^2z^2+7x^4y^2t+7x^2y^4z \\ +21x^2y^2z^2t+21x^2y^2zt^2+7x^3y^2t^2+7x^2y^3z^2 \\ +7x^2y^2t^3+z^7+7x^2z^4t+7yz^4t^2+7xz^2t^4 \\ +7x^3z^2t^2+7y^3z^2t^2+21xy^2z^2t^2+7y^2zt^4 \\ +7x^4zt^2+7y^4z^2t+21x^2yz^2t^2 \end{bmatrix}$$

C_3 kodun ise sahip olduğu $CWE_C(x,y,z,t)$ aşağıdaki gibidir:

$$CWE_C(x,y,z,t)=\begin{bmatrix} y^7+7y^2z^4t+7x^2zt^4+x^7+7x^2y^2z^3 \\ +7x^2y^3t^2+7x^3y^2z^2+7y^2z^2t^3+7x^2z^3t^2 \\ +7y^4zt^2+t^7+21x^2y^2z^2t+21x^2y^2zt^2 \\ +7x^4z^2t+z^7+7x^3y^2t^2+7x^2y^3z^2 \\ +7x^2y^2t^3+7xy^4z^2+7x^4yt^2+7x^4y^2z \\ +7x^2y^4t+7xz^4t^2+7x^2yz^4+7xy^2t^4 \\ +7x^3z^2t^2+7y^3z^2t^2+21xy^2z^2t^2 \\ +7yz^2t^4+21x^2yz^2t^2+7y^2z^3t^2+7x^2z^2t^3 \end{bmatrix}$$

C_3 ve C_5 in kodsözleri Örnek 1 (Bkz.. sf. 41) ve Örnek 2. (Bkz. sf. 46) de verilmiştir. Örnekler Mathematica programı kullanılarak gösterildiğinden ve bu kısma eklenemediğinden en sonda toplu olarak verilmektedir.

BÖLÜM 3. GF(16) DA KODLAR

Bu bölümde GF(16) cisminin elemanlarını kullanarak toplamsal ST-tamamlanan devirli, toplamsal tamamlanan devirli ve toplamsal ST devirli kodlar elde edildi. Bölüm iki de kullanılan GF(4) cisminin elemanları, DNA nın dört bazı (A,T,G,C), ile eşleştirilmişti. Bu bölümde ise bazlar ikişer ikişer alınıp GF(16) daki elemanlar ile eşleştirildi.

GF(16) aşağıdaki gibi oluşturulur. $x^{15}-1$ $\mathbb{Z}_2$ de çarpanlarına aşağıdaki gibi ayrılmaktadır.

$$x^{15}-1=(1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

$f(x)=1+x+x^4$ indirgenemez bir polinomdur. $F_2[x]\big/\left(x^4+x+1\right)$ şeklinde olan bölüm halkası sonlu cisim olur.

$$GF(16)=F_{2^4}=F_2[x]\big/\left(x^4+x+1\right)$$

olur. Bu cismin 16 elemanı aşağıdaki gibi üretilir.

$f(u)=0$ ise
$u^4+u+1=0$ ve $u^4=u+1$ dir.

Elemanların elde edilişi Tablo 3.1. de ayrıntılı verilmektedir.

Tablo 3.1. GF(16) cisminin elemanlarının ifadesi

$$
\begin{aligned}
u^0 &= 1 \\
u^1 &= u \\
u^2 &= u^2 \\
u^3 &= u^3 \\
u^4 &= u+1 \\
u^5 &= u^2+u \\
u^6 &= u^3+u^2 \\
u^7 &= u^3+u+1 \\
u^8 &= u^2+1 \\
u^9 &= u^3+u \\
u^{10} &= u^2+u+1 \\
u^{11} &= u^3+u^2+u \\
u^{12} &= u^3+u^2+u+1 \\
u^{13} &= u^3+u^2+1 \\
u^{14} &= u^3+1.
\end{aligned}
$$

Bunlar $GF(16)=\{0,1,u^1,u^2,u^3,u^4,u^5,u^6,u^7,u^8,u^9,u^{10},u^{11},u^{12},u^{13},u^{14}\}$ şeklinde ifade edilebilen cismin elemanlarıdır.

Her çift baz Tablo 3.2 deki gibi eşleştirildi.

Tablo 3.2. GF(16) elemanlarının karşılık geldiği baz çiftleri

$$
\begin{aligned}
&0 \to AA \\
&1 \to TT \\
&u \to AG \\
&u^2 \to AC \\
&u^3 \to AT \\
&u^4 \to TC \\
&u^5 \to GA \\
&u^6 \to GC \\
&u^7 \to GT \\
&u^8 \to TG \\
&u^9 \to CA \\
&u^{10} \to CT \\
&u^{11} \to GG \\
&u^{12} \to CC \\
&u^{13} \to CG \\
&u^{14} \to TA
\end{aligned}
$$

bu tabloda da görüldüğü gibi birbirinin tamamlayanı olan elemanların toplamı 1 olur. Yani bir elemanın tamamlayanını bulmak için eleman1 ile toplanır.

$$a^c = a + 1$$

Mesela, CA bazının tamamlayanı (Watson-Crick tamamlayanına göre) GT olmaktadır. GF(16)'da $u^9 \to CA$ ve $u^9 = u^3 + u$ tür. CA nın tamamlayanı bulmak için u^9 a 1 eklenir. $u^9 + 1 = u^3 + u + 1 = u^7$ olur ve $u^7 \to GT$ olur.

Baz çiftleri ve GF(16) nın elemanları değişik şekillerde de eşleştirilebilir ama birbirini tamamlayanların toplamı için belirlenen şartı (biz burada $a^c = a + 1$ olacak şekilde seçtik) sağlayacak şekilde olmalıdır.

GF(16) da kullanılan iz fonksiyonu, iz fonksiyonunun tanımından, aşağıdaki gibi olacaktır.

$$tr(x) = x^8 + x^4 + x^2 + x$$

Bu iz fonksiyonuna göre, her elemanın iz fonksiyonu karşılığı Mathematica programı ile aşağıdaki gibi hesaplanır. Elemanların karşılığı Tablo 3.3 deki gibidir.

İz fonksiyonu (Mathematica'da) hesaplaması:

```
i = {0, 1, u, u^2, u^3, 1 + u, u^2 + u, u^3 + u^2 ,
    u^3 + u + 1, u^2 + 1, u^3 + u, u^2 + u + 1,
    u^3 + u^2 + u, u^3 + u^2 + u + 1, u^3 + u^2 + 1,
    u^3 + 1}
```

$\{0,\ 1,\ u,\ u^2,\ u^3,\ 1+u,\ u+u^2,\ u^2+u^3,$
$1+u+u^3,\ 1+u^2,\ u+u^3,\ 1+u+u^2,$
$u+u^2+u^3,\ 1+u+u^2+u^3,\ 1+u^2+u^3,\ 1+u^3\}$

```
CoefficientList[
  Expand[i^8 + i^4 + i^2 + i] /. u^4 → 1 + u /.
                        u^5 → u^2 + u /.
                      u^6 → u^3 + u^2 /.
                    u^7 → u^3 + u + 1 /.
                  u^8 → u^2 + 1 /. u^9 → u^3 + u /.
              u^10 → u^2 + u + 1 /. u^11 → u^3 + u^2 + u
           /. u^12 → u^3 + u^2 + u + 1
           /. u^13 → u^3 + u^2 + 1
           /. u^14 → u^3 + 1 /. u^16 → u /.
       u^24 → u^9 /. u^9 → u^3 + u
  , Modulus → 2]
```

{0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1}

Tablo 3.3. GF(16) da elemanların iz fonksiyon sonuçları

eleman	$tr(x)$	*baz çifti*
0	0	*AA*
1	0	*TT*
u	0	*AG*
u^2	0	*AC*
u^3	1	*AT*
u^4	0	*TC*
u^5	0	*GA*
u^6	1	*GC*
u^7	1	*GT*
u^8	0	*TG*
u^9	1	*CA*
u^{10}	0	*CT*
u^{11}	1	*GG*
u^{12}	1	*CC*
u^{13}	1	*CG*
u^{14}	1	*TA*

Birbirini tamamlayanı olan elemanların iz fonksiyon sonuçları aynı olacak şekilde, elemanlar baz çiftleriyle eşleştirilir. Mesela, CT nin tamamlayanı GA dır ve ikisinin de tr(x) sonucu 0 dır.

Tanım 3.1.: C, GF(16) te, n uzunluğunda bir lineer (toplamsal) koddur. Her $u \in C$ için $u^{r} \in C$ ise C ST dir denir.

Tanım 3.2: C, GF(4) de, n uzunluğunda bir lineer (toplamsal) koddur. Her $u \in C$ için $u^{c} \in C$ ise C ye tamamlanandır denir.

3.1. GF(16) da Toplamsal Tamamlanan Devirli Kodlar

Önerme 3.1.1: $GF(16)$ te $C=\langle h(x), r(x)\rangle$ n uzunluğunda toplamsal devirli bir kod ve $h(x)$ herhangi bir polinom olsun. $r(x)=1+x+...+x^{n-1}$ ise C kodu tamamlanan koddur.

İspat: $a^c=a+1$ ve $r(x)=1+x+...+x^{n-1}$ olduğundan C kodu tamamlanan olacaktır.

Örnek 4. (Bkz. sf. 56) te
$C=\langle u^6+(u^5x^2+u^7x^3+u^9x^4+u^{12}x^5),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle$ tamamlanan kodunun sonuçları verilmektedir ve $d=5$ olmaktadır.

3.2. GF(16) da Toplamsal Sıralı Terslenebilen Devirli Kodlar

Sonlu cisimlerde aşağıdaki önermenin doğruluğu bilinmektedir.

Önerme 3.2.1: GF(16) da, $C=\langle g(x)\rangle$ bir devirli kod olsun. g(x) polinomu KTSE ise C bir ST kod olur.

Önerme 3.2.1 için Örnek 5 (Bkz. sf. 61)i inceleyiniz. g(x) in durumuna göre bir kodun 2 kere üretilmesi mümkün. 7 uzunluğunda yaptığımız örneklerde, eğer g(x) in KTS'sı alındığında kendine dönüşen eleman var ise kodsözler tek olmakta. Eğer tüm elemanlar farklı elemanlara dönüşüyorsa her kodsözden 2 tane bulunabilmektedir.
Mesela $g(x)=u^7+u^6x+u^6x^4+u^7x^5$ olduğunda KTS'sı $g(x)^*=x^5g(\frac{1}{x})=u^7x^5+u^6x^4+u^6x+u^7$ olur. u^7 ve u^7x^5, u^6x ve u^6x^4 birbirilerine dönüşmektedir. Bu kodda bir kodsözden 2 tane bulunmakladır. $g(x)=u^{12}+u^8x^2+u^{12}x^4$ alınırsa $g(x)^*=u^{12}x^4+u^8x^2+u^{12}$ olmaktadır. $u^{12}x^4$ ve u^{12} birbirlerine dönüşmekte, u^8x^2 ise kendine dönüşmektedir. Bu kodda kodsözler tektir.

C kodunun kodsözleri yazılırsa tekrar eden kodlar sadece bir kez yazılır, 2. kez tekrar kod yazılmaz.

3.3. GF(16) da Toplamsal Sıralı Terslenebilen Tamamlanan Devirli Kodlar

Tanım 3.3.1: $q(x)$ n uzunluğundaki C kodunun bir kodsözünün polinom olarak ifadesi olsun. Eğer her bx^i (b sabit terim) $q(x)$ in bir terimi iken bx^{n-i} de $q(x)$ in bir terimi ise $q(x)$ 'e eş terimli polinom denir.

Mesela, 7 uzunluğunda bir C kodunun ST özelliği kazanması için q(x) polinomunu şu şekilde seçeriz: $q(x)=1+x+x^3+x^4$ olsun, ama bu $q(x)$ oluşturulacak C koduna ST özelliği vermez. Çünkü x in kuvveti olan 1 i 7 den çıkardığımızda 6 yı buluruz ve verilen q(x) te x^6 bulunmamaktadır. q(x) e x^6 eklenmelidir.

Teorem 2.1.1 [12] den faydalanarak aşağıdaki önerme yazılabilir.

Önerme 3.3.1 $GF(16)$ te $C=\langle u^i+q(x), r(x)\rangle$ (i = 0….14) toplamsal devirli bir kod olduğuna göre, bu kodun toplamsal ST-tamamlanan devirli kod olabilmesi için, $q(x)$, $r(x)$ ikili (binary) polinomlardır, r(x), $q(x)(x^n-1) \pmod 2$ yi böler ve $k=2n-\deg r$ olur. Aynı zamanda $r(x)=1+x+...+x^{n-1}$ dir ve $q(x)$ eş terimlidir.

İspat: $GF(16)$ te $C=\langle u^i+q(x), r(x)\rangle$ (i = 0….14) toplamsal devirli bir kod.

$u^i+q(x)=u^m+x^j+x^{n-j}+x^s+x^{n-s}$ olsun. $m=0,1,...,14$ ve $j<s, s<\dfrac{n}{2}$.

$$\begin{aligned}(u^i+q(x))^* &= (u^m+x^j+x^{n-j}+x^s+x^{n-s})^* \\ &= u^m x^{n-j}+x^{n-2j}+1+x^{n-j-s}+x^{-j+s} \\ &= x^{n-j}(u^m+x^{-j}+x^{j-n}+x^{-s}+x^{s-n}) \qquad x^k=x^{k+n} \text{ olduğundan} \\ &= x^{n-j}(u^m+x^{n-j}+x^j+x^{n-s}+x^s). \qquad (3.1)\end{aligned}$$

$f(x)$ ve $g(x)$ herhangi iki polinom. $\text{der}(u^i+q(x))f(x)=a,\ r(x)=1+x+...+x^{n-1}$

olduğundan der$r(x)g(x)=n-1$ ve $n-1\geq a$ olur.

$$\begin{aligned}[(u^i+q(x))f(x)+r(x)g(x)]^* &= x^{n-1-a}[(u^i+q(x))f(x)]^*+[r(x)g(x)]^* \\ &= x^{n-1-a}(u^i+q(x))^* f(x)^*+r(x)^* g(x)^* \qquad r(x)^*=r(x) \text{ ve (3.1) den} \\ &= x^{n-1-a}(u^i+q(x))^* f(x)^*+r(x)g(x)^* \in C.\end{aligned}$$

Dolayısıyla C toplamsal ST kod olur. $a\in GF(16)$ olmak üzere, $a^c=a+1$ dir. $r(x)=1+x+...+x^{n-1}$ olarak seçildiğinden C kodunun tamamlayıcı kodlar kısmını üretmektedir. Sonuç olarak C toplamsal devirli ST- tamamlanan bir kod olur.

Aşağıdaki kodların 256 elemanı olduğu hesaplandı. Bu kodlar toplamsal ST-tamamlanan devirli kodlardır.

$C_1=\langle u^i+(x+x^2+x^5+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_2=\langle u^i+(1+x+x^2+x^5+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_3=\langle u^i+(x^3+x^4),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_4=\langle u^i+(1+x^3+x^4),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_5=\langle u^i+(x+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_6=\langle u^i+(1+x+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_7=\langle u^i+(x^2+x^5),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_8=\langle u^i+(1+x^2+x^5),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_9=\langle u^i+(x+x^2+x^3+x^4+x^5+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=2$

$C_{10}=\langle u^i+(1+x+x^2+x^3+x^4+x^5+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=2$

$C_{11}=\langle u^i+(x^2+x^3+x^4+x^5),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_{12}=\langle u^i+(1+x^2+x^3+x^4+x^5),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_{13}=\langle u^i+(x+x^3+x^4+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C_{14}=\langle u^i+(1+x+x^3+x^4+x^6),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle \quad d=3$

$C=\langle u^6+(x^2+x^3+x^4+x^5),(1+x+x^2+x^3+x^4+x^5+x^6)\rangle$ ST-tamamlanan kodunun sonuçları Örnek.3 (Bkz. sf. 51)te verilmektedir ve $d = 3$ olmaktadır.

Yukarıdaki Önerme 3.2.1 faydalanarak şöyle söyleyebiliriz; Eğer $C = \langle g(x), r(x) \rangle$ şeklinde toplamsal devirli bir kodsözde, g(x) KTSE ve $r(x) = 1 + x + ... + x^{n-1}$ ise bu kod toplamsal ST-tamamlanan devirli olur (kendini 2 kez tekrar eden kodlar sayılmazsa).

GF(16) da oluşturulan kodlar DNA zincirinin parçaları ile eşleştirildiğinde; toplamsal ST-tamamlanan devirli ve toplamsal ST devirli kodlarda, şöyle bir durumla karşılaşılmaktadır: DNA kodu AA CG GC TC GA TC olsun. Bunun GF(16) daki uygulamaya göre sıralı tersi TC GA TC GC CG AA şeklinde olmaktadır.

Bu DNA zincir parçası AACGGCTCGATC nin GF(4) teki sıralı tersi CTAGCTCGGCAA şeklinde olmakta fakat GF(16) da bu şekilde olamamaktadır. Bu nedenle GF(16) da oluşturulan toplamsal ST-tamamlanan devirli ve ST devirli kodlar için bir çevirici polinom belirledik. Bu polinom GF(16) deki baz çiftlerini (AG gibi) ters çevirerek GF(4)'de ki gibi AACGGCTCGATC nin sıralı tersi CTAGCTCGGCAA yi GF(16)'da elde edilmesini sağlar.

GF(16) nı her elemanı için çevirici elemanlar aşağıdaki Tablo 3.4'te gösterilmektedir.

Tablo 3.4. Çevirici elemanlar

baz çifti	$GF(16)$ daki karşılığı	çevirici	GF(16)daki kaşılığı	*tersi*
AA	0	0	0	AA
TT	1	0	1	TT
GG	u^{11}	0	u^{11}	GG
CC	u^{12}	0	u^{12}	CC
AT	u^{3}	1	u^{14}	TA
GC	u^{6}	1	u^{13}	CG
AG	u	u^{2}	u^{5}	GA
TC	u^{4}	u^{2}	u^{10}	CT
AC	u^{2}	u^{11}	u^{9}	CA
GT	u^{7}	u^{11}	u^{8}	TG

Bir koddaki her eleman kendi çeviricisini belirler.

