Stockholms matematiska cirkel

Felrättande koder

Ludvig Olsson
Hampus Nyberg

Institutionen för matematik, KTH och
Matematiska institutionen, Stockholms universitet
2024–2025

Stockholms matematiska cirkel genom tiderna
(tidigare KTH:s matematiska cirkel)

2024-2025	Felrättande koder
2023-2024	Elliptiska Kurvor
2022-2023	Variationskalkyl
2021-2022	Matematik och AI
2020-2021	Musik och matematik
2019-2020	Datorernas matematik
2018-2019	Grafteori med inriktning på färgläggning
2017-2018	Geometriska konstruktioner
2016-2017	Vad är ett tal?
2015-2016	Fraktaler
2014-2015	Polytoper
2013-2014	Grupper, mönster och symmetrier
2012-2013	Den matematiska analysens grunder
2011-2012	Diofantiska ekvationer
2010-2011	Polynom
2009-2010	Hyperbolisk geometri
2008-2009	Talteori
2007-2008	Sannolikhetsteori
2006-2007	Gruppteori
2005-2006	Vad är ett tal?
2004-2005	Integraler
2003-2004	Linjär algebra och bioinformatik
2002-2003	Algebra och kryptografi
2001-2002	Analysens grunder
2000-2001	Talföljder, rekursioner och iterationer
1999-2000	Linjära avbildningar

Innehåll

Lista över grekiska alfabetet

A	α	alfa
B	β	beta
Γ	γ	gamma
Δ	δ	delta
E	ε	epsilon
Z	ζ	zeta
H	η	eta
Θ	θ	theta
I	ι	iota
K	κ	kappa
Λ	λ	lambda
M	μ	my
N	ν	ny
Ξ	ξ	xi
O	o	omikron
Π	π	pi
P	ρ	rho
Σ	σ	sigma
T	τ	tau
Υ	υ	ypsilon
Φ	ϕ	fi
X	χ	chi
Ψ	ψ	psi
Ω	ω	omega

Lista över mängdsymboler

$x \in X$	x är ett element i mängden X.
$X \subset Y$	X är en delmängd till Y.
$\forall x \in X$	för varje x som är ett element i mängden X.
$\exists x \in X \ldots$	existerar ett element x i mängden X sådant att $\ldots$
$f \colon X \to Y$	f är en funktionen med definitionsmängd X och målmängd Y.

Några ord på vägen

Detta kompendium är skrivet för att användas som kurslitteratur till Stockholms matematiska cirkel under läsåret 2024–2025 och består av åtta kapitel.

Kompendiet är inte tänkt att läsas enbart på egen hand, utan ska ses som ett skriftligt komplement till undervisningen. Alla elever rekommenderas att läsa igenom varje kapitel själv innan föreläsningen. Det är inte nödvändigt att förstå alla detaljer vid den första genomläsningen.

Som de flesta matematiska skrifter på högre nivå är kompendiet kompakt skrivet. Detta innebär att man i allmänhet inte kan läsa det som en vanlig bok. Istället bör man pröva nya satser och definitioner genom att på egen hand exemplifiera. Därmed uppnår man oftast en mycket bättre förståelse av vad dessa satser och deras bevis går ut på.

Till varje kapitel finns ett antal övningsuppgifter. De udda övningarna har lösningar längst bak i kompendiet. Syftet med dessa är att eleverna ska kunna lösa dem och på egen hand kontrollera att de förstått materialet. Övningar med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa dessa uppgifter även om man inte examineras på dem.

Om man kör fast kan man alltid fråga en kompis, en lärare på sin skola eller någon av författarna. Under årets gång kommer det att finnas övningstillfällen där eleverna kan jobba med uppgifterna, själva eller i grupp, och få hjälp av oss.

De övningsuppgifter som är något svårare markeras med en stjärna ($\star$). Uppgifter som är extra utmanande markeras med två stjärnor ($\star\star$).

Vissa övningar kan ha flera lösningar och det som står i facit bör i detta fall endast ses som ett förslag.

Några ord om cirkeln

Stockholms matematiska cirkel är en kurs för matematikintresserade gymnasieelever, som arrangeras av Kungliga Tekniska högskolan och Stockholms universitet. Cirkeln startade 1999. Vid starten hade den namnet KTH:s matematiska cirkel och hölls i KTH:s ensamma regi. Ambitionen med cirkeln är att sprida kunskap om matematiken och dess användningsområden utöver vad eleverna får genom gymnasiekurser, och att etablera ett närmare samarbete mellan gymnasieskolan och högskolan. Cirkeln ska särskilt stimulera elevernas matematikintresse och inspirera dem till fortsatta naturvetenskapliga och matematiska studier.

Till varje kurs skrivs ett kompendium som distribueras gratis till eleverna. Detta material, föreläsningsschema och övrig information om Stockholms matematiska cirkel finns tillgängligt på

`https://www.math-stockholm.se/cirkel`

Cirkeln godkänns ofta som en gymnasiekurs eller som matematisk breddning på gymnasieskolorna. Det är upp till varje skola att godkänna cirkeln som en kurs och det är lärarna från varje skola som sätter betyg på kursen. Lärarna är självklart också välkomna till cirkeln och många har kommit överens med sin egen skola om att få cirkeln godkänd som fortbildning eller som undervisning.

Vi vill gärna understryka att föreläsningarna är öppna för alla gymnasieelever, lärare eller andra matematikintresserade.

Vi har avsiktligt valt materialet för att ge eleverna en inblick i matematisk teori och tankesätt och presenterar därför både några huvudsatser inom varje område och bevisen för dessa resultat. Vi har också som målsättning att bevisa alla satser som används om de inte kan förutsättas bekanta av elever från gymnasiet.

Årets tema är felrättande koder. När signaler skickas mellan olika apparater finns det ofta bakgrundbrus som gör att mottagaren får fel meddelande. Tanken med felrättande koder är att lösa det här problemet så att man alltid kan rätta de få fel som sker i ett meddelande.

Kapitel 1 är en grundläggande introduktion till mängdlära. Kapitel 2 är en introduktion till klockaritmetik, ett räknesätt som är hur många datorer tänker. I kapitel 3 går vi igenom matriser, stora kvadrater med tal i som man kan multiplicera och addera. I kapitel 4 tolkar vi matriser på ett annat sätt och vi diskuterar vektorrum. I kapitel 5 introducerar vi för första gången felrättande koder. I kapitel 6 ger vi det enklaste sättet att representera felrättande koder på, med hjälp av generator och kontroll-matriser. I kapitel 7 diskuterar vi Hammingkoder, en viss typ av felrättande kod. I Kapitel 8 diskuterar vi Reed-Solomon koder, en annan typ av felrättande kod.

Författarna, sommaren 2024

1 Mängdlära

Temat för årets matematiska cirkel är Felrättande koder. Detta kapitel är en introduktion i den matematiska metoden och ett antal grundbegrepp som vi kommer använda oss av i kursen.

1.1 Definition, axiom, sats och bevis

I detta avsnitt ska vi beskriva den matematiska metoden utifrån fyra begrepp: *definition*, *sats*, *bevis* och *axiom*.

En *definition* bestämmer vad en term betyder så att man kan arbeta matematiskt med den. Till exempel kan vi definiera udda och jämna tal på följande sätt.

Definition 1.1.1. Ett heltal n är *udda* om det finns ett heltal k som uppfyller att $n = 2k + 1$.

Definition 1.1.2. Ett heltal n är *jämnt* om det finns ett heltal k som uppfyller att $n = 2k$.

Ofta har man en intuition om vad en term betyder redan innan man definierar den. Läsaren hade till exempel säkert en uppfattning om vad udda och jämna tal är innan vi definierade dem. Syftet med en definition är att precisera detta.

När definitionen är gjord, så överger man sina tidigare uppfattningar om vad termen betyder och utgår endast ifrån definitionen. Man säger att definitionen är *stipulativ*. En definition är alltså inte rätt eller fel, utan bara mer eller mindre användbar och intuitiv.

Definitioner bygger ofta på begrepp som läsaren är bekant med. Till exempel utgår Definition 1.1.1 och 1.1.2 från att läsaren redan vet vad ett heltal är.

En *sats* är ett påstående som bevisats vara sant. Varje sats hör samman med ett *bevis*: ett argument för att påståendet är sant.

Sats 1.1.3. *Om n är udda, så är $n + 1$ jämnt.*

Bevis. Om n är udda så finns det ett heltal k så att $n = 2k + 1$. Då gäller att

$$n + 1 = 2k + 1 + 1 = 2k + 2 = 2(k + 1).$$

Eftersom $k + 1$ är ett heltal, så är $n + 1$ ett jämnt tal. □

Bevisen kombinerar definitioner och olika logiska slutledningsregler för att nå den önskade slutsatsen. Sats 1.1.3 har en syskonsats. Beviset är mer eller mindre identiskt, och lämnas som övning.

Sats 1.1.4. *Om n är jämnt, så är $n + 1$ udda.*

En sats vars främsta syfte är att användas i beviset av en annan sats kallas för en *hjälpsats* eller ett *lemma*. En sats som följer omedelbart ur en annan sats, till exempel som ett specialfall, kallas för en *följdsats* eller ett *korollarium*.

Ett påstående måste vara bevisat för att få kallas för en sats. Om man har goda skäl att tro att ett påstående är sant men inte formellt bevisat det kallas påståendet för en *förmodan*, eller *hypotes*. Två exempel är *Riemannhypotesen* och *primtalstvillingsförmodan*.

En förmodan kan förbli obevisad i hundratals år. Ett berömt exempel är *Fermats stora sats*, som formulerades av Pierre de Fermat (1607–1665) år 1637 men bevisades först av Andrew Wiles år 1995. Riemannhypotesen, som ännu är obevisad, formulerades 1859 av Bernard Riemann (1826–1866).

Eftersom bevisen utgår ifrån definitionen, och inte vår intuition, så behöver man ibland bevisa saker som känns uppenbara. Läsaren vet till exempel att

(i) alla tal är antingen udda eller jämna, och

(ii) ett tal kan inte vara udda och jämnt samtidigt.

Men om man läser Definition 1.1.1 och 1.1.2 så ingår inte dessa påståenden. Kan man inte tänka sig tal som varken är udda eller jämnt? Eller tal som är både och?

Bevis utgår ifrån antaganden och tidigare kända satser. Dessa tidigare satser måste också bevisas innan de kan anses giltiga. Men dessa bevis måste också bygga på antaganden och satser, som också måste bevisas, och så vidare.

För att undvika en oändlig kedja av bevis, eller ett cirkulärt bevis (ett bevis som använder sig av det man försöker bevisa) så måste man göra grundantaganden som inte behöver bevisa. Dessa kallas för *axiom*. Exempel på axiom är att mängden av heltal existerar och att addition uppfyller

- (Associativitet) För alla heltal n, m, p gäller $(n + m) + p = n + (m + p)$.
- (Identitet) Det finns ett element 0, som vi kallar *nollan*, sådan att för alla heltal n så gäller $0 + n = n + 0 = n$.
- (Inverser) För varje heltal n existerar ett heltal $(-n)$, som vi kallar för *minus* n, sådan att $0 = n + (-n) = (-n) + n$.
- (Kommutativitet) För alla heltal n, m så gäller $n + m = m + n$.

1.2 Bevistekniker

Ett bevis för en sats är ett argument som förklarar varför satsen är sann. Vi har redan sett ett exempel när vi bevisade Sats 1.1.3. I detta avsnitt ska vi gå igenom tre tekniker för att bevisa matematiska satser: direkta bevis, motsägelsebevis och induktionsbevis.[1]

Ett *direkt bevis* utgår ifrån satsens antaganden och definitioner och bevisar satsen rakt på, så att säga. Beviset av Sats 1.1.3 är ett exempel på direkt bevis. Ett annat är följande sats.

[1] Ibland förekommer termen *indirekt bevis*. Vissa använder det som synonym till motsägelsebevis, andra som en synonym till bevisregeln *modus tollens*. Vi undviker den helt.

Sats 1.2.1. *Antalet funktioner från en mängd A med n element till en mängd B med m element är m^n.*

Bevis. Varje funktion från A till B kan beskrivas som en tabell där varje element i A motsvaras av precis ett element i B. Listan innehåller totalt n platser, och på varje plats kan vi välja bland m element att välja bland. Alltså finns det totalt

$$\underbrace{m \cdot m \cdots m \cdot m}_{n \text{ stycken}} = m^n$$

olika funktioner. □

Ibland går det inte att använda direkta bevis, till exempel när man ska bevisa att något inte är fallet. Då kan det vara enklare att anta att det man vill bevisa är falskt, och visa att detta leder till en motsägelse. Om alla steg i beviset är korrekta så måste det ursprungliga antagandet vara fel. Detta kallas för ett *motsägelsebevis*.

Sats 1.2.2. *Ett tal kan inte vara udda och jämnt samtidigt.*

Bevis. Antag att n är ett tal som är båda udda och jämnt. Då finns det två heltal, k och l, så att $n = 2k$ och $n = 2l + 1$. Då gäller att

$$2k = n = 2l + 1 \implies 2k - 2l = 1 \implies 2(k - l) = 1.$$

Med andra ord finns det heltal $m = k - l$ så att $2m = 1$. Kan det finns ett sådant tal? Det finns två fall.

(i) Om $m \leqslant 0$, så är $1 = 2m \leqslant 0$. Motsägelse!

(ii) Om $m \geqslant 1$ så är $2m \geqslant 2 > 1$. Motsägelse! □

Ett berömt motsägelsebevis är följande.

Sats 1.2.3. *Talet $\sqrt{2}$ är irrationellt.*

Bevis. Antag motsatsen, det vill säga att $\sqrt{2} = a/b$ för några heltal a och b. Antag att a och b är förkortade så långt som möjligt. Då kan endast en av a eller b vara jämn, eftersom om båda är jämna kan vi skriva

$$\sqrt{2} = \frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}$$

och då var inte a och b förkortade så långt som möjligt.

Av definitionen av $\sqrt{2}$ får vi att

$$\sqrt{2}^2 = 2 = \frac{a^2}{b^2} \implies 2b^2 = a^2.$$

Den sista ekvationen säger att a^2 är jämn. Eftersom kvadrater av udda tal är udda (se Övning 1.24), så måste a vara ett jämnt tal, det vill säga $a = 2k$ för något heltal k. Då får vi att

$$2b^2 = (2k)^2 = 4k^2 \implies b^2 = 2k^2.$$

Eftersom b^2 är jämnt, så måste b vara jämnt. Men nu har vi bevisat att både a och b är jämna, vilket var omöjligt eftersom vi hade förkortat bråket så långt som möjligt. Detta är en motsägelse. □

Att bevis inkluderar antaganden och små hjälpsatser som inte nämns är snarare regel än undantag, till exempel lägger vi nästan aldrig tid på att visa $2 > 0$ i mitten av ett bevis. Ifall man bevisade precis vartenda antagande och påstående utifrån axiomen varje gång skulle bevisen bli väldigt långa och komplicerade. Läsaren förväntas själv fylla i de luckor som uppstår.

Det händer dock att uppenbara antaganden är mycket svåra, till och med omöjliga, att bevisa utifrån definitionerna. Historien är fylld av matematiker som gjort till synes självklara antaganden som sedan visat sig vara svåra att bevisa.

Beviset av Sats 1.2.3 är ett exempel på det. Vi antar att ett bråk kan förkortas så långt som möjligt. Detta är inte självklart, utan bygger i själva verket på aritmetikens fundamentalsats som vi inte kommer att behandla i kursen.

Den tredje bevistekniken som finns kallas för *induktionsbevis* men den kommer vi inte behöva i den här kursen.

1.3 Olika satser och hur man bevisar dem

I föregående avsnitt diskuterade vi olika bevistekniker. Men vilka tekniker är lämpliga för vilka typer av satser?

- **Implikation:** Man säger att P implicerar Q om Q är sant när P är det. Ett exempel är Sats 1.1.4, som säger att om ett tal n är jämnt, så är talet $n + 1$ udda. Man brukar beteckna implikationer med en tjock pil $\Longrightarrow$, så att P medför Q skrivs

  $$P \implies Q.$$

  En implikation kan bevisas med ett direkt bevis. Då antar man att P är sant, och sedan visar man att Q också måste vara sant (det är så vi bevisar Sats 1.1.4). Man kan också använda ett motsägelsebevis. Då antar man att P är sann och att Q är falsk, och bevisar en motsägelse.

  Ett tredje sätt att bevisa att P implicerar Q är att bevisa att om Q är falsk, så är P falsk. Detta kallas för *omvändningen* av en implikation.

- **Ekvivalens:** En ekvivalens är när två påståenden P och Q implicerar varandra, alltså att om P så Q, och om Q så P. Man brukar använda frasen P om och endast om Q. Man använder tjocka dubbelpilar för att beteckna ekvivalenser, så att P om och endast om Q skrivs som

  $$P \iff Q.$$

  Ekvivalenser bevisas genom att första visa att P implicerar Q, och sedan att Q implicerar P.

- **Universalsats:** En universalsats säger att alla n i en mängd M uppfyller något villkor P. Universalsatser kan bevisas som implikationer, genom att omformulera universalsatsen som att om n ligger i mängden M, så uppfyller n villkoret P, det vill säga

  $$n \in M \implies n \text{ uppfyller } P$$

  Man kan även bevisa en universalsats genom ett motsägelsebevis. Då antar man att det finns ett n i M som inte uppfyller P, och bevisar att det är omöjligt.

- **Existenssats:** En existenssats säger att finns ett objekt n som har egenskapen P. Den typiska existenssatsen är ekvationslösning. Att $x^2 = 3$ har en lösning är en existenssats, och kan omformuleras som att det finns ett tal x så att $x^2 = 3$.

  Ett sätt att bevisa en existenssats är att konstruera det sökta objektet utifrån objekt man redan vet finns. Till exempel så kan man bevisa att det finns ett udda kvadrattal genom att notera att $3^2 = 9$ är udda och ett kvadrattal.

  Man kan också använda ett motsägelsebevis. Då antar man att det inte existerar någon objekt med egenskapen P och visar att det leder till en motsägelse. Dessa bevis har fördelen att vi inte behöver beskriva hur objektet konstrueras. I gengäld kan bevisen vara mycket komplicerade.

En variant på universalsatsen är att inget n i M uppfyller P. Den kan omformuleras som att alla n i M saknar egenskapen P. För dessa typer av satser är motsägelsebevis ofta smidiga: man antar att det finns ett n i M som uppfyller P och härleder en motsägelse.

Universal- och existenssatser är duala till varandra, i bemärkelsen att om du ska bevisa en existenssats med hjälp av ett motsägelsebevis så antar du en universalsats, och vice versa, se bevisen av 1.2.2 och 1.2.3.

1.4 Mängder

En *mängd* är en samling objekt. Man kan samla nästan vad man vill i en mängd: tal, katter, och andra mängder.[2] Det viktiga är att man alltid kan avgöra ifall ett objekt tillhör mängden eller inte. De objekt som ligger i mängden kallas för *element*.

Det lättaste sättet att beskriva en mängd är att räkna upp elementen som ingår i den. För att markera att objekten ligger i en mängd, så omger man listan med *mängdklamrar* { och }. Mängden som innehåller 1, 2 och 3 skrivs alltså som

$$\{1, 2, 3\}.$$

[2] Vi skriver *nästan* av en anledning. Det finns samlingar av objekt som kan beskrivas men som inte utgör en mängd. Detta kallas *Russells paradox*, efter Bertrand Russell (1872–1970). Russells exempel är samlingen av alla mängder som inte innehåller sig själv.

Två mängder A och B är lika om de innehåller samma element, vilket skrivs $A = B$. Det spelar ingen roll i vilken ordning man skriver elementen eller hur många gånger de listas. Därför gäller att

$$\{1, 1, 2, 3\} = \{1, 2, 3\} = \{2, 3, 1\}.$$

Om ett element x tillhör en mängd A brukar man skriva $x \in A$, vilket uttalas som x *tillhör* A. Om x inte tillhör A skriver man $x \notin A$. Antalet element som tillhör en mängd A brukar betecknas med $|A|$.

Mängden på formen $\{\}$ innehåller inte några element alls och kallas den *tomma mängden*. Den brukar betecknas med $\emptyset$ och är unik i aspekten att den saknar element, vi skriver alltså $|\emptyset| = 0$.

En mängd kan innehålla andra mängder som element. Mängden

$$A = \{\{1, 2\}, 3\}$$

har två element vilket skrivs som $|A| = 2$. Dess element är: mängden $\{1, 2\}$ och talet 3. Mängden $\{1, 2\}$ innehåller i sin tur elementen 1 och 2. Däremot innehåller A varken 1 eller 2, det vill säga

$$\{1, 2\} \in A \qquad \text{men } 1 \notin A.$$

Att mängder kan innehålla andra mängder kan ha paradoxala konsekvenser. Till exempel kan vi lägga den tomma mängden i en mängd, och bilda mängden av den tomma mängden.

$$A = \{\emptyset\} = \{\{\}\}$$

Mängden A innehåller ett element, den tomma mängden, och är därför inte tom. Mängden av den tomma mängden är alltså inte lika med den tomma mängden.

Detta verkar motsägelsefullt. Den tomma mängden är ju tom, så mängden av den tomma mängden borde ju också vara tom? Tricket är att skilja på mängden och elementen i mängden. Den tomma mängden är ju ett element i sig, även om den inte innehåller några element, precis som att 0 är ett tal, trots att representerar ett antal som inte finns. Man kan tänka sig att en påse som innehåller en annan tom påse, inte är tom.

Det finns ingen begränsning på hur stor en mängd kan vara, och de flesta mängder man studerar innehåller oändligt många element. Dessa mängder kan naturligtvis inte skrivas ut som en lista. Istället beskriver man dem med *mängdbyggaren*, som har följande allmänna form $\{x \mid \text{villkor på } x\}$. Den här mängden består av alla element som uppfyller villkoret. Ett exempel är mängden

$$\{n \mid n \text{ är jämnt}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

som innehåller alla jämna tal.

En mängd B är en *delmängd* av en mängd A om alla element som tillhör B även tillhör A. Man skriver detta som $B \subset A$. Till exempel så är $\{1, 2\}$ en delmängd av $\{1, 2, 3\}$, eftersom 1 och 2 är element i båda mängderna. Om två mängder är delmängder av varandra så är de lika.

En icke-tom mängd har alltid minst två delmängder: sig själv och den tomma mängden. En delmängd B av A är *äkta* om $B \neq A$.

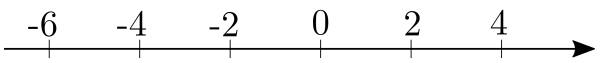
Det är lätt att blanda ihop element och delmängder. Det beror på att mängder kan innehålla andra mängder, så att en delmängd av en mängd kan vara ett element i mängden. Mängden $A = \{\emptyset\}$ är ett bra exempel. Den tomma mängden är både ett element i och en delmängd av A.

I mängden $A = \{1, 2, \{1, 2\}\}$ är $\{1, 2\}$ både en delmängd och ett element. Däremot så är $\{1\}$ enbart en delmängd av A, medan 1 enbart är ett element.

De olika talsystemen kan ses som mängder av tal, och har fått egna beteckningar. De *naturliga talen* betecknas med $\mathbb{N}$ och består av talen 0, 1, 2, 3, och så vidare.[3]

Naturliga tal kan adderas och multipliceras utan problem. Resultatet är alltid ett nytt naturligt tal. För att subtrahera behöver vi införa de negativa talen -1, -2, och så vidare. De naturliga talen tillsammans med de negativa talen kallas för *heltalen*, och betecknas med $\mathbb{Z}$ (av tyskans *Zahl* = tal).

Heltal kan adderas, subtraheras och multipliceras. Man kan däremot inte dividera dem med varandra. För detta krävs *rationella tal*. De definieras som alla kvoter a/b, där a och b är heltal och b är skilt från 0. Mängden av alla rationella tal betecknas med $\mathbb{Q}$.

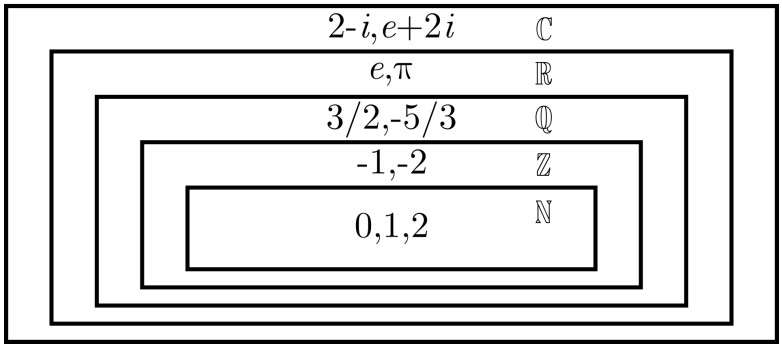


Figur 1.1: Tallinjen runt 0.

De rationella talen ligger på den så kallade *tallinjen*, som går från negativa tal till vänster och till positiva tal till höger (se Figur 1.1). Det finns dock tal som inte är rationella, men som ändå ligger på tallinjen. Ett exempel är $\sqrt{2}$, som är längden på diagonalen i en kvadrat med sidan 1. Lägger man till dessa tal får de *reella talen*, som betecknas med $\mathbb{R}$.[4] Reella tal som inte är rationella kallas för *irrationella*.

[3] Vissa exkluderar 0 från de naturliga talen. Att inkludera 0 har dock fördelar. Om man börjar räkna från 0 och går ett steg i taget kommer man ha gått n steg när man räknat till n. Exempel: om vi räknar till 3 från 0 så får vi $0 \to 1 \to 2 \to 3$, vilket är 3 steg. Om vi börjar från 1 får vi istället $1 \to 2 \to 3$, vilket är 2 steg.

[4] Reella tal är mycket mystiska. Den matematiska cirkeln 2016–2017, *Vad är ett tal?*, handlade om hur man kan definiera dem i termer av rationella tal. Den intresserade läsaren uppmanas att söka upp kompendiet på Cirkelns hemsida: `https://www.math-stockholm.se/samverkan/cirkel/`



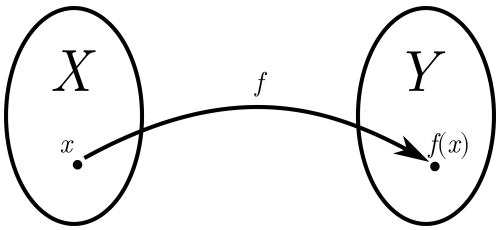
Figur 1.2: De olika talsystemen från $\mathbb{N}$ till $\mathbb{C}$.

De reella talen kan utvidgas ytterligare till de *komplexa talen*, som betecknas med $\mathbb{C}$, genom att lägga till ett tal i som uppfyller $i^2 = -1$.

1.5 Funktioner

En funktion f från en mängd X till en mängd Y beskriver hur man parar ihop element i en mängd X med element i en mängd Y. Det brukar skrivas som $f\colon X \to Y$. Mängden X kallas för *definitionsmängd* och mängden Y kallas för *målmängd*. Man kan se f som en process som tar ett element i mängden X och avger ett element som ligger i mängden Y. När man tillämpar en funktion på ett element x i X så kallas x för funktionens *argument*. Mängden av alla värden en funktion i praktiken antar kallas för funktionens *värdemängd*, och denna betecknas ofta med V_f. Värdemängden är då alltså en delmängd av målmängden, och kan beskrivas som $V_f = \{f(x) \mid x \in X\}$. Till exempel är $\sin(x)$ en funktion från $\mathbb{R}$ till $\mathbb{R}$, så funktionens målmängd är alltså $\mathbb{R}$, men värdemängden är $[-1, 1]$.

Två funktioner är lika när de har samma definitionsmängd, samma målmängd och de är lika på alla element i definitionsmängden. Definitions- och målmängden är alltså en del av funktionen.



Figur 1.3: En funktion f från X till Y.

Funktioner beskrivs ofta med formler. Exempelvis så kan funktionen $f\colon \mathbb{N} \to \mathbb{N}$ som tar ett naturligt tal och returnerar dess kvadrat beskrivas som $f(n) = n^2$. Alla polynom kan ses som en funktion från $\mathbb{R}$ till $\mathbb{R}$, som beräknas genom att man sätter in talet x i uttrycket. En funktion måste dock inte ges av en formel. Det enda som krävs är att funktionen är definierad för alla element i definitionsmängden, och att den alltid ger samma svar. Vi ger nu ett par

exempel på detta och hur man istället kan beskriva en funktion.

Exempel 1.5.1. Vårt första exempel är absolutbeloppet $|x|$ av ett reellt tal x, som definieras som avståndet på tallinjen från x till origo. Detta är en funktion vars definitionsmängd och målmängd är $\mathbb{R}$. Man kan beräkna den genom att man tar bort eventuella minustecken framför talet, det vill säga

$$|x| = \begin{cases} x & \text{om } x \geqslant 0 \\ -x & \text{om } x < 0. \end{cases}$$

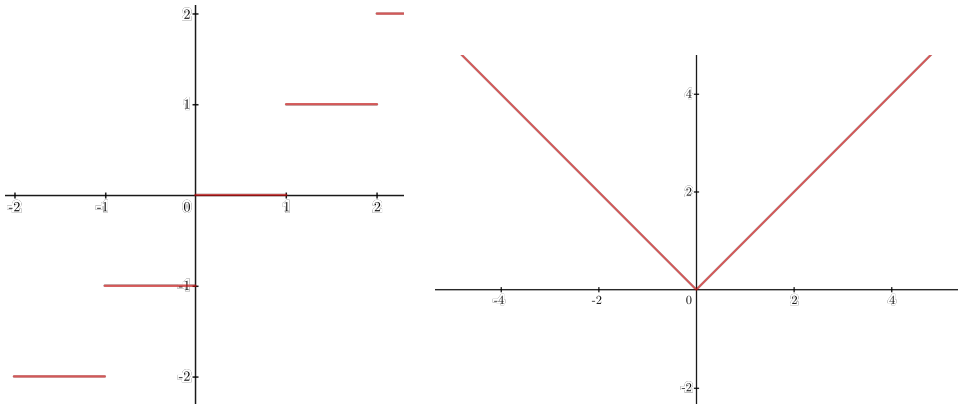
Exempelvis så gäller $|-3| = -(-3) = 3$ och $|2| = 2$.

