1 Giriş

> '96 yılı Aralık ayında NASA'nın Pathfinder adını verdiği ve Mars yüzeyini araştırmak üzere uzaya gönderdiği bir robotun dünyaya geçtiği çok sayıda fotoğraf ve bilimsel veri, tüm dünyayı büyük ölçüde heyecanlandırmıştı. Peki ancak loş bir ampulü yakmaya yetecek bir güç ile çalışan bir radyo vericisine sahip bu araçlardan, yüz milyonlarca kilometre öteden güvenilir ve tamamen bozulmamış bilgiler alabilmek nasıl mümkün olmuştur? Cevap : elektronik mühendisliği, bilgisayar bilimleri ve matematik gibi farklı disiplinlerin bir araya gelmesi ile; kısacası Kodlama Kuramı ile...

Claude Shannon tarafından yazılan ve 1948 yılında yayımlanan "*A mathematical theory of communication*" adlı çalışma, daha önce bazı temel fikirleri anlaşılmış olan bilişim kuramının sağlam temeller üzerine kurulmasını ve popüler hale gelmesini sağlamıştır. Bu çalışmada gürültülü bir iletişim kanalı için kanal kapasitesi adı verilen bir sayının varlığı ve eğer uygun kodlama ve kod çözme teknikleri kullanılırsa, kanal kapasitesi altında istenilen bir oranda güvenilir iletişim gerçekleştirilebileceği matematiksel olarak ifade edilmiş ve kanıtlanmıştır. Fakat Shannon'ın kanıtı yapısal (constructive) değildir. Yani kanıt uygun kodlamanın varlığını söylemekte ancak nasıl yapılabileceğine dair açık bir yöntem vermemektedir. Bunun üzerine uygun kodlamanın nasıl yapılabileceğine ilişkin araştırmalarla birlikte kodlama kuramı da ortaya çıkmaya başlamıştır. İlk adımı ise Richard W. Hamming, hata düzeltme kodları (error–correcting codes) üzerine yaptığı çalışmanın detaylarını yayınlayarak atmıştır. Bundan sonra kodlama kuramı, yarım yüzyılı biraz aşan bir süre içinde oldukça hızlı bir biçimde büyümüş ve genişlemiştir. Problemleri genellikle mühendislik uygulamalarından ortaya çıkıyor olsa bile matematiğin kodlama kuramı için vazgeçilmez bir rolü olduğunu söylemek yanlış olmaz. Bu nedenle kodlama kuramı yalnızca elektronik mühendislerinin ve bilgisayar bilimcilerin değil aynı zamanda matematikçilerin de ilgisini çeken bir alandır.

Kodlama kuramı, *gürültülü* bir **kanal** boyunca veri aktarılması ve bu sırada bozulan **ileti**lerin tamir edilmesi ile ilgilenmektedir. Bilginin daha kolay okunabilir hale gelmesiyle ilgilenen bu alan, daha zor okunmasını sağlamayı amaçlayan şifreleme (cryptography) ile karıştırılmamalıdır. Burada ileti ve kanal kelimeleri ile kapsayabilecekleri en geniş anlamlar kastedilmektedir. İletiler konuşma dili veya yazı olabileceği gibi resim, müzik vb. yapılar da olabilir. Verilerin aktarılması ile kastedilen "buradan başka bir yere iletilmesi" (yani haberleşme) olabileceği gibi "şimdiden sonraya iletilmesi" de (yani saklama da) olabilir. Buna göre söz konusu kanal uzay, atmosfer, telefon teli vb. bir ortam olabileceği gibi veri saklamada zaman olgusu veya verilerin saklanmasında kullanılan ortamlar da (örneğin kompakt disk yüzeyi) kanal olarak düşünülebilir. Dikkat edilirse yukarıda örnekleri sayılan kanalların hiçbiri veri aktarımı konusunda mükemmel değildir. Uzayda ve atmosferde oluşabilecek manyetik alanlar radyo dalgalarını, olumsuz hava koşulları telefon telleri üzerinden aktarılan sinyalleri, bir kompakt disk üzerinde bulunan çizikler ve lekeler disk üzerindeki bilgileri bozabilmektedir. Örnekleri daha da çoğaltılabilecek bunun gibi olumsuzluklara sahip kanallara gürültülü kanal denir. Gürültülere rağmen verilerin iletiminde oluşabilecek hataların sezilmesi ve hatta düzeltilmesi, kodlama kuramının temel problemlerini oluşturmaktadır.

Kanal, ileti, veri aktarımı, iletişim, haberleşme ve veri saklama gibi havalı kelimeler geçiyor olsa da bu kuramın kabul ettiği bir tek basit kavram vardır : simgeler. Simge ile neyi kastettiğimizi tam olarak tanımlayamayız. Simgeler ile yazılı ve sözlü (hatta mimik kullanarak) iletişim kurarız. Simge ile ne kastettiğimizi anlatmak için simgelere

başvuracağımız açık olduğuna göre, simgenin anlamını sezgisel bir seviyede tutmayı tercih edeceğiz. Kodlama kuramının ana konusu kaynak alfabe simgelerini, simgelerin başka bir sistemi (genellikle simgeleri 0 ve 1 olan ikili sistem) ile temsil etmeye dayanır. Bu temsile *kodlama* denir. Kodlamanın iki temel problemi asağıdaki gibidir:

Kaynak kodlaması Verimlilik esasına dayalı olarak kaynak simgelerinin asgari yapıda nasıl temsil edileceği problemidir.

Kanal kodlaması Kaynak simgelerinin bir anlamda birbirlerinden uzak olacak şekilde nasıl temsil edileceği problemidir. Sonuçta ise meydana gelebilecek küçük değişikliklere (gürültüye) rağmen değişen simgelerin sezilmesi ve hatta düzeltilebilmesi mümkün olmaktadır.

Kaynak kodlamalarına örnek olarak yazı karakterlerini 8 bit'e (ya da 1 byte) dönüştüren ASCII (American Standard Code for Information Interchange) kodu verilebilir (bkz: bir sonraki sayfa). ASCII kod tablosunda karakterlerin ikili karşılıkları yerine onaltılı veya sekizli karşılıkları bulunduğuna dikkat ediniz. Ancak bunları da ikili olarak kodlamak aşağıdaki gibi mümkündür:

2'li	**8'li**
000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

2'li	16'lı
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Örneğin ASCII tablosuna göre sekizli olarak "172" şeklinde kodlanan "z" karakteri bilgisayar içinde 1111010 ile temsil edilir.

Yukarıda yapıldığı gibi baştaki iki basamak atılırsa her karakter 7 bitlik bir dizge ile temsil edilebilir. Ancak 1 byte 8 bit olduğuna göre bu temsillere bir basamak daha eklenir. Bu basamak çoğunlukla hata sezme amacıyla kullanılır. Örneğin bu basamağa, tüm dizge içindeki 1'lerin toplam sayısı çift olacak şekilde 1 veya 0 eklenebilir. Bu işleme (çift) **eşlik denetimi (parity check)** diyeceğiz. Örneğin çift eşlik denetim bit'i eklendikten sonra yukarıdaki 1111010 dizgesi 11111010 dizgesine dönüşür.

10'lu	16'lı	8'li	Krkt.	10'lu	16'lı	8'li	Krkt.	10'lu	16'lı	8'li	Krkt.	10'lu	16'lı	8'li	Krkt.
0	0	000	NUL	32	20	040	Space	64	40	100	@	96	60	140	‘
1	1	001	SOH	33	21	041	!	65	41	101	A	97	61	141	a
2	2	002	STX	34	22	042	"	66	42	102	B	98	62	142	b
3	3	003	ETX	35	23	043	#	67	43	103	C	99	63	143	c
4	4	004	EOT	36	24	044	$	68	44	104	D	100	64	144	d
5	5	005	ENQ	37	25	045	%	69	45	105	E	101	65	145	e
6	6	006	ACK	38	26	046	&	70	46	106	F	102	66	146	f
7	7	007	BEL	39	27	047	’	71	47	107	G	103	67	147	g
8	8	010	BS	40	28	050	(	72	48	110	H	104	68	150	h
9	9	011	TAB	41	29	051	)	73	49	111	I	105	69	151	i
10	A	012	LF	42	2A	052	*	74	4A	112	J	106	6A	152	j
11	B	013	VT	43	2B	053	+	75	4B	113	K	107	6B	153	k
12	C	014	FF	44	2C	054	,	76	4C	114	L	108	6C	154	l
13	D	015	CR	45	2D	055	-	77	4D	115	M	109	6D	155	m
14	E	016	SO	46	2E	056	.	78	4E	116	N	110	6E	156	n
15	F	017	SI	47	2F	057	/	79	4F	117	O	111	6F	157	o
16	10	020	DLE	48	30	060	0	80	50	120	P	112	70	160	p
17	11	021	DC1	49	31	061	1	81	51	121	Q	113	71	161	q
18	12	022	DC2	50	32	062	2	82	52	122	R	114	72	162	r
19	13	023	DC3	51	33	063	3	83	53	123	S	115	73	163	s
20	14	024	DC4	52	34	064	4	84	54	124	T	116	74	164	t
21	15	025	NAK	53	35	065	5	85	55	125	U	117	75	165	u
22	16	026	SYN	54	36	066	6	86	56	126	V	118	76	166	v
23	17	027	ETB	55	37	067	7	87	57	127	W	119	77	167	w
24	18	030	CAN	56	38	070	8	88	58	130	X	120	78	170	x
25	19	031	EM	57	39	071	9	89	59	131	Y	121	79	171	y
26	1A	032	SUB	58	3A	072	:	90	5A	132	Z	122	7A	172	z
27	1B	033	ESC	59	3B	073	;	91	5B	133	[	123	7B	173	{
28	1C	034	FS	60	3C	074	<	92	5C	134	\	124	7C	174	|
29	1D	035	GS	61	3D	075	=	93	5D	135	]	125	7D	175	}
30	1E	036	RS	62	3E	076	>	94	5E	136	^	126	7E	176	~
31	1F	037	US	63	3F	077	?	95	5F	137	_	127	7F	177	DEL

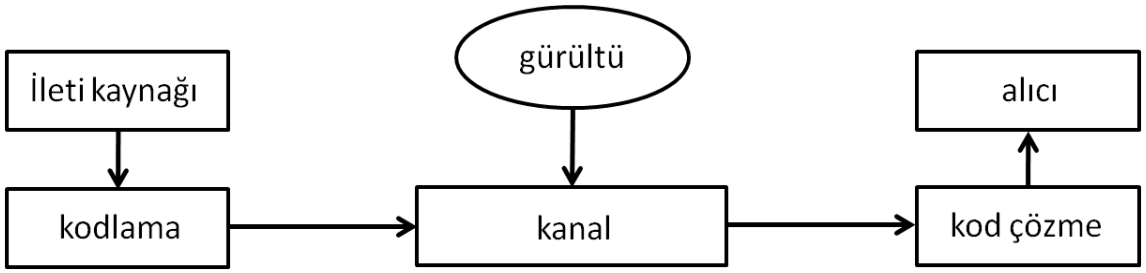
ASCII tablosu

Benzer şekilde 1'lerin sayısı tek olacak şekilde (tek eşlik denetimi) veya rasgele bir ekleme de yapılabilir.

Kaynak kodlamasına örnek olarak bir zamanlar çok yaygın olarak kullanılan Mors kodunu da verebiliriz. Mors kodu, simgeleri "·", "_" ve boşluk olan bir üçlü koddur. Her harf bu simgelerin bir dizilimi ile temsil edilir. Tek bir harf içindeki simgeler arasına bir birim boşluk, harfler arasına üç birim boşluk ve kelimeler arasına da altı birim boşluk konulur. Yukarıda verilen ASCII kodundan farklı olarak, Mors kodu değişken

uzunluklu bir koddur. Harfler, dildeki kullanım sıklıklarına göre değerlendirilip, en sık kullanılanlar için nispeten daha kısa ve kolay dizilimlerle temsil edilir.

Kodlama kuramının, gürültülü bir kanal boyunca veri aktarılması sırasında ileti üzerinde oluşması muhtemel hataların sezilmesi ve hatta onarılması ile ilgilendiğini daha önce söylemiştik. Gürültülü bir kanalı içeren basit bir iletişim modeli aşağıdaki gibi verilebilir:



Şimdi basit iletişim modelimizi bir örnekle açıklamaya çalışalım. Ahmet, Mehmet, Ayşe ve Fatma isimleri için aşağıdaki gibi verilen kaynak kodlamasını düşünelim:

$$\text{Ahmet} \to 00, \qquad \text{Mehmet} \to 01, \qquad \text{Ayşe} \to 10, \qquad \text{Fatma} \to 11.$$

Diyelim ki gürültülü bir kanal üzerinden 00 olarak kodlanan "Ahmet" gönderilsin. Gönderilen ileti üzerinde bozulma olabilir ve ileti 00 yerine 10 olarak alınabilir. Bu durumda "Ahmet" olarak gönderilen ileti, alıcı tarafından "Ayşe" olarak anlaşılacaktır. Ancak, büyük olasılıkla, alıcı, aktarım sırasında bir hata oluştuğunu düşünmeyecektir. Buna göre iletişim başarısız olmuştur. Peki bu durumda ne yapılabilir? Cevap olarak kabaca kanal kodlamasını verebiliriz. Dikkat edilirse yalnız kaynak kodlaması ile başarılı bir iletişim kurmak, özellikle karmaşık sistemler gerektiren durumlarda, oldukça zordur. Yukarıdaki kaynak kodlamasına çift eşlik denetimini uygulayarak bir basamak daha ekleyelim:

$$\text{Ahmet} \to 000, \qquad \text{Mehmet} \to 011, \qquad \text{Ayşe} \to 101, \qquad \text{Fatma} \to 110.$$

Daha önce olduğu gibi "Ahmet" kelimesi gönderilsin ve aktarım sırasında bir adet hata meydana gelmiş olsun. Buna göre alınan ileti 100, 010 veya 001 olasılıklarından biridir. Bu olasılıkların hiçbiri kodlanan iletiler arasında olmadığından aktarımın hatalı olduğu anlaşılacaktır. Ancak yukarıdaki kodlamaya kıyasla iki yerine üç bit taşımak zorunda kalacağımız için, hata sezmek uğruna aktarım hızının düşmesini göze aldığımıza dikkat ediniz. Buna rağmen sadece hatanın varlığını anlayabilir, onu düzeltemeyiz. Çünkü 101 ve 110 iletilerinin de bir adet hata sonucu 100 olarak alınması mümkündür. Doğrusu biraz daha ekleme yaparsak hata düzeltmek te mümkün olur. Örneğin aşağıdaki gibi bir kodlamayı ele alalım:

$$\text{Ahmet} \to 0000, \qquad \text{Mehmet} \to 01111, \qquad \text{Ayşe} \to 10110, \qquad \text{Fatma} \to 11001.$$

Yine “Ahmet” kelimesi gönderilsin ve bir adet hata meydana gelsin. Örneğin 10000 iletisi alınmış olsun. Bu durumda 10000 iletisinin aslında 00000 iletisinden bir adet hata sonucu meydana geldiğini anlayabiliriz. Çünkü 10000 iletisi ile diğer kodlanmış iletiler (01111, 10110 ve 11001) arasında en az iki hata vardır. Bu şekilde aktarım hızının biraz daha azaldığını görebiliriz. Dolayısıyla hataların sezilmesi ve hatta düzeltilmesi amacıyla yapılan bu tür eklemelerin bir sınırı olması gerektiği sonucuna varabiliriz.

Hata düzeltme amacıyla yapılabilecek eklemelere basit ve genel bir örnek verelim. Kabul edelim ki kaynak kodlaması yapılmış olsun ve iletiler k uzunluğundaki bit dizgelerinden oluşsun. Kodlamayı bit dizgelerini, $r \geq 1$ için, $2r + 1$ defa tekrar ederek gerçekleştireceğiz. Örneğin 01 dizgesi, $r = 2$ için, 0101010101 dizgesi olarak kodlanacaktır. Bu yönteme *tekrarlı kod* denir.

Soru. Bir tekrarlı kod en fazla kaç hatayı düzeltebilir?

2 Hata Tespiti, Hata Düzeltme ve Kod Çözme

2.1 İletişim Kanalları

Tanım *$A = \{a_1, a_2, \ldots, a_q\}$ kümesini alalım. A kümesine **"kod alfabesi"** (code alphabet) ve kümenin elemanlarına da **"kod simgeleri"** (code symbols) diyeceğiz.*

*(i) $\omega_1, \ldots, \omega_n \in A$ olmak üzere $\mathrm{w} = w_1 w_2 \ldots w_n$ şeklindeki bir diziye n–uzunluklu bir **q–lu sözcük** denir. w aynı zamanda $(w_1, w_2, \ldots, w_n)$ vektörü ile eşdeğer şekilde de düşünülebilir.*

*(ii) Aynı n uzunluğuna sahip q–lu sözcüklerin boş olmayan bir C kümesine **q–lu öbek kodu** (q–ary block code) veya kısaca **q–lu kod** denir. C kümesinin her elemanına ise **kod–sözcüğü** adı verilir. C içindeki kod–sözcüklerinin sayısına C'nin büyüklüğü denir ve $|C|$ ile gösterilir.*

*(iii) Uzunluğu n olan bir C kodunun **(bilgi) oranı** $(\log_q |C|)/n$ sayısı ile tanımlanmaktadır.*

*(iv) Uzunluğu n olan M büyüklüğünde bir kod için **(n, M)–kodu** ifadesini kullanacağız.*

> Uygulamada ve dersimizde kod alfabesi olarak sıklıkla bir sonlu cisim, genellikle de mertebesi q olan sonlu cisim $(\mathbb{F}_q)$, kullanılmaktadır.

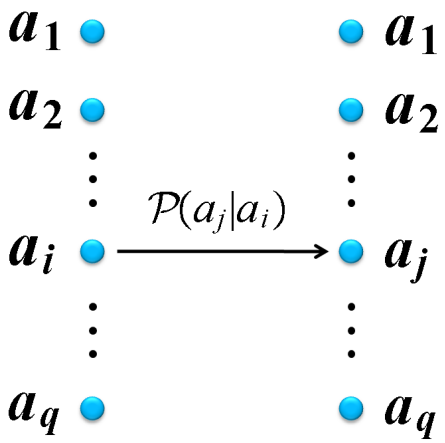
Örnek 1 *$\mathbb{F}_2 = \{0, 1\}$ kod alfabesi üzerinde tanımlanan bir koda **ikili kod** adı verilir. Buna göre bir ikili kod için kod simgeleri 0 ve 1'dir. Aşağıda bazı ikili kod örnekleri yer almaktadır:*
(i) $C_1 = \{00, 01, 10, 11\}$ bir $(2, 4)$–kodudur.
(ii) $C_2 = \{000, 010, 110, 111\}$ bir $(3, 4)$–kodudur.
(iii) $C_3 = \{0101, 1100, 0011, 1010, 1001, 0110\}$ bir $(4, 6)$–kodudur.

Benzer şekilde, **üçlü** ve **dörtlü kod**lar, kod alfabeleri sırasıyla $\mathbb{F}_3 = \{0, 1, 2\}$ ve $\mathbb{F}_4$ (4 elemanlı sonlu cisim) olan kodlara denilmektedir. Ancak bazen kod alfabesi $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ halkası olan kodlara da dörtlü kod denilebilmektedir. Buradan, kod alfabelerinin cebirsel yapılarının kodlar üzerinde etkili olduğu bir kuramı tanıtacağımızı anlamak mümkündür.

Tanım *Bir **iletişim kanalı** sonlu bir $A = \{a_1, \ldots, a_q\}$ **kanal alfabesi** ile **(ileri yönlü) kanal olasılıkları**nın bir $\{\mathcal{P}(a_j|a_i) : 1 \leq i, j \leq q\}$ kümesinden oluşur. Burada $\mathcal{P}(a_j|a_i)$; aynı zamanda $\mathcal{P}(a_j$ alınır $\mid a_i$ gönderilir) biçiminde de gösterilebilen, a_i gönderilmesi halinde a_j alınması (koşullu) olasılığını temsil etmektedir. İleri yönlü kanal olasılıkları her $1 \leq i \leq q$ için*

$$\sum_{j=1}^{q} \mathcal{P}(a_j|a_i) = 1$$

eşitliğini sağlamalıdır. Bunun anlamı ise; her i için, a_i gönderildiğinde A'nın bir elemanının mutlaka alınacağının güvence altında olduğudur.



Tanım *Bir iletişim kanalında gerçekleşen bir iletimin sonucu, daha önce gerçekleşen iletimlerin sonucundan bağımsız ise bu kanala* ***belleksiz kanal*** *denir. Yani, bir belleksiz kanalda, n uzunluklu $\mathbf{c} = c_1 \dots c_n$ ve $\mathbf{x} = x_1 \dots x_n$ gibi iki sözcük için*

$$\mathcal{P}(\ \mathbf{x}\ |\ \mathbf{c}\ ) = \prod_{i=1}^{n} \mathcal{P}(x_i|c_i)$$

olur.

Tanım *Eğer q büyüklüğünde alfabeye sahip bir belleksiz kanalda*

(i) aktarılan her bir simgenin hatalı aktarılmış olması olasılığı aynı ve $1/2$ 'den az,

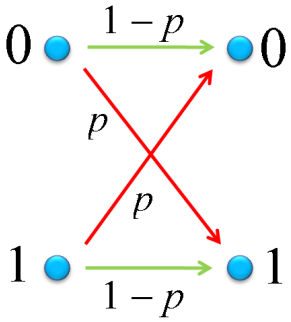
(ii) bir simge hata ile alındığında $q-1$ adet muhtemel hatanın her biri eşdeğer oranda muhtemel

ise bu kanala bir ***q–lu simetrik kanal*** *denir.*

Özel olarak, *ikili simetrik kanal (**İSK**)*, alfabesi $\{0, 1\}$ kümesi ve kanal olasılıkları

$$\mathcal{P}(1|0) = \mathcal{P}(0|1) = p < 1/2$$
$$\mathcal{P}(0|0) = \mathcal{P}(1|1) = 1 - p$$

biçiminde olan bir belleksiz kanaldır. Buna göre bir İSK'da bir bit hata olasılığı p'dir. Bu olasılığa İSK'ın **çapraz olasılığı** denir.



İkili simetrik kanal

Örnek 2 $\{000, 111\}$ *kodunun kod sözcükleri çapraz olasılığı* $p = 0.05$ *olan bir İSK üzerinden gönderiliyor olsun. Kabul edelim ki bir dizi iletim sonunda* 110 *sözcüğünü alıyoruz. İleri yönlü kanal olasılıklarını inceleyerek, gönderilmiş olması daha muhtemel sözcüğü bulmaya çalışabiliriz:*

$$\begin{aligned}\mathcal{P}(110|000) &= \mathcal{P}(1|0)^2 \times \mathcal{P}(0|0) \\ &= (0.05)^2 \times (0.95) = 0.002375\end{aligned}$$

$$\begin{aligned}\mathcal{P}(110|111) &= \mathcal{P}(1|1)^2 \times \mathcal{P}(0|1) \\ &= (0.95)^2 \times (0.05) = 0.045125\end{aligned}$$

İkinci olasılığın birinciden daha büyük olması nedeniyle gönderilmiş olması daha muhtemel olan sözcüğün 111 *olduğu sonucuna varabiliriz.*

2.2 Kod Çözme

Kodlamalı bir iletişim kanalında, yalnızca kod sözcükleri iletilir. Eğer bir iletimde geçerli bir kod sözcüğü alınırsa bu durumda iletimde bir hata olmadığını düşünmek olasıdır. Ancak, tersi bir durumda, iletimde hatalar meydana geldiğini biliriz. Böyle bir durumda, gönderilmiş olması en muhtemel kod sözcüğünü belirlemek üzere bir kurala ihtiyacımız olur. Böyle bir kurala **kod çözme kuralı** adı verilir. Bu bölümde şimdilik iki genel kuralı tanıtmakla yetineceğiz:

1. Azami Olasılık (Kod–Çözme) Kuralı

Kabul edelim ki bir C kodunun kod sözcükleri bir iletişim kanalı üzerinden gönderiliyor olsun Bir $\mathbf{x}$ sözcüğü alınırsa, her $\mathbf{c} \in C$ için

$$\mathcal{P}(\ \mathbf{x} \mid \mathbf{c}\ )$$

kanal olasılıklarını hesaplayabiliriz. *Azami olasılık kod–çözme kuralı*na göre, eğer $\mathbf{c}_{\mathbf{x}}$ sözcüğü için bu kanal olasılıkları azami değer alıyor ise, yani

$$\mathcal{P}(\ \mathbf{x} \mid \mathbf{c}_{\mathbf{x}}\ ) = \max_{\mathbf{c} \in C} \mathcal{P}(\ \mathbf{x} \mid \mathbf{c}\ )$$

ise o zaman $\mathbf{c}_{\mathbf{x}}$, gönderilmiş olması en muhtemel kod sözcüğüdür. Azami olasılık kuralı *tam* ve *tam olmayan* şeklinde ikiye ayrılır. Tam azami olasılık kuralında kanal olasılıklarının azami olduğu birden fazla kod sözcüğü olması halinde bu sözcükler arasında rastgele bir seçim yapılır. Tam olmayan azami olasılık kuralında ise böyle bir durumda sözcüğün yeniden gönderilmesi istenir.

2. Asgari Uzaklık (Kod–Çözme) Kuralı

Kabul edelim ki bir C kodunun kod sözcükleri, çapraz olasılığı p $(< 1/2)$ olan bir İSK üzerinden gönderiliyor olsun. Eğer bir n–uzunluklu bir $\mathbf{x}$ sözcüğü alınır ise bu durumda herhangi bir (n–uzunluklu) $\mathbf{c} \in C$ için ileri yönlü kanal olasılığı

$$\mathcal{P}(\ \mathbf{x} \mid \mathbf{c}\ ) = p^e(1-p)^{n-e}$$

şeklindedir. Burada e, $\mathbf{x}$ ile $\mathbf{c}$ sözcüklerinin birbirlerinden farklı oldukları (veya ayrıldıkları) basamakların sayısını temsil etmektedir. $p < 1/2$ olduğundan $1 - p > p$ olur. Böylece bu olasılığın değeri $n - e$ değeri büyüdükçe, başka bir deyişle de e değeri küçüldükçe, artar. Buna göre, bu olasılık, e'nin mümkün olduğunca küçük tutulabildiği bir $\mathbf{c}$ sözcüğü için azami değere sahiptir. Burada sözü edilen e sayısı, bizi, aşağıdaki tanımda olduğu gibi verilen bir uzaklık kavramını ortaya atmaya itmektedir:

Tanım *Bir A alfabesi üzerinde n–uzunluklu $\mathbf{x}$ ve $\mathbf{y}$ gibi iki sözcük alalım. $\mathbf{x}$ ve $\mathbf{y}$ arasındaki **uzaklık** (ya da **Hamming uzaklığı**), $\mathbf{x}$ ve $\mathbf{y}$ 'nin birbirinden ayrıldığı basamakların sayısı olarak tanımlanır ve $d(\mathbf{x},\mathbf{y})$ şeklinde gösterilir. Buna göre $\mathbf{x} = x_1 \dots x_n$, $\mathbf{y} = y_1 \dots y_n$ ve x_i ile y_i simgelerini 1–uzunluklu sözcükler olarak düşünmek suretiyle*

$$d(x_i, y_i) = \begin{cases} 1, & x_i \neq y_i \\ 0, & x_i = y_i \end{cases}$$

dersek,

$$d(\mathbf{x}, \mathbf{y}) = d(x_1, y_1) + \cdots + d(x_n, y_n)$$

olarak yazılabilir.

Örnek 3 *$A = \{0, 1, 2\}$ olmak üzere $\mathbf{x} = 201102$, $\mathbf{y} = 101212$, ve $\mathbf{z} = 200020$ denirse bu durumda*

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= 3 \\ d(\mathbf{x}, \mathbf{z}) &= 4 \\ d(\mathbf{y}, \mathbf{z}) &= 5 \end{aligned}$$

elde edilir.

Önerme 1 *$\mathbf{x}$, $\mathbf{y}$ ve $\mathbf{z}$, A üzerinde n–uzunluklu sözcükler olsun.Buna göre*

(i) $0 \leq d(\mathbf{x},\mathbf{y}) \leq n$.

