

TD de Logique 11.5 : Arithmétique de Presburger (corrigé)

Exercice 1. Cela se complique un peu par rapport aux théories successeur et ordre.

1. Essentiellement des récurrences. C'est à peine un exercice que d'identifier les énoncés-clefs.

Grâce aux propriétés de divisibilité, on peut sans ajouter de quantificateurs parler de la classe de congruence modulo k (pour chaque entier naturel k).

2. Soit $\mathcal{M}$ un modèle. Alors $\leq$ y définit un ordre total, et l'on voit que $(\mathcal{M}, <) \models T_{\text{ord}}$. Notamment $(\mathcal{M}, <) \simeq \mathbb{N} \sqcup_{<} \bigsqcup_I \mathbb{Z}$, où I est ordonné.

Soit $I_0 = \{0\} \cup I$ l'ensemble des *magnitudes*, où $\mu(a) = 0$ si $a \in \mathbb{N}$ et $\mu(a) = i$ si a est dans la i^{e} copie de $\mathbb{Z}$. On peut munir I_0 d'une structure de semi-groupe abélien ordonné tel que $\mu : \mathcal{M} \rightarrow I$ soit un morphisme. En outre à k fixé, $D_k(x) \vee \dots \vee D_k(x + k - 1)$ impose la k -divisibilité de I_0 . Noter que l'on n'a pas parlé de saturation.

3. Soient $\mathbb{A} \models \mathcal{T}_{\text{Pres}}$ et $\bar{a}, \alpha \in \mathbb{A}$. Comme 1 est dans $\mathcal{L}$ on peut supposer $a_1 = 1$.

Une $\mathcal{L}$ -formule de base $\varphi(\bar{a}, \alpha)$ est une relation additive ; par associativité et commutativité, elle équivaut à $\gamma\alpha + \sum c_i a_i = \delta\alpha + \sum d_i a_i$, où les coefficients sont *naturels*. Par régularité on se ramène à $\gamma\alpha = t(\bar{a})$ (terme à combinaisons $\mathbb{Z}$ -linéaires, grâce à la soustraction définissable).

Une $\hat{\mathcal{L}}$ -formule de base peut également être :

- soit une inégalité ;
- soit une relation de divisibilité $D_k(\gamma\alpha + t(\bar{a}))$.

Si l'on connaît la classe modulo k de chaque a_i , c'est essentiellement une information de type $D_k(\gamma\alpha + \ell)$, d'ailleurs moins fine que $D_k(\alpha + \ell)$.

En conclusion le $\hat{\mathcal{L}}$ -type sans quantificateurs $\text{tp}_0(\alpha/\bar{a})$ porte comme informations :

- des encadrements $t_-(\bar{a}) \leq \gamma\alpha \leq t_+(\bar{a})$ (combinaisons $\mathbb{Z}$ -linéaires) ;
- des congruences $D_k(\gamma\alpha + \ell)$.

4. Va-et-vient entre modèles ω -saturés.

Soient $\mathbb{A}, \mathbb{B}$ des modèles ω -saturés. On montre que les 0-isomorphismes *au sens de $\hat{\mathcal{L}}$* sont des ∞ -isomorphismes. Soient $\bar{a} \simeq_0 \bar{b}$ dans $\hat{\mathcal{L}}$.

Avant l'argument, faisons sentir pourquoi se placer dans $\mathcal{L}$ ne suffirait pas.

- Si a_1, a_2 sont $\mathbb{N}$ -libres avec $a_1 < a_2$ et $b_1 > b_2$, l'ajout de α tel que $a_2 = a_1 + \alpha$ est irreflétable : l'ordre est nécessaire.
- Si a_1 est $\mathbb{N}$ -libre (de magnitude infinie) et pair, mais b_1 $\mathbb{N}$ -libre et impair, l'ajout de α tel que $a_1 = \alpha + \alpha$ est irreflétable : les D_k sont nécessaires.

Mais nous supposons bien $\bar{a} \simeq_0 \bar{b}$ dans $\hat{\mathcal{L}}$. Réflétons l'ajout de α à $\bar{a}$ par un $\beta \in \mathbb{B}$. Soient $p(x) = \text{tp}_0(\alpha/\bar{a})$, et $q(x)$ obtenu en substituant $\bar{b}$ à $\bar{a}$. On veut montrer que q est satisfaisable dans $\mathbb{B}$. Par finitude de $\bar{b}$ et ω -saturation, il suffit de démontrer que q est bien un type de $\mathbb{B}$, i.e. qu'il est finiment satisfaisable.

Un sous-ensemble fini de p porte :

- des encadrements $t_i^-(\bar{a}) \leq m_i \alpha \leq t_i^+(\bar{a})$;

- des congruences $D_{k_i}(n_i\alpha + \ell_i)$, moins fines que $D_{k_i}(\alpha + \ell'_i)$.

Prenant un multiple commun des coefficients m_i (en quantité finie), et ne gardant que les inégalités les plus contraignantes (l'ordre est total), l'information la plus fine possible est une seule conjonction $t^-(\bar{a}) \leq m\alpha \leq t^+(\bar{a})$ et de $D_{k_i}(\alpha + \ell_i)$. Deux cas se présentent.

- Si $t^-(\bar{a})$ et $t^+(\bar{a})$ sont à distance finie (de même magnitude), alors $m\alpha$ est déterminé explicitement en fonction de $\bar{a}$: et le $m\beta$ correspondant convient.
- Si $t^-(\bar{a})$ et $t^+(\bar{a})$ sont à distance infinie, alors $t^-(\bar{b})$ et $t^+(\bar{b})$ aussi, et l'on a une copie de $\mathbb{Z}$ entre eux. Il suffit alors de résoudre un nombre fini de congruences pour β , en fixant $m\beta$ dans cette copie (i.e. en travaillant à magnitude de $m\beta$, et donc de β , fixée).

On a pu refléter α .

5. On conclut par les moyens classiques.

Par élimination des quantificateurs dans $\hat{\mathcal{L}}$, les ensembles infinis d'un modèle $\mathcal{M}$ non-cofinis définissables à paramètres dans l'arithmétique de Presburger sont les ensembles ultimement périodiques, les unions finies d'intervalles et les intersection de ces deux types d'ensemble.

En particulier, dans $(\mathbb{N}, 0, 1, +)$ on ne peut définir que les ensembles ultimement périodiques (en plus des finis/cofinis).

6. On peut invoquer toute la force de la suite et la fameuse « fonction β ». Mais plus modestement, quand le produit est définissable, celui des nombres premiers, ou des carrés, l'est. Or d'après ce qui précède toute partie définissable de $\mathbb{N}$ dans $\{+\}$ est ultimement périodique.