Congruence Preserving Functions on Free Monoids

Patrick Cégielski[1,4], Serge Grigorieff[2,4], Irène Guessarian[2,3,4,*]

Abstract

A function on an algebra is congruence preserving if, for any congruence, it maps congruent elements to congruent elements. We show that, on a free monoid generated by at least three letters, a function from the free monoid into itself is congruence preserving if and only if it is of the form $x \mapsto w_0 x w_1 \cdots w_{n-1} x w_n$ for some finite sequence of words $w_0, \ldots, w_n$. We generalize this result to functions of arbitrary arity. This shows that a free monoid with at least three generators is a (noncommutative) affine complete algebra. As far as we know, it is the first (nontrivial) case of a noncommutative affine complete algebra.

Keywords: Congruence Preservation, Free Monoid, Affine Completeness
2010 MSC: 08A30, 08B20

Contents

*Corresponding author
Email addresses: `cegielski@u-pec.fr` (Patrick Cégielski), `seg@irif.fr` (Serge Grigorieff), `ig@irif.fr` (Irène Guessarian)
[1]LACL, EA 4219, Université Paris-Est Créteil, IUT Sénart-Fontainebleau
[2]IRIF, UMR 8243, CNRS & Université Paris 7 Denis Diderot
[3]Emeritus at UPMC Université Paris 6.
[4]This work was partially supported by TARMAC ANR agreement 12 BS02 007 01.

1. Introduction

We here focus on functions which are congruence preserving on free monoids generated by at least 3 letters. Given an algebra $\mathcal{A} = \langle A, \Omega \rangle$ (where Ω is a family of operations on the set A), a function $f : A^k \to A$ is said to be *congruence preserving* if for every congruence $\sim$ on $\langle A, \Omega \rangle$ and for every $x_1, \ldots, x_k, y_1, \ldots, y_k \in A$, $x_1 \sim y_1, \ldots, x_k \sim y_k$ implies $f(x_1, \ldots, x_k) \sim f(y_1, \ldots, y_k)$. Such functions were introduced in Grätzer [6], where they are said to have the "substitution property."

Let $O(\mathcal{A})$ be the family of all operations (of any arity) on A. A *clone* on A is a subfamily of $O(\mathcal{A})$ containing all projections and closed under composition. An important problem is to compare two particular clones associated to an algebra $\langle A, \Omega \rangle$, namely,

- the smallest clone $Pol(\mathcal{A})$ which contains Ω and all constant functions (the so-called "polynomial functions" by reference to the case of rings),
- the clone $CP(\mathcal{A})$ of congruence preserving functions on A.

Obviously, we have $Pol(\mathcal{A}) \subseteq CP(\mathcal{A}) \subseteq O(A)$. Are these inclusions strict?

In 1921, Kempner [9] showed that $Pol(\mathcal{A}) = O(A)$ holds for the ring $\mathbb{Z}/n\mathbb{Z}$ if and only if n is prime. More recently, since [4], the main concern is whether all congruence preserving functions are polynomial, i.e. $Pol(\mathcal{A}) \stackrel{?}{=} CP(\mathcal{A})$. Algebras where all congruence preserving functions are polynomial are called *affine complete* in the terminology introduced by Werner [12]. They are extensively studied in the book by Kaarli & Pixley [8].

Our main results (Theorems 3.6 and 4.5) prove that if Σ has at least three elements, then the free monoid Σ^* generated by Σ is affine complete. As far as we know, our result provides the first (nontrivial) case of a noncommutative affine complete algebra.

In the commutative case, quite a few algebras have been shown to be affine complete: Boolean algebras (Grätzer, 1962 [4]), p-rings with unit (Iskander, 1972 [7]), vector spaces of dimension at least 2 (Heinrich Werner, 1971 [12]), free modules with more than one free generator (Nöbauer, 1978 [10]), hence also abelian groups. Grätzer, 1964 [5], determined which distributive lattices are affine complete. Bhargava, 1997 [1], proved that the ring $\mathbb{Z}/n\mathbb{Z}$ is affine complete if and only if neither 8 nor any p^2 with p odd prime divides n. When $Pol(\mathcal{A})$ is a strict subfamily of $CP(\mathcal{A})$, the question is how to describe the family $CP(\mathcal{A})$. For distributive lattices, this is done in Haviar & Ploščica, 2008 [11].

Even for such a simple arithmetical algebra as $\mathcal{A} = \langle \mathbb{N}, Suc \rangle$ (where Suc is the successor function), the description of $CP(\mathcal{A})$ involves nontrivial number theory. Indeed, for the algebra $\langle \mathbb{N}, Suc \rangle$ a function $f : \mathbb{N} \to \mathbb{N}$ is congruence preserving if and only if $f(x) \geq x$ and f has the following property: $x - y$ divides $f(x) - f(y)$ for all $x, y \in \mathbb{N}$. In [2] we proved that this property holds if and only if

$$f(x) = \sum_{k\in\mathbb{N}} a_k \binom{x}{k} = a_0 + a_1 x + a_2 \frac{x(x-1)}{2!} + a_3 \frac{x(x-1)(x-2)}{3!} + \cdots$$

where a_k is divided by ℓ for all $2 \leq \ell \leq k$. This result also applies to the expansions of $\langle \mathbb{N}, Suc\rangle$ having the same congruences, e.g. one can expand $\langle \mathbb{N}, Suc\rangle$ with $+$ and $\times$. In [3] we gave a similar characterization of congruence preserving functions on the algebra $\langle \mathbb{Z}, +, \times\rangle$.

To give a flavor of the nontrivial character of congruence preserving functions, let us recall some examples given in our papers [2, 3] of congruence preserving functions $f : \mathbb{N} \to \mathbb{N}$

$$\begin{aligned} f(x) &= \texttt{if } x = 0 \texttt{ then } 1 \texttt{ else } \lfloor ex! \rfloor \quad (e = 2,718\ldots \text{ is the Euler number}),\\ f(x) &= \lfloor e^{1/a} a^x x! \rfloor \quad \text{for } a \in \mathbb{N} \setminus \{0, 1\},\\ f(x) &= \texttt{if } x \in 2\mathbb{N} \texttt{ then } \lfloor \cosh(1/2)\, 2^x\, x! \rfloor \texttt{ else } \lfloor \sinh(1/2)\, 2^x\, x! \rfloor, \end{aligned}$$

and of a Bessel like congruence preserving function $f : \mathbb{Z} \to \mathbb{Z}$

$$f(x) = \texttt{if } x \geq 0 \texttt{ then } \frac{\Gamma(1/2)}{2 \times 4^x \times x!} \int_1^\infty e^{-t/2}(t^2 - 1)^x dt \texttt{ else } -f(-x).$$

It might seem counter-intuitive that, when Σ^* has many generators, the congruence preserving functions are fewer and much simpler than when Σ^* has a unique generator; this stems from the fact that, when Σ^* has a unique generator, Σ^* is isomorphic to the additive group $\mathbb{N}$, which has very few congruences, hence a lot of functions can preserve these few congruences.

After recalling basic definitions in Section 2, we prove in Section 3 that, if Σ has at least three elements, then the only congruence preserving functions from the free monoid Σ^* into itself are those defined by terms with parameters, namely functions of the form $x \mapsto w_0 x w_1 x w_2 \cdots x w_n$ (Theorem 3.6). In Section 4, we extend this result by characterizing congruence preserving functions of arbitrary arity $k \in \mathbb{N}$ (Theorem 4.5). We show that k-ary congruence preserving functions are of the form $(x_1, \ldots, x_k) \mapsto w_0 x_{i_1} w_1 x_{i_2} w_2 \cdots x_{i_n} w_n$ with $x_{i_j} \in \{x_1, \ldots, x_k\}$ for $j = 1, \ldots, n$, i.e. they are defined by terms with parameters. A shorter proof of Theorem 4.5 is given in Section 5 when Σ is infinite.

2. Classical definitions and notations

Recall the notion of congruence on an algebra.

Definition 2.1. A congruence $\sim$ on an algebra $\langle A, \Omega\rangle$ is an equivalence relation on A such that, for every operation $\xi \colon A^k \to A$ of Ω, for all $x_1, \ldots, x_k, y_1, \ldots, y_k \in A$

$$x_i \sim y_i \text{ for } i = 1, \ldots, k \qquad \Longrightarrow \qquad \xi(x_1, \ldots, x_k) \sim \xi(y_1, \ldots, y_k)$$

Definition 2.2. Let $\mathcal{A} = \langle A, \Omega \rangle$ be an algebra and $\sim$ a congruence on $\mathcal{A}$. A function $f : A^k \to A$ is said to *preserve the congruence* $\sim$ if for all $x_1, \ldots, x_k, y_1, \ldots, y_k$ in A,

$$x_i \sim y_i \text{ for } i = 1, \ldots, k \quad \Longrightarrow \quad f(x_1, \ldots, x_k) \sim f(y_1, \ldots, y_k).$$

Definition 2.3. Let $\mathcal{A} = \langle A, \Omega \rangle$ be an algebra. A function $f : A^k \to A$ is *congruence preserving* (abbreviated into CP) if it preserves all congruences on $\mathcal{A}$.

Remark 2.4. 1) A function f is congruence preserving if and only if every congruence on the algebra $\langle A, \Omega \rangle$ is also a congruence on the expanded algebra $\langle A, \Omega \cup \{f\} \rangle$.

2) Grätzer's denomination for congruence preservation is "*substitution property*." (See [6] Chap. I, §8, after Lemma 9, page 44.) Some authors also use the denomination "*congruence compatible*."

