University of the Saarland
Department 6.2 - Informatik
Prof. Dr. W.J. Paul

Computer Architecture III - WS 03

(due: 12/19/2003)

Excercise 1: (Probability) **(2 + 1 + 2 points)**

1. Prove that for two predicates a and a with $a \implies b$ holds:

$$p(b) \geq p(a)$$

2. Let A and B be events. Show:

$$A \subset B \text{ implies } p(A) \leq p(B)$$

3. Let for $i \in \{0, \ldots, n-1\}$ (Ω_i, pr_i) be n discrete probability spaces. Let (Ω, pr) be defined as $\Omega = \Omega_0 \times \ldots \times \Omega_{n-1}$ and for $\omega_i \in \Omega_i$: $pr(\omega_0, \ldots, \omega_{n-1}) = pr_0(\omega_0) \cdot \ldots \cdot pr_{n-1}(\omega_{n-1})$. Show that for $A_i \subseteq \Omega_i$ it holds: $pr(A_0 \times \ldots \times A_{n-1}) = pr_0(A_0) \cdot \ldots \cdot pr_{n-1}(A_{n-1})$.

Excercise 2: (Random Number Generators) **(2 points)**

Prove that there cannot exist a DLX program[1] that outputs random bit strings.

Excercise 3: (Butterfly Networks) **(3 points)**

Prove: In a r dimensional butterfly network $B(r)$ there exists exactly one path from an input i to output j which has length r.

Excercise 4: (Probability II) **(2 + 1 points)**

Let Ω^n be the n-times cross product of Ω. Let for $A_i \subseteq \Omega$ A_i' be defined as $A_i' = \Omega^i \times A_i \times \Omega^{n-i-1}$.

1. Show that the A_i' are mutually independant.

2. Where exactly was the property from part 1. used in the proof of lemma 2?

[1] We don't treat hardware number generators which are actually possible, e.g. circuits exploiting quantum physical effects.