Université Mohammed V de Rabat-Agdal – Faculté des Sciences – Département de Mathématiques et Informatique
Master Codes, Cryptographie et Sécurité de l'Information – 1ère année
2008 – 2009

Systèmes Dynamiques Chaotiques pour le Chiffrement

Sujet d'examen (3h),
en hommage à Edward Norton Lorenz (1917 - 2008)

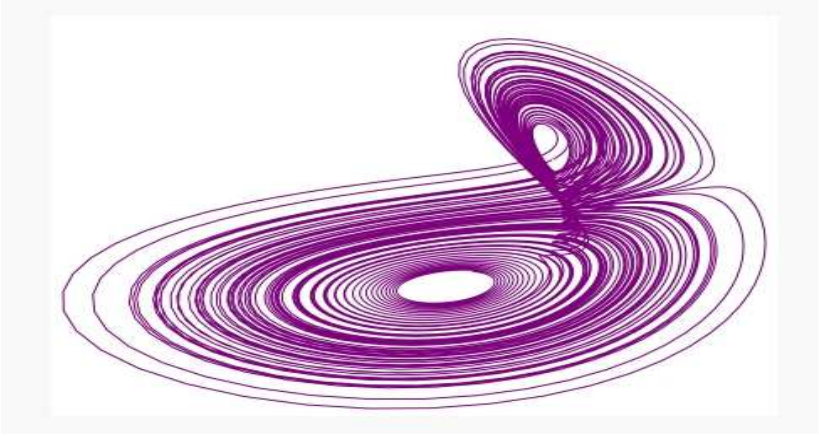
Première partie.

"Le battement d'ailes d'un papillon au Brésil peut-il déclencher une tornade au Texas ?" C'est par cette métaphore emblématique que le météorologue Edward Lorenz, en 1972, a réintroduit le phénomène d'infime sensibilité aux conditions initiales, phénomène mis en évidence numériquement lors de l'étude d'un modèle simplifié de turbulences atmosphériques s'écrivant (système 1):

$$\begin{cases} \dot{x} &= a(y-x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= -bz + xy \end{cases}$$

a, *r* et *b* étant des paramètres strictement positifs.

En dehors des points d'équilibre, des solutions à conditions initiales situées sur l'axe des *z* ou encore quelques familles de solutions périodiques, le comportement qualitatif des solutions du modèle de Lorenz demeure globalement un mystère. Les simulations numériques (encore faut-il y croire .. heureusement qu'il y a un certain lemme de l'ombre!) montrent qu'à partir d'une certaine valeur critique de *r*, le système devient pathologiquement sensible aux variations des conditions initiales, manifestant dès lors une dynamique – bien que déterministe – totalement erratique et imprévisible. A noter tout de même que, géométriquement parlant, presque toutes les orbites semblent "remplir" remarquablement le même domaine. Une telle figure est illustrée ci-après et reste sans doute l'une des figures maîtresses du fameux "effet papillon" de Lorenz …



Dans ce qui suit, et évitant tout recours à un appareil mathématique dissuasif, les candidats sont alors invités à procéder à une étude qualitative partielle du modèle, avec comme seuls pré-requis: quelques rudiments de la théorie qualitative des équations différentielles et … un minimum de curiosité!

1. *Symétrie orbitale:*
Vérifier que si *(x(t),y(t),z(t))* est une solution du modèle, alors il en est de même pour *(-x(t),-y(t),z(t))*.

2. *Un système dissipatif:*
Chercher la divergence du champ de vecteurs et en déduire qu'il s'agit d'un système dissipatif.

3. *Variétés invariantes triviales:*
Vérifier qu'une solution aux conditions initiales situées sur l'axe des *z* tend vers l'origine quant *t* tend vers l'infini. En déduire que l'ensemble $x = y = 0$ est invariant.

4. *(Bifurcation de) Points d'équilibre:*
Montrer que pour $0 < r \leq 1$, l'origine (0,0,0) est le seul point d'équilibre du système et que si $r > 1$, il y a apparition de 2 autres points d'équilibre donnés par

$$\left(\pm\sqrt{b\,(r-1)}, \pm\sqrt{b\,(r-1)}, r-1\right)$$

5. *Attraction – Stabilité:*
   a) Donner la linéarisation du système au voisinage de l'origine sous forme (système 2)

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

   où *A* est une matrice carrée constante de taille 3.
   b) Vérifier que

$$Sp\,(A) = \{-b\} \cup \left\{\lambda\ tq\ \lambda^2 + (a+1)\,\lambda + a\,(1-r) = 0\right\}$$

   c) Discuter alors de la dimension des variétés stables et instables au voisinage de l'origine.
   d) Montrer en utilisant le critère de Routh-Hurwitz que l'origine, en tant que point d'équilibre du système 2, est exponentiellement stable ssi $0 < r < 1$.
   e) Que peut-on alors conclure quant à l'origine, en tant que point d'équilibre du système 1 ? Justifier en rappelant le théorème adéquat.
   f) En utilisant la fonction

$$\Gamma(x,y,z) := \frac{1}{2}\left(rx^2 + a\left(y^2 + z^2\right)\right)$$

   comme fonction de Lyapounov candidate, retrouver une condition suffisante sur les paramètres pour la stabilité asymptotique de l'origine.

6. *Cas dégénéré:*
   Dans cette partie, le paramètre *r* prend la valeur critique 1.
   a) Vérifier que le système 2 est la réunion de deux sous-systèmes découplés, l'un étant bidimensionnel (en *x* et *y*) de matrice *B*, l'autre unidimensionnel (en *z*).
   b) Chercher les valeurs propres de *B* et les sous-espaces propres correspondants. En déduire que *B* est diagonalisable.
   c) Procéder à la diagonalisation de *B* (trouver *P* tq $P^{-1}BP = D$).
   d) Calculer $exp(tB)$ et donner la solution générale du système

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = B \begin{pmatrix} x \\ y \end{pmatrix}$$

   e) En déduire la solution générale du système 2.
   f) Discuter du comportement qualitatif de ces solutions en fonction des conditions initiales.
   g) Dans quels cas peut-on généraliser ce comportement au système de Lorenz au voisinage de sa position d'équilibre? Justifier.

7. *Solutions périodiques:*

Admettons maintenant qu'à tout instant $x = y$, ce qui n'est vrai en toute rigueur que si *a* tend vers l'infini d'après la première équation du modèle de Lorenz.

   a) Vérifier que le système de Lorenz se réduit au système bidimensionnel

$$\begin{cases} \dot{x} &= (r - z - 1)y \\ \dot{y} &= -bz + y^2 \end{cases}$$

   b) En utilisant le critère adéquat, chercher alors le type de domaines candidats à abriter des solutions périodiques.

8. *Un peu d'intuition!*
   a) Essayer de rassembler toutes les données qui porteraient à croire que la figure décrite par les solutions du modèle de Lorenz correspond à un attracteur étrange.
   b) Obtiendrait-on la même allure pour l'attracteur de Lorenz en simulant le modèle à partir de la même condition initiale et pour le même temps d'évolution, mais en utilisant différentes méthodes d'intégration numérique ? Et si on utilise cette fois-ci les mêmes données ci-dessus (condition initiale, temps d'évolution, schéma numérique d'intégration), mais différentes machines ? Par machine, nous entendons le couple ordinateur + logiciel.

Deuxième partie.

Concevoir un cryptosystème utilisant le flot du modèle de Lorenz pour crypter/décrypter

- un message texte,
- une image numérique.

