SÉMINAIRE N. BOURBAKI

DOV TAMARI

Machines logiques et problèmes de mots. II : problèmes de mots indécidables

Séminaire N. Bourbaki, 1954, exp. n° 61, p. 109-119

<http://www.numdam.org/item?id=SB_1951-1954__2__109_0>

Séminaire BOURBAKI
(Février 1952)

MACHINES LOGIQUES ET PROBLEMES DE MOTS

II : PROBLEMES DE MOTS INDECIDABLES

par Dov TAMARI

INTRODUCTION. - Rappelons de notre exposé précédent un résultat de TURING [5] : "Il ne peut y avoir une méthode générale, c'est-à-dire une machine E , pour déterminer si une machine donnée quelconque M imprime, oui ou non, (au moins) une fois un certain des symboles de son tableau (choisi au hasard), disons s_p" .

La méthode des démonstrations de l'indécidabilité de certains problèmes de mots consiste essentiellement dans la réduction d'un problème de décision B (ici problème de mots) à un autre problème A dont l'indécidabilité est déjà démontrée. Etant donnés deux monômes quelconques A et Z d'un système multiplicatif muni d'une certaine relation R , peut-on décider si A et Z sont dans la relation R , ou non ? Autrement dit : R(A , Z) est-elle vraie ou fausse ? En fait nous considérons seulement des systèmes associatifs (dans ce cas les monômes sont dits mots) et des relations de préordre régulière (homogènes de deux côtés). Alors la question prend une forme plus particulière : Peut-on lier A et Z par une chaîne finie de mots $A = M_0 , M_1 , \dots , M_n = Z$ telle que $M_{i-1} \longrightarrow M_i$ est immédiatemment assurée par les axiomes du système (généraux et relations définissantes particulières). On essaie d'interpréter cette chaîne de mots comme une suite de C.C. d'une machine : A correspondra à la C.C. initiale et Z à la C.C. finale d'un certain intervalle de temps pendant lequel on suit le travail de la machine M , ou, plus commodément, celui de sa machine dérivée M' fournissant justement la suite des C.C., par exemple sous forme de U(M) (la machine universelle pourvue de la S.D. de M). En prescrivant pour A un mot quelconque ne contenant pas la lettre s_p et pour Z un mot contenant s_p on peut transférer l'indécidabilité de 1) aux problèmes de mots :

1° des diverses classes de demi-groupes libres et non libres, préordonnés ou abstraits, résultats dûs principalement à POST [3] (voir THUE [4])

2° des semi-groupes (demi-groupes simplifiables) suivant TURING [6].

1a. L'indécidabilité du problème de mots dans la classe des demi-groupes libres préordonnés à un nombre fini de générateurs et de relations définissantes (problème "Semi-Thue").

Soit $a_1 , a_2 , \dots , a_\sigma$ (σ fini) un alphabet abstrait (non-ordonné) engendrant un ensemble de mots $\underset{\sim}{D}$; $\underset{\sim}{D}$, muni d'une multiplication évidemment associative par juxtaposition, constitue un demi-groupe abstrait libre à σ générateurs (à des isomorphismes, c'est-à-dire des changements de notation biunivoques, près) ; en fait $\underset{\sim}{D}$ est ispo facto un semi-groupe, à savoir le type d'isomorphisme du semi-groupe libre à σ générateurs (la simplifiabilité bilatérale $(AC = BC) \vee (CA = CB) \Rightarrow A = B$ est immédiate). Le mot vide I joue le rôle de l'unité : $AI = IA = A$. Notons généralement les mots par des majuscules (sauf ceux réduits à un seul générateur).

