VT03
LMA100: Diskret Matematik
Göteborgs universitet
SK

Repetition II
(felrättande koder, kryptering, grafteorin)

Vi fortsätter att förbereda oss för övningstenta (som skall vara den 9 april) genom att lösa följande övningar och svara på teoretiska frågorna.

1 Felrättande koder

1.1 Frågor om teori

1. Vad menar man med en binär kod? (*Med en binär kod menar man en godtycklig delmängd C till Z_2^n, där Z_2^n är mängden av alla binära vektorer av längden n, dvs.* $Z_2^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \{0, 1\}\}$.)

2. Vad är Hammingsavståndet mellan vektorerna $a = (a_1, a_2, \ldots, a_n)$ och $b = (b_1, b_2, \ldots, b_n)$? (*Det är talet* $d(a, b) =$ *antalet* i *sådana att* $a_i \neq b_i$.)

3. Vad är minimiavståndet $d(C)$ av en kod C? ($d(C)$ *är det minsta avståndet mellan två olika kodord i* C, *dvs.* $d(C) = \min d(a, b)$ *då* $a, b \in C$ *och* $a \neq b$.)

4. Vad menas med vikten $w(a)$ av en vektor $a = (a_1, a_2, \ldots, a_n)$? ($w(a) =$ *antalet* i *sådana att* $a_i \neq 0$.)

5. Vad menas med vikten $w(C)$ av en kod C? (*Med vikten av en kod* C *menar man den minsta vikten av nollskillda kodord dvs.* $w(C) = \min w(a)$ *då* $a \neq 0$.)

6. Vilken kod kallas för lihjär (gruppkod)? (*Man säger att en kod är linjär eller en gruppkod om summan av två godtyckliga kodoord är ett kodord.*)

7. När säger man att en kod C detekterar (korrigerar) t fel? (*Man säger att en kod* C *detekterar* t *fel om* $d(C) > t$. *Man säger att den korrigerar* t *fel om* $d(C) > 2t$.)

8. Vad kan man säga om en binär matris som definierar en kod vars vikt är minst 3? (*En binär matris* H *definierar en kod vars vikt är minst 3 då och endast då alla kolonner i* H *är olika och ingen av dem är nollkolonnen.*)

9. Vad menar man med felsyndrom till en linjär kod C bestående av alla lösningar till ekvationen $Hx = 0$ för någon matris H? (*Om C är en linjär kod bestående av alla lösningar till $Hx = 0$ och $\hat{a}$ är den mottagna vektorn då a har sänts så kallas vektorn $H\hat{a}$ för felsyndrom.*)

10. På vilket sätt konstruerar man en binär Hammingkod av längd $n = 2^r - 1$? (*Om kolonnerna av en matris H består av alla möjliga icke-nolla vektorer av längd r får vi en kontrollmatris för en binär Hammingkod av längd $n = 2^r - 1$. Avkodningen är enklare om man ordnar kolonnerna i ordning som svarar mot den binära representationen av de första n naturliga talen.*)

11. Hur många fel rättar/upptäcker en binär Hammingkod? (*En binär Hammingkod rättar ett fel och upptäcker två fel.*)

1.2 Övningar

Övning 1. Låt koden $C = \{(000000), (010101), (101010), (111111)\}$. Avkoda de mottagna orden:

a) 110101

b) 100100

Övning 2. Visa att den binära koden med de 4 kodorden 00000000, 11111000, 00011111, 11100111 rättar 2 fel. Om man i stället använder koden för felupptäckande, hur många fel upptäcker den koden?

Övning 3. Konstruera (dvs. ange matrisen för) Hammingkoden med 7 informationsbitar.

a) Vilket kodord får man om informationsbitarna är 1010011?

b) Avkoda de mottagna orden

i. 11111111111

ii. 10101010101

iii. 11110000010

2 Kryptering

2.1 Frågor om teori

12. Ge ett exempel på Caesarkryptering. Beskriv krypteringen och dekrypteringen med den.

Caesarkrypteringen är definierat som en funktion $E(x) = x + a$, *där* x, $a \in \mathbb{Z}_{26}$ *(dvs man adderar modulo 26). Tag t ex* $a = 3$. *Då är* $E(x) = x + 3$ *så att* $E(0) = 3$, $E(1) = 4$, $E(24) = 2, \ldots$, *dvs A krypteras till D, B till E, Y till C osv.*

