Comptage de l'ensemble des éléments de la base de Hilbert d'un système d'équations diophantiennes linéaires

Laurent Juban

Comptage de l'ensemble des éléments de la base de Hilbert d'un système d'équations diophantiennes linéaires

Laurent Juban

LORIA Campus scientifique BP 239
54506 Vandœuvre-lès-Nancy Cedex, France.
juban@loria.fr

1 Introduction

La résolution en nombre entiers positifs des équations linéaires à coefficients entiers encore connues sous le nom d'équations diophantiennes linéaires, joue un rôle fondamental dans l'unification modulo AC. En effet, tous les algorithmes généraux d'unification modulo AC connus à ce jour font appel implicitement ou explicitement à ce type d'équations. Les problèmes de construction de la base de Hilbert (ensemble des solutions minimales) d'un système d'équations diophantiennes linéaires a été largement étudié jusqu'à présent. Mais, ce n'est pas le cas pour le problème de comptage de l'ensemble minimal et complet des solutions d'un tel système. Ce problème de comptage appartient dans le cas général à la classe $\#NP$. Nous avons étudié des sous-problèmes en restreignant le nombre d'équations et la multiplicité de chaque variable. Nous avons pu montrer, entre autre, qu'il y a trois cas intéressants à étudier : le cas où la multiplicité de chaque variable est au plus trois qui appartient à la classe $\#NP$, le cas où la multiplicité de chaque variable est au plus deux qui appartient à la classe $\#P$ et le cas le plus simple où chaque variable du système est de multiplicité un qui est polynômial. De plus, nous avons pu montrer que pour toute solution minimale d'un système d'équations diophantiennes linéaires où chaque variable est au plus de multiplicité deux, chaque variable prendra au plus la valeur deux dans toute solution minimale.

2 Préliminaires

Nous allons d'abord rappeler quelques notions concernant les classes de complexité et les classes de comptage. Nous supposons connue la classe des problèmes de décision NP (problème pouvant être résolu en temps polynômial par une machine de Turing non déterministe). FP est la classe des fonctions calculables en temps polynomial. Aux classes de décisions et aux classes de fonctions s'ajoutent les classes de comptage introduites par Valiant [Val79]. $\#P$ est la classe des fonctions calculant le nombre de chemins admissibles d'une machine de Turing non déterministe. Une définition équivalente de la classe $\#P$, mais plus intuitive est la suivante [Koz92]. La classe $\#P$ est la classe des fonctions ω telle que : (i) il existe une fonction polynomiale déterminant, pour un x et un y donnés si $y \in \omega(x)$; (ii) il existe une constante $k \in \mathcal{N}$ telle que pour tout $y \in \omega(x)$, $\|y\| \leq \|x\|^k$. La classe de comptage $\#NP$ est la classe des fonctions calculant le nombre de chemins admissibles d'une machine de Turing non déterministe utilisant un oracle de la classe NP (c'est-à-dire un machine NP^{NP}). Hemaspaandra et Vollmer [HV94] ont introduit une nouvelle notation pour les classes de comptage plus homogène que celle de Valiant. Pour une classe C, la classe de comptage $\#.C$ est la classe des fonctions f telles que, pour un prédicat R C-calculable à deux arguments et un polynôme p, pour tout x : $f(x) = \|\{y \text{ tel que } p(\|x\|) = \|y\| \text{ et } R(x,y)\}\|$. Les classes de comptage $\#.coNP$ et $\#NP$ sont identiques [HV94].

Une équation diophantienne linéaire est une équation à coefficients entiers positifs admettant une solution en nombres entiers positifs. Une solution minimale m de cette équation est une solution non nulle telle qu'il n'existe pas de solution m' telle que $m' < m$. L'ensemble des solutions minimales non nulles d'un système d'équations diophantiennes linéaires est appelé base de Hilbert. Deux systèmes d'équations S et S' sont iso-équivalents si et seulement s'il existe une bijection entre les solutions de S et de S' telle qu'une solution s est minimale pour le système S si et seulement si son image s' par la bijection f est minimale pour le système S'. La multiplicité d'une variable est le nombre de fois où celle-ci apparait dans le système.

