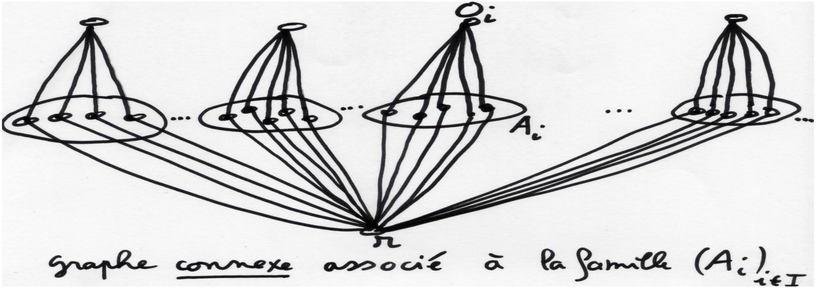
Formes linéaires et Axiomes de Choix Fini
Séminaire ERMIT

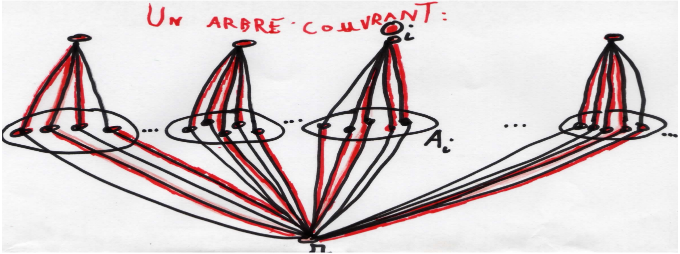
Marianne Morillon

26 février 2008

Théorème (Höft et Howard 1973, [6])

AC $\Leftrightarrow$ *"Tout graphe connexe contient un arbre couvrant."*

- 

- 

Bases et formes linéaires

Soit $\mathbb{K}$ un corps commutatif. Considérons les conséquences suivantes de l'Axiome du Choix (**AC**).

4 axiomes d'algèbre linéaire.

1. **D**($\mathbb{K}$): *Sur tout $\mathbb{K}$-espace vectoriel E non nul, il existe une forme linéaire $f : E \to \mathbb{K}$ non nulle.*
2. **DE**($\mathbb{K}$): *Pour tout $\mathbb{K}$-espace vectoriel E et tout $a \in E \setminus \{0\}$, il existe $f : E \to \mathbb{K}$ linéaire telle que $f(a) = 1$.*
3. **B**($\mathbb{K}$): *Tout $\mathbb{K}$-espace vectoriel admet une base.*
4. **BE**($\mathbb{K}$): *Pour tout $\mathbb{K}$-espace vectoriel E, tout système générateur G de E inclut une base.*

Bien sûr:

AC $\Rightarrow$ **BE**($\mathbb{K}$) $\Rightarrow$ **B**($\mathbb{K}$) $\Rightarrow$ **DE**($\mathbb{K}$) $\Rightarrow$ **D**($\mathbb{K}$).

Un autre équivalent de **AC**

Remarque historique

Halpern (66) [5]: $\forall \mathbb{K} \mathbf{BE}(\mathbb{K}) \Rightarrow \mathbf{AC}$.
Keremedis (96) [8]: $\mathbf{BE}(\mathbb{Z}_2) \Rightarrow \mathbf{AC}$.

Théorème (Howard 2007, [7])

Soit $\mathbb{K}$ *un corps commutatif. Alors* $\mathbf{AC} \Leftrightarrow \mathbf{BE}(\mathbb{K})$*.*

Proof.

