1 Définition d'un automate et déterminisation

Soit $\Sigma = \{ a, b \}$.

Soit A l'ensemble des mots de longueur supérieure à 1 tels que le premier et le dernier symbole sont identiques. Par exemple, $\{ bb, ababaaba \} \subseteq A$, mais $A \cap \{ abaab, a, \epsilon \} = \emptyset$.

1. Construire un AFN N qui accepte A.
2. Donner le graphe de transitions de N.
3. Déterminiser N par la construction des sous-ensembles.
4. Donner le graphe de transitions du résultat.

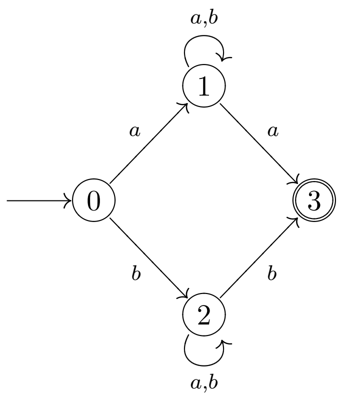
Corrigé :

1. Construire un AFN N qui accepte A.

$Q_N \stackrel{\text{def}}{=} \{0, 1, 2, 3\}$
$\Sigma \stackrel{\text{def}}{=} \{a, b\}$
$S_N \stackrel{\text{def}}{=} 0$
$F_N \stackrel{\text{def}}{=} \{3\}$

	a	b
S0	1	2
1	1,3	1
2	2	2,3
F3		

2. Donner le graphe de transitions de N.



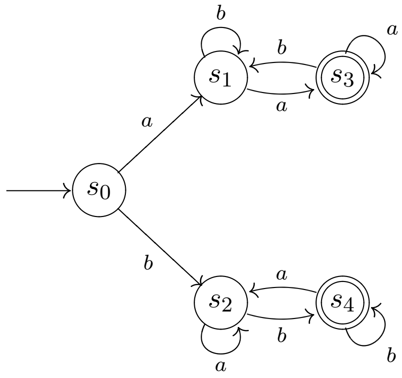
3. Déterminiser N par la construction des sous-ensembles.

$Q_M \stackrel{\text{def}}{=} \{\{0\}, \{1\}, \{2\}, \{1, 3\}, \{2, 3\}\}$
$\Sigma \stackrel{\text{def}}{=} \{a, b\}$
$s_M \stackrel{\text{def}}{=} \{0\}$
$F_M \stackrel{\text{def}}{=} \{\{1, 3\}, \{2, 3\}\}$

	a	b
S{0}	{1}	{2}
{1}	{1,3}	{1}
{2}	{2}	{2,3}
F{1,3}	{1,3}	{1}
F{2,3}	{2}	{2,3}

On peut facilement vérifier que les sous-ensembles $\{0, 1\}$, $\{0, 2\}$, $\{0, 3\}$, $\{1, 2\}$, $\{0, 1, 2\}$, $\{0, 1, 3\}$, $\{0, 2, 3\}$, $\{1, 2, 3\}$, $\{0, 1, 2, 3\}$ décrivent des états qui ne sont pas atteignables.

4. Donner le graphe de transitions du résultat.



où

$$s_0 \stackrel{\text{def}}{=} \{0\} \quad s_1 \stackrel{\text{def}}{=} \{1\} \quad s_2 \stackrel{\text{def}}{=} \{2\} \quad s_3 \stackrel{\text{def}}{=} \{1,3\} \quad s_4 \stackrel{\text{def}}{=} \{2,3\}$$

2 Définition d'un automate

Soit $\Sigma = \{\, a, b \,\}$. Soit $A \subseteq \Sigma^*$ un langage régulier, et $\mathrm{D}(A)$ défini par :

$$\mathrm{D}(A) \stackrel{\text{def}}{=} \Big\{ w \in \Sigma^* \mid (\exists v \in A) \; \big(\quad |w| = |v| \\ \wedge \quad (\exists\, 1 \leq k \leq |w|)\; (\forall\, 1 \leq i \leq |w|)\; (\, i \neq k \implies w_i = v_i \,) \,\big) \Big\}$$

Reformuler tel que :

$$\mathrm{D}(A) \stackrel{\text{def}}{=} \Big\{ w \in \Sigma^* \mid w \in A \;\vee\; (\exists\, 1 \leq k \leq |w|)(\; w_1 \cdots w_{k-1} \overline{w_k} w_{k+1} \cdots w_{|w|} \in A \;) \Big\}$$

