

Contrôle final du cours : Système Digital.
Corrigé.

Question 1 (Soustracteur binaire complet) 1. Réaliser un circuit combinatoire $\bar{a}bc$ dont les deux sorties s, r sont reliées aux trois entrées a, b, c par la relation

$$a - b + c = -s + 2r. \quad (1)$$

2. Réaliser un circuit combinatoire $a\bar{b}\bar{c}$ dont les deux sorties s, r sont reliées aux trois entrées a, b, c par la relation

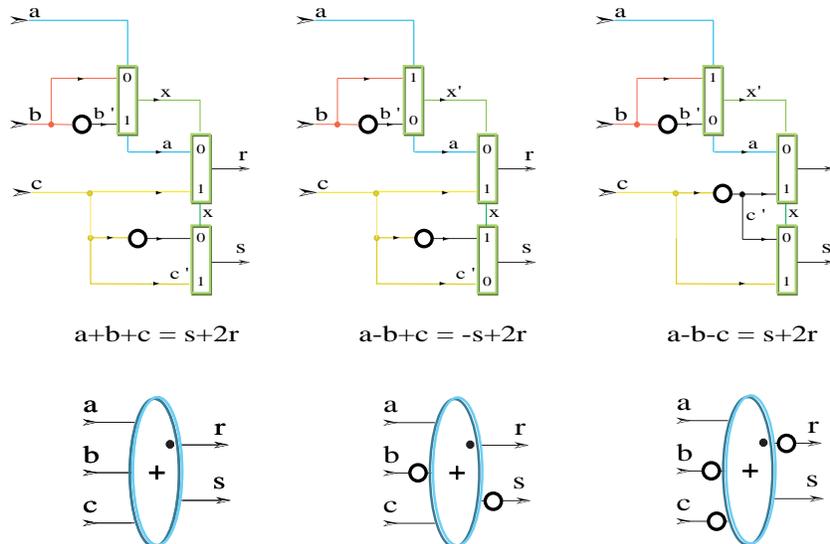
$$a - b - c = s - 2r. \quad (2)$$

Réponse 1 L'additionneur binaire complet calcule la solution de l'équation

$$a + \beta + \gamma = \sigma + 2\rho. \quad (3)$$

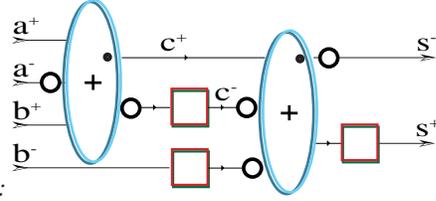
1. En posant $\beta = 1 - b$, $\sigma = 1 - s$ et $\gamma = c$, $\rho = r$ on transforme l'équation (3) en (1). Le circuit $\bar{a}bc$ est donc un additionneur binaire complet dont on inverse l'entrée b et la sortie s .

2. En posant $\beta = 1 - b$, $\gamma = 1 - c$, $\rho = 1 - r$ et $\sigma = s$ on transforme (3) en (2). Le circuit $a\bar{b}\bar{c}$ est donc un additionneur binaire complet dont on inverse les entrées b, c et la sortie r .



Les schémas ci-dessus montrent que les circuits $\bar{a}bc$ et $a\bar{b}\bar{c}$ sont réalisables en cinq **mux**, tout comme abc . Ils donnent aussi les icônes utilisées pour représenter ces circuits par la suite.

- Question 2 (Additionneur série par les poids forts)** 1. Réaliser un circuit synchrone $S = \mathcal{A}(A, B)$ tel que : $S = \frac{A+B}{4}$.
2. Est-il possible de réaliser un additionneur en série, par les poids forts, qui calcule $S = \frac{A+B}{2}$?



Réponse 2 1. Considérons le circuit :

L'invariant (1) de la porte $\bar{a}bc$ donne : $a^+ - a^- + b^+ = -c' + 2c^+$;

celui (2) de $\bar{a}bc$: $c^+ - c^- - b' = s' - 2s^-$.