Howard montre qu'avec $\mathbf{BE}(\mathbb{K})$, tout graphe connexe admet un arbre couvrant (voir page suivante). Ainsi $\mathbf{BE}(\mathbb{K})$ implique **AC** d'après le résultat précédent de Höft et Howard (1973) [6]. Pour d'autres équivalents de **AC** formulés en termes de graphes couvrants, voir Del. et Mor. (2006) [2]. $\square$

$\mathbf{BE}(\mathbb{K}) \Rightarrow \mathbf{AC}$: d'après la preuve de Howard

Soit $G := (V, E)$ le graphe connexe de la page 2, où V (*resp.* E) désigne l'ensemble des sommets (*resp.* arêtes) du graphe G. On identifie E à une partie de $\mathbb{K}^{(V)}$ comme suit: pour tout sommet $x \in A := \sqcup_{i \in I} A_i$, on identifie l'arête $e = \{r, x\}$ au vecteur $x - r$ de $\mathbb{K}^{(V)}$, et l'arête $e = \{x, O_i\}$ au vecteur $O_i - x$. On note W le sous-espace vectoriel de $\mathbb{K}^{(V)}$ engendré par l'ensemble des arêtes du graphe. Noter que l'espace W admet une base -dans **ZF**-. Avec $\mathbf{BE}(\mathbb{K})$, soit B une base de W, incluse dans E. Soit $i_0 \in I$; alors le vecteur $O_{i_0} - r$ de $\mathbb{K}^{(V)}$ appartient à W (car pour tout $x \in A_{i_0}$, $O_{i_0} - r = \{r, x\} + \{x, O_i\}$). Considérons la décomposition dans B de $O_{i_0} - r$:

$$O_{i_0} - r = \sum_{i \in I} \Big(\sum_{x \in A_i} \lambda_x (x - r) + \sum_{x \in A_i} \mu_x (O_i - x) \Big)$$

ici les λ_x, μ_x sont presque tous nuls, $\lambda_x = 0$ lorsque $x - r \notin B$, $\mu_x = 0$ lorsque $O_i - x \notin B$.

$\mathbf{BE}(\mathbb{K}) \Rightarrow \mathbf{AC}$: suite

On regroupe selon la base canonique de $\mathbb{K}^{(V)}$:

$$O_{i_0} - r = \sum_{x \in A} (\lambda_x - \mu_x).x + \sum_{i \in I} (\sum_{x \in A_i} \mu_x).O_i - (\sum_{x \in A} \lambda_x).r$$

L'ensemble $Z_{i_0} := \{x \in A_{i_0} : \lambda_x \neq 0\}$ est un singleton: en effet, pour tout $x \in A$, $\lambda_x = \mu_x$, et $\sum_{x \in A_{i_0}} \mu_x = 1$. Ces égalités montrent que Z_{i_0} est non vide. Si Z_{i_0} contenait au moins deux points distincts x, y, alors les 4 arêtes $\{r, x\}$, $\{x, O_{i_0}\}$, $\{O_{i_0}, y\}$ et $\{r, y\}$ appartiendraient à la base B de W: c'est contradictoire puisqu'elles forment un système lié.

Exemples d'axiomes de "choix fini"

3 axiomes de choix fini pour n entier ≥ 2:

1. **$\mathbf{AC}^n$**: *Toute famille $(A_i)_{i\in I}$ d'ensembles finis non vides ayant au plus n éléments a un produit non vide."*
2. **$\mathbf{AC}^n_{wo}$**: *Pour tout ordinal α et toute famille $(A_i)_{i\in\alpha}$ d'ensembles finis non vides ayant au plus n éléments, le produit $\prod_{i\in\alpha} A_i$ est non vide."*
3. **$\mathbf{PAC}^n$** (Partial **$\mathbf{AC}^n$**): *Pour toute suite $(A_n)_{n\in\mathbb{N}}$ d'ensembles finis non vides ayant au plus n élements, il existe une partie infinie I de $\mathbb{N}$ telle que $\prod_{i\in I} A_i$ est non vide.*

Un équivalent de **AC** dans **ZF** (voir Jech 73 [4])

MC ("Multiple Choice"): *Pour toute famille $(A_i)_{i\in I}$ d'ensembles non vides, il existe une famille $(F_i)_{i\in I}$ d'ensembles finis non vides tels que pour tout $i \in I$, $F_i \subseteq A_i$.*

Existe-t-il un corps $\mathbb{K}$ tel que $\mathbf{B}(\mathbb{K})$ implique **AC**?

Quelques faits connus à propos de $\mathbf{B}(\mathbb{K})$.

