Erratum to
The Complexity of Factors of Multivariate Polynomials

published in

Foundations of Computational Mathematics 4(4): 369–396, 2004.

Peter Bürgisser

Institute of Mathematics, TU Berlin
D-10623 Berlin, Germany
pbuerg@math.tu-berlin.de

December 14, 2018

Vladimir Lysikov kindly pointed out an error in the proof of Theorem 5.7. We provide here a corrected statement and its proof.

Theorem 5.7. For polynomials f over an algebraically closed field k we have $\underline{L}_q(f) \leq 2\underline{L}(f)$ with $q \leq 2^{\underline{L}(f)^2}$.

Proof. We proceed as in Lehmkuhl and Lickteig [2], who proved a similar bound on the order of approximation for border rank (approximative bilinear complexity).

The proof is based on the following geometric description of the set $\{f \in A_n \mid L(f) \leq r\}$. The field k is assumed to be algebraically closed. A straight-line program Γ is a description for a computation of a polynomial from constants $z_1, \ldots, z_m$ and variables $X_1, \ldots, X_n$ (recall that we do not allow divisions). Let $\phi_\Gamma(z)$ denote the polynomial in $A_n := k[X_1, \ldots, X_n]$ computed by Γ from the list of constants $z \in k^m$. Let r_* denote the number of multiplication instructions of Γ. Then we have

$$\phi_\Gamma(z) = \sum_\mu \phi_{\Gamma,\mu}(z) X^\mu,$$

where the sum runs over all $\mu \in \mathbb{N}^n$ with $\mu_1 + \ldots + \mu_n \leq 2^{r_*}$. Moreover, the coefficient polynomials $\phi_{\Gamma,\mu}(z)$ have degree at most 2^{r_*}. We interpret ϕ_Γ as a morphism $k^m \to \{f \in A_n \mid \deg f \leq 2^{r_*}\}$ of affine varieties. Applying [1, Theorem 8.48] to the polynomial map $z \mapsto (z, \phi_\Gamma(z))$, we see

that $\deg \mathrm{graph}(\phi_\Gamma) \leq (2^{r_*})^m =: D$. The image $\mathcal{C}_\Gamma$ of ϕ_Γ is an irreducible, constructible set. We have for fixed r that

$$\{f \in A_n \mid L(f) \leq r\} = \bigcup_\Gamma \mathcal{C}_\Gamma,$$

where the union is over all straight-line programs Γ of length r.

Assume now that f is in the Zariski-closure of the set on the left-hand side. Then we have $f \in \overline{\mathcal{C}_\Gamma}$ for some Γ. (We remark that in the case $k = \mathbb{C}$ the Zariski-closure of constructible sets coincides with the closure with respect to the Euclidean topology (cf. [3, Theorem 2.33]).

We apply now two results proven in Lehmkuhl and Lickteig [2] to the morphism ϕ_Γ. Proposition 1 of [2] claims that there exists an irreducible curve $C \subseteq k^m$ such that $f \in \overline{\phi_\Gamma(C)}$ and $\deg C \leq \deg \mathrm{graph}(\phi_\Gamma)$. The Corollary to Proposition 3 in [2] states that there exists a point $\zeta = (\zeta_1, \ldots, \zeta_m) \in k((\epsilon))^m$ such that $F := \phi_\Gamma(\zeta)$ is defined over $k[[\epsilon]]$, satisfies $F_{\epsilon=0} = f$ and such that all formal Laurent series ζ_i have order at least $-\deg C$. We conclude with Lemma 5.6(2) that $L(F) \leq r$ and hence $\underline{L}(f) \leq r$, which proves the nontrivial direction of Theorem 2.4. Moreover, we have shown that there is a straight-line program of length r, which computes F in $k((\epsilon))[X]$ from the X-variables and constants ζ_i having order at least $-\deg C \geq -D$. By a similar reasoning as in the proof of Lemma 5.6(1), we can construct from this a straight-line program of length at most $2r$, which computes in $k[[\epsilon]][X]$ an element of the form $\epsilon^q f + \epsilon^{q+1} f'$ with $q \leq 2^{r_*} D = 2^{(m+1)r_*}$. We therefore have $\underline{L}_q(f) \leq 2r$. To complete the proof, we note that $(m+1)r_* \leq r^2$, unless $m = r$ and $r = r_*$. However, in this case, the components of ϕ_Γ have degree at most 1 and we get $q \leq 2^{r_*}$ since $\deg \mathrm{graph}\phi_\Gamma \leq 1$. □

By tracing the proofs of the above results it is straightforward to show the following statement.

Remark 5.8. By counting only nonscalar multiplications, one can introduce the notions $\underline{L}^{ns}, \underline{L}^{ns}_q$ in an analogous way. We then have $\underline{L}^{ns} = \underline{L}^{ns}_\infty = \underline{L}^{ns}_q$.

References

[1] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer Verlag, 1997.

[2] T. Lehmkuhl and T. Lickteig. On the Order of Approximation in Approximative Triadic Decompositions of Tensors. *Theoret. Comp. Sci.*, 69:1–14, 1989.

[3] D. Mumford. *Algebraic Geometry I: Complex Projective Varieties.* Springer Verlag, 1976.