DISKRET MATEMATIKK FINNES IKKE

Dan Laksov

KTH, Stockholm

matematikk/thorup/dlbook/September 11, 2004

Diskret matematikk finnes ikke

Dan Laksov

Notater for "Forum för Matematiklärare".

Et prosjekt høsten 2004støttet av:
Marianne och Marcus Wallenbergs Stiftelse
Versjon 1. September 2004

Matematiska Institutionen
KTH

Matematiska Institutionen
KTH
100 44 STOCKHOLM
ISBN ?
©2001 Matematiska Institutionen

FORORD

Disse notatene er et supplement til forelesningene i "Matematisk Forum För Matematiklärare" (eller kort "Forum") det akademiske året 2004-2005. Alt materialet til de syv forelesningene i "Forum" finnes i heftet, men inndelingen av notatene i kapittel og seksjoner svarer bare delvis til innholdet av forelesningen. Heftet er ment som hjelp for hukommelsen, eller for å finne supplerende og utdypende materiale.

Notatene forutsetter bare kjennskap til de enkleste begrepene fra mengdelæren. Presentasjonen av matematikken er så stringent som mulig, og det er bare å håpe at dette ikke har gjort dem uleselige.

INNHOLD

1. KLASSIFIKASJONEN AV MATEMATIKKEN

1.1. Diskret matematikk og AMS-klassifikasjonen

De fleste som har har kommet i kontakt med matematikk i en eller annen form har hørt om *diskret matematikk* og har en vag oppfatning av hva det er. Når man skal presisere hva det er får alle, amatører som profesjonelle, store vanskeligheter. Hensikten med dette heftet er å vise at den enkle forklaringen til dette er at diskret matematikk ikke finnes, og at det er ufruktbart, og tvert imot de ledende strømningene i dagens matematikk, å skille mellom "diskret" matematikk og "annen" matematikk.

Det hjelper ikke at *Skolverket* har oppfunnet et emne *matematik diskret*, som er obligatorisk på matematikk/datalogi grenen av NV-programmet. Navnet skulle egentlig være *diskret matematik*, men i byråkratispråket må alle matematikkemner begynne med ordet *matematik*.

Formelt sett finnes ikke emnet *diskret matematikk* av den enkle grunn at den ikke er med i *AMS-klassifikasjonen* av matematikken. Dette er en liste over matematiske emner som ble sammensatt av *American Mathematical Society* (AMS) og brukes av alle profesjonelle matematikere når de skal skille på ulike deler av matematikken. Listen oppdateres stadig og omfatter i dag 63 hovedområder. Hver av disse er delt opp i en rekke delområder, oftest 10-20 stykker, og hvert delområde er oppdelt i et stort antall spesialområder. Denne findelingen av matematikken viser hvilken enorm bredde matematikken har. En ekspert på et spesialområde kan ofte forstå eksperter på andre spesialområder innen samme delområde, men kan ha store vanskeligheter med emner innefor andre delområder.

→ I Appendiks (A.1) viser vi hovedområdene i AMS-klassifikasjonen og i (A.2) viser
→ vi delområdene til et av disse, området *Algebraisk Geometri* (AMS 14). I (A.3) har vi tatt med klassifikasjonen av hovedområdet Algebraisk Geometri for å vise mangfoldigheten av spesialiteter innenfor et av de mange hovedområdene.

Ettersom *diskret matematikk* hverken er et hovedområde, et delområde, eller er med i findelingen, finnes det "formelt sett" ikke som emne i matematikken. Emnet "matematik diskret" som *Skolverket* har oppfunnet består av et lite utvalg av noen enkle begreper hentet fra emner under findelingen av *Matematisk logikk* (AMS 03), *Kombinatorikk* (AMS 05), *Tallteori* (AMS 11) og *Datalogi* (AMS 05). Den lille delen av kombinatorikk som er med tilhører egentlig *Sannsynlighetsteorien* (AMS 60).

1.2. Hvorfor dele i "diskret" og "annen" matematikk?

Vi kan bare spekulere på hvorfor amatørene på *Skolverket* har funnet det påtreng-

ende å samle en konfetti av matematiske emner under rubrikken *matematik diskret*. En sannsynlig forklaring er at de har latt seg villede av "eksperter" som kjenner et behov av å profilere seg mot områder som påståens være spesielt nyttige for utviklingen av *datamaskiner* og for anvendelsene av disse. Datamaskinene er tilsynelatende "diskrete av naturen". De opererer med 0'er og 1'ere og kan bare inneholde og formidle en endelig mengde informasjon. For å konstruere, operere og programmere datamaskiner kreves det store mengder matematikk. Uten matematikken skulle den raske utviklingen av elektronikk vært umulig og datamaskinene skulle være langsomme monstre som bare kunne administrere små mengder data. I datamaskinenes barndom var det ganske lite og enkel matematikk som kom til anvendelse. De miljøene innenfor matematikk og datalogi som arbeidet på slike områder fant det opportunt å skille den matematikken de drev på med fra annen matematikk ved å kalle den "diskret" og spesielt anpasset for datamaskinen. Dette ga dem en ufortjent prestisje. Desverre sluttet det ikke med dette. Etterhvert som datamaskinene fikk anvendelser innefor teknikk, samfunnsfag, humaniora og naturvitenskap hevdet samme grupper av matematikere og dataloger at den påståtte *diskret* matematikken var spesielt anvendbar også på disse områdene. Ofte besto anvendelsene bare i at man døpte om matematiske begrep, som *grafer*, *mengder* eller *permutasjoner*, til mer fantasieggende ord som veier, ektemenn, eller gener. Dette øker hverken forståelsen av det praktiske problemet eller sjansene for å løse det. Iblandt overskrider det grensen til den pinlige og latterlige. Desverre er det mange som blir lokket av denne virksomheten ettersom de tror man kan gjøre store innsatser uten innsikt i hverken matematikk eller anvendelser.

I virkeligheten har det vist seg at nesten alle deler av matematikken kan brukes i forbindelse med datamaskiner og deres anvendelser. Noe spesielt "diskret" over matematikken eller anvendelsene som har nytte for datamaskinene er det umulig å oppdage. Den gamle terminologien henger imidlertid igjen ettersom det er opportunt med dagens forskningspolitikk å bli forbundet med IT- og dataområdet. Dette skulle ikke spille noen større rolle om det ikke hadde dradd oppmerksomheten bort fra de fundamentale anvendelsene av matematikken, og fra levende grener av matematikken der det kreves store kunnskaper og dyp innsikt for å bidra til utviklingen.

2. "DISKRET" ELLER "KONTINUERLIG"?

2.1. "Diskret" og "kontinuerlig" matematikk

Det er ikke bare formelt at *diskret matematikk* ikke finnes. Forsøkene til å skille "diskret" matematikk fra "annen" matematikk skaper forvirring og uklarhet. Bare ideen å skille ulike deler av matematikken i slike bokser går tvert imot utviklingen av matematikken der hovedlinjene i lang tid har vært å finne teorier og metoder som er felles for all matematikk. Det har vist seg mye mer fruktbart å bryte felles grunn enn å skille mellom de ulike områdene.

Ofte beskrives *diskret matematikk* som motsetningen til *kontinuerlig matematikk*. Vi skal her vise at dette er umulig fordi begrepet *kontinuitet* gjennomsyrer de fleste deler av matematikken.

Intuitivt har vi en følelse av at *diskret* og *kontinuerlig* er motsatte begreper. Beveger vi oss langs *tallinjen* møter vi en kontinuerlig strøm av *reelle tall*. Med jevne mellomrom møter vi et *helt tall*. Vi kan beskrive dette som at de reelle tallene utgjør et *kontinuum*, og at de hele tallene ligger *diskret* på tallinjen.

Mer problematisk er det med de *rasjonale tallene*. Går vi fra et rasjonalt tall til et annet møter vi en "jevn" strøm av rasjonale tall, men også uendelig mange reelle tall som ikke er rasjonale. Det finnes altså uendelig mange "hull" som er reelle, men ikke rasjonale. De rasjonale tallene har derfor både *diskrete* og *kontinuerlige* egenskaper.

Dette er bare en overfladisk del av vanskelighetene med å skille *diskret* og *kontinuerlig*. Vi skal se at selv på de hele tallene kan vi innføre naturlige og nyttige *avstandsbegrep* som gjør at vi kan snakke om *kontinuitet* også for disse.

Vår intuisjon slår feil fordi vi forbinder skillet mellom *diskret* og *kontinuerlig* med avstand. De hele tallene er *diskrete* fordi de ligger på endelig avstand fra hverandre, og de reelle er *kontinierlige* fordi det bare finnes reelle tall nær et gitt tall. På de reelle, rasjonale, og hele tallene, finnes det imidlertid en stor mengde naturlige og brukbare avstandsbegreper i tillegg til den *Eukliske* som er den vår intuisjon er grunnlagt på. De fleste av disse avstandene kan vi ikke anskueliggjøre. Til og med endelige mengder har, som vi skal se, slike avstander. Derfor blir vi ofte lurt til å betrakte hele tall og endelige mengder som *diskrete* skjønt de har, i mange forbindelser, *kontinuerlige egenskaper*.

Oppgaver.

Oppgave 1. Vis at mellom to ulike rasjonale tall finnes det uendelig mange rasjonale tall.

OPPGAVE 2. Vis at mellom to rasjonale tall finnes det uendelig mange reelle tall.

