Flatness and Submersivity in Discrete-Time Dynamical Systems

Philippe Guillot, Université Paris 8, LAGA

Gilles Millérioux, Université de Lorrraine, CRAN

2nd International Workshop on Cryptography and its Applications

19 juin 2019, ORAN Algérie

Résultat

Tout système dynamique à temps discret submersif et plat est totalement contrôlable

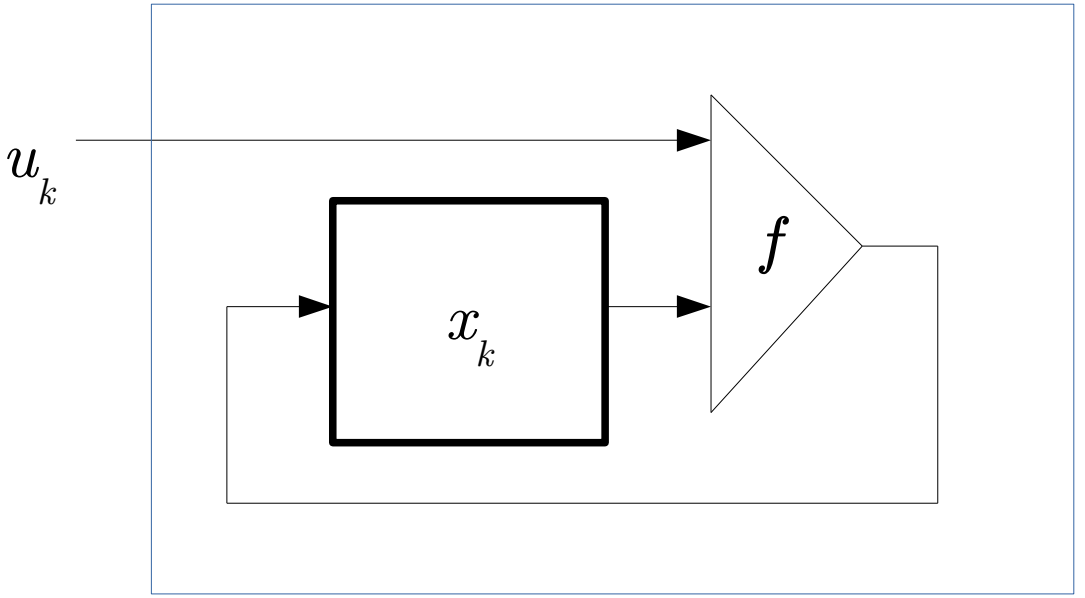
(IEEE Control Systems letters)

Système dynamique à temps discret

$x_{k+1} = f(x_k, u_k)$ Équation dynamique

$(u_k) \in U^{\mathbb{N}}$ Séquence d'entrée, contrôle

$(x_k) \in X^{\mathbb{N}}$ Suite des états internes



Système linéaire

- *U* et *X* sont des espaces vectoriels de dimension finie sur un même corps $\mathbb{F}$ (fini)
- Équation dynamique $x_{k+1} = A\, x_k + B\, u_k$

  A et *B*, matrices de dimensions idoines

Sortie plate

$$y_k = h\left(x_k, u_k, \cdots, u_{k-r+1}\right) \in U$$

Un nombre fini d'itérés passés et/ou futurs de la sortie plate permet de reconstituer l'état interne et l'entrée

$$x_k = \mathscr{F}\left(y_{k+r_1}, \cdots, y_{k+r_2}\right), \qquad r_1, r_2 \in \mathbb{Z}$$

$$u_k = \mathscr{G}\left(y_{k+s_1}, \cdots, y_{k+s_2}\right), \qquad s_1, s_2 \in \mathbb{Z}$$

Sortie 0-plate $y_k = h\left(x_k\right)$

Sortie 1-plate $y_k = h\left(x_k, u_k\right)$

} Sorties matérielles

...