Çevrilmiş olan kodsözler u^z ile gösterilsin. Çevirici kodsöz $z=(u_0,...u_{n-1})$ ve çevirici polinom $z(x)=u_0+u_1x+...+u_{n-1}x^{n-1}$ dir. Bir ST C kodunda $u \in C$ ise $u^r \in C$ dir ve u nun DNA bazlarına çevrilmiş halinin ters dizilimi $u^{rz} \in C$ dir.

Tanım 3.3.1: C, GF(16) da, ST (veya ST-tamamlanan) devirli kod olsun. $u \in C$ ve $u^{rz} \in C$ ise C ye (DNA bazlarına göre) tam-ST denir.

Örnek 3.3.1: C, GF(16) da, bir toplamsal tam-ST bir kod olsun. $u_1=(0,u^{13},u^6,u^4,u^5,u^4)$ $u_1 \in C$ olsun. C ST olduğundan $u_1^r \in C$ dir. $u_1^r=(u^4,u^5,u^4,u^6,u^{13},0)$ olacaktır. Bu kodsözlerin DNA bazları ile ifadesi aşağıdaki gibidir.

$$u_1=(0,u^{13},u^6,u^4,u^5,u^4)=\text{AA CG GC TC GA TC}$$
$$u_1^r=(u^4,u^5,u^4,u^6,u^{13},0)=\text{TC GA TC GC CG AA}$$

u_1 in çevirici kodsözü $z_{u_1}=(0,1,1,u^2,u^2,u^2)$ dır. polinom olarak gösterirsek

$z_{u_1} = x + x^2 + u^2x^3 + u^2x^4 + u^2x^5$ olur.

$$u_1 + z_{u_1} = u_1^z = (0, u^6, u^{13}, u^{10}, u, u^{10})$$

u_1^r nin çeviricisi $z_{u_1^r} = (u^2, u^2, u^2, 1, 1, 0)$ olur ve polinom olarak $z_{u_1^r}(x) = u^2 + u^2x + u^2x^2 + x^3 + x^4$ şeklinde yazılmaktadır.

$u_1^r + z_{u_1^r} = u_1^{rz} = (u^{10}, u, u^{10}, u^{13}, u^6, 0)$ olur.

$$u_1^z = (0, u^6, u^{13}, u^{10}, u, u^{10}) = \text{ AA GC CG CT AG CT}$$
$$u_1^{rz} = (u^{10}, u, u^{10}, u^{13}, u^6, 0) = \text{ CT AG CT CG GC AA}$$

dır.

u_1 in DNA baz eşlemesine göre tam ters dizilimi u_1^{rz} nin DNA bazlarına eşlenmiş haline eşittir. u_1^r nin DNA baz eşlemesine göre tam ST'si u_1^z dir. $u_1^z, u_1^{rz} \in C$ dir.

GF(16) da ST veya tamamlanan devirli kodlarda çevirici $z(x)$ in eklenmesi kodun eleman sayısını artırabilmektedir.

Toplamsal ST devirli koda çevirici eklendiğinde

$$C = \langle g(x); z(x) \rangle = \langle g(x) \rangle \cup \langle g(x) \rangle^z$$

şeklinde ifade edilir.

Toplamsal ST-tamamlanan devirli koda çevirici eklendiğinde

$$C = \langle g(x), r(x); z(x) \rangle = \langle g(x), r(x) \rangle \cup \langle g(x), r(x) \rangle^z$$

veya

$$C=\left\langle u^{i}+q(x),r(x);z(x)\right\rangle=\left\langle u^{i}+q(x),r(x)\right\rangle\cup\left\langle u^{i}+q(x),r(x)\right\rangle^{z}$$

şeklinde gösterilmektedir.

BÖLÜM 4. ÖRNEKLER

Örneklerin sonuçları Mathematica programı ile hesaplanmıştır. Verilen kodların oluşturacağı kodsözler gösterilmektedir.

Örnek 1: $C_3 = \left\langle w + \left(x^2 + x^5\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$ GF(4)'te

$\left(i = f(x) \in {F_2[x]}\big/{(x^7 - 1)} \right)$

Örnek 2: $C_5 = \left\langle w + \left(x^5 + x^2 + 1\right), x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \right\rangle$ GF(4)'te

Örnek 3: $C = \left\langle u^6 + (x^2 + x^3 + x^4 + x^5), (1 + x + x^2 + x^3 + x^4 + x^5 + x^6) \right\rangle$ GF(16)'da

Örnek 4: $C = \left\langle u^6 + (u^5 x^2 + u^7 x^3 + u^9 x^4 + u^{12} x^5), (1 + x + x^2 + x^3 + x^4 + x^5 + x^6) \right\rangle$ GF(16)'da

Örnek 5: g(x) polinomları KTSE seçilip farklı şekillerde örneklendirilmektedir. Aynı kodsözden iki tane üretebilen kodlardan bazıları verilmektedir. Basit olarak, bu tür kodlar iki tane (0000000) kodsözü içermektedir. Sırasıyla, $C = \left\langle u^7 + u^6 x + u^6 x^4 + u^7 x^5 \right\rangle$, $C = \left\langle u^{12} + u^8 x^2 + u^{12} x^4 \right\rangle$, $C = \left\langle u^3 + u^6 x + u^6 x^2 + u^3 x^3 \right\rangle$ kodları incelenmektedir.

Örnek 1 :

$$C_3 = (w + (x^2 + x^5), (1 + x + x^2 + x^3 + x^4 + x^5 + x^6))$$

kodunun elemanları aşağıdaki gibidir.

```
PadRight[CoefficientList[
    Expand[i * (w + x^2 + x^5)] /. w^2 + 1 → w /.
                      x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
               x^10 → x^3 /. x^11 → x^4 /.
          x^12 → x^5 /. x^13 → x^6 /. x^14 → x^7,
   x, Modulus → 2], {128, 7}]
```

```
PadRight[
  CoefficientList[
    Expand[i * (w + x^2 + x^5) +
                      (1 + x + x^2 + x^3 + x^4 + x^
                            5 + x^6)] /. w^2 + 1 → w /.
                x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
          x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
     x^13 → x^6 /. x^14 → x^7, x, Modulus → 2],
  {128, 7}]
```

(0, 0, 0, 0, 0, 0, 0), (w, 0, 1, 0, 0, 1, 0), (0, w, 0, 1, 0, 0, 1),
(1, 0, w, 0, 1, 0, 0), (0, 1, 0, w, 0, 1, 0), (0, 0, 1, 0, w, 0, 1),
(1, 0, 0, 1, 0, w, 0), (0, 1, 0, 0, 1, 0, w), (w, w, 1, 1, 0, 1, 1),
(1, w, w, 1, 1, 0, 1), (1, 1, w, w, 1, 1, 0), (0, 1, 1, w, w, 1, 1),
(1, 0, 1, 1, w, w, 1), (1, 1, 0, 1, 1, w, w),
(w^2, 0, w^2, 0, 1, 1, 0), (w, 1, 1, w, 0, 0, 0),
(w, 0, 0, 0, w, 1, 1), (w^2, 0, 1, 1, 0, w^2, 0),
(w, 1, 1, 0, 1, 1, w), (0, w^2, 0, 1, 1, 0, w^2),
(1, 1, w, 0, 0, 0, w), (0, 0, 0, w, 1, 1, w),
(0, 1, 1, 0, w^2, 0, w^2), (1, 1, 0, w^2, 0, w^2, 0),
(1, 0, w^2, 0, w^2, 0, 1), (0, w^2, 0, w^2, 0, 1, 1),
(0, w, 1, 1, w, 0, 0), (1, w, 0, 0, 0, w, 1), (0, 0, w, 1, 1, w, 0),
(w^2, w, w^2, 1, 1, 1, 1), (w, w^2, 1, w^2, 0, 0, 1),
(w, w, 0, 1, w, 1, 0), (w^2, w, 1, 0, 0, w^2, 1),
(w, w^2, 1, 1, 1, 1, w^2), (w^2, 1, w^2, w, 1, 0, 0),
(w^2, 0, w, 0, w^2, 1, 1), (w, 0, w^2, 1, 1, w^2, 0),
(w^2, 1, w^2, 0, 0, 1, w), (w, 1, 0, w, w, 0, 1),
(w^2, 1, 1, w^2, 0, w, 0), (w, 0, 1, w, 1, 0, w),
(w^2, 0, 0, 1, w, w^2, 1), (w, 1, 0, 0, w^2, 1, w^2),
(w^2, 1, 1, 1, 1, w^2, w), (1, w^2, w, w^2, 1, 1, 1),
(1, w, w^2, 1, w^2, 0, 0), (0, w, w, 0, 1, w, 1),
(1, w^2, w, 1, 0, 0, w^2), (0, w^2, 1, w^2, w, 1, 0),
(1, w^2, 0, w, 0, w^2, 1), (0, w, 0, w^2, 1, 1, w^2),
(1, w, 1, 0, w, w, 0), (0, w^2, 1, 1, w^2, 0, w),
(1, w^2, 0, 0, 1, w, w^2), (1, 1, 1, 1, w^2, w, w^2),
(1, 0, 0, w^2, 1, w^2, w), (0, 0, 1, w, w^2, 1, w^2),
(1, 1, 1, w^2, w, w^2, 1), (0, 1, w, 1, 0, w, w),
(1, 1, w^2, 0, w, 0, w^2), (0, 0, w^2, 1, w^2, w, 1),
(1, 0, w, w, 0, 1, w), (0, 1, w, w^2, 1, w^2, 0),
(1, 1, w^2, w, w^2, 1, 1), (w^2, w^2, w^2, w^2, 1, 0, 1),
(w^2, w, w, 1, w^2, 1, 0), (w, w, w^2, 0, 1, w^2, 1),
(w^2, w^2, w^2, 1, 0, 1, w^2), (w, w^2, 0, w^2, w, 0, 0),
(w^2, w^2, 1, w, 0, w, 1), (w, w, 1, w^2, 1, 0, w^2),
(w^2, w, 0, 0, w, w^2, 0), (w, w^2, 0, 1, w^2, 1, w),
(w^2, w^2, 1, 0, 1, w^2, w^2), (w^2, 1, w, w, w^2, 0, 1),
(w, 1, w^2, w^2, 1, w, 0), (w^2, 0, w^2, w, 0, 0, w),
(w, 0, w, 1, w^2, w^2, 1), (w^2, 1, w, 0, w, 1, w^2),
(w, 1, w^2, 1, 0, w^2, w), (w^2, 1, 0, w^2, w, w, 1),
(w, 0, 0, w, w^2, 0, w^2), (w^2, 0, 1, w^2, 1, w, w),

$(w^2, 1, 0, 1, w^2, w^2, w^2), (1, w^2, w^2, w^2, w^2, 1, 0),$
$(0, w^2, w, w, 1, w^2, 1), (1, w, w, w^2, 0, 1, w^2),$
$(0, w, w^2, 0, w^2, w, 0), (1, w^2, w^2, 1, w, 0, w),$
$(0, w^2, w, 0, 0, w, w^2), (1, w^2, 1, w, w, w^2, 0),$
$(0, w, 1, w^2, w^2, 1, w), (1, w, 0, w, 1, w^2, w^2),$
$(1, w^2, 1, 0, w^2, w, w), (0, 1, w^2, w^2, w^2, w^2, 1),$
$(1, 0, w^2, w, w, 1, w^2), (0, 0, w, w^2, 0, w^2, w),$
$(0, 1, w^2, 1, w, w, w^2), (1, 0, 1, w^2, w^2, w^2, w^2),$
$(w^2, w^2, w, w^2, w^2, 0, 0), (w, w^2, w^2, w, 1, w, 1),$
$(w^2, w, w^2, w^2, 0, 0, w^2), (w, w, w, 0, w^2, w^2, 0),$
$(w^2, w^2, w, 1, w, 1, w), (w, w^2, w^2, 0, 0, w^2, w^2),$
$(w^2, w^2, 0, w, w, w, 0), (w, w, 0, w^2, w^2, 0, w),$
$(w^2, w, 1, w, 1, w, w^2), (w^2, w^2, 0, 0, w^2, w^2, w),$
$(w, 1, w, w^2, w^2, w, 1), (w^2, 0, w, w, w, 0, w^2),$
$(w, 0, w^2, w^2, 0, w, w), (w, 1, w, 1, w, w^2, w^2),$
$(w^2, 0, 0, w^2, w^2, w, w^2), (0, w^2, w^2, w, w^2, w^2, 0),$
$(1, w, w^2, w^2, w, 1, w), (0, w, w, w, 0, w^2, w^2),$
$(0, w^2, w^2, 0, w, w, w), (1, w, 1, w, w^2, w^2, w),$
$(0, 0, w^2, w^2, w, w^2, w^2), (w, w^2, w, w, w^2, w, 0),$
$(w^2, w, w, w^2, w, 0, w), (w, w, w^2, w, 0, w, w^2),$
$(w, w^2, w, 0, w, w^2, w), (w^2, w, 0, w, w^2, w, w),$
$(w, 0, w, w^2, w, w, w^2), (0, w, w^2, w, w, w^2, w),$
$(w, w, w, w, w, w, w), (1, 1, 1, 1, 1, 1, 1),$
$(w^2, 1, 0, 1, 1, 0, 1), (1, w^2, 1, 0, 1, 1, 0),$
$(0, 1, w^2, 1, 0, 1, 1), (1, 0, 1, w^2, 1, 0, 1),$
$(1, 1, 0, 1, w^2, 1, 0), (0, 1, 1, 0, 1, w^2, 1),$
$(1, 0, 1, 1, 0, 1, w^2), (w^2, w^2, 0, 0, 1, 0, 0),$
$(0, w^2, w^2, 0, 0, 1, 0), (0, 0, w^2, w^2, 0, 0, 1),$
$(1, 0, 0, w^2, w^2, 0, 0), (0, 1, 0, 0, w^2, w^2, 0),$
$(0, 0, 1, 0, 0, w^2, w^2), (w, 1, w, 1, 0, 0, 1),$
$(w^2, 0, 0, w^2, 1, 1, 1), (w^2, 1, 1, 1, w^2, 0, 0),$
$(w, 1, 0, 0, 1, w, 1), (w^2, 0, 0, 1, 0, 0, w^2),$
$(1, w, 1, 0, 0, 1, w), (0, 0, w^2, 1, 1, 1, w^2),$
$(1, 1, 1, w^2, 0, 0, w^2), (1, 0, 0, 1, w, 1, w),$
$(0, 0, 1, w, 1, w, 1), (0, 1, w, 1, w, 1, 0), (1, w, 1, w, 1, 0, 0),$
$(1, w^2, 0, 0, w^2, 1, 1), (0, w^2, 1, 1, 1, w^2, 0),$
$(1, 1, w^2, 0, 0, w^2, 1), (w, w^2, w, 0, 0, 0, 0),$
$(w^2, w, 0, w, 1, 1, 0), (w^2, w^2, 1, 0, w^2, 0, 1),$
$(w, w^2, 0, 1, 1, w, 0), (w^2, w, 0, 0, 0, 0, w),$
$(w, 0, w, w^2, 0, 1, 1), (w, 1, w^2, 1, w, 0, 0),$

$(w^2, 1, w, 0, 0, w, 1), (w, 0, w, 1, 1, 0, w^2),$
$(w^2, 0, 1, w^2, w^2, 1, 0), (w, 0, 0, w, 1, w^2, 1),$
$(w^2, 1, 0, w^2, 0, 1, w^2), (w, 1, 1, 0, w^2, w, 0),$
$(w^2, 0, 1, 1, w, 0, w), (w, 0, 0, 0, 0, w, w^2),$
$(0, w, w^2, w, 0, 0, 0), (0, w^2, w, 0, w, 1, 1),$
$(1, w^2, w^2, 1, 0, w^2, 0), (0, w, w^2, 0, 1, 1, w),$
$(1, w, 0, w, w^2, 0, 1), (0, w, 1, w^2, 1, w, 0),$
$(1, w^2, 1, w, 0, 0, w), (0, w^2, 0, 1, w^2, w^2, 1),$
$(1, w, 0, 0, w, 1, w^2), (0, w, 1, 1, 0, w^2, w),$
$(0, 0, 0, 0, w, w^2, w), (0, 1, 1, w, 0, w, w^2),$
$(1, 1, 0, w^2, w, 0, w), (0, 0, 0, w, w^2, w, 0),$
$(1, 0, w^2, 0, 1, w^2, w^2), (0, 0, w, 1, w^2, 1, w),$
$(1, 1, w, 0, w, w^2, 0), (0, 1, w^2, w^2, 1, 0, w^2),$
$(1, 0, w^2, w, 0, w, 1), (0, 0, w, w^2, w, 0, 0),$
$(w, w, w, w, 0, 1, 0), (w, w^2, w^2, 0, w, 0, 1),$
$(w^2, w^2, w, 1, 0, w, 0), (w, w, w, 0, 1, 0, w),$
$(w^2, w, 1, w, w^2, 1, 1), (w, w, 0, w^2, 1, w^2, 0),$
$(w^2, w^2, 0, w, 0, 1, w), (w, w^2, 1, 1, w^2, w, 1),$
$(w^2, w, 1, 0, w, 0, w^2), (w, w, 0, 1, 0, w, w),$
$(w, 0, w^2, w^2, w, 1, 0), (w^2, 0, w, w, 0, w^2, 1),$
$(w, 1, w, w^2, 1, 1, w^2), (w^2, 1, w^2, 0, w, w, 0),$
$(w, 0, w^2, 1, w^2, 0, w), (w^2, 0, w, 0, 1, w, w^2),$
$(w, 0, 1, w, w^2, w^2, 0), (w^2, 1, 1, w^2, w, 1, w),$
$(w, 1, 0, w, 0, w^2, w^2), (w, 0, 1, 0, w, w, w),$
$(0, w, w, w, w, 0, 1), (1, w, w^2, w^2, 0, w, 0),$
$(0, w^2, w^2, w, 1, 0, w), (1, w^2, w, 1, w, w^2, 1),$
$(0, w, w, 0, w^2, 1, w^2), (1, w, w^2, 1, 1, w^2, w),$
$(0, w, 0, w^2, w^2, w, 1), (1, w^2, 0, w, w, 0, w^2),$
$(0, w^2, 1, w^2, 0, w, w), (0, w, 0, 1, w, w^2, w^2),$
$(1, 0, w, w, w, w, 0), (0, 1, w, w^2, w^2, 0, w),$
$(1, 1, w^2, w, 1, w, w^2), (1, 0, w, 0, w^2, w^2, w),$
$(0, 1, 0, w, w, w, w), (w, w, w^2, w, w, 1, 1),$
$(w^2, w, w, w^2, 0, w^2, 0), (w, w^2, w, w, 1, 1, w),$
$(w^2, w^2, w^2, 1, w, w, 1), (w, w, w^2, 0, w^2, 0, w^2),$
$(w^2, w, w, 1, 1, w, w), (w, w, 1, w^2, w^2, w^2, 1),$
$(w^2, w^2, 1, w, w, 1, w^2), (w, w^2, 0, w^2, 0, w^2, w),$
$(w, w, 1, 1, w, w, w^2), (w^2, 0, w^2, w, w, w^2, 0),$
$(w, 1, w^2, w^2, w^2, 1, w), (w^2, 1, w, w, 1, w^2, w^2),$
$(w^2, 0, w^2, 0, w^2, w, w), (w, 1, 1, w, w, w^2, w),$
$(1, w, w, w^2, w, w, 1), (0, w^2, w, w, w^2, 0, w^2),$

