Une caractérisation des lois de Wishart réelles par les formes quadratiques

Gabriel Fraisse† et Sylvie Viguier-Pla‡
† *Université de Perpignan, IUT, Domaine d'Auriac, Carcassonne*
‡ *Laboratoire de Statistique et Probabilités, Université Paul Sabatier, Toulouse*
courriel : gabriel.fraisse@laposte.net, sylvie.viguier-pla@math.univ-toulouse.fr

Résumé

Soient k un entier strictement positif et Σ une $p-$matrice réelle symétrique semi-définie positive. Soit M une $p-$matrice réelle aléatoire symétrique. On suppose que pour tout a de $\mathbb{R}^p$, si $a^*\Sigma a \neq 0$ alors la loi de $\frac{a^*Ma}{a^*\Sigma a}$ est de khi$-$deux à k degrés de liberté, et si $a^*\Sigma a = 0$, alors $a^*Ma = 0$.

On sait que M obéit à la loi de Wishart $W(k, \Sigma)$ si, et seulement si, pour toute $p-$base $\Sigma-$orthogonale $(a_1, \dots, a_p)$, les variables aléatoires (v.a.) $a_1^*M\, a_1, \dots, a_p^*M\, a_p$ sont indépendantes. Nous nous proposons d'affaiblir cette caractérisation en montrant que si, pour toute $(k+1)-$famille $\Sigma-$orthogonale de $p-$vecteurs $(a_1, \dots, a_{k+1})$, les v.a. $a_1^*M\, a_1, \dots, a_{k+1}^*M\, a_{k+1}$ sont indépendantes, alors $\mathcal{L}(M) = W(k, \Sigma)$.

Abstract

A characterization of the real Wishart distribution by quadratic forms. Let k be a strictly positive integer and Σ a real symmetric semi-definite positive $p-$matrix. Let M be a random symmetric $p-$matrix. We suppose that for all a of $\mathbb{R}^p$, if $a^*\Sigma a \neq 0$ then the distribution of $\frac{a^*Ma}{a^*\Sigma a}$ is of chi$-$square with k degrees of freedom, and if $a^*\Sigma a = 0$, then $a^*Ma = 0$.

We know that M is of Wishart distribution $W(k, \Sigma)$ if, and only if, for any $\Sigma-$orthogonal $p-$base $(a_1, \dots, a_p)$, the random variables (r.v.'s) $a_1^*M\, a_1, \dots, a_p^*M\, a_p$ are independent. We suggest to weaken this characterisation showing that if, for any $\Sigma-$orthogonal $(k+1)-$familly of $p-$vectors $(a_1, \dots, a_{k+1})$, the r.v.'s $a_1^*M\, a_1, \dots, a_{k+1}^*M\, a_{k+1}$ are independent, then $\mathcal{L}(M) = W(k, \Sigma)$.

1 Présentation

De façon classique, on définit la loi de Wishart comme suit :

Définition 1. Soit X une $(k, p)-$matrice aléatoire dont les k lignes sont gaussiennes, centrées, identiquement distribuées, indépendantes, de matrice de covariance Σ. Alors la loi de X^*X est dite loi de Wishart de paramètres k et Σ, et est notée $W(k, \Sigma)$.

La caractérisation des matrices de loi de Wishart par les formes quadratiques constitue une part importante de l'étude de ces lois (voir par exemple Masaro et Wong, [3]). Une matrice aléatoire de loi de Wishart ainsi définie possède des propriétés bien connues ([1]) :

Propriété 1. Soit M une $p-$matrice aléatoire réelle de loi de Wishart $W(k, \Sigma)$. Alors on a :
pour tout $p-$vecteur a tel que $a^*\Sigma\, a = 0$, on a $a^*Ma = 0$;
pour tout $p-$vecteur a tel que $a^*\Sigma\, a = 1$, on a $\mathcal{L}(a^*Ma) = \chi^2(k)$;
pour toute $p-$base $\Sigma-$orthogonale $(a_1, \dots, a_p)$ de $\mathbb{R}^p$, les variables aléatoires (v.a.) $a_1^*M\, a_1, \dots,$ $a_p^*M\, a_p$ sont indépendantes.

Ces propriétés caractérisent la loi de Wishart puisqu'elles déterminent sa fonction caractéristique (cf. propriété 23 de l'annexe 1).

La matrice Σ est appelée paramètre d'échelle, et k le degré de liberté (d.d.l.) de la loi de Wishart.

Nous allons montrer qu'il n'est pas nécessaire de considérer une base $(a_1, \ldots, a_p)$ de $\mathbb{R}^p$, mais seulement, une famille $(a_1, \ldots, a_k, a_{k+1})$ de $k+1$ vecteurs $\Sigma-$orthogonaux de $\mathbb{R}^p$.

Pour $p = 2$, cette propriété est vraie.

Pour $p > 2$, il suffira de l'établir pour $\Sigma = I_p$. En effet, si rang$(\Sigma) < p$, on va supposer que c'est vrai par hypothèse de récurrence.

Puis, pour Σ de rang p, comme on peut écrire $\Sigma = A^*A$, avec rang$(A) = p$, on remplacera M par $A^{-1*}MA^{-1}$. Par la suite il suffira donc de travailler avec $\Sigma = I_p$.

Dans une première partie, nous examinerons la loi de Wishart $W(1, I_p)$, avec au préalable le rappel de quelques propriétés de la loi uniforme sur $\{-1, 1\}$, la sphère unité de $\mathbb{R}$.

Dans un deuxième temps, pour généraliser, nous aborderons quelques aspects des $k-$isométries aléatoires.

C'est enfin avec ces outils que, dans une troisième partie, nous donnerons une caractérisation de la loi de Wishart $W(k, I_p)$.

2 Loi de Wishart à 1 degré de liberté

2.1 La loi uniforme sur $\mathcal{S}_1 = \{-1, 1\}$: $\mathcal{U}(\mathcal{S}_1)$

Propriété 2. Si U est une v.a. à valeurs dans $\mathcal{S}_1$, alors $\mathcal{L}(U) = \mathcal{U}(\mathcal{S}_1) \Leftrightarrow \mathcal{L}(U) = \mathcal{L}(-U)$.

Lemme 1. Soit A une partie de $\mathbb{R}^p$, et X une v.a. à valeurs dans A. Soit Y un $q-$vecteur aléatoire indépendant de X. Si f est une fonction continue de $\mathbb{R}^{p+q}$ dans $\mathbb{R}^r$ et $\mathcal{M}$ est une loi de probabilité sur $\mathbb{R}^r$ telles que, $\forall a \in A$, $\mathcal{L}(f(a, Y)) = \mathcal{M}$, alors $\mathcal{L}(f(X, Y)) = \mathcal{M}$.

Preuve. Puisque X et Y sont indépendantes, $\forall a \in A$, $\mathcal{L}(f(X, Y)/X = a) = \mathcal{L}(f(a, Y))$, ce qui prouve le lemme. □

Propriété 3. Soient U une v.a. à valeurs dans $\mathcal{S}_1$ et U_1, U_2, …, U_p des v.a. de loi $\mathcal{U}(\mathcal{S}_1)$. On suppose l'indépendance de U, U_1, U_2, …, U_p.

Alors $\mathcal{L}(UU_i) = \mathcal{U}(\mathcal{S}_1)$ et U, UU_1, UU_2, …, UU_p sont indépendantes.