Introduisons un préordre à partir d'un nombre fini de relations définissantes $A_i \longrightarrow B_i$, $i = 1 , \dots \rho$, $A_i , B_i \in \underset{\sim}{D}$ quelconques, engendrant le $\underset{\sim}{D}_{p_o}$ par

1° fermeture réflexive : $M \longrightarrow M$ pour $M \in \underset{\sim}{D}$ quelconque ;

2° homogénéité bilatérale ou régularité : $A \longrightarrow B \Rightarrow PAQ \longrightarrow PBQ$ ou $(A \longrightarrow B)$ et $(C \longrightarrow D) \Rightarrow AC \longrightarrow BD$ (ces deux formes de l'axiome ne sont plus équivalentes pour le calcul des "longueurs de démonstrations") ;

3° fermeture transitive (ou "de chaînes") : $A \longrightarrow B$, $B \longrightarrow C \Longrightarrow A \longrightarrow C$. Nous supprimons les démonstrations faciles. Remarquons seulement que le préordre n'est pas nécessairement simplifiable : on peut avoir $A = C\overline{A}D \longrightarrow B = C\overline{B}D$ sans avoir ni $\overline{A} \longrightarrow \overline{B}$, ni $C\overline{A} \longrightarrow C\overline{B}$, ni $\overline{A}D \longrightarrow \overline{B}D$.

Soit (A , Z) un couple quelconque de mots de $\underset{\sim}{D}_{p_o}$: $A \longrightarrow Z$, oui ou non ? Ce problème est <u>indécidable</u> (dans sa généralité). On se facilite la tâche en démontrant plus : l'indécidabilité dans une sous-classe ; on localise plus précisément un des domaines de l'indécidabilité en choisissant des types plus particuliers, étroitement liés aux machines de Turing.

L'ensemble des quadruples-instructions d'une table $q_i \, s_j \, \underset{\sim}{A}_k \, q_\ell$ $(i = 1 , \dots , n)$; $j = 0 , 1 , \dots , m$; $\underset{\sim}{A}_k = s_k$ pour $k = 0 , 1 , \dots , m$, $\underset{\sim}{A}_{-1} = \underset{\sim}{R}$, $\underset{\sim}{A}_{-2} = L$ (mouvements à droite et à gauche) ; $k = k(i , j)$, $\ell = \ell(i , j)$ fonctions uniformes à valeurs-indice) se décompose en trois sous-ensembles disjoints

$$\underset{\sim}{(N)} \quad k \geqslant 0 \quad : \quad q_{i_o} \, s_{j_o} \, s_k(i_o , j_o) \, q_\ell(i_o , j_o)$$

$$\underset{\sim}{(R)} \quad k = -1 \quad : \quad q_{i'} \, s_{j'} \, \underset{\sim}{R} \, q_\ell(i' , j')$$

$$\underset{\sim}{(L)} \quad k = -2 \quad : \quad q_{i''} \, s_{j''} \, \underset{\sim}{L} \, q_\ell(i'' , j'') \ .$$

Considérons les q et s comme des générateurs a_i $(\sigma = n + m + 1)$. La bande porte déjà un certain mot $A = s_{j_1} \, s_{j_2} \dots s_{j_{\alpha-1}} \, q_i \, s_{j_\alpha} \dots s_{j_\beta}$ ne contenant pas la lettre s_p ; q_i , la seule q_i de A , vise (scrute) le symbole s_{j_α} et

peut être n'importe où dans le mot sauf à sa fin. A étant ipso facto précédé et suivi de $\ldots s_0\, s_0\, s_0$ et de $s_0\, s_0\, s_0 \ldots$, il est commode d'introduire un symbole "ad hoc" h au lieu du dernier s_0 avant et le premier s_0 après le mot complet (C.C.) et d'écrire, par exemple, hAh etc.

Si $q_{\overline{i}}\, s_{j_\alpha}$ n'est pas une situation possible de notre machine, c'est-à-dire si le couple $\overline{i}/j_\alpha$ n'apparaît pas actuellement dans le tableau, la machine est arrêtée, A est aussi la C.C. finale et aucun problème ne se pose. Autrement, on obtient la C.C. immédiatement suivante par une substitution bien déterminée d'un des trois types :

$$(+)\quad \begin{cases} (N) & q_{i_o}\, s_{j_o} \longrightarrow q_\ell(i_o\,,\, j_o)\, s_k(i_o\,,\, j_o) \\ (R) & q_{i'}\, s_{j'} : \longrightarrow s_j\,,\, q_\ell\,, \quad \text{resp.} \quad q_{i'}\, s_{j'}\, h \longrightarrow s_{j'}, q_\ell\, s_o\, h \\ (L) & s_j\, q_{i''}\, s_{j''} \longrightarrow q_\ell\, s_j\, s_{j''}\,, \quad \text{resp.} \quad h q_{i''}\, s_{j''} \longrightarrow h q_\ell\, s_o\, s_{j''}\,. \end{cases}$$

