Bol. Soc. Esp. Mat. Apl. n°21(2002), 51–63

Algunos aspectos matemáticos del problema del reparto de secretos *

P. Abascal Fuentes

Departamento de Matemáticas. Universidad de Oviedo.

abascal@etsiig.uniovi.es

Resumen

El problema del Reparto de Secretos se engloba en un campo más general que es el de la Criptografía.

El problema que se plantea es repartir una información secreta entre un colectivo de participantes, mediante la construcción de fragmentos de información que se repartirán entre los participantes, de modo que para conocer la información secreta sean necesarios algunos conjuntos predeterminados de participaciones.

Vamos a analizar algunas de las soluciones clásicas planteadas a lo largo de la bibliografía existente sobre el tema, tanto desde el punto de vista de su construcción como del de su eficacia, centrándonos de un modo algo más detallado en su formulación en términos de la Teoría de Códigos.

Palabras clave: *Criptografía, Reparto de secretos, Estructuras de acceso*
Clasificación por materias AMS: *94A60 94A62*

1 Introducción

La Criptografía ha adquirido una notable relevancia en el mundo actual debido a sus múltiples aplicaciones en el campo de las comunicaciones. Básicamente, el problema fundamental es el de la protección de datos, mediante su ocultación o transformación, y la Teoría de Números desempeña un importante papel en su resolución como así se pone de manifiesto en [15].

Asímismo, la Criptografía engloba otros problemas como el del Reparto de Secretos que, como veremos, puede ser atacado desde diferentes ramas de la Matemática.

En líneas generales el problema que dio inicio al estudio del reparto de secretos era tratar de repartir una información secreta entre un colectivo $\mathcal{P}$ de

*Trabajo parcialmente financiado por los Proyectos DGICYT PB98-0753-C02-02 y JCL VA079/02.

Fecha de recepción: 20 de mayo de 2002

l personas, mediante la construcción de l fragmentos de información, de modo que para conocer la información secreta fueran necesarias al menos m de las l participaciones.

Esto es lo que se ha dado en llamar un esquema umbral y, como veremos, ha sido resuelto por Shamir [16] y por Blakley [3], utilizando conceptos matemáticos tan dispares como los polinomios y el espacio afín, respectivamente.

Para situar el problema, supongamos una comunidad de vecinos que tiene una cuenta bancaria común con clave de acceso y se supone que para realizar cualquier transacción sea necesaria la presencia de al menos la mitad de los vecinos. Se trata, entonces, de dar a cada vecino un fragmento de información acerca de la clave, de modo que si se agrupan al menos la mitad de los vecinos puedan recuperar la clave completa para realizar una transacción pero que si se reúnen menos de la mitad no puedan recuperar nada acerca de ella.

Con el paso del tiempo y a modo de generalización se ha considerado que las agrupaciones autorizadas a recuperar la totalidad del secreto no tuvieran necesariamente el mismo número de participantes, sino que pudieran ser unas agrupaciones establecidas y especificadas a priori, por lo que el problema derivó en diseñar un esquema para compartir secretos que se denominó perfecto, esto es, que las agrupaciones no autorizadas a recuperar el secreto no obtuvieran, al reunir sus participaciones, ninguna información acerca del secreto.

2 Problema del Reparto de Secretos

El problema que se plantea es, dado un secreto, repartir unos fragmentos de información entre varias personas, de modo que ciertas agrupaciones de estas personas puedan recuperar el secreto y otras agrupaciones no sean capaces de recuperar nada acerca del secreto.

Para describir el problema vamos a considerar:

$\mathcal{P} = \{P_1, \dots P_l\}$ un conjunto de l *personas* que participan en un esquema para compartir secretos,

$D \notin \mathcal{P}$ el *gestor* del esquema, es decir, una persona confiable y ajena al conjunto de participantes que administra las participaciones y que mantiene oculto el secreto,

$\mathcal{K}$ un conjunto de *secretos* a repartir,

$\Gamma \subseteq 2^{\mathcal{P}}$ el conjunto de subconjuntos de participantes que son capaces de computar el secreto, denominados *agrupaciones autorizadas*. A Γ se le denomina *estructura de acceso*,

$\mathcal{S}$ el conjunto de *participaciones*.

Nota 1 *Se puede comprobar que la estructura de acceso queda perfectamente determinada por el conjunto de sus agrupaciones minimales, que se denomina base de la estructura de acceso y se denota por* Γ_0.

Presentamos el modelo matemático al que deberá ajustarse cualquier construcción que se haga para describir un esquema de reparto de secretos.

Definición 1 *Dados S un conjunto de participaciones y K un conjunto de secretos, un esquema de reparto de secretos se representa como un conjunto de reglas de distribución, esto es aplicaciones*

$$f : \mathcal{P} \cup \{D\} \longrightarrow \mathcal{S} \cup \mathcal{K} \text{ que satisfacen}$$
$$f(D) \in \mathcal{K} \quad y \quad f(P_i) \in \mathcal{S} \quad \text{para } 1 \leq i \leq l,$$

donde $f(D) = K$ es el secreto a compartir y $f(P_i) = s_i$ es la participación que puede recibir cada $P_i \in \mathcal{P}$.

El conjunto de reglas de distribución, denotado por $\mathcal{J}$, es de conocimiento público. Para cada secreto $K \in \mathcal{K}$ consideramos el conjunto de reglas $\mathcal{J}_K = \{f \in \mathcal{J} / f(D) = K\}$ y cuando el gestor del esquema quiera repartir un secreto K tomará aleatoriamente una regla de $\mathcal{J}_K$ y repartirá a cada persona $P_i \in \mathcal{P}$ la participación $s_i \in \mathcal{S}$. Diremos, entonces, que el esquema realiza *la estructura de acceso.*

Definición 2 *Se dice que un esquema es perfecto para realizar una estructura de acceso Γ, cuando se satisfacen las dos propiedades siguientes:*

1. *si un subconjunto autorizado reúne sus participaciones, entonces puede determinar el valor del secreto K,*

2. *si un subconjunto no está autorizado, entonces no puede determinar nada acerca de K.*

Supongamos que Γ es una estructura de acceso y $\mathcal{J}$ un conjunto de reglas de distribución tales que:

1. Si $A \in \Gamma$ y $f, g \in \mathcal{J}$ verifican que $f(P_i) = g(P_i)$ para todo $P_i \in A$, entonces se tiene que $f(D) = g(D)$.

2. Si $B \notin \Gamma$ y $f : B \longrightarrow \mathcal{S}$, entonces existe un entero positivo $\lambda(f, B)$ tal que, para cada $K \in \mathcal{K}$,

$$|\{g \in \mathcal{J}_K \, : \, g(P_i) = f(P_i) \text{ para todo } P_i \in B\}| = \lambda(f, B).$$

La condición 1 afirma que las participaciones dadas a un subconjunto autorizado determinan de forma única el valor del secreto.

La condición 2 asegura que fijada cualquier asignación f de participaciones a los elementos de B (subconjunto no autorizado), existen $\lambda(f, B)$ posibles reglas compatibles con f para cada posible valor del secreto.

Teorema 1 *[6] Si tenemos una familia de reglas de distribución $\mathcal{J}$ que satisface las condiciones 1 y 2 anteiores, entonces $\mathcal{J}$ es un esquema perfecto que realiza la estructura de acceso Γ.*

La *eficiencia* de un esquema se mide a través de la *Tasa de Información*.

Un secreto $K \in \mathcal{K}$ se puede representar como una cadena de bits de longitud $\log_2 |\mathcal{K}|$ y cada participación $s_i \in \mathcal{S}_i$, de cada P_i, por una cadena de longitud $\log_2 |\mathcal{S}_i|$.

Definición 3 *Se denominan tasa de información de* P_i *a* $\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}_i|}$ *y tasa de información del esquema a* $\rho = \min \{\rho_i : 1 \leq i \leq l\}$.

Lema 2 *Para cualquier esquema perfecto* $\rho \leq 1$.

Demostración.

Supongamos que $\mathcal{J}$ es el conjunto de reglas de distribución para un esquema perfecto para compartir secretos que realiza una estructura de acceso Γ.

Sean $B \in \Gamma_0$ y $P_i \in B$, definimos $B' = B - \{P_i\}$ y tomamos una regla de distribución $g \in \mathcal{J}$.

Sea f la restricción de g a B'. Como $B' \notin \Gamma$, existe un número entero $\lambda(f, B') > 0$ que verifica la condición 2 anterior.

De aquí que para cada $K \in \mathcal{K}$ existe una regla de distribución $f_K \in \mathcal{J}_K$ tal que $f_K(P_j) = f(P_j)$ para todo $P_j \in B'$.

Por la condición 1 anterior podemos asegurar que si $K \neq K'$ entonces $f_K(P_i) \neq f_{K'}(P_i)$, luego $|\mathcal{S}_i| \geq |\mathcal{K}|$ y de aquí se deduce que $\rho \leq 1$.

□

Definición 4 *Cuando* $\rho = 1$ *se dice que el esquema es ideal.*

Se puede comprobar que el ejemplo descrito en la sección 1 se ajusta al modelo general puesto que se trata de un $(t/2, t)$-esquema umbral y puede ser resuelto mediante, por ejemplo, el esquema de Shamir expuesto en la sección 3.1.

3 Esquemas clásicos de reparto de secretos

Vamos a describir, en esta sección, algunos de los esquemas que han sido utilizados para resolver el problema del Reparto de Secretos, exponiendo los conceptos matemáticos que se aplican en ellos. Veremos que en algunos casos se obtiene un esquema ideal.

3.1 Esquema de Shamir

Shamir [16] resolvió el problema de repartir secretos entre l personas, de modo que cualquier agrupación de t o más de ellas pudiera recuperarlo y, en caso contrario la agrupación no descubra nada acerca del secreto. Este problema es conocido como un (t, l)-esquema umbral.

El esquema consiste en:

Dados l, s y $t \leq l$ enteros positivos y un secreto $K \in \{0, \ldots, s-1\}$.

- Se toma un primo $p \geq \max\{s, l+1\}$.

- Se escogen aleatoria e independientemente $a_1, \ldots, a_{t-1} \in \mathbb{Z}/p$.
- Se construye el polinomio de grado $t-1$, $q(x) = K + \sum_{i=1}^{t-1} a_i x^i$.
- Se distribuye el secreto en las participaciones $s_i = q(i) \in \mathbb{Z}/p$, $i = 1, \ldots, l$ que se reparten entre los miembros del colectivo.

Mediante el Teorema de Interpolación de Lagrange [10], t personas del colectivo de participantes podrían recuperar el polinomio $q(x)$, puesto que conocen las imágenes de t puntos, y de ahí su término independiente que es el secreto. Ahora bien, $t-1$ personas no obtendrían información adicional sobre la que ya tenían ya que cualquier término independiente sería compatible con la construcción.

Nota 2 *Para la realización del caso particular de un (l, l)-esquema umbral, en el que sólo tenemos una agrupación autorizada consistente en el conjunto formado por todos los participantes, resulta mas sencilla la siguiente construcción.*

Dados l y s enteros positivos y un secreto $K \in \{0, \ldots, s-1\}$,

- *se toma un primo $p \geq \max\{s, l+1\}$,*
- *se escogen aleatoria e independientemente $a_2, \ldots, a_l \in \mathbb{Z}/p$,*
- *se distribuye el secreto en las participaciones $s_1 = K + \sum_{i=2}^{l} a_i$ y $s_i = a_i \quad \forall i = 2, \ldots, l$, que se reparten entre los miembros del colectivo.*

Este tipo de esquemas, aunque sólo es válido para el caso de esquema umbral, es ideal, ya que la longitud de las participaciones es la misma que la del secreto.

3.2 Construcción de tipo geométrico

Blakley [3] fue el precursor de este tipo de construcciones para la resolución de un (t, l)-esquema umbral; posteriormente, diversos autores han propuesto modificaciones del método original de Blakley.

Básicamente, se trata de tomar en un espacio afín una recta pública, que contiene al secreto, y un hiperplano no paralelo a la recta, cuya intersección con la recta es el secreto; las participaciones que se reparten son puntos del hiperplano, de modo que las agrupaciones autorizadas puedan obtener una variedad afín contenida en el hiperplano y que contiene al secreto y así, tras hacer su intersección con la recta pública, recuperar el secreto.

Hemos tomado la construcción geométrica de Simmons [17] como ejemplo de este tipo de esquemas ya que, aunque no es la más general, es suficiente para nuestros propósitos.

Dado $\mathbb{F}_q$ cuerpo con q elementos, se considera $\mathbb{F}_q^n$ con su estructura afín que denotaremos por $A(q, n)$.

Sean V_D una recta y V_l un hiperplano en el espacio afín n-dimensional $A(q, n)$ tal que $|V_D \cap V_l| = 1$

El secreto será el único punto $K = V_D \cap V_l$ y cada participante P_i recibirá como participación un conjunto $d(P_i) = \{x_{ij} : 1 \leq j \leq R_i\}$ de puntos de V_l de modo que

$$V_B \cap V_D = \emptyset \Longleftrightarrow B \notin \Gamma$$

donde V_B es la variedad generada por $\bigcup_{\{i:P_i\in B\}} d(P_i)$, es decir,

$$V_B = \{ \sum_{\{i:P_i\in B\}} \sum_{j=1}^{R_i} \alpha_{ij} x_{ij} : \alpha_{ij} \in \mathbb{F}_q, \sum_{j=1}^{R_i} \alpha_{ij} = 1\}$$

Para recuperar el secreto, una agrupación computará la variedad engendrada por las participaciones que tiene conjuntamente y su intersección con V_D. Si no es vacía, el único punto de intersección es el punto K.

En particular, si se quiere construir un (t, l)-esquema umbral, como se pretendía en la construcción original de Blakley, se reparte un punto a cada uno de los l participantes de modo que cualquier subconjunto de t puntos sean afínmente independientes.

Esta construcción genera un esquema ideal puesto que, tanto el secreto como las participaciones son puntos.

3.3 Construcción basada en circuitos monótonos

En 1987, Ito, Saito y Nishizeki [9] dieron una construcción para resolver el problema general de compartir secretos, que demuestra que siempre existe un esquema que realiza cualquier estructura de acceso, aunque la tasa de información es pésima, es decir, la longitud de las participaciones es mucho mayor que la del secreto.

Básicamente, la idea de su construcción es describir un circuito monótono que reconozca"la estructura de acceso y dar, a partir de esta descripción, el esquema de reparto. El inconveniente de este esquema es que, como veremos, la tasa de información es muy baja.

Supongamos que tenemos un circuito booleano con l entradas $x_1, \ldots, x_l$ correspondientes a los l participantes $P_1, \ldots, P_l$ en el esquema y una salida y. El circuito consiste en puertas O y puertas Y pero ninguna NO; tal circuito se denomina *circuito monótono*.

Si especificamos valores booleanos para las l entradas, podemos definir $B(x_1, \ldots, x_l) = \{P_i : x_i = 1\}$, es decir, el subconjunto de $\mathcal{P}$ correspondiente a las entradas verdaderas.

También podemos definir $\Gamma_{\mathcal{G}} = \{B(x_1, \ldots, x_l) : \mathcal{G}(x_1, \ldots, x_l) = 1\}$ donde $\mathcal{G}(x_1, \ldots, x_l)$ denota la salida Y del circuito dada por las entradas $x_1, \ldots, x_l$.

Si $\Gamma_0 \subset 2^{\mathcal{P}}$, es fácil construir un circuito monótono $\mathcal{G}$ tal que $\Gamma_{\mathcal{G}} = \Gamma_0$. Una forma es, dada Γ_0 la base de una estructura de acceso, se construye la fórmula booleana:

$$\bigvee_{A\in\Gamma_0} (\bigwedge_{P_i\in A} P_i)$$

ahora se trata de repartir participaciones entre los integrantes del esquema y la propuesta de estos autores es, dado un secreto K, para cada agrupación $A \in \Gamma_0$, considerar la construcción de la Nota 2 para resolver el (l_A, l_A)-esquema umbral donde l_A es el número de participantes de la agrupación A.

Entonces, cada participante recibirá una participación por cada agrupación minimal a la que pertenezca; y si una agrupación B pretende recuperar el secreto K deberá encontrar una agrupación minimal A contenida en ella y recuperar el secreto a partir de A.

Como podemos observar, aunque la longitud del secreto es 1, la longitud de la participación de un participante es la misma que el número de agrupaciones de la base en la que esté incluido. Por lo tanto este esquema no es ideal aunque la estructura de acceso admita una construcción ideal.

3.4 Construcción vectorial

Este tipo de construcción para compartir secretos se debe a Brickell [4] y, en líneas generales, podemos decir que cada participante, incluido el gestor, tiene asociado un vector de un espacio vectorial sobre un cuerpo finito de manera que los subconjuntos autorizados son aquellos en los que el vector asociado al gestor se puede expresar como combinación lineal de los vectores asociados a los participantes de la agrupación.

Sean Γ una estructura de acceso y $\mathbb{F}_q^k$ el espacio vectorial de dimensión k sobre el cuerpo finito $\mathbb{F}_q$ y $k \geq 2$.

Supongamos que existe una aplicación $\Phi : \mathcal{P} \cup \{D\} \longrightarrow \mathbb{F}_q^k$ que satisface:

$$\Phi(D) \in < \Phi(P_i) : P_i \in B > \Leftrightarrow B \in \Gamma \tag{1}$$

es decir, que el vector $\Phi(D)$ puede ser expresado como combinación lineal del conjunto $\{\Phi(P_i) : P_i \in B\}$ si y sólo si B es un conjunto autorizado.

Entonces para $\mathcal{K} = \mathcal{S} = \mathbb{F}_q$ se puede construir un esquema ideal definiendo, para cada $a \in \mathbb{F}_q^k$, la regla de distribución del esquema $f_a(x) = a \cdot \Phi(x)$ para todo $x \in \mathcal{P} \cup \{D\}$.

Teorema 3 *[4] Si Φ satisface la condición (1), la colección de reglas de distribución $\mathcal{J} = \left\{f_a : a \in \mathbb{F}_q^k\right\}$ es un esquema ideal que realiza Γ.*

3.5 Construcción mediante grafos

Estas estructuras son utilizadas frecuentemente para construir esquemas cuya estructura de acceso tiene como base solamente agrupaciones con 2 participantes y que, por tanto, se pueden interpretar como las aristas de un grafo no dirigido.

Dado un grafo $\mathcal{G} = (V, E)$, donde V son los vértices y E las aristas que unen cada vértice, denotamos por $\Gamma(\mathcal{G})$ a la estructura de acceso cuyos participantes son los elementos de V y por $\Gamma_0 = E$ a la base de $\Gamma(\mathcal{G})$.

Definición 5 *Se dice que un grafo $\mathcal{G}$ es completo y multipartito, si podemos encontrar una partición de V en subconjuntos $V_1, V_2, ..., V_l$ tal que*

$$(x, y) \in E \Longleftrightarrow x \in V_i \ \wedge \ y \in V_j \quad i \neq j$$

Un grafo multipartito se denota por $K_{n_1,...,n_l}$ si $|V_i| = n_i$, $1 \leq i \leq l$ y por K_l si $n_i = 1 \quad \forall i = 1, ..., l$ y $l = |V|$.

Como resultado fundamental para este tipo de construcciones se tiene el siguiente resultado.

Teorema 4 *[18] Si $\mathcal{G} = (V, E)$ es un grafo multipartito, entonces hay un esquema ideal que realiza la estructura de acceso $\Gamma(\mathcal{G})$.*

3.6 Matroides

Aunque no aportan construcción propia, puesto que se apoyan en la construcción vectorial, su contribución al problema del Reparto de Secretos son importantes resultados acerca de la caracterización de estructuras de acceso que admiten un esquema ideal. Para más detalles sobre estas estructuras y su utilización en el problema del reparto de secretos nos remitimos a [5] ó [11].

Definición 6 *Una matroide es un par $\mathcal{M} = (X, \mathcal{J})$ donde X es un conjunto finito y $\mathcal{J} \subset 2^X$ que verifican:*

$\emptyset \in \mathcal{J}$

Si $A \in \mathcal{J}$ y $B \subset A$ entonces $B \in \mathcal{J}$

Si $A, B \in \mathcal{J}$ y $|A| = |B| + 1$ entonces existe $x \in A - B$ tal que $B \cup \{x\} \in \mathcal{J}$

Los elementos de $\mathcal{J}$ se llaman conjuntos independientes y aquellos subconjuntos de X que no pertenecen a $\mathcal{J}$ se dicen dependientes. Los conjuntos dependientes minimales se denominan circuitos.

Definición 7 *Una matroide $\mathcal{M}$ se dice coordenable sobre un cuerpo $\mathbb{F}$ si existe*

$$f : X \longrightarrow \mathbb{F}^k$$

tal que $A \subset X$ es un conjunto independiente en $\mathcal{M}$ si y sólo si $\{f(x) : x \in A\}$ es linealmente independiente en $\mathbb{F}^k$.

Definición 8 *Una matroide $\mathcal{M}$ se dice conexa si para todo $x, y \in X$ existe un circuito C tal que $x, y \in C$.*

Destacamos los siguientes resultados que permiten la identificación de estructuras de acceso para las cuales podemos encontrar un esquema ideal.

Teorema 5 *[5] Sean $\mathcal{M}$ una matroide conexa y coordenable sobre un cuerpo finito $\mathbb{F}_q$ y $x \in X$ y tomamos $\mathcal{P} = X - \{x\}$.*

Entonces existe un esquema ideal que realiza la estructura de acceso dada por

$$\Gamma_0 = \{C - \{x\} : x \in C \in \mathcal{G}\}$$

donde $\mathcal{G}$ denota el conjunto de circuitos de $\mathcal{M}$.

Teorema 6 *[11] Dada una estructura de acceso* Γ*, se considera* $(X, \mathcal{G})$ *donde* X *es el conjunto de participantes y el gestor, y*

$\mathcal{G} = \mathcal{G}_D \cup \mathcal{E}$

$\mathcal{G}_D = \{A \cup \{D\} : A \in \Gamma_0\}$ *y*

$\mathcal{E}$ *es el conjunto de conjuntos minimales de* $C \cup C' - \{ \bigcap_{\{C'' \in \mathcal{G}_D : C'' \subset C \cup C'\}} C'' \}$

Entonces si $\mathcal{G}$ *no es el conjunto de circuitos de una matroide, no existe ningún esquema ideal que realiza* Γ*.*

4 Construcción basada en códigos correctores

La Teoría de Códigos surgió para tratar de corregir los errores que se podían producir en un canal de comunicación, sin embargo también se ha visto involucrada en el problema de encontrar esquemas de reparto de secretos. En este contexto, algunos trabajos dejan entrever cierto afán por generalizar y unificar las construcciones anteriormente expuestas. Concretamente, la construcción de Shamir ha sido interpretada por Mc-Eliece y Sarwate [12], en términos de códigos Reed-Solomon [13]. Para mas detalles ver [1].

4.1 Códigos correctores de errores

Definición 9 *Sea* $\mathbb{F}_q$ *el cuerpo finito con* q *elementos. Un* $[n, k]$*–código lineal* $\mathcal{C}$ *sobre* $\mathbb{F}_q$ *es un subespacio vectorial de dimensión* k *de* $\mathbb{F}_q^n$*. A los elementos de* $\mathcal{C}$ *se les denomina palabras.*

Definición 10 *Se llama* matriz generatriz *de* $\mathcal{C}$ *a la matriz asociada a una aplicación lineal inyectiva* $f : \mathbb{F}_q^k \longrightarrow \mathcal{C} \subset \mathbb{F}_q^n$*, es decir, a una matriz* $k \times n$ *cuyas filas son una base de* $\mathcal{C}$*.*

Una matriz H *sobre* $\mathbb{F}_q$ *es matriz de control o de chequeo de* $\mathcal{C}$ *si para todo vector* $x \in \mathbb{F}_q^n$ *se verifica que* $x \in \mathcal{C}$ *si y sólo si* $Hx^t = 0$*.* H *es de tamaño* $(n-k) \times n$ *y de rango* $n-k$*.*

Nota 3 *Como una base de* $\mathcal{C}$ *no es única tampoco lo es una matriz generatriz* G*, así, cuando la matriz sea de la forma* $G = [I_k \,|A]$*, donde* I_k *denota la matriz identidad de orden* k*, se dice que* G *es una matriz generatriz estándar. En este caso, tanto la codificación como el código se dicen sistemáticos y, si* $x = (x_1, \ldots, x_k)$*, las palabras del código tienen la forma:*

$$c = xG = (\underbrace{x_1, \quad \ldots \quad , x_k}_{\text{símbolos de información}} , \underbrace{x_{k+1}, \quad \ldots \quad , x_n}_{\text{símbolos de chequeo}})$$

En un canal de comunicación los mensajes pueden sufrir alteraciones de diversos tipos. Según la naturaleza de estas alteraciones podemos distinguir entre *errores*, símbolos recibidos que difieren del enviado a través del canal, y *borrones*, símbolos recibidos que son ilegibles o imposibles de interpretar por el receptor. Maticemos que los borrones se pueden interpretar como errores cuya posición

es conocida, de ahí que este tipo de errores, como veremos en la construcción del esquema, tengan especial relevancia en el problema del reparto de secretos.

Un parámetro importante en la Teoría de Códigos es la distancia mínima, pues el número de errores que puede detectar y corregir un código queda determinado por su valor.

Definición 11 *La aplicación* $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$ *tal que* $d(x,y) = \#\{i \in \{1,\ldots,n\}/x_i \neq y_i\}$ *define una métrica en* $\mathbb{F}_q^n$ *que se denomina distancia de Hamming.*

Dado un código $\mathcal{C}$ *lineal de tipo* $[n,k]$ *sobre* $\mathbb{F}_q^n$ *se define:* $d_{\mathcal{C}} = \min\{d(u,v) : u,v \in \mathcal{C} \wedge u \neq v\}$

$d_{\mathcal{C}}$ *se denomina distancia mínima de* $\mathcal{C}$ *y usualmente se denota por* d.

Si la mínima distancia de un código lineal es d *se dice que es un código de parámetros* $[n,k,d]$.

Proposición 7 *[14] Un código* $\mathcal{C}$ *con mínima distancia* d *puede:*

1. *detectar* t *errores si* $t < d$,
2. *corregir* t *errores si* $2t < d$,
3. *corregir* s *borrones si* $s < d$,
4. *corregir* t *errores y* s *borrones si* $2t + s < d$.

Sean G la matriz generatriz de un código $\mathcal{C}$, $c \in \mathcal{C}$ y J un conjunto de índices. Se denota por $G(J)$ al conjunto de columnas en G correspondientes a J, y análogamente $c(J)$ al conjunto de componentes de c.

Lema 8 *[2] Sean* I *y* J *dos conjuntos de índices disjuntos y* $c_1, c_2 \in \mathcal{C}$.

Si $G(J)$ *es linealmente dependiente de* $G(I)$ *y* $c_1(I) = c_2(I)$ *entonces* $c_1(J) = c_2(J)$.

Lema 9 *[2] Dados* I *y* J *dos conjuntos de índices disjuntos.*

Si $G(J)$ *es linealmente independiente de* $G(I)$ *y, fijado* $c_1 \in \mathcal{C}$, *entonces, para cada* $a \in \mathbb{F}_q^{|J|}$, *en* $\{c \in \mathcal{C} : c_1(I) = c(I)\ y\ c(J) = a\}$ *hay exactamente* $q^{k-(rang(G(I))+rang(G(J)))}$ *palabras.*

4.2 Descripción de esquemas basados en códigos correctores

Vamos a dar la descripción de la construcción de un esquema para compartir secretos mediante códigos correctores de errores. Para ello consideremos que el conjunto de posibles secretos es $\mathcal{K} = \mathbb{F}_q^m$, $m \in \mathbb{N}$ y que $\mathcal{C}$ es un código lineal $[n,k,d]$, $k \geq m$, con matriz generatriz $G \in \mathcal{M}_{k\times n}$. Esta matriz se hace pública y se asocian sus columnas, según ciertos conjuntos de índices a los distintos participantes en el esquema, incluido el gestor, pudiéndose asociar varias columnas a cada participante e, incluso, una misma columna a varios participantes, pero con la consideración de que las columnas asociadas al

gestor deben ser dependientes del conjunto de columnas de cada una de las agrupaciones autorizadas pero independientes del conjunto de columnas de cada una de las agrupaciones no autorizadas.

Denotaremos por J_i y J_D los conjuntos de índices que se asocian a cada participante P_i y al gestor, respectivamente. Y, para cada $A \in 2^{\mathcal{P}}$, denotaremos por $J_A = \bigcup_{P_i \in A} J_i$.

La descripción del esquema es la siguiente:

- Se considera un secreto K con m coordenadas y lo ampliamos hasta obtener un vector (K, a) de longitud k.
- Se codifica el vector (K, a) obteniéndose una palabra

$$(K, a)G = c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$$

- Se reparten las componentes del vector c entre los distintos participantes, dando a cada P_i las componentes correspondientes al conjunto de índices J_i que tiene asociado. En particular, se asignan al gestor las de J_D que, generalmente, son las primeras m componentes, es decir, las correspondientes a K.
- Para recuperar el secreto, una agrupación autorizada A deberá construir el código cuya matriz generatriz viene dada por las columnas correspondientes a $J_D \cup J_A$ y descodificar la palabra construida con las componentes que ellos tienen asignadas, considerándose las componentes que desconocen, es decir las de J_D, como un error de tipo borrón que debe corregir el código.

Así pues, deberemos encontrar un código que verifique que los códigos que construyan las agrupaciones autorizadas tengan una capacidad de corrección suficiente para recuperar el secreto pero de manera que las agrupaciones no autorizadas, con el código que construyan, no puedan saber nada acerca de él.

En ([2]) se describen dos algoritmos para la construcción de matrices generatrices y de control de códigos lineales que realizan una estructura de acceso dada verificando las condiciones anteriores. Además, con los códigos construidos mediante estos algoritmos se consigue un esquema óptimo en el sentido de la tasa de información.

5 Conclusiones

Como hemos visto a lo largo de este trabajo, existe un gran abanico de estructuras matemáticas que pueden ser aplicadas para la resolución del problema del Reparto de Secretos, tanto para la construcción de esquemas como para el estudio de su tasa de información.

Pero el problema del reparto de secretos ha ido evolucionando en el sentido de que se han ido introduciendo nuevos condicionantes por necesidades

de sus propias aplicaciones. Baste poner como ejemplo el caso en el que entre los participantes puedan existir algunos que traten de engañar a los restantes componentes de una agrupación autorizada, mintiendo acerca de sus participaciones para conocer de manera fraudulenta el secreto [19]; o el problema del reparto democrático de secretos en el cuál se construye un esquema sin la necesidad de la intervención de un gestor sino que los gestores del esquema son los propios participantes, [7] ó [8]. Esta evolución ha hecho que se vayan ampliando las posibles herramientas de aplicación para la resolución de tales problemas.

Referencias

[1] P. Abascal. *Compartir secretos mediante esquemas basados en códigos correctores*. PhD thesis, University of Oviedo, 1999.

[2] P. Abascal and J. Tena. Algoritmos de búsqueda de un código corrector de errores realizando una estructura de acceso para compartir secretos. Actas V Reunión Española de Criptología y Seguridad de la Información, 1998.

[3] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, 48:313–317, 1979.

[4] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.*, 9:105–113, 1989.

[5] E.F. Brickell and D.M. Davenport. On the clasification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[6] E.F. Brickell and Stinson D.R. Some improved bounds on the information rate of perfect secret sharing schemes. Proceedings of Crypto '90, Advances in Cryptology, Lecture Notes in Computer Science Springer-Verlag, 1992.

[7] Carpentieri, M. Some democratic secret sharing schemes. Discrete Applied Mathematics, **59**, 1995, pp. 293-298.

[8] Ingemarsson, I. & Simmons, G.J. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. Advances in Cryptology, EUROCRYPT '90, I.B. Damgard, ed., Lecture Notes in Computer Science **473** 1991, pp. 266-282.

[9] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structures. *Proc.IEEE Globecom*, pages 99–102, 1987.

[10] R. Lidl and H. Niederreiter. *Encyclopedia of Mathematics and its Applications. Finite Fields.*, volume 20. Cambridge University Press, 1983.

[11] K.M. Martin. *Discrete structures in the theory of secret sharing*. PhD thesis, University of London, 1991.

[12] R.J. Mc-Eliece and D.V. Sarwate. On sharing secrets and reed-solomon codes. *Comm ACM*, 24(583-584), 1981.

[13] F.J. Mc-Williams and N.J.A. Sloane. *The Theory of error-correcting codes*. North-Holland, 1988.

[14] C. Munuera and J. Tena. *Codificación de la Información*. Secretariado de Publicaciones e Intercambio Cient¡fico. Universidad de Valladolid, 1997.

[15] A. Quirós Gracián. Números primos y criptografía. *Bol. Soc. Esp. Mat. Apl.*, (17):13–21, 2001.

[16] A. Shamir. How to share a secret. *Comm ACM.*, 22(11):612–613, 1979.

[17] G.J. Simmons. An introduction to shared secret and/or shared control schemes and their application. Contemporary Cryptology, The Science of Information Integrity, 1991.

[18] D. R. Stinson. An explication of secret sharing schemes. 2(4):357–390, December 1992.

[19] Tompa, M. & Woll, H. How to share a secret with cheaters. Journal of Cryptology (1988) 1: 133-138.

Boletín de la Sociedad Española de Matemática Aplicada SëMA

Grupo Editor

J.J. Valdés García (U. de Oviedo)
B. Dugnol Álvarez (U. de Oviedo)
C.O. Menéndez Pérez (U. de Oviedo)
E. Fernández Cara (U. de Sevilla)
M. Mateos Alberdi (U. de Oviedo)
P. Pérez Riera (U. de Oviedo)

Comité Científico

E. Fernández Cara (U. de Sevilla)
E. Casas Rentería (U. de Cantabria)
J.M. Mazón Ruiz (U. de Valencia)
J.J. Valdés García (U. de Oviedo)
L. Vega González (U. del País Vasco)
A. Bermúdez de Castro (U. de Santiago)
J.L. Cruz Soto (U. de Córdoba)
I. Peral Alonso (U. Aut. de Madrid)
J.L. Vázquez Suárez (U. Aut. de Madrid)
E. Zuazua Iriondo (U. Comp. de Madrid)

Responsables de secciones

Artículos:	E. Fernández Cara (U. de Sevilla)
Resúmenes de libros:	F.J. Sayas González(U. de Zaragoza)
Noticias de SëMA:	R. Pardo San Gil (Secretaria de SëMA)
Anuncios de Congresos y Seminarios:	J. De Frutos Baraja (U. de Valladolid)
Matemáticas e Industria:	M. Lezaun Iturralde (U. del Pais Vasco)
Educación Matemática	R. Rodríguez del Río (U. Comp. de Madrid)

Página web de SëMA
`http://www.uca.es/sema/`

Dirección Editorial: Boletín de SëMA. Dpto. de Matemáticas. Universidad de Oviedo. Avda. de Calvo Sotelo, s/n. 33007-Oviedo. `boletin_sema@orion.ciencias.uniovi.es`

ISSN 1575-9822
Depósito Legal: AS-1442-2002

Imprime: Grupo Bitácora. C/ Instituto, 17, Entresuelo. 33201 Gijón (Asturias)
Diseño de portada: Ana Cernea

Estimados socios:

En el presente Boletín se dedica una sección especial en homenaje a la memoria del Prof. Jacques Louis Lions, fallecido en junio de 2001 . Cinco destacados matemáticos españoles, E. Casas, A. Bermúdez, J. I. Díaz, E. Fernández Cara y E. Zuazua, entre los muchos que, directa o indirectamente, han estado relacionados con el Prof. Lions han elaborado sendos escritos en los que destacan algunos aspectos, científicos y humanos, que conocieron de primera mano. Estos artículos aparecerán también en la Gaceta Matemática de la RSME.

