Annexe du chapitre 2 - Encodage des entiers

1 Pré-requis

1.1 Division euclidienne

Définition/Propriété 1 (*division euclidienne pour les entiers naturels*)

Soit $(a,b)\in\mathbb{N}\times\mathbb{N}^*$.
Il existe un unique couple $(q,r)\in\mathbb{N}\times[0..b[$ *tel que* $a=b\,q+r$.
On appelle alors q *le* ***quotient*** *et* r *le* ***reste*** *dans la division euclidienne de* a *par* b.
On dit aussi que r *est le* ***reste de*** a ***modulo*** b.

Preuve : • Montrons l'existence d'un tel couple (q,r) de manière constructive.
Si $b>a$, alors le couple $(0,a)$ convient. En effet on a bien $a=0\times b+a$ et $a\in[0..b[$.
Sinon, $b\leqslant a$, et on considère la suite u définie par $u_n=a-nb$ pour tout $n\in\mathbb{N}$. Cette suite à valeurs entières est initialement positive ($u_0=a\geqslant 0$), et strictement décroissante puisque $b>0$, elle est donc strictement négative à partir d'un certain rang. On note n_0 le rang du premier terme strictement négatif de cette suite.
On a alors $0>u_{n_0}=a-b\,n_0$ et $0\leqslant u_{n_0-1}=a-b\,(n_0-1)=a-b\,n_0+b$.
On pose $q=n_0-1$ et $r=a-bq$, ainsi on a bien $a=bq+r$ (par construction).
De plus $r=a-b\,(n_0-1)$, soit $r=u_{n_0-1}\geqslant 0$ et $r-b=u_{n_0-1}-b=u_{n_0}<0$ donc $r<b$.
Ainsi (q,r) est bien un couple de $\mathbb{N}\times[0..b[$ tel que $a=b\,q+r.$, d'où l'existence.

• Montrons l'unicité du couple reste.
On suppose qu'il existe $(q,r)\in\mathbb{N}\times[0..b[$ et $(q',r')\in\mathbb{N}\times[0..b[$ tels que $a=bq+r=bq'+r'$.
On a alors $b\,(q-q')=r'-r$.
Puisque $r\geqslant 0$, on en déduit $b\,(q-q')\leqslant r'$, et puisque $r'<b$, on en déduit $b\,(q-q')<b$.
En divisant par $b>0$, on obtient $q-q'<1$.
Comme $q-q'$ est entier (en tant que différence entre deux entiers) on en déduit que $q-q'\leqslant 0$.
Symétriquement, $q'-q\leqslant 0$, donc $q-q'=0$ soit $q=q'$.
Par suite $r=a-bq=a-bq'=r'$, et finalement on a bien $(q,r)=(q',r')$, d'où l'unicité. □

1.2 Logarithme en base $b\in\mathbb{N}\setminus\{0,1\}$

Soit $b\in\mathbb{N}\setminus\{0,1\}$.

Définition 2 (*Logarithme en base b*)

Pour $n\in\mathbb{N}$, $\log_b(n)=\dfrac{\ln(n)}{\ln(b)}$, *ainsi* $b^{\log_b(n)}=(e^{\ln(b)})^{\log_b(n)}=e^{\ln(b)\log_b(n)}=e^{\ln(n)}=n$.

Remarque 3

Si $b'\in\mathbb{N}\setminus\{0,1\}$, alors $\forall n\in\mathbb{N}$, $\log_b(n)*\log_{b'}(b)=\log_{b'}(n)$.

2 Codage des entiers naturels

2.1 Écriture en base $b \in \mathbb{N}\setminus\{0,1\}$

Soit $b \in \mathbb{N}\setminus\{0,1\}$. On considère l'alphabet $\Sigma = [0..b[$. Les éléments de Σ seront appelés **chiffres**, et les mots sur Σ seront appelés **nombres**.

Définition 4

Soit $a = a_{l-1}\, a_{l-2}\, \dots a_1\, a_0$ un mot sur Σ de longueur $l \in \mathbb{N}$.
*On dira que le mot a est **une écriture en base b** (à l chiffres) de l'entier $n = \sum_{i=0}^{l-1} a_i\, b^i$.*

Notation 5

$$val_b = \begin{pmatrix} \Sigma^* & \to & \mathbb{N} \\ a_{l-1}\, a_{l-2}\, \dots a_1\, a_0 & \mapsto & \sum_{i=0}^{l-1} a_i\, b^i \end{pmatrix}$$

NB : Le mot vide, usuellement noté ε représente alors 0,
et ceci vaut pour n'importe quelle base $b \in \mathbb{N}\setminus\{0,1\}$.

