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

Jean-Claude Deville

Laboratoire de Statistique d'enquête

deville@ensai.fr

Un problème d'échantillonnage équilibré a pour paramètres un vecteur π de probabilités d'inclusion à l'intérieur de C , le N-cube, N p-vecteurs x_k de total X et la pxN matrice de contraintes A de plein rang dont les colonnes sont $a_k = x_k/\pi_k$.

Les contraintes que doivent vérifier un échantillon s s'écrivent donc $As=X=A\pi$. L'intersection $K = C \cap (\pi + ker(A))$ (ensemble des probabilités d'inclusion admissibles) est un polytope convexe compact de dimension $M=N-p$ puisque π est à l'intérieur de C.

Un échantillonnage équilibré est exact si tous les sommets du polytope K sont aussi des sommets de C. Cela revient à dire que l'algorithme du cube n'a jamais besoin de phase d'atterrissage.
L'exactitude du problème se traduit par le fait que les sommets de K sont aussi des sommets de C (les échantillons équilibrés). 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)*.

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 $p\ x(N-p)$ 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.

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 ($M \leq N$)

D'abord quelques faits sur l'intersection K entre un plan affine et C le N-cube. C'est un N-p polytope (polyèdre convexe compact).

Une q-face de C est definie par une partition of $U=[1,...,N]$ 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 is contenue dans une $p+q$ face de C c'est-à-dire un $(p+q)$ cube.

- 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 is incluse dans une $(p+1)$-face de rang p .

-Inversement, pour toute arête $\sigma=[s,s']$ 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 utilisera sans référence les propriétés qui viennent d'être énumérée.

On dira que la variété linéaire $\pi+L$ ($L=ker(A)$) et C sont en 'en position générale' si leur intersection est de dimension $M=dim(L)$ et qu'aucune colonne de A n'est nulle. L est 'en position particulière' si certaines colonnes de A sont nulles : L contient le sous espace généré par les coordonnées de ces colonnes.
L est en position générale si et seulement si il existe un vecteur x de L dont aucune coordonnée n'est nulle. On en déduit, en effet, qu'il existe un sommet du cube s tel que $s+tx$ (t réel positif) est intérieur à $K_s = (s+L) \cap C$ qui est donc de dimension M.
Dans nos conventions, c'est toujours le cas car nous éliminons les probabilités d'inclusion égales à 0 ou 1 (ce qui se produit implicitement dans l'algorithme du cube).

En toute généralité il peut se faire que le problème soit exact (les sommets de K sont des sommets de C) mais que $(dim\ K)=M' < M=dim(L)$. On dira que le problème est 'exact dégénéré'. 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.

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). It contains all the elements of the form *s-s'* where *s* and *s'* are vertices of *K*. This set generate a subgroup G_K of G_A . It is itself generated by the edge of *K* since any segment is a sum of edges. As these two groups lye in a *M=N-p* dimensional subspace of $\mathbb{R}^N$ they are of finite type and have the same rank *M*. This means that each of them admit a basis of *M* elements $g_1 \ldots g_M$ such that the group is exactly the set of $\sum_{i=1}^{M} z_i g_i \ , z_i \in \mathbb{Z}$.

Moreover (theorem of the adapted basis), there exist a basis $g_1 \ldots g_M$ and integers d_i such that d_i divide d_{i+1} (*i=1* to *M-1*) such that:
$G_A = \{\sum_{i=1}^{M} z_i g_i \ , z_i \in \sum_{i=1}^{M} z_i g_i \ , z_i \in \mathbb{Z} \}$ and $G_K = \{\sum_{i=1}^{M} d_i z_i g_i \ , z_i \in \sum_{i=1}^{M} z_i g_i \ , z_i \in \mathbb{Z} \}$.

The integers d_i are the invariant factors of G_K in G_A . They do not depend of the particular adapted basis.

Remark: The theorem holds also if the rank of the smaller group is strictly inferior to M. One has only to introduce 'invariant factors ' equal to 0.