Exempel 1.5.2. *Golvfunktionen* är funktionen som avbildar reella tal x på heltalet man får när man avrundar x nedåt. Vi benämner den funktionen med $\lfloor \ldots \rfloor$. För att förtydliga hur denna och andra funktioner används brukar vi skriva på följande sätt

$$\begin{aligned} \lfloor \ldots \rfloor \colon \mathbb{R} &\to \mathbb{Z} \\ x &\mapsto \lfloor x \rfloor. \end{aligned}$$

eftersom det kanske inte är uppenbart för läsaren att man ska skriva $\lfloor x \rfloor$ när man vill referera till funktionens värde vid punkten x istället för $\lfloor \ldots \rfloor_x$ eller $\lfloor \ldots \rfloor(x)$. Exempelvis så gäller $\lfloor \pi \rfloor = 3$.

En funktion $f \colon \mathbb{R} \to \mathbb{R}$ kan beskrivas genom sin *graf*, som definieras som mängden av punkter i planet på formen $(x, f(x))$.



(a) Grafen av $f(x) = \lfloor x \rfloor$ **(b)** Grafen av funktionen $f(x) = |x|$

Figur 1.4: Golv- och absolutbeloppsfunktionen.

Om man istället betraktar en funktion med ändlig definitionsmängd kan man beskriva den med en tabell.

Exempel 1.5.3. Betrakta funktionen från mängden $\{1, 2, 3\}$ till mängden $\{2, 3, 4, 5\}$ där $f(1) = 3$ och $f(2) = 4$ och $f(3) = 3$. Vi kan beskriva denna med en tabell eftersom vi bara ändligt många element i vår definitionsmängd,

x	f(x)
1	3
2	4
3	3

Vi kan också beskriva den med en formel eftersom definitionsmängden och målmängden är delmängder till de reella talen $\mathbb{R}$ så till exempel gäller

$$f(x) = 4 - (x-2)^2.$$

Exempel 1.5.4. Betrakta funktionen från mängden $\{\text{hund}, \text{katt}\}$ till mängden $\{0, 1\}$ där $f(\text{hund}) = 0$ och $f(\text{katt}) = 1$. Vi kan beskriva denna med en tabell eftersom vi bara har ändligt många element i vår definitionsmängd,

x	f(x)
hund	0
katt	1

.

Det finns dock inte någon vettig formel som beskriver f eftersom det inte finns något välkänt sätt att 'addera' eller 'multiplicera' orden hund och katt på ett sätt som ger ett tal.

Definition 1.5.5. Givet två funktioner sådana att den enas definitionsmängd är den andras målmängd, $f\colon Y \to Z$ och $g\colon X \to Y$ kan vi definiera deras *sammansättning* $f \circ g\colon X \to Z$ enligt regeln

$$(f \circ g)(x) = f(g(x)).$$

Definition 1.5.6. Givet en funktion $f\colon X \to Y$ och en delmängd $A \subset X$ så kallar vi mängden $\{f(x) \mid x \in A\}$ för *bilden av* A och den betecknas $f(A)$. Om x är ett element i X brukar vi även kalla $f(x)$ för *bilden* av x.

Definition 1.5.7. Givet en funktion $f\colon X \to Y$ och en delmängd $B \subset Y$ så kallar vi mängden $\{x \mid f(x) \in B\}$ för *urbilden av* B. Om y är ett element i Y brukar vi kalla urbilden $\{x \mid f(x) = y\}$ för *fibern* av y. Givet ett element x i fibern av y kommer vi i den här kursen beteckna fibern av y med $[x]$.

Definition 1.5.8. Vi säger att en funktion $f\colon X \to Y$ är *surjektiv* om alla element i Y är bilden av något element i X, det vill säga om värdemängden överensstämmer med målmängden. En funktion sägs vara *injektiv* om varje element i värdemängden är bilden av exakt ett element i definitionsmängden. Om en funktion är både surjektiv och injektiv säger vi att funktionen är *bijektiv*.

Notera att en bijektiv funktion är *inverterbar*: Det vill säga, det existerar en funktion som kallas *den inversa funktionen* eller f^{-1} med beskrivningen $f^{-1}\colon Y \to X$ och $f^{-1}(f(x)) = x$ för alla $x \in X$ och $f(f^{-1}(y)) = y$ för alla $y \in Y$. Den inversa funktionen, om den finns, är alltså den funktion som för varje element $y \in Y$ ger det unika elementet $x \in X$ som har egenskapen att $f(x) = y$. I övning 1.14 ser vi exempelvis att en strikt växande funktion $f\colon \mathbb{R} \to \mathbb{R}$ är injektiv. Det är även värt att notera att en injektiv funktion blir bijektiv om vi byter ut målmängden mot värdemängden.

Huruvida en funktion är inverterbar eller ej beror inte bara på regeln som beskriver funktionen, utan på definitionsmängd och målmängden.

Exempel 1.5.9. Betrakta funktionen $f(x) = x^2$ som tar ett tal och kvadrerar det.

Betraktat som funktion från $\mathbb{R}$ till $\mathbb{R}$ är den inte inverterbar. Den är inte surjektiv eftersom det till exempel inte finns något $x \in \mathbb{R}$ så att $x^2 = -1$. Problemet här är alltså att funktionens målmängd inte överensstämmer med dess värdemängd, det vill säga att funktionen inte är surjektiv.

Detta problem kan lösas genom att begränsa målmängden till värdemängden, men även om vi betraktar f som en funktion från $\mathbb{R}$ till dess värdemängd, det vill säga mängden av icke-negativa tal $[0, \infty)$, så är funktionen inte inverterbar. Vi har fortfarande problemet att funktionen inte är injektiv. Till exempel så har vi $(-1)^2 = 1^2 = 1$ och eftersom det finns två element som avbildas på 1, kan vi inte entydigt definiera en invers funktion.

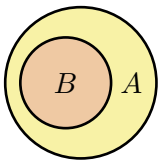
Om vi däremot betraktar f som en funktion från $[0, \infty)$ till $[0, \infty)$ så är den både injektiv och surjektiv, det vill säga bijektiv, och således har funktionen en väldefinierad invers, nämligen $f^{-1}(x) = \sqrt{x}$. Till exempel så är i detta fall $f^{-1}(1) = 1$ eftersom vi bara får välja den positiva roten.

Vi har en liknande situation med $\sin(x)$ och $\cos(x)$. Betraktade som funktioner från $\mathbb{R}$ till $\mathbb{R}$ är dessa funktioner varken injektiva eller surjektiva, men genom att betrakta $\sin(x)$ som en funktion från $[-\pi/2, \pi/2]$ till $[-1, 1]$ och $\cos(x)$ som en funktion från $[0, \pi]$ till $[-1, 1]$ erhåller vi bijektiva, och således inverterbara funktioner.

1.6 Mängdoperationer

I detta avsnitt ska vi beskriva ett antal olika sätt från en eller flera mängder skapa en ny mängd. Vi kallar dessa för *mängdoperationer*. I nästa kapitel kommer vi även att se hur vissa av dessa mängdoperationer går att generalisera till andra situationer.

För att illustrera mängder använder man ibland *Venndiagram*, efter matematikern John Venn (1834–1923). Där representeras mängder som enkla former, oftast cirklar, och formernas förhållanden till varandra motsvarar mängdernas. Till exempel kan man illustrera att B är en delmängd av A genom att rita dem som två cirklar, där B ligger inuti A.



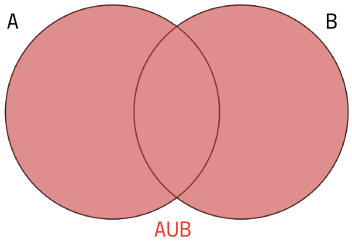
Figur 1.5: Venndiagram för $B \subset A$.

Unionen

Unionen av mängderna A och B är mängden som består av alla element som ligger i A *eller* i B. Den betecknas med $A \cup B$ och definieras som

$$A \cup B = \{x \mid x \in A \text{ eller } x \in B\}.$$

Ett exempel är $\{1, 2, 3\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$.



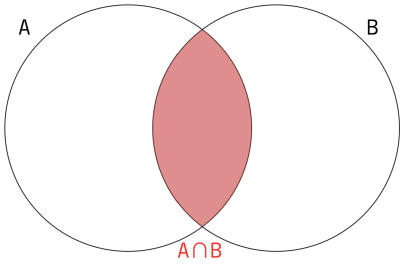
Figur 1.6: Venndiagram för $A \cup B$.

Snittet

Snittet av mängderna A och B är mängden som består av alla element som ligger i A *och* i B. Den betecknas med $A \cap B$ och definieras som

$$A \cap B = \{x \mid x \in A \text{ och } x \in B\}.$$

Ett exempel är $\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$.



Figur 1.7: Venndiagram för $A \cap B$.

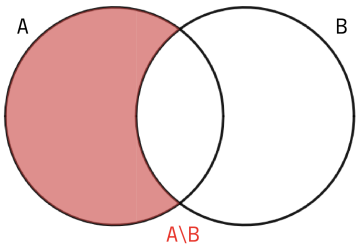
Två mängder A och B sägs vara *disjunkta* om de inte har några gemensamma element, det vill säga om $A \cap B = \emptyset$.

Differensen och komplementet

Differensen av en mängd A och B är mängden som består av alla element som ligger i A men inte i B. Den betecknas med $A \setminus B$ och definieras som

$$A \setminus B = \{x \mid x \in A \text{ och } x \notin B\}.$$

Ett exempel är $\{1, 2, 3\} \setminus \{2, 3, 4\} = \{1\}$.



Figur 1.8: Venndiagram för $A \setminus B$.

Notera att $A \setminus B$ inte är lika med $B \setminus A$, exempelvis gäller

$$\{2,3,4\} \setminus \{1,2,3\} = \{4\} \neq \{1\} = \{1,2,3\} \setminus \{2,3,4\}.$$

Om alla uppträdande mängder är delmängder av en viss mer eller mindre underförstådd grundmängd M talar man ofta om $M \setminus A$ som *komplementet* till A (med avseende på M). Vi kommer att beteckna komplementet till A med A^c. Om vi till exempel pratar om mängder av heltal, och vi till exempel betraktar mängden $A = \{1,2,3\}$, så avser komplementet till A mängden av alla heltal *förutom* $1, 2$ och 3.

Den kartesiska produkten

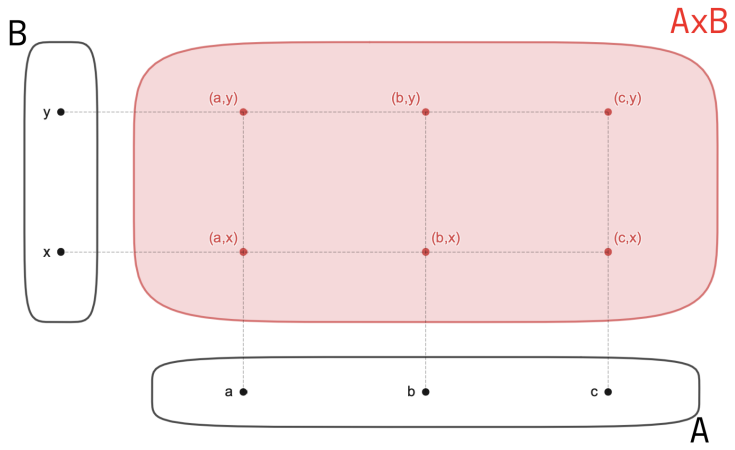
Den kartesiska produkten av två mängder A och B är mängden som består av alla par av element så att det första ligger i A och det andra i B. Den betecknas med $A \times B$ och definieras som

$$A \times B = \{(x,y) \mid x \in A \text{ och } y \in B\}.$$

Två olika exempel är

$$\{a,b,c\} \times \{x,y\} = \{(a,x),(a,y),(b,x),(b,y),(c,x),(c,y)\}$$
$$\{1,2,3\} \times \{2,3,4\} = \{(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)\}.$$

Notera att ordningen är viktig, exempelvis gäller $(1,2) \in \{1,2,3\} \times \{2,3,4\}$ men $(2,1) \notin \{1,2,3\} \times \{2,3,4\}$.



Figur 1.9: Venndiagram för $A \times B$.

När vi tar den kartesiska produkten av en mängd med sig själv brukar vi använda notationen $A^2 = A \times A$. Mer allmänt skriver vi

$$A^n = \underbrace{A \times \ldots \times A}_{n \text{ gånger}} = \{(a_1, \ldots, a_n) \mid \text{ alla } a_i \in A\}.$$

Till exempel är det reella talplanet $\mathbb{R} \times \mathbb{R}$ vilket vi brukar beteckna med $\mathbb{R}^2$.

Mängden av funktioner

Mängden av funktioner från mängden A till mängden B är mängden som består av alla funktioner från A till B. Den betecknas med B^A och definieras som

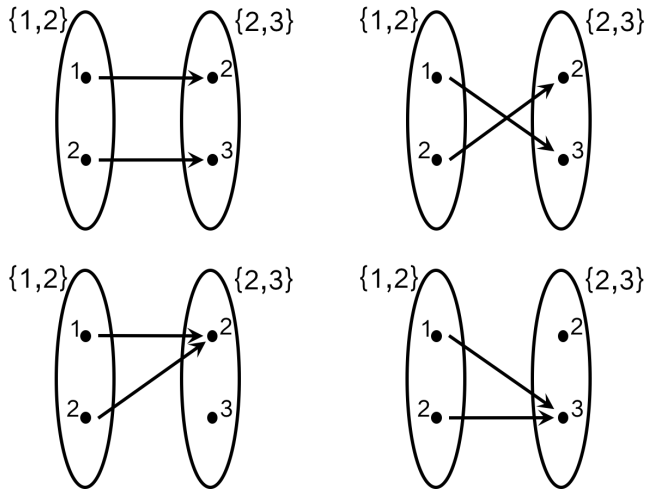
$$B^A = \{f \mid f \colon A \to B\}.$$

Ett exempel är

$$\{2,3\}^{\{1,2\}} = \left\{ \begin{array}{|c|c|}\hline \text{x} & \text{f(x)} \\ \hline 1 & 2 \\ \hline 2 & 2 \\ \hline \end{array}, \begin{array}{|c|c|}\hline \text{x} & \text{f(x)} \\ \hline 1 & 2 \\ \hline 2 & 3 \\ \hline \end{array}, \begin{array}{|c|c|}\hline \text{x} & \text{f(x)} \\ \hline 1 & 3 \\ \hline 2 & 2 \\ \hline \end{array}, \begin{array}{|c|c|}\hline \text{x} & \text{f(x)} \\ \hline 1 & 3 \\ \hline 2 & 3 \\ \hline \end{array} \right\}$$

vilken också kan skrivas som

$$\{2,3\}^{\{1,2\}} = \{f(x) = 2, f(x) = x + 1, f(x) = 4 - x, f(x) = 3\}.$$



Figur 1.10: Illustration av $\{2,3\}^{\{1,2\}}$.

Potensmängd

Vi definierar *potensmängden* av en mängd som mängden av alla delmängder till en mängd A. Den betecknas med

$$2^A = \{B \mid B \subset A\}.$$

Ett exempel är

$$2^{\{a,b,c\}} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\},$$

Kvotmängd (överkurs)

Kvotmängden av A kan definieras på många olika sätt. Vi väljer att definiera kvotmängden av A givet en funktion $f\colon A \to B$ som mängden vars element är fibrerna till f. Elementen i kvotmängden är alltså delmängder till A på formen $\{x \in A\colon f(x) = b\}$. För varje $a \in A$ använder vi notationen

$$[a] = \{x \in A\colon f(x) = f(a)\}.$$

Vi kallar i denna kontext mängden $[a]$ för en *ekvivalensklass* och vi kallar a för en *representant* för ekvivalensklassen $[a]$. Olika element $a \neq b \in A$ kan vara representanter för samma ekvivalensklass, vi säger att a och b är *ekvivalenta* när $[a] = [b]$. Detta inducerar en s.k. *ekvivalensrelation* mellan elementen i A som vi betecknar med $\sim$.

Vi definierar kvotmängden

$$A/\sim \;\; = \{[a] \mid a \in A\}.$$

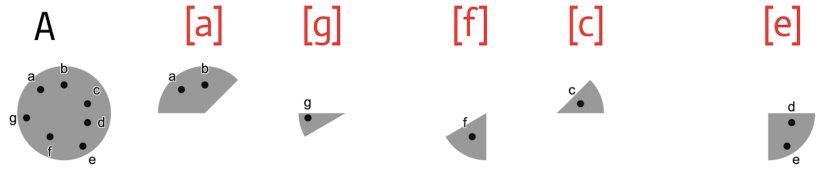
Låt oss demonstrera detta med ett par exempel.

Exempel 1.6.1. Låt $A = \{a, b, c, d, e, f, g\}$ och

$$\phi\colon A \to \{0, 1, 2, 3, 4\}$$
$$\phi(a) = \phi(b) = 0 \quad \phi(g) = 1 \quad \phi(f) = 2 \quad \phi(c) = 3 \quad \phi(d) = \phi(e) = 4.$$

och då blir

$$A/\sim \quad = \{\{a, b\}, \{g\}, \{f\}, \{c\}, \{d, e\}\}.$$



Figur 1.11: Illustration av hur elementen i $A/\sim$ är delmängder till A.

Exempel 1.6.2. Ifall $f\colon \mathbb{Z} \to \{0, 1\}$ definieras som

$$f(n) = \begin{cases} 0 \text{ om } n \text{ jämnt} \\ 1 \text{ om } n \text{ udda.} \end{cases}$$

Då kan vi se att

$$\mathbb{Z}/\sim \quad = \{[0], [1]\}$$

är en mängd med två element, $[0]$ som är mängden av de jämna talen och $[1]$ som är mängden av de udda talen. Till exempel gäller det att $[1] = [3] = [51]$, eftersom talen $1, 3, 51$ kan alla väljas som representanter för de udda talen i detta exempel.

Övningar

Övning 1.1. Lista elementen i följande mängder.

(i) $A = \{n \in \mathbb{N} \mid n < 5\}$.

(ii) $B = \{1, 2, \{2, 3\}\}$.

(iii) $C = \{k \in \mathbb{Z} \mid k^2 < 16\}$.

(iv) $A \cap B$.

(v) $(C \setminus A) \cup B$.

Övning 1.2. Lista elementen i följande mängder.

(i) $A = \{x \in \mathbb{Q} \mid x^2 = 2\}$.

(ii) $B = \{0, 1, 2, 3\}$.

(iii) $C = \{p/q \mid p, q \in \mathbb{N}, 0 \leqslant p < 3 \text{ och } 1 \leqslant q < 3\}$.

(iv) $(B \cup A) \cap C$.

(v) $(C \cap B) \setminus A$.

Övning 1.3. För nedanstående par av mängder A och B, avgör om A och B är lika, disjunkta, någon av dem är en äkta delmängd av den andra eller ingetdera.

(i) $A = \{1, 2, 3\}$ och $B = \{1, 1, 2\}$.

(ii) $A = \{0, 1, 2\}$ och $B = \{n \in \mathbb{N} \mid n^2 < 9\}$.

(iii) $A = \{\{\}\}$ och $B = \{x \in \mathbb{N} \mid 2x = -2\}$.

(iv) $A = \{x \in \mathbb{R} \mid |x| < 1\}$ och $B = \{x \in \mathbb{R} \mid |x - 1| < 1\}$.

(v) $A = \{x \in \mathbb{Q} \mid x^2 = 2\}$ och $B = \{x \in \mathbb{R} \mid x^2 = 2\}$.

Övning 1.4. För nedanstående par av mängder A och B, avgör om A och B är lika, disjunkta eller någon av dem är en äkta delmängd av den andra.

(i) $A = \{-2, 0, 2\}$ och $B = \{x \in \mathbb{Z} \mid |x| < 3 \text{ och } x \text{ är jämnt}\}$.

(ii) $A = \{x \in \mathbb{R} \mid x^2 < 2\}$ och $B = \{x \in \mathbb{Q} \mid x^2 \leqslant 2\}$.

(iii) $A = \{x \in \mathbb{Z} \mid x \text{ är jämnt}\}$ och $B = \{x \in \mathbb{Z} \mid x \text{ är kvadrattal}\}$.

(iv) $A = \{x \in \mathbb{Z} \mid 2x = -2\}$ och $B = \{x \in \mathbb{N} \mid 2x = 2\}$.

(v) $A = \{\emptyset, \{\emptyset\}\}$ och $B = \{\emptyset\}$.

Övning 1.5. Använd mängdbyggaren för att definiera följande mängder.

(i) Mängden av jämna, positiva heltal.

(ii) Mängden av rationella tal r så att $2r$ är ett heltal.

(iii) Mängden av irrationella tal som ligger inom avstånd 1 från origo.

Övning 1.6. Använd mängdbyggaren för att definiera följande mängder.

(i) Mängden av alla kvadrattal som är större än 2.

(ii) Mängden av rationella lösningar till $x^4 + x^2 - 1 = 0$.

(iii) Mängden av rationella tal som är volymen av en kub med rationella sidor.

Övning 1.7. Ange möjlig definitionsmängd och målmängd för följande funktioner.

(i) Funktionen som ger det n:te kvadrattalet.

(ii) Funktionen som beräknar arean av triangel.

(iii) Funktionen beräknar derivatan av ett andragradspolynom.

Övning 1.8. Ange möjlig definitionsmängd och målmängd för följande funktioner.

(i) Funktionen som ger arean av cirkel med radie r.

(ii) Funktionen som ger avståndet mellan 1 och ett tal r på tallinjen.

(iii) Funktionen som ger de rationella nollställena till ett förstagradspolynom med rationella koefficienter.

Övning 1.9. Är följande funktioner eller inte? Om inte, motivera varför.

(i) $f : \mathbb{R} \to \mathbb{R}$ där
$$f(x) = \begin{cases} 1 \text{ om } x \in \mathbb{Q} \\ 0 \text{ om } x \notin \mathbb{Q}. \end{cases}$$

(ii) $f : \mathbb{N} \to \mathbb{Q}$ där $f(n) = \sqrt{n}$.

(iii) $f : \mathbb{R} \to \mathbb{R}$ så att $f(x) = 0$ med sannolikhet $1/2$ och $f(x) = 1$ med sannolikhet $1/2$.

(iv) $f : \{0\} \to \mathbb{R}$ där $f(0) = 1$ om ordet Balkong börjar på B.

Övning 1.10. Är följande funktioner eller inte? Om inte, motivera varför.

(i) $f : \mathbb{Z} \to \mathbb{N}$, där $f(n)$ är siffersumman i det vanliga (decimala) talsystemet. Obs, alla *siffror* är icke-negativa.

(ii) $f : \mathbb{R} \to \mathbb{Q}$, där $f(x) = x/2$.

(iii) $f : \mathbb{N} \to \mathbb{R}$, där $f(n) = \sqrt[n+1]{n+1}$.

(iv) $f : \mathbb{Q} \to \mathbb{Z}$, där $f(p/q) = p$.

Övning 1.11. Avgör om följande funktioner är lika eller inte? Motivera varför.

(i) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$ och $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \sqrt{x^2}$.

(ii) $f : \mathbb{Z} \to \mathbb{Q}$, $f(n) = 1/n$ och $g : \mathbb{N} \to \mathbb{Q}$, $g(m) = 1/m$.

(iii) $f : \mathbb{N} \to \mathbb{Q}$, $f(n) = n/(n+1)$ och $g : \mathbb{N} \to \mathbb{R}$, $g(z) = z/(z+1)$.

Övning 1.12. Avgör om följande funktioner är lika eller inte? Om inte, motivera varför.

(i) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 2x + 1$ och $g : \mathbb{R} \to \mathbb{R}$, $g(x) = (x+1)^2$.

(ii) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$ och $g : \mathbb{Z} \to \mathbb{Z}$, $g(x) = |x|^2$.

Övning 1.13. Vad är värdemängden i exemplen 1.5.3 och 1.5.4? Avgör i vilka av de två exemplen som f är injektiv och i vilka som f är surjektiv.

Övning 1.14. Bevisa att en strängt växande funktion, alltså en funktion med egenskapen

$$x_1 < x_2 \implies f(x_1) < f(x_2)$$

är injektiv.

Övning 1.15. Visa att A och B är disjunkta om och endast om $A \setminus B = A$.

Övning 1.16. Visa att för två mängder A, B så uppfyller operationerna $\cup, \cap, A^C$ (där A^C betecknar mängdkomplement) följande räkneregler,

$$(A \cup B)^C = A^C \cap B^C \qquad (A \cap B)^C = A^C \cup B^C.$$

Övning 1.17. Visa att följande räkneregler håller

$$A \setminus B = A \setminus (A \cap B)$$

Övning 1.18. Visa att sammansättningen av två bijektioner är en bijektion.

Övning 1.19. Visa att

$$A/\sim \quad \subset 2^A.$$

Övning 1.20. Visa att antalet element i $A \times B$ är produkten av antalet element i A och antalet element i B.

Övning 1.21. Visa att den kartesiska produkten av två delmängder är delmängd till den kartesiska produkten av grundmängderna. Alltså om $B \subset A$ och $Y \subset X$ gäller det att

$$B \times Y \subset A \times X.$$

Övning 1.22. Visa att potensmängden $2^A = \{B \mid B \subset A\}$ är ett specialfall av mängdoperationen Y^A för ett par av mängder A, Y. Gör detta genom att visa att följande funktion är en bijektion,

$$\begin{aligned} \chi :& 2^A \to \{0,1\}^A \\ & B \mapsto \chi_B. \end{aligned}$$

Här definierar vi *indikatorfunktionen av* B som

$$\begin{aligned} \chi_B :& A \to \{0,1\} \\ & a \mapsto \begin{cases} 1 \text{ om } a \in B \\ 0 \text{ om } a \notin B. \end{cases} \end{aligned} .$$

Dra slutsatsen att 2^A har $2^{|A|}$ antal element.

Övning 1.23 ($\star$)**.** Använd ett direkt bevis för att bevisa att om n är ett jämnt tal så är $n+1$ ett udda tal (detta är Sats 1.1.4).

Övning 1.24 ($\star$)**.** Använd ett direkt bevis för att bevisa att om n är udda så är n^2 udda.

Övning 1.25 ($\star$)**.** Använd ett motsägelsebevis för att bevisa att summan av ett irrationellt tal och ett rationellt tal är irrationellt.

Övning 1.26 ($\star$)**.** Använd ett motsägelsebevis för att bevisa att om $a+b \geqslant c$ så är antingen $a \geqslant c/2$ eller $b \geqslant c/2$

Övning 1.27 ($\star\star$)**.** Bevisa att om $ab = c$ så är $a \geqslant \sqrt{c}$ och $b \leqslant \sqrt{c}$, eller tvärtom.

Övning 1.28 ($\star$)**.** Bevisa att det finns två irrationella tal a och b så att a^b är rationellt. Tips: använd att $\sqrt{2}$ är irrationellt.

Övning 1.29 ($\star\star$)**.** Bevisa att alla rationella tal kan skrivas som en produkt av två irrationella tal.

Övning 1.30 ($\star$)**.** Visa följande påståenden för heltalen (du bör använda det du bevisat i ena för att bevisa nästa).

(i) Multiplikation med ett positivt tal bevarar olikheter. Alltså för $m > 0$ gäller

$$r \leqslant n \implies mr \leqslant mn.$$

(ii) Ett positivt heltal kan inte dela ett mindre positivt heltal. Alltså

$$0 < r < n \implies n \text{ delar inte } r.$$

(iii) Differensen av två heltal delbara med n är också delbar med n.

2 Modulär aritmetik

Vilken dag är det om 100000 år? Viken tid på dagen är det 5678 timmar in i framtiden? Är det ett skottår om 3000 år? Alla dessa frågor har en liknande struktur, de är system som upprepar sig efter en given mängd tid. För att besvara de här problemen behöver vi lära oss att räkna med sådana system, i ämnet modulär aritmetik, även kallat klockaritmetik.

2.1 Kongruens

Låt n vara ett heltal. Vi påminnner om att ett heltal a är delbart med n om det finns ett $d \in \mathbb{Z}$ så att $a = dn$. Det skrivs även som $n|a$ vilket läses som 'n delar a'. Summan och differensen av två tal delbara med n är också delbara med n.

Definition 2.1.1. Låt $a, b \in \mathbb{Z}$ och n vara ett positivt heltal. Vi säger att a är kongruent med b modulo n, vilket skrivs som

$$a \equiv b \mod n,$$

om n delar $a - b$.

Exempel 2.1.2. En analog klocka har 12 stycken olika timslag. Om vi väntar 5 timmar och sedan 8 timmar till, så kommer avståndet mellan timvisarens start och slutpunkt vara detsamma som om du bara väntade en timme. I klockans värld är alltså $5 + 8 = 1$, vilket kan låta absurt. Ett mer rigoröst sätt att säga det här på är att

$$5 + 8 \equiv 1 \mod 12.$$

Sats 2.1.3. *Låt $a, b, a', b' \in \mathbb{Z}$ och $n, k > 1$ vara heltal. Anta vidare att $a \equiv a'$ och $b \equiv b'$. Då gäller*

(i) $a + b \equiv a' + b' \mod n$.