Lemme 6

Soit $l \in \mathbb{N}$.
Le plus grand entier que l'on peut écrire en base b à l chiffres est $b^l - 1$. Conséquemment, un entier $n \in \mathbb{N}$ ne peut pas s'écrire en base b avec strictement moins de $\lceil \log_b(n+1) \rceil$ chiffres.

Preuve : Notons N_l le plus grand entier qu'on peut écrire en base b à l chiffres.
Par définition de l'écriture en base b, on remarque que ce nombre s'écrit avec l fois le plus grand chiffre disponible, c'est-à-dire qu'il s'écrit $\underbrace{b{-}1\ b{-}1\ \dots\ b{-}1}_{\text{l fois}}$. On a donc

$$N_l = \sum_{i=0}^{l-1}(b-1)b^i = \sum_{i=0}^{l-1} b^{i+1} - \sum_{i=0}^{l-1} b^i = \sum_{i=1}^{l} b^i - \sum_{i=0}^{l-1} b^i = b^l - b^0 = b^l - 1$$

Cela montre le premier point.
Soit $n \in \mathbb{N}$. On note $l = \lceil \log_b(n+1) \rceil$. On considère $l' \in \mathbb{N}$ tel que $l' < l$. Par définition de la partie entière supérieure comme étant le plus petit majorant entier, on en déduit que $l' < \log_b(n+1))$.
Si n pouvait s'écrire avec l' chiffres, on aurait $n \leqslant N_{l'}$, soit $n \leqslant b^{l'} - 1 < b^{\log_b(n+1)} - 1 = (n+1) - 1 = n$, ce qui est absurde. D'où l'impossibilité annoncée. □

Remarque 7

Soit $n \in \mathbb{N}$. Soit $k \in \mathbb{N}$.
$n \in [b^{k-1}..b^k[\ \Leftrightarrow\ n+1 \in]b^{k-1}..b^k] \ \Leftrightarrow\ \log_b(n+1) \in]k-1..k] \ \Leftrightarrow\ \lceil \log_b(n+1) \rceil = k$

Propriété 8 (*existence de l'écriture en base b*)

Pour tout $n \in \mathbb{N}$, il existe un nombre $a = a_{lr-1}\, a_{l-2}\, \dots a_1\, a_0$ qui est l'écriture de n en base b.
Plus précisément, tout entier $n \in \mathbb{N}$ admet une écriture en base b à $\lceil \log_b(n+1) \rceil$ chiffres.

Preuve : Montrons par récurrence sur $l \in \mathbb{N}$ la propriété suivante.

$$\mathcal{H}_l : \forall n \in [0..b^l - 1], n \text{ admet une écriture en base } b \text{ à } l \text{ chiffres.}$$

• Pour $l = 0$, l'intervalle $[0..b^l - 1]$ est réduit à 0, et 0 admet bien une écriture en base b à 0 chiffres : le mot vide. Ainsi $\mathcal{H}_0$ est vraie.

• Soit $l \in \mathbb{N}$ tel que $\mathcal{H}_l$ est vraie. Montrons que $\mathcal{H}_{l+1}$ aussi.
Soit $n \in [0..b^{l+1}-1]$.
Par définition de la division euclidienne, il existe $(q,r) \in \mathbb{N}^2$ tel que $n = b^l\, q + r$ et $r < b^l$, *i.e.* $r \in [0..b^l-1]$.
Par $\mathcal{H}_l$ on en déduit que r admet une écriture en base b à l chiffres qu'on note $(a_i)_{i\in[0..l[}$.
On a alors $r = \sum_{i=0}^{l-1} a_i\, b^i$, et donc $n = q\, b^l + \sum_{i=0}^{l-1} a_i\, b^i$.
Puisque $n < b^{l+1}$, on a nécessairement $q < b$ (sinon on aurait $n \geqslant q\, b^l > b \times b^l = b^{l+1}$).
Ainsi en posant $a_l = q$, on a $(a_i)_{i\in[0..l+1[} \in \Sigma^{l+1}$ et $n = a_l\, b^l + \sum_{i=0}^{l-1} a_i\, b^i$.
Donc n admet bien une écriture en base b à $l+1$ chiffres.
D'où $\mathcal{H}_{l+1}$ est vraie. □

Propriété 9 (*quasi-unicité de l'écriture en base b*)

Soit $n \in \mathbb{N}$.
Si *$a = a_{l-1}\, a_{l-2}\, \ldots a_1\, a_0$ est une écriture de n en base b,*
alors *pour tout $k \in [0\,..\,l-1]$, a_k est le reste modulo b du quotient de n par b^k.*

