

Bemerkung zur 5. Übung

Robert Görke

February 6, 2006

Lemma 5.12

In einem der letzten Teilschritte des Beweises von Lemma 5.12 ist mir in der Übung ein Fehler unterlaufen, und ich hatte nicht die Übersicht ihn zu erkennen. Es gibt dazu eigentlich nicht viel zu erklären, da es ein banaler Flüchtigkeitsfehler war, hier jedoch der Vollständigkeit halber eine Berichtigung:

Falls gilt $\langle C_k, S_{k-1,j} \rangle = 1$, so passiert im Algorithmus $S_{k,j} = S_{k-1,j} \oplus S_{k,k}$ (Hier ist schon der Fehler, ich schrieb an die Tafel, dass gelte: $\langle C_k, S_{k,j} \rangle = 1$). Der Zeuge S_j wird zum aktuellen Kreis orthogonalisiert. Nun funktioniert auch der Beweis wie im Vorlesungsmitschrieb bestens:

Die Orthogonalisierung zu C_k funktioniert:

$$\langle C_k, S_{k,j} \rangle = \underbrace{\langle C_k, S_{k-1,j} \rangle}_{=1 \text{ (hier lag das Problem, s.o.)}} + \underbrace{\langle C_k, S_{k,k} \rangle}_{=1 \text{ (nach Konstruktion)}} = 1 + 1 =_{\text{GF}(2)} 0$$