Quelques éléments de géométrie et d’algèbre pour comprendre la nature d’un échantillonnage équilibré

Jean-Claude Deville
Laboratoire de Statistique d’enquête
OuStatPo
(Ouvroir de Statistique Potentielle)
deville@ensai.fr

Problème d'échantillonnage équilibré :

-un vecteur π de probabilités d'inclusion à l'intérieur de C , le N-cube

- N p-vecteurs x_k de total X

-une pxN matrice de contraintes A de plein rang dont les colonnes sont $a_k = x_k/\pi_k$.

Les contraintes à vérifier par un échantillon s s'écrivent $As=X=A\pi$.

L'intersection $K = C \cap (\pi + ker(A))$ (ensemble des probabilités d'inclusion admissibles) est un polytope (polyèdre convexe compact) de dimension $M=N-p$.

Un échantillonnage équilibré est exact : tous les sommets de K sont aussi des sommets de C (les échantillons équilibrés).

Cela revient à dire que l'algorithme du cube n'a jamais besoin de phase d'atterrissage.

Par suite tous les s-s' joignant deux sommets de K (les 'segments') , en particulier les arêtes, sont des éléments de $\mathbb{Z}^N$: leurs coordonnées valent $0, +1$ ou -1 .

Ces vecteurs engendrent un sous groupe G_K de $\mathbb{Z}^N$ contenu dans $ker(A)$ et qui est donc aussi un sous-groupe de G_A , ensemble des points de coordonnées entières de $ker(A)$.

Petite question : C'est quoi un sommet ? C'est quoi une arête ?

On a le résultat suivant :

Théorème Les propositions suivantes sont équivalentes :

(i) Le problème (A,π) est exact.

(ii) Toutes les *pxp* sous-matrices carrées de A de plein rang ont le même déterminant en valeur absolue.

(iii) $G_A = G_K$.

(iv) Il existe une *pxp* matrice inversible W telle que $WA = (I_p \quad B)$ où I_p est la matrice identité d'ordre p et B une $p\ x(N\text{-}p)$ matrice totalement unimodulaire.

Rappelons qu'une matrice est totalement unimodulaire si toutes ses sous-matrices carrées ont un déterminant qui vaut +1,0 ou -1, y compris celles de rang 1.

La communication donne, en première mondiale, les démonstrations de ces résultats assorties de quelques commentaires.

Positions relatives d'une variété linéaire de dimension M et du N-cube ($M \leq N$)

L'intersection K entre un plan affine et C le N-cube est un N-p polytope (polyèdre convexe compact).

Une q-face de C est definie par une partition of $U=[1,\ldots,N]$ en trois ensembles U_0 U_1 U_{ind} avec $card(U_{ind})=q$ tels que $s_k=0$ if $k \in U_0$, $s_k=1$ si $k \in U_1$ et $s_k \in]0,1[$ if $k \in U_{ind}$. Si $U_{ind} = \emptyset$ s est un sommet de C. Une p-face de C est dite de plein rang si la sous matrice carrée de A dont les colonnes sont dans U_{ind} est de plein rang p .On a les faits suivants :

- Une q-face ($q=0,1,..,M$) de K est contenue dans une $p+q$ face de C .

- En particulier il n'y a au plus qu'un sommet de K dans une p-face de plein rang de C.

- Inversement, pour tout sommet s de K, il existe une p-face de plein rang F_p de C telle que s soit le seul sommet de K dans F_p . Si s appartient à l'intérieur (relatif) de F_p , la p-face est unique et le problème inexact.

-Toute arête de K est incluse dans une ($p+1$)-face de rang p .

-Inversement, pour toute arête σ =[s,s'] de K il existe une $p+1$-face de C de rang p, F_{p+1} telle que σ soit la seule arête de K dans F_{p+1} . Une arête a au plus $p+1$ coordonnées non nulles formant son support. Une arête est un segment de K de minimal support minimal.

Toutes ces propriétés sont assez intuitives et faciles à démontrer. Dans la suite on les utilisera sans référence particulière.

On dira que la variété linéaire $\pi+L$ ($L=ker(A)$) et C sont en ‘en position générale’ si leur intersection est de dimension $M=dim(L)$; $\pi+L$ est ‘en position particulière’ (tangents) si l’intersection est de dimension $M' < M$. Dans ce cas π n’est pas intérieur à C.