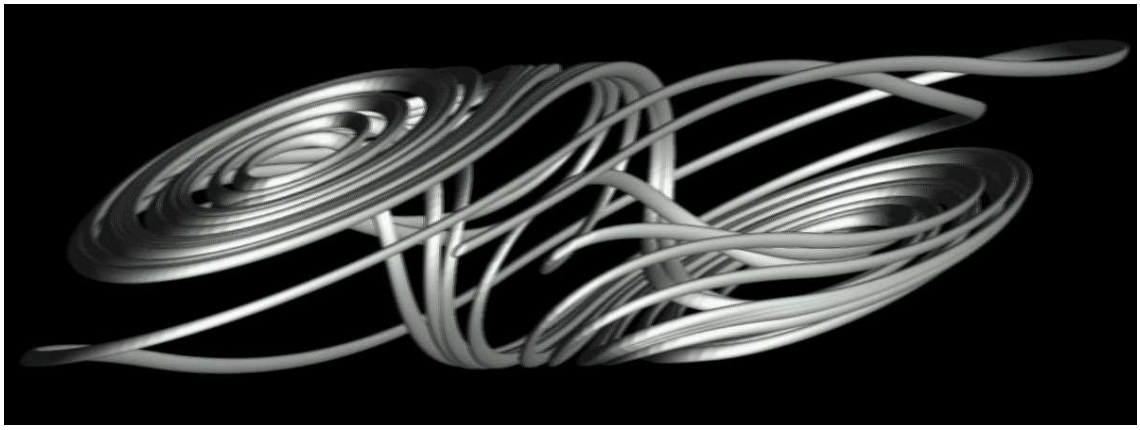
Université Mohammed V de Rabat-Agdal – Faculté des Sciences – Département de Mathématiques et Informatique
Master Codes, Cryptographie et Sécurité de l'Information – 1ère année
2009 – 2010

Systèmes Dynamiques Chaotiques pour le Chiffrement

Sujet d'examen (3h) – Juillet 2010

Première partie.

L'événement qui a conduit à la découverte du fameux circuit de Léon Chua a eu lieu un après-midi du mois d'octobre 1983, au laboratoire du Professeur T. Matsumoto de l'université Waseda, le lendemain de l'arrivée de l'auteur à Tokyo pour un séjour scientifique de la Japan Society for Promotion of Science. Dans un coin du laboratoire orchestré d'instruments électroniques, il a dû assister à une live-démonstration de la première réalisation électronique du monde du modèle de Lorenz, couronnement d'un travail collectif de plus d'un an de l'Equipe de recherche de Matsumoto. Ce petit chef-d'œuvre électronique frôlait la perfection que l'on jugeait inutile l'invention d'un nouveau circuit. En fait, à cette époque, seuls deux modèles autonomes tridimensionnels étaient acceptés comme étant chaotiques : le modèle de Lorenz (cf. examen de l'année dernière) et celui de Rössler dont la non-linéarité est une fonction de deux variables. Cependant, en remarquant ce jour-là – alors qu'il était déjà l'heure de dormir ! – que le mécanisme derrière le comportement chaotique du modèle de Lorenz et celui de Rössler était essentiellement la présence d'au moins deux équilibres instables, Léon Chua entama la conception d'un circuit plus simple – et donc plus robuste – exhibant un tel comportement. En moins d'une heure, guidé par un flair de deux décennies d'exposition quotidienne à des circuits RLC non linéaires, et en procédant par élimination, l'auteur a réussi à schématiser (sur des enveloppes usées !) un ensemble de huit circuits candidats, duquel va émaner un assemblage qui, dès le lendemain matin, soumis au Prof. Matsumoto et programmé sur son ordinateur, va laisser toute l'Equipe stupéfaite : un attracteur étrange !



Le circuit qui portera le nom de Léon Chua va vite devenir un paradigme universel du chaos et déclencher aussitôt une avalanche de publications qui n'a cessé de croître jusqu'à nos jours (cliquer par exemple sur www.eecs.berkeley.edu/~chua/circuitrefs.html). Outre ses applications dans différents domaines tels les réseaux de neurones, le traitement d'images ou même la composition musicale, et en tant que source physique de signaux pseudo-aléatoires, son importance dans des études de synchronisation telle la sécurité de systèmes de communication est avérée. Les équations (généralisées) sont données par (système 1)*:*

$$\left\{ \begin{array}{rcl} \dot{x} & = & \alpha\,(y - f\,(x)) \\ \dot{y} & = & x - y + z \\ \dot{z} & = & -\beta y \end{array} \right.$$

où α et β sont des paramètres réels strictement positifs et f une fonction *impaire* de *x*, suffisamment régulière. C'est la représentation mathématique de la courbe caractéristique de la diode du circuit …

Dans ce qui suit, les candidats sont alors invités à procéder à une étude qualitative très partielle du modèle ; l'étude complète étant compliquée, voire impossible, certaines questions nécessitant l'usage de la machine, nous ramèneront le sujet à l'étude d'un modèle bidimensionnel qui lui est intimement lié.

1. *Symétrie orbitale:*
Vérifier que si *(x(t),y(t),z(t))* est une solution du modèle, il en est de même pour – *(x(t), y(t), z(t))*. Conclure.

2. *Un système dissipatif:*
Chercher la divergence du champ de vecteurs et en déduire une condition suffisante sur *f* pour que le système soit dissipatif. Comment cela se traduit-il sur l'évolution d'un volume fini de conditions initiales de l'espace des phases ?

3. *Solutions triviales:*
Sur un intervalle de temps assez petit, donner la famille de solutions aux conditions initiales situées sur l'intersection de la courbe C_f avec la première bissectrice du plan *(x,y)*.

4. *(dénombrement de) Points d'équilibre:*
Montrer que le système 1 admet autant de points d'équilibre que de zéros pour la fonction *f*, l'origine étant toujours un équilibre.

5. *Stabilité de l'origine:*
Il était tout à fait normal que Léon Chua conçoive son circuit de telle manière à ce que ses points d'équilibre soient instables …

a) Donner la linéarisation du système au voisinage de l'origine sous forme :

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

où *A* est une matrice carrée de taille 3.

b) Sans chercher *Sp(A)*, envisager une distribution des valeurs propres qui pourra déstabiliser l'origine.

c) Relever la difficulté (voire l'impossibilité) de la construction au voisinage de l'origine d'une fonction de Lyapounov de la forme

$$\Gamma(x,y,z) := \frac{1}{2}\left(ax^2 + by^2 + cz^2\right)$$

a, *b* et *c* étant des paramètres strictement positifs.

6. *Circuit RLC:*

Dans cette partie, on revient à l'ancêtre du circuit de Chua – étape nécessaire avant la conception de tout circuit chaotique, et ce en supprimant une variable (un condensateur), obtenant ainsi un circuit oscillant modélisé par le système de Liénard suivant :

$$\begin{cases} \dot{x} &= y - f(x) \\ \dot{y} &= -x \end{cases}$$

a) En considérant d'abord le cas simple où *f* est linéaire : *f(x) = kx*, *k* > 0, chercher les valeurs propres associées à ce système et discuter en fonction de *k* la nature de l'origine en tant que point d'équilibre. Conclure alors en sa stabilité.

b) En considérant maintenant le cas général où la caractéristique *f* est non linéaire, vérifier que la linéarisation du système autour de son unique point d'équilibre est définie par la matrice :

$$\begin{pmatrix} -f'(0) & 1 \\ -1 & 0 \end{pmatrix}$$

En donner les valeurs propres et conclure en la nature du point d'équilibre en fonction de *f'*(0), ainsi qu'en sa stabilité en tant qu'équilibre du système de Liénard.

c) Confirmer le résultat de stabilité (asymptotique) en construisant une fonction de Lyapounov de la forme :

$$\Gamma(x,y) = \frac{1}{2}\left(x^2 + y^2\right)$$

d) Vérifier qu'en posant

$$f(x) := \int_0^x g(t)\,dt$$

le système de Liénard s'écrit sous la forme d'une équation différentielle scalaire de second ordre donnée par :

$$\ddot{x} + g(x)\,\dot{x} + x = 0$$

e) En rappelant le théorème adéquat, donner des conditions suffisantes pour que le système de Liénard admette au moins une solution périodique, voire un cycle limite.

f) Le circuit de van der Pol correspond au cas particulier – mais très important – où *f(x)* := $x^3 - x$. Reprendre les questions b-c-d-e) dans ce cas.

g) En appliquant le critère de Bendixson au cas de van der Pol, chercher le type de domaines susceptibles d'abriter le cycle limite du circuit.

Deuxième partie.

Concevoir un cryptosystème à base de la méthode de Baptista utilisant le flot chaotique du modèle de Léon Chua pour crypter/décrypter

- un message texte,
- une image numérique.

Quels seraient les points faibles d'un cryptosystème à base du circuit de van der Pol ?

Université Mohammed V de Rabat-Agdal – Faculté des Sciences – Département de Mathématiques et Informatique
Master Codes, Cryptographie et Sécurité de l'Information – 1ère année
2010 – 2011

Systèmes Dynamiques Chaotiques pour le Chiffrement

Sujet d'examen (3h)

Premier problème

Une équation de Liénard est une équation différentielle du type

$$\ddot{x} + f(x)\dot{x} + g(x) = 0$$

avec f et g de classe C^1 sur IR, f paire et g impaire.

