G. Nebe, M. Kirschmer

Gitter und Codes, WS 08/09

Lösung 5

Aufgabe 1.

(a) Sei α eine Nullstelle von $f(X)$ (in einem genügend großen Körper, z.B. $\mathbb{F}_8$). Da $f(X)$ irreduzibel ist, hat α Ordnung 7. Damit sind auch α^2 und α^4 Nullstellen von $f(X)$. Damit haben wir alle 3 Nullstellen von $f(X)$ bestimmt. Insbesondere gibt es nur zwei aufeinanderfolgende Nullstellen. Daher ist der designierte Minimalabstand 3.

(b) Aus (a) folgt $d(C) \geq 3$. Weiter ist $(1,1,0,1,0,0,0) \in C$ und hat Gewicht 3. Daher ist $d(C) \leq 3$. Zusammen folgt, daß $d(C) = 3$ gerade der designierte Minimalabstand ist.

(c) Der Minimalabstand ist $d(C) = 3$, die Länge ist $N = 7$. Die Hammingschranke ergibt sich für diese Parameter zu $7 - \log_2(\mathrm{V}_2(7,1)) = 7 - \log_2\left(\binom{7}{0} + \binom{7}{1}\right) = 7 - 3 = 4$. Die Dimension von C ist ebenfalls gleich 4. Die Hammingschranke, die eine obere Schranke für diese Dimension darstellt, wird also angenommen.

Aufgabe 2. Sei $f(X)$ das Erzeugerpolynom eines solchen Codes und $\alpha \neq 1$ eine Nullstelle von $f(X)$. Insbesondere hat α Ordnung 11. Damit sind auch die folgenden Potenzen

$$\alpha, \alpha^3, \alpha^9, \alpha^{27} = \alpha^5, \alpha^{15} = \alpha^4, \alpha^{12} = \alpha$$

Nullstellen von $f(X)$. Der Grad von $f(X)$ ist $11 - 6 = 5$, also haben wir bereits alle Nullstellen von $f(X)$ bestimmt und gezeigt, daß $f(X)$ irreduzibel ist (ohne $f(X)$ zu kennen!). Es gibt insbesondere 3 aufeinanderfolgende Nullstellen. Damit ist der designierte Minimalabstand 4.

Aufgabe 3.

(a) Das zu codierende Wort $x := (0,1,0,0,0,\omega,0,0)$ entspricht dem repräsentierenden Polynom $X^6 + \omega X^2$ (repräsentierend modulo $X^{15} - 1$). Es ist also $(X^6 + \omega X^2) \cdot X^{\deg g}$ mit Rest durch $g(X)$ zu teilen.

Wir erhalten $X^{13} + \omega X^9 = (X^7 + X^6 + \omega^2 X^4 + X^2 + \omega X + \omega) \cdot * + (X^5 + \omega^2 X^3 + \omega^2 X + 1)$, wobei uns $*$ nicht interessiert.

Der Rest ist also $X^5 + \omega^2 X^3 + \omega^2 X + 1$. Dieser entspricht den Kontrollsymbolen $(0,1,0,\omega^2,0,\omega^2,1)$.

Daher wird x zu $(0,1,0,0,0,\omega,0,0,0,1,0,\omega^2,0,\omega^2,1)$ codiert.

(b) Durch Probieren faktorisiert man $g(X)$ in die irreduziblen Faktoren

$$g(X) = (X+\omega)(X^2+X+\omega)(X^2+X+\omega^2)(X^2+\omega^2 X+1)\,.$$

Sei nun α eine primitive 15. Einheitswurzel. Ohne Einschränkung hat α das Minimalpolynom $X^4 + X + 1$. Weiter ist $\alpha^5 \in \{\omega, \omega^2\}$. Indem man eventuell α durch α^8 ersetzt (dies ändert das Minimalpolynom nicht) dürfen wir $\alpha^5 = \omega$ voraussetzen. Mit dieser Identifikation erhalten wir die Nullstellen der einzelnen Faktoren. Es ergibt sich: (Beachte mit x ist stets auch x^4 eine Nullstelle von $g(X)$.)