Le problème qui nous intéresse dans cet article est le problème de comptage des éléments de la base de Hilbert noté $\#Hilbert$. Le problème de comptage de la taille de la base de Hilbert pour un système d'équations diophantiennes où la multiplicité maximale des variables est i et où le nombre d'équations est k, est noté $\#Hilbert_i(k)$. Le cas où le nombre d'équations n'est pas limité est noté $\#Hilbert_i(\omega)$. Dans tous les cas étudiés le nombre de variables n'est jamais fixé.

3 Enumération des résultats

Nous avons montré dans un premier temps que le problème $\#Hilbert$ appartenait à la classe $\#NP$. Ceci en utilisant la définition de Hemaspaandra et Vollmer [HV94]. Il nous a donc fallu montrer que l'on pouvait tester par un algorithme appartenant à la classe $coNP$ qu'un vecteur s était minimal pour le système S (et qu'une solution minimale d'un système est de taille polynomiale par rapport à la taille du système).

Le problème de comptage $\#Hilbert$ étant complexe dans le cas général, nous avons décidé d'étudier des sous-cas de celui-ci en limitant la multiplicité de variables (k) et le nombre d'équations (n), le nombre de variables n'étant jamais limité.

Dans un premier temps, on peut remarquer que le problème de comptage $\#Hilbert$ peut être ramené en temps polynômial (par une réduction parsimonieuse) au problème de comptage $\#Hilbert_3(\omega)$. Cette réduction est semblable à celle permettant de réduire le problème SAT au problème $3SAT$.

Théorème 1 *Soit S un système d'équations diophantiennes linéaires pour lequel chaque variable a la multiplicité un. Alors le problème de comptage de l'ensemble des solutions minimales de S (non nulles) noté $\#Hilbert_1(\omega)$ appartient à la classe FP.*

Théorème 2 $\#Hilbert_2(\omega) \in \#P$

Théorème 3 *Soit E une équation diophantienne linéaire pour laquelle chaque variable a au plus la multiplicité i. Alors le problème de comptage de l'ensemble des solutions minimales de E ($\#Hilbert_i(1)$) appartient à la classe FP.*

Problème	Classe de comptage
$\#Hilbert_1(1)$	FP
$\#Hilbert_1(\omega)$	FP
$\#Hilbert_i(1)$ (i fixé)	FP
$\#Hilbert_2(\omega)$	$\#P$
$\#Hilbert_3(\omega)$	$\#NP$
$\#Hilbert$	$\#NP$

Le résultat que nous trouvons le plus intéressant pour l'instant est l'appartenance à $\#P$ du problème $\#Hilbert_2(\omega)$. Pour prouver ce théorème nous avons utilisé les deux lemmes suivants :

Lemme 4 *Soit $AX = 0$ un système d'équations diophantiennes linéaires tel que chaque variable soit au plus de multiplicité deux, (si $A = (a_i^j)_k^n$ alors $\forall j \sum_{i=1}^{k} \|a_i^j\| \leq 2$) alors il existe un système d'équations diophantiennes linéaires $BY = 0$ où $B = (b_i^j)_{k'}^{n'}$, iso-équivalent au système $AX = 0$, appelé forme réduite du système $AX = 0$ ayant les propriétés suivantes:*

- *Le coefficient multiplicateur de chaque variable est au plus un : $\forall i, j \mid b_i^j \mid \leq 1$;*
- *Chaque variable est au plus de multiplicité deux : $\forall j \sum_{i=1}^{k'} \mid b_i^j \mid \leq 2$;*
- *Chaque équation est du type $x_1 + x_2 = y$ ou $x = y$: $\forall i \mid \sum_{j=1}^{n'} b_i^j \mid \leq 1$ et $\sum_{j=1}^{n'} \mid b_i^j \mid \leq 3$;*
- *Dans le système S', une variable de multiplicité deux apparait dans deux équations distinctes, une de la forme $x = y$ et l'autre de la forme $u + v = w$.*

Ce lemme signifie en fait que l'on peut transformer tout système d'équations diophantiennes linéaires S où chaque variable est au plus de multiplicité deux, en un système iso-équivalent où chaque variable est également au plus de multiplicité deux, mais où toutes les équations seront de la forme $x = y+z$ ou $x = y$ et oùchaque variable de multiplicité deux apparait une fois dans chacune de ces équations. La preuve de ce lemme est assez simple, et consiste à décomposer les équations en sous-équations. Le nombre d'équations ainsi que le nombre de variables du nouveau système est polynômial par rapport au système S. La preuve de ce lemme se trouve en annexe.

