RFIDEC — cours 1 : Rappels de probas/stats (3/3)

Christophe Gonzales

LIP6 - Université Paris 6, France

Plan du cours 1.3

- variables aléatoires
- caractéristiques et variables aléatoires
- indépendances de variables aléatoires
- Ioi binomiale et loi de Poisson
- Ioi normale

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

2/35

Variables aléatoires (1/2)

Exemple

- au début : vous avez 1000€
- jeu : je tire 3 cartes parmi un jeu de 32 cartes et, suivant le tirage, je vous donne ou vous prend de l'argent :



$$P(2000€) = P(3 \text{ rois})$$

$$P(gain \ge 500 €) = P(3 rois) + P(2 rois)$$

Variables aléatoires (2/2)

Définition

- Ω = univers muni d'une loi de proba $P(\cdot)$
- Ω' un autre ensemble
- $\mathbf{2}^{\Omega}$ et $\mathbf{2}^{\Omega'}$ = ensemble des sous-ensembles de Ω et de Ω'
- variable aléatoire = fonction Γ de 2^{Ω} dans $2^{\Omega'}$ telle que :

$$\Gamma^{-1}(A') \in 2^{\Omega} \quad \forall A' \in 2^{\Omega'}.$$

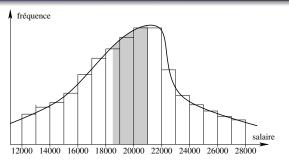
Probabilité sur Ω'

loi de proba $P'(\cdot)$ sur Ω' :

$$P'(A') = P\left(\Gamma^{-1}(A')\right) \quad \forall A' \in 2^{\Omega'}.$$

notation : $P(\Gamma = A') = P(\Gamma^{-1}(A'))$

Probabilités: retour sur le cas continu (1/2)



$$P(X \in I) = \int_{I} p(x) dx$$

avec P = proba et p = fonction de densité

 \implies connaître p = connaître P

intervalles] $-\infty$, x[\Longrightarrow fonction de répartition :

$$F(x) = P(X < x) = \int_{-\infty}^{x} p(y) dy$$

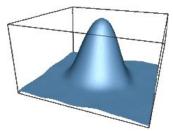
RFIDEC — cours 1 : Rappels de probas/stats (3/3)

5/35

Probabilités: retour sur le cas continu (2/2)

- variables bi-dimensionnelles, ou couples de variables, continues, (X, Y)
- densité de probabilité = p(x, y)
- fonction de répartition = F(x, y)
- alors $\forall x, y$:

$$F(x,y) = P(X < x, Y < y) = \int \int_{\{(x',y'): x' < x, y' < y\}} p(x',y') dx' dy'$$



RFIDEC — cours 1 : Rappels de probas/stats (3/3)

6/35

Caractéristiques d'une loi de probabilités (1/3)

Caractéristiques

- Médiane $M: P(X \le M) \ge \frac{1}{2}$ et $P(X \ge M) \ge \frac{1}{2}$
- Espérance mathématique ou moyenne : E(X)

X discrète : $E(X) = \sum x_k p_k$

X continue : $E(X) = \int x p(x) dx$

l'espérance mathématique n'existe pas toujours

■ Mode : Mo de P (pas toujours unique) :

X discrète : $p(Mo) = \max_k p(x_k)$ X continue : $p(Mo) = \max_k p(x)$

Propriétés de l'espérance

- E(aX + b) = aE(X) + b
- $\forall X, Y, E(X + Y) = E(X) + E(Y)$

Application de l'espérance (1/3)

- $X = \text{variable al\'eatoire} \approx 1 \text{ caract\`ere dans une phrase}$
- domaine de $X = \{x_1, ..., x_{16}\}$

Encodage « classique d'une phrase » :

