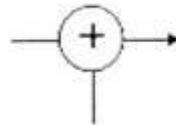


Examen d'Electronique - Logique
(documents autorisés, copie séparée)

Etude de quelques circuits LFSR

Note :

Le symbole suivant dans les figures représente une porte
OU EXCLUSIF (la sortie est signalée par une flèche):



Les circuits LFSR (Linear Feedback Shift Register) sont au cœur de tout système capable de générer des séquences de bit pseudo-aléatoires, utilisées dans des applications de cryptographie, de fiabilité, de communications sans fil, etc....

Un circuit LFSR est un circuit séquentiel synchrone d'une horloge H. On propose ici différentes implantations de circuits LFSR.

Question 1 :

Les circuits LFSR s'inspirent des registres à décalage.

Dessiner le schéma d'un registre à décalage RD dont les caractéristiques sont les suivantes :

- RD effectue des décalages à droite
- RD est synchrone d'une horloge H, sur front montant
- RD dispose d'une sortie série 1 bit à droite et des sorties parallèles
- Les bascules du registre sont des bascules D.

Question 2 :

La figure 1 présente l'implantation dite « de Fibonacci » d'un LFSR d'ordre 3 ; les bascules D sont synchrones sur front montant de H.

- Donner pour une série de 16 périodes de H la liste des 16 états successifs des sorties des 3 bascules, en identifiant clairement la sortie du LFSR (états notés 0 ou 1). L'état initial de ces sorties est : **0 1 0** (sorties des bascules de gauche à droite)

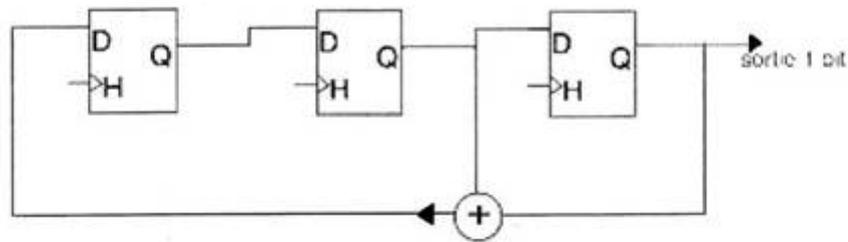


Figure 1

Question 3 :

La figure 2 présente l'implantation dite « de Galois » d'un LFSR d'ordre 3 ; les bascules D sont synchrones sur front montant de H.

- Donner pour une série de 16 périodes de H la liste des 16 états successifs des sorties des 3 bascules, en identifiant clairement la sortie du LFSR (états notés 0 ou 1). L'état initial de ces sorties est : **0 1 0** (sorties des bascules de gauche à droite)

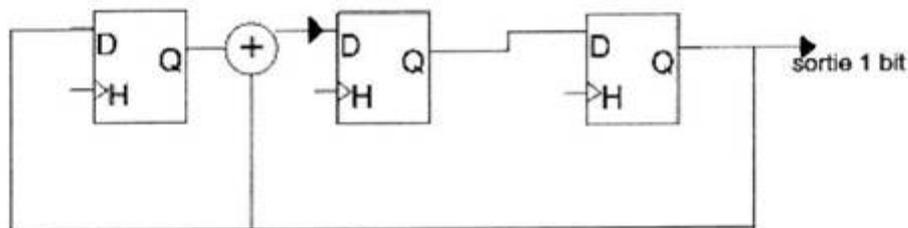


Figure 2

- Quelle est la longueur (en nombre de périodes de H) d'un cycle de répétition sur les sorties pour chacun des LFSR ?

Question 4 :

Le LFSR de Galois d'ordre 3 de la figure 2 peut s'implanter différemment, sous la forme d'un compteur ou séquenceur à base de bascules JK, dont les sorties sont les variables d'état ; dans ce cas, ces variables d'état suivent la séquence des sorties des bascules D de la figure 2.

En vous aidant des résultats de la question 3, synthétiser le séquenceur reproduisant le LFSR de Galois d'ordre 3 :

- Donner les équations des variables d'états
- Dessiner le schéma du circuit résultant.