$f_1(X) := X + w$ hat die Nullstelle $\omega = \alpha^5$.
$f_2(X) := X^2 + X + \omega = X^2 + X + \alpha^5$ hat die Nullstelle α und damit auch α^4.
$f_3(X) := X^2 + X + \omega^2 = \mathrm{Frob}(f_2(X))$ daher die Nullstellen α^2 und α^8.
$f_4(X) := X^2 + \omega^2 X + 1$ hat die Nullstellen α^3 und α^{12}.

Also sind $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ fünf aufeinanderfolgende Nullstellen, welche zu den verschiedenen Polynomen $f_1, \ldots, f_4$ gehören. Damit ist der designierte Minimalabstand 6. (Es ist sogar $d(C) \geq 6$ und das Codewort aus Teil (a) zeigt $d(C) = 6$.)

Es können maximal $\lfloor \frac{6-1}{2} \rfloor = 2$ Fehler korrigiert werden.

(c) Sei $t = 2$; vgl. (b). Das empfangene Wort entspricht dem Polynom

$$r(X) \;:=\; X^{13} + \omega^2 X^{11} + \omega X^9 + \omega X^5 + \omega^2 X^3 + \omega^2 X + 1 \;\in\; \mathbb{F}_4[X]\;.$$

Wir müssen Polynome $\omega(Z) = \sum_{i=0}^{t} \omega_i Z^i$ und $\sigma(Z) = \sum_{i=0}^{t} \sigma_i Z^i$ in $\mathbb{F}_{16}[Z]$ so bestimmen, daß

$$\begin{aligned}
\sigma_0 &= 1\\
\omega_0 &= 0\\
\omega(Z) &\equiv \sigma(Z)\cdot\left(\sum_{i=1}^{2t} r(\alpha^i)Z^i\right) \quad \bmod Z^{2t+1}.
\end{aligned}$$

(Vorsicht! Das Polynom $\omega(X)$ ist nicht zu verwechseln mit dem Element $\omega \in \mathbb{F}_4$.)

Zum Auswerten von $r(X)$ schreiben wir wieder $r(X) = X^{13} + \alpha^{10}X^{11} + \alpha^5 X^9 + \alpha^5 X^5 + \alpha^{10}X^3 + \alpha^{10}X + 1$. Wir erhalten

$$\begin{aligned}
r(\alpha) &= \alpha^{13}\\
r(\alpha^2) &= \alpha\\
r(\alpha^3) &= \alpha^9\\
r(\alpha^4) &= r(\alpha)^4 = \alpha^7\;.
\end{aligned}$$

Aus

$$\omega_2 Z^2 + \omega_1 Z \equiv (\sigma_2 Z^2 + \sigma_1 Z + 1)(r(\alpha^4)Z^4 + r(\alpha^3)Z^3 + r(\alpha^2)Z^2 + r(\alpha)Z) \quad \bmod Z^5$$

folgen per Koeffizientenvergleich die zu erfüllenden Bedingungen

$$\begin{aligned}
\omega_1 &= r(\alpha) && = \alpha^{13}\\
\omega_2 &= \sigma_1 r(\alpha) + r(\alpha^2) && = \alpha^{13}\sigma_1 + \alpha\\
0 &= \sigma_2 r(\alpha) + \sigma_1 r(\alpha^2) + r(\alpha^3) && = \alpha^{13}\sigma_2 + \alpha\sigma_1 + \alpha^9\\
0 &= \sigma_2 r(\alpha^2) + \sigma_1 r(\alpha^3) + r(\alpha^4) && = \alpha\sigma_2 + \alpha^9\sigma_1 + \alpha^7
\end{aligned}$$

Die letzten beiden Bedingungen bilden ein lineares Gleichungssystem in den Unbestimmten σ_1 und σ_2. Dieses besitzt die eindeutige Lösung $(\sigma_1, \sigma_2) = (\alpha^3, \alpha)$. Einsetzen in die ersten beiden Gleichungen liefert $(\omega_1, \omega_2) = (\alpha^{13}, 0)$.