Problème <u>exact</u> (les sommets de K sont des sommets de C) mais $(dim\ K)=M' < M=dim(L)$. On dira que le problème est '<u>exact dégénéré</u>'.

Il est facile de voir qu'alors $K=(s+L')\cap C$ avec L' sous-espace de dimension M'.

En prenant un supplémentaire L'' de L' dans L et une base dans chacun de ces deux sous-espace, soient g_i'' et g_j' , un point de L s'écrit $\sum_i t''_i\, g''_i + \sum_j t'_j\, g'_j$. Si nous ajoutons les contraintes $t''_i=0$ pour tout i on constate que le problème devient exact (non dégénéré !) avec une intersection de plein rang.

Dans nos conventions, le problème est toujours exact non dégénéré, bien que, au cours de l'application de l'algorithme du cube, le cas dégénéré apparaisse presque nécessairement. Les raisons de ce phénomène sont complètement élucidées, mais en dire plus dépasserait les ambitions de cet exposé. (voir l'exemple dans la suite).

Quelque groupes associés à un problème exact

Soit G_A le sous-groupe additif de $\mathbb{Z}^N \cap ker\,(A)$ des points ayant des coordonnées entières (dit points entiers).

Sans autre indication, il peut être réduit à 0, être partout dense dans certaines directions ou discret. Dans ce dernier cas c'est un **groupe libre** (généré par une famille de vecteurs) de **type fini** (les générateurs sont en nombre fini). Toutes les familles minimales de générateurs (qu'on appelle **bases**) ont alors le même cardinal qu'on appelle le **rang** du groupe et qui est égal à la dimension du sous-espace qui contient le sous-groupe. Les matrices de changement de base sont dite **unimodulaires**. Elles sont à coefficients entiers et de déterminant ± 1. Elles forment le groupe linéaire $GL(\mathbb{Z}^r)$ avec *r* rang du groupe.

Si le problème est exact, il contient tous les vecteurs de la forme *s*-*s'* où *s* et *s'* sont des sommets de *K*. Cet ensemble engendre un sous-groupe G_K de G_A lui-même engendré par les arêtes de *K* puisque les segments sont des sommes d'arêtes. Ces deux groupes vivent dans un *M*=*N*-*p* sous-espace de $\mathbb{R}^N$, sont de type fini et ont le même rang *M*.

On peut alors utiliser le théorème ‘de la base adaptée’ qui explicite de façon complète la nature des un sous-groupes d’un groupe libre de type fini. Il est d’abord évident qu’un tel sous-groupe est aussi libre de type fini ; tous les sous-groupes de $\mathbb{Z}^N$ sont donc libres et de type fini (=admettent des bases!) . De plus on a le :

<u>Théorème de la base adaptée</u> : Soient G_A un groupe libre de type fini de rang M et G_K un sous-groupe de G_A . Il existe une base $g_1 \ldots g_M$ de G_A et des entiers d_i avec d_i diviseur de d_{i+1} ($i=1$ to $M-1$) tels que les $d_i\, g_i$ forment une base de G_K .
Autrement dit on a :

$$G_A = \left\{\sum_{i=1}^{M} z_i g_i \ , z_i \in \sum_{i=1}^{M} z_i g_i \ , z_i \in \mathbb{Z}\ \right\}$$
$$\text{et } G_K = \left\{\sum_{i=1}^{M} d_i z_i g_i \ , z_i \in \sum_{i=1}^{M} z_i g_i \ , z_i \in \mathbb{Z}\ \right\}.$$

Les entiers d_i s’appellent les facteurs invariants de G_K dans G_A . Ils ne dépendent pas de la base adaptée particulière qu’on utilise.

<u>Remarque</u>: Le théorème marche aussi si le rang G_K est strictement inférieur à M. On n’a qu’à introduire des ‘facteurs invariants’ égaux à 0.

-Un premier exemple d'utilisation est:

Résultat 1: Tous les facteurs invariants de G_A dans $\mathbb{Z}^N$ valent 1. Par suite G_A admet des sous-groupes supplémentaires de rang p dans $\mathbb{Z}^N$.

