Zeitschrift: L'Enseignement Mathématique

Band: 28 (1982)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: RFDUCIBILITY BY ALGEBRAIC PROJECTIONS

Anhang: Appendix 1

Autor: Valiant, L. G.

DOI: https://doi.org/10.5169/seals-52240

implies that $x_i \geqslant 1$ since $x_i - x_j \geqslant 0$. Similarly if $x_k \geqslant 1$. If $x_j, x_k \leqslant 0$ then $x_j + x_k - x_i \geqslant 0$ ensures that $x_i \leqslant 0$. □

Claim 2. If val $(v_i) = 0$ then $E_i \cup \{ x_i \leqslant 0 \}$ has a solution. If val $(v_i) = 1$ then $E_i \cup \{ x_i \geqslant 1 \}$ has a solution.

Proof. By induction on i it is easy to see that the point

$$x_j = \begin{cases} 1 & \text{if val } (v_j) = 1 \\ 0 & \text{if val } (v_j) = 0 \end{cases}$$

for $1 \leqslant j \leqslant i$ is a solution of E_i. □

Claim 3. If for some $i, j\ (j \leqslant i)$ $E_i \cup \{ x_j \geqslant 1 \}$ has a solution in reals then val $(v_j) = 1$.

Proof. By Claim 1, if $E_i \cup \{ x_j \geqslant 1 \}$ has a solution then $E_i \cup \{ x_j \leqslant 0 \}$ has no solution. Hence by Claim 2 val $(v_j) = 1$. □

Finally we observe that the given program of size C for P_m translates to $3C + 2m$ inequalities in E_C, of which the $2m$ of E_o depend on the values of $y_1, \ldots, y_m$, while the remaining $3C$ are fixed. It remains to note that P_m is the projection under σ of $LP_{2n(n+1)}$ for $n = 3C + 2m$, where σ maps $3C$ of the inequalities to those of $E_C - E_o$, and the remaining $2m$ values of i as follows. If v_i equals y_j or $\bar{y}_j$ then: $\sigma(a_{ik}) = \sigma(b_{ik}) = 0$ if $j \neq k$, $\sigma(d_i) = 0$, $\sigma(a_{ij}) = \sigma(e_i) = v_i$, $\sigma(b_{ij}) = \bar{v}_i$. □

Acknowledgements. It is a pleasure to thank Volker Strassen and Mark Jerrum for suggesting corrections and simplifications on a first draft of this paper.

Appendix 1

We show here that in the concept of p-definability it is immaterial whether the defining polynomials allowed are the p-computable ones or merely those of p-bounded formula size. We shall suppose that the family P is p-definable in the sense of Definition 3, i.e.

$$P_n(x_1, \ldots, x_n) = \sum_{b \in \{0,1\}^{m-n}} Q_m(x_1, \ldots, x_n, b_{n+1}, \ldots, b_m)$$

It will suffice to prove that any p-computable family, such as Q, is p-definable in the sense of Definition 4. By Theorem 5 it then follows that P itself is also p-definable in the sense of Definition 4.

It is known that any p-computable family of homogeneous polynomials has homogeneous program size at most polynomially larger than its unrestricted program size [12]. The inductive proof to follow assumes the former measure throughout and supports homogeneity. We shall assume that Q_m is itself homogeneous. If it were not then we would consider each of its homogeneous components separately in the same way.

Suppose that $Q_m(x_1, ..., x_m)$ has degree d and a minimal program ρ of complexity C. Let U be the subset of the computed terms $\{v_i\}$ such that (i) $\deg(v_i) > d/2$ and (ii) $v_i \leftarrow v_j \times v_k$ with $\deg(v_j) \leqslant d/2$ and $\deg(v_k) \leqslant d/2$. Let W be the subset $\{v_j\}$ such that $v_i \leftarrow v_j \times v_k$ or $v_i \leftarrow v_k \times v_j$ for some $v_i \in U$. For convenience rename the elements of U and W by $\{u_1, ..., u_r\}$ and $\{w_1, ..., w_s\}$ respectively.

Claim 1. There is a polynomial $S_{m+r+1}(x_1, ..., x_m, e_0, ..., e_r)$ of degree $\lfloor d/2 \rfloor + 1$ and homogeneous program complexity at most $2C + d$ such that

$$Q_m(\mathbf{x}) = \sum_{i=1}^{r} \operatorname{val}(u_i) \cdot \operatorname{compl}_i$$

where $\operatorname{compl}_i = S_{m+r+1}(\mathbf{x}, \mathbf{e})$ when $e_0 = e_i = 1$ and $e_j = 0$ for $0 \neq j \neq i$.