1. Vérifier que le changement de variable

$$y := \dot{x} + F(x) \ , \quad \text{où} \quad F(x) := \int_0^x f(t)dt$$

permet d'écrire l'équation de Liénard sous forme d'un système bidimensionnel d'équations différentielles ordinaires en x et y.

2. Le cas où $g(x) = x$ est particulièrement intéressant et sera considéré dans toute la suite. Vérifier que l'on a un unique point d'équilibre.

3. Procéder à la linéarisation du système au voisinage de ce point.

4. Risque-t-on un cas dégénéré ?

5. Donner le polynôme caractéristique associé à la matrice du système linéarisé.

6. En utilisant le critère adéquat, donner une condition nécessaire pour la stabilité asymptotique du point d'équilibre.

7. Rappeler le théorème de Hartman-Grobman et discuter sa validité dans notre cas.

8. Discuter du type du point d'équilibre pour le système linéarisé.

9. Même question pour le point d'équilibre en tant qu'équilibre du système de Liénard.

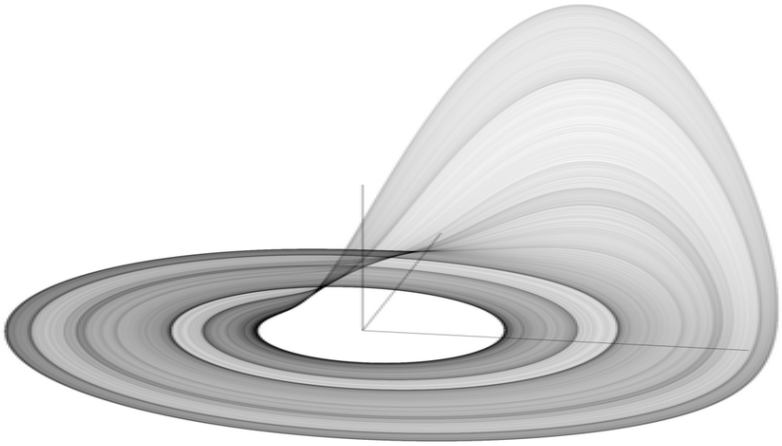
10. Discuter de la stabilité du point d'équilibre en utilisant la méthode de Lyapounov.

11. Appliquer à l'oscillateur de van der Pol en tant que cas particulier des systèmes de Liénard.

12. En utilisant le théorème adéquat, montrer que l'oscillateur de van der Pol admet un cycle limite.

Deuxième problème

Otto Rössler, en 1976, et dans un but purement théorique, à la quête d'un nouvel attracteur étrange, avait proposé un modèle non linéaire dont les équations s'avérèrent pourtant très utiles dans la modélisation de l'équilibre dans certaines réactions chimiques. L'article original de Rössler mentionne que son modèle a été conçu pour fonctionner d'une façon similaire à celui de Lorenz, mais devrait être plus simple à analyser : il ne présente en fait qu'une seule spirale.



Dans un souci purement pédagogique, nous allons considérer ici un modèle légèrement modifié de Rössler, défini par le système tridimensionnel suivant :

$$\begin{cases} \dot{x} &= -y - z \\ \dot{y} &= x + y \\ \dot{z} &= x + z\,(x - \varepsilon) \end{cases}$$

1. Dites en quoi le modèle de Rössler est plus simple que celui de Lorenz.

2. Sous quelle condition le système de Rössler est dissipatif ?

3. Déterminer les deux points d'équilibre du système.

4. Pour quelle valeur du paramètre de contrôle ε les deux points d'équilibre se confondent-ils ?

5. Linéariser dans ce cas le système au voisinage de son unique point d'équilibre.

6. Etudier alors les propriétés de stabilité du point d'équilibre du système linéarisé.

7. Chercher la solution générale du système linéarisé et étudier ses propriétés.

8. Peut-on généraliser ce comportement au système de Rössler ? Justifier.

9. Dans quels cas le modèle de Rössler peut-il être chaotique ?

10. Expliquer enfin comment l'on peut utiliser l'attracteur étrange de Rössler pour crypter/décrypter
    - un message texte,
    - une image numérique.

Université Mohammed V de Rabat-Agdal – Faculté des Sciences – Département de Mathématiques
Master Codes, Cryptographie et Sécurité de l'Information – 1ère année
2011 – 2012

Systèmes Dynamiques Chaotiques pour le Chiffrement

Sujet d'examen (3h) – Juillet 2012

Première partie.

Considérons le modèle prédateur-proie de Lotka-Volterra

$$(1) \qquad \begin{cases} \dot{x} &= ax - bxy \\ \dot{y} &= -cy + dxy \end{cases}$$

où, pour simplifier les calculs, on va supposer que $a = b = c = d = 1$.

1. Justifier que ce système d'équations représente (de manière très simplifiée) l'interaction entre une population de proie et une population de prédateurs, ou plus généralement entre un activateur et un inhibiteur.

2. Déterminer les points d'équilibre du système (1). Interpréter.

3. Montrer que les axes $\{x = 0\}$ et $\{y = 0\}$ sont invariants par le flot du système, et en déduire que le quadrant $\{x > 0 , y > 0\}$ est également invariant par le même flot.

4. Linéariser le système au voisinage de chaque point d'équilibre, préciser la nature de ces derniers et représenter les trajectoires des systèmes linéaires ainsi obtenus.

5. Discuter de la stabilité de ces points en tant qu'équilibres du système (1).

6. Montrer que la fonction $\Gamma(x,y) = \varphi(x)\varphi(y)$, où $\varphi(x) = xe^{-x}$, est une quantité conservée pour le système (1), en d'autres termes, sa dérivée de Lie le long d'une solution est nulle. Conclure en la stabilité du point d'équilibre non nul par la méthode de Lyapounov.

7. En utilisant cette quantité conservée, montrer que toute trajectoire située dans le quadrant $\{x > 0 , y > 0\}$ est bornée.

8. Vérifier que la restriction de la fonction Γ au segment $\{0 \leq x \leq 1, y = 1\}$ est injective.

9. En déduire que toute solution dont la trajectoire appartient au quadrant $\{x > 0 , y > 0\}$ est périodique (mise à part la solution stationnaire représentée par l'équilibre non nul).

10. Symétrie de réversibilité : on note S la transformation

$$\begin{array}{rccc} S : & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \longmapsto & (y,x) \end{array}$$

Vérifier que, si $u(t) = (x(t),y(t))$ est une solution du système (1), alors $S(u(-t))$ en est encore une solution.

11. On note D la droite $\{x = y\}$. Montrer, par un argument basé uniquement sur la symétrie mise en évidence à la question précédente, que toute solution du système (1) dont la trajectoire coupe deux fois la droite D est périodique. En déduire, en utilisant le critère de Bendixson, que toute solution dont la trajectoire appartient au quadrant $\{x > 0, y > 0\}$ et qui n'est pas égale à l'équilibre non nul est périodique.

12. On considère le modèle de Lotka-Volterra perturbé par des termes de saturation :

$$(2) \qquad \left\{ \begin{array}{rcl} \dot{x} & = & x\,(1 - y - \alpha x) \\ \dot{y} & = & y\,(x - 1 - \alpha y) \end{array} \right.$$

où α est un paramètre strictement positif. En quoi le système (2) constitue-t-il un modèle plus pertinent que le précédent ? Déterminer l'unique point d'équilibre du système dans le quadrant $\{x > 0, y > 0\}$. Exprimer le système linéarisé en cet équilibre et montrer que pour α suffisamment petit il s'agit d'un foyer attractif. En rappelant le théorème adéquat, conclure en sa stabilité (asymptotique) en tant qu'équilibre du système (2). De quel bifurcation s'agit-il lorsque α s'annule ?

