Diskrete Mathematik

Frank Bergmann

May 22, 2000

1 Aufgabe 23

1.1 Aufgabenstellung

Bestimmen Sie alle irreduziblen Polynome vom Grade ≤ 4 in $Z_2[x]$.

1.2 Lösung

Nach dem Satz 6.1 der Vorlesung gilt:

> Sei $f(x)$ ein Polynom mit Koeffizienten aus einem Ring mit Einselement. Dann teilt das Polynom $x - s$ genau dann $f(x)$, wenn s Nullstelle von $f(x)$ ist.
>
> Beweis: Wir teilen $f(x)$ durch $x - s$ mit dem Rest:
>
> $$f(x) = m(x)(x - s) + r$$
>
> mit $r \in R$. Durch Einsetzen von s folgt $f(s) = r$. Es teilt also $x - s$ genau dann $f(x)$, wenn $r = f(s) = 0$ ist. Man bemerke: Die Division von $f(x)$ durch $x - s$ ist in jedem Ring mit Einselement möglich, $x - s$ hat 1 als Anfangskoeffizienten.

was bedeutet das nun für diese Aufgabe? Irreduzible Polynome sind im GroSSen und Ganzem die Polynome, die nicht durch die Multiplikation von Polynomen eines geringeren Grades erreicht werden können. Um alle irreduziblen Polynome zu finden, ist es also eine gute Methode erst einmal die Polynome aufzuschreiben, welche reduzibel sind. Die Polynome, die dann übrigbleiben sind dann irreduzibel.

Es stellt sich also die Frage, wie viele Polynome es insgesamt gibt. Für diesen Fall interessieren nur die Polynome vom Grad 1, 2, 3 und 4. Betrachten wir also ein Polynom vom Grad n. Dieses hat die Form:

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

wobei für alle Koeffizienten $a_{n-1,\ldots a_0}$ in $Z_2[x]$ jeweils die Werte 0 und 1 möglich sind. Es gibt also $2^{n=grad(p(x))}$ mögliche Polynome in $Z_2[x]$. Also gibt es für

Polynome vom Grad 1 2 Polynome, für den Grad 2 sind es $2^2 = 4$ Polynome, für den Grad 3 sind es $2^3 = 8$ Polynome. SchlieSSlich ergeben sich für den Grad 4 $2^4 = 16$ mögliche Polynome.

Die folgende Tabelle zeigt diese Polynome:

Grad	Polynome
1	x $x+1$ beide Polynome sind irreduzibel
2	$x \cdot x = x^2$ $x \cdot (x+1) = x^2 + x$ $(x+1) \cdot (x+1) = x^2 + 1$ $\Rightarrow x^2 + x + 1$ ist irreduzibel
3	$x \cdot x^2 = x^3$ $x \cdot \left(x^2+1\right) = (x+1) \cdot \left(x^2+x\right) = x^3 + x$ $x \cdot \left(x^2+x\right) = (x+1) \cdot x^2 = x^3 + x^2$ $x \cdot \left(x^2+x+1\right) = x^3 + x^2 + x$ $(x+1) \cdot \left(x^2+1\right) = x^3 + x^2 + x + 1$ $(x+1) \cdot \left(x^2+x+1\right) = x^3 + 1$ $\Rightarrow x^3 + x^2 + 1$ ist irreduzibel $\Rightarrow x^3 + x + 1$ ist irreduzibel
4	$x \cdot x^3 = x^4$ $x \cdot \left(x^3+1\right) = x^4 + x$ $x \cdot \left(x^3+x\right) = x^4 + x^2$ $x \cdot \left(x^3+x+1\right) = x^4 + x^2 + x$ $x \cdot \left(x^3+x^2\right) = x^2 \cdot \left(x^2+x\right) = x^4 + x^3$ $x \cdot \left(x^3+x^2+1\right) = x^4 + x^3 + x$ $x \cdot \left(x^3+x^2+x\right) = x^4 + x^3 + x^2$ $x \cdot \left(x^3+x^2+x+1\right) = x^4 + x^3 + x^2 + x$ $(x+1) \cdot \left(x^3+1\right) = x^4 + x^3 + x + 1$ $(x+1) \cdot \left(x^3+x+1\right) = x^4 + x^3 + x^2 + 1$ $(x+1) \cdot \left(x^3+x^2+1\right) = x^4 + x^2 + x + 1$ $(x+1) \cdot (x+1) \cdot (x+1) \cdot (x+1) = x^4 + 1$ $\left(x^2+x+1\right) \cdot \left(x^2+x+1\right) = x^4 + x^2 + 1$ $\Rightarrow x^4 + x + 1$ ist irreduzibel $\Rightarrow x^4 + x^3 + 1$ ist irreduzibel $\Rightarrow x^4 + x^3 + x^2 + x + 1$ ist irreduzibel