Proof. In ρ replace each occurrence of u_i on the right hand side of an assignment by an occurrence of $e_i e_0^{\deg(u_i) - \lfloor d/2 \rfloor - 1}$. (Actually this would be simulated by a subprogram that raises e_0 to every power and multiplies by e_i as appropriate.) □

Claim 2. There is a polynomial $T_{n+s+1}(x_1, ..., x_m, c_0, ..., c_s)$ of degree $\lfloor d/2 \rfloor + 1$ and homogeneous program complexity at most $3C + d$ such that for each i $(1 \leqslant i \leqslant s)$

$$\operatorname{val}(w_i) = T_{m+s+1}(\mathbf{x}, \mathbf{c})$$

when $c_0 = c_i = 1$ and $c_j = 0$ for $0 \neq j \neq i$.

Proof. Delete from ρ every instruction with degree greater than $d/2$. Add a subprogram equivalent to the set of instructions

$$z_i \leftarrow w_i \times c_i c_0^{\lfloor d/2 \rfloor - \deg(w_i)}$$

for $i = 1, ..., s$. Add further instructions to sum $z_1, ..., z_s$. □

Now for each i $\operatorname{val}(u_i) = \operatorname{val}(w_j)\operatorname{val}(w_k)$ for some j, k specified by ρ. Hence each of the r additive contributions to Q_m is some product

$$T_{m+s+1}(\mathbf{x}, \mathbf{c})\, T_{m+s+1}(\mathbf{x}, \mathbf{c}')\, S_{m+r+1}(\mathbf{x}, \mathbf{e})$$

where $(\mathbf{c}, \mathbf{c}', \mathbf{e})$ is a fixed (0, 1)-vector of $2s+r+3$ elements. But any such vector can be specified by a conjunction of $2s+r+3$ Boolean literals. Consider the disjunction of the r such conjunctions and let $R(\mathbf{c}, \mathbf{c}', \mathbf{e})$ be the polynomial that simulates this Boolean formula at (0, 1) values. Then clearly

$$Q_m(x) = \sum T(\mathbf{x}, \mathbf{c})\, T(\mathbf{x}, \mathbf{c}')\, S(\mathbf{x}, \mathbf{e})\, R(\mathbf{c}, \mathbf{c}', \mathbf{e}) \ ,$$

where summation is over $(\mathbf{c}, \mathbf{c}', \mathbf{e}) \in \{0, 1\}^{2s+r+3}$.
Let $A(C, d)$ be the upper bound over every homogeneous polynomial having degree d and homogeneous program complexity C, of the minimal size of formula needed to define it in Definition 4. Then the above recursive expression ensures that

$$A(C, d) \leqslant 3A(3C+d, \lfloor d/2 \rfloor + 1) + 0(C) .$$

Clearly also $A(C, 1) \leqslant 2C$. Hence if d is p-bounded in m then so is the solution to this recurrence. □

Appendix 2

For completeness we describe here a direct proof of the p-definability of HC in the sense of Definition 1. $HC_{n \times n}(x_{i,j})$ will be the projection under

$$\sigma(u_{k,m}) = 1 \qquad \text{for} \qquad 1 \leqslant k, m \leqslant n$$

of the polynomial in $\{x_{i,j}, u_{k,m}\}$ defined by

$$Q_{n \times n}(y_{i,j}) \cdot Q_{n \times n}(z_{k,m}) \cdot R^1 \dots R^n$$

with the association $y_{i,j} \leftrightarrow x_{i,j}$ and $z_{k,m} \leftrightarrow u_{k,m}$. Here $Q_{n \times n}$ is the polynomial that defines the permanent in §3. Its first occurrence with argument y plays exactly the same role as in the permanent and ensures a cycle cover. The intention of $z_{k,m}$ is to denote whether the k^{th} node in the circuit (starting from node 1, say) is node m. $Q_{n \times n}(z_{k,m})$ ensures that this intention is realised. For each k R^k captures the fact that if $z_{k,m}$ and $z_{k+1,r}$ are both 1 then $y_{m,r}$ must be also. In Boolean notation we require

$$y_{m,r} \vee (\bar{z}_{k,m} \vee \bar{z}_{k+1,r}) \ .$$

As is well known such Boolean formulae can be simulated by polynomials at $\{0, 1\}$ values (e.g. see Proposition 2 in [13]). To guarantee just one monomial for each cycle we fix $R^1 = z_{11}$. □