Nom : _____ Matricule : _____

INF3500 : Conception et réalisation de systèmes numériques

Examen intra #3 – jeudi 4 décembre 2014

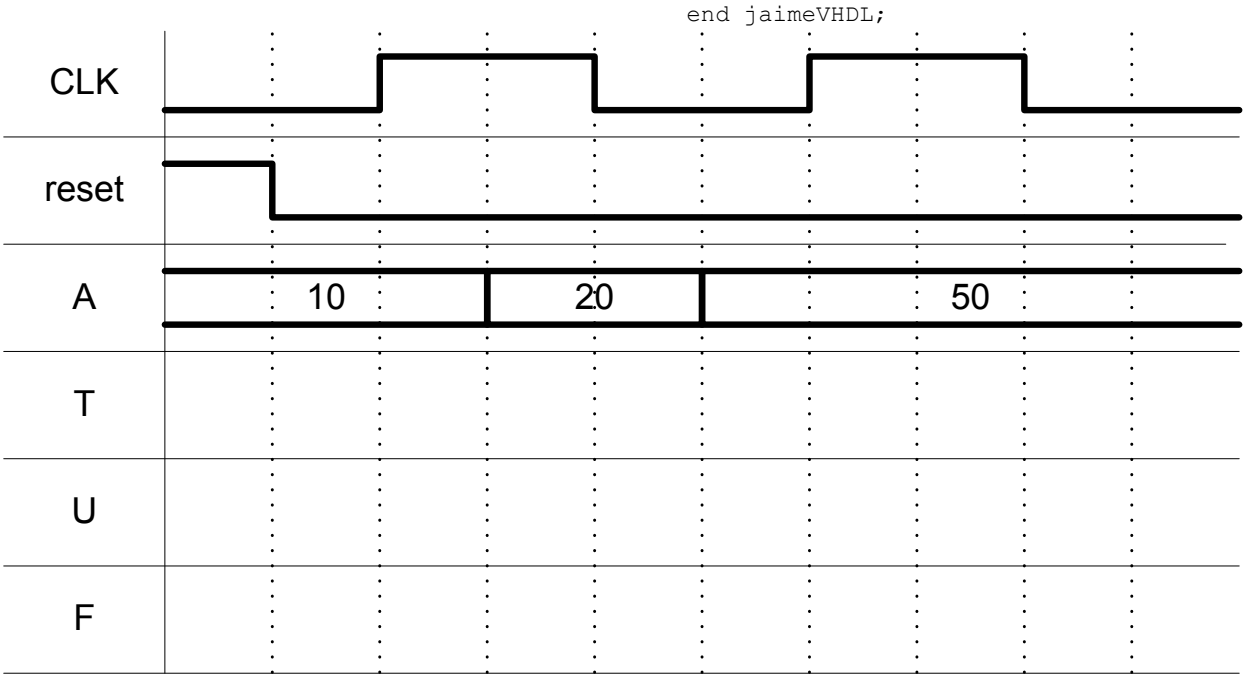
Durée: 1 heure. Documentation: Une feuille recto verso 8.5"×11" ou A4 permise.
Pondération: 0% (formatif). Calculatrice: Programmable permise.
Directives particulières:

- Ordinateurs interdits. Appareils mobiles interdits.
- Répondre à toutes les questions, la valeur de chaque question est indiquée.
- Répondre sur le questionnaire et le remettre.
- Ne posez pas de questions. En cas de doute sur le sens d'une question, énoncez clairement toute supposition que vous faites.

Question 1. (2 points)

Considérez l'extrait de code VHDL suivant et les valeurs des signaux CLK, reset et A montrées sur le chronogramme. Complétez le chronogramme pour les signaux et variables T, U, V et F

