Hausübung 3

Aufgabe 3.1.2 b)

Lösungidee: Zuerst teilen wird die Multiplikation in mehrere Additionen auf. Hierzu shiften wir jeden Takt Eingang A nach rechts und Eingang B nach links. Nun prüfen wir das lsb von A. Ist diese 1, so addieren wir den aktuellen Wert von B auf unser Zwischenergebnis auf. Haben wir 11 mal geshiftet, so ist die ganze Eingangszahl durchlaufen und unsere Multiplikation ist abgeschlossen. Um die 11 Schritte zu registrieren, nutzen wir einen Counter, der jeden Takt um 1 erhöht wird.

Unsere Modulorechnung gestaltet sich wie folgt: Das Polynom wird solange nach links geshiftet, bist es größer als unser Zwischenergebnis ist. Danach wird es wieder um 1 nach rechts geshiftet, damit es schlussendlich kleiner ist als das Zwischenergebnis. Nun wird es mittels XOR mit unserem Zwischenergebnis verbunden und wird erhalten das Endergbnis.

Durch diese Vorgehensweise bleibt unser Modul synthetisierbar, da wird keine Divison nutzen.

Schwächen: Unsere Implementierung benötigt mehr als 12 Takte. Jedoch ist dafür unsere Latenz sehr gering, da nur wenige Gatter genutzt werden müssen. Hierdurch kann eine hohe Taktfrequenz genutzt werden. Ist das aufmultiplizierte Zwischenergebnis kleiner als das geshiftete Polynom ist, so wird das Polynom nicht weit genug geshiftet. Somit kann das Ergebnis größer sein als das Polynom.