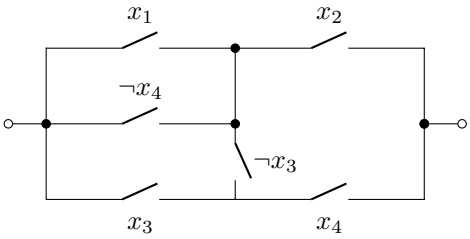
Duale Hochschule Baden-Württemberg

Logik und Algebra

7. Übungsblatt

1. Aufgabe: Es sei $(B, \oplus, \odot, \neg, \mathbb{0}, \mathbb{1})$ eine Boolesche Algebra und $x \in B$ ein beliebiges Element. Zeigen Sie, dass wenn es ein $y \in B$ gibt, mit $x \oplus y = \mathbb{1}$ und $x \odot y = \mathbb{0}$, so ist $y = \neg x$.

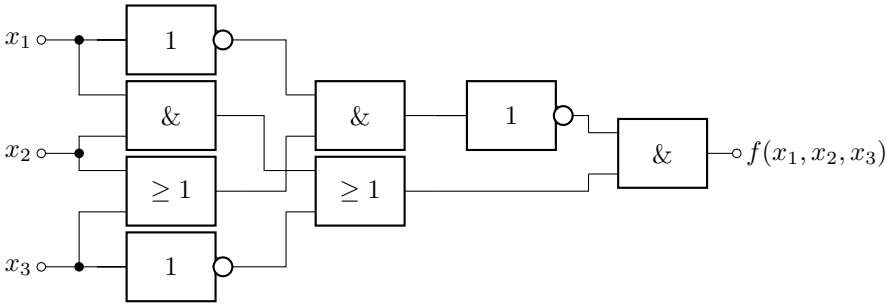
2. Aufgabe: Stellen Sie zu diesem Schaltungsdiagramm mit Brücke (das ist der Schalter $\neg x_3$) ein äquivalentes Schaltungsdiagramm ohne Brücke auf, und bestimmen Sie mit Hilfe eines KV-Diagramms eine Minimalform, dessen Schaltungsdiagramm weniger Schalter benötigt:



3. Aufgabe: Mit einer 7-Segment-Anzeige werden die Zahlen 0-9 so dargestellt:

Die Zahlen werden mit Leitungen b_3, b_2, b_1, b_0 binär als $x = 8b_3 + 4b_2 + 2b_1 + b_0$ übertragen. Bestimmen Sie bei welchen Eingängen das linke untere senkrechte Segment, genannt e, bei den Zahlen $0, 2, 6, 8$ leuchtet. Erstellen Sie das zugehörige KV-Diagramm samt möglichst kleinem Minimalterm und geben Sie die zugehörige Schaltung mit Logikgattern an.

4. Aufgabe: Bestimmen Sie den zugehörigen booleschen Ausdruck für die gegebene Schaltung. Bestimmen Sie mit einem KV-Diagramm eine disjunktive Minimalform und geben Sie dazu eine zugehörige Schaltung mit Logikgattern an.



5. Aufgabe: Vereinfachen Sie den booleschen Ausdruck

$$f(x_1, x_2, x_3, x_3) = (x_2 \vee x_4) \wedge (x_3 \vee \overline{x_4}) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_4}) \wedge (x_1 \vee \overline{x_3} \vee x_4)$$

unter der Nebenbedingung $(x_1 \wedge x_2 \wedge x_3 \wedge \overline{x_4}) \vee (x_2 \wedge x_4) = 0$.

Hinweis: Welche Einträge im KV-Diagramm werden durch die Nebenbedingung frei wählbar?