Soit $M = (Q, \Sigma, \delta, s, F)$ un AF**D** avec $L(M) = A$.
Nous définissons le AF**N** $M' = (Q', \Sigma, \Delta, S, F')$ par

$$\begin{array}{ccl} Q' & \stackrel{\text{def}}{=} & Q \times \{\, 0, 1 \,\} \\ S' & \stackrel{\text{def}}{=} & \{\, (s, 0) \,\} \\ F' & \stackrel{\text{def}}{=} & \{\, (p, 0), (p, 1) \mid p \in F \,\} \\ \Delta(\, (p, f), x \,) & \stackrel{\text{def}}{=} & \{\, (\, \delta(p, x), f \,) \,\} \cup \{\, (\, \delta(p, \overline{x}), 1 \,) \mid f = 0 \,\} \end{array}$$

L'idée de cette définition est que M' peut se comporter exactement comme M : dans ce cas, le paramètre f d'erreur reste inchangé. Mais, M' peut aussi se comporter de manière différente comparée avec M : dans ce cas, on marque une erreur dans la transition de M' exactement dans le cas où M accepterait le symbole complémentaire du symbole x qui est traité dans l'étape indiquée. Noter que l'on peut faire une seule erreur, d'où la condition $f = 0$.

Lemme 1 *Pour tout $w \in \Sigma^*$ (avec $n = |w|$), et pour tout $(p, f) \in \widehat{\Delta}(S, w)$:*

1. *si $f = 0$, alors $\widehat{\delta}(s, w) = p$;*
2. *si $f = 1$, alors $\exists 1 \leq k \leq n : \widehat{\delta}(s, w_1 \cdots w_{k-1} \overline{w_k} w_{k+1} \cdots w_n) = p$.*

Preuve. Par induction sur $w \in \Sigma^*$ (où sur la longueur $|w|$)

cas ϵ Il suffit d'observer que $\widehat{\Delta}(S, \epsilon) = \{\, (s, 0) \,\}$ et $\widehat{\delta}(s, \epsilon) = s$. $\quad\surd$

cas $wx \in \Sigma^*$ Nous supposons que le lemme est vrai pour $w \in \Sigma^*$.

Nous allons démontrer qu'il est alors aussi vrai pour $wx \in \Sigma^*$ où $x \in \Sigma$.

Par définition, $\widehat{\Delta}(S, wx) = \bigcup_{(q,f)\in\widehat{\Delta}(S,w)} \Delta(\,(q, f), x\,)$.

Nous procédons par analyse des cas de $(q, f) \in \widehat{\Delta}(S, w)$ pour traiter tous les éléments de $\widehat{\Delta}(S, wx)$. Dans chaque cas, on peut appliquer la hypothèse de l'induction.

cas $f = 0$ Par induction, $\widehat{\delta}(s, w) = q$.

Par définition nous avons

$$\widehat{\Delta}(\,(q, 0), x\,) = \{\,(\,\delta(q, x), 0\,)\,\} \cup \{\,(\,\delta(p, \overline{x}), 1\,)\,\} \subseteq \widehat{\Delta}(S, wx)$$

cas $(p, f) = (\,\delta(q, x), 0\,) \in \widehat{\Delta}(S, wx)$

Par définition, $\widehat{\delta}(s, wx) = \delta(\widehat{\delta}(s, w), x) = \delta(q, x) = p$. $\surd$

cas $(p, f) = (\,\delta(p, \overline{x}), 1\,) \in \widehat{\Delta}(S, wx)$

Par définition, $\widehat{\delta}(s, w\overline{x}) = \delta(\widehat{\delta}(s, w), \overline{x}) = \delta(q, \overline{x}) = p$.

Donc, nous définissons $k \stackrel{\text{def}}{=} |w| + 1$.

Puis, nous observons que $\widehat{\delta}(s, w_1 \cdots w_{|w|}\overline{x}) = p$. $\surd$

cas $f = 1$ Par induction, $\exists 1{\le}k{\le}n : \widehat{\delta}(s, w_1 \cdots w_{k-1}\overline{w_k}w_{k+1} \cdots w_n) = q$.