16 valeurs possibles ⇒ codage sur 4 bits
 ⇒ phrase de 10 caractères = 40 bits

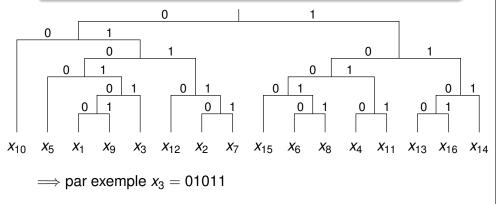
	Proba d'apparition des caractères (×100)														
<i>x</i> ₁	<i>X</i> ₁ <i>X</i> ₂ <i>X</i> ₃ <i>X</i> ₄ <i>X</i> ₅ <i>X</i> ₆ <i>X</i> ₇ <i>X</i> ₈ <i>X</i> ₉ <i>X</i> ₁₀ <i>X</i> ₁₁ <i>X</i> ₁₂ <i>X</i> ₁₃ <i>X</i> ₁₄ <i>X</i> ₁₅ <i>X</i> ₁₆														
1	3	2	6	5	4	2	3	1	21	6	5	9	17	7	8

■ Minimisation de l'espérance du nombre de bits ⇒ compression

Application de l'espérance (2/3)

	Proba d'apparition des caractères (×100)														
<i>X</i> ₁	<i>X</i> ₂	<i>X</i> ₃	<i>X</i> ₄	<i>x</i> ₅	<i>x</i> ₆	<i>X</i> ₇	<i>x</i> ₈	<i>X</i> 9	<i>x</i> ₁₀	<i>X</i> ₁₁	X ₁₂	<i>X</i> ₁₃	<i>X</i> ₁₄	X ₁₅	<i>X</i> ₁₆
1	3	2	6	5	4	2	3	1	21	6	5	9	17	7	8

Codage de Huffman



RFIDEC — cours 1 : Rappels de probas/stats (3/3)

9/35

Caractéristiques d'une loi de probabilités (2/3)

Caractéristiques de dispersion

• variance : V(X) ou σ^2 :

X discrète : $\sigma^2 = \sum [x_k - E(X)]^2 p_k$

X continue : $\sigma^2 = \int [x - E(X)]^2 p(x) dx$

- moyenne des carrés des écarts entre les valeurs prises par X et son espérance E(X)
- écart-type : σ = racine carrée de la variance
- variance et donc écart-type n'existent pas toujours

Application de l'espérance (3/3)

Nombre de bits et proba (×100) par caractère																
X_i	<i>x</i> ₁	<i>X</i> ₂	<i>x</i> ₃	<i>x</i> ₄	<i>x</i> ₅	<i>x</i> ₆	<i>X</i> ₇	<i>x</i> ₈	<i>X</i> 9	<i>X</i> ₁₀	<i>X</i> ₁₁	<i>X</i> ₁₂	<i>X</i> ₁₃	X ₁₄	<i>X</i> ₁₅	<i>X</i> ₁₆
nb bits	6	5	5	4	4	5	5	5	6	2	4	4	4	3	4	4
proba	1	3	2	6	5	4	2	3	1	21	6	5	9	17	7	8

Espérance du nombre de bits = $\sum_{i=1}^{16} p_i |\text{nb bits } x_i| = 3,59 < 4$

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

10/35

Caractéristiques d'une loi de probabilités (3/3)

Propriétés de la variance

•
$$V(X) = E(X^2) - E(X)^2$$

•
$$\forall X, Y, V(X + Y) = V(X) + V(Y) + 2cov(X, Y)$$
 où :

•
$$cov(X, Y) = covariance de X et Y$$

• si
$$X$$
 et Y discrètes et $p_k = P(X = x_k, Y = y_k)$

$$cov(X, Y) = \sum [x_k - E(X)][y_k - E(Y)]p_k$$

• si X et Y continues, de densité p(x, y),

$$cov(X, Y) = \iint [x - E(X)][y - E(Y)]p(x, y)dxdy$$

Indépendance de deux variables aléatoires (1/3)

Indépendance de deux variables discrètes

X et *Y* sont *indépendantes* si $\forall x, \forall y$:

les événements X = x et Y = y sont indépendants

$$\bullet \forall x, \forall y \ t.q. \ P(Y = y) > 0, \ P(X = x | Y = y) = P(X = x)$$

$$\forall y, \forall x \ t.q. \ P(X = x) > 0, \ P(Y = y | X = x) = P(Y = y)$$

Indépendance de deux variables aléatoires (2/3)

