CALCULABILITE DANS LES STRUCTURES ALGEBRIQUES DENOMBRABLES

CALCULABILITE DANS LES STRUCTURES ALGEBRIQUES DENOMBRABLES

Abstract

Computability in Countable algebraic structures

We study the computability in discrete enumerable algebraic structures from the viewpoint of a given class of constructions $\mathfrak{C}$. Our walk is to relativize for the class $\mathfrak{C}$ the methods of constructive mathematics. The most important class we study is $\mathfrak{P}$: the class of polynomial time computable functions.

We introduce the notion of *completely $\mathfrak{C}$-computable algebraic structure* (the $\mathfrak{C}$-computability of evaluation of formulas). We prove that the most elementary algebraic structures are *completely $\mathfrak{P}$-computable in a natural sense*. For example the natural completely $\mathfrak{P}$-computable presentation of the ring of polynomials with integer coefficients is the usual one (dense presentation with integers in binary).

We study the $\mathfrak{P}$-computability of linear algebra. For commutative rings, we give strong links between the three notions:

- $\mathfrak{P}$-computability of determinants
- $\mathfrak{P}$-computability of the product of a list of matrices
- $\mathfrak{P}$-computability of addition, multiplication, exact division, and $\mathfrak{P}$-majoration of determinants (in the case of an integral domain).

(these links are often given for the arithmetic complexity only).

Résumé

Cette étude est consacrée aux ensembles discrets énumérables lorsqu'on adopte le point de vue des constructions d'une classe donnée $\mathfrak{C}$. La classe que nous avons essentiellement en vue est celle des constructions en temps polynomial. La démarche générale que nous suivons est de relativiser à une classe de construction donnée les méthodes de mathématiques constructives.

Dans le A, nous donnons les définitions de base, et quelques résultats élémentaires.

Dans le B, nous nous intéressons aux structures algébriques dénombrables effectives.

Les notions de "calcul algébrique", "calcul algébrique formel" et "calcul de classe $\mathfrak{C}$" interfèrent alors entre elles. Cela nous amène à la notion de "structure algébrique complètement $\mathfrak{C}$-calculable", qui s'avère être une bonne notion. Par définition, une présentation d'une structure algébrique est complètement $\mathfrak{C}$-calculable lorsque l'évaluation des formules est $\mathfrak{C}$-calculable. Nous établissons donc un lien entre la notion introduite et les présentations "par formule" ou "en magma" (§ e).

Nous montrons que les structures algébriques les plus élémentaires sont complètement $\mathfrak{P}$-calculables, et en général "de manière naturelle". Cela implique qu'il y a une $\mathfrak{P}$-présentation naturellement attachée à une structure algébrique élémentaire. Par exemple la $\mathfrak{P}$-présentation naturelle de $(\mathbb{N}, 0, 1, +)$ est la présentation en unaire, tandis que la présentation naturelle de $(\mathbb{N}, 0, 1, +, \times)$ est la présentation en binaire.

De nombreuses structures algébriques "libres de type fini" sont complètement $\mathfrak{P}$-calculables et ont une structure de $\mathfrak{P}$-calculabilité naturelle. Par exemple les algèbres de polynômes (à un nombre fini d'indéterminées) sur $\mathbb{Z}$, $\mathbb{Q}$ ou sur un anneau fini. Un quotient d'une de ces algèbres sera également complètement $\mathfrak{P}$-calculable lorsque l'idéal noyau est une partie $\mathfrak{P}$-détachable de l'algèbre des polynômes.

Il semble très improbable que la clôture algébrique de $\mathbb{Q}$ puisse être présentée de manière complètement $\mathfrak{P}$-calculable; nous donnons néanmoins un exemple (en B.g) d'extension algébrique infinie de $\mathbb{Q}$ présentée de manière que l'addition et le produit y soient complètement $\mathfrak{P}$-calculables.

Dans le C , qui peut être lu à peu près indépendamment du B , l'objectif est de montrer que l'algèbre linéaire "classique" est une algèbre en temps polynomial.

Nous construisons un bon stock d'anneaux commutatifs sur lesquels "le calcul des déterminants est en temps polynomial", à peu de chose près les mêmes que ceux qui ont été montrés complètement $\mathcal{P}$-calculables dans la partie B . Nous mettons en évidence le lien étroit entre la calculabilité des déterminants en temps polynomial d'une part et la calculabilité du produit d'une liste de matrices en temps polynomial d'autre part.

Enfin, nous étudions en détail la méthode du pivot améliorée à la Bareiss et sa calculabilité en temps polynomial.

INTRODUCTION

Les mathématiques "ordinaires" ont un contenu constructif. Telle est du moins la thèse des mathématiques constructives (cf. **[CA]** et **[CAL]** pour une mise en pratique de cette thèse). Cette affirmation peut être interprétée de la manière suivante: tout théorème de mathématiques "ordinaires" , affirmant l'existence de certains objets "concrets" vérifiant certaines propriétés sous certaines hypothèses, doit pouvoir être *réalisé* sous forme d'un algorithme construisant l'objet en question à partir des données fournies dans les hypothèses. En général une preuve constructive d'un théorème fournit de manière immédiate un algorithme primitif récursif qui réalise le théorème en question.

Cette étude (et d'autres dans la même série) se situe dans le contexte général suivant: expliciter, dans les mathématiques ordinaires, les théorèmes qui peuvent être réalisés par des algorithmes de complexité "faible" (en temps polynomial par exemple). Il nous a semblé naturel de prendre une base de mathématiques constructives pour développer ce travail.

Dans cette étude, consacrée aux structures algébriques dénombrables, nous poursuivons les deux objectifs suivants:

- expliciter les interférences entre calcul algébrique et calculabilité au sens de la complexité
- expliciter dans quelle mesure l'algèbre linéaire ordinaire est en temps polynomial.

La démarche générale que nous suivons est de relativiser à une classe de construction donnée les méthodes de mathématiques constructives.

Nous utiliserons les mathématiques constructives de manière informelle[1] (c.-à-d. comme un mathématicien classique utilise la théorie des ensembles).

Disons en très bref que les mathématiques constructives dans le style Bishop n'énoncent que des théorèmes ayant une signification algorithmique. Elles fournissent donc, selon nous, une base naturelle pour tout travail mathématique centré sur la discussion d'algorithmes.

Nous indiquons maintenant deux ou trois définitions sensibles de mathématiques constructives, parce qu'elles nous guideront lorsque nous restreindrons les constructions à une classe préétablie.

---

[1] Les logiciens ont pour leur part beaucoup travaillé sur des systèmes formels qui peuvent rendre compte des mathématiques pratiquées dans un livre tel que **[CA]** (le premier livre de Bishop date de 1967, et la logique intuitionniste de Heyting date de 1930). On pourra par exemple consulter **[FCM]** à ce sujet.

Les notions de construction ou opération sont considérées comme des *notions premières, non définies,* au même titre que la notion d'entier naturel .

Constructivement, un ensemble $(X, \neq_X)$ est donné lorsque:

- on décrit ce qu'il faut faire pour construire un objet de l'ensemble X .
- on décrit, concernant les objets de X , une **relation de séparation** , notée $\neq_X$, et vérifiant les propriétés suivantes (axiomes pour une relation de séparation):

  pour tous x , y , z dans X

  i. $x \neq_X x$ est absurde

  ii. $x \neq_X y$ équivaut à $y \neq_X x$

  iii. $x \neq_X y$ implique $x \neq_X z$ ou $y \neq_X z$

NB: le "ou" , dans iii. , est un "ou" constructif, c.-à-d. doit pouvoir être constaté comme résultat d'une construction.

