

Grafer

En **graf** $G = (V, E)$ består av

- en (ändlig) mängd V vars element kallas **noder** (eller hörn)
- och en mängd E med **kantar** som är ordnade par av noder

Förkortar oftare ab för kanten $\{a, b\}$

Ibland tillåts öglor/loopar, d.v.s. t.ex. $\{a, a\}$

Ibland tillåts multigraf, d.v.s. flera kantar med samma par av noder

Grannar

$x, y \in V$ sägs vara grannar (neighbors, adjacent) i grafen om $xy \in E$

För en graf $G = (V, E)$ definierar vi **grannmängden**

$$N_G(x) := \{y \mid xy \in E\} \text{ (eller bara } N(x))$$

I en grannlista (adjacency list) för G anges för varje hörn vilka dess grannar är.

Ett annat är att använda en **grannmatrix** M med rader och kolumner indexerade av V , där $M = \{m_{i,j}\}$, $m_{i,j} = \begin{cases} 1, & ij \in E \\ 0, & \text{annars} \end{cases}$

D.v.s. 1 i position ij om hörn i och hörn j är grannar, 0 annars.

Antalet grannar en nod x har kallas för dess **Valens** (eller **grad**) och betecknas $d(x)$, $d(x) = |N(x)|$

Grafisomorfi

Informellt: "När de kan ritas likadant så när som på hörnens namn."

Formellt: $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ två grafer, en funktion $f: V_1 \rightarrow V_2$ är en **grafisomorfi**.

a.) f är en bijektion

b.) $\forall x, y \in V_1$ gäller $\{x, y\} \in E_1 \Leftrightarrow \{f(x), f(y)\} \in E_2$

G_1 och G_2 sägs då vara **isomorfa**

Omformulering: Två grafer är isomorfa om man kan permutera ordningen på raderna (och kolumnerna) så att grannmatriserna blir identiska.

Några speciella grafer

$K_n = (V, E)$ där $|V| = n$ och $E = \{xy \mid \forall x, y \in V, x \neq y\}$ kallas den **kompleta grafen** på n noder. Kallas även **klick**.

C_n , **Cykelgrafen**, är grafen på $n \geq 3$ noder $\{1, 2, \dots, n\}$ och med kanter $\{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}, \{n, 1\}\}$

$K_{n,m} = (V, E)$ där $V = \{x_1, \dots, x_n, y_1, \dots, y_m\}$ och $E = \{x_i y_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ kallas den **kompleta bipartita grafen** på n och m noder.

Reguljära grafer

En graf kallas **reguljär** om alla noder har samma valens.

Cykeln C_n är reguljär med valens 2, Kompletta grafen K_n är reguljär med valens $n-1$.

Handskakningslemmat

Sats Satsen om Valensernas Summa: För varje graf $G = (V, E)$ gäller

$$\sum_{x \in V} S(x) = 2 \cdot |E|$$

Kombinatoriskt bevis: Räkna Summa Sak på två olika sätt

Vi säger att en nod är;

- **Udda** om den har udda valens
- **jämn** om den har jämn valens

Lemma (Handskakningslemmat): För varje graf $G=(V,E)$ gäller att antalet udda noder är jämnt.

F2

Delgrafer och Vandringer

Givet en graf $G=(V,E)$, säger vi att en annan graf $G_1=(V_1,E_1)$ är en **delgraf** till G om $V_1 \subseteq V$ och $E_1 \subseteq E$.

En **Vandring** (eller promenad "walk") i en graf $G=(V,E)$ är en sekvens av noder $v_1 v_2 \dots v_k$ där $v_i v_{i+1} \in E$ för $i=1 \dots k-1$.

Några viktiga specialfall:

- En **Väg** (trail): en vandring där alla passerade kanter är olika (noder får upprepas)
- En **stig** (path): en väg med alla v_i olika
- En **krets** (circuit): en sluten väg, dvs en väg $v_1 v_2 \dots v_{k+1}$ med $v_1 = v_{k+1}$
- En **cykel** (cycle): en krets $v_1 v_2 \dots v_{k+1}$ med $v_1 v_2 \dots v_k$ en stig $k \geq 3$
också en delgraf isomorf med cykelgrafen C_k

Sammanhängande

En graf G är **Sammanhängande** om det för varje par av noder $x, y \in V$ finns en stig från x till y .

En **komponent** i G är en maximal sammanhängande delgraf.

Antal Vandringer

Sats Antalet vandringer av längd r mellan noderna i och j i grafen G är ij -elementet i matrisen A^r , där A är grannmatrisen för G .

Eulersk

En graf är **Eulersk** om det finns en krets (sluten väg) som passerar varje kant i grafen exakt en gång. Ibland pratar man också om en **Eulerväg**, vilket är en väg som använder alla kanter en gång, men som får börja och sluta i olika noder.

Sats En sammanhängande graf G är Eulersk om och endast om varje nod har en jämn valens.

Följsats En sammanhängande graf $G=(V,E)$ har en Eulerväg om

och endast om antalet udda noder är 0 eller 2.

Hamiltonsk

En **hamiltoncykel**: en $|V|$ stig (d.v.s. en cykel genom alla grafens noder)

En **hamiltonstig** är en stig genom alla noder

Sats Varje graf $G=(V, E)$ med minst 3 noder sådana att
 $\forall x \in V, \delta(x) \geq |V|/2$ har en hamiltoncykel

Tillämpning

Optimeringsproblem:

- **Brevbärarproblemet**: bestäm kortaste vandring som täcker varje gata minst en gång
- **Handelsresande problemet (TSP)**: bestäm kortaste vandring som besöker varje nod minst en gång

F3

Träd

En graf är ett **träd** $T=(V, E)$ om den är sammanhängande och utan cykler.

Sats För ett träd $T=(V, E)$ gäller: $\forall x, y \in V$ finns det en unik stig från x till y i T .

Sats För ett träd $T=(V, E)$ gäller även: om en kant $i \in E$ tas bort, återstår två träd. (givet $|E| \geq 1$)
 $|E| = |V| - 1$ (om $|V| \geq 1$)

En **skog** $G=(V, E)$ är en graf utan cykler. Består av komponenter som är träd.

Ett träd $T=(V', E')$ är ett **(npp)spännande träd** till en graf $G=(V, E)$ om $V'=V$ och $E' \subseteq E$. D.v.s. T är träd som är en delgraf till G som omfattar samtliga noder. Varje sammanhängande graf har ett spännande träd.

Nodfärgning

En godkänd färgning av noder ska vara sådan att grannar får olika färg.

Formellt: Godkänd **nodfärgning** av grafen $G=(V, E)$ är en funktion $c: V \rightarrow \mathbb{Z}_+$ så att $xy \in E \Rightarrow c(x) \neq c(y)$

Kromatiska talet

Kromatiska talet $\chi(G)$ för G är det minsta antalet färger som G kan nodfärgas med.

En graf med $\chi(G) \leq 2$ kallas bipartit.

En girig algoritm

Låt $\Delta(G)$ betecknar **maxvalensen** för G . En girig algoritm för att approximerar $\chi(G)$ är följande.

1. Ordna hörnen: $v_1, v_2, \dots, v$

2. Välj i ordning $c(v_1), c(v_2), \dots, c(v_n)$ som minsta möjliga positiva heltal, givet de redan valda.

Sats För varje graf G gäller

a.) $\chi(G) \leq \Delta(G) + 1$

b.) om G sammanhängande och inte reguljär så $\chi(G) \leq \Delta(G)$

Kromatiska polynomet

Det **kromatiska polynomet** $\chi_G(k)$ för en graf G är antalet sätt att nödfärga grafen $G=(V,E)$ med (högst) k färger. För enkla grafer blir $\chi(G)$ en produkt, t.ex. kompletta grafen, träd.