Indépendance de deux variables continues

X et *Y* sont *indépendantes* si $\forall I, \forall J$, intervalles,

les événements $X \in I$ et $Y \in J$ sont indépendants

Il suffit que les fonctions de répartition, F_X , F_Y de X et Y et F_{XY} du couple satisfassent :

$$\forall x, y, F_{XY}(x, y) = F_X(x) \times F_Y(y)$$

ou encore que les densités de probabilité p_X , p_Y de X et Y et p_{XY} du couple satisfassent :

$$\forall x, y, p_{XY}(x, y) = p_X(x) \times p_Y(y)$$

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

13/35

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

14/35

Indépendance de deux variables aléatoires (3/3)

Propriété

La covariance de deux variables indépendantes X et Y est toujours nulle

La réciproque est fausse

$$cov(X, Y) = \iint [x - E(X)][y - E(Y)]p_{XY}(x, y)dxdy$$

$$X \text{ et } Y \text{ indep} \Longrightarrow p_{XY}(x, y) = p_X(x) \times p_Y(y)$$

$$\Longrightarrow cov(X, Y) = \int [x - E(X)]p_X(x)dx \int [y - E(Y)]p_Y(y)dy$$

$$Or \int [x - E(X)]p_X(x)dx = \int xp_X(x)dx - \int E(X)p_X(x)dx$$

$$= E(X) - E(X) = 0$$

$$\Longrightarrow cov(X, Y) = 0 \times 0 = 0$$

Indépendance mutuelle de *n* variables (1/3)

Définition

n variables $(X_1, X_2, \ldots, X_k, \ldots, X_n)$

Elles sont *mutuellement indépendantes* si tout événement lié à une partie d'entre elles est indépendant de tout événement lié à toute autre partie disjointe de la précédente

⇒ c'est la généralisation naturelle de l'indépendance de deux variables :

des variables discrètes $(X_1, \ldots, X_k, \ldots, X_n)$ sont mutuellement indépendantes lorsque :

$$\forall x_k \ P\left(\bigcap_{k=1}^n X_k = x_k\right) = \prod_{k=1}^n P(X_k = x_k)$$

Indépendance mutuelle de n variables (2/3)

des variables continues $(X_1, \dots, X_k, \dots, X_n)$ sont mutuellement indépendantes lorsque $\forall x_k (k = 1, ..., n)$:

$$p_{X_1...X_k...X_n}(x_1,...,x_k,...,x_n) = \prod_{k=1}^n p_{X_k}(x_k)$$

L'indépendance mutuelle de *n* variables entraîne leur indépendance deux à deux



la réciproque n'est pas vraie

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

17/35

Soit n dés à 6 faces

• X_k : variable aléatoire indiquant sur quelle face tombe le kème dé

Indépendance mutuelle de n variables (3/3)

• tous les dés sont différents $\Longrightarrow X_1, \dots, X_n$ mutuellement indépendantes

$$p_{X_1...X_k...X_n}(x_1,...,x_k,...,x_n) = \prod_{k=1}^n p_{X_k}(x_k)$$

 \implies stockage mémoire = 6n au lieu de 6ⁿ

<i>n</i> = 10	60	60 millions
n = 20	120	3,6 millions de milliards

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

18/35

Indépendance conditionnelle (1/2)

Indépendance conditionnelle de deux variables discrètes

les événements X = x et Y = y sont indépendants conditionnellement à Z = z

$$P(X=x \cap Y=y|Z=z) = P(X=x|Z=z) \times P(Y=y|Z=z)$$

• si
$$P(Y=y|Z=z) > 0$$
 alors :

$$P(X=x|Y=y,Z=z) = P(X=x|Z=z)$$

 \bullet si P(X=x|Z=z) > 0 alors :

$$P(Y = y|X = x, Z = z) = P(Y = y|Z = z)$$

Indépendance conditionnelle (2/2)

Indépendance conditionnelle de deux variables discrètes

X et Y sont indépendantes conditionnellement à Z si :

$$P(X \cap Y|Z) = P(X|Z) \times P(Y|Z)$$

• si
$$P(Y|Z) > 0$$
 alors $P(X|Y,Z) = P(X|Z)$

• si
$$P(X|Z) > 0$$
 alors $P(Y|X,Z) = P(Y|Z)$

Interprétation

- Conditionnement = apport de connaissances
- Si l'on connaît la valeur de la variable Z, alors connaître celle de Y n'apporte rien sur la connaissance de X



Ces formules s'étendent si *X*, *Y* et/ou *Z* sont remplacés par des ensembles de variables aléatoires disjoints 2 à 2

Application des probas conditionnelles (1/2)



- Classe de 40 étudiants
- assertion : «il y a au moins 2 étudiants qui sont nés le même jour»

Avez-vous intérêt à parier 10 € que cette assertion est vraie ?