An example can be given in the following result:

Résultat 1: All invariant factors of G_A in $\mathbb{Z}^N$ are equal to 1. Therefore G_A admit supplementary subgroups of rank *p* in $\mathbb{Z}^N$.
Proof: By the adapted basis theorem, there exist a basis $h_1,\ldots,h_p,g_1,\ldots,g_M$ 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.

Assume that A_0 , the 'west-*pxp* block'of *A* , it is of full rank (and eventually that $det(A_0)$ takes the maximum absolute value among the full rank square matrixes we can extract from *A*). It does not change the generality of the proof.

Résultat 2: Let e_i ,*i=1* to *N*, denote the canonical basis of $\mathbb{R}^N$ (or $\mathbb{Z}^N$!).The subgroups generated by the e_i ,*i=1* to *p* is supplementary to 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.

Nous allons faire un usage intensif de ce théorème qu'on peut trouver dans tous les bons bouquins d'algèbre (je continue d'aimer beaucoup celui de Godement - où il figure en exercice – et pas seulement à cause des exercices sur la logique nazi(e ?)).

Démonstration *(i)=>(iii)* : G_A=G_K

Le résultat 2 peut se réécrire en rangeant les vecteurs de base dans la matrice d'entiers $G = \begin{pmatrix} I_p & G_{pM} \\ 0 & G_{MM} \end{pmatrix}$ qui est donc unimodulaire (elle appartient à $GL(\mathbb{Z}^N)$). Comme $det(G)=det(G_M)=\pm 1$ la sous-matrice G_M est également unimodulaire (elle appartient à $GL(\mathbb{Z}^M)$). En multipliant G par $\begin{pmatrix} I_p & 0 \\ 0 & G_{MM}^{-1} \end{pmatrix}$ on obtient une nouvelle base adaptée de $\mathbb{Z}^N$, $G_I = \begin{pmatrix} I_p & B \\ 0 & I_M \end{pmatrix}$, avec $B = G_{pM}G_{MM}^{-1}$. On peut la voir comme une 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 σ_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 $G_\sigma = \bigoplus_1^I h_i\mathbb{Z} \ \oplus d_{I+1} \bigoplus_{I+1}^M d'_i h_i\mathbb{Z} = G_1 \oplus d_{I+1}G_2$ avec pour $i>I$, $d_i=d_{I+1}\,d'_i$.

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 $I=M$ ce qui termine la démonstration de cette partie.

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

Soit B_V^W une sous matrice carrée de *B* indicée par un ensemble *V* de colonnes (= individus) et *W* de lignes (=contraintes). Quitte à permuter des lignes et des colonnes (ce qui revient à des multiplications ad hoc par des matrices de permutation, donc unimodulaires), on supposera que cette sous-matrice occupe la position 'nord- ouest' de *B*.

Appelons G_V le sous-groupe de G_A engendré par les colonnes indicées par *V*. Ce 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 $J_q = \begin{pmatrix} I_q \\ 0 \end{pmatrix}$. Supposons que $det(B_V^W) \neq 0$.

Le théorème de la base adaptée (encore lui!), nous exhibe deux *q*x*q* 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 : $B_V^W = B_{gV}\, DB_{dV}$. 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 $\check{b}_k = d_k e_k + \widetilde{b_k}$ la colonne indicée par *k* dans G_{VD}. $G_V = \left\{\sum_{k\in V} z_k \left(d_k e_k + \widetilde{b_k}\right)\right\}, z_k \in \mathbb{Z}$. Si $d_k > 1$ pour un certain *k* $e_k + \widetilde{b_k}$ 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 au signe près.

In the normalized form of the constraints a full rank sub matrix of *B* has its determinant equal to ± 1. 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 $det(A_O) = det(B_q) = \pm 1$.

