
ATTI ACCADEMIA NAZIONALE DEI LINCEI
CLASSE SCIENZE FISICHE MATEMATICHE NATURALI
RENDICONTI

CORINA REISCHER

**Une condition nécessaire et suffisante d'unique
déchiffabilité**

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche,
Matematiche e Naturali. Rendiconti, Serie 8, Vol. 59 (1975), n.5, p. 336–338.*

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1975_8_59_5_336_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Algebra. — *Une condition nécessaire et suffisante d'unique déchiffabilité.* Nota di CORINA REISCHER, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Facendo intervenire i residuali destro e sinistro di due complessi, si assegna una condizione necessaria e sufficiente affinché una parte di un monoide libero venga codificata con decifrabilità unica.

Soit I un alphabet fini, $|I| \geq 2$, et I^* le monoïde libre engendré par I . Un code avec unique déchiffabilité sur l'alphabet I [2], est un ensemble $H \subseteq I^* \setminus \{e\}$ qui possède la propriété d'unique déchiffabilité, c'est-à-dire que l'égalité

$$p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m,$$

avec $p_i, p'_j \in H$, $i = 1, \dots, n$, $j = 1, \dots, m$, entraîne $m = n$ et $p_i = p'_i$, $i = 1, \dots, n$.

Nous avons noté par e le mot vide de I^* .

Soient K_1 et K_2 deux parties du monoïde libre I^* . Le résiduel droit $K_1 : K_2$ est le plus grand complexe $D \subseteq I^*$ tel que $DK_2 \subseteq K_1$. Le résiduel gauche $K_1 :: K_2$ est le plus grand complexe $G \subseteq I^*$ tel que $K_2 G \subseteq K_1$ [1].

On peut en déduire que les opérations « : » et « :: » sont définies partout dans l'ensemble des complexes de I^* et encore plus qu'elles sont isotones quant au premier terme et anti-isotones quant au deuxième terme.

THÉORÈME. *L'ensemble $H \subseteq I^* \setminus \{e\}$ est un code avec unique déchiffabilité sur I si et seulement si pour tout $K \subseteq I^*$,*

$$(I) \quad (H : K) \cap H \neq \emptyset \neq (\hat{H}^* :: K) \cap \hat{H}^* \rightarrow K = \{e\}.$$

Ici H^* est le monoïde libre engendré par H et $\wedge : H^* \rightarrow I^*$ tel que, si $m \in H^*$, $m = (p_1, \dots, p_k)$ avec $p_i \in H$, $i = 1, \dots, k$, alors $\hat{m} = p_1 \cdots p_k$.

Démonstration. Soit H un code avec unique déchiffabilité sur I et $K \subseteq I^*$, tel que

$$(H : K) \cap H \neq \emptyset \neq (\hat{H}^* :: K) \cap \hat{H}^*.$$

Alors, pour tout mot $k \in K$, on a

$$H : \{k\} \supseteq H : K \quad \text{et} \quad \hat{H}^* :: \{k\} \supseteq \hat{H}^* :: K,$$

donc

$$(H : \{k\}) \cap H \neq \emptyset \neq (\hat{H}^* :: \{k\}) \cap \hat{H}^*.$$

(*) Nella seduta del 15 novembre 1975.

Par conséquent,

$$(2) \quad p_1 k = p'_1,$$

et

$$(3) \quad k q_1 \cdots q_h = q'_1 q'_2 \cdots q'_l,$$

avec $p_1, p'_1 \in H$, $q_i, q'_j \in H$, $i = 1, \dots, h$, $j = 1, \dots, l$.

Les relations (2) et (3) impliquent

$$p'_1 q_1 \cdots q_h = p_1 q'_1 \cdots q'_l,$$

donc, en vertu de la propriété d'unique déchiffabilité,

$$p_1 = p'_1, \quad q_1 = q'_1, \dots, q_h = q'_l.$$

En revenant à la relation (2) et en simplifiant avec p_1 on obtient $k = e$, donc $K = \{e\}$.

Soit maintenant $H \subseteq I^* \setminus \{e\}$ tel que pour tout $K \subseteq I^*$ soit satisfaite la condition (1). Nous allons montrer que H est un code avec unique déchiffabilité.