On définit alors une **relation d'égalité**, notée $x =_X y$, par : " $x \neq_X y$ est absurde ". Cette égalité de X est une relation d'équivalence[2].

Un ensemble $(X, \neq_X)$ est appelé **discret** , lorsque, pour tous x et x' dans X , on a : $x \neq_X x'$ ou $x =_X x'$. L'ensemble des nombres réels "n'est pas" discret dans la mesure où on ne sait pas décider "en général" si 2 réels donnés sont égaux ou séparés.

On appelle **fonction** de l'ensemble $(X, \neq_X)$ vers l'ensemble $(Y, \neq_Y)$ une opération de X vers Y qui vérifie la propriété d'extensionnalité suivante :

$$F(x) \neq_Y F(x') \Rightarrow x \neq_X x'.$$

Une fonction $f : X \longrightarrow Y$ est dite **surjective** si on connait une opération r de Y vers X vérifiant : pour tout $y \in Y$, $f(r(y)) =_Y y$. Notez que r n'est pas nécessairement une fonction.

Une **énumération** d'un ensemble X est à très peu de choses près une application surjective de $\mathbb{N}$, ensemble des entiers naturels, sur X : elle est donnée précisément comme suit :

- une fonction $f : \mathbb{N} \longrightarrow X \cup \{u\}$ et une opération $r : X \longrightarrow \mathbb{N}$ qui vérifient : pour tout x de X , on a $f(r(x)) =_X x$.

L'objet u est extérieur à X, il a été rajouté pour le cas où on ne sait pas a priori si X est vide ou non . Si X est "habité", c.-à-d. si on connait un élément de X , il revient au même de dire qu'il existe une application surjective de $\mathbb{N}$ sur X . L'opération r n'est pas nécessairement une fonction. Un ensemble qui possède une énumération est dit **énumérable**.

Si maintenant nous considérons une classe de constructions $\mathfrak{C}$, et que nous estimons que seules les constructions de cette classe sont acceptées, nous obtenons la notion correspondante de $\mathfrak{C}$-ensemble, ou ensemble $\mathfrak{C}$-présenté.

Par exemple, si nous considérons les constructions faisables par une machine de Turing, nous aurons une notion d'ensemble "récursivement présenté".

Pour ce qui concerne une version relativisée à $\mathfrak{C}$ de la notion d'ensemble discret, nous demanderons que l'alternative $x \neq_X x'$ ou $x =_X x'$ puisse être tranchée au moyen d'une $\mathfrak{C}$-construction à partir des entrées x et x' . Si nous voulions relativiser à $\mathfrak{C}$ la notion de

---

2 Cette étude est consacrée aux ensembles discrets énumérables ; dans ce cas (et dans celui des espaces métriques), il y a une relation de séparation au sens constructif. Dans [CA] , Bishop donne une définition de la notion d'ensemble basée sur une relation d'égalité plutôt que de séparation.

relation de séparation, sans hypothèse de discrétion, le problème serait plus délicat, et la réponse à apporter n'est peut-être pas unique[3].

[3] Signalons néanmoins que la notion d'espace métrique séparable complet se laisse relativiser à une classe $\mathfrak{C}$ de manière simple et directe, ce qui permet de traiter dans ce cadre une grande partie de l'analyse. Par exemple on a des définitions naturelles de $\mathfrak{C}$-nombre réel ou de $\mathfrak{C}$-fonction continue de $[0,1]$ vers $\mathbb{R}$.

A) GENERALITES SUR LES $\mathfrak{C}$-ENSEMBLES-DISCRETS

Nous supposerons que la classe de constructions $\mathfrak{C}$ concerne des objets du type "mots sur un alphabet fini". Plus précisément, pour tous alphabets finis A et B , si A* désigne le langage engendré par A , nous supposons définies les constructions de classe $\mathfrak{C}$ de A^{*k} vers B*.

a) Quelques classes de constructions intéressantes

Stabilité par composition

Comme nous avons en vue des classes de constructions qui fournissent des opérations de A^{*k} vers B* , la question de la stabilité de ces opérations par composition se pose naturellement. Ce n'est pas le cas lorsqu'on étudie les algorithmes comme "sélecteurs de langage".

Or, des classes de complexité comme **DTIME**(n^2) ne sont pas stables par composition. Nous introduisons donc pour remédier à cet inconvénient des classes de complexité où la taille de la sortie est mieux majorée que le temps de calcul, ou l'espace de calcul.

Nous notons **SPACERES**(f) la classe des algorithmes où la taille de la sortie (space résultat) est majorée par f(n) , où n est la taille de l'entrée.

Précisons ici quelques abréviations, certaines très classiques, que nous utiliserons:

DTIME(O(f)) pour $\cup_{c,a}$ **DTIME**(c+a.f)

LINTIME	= **DT1** = **DTIME**(O(n))	**DT0**	= $\cup_c$ **DTIME**(n+c)
$\mathcal{P}$	= $\cup_b$ **DTIME**($O(n^b)$)	**DTNLG**	= $\cup_b$ **DTIME**($O(n.\lg^b(n))$)
DSP1	= **DSPACE**(O(n))	**PSPACE**	= $\cup_b$ **DSPACE**($O(n^b)$)
RES0	= $\cup_c$ **SPACERES**(n+c)	**RES1**	= **SPACERES**(O(n))
RESP	= $\cup_b$ **SPACERES**($O(n^b)$)		
$\mathcal{P}_0$	= **RES0** $\cap$ $\mathcal{P}$	$\mathbf{DTNLG_0}$	= **DTNLG** $\cap$ **RES0**
$\mathbf{DTIME_0}(O(n^k))$	= **RES0** $\cap$ **DTIME**($O(n^k)$) etc...		
$\mathcal{P}_1$	= **RES1** $\cap$ $\mathcal{P}$	$\mathbf{DTNLG_1}$	= **DTNLG** $\cap$ **RES1**
$\mathbf{DTIME_1}(O(n^k))$	= **RES1** $\cap$ **DTIME**($O(n^k)$) etc...		

Nous ferons souvent référence également à la classe $\mathbb{P}\mathbf{r}$ des fonctions primitives récursives, et à la classe **Rec** des fonctions récursives.

Ce sont toutes des classes stables par composition . Et on a l'inclusion évidente:

PSPACE $\subset$ **RESP**.

Lorsque $\mathbb{N}$ est présenté en binaire, une opération f de $\mathbb{N}$ vers $\mathbb{N}$ est **RES0** ssi f(n) = O(n) , et elle est **RES1** ssi il existe un k tel que $f(n) = O(n^k)$

Mesures de la grandeur des entrées et sorties

Par ailleurs, on a parfois intérêt à considérer une mesure de l'entrée qui ne soit pas directement la taille de l'objet (pour un type de description choisi), tout en étant polynomialement relié à la taille.

Expliquons-nous sur un exemple : considérons les algèbres $\mathbf{M_n}(\mathbb{Z})$. Pour une matrice $A = (a_{ij})$, la taille $s(A)$ dans une présentation "naturelle" , sera : $s(A) = n^2 + \Sigma s(a_{ij})$

Cependant, si nous considérons $t(A) := n + s(\Sigma |a_{ij}|)$, on peut vérifier facilement que, pour 2 matrices A et B , on obtient l'inégalité : $t(AB) \leq t(A) + t(B)$. Par ailleurs les "mesures" t et s sont polynomialement reliées. Mais avec la mesure t le produit des matrices est **RES0**, ce qui n'est pas le cas avec la mesure "naturelle" s .