(ii) $d(\mathbf{x},\mathbf{y}) = 0 \iff \mathbf{x} = \mathbf{y}$.

(iii) $d(\mathbf{x},\mathbf{y}) = d(\mathbf{y},\mathbf{x})$

(iv) $\left[\textbf{Üçgen eşitsizliği}\right]$ $d(\mathbf{x},\mathbf{z}) \leq d(\mathbf{x},\mathbf{y}) + d(\mathbf{y},\mathbf{z})$.

Kanıt. *(i)*, *(ii)* ve *(iii)* kısımları tanımdan açıkça görülebilir. *(iv)* için $\mathbf{x} = x_1 \dots x_n$, $\mathbf{y} = y_1 \dots y_n$ ve $\mathbf{z} = z_1 \dots z_n$ olsun. Bir $1 \leq i \leq n$ için, $x_i = z_i$ ise $d(x_i, z_i) = 0$ olacağından $d(x_i, z_i) \leq d(x_i, y_i) + d(y_i, z_i)$ olur. Öte yandan $x_i \neq z_i$ olduğunda $x_i \neq y_i$ veya $y_i \neq z_i$ olacağından $d(x_i, z_i) = 1 \leq d(x_i, y_i) + d(y_i, z_i)$ elde edilir. $d(\mathbf{x},\mathbf{z}) = d(x_1, z_1) + \cdots + d(x_n, z_n)$ yazılabildiğinden kanıt tamamlanmış olur. ■

Kabul edelim ki bir C kodunun kod sözcükleri bir iletişim kanalı üzerinden gönderiliyor olsun. *Asgari uzaklık kod çözme kuralı*na göre, eğer $\mathbf{c}_{\mathbf{x}}$, sözcüğü için

$$d(\ \mathbf{x} \mid \mathbf{c}\ ), \qquad c \in C$$

uzaklıkları asgari değer alıyor ise, yani

$$d(\ \mathbf{x} \mid \mathbf{c}_{\mathbf{x}}\ ) = \min_{\mathbf{c} \in C} d(\ \mathbf{x} \mid \mathbf{c}\ )$$

ise o zaman $\mathbf{x}$ sözcüğü $\mathbf{c}_{\mathbf{x}}$ olarak çözülür. Azami olasılık kuralında olduğu gibi asgari uzaklık kuralı da tam ve tam olamayan olmak üzere iki çeşittir.

Teorem 2 *Bir İSK için azami olasılık kuralı ile asgari uzaklık kuralı denktir.*

Kanıt. Simetrik kanalın çapraz olasılığı $p < 1/2$ olsun. Kullanılan kodu C ile, aktarımda alınan n–uzunluklu bir sözcüğü de $\mathbf{x}$ ile gösterelim. n–uzunluklu herhangi bir $\mathbf{c}$ kod sözcüğü için

$$d(\ \mathbf{x}\ |\ \mathbf{c}\ ) = i \iff \mathcal{P}(\ \mathbf{x}\ |\ \mathbf{c}\ ) = p^i(1-p)^{n-i}$$

olur. $p < 1/2$ olduğundan

$$p^0(1-p)^n > p^1(1-p)^{n-1} > p^2(1-p)^{n-2} > \cdots > p^n(1-p)^0$$

yazabiliriz. Tanıma göre azami olasılık kuralı, $\mathbf{x}$ sözcüğünü $\mathcal{P}(\ \mathbf{x}\ |\ \mathbf{c}\ )$ değerini en büyük, yani $d(\ \mathbf{x}\ |\ \mathbf{c}\ )$ değerini en küçük yapan bir $\mathbf{c}$ kod sözcüğü olarak çözer (ya da, tam olmayan kural uygulanıyorsa, $\mathbf{c}$ tek olmadığında yeniden gönderim ister) ve dolayısıyla da asgari uzaklık kuralı ile aynı işi yapmış olur. ■

Örnek 4 $C = \{0000, 0011, 1000, 1100, 0001, 1001\}$ *kodunun sözcükleri bir İSK üzerinden gönderiliyor olsun.* $\mathbf{x} = 0111$ *sözcüğü alınmış ise asgari uzaklık kod çözme kuralına göre* $\mathbf{x}$*,* 0011 *kod sözcüğü olarak çözülür.*

Örnek 5 $C = \{000, 011\}$ *ikili kodu için bir tam olmayan asgari uzaklık kod çözme tablosu yapalım:*

alınan $\mathbf{x}$	$d(\ \mathbf{x}\ \|\ \mathbf{000})$	$d(\ \mathbf{x}\ \|\ \mathbf{011})$	***çözülen***
000	0	2	000
100	1	3	000
010	1	1	–
001	1	1	–
110	2	2	–
101	2	2	–
011	2	0	011
111	3	1	011

2.3 Bir Kodun Uzaklığı

Uzunluk ve büyüklük gibi iki özellikten sonra bir kod için önemli başka bir özellik te o kodun uzaklığıdır.

Tanım *En az iki sözcük içeren bir C kodu için, C'nin (asgari)* ***uzaklığı***

$$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}$$

olarak tanımlanır.

Uzunluğu n, büyüklüğü M ve uzaklığı d olan bir kod için $\boldsymbol{(n, M, d)}$*–**kodu** ifadesi kullanılır. n, M ve d sayılarına kodun* ***parametre****leri denir.*

Örnek 6 *$C = \{0000, 0101, 1111\}$ ikili kodu için $d(C) = 2$ olarak hesaplanır.*

$$\begin{aligned} d(0000, 0101) &= 2, \\ d(0000, 1111) &= 4, \\ d(0101, 1111) &= 2. \end{aligned}$$

Buna göre C bir $(5, 3, 2)$–ikili kodudur.

Örnek 7 *$C = \{10201, 21012, 12021, 20102, 02120\}$ kodu için $d(C) = 3$ olur. Buna göre C bir $(5, 5, 3)$–üçlü kodudur.*

Tanım *u bir pozitif tamsayı ve C bir kod olsun. Eğer C'nin her bir kod sözcüğü üzerinde u ya da daha az sayıda hata meydana geldiğinde, ortaya çıkan, bir kod sözcüğü değilse C koduna bir **u–hata sezici kod** adı verilir. Eğer bir kod u–hata sezici olduğu halde $(u + 1)$–hata sezici kod değilse o zaman bu kod için **tam–u–hata sezici kod** denir.*

Örnek 8 *$C = \{00000, 11000, 11111\}$ şeklinde tanımlanan bir C ikili kodu, 1–hata sezici koddur.*

$$00000 \xrightarrow{2 \text{ hata}} 11000$$

$$00000 \xrightarrow{5 \text{ hata}} 11111$$

$$11000 \xrightarrow{3 \text{ hata}} 11111$$

Aslında C bir tam–1–hata sezici koddur. Çünkü 00000 sözcüğünün ilk iki hanesini değiştirerek geçerli bir kod sözcüğü olan 11000 elde ediliyor. $C = \{000000, 111000, 111222\}$ üçlü kodu ise bir tam–2–hata sezici koddur.

$$000000 \xrightarrow{3 \text{ hata}} 111000$$

$$000000 \xrightarrow{6 \text{ hata}} 111222$$

$$111000 \xrightarrow{3 \text{ hata}} 111222$$

Teorem 3 *Bir C kodu u–hata sezicidir ancak ve ancak $d(C) \geq u+1$. Başka bir deyişle uzaklığı d olan bir kod tam–$(d-1)$–hata sezici koddur.*

Kanıt. Önce $d(C) \geq u + 1$ olsun. Bir $\mathbf{c} \in C$ üzerinde en fazla u adet hata yapılırsa, yani en fazla u adet basamak değiştirilirse elde edilen $\mathbf{x}$ sözcüğü için

$$1 \leq d(\mathbf{c}, \mathbf{x}) \leq u < d(C)$$

olur. Bu durumda, uzaklık tanımından dolayı, $\mathbf{x} \notin C$ elde edilir. Yani C u–hata sezicidir.

Tersine eğer $d(C) < u+1$, yani $d(C) \leq u$ alınırsa, $1 \leq d(\mathsf{c}_1,\mathsf{c}_2) = d(C) \leq u$ olacak şekilde $\mathsf{c}_1,\mathsf{c}_2 \in C$ sözcükleri vardır. Dolayısıyla c_1 kod sözcüğü üzerinde en fazla u adet hata meydana getirerek c_2 kod sözcüğünü elde etmek mümkündür. Buna göre C kodu bir u–hata sezici kod olamaz. Böylece kanıtın ilk kısmı tamamlanmış olur. İkinci kısım için, uzaklığı d olan bir C kodu alalım. Birinci kısımdan dolayı C kodunun bir $(d-1)$–hata sezici kod olacağı açıktır. Eğer C, d–hata sezici olsaydı tekrar birinci ksımdan dolayı $d(C) \geq d+1$ olması gerekirdi. Dolayısıyla C bir tam–$(d-1)$–hata düzeltici koddur. ■

Tanım *v bir pozitif tamsayı ve C bir kod olsun. Eğer tam olmayan asgari uzaklık kod çözme kuralı ile C'nin kod sözcükleri üzerinde v veya daha az sayıda hata düzeltilebiliyor ise C koduna* ***v–hata düzeltici kod*** *denir. Eğer bir kod v–hata düzeltici olduğu halde $(v+1)$–hata düzeltici kod değilse o zaman bu kod için* ***tam–v–hata düzeltici kod*** *denir.*

Örnek 9 *$C = \{000, 111\}$ kodunu ele alalım. Asgari uzaklık kuralına göre*

1. 000 *gönderilir ve yalnız bir hata meydana gelirse,* 100, 010 *veya* 001 *olarak alınan kod sözcüğü,* 000 *olarak çözülür.*

2. 111 *gönderilir ve yalnız bir hata meydana gelirse,* 011, 101 *veya* 110 *olarak alınan kod sözcüğü,* 111 *olarak çözülür.*

Dolayısıyla, C kodu bir 1*–hata düzeltici koddur. Asgari uzaklık kuralı, C kodunun sözcükleri üzerinde meydana gelebilecek iki adet hata sonucu oluşacak sözcükleri yanlış çözeceğinden (neden?) C kodu tam–*1*–hata düzeltici kod olur.*

Teorem 4 *Bir C kodu v–hata düzelticidir ancak ve ancak $d(C) \geq 2v+1$. Başka bir deyişle uzaklığı d olan bir kod tam–$\lfloor (d-1)/2 \rfloor$–hata düzeltici koddur. Burada $\lfloor x \rfloor$, x'den büyük olmayan en büyük tamsayıdır.*

Kanıt. ($\Leftarrow$) $d(C) \geq 2v+1$ olsun. $\mathbf{c}$ gönderilen kod sözcüğü ve $\mathbf{x}$ ise alınan sözcük olsun. Aktarımda v ya da daha az sayıda hata meydana gelmiş ise $d(\mathbf{x},\mathbf{c}) \leq v$ olur. Bu durumda herhangi bir $\mathbf{c}' \in C$, $\mathbf{c}' \neq \mathbf{c}$ kod sözcüğü için

$$\begin{aligned} d(\mathbf{x},\ \mathbf{c}') &\geq d(\mathbf{c},\ \mathbf{c}') - d(\mathbf{x},\ \mathbf{c}) \\ &\geq 2v+1-v = v+1 > d(\mathbf{x},\ \mathbf{c}) \end{aligned}$$

Böylece asgari uzaklık kuralı uygulanırsa, $\mathbf{x}$ sözcüğü $\mathbf{c}$ olarak çözülür. Dolayısıyla C bir v–hata düzeltici koddur.

($\Rightarrow$) C bir v–hata düzeltici kod olsun. $d(C) < 2v+1$ ise $d(\mathbf{c},\mathbf{c}') = d(C) \leq 2v$ olacak şekilde birbirinden farklı $\mathbf{c}$, $\mathbf{c}' \in C$ kod sözcükleri vardır. $\mathbf{c}$ gönderildiğinde ve en fazla v adet hata meydana geldiğinde, tam olmayan asgari uzaklık kuralının alınan sözcüğü $\mathbf{c}'$ olarak çözebileceğini ya da çakışma bildireceğini göstereceğiz. Bu durum C'nin v–hata düzeltici olması ile çelişeceğinden $d(C) \geq 2v+1$ elde edilecektir.

Eğer $d(\mathbf{c},\mathbf{c}') < v+1$ ise $\mathbf{c}$ kod sözcüğü en fazla v adet hata yapılarak $\mathbf{c}'$ kod sözcüğüne dönüştürülebilir ve dolayısıyla da hata sezilemeyeceği için düzeltilemez. Bu durum C'nin v–hata düzeltici olması ile çelişeceğinden $d(\mathbf{c},\mathbf{c}') \geq v+1$ olur. Genelliği bozmadan $\mathbf{c}$ ve $\mathbf{c}'$ kod sözcüklerinin ilk $d = d(C)$ basamakta fark ettiğini kabul edebiliriz. Burada $v+1 \leq d \leq 2v$ dir. Eğer

$$\mathbf{x} = \underbrace{x_1 \ldots x_v}_{\substack{\mathbf{c}' \text{ ile} \\ \text{çakışır}}} \underbrace{x_{v+1} \ldots x_d}_{\substack{\mathbf{c} \text{ ile} \\ \text{çakışır}}} \underbrace{x_{d+1} \ldots x_n}_{\substack{\text{ikisi ile de} \\ \text{çakışır}}}$$

şeklinde bir sözcük alınırsa, her $\mathbf{y} \in C$, $\mathbf{y} \neq \mathbf{c}'$, için

$$d(\mathbf{x}, \mathbf{y}) + d - v = d(\mathbf{x}, \mathbf{y}) + d(\mathbf{x}, \mathbf{c}') \geq d(\mathbf{c}', \mathbf{y}) \geq d$$

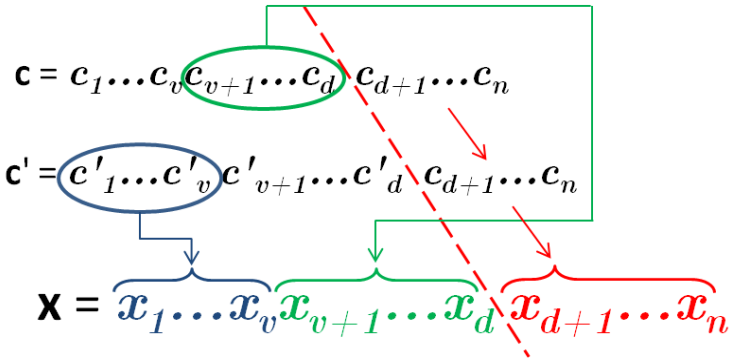
ve buradan da

$$d(\mathbf{x}, \mathbf{y}) \geq v$$

elde edilir. Ayrıca

$$d(\mathbf{x}, \mathbf{c}') = d - v \leq v = d(\mathbf{x}, \mathbf{c})$$

olacağından ya $d(\mathbf{x}, \mathbf{c}') < d(\mathbf{x}, \mathbf{c})$ –ki bu durumda $\mathbf{x}$ sözcüğü $\mathbf{c}'$ olarak çözülür– ya da $d(\mathbf{x}, \mathbf{c}') = d(\mathbf{x}, \mathbf{c})$ olur –ki bu durumda da çakışma bildirilir. ■



3 Sonlu Cisimler

3.1 Cisim Kavramı

Tanım *F boş olmayan bir küme olsun. F'nin elemanları arasında $+$ ve $\cdot$ ile göstereceğimiz, sırasıyla toplama ve çarpma adında, iki tane ikili işlem tanımlanmış olsun. $(F, +, \cdot)$ üçlüsü aşağıdaki koşulları sağlıyorsa, bu üçlüye bir* ***cisim*** *denir:*
Her $a, b, c \in F$ için;

(i) Kapalılık: $a + b,\ a \cdot b \in F$.

(ii) Değişme özelliği: $a + b = b + a$ ve $a \cdot b = b \cdot a$.

(iii) Birleşme özelliği: $(a + b) + c = a + (b + c)$ ve $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) Dağılma özelliği: $a \cdot (b + c) = a \cdot b + a \cdot c$.

(v) Birim eleman: F içinde toplamsal ve çarpımsal birim olarak anılan ve, sırasıyla, 0 ve 1 olarak gösterilen aşağıdaki özelliklere sahip birbirinden farklı iki eleman vardır:
Her $a \in F$ için,

(v–a) $a + 0 = a$;
(v–b) $a \cdot 1 = a$;
(v–c) $a + (-a) = 0$ olacak şekilde F'nin bir "$-a$" elemanı vardır;
(v–d) $a \neq 0$ ise $a \cdot a^{-1} = 1$ olacak şekilde F'nin bir a^{-1} elemanı vardır.

Yukarıdaki tanımda yer alan $a \cdot b$ ifadesi yerine genellikle daha basit olan ab gösterimini, $F \backslash \{0\}$ kümesi yerine de F^* gösterimini kullanacağız. Tanımdan kolayca görülebilir ki F^* kümesi F'deki çarpma işlemine göre bir Abelyan gruptur. F cisminin toplamsal ve çarpımsal birim elemanlarının başka gösterimlerle karışması olasılığı bulunduğunda 0 yerine 0_F ve 1 yerine de 1_F gösterimlerini tercih edeceğiz. Ayrıca $a, b \in F$ için $a+(-b)$ ifadesi için $a - b$ gösterimini kullanacağız.

Örnek 1 **(i)** *İyi bilinen cisimler arasında $\mathbb{Q}$, rasyonel sayılar cismi, $\mathbb{R}$, reel sayılar cismi ve $\mathbb{C}$, karmaşık sayılar cismi sayılabilir. Yukarıdaki aksiyomların bu üç küme için de sağlandığı kolayca gösterilebilir. Ancak, sonsuz eleman içeriyor olmalarından ötürü biz bu cisimlerin hiçbiri ile ilgilenmeyeceğiz.*

(ii) *$\mathbb{Z}_2$ ile gösterdiğimiz $\{0, 1\}$ kümesi, aşağıdaki gibi tanımlanan işlemlerle birlikte bir cisimdir.*

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

$\mathbb{Z}_2$ sahip olabileceğimiz en küçük cisimdir!

Lemma 1 *F bir cisim ve $a, b \in F$ olsun. Buna göre*
(i) $a \cdot 0 = 0$;
(ii) $-(ab) = (-a)b = a(-b)$. Özel olarak $(-1) \cdot a = -a$;
(iii) $ab = 0$ ise $a = 0$ veya $b = 0$.

Kanıt. (i) Dağılma özelliği kullanılarak $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ elde edilir. Eşitliğin her iki tarafı $a \cdot 0$ elemanı ile toplanırsa, $a \cdot 0 = 0$ bulunur.

(ii) $0 = 0 \cdot b = (a+(-a)) \cdot b = ab + (-a)b$ yazılabilir. Buna göre ab ile $(-a)b$ elemanları birbirlerinin toplamsal tersleridir. Yani $-(ab) = (-a)b$. Benzer şekilde $-(ab) = a(-b)$ olduğu da gösterilebilir. Özel olarak $b = -1$ alınırsa ikinci kısım da elde edilir.

(iii) $a \neq 0$ ise $0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$ bulunur. ■

Cisimlere örnek verirken $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ tamsayılar kümesini saymadığımıza dikkat ediniz. Gerçekten tamsayılar kümesi cisim aksiyomlarından (v-d) koşulunu sağlamamaktadır. Ancak yine de tamsayılar üzerinde bir cebirsel yapı mevcuttur. Bu yapılara halka diyeceğiz: Cisim aksiyomlarından (v–d) dışındaki tüm aksiyomları sağlayan boştan farklı bir kümeye **(değişmeli) halka** denir. Buna göre $\mathbb{Z}$ bir halkadır. Bu halkaya *tamsayılar halkası* diyeceğiz. Bir F cismi üzerindeki bütün polinomların kümesi,

$$F[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in F,\ n \geq 0\},$$

polinomlar arasındaki bilinen toplama ve çarpma işlemleri altında bir halka oluşturur.

Tanım *a, b ve m ($m > 1$) birer tamsayı olsun. Eğer m sayısı $a - b$ sayısını böler ise (simgesel olarak, $m \mid a - b$)*

"a, b'ye m modülüne göre denktir"

denir ve

$$a \equiv b \pmod{m}$$

şeklinde gösterilir.

Örnek 2 $25 \equiv 7 \pmod{9}$
$x \equiv 0 \pmod{m} \iff m \mid x$
$x \equiv 0 \pmod{2} \iff x$ *çift sayı*
$x \equiv 1 \pmod{2} \iff x$ *tek sayı*

a ve m tamsayıları için, bölüm algoritmasını kullanarak, tek türlü belirli bir r tamsayısı için $a = mq + r$ ve $0 \leq r < m$ olacak şekilde bir q tamsayısı bulunabilir. Dolayısıyla a sayısı, m modülüne göre $0, 1, \ldots, m-1$ sayılarından bir ve yalnız birine denktir. Buradaki r sayısına a'nın m ile bölümünden kalan denir. r kalanı $(a \pmod{m})$ şeklinde gösterilir.

$a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ ise

$$\begin{aligned} a \pm c &\equiv b \pm d \pmod{m} \\ ac &\equiv bd \pmod{m} \end{aligned}$$

olur.

Bir $m > 1$ tamsayısı için m modülüne göre tüm kalanların kümesini, yani $\{0, 1, \ldots, m-1\}$ kümesini $\mathbb{Z}_m$ veya $\mathbb{Z}/(m)$ şeklinde göstereceğiz. $\mathbb{Z}_m$ kümesinin elemanları arasında $\oplus$ ve $\otimes$ ile göstereceğimiz iki tane işlem aşağıdaki gibi tanımlansın:

$$\begin{aligned} a \oplus b &= (a + b \pmod{m}) \\ a \otimes b &= (ab \pmod{m}) \end{aligned}$$

Kolayca görülebilir ki bu işlemlerle birlikte $\mathbb{Z}_m$ kümesi bir halkadır. Bundan sonra $\mathbb{Z}_m$ halkası üzerindeki $\oplus$ ve $\otimes$ işlemlerini sırasıyla $+$ ve $.$ şeklinde göstereceğiz.

Örnek 3 *Daha önce $\mathbb{Z}_2$ ile gösterdiğimiz iki elemanlı cisim, tam olarak $m = 2$ için yukarıdaki gibi tanımlanan halkadır. Özel olarak sıfırdan farklı her elemanın çarpma işlemine göre tersi bulunduğundan bu halka bir cisimdir.*

Örnek 4 *$m = 4$ alarak dört elemanlı $\mathbb{Z}_4$ halkasını tanımlayabiliriz. $\mathbb{Z}_4$ halkası için toplam ve çarpım tabloları aşağıdaki gibi verilebilir:*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Dikkat edilirse $\mathbb{Z}_4$ halkası cisim değildir. Çünkü çarpım tablosundan da görülebileceği gibi 2 elemanının çarpımsal tersi yoktur.

Yukarıdaki iki örnekten de görülebileceği gibi $\mathbb{Z}_m$, bazı m sayıları için cisim, diğer bazı m sayıları için de yalnızca bir halkadır. Aşağıdaki teorem ile bu durumu açıklığa kavuşturacağız.

Teorem 2 *$\mathbb{Z}_m$ bir cisimdir ancak ve ancak m bir asal sayıdır.*

Kanıt. Kabul edelim ki m bir asal sayı olmasın. Bu durumda $m = ab$ olacak şekilde $1 < a, b < m$ sayıları bulunabilir. Böylece $\mathbb{Z}_m$ içinde $a \neq 0$ ve $b \neq 0$ olduğu halde $0 = m = a \cdot b$ olacağından Lemma 1 (iii) den dolayı $\mathbb{Z}_m$ cisim olamaz.

Şimdi m bir asal sayı olsun. Bir $a \in \mathbb{Z}_m$ için $0 < a < m$ olduğundan a ile m aralarında asaldır. Buna göre $ua + vm = 1$ oacak şekilde u ve v tamsayıları vardır. Burada özel olarak $0 \leq u \leq m - 1$ seçebiliriz. Böylece $ua \equiv 1 \pmod{m}$ elde edilir. Dolayısıyla $u = a^{-1}$, yani a elemanının $\mathbb{Z}_m$ içinde bir çarpımsal tersi vardır. $a \neq 0$ keyfi olarak seçildiğinden $\mathbb{Z}_m$ halkası bir cisim olur. ■

Bir R halkası ve $n \geq 1$ tamsayısı için $a \in R$ ise na ya da $n \cdot a$ ifadesi ile

$$\sum_{i=1}^{n} a = \underbrace{a + a + \cdots + a}_{n}$$

toplamı kastedilmektedir. $0 \cdot a = 0_R$ ve her $n < 0$ tamsayısı için $n \cdot a = -(|n| \cdot a) = |n| \cdot (-a)$ olarak tanımlansın. Buna göre aşağıdaki önermeyi verebiliriz.

Önerme 3 *R bir halka, $m, n \in \mathbb{Z}$ ve $a, b \in R$ olsun. Buna göre*

(i) $m \cdot a = (m \cdot 1_R)a$.

(ii) $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$. *Özel olarak,* $(mn) \cdot 1_R = (m \cdot 1_R)(n \cdot 1_R)$.

(iii) $(mn) \cdot a = m \cdot (n \cdot a) = n \cdot (m \cdot a)$.

(iv) $(m + n) \cdot a = m \cdot a + n \cdot a$.

(v) $n \cdot (a + b) = n \cdot a + n \cdot b$.

Kanıt. (i) $m > 0$ olsun. Buna göre

$$\underbrace{a + \cdots + a}_{m} = (\underbrace{1_R + \cdots + 1_R}_{m})a = (m \cdot 1_R)a$$

olur. $m = 0$ ise $m \cdot a = 0 = 0_R \cdot a = (m \cdot 1_R)a$ bulunur. $m < 0$ olsun. Buna göre

$$m \cdot a = -(|m| \cdot a) = -[(|m| \cdot 1_R)a] = [-(|m| \cdot 1_R)]a = [(-|m|) \cdot 1_R]a = (m \cdot 1_R)a$$

elde edilir.

(ii) $m, n > 0$ ise

$$(m \cdot a)(n \cdot b) = (\overbrace{a + \cdots + a}^{m})(\overbrace{b + \cdots + b}^{n}) = \overbrace{ab + \cdots + ab}^{mn} = (mn) \cdot (ab)$$

olur. m ya da n'den en az biri sıfır ise işimiz tamam. m ya da n den biri, diyelim ki m, negatif olsun. Bu durumda $|m| > 0$ olacağından

$$\begin{aligned}(m \cdot a)(n \cdot b) &= [-(|m| \cdot a)](n \cdot b) = -[(|m| \cdot a)(n \cdot b)] \\ &= -[(|m|n) \cdot (ab)] = (-|m|n) \cdot (ab) \\ &= (mn) \cdot (ab)\end{aligned}$$

elde edilir.

(iii) $(mn) \cdot a \overset{(ii)}{=} (m \cdot 1_R)(n \cdot a) \overset{(i)}{=} m \cdot (n \cdot a)$

■

Tanım *F bir cisim olsun. Eğer $n \cdot 1_F = 0$ olacak şekilde bir n pozitif tamsayısı varsa bu n sayılarının en küçüğüne F cisminin **karakteristiği** denir. Eğer böyle bir n sayısı bulunamaz ise o zaman F cisminin karakteristiği sıfırdır diyeceğiz.*

Kolayca görülebilir ki bir F cismi ve bir n pozitif tamsayısı için $n \cdot 1_F = 0$ ancak ve ancak her $a \in F$ için $n \cdot a = 0$. Buna göre bir cismin karakteristiği sıfırdan farklı ise bu sayı, o cismin bütün elemanlarını sıfırlayan en küçük pozitif tamsayıdır.

Örnek 5 *$\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ cisimlerinin karakteristiği sıfırdır. p bir asal sayı olmak üzere $\mathbb{Z}_p$ cisminin karakteristiği p sayısıdır.*

Teorem 4 *Bir cismin karakteristiği ya sıfırdır ya da bir asal sayıdır.*

Kanıt. Kabul edelim ki bir F cisminin karakteristiği sıfırdan farklı bir p sayısı olsun. $1 \cdot 1 = 1 \neq 0$ olduğundan $p \neq 1$ dir. Kabul edelim ki p asal olmasın. Bu taktirde $p = mn$ olacak şekilde $1 < m, n < p$ tamsayıları vardır. $a = m \cdot 1_F$ ve $b = n \cdot 1_F$ olsun. Buna göre, Önerme 3 (ii)'den,

$$a \cdot b = (m \cdot 1_F)(n \cdot 1_F) = (mn) \cdot 1_F = p \cdot 1_F = 0$$

olur. Lemma 1 (iii) den, $a = 0$ veya $b = 0$ bulunur. $m \cdot 1_F = 0$ veya $n \cdot 1_F = 0$ olacağından bu durum p sayısının seçimi ile çelişir. ■

E ve F iki cisim ve $F \subseteq E$ olsun. Eğer E üzerindeki toplama ve çarpma işlemleri F'ye kısıtlandığında, F üzerindeki toplama ve çarpma işlemleri ile aynı oluyorsa F cismine E'nin bir **altcismi** denir.