Preuve. Pour tout a de $\mathcal{S}_1$, le $p-$uplet $(aU_1, \ldots, aU_p)$ est fait de v.a. indépendantes uniformes sur $\mathcal{S}_1$. D'après le lemme 1, le $p-$uplet $(UU_1, \ldots, UU_p)$ est aussi fait de v.a. indépendantes uniformes sur $\mathcal{S}_1$.

Enfin, comme pour tout $(a, b) \in \mathcal{S}_1^2$, $\mathcal{L}((UU_1, \ldots, UU_p)/U = a) = \mathcal{L}((UU_1, \ldots, UU_p)/U = b)$, U est indépendante de $(UU_1, \ldots, UU_p)$. □

Remarque. Tout produit de deux v.a. indépendantes uniformes sur $\mathcal{S}_1$ est uniforme sur $\mathcal{S}_1$ et indépendant de chacune.

Propriété 4. Soit X une v.a. réelle telle que $\mathcal{L}(X) = \mathcal{L}(-X)$ et $p(X = 0) = 0$. Alors $\mathcal{L}(\frac{X}{|X|}) = \mathcal{U}(\mathcal{S}_1)$, et $|X|$ et $\frac{X}{|X|}$ sont indépendantes.

Preuve. Soit $U = \frac{X}{|X|}$. Cette v.a. U est à valeurs dans $\mathcal{S}_1$ et $\mathcal{L}(U) = \mathcal{L}(-U)$, d'où $\mathcal{L}(U) = \mathcal{U}(\mathcal{S}_1)$.

De plus, $\mathcal{L}(|X|/U = 1) = \mathcal{L}(X/X > 0) = \mathcal{L}(-X/-X > 0) = \mathcal{L}(-X/X < 0) = \mathcal{L}(|X|/U = -1)$, ce qui prouve l'indépendance entre $|X|$ et U. □

Remarque. Si X est une v.a. vérifiant les conditions de la propriété 4, si, de plus, K et U sont deux v.a. indépendantes telles que $\mathcal{L}(K) = \mathcal{L}(X^2)$ et $\mathcal{L}(U) = \mathcal{U}(\mathcal{S}_1)$, alors $\mathcal{L}(\sqrt{K}U) = \mathcal{L}(X)$.

Corollaire 1. Dans le cas particulier où X est de loi normale centrée réduite $\mathcal{N}(0, 1)$, on a : $\mathcal{L}(X^2) = \chi^2(1)$, $\mathcal{L}(\frac{X}{|X|}) = \mathcal{U}(\mathcal{S}_1)$ et $|X|$ et $\frac{X}{|X|}$ sont indépendantes. Réciproquement, si K et U sont deux v.a. indépendantes telles que $\mathcal{L}(K) = \chi^2(1)$ et $\mathcal{L}(U) = \mathcal{U}(\mathcal{S}_1)$, alors $\mathcal{L}(\sqrt{K}U) = \mathcal{N}(0, 1)$.

2.2 La loi de Wishart à 1 degré de liberté $\mathcal{W}(1, I_p)$

Définition 2. Soit X un vecteur gaussien centré tel que $E(XX^*) = I_p$. La loi de Wishart $\mathcal{W}(1, I_p)$ est la loi de probabilité de XX^*.

Lemme 2. Soient X un vecteur aléatoire à valeurs dans $\mathbb{R}^p$ et U une v.a. à valeurs dans $\mathcal{S}_1$. On a : $XX^* = (UX).(UX)^*$.

Remarque. Le fait que $\mathcal{L}(XX^*) = \mathcal{W}(1, I_p)$ n'implique pas forcément $\mathcal{L}(X) = \mathcal{N}(0, I_p)$, même si les coordonnées de X sont de loi $\mathcal{N}(0, I_p)$. En effet, soient, pour $1 \leq i \leq 3$, U_i et K_i des v.a. indépendantes telles que $\mathcal{L}(U_i) = \mathcal{U}(\mathcal{S}_1)$ et $\mathcal{L}(K_i) = \chi^2(1)$. De plus, posons, pour $1 \leq j \leq 3$,

$1 \leq k \leq 3$, $i \neq j$, $i \neq k$, $j \neq k$, $X_i = \sqrt{K_i} U_j U_k$, et X le vecteur aléatoire dont les composantes sont les X_i. Comme $\mathcal{L}(U_1 U_2 U_3 X) = \mathcal{N}(0, I_3)$, on a bien $\mathcal{L}(X_i) = \mathcal{N}(0,1)$. Donc $\mathcal{L}(XX^*) = \mathcal{W}(1, I_3)$, mais $\mathcal{L}(X) \neq \mathcal{N}(0, I_3)$, car les X_i sont liées par leurs signes.

De manière générale, lorsqu'on est en présence d'une matrice aléatoire XX^* de loi de Wishart à 1 d.d.l., les vecteurs aléatoires X qui composent cette forme XX^* ne sont pas forcément de loi gaussienne. Ils sont définis à une v.a. U multiplicative à valeurs dans $\mathcal{S}_1$ près.

On note $\mathcal{S}_p$ la sphère unité de $\mathbb{R}^p$, c'est-à-dire l'ensemble des $p-$vecteurs de norme 1.

Par la suite, on posera M une $p-$matrice aléatoire symétrique. On fait l'hypothèse suivante : pour tout $(a,b) \in \mathcal{S}_p^2$, $\mathcal{L}(a^* M a) = \mathcal{L}(b^* M b) = \chi^2(1)$ et que, si $a^* b = 0$, alors $a^* M a$ et $b^* M b$ sont indépendantes.
Alors on a les propriétés qui suivent.

Propriété 5. Pour tout $(a,b) \in \mathcal{S}_p^2$, $a^* b = 0 \Rightarrow \mathcal{L}((a,b)^* M (a,b)) = \mathcal{W}(1, I_2)$.

Preuve. Soit (a,b) un couple de $p-$vecteurs unitaires orthogonaux, c'est-à-dire tel que $(a|b)^*(a|b) = I_2$. Pour tout couple $(\binom{\alpha_1}{\beta_1}, \binom{\alpha_2}{\beta_2})$ de 2−vecteurs unitaires orthogonaux, c'est-à-dire pour toute 2−isométrie $\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}$, les $p-$vecteurs $(a|b)\binom{\alpha_1}{\beta_1}$ et $(a|b)\binom{\alpha_2}{\beta_2}$ sont unitaires et orthogonaux car :

$$\left((a|b)\binom{\alpha_1}{\beta_1} | (a|b)\binom{\alpha_2}{\beta_2}\right)^* \left((a|b)\binom{\alpha_1}{\beta_1} | (a|b)\binom{\alpha_2}{\beta_2}\right) = \left((a|b)\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}\right)^* \left((a|b)\begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}\right)$$
$$= \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}^* (a|b)^*(a|b) \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}^* \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} = I_2.$$

Ainsi, la 2−matrice aléatoire symétrique $(a|b)^* M (a|b)$ vérifie des conditions suffisantes, énoncées en propriété 1, pour obéir à la loi $\mathcal{W}(1, I_2)$. □

Propriété 6. Il existe un unique $p-$vecteur aléatoire X tel que $\left\{ \begin{smallmatrix} p(X_1 > 0) = 1 \\ M = XX^* \end{smallmatrix} \right.$. Ce vecteur X est ainsi défini : $X_i = \frac{M_{1,i}}{\sqrt{M_{1,1}}}$, $1 \leq i \leq p$.

