Korrektur zur 8. Übung

Aufgabe 32 b) *die Zweite*

Zuerst ist zu bemerken, daß der Schlüssel k für den gesamten Sondierungsvorgang gleich bleibt. Daher braucht man statt der Hash–Funktion $h(k,i) = (h'(k) + \frac{1}{2}i + \frac{1}{2}i^2) \bmod m$ nur die Funktion

$$\tilde{h}(i) = \left(\frac{1}{2}i + \frac{1}{2}i^2\right) \bmod m$$

zu betrachten. Es wird nun gezeigt, daß für je zwei verschiedene Urbilder i und j auch die Bilder $\tilde{h}(i)$ und $\tilde{h}(j)$ verschieden sind. Da Definitionsmenge und Zielmenge gleichmächtig und endlich sind, ist damit $\tilde{h}$ automatisch surjektiv, was der Aufgabenstellung entspricht. Seien nun i und j beliebig aber fest gewählt mit

$$0 \leq i < j \leq m - 1 \tag{1}$$

Es ist zu zeigen: $\tilde{h}(i) \neq \tilde{h}(j)$.

Beweis durch Widerspruch

Angenommen es sei $\tilde{h}(i) = \tilde{h}(j)$. Dann gilt nach Definition der Restbildung:

$$\frac{1}{2}j + \frac{1}{2}j^2 - \frac{1}{2}i - \frac{1}{2}i^2 = am \qquad \text{mit} \quad a \in N_0$$

oder auch äquivalent:

$$\underbrace{(i + j + 1)}_{A}\underbrace{(j - i)}_{B} = j + j^2 - i - i^2 = 2am = a\,\underbrace{2^{p+1}}_{C} \tag{2}$$

1. Hauptfall: $a = 0$

Dann muß gelten $AB = 0$. Im Unterfall, daß $B = 0$, folgt $i = j$ im Widerspruch zu (1)! Im Unterfall, daß $A = 0$, folgt entweder $i < 0$ oder $j < 0$ im Widerspruch zu (1)!

2. Hauptfall: $a \neq 0$

Die Gleichung (2) ist nun gleichbedeutend damit, daß der Term C das Produkt AB teilt. Da C gerade ist, muß mindestens einer der beiden Terme A oder B ebenfalls gerade sein.

1. Unterfall: B ist gerade. Daraus folgt für i und j, daß entweder beide gerade oder beide ungerade sind. Damit ist aber A auf jeden Fall ungerade und kann keine gemeinsamen Teiler mit C haben! Somit muß C vollständig den Term B teilen. Für B gilt jedoch wegen (1):

$$0 < B < 2^p$$

C kann keine Zahl teilen, die kleiner als C ist. Widerspruch!

2. Unterfall: A ist gerade. Daraus folgt für i und j, daß einer der beiden gerade und der andere ungerade ist. Damit ist aber B auf jeden Fall ungerade! Somit muß (analog zu oben) C den Term A teilen. Für A gilt jedoch wegen (1):

$$0 < A < 2^{p+1}$$

Also kann C den Term A nicht teilen. Damit kann C das Produkt AB nicht teilen. Widerspruch! $\square$