# DEFINING MULTIPLICATION FOR POLYNOMIALS OVER A FINITE FIELD

MICHEL RIGO AND LAURENT WAXWEILER

Abstract. Let $P$ and $Q$ be two non-zero multiplicatively independent polynomials with coefficients in a finite field $\mathbb{F}$. Adapting a result of R. Villemaire, we show that multiplication of polynomials is a ternary relation $\{(A, B, C) \in \mathbb{F}[X] \mid A.B = C\}$ definable by a first-order formula in a suitable structure containing both functions $V_P$ and $V_Q$ where $V_A(B)$ is defined as the greatest power of $A$ dividing $B$. Such a result has to be considered in the context of a possible analogue of Cobham's theorem for sets of polynomials whose $P$-expansions are recognized by some finite automaton.

## 1. Introduction

All along this paper, $\mathbb{F}$ is a finite field and $\mathbb{F}[X]$ is the ring of polynomials over $\mathbb{F}$. Let $P, Q$ be two non-constant polynomials. If the only integers $a, b$ such that $P^a = Q^b$ are $a = b = 0$, then $P$ and $Q$ are *multiplicatively independent*. Let $P, Q$ be two polynomials. We write $P \prec Q$, if $\deg P < \deg Q$ ($\preceq$, $\succ$ and $\succeq$ are defined accordingly). As usual, we set $\deg 0 = -\infty$. The set of powers of $P$ is $P^{\mathbb{N}} := \{P^n \mid n \in \mathbb{N}\}$. Let $P$ be a non-constant polynomial. The map $V_P : \mathbb{F}[X] \to P^{\mathbb{N}}$ is defined by $V_P(0) = 1$ and, for all non-zero polynomials $A$, $V_P(A)$ is the largest power of $P$ dividing $A$.

We consider the structure $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P \rangle$. In particular, relying on techniques based on automata, the first-order theory of this structure is known to be decidable [8] and similar structures have been recently and independently considered by A. Sirokofskich in [10]. One can notice that we equip the structure with multiplication by a fixed polynomial $C$, that is, maps of the kind $A \mapsto C \cdot A$.

Interestingly some sets of polynomials can be defined within such a first-order structure. We can write well-formed formulas where variables are ranging over $\mathbb{F}[X]$, using usual logical connectives $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$, existential and universal quantifiers $(\exists Q)$ and $(\forall Q)$ applied only to variables and also the specific operations of the structure: addition of polynomials, comparison of degree, multiplication by a fixed polynomial and the map $V_P$ defined above. Let $\varphi(R_1, \ldots, R_k)$ be a formula with $k$ free variables, i.e., not in the scope of any quantifier. This formula defines a subset of $k$-tuples of polynomials for which the formula is satisfied:

$$M_\varphi = \{(Q_1, \ldots, Q_k) \in (\mathbb{F}[X])^k \mid \langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P \rangle \models \varphi(Q_1, \ldots, Q_k)\}.$$

Note that if $P$ and $Q$ are multiplicatively dependent polynomials of degree at least one, then the structures $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P \rangle$ and $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_Q \rangle$ are equivalent: they give exactly the same definable sets. Let us consider a few examples where $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$. The set of polynomials in $(\mathbb{Z}/2\mathbb{Z})[X]$ which are divisible by $X^2$ is defined by $\varphi(A) \equiv (\exists Q)(A = X^2 \cdot Q)$. The set of powers of $X$ is definable in the structure $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_X \rangle$ by the formula $\varphi(A) \equiv V_X(A) = A$.

It turns out that set of polynomials definable in the structure $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P \rangle$ are exactly the so-called *$P$-recognizable sets*, i.e., sets of polynomials whose $P$-expansions are finite words recognized by some finite automaton over a finite alphabet, see again [8]. Indeed, if $P$ is a non-constant polynomial, then any non-zero polynomial $A \in \mathbb{F}[X]$ can be written in a unique way as $A = \sum_{i=0}^{\ell} C_i P^i$ with $C_\ell \neq 0$ and polynomials $C_0, \ldots, C_\ell$ of degree less than the degree of $P$. Hence this logical characterization provides us with a useful tool to studying these recognizable sets of polynomials as initiated in [7].

The main result of this paper appeared first in the unpublished Ph.D. thesis of the second author [13] and is the following one.

**Theorem 1.** *Let $P$ and $Q$ be two multiplicatively independent polynomials with coefficients in a finite field $\mathbb{F}$. Then multiplication of polynomials is a ternary relation*

$$\{(A, B, C) \in \mathbb{F}[X] \mid A.B = C\}$$

*definable by a first-order formula in $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, V_Q\rangle$.*

This means that adding multiplication to the structure $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, V_Q\rangle$ does not lead to any new first-order definable set of polynomials. It also turns out that any map $V_R$ can also be defined within this structure.

A result similar to Theorem 1 has been obtained in [12] for the integers and the structure $\langle \mathbb{N}, +, V_k, V_\ell\rangle$ where $V_k(n)$ is the largest power of $k \geq 2$ dividing $n \in \mathbb{N}_{\geq 1}$. Our proofs and guidelines rely on those originally developed by Villemaire. We consider that our work is not a mere translation of the original ones: non-trivial adaptations, complements and slight corrections had to be made. Furthermore, the extra arguments that we will present can also be translated to the original context of integers. Also, such a result can provide some insight about the recognizability of sets of polynomials over a finite ring which has still to be studied further.

1.1. **Motivations.** A set $X$ of integers is said to be *$p$-recognizable*, if the set of base $p$ expansions of the elements in $X$ is a regular language over the alphabet of digits $\{0, \ldots, p-1\}$ (that is accepted by some finite automaton). A set $X$ is *ultimately periodic* if there exist $N, q > 1$ such that, for all $n \geq N$, $n \in X \Leftrightarrow n + q \in X$. Villemaire's work can be related to the famous theorem of Cobham [2]: if a set $X$ of integers is both $p$-recognizable and $q$-recognizable with $p$ and $q$ being multiplicatively independent integer bases, then $X$ is ultimately periodic. Cobham's theorem has given a major impulse to studying recognizable sets of integers [1, 3]. In this context, Villemaire's work has led to interesting developments concerning $p$-recognizable sets in a logical setting [5]. In this context, the work of Semenov and Muchnik have also to be mentioned [9, 6]. Therefore, as for the integer case, we hope that our result could shed some new light on a possible analogue of Cobham's theorem in the context of sets of polynomials over a finite field which are $P$-recognizable for all polynomial base $P$. Up to now, $p$-recognizable or $p$-automatic sets of polynomials over a finite field have reveal more properties than those observed for integers and deserve further investigations [7, 8].

1.2. **Organization.** This paper is organized as follows. In Section 2, we give a few definitions needed in the paper. Section 3 is devoted to the following construction. Given two multiplicatively independent polynomials $S, T$, we define two multiplicatively independent polynomials $P, Q$ which are respectively power of $S$ and $T$, some increasing map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ and a finite partition $(E_i)_{i\in\{1,\ldots,c\}}$ of $P^{\mathbb{N}}$ such that for all $i \in \{1, \ldots, c\}$ and all $A, B \in E_i$, $A \prec B \to \exists C \in (P^{\mathbb{N}} \setminus F(P^{\mathbb{N}})) : F(A) \prec C \prec F(B)$. Furthermore, we ensure that $F$ and $(E_i)_{i\in\{1,\ldots,c\}}$ are definable in $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, V_Q\rangle$. In Section 4 we assume the existence of such a map $F$ and partition $(E_i)_{i\in\{1,\ldots,c\}}$ to define multiplication in a enlarged structure where $F$ and $(E_i)_{i\in\{1,\ldots,c\}}$ have been added. Finally, we collect in Section 5 the results of the previous two sections ti get a proof of the main theorem.