Cette existence d'un X satisfaisant l'égalité $M = XX^*$ sera très utile par la suite. L'unicité permet de voir qu'il suffit de fixer le signe de la première composante de X pour avoir unicité de X dans l'expression XX^*. On pourrait de même démontrer qu'il suffit de fixer le signe d'une composante quelconque de X pour avoir cette unicité.

Preuve.
Unicité. Si X existe, par identification, on est sûr qu'il est ainsi défini : $X_i = \frac{M_{1,i}}{\sqrt{M_{1,1}}}$, $1 \leq i \leq p$.
Existence. Vérifions que s'il est défini ainsi, alors $M = XX^*$.

D'après la propriété 5, si a et b sont deux $p-$vecteurs unitaires orthogonaux, alors $\mathcal{L}((a|b)^* M (a|b)) = \mathcal{W}(1, I_2)$.
Observons que le déterminant de toute matrice de loi $\mathcal{W}(1, I_2)$ est nul, puisqu'une telle matrice est de rang 1. Soit $(e_i)_{1 \leq i \leq p}$ la base canonique de $\mathbb{R}^p$: $e_i^* M e_j = M_{ij}$.
• Choisissons d'abord $a = e_1$ et $b = e_i$, $1 < i \leq p$. Comme $e_1^* e_i = 0$ pour tout $i > 1$, on a : $\mathcal{L}((e_1, e_i)^* M (e_1, e_i)) = \mathcal{L}(\binom{X_1}{X_i}(X_1, X_i)) = \mathcal{W}(1, I_2) \Rightarrow M_{11} \times M_{ii} = M_{11}^2$. D'où $M_{ii} = X_i^2$.
• Choisissons ensuite $a = e_i$ et $b = e_j$, $1 < i < j \leq p$. $\mathcal{L}((e_i, e_j)^* M (e_i, e_j)) = \mathcal{W}(1, I_2) \Rightarrow M_{ii} \times M_{ij} = M_{ij}^2$. D'où $M_{ij}^2 = (X_i X_j)^2$.

M_{ij} est du type $M_{ij} = U_{ij} X_i X_j$ avec U_{ij} v.a. à valeurs dans $\mathcal{S}_1$.
• Choisissons enfin $a = \frac{1}{\sqrt{2}}(e_1 + e_i)$ et $b = e_j$, $1 < i < j \leq p$.
$\mathcal{L}((\frac{1}{\sqrt{2}}(e_1 + e_i), e_j)^* M (\frac{1}{\sqrt{2}}(e_1 + e_i), e_j)) = \mathcal{L}\left(\begin{bmatrix} \frac{1}{2}(X_1 + X_i)^2 & \frac{1}{\sqrt{2}}(X_1 X_j + U_{ij} X_i X_j) \\ \frac{1}{\sqrt{2}}(X_1 X_j + U_{ij} X_i X_j) & X_j^2 \end{bmatrix}\right) =$ $\mathcal{W}(1, I_2)$. Puisque cette 2−matrice est de Wishart, son déterminant est nul. Cela équivaut, tout calcul fait, à l'égalité $(U_{ij} - 1) X_1 X_i X_j^2 = 0$. Pour tout k de $\{1, \ldots, p\}$, on a :$\mathcal{L}(X_k^2) = \chi^2(1) \Rightarrow p(X_k = 0) = 0$. D'où $U_{ij} = 1$ et $M_{ij} = X_i X_j$. □

Propriété 7. Si Y est un $p-$vecteur aléatoire tel que $\mathcal{L}(YY^*) = \mathcal{W}(1, I_p)$, alors, pour toute v.a. U uniforme sur $\mathcal{S}_1$ indépendante de Y, $\mathcal{L}(UY) = \mathcal{N}(0, I_p)$.

Preuve. Choisissons d'abord $M = ZZ^*$ avec $\mathcal{L}(Z) = \mathcal{N}(0, I_p)$. On a $\mathcal{L}(M) = \mathcal{W}(1, I_p)$. Pour tout i de $\{1, \ldots, p\}$, $Z_i = U_i |Z_i|$, avec U_1, U_2, …, U_p, $|Z_1|$, $|Z_2|$, …, $|Z_p|$ indépendantes, et $\mathcal{L}(U_i) = \mathcal{U}(\mathcal{S}_1)$, $\mathcal{L}(Z_i^2) = \chi^2(1)$.

On considère X le vecteur aléatoire unique défini comme dans la propriété 6 : $X = U_1 Z$. Soit U une v.a. uniforme sur $\mathcal{S}_1$, indépendante de Z donc de $(M, U_1, \ldots, U_p, |Z_1|, |Z_2|, \ldots, |Z_p|)$. Soit $V_i = U U_1 U_i$.

Les $V_i|Z_i|$ sont les coordonnées de UX. Les V_i sont des v.a. uniformes sur $\mathcal{S}_1$, indépendantes entre elles et indépendantes de $|Z_1|$, $|Z_2|$, ..., $|Z_p|$ (propriété 3). On a donc $\mathcal{L}(UX) = \mathcal{N}(0, I_p)$.

$\mathcal{L}(U, M)$ détermine $\mathcal{L}(UX)$. On a donc prouvé que si $\mathcal{L}(M) = \mathcal{W}(1, I_p)$, alors, pour toute v.a. U uniforme sur $\mathcal{S}_1$ indépendante de M, on a : $\mathcal{L}(UX) = \mathcal{N}(0, I_p)$.

Choisissons à présent $M = YY^*$ avec Y tel que $\mathcal{L}(YY^*) = \mathcal{W}(1, I_p)$. Soit $T = \frac{Y_1}{|Y_1|}$, où Y_1 est la première composante de Y. Cette v.a. est à valeurs dans $\mathcal{S}_1$. Comme $T = T^{-1}$, le vecteur aléatoire X défini dans la propriété 6 s'écrit encore $X = TY$. Soit U une v.a. uniforme sur $\mathcal{S}_1$ indépendante de Y, donc de $(YY^*, T) = (M, T)$. Soit z un $p-$vecteur. Comme U est indépendante de M, $\mathcal{L}((U, T)/M = zz^*) = \mathcal{L}(U, [T/M = zz^*])$. La v.a. U est indépendante de $[T/M = zz^*]$ car elle est indépendante de (M, T). D'où $\mathcal{L}(UT/M = zz^*) = \mathcal{U}(\mathcal{S}_1)$ (propriété 3). Ainsi, pour tout z de $\mathbb{R}^p$, $\mathcal{L}(UT/M = zz^*) = \mathcal{U}(\mathcal{S}_1)$. Ceci prouve que UT est une v.a. uniforme sur $\mathcal{S}_1$ indépendante de M, donc de X. On a : $\mathcal{L}(UTX) = \mathcal{N}(0, I_p)$, c'est-à-dire $\mathcal{L}(UY) = \mathcal{N}(0, I_p)$. □

Propriété 8. La loi de M est de Wishart $\mathcal{W}(1, I_p)$.