(ii) $a \cdot b \equiv a' \cdot b' \mod n$.

(iii) $a^k \equiv (a')^k \mod n$.

Bevis. Vi vet att n delar $a - a'$ och $b - b'$. Då delar även n

$$(a - a') + (b - b') = (a + b) - (a' + b')$$

vilket visar (i). Talet n delar även

$$(a - a')b + (b - b')a' = a \cdot b - b' \cdot a'$$

vilket visar (ii). Sist men inte minst kan vi använda (ii) upprepade gånger och får att

$$a^k \equiv \underbrace{a \cdot a \cdot \cdots \cdot a}_{k \text{ gånger}} \equiv \underbrace{a' \cdot a' \cdots a'}_{k \text{ gånger}} \equiv (a')^k \mod n. \qquad \square$$

Vi kan använda den tidigare satsen för att göra ganska stora beräkningar väldigt fort. Vi försöker besvara frågan som ställdes i början av kapitlet, vilken veckodag är det om 100000 år?

100000 år är $10^5 \cdot 365$ dagar, och veckodagarna börjar om var sjunde dag. Vi vill alltså göra beräkningen modulo 7. Vi har

$$10^5 \cdot 365 \equiv 3^5 \cdot 1 \equiv 9 \cdot 9 \cdot 3 \equiv 2 \cdot 2 \cdot 3 \equiv 12 \equiv 5.$$

Veckodagarna har alltså gått framåt 5 dagar. Om det exempelvis var måndag skulle det alltså vara lördag om 100000 år.

2.2 $\mathbb{Z}/(n)$

Definition 2.2.1. Givet ett positivt heltal n och ett heltal k så definierar vi *principalresten* av k modulo n, skrivet $k\%n$, som

$$k \mapsto \begin{cases} 0 \text{ om } n \text{ delar } k \\ 1 \text{ om } n \text{ delar } k-1 \\ \vdots \\ n-1 \text{ om } n \text{ delar } k-(n-1) \end{cases}.$$

Alternativt så kan $k\%n$ definieras som det unika tal i mängden $\{0, 1, \ldots, n-1\}$ som uppfyller $k \equiv k\%n \mod n$. Ibland skriver vi bara $k\%$ om n är underförstått.

Exempel 2.2.2. Vi har att

$$\begin{aligned} \%2 \colon \mathbb{Z} &\to \{0,1\} \\ k &\mapsto \begin{cases} 0 \text{ om } k \text{ jämnt} \\ 1 \text{ om } k \text{ udda} \end{cases} \end{aligned}$$

vilket exempelvis ger att $17\%2 = 1$ och $100\%2 = 0$. Alternativt så skriver man $17 \equiv 1 \mod 2$ eller $100 \equiv 0 \mod 2$. Ett annat exempel är

$$\begin{aligned} \%3 \colon \mathbb{Z} &\to \{0,1,2\} \\ k &\mapsto \begin{cases} 0 \text{ om } k \text{ delbart med } 3 \\ 1 \text{ om } k-1 \text{ delbart med } 3 \\ 2 \text{ om } k-2 \text{ delbart med } 3. \end{cases} \end{aligned}$$

där vi har använt att $k-2$ är delbart med 3 om och endast om $k-2+3 = k+1$ är det. Vi kan då beräkna

$$5\%3 = 2 \qquad 10\%3 = 1 \qquad 21\%3 = 0.$$

Alternativt så skriver man $5 \equiv 2 \mod 3$, $10 \equiv 1 \mod 3$ eller $21 \equiv 0 \mod 3$.

Hjälpsats 2.2.3. *Om $m \in \{0, \ldots, n-1\}$ så gäller det att $m\%n = m$ och för två heltal $a, b \in \mathbb{Z}$ gäller*

$$a \equiv b \mod n \iff a\%n = b\%n.$$

Bevis. Det första påståendet följer direkt från faktumet att n alltid delar 0. För det andra påståendet visar vi först implikationen åt höger. Antag att n delar $(a-b)$, då gäller

$$b - a\%n = (a - (a-b)) - a\%n = \underbrace{(a - a\%n)}_{\text{delbart med } n} - \underbrace{(a-b)}_{\text{delbart med } n}.$$

Ekvationen ovan medför att $b - a\%n$ är delbart med n. Alltså har $a\%n$ den unika egenskapen som $b\%n$ har, att när man subtraherar den från b får man något delbart med n. Därmed måste $a\%n = b\%n$. Avslutningsvis så ser vi att implikationen åt höger ges av att om vi låter $a\%n = b\%n$ så gäller

$$(a-b) = (a-b) + 0 = (a-b) + (b\%n - a\%n) = \underbrace{(a - a\%n)}_{\text{delbart med } n} - \underbrace{(b - b\%n)}_{\text{delbart med } n}.$$

Alltså är $a - b$ delbart med n, vilket skulle visas. □

Hjälpsats 2.2.4. *Låt $n, k > 1$ vara heltal och $a, b \in \mathbb{Z}$. Då gäller*

(i) $(a+b)\%n \equiv a\%n + b\%n \mod n$.

(ii) $(a \cdot b)\%n \equiv a\%n \cdot b\%n \mod n$.

(iii) $a^k\%n \equiv (a\%n)^k \mod n$.

Bevis. Vi bevisar (i) och lämnar återstående identiteter som övningar. Vi vet från Sats 2.2.3 att $a\%n \equiv a \mod n$. Genom att använda Hjälpsats 2.1.3, (i), dras slutatsen att

$$a\%n + b\%n \equiv a + b \mod n.$$

Genom att återigen använda Sats 2.2.3 kan vi dra slutsatsen

$$a + b \equiv (a+b)\%n \mod n.$$ □

Vi definierar

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}.$$

Vi vill definiera en ”addition” på $\mathbb{Z}/(n)$, så att vi kan addera två element i $\mathbb{Z}/(n)$ och få ut ett nytt tal i $\mathbb{Z}/(n)$. Vi vill även på samma sätt definiera subtraktion och multiplikation i $\mathbb{Z}/(n)$.

Definition 2.2.5. Låt $a, b \in \mathbb{Z}/(n)$. Vi definierar ’$a+b$ i $\mathbb{Z}/(n)$’ som

$$(a+b)\%n,$$

’$-a$ i $\mathbb{Z}/(n) \setminus \{0\}$’ som

$$(-a)\%n = n - a,$$

’-0 i $\mathbb{Z}/(n)$’ som 0 i $\mathbb{Z}/(n)$, ’$a-b$ i $\mathbb{Z}/(n)$’ som $a + (-b)$ i $\mathbb{Z}/(n)$, och sist men inte minst låter vi ’$a \cdot b$ i $\mathbb{Z}/(n)$’ definieras som

$$(a \cdot b)\%n.$$

Eftersom vi använder samma notation för ”vanlig” addition/multiplikation och för addition/multiplikation i $\mathbb{Z}/(n)$, kommer vi att förtydliga i vilken situation additionen och multiplikationen äger rum.

Exempel 2.2.6. Om vi låter $n = 3$ är $\mathbb{Z}/(3) = \{0, 1, 2\}$. Följande tabeller representerar multiplikation och addition i den här situationen.

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

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

Exempel 2.2.7. Om vi låter $n = 4$ ser vi att -1 i $\mathbb{Z}/(4)$ är $(-1)\%n = 3$. Det här beror på att $1 + 3 = 0$ i $\mathbb{Z}/(4)$. Notera också att $3 \cdot 3 = 1$ i $\mathbb{Z}/(4)$, vilket överensstämmer med $(-1) \cdot (-1) = 1$.

Sats 2.2.8. *Låt $n > 1$ vara ett heltal, och $a, b, c \in \mathbb{Z}/(n)$. Då gäller*

(i) $a + b = b + a$.

(ii) $(a + b) + c = a + (b + c)$.

(iii) $a \cdot b = b \cdot a$.

(iv) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

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

Bevis. Vi visar (ii) och återlämnar resten till övningar. Vi vet från Hjälpsats 2.2.4 att

$$(a + b)\%n \equiv a\%n + b\%n \mod n$$

och från Hjälpsats 2.2.3 att

$$a\%n \equiv a \mod n$$

där additionen är i $\mathbb{Z}$. Alltså har vi

$$\begin{aligned}((a + b)\% + c)\% &\equiv (a + b)\% + c \\ &\equiv a\% + b\% + c\% \\ &\equiv a + (b + c)\% = (a + (b + c)\%)\% \mod n.\end{aligned}$$

Nu är $((a+b)\%+c))\%$ och $(a+(b+c)\%)\%$ två tal i $\mathbb{Z}/(n)$ som är kongruenta modulo n. Alltså är de lika. Men de är också lika med $(a + b) + c$ respektive $a + (b + c)$ i $\mathbb{Z}/(n)$. □

2.3 Division i $\mathbb{Z}/(n)$

Tre räknesätt har definierats i $\mathbb{Z}/(n)$, addition, subtraktion och multiplikation, som uppfyller liknande räkneregler som de gör över $\mathbb{Z}$. En naturlig fråga att ställa sig är om vi också kan definiera division.

Definition 2.3.1. Låt $n > 1$ vara ett heltal och låt $a \in \mathbb{Z}/(n)$. En *multiplikativ invers* till a är ett element $a^{-1} \in \mathbb{Z}/(n)$ så att

$$a \cdot a^{-1} = 1$$

i $\mathbb{Z}/(n)$.

Anmärkning 2.3.2. Om a har en multiplikativ invers, är den unik. För att visa det, låt a_1^{-1}, a_2^{-1} vara multiplikativa inverser till a. Då är

$$a_1^{-1} = a_1^{-1} \cdot (a \cdot a_2^{-1}) = (a_1^{-1} \cdot a) \cdot a_2^{-1} = a_2^{-1}.$$

Ett element som garanterat inte har en multiplikativ invers är 0, eftersom $0 \cdot a = 0$ för alla $a \in \mathbb{Z}/(n)$. Kan vi garantera att alla andra element har en invers? För ett godtyckligt n är svaret nej.

Exempel 2.3.3. I $\mathbb{Z}/(4)$ har 2 ingen multiplikativ invers, då

$$0 \cdot 2 = 0, \quad 1 \cdot 2 = 2, \quad 2 \cdot 2 = 0, \quad 3 \cdot 2 = 2,$$

i $\mathbb{Z}/(4)$, så det finns inget $a \in \mathbb{Z}/(4)$ så att $a \cdot 2 = 1$.

Det här är ett problem som går att lösa om vi bara begränsar oss till vissa specifika n. Som påminnelse är ett *primtal* ett tal $p > 1$ som bara är delbart med 1 och p. Enligt *Aritmetikens fundamentalsats* kan alla positiva heltal skrivas som produkten av primtal på ett unikt sätt. Utifrån den satsen följer Hjälpsatsen nedanför, som vi inte bevisar.

Hjälpsats 2.3.4. *Låt p vara ett primtal. Om $a, b \in \mathbb{Z}$, och $p|ab$, så gäller antingen att $p|a$ eller att $p|b$.*

Exempel 2.3.5. Satsen ovan fungerar inte längre om p inte är ett primtal. Om exempelvis $p = 4$ och $a = b = 2$, så delar p talet $ab = 4$, men $p \nmid 2 = a = b$.

Sats 2.3.6. *Alla element i $\mathbb{Z}/(p) - \{0\}$ har en multiplikativ invers om och endast om p är ett primtal.*

Bevis. Anta först att p är ett primtal. Låt $a \in \mathbb{Z}/(p) - \{0\}$, och betrakta funktionen $f : \mathbb{Z}/(p) \to \mathbb{Z}/(p)$ definierad av

$$f(x) = a \cdot x$$

där multiplikationen sker i $\mathbb{Z}/(p)$. Vi påstår att funktionen är injektiv. För att visa det, låt $x, y \in \mathbb{Z}/(p)$ så att $f(x) = f(y)$. Då är

$$a \cdot x \equiv a \cdot y \mod p$$

där multiplikationen sker i $\mathbb{Z}$. Men då delar p talet

$$ax - ay = a(x - y).$$

Enligt Hjälpsats 2.3.4 delar då p antingen a eller $x - y$. Eftersom $0 \neq a < p$, så delar p inte a. Alltså måste p dela $x - y$, och

$$x \equiv y \mod p.$$

Då $0 \leqslant x, y < p$ så är $x = y$. Alltså är f injektiv.

Eftersom f är injektiv och målmängd och definitionsmängd båda har storlek $|\mathbb{Z}/(p)| = p$, så måste f även vara surjektiv. Alltså finns det ett $b \in \mathbb{Z}/(a)$ så att $ab = f(b) = 1$, vilket skulle visas.

Om p inte är ett primtal, kan vi skriva $p = ab$ där $1 < a, b < p$. Vi påstår att a inte kan ha en invers i $\mathbb{Z}/(p)$. För att visa det, låt a^{-1} vara en sådan invers. Då gäller

$$b = b \cdot a \cdot a^{-1} = 0 \cdot a^{-1} = 0$$

i $\mathbb{Z}/(p)$. Det här är en motsägelse då $b < p$. □

Exempel 2.3.7. Säg att vi vill hitta en invers till 3 i $\mathbb{Z}/(7)$. Det enklaste sättet att hitta en invers är att testa sig fram.

$$1 \cdot 3 = 3,$$

$$2 \cdot 3 = 6,$$

$$3 \cdot 3 = 2,$$

$$4 \cdot 3 = 5,$$

$$5 \cdot 3 = 1.$$

Alltså är inversen till 3 i $\mathbb{Z}/(7)$ talet 5.

Exempel 2.3.8. Säg att vi vill lösa ekvationen

$$3x + 2 = 4$$

i $\mathbb{Z}/(7)$. Vi letar alltså efter $x \in \mathbb{Z}/(7)$ för att lösa ekvationen. Normalt sett skulle vi subtrahera 2 från båda sidor först. Eftersom $-2 = 5$ i $\mathbb{Z}/(7)$ lägger vi istället till 5 på båda sidor och får

$$3x + 2 + 5 = 4 + 5$$

$$\iff 3x = 2.$$

i $\mathbb{Z}/(7)$. Nu skulle vi vilja ”dela” båda sidor med 3. Eftersom $3^{-1} = 5$ i $\mathbb{Z}/(7)$ (se tidigare exempel) multiplicerar vi båda sidor med 5 och får

$$(5 \cdot 3)x = 5 \cdot 2$$

$$\iff x = 3.$$

I framtiden är det underförstått att alla multiplikationer och additioner sker i $\mathbb{Z}/(n)$ om inget annat nämns.

Övningar

Övning 2.1. Vad är sista siffran i 11^{34567}?

Övning 2.2. Om det är måndag idag, vilken dag är det om en miljard år

(i) exklusive skottår?

(ii) inklusive skottår?

Övning 2.3. Visa att ett tresiffrigt tal är delbart med 3 och 9 om och endast om siffersumman av talet är delbart med 3 respektive 9.

Övning 2.4. Visa att ett sexsiffrigt tal $abcdef$ är delbart med 11 om och endast om

$$a - b + c - d + e - f$$

är delbart med 11.

Övning 2.5. Beräkna följande uttryck i $\mathbb{Z}/(25)$

(i) $2 + 3$.

(ii) $16 \cdot 10$.

(iii) -13.

(iv) $1 - 24$.

(v) 10^3.

Övning 2.6. Visa att för alla $x \in \mathbb{Z}/(n)$ gäller det att $-1 \cdot x = -x$, oavsett n.

Övning 2.7. Visa att $(-1) \cdot (-1) = 1$ i $\mathbb{Z}/(n)$ oavsett n.

Övning 2.8. Beräkna multiplikativa inversen till 3 eller visa att den inte finns i

(i) $\mathbb{Z}/(4)$

(ii) $\mathbb{Z}/(5)$.

(iii) $\mathbb{Z}/(6)$.

(iv) $\mathbb{Z}/(7)$.

Övning 2.9 ($\star$)**.** Visa att multiplikativa inversen till 2 finns i $\mathbb{Z}/(n)$ om och endast om n är udda, och visa att den i det fallet är $(n + 1)/2$.

3 Vektorer och matriser

3.1 Matriser

I framtiden låter vi F vara antingen $\mathbb{R}$ eller $\mathbb{Z}/(p)$, eftersom vi kan utföra alla fyra räknesätten med båda mängder.

En $n \times m$-*matris* A över F är en rektangulär uppsättning tal i n *rader* och m *kolumner*

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}.$$

Talet a_{ij} är det tal som står på rad i och kolumn j. Här kräver vi att $a_{ij} \in F$ för alla i och j. En annan beteckning är

$$A = [a_{ij}]_{i,j=1}^{n,m}.$$

Exempel 3.1.1. Betrakta matriserna

$$A = \begin{bmatrix} 0 & 3 & 2 \\ \sqrt{2} & -3 & -6 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 1 \\ 0 & 1 \\ 2 & 0 \end{bmatrix}.$$

Här är A en 2×3 matris över $\mathbb{R}$ och B är en 3×2 matris över $\mathbb{Z}/(3)$.

Exempel 3.1.2. En matris av storlek $(n \times m)$ över F där alla tal är noll betecknas 0 och kallas för *nollmatrisen*.

Om $n = m$ kallas A en *kvadratisk* matris. Låt

$$A = [a_{ij}]_{i,j=1}^{n,m}, \quad B = [b_{ij}]_{i,j=1}^{n,m}$$

vara två $n \times m$-matris och $c \in F$. Vi definierar *summan* av två $n \times m$-matriser som

$$A + B = [a_{ij} + b_{ij}]_{i,j=1}^{n,m}$$

och *multiplikation med talet* c som

$$cA = c\,[a_{ij}]_{i,j=1}^{n,m} = [ca_{ij}]_{i,j=1}^{n,m}.$$

När vi adderar två matriser så adderar vi alltså talen på samma position och när vi multiplicerar en matris med ett tal c så multipliceras varje tal i matrisen med c.

Exempel 3.1.3. Låt

$$A = \begin{bmatrix} 0 & 3 & 2 \\ 3 & 4 & 1 \\ 0 & 1 & 3 \\ 2 & 3 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 & 0 \\ 4 & 4 & 4 \\ 2 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}$$

vara matriser över $\mathbb{Z}/(5)$. Vi har att

$$A+B=\begin{bmatrix}0&4&2\\2&3&0\\2&2&1\\2&3&4\end{bmatrix} \text{ och } 2A=\begin{bmatrix}0&1&4\\1&3&2\\0&2&1\\4&1&1\end{bmatrix}.$$

Definition 3.1.4. Låt $A=[a_{ij}]_{i,j=1}^{n,k}$ vara en $n\times k$-matris och $B=[b_{ij}]_{i,j=1}^{k,m}$ en $k\times m$-matris. *Produkten* AB definieras som den $n\times m$-matris C som på rad i och kolumn j har talet

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\ldots+a_{ik}b_{kj}=\sum_{\ell=1}^{k}a_{i\ell}b_{\ell j}. \tag{3.1}$$

Produkten AB är endast definierad om antalet kolumner i A sammanfaller med antalet rader i B. Märk att BA ej nödvändigtvis är definierad även om multiplikationen AB är definierad. Multiplikationen AA är bara definierad om A är kvadratisk. I det fallet definierar vi

$$A^n=\underbrace{A\cdot A\cdots A}_{n \text{ gånger}}.$$

Exempel 3.1.5. Låt

$$A=\begin{bmatrix}0&2\\6&1\end{bmatrix},\quad B=\begin{bmatrix}4&5\\2&3\end{bmatrix}$$

vara matriser över $\mathbb{Z}/(7)$. Från definitionen av multiplikation är

$$AB=\begin{bmatrix}0\cdot4+2\cdot2&0\cdot5+2\cdot3\\6\cdot4+1\cdot2&6\cdot5+1\cdot3\end{bmatrix}=\begin{bmatrix}4&6\\5&5\end{bmatrix}.$$

Exempel 3.1.6. Multiplikationerna

$$\begin{bmatrix}3&2\end{bmatrix}\begin{bmatrix}4\\5\end{bmatrix}=\begin{bmatrix}1\end{bmatrix} \text{ och } \begin{bmatrix}4\\5\end{bmatrix}\begin{bmatrix}3&2\end{bmatrix}=\begin{bmatrix}5&1\\1&3\end{bmatrix}$$

över $\mathbb{Z}/(7)$ visar att även om multiplikationerna AB och BA är definierade behöver de ej sammanfalla.

Sats 3.1.7. *Antag att A,B och C är matriser sådana att nedanstående multiplikationer är definierade. Matrismultiplikation uppfyller* distributiva lagen

$$A(B+C)=AB+AC,\quad (A+B)C=AC+BC$$

och associativa lagen

$$A(BC)=(AB)C.$$

Bevis. Se övning. □

Matriser som består av endast en kolumn kallas för *vektorer*. Vektorer uppfyller därför de räkneegenskaper som matriser gör. Vi definierar

$$F^n = \left\{ v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \mid v_i \in F \text{ för alla } i \right\}.$$

Mängden F^n representerar alltså alla $n \times 1$ matriser. Vi ser att den här definitionen överensstämmer med den tidigare definitionen i kapitel 1.

Exempel 3.1.8. Matrisen

$$v = \begin{bmatrix} 1/2 \\ -5 \\ 9 \end{bmatrix}$$

är en vektor i $\mathbb{R}^3$.

3.2 Inverterbarhet

För ett positivt heltal n, låt I vara den $n \times n$ kvadratiska matrisen sådan att

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Matrisen I kallas *enhetsmatrisen* och uppfyller att

$$AI = IA = A$$

för alla kvadratiska matriser A sådana att multiplikationen är definierad. Ibland används notationen I_n för att belysa att I är en $n \times n$-matris.

Definition 3.2.1. En kvadratisk matris A sägs vara *inverterbar* om det existerar en matris B sådan att

$$AB = BA = I. \tag{3.2}$$

Matrisen B kallas *inversen* till A och betecknas A^{-1}.

Inversen till A är entydig ty antag att det finns två matriser B och C sådana att ((3.2)) är uppfylld. Vi har då att $B = BI = BAC = IC = C$, så matriserna är lika.

Exempel 3.2.2. Låt A vara den inverterbara matrisen

$$A = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}$$

över $\mathbb{R}$. För att beräkna inversen till A måste vi finna en matris A^{-1} sådan att $AA^{-1} = A^{-1}A = I$. Ansätt

$$A^{-1} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$$

och lös ekvationen $AA^{-1} = I$, d.v.s.

$$\begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Vi får ekvationssystemet

$$\begin{cases} x_{11} + 2x_{21} = 0 \\ 3x_{11} + 4x_{21} = 1 \\ x_{12} + 2x_{22} = 1 \\ 3x_{12} + 4x_{22} = 0 \end{cases}$$

Om vi adderar -3 av den första ekvationen till den andra och -3 av den tredje ekvationen till den fjärde får vi

$$\begin{cases} x_{11} + 2x_{21} = 0 \\ -2x_{21} = 1 \\ x_{12} + 2x_{22} = 1 \\ -2x_{22} = -3 \end{cases} \tag{3.3}$$

Från ((3.3)) ser vi att $x_{21} = -1/2, x_{11} = 1, x_{22} = 3/2$ och $x_{12} = -2$. Alltså

$$A^{-1} = \begin{bmatrix} 1 & -2 \\ -1/2 & 3/2 \end{bmatrix}$$

Vi kan även kontrollera att $AA^{-1} = I$.

Exempel 3.2.3. Låt

$$A = \begin{bmatrix} 2 & 4 \\ 1 & 2 \end{bmatrix}$$

Vara en matris över $\mathbb{Z}/(5)$. Ansätt

$$A^{-1} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix},$$

och betrakta ekvationen $AA^{-1} = I$, d.v.s.

$$\begin{bmatrix} 2 & 4 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Vi får ekvationssystemet

$$\begin{cases} x_{11} + 2x_{21} = 0 \\ 2x_{11} + 4x_{21} = 1 \\ x_{12} + 2x_{22} = 1 \\ 2x_{12} + 4x_{22} = 0 \end{cases}$$

Om vi adderar -2 av den första ekvationen till den andra och -2 av den tredje ekvationen till den fjärde får vi

$$\begin{cases} x_{11} & + & 2x_{21} & & & = & 0 \\ & & & & 0 & = & 1 \\ & x_{12} & & + & 2x_{22} & = & 1 \\ & & & & 0 & = & -2 \end{cases}$$

Här ser vi att ekvationssystemet är olösbart. Alltså saknar matrisen A invers.

Anmärkning 3.2.4. Det visar sig att för två kvadratiska matriser A, B så kommer $AB = I$ om och endast om $BA = 0$.

3.3 Transponering av matriser

Definition 3.3.1. Låt $A = [a_{ij}]_{i,j=1}^{n,m}$. Den *transponerade* matrisen A^T till A definieras som $A^T = [a_{ji}]_{j,i=1}^{m,n}$, eller med andra ord, matriser man får om vi reflekterar A i huvuddiagonalen.

Exempel 3.3.2. Låt

$$A = \begin{bmatrix} 2 & 3 \\ 11 & 9 \\ 0 & 1 \end{bmatrix}$$

vara en matris över $\mathbb{Z}/(13)$. Vi har då att

$$A^T = \begin{bmatrix} 2 & 11 & 0 \\ 3 & 9 & 1 \end{bmatrix}.$$

Antag att A är en $n \times m$-matris och att B är en $m \times n$-matris. Av formel ((3.1)) följer att på rad i och kolumn j i $n \times p$-matrisen AB finns elementet $c_{ij} := a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj}$. Därmed har vi att talet på rad i och kolumn j i matrisen $(AB)^T$ är c_{ji}.

Av formel ((3.1)) har vi att talet d_{ij} på rad i och kolumn j i matrisen B^TA^T är

$$\begin{aligned} d_{ij} &= b_{1i}a_{j1} + b_{2i}a_{j2} + \cdots + b_{mi}a_{jm} \\ &= a_{j1}b_{1i} + a_{j2}b_{2i} + \cdots + a_{jm}b_{mi} = c_{ji}. \end{aligned}$$

Alltså är

$$(AB)^T = B^TA^T.$$

Antag nu att A är inverterbar. Då följer att

$$\left(A^{-1}\right)^T = \left(A^T\right)^{-1},$$

eftersom $A^T(A^{-1})^T = (A^{-1}A)^T = I^T = I$, vilket visar att $\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$.

3.4 Skalärprodukt

Definition 3.4.1. Låt $u, v \in F^n$. Vi definierar *skalärprodukten* av u och v som det reella talet $\langle u, v\rangle = u^T v$.

Vi säger att två vektorer u och v är *ortogonala* om $\langle u, v\rangle = 0$.

Exempel 3.4.2. Låt $u = \begin{bmatrix}1\\0\\1\end{bmatrix}$ och $v = \begin{bmatrix}0\\0\\1\end{bmatrix}$ vara vektorer över $\mathbb{Z}/(2)$. Då följer att

$$\langle u, v\rangle = u^T v = \begin{bmatrix}1 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\0\\1\end{bmatrix} = 1\cdot 0 + 0\cdot 0 + 1\cdot 1 = 1.$$

Anmärkning 3.4.3. Säg att $F = \mathbb{R}$. Låt $u = \begin{bmatrix}u_1\\u_2\\\vdots\\u_n\end{bmatrix} \in \mathbb{R}^n$. Vi definierar *längden* av u som

$$\|u\| = \sqrt{\langle u, u\rangle} = \sqrt{u_1^2 + u_2^2 + \cdots u_n^2}.$$

Det här är väldefinierat eftersom $u_1^2 + u_2^2 + \cdots u_n^2 \geqslant 0$. Notera att $|u| = 0 \iff \langle u, u\rangle = 0 \iff u = 0$. Alltså är en icke-noll vektor aldrig ortogonal mot sig själv. Det här gäller inte över till exempel $\mathbb{Z}/(2)$ eftersom

$$\left\langle \begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix} \right\rangle = 1\cdot 1 + 1\cdot 1 = 0.$$

Definition 3.4.4. En matris A kallas symmetrisk om $A = A^T$.

För en symmetrisk matris gäller att $\langle Au, v\rangle = (Au)^T v = u^T A^T v = u^T Av = \langle u, Av\rangle$.

Övningar

Övning 3.1. Beräkna $A + B$ där och sA där $s = 3$ och

$$A = \begin{bmatrix}2 & 0 & 7\\12 & 2 & 0\end{bmatrix}, B = \begin{bmatrix}1 & 0 & 8\\0 & 1 & 11\end{bmatrix},$$

i $\mathbb{Z}/(13)$.

Övning 3.2. Beräkna AB där

$$A = \begin{bmatrix}3 & 4 & 1\\0 & 5 & 2\end{bmatrix}, B = \begin{bmatrix}3 & 4\\0 & 5\\2 & 2\end{bmatrix},$$

i $\mathbb{Z}/(7)$.

Övning 3.3. Bevisa formel (3.1.7) för 2×2-matriser.

Övning 3.4. Beräkna A^2, A^3 och A^4 för matrisen

$$A = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

över $\mathbb{R}$.

Övning 3.5. Låt $u = \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix}^T$ och $v = \begin{bmatrix} 1 \\ -4 \\ -3 \end{bmatrix}^T$ vara vektorer över $\mathbb{R}$. Beräkna $\|u\|$, $\|v\|^2$ och $\langle u, v \rangle$.

Övning 3.6. Bevisa att inversen till matrisen

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

i fallet $ad - bc \neq 0$ är

$$\frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Övning 3.7. Bevisa att om $ab - cd = 0$ så är matrisen

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

inte inverterbar.

Övning 3.8. Visa att om A är en kvadratisk matris sådan att $A^k = 0$, så är $I - A$ inverterbar med inversen $I + A + A^2 + \ldots + A^{k-1}$.