Örneğin $\mathbb{Q}$ rasyonel sayılar cismi, hem $\mathbb{R}$ reel sayılar cisminin, hem de $\mathbb{C}$ karmaşık sayılar cisminin bir altcismidir. Ayrıca $\mathbb{R}$ de $\mathbb{C}$'nin bir altcismidir.

Lemma 5 *F bir cisim ve $E \subseteq F$ olsun. Buna göre E, F'nin bir altcismidir ancak ve ancak $1_F \in E$ ve her $a, b \in E$ $(b \neq 0)$ için, $a - b, ab^{-1} \in E$ olur.*

Kanıt. ($\Rightarrow$) gerektirmesi açık olduğundan yalnızca ($\Leftarrow$) gerektirmesini kanıtlayacağız. E üzerinde tanımlı toplama ve çarpma işlemleri, F'nin işlemleri olduğundan yalnızca E'nin bir cisim olduğunu göstermek yeterlidir. $a, b \in E$ olsun. $a \in E$ olduğundan, kabulümüzden dolayı, $0 = a - a \in E$ olur. Şimdi $0 \in E$ olduğundan $-b = 0 - b \in E$ elde edilir. Dolayısıyla $a + b = a - (-b) \in E$ olur. Böylece E toplama işlemine göre kapalıdır. Şimdi $b \neq 0$ olduğunu varsayalım. $1_F \in E$ olduğundan $b^{-1} = 1_F b^{-1} \in E$ olcağından $ab = a(b^{-1})^{-1} \in E$ elde edilir. Yani E, çarpmaya göre de kapalıdır. E, F'nin bir altkümesi ve F de bir cisim olduğundan (ii), (iii) ve (iv) numaralı cisim aksiyomları sağlanır. Böylece E bir cisim olur. ■

E ve F iki cisim olsun. E'den F'ye birebir ve örten $f : E \to F$ dönüşümü tanımlanabiliyor olsun. Eğer her $x, y \in E$ için $f(x + y) = f(x) + f(y)$ ve $f(xy) = f(x)f(y)$ ise E ve F cisimleri için **eşyapılı cisimler** denir. Bu durumda f dönüşümüne de bir **eşyapı dönüşümü** diyeceğiz. Eşyapılı cisimler, cebirsel olarak, birbirlerinin yerlerini tutabilen cisimlerdir. Çünkü bu cisimlerin elemanları, işlem tabloları bozulmayacak şekilde birebir eşlenebilmektedir. Örneğin $F = \{a, b\}$ kümesi,

Δ	a	b
a	a	b
b	b	a

$*$	a	b
a	a	a
b	a	b

şeklinde tanımlanan Δ ve $*$ işlemleri ile birlikte bir cisim olur. Aslında bu cisim $\mathbb{Z}_2$ cismi ile eşyapılıdır. Çünkü yukarıdaki tablolarda Δ yerine $+$, $*$ yerine $\times$, a ve b yerine de sırasıyla 0 ve 1 yazılırsa $\mathbb{Z}_2$ üzerinde tanımlanan $+$ ve $\times$ işlemlerinin tabloları elde edilmiş olur. Böylece "iki cisim cebirsel olarak aynı yapıya sahiptir" diyebiliriz.

Önerme 6 *F, karakteristiği p olan bir cisim olsun. Buna göre F'nin p elemanlı bir altcismi vardır. Gerçekte bu altcisim $\mathbb{Z}_p$ ile eşyapılıdır.*

Kanıt. F'nin

$$S = \{n \cdot 1_F : n \in \mathbb{Z}\}$$

altkümesini alalım. Öncelikle

$$S = \{r \cdot 1_F : r \in \mathbb{Z},\ 0 \leq r < p\} = \{0_F, 1_F, 2 \cdot 1_F, \ldots, (p-1) \cdot 1_F\}$$

olduğunu göstereceğiz. $x \in S$ olsun. Buna göre $x = n \cdot 1_F$ olacak şekilde bir n tamsayısı vardır. Bölüm algoritmasından dolayı

$$n = pq + r, \qquad 0 \leq r < p$$

olacak şekilde tek türlü belirli r sayısı ile bir q tamsayısı bulunabilir. Buradan, Önerme 3'ün (iii). ve (iv). şıklarını kullanarak,

$$x = n \cdot 1_F = (pq + r) \cdot 1_F = (pq) \cdot 1_F + r \cdot 1_F = q \cdot (\underbrace{p \cdot 1_F}_{0}) + r \cdot 1_F = r \cdot 1_F$$

elde ederiz. Böylece yukarıdaki eşitlik gösterilmiş olur. $0 \leq r, s < p$ olmak üzere S'nin $r \cdot 1_F$ ve $s \cdot 1_F$ gibi iki elemanına F'nin $+$ ve $\cdot$ işlemleri uygulanırsa, Önerme 3 gereğince,

$$\begin{aligned}(r \cdot 1_F) + (s \cdot 1_F) &= (r+s) \cdot 1_F = (r + s \pmod{p}) \cdot 1_F \\ (r \cdot 1_F)(s \cdot 1_F) &= (rs) \cdot 1_F = (rs \pmod{p}) \cdot 1_F\end{aligned}$$

elde edilir. Bundan sonra, Lemma 5 de kullanarak, S'nin, F'nin $\mathbb{Z}_p$ ile eşyapılı bir altcismi olduğunu görmek zor değildir. ■

Yukarıdaki önermede geçen p elemanlı altcisme, F'nin **asal cismi** denir. Aşağıdaki teoremin doğrudan bir sonucu olarak, asal cisim F'nin en küçük altcismi olur.

Teorem 7 *F karakteristiği p olan sonlu bir cisim ise F'nin, bir $n \geq 1$ tamsayısı için, p^n tane elemanı vardır.*

Kanıt. F^* kümesinden bir α_1 elemanı seçelim. Öncelikle $0 \cdot \alpha_1, 1 \cdot \alpha_1, \ldots, (p-1) \cdot \alpha_1$ elemanlarının ikişer ikişer birbirlerinden farklı olduklarını göstereceğiz. Kabul edelim ki $0 \leq i \leq j \leq p-1$ için $i \cdot \alpha_1 = j \cdot \alpha_1$ olsun. Buna göre $(j-i) \cdot \alpha_1 = 0$ ve $0 \leq j-i \leq p-1$ olur. F'nin karakteristiği p olduğundan $j - i = 0$, yani $j = i$ elde edilir.

Eğer $F = \{0 \cdot \alpha_1, 1 \cdot \alpha_1, \ldots, (p-1) \cdot \alpha_1\}$ ise işimiz tamam. Aksi halde $F \setminus \{0 \cdot \alpha_1, 1 \cdot \alpha_1, \ldots, (p-1) \cdot \alpha_1\}$ kümesinden bir α_2 elemanı seçebiliriz. Şimdi ise $0 \leq a_1, a_2 \leq p-1$ olmak üzere, mümkün olan tüm (a_1, a_2) ikilileri için yazılabilecek $a_1\alpha_1 + a_2\alpha_2$ elemanlarının ikişer ikişer birbirlerinden farklı olduklarını göstereceğiz. Kabul edelim ki $0 \leq a_1, a_2, b_1, b_2 \leq p-1$ için

$$a_1\alpha_1 + a_2\alpha_2 = b_1\alpha_1 + b_2\alpha_2$$

olsun. Eğer $a_2 \neq b_2$ ise bu durumda

$$\alpha_2 = [(b_2 - a_2) \cdot 1_F]^{-1}(a_1 - b_1)\alpha_1 = [(b_2 - a_2) \cdot 1_F]^{-1}[(a_1 - b_1) \cdot 1_F] \cdot \alpha_1$$

olur. $[(b_2 - a_2) \cdot 1_F]^{-1}[(a_1 - b_1) \cdot 1_F]$ elemanı F'nin asal cismi içinde olacağından bir $0 \leq n \leq p-1$ için

$$[(b_2 - a_2) \cdot 1_F]^{-1}[(a_1 - b_1) \cdot 1_F] = n \cdot 1_F$$

yazılabilir. Buna göre $\alpha_2 = n \cdot \alpha_1$ elde edilir ki bu durum α_2'nin seçimi ile çelişir. Dolayısıyla $a_2 = b_2$ olur. Bir önceki adımdan dolayı da nihayet $(a_1, b_1) = (a_2, b_2)$ elde edilir. Bu şekilde devam edersek, F sonlu sayıda eleman içerdiğinden, öyle $\alpha_1, \ldots, \alpha_n$ elemanları bulabiliriz ki

$$F = \{a_1\alpha_1 + \cdots + a_n\alpha_n : a_1, \ldots, a_n \in \mathbb{Z}_p\}$$

ve $(a_1, \ldots, a_n)$ sıralı n–lilerinin mümkün olan her seçimi için $a_1\alpha_1 + \cdots + a_n\alpha_n$ tipindeki elemanlar birbirlerinden farklı olur. Dolayısıyla $|F| = p^n$ elde edilir. ■

3.2 Polinom Halkaları

Bir cisim üzerinde tanımlanan polinomların, bilinen polinom toplamı ve çarpımı ile birlikte halka yapısına sahip olduğunu daha önce söylemiştik. Buna göre aşağıdaki tanımı verebiliriz.

Tanım *F bir cisim olsun.*

$$F[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in F,\ n \geq 0 \right\}$$

*kümesine F üzerindeki **polinom halkası** adı verilir. $F[x]$ kümesinin her elemanına bir **polinom** denir. $P(x) = \sum_{i=0}^{n} a_i x^i$ polinomu için $a_n \neq 0$ ise n sayısına $P(x)$ polinomunun **derece**si denir ve $\deg(P(x)) = n$ şeklinde yazılır. Özel olarak $\deg(0) = -\infty$ olarak tanımlanır. $a_0, \ldots, a_n$ elemanlarının herbirine $P(x) = \sum_{i=0}^{n} a_i x^i$ polinomunun katsayısı denir. Özel olarak a_0 katsayısına $P(x)$'in sabit terimi, a_n katsayısına ise $P(x)$'in başkatsayısı adı verilir. $P(x) = \sum_{i=0}^{n} a_i x^i$ polinomu için $a_n = 1$ ise o zaman $P(x)$ polinomuna bir **monik polinom** denir. Pozitif dereceli bir $P(x) \in F[x]$ polinomu için $P(x) = f(x)g(x)$ olacak şekilde dereceleri $P(x)$'in derecesinden küçük sabit olmayan $f(x), g(x) \in F[x]$ polinomları bulunabiliyor ise $P(x)$ polinomuna F üzerinde **indirgenebilir polinom** adı verilir. (Aksi halde $P(x)$ polinomuna F üzerinde **indirgenemez polinom** denir.)*

Örnek 6 **(i)** *$P(x) = x^4 + 2x^3 + 2x + 2 \in \mathbb{Z}_3[x]$ polinomunun derecesi 4'tür. $P(x)$, $\mathbb{Z}_3$ üzerinde bir indirgenebilir polinomdur çünkü $P(x) = (x^2 + 1)(x^2 + 2x + 2)$ yazılabilir.*

(ii) *$g(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$ polinomu derecesi 2 olan bir indirgenemez polinomdur.*

(iii) *$1 + x + x^3$ ve $1 + x^2 + x^3$ polinomları $\mathbb{Z}_2$ üzerinde indirgenemezdir.*

Teorem 8 (Polinomlar için Bölüm Algoritması) *F bir cisim ve $P(x), S(x) \in F[x]$ $(P(x) \neq 0)$ olsun. $\deg(P(x)) \geq 1$ ise $S(x) = P(x)Q(x) + R(x)$ ve $R(x) = 0$ veya $der(R(x)) < der(P(x))$ olacak şekilde tek türlü belirli $Q(x), R(x) \in F[x]$ polinomları bulunabilir.*

Tanım *$P(x)$, $S(x)$, $Q(x)$ ve $R(x)$ yukarıdaki teoremde olduğu gibi alınsın. $R(x)$ polinomuna $S(x)$'in $P(x)$ ile bölümünden kalan adı verilir ve $(S(x) \pmod{P(x)})$ ile gösterilir.*

Örnek 7 *$\mathbb{Z}_5[x]$ halkasından $3x^4 + 2x^3 + 3x + 2$ ve $2x^2 + 1$ polinomlarını düşünelim. Doğal sayılar arasındaki bilinen bölme işleminin benzerini uygulayarak*

$$3x^4 + 2x^3 + 3x + 2 = (2x^2 + 1)(4x^2 + x + 3) + 2x + 4$$

bulunabilir. Buna göre $3x^4 + 2x^3 + 3x + 2$ polinomunun $2x^2 + 1$ ile bölümünden kalan $2x + 4$ polinomudur. Yani

$$(3x^4 + 2x^3 + 3x + 2 \pmod{2x^2 + 1}) = 2x + 4$$

Tanım *F bir cisim ve $P(x), Q(x) \in F[x]$ olsun.*

(i) *Eğer bir $T(x) \in F[x]$ polinomu için $P(x) = T(x)S(x)$ olacak şekilde bir $S(x) \in F[x]$ polinomu varsa bu durumda $T(x)$, $P(x)$'i böler denir ve $T(x) \mid P(x)$ şeklinde gösterilir. Burada $P(x)$ polinomu için $T(x)$ (ve elbette ki $S(x)$) polinomunun bir katı denir.*

(ii) *$P(x)$ ve $Q(x)$ polinomlarını ortak olarak bölen en büyük dereceli monik polinoma, $P(x)$ ve $Q(x)$ polinomlarının* ***en büyük ortak böleni*** *denir ve $(P(x), Q(x))$ ile gösterilir. Eğer $(P(x), Q(x)) = 1$ ise "$P(x)$ ile $Q(x)$ aralarında asaldır" denir.*

(iii) *Hem $P(x)$'in hem de $Q(x)$'in katı olan en küçük dereceli monik polinoma $P(x)$ ve $Q(x)$ polinomlarının* ***en küçük ortak katı*** *denir ve $[P(x), Q(x)]$ ile gösterilir.*

Teorem 9 (Euclid Algoritması) *F bir cisim ve $P(x), Q(x) \in F[x]$ $(Q(x) \neq 0)$ olsun. Aşağıda verilen işlem dizisini $r_n(x) = 0$ olana kadar uygulayalım:*

$$\begin{aligned}
P(x) &= Q(x)t_1(x) + r_1(x), && \deg(r_1(x)) < \deg(Q(x)) \\
Q(x) &= r_1(x)t_2(x) + r_2(x), && \deg(r_2(x)) < \deg(r_1(x)) \\
r_1(x) &= r_2(x)t_3(x) + r_3(x), && \deg(r_3(x)) < \deg(r_2(x)) \\
&\vdots \\
r_{n-3}(x) &= r_{n-2}(x)t_{n-1}(x) + r_{n-1}(x), && \deg(r_{n-1}(x)) < \deg(r_{n-2}(x)) \\
r_{n-2}(x) &= r_{n-1}(x)t_n(x) + r_n(x), && r_n(x) = 0.
\end{aligned}$$

Buna göre $r_{n-1}(x)$'in başkatsayısı c ise $(P(x), Q(x)) = c^{-1}r_{n-1}(x)$ olur.

Örnek 8 *$\mathbb{Z}_2[x]$ halkasında, $x^5 + x^4 + x^2 + 1$ ile $x^3 + x^2 + x$ polinomlarının en büyük ortak bölenini Euclid Algoritması'nı kullanarak hesaplayalım:*

$$\begin{aligned}
x^5 + x^4 + x^2 + 1 &= (x^3 + x^2 + x)(x^2 + 1) + x + 1 \\
x^3 + x^2 + x &= (x + 1)(x^2 + 1) + 1 \\
x + 1 &= 1(x + 1) + 0
\end{aligned}$$

olacağından $(x^5 + x^4 + x^2 + 1\ ,\ x^3 + x^2 + x) = 1$ elde edilir. Yani verilen polinomlar aralarında asaldır.

Not (i) İndirgenemez polinomların, sabit polinomlar ve (bir sabit farkıyla) kendisi dışında hiçbir polinoma bölünemeyen polinomlar olduğu anlaşılmaktadır. (İndirgenemez polinomların bu yönüyle asal sayılara olan benzerliğine dikkat ediniz.)

(ii) Cebir kaynaklarının pek çoğunda da görülebileceği gibi, bir F cismi için, $F[x]$ polinom halkasındaki sabit olmayan her polinom, (sabit farkıyla tek türlü belirli) indirgenemez polinomların bir sonlu çarpımı şeklinde yazılabilmektedir. ($F[x]$ polinom halkasının bu özelliği ile asal çarpanlara ayrılma özelliğine sahip tamsayılar halkasına ne kadar benzediğine dikkat ediniz.)

(iii) Bir F cismi için $P(x), Q(x) \in F[x]$ olsun. Buna göre

$$P(x) = \alpha p_1(x)^{a_1} \dots p_n(x)^{a_n} p_{n+1}(x)^{a_{n+1}} \dots p_k(x)^{a_k}$$

ve

$$Q(x) = \beta p_1(x)^{b_1} \dots p_n(x)^{b_n} q_{n+1}(x)^{b_{n+1}} \dots q_t(x)^{b_t}$$

olacak şekilde $a_i, b_j > 0$ tamsayıları $(1 \leq i \leq k, 1 \leq j \leq t)$, $\alpha, \beta \in F$ ve $p_1(x), \dots, p_k(x)$, $q_{n+1}(x), \dots, q_t(x) \in F[x]$ birbirinden farklı *monik indirgenemez* polinomları vardır. Buna göre

$$(P(x), Q(x)) = p_1(x)^{\min\{a_1, b_1\}} \dots p_n(x)^{\min\{a_n, b_n\}}$$

ve

$$[P(x),Q(x)] = p_1(x)^{\text{maks}\{a_1,b_1\}} \dots p_n(x)^{\text{maks}\{a_n,b_n\}} p_{n+1}(x)^{a_{n+1}} \dots p_k(x)^{a_k} q_{n+1}(x)^{b_{n+1}} \dots q_t(x)^{b_t}$$

yazılabilir. Buna göre $P(x)Q(x) = (P(x),Q(x))[P(x),Q(x)]$ olduğu kolayca görülebilir.

(iv) Yukarıdaki Euclid Algoritması'ndan, tıpkı tamsayılarda olduğu gibi, $P(x), Q(x) \in F[x]$ gibi sıfırdan farklı iki polinom için

$$(P(x),Q(x)) = P(x)u(x) + Q(x)v(x)$$

ve $\text{der}(u(x)) < \text{der}(Q(x))$, $\text{der}(v(x)) < \text{der}(P(x))$ olacak şekilde $u(x), v(x) \in F[x]$ polinomları bulunabilir. Örneğin daha önce Örnek 8'de, $x^5+x^4+x^2+1$, $x^3+x^2+x \in \mathbb{Z}_2[x]$ polinomları için

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

olduğunu göstermiştik. Aynı algoritmadan, adımlarını geri alarak,

$$1 = \left(x^5 + x^4 + x^2 + 1\right)\left(x^2 + 1\right) + \left(x^3 + x^2 + x\right)x^4$$

eşitliği elde edilebilir. Buna göre $u(x) = x^2 + 1$ ve $v(x) = x^4$ olur.

Yukarıdaki notlardan da anlaşılacağı gibi $\mathbb{Z}$ tamsayılar halkası ile herhangi bir F cismi için $F[x]$ polinom halkası arasında asal sayılar ile indirgenemez polinomların karşılık geldiği birtakım benzerlikler vardır. Bu benzerliklere ek olarak, bir m tamsayısı için $\mathbb{Z}_m = \mathbb{Z}/(m)$ halkasını inşa ettiğimiz gibi bir $P(x) \in F[x]$ polinomu için de $F[x]/(P(x))$ halkasını inşa edebiliriz. Buna göre $F[x]/(P(x)) = \{r(x) : r(x) \in F[x]$ ve $\text{der}(r(x)) < \text{der}(P(x))\}$ ve herhangi $r(x), s(x) \in F[x]/(P(x))$ için toplama ve çarpma işlemleri sırasıyla

$$r(x) \oplus s(x) = (r(x) + s(x) \pmod{P(x)})$$

ve

$$r(x) \otimes s(x) = (r(x)s(x) \pmod{P(x)})$$

şeklinde tanımlanırsa, bu işlemlerle birlikte, $F[x]/(P(x))$ kümesinin bir halka olacağını görmek zor değildir. Burada $\oplus$ ve $\otimes$ ile gösterdiğimiz toplama ve çarpma işlemleri için de, daha önce olduğu gibi, $+$ ve $\cdot$ simgelerini kullanmaya devam edeceğiz.

Teorem 10 *F bir cisim ve $P(x) \in F[x]$ olsun. $F[x]/(P(x))$ kümesi, yukarıdaki gibi tanımlanan toplama ve çarpma işlemleri ile birlikte bir halkadır. Ayrıca, $F[x]/(P(x))$'in cisim olması için gerek ve yeter koşul $P(x)$'in F üzerinde indirgenemez olmasıdır.*

Kanıt. Teorem 2'nin kanıtında kullandığımız yöntemin aynısı kullanılarak gösterilebilir. ■

Dikkat edilirse bir F cismi üzerinde derecesi $n \geq 1$ olan bir $P(x)$ polinomu için $F[x]/(P(x))$ halkası derecesi n'den küçük olan F üzerindeki tüm polinomlardan oluşur. Yani

$$F[x]/(P(x)) = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_0, \dots a_{n-1} \in F\}.$$

Buna göre $P(x)$ bir doğrusal polinom (yani derecesi 1 olan bir polinom) ise $F[x]/(P(x))$ halkası F cisminin ta kendisidir.

Örnek 9 **(i)** $\mathbb{R}[x]/(x^2+1)$ *halkasını ele alalım.* $\mathbb{R}[x]/(x^2+1) = \{ax+b : a,b \in \mathbb{R}\}$ *yazılabilir.* x^2+1 *polinomu* $\mathbb{R}$ *üzerinde indirgenemez olduğundan bu halka bir cisimdir. Aslında* x *ile* i *karmaşık sayısı eşleştirilirse bu cismin* $\mathbb{C}$ *karmaşık saylar cismi ile eşyapılı olduğu kolayca görülebilir.*

(ii) $\mathbb{Z}_2[x]/(x^2+1) = \{0, 1, x, 1+x\}$ *halkasını düşünelim. Bu halka üzerindeki toplama ve çarpma işlem tablolaları aşağıdaki gibi verilebilir:*

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0	$1+x$	$1+x$	0

Buna göre çarpım tablosuna bakarak bu halkanın bir cisim olamayacağını söyleyebiliriz ($(1+x)^2 = 0$*).*

(iii) *Şimdi de* $\mathbb{Z}_2[x]/(x^2+x+1) = \{0, 1, x, 1+x\}$ *halkasını ele alalım.* x^2+x+1 *polinomu* $\mathbb{Z}_2$ *üzerinde indirgenemez olduğundan, Teorem 10'dan dolayı bu halka bir cisim olur. Bunu, ayrıca, aşağıdaki işlem tablolarına bakarak söylemek te mümkündür.*

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Yukarıdaki yöntemle dört elemanlı bir cisim inşa etmiş oluruz. Bu cismin elemanlarının dereceleri en fazla 1 *olan polinomlar olduğu görülüyor. Fakat bu elemanları farklı yollarla yazmak ta mümkündür. Örneğin, bu polinomları azalan kuvvet sırasına göre yazdıktan sonra katsayılarını aynı sıra ile tekrar yazarak ikili düzende bir sayı elde edebiliriz. Yani* $a_n x^n + \cdots + a_1 x + a_0$ *şeklindeki bir polinoma ikili düzendeki* $a_n \ldots a_1 a_0$ *sayısı karşılık gelir. Polinomları ikili düzendeki bu sayılarla ifade edebileceğimiz gibi bu sayıları ondalık düzende yazarak ta kullanabiliriz. Buna göre yukarıda elde ettiğimiz cismin elemanlarını aşağıdaki gibi dönüştürebiliriz:*

polinom	*ikilik sayı*	*ondalık sayı*
0	00	0
1	01	1
x	10	2
$1+x$	11	3

Polinomları ondalık düzende yazarak yeniden ifade edersek, yukarıdaki işlem tabloları aşağıdaki hale dönüşür:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Bu tabloların $\mathbb{Z}_4$ *halkasının işlem tablolarından farklı olduğuna dikkat ediniz.*

Yukarıdaki işlemi herhangi bir $n > 1$ *tamsayısı için* $\mathbb{Z}_n$ *üzerindeki tüm polinomlara genişletebiliriz.*

3.3 Sonlu Cisimlerin Yapısı

Bir önceki bölümde indirgenemez polinomları kullanarak nasıl cisim inşa edebileceğimizi gördük. Bu bölümde sonlu cisimlerin hepsinin bu yolla elde edilen cisimlerden ibaret olduğunu göstereceğiz. Hatırlayacak olursak bir F cismi ile bir $P(x) \in F[x]$ indirgenemez polinomu için $F[x]/(P(x))$ ile gösterdiğimiz bir cisim tanımlamıştık. Bu yeni cismin elemanlarını, x yerine α gösterimini kullanarak yeniden yazarsak (Örnek 9 (i)'de yaptığımıza benzer olarak), daha önce tanımlanan toplama ve çarpma işlemlerini yeni yazılan elemanlar için taşımak suretiyle

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, \ldots, a_{n-1} \in F\}$$

ile gösterilen ve $F[x]/(P(x))$ cismi ile eşyapılı bir cisim elde edebiliriz. Bu yolla $F[x]/(P(x))$ cisminin elemanları ile F üzerindeki polinomlar arasında meydana gelebilecek bir karışıklığın da önüne geçmiş oluruz. Burada bir $a \in F$ elemanını $F(\alpha)$ içindeki $a + 0\alpha + \cdots + 0\alpha^{n-1}$ elemanı ile özdeş tutarak $F \subseteq F(\alpha)$ alabiliriz. Ayrıca tanımdan dolayı $P(\alpha) = 0$ olur. Dolayısıyla F cismini $P(x)$ polinomunun bir kökünü içeren $F(\alpha)$ cismine genişletmiş oluyoruz. Aslında göreceğiz ki F'yi $P(x)$ polinomunun bütün köklerini içerecek şekilde genişletebiliriz. Daha önce aşağıdaki tanımı verelim:

Tanım **(i)** *E bir cisim ve F, E'nin bir altcismi ise E cismine F'nin bir genişlemesi denir.*

(ii) *F bir cisim ve $f(x) \in F[x]$ olsun. Eğer $f(x)$, katsayıları F'nin elemanı olan birinci dereceden (doğrusal) polinomların çarpımı şeklide yazılabiliyor ise, yani*

$$f(x) = \alpha(x - \alpha_1)\cdots(x - \alpha_n)$$

olacak şekilde $\alpha, \alpha_1, \ldots, \alpha_n \in F$ elemanları bulunabiliyor ise, o zaman $f(x)$ için "F üzerinde doğrusal çarpanlarına ayrılabilir" denir.

(iii) *F bir cisim ve $f(x) \in F[x]$ olsun. F'nin bir E genişlemesi için $f(x)$, E üzerinde doğrusal çarpanlarına ayrılabilir fakat E'nin F'yi içeren hiçbir öz altcismi üzerinde doğrusal çarpanlarına ayrılamaz ise E cismine $f(x)$'in (F üzerinde) bir **parçalanış cismi** denir.*

Örnek 10 **(i)** *$x^2 + 1 \in \mathbb{Q}[x]$ polinomunun parçalanış cismi, $\mathbb{C}$ karmaşık sayılar cisminin $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ altcismidir.*

(ii) *$x^2 - 2 \in \mathbb{Q}[x]$ polinomunun parçalanış cismi, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ cismidir.*

Aşağıdaki teorem herhangi bir cisim üzerindeki herhangi bir polinom için bir parçalanış cismi bulabileceğimizi söylemekle kalmıyor, aynı zamanda bir polinomun iki parçalanış cisminin de eşyapılı olacağını söylüyor. Asıl konudan uzaklaşmamak amacıyla bu teoremin kanıtını burada vermeden geçeceğiz.

