Fejlrettende koder – Opgaver

Opgave 1: Primitivt element

Vis at 2 er et primitivt element i $\mathbb{F}_{11}$, altså at $ord(2) = 10$, ved at beregne 2^2 og 2^5.

Opgave 2: Reed–Solomon indkodning

I denne opgave betragtes en Reed–Solomon kode med $\mathbb{F}_{11}^*$ som alfabet. Koden har længde $n = 10$ og dimension $k = 6$.

1. Hvad er kodens minimumsafstand d?
2. Hvor mange fejl kan koden rette? Kald denne størrelse for t.
3. Vælg en meddelelse, dvs. vælg k elementer i $\mathbb{F}_{11}$. Kald elementerne i meddelelsen for m_0, m_1, m_2, m_3, m_4 og m_5, og dan det tilhørende polynomium:
$$g(X) = m_5X^5 + m_4X^4 + m_3X^3 + m_2X^2 + m_1X + m_0.$$
4. Bestem kodeordet der svarer til den valgte meddelelse, dvs. udregn:
$$\begin{aligned} c &= (c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_9, c_{10}) \\ &= \big(g(2^0), g(2^1), g(2^2), g(2^3), g(2^4), g(2^5), g(2^6), g(2^7), g(2^8), g(2^9)\big). \end{aligned}$$
5. Indholdet af c er det kodeord der sendes fra afsenderen til modtageren. For at simulere at der er sket fejl under transmissionen laves t fejl på c. Vælg t pladser i c og lav om på indholdet af disse. Det resulterende ord kaldes r:
$$r \;=\; (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_9, r_{10}).$$
De følgende opgaver vil gennemgå hvordan modtageren kan lokalisere og rette disse fejl.

Opgave 3: Fejllokaliseringspolynomium

I denne opgave gennemgås hvorledes positionerne af de fejl der blev tilføjet c i opgave 2 kan findes.

1. Opskriv polynomiet svarende til det modtagne ord r, altså
$$r(X) = r_9X^9 + r_8X^8 + r_7X^7 + r_6X^6 + r_5X^5 + r_4X^4 + r_3X^3 + r_2X^2 + r_1X + r_0.$$
2. Det ligningssystem der skal løses for at finde positionerne med fejl i r er:
$$\begin{aligned} 0 &= b_2 \cdot r(2^3) + b_1 \cdot r(2^2) + b_0 \cdot r(2^1) \\ 0 &= b_2 \cdot r(2^4) + b_1 \cdot r(2^3) + b_0 \cdot r(2^2) \end{aligned}$$

Beregn koefficienterne i dette ligningssystem altså $r(2), r(2^2), r(2^3)$ og $r(2^4)$.

3. Løs det ovenstående ligningssystem, og bestem derved b_0, b_1 og b_2.
4. Opskriv fejllokaliseringspolynomiet
$$Q_1(X) = b_2X^2 + b_1X + b_0.$$
Find samtlige rødder i dette polynomium, fx ved at evaluere det i de forskellige værdier i $\mathbb{F}_{11}$.
5. Bestem i_1 og i_2 så 2^{i_1} og 2^{i_2} er lig med rødderne i $Q_1(X)$. Det vides at hvis der er en fejl på plads i, så må 2^i være en rod i $Q_1(X)$ og altså kan eventuelle fejl på r kun forekomme på plads i_1 eller i_2. Altså er fejlene i r nu lokaliseret.

Opgave 4: Bestemmelse af fejlstørrelser

I denne opgave arbejdes videre med bestemmelse af fejlene på ordet r. Det gennemgås hvorledes man kan finde størrelsen af de fejl der eventuelt måtte forekomme på de mulige fejlpositioner i_1 og i_2, der blev bestemt i opgave 3.

1. Det ligningssystem der skal løses for finde fejlstørrelserne er:
$$\begin{aligned} r(2^1) &= e_{i_2} \cdot (2^1)^{i_2} + e_{i_1} \cdot (2^1)^{i_1} \\ r(2^2) &= e_{i_2} \cdot (2^2)^{i_2} + e_{i_1} \cdot (2^2)^{i_1} \end{aligned}$$
Værdierne af i_1, i_2, $r(2^1)$ og $r(2^2)$ blev bestemt i opgave 3. Indsæt disse i ligningssystemet og bestem derved e_{i_1} og e_{i_2}.
2. Da pladserne i_1 og i_2 er de eneste hvorpå der kan forekomme fejl, er alle de øvrige fejlstørrelser (altså e_i med $i \notin \{i_1, i_2\}$) lig med nul. Træk nu fejlstørrelserne fra det modtagne ord, dvs. beregn
$$c' = \Big(r_0 - e_0, r_1 - e_1, r_2 - e_2, r_3 - e_3, r_4 - e_4, r_5 - e_5, r_6 - e_6, r_7 - e_7, r_8 - e_8, r_9 - e_9, r_{10} - e_{10}\Big).$$
Er c' lig med kodeordet c fra opgave 2?

Materiale

De anvendte slides og opgaver kan findes på henholdsvis

www.math.ku.dk/~m00kb/ecc/slides.pdf,
www.math.ku.dk/~m00kb/ecc/opgaver.pdf.