4 Delrum, baser och dimensioner

4.1 Mer om vektorer

I förra kapitlet definierade vi en vektor som en $n \times 1$ matris för $n \geqslant 1$. Som förut låter vi F stå för $\mathbb{R}$ eller $\mathbb{Z}/(p)$ för något primtal p. Mängden av alla $n \times 1$ vektorer över F noterade vi som F^n. En sådan mängd ska vi kalla för ett *vektorrum*. Vi ska nu studera vektorer i mer detalj.

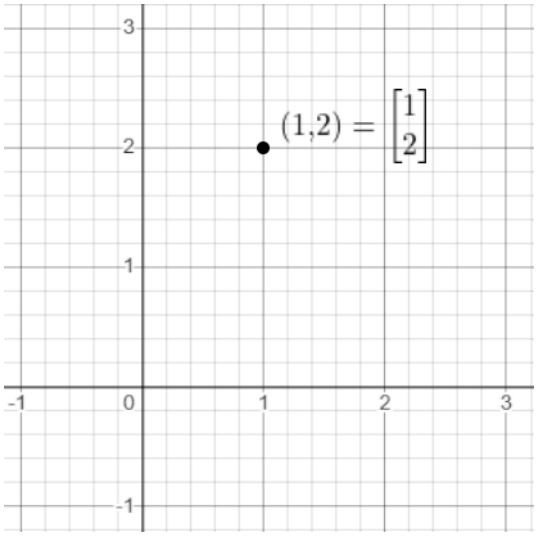
För att skriva vektorer lite mer kompakt kommer vi introducerar vi notationen

$$(a, b, c, d, \dots) = \begin{bmatrix} a \\ b \\ c \\ d \\ \vdots \end{bmatrix}.$$

Exempel 4.1.1. Låt $F = \mathbb{R}$ och $n = 2$. En vektor $v \in F^n = \mathbb{R}^2$ är då på formen

$$(x, y) = \begin{bmatrix} x \\ y \end{bmatrix}$$

där $x, y \in \mathbb{R}$. Dessa vektorer kan nu användas för att beskriva det två dimensionella talplanet.



Figur 4.1: Punkten med x-koordinat 1 och y-koordinat 2 kan beskrivas som vektorn $(1, 2) \in \mathbb{R}^2$.

Precis som matriser kan vektorer adderas med varandra samt multipliceras med element i F. Om $\{v_1, \dots, v_k\} \subset F^n$ är en ändlig mängd vektorer säger vi att en vektor på formen

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$$

för några koefficienter $a_1, a_2, \dots, a_k \in F$ är en *linjärkombination* av $v_1, v_2, \dots, v_k$.

Givet en mängd vektorer $D \subset F^n$ så definierar vi det *linjära höljet* av D, skrivet spann(D), som

$$\begin{aligned}\text{spann}(D) = \{w \in F^n \mid w = a_1v_1 + \cdots + a_kv_k,\\ \text{där } a_1, \ldots, a_k \in F, v_1, \ldots, v_k \in D \text{ och } k \in \mathbb{N}\}.\end{aligned}$$

spann(D) är därmed alla vektorer vi kan få genom att ta linjärkombinationer av vektorer i D.

Eftersom linjärkombinationer av linjärkombinationer fortfarande är linjärkombinationer kommer

$$\text{spann}(D) = \text{spann}(\text{spann}(D))$$

för alla mängder av vektorer D. Mängder $D \subset F^n$ vars linjära hölje är mängden D självt kallar vi för *delrum*. Vi noterar att även vektorrum som F^n räknas som delrum till sig själv.

4.2 Baser

En mängd vektorer $S = \{v_1, \ldots, v_k\}$ sägs vara *linjärt oberoende* om

$$a_1v_1 + a_2v_2 + \cdots + a_kv_k = 0$$

meför att $a_1 = a_2 = \cdots = 0$. En mängd vektorer som inte är linjärt oberoende sägs vara linjärt beroende.

Definition 4.2.1. Låt V vara ett delrum till något vektorrum F^m. En ändlig mängd vektorer $B \subset V$ sägs vara en bas till V om

(i) vektorerna i B är linjärt oberoende,

(ii) $V = \text{spann}(B)$.

Nästa sats ger en anledning till varför baser är viktiga.

Sats 4.2.2. *Låt B vara en bas till ett delrum V. Då kan varje element i v som en linjärkombination av vektorerna i basen på exakt ett sätt.*

Bevis. Att $V = \text{spann}(B)$ meför att varje vektor i V går att uttrycka som en linjärkombination av vektorerna i B. Antag nu att en vektor v kunde uttryckas som två linjärkombinationer

$$\begin{aligned}v &= a_1v_1 + \cdots + a_kv_k\\ v &= b_1v_1 + \cdots + b_kv_k\end{aligned}$$

där $B = \{v_1, \ldots, v_k\}$ och $a_1, \ldots, a_k, b_1, \ldots, b_k$ är element i F. Subtraherar vi de två ekvationerna får vi att

$$0 = (a_1 - b_1)v_1 + \cdots + (a_k - b_k)v_k$$

men $v_1, \ldots, v_k$ är linjärt oberoende så $a_1 = b_1, \ldots, a_k = b_k$. □

Följdsats 4.2.3. *Låt $F = \mathbb{Z}/(p)$ och låt B vara en mängd linjärt oberoende vektorer. Då är*

$$|\operatorname{spann} B| = p^{|B|}$$

Bevis. Eftersom varje uppsättning koefficienter $a_1, \ldots, a_m \in \mathbb{Z}/(p)$ motsvarar precis ett element i $\operatorname{spann} B$ när vi tar den linjärkombinationen

$$a_1 v_1 + \cdots + a_m v_m$$

kan vi istället räkna antalet uppsättningar koefficienter. Eftersom $\mathbb{Z}/(p)$ innehåller p element kan varje koefficient anta p olika värden och vi får då ett total antal av p^m uppsättningar koefficienter. □

Exempel 4.2.4. Låt oss visa att $B = \{(1,2,1),(2,1,1),(1,1,2)\} \subset (\mathbb{Z}/(3))^3$ är en bas till $\operatorname{spann}(B)$. Vi ska därmed visa att vektorerna är linjärt oberoende. Om vi har att

$$a(1,2,1) + b(2,1,1) + c(1,1,2) = 0$$

medför detta att

$$\text{(i)} \quad a + 2b + c = 0,$$

$$\text{(ii)} \quad 2a + b + c = 0,$$

$$\text{(iii)} \quad a + b + 2c = 0.$$

Betraktar vi nu $(i) + (ii)$, $(ii) + (iii)$ och $(iii) + (ii)$ ser vi att $a = b = c = 0$, så B är en bas.

Sats 4.2.5. *Låt $v_1, \ldots, v_n \in F^m$ där $n > m$. Då är vektorerna $v_1, \ldots, v_n$ linjärt beroende.*

Bevis. Antag först att $F = \mathbb{R}$. Ekvationssystemet

$$a_1 v_1 + \cdots + a_n v_n = 0$$

består av m ekvationer med n obekanta variabler. Då ekvationssystemet har fler obekanta variabler än ekvationer finns det oändligt många nollskilda lösningar.

I annat fall är $F = \mathbb{Z}/(p)$ för något primtal p. Då kommer $F^m = (\mathbb{Z}/(p))^m$ innehålla p^m element. Om $v_1, \ldots, v_n$ skulle vara linjärt oberoende hade de bildat en bas för $\operatorname{spann}\{v_1, \ldots, v_n\} \subset (\mathbb{Z}/(p))^m$. Enligt Följdsats 4.2.3 skulle dock detta innebära att $|\operatorname{spann}\{v_1, \ldots, v_n\}| = p^n > p^m$ vilket motsäger att $v_1, \ldots, v_n$ är linjärt oberoende. □

Vi kan nu visa att varje delrum har en bas.

Sats 4.2.6. *Låt $0 \neq V \subset F^n$ vara ett delrum. Då har V en bas. Dessutom gäller det att om $v_1, \ldots, v_k \in V$ är linjärt oberoende vektorer så finns det en bas som innehåller dessa vektorer.*

Bevis. Vi noterar att första delen av satsen följer av andra delen med $k = 0$. Ifall $k = 0$ låt v_1 vara en godtycklig nollskild vektor i V. Vi har då att v_1 är linjärt oberoende då

$$a_1 v_1 = 0$$

meför att $a_1 = 0$. Antag nu att $v_1, \ldots, v_{m-1}$ är linjärt oberoende vektorer i V. Om de är en bas till V är vi klara, annars väljer vi $v_m \in V \setminus \text{spann}\{v_1, \ldots, v_{m-1}\}$. Det är nu lätt att se att $v_1, \ldots, v_m$ är linjärt oberoende. Det går därmed att utöka mängden så länge vi inte har en bas. Eftersom vi kan ha som mest n linjärt oberoende vektorer vet vi att processen måste avslutas. □

Vi visar nu en förstärkning av Sats 4.2.5.

Sats 4.2.7. *Låt B vara en bas för ett delrum $V \subset F^n$. Om B har m vektorer så kommer alla uppsättningar av n vektorer $w_1, \ldots, w_n \in V$ vara linjärt beroende om $n > m$.*

Beviset lämnas som en övning.

Vi är nu redo att visa att alla baser är av samma storlek.

Följdsats 4.2.8. *Låt B, B' vara två baser till ett delrum $V \subset F^n$. Då är $|B| = |B'|$.*

Bevis. Ifall $|B'| > |B|$ ger Sats 4.2.7 att B' måste vara linjärt beroende. Men B' är en bas. Därmed kan inte $|B'|$ vara större än $|B|$. Samma argument med B istället för B' ger att $|B|$ inte kan vara större än $|B'|$. Därmed är $|B| = |B'|$. □

Antalet vektorer i basen till ett delrum V sägs vara *dimensionen* av delrummet. Dimensionen av ett delrum V skriver vi $\dim(V)$.

Exempel 4.2.9. Vi återkommer till vektorrummet $\mathbb{R}^2$. Det linjära höljet till mängden $\{(1,0),(0,1)\} \subset \mathbb{R}^2$ blir hela $\mathbb{R}^2$ då varje vektor $(x,y) \in \mathbb{R}^2$ kan skrivas som

$$\begin{bmatrix} x \\ y \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Det är också lätt att se att mängden är en bas så vi kan konstatera att $\mathbb{R}^2$ har dimension 2.

Några speciellt viktiga vektorer är *enhetsvektorerna* $e_k^n \in F_p^n$. De definieras som

$$e_k^n = (0, \ldots, 0, 1, 0, \ldots, 0) \in F^n$$
$$\uparrow$$
$$\text{i position k.}$$

Exempelvis är $e_1^3 = (1,0,0)$, $e_2^3 = (0,1,0)$ och $e_3^3 = (0,0,1)$.

Sats 4.2.10. *Mängden $\{e_k^n \mid 1 \leqslant k \leqslant n\} \subset F^n$ är en bas till F^n.*

Bevis. Givet en vektor $v = (v_1, \ldots, v_n) \in F^n$ kan vi skriva

$$v = v_1 e_1 + \cdots + v_n e_n$$

så spann $\{e_k^n \mid 1 \leqslant k \leqslant n\} = F^m$. Ifall

$$0 = a_1 e_1 + \cdots + a_n e_n$$

för några koefficienter $a_1, \ldots, a_n \in F$ ser vi att

$$0 = (a_1, a_2, \ldots, a_n)$$

så $a_1, \ldots, a_n = 0$ vilket meför att $\{e_k^n \mid 1 \leqslant k \leqslant n\}$ är linjärt oberoende. Därmed är $\{e_k^n \mid 1 \leqslant k \leqslant n\}$ en bas till F^n. □

Anmärkning 4.2.11. Sats 4.2.10 medför att vektorrummet F^n har dimension n.

Vi visar även att om en mängd vektorer är linjärt beroende så kommer en delmängd av dem vara en bas.

Hjälpsats 4.2.12. *Låt $D = \{v_1, \ldots, v_k\}$ vara en mängd av linjärt beroende vektorer. Då finns det en delmängd $D' \subsetneq D$ med egenskapen att* spann $D' =$ spann D.

Bevis. Om $v_1, \ldots, v_k$ är linjärt beroende så kan vi skriva

$$a_1 v_1 + \cdots + a_k v_k = 0$$

för några koefficienter $a_1, \ldots, a_k \in F$ där åtminstone något $a_j \neq 0$. Vi kan nu ta och skriva

$$v_j = a_j^{-1}(-a_1 v_1 - \cdots - a_{j-1} v_{j-1} - a_{j+1} v_{j+1} - \cdots - a_k v_k)$$

vilket medför att

$$v_j \in \text{spann}\, D \setminus \{v_j\}$$

alltså är spann$(D \setminus \{v_j\}) =$ spann(D). Sätter vi $D' = D$ är vi klara. □

Sats 4.2.13. *Om det linjära höljet av en mängd vektorer D är ett delrum V,* spann$(D) = V$*, gäller det att det finns en delmängd $B \subset V$ som är en bas till D. Om vektorerna i D är linjärt beroende kommer $B \subsetneq D$.*

Bevis. Om D är linjärt oberoende är vi klara. Annars kan vi upprepa Hjälpsats 4.2.12 tills vi får en mängd som är linjärt oberoende och har samma linjära hölje. Detta måste till slut ske då en mängd av bara en (nollskild) vektor automatiskt är linjärt oberoende. □

4.3 Matriser som funktioner

Låt M vara en $n \times m$ matris. I det föregående kapitlet såg vi att om vi vill multiplicera M med en matris A för att bilda produkten MA är det nödvändigt att A är en $m \times k$ matris för något $k \in \mathbb{N}$. Den resulterade matrisen MA är då en $m \times k$ matris. Speciellt om A är en vektor ser vi att även produkten MA kommer vara en vektor. Detta låter oss se matriser även som funktioner från ett rum av vektorer till ett annat.

Definition 4.3.1. Låt M vara en $n \times m$ matris över F. Vi definierar M som en funktion $M : F^m \to F^n$ genom att sätta

$$M(v) = Mv$$

för alla $v \in F^m$.

Nästa sats motiverar vad matrismultiplikation faktiskt innebär.

Sats 4.3.2. *Låt A vara en $n \times k$ matris och B vara en $k \times m$ matris. Då är*

$$A \circ B = AB.$$

Bevis. Låt $v \in F^m$. Vi vill visa att $(A \circ B)v = (AB)v$. Vi har att

$$(A \circ B)v = (A \circ B) \circ v = A \circ (B \circ v) = A \circ (Bv) = A(Bv) = (AB)v$$

där $A(Bv)$ står för matrismultiplikation och inte funktionskomposition. □

Vi kan även relatera linjära höljen med matriser.

Sats 4.3.3. *Låt $M : F^m \to F^n$ vara en $n \times m$ matris. Då är bilden $M(F^m) = \text{spann}\{M_1, \ldots, M_m\}$ där*

$$M = \begin{bmatrix} | & & | \\ M_1 & \cdots & M_m \\ | & & | \end{bmatrix}.$$

Bevis. Multiplicerar vi M med en vektor $v = (v_1, \ldots, v_m)$ får vi

$$Mv = v_1 M_1 + \cdots + v_m M_m$$

så Mv är en linjärkombination av kolumnerna hos M. Vi kan därmed bilda alla linjärkombinationer genom att välja olika vektorer v. □

Bilden $M(F^m)$ kallas för *värderummet* av M. Sats 4.3.3 visar att värderummet är ett delrum av F^n. En annan viktig mängd är *nollrummet* som definieras som $M^{-1}(\{0\})$. Det vill säga, mängden av de vektorer som M avbildar till 0. Det är lätt att se att även nollrummet är ett delrum. Vi kommer skriva värderummet som $V(M)$ och nollrummet som $N(M)$.

Sats 4.3.4 (Dimensionssatsen)**.** *Låt M vara en $n \times m$ matris. Då är*

$$\dim N(M) + \dim V(M) = m$$

Bevis. Låt $w_1, \ldots, w_k \in F^m$ vara en bas för $N(M)$. Sats 4.2.6 ger att det finns vektorer $v_1, \ldots, v_{m-k} \in F^m$ som tillsammans med $w_1, \ldots, w_k$ bildar en bas för F^m. Givet någon vektor $v \in V(M)$ så finns det enligt definition en vektor $u \in F^m$ så att $Mu = v$. Vi kan nu skriva

$$u = a_1 w_1 + \cdots + a_k w_k + b_1 v_1 + \cdots + b_{m-k} v_{m-k}.$$

Därmed är

$$\begin{aligned} v = Mu &= a_1 M w_1 + \cdots + a_k M w_k + b_1 M v_1 + \cdots + b_{m-k} M v_{m-k} \\ &= b_1 M v_1 + \cdots + b_{m-k} M v_{m-k}. \end{aligned}$$

Eftersom v var godtycklig innebär detta att $\text{spann}\{Mv_1, \ldots, Mv_{m-k}\} = V(M)$. Det återstår att visa att $Mv_1, \ldots, Mv_{m-k}$ är linjärt oberoende. Om vi har att

$$0 = c_1 M v_1, \ldots, c_{m-k} M v_{m-k} = M(c_1 v_1, \ldots, c_{m-k} v_{m-k})$$

för några konstanter $c_1, \ldots, c_{m-k} \in F$ innebär det att $c_1 v_1 + \cdots + c_{m-k} v_{m-k} \in N(M)$. Detta ger i sin tur att

$$c_1 v_1 + \cdots + c_{m-k} v_{m-k} = d_1 w_1 + \cdots + d_k w_k$$

för några konstanter $d_1, \ldots, d_k \in F$. Men $\{v_1, \ldots, v_{m-k}, w_1, \ldots, w_k\}$ är en bas. Därmed måste $c_1 = \cdots = c_{m-k} = d_1 = \cdots = d_k = 0$. □

I nästa sats visar vi att transponatet av en matris har samma dimension på värderummet.

Sats 4.3.5. *Låt* $M = \begin{bmatrix} | & & | \\ M_1 & \cdots & M_m \\ | & & | \end{bmatrix}$ *vara en* $n \times m$ *matris. Då är*

$$\dim V(M) = \dim V(M^T).$$

Bevis. Låt $k = \dim V(M)$ och låt $\{w_1, \ldots w_k\}$ vara en bas till $V(M)$. Då kan varje kolumn av M skrivas som en linjärkombination av $w_1, \ldots, w_k$. Ta nu och bilda $n \times k$ matrisen

$$W = \begin{bmatrix} | & & | \\ w_1 & \cdots & w_k \\ | & & | \end{bmatrix}.$$

Från Sats 4.3.3 har vi att linjärkombinationerna av kolumnerna av V överensstämmer med värderummet av W. Eftersom kolumnerna av W är en bas till det linjära höljet av kolumnerna av M kan vi för varje $1 \leqslant i \leqslant m$ finna någon vektor $c_i \in F^k$ så att

$$M_i = W c_i.$$

Bildar vi nu $k \times m$ matrisen

$$C = \begin{bmatrix} | & & | \\ c_1 & \cdots & c_m \\ | & & | \end{bmatrix}$$

kan vi skriva

$$M = WC.$$

Transponatet uppfyller då att

$$M^T = C^T W^T$$

så

$$V(M^T) = V(C^T W^T) = C^T(W^T(F^n)) \subset C^T(F^k)$$

men C^T är en $m \times k$ matris så har som mest k linjärt oberoende kolumner. Därmed är $\dim C^T(F^k) \leqslant k$ vilket medför att

$$\dim V(M^T) \leqslant \dim V(M).$$

Detta gäller för alla matriser M. Särskilt givet en matris M gäller det även för M^T så

$$\dim V(M^{T^T}) = \dim V(M) \leqslant \dim V(M^T)$$

så $\dim V(M) = \dim V(M^T)$. □

Sats 4.3.6. *Låt M vara en $n \times m$ matris. Då är följande påståenden ekvivalenta.*

(i) *M är injektiv*

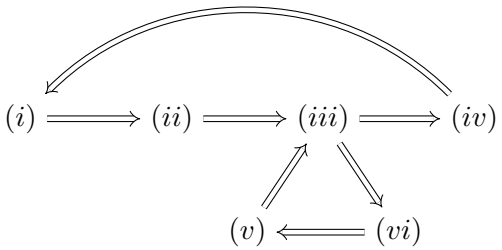
(ii) $N(M) = \{0\}$

(iii) $\dim V(M) = m$

(iv) *Kolumnerna av M är linjärt oberoende*

(v) *M har m linjärt oberoende rader*

(vi) *M^T är surjektiv*



Figur 4.2: Hur vi bevisar Sats 4.3.6

Bevis. $(i) \implies (ii)$:
Om M är injektiv har vi att $Mv = 0$ meför att $v = 0$ så $N(M) = \{0\}$.

$(ii) \implies (iii)$:
Om $N(M) = \{0\}$ följer det att $\dim N(M) = 0$ så enligt Dimensionssatsen

4.3.4 gäller det att $\dim V(M) = m - \dim N(m) = m$.

$(iii) \implies (iv)$:
Enligt sats 4.3.3 är det linjära höljet av kolumnerna $V(M)$. Om kolumnerna är linjärt beroende kan vi enligt Sats 4.2.13 hitta en äkta delmängd av kolumnerna som bildar en bas till $V(M)$. Men eftersom det finns m vektorer skulle då $\dim V(M)$ vara mindre än m, därför måste kolumnerna vara linjärt oberoende.

$(iv) \implies (i)$:
Antag att $Mv = Mw$ för några vektorer $v, w \in F^m$ och att kolumnerna är linjärt oberoende. Vi vill visa att $v = w$. Sätt $u = v - w$, då har vi att $Mu = 0$ och vi vill visa att $u = 0$. Låt $u = (u_1, \ldots, u_n)$ och

$$M = \begin{bmatrix} | & & | \\ M_1 & \cdots & M_m, \\ | & & | \end{bmatrix}.$$

Då är

$$M_1 u_1 + \cdots + M_m u_m = 0$$

men kolumnerna är linjärt oberoende så $u_1 = \cdots = u_m = 0$.

$(iii) \implies (vi)$:
Antag att $\dim V(M) = m$. Vi har att $M^T : F^n \to F^m$ och vi vill visa att $V(M^T) = F^m$. Enligt Sats 4.3.5 är $\dim V(M^T) = m$. Låt B vara en bas av m element till $V(M^T)$. Enligt sats 4.2.6 kan vi skapa en bas till F^m med elementen i B. Men om det behövs fler element än så skulle $\dim F^m > m$. Därmed måste B också vara en bas till F^n vilket innebär att $V(M^T) = F^m$.

$(vi) \implies (v)$:
Vi antar att M^T är surjektiv så $V(M^T) = F^m$. Vi vill visa att M har m linjärt oberoende rader. Vilket blir ekvivalent med att M^T har m linjärt oberoende kolumner. Enligt Sats 4.3.3 kommer det linjära höljet av kolumnerna av M^T vara F^m. Enligt Sats 4.2.13 kommer en delmängd av dessa vara en bas till F^m. Då F^m har dimension m kommer därför m stycken kolumner av M^T vara linjärt oberoende.

$(v) \implies (iii)$:
Om M har m linjärt oberoende rader kommer M^T ha m linjärt oberoende kolumner. Då $M^T : F^n \to F^m$ är $\dim V(M^T) \leqslant m$. Enligt Sats 4.3.3 kommer det linjära höljet av kolumnerna vara $V(M^T)$. Men enligt Sats 4.2.6 kan vi skapa en bas till $V(M^T)$ med de m linjärt oberoende kolumnerna. Om vi behöver fler vektorer så skulle $\dim V(M^T) > m$. Därmed är $\dim V(M^T) = m$. Enligt Sats 4.3.5 är då $\dim V(M) = m$. □

Följdsats 4.3.7. *Låt M vara en $n \times n$ matris. Då är följande påståenden ekvivalenta*

(i) *M är inverterbar,*

(ii) *M är bijektiv,*

(iii) *M är injektiv,*

(iv) *M är surjektiv,*

(v) *Kolumnerna av M är linjärt oberoende,*

(vi) *Raderna av M är linjärt oberoende.*

Vi lämnar beviset till en övning.

Övningar

Övning 4.1. Avgör vilka av följande mängder av vektorer är linärt oberoende

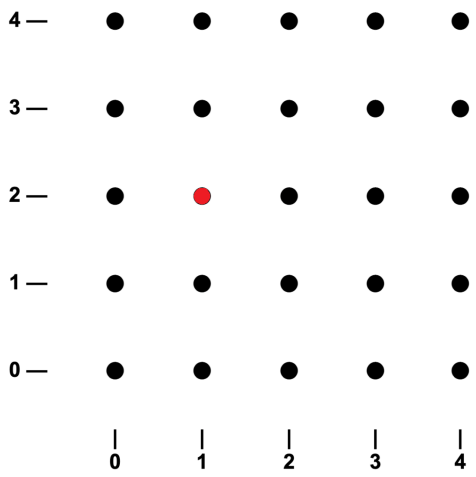
(i) $\{(1,2,3),(3,2,1),(1,0,0)\} \subset \mathbb{R}^3$

(ii) $\{(1,2,3),(3,2,1),(1,0,0)\} \subset \mathbb{Z}/(4)^3$

(iii) $\{(0,0,0,0,0),(1,0,1,2,1),(3,2,1,3,4,5),(\pi,\pi,2,3,77)\} \subset \mathbb{R}^5$

(iv) $\{(1,1,0,0),(1,1,1,0),(1,1,1,1)\} \subset \mathbb{Z}/(4)^4$

Övning 4.2. Bilden visar vektorrummet $(\mathbb{Z}/(5))^2$. Vektorn $(1,2)$ är markerad i rött. Markera de punkter som ingår i det linjära höljet av $(2,3)$.



Övning 4.3. Låt $A, B \subset F^n$ vara mängder av vektorer. Är följande påståenden sanna eller falska? Varför:

(i) $\text{spann}(A \cap B) = \text{spann}(A) \cap \text{spann}(B)$,

(ii) $\text{spann}(A \cup B) = \text{spann}(A) \cup \text{spann}(B)$,

(iii) $A \cap B$ är ett delrum om A, B är delrum.

Övning 4.4. Låt

$$D = \{(x, y, z) \in (\mathbb{Z}/(2))^3 \mid x + y + z = 0\}$$

Finn 4 olika vektorer $v_1, v_2, v_3, v_4 \in (\mathbb{Z}/(2))^3$ vars linjära hölje är D.

Övning 4.5 ($\star$)**.** Låt V, W vara delrum av samma vektorrum och definiera

$$V + W = \{v + w \mid v \in V, w \in W\}.$$

Visa att $V + W$ också är ett delrum.

Övning 4.6. Låt V vara ett delrum. Anta att vektorerna $v_1, \ldots, v_n \in V$ respektive vektorerna $w_1, \ldots, w_n \in V$ är linjärt oberoende. Bevisa eller motbevisa: $v_1 + w_1, \ldots, v_n + w_n$ är linjärt oberoende.

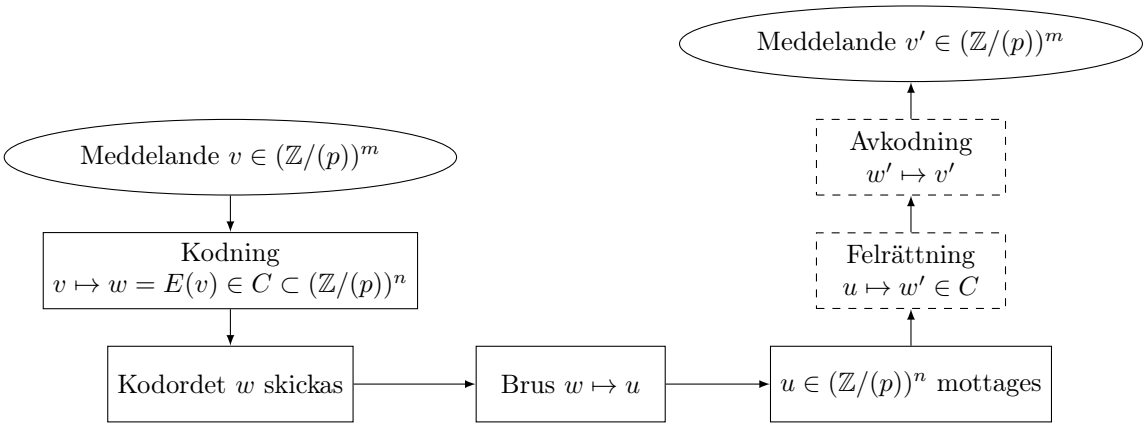
Övning 4.7. Visa att för alla matriser M är nollrummet $V(M)$ ett delrum.

Övning 4.8 ($\star$)**.** Finn alla vektorrum med exakt en bas.

Övning 4.9 ($\star$)**.** Givet två delrum $A \subset B \subset F^n$, visa att $\dim A \leqslant \dim B$ och att om $\dim A = \dim B$ måste $A = B$. Var i Sats 4.3.5 och Sats 4.3.6 använde vi oss av detta?

Övning 4.10 ($\star\star\star$)**.** Bevisa följdsats 4.3.7.

5 Felrättande koder



Figur 5.1: Felrättningsprocessen. Om $v = v'$ har vi lyckats rätta felen.

Låt oss säga att Alice vill skicka meddelandet 'matte är kul' till Bob. Vi ska undersöka hur Alice och Bob kan göra för att Bob ska kunna upptäcka och rätta till fel som kan uppkomma när meddelandet skickas på grund av exempelvis brus.

Vi antar nu att felet ändrar en bokstav till en annan, så när Bob får meddelandet kanske det står 'matte är ful'. För att undvika detta kan Alice istället skicka meddelandet 'matte är kulmatte är kul'. Om Bob nu får meddelandet 'matte är kulmatte är ful' kan han lista ut att ett fel har inträffat och ifall Alice hade upprepat det tre gånger så kan Bob även lista ut vilket det ursprungliga meddelandet var.