Il n'y a pas de difficulté de supposer que la machine commence avec le mot arbitraire $A = a_{j_1}\, a_{j_2}\, a_{j_3} \ldots a_{j_\beta}$. Ajoutons "ad hoc" $2\beta - 1$ instructions avec les 2β I.C. nouvelles $\overline{q}_\alpha$ et q'_α :

$$\overline{q}_1\, s_o\, a_{j_1}\, q'_1\,;\; q'_1\, a_{j_1}\, R\overline{q}_2\,;\; \overline{q}_2\, s_o\, a_{j_2}\, q_2\,;\; \ldots$$

$$\ldots\,;\; \overline{q}_\beta\, s_o\, a_{j_\beta}\, q'_\beta\,;\; q'_\beta\, (\text{non-}a_{j_\alpha})\, Lq'_\beta\,;\; q'_\beta\, a_{j_\alpha}\, a_{j_\alpha}\, q_{\overline{i}}\,.$$

Où aboutira, en commençant avec la bande vide et la I.C. initiale $\overline{q}_1$ au mot désiré, la machine se trouvant dans la I.C. $q_{\overline{i}}$ scrutant le lieu prescrit. Cette C.C. atteinte, la machine suivra son tableau primitivement donné sans que le tableau (initial "ad hoc") supplémentaire intervienne.

Notons notre machine arbitraire T'. Par les méthodes de l'exposé précédent on peut ajouter un dispositif entrant en action au moment où la machine imprime la première fois le symbole s_p (si elle l'imprime) et déclenchant les manipulations suivantes :

1° Rayer toutes les instructions de T' contenant des $s_j = s_p$; autrement dit, la machine s'arrête ;

2° remplacer le q_1 des instructions dont $s_k = s_p$ par une I.C. q_{n+1} nouvellement introduite ;

3° ajouter les nouvelles instructions que nous écrivons immédiatement en forme de substitutions :

(++) $s_x\, q_{n+1} \longrightarrow q_{n+1}$; $hq_{n+1} \longrightarrow hq_{n+2}$; $q_{n+2}\, s_x \longrightarrow q_{n+2}$ (s_x quelconque) .

Appelons la machine, ainsi modifiée de T' primitive, T" ; en tous cas, T" possède encore le déterminisme rigoureux d'une machine de Turing. Le s_p apparaissant la première fois étant un s_k , le q_1 de l'instruction appliquée sera remplacé par q_{n+1} ; en conséquence on rayera les voisins gauches jusqu'à la première lettre ; alors q_{n+1} devient q_{n+2} et on commence à rayer ce qui est peut-être encore resté à droite du premier s_p . Enfin on obtient une dernière C.C. vide $hq_{n+2}h$ avec laquelle la machine T" s'arrête.

CONCLUSION. - Si l'on pouvait décider dans le demi-groupe préordonné qui est le semi-groupe libre abstrait engendré par

$$h\ ,\ s_o\ ,\ s_1\ ,\ \cdots\ ,\ s_m\ ;\ q_1\ ,\ q_2\ ,\ \cdots\ ,\ q_n\ ,\ q_{n+1}\ ,\ q_{n+2}$$

et régulièrement préordonné par les relations définissantes (+) et (++) si $hAh \longrightarrow hq_{n+2}h$, oui ou non, où A est un mot contenant un seul q_i , $i \leq n$, non à la fin, les autres lettres étant des $s_j \neq s_p$, on aurait aussi décidé si T' imprime s_p , en contradiction avec le résultat (1). A plus forte raison, le problème de mots dans la classe des demi-groupes libres préordonnés pour des couples quelconques (A , Z) est indécidable.