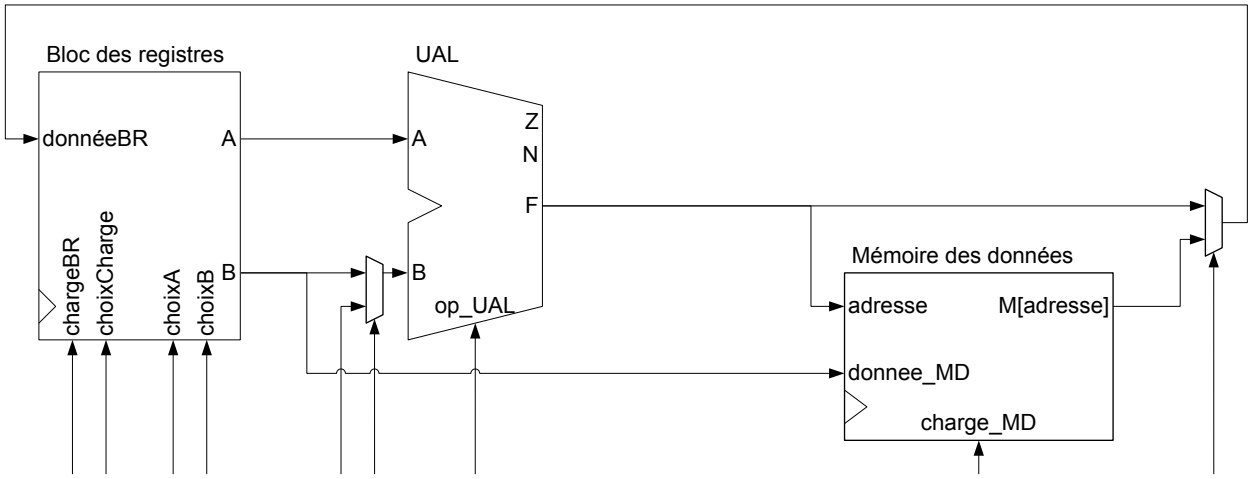
```
library IEEE;
use IEEE.std_logic_1164.all;

entity VHDLEstMonAmi2 is
   port (
      clk, reset : in std_logic;
      A : in integer;
      F : out integer
   );
end VHDLEstMonAmi2;

architecture jaimeVHDL of VHDLEstMonAmi2 is

signal T, U : integer;

begin

process (clk, reset)
variable V : integer := 10;
begin
   if reset = '1' then
      T <= 0;
      U <= 0;
   elsif rising_edge(clk) then
      T <= T + V;
      V := V + 5;
      U <= T + V;
   end if;
end process;

process (A)
begin
   F <= A + T + U;
end process;

end jaimeVHDL;
```



Question 2. (3 points)

Estimez combien de ressources seraient nécessaires pour implémenter le chemin des données du processeur PolyRISC sur un FPGA de la famille Virtex-5. Supposez que le bloc des registres comporte 4 registres de 16 bits, que l'UAL peut effectuer les 8 opérations suivantes : A, B, A + B, A – B, A ET B, A OU B, NON A, A OUX B, et que la mémoire des données comporte 256 mots de 16 bits. Donnez votre réponse en termes de LUT, de bascules et de bits de mémoire Block RAM.

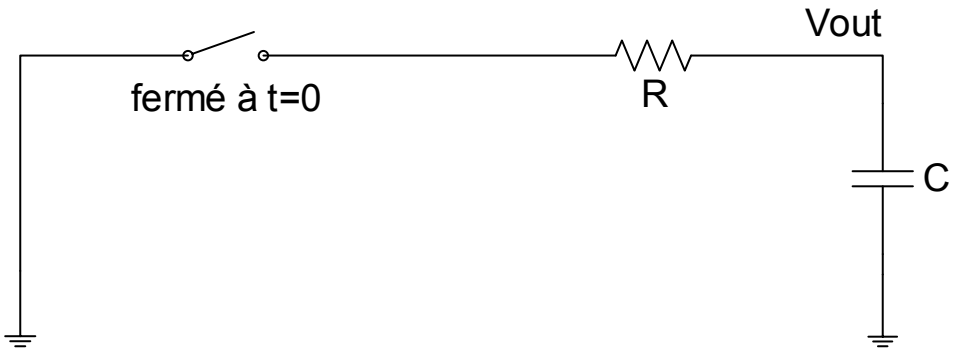
Montrez tous vos calculs et justifiez complètement votre réponse. Utilisez le verso si nécessaire.



Question 3. (2 points)

La sortie d'un inverseur est initialement un 1 logique, correspondant à une tension $V_{out} = V_0$ volt.

