C. R. Acad. Sci. Paris, t. 328, Série I, p. 3-8, 1999
Logique/*Logic*

# Stockage diophantien et hypothèse abc généralisée

**Gunther CORNELISSEN**

Max-Plank-Institut für Mathematik, Gottfried-Claren-Strasse 26, 532d25 Bonn, Allemagne (actuel)
Département de mathématiques pures, Université de Gand, Galglaan 2, 9000 Gand, Belgique
Courriel : gc@cage.rug.ac.be

(Reçu le 6 juillet 1998, accepté après révision le 4 novembre 1998)

**Résumé.** Soit $(M, L, \phi)$ un triple consistant d'un langage du premier ordre $L$ et un ensemble $M$ qui admet une interprétation $\phi$ de $L$. Pour un deuxième tel triple $(M', L', \phi')$, on définit la notion « $(M', L', \phi')$ est positif existentiel dans $(M, L, \phi)$ », qui généralise la notion d'ensemble positif existentiel. Si le produit cartésien $(M \times M, L, \phi \times \phi)$ est positif existentiel dans $(M, L, \phi)$, nous disons qu'il admet stockage positif existentiel. Ceci généralise la notion de fonction de stockage, connue de la théorie de la récursivité. On démontre que $\mathbf{Z}$ et certains corps de fonctions admettent stockage positif existentiel. © Académie des Sciences/Elsevier, Paris

### *Diophantine storing and the generalized abc-hypothesis*

**Abstract.** *Let $(M, L, \phi)$ be a triple consisting of a first order language $L$ and a set $M$ that admits an interpretation $\phi$ of $L$. We define what it means for a second such triple $(M', L', \phi')$ to be positive existential in $(M, L, \phi)$, which generalizes the notion of positive existential set. If the cartesian product $(M \times M, L, \phi \times \phi)$ is positive existential in $(M, L, \phi)$, we say it admits positive existential storing. This generalizes the notion of a storing function, known from recursion theory. We then prove that $\mathbf{Z}$ and certain function fields admit positive existential storing.* © Académie des Sciences/Elsevier, Paris

## *Abridged English Version*

DEFINITIONS 1. – Let $(M, L, \phi)$ be a triple consisting of a first order language $L$ given by $i$-ary predicates $\{P_{i,\alpha}\}$, a set $M$ and an interpretation $\phi$ of $L$ in $M$. We say that another such triple $(M', L' = \{P'_{i,\alpha}\}, \phi')$ is *positive existential* (respectively *diophantine*) in $(M, L, \phi)$ if there is a set-theoretic bijection between $M'$ and a subset of $M$, such that the image is positive existential (respectively diophantine), and such that the induced inclusions $\phi'(P'_{i,\alpha}) \subseteq M^i$ are also positive existential (diophantine). If, for every pair of formulas $p, q$ in $L$, the interpretation of the formula $p \wedge q$ $(p \vee q)$ is equivalent to a diophantine formula, we say that the triple admits $\wedge$ $(\vee)$.

**Note présentée par Jacques TITS.**

FIRST PROPERTIES 2. – *If $(M'', L'') \subseteq (M', L') \subseteq (M, L)$ is a chain of positive existential inclusions in the above sense (respectively diophantine inclusions and such that $(M, L)$ admits $\wedge$), then the inclusion $(M'', L'') \subseteq (M, L)$ is positive existential (respectively diophantine). If furthermore, the positive existential (diophantine) theory of $(M', L')$ is undecidable, the same holds for $(M, L)$.*

*Example* 3. – $(\mathbf{Z}, (0, 1, +, \cdot, =))$ is diophantine in $(k(t), (0, 1, t, +, \cdot, =))$, where $k$ is a formally real or finite field (*see* [2], [3] et [7]).

DEFINITIONS 4. – Let $(M, L, \phi)$ be a triple. The language $L$ admits a natural interpretation $\phi^2$ in the cartesian product $M^2$. We say that $(M, L, \phi)$ admits *positive existential (diophantine) storing* if $(M^2, L, \phi^2)$ is diophantine in $(M, L, \phi)$. If the defining injection $M^2 \subseteq M$ is surjective, we call the storing *surjective* too.

