Correction to the proof of Theorem 1.

In the proof of Lemma 1, the inequality $\mu(M_{d,n}^{p^k}) \le 3\mu(M_{d+1,n+p}^{p^{k-1}})$ is not justified. Here, we propose an alternative proof of the lower bound of Theorem 1: for any odd constant $d \ge 3$, it holds that $\mu(M_n, d) \succeq n^{\lceil d/2 \rceil}$. It generalizes the argument of Theorem 2.

Proof. Consider an arbitrary (generic) arithmetic circuit with s nonscalar multiplication gates. Let it compute some polynomial f of degree $\le d$.

Denote by $u_1, u_2, \ldots, u_s$ polynomials computed in multiplication gates in the order of computation. It means that each u_k is a product of two linear combinations of $1, x_1, \ldots, x_n, u_1, \ldots, u_{k-1}$. Then f is a linear combination of $1, x_1, \ldots, x_n, u_1, \ldots, u_s$.

For a polynomial g, let $g^{[k]}$ denote its degree-k homogeneous component (consisting of all its degree-k monomials)[1]. Therefore, $g = g^{[0]} + g^{[1]} + \ldots + g^{[\deg g]}$. Also, denote $g^{[l..r]} = \sum_{i=l}^{r} g^{[i]}$.

I. We will check by induction that for $\lceil d/2 \rceil \le k \le d$,

$$u_j^{[k]} = \sum_{t=\lceil d/2 \rceil}^{k} \sum_{i=1}^{j-1} a_{j,k,t,i} \cdot v_{i,t} + v_{j,k}, \tag{1}$$

where $a_{j,k,t,i}$ are degree-$(k-t)$ homogeneous polynomials, and $v_{j,k}$ is a homogeneous degree-k component of a product $a_j \cdot b_j$ of two polynomials of degree $< \lceil d/2 \rceil$.

Induction base. Clearly, u_1 is a product of linear polynomials, hence, for $j = 1$ we have the sum empty and can set $v_{1,k} := u_1^{[k]}$.

Induction step from j to $j+1$. Write

$$u_{j+1} = AB, \quad A = \sum_{i=1}^{j} \alpha_i u_i + a, \quad B = \sum_{i=1}^{j} \beta_i u_i + b,$$

where $\alpha_i, \beta_i \in \mathbb{C}$ and $\deg a, b \le 1$. Set

$$a_{j+1} := A^{[0..\lfloor d/2 \rfloor]}, \quad b_{j+1} := B^{[0..\lfloor d/2 \rfloor]}.$$

[1]Further, speaking about a degree-k homogeneous component, we conventionally declare its degree to be k even in the case of all zero coefficients.

We can write

$$u_{j+1}^{[0..d]} = \left(\sum_{t=\lceil d/2\rceil}^{d}\sum_{i=1}^{j}\alpha_i u_i^{[t]} + a_{j+1}\right)\left(\sum_{t=\lceil d/2\rceil}^{d}\sum_{i=1}^{j}\beta_i u_i^{[t]} + b_{j+1}\right) =$$

$$= (a_{j+1}b_{j+1})^{[0..d]} + \sum_{t=\lceil d/2\rceil}^{d}\sum_{i=1}^{j} a_{i,t}u_i^{[t]}, \qquad \deg a_{i,t} \le d-t,$$

since products $u_i^{[t]}u_{i'}^{[t']}$ with $t, t' \ge \lceil d/2\rceil$ cannot contribute to homogeneous components of u_{j+1} of degree $\le d$.

Setting $v_{j+1,k} := (a_{j+1}b_{j+1})^{[k]}$ and applying (1), we further obtain for $\lceil d/2\rceil \le k \le d$ the representation

$$u_{j+1}^{[k]} \quad = \quad v_{j+1,k} \quad + \quad \sum_{t=\lceil d/2\rceil}^{k}\sum_{i=1}^{j} a_{i,t}^{[k-t]}\left(\sum_{t'=\lceil d/2\rceil}^{t}\sum_{i'=1}^{i-1} a_{i,t,t'i'}\cdot v_{i',t'} + v_{i,t}\right),$$

which has (after combining similar terms) the required form (1).

II. As a consequence,

$$f^{[d]} = \sum_{t=\lceil d/2\rceil}^{d}\sum_{i=1}^{s} c_{i,t}\cdot v_{i,t}, \qquad v_{i,t} = (a_i\cdot b_i)^{[t]}$$

where $c_{i,t}$ are degree-$(d-t)$ homogeneous polynomials.

Thus, the coefficients of the degree-d component of an arbitrary polynomial computable by a circuit of multiplicative complexity s can be algebraically parameterized by the coefficients of the polynomials $c_{i,t}$, a_i, and b_i, where $i = 1, \dots, s$ and $t = \lceil d/2\rceil, \dots, d$. Seeing that $\sum_{t=\lceil d/2\rceil}^{d} c_{i,t}$ fills a complete polynomial of degree $< \lceil d/2\rceil$, in total there are $s\cdot 3\binom{n+\lfloor d/2\rfloor}{\lfloor d/2\rfloor} \le 3s(n+1)^{\lfloor d/2\rfloor}$ such complex parameters.

The number of parameters must be at least as large as the number of coefficients, $\binom{n+d-1}{d} \ge n^d/d!$, in a homogeneous component of degree d. Otherwise, the latter coefficients would be algebraically dependent, and it would not be possible to represent every polynomial in $M_{n,d}$. Therefore,

$$\mu(M_{d,n}) \ge \frac{C_{n+d-1}^{d}}{3(n+1)^{\lceil d/2\rceil-1}} \gtrsim \frac{n^{\lceil d/2\rceil}}{3d!}.$$