Por otra parte, anunciamos la incorporación de dos secciones: una nueva, Matemáticas e Industria, y otra sobre Educación Matemática, que ya se venía desarrollando en boletines anteriores:

- **Matemáticas e Industria**. En esta nueva sección, que inauguraremos próximamente, se pretenden mostrar proyectos de Investigación, Desarrollo e Innovación (I+D+I), o experiencias de colaboración con empresas en las que las matemáticas sean parte importante. El objetivo es dar a conocer la actividad de instituciones o grupos de investigación dedicados a aplicaciones industriales de la matemática así como difundir opiniones de responsables empresariales o centros tecnológicos sobre la necesidad de la matemática aplicada. También se desea recoger datos de los recién licenciados en matemáticas, especialmente en lo relativo al tipo de actividad profesional que desarrollan. El responsable de esta sección es el Prof. Mikel Lezaun, de la Universidad del País Vasco, a quien se deben dirigir las respectivas colaboraciones.

- **Educación Matemática**. Esta sección es continuación de la coordinada, en una etapa anterior, por las profesoras Soledad Rodríguez y Alicia Delibes, a quien agradecemos sinceramente su labor. En ella se publicarán artículos relacionados con la docencia de las Matemáticas en cualquier nivel, sea de Enseñanza Secundaria o Universitaria. Creemos que la situación actual, en la que se están produciendo cambios importantes, sobre todo en la Secundaria, con la implantación de nuevos contenidos mínimos, Ley de Calidad, etc., hace que esta sección tenga especial relevancia, por cuanto, de una manera o de otra, nos afecta a todos. El encargado de esta sección será, a partir de ahora, el Prof. Roberto Rodríguez del Río, de la Universidad Complutense de Madrid, a quien se pueden dirigir colaboraciones y sugerencias. Retomamos esta sección con un artículo de Isabel Fernández y José M. Pacheco.

Reiteramos nuestra solicitud de colaboración a todos los socios, en las distintas secciones de Boletín, y cualquier sugerencia que mejore el mismo.

Grupo Editor

Algunos recuerdos de Jacques-Louis Lions

A. Bermúdez de Castro

Departamento de Matemática Aplicada
Universidad de Santiago de Compostela
15782 Santiago de Compostela

mabermud@usc.es

No es, ni mucho menos, el objetivo de estas breves líneas glosar la trayectoria científica del profesor Lions. Personas más autorizadas que yo lo han hecho en diversos foros a lo largo de los últimos meses y entiendo, por el contrario, que el encargo que amablemente se me ha hecho desde SEMA se refiere sobre todo a la relación del profesor Lions con grupos de investigadores de la antigua Universidad de Santiago, hoy dividida en tres tras la creación de las de A Coruña y Vigo. Por ello me voy a limitar esencialmente a evocar algunos recuerdos de sus viajes a Compostela.

Tuve la suerte de conocer a Jacques-Louis Lions a través del profesor Antonio Valle. Corría el año 1972 cuando Valle, que dirigía el departamento de análisis matemático en Santiago, me propuso irme al IRIA (Institut de Recherche en Informatique et Automatique), hoy INRIA, para preparar la tesis doctoral. Por aquel entonces Lions dirigía el laboratorio de investigación del prestigioso centro francés, conocido bajo las siglas LABORIA. A él me incorporé a comienzos del curso 1972-73, concretamente en el proyecto que sobre control óptimo de sistemas distribuidos encabezaba Jean-Pierre Yvon, hoy profesor en la Universidad de Tecnología de Compiègne. Mi trabajo consistió en el estudio de algunos problemas relacionados con el control por *feedback a priori* de ecuaciones en derivadas parciales, que habían sido planteados por Lions, y de los que hablaría al año siguiente en su conferencia plenaria de las Jornadas Hispano-Lusas de Matemáticas, celebradas en la Universidad de Sevilla.

Aquella estancia fue el inicio de una colaboración de nuestro incipiente grupo de investigación con el INRIA, que a lo largo de los años iba a marcar definitivamente la actividad científica del actual departamento de Matemática Aplicada de la Universidad de Santiago. A la relación inicial con los investigadores del proyecto de Yvon siguieron visitas e intercambios con otros proyectos del INRIA y del "Laboratoire d'Analyse Numérique" de la Universidad

de Paris VI. Estas colaboraciones impulsaron con el paso del tiempo la creación en la Universidad de Santiago de un grupo de investigación en simulación numérica y control de procesos regidos por ecuaciones en derivadas parciales. Lions seguía de cerca nuestras actividades y valoraba de modo especial las relaciones que manteníamos con la industria. Además, de vez en cuando nos proponía algún problema o nos apoyaba ante el Consejero Científico de la Embajada de Francia, nuestra única vía de financiación durante los primeros años.

El profesor Lions visitó por primera vez el entonces llamado departamento de Ecuaciones Funcionales en 1981. De aquella estancia recuerdo la admiración que le había causado el verde de nuestra tierra y la luz otoñal sobre el piedra mojada de la plaza del Obradoiro; especialmente a su esposa, muy aficionada a la pintura, arte que ella misma cultivaba. También conservo en la memoria una anécdota que revela muy bien la cordialidad y la sencillez de Lions. Resulta que habíamos organizado una conferencia en el aula magna de la antigua Facultad de Ciencias y, temerosos de que la asistencia de público fuese demasiado reducida, anunciamos el acontecimiento en algunos de los cursos de la licenciatura de matemáticas por si algún alumno, sobre todo de los últimos cursos, se animaba a asistir. No sé muy bien por qué (en aquella época no se obtenían créditos de libre elección por asistir a conferencias) la presencia de estudiantes fue masiva, con la consiguiente sorpresa de todos, incluido Lions. Éste entendió inmediatamente que la conferencia que había preparado no era para aquel auditorio y la adaptó sobre la marcha con toda naturalidad. Recuerdo por ejemplo que incluyó la definición de diferencial de un funcional definido en un espacio de Hilbert, relacionándola con las derivadas parciales de funciones de variables reales. No sospechaba que, por aquel entonces, los alumnos del segundo año de nuestra Facultad estudiaban la diferenciación en espacios normados ...

Lions volvió a Santiago en 1987, con ocasión de un congreso de la IFIP (International Federation for Information Processing) sobre control de sistemas distribuidos, en el que pronunció la conferencia inaugural.

Poco años más tarde, en 1989, fue nombrado Doctor Honoris Causa por la Universidad de Santiago. Tuve el honor de actuar de padrino en una ceremonia que, aunque sometida al rigor de un antiguo ritual, resultó muy emotiva. Viniendo de un país como Francia, donde las ceremonias universitarias apenas existen y los trajes académicos han desaparecido, Lions aceptaba con respeto, y al mismo tiempo con sentido del humor, toda la parafernalia propia de la investidura, incluidas las frases en latín.

Desgraciadamente ésta fue su última visita a Santiago. El año 2000 organizamos una conferencia internacional sobre "Mathematical and Numerical Aspects of Wave Propagation" y le invitamos a pronunciar la conferencia inaugural. Nos respondió inmediatamente con un fax de esos que el mismo escribía a mano, tan escuetos como cordiales, dicendo algo así como: "... en Santiago, el año 2000 y en el mes de julio ... acepto con gusto !"

Sin embargo no pudo venir. Por una desafortunada coincidencia que no fuimos capaces de evitar, nuestro congreso coincidió con el de la Sociedad Europea de Matemáticas en Barcelona. Además de este importante evento,

Lions tenía aquella misma semana otros compromisos ineludibles, derivados de su protagonismo en el impulso del Año Mundial de las Matemáticas que le impidieron viajar a Santiago.

Quisiera terminar estas breves líneas dejando constancia de la gratitud que yo mismo, y muchos colegas de las universidades gallegas, sentimos hacia el profesor Lions por el impulso y la ayuda que, junto con varios de sus colaboradores, nos han prestado al desarrollo de nuestro grupo. Los que hemos tenido la suerte de aprender de él, a través de sus libros, sus conferencias, sus consejos o a veces sus encargos, nos sentimos un poco huérfanos tras su muerte a la que nos resulta difícil acostumbrarnos. En el recuerdo conservaremos siempre su magisterio, pero también su cordialidad, su simpatía y su atinado sentido de la realidad, tan escaso a veces entre los grandes científicos, que le permitió ser también un excelente gestor de grandes instituciones y organismos, y un creador e impulsor de grupos de investigación en todo el mundo.

Jacques-Louis Lions

E. Casas

Departamento de Matemática y Ciencias de la Computación
Universidad de Cantabria
39005 Santander

casas@macc.unican.es

Transcurrido casi un año desde el fallecimiento del Profesor Jacques-Louis Lions y animado por algunas personas, me he decidido a escribir unas breves líneas en su recuerdo, desde la perspectiva de mi relación personal con él y su influencia en mi actividad investigadora.

Mis primeras noticias sobre el Profesor Lions se producen cuando, terminados mis estudios de la Licenciatura en Matemáticas, comienzo a estudiar ecuaciones en derivadas parciales. Entonces descubro que la cita Jacques-Louis Lions y Enrico Magenes (*"Problèmes aux limites non homogènes et applications"*, 3 vols., Dunod 1968–70) era punto de referencia obligado de los textos y artículos de la época. Este nombre me vuelve a aparecer cuando inicio el estudio de los problemas no lineales (*"Quelques méthodes de résolution de problèmes aux limites non linéaires*", Dunod 1969) o en el estudio de las inecuaciones variacionales (*"Les inéquations en méchanique et en phisyque*", Dunod 1972, en colaboración con G. Duvaut; "*Analyse numérique des inéquations variationelles*", 2 vols., Dunod 1976, en colaboración con R. Glowinski y R. Trémolières). Finalmente, al iniciar mi tesis doctoral sobre problemas de control me veo envuelto de forma irremediable en la lectura de su libro *"Contrôle optimal des systèmes gouvernés par des equations aux derivées partielles"*, Dunod 1968, la referencia obligada, que ha marcado toda una época en la Teoría de Control de Ecuaciones en Derivadas Parciales. Tras este libro vendrían otros muchos libros y artículos sobre problemas de control de ecuaciones en derivadas parciales, abordando los sistemas lineales y no lineales, el desarrollo asintótico de las soluciones, etc. Una gran parte del trabajo de investigación del Profesor Lions se dedicó al estudio de la Teoría de Control de Sistemas Distribuidos, lo que ha influido enormemente en la investigación en este tema en todo el mundo. Su primer libro de control fue la base y el fundamento de los desarrollos ulteriores, al menos en lo referente al estudio de problemas de control óptimo. Por supuesto, se ha avanzado mucho en este terreno desde entonces, pero él abrió el camino y dio los primeros pasos que hemos seguido todos los que hemos trabajado en este área de la matemática.

He descrito cómo fue mi primer encuentro con la obra matemática de Lions, pero ¿ cómo fue el encuentro con la persona ? En el primer instante que yo creí que tenía algo que contar sobre teoría de control, pensé en redactar una nota para Comptes Rendus de la Acad. de Sciences de Paris y enviársela a la persona que más había influido en mi trabajo. Fui muy gratamente sorprendido por la celeridad con la que una persona tan ocupada respondió y aceptó mi artículo. Animado por el éxito, me decidí a escribir un segundo artículo y enviárselo de nuevo para su publicación en una revista diferente. Esta vez la respuesta no llegaba. Entre tanto yo había presentado mi tesis doctoral y me desplacé al INRIA para realizar una estancia de dos meses. En aquella época Jacques-Louis Lions era Presidente del INRIA e impartía su famoso curso en el Collège de France. Yo no podía perder la ocasión de conocerle y asistí a algunas de las sesiones. Quedé impresionado por la elegancia de sus exposiciones, su cordialidad, su capacidad para atender a todas las personas que acudíamos a él. Cuando vencí mi timidez y me atreví a preguntarle por aquel artículo del que yo no había recibido todavía respuesta, su contestación fue tan clara como demoledora. Aunque no recuerdo exactamente sus palabras, sí quedó muy claro su mensaje: ¡ aquel artículo estaba muy mal escrito !. La persona a quien yo más admiraba como matemático, todo un modelo para mí, me acababa de decir que mi artículo estaba mal escrito. Esto era como para hundirse y desaparecer de su seminario, sin embargo él supo decírmelo de forma nada hiriente, de manera que yo no me desmoralicé, sino que me esforcé en aprender cómo se debía escribir un artículo e intentar no volver a vivir una experiencia similar. Posteriormente, reescribiría el artículo y aparecería en la revista que yo había pretendido en su primer momento. Pero allí, en ese momento, descubrí una faceta del Profesor Lions, su claridad a la hora de decir las cosas, pero también el respeto hacia su interlocutor, no importa que fuera un principiante que tenía muchas cosas por aprender. Siempre me pareció una persona con educación exquisita. Pasados los años me honró con su amistad y aceptó la invitación que le cursé para asistir al encuentro internacional sobre Control de Ecuaciones en Derivadas Parciales que organizamos en Laredo, en 1994. Pero en aquel congreso, sentado frente a él en la cena de clausura, yo pensaba que había comenzado conociendo a un gran matemático y había terminado por descubrir a un gran hombre.

El legado de Jacques-Louis Lions (1928-2001) a través de sus libros: mi limitada visión

J. I. Díaz

Departamento de Matemática Aplicada
Universidad Complutense
28040 Madrid

jidiaz@sunma4.mat.ucm.es

El 17 de mayo de 2001 fallecía en París uno de los matemáticos más distinguidos del siglo XX: Jacques-Louis Lions.

El legado de Jacques-Louis Lions va mucho más allá de sus 20 libros y casi 600 publicaciones[1]. Su intuición excepcional y una capacidad de trabajo fuera de lo normal le llevaron a abrir nuevos campos de desarrollo para la matemática cultivados después por numerosos especialistas. Fundador de lo que se podría denominar como Matemática Aplicada francesa, su obra ha dejado también una enorme huella en otros muchos paises y en especial en el nuestro. Su activa participación como formador de doctores españoles[2] (lista que comenzaría en los sesenta con Antonio Valle Sánchez y se extendería más tarde a J.A. Fernández Viña, J. L. Andrés Yebra, C. Fernández Pérez y M. Lobo Hidalgo)[3] fue reconocida con su nombramiento como Doctor Honoris Causa por las universidades Complutense, Politécnica de Madrid, Santiago de Compostela y Málaga, y como miembro extranjero de la Real Academia de Ciencias.

Desde la triste fecha de su desaparición han sido muchos los obituarios dedicados a su figura (véase por ejemplo Temam [113], Magenes [107], Ciarlet [11], el dedicado por la AMS a cargo de Lax, Magenes y Temam [42], las notas

[1]La gran actividad mantenida hasta unos meses antes de que le venciera la enfermedad explica que puedan existir trabajos suyos aún en trámites de publicación.

[2]Su primera visita a España data de 1963. Su viaje, financiado por la Embajada de Francia, consistió en tres etapas (Barcelona, Zaragoza y Madrid) en las que impartió una serie de conferencias de las que existen unas notas escritas ([57]). Fue con ocasión de ese viaje cuando entabló gran amistad con Alberto Dou, quien desde entonces favoreció, de manera providencial, los contactos con él y su escuela.

[3]No siempre figuraría oficialmente como su director y, de hecho, su labor de formación se extendió a muchos otros "jovenes" matemáticos españoles.

aparecidas en nuestro país, Valle [115], Díaz [18], y los *Temoignages*[4] vertidos en el número 55**,** de octubre de 2001, de la revista *Matapli* de la sociedad francesa SMAI. Seguramente, muchos otros están por aparecer. A parte de pequeños *workshops* que colateralmente recuerdan su obra, un gran coloquio en su honor ha sido organizado a celebrar en París, del 1 al 5 de julio de este año[5]. Pese a la magnitud de ese evento estoy seguro que no será el último que se organice con esa finalidad.

Cuando los directores de esta revista tuvieron la gentileza de invitarme a escribir una notas sobre el profesor Lions me sugirieron abordar prioritariamente una descripción de su obra científica, dada la avalancha de testimonios de otro tipo que se iba a producir en los que sus responsabilidades en grandes centros e instituciones (INRIA, CNES, UMI, Académie des Sciences, del año mundial de las Matemáticas, etc.) serían objeto de consideración.

Entre otras opciones posibles, me decanté por utilizar la cronología de sus libros como jalones indicativos de tan abrumador empeño, con la intención de ilustrar, aunque sólo fuese de manera sucinta, su inmensa obra[6]. Pero esta perspectiva no podrá dejar de ser limitada en varios sentidos. En primer lugar, difícilmente puede dejar de ser limitado un artículo de este estilo cuando existe tal diferencia de talla científica entre quien lo escribe y el homenajeado. Pero además, el artículo aparece también limitado pues se trata de una glosa en alguna manera inacabada: lo comencé antes del verano del año pasado y lo cierro ahora, en enero de 2002, siguiendo la sugerencia de los directores de la revista de no aplazar su aparición por más tiempo. Cada vez que lo releía añadía nuevos comentarios y referencias y otros muchos que me venían a la cabeza quedaban sin plasmar. Temía que esto se pudiese alargar eternamente, por lo que tomé como buena la sugerencia de los directores. Finalmente, no quisiera dejar de señalar que la redacción de estas líneas está en deuda con numerosos amigos y colegas que leyeron y enriquecieron el manuscrito.

1 De su tesis doctoral a su primer libro: problemas de contorno lineales

Jacques-Louis Lions nació en Grasse, un bello pueblo cercano a Niza. Su padre fue alcalde de dicha localidad durante casi treinta años. Su mujer, Andrée, que le ha sobrevivido, también es oriunda de allí. Los Lions disfrutaban pasando las vacaciones en su localidad natal, alternando con otras estancias en la montaña. La luminosidad y peculiaridades del sur de Francia seguramente impregnaron

[4]Debidos a J. P. Aubin, A. Bensoussan, J. Cea, J.-P. Dias, J.I. Díaz, E. Magenes, J. Periaux, O. Pironneau, J. P. Puel, P.-A. Raviart, E. Rofman, R. Temam, A. Theis, G. Tronel y E. Zuazua.

[5]Información detallada sobre el coloquio y sobre otros testimonios aparecidos sobre Jacques-Louis Lions pueden encontrarse en la página http://acm.emath.fr/congres-jllions

[6]J.-L. Lions solía facilitar únicamente la lista de sus libros junto a una breve descripción de los detalles de su perfil académico y un breve listado de sus distinciones más sobresalientes cuando le requerían su curriculum por motivos oficiales. De alguna manera, otorgaba a sus libros carta de representatividad de su dilatada obra científica.

el carácter abierto y optimista de Lions[7], quien hacía gala, en sobremesas distendidas, del privilegio de ser mediterráneo. Por deseo suyo, sus restos reposan en Grasse.

Su periodo de formación universitaria le llevaría a París, donde ingresaría y permanecería, de 1947 a 1950, en la Ecole Normale Supérieur, una institución creada en tiempos de Napoleón que acoge a los alumnos más brillantes de cada promoción tras unas pruebas de selección de gran dificultad. Su primer puesto de trabajo fue como investigador, sin docencia, en el CNRS, trabajando bajo la dirección de Laurent Schwartz, quien había recibido la *medalla Fields,* en 1950, por su *teoría de las distribuciones.* El tema de tesis de Lions, así como el de otros alumnos de Schwartz, Bernard Malgrange y François Treves, era el desarrollo de la aplicabilidad de la *teoría de las distribuciones* a los problemas de contorno, tema que el propio Schwartz apenas abordaría a lo largo de su dilatada obra[8].

En junio de 1955 y tras una serie de notas en las Comptes Rendus de la Académie des Sciences de París[9], Lions defendía su tesis ([49]), en París, en la que sistematizaba la aplicación de la teoría de las distribuciones a los problemas lineales de contorno. Eran los inicios de una manera de abordar esos problemas de ecuaciones en derivadas parciales mediante la aplicación de resultados abstractos del Análisis Funcional en espacios de Banach y del que el famoso *Lema de Lax-Milgram* ([43]) es un excelente ejemplo para el caso de ecuaciones elípticas. Lions pronto amplió el espectro de problemas considerado en su tesis, abordando numerosos problemas diferentes como, por ejemplo, el dificil caso de las condiciones de contorno de tipo oblicuo ([50]) o el de los problemas lineales de evolución (tanto parabólicos como hiperbólicos) para los que obtuvo un resultado abstracto semejante al de Lax-Milgram y que hoy día es denominado como *Teorema de Lions* en los textos de Análisis Funcional y de Ecuaciones en Derivadas Parciales (véase, por ejemplo, el texto de Brezis [10]). La sistematización de esas contribuciones le conduciría a su primer libro ([55]) que publicaría en 1961 aludiendo a las *ecuaciones diferenciales operacionales* por referirse a ecuaciones abstractas, $u'(t) + Au(t) = f(t)$, sobre espacios de Banach en los que "los coeficientes" dependientes de la solución $u(t)$ vienen dados por un operador no acotado $Au(t)$.

[7]En lo que sigue me referiré a Jacques-Louis Lions meramente por su apellido, especificando su nombre únicamente en caso de posible confusión con su hijo Pierre-Louis.

[8]Lions y Schwartz escribieron un único artículo en colaboración (Lions y Schwartz [92]), de interés marginal para el conjunto de sus obras científicas. En mi opinión, y como se puede deducir de la descripción de sus inquietudes en su autobiografía (véase Schwartz [110]) el interés de Schwartz por las aplicaciones fue mucho más tenue. Pese a esta obvia diferencia, Lions mantenía un gran aprecio y guardaba un recuerdo constante de sus años bajo la dirección de Schwartz. En una ocasión me comentó que preparando las palabras de agradecimiento ante la recepción de la Legión de Honor (en grado de Commandeur) que le entregaría Miterrand unos días más tarde, en 1993, todavía le venía a la cabeza la figura de Schwartz diciéndole que su discurso se podía refinar aún más.

[9]Ésta sería una revista muy apreciada por él a lo largo del resto de su vida científica. En ella presentaría, de manera sistemática, las primeras versiones de sus contribuciones. Lions contribuyó, de manera crucial, a la buena salud que hoy goza tal revista, potenciando la publicación en ella entre sus discípulos, colaboradores y otros autores.

2 Actividad en frentes simultáneos: cuasi-reversibilidad

La actividad de Lions dejará pronto huellas de un interés desplegado en diferentes líneas de investigación. Así, en breve sus trabajos tratarían sobre un tema distinto al de su tesis: el estudio de los soportes para productos de composición y la transformada de Laplace ([47], [48]). En el mismo periodo de elaboración de lo que sería su primer libro también había abordado temas muy diversos tales como el estudio de los espacios de Beppo Levi (junto a J. Deny, [16]), los espacios definidos por una integral de Dirichlet (en colaboración con L. Hörmander [38]), la *transmutación* de operadores diferenciales en el campo complejo (con J. Delsarte [15]). También había comenzado la consideración de temas que, más tarde, serían objeto de sendos libros: los problemas no lineales ([52]) y la interpolación de espacios[10] y sus aplicaciones ([53]).

En 1967 Lions publicaba su segundo libro (en colaboración con Lattès [41]), que traduciría al inglés[11] el mismísimo R. Bellman. Trataba de un tema distinto a los anteriores: el estudio de las condiciones bajo las cuales un problema en ecuaciones en derivadas parciales está "bien puesto" (en el sentido de J. Hadamard) y cuándo es posible vulnerar esas condiciones generales para "hacer reversible" lo que usualmente no lo es. A diferencia de otras ocasiones, la colaboración con R. Lattès no tenía más antecedente que un pequeño trabajo conjunto ([40]).

3 Periodo de actividad mágica: problemas no homogéneos, control y problemas no lineales

En el periodo en que redactaba esos dos libros, Lions desplegó una actividad investigadora que le llevaría a publicar tres libros en 1968, seguidos de otros dos muy cercanos en el tiempo; uno en 1969 y otro en 1970.

Tres de los libros antes mencionados se refieren a la obra en colaboración con Enrico Magenes[12] ([84]) desarrollada con una larga serie de artículos que se iniciaba en 1960. En este caso, el objetivo que los autores abordaban era los *problemas de contorno no homogéneos.* En la práctica, las ecuaciones en derivadas parciales y/o las condiciones de contorno no son homogéneas sino que vienen igualadas a unas funciones independientes de la incógnita del problema (ya sea escalar o vectorial). Se trataba de caracterizar, con la mayor precisión posible, los espacios funcionales requeridos para que tales problemas estuviesen

[10] Esta sería una de sus aportaciones más cercanas a lo que se podría denominar "matemática pura": partiendo de una función perteneciente a dos espacios vectoriales topológicos distintos, se trata de caracterizar los muchos otros espacios en los que esa función queda automáticamente inmersa.

[11] Un aspecto permanente en cada uno de los libros de Lions, sobre el que no volveré a incidir, es su traducción a otros idiomas, entre los cuales el inglés y el ruso son fijos y a veces incluyen el japonés y el chino. A Lions le gustaba hacer referencia explícita a los nombres de los traductores.

[12] Magenes se convertiría en uno de sus mejores amigos. Sería quien pronunciase unas palabras de reconocimiento en los dos homenajes celebrados en París con motivo del 60 y 70 aniversarios de Lions.

bien planteados. Era necesario ir más allá de los espacios de Sobolev de índices naturales (introducidos por L. A. Sobolev a finales de los años treinta) y recurrir a datos en espacios de Sobolev de índices negativos y fraccionarios de manera que las "energías asociadas" a las soluciones estuviesen bien definidas. Las soluciones de los problemas de contorno no tienen por qué ser funciones continuas, aunque siempre son integrables en el sentido de Lebesgue y la correcta interpretación de su *traza,* o restricción, sobre un conjunto de medida nula (como es el borde del abierto sobre el que se plantea la ecuación en derivadas parciales) requiere un análisis fino. En realidad, en el periodo entre 1957 y 1968, Lions estaba desarrollando en paralelo la *teoría de la interpolación* entre espacios de Hilbert, o de Banach, cuyas aplicaciones al caso de los espacios de Sobolev suministraban la materia prima de su extensa y sistemática obra con Magenes. Parece que Lions comenzó a interesarse por estos temas a raíz de una estancia posdoctoral de un año en la Universidad de Kansas con Nachman Aronszajn. Lions comenzó aplicando métodos de la teoría de funciones de variable compleja (al igual que lo haría A. Calderón). Más tarde (bien mediante contribuciones suyas o en colaboración con C. Foias [30] y en especial con J. Peetre [85]) desarrolló nuevos métodos, esta vez de funciones de variable real.

Otro de los libros antes aludidos, en lo que muy bien se podría denominar como "periodo de actividad mágica" de Lions, se refiere a un campo distinto a los anteriores que pasaría a ser su campo principal de actividad[13]: *la Teoría de Control*. El acercamiento de Lions hacia ese tema vino precedido de un trabajo de 1965, en colaboración con Guido Stampacchia ([93], [94]), sobre *inecuaciones variacionales,* tema muy cercano al Cálculo de Variaciones al que me referiré más adelante. Es a partir de 1966 cuando Lions se plantea dar respuesta a una pregunta tan general y ambiciosa como ésta: ¿es posible "controlar" los sistemas regidos por ecuaciones en derivadas parciales? Las herramientas de la Teoría de Control asequibles en ese momento eran el *principio del máximo de Pontryaguin*, el de la *programación dinámica de Bellman* y la *teoría del filtro de R. Kalman*[14]: todas ellas introducidas para sistemas finito-dimensionales dados por ecuaciones diferenciales ordinarias. El impulso decisivo para su extensión a sistemas infinito-dimensionales, regidos por ecuaciones en derivadas parciales, fue dado por Lions en una serie de tres notas en 1966 ([59])[15] a las que siguió su libro ([60]) que no ha cesado de ser objeto obligado de referencia por haber marcado "un antes y un después" en esa teoría, abriendo un fértil campo de investigación.

El último libro, que culmina el "periodo de actividad mágica" de Lions es el dedicado a problemas no lineales aparecido en 1969 ([61]). Tras las breves notas, de 1958, dedicadas a problemas cuasilineales ([52]), Lions se ocupó, en 1959, del

[13]La cátedra del Collège de France que ocuparía Lions desde 1973 hasta su jubilación, en 1998, llevaba como título el de *Analyse Mathématique des Systèmes et de leur Contrôle.*

[14]Lions me comentó en varias ocasiones su profunda admiración por el resultado de Kalman que, en particular, hacía posible el control "en tiempo real" de las trayectorias de las naves espaciales tras fluctuaciones imprevistas.

[15]Un testigo excepcional de aquel momento crucial para la teoría de control para EDPs fue Antonio Valle. Lions citó, durante bastante tiempo, los resultados obtenidos bajo su dirección (Valle [114]).

sistema de ecuaciones de Navier-Stokes que modela la dinámica de los fluidos incompresibles. Pese a las profundas contribuciones sobre tan fundamental sistema, que parten ya de la obra de L. Euler, este complicado problema no lineal no había recibido un tratamiento matemático general hasta la aparición de los resultados de Jean Leray en una serie de trabajos de comienzos de los años treinta (véase, por ejemplo, [44]). La existencia de soluciones globales en el tiempo, para el caso tridimensional y bajo adecuadas hipótesis, fue obtenida en 1950 por E. Hopf. En su nota ([54]) Lions simplificó y extendió el resultado de Hopf, abordando la cuestión de la unicidad de soluciones, para el caso bidimensional[16] en colaboración con G. Prodi[17] ([87]). De esta manera, sus contribuciones junto a las de O.A. Ladyzhenskaya y J. Serrin, daban cuerpo a la forma usual en la que se presenta ahora el tratamiento matemático de la dinámica de fluidos incompresibles (véase, por ejemplo Temam, [112]). Su afamado libro de problemas no lineales fue la fuente en la que muchos autores, entre los que me cuento, iniciaron sus pasos. El texto, abarcaba una gama enormemente variada de problemas no lineales, presentados de una manera altamente original y pedagógica; no tanto en atención al problema particular considerado sino organizado en diferentes capítulos según los métodos empleados. Lions recogía en él tanto sus resultados sobre ecuaciones de evolución no li-neales (obtenidos con W. A. Strauss [95]) como los obtenidos con su admirado J. Leray [18] ([45]), sobre ecuaciones elípticas cuasilineales motivadas por el Cálculo de Variaciones, provenientes en ciertos casos particulares, como ecuaciones de Euler-Lagrange asociadas a puntos estacionarios de adecuados funcionales.

Un capítulo de lectura obligada durante muchos años fue el dedicado al método de monotonía. Los resultados abstractos de la teoría lineal (como el *Lema de Lax-Milgram* o los de su tesis) ahora requerían la noción de *operador monótono* ya sea de un espacio de Hilbert en su dual o bien en sí mismo[19]. El

[16]El problema de la unicidad de soluciones globales y el estudio de posibles singularidades para datos iniciales generales es uno de los siete problemas abiertos que la Fundación Clay distinguió en el 2000 dotando su resolución con un millón de dolares.

[17]Hermano de Romano Prodi, ex-Primer Ministro del gobierno italiano y actual presidente de la Unión Europea.

[18]Lions dejó muchas trazas de su gran admiración por la obra de Leray, encumbrado al Collège de France anteriormente a él. Recuerdo que una noche de mayo de 1998, cenando con él y su esposa, Andrée, en el restaurante "Le coupe chou", cercano al Collège y al que acudía con asiduidad con sus invitados, nos rogó que le dispensásemos pues Leray le había pedido que le telefoneara a las nueve en punto para terminar una conversación iniciada en la mañana. Lions tenía entonces 71 años y Leray 93. En aquella cena me contó detalles sobre como Leray había rehecho, sin saberlo, resultados previos sofisticados a la hora de culminar su artículo en común.

[19]El lector no ha leído mal: pese a que el *teorema de Riesz* permite identificar el dual de un espacio de Hilbert a sí mismo, tal identificación no puede ser aplicada cuando se manejan a la vez dos espacios distintos (aunque uno tenga inclusión continua y densa en el otro $V \subset H$). En ese caso se alcanza lo que Lions, jocosamente, llamaba "trinidad" $V \subset H = H' \subset V'$. Con gran frecuencia el espacio H viene dado por $L^2(\Omega)$, donde Ω es un abierto acotado de $\mathbf{R}^N$. El espacio V suele corresponder a un espacio de Sobolev que incluye las condiciones de contorno (por ejemplo, $V = H_0^1(\Omega)$ para problemas de segundo orden y condiciones de Dirichlet homogéneas).

segundo de los casos es requerido a la hora de extender el *Teorema de Hille-Yosida* de generación de *semigrupos de contracciones* al caso de operadores no lineales. Lions ya se había ocupado tempranamente, en 1957 ([51]), de este bello teorema enlazando las ecuaciones diferenciales en espacios de Hilbert (de dimensión infinita en las aplicaciones a ecuaciones en derivadas parciales) y el Análisis Funcional. La noción de monotonía aparecía también ligada al Cálculo de Variaciones pues la *derivada Gâteaux* de un funcional (que igualada a cero expresa las ecuaciones de Euler-Lagrange) es un operador monótono, supuesto que el funcional sea convexo (propiedad satisfecha en numerosas aplicaciones relevantes). La *teoría de operadores monótonos* estaba siendo desarrollada, en paralelo, por muchos otros autores, tales como Eduardo Zarantonello, George Minty y, especialmente, Felix Browder. Una de las aportaciones fundamentales del trabajo de Leray y Lions [45] fue observar que bastaba que los términos de mayor orden de la ecuación en derivadas parciales fuesen monótonos, aunque la presencia de términos de orden inferior impidiesen que "todo" el operador lo fuese. Propusieron una noción abstracta a ese respecto (*operador del Cálculo de Variaciones*) que más tarde sería redondeada con la noción de *operador pseudo-monótono* por un joven discípulo de Lions en su tesis de tercer ciclo: Haïm Brezis. El libro de Lions extendía unas notas (tomadas por F. Murat) de su curso de tercer ciclo[20] en la universidad de París VI[21] en 1968/1969 que, de un carácter excepcionalmente exhaustivo para su tiempo, contenía también resultados originales suyos o de sus distintos alumnos[22].

4 Modelos: inecuaciones variacionales

Si la obra de Lions, hasta 1969, se puede enmarcar en dos campos típicos de su actividad (el Análisis Matemático y la Teoría de Control), otro de ellos, el de la construcción de modelos, no sería desarrollado sistemáticamente hasta que comenzó su colaboración con Georges Duvaut en el curso 1969-1970 ([25])[23]. Tal colaboración se plasmó en una serie de más de una decena de trabajos y culminaría con el texto [26] en el que se exponía, de manera sistemática, la obtención de modelos para numerosos problemas de la Mecánica y de la Física dados en términos no ya de ecuaciones sino de inecuaciones, que se pueden ilustrar, a modo de ejemplos elementales, mediante problemas de la Mecánica Analítica con ligaduras unilaterales[24]. El texto de Duvaut y Lions se centra en la

[20] Lions tenía por costumbre cambiar de año en año el tema de su curso de postgrado. Desde su afiliación en el Collège de France esto constituía su única obligación docente.

[21] Aunque impartido en el Institute Henri Poincaré.

[22] Lions agradece en el prólogo los comentarios recibidos de sus alumnos C. Bardos, H. Brezis, P. Raviart, L. Tartar y R. Temam.

[23] Como ya se ha comentado, Lions se había ocupado antes del análisis matemático de las ecuaciones de Navier-Stokes pero apenas desde el punto de vista de su obtención a partir de los principios fundamentales de la Mecánica de Fluidos.

[24] No viene mal recordar que si bien la definición de *ligadura unilateral* aparece en las primeras páginas de casi todos los textos de Mecánica Analítica, con el fin de distinguirla de la usual, de tipo *bilateral,* sin embargo, la práctica totalidad de los textos se limitan a la consideración de estas últimas (véase, como ejemplo indicativo, las primeras páginas del texto

consideración de ese tipo de ligaduras en el contexto de la Mecánica de Medios Continuos. Los antecedentes se remontan al llamado *problema de Signorini* en el que de un cuerpo elástico sólo se conoce su imposibilidad de penetrar (aunque con capacidad de apoyarse) en otro cuerpo rígido. Tras el tratamiento dado por G. Fichera [29], Guido Stampacchia había encontrado en [111] un resultado abstracto (generalizando el *Lema de Lax-Milgram*) que permitía mostrar la existencia de solución para inecuaciones variacionales de tipo estacionario. La sistematización matemática a casos más generales y, especialmente, a problemas dinámicos fue fruto de la colaboración entre Stampacchia y Lions ([93], [94]). Con su libro, Duvaut y Lions mostraron la universalidad de ese tipo de formulaciones al hacerlas emerger en contextos insospechados: desde problemas de climatización, flujos de fluidos no-newtonianos (como los polímeros, la lava, los glaciares, etc.), hasta problemas de antenas formulados en términos de inecuaciones variacionales asociadas a las ecuaciones de Maxwell.