## 2. A few definitions

We denote respectively by $\mathcal{S}_P$ and $\mathcal{S}_{P,Q}$ the structures $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P\rangle$ and $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, V_Q\rangle$. The *terms* in $\mathcal{S}_P$ are variables and constants (when the structure contains the function $V_P$ then the constant 1 is easily defined by $A = 1 \equiv V_P(0) = A$ and the constant 0 by $A = 0 \equiv (\forall B)(A \prec B \vee A = B))$ ranging over $\mathbb{F}[X]$ or if $Q, R$ are terms and $C$ is a fixed polynomial, then $Q + R$, $Q \cdot C$, $V_P(Q)$ are terms. If $Q, R$ are terms, then $Q = R$ and $Q \prec R$ are *atomic formulas*. Then one can construct arbitrary formulas using logical connectives $\vee, \wedge, \neg, \to, \leftrightarrow$ and quantifiers $\exists Q$ and $\forall Q$ where $Q$ is a variable.

**Definition 1.** Let $P, Q \in \mathbb{F}[X]$ be non-constant polynomial. A subset $\mathcal{T}$ of $(\mathbb{F}[X])^d$ is *$P$-definable* (resp. *$(P,Q)$-definable*) if there exists a first-order formula $\phi(A_1, \ldots, A_d)$ in the language $\mathcal{S}_P$ (resp. $\mathcal{S}_{P,Q}$) which is satisfied if and only if $(A_1, \ldots, A_d)$ belongs to $\mathcal{T}$. A $k$-ary relation $\mathcal{T}$ is simply a subset of $(\mathbb{F}[X])^k$ and one can define *$P$-definable* (resp. *$(P,Q)$-definable*) relation accordingly. A map from $(\mathbb{F}[X])^k$ to $(\mathbb{F}[X])^\ell$ is a $(k+\ell)$-ary relation. So *$P$-definable* (resp. *$(P,Q)$-definable*) maps are defined accordingly.

**Definition 2.** Let $k \in \mathbb{F}$ be non-zero. The map $\mathrm{lcm}_k : \mathbb{F}[X] \times \mathbb{F}[X] \to \mathbb{F}[X]$ is defined as follows. If $A$ or $B$ is zero, then $\mathrm{lcm}_k(A, B) = 0$. Otherwise, $\mathrm{lcm}_k(A, B)$ is the least common multiple of the polynomials $A$ and $B$ having $k$ as leading coefficient.

**Definition 3.** Any non-zero polynomial $A \in \mathbb{F}[X]$ can be written in a unique way as $A = \sum_{i=0}^{\ell} C_i P^i$ with $C_\ell \neq 0$ and polynomials $C_0, \ldots, C_\ell$ of degree less than the degree of $P$. The word $C_\ell \cdots C_0$ over the finite alphabet of polynomials of degree less than $\deg(P)$ is the *$P$-expansion* or *$P$-representation* of $A$. It is denoted $\mathrm{rep}_P(A)$. We say that the $P$-expansion of $A$ has coefficient $C_j$ occurring for $P^j$. By convention, the $P$-expansion of the zero polynomial is the empty word.

**Definition 4.** The binary relation $X_{P,J}(A, B)$ is true if and only if $A$ is a power $P$ and in the $P$-representation of $B$, $A$ occurs with $J$ as coefficient, $J \prec P$. It is $P$-definable by the formula

$$(V_P(A) = A) \wedge (\exists U)(\exists V)(B = U + J \cdot A + V \wedge V \prec A \wedge (U = 0 \vee A \prec V_P(U))).$$

**Definition 5.** Let $k \geq 1$ be an integer. For all $A \in \mathbb{F}[X]$, $\mathrm{Deg}_k(A)$ is true if and only if $\deg(A) \equiv 0 \bmod k$. Let $C$ be a non-zero polynomial. For all $A \in \mathbb{F}[X]$, $\mathrm{Pre}_C(A)$ is true if and only $\mathrm{rep}_X(C)$ is a prefix of $\mathrm{rep}_X(A)$.

**Proposition 2.** [8] *Let $P$ be a non-constant polynomial. Let $k \geq 1$ be an integer. Let $C$ be a non-zero polynomial. The unary relations $\mathrm{Deg}_k$ and $\mathrm{Pre}_C$ are $P$-definable.*

## 3. A partition of $P^{\mathbb{N}}$

The aim of this section is to prove Theorem 6, namely that if $S, T$ are two multiplicatively independent polynomials, then there exist $P$ and $Q$ which are respectively power of $S$ and $T$ (or $T$ and $S$, see (5) for details), some $(P,Q)$-definable increasing map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ and a finite partition $(E_i)_{i \in \{1,\ldots,c\}}$ of $P^{\mathbb{N}}$ such that for all $i \in \{1, \ldots, c\}$ and all $A, B \in E_i$,

$$A \prec B \to \exists C \in (P^{\mathbb{N}} \setminus F(P^{\mathbb{N}})) : F(A) \prec C \prec F(B).$$

To that end, we consider decomposition of polynomials into a product of irreducible polynomials and we mainly have to consider two particular cases depending on the decompositions discussed in Propositions 3 and 4.

**Lemma 1.** *Let $k \in \mathbb{F}$ be non-zero. Let $P, Q$ be multiplicatively independent polynomials of the kind $P = P_0 R$ and $Q = Q_0 R$ with $P_0, Q_0, R$ pairwise coprime polynomials such that $P_0 \succeq Q_0$. Then the map $\mathrm{lcm}_k$ restricted to the domain $P^{\mathbb{N}} \times Q^{\mathbb{N}}$ is $(P,Q)$-definable.*

*Proof.* Consider the graph $\{(A, B, C) \mid (A, B) \in P^{\mathbb{N}} \times Q^{\mathbb{N}}, \mathrm{lcm}_k(A, B) = C\}$ of the map $\mathrm{lcm}_k$ restricted to $P^{\mathbb{N}} \times Q^{\mathbb{N}}$. This set can be defined by the formula:

$$\begin{aligned} & V_P(A) = V_P(C) = A \wedge V_Q(B) = V_Q(C) = B \\ \wedge \quad & (\forall T)(V_P(T) = A \wedge V_Q(T) = B \to T \succeq C) \wedge Deb_K(C) \end{aligned}$$

where $K$ is the constant polynomial corresponding to the element $k \in \mathbb{F}$. □

**Proposition 3.** *Let $P, Q$ be multiplicatively independent polynomials of the kind $P = P_0 R$ and $Q = Q_0 R$ with $P_0, Q_0, R$ pairwise coprime polynomials such that $P_0 \succeq Q_0$. Then there exist a constant $c \in \mathbb{N}_{\geq 1}$ and a $(P,Q)$-definable map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ increasing with respect to the order relation $\prec$ and such that, for all $k \in \mathbb{N}$,*

$$P^{c+1} \cdot F(P^k) \preceq F(P^{k+c}).$$

*Proof.* Let $G : P^{\mathbb{N}} \to Q^{\mathbb{N}}$ mapping $A \in P^{\mathbb{N}}$ to the smallest power $Q^k$ of $Q$ such that $Q^k \succ A$. The graph $\{(A, B) \mid G(A) = B\}$ of this map is $(P, Q)$-definable by the formula:

$$V_P(A) = A \wedge V_Q(B) = B \wedge B \succ A \wedge (\forall C)(V_Q(C) = C \wedge C \succ A \to C \succeq B).$$

In the same way, the function $H : \mathbb{F}[X] \to P^{\mathbb{N}}$ mapping $A \in \mathbb{F}[X]$ to the smallest power $P^k$ of $P$ such that $P^k \succ A$ is also $(P, Q)$-definable.

Now using the above lemma and composing $(P, Q)$-definable maps, the map

$$F : P^{\mathbb{N}} \to P^{\mathbb{N}}, A \mapsto H(\mathrm{lcm}_1(A, G(A)))$$

is thus $(P, Q)$-definable.

Let $v(k)$ be the smallest integer such that $P^k \prec Q^{v(k)}$. Since $P = P_0R \succeq Q_0R = Q$, for all $k \in \mathbb{N}$, we have $v(k) + 1 \leq v(k + 1)$.