Definition 2.5. Let Σ be a nonempty set. The *free monoid* Σ^* generated by Σ is the monoid $\langle \Sigma^*, \cdot \rangle$
– whose elements are all the finite sequences (or words) of elements from Σ,
– with the concatenation operation: $x_1 \cdots x_n \cdot y_1 \cdots y_p = x_1 \cdots x_n y_1 \cdots y_p$,
– whose unit element is the empty word denoted by ε.

For $x \in \Sigma^*$ and $n \in \mathbb{N}$, the word obtained by concatenating n copies of x is denoted by x^n.

Remark 2.6. The notions of *CP function* and *morphism* are different.

(i) The function $x \mapsto x^2$ is CP but is not a morphism.

(ii) Let $\Sigma = \{a, b\}$, let φ be defined by $\varphi\colon a \mapsto a$ and $\varphi\colon b \mapsto a$, then φ is a morphism but it is not CP. Indeed, let $\sim_a$ be the congruence on Σ^* defined by $x \sim_a y$ if and only if x and y have the same number of occurrences of a. Then $a \sim_a ab$ but $\varphi(a) \not\sim_a \varphi(ab)$.

3. Unary congruence preserving functions on free monoids with at least three generators

Recall first the classical relation between congruences and kernels of surjective homomorphisms.

Proposition 3.1. *A binary relation $\sim$ on an algebra $\langle \mathcal{A}, \Omega \rangle$ is a congruence if and only if there exists some algebra $\langle \mathcal{P}, \Omega' \rangle$, where Ω and Ω' have the same signature, and a surjective homomorphism $\theta\colon A \to P$ such that $\sim$ is the kernel $Ker(\theta)$ of θ, i.e. $\sim\, = \{(x, y) \mid \theta(x) = \theta(y)\}$. Moreover, $\langle \mathcal{P}, \Omega \rangle$ is isomorphic to the quotient algebra $\langle \mathcal{A}, \Omega \rangle / \sim$.*

In an algebra any term (possibly involving elements from the algebra) defines a congruence preserving function. We detail the case of Σ^* in Lemma 3.2.

Lemma 3.2. *All unary functions* $\Sigma^* \to \Sigma^*$ *of the form* $x \mapsto p(x) = w_0 x w_1 x w_2 \cdots x w_n$, *with* $w_0, \ldots, w_n \in \Sigma^*$, *are CP.*

Proof. Any congruence $\sim$ on Σ^* is the kernel of some morphism φ from Σ^* into some monoid, i.e. $x \sim y$ if and only if $\varphi(x) = \varphi(y)$. Let φ be a morphism and $\sim$ the associated congruence. Assume $\varphi(x) = \varphi(y)$, then

$$\begin{aligned}\varphi(p(x)) = \varphi(w_0 x w_1 x w_2 \cdots x w_n) &= \varphi(w_0)\varphi(x)\varphi(w_1)\varphi(x)\varphi(w_2)\cdots\varphi(x)\varphi(w_n)\\ &= \varphi(w_0)\varphi(y)\varphi(w_1)\varphi(y)\varphi(w_2)\cdots\varphi(y)\varphi(w_n)\\ &= \varphi(w_0 y w_1 y w_2 \cdots y w_n) = \varphi(p(y)),\end{aligned}$$

hence $p(x) \sim p(y)$ and p is CP. □

It turns out that the converse is true for CP functions $\Sigma^* \to \Sigma^*$ when Σ has at least three letters. We use restricted notions of congruences obtained by looking at particular monoids. To such a restricted notion of congruence is associated an *a priori* enlarged notion of congruence preservation. In the next definition, we describe a particular form of restricted congruence which is crucial in our proof of Theorem 3.6.

Definition 3.3. A congruence on Σ^* is said to be *restricted* if it is the kernel of a morphism $\Sigma^* \to \Sigma^*$. A function preserving restricted congruences is said to be *RCP*.

Example 3.4. For $a \in \Sigma$, let $\varphi \colon \Sigma^* \mapsto \langle \mathbb{Z}/2\mathbb{Z}, \times \rangle$ be the morphism defined by $\varphi(a) = 0$ and $\varphi(x) = 1$ for $x \in \Sigma \setminus \{a\}$. The kernel of φ corresponds to the congruence "a occurs in x if and only if a occurs in y." It is not a restricted congruence.

Using the above notion, we can prove Theorem 3.5 below.

Theorem 3.5. *Assume* $|\Sigma| \geq 3$. *A function* $f \colon \Sigma^* \to \Sigma^*$ *is RCP if and only if it is of the form* $f(x) = w_0 x w_1 x \cdots w_{n-1} x w_n$ *for some* $w_0, \ldots, w_n \in \Sigma^*$.

Theorem 3.5 implies the following characterization of CP functions.

Theorem 3.6. *Assume* $|\Sigma| \geq 3$. *A function* $f \colon \Sigma^* \to \Sigma^*$ *is CP if and only if it is of the form* $f(x) = w_0 x w_1 x \cdots w_{n-1} x w_n$ *for some* $w_0, \ldots, w_n \in \Sigma^*$.

Proof. The "if" part follows from Lemma 3.2.

For the "only if" part, observe that if f is CP, then it is RCP; hence Theorem 3.5 implies the "only if" part. □

The rest of this section is devoted to the proof of Theorem 3.5, which shall be given after Lemma 3.16.

Notation 3.7. *1) For u in Σ^* and $a \in \Sigma$, let $|u|$ denote the length of u and let $|u|_a$ denote the number of occurrences of a in u.*

2) For $c \in \Sigma$, let $\sim_c$ be the kernel of the morphism $\theta_c \colon \Sigma^* \to \Sigma^*$ such that $\theta_c(c) = c$ and $\theta_c(x) = \varepsilon$ for all $x \neq c$ in Σ. Thus $u \sim_c v$ if and only if $|u|_c = |v|_c$.

Lemma 3.8. *If f is RCP on Σ^* and $a, b \in \Sigma$, then*
(1) $|u| = |v|$ implies $|f(u)| = |f(v)|$.
(2) $|u|_a = |v|_a$ implies $|f(u)|_a = |f(v)|_a$.
(3) $b \neq a$ implies $|f(a^n)|_b = |f(\varepsilon)|_b$.

Proof. (1) Let $\sim$ be the kernel of the morphism $\varphi \colon \Sigma^* \to \Sigma^*$ such that $\varphi(x) = a$ for all x in Σ: $u \sim v$ if and only if $|u| = |v|$. As f is RCP, $u \sim v$ implies $f(u) \sim f(v)$, hence $|f(u)| = |f(v)|$.
(2) Similar to the proof of (1) where $\sim$ is replaced by $\sim_a$.
(3) As for $b \neq a$, $|a^n|_b = |\varepsilon|_b$, this follows from (2). □

Thanks to Lemma 3.8, the following notation makes sense.

Notation 3.9. *Let f be RCP. Denote by $\ell(n)$ the common length of $f(x)$ for x of length n and by $\ell_a(n)$ the number of occurrences of the letter a in the word $f(x)$ for $|x|_a = n$, i.e. for x with n occurrences of a.*

Lemma 3.10. *If f is RCP on Σ^* with Σ containing at least two letters a, b, then the functions $\ell \colon \mathbb{N} \to \mathbb{N}$ and $\ell_a \colon \mathbb{N} \to \mathbb{N}$ defined by Notation 3.9 are affine and of the form*

$$\ell(n) = \big(\ell(1) - \ell(0)\big)n + \ell(0) \quad , \quad \ell_a(n) = \big(\ell(1) - \ell(0)\big)n + \ell_a(0).$$

Thus, letting $p_f = \ell(1) - \ell(0)$ and $e_f = \ell(0) = |f(\varepsilon)|$, we have, for all $x \in \Sigma^*$,

$$|f(x)| = p_f|x| + e_f = p_f|x| + |f(\varepsilon)| \quad , \quad |f(x)|_a = p_f|x|_a + |f(\varepsilon)|_a. \tag{1}$$

Proof. 1) Note that $|z| = \sum_{\alpha\in\Sigma} |z|_\alpha$. Applying this to $f(a^n)$ we get

$$\begin{aligned}
\ell(n) &= |f(a^n)| \\
&= \textstyle\sum_{b\in\Sigma} |f(a^n)|_b \\
&= \ell_a(n) + \textstyle\sum_{b\in\Sigma\setminus\{a\}} |f(\varepsilon)|_b \qquad \text{by Lemma 3.8 (3)} \\
&= \ell_a(n) - |f(\varepsilon)|_a + \textstyle\sum_{b\in\Sigma} |f(\varepsilon)|_b = \ell_a(n) - \ell_a(0) + |f(\varepsilon)| \\
&= \ell_a(n) - \ell_a(0) + \ell(0),
\end{aligned}$$

which yields

$$\ell(n) - \ell(0) = \ell_a(n) - \ell_a(0). \tag{2}$$

2) Let us now take $x = a^{n-1}b$ (recall Σ has at least two letters).

$$\begin{aligned}
\ell(n) &= |f(a^{n-1}b)| = |f(a^{n-1}b)|_a + |f(a^{n-1}b)|_b + \textstyle\sum_{c\neq a,b} |f(a^{n-1}b)|_c \\
&= \ell_a(n-1) + \ell_b(1) + \textstyle\sum_{c\neq a,b} |f(\varepsilon)|_c \\
&= (\ell_a(n-1) - \ell_a(0)) + (\ell_b(1) - \ell_b(0)) + \textstyle\sum_{c\in\Sigma} |f(\varepsilon)|_c \\
&= (\ell_a(n-1) - \ell_a(0)) + (\ell_b(1) - \ell_b(0)) + |f(\varepsilon)| \\
&= (\ell(n-1) - \ell(0)) + (\ell(1) - \ell(0)) + \ell(0) \qquad \text{by equation (2)} \\
&= \ell(n-1) + (\ell(1) - \ell(0)), \\
\ell(n) &= n(\ell(1) - \ell(0)) + \ell(0) \qquad \text{by induction on } n.
\end{aligned}$$