Proof: By the adapted basis theorem, there exist a basis $h_1,\dots,h_p,g_1,\dots,g_M$ of $\mathbb{Z}^N$ and invariant factors d_i such that $G_A = \{\sum_{i=1}^{M} d_i z_i g_i\}$ } and $\mathbb{Z}^N = \{ \sum_{i=1}^{M} z_i g_i\}, z_i \in \mathbb{Z}$. If some $d_i>1, g_i$ does not belong to G_A . But this is impossible since the coordinates of g_i are integers. The h_i are a basis for a supplementary subgroup.

-On peut toujours supposer que A_0 , le 'west-*p*x*p* bloc' de A , est de plein rang (et, au besoin, que $det(A_0)$ à la valeur absolue maximum parmi les sous-matrices carrées de A). On a le :

Résultat 2: Soient e_i ,$i=1$ to N, la base canonique de $\mathbb{R}^N$ (or $\mathbb{Z}^N$!). Le sous groupe engendré par les e_i ,$i=1$ à p est un supplémentaire de G_A .

Proof: As A_0 is full rank, none of the e_i ,$i=1$ to p belong to $ker(A)$. The vector subspace spanned by those vectors is a supplementary of $ker(A)$. If we join an arbitrary basis of G_A to those p vectors we get an adapted basis.

Démonstration *(i)=>(iii)* : $G_A=G_K$ -De résultat 2, les vecteurs de base forment la matrice d'entiers $G = \begin{pmatrix} I_p & G_{pM} \\ 0 & G_{MM} \end{pmatrix}$ qui est donc unimodulaire ($\in GL(\mathbb{Z}^N)$).

-Comme $det(G)=det(G_{MM})=\pm 1$ G_{MM} est aussi unimodulaire ($\in GL(\mathbb{Z}^M)$).

- $G \times \begin{pmatrix} I_p & 0 \\ 0 & G_{MM}^{-1} \end{pmatrix} = G_I = \begin{pmatrix} I_p & B \\ 0 & I_M \end{pmatrix}$ nouvelle base adaptée de $\mathbb{Z}^N$, $B = G_{pM} G_{MM}^{-1}$.

-Forme standardisée de base de $\mathbb{Z}^N$ adaptée à G_A . Elle ne dépend fondamentalement que du choix des *p* premières colonnes de *A* formant une matrice de plein rang.
Dans cette base (qui est aussi une base de l'espace vectoriel $\mathbb{R}^N$!) la matrice de contraintes s'écrit $A = (I \quad -B)$ à la prémultiplication près d'une matrice de $GL(\mathbb{R}^N)$ (ou $GL(\mathbb{Z}^N)$!).

Résultat 3 :En particulier cette normalisation montre que les *p*-vecteurs b_k des variables d'équilibrage sont entiers, ce qui n'avait rien d'évident.

-Montrons maintenant que $G_A = G_K$. Tant que nous y sommes on va même faire un peu plus fort ! Soit s un sommet quelconque de K . On peut trouver M arêtes $\sigma_i = s_i - s$ de K 'partant' de s formant une base vectorielle de L. Soit G_σ le groupe libre des $\sum_1^M z_i\,\sigma_i$ et, par abus de notation, la matrice NxM des σ_i (dont les éléments sont des 0,1 ou -1). On a $G_\sigma \subset G_K \subset G_A$ les trois groupes étant de rang M .

Le théorème de la base adaptée permet d'exhiber une base h_i , $i=1$à M de G_A et des facteurs invariants $d_i \geq 1$ tels que les $d_i h_i$ forment une base de G_σ . On a $d_1 = 1$ sinon tous les éléments de G_σ auraient pour coordonnées des multiples de ce nombre et aucun des σ_i ne seraient dans G_σ . Soit I le nombre des facteurs invariants égaux à 1 ; on a :

$$G_\sigma = \bigoplus_1^I h_i\mathbb{Z} \;\oplus d_{I+1} \bigoplus_{\mathrm{I}+1}^M d'_i h_i\mathbb{Z} = G_1 \oplus d_{I+1} G_2 \quad \text{avec pour } i>I \text{ , } d_i = d_{I+1}\, d'_i \text{ .}$$