En dos libros escritos con Alain Bensoussan ([3], [4]), Lions analizaría las aplicaciones de las inecuaciones variacionales a la *teoría de Control Estocástico* y al *Control impulsional*. Ambos textos son fruto de una intensa colaboración [25] que se inició en 1972 a raíz de la creación por Lions del IRIA (más tarde INRIA). Contienen una gran cantidad de conexiones con problemas planteados en Economía[26]. En el primero de esos libros se ofrece un tratamiento muy exhaustivo de la posibilidad de obtener expresiones formalmente explícitas de las soluciones de EDPs (incluso no lineales). En el caso de las ecuaciones hiperbólicas de primer orden es bien sabido que su solución viene dada explícitamente en términos de las características. En el caso de las ecuaciones parabólicas o elípticas se tienen fórmulas semejantes pero ahora las características deben ser reemplazadas por *procesos estocásticos*. Los métodos probabilisticos aplicados a EDPs son muy adecuados para obtener estimaciones en L^∞ frente a las estimaciones en espacios de Sobolev obtenidas por métodos de energía.

En este libro, Bensoussan y Lions abordan las *ecuaciones de Hamilton-Jacobi* y *problemas de la teoría de juegos* asociados a procesos de control estocástico denominados de *tiempo de parada*. Es por esto que, a mi juicio, el libro puede entenderse como antesala de una buena parte de la obra de Pierre-Louis Lions, quien años más tarde llevaría a cabo un tratamiento mucho más sistemático y general de las ecuaciones de Hamilton-Jacobi (P.L. Lions [104]) que no están en forma divergencial para las que introduciría (junto a Mike Crandall) la crucial

de Goldstein [36]).

[25] Tal colaboración se mantuvo viva hasta el final de sus días. De la gran cercanía entre ambos da buena fe el hecho de que sería Alain Bensoussan (entre los muchos discipulos de Lions con una obra excepcional) quien le sucedería (por dos veces) al abanonar la presidencia del INRIA, primero, y más tarde del CNES (en ese caso no de forma consecutiva).

[26] En realidad la colaboración entre ellos comenzó en torno al Análisis Numérico. Tal y como me señaló Lions, su articulo conjunto con Temam ([7]) de más de 150 páginas podría considerarse como un libro. Curiosamente, aunque tal trabajo apenas fue mencionado en su día entre los especialistas (apareció en las actas de un congreso), en los últimos años está siendo muy citado (especialmente desde que Lions se ocupase, junto con Pironneau, de los métodos de descomposición para el cálculo paralelo).

noción de *soluciones de viscosidad* [27].

El primero de los libros fruto de la colaboración entre Lions y Bensoussan recoge, tempranamente, la construcción de un modelo matemático sofisticado (dado en términos de inecuaciones variacionales) para problemas provenientes ahora (a diferencia del libro con Duvaut) de Economía como, por ejemplo, problemas de opciones mercantiles (allí denominado *Probleme de Warrant*) abordado originalmente en Samuelson-Mac Kean ([108]) antes de la explosión de los modelos matemáticos sobre el riesgo en mercados financieros cuyo exponente más famoso es la conocida ecuación de Black-Scholes [28]. El interés de Lions por mode-los provenientes de la Economía se mantendría a lo largo de su vida (véanse, por ejemplo su trabajos sobre los equilibrios de Pareto ([69]y nuestro artículo en común sobre esos temas [23]).

Ese libro contiene también unos resultados sobre estimaciones de localización de fronteras libres (previamente publicado en forma de artículo en [2]) que abundaba en un resultado pionero de Brezis ([10]). Lions fue uno de los fundadores del amplio campo de los denominados *Free Boundary Problems* que hoy día cultivan multitud de especialistas. No sólo consideró tempranamente las inecuaciones variacionales como problemas típicos que originan fronteras libres (delimitando las regiones donde se alcanzan las restricciones impuestas). Su libro sobre problemas no lineales ([61]) dedicaba también una enorme atención (inusual para la época) a otros problemas de frontera libre que luego han sido objeto de atención pormenorizada y monografías especializadas tales como el problema de Stefan, la ecuación de los medios porosos y diversas ecuaciones para el p-Laplaciano[29].

El segundo libro fruto de la colaboración con Bensoussan ([4]) fue concebido como una continuación de [3]. Los problemas de control considerados se refieren al caso en el que, entre otras cosas, se ha de decidir en qué instantes y con qué impulso se actúa sobre un sistema complejo. Es el llamado *control impulsional* que tiene gran relevancia en las aplicaciones (por ejemplo, en el caso de las centrales hidráulicas) y que conducen a una variante de las inecuaciones variacionales en las que *el obstáculo* depende de la propia solución: son las denominadas *inecuaciones cuasivariacionales*. Además de poseer interesantes aplicaciones a problemas surgidos de la Economía, años más tarde se vería que tal tipo de modelos son de interés también en ciertos problemas de la Mecánica de Medios Continuos (véase, por ejemplo, la monografía de Baiocchi y Capelo [1]). Lions haría una sucinta presentación del contenido de sus dos libros

[27] Los dos excepecionales matemáticos (Jacques-Louis y su hijo Pierre-Louis) apenas se harían mención mutua en sus trabajos. Unicamente, a raiz de la incursión de Pierre-Louis en problemas de la Mecánica de Fluidos, las citas (especialmente del padre a los dos libros de su hijo sobre el tema: [106]) se harían algo más frecuentes, aunque, en todo caso, en grado muy reducido.

[28] El reconocimiento de la importancia del estudio matemático de los "derivados financieros" llegaría en 1997 con la concesión a R.C. Merton y M. Scholes del premio Nobel en Economía. F. Black había fallecido en 1973.

[29] Lions participó de manera activa en los primeros congresos monográficos que se celebraron sobre el tema. Asímismo inauguró la nueva revista *Interfaces and Free Boundaries* con su artículo (Lions [81]).

con Bensoussan en varios cursos que luego aparecerían publicados en forma de libros y que contenían también nuevos resultados y otros temas distintos: el que impartió en la Universidad de Montreal[30] en 1976 ([64]) y el impartido en Beijing en 1981 y que citaba con frecuencia ([66]).

5 Análisis numérico de EDPs

Desde sus comienzos, el nombre de Lions ha sido asociado al tratamiento matemático de los mayores problemas tecnológicos (tanto de su país como de la esfera internacional) inquietud que contrastaba con el espíEl tratamiento de esos sistemas complejos no podría limitarse, obviamente, a aspectos teóricos y cualitativos sino que requería ineludiblemente una aproximación cuantitativa en términos de algoritmos del Análisis Numérico. Sin embargo, es curioso que la primera *publicación oficial* de Lions sobre Análisis Numérico data de 1966 (Lions-Raviart [88]) pese a que su interés en ese campo tuviera sus orígenes en 1958 cuando impartió diferentes cursos sobre el tema tras su llegada a la Universidad de Nancy (de la que fue profesor de 1954 a 1962). De hecho, Lions impartió tempranamente cursos en ParíNancy: lo hizo en el CEA (la agencia francesa de energía nuclear) y más tarde lo haría en Electricité de France, el Instituto del CNRS Blaise Pascal (cuyas notas aparecerían en tres tomos ([58])) y en su propia universidad parisina. Fruto de sus enseñanzas y dirección arrancarían las carreras de prestigiosos especialistas tales como J. Cea, P.A. Raviart, R. Temam, J.P. Aubin, Ph. Ciarlet, R. Glowinski y muchos otros.

Comenzó interesándose por métodos en diferencias finitas. Mámétodo de elementos finitos (aunque en aquellas fechas no fuese denominado como tal) discretizando, no ya la propia ecuación en derivadas parciales sino la formulación variacional correspondiente, dada en términos de multiplicación por adecuadas funciones *test*, para los problemas de contorno que él había sistematizado en su propia tesis. El mérudimentaria por los ingenieros pero le faltaba una fundamentación matemática. A continuación, centró su atención en las condiciones de estabilidad de los algoritmos (tesis de Raviart) y en algoritmos de descomposición (trabajos en colaboración con Temam y Bensoussan). Unas notas de sus cursos de Análisis Numérico, tomadas por sus estudiantes en 1961 (que comenzó impartiendo en la que más tarde pasaría a ser la Universidad París VI) aparecerían en 1973 ([62]) al hacerse cargo de un curso análogo en la Ecole Polytechnique (que mantendría entre 1966 y 1986).

Las etapas naturales que se le planteaban a continuación fueron las de desarrollar métodos de aproximación para las inecuaciones variacionales y la Teoría de Control. La primera tarea la comenzó con su artículo ([63]) y culminó con la

[30]Tuve ocasión personal de constatar tempranamente la generosidad y atención de Lions hacia los más jóvenes cuando, en 1976, tras haber visitado Madrid para recibir el nombramiento de Doctor Honoris Causa por la Universidad Complutense, Jose Luis Andrés Yebra y yo le escribimos solicitandole información sobre las notas de aquel curso. Su respuesta nos dejó impresionados: a vuelta de correo mandó a Jose Luis (antiguo alumno suyo) una copia, de más de trescientas páginas, de sus notas manuscritas (de su puño y letra) de lo que luego sería el texto de su libro y que conservamos como valiosa joya.

publicación, en 1976, de dos volúmenes en colaboración con R. Glowinski y R. Trémolieres ([35]) y la segunda, años más tarde con una serie de artículos en los que Glowinski sería de nuevo su colaborador principal: [32] en 1990 y [33], en 1995 (este último de más de 300 páginas publicado en los dos primeros números de la revista *Acta Numérica*).

Tan sólo unos años antes de su muerte comenzaría a desarrollar un ambicioso programa sobre la adecuada formulación de procesos de descomposición para el cálculo paralelo[31]. Esto le llevó a preparar un largo listado de notas en las Comptes Rendues en colaboración principalmente con O. Pironneau, aunque también con Glowinski y otros autores (véase, por ejemplo, [86], [34] y sus referencias), llegando a anunciar un libro en preparación sobre el tema en colaboración con Pironneau[32].

6 Perturbaciones singulares y Homogeneización

El curso 1970/71 Lions comenzó a impartir una serie de cursos de doctorado sobre problemas de contorno conteniendo un pequeño parámetro, ε, en alguno de los muchos datos posibles de su formulación (término independiente, datos en el contorno, operador diferencial, dominio, etc.) y que en general respondía a regularizaciones del problema limite formal obtenido para $\varepsilon = 0$. De nuevo, su propósito era dar una coherencia matemática a diferentes métodos asintóticos, técnicas clásicas de la Matemática Aplicada (véanse, por ejemplo, el texto de Eckhaus [27]), de uso frecuente en Ingeniería[33], pero con enormes dificultades para justificar resultados rigurosos de convergencia en los espacios funcionales en los que "debía" encontrarse la "solución límite". Un primer resultado de esas inquietudes fue una serie de artículos que culminará con el voluminoso Lecture Notes de la Serie de Springer-Verlag aparecido en 1973 ([65]).

Esa nueva línea de investigación tendría su continuación natural en una larga colaboración con A. Bensoussan y G. Papanicolau (que comenzó con [6]) y que cristalizó con el famoso libro Bensoussan-Lions-Papanicolau [5]) en el que se sistematizaba el llamado *método de homogeneización* referente al estudio de problemas involucrando dos escalas características (espaciales o temporales) bien distintas: una microscópica, rápidamente oscilante, y la macroscópica. Estos métodos se revelaron fundamentales para el estudio de numerosos problemas tales como la construcción de modelos matemáticos para multi-estructuras elásticas (sólidos tridimensionales acoplados con paneles, varillas, etc.), flujos de fluidos en medios porosos y fabricación de nuevos materiales a través de materiales compuestos. El desarrollo matemático de

[31] A este respecto solía mencionar el artículo de Pierre-Louis Lions ([105]) como un avance conceptual relevante.

[32] Quizás debido a sus responsabilidades en grandes instituciones, Lions se mantenía muy al día sobre los progresos en las capacidades de computación de las distintas generaciones de superordenadores. Se ocupó del tema en varios artículos y libros de caracter divulgativo ([46], [75], [73], [24]). A este respecto, manifestó reiteradamente su admiración por la clarividencia de J. von Neumann.

[33] Uno de los ejemplos más ilustrativos es la teoría de la *capa límite* de Prandtl en Hidrodinámica.

ese tipo de técnicas tuvo (y mantiene en la actualidad) un vigor excepcional desarrollado por alumnos directos como Tartar, Ciarlet, Murat y otros, y por matemáticos de gran prestigio como, por ejemplo, E. de Giorgi y O. Oleinik, por citar tan sólo dos de ellos[34].

7 Controlabilidad: el método HUM

Tras la publicación de su primer libro sobre control ([60]), Lions fue abordando nuevos problemas de esa teoría a medida que se iba embarcando en nuevas líneas de investigación. Así, por ejemplo, fue desarrollando, como capítulos aislados, el estudio del control para problemas con perturbaciones singulares y problemas de escalas múltiples.

En 1980 Lions centró su curso en el Collège de France sobre el control de sistemas distribuidos singulares en los que la ecuación de estado presenta singularidades y origina fenómenos peculiares tales como: inestabilidades, fenómenos de explosión en tiempo finito, soluciones múltiples, fenómenos de bifurcación, etc. Fruto de su atención por tales problemas (que mantendría hasta el final de sus días) fue el libro ([67]). Poco a poco fue interesándose más por cuestiones de controlabilidad que por el control óptimo. La controlabilidad para ecuaciones que dan lugar a fenómenos de explosión en tiempo finito atrajo de manera profunda su atención. Una conjetura que mantenía a este respecto era que a medida que un sistema generaba más inestabilidades era más fácil de controlar[35].

En 1986, con motivo de la conferencia impartida al recibir el premio "John von Neumann" otorgado por SIAM ([70]), Lions introdujo un nuevo método general para estudiar la controlabilidad de sistemas: el HUM o "Hilbert Uniqueness Method". Su idea clave fue la de construir unas nuevas normas en el espacio de los datos (condiciones iniciales, datos de contorno, etc.) y aplicar sofisticados teoremas de unicidad retrógrada del tipo de los debidos a Holmgren, Calderón o Mizohata. El método fue primeramente aplicado a ecuaciones hiperbólicas, dando lugar a dos volúmenes ([71]) que correspondían de nuevo a las notas de su curso en el Collège de France (esta vez tomadas por E. Zuazua). En un libro posterior, escrito en colaboración con Lagnese ([83]desarrolló la aplicabilidad de ese método al caso de problemas provenientes

[34]Es de resaltar el papel (más o menos implícito) que varios científicos españoles desempeñaron en los origenes de la teoría de la homogeneización, en especial de la mano de E. Sánchez Palencia quien se interesó muy tempranamente por ese tipo de técnicas, publicando su primer libro sobre el tema ([109]), en 1980. Sánchez-Palencia se instaló en París a mediados de los sesenta tras terminar sus estudios de ingeniero aeronáutico en la Escuela de Madrid e impartió, en 1965, un par de conferencias en el seminario sobre técnicas asintóticas organizado por Amable Liñán (destacado especialista en métodos de escalas múltiples aplicados a problemas de Mecánica de Fluidos y de Combustión). E. Sánchez Palencia mantuvo una estrecha relación con Lions (que se prolongaría hasta el final y que originó varios trabajos en colaboración: véase, por ejemplo, [89], [90] y [91]).

[35]Esto fue rigurosamente mostrado en dos trabajos en colaboración con E. Zuazua sobre ecuaciones de orden superior a dos ([102], [103]). Véanse también nuestros trabajos ([21], [22]) para la ecuación semilineal de orden dos.

de la Teoría de la Elasticidad.

Me parece interesante resaltar, por lo que tiene de significativo sobre las conexiones de la obra de Lions con nuestro país, que la (nada trivial) adaptación de esa fina técnica al caso de ecuaciones parabólicas la presentó Lions en las *Jornadas Hispano-Francesas sobre control de sistemas distribuidos* que, organizadas por Antonio Valle, tuvieron lugar en Málaga, en 1991. En su conferencia (que luego aparecería en las actas [76] y continuaría en [74]) Lions se refirió también a un problema que a partir de ese momento sería objeto de atención de los especialistas en el campo: la controlabilidad de las ecuaciones de Navier-Stokes. Entre los muchos trabajos a los que dieron origen sus conjeturas son de citar los de E. Fernández-Cara ([28], sobre una versión debilitada de la controlabilidad), Coron ([12], para el caso de las ecuaciones de Euler), Fursikov-Imanuvilov [31], Lions-Zuazua ([99], [100], [101] en los que se da un resultado de controlabilidad genérica para el sistema de Stokes y respuestas en términos del desarrollo de Galerkin) e Imanuvilov [39], entre otros muchos trabajos de esos y otros especialistas.

Estos nuevos métodos de demostración de la controlabilidad (aproximada) para ecuaciones parabólicas contrastan con los establecidos previamente por Lions en su libro ([60]) que tenían un carácter no constructivo (empleaban el Teorema de Hahn-Banach). Gracias al carácter constructivo ahora introducido se hizo posible la aproximación numérica de los controles (programa desarrollado principalmente por Lions y Glowinski al que ya me he referido anteriormente).

8 Enciclopedias: Dautray y Ciarlet.

Una descripción de la obra de Lions sería necesariamente parcial sin aludir a su inmensa labor de edición y, más en particular, a la enciclopédia, de mas de cuatro mil páginas[36] concebida y coordinada en colaboración con Robert Dautray entre 1984 y 1985 ([14]). Su título, *Analyse Mathématique et Calcul Numérique pour les Sciences et les Techniques*, da idea de la ambición de la tarea emprendida. La enciclopédia podría ser catalogada como una visión actualizada de la crucial obra de Courant y Hilbert ([13]). Muchos son los temas que no aparecían ni siquiera esbozados en aquella obra de la primera mitad de los cincuenta. Pero como se indica en el prólogo de Dautray y Lions

> La llegada de los ordenadores, sus progresos inmensos e incesantes, han permitido -por primera vez en la historia- calcular con gran seguridad y rapidez, a partir de modelos, cantidades que hasta entonces no habían podido ser más que estimadas de manera muy aproximada. Esto brindó, a investigadores e ingenieros, la posibilidad fundamental de poder utilizar resultados numéricos para la modificación o adaptación de razonamientos, experiencias y realizaciones en curso.

[36] Llama la atención que el listado de colaboradores de tan magna obra se limite a 17 matemáticos franceses, aunque todos ellos de reconocido prestigio internacional de la talla del fallecido Philippe Benilan.

Lions formó parte del comité editorial de un numero casi interminable de revistas y de series de libros. Sin embargo, a él le gustaba resaltar en especial la serie de 12 volúmenes coeditados con Haïm Brezis en Pitman-Longman conteniendo buena parte de las conferencias tenidas en el Seminario semanal que ambos mantuvieron en el Collège de France y que se prolongarían en dos volúmenes más, desde el 1998, esta vez coeditado con Doina Cioranescu. Asimismo, prestó una especial atención a dos series de libros publicados por Masson, ambas coeditadas con P.G. Ciarlet (*Mathématiques Apliquées pour la Maîtrise*, de 21 volúmenes, y *Recherches en Mathématiques Appliquées*, de 42 volúmenes). Finalmente, había comenzado, de nuevo con P.G. Ciarlet, la publicación del *Handbook of Numerical Analysis*, en North-Holland, del que de momento han aparecido 7 volúmenes a los que seguirán otros que están en trámites de publicación.

9 Medio Ambiente: Centinelas para datos incompletos y "El planeta Tierra".

El primer testimonio oficial del interés de Lions por temas de Medio Ambiente (entendido en un sentido amplio que incluye campos tales como la Meteorología, Climatología, Oceanografía, Ecología, etc.) parece ser que fue su conferencia *Pollution, Atmosphère et Climat* impartida en el Colloque Présidence de l'Assemblée Nationale, Hôtel de Lassay, París, el 4 de marzo de 1989. Desde el punto de vista matemático, su interés se acrecentó a medida que iba desarrollando la *teoría de los centinelas* que introdujo para el tratamiento de *sistemas con datos incompletos* (característicos en procesos del Medio Ambiente) en una serie de Notas en las Comptes Rendus ([72]) y que más tarde darían lugar a su libro [77]. Roger Temam subraya en [113] que quizás fuese el hecho de presidir, en 1990, el CNES (Centre National d'Etudes Spatiales) y el Consejo Científico de la Agencia Meterorológica francesa lo que le llevase a ocuparse de ese tipo de temas. En todo caso, lo que me parece digno de reseñar es que fue con motivo del curso que impartió en el Instituto de España, del 15 al 19 de enero de 1990, con el que aparecería el primer trabajo de Lions al respecto. Las notas de su curso (que él trajo previamente mecanografiadas en francés) darían lugar a su libro de divulgación *El Planeta Tierra: el papel de las matemáticas y los superordenadores* que tuve el honor y el placer de traducir al castellano (junto a Miguel Artola). Ello me dio la oportunidad de sugerirle algunos comentarios. El libro apareció publicado en Espasa-Calpe ([73]) junto a un apéndice, de carácter más técnico, para el que solicitó mi colaboración.

En una serie de artículos con Roger Temam y Shouhong Wang (que comenzaron con dos largos artículos [96], [97]) Lions y esos autores lograron culminar el análisis matemático de las ecuaciones que gobiernan el movimiento de la atmósfera, el océano, el sistema acoplado atmósfera-océano [98][37], y que venían siendo utilizadas para la previsión computacional desde los años sesenta en que su admirado von Neumann abordara tan complejo programa.

[37]De hecho, Lions incluía este largo trabajo en su lista de libros.

Desarrollaron también estudios rigurosos de tipo asintótico y numérico. Con motivo de su nombramiento como miembro extranjero de la Real Academia de Ciencias española, Lions impartió una conferencia ([80]) en la que se refirió al programa japonés sobre "El simulador de la Tierra" en el que el objetivo es acoplar globalmente numerosos modelos deterministas y estocásticos sobre cada uno de los subsistemas del planeta Tierra.

Tuve la gran suerte de organizar con él dos cursos de verano[38] de la Universidad Complutense de Madrid en torno a Matemáticas y Medio Ambiente: el primero en El Escorial, en 1991, concentrado en aspectos físicos y la construcción de los modelos ([19]) y el segundo en Almería, en 1992, abordando modelos relacionados con los aspectos económicos originados por el Medio Ambiente ([20]). Fueron experiencias inolvidables para mi. Tuve ocasión de conocer de cerca las dotes de Lions en el diseño de los cursos, ofreciendo una idea de conjunto ante situaciones enormemente complejas y su trato exquisito, tanto desde el punto de vista científico como humano, con todos los participantes[39].

Más recientemente, desde julio de 1999, nuestra relaciones científicas se habían estrechado aún más. En su fax de 29 de julio [40] me informaba que le habían propuesto publicar una segunda edición de su libro del Planeta Tierra (agotado en menos de dos años) pero que su intención era la de preparar todo un nuevo libro incorporando referencias aparecidas desde 1990 y añadiendo varios capítulos complementarios [24]. Me proponía que llevásemos a cabo tal tarea de forma conjunta dada la cercanía de alguno de mis trabajos y mi participación en la preparación del texto original. Desde entonces trabajamos duramente en aquel proyecto[41].

Estas líneas no podrían concluir sin unas palabras de agradecimiento hacia una persona como él al que una buena parte de la matemática aplicada española le debe tanto. Pese a su indudable carisma, ofrecí a una acesibilidad, una generosidad científica y un temperamento tan extraordinariamente afable que colocaba a su interlocutor en el centro de su preocupación y atención. Su ejemplo será siempre un acicate para las presentes y futuras generaciones.

[38] Lions mantuvo una activa participación en múltiples cursos de verano desde sus comienzos (además de los cursos de Montreal de 1962 y 1976, participó en varios en Italia como, por ejemplo, el del C.I.M.E. de 1962, 1967, etc.). En todos ellos dio muestra de su extraordinaria accesibilidad, lo que era de enorme importancia hacia los más jóvenes, en periodo de formación en esa época.

[39] Lions también me ayudó a organizar, en calidad de co-director junto a C.J. van Duijn, el Advanced Institute de la NATO que celebramos sobre esos temas en Santa Cruz de Tenerife, del 11 al 21 de enero de 1995. En aquella ocasión una pequeña enfermedad le impidió participar y pese a mis insistencias no quiso aparecer como coeditor de las actas ([17]).

[40] Lions desplegaba una correspondencia sorprendente por medio del fax de mensajes que solía escribir personalmente de su puño y letra: conservo, como un tesoro, más de cuatrocientas páginas.

[41] El texto estaba practicamente acabado a finales del 2000, unos meses antes de su fallecimiento. Lions hizo explicita mención en uno de sus últimos artículos ([82]).

Referencias

[1] Baiocchi, C., Capelo, A., *Variational and Quasivariational Inequalities,* J. Wiley, New York, 1984.

[2] Bensoussan, A., Lions, J.-L., On the support of the solution of some Variational Inequalities of Evolution, *J. Math. Soc. of Japan*, **28,** 1976,1-27.

[3] Bensoussan, A., Lions, J.-L., *Applications des inéquations variationnelles en Contrôle stochastique*, Dunod-Bordas, Collection M.M.I., Paris, 1978.

[4] Bensoussan, A., Lions, J.-L., *Contrôle impulsionnel et inéquations variationnelles*, Dunod-Bordas, Collection M.M.I., Paris, 1982.

[5] Bensoussan, A., Lions, J. L., Papanicolau, G., Sur quelques phénomènes asymptotiques stationnaires (I), *Comptes Rendus Acad. Sci. Paris*, **281**, 1975. 89-94.

[6] Bensoussan, A., Lions, J. L., Papanicolau, G., *Asymptotic Methods ín Periodic Structures*, North Holland, Amsterdam, 1978.

[7] Bensoussan, A., Lions, J.-L., Temam, R., Sur les méthodes de décomposition, de décentralisation et de coordination et applications, en *Methodes Mathematiques de l'Informatique,* J.-L. Lions y G.I. Marchuk eds. Dunod, Paris 1974, págs. 133-257 (también en *Cahiers IRIA*, **11**, 1972, págs. 5-190).

[8] Brezis, H., Équations et inéquations non linéaires dans les espaces vectoriels en dualité, *Ann. Institut Fourier,* **18,** 1968, 115-175.

[9] Brezis, H., Solutions of variational inequalities with compact support, *Uspekhi Mat. Nauk,* **129**, 1974, 103-108

[10] Brezis, H., *Analyse Fonctionelle,* Masson, Paris, 1983. (Hay traducción española: *Análisis Funcional*, Alianza Editorial, Madrid, 1984).

[11] Ciarlet,Ph., Jacques-Louis Lions 1928-2001, *Matapli,* **55,** 2001, 5-16.

[12] Coron, J.M., On the controllability of 2-D incompressible perfect fluids, *Journal de Mathematiques Pures et Appliquées*, **75,** 1996, 155-188.

[13] Courant, R., Hilbert, D., *Methods of Mathematical Physics,* Vol. 1 y 2. Interscience, Nueva York, 1953.

[14] Dautray, R., Lions, J.-L., *Analyse Mathématique et Calcul Numérique pour les Sciences et les Techniques*, En 3 volumenes, Collection du C.E.A., Série scientifique, Masson, Paris, 1984 y 1985, reedición en 9 volumes, Masson, Paris, 1988. Traducción inglesa *Mathematical Analysis and Numerical Methods for Science and Technology,* 6 volúmenes, Springcr Verlag, Berlin-Heidelberg, 1988-1990.

[15] Delsarte, J., Lions, J.-L., Transmutation d'opérateurs différentielles dans le domaine complexe, *Commentarii Mathematici Helvetici,* 32, 1957, 832-834.

[16] Deny, J., Lions, J.-L., Les espaces du type Beppo Levi et applications, *Annales de l'Institut Fourier,* **5,** 1954, 305-370.

[17] Díaz, J. I., ed., *The Mathematics of Models for Climatology and Environement*, NATO ASI Series, Springer Verlag, 1997.

[18] Díaz, J.I., Jacques-Louis Lions: matemático, El País, 19 de mayo de 2001.

[19] Díaz, J.I., Lions, J.-L., eds., *Mathematics, Climate and Environment,* Research Notes in Applied Mathematics 27, Masson, Paris, 1993.

[20] Díaz, J.I., Lions, J.-L., eds., *Environment, Economics and Their Mathematical Models,* Research Notes in Applied Mathematics 35, Masson, Paris, 1994.

[21] Díaz, J.I., Lions, J.-L., Sur la contrôlabilité approchée de problèmes paraboliques avec phénomènes d'explosion, *Comptes Rendus Acad. Sci. Paris*, **327**, Série I, 1998. 173-177.

[22] Díaz, J.I., Lions, J.-L., On the approximate controllability for some explosive parabolic problems, en *International Series of Numerical Mathematics*, Vol. 133, Birkhäuser Verlag, Basel, 1999, 115-132.

[23] Díaz, J.I., Lions, J.-L., On the Approximate Controllability of Stackelberg-Nash Strategies. En *Mathematics and Environment*, Actas de la Vioconferencia sobre Environment de la EMS, J.I. Díaz ed., Springer Verlag, Berlin, 2002.

[24] Díaz, J.I., Lions, J.-L., *Matemáticas, superordenadores y control para el planeta Tierra,* Editorial de la UCM, 2002.

[25] Duvaut, G., Lions, J.-L., Ecoulement d'un fluide rigide visco-plastique incompressible, *Séminaire sur les Equations aux Dérivées Partielles, Collège de France, années 1969-1970,* **II,** 2, 8-14.

[26] Duvaut, G., Lions, J.-L., *Les inéquations en Mécanique et en Physique,* Dunod, Gauthier Villars, Paris, 1972.

[27] Eckhaus,W., *Singular perturbations*, North Holland, Amsterdam, 1973.

[28] Fernández-Cara, E., Real, J., On a conjecture due to J.-L. Lions, *Nonlinear Analysis,* **21,** 1993, 835-847.

[29] Fichera, G. Problemi elastostatici con vincoli unilaterali: il problema de Signorini con ambigue condizioni al contorno, *Mem. Accad. Naz. Lincei,* **8,** 1964, 91-140.

[30] Foias, C., Sur certains théorèmes d'interpolation, *Acta Scientarum Mathematicarum,* **XXII,** 1961, 269-282.

[31] Fursikov,A., Imanuvilov, O. Yu, On the exact boundary zero controllability of the two dimensional Navier-Stokes equations, *Acta Appl. Math.*, **36,** 1994, 1-10**.**

[32] Glowinski, R., Li, C. M., Lions, J. L., A numerical approach to the exact boundary controllability of the wave equations, *Jap. J. of Applied Math*, **7,** 1990, 1-76.

[33] Glowinski R., Lions J.-L., Exact and approximate controllability for distributed

parameter systems. *Acta Numerica*, 1994, págs. 269-378, 1995, 159-333.

[34] Glowinski, R., Lions, J.-L. y Pironneau, O., Decomposition of energy spaces and applications. *C.R.A.S.,* Paris, **329**, 1, 1999, 445-452.

[35] Glowinski, R., Lions, J. L., Tremolieres, R., *Analyse Numérique des Inéquations Variationnelles*, 2 volúmenes, Dunod, París, 1976

[36] Goldstein, H., *Classical Mechanics*, Second Edition, Addison-Wesley, Massachusetts, 1990. (Hay traducción al castellano: *Mecánica Clásica,* Reverté, Barcelona, 1992).

[37] Hopf, E., Über die Anfangswertaufgabe für die hydrodynammischen Grundlgiccungen, *Math. Nachr.*, **4**, (1950/51), 213-231.

[38] Hörmander, L., Lions, J.-L., Sur la complétion par rapport à une intégrale de Dirichlet, *Mathematica Scandinavica,* **4,** 1956, 259-270.

[39] Imanuvilov, O. Yu, Remarks on the exact controllability for the Navier-Stokes equations, *ESAIM Control Optim. Calc. Var.*, **6,** 2001, 39-72.

[40] Lattès, R., Lions, J.-L., Sur une classe de problèmes aux limites intervenant en Physique des réacteurs. En, *Symposium Centre International provisoire de Calcul,* Birkhäuser, 1960.

[41] Lattès, R., Lions, J.-L., *Quasi-Réversibilité,* Dunod, Paris, 1967.

[42] Lax, P., Magenes, E., Temam, R., Jacques-Louis Lions (1928-2001), *Notices of the AMS,* **48**, 2001, 1315-1321.

[43] Lax, P., Milgram, A.N, Parabolic equations, En *Contributions to the theory of Partial Differential Equations,* Ann. Math. Studies **33**, Princeton, 1954, 167-190.

[44] Leray, J., Etude de diverses équations intégrales non linéaires et de quelques problèmes que pose l'hydrodynamique, *Journal de Mathematiques Pures et Appliquées*, **12**, 1933, págs. 1-82.

[45] Leray, J., Lions, J.-L., Quelques résultats de Visik sur les problèmes elliptiques non linéaires par les méthodes de Minty-Browder, *Bulletin de la Société Mathématique de France,* **93,** 1965, 97-107.

[46] Lichnevsky, A., Lions, J.-L., Super-ordinateurs. Evolutions et tendances, *La vie des sciences, C. R. Acad. Scie., París*, **1**, núm. 4, julio-septiembre 1984, 263-284.

[47] Lions, J.-L., Supports de produits de composition, *C.R.A.S. Paris,* **232,** 1951, 1530-1532.

[48] Lions, J.-L., Supports dans la transformation de Laplace, *C.R.A.S. Paris,* **232,** 1951, 1622-1624.

[49] Lions, J.-L., Problèmes aux limites en Théorie des Distributions, *Acta Matematica*, **94,** 1955**,** 13-153,

[50] Lions, J.-L., Sur les problèmes aux limites du type dèrivée oblique, *Annals of Mathematics,* **62,** 1956**,** 207-239.

[51] Lions, J.-L., Une remarque sur les applications du théorème de Hille-Yosida, *Journal of the Mathematical Society of Japan,* **9,** 1957, 62-70.

[52] Lions, J.-L., Sur certaines problèmes mixtes quasi-linèaires I, *C.R.A.S. Paris,* **246,** 1958, 1644-1647. Sur certaines problèmes mixtes quasi-linèaires II, *C.R.A.S. Paris,* **246,** 1958, 1796-1799.

[53] Lions, J.-L., Espaces intermédiaires entre espaces hilbertiens et applications, *Bulletin Mathematique de la Société Mathématique et Phisique de la R.P. de Roumanie,* **2,** 1958, 419-432.

[54] Lions, J.-L., Sur l'existence des solutions des équations de Navier-Stokes, *C.R.A.S. Paris,* **248,** 1959, 1099-1102.

[55] Lions, J.-L., *Equations différentielles opérationnelles et problèmes aux limites.* Springer-Verlag, Berlin, 1961.

[56] Lions, J.-L., *Problèmes aux limites dans les Equations aux Derivées Partielles,* Les Presses de l'Université de Montreal, 1962.

[57] Lions, J.-L., Ecuaciones Diferenciales y Problemas en los Límites. Notas de tres conferencias impartidas (los días 21.22 y 23 de Marzo de 1963) en la Facultad de Ciencias de la Universidad de Barcelona. *Publ. Seminario Matemático de Barcelona.* Abril 1963.

[58] Lions, J.-L., *Méthodes d'approximation numérique des problèmes aux limites de la Physique Mathématique,* Publications du CNRS, Institut Blaise Pascal, tome 1 (publ.14111) 1962, tome 2 (publ. CA.14.11.1/AI) 1962, tome 3 (publ. CA/14.11.1A/A1) 1963.

[59] Lions, J.-L., Sur le côntrole optimal de systèmes décrits par des équations aux dérivées partielles linéaires. Remarques générales (I), *C.R.A.S. Paris,* **263,** 1966, 661-663. (II) Equations elliptiques, *C.R.A.S. Paris,* **263,** 1966, 713-715. (II) Equations d'évolution, *C.R.A.S. Paris,* **263,** 1966, 776-779.