We write $A \simeq B$, if $\deg(A) = \deg(B)$, i.e., $A \preceq B \wedge B \preceq A$. Let us first prove that $F$ is increasing, i.e., that, for all $k$, $F(P^{k+1}) \succ F(P^k)$. We have

$$\begin{aligned} F(P^{k+1}) &= H(\mathrm{lcm}_1(P^{k+1}, Q^{v(k+1)})) \simeq H(P_0^{k+1}Q_0^{v(k+1)}R^{v(k+1)}) \\ &\succeq H(P_0^{k+1}Q_0^{v(k)+1}R^{v(k)+1}) \succeq H(PP_0^kQ_0^{v(k)}R^{v(k)}). \end{aligned}$$

Since $H(PP_0^kQ_0^{v(k)}R^{v(k)}) = P \cdot H(P_0^kQ_0^{v(k)}R^{v(k)}) \succ H(P_0^kQ_0^{v(k)}R^{v(k)})$, we get

$$F(P^{k+1}) \quad \succ \quad H(\mathrm{lcm}_1(P^k, Q^{v(k)})) = F(P^k).$$

To conclude with this proof, we have to show that there exists a constant $c$ such that, for all $k \in \mathbb{N}$, $P^{c+1} \cdot F(P^k) \preceq F(P^{k+c})$. Observe that

$$P^{c+1} \cdot H(\mathrm{lcm}_1(P^k, G(P^k))) \preceq H(\mathrm{lcm}_1(P^{k+c}, G(P^{k+c})))$$

holds true whenever $P^{c+2} \cdot \mathrm{lcm}_1(P^k, G(P^k)) \preceq \mathrm{lcm}_1(P^{k+c}, G(P^{k+c}))$. This latter condition is equivalent to

$$P_0^2\, Q_0^{v(k)}\, R^{v(k)+c+2} \preceq Q_0^{v(k+c)}\, R^{v(k+c)} \tag{1}$$

which in turn holds whenever $P_0^2\, Q_0^{v(k)}\, R^{v(k)+c+2} \preceq Q_0^{v(k)+c}\, R^{v(k)+c}$. We have just shown that (1) or $2\deg(P_0) + 2\deg(R) \leq c\, \deg(Q_0)$ imply $P^{c+1} \cdot F(P^k) \preceq F(P^{k+c})$.

If $\deg(Q_0) \geq 1$, then the condition is satisfied for any large enough $c$.

Now consider the case where $Q_0$ is a constant in $\mathbb{F}$. In that case, since $\deg(R) = \deg(Q)$, condition (1) becomes $2\deg(P_0) + (v(k)+c+2)\deg(Q) \leq v(k+c)\deg(Q)$. We have, by definition of $v$, $P^{k+c} \prec Q^{v(k+c)}$ and $Q^{v(k)-1} \preceq P^k$ for all $k, c$. Therefore, we get $(k+c)\deg(P) < v(k+c)\deg(Q)$ and $(v(k) - 1)\deg(Q) \leq k\deg(P)$ for all $k, c$. From these two inequalities, we conclude that

$$c\deg(P) = (k + c - k)\deg(P) < (v(k + c) - v(k) + 1)\deg(Q). \tag{2}$$

Note that $\deg(P_0) \geq 1$, because otherwise $P = kR$ and $Q = \ell R$ for some non-zero $k, \ell \in \mathbb{F}$ and one can conclude that $P$ and $Q$ are multiplicatively dependent. Therefore, for large enough $c$,

$$c(\deg(P) - \deg(Q)) \geq 2\deg(P_0) + 3\deg(Q). \tag{3}$$

From (2), we obtain that

$$v(k + c)\deg(Q) > c(\deg(P) - \deg(Q)) + (v(k) + c - 1)\deg(Q)$$

and we conclude the proof. Using (3), we get $v(k+c)\deg(Q) \geq 2\deg(P_0) + (v(k)+c+2)\deg(Q)$. □

**Proposition 4.** *Let $P, Q$ be two polynomials having decomposition into irreducible polynomials of the kind*

$$P = \prod_{i=1}^{m} P_i^{\gamma_i} \prod_{i=1}^{\ell} R_i^{\alpha_i} \text{ and } Q = \prod_{i=1}^{n} Q_i^{\delta_i} \prod_{i=1}^{\ell} R_i^{\beta_i}$$

*where the polynomials $P_1, \ldots, P_m, Q_1, \ldots, Q_n, R_1, \ldots, R_\ell$ are pairwise coprime, $m, n, \ell \in \mathbb{N}$, $\ell \geq 2$ and*

$$1 = \frac{\alpha_1}{\beta_1} \leq \cdots \leq \frac{\alpha_i}{\beta_i} \leq \cdots \leq \frac{\alpha_\ell}{\beta_\ell} = \theta, \text{ with } \theta > 1.$$

*Then the map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}, P^k \mapsto P^{\lceil \theta k \rceil}$ is increasing with respect to the order relation $\prec$ and there exists a constant $c \in \mathbb{N}_{\geq 1}$ such that, for all $k \in \mathbb{N}$, $P^{c+1} \cdot F(P^k) \preceq F(P^{k+c})$.*

*Proof.* For all $c, k \in \mathbb{N}$, we have

$$F(P^{k+c}) = P^{\lceil \theta(k+c) \rceil} \succeq P^{\lceil \theta k + \lfloor \theta c \rfloor \rceil} = F(P^k) \cdot P^{\lfloor \theta c \rfloor}.$$

Taking $c = 1$, leads to $F(P^{k+1}) \succ F(P^k)$ showing that $F$ is increasing. Fix any integer $c$ such that $c \geq 1/(\theta - 1)$. Hence we get $\lfloor \theta c \rfloor \geq \lfloor 1 + c \rfloor$ and $F(P^{k+c}) \succeq F(P^k) \cdot P^{\lfloor \theta c \rfloor} \succeq F(P^k) \cdot P^{c+1}$. □

**Proposition 5.** *Let $P, Q$ be two polynomials satisfying the assumptions of Proposition 4. The map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}, P^k \mapsto P^{\lceil \theta k \rceil}$ defined in Proposition 4 is $(P, Q)$-definable.*

*Proof.* First the map $G : P^{\mathbb{N}} \to Q^{\mathbb{N}}, P^k \mapsto Q^{\lceil \theta k \rceil}$ is $(P, Q)$-definable. We have $B = G(A)$ if and only if

$$V_P(A) = A \wedge V_Q(B) = B \wedge (\forall T)\Big(V_P(T \prod_{i=1}^{\ell} R_i) \succeq A \wedge V_Q(T) \succeq B \to V_P(T) \succeq A\Big) \wedge$$
$$(\forall C)\Big[V_Q(C) = C \wedge (\forall T)\Big(V_P(T \prod_{i=1}^{\ell} R_i) \succeq A \wedge V_Q(T) \succeq C \to V_P(T) \succeq A\Big) \to C \succeq B\Big].$$

Indeed, $A = P^k$ and $B = Q^r$ for some integers $k, r$. Any non-zero polynomial $T$ can be written

$$T = T_0 \prod_{i=1}^{m} P_i^{\gamma_i'} \prod_{i=1}^{n} Q_i^{\delta_i'} \prod_{i=1}^{\ell} R_i^{\epsilon_i}$$

where $T_0$ is a polynomial coprime with all $P_i, Q_i, R_i$ and $\gamma_i', \delta_i', \epsilon_i$ are non-negative integers. Note that

$$V_P(T) = V_P\Big(\prod_{i=1}^{m} (P_i^{\gamma_i})^{\gamma_i'/\gamma_i} \prod_{i=1}^{\ell} (R_i^{\alpha_i})^{\epsilon_i/\alpha_i}\Big) = P^{\min\big\{\lfloor \gamma_i'/\gamma_i \rfloor, \lfloor \epsilon_j/\alpha_j \rfloor | 1 \leq i \leq m, 1 \leq j \leq \ell\big\}},$$

$$V_Q(T) = Q^{\min\big\{\lfloor \delta_i'/\delta_i \rfloor, \lfloor \epsilon_j/\beta_j \rfloor | 1 \leq i \leq n, 1 \leq j \leq \ell\big\}},$$

$$V_P(T \prod_{i=1}^{\ell} R_i) = P^{\min\big\{\lfloor \gamma_i'/\gamma_i \rfloor, \lfloor (1+\epsilon_j)/\alpha_j \rfloor | 1 \leq i \leq m, 1 \leq j \leq \ell\big\}}.$$