Appelons L_1 le sous espace vectoriel engendré par les h_i , $i=1$à I et L_2 son supplémentaire dans L engendré par les h_i , $i=I+1$ à M . G_1 est le groupe des entiers de L_1 (les h_i sont une base adaptée!) et $d_{I+1}G_2$ un sous-groupe des entiers de L_2 constitué d'éléments dont toutes les coordonnées sont des multiples de $d_{I+1}>1$. Aucune des arêtes σ_i n'appartient donc à ce sous-groupe et on a de ce fait $I=M$. ■

<u>Démonstration de *(iii)*=>*(iv)* : *B* telle que A=*(I ,–B)* est totalement unimodulaire.</u>

B_V^W sous matrice carrée de *B* indicée par un ensemble *V* de colonnes (= individus) et *W* de lignes (=contraintes). On peut la supposer en position 'nord- ouest' de *B.*

G_V sous-groupe de G_A engendré par les colonnes indicées par *V* n'est autre que le groupe des entiers du sous espace vectoriel L_V dont une base (vectorielle comme de groupe libre) est, avec un léger abus de notation, $G_V = \begin{pmatrix} B_V^W \\ \tilde{B} \\ J_q \end{pmatrix}$, avec $J_q = \binom{I_q}{0}$.

Supposons que $det(B_V^W) \neq 0$.

Le théorème de la base adaptée (encore lui!), nous exhibe deux qxq matrices unimodulaires B_{gV} et B_{dV} , et une matrice diagonale D de facteurs invariants pour le sous-groupe $Im(B_V^W) \subset \mathbb{Z}^q$ telle que : $B_V^W = B_{gV}\, D B_{dV}$.

On obtient ainsi une nouvelle base de G_V avec $G_{VD} = G_V B_{uV}^{-1} = \begin{pmatrix} D \\ B_{gV}^{-1}\, \tilde{B} B_{dV}^{-1} \\ B_{gV}^{-1}\, B_{dV}^{-1} \\ 0 \end{pmatrix}$.

Reste à voir que $D=I_q$ et, par suite, que $B_V^W = B_{gV}^{-1} B_{uV}^{-1}$.

Soit $\breve{b}_k = d_k e_k + \breve{b}_k$ la colonne indicée par k dans G_{VD} .

$G_V = \left\{\sum_{k \in V} z_k \left(d_k e_k + \breve{b}_k\right)\right\}, z_k \in \mathbb{Z}$.

Si $d_k > 1$ pour un certain k $e_k + \breve{b}_k$ est un point entier qui n'est pas dans G_V , une contradiction qui prouve que $B_V^W \in GL(\mathbb{Z}^q)$ c'est-à-dire que $det(B_V^W) = \pm 1$.

$(iv) \Longrightarrow (ii)$:Les sous-matrices carrées de plein rang ont le même déterminant

Si c'est une sous-matrice de B c'est le point précédent. Suppose that the full rank sub matrix A_0 has p-q columns coming from I_p and q coming from B. Permuting the lines we can write $A_0 = \begin{pmatrix} I_{p-q} & B_{p-q} \\ 0 & B_q \end{pmatrix}$ and $det(A_O) = det(B_q) = \pm 1$.

$(iii) \Longrightarrow (i)$: La réciproque.

Soit s_0 vérifiant $As_0=X$ et $\sigma = s_1 - s_0$ une arête de K . L'ensemble V des coordonnées non nulles de σ a au plus $p+1$ éléments ;l'une d'entre elles, disons k, vérifie $\sigma_k = \pm 1$. Complétons, au besoin, la sous-matrice $A_{V\text{-}k}$ par d'autres colonnes de A pour obtenir une sous-matrice de plein rang A^* et $\sigma_{V\text{-}k}$ en σ^* en ajoutant des zéros pour les nouvelles coordonnées. Par construction on a $A^*\sigma^* = \sigma_k a_k$. Les coordonnées de σ^* sont données par les formules de Cramer et valent donc 0 ou $= \pm 1$ par hypothèse ; s_1 est donc un sommet de C.

Le même argument s'applique à toute paire de sommets adjacent de K : tout sommet de K adjacent à un 'échantillon' est aussi un échantillon et le problème est exact.