Ainsi, un ensemble sera toujours présenté avec une mesure de la grandeur des objets qui le composent.

Si la mesure n'est pas précisée, c'est qu'il s'agit de la taille "naturelle" au sens de la longueur du mot utilisé pour représenter l'objet .

Notons que 2 objets de X , distincts en tant que mots de A* , mais égaux dans X , ont en général 2 mesures distinctes: par exemple un même nombre rationnel peut être représenté par 2 fractions distinctes, de tailles distinctes .

Lorsque la classe de construction $\mathfrak{C}$ considérée est une classe de complexité, il faudra la comprendre au sens de la mesure considérée lorsqu'est définie la présentation de l'ensemble étudié (comme nous venons de le faire en affirmant que le produit des matrices est **RES0** lorsqu'on utilise la mesure t) .

Hypothèses concernant la classe de constructions $\mathfrak{C}$

Nous devons expliciter quelques hypothèses générales concernant la classe $\mathfrak{C}$ des constructions considérées.

Ces hypothèses seront en quelque sorte nos "axiomes de la théorie des $\mathfrak{C}$-ensembles-discrets". Elles seront immédiatement vérifiées pour les classes que nous avons en vue. Elles permettent de faire fonctionner les constructions élémentaires concernant les $\mathfrak{C}$-ensembles-discrets. Comme nous envisageons dans nos applications essentiellement les classes $\mathcal{P}_0$, $\mathcal{P}_1$, $\mathcal{P}$, **DTNLG**, **PSPACE**, $\mathbb{P}\mathbf{r}$, **Rec** , on pourrait très bien se passer de ce paragraphe, qui manifeste un souci de généralité peut-être abusif.

Nous allons formuler nos hypothèses de manière assez lâche, renvoyant un exposé plus détaillé en note (n.1).

Nous abrègerons " construction de classe $\mathfrak{C}$ " en **$\mathfrak{C}$-construction** .

Nous désignerons par A et B des alphabets finis, A* et B* les langages qu'ils engendrent.

L'ensemble **Lst** (A*), des listes d'éléments de A* (ou encore : suites finies d'éléments de A*), peut être réalisé comme une partie d'un langage A°* (où A° est obtenu en rajoutant à A des symboles représentant [,] et ;) . Si X_1 , X_2 ,..., X_n sont des parties de A*, l'ensemble $X_1 \times X_2 \times ... \times X_n$ peut être réalisé comme une partie de **Lst**(A*) (listes convenables de n éléments).

Les $\mathfrak{C}$-constructions doivent permettre d'accomplir 2 tâches :

- définir les $\mathfrak{C}$-parties des ensembles A* , et
- définir les $\mathfrak{C}$-opérations entre $\mathfrak{C}$-parties X et Y d'ensembles A* et B*, lorsqu'on a défini pour X et Y une mesure de la grandeur de leurs objets.

La mesure de la grandeur d'un objet de X ($\mathfrak{C}$-partie de A*) est toujours supposée vérifier les propriétés suivantes:

- c'est un entier naturel > 0 , et
- elle est polynomialement reliée à la taille naturelle (qui est la longueur du mot, sauf pour le mot vide v de taille 1)
- l'identité $I : x \to x$ de $(X, \| \ \|_{A^*})$ vers $(X, \| \ \|_X)$ est une $\mathfrak{C}$-opération

Voici maintenant la formulation de nos hypothèses:

- **constructions élémentaires appartenant à $\mathfrak{C}$:**
  toutes les constructions de la classe $\mathbf{DTNLG_0}$ sont dans $\mathfrak{C}$.
- **rapport entre $\mathfrak{C}$-parties et $\mathfrak{C}$-opérations:**
  une partie X de A* est une $\mathfrak{C}$-partie si et seulement si sa fonction caractéristique (opération de A* vers {**oui**,**non**}) est une $\mathfrak{C}$-opération (ici A* est muni de la mesure naturelle).
- **propriétés de stabilité pour les $\mathfrak{C}$-opérations:**
  * stabilité pour la composition.
  * stabilité pour la définition par cas :
    f et g sont 2 $\mathfrak{C}$-opérations de X vers Y , sl est une $\mathfrak{C}$-opération de X vers {**oui**,**non**} , on définit l'opération $h : X \to Y$, par :

    $h(x) := f(x)$ si $sl(x) =$ **oui** , et $h(x) := g(x)$ sinon
  * stabilité pour **Lst** :
    si $f : X \to Y$ est une $\mathfrak{C}$-opération, il en est de même pour l'opération
    g: **Lst** (X) $\to$ **Lst** (Y) , définie par
    $g([x_1,x_2,...,x_n]) := [f(x_1),f(x_2), ... ,f(x_n)]$.

b) $\mathfrak{C}$-ensembles-discrets , $\mathfrak{C}$-fonctions , $\mathfrak{C}$-structures algébriques

Présentation d'un ensemble énumérable

D'un point de vue constructif, les objets d'un ensemble X sont en général représentés par des mots écrits sur un alphabet fini déterminé A . Seuls certains mots de A* représentent des objets de X .

S'il existe un test (une opération) P de A* vers {**oui**,**non**} indiquant si le mot m représente ou non un objet de X , l'ensemble est alors énumérable . Lorsqu'on a ainsi décrit les objets d'un ensemble énumérable X , on dit qu'on a défini une **présentation** de X.

Tout ensemble énumérable peut naturellement être "présenté".

La catégorie des $\mathfrak{C}$-ensembles-discrets

Définition A.b1 :

Un **$\mathfrak{C}$-ensemble-discret** (ou ensemble-discret-$\mathfrak{C}$-présenté) est donné lorsque:

- on considère un alphabet fini A
- on considère une opération P_X de classe $\mathfrak{C}$ de A^* vers {**oui,non**} acceptant un langage $X \subset A^*$: les mots de X seront les objets de l'ensemble.
- on a défini une opération V_X de classe $\mathfrak{C}$, de $X \times X$ vers {**oui,non**}, qui vérifie, pour tous x, y, z de X :

  $V_X(x,x) =$ **oui** , $V_X(x,y) = V_X(y,x)$,

  $V_X(x,y) = V_X(y,z) =$ **oui** $\Rightarrow$ $V_X(x,z) =$ **oui**

  (l'égalité de x et y comme éléments de X est définie par $V_X(x,y) =$ **oui**) .
- on a défini une mesure de la grandeur des mots de X , polynomialement reliée à la taille. (la mesure doit toujours être un entier > 0)

Notations : La mesure de la grandeur de l'objet x du $\mathfrak{C}$-ensemble-discret X sera en général notée $\|x\|_X$, ou plus simplement $\|x\|$.
En toute rigueur, le $\mathfrak{C}$-ensemble-discret X devrait être noté $(A, P_X, V_X, \| \ \|_X)$.

Remarque : l'identité entre mots de A^* peut être $\mathfrak{C}$-testée; c'est donc une relation d'égalité possible.

Rappelons qu'une fonction de X vers Y est par définition une opération extensionnelle (c.-à-d.: qui se comporte bien par rapport aux relations de séparation définies sur X et Y). Ceci nous amène à définir la catégorie des $\mathfrak{C}$-ensembles discrets comme suit.

Définition A.b2 : Etant donnés deux $\mathfrak{C}$-ensembles-discrets X et Y , on appellera **$\mathfrak{C}$-fonction** de X vers Y une opération de classe $\mathfrak{C}$ de X vers Y qui est une fonction de X vers Y .