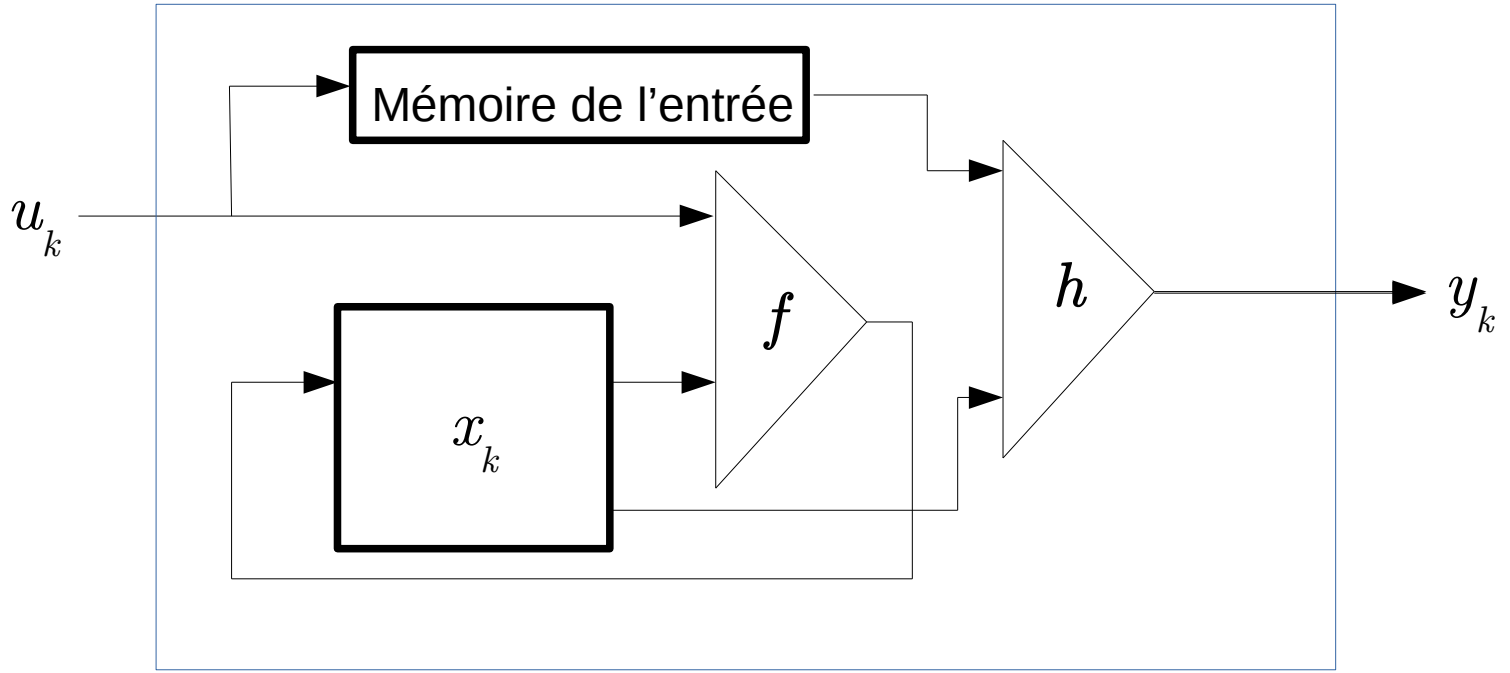
Sortie *r*-plate $y_k = h\left(x_k, u_k, \cdots, u_{k-r+1}\right)$ Mémoire de l'entrée

Système plat

- Il existe une sortie plate
- La platitude est une propriété de l’équation dynamique
- Si une sortie est plate, alors toute décalée est plate
- Motivation cryptologique : chiffrement autosynchronisant

Système 1-plat étendu

- Si un système est *r*-plat, en incluant dans l'état interne la mémoire de l'entrée, on obtient un système 1-plat aux propriétés semblables