$(1, w^2, w^2, w^2, 1, w, w)$, $(1, w, w, 1, w^2, w^2, w^2)$,
$(0, w^2, 0, w^2, w, w, w^2)$, $(1, 1, w, w, w^2, w, w)$,
$(w^2, w, w^2, w^2, w, w^2, 1)$, $(w, w^2, w^2, w, w^2, 1, w^2)$,
$(w^2, w^2, w, w^2, 1, w^2, w)$, $(w^2, w, w^2, 1, w^2, w, w^2)$,
$(w, w^2, 1, w^2, w, w^2, w^2)$, $(w^2, 1, w^2, w, w^2, w^2, w)$,
$(1, w^2, w, w^2, w^2, w, w^2)$,
$(w^2, w^2, w^2, w^2, w^2, w^2, w^2)$

Örnek 2 :

$$C_5 = (w^2 + (x^2 + x^5), (1 + x + x^2 + x^3 + x^4 + x^5 + x^6))$$

kodunun elemanları aşağıdaki gibidir.

```
PadRight[CoefficientList[
    Expand[i * (w^2 + x^2 + x^5)] /. w^2 + 1 → w /.
                    x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
                x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
          x^13 → x^6 /. x^14 → x^7, x, Modulus → 2],
  {128, 7}]
```

```
PadRight[
  CoefficientList[
    Expand[i * (w^2 + x^2 + x^5) +
                      (1 + x + x^2 + x^3 + x^4 + x^
                           5 + x^6)] /. w^2 + 1 → w /.
                x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
            x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
        x^13 → x^6 /. x^14 → x^7, x, Modulus → 2],
  {128, 7}]
```

$(0, 0, 0, 0, 0, 0, 0)$, $(w^2, 0, 1, 0, 0, 1, 0)$, $(0, w^2, 0, 1, 0, 0, 1)$,
$(1, 0, w^2, 0, 1, 0, 0)$, $(0, 1, 0, w^2, 0, 1, 0)$, $(0, 0, 1, 0, w^2, 0, 1)$,
$(1, 0, 0, 1, 0, w^2, 0)$, $(0, 1, 0, 0, 1, 0, w^2)$,
$(w^2, w^2, 1, 1, 0, 1, 1)$, $(1, w^2, w^2, 1, 1, 0, 1)$,
$(1, 1, w^2, w^2, 1, 1, 0)$, $(0, 1, 1, w^2, w^2, 1, 1)$,
$(1, 0, 1, 1, w^2, w^2, 1)$, $(1, 1, 0, 1, 1, w^2, w^2)$,
$(w, 0, w, 0, 1, 1, 0)$, $(w^2, 1, 1, w^2, 0, 0, 0)$,
$(w^2, 0, 0, 0, w^2, 1, 1)$, $(w, 0, 1, 1, 0, w, 0)$,
$(w^2, 1, 1, 0, 1, 1, w^2)$, $(0, w, 0, 1, 1, 0, w)$,
$(1, 1, w^2, 0, 0, 0, w^2)$, $(0, 0, 0, w^2, 1, 1, w^2)$,
$(0, 1, 1, 0, w, 0, w)$, $(1, 1, 0, w, 0, w, 0)$, $(1, 0, w, 0, w, 0, 1)$,
$(0, w, 0, w, 0, 1, 1)$, $(0, w^2, 1, 1, w^2, 0, 0)$,
$(1, w^2, 0, 0, 0, w^2, 1)$, $(0, 0, w^2, 1, 1, w^2, 0)$,
$(w, w^2, w, 1, 1, 1, 1)$, $(w^2, w, 1, w, 0, 0, 1)$,
$(w^2, w^2, 0, 1, w^2, 1, 0)$, $(w, w^2, 1, 0, 0, w, 1)$,
$(w^2, w, 1, 1, 1, 1, w)$, $(w, 1, w, w^2, 1, 0, 0)$,
$(w, 0, w^2, 0, w, 1, 1)$, $(w^2, 0, w, 1, 1, w, 0)$,
$(w, 1, w, 0, 0, 1, w^2)$, $(w^2, 1, 0, w^2, w^2, 0, 1)$,
$(w, 1, 1, w, 0, w^2, 0)$, $(w^2, 0, 1, w^2, 1, 0, w^2)$,
$(w, 0, 0, 1, w^2, w, 1)$, $(w^2, 1, 0, 0, w, 1, w)$,
$(w, 1, 1, 1, 1, w, w^2)$, $(1, w, w^2, w, 1, 1, 1)$,
$(1, w^2, w, 1, w, 0, 0)$, $(0, w^2, w^2, 0, 1, w^2, 1)$,
$(1, w, w^2, 1, 0, 0, w)$, $(0, w, 1, w, w^2, 1, 0)$,
$(1, w, 0, w^2, 0, w, 1)$, $(0, w^2, 0, w, 1, 1, w)$,
$(1, w^2, 1, 0, w^2, w^2, 0)$, $(0, w, 1, 1, w, 0, w^2)$,
$(1, w, 0, 0, 1, w^2, w)$, $(1, 1, 1, 1, w, w^2, w)$,
$(1, 0, 0, w, 1, w, w^2)$, $(0, 0, 1, w^2, w, 1, w)$,
$(1, 1, 1, w, w^2, w, 1)$, $(0, 1, w^2, 1, 0, w^2, w^2)$,
$(1, 1, w, 0, w^2, 0, w)$, $(0, 0, w, 1, w, w^2, 1)$,
$(1, 0, w^2, w^2, 0, 1, w^2)$, $(0, 1, w^2, w, 1, w, 0)$,
$(1, 1, w, w^2, w, 1, 1)$, $(w, w, w, w, 1, 0, 1)$,
$(w, w^2, w^2, 1, w, 1, 0)$, $(w^2, w^2, w, 0, 1, w, 1)$,
$(w, w, w, 1, 0, 1, w)$, $(w^2, w, 0, w, w^2, 0, 0)$,
$(w, w, 1, w^2, 0, w^2, 1)$, $(w^2, w^2, 1, w, 1, 0, w)$,
$(w, w^2, 0, 0, w^2, w, 0)$, $(w^2, w, 0, 1, w, 1, w^2)$,
$(w, w, 1, 0, 1, w, w)$, $(w, 1, w^2, w^2, w, 0, 1)$,
$(w^2, 1, w, w, 1, w^2, 0)$, $(w, 0, w, w^2, 0, 0, w^2)$,
$(w^2, 0, w^2, 1, w, w, 1)$, $(w, 1, w^2, 0, w^2, 1, w)$,
$(w^2, 1, w, 1, 0, w, w^2)$, $(w, 1, 0, w, w^2, w^2, 1)$,
$(w^2, 0, 0, w^2, w, 0, w)$, $(w, 0, 1, w, 1, w^2, w^2)$,

(w, 1, 0, 1, w, w, w), (1, w, w, w, w, 1, 0),
(0, w, w^2, w^2, 1, w, 1), (1, w^2, w^2, w, 0, 1, w),
(0, w^2, w, 0, w, w^2, 0), (1, w, w, 1, w^2, 0, w^2),
(0, w, w^2, 0, 0, w^2, w), (1, w, 1, w^2, w^2, w, 0),
(0, w^2, 1, w, w, 1, w^2), (1, w^2, 0, w^2, 1, w, w),
(1, w, 1, 0, w, w^2, w^2), (0, 1, w, w, w, w, 1),
(1, 0, w, w^2, w^2, 1, w), (0, 0, w^2, w, 0, w, w^2),
(0, 1, w, 1, w^2, w^2, w), (1, 0, 1, w, w, w, w),
(w, w, w^2, w, w, 0, 0), (w^2, w, w, w^2, 1, w^2, 1),
(w, w^2, w, w, 0, 0, w), (w^2, w^2, w^2, 0, w, w, 0),
(w, w, w^2, 1, w^2, 1, w^2), (w^2, w, w, 0, 0, w, w),
(w, w, 0, w^2, w^2, w^2, 0), (w^2, w^2, 0, w, w, 0, w^2),
(w, w^2, 1, w^2, 1, w^2, w), (w, w, 0, 0, w, w, w^2),
(w^2, 1, w^2, w, w, w^2, 1), (w, 0, w^2, w^2, w^2, 0, w),
(w^2, 0, w, w, 0, w^2, w^2), (w^2, 1, w^2, 1, w^2, w, w),
(w, 0, 0, w, w, w^2, w), (0, w, w, w^2, w, w, 0),
(1, w^2, w, w, w^2, 1, w^2), (0, w^2, w^2, w^2, 0, w, w),
(0, w, w, 0, w^2, w^2, w^2), (1, w^2, 1, w^2, w, w, w^2),
(0, 0, w, w, w^2, w, w), (w^2, w, w^2, w^2, w, w^2, 0),
(w, w^2, w^2, w, w^2, 0, w^2), (w^2, w^2, w, w^2, 0, w^2, w),
(w^2, w, w^2, 0, w^2, w, w^2), (w, w^2, 0, w^2, w, w^2, w^2),
(w^2, 0, w^2, w, w^2, w^2, w), (0, w^2, w, w^2, w^2, w, w^2),
(w^2, w^2, w^2, w^2, w^2, w^2, w^2), (1, 1, 1, 1, 1, 1, 1),
(w, 1, 0, 1, 1, 0, 1), (1, w, 1, 0, 1, 1, 0), (0, 1, w, 1, 0, 1, 1),
(1, 0, 1, w, 1, 0, 1), (1, 1, 0, 1, w, 1, 0), (0, 1, 1, 0, 1, w, 1),
(1, 0, 1, 1, 0, 1, w), (w, w, 0, 0, 1, 0, 0), (0, w, w, 0, 0, 1, 0),
(0, 0, w, w, 0, 0, 1), (1, 0, 0, w, w, 0, 0), (0, 1, 0, 0, w, w, 0),
(0, 0, 1, 0, 0, w, w), (w^2, 1, w^2, 1, 0, 0, 1), (w, 0, 0, w, 1, 1, 1),
(w, 1, 1, 1, w, 0, 0), (w^2, 1, 0, 0, 1, w^2, 1), (w, 0, 0, 1, 0, 0, w),
(1, w^2, 1, 0, 0, 1, w^2), (0, 0, w, 1, 1, 1, w), (1, 1, 1, w, 0, 0, w),
(1, 0, 0, 1, w^2, 1, w^2), (0, 0, 1, w^2, 1, w^2, 1),
(0, 1, w^2, 1, w^2, 1, 0), (1, w^2, 1, w^2, 1, 0, 0),
(1, w, 0, 0, w, 1, 1), (0, w, 1, 1, 1, w, 0), (1, 1, w, 0, 0, w, 1),
(w^2, w, w^2, 0, 0, 0, 0), (w, w^2, 0, w^2, 1, 1, 0),
(w, w, 1, 0, w, 0, 1), (w^2, w, 0, 1, 1, w^2, 0),
(w, w^2, 0, 0, 0, 0, w^2), (w^2, 0, w^2, w, 0, 1, 1),
(w^2, 1, w, 1, w^2, 0, 0), (w, 1, w^2, 0, 0, w^2, 1),
(w^2, 0, w^2, 1, 1, 0, w), (w, 0, 1, w, w, 1, 0),
(w^2, 0, 0, w^2, 1, w, 1), (w, 1, 0, w, 0, 1, w),
(w^2, 1, 1, 0, w, w^2, 0), (w, 0, 1, 1, w^2, 0, w^2),

$(w^2, 0, 0, 0, 0, w^2, w)$, $(0, w^2, w, w^2, 0, 0, 0)$,
$(0, w, w^2, 0, w^2, 1, 1)$, $(1, w, w, 1, 0, w, 0)$,
$(0, w^2, w, 0, 1, 1, w^2)$, $(1, w^2, 0, w^2, w, 0, 1)$,
$(0, w^2, 1, w, 1, w^2, 0)$, $(1, w, 1, w^2, 0, 0, w^2)$,
$(0, w, 0, 1, w, w, 1)$, $(1, w^2, 0, 0, w^2, 1, w)$,
$(0, w^2, 1, 1, 0, w, w^2)$, $(0, 0, 0, 0, w^2, w, w^2)$,
$(0, 1, 1, w^2, 0, w^2, w)$, $(1, 1, 0, w, w^2, 0, w^2)$,
$(0, 0, 0, w^2, w, w^2, 0)$, $(1, 0, w, 0, 1, w, w)$,
$(0, 0, w^2, 1, w, 1, w^2)$, $(1, 1, w^2, 0, w^2, w, 0)$,
$(0, 1, w, w, 1, 0, w)$, $(1, 0, w, w^2, 0, w^2, 1)$,
$(0, 0, w^2, w, w^2, 0, 0)$, $(w^2, w^2, w^2, w^2, 0, 1, 0)$,
$(w^2, w, w, 0, w^2, 0, 1)$, $(w, w, w^2, 1, 0, w^2, 0)$,
$(w^2, w^2, w^2, 0, 1, 0, w^2)$, $(w, w^2, 1, w^2, w, 1, 1)$,
$(w^2, w^2, 0, w, 1, w, 0)$, $(w, w, 0, w^2, 0, 1, w^2)$,
$(w^2, w, 1, 1, w, w^2, 1)$, $(w, w^2, 1, 0, w^2, 0, w)$,
$(w^2, w^2, 0, 1, 0, w^2, w^2)$, $(w^2, 0, w, w, w^2, 1, 0)$,
$(w, 0, w^2, w^2, 0, w, 1)$, $(w^2, 1, w^2, w, 1, 1, w)$,
$(w, 1, w, 0, w^2, w^2, 0)$, $(w^2, 0, w, 1, w, 0, w^2)$,
$(w, 0, w^2, 0, 1, w^2, w)$, $(w^2, 0, 1, w^2, w, w, 0)$,
$(w, 1, 1, w, w^2, 1, w^2)$, $(w^2, 1, 0, w^2, 0, w, w)$,
$(w^2, 0, 1, 0, w^2, w^2, w^2)$, $(0, w^2, w^2, w^2, w^2, 0, 1)$,
$(1, w^2, w, w, 0, w^2, 0)$, $(0, w, w, w^2, 1, 0, w^2)$,
$(1, w, w^2, 1, w^2, w, 1)$, $(0, w^2, w^2, 0, w, 1, w)$,
$(1, w^2, w, 1, 1, w, w^2)$, $(0, w^2, 0, w, w, w^2, 1)$,
$(1, w, 0, w^2, w^2, 0, w)$, $(0, w, 1, w, 0, w^2, w^2)$,
$(0, w^2, 0, 1, w^2, w, w)$, $(1, 0, w^2, w^2, w^2, w^2, 0)$,
$(0, 1, w^2, w, w, 0, w^2)$, $(1, 1, w, w^2, 1, w^2, w)$,
$(1, 0, w^2, 0, w, w, w^2)$, $(0, 1, 0, w^2, w^2, w^2, w^2)$,
$(w^2, w^2, w, w^2, w^2, 1, 1)$, $(w, w^2, w^2, w, 0, w, 0)$,
$(w^2, w, w^2, w^2, 1, 1, w^2)$, $(w, w, w, 1, w^2, w^2, 1)$,
$(w^2, w^2, w, 0, w, 0, w)$, $(w, w^2, w^2, 1, 1, w^2, w^2)$,
$(w^2, w^2, 1, w, w, w, 1)$, $(w, w, 1, w^2, w^2, 1, w)$,
$(w^2, w, 0, w, 0, w, w^2)$, $(w^2, w^2, 1, 1, w^2, w^2, w)$,
$(w, 0, w, w^2, w^2, w, 0)$, $(w^2, 1, w, w, w, 1, w^2)$,
$(w, 1, w^2, w^2, 1, w, w)$, $(w, 0, w, 0, w, w^2, w^2)$,
$(w^2, 1, 1, w^2, w^2, w, w^2)$, $(1, w^2, w^2, w, w^2, w^2, 1)$,
$(0, w, w^2, w^2, w, 0, w)$, $(1, w, w, w, 1, w^2, w^2)$,
$(1, w^2, w^2, 1, w, w, w)$, $(0, w, 0, w, w^2, w^2, w)$,
$(1, 1, w^2, w^2, w, w^2, w^2)$, $(w, w^2, w, w, w^2, w, 1)$,
$(w^2, w, w, w^2, w, 1, w)$, $(w, w, w^2, w, 1, w, w^2)$,