Lemme 5 *Toute solution minimale d'un système d'équations diophantiennes linéaires tel que chaque variable soit au plus de multiplicité deux est telle que la valeur de chaque variable dans cette solution est au plus deux.*

La preuve de ce lemme est assez longue. L'idée est de transformer le système S et une solution s' donnée en un graphe non orienté, où chaque boucle représente une nouvelle solution qui est soit la solution nulle, soit une solution s' tel que $s' \leq s$. Ensuite, en utilisant les propriétés du graphe

construit nous pouvons montrer que l'on peut toujours décrémenter de un ou de deux un ensemble de variables pour obtenir une nouvelle solution du système. Ce qui implique que toute solution minimale aura au plus la valeur deux. La preuve de ce lemme se trouve également en annexe.

4 Preuve d'appartenance à #P du problème de comptage $\#Hilbert_2(\omega)$

Pour montrer que le problème $\#Hilbert_2(\omega)$ appartient à la classe $\#P$, nous allons utiliser la définition de la classe $\#P$ donnée par Kozen [Koz92] qui est plus formelle que celle donnée par Valiant [Val79]. Il nous faut donc montrer que pour un vecteur s et un système d'équations diophantiennes linéaires S où chaque variable est au plus de multiplicité deux : (i) il existe un algorithme polynômial permettant de déterminer si s est une solution minimale pour S ; (ii) il existe une constante $k \in \mathcal{N}$ telle que si s est une solution minimale pour S alors $\|s\| \leq \|S\|^k$. La condition (ii) est vérifiée de façon triviale. Il faut alors prouver que l'on peut tester en temps polynomial qu'un vecteur est solution minimale du système S. On peut tester en temps polynomial de façon triviale qu'un vecteur est solution du système S et qu'il vérifie la condition du lemme 5. Ensuite, nous allons ramener ce problème à un problème de recherche de circuit dans un graphe orienté (problème connu comme étant polynomial [CLR90]).

Le graphe $G_S(s)$ construit à partir de S et de s est un graphe biparti orienté ayant la particularité que toute solution minimale s' de S (telle que $s' \leq s$) est représentée par un circuit dans le graphe $G_S(s)$.

Dans un premier temps, nous supprimons toutes les variables du système S de valeur zéro et nous construisons un système S' iso-equivalent au système S telle que toute équation soit de la forme $x = y + z$ ou $x = y$, et telle que chaque variable de multiplicité deux apparaisse une fois dans chacune de ces équations. A la solution s de S, est associée une solution s' de S' telle que s est solution minimale pour S si et seulement si s' est solution minimale de S'.

A chaque variable x du système S' de valeur un (dans s') nous associons deux sommets du graphe $G_S(s)$ (x_u et x_v) et à chaque variable y de valeur deux dans s' nous associons quatre sommets (y_{u_1}, y_{u_2}, y_{v_1} et y_{v_2}). A chaque équation $x + y = z$ (x et y de valeur un, z de valeur deux) de S' nous associons les huit arcs suivants (x_u, z_{v_1}), (y_u, z_{v_1}), (x_u, z_{v_2}), (y_u, z_{v_2}), (z_{u_1}, x_v), (z_{u_1}, y_v), (z_{u_2}, x_v), (z_{u_2}, y_v), à l'équation $x = y$, où x et y sont de valeur un, nous associons les deux arcs suivants (x_v, y_u), (y_v, x_u), et enfin à l'équation

$x = y$, où x et y sont de valeur deux, nous associons les quatres arcs suivants (x_{v_1}, y_{u_1}), (y_{v_1}, x_{u_1}), (x_{v_2}, y_{u_2}), (y_{v_2}, x_{u_2}).

Un parcours dans ce graphe est alors un parcours à travers les équations de S, tel que si on décrémente de un chaque variable visitée, alors nous équilibrons chaque équation visitée. Un circuit représente alors une nouvelle solution s'' (ou la solution nulle si nous parcourons tous les sommets). De même un chemin d'une variable de multiplicité un vers une autre variable de multiplicité un représente également une nouvelle solution.