- $X_i \in \{1, ..., 365\}$ le jour de naissance du *i*ème étudiant
- \bullet que vaut $P(\text{tous les } X_i \text{ sont différents})?$

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

Loi binomiale

Définition

Épreuve binomiale = expérience aléatoire telle que :

- on répète *n* fois la même épreuve de Bernoulli,
- 2 les probas p et q restent inchangées pour chaque épreuve de Bernoulli.

⇒ en choisissant au hasard une classe de 40 étudiants.

on a 10,87% de chances que l'assertion soit fausse

22/35

24/35

3 les épreuves de Bernoulli sont toutes réalisées indépendamment les unes des autres.

Loi binomiale de paramètres n et p

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

- X = nombre de succès de l'épreuve binomiale
- $X \sim \mathcal{B}(n, p)$
- $P(X = k) = C_n^k p^k (1 p)^{n-k}, \forall k = 0, ..., n$
- $E(X) = np \quad V(X) = np(1-p)$

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

Définition

Loi de Bernoulli

Épreuve de Bernoulli = expérience aléatoire qui ne peut prendre que deux résultats (succès et échec)

p = proba de succès, et q = 1 - p = proba d'échec.

Loi de Bernoulli

Variable *X* à support $\mathcal{X} = \{0, 1\}$ telle que :

$$P(X = 1) = p$$
 et $P(X = 0) = 1 - p$

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

E(X) = p V(X) = p(1-p)

 \implies X = le nombre de succès de l'épreuve de Bernoulli

Application des probas conditionnelles (2/2)

 $= P(X_2 \neq X_1) \times P(X_3 \notin \{X_1, X_2\} | X_2 \neq X_1) \times$

 $= \prod_{i=2}^{40} P\left(X_i \notin \{X_j : j < i\} \middle| \bigwedge_{i < i} X_j \notin \{X_k : k < j\}\right)$

 $=\prod_{i=1}^{40}\frac{365-(i-1)}{365}=\prod_{i=1}^{39}\frac{365-i}{365}\approx 10,87\%$

 $P(X_4 \notin \{X_1, X_2, X_3\} | X_2 \neq X_1, X_3 \notin \{X_1, X_2\}) \times \dots$

 $\alpha = P(\text{tous les } X_i \text{ sont différents})$

Loi de Poisson

Définition

- Loi de Poisson ou loi des événements rares :
 loi vers laquelle tend la loi binomiale lorsque n est très grand et p assez petit
- variable discrète $X \sim loi\ de$ Poisson de paramètre $\lambda > 0$: \Longrightarrow les événements élémentaires $e_k = \ll X = k \gg, \ k \in \mathbb{N},$ ont pour probabilités :

$$P(X=k) = \frac{e^{-\lambda} \times \lambda^k}{k!}$$

- ⇒ s'applique dans le cas d'expériences dont les occurrences sont totalement aléatoires (sans régularité) et indépendantes les unes des autres

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

25/35

Définition : loi géométrique de paramètre p loi de la variable donnant le nombre d'e

Lois géométrique et exponentielle

- loi de la variable donnant le nombre d'essais nécessaires pour que se produise un événement de probabilité p
- $P(X = k) = p(1 p)^{(k-1)}, k = 1, ..., n, ...$
- $E(X) = \frac{1}{p}$ $V(X) = \frac{1-p}{p^2}$

Définition : loi exponentielle de paramètre λ

- a pour support \mathbb{N}_+^* et pour densité $p(x) = \lambda \exp{-\lambda x}, x > 0$
- $E(X) = \frac{1}{\lambda}$ $V(X) = \frac{1}{\lambda^2}$
- utilisée en fiabilité : durée de vie de nombreux composants $\lambda = taux$ de défaillance $E(X) = \frac{1}{\lambda} = temps$ moyen entre défaillances