1. Blass 84 ([3]): $(\forall \mathbb{K} \mathbf{B}(\mathbb{K}) \Rightarrow \mathbf{MC})$ -d'où $(\forall \mathbb{K} \mathbf{B}(\mathbb{K}) \Rightarrow \mathbf{AC})$-.
2. Keremedis 01 ([9]): $\mathbf{B}(\mathbb{Q})$ implique $\forall n \in \mathbb{N}^* \mathbf{PAC}^n$.
3. Howard 07 ([7]): $\mathbf{B}(\mathbb{Z}_2)$ implique $\mathbf{AC}^2_{wo}$.

La question de savoir s'il existe un corps commutatif $\mathbb{K}$ tel que $\mathbf{B}(\mathbb{K})$ implique **AC** est (en février 2008) ouverte.

Quelle est la force de $\mathbf{B}(\mathbb{Z}_2)$?

Axiome $\mathbf{D}_{bool}$:

Sur toute algèbre de Boole (AB) non nulle (vue comme $\mathbb{Z}_2$-espace vectoriel), il existe une forme linéaire non nulle.

Axiome $\mathbf{C}(p)$ pour $p \in PRIME$:

Pour toute famille $(A_i)_{i\in I}$ d'ensembles finis non vides, il existe une famille $(F_i)_{i\in I}$ d'ensembles finis tels que pour tout $i \in I$, $F_i \subseteq A_i$, et p ne divise pas $|F_i|$.

Noter que $\mathbf{C}(2)$ implique $\mathbf{AC}^2$. On va renforcer légèrement le résultat précédent de Howard:

Théorème

1. Si $p \in PRIME$, alors $\mathbf{DE}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$.
2. $\mathbf{B}(\mathbb{Z}_2) \Rightarrow \mathbf{DE}(\mathbb{Z}_2) \Rightarrow \mathbf{D}(\mathbb{Z}_2) \Rightarrow \boxed{\mathbf{D}_{bool} \Rightarrow \mathbf{C}(2)} \Rightarrow \mathbf{AC}^2$.
3. $(\forall^{PRIME} p\ C(p)) \Rightarrow \forall^{\mathbb{N}} n \geq 2\ \mathbf{AC}^n$.

$\mathbf{DE}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$

Théorème

Soit $\mathbb{K}$ un corps commutatif. Les énoncés suivants sont équivalents:

1. $\mathbf{DE}(\mathbb{K})$
2. *La "version multiple" du précédent: "Si $(E_i)_{i \in I}$ est une famille de $\mathbb{K}$-espaces vectoriels, si $(a_i)_{i \in I}$ est une famille telle que pour tout $i \in I$, $a_i \in E_i \backslash \{0\}$, alors il existe une famille $(f_i)_{i \in I}$ telle que pour tout $i \in I$, $f_i : E_i \to \mathbb{K}$ est linéaire et $f_i(a_i) = 1$".*

Proof.

Utiliser le Lemme d'algèbre en page suivante. $\square$

Un Lemme pour passer aux formes multiples

Lemme

Etant donnée une famille $(E_i)_{i\in I}$ *de* $\mathbb{K}$-ev, *et une famille* $(a_i)_{i\in I}$ *telle que chaque* $a_i \in E_i \setminus \{0\}$, *il existe un* $\mathbb{K}$-ev E, *un* $a \in E \setminus \{0\}$, *et une famille* $(f_i : E_i \to E)_{i\in I}$ *de morphismes de* $\mathbb{K}$-ev *tels que pour tout* $i \in I$, $f_i(a_i) = a$.

Preuve. (J-P Aubry, voir [1].) Soit $F = \oplus_{i\in I} E_i$ la "somme directe" des E_i. Soit, pour tout $i \in I$, $j_i : E_i \to F$ l'injection canonique et $e_i := j_i(a_i)$. Soit R le *sev* de F engendré par les divers $e_i - e_j$, lorsque $i \neq j \in I$. Soit $\pi : F \to E := F/R$ le morphisme quotient et, pour tout $i \in I$, $f_i := \pi \circ j_i$. Tous les $f_i(a_i) = \pi(e_i)$ sont égaux à un même élément a de E. Il reste à voir que $a \neq 0$. Il suffit de trouver une forme linéaire nulle sur R mais non nulle en les e_i: considérer la forme "somme des coordonnées" sur le *sev* de F engendré par le système libre $\{e_i : i \in I\}$ de E.