$(w, w^2, w, 1, w, w^2, w)$, $(w^2, w, 1, w, w^2, w, w)$,
$(w, 1, w, w^2, w, w, w^2)$, $(1, w, w^2, w, w, w^2, w)$,
(w, w, w, w, w, w, w)

Örnek 3 :

$$C = (u^6 + (x^2 + x^3 + x^4 + x^5),\ (1 + x + x^2 + x^3 + x^4 + x^5 + x^6))$$

kodunun elemanları aşağıdaki gibidir.

```
PadRight[CoefficientList[
    Expand[i ∗ (u^6 + x^2 + x^3 + x^4 + x^5)] /. u^4 → 1 + u /.
                           u^5 → u^2 + u /.
                           u^6 → u^3 + u^2 /.
                           u^7 → u^3 + u + 1 /.
                         u^8 → u^2 + 1 /. u^9 → u^3 + u /.
                     u^10 → u^2 + u + 1 /.
                   u^11 → u^3 + u^2 + u /.
                 u^12 → u^3 + u^2 + u + 1
                /. u^13 → u^3 + u^2 + 1
                /. u^14 → u^3 + 1
                /. x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
           x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
      x^13 → x^6 /. x^14 → x^7 , x, Modulus → 2],
  {128, 7}]
```

```
PadRight[
  CoefficientList[
    Expand[i ∗ (u^6 + x^2 + x^3 + x^4 + x^5) +
                           (1 + x + x^2 + x^3 +
                           x^4 + x^5 + x^6)] /.
                           u^4 → 1 + u /.
                         u^5 → u^2 + u /. u^6 →
                         u^3 + u^2 /. u^7 → u^3 + u + 1 /.
                   u^8 → u^2 + 1 /. u^9 → u^3 + u /.
               u^10 → u^2 + u + 1 /. u^11 → u^3 + u^2 + u
            /. u^12 → u^3 + u^2 + u + 1
            /. u^13 → u^3 + u^2 + 1
            /. u^14 → u^3 + 1
            /. x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
        x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
   x^13 → x^6 /. x^14 → x^7 , x, Modulus → 2], {128, 7}]
```

$(0, 0, 0, 0, 0, 0, 0), (u^{6}, 0, 1, 1, 1, 1, 0), (0, u^{6}, 0, 1, 1, 1, 1),$
$(1, 0, u^{6}, 0, 1, 1, 1), (1, 1, 0, u^{6}, 0, 1, 1), (1, 1, 1, 0, u^{6}, 0, 1),$
$(1, 1, 1, 1, 0, u^{6}, 0), (0, 1, 1, 1, 1, 0, u^{6}), (u^{6}, u^{6}, 1, 0, 0, 0, 1),$
$(1, u^{6}, u^{6}, 1, 0, 0, 0), (0, 1, u^{6}, u^{6}, 1, 0, 0), (0, 0, 1, u^{6}, u^{6}, 1, 0),$
$(0, 0, 0, 1, u^{6}, u^{6}, 1), (1, 0, 0, 0, 1, u^{6}, u^{6}), (u^{13}, 0, u^{13}, 1, 0, 0, 1),$
$(u^{13}, 1, 1, u^{13}, 1, 0, 1), (u^{13}, 1, 0, 1, u^{13}, 1, 1),$
$(u^{13}, 1, 0, 0, 1, u^{13}, 0), (u^{6}, 1, 0, 0, 0, 1, u^{6}),$
$(0, u^{13}, 1, 0, 0, 1, u^{13}), (1, 1, u^{13}, 1, 0, 1, u^{13}),$
$(1, 0, 1, u^{13}, 1, 1, u^{13}), (1, 0, 0, 1, u^{13}, 0, u^{13}),$
$(0, 0, 1, u^{13}, 0, u^{13}, 1), (0, 1, u^{13}, 0, u^{13}, 1, 0),$
$(1, u^{13}, 0, u^{13}, 1, 0, 0), (1, u^{13}, 1, 1, u^{13}, 1, 0),$
$(1, u^{13}, 1, 0, 1, u^{13}, 1), (0, 1, u^{13}, 1, 1, u^{13}, 1),$
$(u^{13}, u^{6}, u^{13}, 0, 1, 1, 0), (u^{13}, u^{13}, 1, u^{6}, 0, 1, 0),$
$(u^{13}, u^{13}, 0, 0, u^{6}, 0, 0), (u^{13}, u^{13}, 0, 1, 0, u^{6}, 1),$
$(u^{6}, u^{13}, 0, 1, 1, 0, u^{13}), (u^{6}, 1, u^{13}, u^{13}, 0, 1, 0),$
$(u^{6}, 1, u^{6}, 1, u^{6}, 0, 0), (u^{6}, 1, u^{6}, 0, 0, u^{6}, 1),$
$(u^{13}, 1, u^{6}, 0, 1, 0, u^{13}), (u^{6}, 0, 0, u^{13}, u^{13}, 0, 0),$
$(u^{6}, 0, 0, u^{6}, 1, u^{6}, 1), (u^{13}, 0, 0, u^{6}, 0, 0, u^{13}),$
$(u^{6}, 0, 1, 0, u^{13}, u^{13}, 1), (u^{13}, 0, 1, 0, u^{6}, 1, u^{13}),$
$(u^{13}, 0, 1, 1, 0, u^{13}, u^{6}), (0, u^{13}, u^{6}, u^{13}, 0, 1, 1),$
$(0, u^{13}, u^{13}, 1, u^{6}, 0, 1), (0, u^{13}, u^{13}, 0, 0, u^{6}, 0),$
$(1, u^{13}, u^{13}, 0, 1, 0, u^{6}), (0, u^{6}, 1, u^{13}, u^{13}, 0, 1),$
$(0, u^{6}, 1, u^{6}, 1, u^{6}, 0), (1, u^{6}, 1, u^{6}, 0, 0, u^{6}),$
$(0, u^{6}, 0, 0, u^{13}, u^{13}, 0), (1, u^{6}, 0, 0, u^{6}, 1, u^{6}),$
$(1, u^{6}, 0, 1, 0, u^{13}, u^{13}), (0, 1, 1, 0, u^{13}, u^{6}, u^{13}),$
$(0, 1, 0, u^{6}, 1, u^{13}, u^{13}), (0, 1, 0, u^{13}, u^{13}, 1, u^{6}),$
$(1, 1, 0, u^{13}, u^{6}, u^{13}, 0), (0, 0, u^{6}, 0, 0, u^{13}, u^{13}),$
$(0, 0, u^{6}, 1, u^{6}, 1, u^{6}), (1, 0, u^{6}, 1, u^{13}, u^{13}, 0),$
$(0, 0, u^{13}, u^{13}, 0, 0, u^{6}), (1, 0, u^{13}, u^{13}, 1, u^{6}, 0),$
$(1, 0, u^{13}, u^{6}, u^{13}, 0, 1), (u^{6}, u^{13}, u^{13}, u^{6}, 1, 0, 1),$
$(u^{6}, u^{13}, u^{6}, 0, u^{13}, 1, 1), (u^{6}, u^{13}, u^{6}, 1, 1, u^{13}, 0),$
$(u^{13}, u^{13}, u^{6}, 1, 0, 1, u^{6}), (u^{6}, u^{6}, 0, u^{6}, u^{6}, 1, 1),$
$(u^{6}, u^{6}, 0, u^{13}, 0, u^{13}, 0), (u^{13}, u^{6}, 0, u^{13}, 1, 1, u^{6}),$
$(u^{6}, u^{6}, 1, 1, u^{6}, u^{6}, 0), (u^{13}, u^{6}, 1, 1, u^{13}, 0, u^{6}),$
$(u^{13}, u^{6}, 1, 0, 1, u^{6}, u^{13}), (u^{13}, 0, u^{6}, u^{13}, u^{6}, 1, 1),$
$(u^{13}, 0, u^{6}, u^{6}, 0, u^{13}, 0), (u^{6}, 0, u^{6}, u^{6}, 1, 1, u^{6}),$
$(u^{13}, 0, u^{13}, 0, u^{6}, u^{6}, 0), (u^{6}, 0, u^{13}, 0, u^{13}, 0, u^{6}),$
$(u^{6}, 0, u^{13}, 1, 1, u^{6}, u^{13}), (u^{13}, 1, 1, u^{6}, u^{13}, u^{6}, 0),$
$(u^{6}, 1, 1, u^{6}, u^{6}, 0, u^{6}), (u^{6}, 1, 1, u^{13}, 0, u^{6}, u^{13}),$

$(u^6, 1, 0, 1, u^6, u^{13}, u^{13}), (1, u^6, u^{13}, u^{13}, u^6, 1, 0),$
$(1, u^6, u^{13}, u^6, 0, u^{13}, 1), (0, u^6, u^{13}, u^6, 1, 1, u^{13}),$
$(1, u^6, u^6, 0, u^6, u^6, 1), (0, u^6, u^6, 0, u^{13}, 0, u^{13}),$
$(0, u^6, u^6, 1, 1, u^6, u^6), (1, u^{13}, 0, u^6, u^{13}, u^6, 1),$
$(0, u^{13}, 0, u^6, u^6, 0, u^{13}), (0, u^{13}, 0, u^{13}, 0, u^6, u^6),$
$(0, u^{13}, 1, 1, u^6, u^{13}, u^6), (0, 1, u^6, u^{13}, u^{13}, u^6, 1),$
$(1, 1, u^6, u^{13}, u^6, 0, u^{13}), (1, 1, u^6, u^6, 0, u^6, u^6),$
$(1, 1, u^{13}, 0, u^6, u^{13}, u^6), (1, 0, 1, u^6, u^{13}, u^{13}, u^6),$
$(u^{13}, u^6, u^6, u^6, u^{13}, 0, 0), (u^{13}, u^6, u^6, u^{13}, 1, u^6, 1),$
$(u^6, u^6, u^6, u^{13}, 0, 0, u^{13}), (u^{13}, u^6, u^{13}, 1, u^{13}, u^{13}, 1),$
$(u^6, u^6, u^{13}, 1, u^6, 1, u^{13}), (u^6, u^6, u^{13}, 0, 0, u^{13}, u^6),$
$(u^{13}, u^{13}, 1, u^{13}, u^6, u^{13}, 1), (u^6, u^{13}, 1, u^{13}, u^{13}, 1, u^{13}),$
$(u^6, u^{13}, 1, u^6, 1, u^{13}, u^6), (u^6, u^{13}, 0, 0, u^{13}, u^6, u^6),$
$(u^6, 1, u^{13}, u^6, u^6, u^{13}, 1), (u^{13}, 1, u^{13}, u^6, u^{13}, 1, u^{13}),$
$(u^{13}, 1, u^{13}, u^{13}, 1, u^{13}, u^6), (u^{13}, 1, u^6, 1, u^{13}, u^6, u^6),$
$(u^{13}, 0, 0, u^{13}, u^6, u^6, u^6), (0, u^{13}, u^6, u^6, u^6, u^{13}, 0),$
$(1, u^{13}, u^6, u^6, u^{13}, 1, u^6), (1, u^{13}, u^6, u^{13}, 1, u^{13}, u^{13}),$
$(1, u^{13}, u^{13}, 1, u^{13}, u^6, u^{13}), (1, u^6, 1, u^{13}, u^6, u^6, u^{13}),$
$(0, 0, u^{13}, u^6, u^6, u^6, u^{13}), (u^6, u^{13}, u^{13}, u^{13}, u^{13}, u^6, 0),$
$(u^{13}, u^{13}, u^{13}, u^{13}, u^6, 0, u^6), (u^{13}, u^{13}, u^{13}, u^6, 0, u^6, u^{13}),$
$(u^{13}, u^{13}, u^6, 0, u^6, u^{13}, u^{13}), (u^{13}, u^6, 0, u^6, u^{13}, u^{13}, u^{13}),$
$(u^6, 0, u^6, u^{13}, u^{13}, u^{13}, u^{13}), (0, u^6, u^{13}, u^{13}, u^{13}, u^{13}, u^6),$
$(u^6, u^6, u^6, u^6, u^6, u^6, u^6), (1, 1, 1, 1, 1, 1, 1),$
$(u^{13}, 1, 0, 0, 0, 0, 1), (1, u^{13}, 1, 0, 0, 0, 0), (0, 1, u^{13}, 1, 0, 0, 0),$
$(0, 0, 1, u^{13}, 1, 0, 0), (0, 0, 0, 1, u^{13}, 1, 0), (0, 0, 0, 0, 1, u^{13}, 1),$
$(1, 0, 0, 0, 0, 1, u^{13}), (u^{13}, u^{13}, 0, 1, 1, 1, 0),$
$(0, u^{13}, u^{13}, 0, 1, 1, 1), (1, 0, u^{13}, u^{13}, 0, 1, 1),$
$(1, 1, 0, u^{13}, u^{13}, 0, 1), (1, 1, 1, 0, u^{13}, u^{13}, 0),$
$(0, 1, 1, 1, 0, u^{13}, u^{13}), (u^6, 1, u^6, 0, 1, 1, 0), (u^6, 0, 0, u^6, 0, 1, 0),$
$(u^6, 0, 1, 0, u^6, 0, 0), (u^6, 0, 1, 1, 0, u^6, 1), (u^{13}, 0, 1, 1, 1, 0, u^{13}),$
$(1, u^6, 0, 1, 1, 0, u^6), (0, 0, u^6, 0, 1, 0, u^6), (0, 1, 0, u^6, 0, 0, u^6),$
$(0, 1, 1, 0, u^6, 1, u^6), (1, 1, 0, u^6, 1, u^6, 0), (1, 0, u^6, 1, u^6, 0, 1),$
$(0, u^6, 1, u^6, 0, 1, 1), (0, u^6, 0, 0, u^6, 0, 1), (0, u^6, 0, 1, 0, u^6, 0),$
$(1, 0, u^6, 0, 0, u^6, 0), (u^6, u^{13}, u^6, 1, 0, 0, 1),$
$(u^6, u^6, 0, u^{13}, 1, 0, 1), (u^6, u^6, 1, 1, u^{13}, 1, 1),$
$(u^6, u^6, 1, 0, 1, u^{13}, 0), (u^{13}, u^6, 1, 0, 0, 1, u^6),$
$(u^{13}, 0, u^6, u^6, 1, 0, 1), (u^{13}, 0, u^{13}, 0, u^{13}, 1, 1),$
$(u^{13}, 0, u^{13}, 1, 1, u^{13}, 0), (u^6, 0, u^{13}, 1, 0, 1, u^6),$
$(u^{13}, 1, 1, u^6, u^6, 1, 1), (u^{13}, 1, 1, u^{13}, 0, u^{13}, 0),$
$(u^6, 1, 1, u^{13}, 1, 1, u^6), (u^{13}, 1, 0, 1, u^6, u^6, 0),$

$(u^6, 1, 0, 1, u^{13}, 0, u^6)$, $(u^6, 1, 0, 0, 1, u^6, u^{13})$,
$(1, u^6, u^{13}, u^6, 1, 0, 0)$, $(1, u^6, u^6, 0, u^{13}, 1, 0)$,
$(1, u^6, u^6, 1, 1, u^{13}, 1)$, $(0, u^6, u^6, 1, 0, 1, u^{13})$,
$(1, u^{13}, 0, u^6, u^6, 1, 0)$, $(1, u^{13}, 0, u^{13}, 0, u^{13}, 1)$,
$(0, u^{13}, 0, u^{13}, 1, 1, u^{13})$, $(1, u^{13}, 1, 1, u^6, u^6, 1)$,
$(0, u^{13}, 1, 1, u^{13}, 0, u^{13})$, $(0, u^{13}, 1, 0, 1, u^6, u^6)$,
$(1, 0, 0, 1, u^6, u^{13}, u^6)$, $(1, 0, 1, u^{13}, 0, u^6, u^6)$,
$(1, 0, 1, u^6, u^6, 0, u^{13})$, $(0, 0, 1, u^6, u^{13}, u^6, 1)$,
$(1, 1, u^{13}, 1, 1, u^6, u^6)$, $(1, 1, u^{13}, 0, u^{13}, 0, u^{13})$,
$(0, 1, u^{13}, 0, u^6, u^6, 1)$, $(1, 1, u^6, u^6, 1, 1, u^{13})$,
$(0, 1, u^6, u^6, 0, u^{13}, 1)$, $(0, 1, u^6, u^{13}, u^6, 1, 0)$,
$(u^{13}, u^6, u^6, u^{13}, 0, 1, 0)$, $(u^{13}, u^6, u^{13}, 1, u^6, 0, 0)$,
$(u^{13}, u^6, u^{13}, 0, 0, u^6, 1)$, $(u^6, u^6, u^{13}, 0, 1, 0, u^{13})$,
$(u^{13}, u^{13}, 1, u^{13}, u^{13}, 0, 0)$, $(u^{13}, u^{13}, 1, u^6, 1, u^6, 1)$,
$(u^6, u^{13}, 1, u^6, 0, 0, u^{13})$, $(u^{13}, u^{13}, 0, 0, u^{13}, u^{13}, 1)$,
$(u^6, u^{13}, 0, 0, u^6, 1, u^{13})$, $(u^6, u^{13}, 0, 1, 0, u^{13}, u^6)$,
$(u^6, 1, u^{13}, u^6, u^{13}, 0, 0)$, $(u^6, 1, u^{13}, u^{13}, 1, u^6, 1)$,
$(u^{13}, 1, u^{13}, u^{13}, 0, 0, u^{13})$, $(u^6, 1, u^6, 1, u^{13}, u^{13}, 1)$,
$(u^{13}, 1, u^6, 1, u^6, 1, u^{13})$, $(u^{13}, 1, u^6, 0, 0, u^{13}, u^6)$,
$(u^6, 0, 0, u^{13}, u^6, u^{13}, 1)$, $(u^{13}, 0, 0, u^{13}, u^{13}, 1, u^{13})$,
$(u^{13}, 0, 0, u^6, 1, u^{13}, u^6)$, $(u^{13}, 0, 1, 0, u^{13}, u^6, u^6)$,
$(0, u^{13}, u^6, u^6, u^{13}, 0, 1)$, $(0, u^{13}, u^6, u^{13}, 1, u^6, 0)$,
$(1, u^{13}, u^6, u^{13}, 0, 0, u^6)$, $(0, u^{13}, u^{13}, 1, u^{13}, u^{13}, 0)$,
$(1, u^{13}, u^{13}, 1, u^6, 1, u^6)$, $(1, u^{13}, u^{13}, 0, 0, u^{13}, u^{13})$,
$(0, u^6, 1, u^{13}, u^6, u^{13}, 0)$, $(1, u^6, 1, u^{13}, u^{13}, 1, u^6)$,
$(1, u^6, 1, u^6, 1, u^{13}, u^{13})$, $(1, u^6, 0, 0, u^{13}, u^6, u^{13})$,
$(1, 0, u^{13}, u^6, u^6, u^{13}, 0)$, $(0, 0, u^{13}, u^6, u^{13}, 1, u^6)$,
$(0, 0, u^{13}, u^{13}, 1, u^{13}, u^{13})$, $(0, 0, u^6, 1, u^{13}, u^6, u^{13})$,
$(0, 1, 0, u^{13}, u^6, u^6, u^{13})$, $(u^6, u^{13}, u^{13}, u^{13}, u^6, 1, 1)$,
$(u^6, u^{13}, u^{13}, u^6, 0, u^{13}, 0)$, $(u^{13}, u^{13}, u^{13}, u^6, 1, 1, u^6)$,
$(u^6, u^{13}, u^6, 0, u^6, u^6, 0)$, $(u^{13}, u^{13}, u^6, 0, u^{13}, 0, u^6)$,
$(u^{13}, u^{13}, u^6, 1, 1, u^6, u^{13})$, $(u^6, u^6, 0, u^6, u^{13}, u^6, 0)$,
$(u^{13}, u^6, 0, u^6, u^6, 0, u^6)$, $(u^{13}, u^6, 0, u^{13}, 0, u^6, u^{13})$,
$(u^{13}, u^6, 1, 1, u^6, u^{13}, u^{13})$, $(u^{13}, 0, u^6, u^{13}, u^{13}, u^6, 0)$,
$(u^6, 0, u^6, u^{13}, u^6, 0, u^6)$, $(u^6, 0, u^6, u^6, 0, u^6, u^{13})$,
$(u^6, 0, u^{13}, 0, u^6, u^{13}, u^{13})$, $(u^6, 1, 1, u^6, u^{13}, u^{13}, u^{13})$,
$(1, u^6, u^{13}, u^{13}, u^{13}, u^6, 1)$, $(0, u^6, u^{13}, u^{13}, u^6, 0, u^{13})$,
$(0, u^6, u^{13}, u^6, 0, u^6, u^6)$, $(0, u^6, u^6, 0, u^6, u^{13}, u^6)$,
$(0, u^{13}, 0, u^6, u^{13}, u^{13}, u^6)$, $(1, 1, u^6, u^{13}, u^{13}, u^{13}, u^6)$,
$(u^{13}, u^6, u^6, u^6, u^6, u^{13}, 1)$, $(u^6, u^6, u^6, u^6, u^{13}, 1, u^{13})$,