OPPGAVE 3. Vis at vi kan nummerere de rasjonale tallene, slik at det finnes "like mange" rasjonale tall som det finnes naturlige tall $0, 1, 2, \ldots$.
(Hint: Bruk Cantor's *diagonaliseringsmetode*).

OPPGAVE 4. Vis at de reelle tallene ikke kan nummereres.
(Hint: Bruk Cantor's *diagonaliseringsmetode*).

2.2. Avstand og metriske rom

Begrepene *avstand* og *kontinuitet* forekommer i nesten alle deler av matematikken. Det er dette som er hovedgrunnen til at det er umulig å skille "kontinuerlig matematikk" fra "annen" matematikk. I denne seksjonen skal vi definere *avstand* og det tilhørende begrepet *metrisk rom* og gi eksempler der avstandene har overraskende egenskaper, helt forskjellige fra de vi er vant til.

På den reelle linjen $\mathbf{R}$ har vi den vanlige *absoluttverdien* $|x-y|$ som gir *avstanden* mellom *punktene* x og y. De egenskapene vi vanligvis bruker for absoluttverdien er:

(1) (Ikke degenererthet) $|x| = 0$ hvis og bare hvis $x = 0$.
(2) (Symmetri) $|x - y| = |y - x|$.
(3) (Triangelulikhet) $|x + y| \leq |x| + |y|$.
(4) (Multiplikativitet) $|xy| = |x||y|$.

I planet $\mathbf{R}^2$ har vi at avstanden mellom punktene $x = (a_1, a_2)$ og $y = (b_1, b_2)$ er gitt ved

$$|x - y| = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}.$$

Mer generelt har vi i det n-dimensjonale *Euklidske rommet* $\mathbf{R}^n$ at avstanden mellom punktene $x = (a_1, a_2, \ldots, a_n)$ og $y = (b_1, b_2, \ldots, b_n)$ er

$$|x - y| = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots + (a_n - b_n)^2}.$$

Denne *avstanden* tilfredsstiller egenskapene:

(1) (Ikke degenererthet) $|x| = 0$ hvis og bare hvis $x = 0$.
(2) (Symmetri) $|x - y| = |y - x|$.
(3) (Triangelulikhet) $|x + y| \leq |x| + |y|$.

Multiplikativiteten for absoluttverdien av reelle tall har ingen mening i det n dimensjonale rommet ettersom vi ikke kan multiplisere to punkter.

Når vi setter

$$d_E(x, y) = |x - y|$$

i disse eksemplene vil $d_E(x, y)$ være et ikke negativt tall som tilfredsstiller egenskapene:

(1) (Ikke degenererthet) $d_E(x, y) = 0$ hvis og bare hvis $x = y$.
(2) (Symmetri) $d_E(x, y) = d_E(y, x)$.
(3) (Triangelulikhet) $d_E(x, z) \leq d_E(x, y) + d_E(y, z)$.

Det er naturlig å bruke egenskapen for avstanden i det *Euklidske rommet* $\mathbf{R}^n$ som modell for avstand i vilkårlige rom.

2.2.1 DEFINISJON. La X være en vilkårlig mengde. En *avstand* d, eller som vi sier *metrikk*, på X tilordner til hvert par av elementer x, y i X et ikke negativt reelt tall $d(x, y)$ slik at

(1) (Ikke degenererthet) $d(x, y) = 0$ hvis og bare hvis $x = y$.
(2) (Symmetri) $d(x, y) = d(y, x)$.
(3) (Triangelulikhet) $d(x, z) \leq d(x, y) + d(y, z)$.

Vi kaller X med en slik avstand d et *metrisk rom*. Iblandt kaller vi paret (X, d) for et *metrisk rom*.

2.2.2 BEMERKNING. Vi skal i mange situasjoner bruke at om (X, d_X) er et metrisk rom og Y er en undermengde av X, og vi skriver $d_X(x, y) = d_Y(x, y)$ når x og y begge er i Y, så vil (Y, d_Y) også være et metrisk rom. Dette er helt klart ettersom
→ aksiomene (1), (2), (3) i Definisjon (2.2.3) er de samme for d_X og d_Y. Vi kaller (Y, d_Y) det *induserte metriske rommet*.

Det er bemerkelsesverdig at vi med en slik enkel definisjon har fått et begrep som både er anvendbart og fleksibelt, og som omfatter interessante eksempler fra store deler av matematiken.

Oppgaver.

→ OPPGAVE 1. Vis at egenskapene (1), (2), (3) fra Seksjon (2.2) holder for absoluttverdien i $\mathbf{R}^n$. (Hint: Bruk Schwartz ulikhet).

→ OPPGAVE 2.. Vis at egenskapene (1), (2), (3) fra Seksjon (2.2) for absouttverdien på $\mathbf{R}^n$ gir egenskapene (1), (2), (3) for d_E definert av $d_E(x, y) = |x - y|$.

2.3. Eksempler på metriske rom

Vi skal her gi de vanligste eksemplene på metriske rom, samt noen mer eksotiske smakebiter. Eksemplene har interesse i seg selv, men fremfor alt viser de hvor omfattende og brukbare metriske rom er. Vi skal senere komme tilbake til anvendelser på koder og i tallteorien.

2.3.1 EKSEMPEL. (Reelle linjen) Vi har sett at den reelle linjen $X = \mathbf{R}$ med den *Euklidske avstanden* $d_E(x, y) = |x - y|$ er et metrisk rom.

→ 2.3.2 EKSEMPEL. (Euklidske rommet) Mer generelt enn i Eksempel (2.3.1) har vi at det n dimensjonale *Euklidske rommet* $X = \mathbf{R}^n$ med avstanden $d_E(x, y) = |x - y|$ er et metrisk rom.

2.3.3 EKSEMPEL. (*Diskret metrikk*) For hver mengde X setter vi

$$d_D(x, y) = \begin{cases} 0 & \text{om} \quad x = y \\ 1 & \text{om} \quad x \neq y. \end{cases}$$

Da er (X, d_D) et metrisk rom.

2.3.4 Eksempel. (*Hamming metrikken*) For hver mengde A skriver vi $X = A^n$ for det n'te *Kartesiske produktet* av A med seg selv n ganger. Det vil si, $X = A^n$ består av alle n'tupler $x = (a_1, a_2, \ldots, a_n)$ av elementer $a_1, a_2, \ldots, a_n$ i A. For $x = (a_1, a_2, \ldots, a_n)$ og $y = (b_1, b_2, \ldots, b_n)$ i X definerer vi avstanden $d_H(x, y)$ mellom x og y som antallet indekser i slik at a_i er forskjellig fra b_i. Det vil si,

$$d_H(x, y) = \{\text{antallet indekser } i \text{ slik at } a_i \neq b_i\}.$$

For eksempel, om $A = \{0, 1\}$ og $X = A^3$ vil

$$d_H((1,0,1),(0,0,1)) = 1, \quad d_H((1,0,1),(1,1,0)) = 2, \quad d_H((1,0,1),(0,1,0)) = 3.$$

Da er d_H en metrikk på X. Det er klart at egenskapene (1) og (2) fra Definisjon
→ (2.2.1) holder. For å vise egenskapen (3) tar vi $z = (c_1, c_2, \ldots, c_n)$. Om i er en indeks som bidrar til $d_H(x, z)$, det vil si $a_i \neq c_i$, så må enten $a_i \neq b_i$ eller $a_i \neq c_i$, eller begge. Derfor bidrar indeksen i til $d_H(x, y)$ eller til $d_H(y, z)$, eller til begge. Dette resonnementet for $i = 1, 2, \ldots, n$ viser at *triangelulikheten* $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$ holder.

Metrikken d kalles *Hamming metrikken* oppkalt etter Richard Hamming (1915-98) som brukte den i kodeteorien. Vi kommer tilbake til Hamming metrikken i
→ forbindelser med koder i et kapittel (4).

2.3.5 Eksempel. (*Taksimetrikken*) På det *Kartesiske produktet* $X = \mathbf{R}^n$ definerer vi avstanden mellom punktene $x = (a_1, a_2, \ldots, a_n)$ og $y = (b_1, b_2, \ldots, b_n)$ ved

$$d_T(x, y) = |a_1 - b_1| + |a_2 - b_2| + \cdots + |a_n - b_n|.$$

→ Det er klart at egenskapene (1) og (2) i for en metrikk i Definisjon (2.3.3) holder for d_T, og egenskapen (3) følger av triangelulikhetene $|a_i - c_i| \leq |a_i - b_i| + |b_i - c_i|$ for $i = 1, 2, \ldots, n$. Derfor er (X, d_T) et metrisk rom. Vi kaller d_T for *Taksimetrikken* ettersom avstanden mellom motsatte hjørner (a_1, a_2) og (b_1, b_2) i et rektangel er summen av avstanden mellom hjørnene (a_1, a_2) og (b_1, a_2), og avstanden mellom hjørnene (b_1, a_2) og (b_1, b_2). Det vil si den avstanden en taksi må kjøre for å komme fra hjørnet (a_1, a_2) til det diagonalt motsatte hjørnet (b_1, b_2) om rektangelet var basen for et hus.

Det bemerkelsesverdige ved Taksimetrikken på $\mathbf{R}^n$ er at den på mange måter er *ekvivalent* med den *Euklidske metrikken*, det vil si, to punkter er *nære* hverandre i en metrikk når de er *nære* i den andre. Mer bestemt. La d_E være den *Euklidske metrikken* og d_T *Taksimetrikken*. Da finnes det positive konstanter C_1 og C_2 slik at for alle x og y i $X = \mathbf{R}^n$ vil

$$C_1 d_E(x, y) \leq d_T(x, y) \leq C_2 d_E(x, y).$$

Mye av "den vanlige" geometrien kan man gjøre i Taksimetrikken. Dette gir mange overraskende resultater, som at "taksi π" er lik $4\sqrt{2}$. Se Dukels artikkel i [S] for en underholdende fremstilling.

