

Algebraic Complexity Open Problems For Happy Hackers

Kenneth W. Regan

`regan@cse.buffalo.edu`

Department of Computer Science and Engineering
State University of New York at Buffalo
Buffalo, NY 14260 USA

Hereditary Formulas

For a [bi-,multi-]linear function f (over an infinite field), every circuit [formula] C computing f can be replaced by a hereditarily [bi-,multi-]linear circuit C' with $s(C') \leq s(C)$.

Is this true for *homogeneous* f ... *hereditarily homogeneous* C' ?

For non-homogeneous f , can we get a small hh formula $H(f)$ for the *least* homogenization of f w.r. to a new variable z ?

Idea: Decompose $f =: f_1 + f_2 + \dots + f_k$ where each f_i is a literal or a product, and $d_1 = \deg(f_1) \leq d_2 \leq \dots \leq d_k = \deg(f)$. Akin to Horner's Rule, define

$$\begin{aligned} H(f) &= H(f_k) + z^{d_k - d_{k-1}} * (H(f_{k-1}) \\ &\quad + z^{d_{k-1} - d_{k-2}} * (\dots + z^{d_2 - d_1} * H(f_1)). \end{aligned}$$

Is this always optimal? Analyze the resulting size... where and why will we need to care that each f_i is a product or literal?

Boolean Derivative Lemma?

For Boolean $f = f(x_1, \dots, x_n)$, define

$$f_i = \partial f / \partial x_i = f[x_i \leftarrow 0] \oplus f[x_i \leftarrow 1].$$

Is $s(f_1, \dots, f_n) = O(s(f))$?

Boolean Derivative Lemma?

For Boolean $f = f(x_1, \dots, x_n)$, define

$$f_i = \partial f / \partial x_i = f[x_i \leftarrow 0] \oplus f[x_i \leftarrow 1].$$

Is $s(f_1, \dots, f_n) = O(s(f))$?

Attempts I know to arithmetize Boolean functions and try to plug in to the usual Derivative Lemma all fail, intuitively either because $x^2 \neq x$, or because $2x = 0$.

Idea: “reverse” Boolean circuits directly?

How bumpy is the universe?

Say $v \in F^n$ has a *bump* at i of *length* r and *gap* ϵ if

$$|v_i| \geq \epsilon \|v\|_1 + \sum_{j=1}^{r-1} |v_{i-j}|.$$

Indices wrap mod n . If $v_{i-1} = \dots = v_{i-r+1} = 0$, the bump is “pure” and the gap is $|v_i|/\|v\|_1$.

Case $r = 1$, bump is an entry, some i gives gap $1/n$.

Case $r = 2$, nontrivial: all lin combs of $(1, 1, \dots, 1)$ and $(1, \omega, \omega^2, \dots, \omega^{n-1})$ give gap $O(1/n^2)$.

Question: Can we write r linear equations so that *no* vector in the $(n - r)$ -dim. solution subspace U has an r -bump with gap (at least) $1/n^{n/r}$? **No** when $r \leq \sqrt{n}$, but for all $r = o(n)$?