ETH zürich
Departement Informatik

Algorithmik für schwere Probleme

Prof. Dr. Dennis Komm
Dr. Hans-Joachim Böckenhauer
https://courses.ite.inf.ethz.ch/schwere_prob_23/

Lösungsvorschläge – Blatt 12

Zürich, 23. Mai 2023

Lösung zu Aufgabe 14

Sei C_{rand} eine (Multi-)Menge von s Wörtern in Σ_2^n, die gleichverteilt und unabhängig voneinander zufällig gewählt wurden. Wir zeigen, dass C_{rand} mit positiver Wahrscheinlichkeit ein Covering Code von Σ_2^n ist. Sei $w \in \Sigma_2^n$ und $c \in C_{\text{rand}}$. Dann ist

$$\text{Prob}[w \in \text{HBall}_r(c)] = \frac{\text{vol}_2(r,n)}{|\Sigma_2^n|} .$$

Es ist also

$$\begin{aligned}
\text{Prob}\Big[w \notin \bigcup_{c \in C_{\text{rand}}} \text{HBall}_r(c)\Big] &= \left(1 - \frac{\text{vol}_2(r,n)}{|\Sigma_2^n|}\right)^s \\
&< e^{-s \cdot \text{vol}_2(r,n)/2^n} \\
&= e^{-n \cdot \ln(2)} \\
&= 2^{-n} ,
\end{aligned}$$

wobei wir ausnutzen, dass $1 - x < e^{-x}$ für $x > 0$. Jetzt können wir die Wahrscheinlichkeit abschätzen, dass *irgendein* Wort $w \in \Sigma_2^n$ nicht in einer solchen Menge $\text{HBall}_r(c)$ enthalten ist:

$$\begin{aligned}
\text{Prob}\Big[\bigcup_{w \in \Sigma_2^n} \Big\{w \notin \bigcup_{c \in C_{\text{rand}}} \text{HBall}_r(c)\Big\}\Big] &\leq \sum_{w \in \Sigma_2^n} \text{Prob}\Big[w \notin \bigcup_{c \in C_{\text{rand}}} \text{HBall}_r(c)\Big] \\
&< 2^n \cdot 2^{-n} \\
&= 1 .
\end{aligned}$$

Das heisst, es muss eine Wahl von C_{rand} geben, die tatsächlich ein Covering Code ist.