För dekryptering kan man använda dekrypteringsfunktionen $D(x) = x + 23$ *därför att D är inversen till E dvs:*

$$x \longmapsto x + 3 \longmapsto (x + 23) + 3 = x.$$

Med andra ord $D(E(x)) = x$ *vilket följer ur likheten* $23 + 3 = 0$. *Till exempel dekrypteras PDW, dvs 15,3,22, till* $15 + 23 = 12$, $3 + 23 = 0$, $22 + 23 = 19$, *dvs MAT.*

13. Beskriv RSA-kryptering.

1) Välj två olika primtal p, q *och beräkna* $n = pq$.

2) Beräkna $\varphi(n) = (p - 1)(q - 1)$ *och välj* e *så att* $SGD(e, \varphi(n)) = 1$. *Beräkna även* d *så att* $ed \equiv 1 (mod\ \varphi(n))$.

3) Publicera n, e *och en "ordbok" för översättning av meddelanden till* $r \in \mathbb{Z}_n$ *(t ex* $A = 10$, $B = 11$, $\ldots$, $Z = 35$ *då* $n > 35$).

4) Den som vill sända meddelanden r *till dig krypterar med hjälp av (den kända) funktionen* $E(r) = r^e (mod\ n)$. *Du är den ende som kan dekryptera med hjälp av funktionen* $D(x) = x^d (mod\ n)$ *(d är hemligt och* $D(r^e) = r^{ed} = r (mod\ n)$*).*

14. På vilket sätt kan man använda RSA-systemet för äkthetskontroll? *Den som känner d i beskrivningen av RSA-kryptering kan signera dokument med ett par* $(r, r^d (mod\ n))$. *Den som vill kontrollera äktheten av signaturen räknar ut* $(r^d)^e = r^{de} = r (mod\ n)$ *(*e, n *är allmänt kända).*

2.2 Övningar

Se övningarna till 17 februari för att förbereda sig till tentamenskrivningen.

3 Grafteorin

3.1 Frågor om teori

15. Vad är en graf? (*En graf är ett par av mängder,* V *och* E, *där* E *består av 2-elements delmängder i* V.

16. Vad är en riktad graf? (*En riktad graf (directed graph) är ett par av mängder,* V *och* E, *där* $E \subseteq V \times V$.)

17. Definiera komplementet till en graf G. (*Komplementet till G är grafen med samma noder som G men där två noder är grannar om och endast om de inte är det i G.*)

18. Vad kallas för graden av en nod v i en graf G? Vad är en isolerade nod? (*Antalet kanter i G som går igenom v kallas för graden av v och betecknas $deg(v)$. En isolerade nod är en nod som har graden noll.*)

19. Vad är en ögla? (*Om en kants två ändpunkter är samma nod, så kallar vi kanten en ögla (loop).*)

20. Vilka kanter kallas för parallella? (*Två eller mer kanter med samma ändpunkter kallas parallella.*)

21. Vad menas med en enkel graf? (*Med en enkel graf (simple graph) menas en graf utan öglor och utan parallella kanter.*)

22. Rita den riktade grafen som svarar mot förbindelsematrisen (the adjacency matrix) A:

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

23. Ge 3 olika exempel av bipartite graf.

24. Vad är den fullständiga grafen? (*Den fullständiga grafen K_n (complete graph) med n noder är en graf där varje par av noder binds samman av precis en kant.*)

25. Vad är den fullständiga bipartite grafen? *Den fullständiga bipartite grafen $K_{m,n}$ (complete bipartite graph) är en graf, vars noder är uppdelade i två mängder, A och B, med m resp. n element, och*

1) Till varje par av noder, v i A och w i B, finns precis en kant som binder samman dem;

2) Inget par av noder i A binds samman av någon kant och inget par av noder i B binds samman av någon kant.

26. Vad menas med en delgraf an någon graf? *H sägs vara en delgraf av G (a subgraph of G) om*

1) Varje nod i H är också en nod i G;

2) Varje kant i H är också en kant i G;

3) Om e är en kant i H, så har e samma ändpunkter i H som e har i G.