$\mathbf{DE}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$: suite

Corollaire

$\mathbf{DE}(\mathbb{Z}_p) \Rightarrow \mathbf{C}(p)$.

Proof.

Soit $(A_i)_{i\in I}$ une famille d'ensembles finis non vides. Pour tout $i \in I$, soit E_i le $\mathbb{Z}_p$-espace vectoriel $\mathbb{K}^{A_i}$; on note aussi a_i l'élément 1_{A_i} de E_i. Soit, par la forme multiple de $\mathbf{DE}(\mathbb{Z}_p)$, une famille $(f_i)_{i\in I}$ telle que pour tout $i \in I$, $f_i : E_i \rightarrow \mathbb{Z}_p$ est linéaire et $f_i(a_i) = 1$. Alors $f_i(a_i) = \sum_{t\in\{0..p-1\}} t|F_i(t)|$, où, pour tout $i \in I$, et tout $t \in \{0..p-1\}$, $F_i(t) := \{x \in A_i : f_i(x) = t\}$. Si $i \in I$, il existe $t \in \{0..p-1\}$ tel que $|F_i(t)|$ n'est pas multiple de p -car p ne divise pas $1 = f_i(a_i)$-. Soit t_i le premier tel élément de $\{0..p-1\}$; alors $F_i := F_i(t_i)$ est une partie de A_i de cardinal non divisible par p. $\square$

$\mathbf{D}_{bool} \Rightarrow \mathbf{C}(2)$

Théorème

Les énoncés suivants sont équivalents à $\mathbf{D}_{bool}$:

1. *Pour toute AB $\mathcal{B}$ et tout $0 \neq a \in \mathcal{B}$, il existe $f : \mathcal{B} \to \mathbb{Z}_2$ linéaire tel que $f(a) = 1$.*
2. *"Si $(\mathcal{B}_i, a_i)_{i\in I}$ est une famille d'AB munies d'éléments non nuls, il existe une famille $(f_i)_{i\in I}$ telle que pour tout $i \in I$, $f_i : \mathcal{B}_i \to \mathbb{Z}_2$ est linéaire et $f_i(a_i) = 1$.*

Preuve. $\mathbf{D}_{bool} \Rightarrow 1$. L'application $x \mapsto x \wedge a$ de $\mathcal{B}$ sur $\mathcal{B}_a := \{x \in \mathcal{B} : x \leq a\}$ est un morphisme d'AB donc r est linéaire. On applique ensuite $\mathbf{D}_{bool}$ à l'AB $\mathcal{B}_a$. $1. \Rightarrow 2.$ Pour tout $i \in I$, l'application $r_i : x \mapsto x \wedge a_i$ est un morphisme d'AB de $\mathcal{B}_i$ sur l'AB $B_i' := \{x \in \mathcal{B}_i : x \leq a_i\}$. On applique ensuite 1) au *coproduit* $(\mathcal{B}, j_i : B_i' \to \mathcal{B})_i$ (voir page suivante) des AB $(B_i', a_i)_i$.

$\mathbf{D}_{bool} \Rightarrow \mathbf{C}(2)$:suite

Corollaire

$\mathbf{D}_{bool} \Rightarrow \mathbf{C}(2)$.

Preuve. Si $(A_i)_{i \in I}$ est une famille d'ensembles finis non vides, considérer pour tout i l'A.B. $\mathcal{B}_i := \mathcal{P}(A_i)$ et utiliser $\mathbf{D}_{bool}$.