För att angripa problemet matematiskt väljer vi att representera meddelanden som vektorer. För att göra detta behöver vi omvandla alla tecken i meddelandet till ett tal. Exempelvis kan vi ta

$$
\begin{aligned}
&\text{' '} \mapsto 0\\
&\text{'a'} \mapsto 1\\
&\text{'b'} \mapsto 2\\
&\vdots\\
&\text{'ö'} \mapsto 29
\end{aligned}
$$

så meddelandet 'matte är kul' representerar vi som

$$\begin{bmatrix} 13 \\ 1 \\ 20 \\ 20 \\ 5 \\ 0 \\ 28 \\ 18 \\ 0 \\ 11 \\ 21 \\ 12 \end{bmatrix}$$

Ett annat alternativ är att vi först skriver om meddelandet i morsekod och därefter representerar meddelandet som en vektor över $\mathbb{Z}_2$. Om vi har ett meddelande som är väldigt långt kan vi alltid dela upp det i mindre delar och göra felrättning på varje del för sig.

Vi kommer nu mer anta att meddelandet vi vill skicka är en vektor över $\mathbb{Z}/(p)$ (där p är ett primtal) och är av längd m. Det vill säga är ett element i $(\mathbb{Z}/(p))^m$. I kontexten kommer vi kalla $\mathbb{Z}/(p)$ för ett *alfabet*, ett element i $\mathbb{Z}/(p)$ för en *bokstav*, ett element i $(\mathbb{Z}/(p))^m$ för ett *ord* och m för *blocklängden*. För att göra ordet robust mot fel så använder vi en *kodningsfunktion*. Kodningsfunktionen är en funktion

$$E : (\mathbb{Z}/(p))^m \to (\mathbb{Z}/(p))^n$$

för något $n > m$. I exemplet ovan kan vi ta $p = 31$, $m = 9$ och $n = 18$ där funktionen E tar vårt ord och upprepar det två gånger.

Det är viktigt att kodningsfunktionen E är injektiv så att information inte förloras. Mängden $E((\mathbb{Z}/(p))^m)$ kallar vi för en *kod*. Elementen i en kod kallar vi för *kodord* och n kallar vi för *kodordslängden*.

För att mäta hur stora fel som uppkommer introducerar vi *Hammingavståndet*. Hammingavståndet mellan två vektorer v, w ger antalet positioner som de skiljer sig åt. Vi betecknar Hammingavståndet med d som då definieras som att

$$d((v_1, \ldots, v_n), (w_1, \ldots, w_n)) = |\{i \mid v_i \neq w_i\}|$$

för alla $v = (v_1, \ldots, v_n) \in (\mathbb{Z}/(p))^n$ och $w = (w_1, \ldots, w_n) \in (\mathbb{Z}/(p))^n$. Vi definierar även Hammingavståndet av en kod som det minsta avståndet som förekommer i koden. Det vill säga

$$d(C) = \min\{d(v, w) \mid v, w \in C, v \neq w\}$$

för en kod C. Hammingavståndet av en kod kallar vi för *separationen* av en kod. Vi är intresserade av att skapa koder där separationen är så stor som möjligt men där n är så låg som möjligt.

Hjälpsats 5.0.1. *Hammingavståndet uppfyller att*

(i) $d(v,w) = 0$ *om och endast om* $v = w$

(ii) $d(v,w) = d(w,v)$

(iii) $d(v,w) \leqslant d(v,u) + d(u,w)$

för alla $v, w, u \in (\mathbb{Z}/(p))^n$.

Bevis. För (i), ifall $v = w$ har vi att

$$\{i \mid v_i \neq w_i\} = \emptyset$$

så $d(v,w) = 0$. Anta nu att $d(v,w) = 0$. Vi har då att

$$v_i = w_i$$

för alla i. Därmed är $v = w$.

(ii) följer av att $\{i \mid v_i \neq w_i\} = \{i \mid w_i \neq v_i\}$. (iii) lämnas som en övning. □

Ett *fel* definierar vi som att en bokstav i ett kodord har ändrats. Om v är kodordet och v' är ordet efter ett fel har inträffat så kommer $d(v,v') = 1$. Detta kan vi även beskriva som att $v' = v + \varepsilon$ där ε är en vektor med bara en nollskild bokstav.

Nästa sats visar hur många fel vi kan upptäcka och hur många fel vi kan rätta till beroende på vad separationen för koden är.

Sats 5.0.2. *Låt* C *vara en kod med separation* $d(C)$*. Då kan vi*

- *Upptäcka upp till* $d(C) - 1$ *fel i varje ord.*
- *Korrigera upp till* $\lfloor \frac{d(C)-1}{2} \rfloor$ *fel i varje ord.*

Bevis. Låt oss säga att det uppstår k stycken fel i ett kodord v. Låt oss även säga att v_j är vektorn efter j stycken fel uppstått. Ifall $v_k \notin C$ vet vi att ett fel måste ha uppstått. Om $k \leqslant d(C) - 1$ har vi dock att

$$\begin{aligned} d(v,v_k) &\leqslant d(v,v_{k-1}) + d(v_{k-1},v_k) \leqslant d(v,v_1) + d(v_1,v_2) + \cdots + d(v_{k-1},v_k) = k \\ &\leqslant d(C) - 1 \end{aligned}$$

Men $d(C)$ är det minsta avståndet mellan två kodord så v_k kan inte vara ett kodord. Antag nu att $k \leqslant \frac{d(C)-1}{2}$ och låt $w \in C$ vara ett annat godtyckligt kodord. Eftersom $d(v,w) \geqslant d(C)$ har vi att

$$\begin{aligned} d(v,v_k) \leqslant k \leqslant \frac{d(C)-1}{2} &\leqslant \frac{d(v,w)-1}{2} \\ &\leqslant \frac{d(w,v_k) + d(v,v_k) - 1}{2} \end{aligned}$$

om vi nu löser ut $d(v,v_k)$ får vi att

$$d(v,v_k) \leqslant d(w,v_k) - 1.$$

Eftersom w var godtycklig så vet vi därmed att v_k är närmare v än något annat kodord. Vi kan därmed korrigera v_k till v. □

Från Sats 5.0.2 ser vi att vilken kodningsfunktion vi väljer inte spelar någon roll i hur många fel vi kan upptäcka och rätta till, så länge de ger upphov till samma kod.

5.1 Linjära koder

När en kod $C \subset (\mathbb{Z}/(p))^n$ är ett delrum sägs koden vara *linjär*. Linjära koder kommer vara fokuset i den här kursen.

Sats 5.1.1. *Till alla linjära koder finns det en kodningsfunktion som är en matris.*

Bevis. Givet en kod $C \subset (\mathbb{Z}/(p))^n$ har vi att $|C| = p^m$ där m är blocklängden. Låt $\{v_1, \ldots, v_m\}$ vara en bas till C.

Vi bildar nu en kodningsfunktion E som är en matris genom att sätta

$$E = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}.$$

Enligt Sats 4.3.6 är E injektiv och enligt Sats 4.3.3 är $V(E) = C$. □

Det visar sig att det är betydligt lättare att beräkna separationen när en kod är linjär. Detta beskrivs av följande sats.

Sats 5.1.2. *Givet en linjär kod C gäller det att separationen $d(C)$ ges av*

$$d(C) = \min\{d(0, v) \mid v \in C, v \neq 0\}.$$

Bevis. Enligt definitionen så är

$$d(C) = \min\{d(v, w) \mid v, w \in C, v \neq w\}$$

så det är tydligt att $\min\{d(0, v) \mid v \in C, v \neq 0\} \leqslant d(C)$. Låt $v, w \in C$ vara två kodord så att $d(v, w) = d(C)$. Eftersom C är ett delrum gäller det att $v - w$ är ett kodord. Vi har då att

$$d(0, v - w) = |\{i \mid 0 \neq v_i - w_i\}| = |\{i \mid w_i \neq v_i\}| = d(v, w).$$

Eftersom $d(0, v - w) \in \{d(0, v) \mid v \in C, v \neq 0\}$ har vi att

$$d(C) = d(0, v - w) \leqslant \min\{d(0, v) \mid v \in C, v \neq 0\} \leqslant d(C)$$

så $d(C) = \min\{d(0, v) \mid v \in C, v \neq 0\}$. □

Ifall en kod inte är linjär behöver vi beräkna $\frac{|C|(|C|-1)}{2}$ Hammingavstånd för att räkna ut separationen. Sats 5.1.2 visar att för linjära koder räcker det att endast beräkna $|C| - 1$ Hammingavstånd.

Exempel 5.1.3. Låt $C \subset (\mathbb{Z}/(3))^5$ vara koden

$$C = \{(0,0,0,0,0),(1,1,1,0,0),(2,2,2,0,0),(0,0,1,1,1),(0,0,2,2,2)$$
$$(1,1,2,1,1),(2,2,1,2,2),(2,2,0,1,1),(1,1,0,2,2)\}.$$

Vi ser att separationen av C kan som mest vara 3 då exempelvis

$$d((1,1,1,0,0),(2,2,2,0,0)) = 3.$$

Vi skulle kunna beräkna separationen genom att räkna ut Hammingavståndet mellan alla par av kodord. Detta skulle dock betyda att vi behövde räkna ut

$$\frac{|C|(|C|-1)}{2} = \frac{9 \cdot 8}{2} = 36$$

stycken Hammingavstånd. Vi försöker istället visa att C är en linjär kod. Låt $v_1 = (1,1,1,0,0)$ och $v_2 = (0,0,1,1,1)$. Då är

$$\begin{aligned}
0v_1 + 0v_2 &= (0,0,0,0,0),\\
1v_1 + 0v_2 &= (1,1,1,0,0),\\
0v_1 + 1v_2 &= (0,0,1,1,1),\\
2v_1 + 0v_1 &= (2,2,2,0,0),\\
0v_1 + 2v_1 &= (0,0,2,2,2),\\
1v_1 + 1v_1 &= (1,1,2,1,1),\\
2v_1 + 2v_2 &= (2,2,1,2,2),\\
2v_1 + 1v_2 &= (2,2,0,1,1),\\
1v_1 + 2v_2 &= (1,1,0,2,2),
\end{aligned}$$

därmed är $C = \text{spann}\{v_1, v_2\}$ vilket innebär att C är en linjär kod. Vi kan därför bestämma separationen genom att beräkna

$$\begin{aligned}
d((0,0,0,0,0),(1,1,1,0,0)) &= 3,\\
d((0,0,0,0,0),(0,0,1,1,1)) &= 3,\\
d((0,0,0,0,0),(2,2,2,0,0)) &= 3,\\
d((0,0,0,0,0),(0,0,2,2,2)) &= 3,\\
d((0,0,0,0,0),(1,1,2,1,1)) &= 5,\\
d((0,0,0,0,0),(2,2,1,2,2)) &= 5,\\
d((0,0,0,0,0),(2,2,0,1,1)) &= 4,\\
d((0,0,0,0,0),(1,1,0,2,2)) &= 4,
\end{aligned}$$

så koden har separation $d(C) = 3$. Låt oss nu se hur vi kan använda C för att felrätta ett meddelande. Enligt Sats 5.0.2 kan koden upptäcka $d(C) - 1 = 2$ fel och kan rätta till $\lfloor \frac{d(C)-1}{2} \rfloor = 1$ fel. Låt oss nu säga att vi vill skicka meddelandet 110212 över alfabetet $\mathbb{Z}/(3)$ till någon. Eftersom $|C|$ har 9 ord måste blocklängden vara 2 då $3^2 = 9$. Vi väljer därför att dela upp meddelandet i tre vektorer $(1,1),(0,2),(1,2) \in (\mathbb{Z}/(3))^2$ och göra felrättningen på varje vektor för sig.

Vi behöver nu en kodningsfunktion $E : \mathbb{Z}/(3)^2 \to C \subset \mathbb{Z}/(3)^5$. Eftersom v_1 och v_2 är linjärt oberoende bildar de en bas till C. Vi kan därför välja kodningsfunktionen till att vara matrisen

$$E = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Vi beräknar nu

$$\begin{aligned} E(1,1) &= (1,1,2,1,1), \\ E(0,2) &= (0,0,2,2,2), \\ E(1,2) &= (1,1,0,2,2). \end{aligned}$$

Låt oss nu säga att det inträffar några fel, så istället för $E(1,1)$ skickas $(1,1,1,1,1)$, istället för $E(0,2)$ skickas $(2,0,2,2,2)$ och istället för $E(1,2)$ skickas $(1,0,0,2,2)$. Vår mottagare kommer då få meddelandet

$$111112022210022.$$

Eftersom ingen av blocken $(1,1,1,1,1)$, $(2,0,2,2,2)$, $(1,0,0,2,2)$ är kodord kan mottagaren se att det har inträffat åtminstone ett fel i varje ord. Däremot ligger $(1,1,1,1,1)$ närmast kodordet $(1,1,2,1,1)$, $(2,0,2,2,2)$ ligger närmast kodordet $(0,0,2,2,2)$ och $(1,0,0,2,2)$ ligger närmast kodordet $(1,1,0,2,2)$. Mottagaren kan därför rätta till de mottagna blocken till dessa kodord genom att finna orden w_1, w_2, w_3 där

$$\begin{aligned} Ew_1 &= (1,1,2,1,1), \\ Ew_2 &= (0,0,2,2,2), \\ Ew_3 &= (1,1,0,2,2). \end{aligned}$$

Vi vet att w_1, w_2, w_3 då kommer vara $(1,1), (0,2), (1,2)$ så mottagaren kan återskapa det ursprungliga meddelandet

$$110212.$$

Vi avslutar det här kapitlet med ett exempel på en kod där $n = m + 1$.

Exempel 5.1.4. Låt p, m vara godtyckliga och $n = m + 1$. Vi definierar då kodningsfunktionen $E : \mathbb{Z}_2^m \to C \subset \mathbb{Z}_2^n$ genom att sätta

$$E((v_1, \ldots, v_m)) = (v_1, \ldots, v_m, v_1 + v_2 + \cdots + v_m)$$

Eftersom koden är linjär (Se övning 5.4) kan separationen beräknas som

$$d(C) = \min\{d(0, v) \mid v \in C, v \neq 0\}.$$

Antag att exakt en bokstav v_k i $v \in (\mathbb{Z}/(p))^m$ är skild från 0. Vi har då att

$$d(0, E(v)) = d(0, (0, \ldots, 0, v_k, 0, \ldots, 0, v_k)) = 2$$

annars ifall ordet v har $l \geqslant 2$ nollskilda bokstäver är det tydligt att $d(0, E(v)) \geqslant l$ så koden har separation 2.

Övningar

Övning 5.1. Låt

$$C = \{(1,0,0,0,0,1),(0,1,1,1,0,1),(0,1,0,0,1,0),(1,0,1,1,1,0)\}$$

vara en kod i $(\mathbb{Z}/(2))^6$.

(i) Vad måste blocklängden m vara för att C ska vara en kod?

(ii) Är C linjär?

(iii) Beräkna separationen $d(C)$.

(iv) Hur många fel kan koden detektera och korrigera?

Övning 5.2. Låt $p = 3$ och $m = 2$. Låt E vara kodningsfunktionen som upprepar ett ord tre gånger.

(i) Skriv ner elementen i koden. Vad är längden av kodorden n?

(ii) Visa att koden är linjär genom att skriva E som en matris.

(iii) Beräkna separationen av koden.

Övning 5.3. Konstruera en kod i $(\mathbb{Z}/(2))^8$ med fyra ord och separation 5.

Övning 5.4. Bevisa att koden i Exempel 5.1.4 är linjär.

Övning 5.5 ($\star$)**.** Bevisa (iii) i Hjälpsats 5.0.1 genom att använda olikheten

$$|A \cup B| \leqslant |A| + |B|\,.$$

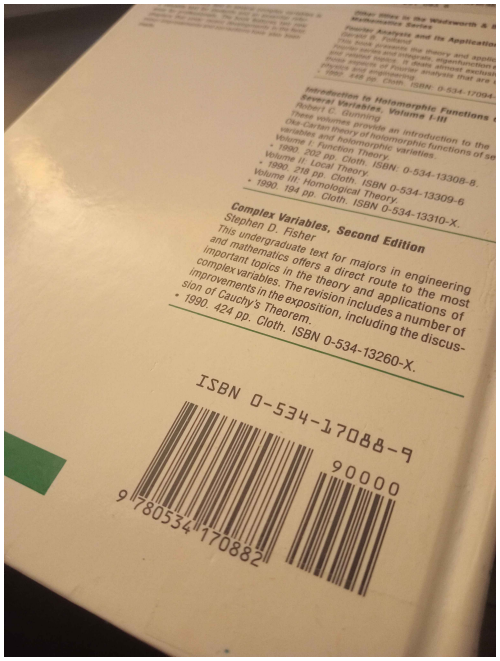
Övning 5.6 ($\star\star$)**.** Låt C vara en kod över $\mathbb{Z}/(2)$ med blocklängd m, kodordslängd n och separation $d(C)$ där $d(C)$ är udda. Definiera nu

$$C' = \{(v_1,\ldots,v_n, v_1+v_2+\cdots+v_n) \mid (v_1,\ldots,v_n) \in C\}.$$

(i) Visa att C' är en med kodordslängd n och separation $d(C)+1$.

(ii) Visa att om C är linjär så är C' linjär.

Övning 5.7 ($\star\star$)**.** ISBN 10-koden ("International Standard Book Number") är en följd av tio element $x_{10},\ldots,x_1$ tagna från mängden $\mathbb{Z}/(p)$. Denna följd är indelad i fyra delar av variabel längd som ofta separeras med bindestreck eller mellanslag. Dessa tecken påverkar dock inte kodens förmåga att upptäcka och korrigera fel.



Figur 5.2: En bok med en ISBN 10 kod.

- Den första delen $x_{10}, \ldots$ (oftast av längd 1) är ursprungslandskoden. Den är 0 eller 1 för engelskspråkiga länder, 2 för franskspråkiga, 3 för tyskspråkiga och så vidare. Denna del av koden kan vara upp till fem siffror. Till exempel har Bhutan koden 99936 och Sverige koden 91.
- Nästa del beskrivet utgivaren. Den består av minst två element.
- Följande del $, \ldots, x_2$, är ett nummer valt av utgivaren för att identifiera boken. Elementen $x_{10}, \ldots, x_2$ är tagna från mängden $\{0, 1, \ldots, 9\} \subset \mathbb{Z}/(11)$.
- Det sista elementet, x_1, bestämmas av

  $$x_1 = -2x_2 - 3x_3 - \cdots - 10x_{10}.$$

  Om $x_1 = 10$ betecknas det dock med ett stort X.

Visa att denna kod kan upptäcka ett fel, ett byte av två intilliggande element och kan rätta till ett olästbart tecken.

6 Generatormatriser och kontrollmatriser

6.1 Generatormatriser

I det här kapitlet kommer vi undersöka linjära koder i mer detalj. Det vill säga de koder där kodningsfunktion E är en matris. En sådan matris kallar vi för en *generatormatris*.

Det kan hända att flera generatormatriser ger upphov till samma kod. Följande sats beskriver när detta inträffar.

Sats 6.1.1. *Låt G vara en $n \times m$ generatormatris till en kod C över ett alfabet $\mathbb{Z}/(p)$. Då är G' en generatormatris till C om och endast om*

$$G' = GM$$

för någon inverterbar $m \times m$ matris M.

Bevis. Antag att $G' = GM$ för någon inverterbar $m \times m$ matris M. Då M är inverterbar har vi att $V(M) = (\mathbb{Z}/(p))^m$. Men nu är $V(G') = V(GM) = G(M((\mathbb{Z}/(p))^m)) = G((\mathbb{Z}/(p))^m) = C$ som vi ville. Eftersom M är en bijektion kommer även G' vara injektiv.

För att visa andra hållet antar vi att både G och G' är generatormatriser till C. Eftersom både G och G' är injektiva kommer kolumnerna hos G respektive G' vara baser till C. Låt nu

$$G = \begin{bmatrix} | & & | \\ G_1 & \cdots & G_m \\ | & & | \end{bmatrix}$$

och

$$G' = \begin{bmatrix} | & & | \\ G'_1 & \cdots & G'_m \\ | & & | \end{bmatrix}.$$

Eftersom kolumnerna av G är en bas kan alla kolumner i G' uttryckas som en linjärkombination av kolumnerna av G. Precis som i beviset av Sats 4.3.5 kan vi uttrycka detta som att

$$G' = GM$$

för någon $m \times m$ matris M. Det återstår att se att M är inverterbar. Men om M inte var injektiv skulle inte heller GM vara injektiv, så M måste vara inverterbar enligt Följdsats 4.3.7. □

Hur ska vi då välja vilken av alla generatormatriser vi ska ta som vår kodningsfunktion? Givet en $n \times m$ generatormatris G vet vi från Sats 4.3.6 att matrisen har m linjärt oberoende rader. Låt oss nu anta att det är de första m raderna som är linjärt oberoende. Vi tar då och skriver

$$G = \begin{bmatrix} G_m \\ G_{n-m} \end{bmatrix}$$

där G_m är en $m \times m$ matris och G_{n-m} är en $(n-m) \times m$ matris. Det följer att G_m är inverterbar. Tar vi och multiplicerar G med G_m^{-1} får vi en ny generator matris på formen

$$GG_m^{-1} = \begin{bmatrix} G_m G_m^{-1} \\ G_{n-m} G_m^{-1} \end{bmatrix} = \begin{bmatrix} I_m \\ G_{n-m} G_m^{-1} \end{bmatrix}$$

där I_m är $m \times m$ identitetsmatrisen.

Definition 6.1.2. En $m \times n$ generatormatris G sägs vara på *normalform* om den kan skrivas på formen

$$G = \begin{bmatrix} I_m \\ A \end{bmatrix}$$

där A är en $(n-m) \times m$ matris.

Att en generatormatris är på normalform innebär att när vi kodar ett ord så börjar vi med att skicka det ordet och därefter skickar vi extra information.

För att vi ska kunna skriva en generatormatris på normalform gäller det att just de första raderna är linjärt oberoende. Vi visar i nästa sats att alla generatormatriser för en kod kommer ha linjärt oberoende rader på samma ställen.

Sats 6.1.3. *Låt G, G' vara två $n \times m$ generatormatriser till en kod C. Skriv*

$$G = \begin{bmatrix} — G_1 — \\ \vdots \\ — G_n — \end{bmatrix} \qquad G' = \begin{bmatrix} — G'_1 — \\ \vdots \\ — G'_n — \end{bmatrix}$$

Eftersom G har m linjärt oberoende rader finns det en mängd av index $S \subset \{1, \ldots, n\}$ där $|S| = m$ och vektorerna i mängden $\{G_j \mid j \in S\}$ är linjärt oberoende. Då kommer vektorerna i mängden $\{G'_j \mid j \in S\}$ också vara linjärt oberoende.

Bevis. Enligt Sats 6.1.1 kan vi skriva

$$G' = GM$$

för en $m \times m$ inverterbar matris M. Då har vi att

$$G' = \begin{bmatrix} — G'_1 — \\ \vdots \\ — G'_n — \end{bmatrix} = \begin{bmatrix} — G_1 M — \\ \vdots \\ — G_n M — \end{bmatrix}$$

Vi bildar nu $m \times m$ matriserna P och P' genom att ta bort alla rader G_k respektive G'_k där $k \notin S$. Vi har då att

$$H' = HM.$$

Nu är raderna av H linjärt oberoende så både H och M är bijektioner. Men då är även H' en bijektion och därmed är dess rader linjärt oberoende. □

Exempel 6.1.4. Låt oss gå tillbaka till koden

$$C = \{(0,0,0,0,0),(1,1,1,0,0),(2,2,2,0,0),(0,0,1,1,1),(0,0,2,2,2)$$
$$(1,1,2,1,1),(2,2,1,2,2),(2,2,0,1,1),(1,1,0,2,2)\}.$$

i Exempel 5.1.3. Vi såg att den hade generatormatrisen

$$G = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Mycket riktigt har G två linjärt oberoende rader, exempelvis $(1,0),(0,1)$, $(1,0),(1,1)$ eller $(0,1),(1,1)$. Om vi nu antog att det fanns en annan generatormatris till C där de första två raderna var linjärt oberoende så medför Sats 6.1.3 att de första två raderna av G också är linjärt oberoende. Därmed finns det ingen generatormatris till C på normalform.

För att undkomma det här problemet introducerar vi konceptet av *ekvivalenta koder*.

Definition 6.1.5. Två koder $C, C' \subset (\mathbb{Z}/(p))^n$ är ekvivalenta om $|C| = |C'| = p^m$ och det existerar någon bijektiv funktion

$$f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

så att

$$C' = \{(v_{f(1)}, v_{f(2)}, \ldots, v_{f(n)}) \mid (v_1, v_2, \ldots, v_n) \in C\}.$$

Sats 6.1.6. *Om två koder är ekvivalenta har de samma separation.*

Bevis. Låt f vara som i definitionen av ekvivalenta koder och $v = (v_1, \ldots, v_n) \in C$ vara ett element där

$$d(0, v) = d(C).$$

Låter vi nu $v' = (v_{f(1)} \ldots, v_{f(n)}) \in C'$ ser vi då att

$$d(0, v') = d(0, v) = d(C).$$

Därmed är $d(C') \leqslant d(C)$. Om vi nu istället hade valt ett element $w \in C'$ där $d(0, w) = d(C')$ kan vi använda f^{-1} för att se att $d(C) \leqslant d(C')$. Det följer att $d(C) = d(C')$. □

Sats 6.1.7. *Två koder $C, C' \subset (\mathbb{Z}/(p))^n$ är ekvivalenta om och endast om deras generatormatriser är har samma rader, möjligtvis i en annan ordning.*

Bevis. Anta att två koder C, C' är ekvivalenta. Givet att

$$G = \begin{bmatrix} — G_1 — \\ \vdots \\ — G_n — \end{bmatrix}$$

är en generatormatris till C vill vi visa att

$$G' = \begin{bmatrix} — G_{f(1)} — \\ \vdots \\ — G_{f(n)} — \end{bmatrix}$$

är en generatormatris till C' där f är som i definition 6.1.5. Alla element i $v' \in C'$ kan nu skrivas på formen

$$v' = (v_{f(1)}, \ldots, v_{f(n)})$$

för exakt en vektor $v = (v_1, \ldots, v_n) \in C$ vilket kan i sin tur skrivas som

$$v = Gw = (G_1 w, \ldots, G_n w).$$

för exakt en vektor $w \in (\mathbb{Z}/(p))^m$. Vi har nu att

$$G'w = (G_{f(1)}w, \ldots, G_{f(n)}w) = (v_{f(1)}, \ldots, v_{f(n)}) = v'.$$

Därmed är $C' = V(G')$ så G' är en generatormatris till C'. □

Sats 6.1.8. *För varje kod C finns det en ekvivalent kod C' som har en generatormatris på normalform.*

Bevis. Välj en generatormatris G till C och m linjärt oberoende rader. Vi kan nu byta plats på raderna så vi får att de m linjärt oberoende raderna är de första raderna. Den nya generatormatrisen kommer då vara en generatormatris till en ekvivalent kod C'. Den nya generatormatrisen kan nu skrivas på normalform enligt diskussionen innan definition 6.1.2. □

6.2 Kontrollmatriser

Om vi nu får ett medelande $v \in (\mathbb{Z}/(p))^n$ hur kan vi ta reda på om v ingår i koden? Givetvis kan vi räkna ut alla kodord i koden och sedan jämföra med v. För stora koder kan dock detta ta lång tid. Kontrollmatriser kommer låta oss göra detta enklare.

Definition 6.2.1. Givet en kod C är en kontrollmatris H en surjektiv $(n - m) \times n$ matris sådant att

$$H(C) = \{0\}.$$

eller ekvivalent att

$$HG = 0$$

där G är en generatormatris.

Vi noterar att kontrollmatriser är funktioner från $(\mathbb{Z}/(p))^n \to (\mathbb{Z}/(p))^{n-m}$.

Sats 6.2.2. *Det existerar en kontrollmatris till alla koder.*

Bevis. Låt $C \subset (\mathbb{Z}/(p))^n$ vara en kod och

$$G = \begin{bmatrix} | & & | \\ G_1 & \cdots & G_m \\ | & & | \end{bmatrix}$$

vara en generatormatris till koden. Eftersom $G_1, \ldots, G_m$ är linjärt oberoende kan vi enligt Sats 4.2.6 bilda en bas till $(\mathbb{Z}/(p))^n$ som inkluderar $G_1, \ldots, G_m$. Låt den basen vara

$$\{G_1, \ldots, G_m, w_{m+1}, \ldots, w_n\}$$

för några vektorer $w_{m+1}, \ldots, w_n \in (\mathbb{Z}/(p))^n$. Låt

$$W = \begin{bmatrix} | & & | \\ w_{m+1} & \cdots & w_n \\ | & & | \end{bmatrix}.$$

Vi definierar nu $n \times n$ matrisen

$$B = \begin{bmatrix} | & & | & | & & | \\ G_1 & \cdots & G_m & w_{m+1} & \cdots & w_n \\ | & & | & | & & | \end{bmatrix} = \begin{bmatrix} G & W \end{bmatrix}.$$

Vi har då att

$$B \begin{bmatrix} I_m \\ 0_{n-m,m} \end{bmatrix} = G.$$

Där $0_{n-m,n}$ är $(n-m) \times n$ matrisen med bara 0'or och I_m är $m \times m$ identitetsmatrisen. Eftersom kolumnerna av G är linjärt oberoende kommer B vara inverterbar. Vi definierar nu H som

$$H = \begin{bmatrix} 0_{n-m,m} & I_{n-m} \end{bmatrix} B^{-1}$$

Vi ska nu visa att H är en kontrollmatris. Antag att $v \in C$. Då kan vi skriva $v = Gw$ för någon vektor $w \in (\mathbb{Z}/(p))^m$. Vi har nu att

$$Hv = \begin{bmatrix} 0_{n-m,m} & I_{n-m} \end{bmatrix} B^{-1} Gw = \begin{bmatrix} 0_{n-m,m} & I_{n-m} \end{bmatrix} \begin{bmatrix} I_m \\ 0_{n-m,m} \end{bmatrix} w = 0w = 0.$$

För att se att H är surjektiv kan vi notera att B^{-1} är bijektiv och att raderna av $\begin{bmatrix} 0_{n-m,m} & I_{n-m} \end{bmatrix}$ spänner upp $(\mathbb{Z}/(p))^{n-m}$. □

Ifall generatormatrisen är på normalform går det dock att finna en kontrollmatris betydligt lättare.