Pour les trois registres, on a : $c^- = \frac{c'}{2}$, $b' = \frac{b^-}{2}$ et $s^+ = \frac{s'}{2}$. En substituant :

$$s^+ - s^- = \frac{a^+ - a^- + b^+ - b^-}{4}.$$

2. La fonction $Y = f(A, B)$ calculée par un circuit en série est nécessairement causale : le chiffre de sortie y_N au temps $N \in \mathbf{N}$ ne dépend que des chiffres d'entrée vus à ce point :

$$y_N = f_N(a_0 \cdots a_N b_0 \cdots b_N),$$

où $f_N \in \mathbf{B}^{2(N+1)} \mapsto \mathbf{B}$ est une fonction combinatoire (booléenne sans mémoire).

Considérons le calcul par un circuit causal : $Y = f(A, B) = (A + B)/2$. Le bit de sortie au cycle 0 ne dépend que de a_0 et b_0 : $y_0 = f_0(a_0, b_0)$. Observons sa valeur, pour l'entrée : $a_0 = 1, b_0 = 0$. Si $y_0 = 0$ ou $y_0 = \bar{1}$, la demi somme est fautive pour l'entrée $a_{N+1} = b_{N+1} = 1$: $(a+b)/2 = \frac{3}{2} > 1$, alors que $Y \leq 1$. Si $y_0 = 1$, la demi somme est fautive pour l'entrée $a_{N+1} = b_{N+1} = \bar{1}$: $(a+b)/2 = -\frac{1}{2} < 0$, alors que $Y \geq 0$. Conclusion : il n'y a pas de circuit causal pour calculer $(A + B)/2$.

- Question 3 (Multiplicateur série par les poids forts)** 1. Réaliser un multiplicateur \mathcal{M}_c par la constante $c = \frac{7}{32}$.
2. Décrire une structure générale de multiplicateur \mathcal{M}_c par le nombre dyadique $c = \frac{n}{2^p}$.
3. Pour quelles valeurs de c \mathcal{M}_c est-il réalisable ?

Réponse 3 1. Partant de la décomposition $P = \frac{7A}{32} = \frac{1}{4}(A - \frac{A}{8})$, on arrive à :

$$P = \mathcal{M}_{\frac{7}{32}}(A) = S(A, \text{reg}(\text{reg}(\text{reg}(A)))).$$

La soustraction en série par les poids forts s'obtient en composant l'additionneur de la question 2 avec le circuit de l'exemple 1 : $\mathcal{O}(B) = -B$, soit $S(A, B) = \mathcal{A}(A, \mathcal{O}(B))$. Toutes les variables dans ces circuits sont représentées par deux bits rbs, présentés en série par les poids forts.

2. La réponse à la question 6 montre que $c \leq 1/3$ est équivalent à l'existence d'une rbsn dont les deux premiers chiffres soient nuls : $c_0 = c_1 = 0$, et $c_N \times c_{N+1} = 0$ pour $N \in \mathbf{N}$.

La multiplication égyptienne (binaire) par les poids faibles de c donne :

$$\begin{aligned} P_{N-1} &= c_{N-1}A, \\ P_{N-2-k} &= c_{N-2-k}A + \frac{P_{N-1-k}}{2}, \end{aligned}$$

pour $0 \leq k < N-1$. On ne conserve que le produit final : $P_0 = c \times A$.

La structure du circuit $P = \mathcal{M}_c(A)$ se calque sur les étapes de la multiplication égyptienne. On groupe une étape dont le chiffre $c_N \neq 0$ est non nul, avec la suivante, dont on sait que le chiffre $c_{N+1} = 0$ est nul. Il y a trois cas de réalisation pour chaque chiffre $c = c_N \in \mathcal{S}$: registres, additionneur \mathcal{A} , ou soustracteur \mathcal{S} en série :

$$\begin{aligned} c = 0 & & P_{N-2-k} &= \mathbf{reg}(P_{N-1-k}); \\ c = 10 & & P_{N-3-k} &= \mathcal{A}(A, \mathbf{reg}(P_{N-1-k})); \\ c = \bar{1}0 & & P_{N-3-k} &= \mathcal{S}(\mathbf{reg}(P_{N-1-k}), A). \end{aligned}$$

Le multiplicateur $\mathcal{M}_{c_0 \dots c_{N-1}}$ comprend N registres et $m(c)$ additionneurs \mathcal{A} . Ici, $m(c) = \sum |c_N|$ est le nombre de chiffres non nuls dans la rbsn du nombre c . On a : $\text{Max}(m(c)) = \frac{N}{2}$, et $\text{Moy}(m(c)) = \frac{N}{3}$, d'après la réponse à la question 7.

