Completely reducible sets

Dominique Perrin

22 juin 2013
General idea

- Study the class of sets such that their syntactic algebra is semisimple introduced by Christophe Reutenauer.
- Establish links with the theory of linear representations of monoids.
- Introduce the class of birecurrent sets.
- Revisit the class of cyclic sets.
A **formal series** on the alphabet $A$ with coefficients in a field $K$ is a map $S : A^* \to K$. We write $S : w \mapsto (S, w)$. Their set $K\langle A \rangle$ is a $K$-algebra:

$$(S + T, w) = (S, w) + (T, w)$$
$$(ST, w) = \sum_{uv=w} (S, u)(T, v)$$

We denote by $X$ the characteristic series of a set $X \subset A^*$.

$$(X + Y, w) = \begin{cases} 
0 & \text{if } w \notin X \cup Y \\
1 & \text{if } w \in (X \cup Y) \setminus X \cap Y \\
2 & \text{if } w \in X \cap Y 
\end{cases}$$

$$(XY, w) = \text{Card}\{(u, v) \in X \times Y \mid w = uv\}$$
Let $\lambda$ be a row $n$-vector, let $\mu$ be a morphism from $A^*$ into the monoid of $n \times n$-matrices and let $\gamma$ be a column $n$-vector, all with coefficients in $K$. The triple $(\lambda, \mu, \gamma)$ is said to be a linear representation (or recognizes) of a series $S$ if for any word $w$, 

$$(S, w) = \lambda \mu(w) \gamma.$$ 

**Example**

$\lambda = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $\mu(0) = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, $\mu(1) = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$, $\gamma = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ recognizes the series $(S, w) = \langle w \rangle_2$ (integer represented by $w$ in base 2).
Let $S$ be a formal series. For $u \in A^*$, we denote by $S \cdot u$ the series defined by $(S \cdot u, v) = (S, uv)$. The syntactic space of $S$, denoted $V_S$, is the vector space generated by the series $S \cdot u$ for $u \in A^*$. The syntactic representation of $S$ is the morphism $\psi_S : K\langle A \rangle \rightarrow \text{End}(V_S)$ defined for $x \in V_S$ and $u \in A^*$ by

$$x \psi_S(u) = x \cdot u$$

Example

Let $A = \{a\}$ and $S = a^+$. Then $\{S, S \cdot a\}$ is a basis of $V_S$ and $S$ is recognized by the linear representation $(\lambda, \mu, \gamma)$ with $\lambda = [1 \ 0]$, $\gamma = [0 \ 1]^t$ and

$$\mu(a) = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$ 

This representation is minimal.
The syntactic algebra of $S$, denoted $\mathcal{A}_S$, is the image of the free algebra $K\langle A \rangle$ by the syntactic representation (Reutenauer, 1980). Denote by $p \mapsto (S, p)$ the extension of $S$ to the free algebra on $A$. Then $\mathcal{A}_S$ is the quotient of the free algebra by the equivalence

$$p \equiv 0 \iff (S, upv) = 0 \text{ for all } u, v \in A^*.$$  \hspace{1cm} (1)

If $(\lambda, \mu, \gamma)$ is a minimal representation of $S$, then $\mu$ is equivalent to the syntactic representation of $S$.

**Example**

The representation $\mu(0) = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, $\mu(1) = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$, $\gamma = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ of $S$ (giving the number represented in base 2) is minimal. The algebra $\mathcal{A}_S$ has thus dimension 3.
Let $V$ be a vector space over a field $K$ and let $M$ be a submonoid of the monoid $\text{End}(V)$ of linear functions from $V$ into itself. A subspace $V'$ of $V$ is \textit{invariant} by $M$ if $V'm \subseteq V'$ for any $m \in M$. The monoid $M$ is called \textit{irreducible} if $V \neq 0$ and the only invariant subspaces are $0$ and $V$. Otherwise, $M$ is called \textit{reducible}.
The monoid $M$ is completely reducible if any invariant subspace has an invariant complement. If $V$ has finite dimension, a completely reducible submonoid of $\text{End}(V)$ has the following form. There exists a decomposition of $V$ into a direct sum of invariant subspaces $V_1, V_2, \ldots, V_k$,

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

such that the restrictions of the elements of $M$ to each of the $V_i$'s form an irreducible submonoid of $\text{End}(V_i)$.

