Journal of Algebra 431 (2015) 107–126

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Character theory of monoids over an arbitrary field ☆

Ariane M. Masuda [a], Luciane Quoos [b], Benjamin Steinberg [c,*]

[a] Department of Mathematics, New York City College of Technology, 300 Jay Street, Brooklyn, NY 11201, USA

[b] Instituto de Matemática, Universidade Federal do Rio de Janeiro, Cidade Universitária, Rio de Janeiro, RJ 21941-909, Brazil

[c] Department of Mathematics, City College of New York, Convent Avenue at 138th Street, New York, NY 10031, USA

ARTICLE INFO

Article history:
Received 27 October 2014
Available online xxxx
Communicated by Volodymyr Mazorchuk

MSC:
20M30
20M35
16G99

Keywords:
Character theory
Representation theory
Monoids

ABSTRACT

The basic character theory of finite monoids over the complex numbers was developed in the sixties and seventies based on work of Munn, Ponizovskiĭ, McAlister, Rhodes and Zalcstein. In particular, McAlister determined the space of functions spanned by the irreducible characters of a finite monoid over $\mathbb{C}$ and the ring of virtual characters. In this paper, we present the corresponding results over an arbitrary field.

As a consequence, we obtain a quick proof of the theorem of Berstel and Reutenauer that the characteristic function of a regular cyclic language is a virtual character of the free monoid. This is a crucial ingredient in their proof of the

☆ The first author was partially supported by PSC-CUNY grants (#66133-00 44 and #67111-00 45). The second author was partially supported by Siemens, project INST.MAT.-18.414. The third author was partially supported by a grant from the Simons Foundation (#245268 to Benjamin Steinberg), the Binational Science Foundation of Israel and the US (#2012080), and CUNY Collaborative Incentive Research Grant #2123. Some of this work was performed while the first, second and third authors were visiting UFRJ, CUNY and IMPA, respectively; they gratefully acknowledge the warm hospitality they received.

* Corresponding author.

E-mail addresses: amasuda@citytech.cuny.edu (A.M. Masuda), luciane@im.ufrj.br (L. Quoos), bsteinberg@ccny.cuny.edu (B. Steinberg).

http://dx.doi.org/10.1016/j.jalgebra.2015.02.017

rationality of the zeta function of a sofic shift in symbolic dynamics.

1. Introduction

The representation theory of finite monoids has enjoyed a rebirth over the past two decades [8,22,27,28,35–37,42–46,52–54], in a large part due to applications to Markov chain theory [3–7,12–18,23,51], data analysis [32–34] and automata theory [1,2,55]. This paper is a further contribution to the representation theory of finite monoids.

We say that two elements a and b of a finite monoid M are character equivalent over a field K if every irreducible character of M over K agrees on a and b. Character equivalence for the field of complex numbers was described by McAlister [38], see also [49] and [30]. The arguments of [38], in fact, work over any algebraically closed field of characteristic 0. In this paper we determine character equivalence for an arbitrary field and we prove that the irreducible characters form a basis for the algebra of K-valued functions on M which are constant on character equivalence classes. As is often the case in the representation theory of finite monoids, the result is obtained via a reduction to the case of finite groups, which was essentially handled by Berman [9].

Recall that a virtual character is a difference of two characters. The virtual characters of M over K form a ring and we show that it is isomorphic to the direct product of the rings of virtual characters of maximal subgroups of M over K (one per regular $\mathcal{D}$-class), as is the case over $\mathbb{C}$ [38]. Moreover, we show that a function that is constant on character equivalence classes is a virtual character if and only if its restriction to each maximal subgroup is a virtual character.

As an application of our results, we give a character theoretic proof of a result of Berstel and Reutenauer [11], which they put to good use in order to prove the rationality of the zeta function of a sofic shift in symbolic dynamics [31]. More precisely, if A^* is the free monoid on a finite set A, then a language $L \subseteq A^*$ is said to be cyclic if:

i) for all $n > 0$, one has $u \in L \iff u^n \in L$;
ii) $uv \in L \iff vu \in L$.

For example, if $\mathcal{X}$ is a subshift of $A^{\mathbb{Z}}$, then the set L of all words w such that $\cdots ww.ww \cdots \in \mathcal{X}$ is cyclic. Recall that a language $L \subseteq A^*$ is regular if it is accepted by a finite state automaton [24]. Berstel and Reutenauer proved that the characteristic function $A^* \longrightarrow \{0, 1\}$ of a regular cyclic language $L \subseteq A^*$ is a virtual character of A^* (over any field). From this, they easily deduced the rationality of the zeta function of L and hence the rationality of zeta functions of sofic shifts.

In a recent paper [40] Perrin gave another proof that the characteristic function of a regular cyclic language is a K-linear combination of irreducible characters over any algebraically closed field K of characteristic 0 using the character theory results of

McAlister [38]. This motivated us to look for a proof of the original result of Berstel and Reutenauer using the character theory of finite monoids over an arbitrary field.

2. Characters of monoids over an arbitrary field

Let M be a monoid and K a field of characteristic $p \geq 0$. A *representation* of M over K is a monoid homomorphism $\varphi\colon M \longrightarrow M_r(K)$. One says that r is the *degree* of φ. A representation is *irreducible* if there is no proper nonzero subspace V of K^r such that $\varphi(m) \cdot v \in V$ for all $m \in M$ and $v \in V$. Mostly we shall assume that M is finite, except in Section 4.

We say that two representations φ_1 and φ_2 of degree r are *equivalent*, written $\varphi_1 \sim \varphi_2$, if there exists an invertible matrix $A \in M_r(K)$ such that $A\varphi_1(m)A^{-1} = \varphi_2(m)$ for all $m \in M$. The set of all equivalence classes of irreducible representations of M over K is denoted $\mathrm{Irr}_K(M)$.

The *character* of a representation φ is the map $\chi_\varphi\colon M \longrightarrow K$ given by

$$\chi_\varphi(m) = \mathrm{Tr}(\varphi(m))$$

where $\mathrm{Tr}(A)$ denotes the trace of a matrix A. Notice that if the degree r is 1, then the character agrees with the representation. An *irreducible character* is the character of an irreducible representation. If $\varphi_1 \sim \varphi_2$, then $\chi_{\varphi_1} = \chi_{\varphi_2}$.

The following theorem is Theorem 9.22 in [29].

Theorem 2.1. *If $\chi_1, \ldots, \chi_m$ are characters of inequivalent irreducible representations of a finite group G over a field K, then they are linearly independent and, in particular, non-zero and distinct.*

It is well known [21, Theorem 27.22] that if K is an algebraically closed field of characteristic 0, then the number of irreducible characters of a finite group G over K is the number of conjugacy classes. Moreover, the irreducible characters form a basis for the space of functions $f\colon G \longrightarrow K$ constant on conjugacy classes. McAlister [38] obtained the appropriate generalization to representations of finite monoids over an algebraically closed field; the result was obtained at the same time independently by Rhodes and Zalcstein, but only published many years later [49]; see also [30]. Our goal is to extend McAlister's results to arbitrary fields.

Definition 2.2. Let K be a field and M a monoid. We say that $m_1, m_2 \in M$ are *character equivalent* if $\chi(m_1) = \chi(m_2)$ for all characters χ of M, or equivalently for all irreducible characters χ of M, over K.

For example, if $K = \mathbb{C}$ and M is a finite group, then character equivalence is conjugacy.

Let M be a finite monoid. Then $e \in M$ is an *idempotent* if $e^2 = e$. The set of idempotents is denoted $E(M)$. The set $eMe = \{eme \,|\, m \in M\} = \{m \in M \,|\, em = m =$

$me\}$ is a monoid with identity e and the multiplication induced from M. Let G_e be the group of invertible elements of eMe. It is called the *maximal subgroup* of M at e.

If m is an element of a finite monoid M, then there exist $r, s > 0$ such that $m^r = m^{r+s}$. By choosing r and s minimal, the set $G = \{m^r, \dots, m^{r+s-1}\}$ is a cyclic group of order s isomorphic to $\mathbb{Z}_s$ via the map sending m^t to the residue class of t mod s [20, Theorem 1.9]. The identity of the group is m^k, where k is the unique integer such that $r \le k \le r+s-1$ and $k \equiv 0 \bmod s$, and is denoted symbolically by m^ω. The group G is generated by $m^\omega m$, which we denote $m^{\omega+1}$. Note that if M is a finite monoid, then $m^{|M|!} = m^\omega$ for all $m \in M$ because, retaining the above notation, $r, s \le |M|$ and hence $|M|! \equiv 0 \bmod s$.

