Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Corina Reischer, Dan Simovici

Lattice characterizations for codes

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **52** (1972), n.3, p. 287–290.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1972_8_52_3_287_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1972.

Algebra. — *Lattice characterizations for codes* (*). Nota di CORINA REISCHER e DAN SIMOVICI, presentata (**) dal Socio B. SEGRE.

RIASSUNTO. — Si assegnano una condizione necessaria e sufficiente affinché un sottogruppo generato da un insieme finito di parole provenienti da un semigruppo libero ammetta la proprietà di decifrabilità unica, ed una caratterizzazione per i codici.

A necessary and sufficient condition that a subgroup generated by a finite set of words from a free semigroup, has the property of unique decipherability is obtained. Moreover, a characterization for codes is established.

1. Let $\mathbf{G} = \{x_1, \cdots, x_m\}$ be a finite set of symbols, let $\mathbf{S}$ be the free semigroup generated by $\mathbf{G}$, and let SK ($\mathbf{S}$) be the set of complexes of the semigroup $\mathbf{S}$.

The set SK ($\mathbf{S}$) can be organized as a semigroup using multiplication of complexes, namely

$$\forall \mathbf{K}_1, \mathbf{K}_2 \in \mathrm{SK}(\mathbf{S}), \qquad \mathbf{K}_1\mathbf{K}_2 = \{k \mid \exists k_1 \in \mathbf{K}_1, \exists k_2 \in \mathbf{K}_2, k = k_1 k_2\}.$$

We shall admit further that

$$\Phi\mathbf{K} = \Phi\mathbf{K} = \varnothing, \qquad \forall \mathbf{K} \in \mathrm{SK}(\mathbf{S}), \tag{1}$$

where $\varnothing$ is the empty complex.

It is easy to see that

$$\mathbf{K}_1(\mathbf{K}_2 \cup \mathbf{K}_3) = \mathbf{K}_1\mathbf{K}_2 \cup \mathbf{K}_1\mathbf{K}_3, \quad (\mathbf{K}_2 \cup \mathbf{K}_3)\mathbf{K}_1 = \mathbf{K}_2\mathbf{K}_1 \cup \mathbf{K}_3\mathbf{K}_1.$$

Hence SK ($\mathbf{S}$) is a multiplicative lattice in the sense used in [1], with respect to the multiplication of complexes.

Let $\mathbf{K}_1, \mathbf{K}_2 \in \mathrm{SK}(\mathbf{S})$. The right-residual $\mathbf{K}_1 : \mathbf{K}_2$ of the complex $\mathbf{K}_1$ by the complex $\mathbf{K}_2$ is the largest complex $\mathbf{R}$, satisfying the condition

$$\mathbf{R}\mathbf{K}_2 \subseteq \mathbf{K}_1.$$

In the same manner, the left-residual, $\mathbf{K}_1 :: \mathbf{K}_2$ is the largest complex $\mathbf{L}$ satisfying the condition

$$\mathbf{K}_2\mathbf{L} \subseteq \mathbf{K}_1.$$

For any two complexes $\mathbf{K}_1$ and $\mathbf{K}_2$, the residuals $\mathbf{K}_1 : \mathbf{K}_2$ and $\mathbf{K}_1 :: \mathbf{K}_2$ always exist. Indeed, if the order relation between complexes in SK ($\mathbf{S}$)

(*) This research was supported by the National Research Council of Canada grant A–7223.

(**) Nella seduta dell'11 marzo 1972.

is inclusion, and (1) is taken into account, it is clear that

$$\mathbf{K}_1 : \mathbf{K}_2 = \bigcup_{\mathbf{H}\mathbf{K}_2 \subseteq \mathbf{K}_1} \mathbf{H}$$

and

$$\mathbf{K}_1 :: \mathbf{K}_2 = \bigcup_{\mathbf{K}_2 \mathbf{H} \subseteq \mathbf{K}_1} \mathbf{H}.$$

2. A complex $\mathbf{K} \in \mathrm{SK}(\mathbf{S})$ has the property of unique decipherability (PUD) iff the equality

$$k_1 \cdots k_r = k_1' \cdots k_s',$$

with $k_i , k_i' \in \mathbf{K}$, $k_i , k_i' \neq e$ implies $k_i = k_i'$ and $r = s$; here e is the null word of $\mathbf{S}$.

A code [2] is a subsemigroup $\mathbf{Z} \subseteq \mathbf{S}$, generated by a finite set of words $\mathbf{W} = \{w_1 , \cdots , w_n\}$ which has the PUD.

We remark that the semigroup $\mathbf{S}$ always has the PUD. Let us consider the free semigroup $\mathbf{W}^*$ generated by the set of symbols $\mathbf{W} = \{w_1 , \cdots , w_n\}$. We shall assume that every subsemigroup of the semigroup $\mathbf{S}$ contains e.

Let us suppose that we have defined a mapping $\varphi : \mathbf{W} \to \mathbf{S}$. Then, by a well-known property of free semigroups, φ can be extended to a semigroup-homomorphism [1] $\varphi : \mathbf{W}^* \to \mathbf{S}$ (the encipherment homomorphism).

THEOREM 1. *$\mathbf{W}^*$ is a code iff the encipherment homomorphism is injective.*

Proof. A symbol $w_i \in \mathbf{W}$ has two interpretations as a generating symbol of the subsemigroup $\mathbf{W}^*$, and as a word in the semigroup $\mathbf{S}$. If $\mathbf{W}^*$ has the PUD, this is just the property of the semigroup-homomorphism φ of being injective.