Coproduit d'algèbres de Boole

Etant donnée une famille $(\mathcal{B}_i)_{i \in I}$ d'algèbres de Boole, il existe une algèbre de Boole $\mathcal{B}$ et une famille $(j_i : \mathcal{B}_i \rightarrow \mathcal{B})_{i \in I}$ de morphismes d'algèbres de Boole (avec $j_i(1) = 1$) tels que, pour toute alg. de Boole $\mathcal{C}$, et toute famille $(g_i : \mathcal{B}_i \rightarrow \mathcal{C})_{i \in I}$ de morphismes d'alg. de Boole, il existe un unique morphisme $g : \mathcal{B} \rightarrow \mathcal{C}$ tel que $g \circ j_i = g_i$.

Preuve. voir [11]. Ebauche: on traite d'abord le cas où les alg. $\mathcal{B}_i$ sont égales à $\mathcal{P}(\mathbb{N})$, puis celui ou elles sont sous-algèbre d'une puissance réduite de $\mathcal{P}(\omega)$ (ce qui est le cas général avec les méthodes décrites par Luxemburg 67 [10]).

$$\begin{tikzcd}
\mathcal{B} \arrow[dr, "g"] & \\
\mathcal{B}_i \arrow[u, "j_i"] \arrow[r, "g_i"] & \mathcal{C}
\end{tikzcd}$$

Annexe: $\left(\forall^{PRIME} p\ C(p)\right) \Rightarrow \forall^{\mathbb{N}} n \geq 2\ \mathbf{AC}^n$.

Soit n un entier ≥ 1 et $(A_i)_{i \in I}$ une famille d'ensembles non vides ayant chacun au plus n éléments. Soit $E := \cup_{i \in I} \mathcal{P}(A_i) \backslash \varnothing$: E est un ensembles de parties non vides ayant chacune au plus n éléments. On applique successivement chacun des axiome C_p, pour p premier $\leq n$; on en déduit une application $\phi : E \rightarrow E$ telle que pour tout $A \in E$, si $1 < |A|$ alors $\phi(A) \subsetneq A$, d'où une fonction de choix sur E et aussi pour la famille $(A_i)_{i \in I}$.

Axiome du choix fini

$\mathbf{AC}^{\mathbf{fin}}$: Toute famille d'ensembles finis non vides a un produit non vide.

Attention!

L'axiome $\forall n \in \mathbb{N}^* \mathbf{AC}^n$ n'implique pas $\mathbf{AC}^{\mathbf{fin}}$.

Références citées

1. J.P. Aubry, Communication personnelle.
2. Delhommé and Morillon, Spanning graphs and the axiom of choice, Reports on Mathematical Logic, 40, 2006, 165–180.
3. Blass, Andreas, Existence of bases implies the axiom of choice, Axiomatic set theory (Boulder, Colo., 1983), Contemp. Math., 31, 31–33, Amer. Math. Soc., 1984.
4. Jech, The Axiom of Choice, NHPC, 1973.
5. Halpern, James D., Bases in vector spaces and the axiom of choice, Proc. Amer. Math. Soc., 17, 1966, 670–673.
6. Höft, Hartmut and Howard, Paul, A graph theoretic equivalent to the axiom of choice, Zeitschrift für Mathematische Logik und Grundlagen der Mathematik, 19, 1973, 191.

Références citées: suite

7. Howard, Paul, Bases, spanning sets, and the axiom of choice, Mathematical Logic Quarterly, 53, 2007, 3, 247–254.
8. Keremedis, Kyriakos, Bases for vector spaces over the two-element field and the axiom of choice, Proc. Amer. Math. Soc., 124, 1996, 8, 2527–2531.
9. Keremedis, Kyriakos, The vector space Kinna-Wagner principle is equivalent to the axiom of choice, MLQ Math. Log. Q., 47, 2001, 2, 205–210.
10. Luxemburg, W.A.J., "Reduced powers of the real number system and equivalents of the Hahn- Banach extension theorem", Appl. Model Theory Algebra, Anal., Probab., Proc. Int. Sympos. Calif. Inst. Technol., 1969, 123-137.
11. Morillon, Algèbres de Boole mesurées et Axiome du choix, Séminaire U. Blaise Pascal, Clermont-Ferrand 1990.