Pour limiter nos recherches à des circuits, nous relions chaque sommet de multiplicité un à un nouveau sommet w (pour tout sommet x de multiplicité un, nous ajoutons au graphe les deux arcs suivants (x, z) et (z, x)).

Nous avons alors les deux propriétés suivantes :

- Toute solution minimale s'' (telle que $s'' \leq s'$) correspond à un circuit dans le graphe $G_S(s')$.
- Tout circuit du graphe ne parcourant pas deux sommets de la forme x_{u_1} et x_{u_2} (ou x_{v_1} et x_{v_2}) est une solution minimale pour S.

On peut ensuite rechercher un tel circuit dans le graphe $G_S(s')$ en temps polynomial grâce à une recherche en profondeur.

5 Conclusion

L'appartenance à $\#P$ du problème $\#Hilbert_2(\omega)$ est le résultat le plus intéressant. Les résultats obtenus montrent la difficulté du comptage de l'ensemble complet et minimal d'unificateurs modulo la théorie AC. En effet, ce problème est la composition du problème $\#Hilbert$ avec le problème consistant à calculer à partir de la base de Hilbert le nombre de combinaisons des vecteurs que l'on peut obtenir tel que chaque composante soit non nulle. Nous avons pu obtenir les bornes supérieures pour les problèmes étudiés, mais nous n'avons actuellement pas de résultat de complétude (borne inférieure).

Annexe

Pour prouver le lemme 5, nous allons transformer le système d'équations diophantiennes linéaires où chaque variable est au plus de multiplicité deux en un système iso-équivalent ayant les propriétés suivantes (lemme 4):

- Chaque équation est de la forme

$$x_1 = y_1$$

$$x_1 + x_2 = x_3$$

- Chaque variable de multiplicité deux apparait dans deux équations distinctes dont une de la forme

$$x = y$$

Preuve du lemme 4 : Soit S un système d'équations diophantiennes linéaires, $AX = 0$, tel que chaque variable soit au plus de multiplicité deux. Alors, le système S' d'équations diophantiennes linéaires $BY = 0$ est obtenu à partir du système S de la façon suivante :

- Chaque variable x de S de multiplicité deux est remplacée par deux nouvelles variables x_1 et x_2, et l'équation $x_1 = x_2$ est ajoutée au système (les variables x_1 et x_2 sont donc de multiplicité deux). Nous obtenons alors un nouveau système S'' iso-équivalent au système S, tel que le coefficient multiplicateur de chaque variable soit au plus un, et tel qu'une variable de multiplicité deux de S'' apparaisse dans deux équations distinctes dont une de la forme $x = y$;

  Exemple 6 *Soit S le système :*

$$2x + y = z \quad y + v = u \quad 2w = z + v$$

  Alors, le système S'' est le suivant :

$$\begin{array}{ccc} x_1 + x_2 + y_1 = z_1 & y_2 + v_1 = u & w_1 + w_2 = z_2 + v_2 \\ x_1 = x_2 & y_1 = y_2 & z_1 = z_2 \\ v_1 = v_2 & w_1 = w_2 & \end{array}$$

- Soit E une équation de S'' de la forme suivante :

$$x_1 + x_2 + \cdots + x_r = y_1 + y_2 + \cdots + y_s$$

  On peut alors transformer la partie gauche de cette équation (ainsi que la partie droite) de la façon suivante :

L'expression $x_1+x_2+\cdots+x_r$, avec $r \geq 3$, est remplacée par l'équation $x_1 + x'_1$, et on ajoute l'ensemble d'équations suivant au système :

$$x'_1 = x_2 + x'_2$$

$$x'_2 = x''_2$$

$$x''_2 = x_3 + x'_3$$

$$\vdots \qquad \vdots$$

$$x''_{r-3} = x_{r-2} + x'_{r-2}$$

$$x'_{r-2} = x''_{r-2}$$

$$x''_{r-2} = x_{r-1} + x_r$$

En procédant de façon semblable pour le terme droite de l'équation nous obtenons un nouveau système d'équations diophantiennes linéaires tel que chaque équation soit de la forme suivante :

$$x_1 + x_2 = y_1 + y_2$$

$$x_1 + x_2 = y_1$$

$$x_1 = y_1$$

Le système peut être encore réduit à des équations de la forme :