1b. <u>L'indécidabilité du problème de mots dans la classe des demi-groupes abstraits quelconques à un nombre fini de générateurs et de relations définissantes (problème de Thue)</u>.

On peut se borner aux demi-groupes effectivement non-libres, le problème de mots des demi-groupes libres abstraits (en fait des semi-groupes) est évidemment décidable d'une manière triviale.

On obtient le demi-groupe abstrait général (non-libre) à un nombre fini de générateurs et de relations définissantes $A_i = B_i$ du $\underset{\sim}{D}_{p_o}$ libre préordonné avec les relations définissantes $A_i \longrightarrow B_i$ et $B_i \longrightarrow A_i$ (dans ce cas particulier le préordre est symétrique) par l'introduction de l'équivalence $\underset{\sim}{E}$ canoniquement associée aux relations de préordre symétriques :

1° $(A \longrightarrow B)$ et $(B \longrightarrow A) \Longleftrightarrow A \equiv B \pmod{\underset{\sim}{E}}$;

2° passage à la structure quotient $\underset{\sim}{D'} = \underset{\sim}{D}_{p_o}/\underset{\sim}{E}$.

Considérons d'abord le système T"' constitué par le mot initial $hq_{n+2}h$ et les opérations inverses de T" . Ce système n'est plus, en général, une machine de Turing parce que les inverses de substitutions univoques ne sont plus nécessairement univoques, et la marche d'une "machine" correspondante ne sera plus déterministique. Ce sera plutôt une "machine avec choix". Toutefois, il est évident que le mot initial de T"', $hq_{n+2}h$ est un mot final de T" si et seulement si son mot initial (de T") hAh peut être atteint par une chaîne de T"' parce que l'existence de la chaîne de T" $hAh = M_o \longrightarrow M_1 \longrightarrow \ldots \longrightarrow M_z = hq_{n+2}h$ équivaut à l'existence de la chaîne inverse dans T"' .

Construisons maintenant un nouveau système T en ajoutant à T"' ses opérations inverses ; autrement dit : T est un système qui a comme T"' le mot initial $hq_{n+2}h$ mais les opérations sont celles de T" et de T"' réunies. On a le lemme suivant :

LEMME. - La classe des mots de T , K(T) , est identique à K(T"') ; autrement dit : l'adjonction à T"' de ses opérations inverses ne sert à rien, elle n'étend pas la classe des mots qu'on peut atteindre à partir de $hq_{n+2}h$.

DÉMONSTRATION. - Evidemment $K(T"') \subset K(T)$. Montrons que $K(T) \subset K(T"')$: Soit

$$hq_{n+2}h = M_o \xrightarrow{O_1} M_1 \xrightarrow{O_2} \ldots \xrightarrow{O_{z-1}} M_{z-1} \xrightarrow{O_z} M_z = M$$

une chaîne quelconque de T , donc M un mot quelconque de K(T) . La première opération de la chaîne, O_1 , est évidemment une opération de T"' parce que qu'aucune opération de T" ne s'applique à $hq_{n+2}h$, l'arrêt de la machine. Soit O_{i+1} la première opération de la chaîne n'étant pas de T"' , donc de T" ; O_i étant encore de T"' , son inverse, $\overline{O}_i$ est de T" ; mais les deux s'appliquent à M_i , la première pour produire M_{i+1} , la seconde pour reconduire éventuellement à M_{i-1} . En conséquence du caractère déterministique (univoque) de T" , $O_{i+1} = \overline{O}_i$ et donc aussi $M_{i-1} = M_{i+1}$. On peut donc supprimer les deux chaînons O_i et O_{i+1} , tout en préservant une chaîne plus courte liant encore les mêmes extrémités. En répétant, éventuellement, ce raisonnement on obtient une chaîne dont toutes les opérations appartiennent à T"' . Donc : $M \in K(T"')$ et $K(T) \subset K(T"')$.

CONCLUSION. - $hq_{n+2}h \in K(T'') \iff hAh \in K(T''') \iff hAh \in K(T)$; c'est-à-dire la décidabilité de $hAh \to hq_{n+2}h$ dans $\underset{\sim}{D}_{p_o}$ libre équivaut à celle de $hAh = hq_{n+2}h$ dans $\underset{\sim}{D}'$. D'où le théorème.