2.3.6 Eksempel. (Den *p-adiske metrikken* på $\mathbf{Z}$) La $X = \mathbf{Z}$ være de hele tallene og velg et primtall p. Hvert heltall n forskjellig fra null kan skrives entydig som $n = p^k m$ der k er et ikke negativt heltall og m er et heltall som ikke er delbart med p. Definer en *norm* på $\mathbf{Z}$ ved

$$|n|_p = 1/p^k.$$

Tallet 0 er spesielt ettersom p^k deler 0 for alle k. Vi setter derfor

$$|0|_p = 0.$$

For eksempel, om $p = 2$ har vi

$$|2|_2 = 1/2, |3|_2 = 1, |4|_2 = 1/2^2, |5|_2 = 1, |6|_2 = 1/2, |7|_2 = 1, |8|_2 = 1/2^3 \ldots.$$

Det er en grei, og instruktiv, oppgave å vise at følgende egenskaper holder:

(1) (Ikke degenererthet) $|n|_p = 0$ hvis og bare hvis $n = 0$.
(2) (Symmetri) $|n|_p = |-n|_p$.
(3) (Ikke arkimedisk triangelulikhet) $|m + n|_p \leq \max(|m|_p, |n|_p)$.
(4) (Multiplikativitet) $|nm|_p = |m|_p|n|_p$.

Merk at egenskapen (3) er sterkere enn den vanlige triangelulikheten ettersom vi vanligvis har $\max(|m|_p, |n|_p) < |m|_p + |n|_p$.

Setter vi

$$d_p(m, n) = |m - n|_p$$

får vi

(1) (Ikke degenererthet) $d_p(x, y) = 0$ hvis og bare hvis $x = y$.
(2) (Symmetri) $d_p(x, y) = d_p(y, x)$.
(3) (Ikke arkimedisk triangelulikhet) $d_p(x, z) \leq \max(d_p(x, y), d_p(y, z))$.

Vi kaller d_p den *p-adiske metrikken* på heltallene.

I den p-adiske metrikker er ikke $\mathbf{Z}$ lenger *diskret*. For eksempel vil det for hvert heltall n finnes uendelig mange heltall $n + p^k$ som ligger så "nær" n som vi vil fordi

$$d_p(n, n + p^k) = |p^k| = 1/p^k$$

som vi kan få så "liten vi vil" ved å velge k "tilstrekkelig stor".

Rommet $(\mathbf{Z}, d_p)$ skiller seg vesentlig fra de hele tallene med metrikken *indusert* av den *Euklidske metrikken* på $\mathbf{R}$. For eksempel vil

$$d_2(2^n - 2^{n-2}, 2^n) = |2^{n-1}|_2 = 1/2^{n-1}$$

mens

$$d_E(2^n - 2^{n-2}, 2^n) = |2^{n-1}| = 2^{n-1}.$$

Det vil si, tallene $2^n - 2^{n-1}$ og 2^n ligger "nære" i den 2-adiske metrikken og "langt fra hverandre" i den Euklidske.

→ 2.3.8 Eksempel. (Den p-adiske metrikken på $\mathbf{Q}$) Vi fortsetter Eksempelet (2.3.7). La $r = m/n$ være et rasjonalt tall. Om $r = m/n = m_1$ vil $mn_1 = nm_1$, så vi får → av multiplikativiteten i (2.3.4) at $|m|_p|n_1|_p = |n|_p|m_1|_p$. Derfor vil $|m|_p/|n|_p = |m_1|_p/|n_1|_p$. Vi kan derfor definere en *norm* på de rasjonale tallene $\mathbf{Q}$ ved

$$|r|_p = |m/n|_p = |m|_p/|n|_p.$$

Det er klart at for alle rasjonale tall r og s vil vi ha

(1) (Ikke degenererthet) $|r|_p = 0$ hvis og bare hvis $n = 0$.
(2) (Symmetri) $|r|_p = |-r|_p$.
(3) (Ikke arkimedisk triangelulikhet) $|r + s|_p \leq \max(|r|_p, |s|_p)$.
(4) (Multiplikativitet) $|rs|_p = |r|_p|s|_p$.

Vi setter

$$d_p(r, s) = |r - s|_p$$

→ og får som i Eksempel (2.3.7)

(1) (Ikke degenererthet) $d_p(x, y) = 0$ hvis og bare hvis $x = y$.
(2) (Symmetri) $d_p(x, y) = d_p(y, x)$.
(3) (Triangelulikheten) $d_p(x, z) \leq d_p(x, y) + d_p(y, z)$.

Vi har altså at $(\mathbf{Q}, d_p)$ er et metrisk rom.

Oppgaver.

→ Oppgave 1.. Vis at (X, d) i Eksempel (.3) er et metrisk rom.

Oppgave 2.. La $A = \{0, 1\}$. Regn ut alle avstandene mellom punktene i $X = A^3$ med Hamming metrikken.

→ Oppgave 3.. Vis at egenskapene (1)-(4) holder i Eksempel (?)

Oppgave 4.. Gi eksempler som viser at $\max(|m|_p, |n|_p) < |m|_p + |n|_p$.

Oppgave 5.. Vis at egenskapene (1), (2), (3) for $||_p$ gir egenskapene (1), (2), (3) → for $d_p(m, n)$ i Eksempel (?).

Oppgave 6.. Vis at om $A = \{0, 1\}$ og $X = A^n$ så er *Taksimetrikken* og *Hammingmetrikken* like.

Oppgave 7.. Generaliser taksimetrikken på $X = \mathbf{R}^n$ til en taksimetrikk på $X = Y^n$ for alle metriske rom (Y, d).

Oppgave 8.. Finn omkretsen av en "taksisirkel", definer de "taksitrigonometriske" funksjonen, og gi de vanlige relasjonene, som "taksitrigonometriske ene'rn".
(Hint: Kikk etter i Dunkels artikkel i [S])

2.4. Kontinuitet

Vi har sett at det finnes avstandsbegrep i mange forskjellige situasjoner, og at avstandsbegrepene kan ha helt ulike egenskaper. For eksempel har det *Kartesiske produktet* $\mathbf{R}^n$ av de reelle tallene med seg selv n ganger, den vanlige *Euklidske metrikken*, men den har også *Taksimetrikken*, *Hammingmetrikken* og den *Diskrete metrikken*. Intuitivt henger avstandsbegrepet sammen med *kontinuitet*, ettersom vi kan snakke om

at punkter ligger "nære" hverandre. Vi skal vise at vårt avstandsbegrep er som skapt for å innføre *kontinuitet*. Igjen bruker vi de reelle tallene som modell.

En funksjon

$$f : \mathbf{R} \to \mathbf{R}$$

er *kontinuerlig* i et punkt x om hvert punkt y som ligger "nær" x avbildes til et punkt $f(y)$ som ligger "nær" $f(x)$. Mer presist uttrykker vi dette ved:

For hvert x i X og for hvert tall $\varepsilon > 0$ finnes det et tall $\delta > 0$ slik at om $|x-y| < \delta$ så vil $|f(x) - f(y)| < \varepsilon$.

I "metrikkspråket" betyr dette at om $d_E(x, y) < \delta$ så skal $d_E(x, y) < \varepsilon$. Dette kan vi overføre direkte til metriske rom:

2.4.1 Definisjon. La (X, d_X) og (Y, d_Y) være metriske rom. En avbildning

$$f : X \to Y$$

er *kontinuerlig* i et punkt x i X om det for hvert tall $\varepsilon > 0$ finnes et tall $\delta > 0$ slik at om $d_X(x, y) < \delta$ så vil $\delta_Y(f(x), f(y)) < \varepsilon$. Vi sier at f er *kontinuerlig* om den er kontinuerlig i alle punkter x.

Igjen skal vi gi noen eksempler. Spesielt instruktive er eksempler der den underliggende mengden for de metriske rommene er den samme, men har ulike metrikker. Da ser man klart hvilken betydning metrikkene har for vår intuisjon om *avstand* og *kontinuitet*.

2.4.2 Konvensjon. Når vi har en avbildning $f : X \to Y$ mellom to metriske rom (X, d_X) og $Y, d_Y)$ skriver vi dette iblandt $f : (X, k_X) \to (Y, d_Y)$ for enkelhets skyld.

2.4.2 Eksempel. *Identitetsavbildningen*

$$\mathrm{id} : (\mathbf{R}^n, d_E) \to (\mathbf{R}^n, d_T)$$

er kontinuerlig. Dette er fordi det finnes en positiv konstant C slik at $d_E(x, y) <$
→ $Cd_T(x, y)$ for alle x og y (se Oppgave (?)). Gir vi et tall $\varepsilon > 0$ velger vi $\delta = \varepsilon/C$. Om $d_T(x, y) < \delta$ vil $d_E(x, y) < Cd_T(x, y) < C\delta = \varepsilon$ så id er kontinuerlig.

På samme måte viser vi at $\mathrm{id} : (\mathbf{R}^n, d_T) \to (\mathbf{R}^n, d_E)$ er kontinuerlig.