För $G=(V,E)$, $e \in E$ definierar vi grafen $G-e$ som grafen G med kanten e borttagen, $G|e$ som grafen G med kanten e kontraherad.

Sats För varje graf $G=(V,E)$, $e \in E$ gäller: $\chi_G(k) = \chi_{G-e}(k) - \chi_{G|e}(k)$.

Med rekursion kan man visa följande om det kromatiska polynomet:

1. $\chi(G)$ är ett polynom
2. Dess högsta gradsterm är $k^{|V|}$. Nästhögsta gradsterm är $-|E|k^{|V|-1}$
3. Koefficienterna är heltal och alternerande ≥ 0 och ≤ 0
4. Konstanttermen är 0 (om $|V| > 0$)

Kromatiska talet $\chi(G)$ är det minsta $k=0,1,2,\dots$, med $\chi(G) \neq 0$

F4.

Bipartita grafer

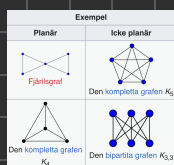
Grafer $G=(V,E)$ med $\chi(G) \leq 2$ kallas en **bipartit**. Man kan då dela upp nodmängderna i de två färgklasserna $V=X \cup Y$, där $X \cap Y = \emptyset$. Alltså gäller att alla kanter går mellan en nod i X och en nod i Y .

Planära grafer

En **plan graf** är en "konkret graf" i ett plan, där noderna är olika punkter i planet och kanterna är kurvor som förbinder sina noder, utan att olika kanter har andra punkter än sina noder gemensamt.

Definition: En graf $G=(V,E)$ är **planär** om den är isomorf med en plan graf.

En graf kan ritas utan korsande kanter på en sfär precis om den kan det i ett plan.



Kanterna (och noderna) i en plan graf delar in planet i sammanhängande **regioner** ("delar" = "områden" = "fasetter")

För en plan graf betecknar vi antalet noder med n , antalet kanter med k , antalet regioner för r och antalet komponenter för c .

Sats För varje plan graf gäller $n - k + r - c = 1$

Om grafen är sammanhängande gäller Eulers polyederformel:

$$n - k + r = 2$$

Följder av polyederformeln

Följd är att r är samma för alla inbäddningar av en planär graf.

Följsats 1:

För en planär graf med n noder, k kanter och c komponenter gäller om $k \geq 2$: $3n \geq k + 3(c+1)$

Om grafen är sammanhängande ($c=1$) gäller: $3n \geq k+6$

Följsats 2: G planär, bipartit, och $k \geq 2$: $2n \geq k(c+1)$

Om G också är sammanhängande gäller: $2n \geq k+4$

Följsats 3: $G=(V, E)$ planär och $e \geq 2$ då gäller $\frac{1}{n} \sum_{x \in V} \delta(x) < 6$

Karakterisering av planära grafer

Om en graf är icke-planär "innehåller" den alltid (minst) en av K_5 och $K_{3,3}$:

Wagners Sats: Grafen G är icke-planär om en graf som är isomorf med K_5 eller $K_{3,3}$ kan fås från G med en följd (o eller flera) av operationerna:

- ta bort en nod (och dess kanter)
- ta bort en kant
- kontrahera en kant ("dra ihop" noderna vid kanten till en ny nod.)

En graf som fås med dessa operationer kallas en **minor**.

Fyrfärgssatsen

Sats G planär $\Rightarrow \chi(G) \leq 4$

Duala grafen

Givet en plan graf G kan vi finna dess **duala graf** $G^\perp$ så:

- lägg en $G^\perp$ -nod i varje G -region
- för varje G -kant, drag en $G^\perp$ -kant mellan $G^\perp$ -noderna i G -regionerna vid den

$G^\perp$ är alltid en plan graf, men den är inte säkert enkel (kan ha öglor och multipla kanter). G behöver ej heller vara enkel.

För varje plan graf G är $G^\perp$ sammanhängande.

Sats För varje plan graf G gäller: G är sammanhängande $(\Leftrightarrow) G \cong (G^\perp)^\perp$

Regelbundna polyedrar

En regelbunden polyeder är en konvex polyeder med alla sidor regelbundna b -hörningar och alla hörn kongruenta, all grad a . Vi ska nu visa att det finns exakt fem stycken: tetraedern, kuben, oktaedern, dodekaedern och ikosaedern (kallas **platonska kropparna**).

Plan grafen för en regelbunden polyeder är dubbelt reguljär.

$$n - k + r = 2, \quad 2k = an = br$$

Detta ger $2 = \frac{2k}{a} - k + \frac{2k}{b} = (2a - ab + 2b) \frac{k}{ab}$ och därför måste $2a - ab + 2b > 0$, vilket är samma som $(a-2)(b-2) < 4$, $2k = an = br$. Eftersom $a, b \geq 3$ blir de enda möjligheterna.

FS.

Bipartita grafer

En bipartit graf $G = (X \cup Y, E)$: $X \cap Y = \emptyset$, alla kanter mellan X och $Y \Leftrightarrow \Leftrightarrow G$ är 2-(nod) färgbar

Sats G bipartit $\Rightarrow \sum_{x \in X} \delta(x) = \sum_{y \in Y} \delta(y) = |E|$

Sats G bipartit $\Leftrightarrow$ det finns ingen udda cykel i G .

Kantfärgningar

En kantfärgning av grafen $G = (V, E)$:

- en funktion $f: E \rightarrow \mathbb{Z}_+$
- Så att $|e_1 \cap e_2| = 1 \Rightarrow f(e_1) \neq f(e_2)$
- d.v.s. kanter till samma nod har olika färg

Kromatiskt index $\chi'(G)$ för G :

- minsta antalet färger som G kan kantfärgas med

Lemma $G = (V, E)$ graf, $\chi'(G) \geq \Delta(G)$

Sats För bipartit graf $G = (X \cup Y, E)$ gäller $\chi'(G) = \Delta(G)$

Sats För alla grafer G gäller $\Delta(G) \leq \chi(G) \leq \Delta(G) + 1$

Latinsk kvadrat

En **latinsk kvadrat** är en $n \times n$ -matris där talen $1, \dots, n$ finns exakt en gång i varje rad och i varje kolumn.

Finns möjlig bijektion mellan $n \times n$ -latinska kvadrater och kantfärgningar av $K_{n,n}$. Kanten mellan r_i, k_j färgas med siffran s som står på (i, j) .

En annan möjlig bijektion mellan $n \times n$ -latinska kvadrater och kantfärgningar av $K_{n,n}$. Kanten mellan s och k_j färgas med raden r_i som står på position (i, j) i matrisen.

Latinska rektangel

Låt $m \times n$ -latinsk rektangel vara en $m \times n$ -matris där $1, \dots, n$ förekommer exakt en gång i varje rad och högst en gång i varje kolumn.

Sats En latinsk $m \times n$ -rektangel ($m < n$) kan utvidgas till en latinsk $n \times n$ -kvadrant.

F6.

Matchningar

En **matchning** M för grafen $G=(V,E)$: $M \subseteq E$, kanterna i M parvis disjunkta.
Noder som tillhör någon kant i M kallas **mättade** annars **omättade**.