Teorem 11 *F bir cisim ve $f(x) \in F[x]$ ise $f(x)$'in F üzerinde bir parçalanış cismi vardır ve eşyapılı olma farkıyla tektir.*

Lemma 12 *F bir cisim ve $|F| = q < \infty$ olsun. Buna göre her $\beta \in F$ için $\beta^q = \beta$ olur.*

Kanıt. $\beta = 0$ için durum açıktır. $\beta \neq 0$ olsun. $F^* = \{\beta_1, \ldots, \beta_{q-1}\}$ olarak yazalım. Buna göre $F^* = \{\beta\beta_1, \ldots, \beta\beta_{q-1}\}$ yazabiliriz. Dolayısıyla

$$\beta_1 \ldots \beta_{q-1} = \beta\beta_1 \ldots \beta\beta_{q-1} = \beta^{q-1}\beta_1 \ldots \beta_{q-1},$$

yani $\beta^{q-1} = 1$ elde edilir. Dolayısıyla $\beta^q = \beta$ bulunur. ■

Lemma 13 *p bir asal sayı, n ve r, $r < p^n$ olacak şekilde iki pozitif tamsayı olsun. Buna göre p^n'nin r'li kombinasyonu $\binom{p^n}{r}$ ile gösterilirse*

$$p \mid \binom{p^n}{r}$$

olur.

Kanıt. Uygun bir $0 < m < n$ tamsayısı için $(r, p^n) = p^m$ yazabiliriz. Buna göre

$$\begin{aligned}\binom{p^n}{r} &= \frac{p^n(p^n-1)\ldots(p^n-r+1)}{r!} \\ &= \frac{p^n}{r}\binom{p^n-1}{r-1} = \frac{p^{n-m}}{r/p^m}\binom{p^n-1}{r-1}\end{aligned}$$

yazılabilir. $\binom{p^n}{r}, \binom{p^n-1}{r-1} \in \mathbb{Z}$ ve p^{n-m} ile r/p^m tamsayıları aralarında asal olduğundan $r/p^m | \binom{p^n-1}{r-1}$ olur. Yani $\binom{p^n}{r}$ sayısı p^{n-m}'nin, özel olarak ta p'nin, bir katıdır. ■

Yukarıdaki lemmayı Binom Teoremi ile birlikte kullanırsak, karakteristiği $p > 0$ olan bir F cisminden alınan herhangi iki α ve β elemanı ile her $n \geq 0$ tamsayısı için

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

olacağını gösterebiliriz.

Teorem 14 *Her p asal sayısı ve $n \geq 1$ tamsayısı için p^n elemanlı bir cisim vardır ve eşyapılı olma farkıyla tektir.*

Kanıt. (Varlık) Teorem 11 gereğince $x^{p^n} - x \in \mathbb{Z}_p[x]$ polinomunun $\mathbb{Z}_p$ üzerinde bir E parçalanış cismi vardır. Buna göre E, $x^{p^n} - x$ polinomunun tüm köklerini içerir. $x^{p^n} - x$ polinomunun (E içindeki) tüm köklerinin kümesi K olsun. Önce $|K| = p^n$ olduğunu göstereceğiz. Bunun için $x^{p^n} - x$ polinomunun tüm köklerinin tek katlı olduğunu, yani her $\alpha \in K$ için $(x-\alpha)^2 \nmid x^{p^n} - x$ olduğunu göstermek yeterlidir. Buna göre $\alpha \in K$ alalım. E'nin karakteristiği p olacağından, yukarıdaki gözlemi de kullanarak, $E[x]$ içinde $(x-\alpha)^{p^n} = x^{p^n} - \alpha^{p^n}$ elde edilir. Kabulümüzden dolayı $\alpha^{p^n} = \alpha$ olacağından, yine $E[x]$ içinde

$$\begin{aligned}x^{p^n} - x &= x^{p^n} - \alpha^{p^n} - x + \alpha \\ &= (x-\alpha)^{p^n} - (x-\alpha) \\ &= (x-\alpha)[(x-\alpha)^{p^n-1} - 1]\end{aligned}$$

bulunur. $x - \alpha \nmid (x-\alpha)^{p^n-1} - 1$ olduğundan $(x-a)^2 \nmid x^{p^n} - x$ olur. Böylece $x^{p^n} - x$ polinomunun E içindeki tüm kökleri tek katlıdır. Dolayısıyla $|K| = p^n$ olur. Şimdi de

K kümesinin E'nin bir altcismi olduğunu göstereceğiz. Öncelikle $1^{p^n} = 1$ olduğundan $1 \in K$ olur. $\alpha, \beta \in K$ olsun.Bu durumda

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} + (-\beta)^{p^n} = \alpha + (-1)^{p^n}\beta = \begin{cases} \alpha - \beta, & p > 2 \text{ ise} \\ \alpha + \beta, & p = 2 \text{ ise} \end{cases}$$

bulunur. Fakat $p = 2$ ise $+1 = -1$ olacağından, her durumda, $(\alpha - \beta)^{p^n} = \alpha - \beta$ olur. Yani $\alpha - \beta \in K$. Ayrıca $\beta \neq 0$ ise

$$(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{-1})^{p^n} = a^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}$$

olacağından $\alpha\beta^{-1} \in K$ olur. Böylece Lemma 5'den K, E'nin bir altcismi olur.

(Teklik) F, p^n elemanlı bir cisim olsun. Teorem 7'den dolayı F'nin karakteristiği p olur. Önerme 6 gereğince F'nin, $\mathbb{Z}_p$ ile eşyapılı bir altcismi olacağından, genelliği bozmadan, $\mathbb{Z}_p \subseteq F$ kabul edebiliriz. Lemma 12'den dolayı F, $x^{p^n} - x$ polinomunun bütün köklerinden ibaret olur. Buna göre F, $x^{p^n} - x$ polinomunun $\mathbb{Z}_p$ üzerinde bir parçalanış cismidir. Teorem 11'i kullanarak istenilen elde edilir. ■

BU ANDAN ITIBAREN q ELEMANLI HERHANGI BIR CISMI $\mathbb{F}_q$ ILE GOSTERECEGIZ.

Tanım *Eğer $\alpha \in \mathbb{F}_q$ için $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ yazılabiliyorsa, α elemanına $\mathbb{F}_q$ cisminin bir **ilkel elemanı** denir.*

Örnek 11 *α, $x^2 + x + 1 \in \mathbb{F}_2[x]$ polinomunun bir kökü olmak üzere, daha önce Örnek 9 (iii)'de verilen, $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ cismini düşünelim. Buna göre*

$$\alpha^2 = -(\alpha + 1) = \alpha + 1,\ \alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha + \alpha^2 = a + \alpha + 1 = 1$$

olur. Dolayısıyla $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\} = \{0, \alpha, \alpha^2, \alpha^3\}$, yani α, $\mathbb{F}_4$'ün bir ilkel elemanıdır.

Tanım *Bir $\alpha \in \mathbb{F}_q^*$ için $\alpha^k = 1$ olacak şekildeki en küçük k pozitif tamsayısına α'nın **mertebesi** denir ve $m(\alpha)$ ile gösterilir.*

Örnek 12 *$x^2 + 1$ polinomu, $\mathbb{F}_3$ üzerinde, doğrusal çarpanı olmadığından dolayı indirgenemezdir. α, $x^2 + 1$ polinomunun bir kökü olmak üzere $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ cisminin α elemanını düşünelim. $\alpha^2 = -1$, $\alpha^3 = \alpha\alpha^2 = \alpha(-1) = -\alpha = 2\alpha$ ve $\alpha^4 = (\alpha^2)^2 = 1$ olacağından $m(\alpha) = 4$ bulunur.*

Lemma 15 **(i)** *Her $\alpha \in \mathbb{F}_q^*$ için $\alpha^m = 1$ ise $m(\alpha) \mid m$. Özel olarak $m(\alpha) \mid q - 1$.*
(ii) *$\alpha, \beta \in \mathbb{F}_q^*$ için $(m(\alpha), m(\beta)) = 1$ ise $m(\alpha\beta) = m(\alpha)m(\beta)$.*

Kanıt. (i) Bir $m > 0$ tamsayısı için $\alpha^m = 1$ olsun. Uygun $a \geq 0$ ve $0 \leq b < m(\alpha)$ tamsayıları için $m = a \cdot m(\alpha) + b$ yazabiliriz. Buna göre

$$1 = \alpha^m = \alpha^{a \cdot m(\alpha) + b} = (\alpha^{m(\alpha)})^a \cdot \alpha^b = \alpha^b$$

olur. Dolayısıyla $b = 0$ elde edilir. Yani $m(\alpha) \mid m$. Şimdi, Lemma 12'den dolayı, $m = q - 1$ alarak bu kısmın kanıtını tamamlayabiliriz.

(ii) $r = m(\alpha)\cdot m(\beta)$ olsun. Bu durumda $\alpha^r = 1 = \beta^r$ olur. Böylece $(\alpha\beta)^r = \alpha^r\beta^r = 1$ ve buradan da $m(\alpha\beta) \leq r$ elde edilir. Diğer taraftan $t = m(\alpha\beta)$ denirse

$$1 = (\alpha\beta)^{t\cdot m(\alpha)} = (\alpha^{m(\alpha)})^t\beta^{t\cdot m(\alpha)} = \beta^{t\cdot m(\alpha)}$$

olacağından, lemmanın birinci kısmı kullanılarak, $m(\beta) \mid t\cdot m(\alpha)$ elde edilir. Fakat $(m(\alpha), m(\beta)) = 1$ olduğundan $m(\beta) \mid t$ dir. Benzer şekilde $m(\alpha) \mid t$ olduğunu gösterebiliriz. Dolayısıyla $r = [m(\alpha), m(\beta)] \mid t$, yani $r \leq t$ bulunur. Böylece $r = t$, yani istenilen eşitlik elde edilir. ■

Önerme 16 **(i)** *$\mathbb{F}_q$ cisminin sıfırdan farklı bir elemanının ilkel olması için gerek ve yeter koşul bu elemanın mertebesinin $q-1$ olmasıdır.*

(ii) *Her sonlu cisim en az bir ilkel eleman içerir.*

Kanıt. **(i)** Bir $\alpha \in \mathbb{F}_q^*$ için $m(\alpha) = q-1$ ancak ve ancak $\alpha, \alpha^2, \ldots, \alpha^{q-1}$ elemanları birbirinden farklıdır. Fakat bu $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ olması demektir.

(ii) $\mathbb{F}_q$ cisminin sıfırdan farklı bütün elemanlarının mertebelerinin en küçük ortak katı m olsun. Kabul edelim ki m, birbirinden farklı $r_1, \ldots, r_n$ asal sayıları için

$$m = r_1^{k_1}\ldots r_n^{k_n}$$

şeklinde asal çarpanlarına ayrılsın. m'nin seçiminden dolayı $r_1^{k_1} \mid m(\alpha)$ olacak şekilde bir $\alpha \in \mathbb{F}_q^*$ elemanı vardır. $\beta_1 = \alpha^{m(\alpha)/r_1^{k_1}}$ olsun. $(\beta_1)^{r_1^{k_1}} = \alpha^{m(\alpha)} = 1$ olduğundan $m(\beta_1) \mid r_1^{k_1}$ olur. Buna göre $m(\beta_1) = r_1^s$ olacak şeklide bir $s \leq k_1$ tamsayısı vardır. Öte yandan $\alpha^{(m(\alpha)/r_1^{k_1})r_1^s} = (\beta_1)^{r_1^s} = 1$ olacağından $m(\alpha) \mid (m(\alpha)/r_1^{k_1})r_1^s$ yazılabilir. Bu ise $r_1^s/r_1^{k_1} \in \mathbb{Z}$, yani $s = k_1$ anlamına gelir. Dolayısıyla $m(\beta_1) = r_1^{k_1}$ olur. Benzer şekilde, her $i = 1, \ldots, n$ için, $m(\beta_i) = r_i^{k_i}$ olacak şekilde $\beta_i \in \mathbb{F}_q^*$ bulunabilir. $\beta = \beta_1\ldots\beta_n$ olsun. Lemma 15 (ii)'den $m(\beta) = m$ olur. Aynı lemmanın (i) şıkkından dolayı $m \mid q-1$ olur. Ayrıca m'nin seçiminden dolayı $\mathbb{F}_q^*$'ın her elemanı $x^m - 1$ polinomunun bir köküdür. Buna göre $q-1 \leq m$ olur. Dolayısıyla $m = q-1$, yani β bir ilkel eleman olur. ■

Not **(i)** İlkel elemanlar tek olmak zorunda değildir. Mesela Örnek 11'de verilen $\mathbb{F}_4$ cisminin α ve $\alpha+1$ gibi iki tane ilkel elemanı vardır.

(ii) $\mathbb{F}_q$ üzerinde derecesi m olan bir indirgenemez polinomun α gibi bir kökü için α, $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ cisminin bir ilkel elemanı ise bu durumda

$$\mathbb{F}_{q^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} : a_i \in \mathbb{F}_q\} = \{0, \alpha, \alpha^2, \ldots, \alpha^{q^m-1}\}$$

olacağından, $\mathbb{F}_{q^m}$ cisminin bir elemanı hem α'nın bir polinomu hem de α'nın bir kuvveti olarak yazılabilir. Eğer elemanları, toplama yaparken α'nın polinomları, çarpma yaparken de α'nın kuvvetleri cinsinden yazarsak işlemleri yapmamız oldukça kolaylaşır.

Örnek 13 *α, $x^3+x+1 \in \mathbb{F}_2[x]$ polinomunun bir kökü olmak üzere $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ cismini ele alalım. Lemma 15 (i)'den dolayı $m(\alpha) \mid 8-1 = 7$ olacağından $m(\alpha) = 7$, yani α, $\mathbb{F}_8$ cisminin bir ilkel elemanı olur. Aslında $\mathbb{F}_8$'in 0 ve 1'den farklı her elemanı bir ilkel elemandır. $\mathbb{F}_8$'in elemanlarını içeren aşağıdaki gibi bir tablo yapalım:*

0	$1 = \alpha^7 = \alpha^0$	α	α^2
$\alpha+1 = \alpha^3$	$\alpha^2+\alpha = \alpha^4$	$\alpha^2+\alpha+1 = \alpha^5$	$\alpha^2+1 = \alpha^6$

Bu tabloya bakarak toplama ve çarpma işlemlerini kolaylıkla yapabiliriz. Örneğin

$$\alpha^6 + \alpha^3 = (\alpha^2 + 1) + (\alpha + 1) = \alpha^2 + \alpha = \alpha^4, \qquad \alpha^6\alpha^3 = \alpha^9 = \alpha^2$$

elde edilir.

Yukarıdaki örnekten de görülebileceği gibi, eğer bir sonlu cismin elemanlarını hem polinom hem de kuvvet şeklinde göteren bir tabloya sahip olursak, bu cismin elemanları arasında toplama ve çarpma işlemlerini oldukça kolay bir şekilde yapabiliriz. Bu tablonun işlevini "**Zech Logaritma Tablosu**" adı verilen başka bir tablo ile biraz daha basitleştirebiliriz. Zech logaritma tablosu bir $\alpha \in \mathbb{F}_q$ ilkel elemanı için $0 \leq i \leq q-2$ veya $i = \infty$ değerlerine, $\alpha^i + 1 = \alpha^{z(i)}$ ile tanımlanan $z(i)$ değerlerini karşılık getiren bir tablodur (burada $\alpha^\infty = 0$ olarak kabul edilmektedir). Buna göre tabloyu kullanarak $\mathbb{F}_q$ cisminin α^i ve α^j $(0 \leq i \leq j \leq q-2)$ gibi iki elemanı için

$$\alpha^j + \alpha^i = \alpha^i(\alpha^{j-i} + 1) = \alpha^{i+z(j-i) \pmod{q-1}}, \qquad \alpha^i\alpha^j = \alpha^{i+j \pmod{q-1}}$$

sonuçlarını elde edebiliriz.

Örnek 14 *α, $x^3+2x+1 \in \mathbb{F}_3[x]$ polinomunun bir kökü olsun. x^3+2x+1 polinomu $\mathbb{F}_3$ üzerinde bir indirgenemez polinom olduğundan, $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ olur. α elemanının mertebesi $27-1 = 26$ sayısının bir pozitif bölenidir. Yani $m(\alpha)$, 2, 13 veya 26 sayılarından biridir. $m(\alpha) = 2$ olsaydı $\alpha = 1$ veya $\alpha = -1$ olurdu ($x^2 - 1$ polinomunun en fazla iki tane kökü vardır). Fakat bunların hiçbiri $x^3 + 2x + 1$ polinomunun kökü değildir. Dolayısıyla $m(\alpha) \neq 2$. Öte yandan $\alpha^3 = \alpha + 2$ olduğundan $\alpha^9 = \alpha^3 + 2^3 = \alpha^3 + 2$ ve buradan $\alpha^{12} = \alpha^3\alpha^9 = \alpha^2 + 2$ elde edilir. Dolayısıyla $\alpha^{13} = \alpha^3 + 2\alpha = -1 \neq 1$ olacağından $m(\alpha) \neq 13$ olur. Böylece $m(\alpha) = 26$, yani α, $\mathbb{F}_{27}$'nin bir ilkel elemanıdır. $\mathbb{F}_{27}$'nin α'ya göre Zech Logaritma Tablosunu aşağıdaki gibi yapabiliriz:*

i	$z(i)$	i	$z(i)$	i	$z(i)$
∞	0	8	15	17	20
0	13	9	3	18	7
1	9	10	6	19	23
2	21	11	10	20	5
3	1	12	2	21	12
4	18	13	∞	22	14
5	17	14	16	23	24
6	11	15	25	24	19
7	4	16	22	25	8

Yukarıdaki tablodan faydalanarak $\mathbb{F}_{27}$ içinde toplama ve çarpma işlemlerini kolaylıkla yapabiliriz. Örneğin

$$\alpha^{11} + \alpha^7 = \alpha^7(\alpha^4 + 1) = \alpha^7\alpha^{18} = \alpha^{25}, \qquad \alpha^7 \cdot \alpha^{11} = \alpha^{18}.$$

3.4 Minimal Polinomlar

Lemma 17 *$d, n > 0$ iki tamsayı olsun. Buna göre $d \mid n$ ancak ve ancak $x^d - 1 \mid x^n - 1$.*

Kanıt. $(\Rightarrow)$: $n = dk$ olsun. Buna göre

$$x^n - 1 = (x^d)^k - 1 = (x^d - 1)(x^{dk-d} + x^{dk-2d} + \cdots + x^d + 1)$$

olacağından $x^d - 1 \mid x^n - 1$ elde edilir.

$(\Leftarrow)$: $x^d - 1 \mid x^n - 1$ olsun. Bölüm algoritmasından $n = dk + r$, $0 \leq r < d$ olacak şekilde $k, r \in \mathbb{Z}$ vardır.

$$x^n - 1 = (x^{dk+r} - x^r) + (x^r - 1) = x^r(x^{dk} - 1) + (x^r - 1)$$

ve $x^d - 1 \mid x^{dk} - 1$ olacağından $x^d - 1 \mid x^r - 1$ elde edilir ki bu da ancak $r = 0$ olması ile mümkündür. ■

Önerme 18 *$d, n > 0$ iki tamsayı ve p bir asal sayı olsun. $d \mid n$ ancak ve ancak $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.*

Kanıt. $(\Rightarrow)$: $d \mid n$ olsun. Yukarıdaki lemmadan $p^d - 1 \mid p^n - 1$ olur. Uygun bir t tamsayısı için $p^n - 1 = (p^d - 1)t$ yazalım. $\mathbb{F}_{p^n}$ cisminin, $x^{p^d} - x$ polinomunun bütün köklerini içerdiğini gösterirsek, Teorem 14'ün kanıtında olduğu gibi, $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ sonucunu elde edebiliriz.

$\alpha \in \mathbb{F}_{p^n}$ bir ilkel eleman olsun. $m(\alpha^t) = m$ olsun. $(\alpha^t)^{p^d-1} = \alpha^{p^n-1} = 1$ olduğundan $m \mid p^d - 1$ olur. Ayrıca $\alpha^{mt} = (\alpha^t)^m = 1$ olduğundan $p^n - 1 = m(\alpha) \mid mt$ bulunur. Uygun k ve l tamsayıları için

$$p^d - 1 = mk \qquad \text{ve} \qquad mt = (p^n - 1)l$$

yazabiliriz. Buna göre $mt = (p^n - 1)l = (p^d - 1)tl = mktl$ ve buradan da $k = l = 1$ elde edilir. Yani $m(\alpha^t) = p^d - 1$ dir. Her $1 \leq i \leq p^d - 2$ için $(\alpha^{it})^{p^d-1} = 1$ olacağından $\{0, 1, \alpha^t, \alpha^{2t}, \ldots, \alpha^{(p^d-2)t}\}$ kümesi $x^{p^d} - x$ polinomunun tüm köklerinin kümesidir.

$(\Leftarrow)$: $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ olsun. Teorem 7'nin kanıtında kullandığımız yöntemin aynısını kullanarak

$$|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^d}|^k$$

olacak şekilde bir $k \in \mathbb{Z}$ olacağını gösterebiliriz. Dolayısıyla $n = dk$ olur. ■

Yukarıdaki önermeden dolayı eğer q bir asal sayının bir kuvveti ise bu durumda her $m > 0$ tamsayısı için $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ yazabiliriz. Bu bölümde bir $\alpha \in \mathbb{F}_{q^m}$ için $f(\alpha) = 0$ olacak şekildeki en küçük dereceli $f(x) \in \mathbb{F}_q[x]$ polinomları ile ilgileneceğiz.

Tanım *$\alpha \in \mathbb{F}_{q^m}$ olsun. $P(\alpha) = 0$ olacak şekildeki en küçük dereceli bir monic $P(x) \in \mathbb{F}_q[x]$ polinomuna α elemanının $\mathbb{F}_q$ üzerinde bir **minimal polinomu** denir.*

Örnek 15 *$x^2 + x + 1 \in \mathbb{F}_2[x]$ polinomunun bir kökü α olsun. x ve $x + 1$ polinomlarının α'nın minimal polinomları olamayacağı açıktır. Dolayısıyla $x^2 + x + 1$ polinomu α'nın bir minimal polinomudur. Ayrıca $x^2 + x + 1$ polinomu $\alpha + 1 \in \mathbb{F}_4$ elemanının da bir minimal polinomudur.*

Teorem 19 **(i)** *$\alpha \in \mathbb{F}_{q^m}$ elemanının $\mathbb{F}_q$ üzerinde $P(x)$ gibi bir minimal polinomu varsa, $f(\alpha) = 0$ olacak şekildeki her $f(x) \in \mathbb{F}_q[x]$ için $P(x) \mid f(x)$ dir.*

(ii) *$\mathbb{F}_{q^m}$'in her elemanının $\mathbb{F}_q$ üzerinde bir minimal polinomu vardır ve tektir. Bu polinom ayrıca $\mathbb{F}_q$ üzerinde indirgenemezdir.*

(iii) *Eğer bir $M(x) \in \mathbb{F}_q[x]$ monik indirgenemez polinomunun bir kökü $\alpha \in \mathbb{F}_{q^m}$ ise bu durumda $M(x)$ polinomu α'nın $\mathbb{F}_q$ üzerindeki minimal polinomudur.*

Kanıt. (i) Bölüm Algoritmasını kullanarak $f(x) = P(x)Q(x) + r(x)$ ve $r(x) = 0$ veya $0 \leq \text{der}(r(x)) < \text{der}(P(x))$ olacak şekilde $Q(x)$ ve $r(x)$ polinomları bulabiliriz. Buna göre

$$0 = f(\alpha) = P(\alpha)Q(\alpha) + r(\alpha) = r(\alpha)$$

olacağından, minimal polinomun tanımı gereğince, $r(x) = 0$ elde edilir. Yani $P(x) \mid f(x)$ dir.

(ii) Lemma 12'den $\mathbb{F}_{q^m}$'in her elemanı $x^{q^m} - x \in \mathbb{F}_q[x]$ polinomunun bir köküdür. Doğal sayıların iyi sıralanma ilkesini kullanarak her eleman için bu şekilde bir en küçük dereceli polinom olacağını söyleyebiliriz.

Kabul edelim ki $P_1(x)$ ve $P_2(x)$ polinomları $\alpha \in \mathbb{F}_{q^m}$ elemanının $\mathbb{F}_q$ üzerinde birer minimal polinomu olsun. (i) şıkkından dolayı $P_1(x) \mid P_2(x)$ ve $P_2(x) \mid P_1(x)$ olur. $P_1(x)$ ve $P_2(x)$ polinomları monik olduğundan $P_1(x) = P_2(x)$ olmak zorundadır.

Şimdi $P(x)$, bir $\alpha \in \mathbb{F}_{q^m}$ elemanının $\mathbb{F}_q$ üzerindeki minimal polinomu olsun. Eğer $P(x)$ indirgenebilir ise o zaman $P(x) = f(x)g(x)$ olacak şekilde dereceleri $P(x)$'in derecesinden küçük $f(x)$ ve $g(x)$ polinomları bulunabilir. Fakat bu durumda $0 = P(\alpha) = f(\alpha)g(\alpha)$ olacağından $f(\alpha) = 0$ veya $g(\alpha) = 0$ olur. Bu durum $P(x)$'in minimal polinom olması ile çelişeceğinden $P(x)$ indirgenemezdir.

(iii) α'nın $\mathbb{F}_q$ üzerindeki minimal polinomu $P(x)$ ise (i) şıkkından dolayı $P(x)|M(x)$ olur. Fakat $M(x)$ indirgenemez ve monik olduğundan $P(x) = M(x)$ olmak zorundadır. ■

Örnek 16 *$f(x) \in \mathbb{F}_q[x]$ derecesi m olan bir monik indirgenemez polinom olsun. Eğer α, $f(x)$'in bir kökü ise $\alpha \in \mathbb{F}_{q^m}$ elemanının $\mathbb{F}_q$ üzerindeki minimal polinomu $f(x)$'in ta kendisidir.*

Bir $\alpha \in \mathbb{F}_{q^m}$ ilkel elemanının minimal polinomunu biliyorsak bu taktirde herhangi bir i için α^i elemanının da minimal polinomunu bulabiliriz. Bunu nasıl yapabileceğimizi göstermeden önce aşağıdaki tanımı verelim.

Tanım *n ile q aralarında asal olsun.*

$$C_i = \{(i \cdot q^j \pmod{n}) : j = 0, 1, \ldots\}$$

*ile tanımlanan kümeye q'nun n modülüne göre i'yi içeren **dairesel koseti (cyclotomic coset)** adı verilir. Eğer $C_{i_1}, \ldots C_{i_t}$ kümeleri birbirinden farklı ve $\bigcup_{j=1}^{t} C_{i_j} = \mathbb{Z}_n$ ise $\{i_1, \ldots, i_t\}$ kümesine q'nun n modülüne göre dairesel kosetlerinin bir **tam temsilci kümesi** denir.*

Not (i) $i_1, i_2 \in \mathbb{Z}_n$ için ya $C_{i_1} = C_{i_2}$ ya da $C_{i_1} \cap C_{i_2} = \varnothing$ olacağından, dairesel kosetleri, $\mathbb{Z}_n$ kümesinin bir parçalanmasını teşkil ederler.

(ii) Eğer bir $m \geq 1$ sayısı için $n = q^m - 1$ ise, $q^m \equiv 1 \pmod{q^m - 1}$ olduğundan, her dairesel koseti en fazla m tane eleman içerir. Eğer $(i, q^m - 1) = 1$ ise $|C_i| = m$ olur.