2.4.4 Eksempel. Identitetsavbildningen

$$\mathrm{id} : (\mathbf{R}^n, d_E) \to (\mathbf{R}^n, d_H)$$

er ikke kontinuerlig. Dette er fordi, for $1 > \varepsilon > 0$, vil det for hvert tall $\delta > 0$ finnes et y med $d_E(x, y) < \delta$ og $x \neq y$. Men da er $d_H(x, y) \geq 1$.

På den annen side er omvendt

$$\mathrm{id} : (\mathbf{R}^n, d_H) \to (\mathbf{R}^n, d_E)$$

kontinuerlig, fordi for hvert tall $\varepsilon > 0$ kan vi velge $\delta \leq 1$. Da vil $d_H(x, y) < \delta$ medføre at $x = y$ så $d_E(x, y) = 0 < \varepsilon$.

2.4.4 Eksempel. (Den *konstante avbildningen*) La (X, d_X) og (Y, d_Y) være metriske rom. Hver *konstant avbildning*

$$f : (X, d_X) \to (Y, d_Y),$$

det vil si $f(x) = f(y)$ for alle x og y i X, er kontinuerlig fordi $d_Y(f(x), f(y)) = 0$ for alle x og y.

Oppgaver.

Oppgave 1.. Vis at identitetsavbildning $\mathrm{id} : (\mathbf{R}, d_T) \to (\mathbf{R}, d_E)$ er kontinuerlig.

3. TOPOLOGISKE ROM OG KONTINUITET

3.1. Definisjon og eksempler

Den "naturlige omgivelsen" for kontinuerlige avbildninger er *topologiske rom*. Slike rom er en av grunnstenene i matematikken. De foreklommer i nesten alle deler av matematikken og tilhører de begrepene som forener mange ulike områder. Dette er en av forklaringene til vanskelighetene med å skille mellom *diskret* og *kontinuerlig* matematikk.

Vi skal her definere topologiske rom og diskutere sammenhengen med metriske rom. Videre gir vi noen eksempler på topologiske rom. For å vise hvor flytende skillet mellom *diskret* og *kontinuerlig* er gir vi et *topologisk bevis* for at det finnes uendelig mange *primtall*.

Igjen tar vi det *Euklidske rommet* $\mathbf{R}^n$ som modell. Med en ε-*omegn*, eller en *sfære* med radius ε, om et punkt x i $\mathbf{R}^n$ mener vi alle punkter med avstand mindre enn ε fra x, det vil si, mendgen

$$U_\varepsilon(x) = \{y \in \mathbf{R}^n : |x - y| < \varepsilon\}.$$

Som for de reelle tallen kaller vi en undermengde U av $\mathbf{R}^n$ *åpen* om det for hvert punkt x i U finnes en ε-omegne som ligger i U. Det er klart at X selv er åpen, og at den tomme mengden $\emptyset$ er åpen siden den ikke har noen elementer og den derfor ikke behøver å tilfredsstille noen betingelse. Videre følger det umiddelbart av definisjonen av åpen at unionen av åpne mengder er åpen. Vi har også at snittet av en endelig mengde åpne mengder er åpen, for la $U_1, U_2, \ldots, U_n$ være åpne og ta x i snittet $U_1 \cap U_2 \cap \cdots \cap U_n$. Da finnes det for hver i et tall $\varepsilon_i > 0$ slik at $U_{\varepsilon_i}(x)$ er inneholdt i U_i. Velger vi tallet $\varepsilon > 0$ mindre enn alle tallene $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ får vi at $U_\varepsilon(x)$ er inneholdt i snittet av $U_{\varepsilon_1}, U_{\varepsilon_2}, \ldots, U_{\varepsilon_n}$, og derfor inneholdt i snittet $U_1, \cap U_2 \cap \cdots \cap U_n$. Det vil si dette snittet er åpent.

De egenskapene som vi nettopp har sett holder for de åpne mengdene i $\mathbf{R}^n$ viser set å være fundamentale i analysen. Det er derfor naturlig å bruke disse som en "modell" for en mer generell situasjon:

3.1.1 Definisjon. La X være en mengde. En *topologi* på X er en familie $\mathcal{U}$ av undermengder av X slik at

(1) Mengden X selv og den *tomme mengden* $\emptyset$ er med i $\mathcal{U}$.
(2) Om vi har en familie $\{U_i\}_{i \in I}$ av undermengder U_i av X som er med i $\mathcal{U}$ så vil unionen $\cup_{i \in I} U_i$ også også være med i $\mathcal{U}$.

(3) Om $U_1, U_2, \ldots, U_n$ er undermengder av X som er med i $\mathcal{U}$ så vil snittet $\cap_{i=1}^n U_i = U_1 \cap U_2 \cap \cdots \cup U_n$ være med i $\mathcal{U}$.

Vi sier at X er et *topologisk rom* med *topologi* $\mathcal{U}$, og undermengdene U av X som er med i $\mathcal{U}$ kalles *åpne*.

3.1.2 Eksempel. (*Triviell topologi*) La X være en mengde og la $\mathcal{U}$ bestå av den tomme mengden $\emptyset$ og X. Da er X et *toplogiske rom* med *topologi* $\mathcal{U}$. Vi kaller dette den *trivielle topologien* og betegner med X_{triv} mengden X med denne topologien.

3.1.3 Eksempel. (*Diskret topologi*) La X være en mengde og la $\mathcal{U}$ bestå av alle undermengdene av X. Da er X et *topologisk rom* med *topologi* $\mathcal{U}$. I denne topologien er alle undermengdene av X åpne. Vi kaller dette den *diskrete topologien* og betegner med X_{diskr} mengden X med denne topologien.

3.1.4 Eksempel. (Metriske og topologiske rom) La X være et metrisk rom med metrikk d. Vi lar $\mathcal{U}$ være familien av alle mengder U som er slik at:

For hver x i U finnes et tall $\varepsilon > 0$ slik at om $d(x, y) < \varepsilon$ så vil y være i U.

Da er X et topologisk rom med topologi $\mathcal{U}$. For å se dette resonnerer vi som for $\mathbf{R}^n$ ovenfor. Det er klart at $\emptyset$ og X er med i $\mathcal{U}$. Videre er det klart at betingelsen (2) i
→ Definisjon (3.1.1) holder. For å vise at betingelsen (3) holder tar vi $U_1, U_2, \ldots, U_n$ i $\mathcal{U}$ og x in $U_1 \cap U_2 \cap \cdots \cap U_n$. For hver i kan vi finne et tall $\varepsilon_i > 0$ slik at $d(x, y) < \varepsilon_i$ medfører at y er i U_i. Velger vi et tall $\varepsilon > 0$ som er mindre enn $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ får vi at $d(x, y) < \varepsilon$ medfører at y er i $U_1 \cap U_2 \cap \cdots \cap U_n$.

Vi sier at $\mathcal{U}$ er topologien "gitt" av metrikken d og betegner med X_d mengden X med denne topologien.

Merk at i X_d er *sfæren*

$$U_\varepsilon(x) = \{y \in X : d(x, y) < 0\}$$

om x med radien $\varepsilon > 0$ åpen, fordi om x' er i $U_\varepsilon(x)$ velger vi $\varepsilon' = \varepsilon - d(x, x') > 0$. Om $d(x', y) < \varepsilon'$ får vi av triangelulikheten at $d(x, y) \leq d(x, x') + d(x', y) < \varepsilon - \varepsilon' + \varepsilon' = \varepsilon$ så y er i $U_\varepsilon(x)$. Det vil si sfæren $U_{\varepsilon'}(x')$ er inneholdt i $U_\varepsilon(x)$.

3.1.5 Eksempel. (*Endelig komplement topologien*) La X være en mengde og la $\mathcal{U}$ bestå av den tomme mengden $\emptyset$ og alle undermengder U av X slik at komplementet
→ $X \setminus U$ består av et endelig antall elementer. Da er det klart at egenskapen (1) i
→ Definisjon (3.1.1) er oppfylt. Videre holder egenskapen (2) fordi om $\{U_i\}_{i \in I}$ er en familie av undermengder U_i av X slik at hver $X \setminus U_i$ er endelig så vil $X \setminus \cup_{i \in I} U_i$ være inneholdt i $X \setminus U_j$ for hver j i I så $\cup_{i \in I} U_i$ er med i $\mathcal{U}$.

Videre, om $X \setminus U_1, X \setminus U_2, \ldots, X \setminus U_n$ er endelige så vil unionen av disse mengdene være endelig. Men $X \setminus \cap_{i=1}^n U_i$ er lik denne unionen så $\cap_{i=1}^n = U_1 \cap U_2 \cap \cdots \cap U_n$ er med i $\mathcal{U}$. Derfor er X et *topologisk rom* med *topologi* $\mathcal{U}$.

Denne topologien virker "eksotisk", men er viktig i geometrien. For eksempel får vi denne topologien på den *komplekse linjen* $\mathbf{R}$ om vi lar de åpne mengdene være komplementet til nullpunktene til polynomer.

3.1.6 Eksempel. (Det finnes uendelig mange primtall (se[CG])) Vi kaller en undermengde V av de hele tallene $\mathbf{Z}$ *periodisk* om det finnes et tall v slik at for alle m i V så vil både $m + v$ og $m - v$ være i V. Vi kaller tallet v en *periode* for V. Det

er klart, ved induksjon etter n, at V er periodisk med en periode v hvis og bare hvis $m + nv$ er i V for alle m i V og alle hele tall n.