Et pour finir : $(ii) \Longrightarrow (i)$

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

Let s_0 such that $As_0 = X$ and $\sigma = s_1 - s_0$ an edge of *K*. The set *V* of nonzero coordinates of σ has at most *p+1* elements and one of them, say *k*, is such that $\sigma_k = \pm 1$. Complete, eventually, the sub matrix of *A* with column in *V-k* to a full rank sub matrix A^* and σ_{V-k} to σ^* by adding zero for the new coordinates. By construction we have $A^*\sigma^* = \sigma_k a_k$. The coordinates of σ^* are given by the Cramer rules and are therefore equal to 0 or $= \pm 1$ since all full rank sub matrices of *A* have the same absolute value. So s_1 is a vertex of the *N*-cube *C*.

The same argument applies for any pair of adjacent vertices of *K*. Therefore any vertex of *K* adjacent to a'sample' is also a sample. As the set of edges is connected, any extreme point of *K* is a vertex of *C* and the problem is 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:

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

Pour $\underline{n} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ le polytope K est le triangle of $\mathbb{R}^4$ de sommets : $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1/2 & 0 & 1 \\ 1/2 & 0 & 0 \end{pmatrix}$.

For $\underline{n}=\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ c'est le triangle de $\mathbb{R}^4$ de sommets : $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1/2 & 0 & 0 \\ 1/2 & 0 & 1 \end{pmatrix}$.

Pour $\underline{n}=\begin{pmatrix} 2 \\ 0 \end{pmatrix}$ it is the the triangle of $\mathbb{R}^4$ whose summits are: $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1/2 & 1 & 1 \\ 1/2 & 0 & 1 \end{pmatrix}$.

For $\underline{n}= \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ it is the the triangle of $\mathbb{R}^4$ whose summits are: $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1/2 & 1 & 0 \\ 1/2 & 1 & 1 \end{pmatrix}$.

Pour toute autre valeur de $\underline{n}$, K est vide ou réduit à un unique point.
On voit bien que certaines arêtes ne sont pas entières.
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

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

--Voici un autre exemple laissé à la méditation du lecteur. 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 ?)

-On remarquera que le théorème utilise des propriétés du noyau de la matrice des 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 (ou sans solution, ce qui est un cas extrême de dégénérescence !).

-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. Dans le cas Poissonnien ça se calcule de façon raisonnablement simple (voir mon exposé à 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…

Quelques commentaires et con clusion.

J'ai passé presque quinze années de ma vie (pas à temps plein !) à étudier cette histoire d'exactitude à cause du référé d'une revue qui m'interdisait de parler d'échantillonnage équilibré tant que je ne saurais pas dire quand c'est possible. Je tiens à le remercier chaleureusement de m'avoir poussé à cette recherche, qui, à ce jour, aura été la plus excitante de mon existence.

La compréhension de ce qui se passe quand les données d'exactitude dégénèrent aura été longue, trop longue…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.*

References:

Deville, J.-C., Tillé, Y.,(2004) : Efficient balanced sampling: The cube method, *Biometrika*, vol 91, pp 893-912.
Présente la problématique de l'exactitude et l'algorithme du cube.

Ziegler,G,M (1995) : Lectures on polytopes, *Springer*.
Une bible sur les polytopes convexes.

Ziegler G.M. (2000): Lectures on 0-1-polytopes. In G. Kalai and G.M. Ziegler, editors, Polytopes: Combinatorics and Computation, volume 29 of DMV Seminars, pages 1–41.Birkhauser-verlag, Basel, 2000.
Quelques compléments à la référence précédente.

Godement R. (1964) : *Cours d'Algèbre*, Hermann, 1964
Dans le genre, voir aussi Bourbaki, *Algèbre, Chapitre VII*.

Kruskal J.B., Hoffman A.J.(1957): Integral Boundary Points of Convex Polyhedra, *Linear Inequalities and Related Systems*, H. W. Kuhn and A. W. Tucker (editors), Princeton University Press, Princeton, New Jersey, pp. 223-246, Study No. 38 of the Princeton Annals of Mathematics.
Dans un contexte différent (la programmation linéaire en nombres entiers) et avec des hypothèses plus restrictives, une apparition historique des matrices totalement unimodulaires en statistique.