Om $G=(X \cup Y, E)$ bipartit säger vi att en matchning M är **komplett** (av X)
om varje nod i X är mättad av M .

Största matchning M : Så många av G 's noder som möjligt ingår,
d.v.s. att $|M|$ är maximal.

En M -alternerande stig har varannan kant i M och varannan utanför M .

En M -utökande stig är en alternerande stig som börjar och slutar i omättad nod.

Berges lemma G bipartit graf, M största matchning i $G \Leftrightarrow \nexists M$ -utökande stig.

För $A \subseteq V$ definierar vi $N(A) = \{y \in Y \mid \{x, y\} \in E \text{ för något } x \in A\}$.

Halls Sats För bipartit graf $G=(X \cup Y, E)$ gäller:

G har en komplett matchning (av X) $\Leftrightarrow |N(A)| \geq |A|$, alla $A \subseteq X$

Största matchning

Berges lemma kan användas för en algoritm att hitta en största matchning i en graf G .

1. Börja med matchning M .

2. Sök efter M -utökande stig S med bred-först-sökning.

2.1. Börja från omättad nod $x \in X$

2.2. Beträkta alla en grannar $N(x) = \{y_1, \dots, y_k\}$. Om ngn y_i är omättad så är kanten xy_i en M -utökande stig.

2.3. Om ej, lägg till noder $x_1, \dots, x_k$ matchade med $y_1, \dots, y_k$ av M .

2.4. Gör om 2.2 för alla $x_1, \dots, x_k$

:

3. Om M -utökande stig finns, konstruera större matchning M' och gör 2 igen. Annars gör 2 med annan startnod x .
4. Om M -utökande stig inte finns efter att ha kört från 2 med alla omättade noder x , då är M en största matchning enligt Berges lemma.

Defekt

Sats Om M är en största matchning i bipartit graf $G = (X \cup Y, E)$ gäller: $|M| = |X| - d(G)$, där $d(G) = \max_{A \subseteq X} (|A| - |N(A)|)$, grafens defekt/underskott.

Transversaler

Om $\mathcal{X} = \{S_i\}_{i=1}^k$ är en uppsättning mängder, kallas en mängd $\{a_i\}_{i=1}^k$ med $a_i \in S_i$ för alla i och $a_i \neq a_j$ om $i \neq j$ för en transversal (eller ett system av skilda representanter) för $\mathcal{X}$.

Sats $\mathcal{X} = \{S_i\}_{i=1}^k$ har en transversal om och endast om $\left| \bigcup_{i \in T} S_i \right| \geq |T|$ för alla $T \subseteq \{1, 2, \dots, k\}$.

F7

Permutationer

Bijektion $\pi: X \rightarrow X$

T.ex. $X = \{1, 2, \dots, n\}$ för något $n \in \mathbb{Z}^+$.

Kan skrivas som funktion, $\pi(1) = 4$, $\pi(2) = 5$, $\pi(3) = 2$, $\pi(4) = 1$
 $\pi(5) = 3$, $\pi(6) = 6$

Tvåradarsnotation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{bmatrix}$

Enradarsnotation 452136

Cykelnotation (14)(253)(6)

Går även att skriva som riktad graf

Mängden av alla permutationer av $\{1, 2, \dots, n\}$ skrivs S_n .

Antal permutationer är $|S_n| = n!$

Sats om permutationer

Om $\pi, \sigma, \tau \in S_n$:

1. $\pi\sigma \in S_n$

2. $\pi(\sigma\tau) = (\pi\sigma)\tau$

3. Det finns $\text{id} \in S_n$ så att $\pi \text{id} = \text{id} \pi = \pi$ för alla π

4. Det finns $\pi^{-1} \in S_n$ så att $\pi\pi^{-1} = \pi^{-1}\pi = \text{id}$

Ordningen av en permutation π är det lägsta $k \geq 1$ s.t.
 $\pi^k = \text{id}$. Skrivs som $o(\pi) = k$

Lemmer Ordningen för en permutation $\pi \in S_n$ är minsta gemensamma multipliken av cykel längderna i π .

Permutationsmatriser

Permutationen $\pi \in S_n$ kan beskrivas med **permutationsmatriser**:

M_π , en $(n \times n)$ -matris med element $m_{ij} = \begin{cases} 1, & \text{om } \pi(j) = i \\ 0, & \text{annars} \end{cases}$

$M_{\pi\sigma} = M_{\pi\sigma}$, d.v.s. sammansättningen i S_n motsvaras precis av matrismultiplikation.

Partitioner av heltal

En **partition** av $n \in \mathbb{N}$:

$$n = n_1 + n_2 + \dots + n_k, \quad n_1 \geq n_2 \geq \dots \geq n_k \geq 1$$

Antalet partitioner av n i precis k delar: $p_k(n)$ och totala antalet partitioner av n : $p(n)$

Permutationers Cykeltyp

En permutations **cykeltyp** är partitionen som ges av **cykellängderna**

Ex. $\pi = (1 \ 2 \ 7)(3 \ 5)(4 \ 11 \ 8 \ 6)(9 \ 10)$ ger cykeltyp $[2^2 \ 3 \ 4]$

Sats Antalet permutationer av typ $[1^{c_1} 2^{c_2} \dots k^{c_k}]$:

$$\frac{n!}{1^{c_1} 2^{c_2} \dots k^{c_k} c_1! \dots c_k!}$$

Konjugerade permutationer

Två permutationer $\alpha, \beta \in S_n$ är konjugerade om det finns en permutation $\sigma \in S_n$ sådan att $\beta = \sigma \alpha \sigma^{-1}$.

Detta definierar en ekvivalensrelation på S_n .

Sats $\alpha, \beta \in S_n$ är konjugerade om och endast om de har samma cykeltyp.

Konsekvens 1: Ekvivalensklasser av konjugerade permutationer motsvarar bijektivt partitioner av n .
 $[1^{c_1} 2^{c_2} \dots k^{c_k}]$, där $n = 1 \cdot c_1 + 2 \cdot c_2 + \dots + k \cdot c_k$

Konsekvens 2: $\pi \in S$ och $\sigma \pi$ har samma cykelstruktur

Udda/jämna permutationer

En transposition är en permutation av typ $[1^{n-2} 2]$,
 d.v.s. $\tau = (a b) \in S_n$, $a \neq b$

Om π är av typ $[1^{c_1} 2^{c_2} \dots k^{c_k}]$ är $c(\pi) = c_1 + c_2 + \dots + c_k$,
 antalet cykler i π .

För alla $\pi \in S_n$: $\pi = \tau_r \dots \tau_2 \tau_1$ för något r och några transpositioner $\tau_1, \tau_2, \dots, \tau_r$

Sats Om π skrivs som sammansättningen av transpositioner på två olika sätt $\pi = \tau_r \dots \tau_2 \tau_1 = \tau'_r \dots \tau'_2 \tau'_1$ har r och r' samma paritet.

Def. π är en jämn (udda) permutation om och endast om r är jämnt (udda).