Vi har:

(1) Om V er periodisk med en periode v så er komplementet $\mathbf{Z} \setminus V$ også periodisk med en periode v.
(2) Om V og W er periodiske med perioder v, respektive w, så er unionen $V \cup W$ periodisk med periode vw.

Egenskapen (1) følger av at om m ikke er i V så kan heller ikke $m+v$ eller $m-v$ være i V, for om $m+v$ eller $m-v$ er i V så er også $m = m+v-v$ eller $m = m-v+v$ i V, hvilket er mot forutsetningen at m ikke er i V. At egenskapen (2) holder er opplagt.

Vi merker at av egenskapen (2) følger, ved induksjon etter antallet periodiske mengder, at enhver endelig union av periodiske mengder er periodisk.

Nu kan vi lett vise at det finnes uendelig mange primtall. Anta motsatsen og at $p_1, p_2, \ldots, p_n$ er alle primtall. La V_i være mengden av alle tall np_i for alle heltall n. Da er V_i periodisk med en periode p_i. Ettersom alle tall forskjellige fra -1 og 1 er delbare med et primtall vil $V_1 \cup V_2 \cup \cdots \cup V_n$ bestå av alle tall untatt $\{-1, 1\}$. Men vi har sett at unionen av et endelig antall periodiske mengder er periodisk, og at komplementet til en periodisk mengde er periodisk. Derfor må komplementet til $V_1 \cup V_2 \cup \cdots \cup V_n$ være periodisk. Men $\{-1, 1\}$ er ikke periodisk. Derfor har vi fått en motsigelse til antagelsen om at vi har et endelig antall primtall.

→ 3.1.7 Merk. Eksempel (3.1.6) er et *kontinuerlig* bevis for at det finnes uendelig mange primtall. For å se sammenhengen med *topologiske rom* merker vi at om vi har en mengde X og en familie $\mathcal{V}$ av undermengder av X slik at X er unionene av alle mengdene i $\mathcal{V}$ og snittet av et endelig antall mengder i $\mathcal{V}$ vil være i $\mathcal{V}$, så vil familien $\mathcal{U}$ som består av alle undermengder av X som er unionen av mengder i $\mathcal{V}$ danne en topologi for X.

→ Det er klart at $\emptyset$ og X begge er med i $\mathcal{U}$, og at egenskap (2) for topologiske rom
→ holder. For å vise at egenskapen (3) holder tar vi $U_1, U_2, \ldots, U_n$ i $\mathcal{U}$ og x i snittet $U_1 \cap U_2 \cap \cdots \cap U_n$ av disse mengdene. For hver i vil det finnes en V_i som er med i $\mathcal{V}$, som inneholder x, og som er inneholdt i U_i. La $U = V_1 \cap V_2 \cap \cdots \cap V_n$. Da er U med i $\mathcal{V}$ ved antagelsen at snittet av et endelig antall mengder som er med i $\mathcal{V}$ er med i $\mathcal{V}$. Videre er det klart at U inneholder x og er inneholdt i $U_1 \cap U_2 \cap \cdots \cap U_n$. Derfor er $U_1 \cap U_2 \cap \cdots \cap U_n$ unionen av mengder som er med i $\mathcal{V}$ så U er med i $\mathcal{U}$.

La nu $\mathcal{V}$ bestå av alle periodiske mengder i $\mathbf{Z}$. Det er klart at unionen av periodiske mengder er $\mathbf{Z}$. Vi må vise at snittet av et endelig antall periodiske mengder er
→ periodisk. Dette følger av (1) og (2) ovenfor fordi, om $V_1, V_2, \ldots, V_n$ er periodiske
→ undermengder av $\mathbf{Z}$, så følger det av (1) at komplementene $X \setminus V_1, X \setminus V_2, \ldots, X \setminus V_n$
→ også være periodiske, og derfor av (2) vil $(X \setminus V_1) \cup (X \setminus V_2) \cup \cdots \cup (X \setminus V_n) = X \setminus \cap_{i=1}^n V_i$
→ være periodisk. Det følger da, igjen av (1), at snittet $\cap_{i=1}^n V_i$ er periodisk.

Som vi så ovenfor vil derfor familien $\mathcal{U}$ som består av alle undermengder av $\mathbf{Z}$ som er unionen av periodiske undermengder vil danne en topologi. En analyse av beviset viser at denne topologien er essensiell i beviset for at vi har uendelig mange primtall. Det opprinnelige beviset av Fürstenberg var også "rent topologisk" (se [R]).

Oppgaver.

OPPGAVE 1. Vis at X med den diskrete topologien er et metrisk rom.

→ OPPGAVE 2. Vis at (X, d_T) og (X, d_E) fra Eksemplene (?) og (?) gir samme topologiske rom. Det er dette vi mener når vi sier at metrikkene d_T og d_E er *ekvivalente*.

OPPGAVE 3. Vis at X med den *trivielle topologien* ikke kommer fra en metrikk om X har mer enn 1 element.

OPPGAVE 4. Vis at snittet av uendelig mange åpne mengder i $\mathbf{R}^n$ ikke behøver å være åpen.

OPPGAVE 5. Vi at vi får en topologi på den reelle linjen ved å la de åpne mengdene være komplementet til nullpunktene til polynomer med reelle koeffisienter. Er dette den *endelig komplement topologien*?

3.2. Kontinuitet

I *topologiske rom* finner begrepet *kontinuitet* sin riktige plass med føgende definisjon:

3.2.1 DEFINISJON. La X og Y være topologiske rom med topologier $\mathcal{U}$, respektive $\mathcal{V}$. En avbildning

$$f : X \to Y$$

er *kontinuerlig* om det *inverse bildet* $f^{-1}(V)$ av hver åpen mengde i Y er åpen i X.

For at denne definisjonen skal være brukbar er det viktig at om X og Y også er *metriske rom* og topologiene er gitt av metrikkene på de topologiske rommene, som i → Eksempel (3.1.4) så må *kontinuitet* for *topologiske rom* sammenfalle med *kontinuitet* for *metriske rom*. Neste setning viser at dette er sant.

3.2.2 SETNING. *La X og Y være metriske rom med metrikker d_X, respektive d_Y, og la $\mathcal{U}$ og $\mathcal{V}$ være topologiene gitt av d_X, respektive d_Y. En avbildning*

$$f : X \to Y$$

er en kontinuerlig avbildning av metriske rom $f : (X, d_X) \to (Y, d_Y)$ hvis og bare hvis den er kontinuerlig av topologiske rom $f : X_{d_X} \to X_{d_Y}$.

PROOF. Anta at $f : (X, d_X) \to (Y, d_Y)$ er en kontinuerlig avbildning av metriske rom og la V være åpen i Y. Vi må vise at $f^{-1}(V)$ er åpen i X. Det vil si, for alle x i $f^{-1}(V)$ må vi finne et tall $\delta > 0$ slik at om $d_X(x, x') < \delta$ så vil x' være i V. Vi har at $f(x)$ er i V, og ettersom V er åpen i Y finnes det et tall $\varepsilon > 0$ slik at om $d_Y(f(x), y') < \varepsilon$ så vil y' være i V. Ettersom f er kontinuerlig av metriske rom ved antagelsen kan vi finne et tall $\delta > 0$ slik at når $d_X(x, x') < \delta$ så vil $d_Y(f(x), f(x')) < \varepsilon$. Men da er $f(x')$ i V, eller ekvivalent, vi har at x' er i $f^{-1}(V)$. Om $d_X(x, x') < \delta$ er altså x' i $f^{-1}(V)$ hvilket viser at $f^{-1}(V)$ er åpen i X.

Anta omvendt at $f : X \to Y$ er en kontinuerlig avbildning av topologiske rom. Vi må vise at for hvert tall $\varepsilon > 0$ kan vi finne et tall $\delta > 0$ slik at om $d_X(x, x') < \delta$ så

→ vil $d_Y(f(x), f(x')) < \varepsilon$. Vi så i Eksempel (3.1.4) at *sfæren* $U_\varepsilon(f(x))$ med radius ε og sentrum $f(x)$ er åpen i X. Vi har at $f(x)$ er i $U_\varepsilon(f(x))$ så x er i $f^{-1}(U_\varepsilon(f(x)))$. Ettersom f er kontinuerlig er $f^{-1}(U_\varepsilon(f(x)))$ åpen i X. Det følger derfor av at topologien på X er gitt av metrikken d_X at det finnes et tall $\delta > 0$ slik at om $d_X(x, x') < \delta$ så vil x' være i $f^{-1}(U_\varepsilon(f(x)))$. Men da er $f(x')$ i $U_\varepsilon(f(x))$, det vil si, vi har $d_Y(f(x), f(x')) < \varepsilon$. Vi har altså vist at om $d_X(x, x') < \delta$ så vil $d_Y(f(x), f(x')) < \varepsilon$, hvilket viser at f er en kontinuerlig avbildning av metriske rom.

3.2. Oppgaver.

OPPGAVE 1. Vis at alle avbildninger

$$f : X_{\text{disk}} \to X_{\text{triv}}$$

er kontinuerlige.

OPPGAVE 2. Vis at de eneste kontinuerlige avbildningene

$$f : X_{\text{triv}} \to X_{\text{disk}}$$

er de *konstante avbildningene*.