Par définition nous avons

$$\widehat{\Delta}(\,(q, 1), x\,) = \{\,(\,\delta(q, x), 1\,)\,\} \subseteq \widehat{\Delta}(S, wx)$$

Il existe alors un seul cas/élément à observer.

cas $(p, f) = (\,\delta(q, x), 1\,)$

Soit $\overline{w} = w_1 \cdots w_{k-1}\overline{w_k}w_{k+1} \cdots w_n$

Par définition, $\widehat{\delta}(s, \overline{w}x) = \delta(\widehat{\delta}(s, \overline{w}), x) = \delta(q, x) = p$.

En reprenant le même k de l'induction, nous observons que

$\widehat{\delta}(s, \overline{w}x) = \widehat{\delta}(s, w_1 \cdots w_{k-1}\overline{w_k}w_{k+1} \cdots w_n x) = p$. $\surd$

$\blacksquare$

Lemme 2 $L(M') = \mathrm{D}(L(M))$.

Preuve.

$L(M')$	$=$	$\{\,w \mid \widehat{\Delta}(S, w) \cap F' \neq \emptyset\,\}$	par déf. de M' et $L(M')$
	$=$	$\{\,w \mid \exists(p, f) \in \widehat{\Delta}(S, w) \wedge p \in F\,\}$	par déf. de F'
	$=$	$\{\,w \mid \widehat{\delta}(s, w) \in F \vee (\exists k : \widehat{\delta}(s, w_1 \cdots \overline{w_k} \cdots w_n) \in F\,\}$	par Lemme 1
	$=$	$\mathrm{D}(L(M))$	par déf. de $\mathrm{D}(\cdot)$

$\blacksquare$

Corollaire 3 $L(M') = \mathrm{D}(A)$.

Preuve. Avec Lemme 2 et $L(M) = A$. $\blacksquare$

Donc, $\mathrm{D}(A)$ est aussi régulier.

3 Minimisation d'automate

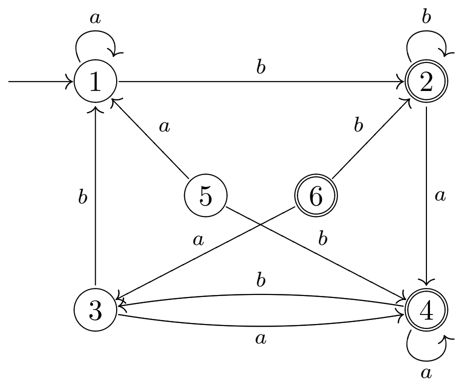
Soit $M = (\{1,2,3,4,5,6\}, \{a,b\}, \delta_M, 1, \{2,4,6\})$ et δ_M définie par :

δ_M	a	b
$S1$	1	2
$F2$	4	2
3	4	1
$F4$	4	3
5	1	4
$F6$	3	2

1. Donner le graphe de transitions de M.
2. Quels sont les états non-atteignables ?
3. Minimiser M, écrivez chaque étape de l'algorithme.
4. Convertir le langage résultant en une expression régulière (via le lemme d'Arden).

Corrigé :

1. Donner le graphe de transitions de M.



2. Quels sont les états non-atteignables ?
   Les états non-atteignables sont 5 and 6.

3. Minimiser M, écrivez chaque étape de l'algorithme.
   On doit d'abord éliminer les états qui ne sont pas atteignables. On a déjà vu que les états 5 et 6 ne sont jamais atteints. On peut donc déjà réduire l'automate en :

δ_M	a	b
$S1$	1	2
$F2$	4	2
3	4	1
$F4$	4	3

   On peut maintenant appliquer l'algorithme de minimisation :

1			
-	2		
-	-	3	
-	-	-	4

On marque tous les couples d'états qui ont un état final et un autre non-final.

1			
√	2		
-	√	3	
√	-	√	4

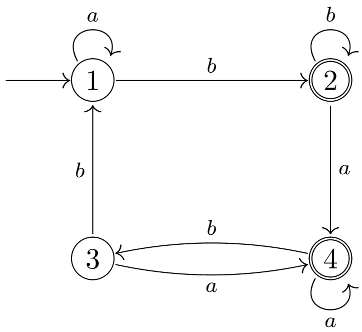
On regarde les transitions possibles depuis les couples qui ne sont pas encore marqués. On met en évidence les états déjà marqués.

input a :	{1, 3}	$\rightarrow$	{1, 4}	√
input b :	{2, 4}	$\rightarrow$	{2, 3}	√

Après la première étape on peut marquer deux autres états :

