ÖVNING 10 - DISKRET MATEMATIK

ERIC AHLQVIST

1. Felrättande koder

Biggs 24.1.1. Hitta minsta avståndet mellan två ord i följande koder

(a) $\{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$
(b) $\{10000, 01010, 00001\}$
(c) $\{000000, 101010, 010101\}$

och bestäm i dessa tre fall antalet fel som kan detekteras och rättas till.

Lösning.

(a) $\delta = 2, e = 0$
(b) $\delta = 2, e = 0$
(c) $\delta = 3, e = 1$.

Biggs 24.1.2. Vilka av dessa koder kan utökas utan att ändra δ?

Lösning. (b) och (c) kan utökas med 01101 resp. 111111 men (a) kan ej utökas eftersom om vi har ≤ 1 st ettor så är vi på avstånd ≤ 1 från 0000 och om vi har ≥ 3 stycken ettor så är vi på avstånd ≤ 1 från 1111. Dvs antalet ettor måste vara 2, men alla sådana ord finns redan.

2. Linjära koder

En kod $C \subseteq (\mathbb{Z}/2\mathbb{Z})^n$ kallas för *linjär* om den är sluten med avseende på addition. Observera att om $a \in C$ så har vi $a + a = 0$ (där $0 := (0, \ldots, 0)$) och därför ser vi att en icke-tom kod C är linjär om och endast om C är en delgrupp av $(\mathbb{Z}/2\mathbb{Z})^n$.

Biggs 24.2.2. Tag $x \in (\mathbb{Z}/2\mathbb{Z})^n$. Vad är antalet ord vi kan få genom att ändra ≤ 2 bitar i x?

Lösning. Ändring av exakt 2 bitar ger $n(n-1)/2$ ord (välj vilka bitar som ska ändras). Ändring av exakt 1 bit ger n ord och ändring av 0 bitar ger ett ord (nämligen x). Dvs antalet sådana ord är

$$n(n-1)/2 + n + 1 = \frac{1}{2}(n^2 + n + 2)\,.$$

3. Konstruktion av linjära koder

Biggs 24.3.1. Låt

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

och definiera

$$C = \ker H = \{x \in (\mathbb{Z}/2\mathbb{Z})^7 : Hx = 0\}\,.$$

Skriv ner alla ord i C.

Lösning. Vi ser att H har rank 4 eftersom den innehåller alla standardbasvektorer som kolumnvektorer. Därför har C dimension $\dim(C) = 7-4 = 3$. Elementen i C är exakt de ord som har ett jämnt antal ettor gemensamt med var och en av raderna i H. Totalt

$$2^{\dim(C} = 2^3 = 8$$

stycken ord. Det räcker nu att hitta en bas för C och se vilka ord den genererar. Vi kan t.ex. välja

$$a = (0001011),\ b = (1111011),\ c = (0110111)$$

som bas. Då får vi

$$\begin{aligned} a + b &= (1110000) \\ a + c &= (0111100) \\ b + c &= (1001100) \\ a + b + c &= (1000111) \\ a + a &= (0000000)\,. \end{aligned}$$

Eftersom vi hittat 8 olika ord i C är vi klara.

4. Felrättning i linjära koder

Biggs 24.4.1. Låt

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

och definiera

$$C = \ker H = \{x \in (\mathbb{Z}/2\mathbb{Z})^6 : Hx = 0\}\,.$$

Om vi får ordet $x = 110110$ och endast ett fel har uppstått, vad är det tänkta ordet?

Lösning. Vi har att

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

vilket betyder att vi ska addera 1 till det index i i x sådant att kolumn i i H är

$$\mathrm{kol}_i(H) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}\,,$$

dvs index 2. Det rätta ordet är därför 100110.

5. RSA-Kryptering

Sats 5.1. *Låt p och q vara två olika primtal, låt $n = pq$ och $m = (p-1)(q-1)$. Om $x \in \mathbb{Z}/n\mathbb{Z}$ och $s \in \mathbb{N}$ uppfyller*

$$s \equiv 1 \mod m$$

så har vi att

$$x^s = x \mod n\,.$$

Konstruktion av RSA-system.