CONSTRUCTION PRINCIPLE 5. – *Let $R$ be a ring and $L = (c^{(i)}, +, \times, =)$ a language that can be interpreted in $R$ in the natural way (where $c^{(i)}$ are constants), which admits $\wedge$ and $\vee$. Suppose that there exist:* (a) *a disjoint finite cover $\{U_i\}_{i=0}^n$ of $R^2$, and* (b) *polynomial injections $U_i \to R$ such that the images are disjoint and diophantine in $(R, L)$. Then $(R, L)$ admits diophantine storing.*

If the above principle applies, we say that $(R, L)$ admits storing by $n$ functions. It is known that $\mathbf{Z}$ admits storing by one function, but not whether one can choose it to be surjective, nor whether $\mathbf{Q}$ admits storing by one function at all. One can use the above construction principle to paste together Cantor functions and prove the following:

PROPOSITION 6. – $(\mathbf{Z}, (0, 1, +, \cdot, =))$ *admits surjective storing by* 4 *functions.*

PROPOSITION 7. – *Let $K$ be the function field of a smooth projective curve of genus $g$, irreducible over a field $k$. Let $t \in K - k$ be a non-constant function such that $K/k(t)$ is separable, and let $N_t$ be the number of inequivalent $K$-valuations such that $v(t) \neq 0$. If $\mathrm{char}(k) = 0$, assume that there exists an odd number $m > 64 \cdot (N_t + \max\{5, 2g + 3\})$ such that $K$ only contains the trivial $m$-th root of unity, and such that $t$ is not an $m$-th power. Then $(K, (0, 1, t, +, \cdot, =))$ admits storing by one function.*

The function is of the form $(x, y) \mapsto x^m + ty^m$, and the proof uses Mason's generalized abc-hypothesis for $K$.

---

DÉFINITIONS 1. – Soit $(M, L, \phi)$ un triple consistant d'un langage du premier ordre $L$, spécifié par des prédicats (constantes, relations) $\{P_{i,\alpha}\}$ $i$-aires, un ensemble $M$ et une interprétation $\phi$ de $L$ dans $M$ (*cf.* [5]). Tous les caractères romains, indexés par des nombres naturels, sont admis comme variables s'ils ne figurent pas dans les prédicats. Souvent, nous omettrons $\phi$ de la notation. Nous considérons l'interprétation $\phi(P_{i,\alpha})$ d'un prédicat comme sous-ensemble de $M^i$. Une formule de $L$ est appelée *positive existentielle* si elle est de la forme $(\exists x)a$ où $x$ est une liste de variables et $a$ est une formule sans négations et quantificateurs. Une telle formule est dite *diophantienne* si $a$ est atomique. Un sous-ensemble $S \subseteq M^r$ $(r \in \mathbf{Z}_{>0})$ est dit *positif existentiel* (respectivement *diophantien*) *$\phi$-définissable* s'il y a une formule positive existentielle (respectivement diophantienne) dans $L$ qui décide l'appartenance à $S$ (en termes de $\phi$-vérité).

Nous disons d'un autre tel triple $(M', L' = \{P'_{i,\alpha}\}, \phi')$ qu'*il est positif existentiel* (respectivement *diophantien*) *dans* $(M, L, \phi)$ s'il y a une injection d'ensembles $M' \subseteq M$, tel que l'image est positive existentielle (respectivement diophantienne) $\phi$-définissable, et les inclusions induites $\phi'(P'_{i,\alpha}) \subseteq M^i$ sont, elles aussi, positives existentielles (respectivement diophantiennes) $\phi$-définissables. Nous écrivons $(M', L') \subseteq_{\mathrm{pe}} (M, L)$ (respectivement $(M', L') \subseteq_{\mathrm{d}} (M, L)$). Pour nous, $M' \subseteq M$ signifie qu'il y a une bijection entre $M'$ et un sous-ensemble de $M$.

Si, pour chaque paire de formules atomaires $p, q$ dans $L$, l'interprétation de la formule $p \wedge q$ (respectivement $p \vee q$) équivaut (en termes de $\phi$-vérité) à une formule diophantienne, nous disons que le triple *admet* $\wedge$ (respectivement $\vee$).