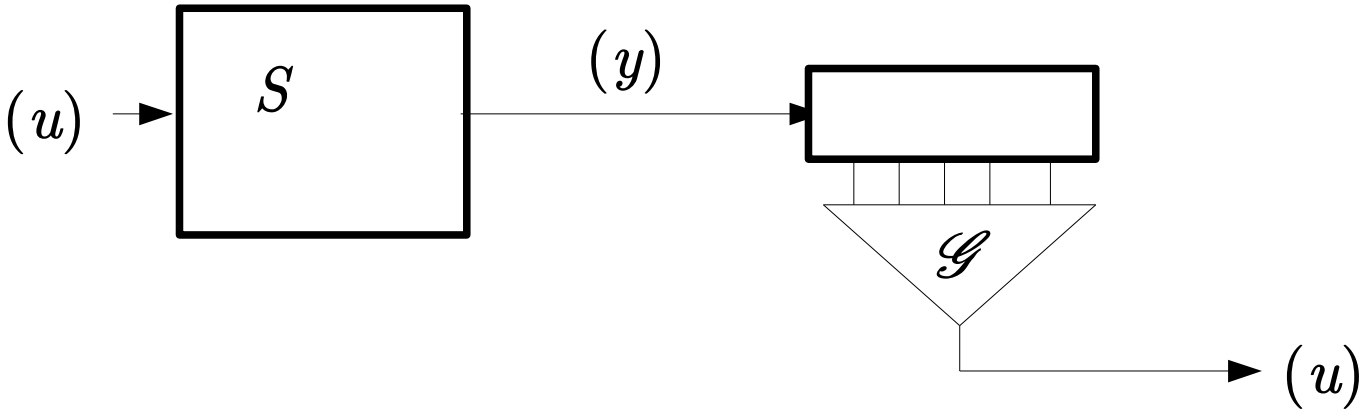
Inversibilité à gauche

- S, avec une sortie matérielle $h : (x, u) \rightarrow y = h(x, u)$ est inversible à gauche si pour tout état initial x_0 l'application $(u) \rightarrow (y)$ est injective
- Il existe un système inverse à gauche $(y) \rightarrow (u)$
- Application en cryptographie :