Preuve : Soit $k \in [0\,..\,l-1]$.
On a $n = \sum_{i=0}^{l-1} a_i\, b^i = \sum_{i=0}^{k-1} a_i\, b^i + \sum_{i=k}^{l-1} a_i\, (b^{i-k}\, b^k) = \underbrace{\sum_{i=0}^{l-1} a_i\, b^i}_{:=r_k} + \underbrace{\left(\sum_{i=k}^{l-1} a_i\, b^{i-k}\right)}_{:=q_k} b^k$.
On note $r_k = \sum_{i=0}^{k-1} a_i\, b^i$. On a $r_k \in \mathbb{N}$ et puisque $\forall i \in [0..l-1], a_i \in [0..b[$, on a aussi

$$r_k \leqslant \sum_{i=0}^{k-1} (b-1)\, b^i = \sum_{i=0}^{k-1} b^{i+1} - \sum_{i=0}^{k-1} b^i = b^k - 1 < b^k$$

On note $q_k = \sum_{i=k}^{l-1} a_i\, b^{i-k}$.
Pour tout $i \in [k\,..\,l-1]$, $i-k \geqslant 0$ donc $b^{i-k} \in N$, ainsi q_k est une somme d'entiers positifs et donc $q_k \in \mathbb{N}$.
On déduit alors de la première égalité que q_k est le quotient et r_k le reste dans la division euclidienne de n par b^k. On cherche donc à montrer que a_k est le reste modulo b de q_k.
On a

$$q_k = \sum_{i=k}^{l-1} a_i\, b^{i-k} = a_k\, \underbrace{b^{k-k}}_{=1} + \sum_{i=k+1}^{l-1} a_i\, (b^{i-k-1} \times b) = a_k + b \times \left(\sum_{i=k+1}^{l-1} a_i\, b^{i-k-1}\right)$$

D'une part on sait que $a_k < b$ car $a_k \in \Sigma$. D'autre part, comme $i-k-1 \geqslant 0$ pour tout $i \in [k+1\,..\,l-1[$, $\sum_{i=k+1}^{l-1} a_i\, b^{i-k-1} \in \mathbb{N}$. On déduit donc de l'égalité précédente que a_k est bien le reste de q_k modulo b. □

Corollaire 10

Soit $n \in \mathbb{N}$.
Si *$a = a_{l-1}\, a_{l-2}\, \ldots a_1\, a_0$ et $a' = a'_{l'-1}\, a'_{l'-2}\, \ldots a'_1\, a'_0$ sont deux écritures de n en base b avec $l \leqslant l'$,*
alors *pour tout $k \in [0..r[$ on a $a_k = a'_k$, et pour tout $k \in]l..l'[$ on a $a'_k = 0$.*
En particulier on a l'unicité de l'écriture en base b à longueur fixée.

Notation 11

Pour tout $l \in \mathbb{N}$ on peut maintenant définir l'écriture en base b à l chiffres :
$ecr_b^l = \begin{pmatrix} [0..b^k[& \to & \Sigma^l \\ n & \mapsto & a_{l-1} \ldots a_1\, a_0 \end{pmatrix}$ *où $\forall k \in [0..l[$, a_k est le reste modulo b du quotient de n par b^k.*

3 Encodage des entiers relatifs

On s'intéresse ici à l'encodage des entiers relatifs tel qu'il est fait sur les ordinateurs. On s'appuie donc sur le codage des entiers naturels en binaire, *i.e.* en base 2. Ainsi dans cette section $\Sigma = \{0,1\}$. De plus on utilisera un chiffre du nombre pour donner le signe de l'entier encodé : 0 pour positif, 1 pour négatif. Ce chiffre a donc une signification particulière et ne représente pas la même chose que les autres 0 ou 1. De plus pour des raisons pratiques qui apparaîtront plus bas, ce chiffre de signe est le chiffre le plus à gauche du nombre, soit à l'opposé du chiffre des unités. On a donc besoin de travailler à longueur fixée pour pouvoir identifier ce chiffre au statut particulier, et cela limite bien sûr les entiers que l'on peut encoder.

Soit $l \in \mathbb{N}$. On note $I^l = \left[-2^{l-1}..\,2^{l-1}\right[$. On remarque que $\text{card}(I^l) = 2^l$.

Notation 12

$$\varphi^l = \begin{pmatrix} I^l \to \{0,1\}^l \\ z \mapsto \begin{cases} 0\,\text{ecr}_b^{l-1}(z) & \text{si } z \geqslant 0 \\ 1\,\text{ecr}_b^{l-1}\left(z + 2^{l-1}\right) & \text{sinon} \end{cases} \end{pmatrix} \text{ et } \psi^l = \begin{pmatrix} \{0,1\}^l & \to & I^l \\ a_{l-1}\dots a_1\,a_0 & \mapsto & -a_{l-1}\,2^{l-1} + \text{val}_2(a_{l-2}\dots a_0) \end{pmatrix}$$

Propriété 13

Ces fonctions sont bien définies et sont réciproques.