$(u^6, u^6, u^6, u^{13}, 1, u^{13}, u^6)$, $(u^6, u^6, u^{13}, 1, u^{13}, u^6, u^6)$,
$(u^6, u^{13}, 1, u^{13}, u^6, u^6, u^6)$, $(u^{13}, 1, u^{13}, u^6, u^6, u^6, u^6)$,
$(1, u^{13}, u^6, u^6, u^6, u^6, u^{13})$,
$(u^{13}, u^{13}, u^{13}, u^{13}, u^{13}, u^{13}, u^{13})$

Örnek 4 :

$$C = (u^6 + (u^5\, x^2 + u^7\, x^3 + u^9\, x^4 + u^{12}\, x^5),$$
$$(1 + x + x^2 + x^3 + x^4 + x^5 + x^6))$$

kodunun elemanları aşağıdaki gibidir.

```
PadRight[
  CoefficientList[
    Expand[i * (u^6 + (u^5) * x^2 + (u^7) * x^3 + (u^9) x^4 + (u^12) x^5)] /.
                                          u^4 → u^4  /. u^5 → u^2 + u  /.
                                          u^6 → u^3 + u^2  /.
                                        u^7 → u^3 + u + 1  /.
                                      u^8 → u^2 + 1  /. u^9 → u^3 + u  /.
                                  u^10 → u^2 + u + 1  /. u^11 → u^3 + u^2 + u
                               /. u^12 → u^3 + u^2 + u + 1
                           /. u^13 → u^3 + u^2 + 1
                         /. u^14 → u^3 + 1
                       /.  x^7 → 1  /. x^8 → x  /. x^9 → x^2  /.
                 x^10 → x^3  /. x^11 → x^4  /. x^12 → x^5  /.
          x^13 → x^6  /. x^14 → x^7 , x, Modulus → 2], {128, 7}]
```

```
PadRight[
  CoefficientList[
    Expand[i * (u^6 + (u^5) * x^2 + (u^7) * x^3 + (u^9) x^4 + (u^12) x^5) +
                                          (1 + x + x^2 + x^3 + x^4 +
                                          x^5 + x^6)] /. u^4 → u^4  /.
                                          u^5 → u^2 + u  /.
                                          u^6 → u^3 + u^2  /.
                                        u^7 → u^3 + u + 1  /.
                                      u^8 → u^2 + 1  /. u^9 → u^3 + u  /.
                                  u^10 → u^2 + u + 1  /. u^11 → u^3 + u^2 + u
                               /. u^12 → u^3 + u^2 + u + 1
                           /. u^13 → u^3 + u^2 + 1
                         /. u^14 → u^3 + 1
                       /.  x^7 → 1  /. x^8 → x  /. x^9 → x^2  /.
                 x^10 → x^3  /. x^11 → x^4  /. x^12 → x^5  /.
          x^13 → x^6  /. x^14 → x^7 , x, Modulus → 2], {128, 7}]
```

$(0, 0, 0, 0, 0, 0, 0)$, $(u^6, 0, u^5, u^7, u^9, u^{12}, 0)$, $(0, u^6, 0, u^5, u^7, u^9, u^{12})$,
$(u^{12}, 0, u^6, 0, u^5, u^7, u^9)$, $(u^9, u^{12}, 0, u^6, 0, u^5, u^7)$,
$(u^7, u^9, u^{12}, 0, u^6, 0, u^5)$, $(u^5, u^7, u^9, u^{12}, 0, u^6, 0)$,
$(0, u^5, u^7, u^9, u^{12}, 0, u^6)$, $(u^6, u^6, u^5, u^{13}, 1, u^8, u^{12})$,
$(u^{12}, u^6, u^6, u^5, u^{13}, 1, u^8)$, $(u^8, u^{12}, u^6, u^6, u^5, u^{13}, 1)$,
$(1, u^8, u^{12}, u^6, u^6, u^5, u^{13})$, $(u^{13}, 1, u^8, u^{12}, u^6, u^6, u^5)$,
$(u^5, u^{13}, 1, u^8, u^{12}, u^6, u^6)$, $(u^4, 0, u^9, u^7, u^6, u^2, u^9)$,
$(u^5, u^{12}, u^5, u^{10}, u^9, u^{14}, u^7)$, $(u^{10}, u^9, u^{14}, u^7, u^5, u^{12}, u^5)$,
$(u^9, u^7, u^6, u^2, u^9, u^4, 0)$, $(u^6, u^5, u^{13}, 1, u^8, u^{12}, u^6)$,
$(0, u^9, u^7, u^6, u^2, u^9, u^4)$, $(u^{12}, u^5, u^{10}, u^9, u^{14}, u^7, u^5)$,
$(u^9, u^{14}, u^7, u^5, u^{12}, u^5, u^{10})$, $(u^7, u^6, u^2, u^9, u^4, 0, u^9)$,
$(u^6, u^2, u^9, u^4, 0, u^9, u^7)$, $(u^2, u^9, u^4, 0, u^9, u^7, u^6)$,
$(u^9, u^4, 0, u^9, u^7, u^6, u^2)$, $(u^7, u^5, u^{12}, u^5, u^{10}, u^9, u^{14})$,
$(u^5, u^{10}, u^9, u^{14}, u^7, u^5, u^{12})$, $(u^{14}, u^7, u^5, u^{12}, u^5, u^{10}, u^9)$,
$(u^4, u^6, u^9, u^{13}, u^{10}, u^{11}, u^8)$, $(u^5, u^4, u^5, 1, 1, u^4, u^2)$,
$(u^{10}, u^5, u^{14}, u^{13}, u^{13}, u^8, u^{14})$, $(u^9, u^{10}, u^6, u, 1, u^{14}, u^{12})$,
$(u^6, u^9, u^{13}, u^{10}, u^{11}, u^8, u^4)$, $(u^{14}, u^{12}, u^9, u^{10}, u^6, u, 1)$,
$(u^3, u^9, u^8, u^7, 0, u^2, u^6)$, $(u^8, u^7, 0, u^2, u^6, u^3, u^9)$,
$(u^4, u^5, 1, 1, u^4, u^2, u^5)$, $(u^{13}, u^8, u^{14}, u^{10}, u^5, u^{14}, u^{13})$,
$(0, u^2, u^6, u^3, u^9, u^8, u^7)$, $(u^5, u^{14}, u^{13}, u^{13}, u^8, u^{14}, u^{10})$,
$(1, 1, u^4, u^2, u^5, u^4, u^5)$, $(u^{10}, u^6, u, 1, u^{14}, u^{12}, u^9)$,
$(u^9, u^{13}, u^{10}, u^{11}, u^8, u^4, u^6)$, $(u^8, u^4, u^6, u^9, u^{13}, u^{10}, u^{11})$,
$(u^2, u^5, u^4, u^5, 1, 1, u^4)$, $(u^{14}, u^{10}, u^5, u^{14}, u^{13}, u^{13}, u^8)$,
$(u^{12}, u^9, u^{10}, u^6, u, 1, u^{14})$, $(1, u^{14}, u^{12}, u^9, u^{10}, u^6, u)$,
$(u^6, u^3, u^9, u^8, u^7, 0, u^2)$, $(u^9, u^8, u^7, 0, u^2, u^6, u^3)$,
$(u^{13}, u^{13}, u^8, u^{14}, u^{10}, u^5, u^{14})$, $(u^7, 0, u^2, u^6, u^3, u^9, u^8)$,
$(u^5, 1, 1, u^4, u^2, u^5, u^4)$, $(u^{13}, u^{10}, u^{11}, u^8, u^4, u^6, u^9)$,
$(u^6, u, 1, u^{14}, u^{12}, u^9, u^{10})$, $(1, u^4, u^2, u^5, u^4, u^5, 1)$,
$(u^{10}, u^{11}, u^8, u^4, u^6, u^9, u^{13})$, $(u^{14}, u^{13}, u^{13}, u^8, u^{14}, u^{10}, u^5)$,
$(u^2, u^6, u^3, u^9, u^8, u^7, 0)$, $(u, 1, u^{14}, u^{12}, u^9, u^{10}, u^6)$,
$(u^8, u^{14}, u^{10}, u^5, u^{14}, u^{13}, u^{13})$, $(u^4, u^2, u^5, u^4, u^5, 1, 1)$,
$(u^{11}, u^8, u^4, u^6, u^9, u^{13}, u^{10})$, $(u^{14}, u^4, u^9, 1, u^{10}, u^3, u^{11})$,
$(u^3, u^5, u^8, u^{13}, u^7, u^{11}, u^4)$, $(u^8, u^{10}, 0, u, u^{10}, u, u^8)$,
$(u^4, u^9, 1, u^{10}, u^3, u^{11}, u^{14})$, $(u^{13}, u^{14}, u^{14}, 1, u^{13}, u^4, u)$,
$(0, u^3, u^6, u^{11}, 1, u^{12}, u^2)$, $(u^5, u^8, u^{13}, u^7, u^{11}, u^4, u^3)$,
$(1, u^{13}, u^4, u, u^{13}, u^{14}, u^{14})$, $(u^{10}, 0, u, u^{10}, u, u^8, u^8)$,
$(u^9, 1, u^{10}, u^3, u^{11}, u^{14}, u^4)$, $(u, u^8, u^8, u^{10}, 0, u, u^{10})$,
$(u^{12}, u^2, 0, u^3, u^6, u^{11}, 1)$, $(u^{14}, u^{14}, 1, u^{13}, u^4, u, u^{13})$,
$(u^{11}, 1, u^{12}, u^2, 0, u^3, u^6)$, $(u^3, u^6, u^{11}, 1, u^{12}, u^2, 0)$,
$(u^8, u^{13}, u^7, u^{11}, u^4, u^3, u^5)$, $(u^7, u^{11}, u^4, u^3, u^5, u^8, u^{13})$,

$(u^{13}, u^4, u, u^{13}, u^{14}, u^{14}, 1)$, $(0, u, u^{10}, u, u^8, u^8, u^{10})$,
$(1, u^{10}, u^3, u^{11}, u^{14}, u^4, u^9)$, $(u^{11}, u^{14}, u^4, u^9, 1, u^{10}, u^3)$,
$(u^4, u^3, u^5, u^8, u^{13}, u^7, u^{11})$, $(u^8, u^8, u^{10}, 0, u, u^{10}, u)$,
$(u, u^{13}, u^{14}, u^{14}, 1, u^{13}, u^4)$, $(u^2, 0, u^3, u^6, u^{11}, 1, u^{12})$,
$(u^{14}, 1, u^{13}, u^4, u, u^{13}, u^{14})$, $(u^{10}, u, u^8, u^8, u^{10}, 0, u)$,
$(1, u^{12}, u^2, 0, u^3, u^6, u^{11})$, $(u^6, u^{11}, 1, u^{12}, u^2, 0, u^3)$,
$(u^{13}, u^7, u^{11}, u^4, u^3, u^5, u^8)$, $(u^3, u^{11}, u^{14}, u^4, u^9, 1, u^{10})$,
$(u^{11}, u^4, u^3, u^5, u^8, u^{13}, u^7)$, $(u^4, u, u^{13}, u^{14}, u^{14}, 1, u^{13})$,
$(u, u^{10}, u, u^8, u^8, u^{10}, 0)$, $(u^{10}, u^3, u^{11}, u^{14}, u^4, u^9, 1)$,
$(u, u^{14}, u^8, 1, u^7, u^3, u^3)$, $(u^{12}, u^3, 0, u^{11}, u^{10}, u^2, u^{11})$,
$(u^{14}, u^8, 1, u^7, u^3, u^3, u)$, $(u^{11}, u^{13}, u^{12}, u, u^7, u, u^4)$,
$(u^3, 0, u^{11}, u^{10}, u^2, u^{11}, u^{12})$, $(u^8, 1, u^7, u^3, u^3, u, u^{14})$,
$(u^7, u, u^4, u^{11}, u^{13}, u^{12}, u)$, $(u^{13}, u^{12}, u, u^7, u, u^4, u^{11})$,
$(0, u^{11}, u^{10}, u^2, u^{11}, u^{12}, u^3)$, $(1, u^7, u^3, u^3, u, u^{14}, u^8)$,
$(u^2, u^{11}, u^{12}, u^3, 0, u^{11}, u^{10})$, $(u, u^4, u^{11}, u^{13}, u^{12}, u, u^7)$,
$(u^{12}, u, u^7, u, u^4, u^{11}, u^{13})$, $(u^{11}, u^{10}, u^2, u^{11}, u^{12}, u^3, 0)$,
$(u^7, u^3, u^3, u, u^{14}, u^8, 1)$, $(u^3, u, u^{14}, u^8, 1, u^7, u^3)$,
$(u^{11}, u^{12}, u^3, 0, u^{11}, u^{10}, u^2)$, $(u^4, u^{11}, u^{13}, u^{12}, u, u^7, u)$,
$(u, u^7, u, u^4, u^{11}, u^{13}, u^{12})$, $(u^{10}, u^2, u^{11}, u^{12}, u^3, 0, u^{11})$,
$(u^3, u^3, u, u^{14}, u^8, 1, u^7)$, $(u^2, u, u^{12}, u^{11}, u^7, u^2, u^3)$,
$(u, u^{12}, u^{11}, u^7, u^2, u^3, u^2)$, $(u^{12}, u^{11}, u^7, u^2, u^3, u^2, u)$,
$(u^{11}, u^7, u^2, u^3, u^2, u, u^{12})$, $(u^7, u^2, u^3, u^2, u, u^{12}, u^{11})$,
$(u^2, u^3, u^2, u, u^{12}, u^{11}, u^7)$, $(u^3, u^2, u, u^{12}, u^{11}, u^7, u^2)$,
$(u^2, u^2, u^2, u^2, u^2, u^2, u^2)$, $(1, 1, 1, 1, 1, 1, 1)$, $(u^{13}, 1, u^{10}, u^9, u^7, u^{11}, 1)$,
$(1, u^{13}, 1, u^{10}, u^9, u^7, u^{11})$, $(u^{11}, 1, u^{13}, 1, u^{10}, u^9, u^7)$,
$(u^7, u^{11}, 1, u^{13}, 1, u^{10}, u^9)$, $(u^9, u^7, u^{11}, 1, u^{13}, 1, u^{10})$,
$(u^{10}, u^9, u^7, u^{11}, 1, u^{13}, 1)$, $(1, u^{10}, u^9, u^7, u^{11}, 1, u^{13})$,
$(u^{13}, u^{13}, u^{10}, u^6, 0, u^2, u^{11})$, $(u^{11}, u^{13}, u^{13}, u^{10}, u^6, 0, u^2)$,
$(u^2, u^{11}, u^{13}, u^{13}, u^{10}, u^6, 0)$, $(0, u^2, u^{11}, u^{13}, u^{13}, u^{10}, u^6)$,
$(u^6, 0, u^2, u^{11}, u^{13}, u^{13}, u^{10})$, $(u^{10}, u^6, 0, u^2, u^{11}, u^{13}, u^{13})$,
$(u, 1, u^7, u^9, u^{13}, u^8, u^7)$, $(u^{10}, u^{11}, u^{10}, u^5, u^7, u^3, u^9)$,
$(u^5, u^7, u^3, u^9, u^{10}, u^{11}, u^{10})$, $(u^7, u^9, u^{13}, u^8, u^7, u, 1)$,
$(u^{13}, u^{10}, u^6, 0, u^2, u^{11}, u^{13})$, $(1, u^7, u^9, u^{13}, u^8, u^7, u)$,
$(u^{11}, u^{10}, u^5, u^7, u^3, u^9, u^{10})$, $(u^7, u^3, u^9, u^{10}, u^{11}, u^{10}, u^5)$,
$(u^9, u^{13}, u^8, u^7, u, 1, u^7)$, $(u^{13}, u^8, u^7, u, 1, u^7, u^9)$,
$(u^8, u^7, u, 1, u^7, u^9, u^{13})$, $(u^7, u, 1, u^7, u^9, u^{13}, u^8)$,
$(u^9, u^{10}, u^{11}, u^{10}, u^5, u^7, u^3)$, $(u^{10}, u^5, u^7, u^3, u^9, u^{10}, u^{11})$,
$(u^3, u^9, u^{10}, u^{11}, u^{10}, u^5, u^7)$, $(u, u^{13}, u^7, u^6, u^5, u^{12}, u^2)$,
$(u^{10}, u, u^{10}, 0, 0, u, u^8)$, $(u^5, u^{10}, u^3, u^6, u^6, u^2, u^3)$,
$(u^7, u^5, u^{13}, u^4, 0, u^3, u^{11})$, $(u^{13}, u^7, u^6, u^5, u^{12}, u^2, u)$,