Letting $p_f = \ell(1) - \ell(0)$, we have $\ell(n) = np_f + \ell(0) = np_f + |f(\varepsilon)|$. Similarly, applying equation (2), we have $\ell_a(n) = \ell(n) + \ell_a(0) - \ell(0) = np_f + \ell_a(0) = p_f n + |f(\varepsilon)|_a$. □

Notation 3.11. *For $c, d \in \Sigma$ let $\varphi_{d,c}$ denote the morphism identifying d with c: $\varphi_{d,c}(d) = c$ and $\varphi_{d,c}(x) = x$ for $x \neq d$.*

Lemma 3.12. *Assume Σ contains at least two letters and $f : \Sigma^* \to \Sigma^*$ is RCP. If there is some $u \neq \varepsilon$ such that $f(u) = \varepsilon$, then f is constant on Σ^* with value ε.*

Proof. By equation (1) of Lemma 3.10, we have $|f(x)| = p_f|x| + e_f$ for all $x \in \Sigma^*$. In particular, $0 = |\varepsilon| = |f(u)| = p_f|u| + e_f$, hence $p_f = e_f = 0$. Thus, $|f(x)| = 0$ and $f(x) = \varepsilon$ for all x. □

We now show that if the first letter of $f(x)$ is b for *some letter* $x \in \Sigma$ different from b, then the same is true for *every word* $x \in \Sigma^*$.

Lemma 3.13. *Assume $|\Sigma| \geq 3$ and $f : \Sigma^* \to \Sigma^*$ is RCP. If there are $a, b \in \Sigma$ such that $a \neq b$ and $f(a) \in b\Sigma^*$, then $f(x) \in b\Sigma^*$ for all words $x \in \Sigma^*$.*

Proof. We first prove that $f(c) \in b\Sigma^*$ for all $c \in \Sigma$. We argue by cases and use the morphisms identifying letters defined in Notation 3.11.

• *Case $c \notin \{a, b\}$.* Since $\varphi_{a,c}(a) = \varphi_{a,c}(c)$ we have $\varphi_{a,c}(f(a)) = \varphi_{a,c}(f(c))$. As the first letter of $f(a)$ is b which is not in $\{a, c\}$, it is equal to the first letter of $\varphi_{a,c}(f(a))$. As $\varphi_{a,c}(f(a)) = \varphi_{a,c}(f(c))$, the first letter of $\varphi_{a,c}(f(c))$ is b, hence the first letter of $f(c)$ must also be b. Thus, $f(c) \in b\Sigma^*$.

• *Case $c = a$.* Trivial since condition $f(a) \in b\Sigma^*$ is our assumption.

• *Case $c = b$.* We know (by the two previous cases) that $f(x) \in b\Sigma^*$ for all $x \in A \setminus \{b\}$. As $|\Sigma| \geq 3$ there exists $d \notin \{a, b\}$. Let $x \in \{a, d\}$. Observe that $\varphi_{x,b}(d) = \varphi_{x,b}(b)$, whence

$\varphi_{x,b}(f(d)) = \varphi_{x,b}(f(b))$. As $f(x) \in b\Sigma^*$, we get $f(b) \in \{x, b\}\Sigma^*$, for both $x = a$ and $x = d$. Thus, $f(b) \in \{a, b\}\Sigma^* \cap \{d, b\}\Sigma^* = b\Sigma^*$.

We next prove by induction on $n = |x|$ that $f(x) \in b\Sigma^*$ for all words $x \in \Sigma^*$.

• *Base case $n = 1$:* The case $n = 1$ coincides with what was proved above.

• *Base case $n = 0$:* Since $|\Sigma| \geq 3$, there are $c, d \in \Sigma$ such that b, c, d are pairwise distinct. The base case $n = 1$ insures that $f(c) = bu$ and $f(d) = bv$ for some $u, v \in \Sigma^*$. For $c \in \Sigma$ let $\psi_c : \Sigma^* \to \Sigma^*$ be the morphism which erases c, i.e. $\psi_c(c) = \varepsilon$ and $\psi_c(x) = x$ for every $x \in \Sigma \setminus \{c\}$. As $\psi_c(\varepsilon) = \psi_c(c)$, we have $\psi_c(f(\varepsilon)) = \psi_c(f(c)) = \psi_c(bu) = bs$ for some $s \in \Sigma^*$. Equality $\psi_c(f(\varepsilon)) = bs$ shows that $f(\varepsilon) \in c^*b\Sigma^*$. Arguing with ψ_d we similarly get $f(\varepsilon) \in d^*b\Sigma^*$. Thus, $f(\varepsilon) \in c^*b\Sigma^* \cap d^*b\Sigma^* = b\Sigma^*$.

• *Inductive step: from $\leq n$ to $n + 1$ where $n \geq 1$.* We assume that $f(y) \in b\Sigma^*$ for every $y \in \Sigma^*$ of length at most n. Let $x \in \Sigma^{n+1}$, we prove that $f(x) \in b\Sigma^*$. We argue by cases.

▶ *Case 1: $|\{c \in \Sigma \setminus \{b\} \mid c$ occurs in $x\}| \geq 2$.* Then $x = ucvdw$ where $u, v, w \in \Sigma^*$ and c, d, b are pairwise distinct letters in Σ. We consider the erasing morphisms ψ_c and ψ_d. As $|uvdw| = n$, the induction hypothesis yields $f(uvdw) = bt$ for some $t \in \Sigma^*$. Now, $\psi_c(x) = \psi_c(uvdw)$, hence $\psi_c(f(x)) = \psi_c(f(uvdw)) = \psi_c(bt) = bs$ for some $s \in \Sigma^*$. Equality $\psi_c(f(x)) = bs$ shows that $f(x) \in c^*b\Sigma^*$. Arguing similarly with ψ_d and $ucvw$, we get $f(x) \in d^*b\Sigma^*$. Thus, $f(x) \in c^*b\Sigma^* \cap d^*b\Sigma^* = b\Sigma^*$.

▶ *Case 2: c is the unique letter in $\Sigma \setminus \{b\}$ which occurs in x and it occurs at least twice.* Then $x = ucvcw$ where $u, v, w \in \Sigma^*$. As $|\Sigma| \geq 3$, there exists $d \notin \{b, c\}$. The word $ucvdw$ is relevant to the previous *Case 1*, hence $f(ucvdw) = bt$ for some $t \in \Sigma^*$. We consider the morphism $\varphi_{d,c}$ which identifies d with c. We have $\varphi_{d,c}(ucvdw) = x = \varphi_{d,c}(x)$. Hence $\varphi_{d,c}(f(x)) = \varphi_{d,c}(f(ucvdw)) = \varphi_{d,c}(bt) = bs$ for some $s \in \Sigma^*$. Since $b \notin \{c, d\}$, equality $\varphi_{d,c}(f(x)) = bs$ shows that $f(x) \in b\Sigma^*$.

▶ *Case 3: c is the unique letter in $\Sigma \setminus \{b\}$ which occurs in x and it occurs only once.* Then $x = b^k cb^\ell$ where $k + \ell = n \geq 1$. The word c^{n+1} is relevant to *Case 2*, hence $f(c^{n+1}) = bt$ for some $t \in \Sigma^*$. Consider the morphism $\varphi_{c,b}$ which identifies b with c. We have $\varphi_{c,b}(x) = \varphi_{c,b}(c^{n+1})$. Hence $\varphi_{c,b}(f(x)) = \varphi_{c,b}(f(c^{n+1})) = \varphi_{c,b}(bt) = bs$ for some $s \in \Sigma^*$. Equality $\varphi_{c,b}(f(x)) = bs$ shows that $f(x) \in \{b, c\}\Sigma^*$.

As $|\Sigma| \geq 3$, there exists $d \notin \{b, c\}$. Let y be obtained from x by replacing the first occurrence of b by d. The word y is relevant to *Case 1*, hence $f(y) = bt$ for some $t \in \Sigma^*$. Consider the morphism $\varphi_{d,b}$ which identifies d with b. We have $\varphi_{d,b}(y) = x = \varphi_{d,b}(x)$. Hence $\varphi_{d,b}(f(x)) = \varphi_{d,b}(f(y)) = \varphi_{d,b}(bt) = bs$ for some $s \in \Sigma^*$. Equality $\varphi_{d,b}(f(x)) = bs$ shows that $f(x) \in \{b, d\}\Sigma^*$. Thus, $f(x) \in \{b, c\}\Sigma^* \cap \{b, d\}\Sigma^* = b\Sigma^*$.

▶ *Case 4: $x = b^{n+1}$.* As $|\Sigma| \geq 3$, there exist $c, d \in \Sigma$ such that b, c, d are pairwise distinct. The words $b^n c$ and $b^n d$ are relevant to *Case 3*, hence $f(b^n c) = bt$ and $f(b^n d) = bs$ for some $s, t \in \Sigma^*$. Consider the morphism $\varphi_{c,b}$ which identifies c with b. We have

$\varphi_{c,b}(b^n c) = x = \varphi_{c,b}(x)$. Hence $\varphi_{c,b}(f(x)) = \varphi_{c,b}(f(b^n c)) = \varphi_{c,b}(bt) = br$ for some $r \in \Sigma^*$, whence $f(x) \in \{b, c\}\Sigma^*$. Arguing similarly with $b^n d$ and the morphism $\varphi_{d,b}$ which identifies d with b, we get $f(x) \in \{b, d\}\Sigma^*$. Thus, $f(x) \in \{b, c\}\Sigma^* \cap \{b, d\}\Sigma^* = b\Sigma^*$. □

We now show that if x is a prefix of $f(x)$ for every letter $x \in \Sigma$, then the same is true for every word $x \in \Sigma^*$.

