How to not protect a webpage

Skrupellos
JID: skrupellos@swissjabber.de

19. August 2010

Dies ist das Handout zur Präsentation "How to not protect a webpage". Es zeigt sehr ausführlich die einzelnen Schritte des Kapitels "Hash, Umkehrung" der Präsentation. Die Nummern der Rechnungen aus diesem Handout stimmen mit denen der Präsentation überein.

1 Die Ausganssitualtion

$$h(a) = \sum_{n=0}^{7} a_n 3^n \tag{1}$$

2 a_i isolieren

Um genauere aussagen über ein a_i treffen zu können, muss es aus der Summe herausgelöst werden. Dazu kann die Summe an der stelle i in eine Addition aus einer Summe der oberen Elemente in a bis a_{i+1}, a_i selbst und eine Summe der restlichen Elemente in a ab a_{i-1} augeteilt werden.

$$h(a) = \sum_{n=i}^{7} a_n 3^n + \sum_{n=0}^{i-1} a_n 3^n \tag{2}$$

$$h(a) = \sum_{n=i+1}^{7} a_n 3^n + \sum_{n=i}^{i} a_n 3^n + \sum_{n=0}^{i-1} a_n 3^n \tag{3}$$

$$h(a) = \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \sum_{n=0}^{i-1} a_n 3^n \tag{4}$$

3 Ober- und Untergrenze

$$h(a) \geq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \sum_{n=0}^{i-1} 1 \cdot 3^n \tag{5}$$

$$\wedge h(a) \leq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \sum_{n=0}^{i-1} 26 \cdot 3^n \tag{6}$$

4 Summe auflösen

Eine Summe der Form $\sum_{n=0}^{t} c^n$ kann durch $\frac{c^{t+1}-1}{c-1}$ ersetzt werden[1]. Dies erleichter das Rechnen, da die Folge aufgelöst ist.

$$h(a) \geq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + 1 \cdot \sum_{n=0}^{i-1} 3^n \tag{7}$$

$$\wedge h(a) \leq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + 26 \cdot \sum_{n=0}^{i-1} 3^n \tag{8}$$

$$h(a) \geq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + 1 \cdot \frac{3^{i-1+1} - 1}{3 - 1} \tag{9}$$

$$\wedge h(a) \leq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + 26 \cdot \frac{3^{i-1+1} - 1}{3 - 1} \tag{10}$$

$$h(a) \geq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \frac{3^{i-1+1} - 1}{3 - 1} \cdot 1 \tag{11}$$

$$\wedge h(a) \leq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \frac{3^{i-1+1} - 1}{3 - 1} \cdot 26 \tag{12}$$

$$h(a) \geq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \frac{3^{i} - 1}{3 - 1} \cdot 1 \tag{13}$$

$$\wedge h(a) \leq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \frac{3^{i} - 1}{3 - 1} \cdot 26 \tag{14}$$

[1] http://de.wikipedia.org/wiki/Geometrische_Reihe#Herleitung_der_Formel_f.C3.BCr_die_Partialsummen

$$h(a) \geq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \frac{3^i - 1}{2} \cdot 1 \tag{15}$$

$$\wedge h(a) \leq \sum_{n=i+1}^{7} a_n 3^n + a_i 3^i + \frac{3^i - 1}{2} \cdot 26 \tag{16}$$

5 Nach a_i auflösen

Um nun Informationen über jedes a_i zu bekommen, muss das Ungleichungssystem nach a_i aufgelöst werden.