Örnek 17 **(i)** 2*'nin* 15 *modülüne göre dairesel kosetlerini aşağıdaki gibi elde edebiliriz:*

$C_0 = \{0\}$ $C_1 = \{1, 2, 4, 8\}$ $C_3 = \{3, 6, 9, 12\}$
$C_5 = \{5, 10\}$ $C_7 = \{7, 11, 13, 14\}$

(ii) 3*'ün* 26 *modülüne göre dairesel kosetleri aşağıdaki gibi listelenebilir:*

$C_0 = \{0\}$ $C_1 = \{1, 3, 9\}$ $C_2 = \{2, 6, 18\}$
$C_4 = \{4, 12, 10\}$ $C_5 = \{5, 15, 19\}$ $C_7 = \{7, 21, 11\}$
$C_8 = \{8, 24, 20\}$ $C_{13} = \{13\}$ $C_{14} = \{14, 16, 22\}$
$C_{17} = \{17, 25, 23\}$

Teorem 20 *$\alpha \in \mathbb{F}_{q^m}$ bir ilkel eleman ve C_i, q'nun $q^m - 1$ modülüne göre i'yi içeren dairesel koseti olsun. Buna göre α^i elemanının $\mathbb{F}_q$ üzerindeki minimal polinomu*

$$M^{(i)}(x) := \prod_{j \in C_i} (x - \alpha^j)$$

polinomudur.

Kanıt. Kanıtı üç adımda vereceğiz.

I. Adım : $i \in C_i$ olduğundan $x - \alpha^i$, $M^{(i)}(x)$'in bir çarpanıdır. Yani α^i, $M^{(i)}(x)$ polinomunun bir köküdür.

II. Adım : $|C_i| = r$ ise $\text{der}(M^{(i)}(x)) = r$ olur. $M^{(i)}(x) = a_r x^r + \cdots + a_1 x + a_0$ olsun. Buna göre

$$\begin{aligned} a_r^q x^r + \cdots + a_1^q x + a_0^q &= \prod_{j \in C_i} (x - \alpha^{qj}) = \prod_{j \in C_{qi}} (x - \alpha^j) \\ &= \prod_{j \in C_i} (x - \alpha^j) = M^{(i)}(x). \end{aligned}$$

olur. Dolayısıyla her $k = 0, 1, \ldots, r$ için $a_k^q = a_k$, yani $a_k \in \mathbb{F}_q$. Böylece $M^{(i)}(x) \in \mathbb{F}_q[x]$ elde edilir.

III. Adım : α bir ilkel eleman olduğundan her $j \neq k$ için $\alpha^j \neq \alpha^k$ olur. Dolayısıyla $M^{(i)}(x)$ polinomunun katlı kökü yoktur. Şimdi bir $f(x) \in \mathbb{F}_q[x]$ için $f(\alpha^i) = 0$ olsun. $f(x) = f_n x^n + \cdots + f_1 x + f_0$ ($f_k \in \mathbb{F}_q$) olsun. Bir $j \in C_i$ alalım. $j \equiv iq^l \pmod{q^m - 1}$ olacak şeklide bir l tamsayısı vardır. Buna göre

$$\begin{aligned} f(\alpha^j) &= f(\alpha^{iq^l}) = f_n \alpha^{niq^l} + \cdots + f_1 \alpha^{iq^l} + f_0 \\ &= f_n^{q^l} \alpha^{niq^l} + \cdots + f_1^{q^l} \alpha^{iq^l} + f_0^{q^l} \\ &= (f_n \alpha^{ni} + \cdots + f_1 \alpha^i + f_0)^{q^l} \\ &= f(\alpha^i)^{q^l} = 0 \end{aligned}$$

bulunur. Dolayısıyla $M^{(i)}(x) \mid f(x)$ olur.

Yukarıdaki üç adım sonunda $M^{(i)}(x)$ polinomunun, α'nın $\mathbb{F}_q$ üzerindeki minimal polinomu olduğu sonucuna varabiliriz. ■

Not **(i)** α^i elemanının minimal polinomunun derecesi i'yi içeren dairesel kosetinin eleman sayısına eşittir.

(ii) α^i ve α^k elemanları aynı minimal polinoma sahiptir ancak ve ancak i ve k aynı çembereşbölüm eşkümesi içindedir.

Örnek 18 *α, $x^2+x+2 \in \mathbb{F}_3[x]$ polinomunun bir kökü olsun. Buna göre α ve α^3 elemanlarının minimal polinomları x^2+x+2 polinomudur. α^2 elemanının minimal polinomu ise x^2+1 olarak bulunur. 3'ün* mod *8'e göre dairesel kosetleri $C_1=\{1,3\}=C_3$, $C_2=\{2,6\}=C_6$, $C_4=\{4\}$ ve $C_5=\{5,7\}=C_7$ olarak bulunur. Buna göre α^2 elemanının $\mathbb{F}_3$ üzerindeki minimal polinomu*

$$M^{(2)}(x)=(x-\alpha^2)(x-\alpha^6)=x^2-(\alpha^2+\alpha^6)x+1$$

olur. Burada

$$\begin{aligned}\alpha^2+\alpha^6 &= (2\alpha+1)+(2\alpha+1)^3\\ &= 2\alpha+1+2\alpha^3+1\\ &= 2\alpha+2+2\alpha(2\alpha+1)\\ &= 2\alpha+2+\alpha^2+2\alpha=\alpha^2+\alpha+2=0\end{aligned}$$

olacağından

$$M^{(2)}(x)=x^2+1$$

elde edilir.

Benzer şekilde α^5 elemanının minimal polinomunun x^2+2x+2 olduğunu görebiliriz.

Teorem 21 *$n>0$ bir tamsayı ve $(n,q)=1$ olsun. Kabul edelim ki bir $m>0$ tamsayısı için $n \mid q^m-1$ olsun. $\alpha \in \mathbb{F}_{q^m}$ bir ilkel eleman, α^j'nin $\mathbb{F}_q$ üzerindeki minimal polinomu $M^{(j)}(x)$ ve $\{s_1,\ldots,s_t\}$ q'nun n modülüne göre dairesel kosetlerinin bir tam temsilci kümesi olsun. Buna göre x^n-1 polinomu aşağıdaki gibi $\mathbb{F}_q$ üzerindeki monik indirgenemez polinomların çarpımı şeklinde yazılabilir:*

$$x^n-1=\prod_{i=1}^{t} M^{((q^m-1)s_i/n)}(x).$$

Kanıt. $r=(q^m-1)/n$ olsun. $m(\alpha^r)=n$ olacağını Önerme 16 (ii)'nin kanıtındakine benzer bir yolla gösterebiliriz. Buna göre $1,\alpha^r,\alpha^{2r},\ldots,\alpha^{(n-1)r}$ elemanları x^n-1 polinomunun $\mathbb{F}_{q^m}$ içindeki tüm kökleridir. Dolayısıyla, Teorem 19 (i) ve Teorem 20'den, her $0 \le i \le n-1$ için $M^{(ir)}(x) \mid x^n-1$ olur. Kolayca görülebilir ki

$$x^n-1=[M^{(0)}(x),M^{(r)}(x),M^{(2r)}(x),\ldots,M^{((n-1)r)}(x)].$$

Kanıtı tamamlamak için $M^{(0)}(x),M^{(r)}(x),M^{(2r)}(x),\ldots,M^{((n-1)r)}(x)$ polinomları arasından birbirinden farklı olanları belirlemek yeterlidir. Dikkat edilirse $M^{(ir)}(x)=M^{(jr)}(x)$ ancak ve ancak ir ve jr, q'nun $q^m-1=nr$ modülüne göre aynı dairesel koseti içindedir. Bu ise i ve j'nin q'nun n modülüne göre aynı dairesel koseti içinde olması ile denktir. Dolayısıyla $M^{(0)}(x),M^{(r)}(x),M^{(2r)}(x),\ldots,M^{((n-1)r)}(x)$ polinomları arasından birbirinden farklı olanlar $M^{(s_1r)}(x),M^{(s_2r)}(x),\ldots,M^{(s_tr)}(x)$ polinomlarıdır. İndirgenemez polinomların en küçük ortak katı bu polinomların çarpımı olacağından, kanıt tamamlanır. ■

Sonuç 22 *$n>0$ bir tamsayı ve $(n,q)=1$ olsun. $x^n-1 \in \mathbb{F}_q[x]$ polinomunun $\mathbb{F}_q$ üzerindeki monik indirgenemez polinomlarının sayısı q'nun n modülüne göre dairesel kosetlerinin sayısına eşittir.*

Örnek 19 **(i)** $x^{13}-1 \in \mathbb{F}_3[x]$ *polinomunu ele alalım.* $\{0,1,2,4,7\}$ *kümesinin* 3*'ün* 13 *modülüne göre dairesel kosetlerinin bir tam temsilci kümesi olduğunu görmek zor değildir.* $13 \mid 3^3-1$ *olduğundan* $\mathbb{F}_{27}$ *cismini düşüneceğiz.* α, $x^3+2x+1 \in \mathbb{F}_3[x]$ *polinomunun bir kökü olsun. Daha önce gördüğümüz gibi* α, $\mathbb{F}_{27}$ *cisminin bir ilkel elemanıdır (Örnek 14). Ayrıca Örnek 17 (ii)'den* 3*'ün* 26 *modülüne göre* 2*'nin katlarını içeren bütün dairesel kosetlerini biliyoruz. Buna göre*

$$M^{(0)}(x) = x+2$$
$$M^{(2)}(x) = (x-\alpha^2)(x-\alpha^6)(x-\alpha^{18}) = x^3+x^2+x+2$$
$$M^{(4)}(x) = (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10}) = x^3+x^2+2$$
$$M^{(8)}(x) = (x-\alpha^8)(x-\alpha^{20})(x-\alpha^{24}) = x^3+2x^2+2x+2$$
$$M^{(14)}(x) = (x-\alpha^{14})(x-\alpha^{16})(x-\alpha^{22}) = x^3+2x+2.$$

Teorem 21'den, $x^{13}-1$ *polinomunu* $\mathbb{F}_3$ *üzerindeki monik indirgenemez polinomların çarpımı şeklinde aşağıdaki gibi yazabiliriz:*

$$\begin{aligned} x^{13}-1 &= M^{(0)}(x)M^{(2)}(x)M^{(4)}(x)M^{(8)}(x)M^{(14)}(x) \\ &= (x+2)(x^3+x^2+x+2)(x^3+x^2+2)(x^3+2x^2+2x+2)(x^3+2x+2) \end{aligned}$$

(ii) $x^{21}-1 \in \mathbb{F}_2[x]$ *polinomunu düşünelim.* $\{0,1,2,4,7\}$ *kümesinin* 2*'nin* 21 *modülüne göre dairesel kosetlerinin bir tam temsilci kümesi olduğunu kolayca görebiliriz.* $21 \mid 2^6-1$ *olduğundan* $\mathbb{F}_{64}$ *cismini düşüneceğiz.* α, $x^6+x+1 \in \mathbb{F}_2[x]$ *polinomunun bir kökü olsun. Buna göre* α, $\mathbb{F}_{64}$ *cisminin bir ilkel elemanı olur.* 2*'nin* 63 *modülüne göre* 3*'ün katlarını içeren dairesel kosetlerini aşağıdaki gibi yazabiliriz:*

$$C_0 = \{0\}, \qquad C_3 = \{3,6,12,24,48,33\},$$
$$C_9 = \{9,18,36\}, \qquad C_{15} = \{15,30,60,57,51,39\},$$
$$C_{21} = \{21,42\}, \qquad C_{27} = \{27,54,45\}.$$

Dolayısıyla

$$\begin{aligned} M^{(0)}(x) &= x+1 \\ M^{(3)}(x) &= x^6+x^4+x^2+x+1 \\ M^{(9)}(x) &= x^3+x^2+1 \\ M^{(15)}(x) &= x^6+x^5+x^4+x^2+1 \\ M^{(21)}(x) &= x^2+x+1 \\ M^{(27)}(x) &= x^3+x+1 \end{aligned}$$

elde edilir. Buna göre

$$\begin{aligned} x^{21}-1 &= M^{(0)}(x)M^{(3)}(x)M^{(9)}(x)M^{(15)}(x)M^{(21)}(x)M^{(27)}(x) \\ &= (x+1)(x^6+x^4+x^2+x+1)(x^3+x^2+1)(x^6+x^5+x^4+x^2+1) \\ &\quad \times(x^2+x+1)(x^3+x+1) \end{aligned}$$

elde edilir.

4 Doğrusal Kodlar

$\mathbb{F}_q$ sonlu cismi üzerindeki n uzunluklu bir doğrusal kod $\mathbb{F}_q^n$ uzayının bir alt uzayından başka birşey değildir. Doğrusal kodlar birer vektör uzayı olduğundan, üzerlerindeki cebirsel yapı sayesinde tanımlanmaları ve kullanılmaları doğrusal olmayan kodlara nazaran daha kolay olmaktadır. Doğrusal kodlardan bahsetmeye başlamadan önce vektör uzayı kavramını biraz hatırlayalım.

4.1 Sonlu Cisimler Üzerindeki Vektör Uzayları

Bu bölümde sonlu cisimler üzerindeki vektör uzayları ile ilgili bazı temel tanım ve sonuçlara (kanıtlarını vermeksizin) değineceğiz. Bir vektör uzayı, kabaca, toplanabilir ve ölçeklenebilir bir nesneler topluluğudur. Doğrusal cebir derslerinde vektör uzaylarını, üzerinde skalerle çarpma adı verilen ve belli özellikleri sağlayan bir çarpma işlemi bulunan toplamsal Abelyan gruplar olarak tanımlarız.

Tanım *$(V,+)$ bir toplamsal Abelyan grup olsun. $\mathbb{F}_q$ cisminin elemanları ile V'nin elemanları arasında skalerle çarpma adı verilen ve aşağıdaki özellikleri sağlayan bir çarpma işlemi varsa, V'ye, $\mathbb{F}_q$ üzerinde bir* ***vektör uzayı*** *veya kısaca bir $\mathbb{F}_q$–**uzayı** denir:*

Her $u, v \in V$ ve $\lambda, \mu \in \mathbb{F}_q$ için
(i) $\lambda v \in V$
(ii) $\lambda(u+v) = \lambda u + \lambda v$ *ve* $(\lambda+\mu)v = \lambda v + \mu v$
(iii) $(\lambda\mu)v = \lambda(\mu v)$
(iv) $1_{\mathbb{F}_q} v = v$

$\mathbb{F}_q^n$ ile girişleri $\mathbb{F}_q$ cisminden olan n uzunluklu vektörlerin kümesini göstereceğiz. Yani

$$\mathbb{F}_q^n = \{(v_1, \ldots, v_n) : v_i \in \mathbb{F}_q\}.$$

$\mathbb{F}_q^n$ kümesi üzerindeki toplama işlemini bileşensel olarak ve $\mathbb{F}_q$ üzerindeki toplamadan faydalanarak tanımlayalım: $\mathbf{v} = (v_1, \ldots, v_n)$ ve $\mathbf{w} = (w_1, \ldots, w_n)$ için

$$\mathbf{v} + \mathbf{w} = (v_1 + w_1, \ldots, v_n + w_n) \in \mathbb{F}_q^n.$$

Ayrıca $\mathbb{F}_q^n$ üzerinde skalerle çarpma işlemini, yine bileşensel olarak, her $\lambda \in \mathbb{F}_q$ ve $\mathbf{v} = (v_1, \ldots, v_n)$ için

$$\lambda\mathbf{v} = (\lambda v_1, \ldots, \lambda v_n) \in \mathbb{F}_q^n$$

şeklinde tanımlarsak $\mathbb{F}_q^n$ kümesi $\mathbb{F}_q$ üzerinde bir vektör uzayı olur.

Herhangi bir vektör uzayının toplamsal birim elemanını $\mathbf{0}$ ile gösteririz. Buna göre $\mathbb{F}_q^n$ içinde $\mathbf{0} = (0, \ldots, 0) \in \mathbb{F}_q^n$ olur. Sadece $\mathbf{0}$ elemanından oluşan küme de bir vektör uzayıdır. Bu uzaya **sıfır uzayı** adı verilir.

Örnek 1 *Aşağıdaki kümeler $\mathbb{F}_q$ üzerinde birer vektör uzayıdır:*

(i) $C_1 = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_q\}$.

(ii) $C_2 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ *$(q = 2)$.*

(iii) $C_3 = \{(0,0,0), (0,1,2), (0,2,1)\}$ *$(q = 3)$.*

Not. Herhangi bir karmaşaya neden olmadığı sürece $(v_1, \ldots, v_n)$ vektörünü $v_1 \ldots v_n$ şeklinde göstermek bazı durumlarda daha kullanışlı olabilmektedir. Yerine göre bu iki gösterimi de tercih edeceğiz.

Tanım *V bir vektör uzayı ve C, V'nin boş olmayan bir altkümesi olsun. Eğer C, V üzerindeki toplama ve skalerle çarpma işlemi ile bir vektör uzayı oluyor ise C'ye V'nin bir* ***alt uzayı*** *denir.*

Örnek 2 *Bir önceki örnekte verilen gösterimleri kullanarak aşağıdakileri söyleyebiliriz:*

(i) $\mathbf{0}$ *her vektör uzayının alt uzayıdır. C_1 ise $\mathbb{F}_q^n$ 'nin bir alt uzayıdır.*

(ii) *C_2, $\mathbb{F}_2^4$ 'ün bir alt uzayıdır.*

(iii) *C_3, $\mathbb{F}_3^3$ 'ün bir alt uzayıdır.*

Önerme 1 *V bir vektör uzayı ve C, V'nin boş olmayan bir alt kümesi olsun. C, V'nin bir alt uzayıdır ancak ve ancak her $\lambda, \mu \in \mathbb{F}_q$ ve $\mathbf{x}$, $\mathbf{y} \in C$ için $\lambda\mathbf{x}+\mu\mathbf{y} \in C$ dir.*

Dikkat edilirse, yukarıdaki önermeden, $\mathbb{F}_2$ cisminin sıfırdan farklı tek elemanı 1 olduğundan, $\mathbb{F}_2$ üzerindeki bir vektör uzayının bütün alt uzayları, toplamsal kapalı alt kümelerinden ibaret olur. Yani C'nin $\mathbb{F}_2$ üzerindeki bir V vektör uzayının alt uzayı olabilmesi için gerek ve yeter koşul her $\mathbf{x}$, $\mathbf{y} \in C$ için $\mathbf{x}+\mathbf{y} \in C$ olmasıdır.

Tanım *V bir $\mathbb{F}_q$–uzayı ve $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r \in V$ olsun.*

(i) *$\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$ olmak üzere V'nin $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_r\mathbf{v}_r$ şeklindeki bir elemanına $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ elemanlarının bir* ***doğrusal kombinasyonu*** *denir.*

(ii) *Hepsi birden sıfır olmayan her $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$ için $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_r\mathbf{v}_r \neq 0$ ise $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ kümesine* ***doğrusal bağımsız*** *denir. $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ kümesi doğrusal bağımsız değilse, yani hepsi birden sıfır olmayan her $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$ için $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_r\mathbf{v}_r = 0$ ise, $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ kümesine* ***doğrusal bağımlı*** *denir.*

Yukarıdaki tanıma göre her $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$ için

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_r\mathbf{v}_r = 0 \qquad \Rightarrow \qquad \lambda_1 = \lambda_2 = \cdots = \lambda_r = 0$$

oluyorsa $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ kümesi doğrusal bağımsız olur.

Örnek 3 **(i)** $\mathbf{0}$*'ı içeren her küme doğrusal bağımlıdır.*

(ii) *Herhangi bir $\mathbb{F}_q$ için, $\{(0,0,0,1), (0,0,1,0), (0,1,0,0)\}$ kümesi doğrusal bağımsız ve $\{(0,0,0,1), (1,0,0,0), (1,0,0,1)\}$ kümesi ise doğrusal bağımlıdır.*

Önerme 2 *V bir $\mathbb{F}_q$–uzayı ve $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$, V'nin boş olmayan bir alt kümesi olsun.*

$$< S >= \{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_k\mathbf{v}_k : \lambda_i \in \mathbb{F}_q\}$$

şeklinde tanımlanan küme V'nin bir alt uzayıdır. Gerçekte $< S >$, V'nin S kümesini içeren en küçük alt uzayıdır.

Tanım **(i)** *Yukarıdaki önermede görülen $< S >$ alt uzayına V'nin S tarafından üretilen (veya gerilen) alt uzayı denir. Eğer $S = \emptyset$ ise $< S >= 0$ olarak tanımlanır.*

(ii) *V'nin bir C alt uzayı için $C =< S >$ olacak şeklide V'nin bir S alt kümesi varsa, yani C bir S kümesi tarafından üretilirse, S kümesine C'nin bir üreteç kümesi denir.*

Not. Eğer S, V'nin bir alt uzayı ise bu durumda $< S >= S$ olur.

Örnek 4 **(i)** $q = 2$ *olsun.* $S = \{0001, 0010, 0100\}$ *ise* $< S >= \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}$ *olur.*

(ii) $q = 2$ *ve* $S = \{0001, 1000, 1001\}$ *ise* $< S >= \{0000, 0001, 1000, 1001\}$ *olur.*

(iii) $q = 3$ *ve* $S = \{0001, 1000, 1001\}$ *ise* $< S >= \{0000, 0001, 0002, 1000, 2000, 1001, 1002, 2001, 2002\}$ *olur.*

Tanım V *bir* $\mathbb{F}_q$*–uzayı olsun.* $V =< B >$ *olacak şekilde* V*'nin doğrusal bağımsız bir* B *alt kümesi varsa bu* B *kümesine* V*'nin bir* ***bazı*** *denir.*

Not. **(i)** V bir vektör uzayı ve $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$, V'nin bir bazı ise V'nin her elemanı, B'nin elemanlarının bir (tek) doğrusal kombinasyonu şeklinde yazılabilir. Yani $\mathbf{v} \in V$ ise $\mathbf{v} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_k\mathbf{v}_k$ olacak şekilde (tek türlü belirli) $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_q$ elemanları bulunabilir.

(ii) Her vektör uzayının en az bir bazı vardır. Ayrıca bir vektör uzayının çok sayıda farklı bazı bulunabilir. Ancak bir vektör uzayının tüm bazları aynı sayıda eleman içerir. Bu sabit sayıya o vektör uzayının **boyutu** diyeceğiz ve k–boyutlu bir vektör uzayı için $\text{boy}_{\mathbb{F}_q}(V) = k$ şeklinde yazacağız.

Teorem 3 V *bir* $\mathbb{F}_q$*–uzayı ve* $\text{boy}_{\mathbb{F}_q}(V) = k$ *olsun. Buna göre*

(i) V, q^k *tane eleman içerir.*

(ii) V*'nin* $\dfrac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$ *tane farklı bazı vardır.*

Örnek 5 $q = 2$, $S = \{0001, 0010, 0100\}$ *ve* $V =< S >$ *olsun. Buna göre*

$$V = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}$$

olur. Dikkat edilirse S *kümesi doğrusal bağımsızdır. Buna göre* $\text{boy}(V) = 3$ *tür. Dolayısıyla* $|V| = 2^3 = 8$ *olur. Yukarıdaki teoremden,* V*'nin tüm farklı bazlarının sayısı*

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i) = \frac{1}{3!}(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 28$$

olur.

Tanım $\mathbf{v} = (v_1, \ldots, v_n)$, $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ *olsun.*

(i) $\mathbf{v}$ *ile* $\mathbf{w}$ *arasında*

$$\mathbf{v} \cdot \mathbf{w} = v_1w_1 + \cdots + v_nw_n$$

şeklinde tanımlı işleme $\mathbf{v}$ *ile* $\mathbf{w}$ *vektörlerinin* ***nokta çarpımı*** *(veya* ***Öklid iç çarpımı****) adı verilir.*

(ii) *Eğer* $\mathbf{v}\cdot\mathbf{w} = 0$ *ise* $\mathbf{v}$ *ve* $\mathbf{w}$ *vektörleri için* ***dik****tir denir.*

(iii) S, $\mathbb{F}_q^n$*'nin boş olmayan bir alt kümesi ise*

$$S^{\perp} = \{\mathbf{v} \in \mathbb{F}_q^n : her\ \mathbf{s} \in S\ için\ \mathbf{v} \cdot \mathbf{s} = 0\}$$

*şeklinde tanımlanan kümeye S kümesinin **dikgen tümleri** (orthogonal complement) denir.*

Not. (i) Kolayca görülebilir ki boş olmayan her $S \subseteq \mathbb{F}_q^n$ alt kümesi için $S^\perp$ kümesi $\mathbb{F}_q^n$'nin bir alt uzayıdır ve $< S >^\perp = S^\perp$.

(ii) Nokta çarpımı, $\mathbb{F}_q^n$ üzerinde bir iç çarpımdır. $\mathbb{F}_q^n$ üzerinde bir iç çarpım, aşağıdaki özellikleri sağlayan bir $< , >: \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ fonksiyonudur:

her $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$ için

(a) $< \mathbf{u} + \mathbf{v} , \mathbf{w} >=< \mathbf{u} , \mathbf{w} > + < \mathbf{v} , \mathbf{w} >$

(b) $< \mathbf{u} , \mathbf{v} + \mathbf{w} >=< \mathbf{u} , \mathbf{v} > + < \mathbf{u} , \mathbf{w} >$

(c) her $\mathbf{u} \in \mathbb{F}_q^n$ için $< \mathbf{u} , \mathbf{v} >= 0 \iff \mathbf{v} = 0$

(d) her $\mathbf{v} \in \mathbb{F}_q^n$ için $< \mathbf{u} , \mathbf{v} >= 0 \iff \mathbf{u} = 0$

Kodlama kuramı içinde çeşitli iç çarpımlar kullanılmaktadır. Bu ders boyunca bizim iç çarpım ile kastedeceğimiz, aksi belirtilmedikçe, yukarıda tanımlanan nokta çarpımı olacaktır.

Örnek 6 **(i)** *$q = 2$ ve $n = 4$ olsun. $\mathbf{u} = (1, 1, 1, 1)$, $\mathbf{v} = (1, 1, 1, 0)$ ve $\mathbf{w} = (1, 0, 0, 1)$ ise $\mathbf{u}\cdot\mathbf{v} = 1$, $\mathbf{u}\cdot\mathbf{w} = 0$ ve $\mathbf{v}\cdot\mathbf{w} = 1$ bulunur. Buna göre $\mathbf{u}$ ile $\mathbf{w}$ diktir.*

(ii) *$q = 2$ ve $S = \{0100, 0101\}$ olsun. Buna göre $S^\perp = \{0000, 0010, 1000, 1010\}$ olur.*

Teorem 4 *$S \subseteq \mathbb{F}_q^n$ olsun. Buna göre*

$$\text{boy}(< S >) + \text{boy}(S^\perp) = n$$

olur.

Örnek 7 *$q = 2$, $n = 4$ ve $S = \{0100, 0101\}$ olsun. Buna göre*

$$< S >= \{0000, 0100, 0001, 0101\}.$$

S doğrusal bağımsızdır. Dolayısıyla $\text{boy}(< S >) = 2$ dir. Bir önceki örnekte

$$S^\perp = \{0000, 0010, 1000, 1010\}$$

olduğunu görmüştük. $\{0010, 1000\}$ kümesi $S^\perp$ için bir baz olduğuna göre $\text{boy}(S^\perp) = 2$ olur. Dolayısıyla

$$\text{boy}(< S >) + \text{boy}(S^\perp) = 2 + 2 = 4$$

olduğunu doğrulamış oluruz.

4.2 Doğrusal Kodlar

Tanım *$\mathbb{F}_q$ üzerinde, uzunluğu n olan bir **doğrusal kod** $\mathbb{F}_q^n$'nin bir alt uzayıdır.*

Örnek 8 *Aşağıdakiler birer doğrusal koddur:*

(i) *$C = \{(\lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_q\}$. C'ye özel olarak tekrar kodu adı verilir.*

(ii) *$C = \{000, 001, 010, 011\}$ ($q = 2$).*

(iii) *$C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$ ($q = 3$).*

(iv) *$C = \{000, 001, 010, 011, 100, 101, 110, 111\}$ ($q = 2$).*

Tanım *C, $\mathbb{F}_q$ üzerinde uzunluğu n olan bir doğrusal kod olsun.*

(i) *$\mathbb{F}_q^n$'nin $C^\perp$ alt uzayına C kodunun **duali** denir.*

(ii) *C doğrusal kodunun boyutu, C'nin $\mathbb{F}_q$ üzerindeki vektör uzayı olarak boyutu, yani* $\text{boy}_{\mathbb{F}_q}(C)$ *şeklinde tanımlanır.*

Teorem 5 *C, $\mathbb{F}_q$ üzerinde uzunluğu n olan bir doğrusal kod olsun.*

(i) $|C| = q^{\text{boy}(C)}$, *yani* $\text{boy}(C) = \log_q |C|$.

