SF2715 Tillämpad kombinatorik
Kompletterande material och övningsuppgifter
Del V

Jakob Jonsson

7 maj 2009

Detta häfte innehåller kompletterande material till del V av kursen SF2715 Tillämpad kombinatorik, som ges på KTH under andra halvan av våren 2009. Se det första häftet för allmän information om häftets upplägg.

Utöver övningsuppgifter innehåller häftet även en grafteoretisk tolkning av begreppet Hammingavstånd. Med hjälp av denna tolkning kan vi generalisera vissa av de begränsningar på kodstorleken som diskuteras i avsnitt 17.4 i Cameron.

Innehåll

1 Notation och konventioner

Följande gäller för det här häftet:

- När vi säger att en kod C har längd n menar vi att varje kodord i C har längd n.
- När vi säger att M är en generatormatris till C menar vi att C är den linjära kod vars kodord utgörs av alla linjärkombinationer av *raderna* i matrisen.
- När vi säger att A är en kontrollmatris (*check matrix*) till C menar vi att C är den linjära kod vars kodord utgörs av alla radvektorer w av längd n som uppfyller ekvationen

$$A \cdot w^T = 0 \Longleftrightarrow w \cdot A^T = 0.$$

Detta innebär att vi använder samma notation som i Cameron.

2 Generalisering till grafer

Syftet med detta avsnitt är att generalisera begreppet koder till grafer. Vi gör detta för att öka förståelsen för några av resultaten i avsnitt 17.4 i Cameron. De begrepp som införs i detta avsnitt är helt analoga med motsvarande begrepp i avsnitt 17.2 och 17.4 i Cameron.

Man kan tolka koder i termer av grafer på följande vis. Låt S vara vårt alfabet och n längden på orden. Anta att S innehåller q element. Bilda en graf $G(q, n)$, där vi har ett hörn för varje ord och en kant mellan två hörn om de skiljer sig åt på exakt en position. Avståndet $d_G(v, w)$ mellan två hörn v och w i en graf G definieras som antalet kanter i den kortaste stigen mellan hörnen.

Hjälpsats 2.1 *Hammingavståndet mellan två ord v och w är lika med avståndet $d_{G(q,n)}(v, w)$ mellan motsvarande hörn i grafen $G(q, n)$.*

Om två ord a och b skiljer sig åt på k positioner kan vi nämligen ta oss från a till b i k steg genom att i varje steg ändra symbol på en av de k positionerna där a och b skiljer sig åt. Exempelvis kan vi ta oss från 001122 till 011220 i tre steg längs stigen

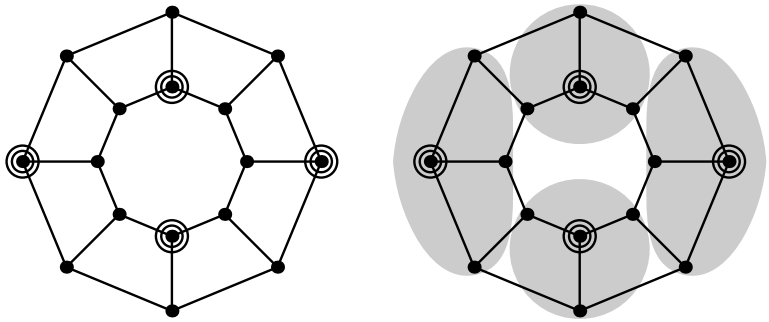
$$(001122, 00112\underline{0}, 001\underline{2}20, 0\underline{1}1220).$$

Ta nu en godtycklig graf G, och definiera en *kod* i G att vara en delmängd C av hörnmängden V sådan att C innehåller minst 2 hörn. Medlemmarna i C kallar vi för *kodord*. Vi säger att C är e-rättande om det för varje hörn v i G finns högst ett kodord c från C sådant att $d_G(v, c) \leq e$.

Följande hjälpsats är analog med Proposition 17.2.2 i Cameron. Beviset lämnas som övning.

Hjälpsats 2.2 *En kod C i grafen G är e-rättande om och endast om det minimala avståndet i C är minst $2e + 1$.*

En av huvudpoängerna med att generalisera till allmänna grafer är att det blir lättare att illustrera de olika resultaten geometriskt. $G(2, n)$ har formen av en hyperkub av dimension n, vilket blir besvärligt att illustrera redan för $n = 4$.