$$x_1 + x_2 = y_1$$

$$x_1 = x_2$$

En effet, l'équation $x_1+x_2 = y_1+y_2$ est équivalente aux trois équations suivantes :

$$x_1 + x_2 = z_1$$

$$z_2 = y_1 + y_2$$

$$z_1 = z_2$$

Le nouveau système S' ainsi obtenu est iso-équivalent au système S'', et donc au système S. En effet chaque nouvelle variable z introduite vérifie une contrainte de la forme $z = x_1 + x_2 + \cdots + x_p$ où $x_1, \cdots, x_p$ sont des variables déjà présentent dans le système S. De plus la construction de S' implique que chaque équation est du type $x_1 + x_2 = y$ ou $x = y$, donc les propriétés du système S'' sont conservées. Le système S' ainsi construit a donc toutes les propriétés voulues. □

Dans un premier temps, nous allons prouver le lemme 5 dans une version simplifiée sans considérer les équations du type $x_a + x_b = x_c$ telles que $x_a = x_b$.

Preuve du lemme 5 (version simplifiée) : Soit S un système d'équations diophantiennes linéaires tel que chaque variable soit au plus de multiplicité deux. Pour prouver que pour toute solution minimale de S, la valeur maximale de chaque variable est au plus deux, il suffit de le montrer pour un système d'équations diophantiennes linéaires S' (où chaque variable est au plus de multplicité deux) ayant les propriétés suivantes :

- Chaque équation est de la forme suivante :

$$x_1 + x_2 = y_1$$

$$x_1 = y_1$$

- Chaque variable de multiplicité deux apparait au moins une fois dans une équation de la forme $x_1 = x_2$.

L'idée de la preuve est la suivante :

Soit S un système d'équations diophantiennes linéaires sur l'ensemble de variables $X = \{x_1, \cdots, x_k\}$, et soit $s = s_1 \cdots s_k$ une solution minimale de ce système telle qu'il existe $s_i \geq 3$. Nous allons prouver par l'absurde que s n'est pas une solution minimale pour le système S.

Soit x_i une variable telle que $s_i \geq 3$, et soit E_1 et E_2 les deux uniques équations où la variable x_i apparait :

- E_1 est de la forme $x_i + x_j = y_k$, $x_i = y_j + y_k$ ou $x_i = y_j$;
- E_2 (si x_i est de multiplicité deux) est nécessairement de la forme $x_i = y_j$.

Si nous décrémentons la variable x_i de un, et si celle-ci est de multiplicité deux, alors nous devons décrémenter la variable y_1 telle que $x_i = y_1$. Mais la variable y_1 étant présente dans une deuxième équation du type (on peut avoir $x_i = x_j$ mais ce cas particulier sera traité ultérieurement) :

$$y_1 = y_2 + y_3$$

$$y_1 + y_2 = y_3$$

$$y_1 = y_2$$

nous devons alors décrémenter la variable y_2 ou y_3 dans le premier cas, y_3 dans le second cas et y_2 dans le dernier cas. Le but étant de décrémenter la variable x_i en répercutant les modifications nécessaires pour obtenir une nouvelle solution en équilibrant chaque équation visitée. Dans un premier temps, nous ne nous intéressons pas au fait d'équilibrer l'équation E_1. La décrémentation de la variable x_i entraine un parcours parmi les variables et les équations de S que l'on peut assimiler à un parcours de graphe assez particulier. En effet, si une variable apparait dans une équation de la forme $x_1 + x_2 = x_3$ ou $x_1 = x_2 + x_3$, on doit équilibrer cette équation. Mais pour équilibrer celle-ci, nous devons décrémenter une nouvelle variable qui peut être de multiplicité deux et apparaitre dans une seconde équation de la forme $x = y$.

Le graphe construit a un seul nœud sans prédecesseurs (la variable x_i) et un nœud de ce graphe n'a pas de successeurs si et seulement si :

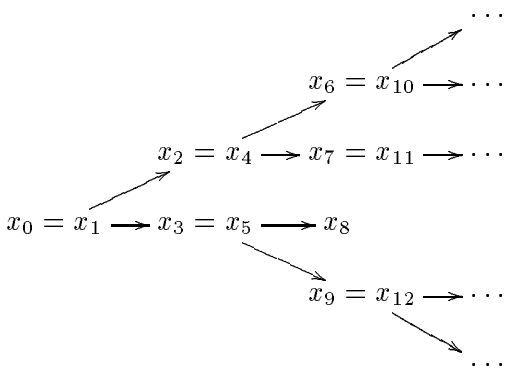
- C'est une variable de multiplicité un ;
- C'est une variable de l'équation E_1.

