Notes about Algebraic Complexity

Xinhao Nie

Aarhus University

August 22, 2025

1 SqrtSum

Definition 1.1. *Given positive integers $a_1, \dots a_n$ and an integer t, we want to decide whether $\sum_{i=1}^{n} \sqrt{a_i} \leq t$.*

n

Lemma 1. *We can test whether $\sum_{i=1}^{n} \sqrt{a_i} = t$ in polynomial time.*

Proof. The paper 'Decreasing the Nesting Depth of Expressions Involving Square Roots' implicitly implies this result in its section 5.

First denest any individual radical that denests, which means for all a_i is not perfect sqaure number. Then we choose pair of remaining radicals $\sqrt{a_i}$ and $\sqrt{a_j}$ if their product denests in $\mathbb{Q}$. If $\sqrt{a_i}\sqrt{a_j}$ denests as $k \in \mathbb{Q}$, then replace $\sqrt{a_i} + \sqrt{a_j}$ by

$$(1 + \frac{k}{a_i})\sqrt{a_i} \in \mathbb{Q}(\sqrt{a_i}),$$

and iterate the process of looking for a pair of radicals that desnests. Its correctness can be easily checked.

If at some point no product of a pair of radicals denests, then we claim that the entire linear combination could not denest. Next we should prove this claim. The rough idea is that we show $\forall \sqrt{a_i} = \lambda \mathbf{e}_j$ where $\lambda \in \mathbb{Q}$ and $\langle \mathbf{e}_1, \dots, \mathbf{e}_{2^m} \rangle$ span the vector space $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m})$ over $\mathbb{Q}$ if $[\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}) : \mathbb{Q}] = 2^m$. Concretely, all basis $\mathbf{e}$ are the subproducts of m square roots. Then, we can concluded that if $\sum_{i=1}^{n} \sqrt{a_i} = t$, each square root must be eliminated because they are distinct basis. In other words, if there is no product of a pair of radicals denests, then it cannot equal to a rational number.

Together with some fact about basis of extension $\mathbb{Q}$ over $\mathbb{Q}$, above statement is directly showed by Lemma 1 in the original paper. But it's more general, here we beriefly prove what we use. Suppose that $[\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m}) : \mathbb{Q}] = 2^m$ and prove by induction if $\sqrt{a_{m+1}} \in \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m})$ then $\sqrt{a_{m+1}} = \lambda\sqrt{a_1 \dots a_m}$.

Basis(0): $\lambda = \sqrt{a_1}$. Hypothesis(m-1) and Induction(m): Write $\sqrt{a_{m+1}} = b\sqrt{a_m} + c$, where $b, c \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{m-1}})$. By squaring,

$$a_{m+1} = b^2 a_m + c^2 + 2bc\sqrt{a_m},$$

which indicates $c = 0$, since $a_{m+1} \in \mathbb{Q}$. Then, we have

$$\sqrt{a_{m+1}a_m} = ba_m \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{m-1}}).$$

By hypothesis, $\sqrt{a_{m+1}a_m} = \lambda\sqrt{a_1 \ldots a_{m-1}}$, which implies $\sqrt{a_{m+1}} = \lambda a_m^{-1}\sqrt{a_1 \ldots a_{m-1}a_m}$. Thus, we can write each $\sqrt{a_i} = \lambda\sqrt{a_1 \ldots a_m}$. Moreover, the 2^m subproducts of $\sqrt{a_1}, \ldots, \sqrt{a_m}$ are the basis of $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ over $\mathbb{Q}$. The proof is here.

□