ELECINF102
Processeurs et Architectures Numériques

Contrôle de connaissances

Vendredi 14 juin 2013 à 8h30

Document autorisé : une feuille recto-verso

Durée: 1h30 minutes

Ce contrôle comporte quatre parties **indépendantes** :

1. Questions de cours
2. Cryptographie
3. Vitesse d'une balle de tennis
4. Rétroconception

Consignes importantes : Les schémas demandés dans les différents exercices doivent être impérativement clairs, lisibles et sans ambiguïté. Les dimensions des bus doivent être indiquées. Si nécessaire le sens des signaux doit être précisé.

N'oubliez pas d'inscrire nom, prénom, et numéro de casier sur votre copie.

Bon courage !

1 Questions de cours

Question 1 : Quelle est la valeur décimale du mot binaire (101001) si sa représentation est non signée ? Même question avec la représentation signée en complément à 2.

Question 2 : Soit la portion de circuit suivante :

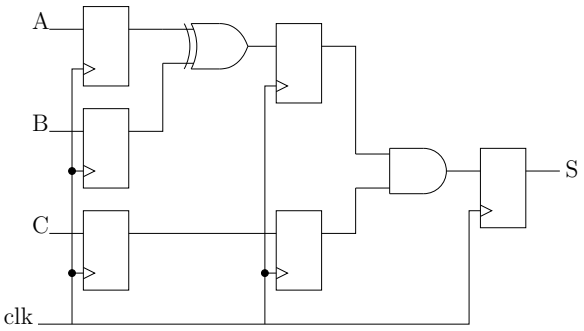


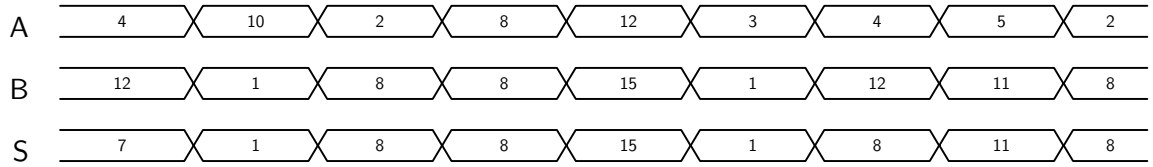
Figure 1 – *Circuit pipeline*

Calculez la fréquence maximale de l'horloge (clk) pour que cette portion de circuit fonctionne correctement sachant que :

- le temps de propagation des portes AND est de 1 ns,
- le temps de propagation des portes XOR est de 2 ns,
- le temps de propagation (t_{co}) des bascules est de 1 ns,
- le temps de pre-positionnement (t_{su}) ainsi que le le temps de maintien (t_h) des bascules sont considérés comme nuls.

Question 3 : Dans le nanoprocesseur étudié dans le module PAN, pourquoi est–il nécessaire de stocker l'instruction dans un registre ?

Question 4 : Les chronogrammes ci-dessous, A et B étant des entrées et S une sortie, représentent-ils une fonction combinatoire ou séquentielle ? Pourquoi ?

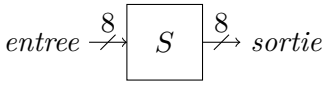


Question 5 : Dans un processus **always @(posedge clk)**, ajoutez, un registre à décalage disposant de N bascules D_i, $i \in [0, N-1]$ d'une entrée E et d'une sortie S. Le code sera le plus compact possible.

2 Cryptographie

Dans cet exercice, nous allons nous intéresser à une étape fondamentale d'un algorithme de chiffrement : les tables de substitution (ou *SBox*).

Nous disposons d'une fonction combinatoire S prenant en entrée un mot de 8 bits et produisant un mot de 8 bits :



L'algorithme consiste à appliquer la fonction S aux quatres mots (e_1, e_2, e_3, e_4) pour produire les quatre mots $s_1 = S(e_1)$, $s_2 = S(e_2)$, $s_3 = S(e_3)$, $s_4 = S(e_4)$. Le but de cet exercice est de concevoir un module `substitution` prenant en entrée les quatre mots e_1, e_2, e_3, e_4 et produisant les sorties s_1, s_2, s_3, s_4.

