Advanced Logics
Winter term 2015

Institut für Theoretische Informatik
Leibniz Universität Hannover

Solution to exercise sheet 6

Exercise 1: Prove that

$$\mathrm{AG}\phi \in \mathrm{CTL}(\{\mathrm{EU}\}, \mathsf{N}),$$

where $\phi \in \mathrm{CTL}(\{\mathrm{EU}\}, \mathsf{N})$ via equivalent transformations (according to the semantics) of $\neg(\neg\psi \mathrm{EU} \neg\phi)$.

Solution:

$$M, s \models \phi \mathrm{EU} \psi \text{ iff } \exists \pi = (\underbrace{s_0}_{=s}, s_1, \dots) \exists i \geq 0 \quad \forall 1 \leq j < i : M, s_j \models \phi \text{ and } M, s_i \models \psi$$

$$M, s \models \neg(\phi \mathrm{EU} \psi) \text{ iff } \forall \pi = (\underbrace{s_0}_{=s}, s_1, \dots) \forall i \geq 0 \quad \exists 1 \leq j < i : M, s_j \not\models \phi \text{ or } M, s_i \not\models \psi$$

$$M, s \models \neg(\neg\phi \mathrm{EU} \neg\psi) \text{ iff } \forall \pi = (\underbrace{s_0}_{=s}, s_1, \dots) \forall i \geq 0 \quad \exists 1 \leq j < i : \underbrace{M, s_j \models \phi}_{\equiv((\mathrm{EF}\neg\psi)\mathrm{AU}\phi)} \text{ or } \underbrace{M, s_i \models \psi}_{\equiv \mathrm{AG}\psi}$$

$$\text{iff } M, s \models ((\mathrm{EF}\neg\psi)\mathrm{AU}\phi) \vee \mathrm{AG}\psi$$

Hence $\neg(\top \mathrm{EU} \neg\phi) \equiv \mathrm{AG}\phi$. Observe that these transformations are valid as it holds $\mathrm{AG}\phi \equiv \neg\mathrm{EF}\neg\phi \equiv \neg(\top \mathrm{EU} \neg\phi)$. □

Exercise 2: An AC^0-circuit has constant depth and may use $\wedge$- and $\vee$-gates of unbounded fan-in. A *circuit family* is a sequence $\mathcal{C} = (C_n)_{n \in \mathbb{N}}$ where C_n is a circuit with n inputs. The function computed by $\mathcal{C}$ is given by $f_{\mathcal{C}}(w) = f_{C_{|W|}}(w)$ and $f_{\mathcal{C}} \colon \{0,1\}^* \to \{0,1\}^*$. A TC^0-circuit is an AC^0-circuit which additionally may use gates for the majority function MAJ. A $\leq_{\mathbf{cd}}$-reduction is computable via an AC^0-circuit family. The language $\mathrm{MAJ} =_{\mathsf{def}} \{w \in \{0,1\}^\star \mid |w|_1 \geq |w|_0\}$ is TC^0-complete w.r.t. $\leq_{\mathbf{cd}}$-reductions.
An oracle gate for

- BCOUNT with n inputs outputs the number of of 1s in binary.
- LEQ gets two binary numbers as input and outputs true iff the first bit string is less than or equal to the second one.
- SUB gets two binary numbers a, b as input and outputs $\max\{0, a - b\}$.

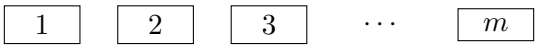
It is known that $\mathsf{LEQ}, \mathsf{SUB} \in \mathsf{AC}^0$ and $\mathsf{BCOUNT} \in \mathsf{TC}^0$.
Let T be a set of CTL-operators and let B be a finite set of Boolean functions.
Now prove the following:

1. Given a formula $\phi \in \mathrm{CTL}(T, B)$ then there exists a TC^0-circuit family C with oracle gates from LEQ, BCOUNT and SUB which verifies the syntactical correctness of the given formula. The main part of the circuit will then check if the opening and closing brackets are consistent. Hence this shows that $\mathrm{CTL}(T, B) \leq_{\mathbf{cd}} \mathrm{MAJ}$.

2. It also holds $\mathrm{MAJ} \leq_{\mathbf{cd}} \mathrm{CTL}(T, B)$.

Together these two items imply $\mathrm{CTL}(T, B)$ is TC^0-complete w.r.t. $\leq_{\mathbf{cd}}$ reductions.