Preuve. Soit X le $p-$vecteur aléatoire défini comme dans la propriété 6. Soit U une v.a. uniforme sur $\mathcal{S}_1$ indépendante de M. Posons $Y = UX$. On a $M = YY^*$. Soit a un vecteur de $\mathcal{S}_p$. Puisque $\mathcal{L}(a^*XX^*a) = \chi^2(1) = \mathcal{W}(1, I_1)$, et que U est une v.a. uniforme sur $\mathcal{S}_1$ indépendante de a^*X, on a $\mathcal{L}(a^*Y) = \mathcal{L}(Ua^*X) = \mathcal{N}(0, 1)$ (propriété 7). Ceci étant vrai pour tout $p-$vecteur unitaire a, le vecteur aléatoire Y est gaussien. Vérifions que les coordonnées Y_i, $1 \leq i \leq p$, de Y sont centrées réduites, et de covariances nulles. Elles sont liées aux coordonnées X_i de X par les égalités $Y_i = UX_i$, $1 \leq i \leq p$. Pour tout couple d'entiers (i, j) tel que $1 \leq i < j \leq p$, $\mathcal{L}((e_i|e_j)^*M(e_i|e_j)) = \mathcal{W}(1, I_2)$; or $((e_i|e_j)^*M(e_i|e_j)) = (Y_iY_j)^*(Y_iY_j) = (U(X_iX_j))^*(U(X_iX_j))$; d'où $\mathcal{L}(\binom{Y_i}{Y_j}) = \mathcal{N}(0, I_2)$ (propriété 7). Ainsi, $\mathcal{L}(Y) = \mathcal{N}(0, I_p)$ et $\mathcal{L}(M) = \mathcal{L}(YY^*) = \mathcal{W}(1, I_p)$.

3 Les $k-$isométries aléatoires

3.1 La loi uniforme sur $\mathcal{S}_k$: $\mathcal{U}(\mathcal{S}_k)$

Propriété 9. Soit U une v.a. à valeurs dans $\mathcal{S}_k$. Alors $\mathcal{L}(U) = \mathcal{U}(\mathcal{S}_k) \Leftrightarrow (\forall(a, b) \in \mathcal{S}_k^2), \mathcal{L}(a^*U) = \mathcal{L}(b^*U)$.

Propriété 10. Soient $U_1, U_2, \ldots, U_p$ p vecteurs aléatoires indépendants chacun de loi $\mathcal{U}(\mathcal{S}_k)$. Soit de plus R une $k-$isométrie aléatoire (c'est-à-dire une $k-$matrice aléatoire telle $R^*R = I_k$) indépendante de $(U_1, U_2, \ldots, U_p)$. Alors $\mathcal{L}(RU_i) = \mathcal{U}(\mathcal{S}_k)$, pour $i = 1, \ldots, p$, et R, RU_1, ..., RU_p sont indépendantes.

Preuve. Soit A une $k-$isométrie non aléatoire. Sa transposée A^* est elle aussi une $k-$isométrie. Comme $(\forall(a, b) \in \mathcal{S}_k^2)$, $(A^*a, A^*b) \in \mathcal{S}_k^2)$, on a, pour tout i de $1, \ldots, p$, $(\forall(a, b) \in \mathcal{S}_k^2)$, $\mathcal{L}(a^*AU_i) = \mathcal{L}(b^*AU_i)$. Il en découle (propriété 9) que le $p-$uplet $(AU_1, \ldots, AU_p)$ est fait de vecteurs aléatoires indépendants uniformes sur $\mathcal{S}_k$. Ceci étant vrai pour toute $k-$isométrie A, c'est encore vrai pour toute $k-$isométrie aléatoire R indépendante de $(U_1, \ldots, U_p)$.

De plus, pour tout couple (A, B) de $k-$isométries,
$\mathcal{L}((RU_1, \ldots, RU_p)/R = A) = \mathcal{L}((RU_1, \ldots, RU_p)/R = B)$.
D'où l'indépendance entre R et $(RU_1, \ldots, RU_p)$. □

Propriété 11. Soit X un $k-$vecteur aléatoire tel que $P(X = 0) = 0$, tel que $(\forall(a, b) \in \mathcal{S}_k^2), \mathcal{L}(a^*X) = \mathcal{L}(b^*X)$, et tel que, pour toute $k-$base orthonormée $(a_1, \ldots, a_k)$, les v.a. $(a_1^*X, \ldots, a_k^*X)$ soient indépendantes. Alors $\mathcal{L}(\frac{1}{\|X\|}X) = \mathcal{U}(\mathcal{S}_k)$, et $\|X\|$ et $\frac{1}{\|X\|}X$ sont indépendants.

Preuve. Posons $U = \frac{1}{\|X\|}X$. Soit $(a, b) \in \mathcal{S}_k^2$. On complète a en une $k-$base orthonormée $(a, a_2, \ldots, a_k)$. De même, on complète b en une $k-$base orthonormée $(b, b_2, \ldots, b_k)$. Selon les hypothèses,

$$\mathcal{L}\left(\begin{bmatrix} a^*X \\ a_2^*X \\ \ldots \\ a_k^*X \end{bmatrix}\right) = \mathcal{L}\left(\begin{bmatrix} b^*X \\ b_2^*X \\ \ldots \\ b_k^*X \end{bmatrix}\right).$$

D'où : $\mathcal{L}\left(\frac{a^*X}{\sqrt{(a^*X)^2+(a_2^*X)^2+\ldots+(a_k^*X)^2}}\right) = \mathcal{L}\left(\frac{b^*X}{\sqrt{(b^*X)^2+(b_2^*X)^2+\ldots+(b_k^*X)^2}}\right)$, c'est-à-dire $\mathcal{L}(a^*U) = \mathcal{L}(b^*U)$.

Ceci étant vrai pour tout couple (a, b) d'éléments de $\mathcal{S}_k$, U est uniforme sur $\mathcal{S}_k$.

$\mathcal{L}(\|X\|/U = a) = \mathcal{L}(\|-X\|/U = a) = \mathcal{L}(\|X\|/U = -a)$. D'où $\mathcal{L}(\|X\|/U = a) = \mathcal{L}(\|X\|/U \in \{a, -a\})$.
Par ailleurs, $\mathcal{L}(\|X\|/U \in \{a, -a\}) = \mathcal{L}(|a^*X|/a_2^*X = \ldots = a_k^*X = 0) = \mathcal{L}(|a^*X|)$, à cause de l'indépendance de a^*X et de $(a_2^*X, \ldots, a_k^*X)$.

Cette loi étant la même pour tout a, $\|X\|$ et U sont indépendants. □

Remarque. Si K est une matrice aléatoire telle que $\mathcal{L}(K) = \mathcal{L}(\|X\|^2)$, et si U est un $k-$vecteur aléatoire uniforme sur $\mathcal{S}_k$ et indépendant de K, alors $\mathcal{L}(\sqrt{K}U) = \mathcal{L}(X)$.

Corollaire 2. Dans le cas particulier où $\mathcal{L}(X) = \mathcal{N}(0, I_k)$, alors $\mathcal{L}(\|X\|^2) = \chi^2(k)$, $\mathcal{L}(\frac{X}{\|X\|}) = \mathcal{U}(\mathcal{S}_k)$, et $\|X\|$ et $\frac{1}{\|X\|}X$ sont indépendants. Réciproquement, si K est une matrice aléatoire telle que $\mathcal{L}(K) = \chi^2(k)$, si U est une v.a. indépendante de K telle que $\mathcal{L}(U) = \mathcal{U}(\mathcal{S}_k)$, alors $\mathcal{L}(\sqrt{K}U) = \mathcal{N}(0, I_k)$.

3.2 Les $k-$isométries aléatoires uniformes

Définition 3. Une $k-$isométrie aléatoire R sera dite uniforme si, pour tout a de $\mathcal{S}_k$, $\mathcal{L}(Ra) = \mathcal{U}(\mathcal{S}_k)$.