The implication $V_P(T \prod_{i=1}^{\ell} R_i) \succeq A \wedge V_Q(T) \succeq B \to V_P(T) \succeq A$ is equivalent to

$$\begin{aligned} &\min\big\{\lfloor \gamma_i'/\gamma_i \rfloor, \lfloor (1+\epsilon_j)/\alpha_j \rfloor \mid 1 \leq i \leq m, 1 \leq j \leq \ell\big\} \geq k \\ \wedge \quad &\min\big\{\lfloor \delta_i'/\delta_i \rfloor, \lfloor \epsilon_j/\beta_j \rfloor \mid 1 \leq i \leq n, 1 \leq j \leq \ell\big\} \geq r \\ \to \quad &\min\big\{\lfloor \gamma_i'/\gamma_i \rfloor, \lfloor \epsilon_j/\alpha_j \rfloor \mid 1 \leq i \leq m, 1 \leq j \leq \ell\big\} \geq k \end{aligned}$$

and it is satisfied, for all possible $T_0, \gamma_1', \ldots, \gamma_m', \delta_1', \ldots, \delta_n', \epsilon_1, \ldots, \epsilon_\ell$ describing the polynomial $T$, if and only if the following implication holds for all $\epsilon_1, \ldots, \epsilon_\ell$:

$$\begin{aligned} &\min\big\{\lfloor (1+\epsilon_j)/\alpha_j \rfloor \mid 1 \leq j \leq \ell\big\} \geq k \wedge \min\big\{\lfloor \epsilon_j/\beta_j \rfloor \mid 1 \leq j \leq \ell\big\} \geq r \\ \to \quad &\min\big\{\lfloor \epsilon_j/\alpha_j \rfloor \mid 1 \leq j \leq \ell\big\} \geq k. \end{aligned}$$

This is equivalent to the fact that there is no $j \in \{1, \ldots, \ell\}$ and no $\epsilon_j$ such that $(1 + \epsilon_j)/\alpha_j \geq k > \epsilon_j/\alpha_j$ and $\epsilon_j/\beta_j \geq r$, i.e., such that $k\alpha_j - 1 = \epsilon_j \geq r\beta_j$. This latter inequalities occur for no $j \in \{1, \ldots, \ell\}$ and no $\epsilon_j$ if and only if $r/k \geq \max\{\alpha_j/\beta_j \mid 1 \leq j \leq \ell\} = \theta$. In other words, the middle part of the formula describes that $B$ is a power of $Q$ having an exponent at least $k\theta$. In the same way, the last part of the formula means that any polynomial $C$ which is a power of $Q$ having an exponent at least $k\theta$ is such that $C \succeq B$.

Now consider the map $H : Q^{\mathbb{N}} \to P^{\mathbb{N}}, Q^k \mapsto P^k$ which is $(P,Q)$-definable because $B = H(A)$ if and only if

$$V_Q(A) = A \wedge V_P(B) = B \wedge (\forall T)\Big(V_Q(T\prod_{i=1}^{\ell} R_i) \succeq A \wedge V_P(T) \succeq B \to V_Q(T) \succeq A\Big) \wedge$$

$$(\forall C)\Big[V_P(C) = C \wedge (\forall T)\Big(V_Q(T\prod_{i=1}^{\ell} R_i) \succeq A \wedge V_P(T) \succeq C \to V_Q(T) \succeq A\Big) \to C \succeq B\Big].$$

The reasoning is the same as above. Indeed, $A = Q^k$ and $B = P^r$ for some integers $k, r$. Notice that $\max\{\beta_j/\alpha_j \mid 1 \le j \le \ell\} = 1$ and therefore $B$ the smallest power of $P$ having an exponent at least $k$, that is, $P^k$.

To conclude with the proof, the map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}, P^k \mapsto P^{\lceil \theta k \rceil}$ is defined by $F(A) = B$ if and only if $(\exists C)(G(A) = C \wedge H(C) = B)$. □

We can now give the main result of this section.

**Theorem 6.** *Let $S, T$ be two multiplicatively independent polynomials. There exist two multiplicatively independent polynomials $P, Q \in S^{\mathbb{N}} \cup T^{\mathbb{N}}$, an increasing map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ and a finite partition $(E_i)_{i\in\{1,\dots,c\}}$ of $P^{\mathbb{N}}$ which are $(P,Q)$-definable and such that, for all $i \in \{1,\dots,c\}$ and all $A, B \in E_i$,*

$$A \prec B \to \exists C \in (P^{\mathbb{N}} \setminus F(P^{\mathbb{N}})) : F(A) \prec C \prec F(B). \tag{4}$$

**Remark 1.** In [12], R. Villemaire explains that condition (4) implies that the restriction of $F$ to $E_i$ can be seen as a "skipping" function, i.e., it skips at least one element of $P^{\mathbb{N}}$ between any two consecutive arguments.

*Proof.* Consider the following general decomposition of $S$ and $T$

$$S = k\prod_{i=1}^{m} S_i^{\gamma_i} \prod_{i=1}^{\ell} R_i^{\alpha_i} \text{ and } T = k' \prod_{i=1}^{n} T_i^{\delta_i} \prod_{i=1}^{\ell} R_i^{\beta_i}$$

where $S_1,\dots,S_m,T_1,\dots,T_n,R_1,\dots,R_\ell$ are irreducible pairwise coprime polynomials, $k, k'$ are non-zero elements in $\mathbb{F}$ and

$$0 < \theta_1 = \frac{\alpha_1}{\beta_1} \le \cdots \le \frac{\alpha_i}{\beta_i} \le \cdots \le \frac{\alpha_\ell}{\beta_\ell} = \theta_2.$$

Our aim is to define suitable powers of $S$ and $T$ to be under the assumptions of either Proposition 3 or Proposition 4 where particular kind of decompositions are considered.

If $\ell \ge 2$ and $\theta_1 < \theta_2$, then we consider $P = S^{\beta_1(\#\mathbb{F}-1)}$ and $Q = T^{\alpha_1(\#\mathbb{F}-1)}$ to be under the assumptions of Propositions 4 and 5 (note that $k^{\#\mathbb{F}-1} = k'^{\#\mathbb{F}-1} = 1$).

If $\ell \in \{0,1\}$ or $\theta_1 = \theta_2$ (if $\ell = 0$, we set $\alpha_1 = \beta_1 = 1$), then to be under the conditions of Proposition 3, we consider

$$\begin{cases} P = S^{\beta_1(\#\mathbb{F}-1)}, & Q = T^{\alpha_1(\#\mathbb{F}-1)}, \quad \text{if } S^{\beta_1} \succeq T^{\alpha_1}; \\ P = T^{\alpha_1(\#\mathbb{F}-1)}, & Q = S^{\beta_1(\#\mathbb{F}-1)}, \quad \text{otherwise}. \end{cases} \tag{5}$$

Therefore there exists a constant $c \in \mathbb{N}_{\ge 1}$ and an increasing $(P,Q)$-definable map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ satisfying $P^{c+1} \cdot F(P^k) \preceq F(P^{k+c})$ for all $k$. Observe that this latter property implies that, for all $k$, there exists $s$ such that $F(P^k) \prec P^s \prec F(P^{k+c})$ and $P^s \notin \{F(P^k), F(P^{k+1}), \dots, F(P^{k+c})\}$.

