Föreläsning 6

MA1508

Matrismetoder för koder, mm

Vi betraktade förra gången en kod som kunde beskrivas med ekvationssystemet

$$\begin{cases} x_1 + x_3 = 0 \\ x_1 + x_5 = 0 \\ x_2 + x_4 = 0 \\ x_2 + x_6 = 0 \end{cases}.$$

Nu när vi har tillgång till matriser kan vi skriva det ekvationssystemet som

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Notera mönstret hur vi får elementen i matrisen från koefficienterna i ekvationssystemet. Att skriva upp matrisen är ett bekvämt sätt att representera ekvationssystemet.

Koder där kodorden är de strängar som uppfyller

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

för någon matris A kallas *linjära*, och där vi menar att det bara är nollor i högerledet. A kallas checkmatrisen för koden.

Exempel 1. Koden av längd 4 med en paritetsbit kan beskrivas av ekvationen

$$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0$$

Den är alltså linjär. △

Sats. *Om K är en linjär kod så kommer antalet kodord alltid vara 2^k, för något heltal k. Strängen med bara nollor kommer tillhöra K. Om u och v är kodord så är $u+v$ också ett kodord.*

Bevis. Att visa att strängen med bara nollor tillhör varje linjär kod är enkelt, och likaså att summan av två kodord är ett kodord. Att visa att antalet kodord kan skrivas som 2^k är svårare. □

Det finns också konceptet *generatormatriser*. Det kan enklast förklaras som att kodorden då är de strängar vi kan få som summan av en eller flera rader i matrisen, och nollsträngen. (Som kan ses som fallet när vi tar summan av inga av raderna.)

Exempel 2. Anta att en kod har generatormatrisen

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

Då är kodorden följande 000, 101 (första raden), 011 (andra raden) och 110 (summan av första och andra raden.) △

Sats. *Alla linjära koder har en generatormatris och alla koder som har en generatormatris är linjära.*

Frågor om generatormatris kommer ej på tentan.

Hammingkoden

Hammingkoden är en kod med checkmatrisen

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

Om vi tittar noggrant på checkmatrisen kan vi se att vi kan välja de 4 sista bitarna hur som helst, men då är de första 3 bitarna bestämda. Det blir en $(7,4)$-kod alltså.

Vi visar nu att den är 1-felrättande. Boken har ett argument för det, vi visar ett annat vis så ni har chans att se olika angreppssätt.

Anta kodordet, c, skickats men att det blir fel i bit nummer i. Låt f vara strängen som består av nollor utom på plats i, där det står en etta. Jag påstår det mottagna kodordet är $c+f$. Låt oss multiplicera H med $c+f$ (skrivet som en matris med 1 kolonn. Jag påstår att vi kan räkna såhär:

$$H \cdot (c+f) = Hc + Hf = Hf.$$

Att kontrollera att man faktiskt kan räkna så blir att fundera lite på definitionen av matrismultiplikation.

Låt oss nu ta ta exemplet där $f = 0001000$.

Då blir

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

Svaret är samma sak som den fjärde kolonnen i matrisen och vi kan tänka igenom definitionen av matrismultiplikation igen och inse att när vi multiplicerar H med en vektor som består av nollor överallt utom på plats i, så kommer svaret bli likadant som kolonn i i H. Finns det två kolonner i H som är lika? Nej, det finns det inte. Det här betyder att om vi räknar $H(f + c)$ och f innehåller precis en etta, så kan vi genom att känna igen vilken kolonn vi får som svar avgöra var felet har inträffat. Får vi kolonn nummer i som svar är det i bit nummer i som felet inträffat.

Exempel 3. Alice och Bob använder Hammingkoden. Bob tar emot 1010000. Är det ett kodord? Om inte, vilket kodord ska han gissa Alice skickade? (Anta det inte sker mer än ett fel.)

△

Även om A inte är Hammingmatrisen är det sant att om f är en vektor med exakt en etta så blir Af lika med kolonn nummer i i A. Om A inte har någon kolonn som består av bara nollor, och inte två kolonner som är lika, så kan koden med A som checkmatris alltid rätta 1 fel. (Kanske fler.)

Exempel 4. Koden med checkmatrisen

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

kan rätta ett fel.

△

Hammingavstånd

Definition. Med *Hammingavståndet* mellan två strängar, x och y, av samma längd menar vi antalet platser de skiljer sig åt på. Brukar betecknas $d(x, y)$.

Exempel 5.

$$d(11000, 10101) = 3.$$

△

Sats. *Om x, y, z är strängar av samma längd så gäller att*

1. $d(x, y) \geq 0$

2. $d(x, y) = 0$ *om och endast om* $x = y$.

3. $d(x, z) \leq d(x, y) + d(y, z)$.

Nästa gång kommer vi koppla Hammingavståndet till koders felrättande kapacitet och andra saker vi pratat om.