ANNALES DE L'I. H. P., SECTION B

JACQUES-EDOUARD DIES

Information et complexité

Annales de l'I. H. P., section B, tome 14, nº 1 (1978), p. 113-118

<http://www.numdam.org/item?id=AIHPB_1978__14_1_113_0>

Ann. Inst. Henri Poincaré, Section B :
Vol. XIV, n° 1, 1978, p. 113-118. *Calcul des Probabilités et Statistique.*

Information et complexité

par

Jacques-Edouard DIES
29, rue de l'Église,
Castelginest, 31140 Aucamville

RÉSUMÉ. — Nous complétons certains résultats de notre précédent article « Information et Complexité » [*2*]. La famille des décodeurs n'étant pas, comme nous l'a indiqué C. P. Schnorr, effectivement énumérable, l'identification des mesures de complexité et des mesures hartleyennes de l'information conduit à une théorie proche de celle de Willis. Nous montrons qu'une telle identification est complète pour les machines de Chaitin à condition d'introduire une famille de pseudomesures semicalculables caractérisant dans un certain sens lesdites machines. Enfin nous donnons une démonstration simplifiée de la caractérisation des suites aléatoires à l'aide de la complexité de Chaitin, résultat que nous étendons à d'autres mesures de complexité et dont nous donnons une application.

ABSTRACT. — Some results of our paper « Information et Complexité » [*2*] are completed. The family of the decoders not being effectively enumerable, as C. P. Schnorr has indicated to us, the identification of the complexity measures and the hartleyan measures of information leads to a theory near to Willis's one. We prove that such an identification is complete for the Chaitin machines if we introduce a family of semicomputable measures characterizing in some sense the afore said machines. Last we give a simplified proof of the characterization of random sequences by means of the Chaitin complexity, this result can be extended to other complexity measures and we show an application of it.

1. Nous conservons les notations et la numérotation des résultats de [*2*] ; dans cet article, certaines opérations n'étant pas effectives, l'énoncé

de certains résultats doit être complété, la démonstration n'étant pas modifiée.

Nous avons ainsi

THÉORÈME 2.3. — $\forall \mu_0 \in M_0$ tel que $\{ x : \mu_0(xX^\infty) = 0 \}$ soit récursivement décidable, $\exists \mu_- \in M_-$: $\mu_0 \sim \mu_-$.

THÉORÈME DE TOTALISATION. — Pour tout $f \in D_0^2$ tel que pour tout $n \in N$ $\Delta f(., n)$ soit récursivement décidable, on peut effectivement construire $\bar{f} \in D$ tel que $K_{\bar{f}}(x) = K_f(x \mid |x|)$.

Par contre D n'est pas effectivement énumérable; en conséquence, contrairement au théorème 3.1, D ne possède pas de décodeur optimal. Il n'est donc pas possible de développer pour D les résultats des §§ 3.3, 3.4 et 3.5. En fait, le théorème de totalisation précédent permet de développer pour D une théorie voisine de celle des machines de Willis [9].

Toutefois, les résultats des §§ 3.3, 3.4 et 3.5 sont valables pour D_0 et D_0^2.

2. Rappelons certains résultats de Zvonkin et Levin [3] : $\mathcal{M}$ est l'ensemble des *mesures semicalculables* définies par

$$\mu \in \mathcal{M} \Leftrightarrow \begin{cases} \mu \text{ énumérable inférieurement,} \\ \mu(\Lambda) \leqslant 1, \ \mu(x0) + \mu(x1) \leqslant \mu(x). \end{cases}$$

On peut, dans un certain sens, caractériser $\mathcal{M}$ par la famille des fonctions

$$\lambda_\varphi(x) = \lambda \{ \bigcup_p pX^\infty : \varphi(p) = x \}.$$

où φ est un processus algorithmique.