To conclude the proof, we have to show that the sets $E_1,\dots,E_c$ are $(P,Q)$-definable. Let $i \in \{1,\dots,c\}$. A polynomial $A$ belongs to $E_i$ if and only if it satisfies the following formula:

$$V_P(A) = A \wedge \bigwedge_{j=1}^{i-1} \big(P^j \cdot F(A) = F(P^j \cdot A)\big) \wedge P^i \cdot F(A) \prec F(P^i \cdot A).$$

Indeed, $V_P(A) = A$ means that $A = P^t$ for some $t$ and $P^c \cdot F(P^t) \prec P^{c+1} \cdot F(P^t) \preceq F(P^{t+c})$. Furthermore, for $j \le c$, since $F$ is increasing, $F(A) \prec F(P \cdot A) \prec \cdots \prec F(P^j \cdot A)$ and we get $\deg(F(P^j \cdot A)) \ge \deg(F(A)) + j$, i.e., $F(P^j \cdot A) \succeq P^j \cdot F(A)$. So $(E_i)_{i\in\{1,\dots,c\}}$ makes a partition of

$P^{\mathbb{N}}$, roughly speaking $A$ belongs to $E_i$ if the first time we get a strict inequality when comparing the degree of $P^j \cdot F(A)$ and $F(P^j \cdot A)$ is $P^i \cdot F(A) \prec F(P^i \cdot A)$ (and we know that it always occurs for some $i \leq c$). Now we show that condition (4) is satisfied. Observe that if $P^s$ belongs to $E_i$ for some $i \geq 2$, then $P^{s+1}$ belongs to $E_{i-1}$. Denote by $\mu(s)$ the unique integer $i$ such that $P^s$ belongs to $E_i$. We have either $\mu(s) > 1$ and $\mu(s+1) = \mu(s) - 1$, or $\mu(s) = 1$ and $\mu(s+1) \geq 1$. Hence if $P^s$ and $P^t$ belong to $E_i$, $s < t$ and $i \in \{1, \dots, c\}$, then there exists $j$ such that $s \leq j < t$ and $P_j \in E_1$. Therefore, we get $F(P^s) \preceq F(P^j) \prec P \cdot F(P^j) \prec F(P^{j+1}) \preceq F(P^t)$ and one can notice that $P \cdot F(P^j)$ belongs to $P^{\mathbb{N}} \setminus F(P^{\mathbb{N}})$. □

## 4. Multiplication is $\mathcal{P}$-definable

In this section, we fix a triple $\mathcal{P} = (P, (E_i)_{i \in \{1,\dots,c\}}, F)$ where $P$ is a polynomial of degree at least 1, $(E_i)_{i \in \{1,\dots,c\}}$ is a finite partition of $P^{\mathbb{N}}$ and $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ is an increasing map such that (4) is satisfied. As pointed out in [12], similar proof techniques are discussed in [4] and [11].

**Definition 6.** A subset $\mathcal{T}$ of $(\mathbb{F}[X])^d$ is *$\mathcal{P}$-definable* if there exists a first-order formula $\phi(A_1, \dots, A_d)$ in the language $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, F, (E_i)_{i \in \{1,\dots,c\}} \rangle$ which is satisfied if and only if $(A_1, \dots, A_d)$ belongs to $\mathcal{T}$. As usual we can extend this notion to relations and maps.

First we define some useful $\mathcal{P}$-definable functions leading to the main theorem of this section (Theorem 10) expressing that multiplication of polynomials is $\mathcal{P}$-definable.

**Definition 7.** Let $i \in \{1, \dots, c\}$. The map $K_i : P^{\mathbb{N}} \times E_i \to P^{\mathbb{N}}$ is defined by

$$K_i(A, B) = F^{m_{A,B}}(S(F(B)))$$

where $S(F(B))$ is the polynomial of minimal degree in $\{C \mid \deg(C) > \deg(F(B))\} \cap (P^{\mathbb{N}} \setminus F(P^{\mathbb{N}}))$ and $m_{A,B}$ is the smallest positive integer such that $A \preceq F^{m_{A,B}}(S(F(B)))$. Note that such a definition is legitimate, (4) implies that $P^{\mathbb{N}} \setminus F(P^{\mathbb{N}})$ is infinite. Hence the polynomial $S(F(B))$ exists. Furthermore, since $F$ is increasing with respect to $\prec$, the integer $m_{A,B}$ exists too.

**Proposition 7.** *Let $i \in \{1, \dots, c\}$. The map $K_i$ is $\mathcal{P}$-definable and, for all $A \in P^{\mathbb{N}}$, the map $K_{i,A} : E_i \to P^{\mathbb{N}}, B \mapsto K_i(A, B)$ is one-to-one and has $A$ as a lower bound with respect to $\prec$.*

*Proof.* From the definition of $K_i$, for all polynomials $A \in P^{\mathbb{N}}$, we have

$$A \preceq K_i(A, B). \tag{6}$$

Let us show that the map $K_{i,A}(B) : B \mapsto K_{i,A}(B) = K_i(A, B)$ is one-to-one. Take $B, B' \in E_i$ such that $K_{i,A}(B) = K_{i,A}(B')$. We have $F^{m_{A,B}}(S(F(B))) = F^{m_{A,B'}}(S(F(B')))$ but since the increasing map $F$ is also one-to-one, we get

$$F^{\max\{m_{A,B} - m_{A,B'}, 0\}}(S(F(B))) = F^{\max\{m_{A,B'} - m_{A,B}, 0\}}(S(F(B'))).$$

Since $S$ and $F$ have disjoint codomains, then $S(F(B)) = S(F(B'))$. Again (4) means that the map $S$ restricted to $F(E_i)$ is one-to-one and therefore $B = B'$.

Let $i \in \{1, \dots, c\}$. To conclude with the proof, let us show that $K_i$ is $\mathcal{P}$-definable. The fact that $S(B) = C$, i.e., $C$ is the polynomial of minimal degree in $\{C \mid \deg(C) > \deg(B)\} \cap (P^{\mathbb{N}} \setminus F(P^{\mathbb{N}}))$ is $\mathcal{P}$-definable by the formula

$$\begin{aligned} & V_P(C) = C \wedge B \prec C \wedge (\forall A)(V_P(A) = A \to C \neq F(A)) \\ \wedge \quad & (\forall T)\big[\big(V_P(T) = T \wedge B \prec T \wedge (\forall A)(V_P(A) = A \to T \neq F(A))\big) \to C \preceq T\big]. \end{aligned}$$

Assuming $A \in P^{\mathbb{N}}$ and $B \in E_i$, consider the following formula $\varphi_1(A, B, U)$ where $X_{P,1}$ is introduced in Definition 4

$$X_{P,1}(S(F(B)), U) \wedge X_{P,1}(F(S(F(B))), U) \wedge (\forall V)(V \prec A \wedge X_{P,1}(V, U) \to X_{P,1}(F(V), U)).$$

If this formula holds true[1], then the $P$-expansion of $U$ has coefficient 1 occurring in particular for the following powers of $P$: $S(F(B)), F(S(F(B))), F(F(S(F(B)))), \dots, F^{m_{A,B}}(S(F(B)))$. Also obverse that the polynomial $Z = S(F(B)) + F(S(F(B))) + F(F(S(F(B)))) + \cdots + F^{m_{A,B}}(S(F(B)))$

[1] The reader may notice that such a formula give also some insight about the coefficient of some other powers of $P$ in the $P$-expansion of $U$ but our aim is to focus on some particular powers of $P$ occurring in the $P$-expansion.

is such that $\varphi_1(A,B,Z)$ holds true. Notice that for $A,B$ given, such a polynomial $Z$ is of minimal degree.

Assuming $A \in P^{\mathbb{N}}$ and $B \in E_i$, the formula $\varphi_2(A,B,U) \equiv (\forall W)(\varphi_1(A,B,W) \to U \preceq W)$ holds true if and only if $\varphi_1(A,B,W)$ is satisfied for no polynomial $W$ of degree less than $U$. Hence the fact that the formula $\varphi_1 \wedge \varphi_2$ holds for $(A,B,U)$ implies that $U$ has the same degree as $F^{m_{A,B}}(S(F(B)))$.