3. On peut se limiter à $c \geq 0$, puisque $(-c) \times A = -(c \times A)$.

Signalons les cas triviaux $c \in \{0, 1, \frac{1}{2}\}$. Hors de ces cas triviaux, nous devons montrer que $c \times A$ n'est pas causal si :

$$c = \frac{1}{2}(c_N) > \frac{1}{3} = \frac{1}{2}00(01).$$

Montrons le d'abord quand $c \geq 3/4 = \frac{1}{2}011$: on écrit $c = 1/2 + c'/4$, avec $c' \geq 1$, et on pose $B = c'A/2$ dans l'argument $cA = (A+B)/2$ de la réponse 2.2.

Considérons ensuite le cas $c > 1/3$; dans toute rbs de c , il y a nécessairement deux chiffres consécutifs tels que : $c_k = c_{k+1} = 1$, et $c_N c_{N+1} = 0$ pour $N < k$. Par l'algorithme de multiplication qui précède, on peut décomposer $A \times \frac{1}{2}c_0 \dots c_{k-2}011c_{k+2} \dots$ en une suite d'opérations causales $(A/2, (A+B)/4, -A)$, dont le dernier argument est le produit $A \times \frac{1}{2}011c_{k+2} \dots = A \times c'$. Comme $c' \geq 3/4$, nous savons qu'il n'est pas causal.

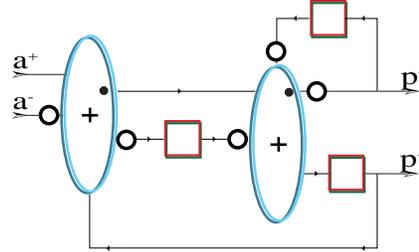
Question 4 (Diviseur série par les poids forts) 1. Réaliser un circuit de division par 3, en série par les poids forts : $P = \mathcal{M}_{\frac{1}{3}}(A) = \frac{A}{3}$.

2. Décrire une structure de multiplicateur par la constante $c = \frac{n}{d} \in \mathbf{Q}$. Pour quelles valeurs de c est-il réalisable ?

Réponse 4 1. La représentation binaire de $1/3$ est :

$$\frac{1}{3} = \frac{1}{4} \left(1 + \frac{1}{3}\right) = \frac{1}{2} 0(01).$$

On a donc $P = \frac{A}{3} = \frac{1}{4} \left(A + \frac{A}{3}\right) = \mathcal{S}(A, P)$, ce qui amène le circuit suivant de division par trois $\mathcal{M}_{\frac{1}{3}}$:



2. Le Multiplicateur \mathcal{M}_c par la constante c est causal si $|c| \leq \frac{1}{3}$. Un nombre rationnel $c = \frac{n}{d}$ admet une rbsn qui est ultimement périodique :

$$c = \frac{n}{d} = \frac{1}{2} c_0 \cdots c_{i-1} (c_i \cdots c_{i+p-1}),$$

où $i \in \mathbf{N}$ est la longueur de la partie initiale, $p \in \mathbf{N}$ est la longueur de la partie périodique, et $c_0 = c_1 = c_{\mathbf{N}} c_{\mathbf{N}+1} = 0$. Quitte à allonger la partie initiale, on peut supposer $c_{i+p-1} = 0$. Reprenons les équations de la multiplication égyptienne, à une substitution près de la condition initiale :

$$P_{i+p-1} = \frac{P_i}{2},$$

$$P_k = c_k A + \frac{P_{k+1}}{2}.$$

Le multiplicateur résultant a la même structure que le multiplicateur par le nombre dyadique $c = \frac{n}{d} = \frac{1}{2} c_0 \cdots c_{i-1} c_i \cdots c_{i+p-1}$, sauf que l'entrée de la tranche finale $i + p - 1$ reprend la sortie de la tranche i , pour former une boucle en retour - feedback.