[60] Lions, J.-L., *Sur le contrôle optimal de systèmes gouvernés par des équations aux dérivées partielles*, Dunod, Gauthier Villars, Paris, 1968.

[61] Lions, J.-L., *Quelques méthodes de résolution des problèmes aux limites non linéaires*, Dunod, Gauthier Villars, Paris, 1969.

[62] Lions, J.-L., *Cours d'Analyse Numérique*, Ecole Polytechnique, Paris, 1973.

[63] Lions, J.-L., Approximation numérique des inequations d'evolution. En *Constructive Aspects of Functional Analysis, Part I,* Cremonese, Roma, 1973, 295-361.

[64] Lions, J.-L., *Sur quelques questions d'Analyse, de Mécanique et de Contrôle optimal*, Les Presses de l'Université de Montreal, 1976.

[65] Lions, J. L., *Perturbations singulières dans les problèmes aux limites et en contrôle optimal*, Lecture Notes in Math., 323, Springer, 1973.

[66] Lions, J. L., *Some methods in the Mathematical Analysis of Systems and Their Control*, Science Press, Beijing y Gordon Breach, Nueva York, 1981.

[67] Lions, J. L., *Contrôle des systèmes distribués singulièrs*, Gauthier-Villars, París, 1983.

[68] Lions, J. L., Remarks on systems with incomplete data, en *Variational Methods in Geosciences*. Y. K. Sasaki, ed., Elsevier, 1986, págs. 145-159.

[69] Lions, J. L., Contrôle de Pareto de Systémes distribués, *CRAS Paris*, **302**, 1986, págs. 223-227 y 413-417.

[70] Lions, J. L., Exact Controllability, Stabilization and Perturbations for Distributed Systems, *SIAM Review*, **30,** 1988, 1-68.

[71] Lions, J. L., *Contrôlabilité Exacte, Perturbations et Stabilisation de Systèmes Distribués*, tomo 1, *Contrólabilité Exacte*, tomo 2, *Perturbations*, Masson, Paris, 1988.

[72] Lions, J. L., Sur les sentinelles des systèmes distríbués. 1) Le cas des conditions initiales incomplètes, en *CRAS París*, **307**, 1988, 819-823. 2) Conditíons frontières, termes sources, coefficients incomplètement connus, *íd.*, 865-870. 3) Colloque IFAC, Perpignan, junio 1989.

[73] Lions, J.-L., *El planeta Tierra. El papel de las Matemáticas y de los superordenadores.* Serie del Instituto de España **8,** Espasa-Calpe, Madrid, 1990.

[74] Lions J.-L., Are there connections between turbulence and controllability? in *Analyse et Optimisation des Systèmes*, Springer Verlag, Lecture Notes in Control and Information Sciences, **144**, 1990, A. Bensoussan and J.-L. Lions eds.

[75] Lions, J. L., De la machine à calculer de Blaise Pascal aux ordinateurs, *La vie des Sciences, C.R.A.S. Paris,* **8,** 1991, 221-240.

[76] J.-L. Lions, Remarques sur la contrôlabilité approchée. En *Jornadas Hispano-Francesas sobre control de sistemas distribuidos*, Univ. de Málaga, 1991, 77–87.

[77] Lions, J. L., *Sentinelles pour les systémes distribués á données incomplétes*, Masson, Paris, 1992.

[78] Lions, J. L., Contrôle à moindres regrets des systèmes distribués, *CRAS Paris*, **315,** 1992, págs.1253-1257.

[79] Lions, J.-L., Some Remarks on Stackelberg's Optimization, *Mathematical Models and Methods in Applied Sciences*, **4,** 1994, 477-487.

[80] Lions J.-L., Le simulateur de la Terre, *Rev. R. Acad. Cien. Exact. Fis. Nat.,* **92,** 1998, 71-85

[81] Lions J.-L., Parallel algorithms for the solution of variational inequalities, *Interfaces and Free Boundaries,* **1,** 1999, 3-16.

[82] Lions J.-L., Some Remarks on the Mathematical Modelling of Planet Earth System, *Atti dei Convegni Lincei*, Accademia Nazionale dei Lincei, **158,** 2000, 73-93.

[83] Lions, J.-L., Lagnese, J.E., *Modelling. Analysis and Control of Thin Plates*, Masson, Paris, 1988.

[84] Lions, J.-L., Magenes, E., *Problèmes aux limites non homogènes et applications,* Dunod, Paris, Vol.1 1968, Vol.2 1968, Vol. 3, 1970.

[85] Lions, J.-L., Peetre, J., Sur une classe d'espaces d'interpolation, *Publications Mathématiques de l'I.H.E.S.,* **19,** 1963, 5-68.

[86] Lions, J.-L., Pironneau, O., Algorithmes parallèles pour la solution des problèmes aux limites, *CRAS Paris*, **327**, 1998, 947-952.

[87] Lions, J.-L., Prodi, G., Un théorème d'existence et d'unicité dans les équations de Navier-Stokes en dimension 2, *C.R.A.S. Paris,* **248,** 1959, 3519-3521.

[88] Lions, J.-L., Raviart, P. A., Remarques sur la résolution et l'approximation d'équations d'évolution couplées, *International Computation Center Bulletin*, (UK), **5,** 1-21.

[89] Lions, J.-L., Sánchez-Palencia, E., Ecoulement d'un fluide viscoplastique de Bingham dans un milieu poreux, *Journal de Mathématiques Pures et Appliquées,* **60,** 1981, 341-360.

[90] Lions, J.-L., Sánchez-Palencia, E., Problèmes aux limites sensitifs, *C. R. A. S., Paris,* **319,** 1994, 1021-1026.

[91] Lions, J.-L., Sánchez-Palencia, E., Sensivity problems for some shells with edges, *Topological Methods in Nonlinear Analysis*, **9,** 1997, 1-16.

[92] Lions, J.-L., Schwartz, L., Problèmes aux limites sur des espaces fibrés. *Acta Matematica*, **94,** 1955, 155-159**.**

[93] Lions, J.-L., Stampacchia, G., Inéquations variationnelles non coercives, *C.R.A.S., Paris,* **261,** 1965, 25-27.

[94] Lions, J.-L., Stampacchia, G., Variational Inequalities, *Communications on Pure and Applied Mathematics,* **20,** 1967, 493-519.

[95] Lions, J.-L., Strauss, W.A., Some Nonlinear Evolution Equations, *Bulletin de la Société Mathématique de France,* **93,** 1965, 43-96.

[96] Lions, J.-L., Temam, R., Wang, S., New formulations of the primitive equations of atmosphere and applications, *Nonlinearity,* **5**, 1992, 237-288.

[97] Lions, J.-L., Temam, R., Wang, S., On the Equations of the Large-scale Ocean, New formulations of the primitive equations of atmosphere and applications, *Nonlinearity,* **5**, 1992, 1007-1053.

[98] Lions, J.-L., Temam, R., Wang, S., Models for the coupled atmosphere and ocean, *Computational Mechanics Advances*, **1,** 1993

[99] Lions, J.-L., Zuazua, E., A generic uniqueness result for the Stokes system and its control theoretical consequences, in *PDE and Applications*, eds. P. Marcellini, G. Talenti and E. Visentini, Dekker, **177,** 1996, 221-235.

[100] Lions, J.-L., Zuazua, E., Contròlabilité exacte des approximations de Galerkin des èquations de Navier Stokes. *C.R.A.S.* Paris, **234**, 1, 1997, 1015-1021.

[101] Lions, J.-L., Zuazua, E., Exact boundary controllability of Galerkin's approximations of Navier Stokes equations. *Annali Scuola Norm. Sup. Pisa*, **ÌXXVI**, 4, 1998, 605-621.

[102] Lions, J.-L., Zuazua, E., The cost of controlling unstable systems : time irreversible systems. *Revista Mat. Complutense.* **10**, 2, 1997, 481-523.

[103] Lions, J.-L., Zuazua, E., On the cost of controlling unstable systems : the case of boundary controls. *J. d'Analyse Math.* **73**, 1997, 225-249.

[104] Lions, P.L., *Generalized solutions of Hamilton-Jacobi equations*, Pitman, London, 1982.

[105] Lions, P. L. On the Schwarz Alternating Method, en *Domain Decomposition Methods for Partial Differential Equations*, Glowinski et al., ed., SIAM, Philadelphia, 1988, 1-42.

[106] Lions, P. L., *Mathematical Topics in Fluid Mechanics. Volume1. Incompressible Models.* 1996, *Volume 2. Compressible Models.* 1999, Clarendon Press, Oxford.

[107] Magenes, E., Ricordo di Jacques-Louis Lions, *UMI Bolletin*, 2001, 24.

[108] Samuelson, P.A., Mac Kean, H., Rational theory of Warrant Pricing, *Industrial Management Review,* **6**, 1965, 13-39.

[109] Sanchez-Palencia, E., *Non homogeneous Media and Vibration Theory*, Springer, Verlag, Berlin, 1980.

[110] Schwartz, L., *Un mathématicien aux prises avec le siècle*, Editions Odile Jacob, Paris, 1997.

[111] Stampacchia, G., Formes bilinéaires coercitives sur les ensembles convexes, *C.R.A.S., Paris,* **258,** 1964, 4413-4416.

[112] Temam, R., *Navier-Stokes equations, Theory and Numerical Analysis*, 3^a. ed., North Holland, Amsterdam, 1984.

[113] Temam, R., Obituary of J.-L. Lions, *SIAM News,* **34,** 6, 2001, 2-4**.**

[114] Valle, A., Un problème de contrôle optimum dans certaines èquations differentielles d'évolution. *Annali Scuola Norm. Sup. Pisa*, **20**, 1966, 25-30.

[115] Valle, A., En memoria de Jacques-Louis Lions, *Boletín de SEMA*, **18,** 2001, 9-13.

En memoria de Jacques-Louis Lions

E. Fernández Cara

Departamento de Ecuaciones Diferenciales y Análisis Nnumérico
Universidad de Sevilla
41080 SEVILLA

cara@numer.us.es

Mis primeros recuerdos del Profesor Lions se remontan a finales de 1979. Naturalmente, había oído hablar mucho de él y conocía con cierto detalle lo que había sido su trayectoria científica hasta ese momento. Además, varios compañeros algo mayores que yo habían tenido la ocasión de conocerle personalmente en Sevilla, en unas Jornadas organizadas por el Profesor Antonio Valle en 1976. Uno de ellos, José Real, me había dicho de él y de su charla algo que recuerdo muy bien:

En la conferencia de Lions, todo estaba absolutamente claro. Todo.

A finales de 1979, yo era becario predoctoral en el I.N.R.I.A - Rocquencourt, cerca de París. Justamente por aquella época y tan sólo unos días antes de mi llegada, Lions había sido designado Presidente del Instituto. Su cambio de despacho originó toda una avalancha de "mudanzas". Así que, durante varias semanas, me instalaron en una sala compartida con otros dos becarios en la que, casualmente, Lions había guardado una colección de artículos seleccionados personalmente.

Confieso que, muy a menudo, por la tarde, cuando no quedaba casi nadie, no podía resistir la tentación de ojear a hurtadillas estos trabajos. Por supuesto, yo era un inexperto estudiante en aquella época y carecía de criterio serio para seleccionar temas, autores y resultados. No obstante, creo que aprendí mucho descubriendo cuáles eran, al parecer, los artículos preferidos de Lions y preguntándome por qué había seleccionado éste o aquél.

También pienso que este archivo me ayudó a comprender, al menos en parte, cómo pensaba Lions que había que estudiar y desarrollar las Matemáticas y qué era lo que le interesaba principalmente a él. Con el tiempo, pude intuir que Lions pretendía hacer que las Matemáticas fueran capaces de describir con la mayor precisión posible el mundo real. Sus objetivos prioritarios siempre arrancaban de problemas reales concretos que intentaba *modelar*, posteriormente

analizar y comprender cualitativa y cuantitativamente y, finalmente, *controlar*. De algún modo, posiblemente influido por sus orígenes y aficiones, había llegado a la conclusión de que la herramienta más eficaz para ello eran las ecuaciones en derivadas parciales (EDPs). Una vez encarada la resolución de alguno de estos problemas, sus portentosas cualidades le permitían desarrollar la teoría matemática adecuada, ayudándose simultáneamente de conceptos y resultados clásicos hábilmente "revisitados" y de técnicas y conceptos nuevos, creados específicamente para ello.

Recuerdo que, en aquella época, yo miraba a Lions casi como a un dios. Con frecuencia, Juan M. Viaño y yo le veíamos llegar al comedor del I.N.R.I.A. con sus colaboradores más próximos, con paso decidido, dispuesto a rentabilizar el tiempo dedicado al almuerzo sin perder por ello el buen humor. Como a muchas personas que conozco, algo que nunca dejó de impresionarme fue su enorme capacidad de trabajo. Era capaz de resolver 20 problemas distintos, todos de envergadura, al cabo del día. Y era capaz de simultanear todo esto con una dedicación constante a las Matemáticas, manteniéndose en la vanguardia de la Ciencia, en el límite de lo conocido y lo que está aún por descubrir.

En fechas posteriores, a partir de 1987, tuve la ocasión de conocer más de cerca a Lions como gestor. Fue en el marco del Proyecto HERMES, parcialmente financiado por el C.N.E.S. (Centre National des Etudes Spatiales), del que había sido nombrado Presidente. Me acuerdo muy en particular de una reunión que hubo en Madrid hacia 1989 a la que asistimos rodeados de representantes de distintas empresas y organismos. En un pequeño descanso, con cierta complicidad, sacó tiempo para hablarme de un problema matemático que le preocupaba y que consideraba interesante. Yo era consciente de su actividad al frente del C.N.E.S. y de quién sabe cuántas instituciones más. Era ya una persona convocada con frecuencia por los consejos de administración de multitud de empresas e incluso por responsables del más alto rango político en Francia y en Europa. Resultaba asombroso que pudiera organizarse para hacer Matemáticas.

Hoy sabemos que justamente en esta época estaba desarrollando algunas de las ideas que más han dado que hablar y más trabajo han generado. Eran los años del método H.U.M. y de su renovado interés por el control de sistemas gobernados por EDPs.

Con objeto de clarificar hasta qué punto él iba por delante y cómo era capaz de intuir qué era importante y qué había que impulsar, he aquí el enunciado del problema del que me habló.

Problema 1: Para un sistema disipativo "simple" de la forma

$$\begin{cases} y_t + Ay = \xi \\ y|_{t=0} = y^0 \end{cases} \tag{1}$$

(donde A es, por ejemplo, un operador en derivadas parciales lineal, de propiedades similares a las del operador de Laplace), es posible definir el concepto de *centinela*. En términos "vagos", si ponemos $y^0 = y_1^0 + \tau y_2^0$ con τ "pequeño" y llamamos y_τ a la correspondiente solución de (1), un centinela es un funcional $\Phi = \Phi(y)$ *tan parecido como sea posible a un promedio de los valores de* y insensible a la presencia de la perturbación τy_2^0 , i.e. tal que

$$\frac{\partial}{\partial \tau}\Phi(y_\tau)\bigg|_{\tau=0} = 0.$$

Entre otras cosas, disponer de un centinela puede ser útil para conocer la influencia que tiene ξ (un término de *polución*) cuando la información sobre el dato inicial es incompleta. Pero, ¿es posible recurrir al concepto de centinela para modelar y describir cuantitativamente la *Turbulencia* ? En otras palabras, si cambiáramos (1) por el sistema de Navier-Stokes, ¿sería posible utilizar la idea de centinela para definir variables macroscópicas $z = z(x,t)$ que contengan información relevante distribuida en tiempo y espacio, de nuevo independiente de τy_2^0 , cuya aproximación numérica sea factible ?

A partir de 1987, Lions prodigó enormemente sus visitas a España. En muchos casos, el "culpable" directo o indirecto fue (de nuevo) Antonio Valle. Consciente de lo extremadamente útil que resultaban sus visitas, en especial para los más jóvenes, tanto él como muchos otros colegas españoles hicimos todo lo posible por tenerlo cerca.

A raíz de una de estas visitas, comencé a interesarme más, junto con varios compañeros de mi Departamento, por las cuestiones que le interesaban a él. Esto ocurrió en Málaga, en otoño de 1990 y acabó por hacer más intensa y fluida mi relación con él. A partir de 1993, tuve la enorme suerte de contarme entre las personas que, de vez en cuando, recibían un Fax con sus cuestiones, observaciones y consejos.

A modo de ejemplo, he aquí uno de los problemas que me planteó hace varios años, formulado con su estilo propio:

Problema 2: Se considera el sistema parabólico

$$(2) \qquad \begin{cases} y_t - \Delta y + a(x,t)y = v\chi_\omega & \text{en } \Omega \times (0,T), \\ y(x,t) = 0 & \text{sobre } \partial\Omega \times (0,T), \\ y(x,0) = y^0(x) & \text{en } \Omega, \end{cases}$$

donde $\Omega \subset \mathbf{R}^N$ es un abierto acotado, $\omega \subset\subset \Omega$ es un abierto "pequeño" y χ_ω es la función característica de ω.

Sabemos que, cualquiera que sea $a \in L^\infty(\omega \times (0,T))$, (2) tiene la propiedad de la controlabilidad aproximada con controles $v \in L^2(\omega \times (0,T))$. Esto es, la

variedad lineal formada por los estados finales $\{ y(\cdot\,, T) : v \in L^2(\omega \times (0,T))\}$ es densa en $L^2(\Omega)$. Sean $M \subset L^\infty(\Omega \times (0,T))$ y pongamos

$$V(T;M) = \{ y(\cdot\,, T) : v \in L^2(\omega \times (0,T)),\ a \in M \}.$$

Cuanto mayor es M, más cerca está $V(T;M)$ de su adherencia $L^2(\Omega)$, pero siempre tenemos $V(T;M) \neq L^2(\Omega)$. Entonces, ¿qué significa realmente que $V(T;M)$ se va acercando a $L^2(\Omega)$? Por otra parte, para un sistema similar a (2) con la ecuación cambiada por

$$y_t - \Delta y + a(x,t)y + y^3 = v\chi_\omega\,,$$

en general la familia $V(T;M)$ no es densa en $L^2(\Omega)$. ¿Es cierto que, cuando $M \subset L^\infty(\Omega \times (0,T))$ es "muy grande", la correspondiente $V(T;M)$ es densa ? Finalmente, ¿pueden usarse estas ideas para resolver problemas de controlabilidad estocástica del mismo tipo ?

Está en la mente de muchos que habrá un antes y un después de Lions en las Matemáticas, en particular en la Matemática Aplicada francesa. A mí me parece apropiado extender esta afirmación, de manera que cubra también el ámbito de la Matemática Aplicada española. Si observamos seriamente la evolución y la situación actual de los numerosos Departamentos de Universidades españolas donde se estudian problemas ligados a las ecuaciones diferenciales, veremos que, en un alto porcentaje de ellos, hay personas que han sido alumnos de Lions o alumnos de alguno de sus alumnos. Y también comprobaremos que la influencia de esta presencia ha ido creciendo de forma espectacular en los últimos años. De manera que se puede decir que, en la actualidad, el espíritu de la investigación matemática realizada por Lions (e incluso en algunos casos los mismos temas y problemas que él propuso) forman parte del programa de trabajo de buena parte de nuestros compañeros.

La influencia de Lions en las Matemáticas que se han hecho en España comenzó con su feliz contacto con Antonio Valle, a mediados de los sesenta. Gracias a la abnegada labor docente de éste y a las horas que dedicó a la caza y captura de Becas y Ayudas de todo organismo viviente, se pudieron establecer varios lazos, escasos en número pero de fundamental importancia, que sirvieron para que personas como Alfredo Bermúdez, Carlos Moreno, José Real y José D. Martín pudieran realizar sus Tesis Doctorales bajo la dirección de algunos de los primeros alumnos de Lions. Paralelamente, se fue produciendo la entrada en escena de otros investigadores españoles, entre los cuales estuvieron Jesús Hernández, Ildefonso Díaz, Juan Luis Vázquez y Miguel A. Herrero, que iniciaron una colaboración científica con otros miembros de la "Escuela" creada por Lions. En los años posteriores, la afluencia de estudiantes y jóvenes profesores se fue incrementando progresivamente, hasta llegar a niveles insospechados que llegaron a hacer hablar de "colonias españolas" en París. Que yo recuerde, por esas "colonias" pasaron personas como María J. Esteban, Juan M. Viaño, Luis Ferragut, Tomás Chacón, Carlos Parés, Francisco Palma,

Francisco Ortegón, Rafael Muñoz, Juan Casado, José M. Rodríguez Seijo, Javier Barón, etc. Mención especial debo hacer de Enrique Zuazua, que fue un verdadero testigo de excepción del acercamiento de Lions a España y mantuvo con él un contacto permanente y muy personal casi hasta el último momento en que le fue posible.

Sin duda, Lions fue sensible a la evolución de nuestro país, al que llegó a profesar una profunda simpatía. En cierta ocasión le oí decir con gran sencillez en presencia del Secretario de Estado de Universidades y del Embajador de Francia que él no creía realmente que existiera ya diferencia científica apreciable entre España y Francia. Naturalmente, era una elegante y educada exageración, pero el hecho es que se fue acercando cada vez más a investigadores españoles.

De todas sus visitas a España, guardo un recuerdo muy especial de la última, la que tuvo lugar en Madrid en febrero de 2000 y le permitió hablar ante el Parlamento. La iniciativa de la Real Academia de Ciencias y en especial de Ildefonso Díaz hizo posible que Lions disertara con admirable capacidad ante el gran público, con palabras bien escogidas, sobre las Matemáticas más complicadas y actuales, en un acto sin precedentes.

No obstante, me quedó un cierto sabor agridulce del 2000. Junto con varios compañeros, habíamos previsto una visita de Lions a Sevilla para mediados de marzo de ese año. Nuestra intención era, una vez más, hacerle hablar ante un público diverso, como acto central de una serie de actividades conmemorativas del Año Mundial de las Matemáticas. Debido a la convocatoria de elecciones legislativas y autonómicas para esos días, nos vimos forzados a retrasar estos actos y por tanto su visita casi en el último momento. Por desgracia, ya no pudimos volver a encontrar una fecha que le resultara posible. En poco tiempo, como sabemos ahora, se agudizó su enfermedad y se vio repentinamente obligado a reducir e incluso detener su extraordinario ritmo de actividades.

Jacques-Louis Lions era una persona de talla excepcional. He tenido la gran suerte de haberle conocido y espero sinceramente haber sido capaz de aprender algo de sus muchas virtudes. Lamento profundamente que nos haya dejado tan pronto.

Era una persona capaz de hacer fácil lo difícil. Tanto en su manera de plantear y abordar la resolución de problemas matemáticos como en las actividades de gestión y en las relaciones humanas, su clarividencia le permitía simplificar los conflictos superando una tras otra todas las dificultades y vislumbrar la solución con rapidez. Ayudado además de un optimismo vital envidiable, era capaz de conseguir que la gran mayoría de las tareas que se encomendaba a sí mismo salieran a flote. Una lección que nos dejó es que no hay que dejarse vencer fácilmente por las circunstancias.

Tenía además la rarísima virtud de conseguir que sus cursos y conferencias, aparte de amenos, fueran interesantes y útiles para oyentes de todo tipo, desde

estudiantes de segundo o tercer año hasta Catedráticos de Universidad, desde personas interesadas por el Algebra y la Geometría hasta especialistas del análisis teórico y numérico de las EDPs. Las ideas que presentaba siempre aportaban algo nuevo, siempre eran aprovechables y, con gran frecuencia, abrían nuevas posibilidades.

Otro rasgo que me fascinó de Lions fue su capacidad de iniciativa. Era capaz de lanzar propuestas constructivas tanto en Matemáticas como en sus otros ámbitos de trabajo. Y, llegado el caso, era capaz de convencer a las personas indicadas de poner manos a la obra. Todo esto no era por casualidad. Sus propuestas habían sido siempre seriamente meditadas, aunque muchas veces en tiempo "record", dada su rapidez mental. Por otra parte, de todas las posibles vías, casi siempre se decantaba por la más constructiva, aunque esto significara innovación y pisar terreno aún no explorado. Ante una sugerencia o ruego de Lions, uno tan sólo podía aceptar, con independencia del trabajo o dificultad que trajera consigo.

Durante todo el tiempo que le conocí, Lions consiguió estar por encima de envidias y de sentimientos malsanos. Se podría decir que sus actividades fueron observadas por el 99 % de sus colegas y discípulos sin desconfianza y sin malas interpretaciones. A decir verdad, creo que este hecho le honra a él y a la "Escuela" que supo crear, que ha demostrado profesionalidad y honradez a raudales. A menudo tuve la impresión de que, en presencia de Lions, los intereses oscuros o inconfesables estaban de más. Su actitud, siempre positiva y al mismo tiempo comprensiva con los sentimientos de los demás, contribuía en gran medida a que las reuniones de trabajo, las científicas y las de otro tipo, fueran sobre todo limpias. Y esto hacía indudablemente posible el progreso, la mejora y el beneficio para todos.

Desde la óptica de las relaciones humanas, quizá sea ésta la mejor lección que hayamos recibido de este hombre de excepción. Tal vez nos convenga a todos imitarle en limpieza de sentimientos y esforzarnos como él por usar nuestro tiempo y nuestras energías en prestar nuestra colaboración a la resolución de cuestiones verdaderamente trascendentes.

Jacques-Louis Lions: Hasta siempre

E. Zuazua

Departamento de Matemáticas
Universidad Autónoma de Madrid
28049 Madrid

enrique.zuazua@uam.es

Agur, Jauna!

1 El hombre

La tarea de escribir sobre el reciente y prematuramente desaparecido Jacques-Louis Lions me resulta muy difícil.

Conocí a Lions en la primavera de 1986 cuando yo iniciaba mi Tesis Doctoral en el Laboratoire d'Analyse Numérique de l'Université de Paris VI, fundado por él, y hoy denominado Laboratoire Jacques-Louis Lions.

Las circunstancias en las que encontré a Lions fueron sin duda un tanto singulares. Él, en aquella época, era Presidente del CNES (Centre National d'Etudes Spatiales), acababa de recibir el premio John von Neumann de la SIAM (Society for Industrial and Applied Mathematics) y se estaba dedicando intensamente al estudio de la controlabilidad de sistemas, para lo cual había introducido el hoy clásico método Hilbert Uniqueness Method (HUM). Tal y como él acostumbraba a hacer, se había puesto en contacto con diversos colaboradores, entre ellos Alain Haraux, mi director de Tesis, con el objeto de clarificar algunas cuestiones relacionadas con la ecuación de ondas. Lions estaba a punto de iniciar su curso 1986-87 en el Collège de France y pensó que Alain podría redactar las notas del curso, pero éste, a su vez, pensó en mí pues él iba a ausentarse durante el semestre. Así, al final de una de aquellas conferencias del inolvidable seminario de los viernes por la tarde en el Collège de France, fui presentado a Lions quien, con la mirada cálida pero firme que le caracterizaba y aquella sonrisa que delataba su aguda inteligencia y singular ingenio, me preguntó si era capaz de escribir en francés. Yo, con franqueza, le dije que, con la ayuda de mi diccionario, sí. Esa respuesta le bastó y me confió aquella tarea

que ocupó buena parte de mi tiempo durante un año y que influyó de manera decisiva en mi carrera profesional.

Nunca supe cuál era el sorprendente mecanismo que él utilizaba para seleccionar las personas a las que confiaba tareas profesionales y que conducía, por ejemplo, a dejar en manos de un joven estudiante con escasa experiencia, semejante tarea. Yo creo que había mucho de intuición y otro tanto de aquel espíritu mediterráneo que le empujaba a asumir riesgos con el único objetivo de descubrir y entender nuevas cosas a través de las Matemáticas. En efecto, siempre tuve la sensación que Lions se interesaba en los problemas de Matemáticas en la medida en que estos representaban pequeños laboratorios de cuestiones mucho más transcendentes del mundo que nos rodea.

Evidentemente, sus apuestas no siempre fueron acertadas. Pero el optimismo que le caractizaba hacía que cada una de esas apuestas erradas se convirtiese en realidad en un acierto. Eso, junto con la extraordinaria energía con que la naturaleza le había regalado, hicieron de Lions muy pronto un hombre sabio y así, además de continuar con su trabajo como matemático, se vio llamado a desempeñar muchas otras tareas de gran envergadura.

Se ha escrito mucho sobre Lions y aún se seguirá escribiendo. Creo pues que mi aportación ha de ser breve. Sería sin duda pretencioso por mi parte ocupar muchas páginas de esta revista hablando de una persona de su trascendencia y proyección para la que las Matemáticas fueron el eje central de su polifacética tarea profesional en la que no solamente estableció y mantuvo numerosas colaboraciones científicas a lo largo de todo el planeta sino que fue a la vez una persona implicada en tareas de gestión del más alto nivel. Entre otras, la presidencia del Institut National de la Recherche en Informatique et Automatique (INRIA) que él fundó, del CNES antes citado o de la Academia de Ciencias de Paris y de la Unión Matemática Internacional.

Sí que me gustaría mencionar una de las frases que le escuché en más de una ocasión: "Los problemas no resueltos vuelven a surgir una y otra vez". Tuve la ocasión de comprobar eso en varias ocasiones a lo largo de los años en los que colaboramos. Efectivamente, los problemas que en su momento no habíamos resuelto surgían nuevamente en más de una ocasión condicionando de ese modo la comprensión y el avance en la materia a la resolución de la vieja cuestión. En Matemáticas eso es frecuente, si no sistemático: descifrar una pequeña clave abre las puertas a infinidad de nuevas avenidas. Tal vez por eso Lions fue, dentro de su flexibilidad a la hora de tomar decisiones, una persona de convicciones firmes y sumamente resolutiva. Así, rara vez tuvo que echarse atrás en una decisión que ya hubiese tomado.

En lo que respecta a su contribución a las Matemáticas se ha dicho mucho también y creo que el artículo de Philippe Ciarlet que, traducido al castellano, se ha publicado en este Boletín es un fiel reflejo de su obra. Yo conocí de cerca sus realizaciones a partir de 1986 y más de cerca las desarrolladas en el ámbito del Control.

La Teoría del Control es sin duda una de esas disciplinas en las que las contribuciones de Lions marcarán un antes y un después. La revista ESAIM:COCV (European Series in Applied and Industrial

Mathematics: Control, Optimization and the Calculus of Variations) (`http://esaim.emath.fr/`) publicará en breve un número especial en su memoria en el que se recogerán contribuciones de sus colaboradores más próximos en esta disciplina y podrá ser de utilidad para todos los interesados en conocer las aportaciones de Lions a este campo. Qué duda cabe, éstas son profundas y variadas, lo mismo que su rica descendencia matemática en la que a alumnos directos hay que sumar los muchos investigadores que colaboraron con él.

2 Sus contribuciones al Control

Una de las áreas de trabajo preferidas de Lions fue la de la Teoría del Control que él cultivó de una manera muy personal y con enorme eficacia. Cuando a finales de los sesenta comenzó a interesarse por este campo, su formación era la de un matemático puro que había contribuido de manera decisiva a lo que hoy forma ya parte de los fundamentos de la teoría moderna de las Ecuaciones en Derivadas Parciales y después había cultivado el ámbito del Análisis Numérico.

En la Teoría del Control Lions encontró el laboratorio perfecto donde ensayar todas sus técnicas e ideas. En efecto, controlar un sistema, algo fundamental tanto en la propia supervivencia de la especie humana como en los ámbitos más avanzados y sofisticados del desarrollo tecnológico, exige no sólo saber si las soluciones existen o no, si son regulares, o ser capaces de aproximarlas numéricamente. Efectivamente, controlar un sistema necesita también de una profunda comprensión de las propiedades cualitativas del sistema para poder prever la respuesta de las soluciones y su sensibilidad a las variaciones que en el sistema se introduzcan a través de los controles. Así, el Control fue siempre una de las piezas clave del paradigma que él popularizó: *Modelización - Análisis - Simulación Numérica - Control.*

Tras publicar en 1969 su célebre libro sobre Ecuaciones en Derivadas Parciales No-Lineales [3], que constituye todavía hoy en día una referencia básica, Lions se interesó por la Teoría de la Homogeneización. Su libro [1] en colaboración con Alain Bensoussan y George Papanicolaou es una referencia obligada en esta disciplina.

Pero ya para entonces Lions se interesaba por la Teoría del Control y en 1968 había publicado un libro [2] en francés en el que generalizaba a las EDP el principio del máximo que Pontryagin y sus colaboradores habían desarrollado en el caso de sistemas de ecuaciones diferenciales ordinarias y que constituyó uno de los hitos más importantes de la Teoría del Control. Este libro fue posteriormente traducido al inglés en 1971 e influyó de manera muy importante en el área.

Más adelante Lions escribió un nuevo libro sobre el Control de Sistemas Singulares [4] y otro en colaboración con A. Bensoussan [5] sobre el control de sistemas estocásticos. Más tarde publicó en China un libro con algunas contribuciones de Li-Ta-Tsien [6]. Todos ellos son obras bien conocidas en el campo.

Esta actividad se vió reforzada y continuada a partir de 1973 por sus cursos

anuales en el Collège de France en el marco de su cátedra "Analyse et Contrôle des Systèmes" en los que, cada año desarrollaba, un nuevo tema. No puedo dejar de resaltar que resulta sorprendente que una persona que compaginaba su cátedra del Collège de France con cargos como la presidencia del CNES fuese capaz de desarrollar cada otoño un nuevo curso que constituía foro de encuentro de muchos profesores franceses y extranjeros, jóvenes y seniors, y que insipiró a tantos investigadores en sus trabajos posteriores.

Más adelante Lions se interesó por los problemas de controlabilidad en los que se pretende saber si un sistema de evolución puede llevarse de un dato inicial a un dato final mediante la acción de un control adecuado. En 1986 Lions publicó una Nota en los Comptes Rendus de l'Académie des Sciences de Paris [7] en la que introdujo su ya célebre método HUM para la controlabilidad de sistemas lineales de evolución. Lions desarrolló un poco más esta teoría en su artículo publicado en SIAM Review [8] en la ocasión de la recepción del premio John von Neumann. Este tema fue el que eligió para sus cursos en el Collège de France en los años académicos 1986-87 y 1987-88. Los textos de estos cursos [9] y [10] fueron publicados en 1988 por Masson en sendos volúmenes de la colección RMA (Recherche en Mathématiques Appliquées) que Lions dirigía junto con Philippe Ciarlet.

Estos dos textos constituyeron una contribución central de Lions y el inicio de un fructífero período de investigación en el área durante los últimos quince años. Asimismo, sus trabajos posteriores en otros temas estuvieron fuertemente marcados por las técnicas y puntos de vista desarrollados en estos dos volúmenes y su trabajo posterior en este ámbito.

Existen aún numerosos problemas abiertos en Teoría del Control. Pero el área conoce dos eras: la anterior y posterior a las contribuciones de Lions.

Lions, en su trabajo en este campo, hizo gala de su talante abierto y creativo: Todos los métodos eran buenos si servían para resolver problemas y, además, la vida diaria o el mundo de la Industria por el que tanto se interesó, estaba llena de problemas que podían ser formulados en términos matemáticos que conducían con frecuencia a interesantes problemas de control.

Para Lions el binomio *"Matemáticas - Mundo real"* fue siempre indisoluble.

3 Un problema abierto

En homenaje a Lions, entendiendo que para él las cuestiones matemáticas habían siempre de jugar un papel central, y que fue en ese contexto que tuve la ocasión de conocerlo, me gustaría concluir estas líneas formulando un problema abierto que desde hace quince años le intrigó y que, a pesar de los esfuerzos de muchos, sigue aún estándolo. El lector interesado en una presentación más detallada de este problema podrá consultar [11]. La teoría lineal correspondiente es una de las contribuciones maestras de Lions a la que antes hacíamos referencia ([7]–[10]).