27. Vad är en väg i en graf G? (*En väg (walk) från en nod v till en nod w i grafen G är en (ändlig) följd*

$$ve_1v_1e_2v_2 \ldots v_{n-1}e_nw$$

av alternerande närliggande noder och kanter, d.v.s. kanten e_i har ändpunkterna v_{i-1} och v_i och $v_0 = v$ och $v_n = w$.)

28. Vad är en stig? (*En stig (trail) från noden v till noden w i grafen G är en väg, där samtliga kanter är olika.*)

29. Vad är en enkel stig? (*En enkel stig (path) är en stig, där även samtliga noder är olika.*)

30. Vad är en sluten (öppen) väg? (*En sluten väg (closed walk) är en väg som börjar och slutar i samma nod. En väg som inte är sluten kallas öppen (open walk).*)

31. Vad är en cykel? En cykel (circuit) är en stig som börjar och slutar i samma nod, d.v.s. en sluten stig.

32. Vad är en enkel cykel? En enkel cykel (cycle) är en cykel, där även samtliga noder, förutom den första och den sista, är olika.

33. Vad är en Eulercykel? (*En cykel som innehåller alla kanter i grafen kallas för en Eulersk cykel.*)

34. Vad är Hamiltonväg (Hamiltoncykel)? (*Det är en väg (en cykel) som passerar varje nod precis en gång.*)

35. Vilken graf kallas för hamiltongraf? (*En graf, som innehåller en Hamiltonväg kallas hamiltongraf (hamiltonian).*)

36. Vilken graf kallas för sammanhängande? (*En graf är sammanhängande om det finns en väg mellan varje par av noder.*)

37. När en sammanhängande graf G utan isolera noder innehåler en Eulercykel? (*Sådan graf innehåler en Eulercykel om och endast om alla noder i G har jämnt gradtal.*)

38. Antag att G är en sammanhängande graf utan isolera noder, och låt a och b vara två noder i G. När gäller att det finns en Eulerväg genom G med start i a och mål i b? (*Om och endast om graderna av a och b är udda och alla andra noder i G har jämn grad.*)

39. Vad är ett träd? (*En graf är ett träd (tree) om den är sammanhängande och om den inte innehåler någon cykel.*)

40. Vad menas med en "färning" ("färgläggning") av en graf? (*Med en färning av en graf menas ett sätt att tilldela färger till grafens noder, så att två noder som förbinds av en kant får olika färg.*)

41. Vad är "kromatiska talet" för en graf G? (*Det minsta antalet färger som möjliggör en färning av en graf G kallas det kromatiska talet för G och betecknas $\chi(G)$.*)

3.2 Övningar

Se övningarna till 24 februari och 3 mars för att förbereda sig till tentamenskrivningen.

Lösningsförslag till utvalda uppgifter

Felrättande koder

1. Svar: a) 010101 b) 000000

2. Eftersom $11111000 + 00011111 = 11100111$ är koden linjär, så dess minimiavstånd är lika med dess minimivikt som är 5; rättar 2 fel ty $5 > 2 \cdot 2$, upptäcker 4 fel ty $5 > 4$.

3.

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

a) Kodordet är $x = c_1c_2 1 c_3 010 c_4 011$, där c_1, c_2, c_3 och c_4 bestäms av $H \cdot x = 0$, alltså

$$\begin{cases} c_4 + 0 + 1 + 1 = 0 \\ c_3 + 0 + 1 + 0 = 0 \\ c_2 + 1 + 1 + 0 + 1 + 1 = 0 \\ c_1 + 1 + 0 + 0 + 0 + 1 = 0 \end{cases} \Leftrightarrow \begin{cases} c_4 = 0 \\ c_3 = 1 \\ c_2 = 0 \\ c_1 = 0 \end{cases}$$

så $x = 00110100011$.

b) Beräkna syndromet $H \cdot x$ för de tre orden: man får

i.

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

inget fel – vi fick kodord;
meddelande (stryk kontrollbitarna) är 1111111.

ii.

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

fel i bit 2 – kontrollbit så ingen informationsbit behöver ändras; meddelande är 1101101.

iii.

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

ger det binra talet $(1110)_2 = 14 > 11$ s vi har mer än ett fel och kan inte avkoda.