Figur 1: De markerade hörnen bildar en 1-rättande kod. I figuren till höger har vi markerat bollarna med radie 1 runt de fyra kodorden.

I Figur 1 ges ett exempel på en graf med en 1-rättande kod av storlek 4. Att koden är 1-rättande ser vi genom att notera att det för varje hörn i grafen bara finns ett enda kodord som är på avståndet högst 1. Alternativt kan vi notera att avståndet mellan varje par av kodord är minst $2 \cdot 1 + 1 = 3$. I bilden till höger i figuren har vi för varje kodord markerat "bollen" bestående av alla hörn som ligger på avståndet högst ett från det givna kodordet. Att koden är 1-rättande innebär precis att bollarna är disjunkta; se Hjälpsats 2.3 nedan.

Begreppet "boll" visar sig vara väldigt användbart för allmänna grafer G. Låt w vara ett hörn i G och r ett positivt tal. Vi definierar *bollen* $B_r(w)$ *med radie* r *och centrum* w som mängden av hörn v på avstånd högst r från w;

$$B_r(w) = \{v \in V : d_G(v, w) \leq r\}.$$

Hjälpsats 2.3 *En mängd* C *är en* e*-rättande kod om och endast om bollarna i mängden* $\{B_e(c) : c \in C\}$ *är parvis disjunkta.*

Bevis. Att C inte är e-rättande är ekvivalent med att något hörn ligger på avståndet högst e från två olika kodord c_1 och c_2. Detta är i sin tur ekvivalent med att bollarna $B_e(c_1)$ och $B_e(c_2)$ har en icketom skärning. □

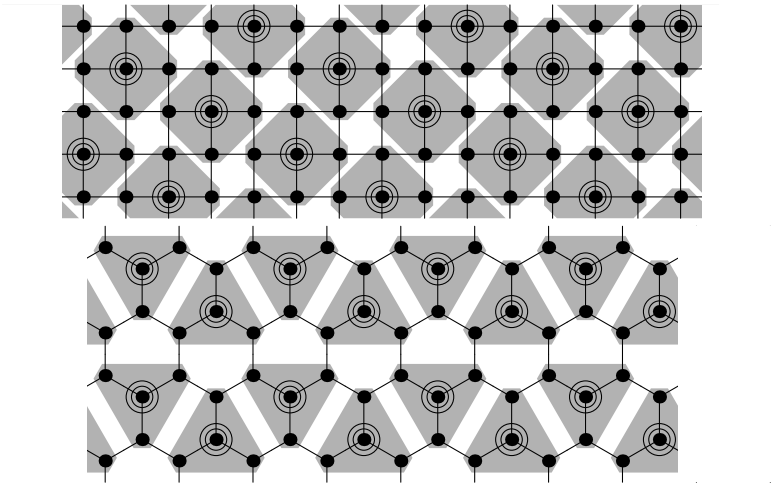
Följande storheter är alltså identiska:

- Maximala antalet disjunkta bollar med radie e som får plats i grafen G.
- Maximala storleken på en e-rättande kod i G.

Låt oss säga att G är r-likformig om alla bollar i G med radie r innehåller samma antal element. Vi låter b_r beteckna detta antal. Observera att $G(q, n)$ är r-likformig för alla r och att vi i detta fall har att

$$b_r = \sum_{k=0}^{r} \binom{n}{k} (q-1)^k. \tag{1}$$

Säg nämligen att vi vill bilda ett ord $v = (v_1, \ldots, v_n)$ på avståndet k från ett givet ord $w = (w_1, \ldots, w_n)$. Först väljer vi de k positioner i där vi vill att v_i och w_i ska vara olika. Detta val kan vi göra på $\binom{n}{k}$ olika sätt. Sedan väljer vi ett v_i skilt från w_i för varje sådan position i. Detta val kan vi göra på $(q-1)^k$



Figur 2: Vi har markerat 1-rättande koder i två så kallade gittergrafer. I båda fallen är graferna ritade på en torus. Detta innebär att kanterna som sticker ut från hörnen längst till höger ska passas ihop med kanterna som sticker ut från hörnen längst till vänster, och analogt för kanterna längst upp och längst ned.

olika sätt. Antalet ord på avståndet k är alltså $\binom{n}{k}(q-1)^k$, vilket medför att antalet ord på avståndet högst r ges av formeln (1).