Lemma 3.14. *Assume $|\Sigma| \geq 3$ and $f : \Sigma^* \to \Sigma^*$ is RCP. If $f(a) \in a\Sigma^*$ for all $a \in \Sigma$, then $f(x) \in x\Sigma^*$ for all $x \in \Sigma^*$.*

Proof. We argue by induction on the length of x.
Base case $|x| = 0$. Condition $f(\varepsilon) \in \varepsilon\Sigma^*$ is trivial.
Base case $|x| = 1$. This is our assumption.
Inductive step: from $n \geq 1$ to $n + 1$. Assuming $f(x_1 \cdots x_n) \in x_1 \cdots x_n\Sigma^*$ for all $x_1, \ldots,$ $x_n \in \Sigma$ and letting $x_{n+1} = b$, we prove $f(x_1 \cdots x_n b) \in x_1 \cdots x_n b\Sigma^*$ for all $x_1, \ldots, x_n, b \in \Sigma$. We distinguish two cases $b \neq x_n$ and $b = x_n$.

Case 1: *If $b \neq x_n$, then $f(x_1 \cdots x_{n-1}x_n b) \in x_1 \cdots x_{n-1}x_n b\Sigma^*$.*
Let $x_1 \cdots x_{n-1} = x_n^{\ell_0} y_1 x_n^{\ell_1} \cdots y_p x_n^{\ell_p}$ with $y_1, \ldots, y_p \in \Sigma \setminus \{x_n\}$ and $p, \ell_0, \ldots, \ell_p \in \mathbb{N}$. Let us show that there are $k_0, \ldots, k_p \in \mathbb{N}$ and $w \in \Sigma^*$ such that

$$f(x_1 \cdots x_{n-1}x_n b) = f(x_n^{\ell_0} y_1 x_n^{\ell_1} \cdots y_p x_n^{\ell_p} x_n b) = x_n^{k_0} y_1 x_n^{k_1} \cdots y_{p-1} x_n^{k_{p-1}} y_p x_n^{k_p} bw. \qquad (3)$$

Indeed, since $|x_1 \cdots x_{n-1}b| = n$, we have $f(x_1 \cdots x_{n-1}b) \in x_1 \cdots x_{n-1}b\Sigma^*$ by the induction hypothesis. Thus, $f(x_1 \cdots x_{n-1}b) = x_1 \cdots x_{n-1}bu = x_n^{\ell_0} y_1 x_n^{\ell_1} \cdots y_p x_n^{\ell_p} bu$ for some $u \in \Sigma^*$. Let $\psi : \Sigma^* \to \Sigma^*$ be the morphism which erases x_n, i.e. $\psi(x_n) = \varepsilon$ and $\psi(y) = y$ for $y \in \Sigma \setminus \{x_n\}$. We have $\psi(x_1 \cdots x_{n-1}x_n b) = \psi(x_1 \cdots x_{n-1}b)$, hence $\psi(f(x_1 \cdots x_{n-1}x_n b)) = \psi(f(x_1 \cdots x_{n-1}b)) = \psi(x_n^{\ell_0} y_1 x_n^{\ell_1} \cdots y_p x_n^{\ell_p} bu) = y_1 y_2 \ldots y_p b\psi(u)$. Thus, $f(x_1 \cdots x_{n-1}x_n b)$ is obtained by inserting some occurrences of x_n in $y_1 y_2 \cdots y_p b\psi(u)$, hence equation (3) holds.

As $|\Sigma| \geq 3$, there is c such that $c \notin \{b, x_n\}$. Let $\varphi : \Sigma^* \to \Sigma^*$ be the morphism such that $\varphi(b) = bc$, $\varphi(c) = x_n bc$, and $\varphi(y) = y$ for $y \in \Sigma \setminus \{b, c\}$. We have $\varphi(x_n b) = \varphi(c)$, hence $\varphi(x_1 \cdots x_{n-1}x_n b) = \varphi(x_1 \cdots x_{n-1}c)$. Thus $\varphi(f(x_1 \cdots x_{n-1}x_n b)) = \varphi(f(x_1 \cdots x_{n-1}c))$. Applying φ to equation (3)

$$\begin{aligned} \varphi(f(x_1 \cdots x_{n-1}x_n b)) &= \varphi(x_n^{k_0} y_1 x_n^{k_1} \cdots y_{p-1} x_n^{k_{p-1}} y_p x_n^{k_p} bw) \\ &= x_n^{k_0} \varphi(y_1) x_n^{k_1} \cdots \varphi(y_p) x_n^{k_p} bc\varphi(w). \end{aligned} \qquad (4)$$

As $|x_1 \cdots x_{n-1}c| = n$, by the induction hypothesis for length n, there is $u \in \Sigma^*$ such that

$$f(x_1 \cdots x_{n-1}c) = x_1 \cdots x_{n-1}cu = x_n^{\ell_0} y_1 x_n^{\ell_1} \cdots y_p x_n^{\ell_p} cu.$$

Hence

$$\varphi(f(x_1\cdots x_{n-1}c))=\varphi(x_n^{\ell_0}y_1x_n^{\ell_1}\cdots y_px_n^{\ell_p}cu)=x_n^{\ell_0}\varphi(y_1)x_n^{\ell_1}\cdots\varphi(y_p)x_n^{\ell_p}x_nbc\varphi(u). \qquad (5)$$

As $\varphi(f(x_1\cdots x_{n-1}x_nb))=\varphi(f(x_1\cdots x_{n-1}c))$, we infer from Equations (4) and (5)

$$x_n^{k_0}\varphi(y_1)x_n^{k_1}\varphi(y_2)x_n^{k_2}\cdots\varphi(y_p)x_n^{k_p}bc\varphi(w)=x_n^{\ell_0}\varphi(y_1)x_n^{\ell_1}\varphi(y_2)x_n^{\ell_2}\cdots\varphi(y_p)x_n^{\ell_p}x_nbc\varphi(u)$$

Since $y_1\neq x_n$, the word $\varphi(y_1)$ contains a letter distinct from x_n and the last equality implies $k_0=\ell_0$. Thus $x_n^{k_1}\varphi(y_2)x_n^{k_2}\cdots\varphi(y_p)x_n^{k_p}bc\varphi(w)=x_n^{\ell_1}\varphi(y_2)x_n^{\ell_2}\cdots\varphi(y_p)x_n^{\ell_p}x_nbc\varphi(u)$. Iterating the previous argument we get $k_i=\ell_i$ for $i=0,\ldots,p-1$ and the residual equality $x_n^{k_p}bc\varphi(w)=x_n^{\ell_p}x_nbc\varphi(u)$. This last equality implies $k_p=\ell_p+1$. Thus,

$$\begin{aligned} f(x_1\cdots x_{n-1}x_nb) &= x_n^{k_0}y_1x_n^{k_1}\cdots y_{p-1}x_n^{k_{p-1}}y_px_n^{k_p}bw\\ &= x_n^{\ell_0}y_1x_n^{\ell_1}\cdots y_{p-1}x_n^{\ell_{p-1}}y_px_n^{\ell_p}x_nbw\\ &= x_1\cdots x_{n-1}x_nbw. \end{aligned}$$

Case 2: *If $b=x_n$, then $f(x_1\cdots x_{n-1}bb)\in x_1\cdots x_{n-1}bb\Sigma^*$.*
Let $a\in\Sigma\backslash\{b\}$ and consider the morphism $\varphi_{a,b}$ identifying a with b. As $\varphi_{a,b}(x_1\cdots x_{n-1}bb)=\varphi_{a,b}(x_1\cdots x_{n-1}ba)$, we have $\varphi_{a,b}(f(x_1\cdots x_{n-1}bb))=\varphi_{a,b}(f(x_1\cdots x_{n-1}ba))$. As $a\neq b$, we can apply Case 1 which implies that $f(x_1\cdots x_{n-1}ba)=x_1\cdots x_{n-1}baw$ for some $w\in\Sigma^*$. Thus,

$$\varphi_{a,b}(f(x_1\cdots x_{n-1}bb)) \;=\; \varphi_{a,b}(x_1\cdots x_{n-1}baw) \;=\; \varphi_{a,b}(x_1\cdots x_{n-1})bb\varphi_{a,b}(w),$$

hence

$$f(x_1\cdots x_{n-1}bb) \;\in\; \varphi_{a,b}^{-1}(\varphi_{a,b}(x_1\cdots x_{n-1}))\{aa,ab,ba,bb\}\Sigma^*.$$

Similarly, let $c\notin\{a,b\}$. Considering the morphism $\varphi_{c,b}$ which identifies c with b, we get

$$f(x_1\cdots x_{n-1}bb) \;\in\; \varphi_{c,b}^{-1}(\varphi_{c,b}(x_1\cdots x_{n-1}))\{cc,cb,bc,bb\}\Sigma^*.$$

Let $z=z_1\cdots z_{n-1}$ be the length $n-1$ prefix of $f(x_1\cdots x_{n-1}bb)$. As $\varphi_{a,b}$ and $\varphi_{c,b}$ preserve length, $z\in\varphi_{a,b}^{-1}(\varphi_{a,b}(x_1\cdots x_{n-1}))\cap\varphi_{c,b}^{-1}(\varphi_{c,b}(x_1\cdots x_{n-1}))$. Since $z\in\varphi_{a,b}^{-1}(\varphi_{a,b}(x_1\cdots x_{n-1}))$, $z_i\in\{a,b\}\Leftrightarrow x_i\in\{a,b\}$ and $z_i\notin\{a,b\}\Rightarrow z_i=x_i$. Similarly, $z\in\varphi_{c,b}^{-1}(\varphi_{c,b}(x_1\cdots x_{n-1}))$ implies that $z_i\in\{c,b\}\Leftrightarrow x_i\in\{c,b\}$ and $z_i\notin\{c,b\}\Rightarrow z_i=x_i$. Thus,
- if $z_i=b$, then both z_i and x_i are in $\{a,b\}\cap\{c,b\}=\{b\}$ and $z_i=x_i=b$,
- if $z_i\neq b$, then either $z_i\notin\{a,b\}$ or $z_i\notin\{c,b\}$, and in both cases $z_i=x_i$.
This proves that $z=x_1\cdots x_{n-1}$.