En outre, il existe R, mesure semicalculable universelle, telle que, KR(x) désignant la complexité de Loveland,

$$| KR(x) - J_R(x) | \precsim 2 \log KR(x).$$

Introduisons les deux familles $\mathcal{M}_1^*$ et $\mathcal{M}_2^*$ définies par :

$$\mu \in \mathcal{M}_1^* \Leftrightarrow \begin{cases} \mu \text{ énumérable inférieurement,} \\ \sum_{x \in X^*} \mu(x) \leqslant 1. \end{cases}$$

$$\mu \in \mathcal{M}_2^* \Leftrightarrow \begin{cases} \mu \text{ énumérable inférieurement,} \\ \forall n \in N, \quad \sum_{x \in X^n} \mu(x) \leqslant 1. \end{cases}$$

Il est clair que $\mathcal{M}_1^* \sim \mathcal{N} \subset \mathcal{M} \subset \mathcal{M}_2^*$;

Notons que l'extension de $\mathscr{M}$ à $\mathscr{M}_2^*$ n'est pas artificielle; comme l'a montré Gacs [8], la complexité monotone K$m(x)$ (voir paragraphe suivant) ne peut pas être équivalente à $J_R(x)$ donc $Km(x) = J_S(x)$ avec $S \in \mathscr{M}_2^* \setminus \mathscr{M}$.

Les théorèmes 3.4, 3.5, 3.6, 3.7 et 3.8 se conservent en remplaçant M_+ par $\mathscr{M}_2^*$ (resp. $\mathscr{M}_1^*$), D par D_0^2 (resp. D_0) et $K(x)$ par $K_0(x \mid |x|)$ (resp. $K_0(x)$).

Nous formulerons l'équivalent des théorèmes 3.2 et 3.3 pour $\mathscr{M}_2^*$ et D_0^2 mais la démonstration doit être modifiée.

THÉORÈME 3.2. — Si $f \in D_0^2$,

$$\lambda_f(x) = \lambda\left\{\bigcup_p pX^\infty : f(p, |x|) = x\right\} \in \mathscr{M}_2^* .$$

Démonstration. — Appliquant le lemme de Chaitin-Kraft au code instantané $\Delta f(., n)$ nous avons

$$\sum_{x \in X^n} \lambda_f(x) \leqslant \sum_{p \in \Delta f(.,n)} 2^{-|p|} \leqslant 1 .$$

Soit $f(p; n, \tau)$ l'algorithme simulant le travail de la « machine concrète » [*1*, p. 330], le nombre d'opérations élémentaires étant inférieur à τ.

Posons $\bar{f}(i, x, \tau) = \partial\{p \in X^i : f(p, |x|, \tau) = x\}$ et

$$\bar{f}(i, x) = \partial\{p \in X^i : f(p, |x|) = x\} .$$

Alors $\bar{f}(i, x, \tau)$ est une fonction récursive générale, croissant en τ et $\bar{f}(i, x) = \lim_{\tau \to \infty} \bar{f}(i, x, \tau)$.

En outre, $\lambda_f(x) = \sum_{i \in N} \bar{f}(i, x) . 2^{-i}$.

Donc,

$$[\lambda_f(x) > 2^{-n}] \Leftrightarrow \exists t \ \exists \tau \left[\sum_{0 \leqslant i \leqslant t} \bar{f}(i, x, \tau) . 2^{-i} > 2^{-n}\right]$$

Donc λ_f est énumérable inférieurement.

Par conséquent $\lambda_f \in \mathscr{M}_2^*$. □

THÉORÈME 3.3.

$$\forall \mu \in \mathscr{M}_2^* \qquad \exists f \in D_0^2 : \mu \sim \lambda_f .$$

Démonstration. — Soit $\mu \in \mathscr{M}_2^*$; d'après le théorème 3.4, il existe $g \in D_0^2$ tel que