Remarque 7 *Dans un premier temps, pour clarifier cette preuve nous considérons que nous n'avons pas d'équations de la forme $x_a + x_b = x_c$ et $x_a = x_b$. Nous allons donc prouver le lemme 5 sans tenir compte de ce cas, et ensuite montrer que cette preuve s'applique également à celui-ci.*

Exemple 8 *Supposons que les équations suivantes appartiennent au système S :*

$$\begin{array}{ccc} x_0 + x_? = x_? & x_0 = x_1 & x_1 = x_2 + x_3 \\ x_2 = x_4 & x_3 = x_5 & x_4 = x_6 + x_7 \\ x_6 = x_{10} & x_7 = x_{11} & x_{11} + x_? = x_? \\ x_5 = x_8 + x_9 & x_9 = x_{12} & x_{12} = x_? + x_? \end{array}$$

Les variables $x_?$ étant des variables quelconques, x_0 étant une variable de valeur supérieure à trois, c'est-à-dire que l'on peut supposer que l'équation $x_0 + x_? = x_?$ est l'équation E_1.

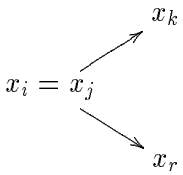


Les nœuds et les arcs de ce graphe ont les propriétés suivantes :

Le nœud $x_i = x_j$ signifie que les variables x_i et x_j sont de multiplicité deux et donc, décrémenter x_i implique qu'il faut décrémenter x_j.

$x_i \longrightarrow x_j$

signifie que la variable x_j est de multiplicité un ou deux et l'équation correspondante dans le système S est la suivante : $x_i + x_r = x_j$ ou $x_i = x_j$. On veut décrémenter x_i ce qui signifie que l'on doit décrémenter x_j pour que l'équation soit équilibrée. On cherche à prouver qu'il existe une solution $s' < s$ $(s' \neq 0)$, donc on ne désire pas incrémenter une variable. En effet, incrémenter x_r permet également d'équilibrer l'équation $x_i + x_r = x_j$.



signifie que les variables x_k et x_r sont de multiplicité un ou deux et l'équation correspondante dans le système S est $x_j = x_k + x_r$. On veut que cette équation soit équilibrée, on doit donc décrémenter x_k ou x_r.

Le graphe est construit à partir de la solution s supposée minimale. Chaque variable parcourue dans ce graphe est telle que sa valeur dans s soit non nulle. En effet, pour vérifier si une solution est minimale pour un système, les variables ayant une valeur nulle non pas besoin d'être prises en considération. Une équation de S de la forme $x_1 + x_2 = x_3$ telle que la valeur de x_2 soit nulle pour la solution minimale s est vue comme l'équation $x_1 = x_3$.

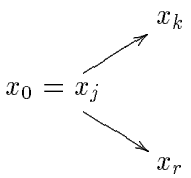
Le graphe construit de la manière ci-dessus est appelé graphe de dépendance du système S pour la solution s.

Lemme 9 *Soit S un système d'équations diophantiennes linéaires sous forme réduite pour lequel chaque variable est au plus de multiplicité deux, et soit s une solution minimale de ce système. Le graphe de dépendance du système S pour la solution s ne comporte pas de cycle.*

Preuve : Nous allons d'abord montrer que nous ne pouvons pas boucler sur la variable x_0 de valeur supérieure à trois (seul nœud du graphe sans prédécesseurs et variable génératrice du graphe de dépendance). Supposons que l'équation E_1 soit de la forme :

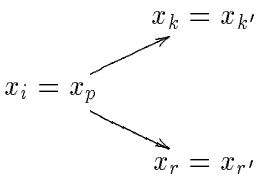
$$x_0 = x_1 + x_2$$

nous avons alors le nœud suivant dans le graphe de dépendance :