Sats 6.2.3. *Givet en kod C där generatormatrisen på normalform är*

$$G = \begin{bmatrix} I_m \\ A \end{bmatrix}$$

så kommer matrisen

$$H = \begin{bmatrix} -A & I_{n-m} \end{bmatrix}$$

vara en kontrollmatris.

Bevis. Vi har att

$$HG = \begin{bmatrix} -A & I_{n-m} \end{bmatrix} \begin{bmatrix} I_m \\ A \end{bmatrix} = \begin{bmatrix} -A + A \end{bmatrix} = 0. \qquad \square$$

En kontrollmatris på formen

$$H = \begin{bmatrix} -A & I_{n-m} \end{bmatrix}$$

för en matris $(n-m) \times m$ matris A säger vi är på normalform.

Hur kan vi nu använda kontrollmatrisen för att ta reda på om en given vektor v i $(\mathbb{Z}/(p))^n$ är ett kodord? Från villkoret

$$H(C) = \{0\}$$

så vet vi att om $v \in C$ så kommer

$$Hv = 0.$$

Därmed om $Hv \neq 0$ vet vi att v inte är ett kodord och att ett fel har inträffat. Men om istället $Hv = 0$ kan vi säga att v måste vara ett kodord? Nästa sats visar att svaret på denna fråga är ja.

Sats 6.2.4. *Givet en kod C och en vektor $v \in (\mathbb{Z}/(p))^n$ så är $v \in C$ om och endast om*

$$Hv = 0.$$

Bevis. Vi ska visa att $N(H) = C$. Det är tydligt att $C \subset N(H)$ och att

$$\dim(C) = m.$$

Eftersom H är surjektiv är $V(H) = (\mathbb{Z}/(p))^{n-m}$ så $\dim V(H) = n - m$. Enligt Dimensionssatsen 4.3.4 har vi nu att

$$\dim V(H) + \dim N(H) = n$$

vilket medför att $\dim N(H) = m$. Men om $C \subsetneq N(H)$ skulle Sats 4.2.6 medföra att vi kunde skapa en bas till $N(H)$ med fler än m element. Därmed måste $N(H) = C$. $\square$

Därmed kan vi nu enkelt se om en vektor v är ett kodord genom att beräkna ifall $Hv = 0$ för någon kontrollmatris H.

Kontrollmatriser låter oss även lätt beräkna separationen av en kod.

Sats 6.2.5. *En kod C med kontrollmatris H har separation $k = d(C)$ om och endast om H har k linjärt beroende kolumner och alla val av $k-1$ kolumner är linjärt oberoende.*

Bevis. Anta först att H har k linjärt beroende kolumner och att alla val av $k-1$ kolumner är linjärt oberoende. Låt

$$H = \begin{bmatrix} | & & | \\ H_1 & \cdots & H_n \\ | & & | \end{bmatrix}$$

och $S \subset \{H_1, \ldots, H_n\}$ vara k linjärt beroende kolumner. Då finns det en lösning till

$$0 = a_1 H_1 + \cdots + a_n H_n = H \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

där $a_k = 0$ om $H_k \notin S$ och inte alla andra a_k där $H_k \in S$ är 0. Vi kan faktiskt säga att ingen koefficient a_k är 0 om $H_k \in S$ då detta skulle motsäga att alla val av $k-1$ (eller färre) kolumner är linjärt oberoende. Men då har vi att $v = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in C$ och att $d(0, v) = k$. Dessutom kan det inte finnas något kodord med lägre separation då detta igen skulle motsäga att alla val av $k-1$ (eller färre) kolumner är linjärt oberoende.

Vi antar nu istället att $d(C) = k$. Anta att det finns någon uppsättning av $k-1$ kolumner som är linjärt beroende. Då måste det också finnas någon uppsättning av $k-2$ kolumner som är linjärt beroende, annars hade $d(C) = k-1$ enligt den första delen. Men då måste det också finnas någon uppsättning av $k-3$ kolumner som är linjärt beroende och så vidare. Men en mängd av bara en (nollskild) vektor kan inte vara linjärt beroende så tillslut får vi en motsägelse. Därmed måste alla uppsättningar av $k-1$ kolumner vara linjärt oberoende.

Vi antar nu att alla uppsättningar av k kolumner är linjärt oberoende. Alla uppsättningar av $k+1$ kolumner måste då vara linjärt oberoende då den första delen annars skulle implicera att $d(C) = k+1$. På samma sätt skulle tillslut alla kolumner behöva vara linjärt oberoende, men som mest $n - m < n$ kolumner kan vara linjärt oberoende enligt Sats 4.3.6. Därmed måste det finnas k linjärt beroende kolumner. □

Sats 6.2.5 ger oss även en över begränsning på hur stor separationen kan vara.

Följdsats 6.2.6. *Givet en linjär kod $C \subset (\mathbb{Z}/(p))^n$ där blocklängden är m gäller det att*

$$d(C) \leqslant n - m + 1$$

Bevis. Från Sats 4.3.6 vet vi att H har $n-m$ linjärt oberoende kolumner. Det följer att om $d(C) \geqslant n - m + 1$ skulle H ha $n - m + 1$ linjärt oberoende kolumner vilket är en motsägelse. □

I kapitel 8 kommer vi konstruera en familj av koder där $d(C) = n - m + 1$.

Slutligen ska vi beskriva hur vi kan snabbt rätta till enstaka fel med hjälp av kontrollmatriser. Givet en kod C med kontrollmatris antar vi att ett kodord $v \in C$ får ett fel $v \mapsto v + \varepsilon = v'$ där $d(v, v') = d(0, \varepsilon) = 1$. Ifall vi kan ta reda på ε kan vi då beräkna v genom $v = v' - \varepsilon$.

Vi skriver H och ε på formerna

$$H = \begin{bmatrix} | & & | \\ H_1 & \cdots & H_m \\ | & & | \end{bmatrix}, \qquad \varepsilon = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \varepsilon_k \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

där ε_k på koordinat k. Om vi nu tar och beräknar $H(v')$ får vi att

$$H(v') = H(v + \varepsilon) = Hv + H\varepsilon = H_k\varepsilon_k$$

Om det finns det en unik kolumnvektor som är proportionell till $H_k\varepsilon_k$ kan vi nu rätta felet. Detta gör vi genom att läsa vilken position den kolumnen nu är vilket innebär att kan vi finna k och därmed ε_k. Om det är givet att separationen $d(C) \geqslant 3$ kommer alla par kolumner av H vara linjär oberoende så detta är då alltid möjligt.

Exempel 6.2.7. Låt $C \subset (\mathbb{Z}/(3))^n$ vara en kod med generatormatris

$$G = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 2 \end{bmatrix}$$

Då blocklängden $m = 3$ har vi att $|C| = 27$ ord. Vi ska räkna ut separationen av C och visa hur vi kan felrätta enstaka fel utan att behöva räkna ut alla ord i C. Då de första tre raderna är linjärt oberoende finns det en generatormatris på normalform till C. Ifall det inte hade varit fallet hade det varit bättre att jobba med en ekvivalent kod. Matrisen

$$G_3 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 2 \end{bmatrix}$$

har invers

$$G_3^{-1} = \begin{bmatrix} 0 & 2 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix}.$$

Vi kan nu finna en generatormatris på normalform G' genom att beräkna $G' = GG_3^{-1}$:

$$G' = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 2 \end{bmatrix} \begin{bmatrix} 0 & 2 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

vilket ger oss en kontrollmatris på normalform H,

$$H = \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Det är nu lätt att se att par av kolumner av H är linjärt oberoende men att vi kan finna tre kolumner som är linjärt beroende (exempelvis kolumn 1, 4 och 5). Därmed har koden separation $d(C) = 3$ och kan rätta upp till ett fel. Låt oss nu säga att vi vill skicka meddelandet 112. Vi sätter $v = (1, 1, 2) \subset (\mathbb{Z}/(3))^3$ och beräknar

$$w = Gv = (1, 1, 2, 2, 1, 1, 2).$$

Ifall det nu inträffar ett fel och mottagaren får meddelandet $u = (1, 0, 2, 2, 1, 1, 2)$ tar mottagaren och beräknar

$$Hu = (1, 0, 1, 0).$$

Eftersom $Hw' \neq 0$ vet mottagaren att ett fel har inträffat. Men då den andra kolumnen av H uppfyller

$$2H_2 = (1, 0, 1, 0)$$

kan vi sätta $\varepsilon = (0, 2, 0, 0, 0, 0, 0)$ då

$$Hu = H\varepsilon = (1, 0, 1, 0)$$

Vi rättar nu till u genom att sätta $w' = u - \varepsilon = (1, 1, 2, 2, 1, 1, 2)$. Då G var på normalform kan vi även lätt avkoda meddelandet genom att bara ta de 3 första bokstäverna vilket ger oss slutligen meddelandet 112 vilket är vad vi ville skicka.

Övningar

Övning 6.1. Låt C vara en kod över $\mathbb{Z}/(2)$ med generatormatris

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Skriv ut alla kodord i C och beräkna separationen $d(C)$.

Övning 6.2. Låt C vara en kod över $\mathbb{Z}/(2)$ med generatormatris

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Finn en generatormatris till G på normalform.

Tips: Du kan använda ex. `https://www.desmos.com/matrix` för att räkna ut inverser (om du tolkar resultatet rätt).

Övning 6.3. Betrakta en kod $C \subset (\mathbb{Z}/(2))^6$ med generatormatris

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

(i) Vilka av följande ord är kodord?

$$111001,\ 010100,\ 110111,\ 100001$$

(ii) Vilka av dessa går rätta? Rätta dessa!

Övning 6.4. Låt C vara en kod över $(\mathbb{Z}/(2))^7$ med generatormatris

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Felrätta följande ord om möjligt.

$$1101011,\ 0110111,\ 0111000$$

Övning 6.5 ($\star$)**.** Låt $C_1, C_2 \subset (\mathbb{Z}/(2))^4$ vara två koder med kontrollmatriser

$$H_1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{respektive} \quad H_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

Skriv ner alla kodord till H_1 respektive H_2. Hur är koderna C_1 och C_2 relaterade?

Övning 6.6 ($\star\star$)**.** Låt $C \subset (\mathbb{Z}/(5))^6$ vara en kod med en generatormatris

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 4 \end{bmatrix}.$$

Visa att $d(C) = 4$.

Övning 6.7 ($\star\star\star$)**.** Låt H vara en $(n-m) \times n$ kontrollmatris till en kod C. Beskriv när en annan $(n-m) \times n$ matris H' är en kontrollmatris till C.

Ledtråd: Jämför med sats 6.1.1.

7 Hammingkoder

7.1 Perfekta koder

Definition 7.1.1. Låt $C \subset (\mathbb{Z}/(p))^n$ vara en kod. Vi säger att C är *perfekt* om $d(C) = 2k+1$ och det för varje kodord $c \in (\mathbb{Z}/(p))^n$ finns ett unikt $c' \in C$ som uppfyller att

$$d(c, c') \leqslant k.$$

Med andra ord, om vi låter *Bollen kring ett ord* $c \in C$ med radius k vara mängden

$$B(c, k) = \{w \in (\mathbb{Z}/(p))^n \mid d(w, c) \leqslant k\},$$

så är $B(c, k) \cap B(c', k) = \emptyset$ om $c \neq c'$ och

$$\bigcup_{c \in C} B(c, k) = (\mathbb{Z}/(p))^n.$$

Det gäller alltid att $B(c, k) \cap B(c', k) = \emptyset$ för alla koder.

Exempel 7.1.2. Låt $C \subset (\mathbb{Z}/(2))^7$ vara en kod med kontrollmatris

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Vilka två av dessa rader som helst är linjärt oberoende, då de annars är multiplar av varandra och i $\mathbb{Z}/(2)$ innebär det antingen att de är identiska eller att en av dem är 0. Alltså är $d(c, c') = 3$, så vi ser från Sats 5.0.2 att koden kan rätta ett fel. Koden är också perfekt, något som inte är helt uppenbart från representationen ovan.

Vi påminner lite kort om följande kombinatoriska redskap.

Definition 7.1.3. Låt $0 \leqslant k \leqslant n$ vara heltal. Vi definierar "n över k" som

$$\binom{n}{k} = \text{antalet sätt att välja } k \text{ färger från en lista av } n \text{ färger.}$$

Det finns en även en enkel formel

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

där

$$0! = 1, \quad r! = r \cdot (r-1) \cdot \cdots \cdot 3 \cdot 2 \cdot 1.$$

Vi vill hitta ett sätt att enkelt kontrollera att en kod är perfekt. För att göra det behöver vi följande formel.

Hjälpsats 7.1.4. *Låt $r > 0$ vara ett heltal och $c \in (\mathbb{Z}/(p))^n$ vara en vektor.*

$$|B(c,r)| = \binom{n}{0} + \binom{n}{1}(p-1) + \binom{n}{2}(p-1)^2 + \cdots + \binom{n}{r}(p-1)^r.$$

Bevis. Vi påstår att antalet ord w i $(\mathbb{Z}/(p))^n$ som skiljer sig från c på exakt j platser är

$$\binom{n}{j}(p-1)^j. \tag{7.1}$$

Först väljs de j positioner där w skiljer sig från c, och det kan göras på

$$\binom{n}{j}$$

sätt. Sedan väljs vilka element från $\mathbb{Z}/(p)$ som ska vara i dessa j positioner. Då vi har j element i dessa positioner och vi har $p-1$ val för varje position (de får inte vara samma som i c) har vi totalt

$$(p-1)^j$$

val. Slår vi ihop dessa resultat får vi formeln i ekvation (7.1).

Antalet element i $B(c,r)$ är summan av alla element av avstånd j för $1 \leqslant j \leqslant r$. □

Sats 7.1.5. *Låt $C \subset \mathbb{Z}/(p)^n$ vara en kod så att $|C| = N$ och $d(C) = 2r+1$. Då gäller följande formel*

$$\binom{n}{0} + \binom{n}{1}(p-1) + \binom{n}{2}(p-1)^2 + \cdots + \binom{n}{r}(p-1)^r \leqslant \frac{p^n}{N}. \tag{7.2}$$

Likhet gäller i olikhet (7.2) om och endast om C är perfekt.

Bevis. Vi ser att vänsterled i olikhet (7.2) är exakt antal element i $B(c,r)$ för något $c \in C$. Om $c \neq c'$ och

$$w \in B(c,r) \cap B(c',r),$$

har vi att

$$d(c,c') \leqslant d(c,r) + d(c',r) \leqslant 2r,$$

vilket är en motsägelse då $d(C) = 2r+1$. Alltså är

$$B(c,r) \cap B(c',r) = \emptyset.$$

Då alla bollar $B(c,r)$ är helt distinkta så gäller

$$\left| \bigcup_{c \in C} B(c,r) \right| = NB(c,r) = N\left(\binom{n}{0} + \binom{n}{1}(p-1) + \binom{n}{2}(p-1)^2 + \cdots + \binom{n}{r}(p-1)^r \right). \tag{7.3}$$

Eftersom

$$\bigcup_{c \in C} B(c, r) \subset (\mathbb{Z}/(p))^n$$

så är även

$$\left| \bigcup_{c \in C} B(c, r) \right| \leqslant (\mathbb{Z}/(p))^n = p^n. \tag{7.4}$$

Lägger vi ihop ekvation (7.3) och (7.4) får vi

$$\binom{n}{0} + \binom{n}{1}(p-1) + \binom{n}{2}(p-1)^2 + \cdots + \binom{n}{r}(p-1)^r \binom{n}{i}(p-1)^i \leqslant \frac{p^n}{N}.$$

Likhet sker om vi har likhet i ekvation (7.4), vilket är då

$$\bigcup_{c \in C} B(c, r) = (\mathbb{Z}/(p))^n.$$

Det innebär att varje $B(c, r)$ innehåller ett unikt kodord. Det här är exakt betydelsen av att vara perfekt.

□

7.2 Hammingkoder

Koden i Exempel 7.1.2 har en kontrollmatris vars kolumner är alla vektorer i $(\mathbb{Z}/(2))^3$ som inte är 0. Vi kan generalisera det här till en godtyckligt stor matris.

Exempel 7.2.1. Låt $r > 0$ vara ett heltal. En binär *Hammingkod* av *redundans* r är en kod med kontrollmatris H av storlek $r \times (2^r - 1)$ vars kolumner är alla vektorer i $(\mathbb{Z}/(2))^r$ utom 0. Då en omordning av kolumner i H motsvarar ekvivalenta koder är alla Hammingkoder av redundans r ekvivalenta. Vi kallar en sådan kod för hammingkod och det är underförstått att den är binär.

Exempel 7.1.2 är ett litet exempel på en Hammingkod.

För att förstå vad som gör hammingkoder användbara, går vi igenom lite

Definition 7.2.2. Låt $n \geqslant 0$ vara ett heltal. Om $n \leqslant 2^r$ för något positivt heltal r kan vi skriva n på formen

$$n = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_r \cdot 2^r,$$

där alla $a_i \in \{0, 1\}$ och är unikt bestämda. Vi kan då bilda en vektor i $(\mathbb{Z}/(2))^r$, definierad genom

$$v = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_r \end{bmatrix}$$

Vektorn v kallas för den *binära representationen* av n.

Definition 7.2.3. Låt $r > 0$ vara ett heltal och låt H_r vara den $r \times (2^r - 1)$ matris där kolumn i är den binära representationen av i. Det här är en kontrollmatris till en Hammingkod av redundans r, och kallas för den lexikografiska kontrollmatrisen.

Exempel 7.2.4. Vi skriver ned de tre första lexikografiska kontrollmatriserna

$$H_1 = [1],$$
$$H_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},$$
$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Det finns ett väldigt enkelt att sätt att felrätta med en hammingkod.

Sats 7.2.5. *Låt C vara en hammingkod av redundans r och säg att vi vill felrätta $w \in (\mathbb{Z}/(2))^{2^r-1}$. Låt H_r vara den lexikografiska kontrollmatrisen till C. Antingen är $H_r w = 0$ vilket innebär att inget fel har skett. Om $H_r w$ inte är 0, är det en binär representation av ett tal $0 \leqslant j \leqslant 2^r - 1$. Det är då i plats j felet har skett.*

Bevis. Säg att $w \in (\mathbb{Z}/(2))^{2^r-1}$ har blivit fel i position j, så $w = c + e_j$ där $c \in C$ och

$$e_j = (0, 0, \ldots, \underbrace{1}_{\text{position } j}, \ldots, 0).$$

Då är

$$H_r w = H_r(c + e_j) = H_r c + H_r e_j = 0 + H_r e_j = h_j,$$

där h_j är kolumn nummer j i H_r. Men h_j är den binära representationen av talet j, vilket skulle visas. □

Det går att konstruera Hammingkoder över $\mathbb{Z}/(p)$ med samma princip. Vi vill kunna rätta ett fel. Säg att vi väljer redundans r, så att vår kontrollmatris H har r rader. Då vill vi välja kolumner så att vilka två av dem som helst är linjärt oberoende. Vår första kolumn h_1 kan vara vilken kolumn som helst förutom 0, så vi har

$$|(\mathbb{Z}/(p))^r| - 1 = p^r - 1$$

valmöjligheter. Vårt andra val kan vara vilken vektor som helst utom 0 och en vektor på formen sh_0, $s \in \mathbb{Z}/(p) - \{0\}$. Det finns alltså

$$|(\mathbb{Z}/(p))^r| - 1 - |\mathbb{Z}/(p) \setminus \{0\}| = p^r - 1 - (p - 1)$$

sådana valmöjligheter. Fortsätter vi på samma sätt ser vi att det finns

$$p^r - 1 - i(p - 1)$$

möjligheter för kolumn nummer i. Vi kommer att få slut på val då

$$0 = p^r - 1 - i(p - 1) \iff i = \frac{p^r - 1}{p - 1}.$$

Definition 7.2.6. En kod med kontrollmatris H över $\mathbb{Z}/(p)$ av storlek

$$r \times ((p^r - 1)/(p - 1))$$

där ingen av kolumnerna är multiplar av andra kolumner är en hammingkod över $\mathbb{Z}/(p)$ av redundans r.

Hjälpsats 7.2.7. *Låt C vara en Hammingkod över $\mathbb{Z}/(p)$ av redundans r. Då är $|C| = p^k$ element där*

$$k = \frac{p^r - 1}{p - 1} - r$$

Bevis. Vår kontrollmatris H har

$$n = \frac{p^r - 1}{p - 1}$$

kolumner av längd r. Då

$$\frac{p^r - 1}{p - 1} \geqslant p^{r-1}$$

genererar kolumnerna ett rum av dimension r. Alltså är $\dim V(H) = r$. Ett kodord w ligger i C om och endast om $w \in N(H)$. Vi vet att

$$\dim N(H) = n - \dim V(H) = \frac{p^r - 1}{p - 1} - r.$$

□

Vi har nu en väldigt lång lista av perfekta koder.

Sats 7.2.8. *Alla Hammingkoder är perfekta.*

Bevis. Vi måste visa att likhet i Sats 7.1.5 gäller. Längden på våra kodord är

$$n = \frac{p^r - 1}{p - 1},$$

då vår kontrollmatris H har så många kolumner. Eftersom

$$|C| = p^k, \quad k = n - r$$

där C är en Hammingkod över $\mathbb{Z}/(p)$ med redundans r, och $d(C) = 3$, blir olikheten

$$\binom{n}{0} + \binom{n}{1}(p-1)^1 \leqslant p^{r-k},$$

där

$$k = n - r.$$

Vi skriver om olikheten till

$$\begin{aligned} & 1 + n(p-1) \leqslant p^r \\ \iff & 1 + \frac{p^r - 1}{p - 1}(p-1) \leqslant p^r \\ \iff & 1 + p^r - 1 \leqslant p^r \\ \iff & p^r \leqslant p^r. \end{aligned}$$

Vi har alltså likhet, vilket skulle visas. □

7.3 Klassificering av perfekta koder

Det visar sig att det totalt finns väldigt få linjära perfekta koder, och att Hammingkoderna utgör nästan alla.

Definition 7.3.1. En *repetitionskod* av längd n är en kod på formen

$$C = \{(a, a, a, \ldots, a) \mid a \in \mathbb{Z}/(p)\}.$$

Om $n = 2k + 1$ är udda gäller det att $d(C) = k$.

En repetitionskod är endast perfekt om den är över $\mathbb{Z}/(2)$ och har udda längd, men vi återlämnar det beviset till övningarna. Vi kallar en sådan kod för en *binär repetitionskod*. De är nu endast två till koder som är perfekta.

Definition 7.3.2. Den binära Golay koden, G_{23}, är en kod över $\mathbb{Z}/(2)$ med kontrollmatris

$$H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0
\end{bmatrix}$$

Det är en perfekt kod med separation 7. Den ternära Golay koden, G_{11}, är en kod över $\mathbb{Z}/(3)$ med kontrollmatris

$$H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\
1 & 2 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 2 \\
0 & 1 & 2 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 2 \\
0 & 0 & 1 & 2 & 0 & 2 & 2 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 2 & 0 & 2 & 2 & 1 & 1 & 1
\end{bmatrix}.$$

Det är en perfekt kod med separation 5.

Vi kan nu nämna (men inte bevisa) följande förvånande sats

Sats 7.3.3. *Låt C vara en perfekt linjär kod. Då är C ekvivalent med en av följande:*

- *En binär repetitionskod.*
- *En Hammingkod.*
- G_{23}.
- G_{11}.

Övningar

Övning 7.1. Hur många element finns i $B(2, (0, 0, 0))$ över $\mathbb{Z}/(5)$?

Övning 7.2. Vad är den binära formen av 21, 12 och 17 av längd 5?

Övning 7.3. Betrakta den lexikografiska hamiltonkoden

$$H_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Använd den för att rätta meddelande

$$v = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

Övning 7.4. Hitta en kontrollmatris H till en Hamiltonkod av redundans 2 över $\mathbb{Z}/(3)$.

Övning 7.5. Visa att en binär repetitionskod av udda längd är perfekt.

8 Reed-Solomon koder

I det här kapitlet ska vi konstruera en familj av koder med väldigt hög separation. Från Följdsats 6.2.5 såg vi att separationen av en kod C med blocklängd m och kodlängd n har den övre begränsningen

$$d(C) \leqslant n - m + 1.$$

Koderna som vi konstruerar här kommer uppnå den här begränsningen givet att koden är över $\mathbb{Z}/(p)$ där $p \geqslant n$.

Vi kommer dock börja med att beskriva en viss typ av polynom över $\mathbb{Z}/(p)$.

8.1 Polynom

Definition 8.1.1. Ett *polynom*[5] över $\mathbb{Z}/(p)$ är en funktion $P : \mathbb{Z}/(p) \to \mathbb{Z}/(p)$ där det existerar några koefficienter $a_0, \ldots, a_{p-1} \in \mathbb{Z}_p$ så att

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1}$$

för alla $x \in \mathbb{Z}/(p)$.

Exempel 8.1.2. Över $\mathbb{Z}/(2)$ finns det 4 stycken polynom definierade av

$$\begin{aligned} x &\mapsto 0, \\ x &\mapsto 1, \\ x &\mapsto x, \\ x &\mapsto 1 + x. \end{aligned}$$

för alla $x \in \mathbb{Z}_p$.

Vi säger att ett polynom P har grad $d \leqslant p - 1$ om P kan skrivas på formen

$$P(x) = a_0 + \cdots + a_d x^d$$

för alla $x \in \mathbb{Z}/(p)$ och för några koefficienter $a_0, \ldots, a_d \in \mathbb{Z}/(p)$ där $a_d \neq 0$. Alla polynom förutom polynomet $P(x) = 0$ har en grad.

Vi påpekar att vi ännu än inte har visat att samma polynom inte kan skrivas på olika sätt och därmed har inte ännu exkluderat möjligheten att ett polynom har flera olika olika grader.

Hjälpsats 8.1.3. *Låt $P, Q : \mathbb{Z}/(p) \to \mathbb{Z}/(p)$ vara två polynom av grad $d, h \leqslant p - 1$.*

(i) *Om $d + h \leqslant p - 1$ är produkten PQ givet av $PQ : x \mapsto P(x)Q(x)$ för alla $x \in \mathbb{Z}/(p)$ ett polynom av grad $d + h$.*

(ii) *Om $H : \mathbb{Z}/(p) \to \mathbb{Z}/(p)$ är givet av $H(x) = P(a - x)$ för alla $x \in \mathbb{Z}/(p)$ och något $a \in \mathbb{Z}/(p)$ är H ett polynom av grad d.*

[5] Det finns även andra sätt att definiera polynom över $\mathbb{Z}/(p)$. Mängden av polynom som vi beskriver här burkar noteras som $(\mathbb{Z}/(p))[x]/(1 - x^p)$.

Bevis. (i) Låt

$$P(x) = a_0 + \cdots + a_d x^d$$
$$Q(x) = b_0 + \cdots + b_h x^d$$

för alla $x \in \mathbb{Z}/(p)$ och för några koefficienter $a_0, \ldots, a_d, b_0, \ldots, b_h \in \mathbb{Z}/(p)$ där $a_d, b_h \neq 0$. Då har vi att

$$\begin{aligned} P(x)Q(x) &= (a_0 + \cdots + a_d x^d)(b_0 + \cdots + b_h x^d) \\ &= a_d b_h x^{d+h} + (a_{d-1} b_h + a_d b_{h-1}) x^{d+h-1} + \cdots + a_0 b_0 \end{aligned}$$

för alla $x \in \mathbb{Z}/(p)$. Då $a_d b_h \neq 0$ har PQ grad $d+h$ om $d+h \leqslant p-1$.

(ii) Vi har att

$$H(x) = P(a-x) = a_0 + a_1(a-x) + \cdots + a_d(a-x)^d$$

för alla $x \in \mathbb{Z}/(p)$. Då $a-x$ är ett polynom av grad 1 kommer $(a-x)^d$ vara ett polynom grad d enligt (ii). Därmed kommer termen $a_d(a-x)^d$ vara ett polynom av grad d. Av samma anledning kommer alla andra termer vara polynom av lägre grad än d så de kan inte påverka koefficienten framför x^d. Därmed kommer H ha grad d.

□

Ett *nollställe* eller *rot* av ett polynom P över $\mathbb{Z}/(p)$ är ett tal $x \in \mathbb{Z}/(p)$ så att $P(x) = 0$.

Sats 8.1.4 (Faktorsatsen)**.** *Låt P vara ett polynom av grad $d \leqslant p-1$ över $\mathbb{Z}/(p)$. Då är $a \in \mathbb{Z}/(p)$ ett nollställe till P om och endast om det finns något polynom G av grad $d-1$ så att*

$$P(x) = (a-x)G(x)$$

för alla $x \in \mathbb{Z}/(p)$.

