2. BCH-Decodierer

Codierungstheorie
Anton Malevich
15.09.2017

Aufgabe 1

Sei C der binäre 2-fehlerkorrigierende BCH-Code. Die Kontrollmatrix ist gegeben durch

$$\mathbf{H16} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix};$$

über $\mathbb{F}_{16}$ (mit der Regel $\alpha^4 = \alpha + 1$). Das Multiplizieren in $\mathbb{F}_{16}$ wird anhand der Tabelle durchgefuehrt.

```
AlphaPowers = {{1, 0, 0, 0}, {0, 1, 0, 0}, {0, 0, 1, 0}, {0, 0, 0, 1}, {1, 1, 0, 0},
    {0, 1, 1, 0}, {0, 0, 1, 1}, {1, 1, 0, 1}, {1, 0, 1, 0}, {0, 1, 0, 1},
    {1, 1, 1, 0}, {0, 1, 1, 1}, {1, 1, 1, 1}, {1, 0, 1, 1}, {1, 0, 0, 1}};
MapIndexed[α^#2[[1]]-1 ↔ #1 &, AlphaPowers];
TableForm@%
```

$1 \leftrightarrow \{1, 0, 0, 0\}$
$\alpha \leftrightarrow \{0, 1, 0, 0\}$
$\alpha^2 \leftrightarrow \{0, 0, 1, 0\}$
$\alpha^3 \leftrightarrow \{0, 0, 0, 1\}$
$\alpha^4 \leftrightarrow \{1, 1, 0, 0\}$
$\alpha^5 \leftrightarrow \{0, 1, 1, 0\}$
$\alpha^6 \leftrightarrow \{0, 0, 1, 1\}$
$\alpha^7 \leftrightarrow \{1, 1, 0, 1\}$
$\alpha^8 \leftrightarrow \{1, 0, 1, 0\}$
$\alpha^9 \leftrightarrow \{0, 1, 0, 1\}$
$\alpha^{10} \leftrightarrow \{1, 1, 1, 0\}$
$\alpha^{11} \leftrightarrow \{0, 1, 1, 1\}$
$\alpha^{12} \leftrightarrow \{1, 1, 1, 1\}$
$\alpha^{13} \leftrightarrow \{1, 0, 1, 1\}$
$\alpha^{14} \leftrightarrow \{1, 0, 0, 1\}$

Mathematica kann auch anhand dieser Tabelle rechen.

```
<< FiniteFields`
𝔽 = PowerListToField[AlphaPowers];
```

Hier sind Beispiele einiger wichtigen Rechenoperationen.

```
𝔽[{0, 0, 1, 1}] + 𝔽[{1, 0, 1, 0}]
𝔽[{0, 0, 1, 1}] * 𝔽[{1, 0, 1, 0}]
```

$\{1, 0, 0, 1\}_2$

$\{1, 0, 0, 1\}_2$

```
FieldInd[%]
FieldExp[𝔽, 14]
```

```
14
```

```
{1, 0, 0, 1}_2
```

- Überprüfen Sie per Hand, dass $\alpha^6 + \alpha^8 = \alpha^{14} = \alpha^6 * \alpha^8$ in $\mathbb{F}_{16}$ ist.

  Die Kontrollmatrix über $\mathbb{F}_2$ ist

```
H16 /. (MapIndexed[α^#2[[1]]-1 → #1 &, AlphaPowers]);
H2 = Join[%[[1]]^T, %[[2]]^T];
MatrixForm@%
```

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

- Berechnen Sie die Minimaldistanz von C.

  Die Kontrollmatrix über $\mathbb{F}_{16}$ (in der Form, die Mathematica versteht) ist

```
H = (H16 /. {1 → 𝔽[{1, 0, 0, 0}], α → 𝔽[{0, 1, 0, 0}], α^i_ :→ FieldExp[𝔽, i]});
```

  Es sei nun der Vektor

```
y = {0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0};
```

  empfangen worden. Was wurde gesendet?