Soit

$$(4) \quad p_1 p_2 \cdots p_n = p'_1 p'_2 \cdots p'_m,$$

avec $p_i, p'_j \in H$, $i = 1, \dots, n$, $j = 1, \dots, m$.

Si $p_1 \neq p'_1$ alors on peut supposer $p_1 = p'_1 k$ et, de la relation (4), on obtient

$$k p_2 \cdots p_n = p'_2 \cdots p'_m;$$

donc

$$(H : \{k\}) \cap H \neq \emptyset \neq (\hat{H}^* : \{k\}) \cap \hat{H}^*,$$

c'est-à-dire la condition (1), donc $k = e$ et, par conséquent, $p_1 = p'_1$.

En simplifiant la relation (4) avec p_1 , on obtient $p_2 \cdots p_n = p'_2 \cdots p'_m$, et on continue le procédé.

Après un nombre fini de pas, on trouve $n = m$ et $p_i = p'_i$, $i = 1, \dots, n$.

Utilisant les quotients à gauche et à droite de H par un mot $r \in I^*$, introduit par Sabidussi [5], on peut donner la caractérisation suivante:

L'ensemble $H \subseteq I^ \setminus \{e\}$ est un code avec unique déchiffabilité sur I , si, et seulement si,*

$$Hr^{-1} \neq \emptyset \neq r^{-1}\hat{H}^* \Rightarrow r = e$$

pour tout $r \in I^$, ou*

$$Hr^{-1} = \{q \mid q \in I^*, qr \in H\}$$

et

$$r^{-1}\hat{H}^* = \{q \mid q \in I^*, rq \in \hat{H}^*\}.$$

Dans un travail antérieur [3], nous avons donné une caractérisation en terme de treillis pour les sous-semi-groupe de I^* qui possèdent la propriété d'unique déchiffabilité, à savoir le sous-semi-groupe $Z \subseteq I^*$ possède la propriété d'unique déchiffabilité si, et seulement si, pour tout $K \subset I^*$,

$$(Z : K) \cap Z \neq \emptyset \neq (Z :: K) \cap Z \Rightarrow K = \{e\},$$

qui est un cas particulier de ce théorème.

Le théorème précédent diffère de la caractérisation donnée par nous en [4].

Nous faisons la remarque que $\text{Seg}_n(H)$ introduit par Sardinias et Patterson [6] peuvent être exprimés par le résiduel gauche, à savoir

$$\text{Seg}_1(H) = H :: H$$

$$\text{Seg}_{n+1}(H) = (\text{Seg}_n(H) :: H) \cup (H :: \text{Seg}_n(H)),$$

et la caractérisation trouvée par eux pour les codes $H \subset I^*$ avec unique déchiffabilité revient à

$$[(\text{Seg}_n(H) :: H) \cup (H :: \text{Seg}_n(H))] \cap H = \emptyset,$$

pour tout $n \geq 1$.

Finalement, nous faisons remarquer que la condition que nous avons trouvé diffère de la condition de Nivat [2],

$$\hat{H}^* u \cap \hat{H}^* \neq \emptyset \neq u \hat{H}^* \cap \hat{H}^* \Rightarrow u \in \hat{H}^*,$$

pour tout $u \in I^*$.

BIBLIOGRAPHIE

- [1] G. BIRKHOFF (1968) - *Lattice Theory*, « Amer. Math. Soc. Providence ».
- [2] M. NIVAT (1966) - *Éléments de la théorie générale des codes*, da « Automata Theory » (E. R. Caianiello, ed.), Academic Press, New York, London, 278-294.
- [3] C. REISCHER et D. SIMOVICI (1972) - *Lattice characterizations for codes*, « Acad. Naz. dei Lincei Rend. di Sc. fis. mat. e nat. », ser. VII, 52, 287-290.
- [4] C. REISCHER et D. SIMOVICI (1973) - *Elemente de teoria generala a codurilor*, Universitatea « Al. I. Cuza », Iași, Romania.
- [5] G. SABIDUSSI (1969) - *Finite automate over monoids*, « Math. Reporth », No 2, Vol. 1, Dep. of Math., McMaster Univ., March.
- [6] A. A. SARDINAS et G. W. PATTERSON (1953) - *A necessary and sufficient condition for the unique decomposition of code messages*, IRE Intern. Conv., « Record », 8, 107-108.