Bevis. Om $P(x) = (a-x)G(x)$ ser vi direkt att $P(a) = 0$. Anta nu istället att $P(a) = 0$. Vi låter nu $H(x) = P(a-x)$ för alla $x \in \mathbb{Z}/(p)$. Enligt Sats 8.1.3 är H är ett polynom av grad d. Vi kan då skriva

$$H(x) = c_0 + \cdots + c_d x^d$$

för några koefficienter $c_0, \ldots, c_d \in \mathbb{Z}/(p)$ där $c_d \neq 0$. $H(0) = P(a-0) = 0$ så $c_0 = 0$. Vi kan nu skriva

$$H(x) = x(c_1 + c_2 x + \cdots c_d x^{d-1})$$

för alla $x \in \mathbb{Z}/(p)$. Låt $K(x) = (c_1 + c_2 x + \cdots c_d x^{d-1})$ för alla $x \in \mathbb{Z}/(p)$. Då $c_d \neq 0$ är K ett polynom av grad $d-1$. Nu har vi att

$$P(x) = H(a-x) = (a-x)K(a-x)$$

för alla $x \in \mathbb{Z}/(p)$. Vi kan nu definiera $G(x) = K(a-x)$ för alla $x \in \mathbb{Z}/(p)$. Enligt Sats 8.1.3 är G ett polynom av grad $d-1$ som vi ville. □

Sats 8.1.5. *Låt P vara ett polynom över $\mathbb{Z}/(p)$ av grad $d \leqslant p-1$. Då har P som mest d nollställen.*

Bevis. Anta att P har åtminstone $d+1$ nollställen $x_1, \ldots, x_{d+1}$. Om vi nu använder Faktorsatsen 8.1.4 upprepat kan vi skriva P som

$$P(x) = (x_1 - x)(x_2 - x)\cdots(x_d - x)G(x)$$

för alla $x \in \mathbb{Z}/(d)$ och för ett polynom $G(x)$ av grad 0. Men då är G en nollskild konstant. Vi har nu att

$$P(x_{d+1}) = (x_1 - x_{d+1})(x_2 - x_{d+1})\cdots(x_d - x_{d+1})G \neq 0$$

då alla faktorer är nollskilda. Men detta är en motsägelse. □

Följdsats 8.1.6. *Låt P vara ett polynom över $\mathbb{Z}/(p)$. Då finns det exakt en uppsättning koefficienter $a_0, \ldots, a_{p-1}$ så att*

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1}x^{p-1}$$

för alla $x \in \mathbb{Z}/(p)$.

Beviset lämnar vi till en övning.

8.2 Vandermondematriser

Definition 8.2.1. En $n \times m$ Vandermondematris V över F är en matris på formen

$$V = \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{m-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{m-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \cdots & a_{n-1}^{m-1} \end{bmatrix}$$

för några distinkta element $a_0, \ldots, a_{n-1} \in F$.

Ifall $F = \mathbb{Z}/(p)$ är det nödvändigt att $n \leqslant p$ för att det ska finnas n stycken distinkta element $a_0, \ldots, a_n \in \mathbb{Z}/(p)$.

Exempel 8.2.2. Fixera $m \geqslant 1$. Över $\mathbb{Z}_2$ finns det då fyra $n \times m$ Vandermondematriser. Dessa är

$$\begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 1 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Sats 8.2.3. *Alla kvadratiska Vandermondematriser över $\mathbb{Z}/(p)$ är inverterbara.*

Bevis. Låt

$$V = \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{d-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{d-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{d-1} & a_{d-1}^2 & \cdots & a_{d-1}^{d-1} \end{bmatrix}$$

vara en kvadratisk $(d-1) \times (d-1)$ över $\mathbb{Z}/(p)$, $d \leqslant p$, för några distinkta konstanter $a_0, \ldots, a_{d-1} \in \mathbb{Z}/(p)$. Vi visar att $N(V) = \{0\}$. Låt $v = \{v_0, \ldots, v_{d-1}\} \in N(V)$. Då kommer

$$\begin{aligned} Vv &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{d-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{d-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{d-1} & a_{d-1}^2 & \cdots & a_{d-1}^{d-1} \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{d-1} \end{bmatrix} \\ &= \begin{bmatrix} v_0 & + & v_1 a_0 & + & \cdots & + & v_{d-1} a_0^{d-1} \\ v_0 & + & v_1 a_1 & + & \cdots & + & v_{d-1} a_1^{d-1} \\ v_0 & + & v_1 a_2 & + & \cdots & + & v_{d-1} a_2^{d-1} \\ & & & & \vdots & & \\ v_0 & + & v_1 a_{d-1} & + & \cdots & + & v_{d-1} a_{d-1}^{d-1} \end{bmatrix}. \end{aligned}$$

Vi ser därmed att om vi definierar polynomet

$$P(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_{d-1} x^{d-1}$$

för alla $x \in \mathbb{Z}/(p)$ så kommer $a_0, \ldots, a_{d-1}$ vara nollställen till P. Om $P = 0$ är $v_0, \ldots, v_{d-1} = 0$ och vi är klara. Annars har P någon grad $g \leqslant d-1$. Men enligt Sats 8.1.5 kan P ha som mest $d-1$ stycken nollställen vilket är en motsägelse. □

8.3 Reed-Solomon koder

Definition 8.3.1. En *Reed-Solomon* kod $C \subset (\mathbb{Z}/(p))^n$ med kodordslängd $n \leqslant p$ och blocklängd m är en kod där $(n-m) \times n$ kontrollmatrisen H kan skrivas som

$$H = V^T$$

där V är en $n \times (n-m)$ Vandermondematris över $\mathbb{Z}/(p)$.

Sats 8.3.2. *Alla $(n-m) \times n$ matriser på formen*

$$H = V^T$$

för en $n \times (n-m)$ Vandermondematris över $\mathbb{Z}/(p)$ är en kontrollmatris till en kod $C = N(H) \subset (\mathbb{Z}/(p))^{n-m}$.

Bevis. Låt

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & & \vdots \\ a_0^{n-m-1} & a_1^{n-m-1} & \cdots & a_{n-1}^{n-m-1} \end{bmatrix}$$

där $a_0, \ldots, a_{n-1}$ är distinkta. För att H ska vara en kontrollmatris måste H vara surjektiv. Vi har att $n-m \times n-m$ matrisen

$$\begin{bmatrix} 1 & a_0 & \cdots & a_0^{n-m-1} \\ 1 & a_1 & \cdots & a_1^{n-m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-m-1} & \cdots & a_{n-m-1}^{n-m-1} \end{bmatrix}$$

är inverterbar enligt Sats 8.2.3. Därmed är dess rader linjärt oberoende och H har därför $n-m$ linjärt oberoende kolumner. Det följer att $\dim V(H) = n-m$ vilket medför att $V(H) = \mathbb{Z}^{n-m}$. Därmed är H surjektiv. Vi låter $C = N(H)$ som i satsen. För att C ska vara en kod måste C ha dimension m. Enligt Dimensionssatsen 4.3.4 är $\dim N(H) = n - \dim V(H) = n - (n-m) = m$. □

Sats 8.3.3. *En Reed-Solomon kod $C \subset (\mathbb{Z}/(p))^n$ med blocklängd m har separation $d(C) = n - m + 1$.*

Bevis. Låt

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & & \vdots \\ a_0^{n-m-1} & a_1^{n-m-1} & \cdots & a_{n-1}^{n-m-1} \end{bmatrix}$$

där $a_0, \ldots, a_{n-1}$ är distinkta.

Enligt Sats 6.2.5 har C separation $n-m+1$ om och endast om alla val av $n-m$ kolumner är linjärt oberoende och det finns $n-m+1$ linjärt beroende kolumner. Betrakta nu matrisen

$$\begin{bmatrix} 1 & a_{k_0} & \cdots & a_{k_0}^{n-m-1} \\ 1 & a_{k_1} & \cdots & a_{k_1}^{n-m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{k_{n-m-1}} & \cdots & a_{k_{n-m-1}}^{n-m-1} \end{bmatrix}$$

för något urval $k_0, \ldots, k_{n-m-1} \subset \{0, \ldots, n-1\}$, $k_i \neq k_j$ då $i \neq j$. Enligt Följdsats 8.2.3 är matrisen inverterbar så raderna är linjärt oberoende. Därmed är alla val av $n-m$ kolumner av H linjärt oberoende. Det återstår att visa att H har $n-m+1$ linjärt beroende kolumner. Men väljer vi vilka $n-m+1$ kolumner som helst måste de vara linjärt beroende då $\dim V(H)$ annars skulle ha varit större än $n-m$. □

Exempel 8.3.4. Låt $p = n = 11$ och $m = 4$. Då kan vi skapa en kod Reed-Solomon kod $C \subset \mathbb{Z}/(11)^{11}$ med kontrollmatris

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 1 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 \\ 0 & 1 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 & 8^3 & 9^3 & 10^3 \\ 0 & 1 & 2^4 & 3^4 & 4^4 & 5^4 & 6^4 & 7^4 & 8^4 & 9^4 & 10^4 \\ 0 & 1 & 2^5 & 3^5 & 4^5 & 5^5 & 6^5 & 7^5 & 8^5 & 9^5 & 10^5 \\ 0 & 1 & 2^6 & 3^6 & 4^6 & 5^6 & 6^6 & 7^6 & 8^6 & 9^6 & 10^6 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \\ 0 & 1 & 8 & 5 & 9 & 4 & 7 & 2 & 6 & 3 & 10 \\ 0 & 1 & 5 & 4 & 3 & 9 & 9 & 3 & 4 & 5 & 1 \\ 0 & 1 & 10 & 1 & 1 & 1 & 10 & 10 & 10 & 1 & 10 \\ 0 & 1 & 9 & 3 & 4 & 5 & 5 & 4 & 3 & 9 & 1 \end{bmatrix}.$$

Från Sats 8.3.3 har vi att $d(C) = n - m + 1 = 8$ så koden kan upptäcka 7 fel samt rätta 3 fel.

Övningar

Övning 8.1. Visa Följdsats 8.1.6.

Övning 8.2 ($\star$)**.** (i) Hur många polynom över $\mathbb{Z}/(p)$ finns det? Hur många funktioner från $\mathbb{Z}/(p)$ till $\mathbb{Z}/(p)$ finns det? Är alla funktioner polynom?

(ii) Definiera $f : \mathbb{Z}/(3) \to \mathbb{Z}/(3)$ genom att $f(0) = f(1) = 1$ och $f(2) = f(2)$. Är f ett polynom? Vad har f för grad?

Övning 8.3. Konstruera en kod med blocklängd 4, kodordslängd 8 och separation 5 över $\mathbb{Z}/(17)$.

Övning 8.4 ($\star$)**.** Låt $C \subset (\mathbb{Z}/(7))^4$ vara en Reed-Solomon kod med en 2×4 kontrollmatris

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{bmatrix}.$$

(i) Vad är blocklängden och separationen av C?

(ii) Finn en generatormatris till C.

Lösningar till övningsuppgifterna

Kapitel 1

Övning 1.1. (i) 0, 1, 2, 3, 4.

(ii) 1, 2, $\{2, 3\}$.

(iii) -3, -2, -1, 0, 1, 2, 3.

(iv) 1, 2.

(v) -3, -2, -1, 1, 2, $\{2, 3\}$.

Övning 1.2. (i) Mängden är tom.

(ii) 0, 1, 2, 3.

(iii) 0, 1, 2, 1/2.

(iv) 0, 1, 2.

(v) 0, 1, 2.

Övning 1.3. (i) B är en äkta delmängd av A.

(ii) A och B är lika.

(iii) Mängderna är disjunkta eftersom $B = \emptyset$ och alla mängder är disjunkta med den tomma mängden. B är en äkta delmängd till A.

(iv) Mängderna är varken disjunkta, lika eller äkta delmängder av varandra.

(v) Mängderna är disjunkta eftersom $A = \emptyset$.

Övning 1.4. (i) A och B är lika.

(ii) B är en äkta delmängd av A.

(iii) A och B är varken lika, disjunkta eller äkta delmängder av varandra.

(iv) A och B är disjunkta.

(v) B är en äkta delmängd av A.

Övning 1.5. Observera att dessa svar är förslag. Uppgifterna har flera korrekta svar.

(i) $\{n \in \mathbb{Z} \mid n = 2k \text{ för något heltal } k \geqslant 1\}$.

(ii) $\{p/2 \mid p \text{ är ett heltal }\}$.

(iii) $\{r \in \mathbb{R} \mid r \notin \mathbb{Q} \text{ och } |r| < 1\}$.

Övning 1.6. Observera att dessa svar är förslag. Uppgifterna har flera korrekta svar.

(i) $\{n \in \mathbb{Z} \mid n = k^2 \text{ för något heltal } k \geqslant 2\}$.

(ii) $\{x \in \mathbb{Q} \mid x^4 + x^2 - 1 = 0\}$.

(iii) $\{x \in \mathbb{R} \mid x = r^3 \text{ för något } r \in \mathbb{Q}\}$.

Övning 1.7. (i) Definitionsmängd: $\{1, 2, 3, \ldots\}$. Målmängd: $\mathbb{N}$.

(ii) Definitionsmängd: $\{T \mid T \text{ är en triangel }\}$. Målmängd: $\mathbb{R}$.

(iii) Definitionsmängd: $\{p(x) \mid p(x) \text{ är ett andragradspolynom}\}$. Målmängd: $\{p(x) \mid p(x) \text{ är ett förstagradspolynom}\}$.

Övning 1.8. (i) Definitionsmängd: $\{r \in \mathbb{R} \mid r \geqslant 0\}$. Målmängd: $\{r \in \mathbb{R} \mid r \geqslant 0\}$.

(ii) Definitionsmängd: $\mathbb{R}$. Målmängd: $\{r \in \mathbb{R} \mid r \geqslant 0\}$.

(iii) Definitionsmängd: $\{px + q \mid p, q \in \mathbb{Q}\}$. Målmängd: $\mathbb{Q}$.

Övning 1.9. (i) Detta är en funktion. Den är definierad för alla värden i definitionsmängden, den ger alltid samma värde för ett givet argument, och alla funktionsvärden ligger i målmängden.

(ii) Detta är inte en funktion, då funktionens värden inte ligger i målmängden ($f(2) = \sqrt{2} \notin \mathbb{Q}$).

(iii) Detta är inte en funktion, eftersom dess värden är slumpmässiga.

(iv) Detta är en funktion. Eftersom ordet Balkong börjar på B, så har funktionen ett definierat värde som ligger i målmängden.

Övning 1.10. (i) Detta är en funktion, då varje heltal skrivs på bara ett sätt i talsystemet.

(ii) Detta är inte en funktion, eftersom funktionens värden inte alltid ingår i målmängden.

(iii) Detta är en funktion, då den är definierad och unik för alla naturliga tal.

(iv) Detta är inte en funktion, eftersom samma rationella tal kan skrivas på olika sätt. Till exempel så är $1/2 = 2/4$, medan $f(1/2) = 1$ och $f(2/4) = 2$.

Övning 1.11. (i) Funktionerna är lika. De har samma definitionsmängd, målmängd och $\sqrt{x^2} = |x|$ för alla x.

(ii) Funktionerna är inte lika, då deras definitionsmängder inte är samma.

(iii) Funktionerna är inte lika, då deras målmängder är olika.

Övning 1.12. (i) Funktionerna är lika. De har samma definitionsmängd, målmängd och $(x + 1)^2 = x^2 + 2x + 1$.

(ii) Funktionerna är lika. De har samma definitionsmängd, målmängd och $x^2 = |x|^2$ (kom ihåg att $(-x)^2 = (-1)^2 x^2 = x^2$).

Övning 1.13. I exempel 1.5.3 är värdemängden $\{3, 4\}$. Funktionen är inte injektiv och inte surjektiv. I exempel 1.5.4 är värdemängden $\{0, 1\}$ och funktionen är bijektiv, alltså surjektiv och injektiv.

Övning 1.14. Antag att $x_1 \neq x_2$, då kan vi anta utan förlust av generalitet att $x_1 < x_2$. Per definition $f(x_1) < f(x_2) \implies f(x_1) \neq f(x_2)$. Alltså måste olika x ge olika funktionsvärden.

Övning 1.15. Vi gör ett direkt bevis. Om $A \cap B = \emptyset$ betyder det att inga element i A tas bort i $A \setminus B$. Alltså har vi $A \cap B = \emptyset \implies A \setminus B = A$. På samma sätt har vi att om $A \setminus B = A$ betyder det att det inte finns några gemensamma element i A och B som tas bort i $A \setminus B$, alltså har vi $A \setminus B = A \implies A \cap B = \emptyset$.

Övning 1.16. Vi gör ett direkt bevis. Det räcker att visa $(A \cup B)^C = A^C \cap B^C$ eftersom det andra påståendet följer från det i och med att alla mängder är komplementet till sitt komplement.

$$(A \cup B)^C = \{x \mid x \notin A \text{ och } x \notin B\} = A^C \cap B^C.$$

Övning 1.17. Vi gör ett direkt bevis. Mängden $A \setminus B$ är mängden av element som ligger i A och inte i B. Alltså är det mängden vi får när vi 'tar bort elementen som ligger i B *från* A'. Alltså tar vi egentligen bara bort elementen som ligger i $A \cap B$ från A. De som inte låg i A från första början struntar vi alltså i.

Övning 1.18. Vi gör ett direkt bevis. Låt $g : X \to Y$ och $f : Y \to Z$ vara bijektioner. Vi verifierar att $f \circ g$ är injektiv,

$$(f \circ g)(x) = (f \circ g)(y) \overset{f \text{ injektiv}}{\implies} g(x) = g(y) \overset{g \text{ injektiv}}{\implies} x = y.$$

På samma sätt ser vi att funktionen är surjektiv eftersom bilden av $f \circ g$ är bilden med f av värdemängden för g. Eftersom g är surjektiv blir bilden för $f \circ g$ densamma som bilden för f och eftersom f antas vara surjektiv har vi att bilden av f är hela Z. Alltså är $f \circ g$ surjektiv.

Övning 1.19. Detta följer från definitionerna. Kom ihåg att potensmängden 2^A är mängden av delmängder till A, och $A/\sim$ är en mängd vars element är vissa (men inte alla) delmängder till A.

Övning 1.20. Vi gör ett direkt bevis. Hur många par av element A respektive B finns det? Jo, exakt lika många som det finns sätt att välja ett element ur den ena och sedan den andra vilket är $(|A|) \cdot (|B|)$.

Övning 1.21. Vi gör ett direkt bevis. För varje par $(b, y) \in B \times Y$ har vi per definition att $b \in B$ och $y \in Y$ och med antagandet $B \subset A$ och $Y \subset X$ betyder det att $b \in A$ och $y \in X$ vilket betyder att $(b, y) \in A \times X$.

Övning 1.22. Vi löser problemet genom att konstruera den inversa funktionen. Notera att vi har en funktion

$$\begin{aligned} \phi : &\{0,1\}^A \to \{B \mid B \subset A\} \\ &f \mapsto \{a \in A \mid f(a) = 1\}. \end{aligned}$$

Det är nu tydligt att $\phi \circ \chi$ och $\chi \circ \phi$ är varandras inverser.

Övning 1.23. Om n är jämnt så finns det per definition ett heltal k så att $n = 2k$. Då gäller att $n + 1 = 2k + 1$, det vill säga $n + 1$ är udda.

Övning 1.24. Om n är udda, så finns det ett heltal k så att $n = 2k + 1$. Då gäller att

$$n^2 = (2k + 1)(2k + 1) = 4k^2 + 2k + 2k + 1 = 2\left(2k^2 + 2k\right) + 1.$$

Eftersom $2k^2 + 2k$ är ett heltal, bevisar detta att n^2 är udda.

Övning 1.25. Antag motsatsen, det vill säga att det finns ett rationellt tal p/q och ett irrationellt tal r vars summa är rationell. Skriv summan som kvoten s/t. Då gäller

$$\frac{p}{q} + r = \frac{s}{t} \implies r = \frac{s}{t} - \frac{p}{q} = \frac{sq - pt}{tq}$$

genom att skriva vänsterledet på gemensamt bråkstreck. Men detta bevisar att r är rationellt, vilket är en motsägelse.

Övning 1.26. Antag motsatsen, det vill säga att $a < c/2$, $b < c/2$ och $a + b \geqslant c$. Då gäller att

$$a + b < c/2 + b < c/2 + c/2 = c.$$

Alltså gäller $a + b < c$, vilket är en motsägelse.

Övning 1.27. Antag motsatsen till satsen. Den kan delas in i två fall. I det ena fallet gäller att $ab = c$ och $a < \sqrt{c}$ och $b < \sqrt{c}$. Då gäller att

$$ab < a\sqrt{c} < \sqrt{c}\sqrt{c} = \sqrt{c}^2 = c.$$

Alltså gäller $ab < c$, vilket är en motsägelse.

I det andra fallet gäller att $ab = c$ och $a > \sqrt{c}$ och $b > \sqrt{c}$. Då gäller att

$$ab > a\sqrt{c} > \sqrt{c}\sqrt{c} = \sqrt{c}^2 = c.$$

Alltså gäller $ab > c$, vilket är en motsägelse.

Övning 1.28. Sätt $a = b = \sqrt{2}$. Om a^b är rationellt så är vi klara, för då är a och b irrationella tal så att a^b är rationellt. Om a^b är irrationellt, så kan vi sätta $c = a^b$ och få att

$$c^b = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

vilket är rationellt.

Kommentar: *Beviset säger oss bara att något av fallen gäller, inte vilket. Man säger att beviset är icke-konstruktivt.*

Övning 1.29. Låt $r = p/q$ vara ett rationellt tal. Genom att förlänga med $\sqrt{2}$ kan vi skriva

$$r = \sqrt{2}\frac{r}{\sqrt{2}}.$$

Vi vet att $\sqrt{2}$ är irrationellt. Om vi kunde visa att $r/\sqrt{2}$ är irrationellt så vore vi klara.

Antag motsatsen, det vill säga att $r/\sqrt{2}$ är en kvot av två heltal a och b. Genom algebraiska manipulationer får vi att

$$\frac{r}{\sqrt{2}} = \frac{a}{b} \implies \frac{1}{\sqrt{2}} = \frac{qa}{pb} \implies \sqrt{2} = \frac{pb}{qa}.$$

Men detta innebär att $\sqrt{2}$ är rationellt, vilket är en motsägelse. Alltså är $r/\sqrt{2}$ irrationellt, vilket avslutar vårt bevis.

Övning 1.30. För det första påståendet gör vi ett direkt bevis. Om $r = n$ finns det inget att visa, så antag att $r < n$. Detta är ekvivalent med existensen av ett positivt heltal tal k sådan att $n = r + k$. Då produkten av två positiva heltal är ett positivt heltal kan vi skriva

$$mr < mr + mk = m(r + k) = mn.$$

För det andra påståendet gör vi ett motsägelsebevis. Antag att $r < n$ och att det finns ett positivt heltal k sådant att $r = nk$. Då kan vi med den tidigare uppgiften se att

$$1 \leqslant k \implies n \leqslant nk.$$

I sin tur har vi då att $r < n \leqslant nk = r$. Det är en motsägelse att ett tal är mindre än sig självt.

För det tredje påståendet så gör vi ett direkt bevis.

$$nk - n\ell = n(k - \ell).$$

Kapitel 2

Övning 2.1. Sista siffran till 11^{34567} är principalresten av talet modulo 10. Vi vet att

$$11^{34567} \equiv 1^{34567} \equiv 1 \mod 10.$$

Övning 2.2. (i) Vi räknar modulo 7. Då varje år har 365 dagar exklusive skottår får vi

$$10^9 \cdot 365 \equiv 3^9 \cdot 1 \equiv 9 \cdot 9 \cdot 9 \cdot 9 \cdot 3 \equiv 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \equiv 6 \mod 7.$$

Det är alltså 6 dagar i framtiden, vilket blir Söndag.

(ii) Vi vill lägga till en extra dag var fjärde år på den föregående beräkningen. Vi får då

$$6 + 10^9/4 \equiv 6 + 100/4 \cdot 10^7 \equiv 6 + 25 \cdot 3^7$$
$$\equiv 6 + 4 \cdot 9 \cdot 9 \cdot 9 \cdot 3 \equiv 6 + 4 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \equiv 4 \mod 7.$$

Det är 4 dagar i framtiden den här gången, vilket blir fredag.

Övning 2.3. Ett tresiffrigt tal är ett tal på formen

$$a + b \cdot 10 + c \cdot 100.$$

Vi har att

$$a + b \cdot 10 + c \cdot 100 \equiv a + b \cdot 1 + c \cdot 1 \equiv a + b + c \mod 3.$$

Alltså är HL 0 om och endast om VL är 0, vilket skulle visas. Motsvarande bevis fungerar för 9.

Övning 2.4. Talet har formen

$$10^5a + 10^4b + 10^3c + 10^2d + 10e + f.$$

Vi vill räkna modulo 11, och

$$10 \equiv -1 \mod 11.$$

Det ger oss

$$\begin{aligned} &10^5a + 10^4b + 10^3c + 10^2d + 10e + f \\ \equiv\ &(-1)^5a + (-1)^4b + (-1)^3c + (-1)^2d + (-1)e + f \\ \equiv\ &-a + b - c + d - e + f \equiv -(a - b + c - d + e - f) \mod 11. \end{aligned}$$

Det här är 0 om och endast om $a - b + c - d + e - f$ är 0.

Övning 2.5. (i) $2 + 3 = 5$.

(ii) $16 \cdot 10 = 160$, vilket har principalrest 10 modulo 25.

(iii) -13 i $\mathbb{Z}/(25)$ är $25 - 13 = 12$.

(iv) -13 i $\mathbb{Z}/(25)$ är $25 - 24 = 1$, så $1 - 24 = 1 + 1 = 2$.

(v) $10^3 = 100$ som är delbart med 25, så $100 = 0$ i $\mathbb{Z}/(25)$.

Övning 2.6. Vi använder räkneregeln i hjälpsats 2.2.8 som säger att

$$a(b + c) = ab + ac.$$

Vi får bland annat att

$$0 = x \cdot 0 = x \cdot (1 - 1) = x + (-1) \cdot x.$$

Nu adderar vi $-x$ till båda sidor och får

$$-x = x - x + (-1) \cdot x \iff -x = -1 \cdot x.$$

Övning 2.7. Vi har att

$$0 = (-1) \cdot 0 = (-1) \cdot (1 + (-1)) = (-1) \cdot 1 + (-1) \cdot (-1).$$

Från föregående uppgift vet vi att $(-1) \cdot 1 = -1$. Vi kan nu addera 1 till båda sidor och får

$$1 = -1 + 1 + (-1) \cdot (-1) = (-1) \cdot (-1).$$

Övning 2.8. (i) Eftersom $3 \cdot 3 = 1$ i $\mathbb{Z}/(4)$, så gäller $3^{-1} = 3$.

(ii) Eftersom $2 \cdot 3 = 1$ i $\mathbb{Z}/(5)$, så gäller $3^{-1} = 2$.

(iii) Vi har

$$0 \cdot 3 = 0, 1 \cdot 3 = 3, 2 \cdot 3 = 0, 3 \cdot 3 = 3, 4\dot{3} = 0, 5 \cdot 3 = 3,$$

i $\mathbb{Z}/(6)$. Då ingen av dessa är 1, har 2 ingen multiplikativ invers i det här fallet.

(iv) Eftersom $5 \cdot 3 = 1$ i $\mathbb{Z}/(7)$, så gäller $3^{-1} = 5$.

Övning 2.9. Om n är ett jämnt tal gäller det att $2\dot{n}/2 = 0$ i $\mathbb{Z}/(n)$. Om det skulle finnas en multiplikativ invers 2^{-1} till 2 skulle vi få

$$n/2 = (2^{-1} \cdot 2) \cdot n/2 = 2^{-1} \cdot (2 \cdot n/2) = 0.$$

Det här är en motsägelse.

Om istället n är ett udda tal är $(n+1)/2 \in \mathbb{Z}/(n)$, och

$$2 \cdot (n+1)/2 = n + 1 = 1$$

i $\mathbb{Z}/(n)$.