Finally, the two letters of $f(x_1\cdots x_{n-1}bb)$ which follow z are in $\{aa,ab,ba,bb\}\cap\{cc,cb,bc,bb\}=\{bb\}$. Thus, $f(x_1\cdots x_{n-1}bb)\in x_1\cdots x_{n-1}bb\Sigma^*$ and Case 2 is proved, finishing the proof of the Lemma. □

As a corollary of Lemmata 3.12, 3.13 and 3.14, we get

Lemma 3.15. *Assume* $|\Sigma| \geq 3$ *and* $f\colon \Sigma^* \to \Sigma^*$ *is RCP. Exactly one of the below three conditions holds:*

(C_1) either there exists $b \in \Sigma$ *such that* $f(x) \in b\Sigma^*$ *for all* $x \in \Sigma^*$*,*
(C_2) or $f(x) \in x\Sigma^*$ *for all* $x \in \Sigma^*$*,*
(C_3) or f *is constant on* Σ^* *with value* ε*.*

The proof of Theorem 3.5 relies on the property of RCP functions which is stated in the next Lemma 3.16.

Lemma 3.16. *Assume* $|\Sigma| \geq 3$ *and* $f\colon \Sigma^* \to \Sigma^*$ *is RCP and such that either* $f(x) = ag(x)$ *for all* $x \in \Sigma^*$*, or* $f(x) = xg(x)$ *for all* $x \in \Sigma^*$*. Then* g *is also RCP.*

Proof. For $\varphi\colon \Sigma^* \to \Sigma^*$ a morphism, $\varphi(x) = \varphi(y)$ implies $\varphi(f(x)) = \varphi(f(y))$. If $f(z) = ag(z)$ for all $z \in \Sigma^*$, then $\varphi(a)\varphi(g(x)) = \varphi(a)\varphi(g(y))$. Cancelling the common prefix $\varphi(a)$, we get $\varphi(g(x)) = \varphi(g(y))$. Similarly, if $f(z) = zg(z)$ for all $z \in \Sigma^*$, we conclude by cancelling the common prefix $\varphi(x)$. □

Proof of Theorem 3.5. The sufficiency of the condition follows from Lemma 3.2.
We now prove the necessity of the condition:

$$\text{if } f \text{ is RCP, then it is of the form } f(x) = w_0 x w_1 x \cdots w_{n-1} x w_n. \tag{6}$$

We argue by induction on $p_f + e_f$, where p_f, e_f are defined in Lemma 3.10.
• *Basis:* If $p_f + e_f = 0$, then $p_f = e_f = 0$ and $f(x) = \varepsilon$ which is of the required form with $n = 0$ and $w_0 = \varepsilon$.
• *Induction:* Assume that condition (6) holds for every function h such that $p_h + e_h \leq m$ and let f be RCP with $p_f + e_f = m + 1$. We first note that, as $p_f + e_f \geq 1$, f cannot be the constant function with value ε. Hence, by Lemma 3.15, f is of the form $f(x) = ag(x)$ or $f(x) = xg(x)$. Moreover, by Lemma 3.16, g is RCP.
– If $f(x) = ag(x)$ for all $x \in \Sigma^*$, then $|f(x)| = 1 + |g(x)|$, $p_f = p_g$ and $e_f = e_g + 1$.
– If $f(x) = xg(x)$ for all $x \in \Sigma^*$, then $|f(x)| = |x| + |g(x)|$, $p_f = p_g + 1$ and $e_f = e_g$.
Hence in both cases $p_g + e_g = p_f + e_f - 1$. Thus, by the induction hypothesis, g is of the required form and so is f. □

4. Non-unary congruence preserving functions on free monoids with at least three generators

In the present Section we extend Theorem 3.6 and characterize CP functions $f\colon (\Sigma^*)^k \to \Sigma^*$ of arbitrary arity k (cf. Theorem 4.5). To this end we use the notion of *RCP k-ary function*. The idea of the proof is similar to the idea of the proof of Theorem 3.6.

Lemma 4.1. *Let $k \geq 1$, $f : (\Sigma^*)^k \to \Sigma^*$ be RCP, $u_1, \ldots, u_k, v_1, \ldots, v_k \in \Sigma^*$, $a, b \in \Sigma$ and $n_1, \ldots, n_k \in \mathbb{N}$.*
(1) $|u_i| = |v_i|$ for all $i \in \{1, \ldots, k\}$ implies $|f(u_1, \ldots, u_k)| = |f(v_1, \ldots, v_k)|$.
(2) $|u_i|_a = |v_i|_a$ for all $i \in \{1, \ldots, k\}$ implies $|f(u_1, \ldots, u_k)|_a = |f(v_1, \ldots, v_k)|_a$.
(3) $b \neq a$ implies $|f(a^{n_1}, \ldots, a^{n_k})|_b = |f(\varepsilon, \ldots, \varepsilon)|_b$.

Proof. Similar to the proof of Lemma 3.8. □

Thanks to Lemma 4.1 the following notations make sense.

Notation 4.2. *Let $k \geq 1$. Denote by $\vec{0}$ the k-tuple $(0, \ldots, 0)$ and by $\vec{e_1}, \ldots, \vec{e_k}$ the k-tuples $(1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$ respectively. If $k \geq 1$ and $f : (\Sigma^*)^k \to \Sigma^*$ is RCP, let*

$$\begin{aligned}
\ell(n_1, \ldots, n_k) &= \textit{common value of } |f(x_1, \ldots, x_k)| \textit{ with } (x_1, \ldots, x_k) \in \Sigma^{n_1} \times \cdots \times \Sigma^{n_k} \\
\ell_a(n_1, \ldots, n_k) &= \textit{common value of } |f(x_1, \ldots, x_k)|_a \textit{ with } |x_1|_a = n_1, \ldots, |x_k|_a = n_k \\
\Delta\ell(n_1, \ldots, n_k) &= \ell(n_1, \ldots, n_k) - \ell(\vec{0}) = \ell(n_1, \ldots, n_k) - |f(\varepsilon, \ldots, \varepsilon)| \\
\Delta\ell_a(n_1, \ldots, n_k) &= \ell_a(n_1, \ldots, n_k) - \ell_a(\vec{0})
\end{aligned}$$

Lemma 4.3. *If Σ contains at least two letters and $f : (\Sigma^*)^k \to \Sigma^*$ is RCP, then we have*

$$|f(x_1, \ldots, x_k)| = p_{f,1}|x_1| + \cdots + p_{f,k}|x_k| + e_f, \tag{7}$$

$$\textit{for all } a \in \Sigma \qquad |f(x_1, \ldots, x_k)|_a = p_{f,1}|x_1|_a + \cdots + p_{f,k}|x_k|_a + |f(\varepsilon, \ldots, \varepsilon)|_a, \tag{8}$$

with $p_{f,i} = \Delta\ell(\vec{e_i}) = \ell(\vec{e_i}) - \ell(\vec{0}) = |f(\overbrace{\varepsilon, \ldots, \varepsilon}^{(i-1)\ \textit{times}}, a, \varepsilon, \ldots, \varepsilon)| - |f(\varepsilon, \ldots, \varepsilon)|$
and $e_f = |f(\varepsilon, \ldots, \varepsilon)|$.

Proof. Observe that $|z| = \sum_{c \in \Sigma} |z|_c$. Using Notation 4.2, we have

$$\begin{aligned}
\ell(n_1, \ldots, n_k) &= |f(a^{n_1}, \ldots, a^{n_k})| = \sum_{b \in \Sigma} |f(a^{n_1}, \ldots, a^{n_k})|_b \\
&= |f(a^{n_1}, \ldots, a^{n_k})|_a + \sum_{b \in \Sigma \setminus \{a\}} |f(\varepsilon, \ldots, \varepsilon)|_b \quad \text{by Lemma 4.1 (3)}
\end{aligned}$$

$$
\begin{aligned}
&= \big(|f(a^{n_1},\ldots,a^{n_k})|_a - |f(\varepsilon,\ldots,\varepsilon)|_a\big) + \sum_{b\in\Sigma} |f(\varepsilon,\ldots,\varepsilon)|_b \\
&= \big(|f(a^{n_1},\ldots,a^{n_k})|_a - |f(\varepsilon,\ldots,\varepsilon)|_a\big) + |f(\varepsilon,\ldots,\varepsilon)| \\
&= \ell_a(n_1,\ldots,n_k) - \ell_a(\vec{0}) + \ell(\vec{0}), \qquad \text{hence}
\end{aligned}
$$

$$
\Delta\ell(n_1,\ldots,n_k) = \Delta\ell_a(n_1,\ldots,n_k). \tag{9}
$$

Now, let $\vec{x} = (x_1, x_2, \ldots, x_k) = (a^{n_1-1}b, a^{n_2}, \ldots, a^{n_k})$ with $a \neq b$ (possible as Σ has at least two letters). Then