Preuve : φ^l est bien définie car ecr_b^{l-1} est bien définie et à valeur dans $\{0,1\}^{l-1}$, en ajoutant un 0 ou un 1 à gauche on obtient bien un mot de $\{0,1\}^l$.
ψ^l est bien définie car val_2 est bien définie, et qu'à un mot de $\{0,1\}^{l-1}$ (ici $a_{l-2}\dots a_0$) elle associe une valeur comprise dans $[0..\,2^{l-1}[$, en ajoutant 0 ou -2^{l-1}, on obtient bien une valeur dans $[0..\,2^{l-1}[\cup [-2^{l-1}..0[$ soit dans $[-2^{l-1}..\,2^{l-1}[= I^l$.

Soit $z \in I^l$.
- Si $z \geqslant 0$, on a $\varphi^l(z) = 0\,\text{ecr}_b^{l-1}(z)$ donc $\psi^l(\varphi^l(z)) = -0 \times 2^{l-1} + \text{val}_2(\text{ecr}_b^{l-1}(z))$.
Or par définition de l'écriture en base 2, $\text{val}_2(\text{ecr}_b^{l-1}(z)) = z$, donc $\psi^l(\varphi^l(z)) = z$.
- Si $z < 0$, on a $\varphi^l(z) = 1\,\text{ecr}_b^{l-1}(z + 2^{l-1})$ donc $\psi^l(\varphi^l(z)) = -1 \times 2^{l-1} + \text{val}_2(\text{ecr}_b^{l-1}(z + 2^{l-1}))$.
Or par définition de val_2, $\text{val}_2(\text{ecr}_b^{l-1}(z + 2^{l-1})) = z + 2^{l-1}$, donc $\psi^l(\varphi^l(z)) = -2^{l-1} + (z + 2^{l-1}) = z$.
Donc $\psi^l \circ \varphi^l = \text{Id}_{I^l}$.

Soit $a \in \{0,1\}^l$. On note $a_{l-1}\dots a_1\,a_0$ les lettres de a, et $\tilde{a}$ son suffixe $a_{l-2}\dots a_1\,a_0$. Ainsi $\tilde{a} \in \Sigma^{l-1}$.
On a $\psi^l(a) = -a_{l-1}\,2^{l-1} + \text{val}_2(\tilde{a})$. Par définition de val_2, on sait que $\text{val}_2(\tilde{a}) \in [0..2^{l-1}[$.
- Si $a_{l-1} = 0$, on a $\psi^l(a) = \text{val}_2(\tilde{a})$, donc $\psi^l(a) \in [0..2^{l-1}[$, en particulier $\psi^l(a) \geqslant 0$.
On a alors $\varphi^l(\psi^l(a)) = 0\,\text{ecr}_b^{l-1}(\text{val}_2(\tilde{a}))$, or par définition de l'écriture en base 2, $\text{ecr}_b^{l-1}(\text{val}_2(\tilde{a})) = \tilde{a}$, et puisque $0 = a_{l-1}$, on en déduit $\varphi^l(\psi^l(a)) = a_{l-1}\,\tilde{a} = a$.
- Si $a_{l-1} = 1$, on a $\psi^l(a) = -2^{l-1} + \text{val}_2(\tilde{a})$, donc $\psi^l(a) \in [-2^{l-1}..0[$, en particulier $\psi^l(a) < 0$.
On a alors $\varphi^l(\psi^l(a)) = 1\,\text{ecr}_b^{l-1}(\text{val}_2(\tilde{a}))$, or par définition de l'écriture en base 2, $\text{ecr}_b^{l-1}(\text{val}_2(\tilde{a})) = \tilde{a}$, et puisque $1 = a_{l-1}$, on en déduit $\varphi^l(\psi^l(a)) = a_{l-1}\,\tilde{a} = a$.
Donc $\varphi^l \circ \psi^l = \text{Id}_{\Sigma^l}$. □

Notation 14

On appelle ***complément à 2*** *d'un nombre écrit sur $\{0,1\}$ le nombre obtenu en remplaçant les 0 par des 1 et vice-versa.*

$$comp_2 = \begin{pmatrix} \Sigma^* & \to & \Sigma^* \\ a_{k-1}\dots a_1\,a_0 & \mapsto & \overline{a}_{k-1}\dots\overline{a}_1\,\overline{a}_0 \text{ où } \forall i \in [0..k[,\ \overline{a}_i = 1 - a_i \end{pmatrix}$$

Propriété 15 (*complément à 2 et opposé*)

$\forall z \in \mathbb{Z},\ \psi^l\Big(comp_2\big(\varphi^l(z)\big)\Big) = -z-1.$

Autrement dit, le complément à 2 de l'écriture d'un entier relatif encode son opposé moins 1.