2.1 Version combinatoire

Question 1 : Réalisez un *schéma* du module `substitution`.

2.2 Version séquentielle

Malheureusement, la fonction S est coûteuse en matériel et donc on suppose maintenant que l'on ne peut plus disposer que d'un seul bloc matériel réalisant la fonction S. Ce bloc devra donc traiter successivement les quatre mots en entrée pour produire les quatre mots en sortie.

Notre module `substitution` est maintenant muni des entrées et sorties *supplémentaires* suivantes :

Signal	Direction	Taille	Description
`clk`	Entrée	1 bit	L'horloge
`e_valid`	Entrée	1 bit	Signal indiquant (quand il est à 1) que les valeurs présentées sur `e1` à `e4` sont valides et à prendre en compte. Il ne dure qu'un cycle et ne peut repasser à 1 qu'après le passage à 1 de `s_valid`
`s_valid`	Sortie	1 bit	Signal indiquant (quand il est à 1) que les valeurs présentes sur les sorties `s1` à `s4` sont valides et à prendre en compte. Ce signal doit donc être mis à 1, *pendant un cycle d'horloge*, une fois que le calcul est terminé.

Question 2 : Dessinez un *schéma* du nouveau module `substitution` (vous n'avez le droit d'utiliser qu'un seul bloc S).

3 Vitesse d'une balle de tennis

Nous voulons concevoir un système qui permet de mesurer la vitesse d'une balle de tennis lors de son passage entre deux portiques. Les portiques contiennent un système optique composé d'un émetteur et d'un récepteur de lumière infrarouge (non visible). À son passage, la balle coupe le faisceau lumineux et une impulsion électrique est générée au niveau de chaque portique (un signal passe à 1 puis redescend à 0).

Pour mesurer la vitesse de la balle, nous devons mesurer le temps entre les impulsions générées au niveau de chaque portique. La distance entre les portiques étant connue, il suffira par la suite de faire une simple division (non demandée ici).

Dimensionnement du système

Les deux portiques sont situés à 10 mètres l'un de l'autre. Les balles de tennis ont un diamètre de 10cm et se déplacent à une vitesse qui varie entre 3,6km/h et 360km/h. Le système de traitement réalisé en logique synchrone dispose d'une horloge *clk*.

Pour être sûr de détecter le passage de la balle, l'impulsion générée par le récepteur du portique doit durer au moins deux périodes de l'horloge *clk*.

Question 1 : À laquelle des fréquences suivantes doit–on faire fonctionner notre système ?

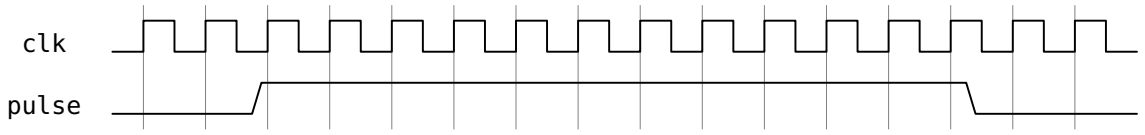
- 10 Hz
- 1 KHz
- 100 KHz

Le temps de vol de la balle entre les deux portiques sera mesuré comme un multiple de la période de l'horloge *clk*.

Question 2 : Sur combien de bits faut–il compter pour mesurer le temps de vol pour toutes les vitesses prévues ?

Mise en forme des impulsions

La durée des impulsions (`pulse`) au niveau des portiques dépend de la taille de la balle et de la vitesse à laquelle elle passe. Pour simplifier la suite nous voulons générer à chaque passage de balle une impulsion (`top`) dont la durée est d'une seule période de l'horloge.



Question 3 : Proposez le schéma ou le code SystemVerilog d'un système générant un top d'un cycle d'horloge à chaque passage de balle.

Calcul du temps de vol

Considérant que nous avons maintenant des tops d'un cycle d'horloge, nous voulons mesurer le temps de vol entre les deux portiques.

Question 4 : Proposez le schéma d'un système permettant de compter le nombre de cycles d'horloge entre les deux impulsions générées au niveau de chaque portique.