In a suitable basis, $m$ in $M$ has a diagonal form by blocks,

$$m = \begin{bmatrix}
m_1 & & & \ & m_2 & & \\
& & \ddots & \\
& & & & m_k
\end{bmatrix}.$$
Let $M$ be a monoid and let $V$ be a finite dimensional vector space over a field $K$. A linear representation of $M$ over $V$ is a morphism $\varphi$ from $M$ into $\text{End}(V)$. A subspace $W$ of $V$ is invariant under $\varphi$ if it is invariant under $\varphi(M)$. The representation is completely reducible if the monoid $\varphi(M)$ is completely reducible.
A series is **completely reducible** if its syntactic representation is completely reducible. This is equivalent to the semisimplicity of its syntactic algebra. The following result was suggested to me by Christophe Reutenauer (personal communication).

**Proposition**

*Any linear combination of completely reducible series is completely reducible.*
The syntactic representation (resp. algebra) of a set $X \subset A^*$ is the syntactic representation (resp. algebra) of its characteristic series. A rational set is completely reducible if its characteristic series is completely reducible.

Example

The sets $a^*$, $a^+$ and $1$ are completely reducible. Indeed, the syntactic algebras of $a^*$ and $1$ have dimension 1. Concerning $a^+$, the linear representation seen before takes in the basis $S - S \cdot a, S \cdot a$ the form $(\lambda', \mu', \gamma')$ with $\lambda' = [1 \ 1]$, $\gamma' = [-1 \ 1]^t$ and

$$\mu'(a) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$
Example

The sets $X = (ab)^*$ and $Y = (ab)^*a$ are completely reducible. Indeed, $X$ is recognized by the linear representation $(\lambda, \mu, \gamma)$ with $\lambda = [1 \ 0]$ $\gamma = [1 \ 0]^t$ and

$$
\mu(a) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \mu(b) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}
$$

Since there are no nontrivial invariant subspaces, the representation $\mu$ is completely reducible. The series $Y$ is recognized by $(\lambda, \mu, \gamma')$ with $\gamma' = [0 \ 1]^t$. 
The set $X = a$ is not completely reducible. Indeed, $X$ is recognized by the linear representation $(\lambda, \mu, \gamma)$ with $\lambda = [1 \ 0]$, $\gamma = [0 \ 1]^t$ and

$$\mu(a) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$ 

This representation is minimal. The subspace generated by $[0 \ 1]$ is the only nontrivial invariant subspace. Thus $X$ is not completely reducible.
The family of completely reducible sets is closed by residual, complement and reversal.
The family of completely reducible sets is not closed by intersection, as shown by the example below. Since it is closed by complement is not closed by union either.

**Example**

Let $X = (ab)^*a$ and $Y = (ac)^*a$. The sets $X$ and $Y$ are completely reducible. We have $X \cap Y = a$ which is not completely reducible.
A characterization on a one-letter alphabet

Theorem

A rational set $X \subset a^*$ is completely reducible if and only if $X \cap A^+$ is periodic and the period of $X$ does not divide the characteristic of $K$. 

Dominique Perrin

Completely reducible sets
Birecurrent sets

The **minimal automaton** of a set $X \subset A^*$ is the automaton with set of states the nonempty sets $u^{-1}X$ for $u \in A^*$ and the transitions $(u^{-1}X, a) \mapsto (ua)^{-1}X$. The state $1^{-1}X = X$ is the initial state and the set of final states is the set of $u^{-1}X$ such that $u \in X$ or, equivalently, $1 \in u^{-1}X$.

A nonempty set $X$ is called **recurrent** if its minimal automaton is strongly connected. It is said to be **birecurrent** if $X$ and its reverse $\tilde{X}$ are recurrent.
The submonoid generated by a prefix code is recurrent. Indeed, let $X$ be prefix code. The submonoid generated by $X$ is right unitary, which means by definition that for any words $u, v$ if $u, uv \in X^*$, then $v \in X^*$. This implies that for any $x \in X^*$, one has $x^{-1}X^* = X^*$. Thus the minimal automaton of $X^*$ is of the form $A = (Q, i, i)$ with a set of terminal states reduced to the initial state. Since $A$ is trim, this implies that $A$ is strongly connected. Thus the submonoid generated by a bifix code is birecurrent. The following example shows that other cases occur.