Tecknet (signum) för π , $\text{sgn } \pi = (-1)^r = \begin{cases} +1 & \pi \text{ jämn} \\ -1 & \pi \text{ udda} \end{cases}$

Uppgifter följande:

$$\text{sgn}(\pi\sigma) = \text{sgn } \pi \cdot \text{sgn } \sigma$$

$$\text{sgn } \pi^{-1} = \text{sgn } \pi$$

$$\text{sgn}(\sigma\alpha\sigma^{-1}) = \text{sgn } \alpha$$

För en cykel av längd j gäller:

$$(x_1 x_2 \dots x_j) = (x_1 x_j)(x_1 x_{j-1}) \dots (x_1 x_3)(x_1 x_2)$$

$$\text{sgn}(x_1 x_2 \dots x_j) = (-1)^{j-1}$$

Konsekvens: En cykel är en jämn permutation om och endast om den har en udda längd.

Samma tecken i hela konjugatklassen. Om π är av typ $[1^{c_1} 2^{c_2} \dots k^{c_k}]$ är:

$$\text{sgn } \pi = (-1)^{n - c(\pi)} = (-1)^{c_2 + c_4 + \dots}$$

En jämn permutation är en med ett jämnt antal cykler av jämn längd.

Sats 1 S_n ($n \geq 2$) är hälften av permutationerna jämna, hälften udda.

Vidare gäller: Om A är $n \times n$ -matris är

$$\det A = \sum_{\pi \in S_n} \text{sgn } \pi \cdot a_{\pi(1)1} a_{\pi(2)2} \dots a_{\pi(n)n}$$

$$\Rightarrow \text{sgn } \pi = \det M_\pi$$

Grupper

En **grupp** G ($G, *$) är en mängd G tillsammans med en binär operation $*$ som uppfyller:

G1 (Sluten) För alla $x, y \in G$ gäller att $x * y \in G$

G2 (Associativ) För alla $x, y, z \in G$ gäller $(x * y) * z = x * (y * z)$

G3 (Identitet) Det finns $e \in G$ så att $e * x = x * e = x$, e kallas **identiteten** (även enhetselementet)

G4 (Invers) För alla $x \in G$ finns $x' \in G$ så att $x' * x = x * x' = e$, x' kallas **inversen** till x .

Om det gäller att $x * y = y * x$ för alla $x, y \in G$ kallas gruppen för **abelsk/kommutativ**

Förkortad notation:

$$x * y = xy$$

$$e = 1$$

$$x' = x^{-1}$$

Satser om grupper

Sats G grupp, $x, y, z \in G$

i. $xy = xz \Rightarrow y = z$

ii. $yx = zx \Rightarrow y = z$

Sats G grupp, $a, b \in G$, då har ekv. $ax = b$ unik lösning i G .

Sats G är en grupp

i. $\forall a \in G, ax = a$ har unik lösning, $\Rightarrow$ identiteten 1 är unik

ii. $\forall a \in G, ax = 1$ har unik lösning $\Rightarrow$ inversen a^{-1} är unik

iii. Gruppoperation är en latinsk kvadrat, om G ändlig grupp

Grupper, ordning

Notationser av grupper med rekursion.

$$\begin{aligned}x^1 &:= x & x^r &:= x x^{r-1}, r \geq 2 \\ x^{-1} &:= x^{-1} & x^{-s} &:= x^{-1} x^{1-s}, s \geq 2 \\ x^0 &:= 1\end{aligned}$$

$$\text{Räknelagar } x^m x^n = x^{m+n}, (x^m)^n = x^{mn}$$

Ordningen för ett element $g \in G$ skrivs $o(g)$ och def.

$$o(g) = \begin{cases} \text{om } g^n = 1, \text{ något } n > 0: \text{minsta sådant } n \\ \text{annars: } \infty \end{cases}$$

Sats om $o(g) = m$ så gäller $g^s = 1 \Leftrightarrow m | s$

Gruppisomorfier

$(G_1, *)$, $(G_2, \circ)$ två grupper och $\beta: G_1 \rightarrow G_2$ är en bijektion.

β är en **isomorfier** om $\forall g, g' \in G_1$

Då är G_1 o G_2 **isomorfa** och skriver $(G_1, *) \approx (G_2, \circ)$ eller $G_1 \approx G_2$

Isomorfier är en ekvivalensrelation på mängden av grupper.

Cykliska grupper

En grupp är **cyklisk** om för något $x \in G$ varje $g \in G$ är x^n för något $n \in \mathbb{Z}$.

x **genererar** G , $G = \langle x \rangle$

$$o(x) = m : C_m = \{1, x, x^2, \dots, x^{m-1}\} \cong (\mathbb{Z}_m, +)$$

$$o(x) = \infty : C_\infty = (\dots, x^{-2}, x^{-1}, x, x^2, \dots) \cong (\mathbb{Z}, +)$$

Direkta produkter av grupper

Om A, B är grupper, är $(A \times B, *)$ med $(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2)$ också en grupp och kallas den **direkta produkten** av A och B .

Sats Om m och n är relativt prima så är $C_{mn} \cong C_m \times C_n$

G_1 och G_2 abelska $\Rightarrow G_1 \times G_2$ abelsk

Delgrupper

H är delgrupp till $(G, *)$ om $H \subseteq G$ och $(H, *)$ är en grupp.

Sats Om G är en grupp och $H \subseteq G$ gäller att

$$H \text{ är en delgrupp till } G \Leftrightarrow \begin{cases} \text{S0} & H \neq \emptyset \\ \text{S1} & x, y \in H \Rightarrow xy \in H \\ \text{S2} & x \in H \Rightarrow x^{-1} \in H \end{cases}$$

Om H är ändlig räcker S0 och S1.

Om G är en grupp är $Z(G) = \{z \in G \mid zg = gz \text{ för alla } g \in G\}$ en delgrupp till G och kallas för **G 's centrum**.

Varje $x \in G$ genererar en cyklisk delgrupp.

$$\langle x \rangle = \{x^i \mid i \in \mathbb{Z}\}$$

Där $\sigma(x) = |\langle x \rangle|$

Cayleygraf

En Cayleygraf för en grupp beskriver gruppen fullständigt.

Grafen har ett hörn för varje element i gruppen och om gruppen genereras av $a, b, \dots$ har den riktade kanter med olika märkningar/färgar svarande mot $a, b, \dots$.

En grupp kan ha olika, icke-isomorfa, Cayleygrafer med olika generatorer.

Sidoklasser

Om H är en delgrupp till G och $g \in G$ är

$$gH = \{gh \mid h \in H\} \text{ en vänstersidoklass till } H \text{ och}$$

$$Hg = \{hg \mid h \in H\} \text{ en högersidoklass}$$

$$|H| = |gH| = |Hg|$$

Sidoklasserna ger en partition av G i lika stora mängder.

Sats H delgrupp till G . Vänstersidoklasserna till H formar en mängdpartition av G . D.v.s. för $g_1 \neq g_2 \in G$ gäller

$$g_1H \neq g_2H \text{ eller } g_1H \cap g_2H = \emptyset$$

(Gäller även högersidoklasserna)

Lagranges Sats

Sats G ändlig grupp och H delgrupp till G . Då finns positivt heltal k så att $|G| = k \cdot |H|$

Antalet sidoklasser till H i G betecknas $|G:H| = \frac{|G|}{|H|}$, och kallas H 's **index** i G .

Sats G ändlig grupp, $g \in G$ och $|G| = n$, då gäller: i) $o(g) \mid n$ ii) $g^n = 1$

Sats G grupp och $|G| = p$ för något primtal p . Då är $G \cong C_p$

Normal delgrupp

Delgruppen N till G kallas en **normal delgrupp** om m.