On suppose dans ce paragraphe que R est une $k-$isométrie aléatoire uniforme.

Propriété 12. R^* est une $k-$isométrie aléatoire uniforme.

Preuve. Soient a, b et c trois vecteurs unitaires de $\mathbb{R}^k$. Puisque $\mathcal{L}(Ra) = \mathcal{L}(Rb)$, on a : $\mathcal{L}(c^*Ra) = \mathcal{L}(c^*Rb)$, ou encore : $\mathcal{L}(a^*R^*c) = \mathcal{L}(b^*R^*c)$.

Puisque $(\forall (a, b) \in \mathcal{S}_k^2)$, $\mathcal{L}(a^*R^*c) = \mathcal{L}(b^*R^*c)$, on a, pour tout c de $\mathcal{S}_k$, $\mathcal{L}(R^*c) = \mathcal{U}(\mathcal{S}_k)$. □

Propriété 13. Pour tout $k-$vecteur aléatoire unitaire U indépendant de R, $\mathcal{L}(RU) = \mathcal{L}(R^*U) = \mathcal{U}(\mathcal{S}_k)$.

Propriété 14. Pour toute $k-$isométrie aléatoire S indépendante de R, RS et SR sont des $k-$isométries aléatoires uniformes.

Preuve. Soit S une $k-$isométrie aléatoire indépendante de R. Pour tout a de $\mathcal{S}_k$, Sa est un vecteur unitaire indépendant de R. □

3.3 Les $k-$isométries aléatoires canoniques

Soit U une $k-$matrice aléatoire dont les colonnes U_1, ..., U_k sont indépendantes et telles que $\mathcal{L}(U_i) = \mathcal{U}(\mathcal{S}_k)$.

Orthonormalisons par le procédé de Schmidt la $k-$famille $(U_1, \ldots, U_k)$. La famille orthonormale résultante sera notée $(R_1, \ldots, R_k)$.

Comme $\|U_1\| = 1$, $R_1 = U_1$.

Posons $V_2 = U_2 - R_1R_1^*U_2$, alors $R_2 = \frac{V_2}{\|V_2\|}$.

Posons $V_3 = U_3 - (R_1R_1^* + R_2R_2^*)U_3$, alors $R_3 = \frac{V_3}{\|V_3\|}$.

Et ainsi de suite.

La matrice aléatoire R dont les colonnes sont les R_i est une $k-$isométrie aléatoire.

Ce procédé de construction caractérise la loi de probabilité de R. Par la suite, nous nommerons cette loi la loi des isométries aléatoires semi-canoniques à gauche et nous la noterons $g - \mathcal{I}_k$. La justification de cette dénomination vient de la propriété suivante, qui traduit la stabilité de cette classe d'isométries par le produit à gauche avec toute isométrie aléatoire indépendante :

Propriété 15. Si R est une isométrie aléatoire telle que $\mathcal{L}(R) = g - \mathcal{I}_k$, alors, pour toute $k-$isométrie aléatoire S indépendante de R, $\mathcal{L}(SR) = g - \mathcal{I}_k$. De plus, S et SR sont indépendantes.

Preuve. Supposons que R soit obtenue à partir de U par le procédé d'orthonormalisation décrit plus haut. Soit A une $k-$isométrie non aléatoire, donc indépendante de U. Alors les colonnes de AU sont uniformes sur $\mathcal{S}_k$ et indépendantes, comme celles de U. L'orthonormalisation des colonnes de AU conduit à la matrice AR. Ainsi, pour toute $k-$isométrie non-aléatoire A, $\mathcal{L}(AR) = g - \mathcal{I}_k$. C'est encore vrai si on remplace A par une isométrie aléatoire S indépendante de R. L'isométrie aléatoire SR est indépendante de S puisque si A et B sont deux $k-$isométries, alors $\mathcal{L}(SR/S = A) = \mathcal{L}(SR/S = B)$.
□

Propriété 16. Les $k-$isométries aléatoires semi-canoniques à gauche sont uniformes, ainsi que leurs adjointes.

Preuve. Soit R une isométrie telle que $\mathcal{L}(R) = g - \mathcal{I}_k$. Soient a et b deux éléments de $\mathcal{S}_k$. On peut compléter les deux lignes unitaires a^* et b^* en deux isométries A et B par la création de lignes a_i^* et b_i^* $(2 \le i \le k)$ telles que $A^* = (a|a_2|\dots|a_k)$ et $B^* = (b|b_2|\dots|b_k)$. Puisque $\mathcal{L}(AR) = \mathcal{L}(BR)$, on a : $\mathcal{L}(a^*R) = \mathcal{L}(b^*R)$. Il en résulte : $(\forall(a,b,c) \in \mathcal{S}_k^3)$, $\mathcal{L}(a^*Rc) = \mathcal{L}(b^*Rc)$. D'où $(\forall c \in \mathcal{S}_k)$, $\mathcal{L}(Rc) = \mathcal{U}(\mathcal{S}_k)$. □

3.4 Les $k-$isométries aléatoires canoniques

Définition 4. Nous appellerons $k-$isométries canoniques les produits du type RS^*, avec R et S $k-$isométries semi-canoniques à gauche indépendantes. Nous noterons $\mathcal{I}_k$ la loi de probabilité ainsi définie.

Propriété 17.
P17.1. Les isométries aléatoires canoniques sont uniformes.
P17.2. La transposée de toute isométrie aléatoire canonique est canonique.
P17.3. Si R est une isométrie telle que $\mathcal{L}(R) = \mathcal{I}_k$ alors, pour toute $k-$isométrie aléatoire S indépendante de R, $\mathcal{L}(RS) = \mathcal{L}(SR) = \mathcal{I}_k$. De plus, RS et SR sont indépendantes de S.
P17.4. Le produit de deux $k-$isométries aléatoires canoniques indépendantes est une $k-$isométrie aléatoire canonique indépendante de chacune d'entre elles.

Preuve. De par la propriété 14, le produit, à droite ou à gauche, d'une isométrie aléatoire uniforme par une isométrie aléatoire (pas nécessairement uniforme) indépendante est uniforme. D'où P17.1.

La propriété P17.2 découle de la construction d'une isométrie aléatoire canonique.

La propriété P17.3 est déduite de la propriété 14.

Enfin, P17.4 est une conséquence de P17.3, en prenant S uniforme. □

4 La loi de Wishart à k degrés de liberté $\mathcal{W}(k, I_p)$

Définition 5. Soit X une $(k,p)-$matrice aléatoire dont les termes sont normaux, centrés, réduits et indépendants. On écrira $\mathcal{L}(X) = \mathcal{N}(0,k,p,I_{kp})$. La loi de Wishart à k d.d.l. de paramètre d'échelle I_p est la loi de probabilité de la $p-$matrice aléatoire X^*X. Cette loi est notée $\mathcal{W}(k, I_p)$.

Propriété 18. Si X est une matrice aléatoire à k lignes et p colonnes de la forme $(X_1|\dots|X_p)$, et si R est une $k-$isométrie aléatoire, alors $X^*X = (RX)^*(RX)$.

De même que, pour tout $p-$vecteur aléatoire X, le produit X^*X ne détermine X qu'à une v.a. multiplicative uniforme sur $\mathcal{S}_1$ près, ici, le produit X^*X ne détermine X qu'à une $k-$isométrie aléatoire multiplicative près.

