22.4.01 Amos Beimel

Topics in the Frontiers of Computer Science – Exercise 2

Deadline: 6.5.01

Exercise 1

Let $\vec{v}, \vec{v'}$ be two non-zero vectors over some field $\mathcal{F}$. Prove that for every span program $(M, \rho, \vec{v})$ over $\mathcal{F}$ there is a span program of equal size $(M', \rho, \vec{v'})$ accepting the same access structure.

Exercise 2

Let $n = \binom{m}{2}$ and consider a complete undirected graph with m vertices denoted $\{v_1, \ldots, v_m\}$ and n edges. Define the access structure CON whose participants are the edges, and a set of edges is in the access structure if it contains a path from v_1 to v_m. Prove that CON has a span program of size n over every field $\mathcal{F}$.

Exercise 3

Let $L_1, \ldots, L_m$ be m subsets of $\{0, \ldots, m-1\}$ such that the intersection of every two subsets is of size at most one. Define the access structure $LINES$, which has $n = 2m$ participants denoted $\{a_1, \ldots, a_m, b_1, \ldots, b_m\}$, and whose minimal sets are $\{\{a_i, b_j\} : j \in L_i\}$.

1. Prove that for every field $\mathcal{F}$, every monotone span program over $\mathcal{F}$ has size at least $\sum_{i=1}^{m} |L_i|$.
2. Let p be a prime number and $m = p^2$. For every $(a, b) \in \mathcal{Z}_p \times \mathcal{Z}_p$ define
$$L_{(a,b)} = \{(x, y) \in \mathcal{Z}_p \times \mathcal{Z}_p : y \equiv ax + b \pmod{p}\}.$$
Prove that for every $a_1, b_1, a_2, b_2 \in \mathcal{Z}_p$ such that either $a_1 \neq a_2$ or $b_1 \neq b_2$ (or both)
$$\left| L_{(a_1,b_1)} \cap L_{(a_2,b_2)} \right| \leq 1.$$
3. Identify each pair $(x, y) \in \mathcal{Z}_p \times \mathcal{Z}_p$ with the number $xp + y \in \{0, \ldots, m-1\}$, and similarly for every pair $(a, b) \in \mathcal{Z}_p \times \mathcal{Z}_p$. What is the lower bound for the access structure $LINES$ defied with the sets $L_{(a,b)}$?