À t = 0 s, l'entrée de l'inverseur passe instantanément de 0 à 1, commandant alors une sortie de 0 logique ou une tension $V_{out} = 0$ volt. On peut modéliser cette situation par le circuit suivant.



L'équation pour la tension de sortie est : $V_{out} = V_0 \times e^{-t/RC}$, où R et C sont respectivement les résistances et capacités du circuit, dues aux transistors et interconnexions.

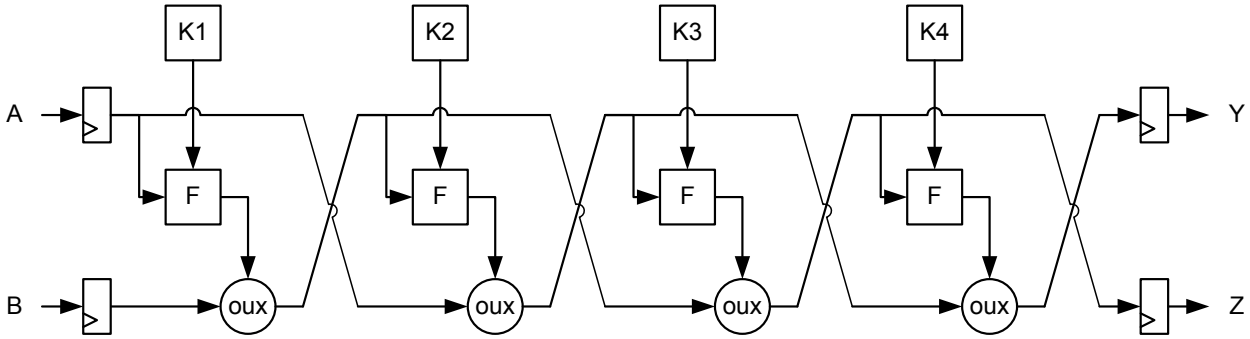
a. Donnez une expression pour la valeur du délai de descente t_{PHL} en fonction de R et C.

b. Quel est l'effet sur t_{PHL} de doubler la valeur de R en maintenant C constante?

c. Quelle est la valeur de tPHL pour R = 10 Ω et C = 1 nF?

Question 4. (3 points)

Le réseau de Feistel est utilisé dans les algorithmes de chiffrement par bloc. Plusieurs algorithmes utilisent le réseau de Feistel, dont DES, Blowfish et RC5. Le diagramme suivant illustre un réseau de Feistel simple à quatre étages. Les algorithmes cryptographiques basés sur un réseau de Feistel diffèrent principalement dans le nombre d'étages et dans la nature de la fonction F.



Le message à chiffrer est décomposé en un flux de nombres appliqués aux entrées A et B du réseau. Les quatre clés secrètes K1, K2, K3 et K4 restent constantes pour le chiffrement du message. Les sorties Y et Z sont un flux de nombres représentant le message chiffré.

On constate qu'à chaque étage le signal du haut est combiné à la clé par la fonction F. On effectue ensuite un ou-exclusif bit à bit avec le signal du bas. À la fin de chaque étage, les signaux du haut et du bas sont interchangés pour le prochain étage.

Un réseau de Feistel à quatre étages est implémenté sur un FPGA. Tous les signaux du réseau ont 16 bits de large. Après implémentation, on a caractérisé les différentes parties du réseau comme suit. Les bascules ont un délai de 1 ns, un temps de préparation t_{su} de 0.25 ns, et un temps de maintien t_h de 0.1 ns. Les blocs de fonction F ont un délai de 5 ns, et les ou-exclusif ont un délai de 3 ns. Les fils d'interconnexion ont des délais de 0.1 ns chacun. Les blocs des clés K1, K2, K3 et K4 n'ont pas de délai, ce sont des constantes.

a. Identifiez le chemin critique du circuit sur le diagramme et donnez la fréquence maximale d'opération.

b. Pipeliner le circuit pour atteindre un débit de 50×10^6 résultats par seconde, où un résultat est une paire (Y, Z). Minimisez la latence.