Lösung 6. Übungsblatt

Lösung 1:

(a) Binärcodes zu $N = 7$ Codebitlänge und $n = 4$ Datenbits zum Generatorpolynom $p(x) = x^3 + x^2 + 1$:

Datenbits	Datenpolynom $q(x)$	Produkt $q(x) \cdot p(x)$	Codebits
$(0,0,0,0)$	0	0	$(0,0,0,0,0,0,0)$
$(0,0,0,1)$	1	$x^3 + x^2 + 1$	$(0,0,0,1,1,0,1)$
$(0,0,1,0)$	x	$x^4 + x^3 + x$	$(0,0,1,1,0,1,0)$
$(0,0,1,1)$	$x + 1$	$x^4 + x^2 + x + 1$	$(0,0,1,0,1,1,1)$
$(0,1,0,0)$	x^2	$x^5 + x^4 + x^2$	$(0,1,1,0,1,0,0)$
$(0,1,0,1)$	$x^2 + 1$	$x^5 + x^4 + x^3 + 1$	$(0,1,1,1,0,0,1)$
$(0,1,1,0)$	$x^2 + x$	$x^5 + x^3 + x^2 + x$	$(0,1,0,1,1,1,0)$
$(0,1,1,1)$	$x^2 + x + 1$	$x^5 + x + 1$	$(0,1,0,0,0,1,1)$
$(1,0,0,0)$	x^3	$x^6 + x^5 + x^3$	$(1,1,0,1,0,0,0)$
$(1,0,0,1)$	$x^3 + 1$	$x^6 + x^5 + x^2 + 1$	$(1,1,0,0,1,0,1)$
$(1,0,1,0)$	$x^3 + x$	$x^6 + x^5 + x^4 + x$	$(1,1,1,0,0,1,0)$
$(1,0,1,1)$	$x^3 + x + 1$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	$(1,1,1,1,1,1,1)$
$(1,1,0,0)$	$x^3 + x^2$	$x^6 + x^4 + x^3 + x^2$	$(1,0,1,1,1,0,0)$
$(1,1,0,1)$	$x^3 + x^2 + 1$	$x^6 + x^4 + 1$	$(1,0,1,0,0,0,1)$
$(1,1,1,0)$	$x^3 + x^2 + x$	$x^6 + x^2 + x$	$(1,0,0,0,1,1,0)$
$(1,1,1,1)$	$x^3 + x^2 + x + 1$	$x^6 + x^3 + x + 1$	$(1,0,0,1,0,1,1)$

(b) Systematisierte Version des Codes:

Datenbits	Codebits
$(0,0,0,0)$	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},0,0,0)$
$(0,0,0,1)$	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},1,0,1)$
$(0,0,1,0)$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},1,1,1)$
$(0,0,1,1)$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},0,1,0)$
$(0,1,0,0)$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},0,1,1)$
$(0,1,0,1)$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},1,1,0)$
$(0,1,1,0)$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0},1,0,0)$
$(0,1,1,1)$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},0,0,1)$

Datenbits	Codebits
$(1,0,0,0)$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},1,1,0)$
$(1,0,0,1)$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},0,1,1)$
$(1,0,1,0)$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},0,0,1)$
$(1,0,1,1)$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},1,0,0)$
$(1,1,0,0)$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},1,0,1)$
$(1,1,0,1)$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},0,0,0)$
$(1,1,1,0)$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},0,1,0)$
$(1,1,1,1)$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},1,1,1)$

Lösung 2: Empfangene Daten, korrigierte Codewörter, Datenbits und Ergebnis:

Empfangene Daten		Korrigierte Codewörter		Daten		Dezimal	Ascii
$(0,0,0,1,1,0,1)$	$(0,0,0,1,1,1,0)$	$(0,0,\mathbf{1},1,1,0,1)$	$(\mathbf{1},0,0,1,1,1,0)$	$(0,0,1,1)$	$(1,0,1,0)$	58	:
$(0,0,1,1,1,1,0)$	$(1,1,0,1,1,1,1)$	$(0,0,1,\mathbf{0},1,1,0)$	$(1,1,\mathbf{1},1,1,1,1)$	$(0,0,1,0)$	$(1,1,0,1)$	45	−
$(1,0,1,0,1,1,0)$	$(1,0,1,1,0,1,1)$	$(\mathbf{0},0,1,0,1,1,0)$	$(1,0,1,\mathbf{0},0,1,1)$	$(0,0,1,0)$	$(1,0,0,1)$	41	)

Die Nachricht lautet :-) .