Sats 2.4 (Hamming-gränsen) *Om G är e-likformig har varje e-rättande kod i G högst $|V|/b_e$ kodord.*

Bevis. Låt C vara en e-rättande kod. Enligt Hjälpsats 2.3 är bollarna i mängden $\{B_e(c) : c \in C\}$ parvis disjunkta, vilket innebär att varje hörn i G är med i som mest en av bollarna. Detta ger att

$$|V| \geq |C| \cdot b_e \iff |C| \leq \frac{|V|}{b_e},$$

vilket är den sökta olikheten. □

Likhet ges precis då varje hörn i grafen tillhör *exakt* en av bollarna. Koden i Figur 1 är ett sådant exempel, och Hamming-gränsen är mycket riktigt lika med antalet kodord, ty $|V|/b_1 = 16/4 = 4$.

För att göra kopplingen till vanliga koder explicit använder vi nu Sats 2.4 och (1) för att dra följande slutsats:

Följdsats 2.5 (17.4.2 i Cameron) *Låt $n \geq 3$, $q \geq 2$ och $e \geq 1$. Varje e-rättande kod av längd n över ett alfabet av storlek q har högst*

$$\frac{|V|}{b_e} = \frac{q^n}{\sum_{k=0}^{e}\binom{n}{k}(q-1)^k}$$

kodord.

Notera att faktorn $(q-1)^k$ är lika med 1 i det viktiga specialfallet $q = 2$.

Låt oss även ge en generalisering av (17.4.1) i Cameron:

Sats 2.6 *Om G är $2e$-likformig finns det en e-rättande kod i G med minst $|V|/b_{2e}$ kodord.*

Bevis. Låt C vara en kod i G som är maximal. Anta att det finns något hörn x som inte är med i bollen $B_{2e}(c)$ för något kodord c. Då är x på avståndet minst $2e+1$ från vart och ett av kodorden i C, vilket innebär att $C \cup \{x\}$ är en kod, en motsägelse. Alltså är alla hörn med i minst en boll $B_{2e}(c)$ sådan att c är ett kodord, vilket innebär att

$$|V| \leq |C| \cdot b_{2e} \iff |C| \geq \frac{|V|}{b_{2e}}.$$

Detta är den sökta olikheten. □

I specialfallet med vanliga koder erhåller vi följande, där vi än en gång använder oss av formeln (1):

Följdsats 2.7 (17.4.1 i Cameron) *Låt $n \geq 3$, $q \geq 2$ och $e \geq 1$. Det finns en e-rättande kod av längd n över ett alfabet av storlek q med minst*

$$\frac{|V|}{b_{2e}} = \frac{q^n}{\sum_{k=0}^{2e} \binom{n}{k}(q-1)^k}$$

kodord.

Detta resultat brukar kallas för Varshamov-Gilbert-gränsen. Om man vill kan förkorta detta som VG-gränsen. Än en gång kan man notera att faktorn $(q-1)^k$ blir lika med 1 i specialfallet $q = 2$.

Ö Övningsuppgifter

Ö.1 Två koder med sju kodord

(a) Låt C vara koden bestående av följande sju kodord av längd 10:

$$\begin{aligned} a &= 00000\,00000 \\ b &= 11000\,11100 \\ c &= 00110\,01110 \\ d &= 10001\,00111 \\ e &= 01100\,10011 \\ f &= 00011\,11001 \\ g &= 11111\,11111 \end{aligned}$$

Beräkna avståndet mellan varje par av kodord i C, och ange det minimala avståndet i C.

(b) Låt C' vara koden bestående av följande sju kodord av längd 11:

$$\begin{aligned} a &= 00000\,00000\,0 \\ b &= 11000\,11100\,1 \\ c &= 00110\,01110\,1 \\ d &= 10001\,00111\,1 \\ e &= 01100\,10011\,1 \\ f &= 00011\,11001\,1 \\ g &= 11111\,11111\,0 \end{aligned}$$

Vi lägger alltså till en bit till vart och ett av kodorden i (a). Beräkna avståndet mellan varje par av kodord i C', och ange också det minimala avståndet i C'.