Et voila le travail.

Quelques compléments.

Corollaire: Si le problème est exact le résultat (*iv*) prouve que les contraintes peuvent s'écrire à l'aide d'une matrice dont les éléments valent uniquement 0 , +1 or -1.

Malheureusement, cette condition n'est pas suffisante. Voici le contrexemple minimal et typique:

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & -1 & 1 \end{pmatrix} \quad ker(A) \text{ est généré par } \begin{pmatrix} 1 & 0 & -1/2 & -1/2 \\ 0 & 1 & +1/2 & -1/2 \end{pmatrix},$$

Vous pouvez essayer tous les seconds membres, c'est toujours inexact (des solutions avec des ½) où dégénéré.

Par exemple avec $X = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ K est le triangle de $\mathbb{R}^4$ de sommets : $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1/2 & 0 & 0 \\ 1/2 & 0 & 1 \end{pmatrix}$.

-De façon générale, on peut montrer, toujours avec une base adaptée, la chose suivante : si le problème est non-exact entier, le groupe $m_* G_K$ est un sous-groupe strict de G_A , avec m p.p.c.m des déterminants des matrices de plein rang. Dans le cas de l'exemple, une base de L

est : $\begin{pmatrix} 2 & 1 \\ 0 & 1 \\ -1 & 0 \\ -1 & -1 \end{pmatrix}$, $m = 2$ et $m_* G_K = \begin{pmatrix} 2 \\ 0 \\ -1 \\ -1 \end{pmatrix} \mathbb{Z} \oplus 2 \begin{pmatrix} 1 \\ 1 \\ 0 \\ -1 \end{pmatrix} \mathbb{Z}$.

--Voici un autre exemple laissé vos méditations. C'est le cas quasiment général et minimal du cas où il y a trois contraintes :

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Tout ajout d'une colonne autre que les six ci-dessus conduit à un problème inexact. Les problèmes exacts à trois contraintes ont au plus six colonnes distinctes et sont isomorphes. Généralisations ?
Que se passe-t-il quand on supprime une des trois dernières colonnes ? (Ca dégénère comment ?)

-Le théorème utilise des propriétés du noyau de la matrice de contraintes indépendamment de la valeur de ces contraintes. Certaines d'entre elles conduisent à un problème exact de plein rang, les autres à un problème dégénéré.

-Du coup on peut dire que $\forall A\ \exists s_0 : As = As_0$ est exact mais parfois dégénéré (c'est en fait ce que contient la dernière démonstration), mais qu'il existe toujours quand M>1 au moins un cas exact.

-L'exactitude permet de parler de plan conditionnel à une (matrice de) contraintes. Pour le cas Poissonnien voir mon exposé de Dijon au colloque francophone.

-L'étude de l'espace image $=\{As, s \in C\}$ révèle l'existence de 'bulles' dans le cas entier non-exact. L'étude approfondie de cet ensemble est passionnante mais dépasse le cadre de cet exposé, bien que son absence le rende quelque peu mystificateur.

-Les arêtes de K sont les éléments de support minimal de G_A . Leur classification selon ce critère mérite une attention certaine.

etc….

Une conclusion.

La compréhension de ce qu'est un problème équilibré exact aura été longue, trop longue… En particulier ce qui se passe quand ça dégénère m'a causé quelques angoisses capillomortifères. La raison principale vient des illusions d'optique dues au fait que '2+1=3' fausse beaucoup l'intuition géométrique venant de l'espace ordinaire, et que ce n'est pas facile d'en sortir.

Post Scriptomme : Je ne suis pas le premier à qui ça arrive. Je viens juste de trouver dans un bouquin d'histoire des maths* la savoureuse phrase suivante : *Gauss avait su se libérer de l'« apriorisme » kantien qui régnait sans partage ; certains propos que l'on rapporte de lui indiquent, en outre, qu'il s'était tout aussi bien affranchi de la prétendue nécessité de l'espace à trois dimensions, qu'il considérait à juste titre comme une infirmité de l'esprit humain.*

*Amy Dahan-Dalmedico et Jeanne Peiffer, *Une histoire des mathématiques, routes et dédales,* Seuil , Coll. Points Sciences

Et merci pour cet instant.