Dans tout ce paragraphe, on supposera que M est une $p-$matrice aléatoire symétrique $(M^* = M)$. On pose $q = min(k+1, p)$, et on suppose que pour toute famille orthogonale $(a_1, \dots, a_q)$ de $\mathcal{S}_p^q$, les v.a. $a_i^*Ma_i$ sont indépendantes et de loi $\chi^2(k)$, pour $i = 1, \dots, q$.

Propriété 19. Pour toute famille orthogonale $(a_1, \dots, a_q)$ de $\mathcal{S}_p^q$, la $q-$matrice aléatoire symétrique de terme général $a_j^*Ma_j$ obéit à la loi $W(k, I_q)$.

Preuve. Soit $(a_1, \dots, a_q)$ une famille de $p-$vecteurs unitaires 2 à 2 orthogonaux, c'est-à-dire telle que $(a_1|\dots|a_q)^*(a_1|\dots|a_q) = I_q$.

Pour toute $q-$isométrie A, les q colonnes de la matrice $(a_1|\dots|a_q)A$ sont des $p-$vecteurs unitaires 2 à 2 orthogonaux ; en effet, $((a_1|\dots|a_q)A)^*((a_1|\dots|a_q)A) = A^*(a_1|\dots|a_q)^*(a_1|\dots|a_q)A = A^*A = I_q$. Ainsi, la $q-$matrice aléatoire symétrique $(a_1|\dots|a_q)^*M(a_1|\dots|a_q)$ vérifie des conditions suffisantes, énoncées en propriété 1, pour obéir à la loi $W(k, I_q)$. □

Propriété 20. Il existe une unique $(k,p)-$matrice aléatoire X possédant les propriétés suivantes :

pour $1 \le j < i \le q$, $X_{i,j} = 0$; pour $1 \le j \le q$, $X_{j,j} > 0$; $M = X^*X$.

Preuve.
Unicité. On construit successivement $X_{1,1} = \sqrt{M_{1,1}}$, $X_{1,2}$ telle que $X_{1,1}X_{1,2} = M_{1,2}$, $X_{2,2}$ telle que $X_{1,2}^2 + X_{2,2}^2 = M_{2,2}$, $X_{1,3}$ telle que $X_{1,1}X_{1,3} = M_{1,3}$, $X_{2,3}$ telle que $X_{1,2}X_{1,3} + X_{2,2}X_{2,3} = M_{2,3}$, et ainsi de suite. C'est la seule possibilité.
Existence. Si $p = q$, alors $\mathcal{L}(M) = \mathcal{W}(k, I_p)$ et $M = X^*X$. On suppose donc que $p > q$, c'est-à-dire $q = k+1$. Par construction, pour $1 \le i \le k$ et $1 \le j \le p$, $M_{i,j} = X_i^*X_j$. Il reste à montrer que, pour $k < j \le p$, $M_{j,j} = X_j^*X_j$ et que, pour $k < r < s \le p$, $M_{r,s} = X_r^*X_s$.

Rappelons que pour toute $q-$famille orthonormée de $p-$vecteurs $(a_1, \ldots, a_q)$,
$\mathcal{L}((a_1|\ldots|a_q)^* M(a_1|\ldots|a_q)) = \mathcal{W}(k, I_q)$.
On notera A la $(k,q)-$matrice $(a_1|\ldots|a_q)$. Toute $(k,r)-$matrice aléatoire X telle que $\mathcal{L}(X) = \mathcal{N}(0,k,r,kr)$ est de rang $min(k,r)$. Il en est de même de la $r-$matrice aléatoire X^*X. Ainsi, toute matrice aléatoire de loi $\mathcal{W}(k, I_r)$ est de rang $min(k,r)$. Son déterminant est donc nul si et seulement si $r > k$.

On désigne encore par $(e_i)_{1\leq i \leq p}$ la base canonique de $\mathbb{R}^p$.
it a) Choisissons $a_i = e_i$, pour $i = 1, \ldots, k$, et $a_q = e_j$ pour $j = k+1, \ldots, p$.

On sait que $det(A^*MA) = 0$. On développe ce déterminant par rapport à la dernière colonne. Le coefficient de $M_{j,j}$, au signe près, est le déterminant non nul de la $k-$matrice de Wishart à k d.d.l. $(a_1|\ldots|a_k)^* M(a_1|\ldots|a_k)$. On a donc $M_{j,j}$ déterminée ; elle est égale à $X_j^* X_j$.
it b) Choisissons $a_i = e_i$, pour $i = 1, \ldots, k-1$, $a_k = e_r$ et $a_q = e_s$ pour $k < r < s \leq p$.

Ici encore $det(A^*MA) = 0$. On développe ce déterminant par rapport à la dernière colonne. On obtient une équation du second degré en $M_{r,s}$. Elle est vraiment du second degré puisque le coefficient de $M_{r,s}^2$, au signe près, est le déterminant non nul de la $(k-1)-$matrice de loi de Wishart à k d.d.l. $(a_1|\ldots|a_{k-1})^* M(a_1|\ldots|a_{k-1})$ A partir de cette équation, $M_{r,s}^2$ est exprimable comme un polynôme de degré au plus 1 en $M_{r,s}$ du type $M_{r,s}^2 = \alpha M_{r,s} + \beta$, avec α et β variables aléatoires.
it b) Choisissons $a_i = e_i$, pour $i = 1, \ldots, k-1$, $a_k = \frac{1}{\sqrt{2}}(e_k + e_r)$ et $a_q = e_s$ pour $k < r < s \leq p$.

On a toujours $det(A^*MA) = 0$, et on développe ce déterminant par rapport à la dernière colonne. On obtient une autre équation du second degré en $M_{r,s}$, ramenée à une équation du premier degré grâce à l'égalité $M_{r,s}^2 = \alpha M_{r,s} + \beta$. C'est vraiment une équation du premier degré. En effet, au signe près, le coefficient de $M_{r,s}$ est le déterminant du produit $(X_1|\ldots|X_{k-1}|X_s)^*(X_1|\ldots|X_{k-1}|X_k)$; chacune des $k-$matrices $(X_1|\ldots|X_{k-1}|X_s)^*(X_1|\ldots|X_{k-1}|X_k)$, qui égale
$(e_1|\ldots|e_{k-1}|e_s)^* M(e_1|\ldots|e_{k-1}|e_s)$ et $(X_1|\ldots|X_{k-1}|X_k)^*(X_1|\ldots|X_{k-1}|X_k)$, qui égale
$(e_1|\ldots|e_{k-1}|e_k)^* M(e_1|\ldots|e_{k-1}|e_k)$, étant de loi de Wishart à k d.d.l., elle est de rang k ; il en est de même de chacune des matrices $(X_1|\ldots|X_{k-1}|X_s)^*$ et $(X_1|\ldots|X_{k-1}|X_k)$; leurs déterminants sont non nuls. Une solution est toujours $M_{r,s} = X_r^* X_s$, et c'est la seule. $\square$

Propriété 21. Si Y est une $(k,p)-$matrice aléatoire telle que $\mathcal{L}(Y^*Y) = \mathcal{W}(k, I_p)$, alors pour toute $k-$isométrie aléatoire canonique R indépendante de Y, on a : $\mathcal{L}(RY) = \mathcal{N}(0,k,p,I_{kp})$.