(1) $$K_g(x \mid |x|) \asymp J_\mu(x) .$$

Soit $U_m = \{ (x, n) \in X^m \times N : n \geqslant K_g(x \mid |x|) + 1 \}$ $(U_m)_{m \in N}$ est consistant car $\lambda_g(x) \geqslant 2^{-K_g(x \mid |x|)}$. En appliquant le lemme de Chaitin-Kraft, il existe $f \in D_0^2$ tel que $\partial \{ p \in X^i : f(p, |x|) = x \} = \begin{cases} 1 \text{ si } n \geqslant K_g(x \mid |x|) + 1 \\ 0 \text{ autrement.} \end{cases}$

Donc

$$2^{-K_f(x \mid |x|)} \leqslant \lambda_f(x) \leqslant 2^{-K_f(x \mid |x|)+1}$$

Mais

$$K_f(x \mid |x|) \asymp K_g(x \mid |x|)$$

D'où

(2) $$K_g(x \mid |x|) \asymp J_{\lambda_f}(x).$$

(1) et (2) impliquent $\mu \sim \lambda_f$. □

3. Nous allons donner maintenant une démonstration plus rapide du théorème 4.1 que nous allons étendre à d'autres mesures de complexité puis nous indiquerons l'une des nombreuses conséquences de ce théorème.

μ étant une mesure de probabilité calculable, Levin [4] et Schnorr [7] ont caractérisé X_μ^∞ à l'aide de la complexité monotone $Km(x)$. Rappelons ce résultat [8, § 4] :

$f \in F(X^* \times N, X^*)$ est dite *monotone* si

1. $\forall (x, n) \in \Delta f : |f(x, n)| = n$
2. $\forall (x, n), (xy, n + k) \in \Delta f : f(x, n) \sqsubset f(xy, n + k)$.

Alors $Km_f(x)$ est la complexité monotone de x par rapport à f et $Km(x)$ est la complexité monotone de x par rapport à une fonction monotone universelle.

THÉORÈME 4.0. — Pour toute mesure de probabilité calculable μ,

$$\omega \in X_\mu^\infty \Leftrightarrow Km(\omega) \succcurlyeq J_\mu(\omega).$$

Donnons maintenant une démonstration simplifiée que nous a suggéré C. P. Schnorr, du

THÉORÈME 4.1. — Pour toute mesure de probabilité calculable μ,

$$\omega \in X_\mu^\infty \Leftrightarrow K_0(\omega) \succcurlyeq J_\mu(\omega).$$

Démonstration. — [⇒] Pour toute $f \in D_0$, on peut construire une fonction monotone $\tilde{f}$ telle que $Km_{\tilde{f}}(x) \leqslant K_f(x)$.

Il suffit de définir $\tilde{f}$ par :

$$\tilde{f}(x, n) = f(x) \quad \text{si} \quad x \in \Delta f \quad \text{et} \quad |f(x)| = n.$$

Donc $Km(x) \preccurlyeq K_0(x)$; il suffit alors d'appliquer le théorème 4.0.

[$\Leftarrow$]

Soit $Y \subset N \times X^*$ un test de Martin-Löf; on peut supposer que Y_i est un code instantané [6, lemme 2.7].

Pour tout code instantané $A \subset X^*$ nous avons

$$\mu(AX^\infty) = \sum_{x \in A} \mu(x).$$

Comme $\mu(Y_i X^\infty) \leqslant 2^{-i}$, nous avons

$$\sum_i i \sum_{x \in Y_i} \mu(x) \leqslant \sum_i i.2^{-i} \leqslant 2^k, \qquad \text{pour un } k \in N.$$

Posons

$$T_i = \{ (x, n) \in X^* \times N : x \in Y_i \text{ et } n > J_\mu(x) - \ulcorner \log i \urcorner + k \}$$

et

$$T = \bigcup_i T_i.$$

T est récursivement énumérable et consistant; en appliquant le lemme de Chaitin-Kraft il vient

$$K_0(x) \leqslant J_\mu(x) - \ulcorner \log i \urcorner + k + 1 \qquad (x \in Y_i)$$

Mais

$$\omega \in o(Y) \Rightarrow \forall i \ \exists n : \omega^n \in Y_i$$

Donc

$$\forall i \ \exists n : \ K_0(\omega^n) \leqslant J_\mu(\omega^n) - \ulcorner \log i \urcorner + k + 1 . \qquad \square$$

Levin [5] a introduit et étudié la complexité-préfixe $KP(x)$ et Schnorr [7] la complexité des processus $K_P(x)$.