*Exemples* 2. – Un sous-ensemble $S$ positif existentiel $\phi$-définissable est positif existentiel dans $(M, L, \phi)$ si on le considère comme triple $(S, L, \phi_S)$, où $\phi_S$ est la restriction de $\phi$ à $S$ (c'est-à-dire, $\phi_S(\exists x) = (\exists x \in S)$ opposé à $\phi(\exists x) = (\exists x \in M)$).

*Démonstration.* – Soit $(\exists y \in M) P_S(x, y)$ la formule positive existentielle qui équivaut à « $x \in S$ » (où $y = (y_1, ..., y_m)$ est une liste de variables). Soit $P$ un prédicat de $L$. Alors $(x_1, ..., x_n) \in \phi_S(P_i)$ équivaut à

$$(\exists y^{(j)}) \bigwedge_j P_S(x_j, y^{(j)}) \wedge P_i(x_1, ..., x_i),$$

formule positive existentielle. □

Soit $R$ un anneau commutatif avec unité. De façon naturelle, il admet une interprétation pour chaque langage $L$ donné par des prédicats $(c_1^{(i)}, +_3, \cdot_3, =_2)$, dont les indices indiquent le degré, et $c_1^{(i)}$ sont des constantes arbitraires (moins en nombre que $|R|$). Des exemples typiques sont les nombres $(\mathbf{Z}, (0, 1, +, \cdot, =))$ et les polynômes $(\mathbf{R}[t], (0, 1, t, +, \cdot, =))$. Si $R$ n'a pas de diviseurs de zéro et il y a un polynôme $f$ dont les coefficients sont interprétables pour $L$ (c'est-à-dire, dans $\phi(L)$), et qui n'a pas de zéro dans le corps des fractions de $R$, alors $R$ admet $\vee$ et $\wedge$.

*Démonstration.* – Si $p$ et $q$ sont des polynômes, alors $R \models (p = 0 \vee q = 0) \iff (pq = 0)$, et $R \models (p = 0 \wedge q = 0) \iff q^{\deg(f)} f(p/q) = 0$. □

PREMIÈRES PROPRIÉTÉES 3. – *Si* $(M'', L'') \subseteq_{\mathrm{pe,d}} (M', L') \subseteq_{\mathrm{pe,d}} (M, L)$ *est une chaîne d'inclusions positives existentielles (respectivement diophantiennes et telle que* $(M, L)$ *admet* $\wedge$*), alors l'inclusion* $(M'', L'') \subseteq_{\mathrm{pe,d}} (M, L)$ *est positive existentielle (respectivement diophantienne). Si, en outre, la théorie positive existentielle (respestivement diophantienne) de* $(M', L')$ *est indécidable, il en est de même pour* $(M, L)$.

La *théorie* (positive existentielle, diophantienne) de $(M, L)$ consiste en des formules (positives existentielles, diophantiennes) de $L$ qui sont vraies dans le modèle $M$. Les démonstrations sont faciles.

Remarquons que ces notions et propriétés permettent de définir des catégories dont les objets sont les triples (respectivement les triples admettant $\wedge$), et les morphismes sont donnés par $\subseteq_{\mathrm{pe}}$ (respectivement $\subseteq_{\mathrm{d}}$). Alors la machinerie homologique est applicable.

*Exemples.* – 4. – Les résultats concernant le dixième problème de Hilbert obtenus par Denef [2], [3] et Pheidas [7] se traduisent de la façon suivante dans notre terminologie : $(\mathbf{Z}, (0, 1, +, \cdot, =))$ est positif existentiel dans les anneaux de polynômes $(R[t], (0, 1, t, +, \cdot, =))$, où $R$ est anneau commutatif unitaire sans diviseurs de zéro, et dans les corps de fonctions $(k(t), (0, 1, t, +, \cdot, =))$ tel que $k$ est formellement réel ou fini. Notons : nos définitions permettent de donner un sens précis à des questions comme « $(\mathbf{F}_q(t), (0, 1, t, +, \times, =))$ est-il diophantien dans $(\mathbf{Q}, (0, 1, +, \times, =))$ ? ».

DÉFINITION 5. – Soit $(M, L, \phi)$ un triple. Notons que le langage $L$ admet aussi une interprétation naturelle $\phi^2$ dans le produit cartésien $M^2$ de façon « diagonale » (c'est-à-dire, $\phi^2(P_{i,\alpha}) = \phi(P_{i,\alpha}) \times \phi(P_{i,\alpha}) \subseteq M^{2i}$). Nous disons que $(M, L)$ admet *stockage positif existentiel* (respectivement *diophantien*) si $(M^2, L, \phi^2)$ est positif existentiel (respectivement diophantien) dans $(M, L, \phi)$.