Definition 2.3. Let M be a finite monoid and let $p = 0$ or be prime. Let $m \in M$.

a) We say that m is a *group element* if there exists $s > 0$ such that $m = m^s$ or, equivalently, $m = m^{\omega+1}$.
b) For a group element m, the minimal $s > 0$ such that $m = m^{s+1}$ is its *order*, denoted $|m|$, in which case $\{m, \dots, m^s\}$ is a cyclic group of order $|m|$.
c) We say m is *p-regular* if m is a group element and $p = 0$ or p does not divide $|m|$.

If $p > 0$ is a prime and g is an element of a finite group G with identity e, then g can be uniquely factored as $g = g_p g_{p'}$ where g_p has order a p-power, $g_{p'}$ has order prime to p (i.e., $g_{p'}$ is p-regular) and g_p, $g_{p'}$ commute. Indeed, if $|g|$ is $p^k t$ with $\gcd(t, p) = 1$, then $g_p = g^r$ and $g_{p'} = g^s$ where $r \equiv 1 \bmod p^k$, $r \equiv 0 \bmod t$ and $s \equiv 1 \bmod t$, $s \equiv 0 \bmod p^k$. See [21, Lemma 40.3] and its proof for details. If $p = 0$, we define $g_p = e$ and $g_{p'} = g$.

If M is a finite monoid, then for any $m \in M$, we observe that $m^{\omega+1}$ is always a group element and so $m_{p'}^{\omega+1}$ makes sense.

Let us fix some notation that will be used throughout this section. Let K be a field of characteristic $p \ge 0$. Let n be the least common multiple of the orders of the p-regular elements of M. Notice that $p \nmid n$ and that we have a homomorphism θ from the Galois group $\mathrm{Gal}(K(\xi_n)/K)$ into the multiplicative group $\mathbb{Z}_n^*$, where ξ_n is a primitive nth-root of unity in a fixed algebraic closure $\bar{K}$ of K, defined as follows. If $\sigma \in \mathrm{Gal}(K(\xi_n)/K)$, then $\sigma(\xi_n) = \xi_n^\ell$, where $\ell \in \mathbb{Z}_n^*$, and we put $\theta(\sigma) = \ell$. Let $T = \theta(\mathrm{Gal}(K(\xi_n)/K)) \le \mathbb{Z}_n^*$, also denoted $\mathrm{Im}\,\mathrm{Gal}(K(\xi_n)/K)$.

Let us now assume that M is a group G. Following Berman [9], we say that p-regular elements $g, h \in G$ are *K-conjugate*, denoted $g \sim_K h$, if there exist $x \in G$ and $j \in T$ such that $xgx^{-1} = h^j$. It is easy to check that this is an equivalence relation on the set p-reg(G) of p-regular elements of G.

Theorem 2.4. *(See Berman [9].) Let G be a finite group and K a field of characteristic $p \ge 0$. Then the number of equivalence classes of irreducible representations of G over K is the number of K-conjugacy classes of p-regular elements of G.*

This result can be found in characteristic 0 as [21, Theorem 42.8]; a proof in characteristic p using Brauer characters can be found in [47].

We shall need the following lemma clarifying $\sim_K$.

Lemma 2.5. *If t is such that the orders of all p-regular elements of a finite group G divide t and $T' = \operatorname{Im}\operatorname{Gal}(K(\xi_t)/K)$ in $\mathbb{Z}_t^*$, then $g \sim_K h$ if and only if there exist $x \in G$ and $j \in T'$ such that $xgx^{-1} = h^j$.*

Proof. Let n be the least common multiple of the orders of the p-regular elements of G and observe that it is a divisor of t. Then since $K(\xi_t)/K$ is abelian, it follows that the subfield $K(\xi_n)$ is $\operatorname{Gal}(K(\xi_t)/K)$-invariant and that the restriction map $\operatorname{Gal}(K(\xi_t)/K) \longrightarrow \operatorname{Gal}(K(\xi_n)/K)$ is a surjective homomorphism. Also if $\sigma \in \operatorname{Gal}(K(\xi_t)/K)$ with $\sigma(\xi_t) = \xi_t^j$, then $\sigma(\xi_n) = \xi_n^j$. Therefore, if $\alpha\colon \mathbb{Z}_t^* \longrightarrow \mathbb{Z}_n^*$ is the surjective homomorphism given by $\alpha(j) = j \bmod n$, then $T = \alpha(T')$. Moreover, if $j \in T'$, then $h^j = h^{\alpha(j)}$ because $|h|$ divides n, which divides t. The lemma follows. □

Recall that two idempotents e and f in a monoid M are $\mathcal{D}$*-equivalent*, written $e\,\mathcal{D}\,f$, if there exist $x, y \in M$ with $xyx = x$, $yxy = y$, $xy = e$ and $yx = f$; see [20, Section 2.3] or [56, Proposition 1.3] for details. An equivalence class for the $\mathcal{D}$-relation is called a $\mathcal{D}$*-class*. It is well known that in a finite monoid M, one has that $e\,\mathcal{D}\,f$ if and only if $MeM = MfM$ [48, Appendix A]. (In general, elements $m, n \in M$ are called $\mathcal{J}$*-equivalent* if $MmM = MnM$.) Note that the $\mathcal{D}$-relation is customarily defined for arbitrary elements of a monoid, but we have restricted the definition here to idempotents.

The following well-known lemma, cf. [56, Proposition 1.4] or [20, Theorem 2.20], will play a key role later.

Lemma 2.6. *Let M be a monoid and let $e, f \in M$ be $\mathcal{D}$-equivalent idempotents. Suppose that $x, y \in M$ with $xyx = x$, $yxy = y$, $xy = e$ and $yx = f$. Then $\varphi\colon eMe \longrightarrow fMf$ and $\psi\colon fMf \longrightarrow eMe$ defined by $\varphi(a) = yax$ and $\psi(b) = xay$ are inverse isomorphisms of monoids. Consequently, φ and ψ restrict to inverse isomorphisms of G_e and G_f.*

Let $e_1, \ldots, e_k$ be elements in $E(M)$ representing the distinct $\mathcal{D}$-classes of idempotents of M. We can define a partial order on the set $\{e_1, \ldots, e_k\}$ by $e_i \preceq e_j$ if and only if $Me_iM \subseteq Me_jM$.

The following is a fundamental result, proved independently by Munn [39] and Ponizovskiĭ [41] based on earlier work of Clifford [19]; see [20, Theorem 5.33] or [49]. A simpler, module-theoretic approach can be found in [27].

Theorem 2.7 *(Clifford–Munn–Ponizovskiĭ). Let M be a finite monoid, K a field and $e_1, \ldots, e_k$ idempotents representing the $\mathcal{D}$-classes of idempotents of M. If $\varphi\colon M \longrightarrow M_r(K)$ is an irreducible representation, then there exists a unique minimal idempotent e_i (with respect to $\preceq$) among $e_1, \ldots, e_k$ such that $\varphi(e_i) \neq 0$. Moreover, one has that*

i) *for $m \in M$, $\varphi(m) \neq 0$ if and only if $e_i \in MmM$;*
ii) $\varphi_{|G_{e_i}} \sim \begin{bmatrix} \hat{\varphi} & 0 \\ 0 & 0 \end{bmatrix}$, *where $\hat{\varphi}$ is an irreducible representation of the group G_{e_i}.*

The element e_i is called the apex *of φ.*

In addition, the map

$$\psi\colon \mathrm{Irr}_K(M) \longrightarrow \bigsqcup_{i=1}^{k} \mathrm{Irr}_K(G_{e_i})$$

given by $\psi(\varphi) = \hat{\varphi}$ *is a bijection.*

Let us interpret part of the above theorem in terms of characters.