  chiffrement / déchiffrement

- Si h est une sortie 0 ou 1 – plate, alors S est inversible à gauche

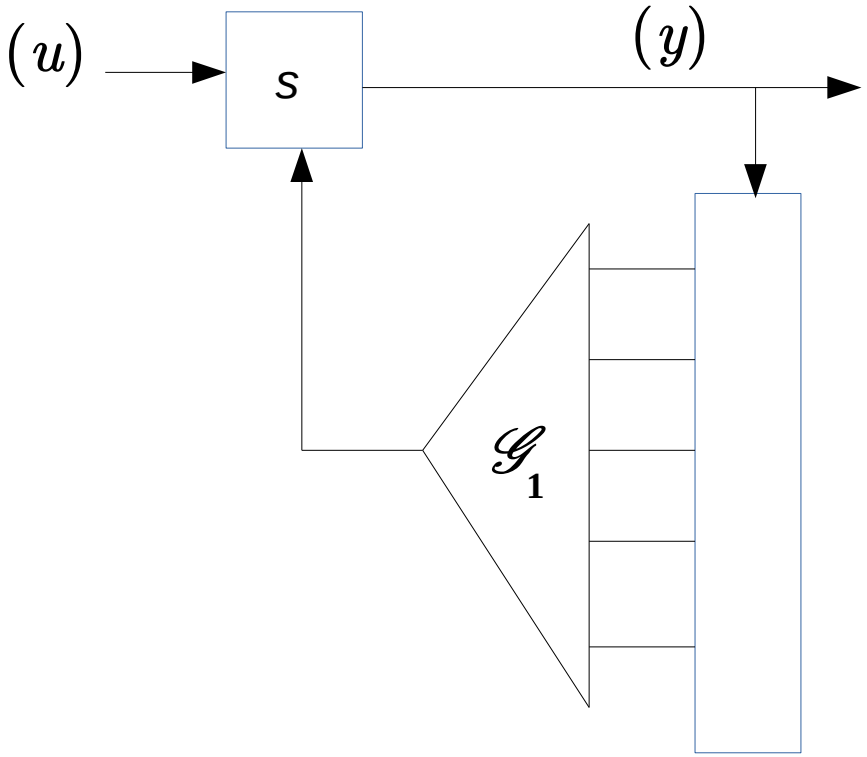
Inverse à gauche canonique

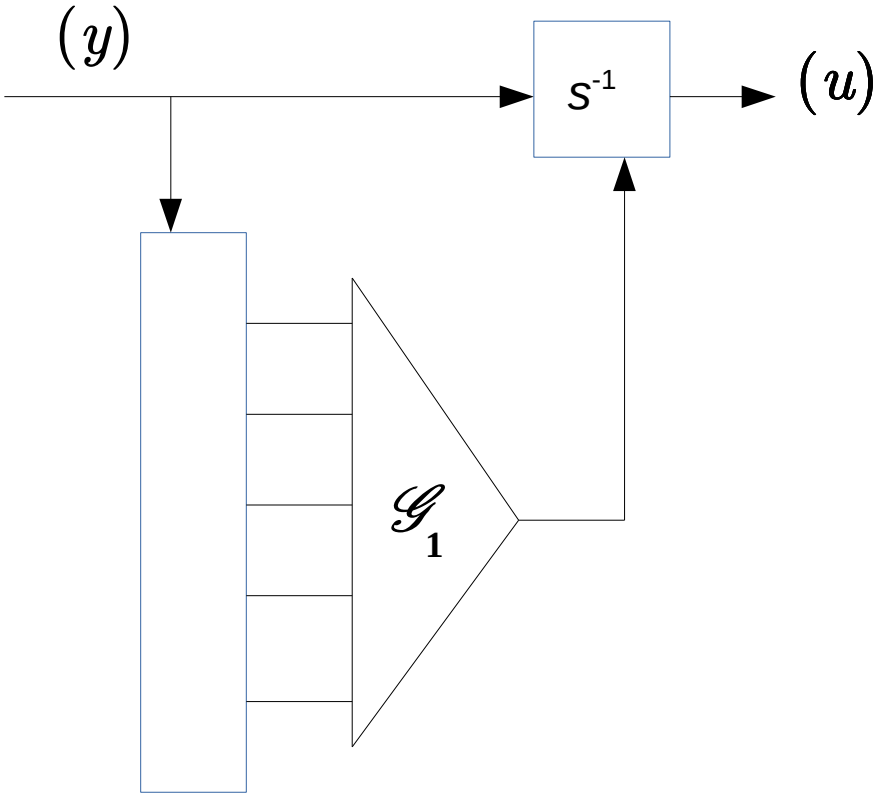


(y) est une sortie 0 ou 1 – plate

L'inverse à gauche est autosynchronisant

Forme canonique systèmes direct et inverse chiffrement autosynchronisant





Submersivité

- La fonction *f* est surjective

  Tout état est atteignable à partir d'un certain autre état pour un certain contrôle.
- Cas linéaire : la matrice [*A* : *B*] est de rang plein
- La submersivité exprime qu'il est possible de « *revenir en arrière* »

Atteignabilité

(1) x_f est atteignable à partir de x_i s'il existe un contrôle qui mène de x_i à x_f

(2) Un système est atteignable à partir de x_i si tout état x_f est atteignable à partir de x_i

(3) Un système est totalement atteignable s'il est atteignable à partir de tout x_i

Toujours $(3) \Rightarrow (2) \Rightarrow (1)$

Système linéaire : $(2) \Rightarrow (3)$

Contre-exemple dans les autres cas.