Notons que si $f : M^2 \hookrightarrow M$ est l'injection positive existentielle définissante, il ne faut point que $f(\phi^2(P_{i,\alpha})) = \phi(P_{i,\alpha})$. Si en outre, $f$ est bijectif, nous disons que $(M, L)$ admet stockage positif existentiel *surjectif*.

PRINCIPE DE CONSTRUCTION 6. – *Soient $R$ un anneau et $L$ un langage qui s'interprète dans $R$ comme dans §2, et tel que $(R, L)$ admet $\wedge$ et $\vee$. Supposons que les objets suivants existent :* (a) *un recouvrement disjoint fini $\{U_i\}_{i=0}^{n}$ de $R^2$, et* (b) *des injections polynomiales $f_i : U_i \to R$ dont les images sont disjointes et diophantiennes dans $(R, L)$. Alors $(R, L)$ admet stockage diophantien.*

*Démonstration.* – Soit $f : R^2 \hookrightarrow R$ l'injection définie par

$$f(x) = y \iff x \in U_i \wedge f_i(x) = y,$$

alors $\mathrm{im}(\phi)$ est diophantien dans $(R, L)$, comme ceci admet $\vee$. Définissons une interpretation $\phi_f$ de $L$ dans $\mathrm{im}(f)$. Soit $P$ un prédicat de degré $i$ dans $L$, alors

$$(y_1, \ldots, y_i) \in \phi_f(P) \iff \exists (x_{11}, x_{12}, \ldots, x_{i1}, x_{i2}) \in R^{2i} : \bigwedge_{j=1}^{i} y_j = f(x_{j1}, x_{j2})$$
$$\wedge\, ((x_{11}, x_{12}), \ldots, (x_{i1}, x_{i2})) \in \phi^2(P).$$

Comme $f$ est donné par des polynômes et $R$ admet $\wedge$, $(\mathrm{im}(f), L, \phi_f) \subseteq_{\mathrm{d}} (R, L, \phi)$. En outre, il y a une bijection d'ensembles $(\mathrm{im}(f), L, \phi_f) = (R^2, L, \phi^2)$. □

Si ce principe est applicable, nous disons que $(R, L)$ *admet stockage par $n$ fonctions*. Si on peut prendre $n = 1$, $R$ admet une fonction de stockage, propriété connue de la théorie de la récursivité. Lew et Rosenberg [4] démontrent, entre autre, la non-existence de fonctions de stockage quadratiques pour $\mathbf{Z}$ (c'est-à-dire telles que $n = 1$ et $\deg(f_1) = 2$).

Bjorn Poonen (communication privée) a remarqué l'existence d'une fonction de stockage pour $\mathbf{Z}$ de la façon suivante : soit $C_{>0} : \mathbf{Z}_{>0}^2 \to \mathbf{Z}_{>0}$ la fonction de Cantor (*cf.* [5]), et soit $f : \mathbf{Z} \hookrightarrow \mathbf{Z}_{>0}$ une injection polynomiale (disons $f(x) = 2x^2 + x + 1$), alors la composition $(x, y) \mapsto C_{>0}(f(x), f(y))$ est une fonction de stockage pour $\mathbf{Z}$. Il serait possible de généraliser ce résultat aux ordres dans les corps de nombres quelconques en utilisant le théorème de Roth.

L'existence d'une telle fonction de stockage *surjective* pour $\mathbf{Z}$ n'est pas établie. De même pour le corps $\mathbf{Q}$ des nombres rationnels. Les deux propositions suivantes peuvent être considérées comme des résultats partiels ultérieurs concernant ces questions.