REMARQUE. - A plus forte raison on a l'indécidabilité dans les classes plus générales comme celle des demi-groupes préordonnés quelconques. Mais il n'est pas immédiatement évident (par la démonstration ci-dessus) qu'on a déjà l'indécidabilité pour les demi-groupes à deux générateurs, disons a et b . Mais d'après HALL jr., on a le théorème suivant :

THÉORÈME. - Le problème de mots d'un $D' = \underset{\sim}{D}_\sigma / E_\sigma$ quelconque peut être réduit à celui d'un $D'(a , b) = \underset{\sim}{D}_2 / E_2$, c'est-à-dire d'un demi-groupe à deux générateurs. D'où le

COROLLAIRE. - Le problème de mots dans la classe des demi-groupes à deux générateurs est indécidable.

DÉMONSTRATION. - Supposons d'abord qu'aucun mot A_i et B_i des relations définissantes de l'équivalence E_σ ne soit vide. Alors le mot vide n'est équivalent qu'à lui-même. Par la correspondance biunivoque

$$a_i \leftrightarrow \underbrace{babaa \ldots aabaab}_{(i+2)\text{fois}} = a_i! \leftarrow a_i!$$

on représente fidèlement (isomorphiquement) non seulement le demi-groupe libre $\underset{\sim}{D}_\sigma$ dans une partie du demi-groupe libre $\underset{\sim}{D}_2$ qu'on notera $\underset{\sim}{D}_\sigma!$, mais aussi, $\underset{\sim}{D}_\sigma!$ étant une réunion de classes mod $\underset{\sim}{E}_2$ de

$$\underset{\sim}{D}_2 \quad (Z' \equiv X\,!(E_2) \Rightarrow Z' = Z!(Z \equiv X(E_\sigma)) ,$$

$\underset{\sim}{D}' = \underset{\sim}{D}_\sigma / \underset{\sim}{E}_\sigma \cong \underset{\sim}{D}_\sigma!/\underset{\sim}{E}_2 = \underset{\sim}{D}'_\sigma!$ où $\underset{\sim}{E}_2$ est l'équivalence engendré dans $\underset{\sim}{D}_2$ par les relations définissantes $A_i\,! \equiv B_i\,!$; ceci en vertu d'un lemme qu'on démontre par induction : $M! = P'babNbaabQ' \Longrightarrow M = PRQ$ où $P' = P!$, $babNbaab = R!$, $Q' = Q!$.

Dans le cas où il y a des mots vides dans les relations définissantes de $\underset{\sim}{E}_\sigma$ on procède de la même manière sauf qu'on fait correspondre à une relation définissante de $\underset{\sim}{E}_\sigma$ de la forme $I \equiv B_i \pmod{\underset{\sim}{E}_\sigma}$ la relation définissante $baab = baab(B_i!) \pmod{\underset{\sim}{E}_2}$.

2. L'indécidabilité du problème de mots dans la classe des semi-groupes (demi-groupes simplifiables) à un nombre fini de générateurs et de relations définissantes (Théorème de Turing [6]).

L'idée principale de la démonstration de Turing [6] est la même que celle de Post [3], mais de nouvelles astuces sont nécessaires ou, du moins, commodes pour surmonter les difficultés créées par la simplifiabilité, jusqu'à déborder le cadre des machines M.T.

Perfectionnons d'abord la machine de Turing : on divise les I.C., les q_i, en deux classes, les gauches, notées ℓ_i, et les droites notées r_i, en convenant d'écrire les r_i à gauche du symbole visé (elles visant donc à droite) et les ℓ_i inversement. Une situation $q_i\, s_h$ est donc ou bien $r_j\, s_h$, ou bien $s_h\, \ell_i$. L'adjonction éventuelle de I.C. superflues permet d'égaliser le nombre des ℓ_i et des r_i ($i = 1, \ldots, R$). Cet astuce entraîne la possibilité de diverses économies dans la composition d'une table.