Preuve : Soit $z \in I^l$. On note $a_{l-1}\,a_{l-2}\ldots a_1\,a_0 = \varphi^l(z)$, et $\widetilde{a} = a_{l-2}\ldots a_1\,a_0$.
Ainsi, puisque $z = \psi^l(\varphi^l(z))$, on a $z = -2^{l-1}a_{l-1} + \mathrm{val}_2(\widetilde{a})$ $(\bigstar)$.
On note aussi $\overline{a}_{l-1}\,\overline{a}_{l-2}\ldots\overline{a}_1\,\overline{a}_0 = \mathrm{comp}_2(\varphi^l(z))$ et $\hat{a} = \overline{a}_{l-2}\ldots\overline{a}_1\,\overline{a}_0$.
Par définition de comp_2, on remarque que $\forall i \in [0..l-1],\ \overline{a}_i = 1-a_i$).
On peut alors écrire $\psi^l(\mathrm{comp}_2(\varphi^l(z))) = \psi^l(\overline{a}_{l-1}\,\overline{a}_{l-2}\ldots\overline{a}_1\,\overline{a}_0) = -2^{l-1}\,\overline{a}_{l-1} + \mathrm{val}_2(\hat{a})$.
Or on a

$$\begin{aligned}
\mathrm{val}_2(\hat{a}) &= \mathrm{val}_2(\overline{a}_{l-2}\ldots\overline{a}_1\,\overline{a}_0)\\
&= \sum_{i=0}^{l-2}\overline{a}_i\,2^i\\
&= \sum_{i=0}^{l-2}(1-a_i)\,2^i\\
&= \sum_{i=0}^{l-2}2^i \;-\; \sum_{i=0}^{l-2}a_i\,2^i\\
&= (2^{l-1}-1) \;-\; \mathrm{val}_2(\tilde{a})
\end{aligned}$$

Donc on obtient

$$\begin{aligned}
\psi^l(\mathrm{comp}_2(\varphi^l(z))) &= -2^{l-1}\,\overline{a}_{l-1} + \Big((2^{l-1}-1) \;-\; \mathrm{val}_2(\tilde{a})\Big)\\
&= -2^{l-1}\,(\overline{a}_{l-1}-1) \;-1\; -\; \mathrm{val}_2(\tilde{a})\\
&= -2^{l-1}\,((1-a_{l-1})-1) \;-1\; -\; \mathrm{val}_2(\tilde{a})\\
&= -2^{l-1}\,((\cancel{1}-a_{l-1})\cancel{-1}) \;-1\; -\; \mathrm{val}_2(\tilde{a})\\
&= -2^{l-1}\,(-a_{l-1}) \;-\; \mathrm{val}_2(\tilde{a}) \;-1\\
&= -\Big(-2^{l-1}\,a_{l-1} + \mathrm{val}_2(\tilde{a})\Big) \;-1\\
&= -z \;-1 \quad \text{par } (\bigstar)
\end{aligned}$$

□

Notation 16

$$add_2^l = \begin{pmatrix} \Sigma^l\times\Sigma^l & \to & \Sigma^{l+1} \\ (a,b) & \mapsto & c_l\,c_{l-1}\ldots c_0 \end{pmatrix} \text{ où } \begin{cases} \forall i\in[0..l-1], c_i = (a_i+b_i+r_i)\%2 \text{ et } c_l = r_l, \\ r_0 = 0 \text{ et } \forall i\in[1..l], r_i = \begin{cases} 1 \text{ si } a_{i-1}+b_{i-1}+r_{i-1}\geqslant 2 \\ 0 \text{ sinon} \end{cases} \\ a = a_{l-1}\,a_{l-2}\ldots a_0 \text{ et } b = b_{l-1}\,b_{l-2}\ldots b_0 \end{cases}$$

Remarque 17

Il s'agit seulement d'une écriture formelle de l'algorithme d'addition réalisé par la machine présentée en cours, algorithme qui est lui même l'équivalent en base 2 de l'algorithme d'addition des nombres en base 10 que vous connaissez. En particulier, r_i est la retenue à prendre en compte à l'étape i.

Propriété 18 (*addition des entiers naturels*)

$\forall (a,b)\in\Sigma^l\times\Sigma^l,\ val_2(add_2^l(a,b)) = val_2(a) + val_2(b).$

Autrement dit add_2^l réalise l'addition sur les écritures binaires des entiers naturels.