PROPOSITION 7. – $(\mathbf{Z}, (0, 1, +, \cdot, =))$ *admet stockage surjectif par 4 fonctions.*

*Démonstration.* – Soient $C_{>0} : \mathbf{Z}_{>0}^2 \to \mathbf{Z}_{>0}$ et $C_{\geq 0} : \mathbf{Z}_{\geq 0}^2 \to \mathbf{Z}_{\geq 0}$ respectivement les fonctions de Cantor de $\mathbf{Z}_{>0}$ et $\mathbf{Z}_{\geq 0}$ (*voir* [5]), qui sont des bijections polynomiales. Considérons le recouvrement polynomial surjectif $\mathbf{Z}^2 \to \mathbf{Z}$ donné par :

$$\begin{cases} (x, y) \mapsto 2C_{\geq 0}(x, y) & \text{si } (x, y) \in U_1 := \{x \geq 0 \wedge y \geq 0\}, \\ (x, y) \mapsto -2C_{\geq 0}(-x, -y) & \text{si } (x, y) \in U_2 := \{x \leq 0 \wedge y \leq 0\} - \{(0, 0)\}, \\ (x, y) \mapsto 2C_{>0}(-x, y) - 1 & \text{si } (x, y) \in U_3 := \{x < 0 \wedge y > 0\}, \\ (x, y) \mapsto -2C_{>0}(x, -y) + 1 & \text{si } (x, y) \in U_4 := \{x > 0 \wedge y < 0\}. \end{cases}$$

Les images des différents $\{U_i\}_{i=1}^{4}$ sont $2\mathbf{Z}_{\geq 0}$, $-2\mathbf{Z}_{>0}$, $2\mathbf{Z}_{\geq 0} + 1$ et $-2\mathbf{Z}_{>0} + 1$, donc diophantiennes dans $\mathbf{Z}$ (comme $\mathbf{Z}_{\geq 0}$ l'est par le théorème des quatres carrés de Lagrange, et comme $x \neq 0 \iff (x \geq 0) \wedge (-x \geq 0)$). Alors le principe du §6 est applicable. □

PROPOSITION 8. – *Soit $K$ le corps des fonctions d'une courbe propre lisse de genre $g$, irréductible sur un corps $k$. Soit $t \in K - k$ une fonction non constante telle que $K/k(t)$ soit séparable, et soit $N_t$ le nombre des valuations $v$ inéquivalente de $K$ telle que $v(t) \neq 0$. Si* $\mathrm{car}(k) = 0$, *supposons en outre qu'il existe un nombre naturel impair $m > 64 \cdot (N_t + \max\{5, 2g + 3\})$ tel que $K$ ne contient*

*que la racine triviale d'unité d'ordre $m$, et tel que $t$ n'est pas $m$-puissance. Alors $(K, (0, 1, t, +, \cdot, =))$ admet une fonction de stockage.*

*Démonstration.* – Si $\mathrm{car}(k) = p > 0$, choisissons $m = p$. Sinon, soit $m$ comme ci-dessus. Il suffit de démontrer que la fonction $f : (x, y) \mapsto x^m + ty^m$ est injective, donc que les seules solutions de l'équation $A_1 + A_2 + A_3 + A_4 = 0$, où

$$A_1 = x_1^m,\ A_2 = tx_3^m,\ A_3 = -x_2^m,\ A_4 = -tx_4^m,$$

satisfont à $A_1 + A_3 = 0$. Si $\mathrm{car}(k) = p$, alors la dérivée par rapport à $t$ est une dérivation globale sur $K$ (comme $K/k(t)$ est séparable), et en l'appliquant à l'équation, le résultat est immédiat.

Supposons donc que $\mathrm{car}(k) = 0$. Paraphrasons un résultat auxiliaire de Mason ([6], Lemme 2) : *soit $n \geq 3$, et $A_1 + \cdots + A_n = 0$ pour $(A_1, \cdots, A_n) \in K^n$. Alors ou bien une sous-somme est zéro (c'est-à-dire $e_1A_1 + \cdots + e_nA_n = 0$, $e_i \in \{0, 1\}$ et $(\exists i)(e_i = 0)$), ou bien l'inégalité suivante vaut :*

$$\sum_v \max\{0, -v(A_1), \ldots, -v(A_n)\} \leq 4^{n-2}(|S| + \max\{0, 2g - 2\}).$$

*Ici, $v$ parcourt les $k$-valuations discrètes normalisées inéquivalentes de $K$, et $S$ est l'ensemble des valuations pour lesquelles les $A_i$ ne sont pas tous des unités.*

