Nom : _____ Matricule : _____

INF3500 : Conception et réalisation de systèmes numériques

Examen intra #2 – 14 mars 2017

Durée: 1 heure. Documentation: Une feuille recto verso 8.5"×11" ou A4 permise.
Pondération: 10%. 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. **(1 point)** Considérez le code VHDL suivant. Donnez un schéma de portes logiques et d'éléments à mémoire correspondant.

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

entity cctsequentielex5 is
    port (
        clk, reset : in STD_LOGIC;
        X, Y : in STD_LOGIC;
        S1, S2 : out STD_LOGIC
    );
end cctsequentielex5;
```

```
architecture arch of cctsequentielex5 is
signal Q1, Q2 : std_logic;
begin
    process(CLK, reset) is
    begin
        if (reset = '0') then
            Q1 <= '0';
            Q2 <= '0';
        elsif (rising_edge(CLK)) then
            Q1 <= X and Q2;
            Q2 <= Q1 or Y;
        end if;
    end process;

    process(Q1, Q2) is
    begin
        S1 <= Q1 or Q2;
        S2 <= Q1 and Q2;
    end process;
end arch;
```

(*Utilisez le verso si nécessaire*)

Question 2. (3 points)

L'exponentiation modulaire est une fonction très utile en cryptographie. Elle est définie par $R = B^E \bmod M$. Par exemple, pour $B, E, M = \{5, 3, 32\}$, on a $R = 125 \bmod 32 = 29$. L'exponentiation modulaire est difficile à calculer directement pour de grands nombres (par exemple, quand B, E