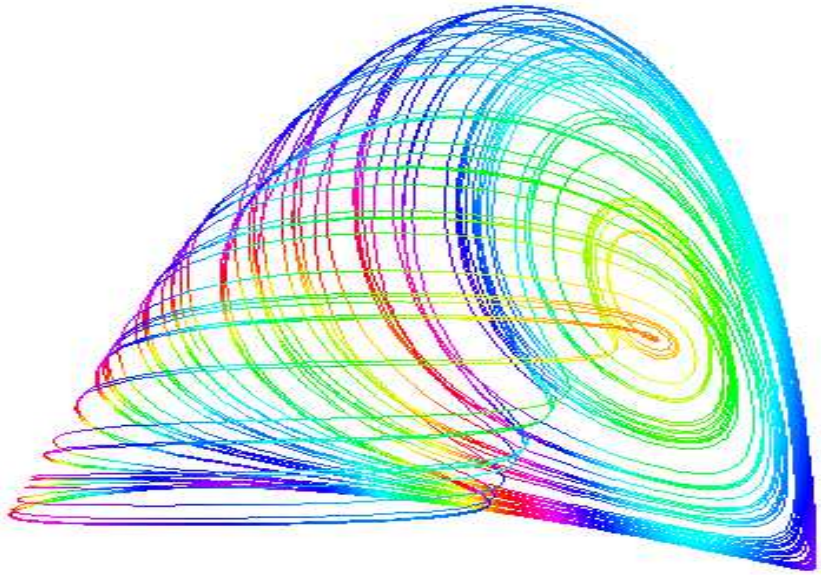
Deuxième partie.

Considérons maintenant le modèle plus élaboré de trois espèces interagissant dans un mode prédateur-proie, selon une réponse fonctionnelle logistique de type Verhulst (1838) pour la proie x et une réponse fonctionnelle de type Gause (1935) pour le prédateur y et pour le super-prédateur z :

$$(3) \qquad \left\{ \begin{array}{rcl} \dot{x} & = & a\left(1 - \frac{\lambda}{a}x\right)x - bx^k y \\ \dot{y} & = & dx^k y - cy - ey^p z \\ \dot{z} & = & (fy^p - g)\,z \end{array} \right.$$

C'est le modèle de Volterra-Gause sous sa forme la plus générale. Le paramètre a représente le taux de croissance maximum d'une proie en l'absence de prédateur et a/λ¸ la " population limite ". Le taux de prédation du prédateur représenté par une réponse fonctionnelle de type Gause s'écrit : x^k. Celui du super-prédateur est représenté par une réponse fonctionnelle du même type qui s'écrit : y^p. Le paramètre b est le taux maximum de prédation. Le paramètre c est le taux de mortalité naturelle du prédateur. Le paramètre d est le taux maximum de croissance du prédateur en l'absence de super-prédateur. Les paramètres e, f et g sont respectivement similaires à b, d et à c excepté que dans ce cas, le prédateur y est la proie du super-prédateur z.
Pour des valeurs bien choisies des paramètres, les simulations numériques du modèle résultent en un formidable attracteur étrange sous forme d'une coquille d'escargot, ce qui analytiquement peut être mis en évidence en considérant le diagramme de bifurcation du modèle dédimensionné exhibant une cascade de (dé)doublement de période induite par un paramètre fonction de λ, a, c et d.

C’est la signature du chaos d’une chaîne alimentaire à trois niveaux :



Malgré son apparence familière, cet attracteur se comporte d’une manière complexe. Partant de n’importe quelle condition initiale prise dans le premier octant, le flot se dirige vers un point d’équilibre *I* situé sur l’axe des *x*, et qui est attractif suivant cette direction propre. Suivant ensuite sa direction propre répulsive, le flot atteint le bassin d’attraction d’un autre point d’équilibre, situé sur le plan $z = 0$ et s’y comportant comme un foyer attractif, et tourne autour de ce point. Cependant, comme ce point possède une direction propre répulsive, le flot quitte ce plan et se dirige vers le bassin d’attraction d’un tout autre équilibre tridimensionnel possédant une direction attractive. Mais, comme ce point se comporte comme un foyer répulsif, le flot tourne autour de ce point en s’éloignant dans la direction du point *I* qui possède une direction propre attractive suivant l’axe des *z*. Le flot est alors “réinjecté” par ce “point-selle”.

Question 1.
Déterminer *I* et écrire la matrice jacobienne du système (3) en ce point et en l’origine. En déduire les valeurs propres pour chaque cas et conclure en la stabilité des deux points d’équilibre.

Question 2.
Expliquer comment pourrait-on concevoir un cryptosystème utilisant le flot chaotique du modèle de Volterra-Gause pour crypter/décrypter

- un message texte,
- une image numérique.

Université Mohammed V de Rabat-Agdal – Faculté des Sciences – Département de Mathématiques
Master Codes, Cryptographie et Sécurité de l'Information – 2ème semestre
2012 – 2013

Systèmes Dynamiques Chaotiques pour le Chiffrement

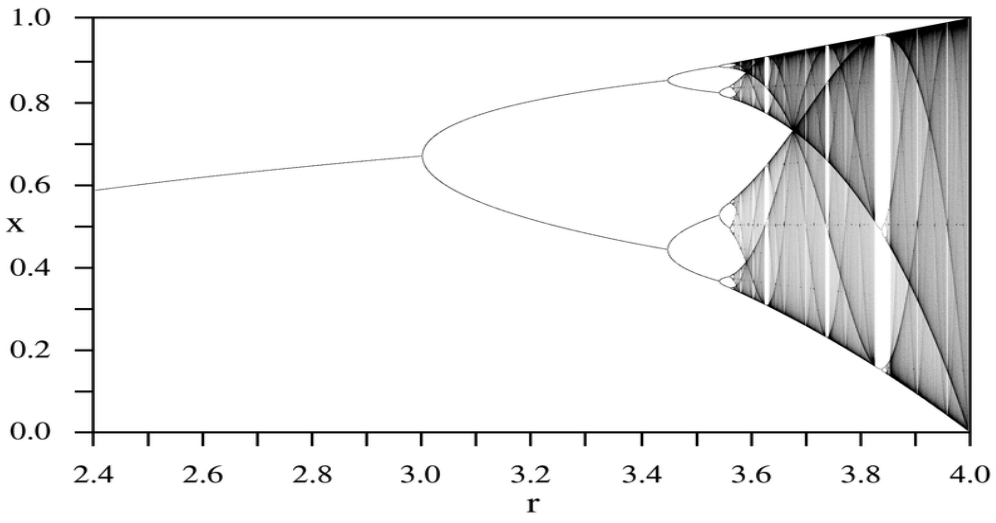
Sujet d'examen (3h) – Juin 2013

Si l'on trouve que le sujet de l'épreuve n'était pas prévisible, c'est tout à fait normal dans un examen sur la théorie du chaos !

Première partie.
En dynamique des populations, les premiers biologistes férus de mathématiques ont commencé par créer des modèles simples pour comprendre cette évolution, le modèle le plus simple qui en émane étant un schéma malthusien : une démographie croissant indéfiniment, sans aucune contrainte alimentaire, morale ou territoriale. Loin d'être réaliste, puisqu'il ne tient pas compte des dures réalités de l'existence, le modèle fut encore élaboré en incorporant un facteur de freinage de croissance non linéaire, d'où la *suite logistique*

$$\begin{cases} x_0 \in]0,1[\ , \\ x_{n+1} = r x_n (1 - x_n) \ , \quad n \geq 0 \end{cases}$$

Ce modèle fut popularisé en 1976 par Robert May, physicien de Princeton devenu biologiste, et qui est un des personnages clés dans l'histoire de la prise de conscience par les scientifiques de l'une des plus belles bifurcations tenant lieu de "route vers le chaos". En fait, selon le taux de croissance *r*, que l'on suppose positif, la population peut converger pour se stabiliser au fil des années, être soumise à oscillations ou encore être la proie d'une dynamique complètement erratique et chaotique. Le diagramme de bifurcation ci-dessous résume qualitativement ce comportement :



1. Que représente “l’axe des ordonnées” dans le diagramme ?
   (Utiliser rigoureusement des termes de la théorie des systèmes dynamiques).

2. En cas de convergence, chercher les limites possibles de la suite logistique. En déduire les valeurs de *r* pour lesquelles une extinction de la population est inévitable, quel que soit son effectif initial.

3. D’après le diagramme de bifurcation, donner une estimation de l’intervalle sur lequel

   a) la population finit par se stabiliser autour d’une valeur fixe ;
   b) la population finit par osciller entre deux valeurs ;
   c) la population finit par osciller entre quatre valeurs.

   De quelle bifurcation s’agit-il ?

4. A partir de quelle valeur approximative le chaos commence-t-il à s’installer ? Donner la valeur de *r* pour laquelle le chaos est total et préciser l’attracteur étrange correspondant.