Vänstersidoklasserna = högersidoklasserna, d.v.s.

$$gN = Ng \text{ för alla } g \in G$$

$\Rightarrow G/N = \{gN \mid g \in G\}$ **kvotgruppen**

Automorfier

$\Gamma = (V, E)$ en graf med $V = \{1, 2, \dots, n\}$

En bijektion $\pi: V \rightarrow V$, sådan att $xy \in E \Leftrightarrow \pi(x)\pi(y) \in E$ kallas en **automorfi**, d.v.s. en isomorfi från grafen till sig själv.

Mängden av alla automorfier $\text{Aut}(\Gamma)$ bildar en grupp med sammansättning av bijektioner som operation.

Gruppverkan

För en grupp G säg vi att G verkar på X (X är en mängd) om

$\forall g \in G, \quad g: X \rightarrow X$ är en bijektion och

$$- \forall g_1, g_2 \in G, x \in X \quad (g_1 * g_2)(x) = g_1(g_2(x))$$

$$- \forall x \in X, \quad 1_G(x) = x$$

OBS: G, X är ändlig i denna kurs

OBS: skriv ut gx istället för $g(x)$

Sats $|G| = |G_X| \cdot |G_x|$

För $g \in G$ definieras g 's fixpunktmängd som $F(g) := \{x \in X \mid g(x) = x\}$

Sats Burnsidess lemma, antalet banor, N , då G verkar på X beräknas med $N = \frac{1}{|G|} \sum_{g \in G} |F(g)|$

Banor

Om G verkar på X och $x \in X$ så kallas $G_x := \{g(x) : g \in G\}$ för **banor** (orbit) en delmängd till X . Banorna bildar en mängdoperation av X

Stabilisatorn

Stabilisatorn för $x \in X$: $G_x := \{g \in G \mid g(x) = x\}$, en delgrupp till G .

Repetition, modulär aritmetik

$x \equiv y \pmod{m}$, eller $x \equiv_m y$ innebär $m \mid (x-y)$ ocn läses
 "x är kongruent med y modulo m".

Mängden av alla heltal, $\mathbb{Z}$, delas in i m st klasser av kongruenta tal:

$$[0]_m = \{0, \pm m, \pm 2m, \dots\}$$

$$[1]_m = \{1, \pm m+1, \pm 2m+1, \dots\}$$

$$\vdots$$

$$[m-1]_m = \{-1, \pm m-1, \pm 2m-1, \dots\}$$

Dessa utgör ("heltalen modulo m"): $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$

Sats $x_1 \equiv_m x_2, y_1 \equiv_m y_2 \Rightarrow x_1 + y_1 \equiv_m x_2 + y_2, x_1 y_1 \equiv_m x_2 y_2$

Vi kan alltså definiera + och $\cdot$ på $\mathbb{Z}_m$:

$$[a]_m \circ [b]_m = [a \circ b]_m \text{ för } \circ = +, \cdot$$

Oftast skriver man $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ ocn räknar + och $\cdot$ "som vanligt men (mod m)".

$r \in \mathbb{Z}_m$ är **inverterbart** om och endast om det finns $x \in \mathbb{Z}_m$ med $rx = 1$ i $\mathbb{Z}_m$. x et kallas r^{-1} , r 's **invers**.

$\exists x = 1$ i $\mathbb{Z}_m$ om.m. $\exists x - km = 1$ för något $k \in \mathbb{Z}$, så r^{-1} kan bestämmas med Euklides algoritm.

Sats $r \in \mathbb{Z}_m$ är inverterbart om.m. $\text{sgd}(r, m) = 1$ ($\in \mathbb{Z}$)

Definier $U_m = U(\mathbb{Z}_m) = \{x \in \mathbb{Z}_m : x \text{ inverterbar}\}$

Sats $(U_m, \cdot)$ är en grupp, med multiplikation modulo m .

Linjära ekvationer i $\mathbb{Z}_m$

Linjära kongruenser är linjära ekvationer i $\mathbb{Z}_m$:

$$ax \equiv b \pmod{m} \Leftrightarrow ax = b + km \Leftrightarrow ax - km = b \text{ för något } k \in \mathbb{Z}$$

Så ekvationen är lösbar om $m \mid d = \text{Sgd}(a, m) \mid b$

Allmänt för $ax \equiv b \pmod{m}$:

- Om $d = \text{Sgd}(a, m) \mid b$, så finns d olika lösningar $\pmod{m}$, d.v.s. d olika lösningar i $\mathbb{Z}_m$.
- Ingen lösning alls om $\text{Sgd}(a, m) \nmid b$

Räkneregler:

$$ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \pmod{m} \text{ om } \text{Sgd}(a, m) = 1$$

$$ax \equiv ay \pmod{an} \Leftrightarrow x \equiv y \pmod{n}$$

$$a \nmid y \Rightarrow ax \not\equiv y \pmod{an}$$

Kinesiska restsatsen

Sats Låt $m_1, m_2, \dots, m_k$ vara positiva tal så att $\text{Sgd}(m_i, m_j) = 1$ för alla $1 \leq i < j \leq k$. Då har systemet av kongruenser (där alla $a_i \in \mathbb{Z}$)

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

en lösning, och denna är unik modulo $m = m_1 m_2 \dots m_k$

Kinesiska restsatsen, teoretisk beskrivning

Modulerna m_i är parvis relativt prima och $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$.

Vi definierar den "naturliga avbildningen"

$$f: \mathbb{Z}_m \rightarrow (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}) \quad \text{enligt} \\ [x]_m \mapsto ([x]_{m_1}, [x]_{m_2}, \dots, [x]_{m_k})$$

Kinesiska restsatsen ger inversen till denna avbildning:

$$x = f^{-1}(a_1, a_2, \dots, a_k).$$

Från definitionen av direkt produkt får vi:

$$([x]_{m_1}, \dots, [x]_{m_k}) + ([y]_{m_1}, \dots, [y]_{m_k}) = \\ = ([x]_{m_1} + [y]_{m_1}, \dots, [x]_{m_k} + [y]_{m_k}) = ([x+y]_{m_1}, \dots, [x+y]_{m_k})$$

Vilket ger gruppisomorfin $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$

Sats Om $m_1, \dots, m_k$ är parvis relativt prima gäller för cykliska grupper:

$$C_{m_1 \dots m_k} \cong C_{m_1} \times \dots \times C_{m_k}$$

Samma sak gäller för multiplikation definierad koordinatvis

$$([x]_{m_1}, \dots, [x]_{m_k}) \cdot ([y]_{m_1}, \dots, [y]_{m_k}) = \\ ([x]_{m_1} \cdot [y]_{m_1}, \dots, [x]_{m_k} \cdot [y]_{m_k}) = ([x \cdot y]_{m_1}, \dots, [x \cdot y]_{m_k})$$

Detta ger oss en isomorfi av ringar:

$$(\mathbb{Z}_{m_1}, +, \cdot) \cong (\mathbb{Z}_{m_1}, +, \cdot) \times \dots \times (\mathbb{Z}_{m_k}, +, \cdot)$$

F14.