$(u^3, u^{11}, u^7, u^5, u^{13}, u^4, 0), (u^{14}, u^7, u^2, u^9, 1, u^8, u^{13}),$
$(u^2, u^9, 1, u^8, u^{13}, u^{14}, u^7), (u, u^{10}, 0, 0, u, u^8, u^{10}),$
$(u^6, u^2, u^3, u^5, u^{10}, u^3, u^6), (1, u^8, u^{13}, u^{14}, u^7, u^2, u^9),$
$(u^{10}, u^3, u^6, u^6, u^2, u^3, u^5), (0, 0, u, u^8, u^{10}, u, u^{10}),$
$(u^5, u^{13}, u^4, 0, u^3, u^{11}, u^7), (u^7, u^6, u^5, u^{12}, u^2, u, u^{13}),$
$(u^2, u, u^{13}, u^7, u^6, u^5, u^{12}), (u^8, u^{10}, u, u^{10}, 0, 0, u),$
$(u^3, u^5, u^{10}, u^3, u^6, u^6, u^2), (u^{11}, u^7, u^5, u^{13}, u^4, 0, u^3),$
$(0, u^3, u^{11}, u^7, u^5, u^{13}, u^4), (u^{13}, u^{14}, u^7, u^2, u^9, 1, u^8),$
$(u^7, u^2, u^9, 1, u^8, u^{13}, u^{14}), (u^6, u^6, u^2, u^3, u^5, u^{10}, u^3),$
$(u^9, 1, u^8, u^{13}, u^{14}, u^7, u^2), (u^{10}, 0, 0, u, u^8, u^{10}, u),$
$(u^6, u^5, u^{12}, u^2, u, u^{13}, u^7), (u^{13}, u^4, 0, u^3, u^{11}, u^7, u^5),$
$(0, u, u^8, u^{10}, u, u^{10}, 0), (u^5, u^{12}, u^2, u, u^{13}, u^7, u^6),$
$(u^3, u^6, u^6, u^2, u^3, u^5, u^{10}), (u^8, u^{13}, u^{14}, u^7, u^2, u^9, 1),$
$(u^4, 0, u^3, u^{11}, u^7, u^5, u^{13}), (u^2, u^3, u^5, u^{10}, u^3, u^6, u^6),$
$(u, u^8, u^{10}, u, u^{10}, 0, 0), (u^{12}, u^2, u, u^{13}, u^7, u^6, u^5),$
$(u^3, u, u^7, 0, u^5, u^{14}, u^{12}), (u^{14}, u^{10}, u^2, u^6, u^9, u^{12}, u),$
$(u^2, u^5, 1, u^4, u^5, u^4, u^2), (u, u^7, 0, u^5, u^{14}, u^{12}, u^3),$
$(u^6, u^3, u^3, 0, u^6, u, u^4), (1, u^{14}, u^{13}, u^{12}, 0, u^{11}, u^8),$
$(u^{10}, u^2, u^6, u^9, u^{12}, u, u^{14}), (0, u^6, u, u^4, u^6, u^3, u^3),$
$(u^5, 1, u^4, u^5, u^4, u^2, u^2), (u^7, 0, u^5, u^{14}, u^{12}, u^3, u),$
$(u^4, u^2, u^2, u^5, 1, u^4, u^5), (u^{11}, u^8, 1, u^{14}, u^{13}, u^{12}, 0),$
$(u^3, u^3, 0, u^6, u, u^4, u^6), (u^{12}, 0, u^{11}, u^8, 1, u^{14}, u^{13}),$
$(u^{14}, u^{13}, u^{12}, 0, u^{11}, u^8, 1), (u^2, u^6, u^9, u^{12}, u, u^{14}, u^{10}),$
$(u^9, u^{12}, u, u^{14}, u^{10}, u^2, u^6), (u^6, u, u^4, u^6, u^3, u^3, 0),$
$(1, u^4, u^5, u^4, u^2, u^2, u^5), (0, u^5, u^{14}, u^{12}, u^3, u, u^7),$
$(u^{12}, u^3, u, u^7, 0, u^5, u^{14}), (u, u^{14}, u^{10}, u^2, u^6, u^9, u^{12}),$
$(u^2, u^2, u^5, 1, u^4, u^5, u^4), (u^4, u^6, u^3, u^3, 0, u^6, u),$
$(u^8, 1, u^{14}, u^{13}, u^{12}, 0, u^{11}), (u^3, 0, u^6, u, u^4, u^6, u^3),$
$(u^5, u^4, u^2, u^2, u^5, 1, u^4), (0, u^{11}, u^8, 1, u^{14}, u^{13}, u^{12}),$
$(u^{13}, u^{12}, 0, u^{11}, u^8, 1, u^{14}), (u^6, u^9, u^{12}, u, u^{14}, u^{10}, u^2),$
$(u^{14}, u^{12}, u^3, u, u^7, 0, u^5), (u^{12}, u, u^{14}, u^{10}, u^2, u^6, u^9),$
$(u, u^4, u^6, u^3, u^3, 0, u^6), (u^4, u^5, u^4, u^2, u^2, u^5, 1),$
$(u^5, u^{14}, u^{12}, u^3, u, u^7, 0), (u^4, u^3, u^2, 0, u^9, u^{14}, u^{14}),$
$(u^{11}, u^{14}, 1, u^{12}, u^5, u^8, u^{12}), (u^3, u^2, 0, u^9, u^{14}, u^{14}, u^4),$
$(u^{12}, u^6, u^{11}, u^4, u^9, u^4, u), (u^{14}, 1, u^{12}, u^5, u^8, u^{12}, u^{11}),$
$(u^2, 0, u^9, u^{14}, u^{14}, u^4, u^3), (u^9, u^4, u, u^{12}, u^6, u^{11}, u^4),$
$(u^6, u^{11}, u^4, u^9, u^4, u, u^{12}), (1, u^{12}, u^5, u^8, u^{12}, u^{11}, u^{14}),$
$(0, u^9, u^{14}, u^{14}, u^4, u^3, u^2), (u^8, u^{12}, u^{11}, u^{14}, 1, u^{12}, u^5),$
$(u^4, u, u^{12}, u^6, u^{11}, u^4, u^9), (u^{11}, u^4, u^9, u^4, u, u^{12}, u^6),$
$(u^{12}, u^5, u^8, u^{12}, u^{11}, u^{14}, 1), (u^9, u^{14}, u^{14}, u^4, u^3, u^2, 0),$

$(u^{14}, u^4, u^3, u^2, 0, u^9, u^{14})$, $(u^{12}, u^{11}, u^{14}, 1, u^{12}, u^5, u^8)$,
$(u, u^{12}, u^6, u^{11}, u^4, u^9, u^4)$, $(u^4, u^9, u^4, u, u^{12}, u^6, u^{11})$,
$(u^5, u^8, u^{12}, u^{11}, u^{14}, 1, u^{12})$, $(u^{14}, u^{14}, u^4, u^3, u^2, 0, u^9)$,
$(u^8, u^4, u^{11}, u^{12}, u^9, u^8, u^{14})$, $(u^4, u^{11}, u^{12}, u^9, u^8, u^{14}, u^8)$,
$(u^{11}, u^{12}, u^9, u^8, u^{14}, u^8, u^4)$, $(u^{12}, u^9, u^8, u^{14}, u^8, u^4, u^{11})$,
$(u^9, u^8, u^{14}, u^8, u^4, u^{11}, u^{12})$, $(u^8, u^{14}, u^8, u^4, u^{11}, u^{12}, u^9)$,
$(u^{14}, u^8, u^4, u^{11}, u^{12}, u^9, u^8)$,
$(u^8, u^8, u^8, u^8, u^8, u^8, u^8)$

Örnek 5

```
PadRight[
  CoefficientList[
    Expand[i * (u^7 + (u^6) x + (u^6) x^4 + (u^7) x^5)] /.
                                        u^4 → 1 + u /. u^5 → u^2 + u /.
                                      u^6 → u^3 + u^2 /. u^7 →
                                      u^3 + u + 1 /. u^8 → u^2 + 1 /.
                                  u^9 → u^3 + u /. u^10 → u^2 + u + 1 /.
                               u^11 → u^3 + u^2 + u /.
                              u^12 → u^3 + u^2 + u + 1
                             /. u^13 → u^3 + u^2 + 1
                             /. u^14 → u^3 + 1
                             /. x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
                         x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
        x^13 → x^6 /. x^14 → x^7 , x, Modulus → 2],
  {128, 7}]
```

```
{{0, 0, 0, 0, 0, 0, 0},
  {1 + u + u^3, u^2 + u^3, 0, 0, u^2 + u^3, 1 + u + u^3, 0},
  {0, 1 + u + u^3, u^2 + u^3, 0, 0, u^2 + u^3, 1 + u + u^3},
  {1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3, 0, 0, u^2 + u^3},
  {u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3, 0, 0},
  {0, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3, 0},
  {0, 0, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3},
  {u^2 + u^3, 0, 0, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3},
  {1 + u + u^3, 1 + u + u^2, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^2,
   1 + u + u^3}, {1 + u + u^3, 1 + u + u^3, 1 + u + u^2,
   u^2 + u^3, 0, u^2 + u^3, 1 + u + u^2}, {1 + u + u^2,
   1 + u + u^3, 1 + u + u^3, 1 + u + u^2, u^2 + u^3, 0, u^2 + u^3},
  {u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2,
   u^2 + u^3, 0}, {0, u^2 + u^3, 1 + u + u^2, 1 + u + u^3,
   1 + u + u^3, 1 + u + u^2, u^2 + u^3}, {u^2 + u^3, 0, u^2 + u^3,
   1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2},
  {0, u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3},
  {1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3, 0, 1 + u + u^3, 0},
  {1 + u + u^3, 0, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2, 0},
  {1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0, u^2 + u^3},
  {1 + u + u^2, u^2 + u^3, 0, u^2 + u^3,
```

$1 + u + u^2, 1 + u + u^3, 1 + u + u^3\}$,
$\{u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0\}$,
$\{1 + u + u^2, 0, 1 + u + u^3, 0, 1 + u + u^3, 0, 1 + u + u^2\}$,
$\{0, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3\}$,
$\{u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3\}$,
$\{u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3, u^2 + u^3\}$,
$\{1 + u + u^3, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3\}$,
$\{u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3\}$,
$\{0, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3, 0, 1 + u + u^3\}$,
$\{0, 1 + u + u^3, 0, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2\}$,
$\{1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3, 0\}$,
$\{0, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^2,$
$1 + u + u^2\}, \{1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^3, 0,$
$1 + u + u^2, 1 + u + u^3\}, \{1 + u + u^3, 1 + u + u^3, 1 + u + u^2, 0,$
$1 + u + u^2, 1 + u + u^3, 1 + u + u^3\}, \{1 + u + u^3, 1 + u + u^2,$
$0, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^2\}, \{1 + u + u^2,$
$1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, 0\}$,
$\{u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^3,$
$u^2 + u^3\}, \{0, 0, 0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3\}$,
$\{0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0, 0\}$,
$\{u^2 + u^3, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^2,$
$1 + u + u^3, 1 + u + u^2\}, \{1 + u + u^2, 1 + u + u^3,$
$1 + u + u^3, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2, 0\}$,
$\{1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0, 0, 0, u^2 + u^3\}, \{1 + u + u^3,$
$1 + u + u^2, 0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3\}$,
$\{1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2, u^2 + u^3,$
$u^2 + u^3\}, \{1 + u + u^2, 0, 1 + u + u^3, u^2 + u^3, u^2 + u^3,$
$1 + u + u^2, 1 + u + u^3\}, \{1 + u + u^2, u^2 + u^3, u^2 + u^3,$
$1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^2\}, \{1 + u + u^2, 0,$
$1 + u + u^2, 1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^2\}$,
$\{1 + u + u^3, 1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^3, 0,$
$1 + u + u^2\}, \{1 + u + u^3, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2,$
$0, 1 + u + u^2, 1 + u + u^3\}, \{1 + u + u^2, 1 + u + u^3,$
$1 + u + u^2, 0, 1 + u + u^3, u^2 + u^3, u^2 + u^3\}, \{u^2 + u^3,$
$u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^3\}$,
$\{u^2 + u^3, 0, 0, 0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2\}$,
$\{0, 0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0\}$,
$\{0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3,$
$1 + u + u^2\}, \{u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0, 0, 0\}$,
$\{u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2,$

$u^2 + u^3\}$, $\{u^2 + u^3, u^2 + u^3, 1 + u + u^2, 1 + u + u^2,$
$0, 1 + u + u^2, 1 + u + u^2\}$, $\{0, 1 + u + u^3, u^2 + u^3,$
$u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2\}$,
$\{0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2, u^2 + u^3, u^2 + u^3,$
$1 + u + u^3\}$, $\{u^2 + u^3, 1 + u + u^2, 1 + u + u^2, 0,$
$1 + u + u^2, 1 + u + u^2, u^2 + u^3\}$, $\{1 + u + u^2, 0,$
$1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3\}$,
$\{1 + u + u^2, u^2 + u^3, 0, 0, 0, u^2 + u^3, 1 + u + u^2\}$,
$\{1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^2, 1 + u + u^3,$
$1 + u + u^2, 0\}$, $\{1 + u + u^3, 1 + u + u^3, 1 + u + u^3,$
$1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^2\}$, $\{1 + u + u^2,$
$1 + u + u^3, 1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^3, 0\}$,
$\{1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^2, 1 + u + u^2,$
$u^2 + u^3, u^2 + u^3\}$, $\{u^2 + u^3, u^2 + u^3, 1 + u + u^2,$
$1 + u + u^2, 0, 1 + u + u^2, 1 + u + u^2\}$, $\{0, 1 + u + u^3,$
$u^2 + u^3, u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2\}$,
$\{0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2, u^2 + u^3, u^2 + u^3,$
$1 + u + u^3\}$, $\{u^2 + u^3, 1 + u + u^2, 1 + u + u^2, 0,$
$1 + u + u^2, 1 + u + u^2, u^2 + u^3\}$, $\{1 + u + u^2, 0,$
$1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3\}$,
$\{1 + u + u^2, u^2 + u^3, 0, 0, 0, u^2 + u^3, 1 + u + u^2\}$,
$\{1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^2,$
$1 + u + u^3, 1 + u + u^2, 0\}$, $\{1 + u + u^3, 1 + u + u^3,$
$1 + u + u^3, 1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^2\}$,
$\{1 + u + u^2, 1 + u + u^3, 1 + u + u^2, u^2 + u^3, u^2 + u^3,$
$1 + u + u^3, 0\}$, $\{1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^2,$
$1 + u + u^2, u^2 + u^3, u^2 + u^3\}$, $\{u^2 + u^3, 1 + u + u^3,$
$0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2, u^2 + u^3\}$,
$\{u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0, 0, 0\}$,
$\{0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3,$
$1 + u + u^2\}$, $\{0, 0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0\}$,
$\{u^2 + u^3, 0, 0, 0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2\}$,
$\{u^2 + u^3, u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2,$
$0, 1 + u + u^3\}$, $\{1 + u + u^2, 1 + u + u^3, 1 + u + u^2, 0,$
$1 + u + u^3, u^2 + u^3, u^2 + u^3\}$, $\{1 + u + u^3, 1 + u + u^3,$
$1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^2, 1 + u + u^3\}$,
$\{1 + u + u^3, 1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^3, 0,$
$1 + u + u^2\}$, $\{1 + u + u^2, 0, 1 + u + u^2, 1 + u + u^2,$
$u^2 + u^3, u^2 + u^3, 1 + u + u^2\}$, $\{1 + u + u^2, u^2 + u^3,$
$u^2 + u^3, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^2\}$,