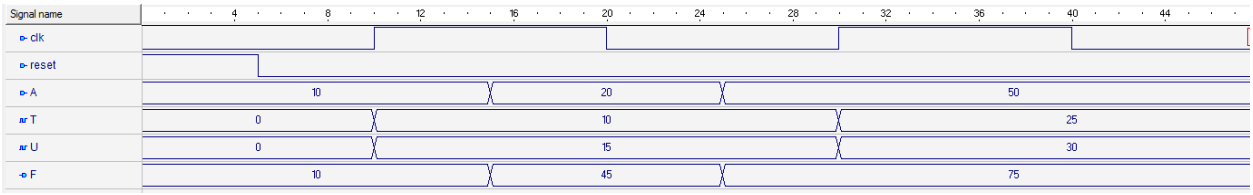
i. Montrez sur le diagramme où vous insérez des registres de pipeline

ii. Indiquez le nouveau chemin critique du circuit et donnez la fréquence maximale d'opération

iii. Donnez la nouvelle latence.

Solutions

Q1.



Q2.

1. Bloc des registres (il faut avoir le diagramme du bloc des registres ou en estimer le contenu).

Il faut 4 × 16 = 64 bascules.

Les deux multiplexeurs de sortie ont chacun 6 entrées : un bit par registre et deux bits pour le choix de la sortie. Donc il faut 1 LUT par bit pour chacun des multiplexeurs, donc 16 LUT chacun, donc 32 LUT.

Il faut 4 LUT pour les 4 portes ET.

Le décodeur a deux entrées et 4 sorties, il faut 4 LUT.

Total BR : 64 bascules, 40 LUT environ.

2. UAL

Les fonctions + et – peuvent être combinées, il faut 1 LUT par bit ajouté/soustrait, donc 16 LUT.

Les 6 fonctions logiques A, B, ET, OU, NON et OUX ont 5 entrées : les bits Ai et Bi, et 3 bits pour choisir quelle opération est faite. Donc il faut 16 LUT pour ces fonctions.

Finalement il faut choisir entre une somme ou une fonction logique pour chaque bit, donc 16 autres LUT.

Total UAL : environ 48 LUT.

3. Mémoire des données

Il y a 256 mots de 16 bits, donc il faut 4096 bits de mémoire en Block RAM.

4. Deux multiplexeurs

Les deux multiplexeurs nécessitent chacun 1 LUT par bit, soit 2 fois 16 LUT donc 32 LUT.

5. Grand total : environ 64 bascules, 120 LUT et 4096 bits de Block RAM.

(Le FPGA XC5VLX50T contient 28800 LUT, 28800 bascules, et un total de 2160 Kb de Block RAM).

Q3.

a. TPHL est mesuré du moment où le signal d'entrée passe à 50% de sa valeur jusqu'au moment où le signal de sortie passe à 50% de la sienne. Comme le signal d'entrée passe de 0 à 1 instantanément à t = 0, il faut trouver le moment où V_{out} a une valeur de Vo/2.

$V_{out} = V_0 \times e^{-t/RC}$

$V_{out}/Vo = e^{-t/RC}$

$0.5 = e^{-tPHL/RC}$

$t_{PHL} = -\ln(0.5) \times RC \approx 0.693 \times RC$

b. De par la relation, si on double R on double t_{PHL}

c. On calcule t_{PHL} = 6.93 ns.

Q4.

a. Le chemin critique va de la bascule pour le signal A à la bascule pour le signal Y, en passant par les quatre boîtes 'F' et les quatre ou-exclusifs. Le délai total est donné par :

délai bascule + 4 × délai ‘F’ + 4 × délai ‘oux’ + 9 × délai fil + tsu = 1 + 4 × 5 + 4 × 3 + 9 × 0.1 + 0.25 = 34.15 ns. La fréquence maximale d’horloge est 29.3 MHz

b. On insère un registre de pipeline à la sortie du 2^{e} étage.

Le chemin critique est alors délai bascule + 2 × délai ‘F’ + 2 × délai ‘oux’ + 5 × délai fil + tsu = 1 + 2 × 5 + 2 × 3 + 5 × 0.1 + 0.25 = 17.75 ns. La fréquence maximale d’horloge est 56.3 MHz. On peut alors opérer à une fréquence d’horloge de 50 MHz et atteindre un débit de 50 × 10^{6} résultats par seconde.

La latence est maintenant de 2 cycles, incluant le registre de pipeline et le registre des ports de sortie.