Ainsi on voit que le changement $r_i \to \ell_i$ seul exprime déjà un mouvement $\underset{\sim}{L}$. On peut donc réunir dans la même instruction-quadruple un changement de symbole, une impression $s_h \to s_{h'}$, et on obtient des instructions de la forme (en employant l'écriture des substitutions, une instruction s'écrit situation $\to$ $\to$ comportement)

$$r_i\, s_h \to \ell_{i'}\, s_{h'} \text{ et de même } s_h\, \ell_i \to s_{h'}\, r_{i'}.$$

Remarquons que les deux comportements ne sont pas des situations. C'est, en fait une règle parce qu'autrement cette 2e situation entraînera un second comportement et ainsi toute une suite déjà bien déterminée par la première situation, jusqu'au premier comportement qui n'est plus une situation. La suite intermédiaire étant évidemment sans intérêt on retient seulement des comportements n'étant pas des situations, à savoir avec l'ordre (I.C. et symbole) inversé. Les comportements sont donc $s_{h'}\, r_{i'}$ et $\ell_{i'}\, s_{h'}$ et les instructions des quatre types :

$$r_i\, s_h \to \ell_{i'}\, s_{h'} \qquad s_h\, \ell_i \to s_{h'}\, r_{i'}$$

$$r_i\, s_h \to s_{h'}\, r_{i'} \qquad s_h\, \ell_i \to \ell_{i'}\, s_{h'},$$

auxquelles s'ajoutent encore des formes particulières pour les opérations à la "frontière" (TURING emploie les notations s_4, s_3, ℓ_0 au lieu des notations de POST de la même signification s_h, s_p, q_{n+2} ; rappelons que les

symboles fixes s_o , espace vide, $s_1 = 0$ et $s_2 = 1$ suffisent pour une M.T.). L'idée générale de la démonstration s'appuie donc sur l'existence d'une machine universelle $\mathcal{U}$ telle qu'il n'existe pas de méthode générale pour déterminer si $s_4\ \ell_o\ s_4$ est une Conf.C. descendant d'une C.C. donnée $s_4\ C\ s_4$, où $\mathcal{U}$ procède à $s_4\ \ell_o\ s_4$, aprés avoir imprimé une fois s_3 , et s'arrête, ℓ_o étant une nouvelle I.C. adjointe "ad hoc" sans apparâtre parmi les situations.

Faisons correspondre à $\mathcal{U}$ un semi-groupe $\underset{\sim}{S}_o$ d'une manière qui peut apparaître à première vue assez compliquée :

Les instructions (entrées) de la table étant numérotées I_1 , I_2 , ... , I_M , faisons correspondre à chacune deux relations définissantes dites l'une "de la 1re phase", Φ_1 , l'autre "de la 2e phase", Φ_2 , (ces noms s'expliquent bientôt) moyennant deux fonctions (changements de notation) φ_1 et φ_2 ; à I_m : $S_m \rightarrow C_m$ correspond $\varphi_1(S_m) \rightarrow \sigma_m\ \varphi_1(C_m)\tau_m$ et $\sigma_m\ \varphi_2(C_m)\tau_m \rightarrow \varphi_2(S_m)$ où

$$\varphi_1(\ell_i) = u_i \quad \varphi_1(s_h X) = j_h\ \varphi_1(X)\ , \quad \varphi_2(\ell_i) = w_i \quad \varphi_2(s_h X) = n_h\ \varphi_2(X)$$

$$\varphi_1(r_i) = v_i \quad \varphi_1(X s_h) = \varphi_1(X) k_h\ , \quad \varphi_2(r_i) = z_i \quad \varphi_2(X s_h) = \varphi_2(X) p_h\ .$$

Remarquons que $\varphi_1(s_h)$ et $\varphi_2(s_h)$ n'ont pas de sens univoque, mais les fonctions inverses sont univoques.

Ainsi on obtient pour

$$I_m : r_i\ s_h \rightarrow \ell_i,\ s_h, \quad (\Phi_1)\ v_i\ k_h \rightarrow \sigma_m\ u_i,\ k_h, \tau_m, \quad (\Phi_2)\ \sigma_m\ w_i,\ p_h, \tau_m \rightarrow z_i\ p_h\ ;$$

etc.