Preuve : On montre en fait que cette propriété est vraie pour tout $l \in \mathbb{N}$, par récurrence sur l. Pour tout $l \in \mathbb{N}$ on définit la propriété $\mathcal{P}_l$ comme suit.

$$\mathcal{P}_l : \forall (a,b) \in \Sigma^l \times \Sigma^l, \text{val}_2(\text{add}_2^l(a,b)) = \text{val}_2(a) + \text{val}_2(b)$$

• Pour $l = 0$, on a $\Sigma^l = \Sigma^0 = \{\varepsilon\}$. Or pour $a = \varepsilon$ et $b = \varepsilon$, on a d'une part $\text{val}_2(a) = 0$ et $\text{val}_2(b) = 0$, donc $\text{val}_2(a) + \text{val}_2(b) = 0$, et d'autre part $\text{add}_2^l(a,b) = \text{add}_2^l(\varepsilon,\varepsilon) = c_0 = r_0 = 0$. Donc on a bien $\text{val}_2(\text{add}_2^l(a,b)) = \text{val}_2(a) + \text{val}_2(b)$, et $\mathcal{P}_0$ est vraie.

• Soit $l \in \mathbb{N}$, on suppose $\mathcal{P}_l$ vraie.
Soit $(a,b) \in \Sigma^{l+1} \times \Sigma^{l+1}$. On note $a = a_l\, a_{l-1} \dots a_0$ et $b = b_l\, b_{l-1} \dots b_0$, et $\tilde{a} = a_{l-1} \dots a_0$ et $\tilde{b} = b_{l-1} \dots b_0$.
On note aussi $\text{add}_2^{l+1}(a,b) = c_{l+1}\, c_l\, c_{l-1} \dots c_0$.
On veut montrer que $\text{val}_2(c_{l+1}\, c_l\, c_{l-1} \dots c_0) = \text{val}_2(a) + \text{val}_2(b)$.

Ainsi, par définition de add_2^{l+1}, on a $\forall i \in [0..l]$, $c_i = (a_{i-1} + b_{i-1} + r_{i-1})\%2$ et $c_{l+1} = r_{l+1}$ avec $r_0 = 0$ et $\forall i \in [1..l+1]$, $r_i = (a_{i-1} + b_{i-1} + r_{i-1})/2$ (★) En effet, puisque $(a_{i-1} + b_{i-1} + r_{i-1}) \leqslant 3 < 2\times 2$, le quotient de $(a_{i-1} + b_{i-1} + r_{i-1})$ par 2 est 0 ou 1, c'est 0 si $(a_i + b_i + r_i) < 2$, auquel cas $r_i = 0$, et c'est 1 sinon, auquel cas $r_i = 1$.

On remarque que les chiffres les plus à droite de $\text{add}_2^l(\widetilde{a},\widetilde{b})$ sont les mêmes pour $\text{add}_2^{l+1}(a,b)$. En fait par définition de add_2^l, on a $\text{add}_2^l(\widetilde{a},\widetilde{b}) = \widetilde{c_l}\, c_{l-1} \dots c_0$, où $\widetilde{c_l} = r_l$.

D'après $\mathcal{P}_l$, on a donc $\text{val}_2(\widetilde{c_l}\, c_{l-1} \dots c_0) = \text{val}_2(\widetilde{a}) + \text{val}_2(\widetilde{b})$.
Ainsi on peut réécrire la somme $\text{val}_2(a) + \text{val}_2(b)$ comme suit.

$$\begin{aligned}
\text{val}_2(a) + \text{val}_2(b) &= \text{val}_2(a_l\, \widetilde{a}) + \text{val}_2(b_l\, \widetilde{b}) \\
&= 2^l a_l + \text{val}_2(\widetilde{a}) + 2^l b_l + \text{val}_2(\widetilde{b}) \\
&= 2^l (a_l + b_l) + \Big(\text{val}_2(\widetilde{a}) + \text{val}_2(\widetilde{b})\Big) \\
&= 2^l (a_l + b_l) + \text{val}_2(\widetilde{c_l}\, c_{l-1} \dots c_0) \\
&= 2^l (a_l + b_l) + 2^l \widetilde{c_l} + \text{val}_2(c_{l-1} \dots c_0) \\
&= 2^l (a_l + b_l + \widetilde{c_l}) + \text{val}_2(c_{l-1} \dots c_0)
\end{aligned}$$

D'autre part on a $\text{val}_2(c_{l+1}\, c_l\, c_{l-1} \dots c_0) = 2^{l+1} c_{l+1} + 2^l c_l + \text{val}_2(c_{l-1} \dots c_0)$.