Preuve. Soit Z une $(k,p)-$matrice aléatoire telle que $\mathcal{L}(Z) = \mathcal{N}(0,k,p,I_{kp})$ et $M = Z^*Z$. Pour tout i de $1, \ldots, p$, les vecteurs aléatoires Z_i sont de la forme $\|Z_i\| U_i$, avec U_1, ..., U_p, $\|Z_1\|$, ..., $\|Z_p\|$ indépendants, $\mathcal{L}(U_i) = \mathcal{U}(\mathcal{S}_k)$, et $\mathcal{L}(\|Z_i\|^2) = \chi^2(k)$.

Soit T la $k-$isométrie aléatoire semi-canonique à gauche obtenue en orthonormalisant la famille $(U_1, \ldots, U_k)$ par le procédé de Schmidt, comme décrit en § 3.3. Si $p < k$, on choisit les $k-p$ derniers U_i, $p < i \leq k$ quelconques uniformes sur $\mathcal{S}_k$, indépendants entre eux et indépendants de $(M, U_1, \ldots, U_p)$.

Alors la $(k,p)-$matrice aléatoire X définie dans la propriété 20 est $X = T^*Z$. Soit S une $k-$isométrie aléatoire canonique indépendante de Z donc de $(M, T, U_1, \ldots, U_p, \|Z_1\|, \ldots, \|Z_p\|)$. Alors $STX = STT^*Z = SZ$.

Posons, pour $i = 1, \ldots, p$, $V_i = SU_i$. Les V_i sont des vecteurs aléatoires uniformes sur $\mathcal{S}_k$, indépendants entre eux et indépendants de $\|Z_1\|$, ..., $\|Z_p\|$.

On a : $\mathcal{L}(STX) = \mathcal{N}(0,k,p,I_{kp})$. Soit z une $(k,p)-$matrice. $\mathcal{L}((S,T)/M = z^*z) = \mathcal{L}((S, [T/M = z^*z])$ car S est indépendante de (M,T). On déduit (paragraphe 3.4) : $\mathcal{L}(ST/M = z^*z) = \mathcal{I}_k$. Ceci étant vrai pour toute $(k,p)-$matrice z, ST est une $k-$isométrie aléatoire canonique indépendante de M. On a trouvé une $k-$isométrie aléatoire canonique $R(= ST)$ indépendante de M telle que $\mathcal{L}(RX) = \mathcal{N}(0,k,p,I_{kp})$. La loi de (R,M) déterminant celle de RX, pour toute $k-$isométrie aléatoire canonique R indépendante de M, on a : $\mathcal{L}(RX) = \mathcal{N}(0,k,p,I_{kp})$.

Choisissons à présent $M = Y^*Y$. Soit Q la $k-$isométrie aléatoire semi-canonique à gauche obtenue en orthonormalisant la famille $(Y_1/\|Y_1\|, \ldots, Y_k/\|Y_k\|)$ par le procédé de Schmidt. La $(k,p)-$matrice aléatoire X définie dans la propriété 20 est : $X = Q^*Y$.

Soit R une $k-$isométrie aléatoire canonique indépendante de Y, donc de (M,Q). Soit z une $(k,p)-$matrice. $\mathcal{L}((R,Q)/M = z^*z) = \mathcal{L}((R, [Q/M = z^*z])$ car R est indépendante de M. R et $[Q/M = z^*z]$ sont indépendantes car R est indépendante de (M,Q). On déduit (paragraphe 3.4) : $\mathcal{L}(RQ/M = z^*z) = \mathcal{I}_k$. Ceci étant vrai pour toute $(k,p)-$matrice z. RQ est une $k-$isométrie aléatoire canonique indépendante de M, donc de X. Elle est telle que $\mathcal{L}(RQX) = \mathcal{N}(0,k,p,I_{kp})$. Or $RQX = RY$, d'où la propriété. $\square$

Propriété 22. $\mathcal{L}(M) = \mathcal{W}(k, I_p)$.

Preuve. C'est vrai, d'après la propriété 19, pour $p \leq k+1$. Montrons-le pour $p > k+1$.

Soit X la $(k,p)-$matrice aléatoire définie dans la propriété 20. Soit R une $k-$isométrie aléatoire canonique indépendante de X. Soit $Y = RX$, et $M = Y^*Y$. Soit $(u_1, \ldots, u_p)$ une famille de $k-$vecteurs non tous nuls. La famille $(u_1, \ldots, u_p)$ est de rang $j \leq k$. Tous les u_i sont combinaisons linéaires de j d'entre eux, par exemple des j premiers.

Il existe donc une $(p,j)-$matrice A telle que $\sum_{i=1}^{p} u_i^* Y_i = \sum_{i=1}^{j} u_i^* Z_i$ avec $Z = YA = RXA$.

On orthonormalise les colonnes de A par le procédé de Schmidt. Cela revient à multiplier à droite A par une certaine $j-$matrice inversible B. On a $ZB = RXC$, avec $C = AB$. Les j colonnes de C sont des $p-$vecteurs unitaires et 2 à 2 orthogonaux. On a : $B^*Z^*ZB = C^*MC$.

Puisque $\mathcal{L}(C^*MC) = \mathcal{W}(k, I_j)$, on a : $\mathcal{L}(ZB) = \mathcal{L}(RXC) = \mathcal{N}(0, k, j, I_{kj})$. La matrice aléatoire ZB étant gaussienne (c'est-à-dire le vecteur constitué de ses termes étant gaussien), il en est de même de la matrice aléatoire $Z = ZBB^{-1}$. La v.a. $\sum_{i=1}^{j} u_i^* Z_i$ est donc normale. Ainsi, pour tout $(u_1, u_2, \ldots, u_p)$, la v.a. $\sum_{i=1}^{p} u_i^* Y_i$ est normale. Cela signifie que la matrice aléatoire Y est gaussienne. Assurons-nous que les termes de la $(k,p)-$matrice aléatoire $Y = (Y_1|\ldots|Y_p)$ sont des v.a. centrées, réduites et de covariances nulles :
la matrice $(e_i|e_j)^*M(e_i|e_j)$, $1 \leq i < j \leq p$, est de loi $\mathcal{W}(k, I_2)$ (propriété 19) ; $(e_i|e_j)^*M(e_i|e_j) = (X_i|X_j)^*M(X_i|X_j)$; il résulte de la propriété 21 que $\mathcal{L}(R(X_i|X_j)) = \mathcal{N}(0, k, 2, I_{2k})$; $R(X_i|X_j) = (Y_i|Y_j)$; $\mathcal{L}((Y_i|Y_j)) = \mathcal{N}(0, k, 2, I_{2k})$;
les termes des $k-$vecteurs aléatoires Y_i et Y_j sont bien des v.a. normales, centrées, réduites et de covariances nulles. Ainsi, $\mathcal{L}(Y) = \mathcal{N}(0, k, p, I_{kp})$. D'où $\mathcal{L}(M) = \mathcal{W}(k, I_p)$. $\square$

Références

[1] Eaton, M.L. (1983) *Multivariate Statistics.* Wiley, New-York.