(1) Välj två primtal p och q;
(2) Sätt $n = pq$ och $m = (p-1)(q-1)$;
(3) Välj $e \in \mathbb{N}$ med sdg$(e, m) = 1$ och $d \in \mathbb{N}$ så att $ed \equiv 1 \mod m$;
(4) Definiera

$$E, D\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

genom $E(x) = x^e$ och $D(x) = x^d$;
(5) Offentliggör n och e, håll d hemlig och elda upp m.

Anmärkning 5.2. Enligt Sats 5.1 har vi att $E \circ D = D \circ E = \mathrm{id}$.

Extra Övn 10 (1). Givet ett RSA-krypto med $n = 77$,

(a) Varför kan vi inte ha $e = 45$?
(b) Givet att $e = 13$, vad är d?
(c) Kryptera $a = 3$;
(d) Dekryptera $b = 2$.

Lösning. Vi har att $n = 77 = 7 \cdot 11$ och därför $m = \phi(n) = 6 \cdot 10 = 60$.
(a) Vi har sgd$(60, 45) = 15 \neq 1$.
(b) Vi har $e = 13$ och vill hitta d så att $ed \equiv 1 \mod m$, dvs vi vill finna $d \in \mathbb{N}$ så att $1 = de + km$ för något $k \in \mathbb{Z}$. Detta gör vi med hjälp av Euklides algoritm och finner att $d = 37$.
(c) Vi vill beräkna $E(2) = 3^{13}$. Vi räknar i ringen $\mathbb{Z}/77\mathbb{Z}$ där vi har att

$$\begin{aligned} 3^{13} &= (3^4)^3 \cdot 3 \\ &= (81)^3 \cdot 3 \\ &= 4^3 \cdot 3 \\ &= 192 \\ &= 38\,. \end{aligned}$$

(d) Vi vill beräkna $D(2) = 2^{37}$. Vi räknar i ringen $\mathbb{Z}/77\mathbb{Z}$ där vi har att

$$\begin{aligned} 2^{37} &= (2^6)^6 \cdot 2 \\ &= (-13)^6 \cdot 2 \\ &= 169^3 \cdot 2 \\ &= 15^3 \cdot 2 \\ &= 225 \cdot 15 \cdot 2 \\ &= 71 \cdot 2 \cdot 15 \\ &- 12 \cdot 15 \\ &= 51\,. \end{aligned}$$

6. Primalitetstest

Sats 6.1 (Eulers Sats)**.** *Om x är inverterbar i $\mathbb{Z}/n\mathbb{Z}$ (dvs sgd(x,n)=1) så har vi*

$$x^{\phi(n)} \equiv 1 \mod n\,.$$

Korollarium 6.2 (Fermats Lilla Sats)**.** *Om p är ett primtal och p inte delar x så har vi att*

$$x^{p-1} \equiv 1 \mod p\,.$$

Extra Övn 10 (5). Beräkna $43^{139802} \mod 101$.

Lösning. Eftersom 101 är ett primtal ger Fermats Sats att $43^{100} \equiv 1 \mod 101$. Vi har att $139802 = 1398 \cdot 100 + 2$ och om vi räknar modulo 101 har vi att

$$\begin{aligned} 43^{139802} &= 43^2 \\ &= 1849 \\ &= 31\,. \end{aligned}$$

Krypto 4. Visa att om p och q är olika primtal så har vi

$$p^{q-1} + q^{p-1} \equiv 1 \mod pq\,.$$

Lösning. Vi har enligt kinesiska restsatsen en isomorfi

$$\varphi \cong \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\,.$$

Fermats lilla sats ger

$$\begin{aligned} p^{q-1} &\equiv 1 \mod q\,, \\ q^{p-1} &\equiv 1 \mod p\,. \end{aligned}$$

Vi har att

$$\begin{aligned} \varphi(p^{q-1} + q^{p-1}) &= (p^{q-1} + q^{p-1} \mod p, p^{q-1} + q^{p-1} \mod q) \\ &= (1, 1) \\ &= \varphi(1) \end{aligned}$$

och eftersom φ är en injektiv ringhomomorfi har vi att $p^{q-1} + q^{p-1} = 1$ i $\mathbb{Z}/pq\mathbb{Z}$.