On a donc défini la catégorie des $\mathfrak{C}$-ensembles-discrets.

On appellera **$\mathfrak{C}$-équivalence** un isomorphisme dans cette catégorie. Lorsque on a deux classes de constructions $\mathfrak{C}_1$ et $\mathfrak{C}_2$ avec $\mathfrak{C}_1 \subset \mathfrak{C}_2$, il y a un foncteur d'oubli de la catégorie des $\mathfrak{C}_1$-ensembles-discrets vers celle des $\mathfrak{C}_2$-ensembles-discrets.

Quelques $\mathfrak{C}$-équivalences (plus de détails en note n.2)

Pour un entier n (abstrait) nous noterons **lg**(n) sa longueur lorsqu'il est écrit en binaire. L'ensemble $\mathbb{N}$ des entiers naturels présentés en binaire est une **DT0**-partie de $\{0,1\}^*$, qui est **DT0**-équivalente à $\{0,1\}^*$, donc $\mathfrak{C}$-équivalente à $\{0,1\}^*$ ($\mathfrak{C}$ contient $\mathbf{DTNLG_0}$). De même, l'ensemble $\mathbb{N}$ présenté en base b est une **DT0**-partie de A^* , qui est **DT0**-équivalente à A^*, où A est un alphabet à b lettres : {0,1,...,b-1} . Le changement de base de numérotation est une fonction de classe $\mathbf{DTNLG_1}$. En prenant **lg**(n) pour mesure de l'entier n écrit en base b , les présentations de $\mathbb{N}$ en binaire et en base b sont donc $\mathfrak{C}$-équivalentes. De même, en modifiant convenablement la mesure des mots dans A^* , les ensembles A^* sont 2 à 2 $\mathfrak{C}$-équivalents .

Soit par ailleurs $X = (A, P_X, V_X, \| \ \|_X)$ un $\mathfrak{C}$-ensemble-discret. Notons X' le $\mathfrak{C}$-ensemble-discret $X' := (A, P_X, V_X, \| \ \|_{X'})$, où seule la mesure de la grandeur des objets a été modifiée. Soit la fonction $I : x \rightarrow x$, définie de X vers X': I est une $\mathfrak{C}$-équivalence

si la classe $\mathfrak{C}$ contient $\mathfrak{P}$, puisque les mesures sont polynomialement reliées entre elles. Il est donc bien clair que l'introduction d'une mesure de la taille des objets n'a d'intérêt pratique que pour les classes de constructions strictement plus petites que $\mathfrak{P}$. Dans le cas contraire, la catégorie obtenue sans introduire de mesure de la taille des objets, équivalente à la catégorie des $\mathfrak{C}$-ensembles-discrets, est bien suffisante.

Sous-$\mathfrak{C}$-ensembles-discrets, applications $\mathfrak{C}$-surjectives, $\mathfrak{C}$-quotients

Si X est le $\mathfrak{C}$-ensemble-discret $(A, P_X, V_X, \| \|_X)$, un **sous-$\mathfrak{C}$-e-d** Y de X est défini lorsqu'on a donné une $\mathfrak{C}$-fonction f de X vers {**oui**,**non**}. Cela définit la $\mathfrak{C}$-partie $Y := \{ x \in X ; f(x) = \textbf{oui} \}$ de A*.

On définit l'égalité et la mesure sur Y comme induites par celles de X . L'injection canonique $Y \to X$ est alors une $\mathfrak{C}$-fonction . Les sous-$\mathfrak{C}$-e-d de X sont stables par intersection, réunion et différence. Un sous-$\mathfrak{C}$-e-d de X est encore appelé une **partie $\mathfrak{C}$-détachable** de X , ou une **$\mathfrak{C}$-partie** de X .

Notez que toute $\mathfrak{C}$-partie Z de A* contenue dans X ne définit pas nécessairement une partie $\mathfrak{C}$-détachable de X , parce que l'égalité dans X peut être plus lâche que celle dans A*, et Z n'est pas forcément saturée pour la relation d'égalité dans X.

Une $\mathfrak{C}$-fonction f de X vers Y est dite **$\mathfrak{C}$-surjective** lorsqu'on connait une $\mathfrak{C}$-opération $r : Y \to X$ qui vérifie, pour tout y de Y : $f(r(y)) =_Y y$.
Notez que r n'est pas nécessairement une fonction.
La composée de deux fonctions $\mathfrak{C}$-surjectives est une fonction $\mathfrak{C}$-surjective.

Un **$\mathfrak{C}$-quotient** de $X = (A, P_X, V_X, \| \|_X)$ est par définition un $\mathfrak{C}$-ensemble-discret de la forme $X' = (A, P_X, V_{X'}, \| \|_X)$, où l'on a, pour tous x , y de X :

$$x =_X y \quad \Rightarrow \quad x =_{X'} y \ .$$

La projection canonique de X sur X' est alors une $\mathfrak{C}$-fonction $\mathfrak{C}$-surjective. Notez que $V_{X'}$ est une $\mathfrak{C}$-fonction de $X \times X$ vers {**oui**,**non**} . (voir le § qui suit pour $X \times X$ comme $\mathfrak{C}$-ensemble-discret)

Produit de 2 $\mathfrak{C}$-ensemble-discrets , $\mathfrak{C}$-structures algébriques

On a une notion naturelle de produit de 2 $\mathfrak{C}$-ensembles-discrets : on écrit les mots représentant les éléments x et y de X et Y l'un à la suite de l'autre, séparés par un symbole ne faisant pas partie des alphabets utilisés. Et on pose:

$$\| (x,y) \| = \| x \| + \| y \| \ .$$

Il s'agit d'ailleurs du produit dans la catégorie des $\mathfrak{C}$-ensembles-discrets pour des classes $\mathfrak{C}$ comme $\mathfrak{P}$, $\mathfrak{P}_1$, $\mathbf{DTIME}_1(O(n^k))$, $\mathbb{P}\mathbf{r}$, **Rec.** (n.3)

A partir de ces notions de sous-$\mathfrak{C}$-e-d et de produit de 2 $\mathfrak{C}$-ensembles-discrets, nous pouvons parler de $\mathfrak{C}$-lois de composition, de $\mathfrak{C}$-relations binaires etc... et donc de $\mathfrak{C}$-monoïdes, $\mathfrak{C}$-groupes, $\mathfrak{C}$-anneaux, $\mathfrak{C}$-ensembles-ordonnés et plus généralement de **$\mathfrak{C}$-structure algébrique**[1] d'un type donné .

Il faut noter qu'il s'agit de structures algébriques sur des ensembles discrets énumérables.

---

[1] Nous ne chercherons pas ici à donner la définition précise la plus générale possible de la notion de $\mathfrak{C}$-structure algébrique. Disons que cette structure ne doit impliquer qu'un nombre fini d'ensembles, avec un nombre fini de lois de compositions, de constantes, et de relations (unaire ou binaire ou ternaire ou ...).