Solution: (1) Fix a finite set of atomic propositions PROP and a set B' of used Boolean connectives. At first we need to consider the binary representation of formulas. As there are only constant many different symbols we can use a block encoding scheme.



Each block corresponds with its pattern to a symbol of a given formula $\phi \in \mathrm{CTL}(T, B)$. The simple part requires the detection of trivial errors, e.g., two propositions occurring at position i and $i+1$ without connective in between, or the repetition of two $\wedge$ symbols. This kind of errors can be spotted with constant depth.
Now turn towards the consistent use of brackets. Here we will build a circuit of depth 2 below each such block. Each of these blocks has two out-gates: o_i and c_i s.t. $o_i = 1$ iff block i encodes '(' and $c_i = 1$ iff block i encodes ')'.

Depending on these gates, o_i and c_i, we can use BCOUNTgates to count opening and closing brackets. With SUBgates we can compute how many opening, resp., closing brackets have to be closed, resp., opened. If for every prefix of the input enough closing brackets are available, and if for every suffix enough opening brackets are there, then we can conclude that the input is consistently bracketed.
Finally we can define this kind of test with a circuit of depth 4 as follows (m is the number of blocks):

$$\bigwedge_{i=1}^{m} \mathsf{LEQ}\Big(\mathsf{SUB}(\mathsf{BCOUNT}(o_1, \ldots, o_i), \mathsf{BCOUNT}(c_1, \ldots, c_i)), \mathsf{BCOUNT}(c_i, \ldots, c_m)\Big) \wedge$$
$$\bigwedge_{i=1}^{m} \mathsf{LEQ}\Big(\mathsf{SUB}(\mathsf{BCOUNT}(c_m, \ldots, c_i), \mathsf{BCOUNT}(o_m, \ldots, o_i)), \mathsf{BCOUNT}(o_1, \ldots, o_i)\Big).$$

(2) Given $w \in \{0,1\}^n$ then it holds $|w|_1 \geq |w|_0$ iff there is a k s.t. $0 \leq k \leq n$: $|w|_1 = |w0^k|_0$. Hence, $w \in \mathrm{MAJ}$ iff $\bigvee_{0 \leq k \leq n} |1^n w 0^{n+k}|_1 = |1^n w 0^{n+k}|_0$ is satisfiable. More, if $w \in \mathrm{MAJ}$ then it holds $|u|_1 \geq |u|_0$ for every prefix u of $1^n w 0^{n+k}$ s.t. $k = |w|_1 - |w|_0$. For ℓ which satisfy $|1^n w 0^{n+\ell}|_1 = |1^n w 0^{n+\ell}|_0$ the expression $1^n w 0^{n+\ell}$ can hence be seen as a balanced bracketed.
Let $p \in \mathsf{PROP}$ and $\otimes$ be a binary projection $x_1 \otimes x_2 =_{\mathsf{def}} x_1$. Independent of how B is defined there always exists such a function in $[B]$. Now it is not difficult to define a

homomorphism h which maps $\{0,1\}^\star$ to $\{(,),p,\otimes\}^\star$ s.t. $1^n w 0^{n+\ell} \in \text{MAJ}$ iff $h(1^n w 0^{n+\ell})$ is a syntactical correct CTL(T,B) formula. Hence define

$$h(w_i) =_{\mathsf{def}} \begin{cases} (, & \text{if } w_i = w_{i+1} = 1 \text{ or } w_i = 1, i = n \\ (p, & \text{if } 1 = w_i \neq w_{i+1} = 0 \\ ), & \text{if } w_i = w_{i+1} = 0 \text{ or } w_i = 0, i = n \\ )\otimes, & \text{if } 0 = w_i \neq w_{i+1} = 1, \end{cases}$$

for $w = w_1 w_2 \dots w_n$ und $1 \leq i \leq n$. Then it holds $w \in \text{MAJ}$ $gdw.$ $\bigvee_{0 \leq k \leq n} h(1^n w 0^{n+k}) \in$ CTL(T,B).
Now it is clear how one can construct an AC^0 circuit with oracle gates for CTL(T,B) to decide MAJ and thus MAJ $\leq_{\mathbf{cd}}$ CTL(T,B). $\square$