Il reste donc à montrer que $2^l(a_l + b_l + \widetilde{c_l}) = 2^{l+1} c_{l+1} + 2^l c_l$, soit en divisant par 2^l que $a_l + b_l + \widetilde{c_l} = 2\, c_{l+1} + c_l$.
Or on a déjà $c_{l+1} = r_{l+1}$ et $r_{l+1} = (a_l + b_l + r_l)/2$ d'après (★), et $c_l = (a_l + b_l + r_l)\%2$ par définition directe de add_2^{l+1}.Par définition de la division euclidienne, on a donc bien $(a_l + b_l + r_l) = 2 * c_{l+1} + c_l$.

Ainsi $\mathcal{P}_{l+1}$ est vraie.

Par récurrence on en déduit que $\forall l \in \mathbb{N}, \mathcal{P}_l$ est vraie. □

Propriété 19 (*addition des entiers relatifs*)

Soit $(y,z) \in I^l \times I^l$.
***Si** $y+z \in I^l$, **alors** en notant $c_l\, c_{l-1} \dots c_0 = \text{add}_2^l\Big(\varphi^l(y), \varphi^l(z)\Big)$, on a $\psi^l(c_{l-1} \dots c_0) = y + z$.*

Autrement dit add_2^l réalise aussi l'addition sur les écritures des entiers relatifs pourvu que la somme soit dans l'intervalle I^l.

Preuve : On note $a = a_{l-1}\, a_{l-2} \dots a_0 = \varphi^l(y)$, et $\widetilde{a} = a_{l-2} \dots a_0$, ainsi on a $y = -2^{l-1} a_{l-1} + \text{val}_2(\widetilde{a})$.
De même, on note $b = b_{l-1}\, b_{l-2} \dots b_0 = \varphi^l(z)$, et $\widetilde{b} = b_{l-2} \dots b_0$, ainsi on a $z = -2^{l-1} b_{l-1} + \text{val}_2(\widetilde{b})$.
Enfin en notant $c = c_l\, c_{l-1}\, c_{l-2} \dots c_0$ et $\widetilde{c} = c_{l-2} \dots c_0$, on a $\psi^l(c_{l-1}\, c_{l-2} \dots c_0) = -2^{l-1} c_{l-1} + \text{val}_2(\widetilde{c})$.

De plus, par définition de val_2, on a $\left|\begin{array}{l}\mathrm{val}_2(a) = 2^{l-1}a_{l-1} + \mathrm{val}_2(\widetilde{a})\\ \mathrm{val}_2(b) = 2^{l-1}b_{l-1} + \mathrm{val}_2(\widetilde{b})\\ \mathrm{val}_2(c) = 2^{l}c_{l} + 2^{l-1}c_{l-1} + \mathrm{val}_2(\widetilde{c})\end{array}\right.$

D'après la propriété 18, comme $\mathrm{val}_2(c) = \mathrm{val}_2\big(\mathrm{add}_2^l(a,b)\big)$, on a $\mathrm{val}_2(c) = \mathrm{val}_2(a) + \mathrm{val}_2(b)$ (★).

On peut donc réécrire l'égalité qu'on cherche à démontrer comme suit.

$$\begin{aligned}
&\psi^l(c_{l-1}\,c_{l-2}\,\ldots c_0) = y+z\\
\Leftrightarrow\ & -2^{l-1}c_{l-1} + \mathrm{val}_2(\widetilde{c}) = \Big(-2^{l-1}a_{l-1} + \mathrm{val}_2(\widetilde{a})\Big) + \Big(-2^{l-1}b_{l-1} + \mathrm{val}_2(\widetilde{b})\Big)\\
\Leftrightarrow\ & -2^{l-1}c_{l-1} + \mathrm{val}_2(\widetilde{c}) = -2^{l-1}(a_{l-1}+b_{l-1}) + \mathrm{val}_2(\widetilde{a}) + \mathrm{val}_2(\widetilde{b})\\
\Leftrightarrow\ & -2^{l-1}c_{l-1} + \Big(\mathrm{val}_2(c) - 2^l c_l - 2^{l-1}c_{l-1}\Big) = -2^{l-1}(a_{l-1}+b_{l-1}) + \Big(\mathrm{val}_2(a) - 2^{l-1}a_{l-1}\Big) + \Big(\mathrm{val}_2(b) - 2^{l-1}b_{l-1}\Big)\\
\Leftrightarrow\ & -2^{l-1}(c_{l-1}+2c_l+c_{l-1}) + \mathrm{val}_2(c) = -2^{l-1}(a_{l-1}+b_{l-1}+a_{l-1}+b_{l-1}) + \mathrm{val}_2(a) + \mathrm{val}_2(b)\\
\Leftrightarrow\ & -2^{l}(c_{l-1}+c_l) + \cancel{\mathrm{val}_2(c)} = -2^{l}(a_{l-1}+b_{l-1}) + \cancel{\mathrm{val}_2(a) + \mathrm{val}_2(b)} \quad \text{par (★)}\\
\Leftrightarrow\ & -2^{l}(c_{l-1}+c_l) = -2^{l}(a_{l-1}+b_{l-1})\\
\Leftrightarrow\ & c_{l-1}+c_l = a_{l-1}+b_{l-1}
\end{aligned}$$