$$h(a) - a_i 3^i \geq \sum_{n=i+1}^{7} a_n 3^n + \frac{3^i - 1}{2} \cdot 1 \tag{17}$$

$$\wedge h(a) - a_i 3^i \leq \sum_{n=i+1}^{7} a_n 3^n + \frac{3^i - 1}{2} \cdot 26 \tag{18}$$

$$- a_i 3^i \geq -h(a) + \sum_{n=i+1}^{7} a_n 3^n + \frac{3^i - 1}{2} \cdot 1 \tag{19}$$

$$\wedge - a_i 3^i \leq -h(a) + \sum_{n=i+1}^{7} a_n 3^n + \frac{3^i - 1}{2} \cdot 26 \tag{20}$$

$$a_i 3^i \leq h(a) - \sum_{n=i+1}^{7} a_n 3^n - \frac{3^i - 1}{2} \cdot 1 \tag{21}$$

$$\wedge a_i 3^i \geq h(a) - \sum_{n=i+1}^{7} a_n 3^n - \frac{3^i - 1}{2} \cdot 26 \tag{22}$$

$$a_i \leq \frac{h(a) - \sum_{n=i+1}^{7} a_n 3^n - \frac{3^i - 1}{2} \cdot 1}{3^i} \tag{23}$$

$$\wedge a_i \geq \frac{h(a) - \sum_{n=i+1}^{7} a_n 3^n - \frac{3^i - 1}{2} \cdot 26}{3^i} \tag{24}$$

6 Vereinfachen

Das ganze kann jetzt noch weiter vereinfacht werden.

6.1 Aufteilen

$$a_i \leq \frac{h(a)}{3^i} - \frac{\sum_{n=i+1}^{7} a_n 3^n}{3^i} - \frac{\frac{3^i-1}{2} \cdot 1}{3^i} \tag{25}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{\sum_{n=i+1}^{7} a_n 3^n}{3^i} - \frac{\frac{3^i-1}{2} \cdot 26}{3^i} \tag{26}$$

$$a_i \leq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 1}{3^i} - \frac{\sum_{n=i+1}^{7} a_n 3^n}{3^i} \tag{27}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 26}{3^i} - \frac{\sum_{n=i+1}^{7} a_n 3^n}{3^i} \tag{28}$$

6.2 Driter Summand

$$a_i \leq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 1}{3^i} - \frac{1}{3^i} \cdot \sum_{n=i+1}^{7} a_n 3^n \tag{29}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 26}{3^i} - \frac{1}{3^i} \cdot \sum_{n=i+1}^{7} a_n 3^n \tag{30}$$

$$a_i \leq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 1}{3^i} - \sum_{n=i+1}^{7} a_n 3^n \cdot \frac{1}{3^i} \tag{31}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 26}{3^i} - \sum_{n=i+1}^{7} a_n 3^n \cdot \frac{1}{3^i} \tag{32}$$

$$a_i \leq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 1}{3^i} - \sum_{n=i+1}^{7} a_n \cdot \frac{3^n}{3^i} \tag{33}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 26}{3^i} - \sum_{n=i+1}^{7} a_n \cdot \frac{3^n}{3^i} \tag{34}$$

$$a_i \leq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 1}{3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{35}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{\frac{3^i-1}{2} \cdot 26}{3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{36}$$

6.3 Zweiter Summand

$$a_i \leq \frac{h(a)}{3^i} - \frac{(3^i-1) \cdot 1}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{37}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} - \frac{(3^i-1) \cdot 26}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{38}$$

$$a_i \leq \frac{h(a)}{3^i} + \frac{(1-3^i) \cdot 1}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{39}$$

$$\wedge a_i \geq \frac{h(a)}{3^i} + \frac{(1-3^i) \cdot 26}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{40}$$

6.4 Erster Summand

$$a_i \leq \frac{2 \cdot h(a)}{2 \cdot 3^i} + \frac{(1-3^i) \cdot 1}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{41}$$

$$\wedge a_i \geq \frac{2 \cdot h(a)}{2 \cdot 3^i} + \frac{(1-3^i) \cdot 26}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{42}$$

6.5 Zusammenführen

$$a_i \leq \frac{2 \cdot h(a) + (1-3^i) \cdot 1}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{43}$$

$$\wedge a_i \geq \frac{2 \cdot h(a) + (1-3^i) \cdot 26}{2 \cdot 3^i} - \sum_{n=i+1}^{7} a_n 3^{n-i} \tag{44}$$