5. Toujours d’après le diagramme, existe-t-il des valeurs isolées de *r* appartenant à la région chaotique, mais correspondant à un comportement de la suite qui ne l’est pas ? En donner approximativement une valeur remarquable et préciser dans ce cas la période des oscillations.

6. Le diagramme de bifurcation de la suite logistique est souvent représenté pour $r \leq 4$. Que se passe-t-il quand $r > 4$?

7. Pourrait-on enfin estimer à l’œil nu la constante de Feigenbaum, à savoir la limite du rapport de la longueur de deux intervalles des valeurs de *r* correspondant à deux bifurcations successives ?

Deuxième partie.

On considère la suite de terme général u_n défini par

$$u_n = Frac(10^n \pi) = 10^n \pi - E\,(10^n \pi) \quad , \quad n \in \mathbb{N}$$

où *E*(.) désigne la partie entière.

1. Sachant que $\pi \approx 3{,}14159\ldots$, donner les premières valeurs u_0, u_1 et u_2, au troisième décimal près.

2. Vérifier que la suite $(u_n)_{n\geq 0}$ ne peut être périodique ($u_m \neq u_n$ pour tout $m \neq n$).

3. Quelles hypothèses relevant de la théorie des nombres, irrationnels en général et π en particulier, permettraient de conjecturer que la suite $(u_n)_{n\geq 0}$ est dense dans l’intervalle [0,1] ?

4. Expliquer alors en quoi le développement décimal d’un irrationnel (poussé à un ordre aussi élevé que possible) serait mathématiquement plus avantageux pour la conception numérique d’un cryptosystème chaotique que l’utilisation d’une simple suite récurrente.

Troisième partie.
On se propose de montrer que l'application

$$\begin{array}{rccc} f\ : & [0,1] & \longrightarrow & [0,1[\\ & x & \longmapsto & Frac\,(10x) \end{array}$$

est chaotique. Rappelons qu'il n'y a pas de définition universellement adoptée du chaos dans la communauté scientifique. Nous allons ici adopter la définition proposée par Robert Devaney (Université de Boston) qui semble avoir l'assentiment de la majorité des spécialistes de la théorie qualitative des équations différentielles. Cette définition du chaos fait intervenir trois notions : la transitivité, la sensibilité aux conditions initiales et la densité des points périodiques. Rappelons d'abord le sens précis de ces notions :

Une fonction f définie sur un intervalle I de IR à valeurs dans I est dite transitive si pour toute paire de points x et $y \in I$ et tout $\varepsilon > 0$, il existe un $z \in]x - \varepsilon\ ,\ x + \varepsilon[$ et n entier tels que $f^n(z) \in]y - \varepsilon\ ,\ y + \varepsilon[$.

Nous dirons que f est sensible aux conditions initiales s'il existe un $\delta > 0$ tel que pour tout $x \in I$ et tout $\varepsilon > 0$, il existe $y \in]x - \varepsilon\ ,\ x + \varepsilon[$ et n entier tels que $|f^n(x) - f^n(y)| > \delta$.

Enfin, un point x est dit périodique si $f^n(x) = x$ pour un entier $n \geq 2$.

Nous avons donc la définition suivante :
f est une fonction chaotique si

(i) f est transitive ;
(ii) Per(f), l'ensemble des points périodiques de f, est dense dans I ;
(iii) f est sensible aux conditions initiales.

1. Donner au troisième décimal près $f^n(\pi)$ pour $n = 1$ et $n = 2$.

2. Exprimer de manière simple $f^n(x)$.

3. Caractériser les points périodiques de f. En déduire la propriété (ii) pour f.

4. Montrer que f est transitive. On pourra construire explicitement z à partir de x et y, sinon se référer au résultat 3) de la deuxième partie, que l'on peut admettre.

5. Montrer la sensibilité aux conditions initiales de la fonction f et conclure. Là-aussi, on peut construire y à partir de x. Ne pas hésiter à représenter les réels en question sous la forme

$$0,d_1d_2d_3\ldots d_n\ldots$$

où d_i est un chiffre entre 0 et 9.

Université Mohammed V de Rabat-Agdal – Faculté des Sciences – Département de Mathématiques
Master Codes, Cryptographie et Sécurité de l'Information – 2ème semestre
2013 – 2014

Systèmes dynamiques chaotiques pour le chiffrement

Sujet d'examen (3h) – Juin 2014

Première partie.
On se propose d'étudier les bifurcations de la fonction logistique

$$\begin{array}{rccc} f_r : & [0,1] & \longrightarrow & [0,1] \\ & x & \longmapsto & rx(1-x) \end{array}$$

$r \in [0,4]$, et ce via l'étude de la fonction

$$\begin{array}{rccc} g_s : & [-\frac{r}{2}, \frac{r}{2}] & \longrightarrow & [-\frac{r}{2}, \frac{r}{2}] \\ & x & \longmapsto & x^2 + s \end{array}$$

$s \in IR$, fonction qui est plus simple et qui est topologiquement équivalente à f_r dans le sens où il existe un homéomorphisme

$$\begin{array}{rccc} \varphi_r : & [0,1] & \longrightarrow & [-\frac{r}{2}, \frac{r}{2}] \\ & x & \longmapsto & \frac{r}{2}(1-2x) \end{array}$$

tel que $g_s \circ \varphi_r = \varphi_r \circ f_r$. Les deux applications f_r et g_s auront alors le même comportement qualitatif ; elles ont, entre autres, le même nombre de points fixes et d'orbites périodiques.

Rappelons pour commencer qu'un point fixe d'une application f est un point invariant par f, c.-à-d. $f(p) = p$. Si f est de classe C^1 et sa dérivée vérifie $|f'(p)| < 1$ (resp. $|f'(p)| > 1$), p est attractif (resp. répulsif). Si $|f'(p)| = 1$, on ne peut conclure. p est alors attractif (resp. répulsif) si la suite des itérées $(f^n(x))_{n \in IN}$, x voisin de p, converge vers p (resp. s'en éloigne). Il se peut aussi que la suite $(f^n(x))_{n \in IN}$ tende à osciller entre deux ou plusieurs valeurs différentes $u_1, u_2, \ldots, u_n$. On parle alors d'orbites périodiques, et l'on a

$$f(u_i) = u_{i+1} \ , \quad 1 \leq i \leq n \ , \quad avec \quad u_{n+1} = u_1$$

1) Montrer que les applications f_r et g_s sont topologiquement équivalents par l'homéomorphisme φ_r (qui est aussi un difféomorphisme) lorsque r et s sont liés par la relation suivante :

$$s = \frac{r}{2}(1 - \frac{r}{2})$$

On suppose désormais que cette relation est vérifiée et que l'on a $g_s \circ \varphi_r = \varphi_r \circ f_r$.

2) Vérifier que si p est un point fixe de f_r, alors $\varphi_r(p)$ est un point fixe de g_s.

3) Montrer que les points fixes de f_r et g_s sont de même nature.

Nous nous intéressons maintenant aux bifurcations de l'application g_s pour $s \in [-2,1/4]$ (et par conséquent celles de l'application f_r pour $r \in [0,4]$). Nous admettons le critère suivant : g_s a une bifurcation en s_0 si et seulement si il existe un point fixe p de g_{s0} tel que la dérivée $g_{s0}'(p) = \pm 1$.

4) a) Montrer en utilisant le critère que l'application g_s admet une première bifurcation en $s = 1/4$.

b) Montrer en l'occurrence que g_s admet un point fixe p en $s = 1/4$, deux point fixes p_1 et p_2 lorsque $s < 1/4$ et aucun point fixe pour $s > 1/4$.

c) Etudier la nature de p_1 et p_2 en fonction de s.

d) En déduire une deuxième bifurcation de g_s en $s = -3/4$ et confirmer ce fait en utilisant le critère.

5) a) En admettant que la bifurcation en $s = -3/4$ donne naissance à une orbite périodique de période 2, nous nous intéressons aux points fixes de g_s^2. Chercher ces points fixes pour $s < -3/4$.

b) En déduire une troisième bifurcation de g_s en $s = -5/4$ en appliquant le critère à l'application g_s^2.

6) Rappelant que les applications f_r et g_s sont topologiquement équivalentes, calculer les valeurs de bifurcation de f_r à partir de celles trouvées pour g_s.

7) On dit que f_r admet une bifurcation selle-nœud (resp. de (dé)doublement de période) en r_0 s'il existe un point fixe p de f_{r0} tel que la dérivée $f_{r0}'(p) = 1$ (resp. $f_{r0}'(p) = -1$).