Corollary 2.8. *Let* $\varphi\colon M \longrightarrow M_r(K)$ *be an irreducible representation with apex* e_i*. If* χ *is the character of* φ*, then* $\chi_{|G_{e_i}} = \chi_{\hat{\varphi}}$ *where* $\hat{\varphi}$ *is as in Theorem 2.7.*

Proof. This is immediate from ii) of Theorem 2.7. □

We can now prove the analogue of Theorem 2.1 for monoids.

Theorem 2.9. *If* $\chi_1, \dots, \chi_s$ *are characters of inequivalent irreducible representations of a finite monoid* M *over a field* K*, then they are non-zero, distinct and linearly independent.*

Proof. Without loss of generality, we may suppose that there are $c_1, \dots, c_s$ in $K \setminus \{0\}$ such that

$$0 = c_1\chi_1 + \cdots + c_s\chi_s.$$

Let $e = e_i$ be minimal with respect to $\preceq$ among the apexes of the representations $\chi_1, \dots, \chi_s$. Reordering the representations we can assume that e is the apex for $\chi_1, \dots, \chi_t$ where $1 \leq t \leq s$, and that $\chi_{t+1}, \dots, \chi_s$ have a different apex than e.

Any g in the group G_e satisfies $MeM = MgM$. So, if e_ℓ is the apex of χ_j with $j > t$ (and hence $\ell \neq i$), then $Me_\ell M \nsubseteq MeM = MgM$ by minimality of e. Therefore, $\varphi_j(g) = 0$ by i) of Theorem 2.7. We conclude that $\chi_j(g) = 0$, for all $g \in G_e$ and $t < j \leq s$.

Therefore, for any $g \in G_e$, we obtain

$$0 = c_1\chi_1(g) + \cdots + c_t\chi_t(g).$$

But $\chi_{1|G_e}, \dots, \chi_{t|G_e}$ are characters of distinct irreducible representations of G_e by Theorem 2.7 and Corollary 2.8, a contradiction with the linear independence of irreducible characters of finite groups, cf. Theorem 2.1. □

Remark 2.10. In [26, Theorem 2.1] it is shown that, for arbitrary monoids (possibly infinite), the only obstruction to characters of distinct irreducible representations being linearly independent is that one or more of the characters might be identically zero and that this can indeed happen for infinite groups.

The following lemma is crucial for understanding character equivalence. We recall that if n is the least common multiple of the orders of the p-regular elements of M, then T denotes the image of $\mathrm{Gal}(K(\xi_n)/K)$ in $\mathbb{Z}_n^*$.

Lemma 2.11. *If χ is a character of M over a field K of characteristic $p \geq 0$ and $a, b \in M$, then*

a) $\chi(ab) = \chi(ba)$;
b) $\chi(a) = \chi(a_{p'}^{\omega+1})$;
c) $\chi(a) = \chi(a^j)$ *if a is p-regular and $j \in T$.*

Proof. Let $\varphi: M \longrightarrow M_\ell(K)$ be a representation. Since $\chi(m) = \mathrm{Tr}(\varphi(m))$, it follows that

$$\chi(ab) = \mathrm{Tr}(\varphi(ab)) = \mathrm{Tr}(\varphi(a)\varphi(b)) = \mathrm{Tr}(\varphi(b)\varphi(a)) = \mathrm{Tr}(\varphi(ba)) = \chi(ba).$$

To show (b), let $r, s > 0$ be the minimal integers such that $a^r = a^{r+s}$. Write $s = p^k t$ where p^k and t are coprime. If $p = 0$, we take $k = 0$ and interpret $p^k = 1$ and $t = s$ (to avoid having to write out two separate cases). Then

$$\varphi(a)^r = \varphi(a)^{r+s} \Longrightarrow \varphi(a)^r(\varphi(a)^s - 1) = 0 \Longrightarrow \varphi(a)^r(\varphi(a)^t - 1)^{p^k} = 0.$$

Let $p(x) = x^r(x^t - 1)^{p^k}$. Then $p(\varphi(a)) = 0$ and so the minimal polynomial of $\varphi(a)$ divides $p(x)$. Let $\bar{K}$ be an algebraic closure of K containing $K(\xi_n)$. Then in $M_\ell(\bar{K})$ we have

$$\varphi(a) \sim \begin{bmatrix} \lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_\ell \end{bmatrix},$$

where the non-zero elements among $\lambda_1, \ldots, \lambda_\ell \in \bar{K}$ are roots of $x^t - 1$. Let $z \geq r$ such that $z \equiv 1 \bmod t$ and $z \equiv 0 \bmod p^k$. Then $a^z = a_{p'}^{\omega+1}$. Therefore,

$$\varphi(a_{p'}^{\omega+1}) = \varphi(a^z) = \varphi(a)^z \sim \begin{bmatrix} \lambda_1^z & * & \cdots & * \\ 0 & \lambda_2^z & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_\ell^z \end{bmatrix}.$$

Observe that, if $\lambda_i \neq 0$, then $\lambda_i^t = 1$ and so $\lambda_i^z = \lambda_i$ because $z \equiv 1 \bmod t$. Of course, $\lambda_i^z = \lambda_i$ is also true if $\lambda_i = 0$. Therefore,

$$\chi(a) = \mathrm{Tr}(\varphi(a)) = \sum_{i=1}^{\ell} \lambda_i = \sum_{i=1}^{\ell} \lambda_i^z = \mathrm{Tr}(\varphi(a^z)) = \chi(a_{p'}^{\omega+1}),$$

which establishes (b).

Now let n be the lcm of the orders of the p-regular elements of M, $T = \operatorname{Im}\operatorname{Gal}(K(\xi_n)/K) \le \mathbb{Z}_n^*$, and $L = K(\xi_n)$. If a is p-regular, then $a = a^{t+1}$ with $t = |a|$ coprime to p. Thus $p(\varphi(a)) = 0$, for $p(x) = x(x^t - 1)$, and t divides n. Consequently all eigenvalues of $\varphi(a)$ (over $\bar{K}$) belong to L. Then over $M_\ell(L)$ we have

$$\varphi(a) \sim \begin{bmatrix} \lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_\ell \end{bmatrix} \quad \text{and} \quad \varphi(a^j) \sim \begin{bmatrix} \lambda_1^j & * & \cdots & * \\ 0 & \lambda_2^j & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_\ell^j \end{bmatrix}.$$

We define $\alpha\colon \operatorname{Gal}(L/K)) \longrightarrow \operatorname{Aut}(M_\ell(L))$ by

$$\alpha(g)\left(\begin{bmatrix} a_{11} & \dots & a_{1\ell} \\ \vdots & & \vdots \\ a_{\ell 1} & \dots & a_{\ell\ell} \end{bmatrix}\right) = \begin{bmatrix} g(a_{11}) & \dots & g(a_{1\ell}) \\ \vdots & & \vdots \\ g(a_{\ell 1}) & \dots & g(a_{\ell\ell}) \end{bmatrix}.$$

We note that $M_\ell(K)$ is the set of fixed points of $\operatorname{Gal}(L/K)$ acting on $M_\ell(L)$ and hence $\alpha(g)(\varphi(a)) = \varphi(a)$ for all $g \in \operatorname{Gal}(L/K)$. Let $j \in T$ and let $g \in \operatorname{Gal}(L/K)$ be such that $g(\xi_n) = \xi^j$. Note that if λ is either 0 or an nth-root of unity, then $g(\lambda) = \lambda^j$. Also note that if A and B are similar matrices, then so are $\alpha(g)(A)$ and $\alpha(g)(B)$. Thus we have

$$\varphi(a) = \alpha(g)(\varphi(a)) \sim \begin{bmatrix} g(\lambda_1) & * & \cdots & * \\ 0 & g(\lambda_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & g(\lambda_\ell) \end{bmatrix} = \begin{bmatrix} \lambda_1^j & * & \cdots & * \\ 0 & \lambda_2^j & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_\ell^j \end{bmatrix}$$

and so $\chi(a) = \operatorname{Tr}(\varphi(a)) = \sum_{i=1}^{\ell} \lambda_i^j = \operatorname{Tr}(\varphi(a^j)) = \chi(a^j)$, as required. □

The following theorem is the main result of this paper.