Damit ist $\sigma(Z) = \alpha Z^2 + \alpha^3 Z + 1$ und $\omega(Z) = \alpha^{13}Z$. Die Nullstellen von $\sigma(Z)$ sind α^4 und α^{10} wie man leicht ausprobiert. Es sind also der 4. und 10. Koeffizient des empfangenen Wortes zu korrigieren:

Es ist $\frac{-\omega(\alpha^4)\alpha^{-4}}{\sigma'(\alpha^4)} = \alpha^{10} = \frac{-\omega(\alpha^{10})\alpha^{-10}}{\sigma'(\alpha^{10})}$. Das (wahrscheinlich) gesendete Codewort ist demnach das Wort, welches $r(X) - (\omega^2 X^{15-4} + \omega^2 X^{15-10}) = X^{13} + \omega X^9 + X^5 + \omega^2 X^3 + \omega^2 X + 1$ entspricht. Dieses ist $(0,1,0,0,0,\omega,0,0,0,1,0,\omega^2,0,\omega^2,1)$ und liegt nach Teil (a) im Code.

Aufgabe 4.

(a) Sortieren wor die Codewörter von C nach der Anzahl der auftretenden 0 bzw. 1-Einträge, so ergibt sich:

Codewörter		zugehöriges Monom
$(0,0,0,0,0)$		X_0^5
$(1,0,-1,1,0)$		$X_0^2X_1^2X_{-1}^1$
$(-1,0,1,-1,0)$		$X_0^2X_1X_{-1}^2$
$(0,-1,1,1,1)$,	$(1,1,1,0,-1)$	$X_0X_1^3X_{-1}$
$(-1,1,0,1,-1)$,	$(1,-1,0,-1,1)$	$X_0X_1^2X_{-1}^2$
$(0,1,-1,-1,-1)$,	$(-1,-1,-1,0,1)$	$X_0X_1X_{-1}^3$

Also ist

$$p_C(X_0, X_1, X_{-1}) = X_0^5 + X_0^2X_1^2X_{-1}^1 + X_0^2X_1X_{-1}^2 + 2X_0X_1^3X_{-1} + 2X_0X_1^2X_{-1}^2 + 2X_0X_1X_{-1}^3\;.$$

Ist nun $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel, so erhalten wir mit der MacWilliams-Identität (und einem Computeralgebrasystem):

$$\begin{aligned}
p_{C^\perp}(X_0, X_1, X_{-1}) &= \frac{1}{|C|} p_C(X_0 + X_1 + X_{-1},\ X_0 + \zeta_3 X_1 + \zeta_3^2 X_{-1},\ X_0 + \zeta_3^2 X_1 + \zeta_3 X_{-1}) \\
&= X_0^5 + X_0^3 X_1^2 + X_0^3 X_{-1}^2 + 2X_0^2 X_1^3 + 5X_0^2 X_1^2 X_{-1} + 5X_0^2 X_1 X_{-1}^2 + 2X_0^2 X_{-1}^3 \\
&+ 2X_0 X_1^3 X_{-1} + 2X_0 X_1^2 X_{-1}^2 + 2X_0 X_1 X_{-1}^3 + X_1^4 X_{-1} + X_1^3 X_{-1}^2 + X_1^2 X_{-1}^3 + X_1 X_{-1}^4
\end{aligned}$$

(b) Aus obiger Tabelle oder von p_C liest man $h_C(X,Y) = X^5 + 2X^2Y^3 + 6XY^4$ ab. Mit der MacWilliams-Identität oder aus $p_{C^\perp}$ folgt $h_{C^\perp}(X,Y) = X^5 + 2X^3Y^2 + 14X^2Y^3 + 6XY^4 + 4Y^5$.