1			
√	2		
√	√	3	
√	√	√	4

Donc l'automate minimal est :



4. Convertir le langage résultant en une expression régulière (via le lemme d'Arden).
Afin d'éviter toutes confusions, on représente l'état 1 avec q_1, l'état 2 avec q_2, l'état 3 avec q_3 et l'état 4 avec q_4.
Le système d'équations décrivant les états de l'automate est :

$$\begin{cases} q_1 \equiv aq_1 + bq_2 \\ q_2 \equiv bq_2 + aq_4 + \epsilon \\ q_3 \equiv aq_4 + bq_1 \\ q_4 \equiv aq_4 + bq_3 + \epsilon \end{cases}$$

On substitue q_3 dans q_4 et on a :

$$\begin{array}{rcll} q_4 & \equiv & aq_4 + b\left(aq_4 + bq_1\right) + \epsilon & \\ & \equiv & aq_4 + baq_4 + bbq_1 + \epsilon & \text{distributivité} \\ & \equiv & \left(a + ba\right) q_4 + bbq_1 + \epsilon & \text{distributivité} \\ & \equiv & \left(a + ba\right)^* \left(bbq_1 + \epsilon\right) & \text{lemme d'Arden} \\ & \equiv & \left(a + ba\right)^* bbq_1 + \left(a + ba\right)^* & \text{distributivité} \end{array}$$

On substitue le résultat obtenu pour q_4 dans q_2.

$$\begin{array}{rcll} q_2 & \equiv & bq_2 + a\left(\left(a+ba\right)^* bbq_1 + \left(a+ba\right)^*\right) + \epsilon & \\ & \equiv & b^*\left(a\left(\left(a+ba\right)^* bbq_1 + \left(a+ba\right)^*\right) + \epsilon\right) & \text{lemme d'Arden} \\ & \equiv & b^*\left(a\left(a+ba\right)^* bbq_1 + a\left(a+ba\right)^* + \epsilon\right) & \text{distributivité} \\ & \equiv & b^*a\left(a+ba\right)^* bbq_1 + b^*a\left(a+ba\right)^* + b^* & \text{distributivité} \end{array}$$

On substitue le résultat obtenu pour q_2 dans q_1.

$$\begin{array}{rcll} q_1 & \equiv & aq_1 + b\left(b^*a\left(a+ba\right)^* bbq_1 + b^*a\left(a+ba\right)^* + b^*\right) & \\ & \equiv & aq_1 + bb^*a\left(a+ba\right)^* bbq_1 + bb^*a\left(a+ba\right)^* + bb^* & \text{distributivité} \\ & \equiv & \left(a + bb^*a\left(a+ba\right)^* bb\right) q_1 + bb^*a\left(a+ba\right)^* + bb^* & \text{distributivité} \\ & \equiv & \left(a + bb^*a\left(a+ba\right)^* bb\right)^* \left(bb^*a\left(a+ba\right)^* + bb^*\right) & \text{lemme d'Arden} \end{array}$$

Comme on a vu dans les exercices du cours, c'est tout a fait possible que vous êtes parvenue a une solution qui est différente de celle ci-dessus. Cependant, les axiomes qu'on a appliqués préservent les équivalences et, en plus, le lemme d'Arden nous donne la $\leq$-plus petite solution de l'équation $x \equiv yx + z$. Alors (si vous avait fait tout correctement) il doit être possible de démontrer que la solution ici dessus et les vôtres sont équivalentes.

4 Kleene

Démontrer en utilisant les lois de Kleene que $(ab)^*a = a(ba)^*$.

Corrigé :

On va démontrer que $(ab)^* a \leq a\,(ba)^*$ et que $a\,(ba)^* \leq (ab)^* a$. Donc, par la propriété d'anti-symétrie de $\leq$, $(ab)^* a = a\,(ba)^*$.
On commence avec $(ab)^* a \leq a\,(ba)^*$. Puisque on sait que $\beta + \alpha\gamma \leq \gamma \Rightarrow \alpha^*\beta \leq \gamma$. on pose $\alpha = ab,\ \beta = a,\ \gamma = a\,(ba)^*$ dans l'expression précédente. On peut alors dire que $(ab)^* a \leq a\,(ba)^*$ si on arrive à démontrer que $a + (ab)\,a\,(ba)^* \leq a\,(ba)^*$.