Ces relations (des deux phases) sont dites "relations principales". Pour les symboles $x(u_i\ ,\ v_i\ ,\ w_i$ et z_i , les valeurs des I.C. ℓ_i et $r_i)$ valent, en plus, les relations de commutation $\sigma_m\ x = x\ \tau_m$ (en fait, il suffit que $\sigma_m\ u_i \rightarrow u_i\ \tau_m$, $v_i\ \tau_m \rightarrow \sigma_m\ v_i$ et $w_i\ \tau_m \rightarrow \sigma_m\ w_i$, $\sigma_m\ z_i \rightarrow z_i\ \tau_m$) auxquelles s'ajoute encore une autre relation de commutation $y\ \tau_m \rightarrow \sigma_m\ y$ et les relations particulières $j_4\ u_o \rightarrow n_4\ y$, $y k_4 \rightarrow w_o\ p_4$. Résumons donc les générateurs de $\underset{\sim}{S}_o$:

$$y\ ;\ \sigma_m\ ,\ \tau_m \quad (m = 1\ ,\ \ldots\ ,\ M);\ u_o, w_o,\ u_i, v_i, w_i, z_i \quad (i = (0)1\ ,\ \ldots\ , \varphi);$$

et

$$j_h\ ,\ k_h\ ,\ n_h\ ,\ p_h \quad (h = C\ ,\ 1\ ,\ \ldots\ ,\ N) \quad (N = 4)\ .$$

On appelle les j_h , n_h , σ_h symboles gauches, les k_h , p_h , t_m symboles droits ; un mot avec un seul symbole actif, tel que tous les symboles à sa gauche sont des symboles gauches et tous ceux à sa droite des droits est dit mot normal ; par exemple toutes les relations définissantes constituent des mots normaux. On divise encore les générateurs en symboles de Φ_1 ; u_i , v_i , j_h , k_h ; de Φ_2 : w_i , z_i , n_h , p_h ; y appartient à une phase intermédiaire, et les σ_m et τ_m appartiennent à toutes les Φ .

Nous sommes maintenant en état d'esquisser les grandes lignes du processus à trois phases, $\mathfrak{V}'$, construit par Turing :

A la C.C. initiale $C = C_o$ de la machine $\mathfrak{V}$ on fait correspondre le mot $\varphi_1(C) = H_o \leftarrow S_{\underset{\sim}{m}\,o}$. Correspondant à la suite des C.C. de la machine , on obtient $C = C_o$, C_1 , ... , C_r , ... une chaîne de mots normaux H_o , H_1 , ... , H_r , ... par l'application des Φ_1 relations. Il est immédiat que les H_r sont des mots $\varphi_1(C_r)$ avec, en plus des couples ... σ_{m_i} ... τ_{m_i} ... ($i = 1$, ... , r) parsemés, sédiments du passage par le i-ième pas ; mais en notant γ_1 la fonction inverse de φ_1 , prolongée encore pour faire disparaître, c'est-à-dire ignorer, les σ_m et les τ_m , alors chaque mot H_r détermine bien sa C_r par $\gamma_1(H_r) = C_r$. Si $\mathfrak{V}$ n'imprime jamais s_3 elle continuera à travailler sans fin (pourvu qu'elle soit bonne !) et n'arrivera donc jamais à la C.C. $s_4 \; \ell_o \; s_4$ parce que le dispositif de modification n'agira pas ($\mathfrak{V}$ est une machine universelle spécialisée par la C.C. initiale avec, en plus, ce dispositif). Mais si $\mathfrak{V}$ imprime une fois s_3 , donc arrive à $C_R = s_4 \; \ell_o \; s_4$ où elle s'arrête, la chaîne arrivera au mot $H_r = \Sigma\, j_{\not\Phi} \Sigma'' \, u_o \, T' \, k_4 \, T''$ où les Σ et T sont des mots composés de σ ou de τ exclusivement. C'est la fin de Φ_1 , et la phase intermédiaire peut commencer. Elle transforme (vérification facile) le Φ_1-mot H_R dans le Φ_2-mot $\chi(H_R) = \Sigma' \, n_4 \, \Sigma'' \, w_o \, T' \, p_4 \, T''$ légitimement dans les $S_{\underset{\sim}{m}\,o}$ moyennant les relations de commutation et les relations spéciales. On vérifie que la fonction χ est le changement de notation remplaçant les Φ_1-symboles par les Φ_2-symboles correspondants aussi dans la Φ_2 , qui n'est pas autre chose que l'opération inverse de toute la Φ_1 , en exécutant les opérations inverses dans l'ordre inverse ; en particulier, Φ_2 fait disparaître l'un après l'autre les ... σ_m ... τ_m ... parsemés. D'ailleurs, en appliquant d'une manière analogue la fonction γ_2 , l'inverse de φ_2 avec, en plus, $\gamma_2(\sigma_m) = I$ (mot vide) = $\gamma_2(\tau_m)$, on aura de même $\gamma_2(\chi(H_r) = C_r$. On arrive ainsi, enfin au mot $\varphi_2(C) = \chi(H_o)$ et on a démontré :
$C = C_o \rightarrow s_4 \; \ell_o \; s_4$ dans $\mathfrak{V} \Longrightarrow \varphi_1(C) \rightarrow \varphi_2(C)$ dans $S_{\underset{\sim}{m}\,o}$ (resp. $\varphi_1(C) = \varphi_2(C)$);

