Fejlkorligerende køder $\mapsto$ Fejlkorrigerende koder

Denne note er skrevet med udgangspunkt i [1, p. 240-243, 249]. Et videre studium kan eksempelvis tage udgangspunkt i [2]. Eventuelle kommentarer kan sendes til olav@math.aau.dk

I kurset "Lineær Algebra" arbejder vi normalt med matricer, hvor elementerne er reelle tal. Nærværende note omhandler tilfældet, hvor elementerne i matricerne er tal i talstrukturen $\mathbb{Z}_2 = \{0, 1\}$. Regnereglerne i $\mathbb{Z}_2$ er som følger[1]:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Bemærk, at $1 + 1 = 0 = 1 - 1$. Derfor er plus og minus det samme i $\mathbb{Z}_2$.

Eksempel 1 *Betragt vektorene*

$$\vec{u} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \vec{v} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

i $\mathbb{Z}_2^4$. *Vi har* $\vec{u} \cdot \vec{v} = 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 = 1 + 0 + 0 + 1 = 1 + 1 = 0$. $\square$

De fleste resultater, I kender for matricer over $\mathbb{R}$, gælder også for matricer over[2] $\mathbb{Z}_2$.

Betragt situationen, hvor vi vil kommunikere over en støjfyldt kanal (tænk på et langt ikke-afskærmet datakabel). Vi ønsker at sende en følge af 0'er og 1'er svarende til indholdet af en fil. At kanalen er støjfyldt betyder, at nogle af 0'erne bliver lavet om til 1'er, inden de når frem til modtageren. Tilsvarende bliver nogle af 1'erne lavet om til 0'er. En simpel måde, hvorpå vi kan beskytte vores datatransmission, er hvis afsenderen sender tre kopier

[1] Læseren med kendskab til logik vil bemærke, at kompositionen $+$ svarer til XOR, samt at kompositionen $\cdot$ svarer til AND.

[2] Dette skyldes, at $\mathbb{Z}_2$ er et såkaldt legeme.

af hvert enkelt binært symbol. Istedet for 0 sendes altså 000, og istedet for 1 sendes 111. De tilsvarende vektorer

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

kaldes kodeord. Antag nu, at modtageren i den anden ende af informationskanalen modtager 110. Denne vil nu regne med, at der nok er sket fejl i tredie position, hvorfor den sendte besked antages at være 1. Tilsvarende vil man dekode 001 til 000, og dermed vil man antage, at den sendte besked er 0. Bemærk, at vi kan rette en fejl, men ikke to eller tre. Lad os bringe ovenstående på matrix form. Beskederne 0 og 1 identificeres med vektorerne [0] og [1], og som nævnt ovenfor skrives kodeordene som søjlevektorer af længde 3.

Mængden af kodeord kaldes en kode.

Indkodningen ovenfor af beskeder til kodeord svarer til den lineær transformation

$$T : \mathbb{Z}_2 \to \mathbb{Z}_2^3$$

som repræsenteres af matricen

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Altså er indkodningen givet ved $G\vec{m}$, hvor $\vec{m}$ tilhører $\mathbb{Z}_2 = \{0, 1\}$. Matricen G kaldes en generatormatrix.
Hvis vi vil tjekke, om

$$\vec{c} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \in \mathbb{Z}_2^3$$

er et kodeord, skal vi undersøge, om alle tre komponenter er ens. Dette svarer til at tjekke, om

$$\begin{cases} c_1 &= c_2 \\ c_1 &= c_3 \end{cases}$$

holder, hvilket er det samme som at tjekke, om

$$\begin{cases} c_1 + c_2 &= 0 \\ c_1 + c_3 &= 0 \end{cases}$$

holder (husk + og − er det samme), hvilket igen er det samme som at tjekke om

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

holder. Matricen

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

kaldes for en paritetstjekmatrix.
Koden $C = \{[0\,0\,0]^T, [1\,1\,1]^T\}$ er lig søjlerummet hørende til G og samtidig lig nulrummet hørende til H (læseren opfordres til at tjekke dette). Koden C er et underrum af $\mathbb{Z}_2^3$ med dimension 1. Antag, at $\vec{c} = [1\,1\,1]^T$ er afsendt, men at $\vec{r} = [1\,0\,1]^T$ er modtaget. Vi har $\vec{r} = \vec{c} + \vec{e}$, hvor $\vec{e} = [0\,1\,0]^T$ er fejlvektoren. I stedet for den tidligere beskrevne dekodningsmetode (den, hvor vi ser hvilket symbol 0 eller 1, der forekommer flest gange) dekoder vi nu vha. paritetstjekmatricen. Det vil hjælpe os til at demonstrere et snedigt generelt princip. Vi udregner

$$H\vec{r} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{1}$$

Da dette er forskelligt fra $[0\,0]^T$, er der sket fejl. Bemærk, at $H\vec{r} = H(\vec{c}+\vec{e})$, hvor $\vec{e}$ er fejlvektoren beskrevet ovenfor. Men $H\vec{c} = \vec{0}$, og derfor har vi $H\vec{e} = H\vec{r} = [1\,0]^T$. Læg mærke til, at hver ikke-nul vektor i $\mathbb{Z}_2^2$ forekommer præcis n gang som søjle i H, samt at højre side af (1) svarer til anden søjle i H. Vi konkluderer, at hvis der kun er sket en fejl, da er det i position 2. Altså $\vec{e} = [0\,1\,0]^T$, og dermed

$$\vec{c} = \vec{r} - \vec{e} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

Den afsendte besked er altså lig 1.
Vi genereliserer nu ovenstående konstruktion af koder.