Eulers ϕ -funktion

Eulers ϕ -funktion: $\phi(n) = |\{x \in \{1, 2, \dots, n\} \mid \text{sgcd}(x, n) = 1\}|$

Sats Om $n \geq 2$, $n = p_1^{e_1} \dots p_r^{e_r}$ ($p_1, \dots, p_r$ olika primtal, alla $e_i \geq 1$):

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

Det följer också att ϕ är **multiplikativ**, d.v.s. $\text{sgcd}(m, n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$

Sats För alla positiva heltal n gäller att $\sum_{d|n} \phi(d) = n$

Eulers och Fermats Satsar

γ är invertierbar i $\mathbb{Z}_m \Rightarrow \gamma^{\phi(m)} = 1$ i $\mathbb{Z}_m$, d.v.s. uttryckt i $\mathbb{Z}$
(**Eulers sats**): $\text{sgcd}(\gamma, m) = 1 \Rightarrow \gamma^{\phi(m)} \equiv_m 1$

Speciellt om p primtal: $\gamma \neq 0 \Rightarrow \gamma^{p-1} = 1$ i $\mathbb{Z}_p$, d.v.s. i $\mathbb{Z}$
(**Fermats lilla Sats**): $p \nmid \gamma \Rightarrow \gamma^{p-1} \equiv_p 1$

Så $\gamma^p = \gamma$, alla $\gamma \in \mathbb{Z}_p$ och $\gamma^p \equiv_p \gamma$, alla $\gamma \in \mathbb{Z}$

Möbiusfunktioner

Möbiusfunktioner

$$\mu(d) = \begin{cases} 1 & d = 1 \\ 0 & k^2 \mid d, \text{ något } k \geq 2 \\ (-1)^r & d = p_1 p_2 \dots p_r, \text{ olika primtal} \end{cases}$$

Sats $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$

Sats $\sum_{d|n} \mu(d) = \delta(n) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$

Möbius inversionsformel

$f, g: \mathbb{Z}_+ \rightarrow \mathbb{C}$ (aritmetiska funktioner)

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Cykliska grupper

Sats Om G är en grupp med $|G| = n \geq 2$, så är (i), (ii) och (iii) ekvivalenta.

$$\begin{cases} \text{(i).} & G \text{ är cyklisk} \\ \text{(ii).} & \forall d | n \Rightarrow |\{x \in G; x^d = 1\}| = d \\ \text{(iii).} & \forall d | n \Rightarrow |\{x \in G; o(x) = d\}| = \phi(d) \end{cases}$$

Följsats Alla delgrupper till C_n är cykliska.

Det finns precis en grupp av ordning d , alla $d | n$.

Om $d | d'$, $d' | n$ och C_n 's delgrupper av ordningar $< d$ är C_0, C_1 så $C_d \subseteq C_{d'}$.

F15.

Kropp

Definition: En **kropp** $(F, +, \times)$ (eng. "field") är en mängd F och två operationer $+$, $\times$ sådana att

F1) $(F, +)$ är en kommutativ grupp med 0 som identitet

F2) $(F \setminus \{0\}, \times)$ är en kommutativ grupp

F3) $\times$ är distributiv m.a.p. $+$, för alla $a, b, c \in F$

$$a \times (b + c) = a \times b + a \times c, (a + b) \times c = a \times c + b \times c$$

Notation: $\times$ -tecknet skrivs oftast inte ut, eller skrivs $\cdot$, dvs. ab eller $a \cdot b$ för $a \times b$.

$(F, +)$ kallas den **additiva gruppen** i F .

$(F \setminus \{0\}, \times)$ kallas den **multiplikativa gruppen** i F .

Ring

$(R, +, \times)$ är en ring om:

R1) $(R, +)$ är en kommutativ grupp med identitetslement 0.

R2) $(R, \times)$ är sluten och associativ med identitetslement 1.

R3) $\times$ är distributiv m.a.p. $+$, för alla $a, b, c \in R$.

$$a \times (b + c) = a \times b + a \times c, (a + b) \times c = a \times c + b \times c$$

För en ring R säger vi att $a \in R$ är **inverterbar** om det finns $a^{-1} \in R$ så att $aa^{-1} = a^{-1}a = 1$

$U(R)$ = de inverterbara elementen i R .

Sats För en ring $(R, +, \times)$ så är $(U(R), \times)$ en grupp.

Polynomring

$\mathbb{Z}[x]$ betecknar mängden av polynom med heltalskoefficienter

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad a_i \in \mathbb{Z}$$

$\mathbb{Z}[x]$ är en ring med addition och multiplikation av polynom

$$a(x) + b(x), \quad a(x)b(x)$$

Additiv identitet är 0 och multiplikativ identitet är 1.

På samma sätt kan en ring R beteckna med $R[x]$ mängden av polynom med koefficienter i R .

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad a_i \in R, \quad \forall n \geq 0$$

$a(x) + b(x), \quad a(x)b(x)$ definieras "som vanligt", räkningar sker i R .

$R[x]$ är en ring med addition och multiplikation av polynom.

$a(x)$ är grad , $\deg(x)$ är det största n med $a_n \neq 0$

(Om alla $a_n = 0$ dvs $a(x)$ är nollpolynomet, kan vi låta $\deg a(x)$ vara $-\infty$)

Om $a(x), b(x) \in R[x]$ gäller

$$\deg(a(x) + b(x)) \leq \max(\deg a(x), \deg b(x))$$

$$\deg(a(x)b(x)) \leq \deg a(x) + \deg b(x)$$

Om $a(x), b(x) \in F[x]$, polynom över en kropp F gäller

$$\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$$

$F[x]$ är också en ring.

Andra ringutvidgningar

De Gaussiska heltalen $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ där $i^2 = -1$

Ex. $\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} : a, b \in \mathbb{Z}\}$, $\mathbb{Z}[i], \mathbb{Z}[\sqrt{3}]$ är ringar, $\mathbb{Q}[\sqrt{3}]$ är en kropp.

Polynomdivision

Polynomdivision: $F[x]$, F en kropp, "vanliga algoritmen"

Sats Om $a(x), b(x) \in F[x]$, $b(x) \neq 0$ finns entydigt bestämda $q(x), r(x) \in F[x]$, $\deg r(x) < \deg b(x)$ med

$$a(x) = b(x)q(x) + r(x)$$

Största gemensamma delare

$b(x) \mid a(x)$ betyder $a(x) = b(x)h(x)$ för något $h(x) \in F[x]$

Definition: Om $a(x), b(x) \in F[x]$ och

- i) $d(x) \mid a(x)$, $d(x) \mid b(x)$
- ii) $c(x) \mid a(x)$, $c(x) \mid b(x) \Rightarrow c(x) \mid d(x)$ Så kallas $d(x)$ en största gemensam delare. Om dessutom
- iii) $d(x)$ är moniskt, dvs högsta gradskoefficienten är 1 kallas $d(x)$ den (moniska) största gemensamma delaren till $a(x)$ och $b(x)$

$\forall$ skriver $d(x) = \text{sgd}(a(x), b(x))$

Euclides algoritm

Sats För $a(x), b(x) \in F[x]$, (F en kropp) existerar $d = \text{sgd}(a(x), b(x))$ entydigt och $d(x) = \lambda(x)a(x) + \mu(x)b(x)$ för några $\lambda(x), \mu(x) \in F[x]$

Irreducibla polynom

$U(F[x]) \cong F \setminus \{0\}$ (konstanta polynom)

Om F är en kropp och $f(x) \in F[x]$ säger $\forall$ att $f(x)$ är **irreducibelt** om

$f(x) = g(x)h(x) \Rightarrow$ precis en av $g(x)$ och $h(x)$ tillhör $U(F[x])$

Om $f(x) = g(x)h(x)$,

$g(x), h(x) \in F[x]$ oln $\deg g(x), \deg h(x) \geq 1$. Då kallas $f(x)$ **reducibelt**.

