**Zeitschrift:** L'Enseignement Mathématique
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique
**Band:** 28 (1982)
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** RFDUCIBILITY BY ALGEBRAIC PROJECTIONS
**Autor:** Valiant, L. G.
**Anhang:** Appendix 2
**DOI:** https://doi.org/10.5169/seals-52240

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

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

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

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

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

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 $R^1 = z_{11}$. □