Kapitel 3

Övning 3.1. Vi beräknar

$$A + B = \begin{bmatrix} 2 & 0 & 7 \\ 12 & 2 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 11 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 2 \\ 12 & 3 & 11 \end{bmatrix},$$

$$sA = 3 \begin{bmatrix} 2 & 0 & 7 \\ 12 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 0 & 8 \\ 10 & 9 & 7 \end{bmatrix}.$$

Övning 3.2. Vi beräknar

$$AB = \begin{bmatrix} 3 & 4 & 1 \\ 0 & 5 & 2 \end{bmatrix} \begin{bmatrix} 3 & 4 \\ 0 & 5 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 3 \cdot 3 + 4 \cdot 0 + 1 \cdot 2 & 3 \cdot 3 + 4 \cdot 5 + 1 \cdot 2 \\ 0 \cdot 3 + 5 \cdot 0 + 2 \cdot 2 & 0 \cdot 3 + 5 \cdot 5 + 2 \cdot 2 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 4 & 1 \end{bmatrix}.$$

Övning 3.3. Låt de tre 2×2 matriser vi multiplicerar vara

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}, \quad B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}, \quad C = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}.$$

Vi beräknar nu

$$A(B + C) = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} b_1 + c_1 & b_2 + c_2 \\ b_3 + c_3 & b_4 + c_4 \end{bmatrix}$$

$$= \begin{bmatrix} a_1(b_1 + c_1) + a_2(b_3 + c_3) & a_1(b_2 + c_2) + a_2(b_4 + c_4) \\ a_3(b_1 + c_2) + a_4(b_3 + c_3) & a_3(b_2 + c_2) + a_4(b_4 + c_4) \end{bmatrix}.$$

Det här kan vi skriva om som

$$\begin{bmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{bmatrix} + \begin{bmatrix} a_1c_1 + a_2c_3 & a_1c_2 + a_2c_4 \\ a_3c_2 + a_4c_3 & a_3c_2 + a_4c_4 \end{bmatrix} = AB + AC.$$

Övning 3.4. Direkt uträkning ger

$$A^2 = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2}I.$$

Alltså kan vi räkna ut

$$A^3 = A^2 \cdot A = \frac{1}{2}I \cdot A = \frac{1}{2}A,$$

$$A^4 = A^2 \cdot A^2 = \frac{1}{2}I \cdot \frac{1}{2}I = \frac{1}{4}I.$$

Övning 3.5. Direkt uträkning ger

$$\|u\| = \sqrt{\langle u, u\rangle} = \sqrt{2^2 + 3^2 + (-1)^2} = \sqrt{14},$$

$$\|v\|^2 = \langle v, v\rangle = 1^2 + (-4)^2 + (-3)^2 = 26,$$

$$\langle u, v\rangle = 2 \cdot 1 + 3 \cdot (-4) + (-1) \cdot (-3) = -7.$$

Övning 3.6. Vi bara multiplicerar ihop

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} ad - bc & -ab + ab \\ dc - dc & -bc + ad \end{bmatrix} = I.$$

Övning 3.7. Låt M^{-1} vara inversen till M. Betrakta vektorerna

$$v = \begin{bmatrix} d \\ -c \end{bmatrix}, \quad w = \begin{bmatrix} b \\ -a \end{bmatrix}$$

Då är

$$Mv = \begin{bmatrix} ad - bc \\ dc - cd \end{bmatrix} = 0, \quad Mw = \begin{bmatrix} ba - ab \\ ad - bc \end{bmatrix} = 0.$$

Det här innebär att

$$v = M^{-1}Mv = M^{-1}0 = 0,$$

och av samma anledning är $w = 0$. Men då är $a = b = c = d = 0$, vilket innebär att $M = 0$. Det är inte en inverterbar matris, så vi har en motsägelse.

Övning 3.8. Vi multiplicerar ihop de två matriserna och får

$$(I - A)(I + A + A^2 + \ldots + A^{k-1})$$

$$= I + A + A^2 + \ldots + A^{k-1} - A(I + A + A^2 + \ldots + A^{k-1})$$

$$= I + A + A^2 + \ldots + A^{k-1} - A - A^2 - A^3 + \ldots - A^k)$$

$$= I - A^k = I.$$

Kapitel 4

Övning 4.1. (i) Ja, Här är ett sätt att se varför: Låt $v_1 = (1,2,3)$, $v_2 = (3,2,1)$, $v_3 = (1,0,0)$. Vi kan då skriva $e_1^3 = v_3, e_2^3 = \frac{1}{4}(3v_2 - v_1 - v_3)$ och $e_3^3 = \frac{1}{2}(v_1 - v_2 + 2v_3)$. Därmed är matrisen

$$\begin{bmatrix} 1 & 3 & 1 \\ 2 & 2 & 0 \\ 3 & 1 & 0 \end{bmatrix}$$

surjektiv så kolumnerna är linjärt oberoende.

(ii) Nej då $(1,2,3) + (3,2,1) = (0,0,0)$.

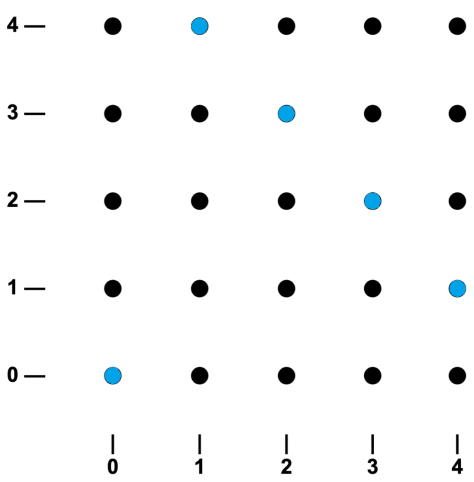
(iii) Nej då 0 ingår i mängden.

(iv) Ja, här är ett sätt att se varför: Låt $a, b, c \in (\mathbb{Z}/(2))$ vara koefficienter så att

$$0 = a(1,1,0,0) + b(1,1,1,0) + c(1,1,1,1).$$

Vi vill visa att $a, b, c = 0$. Vi får att $0 = (a+b+c, a+b+c, b+c, c)$ så $a+b+c = 0$, $b+c = 0$ och $c = 0$. Men $c = 0$ medför då att $b = 0$ vilket i sin tur medför att $a = 0$.

Övning 4.2. Vi har att $0(2,3) = (0,0), 1(2,3) = (2,3), 2(2,3) = (4,1), 3(2,3) = (1,4), 4(2,3) = (3,2)$. Bilden visar dessa punkter i blått.



Övning 4.3. (i) Nej, exempelvis är

$$\text{spann}(\{e_1^2\} \cap \{2e_1^2\}) = \{\}$$

men

$$\text{spann}(\{e_1^2\}) \cap \text{spann}(\{2e_1^2\}) = \text{spann}(\{e_1^2\}).$$

(ii) Nej, exempelvis är

$$\text{spann}(\{e_1^2\} \cup \{e_2^2\}) = F^2$$

men varken $\text{spann}\{e_1^2\}$ eller $\text{spann}\{e_2^2\}$ inkluderar $(1,1) \in F^2$.

(iii) Ja. Givet en mängd vektorer $v_1, \dots, v_k \in A \cap B$ kommer $\operatorname{spann}\{v_1, \dots, v_k\} \subset A$ och $\operatorname{spann}\{v_1, \dots, v_k\} \subset B$ så $\operatorname{spann}\{v_1, \dots, v_k\} \subset A \cap B$. Därmed är $A \cap B$ ett delrum.

Övning 4.4. Vi väljer vektorerna $v_0 = (0,0,0), v_1 = (1,1,0), v_2 = (0,1,1), v_3 = (1,0,1)$. Det är enkelt att se att $v_0, v_1, v_2, v_3 \in D$. Låt nu $(x,y,z) \in (\mathbb{Z}/(2))^3$. Då är $y = x + z$. Vi kan därmed skriva $(x,y,z) = (x, x+z, z) = (x,x,0) + (0,z,z) = xv_1 + zv_2$ så $\operatorname{spann}\{v_0, v_1, v_2, v_3\} = D$.

Övning 4.5. Låt $V = \operatorname{spann}\{v_1, \dots, v_k\} = \operatorname{spann}(V')$ och $W = \operatorname{spann}\{w_1, \dots, w_l\} = \operatorname{spann}(W')$. Vi ska visa att $V + W = \operatorname{spann}(V' \cup W')$. Antag först att $u \in \operatorname{spann}(V' \cup W')$. Vi kan då skriva

$$u = a_1v_1 + \cdots + a_kv_k + b_1w_1 + \cdots + b_lw_l \in V + W$$

för några koefficienter $a_1, \dots, a_k, b_1, \dots, b_l$.

Annars, anta att $u \in V + W$. Då är $u = v + w$ för något $v \in V$ och $w \in W$. Vi kan skriva v på formen $v = a_1v_1 + \cdots + a_kv_k$ och w på formen $b_1w_1 + \cdots + b_lw_l$ för några koefficienter $a_1, \dots, a_k, b_1, \dots, b_l$. Men då är

$$u = v + w = a_1v_1 + \cdots + a_kv_k + b_1w_1 + \cdots + b_lw_l \in \operatorname{spann}(V' \cup W').$$

Övning 4.6. Nej, e.g. välj $w_k = -v_k$ för alla $1 \leqslant k \leqslant n$.

Övning 4.7. Vi vill visa att $\operatorname{spann} V(M) = V(M)$. Låt $w = a_1v_1 + \cdot + a_nv_n \in \operatorname{spann} V(M)$ där $v_1, \dots, v_n \in V(M)$ och $a_1, \dots, a_n \in F$. Då har vi att

$$Mw = M(a_1v_1 + \cdot + a_nv_n) = a_1Mv_1 + \cdots + a_nMv_n = 0$$

så $w \in V(M)$.

Övning 4.8. Låt B vara en bas till F^n. Välj en vektor $v \in B$. Ifall $F \neq \mathbb{Z}/(2)$ kan vi byta ut v mot $2v$ vilket ger oss en ny bas. Därmed måste $F = \mathbb{Z}/(2)$. Ifall $n \geqslant 2$ väljer vi två vektorer $v, w \in B$ och byter ut v mot $v + w$. Då $v + w - w = v$ är det linjära höljet av den nya mängden fortfarande F^n. Dessutom är mängden linjärt oberoende då

$$0 = a(v + w) + bw + c_1v_1 + \cdots + c_{n-2}v_{n-2} = 0$$

medför att $a, a+b, c_1, \dots, c_{n-2} = 0$ där $v_1, \dots, v_{n-2}$ är de resterande elementen av B. Men då är även $b = 0$ och den nya mängden är en annan bas. Däremot är $\{(1)\}$ den enda basen till $\mathbb{Z}/(2)$.

Övning 4.9. Anta att $A \subset B$. Låt D vara en bas till A. Enligt Sats 4.2.6 kan vi bilda en bas åt B som inkluderar elementen i D, då måste $\dim A \leqslant \dim B$. Om nu B innehåller fler element än A måste basen även innehålla något element från $B \setminus A$. Men då skulle $\dim B > |D| = \dim A$.

Övning 4.10. Att (ii) till (vi) är ekvivalenta följer direkt från sats 4.3.6. Anta nu att M är inverterbar. Eftersom $MM^{-1}v = M^{-1}Mv = v$ för alla vektorer $v \in F^n$ är M^{-1} en invers till M. Därmed måste M vara bijektiv.

Anta nu istället att M är bijektiv. Då finns det en funktion bijektiv funktion $f : F^n \to F^n$ så att

$$Mf(v) = f(Mv) = v$$

för alla funktioner v. Det går lätt att se att $f(a_1v_1 + \cdots a_kv_k) = a_1f(v_1) + \cdots + a_kv_k$ för alla koefficienter $a_1, \ldots, a_k \in F$ och alla vektorer $v_1, \ldots, v_k \in F^n$. Definiera nu f som en matris genom

$$f = \begin{bmatrix} f(e_1^n) & f(e_2^n) & \cdots & f(e_n^n) \end{bmatrix}.$$

För alla vektorer $v \in F^m$ vill vi visa att $f(v) = fv$. Låt $v = (v_1, \ldots, v_m)$. Då har vi att

$$\begin{aligned} fv &= \begin{bmatrix} f(e_1^n) & f(e_2^n) & \cdots & f(e_n^n) \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \\ &= f(e_1^n)v_1 + f(e_2^n)v_2 + \cdots + f(e_n^n)v_n \\ &= f(v_1e_1^n + v_2e_2^n + \cdots + v_ne_n^n) \\ &= f(v). \end{aligned}$$

Därmed är $f = M^{-1}$ så M är inverterbar.

Kapitel 5

Övning 5.1. (i) Då koden har 4 kodord måste blocklängden vara $m = 2$ då $|C| = p^m$.

(ii) Nej, en linjär kod måste ha 0 som ett element.

(iii) Varje två kodord skiljer sig i fyra positioner så $d(C) = 4$.

(iv) Enligt Sats 5.0.2 kan koden detektera 3 fel och korrigera ett fel.

Övning 5.2. (i) Längden är 6 och koden C är

$$\begin{aligned} C = \{&(0,0,0,0,0,0), (0,1,0,1,0,1), (0,2,0,2,0,2), (1,0,1,0,1,0), \\ &(1,1,1,1,1,1), (1,2,1,2,1,2), (2,0,2,0,2,0), (2,1,2,1,2,1), (2,2,2,2,2,2)\} \end{aligned}$$

(ii) Vi kan skriva E som tre identitetsmatriser, det vill säga,

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(iii) Eftersom koden är linjär räcker det att se hur många bokstäver i kodorden som är nollskilda. Vi ser att det är som minst 3, så separationen är 3.

Övning 5.3. Vi kan exempelvis ta

$$C = \{(0,0,0,0,0,0,0,0), (1,1,1,1,1,0,0,0),\\ (0,0,0,1,1,1,1,1), (1,1,1,0,0,1,1,1)\}$$

Övning 5.4. Vi har att E är $n \times m$ matrisen

$$E = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

det vill säga, en $m \times m$ identitetsmatris med en extra rad av 1'or. Detta kan veriferas genom att beräkna

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \\ v_1 + \cdots + v_m \end{bmatrix}$$

som vi ville. Då E är en matris måste koden vara linjär.

Övning 5.5. Låt $A = \{i \mid v_i \neq u_i\}$, $B = \{i \mid w_i \neq u_i\}$ och $C = \{i \mid v_i \neq w_i\}$. Vi vill visa att

$$|C| \leqslant |A| + |B|\,.$$

För varje $i \in C$ har vi att $v_i \neq w_i$. Men om nu $i \notin A$ och $i \notin B$ skulle vi ha att $v_i = u_i$ och $u_i = w_i$ vilket medför att $v_i = w_i$. Därmed så måste i ingå i åtminstone en av mängderna A, B. Så

$$C \subset A \cup B$$

vilket medför att

$$|C| \leqslant |A \cup B| \leqslant |A| + |B|\,.$$

Övning 5.6. (i) Vi börjar med att definiera en funktion $H : (\mathbb{Z}/(2))^n \to (\mathbb{Z}/(2))^{n+1}$ genom att sätta

$$H(v_1, \ldots, v_n) = (v_1, \ldots, v_n, v_1 + v_2 + \cdots + v_n)$$

för alla vektorer $(v_1, \ldots, v_n) \in (\mathbb{Z}/(2))^n$. Vi har då att

$$d(H(v), H(w)) = d(v, w) + d(v_1 + \cdots + v_n, w_1 + \cdots + w_n).$$

Vi noterar även att vi kan skriva $C' = H(C)$ så vi behöver endast visa att $d(H(v), H(w)) \geqslant d(C) + 1$ för alla $v, w \in C$.

Enligt definitionen av separation så vet vi att för varje par $v, w \in C$ där $v \neq w$ är antingen $d(v, w) = d(C)$ eller $d(v, w) \geqslant d(C) + 1$. Ifall

$d(v,w) \geqslant d(C)+1$ har vi att $d(H(v),H(w)) \geqslant d(v,w) = d(C)+1$. Anta nu att $d(v,w) = d(C)$ och betrakta summan $s = v_1 + \cdots + v_n + w_1 + \cdots + w_n$. Eftersom v och w skiljer sig på $d(C)$ positioner kommer dessa bokstäver addera till $d(C) = 1$ medans bokstäverna för de positioner där de överensstämmer kommer addera till 0. Därmed är $s = 1$ men detta innebär att $d(v_1+\cdots+v_n, w_1+\cdots+w_n) = 1$ så $d(H(v),H(w)) = d(C)+1$.

(ii) Vi antar att C är linjär. Då är $C = E((\mathbb{Z}/(2))^m)$ för någon matris E. Vi kan skriva H som matrisen $n+1 \times n$

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

Då är en kodningsfunktion till C'

$$H(E) = HE$$

vilket är en matris så C' är ett delrum av $(\mathbb{Z}/(2))^n$ och är därmed linjär.

Övning 5.7. Anta att ett element x_k byts ut till något $x'_k \in \mathbb{Z}/(p)$. Vi kan skriva $x'_k = x_k + \varepsilon$ för något $\varepsilon \in \mathbb{Z}/(p)$ där $\varepsilon \neq 0$. Som koden är konstruerad ska

$$x_1 + 2x_2 + \cdots + 10x_{10} = 0$$

men i vårt fall får vi

$$\begin{aligned} &x_1 + \cdots + (k-1)x_{k-1} + kx'_k + (k+1)x_{k+1} + \cdots + 10x_{10} \\ =&x_1 + \cdots + 10x_{10} + kx'_k - kx_k \\ =&0 + k\varepsilon \neq 0 \end{aligned}$$

då både k, ε är nollskilda. Därmed kan koden upptäcka ett fel. Antag nästa att två element x_k byts plats med x_{k+1}. Då får vi istället summan

$$\begin{aligned} &x_1 + \cdots + (k-1)x_{k-1} + kx'_{k+1} + (k+1)x_k + (k+2)x_{k+2} + \cdots + 10x_{10} \\ =&x_1 + \cdots + 10x_{10} + x_k - x_{k+1} \\ =&0 + x_k - x_{k+1} \neq 0 \end{aligned}$$

givet att $x_k \neq x_{k+1}$. Ifall $x_k = x_{k+1}$ har inget fel inträffat. Därmed kan koden även upptäcka om två intillägande element har bytts plats. Slutligen anta att ett tecken x_k är oläsbart. Då kan vi beräkna x_k genom

$$x_k = k^{-1}(-x_1 - \cdots - (k-1)x_{k-1} - (k+1)x_{k+1} - \cdots - 10x_{10})$$

så koden kan rätta till fel av den typen.

Kapitel 6

Övning 6.1. Blocklängden är 3 så det finns $2^3 = 8$ ord i koden. Vi beräknar

$$\begin{aligned}
G(0,0,0) &= (0,0,0,0,0,0,0)\\
G(0,0,1) &= (0,0,1,0,1,1,1)\\
G(0,1,0) &= (0,1,0,1,0,0,1)\\
G(1,0,0) &= (1,0,0,1,1,0,1)\\
G(0,1,1) &= (0,1,1,1,1,1,0)\\
G(1,1,0) &= (1,1,0,0,1,0,0)\\
G(1,0,1) &= (1,0,1,1,0,1,0)\\
G(1,1,1) &= (1,1,1,0,0,1,1)
\end{aligned}$$

eftersom det minsta Hammingavståndet till 0 är 3, e.g. $d(0, G(0,1,0)) = 3$ är separationen 3.

Övning 6.2. Matrisen

$$G_4 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

har inversen

$$G_4^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Vi beräknar nu generatormatrisen på normalform genom att ta GG_4^{-1}.

$$GG_4^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Övning 6.3. Eftersom G är på normalform har vi att kontrollmatrisen H på normalform är

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Det följer att $d(C)$ har separation 3 (H har 3 linjärt beroende kolumner men alla par av kolumner är linjärt oberoende) och kan därmed rätta upp till ett fel. För att se vilka av de givna orden som är kodord multiplicerar vi dem med

H.

$$\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}$$

$$\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}0\\1\\0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}0\\0\\1\end{bmatrix}$$

$$\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\0\\1\\1\\1\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix}$$

$$\begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}1\\1\\1\end{bmatrix}$$

Vi ser nu att endast 111001 är ett kodord. Eftersom $(0,0,1)$ och $(1,0,0)$ dyker upp som kolumner i H går ordern 010100 och 110111 att korrigera.

Däremot är $(1,1,1)$ inte en kolumn i H så det måste ha skett åtminstone två fel i ordet 100001. Då $(1,1,1)$ är summan av exempelvis den första och den sista kolumnen eller den näst första och den näst sista kolumnen skulle vi kunna rätta till antingen 000000 eller 110011. Vi kan därför inte rätta till ordet.

För att rätta till 010100 noterar vi att $(0,0,1)$ är kolumn 6 i H, så vi kan rätta 010100 till 010101. $(1,0,0)$ är kolumn 4 i H så vi kan rätta 110111 till 110011.

Övning 6.4. Eftersom G är på normalform har vi att kontrollmatrisen H på normalform är

$$H=\begin{bmatrix}1&1&0&0&1&0&0\\0&0&1&1&0&1&0\\1&1&1&1&0&0&1\end{bmatrix}.$$

Det följer att $d(C)$ har separation 2 (H har 2 linjärt beroende kolumner). För att se vilka av de givna orden som är kodord multiplicerar vi dem med H.

$$H(1,1,0,1,0,1,1)=(0,0,0)$$
$$H(0,1,1,0,1,1,1)=(0,0,1)$$
$$H(0,1,1,1,0,0,0)=(1,0,1)$$

Vi ser att 1101011 redan är ett kodord och att $(1,0,1)$ förekommer två gånger i H och ordet 0111000 kan alltså inte rättas. Däremot har vi att $(0,0,1)$ uppkommer endast i kolumn 7 i H. Vi kan därmed rätta 0110111 med vektorn $(0,0,0,0,0,0,1)$ vilket ger oss kodordet 0110110.

Övning 6.5. Vi vill finna nollrummet för H_1 respektive för H_2. Låt $v = (v_1, v_2, v_3, v_4) \in N(H_1)$. Från första raden av H har vi att $v_2 + v_3 = 0$ så $v_2 = v_3$. Från den andra raden ser vi att om $v_3 = v_2 = 1$ är $v_1 \neq v_4$ och om $v_3 = v_2 = 0$ är $v_1 = v_4$. Detta ger oss kodorden

$$C_1 = \{(0,0,0,0), (1,0,0,1), (1,1,1,0), (0,1,1,1)\}$$

För $v = (v_1, v_2, v_3, v_4) \in C_2$ har vi att $v_2 + v_3 + v_4 = 0$ och att $v_1 + v_3 + v_4 = 0$. Adderar vi de här ekvationerna får vi att $v_1 + v_2 = 0$. Om $v_1 = v_2 = 1$ är $v_3 \neq v_4$ och om $v_1 = v_2 = 0$ är $v_3 \neq v_4$. Vi får därmed att

$$C_2 = \{(0,0,0,0), (0,0,1,1), (1,1,1,0), (1,1,0,1)\}$$

Vi ser nu att koderna är ekvivalenta då vi kan byta plats på den första och tredje positionen i för att gå från till kodord i C_1 till C_2 eller vice versa.

Övning 6.6. Eftersom generatormatrisen är på normalform kan vi enkelt finna en kontrollmatris på normalform H. Den blir

$$H = \begin{bmatrix} 4 & 4 & 4 & 1 & 0 & 0 \\ 4 & 3 & 2 & 0 & 1 & 0 \\ 4 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} | & & | \\ H_1 & \dots & H_6 \\ | & & | \end{bmatrix}$$

Det är tydligt att H innehåller 4 linjärt beroende kolumner. Vi ska nu visa att alla val av tre kolumner är linjärt oberoende. Kolumnerna M_1, M_2, M_3 är linjärt oberoende då

$$a(4,4,4) + b(4,3,2) + c(4,3,1) = 0$$

innebär att $a = -b - c$ vilket ger att

$$-4b - 4c + 3b + 3c = -b - c = 0$$

så $b = -c$ vilket ge att $a = 0$. Vi har nu att

$$-2c + c = 0$$

så $a = b = c = 0$. Sedan kan vi säga att alla val av tre kolumner som inkluderar en av kolumnerna M_4, M_5 eller M_6 kommer vara linjärt oberoende då kolumnerna M_1, M_2, M_3 alla skiljer sig i två positioner. Ifall vi har ett val av tre kolumner som inkluderar två av de sista kolumnerna kommer dessa också vara linjärt oberoende då de sista två vi valde kommer ha en position som är nollskild. Slutligen om vi väljer alla tre av de sista kolumnerna är de linjärt oberoende då de är enhetsbasen.

Övning 6.7. Vi påstår att H' är en kontrollmatris till C om och endast om

$$H' = MH$$

för en inverterbar $(n-m) \times (n-m)$ matris M.

Anta att $H' = MH$. Vi vill visa att $N(MH) = C$. Om $v \in C$ har vi att $Hv = 0$ så $MHv = 0$ vilket medför att $v \in N(HM)$. Om $v \in N(MH)$ är $MHv = 0$ men M är injektiv så $Hv = 0$ vilket medför att $v \in C$. Då M är surjektiv måste också H' vara surjektiv.

Anta nu istället att H också är en kontrollmatris till C. Då har vi att

$$H^T$$

är injektiv och har linjärt oberoende kolumner. Dess kolumner kommer då bilda en bas av $(\mathbb{Z}/(p))^{n-m}$ så kolumnerna av H'^T kan skrivas som en linjärkombination av dem. Detta uttrycker vi som att

$$H'^T = H^T N$$

för någon $(n-m) \times (n-m)$ matris N. Tar vi transponatet av båda sidorna får vi att

$$H' = N^T H.$$

Vi sätter $M = N^T$ och noterar att M måste vara surjektiv för att H' ska vara surjektiv. Därmed är M inverterbar.

Kapitel 7

Övning 7.1. Vi beräknar

$$|B(2,(0,0,0))| = \binom{3}{0} + \binom{3}{1}(5-1)^1 + \binom{3}{2}(5-1)^2 = 1+3\cdot 4+\frac{3(3-1)}{2}\cdot 16 = 61.$$

Övning 7.2. Vi har att

$$21 = 1\cdot 1 + 0\cdot 2^1 + 1\cdot 2^2 + 0\cdot 2^3 + 1\cdot 2^4,$$

$$12 = 0\cdot 1 + 0\cdot 2^1 + 1\cdot 2^2 + 1\cdot 2^3 + 0\cdot 2^4,$$

$$17 = 1\cdot 1 + 0\cdot 2^1 + 0\cdot 2^2 + 0\cdot 2^3 + 1\cdot 2^4.$$

Vi får alltså binära representationer

$$\begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix}, \quad \begin{bmatrix}0\\0\\1\\1\\0\end{bmatrix}, \quad \begin{bmatrix}1\\0\\0\\0\\1\end{bmatrix}.$$

Övning 7.3. Vi beräknar

$$H_2 v = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Det här är den binära formen av $0+1\cdot 2^1 = 2$, så v är fel i den andra positionen. Alltså är den rättade versionen

$$w = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Övning 7.4. Vi vet att H kommer att ha dimensioner

$$3 \times \frac{3^2 - 1}{3 - 1} = 3 \times 4.$$

Vi väljer som första kolonnvektor

$$v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Den andra kolumnvektorn får inte vara v eller

$$2v_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}.$$

Vi väljer

$$v_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Vår tredje vektor får inte vara $v_1, v_2, 2v_1, 2v_2$, så vi väljer

$$v_3 = \begin{bmatrix} 2 \\ 2 \end{bmatrix}.$$

Den sista återstående vektorn får inte vara $v_1, v_2, v_3, 2v_1, 2v_2, 2v_3$ så vi väljer till sist

$$v_4 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

Sist men inte minst får vi alltså

$$H = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Det finns många andra lösningar.

Övning 7.5. Låt C vara en binär repetitionskod av udda längd $2k + 1$, där ett meddelande av längd 1 repeteras $2k + 1$ gånger. Vi har att $C = \{0, v\}$, där v är ordet av bara ettor. Dessutom är $d(C) = k$. Vi måste visa alla ord $w \in (\mathbb{Z}/(2))^{2k+1}$ har avstånd som mest k till ett ord i C. Om w har mest nollor gäller $d(w, 0) \leqslant k$, om w har mest ettor gäller $d(w, v) \leqslant k$.

Kapitel 8

Övning 8.1. Låt $P(x)$ vara ett polynom över $\mathbb{Z}/(p)$. Skriv

$$P(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1} = b_0 + b_1 x + \cdots + b_{p-1}x^{p-1}$$

för alla $x \in \mathbb{Z}/(p)$ och för några konstanter $a_0, \ldots, a_{p-1}, b_0, \ldots, b_{p-1} \in \mathbb{Z}/(p)$. Vi vill visa att $a_k = b_k$ för alla $0 \leqslant k \leqslant p-1$. Sätt $c_k = b_k - a_k$. Vi kan nu skriva

$$0 = c_0 + c_1 x + \cdots + c_{p-1}x^{p-1}$$

för alla $x \in \mathbb{Z}/(p)$. Därmed har polynomet $c_0 + c_1 x + \cdots + c_{p-1}x^{p-1}$ p stycken nollställen. Men enligt Sats 8.1.5 kan inte polynomet ha någon grad. Därmed är $c_0 = c_1 = \cdots = c_{p-1} = 0$.

Övning 8.2. (i) Det finns p^p polynom över $\mathbb{Z}/(p)$ och p^p funktioner från $\mathbb{Z}/(p)$ till $\mathbb{Z}/(p)$ då varje koefficient kan anta p olika värden. Alla funktioner är därmed polynom.

(ii) f kan skrivas som

$$f(x) = 1 + 1x + 2x^2$$

för alla $x \in \mathbb{Z}/(p)$. Därmed har f grad 2.

Övning 8.3. Vi låter koden vara en Reed-Solomon kod $C \subset (\mathbb{Z}/(17))^8$ givet av en 4×8 kontrollmatris

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 \\ 0 & 1 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 \end{bmatrix}.$$

Enligt Sats 8.3.3 kommer C ha separation $8 - 4 + 1 = 5$.

Övning 8.4. (i) Blocklängden är $4-2 = 2$ och separationen är $4-2+1 = 3$.

(ii) $C = N(H)$ och C har dimension 2 så vi försöker hitta två linjärt oberoende vektorer i $N(H)$. Om $v = (x, y, z, w) \in N(H)$ har vi att

$$0 = Hv = \begin{bmatrix} x + y + z + w \\ y + 2z + 3w \end{bmatrix}.$$

Väljer vi nu till exempel $z = 1, w = 0$ får vi att $y = 5, x = 1$ så $(1, 5, 1, 0) \in N(H)$. Väljer vi $z = 0, w = 1$ får vi istället $y = 4$, $x = 2$ så $(2, 4, 0, 1) \in N(H)$. Därmed kommer matrisen

$$\begin{bmatrix} 1 & 2 \\ 5 & 4 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

vara en generatormatris till C.

Referenser och förslag till vidare läsning

Sigmundur Gudmundsson (TRANS.), Karl-Gustav Andersson: *Finite Fields and Error-Correcting Codes*
Lecture Notes in Mathematics, Lund University, 2015
`http://www.matematik.lu.se/matematiklu/personal/sigma/Andersson.pdf`

Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, Alfred Wassermann: *Error-Correcting Linear Codes, Classification by Isometry and Applications*
Algorithms and Computation in Mathematics, Vol. 18, Springer, Berlin, 2006