Now consider the formula $\varphi_3(C,U) \equiv X_{P,1}(C,U) \wedge (\forall Y)(X_{P,1}(Y,U) \to Y \preceq C)$. It holds true if and only if $C$ is the largest power of $P$ occurring in the $P$-expansion of $U$ with a coefficient 1. Finally observe that $C = F^{m_{A,B}}(S(F(B)))$ is $\mathcal{P}$-definable by the formula

$$V_P(A) = A \wedge B \in E_i \wedge (\exists U)(\varphi_1(A,B,U) \wedge \varphi_2(A,B,U) \wedge \varphi_3(C,U)).$$

□

**Definition 8.** We define the map $K : P^{\mathbb{N}} \times (\mathbb{F}[X])^c \to \mathbb{F}[X], (U,B_1,\ldots,B_c) \mapsto \sum_{P^j \preceq U} P_j P^j$ where, for all $j \in \mathbb{N}$ such that $P^j \preceq U$, $P_j$ is the unique polynomial of degree less than $\deg(P)$ such that

$$\bigwedge_{i=1}^{c} [P^j \in E_i \to X_{P,P_j}(K_i(U,P^j),B_i)]$$

where $X_{P,P_j}$ was given in Definition 4.

**Proposition 8.** *The map $K$ given above is $\mathcal{P}$-definable.*

*Proof.* The graph of $K$ given by

$$\{(U,B_1,\ldots,B_c,L) \in P^{\mathbb{N}} \times (\mathbb{F}[X])^{c+1} \mid K(U,B_1,\ldots,B_c) = L\}$$

is $\mathcal{P}$-definable with the following formula:

$$V_P(U) = U \wedge L \prec U \cdot P \wedge (\forall V)\left[\bigwedge_{i=1}^{c} (V \in E_i \wedge V \preceq U \to \bigwedge_{J \prec P} (X_{P,J}(V,L) \leftrightarrow X_{P,J}(K_i(U,V),B_i)))\right].$$

□

We now define a map sending a polynomial $B$ onto the largest power of $P$ not larger than $\deg(B)$. The special case of the polynomial $B = 0$ is also taken into account.

**Definition 9.** We define the map $L : \mathbb{F}[X] \to P^{\mathbb{N}}, B \mapsto \max(\{1\} \cup \{Q \in P^{\mathbb{N}} \mid Q \preceq B\})$.

**Proposition 9.** *The map $L$ given above is $\mathcal{P}$-definable.*

*Proof.* The fact that $L(B) = C$ is defined by

$$(B = 0 \wedge C = 1) \vee (V_P(C) = C \wedge C \preceq B \prec C \cdot P).$$

□

**Definition 10.** In the language $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, F, (E_i)_{i \in \{1,\ldots,c\}} \rangle$, we consider the formula $\kappa(T)$ given as:

$$(\forall U)(\forall V)(\forall W) \bigwedge_{i=1}^{c} \Big(W \in E_i \wedge X_{P,1}(U,T) \wedge X_{P,1}(V,T) \wedge U \succ V \succeq W \to U \succ K_i(V,W)\Big).$$

Assume that $\kappa(T)$ holds true. Let $U$ and $V$ be two arbitrary powers of $P$ such that $\deg(U) > \deg(V)$ and the $P$-expansion of $T$ has a coefficient 1 occurring for $U$ and $V$. Then the degree of $U$ is greater than the degree of all polynomials in

$$\bigcup_{i=1}^{c} \{K_i(V,W) \mid W \in E_i, W \preceq V\}.$$

**Theorem 10.** *The multiplication of polynomials $\{(A,B,C) \in \mathbb{F}[X] \mid A.B = C\}$ is a ternary $\mathcal{P}$-definable relation.*

*Proof.* We will build a formula $\varphi(A,B,C)$ in $\langle \mathbb{F}[X],+,\prec,(\cdot C : C\in\mathbb{F}[X]),V_P,F,(E_i)_{i\in\{1,\ldots,c\}}\rangle$ such that $\varphi(A,B,C)$ holds true if and only if $AB=C$. We may assume that $A,B,C$ are non-zero (this case can easily be treated separately). Consider the $P$-expansions $B$ as $B=\sum_{n=0}^{N}B_nP^n$ with $B_N\neq 0$.

For all $i\in\{1,\ldots,c\}$, there exists (at least) one polynomial $Y_i$ satisfying

$$X_{P,B_n}(K_i(L(B),P^n),Y_i)$$

for all $P^n\in E_i$ such that $n\leq N$. Indeed, the only constraint on $Y_i$ is that its $P$-expansion has some specific coefficients $B_n$ for some particular powers of $P$, namely the $K_i(L(B),P^n)$ for all $P^n\in E_i$ such that $n\leq N$. Hence these facts can be summarized by considering the following formula

$$(\exists Y_1)\cdots(\exists Y_c)[K(L(B),Y_1,\ldots,Y_c)=B].$$

For each coefficient of the $P$-expansion of $B$ corresponds exactly the same coefficient (for a power of $P$ determined by one of the $K_i$'s) in the $P$-expansion of one of the $Y_i$'s. We say that the coefficients of the $P$-expansion of $B$ are *coded* in a part of the coefficients of the $P$-expansion of the polynomials $Y_1,\ldots,Y_c$. In the same way, we can code the coefficients of a $P$-expansion[2] of the zero polynomial in a part of the coefficients of the $P$-expansion of the polynomials $Z_1,\ldots,Z_c$ with

$$(\exists Z_1)\cdots(\exists Z_c)[K(L(B),Z_1,\ldots,Z_c)=0].$$

Consider the following two finite sequences of polynomials:

$$\begin{array}{l}
0,\\
A\cdot B_N,\\
A\cdot B_N\cdot P+A\cdot B_{N-1},\\
A\cdot B_N\cdot P^2+A\cdot B_{N-1}\cdot P+A\cdot B_{N-2},\\
\vdots\\
A\cdot B_N\cdot P^N+A\cdot B_{N-1}\cdot P^{N-1}+A\cdot B_{N-2}\cdot P^{N-2}+\cdots+A\cdot B_0=A\cdot B
\end{array}$$

and

$$\begin{array}{l}
B,\\
B-B_N\cdot P^N,\\
B-B_N\cdot P^N-B_{N-1}\cdot P^{N-1},\\
\vdots\\
B-B_N\cdot P^N-B_{N-1}\cdot P^{N-1}-\cdots-B_0=0.
\end{array}$$

Observe that the two above formulas code the first term of these two sequences.

Assume that we have a polynomial satisfying

$$\lambda(T)\equiv\kappa(T)\wedge(\forall E)(X_{P,1}(E,T)\rightarrow L(B)\preceq E)\wedge X_{P,1}(L(B),T).$$

Consider two polynomials $U,V$ such that $V\prec U$, $X_{P,1}(U,T)\wedge X_{P,1}(V,T)$ and $(\forall W)(V\prec W\prec U\rightarrow\neg(X_{P,1}(W,T)))$. Recall that coefficients occurring in a $P$-expansion are exactly the polynomial of degree less than $\deg(P)$. Consider the following formula for some polynomial $J$ of degree less than $\deg(P)$:

$$X_{P,J}[L(K(V,W_1,\ldots,W_c)),K(V,W_1,\ldots,W_c)]\rightarrow\xi_1\wedge\xi_2\wedge\xi_3\wedge\xi_4\wedge\xi_5 \tag{7}$$

where the polynomials $W_i$ are used to code a third sequence of polynomials. Furthermore, we first have to set

$$(\exists W_1)\cdots(\exists W_c)[K(L(B),W_1,\ldots,W_c)=B].$$

[2] We can consider here any expansion of the kind $0=\sum_{t=0}^{\ell}C_iP^i$ where all $C_i=0$. Indeed, the greedy expansion given in Definition 3 does not allow such an expansion.