Faktorisering

Sats F en kropp. Om $r(x) \in F[x]$ är irreducibelt oln $r(x) \mid s_1(x) \dots s_k(x)$ så $r(x) \mid s_i(x)$ för något i $1 \leq i \leq k$

Sats F en kropp. Om $f(x) = g_1(x) \dots g_r(x) = h_1(x) \dots h_s(x) \in F[x]$, med $g_i(x), h_j(x)$ irreducibla, så är $r=s$ oln $g_i(x) = u_i h_{\pi(i)}(x) \forall i$, för $u_i \in F \setminus \{0\}$, $\pi \in S_r$

Sats Faktorsatsen: F en kropp, $f(x) \in F[x]$, $\alpha \in F$
 $(x - \alpha) \mid f(x) \Leftrightarrow f(\alpha) = 0 \in F$

Sats F en kropp, $f(x) \in F[x]$, $\deg(f(x)) = n \geq 1$. Då har ekvationen $f(x) = 0$ högst n rötter i F .

F17.

Ändliga grupper

Om F är en ändlig kropp är F 's karakteristisk $0_+(1)$ (ordningen för mult. id. under addition)

Sats Karakteristiken är ett primtal p .

Då gäller för varje $a \in F$, $n \in \mathbb{Z}$ att $na = a + \dots + a = 0$ om m. $a=0$ eller $p|n$, så xa är definierad för alla $x \in \mathbb{Z}_p$. För $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ säger vi att karakteristiken är 0.

Ändliga kroppar, additiv grupp

Sats F en ändlig kropp med karakteristisk p . Då är den additiva gruppen $(F, +) \cong \mathbb{C}_p \times \dots \times \mathbb{C}_p = (\mathbb{C}_p)^r$ för något $r \geq 1$. Speciellt är $|F| = p^r$

Ändliga grupper, konstruktion

$F[x]/(k(x))$ med relation $a(x) \sim b(x)$ ger ringstruktur på ekvivalensklasser.

Sats För p primtal och $k(x)$ irreducibelt polynom i $\mathbb{Z}_p[x]$, $\deg(k(x)) = r \geq 1$. Då är $\mathbb{Z}_p[x]/(k(x))$ en kropp med p^r element.

F18.

Ändliga grupper, multiplikativa gruppen

Sats Den multiplikativa gruppen för en ändlig kropp är cyklisk.
D.v.s. för $|F| = p^r$ så är $(F \setminus \{0\}, \cdot) \cong C_{p^r-1}$

Ändliga kroppar, Megasatsen

Megasatsen: För varje ändlig kropp F med karakteristiken p gäller:

$$|F| = p^r$$

$$(F, +) \cong (C_p)^r$$

$$(F \setminus \{0\}, \cdot) \cong C_{p^r-1}$$

Något $r \geq 1$

r -dimensionellt vektorrum över $\mathbb{Z}_p$.

Multiplikativa gruppen är cyklisk

För varje $r \geq 1$ och primtal p finns precis en kropp F med $|F| = p^r$

Primitiva polynom och element

Ett element $f \in F$ kallas **primitivt element** i F om det genererar hela den multiplikativa gruppen, d.v.s. $(F \setminus \{0\}, \cdot) = \langle f \rangle$

$k(x) \in F[x]$ är ett **primitivt irreducibelt polynom** om (x) är ett primitivt element i $F[x]/(k(x))$

Mer om kroppar

Vi har sett: $k(x)$ är irreducibelt i $\mathbb{Z}_p[x]$ av grad r , då är $\mathbb{Z}_p[x]/(k(x))$ en kropp med p^r element.

Om vi definierar α som ett element som uppfyller $k(\alpha) = 0$.

Då kan vi se $\mathbb{Z}_p[x]/(k(x))$ som $\mathbb{Z}_p[\alpha] = \{a_{r-1}\alpha^{r-1} + \dots + a_1\alpha + a_0 : a_i \in \mathbb{Z}_p\}$

då α^r kan reduceras med $k(\alpha) = 0$. Detta är samma idé som $\mathbb{C} = \mathbb{R}[i]$, där $i^2 = -1$. Kan också skrivas $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

Felrättande koder, introduktion

Naiv felrättande kod: $0 \rightarrow 000, 1 \rightarrow 111$

Vi kan då korrigera ett fel i en 3-tupplet, men meddelandet blir 3 gånger så långt.

Mått: Bättre in budskapet på smartare sätt så att vi kan korrigera utan att tredubbla längden.

Bokstäverna i orden vi skickar tas från en kropp V , då kommer orden vara i ett vektorrum V^n över en kropp, vilket också är en grupp som är en direkt produkt av den additiva gruppen i kroppen.

Vi kommer nästan bara prata om $V = \mathbb{Z}_2$.

OBS: Diskuterar endast att en bokstav ändras, ej att tecken försvinner och hela meddelandet blir kortare.

Felrättande koder

En (binär) kod C är en mängd n -tupler av 0:or och 1:or, d.v.s. $C \subseteq V^n$, ($V = \mathbb{Z}_2 = \{0, 1\}$)

För två kodord $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in (\mathbb{Z}_2)^n$ så är avståndet (Hammingavståndet)

$$d(\mathbf{x}, \mathbf{y}) := \# \{i : x_i \neq y_i\}$$

d.v.s antal positioner de skiljer sig åt.

d är en metrik (som är ett annat namn på avståndsfunktion), d.v.s den uppfyller:

Minimala avståndet för koden C :

$$\delta := \min\{\delta(x, y) \mid x, y \in C, x \neq y\}$$

C kan upptäcka upp till $\delta - 1$ fel

Sats En kod C kan rätta e fel (till närmaste kodord) om $\delta(C) \geq 2e + 1$

Sfärpackningssatsen

Sats Om koden C , av längd n , rättar upp till e fel, så gäller

$$|C| \left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{e} \right) \leq 2^n (= |V^n|)$$

Linjära koder

C är en linjär kod om $x, y \in C \Rightarrow x + y \in C$

Obs. C är en delgrupp till V^n (t.o.m. delrum till vektorrummet V^n)

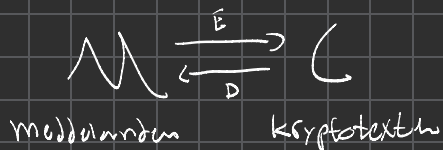
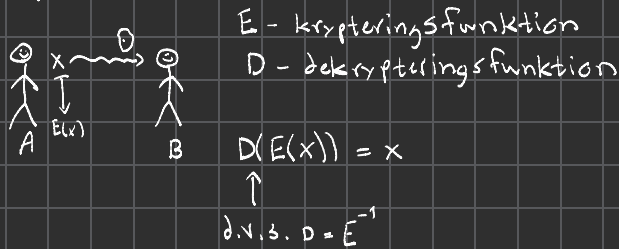
LaGranges sats $\Rightarrow |C| \mid 2^n$, dvs $|C| = 2^k$, något $k \in \mathbb{Z}_+$,
 k kallas dimensionen för koden C .

För en linjär kod är minimala avståndet δ lätt att räkna ut. Sätt
Vikten för C till $w(C) :=$ antal ettor i C och minimala (nollskilda)
Vikten $w_{\min} := \min\{w(C) \mid C \in C, C \neq 0\}$

Sats För en linjär kod C gäller $\delta(C) = w_{\min}(C)$

Sats Om H:s alla kolumner är olika och $\neq \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$, så rättar C (minst) ett fel.