Lösung 3:

	Alice	Bob
1.	Sende öffentlich $p = 17$, $\alpha = 3$	
2.	Geheime Zufallszahl $a = 3$	Geheime Zufallszahl $b = 4$
	Berechne $\alpha^a = 3^3 \equiv 10 \mod 17$	Berechne $\alpha^b = 3^4 \equiv 13 \mod 17$
	Sende öffentlich 10	Sende öffentlich 13
3.	Berechne $(\alpha^b)^a = 13^3 \equiv 4 \mod 17$	Berechne $(\alpha^a)^b = 10^4 \equiv 4 \mod 17$
4.	Verwende 4 als temporären Schlüssel	

Lösung 4:

(a) Durchführung des euklidischen Algorithmus für 88 und 9:

k	a_k	r_k	u_k	v_k
0	88		1	0
1	9	$\lfloor \frac{88}{9} \rfloor = 9$	0	1
2	$88 - 9 \cdot 9 = 7$	$\lfloor \frac{9}{7} \rfloor = 1$	$1 - 9 \cdot 0 = 1$	$0 - 9 \cdot 1 = -9$
3	$9 - 1 \cdot 7 = 2$	$\lfloor \frac{7}{2} \rfloor = 3$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-9) = 10$
4	$7 - 3 \cdot 2 = 1$		$1 - 3 \cdot (-1) = 4$	$-9 - 3 \cdot 10 = -39$

(b) Die Zahl 115 hat die zwei Primfaktoren $115 = 5 \cdot 23$ (erraten oder mit Faktorisierung von 88 probieren und Addition von 1 zu Faktoren). Mit $p = 5$, $q = 23$ ist $(p-1) \cdot (q-1) = 4 \cdot 22 = 88$. Mit $\mathrm{ggT}((p-1)(q-1), 9) = \mathrm{ggT}(88, 9) = 1$ ist 9 ein zulässiger Exponent für das RSA-Verfahren und mit $1 = 4 \cdot 88 - 39 \cdot 9$ und $88 - 39 = 49$ ist $9 \cdot 49 = 441 \equiv 1 \mod 88$. Damit ist $(49, 115)$ der zugehörige private Schlüssel.

(c) Mit $m = 2$ ist $m^e = 2^9 = 512 \equiv 52 \mod 115$. Test (nicht gefragt):

$$52^{49} = 1213846689193589070140233234890629087757157219333010658528341529201325969042950848512 \equiv 2 \mod 115$$

Lösung 5:

(a)

k	a_k	r_k	u_k	v_k
0	220		1	0
1	17	$\lfloor \frac{220}{17} \rfloor = 12$	0	1
2	$220 - 12 \cdot 17 = 16$	$\lfloor \frac{17}{16} \rfloor = 1$	$1 - 12 \cdot 0 = 1$	$0 - 12 \cdot 1 = -12$
3	$17 - 1 \cdot 16 = 1$		$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-12) = 13$

(b) Es ist $253 = 23 \cdot 11$ und mit $p = 23$, $q = 11$ ist $(p-1) \cdot (q-1) = 22 \cdot 10 = 220$. Da $\mathrm{ggT}(220, 17) = 1$ ist 17 ein zulässiger Exponent für das RSA-Verfahren. Da $1 = -220 + 13 \cdot 17$ ist $(13, 253)$ der zugehörige private Schlüssel.

(c) Das Kodieren von $m = 2$ mit dem privaten Schlüssel ergibt $s = m^{13} = 8192 \equiv 96$. Das unterschiebene Dokument ist dann $(m, s) = (2, 96)$. Empfänger berechnen $s^{17} = m^{13 \cdot 17} \equiv m^1 \mod 253$ und vergleichen das Ergebnis mit dem Dokument. Nur wer im Besitz des privaten Schlüssels ist, kann eine solche Signatur erzeugen. Einzige offene Frage verbleibt, ob der öffentliche Schlüssel der richtige ist...

$$s^{17} = 96^{17} = 4995868076798137881795553463894016 \equiv 2 \mod 253$$