Let us describe the five formulas $\xi_i$'s. The first one is the case where the $P$-expansion of $B$ does not contain any 0.

$$\begin{aligned}
\xi_1 \equiv \Big[&K(V,Y_1,\dots,Y_c)=K(V,W_1,\dots,W_c)\wedge \\
&L(K(V,W_1,\dots,W_c)) \preceq P\cdot(K(V,W_1,\dots,W_c)-J\cdot L(K(V,W_1,\dots,W_c)))\Big] \quad \to \\
\Big[&K(U,Z_1,\dots,Z_c)=K(V,Z_1,\dots,Z_c)\cdot P+J\cdot A\wedge \\
&K(U,Y_1,\dots,Y_c)=K(V,Y_1,\dots,Y_c)-J\cdot L(K(V,Y_1,\dots,Y_c))\wedge \\
&K(U,W_1,\dots,W_c)=K(V,W_1,\dots,W_c)-J\cdot L(K(V,W_1,\dots,W_c))\Big].
\end{aligned}$$

This means that if $J$ is the leading coefficient in the $P$-expansion of $K(V,Y_1,\dots,Y_c)$, then the polynomials $K(U,Z_1,\dots,Z_c)$ and $K(U,Y_1,\dots,Y_c)$ are respectively equal to $K(V,Z_1,\dots,Z_c)\cdot P+J\cdot A$ and $K(V,Y_1,\dots,Y_c)-J\cdot L(K(V,Y_1,\dots,Y_c))$. Hence if $K(V,Z_1,\dots,Z_c)$ and $K(V,Y_1,\dots,Y_c)$ are two corresponding terms in the two sequences of polynomials defined above, then $K(U,Z_1,\dots,Z_c)$ and $K(U,Y_1,\dots,Y_c)$ are the next terms in these sequences. Actually we are coding the coefficients of some polynomials of these sequences in terms of the previous ones. Those codings are made through some coefficients of $Y_1,\dots,Y_c,Z_1,\dots,Z_c$. Note that the successive iterations of the coding do not lead to any contradiction. It is a consequence of the fact that $T$ satisfies $\kappa(T)$ and the maps $B\mapsto K_i(A,B)$ has $A$ as a lower bound with respect to $\prec$. Finally, the extra polynomials $W_1,\dots,W_c$ are of no real use in this situation where the $P$-expansion of $B$ does not contain any 0.

The second case is the one where the $P$-expansion of the polynomial $B$ has a zero coefficient for $L(K(V,W_1,\dots,W_c))/P$. We use the polynomials $W_i$ in particular to keep trace of $J$. Note that $(J-J/P)\cdot L(K(V,W_1,\dots,W_c))$ exists because $L(K(V,W_1,\dots,W_c))$ is non-constant and $K(V,W_1,\dots,W_c)\neq J\cdot L(K(V,W_1,\dots,W_c))$ furthermore it is easily definable. Note that for the next iteration $K(U,Y_1,\dots,Y_c)\neq K(U,W_1,\dots,W_c)$. Here is the formula:

$$\begin{aligned}
\xi_2 \equiv \Big[&K(V,Y_1,\dots,Y_c)=K(V,W_1,\dots,W_c)\wedge \\
&L(K(V,W_1,\dots,W_c)) \succ P\cdot(K(V,W_1,\dots,W_c)-J\cdot L(K(V,W_1,\dots,W_c)))\wedge \\
&K(V,W_1,\dots,W_c)\neq J\cdot L(K(V,W_1,\dots,W_c))\Big] \quad \to \\
\Big[&K(U,Z_1,\dots,Z_c)=K(V,Z_1,\dots,Z_c)\cdot P+J\cdot A\wedge \\
&K(U,Y_1,\dots,Y_c)=K(V,Y_1,\dots,Y_c)-J\cdot L(K(V,Y_1,\dots,Y_c))\wedge \\
&K(U,W_1,\dots,W_c)=K(V,W_1,\dots,W_c)-(J-J/P)\cdot L(K(V,W_1,\dots,W_c))\Big].
\end{aligned}$$

As a third case, we consider the case where the $P$-expansion of $B$ has several consecutive zeros and therefore we will deal several times with this case (after taking $\xi_2$ into account). Note that $K(U,Z_1,\dots,Z_c)=K(V,Z_1,\dots,Z_c)\cdot P$ and $K(U,Y_1,\dots,Y_c)=K(V,Y_1,\dots,Y_c)$ because in the situation described here the coefficient at this stage is zero. Here is the formula:

$$\begin{gathered}\xi_3 \equiv \Big[K(V,Y_1,\dots,Y_c) \neq K(V,W_1,\dots,W_c)\wedge \\ L(K(V,W_1,\dots,W_c)) \succ P\cdot(K(V,W_1,\dots,W_c) - J\cdot L(K(V,W_1,\dots,W_c)))\Big] \quad \to \\ \Big[K(U,Z_1,\dots,Z_c) = K(V,Z_1,\dots,Z_c)\cdot P\wedge \\ K(U,Y_1,\dots,Y_c) = K(V,Y_1,\dots,Y_c)\wedge \\ K(U,W_1,\dots,W_c) = K(V,W_1,\dots,W_c) - (J - J/P)\cdot L(K(V,W_1,\dots,W_c))\Big].\end{gathered}$$

Now consider the case where we have dealt with $\xi_2$ and possibly one or several times with $\xi_3$ during the previous iterations but we are back to a simple situation where $K(U,Y_1,\dots,Y_c) = K(U,W_1,\dots,W_c)$. Observe that $K(U,Z_1,\dots,Z_c) = K(V,Z_1,\dots,Z_c)\cdot P$ and $K(U,Y_1,\dots,Y_c) = K(V,Y_1,\dots,Y_c)$ because in the situation described here the coefficient at this stage is again zero. Here is the formula:

$$\begin{gathered}\xi_4 \equiv \Big[K(V,Y_1,\dots,Y_c) \neq K(V,W_1,\dots,W_c)\wedge \\ L(K(V,W_1,\dots,W_c)) \preceq P\cdot(K(V,W_1,\dots,W_c) - J\cdot L(K(V,W_1,\dots,W_c)))\Big] \quad \to \\ \Big[K(U,Z_1,\dots,Z_c) = K(V,Z_1,\dots,Z_c)\cdot P\wedge \\ K(U,Y_1,\dots,Y_c) = K(V,Y_1,\dots,Y_c)\wedge \\ K(U,W_1,\dots,W_c) = K(V,W_1,\dots,W_c) - J\cdot L(K(V,W_1,\dots,W_c))\Big].\end{gathered}$$

Finally, when $K(V,W_1,\dots,W_c) = J\cdot L(K(V,W_1,\dots,W_c))$, we consider the following formula where one can assume (as it will be discussed at the end of the proof) that $V_P(B) = 1$. Indeed as discussed below we can avoid the situation where $K(V,Y_1,\dots,Y_c) \neq K(V,W_1,\dots,W_c)$ and $K(V,W_1,\dots,W_c) = J\cdot L(K(V,W_1,\dots,W_c))$. So we consider the formula:

$$\begin{gathered}\xi_5 \equiv \Big[K(V,Y_1,\dots,Y_c) = K(V,W_1,\dots,W_c)\wedge \\ K(V,W_1,\dots,W_c) = J\cdot L(K(V,W_1,\dots,W_c))\Big] \quad \to \\ \Big[K(U,Z_1,\dots,Z_c) = K(V,Z_1,\dots,Z_c)\cdot P + J\cdot A \wedge K(U,Y_1,\dots,Y_c) = 0\Big].\end{gathered}$$

One has therefore to consider the formula (7) with a conjunction on all the possible $J \prec P$ and quantifying over all polynomials $U$ and $V$ verifying the conditions described above. Proceeding this way, we can code the two sequences as soon as we have a polynomial $T$ satisfying $\lambda(T)$ and having enough coefficients 1 in its $P$-expansion. But such conditions can always be fulfilled.