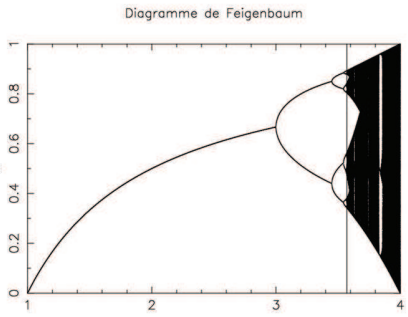
a) Montrer que la première bifurcation de f_r est de type selle-nœud et que c'est l'unique bifurcation de ce type.

b) Montrer que la deuxième et la troisième bifurcation de f_r sont des bifurcations de (dé)doublement de période.

8) En admettant que pour $r = 3,82$, l'application f_r^3 admet trois points fixes, rappeler le théorème de Sharkovski et en déduire que l'application logistique est chaotique.

9) On sait donc qu'une cascade de bifurcations par (dé)doublement de période est une route vers le chaos. Expliquer brièvement ce phénomène en relevant les traits principaux du chaos déterministe.

10) On admet que la valeur r_∞ à partir de laquelle le chaos s'installe (point de Feigenbaum) est de l'ordre de 3,57. En fait, ce point marque un changement radical dans la dynamique de la fonction logistique, celle-ci ne répondant plus au principe de (dé)doublement de période pour $r > r_\infty$. Nous nous intéressons alors à l'ensemble C des points ayant pour abscisse r_∞ dans le diagramme de bifurcation de la fonction logistique :



a) En admettant que *C* est un ensemble (triadique) de Cantor, décrire le procédé qui, à partir de l'intervalle [0,1], et répété à l'infini, permet d'obtenir l'ensemble *C*.

b) Donner quelques propriétés géométriques de *C* et préciser sa dimension.

Deuxième partie.

On s'intéresse dans cette partie au développement d'un réel en une fraction égyptienne qui est une somme de fractions unitaires, appelé aussi développement en série de Engel (DSE), et qui est défini par :

$$x = \frac{1}{a_0} + \frac{1}{a_0 a_1} + \frac{1}{a_0 a_1 a_2} + \cdots$$

où $(a_n)_{n\in IN}$ est une suite croissante d'entiers avec $a_0 \geq 2$. On note alors

$$x = [a_0, a_1, \ldots, a_n, \ldots]$$

Comme exemple, on a le DSE de ½ :

$$\frac{1}{2} = \sum_{k=1}^{\infty} \frac{1}{3^k} = [3, 3, 3, \ldots]$$

qui correspond à une suite infinie stationnaire. Le développement de la constante de Neper est donné par :

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = [1, 1, 2, 3, 4, \ldots]$$

Un algorithme pour le calcul du DSE d'un réel $x \in$]0,1] est défini par la donnée de deux suites $(x_n)_{n\in IN}$ et $(a_n)_{n\in IN}$ construites de la manière suivante :

$$x_0 := x$$
$$a_n := 1 + E\left(\tfrac{1}{x_n}\right) \quad \text{et} \quad x_{n+1} := a_n x_n - 1 \quad \text{pour tout} \quad n \in IN$$

où *E*(.) désigne la partie entière.

1) Montrer que les suites $(x_n)_{n\in IN}$ et $(a_n)_{n\in IN}$ sont bien définies.

2) Montrer que la suite $(x_n)_{n\in IN}$ est décroissante.

3) Montrer que la suite $(a_n)_{n\in IN}$ est croissante et que $a_0 \geq 2$.

4) En déduire que la suite $(S_n)_{n\in IN}$ définie par

$$S_n = \sum_{k=0}^{n} \frac{1}{a_0 \ldots a_k}$$

est convergente. On pourra utiliser le critère de d'Alembert.

5) Montrer (par récurrence sur n) que pour tout $n \in IN$,

$$x = S_n + \frac{x_{n+1}}{a_0 \ldots a_n}$$

En déduire que x admet le DSE donné par $x = [a_0, a_1, \ldots, a_n, \ldots]$.

Troisième partie.

On se propose de concevoir un cryptosystème chaotique en utilisant le DSE de la partie fractionnaire d'un nombre irrationnel. Comme exemple, on considère le développement de la partie fractionnaire de π, donné par :

$$Frac(\pi) = [8, 8, 17, 19, 300, 1991, 2492, 7236, 10586, 34588, 63403, ...]$$

1) Proposer un procédé simple pour "ramener" tous les entiers du développement ci-dessus à l'intervalle]0,1[.

2) En supposant que la suite de réels ainsi obtenue est pseudo-aléatoire, expliquer par un simple organigramme comment celle-ci peut être utilisée pour chiffrer un texte avec la méthode de Baptista.

3) En quoi serait-il plus avantageux d'utiliser le DSE ci-dessus pour la conception d'un cryptosystème chaotique que le fait d'itérer la suite logistique ?

4) *DSE pour DES ...*
Proposer un procédé simple pour obtenir des entiers de grande taille à partir du DSE de *Frac*(π) et expliquer comment ceux-ci peuvent être utilisés pour un chiffrement par bloc de données numériques en format binaire.

Université Mohammed V – Faculté des Sciences – Rabat
Master Codes, Cryptographie et Sécurité de l'information
Troisième Semestre
2015 – 2016

Systèmes Dynamiques, Chaos et Cryptographie

Contrôle final (3h) - Février 2016

On se propose de montrer que l'application *Shift* (décalage), définie sur l'espace des suites binaires infinies, est chaotique. Par conjugaison topologique, on en déduira un résultat surprenant concernant la chaoticité de l'application logistique sur un ensemble de Cantor.

On introduit les notions suivantes :

(a) L'ensemble de toutes les suites infinies de 0's et 1's est appelé l'espace symbolique de 0 et 1 et est noté $\sum_2$. Plus précisément,

$$\sum_2 := \{(s_0 s_1 s_2 ... s_n ...) \ / \ s_n = 0 \text{ ou } s_n = 1 \text{ pour tout } n \geq 0\}$$

(b) L'application Shift est définie comme suit :

$$\begin{array}{rccc} \sigma : & \sum_2 & \longrightarrow & \sum_2 \\ & (s_0 s_1 s_2 ... s_n ...) & \longmapsto & (s_1 s_2 ... s_n ...) \end{array}$$

En d'autres termes, cette application "oublie" le premier bit de la suite. Par exemple, $\sigma(01110101...) = (1110101...)$.

(c) On définit la distance entre deux "points" de $\sum_2$, $s = (s_0 s_1 s_2 ... s_n ...)$ et $t = (t_0 t_1 t_2 ... t_n ...)$, par

$$d(s,t) := \sum_{n=0}^{\infty} \frac{|s_n - t_n|}{2^n}$$

Comme exemple, la distance entre $s = (000...)$ et $t = (010101...)$ est

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{|s_n - t_n|}{2^n} &= \frac{0}{2^0} + \frac{1}{2^1} + \frac{0}{2^2} + \frac{1}{2^3} + \frac{0}{2^4} + \frac{1}{2^5} + \cdots \\ &= \sum_{n=0}^{\infty} \frac{1}{2^{2n+1}} \\ &= \frac{1}{2} \sum_{n=0}^{\infty} \frac{1}{4^n} \\ &= \frac{1}{2} \left(\frac{1}{1 - \frac{1}{4}} \right) = \frac{2}{3}\end{aligned}$$

On admet enfin que l'application Shift est continue, $\sum_2$ muni de la distance d étant un espace métrique.

Première partie.

1) Vérifier que $0 \leq d(s,t) \leq 2$ pour tout $s, t \in \sum_2$.

2) Montrer le lemme suivant :
Pour $s, t \in \sum_2$, si les $(n+1)$ premiers bits s_i et t_i sont identiques, alors $d(s,t) \leq \frac{1}{2^n}$. Inversement, si $d(s,t) \leq \frac{1}{2^n}$, alors les n premiers bits s_i et t_i sont identiques.

En un sens, deux points de $\sum_2$ sont d'autant plus proches l'un de l'autre que leurs bits initiaux coïncident.

3) Montrer que le sous-ensemble de $\sum_2$ formé des suites finissant avec une infinité de 0's successifs est dense dans $\sum_2$, c.-à-d., si

$$A := \{(s_0 s_1 s_2 ... s_n ...) \ / \ \exists N \geq 0 \text{ vérifiant } s_n = 0 \text{ pour tout } n \geq N\}$$

alors A est dense dans $\sum_2$.