Theorem 2.12. *Let M be a finite monoid, $a, b \in M$ and K a field of characteristic $p \ge 0$. Let $T = \operatorname{Im}\operatorname{Gal}(K(\xi_n)/K) \le \mathbb{Z}_n^*$ with n the least common multiple of the orders of p-regular elements of M. Then the following conditions are equivalent:*

a) *a and b are character equivalent over K;*
b) *a and b are equivalent by $\equiv$, where $\equiv$ is the least equivalence relation in M satisfying:*
   i) $m_1 m_2 \equiv m_2 m_1$, $\forall\, m_1, m_2 \in M$
   ii) $m \equiv m_{p'}^{\omega+1}$, $\forall\, m \in M$
   iii) *if $m \in M$ is p-regular and $j \in T$, then $m \equiv m^j$;*
c) *a and b are equivalent by $\approx$, where $a \approx b$ if and only there exist $x, y \in M$ and $j \in T$ such that*

i) $xyx = x, yxy = y$
ii) $xa_{p'}^{\omega+1}y = (b_{p'}^{\omega+1})^j$
iii) $xy = b^\omega$, $yx = a^\omega$.

Moreover, the distinct irreducible characters of M form a basis for the space of K-valued functions on M that are constant on $\equiv$-classes.

Proof. First we prove that $\approx$ is an equivalence relation. It is reflexive, since given $a \in M$, it is enough to choose $x = y = a^\omega$ and $j = 1$.

Now suppose that $a \approx b$ with x, y, j as above and put $g = a_{p'}^{\omega+1}$ and $h = b_{p'}^{\omega+1}$. Let j' be the inverse of j in the group $T \leq \mathbb{Z}_n^*$. Since the order of h divides n by choice of n, we have $h^{jj'} = h$. Thus, using Lemma 2.6, we have that

$$yhx = yh^{jj'}x = y(xgy)^{j'}x = yxg^{j'}yx = a^\omega g^{j'} a^\omega = g^{j'}$$

and so $b \approx a$.

Finally, if $a \approx b$ and $b \approx c$, there exist $x_1, x_2, y_1, y_2 \in M$ and $j_1, j_2 \in T$ such that:

a) $x_i y_i x_i = x_i, y_i x_i y_i = y_i$ for $i = 1, 2$;
b) $x_1 a_{p'}^{\omega+1} y_1 = (b_{p'}^{\omega+1})^{j_1}$;
c) $x_2 b_{p'}^{\omega+1} y_2 = (c_{p'}^{\omega+1})^{j_2}$;
d) $y_1 x_1 = a^\omega$, $x_1 y_1 = b^\omega$;
e) $y_2 x_2 = b^\omega$, $x_2 y_2 = c^\omega$.

By choosing $x_3 = x_2 x_1$ and $y_3 = y_1 y_2 \in M$, we obtain

$$x_3 = x_2 x_1 = x_2 x_1 y_1 x_1 = x_2 b^\omega x_1 = x_2 b^\omega b^\omega x_1 = x_2 x_1 y_1 y_2 x_2 x_1 = x_3 y_3 x_3$$

and similarly $y_3 x_3 y_3 = y_3$. Also, we have $y_3 x_3 = y_1 y_2 x_2 x_1 = y_1 b^\omega x_1 = y_1 x_1 y_1 x_1 = a^\omega$ and $x_3 y_3 = x_2 x_1 y_1 y_2 = x_2 b^\omega y_2 = x_2 y_2 x_2 y_2 = c^\omega$.

Finally, putting $g = a_{p'}^{\omega+1}$, $h = b_{p'}^{\omega+1}$ and $k = c_{p'}^{\omega+1}$, we have

$$x_3 g y_3 = x_2 x_1 g y_1 y_2 = x_2 h^{j_1} y_2 = (x_2 h y_2)^{j_1} = (k^{j_2})^{j_1} = k^{j_1 j_2}$$

where we have again used Lemma 2.6. Thus $a \approx c$. This concludes the proof that $\approx$ is an equivalence relation. Next we show that it satisfies i)–iii) of b). This will show that b) implies c).

To show i), suppose that $m_1, m_2 \in M$. We want to show that $m_1 m_2 \approx m_2 m_1$. If $k = |M|!$, then $(m_1 m_2)^\omega = (m_1 m_2)^k$ and $(m_2 m_1)^\omega = (m_2 m_1)^k$. Let $x = m_1 (m_2 m_1)^{2k-1}$ and $y = (m_2 m_1)^k m_2$. Then

$$yx = (m_2 m_1)^k m_2 m_1 (m_2 m_1)^{2k-1} = (m_2 m_1)^{3k} = (m_2 m_1)^\omega$$

and

$$\begin{aligned} xy &= m_1(m_2m_1)^{2k-1}(m_2m_1)^k m_2 = m_1(m_2m_1)^{3k-1}m_2 \\ &= m_1m_2(m_1m_2)^{3k-1} = (m_1m_2)^{3k} = (m_1m_2)^\omega. \end{aligned}$$

Clearly then $xyx = m_1(m_2m_1)^{2k-1}(m_2m_1)^\omega = m_1(m_2m_1)^{2k-1} = x$ because $(m_2m_1)^{2k-1} \in G_{(m_2m_1)^\omega}$. Also, we have $yxy = (m_2m_1)^\omega(m_2m_1)^\omega m_2 = y$. We compute that $y(m_1m_2)^{\omega+1}x = (m_2m_1)^k m_2(m_1m_2)^{k+1}m_1(m_2m_1)^{2k-1} = (m_2m_1)^{4k+1} = (m_2m_1)^{\omega+1}$. By Lemma 2.6, the assignment $z \mapsto yzx$ is a group isomorphism from $G_{(m_1m_2)^\omega}$ to $G_{(m_2m_1)^\omega}$ with inverse $w \mapsto xwy$. Thus $y(m_1m_2)^{\omega+1}_{p'}x = (m_2m_1)^{\omega+1}_{p'}$ and so $m_1m_2 \approx m_2m_1$ (with $j = 1$).

Condition ii) is trivially verified by taking $x = m^\omega = y$ and $j = 1$ and iii) is trivially satisfied with $x = m^\omega = y$. This completes the proof that b) implies c).

Next we prove that c) implies b). Let $a, b \in M$ and suppose that $a \approx b$ with x, y as in c). Then

$$a \equiv a^{\omega+1}_{p'} = a^{\omega+1}_{p'}a^\omega = a^{\omega+1}_{p'}yx \equiv xa^{\omega+1}_{p'}y = (b^{\omega+1}_{p'})^j \equiv b^{\omega+1}_{p'} \equiv b.$$

That b) implies a) is immediate from Lemma 2.11. For the converse, let

$$\begin{aligned} K^{M/\equiv} &= \{f\colon M/\equiv \longrightarrow K\} \\ &= \{f\colon M \longrightarrow K \mid a \equiv b \Longrightarrow f(a) = f(b)\} \end{aligned}$$

where the last equality is an abuse of notation. Then $\dim K^{M/\equiv} = |M/\equiv|$. If χ is a character, then $\chi \in K^{M/\equiv}$. Let $\chi_1, \ldots, \chi_r$ be the characters of the inequivalent irreducible representations of M. By Theorem 2.9, we have that $\chi_1, \ldots, \chi_r$ are linearly independent. Thus $r \le \dim K^{M/\equiv} = |M/\equiv|$.

Claim 1. *If $r = |M/\equiv|$, then $\equiv$ is character equivalence.*

Proof. We already have that $a \equiv b$ implies that a and b are character equivalent. Let C be the $\equiv$-class of the element a. Let

$$\delta_C(x) = \begin{cases} 1, & \text{if } x \in C \\ 0, & \text{if } x \notin C \end{cases}.$$

Under the assumption that $r = |M/\equiv|$, we have that $\{\chi_1, \ldots, \chi_r\}$ is a basis for $K^{M/\equiv}$. Therefore, $\delta_C = \sum_{i=1}^r k_i\chi_i$ for some $k_i \in K$. If a and b are character equivalent, then

$$\delta_C(b) = \sum_{i=1}^r k_i\chi_i(b) = \sum_{i=1}^r k_i\chi_i(a) = \delta_C(a) = 1.$$

So $b \in C$ and $a \equiv b$. $\square$

We now complete the proof that a) implies b) by showing that $r \geq |M/{\equiv}|$. This will also show that $\{\chi_1, \dots, \chi_r\}$ is a basis for $K^{M/\equiv}$. Let $e_1, \dots, e_k$ be representatives of the $\mathcal{D}$-classes of idempotents of M.