[2] Letac, G., Massam, H. (2007) Wishart distributions for decomposable graphs. *Annals of Statistics*, **35** 1278-1323

[3] Masaro, J., Wong, C.S. (2003) Wishart distributions associated with matrix quadratic forms. *J. Mult. Analysis*, **85** 1-9

Annexe 1. La caractérisation des matrices aléatoires de loi de Wishart

Propriété 23. Soit k un entier strictement positif et Σ une $p-$matrice réelle symétrique ($M^* = M$) d'espérance mahtématique semi-définie positive. Soit M une $p-$matrice aléatoire réelle symétrique. On suppose que :

- $(\forall a \in \mathbb{R}^p)$, $a^*\Sigma a = 0 \Rightarrow a^*Ma = 0$;
- $(\forall a \in \mathbb{R}^p)$, $a^*\Sigma a \neq 0 \Rightarrow \mathcal{L}(\frac{a^*M\,a}{a^*\Sigma\,a}) = \chi^2(k)$;
- pour toute $p-$base $\Sigma-$orthogonale $(a_1 \ldots, a_p)$, les v.a. $a_1^*M\,a_1, \ldots, a_p^*M\,a_p$ sont indépendantes.

Ces conditions déterminent la fonction caractéristique de M.

Preuve. Soit A une matrice réelle symétrique. L'image de A par la fonction caractéristique de M est le nombre $\phi_M(A) = E(e^{i<A,M>}) = E(exp(trace(iAM)))$.

1. Cherchons un couple (U, D) de $p-$matrices réelles telles que

- U soit régulière ;
- D soit diagonale ;
- $U^*\Sigma U$ soit diagonale, à termes diagonaux égaux à 0 ou à 1 ;
- $A = UDU^*$.

Soit $\Sigma' = \Sigma + Q$, avec Q projecteur orthogonal de $\mathbb{R}^p$ sur le sous-espace propre de Σ associé à la valeur propre 0.

La matrice Σ' est symétrique définie positive, elle peut s'écrire sous la forme $\Sigma' = Td^2T^*$, avec $TT^* = I_p$ (I_p est la matrice identité de dimension p) et d une $p-$matrice à termes diagonaux strictement positifs.

La famille $(t_1, \ldots, t_p)$ des colonnes de T est une $p-$base orthonormée de vecteurs propres de Σ. Le projecteur Q est alors du type $Q = T\delta^2T^*$, où δ est la matrice diagonale de terme diagonal δ_j égal à 0 si le vecteur Σt_j n'est pas nul, et à 1 sinon, pour $j = 1, \ldots, p$. Autrement dit, pour tout $j = 1, \ldots, p$, $\delta_j = 1 \Rightarrow d_j = 1$.

Posons $B = dT^*ATd$. Nous déduisons l'égalité $A = T^{-1}Bd^{-1}T^*$.

La matrice B étant réelle symétrique, elle est du type $B = VDV^*$, avec D matrice diagonale et $V^*V = I_p$. Posons $U = Td^{-1}V$. Nous avons $A = UDU^*$ et $U^*\Sigma' U = I_p$. De plus, la matrice $U^*\Sigma U = I_p - U^*QU$ est diagonale, à termes diagonaux égaux à 0 ou à 1.

2. Calcul de $\Phi_M(A)$.

Soit a_j le $j^{ème}$ vecteur colonne de la matrice U et α_j le $j^{ème}$ terme diagonal de la matrice D, $j = 1, \ldots, p$.

Alors $trace(iAM) = trace(iUDU^*M) = trace(iDU^*MU) = \sum_{j=1}^{p} i\alpha_j a_j^* M a_j$, d'où $e^{trace(iAM)} = \Pi_{j=1}^{p} e^{i\alpha_j a_j^* M a_j}$.

Les v.a. $a_j^* M a_j$ étant indépendantes, $E(trace(iAM)) = \Pi_{j=1}^{p} E(e^{i\alpha_j a_j^* M a_j})$.

Les hypothèses déterminant les lois de probabilité des v.a. $a_j^* M a_j$, elles déterminent le nombre $\Phi_M(A) = E(trace(iAM))$. Ainsi, pour toute $p-$matrice réelle symétrique A, $\Phi_M(A)$ est déterminé. □

Annexe 2. La loi de Wishart pour une $p-$matrice déterminée par récurrence

Propriété 24. Soient k un entier strictement positif et Σ une $p-$ matrice réelle symétrique semi-définie positive. Soit M une $p-$matrice aléatoire réelle symétrique. On suppose que

- • $\forall a \in \mathbb{R}^p$, $a^*\Sigma a = 0 \Rightarrow a^* M a = 0$;
- • $\forall a \in \mathbb{R}^p$, $a^*\Sigma a \neq 0 \Rightarrow \mathcal{L}\frac{a^*Ma}{a^*\Sigma a} = \chi^2(k)$;
- • pour toute $(k+1)-$famille $\Sigma-$orthogonale $(a_1, \ldots, a_{k+1})$, les v.a. $a_1^* M a_1, \ldots, a_{k+1}^* M a_{k+1}$ sont indépendantes.

On suppose, en hypothèse de récurrence, que si l'on remplaçait p par $p-1$, alors ces conditions seraient suffisantes pour que $\mathcal{L}(M) = \mathcal{W}(k, \Sigma)$.

Sous cette hypothèse de récurrence, si $rang(\Sigma) < p$, alors $\mathcal{L}(M) = \mathcal{W}(k, \Sigma)$.

Preuve. On suppose : $rang(\Sigma) < p$.

Soit $(a_1, \ldots, a_p)$ une $p-$base $\Sigma-$orthogonale. L'un au moins des $a_i^*\Sigma a_i$ est nul. Par exemple, on peut supposer : $a_p^*\Sigma a_p = 0$ (donc aussi $a_p^* M a_p = 0$). Soit $A = (a_1|\ldots|a_{p-1})$.

$A^*\Sigma A$ est une $(p-1)-$matrice réelle symétrique semi-définie positive.

- • $\forall b \in \mathbb{R}^{p-1}$, $b^*A^*\Sigma Ab = 0 \Rightarrow b^*A^*MAba^*Ma = 0$;
- • $\forall b \in \mathbb{R}^{p-1}$, $b^*A^*\Sigma Ab \neq 0 \Rightarrow \mathcal{L}\left(\frac{b^*A^*MAb}{b^*A^*\Sigma Ab}\right) = \chi^2(k)$;
- • pour toute $(k+1)-$famille $A^*\Sigma A-$orthogonale $(b_1, \ldots, b_{k+1})$ de $(p-1)-$vecteurs, les v.a. $b_i^*A^*MAb_i$, $1i \leq p-1$, sont indépendantes, puisque la $(k+1)-$famille de n vecteurs $(Ab_1, \ldots, Ab_{k+1})$ est $\Sigma-$orthogonale.

Par hypothèse de récurrence, la $(p-1)-$matrice symétrique aléatoire A^*MA est de loi $\mathcal{W}(k, A^*\Sigma A)$. On en déduit que pour toute $(p-1)-$base $A^*\Sigma A-$orthogonale $(b_1, b_2, \ldots, b_{p-1})$ les v.a. $b_i^*A^*MAb_i$, $i = 1, \ldots, p-1$, sont indépendantes.

La matrice $A^*\Sigma A$ étant diagonale, la famille des colonnes de la $(p-1)-$matrice unité est $A^*\Sigma A-$orthogonale. Il en résulte que les v.a. $a_i^* M a_i$, $i = 1, \ldots, p-1$, sont indépendantes et, puisque $a_p^* M a_p = 0$, que les v.a. $a_i^* M a_i$, $1 \leq i \leq p$, sont indépendantes.

Puisque, pour toute $p-$base $\Sigma-$orthogonale $(a_1, \ldots, a_p)$, les v.a. $a_i^* M a_i$, $i = 1, \ldots, p$, sont indépendantes, $\mathcal{L}(M) = \mathcal{W}(k, \Sigma)$. □