Example

Let $X = \{a, ba\}$. The set $X$ is a prefix code which is not bifix. The submonoid $X^*$ is birecurrent. Indeed, the minimal automata of $X^*$ and $\tilde{X}^*$ are represented in Figure 1. Both are strongly connected.
Assume that $K$ has characteristic 0.

**Theorem**

*A birecurrent set is completely reducible.*

This implies the following result, originally from (Reutenauer, 1981), where the result is proved with a partial converse.

**Corollary**

*The submonoid generated by a rational bifix code is completely reducible.*
Let $\mathcal{A}$ be an algebra and $e \neq 0$ be an idempotent of $\mathcal{A}$. Then $e\mathcal{A}e$ is an algebra. For an $\mathcal{A}$-module $V$, the space $Ve$ is an $e\mathcal{A}e$-module called the condensed module of $V$ and $e$ the condensation idempotent. The map from $V$ to $Ve$ is called in (Green, 2007) the Schur functor and the following statement is proved.

Proposition (Green)

If $V$ is a finite dimensional irreducible $\mathcal{A}$-module such that $Ve \neq 0$, then $Ve$ is an irreducible $e\mathcal{A}e$-module.
The following statement does not seem to have been explicitly stated before. It shows that any irreducible representation of a condensation idempotent can be lifted to an irreducible representation of $M$.

**Theorem**

Let $\mathbb{A}$ be a finite dimensional algebra and let $e \in \mathbb{A}$ be an idempotent. Let $V$ be a finite dimensional $\mathbb{A}$-module. Then the following are equivalent.

(i) $V = \bigoplus_{i=1}^{m} V_i$ with the $V_i$ irreducible $\mathbb{A}$-modules and $V_i e \neq 0$ for $1 \leq i \leq m$.

(ii) $Ve$ is completely reducible over $e\mathbb{A}$, $V = Ve\mathbb{A}$ and $\{v \in V \mid v\mathbb{A}e = 0\} = 0$.

Moreover, if (i) holds, then $Ve = \bigoplus_{i=1}^{m} V_i e$ with the $V_i e$ irreducible $e\mathbb{A}$-modules.
Proof of the main result

Proposition

Let $A = (Q, i, T)$ be the minimal automaton of a set $X$. Set $S = X$, $\tilde{S} = \tilde{X}$ and $\varphi = \varphi_A$. For any word $x \in A^*$, one has

(i) $i\varphi(x) = i$ if and only if $S \cdot x = S$,
(ii) $\varphi(x) T = T$ if and only if $\tilde{S} \cdot \tilde{x} = \tilde{S}$.
Proposition

Let $A = (Q, i, T)$ be the minimal automaton of a birecurrent set $X$. Set $\varphi = \varphi_A$ and $M = \varphi(A^*)$. The monoid $M$ contains an idempotent $e$ such that

(i) $ie = i$ and $eT = T$.

(ii) The set $eMe$ is the union of a finite group $G$ and of the element 0, provided $0 \in M$.

The group $G$ defined above is called the Suschkevitch group of the monoid $M$. It is the group of the 0-minimal ideal of $M$. By Maschke’s theorem, $G$ is completely reducible. This allows to lift the irreducible constituents of $G$ to $M$. 

Dominique Perrin
Completely reducible sets
**Example**

Consider again the birecurrent set \( \{ a, ba \}^* \). The minimal ideal of \( M \) is represented in Figure 2.

\[
\begin{array}{cc}
  1, 3 & 2, 4 \\
  1, 2/3, 4 & b \quad ba \\
  1, 4/2, 3 & ab \quad aba \\
\end{array}
\]

**Fig.**: The 0-minimal ideal of \( M \).

The idempotent \( e = \varphi_A(b^2) \) is such that \( 1e = 1 \) and \( eT = T \). The set \( eMe \) is the group \( \mathbb{Z}/2\mathbb{Z} \).
A subset $X$ of a monoid $M$ is cyclic if it satisfies the two following conditions.

(i) For any $u, v \in M$, one has $uv \in X$ if and only if $vu \in X$.
(ii) For any $w \in M$ and any integer $n \geq 1$, one has $w^n \in X$ if and only if $w \in X$.