Claim 2. $|M/{\equiv}| \leq |\bigsqcup_{i=1}^{k} p\text{-reg}(G_{e_i})/{\sim_K}|$.

Proof. We define a surjective function $f\colon \bigsqcup_{i=1}^{k} p\text{-reg}(G_{e_i}) \longrightarrow M/{\equiv}$ such that if $g, h \in p\text{-reg}(G_{e_i})$ satisfy $g \sim_K h$, then $f(g) = f(h)$. The claim will then follow.

Let us put $f(g) = [g]_{\equiv}$. Suppose that $g, h \in G_{e_i}$ with $g \sim_K h$. Then, applying Lemma 2.5, there exist $x \in G_{e_i}$ and $j \in T$ such that $xgx^{-1} = h^j$. Putting $y = x^{-1}$, we have that $xyx = x$, $yxy = y$, $xy = e_i = yx$ and $xgy = h^j$ implying that $g \equiv h$. To show that f is surjective, let $m \in M$. Then $m_{p'}^{\omega+1} \in p\text{-reg}(G_{m^\omega})$. There exists i such that $m^\omega \mathrel{\mathcal{D}} e_i$, and $x, y \in M$ such that $xyx = x$, $yxy = y$, $xy = e_i$, $yx = m^\omega$. By Lemma 2.6 there is an isomorphism $\varphi\colon G_{m^\omega} \longrightarrow G_{e_i}$ with $\varphi(a) = xay$. So $xm_{p'}^{\omega+1}y = \varphi(m_{p'}^{\omega+1}) \in p\text{-reg}(G_{e_i})$ and $[m]_{\equiv} = [xm_{p'}^{\omega+1}y]_{\equiv} = f(xm_{p'}^{\omega+1}y)$. This establishes that f is surjective, completing the proof of the claim. □

In light of Claim 2, Theorem 2.4 and Theorem 2.7, we have

$$|M/{\equiv}| \leq |\bigsqcup_{i=1}^{k} p\text{-reg}(G_{e_i})/{\sim_K}| = \sum_{i=1}^{k} |\operatorname{Irr}_K(G_{e_i})| = |\operatorname{Irr}_K(M)| = r$$

as required. This completes the proof of the theorem. □

Let us specialize the result to the case that K is algebraically closed. In this case $K(\xi_n) = K$ and so $T = \{1\}$. Thus we recover McAlister's result [38, Theorem 2.2] and obtain its analogue in positive characteristic.

Corollary 2.13. *Let M be a finite monoid, $a, b \in M$ and K an algebraically closed field.*

1) *If the characteristic of K is 0, then the following are equivalent:*
   a) *a and b are character equivalent over K;*
   b) *there exist $x, y \in M$ such that*
      i) $xyx = x, yxy = y$
      ii) $xa^{\omega+1}y = b^{\omega+1}$
      iii) $xy = b^\omega$, $yx = a^\omega$.
2) *If the characteristic of K is $p > 0$, then the following are equivalent:*
   a) *a and b are character equivalent over K;*
   b) *there exist $x, y \in M$ such that*
      i) $xyx = x, yxy = y$
      ii) $xa_{p'}^{\omega+1}y = b_{p'}^{\omega+1}$
      iii) $xy = b^\omega$, $yx = a^\omega$.

Let us next specialize to a finite field $\mathbb{F}_q$ of order q. Then $\mathrm{Gal}(\mathbb{F}_q(\xi_n)/\mathbb{F}_q)$ is generated by the Frobenius automorphism $c \mapsto c^q$. Thus T is the subgroup of $\mathbb{Z}_n^*$ generated by q and so we have the following corollary.

Corollary 2.14. *Let M be a finite monoid, $a, b \in M$ and $\mathbb{F}_q$ be a field of order q and characteristic p. Then the following conditions are equivalent:*

a) *a and b are character equivalent over $\mathbb{F}_q$;*
b) *there exist $x, y \in M$ and $k \geq 0$ such that*
   i) $xyx = x, yxy = y$
   ii) $xa_{p'}^{\omega+1}y = (b_{p'}^{\omega+1})^{q^k}$
   iii) $xy = b^\omega$, $yx = a^\omega$.

Finally, we specialize to the case that $K = \mathbb{Q}$. In this case, $T = \mathbb{Z}_n^*$. If $g \in M$ is a group element, then since $|g|$ divides n, we have that $\{g^j \mid j \in \mathbb{Z}_n^*\}$ is precisely the set of generators of $\langle g \rangle$. From this we obtain our next result.

Corollary 2.15. *Let M be a finite monoid and $a, b \in M$. Then the following conditions are equivalent:*

a) *a and b are character equivalent over $\mathbb{Q}$;*
b) *there exist $x, y \in M$ such that*
   i) $xyx = x, yxy = y$
   ii) $x\langle a^{\omega+1}\rangle y = \langle b^{\omega+1}\rangle$
   iii) $xy = b^\omega$, $yx = a^\omega$.

We remark that $K^{M/\equiv}$ is a ring with pointwise addition and multiplication (in fact, a K-algebra) and that the proof of Theorem 2.12 also establishes the following result.

Corollary 2.16. *Let M be a finite monoid and K a field. Let $e_1, \ldots, e_k$ be representatives of the $\mathcal{D}$-classes of idempotents of M. Then the map*

$$\psi\colon \bigsqcup_{i=1}^{k} p\text{-reg}(G_{e_i})/{\sim_K} \longrightarrow M/{\equiv}$$

given by $\psi([g]_{\sim_K}) = [g]_\equiv$ is a bijection and hence induces a ring isomorphism

$$\Psi\colon K^{M/\equiv} \longrightarrow \prod_{i=1}^{k} K^{p\text{-reg}(G_{e_i})/\sim_K}$$

given by

$$\Psi(f) = \left(f\psi|_{p\text{-reg}(G_{e_1})/\sim_K}, \ldots, f\psi|_{p\text{-reg}(G_{e_k})/\sim_K} \right)$$

for $f \in K^{M/\equiv}$.

3. Virtual characters

A mapping $f: M \longrightarrow K$ in $K^{M/\equiv}$ is called a *virtual character* if f is a $\mathbb{Z}$-linear combination of irreducible characters or equivalently $f = \chi_1 - \chi_2$ where χ_1, χ_2 are characters of M. Note that the virtual characters form a subring of $K^{M/\equiv}$ because the product of two characters is the character of the tensor product of the corresponding representations [38,49].

We will need a characterization of virtual characters in Section 4. This extends results of McAlister [38] proven for the field of complex numbers.

Lemma 3.1. *Let χ be a character of a monoid M and let $e \in E(M)$. Then $\chi_{|G_e}$ is either identically zero or a character of G_e.*

Proof. Let $\rho: M \longrightarrow M_r(K)$ be a representation whose character is χ. Then $\rho(e)$ is an idempotent matrix and hence we have an internal direct sum decomposition $K^r = \operatorname{Im}\rho(e) \oplus \ker\rho(e)$. Clearly, $G_e = eG_ee$ acts by automorphisms on $\operatorname{Im}\rho(e)$ and annihilates $\ker\rho(e)$. Thus

$$\rho_{|G_e} \sim \begin{bmatrix} \hat{\rho} & 0 \\ 0 & 0 \end{bmatrix}$$

where $\hat{\rho}$ is a representation of G_e and so $\chi_{|G_e} = \chi_{\hat{\rho}}$ is a character. □

We can now characterize the ring of virtual characters. If M is a monoid, let $\operatorname{Ch}_K(M)$ denote the ring of virtual characters of M (over K). The above lemma shows that there is a natural ring homomorphism $\rho_e: \operatorname{Ch}_K(M) \longrightarrow \operatorname{Ch}_K(G_e)$ given by restriction for each $e \in E(M)$.

Theorem 3.2. *Let M be a finite monoid and K a field. Let $e_1, \ldots, e_k$ be representatives of the $\mathcal{D}$-classes of idempotents of M. Then $f \in K^{M/\equiv}$ is a virtual character if and only if $f_{|G_{e_i}}$ is a virtual character for $i = 1, \ldots, k$. Moreover, there is a ring isomorphism*

$$\Phi: \operatorname{Ch}_K(M) \longrightarrow \prod_{i=1}^{k} \operatorname{Ch}_K(G_{e_i})$$

given by

$$\Phi(f) = (f_{|G_{e_1}}, \ldots, f_{|G_{e_k}})$$

for $f \in \operatorname{Ch}_K(M)$.