Svårighetsgrad: E

Ö.2 Övre och nedre gränser på binära koder av längd 90

(a) Visa att det finns en 1-rättande binär kod av längd 90 med 2^{78} element.

(b) Visa att det inte finns någon 2-rättande binär kod av längd 90 med fler än 2^{78} element.

Svårighetsgrad: D

Ö.3 Tillämpning av Plotkin-gränsen

(a) Låt $q \geq 2$, och låt d vara ett positivt heltal sådant att $d-1$ är delbart med $q-1$. Definiera

$$n = \frac{qd-1}{q-1} = d + \frac{d-1}{q-1}.$$

Använd Plotkin-gränsen för att visa att qd är en övre begränsning på antalet kodord i en kod av längd n över ett alfabet av storlek q med egenskapen att kodens minimala avstånd är d.

(b) Låt C vara den binära kod som består av följande 8 kodord av längd 7:

$$\begin{aligned} a &= 0000\,000 \\ b &= 1111\,000 \\ c &= 1100\,110 \\ d &= 0011\,110 \\ e &= 1010\,101 \\ f &= 0101\,101 \\ g &= 1001\,011 \\ h &= 0110\,011 \end{aligned}$$

Beräkna avståndet mellan varje par av kodord i C.

(c) Finns det någon kod av längd 7 med fler än 8 kodord och med samma minimala avstånd som C?

Svårighetsgrad: (a): C, (b): E, (c): E

Ö.4 Utvidgad kod I

Låt C vara en e-rättande kod vars kodord har längd n. Låt $k \geq 1$. För ett givet kodord c, definiera c^k att vara det ord av längd kn som man erhåller om man upprepar ordet c sammanlagt k gånger. Exempelvis är $(0111)^3 = (0111\ 0111\ 0111)$. Låt

$$C^{(k)} = \{c^k : c \in C\}.$$

(a) Visa att $C^{(k)}$ är e_k-rättande, där e_k är lika med $ke + \frac{k-1}{2}$ avrundat nedåt.

(b) Anta att en avkodningsmetod för C är given. För ett givet ord w av längd n kan vi alltså beräkna det unika kodord $c \in C$ med egenskapen att Hammingavståndet mellan c och w är högst e (om ett sådant kodord c finns). Definiera en avkodningsmetod för $C^{(k)}$ i termer av denna avkodningsmetod. Avkodningsmetoden ska fungera för alla ord som är på Hammingavstånd högst e_k från något ord i $C^{(k)}$, där e_k är definierat som i (a).

Svårighetsgrad: (a): D, (b): A

Ö.5 Dubbla antalet kodord

Låt C vara en binär kod av längd n med minimalt avstånd d sådan att alla kodord består av högst $\frac{n-d}{2}$ ettor. Utvidga C till en binär kod av längd n med dubbelt så många kodord som C och med samma minimala avstånd d.

Svårighetsgrad: B

Ö.6 Linjär kod I

Låt C vara den binära linjära kod av längd 11 som har generatormatris

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

(a) Avgör om C är 2-rättande. Motivera ditt svar med ett bevis eller motexempel.

(b) Bestäm en kontrollmatris (*check matrix*) till C.

(c) Vad är den maximala storleken på en binär 2-rättande linjär kod av längd 11? *Ledning:* Studera Hamming-gränsen.

Svårighetsgrad: (a): E, (b): E, (c): C

Ö.7 Linjär kod II

Låt nu C vara den binära linjära kod av längd 11 som har *kontrollmatris*

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

(a) Hur många kodord innehåller C?

(b) Visa att C är 1-rättande.

(c) Bestäm en generatormatris till C.

(d) Bestäm bitarna a_1, a_2, a_3, a_4 så att vektorn

$$w = (a_1, a_2, a_3, a_4, 1, 1, 0, 1, 1, 0, 0)$$

blir ett kodord.

Svårighetsgrad: E

Ö.8 Linjär kod III

Låt C vara den binära linjära kod av längd 11 som har generatormatris

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

(a) Avgör om C är 2-rättande. Motivera ditt svar med ett bevis eller motexempel.