Question 5 (Algorithme de calcul d'une rbs) Soit $R \in [-2, 2]$ un nombre réel, défini par deux applications rationnelles calculables $g, d \in \mathbf{N} \mapsto \mathbf{Q}$ telles que :

- (i) $-2 \leq g(0) < \cdots < g(\mathbf{N}) < g(\mathbf{N}+1) < \cdots < d(\mathbf{N}+1) < d(\mathbf{N}) < \cdots < d(0) \leq \frac{2}{2}$
- (ii) $\forall \mathbf{N} \in \mathbf{N} : d(\mathbf{N}) - g(\mathbf{N}) < 2^{1-\mathbf{N}}$.

Il résulte directement de (i) et (ii) que :

$$R = \lim_{\mathbf{N} \rightarrow \infty} g(\mathbf{N}) = \lim_{\mathbf{N} \rightarrow \infty} d(\mathbf{N}).$$

Donner un algorithme de calcul d'une rbs de R :

$$R = \frac{1}{2}r_0r_1 \cdots r_N \cdots = \sum r_N 2^{-N},$$

avec $r_N \in \{\bar{1}, 0, 1\}$.

Réponse 5 Posons $R_0 = R, g_0 = g, d_0 = d$ et calculons, de proche en proche pour $N \in \mathbf{N}$, la suite des réels calculables $R_N = g_N(\infty) = d_N(\infty)$, donnés par les fonctions rationnelles $g_N, d_N \in \mathbf{N} \mapsto \mathbf{Q}$ qui satisfont (i) et (ii), tels que :

$$R = \frac{1}{2}r_0r_1 \cdots r_{N-1} + 2^{-N}R_N.$$

Par (ii), on a $d_N(1) - g_N(1) < 1$ et trois cas se présentent :

1. $g_N(1) < -1$: choisir $r_N = \bar{1}$;
2. $-1 \leq g_N(1) < d_N(1) \leq 1$: choisir $r_N = 0$;
3. $1 < d_N(1)$: choisir $r_N = 1$.

On pose alors $R_{N+1} = 2(R_N - r_N)$ et on vérifie, dans les trois cas, que $-2 \leq R_{N+1} \leq 2$. Pour tout entier $k \in \mathbf{N}$, définissons alors : $g_{N+1}(k) = 2(g_N(k+1) - r_N)$, et $d_{N+1}(k) = 2(d_N(k+1) - r_N)$. On a $g_{N+1}(k) < 2(g_N(k+2) - r_N) = g_{N+1}(k+1)$, et $d_{N+1}(k) > d_N(k+1)$. Donc, g_{N+1}, d_{N+1} vérifient (i). Comme $d_{N+1}(k) - g_{N+1}(k) = 2(d_N(k+1) - g_N(k+1)) < 2 \times 2^{-k} = 2^{1-k}$, on a aussi (ii).

Question 6 (Représentation binaire signée normale : rbsn)

1. Montrer qu'il existe (sous des hypothèses que l'on précisera) une représentation normale rbsn du nombre réel

$$R = \frac{1}{2}r_0r_1 \cdots r_N \cdots = \sum r_N 2^{-N},$$

dans laquelle le chiffre r_{N+1} suivant tout chiffre $r_N \in \{\bar{1}, 1\}$ non nul est nul : $r_N r_{N+1} = 0$ pour tout $N \in \mathbf{N}$.

Exemple :

$$\frac{11}{16} = \frac{1}{2}10\bar{1}0\bar{1}.$$

2. Décrire l'algorithme de calcul de la rbsn d'un nombre rationnel : $R = \frac{n}{d} \in \mathbf{Q}$. Caractériser les suites de chiffres obtenues.
3. La rbsn est elle unique ?
4. Considérons un circuit normaliseur : son entrée est une rbs de R , sa sortie une rbsn. S'il en existe un, le construire. Sinon, montrer pourquoi !