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

26/35

Loi normale



Loi extrêmement importante : souvent une très bonne approximation de la loi réelle

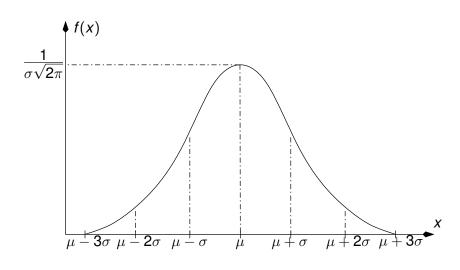
<u>Définition :</u> loi normale de paramètres μ et σ^2

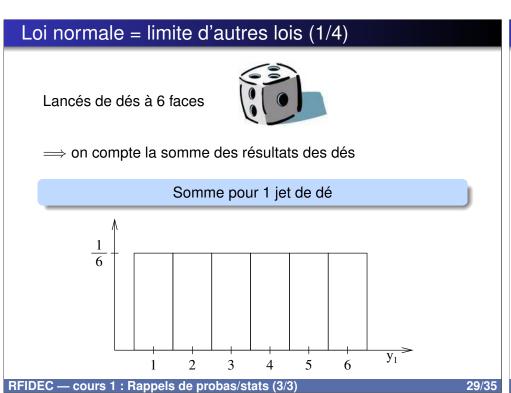
- notée $\mathcal{N}(\mu, \sigma^2)$
- s'applique pour des variables aléatoires continues
- ullet densité positive sur tout $\mathbb R$:

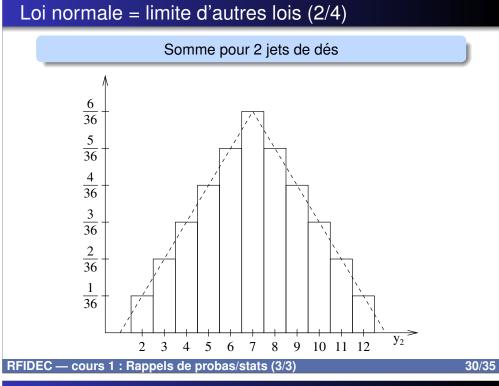
$$f(x) = \frac{1}{\sqrt{2\pi}.\sigma} \exp\left\{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right\}$$

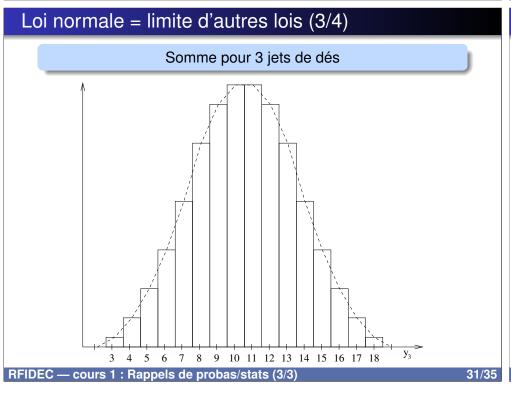
• $E(X) = \mu \quad V(X) = \sigma^2$

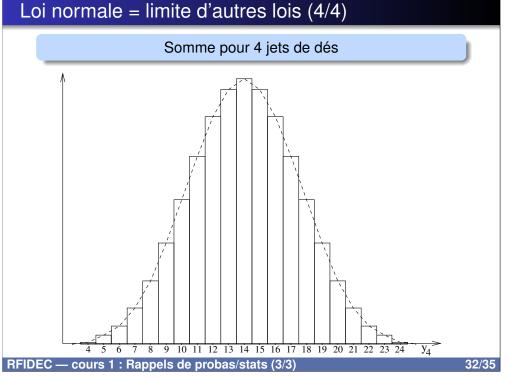
Fonction de densité de la loi normale











Loi normale en pratique

Théorème

 $X \sim \mathcal{N}(\mu; \sigma^2)$

Alors la variable Y = aX + b obéit à la loi $\mathcal{N}(a\mu + b; a^2\sigma^2)$.