Proof. Lemma 3.1 implies that the restriction of a virtual character of M to G_{e_i} is a virtual character and hence Φ is a well-defined homomorphism. We prove that Φ

is surjective by induction using the order $\preceq$ defined after Lemma 2.6. More precisely, order $e_1, \ldots, e_k$ so that $e_i \preceq e_j$ implies $i \leq j$. First note that in a finite monoid M with identity 1, one has that G_1 is the group of invertible elements of M and that $1 \in MmM$ if and only if $m \in G_1$ (cf. [56, Proposition 1.2]). In particular, $M \setminus G_1$ is closed under multiplication and 1 is not $\mathcal{D}$-equivalent to any other idempotent. Also $Me_jM \subseteq M = M1M$ and so $1 = e_k$.

If $\varphi \in \mathrm{Irr}_K(G_{e_k}) = \mathrm{Irr}_K(G_1)$, then φ extends to an irreducible representation φ' of M by putting

$$\varphi'(m) = \begin{cases} \varphi(m), & \text{if } m \in G_{e_k} \\ 0, & \text{else.} \end{cases}$$

Then $\Phi(\chi_{\varphi'}) = (0, 0, \ldots, 0, \chi_\varphi)$. It follows that $\{0\} \times \cdots \times \{0\} \times \mathrm{Ch}_K(G_{e_k})$ is in the image of Φ.

Assume that $\{0\} \times \cdots \times \mathrm{Ch}_K(G_{e_{i+1}}) \times \cdots \times \mathrm{Ch}_K(G_{e_k})$ is in the image of Φ by induction. Let $\varphi \in \mathrm{Irr}_K(G_{e_i})$. Then by Theorem 2.7 and Corollary 2.8, there is an irreducible representation φ' of M whose character χ satisfies $\chi_{|G_{e_i}} = \chi_\varphi$ and $\chi(m) = 0$ if $e_i \notin MmM$. It follows that $\Phi(\chi) = (0, \ldots, 0, \chi_{\varphi_i}, f_{i+1}, \ldots, f_k)$ where $f_j \in \mathrm{Ch}_K(G_{e_j})$ for $i+1 \leq j \leq k$. But then using the induction hypothesis, we deduce $(0, \ldots, 0, \chi_{\varphi_i}, 0, \ldots, 0)$ is in the image of Φ and so $\{0\} \times \cdots \times \mathrm{Ch}_K(G_{e_i}) \times \cdots \times \mathrm{Ch}_K(G_{e_k})$ is in the image of Φ. We conclude by induction that Φ is surjective.

Injectivity of Φ follows from the injectivity of Ψ in Corollary 2.16.

Suppose that $f \in K^{M/\equiv}$ satisfies $f_{|G_{e_i}} \in \mathrm{Ch}_K(G_{e_i})$ for $i = 1, \ldots, k$. Write $f = c_1\chi_1 + \cdots + c_s\chi_s$ with $\chi_1, \ldots, \chi_s$ irreducible characters of M and $c_1, \ldots, c_s \in K \setminus \{0\}$. We prove by induction on s that $f \in \mathrm{Ch}_K(M)$. If $s = 0$, there is nothing to prove.

Let e_i be a minimal (with respect to $\preceq$) element among the apexes of $\chi_1, \ldots, \chi_s$. Without loss of generality, we may assume that $\chi_1, \ldots, \chi_t$ have apex e_i and $\chi_{t+1}, \ldots, \chi_s$ have apex different than e_i. Then, as in the proof of Theorem 2.9, we have that $\chi_j(G_{e_i}) = 0$ if $j > t$ and that $\chi_1, \ldots, \chi_t$ restrict to distinct irreducible characters of G_{e_i}. Since $f_{|G_{e_i}}$ is a virtual character, we deduce by the linear independence of the irreducible characters of G_{e_i} over K that $c_1, \ldots, c_t \in \mathbb{Z}\cdot 1$. Moreover, $c_{t+1}\chi_{t+1} + \cdots + c_s\chi_s = f - (c_1\chi_1 + \cdots + \cdot + c_t\chi_t)$ still restricts to a virtual character at each G_{e_j} because f does, each χ_j does (by Lemma 3.1) and $c_1, \ldots, c_t \in \mathbb{Z} \cdot 1$. Thus $f - (c_1\chi_1 + \cdots + \cdot + c_t\chi_t)$ is a virtual character by induction, and hence so is f because $c_1, \ldots, c_t \in \mathbb{Z} \cdot 1$. $\square$

4. An application: a theorem of Berstel and Reutenauer

Let A be a finite set and A^* the free monoid on A, that is, the set of all words in the alphabet A. The empty word will be denoted 1. A subset $L \subseteq A^*$ is often called a (formal) *language*. In automata theory, a language $L \subseteq A^*$ is called *regular* (or *rational*) if it is accepted by a finite state automaton or equivalently if there is a finite monoid M and a surjective monoid homomorphism $\eta\colon A^* \longrightarrow M$ such that $L = \eta^{-1}(\eta(L))$ [24,25]. The *zeta function* of L is

$$\zeta_L(x) = \exp\left(\sum_{n=1}^{\infty} \frac{a_n}{n} x^n\right)$$

where a_n is the number of words in L of length n; see [10,11]. The length of a word w is denoted $|w|$.

Let K be a field and let $K\langle A\rangle$ be the ring of polynomials in non-commuting variables A with coefficients in K, that is, the free K-algebra on A. Let $K\langle\langle A\rangle\rangle$ be the ring of formal power series in non-commuting variables A with coefficients in K. A power series is *rational* if it belongs to the smallest K-subalgebra of $K\langle\langle A\rangle\rangle$ containing the polynomials and closed under inversion of power series with non-zero coefficient of 1.

One has a right $K\langle A\rangle$-module structure on $K\langle\langle A\rangle\rangle$ by defining

$$\left(\sum_{w\in A^*} c_w w\right)\cdot a = \sum_{w\in A^*} c_w wa$$

for $a \in A$. A celebrated theorem of Schützenberger states that a power series f is rational if and only if the $K\langle A\rangle$-submodule generated by f is finite dimensional over K [11]. Perrin defines a power series to be *completely reducible* if the representation of A^* associated to the $K\langle A\rangle$-submodule generated by f is a direct sum of irreducible representations [40]. The completely reducible series form a $K\langle A\rangle$-submodule.

Let us say that a power series $f \in K\langle\langle A\rangle\rangle$ is a *trace series* if there is a character $\chi\colon A^* \longrightarrow K$ of a finite dimensional representation of A^* over K such that $f = \sum_{w\in A^*} \chi(w)\cdot w$. Perrin observes that trace series, and hence linear combinations of trace series, are completely reducible [40]; see also [11].

If $L \subseteq A^*$ is a language, then its *characteristic series* is

$$f_L = \sum_{w\in L} w \in K\langle\langle A\rangle\rangle.$$

If L is regular, then it is well known that f_L is rational [11]. A language L is said to be *cyclic* if:

i) for all $s > 0$, one has $u \in L \iff u^s \in L$;
ii) $uv \in L \iff vu \in L$.

The key example is the following. Let $\mathcal{X} \subseteq A^{\mathbb{Z}}$ be a symbolic dynamical system, that is, a non-empty closed subspace (in the product topology) invariant under the shift map $\sigma\colon A^{\mathbb{Z}} \longrightarrow A^{\mathbb{Z}}$ defined by

$$\sigma(\cdots a_{-2}a_{-1}.a_0a_1\cdots) = \cdots a_{-2}a_{-1}a_0.a_1\cdots$$

(see [31] for background on symbolic dynamics, including notation). Let L be the set of all words $w \in A^*$ such that $\cdots ww.ww\cdots$ is a periodic point of $\mathcal{X}$. Then L is a cyclic language. If $\mathcal{X}$ is a shift of finite type, or more generally a sofic shift, then L will be regular. The zeta function for L gives the zeta function of the shift, and the rationality of the zeta function of a sofic shift follows from the rationality of the zeta function of any regular cyclic language [10,11].