Réponse 6 1. Pour qu'il existe une rbsn, il est nécessaire que $|R| \leq \frac{4}{3} = \frac{1}{2}(10)$. Pour montrer que cette condition est aussi suffisante, posons $R_0 = \bar{R}$ et calculons de proche en proche, pour $N \in \mathbf{N}$, la suite des chiffres r_N de

$$R = \frac{1}{2}r_0r_1 \cdots r_{N-1} + 2^{-N}R_N.$$

Trois cas principaux se présentent :

- (a) $R_N < -\frac{2}{3}$: choisir $r_N = \bar{1}$;
 (b) $-\frac{2}{3} < R_N < \frac{2}{3}$: choisir $r_N = 0$;
 (c) $R_N > \frac{2}{3}$: choisir $r_N = 1$.

Pour les valeurs $R = \pm\frac{2}{3}$ non traitées, le choix $r_N \in \{0, 1, \bar{1}\}$ est arbitraire : $\frac{2}{3} = \frac{1}{2}(01) = \frac{1}{2}1(0\bar{1})$.

Dans tous les cas, posons $R_{N+1} = 2(R_N - r_N)$ et vérifions que : $|R_{N+1}| \leq \frac{4}{3}$. Pour $r_N \neq 0$, on trouve la condition plus forte $|R_{N+1}| \leq \frac{2}{3}$, qui implique $r_{N+1} = 0$, et donc la condition de normalisation : $r_N r_{N+1} = 0$.

2. La représentation rbsn d'un nombre rationnel $R = \frac{n}{d} \in \mathbf{Q}$ tel que $|R| \leq \frac{4}{3}$ est ultimement périodique :

$$R = \frac{n}{d} = \frac{1}{2}r_0 \cdots r_{i-1}(r_i \cdots r_{i+p-1}).$$

On cherche la période en testant, dans l'algorithme de la question précédente, si chaque nouveau nombre R_{N+1} est égal à l'un des R_k déjà calculés pour $k < N + 1$. Quand $R \in \mathbf{Q}$ est un nombre rationnel, ce test est possible car tous les $R_N \in \mathbf{Q}$ sont aussi des nombres rationnels. La période est identifiée et l'algorithme termine, quand on trouve : $R_{p+i} = R_i$.

3. La rbsn est elle unique ? Non, puisque : $\frac{2}{3} = \frac{1}{2}(01) = \frac{1}{2}1(0\bar{1}) = 1 - \frac{1}{3}$. Les nombres de la forme $R = \pm\frac{2^{-N}}{3}$ - c'est à dire ceux dont la représentation binaire usuelle est ultimement périodique, de période (01) - ont donc deux rbsn. Pour les autres nombres réels, la rbsn est unique.
4. Soit C un nombre réel calculable arbitraire tel que $|C| < \frac{2}{3}$. Le premier chiffre de la rbsn de $C + \frac{2}{3}$ vaut : 0 si $C < 0$, et 1 si $C > 0$; les deux choix sont possibles quand $C = 0$. Un circuit normaliseur permettrait donc de décider, en en temps fini, entre $C \leq 0$ et $C \geq 0$. Le cours montre que cette question est indécidable, pour C calculable arbitraire. Il n'existe donc pas de circuit normaliseur.

Question 7 (Entropie de la rbsn) Soit R un réel aléatoire, résultant d'un tirage uniforme sur l'intervalle $-1 < R < 1$. On en considère une (la ?) rbsn :

$$R = \frac{1}{2}r_0r_1 \cdots r_N \cdots = \sum r_N 2^{-N},$$

avec $r_N r_{N+1} = 0$ pour tout N .

1. Calculer les probabilités des trois symboles de R : $r_N \in \{\bar{1}0, 0, 10\}$.
2. Calculer l'entropie $H = \sum_{s \in \{\bar{1}, 0, 1\}} Pr(s) \log_2 \frac{1}{Pr(s)}$ de cette source.
3. Montrer qu'il existe un code binaire optimal de R , de longueur moyenne égale à l'entropie H .
4. Quel est le nombre moyen des chiffres non nuls de R : $Pr(r_N \neq 0)$?

Réponse 7 1. Comme le tirage est uniforme sur $[-\frac{4}{3}, \frac{4}{3}]$ la probabilité de chaque symbole $r_N \in \{\bar{1}0, 0, 10\}$ est proportionnelle à la longueur de l'intervalle correspondant, divisée par $8/3$, soit : $Pr(0) = 1/2$, et $Pr(1) = Pr(\bar{1}) = 1/4$.