(b) Bestäm en kontrollmatris till C.

Svårighetsgrad: E

Ö.9 Utvidgad kod II

Låt C vara en linjär e-rättande binär kod av längd n med 2^k kodord.

(a) Låt C' vara den binära koden av längd $3n$ bestående av alla tripplar $(a, b, a+b)$, där $a, b \in C$. Visa att C' är $2e$-rättande och består av 2^{2k} kodord.

(b) Låt nu C' vara den binära koden av längd $6n$ bestående av alla följder $(a, b, c, a+b, a+c, b+c)$, där $a, b, c \in C$. Visa att C' är $(3e+1)$-rättande och består av 2^{3k} kodord.

Svårighetsgrad: (a): C, (b): B

Ö.10 Brus som skapar sviter av fel

I en tillämpning har man tillgång till en brusig kanal genom vilken man kan skicka binära ord av längd n. Tråkigt nog kan godtyckligt många bitar i ett givet ord bli felaktiga, men i gengäld bildar de felaktiga bitarna alltid en sammanhängande svit i ordet. Skickar vi ordet $(a_1, \ldots, a_n)$ blir slutresultatet alltså antingen ordet självt eller ett ord på formen

$$(a_1, \ldots, a_{i-1}, \overline{a_i}, \overline{a_{i+1}}, \ldots, \overline{a_{j-1}}, \overline{a_j}, a_{j+1}, \ldots, a_n),$$

där $1 \leq i \leq j \leq n$; $\overline{a_k} = 1 - a_k$.

Låt nu C vara en binär 2-rättande kod av längd n, alltså samma längd som på de ord som kan skickas genom kanalen. Man vill definiera en transformation $\varphi : C \to \{0,1\}^n$ med följande egenskap för varje kodord $\mathsf{b} \in C$:

- Om $\varphi(\mathsf{b})$ skickas genom kanalen, så är b entydigt bestämt av det mottagna ordet.

Hitta en lämplig transformation φ, och visa att den har önskade egenskaper för varje val av C.

Svårighetsgrad: A

Ö.11 Fördjupningsuppgift: Kod bestående av multiplar av ett polynom

Låt $r \geq 1$, och låt $f(x)$ vara ett polynom av grad r över kroppen med q element, där q är en primtalspotens. Låt $k \geq 1$, och studera koden

$$C = \{f(x)g(x) : \deg g \leq k-1\}.$$

Här identifierar vi ett polynom $\sum_{i=0}^{r+k-1} a_i x^i$ med vektorn $(a_0, a_1, \ldots, a_{r+k-1})$, vilket innebär att C är en kod av längd $r+k$.

(a) Visa att C ej är 1-rättande om k är tillräckligt stort. *Ledning:* Studera Hamming-gränsen.

(b) Anta att $f(x)$ har en nollskild konstantterm. Visa att det finns ett polynom $g(x)$ sådant att $f(x)g(x) = x^N - b$ för något $N \geq 1$ och någon nollskild skalär b.

Ö.12 Fördjupningsuppgift: Polynombaserade koder

Låt $\mathbb{F}$ vara en ändlig kropp, och låt $x_1, \ldots, x_n$ vara olika element i $\mathbb{F}$. Låt $k \leq n$, och definiera

$$C = \{(f(x_1), \ldots, f(x_n)) : f \text{ polynom över } \mathbb{F} \text{ av grad högst } k-1\}.$$

Visa att C är en linjär kod över $\mathbb{F}$ med minimalt avstånd $n-k+1$.

Ledning. Använd faktorsatsen, som säger följande: Om f är ett polynom över $\mathbb{F}$ och $a_1, \ldots, a_k$ är olika element från $\mathbb{F}$ sådana att

$$f(a_1) = f(a_2) = \cdots = f(a_k) = 0,$$

så är

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)g(x)$$

för något polynom g.

(I fallet då $\{x_1, \ldots, x_n\}$ är lika med $\mathbb{F} \setminus \{0\}$ är koden en så kallad Reed-Solomon-kod. Felkorrigering med Reed-Solomon-koder används i bland annat CD- och DVD-skivor och vid en rad former av dataöverföring.)