Berstel and Reutenauer [10,11] proved that if L is a regular cyclic language, then the characteristic series f_L of L is a $\mathbb{Z}$-linear combination of trace series over any field K, and hence is completely reducible. They also used this to prove the rationality of ζ_L. We show that this result is an immediate corollary of Theorem 2.12 and Theorem 3.2. Perrin proved, using the results of McAlister [38] that f_L is a K-linear combination of trace series in the case that K is an algebraically closed field of characteristic 0.

Theorem 4.1. *(See Berstel and Reutenauer [10].) Let $L \subseteq A^*$ be a regular cyclic language and let K be a field. Then the characteristic series f_L of L is a $\mathbb{Z}$-linear combination of trace series.*

Note that since a non-negative integral combination of trace series is again a trace series, the theorem really asserts that f_L is a difference of trace series.

Theorem 4.1 is a straightforward consequence of the following lemma about finite monoids.

Lemma 4.2. *Let M be a finite monoid and K a field. Let X be a subset of M such that:*

i) *for all $s > 0$, one has $m \in X \iff m^s \in X$;*
ii) *$m_1m_2 \in X \iff m_2m_1 \in X$.*

Then the characteristic function $I_X: M \longrightarrow K$ of X defined by

$$I_X(m) = \begin{cases} 1, & \text{if } m \in X \\ 0, & \text{if } m \notin X \end{cases}$$

is a virtual character of M over K.

Proof. We retain the notation of Theorem 2.12. By hypotheses we have, for $m_1, m_2, m \in M$,

$$\begin{aligned} I_X(m_1m_2) &= I_X(m_2m_1) \\ I_X(m) &= I_X(m_{p'}^{\omega+1}) \\ I_X(m) &= I_X(m^j) \qquad \text{for } j \in T. \end{aligned}$$

Therefore, $I_X \in K^{M/\equiv}$ by Theorem 2.12.

If $e \in E(M)$ and $g \in G_e$, then $g^k = e$ for some $k > 0$. Thus $g \in X$ if and only if $e \in X$. We conclude that either $G_e \subseteq X$ or $G_e \cap X = \emptyset$. In the latter case, I_X restricts to 0 on G_e

and hence is a virtual character; in the former I_X restricts to the character of the trivial representation of G_e. We conclude that I_X is a virtual character by Theorem 3.2. □

We can now prove the theorem of Berstel and Reutenauer.

Proof of Theorem 4.1. Let $\eta\colon A^* \longrightarrow M$ be a surjective monoid homomorphism with $L = \eta^{-1}(\eta(L))$ and M finite. Let $X = \eta(L)$. Then

$$f_L = \sum_{w\in L} w = \sum_{w\in A^*} I_X(\eta(w)) \cdot w = \sum_{w\in A^*} I_X \circ \eta(w) \cdot w \tag{4.1}$$

where I_X is as in Lemma 4.2. Since L is a cyclic language and $L = \eta^{-1}(X)$, one easily checks that X satisfies the hypotheses of Lemma 4.2 and hence $I_X = \chi_1 - \chi_2$ where χ_1, χ_2 are characters of M. Indeed, we have

$$\eta(w) \in X \iff w \in L \iff w^s \in L \iff \eta(w)^s \in X$$

for all $s > 1$ and $w \in A^*$, and

$$\eta(u)\eta(v) \in X \iff uv \in L \iff vu \in L \iff \eta(v)\eta(u) \in X$$

for all $u, v \in A^*$.

Observe that if $\chi\colon M \longrightarrow K$ is a character, then $\chi \circ \eta\colon A^* \longrightarrow K$ is a character. Thus $I_X \circ \eta = \chi_1 \circ \eta - \chi_2 \circ \eta$ and so f_L is a $\mathbb{Z}$-linear combination of trace series by (4.1). □

Because it is so pretty, we recall how Theorem 4.1 implies the rationality of ζ_L for a regular cyclic language L. Also, this will highlight the importance of using virtual characters.

Theorem 4.3. *(See Berstel and Reutenauer [10].) Let $L \subseteq A^*$ be a regular cyclic language. Then ζ_L is rational.*

Proof. By Theorem 4.1 there exist characters $\chi_1, \chi_2\colon A^* \longrightarrow \mathbb{C}$ such that

$$f_L = \sum_{w\in L} w = \sum_{w\in A^*} (\chi_1(w) - \chi_2(w))\, w.$$

Let $\varphi_i\colon A^* \longrightarrow M_{n_i}(\mathbb{C})$ be representations with $\chi_i = \chi_{\varphi_i}$, for $i = 1, 2$. Let $M_1 = \sum_{a\in A} \varphi_1(a)$ and $M_2 = \sum_{a\in A} \varphi_2(a)$. A simple induction argument shows that

$$M_i^n = \sum_{|w|=n} \varphi_i(w) \tag{4.2}$$

for $i = 1, 2$. If a_n is the number of words of length n in L, then, for $n \geq 1$,

$$\begin{aligned} a_n &= \sum_{|w|=n} \chi_1(w) - \chi_2(w) \\ &= \sum_{|w|=n} \mathrm{Tr}(\varphi_1(w)) - \mathrm{Tr}(\varphi_2(w)) \\ &= \mathrm{Tr}\left(\sum_{|w|=n} \varphi_1(w)\right) - \mathrm{Tr}\left(\sum_{|w|=n} \varphi_2(w)\right) \\ &= \mathrm{Tr}(M_1^n) - \mathrm{Tr}(M_2^n) \end{aligned}$$

by (4.2).

Therefore,

$$\zeta_L(x) = \exp\left(\sum_{n=1}^{\infty} \frac{\mathrm{Tr}(M_1^n) - \mathrm{Tr}(M_2^n)}{n} x^n\right) = \frac{\exp\left(\sum_{n=1}^{\infty} \frac{\mathrm{Tr}(M_1^n)}{n} x^n\right)}{\exp\left(\sum_{n=1}^{\infty} \frac{\mathrm{Tr}(M_2^n)}{n} x^n\right)}$$

and so it suffices to show that if B is a $k \times k$-matrix over $\mathbb{C}$, then the series

$$g(x) = \exp\left(\sum_{n=1}^{\infty} \frac{\mathrm{Tr}(B^n)}{n} x^n\right)$$

is rational. But if $\lambda_1, \ldots, \lambda_k$ are the eigenvalues of B with multiplicities, then

$$g(x) = \exp\left(\sum_{n=1}^{\infty} \frac{\lambda_1^n + \cdots + \lambda_k^n}{n} x^n\right) = \prod_{i=1}^{k} \exp\left(-\log(1-\lambda_i x)\right) = \prod_{i=1}^{k} \frac{1}{1-\lambda_i x}$$

is rational (in fact, it is $1/\det(1 - xB)$). $\square$

Acknowledgment

The third author would like to thank Geoff Robinson [50] for pointing him toward Berman's paper [9].

References

[1] J. Almeida, S. Margolis, B. Steinberg, M. Volkov, Representation theory of finite semigroups, semigroup radicals and formal language theory, Trans. Amer. Math. Soc. 361 (3) (2009) 1429–1461.
[2] J. Almeida, B. Steinberg, Matrix mortality and the Černý–Pin conjecture, in: Developments in Language Theory, in: Lecture Notes in Comput. Sci., vol. 5583, Springer, Berlin, 2009, pp. 67–80.
[3] C.A. Athanasiadis, P. Diaconis, Functions of random walks on hyperplane arrangements, Adv. in Appl. Math. 45 (3) (2010) 410–437.
[4] A. Ayyer, S. Klee, A. Schilling, Combinatorial Markov chains on linear extensions, J. Algebraic Combin. 39 (4) (2014) 853–881.
[5] A. Ayyer, S. Klee, A. Schilling, Markov chains for promotion operators, Fields Inst. Commun. (71) (2014) 285–304.