$$\begin{array}{rcll} a + (ab)\,a\,(ba)^* & = & a + aba\,(ba)^* & \text{associativité de } \cdot \\ & = & a\left(1 + ba\,(ba)^*\right) & \text{distributivité de } \cdot \\ & = & a\,(ba)^* & 1 + \alpha\alpha^* = \alpha^* \\ & \leq & a\,(ba)^* & \text{reflexivité de } \leq \\ & & & \square \end{array}$$

On continue avec $a\,(ba)^* \leq (ab)^* a$. Puisque on sait que $\beta + \gamma\alpha \leq \gamma \Rightarrow \beta\alpha^* \leq \gamma$, on pose $\alpha = ba,\ \beta = a,\ \gamma = (ab)^* a$ dans l'expression précédente. On peut dire que $a\,(ba)^* \leq (ab)^* a$ si on arrive à démontrer que $a + (ab)^* a\,(ba) \leq (ab)^* a$.

$$\begin{array}{rcll} a + (ab)^* a\,(ba) & = & a + (ab)^* aba & \text{associativité de } \cdot \\ & = & \left(1 + (ab)^* a\,(b)\right) a & \text{distributivité de } \cdot \\ & = & (ab)^* a & 1 + \alpha^*\alpha = \alpha^* \\ & \leq & (ab)^* a & \text{reflexivité de } \leq \\ & & & \square \end{array}$$

On a montré que $(ab)^* a \leq a\,(ba)^*$ mais aussi que $a\,(ba)^* \leq (ab)^* a$. Alors, par la propriété d'anti-symétrie de $\leq$, on peut affirmer que $a\,(ba)^* = (ab)^* a$.

5 Non-régularité

Montrer que le langage $L \stackrel{\text{def}}{=} \{ x \in \{ a, b, c \}^* \mid \exists n \in \mathbb{N} : |x| = n^2 \}$ n'est pas régulier.
Solution :

1. Nous utilisons la version de Hopcroft et Ullmann du lemme de gonflement.

   Étant données $n \geq 0$, nous posons $y = a^{n^2}$. Il est clair que $y \in L$ et que $|y| \geq n$. Nous procédons à prouver que pour tous les mots u, v, w tels que $y = uvw$, $v \neq \epsilon$, et $|uv| \leq n$, il existe un $k \geq 0$ tel que le mot $uv^k w \notin A$.

   – Si $n = 0$, alors il n'existe pas de mots u, v, w tels que $y = uvw$ et $v \neq \epsilon$.

   – Si $n > 0$, nous prenons des mots u, v, w tels que $y = uvw$, $v \neq \epsilon$, et $|uv| \leq n$. Alors, il existe $i, j, l \in \mathbb{N}$ tels que $i + j + l = n^2$, $u = a^i$, $v = a^j$, $w = a^l$, $j > 0$ et $i + j \leq n$. Posons $k = 2$. Nous avons que

   $$n^2 = i + j + l < i + 2j + l < i + j + l + 2j + 1 \leq i + j + l + 2n + 1 = (n + 1)^2.$$

   Comme $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ est monotone et $n^2 < i + 2j + l < (n + 1)^2$, il n'existe pas de $m \in \mathbb{N}$ tel que $i + 2j + l = m^2$. Donc, $uv^2 w \notin L$.

2. Avec les relations de Myhill-Nérode. Rappelons la définition de $\equiv_L$:

   $$\equiv_L \subseteq \{a, b, c\}^* \times \{a, b, c\}^* \text{ tel que } m \equiv_L n \text{ ssi } (\forall m' \in \{a, b, c\}^* : mm' \in L \Leftrightarrow nm' \in L)$$

   Nous savons que L est régulier ssi $\equiv_L$ a un nombre fini de classes d'equivalence.

   Soient $m, n \in \mathbb{N}$ tels que $m > n$. Posons $w = a^{2n+1}$. Nous avons que $a^{n^2} w = a^{(n+1)^2} \in L$. Comme $m^2 < m^2 + 2n + 1 < m^2 + 2m + 1 = (m+1)^2$ et $f : \mathbb{N} \to \mathbb{N} : x \mapsto x^2$ est monotone, il n'existe pas de $l \in \mathbb{N}$ tel que $m^2 + 2n + 1 = l^2$. Donc, $a^{m^2} w \notin L$.