Consideramos la ecuación de ondas semilineal

$$\begin{cases} y_{tt} - y_{xx} + y^3 = \chi_\omega(x)u(t,x) & \text{en} \quad (0,1)\times(0,T), \\ y = 0 & \text{para} \quad t \in (0,T);\ x = 0,1 \\ y(0) = y_0, \quad y_t(0) = y_1 & \text{en} \quad (0,1). \end{cases} \tag{1}$$

Se trata de un modelo no-lineal simplificado para las vibraciones de una cuerda. El *estado*, que representa la deformación de la cuerda, viene dado por $y = y(x,t)$. El *control* viene dado por la función $u = u(x,t)$ que actúa sólo en una parte de la cuerda pues χ_ω denota la función característica del subintervalo $\omega = (\alpha,\beta)$. El problema que nos ocupa es sólo relevante cuando (α,β) es un subintervalo estricto de $(0,1)$. En caso contrario, el control actúa en todo el dominio y hace que la presencia de la no-linealidad sea totalmente irrelevante.

El sistema anterior está bien puesto: Para cualquier par de datos iniciales (y_0, y_1) en el espacio de energía $H_0^1(0,1)\times L^2(0,1)$, y cada control u en $L^2((0,1)\times(0,T))$ existe una única solución y en $C([0,T];H_0^1(0,1))\cap C^1([0,T];L^2(0,1))$.

Además es conocido que, para cada dato inicial (y_0,y_1) de energía finita, existe un tiempo $T(y_0,y_1) > 0$, de modo que la solución se puede llevar al equilibrio en ese instante mediante un control adecuado. Es decir, existe $u \in L^2((0,1)\times(0,T(y_0,y_1)))$ tal que la solución de (1) satisface

$$y(T) \equiv y_t(T) \equiv 0, \tag{2}$$

en ese instante.

Se trata de un resultado de *controlabilidad*. El resultado es de naturaleza global pues es válido para todos los datos iniciales pero no es uniforme pues el tiempo de control depende del dato inicial (las estimaciones de las que se dispone hasta el momento indican que T depende de manera logarítimica de la norma de los datos iniciales a controlar) en contraposición con lo que ocurre en el marco de las ecuaciones lineales.

El problema abierto al que hacía referencia es: *¿La ecuación (1) es controlable en un tiempo independiente de la talla de los datos iniciales a controlar?*

Esto es así en el caso de la ecuación de ondas lineal para la cual el tiempo puede calcularse fácilmente viendo cuánto tiempo una característica del sistema puede propagarse sin interceptar la región ω donde el control actúa. Se obtiene así un tiempo de control $T = 2\max(\alpha,\ 1-\beta)$.

Como decíamos más arriba, a pesar de intensos y múltiples esfuerzos, el problema está aún abierto. Estoy seguro de que a Lions le hubiese gustado conocer la respuesta y que ésta exigirá de ideas innovadoras con respecto a lo que hasta hoy se conoce.

4 A modo de conclusión

Lamento profundamente la pérdida de Lions que se manifiesta ya en el día a día, pues ya no llegan aquellos faxes en los que, con la amabilidad, elegancia y profundidad de pensamiento que le caracterizaban, planteaba alguna de aquellas

cuestiones matemáticas que constituían para mí y muchos otros, mucho más que un trabajo, uno de los mayores alicientes para empezar los días con optimismo y trabajar con pasión.

Nos queda el indeleble legado del maestro, pues lo era, y del hombre que, pese al gran prestigio profesional y social del que gozaba, siempre estuvo dispuesto a escuchar, sin distinguir edades ni procedencias. Después de ver el volumen de correo que recibía a diario en el Collège de France, nunca conseguí entender cómo hacía para responder a tantas cartas y con tanta celeridad y eficacia, aportando casi siempre la idea o sugerencia acertada.

Lions, mediante su obra y escuela, seguirá influyendo en buena medida en nuestra concepción de las Matemáticas y, a través de ellas, en nuestra manera de entender el mundo que fue siempre su gran fuente de problemas abiertos.

Espero que sus valores humanos, su concepción del mundo y su manera de hacer también dejen su traza. Lions fue siempre muy francés, en el mejor sentido de la palabra, siendo universal. La Universidad española, que lo es de manera tan peculiar, tiene mucho que aprender del legado de hombres como él.

Pero el siglo XXI que estrenamos será sin duda otra cosa. Con Lions se nos va, ya casi del todo, una etapa épica de las Matemáticas que cada vez es más difícil reconocer hoy en el día a día.

Queda en cualquier caso su huella y mi más profundo agradecimiento.

Referencias

[1] A. Bensoussan, J. L. Lions y G. Papanicolaou, *Asymptotic Analysis for Periodic Structures* en "Studies in Mathematics and its Applications", vol. 5, North-Holland, Amsterdam (1978).

[2] J. L. Lions, *Sur le Contrôle optimal de systèmes gouvernés par des équations aux dérivées partielles*, Dunod, Gauthier Villars, Paris (1968). Traducción al inglés (S.K. Mitter), Springer-Verlag, Lecture Notes, vol. 170 (1971).

[3] J. L. Lions, *Quelques méthodes de résolution des problèmes aux limites non linéaires,* en "Etudes Mathématiques", Dunod, Gauthier Villars, Paris (1969).

[4] J. L. Lions, *Perturbations singulières dans les problèmes aux limites et en Contrôle optimal,* Springer Verlag, New York, Lecture Notes in Mathematics, vol. 323 (1973).

[5] J. L. Lions, *Applications des inéquations variationnelles en contrôle stochastique*, Dunod-Bordas, Collection M.M.I., Paris (1978).

[6] J. L. Lions, *Some Methods in the Mathematical Analysis of Systems and their Control*, Science Press, Beijing (China) y Gordon & Breach Science Publishers Inc., New York (1981).

[7] J. L. Lions, Contrôlabilité exacte des systèmes distribués. Comptes Rendus Acad. Sci. Paris, t. 302 (13), série I, 471-475, Avril 1986.

[8] J. L. Lions, Exact Controllability, Stabilization and Perturbations for Distributed Systems, John Von NEUMANN Lecture 1986, SIAM Annual Meeting, 1986, Boston, SIAM Review, **30** (1) (1988), 1-68.

[9] J. L. Lions, Contrôlabilité exacte, Perturbations et Stabilisation de Systèmes Distribués: Contrôlabilité exacte, Masson, Paris, Collection R.M.A. (Recherches en Mathématiques Appliquées), vol. 8, 1988.

[10] J. L. Lions, Contrôlabilité exacte, Perturbations et Stabilisation de Systèmes Distribués: ContrÙlabilité exacte, Masson, Paris, Collection R.M.A. (Recherches en Mathématiques Appliquées), vol. 9, 1988.

[11] X. Zhang y E. Zuazua, Exact controllability of the semilinear wave equation, en *"Open problems in mathematical systems theory and control"*, en vías de publicación.(`http://www.inma.ucl.ac.be/ blondel/op/`).

Bol. Soc. Esp. Mat. Apl. nº 21(2002), 65–87

Aplicaciones de los autómatas celulares a la generación de bits *

L. Hernández Encinas[1], A. Martín del Rey[2]
y G. Rodríguez Sánchez[2]

[1] Departamento de Tratamiento de la Información y Codificación,
Instituto de Física Aplicada, C.S.I.C.
[2] Departamento de Matemática Aplicada, E.T.S.I.I.,
Universidad de Salamanca

luis@iec.csic.es, delrey@usal.es, gerardo@usal.es

Resumen

Se presentan en este artículo la principales propiedades de los autómatas celulares lineales, y en particular de los llamados de Wolfram. Se definen, además, algunas nociones de criptografía con el fin de señalar las principales aplicaciones de los autómatas celulares a la misma, como la generación de números pseudoaleatorios para los cifrados en flujo o la generación de claves.

Palabras clave: *Autómatas celulares, criptografía, números pseudoaleatorios, generadores de bits.*

Clasificación por materias AMS: *68Q80, 94A60, 11K45, 65C10, 68W20.*

1 Introducción

Uno de los objetivos de las Matemáticas ha sido el de proporcionar herramientas que expliquen algunos de los fenómenos naturales que nos rodean. En general, este proceso se lleva a cabo buscando modelos matemáticos que den respuesta a dichos fenómenos. Así, se puede mencionar el gran desarrollo que ha tenido desde hace unos años el estudio del caos ([6, 10]) y de los sistemas dinámicos ([9, 21]). En el estudio de estos últimos cabe destacar el de los llamados sistemas dinámicos discretos, en particular de los autómatas celulares.

*Los autores agradecen al Dr. J. Muñoz Masqué, del Instituto de Física Aplicada del C.S.I.C., sus sugerencias en la redacción final de este artículo. Este trabajo ha sido parcialmente subvencionado por la Fundación "Samuel Solórzano Barruso". El trabajo de A. M. R. se ha desarrollado durante una estancia en el Dpto. de Tratamiento de la Información y Codificación del C.S.I.C., cuya hospitalidad agradece.

Fecha de recepción: 2 de abril de 2002

Un *autómata celular* es un modelo formal compuesto por un conjunto de células que toman determinados valores. Estos valores van evolucionando con el paso discreto del tiempo según una determinada expresión matemática, que es sensible a los estados de las células vecinas (para un estudio más extenso, véase [22]).

Uno de los ejemplos más extendidos y populares de los autómatas celulares posiblemente sea el conocido como *juego de la vida de Conway* ([5]). El juego consiste en un conjunto de células dispuestas en el plano, cada una de las cuales puede adoptar dos estados: viva (representada por ■ o por un 1) o muerta (representada mediante □ o por un 0). Cada célula está rodeada por otras 8 vecinas, de modo que la distribución de estas 9 células es la de un cuadrado 3×3 (véase la Figura 1), situándose en el centro la considerada en primer lugar.

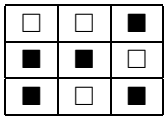


Figura 1. Ejemplo de una célula y su vecindad

A medida que discurre el tiempo, las células nacen y mueren según la siguiente regla: una célula muerta en un momento dado, cambia de estado en el instante siguiente si tiene exactamente 3 células vivas a su alrededor, en caso contrario permanece muerta en el siguiente instante. Por su parte, una célula viva en un instante dado, permanece viva en el instante siguiente si hay 2 ó 3 células vivas a su alrededor; en caso contrario pasa a estar muerta en el instante siguiente. En este caso particular, los autómatas celulares son bidimensionales, dado que la distribución y evolución de las células se lleva a cabo en el plano. Resulta sorprendente que con una regla de evolución tan sencilla como la anterior y partiendo de diferentes configuraciones iniciales se llegue, después de un número determinado de iteraciones, a resultados o configuraciones que puedan ser catalogados de forma tan precisa como la siguiente:

- *Configuraciones estables*: son aquellas disposiciones de células que permanecen inalterables con el paso del tiempo, una vez que se ha llegado a ellas. Algunas de estas diposiciones se pueden observar en la Figura 2.

Figura 2. Configuraciones estables

- *Configuraciones cíclicas*: son disposiciones, como algunas de las mostradas en la Figura 3, que se van obteniendo una detrás de otra cíclicamente.

Figura 3. Configuraciones cíclicas

- *Configuraciones móviles*: son las disposiciones de células que, sin modificar su estructura, se van desplazando en el plano a medida que pasa el tiempo (ver Figura 4).

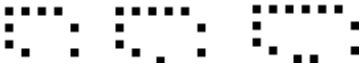


Figura 4. Configuraciones móviles

A lo largo de este artículo se considerarán autómatas

celulares unidimensionales, es decir, aquéllos cuyas células se pueden representar linealmente. Existen otros tipos de autómatas de dimensiones mayores (dependiendo de la disposición del conjunto de sus células), como el del juego de la vida de Conway (que, como ya se ha dicho, es de dimensión 2), pero que no serán tratados aquí. Para un estudio más detallado y extenso de estos autómatas puede consultarse [17].

Las aplicaciones de la teoría de autómatas celulares abarcan aspectos de la ciencia tan diversos como el comportamiento de las moléculas de un gas, el de las personas votando en un sufragio, el estudio de las bacterias eliminadoras de manchas petrolíferas, la evolución de la población, del tráfico, etc. (véanse, por ejemplo [13, 16]). No obstante, las aplicaciones de los autómatas celulares lineales son lo suficientemente interesantes como para no extendernos en los de complejidad mayor. En particular, en este artículo nos vamos a detener en algunas de las aplicaciones que los autómatas celulares tienen en criptología (otras aplicaciones pueden verse en [8, 26]).

Entre otras aplicaciones a la criptología cabe hacer mención a la propuesta en [14], donde se utilizan determinados autómatas celulares para sistemas de cifrado; sin embargo, ésta se demostró insegura en [1]. Por otra parte, el uso de autómatas híbridos o no uniformes (es decir, aquellos autómatas celulares en los que la evolución de los estados de las distintas células viene determinada por más de una expresión matemática) ha sido propuesto en [2, 23, 24, 25].

El resto del artículo se distribuye como sigue. En primer lugar se presentan algunas nociones elementales de criptología en la Sección 2, para pasar en la 3 a la definición de forma más rigurosa de los autómatas celulares unidimensionales. Se presentarán también algunas de sus propiedades y se incluirán algunos ejemplos. En la Sección 4 se analizará su aplicación como generadores de números pseudoaleatorios para cifrados en flujo y en la Sección 5 se verá cómo pueden ser aplicados para generar claves a utilizar en diferentes criptosistemas, en particular a la generación de números primos. Finalmente, se expondrán las conclusiones de este trabajo en la Sección 6.

2 Nociones básicas de criptología

En la actualidad, la gran cantidad de información transmitida mediante redes de ordenadores (Internet, bases de datos remotas, email, etc.) y, en la mayoría de los casos, la necesidad de su confidencialidad (datos personales, cuentas bancarias, números de tarjetas de crédito, etc.) hace necesario que esta información se transmita de manera fiable y segura. Esta seguridad requiere del diseño e implementación de protocolos que garanticen el secreto de los datos enviados. De aquí el auge de la *criptología* (del griego *cripto* –oculto– y *logos* –tratado, ciencia–), cuyo estudio tiene dos ramas claramente diferenciadas: la *criptografía*, que se ocupa del cifrado seguro de la información a enviar, y el *criptoanálisis*, cuya tarea es la de analizar técnicas y métodos para obtener la información cifrada ([4, 12]).

El proceso para cifrar un mensaje consiste en transformarlo mediante un algoritmo de modo que sólo quien esté autorizado podrá invertir el proceso de cifrado (descifrado) para recuperar el texto original. En el algoritmo se utilizan determinados parámetros que se conocen como *claves*, mientras que el mensaje cifrado se denomina *criptograma* y todo este proceso se conoce como *criptosistema*. Si la clave es única y sólo es conocida por las dos personas que se intercambian el mensaje, el criptosistema se llama de *clave simétrica* (o secreta); en otro caso, es decir, si la clave que permite cifrar mensajes es conocida públicamente, mientras que la que descifra es mantenida en secreto, el criptosistema se denomina de *clave asimétrica* (o pública). Dentro de los criptosistemas de clave simétrica existen dos categorías: *cifrados en flujo* y *cifrados en bloque*. De entre los segundos cabe mencionar los criptosistemas DES, IDEA, Triple-DES y Rijndael (para mayor información, ver [4, 12, 19]).

Por su parte, los cifrados en flujo modifican un mensaje mediante una secuencia pseudoaleatoria de bits que se genera a partir de una clave secreta y un algoritmo determinístico. Una vez que el remitente ha expresado el mensaje que se desea transmitir mediante ceros y unos (utilizando, por ejemplo, la equivalencia en ASCII entre las letras y bytes de 8 bits), suma, bit a bit, dicho mensaje con la secuencia pseudoaleatoria, obteniendo el criptograma. Para descifrar el criptograma y obtener el texto claro, el destinatario genera la misma secuencia pseudoaleatoria que el remitente, utilizando el mismo algoritmo determinístico y la misma clave, y suma esta secuencia con el criptograma (la operación de suma bit a bit es una involución). Según este protocolo, para utilizar los cifrados en flujo se debe ser capaz de generar la misma secuencia de bits, tanto en origen como en destino. De ahí que dicha secuencia tenga que ser pseudoaleatoria y dependa de una clave secreta para que nadie, que no sea el remitente o el destinatario, pueda recuperar el mensaje que se está transmitiendo.

La seguridad de los criptosistemas de clave simétrica suele basarse en la dificultad de los ataques llamados de *fuerza bruta*, que consisten en probar todas y cada una de las posibles claves que se pueden emplear en el algoritmo a utilizar. Por su parte, la seguridad de los de clave pública se basa en la dificultad de resolver un problema matemático, aperentemente difícil computacionalmente

hablando. No obstante, no siempre es necesario calcular la clave para poder descifrar mensajes. En ocasiones, si se dispone de información adicional es posible llevar ataques diferentes de los de fuerza bruta o de resolver el problema matemático subyacente. Así, existen principalmente cuatro tipos de ataques a un criptosistema:

1. *Ataque al texto cifrado*: en este caso sólo se conoce un trozo del criptograma correspondiente a un texto claro.

2. *Ataque al texto claro conocido*: en este ataque se utiliza el conocimiento de un trozo del texto claro y su correspondiente criptograma.

3. *Ataque al texto claro elegido*: en este caso, el atacante elige un texto claro y consigue el criptograma correspondiente (no es imprescindible conocer la clave para este ataque, bastaría con que el atacante tuviera acceso temporal a la máquina donde se encuentra implementado el criptosistema).

4. *Ataque al texto cifrado elegido*: en éste, el atacante puede conseguir el texto claro a partir de un texto cifrado que elija (tampoco en este caso se tiene por qué conocer la clave, pues el atacante podría tener temporal acceso a la máquina que lleva a cabo el descifrado de los mensajes).

3 Autómatas celulares

Se denomina *autómata celular d-dimensional* a una colección finita o infinita de células idénticas dispuestas uniformemente según un espacio de d dimensiones y que poseen un estado determinado, que va cambiando con el paso discreto del tiempo según una determinada regla. Esta regla está influida por los estados de las células vecinas ([28]). Consecuentemente, los cuatro
elementos que determinan un autómata celular son los siguientes:

1. Su *dimensión* d. Los autómatas celulares más utilizados suelen ser los unidimensionales o lineales (es decir $d = 1$ y las células se disponen según una linea recta), y los bidimensionales (en cuyo caso $d = 2$ y las células se distribuyen según un plano).

2. El *conjunto de estados* S. Normalmente se considera que el número de estados que puede adoptar una célula es finito, es decir $\#S = k$, por lo que el conjunto que se suele tomar es $S = \mathbb{Z}_k$.

3. La *vecindad* de cada célula del autómata. Es el conjunto de células dispuestas alrededor de una dada y cuyos estados influyen en el estado de la célula considerada en el instante siguiente.

4. La *regla de transición* f. Esta regla rige la evolución de los estados de las células teniendo en cuenta la vecindad de las mismas.

Los primeros autómatas celulares rigurosamente establecidos se debieron a von Neumann ([15]) y a Ulam ([27]). Si bien es verdad que durante cerca de treinta años los autómatas celulares han sido considerados como una especie de curiosidad matemática sin apenas aplicaciones, en la actualidad y gracias fundamentalmente a los trabajos de Wolfram ([30, 31]), se están convirtiendo en una de las herramientas imprescindibles en el estudio de múltiples fenómemos naturales.

3.1 Autómatas celulares lineales

Salvo que se diga lo contrario, consideraremos sólo autómatas celulares unidimensionales, es decir, aquellos para los que $d = 1$, de modo que sus células están dispuestas una a continuación de otra a modo de una cadena. Estos autómatas celulares serán denotados sencillamente por AC. Si el AC lineal consta de n células, cada una de ellas se nombrará por $\langle i \rangle$ con $0 \leq i \leq n-1$. Un ejemplo de un AC lineal con 5 células es el siguiente:

$\langle 0 \rangle$	$\langle 1 \rangle$	$\langle 2 \rangle$	$\langle 3 \rangle$	$\langle 4 \rangle$

Si, además, S_k es el conjunto de k estados y $a_i^{(t)} \in S_k$, $0 \leq i \leq n-1$, es el estado de la célula $\langle i \rangle$ en el instante t, entonces se denomina *configuración del* AC *en el instante* t y se denota por $C^{(t)}$ al siguiente vector:

$$C^{(t)} = \left(a_0^{(t)}, a_1^{(t)}, \ldots, a_{n-1}^{(t)}\right) \in \overbrace{S_k \times \ldots \times S_k}^{n}.$$

La evolución de un AC a lo largo del tiempo se representa de forma sencilla sin más que escribir las sucesivas configuraciones de sus células, una debajo de otra (*diagrama de evolución* del AC). A continuación se muestra un ejemplo del diagrama de evolución de un AC de 4 células.

$a_0^{(0)}$	$a_1^{(0)}$	$a_2^{(0)}$	$a_3^{(0)}$	$\rightsquigarrow$	$C^{(0)}$
$a_0^{(1)}$	$a_1^{(1)}$	$a_2^{(1)}$	$a_3^{(1)}$	$\rightsquigarrow$	$C^{(1)}$
$a_0^{(2)}$	$a_1^{(2)}$	$a_2^{(2)}$	$a_3^{(2)}$	$\rightsquigarrow$	$C^{(2)}$
		$\ldots$			$\ldots$

Denotaremos por V_i a la vecindad de la célula $\langle i \rangle$, es decir, al conjunto de células cuyo estado va a influir en el de $\langle i \rangle$ según la regla de transición que se considere. Las vecindades más comunes en los AC son de caracter *simétrico*, de modo que la célula $\langle i \rangle$ es la célula central. Estas vecindades pueden escribirse de la siguiente manera:

$$V_i(r) = \{\langle i-r \rangle, \ldots, \langle i-1 \rangle, \langle i \rangle, \langle i+1 \rangle, \ldots, \langle i+r \rangle\}, \tag{1}$$

donde r recibe el nombre de *radio de la vecindad*. Existen otros tipos de vecindades no simétricas como por ejemplo las definidas por

$$V_i = \{\langle i-1\rangle, \langle i\rangle, \langle i+1\rangle, \langle i+2\rangle\},$$

o vecindades arbitrarias como la siguiente

$$V_i = \{\langle i-3\rangle, \langle i\rangle, \langle i+1\rangle\}.$$

Dada la célula $\langle i\rangle$, con $i < r$ ó $i > n-r$, la determinación de la vecindad $V_i(r)$ queda restringida a determinadas condiciones de contorno del AC. Usualmente estas condiciones son de dos tipos:

- *Condiciones de contorno periódicas*: en este caso se supone que las n células del AC están dispuestas uniformemente según una circunferencia (ver Figura 5):

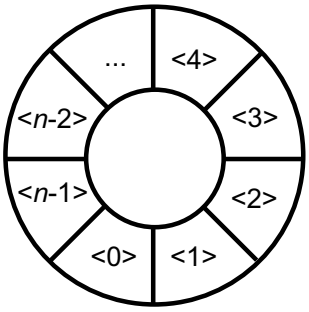


Figura 5. Disposición periódica

  de tal forma que a la izquierda de la célula $\langle 0\rangle$ están las células $\langle n-1\rangle$, $\langle n-2\rangle, \ldots$, mientras que a la derecha de la célula $\langle n-1\rangle$ estarían las células $\langle 0\rangle, \langle 1\rangle, \ldots$

- *Condiciones de contorno reflexivas*: en este otro caso se supone que a la izquierda de la célula $\langle 0\rangle$ se encuentran las células $\langle 1\rangle, \langle 2\rangle, \ldots$, mientras que a la derecha de la célula $\langle n-1\rangle$ se encuentran las células $\langle n-2\rangle, \langle n-3\rangle, \ldots$:

$$\langle n-1\rangle \quad \cdots \quad \langle 1\rangle \;\boxed{\langle 0\rangle \mid \langle 1\rangle \mid \cdots \mid \langle n-1\rangle}\; \langle n-2\rangle \quad \cdots \quad \langle 0\rangle$$

De aquí en adelante, si no se hace referencia expresa a lo contrario, se supondrá que las vecindades usadas son las simétricas y las condiciones de contorno son las periódicas.

Finalmente, la evolución de los estados de las distintas células del AC viene determinada por la denominada regla de transición $f : S_k^{2r+1} \to S_k$. Así, si

$V_i(r)$ es la vecindad definida en el AC según (1), entonces el estado de la célula $\langle i \rangle$ en el instante $t+1$ vendrá dado por una expresión matemática que depende de los estados de los elementos de $V_i(r)$ en el instante t:

$$a_i^{(t+1)} = f\left(a_{i-r}^{(t)}, \ldots, a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}, \ldots, a_{i+r}^{(t)}\right).$$

Si el AC tiene k estados y el radio de la vecindad es r, el número de posibles reglas que se pueden definir es $k^{k^{2r+1}}$.

Ejemplo. Consideremos un AC de $n = 11$ células, en el que $k = 2$ y $r = 1$ (obviamente suponemos condiciones de contorno periódicas, de tal forma que a efectos de notación, los subíndices se toman módulo n, es decir, en nuestro ejemplo, $a_{-1}^{(t)} = a_{10}^{(t)}$ y $a_{11}^{(t)} = a_0^{(t)}$). El conjunto de estados de este AC es $\mathbb{Z}_2$ y la vecindad de cada célula depende exclusivamente de las dos que la rodean. Supongamos, además, que la regla de transición que rige su evolución viene dada por la siguiente expresión:

$$a_i^{(t+1)} = \left(a_{i-1}^{(t)} + a_i^{(t)} + a_{i+1}^{(t)}\right) \bmod 2, \quad i \geq 0. \tag{2}$$

Si el estado inicial de este AC es el definido por la siguiente configuración

$$C^{(0)} = (0,0,0,0,0,1,0,0,0,0,0),$$

calculando 8 iteraciones sucesivas según la función de transición considerada, se obtiene la tabla de evolución siguiente:

$a_{10}^{(t)}$	$a_0^{(t)}$	$a_1^{(t)}$	$a_2^{(t)}$	$a_3^{(t)}$	$a_4^{(t)}$	$a_5^{(t)}$	$a_6^{(t)}$	$a_7^{(t)}$	$a_8^{(t)}$	$a_9^{(t)}$	$a_{10}^{(t)}$	$a_0^{(t)}$
0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	1	1	1	0	0	0	0	0
0	0	0	0	1	0	1	0	1	0	0	0	0
0	0	0	1	1	0	1	0	1	1	0	0	0
0	0	1	0	0	0	1	0	0	0	1	0	0
1	1	1	1	0	1	1	1	0	1	1	1	1
0	0	1	0	0	0	1	0	0	0	1	0	0
0	0	1	1	0	1	1	1	0	1	1	0	0

Si ahora se sustituye cada uno de los bits 1 por un cuadrado negro (■) y cada uno de los bits 0 por un cuadrado blanco (□), tal y como se hizo para el caso del AC del juego de la vida de Conway, se obtiene una tabla en la que se muestra el diagrama de evolución de este AC para las 8 iteraciones mostradas en la tabla anterior:

$a_{10}^{(t)}$	$a_0^{(t)}$	$a_1^{(t)}$	$a_2^{(t)}$	$a_3^{(t)}$	$a_4^{(t)}$	$a_5^{(t)}$	$a_6^{(t)}$	$a_7^{(t)}$	$a_8^{(t)}$	$a_9^{(t)}$	$a_{10}^{(t)}$	$a_0^{(t)}$
	□	□	□	□	□	■	□	□	□	□	□	
	□	□	□	□	■	■	■	□	□	□	□	
	□	□	□	■	□	■	□	■	□	□	□	
	□	□	■	■	□	■	□	■	■	□	□	
	□	■	□	□	□	■	□	□	□	■	□	
	■	■	■	□	■	■	■	□	■	■	■	
	□	■	□	□	□	■	□	□	□	■	□	
	□	■	■	□	■	■	■	□	■	■	□	

Para observar de forma más detallada la evolución de este AC con la configuración inicial dada, se puede proceder a determinar, por ejemplo, las 50 primeras iteraciones. Llevando a cabo un proceso similar al anterior, de modo que sólo se sustituyen los bits 1 por ■, dejando en blanco los lugares correspondientes a los bits 0, se obtiene una representación de su diagrama de evolución, que se puede observar en la Figura 6.

Figura 6. Ejemplo del diagrama de evolución del AC definido en (2)

3.2 Autómatas celulares de Wolfram

Consideremos el caso particular de los AC definidos de modo que su conjunto de estados es $S = \mathbb{Z}_2$ y el radio de la vecindad es $r = 1$. Para este caso particular de AC, el número de reglas de transición existentes es, según se mencionó anteriormente, $2^{2^{2r+1}} = 2^8 = 256$. Wolfram ([28]) ideó una notación consistente en asignar a cada una de las 256 reglas de transición un número comprendido entre 0 y 255. Dado que $r = 1$ la vecindad de una célula está formada por ella misma, la célula situada a su izquierda y la célula situada a su derecha. Como el conjunto de estados es $\mathbb{Z}_2$, los dos estados en que puede encontrarse una célula son 0 ó 1. Consecuentemente existen $2^3 = 8$ posibles configuraciones de la vecindad de una célula dada, a saber:

$$111 \quad 110 \quad 101 \quad 100 \quad 011 \quad 010 \quad 001 \quad 000$$

El primer dígito de cada configuración representa el estado de la célula de la izquierda, el dígito central el estado de la célula de cuya vecindad hablamos

y el último dígito hace referencia al estado de la célula de la derecha. Es claro que toda regla de transición consiste en asignar a cada una de estas posibles configuraciones de la vecindad un elemento de $\mathbb{Z}_2$. El número a asignar a una regla de transición se calculará de la siguiente forma:

1. Se aplica la regla de transición a cada una de las 8 configuraciones anteriores,
2. Se concatenan los bits obtenidos,
3. Se interpreta dicha concatenación como un número en base 2 y
4. Se considera la expresión decimal de dicho número.

El número así obtenido se denomina el *número de Wolfram* de la regla de transición considerada. En el caso concreto de la regla dada en (2) este proceso sería el siguiente:

$$\left.\begin{array}{llll} 111 \to 1, & 110 \to 0, & 101 \to 0, & 100 \to 1, \\ 011 \to 0, & 010 \to 1, & 001 \to 1, & 000 \to 0, \end{array}\right\} \Rightarrow 10010110_2 = 150,$$

de modo que el número de Wolfram de la regla de transición mencionada es el 150.

El propio Wolfram, tras múltiples simulaciones de los diferentes AC, estableció la siguiente clasificación de los mismos en virtud del comportamiento manifestado en los diagramas de evolución ([29]):

- AC *de clase* 1: son aquellos que evolucionan hacia estados homogéneos o constantes —o todo ceros, o todo unos—. Además, dicha evolución es independiente de la configuración inicial considerada.
- AC *de clase* 2: son los autómatas que dan lugar a conjuntos de estructuras periódicas y estables. En ellos la evolución del estado de una determinada célula a lo largo del tiempo estará influida por los estados de un grupo fijo de células de la configuración inicial.
- AC *de clase* 3: son todos aquellos autómatas celulares cuyo comportamiento se vuelve caótico con el paso del tiempo, de tal forma que el cambio de estado de una célula va a depender cada vez más de un mayor número de estados iniciales. Se ha conjeturado que el cálculo de dicho estado se puede hacer mediante un simple algoritmo.
- AC *de clase* 4: son aquellos que dan lugar a estructuras complejas, las cuales pueden permanecer localizadas en el espacio o bien moverse a lo largo del mismo. En esta clase, la evolución del estado de una célula en particular dependerá de una gran cantidad de estados iniciales, de manera que la determinación exacta de dicho estado es un problema cuya complejidad es equivalente a la propia simulación explícita del AC.

4 Los AC como generadores pseudoaleatorios

Como ya se mencionó (ver §2), para utilizar un cifrado en flujo es necesario disponer de un generador de bits pseudoaleatorio que genere la misma secuencia de bits, tanto en origen como en destino, a partir de una misma clave secreta. A continuación presentaremos algunos de los generadores de bits más utilizados en este tipo de cifrados, para pasar posteriormente a comentar el uso de los autómatas celulares como generadores pseudoaleatorios de secuencias cifrantes.

4.1 Generación de bits pseudoaleatorios

Un *generador de bits (o de números) aleatorio* es un dispositivo que proporciona como salida una secuencia de dígitos binarios (o de números) que son estadísticamente independientes. Algunos de los generadores de bits aleatorios diseñados por hardware están basados en la aleatoriedad de fenómenos físicos, como por ejemplo: La emisión de partículas durante un proceso radiactivo entre dos instantes de tiempo, el ruido producido por un diodo semiconductor en una corriente, etc. Debido a la imposibilidad práctica de que una secuencia obtenida por uno de estos generadores se pueda volver a obtener exactamente de la misma forma, en diferentes momentos, estos generadores de bits no suelen ser utilizados en criptología, al menos en los cifrados en flujo. Es posible utilizarlos en otras aplicaciones criptográficas como para generar determinados tipos de números (primos, de determinada longitud, etc.)

Por su parte, un *generador de bits (o de números) pseudoaleatorio* es un algoritmo determinístico que al darle como entrada una secuencia auténticamente aleatoria de longitud pequeña, proporciona una secuencia de bits (o de números) de longitud mucho mayor y que parece ser aleatoria. Las salidas de estos generadores no son aleatorias en el sentido de que cada vez que se ejecute el algoritmo con los mismos parámetros se van a obtener las mismas salidas. No obstante, lo que se desea conseguir con estos generadores es que las salidas obtenidas parezcan aleatorias, es decir, que resulte imposible poder distinguir entre la secuencia pseudoaleatoria obtenida y una realmente aleatoria en un tiempo polinómico ([4, Apéndice B]).

Estos generadores de números requieren verificar determinadas características en función de las aplicaciones prácticas a las que estén destinados. Una de ellas es la *aleatoriedad*, que debe analizarse para cada una de las secuencias que se generen y antes de ser utilizada en la práctica, de modo que la serie de números a emplear cumpla las propiedades que se supone verifican las series de números aleatorios (por ejemplo, los póstulados de Golomb [7]). Para llevar a cabo este análisis se recurre a determinados tests estadísticos diseñados ad hoc (véanse [4, Apéndice A], [12, Chapter 5]).

Una característica adicional que se requiere en criptografía es la *seguridad*, es decir, se trata de conseguir alguna garantía de que estos generadores son seguros en el sentido de que las salidas son imprevisibles. Para ello se recurre a analizar las operaciones matemáticas en las que se basa la definición del generador y la dificultad de los problemas matemáticos subyacentes.

Algunos de los generadores de bits pseudoaleatorios más utilizados son los siguientes:

1. *Generadores de bits lineales en congruencias*: son los generadores que utilizan la siguiente expresión recursiva:

$$x_{i+1} = (a \cdot x_i + c) \bmod m, \quad i \geq 0,$$

a partir de una semilla aleatoria dada x_0, considerando como secuencia de bits, el bit de paridad (es decir, el bit menos significativo) de cada uno de los números x_i generados.

2. *Generadores cuadráticos*: son los generadores definidos por

$$x_{i+1} = (a \cdot x_i^2 + b \cdot x_i + c) \bmod m, \quad i \geq 0.$$

También en este caso se considera como secuencia la definida por paridad(x_i).

3. *Generadores de registro de desplazamiento realimentados linealmente (LFSR)*: son generadores cuya regla de recurrencia está definida por:

$$x_i = a_1 \cdot x_{i-1} \oplus a_2 \cdot x_{i-2} \oplus \ldots \oplus a_r \cdot x_{i-r}, \quad i > r,$$

siendo $\oplus$ la operación XOR.

4.2 Los AC de Wolfram como cifradores en flujo

Como ya hemos mencionado, una de las principales aplicaciones de los AC a la criptografía es su uso como generadores de bits para los cifrados en flujo. En esta sección veremos cómo los AC lineales, en particular los AC de Wolfram, pueden generar números pseudoaleatorios.