4. BLOKK-KODER OG HAMMING METRIKKEN

4.1. Et eksempel på blokk-koder

Vi skal her gi et viktig eksempel på en endelig mengde med en avstand, det vil si en metrikk som kommer fra kodeteorien. Som alle vet kan all informasjon overføres til digital kode, det vil si, til strenger av 0'er og 1'ere. Det vanlige er at all informasjon som skal lagres eller sendes skrives som strenger av 0'er og 1'ere av en fast *lengde* n. Vi skal bruke en mer fantsieggende terminologi og si at informasjon er overført til *ord av lengde* n *med bokstaver fra alfabetet* $0, 1$. For eksempel er *byte* en vanlig enhet for informasjon, og betyr den informasjonen som rommes i de $2^8 = 256$ ordene av lengde 8 fra alfabetet $0, 1$.

Avstanden mellom to ord definierer vi som antallet posisjoner der ordene er ulike, det vil si, vi bruker *Hamming metrikken* som vi stiftet bekjenskap med i Eksempel
→ (2.3.4). For eksempel er avstanden $d(x, y)$ mellom ordene $x = 01100111$ og $y = 10101100$ lik 5 fordi de skiller seg i første, andre, femte, syvende og åttende posisjon. Avstanden mellom $x = 11110000$ og $y = 00001111$ er 8 ettersom x og y skiller seg i alle de 8 posisjonene.

At Hamming metrikken er både naturlig og viktig ser vi når vi bruker den på *feilrettende koder*. Anta at vi vil sende informasjon i form av ord av lengde 8 med bokstaver fra alfabetet $0, 1$ over en kanal der det forekommer støy slik at det ordet som blir mottat kan skille seg fra det ordet vi sendte. Hva skal vi gjøre for å oppdage, eller til og med rette, feil? Den vanligste måten å oppdage feil på er ved å foreta en *paritetskontroll*, det vil si, vi lar selve meddelelsen være de første 7 bokstavene og lar den 8'ende bokstaven være 0 om det forekommer et like antall 1'ere blandt de syv første bokstaven, og lar den være 1 om det forekommer et odde antall 1'ere. Vi kaller den 8'ende bokstaven for et *kontrollsiffer*. For eksempel har ordene 01100110 og 10101111 rett paritet. Sender vi ordet 01100110 og det oppstår en feil slik at vi mottar 01101110 eller 01100111 så har ordet vi mottar feil paritet og vi vet at en feil har oppstått. Derimot kan vi ikke oppdage to feil ettersom ordet 00000110 har rett paritet og forekommer fra 01100110 om vi gjør en feil i andre og tredje posisjonen. Vi kan heller ikke rette en feil fordi ordet 01101110 som har feil paritet kan fremkomme fra 01100110 og 01101100, begge med rett paritet, om vi gjør en feil.

Prisen for å oppdage en feil er at vi bare kan sende $2^7 = 128$ meddelelser, ettersom den 8'ende bokstaven er bestemt av de 7 første. Vil vi dessuten rette en feil er prisen mye høyere. For å se dette bruker vi Hammingmetrikken for å få et geometrisk bilde av situasjonen. Om vi skal rette en feil må avstanden mellom to *kodeord* være

minst 3. Dette er fordi, om vi sender et kodeord x og mottar ordet x' med 1 feil, vil $d(x, x') = 1$. Om y er et annet kodeord og $d(x, y) \geq 3$ får vi av triangelulikheten at

$$3 \leq d(x, y) \leq d(x, x') + d(x', y) = 1 + d(x', y),$$

det vil si, vi har $d(x', y) \geq 2$. Med andre ord må det har forekommet minst 2 feil om vi sendte y og mottok x'. Derfor må vi ha sendt x om det bare har forekommet en feil. Vi kan formulere kravet at avstanden mellom to kodeord skal være minst 3 geometrisk ved å si at for å rette en feil må hver sfære med radius 1 omkring et kodeord ikke inneholde noe annet kodeord.

Vi kan håpe at det rekker å bruke to kontrollsifre for å rette en feil. Faktum er at det ikke engang rekker med tre kontrollsifre. For å se dette merker vi at en sfære med radius 1 omkring et ord x inneholder nøyaktig 9 ord, nemlig x og de 8 ordene vi får av x ved å endre på en bokstav. Om vi skal rette en feil så vi at sfærene av radius 1 om kodeordene må være disjunkte. Bruker vi 3 kontrollsifre kan vi velge de fem første sifrene fritt så vi har 2^5 kodeord og de 2^5 sfærene om disse med radius 1 må være disjunkte. Dette gir $2^5(2^3+1) = 2^8+2^5$ kodeord, som er mer enn det totale antallet 2^8 kodeord av lengde 8 med bokstaver fra alfabetet $0, 1$. Dette er umulig, så vi har vist at vi må bruke minst 4 kontrollsifre for å rette en feil. I sannhet en høy pris. Dette forklarer hvorfor det er så viktig å finne gode koder med få kontrollsifre i forhold til antallet kodeord.

Mer generelt består en *blokk-kode* av lengde n fra et alfabet A av en undermengde C av mengden B av alle ord av lengde n med bokstaver fra alfabetet A. Elementene i C kalles *kodeord*. Avstanden $d(x, y)$ mellom *ordene* x og y er antallet posisjoner der ordene x og y er forskjellige, det vil si, vi bruker *Hamming metrikken* fra Eksempel
→ (2.3.4). *Hamming distansen* d_C for en kode C er den minste avstanden mellom to kodeord, det vil si

$$d_C = \min\{d(x, y) : \text{for alle ulike punkter } x \text{ og } y \text{ i } C\}.$$

En kode med Hamming distanse d_C kan rette $\lfloor (d_C - 1)/2 \rfloor$ feil. Dette sees som ovenfor. Om ordet x i C er et kodeord og x' et ord vi får fra x om vi gjør høyst $\lfloor (d_C - 1)/2 \rfloor$ feil så gir triangelulikheten at for hvert kodeord y så vil

$$d_C \leq d(x, y) \leq d(x, x') + d(x', y) \leq \lfloor (d_C - 1)/2 \rfloor + d(x', y) < d_C/2 + d(x', y).$$

Det vil si at $(d_C - 1)/2 < d_C/2 < d(x', y)$ så x er det eneste kodeordet som kan gi opphav til x' om vi gjør høyst $\lfloor (d_C - 1)/2 \rfloor$ feil.

Oppgaver.

OPPGAVE 1. Med alfabetet $\{0, 1\}$ og ordlengde 8, konstruer en kode med 2^4 kodeord som kan rette en feil.

4.2. Et eksempel på lineære koder

Det er lett å forstå at det er vanskelig å konstruere koder med mange kodeord i forhold til kontrollsifre. Kodene skal også være lette å bruke, så det må finnes enkle regler for *kodning* og *avkodning*. Vi skal se at oppgaven blir mye lettere om vi har

de vanlige *aritmetiske operasjonen*, *addisjon*, *subtraksjon*, *multiplikasjon* og *divisjon* i vårt *alfabet*. Dette har vi i $\{0,1\}$ som har *addisjontabell* og *multiplikasjonstabell*

$+$	0	1
0	0	1
1	1	0

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

Det samme gjelder for alfabetet $\{0,1,2\}$ der de aritmetiske operasjonene er gitt av *addisjonstabellen* og *multiplikasjonstabellen*

$+$	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

Vi kaller slike *alfabeter*, der vi kan *addere*, *subtrahere*, *multiplisere* og *dividere*, og de vanlige renereglene gjelder for *kropper*. For hver potens $q = p^k$ av et primtall p finnes det "essensielt" en eneste kropp med q elementer, som betegnes med $\mathbf{F}_q$. Disse er de eneste kroppene med et endelig antall elementer. Kropper med et endelig antall elementer kalles *Galois kropper*. Det finnes selvsagt et stort utvalg av kropper med uendelig mange elementer, som de rasjonale tallene $\mathbf{Q}$, de reelle tallene $\mathbf{R}$ og de *komplekse tallene* $\mathbf{C}$.

Vi illustrer de store vinningene vi får ved å benytte de artimetiske operasjonene med et eksempel der alfabetet er $\mathbf{F}_2 = \{0,1\}$ har to elementer, og kodeordene lengde 7.

Når alfabetet er en kropp er det vanlig å skrive kodeordene på *vektor form*, slik at om $x = 0110011$ og $y = 1010110$ så skriver vi $x = (0,1,1,0,0,1,1)$ og $y = (1,0,1,0,1,1,0)$. vi kan nu *addere ord*, ved å addere dem *komponentvis*, som vi gjør med vektorer. For eksempel har vi

$$x + y = (0+1, 1+0, 1+1, 0+0, 0+1, 1+1, 1+0) = (1,1,0m0,1,0,1).$$

Anta vi vil kode de 2^3 ordene av lengde 3 fra alfabetet $\{0,1\}$, som vi skriver

$$\begin{aligned} x_0 &= (0,0,0), \quad x_1 = (1,0,0), \quad x_2 = (0,1,0), \quad x_3 = (0,0,1) \\ x_4 &= (1,1,0), \quad x_5 = (1,0,1), \quad x_6 = (0,1,1), \quad x_7 = (1,1,1). \end{aligned}$$

For å gjøre en enkel *paritetskontroll*, som vi gjorde ovenfor, rekker det å multiplisere med matrisen

$$P = \begin{pmatrix} 1&0&0&1 \\ 0&1&0&1 \\ 0&0&1&1 \end{pmatrix}.$$

Matrisemultiplikasjon gir

$$\begin{aligned} x_0P &= (0,0,0,0), \quad x_1P = (1,0,0,1), \quad x_2P = (0,1,0,1) \quad x_3P = (0,0,1,0) \\ x_4P &= (1,1,0,0), \quad x_5P = (1,0,1,0), \quad x_6P = (0,1,1,0), \quad x_7P = (1,1,1,1)), \end{aligned}$$

det vil si, matrisemultiplikasjonen legger til en koordinat som gir *pariteten* av antallet 1'ere i de første 3 koordinatene.