**Theorem (Berstel, Reutenauer, 1990)**

A cyclic rational set of words is completely reducible.
A series $S$ is a *trace series* if there exists a linear representation $\mu$ of $A^*$ such that for any $w \in A^*$

$$(S, w) = \text{Tr}(\mu w).$$

**Proposition (Berstel, Reutenauer, 1990)**

*The syntactic algebra of a linear combination of trace series is semisimple.*
A rational set of words \( X \) is **strongly cyclic** if there is a morphism \( \varphi \) from \( A^* \) into a finite monoid \( M \) which has a zero such that \( X = \{ x \in M \mid 0 \notin \varphi(x^*) \} \).

For a sequence of sets \( X_1, \ldots, X_n \) such that \( X_1 \supseteq X_2 \supseteq \ldots \supseteq X_n \), the *chain of differences* of the sequence is the set

\[
X = (X_1 - X_2) + (X_3 - X_4) + \ldots.
\]  

**Proposition (Beal, Carton, Reutenauer, 1996)**

*Any cyclic rational set of words \( X \) is a chain of differences of strongly cyclic rational sets.*
Example

Consider the automaton $\mathcal{A}$, called the even automaton, represented in Figure 3 on the left. The automaton on the right will be used below.

Let $X$ be the set of cyclically nonzero words for this automaton. We have

$$X = a^* \cup (a^2)^* b\{aa, b\}^* \cup a(a^2)^* b\{aa, b\}^* a.$$ 

The set $X$ is the union of two cyclic sets $a^*$ and $(a^2)^* b\{aa, b\}^* \cup a(a^2)^* b\{aa, b\}^*$. The first one is strongly cyclic but the second is not.
The following combinatorial lemma on permutations is easy to prove.

**Lemma (Lind, Marcus, 1995)**

Let $\pi$ be a permutation of a finite set $P$ and let $\mathcal{R} = \{R \subset P \mid R \neq \emptyset, \pi(R) = R\}$. Then

$$\sum_{R \in \mathcal{R}} (-1)^{\text{Card}(R)+1} \varepsilon(\pi, R) = 1$$

where $\varepsilon(\pi, R)$ denotes the signature of the restriction of $\pi$ to the set $R$.

We use this lemma to prove the following result.

**Proposition**

If $X$ is a strongly cyclic rational set, the series $X$ is a linear combination of trace series.
Example

Consider again the even automaton $\mathcal{A}$ represented in Figure 3 on the left. Let $X$ be the set of cyclically nonzero words for $\mathcal{A}$. The minimal automaton of $X$ is represented in Figure 4.

![Diagram](image)

**Fig.** The minimal automaton of $X$. 

Dominique Perrin

Completely reducible sets
Example

To obtain the syntactic representation of $X$ we write the linear representation associated with the automaton $\mathcal{A}$ in the basis formed of the row vectors

$$1 - 3 - 6, \quad 2 - 4 - 5, \quad 3, \quad 5, \quad 4, \quad 6$$

$$\psi(a) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad \psi(b) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The initial and terminal vectors in this basis are

$$\lambda = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad \gamma = \begin{bmatrix} -1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}^t$$

In this way, the representation is a direct sum of three
Let $M$ be a monoid. A character on $M$ is a map of the form $m \mapsto \text{Tr}(\rho m)$ where $\rho : M \to \text{End}(V)$ is a linear representation of $M$ over a finite dimensional vector space $V$. The character is irreducible if the representation is irreducible. Any character is a sum of irreducible characters.

**Theorem (McAlistair, 1972)**

Let $M$ be a finite monoid and let $K$ be an algebraically closed field. A map $f : M \to K$ is a linear combination of irreducible characters if and only if

(i) $f(xy) = f(yx)$ for any $x, y \in M$,
(ii) $f(x^\omega x) = f(x)$ for any $x \in M$. 

Dominique Perrin

**Completely reducible sets**
This result gives an easy proof of the theorem over an algebraically closed field. Indeed, assume that $X$ is a cyclic rational set with syntactic morphism $\varphi : A^* \rightarrow M$. Let $P = \varphi(X)$. Then the characteristic function of $P$ satisfies the conditions of McAlistair’s Theorem. This is clear for condition (i). Next, $x^\omega x \in P$ implies that $x^n \in P$ for some $n \geq 1$ and thus implies $x \in P$. Conversely, if $x \in P$, then $x^n \in P$ for all $n \geq 1$ and thus in particular $x^\omega x \in P$. Thus condition (ii) is also true. Thus the characteristic function of $P$ is a linear combination of irreducible characters. This implies that the characteristic series of $X$ is a linear combination of trace series.