Conversely, if φ is injective and the words $w_1 \cdots w_r$ and $w_1' \cdots w_s'$ are equal in the semigroup $\mathbf{S}$, then they have the same inverse image by φ in the subsemigroup $\mathbf{W}^*$, which means that they are composed of exactly the same set of words, hence $\mathbf{W}^*$ has the PUD.

3. By using the right-residual and left-residual of two elements from $\mathrm{SK}(\mathbf{S})$ we shall give a characterization for codes.

THEOREM 2. *Let $\mathbf{Z}$ be a subsemigroup of $\mathbf{S}$ generated by a finite set of words, and let $\mathbf{K} \in \mathrm{SK}(\mathbf{S})$. Then $\mathbf{Z}$ is a code iff*

$$(2) \qquad (\mathbf{Z} : \mathbf{K}) \cap \mathbf{Z} \neq \varnothing \neq (\mathbf{Z} :: \mathbf{K}) \cap \mathbf{Z} \quad \textit{implies} \quad \mathbf{K} = \{e\}.$$

Proof. Let $\mathbf{Z}$ be a code and let $\mathbf{K} \in \mathrm{SK}(\mathbf{S})$ with $(\mathbf{Z} : \mathbf{K}) \cap \mathbf{Z} \neq \varnothing \neq (\mathbf{Z} :: \mathbf{K}) \cap \mathbf{Z}$.

Then for any $k \in \mathbf{K}$, taking into account the antiisotony property of the operations " : " and " :: ", we have

$$\mathbf{Z} : \{k\} \supseteq \mathbf{Z} : \mathbf{K} \quad \text{and} \quad \mathbf{Z} :: \{k\} \supseteq \mathbf{Z} :: \mathbf{K};$$

hence

$$(\mathbf{Z} : \{k\}) \cap \mathbf{Z} \neq \varnothing \neq (\mathbf{Z} : : \{k\}) \cap \mathbf{Z}.$$

Therefore

$$p_1 k = p_1', \tag{3}$$

$$k p_2 = p_2', \tag{4}$$

where $p_1, p_2, p_1', p_2' \in \mathbf{Z}$. Relations (3) and (4) imply

$$p_1' p_2 = p_1 p_2'.$$

It follows from the PUD that $p_1 = p_1'$ and $p_2 = p_2'$. Comparison with (3) or (4) yields $k = e$, therefore $\mathbf{K} = \{e\}$.

Let now $\mathbf{Z}$ be a subsemigroup of $\mathbf{S}$, such that condition (2) holds. Suppose that

$$p_1, \cdots, p_r, p_1', \cdots, p_s' \in \mathbf{Z}$$

and

$$p_1 \cdots p_r = p_1' \cdots p_s'. \tag{5}$$

If $p_1 \neq p_1'$, then we may assume that $p_1 = p_1' h_1$; hence from (5) we get $h_1 p_2 \cdots p_r = p_2' \cdots p_s'$. Therefore

$$(\mathbf{Z} : \{h_1\}) \cap \mathbf{Z} \neq \varnothing \neq (\mathbf{Z} : : \{h_1\}) \cap \mathbf{Z}.$$

Taking (2) into account, we have $\{h_1\} = e$, hence $h_1 = e$ and $p_1 = p_1'$. Dividing (5) by p_1, we have

$$p_2 \cdots p_r = p_2' \cdots p_s'.$$

If $p_2 \neq p_2'$, then $p_2 \neq p_2' h_2$ and as above we obtain $h_2 = e$ and $p_2 = p_2'$.

Continuing in the same manner we have $p_i = p_i'$ and $r = s$, therefore $\mathbf{Z}$ has the PUD.

Remark 1. Let $\mathbf{S}_1$ be a subsemigroup of the free semigroup $\mathbf{S}$.

If $\mathbf{K} \subseteq \mathbf{S}_1$, then

$$\mathbf{S}_1 : \mathbf{K} \supseteq \mathbf{S}_1 \quad \text{and} \quad \mathbf{S}_1 :: \mathbf{K} \supseteq \mathbf{S}_1;$$

hence

$$(\mathbf{S}_1 : \mathbf{K}) \cap \mathbf{S}_1 \supset \varnothing \subset \mathbf{S}_1 = (\mathbf{S}_1 :: \mathbf{K}) \cap \mathbf{S}_1. \tag{6}$$

But if the subsemigroup $\mathbf{S}_1$ is a code, then $\mathbf{S}_1$ has the PUD; hence the only complex $\mathbf{K} \subseteq \mathbf{S}_1$ with the property (6) is the complex $\mathbf{K} = \{e\}$.

Remark 2. Using the encipherment homomorphism φ, Theorem 2 can be restated as follows:

The semigroup-homomorphism $\varphi : \mathbf{W}^* \to \mathbf{S}$ *is injective iff*

$$(\varphi(\mathbf{W}^*) : \mathbf{K}) \cap \varphi(\mathbf{W}^*) \neq \varnothing \neq (\varphi(\mathbf{W}^*) :: \mathbf{K}) \cap \varphi(\mathbf{W}^*)$$

implies $\mathbf{K} = \{e\}$ *for every* $\mathbf{K} \in \mathrm{SK}(\mathbf{S})$.

References

[1] G. Birkhoff, *Lattice theory*, «Amer. Math. Soc. Providence» (1968).

[2] M. Nivat, *Eléments de la théorie générale des codes*, in E. R. Caianiello (Ed), Automata Theory, Academic Press, New York 1965.