Chaque fois que c'est possible , nous considèrerons que les axiomes de la structure algébrique sont présentés comme purement universels: par exemple pour les groupes, anneaux et corps . Ainsi, dans un $\mathfrak{C}$-groupe, non seulement la loi produit, mais aussi la loi unaire : $x \rightarrow x^{-1}$, doivent être des $\mathfrak{C}$-fonctions. (n.4)

Remarques :

1 - Dans le cas de la classe **Rec**, notre notion de **Rec**-structure est exactement équivalente à la notion de structure algébrique récursivement présentée définie dans [F-S].(n.5)

2 - Tout $\mathfrak{C}$-ensemble-discret définit évidemment un ensemble au sens constructif. Lorsqu'un ensemble X est déjà défini constructivement, une **$\mathfrak{C}$-présentation** de cet ensemble est donnée par : - un $\mathfrak{C}$-ensemble-discret X' d'une part, - une bijection entre X et X', d'autre part. Ainsi un $\mathfrak{C}$-ensemble-discret peut-il être considéré comme un ensemble "abstrait" muni d'une structure de $\mathfrak{C}$-calculabilité additionnelle.
De la même manière, lorsqu'un ensemble est muni d'une structure algébrique précise, nous parlerons de **$\mathfrak{C}$-présentation de cette structure algébrique** pour une $\mathfrak{C}$-présentation de l'ensemble X qui fait des lois de composition des $\mathfrak{C}$-fonctions (et des relations unaires, binaires etc ... des $\mathfrak{C}$-relations).

Structures algébriques naturellement primitives récursives

Notons $\mathbb{N}$ pour l'ensemble des entiers naturels présentés en binaire.

Si nous considérons la classe $\mathbb{P}\mathbf{r}$ des fonctions primitives récursives, nous avons immédiatement le résultat suivant (les axiomes de Peano sont là pour ça en quelque sorte...):

Si $\mathbb{N}'$ est une $\mathbb{P}\mathbf{r}$-présentation de la structure algébrique ($\mathbb{N}$, 0 , $n \rightarrow n + 1$) , alors la fonction "identité" de $\mathbb{N}$ vers $\mathbb{N}'$ est une $\mathbb{P}\mathbf{r}$-fonction[1].

De manière générale nous dirons qu'une **structure algébrique est naturellement primitive récursive** lorsque il existe une $\mathbb{P}\mathbf{r}$-présentation "naturelle" de cette structure au sens qu'elle est $\mathbb{P}\mathbf{r}$-initiale parmi toutes les $\mathbb{P}\mathbf{r}$-présentations de cette structure. (c.-à-d.: la bijection "identité" qui va de la $\mathbb{P}\mathbf{r}$-structure naturelle vers une autre $\mathbb{P}\mathbf{r}$-présentation est une $\mathbb{P}\mathbf{r}$-fonction). Il est clair que la $\mathbb{P}\mathbf{r}$-présentation "naturelle" est alors unique à $\mathbb{P}\mathbf{r}$-isomorphisme près.

Pour une autre classe de constructions $\mathfrak{C}$, nous pourrions parler de **structure algébrique naturellement de type $\mathfrak{C}$** . En fait, il s'avère que ce n'est pas "la bonne" notion. La bonne notion est celle de structure algébrique "naturellement complètement $\mathfrak{C}$-calculable", que nous étudierons au B .

Si une structure algébrique est naturellement primitive récursive, tous les automorphismes de la $\mathfrak{C}$-structure naturelle sont primitifs récursifs.

Les structures algébriques "de type fini" qui peuvent être $\mathbb{P}\mathbf{r}$-présentées possèdent une $\mathbb{P}\mathbf{r}$-présentation naturelle (la seule qu'on considère en général). (n.6) . Mais il y a des groupes de présentation finie pour lesquels l'égalité n'est pas récursivement décidable (Théorème de Novikoff), donc qui ne peuvent pas être **Rec**-présentés.

---

[1] Divertissement mathématique : toute $\mathbb{P}\mathbf{r}$-présentation de la structure algébrique ($\mathbb{N}$, 0 , $n \rightarrow n+1$, $n \rightarrow n \dot{-} 1$) est-elle $\mathbb{P}\mathbf{r}$-équivalente à la présentation standard ?
Voici par ailleurs un exemple de structure algébrique constructivement définie qui "n'est pas" constructivement isomorphe à ($\mathbb{N}$, $n \rightarrow n + 1$): l'ensemble sous-jacent est $\mathbb{N}$, le successeur de a est $a + 1$ sauf éventuellement dans les 2 cas suivants : si a est le 1er contre-exemple à la conjecture de Machin-Bidule, le successeur de a est 0, et le successeur de $a - 1$ est $a + 1$. Dans cet exemple, la fonction successeur est bien définie, mais on ne sait pas déterminer un élément n'ayant pas de prédécesseur tant qu'on n'a pas résolu la conjecture de Machin-Bidule.

Notez que $(\mathbb{N}, \times)$ n'est pas naturellement primitive récursive puisqu'il existe des automorphismes non primitifs récursifs de cette structure.

Problème ouvert : construire un groupe de présentation finie pour lequel l'égalité est récursive mais pas primitive récursive. (si la réponse est positive cela donne un exemple de groupe discret **Rec**-présenté mais qui ne peut pas être $\mathbb{P}$**r**-présenté)
NB: comme la plupart des problèmes ouverts signalés dans ce texte, celui-ci n'est pas "garanti ouvert" par l'auteur.

Sous-structures et structures quotients

Etant donnée une $\mathfrak{C}$-structure algébrique X, si Y est une partie $\mathfrak{C}$-détachable qui est une sous-structure, on obtient de manière évidente une $\mathfrak{C}$-présentation de la structure algébrique Y, on dit que Y est une **$\mathfrak{C}$-sous-structure** de X.

On définit de même une notion de **$\mathfrak{C}$-structure-quotient** lorsqu'un $\mathfrak{C}$-quotient est une structure quotient.

$\mathfrak{C}$-sous-structures et $\mathfrak{C}$-structures-quotients vérifient les propriétés caractéristiques universelles habituelles.

Pour qu'un quotient d'un $\mathfrak{C}$-groupe soit un $\mathfrak{C}$-quotient il faut et suffit que le noyau de la projection soit un $\mathfrak{C}$-sous-groupe, c.-à-d. un sous-groupe $\mathfrak{C}$-détachable.

ooooooooooooooooooooooooooo

Désormais, sauf mention explicite du contraire, nous utiliserons "ensemble" pour "ensemble discret", et "$\mathfrak{C}$-ensemble" pour "$\mathfrak{C}$-ensemble-discret".

ooooooooooooooooooooooooooo

c) Entiers naturels

Présentation en unaire

Nous noterons $\mathbb{N}_1$ l'ensemble des entiers naturels présenté en unaire, par exemple sous forme $\{1\}^*$ ou sous forme **Lst** (c.-à-d. **Lst**(alphabet vide)), ou sous toute autre forme $\mathfrak{C}$-équivalente.

La structure algébrique $(\mathbb{N}_1, 0, 1, +, \dot{-}, \mathbf{div}, \mathbf{mod}, >)$ est une $\mathfrak{P}_0$-structure; le produit est $\mathfrak{P}$ mais pas **RES1**. ($a \dot{-} b$ est égal à $a - b$ si $a > b$, et à 0 sinon)

Présentation en binaire

Nous noterons $\mathbb{N}$ l'ensemble des entiers naturels présenté en binaire, ou de toute autre manière $\mathfrak{C}$-équivalente. Par exemple présenté en base b, (dès que $\mathfrak{C}$ contient $\mathbf{DTNLG}_0$), mais en prenant pour mesure, au lieu de la longueur t_0 du mot : $1 + \mathrm{Ent}(t_0 . (\log(2)/\log(b)))$.

Du point de vue de la théorie des langages, le $\mathfrak{C}$-ensemble $\mathbb{N}$ joue un rôle essentiel du fait qu'il est $\mathfrak{C}$-équivalent à $\{0,1\}^*$, ou encore à B^* pour n'importe quel alphabet fini B ayant au moins 2 lettres (dès que $\mathfrak{C}$ contient $\mathbf{DTNLG}_0$).