(Indication : Pour $t \in \sum_2$ et $\varepsilon > 0$, trouver $s \in A$ tel que $d(s,t) < \varepsilon$ en utilisant le lemme.)

4) On se propose de montrer que les points périodiques de σ sont denses dans $\sum_2$.
   a) Caractériser un point périodique de σ.
   b) Trouver tous les points 3-périodiques de σ. Le théorème de Sharkovsky est-il applicable dans ce cas ? Justifier.
   c) Montrer que l'ensemble des points périodiques de σ est dense dans $\sum_2$.
   Indication : Suivre la démarche de la question 3 :

Pour $t \in \sum_2$ et $\varepsilon > 0$, trouver s périodique tel que $d(s,t) < \varepsilon$, en utilisant le lemme.

d) Montrer que σ admet 2^n points n-périodiques.

5) On se propose de montrer que σ est topologiquement transitive sur $\sum_2$. Pour cela, on introduit la suite de Morse s^* qui commence par 0 1 00 01 10 11; elle contient ensuite tous les blocs possibles de 0 et 1 à 3 bits (il y en a 8), puis tous les blocs de 0 et 1 à 4 bits (il y en a 16), et ainsi de suite.

a) Le point s^* est-il périodique ? Justifier.

b) Montrer que l'orbite de s^*, c.-à-d. l'ensemble $\left\{s^*, \sigma(s^*), \sigma^2(s^*), \dots\right\}$, est dense dans $\sum_2$, puis conclure.

6) Infime sensibilité aux conditions initiales :
Montrer que pour $s \in \sum_2$ et $\varepsilon > 0$, il existe $t \in \sum_2$ et un entier N tels que $d(s,t) < \varepsilon$ et $d(\sigma^n(s), \sigma^n(t)) = 2$ dès que $n > N$, puis conclure.

7) Considérons la fonction logistique $f_\lambda(x) = \lambda x(1-x)$ et l'ensemble

$$\Lambda := \{x \ / \ f_\lambda^n(x) \in [0,1] \text{ pour tout } n\}$$

On sait que pour $\lambda > 4$, Λ est un ensemble de Cantor. En fait, on a

$$\Lambda = \bigcap_{n=1}^{\infty} \Lambda_n$$

où $\Lambda_n := \{x \ / \ f_\lambda^n(x) \in [0,1]\}$, et en particulier, $\Lambda_1 = I_0 \cup I_1$ où $I_0 = \left[0, \frac{1}{2} - \frac{\sqrt{\lambda^2-4\lambda}}{2\lambda}\right]$ et $I_1 = \left[\frac{1}{2} + \frac{\sqrt{\lambda^2-4\lambda}}{2\lambda}, 1\right]$.
Pour tout $x \in \Lambda$, on définit alors *l'itinéraire* de x comme étant le point de $\sum_2$ donné par

$$\varphi(x) = (s_0 s_1 s_2 ... s_n ...) \text{ où, pour tout } n \geq 0, \ s_n = \begin{cases} 0 \text{ si } & f_\lambda^n(x) \in I_0 \\ 1 \text{ si } & f_\lambda^n(x) \in I_1 \end{cases}$$

a) Vérifier que l'application $\varphi : \Lambda \longrightarrow \sum_2$ est bien définie.

b) Calculer $\varphi\left(\frac{1-\sqrt{5}}{2}\right)$ pour $\lambda = 5$.

c) Que peut-on conclure si l'on admet que l'application φ réalise une conjugaison topologique entre f_λ et σ, pour $\lambda > 4$?

Deuxième partie.

Expliquer brièvement comment l'application itinéraire φ, combinée à l'application logistique f_λ, pourraient être utilisées pour concevoir un cryptosystème chaotique.

Université Mohammed V – Faculté des Sciences – Rabat
Master Codes, Cryptographie et Sécurité de l'Information
Troisième Semestre
2016 – 2017

Systèmes Dynamiques, Chaos et Cryptographie

Contrôle final (3h) - Février 2017

On se propose de montrer que l'application

$$\begin{array}{rccl} f_p: & [0,1[& \longrightarrow & [0,1[\\ & x & \longmapsto & Frac(px) := px \mod 1 \end{array}$$

est chaotique pour $p \in \mathbb{N}\backslash\{0,1\}$, f_p étant non linéaire, discontinue et non inversible. On établira ainsi un lien avec une conjecture non encore résolue, celle de l'universalité (et peut-être même la normalité) de certains irrationnels ..

Première partie.

Pour simplifier, nous nous intéressons d'abord au cas $p = 2$, et pour alléger l'écriture, l'application correspondante sera notée f au lieu de f_2, définie sur $I = [0,1[$. Arithmétiquement, il s'agit d'une itération très simple : pour $x \in I$, on multiplie par 2 et si le résultat dépasse l'unité, on soustrait 1. Géométriquement, f correspond à l'application de dédoublement des angles sur le cercle unité ..

Rappelons que tout $x \in I$ admet un développement binaire

$$x = \sum_{n=1}^{\infty} \frac{x_n}{2^n}$$

où $x_n \in \{0,1\}$, celui-ci étant unique si l'on ajoute la condition nécessaire que la suite des x_n ne se termine pas par une suite (infini) de 1's. En fait, sans cette condition, $1/2$ peut aussi s'écrire

$$\frac{1}{2} = \frac{0}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + ...$$

Techniquement, pour calculer le développement binaire de x, on multiplie par 2 et on prend la partie entière pour déterminer x_1. On répète ensuite le processus, en multipliant le reste (c.-à-d. la partie fractionnaire) par 2 et en prenant la partie entière pour déterminer x_2, et ainsi de suite. On écrit alors

$$x = \cdot x_1 x_2 x_3 ...$$

et on désignera x_n par le *n-ème* bit de la représentation binaire de x.

1. Vérifier que, par exemple,

$$\frac{1}{4} = \cdot 01000... = \cdot 01\overline{0} \quad \text{et} \quad \frac{7}{10} = \cdot 1011001100110... = \cdot 1\overline{0110}$$

où la barre supérieure signifie une répétition infinie de la même suite.

2. Montrer que dans la représentation binaire, f correspond à un *décalage* :

$$\begin{array}{ccccc} f: & I & \longrightarrow & I \\ & x = \cdot x_1 x_2 x_3 x_4 ... & \longmapsto & f(x) = \cdot x_2 x_3 x_4 ... \end{array}$$

Indication :
Remarquer que $2x = x_1 + \underbrace{\sum_{n=1}^{\infty} \frac{x_{n+1}}{2^n}}_{<1}$ puis discuter selon que $x_1 = 0$ ou $x_1 = 1$.
Ce fait est fondamental pour comprendre aisément la dynamique de f. Il va nous permettre d'illustrer - entre autres - une des caractéristiques principales du chaos : la sensibilité aux conditions initiales ..

3. Vérifier que pour deux points x et y dont le développement binaire ne diffère qu'au niveau du $(n+1)$-*ème* bit ($x_{n+1} \neq y_{n+1}$), on a

$$|x - y| = 2^{-(n+1)} \quad \text{et} \quad |f^n(x) - f^n(y)| = \frac{1}{2}$$

4. Montrer le lemme suivant :
Si x et y s'accordent sur les N premiers bits ($x_n = y_n \ \forall n \leq N$), alors

$$|x - y| \leq \frac{1}{2^N}$$

5. En déduire que pour qu'un ensemble $E \subset I$ y soit dense, il suffit que

$$\forall y \in I, \ \forall N \in \mathbb{N}, \ \exists x \in E \ \text{ tel que } \ x_n = y_n \ \forall n \leq N$$

Rappelons que f possède la propriété de (d'extrême) sensibilité aux conditions initiales si

$$\exists \delta > 0,\ \exists c < \infty \ \text{ tels que } \ \forall x \in I,\ \forall \varepsilon > 0,\ \exists y \in I,\ \exists n \leq c|\ln \varepsilon|$$
$$\text{vérifiant } \ |y - x| < \varepsilon \ \text{ et } \ |f^n(y) - f^n(x)| \geq \delta$$

Remarquer que, contrairement à l'usage, on a imposé au nombre d'itérations pour que les orbitent de x et y se séparent d'une distance d'au moins δ qu'il ne soit pas trop grand, c.-à-d. ne croissant que logarithmiquement lorsque ε diminue.

