



AALBORG UNIVERSITY
DENMARK

Aalborg Universitet

Fejlkorrigerende koder

Christensen, René Bødker

Creative Commons License
Ikke-specificeret

Publication date:
2020

Document Version
Også kaldet Forlagets PDF

[Link to publication from Aalborg University](#)

Citation for published version (APA):
Christensen, R. B. (2020). Fejlkorrigerende koder. Lyd og/eller billed produktion (digital), .

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.



Opgaver: Fejlkorrigerende koder

René Bødker Christensen, Videnskabelig assistent
Institut for Matematiske Fag, Aalborg Universitet

Øvelse 1:

Indkod følgende beskeder ved hjælp af Hamming-koden.

- a. (1, 1, 0, 0)
- b. (1, 0, 1, 1)



Øvelse 2:

Vi har modtaget ordet (0, 0, 1, 1, 0, 0, 1). Er dette et kodeord i Hamming-koden?

Find det rigtige kodeord, hvis der maksimalt er sket én fejl. Hvad er den tilsvarende besked?



Øvelse 3:

Hvis ordet (0, 1, 1, 0, 1, 0, 0) indeholder højst én fejl, hvad er så beskeden?



Øvelse 4:

Tag ét af kodeordene fra Øvelse 1, og tilføj to fejl. Hvad sker der, når vi dekoder som før?



I praksis vil vi bruge en computer til at indkode beskederne, men her er figuren med de tre cirkler en upraktisk beskrivelse af indkodningen. I stedet bruger vi det, der kaldes en *generatormatrix*, som også kan bruges til andre (lineære) koder end Hamming-koden.

For eksempel kan Hamming-koden, vi har arbejdet med, beskrives ved generatormatricen

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

Antallet af rækker i G fortæller, hvor mange symboler beskeden indeholder – 4 i dette tilfælde – og antallet af søjler giver antallet af symboler i et kodeord – 7 for Hamming-koden.

For at indkode beskeden (a, b, c, d) ved hjælp af generatormatricen, tager vi summen af a gange den første række, b gange den anden række, c gange den tredje række og d gange den fjerde. Eksempelvis vil $(1, 0, 0, 1)$ indkodes til

$$1 \cdot (1, 0, 0, 0, 1, 1, 1) + 0 \cdot (0, 1, 0, 0, 1, 0, 1) + 0 \cdot (0, 0, 1, 0, 1, 1, 0) + 1 \cdot (0, 0, 0, 1, 0, 1, 1)$$

som giver

$$(1, 0, 0, 0, 1, 1, 1) + (0, 0, 0, 1, 0, 1, 1) = (1, 0, 0, 1, 1, 0, 0).$$

Bemærk her, at vi lægger rækkerne sammen elementvist,¹ og at vi lader $1 + 1$ være 0, så vi altid ender med symbolerne 0 og 1.

Øvelse 5:

Indkod beskederne fra Øvelse 1 ved at bruge generatormatricen G . Tjek, at resultatet er det samme.

¹Hvis I har haft om vektorer, vil I genkende dette som sum af vektorer

De regneregler vi har brugt indtil videre kan opsummeres i såkaldte additions- og multiplikationstabeller:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Vi siger, at vi arbejder med 'det endelige legeme' med to elementer, som noteres med \mathbb{F}_2 . Når vi arbejder her bruger vi ofte \equiv i stedet for det almindelige lighedstegn. Reglen i \mathbb{F}_2 kan således opsummeres ved $2 \equiv 0$, og vi bruger dette til at reducere til enten 0 eller 1.

I stedet for 2, kan man bruge et hvilket som helst andet primtal.² Arbejder vi eksempelvis i \mathbb{F}_5 , bruger vi reglen $5 \equiv 0$ til at reducere ethvert resultat til et af tallene 0, 1, 2, 3 eller 4. For eksempel vil $4 \cdot 3$ give 2, da

$$4 \cdot 3 \equiv 12 \equiv 2 \cdot 5 + 2 \equiv 2 \cdot 0 + 2 \equiv 2,$$

mens $2 \cdot 2$ giver 4 som normalt, da dette allerede er reduceret.

Øvelse 6:

Udfyld additions- og multiplikationstabellerne for det endelige legeme \mathbb{F}_3 . Det vil sige, at vi nu har reglen $3 \equiv 0$.

$$\begin{array}{c|ccc} + & 0 & 1 & 2 \\ \hline 0 & & & \\ 1 & & & \\ 2 & & & \end{array} \quad \begin{array}{c|ccc} \cdot & 0 & 1 & 2 \\ \hline 0 & & & \\ 1 & & & \\ 2 & & & \end{array}$$



Øvelse 7:

Udfyld additions- og multiplikationstabellerne for det endelige legeme \mathbb{F}_5 .

$$\begin{array}{c|ccccc} + & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & & & & & \\ 1 & & & & & \\ 2 & & & & & \\ 3 & & & & & \\ 4 & & & & & \end{array} \quad \begin{array}{c|ccccc} \cdot & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & & & & & \\ 1 & & & & & \\ 2 & & & & & \\ 3 & & & & & \\ 4 & & & & & \end{array}$$




I de to næste opgaver, skal I arbejde med en kode over \mathbb{F}_3 . I skal altså bruge regnereglerne fra Øvelse 6. Koden, I skal se på, har generatormatrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 2 & 1 \end{bmatrix}. \quad (1)$$

²Man kan også bruge p^r , hvor p er et primtal, og r et positivt heltal. Dette kræver dog en mere kompliceret konstruktion.

Øvelse 8:

Betragt koden over \mathbb{F}_3 med generatormatricen G givet i (1).

Tjek, at beskeden $(2, 2)$ indkodes til $(2, 2, 2, 2, 2)$. Hvad er afstanden fra $(2, 2, 2, 2, 2)$ til kodeordet $(1, 2, 1, 0, 1)$? 

Husk nu, at vi kan rette e fejl, hvis $2e < d$, hvor d er mindsteafstanden for koden. Når vi arbejder med lineære koder (som vi gør her), viser det sig, at vi kan finde mindsteafstanden en smule lettere. I stedet for at sammenligne afstandene mellem *alle* par af kodeord, kan vi nøjes med at finde det kodeord, der har færrest symboler forskellige fra 0 (bortset fra kodeordet, der kun indeholder 0'er). Antallet af ikke-nul symboler i dét kodeord viser sig at være mindsteafstanden.

For eksempel vil koden over \mathbb{F}_2 med kodeord $(0, 0, 0, 0)$, $(1, 1, 0, 0)$, $(0, 0, 1, 1)$ og $(1, 1, 1, 1)$ have mindsteafstanden 2, da $(1, 1, 0, 0)$ og $(0, 0, 1, 1)$ begge har 2 ikke-nul symboler, og der er ingen kodeord – udover nulkodeordet $(0, 0, 0, 0)$ – med færre ikke-nul symboler.

Øvelse 9:

Opskriv alle de forskellige kodeord i koden over \mathbb{F}_3 med generatormatricen fra (1) (der er 9 kodeord). Hvad er mindsteafstanden, og hvor mange fejl, kan der rettes? 