La structure algébrique $(\mathbb{N}, 0, 1, +, \dot{-}, \times, \mathbf{div}, \mathbf{mod}, >)$ est une $\mathfrak{P}_0$-structure.

Notation: nous réservons la notation **lg**(n) pour "longueur de l'entier n s'il était écrit en binaire" (même si l'entier n considéré à ce moment-là n'est pas exprimé en binaire).

Le $\mathfrak{C}$-ensemble $\mathbb{N}_1$ est $\mathfrak{C}$-équivalent à la $\mathfrak{C}$-partie $\mathbf{N}_1$ de $\mathbb{N}$ formée des puissances de 2 . Mais il n'existe pas de $\mathfrak{P}$-fonction injective de $\mathbb{N}$ vers $\mathbb{N}_1$. Les $\mathfrak{P}$-ensembles $\mathbb{N}$ et $\mathbb{N}_1$ ne sont pas $\mathfrak{P}$-équivalents. La fonction $n \to n$ de $\mathbb{N}_1$ vers $\mathbb{N}$ est une $\mathfrak{P}$-fonction, mais pas une $\mathfrak{P}$-équivalence.

Autres présentations

Il existe bien d'autres présentations de l'ensemble des entiers naturels, 2 à 2 non $\mathfrak{P}$-équivalentes.

Par exemple on peut noter $\mathbb{N}_b$ le $\mathfrak{P}$-ensemble obtenu par une présentation "en bibase b" :
un entier n est présenté sous forme d'une liste de couples (i , a_i), où i est un entier écrit en base b , et a_i est un chiffre de cette base, les i arrivant en ordre croissant, et avec : $n = \Sigma\, a_i b^i$. La structure algébrique ($\mathbb{N}_b$, + , × , >) est une $\mathfrak{P}_1$-structure, mais rien ne va plus avec la soustraction ou la division. (cf., dans $\mathbb{N}_b$ la soustraction $b^i - 1$) . La fonction $n \to n$ de $\mathbb{N}$ vers $\mathbb{N}_b$ est une $\mathfrak{P}$-fonction, mais non pas une $\mathfrak{P}$-équivalence.

Nous allons voir maintenant comment la notion classique de dénombrabilité se scinde en plusieurs notions bien distinctes du point de vue constructif et du point de vue des $\mathfrak{C}$-ensembles.

Enumérations[1]:

Rappelons qu'une énumération d'un ensemble X est donnée par une fonction $f : \mathbb{N} \to X \cup \{u\}$ et une opération $r : X \to \mathbb{N}$ qui vérifient : pour tout x de X , on a $r(f(x)) =_X x$. (l'objet u est extérieur à X).

Lorsque X est un $\mathfrak{C}$-ensemble , f une $\mathfrak{C}$-fonction et r une $\mathfrak{C}$-opération, nous disons que X est **$\mathfrak{C}$-énumérable**, et que **f est une $\mathfrak{C}$-énumération** de X .

Toute $\mathfrak{C}$-fonction surjective de $\mathbb{N}$ sur un $\mathfrak{C}$-ensemble X n'est pas forcément une $\mathfrak{C}$-énumération car elle peut n'être pas $\mathfrak{C}$-surjective. (cf. par exemple la fonction $n \to \mathbf{lg}(n)$ de $\mathbb{N}$ vers $\mathbb{N}$: c'est une $\mathfrak{P}$-fonction surjective qui n'est pas $\mathfrak{P}$-surjective)

Par contre on a :

Tout $\mathfrak{P}$-ensemble X est $\mathfrak{P}$-énumérable.
Plus généralement , si $\mathfrak{C}$ est une classe de constructions contenant $\mathfrak{P}$, tout $\mathfrak{C}$-ensemble X est $\mathfrak{C}$-énumérable.

En effet, remarquons tout d'abord que la mesure de la grandeur des objets de X n'intervient pas, puisque nous raisonnons à une $\mathfrak{C}$-équivalence près, et que $\mathfrak{C}$ contient $\mathfrak{P}$. D'autre part, si X est construit sur l'alphabet A , on pourra composer une $\mathfrak{P}$-équivalence $\mathbb{N} \to A^*$ avec la $\mathfrak{C}$-fonction de A^* dans $X \cup \{u\}$ définie comme suit:

- si $x \in X$, $x \to x$, sinon $x \to u$.

On vérifie que la composée est bien une $\mathfrak{C}$-énumération.

Remarque : Un mathématicien classique qui veut se faire une idée de ce que peut bien signifier un ensemble énumérable discret pour un constructiviste peut se tenir le discours suivant : admettons une notion a priori d'effectivité (ce qui est plus facile que d'admettre une notion a priori d'ensemble à la Cantor - Zermelo - Frankel) ; notons **Constr** la classe de toutes les fonctions effectivement calculables portant sur des langages A^* ; alors la catégorie

---

[1] La terminologie énumération, dénombrement, numérotation choisie ici est "assez" arbitraire, et ne prétend naturellement pas être exhaustive.

des ensembles énumérés discrets pour un constructiviste est équivalente à celle des **Constr**-ensembles-discrets , au sens des définitions ci-dessus, qui peuvent être lues avec des lunettes "classiques".

Dénombrements

Un **dénombrement** d'un ensemble X est par définition une énumération (f,r) de X telle que r soit une fonction.

Un ensemble discret qui possède une énumération (f,r) possède un dénombrement (f,r') : r'(x) est le plus petit entier n inférieur ou égal à r(x) tel que : $x =_X f(n)$. Par ailleurs un ensemble dénombrable X est nécessairement discret. Autrement dit, "dénombrable" équivaut à "énumérable et discret".

La notion de dénombrement, relativisée à la classe de constructions $\mathfrak{C}$, donne les notions de **$\mathfrak{C}$-dénombrement**, et de $\mathfrak{C}$-ensemble **$\mathfrak{C}$-dénombrable.**

Par le même argument que ci-dessus, tout **PSPACE**-ensemble-discret est **PSPACE**-dénombrable. Et de même pour toute classe $\mathfrak{C}$ stable par récurrence bornée (une définition par récurrence bornée est une définition par récurrence primitive où on astreint la fonction définie à rester majorée par une fonction donnée préalablement). Par contre l'ensemble énumérable $\mathbb{P}\mathbf{r}(\mathbb{N},\mathbb{N})$ des $\mathbb{P}\mathbf{r}$-fonctions de $\mathbb{N}$ vers $\mathbb{N}$ n'est pas **Rec**-dénombrable. (l'égalité n'y est pas **Rec**-décidable)

Si (f,r) est un $\mathfrak{C}$-dénombrement du $\mathfrak{C}$-ensemble X , la $\mathfrak{C}$-opération $x \to f(r(x))$ "choisit" un élément particulier dans chaque classe d'équivalence de la relation $=_X$. Autrement dit, les différents "représentants" d'un élément de $(X, =_X)$ possèdent une "forme réduite canonique", qui peut être $\mathfrak{C}$-calculée.

Un $\mathfrak{P}$-ensemble-discret n'est pas "a priori" $\mathfrak{P}$-dénombrable: cette question a manifestement à voir avec le fameux problème $\mathfrak{P} = \mathcal{N}\mathfrak{P}$? . (cf. n.7)

Numérotations:

Par définition, une **numérotation** d'un ensemble X est une énumération (f,r) qui vérifie:

i. si $f(n) = u$, alors pour tout $m > n$, $f(m) = u$

ii. si $f(p) \neq u$ et $f(p) =_X f(q)$, alors $p = q$

Toute numérotation est un dénombrement.

