The Complexity of the Chinese Remainder Theorem

Miguel Campercholi

A *congruence system* on an algebra A is a tuple $(\theta_1, \ldots, \theta_k; a_1, \ldots, a_k)$, with $\theta_i \in \operatorname{Con} A$ and $a_i \in A$, such that $\langle a_i, a_j \rangle \in \theta_i \vee \theta_j$ for $i, j \in \{1, \ldots, k\}$. An element $a \in A$ is a *solution* to the system $(\theta_1, \ldots, \theta_k; a_1, \ldots, a_k)$ provided that $\langle a, a_i \rangle \in \theta_i$ for $i \in \{1, \ldots, k\}$. Call a tuple $\theta_1, \ldots, \theta_k$ of congruences of A a *Chinese Remainder tuple* (CR tuple) if every system with these congruences is solvable. Due to the Chinese Remainder Theorem, every tuple of congruences of the ring of integers is a CR tuple (hence the choice of nomenclature). Pixley showed that this property of the integers is actually true of any algebra whose congruences are arithmetic (in fact it is equivalent to arithmeticity). It follows that non-arithmetic algebras must have congruence tuples that are not CR tuples.

In my talk I will discuss the computational complexity of deciding whether a tuple of congruences of a finite algebra is a Chinese Remainder tuple. As we shall see, the general problem is coNP-complete, however it turns out to be tractable when restricted to some well-known classes of algebras.