et M sont exprimés avec 512 bits ou plus). Il existe par contre un algorithme itératif qui permet d'obtenir la réponse en e cycles d'horloge, où e est le nombre de bits de E. On peut décrire cet algorithme avec les micro-opérations suivantes.

init : R ← 1, B ← B0, E ← E0, M ← M0, fini ← 0; init' ET E mod 2 = 1: R ← (R × B) mod M; init' : B ← (B × B) mod M;	init' : E ← E >> 1; init' ET E = 0 : fini ← 1

Donnez le diagramme d'un chemin des données correspondant à ces micro-opérations. Supposez que R, B et E sont exprimés avec W bits, que $M = 2^W$, que B0, E0 et M0 sont les valeurs entrées du système, et que init est un signal de contrôle pour démarrer les calculs.

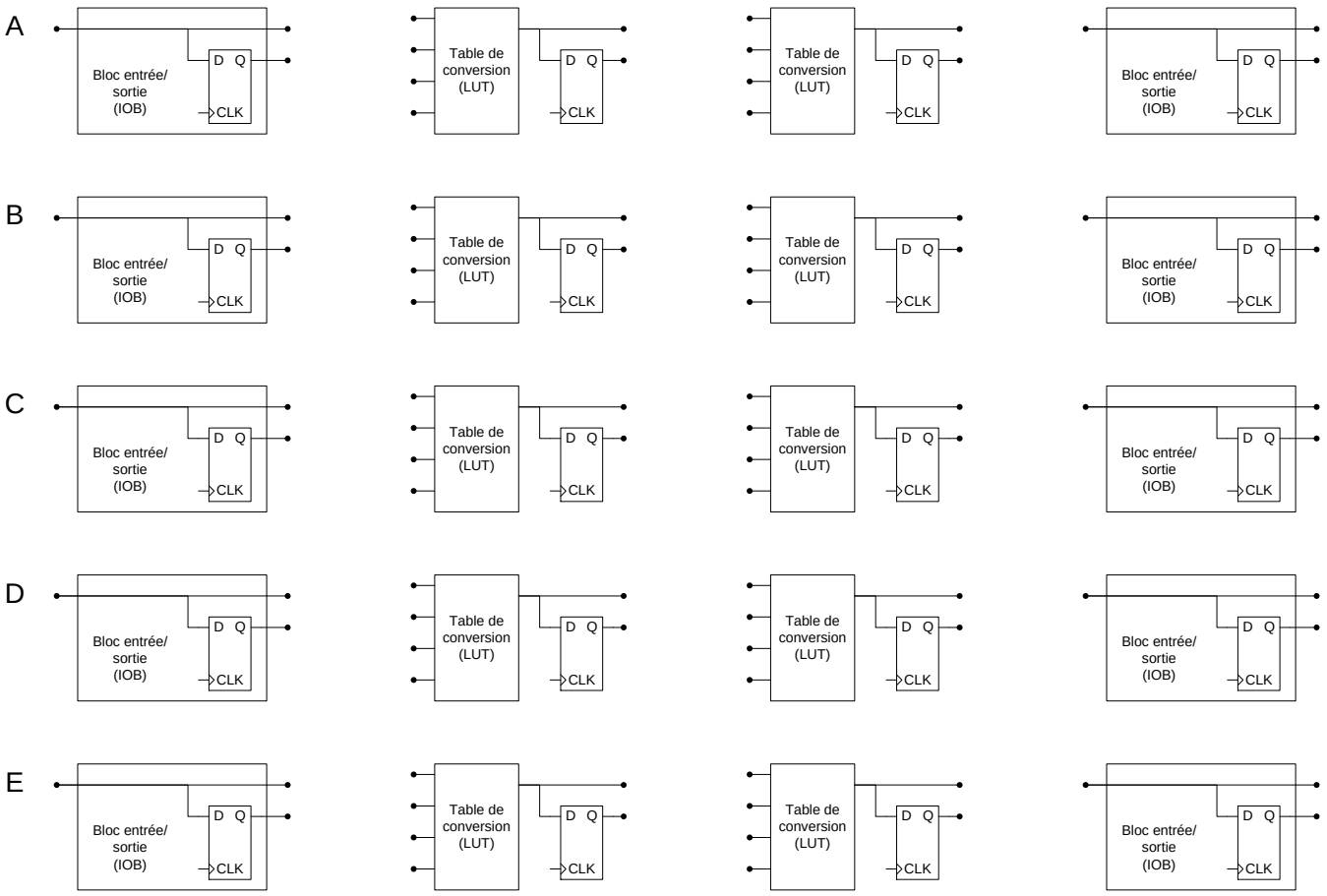
(utilisez le verso si nécessaire)

Question 3. (4 points)

Considérez le code VHDL et le modèle de FPGA suivants.

a. (1.5 points) Montrez, sur le modèle du FPGA, un résultat possible de la synthèse et de l'implémentation de ce code. Indiquez directement sur le dessin où les signaux et ports de sortie se situent ainsi que les interconnexions entre les blocs. Les interconnexions peuvent contourner les blocs. Indiquez quand une bascule doit être utilisée. Indiquez par une équation la fonction logique réalisée par chaque LUT que vous utilisez. Respectez l'assignation donnée pour les ports d'entrée.

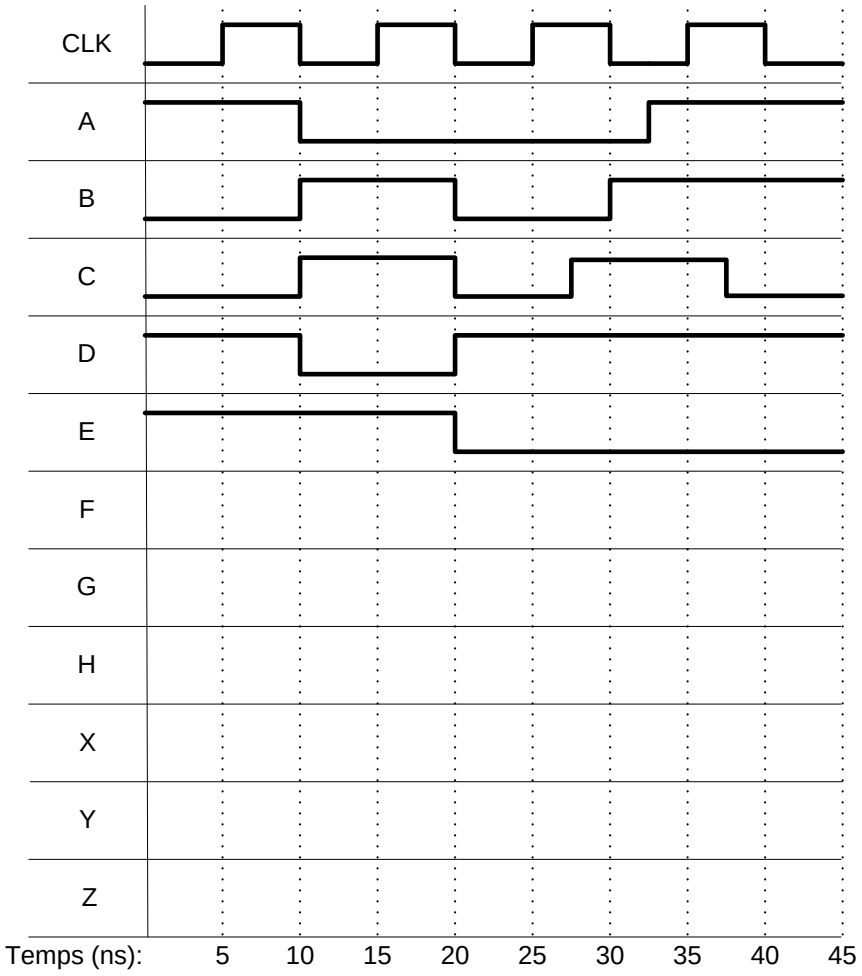
```
library ieee;
use ieee.std_logic_1164.all;