(ii) $C^\perp$ *bir doğrusal koddur ve* $\text{boy}(C) + \text{boy}(C^\perp) = n$.

(iii) $(C^\perp)^\perp = C$.

Kanıt. (i) ve (ii) kısımları daha önce vektör uzayları için söylenen bazı sonuçların tekrarlanmasıdır.

(iii) : (ii) kısmındaki eşitliği hem C hem de $C^\perp$ için ayrı ayrı uygulayarak elde edeceğimiz iki eşitliği karşılaştırırsak $\text{boy}(C) = \text{boy}((C^\perp)^\perp)$ eşitliğini elde ederiz. Dolayısıyla $C \subseteq (C^\perp)^\perp$ olduğunu göstermek yeterlidir. $\mathbf{c} \in C$ olsun. $C^\perp$ kümesinin tanımından her $\mathbf{x} \in C^\perp$ için $\mathbf{c} \cdot \mathbf{x} = 0$ olduğunu söyleyebiliriz. Buna göre $\mathbf{c} \in (C^\perp)^\perp$ olur. Dolayısıyla istenilen elde edilir. ■

Örnek 9 **(i)** *$q = 2$ olsun. $C = \{0000, 1010, 0101, 1111\}$ kodunu ele alalım. Buna göre* $\text{boy}(C) = \log_2 |C| = \log_2 4 = 2$ *olur. Ayrıca $C^\perp = \{0000, 1010, 0101, 1111\} = C$ olduğunu görmek zor değildir.*

(ii) *$q = 3$ olsun. $C = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$ kodunu ele alalım. Buna göre* $\text{boy}(C) = \log_3 |C| = \log_3 9 = 2$ *olur. Ayrıca $C^\perp = \{000, 100, 200\}$ olduğu görülebilir. Dolayısıyla* $\text{boy}(C^\perp) = 1$ *dir.*

Not. $\mathbb{F}_q$ üzerinde n–uzunluklu ve boyutu k olan bir C doğrusal kodu için genellikle q–lu $[n, k]$–kodu (veya q belli ise sadece $[n, k]$–kodu) ifadesi kullanılır. Eğer, ek olarak, C'nin uzaklığı d ise C'ye kimi zaman $[n, k, d]$–doğrusal kodu denir.

Tanım *C bir doğrusal kod olsun.*

(i) *$C \subseteq C^\perp$ ise C'ye bir **kendi–dikgen** (self–orthogonal) kod,*

(ii) *$C = C^\perp$ ise C'ye bir **kendi–dual** (self–dual) kod*

denir.

Örnek 10 *Örnek 9 (i)'deki kod bir kendi–dual koddur.*

Önerme 6 *n-uzunluklu bir kendi–dikgen kodun boyutu $n/2$ sayısından küçük veya eşittir. n–uzunluklu bir kendi–dual kodun boyutu $n/2$ sayısına eşittir.*

4.3 Hamming Ağırlığı

Tanım *$\mathbf{x}$, $\mathbb{F}_q^n$ içinde bir sözcük olsun.* $\text{wt}(\mathbf{x})$ *ile gösterilen ve $\mathbf{x}$'in (**Hamming**) **ağırlığı** adı verilen sayı, $\mathbf{x}$'in sıfırdan farklı koordinatlarının sayısı olarak tanımlanır. Yani d Hamming uzaklığı olmak üzere*

$$\text{wt}(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}).$$

Bir $x \in \mathbb{F}_q$ elemanını 1–uzunluklu bir sözcük olarak görürsek, x'in ağırlığını

$$\mathrm{wt}(x) = d(x,0) = \begin{cases} 1, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

şeklinde tanımlayabiliriz. Buna göre $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ için $\mathbf{x}$'in ağırlığı aynı zamanda

$$\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(x_1) + \mathrm{wt}(x_2) + \cdots + \mathrm{wt}(x_n)$$

eşitliği ile de verilebilir.

Lemma 7 $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ *ise* $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$.

Kanıt. $x, y \in \mathbb{F}_q$ için $d(x,y) = 0 \iff x = y \iff x - y = 0 \iff \mathrm{wt}(x-y) = 0$ olacağından kanıt açıktır. ■

q çift olduğunda her $a \in \mathbb{F}_q$ için $a = -a$ olduğundan aşağıdaki sonucu verebiliriz.

Sonuç 8 *q çift olsun.* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ *ise* $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} + \mathbf{y})$.

$\mathbb{F}_q^n$ de iki $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ ve $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ elemanı için

$$\mathbf{x} \star \mathbf{y} = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

olsun.

Lemma 9 $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ *ise* $\mathrm{wt}(\mathbf{x} + \mathbf{y}) = \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) - 2\,\mathrm{wt}(\mathbf{x} \star \mathbf{y})$.

Kanıt. Kanıtı $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2$ için vermek yeterlidir. Bunun için ise aşağıdaki tabloyu verebiliriz.

$\mathbf{x}$	$\mathbf{y}$	$\mathbf{x} \star \mathbf{y}$	$\mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) - 2\,\mathrm{wt}(\mathbf{x} \star \mathbf{y})$	$\mathrm{wt}(\mathbf{x} + \mathbf{y})$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

■

Yukarıdaki lemmadan dolayı $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ için $\mathrm{wt}(\mathbf{x} + \mathbf{y}) \leq \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y})$ olduğunu söyleyebiliriz. Aslında bu eşitsizlik herhangi bir $\mathbb{F}_q$ için de doğrudur.

Lemma 10 *Herhangi bir q ve* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ *için* $\mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) \geq \mathrm{wt}(\mathbf{x} + \mathbf{y}) \geq \mathrm{wt}(\mathbf{x}) - \mathrm{wt}(\mathbf{y})$.

Kanıt. Lemma 7 ve uzaklık için daha önce verdiğimiz üçgen eşitsizliğini birlikte kullanırsak

$$\mathrm{wt}(\mathbf{x} + \mathbf{y}) = d(\mathbf{x}, -\mathbf{y}) \leq d(\mathbf{x}, \mathbf{0}) + d(\mathbf{0}, -\mathbf{y}) = \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(-\mathbf{y}) = \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y})$$

elde edilir. Ayrıca

$$\mathrm{wt}(\mathbf{x} + \mathbf{y}) + \mathrm{wt}(\mathbf{y}) = d(\mathbf{x} + \mathbf{y}, \mathbf{0}) + d(\mathbf{0}, \mathbf{y}) \geq d(\mathbf{x} + \mathbf{y}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} + \mathbf{y} - \mathbf{y}) = \mathrm{wt}(\mathbf{x})$$

elde edilir. Dolayısıyla $\mathrm{wt}(\mathbf{x} + \mathbf{y}) \geq \mathrm{wt}(\mathbf{x}) - \mathrm{wt}(\mathbf{y})$ olur. ■

Tanım *C herhangi bir kod olsun.* $\mathrm{wt}(C)$ *ile gösterilen ve C'nin* ***minimum ağırlığı*** *adı verilen sayı, C'nin sıfırdan farklı elemanlarının ağırlıklarının en küçüğü olarak tanımlanır.*

Teorem 11 *C, $\mathbb{F}_q$ üzerinde bir doğrusal kod olsun. $d(C) = \mathrm{wt}(C)$.*

Kanıt. Tanımdan dolayı $d(\mathbf{x}' , \mathbf{y}') = d(C)$ olacak şekilde $\mathbf{x}' , \mathbf{y}' \in C$ vardır. Buna göre $\mathbf{x}' - \mathbf{y}' \in C$ olacağından,

$$d(C) = d(\mathbf{x}' , \mathbf{y}') = \mathrm{wt}(\mathbf{x}' - \mathbf{y}') \geq \mathrm{wt}(C)$$

elde edilir.

Tersine, $\mathrm{wt}(C) = \mathrm{wt}(\mathbf{z})$ olacak şekilde bir $\mathbf{z} \in C - \{0\}$ vardır. Buna göre

$$\mathrm{wt}(C) = \mathrm{wt}(\mathbf{z}) = d(\mathbf{z} , \mathbf{0}) \geq d(C)$$

olur. Dolayısıyla istenen elde edilir. ■

Örnek 11 *$C = \{0000, 1000, 0100, 1100\}$ şeklinde tanımlanan ikili doğrusal kodunu ele alalım. Buna göre*

$$\begin{aligned} \mathrm{wt}(1000) &= 1, \\ \mathrm{wt}(0100) &= 1, \\ \mathrm{wt}(1100) &= 2 \end{aligned}$$

olduğunu görebiliriz. Böylece $d(C) = 1$ olur.

4.4 Doğrusal Kodların Bazları

Doğrusal kodlar vektör uzayı olduğuna göre tüm elemanları baz elemanları cinsinden yazılabilir. Bu bölümde gerek doğrusal kodların gerek se duallerinin bazlarını bulmaya yarayan bazı algoritmalar vereceğiz. Daha önce doğrusal cebirden bilinen bazı kavramları hatırlayalım.

Tanım *A, $\mathbb{F}_q$ üzerinde bir matris olsun. Aşağıda tanımlanan işlemlerden her birine birer **temel satır işlemi** denir:*

(a) *iki satırın yerini değiştirmek,*

$$\begin{bmatrix} \vdots & & \vdots \\ a_{i1} & \cdots & a_{im} \\ \vdots & & \vdots \\ a_{j1} & \cdots & a_{jm} \\ \vdots & & \vdots \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} \vdots & & \vdots \\ a_{j1} & \cdots & a_{jm} \\ \vdots & & \vdots \\ a_{i1} & \cdots & a_{im} \\ \vdots & & \vdots \end{bmatrix}$$

(b) *bir satırı sıfırdan farklı bir skaler ile çarpmak,*

$$\begin{bmatrix} \vdots & & \vdots \\ a_{i1} & \cdots & a_{im} \\ \vdots & & \vdots \end{bmatrix} \xrightarrow{R_1 \to \lambda R_1} \begin{bmatrix} \vdots & & \vdots \\ \lambda a_{i1} & \cdots & \lambda a_{im} \\ \vdots & & \vdots \end{bmatrix}$$

(c) *bir satırın yerine kendisi ile başka bir satırın skaler çarpımının toplamını yazmak.*

$$\begin{bmatrix} \vdots & & \vdots \\ a_{i1} & \cdots & a_{im} \\ \vdots & & \vdots \\ a_{j1} & \cdots & a_{jm} \\ \vdots & & \vdots \end{bmatrix} \xrightarrow{\lambda R_1 + R_2 \to R_2} \begin{bmatrix} \vdots & & \vdots \\ a_{i1} & \cdots & a_{im} \\ \vdots & & \vdots \\ \lambda a_{i1} + a_{j1} & \cdots & \lambda a_{im} + a_{jm} \\ \vdots & & \vdots \end{bmatrix}$$

Tanım *Eğer iki matristen biri, diğeri üzerine bir dizi temel satır işlemi uygulanarak elde edilebiliyor ise bu iki matrise* ***satır denk*** *matrisler denir.*

Aşağıdakiler doğrusal cebir derslerinden iyi bilinmektedir.

(i) $\mathbb{F}_q$ üzerindeki her matris satır eşelon formda veya satır indirgenmiş eşelon formda bir matris ile satır denktir.

(ii) Her matrisin satır indirgenmiş eşelon formu tektir; fakat satır eşelon formu çeşitli olabilir.

Artık algoritmalarımızı vermeye başlayabiliriz.

Algoritma 1

Bu algoritma $\mathbb{F}_q^n$ uzayının boştan farklı bir S alt kümesi verildiğinde $C =< S >$ alt uzayının bir bazını nasıl bulabileceğimizi göstermektedir. Bunun için aşağıdaki adımları izleriz:

- satırları S kümesinin elemanlarından oluşan A matrisini oluştur.
- A üzerinde temel satır işlemleri yaparak A'ya denk satır eşelon formda bir matris bul.
- Bu satır eşelon formun sıfırdan farklı satırları C'nin bir bazıdır.

Örnek 12 *$q = 3$ olsun. $S = \{12101, 20110, 01122, 11010\}$ olmak üzere $C =< S >$ alt uzayının bir bazını bulalım.*

$$A = \begin{pmatrix} 12101 \\ 20110 \\ 01122 \\ 11010 \end{pmatrix} \rightarrow \begin{pmatrix} 12101 \\ 02211 \\ 01122 \\ 02212 \end{pmatrix} \rightarrow \begin{pmatrix} 12101 \\ 01122 \\ 00001 \\ 00000 \end{pmatrix}$$

olacağından, yukarıdaki algoritmadan dolayı, $\{12101, 01122, 00001\}$ kümesi C'nin bir bazı olur.

Algoritma 2

Bu algoritma da, yukarıdaki algoritma gibi, $\mathbb{F}_q^n$ uzayının boştan farklı bir S alt kümesi verildiğinde $C =< S >$ alt uzayının bir bazını nasıl bulabileceğimizi göstermektedir. Bunun için aşağıdaki adımları izleriz:

- sütunları S kümesinin elemanlarından oluşan A matrisini oluştur.
- A üzerinde temel satır işlemleri yaparak A'ya denk, satır eşelon formda bir matris bul.
- sıfırdan farklı satırların, soldan sağa doğru sıfırdan farklı ilk elemanlarının bulunduğu sütunları (kısaca **öncü sütunları**nı) belirle.
- A matrisinin bu sütunlara karşılık gelen sütunları, C'nin bir bazını verir.

Örnek 13 *$q = 2$ olsun. $S = \{11101, 10110, 01011, 11010\}$ olmak üzere $C =< S >$ alt uzayının bir bazını bulalım.*

$$A = \begin{pmatrix} 1101 \\ 1011 \\ 1100 \\ 0111 \\ 1010 \end{pmatrix} \rightarrow \begin{pmatrix} 1101 \\ 0110 \\ 0001 \\ 0111 \\ 0111 \end{pmatrix} \rightarrow \begin{pmatrix} 1101 \\ 0110 \\ 0001 \\ 0000 \\ 0000 \end{pmatrix}$$

olacağından, yukarıdaki algoritmadan dolayı, $\{11101, 10110, 11010\}$ kümesi C'nin bir bazıdır.

Not. Dikkat edilirse ikinci algoritmada elde edilen baz, S kümesinin her zaman bir alt kümesidir. Bu durum birinci algoritma için her zaman mümkün değildir.

Algoritma 3

Bu algoritma $\mathbb{F}_q^n$ uzayının boştan farklı bir S alt kümesi verildiğinde, $C =< S >$ olmak üzere, $C^\perp$ alt uzayının bir bazını nasıl bulabileceğimizi göstermektedir. Bunun için aşağıdaki adımları izleriz:

- satırları S kümesinin elemanlarından oluşan A matrisini oluştur.
- A üzerinde temel satır işlemleri yaparak A'nın satır indirgenmiş eşelon formunu bul.
- bu eşelon formun sıfırdan farklı tüm satırlarını yeni bir G $(k \times n)$ matrisi olarak yaz.
- G'nin sütunlarının yerlerini
$$G' = (I_k|X)$$
tipindeki matrisi elde edecek şekilde değiştir. (Burada I_k, k–boyutlu birim matrisi göstermektedir.)
- $H' = (-X^T|I_{n-k})$ matrisini oluştur. (Burada X^T, X matrisinin transpozunu göstermektedir.)
- daha önce G'nin sütunlarını karıştırırken yaptığımız işlemleri geri alarak, H' matrisinin sütunlarının yerlerini değiştir ve yeni H matrisini yaz.
- H matrisinin satırları $C^\perp$ alt uzayının bir bazıdır.

Örnek 14 *$q = 3$ olsun. A matrisinin satır indirgenmiş eşelon formu*

$$G = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \end{array}$$

ise $C^{\perp}$ uzayının bir bazını bulalım. G'nin öncü sütunları $1, 4, 5, 7$ ve 9 nolu sütunlardır. G'nin sütularını yeni sırası $1, 4, 5, 7, 9, 2, 3, 6, 8, 10$ olacak şekilde taşırsak

$$G' = (I_5|X) = \begin{array}{c} \begin{array}{cccccccccc} 1 & 4 & 5 & 7 & 9 & 2 & 3 & 6 & 8 & 10 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \end{array}$$

elde ederiz. Yukarıdaki algoritmada tarif edildiği gibi H' ve H matrislerini

$$H' = \begin{array}{c} \begin{array}{cccccccccc} 1 & 4 & 5 & 7 & 9 & 2 & 3 & 6 & 8 & 10 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

$$H = \begin{array}{c} \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

şeklinde buluruz. Buna göre algoritmadan, H matrisinin satırları $C^{\perp}$ uzayının bir bazı olur.

4.5 Üreteç ve Eşlik–Denetim Matrisleri

Tanım *C bir kod olsun.*
(i) *Satırları C'nin bir bazı olan bir matrise C kodunun bir* ***üreteç matrisi*** *denir.*
(ii) *$C^{\perp}$ dual uzayının bir üreteç matrisine C kodunun bir* ***eşlik–denetim matrisi*** *denir.*

Not. (i) C bir $[n, k]$–doğrusal kodu ise C'nin her üreteç matrisi $k \times n$ boyutlu, her eşlik–denetim matrisi ise $(n - k) \times n$ boyutludur.

(ii) Bir önceki bölümde verilen (3) nolu altgoritma ile bir C doğrusal kodunun hem üreteç hem de eşlik–denetim matrisini bulabiliriz.

(iii) Bir vektör uzayının çeşitli bazları olabildiği için bir doğrusal kodun üreteç matrisleri de çok çeşitli olabilir. Hatta doğrusal kodun bazını sabit tutsak bile bir üreteç matrisinin satırlarının yerlerini değiştirerek yeni üreteç matrisleri elde etmiş oluruz.

(iv) $k \times n$ boyutlu bir G matrisinin bir C kodunun üreteç matirisi olduğunu göstermek için G'nin satırlarının C'nin kod sözcükleri olduğunu ve bu satırların doğrusal bağımsız olduğunu görmek yeterlidir. Alternatif olarak C'nin, G'nin satır uzayı içinde olduğu da gösterilebilir.

Tanım **(i)** *Bir üreteç matrisi* $(I_k|X)$ *yapısında ise bu matris için "standart yapıdadır" denir.*

(ii) *Bir eşlik–denetim matrisi* $(Y|I_{n-k})$ *yapısında ise bu matris için de "standart yapıdadır" denir.*

Lemma 12 C, $\mathbb{F}_q$ *üzerinde bir* $[n,k]$*–doğrusal kodu ve* G, C*'nin bir üreteç matrisi olsun. Buna göre* $\mathbf{v} \in \mathbb{F}_q^n$ *elemanı* $C^\perp$ *içindedir ancak ve ancak* $\mathbf{v}$ G*'nin her satırına diktir. Yani* $\mathbf{v} \in C^\perp \iff \mathbf{v}G^T = 0$*. Özel olarak,* $(n-k) \times n$ *boyutlu bir* H *matrisi verildiğinde,* H, C*'nin bir eşilik–denetim matrisidir ancak ve ancak* H*'nin satırları doğrusal bağımsız ve* $HG^T = 0$ *dır.*

Not. Yukarıdaki lemmayı ona denk olan başka bir ifadeyle aşağıdaki şeklide de vermek mümkündür:

$C, \mathbb{F}_q$ *üzerinde bir* $[n,k]$*–doğrusal kodu ve* H, C*'nin bir eşlik–denetim matrisi olsun. Buna göre* $\mathbf{v} \in \mathbb{F}_q^n$ *elemanı* C *içindedir ancak ve ancak* $\mathbf{v}$ H*'nin her satırına diktir. Yani* $\mathbf{v} \in C \iff \mathbf{v}H^T = 0$*. Özel olarak,* $k \times n$ *boyutlu bir* G *matrisi verildiğinde,* G, C*'nin bir üreteç matrisidir ancak ve ancak* G*'nin satırları doğrusal bağımsız ve* $GH^T = 0$ *dır.*

Teorem 13 C *bir doğrusal kod ve* H, C*'nin bir eşlik–denetim matrisi olsun. Buna göre*

(i) $d(C) \geq d$ *ancak ve ancak* H*'nin herhangi* $d-1$ *adet sütunu doğrusal bağımsızdır.*

(ii) $d(C) \leq d$ *ancak ve ancak* H*'nin* d *adet doğrusal bağımlı sütunu vardır.*

Sonuç 14 C *bir doğrusal kod ve* H, C*'nin bir eşlik–denetim matrisi olsun. Buna göre aşağıdakiler denktir:*

(i) $d(C) = d$

(ii) H*'nin herhangi* $d-1$ *adet sütunu doğrusal bağımsızdır ve* H*'nin* d *adet doğrusal bağımlı sütunu vardır.*

Örnek 15 C*, eşlik–denetim matrisi*

$$H = \begin{pmatrix} 10100 \\ 11010 \\ 01001 \end{pmatrix}$$

olan bir ikili doğrusal kod olsun.

Teorem 15 C *bir* $[n,k]$*–doğrusal kodu ve* $G = (I_k|X)$, C*'nin standart yapıdaki üreteç matrisi olsun. Buna göre* C*'nin eşlik–denetim matrisi* $H = (-X^T|I_{n-k})$ *olur.*

Örnek 16 $S = \{11101, 10110, 01011, 11010\}$ *olmak üzere* $C =< S >$ *ikili doğrusal kodu için bir eşlik–denetim matrisi bulunuz.*

Aşağıdaki örnekten de görülebileceği gibi her doğrusal kodun standart yapıda bir üreteç matrise sahip olma zorunluluğu yoktur.

Örnek 17 $C = \{000, 001, 100, 101\}$ *ikili doğrusal kodunu ele alalım.*

4.6 Doğrusal Kodların Denkliği

Doğrusal kodlar, standart yapıda üreteç matrisine sahip olmak zorunda değillerse de kod sözcüklerinin koordinatlarının uygun bir şeklide yerlerini değiştimek suretiyle, hatta bazı koordinatları sıfırdan farklı uygun skalerlerle çarpmak suretiyle, standart yapıda bir üreteç matrisine sahip bir doğrusal kod elde edilebilir.

Tanım *$\mathbb{F}_q$ üzerinde iki adet (n, M)–kodundan biri diğerinden aşağıdaki işlemlerin bir dizisi uygulanarak elde edilebiliyor ise bu iki kod için "denktir" denir:*

(i) *kod sözcüklerinin koordinatlarının permütasyonu;*

(ii) *sabit bir konumdaki koordinatın sıfırdan farklı bir skaler ile çarpımı.*

Örnek 18 *$\mathbb{F}_3$ üzerinde $C = \{000, 011, 001, 002, 010, 020, 012, 021, 022\}$ kodunun sözcüklerinin 3. koordinatlarını 2 ile çarpıp, koordinatları 2, 3, 1 sırasında yazarsak C'ye denk olan*

$$C' = \{000, 120, 020, 010, 100, 200, 110, 220, 210\}$$

kodunu elde ederiz.

Teorem 16 *Her doğrusal kod, standart yapıda üreteç matrisine sahip bir kod ile denktir.*

Örnek 19 *C aşağıdaki gibi bir üreteç matirisine sahip ikili kod olsun:*

$$G = \begin{pmatrix} 1100001 \\ 0010011 \\ 0001001 \end{pmatrix}.$$

G'nin sütunlarını 1, 3, 4, 2, 5, 6, 7 sırasında yazarsak stantart yapıdaki

$$G' = \left(\begin{array}{c|c} 100 & 1001 \\ 010 & 0011 \\ 001 & 0001 \end{array}\right)$$

matrisini elde ederiz. C', G' matrisi tarafından üretilen kod ise C' ile C kodları denk olur.

Örnek 20 *Örnek 17'de $C = \{000, 001, 100, 101\}$ kodunun standart yapıda bir üreteç matrisine sahip olmadığını görmüştük. Ancak ikinci ve üçüncü koordinatların yerlerini değiştirerek C'ye denk olan $C' = \{000, 010, 100, 110\}$ kodunu elde ederiz. Dikkat edilirse C' kodu standart yapıda olan*

$$\begin{pmatrix} 100 \\ 010 \end{pmatrix}$$

üreteç matrisine sahiptir.

4.7 Doğrusal Kodlar ile Kodlama

C, $\mathbb{F}_q$ üzerinde bir $[n, k, d]$–doğrusal kodu olsun. C'nin her kod sözcüğü bir bilgi parçasını temsil edebilir. Böylece C kodu sayesinde q^k adet farklı bilgi parçası temsil edilebilir. $\{\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k\}$, C'nin bir bazı ise her kod sözcüğü $\mathbf{v}$, uygun $u_1, u_2, \ldots, u_k \in \mathbb{F}_q$ için $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k$ vektörlerinin

$$\mathbf{v} = u_1\mathbf{r}_1 + \cdots + u_n\mathbf{r}_k$$

doğrusal kombinasyonu şeklinde yazılabilir. G, C'nin i–yinci satırı $\mathbf{r}_i$ olan üreteç matirisi olsun. Bir $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ verildiğinde

$$\mathbf{v} \;=\; \mathbf{u}G = u_1\mathbf{r}_1 + \cdots + u_n\mathbf{r}_k$$

C'nin bir kod sözcüğü olur. Tersine her $\mathbf{v} \in C$ için $\mathbf{v} = \mathbf{u}G$ olacak şekilde tek türlü $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ vardır. Böylece her $\mathbf{u} \in \mathbb{F}_q^k$ sözcüğü $\mathbf{v} = \mathbf{u}G$ şeklinde kodlanabilir.

$\mathbb{F}_q^k$ kümesinin $\mathbf{u}$ elemanlarının $\mathbf{v} = \mathbf{u}G$ şeklinde kod sözcükleri olarak temsil edilmesi işlemine **kodlama** denir.

Örnek 21

$$G = \begin{pmatrix} 10110 \\ 01011 \\ 00101 \end{pmatrix}$$

olmak üzere C, üreteç matrisi G olan bir ikili $[5, 3]$–doğrusal kodu olsun. Buna göre $\mathbf{u} = 101$ *mesajı*

$$\mathbf{v} \;=\; \mathbf{u}G = (101)\begin{pmatrix} 10110 \\ 01011 \\ 00101 \end{pmatrix} = 10011$$

olarak kodlanır. Dikkat edilirse C kodunun bilgi oranı $3/5$ tir. Yani 5 bitten yalnız 3'ü mesajı taşımak için kullanılır.

Not. Standart yapıda üreteç matrise sahip kodlarla çalışmak önemli kolaylıklar sağlayabilmektedir. Örneğin C standat yapıda üreteç matrisine sahip bir $[n, k, d]$–doğrusal kodu olsun. $\mathbf{v} = \mathbf{u}G$ kod sözcüğünden $\mathbf{u}$ mesajını çözmek kolaydır. Çünkü

$$\mathbf{v} \;=\; \mathbf{u}G = \mathbf{u}(I|X) = (\mathbf{u}, \mathbf{u}X),$$

yani $\mathbf{v} = \mathbf{u}G$ kod sözcüğünün ilk k basamağı $\mathbf{u}$'yu vermektedir. Bu basamaklara **mesaj basamakları**, geri kalan $n - k$ adet basamağa ise **kontrol basamakları** adı verilir. Burada kontrol basamakları mesaja, onu gürültüden korumak için eklenen fazlalığı temsil etmektedir.

4.8 Doğrusal Kodların Çözülmesi

Bir kod ancak verimli bir kod çözme düzeni uygulanabiliyorsa pratik kullanıma elverişli olur. Bu bölümde doğrusal kodlar için asgari uzaklık kod çözme kuralı ile onu biraz daha iyileştiren bir değişikliği ele alacağız.

4.8.1 Kosetler

Tanım *C, $\mathbb{F}_q$ üzerinde n–uzunluklu bir doğrusal kod ve $\mathbf{u} \in \mathbb{F}_q^n$ herhangi bir vektör olsun.*

$$\mathbf{u} + C = \{\, \mathbf{u} + \mathbf{v} \;:\; \mathbf{v} \in C\}$$

kümesine C'nin $\mathbf{u}$' yu içeren koseti denir.