Pour montrer cette égalité on utilise le fait que c est obtenu par addition bit à bit des nombres a et b.
On note $r_0 = 0$ et $\forall i \in [1..\,l]$, $r_i = (a_{i-1} + b_{i-1} + r_{i-1})/2$, où l'on désigne par "/2" le quotient par 2.
Par définition de add_2^l, on a alors $\forall i \in [0..\,l-1]$, $c_i = (a_i + b_i + r_i)\%2$ où "%2" désigne le reste modulo 2.
En particulier, on a $c_l = r_l = (a_{l-1} + b_{l-1} + r_{l-1})/2$ et $c_{l-1} = (a_{l-1} + b_{l-1} + r_{l-1})\%2$.

On remarque aussi qu'avec ces notations, $\mathrm{add}_2^{l-1}(\widetilde{a},\widetilde{b}) = r_{l-1}\,c_{l-2}\,\ldots\,c_0$ (♣) (c'est la définition de add_2^{l-1}).

• Si $(a_{l-1}, b_{l-1}) = (0,0)$, alors $a_{l-1} + b_{l-1} + r_{l-1} = r_{l-1} < 2$, donc $c_l = 0$ et $c_{l-1} = r_{l-1}$.
Ainsi $c_{l-1} + c_l = a_{l-1} + b_{l-1} \Leftrightarrow r_{l-1} = 0$.
Comme $a_{l-1} = 0$, $y = \mathrm{val}_2(\widetilde{a})$, et comme $b_{l-1} = 0$, $z = \mathrm{val}_2(\widetilde{b})$, donc $y + z = \mathrm{val}_2(\widetilde{a}) + \mathrm{val}_2(\widetilde{b})$, ce qui d'après la propriété 18 donne $y + z = \mathrm{val}_2(\mathrm{add}_2^{l-1}(\widetilde{a},\widetilde{b}))$ Or $y + z < 2^{l-1}$ puisque par hypothèse $y + z \in I^l$, donc le chiffre de poids 2^{l-1} de $\mathrm{add}_2^{l-1}(\widetilde{a},\widetilde{b})$ est nécessairement nul, soit $r_{l-1} = 0$ d'après (♣).

• Si $(a_{l-1}, b_{l-1}) = (0,1)$ ou $(1,0)$, alors $a_{l-1} + b_{l-1} + r_{l-1} = 1 + r_{l-1}$.
Si $r_{l-1} = 1$, alors $1 + r_{l-1} = 2$ donc $c_l = 1$ et $c_{l-1} = 0$.
Si $r_{l-1} = 0$, alors $1 + r_{l-1} = 1$ donc $c_l = 0$ et $c_{l-1} = 1$.
Ainsi dans les deux cas on a $c_l + c_{l-1} = 1 = a_{l-1} + b_{l-1}$.

• Si $(a_{l-1}, b_{l-1}) = (1,1)$, alors $a_{l-1} + b_{l-1} + r_{l-1} = 2 + r_{l-1} \geqslant 2$, donc $c_l = 1$ et $c_{l-1} = r_{l-1}$.
Ainsi $c_{l-1} + c_l = a_{l-1} + b_{l-1} \Leftrightarrow 1 + r_{l-1} = 2 \Leftrightarrow r_{l-1} = 1$.
Comme $a_{l-1} = 1$, $y = -2^{l-1} + \mathrm{val}_2(\widetilde{a})$, et comme $b_{l-1} = 1$, $z = -2^{l-1} + \mathrm{val}_2(\widetilde{b})$.
Donc $y + z = -2^l + \mathrm{val}_2(\widetilde{a}) + \mathrm{val}_2(\widetilde{b})$, soit $y + z = -2^l + \mathrm{val}_2(\mathrm{add}_2^{l-1}(\widetilde{a},\widetilde{b}))$ d'après la propriété 18.
Or $y + z \in I^l$, ce qui implique $y + z \geqslant -2^{l-1}$, soit $y + z \geqslant -2^l + 2^{l-1}$, donc $\mathrm{val}_2(\mathrm{add}_2^{l-1}(\widetilde{a},\widetilde{b})) \geqslant 2^{l-1}$.
Donc le chiffre de poids 2^{l-1} de $\mathrm{add}_2^{l-1}(\widetilde{a},\widetilde{b})$ est nécessairement 1, soit $r_{l-1} = 1$. d'après (♣).

□