6. Montrer que f satisfait à la propriété d'extrême sensibilité aux conditions initiales. On pourra s'inspirer de la question 3.

7. Caractériser les points périodiques de f, c.-à-d. les points x dont l'orbite $\{x, f(x), f^2(x), ...\}$ est périodique. Le théorème de Sharkovsky s'applique-t-il dans ce cas? Justifier.

8. En utilisant le lemme, montrer que l'ensemble des points périodiques est dense dans I.

9. Montrer qu'il existe une orbite dense dans I. Indication : penser à la suite de Morse.

10. En déduire la transitivité topologique de f puis conclure.

Un point x (ou son orbite) est dit(e) finalement périodique de période k s'il existe un entier $N \geq 0$ tel que $f^{n+k}(x) = f^n(x)$ pour tout $n \geq N$.

11. Montrer que l'ensemble des points finalement périodiques de période 1 coïncide avec l'ensemble des rationnels dyadiques dans l'intervalle I. Un rationnel dyadique est un nombre de la forme $\dfrac{m}{2^n},\ m \in \mathbb{Z},\ n \in \mathbb{N}$.

12. Montrer qu'il existe des points dont l'orbite n'est ni périodique, ni finalement périodique, ni dense dans I.

Deuxième partie.

1. Expliquer comment on peut généraliser la première partie et montrer que l'application f_p est chaotique sur I.

2. On conjecture que π est un nombre univers en base 10, c.-à-d. que son développement décimal contient *toute* suite finie de chiffres entre 0 et 9. Montrer que cette conjecture équivaut au fait que l'orbite de $Frac(\pi)$ soit dense dans I pour $p = 10$. Dites alors en quoi la conjecture semble être vraie.

Troisième partie.

Expliquer brièvement comment l'application f_p pourrait être utilisée pour concevoir un cryptosystème chaotique.

– – – – –

"Sixteen-digit, 64-bit floating-point arithmetic
is standard on most computers these days, and that's sufficient
for almost all scientific applications, but a few crazy people need more. I'm one."

David Bailey, Berkeley Lab, USA.

– – – – –

Université Mohammed V – Faculté des Sciences – Rabat
Master Codes, Cryptographie et Sécurité de l'Information
Troisième Semestre
2017 – 2018

Systèmes Dynamiques, Chaos et Cryptographie

Contrôle final (3h)

On se propose de montrer que la fonction logistique possède un ensemble (resp. non) dénombrable de points (resp. non) périodiques sur l'intervalle $[0,1]$. Pour ce faire, une conjugaison topologique avec l'application dite en accent circonflexe et une correspondance de celle-ci avec l'opérateur décalage sur l'ensemble des suites binaires seront établies.

Première partie.

Notons $\sum_2 := \prod_0^{+\infty}\{0,1\}$ l'ensemble des suites binaires $s = (s_k)_{k\in\mathbb{N}}$, $s_k = 0$ ou 1, et σ l'opérateur de décalage à gauche défini par

$$\sigma(s)_k = s_{k+1}\ , \quad k \in \mathbb{N}$$

L'étude de la chaoticité de σ a déjà fait l'objet de sujets d'examen pour ce même module. Nous admettons donc qu'il existe un ensemble dénombrable dans $\sum_2$ de suites s telles que la suite $(\sigma^k(s))_{k\in\mathbb{N}}$ est périodique, c.-à-d. pour lesquelles il existe $p \in \mathbb{N}^*$ tel que $\sigma^p(s) = s$, et qu'il existe un ensemble non dénombrable de suites s telles que la suite $(\sigma^k(s))_{k\in\mathbb{N}}$ n'est jamais périodique, c.-à-d. $\sigma^{n+m}(s) \neq \sigma^m(s)$ pour tout $n \in \mathbb{N}$, $m \in \mathbb{N}^*$.

Nous considérons l'application, dite en accent circonflexe, définie par

$$\begin{array}{rccl} T: & [0,1] & \longrightarrow & [0,1] \\ & x & \longmapsto & 1-|1-2x| = \left\{ \begin{array}{ll} 2x & \text{si} \quad 0 \leq x \leq 1/2 \\ 2-2x & \text{si} \quad 1/2 \leq x \leq 1 \end{array} \right. \end{array}$$

1. Tracer le graphe de T sur $[0,1]$.

2. Pour I et J deux sous-intervalles de $[0,1]$, nous notons $I \rightharpoonup J$ lorsqu'il existe un intervalle fermé non vide $K \subset I$ tel que $T(K) = J$. Nous admettons que si $I \rightharpoonup J$, alors, pour tout intervalle fermé non vide $M \subset J$, il existe un intervalle fermé non vide $L \subset I$ tel que $T(L) = M$. En considérant $I_0 = [0, 1/2]$ et $I_1 = [1/2, 1]$, montrer que

$$I_0 \rightharpoonup I_1 \ , \quad I_1 \rightharpoonup I_0 \ , \quad I_0 \rightharpoonup I_0 \ , \quad I_1 \rightharpoonup I_1$$

3. Montrer par récurrence sur $n \in \mathbb{N}^*$ que pour toute suite binaire $s_0 s_1 ... s_{n-1}$ de longueur n, l'ensemble

$$J_{s_0 s_1 ... s_{n-1}} := \{x \in [0,1] \ / \ x \in I_{s_0}, \ T(x) \in I_{s_1}, ..., T^{n-1}(x) \in I_{s_{n-1}}\}$$

est un intervalle fermé non vide, et que

$$J_{s_0 s_1 ... s_{n-1} s_n} \subset J_{s_0 s_1 ... s_{n-1}}$$

Indication: considérer l'intervalle fermé non vide $J_{s_1 ... s_n} \subset I_{s_1}$ et se rappeler que $I_{s_0} \rightharpoonup I_{s_1}$.

4. Que peut-on dire de la suite $(T^k(1/2))_{k \in \mathbb{N}}$?

5. Pour tout $x \in [0,1]$, on définit son itinéraire comme étant le point de $\sum_2$ donné par

$$\varphi(x) = s_0 s_1 s_2 ... s_k ... \text{ où, pour tout } k \geq 0, \ s_k = \begin{cases} 0 \text{ si } \ T^k(x) \in I_0 \\ 1 \text{ si } \ T^k(x) \in I_1 \end{cases}$$

Et par convention, on posera $s_k = 0$ si $T^k(x) = 1/2$. Montrer que pour toute suite $s \in \sum_2$, on peut associer un $x \in [0,1]$ dont l'itinéraire est s.
Indication: remarquer qu'un tel x existe si

$$\bigcap_{n \in \mathbb{N}} J_{s_0 s_1 ... s_n} \neq \varnothing$$

6. Montrer que si $T^k(x_1)$ et $T^k(x_2)$ sont dans le même intervalle I_0 ou I_1, alors

$$|T^{k+1}(x_1) - T^{k+1}(x_2)| = 2|T^k(x_1) - T^k(x_2)|$$

En déduire l'unicité du point x de la question précédente.

7. Montrer que T admet un ensemble dénombrable de points périodiques et un ensemble non dénombrable de points non périodiques. On pourra vérifier d'abord que si s est l'itinéraire de x, $\sigma(s)$ sera celui de $T(x)$.

8. On considère l'application

$$\begin{array}{rccc} h: & [0,1] & \longrightarrow & [0,1] \\ & x & \longmapsto & \sin^2(\pi x/2) \end{array}$$

Montrer que h réalise une conjugaison topologique entre T et la fonction logistique $f_4(x) = 4x(1-x)$, c.-à-d.

$$f_4 \circ h = h \circ T$$

En d'autres termes, le diagramme suivant est commutatif:

$$\begin{array}{ccc} [0,1] & \xrightarrow{T} & [0,1] \\ h \downarrow & & \downarrow h \\ [0,1] & \xrightarrow[f_4]{} & [0,1] \end{array}$$

9. En déduire la même propriété pour la fonction logistique quant aux points (non) périodiques.

10. Aurions-nous pu obtenir ce résultat directement ? Justifier en rappelant le théorème adéquat.

11. En supposant que l'ensemble des points périodiques de f_4 est dense dans $[0,1]$, que reste-t-il à démontrer au minimum pour que la fonction soit chaotique au sens de R. Devaney ?

Deuxième partie.

Expliquer brièvement comment l'application f_4 pourrait être utilisée de deux manières différentes pour concevoir un cryptosystème chaotique.