Question 5 : Donnez le code SystemVerilog correspondant.

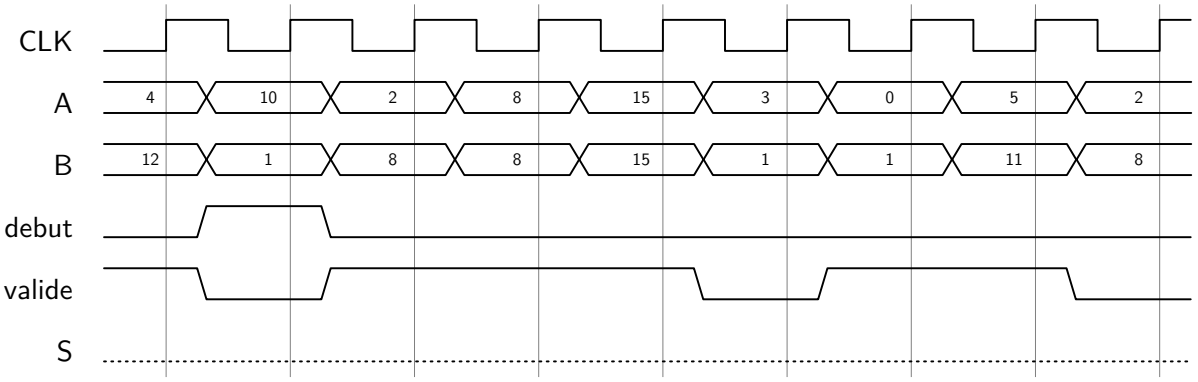
4 Où le lecteur découvre la Rétroconception (reverse–engineering)

La rétroconception n'est pas la conception à la mode antique, mais l'analyse de la conception d'autres ingénieurs ou scientifiques de manière à comprendre, copier et éventuellement améliorer un dispositif existant.

Vous disposez du code SystemVerilog de l'opérateur F1 suivant, qui est manifestement en logique synchrone...

Question 1 : Complétez le chronogramme correspondant au test de la fonction F1. Vous indiquerez précisément, à chaque cycle, la valeur de la sortie S. Expliquez le traitement effectué par la fonction.

```
module F1(
         input  logic clk,debut,valide,
         input  logic [3:0] A,B,
         output logic [7:0] S
         );
always @(posedge clk)
begin
  if(debut)
     S <= 8'b0 ;
  else if(valide)
       S <= A * B + S ;
end
endmodule
```



Noubliez pas de placer la feuille avec le chronogramme dans votre copie (attention il peut y avoir des questions au verso de la feuille...)

- **Nom :**
- **Prénom :**
- **Casier :**

Question 2 : Vous disposez d'une variante F2 du code SystemVerilog de l'opérateur. L'opérateur F2 réalise–t–il le même calcul que l'opérateur F1 ? Justifiez votre réponse qu'elle soit positive ou négative.

```
module F2(
         input  logic clk, debut, valide,
         input  logic [3:0] A,B,
         output logic [7:0] S
         );
logic [7:0] P ;
always @(posedge clk)
begin
  if(debut)
     S <= 8'b0 ;
  else if(valide)
    begin
       P <= A * B ;
       S <= P + S ;
    end
end
endmodule
```

Question 3 : Vous disposez d'une variante F3 du code SystemeVerilog de l'opérateur. L'opérateur F3 réalise–t–il le même calcul que l'un des opérateurs F1 ou F2 ? Justifiez votre réponse.

```
module F3(
         input  logic clk, debut, valide,
         input  logic [3:0] A,B,
         output logic [7:0] S
         );
logic [7:0] P,X;

always @( * )
  P <= A * B ;

always @( * )
begin
  if(debut)       X <= 8'b0 ;
  else if(valide) X <= P + S ;
  else            X <= S ;
end

always @(posedge clk)
  S <= X ;

endmodule
```

Question 4 : Nous désirons choisir, parmi F1 F2 ou F3, l'opérateur pouvant fonctionner à la fréquence d'horloge la plus élevée (indépendamment la fonction réalisée). Quel opérateur choisissez vous ? Justifiez votre réponse.