Consideraremos los AC de Wolfram definidos por las reglas de transición números 30 y 45, respectivamente, que parecen ser los que tienen mejores propiedades como generadores de bits pseudoaleatorios ([31]):

$$\begin{aligned} a_i^{(t+1)} &= \left(a_{i-1}^{(t)} + a_i^{(t)} + a_{i+1}^{(t)} + a_i^{(t)} \cdot a_{i+1}^{(t)}\right) \bmod 2 \\ &= a_{i-1}^{(t)} \text{ XOR } \left(a_i^{(t)} \text{ OR } a_{i+1}^{(t)}\right), \qquad (3) \\ a_i^{(t+1)} &= \left(1 + a_{i-1}^{(t)} + a_{i+1}^{(t)} + a_i^{(t)} \cdot a_{i+1}^{(t)}\right) \bmod 2 \\ &= a_{i-1}^{(t)} \text{ XOR } \left(a_i^{(t)} \text{ OR } \left(\text{NOT } a_{i+1}^{(t)}\right)\right), \qquad (4) \end{aligned}$$

Los diagramas de evolución de cada uno de los dos AC anteriores pueden verse en las Figuras 7 y 8, respectivamente.

Figura 7. Diagrama de evolución del AC de regla 30

Figura 8. Diagrama de evolución del AC de regla 45

La obtención de tales representaciones se ha hecho de forma análoga a como se hizo para el AC definido por la regla dada en (2) (ver Figura 6). En este caso, se han considerado 50 iteraciones para cada uno de los dos AC definidos en (3) y (4) con la misma configuración inicial, a saber:

$$\left(0, \overset{(50}{\ldots}, 0, 1, 0, \overset{(50}{\ldots}, 0\right).$$

Se podría pensar en utilizar estos dos AC como generadores pseudoaleatorios sin más que considerar como semilla a la configuración inicial y tomar como salida la lista de ceros y unos definida por la última configuración. Sin embargo, hacerlo así supondría que se generaría una lista de tantos bits como bits de partida, dado que el número de células de todas las configuraciones es el mismo, por lo que este procedimiento no parece adecuado. Si lo que se desea es obtener una secuencia de bits cuya longitud sea mucho mayor que la longitud de la semilla o configuración inicial, es conveniente considerar como secuencia de salida la evolución de una de las células del AC. Con ello sólo haría falta conocer el estado inicial de unas pocas células e iterar el AC tantas veces como bits se requieran.

Si se considera como salida del AC la evolución de la célula central (sin considerar su estado inicial), a lo largo de 100 iteraciones, para la configuración inicial o semilla dada por

$$(0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0), \tag{5}$$

se tiene la siguiente salida de 100 bits:

$$1,0,1,1,1,0,0,1,1,0,0,0,1,0,1,1,0,0,1,0,0,1,1,1,1,0,1,1,1,1,0,1,0,1,$$
$$1,1,1,0,1,0,1,0,0,1,0,0,0,1,0,1,1,1,0,0,0,0,0,1,0,0,1,1,0,1,1,1,1,1,$$
$$0,0,1,0,0,1,0,0,1,0,0,1,0,1,1,1,1,0,1,0,1,1,1,0,0,1,0,1,0,1,0,0. \qquad (6)$$

El diagrama de evolución en este caso se presenta en la Figura 9 (la evolución de la célula central se ha girado 90 grados y sigue un recorrido evolutivo de izquierda a derecha).

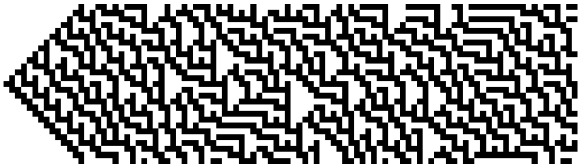


Figura 9. Diagrama de evolución del AC de regla 30 con 100 iteraciones

Se puede observar que con la configuración inicial de 25 células dada en (5), se ha obtenido la secuencia de 100 bits presentada en (6), si bien esta longitud podría ser mucho mayor sin más que iterar más veces la evolución del AC considerado.

La decisión de la secuencia de bits a utilizar como salida dependerá del tipo de AC de que se trate. Téngase en cuenta que exiten AC cuya evolución es muy simétrica, lo que dificulta su uso como generadores de números pseudoaleatorios. Como ejemplo puede verse el AC definido por la regla 22, cuya expresión es:

$$a_i^{(t+1)} = \left(a_{i-1}^{(t)} + a_i^{(t)} + a_{i+1}^{(t)} + a_{i-1}^{(t)} \cdot a_i^{(t)} \cdot a_{i+1}^{(t)}\right) \bmod 2$$

y cuya representación se muestra en la Figura 10.

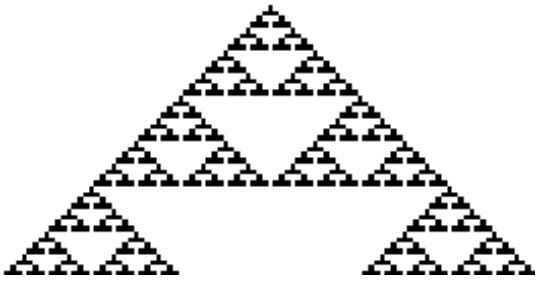


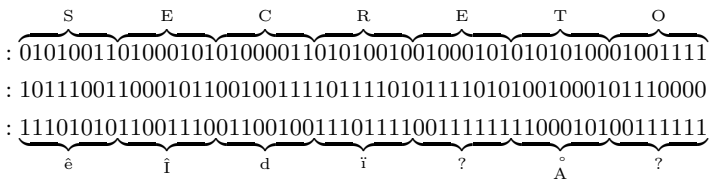
Figura 10. Diagrama de evolución del AC de regla 22

Una vez que se ha generado una secuencia pseudoaleatoria de bits (formada por los valores de los estados de las células que ocupan la posición $\langle i \rangle$ a lo largo del tiempo), se puede considerar el cifrado en flujo cuya clave secreta (que comparten tanto el remitente como el destinatario del mensaje) es la configuración inicial considerada.

Ejemplo. Supongamos que se tiene el AC definido en (3), para el que se utiliza la semilla (5) y como salida de bits pseudoaleatorios la dada en (6). Para obtener el criptograma, C, correspondiente al mensaje

SECRETO

basta con concatenar el valor en binario de cada una de las letras del mensaje, según el código ASCII, y luego sumar, bit a bit, el mensaje obtenido, M, con la secuencia de bits o clave, K:



De este modo, el criptograma que se envía es el siguiente:

êÎdï?Å?

El destinatario recupera el mensaje original sin más que concatenar el valor en binario de cada una de las letras o símbolos del criptograma recibido y sumar, bit a bit, el criptograma, C, con la clave, K, dado que esta operación es una involución.

La seguridad de este criptosistema está basada en la impredecibilidad de la clave K, es decir, en la dificultad de poder obtener la secuencia pseudoaleatoria generada por el AC. De ahí la importancia de que los AC elegidos como generadores de bits pseudoaleatorios tengan buenas propiedades estadísticas.

En [11] se estudia la seguridad del criptosistema definido anteriormente con el AC dado en (3) mediante el ataque al texto claro conocido. Los autores desarrollan un algoritmo de criptoanálisis para este AC, de modo que el ataque tiene éxito sobre un PC si el tamaño de la clave (es decir, el número de células de la configuración inicial del AC) está comprendido entre 300 y 500 bits. Para adversarios con mayores potencias de cálculo (por ejemplo, computación en paralelo), se recomienda que el tamaño de la clave sea superior a 1000 bits. El ataque se fundamenta en el hecho de que a partir de la expresión dada en (3), es posible obtener la siguiente fórmula lineal en a_{i-1} para el instante t:

$$a_{i-1}^{(t)} = \left(a_i^{(t+1)} + a_i^{(t)} + a_{i+1}^{(t)} + a_i^{(t)} \cdot a_{i+1}^{(t)}\right) \bmod 2, \tag{7}$$

que permite calcular el valor del estado de la célula $\langle i-1\rangle$ en un instante dado, en función de los valores de los estados de las células $\langle i\rangle$ e $\langle i+1\rangle$ en el mismo instante y de la célula $\langle i\rangle$ en el instante siguiente. Es decir, si se conocen los valores de n estados consecutivos de la célula $\langle i\rangle$ y de $n-1$ estados de la célula adyacente $\langle i+1\rangle$, es posible deteminar $n-1$ estados de la otra célula adyacente a la célula $\langle i\rangle$, esto es de la $\langle i-1\rangle$. En efecto, consideremos el siguiente

Ejemplo. Supongamos que se conocen los valores de $n = 5$ estados de la célula $\langle 5\rangle$ para los instantes $t, \ldots, t+4$: $(0, 0, 1, 1, 0)$ y de $n-1 = 4$ estados de la célula adyacente $\langle 6\rangle$ para los instantes $t, \ldots, t+3$: $(1, 1, 1, 0)$. Entonces, aplicando la expresión (7) para el instante $t+3$ y para el estado $i-1 = 4$, se tiene

$$\begin{aligned} a_4^{(t+3)} &= \left(a_5^{(t+4)} + a_5^{(t+3)} + a_6^{(t+3)} + a_5^{(t+3)} \cdot a_6^{(t+3)}\right) \bmod 2 \\ &= (0 + 1 + 0 + 1 \cdot 0) \bmod 2 = 1, \end{aligned}$$

ahora, reiterando esta misma expresión, se calculan los siguientes valores:

$$\begin{aligned} a_4^{(t+2)} &= \left(a_5^{(t+3)} + a_5^{(t+2)} + a_6^{(t+2)} + a_5^{(t+2)} \cdot a_6^{(t+2)}\right) \bmod 2 \\ &= (1 + 1 + 1 + 1 \cdot 1) \bmod 2 = 0, \\ a_4^{(t+1)} &= \left(a_5^{(t+2)} + a_5^{(t+1)} + a_6^{(t+1)} + a_5^{(t+1)} \cdot a_6^{(t+1)}\right) \bmod 2 \\ &= (1 + 0 + 1 + 0 \cdot 1) \bmod 2 = 0, \\ a_4^{(t)} &= \left(a_5^{(t+1)} + a_5^{(t)} + a_6^{(t)} + a_5^{(t)} \cdot a_6^{(t)}\right) \bmod 2 \\ &= (0 + 0 + 1 + 0 \cdot 1) \bmod 2 = 1, \end{aligned}$$

con lo que se obtienen los valores de los estados de la célula $\langle 4\rangle$ para los instantes $t, \ldots, t+3$: $(1, 0, 0, 1)$.

A partir de la expresión (7) y con el criptosistema descrito anteriormente, si se considera el ataque al texto claro conocido, se dispone de la pareja formada por un trozo de texto claro y su correspondiente criptograma. Sumando bit a bit ambas secuencias, se obtiene la evolución de la célula que ocupa la posición i-ésima, es decir, una parte de la secuencia cifrante. Ahora bien, por la fórmula (7) si se conocieran además los estados de la célula $\langle i+1\rangle$, adyacente a la célula $\langle i\rangle$, en cada instante de tiempo, se podría recuperar el diagrama de evolución completo del AC utilizado y, en particular, la configuración inicial, esto es, la clave del criptosistema que permitiría descifrar cualquier otro criptograma. Así pues, este ataque prueba que el conocimiento de la evolución de la célula $\langle i+1\rangle$ es equivalente al conocimiento de la clave. A partir de este hecho, el criptoanálisis sólo busca cómo determinar dicha evolución.

Concretamente, el algoritmo dado en [11] permite obtener la clave de $2n+1$ bits del criptosistema a partir del conocimiento de n bits de la secuencia cifrante, que es la evolución de una de las células del AC. Para ello se supone que la célula cuya evolución se conoce es la central, es decir, se conocen los n valores $a_i^{(t+k)}$, con $k = 0, \ldots, n-1$. A continuación se generan de forma aleatoria los $n-1$ valores de las células que están a su derecha para el instante t, es decir, $a_{i+j}^{(t)}$, con $j = 1, \ldots, n-1$. A partir de aquí, se determinan los valores de las células que aparecen en el triángulo derecho de la configuración del AC, es decir, los estados de las células $a_{i+j}^{(t+k)}$, siendo $j = 1, \ldots, n-k$, con $k = 1, \ldots, n-1$. Posteriormente se deduce el valor de las células del triángulo izquierdo, es decir,

de $a_{i-j}^{(t+k)}$, siendo $k = 0, \ldots, n-j$, con $j = 1, \ldots, n-1$. Con ello se obtiene la configuración inicial completa que corresponde a la secuencia cifrante del AC dado. Se puede comprobar que con la configuración inicial obtenida se genera un AC que tiene como evolución de la célula $\langle i \rangle$ la dada originalmente. El algoritmo escrito en pseudocódigo es el siguiente:

1. For j from 1 to $n-1$ do $a_{i+j}^{t} := \text{rand}(0.,1)$
2. For k from 1 to $n-1$ do
   For j from 1 to $n-k$ do
   $a_{i+j}^{k} := \left(a_{n+j-1}^{k-1} + a_{n+j}^{k-1} + a_{n+j+1}^{k-1} + a_{n+j}^{k-1} \cdot a_{n+j+1}^{k-1}\right) \bmod 2$
3. For j from 1 to $n-1$ do
   For k from $n-j$ by -1 to 0 do
   $a_{n-j}^{k} := \left(a_{n-j+1}^{k+1} + a_{n-j+1}^{k} + a_{n-j+2}^{k} + a_{n-j+1}^{k} \cdot a_{n-j+2}^{k}\right) \bmod 2$

A modo de ejemplo, se presenta el siguiente caso.

Ejemplo. Supongamos que la secuencia cifrante viene dada por los siguientes $n = 11$ valores: $s = (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$. Aplicando el primer paso del algoritmo obtenemos los siguientes $n - 1 = 10$ valores aleatorios: $1, 1, 0, 0, 1, 0, 1, 1, 1, 0$. Mediante el segundo paso del algoritmo se construye el triángulo de la derecha:

$$
\begin{array}{cccccccccc}
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & & \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & & & \\
0 & 1 & 0 & 1 & 0 & 1 & & & & \\
1 & 1 & 0 & 1 & 0 & & & & & \\
1 & 0 & 0 & 1 & & & & & & \\
0 & 1 & 1 & & & & & & & \\
1 & 1 & & & & & & & & \\
0 & & & & & & & & &
\end{array}
$$

Con el siguiente paso se determina el triángulo de la izquierda:

$$
\begin{array}{cccccccccc}
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
 & & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
 & & & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & & & & 1 & 0 & 0 & 1 & 0 & 0 \\
 & & & & & 1 & 1 & 1 & 1 & 0 \\
 & & & & & & 0 & 0 & 0 & 1 \\
 & & & & & & & 0 & 1 & 1 \\
 & & & & & & & & 1 & 0 \\
 & & & & & & & & & 0
\end{array}
$$

Finalmente, se puede comprobar que la configuración inicial (esto es, la clave) de $2n - 1 = 21$ bits obtenida

$$C^{(0)} = (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$$

genera, mediante el AC, la secuencia cifrante original. En efecto, la evolución del AC con dicha configuración es la siguiente:

1	0	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	1	1	1	0
1	1	1	1	0	1	0	1	1	1	0	0	0	1	1	1	0	1	0	0	0
1	0	0	0	0	1	0	1	0	0	1	0	1	1	0	0	0	1	1	0	1
0	1	0	0	1	1	0	1	1	1	1	0	1	0	1	0	1	1	0	0	1
0	1	1	1	1	0	0	1	0	0	0	0	1	0	1	0	1	0	1	1	1
0	1	0	0	0	1	1	1	1	0	0	1	1	0	1	0	1	0	1	0	0
1	1	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	0	1	1	0
1	0	0	0	1	0	1	0	1	1	0	0	1	1	1	0	1	0	1	0	0
1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1
0	0	0	1	0	0	1	0	1	0	1	0	0	1	0	1	1	0	1	0	0
0	0	1	1	1	1	1	0	1	0	1	1	1	1	0	1	0	0	1	1	0

Obsérvese que el algoritmo requiere del conocimiento de n bits de la secuencia cifrante, es decir, de n valores de la evolución de una célula para poder determinar una clave de $2n-1$ bits (esto es, una configuración de $2n-1$ células). Así pues, si se conocen menos de n valores de la secuencia cifrante, no es posible recuperar la clave original, supuesto que ésta tenga $2n-1$ bits. En efecto, basta con observar cómo en el siguiente ejemplo, no se recupera la clave original, lo que lleva a que la evolución de la célula central del AC obtenido con el algoritmo anterior no conduzca a la secuencia cifrante de partida.

Ejemplo. Supongamos ahora que la clave tiene la misma longitud que antes, es decir, $2n-1=21$ bits, pero sólo se conocen 6 valores de la secuencia cifrante: $(1,0,1,1,0,0)$. En este caso, el algoritmo anterior daría la siguiente evolución y configuración inicial:

1	1	0	0	1	1	1	1	0	0	1
	0	1	1	1	0	0	0	1	1	
		1	0	0	1	0	1	1		
			1	1	1	0	1			
				0	0	0				
					0					

mientras que la evolución del AC con la clave obtenida proporciona los siguientes resultados:

1	1	0	0	1	1	1	1	0	0	1
0	0	1	1	1	0	0	0	1	1	1
1	1	1	0	0	1	0	1	1	0	0
1	0	0	1	1	1	0	1	0	1	1
0	1	1	1	0	0	0	1	0	1	0
1	1	0	0	1	0	1	1	0	1	1
0	0	1	1	1	0	1	0	0	1	0
1	0	0	0	1	0	1	0	1	1	0
1	1	0	1	1	0	1	0	1	0	1
0	0	0	1	0	0	1	0	1	0	1
0	0	1	1	1	1	1	0	1	0	1

Como se puede ver, no todos los valores de la evolución de la célula central de este caso $(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$ coinciden con los valores de la secuencia dada en el primer ejemplo: $s = (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$.

Para el AC definido en (4), el criptoanálisis es aún más efectivo, es decir, se deben considerar claves de longitudes mayores para obtener la misma seguridad que con el AC definido en (3).

5 Los AC como generadores de claves

En numerosos criptosistemas es necesario generar claves numéricas de forma aleatoria. Por ejemplo, en el criptosistema RSA ([18, 20]) hace falta obtener dos números primos grandes, de modo que a partir de ellos se genere el módulo para la clave pública. También hace falta generar una clave de sesión a la hora de cifrar mediante otros muchos criptosistemas, como, por ejemplo, en el propuesto por ElGamal ([3]), basado en el logaritmo discreto. Por tanto, y dado que los AC de Wolfram pueden generar números aleatorios, cabe la posibilidad de utilizarlos con este fin.

En general, las claves numéricas que se utilizan vienen caracterizadas por su longitud, de ahí que para generar una clave de k bits sea necesario partir de una determinada configuración del AC de Wolfram definido en (3) e iterarlo k veces. Si la única restricción es que la clave sea aleatoria y de k bits, para garantizar que el número a obtener tenga exactamente k bits se puede generar una secuencia pseudoaleatoria de $k - 1$ bits y añadir un bit 1 a la izquierda. Posteriormente, si se desea que la clave generada sea un número en base 10, bastará con transformar la colección de bits, considerada como un número en binario, a base decimal.

Ejemplo. Si se desea generar una clave de 256 bits, bastará con utilizar una configuración inicial de, por ejemplo, 25 células e iterar el AC 255 veces. Así, si la configuración inicial es

$$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0),$$

después de 255 iteraciones se obtiene la siguiente secuencia pseudoaleatoria de bits:

$$0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1,$$
$$0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1,$$
$$0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0,$$
$$0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0,$$
$$1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0,$$
$$0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1,$$
$$1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1,$$
$$0, 1, 1, 0, 1, 0, 1, 0, 0, 1.$$

Como dicha secuencia comienza por 0, al añadir el bit 1 delante y convertir el número obtenido en base decimal, se obtiene que el valor de la clave es un número de 77 dígitos:

77330 85567 53433 11675 30533 45272 09632 25354 28229 51380 28346 06129 11250 49192 67608 73.

En el caso de que se deseen generar números con otras condiciones añadidas, como ser primos, por ejemplo, se puede realizar el proceso anterior de forma parecida, si bien se deberá utilizar algún criterio o test que asegure (aunque sea de forma probabilística) que el número obtenido sea primo. Una forma de ahorrar algún tiempo de computación para generar un número primo de exactamente k bits, consiste en generar una secuencia pseudoaleatoria de $k-2$ bits y luego añadir sendos bits 1 al inicio y al final de dicha secuencia. De esta forma queda garantizado que el número decimal en el que se convierte dicha secuencia tiene exactamente k bits y que es impar (hecho que se deduce porque el último bit del número —el bit de paridad— es un 1). En el caso del número generado anteriormente, se puede afirmar que es compuesto dado que su factorización como producto de primos es la siguiente:

$$19 \cdot 29 \cdot 313 \cdot 2663 \cdot 125093 \cdot 1346023694316866997551227374112895407476083323419667212185295469.$$

Uno de los criterios de primalidad más extendidos es el debido a Miller-Rabin ([4, 12]). Éste es un test probabilístico para decidir si un número dado es o no primo y está basado en los pseudoprimos de Euler (dados dos números enteros, a y n, se dice que n es un *pseudoprimo de Euler de base* a si son primos entre sí y si $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n$, donde $\left(\frac{a}{n}\right)$ representa el símbolo de Legendre). Si la salida del test afirma que el número es *compuesto*, entonces el número evaluado es, en efecto, compuesto; mientras que si la salida del test indica que es *primo*, dicho número es primo con una probabilidad $1-(1/4)^t$, siendo t el número de veces que se lleva a cabo el test. Por tanto, para obtener una probabilidad del $99,99\,\%$ de que un número dado sea primo, basta con ejecutar el test de Miller-Rabin $t=7$ veces para diferentes valores de la base. Como ejemplo de lo que acabamos de señalar presentamos el siguiente

Ejemplo. Si se desea generar un número primo de 100 bits,
consideramos la siguiente configuración inicial para el AC:

$$(1,0,0,1,0,1,0,1,0,1,1,1,1,1,1,0,1,0,0,1,1,0,1,0,0,0)$$

y lo iteramos 98 veces, obteniendo la siguiente secuencia de bits:

$$1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,0,1,1,1,0,1,0,1,0,1,0,1,1,1,0,0,1,1,0,$$
$$0,0,0,1,0,1,0,0,0,1,0,1,1,1,1,1,1,1,0,1,1,0,1,0,1,0,0,1,0,1,1,1,1,1,0,$$
$$1,0,0,1,1,0,0,0,0,1,0,1,0,1,1,0,0,1,0,0,1,1,1,1,1,0,1,0.$$

Añadiendo ahora un bit 1 al inicio y otro al final de la secuencia anterior, se obtienen 100 bits. La expresión de esta secuencia de bits en base 10 es

$$950984169159075177987037645301.$$

Ejecutando el test de Miller-Rabin 7 veces a dicho número se obtiene como salida que dicho número es primo, por lo que se puede asegurar con una probabilidad del $99,99\,\%$ de que lo es.

6 Conclusiones

En el presente artículo hemos definido y señalado algunas características y propiedades de los autómatas celulares, en particular, de los AC lineales y, de forma más concreta, de los llamados autómatas celulares de Wolfram. De entre todos ellos, nos hemos detenido con mayor detalle en el definido por la regla 30. También hemos presentado algunas nociones básicas de criptografía con el fin de comentar algunas aplicaciones de los AC a esta ciencia. A modo de resumen podemos señalar que los autómatas celulares lineales, y principalmente el definido por la regla 30, que es el que presenta mejores propiedades pseudoaleatorias, pueden ser utilizados como generadores de bits pseudoaleatorios con diferentes propósitos. Uno de ellos es el de ser utilizados en el algoritmo que genera la secuencia cifrante en los cifrados en flujo, siempre que se tengan en cuenta determinadas precauciones. Estas precauciones están relacionadas con temas referidos a su seguridad o impredecibilidad, dado que existen procedimientos y algoritmos que permiten determinar la secuencia generada por un AC, si la longitud de la configuración inicial, que es utilizada como clave, no es lo suficientemente grande. Por otra parte, también hemos señalado la posibilidad de utilizar las secuencias de bits generadas por un AC de Wolfram como claves de sesión, o para generar determinadas claves parciales, verificando propiedades particulares, como ser números primos, por ejemplo.

Referencias

[1] S. R. Blackburn, S. Murphy and K. G. Paterson. *Comments on: Theory and applications of cellular automata in cryptography.* IEEE Trans. Comput. **46**, 5 (1997), 637–639.

[2] K. Cattell, S. Zhang, M. Serra and J. C. Muzio. *2-by-n hybrid cellular automata with regular configuration: theory and application.* IEEE Trans. Comput. **48**, 3 (1999), 285–295.

[3] T. ElGamal. *A public-key cryptosystem and a signature scheme based on discrete logarithm*, IEEE Trans. Inform. Theory **31** (1985), 469–472.

[4] A. Fúster, D. de la Guía, L. Hernández, F. Montoya y J. Muñoz. *Técnicas criptográficas de protección de datos.* RA-MA, 2^a ed., Madrid, 2000.

[5] M. Gardner. *The fantastic combinations of John Conway's new game of 'life'.* Scientific American, Octubre (1970), 100.

[6] J. Gleick. *Caos: La creación de una ciencia.* Seix Barral, Barcelona, 1988.

[7] S. W. Golomb. *Shift register sequences.* Holden-Day, San Francisco, 1967.

[8] D. de la Guía y A. Fúster. *Estudio de autómatas celulares para criptografía.* Actas de la IV Reunión Española de Criptología, 167–174, J. Tena y M. F. Blanco (ed.), Universidad de Valladolid, 1996.

[9] M. W. Hirsch y S. Smale. *Ecuaciones diferenciales, sistemas dinámicos y álgebra lineal.* Alianza Universidad Textos, Madrid, 1983.

[10] E. N. Lorenz. *La esencia del caos.* Debate, Pensamiento, Barcelona, 1995.

[11] W. Meier and O. Staffelbach. *Analysis of pseudo random sequences generated by cellular automata.* Advances in Cryptology-Proceedings of EUROCRYPT'91, LNCS **547** (1991), 186–199, Springer-Verlag, Berlín.

[12] A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of applied cryptography.* CRC Press, Boca Ratón, FL., 1997.

[13] K. Nagel and M. Schreckenber, *A cellular automaton model for freeway traffic.* J. Physique I, **2** (1992), 2221.

[14] S. Nandi, B. K. Karr and P. Pal Chaudhuri. *Theory and applications of cellular automata in cryptography.* IEEE Trans. Comput. **43**, 12 (1994), 1346–1357.

[15] J. von Neumann. *Theory of selft-reproducing automata.* A. W. Burks (ed.), University of Illinois Press, 1966.

[16] D. Ostrov and R. Rucker. *Continuous-valued cellular automata for nonlinear wave equations.* Complex Systems **10** (1996), 91–119.

[17] N. H. Packard and S. Wolfram. *Two-dimensional cellular automata.* J. Statist. Phys. **38** (1985), 901–946.

[18] A. Quirós Gracián. *Números primos y criptografía.* Bol. Soc. Esp. Mat. Apl. **17** (2001), 13–21.

[19] Rijndael: accesible en http://csrc.nist.gov/encryption/aes/

[20] R. L. Rivest, A. Shamir and L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems.* Commun. ACM **21** (1978), 120–126.

[21] R. Schmitz. *Use of chaotic dynamical systems in cryptography.* J. Franklin Inst. **338** (2001), 429–441.

[22] M. Sipper. *The evolution of parallel cellular machine: The cellular programming approach.* Springer-Verlag, Berlin, 1997.

[23] M. Sipper and M. Tomassini. *Generating parallel random number generators by cellular programming.* Internat. J. Modern Phys. C **7**, 2 (1996), 181-190.

[24] —. *Computation in artificially evolved, non-uniform cellular automata.* Theoret. Comput. Sci. **217**, 1 (1999), 81-98.

[25] S. Tezuka and M. Fushimi. *A method of designing cellular automata as pseudorandom number generator for built-in-self-test for VLSI.* Finite fileds: Theory, applications and algorithms, 363–367, Contemp. Math. **168**, Amer. Math. Soc. Providence, RI, 1994.

[26] A. J. Tomeu Hardasmal y R. Ruíz Rentero. *Cifrado de cadenas mediante autómatas celulares.* Actas de la IV Reunión Española de Criptología, 175–182, J. Tena y M. F. Blanco (ed.), Universidad de Valladolid, 1996.

[27] S. Ulam. *On some mathematical problems connected with patterns of growth of figures.* A. W. Burks (ed.), Essays on Cellular Automata, University of Illinois Press, 1970.

[28] S. Wolfram. *Cellular automata.* Los Alamos Science **9** (1983), 2–21.

[29] —. *Universality and complexity in cellular automata.* Physica D **10** (1984), 1–35.

[30] —. *Cryptography with cellular automata.* Advances in Cryptology-Proceedings of CRYPTO'85, LNCS **218** (1986), 429–432, Springer-Verlag, Berlín.

[31] —. *Random sequence generation by cellular automata.* Adv. in Appl. Math. **7** (1986), 123–169.

Bol. Soc. Esp. Mat. Apl. nº 21(2002), 89–115

Sistemas dinámicos estocásticos no autónomos y sistemas multivaluados

J. A. Langa Rosado

Departamento de Ecuaciones Diferenciales y Análisis Numérico,
Universidad de Sevilla

langa@numer.us.es

Resumen

Uno de los conceptos más importantes para la descripción del comportamiento asintótico de ecuaciones en derivadas parciales de evolución disipativas es el de atractor global. Presentamos los trabajos realizados en esta línea para ecuaciones en derivadas parciales estocásticas (presencia de ruidos en alguno de los términos), para inclusiones diferenciales (es decir, en donde la variación de la variable incógnita no verifica una determinada expresión, sino un conjunto de expresiones), para ecuaciones con retardo (modelos que tienen en cuenta en cada instante parte de la dinámica pasada) y para ecuaciones en derivadas parciales no autónomas (es decir, donde los términos que afectan a la incógnita son dependientes del tiempo). Esta diversidad de situaciones nos ha obligado a adentrarnos en disciplinas a veces muy distintas del Análisis Funcional, las funciones multivaluadas o los procesos estocásticos, o teorías como la de la medida o la de la dimensión de conjuntos. En una cantidad importante de los trabajos que resumimos hay una idea motor de fondo que recorre todos ellos: el hecho de poder describir la dinámica infinito dimensional propia de estos modelos con sólo una cantidad finita de grados de libertad.

Palabras clave: *Sistemas dinámicos estocásticos, atractores aleatorios, iclusiones diferenciales*

Clasificación por materias AMS: *60H15, 37L30, 37B55, 49K20*

1 Introducción

1.1 Teoría de atractores globales

No cabe duda de la fuerza y aptitud que las Ecuaciones en Derivadas Parciales (EDPs) tienen a la hora de modelizar fenómenos de distintas disciplinas

Fecha de recepción: 9 de abril de 2002

científicas como la Física, la Química, la Biología, la Economía, la Ingeniería, etc.

Podemos expresar, de manera general, una ecuación en derivadas parciales de evolución autónoma como:

$$\left\{ \begin{array}{rcl} \dfrac{\partial u}{\partial t} & = & F(u), \quad t \geq 0,\ x \in D \subset \mathbb{R}^n \\ u(0,x) & = & u_0(x), \end{array} \right. \tag{1}$$

donde $u = u(t,x)$ es la función a determinar que representa cierta propiedad de determinado fenómeno natural y F indica el conjunto de transformaciones, en general no lineales, que manifiestan la manera en que u cambia cuando el tiempo evoluciona.

Cuando un comportamiento del mundo real puede ser descrito mediante un buen modelo a partir de un sistema de ecuaciones diferenciales, en cierto modo hemos sabido desentrañar las propiedades que describen la dinámica del fenómeno estudiado a partir de un conjunto de ideas e instrumentos matemáticos. Pero el objeto del modelado no es sólo entender el fenómeno, sino mucho más importante, predecir el comportamiento futuro del mismo. En este sentido, una de las preguntas básicas para cualquier modelo en EDPs es aquélla acerca de su comportamiento asintótico, esto es, cuando el tiempo crece y tiende a infinito.

Es común por otra parte que, debido por ejemplo a la fricción, muchos de estos sistemas tengan la propiedad de "perder energía"; desde un punto de vista matemático esta propiedad conduce al concepto de *disipación*. Es decir, las soluciones del sistema permanencen en un acotado fijo para tiempos grandes. En este sentido, todo el comportamiento asintótico de las soluciones se da en un conjunto acotado del *espacio de fases* H ($L^2(\Omega)$, por ejemplo) en donde evolucionan las soluciones, lo que supone una simplificación interesante en la dinámica del modelo (ver Figura 1). Sin embargo, aún este conjunto puede ser significativamente grande.

Hace ya más de tres décadas el concepto de *atractor global* fue introducido para explicar con más precisión el comportamiento asintótico de los sistemas disipativos. Desde entonces, podemos contar por miles los trabajos de investigación que se han centrado en este concepto y variantes del mismo, dando lugar a verdaderas nuevas ramas de la teoría de Sistemas Dinámicos (ver los trabajos de Hale [41], Temam [62], Babin y Vishik [4], Vishik [64], Ladyzhenskaya [44], Robinson [57]).

Dada una solución de un sistema de EDPs autónomo para el cual suponemos existencia y unicidad de soluciones, definimos el correspondiente semigrupo $S(t) : H \to H$, mediante la igualdad $S(t)u_0 = u(t;u_0)$, donde $u(t;u_0)$ es la solución de (1) en el tiempo t que estaba en u_0 para $t = 0$. Un atractor global $\mathcal{A}$ es un conjunto compacto del espacio de fases H, invariante para el semigrupo, i.e. verificando $S(t)\mathcal{A} = \mathcal{A}$ para todo $t \in \mathbb{R}^+$ y que atrae de manera uniforme a todos los acotados $D \subset H$, es decir,

$$\lim_{t \to +\infty} \operatorname{dist}(S(t)D, \mathcal{A}) = 0,$$

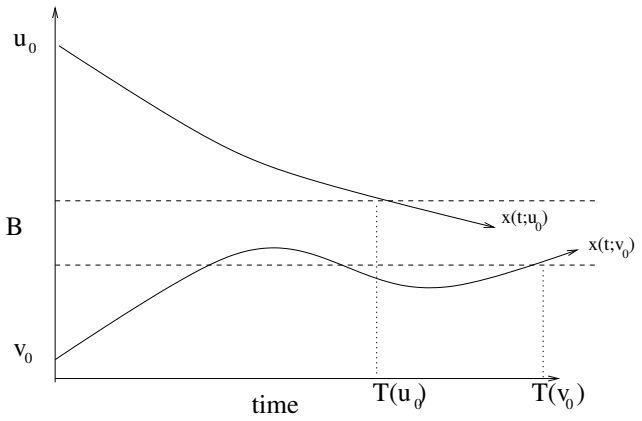


Figura 1: *Conjunto acotado $B \subset \mathbb{R}$ que absorbe soluciones del sistema (1) que comienzan en u_0, v_0.*

con 'dist' la semidistancia de Hausdorff. Cuando determinamos un atractor global para un sistema, estamos precisando dónde se da la dinámica asintótica del mismo, prediciendo así el futuro de los fenómenos asociados.

1.2 Dimensión del atractor global

Sin duda, una de las propiedades más interesantes de los atractores globales para EDPs es que, en muchos casos interesantes (por ejemplo para las ecuaciones de Navier-Stokes), se trata de conjuntos de dimensión fractal (y, por tanto, de dimensión de Hausdorff) finita, es decir,

$$d_f(\mathcal{A}) = \limsup_{\varepsilon \to 0} \frac{log(N_\varepsilon(\mathcal{A}))}{log(1/\varepsilon)} < +\infty.$$

Aquí, $N_\varepsilon(\mathcal{A})$ indica el mínimo número de bolas de radio ε necesarias para recubrir $\mathcal{A}$. Esto significa que, aunque el espacio de fases es un espacio infinito-dimensional, lo que determina el comportamiento asintótico es un conjunto, de extremada complejidad geométrica en algunas ocasiones, pero que puede ser descrito a partir de un número finito de variables. La pregunta que hace ya décadas importantes investigadores se hicieron fue la siguiente: ¿Es cierto que para tiempos grandes los sistemas dinámicos disipativos e infinito-dimensionales tienen únicamente una cantidad finita de grados de libertad? O, mucho mejor, ¿existirán ecuaciones diferenciales ordinarias (EDOs) que describan el comportamiento asintótico de las EDPs disipativas? Estas preguntas han conducido, bajo mi punto de vista, a los resultados más bellos e interesantes en la teoría de sistemas dinámicos en dimensión infinita (ver Foias et al. [38], Robinson [57], Eden et al. [32]). Por otra parte, han motivado buena parte de nuestra investigación hasta el momento.