$$
\begin{aligned}
\ell(n_1,\ldots,n_k) &= |f(a^{n_1-1}b, a^{n_2},\ldots,a^{n_k})| \\
&= |f(\vec{x})|_a + |f(\vec{x})|_b + \sum_{c\neq a,b} |f(\vec{x})|_c \\
&= \ell_a(n_1-1,n_2,\ldots,n_k) + \ell_b(\vec{e_1}) + \sum_{c\neq a,b} \ell_c(\vec{0}) \\
&= \Delta\ell_a(n_1-1,n_2,\ldots,n_k) + \Delta\ell_b(\vec{e_1}) + \sum_{c\in\Sigma} \ell_c(\vec{0}) \\
&= \Delta\ell_a(n_1-1,n_2,\ldots,n_k) + \Delta\ell_b(\vec{e_1}) + \ell(\vec{0}),
\end{aligned}
$$

$$
\begin{aligned}
\text{hence:} \quad \Delta\ell(n_1,\ldots,n_k) &= \Delta\ell_a(n_1-1,n_2,\ldots,n_k) + \Delta\ell_b(\vec{e_1}). \\
\text{Using (9),} \quad \Delta\ell(n_1,\ldots,n_k) &= \Delta\ell(n_1-1,n_2,\ldots,n_k) + \Delta\ell(\vec{e_1}). \\
\text{Iterating,} \quad \Delta\ell(n_1,\ldots,n_k) &= \Delta\ell(0,n_2,\ldots,n_k) + n_1\Delta\ell(\vec{e_1}). && (10) \\
\text{Similarly,} \quad \Delta\ell(0,n_2,\ldots,n_k) &= \Delta\ell(0,0,n_3,\ldots,n_k) + n_2\Delta\ell(\vec{e_2}). && (11) \\
&\;\;\vdots \\
\Delta\ell(0,0,\ldots,0,n_k) &= \Delta\ell(\vec{0}) + n_k\Delta\ell(\vec{e_k}) \;=\; n_k\Delta\ell(\vec{e_k}). && (12)
\end{aligned}
$$

Summing lines (10) to (12) gives:

$$
\Delta\ell(n_1,\ldots,n_k) = \sum_{i=1}^{i=k} n_i \Delta\ell(\vec{e_i}). \tag{13}
$$

Equality (13) together with Lemma 4.1 implies equation (7). Equation (8) then follows from equation (9). □

We use the characterization of unary CP functions $f\colon \Sigma^* \to \Sigma^*$ given in Theorem 3.6 to characterize k-ary CP functions $f\colon (\Sigma^*)^k \to \Sigma^*$ in Theorem 4.5. The key result for proving this characterization is Lemma 4.4, which extends Lemma 3.15 to arity $k \geq 2$.

Lemma 4.4. *Assume $|\Sigma| \geq 3$ and let $f\colon (\Sigma^*)^k \to \Sigma^*$ be RCP. Exactly one of the below three conditions holds*

(C_1) either there exists $b \in \Sigma$ such that $f(x_1, \ldots, x_k) \in b\Sigma^*$ for all $x_1, \ldots, x_k \in \Sigma^*$,
(C_2) or there exists $i \in \{1, \ldots, k\}$ such that $f(x_1, \ldots, x_k) \in x_i\Sigma^*$ for all $x_1, \ldots, x_k \in \Sigma^*$,
(C_3) or $f(x_1, \ldots, x_k)$ is constant with value ε for all $x_1, \ldots, x_k$.

Before proving Lemma 4.4, we first show how Lemma 4.4 together with Lemma 4.3 entails the following characterization of k-ary CP functions, extending Theorem 3.6.

Theorem 4.5. *Let $|\Sigma| \geq 3$. A function $f\colon (\Sigma^*)^k \to \Sigma^*$ is CP if and only if there exist $n \in \mathbb{N}$, $w_0, \ldots, w_n \in \Sigma^*$ and $i_j \in \{1, \ldots . k\}$ for $j = 1, \ldots, n$, such that for all $x_1, \ldots, x_k \in \Sigma^*$, $f(x_1, \ldots, x_k) = w_0 x_{i_1} w_1 x_{i_2} w_2 \cdots x_{i_n} w_n$.*

Proof. The "if" part (sufficiency of the condition) is clear as in the unary functions case.

For the "only if" part we first note that if f is CP, then it is RCP. We next prove that if f is RCP, then it is of the form stated in the Theorem. The proof is by induction on $p_{f,1} + p_{f,2} + \cdots + p_{f,k} + e_f$ where $|f(x_1, \ldots, x_k)| = p_{f,1}|x_1| + p_{f,2}|x_2| + \cdots + p_{f,k}|x_k| + e_f$ (cf. Lemma 4.3).

Basis: if $p_{f,1} + p_{f,2} + \cdots + p_{f,k} + e_f = 0$, then $p_{f,1} = \cdots = p_{f,k} = e_f = 0$ and $f(x_1, \ldots, x_k) = \varepsilon$ which is of the required form with $n = 0$ and $w_0 = \varepsilon$.

Induction: Otherwise, $p_{f,1} + p_{f,2} + \cdots + p_{f,k} + e_f \geq 1$ implies that $f \neq \varepsilon$. Thus, by Lemma 4.4, there exists an RCP function g such that
– either there exists $b \in \Sigma$ such that $f(x_1, \ldots, x_k) = bg(x_1, \ldots, x_k)$ for all $x_1, \ldots, x_k \in \Sigma^*$, hence $p_{f,i} = p_{g,i}$ for $i = 1, \ldots, k$ and $e_f = |f(\varepsilon, \ldots, \varepsilon)| = |g(\varepsilon, \ldots, \varepsilon)| + 1 = e_g + 1$,
– or there exists $i \in \{1, \ldots, k\}$ such that $f(x_1, \ldots, x_k) = x_i g(x_1, \ldots, x_k)$ for all $x_1, \ldots, x_k \in \Sigma^*$, then $p_{f,j} = p_{g,j}$ for all $j \neq i$, $p_{f,i} = p_{g,i} + 1$ and $e_f = e_g$.
In both cases $p_{g,1} + p_{g,2} + \cdots + p_{g,k} + e_g = p_{f,1} + p_{f,2} + \cdots + p_{f,k} + e_f - 1$. By the induction hypothesis, g is of the required form and so is f. □

The rest of this section is devoted to the proof of Lemma 4.4, which shall be given after Lemma 4.10. Lemmata 4.6 and 4.9 extend to arity k Lemmata 3.12 and 3.13 respectively. These two Lemmata deal with conditions (C_3) and (C_1) of Lemma 4.4 respectively.

Lemma 4.6. *Assume Σ has at least two letters and $f : (\Sigma^*)^k \to \Sigma^*$ is RCP. If there are $u_1 \neq \varepsilon, \ldots, u_k \neq \varepsilon$ such that $f(u_1, \ldots, u_k) = \varepsilon$, then f is constant with value ε.*

Proof. Similar to the proof of Lemma 3.12. Since $|f(u_1, \ldots, u_k)| = 0$ and no $|u_i|$ is null, equality $|f(u_1, \ldots, u_k)| = p_{f,1}|u_1| + \cdots + p_{f,k}|u_k| + e_f$ yields $p_{f,1} = \cdots = p_{f,k} = e_f = 0$, hence f is the constant ε. □

We now define functions obtained by "freezing" some arguments of a given function. Such functions will be used in the proofs of subsequent Lemmata.

Definition 4.7 (Freezing arguments)**.** Let $f\colon (\Sigma^*)^k \to \Sigma^*$. For $i \in \{1,\ldots,k\}$ and $u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k \in \Sigma^*$, we denote by $f_i^{v_1\cdots v_{i-1}v_{i+1}\cdots v_k}$ and $f^u_{1\cdots(i-1)(i+1)\cdots k}$ the unary and $k-1$-ary functions over Σ^* such that, for all $x, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k \in \Sigma^*$,

$$\begin{aligned} f_i^{v_1\cdots v_{i-1}v_{i+1}\cdots v_k}(x) &= f(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_k), \\ f^u_{1\cdots(i-1)(i+1)\cdots k}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) &= f(x_1, \ldots, x_{i-1}, u, x_{i+1}, \ldots, x_k). \end{aligned}$$

Lemma 4.8. *If $f\colon (\Sigma^*)^k \to \Sigma^*$ is RCP, then the functions $f_i^{v_1\cdots v_{i-1}v_{i+1}\cdots v_k}$ and $f^u_{1\cdots(i-1)(i+1)\cdots k}$ are also RCP for all $i \in \{1,\ldots,k\}$ and $u, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k \in \Sigma^*$.*

Proof. Straightforward. □

Lemma 4.9. *Let $|\Sigma| \geq 3$ and $f\colon (\Sigma^* \setminus \{\varepsilon\})^k \to \Sigma^*$ be RCP. Assume there exist $b \in \Sigma$ and $(x_1, \ldots, x_k) \in (\Sigma^* \setminus \{\varepsilon\})^k$ such that none of $x_1, \ldots, x_k$ has b as the first letter and $f(x_1, x_2, \ldots, x_k) \in b\Sigma^*$. Then $f(z_1, z_2, \ldots, z_k) \in b\Sigma^*$ for all $(z_1, z_2, \ldots, z_k) \in (\Sigma^*)^k$.*