Vi kan utvide paritetskontrollen til mer kompliserte *kontrollsifre* ved å multiplisere med større matriser. Multipliserer vi for eksempel alle ordene av lengde 3 med med 3×6-matrisen

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

får vi

$$\begin{aligned} &x_0P = (0,0,0,0,0,0), \quad x_1P = (1,0,0,1,1,0), \quad x_2P = (0,1,0,1,0,1) \\ &x_3P = (0,0,1,0,1,1), \quad x_4P = (1,1,0,0,1,1), \quad x_5P = (1,0,1,1,0,1) \\ &x_6P = (0,1,1,1,1,0), \quad x_7P = (1,1,1,0,0,0)). \end{aligned}$$

Ettersom de ordene $x_0, x_1, \ldots, x_7$ i den opprinnelige meddelsen kan legges sammen og multipliseres med elementer K kan vi legge sammen ord i *blokk-koden* og multiplisere dem med elementer i K, og få nye ord i *blokk-koden* fordi regnereglene for matrisemultiplikasjon gir

$$x_iP + x_jP = (x_i + x_j)P \quad \text{og} \quad a(x_iP) = (ax_i)P.$$

Vi kaller derfor koden for en *lineær kode*. Som vi nettopp så kan vi med matrisemultiplikasjon enkelt kode meddelelsene slik at vi får en lineær kode. Det er også mye enklere å regne ut *Hamming distansen* til lineære koder, fordi vi lett viser at

$$d_H(x,y) = d_H(0, x-y)$$

for alle ord x og y. Istedenfor å regne ut avstanden $d_H(x,y)$ for alle de $2^3 2^3 = 64$ parene x, y rekker det å regne ut de syv tallene $d_H(0, x_iP)$ for $0, 1, \ldots, 7$. Vi ser umiddelbart at *Hamming distansen* er 3, så koden kan rette 1 feil. For lange ord får vi en veldig besparing når vi skal regne ut Hamming distansen.

Når vi har aritmetiske operasjoner i *alfabetet* og betrakter lineære koder er det også mye enklere å *avkode* kodeordene. For eksempel kan vi danne 6×3 matrisen

$$H = \begin{pmatrix} 1&1&0 \\ 1&0&1 \\ 0&1&1 \\ 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}.$$

Vi kontrollerer lett at

$$PH = \begin{pmatrix} 1&0&0&1&1&0 \\ 0&1&0&1&0&1 \\ 0&0&1&0&1&1 \end{pmatrix} \begin{pmatrix} 1&1&0 \\ 1&0&1 \\ 0&1&1 \\ 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} = \begin{pmatrix} 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}.$$

Det betyr at $(x_iP)H = 0$ for alle kode ord x_iP. Det er også lett å kontrollere at det omvendte gjelder, det vil si, om $yH = 0$ for et ord y så vil $y = x_iP$ være

et kodeord for noe i. Dette kan også vises teoretisk ved å merke at søylene i H danner et *vektorrom* av dimensjon 3. Derfor gir $yH = 0$ tre *uavhengige ligninger* i seks *ukjente*. Løsningene danner derfor et $6 - 3 = 3$ dimensjonalt vektorrom. Dette rommet inneholder $x_0P, x_1P, \ldots, x_7P$, der x_1P, x_2P, x_3P er *lineært uavhengige*. Derfor vil $x_0P, x_1P, \ldots, x_7P$ være alle løsningene.

Sender vi en vektor x_iP og det ved overføringen blir en feil i j'te posisjonene mottar vi vektoren $y = x_iP + e_j$, der e_j er 6 vektoren med 1 i j'te posisjon og 0'er ellers. Vi får

$$yH = (x_iP + e_j)H = x_iPH + e_jH = e_jH,$$

det vil si, vi får j'te raden i H. For eksempel, om vi sender $x_1P = (1, 0, 0, 1, 1, 0)$ og mottar $y = (1, 1, 0, 1, 1, 0)$ får vi $yH = (1, 0, 1)$ som er andre radne i H. Mottar vi $y = (1, 0, 0, 1, 1, 1)$ får vi $yH = (0, 0, 1)$ som er 6'te raden i H. Vi kan derfor rette en feil ved å regne ut yH. Om $yH = 0$ vil $y = x_iP$ for noe i og vi *avkoder* y som x_i. Om yH er j'te rekke i H har vi at $(y - e_j)H = yH - e_jH = 0$ så $y - e_j = x_iP$ for noe i, og vi avkoder y til x_i. På denne måten retter vi 1 feil.

Merk at vi ikke kan oppdage to feil, for om vi mottar $y = (1, 10, 1, 1, 1)$ som er x_1P med feil i 2'ndre og 6'te posisjon får vi $yH = (1, 0, 0)$ som vi også får om vi mottar $(1, 1, 1, 1, 0, 0)$ som er x_7P med 1 feil i 4'de posisjon.

Oppgaver.

Oppgave 1. Vis at addisjonstabellen og multiplikasjonstabellen i alfabetet med tre elementer $\{0, 1, 2\}$ gjør at vi også kan subtrahere og dividere.

Oppgave 2. Vis at $d_H(x, y) = d_H(0, x - y)$ for alle vektorer x og y med elementer fra en kropp.

Oppgave 3. Fant vi matrisen H ved et "mirakel", eller kan du se noe system?

Oppgave 4. Kontroller at $yH = 0$ hvis og bare hvis x sammenfaller med et av ordene $x_0, x_1, \ldots, x_7$.

A. APPENDIX. AMS-KLASSIFIKASJONEN

A.1 Hovedområder

00 General
01 History and biography
03 Mathematical logic
05 Combinatorics
06 Order, lattices, ordered algebraic structures
08 General algebraic systems
11 Number theory
12 Field theory and polynomials
13 Commutative rings and algebras
14 Algebraic geometry
15 Linear and multilinear algebra; matrix theory
16 Associative rings and algebras
17 Nonassociative rings and algebras
18 Category theory, homological algebra
19 K-theory
20 Group theory and generalizations
22 Topological groups, Lie groups
26 Real functions
28 Measure and integration
30 Functions of a complex variable
31 Potential theory
32 Several complex variables and analytic spaces
33 Special functions
34 Ordinary differential equations
35 Partial differential equations
37 Dynamical systems and ergodic theory
39 Finite differences and functional equations
40 Sequences, series, summability
41 Approximations and expansions
42 Fourier analysis
43 Abstract harmonic analysis
44 Integral transforms, operational calculus
45 Integral equations
46 Functional analysis

47 Operator theory
49 Calculus of variations and optimal control
51 Geometry
52 Convex and discrete geometry
53 Differential geometry
54 General topology
55 Algebraic topology
57 Manifolds and cell complexes
58 Global analysis, analysis on manifolds
60 Probability theory and stochastic processes
62 Statistics
65 Numerical analysis
68 Computer science
70 Mechanics of particles and systems
73 Mechanics of deformable solids
76 Fluid mechanics
78 Optics, electromagnetic theory
80 Classical thermodynamics, heat transfer
81 Quantum Theory
82 Statistical mechanics, structure of matter
83 Relativity and gravitational theory
85 Astronomy and astrophysics
86 Geophysics
90 Economics, operations research, programming
91 Game theory, economics, social and behavioral sciences
92 Biology and other natural sciences
93 Systems theory; control
94 Information and communication, circuits
97 Mathematics education

A.2 Delområder av Algebraisk Geometri

14-XX Algebraic geometry

14Axx Foundations
14Bxx Local theory
14Cxx Cycles and subschemes
14Dxx Families, fibrations
14Exx Birational Geometry
14Fxx (Co)homology theory [See also 13Dxx]
14Gxx Arithmetic problems. Diophantine geometry [See also]
14Hxx Curves
14Jxx Surfaces and higher-dimensional varieties (For analytic theory, see 32Jxx)
14Kxx Abelian varieties and schemes
14Lxx Algebraic Groups (For linear algebraic groups, see 20Gxx;
14Mxx Special varieties
14Nxx Projective and enumerative geometry
14Pxx Real algebraic and real analytic geometry
14Qxx Computational aspects in algebraic geometry
14Rxx Affine Geometry

A.3 Spesialområdene av Algebraisk Geometri

14-XX Algebraic geometry

14A05 Relevant commutative algebra [See also 13-xx]
14A10 Varieties and morphisms
14A15 Schemes and morphisms
14A20 Generalizations (algebraic spaces, stacks)
14A22 Noncommutative algebraic geometry
14A25 Elementary questions
14A99 None of the above, but in this section

14Bxx Local theory

14B05 Singularities [See also 14E15, 14H20, 4J17, 32Sxx, 58Kxx]
14B07 Deformations of singularities [See also 14D15, 32S30]
14B10 Infinitesimal methods [See also 13D10]
14B12 Local deformation theory, Artin approximation, etc. [See also 13B40, 13D10]
14B15 Local cohomology [See also 13D45, 32C36]
14B20 Formal neighborhoods
14B25 Local structure of morphisms: tale, flat, etc. [See also 13B40]
14B99 None of the above, but in this section