$\{1 + u + u^2, 0, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^2,$
$1 + u + u^3\}, \{1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^3,$
$1 + u + u^2, u^2 + u^3, u^2 + u^3\}, \{1 + u + u^3, 1 + u + u^2,$
$0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3\},$
$\{1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0, 0, 0, u^2 + u^3\},$
$\{1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^3,$
$1 + u + u^3, 1 + u + u^2, 0\}, \{u^2 + u^3, u^2 + u^3,$
$1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^2\},$
$\{0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3, 0, 0\},$
$\{0, 0, 0, u^2 + u^3, 1 + u + u^2, 1 + u + u^2, u^2 + u^3\}, \{u^2 + u^3,$
$1 + u + u^2, 1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^3, u^2 + u^3\},$
$\{1 + u + u^2, 1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^2,$
$1 + u + u^2, 0\}, \{1 + u + u^3, 1 + u + u^2, 0, 1 + u + u^3,$
$u^2 + u^3, u^2 + u^3, 1 + u + u^2\}, \{1 + u + u^3, 1 + u + u^3,$
$1 + u + u^2, 0, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3\},$
$\{1 + u + u^2, u^2 + u^3, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^2,$
$1 + u + u^3\}, \{0, 1 + u + u^2, 1 + u + u^2, u^2 + u^3,$
$u^2 + u^3, 1 + u + u^2, 1 + u + u^2\}, \{u^2 + u^3, 0, u^2 + u^3,$
$1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2\},$
$\{u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3\},$
$\{0, u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2,$
$u^2 + u^3\}, \{0, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3\},$
$\{u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3, u^2 + u^3\},$
$\{u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3, 1 + u + u^2, u^2 + u^3,$
$0\}, \{1 + u + u^2, 0, 1 + u + u^3, 0, 1 + u + u^3, 0, 1 + u + u^2\},$
$\{1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3, 0\},$
$\{1 + u + u^3, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3\},$
$\{1 + u + u^2, 1 + u + u^3, 1 + u + u^3,$
$1 + u + u^2, u^2 + u^3, 0, u^2 + u^3\},$
$\{u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0\},$
$\{0, 1 + u + u^3, 0, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2\},$
$\{0, 1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3, 0, 1 + u + u^3\},$
$\{u^2 + u^3, 0, u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3\},$
$\{1 + u + u^3, 1 + u + u^3, 1 + u + u^2, u^2 + u^3,$
$0, u^2 + u^3, 1 + u + u^2\}, \{1 + u + u^2, u^2 + u^3,$
$0, u^2 + u^3, 1 + u + u^2, 1 + u + u^3, 1 + u + u^3\},$
$\{1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3, 0, u^2 + u^3\},$
$\{1 + u + u^3, 0, 1 + u + u^3, 0, 1 + u + u^2, 1 + u + u^2, 0\},$
$\{1 + u + u^2, 1 + u + u^2, 0, 1 + u + u^3, 0, 1 + u + u^3, 0\},$
$\{0, u^2 + u^3, 1 + u + u^3, u^2 + u^3, u^2 + u^3, 1 + u + u^3, u^2 + u^3\},$

```
  {1 + u + u^3, 1 + u + u^2, u^2 + u^3, 0, u^2 + u^3, 1 + u + u^2,
    1 + u + u^3}, {u^2 + u^3, 0, 0, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3},
  {0, 0, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3},
  {0, u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3, 0},
  {u^2 + u^3, 1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3, 0, 0},
  {1 + u + u^3, 0, 1 + u + u^3, u^2 + u^3, 0, 0, u^2 + u^3},
  {0, 1 + u + u^3, u^2 + u^3, 0, 0, u^2 + u^3, 1 + u + u^3},
  {1 + u + u^3, u^2 + u^3, 0, 0, u^2 + u^3, 1 + u + u^3, 0},
  {0, 0, 0, 0, 0, 0, 0}}
```

```
PadRight[
  CoefficientList[
    Expand[i ∗ (u^12 + (u^8) x^2 + (u^12) x^4)] /. u^4 → 1 + u  /.
                              u^5 → u^2 + u  /.
                            u^6 → u^3 + u^2  /. u^7 →
                            u^3 + u + 1  /. u^8 → u^2 + 1  /.
                        u^9 → u^3 + u  /. u^10 → u^2 + u + 1  /.
                    u^11 → u^3 + u^2 + u /.
                  u^12 → u^3 + u^2 + u + 1
                 /. u^13 → u^3 + u^2 + 1
                 /. u^14 → u^3 + 1
                 /.  x^7 → 1  /. x^8 → x  /. x^9 → x^2  /.
             x^10 → x^3  /. x^11 → x^4  /. x^12 → x^5  /.
       x^13 → x^6  /. x^14 → x^7 , x, Modulus → 2],
  {128, 7}]
```

```
{{0, 0, 0, 0, 0, 0, 0},
  {1 + u + u^2 + u^3, 0, 1 + u^2, 0, 1 + u + u^2 + u^3, 0, 0},
  {0, 1 + u + u^2 + u^3, 0, 1 + u^2, 0, 1 + u + u^2 + u^3, 0},
  {0, 0, 1 + u + u^2 + u^3, 0, 1 + u^2, 0, 1 + u + u^2 + u^3},
  {1 + u + u^2 + u^3, 0, 0, 1 + u + u^2 + u^3, 0, 1 + u^2, 0},
  {0, 1 + u + u^2 + u^3, 0, 0, 1 + u + u^2 + u^3, 0, 1 + u^2},
  {1 + u^2, 0, 1 + u + u^2 + u^3, 0, 0, 1 + u + u^2 + u^3, 0},
  {0, 1 + u^2, 0, 1 + u + u^2 + u^3, 0, 0, 1 + u + u^2 + u^3},
  {1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2, 1 + u^2, 1 + u + u^2 + u^3,
    1 + u + u^2 + u^3, 0}, {0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3,
    1 + u^2, 1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3},
```

$\{1 + u + u^2 + u^3, 0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2,$
$1 + u^2, 1 + u + u^2 + u^3\}, \{1 + u + u^2 + u^3, 1 + u + u^2 + u^3,$
$0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2, 1 + u^2\},$
$\{1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 0, 1 + u + u^2 + u^3,$
$1 + u + u^2 + u^3, 1 + u^2\}, \{1 + u^2, 1 + u^2, 1 + u + u^2 + u^3,$
$1 + u + u^2 + u^3, 0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3, 0, u + u^3, 0, u + u^3, 0, 1 + u + u^2 + u^3\},$
$\{0, 0, 1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2, 0\},$
$\{1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2, 0, 0, 0, 1 + u^2\},$
$\{u + u^3, 0, u + u^3, 0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 0\},$
$\{1 + u + u^2 + u^3, 1 + u^2, 1 + u^2, 1 + u + u^2 + u^3,$
$1 + u + u^2 + u^3, 0, 1 + u + u^2 + u^3\},$
$\{0, u + u^3, 0, u + u^3, 0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$
$\{0, 1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2, 0, 0\},$
$\{1 + u + u^2 + u^3, 1 + u^2, 0, 0, 0, 1 + u^2, 1 + u + u^2 + u^3\},$
$\{0, u + u^3, 0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 0, u + u^3\},$
$\{u + u^3, 0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 0, u + u^3, 0\},$
$\{0, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 0, u + u^3, 0, u + u^3\},$
$\{1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 0, u + u^3, 0, u + u^3, 0\},$
$\{0, 0, 0, 1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2\},$
$\{1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u^2, 0, 0, 0\},$
$\{1 + u^2, 0, 0, 0, 1 + u^2, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3, 1 + u + u^2 + u^3, u + u^3,$
$1 + u^2, u + u^3, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$
$\{0, 1 + u + u^2 + u^3, 1 + u^2, u + u^3, 1 + u + u^2 + u^3, u + u^3, 0\},$
$\{1 + u + u^2 + u^3, 0, 1 + u^2, 1 + u^2, 0, 1 + u + u^2 + u^3, 1 + u^2\},$
$\{u + u^3, 1 + u + u^2 + u^3, u + u^3, 1 + u^2, 1 + u + u^2 + u^3, 0, 0\},$
$\{1 + u + u^2 + u^3, u + u^3, 1 + u^2, u + u^3,$
$1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$
$\{0, 0, u + u^3, 1 + u + u^2 + u^3, u + u^3, 1 + u^2, 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3, 1 + u + u^2 + u^3, u + u^3, 0, 1 + u^2, 0, u + u^3\},$
$\{u + u^3, 0, 1 + u^2, 0, u + u^3, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3, 1 + u^2, u + u^3, 1 + u + u^2 + u^3, u + u^3, 0, 0\},$
$\{0, 1 + u + u^2 + u^3, 1 + u^2, 1 + u + u^2 + u^3, 0, 1 + u^2, 1 + u^2\},$
$\{1 + u^2, 0, u + u^3, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3, u + u^3, 0\},$
$\{0, 1 + u^2, 1 + u^2, 0, 1 + u + u^2 + u^3, 1 + u^2, 1 + u + u^2 + u^3\},$
$\{u + u^3, 1 + u + u^2 + u^3, u + u^3, 0, 0, 1 + u + u^2 + u^3, 1 + u^2\},$
$\{1 + u + u^2 + u^3, u + u^3, 1 + u^2, 1 + u + u^2 + u^3, 0, 0, u + u^3\},$
$\{u + u^3, 1 + u^2, u + u^3, 1 + u + u^2 + u^3,$
$1 + u + u^2 + u^3, 1 + u + u^2 + u^3, 1 + u + u^2 + u^3\},$

$\{1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,$
$u + u^3,\ 1 + u^2,\ u + u^3,\ 1 + u + u^2 + u^3\},$
$\{0,\ 0,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ u + u^3,\ 1 + u + u^2 + u^3,\ u + u^3\},$
$\{1 + u^2,\ 1 + u + u^2 + u^3,\ 0,\ 1 + u^2,\ 1 + u^2,\ 0,\ 1 + u + u^2 + u^3\},$
$\{0,\ u + u^3,\ 1 + u + u^2 + u^3,\ u + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 0\},$
$\{1 + u + u^2 + u^3,\ 0,\ 0,\ u + u^3,\ 1 + u + u^2 + u^3,\ u + u^3,\ 1 + u^2\},$
$\{u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ u + u^3,\ 0,\ 1 + u^2,\ 0\},$
$\{1 + u + u^2 + u^3,\ u + u^3,\ 0,\ 1 + u^2,\ 0,\ u + u^3,\ 1 + u + u^2 + u^3\},$
$\{1 + u^2,\ 0,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 0,\ 1 + u^2\},$
$\{0,\ 1 + u^2,\ 0,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ u + u^3\},$
$\{1 + u^2,\ u + u^3,\ 1 + u + u^2 + u^3,\ u + u^3,\ 0,\ 0,\ 1 + u + u^2 + u^3\},$
$\{1 + u^2,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,$
$1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ u + u^3\},$
$\{u + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 0,\ 0,\ u + u^3,\ 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3,\ u + u^3,\ 0,\ 0,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ u + u^3\},$
$\{u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,$
$1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ u + u^3,\ 1 + u^2\},$
$\{1 + u^2,\ 1 + u^2,\ 0,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 0\},$
$\{0,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ u + u^3,\ 0,\ 1 + u^2\},$
$\{1 + u^2,\ 1 + u + u^2 + u^3,\ 0,\ 0,\ u + u^3,\ 1 + u + u^2 + u^3,\ u + u^3\},$
$\{1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 0,\ 1 + u^2,\ 1 + u^2,\ 0\},$
$\{u + u^3,\ 0,\ 0,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ u + u^3,\ 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,\ 1 + u + u^2 + u^3,$
$u + u^3,\ 1 + u^2,\ u + u^3\},\ \{0,\ 1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,$
$u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3\},\ \{1 + u + u^2 + u^3,\ 0,$
$u + u^3,\ 1 + u^2,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ u + u^3\},\ \{u + u^3,$
$1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u^2,\ u + u^3,\ 0,\ 1 + u + u^2 + u^3\},$
$\{1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,$
$0\},\ \{0,\ 0,\ 1 + u^2,\ u + u^3,\ 0,\ u + u^3,\ 1 + u^2\},\ \{1 + u^2,$
$1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 0\},$
$\{0,\ u + u^3,\ 1 + u^2,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ u + u^3,$
$1 + u + u^2 + u^3\},\ \{u + u^3,\ 0,\ u + u^3,\ 1 + u^2,\ 0,\ 0,\ 1 + u^2\},$
$\{1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u^2,\ u + u^3,\ 0,\ 1 + u + u^2 + u^3,$
$u + u^3\},\ \{u + u^3,\ u + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,$
$0,\ 1 + u + u^2 + u^3\},\ \{0,\ 1 + u + u^2 + u^3,\ u + u^3,$
$1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u^2,\ u + u^3\},\ \{1 + u^2,\ 0,$
$1 + u^2,\ 1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3\},$
$\{0,\ 1 + u^2,\ u + u^3,\ 0,\ u + u^3,\ 1 + u^2,\ 0\},\ \{u + u^3,$
$1 + u + u^2 + u^3,\ 1 + u^2,\ 0,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ u + u^3\},$
$\{1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2,$

$0,\ 1 + u^2\}, \{u + u^3,\ 1 + u^2,\ 1 + u^2,\ 1 + u + u^2 + u^3,$
$u + u^3,\ 1 + u + u^2 + u^3,\ 0\}, \{1 + u^2,\ 1 + u + u^2 + u^3,$
$u + u^3,\ 1 + u + u^2 + u^3,\ 0,\ u + u^3,\ 1 + u^2\},$
$\{0,\ u + u^3,\ 1 + u^2,\ 0,\ 0,\ 1 + u^2,\ u + u^3\}, \{1 + u^2,\ 1 + u^2,$
$u + u^3,\ 0,\ 1 + u + u^2 + u^3,\ u + u^3,\ 1 + u + u^2 + u^3\},$
$\{u + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 0,\ 1 + u + u^2 + u^3,$
$u + u^3\}, \{1 + u + u^2 + u^3,\ 0,\ 1 + u + u^2 + u^3,\ u + u^3,$
$u + u^3,\ u + u^3,\ u + u^3\}, \{u + u^3,\ 1 + u + u^2 + u^3,\ 0,$
$u + u^3,\ 1 + u^2,\ 1 + u^2,\ 1 + u + u^2 + u^3\}, \{1 + u + u^2 + u^3,$
$u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u^2,\ u + u^3,\ 0\},$
$\{1 + u^2,\ 0,\ 0,\ 1 + u^2,\ u + u^3,\ 0,\ u + u^3\}, \{0,\ 1 + u^2,$
$1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2\},$
$\{1 + u^2,\ u + u^3,\ 0,\ u + u^3,\ 1 + u^2,\ 0,\ 0\}, \{u + u^3,\ 0,$
$1 + u + u^2 + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u^2\},$
$\{1 + u + u^2 + u^3,\ 1 + u^2,\ 0,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ u + u^3,$
$u + u^3\}, \{u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 0,\ 1 + u^2,$
$1 + u + u^2 + u^3\}, \{1 + u^2,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ u + u^3,$
$1 + u + u^2 + u^3,\ 0,\ u + u^3\}, \{u + u^3,\ 1 + u + u^2 + u^3,\ 0,$
$1 + u + u^2 + u^3,\ u + u^3,\ u + u^3,\ u + u^3\}, \{1 + u + u^2 + u^3,$
$u + u^3,\ 1 + u + u^2 + u^3,\ 0,\ u + u^3,\ 1 + u^2,\ 1 + u^2\},$
$\{u + u^3,\ 1 + u^2,\ 0,\ 0,\ 1 + u^2,\ u + u^3,\ 0\}, \{1 + u^2,\ u + u^3,$
$0,\ 1 + u + u^2 + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 1 + u^2\},$
$\{u + u^3,\ u + u^3,\ 1 + u + u^2 + u^3,\ 0,\ 1 + u + u^2 + u^3,\ u + u^3,$
$u + u^3\}, \{0,\ 0,\ u + u^3,\ u + u^3,\ 1 + u^2,\ u + u^3,\ u + u^3\},$
$\{1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ u + u^3,\ u + u^3,\ 1 + u^2,$
$1 + u + u^2 + u^3\}, \{0,\ u + u^3,\ u + u^3,\ 1 + u^2,\ u + u^3,\ u + u^3,\ 0\},$
$\{u + u^3,\ 0,\ 1 + u^2,\ 1 + u^2,\ 1 + u^2,\ 0,\ u + u^3\},$
$\{1 + u + u^2 + u^3,\ 1 + u^2,\ u + u^3,\ u + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,$
$1 + u^2\}, \{u + u^3,\ u + u^3,\ 1 + u^2,\ u + u^3,\ u + u^3,\ 0,\ 0\},$
$\{1 + u^2,\ 0,\ u + u^3,\ u + u^3,\ 0,\ 1 + u^2,\ 1 + u^2\},$
$\{0,\ 1 + u^2,\ 1 + u^2,\ 1 + u^2,\ 0,\ u + u^3,\ u + u^3\},$
$\{1 + u^2,\ u + u^3,\ u + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2,$
$1 + u + u^2 + u^3\}, \{u + u^3,\ 1 + u^2,\ u + u^3,\ u + u^3,\ 0,\ 0,\ u + u^3\},$
$\{1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2,$
$u + u^3,\ u + u^3\}, \{0,\ u + u^3,\ u + u^3,\ 0,\ 1 + u^2,\ 1 + u^2,\ 1 + u^2\},$
$\{1 + u^2,\ 1 + u^2,\ 1 + u^2,\ 0,\ u + u^3,\ u + u^3,\ 0\}, \{u + u^3,\ u + u^3,$
$1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2\},$
$\{1 + u^2,\ u + u^3,\ u + u^3,\ 0,\ 0,\ u + u^3,\ u + u^3\},$
$\{u + u^3,\ 0,\ 0,\ u + u^3,\ u + u^3,\ 1 + u^2,\ u + u^3\},$
$\{1 + u + u^2 + u^3,\ 1 + u^2,\ 1 + u + u^2 + u^3,\ 1 + u^2,\ u + u^3,$