Proof. By induction on k. *Base case:* $k = 1$. It follows from Lemma 3.15.
Induction. Let $k \geq 2$ and assume the Lemma holds for arities $n < k$. Let $\vec{x} = (x_2, \ldots, x_k)$. The function $f_1^{\vec{x}}$ is RCP by Lemma 4.8. As $x_1 \notin b\Sigma^*$ and $f_1^{\vec{x}}(x_1) = f(x_1, x_2, \ldots, x_k) \in b\Sigma^*$, Lemma 3.15 implies that $f_1^{\vec{x}}(z_1) \in b\Sigma^*$ for all $z_1 \in \Sigma^*$, hence also $f^{z_1}_{2\cdots k}(\vec{x}) = f(z_1, \vec{x}) = f_1^{\vec{x}}(z_1) \in b\Sigma^*$. As $f^{z_1}_{2\cdots k}$ is a $(k-1)$-ary RCP function by Lemma 4.8 and as the first letters of $x_2, \ldots, x_k$ are all different from b, the induction hypothesis insures that $f^{z_1}_{2\cdots k}(z_2, \ldots, z_k) \in b\Sigma^*$ for all $(z_2, \ldots, z_k) \in (\Sigma^*)^{k-1}$. As $f(z_1, z_2, \ldots, z_k) = f^{z_1}_{2\cdots k}(z_2, \ldots, z_k)$, we have for all $z_1, z_2, \ldots, z_k$, $f(z_1, z_2, \ldots, z_k) \in b\Sigma^*$ and the induction is proved. □

Lemma 4.10. *Let $|\Sigma| \geq 3$ and let $f\colon (\Sigma^*)^k \to \Sigma^*$ be RCP. Assume the two following conditions hold*

- *(*) For every $i \in \{1,\ldots,k\}$ and $u \in \Sigma^*$, the function $f^u_{1\cdots(i-1)(i+1)\cdots k}$ satisfies exactly one of the conditions (C_1), (C_2), (C_3) of Lemma 4.4.*
- *(**) There exist $y \in \Sigma^* \setminus \{\varepsilon\}$ and an index $i \in \{2, \ldots, k\}$ such that $f(y, x_2, \ldots, x_k) \in x_i\Sigma^*$ for all $(x_2, \ldots, x_k) \in (\Sigma^*)^{k-1}$.*

Then $f(z_1, z_2, \ldots, z_k) \in z_i\Sigma^*$ for all $(z_1, z_2, \ldots, z_k) \in (\Sigma^*)^k$.

Proof. By condition (*), there are exactly three possible cases, one of which splits into two subcases. The proof idea is that for all $y' \in \Sigma^*$, all cases lead to a contradiction except subcase 3.2. Finally, stating that subcase 3.2 holds for all $y' \in \Sigma^*$ is exactly the conclusion of the Lemma.

Let i and y be as given in condition (**). Condition (**) implies

$$\text{for all } \vec{a} = (a, \dots, a) \in \Sigma^{k-1} \qquad f^{y}_{2\cdots k}(\vec{a}) = f^{\vec{a}}_{1}(y) = f(y, \vec{a}) \ \in \ a\Sigma^*. \tag{14}$$

Case 1. Condition (C_1) holds for y', i.e. *for some* $b \in \Sigma$, $f^{y'}_{2\cdots k}(\vec{x}) \in b\Sigma^*$ *for all* $\vec{x} \in (\Sigma^*)^{k-1}$. We show that this case is impossible. Since $|\Sigma| \geq 3$, there exists $a \in \Sigma$ which is different from b and from the first letter of y. Set $\vec{a} = (a, \dots, a) \in \Sigma^{k-1}$. **Case 1** hypothesis implies

$$f^{\vec{a}}_{1}(y') = f^{y'}_{2\cdots k}(\vec{a}) \ \in \ b\Sigma^*. \tag{15}$$

As $f^{\vec{a}}_{1}$ is a unary RCP function, it has one of the three forms given in Lemma 3.15. Conditions (14) and (15) show that $f^{\vec{a}}_{1}$ can only be of the form $z \mapsto zg(z)$ for all z. Applying condition (14), we see that the first letter of y should be a, contradicting the choice of a.

Case 2. Condition (C_3) holds for y', i.e. $f^{y'}_{2\cdots k}(\vec{x}) = \varepsilon$ *for all* $\vec{x} \in (\Sigma^*)^{k-1}$.

This case also is excluded. Let a be different from the first letter of y and $\vec{a} = (a, \dots, a) \in \Sigma^{k-1}$. By condition (14), $f^{\vec{a}}_{1}$ is not the constant function ε. Thus, by Lemma 3.15 the RCP function $f^{\vec{a}}_{1}$ can have two possible forms

– Either there is some $b \in \Sigma$ such that $f^{\vec{a}}_{1}(z) \in b\Sigma^*$ for all z, in particular $f^{\vec{a}}_{1}(y') \in b\Sigma^*$. As $f^{\vec{a}}_{1}(y') = f^{y'}_{2\cdots k}(\vec{a})$, **Case 2.** hypothesis implies $f^{\vec{a}}_{1}(y') = \varepsilon$, a contradiction.

– Or $f^{\vec{a}}_{1}(z) \in z\Sigma^*$ for all z, which, letting $z = y$, implies $f^{\vec{a}}_{1}(y) \in y\Sigma^*$. This contradicts condition (14) because a is assumed to be different from the first letter of y.

Case 3. Condition (C_2) holds for y', i.e. *there exists an index* $j \in \{2 \dots k\}$ *such that* $f^{y'}_{2\cdots k}(z_2, \dots, z_k) \in z_j\Sigma^*$ *for all* $(z_2, \dots, z_k) \in (\Sigma^*)^{k-1}$. This case naturally splits into two subcases.

Subcase 3.1. If $j \neq i$, we deduce a contradiction by letting $a \in \Sigma$ be different from the first letter of y and considering the $(k-1)$-ary RCP function $f^{a}_{1\cdots(i-1)(i+1)\cdots k}$. For every $(k-1)$-tuple $\vec{z} = (z_1, z_2, \dots, z_{i-1}, z_{i+1}, \dots, z_k)$, we have

$$\text{by condition (**)}, \qquad z_1 = y \implies f^{a}_{1\cdots(i-1)(i+1)\cdots k}(\vec{z}) \ \in \ a\Sigma^*, \tag{16}$$

$$\text{by } \textbf{Case 3.} \text{ hypothesis}, \qquad z_1 = y' \implies f^{a}_{1\cdots(i-1)(i+1)\cdots k}(\vec{z}) \ \in \ z_j\Sigma^*. \tag{17}$$

By condition (*) the function $f^{a}_{1\cdots(i-1)(i+1)\cdots k}$ has three possible forms.

(C_1) Either for some $b \in \Sigma$, $f^{a}_{1\cdots(i-1)(i+1)\cdots k}(\vec{z}) \in b\Sigma^*$ for every $\vec{z} \in (\Sigma^*)^{k-1}$. It is excluded because it contradicts (17) when $z_1 = y'$ and the first letter of z_j is different from b.

(C_2) Or for some $\ell \in \{1, \ldots, i-1, i+1, \ldots, k\}$, we have $f^a_{1\cdots(i-1)(i+1)\cdots k}(\vec{z}) \in z_\ell \Sigma^*$ for every $\vec{z} \in (\Sigma^*)^{k-1}$. This contradicts (16) when $z_1 = y$. Indeed, if $\ell \neq 1$, then the first letter of z_ℓ can be chosen different from a, and if $\ell = 1$, then the first letter of y already is different from a.

(C_3) Or $f^a_{1\cdots(i-1)(i+1)\cdots k} = \varepsilon$. This is impossible because it contradicts (16).

Subcase 3.2. If $j = i$, then $f(y', z_2, \ldots, z_k) = f^{y'}_{2\cdots k}(z_2, \ldots, z_k) \in z_i \Sigma^*$ for all $z_2, \ldots, z_k \in \Sigma^*$. For all y' this is the only non-contradictory case, hence $f(y', z_2, \ldots, z_k) \in z_i \Sigma^*$ for all $y', z_2, \ldots, z_k$ and the conclusion of the Lemma holds. □

We finally prove Lemma 4.4.

Proof of Lemma 4.4. We argue by induction on the arity k.
Basis. For $k = 1$ this is Lemma 3.15.
Induction. Let $k \geq 2$. Assume the result holds for arity $< k$ and prove that it also holds for arity k. Consider the $(k-1)$-ary functions $f^a_{2\cdots k}$, for $a \in \Sigma$. They are RCP by Lemma 4.8. By the induction hypothesis they must satisfy exactly one of the conditions (C_1), (C_2), (C_3), hence

1. Either *there exists $a \in \Sigma$ such that $f^a_{2\cdots k}$ satisfies (C_1) relative to some $b \neq a$,* i.e. $f^a_{2\cdots k}(x_2, \ldots, x_k) \in b\Sigma^*$ for all $x_2, \ldots, x_k \in \Sigma^*$. By Lemma 4.9, f satisfies (C_1).
2. Or *for all $a \in \Sigma$ the function $f^a_{2\cdots k}$ satisfies (C_1) relative to $b = a$,* i.e. for all $x_2, \ldots, x_k \in \Sigma^*$, we have $f^a_{2\cdots k}(x_2, \ldots, x_k) \in a\Sigma^*$. For any $u_2, \ldots, u_k \in \Sigma^*$, the unary function $f^{u_2\cdots u_k}_1$ satisfies $f^{u_2\cdots u_k}_1(a) \in a\Sigma^*$ for any $a \in \Sigma$. By Lemma 3.14, we have $f^{u_2\cdots u_k}_1(u) \in u\Sigma^*$ for any $u \in \Sigma^*$. As this holds for any $u_2, \ldots, u_k \in \Sigma^*$, we infer that f satisfies (C_2) relative to the index 1.
3. Or *there exists $a \in \Sigma$ such that $f^a_{2\cdots k}$ satisfies (C_2) relative to an index $i \in \{2 \ldots k\}$,* i.e. $f^a_{2\cdots k}(x_2, \ldots, x_k) \in x_i\Sigma^*$ for all $x_2, \ldots, x_k \in \Sigma^*$. Then Lemma 4.10 (**) holds. As for every $u \in \Sigma^*$ and $i \in \{1, \ldots, k\}$, the arity of $f^u_{1\cdots(i-1)(i+1)\cdots k}$ is $(k-1)$, the induction hypothesis insures that condition (*) of Lemma 4.10 also holds. Applying Lemma 4.10, we see that f satisfies (C_2) with the same index i.
4. Or *there exists $a \in \Sigma$ such that $f^a_{2\cdots k}$ satisfies (C_3).* Then $f(a, a, \ldots, a) = \varepsilon$ and Lemma 4.6 shows that f satisfies (C_3). □

5. The *k*-ary case with infinite alphabet

The proof of the passage to arity k is much simpler if the alphabet Σ is infinite, rather than of cardinality at least 3.