[6] A. Ayyer, A. Schilling, B. Steinberg, N.M. Thiéry, Directed nonabelian sandpile models on trees, Comm. Math. Phys. (2015), in press.
[7] A. Ayyer, A. Schilling, B. Steinberg, N.M. Thiéry, $\mathscr{R}$-trivial monoids and Markov chains, Internat. J. Algebra Comput. (2015), http://dx.doi.org/10.1142/S0218196715400081, in press.
[8] C. Berg, N. Bergeron, S. Bhargava, F. Saliola, Primitive orthogonal idempotents for R-trivial monoids, J. Algebra 348 (2011) 446–461.
[9] S.D. Berman, The number of irreducible representations of a finite group over an arbitrary field, Dokl. Akad. Nauk SSSR (N.S.) 106 (1956) 767–769.
[10] J. Berstel, C. Reutenauer, Zeta functions of formal languages, Trans. Amer. Math. Soc. 321 (2) (1990) 533–546.
[11] J. Berstel, C. Reutenauer, Noncommutative Rational Series with Applications, Encyclopedia Math. Appl., vol. 137, Cambridge University Press, Cambridge, 2011.
[12] P. Bidigare, P. Hanlon, D. Rockmore, A combinatorial description of the spectrum for the Tsetlin library and its generalization to hyperplane arrangements, Duke Math. J. 99 (1) (1999) 135–174.
[13] A. Björner, Random walks, arrangements, cell complexes, greedoids, and self-organizing libraries, in: Building Bridges, in: Bolyai Soc. Math. Stud., vol. 19, Springer, Berlin, 2008, pp. 165–203.
[14] A. Björner, Note: Random-to-front shuffles on trees, Electron. Commun. Probab. 14 (2009) 36–41.
[15] K.S. Brown, Semigroups, rings, and Markov chains, J. Theoret. Probab. 13 (3) (2000) 871–938.
[16] K.S. Brown, Semigroup and ring theoretical methods in probability, in: Representations of Finite Dimensional Algebras and Related Topics in Lie Theory and Geometry, in: Fields Inst. Commun., vol. 40, Amer. Math. Soc., Providence, RI, 2004, pp. 3–26.
[17] K.S. Brown, P. Diaconis, Random walks and hyperplane arrangements, Ann. Probab. 26 (4) (1998) 1813–1854.
[18] F. Chung, R. Graham, Edge flipping in graphs, Adv. in Appl. Math. 48 (1) (2012) 37–63.
[19] A.H. Clifford, Matrix representations of completely simple semigroups, Amer. J. Math. 64 (1942) 327–342.
[20] A.H. Clifford, G.B. Preston, The Algebraic Theory of Semigroups, vol. I, Math. Surveys, vol. 7, American Mathematical Society, Providence, RI, 1961.
[21] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley Classics Lib., John Wiley & Sons Inc., New York, 1988, reprint of the 1962 original, A Wiley–Interscience Publication.
[22] T. Denton, F. Hivert, A. Schilling, N. Thiéry, On the representation theory of finite $\mathcal{J}$-trivial monoids, Sém. Lothar. Combin. 64 (2011), Art. B64d, 34 pp. (electronic).
[23] P. Diaconis, From shuffling cards to walking around the building: an introduction to modern Markov chain theory, in: Proceedings of the International Congress of Mathematicians, vol. I, Berlin, 1998, in: Doc. Math., Extra Volume, 1998, pp. 187–204.
[24] S. Eilenberg, Automata, Languages, and Machines, vol. A, Pure Appl. Math., vol. 58, Academic Press, New York, 1974.
[25] S. Eilenberg, Automata, Languages, and Machines, vol. B, Academic Press, New York, 1976, with two chapters ("Depth decomposition theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure Appl. Math., vol. 59.
[26] A. Freedman, R.N. Gupta, R.M. Guralnick, Shirshov's theorem and representations of semigroups, Pacific J. Math. (1997) 159–176 (special issue), Olga Taussky-Todd: in memoriam.
[27] O. Ganyushkin, V. Mazorchuk, B. Steinberg, On the irreducible representations of a finite semigroup, Proc. Amer. Math. Soc. 137 (11) (2009) 3585–3592.
[28] F. Hivert, A. Schilling, N. Thiéry, The biHecke monoid of a finite Coxeter group and its representations, Algebra Number Theory 7 (3) (2013) 595–671.
[29] I.M. Isaacs, Character Theory of Finite Groups, Pure Appl. Math., vol. 69, Academic Press [Harcourt Brace Jovanovich, Publishers], New York, London, 1976.
[30] G. Kudryavtseva, V. Mazorchuk, On three approaches to conjugacy in semigroups, Semigroup Forum 78 (1) (2009) 14–20.
[31] D. Lind, B. Marcus, An Introduction to Symbolic Dynamics and Coding, Cambridge University Press, Cambridge, 1995.
[32] M. Malandro, D. Rockmore, Fast Fourier transforms for the rook monoid, Trans. Amer. Math. Soc. 362 (2) (2010) 1009–1045.
[33] M.E. Malandro, Fast Fourier transforms for finite inverse semigroups, J. Algebra 324 (2) (2010) 282–312.
[34] M.E. Malandro, Inverse semigroup spectral analysis for partially ranked data, Appl. Comput. Harmon. Anal. 35 (1) (2013) 16–38.

[35] S. Margolis, B. Steinberg, The quiver of an algebra associated to the Mantaci–Reutenauer descent algebra and the homology of regular semigroups, Algebr. Represent. Theory 14 (1) (2011) 131–159.
[36] S. Margolis, B. Steinberg, Quivers of monoids with basic algebras, Compos. Math. 148 (5) (2012) 1516–1560.
[37] S.W. Margolis, F. Saliola, B. Steinberg, Combinatorial topology and the global dimension of algebras arising in combinatorics, J. Eur. Math. Soc. (JEMS) (2015), in press.
[38] D.B. McAlister, Characters of finite semigroups, J. Algebra 22 (1972) 183–200.
[39] W.D. Munn, Matrix representations of semigroups, Proc. Cambridge Philos. Soc. 53 (1957) 5–12.
[40] D. Perrin, Completely reducible sets, Internat. J. Algebra Comput. 23 (4) (2013) 915–941.
[41] I.S. Ponizovskiĭ, On matrix representations of associative systems, Mat. Sb. N.S. 38 (80) (1956) 241–260.
[42] M.S. Putcha, Complex representations of finite monoids, Proc. Lond. Math. Soc. (3) 73 (3) (1996) 623–641.
[43] M.S. Putcha, Monoid Hecke algebras, Trans. Amer. Math. Soc. 349 (9) (1997) 3517–3534.
[44] M.S. Putcha, Complex representations of finite monoids. II. Highest weight categories and quivers, J. Algebra 205 (1) (1998) 53–76.
[45] M.S. Putcha, Hecke algebras and semisimplicity of monoid algebras, J. Algebra 218 (2) (1999) 488–508.
[46] M.S. Putcha, Semigroups and weights for group representations, Proc. Amer. Math. Soc. 128 (10) (2000) 2835–2842.
[47] I. Reiner, On the number of irreducible modular representations of a finite group, Proc. Amer. Math. Soc. 15 (1964) 810–812.
[48] J. Rhodes, B. Steinberg, The q-Theory of Finite Semigroups, Springer Monogr. Math., Springer, New York, 2009.
[49] J. Rhodes, Y. Zalcstein, Elementary representation and character theory of finite semigroups and its application, in: Monoids and Semigroups with Applications, Berkeley, CA, 1989, World Sci. Publ., River Edge, NJ, 1991, pp. 334–367.
[50] G. Robinson, Which functions are linear combinations of irreducible characters for a given field $\Bbbk$?, MathOverflow, http://mathoverflow.net/q/119038 (version: 2013-01-17).
[51] F. Saliola, Eigenvectors for a random walk on a left-regular band, Adv. in Appl. Math. 48 (2) (2012) 306–311.
[52] F.V. Saliola, The quiver of the semigroup algebra of a left regular band, Internat. J. Algebra Comput. 17 (8) (2007) 1593–1610.
[53] B. Steinberg, Möbius functions and semigroup representation theory, J. Combin. Theory Ser. A 113 (5) (2006) 866–881.
[54] B. Steinberg, Möbius functions and semigroup representation theory. II. Character formulas and multiplicities, Adv. Math. 217 (4) (2008) 1521–1557.
[55] B. Steinberg, A theory of transformation monoids: combinatorics and representation theory, Electron. J. Combin. 17 (1) (2010), Research Paper 164, 56 pp. (electronic).
[56] B. Tilson, Depth decomposition theorem, chapter XI, in: Eilenberg [25], 1976, pp. 287–312.