14Cxx Cycles and subschemes

14C05 Parametrization (Chow and Hilbert schemes)
14C15 Chow groups and rings
14C17 Intersection theory, characteristic classes, intersection multiplicities [See also 13H15]
14C20 Divisors, linear systems, invertible sheaves
14C21 Pencils, nets, webs [See also 53A60]
14C22 Picard groups
14C25 Algebraic cycles
14C30 Transcendental methods, Hodge theory [See also 14D07, 32G20, 32J25, 32S35], Hodge conjecture
14C34 Torelli problem [See also 32G20]
14C35 Applications of methods of algebraic K-theory [See also 19Exx]
14C40 Riemann-Roch theorems [See also 19E20, 19L10]
14C99 None of the above, but in this section

14Dxx Families, fibrations

14D05 Structure of families (Picard-Lefschetz, monodromy, etc.)
14D06 Fibrations, degenerations
14D07 Variation of Hodge structures [See also 32G20]
14D10 Arithmetic ground fields (finite, local, global)
14D15 Formal methods; deformations [See also 13D10, 14B07, 32Gxx]
14D20 Algebraic moduli problems, moduli of vector bundles (For analytic moduli problems, see 32G13)
14D21 Applications of vector bundles and moduli spaces in mathematical physics (twistor theory, instantons, quantum field theory)

14D22 Fine and coarse moduli spaces
14D99 None of the above, but in this section

14Exx Birational Geometry
14E05 Rational and birational maps
14E07 Birational automorphisms, Cremona group and generalizations
14E08 Rationality questions
14E15 Global theory and resolution of singularities [See also 14B05, 32S20, 32S45]
14E20 Coverings [See also 14H30]
14E22 Ramification problems [See also 11S15]
14E25 Embeddings
14E30 Minimal model program (Mori theory, extremal rays)
14E99 None of the above, but in this section

14Fxx (Co)homology theory [See also 13Dxx]
14F05 Vector bundles, sheaves, related constructions [See also 14H60, 14J60, 18F20, 32Lxx, 46M20]
14F10 Differentials and other special sheaves [See also13Nxx, 32C38]
14F17 Vanishing theorems [See also 32L20]
14F20 tale and other Grothendieck topologies and cohomologies
14F22 Brauer groups of schemes [See also 12G05, 16K50]
14F25 Classical real and complex cohomology
14F30 p-adic cohomology, crystalline cohomology
14F35 Homotopy theory; fundamental groups [See also 14H30]
14F40 de Rham cohomology [See also 14C30, 32C35, 32L10]
14F42 Motivic cohomology
14F43 Other algebro-geometric (co)homologies (e.g., intersection, equivariant, Lawson, Deligne (co)homologies)
14F45 Topological properties
14F99 None of the above, but in this section

14Gxx Arithmetic problems. Diophantine geometry [See also 11Dxx, 11Gxx]
14G05 Rational points
14G10 Zeta-functions and related questions [See also 11G40] (Birch-Swinnerton-Dyer conjecture)
14G15 Finite ground fields
14G20 Local ground fields
14G22 Rigid analytic geometry
14G25 Global ground fields
14G27 Other nonalgebraically closed ground fields
14G32 Universal profinite groups (relationship to moduli spaces, projective and moduli towers, Galois theory)
14G35 Modular and Shimura varieties [See also 11F41, 11F46, 11G18]
14G40 Arithmetic varieties and schemes; Arakelov theory; heights [See also 11G50]
14G50 Applications to coding theory and cryptography [See also 94A60, 94B27, 94B40]

14G99 None of the above, but in this section

14Hxx Curves

14H05 Algebraic functions; function fields [See also 11R58]
14H10 Families, moduli (algebraic)
14H15 Families, moduli (analytic) [See also 30F10, 32Gxx]
14H20 Singularities, local rings [See also 13Hxx, 14B05]
14H25 Arithmetic ground fields [See also 11Dxx, 11G05, 14Gxx]
14H30 Coverings, fundamental group [See also 14E20, 14F35]
14H37 Automorphisms
14H40 Jacobians, Prym varieties [See also 32G20]
14H42 Theta functions; Schottky problem [See also 14K25, 32G20]
14H45 Special curves and curves of low genus
14H50 Plane and space curves
14H51 Special divisors (gonality, Brill-Noether theory)
14H52 Elliptic curves [See also 11G05, 11G07, 14Kxx]
14H55 Riemann surfaces; Weierstrass points; gap sequences [See also 30Fxx]
14H60 Vector bundles on curves and their moduli [See also 14D20, 14F05]
14H70 Relationships with integrable systems
14H81 Relationships with physics
14H99 None of the above, but in this section

14Jxx Surfaces and higher-dimensional varieties (For analytic theory, see 32Jxx)

14J10 Families, moduli, classification: algebraic theory
14J15 Moduli, classification: analytic theory; relations with modular forms [See also 32G13]
14J17 Singularities [See also 14B05, 14E15]
14J20 Arithmetic ground fields [See also 11Dxx, 11G25, 11G35, 14Gxx]
14J25 Special surfaces For Hilbert modular surfaces, see 14G35
14J26 Rational and ruled surfaces
14J27 Elliptic surfaces
14J28 $K3$ surfaces and Enriques surfaces
14J29 Surfaces of general type
14J30 3-folds
14J32 Calabi-Yau manifolds, mirror symmetry
14J35 4-folds
14J40 n-folds ($ngt; 4$)
14J45 Fano varieties
14J50 Automorphisms of surfaces and higher-dimensional varieties
14J60 Vector bundles on surfaces and higher-dimensional varieties, and their moduli [See also 14D20, 14F05, 32Lxx]
14J70 Hypersurfaces
14J80 Topology of surfaces (Donaldson polynomials, Seiberg-Witten invariants)
14J81 Relationships with physics
14J99 None of the above, but in this section

14Kxx Abelian varieties and schemes

14K02 Isogeny

14K05 Algebraic theory
14K10 Algebraic moduli, classification [See also 11G15]
14K12 Subvarieties
14K15 Arithmetic ground fields [See also 11Dxx, 11Fxx, 11Gxx, 4Gxx]
14K20 Analytic theory; abelian integrals and differentials
14K22 Complex multiplication [See also 11G15]
14K25 Theta functions [See also 14H42]
14K30 Picard schemes, higher Jacobians [See also 14H40, 32G20]
14K99 None of the above, but in this section

14Lxx Algebraic Groups (For linear algebraic groups, see 20Gxx; for Lie algebras, see 17B45)

14L05 Formal groups, p-divisible groups [See also 55N22]
14L10 Group varieties
14L15 Group schemes
14L17 Affine algebraic groups, hyperalgebra constructions [See also 17B45, 18D35]
14L24 Geometric invariant theory [See also 13A50]
14L30 Group actions on varieties or schemes (quotients) [See also 13A50, 14L24]
14L35 Classical groups (geometric aspects) [See also 20Gxx, 51N30]
14L40 Other algebraic groups (geometric aspects)
14L99 None of the above, but in this section

14Mxx Special varieties

14M05 Varieties defined by ring conditions (factorial, Cohen-Macaulay, seminormal) [See also 13F45, 13H10]
14M06 Linkage [See also 13C40]
14M07 Low codimension problems
14M10 Complete intersections [See also 13C40]
14M12 Determinantal varieties [See also 13C40]
14M15 Grassmannians, Schubert varieties, flag manifolds [See also 32M10, 51M35]
14M17 Homogeneous spaces and generalizations [See also 32M10, 53C30, 57T15]
14M20 Rational and unirational varieties
14M25 Toric varieties, Newton polyhedra [See also 52B20]
14M30 Supervarieties [See also 32C11, 58A50]
14M99 None of the above, but in this section

14Nxx Projective and enumerative geometry

14N05 Projective techniques [See also 51N35]
14N10 Enumerative problems (combinatorial problems)
14N15 Classical problems, Schubert calculus
14N20 Configurations of linear subspaces
14N25 Varieties of low degree
14N30 Adjunction problems
14N35 Gromov-Witten invariants, quantum cohomology [See also 53D45]
14N99 None of the above, but in this section

14Pxx Real algebraic and real analytic geometry

14P05 Real algebraic sets [See also 12Dxx]
14P10 Semialgebraic sets and related spaces
14P15 Real analytic and semianalytic sets [See also 32B20, 32C05]
14P20 Nash functions and manifolds [See also 32C07, 58A07]
14P25 Topology of real algebraic varieties
14P99 None of the above, but in this section

14Qxx Computational aspects in algebraic geometry

14Q05 Curves
14Q10 Surfaces, hypersurfaces
14Q15 Higher-dimensional varieties
14Q20 Effectivity
14Q99 None of the above, but in this section

14Rxx Affine Geometry

14R05 Classification of affine varieties
14R10 Affine spaces (automorphisms, embeddings, exotic structures, cancellation problem)
14R15 Jacobian problem
14R20 Group actions on affine varieties [See also 13A50, 14L30]
14R25 Affine fibrations [See also 14D06]
14R99 None of the above, but in this section

BIBLIOGRAFI

[AMS] *AMS subject classification 2000*, American Mathematica Society, Providence, RI, 2000.

[CG] D. Cass & G. Wildenberg, *Math bite: A novel proof of the infinitude of primes, revisited*, Mathematics Magzine **76 (3)** (June 2003), 203.

[L] Dan Laksov, *Diskret matematikk finnes ikke*, NORMAT **52** (2004), 21-38.

[R] P. Ribenboim, *The little book of big primes*, Springer Verlag, New Yord, 1991.

[S] *Välj specialarbete i Matematik*, Redaktør Dan Laksov. Se også nettversjonen `http://www.math.kth.se/~laksov`, THD AB, Bandhagen, 1989.

INDEX