Nous avons la

PROPOSITION 4.3.

$$Km(x) \precsim J_R(x) \precsim K_P(x) \precsim K_0(x) \asymp KP(x).$$

On déduit de cette proposition et des théorèmes 4.0 et 4.1 que l'on peut caractériser X_μ^∞ à l'aide de $J_R(x)$, $K_P(x)$ et $KP(x)$.

Indiquons pour terminer une des nombreuses applications du théorème 4.1; $\omega \in X^\infty$ sera dite *récursivement énumérable* si $\{ i : \omega_i = 1 \}$ est un ensemble récursivement énumérable; une telle suite est, dans un certain sens, « assez régulière ». Soit $\mathscr{I}$ l'ensemble des réels calculables de [0, 1] et $\theta \in \mathscr{I}$ Θ désigne la mesure de Bernoulli de paramètre θ; autrement dit, si $x \in X^n$ et $s_n = x_1 + x_2 + \ldots + x_n$,

$$\Theta(x) = \theta^{s_n}(1 - \theta)^{n - s_n}.$$

Nous avons alors le

THÉORÈME 4.4. — Si $\omega \in X^\infty$ est récursivement énumérable, alors

$$\omega \notin \bigcup_{\theta \in \mathcal{I}} X_\Theta^\infty .$$

Démonstration. — Pour toute $\omega \in X^\infty$ récursivement énumérable, Barzdin' [3] a démontré que $KR(\omega^n) \preccurlyeq \log n$.

D'autre part, un théorème de Levin [3] indique que

$$| KR(x) - J_R(x) | \preccurlyeq 2 \log KR(x) .$$

Il existe donc C_1 et C_2 telles que

$$R(\omega^n) \geqslant \{ C_1 n [\log (C_2 n)]^2 \}^{-1}$$

D'autre part, si $\theta \geqslant 1 - \theta$, $\Theta(\omega^n) \leqslant \theta^n$.

Par conséquent,

$$\overline{\lim_n} \frac{R(\omega^n)}{\Theta(\omega^n)} \geqslant \overline{\lim_n} \frac{1}{C_1 n [\log (C_2 n)]^2 \theta^n} = \infty$$

Donc, d'après le théorème 4.1 et la proposition 4.3,

$$\omega \notin X_\Theta^\infty . \quad \square$$

BIBLIOGRAPHIE

[1] CHAITIN, A theory of program size formally identical to information theory, *J. A. C. M.*, t. **22**, 1975.

[2] DIES, Information et complexité, *Ann. Inst. Henri Poincaré*, t. XII-**4**, 1976, p. 365-390.

[3] LEVIN-ZVONKIN, La complexité des objets finis..., *Russ. Math. Survs.*, t. **156**, 1970.

[4] LEVIN, On the notion of random sequences, *Soviet Math. Dokl.*, t. **15**, 1973.

[5] LEVIN, Various measures of complexity for finite objects (axiomatic description), *Soviet Math. Dokl.*, t. **17**, 1976.

[6] SCHNORR, A unified approach to the definition of random sequences, *Math. System Theory*, t. **5**, 1971.

[7] SCHNORR, Process complexity and effective random tests, *J. C. S. S.*, t. **7**, 1973.

[8] SCHNORR, A survey of the theory of random sequences, *in* Proceedings of the 5 International Congress of Logic, *Methodology and Philosophy of Sciences*, 1975.

[9] WILLIS, Computational complexity and probability constructions, *J. A. C. M.*, t. **17**, 1970, p. 241-259.

(Manuscrit reçu le 5 octobre 1977).