2. L'entropie vaut : $H = -\log_2(1/2)/2 - \log_2(1/4)/4 - \log_2(1/4)/4 = 1.5$ Sh.
3. La longueur moyenne $m = l(0)/2 + l(10)/4 + l(\bar{1}0)/4$ du code $c(0) = 0, c(10) = 10, c(\bar{1}0) = 11$ est égale à l'entropie : $m = H = 1.5$.
4. Partons d'une suite binaire $S = s_0 \cdots s_{l-1}$ de longueur $l \in \mathbf{N}$, qui soit aléatoire équiprobable : $Pr(s_k = 0) = Pr(s_k = 1) = \frac{1}{2}$. On obtient une suite aléatoire $R_{\mathbf{N}} = r_0 \cdots r_{\mathbf{N}-1}$ de \mathbf{N} chiffres $r_k \in \{\bar{1}, 0, 1\}$, en substituant dans S chaque bit non nul $s_k = 1$ par les chiffres 10 ou $\bar{1}0$, au hasard équiprobable. La longueur moyenne de R est donnée par $\mathbf{N} = l \times (Pr(0) + 2Pr(10) + 2Pr(\bar{1}0)) = 3l/2$. Le nombre moyen de chiffres non nuls de R est donc : $Pr(r_{\mathbf{N}} \neq 0) = \mathbf{N}/3$.

Avec un peu de travail, on peut préciser cette réponse. Soit $\mathcal{R}_{\mathbf{N}}$ l'ensemble des nombres réels dont tous les chiffres de la rbsn sont nuls, à partir du rang \mathbf{N} . Comme cette rbsn commence forcément par 0, 10 ou $\bar{1}0$, la taille $R_{\mathbf{N}} = |\mathcal{R}_{\mathbf{N}}|$ de cet ensemble est donnée par : $R_0 = 1, R_1 = 3$ et $R_{\mathbf{N}+2} = R_{\mathbf{N}+1} + 2R_{\mathbf{N}}$.

La série génératrice $R(z) = \sum R_{\mathbf{N}}z^{\mathbf{N}}$ est solution de l'équation : $R(z) - 1 - 3z = z(R(z) - 1) + 2z^2R(z)$, soit :

$$R(z) = \frac{1 + 2z}{1 - z - 2z^2} = \frac{1}{3} \left(\frac{4}{1 - 2z} - \frac{1}{1 + z} \right).$$

En développant, on trouve la formule explicite :

$$R_{\mathbf{N}} = \frac{1}{3}(2^{\mathbf{N}+2} - (-1)^{\mathbf{N}}).$$

Soit $U_{\mathbf{N}}$ le nombre de chiffres non nuls, dans l'écriture rbsn des nombres dyadiques $r \in \mathcal{R}_{\mathbf{N}}$. On a : $U_0 = 0, U_1 = 2$ et $U_{\mathbf{N}+2} = U_{\mathbf{N}+1} + U_{\mathbf{N}} + 2R_{\mathbf{N}}$. La série génératrice $U(z) = \sum U_{\mathbf{N}}z^{\mathbf{N}}$ est solution de l'équation : $U(z) - 2z = zU(z) + z^2U(z) + 2z^2R(z)$, soit :

$$U(z) = \frac{2z}{(1 - z - 2z^2)^2} = \frac{2z}{27} \left(\frac{20 - 16z}{(1 - 2z)^2} + \frac{7 + 4z}{(1 + z)^2} \right).$$

En développant, on trouve la formule explicite :

$$U_{\mathbf{N}} = \frac{2}{27} ((3\mathbf{N} + 2)2^{\mathbf{N}+1} - (3\mathbf{N} + 4)(-1)^{\mathbf{N}}).$$

Le nombre moyen de chiffres non nuls dans les rbsn de $\mathcal{R}_{\mathbf{N}}$ est donné par :

$$U_{\mathbf{N}}/R_{\mathbf{N}} = \frac{\mathbf{N}}{3} + \frac{2}{9} + O(\mathbf{N}2^{-\mathbf{N}}).$$

A la limite $\mathbf{N} \mapsto \infty$, nous retrouvons bien : $Pr(r_{\mathbf{N}} \neq 0) = 1/3$.