Problem Set 6

Jaan Tollander de Balsch

March 1, 2020

For the theory, we refer to Papadimitriou (1994).

H6.1

We define the cumulative polynomial-time hierarchy as follows.

$$\Sigma_0^p = \mathbf{P}, \quad \Sigma_{k+1}^p = \mathbf{NP}^{\Sigma_k^p}, \quad \mathbf{PH} = \bigcup_{k \geq 0} \Sigma_k^p.$$

Let us prove that

$$\mathbf{PH} \subseteq \mathbf{PSPACE}.$$

We will use induction to prove that $\Sigma_k^p \subseteq \mathbf{PSPACE}$ for all $k \geq 0$.

Base step: Let prove that statement holds for $k = 0$.

$$\Sigma_0^p = \mathbf{P} \subseteq \mathbf{PSPACE}.$$

Inductive step: Assuming that the statement holds for k, we have

$$\Sigma_k^p \subseteq \mathbf{PSPACE}.$$

Then the statement for $k+1$ is

$$\Sigma_{k+1}^p = \mathbf{NP}^{\Sigma_k^p} \subseteq \mathbf{NPSPACE} = \mathbf{PSPACE}$$

By *Savitch's theorem*, deterministic and non-deterministic polynomial spaces are equivalent.

H6.2

For this exercise, we refer to the paper by Mc Loughlin (1984).

A binary linear code of length n:

- *Parity check matrix* $H \in \{0,1\}^{m \times n}$.
- *Codeword* $y \in \{0,1\}^n$ which satisfies $Hy = 0 \mod 2$.
- *Covering radius*

$$\rho_H = \max_{x \in \{0,1\}^n} \min_{y \in C_H} d(x,y)$$

  where d is Hamming distance and C_H is the set of all code words.

We define the problem COVERING RADIUS as:

INSTANCE: A parity check matrix $H \in \{0,1\}^{m \times n}$ and an integer r.

QUESTION: Is the covering radius of the code defined by H at most r?

We define the language COVERING RADIUS.

$$L = \{H; r \mid H \in \{0,1\}^{m \times n} \text{ such that } \rho_H \leq r\}$$

That is, L contains all strings $H; r$ where H is a parity check matrix with a covering radius of at most r.

The language L is in Π_2^p iff there is a relation $R \subseteq (\Sigma^*)^3$ such that

$$L = \{z \mid \forall x \exists y, (x,y,z) \in R\},$$

and whenever $(x,y,z) \in R$ then $|x|, |y| \leq |z|^t$ for some t.

We can write the COVERING RADIUS question in the form, $\forall x \exists y$ such that $d(x,y) \leq r$, where x and y are binary vectors and $Hy = 0$ holds.

If we represent x and y as strings and set string $z = H; r$, then, have $|x|, |y| \leq |z|^t$ for some t whenever $(x,y,z) \in R$.

H6.3

References

Mc Loughlin, A.M., 1984. The Complexity of Computing the Covering Radius of a Code. *IEEE Transactions on Information Theory*, 30(6), pp.800–804.

Papadimitriou, C.H., 1994. *Computational complexity.* Addison-Wesley.pp.I–XV, 1–523.