  Zunächst berechnen wir das Syndrom

```
{S1, S3} = H.y; S2 = S1^2; S4 = S2^2;
S = {S1, S2, S3, S4}
```

```
{{1, 0, 0, 1}_2, {1, 0, 1, 1}_2, {0, 1, 0, 0}_2, {0, 1, 1, 1}_2}
```

  Nun dividieren wir x^4 durch das Syndrompolynom $r_0(x)$ mit Rest

```
r[0, x_] = S.Array[x^# &, 4, 0]
```

```
x^2 {0, 1, 0, 0}_2 + x^3 {0, 1, 1, 1}_2 + {1, 0, 0, 1}_2 + x {1, 0, 1, 1}_2
```

```
{q[1, x_], r[1, x_]} = PolynomialQuotientRemainder[𝔽[{1, 0, 0, 0}] x^4, r[0, x], x]
Exponent[r[1, x], x] < 2
```

```
{{0, 1, 0, 1}_2 + x {1, 1, 0, 0}_2, {1, 0, 1, 0}_2 + x {1, 1, 0, 0}_2 + x^2 {1, 1, 0, 0}_2}
```

```
False
```

```
{q[2, x_], r[2, x_]} = PolynomialQuotientRemainder[r[0, x], r[1, x], x]
Exponent[r[2, x], x] < 2
```

```
{{0, 0, 1, 0}_2 + x {1, 1, 0, 1}_2, {0, 1, 1, 1}_2}
```

```
True
```

  Nun müssen wir $b_2(x)$ finden. $b_k(x)$ ist rekursiv definiert

```
ClearAll[b];
b[-1, x_] = 0;
b[0, x_] = 𝔽[{1, 0, 0, 0}];
b[k_?Positive, x_] := Expand[b[k - 2, x] + q[k, x] b[k - 1, x]]
```

```
b[2, x]
```

$$x\,\{0, 1, 1, 1\}_2 + x^2\,\{0, 1, 1, 1\}_2 + \{1, 1, 1, 1\}_2$$

Nun suchen wir die Nullstellen von $b_2(x)$. Das sind α^7 und α^9.

```
ZerosPositions = Position[Table[b[2, FieldExp[𝔽, i]], {i, 0, 14}], 0, {1}]
```

```
{{8}, {10}}
```

Die Fehlerpositionen finden wir durch Kehrwerte der Nullstellen.

```
FieldInd[FieldExp[𝔽, 1 - #[[1]]] & /@ ZerosPositions;
Pos = Sort[% + 1]
```

```
{7, 9}
```

Das gesendete Codewort ist also

```
f = ReplacePart[Array[0 &, 15], Thread[Pos → 1]]
c = Mod[y - f, 2]
```

```
{0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0}
```

```
{0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0}
```

- Benutzen Sie den BCH-Decodierer um die Wörter {1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0} und {1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0} zu decodieren.
- Programmieren Sie den BCH-Decodierer für den Code C.

Aufgabe 2

Wir betrachten Code den binären [7, 4, 3] Hamming-Code $C = \mathrm{Ham}_2(3)$ als 1-fehlerkorrigierenden BCH-Code. Die Kontrollmatrix ist gegeben durch $H = (\,1 \;\; \alpha \;\; \alpha^2 \;\; \alpha^3 \;\; \alpha^4 \;\; \alpha^5 \;\; \alpha^6\,)$ über $\mathbb{F}_8$ ($\alpha^3 = \alpha + 1$).

- Benutzen Sie den BCH-Decodierer um die Wörter (0 101 010) und (1 010 111) zu decodieren.
- Implementieren Sie den BCH-Decodierer für den Code C.

Aufgabe 3

- Konstruieren Sie den binären 2-fehlerkorrigierenden BCH-Code C mit Länge $n = 31$. Dabei soll die Kontrollmatrix H über $\mathbb{F}_{32}$ (mit der Regel $\alpha^5 = \alpha^2 + 1$) gegeben sein.
- Was ist die Dimension des Codes?
- Implementieren Sie den BCH-Decodierer für den Code C.