$u + u^3, 1 + u^2\}, \{u + u^3, u + u^3, 0, 1 + u^2, 1 + u^2, 1 + u^2, 0\},$
$\{1 + u^2, 1 + u^2, 0, u + u^3, u + u^3, 0, 1 + u^2\}, \{u + u^3, 1 + u^2,$
$1 + u + u^2 + u^3, 1 + u^2, 1 + u + u^2 + u^3, 1 + u^2, u + u^3\},$
$\{u + u^3, u + u^3, 0, 0, u + u^3, u + u^3, 1 + u^2\},$
$\{1 + u^2, 0, 1 + u^2, u + u^3, 1 + u^2, 1 + u^2, u + u^3\},$
$\{0, 1 + u^2, u + u^3, 1 + u^2, 1 + u^2, u + u^3, 1 + u^2\},$
$\{1 + u^2, u + u^3, 1 + u^2, 1 + u^2, u + u^3, 1 + u^2, 0\},$
$\{u + u^3, 1 + u^2, 1 + u^2, u + u^3, 1 + u^2, 0, 1 + u^2\},$
$\{1 + u^2, 1 + u^2, u + u^3, 1 + u^2, 0, 1 + u^2, u + u^3\},$
$\{1 + u^2, u + u^3, 1 + u^2, 0, 1 + u^2, u + u^3, 1 + u^2\},$
$\{u + u^3, 1 + u^2, 0, 1 + u^2, u + u^3, 1 + u^2, 1 + u^2\},$
$\{1 + u^2, 1 + u^2, 1 + u^2, 1 + u^2, 1 + u^2, 1 + u^2, 1 + u^2\}\}$

```
PadRight[
  CoefficientList[
    Expand[i * (u^3 + (u^6) x + (u^6) x^2 + (u^3) x^3)] /.
                                          u^4 → 1 + u /. u^5 → u^2 + u /.
                                        u^6 → u^3 + u^2 /. u^7 →
                                        u^3 + u + 1 /. u^8 → u^2 + 1 /.
                                   u^9 → u^3 + u /. u^10 → u^2 + u + 1 /.
                                u^11 → u^3 + u^2 + u /.
                              u^12 → u^3 + u^2 + u + 1
                             /. u^13 → u^3 + u^2 + 1
                             /. u^14 → u^3 + 1
                             /. x^7 → 1 /. x^8 → x /. x^9 → x^2 /.
                         x^10 → x^3 /. x^11 → x^4 /. x^12 → x^5 /.
                  x^13 → x^6 /. x^14 → x^7 , x, Modulus → 2],
  {128, 7}]
```

$\{\{0, 0, 0, 0, 0, 0, 0\}, \{u^3, u^2 + u^3, u^2 + u^3, u^3, 0, 0, 0\},$
$\{0, u^3, u^2 + u^3, u^2 + u^3, u^3, 0, 0\},$
$\{0, 0, u^3, u^2 + u^3, u^2 + u^3, u^3, 0\},$
$\{0, 0, 0, u^3, u^2 + u^3, u^2 + u^3, u^3\},$
$\{u^3, 0, 0, 0, u^3, u^2 + u^3, u^2 + u^3\},$
$\{u^2 + u^3, u^3, 0, 0, 0, u^3, u^2 + u^3\},$
$\{u^2 + u^3, u^2 + u^3, u^3, 0, 0, 0, u^3\}, \{u^3, u^2, 0, u^2, u^3, 0, 0\},$
$\{0, u^3, u^2, 0, u^2, u^3, 0\}, \{0, 0, u^3, u^2, 0, u^2, u^3\},$
$\{u^3, 0, 0, u^3, u^2, 0, u^2\}, \{u^2, u^3, 0, 0, u^3, u^2, 0\},$

$\{0, u^2, u^3, 0, 0, u^3, u^2\}, \{u^3, u^2+u^3, u^2, u^2, u^2+u^3, u^3, 0\},$
$\{u^3, u^2+u^3, u^2+u^3, 0, u^2+u^3, u^2+u^3, u^3\},$
$\{0, u^2+u^3, u^2+u^3, u^3, u^3, u^2+u^3, u^2+u^3\},$
$\{u^2, u^2, u^2+u^3, u^3, 0, u^3, u^2+u^3\},$
$\{u^2, 0, u^2, u^3, 0, 0, u^3\}, \{u^2+u^3, u^2, u^2, u^2+u^3, u^3, 0, u^3\},$
$\{u^2+u^3, u^2+u^3, 0, u^2+u^3, u^2+u^3, u^3, u^3\},$
$\{u^2+u^3, u^2+u^3, u^3, u^3, u^2+u^3, u^2+u^3, 0\},$
$\{u^2, u^2+u^3, u^3, 0, u^3, u^2+u^3, u^2\},$
$\{u^2+u^3, u^3, 0, u^3, u^2+u^3, u^2, u^2\},$
$\{u^3, 0, u^3, u^2+u^3, u^2, u^2, u^2+u^3\},$
$\{0, u^3, u^2+u^3, u^2, u^2, u^2+u^3, u^3\},$
$\{u^3, u^3, u^2+u^3, u^2+u^3, 0, u^2+u^3, u^2+u^3\},$
$\{u^2+u^3, 0, u^2+u^3, u^2+u^3, u^3, u^3, u^2+u^3\},$
$\{u^2+u^3, u^3, u^3, u^2+u^3, u^2+u^3, 0, u^2+u^3\},$
$\{u^3, u^2, u^3, u^3, u^2, u^3, 0\}, \{u^3, u^2, 0, u^2+u^3, u^2, u^2+u^3, u^3\},$
$\{0, u^2, 0, u^2, 0, u^2+u^3, u^2+u^3\},$
$\{u^2, u^2+u^3, 0, u^2, u^3, u^3, u^2+u^3\},$
$\{u^2, u^3, u^3, u^2, u^3, 0, u^3\}, \{u^3, u^2+u^3, u^2, u^2+u^3, 0, u^2, u^3\},$
$\{0, u^2+u^3, u^2, u^2, u^2, u^2, u^2+u^3\},$
$\{u^2, u^2, u^2, u^2, u^2+u^3, 0, u^2+u^3\},$
$\{u^2, 0, u^2+u^3, u^2, u^2+u^3, u^3, u^3\},$
$\{0, u^2+u^3, u^2+u^3, 0, u^2, 0, u^2\},$
$\{u^2, u^2, u^2+u^3, 0, u^2+u^3, u^2, u^2\},$
$\{u^2, 0, u^2, 0, u^2+u^3, u^2+u^3, 0\},$
$\{u^2+u^3, u^2, u^2+u^3, u^3, u^3, u^2, 0\},$
$\{u^2+u^3, 0, u^2, u^3, u^3, u^2+u^3, u^2\}, \{u^3, u^3, u^2, u^3, 0, u^3, u^2\},$
$\{0, u^3, u^2, u^3, u^3, u^2, u^3\}, \{u^3, u^3, u^2, 0, u^2+u^3, u^2, u^2+u^3\},$
$\{u^2+u^3, 0, u^2, 0, u^2, 0, u^2+u^3\},$
$\{u^2+u^3, u^2, u^2+u^3, 0, u^2, u^3, u^3\},$
$\{u^3, u^3, u^2+u^3, u^2, u^2+u^3, 0, u^2\},$
$\{u^2+u^3, 0, u^2+u^3, u^2, u^2, u^2, u^2\},$
$\{u^2+u^3, u^2, u^2, u^2, u^2, u^2+u^3, 0\},$
$\{u^2, 0, u^2+u^3, u^2+u^3, 0, u^2, 0\},$
$\{u^2, u^2, u^2, u^2+u^3, 0, u^2+u^3, u^2\},$
$\{0, u^2+u^3, u^2, u^2+u^3, u^3, u^3, u^2\},$
$\{u^3, u^2, u^3, 0, u^3, u^2, u^3\}, \{0, u^2, u^3, u^3, u^2+u^3, u^2, u^2+u^3\},$
$\{u^2, u^2+u^3, u^3, u^3, u^2, 0, u^2+u^3\},$
$\{u^2, u^3, 0, u^3, u^2, u^3, u^3\}, \{0, u^2, 0, u^2+u^3, u^2+u^3, 0, u^2\},$
$\{u^2, u^2+u^3, 0, u^2+u^3, u^2, u^2, u^2\},$
$\{u^2, u^3, u^3, u^2+u^3, u^2, u^2+u^3, 0\},$

$\{u^2 + u^3, u^2 + u^3, 0, u^2, 0, u^2, 0\}$,
$\{u^2 + u^3, u^3, u^3, u^2, 0, u^2 + u^3, u^2\}$, $\{u^3, 0, u^3, u^2, u^3, u^3, u^2\}$,
$\{u^3, u^2, u^3, 0, u^3, u^2, u^3\}$, $\{0, u^2, u^3, u^3, u^2 + u^3, u^2, u^2 + u^3\}$,
$\{u^2, u^2 + u^3, u^3, u^3, u^2, 0, u^2 + u^3\}$,
$\{u^2, u^3, 0, u^3, u^2, u^3, u^3\}$, $\{0, u^2, 0, u^2 + u^3, u^2 + u^3, 0, u^2\}$,
$\{u^2, u^2 + u^3, 0, u^2 + u^3, u^2, u^2, u^2\}$,
$\{u^2, u^3, u^3, u^2 + u^3, u^2, u^2 + u^3, 0\}$,
$\{u^2 + u^3, u^2 + u^3, 0, u^2, 0, u^2, 0\}$,
$\{u^2 + u^3, u^3, u^3, u^2, 0, u^2 + u^3, u^2\}$,
$\{u^3, 0, u^3, u^2, u^3, u^3, u^2\}$, $\{0, u^2 + u^3, u^2, u^2 + u^3, u^3, u^3, u^2\}$,
$\{u^2, u^2, u^2, u^2 + u^3, 0, u^2 + u^3, u^2\}$,
$\{u^2, 0, u^2 + u^3, u^2 + u^3, 0, u^2, 0\}$,
$\{u^2 + u^3, u^2, u^2, u^2, u^2, u^2 + u^3, 0\}$,
$\{u^2 + u^3, 0, u^2 + u^3, u^2, u^2, u^2, u^2\}$,
$\{u^3, u^3, u^2 + u^3, u^2, u^2 + u^3, 0, u^2\}$,
$\{u^2 + u^3, u^2, u^2 + u^3, 0, u^2, u^3, u^3\}$,
$\{u^2 + u^3, 0, u^2, 0, u^2, 0, u^2 + u^3\}$,
$\{u^3, u^3, u^2, 0, u^2 + u^3, u^2, u^2 + u^3\}$, $\{0, u^3, u^2, u^3, u^3, u^2, u^3\}$,
$\{u^3, u^3, u^2, u^3, 0, u^3, u^2\}$, $\{u^2 + u^3, 0, u^2, u^3, u^3, u^2 + u^3, u^2\}$,
$\{u^2 + u^3, u^2, u^2 + u^3, u^3, u^3, u^2, 0\}$,
$\{u^2, 0, u^2, 0, u^2 + u^3, u^2 + u^3, 0\}$,
$\{u^2, u^2, u^2 + u^3, 0, u^2 + u^3, u^2, u^2\}$,
$\{0, u^2 + u^3, u^2 + u^3, 0, u^2, 0, u^2\}$,
$\{u^2, 0, u^2 + u^3, u^2, u^2 + u^3, u^3, u^3\}$,
$\{u^2, u^2, u^2, u^2, u^2 + u^3, 0, u^2 + u^3\}$,
$\{0, u^2 + u^3, u^2, u^2, u^2, u^2, u^2 + u^3\}$,
$\{u^3, u^2 + u^3, u^2, u^2 + u^3, 0, u^2, u^3\}$,
$\{u^2, u^3, u^3, u^2, u^3, 0, u^3\}$, $\{u^2, u^2 + u^3, 0, u^2, u^3, u^3, u^2 + u^3\}$,
$\{0, u^2, 0, u^2, 0, u^2 + u^3, u^2 + u^3\}$,
$\{u^3, u^2, 0, u^2 + u^3, u^2, u^2 + u^3, u^3\}$,
$\{u^3, u^2, u^3, u^3, u^2, u^3, 0\}$, $\{0, u^2, u^3, 0, 0, u^3, u^2\}$,
$\{u^2, u^2 + u^3, u^3, 0, u^3, u^2 + u^3, u^2\}$, $\{u^2, u^3, 0, 0, u^3, u^2, 0\}$,
$\{u^2 + u^3, u^2 + u^3, u^3, u^3, u^2 + u^3, u^2 + u^3, 0\}$,
$\{u^2 + u^3, u^3, 0, u^3, u^2 + u^3, u^2, u^2\}$, $\{u^3, 0, 0, u^3, u^2, 0, u^2\}$,
$\{u^2 + u^3, u^2 + u^3, 0, u^2 + u^3, u^2 + u^3, u^3, u^3\}$,
$\{u^2 + u^3, u^3, u^3, u^2 + u^3, u^2 + u^3, 0, u^2 + u^3\}$,
$\{u^3, 0, u^3, u^2 + u^3, u^2, u^2, u^2 + u^3\}$,
$\{0, 0, u^3, u^2, 0, u^2, u^3\}$, $\{u^2 + u^3, u^2, u^2, u^2 + u^3, u^3, 0, u^3\}$,
$\{u^2 + u^3, 0, u^2 + u^3, u^2 + u^3, u^3, u^3, u^2 + u^3\}$,
$\{u^3, u^3, u^2 + u^3, u^2 + u^3, 0, u^2 + u^3, u^2 + u^3\}$,

$\{0, u^3, u^2 + u^3, u^2, u^2, u^2 + u^3, u^3\}, \{0, u^3, u^2, 0, u^2, u^3, 0\},$
$\{u^2, 0, u^2, u^3, 0, 0, u^3\}, \{u^2, u^2, u^2 + u^3, u^3, 0, u^3, u^2 + u^3\},$
$\{0, u^2 + u^3, u^2 + u^3, u^3, u^3, u^2 + u^3, u^2 + u^3\},$
$\{u^3, u^2 + u^3, u^2 + u^3, 0, u^2 + u^3, u^2 + u^3, u^3\},$
$\{u^3, u^2 + u^3, u^2, u^2, u^2 + u^3, u^3, 0\},$
$\{u^3, u^2, 0, u^2, u^3, 0, 0\}, \{u^2 + u^3, u^2 + u^3, u^3, 0, 0, 0, u^3\},$
$\{u^2 + u^3, u^3, 0, 0, 0, u^3, u^2 + u^3\},$
$\{u^3, 0, 0, 0, u^3, u^2 + u^3, u^2 + u^3\},$
$\{0, 0, 0, u^3, u^2 + u^3, u^2 + u^3, u^3\},$
$\{0, 0, u^3, u^2 + u^3, u^2 + u^3, u^3, 0\},$
$\{0, u^3, u^2 + u^3, u^2 + u^3, u^3, 0, 0\},$
$\{u^3, u^2 + u^3, u^2 + u^3, u^3, 0, 0, 0\}, \{0, 0, 0, 0, 0, 0, 0\}\}$

BÖLÜM 5. SONUÇLAR

GF(16) da toplamsal devirli ST , ST-tamamlanan ve tamamlanan kodlar üretildi. Tamamlanan kodlarda d uzaklığının, benzerlerine göre (aynı uzunluk ve aynı eleman sayısı), büyük olabileceği görüldü.

BÖLÜM 6. TARTIŞMA VE ÖNERİLER

GF(4), GF(16) da oluşturulan yapılar $GF(2^m)$ e genelleştirilebilir ve DNA dizilimine göre tam ters dizilimi bulmada tek bir işlem oluşturulabilir.

KAYNAKLAR

[1] ÇALLIALP, F., Cebir, Sakarya Üniversitesi Yay. No: 16, Sakarya, 1995.

[2] MONTGOMERY, H.L., NIVEN, I., ZUCKERMAN, H.S., An Introduction to the Theory of Numbers, Wiley, 1991.

[3] ROMAN, S., Coding And İnformation Theory, Graduate Texts in Mathematics, Springer Verlag, 1992.

[4] MACWILLIAMS, F.J. and SLOANE, N.J., The Theory of Error Correcting Codes, North Holland Pub. Co., 1977.

[5] ADLEMAN, L., Molecular Computation of Solutions to Combinational Problems, Science, v. 266, 1021-1024, 1994.

[6] KING, O., Bounds for DNA Codes with Constant GC-Content, J. Combin, 1–13 2003.

[7] FRUGTOS, A.G., LIU, Q., THIEL, A.J., SANNER, A.M.W., CONDON, A.E., SIMITH L.M., CORN, R.M., Demonstration of a Word Design Strategy for DNA Computing on Surfaces, Nucleic Acids Res. 25 4748–4757, 1997.

[8] ŞİAP, İ., ABUALRUB, T., GHAYREB, A., Cyclic DNA Codes Over the Ring $F_2[u]/(u^2-1)$ based on the deletion distance, Submitted.

[9] ŞİAP, İ., ABUALRUB, T., GHAYREB, A., A Similarity Cyclic DNA Codes over Rings, International Conference on Bioinformatics and Biomedical Engineering, May 16th to 18th 2008, in Shanghai, PRC, IEEE, pp.. 612-615.

[10] RYKOV, V., MACULA, A.J., TORNEY, D., WHİTE, P., DNA Sequences and Quaternary Cyclic Codes, IEEE, International Symposium on Information Theory (ISIT 2001), p. 248, Washington, DC, 2001.

[11] ZHE-XİAN, WAN., Lectures on finite fields and galois rings, World Scientific, 2003.

[12] CALDERBANK, A.R., RAİNS, E.M., SHOR, P.W., SLOANE, N.J.A., Quantum Error Correction Via Codes Over GF(4), IEEE Trans. Inf. Theory 1369–1387, 1998.

[13] MASSEY, J.L., Reversible Codes, Inf. Control, 369–380, 1964

[14] ABUALRUB, T., GHRAYEB, A., XIANG, N.Z., Construction of Cyclic Codes Over GF(4) for DNA Compoting, Journal of the Franklin Institute, 448-457, 2006.

[15] ABUALRUB, T., GHRAYEB, A., XIANG, N.Z., A Special Class of Additive Cyclic Codes for DNA Computing, Adaptive and Natural Computing Algorithms, Springer Vienna, 284-287, 2005.

[16] TUPLAN, D.C., HOOS, H., CONDON, A., Stochastic Local Search Algorithms for DNA Word Design, Lecture, Notes in Computer Science, Springer, Berlin, 2003, pp. 229–241.

ÖZGEÇMİŞ

Elif Segah Öztaş, 26.11.1985 yılında Elazığ'da doğdu. İlk öğretimini Elazığ'da okudu. İstanbul Atatürk Anadolu lisesinden 2003 yılında mezun oldu aynı yıl Sakarya Üniversitesini Matematik bölümünü kazandı. 2007 de Sakarya Üniversitesinden mezun olup aynı yıl Sakarya üniversitesinde yüksek lisansa başladı.