Definition 1 *Et k-dimensionalt underrum af $\mathbb{Z}_2^n$ kaldes en $[n,k]$-kode. Givet en $[n,k]$-kode C, da kaldes en $n \times k$ matrix G for en en tilhørende generatormatrix, når søjlerne i G er en basis for C. Tilsvarende kaldes en $(n-k) \times n$ matrix H for en paritetstjekmatrix for C, når C er nulrummet hørende til H.*

En $[n,k]$-kode kan altså bruges til at indkode beskeder af længde k. En besked $\vec{m} \in \mathbb{Z}_2^k$ identificeres med et kodeord $\vec{c} \in \mathbb{Z}_2^n$ ved $\vec{c} = G\vec{m}$.

Definition 2 *Lad $k < n$. En $[n,k]$ kode kaldes systematisk, hvis den har en generatormatrix af formen*

$$G = \begin{bmatrix} I_k \\ A \end{bmatrix}.$$

(Her er A selvfølgelig en $(n-k) \times k$ matrix).

Bemærkning 1 *Givet et kodeord i en systematisk kode, da optræder den indkodede besked som de første k indgange.*

Sætning 1 *Lad C være en systematisk $[n,k]$-kode med generatormatrix*

$$G = \begin{bmatrix} I_k \\ A \end{bmatrix}.$$

Så er $H = [A\, I_{n-k}]$ en paritetstjekmatrix for C (dvs. $\vec{c} \in C$, hvis og kun hvis $H\vec{c} = \vec{0}$).

Bevis: Lad $\vec{c} \in C$ være et vilkårligt kodeord, dvs. $\vec{c}$ er af formen $\vec{c} = G\vec{m}$. Men så er

$$\begin{aligned} H\vec{c} &= HG\vec{m} = [A\, I_{n-k}] \begin{bmatrix} I_k \\ A \end{bmatrix} \vec{m} \\ &= (A + A)\vec{m} = O\vec{m} = \vec{0}. \end{aligned}$$

Vi har nu vist, at C er indeholdt i nulrummet hørende til H. Men såvel nulrummet hørende til H som C har dimension k, så C må være lig med nulrummet. □

Eksempel 2 *Koden med paritetstjekmatrix*

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = \left[\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right] = [A\, I_3]$$

kaldes en binær Hammingkode. Ifølge Definition 2 og Sætning 1 er den systematisk med generatormatrix

$$G = \begin{bmatrix} I_4 \\ A \end{bmatrix}.$$

Der er således tale om en $[7,4]$-kode. Bemærk, at søjlerne i H består af samtlige ikke-nul vektorer. Hver af disse forekommer præcis en gang. Beskeden $\vec{m} = [1\,0\,1\,0]^T$ indkodes nu til

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Der sker nu fejl under transmissionen, således modtages

$$\vec{r} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Modtageren kender ej det afsendte ord, men leder efter $\vec{c} \in C$, således at der gælder $\vec{r} = \vec{c} + \vec{e}$, hvor $\vec{e}$ kun har en ikke-nul indgang. Der regnes

$$H\vec{r} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Bemærk, at $H\vec{c} = \vec{0}$ (jævnfør definitionen af H), og derfor har vi $H\vec{r} = H(\vec{c}+\vec{e}) = H\vec{e}$. Hvis der kun er en ikke-nul indgang i $\vec{e}$, da må det være den femte, da $[1\,0\,0]^T$ er den femte søjle i H. Modtageren dekoder derfor korrekt til

$$\vec{c} = \vec{r} + \vec{e} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}. \qquad \square$$

Vi har i Eksempel 2 argumenteret for, at man kan bruge følgende dekodningsalgoritme for Hammingkoden:

1. Modtageren udregner $H\vec{r}$.
2. Hvis $H\vec{r} = \vec{0}$, da konkluderes det, at der nok ikke er sket fejl.
3. Hvis $H\vec{r} \neq \vec{0}$, da undersøges hvilket søjlenummer j, som svarer hertil. Fejlen antages at være sket i position j, og der dekodes i overensstemmelse hermed.

Ved at argumentere som ovenfor kan man vise følgende sætning.

Sætning 2 *En $[n, k]$-kode med paritetstjekmatrix H kan rette (mindst) en fejl, hvis og kun hvis søjlerne i H er parvis forskellige, og alle er forskellige fra $\vec{0}$.*

Opgave 1 *Vi indkoder beskederne i $\mathbb{Z}_2^2$ på følgende vis:*

$$T\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad T\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad T\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Der er altså tale om en $[n, k] = [4.2]$-kode. Vis ved et modeksempel, at koden ikke kan rette fejl.

Opgave 2 *Lad $\vec{m} = [1\ 1\ 0\ 0]$. Find det tilhørende kodeord i den binære Hammingkode. Gør det samme for $\vec{m}$ lig henholdsvis $[0\ 1\ 1\ 1]$ og $[1\ 1\ 1\ 1]$.*

Opgave 3 *Betragt den binære Hammingkode. Modtageren modtager $\vec{r} = [0\ 1\ 0\ 0\ 0\ 0\ 0]^T$. Foretag dekodning. Udfør tilsvarende beregning for $\vec{r} = [1\ 1\ 0\ 0\ 1\ 1\ 0]^T$.*

Opgave 4 *Betragt den binære Hammingkode. Antag at der er sket mere end en fejl. Argumenter for, at modtageren dekoder forkert.*

Opgave 5 *Bevis Sætning 2.*

Opgave 6 *Betragt koden med generatormatrix*

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

List alle kodens kodeord. Find den tilhørende paritetstjekmatrix. Kan koden rette fejl? (Argumenter for dit svar.)

References

[1] David Poole, "Linear Algebra - A Modern Introduction," Sec. ed., Thomson, 2006

[2] J. Justesen og T. Høholdt, " A Course In Error-Correcting Codes," European Mathematical Society, *Textbooks in Mathematics*, 2004