El interés que posee la descripción con un número finito de grados de libertad la dinámica asintótica de un sistema dado tiene una clara motivación: la posibilidad de usar técnicas y razonamientos propios de las EDOs para el tratamiento de EDPs.

2 Atractores aleatorios

2.1 El concepto de sistema dinámico

Consideremos la siguiente EDPs estocástica

$$\begin{cases} \dfrac{\partial u}{\partial t} &= F(u) + g(u)\dfrac{dW_t}{dt}, \quad t \geq 0,\ x \in D \subset \mathbb{R}^n, \\ u(0,x) &= u_0(x), \end{cases} \tag{2}$$

donde $\frac{dW_t}{dt}$ es la *derivada* temporal de un proceso de Wiener W_t definido en el espacio de probabilidad $(\Omega, \mathcal{F}, P)$ y $g(u) \equiv Cte.$ ó $g(u) \equiv u$ (es decir, estamos en los casos de ruido aditivo o ruido lineal multiplicativo).

Hasta hace pocos años no existían herramientas apropiadas para describir el comportamiento asintótico de EDPs estocásticas en el espacio de fases, es decir, en analogía a lo que ya era bien conocido en el caso determinista. Conceptos como medidas invariantes o atractores de probabilidad eran usados con más o menos éxito (Schmalfuss [60], Morimoto [54]). Por otro lado, en los años ochenta fue desarrollada la teoría de *flujos estocásticos* (Elworthy [33]), que dio lugar en los noventa a la de *sistemas dinámicos aleatorios* (Arnold [1]).

2.2 Nuevos conceptos para el análisis asintótico en tiempo

No fue hasta 1994 cuando se dispuso del marco necesario para poder introducir el concepto de *atractor aleatorio* para ciertas ecuaciones diferenciales estocásticas (véase Crauel y Flandoli [28]; véase también un resumen sobre esta teoría en Caraballo y Langa [15]). Ni siquiera el marco conceptual estaba desarrollado; por otra parte, para generalizar a esta situación el concepto de atractor global determinista hay grandes dificultades. Por un lado, una ecuación diferencial estocástica puede, en ciertas circunstancias, ser interpretada como una ecuación perturbada con términos no autónomos (esto hace necesario definir, en vez de un semigrupo de operadores, una familia biparamétrica de operadores $S(t,s) : H \to H$, $t \geq s$). Por otro lado, la presencia de términos estocásticos (procesos de Wiener en sentido de Ito o de Stratonovich) hace necesario en realidad trabajar con procesos tri-paramétricos $S(t,s,\omega) : H \to H$, donde $\omega \in \Omega$ y $(\Omega, P, \mathcal{F})$, es el espacio de probabilidad asociado. De hecho, existe un grupo de transformaciones $\{\theta_t : \Omega \to \Omega,\ t \in \mathbb{R}\}$ tal que $(t,\omega) \mapsto \theta_t\omega$ es medible, $\theta_0 = \mathrm{id}$, $\theta_{t+s} = \theta_t\theta_s$ y $S(t,s,\omega) = S(t-s, 0, \theta_s\omega)$, para $s,t \in \mathbb{R}$ (ver Crauel et al. [27]).

La familia de operadores $S(t,s,\omega)$ se denomina *sistema dinámico aleatorio* (SDA).

Una nueva dificultad se añade: los sistemas dejan de ser disipativos, en el sentido de que, debido a las fuertes fluctuaciones provocadas por los términos

estocásticos, cabe esperar que la evolución de cualquier solución del sistema se salga de todo conjunto acotado del espacio de fases. Sin embargo, bajo ciertas condiciones, el efecto disipativo ejercido por los términos de difusión permanece presente, aunque más débilmente, como se pone de manifiesto, por ejemplo, en Caraballo et al. [21]. En Crauel y Flandoli [28] se propone la siguiente definición del concepto de atractor global estocástico:

Definición 1 *Un conjunto aleatorio* $\mathcal{A}(\omega)$ *(*$\mathcal{A} : \Omega \to \mathcal{P}(H)$, $\mathcal{P}(H)$ *es el conjunto de las partes de* H*) es el atractor aleatorio asociado al SDA* S *si se tiene* $P-c.s.$ *lo siguiente:*

i) $\mathcal{A}(\omega)$ *es un conjunto aleatorio compacto; es decir,* $\mathcal{A}(\omega)$ *es compacto y para todo* $x \in H$ *la aplicación* $\omega \mapsto dist(x, \mathcal{A}(\omega))$ *es medible,*

ii) $S(t,s,\omega)\mathcal{A}(\theta_s\omega) = \mathcal{A}(\theta_t\omega)\ \forall t \geq 0 \quad (invarianza)$ *y*

iii) para todo $B \subset X$ *acotado*

$$\lim_{s\to+\infty} dist(S(0,-s,\omega)B, \mathcal{A}(\omega)) = 0 \quad \textit{(propiedad de atracción "pullback").}$$

Nota: Para cada $x \in B$, $S(0,-s,\omega)x$ puede interpretarse como la posición en el tiempo final (el *presente*) $t = 0$ de la trayectoria que estaba en x en el instante inicial $-s$ (el *pasado*). Así, la propiedad de atracción se da en relación al comportamiento asintótico de los tiempos iniciales (en el pasado), fijando el tiempo final. Observemos que esta interpretación también es válida para atractores globales clásicos.

El resultado general sobre existencia de atractores aleatorios es el siguiente, debido a Crauel y Flandoli ([28], Teorema 3.11). Se trata de una generalización de los resultados clásicos de existencia de atractor global en el caso determinista autónomo:

"Supongamos que existe $D(\omega)$ *absorbente y compacto, es decir, tal que para todo acotado* $B \subset X$ *existe un tiempo* $T(B,\omega)$ *verificando* $S(0,-s,\omega)B \subset D(\omega)$ *para todo* $s \geq T(B,\omega)$*. Entonces existe un único atractor aleatorio para el SDA* $S(t,s,\omega)$*."*

El mismo concepto de atractor es válido para EDPs no autónomas

$$\frac{\partial}{\partial t} = F(t,u),$$

donde F es, en general, no acotada (Kloeden y Schmalfuss [43]). En efecto, en este caso definimos una familia biparamétrica de *procesos* (Sell [61]) $S(t,s)$. Diremos que la familia de conjuntos compactos $\{\mathcal{A}(t)\}_{t\in\mathbf{R}}$ es el *atractor (global) no autónomo* asociado a S si es invariante, es decir,

$$S(t,s)\mathcal{A}(s) = \mathcal{A}(t), \text{ para todo } t \geq s,$$

y atrae a todos los conjuntos acotados $B \subset H$, esto es

$$\lim_{s\to+\infty} \text{dist}(S(t,-s)B, \mathcal{A}(t)) = 0, \quad \forall t \in \mathbb{R}.$$

Observamos en las Figuras 2 y 3 que los conceptos de invarianza y atracción difieren bastante de los conceptos clásicos para atractores globales de EDPs deterministas y autónomas.

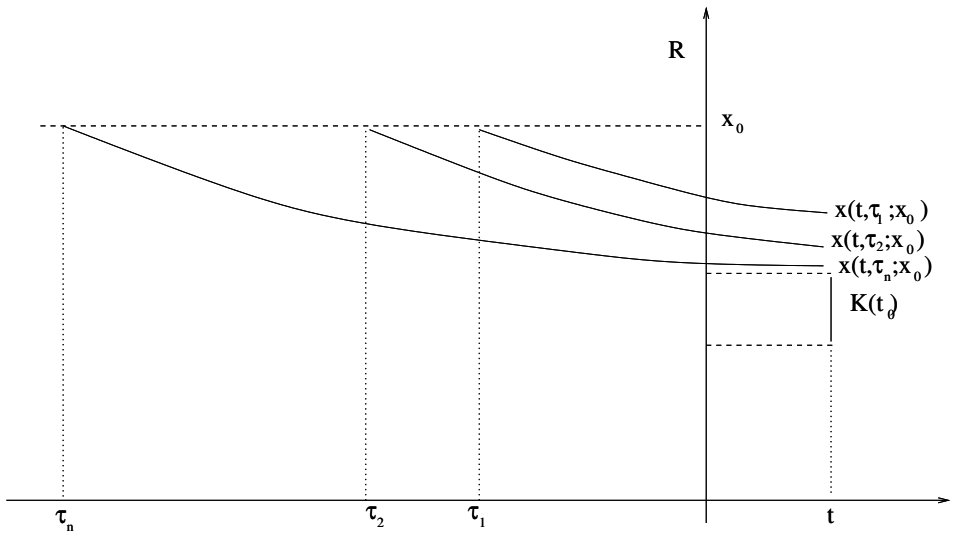


Figura 2: *Atracción "pullback" hacia el conjunto $K(t_0)$ de las trayectorias que comienzan en el punto x_0 en una sucesión de instantes iniciales $\{\tau_n\}$ que tiende a $-\infty$.*

Chepyzhov y Vishik [24] definieron, con otra terminología, un concepto similar de atractor para EDPs no autónomas disipativas.

Para una ecuación a la vez no autónoma -en términos deterministas- y estocástica, es posible definir el marco de sistema dinámico y el concepto de atractor no autónomo y aleatorio $\{A(t,\omega)\}_{t\in\mathbb{R},\omega\in\Omega}$ tal y como aparece en Caraballo y Langa [14].

3 Los resultados sobre semicontinuidad superior

La primera observación que hemos indicado a partir de las definiciones anteriores es que el concepto de atractor difiere sustantivamente del de atractor global para EDPs deterministas y autónomas. En efecto, permitir que la ecuación posea una propiedad de disipatividad sólo si la analizamos asintóticamente respecto de los tiempos iniciales ha hecho que, por un lado, la propiedad de invarianza sea posible si consideramos una familia de compactos que, en general, no tiene por qué estar acotada; por otro lado, también ha hecho que la propiedad de atracción tenga que ser definida con referencia a tiempos iniciales y para tiempos finales fijos. Además, como mencionamos anteriormente, otros conceptos de conjuntos atrayentes para estas ecuaciones habían sido previamente introducidos en la

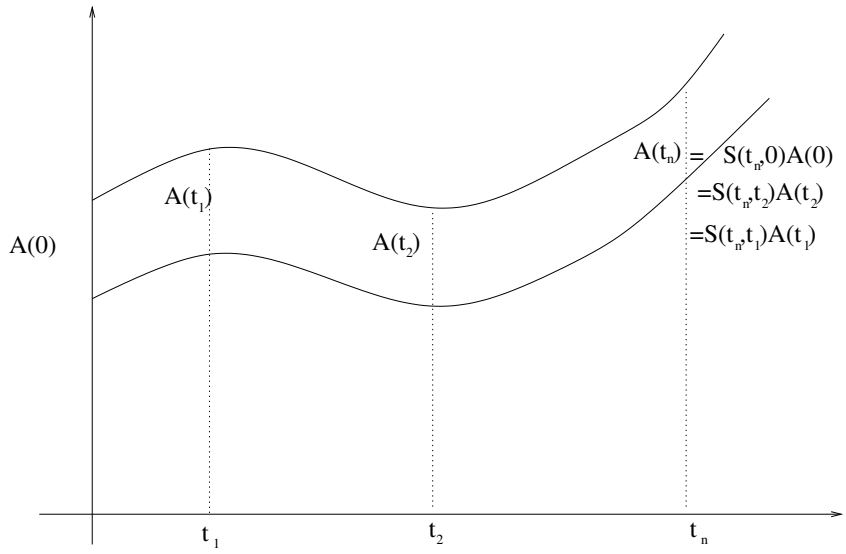


Figura 3: *Propiedad de invarianza del atractor no autónomo* $\mathcal{A}(t)$.

literatura.

Por todo ello, lo primero que quisimos investigar era si las definiciones anteriores eran apropiadas en el sentido de, en el caso de interpretar las ecuaciones estocásticas y/o no autónomas como pequeñas perturbaciones de EDPs disipativas, deterministas y autónomas, era posible obtener resultados de perturbación y convergencia para los atractores asociados. En efecto, en Caraballo et al. [6] y Caraballo y Langa [14] pudimos establecer resultados generales que garantizaban lo siguiente:

Supongamos que tenemos un semigrupo de operadores asociado a una EDP determinista y autónoma $S_0 : \mathbb{R}_+ \times H \to H$ en las condiciones de existencia de atractor global $\mathcal{A}$. Perturbemos el sistema mediante términos no autónomos y estocásticos dependientes de un pequeño parámetro $\sigma \in (0, 1]$, de manera que obtengamos familias de procesos

$$S_\sigma : \mathbb{R} \times \mathbb{R} \times \Omega \times H \to H$$

para los que suponemos que existen conjuntos absorbentes compactos $K_\sigma(t, \omega)$ y, por consiguiente, atractores aleatorios $\mathcal{A}_\sigma(t, \omega)$. Supongamos que se verifica:

$(H1)$ Para todo $\omega \in \Omega$ y todo $t \in \mathbb{R}$,

$$\text{dist}(S_\sigma(t, 0, \omega)x, S_0(t)x) \to 0, \text{ cuando } \sigma \searrow 0$$

uniformemente en los acotados de H.

$(H2)$ Existe un compacto $K \subset H$ tal que

$$\lim_{\sigma \searrow 0} \operatorname{dist}(K_\sigma(t,\omega), K) = 0, \quad \forall \omega \in \Omega,\ \forall t \in \mathbb{R}.$$

Entonces se tiene el siguiente

Teorema 1 *Bajo las condiciones* $(H1)$ *y* $(H2)$

$$\lim_{\sigma \searrow 0} dist(\mathcal{A}_\sigma(t,\omega), \mathcal{A}) = 0, \quad \forall \omega \in \Omega,\ \forall t \in \mathbb{R}.$$

En particular, este resultado garantiza que el concepto de atractor no autónomo y aleatorio es la "buena"generalización para el estudio de propiedades asintóticas de este tipo de EDPs.

Este resultado es de carácter general, y pudo ser aplicado a distintos modelos, como las ecuaciones estocásticas bidimensionales de Navier-Stokes, ecuaciones de reacción-difusión (Caraballo et al. [6]), y ecuaciones diferenciales no autónomas y estocásticas del tipo $du = f(t,u)\,dt + u\,dW_t$ (Caraballo y Langa [14]).

4 Comportamiento asintótico finito-dimensional

4.1 El caso estocástico

Anteriormente nos referimos a que una de las propiedades más interesantes de la teoría de atractores globales era que, en muchos casos, se trataba de conjuntos compactos finito-dimensionales. En el caso estocástico, los mejores resultados acerca de la dimensión finita de atractores aleatorios aparecen en Debussche [31] (ver Flandoli y Langa [34] y Langa [52] para su aplicación a las ecuaciones de Navier-Stokes). En estos trabajos se muestra que, para cada $\omega \in \Omega$, el atractor $\mathcal{A}(\omega)$ posee dimensión fractal finita, siendo ésta uniforme para todos los $\omega \in \Omega$. Por otro lado, puede ocurrir que $\cup_{\omega\in\Omega}\mathcal{A}(\omega)$ sea un conjunto no acotado y, además, que $\dim(\cup_{\omega\in\Omega}\mathcal{A}(\omega)) = +\infty$, donde 'dim' señala la dimensión de Hausdorff o dimensión fractal del conjunto. Es decir, la descripción global del comportamiento asintótico del sistema se hace sobre un conjunto no acotado e infinito-dimensional.

Por otro lado, sí es posible dar resultados que relacionan de manera precisa la dinámica asintótica de los sistemas con la dinámica que podemos observar en los atractores. En efecto, tanto para atractores globales deterministas (Langa y Robinson [46], Langa [48]) como para atractores aleatorios (Caraballo y Langa [7]), es posible demostrar que, para cualquier trayectoria del sistema, existe una sucesión de trayectorias en el atractor que describen la dinámica de la misma con una precisión tan certera como deseemos:

Proposición 2 *Supongamos que el proceso* $S(t,s)$ *satisface, para* $L > 0$, $u_1, u_2 \in H$,

$$|S(t,s)u_1 - S(t,s)u_2| \leq \exp(L(t-s))|u_1 - u_2|. \tag{3}$$

Sean $u_0 \in H$ *y* $\{\varepsilon_n\}$, $\{T_n\}$ *sucesiones positivas con* $\varepsilon_n \searrow 0$ *y* $T_{n+1} - T_n \nearrow +\infty$ *. Entonces existen unos* v_n *con* $\{v_n\}_{n\in\mathbb{N}}$, $v_n \in \mathcal{A}(T_n)$ *para todo* $n \in \mathbb{N}$ *y una sucesión* $\{\tau_n\}_{n\in\mathbb{N}}$ *no creciente, tales que,*

$$\sup_{s\le\tau_n;\ 0\le t\le T_{n+1}-T_n} |S(T_n+t,s)u_0 - S(T_n+t,T_n)v_n| \le \varepsilon_n.$$

Además, los "saltos" entre dos trayectorias consecutivas verifican

$$\lim_{n\to\infty} |S(T_{n+1},T_n)v_n - v_{n+1}| = 0. \tag{4}$$

Por tanto, la pregunta que surge a partir de estos resultados y los de Debussche antes citados es ésta: ¿Pueden dar los atractores aleatorios alguna información sobre la dependencia de un número finito de parámetros del comportamiento asintótico de los sistemas estocásticos? El resultado principal en este contexto, con respuesta afirmativa, aparece en Flandoli y Langa [34] y ha influido en varios trabajos posteriores (Chueshov [25], Chueshov et al. [26], Flandoli y Berselli [5]).

Para ello tuvimos que generalizar al caso estocástico la *propiedad de aplastamiento* (la "squeezing property"), de gran utilidad en el caso determinista (ver Robinson [57]). Consideremos un proyector ortogonal $P_N \equiv P$ de H sobre el subespacio finito-dimensional PH (N denota la dimensión de P). Sea $Q : H \to QH$ el proyector asociado sobre su complemento ortogonal QH, i.e. $Q = I - P$. En las aplicaciones, P denota el proyector ortogonal sobre las N autofunciones de cierto operador lineal (el Laplaciano, por ejemplo). Supongamos (propiedad de aplastamiento) que, asociado al sistema dinámico aleatorio $S(t,s,\omega)$ y al par (P,Q), existen $\delta \in (0,1)$ y una variable aleatoria $c(\omega)$ de esperanza finita tales que, o bien

$$|Q(S(1,0,\omega)u - S(1,0,\omega)v)| \le |P(S(1,0,\omega)u - S(1,0,\omega)v)|,$$

o bien

$$|S(1,0,\omega)u - S(1,0,\omega)v| \le \exp(\int_0^1 c(\theta_s\omega)\,ds)|u-v|,$$

para todo $u, v \in K(\omega)$, con $K(\omega)$ un conjunto absorbente y compacto arbitrario.

Teorema 3 *En estas condiciones, si para* $k > 0$,

$$\lim_{t\to+\infty} e^{kt}|P(S(t,0,\omega)u - S(t,0,\omega)v)| = 0,$$

entonces

$$\lim_{t\to+\infty} e^{(k-E(c(\omega)))t}|S(t,0,\omega)u - S(t,0,\omega)v| = 0.$$

Obsérvese que la propiedad sobre modos determinantes se da tomando límites cuando el tiempo crece hacia $+\infty$, que los datos iniciales han de estar en el conjunto absorbente $K(\omega)$ y que sólo se verifica si suponemos una convergencia exponencial a cero de los primeros modos asociados a las soluciones.

4.2 Modos determinantes para tiempos finales fijos

Como hemos indicado, el resultado precedente dio lugar a otros que han tratado de generalizarlo. En particular, los resultados sobre modos determinantes fueron ampliados al caso de proyecciones determinantes en Berselli y Flandoli [5], Chueshov [25], o Chueshov et al. [26], donde además se trataron de eliminar algunas de las hipótesis particulares que indicamos en el último párrafo de la sección anterior. Sin embargo, en todos estos trabajos quedó abierto el caso de la determinación finita del número de grados de libertad en el sentido "pullback". En Langa [52] aparece este caso resuelto. También ha sido posible eliminar en [52] todas las restricciones que aparecen en trabajos precedentes, en particular la hipótesis acerca de la convergencia exponencial de los primeros modos o de la necesidad de tomar los datos iniciales en el conjunto absorbente. Las ecuaciones estocásticas bidimensionales de Navier-Stokes sirven de modelo para ilustrar estos resultados.

En el caso de una EDP no autónoma y determinista, el concepto de atractor que hemos introducido es más débil aún que el de atractor aleatorio. Esto se debe a que, para un proceso de Wiener, las propiedades de ergodicidad y crecimiento sublineal hacen posible cierto control y homogeneidad en el comportamiento asintótico de las trayectorias. Por ejemplo, la propiedad de atracción de los atractores aleatorios para tiempos iniciales implica una atracción (en probabilidad) "hacia adelante en el tiempo", i.e. para $t \to +\infty$ en $S(t,s,\omega)$ (Crauel y Flandoli [28]). Sin embargo, términos no autónomos, que no procedan de otros estocásticos, pueden hacer que la ecuación tenga un comportamiento asintótico para los tiempos iniciales que no tenga relación alguna para el comportamiento para $t \to +\infty$. En Caraballo et al. [20] pudimos establecer, creemos que por primera vez en la literatura, un resultado de carácter general sobre la dimensión finita de atractores no autónomos para un caso donde la teoría de Chepyzhov y Vishik [24] no podía ser aplicada.

Más precisamente, supongamos que existen $\{K(t)\}_{t\in\mathbb{R}}$ compacto, absorbente y positivamente invariante, es decir, tal que $S(t,s)K(s) \subseteq K(t)$ para $t \geq s$, y existen $k_0, k_1, \theta > 0$ tales que

$$|K(t)|^+ \leq k_0 |t|^\theta + k_1, \ \forall t \in \mathbb{R}, \tag{5}$$

donde $|K(t)|^+ = \sup_{y\in K(t)} |y|$.

Supongamos que para cada $t \in \mathbb{R}$ existe $\delta(t) \in (0,1)$ tal que para $u, v \in K(\tau), \tau \leq t-1$,

$$|Q(S(\tau+1,\tau)u - S(\tau+1,\tau)v)| \leq \delta(t)|u-v|. \tag{6}$$

Teorema 4 *En estas condiciones, la dimensión fractal de $\mathcal{A}(t)$ es finita para cada $t \in \mathbb{R}$.*

Resulta natural plantear a continuación la siguiente pregunta: ¿Podemos, a pesar de la débil propiedad de atracción debida a la escasa disipatividad del sistema, concluir resultados sobre modos determinantes en el sentido de Foias y Prodi en [36]? La respuesta, afirmativa, aparece en el siguiente resultado (cf. Langa [48]):

Teorema 5 *Consideremos $\alpha^1, \alpha^2 : \mathbb{R} \to H$ tales que $\alpha^i(t)$ $(\equiv \alpha_t^i) \in K(t)$ para todo $t \in \mathbb{R}$. Entonces, si existe $\beta \geq 0$ para el cual*

$$\lim_{s \to -\infty} |P(S(t,s)\alpha_s^1 - S(t,s)\alpha_s^2)| \leq \beta, \tag{7}$$

también se tiene

$$\lim_{s \to -\infty} |S(t,s)\alpha_s^1 - S(t,s)\alpha_s^2| \leq \beta. \tag{8}$$

Fijémonos que este resultado muestra que el comportamiento asintótico (respecto a los tiempos iniciales) depende de un número finito de parámetros.

5 Sobre una conjetura de Foias y Temam

En 1984 Foias y Temam ([37]) enunciaron una conjetura en relación a la parametrización del atractor global para las ecuaciones de Navier-Stokes a partir de un número finito de elementos en el dominio espacial. La conjetura ha sido resuelta recientemente por Friz y Robinson [39] para el caso determinista autónomo. En Langa y Robinson [47] pudimos extender los resultados al caso de los atractores para las siguientes ecuaciones bidimensionales de Navier-Stokes no autónomas:

$$\begin{cases} dX = [\nu \Delta X - \langle X, \nabla \rangle X + f(t) + \nabla p]dt + g(t,X)dW(t) \\ divX = 0 \text{ en } [0,\infty) \times D, \\ X = 0 \text{ sobre } [0,\infty) \times \Gamma, \\ X(0,x) = X_0(x), \quad x \in D, \end{cases}$$

donde $f \in C_b^0(\mathbb{R}^+, H)$, es decir, f es continua y acotada. El resultado es el siguiente:

Teorema 6 *Supongamos que las soluciones en el atractor no autónomo $\mathcal{A}(t)$ son uniformemente acotadas en el conjunto de funciones analíticas. Entonces, para $k > 0$ suficientemente grande, casi cualquier elección de k puntos $(x_1, \ldots, x_k)$ en el dominio $D \subset \mathbb{R}^m$ en el que toman valores las soluciones hace inyectiva a la aplicación*

$$\begin{aligned} E &: H \to \mathbb{R}^{nk} \\ u &\mapsto (u(x_1), \ldots, u(x_k)) \end{aligned}$$

en $\cup_{t \in \mathbb{R}} A(t)$. Además, para cada $I \subset R$ compacto esta aplicación es un homeomorfismo (y, por tanto, proporciona una parametrización) de $\cup_{t \in I} A(t)$ en su imagen.

A partir de este teorema, que también puede ser probado en el caso de atractores aleatorios (ver [47]), los resultados clásicos sobre nodos determinantes (Foias y Temam [37]) son ahora sólo un corolario.

Dicho resultado, para el caso de atractores aleatorios, ha sido también utilizado en Langa [52] para mejorar los resultados sobre modos determinantes "desde $-\infty$".

6 Ito versus Stratonovich en el análisis de la estabilidad de EDPs estocásticas

Existe un gran cantidad de trabajos en torno a la teoría de estabilidad de EDPs estocásticas. En ellos podemos hacer una clara clasificación entre aquellos resultados "en primera aproximación", es decir, aquéllos para los que, dada una EDP determinista, se caracterizan las perturbaciones con términos estocásticos que mantienen la estabilidad del sistema; y, por otro lado, resultados de estabilización mediante ruidos de EDPs deterministas.

En Caraballo y Langa [8] se hace un estudio acerca de la estabilización por ruidos de tipo Ito y Stratonovich para EDPs estocásticas.

Consideremos el problema de Cauchy asociado a una ecuación de evolución lineal

$$\begin{cases} \dfrac{du(t)}{dt} = Au(t) \\ u(0) = u_0 \in H. \end{cases} \tag{9}$$

Consideremos a continuación las ecuaciones estocásticas asociadas a (9), con las dos posibles interpretaciones de la integral, de tipos Stratonovich e Ito respectivamente:

$$\begin{cases} du(t) = Au(t)dt + Bu(t) \circ dW_t \\ u(0) = u_0 \in H, \end{cases} \tag{10}$$

$$\begin{cases} du(t) = Au(t)dt + Bu(t)dW_t \\ u(0) = u_0 \in H, \end{cases} \tag{11}$$

donde de nuevo B es un operador lineal que conmuta con A.

La conclusión del análisis realizado en [8] es la siguiente: hay estabilización de EDPs deterministas cuando las ecuaciones se intrepretan en el sentido de la integral de Ito, pero no en general cuando la integral considerada es de tipo Stratonovich. Observemos que hay una amplia literatura, no sólo en Matemáticas, sino también, por ejemplo, en Física, acerca de la conveniencia de elección de una u otra integral estocástica. En el estudio antes citado intentamos escribir una serie de resultados que arrojaran cierta luz sobre esta cuestión. En realidad, a partir de la integral de Ito podemos escribir resultados de estabilización del correspondiente modelo determinista, de desestabilización, o simplemente de equivalencia respecto al comportamiento asintótico entre ambas.

Un siguiente paso en esta línea de la teoría de la estabilidad para EDPs estocásticas fue enfrentarnos a las ecuaciones de Navier-Stokes. En efecto, en Caraballo et al. [16] tratamos diversos aspectos en relación a la estabilidad de las siguientes ecuaciones bidimensionales de tipo Navier-Stokes

$$\begin{cases} dX = [\nu\Delta X - \langle X, \nabla\rangle X + f(X) + \nabla p]dt + g(t,X)dW(t) \\ divX = 0 \text{ en } [0,\infty)\times D, \\ X = 0 \text{ sobre } [0,\infty)\times\Gamma, \\ X(0,x) = X_0(x), \ \ x \in D, \end{cases}$$

con D dominio de $\mathbb{R}^2$ con frontera Γ y $g(t,x)dW(t)$ el término estocástico, con $W(t)$ un proceso de Wiener infinito-dimensional. Este modelo puede ser reescrito en versión abstracta, con una adecuada elección de espacios y operadores (cf. Caraballo et al. [16] para los detalles y notación) de la siguiente forma:

$$dX(t) = [-\nu AX(t) - B(X(t)) + f(X(t))]\,dt + g(t, X(t))dw(t), \tag{12}$$

donde $f : V \to V'$, $g : [0,\infty) \times V \to \mathcal{L}(K,H)$ son funciones continuas que verifican condiciones adicionales, siendo H la adherencia de $\left\{u \in C_0^\infty(D,\mathbb{R}^2) : div\ u = 0\right\}$ en $L^2(D,\mathbb{R}^2)$ con la norma L^2 habitual y V la adherencia de $\left\{u \in C_0^\infty(D,\mathbb{R}^2) : div\ u = 0\right\}$ en $H^1(D,\mathbb{R}^2)$ con la norma H^1 habitual. V' es el dual de V. También consideramos la versión determinista de este problema,

$$dX(t) = [-\nu AX(t) - B(X(t)) + f(X(t))]\,dt. \tag{13}$$

Tras dar la definición de solución variacional, efectuamos un estudio sobre la estabilidad exponencial de las soluciones de (12). Por ejemplo, probamos el siguiente resultado:

Teorema 7 *Supongamos que se verifican las siguientes condiciones:*

Condición A: *Existe* $\eta > 0$ *tal que*

$$\| f(u) - f(v) \|_{V'} \leq \eta \| u - v \|, u, v \in V;$$

Condición B: *La función* g *satisface* $\| g(t,u) \|_2^2 \leq \gamma(t) + (\xi + \delta(t)) \mid u - u_\infty \mid^2$, *donde* $\xi > 0$ *es una constante y* γ y δ *son funciones integrables no negativas tales que existen* $\theta > 0$,*y* $M_\gamma,\ M_\delta \geq 1$, *con*

$$\gamma(t) \leq M_\gamma e^{-\theta t}, \quad \delta(t) \leq M_\delta e^{-\theta t}, \quad \forall t \geq 0,$$

y $u_\infty \in V$ *es la única solución estacionaria de la ecuación (13) (lo cual es cierto para valores grandes de la viscosidad* ν*). Supongamos además que*

$$2\nu > \lambda_1^{-1}\xi + 2\eta + \frac{2c_1}{\sqrt{\lambda_1}} \| u_\infty \| .$$

Entonces cualquier solución X *de (12) converge a la solución estacionaria* u_∞ *exponencialmente en media cuadrática. Es decir, existen* $a \in (0,\theta)$ y $M_0 = M_0(X(0)) > 0$ *tales que*

$$E \mid X(t) - u_\infty \mid^2 \leq M_0 e^{-at}, \quad \forall t \geq 0.$$

De hecho, también se puede probar que la convergencia se verifica $P - c.s.$

A continuación, abordamos el problema de la estabilización mediante ruidos, así como una amplia discusión acerca de la estabilización en sentido Ito y Stratonovich.

7 Sistemas dinámicos aleatorios multivaluados

7.1 Flujo estocástico multivaluado

Hace unos años pudimos contribuir al desarrollo de una teoría en la que aún hoy continuamos trabajando con asiduidad. La cuestión que nos planteamos inicialmente fue la siguiente: ¿cuál es el concepto de atractor global apropiado para modelos estocásticos con funciones multivaluadas? Consideremos la siguiente inclusión diferencial

$$\begin{cases} \dfrac{du}{dt} \in Au\,(t) + F\,(u\,(t)) + \displaystyle\sum_{i=1}^{m} \phi_i \frac{dW_i\,(t)}{dt},\ t \in (0,T)\,, \\ u\,(0) = u_0, \end{cases} \tag{14}$$

con $A : D\,(A) \subset H \to H$ un operador lineal m-disipativo de dominio $D(A)$, los $\phi_i \in D\,(A)$ y los $W_i\,(t)$ procesos de Wiener independientes.

Se supone que $F : H \to C_v(H)$ es multivaluada, con $C_v(H)$ la familia de subconjuntos de H no vacíos, convexos, cerrados y acotados, con

$$\mathrm{dist}_H(F(y_1), F(y_2)) \leq C\,\|y_1 - y_2\|\,, \quad \forall y_1, y_2 \in H,$$

donde $dist_H(\cdot,\cdot)$ denota la métrica de Hausdorff sobre conjuntos acotados, i.e.

$$\mathrm{dist}_H(A,B) = \mathrm{máx}\{\mathrm{dist}(A,B), \mathrm{dist}(B,A)\}.$$

El problema, sin embargo, requería de un paso previo para el que no existían resultados conocidos en la literatura: ¿cómo definir un flujo, i.e., un sistema dinámico, estocástico multivaluado? Partiendo de la teoría de sistemas dinámicos aleatorios en Arnold [1] y de la de flujos (deterministas) multivaluados en Melnik y Valero [53], pudimos dar la siguiente definición:

Definición 2 *Una aplicación multivaluada $G : \mathbb{R}^+ \times \Omega \times H \to C(H)$ ($C(H)$ denota la familia de los conjuntos cerrados de H) se denomina sistema dinámico aleatorio multivaluado si es medible (en el sentido de Aubin y Frankowska [3]) y satisface*

i) $G(0,\omega) = Id$ *en* H;

ii) $G(t+s,\omega)x = G(t,\theta_s\omega)G(s,\omega)x \quad \forall\ t,s \in \mathbb{R}^+, x \in X,\ \mathbb{P}-c.s.$ (propiedad del cociclo)

En las aplicaciones, es concretamente la medibilidad de esta aplicación lo que resulta difícil de probar. En efecto, no es en absoluto inmediato que diversos modelos estocásticos multivaluados definan un sistema dinámico con estas propiedades. No obstante, pudimos probar en Caraballo et al. [9] que la inclusión diferencial (14) genera un flujo estocástico multivaluado, y que lo mismo le ocurre cuando el ruido es de tipo multiplicativo (Caraballo et al. [10]). Además, quedó probada la equivalencia entre los flujos estocásticos multivaluados así definidos y las correspondientes soluciones para este tipo de modelos que ya eran previamente conocidas en la literatura (ver Caraballo et al. [22]).

7.2 Atractores globales aleatorios

De esta manera, es posible describir el marco donde la teoría de atractores para este tipo de problemas va a ser desarrollada. En efecto, en los trabajos anteriormente citados, basados en la definición de atractor aleatorio para el caso univaluado, desarrollamos la teoría análoga para EDP, ahora en el caso de la inclusiones diferenciales en dimensión infinita. En particular, ilustramos los resultados a partir de diferentes inclusiones diferenciales del tipo (14). Las dificultades técnicas y conceptos distintos a los que hay que hacer frente en este contexto hacen que los trabajos anteriores requieran una cierta complicación técnica.

Finalmente, en Caraballo et al. [12] demostramos diversos resultados de semicontinuidad superior de los atractores para inclusiones estocásticas al atractor proveniente de inclusiones deterministas, tal y como se define en Melnik y Valero [53] (lo cual parece indicar que éste es el concepto apropiado de atractor) . De nuevo, merece la pena destacar las muchas dificultades técnicas a superar para la obtención de los resultados anteriores.

