Martin Ziegler

Issued on 2014-06-03
Solutions due: 2014-06-10

Algebraic Complexity Theory

SS 2014, Exercise Sheet #7

EXERCISE 12:

a) Devise a Boolean term $\mathsf{equal}(x,y)$ evaluating to `true` iff $x=y$.

b) Devise a Boolean term $\mathsf{uniq}(x_1,\ldots,x_n)$ evaluating to `true` iff precisely one of $x_1,\ldots,x_n$ is `true`. How 'long' is uniq asymptotically?

c) Describe an encoding $\langle\varphi\rangle$ of Boolean terms $\varphi=\varphi(x_1,\ldots,x_n)$ over finite binary strings. How long is $\langle\varphi\rangle$ asymptotically, compared to the syntactic length of φ ?

d) Construct within time polynomial in the (syntactic or binary) length of φ a Boolean term ψ in conjunctive normal form (CNF) with the following property: φ is satisfiable iff ψ is. (Hint: Add variables for the results of all sub-expressions.)

e) Strengthen (d) to make ψ in 3-CNF.

EXERCISE 13:

Let $\mathbb{F}\subseteq\mathbb{R}$ denote a ring and abbreviate $\vec{X}:=(X_1,\ldots,X_n)$ and $\vec{Y}:=(Y_1,\ldots,Y_m)$.

a) Prove that every constructible subset of $\mathbb{R}$ is finite or co-finite;
and that every semi-algebraic subset of $\mathbb{R}$ is a finite union of intervals.

b) Construct to $p\in\mathbb{F}[\vec{X}]$ some $q\in\mathbb{F}[\vec{X},\vec{Y}]$ such that
$$\forall\vec{x}\in\mathbb{R}^n: \quad \big(p(\vec{x})\neq 0 \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: q(\vec{x},\vec{y})=0\big)$$

c) Construct to $p\in\mathbb{F}[\vec{X}]$ some $q\in\mathbb{F}[\vec{X},\vec{Y}]$ such that
$$\forall\vec{x}\in\mathbb{R}^n: \quad \big(p(\vec{x})\geq 0 \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: q(\vec{x},\vec{y})=0\big)$$

d) Construct to $p_1,p_2\in\mathbb{F}[\vec{X}]$ some $q\in\mathbb{F}[\vec{X},\vec{Y}]$ such that
$$\forall\vec{x}\in\mathbb{R}^n: \quad \big(p_1(\vec{x})=0\wedge p_2(\vec{x})=0 \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: q(\vec{x},\vec{y})=0\big)$$

e) Construct to $p_1,p_2\in\mathbb{F}[\vec{X}]$ some $q\in\mathbb{F}[\vec{X},\vec{Y}]$ such that
$$\forall\vec{x}\in\mathbb{R}^n: \quad \big(p_1(\vec{x})=0\vee p_2(\vec{x})=0 \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: q(\vec{x},\vec{y})=0\big)$$

f) Let $\varphi(z_1,\ldots,z_N)$ denote a Boolean combination of in-/equalities on $z_1,\ldots,z_N\in\mathbb{R}$.
Show that, to $p_1,\ldots,p_N\in\mathbb{F}[\vec{X}]$, there exists some $q\in\mathbb{F}[\vec{X},\vec{Y}]$ with
$$\forall\vec{x}\in\mathbb{R}^n: \quad \varphi\big(p_1(\vec{x}),\ldots,p_N(\vec{x})\big) \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: q(\vec{x},\vec{y})=0$$

g) Construct to $p\in\mathbb{F}[\vec{X}]$ within polynomial time some quadratic $q_1,\ldots,q_m\in\mathbb{F}[\vec{X},\vec{Y}]$ such that
$$\forall\vec{x}\in\mathbb{R}^n: \quad \big(p(\vec{x})=0 \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: \textstyle\bigwedge_{k=1}^m q_k(\vec{x},\vec{y})=0\big)$$

h) Construct to $p\in\mathbb{F}[\vec{X}]$ within polynomial time some quartic $q\in\mathbb{F}[\vec{X},\vec{Y}]$ such that
$$\forall\vec{x}\in\mathbb{R}^n: \quad \big(p(\vec{x})=0 \;\Leftrightarrow\; \exists\vec{y}\in\mathbb{R}^m: q(\vec{x},\vec{y})=0\big)$$

i) Which of (a)–(h) extend from $\mathbb{R}$ to $\mathbb{C}$?