entity module10 is
   port (
      clk, A, B, C, D, E: in std_logic;
      X, Y, Z: out std_logic
   );
end module10;

architecture arch of module10 is

signal F, G, H : std_logic;

begin

   X <= not(A and B and E);
   Y <= G xor H;

   process(clk) is
   begin
      if rising_edge(CLK) then
         F <= A and B and C and D;
         G <= F xor E;
         H <= B or C or D;
      end if;
   end process;

   process(A, B, C)
   begin
      if A = '1' then
         Z <= B or C;
      else
         Z <= B and C;
      end if;
   end process;

end arch;
```



b. (0.5 point) Donnez le contenu de la LUT qui implémente la fonction pour le signal Z. Identifiez clairement les entrées.

				Z
0	0	0	0	
0	0	0	1	
0	0	1	0	
0	0	1	1	
0	1	0	0	
0	1	0	1	
0	1	1	0	
0	1	1	1	
1	0	0	0	
1	0	0	1	
1	0	1	0	
1	0	1	1	
1	1	0	0	
1	1	0	1	
1	1	1	0	
1	1	1	1	

c. (1.5 points) Complétez le chronogramme suivant pour ce code VHDL.



d. (1.5 points) Combien de vecteurs de test seraient requis, au minimum, pour effectuer un test exhaustif de l'entité `module10`? Justifiez complètement votre réponse.

Question 4. (2 points)

Considérez le chemin des données suivant pour implémenter l'algorithme de division de Goldschmidt.

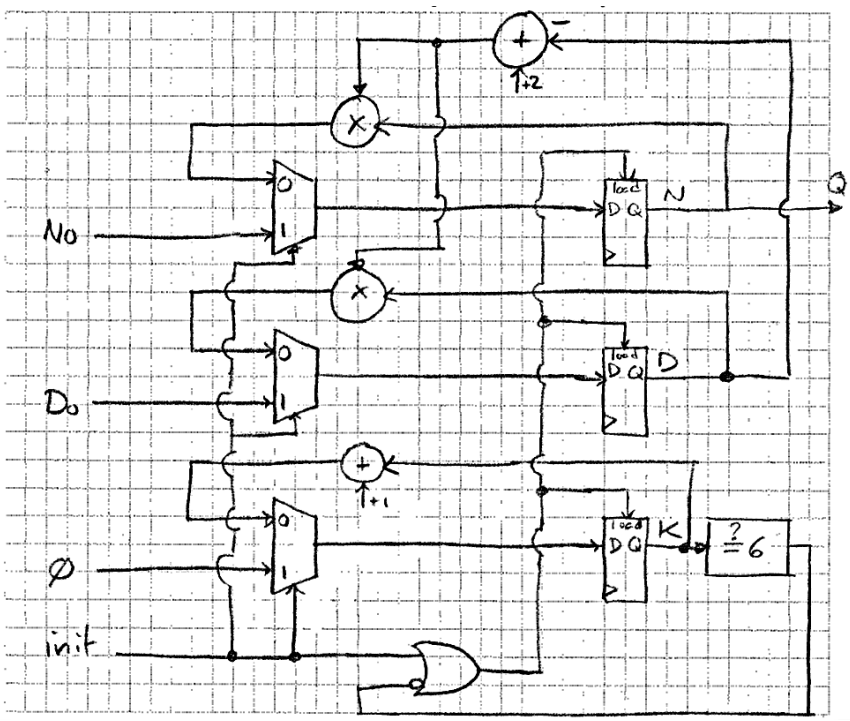
Dans le schéma, les registres N et D et les signaux N_0 et D_0 ont chacun 16 bits de large.

Le registre K a 3 bits de large.

Le signal init a un seul bit.

Estimez le nombre de ressources nécessaires en termes de tables de conversion (LUT), bascules (FF) et tranches DSP48 pour implémenter ce chemin des données sur un FPGA de la famille Virtex 7 de Xilinx.

Justifiez complètement votre réponse.



	nombre	Justification
#LUT		
#FF		
#DSP48E1		