⇒ toute transformée affine d'une variable aléatoire suivant une loi normale suit aussi une loi normale

Corollaire

• X une variable aléatoire obéissant à une loi $\mathcal{N}(\mu; \sigma^2)$

 $\Longrightarrow Z = \frac{X - \mu}{\sigma}$ suit la loi $\mathcal{N}(0; 1)$

• Z suit une loi normale centrée (à cause de la moyenne en 0) réduite (à cause du σ^2 égal à 1)

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

33/3

Loi normale bi-dimensionnelle

Définition : loi normale bi-dimensionnelle

- couple de variables (X, Y)
- densité dans \mathbb{R}^2 :

$$f(x,y) = \frac{1}{2\pi\sigma_x\sigma_y\sqrt{1-\rho^2}} \times$$

$$\exp\left\{-\frac{1}{2(1-\rho^2)}\left[(\frac{x-\mu_x}{\sigma_x})^2-2\rho\frac{(x-\mu_x)(y-\mu_y)}{\sigma_x\sigma_y}+(\frac{y-\mu_y}{\sigma_y})^2\right]\right\}$$

où $\rho = \frac{cov(X,Y)}{\sigma_X\sigma_Y} = coefficient de corrélation linéaire$

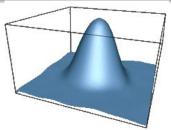
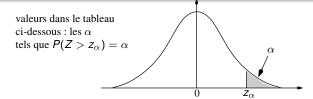


Table de la loi normale centrée réduite



z_{α}	0,00	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09
0,0	0,5000	0,4960	0,4920	0,4880	0,4840	0,4801	0,4761	0,4721	0,4681	0,4641
0,1	0,4602	0,4562	0,4522	0,4483	0,4443	0,4404	0,4364	0,4325	0,4286	0,4247
0,2	0,4207	0,4168	0,4129	0,4090	0,4052	0,4013	0,3974	0,3936	0,3897	0,3859
0,3	0,3821	0,3783	0,3745	0,3707	0,3669	0,3632	0,3594	0,3557	0,3520	0,3483
0,4	0,3446	0,3409	0,3372	0,3336	0,3300	0,3264	0,3228	0,3192	0,3156	0,3121
0,5	0,3085	0,3050	0,3015	0,2981	0,2946	0,2912	0,2877	0,2843	0,2810	0,2776
0,6	0,2743	0,2709	0,2676	0,2643	0,2611	0,2578	0,2546	0,2514	0,2483	0,2451
0,7	0,2420	0,2389	0,2358	0,2327	0,2297	0,2266	0,2236	0,2206	0,2177	0,2148
0,8	0,2119	0,2090	0,2061	0,2033	0,2005	0,1977	0,1949	0,1922	0,1894	0,1867
0,9	0,1841	0,1814	0,1788	0,1762	0,1736	0,1711	0,1685	0,1660	0,1635	0,1611
1,0	0,1587	0,1562	0,1539	0,1515	0,1492	0,1469	0,1446	0,1423	0,1401	0,1379
1,1	0,1357	0,1335	0,1314	0,1292	0,1271	0,1251	0,1230	0,1210	0,1190	0,1170
1,2	0,1151	0,1131	0,1112	0,1093	0,1075	0,1056	0,1038	0,1020	0,1003	0,0985
1,3	0,0968	0,0951	0,0934	0,0918	0,0901	0,0885	0,0859	0,0853	0,0838	0,0823
1,4	0,0808	0,0793	0,0778	0,0764	0,0749	0,0735	0,0722	0,0708	0,0694	0,0681
1,5	0,0668	0,0655	0,0643	0,0630	0,0618	0,0606	0,0594	0,0582	0,0571	0,0559
1,6	0,0548	0,0537	0,0526	0,0516	0,0505	0,0495	0,0485	0,0475	0,0466	0,0455
1,7	0,0446	0,0436	0,0427	0,0418	0,0409	0,0401	0,0392	0,0384	0,0375	0,0367
1,8	0,0359	0,0352	0,0344	0,0336	0,0329	0,0322	0,0314	0,0307	0,0301	0,0294
1,9	0,0287	0,0281	0,0274	0,0268	0,0262	0,0256	0,0250	0,0244	0,0239	0,0233

RFIDEC — cours 1 : Rappels de probas/stats (3/3)

34/35