Theorem 5.1. *Assume Σ is infinite. Then every RCP function $f : (\Sigma^*)^k \to \Sigma^*$ is of the form $f(x_1, \dots, x_k) = w_0 x_{i_1} w_1 x_{i_2} w_2 \cdots x_{i_n} w_n$, where $x_{i_j} \in \{x_1, \dots, x_k\}$ for $j = 1, \dots, n$.*

Proof. We argue by induction on the arity k.

Base case $k = 1$. This is Theorem 3.5.

Induction. Let $k \geq 2$. We assume the theorem is true for arity $k-1$ and we prove it for arity k. For every $\vec{x} = (x_2, \dots, x_k) \in (\Sigma^*)^{k-1}$, the unary function $f_1^{\vec{x}} : \Sigma^* \to \Sigma^*$, obtained from f by freezing all arguments but the first one, is RCP. With the notations of Lemma 4.3, we have, for all $x_1 \in \Sigma^*$,

$$|f_1^{\vec{x}}(x_1)| = |f(x_1, x_2, \dots, x_k)| = m|x_1| + n, \tag{18}$$

where $m = p_{f,1}$ does not depend on $\vec{x}$ and $n = p_{f,2}|x_2| + \cdots + p_{f,k}|x_k| + e_f$.

Since the unary function $f_1^{\vec{x}}$ is RCP, applying Theorem 3.5 and equation (18), we see that, for all $\vec{x} \in (\Sigma^*)^{k-1}$, there exist $m+1$ words $u_0(\vec{x}), \dots, u_m(\vec{x})$ (which depend only on $\vec{x}$) such that, for all x_1,

$$f_1^{\vec{x}}(x_1) \;=\; f(x_1, x_2, \dots, x_k) \;=\; u_0(\vec{x})\, x_1\, u_1(\vec{x})\, x_1 \cdots u_{m-1}(\vec{x})\, x_1\, u_m(\vec{x}). \tag{19}$$

Claim. *The functions $\vec{x} \mapsto u_0(\vec{x}), \dots, \vec{x} \mapsto u_m(\vec{x})$ are RCP.*

Proof of Claim. Let $\varphi : \Sigma^* \to \Sigma^*$ be a morphism and $\vec{y} = (y_2, \dots, y_k), \vec{z} = (z_2, \dots, z_k)$ in $(\Sigma^*)^{k-1}$ be such that $\varphi(y_2) = \varphi(z_2), \dots, \varphi(y_k) = \varphi(z_k)$. We have to prove that $\varphi(u_i(\vec{y})) = \varphi(u_i(\vec{z}))$ for $i = 0, \dots, m$.

Let Γ be a finite subset of Σ such that $y_2, \dots, y_k$, $z_2, \dots, z_k$, $u_0(\vec{y}), \dots, u_m(\vec{y})$, $u_0(\vec{z}), \dots, u_m(\vec{z})$ and their images by φ are all in Γ^*. Let $a \in \Sigma \setminus \Gamma$ (this is where we use the hypothesis that Σ is infinite). Define a morphism $\psi : \Sigma^* \to \Sigma^*$ as follows: $\psi(c) = \varphi(c)$ for all $c \in \Gamma$ and $\psi(c) = a$ for all $c \in \Sigma \setminus \Gamma$. In particular, we have $\psi(u_i(\vec{y})) = \varphi(u_i(\vec{y}))$ and $\psi(u_i(\vec{z})) = \varphi(u_i(\vec{z}))$ for $i = 0, \dots, m$, and these words contain no occurrence of a. Thus, applying the morphism ψ to (19) with $x_1 = a$ and $\vec{x} = \vec{y}$, we get

$$\begin{aligned} \psi(f(a, \vec{y})) &= \psi(u_0(\vec{y}))\, \psi(a)\, \psi(u_1(\vec{y}))\, \psi(a) \cdots \psi(u_{m-1}(\vec{y}))\, \psi(a)\, \psi(u_m(\vec{y})) \\ &= \varphi(u_0(\vec{y}))\, a\, \varphi(u_1(\vec{y}))\, a \cdots \varphi(u_{m-1}(\vec{y}))\, a\, \varphi(u_m(\vec{y})). \end{aligned} \tag{20}$$

Similarly,
$$\psi(f(a, \vec{z})) = \varphi(u_0(\vec{z}))\, a\, \varphi(u_1(\vec{z}))\, a \cdots \varphi(u_{m-1}(\vec{z}))\, a\, \varphi(u_m(\vec{z})). \tag{21}$$

As $\psi(y_2) = \varphi(y_2) = \varphi(z_2) = \psi(z_2), \dots, \psi(y_k) = \varphi(y_k) = \varphi(z_k) = \psi(z_k)$ and f is RCP, we have $\psi(f(a, \vec{y})) = \psi(f(a, \vec{z}))$. Applying equations (20) and (21), we get

$$\begin{aligned} &\varphi(u_0(\vec{y}))\, a\, \varphi(u_1(\vec{y}))\, a \cdots \varphi(u_{m-1}(\vec{y}))\, a\, \varphi(u_m(\vec{y})) \\ &\qquad = \varphi(u_0(\vec{z}))\, a\, \varphi(u_1(\vec{z}))\, a \cdots \varphi(u_{m-1}(\vec{z}))\, a\, \varphi(u_m(\vec{z})). \end{aligned} \tag{22}$$

Since a does not occur in $\varphi(u_i(\vec{y}))$ and $\varphi(u_i(\vec{z}))$, for $i = 0, \ldots, m$, equality (22) yields $\varphi(u_0(\vec{y})) = \varphi(u_0(\vec{z}))$, …, $\varphi(u_m(\vec{y})) = \varphi(u_m(\vec{z}))$. This proves the Claim.

Finally, applying the induction hypothesis, the RCP $(k-1)$-ary functions $u_0(\vec{x}), \ldots,$ $u_m(\vec{x})$ are represented by terms in $x_2, \ldots, x_k$. Using equation (19), we then get a term which represents the k-ary function $f(x_1, x_2, \ldots, x_k)$. □

6. Conclusion

We proved that, when Σ has at least three letters, the free monoid Σ^* is affine complete, i.e. a function is CP if and only if it is "polynomial." An essential tool in the proof was to use restricted congruence preserving functions, which happen to coincide with CP functions in case Σ has at least three letters.

If Σ has just one letter, the monoid Σ^* reduces to the semigroup $\langle \mathbb{N}, + \rangle$ where "polynomial" functions are a strict subset of CP functions. Indeed, we proved in [2] that, on the additive semigroup of integers, there exist non polynomial CP functions, e.g. $f(x) = \lfloor e^{1/a} a^x x! \rfloor$ for $a \in \mathbb{N} \setminus \{0, 1\}$.

An open problem is how to characterize CP functions when Σ has exactly two letters: is $\{a, b\}^*$ affine complete or are there non-polynomial CP functions, i.e. do Theorems 3.6 and 4.5 extend to binary alphabets?

Acknowledgements
We thank the anonymous referee for a very careful reading and quite helpful comments and Henri Justin for correcting the English.

[1] M. Bhargava, *Congruence preservation and polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$*, Discrete Mathematics 173: 15 – 21, 1997.

[2] P. Cégielski, S. Grigorieff, I. Guessarian, *Newton representation of functions over natural integers having integral difference ratios*, International Journal of Number Theory 11(7): 2109–2139, 2015.

[3] P. Cégielski, S. Grigorieff and I. Guessarian, *Integral Difference Ratio functions on Integers*, LNCS 8808: 277–291, Computing with new resources, Essays dedicated to Jozef Gruska on the occasion of his 80th birthday, C. Calude, R. Freivalds, I. Kazuo (Eds.), Springer, 2014.

[4] G Grätzer, *On Boolean functions (notes on lattice theory. II)*, Rev. Math. Pures Appl. (Académie de la République Populaire Roumaine) 7(4): 693–697, 1962.

[5] G Grätzer, *Boolean functions on distributive lattices*, Acta Mathematica Hungarica 15(1-2): 193–201, 1964.

[6] G Grätzer, *Universal Algebra*, 2nd edition, Springer Verlag, 1979.

[7] A. Iskander, *Algebraic functions on p-rings*, Colloquium Mathematicae 25: 37–41, 1972.

[8] K. Kaarli, A.F. Pixley, *Polynomial completeness in algebraic systems*, Chapman & Hall/CRC, 2001.

[9] A. J. Kempner, *Polynomials and their residue systems*, American Math. Soc. Transactions 22: 240–288, 1921.

[10] W. Nöbauer, *Affinvollständige Moduln*, Mathematische Nachrichten 86: 85–96, 1978.

[11] M. Ploščica and M. Haviar, *Congruence-preserving functions on distributive lattices*, Algebra universalis 59: 179–196, 2008.

[12] H. Werner, *Produkte von KongruenzenKlassengeometrien universeller Algebren*, Mathematische Zeitschrift 121: 111–140, 1971.