7.3 Inclusiones diferenciales no autónomas y estocásticas

Una etapa más se da en Caraballo et al. [19], donde pudimos escribir con máxima generalidad resultados sobre atractores globales válidos al mismo tiempo para inclusiones diferenciales con términos deterministas no autónomos y términos estocásticos. En concreto, probamos la existencia de atractor global para la siguiente inclusión diferencial:

$$\begin{cases} \dfrac{\partial u}{\partial t} - \Delta u \in f\left(t,u\right) + g_1\left(t\right) + g_2\left(t\right) + \displaystyle\sum_{i=1}^{m} \phi_i \frac{dw_i\left(t\right)}{dt}, \text{ en } D \times \left(\tau, T\right), \\ u\mid_{\partial D} = 0, \\ u\mid_{t=\tau} = u_\tau, \end{cases} \tag{15}$$

con $\tau \in \mathbb{R}$, $D \subset \mathbb{R}^n$ un abierto acotado de frontera suficientemente regular, las ∂D, $\phi_i \in D(\Delta) = H^2(\Omega) \bigcap H_0^1(\Omega)$, $f : \mathbb{R} \times \mathbb{R} \to C_v\left(\mathbb{R}\right)$, $g_1 \in L^\infty\left(\mathbb{R}, L^2\left(D\right)\right)$ y $g_2 \in L^2_{loc}\left(\mathbb{R}, L^2\left(D\right)\right)$. Bajo ciertas condiciones de Lipschitz-continuidad para f y de crecimiento polinomial en t para g_2, se puede definir el marco apropiado (denominado *proceso dinámico multivaluado*) en el que probar la existencia de atractor global para este problema. Este contexto engloba las teorías anteriormente desarrolladas.

8 Atractores para ecuaciones con retardo

Los principales trabajos de existencia de atractores para ecuaciones diferenciales con retardo son debidos a Hale (ver [41] para una lista de las principales referencias). En todos estos trabajos, cuando se trata del caso no autónomo, sólo se permiten condiciones de periodicidad o quasi-periodicidad a los téminos

dependientes del tiempo. En Caraballo et al. [17] pudimos generalizar este concepto al caso de ecuaciones diferenciales con términos no autónomos de carácter general. En concreto, definimos y probamos la existencia de atractores para

$$\begin{cases} \dot{x}(t) &= f(t, x_t) \\ x_s &= \psi, \quad \psi \in C^0([-h, 0]; \mathbb{R}^n), \end{cases}$$

con

$$| f(t, \psi_1) - f(t, \psi_2) | \leq \gamma_1(t) \|\psi_1 - \psi_2\|_{C^0([-h,0];\mathbb{R}^n)},$$

$$\langle f(t, \psi), \psi(0) \rangle \leq (-\alpha + \gamma_1(t)) \mid \psi(0) \mid^2 + \gamma_2(t),$$

bajo la hipótesis de que, para cada $\varepsilon > 0$,

$$\int_{-\infty}^{t} \gamma_1(s) ds < \infty, \qquad \int_{-\infty}^{t} e^{\varepsilon s} \gamma_2(s) ds < \infty.$$

Para ello, nos basamos en el concepto de atractor no autónomo previamente introducido y, a partir de él, pudimos avanzar en la teoría de atractores para ecuaciones con retardo que, como hemos comentado, llevaba muchos años sin poder ser tratada. Los resultados que también probamos de semicontinuidad superior para este atractor hacia el definido por Hale en [41] parecen confirmar que la generalización propuesta en [17] es acertada.

9 Estudio de fenómenos de bifurcación

Recientemente, hemos comenzado a trabajar en una nueva línea de investigación cuyo campo de trabajo permanece en la actualidad prácticamente abierto en casi todas sus vertientes.

Es conocido que, en general, un atractor global puede tener subconjuntos, suficientemente grandes, que no sólo no atraen, sino que repelen las soluciones de una cierta ecuación diferencial. En este sentido, el atractor global es un conjunto "demasiado grande" si queremos "afinar" la dinámica asintótica de ciertos sistemas. Esto justifica resultados de seguimiento de trayectorias sobre otras en el atractor tal y como aparecen en Langa y Robinson [46] y Caraballo y Langa [7], que indican cómo la dinámica en los atractores está relacionada con la dinámica asintótica global de los sistemas diferenciales. Pero aún podemos dar un paso más: si somos capaces de describir la estructura geométrica de los atractores e interpretar en estos términos el comportamiento asintótico de las trayectorias, probablemente sabremos más sobre cómo es realmente el comportamiento asintótico de las ecuaciones. En el caso de EDOs, este problema ha dado lugar a centenares de trabajos que en muchas ocasiones están relacionados con el análisis de fenómenos de bifurcación. Menos numerosos son estos resultados acerca de la estructura de atractores globales deterministas en el caso de EDPs. En el marco estocástico, no existe todavía una teoría general para describir la estructura de los atractores aleatorios, ni siquiera en el caso finito-dimensional. En lo que a bifurcación se refiere lo único que puede hallarse

en la literatura son ejemplos que apuntan a conceptos que empiezan a ser concretados (ver Arnold [1], Capítulo 9, para una discusión amplia sobre estos problemas para EDOs estocásticas).

En el caso de dimensión infinita no conocíamos resultados, ni siquiera en ejemplos concretos, acerca de bifurcación estocástica. Por todo ello es por lo que encontramos especialmente sugerente adentrarnos en este campo de investigación.

9.1 Bifurcación estocástica de tipo "pitchfork"

En Caraballo et al. [18] describimos la bifurcación de tipo "pitchfork" (o de tipo *tenedor*) que se produce en la siguiente EDP estocástica con ruido multiplicativo

$$du = (\Delta u + \beta u - u^3)\, dt + \sigma u \circ dW_t,$$

es decir, estamos ante la ecuación de Chafee-Infante con ruido lineal multiplicativo.

En efecto, en Caraballo et al. [13] pudimos expresar cotas superiores precisas (generalizando las mejores cotas que se conocen en el caso determinista $\sigma = 0$) para la dimensión de los atractores aleatorios $\mathcal{A}(\omega)$ asociados a esta ecuación. En [18] dimos un resultado sobre acotación inferior para la dimensión de estos mismos atractores, probando que existían variedades inestables aleatorias contenidas en el atractor. Además, puesto que el cono de soluciones positivas y negativas son conjuntos invariantes, gracias al principio del máximo estocástico, demostramos que, en el caso unidimensional, estas variedades se movían, en un entorno del origen, precisamente en estos conos.

De esta manera, pudimos dar una información precisa de la estructura interna de los conjuntos $\mathcal{A}(\omega)$. A continuación, estudiamos cómo esta estructura cambiaba drásticamente cuando el parámetro β pasaba de ser menor a ser mayor que el primer autovalor del problema de Dirichlet asociado al operador $A = -\Delta$, mostrando que lo que se tiene es, como en el caso determinista, una bifurcación de dos nuevas ramas de conjuntos invariantes y globalmente asintóticamente estables, mientras que el cero pasa a convertirse en un punto inestable (hubo que definir apropiadamente los conceptos de estabilidad e inestabilidad para conjuntos aleatorios invariantes. Además, los resultados son independientes de la intensidad del parámetro σ en el término del ruido. A partir de la teoría de sistemas dinámicos aleatorios que conservan el orden (Arnold y Chueshov [2]), se puede probar además que, en el caso unidimensional, existen puntos fijos aleatorios que bifurcan desde la solución nula. Es decir, la situación es totalmente análoga a la observada en el caso determinista (ver Hale [41]) y que se describe como una bifurcación de tipo "pitchfork". Hasta el momento no conocemos un resultado general de estas características, pues ni siquiera el concepto de variedad invariante asociada a una solución estacionaria está claramente definido y, por tanto, no existen métodos para probar su existencia. En efecto, para la prueba de este resultado tuvimos que generalizar al caso estocástico una de las pruebas clásicas en el campo determinista para la existencia de *variedades inerciales* (Foias et al. [38]).

9.2 Conceptos de bifurcación para ecuaciones diferenciales no autónomas

De la misma manera que el problema de la estructura de atractores aleatorios está abierto, el problema análogo para atractores no autónomos estaba también prácticamente intacto en el caso de términos dependientes del tiempo generales. Por ejemplo, nada se sabía sobre los fenómenos de bifurcación para ecuaciones del tipo

$$\dot{u} = \lambda u - b(t)u^3,$$

con $b(t) > 0$ y $\lim_{t\to+\infty} b(t) = 0$. En Caraballo y Langa [14] escribimos, para el caso estocástico, un ejemplo de bifurcación de tipo "pitchfork", muy relacionado con la ecuación anterior.

En Langa et al. [49] introdujimos los conceptos básicos que, en nuestra opinión, deben servir de base para una teoría de bifurcación para ecuaciones diferenciales no autónomas del tipo

$$\begin{cases} \dfrac{dx(t)}{dt} = F(\lambda, t, x(t)) \\ x(s) = x_0, \end{cases} \tag{16}$$

con $\lambda \in \mathbb{R}$, $x_0 \in H$.

Para ello se define el concepto de trajectoria completa $x(\cdot)$, con $S(t,s)x(s) = x(t)$, para todo $t \geq s$, que no es más que una concreción de la idea de invarianza de un conjunto dependiente del tiempo. La idea central de un fenómeno de bifurcación en este caso será investigar los valores del parámetro λ para los que se da un cambio cualitativo en la estructura de los conjuntos con propiedades asintóticas relevantes. Sin embargo, del concepto de atractor no autónomo sólo podemos deducir lo que significa la estabilidad asintótica en el sentido "pullback", es decir, una trayectoria completa se dice asintóticamente estable si satisface una propiedad de atracción como la del atractor no autónomo. Es por ello que se introducen las definiciones sobre atracción, estabilidad e inestabilidad local, global y asintótica relativa a conjuntos invariantes.

Todos estos nuevos conceptos son a continuación ilustrados en diversos ejemplos, de manera que podamos, como mínimo, generalizar los ejemplos clásicos de bifurcación:

a) Bifurcación de tipo "pitchfork", para la ecuación

$$\dot{u} = \lambda u - b(t)u^3,$$

con $b(t) > 0$ y $\lim_{t\to+\infty} b(t) = 0$.

b) Bifurcación de Hopf, para

$$\begin{cases} x' = \alpha x - \beta y - h(t)(x^2 + y^2)x \\ y' = \beta x + \alpha y - h(t)(x^2 + y^2)y \\ x(s) = x_0; \quad y(s) = y_0, \end{cases}$$

con $h(t) > 0$, $\lim_{t\to+\infty} h(t) = 0$, $\int_{-\infty}^{t} h(\tau)e^{2\alpha\tau}d\tau < +\infty$, $\alpha, \beta \in \mathbb{R}$, para todo $t \in \mathbb{R}$.

c) Bifurcación de atractores a partir de la solución nula, para $u \in \mathbb{R}^m$ y

$$\dot{u} = \hat{A}u + F(u,t),$$

donde

- $\hat{A}$ es una matriz real de orden $m \times m$ y del tipo

$$\hat{A} = \begin{pmatrix} \lambda & 0 \\ 0 & -A \end{pmatrix},$$

con A de orden $(m-1)\times(m-1)$ verificando

$$y^T Ay \geq \mu|y|^2 \quad y \in \mathbb{R}^{m-1},$$

- $F(0,t) = 0$ para todo $t \in \mathbb{R}$, y, para $p > 0$,

$$|F(u,t) - F(v,t)| \leq a(t)[|u|^{2p} + |v|^{2p}]|u - v|,$$

donde, para cada $t \in \mathbb{R}$

$$\sup_{s\in(-\infty,t]} a(s) = \alpha(t) < \infty.$$

d) Bifurcación de tipo punto de silla (cf. Glendinning [40]), para la ecuación

$$\dot{x} = a - b(t)x^2$$

con $0 < b(t) \leq B$, $b(t) \to 0$ cuando $|t| \to \infty$, y $\int_{-\infty}^{0} b(s)ds = \int_{0}^{\infty} b(s)ds = \infty$.

9.3 El sistema de Lotka-Volterra

Para el caso de un sistema de ecuaciones diferenciales también quisimos aplicar estos nuevos conceptos de bifurcación. De esta manera, estudiamos el caso del sistema de Lotka-Volterra (Langa et al. [51]):

$$\left\{ \begin{array}{rcl} \dot{u} & = & u(\lambda - a(t)u - bv) \\ \dot{v} & = & v(\mu - cv - du) \end{array} \right. \tag{17}$$

con λ, μ como indicadores de la tasa de crecimiento y $a(t), c, b, d > 0$, midiendo, respectivamente, los dos primeros la limitación del medio y los dos últimos el nivel de competición frente a los recursos naturales. Suponemos $0 < a(t) < A$; $u = u(t), v = v(t)$ representan el número relativo de individuos de las poblaciones u, v, que en este caso están en competición en un mismo "hábitat". Al imponer que $a(t) \to 0$ cuando $t \to +\infty$, todos los resultados anteriores sobre

comportamiento asintótico (hoy clásicos) para este modelo de poblaciones no daban información sobre nuestro caso.

Observemos que tenemos ahora dos parámetros λ, μ cuyos valores pueden producir fenómenos de cambio de estabilidad y estructura de los conjuntos invariantes. Pudimos probar que, con los nuevos conceptos introducidos, existe una analogía completa con el caso autónomo; ver, por ejemplo, la Figura 4, donde, en el caso $db < cA$, $U(t), V(t)$ y $\alpha(t;a)$ representan soluciones de (17) que generalizan a las correspondientes soluciones estacionarias globalmente asintóticamente estables del caso estacionario (ver Murray [55]). Para el caso

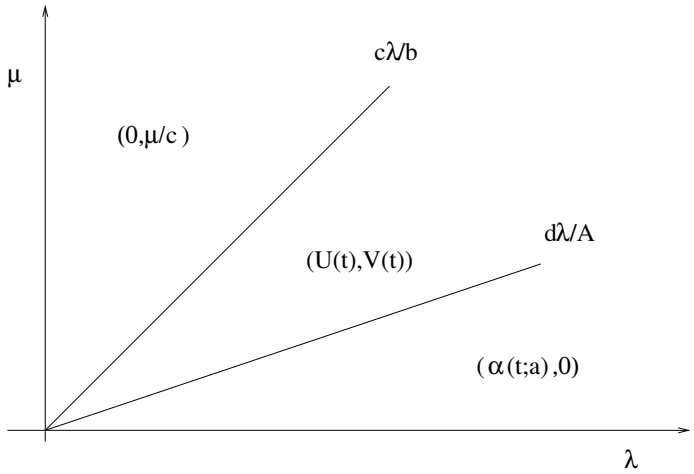


Figura 4: *Comportamiento asintótico global del problema (17) dependiente de los parámetros λ y μ, con $Ac > bd$. Para $\lambda, \mu > 0$ obtenemos tres regiones diferentes para este comportamiento; hemos escrito las trayectorias completas globalmente asintóticamente atrayentes en cada una de estas regiones.*

$db > cA$, y a partir de la teoría de ecuaciones asintóticamente autónomas en Thieme [63], generalizamos el concepto de *curva separatriz* para el caso no autónomo. De nuevo conseguimos de esta manera un comportamiento comparable al que se da en el caso determinista autónomo.

10 Sobre el concepto de permanencia para EDPs no autónomas

En el contexto de las Ecuaciones Diferenciales, el concepto de *permanencia* aparece normalmente asociado a modelos procedentes de la dinámica de poblaciones. Básicamente, indica si, en el futuro, determinada especie o conjuntos de especies, continúa existiendo. En términos matemáticos, esto significa que existe un conjunto absorbente acotado para todos los datos iniciales positivos estrictamente alejado de la solución nula para todo tiempo

suficientemente grande. La cota para este conjunto que define la permanecia del sistema es por tanto, inferior y superior. Sin embargo, sabemos que, para una ecuación no autónoma, no es esperable encontrar cotas superiores uniformes para los conjuntos absorbentes.

10.1 Permanencia en sentido *pullback*

El primer problema que nos planteamos fue, por tanto, analizar si existía alguna manera de desarrollar el concepto de permanencia en EDPs no autónomas. Para ello, en Langa y Suárez [45] investigamos una de las EDPs más simples:

$$u_t - \Delta u = \lambda u - b(t)u^3,$$

con $b(t) > 0$ y $\lim_{t\to+\infty} b(t) = 0$, pero imponiendo condiciones de manera que los numerosos resultados conocidos acerca del comportamiento asintótico de esta ecuación no pudieran ser utilizados. En efecto, probamos que cualquier solución es no acotada cuando $t \to +\infty$. Es decir, no es posible dar resultados de permanencia para esta ecuación. Sin embargo, e inspirados por la teoría de atractores no autónomos, propusimos en [45] la siguiente definición:

Definición 3 *Diremos que un sistema tiene la propiedad de permanencia en sentido "pullback" si existe una familia de conjuntos dependientes del tiempo $U : \mathbb{R} \longmapsto H$, verificando que*

1. *$U(t)$ es un conjunto absorbente (en el sentido "pullback"),*
2. *$d(U(t), \{0\}) > 0$ para todo $t \in \mathbb{R}$,*

donde $d(A, b) = \inf_{a\in A} d(a, b)$.

A continuación, probamos que para la ecuación anterior existe un conjunto con estas características. Este resultado puede ser visto también desde la teoría de bifurcación para ecuaciones no autónomas. En efecto, quizás el punto más importante en este trabajo consiste en demostrar que la solución nula, a partir del primer autovalor λ_1 del Laplaciano, pasa a ser inestable, transfiriendo la estabilidad asintótica que gozaba hasta ese valor a dos nuevas trayectorias completas que se mueven en el cono de soluciones positivas y negativas respectivamente. De esta forma, en λ_1 se produce una bifurcación desde la solución nula hacia nuevos conjuntos invariantes. Para probar que éste es el fenómeno que se observa, tuvimos que generalizar a este caso de EDPs no autónomas la teoría de sistemas estocásticos *que preservan el orden* en Arnold y Chueshov [2].

10.2 El caso de un sistema de EDPs

Para el caso de un sistema de EDPs el problema de la permanencia se complica en varios aspectos. En Langa et al. [50], estudiamos el problema de la permanencia para el siguiente sistema de tipo Lotka-Volterra:

$$\begin{cases} u_t - \Delta u = u(\lambda - a(t)u - bv) & \text{en } D \times (s, +\infty), \\ v_t - \Delta v = v(\mu - cv - du) & \text{en } D \times (s, +\infty), \\ u = v = 0 & \text{sobre } \partial D \times (s, +\infty), \\ u(s,x) = u_0(x), \quad v(s,x) = v_0(x) & \text{en } D, \end{cases} \tag{18}$$

donde D es un dominio acotado en $\mathbb{R}^N$, $N \geq 1$, con frontera regular $\partial\Omega$, b, c, d son constantes positivas, $\lambda, \mu \in \mathbb{R}$ y $0 < a(t) \leq A$. De nuevo la pregunta que nos hacemos es determinar si las dos especies sobrevivirán en el futuro.

Si imponemos que $a(t) \to 0$ cuando $t \to +\infty$, una vez más no es posible aplicar los resultados conocidos sobre permanencia para este sistema. En efecto, probamos en primer lugar que, para ciertos valores de los parámetros λ, μ, una de las especies se va a infinito, lo que produce extinción en la otra. Por ello, usamos el concepto de la permanencia en sentido "pullback" para dar nueva información acerca del comportamiento asintótico del sistema. En este sentido, de nuevo encontramos una situación análoga a la del caso autónomo, es decir, existen curvas $\lambda = \phi(\mu)$ y $\mu = \varphi(\lambda)$ tales que delimitan regiones de permanencia y extinción para las especies (ver Figura 5). El estudio de la ecuación logística

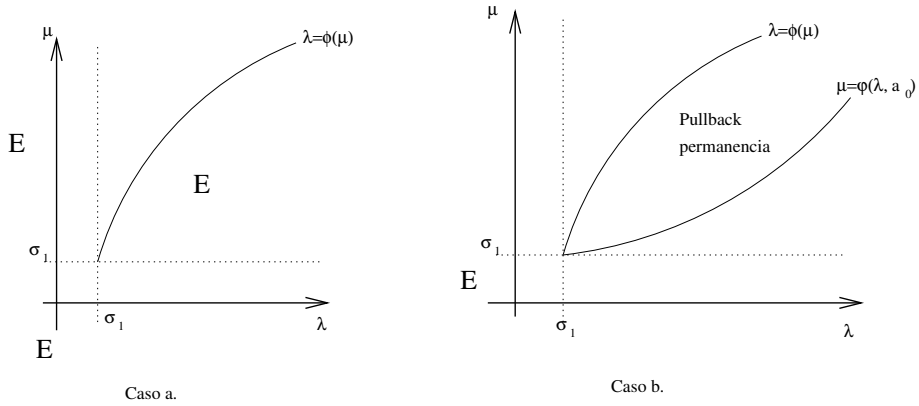


Figura 5: *Caso a. Extinción de una de las especies cuando $t \to +\infty$. Caso b. E: Regiones de permanencia en el sentido pullback y extinción para tiempos iniciales tendiendo a $-\infty$.*

que desarrollamos en [45] juega un papel fundamental. Igualmente, fue necesario concretar para esta situación la teoría de sistemas *que preservan el orden* y la de sub y supersoluciones para EDPs no autónomas.

Referencias

[1] L. Arnold, "Random dynamical systems", Springer Monographs in Mathematics, Springer, Berlin 1998.

[2] L. Arnold, I. Chueshov, *Order-preserving random dynamical systems*, Dynam. Stability Sys. 13 (1998), 265-280.

[3] J.P. Aubin, H. Frankowska, "Set-Valued Analysis", Birkhäuser, Boston (1990).

[4] A.B. Babin and M.I. Vishik, "Attractors of evolution equations", North Holland 1992.

[5] L. Berselli and F. Flandoli, *Remarks on determining projections for stochastic dissipative equations*, Discrete and Cont. Dyn. Systems vol. 5, n^{o}1 (1999), 197-214.

[6] T. Caraballo, J.A. Langa and J.C. Robinson, *Upper semicontinuity of attractors for small random perturbations of dynamical systems*. Commun. Part. Diff. Eq. 23 (1998), 1557-1581.

[7] T. Caraballo and J.A. Langa, *Tracking properties of trajectories on random attracting sets,* Stochastic Anal. and Appl. 17 (3) (1999), 339-358.

[8] T. Caraballo and J.A. Langa, *Comparison of the long-time behaviour of linear Ito and Stratonovich partial differential equations*, Stoch. Anal. and Appl. 19(2) (2001), 183-195.

[9] T. Caraballo, J.A. Langa, J. Valero, *Random atractors for multivalued random dynamical systems*, Nonlinear Anal. TMA 48(6) (2002), 805-829.

[10] T. Caraballo, J.A. Langa, J. Valero, *Global attractors for multivalued random dynamical systems generated by random differential inclusions with multiplicative noise*, J. Math. Anal. and Appl. 260 (2001), 602-622.

[11] T. Caraballo, J.A. Langa, J. Valero, *Global attractors for multivalued random semiflows generated by random differential inclusions with additive noise*, C.R. Acad. Sci. Paris, Serie I, t. 332 (2001), 131-136.

[12] T. Caraballo, J.A. Langa, J. Valero, *Approximations of attractors for multivalued random dynamical systems*, Int. J. of Math. Game Th. and Algebra 11(4) (2001), 67-92.

[13] T. Caraballo, J.A. Langa and J.C. Robinson, *Stability and random attractors for a reaction-difussion equation with multiplicative noise*, Discrete and Cont. Dyn. Systems 6, n^{o}4 (2000), 875-892.

[14] T. Caraballo, J.A. Langa, *On the upper semicontinuity of non autonomous and random dynamical systems*, Dynamics of Cont. Discrete and Impulsive Systems, por aparecer.

[15] T. Caraballo and J.A. Langa, *On the theory of random attractors and some open problems*, en Stochastic Partial Differential Equations and Applications, Da Prato and Tubaro (Eds.), Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, New York, 2002.

[16] T. Caraballo, J.A. Langa, T. Taniguchi, *The exponential behaviour and stabilizability of stochastic 2D-Navier-Stokes equations*, J. Diff. Equs, por aparecer.

[17] T. Caraballo, J.A. Langa and J.C. Robinson, *Attractors for differential equations with variable delays*, J. Math. Anal. and Appl. 260 (2001), 421-438.

[18] T. Caraballo, J.A. Langa and J.C. Robinson, *A stochastic pitchfork bifurcation in a reaction-diffusion equation*, Proc. Royal Soc. London A 457 (2001), 2041-2061.

[19] T. Caraballo, J.A. Langa, V. Melnik, J. Valero, *Pullback attractors of nonautonomous and stochastic multivalued dynamical systems*, Set Valued Analysis, por aparecer.

[20] T. Caraballo, J.A. Langa, J. Valero, *Dimension of attractors of non-autonomous reaction-diffusion equations*, ANZIAM Journal (formerly Journal of the Australian Mathematical Society, Series B - Applied Mathematics), por aparecer.

[21] T. Caraballo, P.E. Kloeden, J.A. Langa, *Atractores globales para ecuaciones diferenciales no autónomas*, CUBO, Revista Iberoamericana de Educación Matemática, en prensa.

[22] T. Caraballo, J.A. Langa, J. Valero, *On the relationship between solutions of stochastic and random differential inclusions*, prepublicación.

[23] C. Castaing and M. Valadier, "Convex Analysis and Measurable Multifunctions", LNM 580, Springer-Verlag, Berlin 1977.

[24] V. Chepyzhov and M. Vishik, *A Hausdorff dimension estimate for kernel sections of non-autonomous evolution equations*, Indiana Univ. Math. J. 42 (1993), 1057-1076.

[25] I.D. Chueshov, *On determining functionals for stochastic Navier-Stokes equations*, Stoch. and Stoch. Reports 68 (1999), 45-64.

[26] I.D. Chueshov, J. Duan, B. Schmalfuss, *Determining functionals for random partial differential equations*, prepublicación.

[27] H. Crauel, A. Debussche and F. Flandoli, *Random attractors*. J. Dyn. Diff. Eq. 9 (1995), 307-341.

[28] H. Crauel and F. Flandoli, *Attractors for random dynamical systems*. Prob. Theory Rel. Fields 100 (1994), 365-393.

[29] G. Da Prato, A. Debussche, *Construction of stochastic inertial manifold using backward integration*, Stoch. Stoch. Rep. 59 (1997), 305-324.

[30] A. Debussche, *On the finite dimensionality of random attractors*, Stoch. Anal. and Appl. 15 (1997), 473-492.

[31] A. Debussche, *Hausdorf dimension of a random invariant set*, J. Math. Pures Appl. 77 (1998), 10, 967-988.

[32] A. Eden, C. Foias, B. Nicolaenko and R. Temam, "Exponential attractors for dissipative evolution equations", RAM, Wiley, Chichester, 1994.

[33] K.D. Elworthy, "Stochastic differential equations on manifolds", Cambridge University Press, Cambridge 1982.

[34] F. Flandoli and J.A. Langa, *Determining modes for dissipative random dynamical systems.* Stoch. Stoch. Rep. 66 (1999), 1-25.

[35] F. Flandoli and B. Schmalfuss, *Random attractors for the 3D stochastic Navier-Stokes equation with multiplicative white noise*, Stoch. Stoch. Rep. 59 (1996), 21-45.

[36] C. Foias and G. Prodi, *Sur le comportement global des solutions non-stationnaires des equations de Navier-Stokes en dimension 2*, Rend. Sem. Mat. Univ. Padova 39 (1967), 1-34.

[37] C. Foias, R. Temam, *Determination of the solutions of the Navier-Stokes equations by a set of nodal values,* Mathematics of Computation **43** (1984), 117–133.

[38] C. Foias, G. Sell, R. Temam, *Inertial manifolds for dissipative evolution equations*, J. Diff. Equs. 73 (1988), 311-353.

[39] P. Friz, J.C. Robinson, *Parametrising the attractor of the two-dimensional Navier-Stokes equations with a finite set of nodal values*, Physica D148 (2001) 201-220

[40] P. Glendinning, "Stability, instability and chaos: an introduction to the theory of nonlinear differential equations", Cambridge Texts in Applied Mathematics, Cambridge 1994.

[41] J. Hale, "Asymptotic Behavior of Dissipative Systems", Math. Surveys and Monographs, AMS, Providence 1988.

[42] H. Keller and B. Schmalfuss, *Attractors for stochastic differential equations via transformation into random differential equations*, prepublicación.

[43] P. Kloeden, B. Schmalfuss, *Nonautonomous systems, cocycle attractors and variable time-step discretization*, Numer. Algorithms 14 (1997), 141-152.

[44] O. Ladyzhenskaya, "Attractors for Semigroups and Evolution Equations", Accademia Nazionale dei Lincei, Cambridge University Press, Cambridge 1991.

[45] J.A. Langa, A. Suárez, *Pullback permanence for non-autonomous partial differential equations*, prepublicación

[46] J.A. Langa and J.C. Robinson, *Determining asymptotic behaviour from the dynamics on attracting sets*, J. Dyn. and Diff. Eqs. vol 11, n^{o}2 (1999), 319-331.

[47] J.A. Langa and J.C. Robinson, *A finite number of points observations which determine a non-autonomous flow*, Nonlinearity 14 (2001), 673-682.

[48] J.A. Langa, *Asymptotically finite dimensional pullback behaviour of non autonomous PDEs*, Archiv der Mathematic, por aparecer.

[49] J.A. Langa, J.C. Robinson and A. Suárez, *Stability, instability and bifurcation phenomena in non-autonomous differential equations*, Nonlinearity, por aparecer.

[50] J.A. Langa, J.C. Robinson and A. Suárez, *Permanence in the non-autonomous Lotka-Volterra competition model*, prepublicación.

[51] J.A. Langa, J.C. Robinson and A. Suárez, *Forwards and pullback behaviour of a non-autonomous Lotka-Volterra system*, prepublicación.

[52] J.A. Langa, *Finite dimensional pullback asymptotic behaviour of stochastic partial differential equations*, prepublicación.

[53] V. Melnik, J. Valero, *On Attractors of multivalued semi-flows and differential inclusions*, Set-Valued Anal. 6 (1998), 83-111.

[54] H. Morimoto, *Attractors of probability measures for semilinear stochastic evolution equations*, Stochastic Anal. Appl. 10(2) (1992), 205-212.

[55] J.D. Murray, "Mathematical Biology", Springer-Verlag, New York 1993.

[56] J.C. Robinson, *Some approaches to finite-dimensional behaviour in the Navier-Stokes equations*, Curso impartido en el Departamento de Ecuaciones Diferenciales y Análisis Numérico (1997), Universidad de Sevilla.

[57] J.C. Robinson, "Infinite-dimensional Dynamical Systems", Cambridge University Press 2001.

[58] J.C. Robinson, *A rigorous treatment of experimental observations for the two-dimensional Navier-Stokes equations*, Proc. Royal Soc. London A 457, 107-1020.

[59] B. Schmalfuss, *Backward cocycles and attractors of stochastic differential equations*, In "V. Reitmann, T. Riedrich and N Koksch, editors, International Seminar on Applied Mathematics-Nonlinear Dynamics: Attractor Approximation and Global Behaviour," 185-192, 1992.

[60] B. Schmalfuss, *Measure attractor and random attractors for stochastic partial differential equations*, Stochastic Anal. Appl. 17 (6) (1999), 1075-1101.

[61] G. Sell, *Nonautonomous differential equations and topological dynamics I, II*, Amer. Math. Soc. 127 (1967), 241-262, 263-283.

[62] R. Temam, "Infinite-Dimensional Dynamical Systems in Mechanics and Physics", Springer-Verlag, New York 1988 (and 2nd edition 1996).

[63] H. Thieme, *Asymptotically autonomous differential equations in the plane*, Rocky Mountain J. Math 24 (1994), 351-380.

[64] M.I. Vishik, "Asymptotic behaviour of solutions of evolutionary equations", Cambridge University Press

Bol. Soc. Esp. Mat. Apl. nº 21(2002), 117–118

Enseñar matemáticas es hacer democracia

I. Fernández y J. M. Pacheco

Departamento de Matemáticas
Universidad de Las Palmas de Gran Canaria
Campus de Tafira Baja, 35017 Las Palmas de Gran Canaria

pacheco@dma.ulpgc.es

No cabe duda de que algunas Matemáticas forman parte de la vida cotidiana de manera harto aparente, y también es verdad que en cualquier sociedad medianamente desarrollada todos sus componentes son expuestos al contacto con las Matemáticas a edades tempranas. Además, la dificultad de adquirir las habilidades matemáticas mínimas en Aritmética y Geometría no es superior a la de aprender a redactar unas líneas con corrección. Ambas capacidades están muy relacionadas, pues en los dos casos se trata de expresar una secuencia lógica de ideas. En Aritmética y Geometría se consigue ejercitando las capacidades de observación y cálculo para que la mente se acostumbre a reconocer razonamientos válidamente construidos. Con referencia a la capacidad lingüística, la observación tiene su equivalente en la adquisición de un vocabulario rico, y el cálculo en la redacción, para que la expresión oral y escrita fluyan lo más suavemente posible.

No hay, pues, distinción nítida entre Ciencias y Letras. La elección de una vía cultural preferente (o cegar una, otra o ambas) corresponde a las influencias ambientales en forma de entornos educativos, familiares y mediáticos. Será difícil que un joven llegue a apreciar la Literatura si sólo ve telenovelas de ínfima calidad, y también será difícil que aprecie las Matemáticas si quienes se las enseñan no disfrutan con ellas y no transmiten el entusiasmo necesario para obviar las dificultades del cálculo y de los ejercicios pertinentes para alcanzar la habilidad mínima que haga agradable la práctica de las Matemáticas. También el solfeo y la conjugación de los verbos irregulares son en principio ajenos al goce con la Música o la Literatura.

Hay filósofos cuya opinión es que la Filosofía no se enseña, se hace, para lo cual hay que dominar un vocabulario y relacionar los conceptos expresados por esas palabras de manera adecuada. Ese juego *produce* Filosofía. Lo mismo podríamos decir de las Matemáticas: Éstas se *hacen* desde el principio, y éste consiste en calcular y en interpretar figuras. No se deben de confundir los términos *hacer Matemáticas* y *descubrir las Matemáticas*, como pretenden algunas líneas didácticas con ínfulas de innovación. En los niveles elementales está descubierto casi todo, y hacer Matemáticas significa principalmente

adquirir familiaridad y soltura con los conceptos y técnicas del cálculo aritmético y de las figuras geométricas. El *producto matemático* consiste en la aceptación de las Matemáticas como *método* –otros, exagerando con Galileo, dirían *lenguaje*– para la exploración del mundo.

Pero que nadie se engañe: *Hay que enseñar –y aprender–* a calcular y a interpretar figuras, al igual que a manejar el lenguaje habitual con corrección. La labor docente tiene como objetivo primordial *consolidar conocimientos y actitudes*, lo que incluye enseñar y aprender (también a enseñar) en continua lucha contra hábitos y vicios muy extendidos: En última instancia, hay que aprender para despertar el pensamiento crítico y modificar actitudes sociales y culturales tendentes al adocenamiento y la ignorancia colectiva.

Si reflexionamos un poco acerca de *¿qué consolidar en Matemáticas básicas*?, el catálogo es sorprendentemente reducido:

1. No dudar acerca de qué operaciones aritméticas deben de llevarse a cabo con los datos de un problema, y efectuarlas.

2. Reconocer la proporcionalidad (esto antes se llamaba regla de tres) y operar con fracciones.

3. Comprensión y habilidad en el manejo del sistema métrico decimal.

4. Reconocer las propiedades más visibles de las figuras planas y espaciales más elementales.

Dominar las habilidades elementales citadas en los cuatro puntos anteriores ya proporciona un bagaje matemático bastante elevado: Nos deja en puertas del Álgebra y del Cálculo Infinitesimal, esto es, a un nivel casi preuniversitario. Tal vez alguien se pregunte por qué no incluir entre estos objetivos el manejo de máquinas o programas de cálculo. Opinamos que lo importante es *saber qué hacer y tener una idea aproximada del resultado esperado.* Teniendo esto claro, la dificultad de usar tales máquinas o programas no supera a la de manejar un electrodoméstico cualquiera.

Sólo sobre cimientos sólidos se construirán edificios también sólidos. Hay que *estimular* al Profesorado, *formarlo sin deformarlo* y dotarlo de la *relevancia y consideración que se merece y hoy se le niega* para que su actuación, en lugar de entorpecer y sesgar el desarrollo intelectual de los jóvenes, los conduzca por los caminos del razonamiento válido y de la expresión lingüística correcta: *No hay más talento que el despertado por una buena educación.* Y esto vale para todos los talentos.