Örnek 22 *$q = 2$ ve $C = \{000, 101, 010, 111\}$ olsun. Buna göre*

$$\begin{aligned} 000 + C &= \{000, 101, 010, 111\} \\ 001 + C &= \{001, 100, 011, 110\} \\ 010 + C &= \{010, 111, 000, 101\} \\ 100 + C &= \{100, 001, 110, 011\} \\ 011 + C &= \{011, 110, 001, 100\} \\ 101 + C &= \{101, 000, 111, 010\} \\ 110 + C &= \{110, 011, 100, 001\} \\ 111 + C &= \{111, 010, 101, 000\} \end{aligned}$$

olur. Dikkat edilirse aşağıdaki gibi iki adet farklı koset vardır:

$$\begin{aligned} 000 + C &= 010 + C = 101 + C = 111 + C \\ 001 + C &= 011 + C = 100 + C = 110 + C = \mathbb{F}_2^3 \backslash C. \end{aligned}$$

Teorem 17 *C, $\mathbb{F}_q$ üzerinde bir $[n, k, d]$–doğrusal kodu olsun.*

(i) *$\mathbb{F}_q^n$'deki her vektör C'nin bir koseti tarafından içerilir.*

(ii) *Her $\mathbf{u} \in \mathbb{F}_q^n$ için $|\mathbf{u} + C| = |C| = q^k$.*

(iii) *Her $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ için $\mathbf{u} \in \mathbf{v} + C \Rightarrow \mathbf{u} + C = \mathbf{v} + C$.*

(iv) *İki koset ya eşittir ya da ayrıktır.*

(v) *C'nin toplam q^{n-k} adet farklı koseti vardır.*

(vi) *Her $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ için $\mathbf{u} - \mathbf{v} \in C$ ancak ve ancak $\mathbf{u}$ ve $\mathbf{v}$ aynı koset içindedir.*

Örnek 23 *$C = \{0000, 1011, 0101, 1110\}$ ikili kodunu ele alalım. C'nin tüm kosetleri*

$$\begin{aligned} 0000 + C &= \{0000, 1011, 0101, 1110\} \\ 0001 + C &= \{0001, 1010, 0100, 1111\} \\ 0010 + C &= \{0010, 1001, 0111, 1100\} \\ 1000 + C &= \{1000, 0011, 1101, 0110\} \end{aligned}$$

olarak bulunur.

Tanım *Bir kosetteki ağırlığı en küçük olan bir elemana kosetin bir **öncüsü** denir.*

Örnek 24 *Bir önceki örnekte bulduğumuz kosetlerin ilk elemanları, bu kosetlerin öncüleridir.*

4.8.2 Doğrusal Kodlar için Asgari Uzaklık Kod Çözme Kuralı

C bir doğrusal kod olsun. Kabul edelim ki bir $\mathbf{v}$ kod sözcüğü gönderilmiş ve $\mathbf{w}$ alınmış olsun.

$$\mathbf{e} = \mathbf{w} - \mathbf{v} \in \mathbf{w} + C$$

şeklinde tanımlı $\mathbf{e}$ vektörüne **hata dizgesi** diyeceğiz. Buna göre $\mathbf{w} - \mathbf{e} = \mathbf{v} \in C$ olacağından, Teorem 17 (iv) gereğince, $\mathbf{e}$ hata dizgesi ile $\mathbf{w}$ sözcüğü aynı koset içinde olur.

Asgari uzaklık kod çözme kuralına göre alınan sözcük, kendisi ile en küçük uzaklığa sahip olan kod sözcüğü olarak çözülür. Yani $\mathbf{w}$ sözcüğü $d(\mathbf{v}, \mathbf{w})$ uzaklığını en küçük yapan $\mathbf{v}$ kod sözcüğü olarak çözülür. $d(\mathbf{v}, \mathbf{w}) = \text{wt}(\mathbf{w} - \mathbf{v}) = \text{wt}(\mathbf{e})$ olduğundan, $\mathbf{w} + C$ kosetinin, wt($\mathbf{e}$) en küçük olacak şekildeki $\mathbf{e}$ elemanını seçip $\mathbf{v} = \mathbf{e} - \mathbf{w}$ yazmak ta aynı işi görür.

Örnek 25 *$q = 2$ ve $C = \{0000, 1011, 0101, 1110\}$ olsun. Buna göre* ***(i)*** *$\mathbf{w} = 1101$ ve* ***(ii)*** *$\mathbf{w} = 1111$ sözcüklerini çözelim:*

Öncelikle Örnek 23'de olduğu gibi C'nin tüm kosetlerini yazalım:

$0000 + C$:	0000	1011	0101	1110
$0001 + C$:	0001	1010	0100	1111
$0010 + C$:	0010	1001	0111	1100
$1000 + C$:	1000	0011	1101	0110

(i) $\mathbf{w} = 1101$:
(ii) $\mathbf{w} = 1111$:

4.8.3 Sendrom ile Kod Çözme

Yukarıdaki gibi kod çözme işlemi n küçük alındığı sürece oldukça iyi çalışmaktadır. Fakat n büyük olursa, bu işlem çok zaman alabilir. Alınan sözcüğün ait olduğu koseti tanımlamada sendrom kavramından faydalanarak biraz zaman kazanabiliriz.

Tanım *C, $\mathbb{F}_q$ üzerinde bir $[n, k]$–doğrusal kodu ve H, C'nin bir eşlik–denetim matrisi olsun. $\mathbf{w} \in F_q^n$ için $S(\mathbf{w}) = \mathbf{w}H^T \in F_q^{n-k}$ sözcüğüne $\mathbf{w}$'nun* ***sendromu*** *denir. Sendrom, eşlik–denetim matrisinin seçimine bağlı olduğundan, $\mathbf{w}$'nun sendromunu $S_H(\mathbf{w})$ ile göstermek yerinde olur. Fakat bir karmaşaya neden olmadığı durumlarda, daha sade olması açısında, $S(\mathbf{w})$ gösterimini tercih edeceğiz.*

Teorem 18 *C, bir $[n, k]$–doğrusal kodu ve H, C'nin bir eşlik–denetim matrisi olsun. $\mathbf{u}$,$\mathbf{v} \in \mathbb{F}_q^n$ için*

(i) *$S(\mathbf{u} + \mathbf{v}) = S(\mathbf{u}) + S(\mathbf{v})$.*

(ii) *$S(\mathbf{u}) = 0$ ancak ve ancak $\mathbf{u} \in C$.*

(iii) *$S(\mathbf{u}) = S(\mathbf{v})$ ancak ve ancak $\mathbf{u}$ ve $\mathbf{v}$ C'nin aynı koseti içindedir.*

Not. (i) Yukarıdaki teoremin üçüncü kısmından dolayı, aynı sendroma sahip sözcüklerin bir koseti teşkil edeceğini söyleyebiliriz. Buna göre bir kosetin sendromunu onun herhangi bir elemanının sendromu olarak tanımlamak mümkündür. Başka bir deyişle, sendromlar ile kosetler arasında bir birebir eşleme vardır.

(ii) Sendromlar $\mathbb{F}_q^{n-k}$ uzayında olduğundan en fazla q^{n-k}adet sendrom vardır. Teorem 17 (v) den dolayı C'nin q^{n-k} adet koseti bulunur. Dolayısıyla bunlara karşılık q^{n-k} adet farklı sendrom bulunmaktadır. Yani $\mathbb{F}_q^{n-k}$ kümesinin her elemanı bir sendromdur.

Tanım *Koset öncüleri ile bunların sendromlarını eşleştiren br tabloya* ***sendrom tablosu*** *denir.*

Tam asgari uzaklık kod çözmeyi kullanacak olduğumuzu varsayarsak, bir sendrom tablosu yapmak için aşağıdaki adımları izleyebiliriz:

1. Koda ait bütün kosetleri listeleriz ve her kosetten $\mathbf{u}$ gibi bir öncü seçeriz.

2. Koda ait H gibi bir eşlik–denetim matrisi buluruz ve her $\mathbf{u}$ için $S(\mathsf{u}) = \mathsf{u}H^T$ sendromu hesaplanır.

Not. Eğer *tam olmayan* asgari uzaklık kod çözme kuralını kullanacak olursak, yukarıdaki birinci adımda birden fazla öncü ile karşılaşmamız halinde, bir öncü seçimi yapmadan, ilgili yere yalnızca '$*$' işareti koyacağız.

Örnek 26 *$C = \{0000, 1011, 0101, 1110\}$ ikili doğrusal kodu için,* tam *asgari uzaklık kod çözmeyi kullanacak olduğumuzu varsayarsak, bir sendrom tablosu yapalım.*

Önerme 19 *C bir doğrusal kod ve $d(C) = d$ olsun. Bir $\mathbf{e} \in \mathbb{F}_q^n$ için,*

$$\mathrm{wt}(\mathbf{e}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

ise $\mathbf{e}$, C'nin kendisini içeren kosetinin tek öncü elemanıdır.

Not. Dikkat edilirse koset öncüleri hata dizgelerine karşılık gelmektedir. C bir doğrusal kod ve $d(C) = d$ ise

$$\mathrm{wt}(\mathbf{e}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

olacak şekildeki her $\mathbf{e}$ sözcüğü, içinde bulunduğu kosetin tek öncü elemanı olacağından, hata dizgelerini bulurken önce bu özellikteki $\mathbf{e}$ sözcüklerini belirleyerek işe başlamak, sendrom tablosu hazırlamada büyük kolaylık sağlayacaktır.

Örnek 27 *C bir doğrusal kod ve*

$$H = \begin{pmatrix} 1\,0\,1\,1\,0\,0 \\ 1\,1\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1 \end{pmatrix}$$

matrisi C'nin bir eşlik–denetim matrisi olsun. Tam *asgari uzaklık kod çözmeyi kullanacak olduğumuzu varsayarsak C için bir sendrom tablosu yapacağız:*

Sendrom ile kod çözme işlemi

Adım 1. Alınan $\mathbf{w}$ sözcüğü için $S(\mathbf{w})$ sendromunu hesaplarız.

Adım 2. Sendrom tablosundan $S(\mathbf{u}) = S(\mathbf{w})$ olacak şeklideki $\mathbf{u}$ koset öncüsünü buluruz.

Adım 3. $\mathbf{w}$ sözcüğünü $\mathbf{v} = \mathbf{w} - \mathbf{u}$ olarak çözeriz.

Örnek 28 *$q = 2$ ve $C = \{0000, 1011, 0101, 1110\}$ olsun. Daha önce 25'de yaptığımız işi burada sendrom ile kod çözme tekniğini kullanarak yapalım. Buna göre alınan (i) $\mathbf{w} = 1101$ ve (ii) $\mathbf{w} = 1111$ sözcüklerini aşağıdaki gibi çözebiliriz:*

4.9 Bazı Doğrusal Kodlar : Hamming ve Golay Kodları

4.9.1 Hamming Kodları

Hamming kodları R. W. Hamming ve M. J. E. Golay tarafından keşfedilmiştir. İlginç özellikleri ile birlikte kolay kodlanmaları ve çözülmeleri nedeniyle önemli bir kod sınıfını teşkil ederler. Hamming kodları bütün sonlu cisimler üzerinde tanımlanabiliyor olmalarına rağmen biz özel olarak ikili Hamming kodları ile başlayacağız.

Tanım *$r \geq 2$ olmak üzere uzunluğu $n = 2^r - 1$ ve eşlik–denetim matrisi, sütunları $\mathbb{F}_2^r$'nin bütün sıfırdan farklı vektörlerinden oluşan bir matris olan ikili koda bir* ***ikili Hamming kodu*** *denir. Bu kodu* $\mathrm{Ham}(r, 2)$ *ile göstereceğiz.*

Dikkat edilirse yukarıdaki tanımda sözü edilen eşlik–denetim matrisinin sütunları için bir sıralama belirtilmemiştir. Dolayısıyla, bu tanım ancak kodların denkliği farkı ile iyi tanımlıdır.

Bu tanımda tarif edilen matrisin bir kod için eşlik–denetim matrisi olmaya elverişli olduğu garantidir. (Neden?)

Örnek 29 $\mathrm{Ham}(3, 2)$ *olarak uzunluğu* 7 *ve eşlik–denetim matrisi*

$$H = \begin{pmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{pmatrix}$$

olan kodu alabiliriz.

Önerme 20 *(i) Aynı uzunluğa sahip bütün ikili Hamming kodları denktir.*

(ii) $\mathrm{Ham}(r, 2)$ *kodunun boyutu $k = 2^r - 1 - r$ dir.*

(iii) $\mathrm{Ham}(r, 2)$ *kodunun uzaklığı $d = 3$ tür. Buna göre* $\mathrm{Ham}(2, r)$ *kodu tam–1–hata düzelticidir.*

Hamming Kodları ile Kod Çözme

$\mathrm{Ham}(r, 2)$ kodu için toplam $q^{n-k} = 2^{2^r-1-(2^r-1-r)} = 2^r = n + 1$ adet farklı koset vardır. $\mathrm{Ham}(r, 2)$ uzaklığı 3 olan bir kod olduğundan Önerme 19'den dolayı ağırlığı en çok 1 olan $n + 1$ adet vektör koset öncülerinin tamamını verir. j.yinci konumda 1 ve diğer konumlarda 0 bulunan vektörü e_j ile gösterirsek e_j'nin sendromu $e_j H^T$, yani H'nin j.yinci sütununun transpozudur.

Eğer H'yi j.yinci sütunu j sayısının ikilik düzendeki karşılığı olacak şekilde düzenlersek, kod çözmeyi aşağıdaki adımları takip ederek yapabiliriz:

Adım 1. Bir $\mathbf{w}$ sözcüğü alındığında $\mathbf{w}$'nun sendromunu hesaplarız.

Adım 2. $S(\mathbf{w}) = 0$ olursa $\mathbf{w}$'nun gönderilen kod sözcüğü olduğunu kabul ederiz.

Adım 3. $S(\mathbf{w}) \neq 0$ ise $S(\mathbf{w})$, uygun bir $1 \leq j \leq 2^r - 1$ için, j'nin ikilik düzendeki karşılığıdır. Böylece gönderilen sözcüğü $\mathbf{w} - \mathbf{e}_j$ olarak buluruz.

Örnek 30 *Bir önceki örnekte verilen Hamming kodunu ele alalım.* $\mathbf{w} = 1001001$ *olarak alınan sözcüğü aşağıdaki gibi çözebiliriz:*

Tanım $\mathrm{Ham}(r, 2)$ *ikili Hamming kodunun dualine ikili simpleks kod denir ve* $S(r, 2)$ *ile gösterilir.*

Tanım $\mathbb{F}_q$ *üzerindeki herhangi bir* C *kodu için*

$$\overline{C} = \left\{ \left(c_1, \ldots, c_n, -\sum_{i=1}^{n} c_i \right) : (c_1, \ldots c_n) \in C \right\}$$

şeklindeki koda C*'nin* ***genişletilmiş kodu*** *denir.* $q = 2$ *olduğunda* $-\sum_{i=1}^{n} c_i = \sum_{i=1}^{n} c_i$ *ek koordinatına* ***eşlik–denetim koordinatı*** *denir.*

Teorem 21 C, $\mathbb{F}_q$ *üzerinde bir* (n, M, d)*–kodu ise* $\overline{C}$, $\mathbb{F}_q$ *üzerinde bir* $(n+1, M, d')$*–kodudur öyle ki* $d \leq d' \leq d+1$. *Eğer* C *kodu doğrusal ise* $\overline{C}$ *kodu da doğrusaldır. Ayrıca* C *doğrusal olduğunda* H, C*'nin bir eşlik–denetim matrisi ise*

$$\left(\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right)$$

matrisi de $\overline{C}$ *kodunun bir eşlik–denetim matrisidir.*

Tanım $\mathrm{Ham}(r, 2)$ *kodundan, eşlik–denetim koordinatı ekleyerek elde edilen genişletilmiş koda,* ***genişletilmiş ikili Hamming kodu*** *denir ve* $\overline{\mathrm{Ham}(r, 2)}$ *ile gösterilir.*

Önerme 22 (i) $\overline{\mathrm{Ham}(r, 2)}$, *bir ikili* $[2^r, 2^r - 1 - r, 4]$*–doğrusal kodudur.*
(ii) H, $\mathrm{Ham}(r, 2)$ *için bir eşlik–denetim matrisi olmak üzere*

$$\left(\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right)$$

matrisi de $\overline{\mathrm{Ham}(r, 2)}$ *için bir eşlik–denetim matrisidir.*

Örnek 31 $\overline{\mathrm{Ham}(3, 2)}$ *genişletilmiş ikili Hamming kodunu ele alalım. Tam olmayan kod çözme kuralı bu kod için aşağıdaki gibi çalışır.*

Tanım $r \geq 2$ *olsun.* H *matrisi, sütunlarına* $\mathbb{F}_q^r$ *uzayının* 1*–boyutlu her alt uzayından (yalnızca) birer adet sıfırdan farklı vektör yazılması ile elde edilmiş bir matris olsun. Eşlik–denetim matrisi* H *olan bir* q*–lu doğrusal koda bir* q*–lu Hamming kodu denir ve genellikle* $\mathrm{Ham}(r, q)$ *şeklinde gösterilir.*

Yukarıdaki tanımda tarif edilen H matrisinin sütunları için bir kısıtlama verilmemiş olmasına rağmen bu kurala uygun şeklide elde edilmiş bütün matrislerin doğurduğu kodlar denk olacağından, tanımımız kodların denk olması farkı ile iyi tanımlıdır.

$q = 2$ alındığında yukarıdaki gibi tanımlanan ikili Hamminig kodu ile daha önce, konunun başında, tanımladığımız ikili Hamming kodu çakışmaktadır. (Neden?)

Not. $\mathrm{Ham}(q, r)$ için bir eşlik–denetim matrisi bulmanın bir kolay yolu, sütunları $\mathbb{F}_q^r$ 'nin (soldan sağa) sıfırdan farklı ilk girişi 1 olan bütün sıfırdan farklı vektörlerinden

ibaret olan matrisi almaktır. Örneğin Ham$(3,3)$ için bir eşlik–denetim matrisi yazmak istersek, sütunları 100, 101, 102, 110, 111, 112, 120, 121, 122, 010, 011, 012 ve 001 vektörlerinden oluşan matrisi yani

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 \end{pmatrix}$$

Önerme 23 Ham(r,q) *bir* $[(q^r-1)/(q-1),(q^r-1)/(q-1)-r,3]$*–doğrusal kodudur.*

q–lu Hamming Kodları ile Kod Çözme

Ham(r,q) bir tam–1–hata düzeltici kod olduğundan, sıfırdan farklı tüm koset öncüleri ağırlığı 1 olan vektörlerdir. (Neden?) Buna göre tipik bir koset öncüsü j–yinci konumunda bir $b \in \mathbb{F}_q \backslash \{0\}$ bulunduran ve diğer tüm konumları sıfır olan, $\mathbf{e}_{j,b}$ ile gösterdiğimiz, vektör olur. Dikkat edilirse $\mathbf{c}_j$, H'nin j–yinci sütunu olmak üzere

$$S(\mathbf{e}_{j,b}) = b\mathbf{c}_j^T$$

olur. Kod çözme işlemini aşağıdaki adımları izleyerek yapabiliriz:

Adım 1. Bir $\mathbf{w}$ sözcüğü alındığında $\mathbf{w}$'nun sendromunu hesaplarız.

Adım 2. $S(\mathbf{w}) = 0$ olursa $\mathbf{w}$'nun gönderilen kod sözcüğü olduğunu kabul ederiz.

Adım 3. $S(\mathbf{w}) \neq 0$ ise $S(\mathbf{w}) = S(\mathbf{e}_{j,b})$ olacak şekildeki tek türlü belirli $\mathbf{e}_{j,b}$ sözcüğünü buluruz. Buna göre $\mathbf{w}$ sözcüğü $\mathbf{w} - \mathbf{e}_{j,b}$ olarak çözülür.

4.9.2 Golay Kodları

Tanım *A matrisi*

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

şeklinde bir 12×12 *kare matris ve*

$$G = (I_{12}|A)$$

olmak üzere üreteç matrisi G *olan ikili doğrusal koda bir* ***genişletilmiş ikili Golay kodu*** *denir ve* G_{24} *ile gösterilir.*

Not. 1977 senesinde Jüpiter ve Satürn gezegenlerine gönderilen Voyager 1 ve 2 adlı uzay araçlarından geçilen bilimsel verilerin kodlanması ve çözülmesinde bu kod kullanılmıştır.

Önerme 24 **(i)** *G_{24} kodunun uzunluğu 24 ve boyutu ise 12 dir.*

(ii) *12×24 boyutlu $H = (A|I_{12})$ matrisi G_{24} kodu için bir eşlik–denetim matrisidir.*

(iii) *G_{24} kodu bir kendi–dual koddur, yani $G_{24} = G_{24}^{\perp}$.*

(iv) *12×24 boyutlu $H' = (I_{12}|A)$ $(= G)$ matrisi G_{24} kodu için başka bir eşlik–denetim matrisidir.*

(v) *12×24 boyutlu $G' = (A|12)$ $(= H)$ matrisi G_{24} kodu için başka bir üreteç matrisidir.*

(vi) *G_{24}'ün kod sözcüklerinin ağırlıkları 4'ün katıdır.*

(vii) *G_{24} kodunun ağırlığı 4 olan bir elemanı yoktur. Dolayısıyla G_{24}'ün uzaklığı 8 'dir.*

Tanım 25 *$\widehat{A}$ matrisi bir önceki tanımda verilen A matrisinden son sütunun çıkarılması ile elde edilen 12×11 boyutlu matris ve*

$$\widehat{G} = (I_{12}|\widehat{A})$$

*olmak üzere üreteç matrisi $\widehat{G}$ olan ikili doğrusal koda bir **ikili Golay kodu** denir ve G_{24} ile gösterilir.*

Önerme 26 *G_{23} kodunun uzunluğu 23 ve boyutu 12'dir. Bu kodun genişletilmiş kodu G_{24} kodudur ve bu kodun bir eşlik–denetim matrisi*

$$\widehat{H} = (\widehat{A}^T|I_{11})$$

şeklinde verilebilir. Ayrıca G_{23}'ün uzaklığı 7'dir.

5 Doğrusal Kodların İnşası

Teorem 1 *Kabul edelim ki $\mathbb{F}_q$ üzerinde bir $[n,k,d]$–doğrusal kodu bulunsun. Buna göre*
(i) *$r \geq 1$ olmak üzere $\mathbb{F}_q$ üzerinde bir $[n+r,k,d]$–doğrusal kodu vardır.*
(ii) *$1 \leq r \leq k-1$ olmak üzere $\mathbb{F}_q$ üzerinde bir $[n,k-r,d]$–doğrusal kodu vardır.*
(iii) *$1 \leq r \leq d-1$ olmak üzere $\mathbb{F}_q$ üzerinde bir $[n-r,k,d-r]$–doğrusal kodu vardır.*
(iv) *$1 \leq r \leq d-1$ olmak üzere $\mathbb{F}_q$ üzerinde bir $[n,k,d-r]$–doğrusal kodu vardır.*
(v) *$1 \leq r \leq k-1$ olmak üzere $\mathbb{F}_q$ üzerinde bir $[n-r,k-r,d]$–doğrusal kodu vardır.*

Not. Yukarıdaki teorem öncekine göre daha kötü parametrelere sahip yeni kodlar ürettiği için kod inşa etmek için pek elverişli değildir. Fakat bu teorem kodlar üzerinde çalışırken oldukça kullanışlıdır.

Sonuç 2 *Eğer $\mathbb{F}_q$ üzerinde bir $[n,k,d]$–doğrusal kodu varsa o zaman $r \geq 0$, $0 \leq s \leq k-1$ ve $0 \leq t \leq d-1$ olmak üzere $\mathbb{F}_q$ üzerinde bir $[n+r,k-s,d-t]$–doğrusal kodu vardır.*

Örnek 1 *7 uzunluklu bir ikili Hamming kodu bir $[7,4,3]$–doğrusal kodudur. Buna göre $n \geq 7$ için $[n,4,3]$–doğrusal kodları ve $1 \leq k \leq 4$ için $[7,k,3]$–doğrusal kodları elde edebiliriz.*

Teorem 3 *$i = 1,2$ için C_i, $\mathbb{F}_q$ üzerinde bir $[n_i,k_i,d_i]$–doğrusal kodu olsun. C_1 ve C_2 kodlarının dik toplamı olarak adlandırılan*

$$C_1 \oplus C_2 = \{(\mathbf{c}_1, \mathbf{c}_2) : \ \mathbf{c}_1 \ \in C_1, \ \mathbf{c}_2 \ \in C_2\}$$

$\mathbb{F}_q$ üzerinde bir $[n_1+n_2, k_1+k_2, \min\{d_1,d_2\}]$–doğrusal kodudur.

Not. $i = 1,2$ için G_i, C_i doğrusal kodunun bir üreteç matrisi olsun. Bu durumda

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

matrisi de $C_1 \oplus C_2$ kodunun bir üreteç matrisidir. (Burada 0 ile "sıfır matrisi" kastedilmektedir. İki sıfır matrisi farklı boyutlarda alınmış olabilir.)

Örnek 2 *Bir ikili $[3,2,2]$–doğrusal kodu olan $C_1 = \{000, 110, 101, 011\}$ ile ikili $[4,1,4]$–doğrusal kodu olan $C_2 = \{0000, 1111\}$ kodu alınırsa*

$$C_1 \oplus C_2 = \{0000000, 1100000, 1010000, 0110000, 0001111, 1101111, 1011111, 0111111\}$$

kodu bir ikili $[7,3,2]$–doğrusal kodu olur.

Teorem 4 *$i = 1,2$ için C_i, $\mathbb{F}_q$ üzerinde bir $[n,k_i,d_i]$–doğrusal kodu olsun. Buna göre*

$$C = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \ \mathbf{u} \in C_1, \ \mathbf{v} \in C_2\}$$

$\mathbb{F}_q$ üzerinde bir $[2n, k_1+k_2, \min\{2d_1,d_2\}]$–doğrusal kodudur.

Not. $i = 1, 2$ için G_i, C_i doğrusal kodunun bir üreteç matrisi ise, kolayca görülebilir ki,

$$\begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}$$

matrisi de yukarıdaki teoremdeki gibi $(\mathbf{u}, \mathbf{u}+\mathbf{v})$–inşası ile elde edilen C kodunun bir üreteç matrisidir.

Örnek 3 *$C_1 = \{000, 110, 101, 011\}$ bir ikili $[3, 2, 2]$–doğrusal kodu ve $C_2 = \{000, 111\}$ bir ikili $[3, 1, 3]$–doğrusal kodu olsun. Buna göre*

$$C = \{000000, 110110, 101101, 011011, 000111, 110001, 101010, 011100\}$$

bir ikili $[6, 3, 3]$–doğrusal kodudur.

Tüm girişleri 1 olan vektörü $\mathbf{1} = (1, \ldots, 1)$ ve tüm girişleri 0 olan vektörü ise $\mathbf{0} = (0, \ldots, 0)$ şeklinde göstereceğiz.,

Sonuç 5 *A bir ikili $[n, k, d]$–doğrusal kodu olsun. Buna göre*

$$C = \{(\mathbf{c}, \mathbf{c}) : \ \mathbf{c} \in A\} \cup \{(\mathbf{c}, \mathbf{1}+\mathbf{c}) : \ \mathbf{c} \in A\}$$

bir ikili $[2n, k+1, \min\{n, 2d\}]$–doğusal kodudur.

Örnek 4 *$A = \{00, 01, 10, 11\}$ bir ikili $[2, 2, 1]$–doğrusal kodudur.*

$$\begin{aligned} C &= \{(\mathbf{c}, \mathbf{c}) : \ \mathbf{c} \in A\} \cup \{(\mathbf{c}, \mathbf{1}+\mathbf{c}) : \ \mathbf{c} \in A\} \\ &= \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\} \end{aligned}$$

olur ve C bir ikili $[4, 3, 2]$–doğrusal kodudur.

5.1 Reed–Muller Kodları

Tanım *Her $m \geq 1$ tamsayısı için aşağıdaki gibi özyineli (recursive) olarak tanımlanan ve $\mathcal{R}(1, m)$,le gösterilen kodlara (birinci derece) Reed–Muller kodları denir:*

(i) $\mathcal{R}(1, 1) = \mathbb{F}_2^2$,

(ii) *$m \geq 1$ için*

$$R(1, m+1) = \{(\mathbf{u}, \mathbf{u}) : \ \mathbf{u} \in \ R(1, m)\} \cup \{(\mathbf{u}, \mathbf{u}+\mathbf{1}) : \ \mathbf{u} \in R(1, m)\}.$$

Örnek 5 $\mathcal{R}(1, 2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$.