- *N.B.* Atteignable $\Rightarrow$ Submersif

Contrôlabilité

(1) x_i est contrôlable vers x_f s'il existe un contrôle mène de x_i à x_f

(2) Un système est contrôlable vers x_f si tout état mène à x_f

(3) Un système est totalement contrôlable s'il est contrôlable vers tout x_f

Toujours $(3) \Rightarrow (2) \Rightarrow (1)$

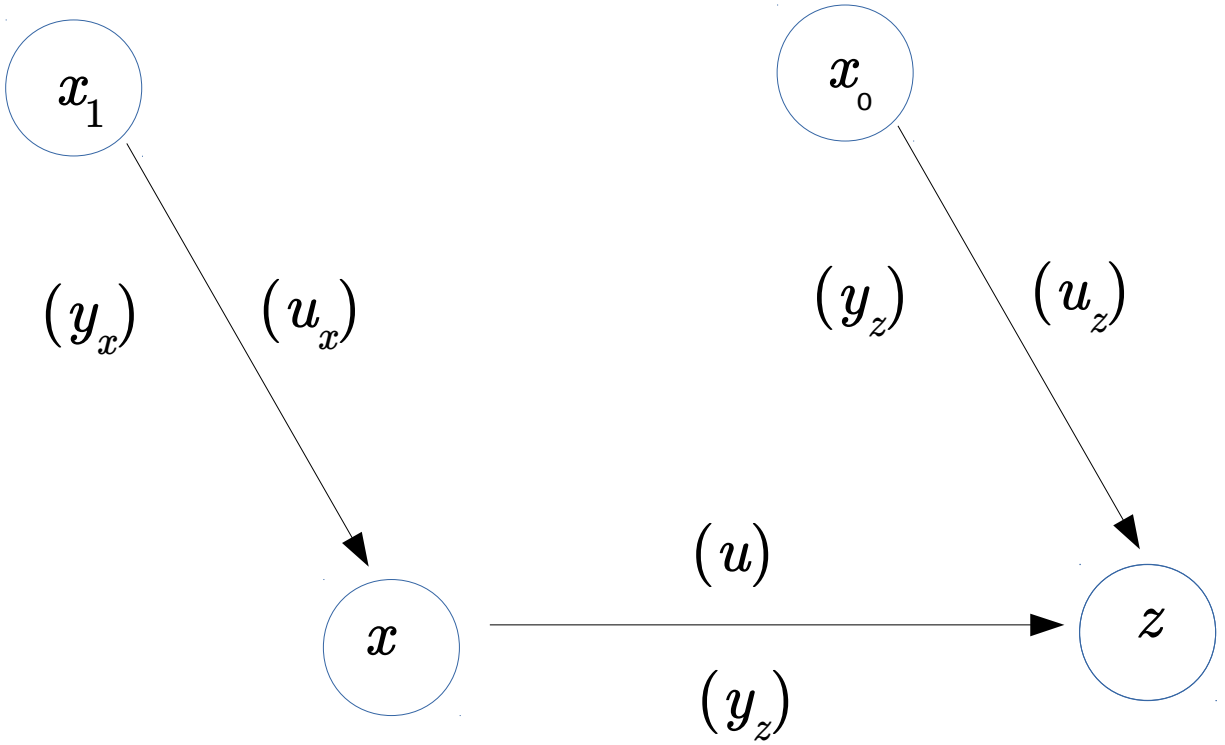
Contre-exemple dans les autres cas.

- totalement atteignable $\Leftrightarrow$ totalement contrôlable

Théorème

- Si *S* est plat et submersif, alors il est totalement contrôlable ($\Leftrightarrow$ totalement atteignable)
- Pas de condition de linéarité
- Submersivité nécessaire, contre exemple si non submersif
- Réciproque fausse : contre exemple non linéaire
- Si *S* est linéaire et totalement contrôlable, alors il est plat (et submersif)

Esquisse 0 ou 1 plat



$$x = \mathcal{G}((y_x))$$

$$z = \mathcal{G}((y_z))$$

Cas général

- Si un système est r-plat et submersif, alors le système étendu est 1-plat et submersif
- Il est donc totalement contrôlable.
- Le système initial est donc aussi totalement contrôlable.

Récapitulation

Atteignable depuis x_i — Contrôlable vers x_f

$\Uparrow$ $(\Downarrow$ si linéaire $)$ — $\Uparrow$

Totalement atteignable $\Leftrightarrow$ Totalement contrôlable

$\Uparrow$ $(\Downarrow$ si linéaire $)$

plat et submersif

Conclusion

Coopération de deux équipes :

- Théorie du contrôle (CRAN, Université de Lorraine)
- Cryptologie (Laga, Université Paris 8)