Les ensembles finis sont numérotables. Les ensembles infinis dénombrables sont numérotables. L'ensemble des contre-exemples à la conjecture de Goldbach "n'est pas" numérotable.

La notion de numérotation, relativisée à la classe de constructions $\mathfrak{C}$, donne les notions de **$\mathfrak{C}$-numérotation**, et de $\mathfrak{C}$-ensemble **$\mathfrak{C}$-numérotable.**

L'ensemble $\mathbb{Q}$ des nombres rationnels est de manière naturelle un $\mathfrak{P}$-ensemble, qui est $\mathfrak{P}$-dénombrable, mais qui ne semble pas $\mathfrak{P}$-numérotable. Cela confirmerait l'impression intuitive que l'ensemble $\mathbb{Q}$ est un petit peu plus compliqué que $\mathbb{N}$ ou que l'ensemble des nombres décimaux.

Si $f : \mathbb{N} \to \mathbb{N}$ est une fonction récursive qui croît plus vite que toute fonction $\mathbb{P}\mathbf{r}$, construite par récurrence double, son image peut être une partie $\mathbb{P}\mathbf{r}$-détachable de $\mathbb{N}$, (et donc un $\mathbb{P}\mathbf{r}$-ensemble), mais elle n'est pas $\mathbb{P}\mathbf{r}$-numérotable. (n.8)

De la même manière, et plus simplement, $\mathbb{N}_1$ est un ensemble $\mathfrak{P}$-dénombrable qui n'est pas $\mathfrak{P}$-numérotable.

$\mathfrak{P}$-ensembles $\mathfrak{P}$-réductibles

Nous introduisons enfin une notion qui est une version affaiblie de la $\mathfrak{P}$-dénombrabilité. Elle nous sera utile dans certains théorèmes par la suite.

Un $\mathfrak{P}$-ensemble X est dit **$\mathfrak{P}$-réductible** si on a un polynôme Q et une $\mathfrak{P}$-opération

r : $X \to X$, qui vérifient :

- pour tout x de X , $r(x) =_X x$
- si $y =_X x$, alors $\|r(x)\| < Q(\| y \|)$

On peut dire que l'opération r remplace le représentant x par un autre représentant r(x) , mais de taille raisonnable: c'est une sorte de forme réduite non canonique, mais utilisable pour les calculs de classe $\mathfrak{P}$.

La notion de $\mathfrak{P}$-réductibilité est une notion qui apparaît naturellement dans certaines preuves de $\mathfrak{P}$-calculabilité. Néanmoins, il semble que tous les exemples utiles d'ensembles $\mathfrak{P}$-réductibles soient également, de manière immédiate, des ensembles $\mathfrak{P}$-dénombrables. La notion de $\mathfrak{P}$-réductibilité n'est donc pas nécessaire pour les applications les plus courantes des théorèmes où elle intervient. Elle constitue sans doute un raffinement peu utile de la notion de $\mathfrak{P}$-dénombrabilité.

d) Présentations des entiers relatifs et des nombres rationnels

Symétrisation d'un $\mathfrak{C}$-monoïde commutatif régulier

La construction du symétrisé du monoïde commutatif régulier M , en munissant $M \times M$ de la relation d'égalité convenable, fonctionne sans problème du point de vue des $\mathfrak{C}$-structures algébriques.

En termes savants: le foncteur d'oubli des $\mathfrak{C}$-groupes abéliens vers les $\mathfrak{C}$-monoïdes commutatifs réguliers possède un adjoint à gauche.

On notera que lorsqu'un $\mathfrak{P}$-monoïde commutatif n'est pas régulier, l'égalité dans le groupe obtenu classiquement par symétrisation peut ne pas être décidable[1].

Soit M un $\mathfrak{C}$-monoïde commutatif régulier, G un $\mathfrak{C}$-groupe, $f : M \to G$ un homomorphisme qui fait de G le symétrisé de M . Pour que f fasse de G le $\mathfrak{C}$-symétrisé de M , il faut et suffit que :

- f est une $\mathfrak{C}$-fonction, et
- il existe 2 $\mathfrak{C}$-opérations g_1 et g_2 de G vers M telles que, pour tout x dans G , on ait : $x =_G f(g_1(x)) - f(g_2(x))$.

---

[1] Soit (u_p) une $\mathfrak{P}$-suite d'entiers, d'image non récursive. Considérons le monoïde commutatif librement engendré par une suite (a_n) et codé par la partie de **Lst**(ℕ) formée par les listes croissantes d'entiers. Introduisons la relation d'équivalence stable engendrée par les relations $a_{3n+1}.a_{3p+2} = a_{3n}.a_{3p+2}$ si $n = u_p$. On obtient un $\mathfrak{P}$-monoïde commutatif. Mais dans le symétrisé, $a_{3n+1} = a_{3n}$ si et seulement si n est une valeur prise par la suite (u_p) .

Les propriétés d'admettre un $\mathfrak{P}$-dénombrement ou une $\mathfrak{P}$-numérotation ne passent pas "a priori" d'un $\mathfrak{P}$-monoïde commutatif régulier à son symétrisé[1].

Nous dirons qu'un $\mathfrak{C}$-monoïde commutatif M noté multiplicativement est **$\mathfrak{C}$-divisible** lorsqu'il existe une $\mathfrak{C}$-opération D de $M \times M$ vers $M \cup \{u\}$ vérifiant :

si $D(a,b) = u$, alors pour tout $x \in M$: $a.x \neq b$, et , si $D(a,b) \in M$,
alors : $a.D(a,b) = b$.

Un $\mathfrak{C}$-monoïde commutatif régulier M est $\mathfrak{C}$-divisible si et seulement si M "est" une partie $\mathfrak{C}$-détachable de son symétrisé: plus précisément: si l'homomorphisme $f : M \to G$ est une $\mathfrak{C}$-équivalence entre M et une $\mathfrak{C}$-partie de G .

La présentation standard $\mathbb{Z}$

La présentation des entiers relatifs sous forme d'un nombre en binaire avec un signe, sera considérée comme la présentation standard, et sera notée $\mathbb{Z}$.

Elle fait de ($\mathbb{Z}$, + , − , × , **div** , **mod** , <) une $\mathfrak{P}_0$-structure. De plus ce $\mathfrak{P}_0$-groupe est $\mathfrak{P}_0$-isomorphe au $\mathfrak{P}_0$-symétrisé de $\mathbb{N}$ [(2)].

De manière générale nous noterons $\mathbb{Z}$ toute présentation des entiers relatifs $\mathfrak{P}_1$-isomorphe à la présentation standard et faisant de ($\mathbb{Z}$, + , − , × , **div** , **mod** , <) une $\mathfrak{P}_0$-structure.

C'est le cas par exemple pour la présentation en base 3 avec les chiffres 0 , 1 , -1 ou encore en base 2 avec les chiffres 0 , 1 , -1 et la relation d'égalité convenable (cette présentation peut être utile pour l'écriture de valeurs approchées successives de nombres réels).

Autres présentations des entiers relatifs

Les autres présentations de l'ensemble des entiers naturels que nous avons décrites donnent par symétrisation des présentations des entiers relatifs non $\mathfrak{P}$-isomorphes à la présentation standard. Nous noterons $\mathbb{Z}_1$ le symétrisé de $\mathbb{N}_1$: on obtient une présentation $\mathfrak{P}_1$-isomorphe en prenant un entier codé en unaire avec un signe[3].