Önerme 6 *$m \geq 1$ için $\mathcal{R}(1, m)$ Reed–Muller kodu bir ikili $[2^m, m+1, 2^{m-1}]$–doğrusal kodudur öyle ki $\mathbf{0}$ ve $\mathbf{1}$ haricindeki tüm kod sözcüklerinin ağırlıkları 2^{m-1}'dir.*

Önerme 7 **(i)** $\mathcal{R}(1,1)$ *kodunun bir üreteç matrisi*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

olarak alınabilir.

(ii) G_m, $\mathcal{R}(1,m)$ *kodunun bir üreteç matirisi ise* $\mathcal{R}(1,m+1)$ *kodunun bir üreteç matrisi*

$$G_{m+1} = \begin{pmatrix} G_m & G_m \\ 0\cdots 0 & 1\cdots 1 \end{pmatrix}$$

olarak alınabilir.

Örnek 6

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

üreteç matrisini kullanarak

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

elde ederiz.

Önerme 8 $\mathcal{R}(1,m)^{\perp}$ *dual kodu* $\overline{\mathrm{Ham}(m,2)}$ *genişletilmiş ikili Hamming koduna denktir.*

Tanım **(i)** 2^m *uzunluklu* $\{\mathbf{0},\mathbf{1}\}$ *koduna bir sıfırıncı mertebeden Reed–Muller kodu denir ve* $\mathcal{R}(0,m)$ *ile gösterilir.*

(ii) *Birinci mertebeden Reed–Muller kodları yukarıda verildiği gibidir.*

(iii) $r \geq 2$ *olmak üzere her* $m \geq r-1$ *için*

$$\mathcal{R}(r,m+1) = \begin{cases} F_2^{2^r}, & m = r-1 \\ \{(\mathbf{u},\mathbf{u}+\mathbf{v}) :\ \mathbf{u} \in \mathcal{R}(r,m),\ \mathbf{v} \in \mathcal{R}(r-1,m)\}, & m > r-1 \end{cases}$$

kuralıyla özyineli olarak tanımlanan koda r*–yinci mertebeden bir Reed–Muller kodu denir ve* $\mathcal{R}(r,m)$ *ile gösterilir.*

6 Devirli Kodlar

6.1 Temel Tanımlar

Tanım *$S \subseteq \mathbb{F}_q^n$ için eğer $(a_0, a_1, \ldots, a_{n-1}) \in S$ iken $(a_{n-1}, a_1, \ldots, a_{n-2}) \in S$ oluyorsa S kümesine **devirli** denir. Eğer bir C doğrusal kodu devirli ise bu koda bir **devirli kod** adı verilir.*

Soru. C bir devirli kod ise $C^\perp$ dual kodunun da devirli olacağını gösteriniz.

Örnek 1 *$\{(0,1,1,2),(2,0,1,1),(1,2,0,1),(1,1,2,0)\} \subset \mathbb{F}_3^4$ ve $\{11111\} \subset \mathbb{F}_2^5$ kümeleri birer devirli kümelerdir. Fakat bu kümeler vektör uzayı olmadıkları için birer devirli kod değildir.*

Örnek 2 *Aşağıdaki kodlar birer devirli koddur:*

(i) *$\{\mathbf{0}\}$, $\{\lambda \cdot \mathbf{1} \ : \lambda \in \mathbb{F}_q\}$ ve $\mathbb{F}_q^n$,*

(ii) *$\{000, 110, 101, 011\}$ ikili $[3,2,2]$–doğrusal kodu,*

(iii) *$S(3,2) = \{0000000, 1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101\}$ ikili simpleks kodu.*

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n-1), (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \qquad (*)$$

ile tanımlı dönüşüm $\mathbb{F}_q$ üzerindeki vektör uzaylarının bir izomorfizmasıdır. Buna göre gerektiğinde $\mathbb{F}_q^n$ uzayını $\mathbb{F}_q[x]/(x^n-1)$ ile, $(a_0, a_1, \ldots, a_{n-1})$ elemanını ise $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ ile tanımlayabiliriz. $\mathbb{F}_q[x]/(x^n-1)$'in bir halka olacağını daha önce söylemiştik. Dikkat edilirse $n \neq 1$ ise bu halka bir cisim olamaz.

Örnek 3 *$C = \{000, 110, 101, 011\}$ devirli kodunu ele alalım. Buna göre $\pi(C) = \{0, 1+x, 1+x^2, x+x^2\} \subset \mathbb{F}_2[x]/(x^3-1)$ olur.*

Tanım *R bir halka ve I, R'nin boştan farklı bir alt kümesi olsun. Eğer her $a, b \in I$ ve $r \in R$ için*

(i) $a - b \in I$ ve

(ii) $ra \in I$

*ise I kümesine R'nin bir **ideali** denir.*

Örnek 4 *$I := \pi(C) = \{0, 1+x, 1+x^2, x+x^2\}$ kümesi $\mathbb{F}_2[x]/(x^3-1)$ halkasının bir idealidir.*

Örnek 5 **(i)** *Tüm çift tamsayıların kümesi $\mathbb{Z}$ tamsayılar halkasının bir idealidir.*

(ii) *Daha genel olarak, bir m tamsayısı için, m tarafından bölünebilen tüm tamsayıların kümesi $\mathbb{Z}$ halkasının bir idealidir.*

(iii) *Bir $f(x) \in \mathbb{F}_q[x]$ için $\mathbb{F}_q[x]$ polinom halkasının $f(x)$ tarafından bölünebilen tüm elemanlarının kümesi $\mathbb{F}_q[x]$ halkasının bir ideali olur.*

(iv) *$g(x)$, x^n-1 polinomunun bir böleni olmak üzere, $F_q[x]/(x^n-1)$in $g(x)$ tarafından bölünebilen tüm polinomlarının kümesi $F_q[x]/(x^n-1)$ halkasının bir idealidir.*

Tanım *R bir halka ve I, R'nin bir ideali olmak üzere, eğer*

$$I =< g >= \{gr : r \in R\}$$

olacak şekilde bir $g \in I$ varsa I idealine bir ***temel ideal*** *denir. Buradaki g elemanına I idealinin bir üreteci denir. (Bu durumda "I ideali g elemanı tarafından üretilir" diyeceğiz.)*

R halkasının tüm idealleri temel ideal ise R'ye bir ***temel ideal halkası*** *adı verilir.*

Örnek 6 *Örnek 4'deki I ideali bir temel idealdir. Çünkü $I =< 1 + x >$ yazılabilir.*

$$\begin{aligned} 0 \cdot (1+x) &= 0 = (1 + x + x^2)(1 + x), \\ 1 \cdot (1+x) &= 1 + x = (x + x^2)(1 + x), \\ x \cdot (1+x) &= x + x^2 = (1 + x^2)(1 + x), \\ x^2 \cdot (1+x) &= 1 + x^2 = (1 + x)(1 + x). \end{aligned}$$

Teorem 1 *$\mathbb{Z}$, $F_q[x]$ ve $F_q[x]/(x^n - 1)$ halkaları birer temel ideal bölgeleridir.*

6.2 Üreteç Polinomları

Teorem 2 *π, $(*)$ olarak tanımlanan dönüşüm ve C, $\mathbb{F}_q^n$'nin bir alt kümesi olsun. Buna göre C bir devirli koddur ancak ve ancak $\pi(C)$, $F_q[x]/(x^n - 1)$ halkasının bir idealidir.*

Örnek 7 **(i)** *$C = \{000, 111, 222\}$ bir üçlü devirli koddur. Buna karşılık gelen ideal ise $\pi(C) = \{0, 1 + x + x^2, 2 + 2x + 2x^2\}$ olur.*

(ii) *$I = \{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\}$, $F_2[x]/(x^4 - 1)$ halkasının bir idealidir. Buna karşılık gelen devirli kod ise $\pi^{-1}(I) = \{0000, 1010, 0101, 1111\}$ olur.*

(iii) *$\{\mathbf{0}\}$ ve $\mathbb{F}_q^n$ aşikar kodlarına karşılık gelen idealler $\{0\}$ ve $F_q[x]/(x^n - 1)$ aşikar idealleridir.*

Teorem 3 *I, $\mathbb{F}_q[x]/(x^n-1)$'in bir ideali ve $g(x)$, I'nın sıfırdan farklı monik elemanları arasında derecesi en küçük olanlardan biri olsun. (Daha sonra göreceğiz ki bu eleman aslında tektir). Buna göre $g(x)$, I idealinin bir üretecidir ve $x^n - 1$ polinomunu böler.*

Örnek 8 *Bir önceki örneğin (i) kısmında $1+x+x^2$ polinomu en küçük dereceye sahiptir ve x^3-1 polinomunu böler. Aynı örneğin (ii) kısmında $1+x^2$ polinomu en küçük dereceli olan polinomdur ve bu polinom da $x^4 - 1$ polinomunu böler.*

$\mathbb{F}_q^n$ kodu için en küçük dereceli monik polinom 1 dir.

$\mathbb{F}_q[x]/(x^n - 1)$ halkasının her idealinin bir temel ideal olduğunu biliyoruz. Buna göre bir C devirli kodu $\pi(C)$ idealinin herhangi bir üreteci ile belirlenebilir. Genellikle $\mathbb{F}_q[x]/(x^n - 1)$'in bir ideali için birden çok üreteç bulunabilir. Aşağıdaki teoreme göre bazı ek özelliklerle tek türlü üreteç bulmak mümkündür.

Teorem 4 *I, $\mathbb{F}_q[x]/(x^n - 1)$'in bir ideali olsun. I'nın sıfırdan farklı monik elemanları arasında derecesi en küçük olan yalnız bir tek polinom vardır. Teorem 3'e göre bu eleman I'nın bir üretecidir.*

Tanım 5 *I, $\mathbb{F}_q[x]/(x^n-1)$'in bir ideali olsun. I'nın sıfırdan farklı monik elemanları arasında derecesi en küçük olan polinoma I'nın* ***üreteç polinomu*** *adı verilir. Bir C devirli kodu için $\pi(C)$ idealinin üreteç polinomuna C kodunun üreteç polinomu denir.*

Örnek 9 **(i)** *$\{000, 110, 011, 101\}$ devirli kodunun üreteç polinomu $1+x$ olur.*

(ii) *Örnek 2 (iii)'de verilen $S(3,2)$ simpleks kodunun üreteç polinomu $1+x^2+x^3+x^4$ olur.*

Teorem 6 *x^n-1 polinomunun her monik böleni F_q^n'deki bir devirli kodun üreteç polinomudur.*

Sonuç 7 *$\mathbb{F}_q^n$ içindeki devirli kodlar ile $x^n-1 \in F_q[x]$ polinomunun monik bölenleri arasında bir birebir eşleme vardır.*

Örnek 10 *6–uzunluklu bütün ikili devirli kodları bulmak için $x^6-1 \in F_2[x]$ polinomunu çarpanlarına ayırırız:*

$$x^6-1 = (1+x)^2(1+x+x^2)^2.$$

x^6-1 polinomunun bütün monik bölenleri

$$\begin{array}{ccc} 1, & 1+x, & 1+x+x^2, \\ (1+x)^2, & (1+x)(1+x+x^2), & (1+x)^2(1+x+x^2), \\ (1+x+x^2)^2, & (1+x)(1+x+x^2)^2 & 1+x^6 \end{array}$$

şeklinde listelenebilir. Buna göre 6–uzunluklu dokuz adet ikili devirli kod bulunmaktadır. π dönüşümünü baz alarak bu dokuz kodu da yazabiliriz. Örneğin $(1+x+x^2)^2$ polinomuna karşılık gelen devirli kod

$$\{000000, 101010, 010101, 111111\}$$

olur.

Yukarıdaki örnekte de görüldüğü gibi x^n-1 polinomunun monik bölenlerinin sayısını biliyorsak n–uzunluklu devirli kodların sayısını bulabiliriz. Buna göre aşağıdaki sonucu verebiliriz.

Teorem 8 *$p_1(x), \ldots, p_r(x) \in \mathbb{F}_q[x]$ birbirinden farklı indirgenemez polinomlar ve her $i = 1, \ldots, r$ için $e_i \geq 1$ olmak üzere*

$$x^n - 1 = \prod_{i=1}^{r} p_i^{e_i}(x)$$

olsun. Buna göre $\mathbb{F}_q$ üzerinde n–uzunluklu $\prod_{i=1}^{r}(e_i+1)$ adet devirli kod vardır.

Örnek 11 *Aşağıdaki tablolar $q = 2, 3$ ve $1 \leq n \leq 10$ için x^n-1 polinomunun çarpanlarına nasıl ayrıldığını ve q–lu n–uzunluklu devirli kodların sayısı göstermektedir:*

n	$x^n-1 \in \mathbb{F}_2[x]$	*#ikili devirli kodlar*
1	$1+x$	2
2	$(1+x)^2$	3
3	$(1+x)(1+x+x^2)$	4
4	$(1+x)^4$	5
5	$(1+x)(1+x+x^2+x^3+x^4)$	4
6	$(1+x)^2(1+x+x^2)^2$	9
7	$(1+x)(1+x^2+x^3)(1+x+x^3)$	8
8	$(1+x)^8$	9
9	$(1+x)(1+x+x^2)(1+x^3+x^6)$	8
10	$(1+x)^2(1+x+x^2+x^3+x^4)^2$	9

n	$x^n-1 \in \mathbb{F}_3[x]$	*#üçlü devirli kodlar*
1	$2+x$	2
2	$(2+x)(1+x)$	4
3	$(2+x)^3$	4
4	$(2+x)(1+x)(1+x^2)$	8
5	$(2+x)(1+x+x^2+x^3+x^4)$	4
6	$(2+x)^3(1+x)^3$	16
7	$(2+x)(1+x^2+x^3+x^4+x^5+x^6)$	4
8	$(2+x)(1+x)(1+x^2)(2+x+x^2)$ $(2+2x+x^2)$	32
9	$(2+x)^9$	10
10	$(2+x)(1+x)(1+x+x^2+x^3+x^4)$ $(1+2x+x^2+2x^3+x^4)$	16

Devirli kodlar üreteç polinomları ile tam olarak belirli olduklarına göre parametleri de üreteç polinomları ile elde edilebilir. Aşağıdaki teorem bir devirli kodun boyutunu üreteç polinomundan nasıl bulabileceğimizi söylemektedir.

Teorem 9 *$g(x)$, $F_q[x]/(x^n-1)$'in bir idealinin üreteç polinomu olsun. Eğer $g(x)$'in derecesi $n-k$ ise bu ideale karşılık gelen devirli kodun boyutu k olur.*

Örnek 12 **(i)** $x^7-1=(1+x)(1+x^2+x^3)(1+x+x^3) \in F_2[x]$ *olduğundan sadece iki adet ikili $[7,3]$–devirli kodu mevcuttur. Bunlar*

$$< \ (1+x)(1+x^2+x^3) >= \{0000000, 1110100, 0111010, 0011101, 1001110, 0100111, 1010011, 1101001\}$$

ve

$$< \ (1+x)(1+x+x^2) >= \{0000000, 1011100, 0101110, 0010111, 1001011, 1100101, 1110010, 0111001\}$$

şeklinde yazılır.

(ii) $x^7-1=(2+x)(1+x^2+x^3+x^4+x^5+x^6) \in \mathbb{F}_3[x]$ *olduğundan hiç üçlü $[7,2]$–devirli kodu olmadığını söyleyebiliriz.*

6.3 Üreteç ve Eşlik–Denetim Matrisleri

Teorem 10 *$g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$ $(g_{n-k} \neq 0)$, $\mathbb{F}_q^n$ içindeki bir C devirli kodunun üreteç polinomu olsun. Buna göre*

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \cdot \\ \cdot \\ \cdot \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & \cdot & \cdot & & g_{n-k} & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & g_0 & g_1 & \cdot & \cdot & \cdot & \cdot & g_{n-k} \end{pmatrix}$$

matrisi C'nin bir üreteç matrisidir. (Bir vektörü aynı zamanda polinom olarak ta ifade ettiğimize dikkat ediniz).

Örnek 13 *Üreteç polinomu* $g(x) = 1+x^2+x^3$ *olan ikili* $[7, 4]$*–devirli kodunu ele alalım.*

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ x^3g(x) \end{pmatrix} = \begin{pmatrix} 1\,0\,1\,1\,0\,0\,0 \\ 0\,1\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{pmatrix}$$

matrisi bu kodun bir üreteç matrisidir. Bu matris standart yapıda değildir. Ancak G *matrisine uygun satır işlemleri uygulayarak standart yapıdaki*

$$G' = \begin{pmatrix} 1\,0\,0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{pmatrix}$$

matrisine ulaşabiliriz. Bundan sonra eşlik–denetim matrisini bulmak kolaydır.

Yukarıdaki örnekten de görüldüğü gibi bir devirli kodun bir üreteç matrisi bulunduktan sonra eşlik–denetim matrisi de elde edilebilir. Ancak bir devirli kodun dual kodu da devirli olduğuna göre, dual kodun üreteç matirisi onun üreteç polinomundan bulunabilir. Buna göre soru, bir devirli kodun dualinin üreteç polinomunun bulunmasıdır.

Tanım $h(x) = \sum_{i=0}^{k} a_i x^i$, $\mathbb{F}_q$ *üzerinde derecesi* k *olan bir polinom olsun.* $h(x)$ *polinomunun* ***karşıtı*** *adı verilen polinom*

$$h_K(x) = x^k h(1/x) = \sum_{i=0}^{k} a_{k-i} x^i$$

şeklinde tanımlanır.

Not. $h(x) \mid x^n - 1$ ise $h_K(x) \mid x^n - 1$ olacağına dikkat ediniz.

Örnek 14 **(i)** $h(x) = 1 + 2x + 3x^5 + x^7 \in \mathbb{F}_5[x]$ *polinomu için* $h(x)$*'in karşıtı*

$$\begin{aligned} h_K(x) &= x^7 h(1/x) \\ &= x^7(1 + 2(1/x) + 3(1/x)^5 + (1/x)^7) \\ &= 1 + 3x^2 + 2x^6 + x^7 \end{aligned}$$

polinomudur.

(ii) $x^7 - 1$ *polinomunun* $h(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$ *bölenini ele alalım. Buna göre* $h_K(x) = 1 + x^2 + x^3$ *polinomu da* $x^7 - 1$ *polinomunun bir bölenidir.*

Teorem 11 $g(x)$*, bir* C q*–lu* $[n, k]$*–devirli kodunun üreteç polinomu olsun.* $h(x) = (x^n - 1)/g(x)$ *ve* h_0*,* $h(x)$*'in sabit terimi ise* $h_0^{-1}h_K(x)$ *polinomu* $C^\perp$ *kodunun üreteç polinomudur.*

Tanım C *bir* n*–uzunluklu bir* q*–lu devirli kod olsun.* $h(x) = (x^n-1)/g(x)$ *ve* h_0*,* $h(x)$*'in sabit terimi olmak üzere* $h_0^{-1}h_K(x)$ *polinomuna* C *kodunun* ***eşlik–denetim polinomu*** *denir.*

Sonuç 12 *C üreteç polinomu $g(x)$ olan bir q–lu $[n,k]$–devirli kodu olsun. $h(x) = (x^n-1)/g(x)$ olsun. $h(x) = h_0 + h_1x + \cdots + h_kx^k$ ise*

$$H = \begin{pmatrix} h_K(x) \\ xh_K(x) \\ \cdot \\ \cdot \\ \cdot \\ x^{k-1}h_K(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdot & \cdot & \cdot & h_0 & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & h_k & h_{k-1} & \cdot & \cdot & & h_0 & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & h_k & h_{k-1} & \cdot & \cdot & \cdot & \cdot & h_0 \end{pmatrix}$$

matrisi C'nin bir eşlik–denetim matrisidir.

Örnek 15 *Örnek 13'de ele aldığımız kodun bir eşlik–denetim matrisini bulalım:*

Devirli Kodlar ile Kod Çözme

Devirli kodlar ile kod çözme tüm doğrusal kodlarda olduğu gibi üç adımdan oluşur: sendromun hesaplanması, sendroma karşılık gelen hata dizgesinin bulunması ve hatanın düzeltilmesi... Devirli kodların cebirsel ve geometrik özelliklerinden dolayı bu adımlar genelde kolaydır. Göreceğiz ki bu özellikler düzgün bir şekilde kullanıldığı taktirde bu kolaylıklardan faydalanılabilir.

Sonuç 12'den kolayca görülebilir ki bir devirli kodun eşlik–denetim matrisi uygun satır işlemleri ile

$$H = (I_{n-k} \mid A)$$

şekline dönüştürülebilir. Dikkat edilirse bu yapıdaki bir eşlik–denetim matrisi tek türlü belirlidir.

Teorem 13 *C bir q–lu devirli kod ve $H = (I_{n-k} \mid A)$, C'nin bir eşlik–denetim matrisi olsun. Kabul edelim ki $g(x)$, C'nin üreteç polinomu olsun. Buna göre bir $\mathbf{w} \in \mathbb{F}_q^n$ sözcüğünün (H'ye göre) sendromu $(w(x) \pmod{g(x)})$ olur. (Burada $w(x)$, $\mathbf{w}$ sözcüğüne π dönüşümü ile karşılık gelen polinomdur ve vektörler aynı zamanda polinom karşılıkları ile de ifade edilmektedir).*

Örnek 16 *Üreteç polinomu $g(x) = 1 + x^2 + x^3$ olan ikili $[7,4,3]$–Hamming kodunu ele alalım (bkz. Örnek 15). Kabul edelim ki $\mathbf{w} = 0110110$ alınsın.*

Yukarıdaki teoreme göre alınan bir $w(x)$ sözcüğünün sendromu

$$s(x) = (w(x) \pmod{g(x)})$$

olarak bulunduğundan dolayı $w(x) - s(x)$ bir kod sözcüğü olur.

Sonuç 14 *$g(x)$ bir C devirli kodunun üreteç polinomu olsun. Alınan bir $w(x)$ sözcüğü için, $w(x)$ polinomunun $g(x)$ ile bölümünden kalan $s(x)$ ve $\mathrm{wt}(s(x)) \leq \lfloor (d(C)-1)/2 \rfloor$ ise bu durumda $s(x)$, $w(x)$ için hata dizgesidir, yani $w(x)$, asgari uzaklık kod çözme kuralı ile, $w(x) - s(x)$ olarak çözülür.*

Örnek 17 *Bir önceki örnekte olduğu gibi $w(x) = x + x^2 + x^4 + x^5$ polinomunun $g(x) = 1+x^2+x^3$ ile bölümünden kalan x dir. Buna göre $w(x)$ sözcüğü $w(x)-x = x^2+x^4+x^5 = 0010110$ olarak çözülür. Eğer $w_1(x) = 1 + x^2 + x^3 + x^4$ alınırsa $(w_1(x) \pmod{g(x)}) = 1 + x + x^2$ olur. Bu durumda ise 111 sendromuna (bir önceki örnekteki $(I_{n-k} \mid A)$ yapısındaki eşlik–denetim matrisine göre) 0000100 koset öncüsü karşılık geldiğine göre sendrom ile kod çözmeyi kullanarak $w_1(x)$ sözcüğünü $w_1(x)-x^4 = 1+x^2+x^3 = 1011000$ olarak çözülür.*

Yukarıdaki örnekten de görülebileceği gibi bazı alınan sözcükler için "kalan"ı sözcükten atarak hemen sözcüğü çözebiliriz. Ancak bazı alınan sözcükler için sendrom ile kod çözmeyi kullanmak zorunda kalıyoruz. Devirli kodların özelliklerinden dolayı sendrom ile kod çözmeyi bazı alınan sözcükler için kolaylaştırmak mümkündür.

Lemma 15 *C üreteç polinomu $g(x)$ olan bir q–lu $[n,k]$–devirli kodu olsun. $s(x) = \sum_{i=0}^{n-k-1} s_i x^i$ polinomu $w(x)$'in sendromu olsun. Buna göre $w(x)$'in $xw(x)$ devirli kaydırmasının sendromu $xs(x) - s_{n-k-1}g(x)$ olur.*

Örnek 18 *Örnek 16'de olduğu gibi $w(x) = x+x^2+x^4+x^5$ sözcüğünün sendromu x'tir. Böylece $xw(x)$ ve $x^2w(x)$ sözcüklerinin sendromları sırasıyla $x \cdot x = x^2$ ve $x \cdot x^2 - g(x) = 1 + x^2$ olur.*

Tanım *n–uzunluklu bir vektörde **sıfırın l–uzunluklu bir devirli dizisi**, l adet sıfırın dairesel olarak yanyana bir dizilimidir.*

Örnek 19 **e** $= (1,3,0,0,0,0,0,1,0)$ *vektörü sıfırın 5–uzunluklu bir devirli dizisini içerir. Başka bir $(0,0,1,2,0,0,0,1,0,0)$ vektörü ise sıfırın 4–uzunluklu bir devirli dizisini içerir.*

Devirli Kodlar için Kod Çözme Algoritması

C üreteç polinomu $g(x)$ olan bir q–lu $[n,k,d]$–devirli kodu olsun.Hata dizgesi $e(x)$ olan bir $w(x)$ sözcüğü alınmış olsun. Kabul edelim ki $\mathrm{wt}(e(x)) \leq \lfloor (d-1)/2 \rfloor$ ve $e(x)$ sıfırın en az k–uzunluklu bir devirli dizisini içersin. Aşağıdaki algoritma $e(x)$ hata dizgesini bulmak içindir:

Adım 1: Her $i = 0, 1, \ldots$ için $x^i w(x)$ sözcüğünün sendromu hesaplanır. $s_i(x)$ ile $(x^i w(x) \pmod{g(x)})$ sendromunu gösterelim.

Adım 2: $\mathrm{wt}(s_m(x)) \leq \lfloor (d-1)/2 \rfloor$ olacak şekilde bir m sayısı bulunur.

Adım 3: $x^{n-m}s_m(x)$'in $x^n - 1$ ile bölümünden kalan hesaplanır. Bu kalana $e(x)$ denirse $w(x)$, $w(x) - e(x)$ olarak çözülür.

Örnek 20 **(i)** *Örnek 17'de olduğu gibi $w_1(x) = 1011100 = 1 + x^2 + x^3 + x^4$ sözcüğü alınmış olsun. $x^i w(x)$ sözcüğünün sendromu $s_i(x)$ olmak üzere $\mathrm{wt}(s_i(x)) \leq \lfloor (d-1)/2 \rfloor$ olana kadar sendromları hesaplayalım:*

i	$s_i(x)$
0	$1 + x + x^2$
1	$1 + x$
2	$x + x^2$
3	1

Buna göre $w_1(x)$ sözcüğünü $w_1(x) - x^4 s_3(x) = w_1(x) - x^4 = 1 + x^2 + x^3 = 1011000$ olarak çözeriz.

(ii) *Üreteç polinomu $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ olan $[15,7]$–devirli kodunu ele alalım. Bu kodun uzaklığının 5 olacağını eşlik–denetim matrisinden söyleyebiliriz. Ağırlığı en fazla 2 olan bir hata dizgesinin sıfırın en az 7–uzunluklu bir devirli dizisini*

içermesi gerekeceği açıktır. Buna göre böyle bir hata dizgesini yukarıdaki algoritmayı kullanarak düzeltebiliriz.

$$w(x) = 110011101100010 = 1 + x + x^4 + x^5 + x^6 + x^8 + x^9 + x^{13}$$

sözcüğü alınmış olsun. Aşağıdaki tabloda $x^i w(x)$ *dairesel kaymaları için* $s_i(x)$ *sendromlarını* $\mathrm{wt}(s_i(x)) \leq 2$ *olana kadar hesapladık:*

i	$s_i(x)$
0	$1 + x^2 + x^5 + x^7$
1	$1 + x + x^3 + x^4 + x^7$
2	$1 + x + x^2 + x^5 + x^6 + x^7$
3	$1 + x + x^2 + x^3 + x^4$
4	$x + x^2 + x^3 + x^4 + x^5$
5	$x^2 + x^3 + x^4 + x^5 + x^6$
6	$x^3 + x^4 + x^5 + x^6 + x^7$
7	$1 + x^5$

Buna göre $w(x)$ *sözcüğü* $w(x) - x^8 s_7(x) = w(x) - x^8 - x^{13} = 1 + x + x^4 + x^5 + x^6 + x^9 =$ 110011100100000 *olarak çözülür.*