autrement dit : une condition suffisante pour que $\varphi_1(C) \to \varphi_2(C)$ soit une relation de S_{mo} est que $s_4 \ \ell_o \ s_4$ soit un descendant de C dans la machine $\mathcal{O}$, (donc que $\mathcal{O}$ imprime s_3) ; (ou, inversement, cette relation dans S_{mo} est une condition nécessaire pour que la machine imprime s_3).

Pour démontrer l'équivalence du problème de mots dans S_{mo} avec le problème insoluble connu à propos des machines, on doit montrer qu'aussi inversement $\varphi_1(C) \to \varphi_2(C)$ dans $S_{mo} \Longrightarrow \mathcal{O}(C)$ imprime s_3 (ou ce qui revient au même, $s_4 \ \ell_o \ s_4$ est une C.C. descendante de C dans $\mathcal{O}$).

Cette partie est beaucoup plus pénible. TURING démontre pour cela non moins de 16 lemmes. L'idée est, brièvement, celle d'une induction suivant la longueur des chaînes de mots, c'est-à-dire, la longueur des démonstrations des relations entre les divers couples de mots de S_{mo}. Pour qu'on puisse parler d'une longueur bien définie, il est nécessaire de fixer exactement les divers types des conclusions qu'on veut compter comme un pas élémentaire à partir des axiomes (généraux et relations définissantes), ce qu'on peut faire assez arbitrairement. TURING énumère ainsi trois groupes :

I_1 : $A = A$ (reflexivité générale) ;

$A = B \Rightarrow B = A$ (symétrie) ;

$A = B \ , \ B = C \Rightarrow A = C$.

I_2 : $A = B \Rightarrow Ag = Ag$ pour chaque générateur g

$A = B \Rightarrow gA = gB$ pour chaque générateur g .

II : $A_i = B_i$ (relations définissantes).

III : $Ag = Bg \Rightarrow A = B$; $gA = gB \Rightarrow A = B$ pour chaque générateur g .

La longueur de la démonstration de $A = B$, notée A/B, est un polynôme $ax^2 + bx + c + 2d$ où a est le nombre d'applications de III, b celui de II, c de I_1 et d de I_2. Ces polynômes sont bien ordonnés de la manière usuelle et on peut, en particulier, considérer les démonstrations les plus courtes (toutes d'une même longueur) et ainsi donner à A/B un sens univoque. Le lemme 19, par exemple dit : les chaînes les plus courtes entre mots normaux n'emploient que des mots normaux et les axiomes I et II ($A/B < x^2$) .