Corps des fractions d'un $\mathfrak{C}$-anneau intègre

La construction du corps des fractions d'un anneau intègre M , en munissant $M \times (M - \{0\})$ de la relation d'égalité convenable, fonctionne sans problème du point de vue des $\mathfrak{C}$-structures algébriques pour les classe $\mathfrak{C}$ suivantes : $\mathfrak{P}$, $\mathfrak{P}_1$, **PSPACE** , **RES1** , $\mathbb{P}r$, **Rec** .

On a par contre de petits ennuis avec l'addition pour la classe $\mathfrak{P}_0$: par exemple dans le corps des fractions de $\mathbb{Z}$ l'addition est seulement dans **SPARES**(2.n) (additionner 1/1 et $1/2^n$ pour s'en convaincre).

Un $\mathfrak{P}$-anneau intègre est dit $\mathfrak{P}$-divisible lorsque le monoïde multiplicatif M - {0} est $\mathfrak{P}$-divisible . L'anneau est alors identifiable à une $\mathfrak{P}$-partie de son corps de fractions.

---

[1] La première question ($\mathfrak{P}$-dénombrement) aura une réponse positive si $\mathfrak{P} = \mathfrak{M}\mathfrak{P}$ (cf. n.7) . La deuxième question pourrait faire l'objet d'un divertissement mathématique.

[2] Divertissement mathématique : Soit $\mathbb{Z}'$ une autre présentation des entiers relatifs et supposons que la structure :
($\mathbb{Z}'$, + , − , × , div , mod , <) soit une $\mathfrak{P}_0$-structure et $\mathbb{Z}'$ un $\mathfrak{P}$-ensemble $\mathfrak{P}$-réductible, alors la fonction $z \to z$ de $\mathbb{Z}$ vers $\mathbb{Z}'$ est-elle nécessairement un $\mathfrak{P}$-isomorphisme ?

[3] Divertissement mathématique : notons $\mathbb{Z}_2$ le symétrisé de $\mathbb{N}_2$. On voit facilement que $\mathbb{N}_2$ est $\mathfrak{P}$-numérotable. Est-ce que $\mathbb{Z}_2$ est $\mathfrak{P}$-numérotable ?

$\mathbb{Q}$ comme $\mathcal{P}_0$-structure

Si on mesure la grandeur de la fraction a/b par: $\|a/b\| := \mathbf{lg}(|a|+b)$, on constate immédiatement que:

En notant $\mathbb{Q}$ l'ensemble des rationnels présenté comme $\mathbb{Z} \times \mathbb{N}^+$ muni de la relation d'égalité convenable et de la mesure définie ci-dessus, on obtient une $\mathcal{P}_0$-présentation $\mathcal{P}_1$-équivalente à celle obtenue avec la mesure naturelle, et la structure ($\mathbb{Q}$, + , − , × , / , Ent , < , numérateur de la fraction réduite) est une $\mathcal{P}_0$-structure[1].

On notera $\mathbb{D}$ l'ensemble des nombres dyadiques dans sa présentation naturelle (binaire avec virgule et signe) et avec une mesure qui fait de :

$$(\mathbb{D} , + , - , \times , \text{Ent} , < , (x, n) \rightarrow x/2^n : \mathbb{D} \times \mathbb{N}_1 \rightarrow \mathbb{D})$$

une $\mathcal{P}_0$-structure. (par exemple la mesure héritée de celle de $\mathbb{Q}$).

---

[1] $\mathbb{Q}$ est $\mathcal{P}_0$-dénombrable puisque le calcul de la réduite d'une fraction est $\mathcal{P}_0$.
$\mathbb{Q}$ est $\mathbb{P}\mathbf{r}$-numérotable et c'est un corps naturellement primitif récursif. Donner une numérotation de $\mathbb{Q}$ revient à donner une numérotation de $\mathbb{Z} \times \mathbb{N}^+$ pour laquelle:
- (a) on sait numéroter en ordre croissant les fractions réduites, et :
- (b) on sait pour chaque fraction réduite le numéro qui lui est attribué.

$\mathbb{Q}$ est **PSPACE**-numérotable. Problème : $\mathbb{Q}$ est-il $\mathcal{P}$-numérotable ?

B) STRUCTURES ALGEBRIQUES COMPLETEMENT $\mathcal{P}$-CALCULABLES

a) Généralités sur les structures algébriques complètement $\mathcal{P}$-calculables et sur les structures naturellement c-$\mathcal{P}$-c

Structures algébriques complètement $\mathcal{C}$-calculables

Si X est une $\mathcal{C}$-structure algébrique , avec *un nombre fini* de lois de composition, on peut définir un $\mathcal{C}$-ensemble **Calc**(X) dont les éléments sont les écritures de calculs à effectuer dans cette $\mathcal{C}$-structure. Par exemple, dans le corps $\mathbb{Q}$:

(1/2 +1/(3/4 +1/(5 /(6 - 17/7)))) × (3/5 + 5/7 - 15 /(1+ 13/4))

Définition B.a1 :

On dira que la structure algébrique X est **complètement $\mathcal{C}$-calculable** si l'opération naturelle : "faisons la calcul indiqué" qui transforme un élément de **Calc**(X) en un élément de X ∪ {u} (union disjointe; u vaut pour "non défini") est une $\mathcal{C}$-opération[1].

Une $\mathcal{P}$-structure n'est pas nécessairement complètement $\mathcal{P}$-calculable, comme nous le verrons sur plusieurs exemples (les polynômes en présentation creuse, ou les réels algébriques en présentation naïve notamment). Cela tient à une possible explosion de la taille des objets lors des calculs successifs. On démontre par contre immédiatement.

Proposition B.a1 :

Pour qu'une $\mathcal{P}$-structure algébrique X soit complètement $\mathcal{P}$-calculable il faut et suffit que l'opération naturelle : "faisons la calcul indiqué" , de **Calc**(X) vers X ∪ {u} soit **RESP** (c.-à-d. polynomialement majorée en taille).

Toute $\mathcal{P}_0$-structure est complètement $\mathcal{P}_1$-calculable.

Toute $\mathbb{P}$r-structure est complètement $\mathbb{P}$r-calculable .

Remarque : Dans la plupart des exemples de $\mathcal{P}_0$-structures que nous étudions, on a en fait une majoration de la mesure de la sortie par la mesure de l'entrée (sans avoir à rajouter une constante), ce qui implique que la structure est en fait complètement $\mathcal{P}_0$-calculable.

Exemple : fractions continues dans $\mathbb{Q}$

Considérons **Lst**($\mathbb{Q}$) , $\mathcal{P}_0$-ensemble des listes d'éléments de $\mathbb{Q}$. On a une application "fraction continue" de **Lst**($\mathbb{Q}$) vers $\mathbb{Q}$ [2] , donnée par :

---

[1] On aurait une définition analogue pour une $\mathcal{C}$-structure algébrique impliquant plusieurs $\mathcal{C}$-ensembles. Par exemple avec 3 $\mathcal{C}$-ensembles X, Y, Z l'opération "faisons le calcul indiqué" a pour source l'ensemble **Calc**(X,Y,Z) analogue de **Calc**(X) , et pour but l'ensemble X ∪ Y ∪ Z ∪ {u} (union disjointe).

[2] En fait, cette application est définie sur des $\mathcal{P}$-parties convenables de **Lst**($\mathbb{Q}$) ; par exemple: tous les q_i sont > 0 à partir du 2ème.