   Nous avons montré que pour toutes $m, n \in \mathbb{N}$ tels que $m > n$ nous avons $a^{m^2} \not\equiv_L a^{n^2}$. Alors $\equiv_L$ a un nombre infini de classes d'equivalence, d'où L n'est pas régulier.

6 Indécidabilité

Soit MdT l'ensemble de toutes les MdT.
Nous définissons la fonction

$$\begin{array}{rcccc} \sigma & : & \text{MdT} & \to & \text{MdT} \times \text{MdT} \\ & & M & \mapsto & (M, M) \end{array}$$

Observer que FIN $\subseteq$ MdT et FINI $\subseteq$ MdT $\times$ MdT.

σ est une réduction, parce que
– $M \in$ FIN ssi $\sigma(M) = (M, M) \in$ FINI (parce que pour tout $A : A = A \cap A$) ;
– former le produit d'un élément avec soi-même est « intuitivement calculable ».
Donc, FIN $\leq_{\text{red}}$ FINI.

Comme FIN n'est pas r.e., alors FIN n'est pas récursif non plus.
(Se souvenir : tout ensemble récursif est aussi r.e.)

Avec Théorème 2 du transparent 11/16 de la Leçon 12, FINI ne peut pas être récursif.

7 Fonctions récursives

Représenter les fonctions suivantes de type $\mathbb{N} \to \mathbb{N}$ en fonction des schémas et exemples des fonctions partiellement récursives qui ont été donnés en cours :

1.

$$\begin{aligned}
\mathbf{plus5}(x) &\stackrel{\text{def}}{=} \mathbf{Comp}_{1,1}(\mathbf{Comp}_{1,1}(\mathbf{Comp}_{1,1}(\mathbf{Comp}_{1,1}(\mathbf{s},\mathbf{s}),\mathbf{s}),\mathbf{s}),\mathbf{s})(x)\\
&(= (\mathbf{s}\circ\mathbf{s}\circ\mathbf{s}\circ\mathbf{s}\circ\mathbf{s})(x))\\
&(= \mathbf{s}(\mathbf{s}(\mathbf{s}(\mathbf{s}(\mathbf{s}(x))))))
\end{aligned}$$

2. Nous utilisons les fonctions **mult**, **plus** et **sub** vues au cours.

$$\begin{aligned}
\mathbf{cbrt}(x) &\stackrel{\text{def}}{=} \mu_1(\mathbf{Comp}_{2,2}(\mathbf{absdiff},(\mathbf{Comp}_{1,2}(\mathbf{cube},\pi_1^2),\pi_2^2)))(x)\\
&(= \mu y.((\mathbf{absdiff}\circ(\mathbf{cube}\circ\pi_1^2,\pi_2^2))(y,x)=0)(x))\\
&(= \mu y.(\mathbf{absdiff}(\mathbf{cube}(y),x)=0))\\
\mathbf{absdiff}(u,v) &\stackrel{\text{def}}{=} \mathbf{Comp}_{2,2}(\mathbf{plus},(\mathbf{sub},\mathbf{Comp}_{2,2}(\mathbf{sub},(\pi_2^2,\pi_1^2))))(u,v)\\
&(= (\mathbf{plus}\circ(\mathbf{sub},\mathbf{sub}\circ(\pi_2^2,\pi_1^2)))(u,v))\\
&(= \mathbf{plus}(\mathbf{sub}(u,v),\mathbf{sub}(v,u)))\\
\mathbf{cube}(w) &\stackrel{\text{def}}{=} \mathbf{Comp}_{2,1}(\mathbf{mult},(\pi_1^1,\mathbf{Comp}_{2,1}(\mathbf{mult},(\pi_1^1,\pi_1^1))))(w)\\
&(= (\mathbf{mult}\circ(\pi_1^1,\mathbf{mult}\circ(\pi_1^1,\pi_1^1)))(w))\\
&(= \mathbf{mult}(w,\mathbf{mult}(w,w)))
\end{aligned}$$

3.

$$\begin{aligned}
\mathbf{f}(x) &\stackrel{\text{def}}{=} \mathbf{Comp}_{1,1}(\mathbf{plus5},\mathbf{cbrt})(x)\\
&(= (\mathbf{plus5}\circ\mathbf{cbrt})(x))\\
&(= \mathbf{plus5}(\mathbf{cbrt}(x)))
\end{aligned}$$