Supposons qu'aucune sous-somme de $A_1 + \cdots + A_4$ ne soit égale à zéro. Soit $\infty$ une place de $K$, tel que la valuation $v_\infty$ correspondante satisfait à $v_\infty(t) < 0$. En multipliant $x_1, \ldots, x_4$ avec un élément de l'anneau des fonctions régulières en dehors de $\infty$, nous pouvons supposer que $v(x_i) \geq 0$ pour tout $v \neq v_\infty$. Comme $\sum_v v(x) = 0$ pour tout $x \in K$, on voit que $v_\infty(x_i) \leq 0$. Dans l'inégalité du lemme (appliquée pour $n = 4$ dans notre cas), on peut remplacer la partie inférieure par $-mv_\infty(x_i)$ pour tout $i = 1, \ldots, 4$. On peut aussi estimer

$$|S| \leq N_t + \sum_{i, v(x_i) \neq 0} 1 \leq N_t + \sum_{i, v_\infty(x_i) \neq 0} 1 + \sum_{i, v \neq v_\infty} v(x_i) \leq N_t + 4 - v_\infty(x_1 \cdot x_2 \cdot x_3 \cdot x_4).$$

L'addition des quatres inégalités obtenues donne

$$(m - 4^3)(-v_\infty(x_1 \cdot x_2 \cdot x_3 \cdot x_4)) \leq 4^3 \cdot (N_t + \max\{4, 2g + 2\}),$$

d'où une contradiction.

Si par exemple $A_1 = 0$, on peut appliquer le lemme de Mason (pour $n = 3$) de façon analogue à $A_2 + A_3 + A_4 = 0$ pour obtenir une contradiction. Si $A_1 + A_2 = 0$ ou $A_1 + A_4 = 0$, alors $\pm t$ serait une puissance d'ordre $m$ dans $K$, ce qui est impossible ($m$ est impair). Donc $A_1 + A_3 = 0$, ce qu'il fallait démontrer. □

*Exemples.* 9. – Un $t$ tel que $K/K(t)$ est séparable existe si $k$ est parfait ; si $\mathrm{car}(k) = 0$ ou si $\mathrm{car}(k) = p$ et $K^p \neq K$. La proposition s'applique à tout corps de fonctions réel (c'est-à-dire tel que $k \subseteq \mathbf{R}$), et à tout corps de fonctions sur la clôture séparable d'un corps fini. Est-ce que le résultat reste valable pour les corps de fonctions complexes, ou pour des corps de fonctions munis du langage $(0, 1, +, \cdot, \text{« } \notin k \text{ »})$ ?

*Remarque* 10. – Le lemme de Mason est une sorte d'hypothèse abc généralisée pour les corps de fonctions. L'hypothèse abc généralisée (non démontrée) pour $\mathbf{Q}$ (*cf.* [1]) implique que $\mathbf{Q}$ admet $(x, y) \mapsto x^N + 3y^N$ comme fonction de stockage pour $N$ impair et assez grand. Cette dernière suggestion (même pour $N = 7$) est due à Don Zagier, en réponse à une question de Harvey Friedman.

---

L'auteur est Chargé de Recherches du Fonds de la Recherche Scientifique–Flandres (Belgique) (FWO). Cette Note était accomplie au Max-Planck-Institut für Mathematik.

## Références bibliographiques

[1] Browkin J., Brzeziński J., Some remarks on the *abc*-conjecture, Math. Comp. 62 (1994) 206 931–939.
[2] Denef J., The Diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc. 242 (1978) 391–399.
[3] Denef J., The Diophantine problem for polynomial rings of positive characteristic, Logic Colloquium '78 (Mons, 1978), Stud. Logic Foundations Math., Vol. 97, North-Holland, Amsterdam, 1979, pp. 131–145.
[4] Lew J.S., Rosenberg A.L., Polynomial indexing of integer lattice-points. I. General concepts and quadratic polynomials, II. Nonexistence results for higher-degree polynomials, J. Number Theory 10 (2) (1978) 192–243.
[5] Manin Y.I., A course in mathematical logic, Graduate Texts in Math., Vol. 54, Springer, Berlin–Heidelberg–New York, 1977.
[6] Mason R.C., Norm form equations I, J. Number Theory 22 (2) (1986) 190–207.
[7] Pheidas T., Hilbert's tenth problem for fields of rational functions over finite fields, Invent. Math. 103 (1) (1991) (1) 1–8.