- Kryptering



Exempel: Ceasar skiffer

S	V	A	N	T	E	Ä	R	B	Ä	S	T	← meddelande
T	x	B			ö							
U	Y	C			A							
V	Z	D			B							← kryptotext

$$E(x) = x + 3 \pmod{29}$$

$$D(x) = x - 3 \pmod{29}$$

Substitutionskrypto

när varje bokstav byts mot en annan

Enkelt att knäcka med statistik

Vigenerkrypto

Exempel: Nyckel (2, 1, 4)

KLARTEXTEN HÄR

$$+ 214214214$$

M	M	E
---	---	---

Blankett skiffer

Nyckeln är lika lång som texten

Ett problem är att kunskap om E ger kunskap om D.

Kryptering med öppna nycklar

A skaffar sig funktioner E_A och D_A sådana att

$$D_A(E_A(x)) = x \text{ och } E_A(D_A(x)) = x$$

A berättar E_A offentligt, håller D_A hemlig.

När B vill skicka x till A, så skickar han $E_A(x)$.

Om inversen D_A är svår att räkna ut är det bara A som kan se $D_A(E_A(x)) = x$.

Många fördelar

B kan skicka hemligheter till A utan att de träffas först.

nycklar som behövs är mycket färre

n personer behövs n öppna kryptofunktioner, men $\binom{n}{2}$ klassiska krypton.

RSA-krypto

A bestämmer två stora primtal p, q

$$\text{Låt } n = p \cdot q, \quad m = (p-1)(q-1) (= \phi(n))$$

A väljer också kryptonyckel e , $1 < e < m$, $\text{sgcd}(m, e) = 1$

A bestämmer enkrypteringsnyckel d , s.a. $ed \equiv 1 \pmod{m}$
(m.h.a. Euklides algoritmen)

A offentliggör n och e men hemlighåller d . (m, p, q glöms bort, alltså hemliga)

Nu är $E_A(x) \equiv x^e \pmod{n}$ och $D_A(x) \equiv x^d \pmod{n}$

Sats $D_A(E_A(x)) = x$ och $E_A(D_A(x)) = x$

Beweis: Både sätterna vill $x^{ed} \equiv x \pmod{n}$

Eulers sats ger $x^{\phi(n)} \equiv 1 \pmod{n}$

$ed \equiv_m 1 \Rightarrow ed = k \cdot m + 1$ något $k \in \mathbb{Z}$.

D.v.s. $x^{ed} = x^{k \cdot m + 1} = (x^{\phi(n)})^k \cdot x = 1^k \cdot x \equiv_n x$

Exempel: A har valt $p=5, q=11$

$$n = 5 \cdot 11 = 55$$

$$m = \phi(n) = \phi(55) = (5-1)(11-1) = 40$$

A väljer $e=3$ så att $\text{sgd}(40, 3) = 1$

Euklides

Euklides baklänges

$$40 = 13 \cdot 3 + 1$$

$$1 = 40 - 13 \cdot 3$$

$$d \equiv -13 \equiv 27 \pmod{40}$$

a.) Kryptera 4 och skicka till A

b.) Avkryptera 7



$$a.) E_A(4) = 4^3 = 64 \equiv 9 \pmod{55}$$

Släckar 9 till A.

$$b.) D_A(7) = 7^{27} \pmod{55}$$

Kan räknas ut med upprepad kvadrering.

$$7^2 = 49, \quad 7^4 = (7^2)^2 \equiv (-6)^2 = 36 \pmod{55}$$

$$7^8 = (7^4)^2 \equiv 36^2 \equiv (-19)^2 = 361 \equiv 31 \pmod{55}$$

$$7^{16} = (7^8)^2 \equiv (31)^2 = 961 \equiv_{55} 411 \equiv_{55} 81 \equiv 26 \pmod{55}$$

$$\text{Då } 27 = 16 + 8 + 2 + 1$$

$$\text{Så } 7^{27} = 7^{16+8+2+1} = 7^{16} 7^8 7^2 7^1 \equiv_{55} 26 \cdot 31 \cdot 49 \cdot 7 \equiv \dots \equiv 28 \pmod{55}$$

$$\text{Svar: } D_A(7) = 28$$

Funktor om

- Svårt att primtalsfaktorisera stora tal
- Enkelt att hitta stora primtal
- Beräkningar kan göras effektivt.

$(x^e \pmod{n})$ m.h.a. upprepad kvadrering

Frågor

Vad är d i ett RSA-system med $n=143$, $e=43$

A. 11 B. 23 C. 59



$$143 = 11 \cdot 13$$

$$m = 10 \cdot 12 = 120$$

$$11 \cdot 47 \equiv 517 \pmod{120} \equiv 37 \pmod{120}$$

$$23 \cdot 47 \equiv 1081 = 9 \cdot 120 + 1 \equiv 1 \pmod{120}$$

Elektronisk signatur

Om B vill skicka x till A och berisa att det kommer från honom. Då kan B skicka $D_B(x)$

Nu kan alla (även A), använda E_B och beräkna $E_B(D_B(x)) = x$

Om B vill skicka x till A både kryptat och med signatur, d. kan B skicka

$$y = D_B(E_A(x)) \rightsquigarrow A$$

A kan då läsa, men ingen annan

$$D_A(E_B(y)) = D_A E_B D_B E_A(x) = D_A E_A(x) = x$$

Primtalstest Är N ett primtal

Nårit kollar $p|N \quad \forall$ primtal $p \leq \sqrt{n}$

Finns "effektivt" test som $O((\log N)^6)$ från 2002

Probabilistiskt test

Fermat test med bas b , $1 < b < N$

$$\text{Är } b^{N-1} \equiv 1 \pmod{N}$$



Är svaret nej: $\Rightarrow$ då är N inte ett primtal

Är svaret ja: $\Rightarrow N$ är kanske ett primtal

Idé: Vi testar för många olika baser b . För N alltid 'ja'. Så är N primtal med hög sannolikhet

Tyvärr existerar tal som ej är primtal men klarar Fermat testet $\forall b, 1 < b < N$.

Detta tal heter Carmichaeltal.

Om N klarar Fermat testet för bas b utan att vara primtal kallas N för pseudoprimtal för bas b .

Exempel: $2^{10} = 1024 \equiv_{341} 1$

$$2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{341} \quad (341 = 11 \cdot 31)$$

341 klarar Fermat testet i bas 2 men är ej primtal

Så $b=3$ visar att 341 ej primtal

Minsta Carmichaeltalet är 561

Bättre primtalstest är Miller-Rabins test

$N-1 = w \cdot 2^r$ där w är ett udda tal

$$\begin{aligned} \text{test med bas } b \text{ beräknas} \quad & b^4 \equiv \quad \quad \quad (\text{mod } N) \\ & b^{2^2} \equiv -1 \text{?} \\ & \vdots \\ & b^{2^{r-1}} \equiv -1 \text{?} \\ & b^{2^r} \equiv 1 \text{?} \quad (\text{mod } N) \end{aligned}$$

Om N är ett primtal så är antingen 1 eller något
är -1 .

Fråga: Är $b^N \equiv 1$ sant om N primtal

eller

$$(b^N)^{2^i} \equiv -1 \text{ ngt } i$$

Nej $\rightarrow N$ inte primtal

Ja $\rightarrow N$ kanske primtal

N primtal med sannolikhet $\geq \frac{3}{4}$

Testa k gånger om sannolikhet N är primtal $\geq 1 - \left(\frac{1}{4}\right)^k$