To conclude with the proof, we have two complementary cases to take into account. As a first case, if $B$ is not a multiple of $P$, then the second sequence $(B, B - B_N\cdot P^N,\dots)$ is eventually equal to zero only for the last term of the sequence. One has therefore to quantify the existence of a polynomial $T$ such that

$$K(U,Y_1,\dots,Y_c) = 0 \to K(U,Z_1,\dots,Z_c) = C.$$

Let $\omega(A,B,C)$ be the formula we just have constructed. If $B$ is not a multiple of $P$, the formula holds true if and only if $AB = C$. Now, if $B$ is a multiple of $P$, then the second sequence is equal to zero before its last term. The trick is to replace $B$ by $B+1$ (hence $B+1$ is not a multiple of $P$) and $C$ by $C+A$. In that case, $B+1$ is non-zero and if $C+A = 0$ then we don't have $AB = C$.

We can thus consider the formula

$$[V_P(B) = 1 \to \omega(A, B, C)] \wedge [V_P(B) \neq 1 \to \omega(A, B + 1, C + A) \wedge C + A \neq 0].$$

□

**Corollary 11.** *For all polynomials $Q$ of degree at least 1, the map $V_Q$ is $\mathcal{P}$-definable.*

*Proof.* Assume that $Q$ is written as $Q_1^{\alpha_1} \cdots Q_n^{\alpha_n}$ where the $Q_i$'s are non-constant irreducible pairwise distinct polynomials and the $\alpha_i$'s are positive integers. Recall that $Q$ is given once and for all. In particular, $n$ and $\deg(Q_i^{\alpha_i})$ are known constants for all $i = 1, \ldots, n$. Thus the following formula is finite and well-defined. For $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, the formula $V_Q(A) = A$ holds if and only if

$$(\exists B_1) \cdots (\exists B_n)\big[A = B_1 \cdots B_n \wedge \bigwedge_{i=1}^{n} ((\forall C_i)(C_i \mid B_i \to C_i \simeq 1 \vee Q_i \mid C_i))$$
$$\wedge \bigwedge_{i=1}^{n-1} B_i^{\deg(Q_{i+1}^{\alpha_{i+1}})} \simeq B_{i+1}^{\deg(Q_i^{\alpha_i})}\big] \wedge \mathrm{Deg}_{\deg Q}(A)$$

where $D \mid E$ means that $D$ divides $E$ which can be defined using multiplication (and this operation is $\mathcal{P}$-definable thanks to Theorem 10) and recall that $A \simeq B$ is a shorthand for $\deg(A) = \deg(B)$, i.e., $A \preceq B \wedge B \preceq A$. The central part of the formula stipulates that $B_i$ is a power of $Q_i$ for all $i = 1, \ldots, n$. The extra condition $\mathrm{Deg}_{\deg Q}(A)$ on the degree of $A$ (see Definition 5 and note that this predicate is $\mathcal{P}$-definable) is to avoid a problem arising when $\gcd(\alpha_1, \ldots, \alpha_n) = p > 1$, because therefore $Q^{1/p}$ is a polynomial whose powers are satisfied by the formula. As an example, for $Q = X^2$ (and $n = 1$), the formula without this extra condition would be satisfied not only for $1, X^2, X^4, \ldots$ but also wrongly for $X, X^3, X^5, \ldots$.

For an arbitrary finite field $\mathbb{F}$, the formula described above can also be satisfied for polynomials of the kind $kQ^t$ where $k \in \mathbb{F}$. This problem can easily be solved using again $\mathrm{Deg}_k$ and $\mathrm{Pre}_C$.

It is now easy to consider the formula $V_Q(A) = B$:

$$(V_Q(B) = B) \wedge B|A \wedge (\forall C)((V_Q(C) = C \wedge C \mid A) \to C \preceq B).$$

□

## 5. Multiplication is $(S, T)$-definable

We are now able to prove the main result of this paper which was already stated in the introduction as Theorem 1.

**Lemma 2.** *Let $P \in \mathbb{F}[X]$ be a non-constant polynomial and $m > 0$ be an integer. A subset of $(\mathbb{F}[X])^n$ is $P$-definable if and only if it is $P^m$-definable.*

*Proof.* In [7], it is proved that a set $\mathcal{T}$ is $P$-recognizable if and only if it is $P^m$-recognizable and in [8], it is proved that $\mathcal{T}$ is $P$-recognizable if and only if it is $P$-definable. An alternative proof (see [13]) is to show that $V_{P^m}$ is $P$-definable and $V_P$ is $P^m$-definable. □

**Theorem.** *Let $S$ and $T$ be two non-zero multiplicatively independent polynomials with coefficients in a finite field $\mathbb{F}$. Then multiplication of polynomials is a ternary relation*

$$\{(A, B, C) \in \mathbb{F}[X] \mid A.B = C\}$$

*definable by a first-order formula in $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_S, V_T\rangle$.*

*Proof.* Since $S$ and $T$ are two non-zero multiplicatively independent polynomials, by Theorem 6 there exist two multiplicatively independent polynomials $P, Q \in S^{\mathbb{N}} \cup T^{\mathbb{N}}$, an increasing map $F : P^{\mathbb{N}} \to P^{\mathbb{N}}$ and a finite partition $(E_i)_{i \in \{1,\ldots,c\}}$ of $P^{\mathbb{N}}$ which are $(P, Q)$-definable and such that, for all $i \in \{1, \ldots, c\}$ and all $A, B \in E_i$,

$$A \prec B \to \exists C \in (P^{\mathbb{N}} \setminus F(P^{\mathbb{N}})) : F(A) \prec C \prec F(B).$$

Considering the corresponding triple $\mathcal{P} = (P, (E_i)_{i\in\{1,\ldots,c\}}, F)$, the multiplication is $\mathcal{P}$-definable by Theorem 10 and therefore definable in $\langle \mathbb{F}[X], +, \prec, (\cdot C : C \in \mathbb{F}[X]), V_P, V_Q\rangle$. We can conclude using the previous lemma: $V_P$ and $V_Q$ are respectively $S$-definable and $T$-definable. Hence multiplication is $(S, T)$-definable. □

## References

[1] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and $p$-recognizable sets of integers, *Bull. Belg. Math. Soc.* **1** (1994), 191–238.

[2] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, *Math. Systems Theory* **3** (1969), 186–192.

[3] F. Durand, M. Rigo, On Combham's theorem, to appear in *Handbook of Automata: from Mathematics to Applications*, European Math. Society Publishing house.

[4] C.C. Elgot, M.O. Rabin, Decidability and undecidability of extensions of second (first) order theory pf (generalized) successor, *J. Symbolic Logic* **32** (1966), 169–181.

[5] C. Michaux, R. Villemaire, Presburger arithmetic and recognizability of sets of natural numbers by automata: new proofs of Cobham's and Semenov's theorems, *Ann. Pure Appl. Logic* **77** (1996), 251-277.

[6] An. A. Muchnik, The definable criterion for definability in Presburger arithmetic and its applications, *Theoret. Comput. Sci.* **290** (2003), 1433-1444.

[7] M. Rigo, Syntactical and automatic properties of sets of polynomials over finite fields, *Finite Fields Appl.* **14** (2008), 258–276.

[8] M. Rigo, L. Waxweiler, Logical characterization of recognizable sets of polynomials over a finite field, to appear in *Int. J. Found. Comput. Sci.*.

[9] A. L. Semenov, The Presburger nature of predicates that are regular in two number systems, *Sibirsk. Mat. Ž.* **18** (1977), 403-418.

[10] A. Sirokofskich, On an exponential predicate in polynomials over finite fields, *Proc. Amer. Math. Soc.* **138** (2010), 2569–2583.

[11] W. Thomas, A note on undecidable extensions of monadic second order successor arithmetic, *Arch. Math. Logik Grundlagenforsch* **17** (1975), 43–44.

[12] R. Villemaire, The theory of $\langle \mathbf{N}, +, V_k, V_l\rangle$ is undecidable, *Theoret. Comput. Sci.* **106** (1992), 337–349.

[13] L. Waxweiler, *Caractère reconnaissable d'ensembles de polynômes à coefficients dans un corps fini*, Ph. D. thesis, University of Liège, December 2009, `http://orbi.ulg.ac.be/handle/2268/11381`

University of Liège,
Department of Mathematics,
Grande traverse 12 (B37)
B-4000 Liège,
Belgium
M.Rigo@ulg.ac.be