Nous supposons les variables x_1 et x_2 de valeur non nulle car, si la variable x_2 est nulle dans la solution s, l'équation $x_0 = x_1 + x_2$ est vue comme l'équation $x_0 = x_1$. La variable x_0 apparait uniquement dans les équations $x_0 = x_j$ et $x_0 = x_1 + x_2$. Mais, pour parcourir une variable dans le graphe de dépendance, il faut d'abord parcourir une variable apparaissant dans la même équation mais de coté opposé. Donc, s'il existe une boucle incluant la variable x_0 nous aurons parcouru la variable x_1 ou x_2 (ou x_j) auparavant, mais ces variables sont des éléments sans succésseurs d'après la construction du graphe. Nous ne pouvons donc pas avoir une boucle contenant la variable x_0. Il en est de même si l'équation E_1 est $x_0 + x_1 = x_2$ ou $x_0 = y_1$.

Supposons maintenant qu'il existe une boucle et soit x_p le premier élément de la boucle découvert (c'est-à-dire le premier élément apparaissant en double sur un chemin lors de la constuction du graphe). Si x_p apparait une première fois dans un nœud de la forme ci-dessous :



alors la variable x_p ne peut pas être le premier élément d'une boucle, sinon les variables x_k, x_r ou x_i seraient visitées auparavant. Il en est de même pour les variables x_k et x_r.

Si la variable x_p apparait une première fois dans un nœud de la forme ci-dessous :

$$x_i = x_p \longrightarrow x_r = x_{r'}$$

alors celui-ci correspond à une équation de la forme suivante :

- $x_p = x_r$ et nous ne pouvons pas boucler sur x_p ou x_r ;
- $x_p + x_? = x_r$ et dans ce cas nous pouvons boucler sur la variable x_r, car la variable $x_?$ n'a pas été visitée, mais nous sommes alors dans la situation suivante :

  nous voulons décrémenter la variable x_p, cela nous améne à décrémenter une suite de variables $x_r, y_1, \cdots, y_p, x_?$ en équilibrant toutes les équations où apparaissent ces variables jusqu'à $x_?$. Supposons que nous décrémentons toutes ces variables (mais uniquement ces variables sans même décrémenter x_p), nous obtenons alors une nouvelle solution s' non nulle (car $x_p \neq 0$), telle que $s' < s$ (car nous avons juste décrémenté des variables). La solution s n'ést donc pas minimale pour le système S (contradiction). Cette nouvelle solution s' peut être représentée à partir du système S et de la solution s de la façon suivante :

$$x_p \quad + \quad x_? \quad \underset{-1}{=} \quad x_r$$

Le graphe de dépendance constuit à partir d'une solution minimale ne contient donc pas de cycle, et chaque variable sans successeurs est soit une variable de l'équation E_1 ($\neq x_0$), soit une variable de multiplicité un. □

On peut maintenant prouver le lemme 5 dans une version simplifiée, c'est-à-dire sans considérer les équations de la forme $x_a + x_b = x_c$ telles que $x_a = x_b$. Pour cela, nous allons considérer l'ensemble des cas possibles sachant que chaque nœud sans successeurs du graphe de dépendance est soit une variable de multiplicité un, soit une variable de l'équation E_1, et que chaque équation visitée (sauf E_1) est équilibrée :

Cas 1 : Supposons d'abord que l'équation E_1 soit de la forme :

$$x_i + x_j = y_k$$

et que x_i soit une variable de valeur supérieure ou égale à trois dans la solution s. Notons $\begin{array}{c} x_i \\ \downarrow \\ x'_i \end{array}$ le fait qu'il existe un chemin dans le graphe de dépendance de S pour s de la variable x_i vers une variable x'_i de multiplicité un (c'est-à-dire un nœud sans successeurs dans le graphe de dépendance) et, notons $x_i \overset{+}{\frown} y_k$ le fait qu'il existe un chemin dans le graphe de dépendance de S pour s de x_i vers y_k.

Cas 1.1 : $\begin{array}{ccccc} x_i & + & x_j & = & y_k \\ \downarrow & & & & \downarrow \\ x'_i & & & & y'_k \end{array}$

Dans ce cas, on peut supposer que ces deux chemins ne sont pas contradictoires, c'est-à-dire que l'on ne décrémente pas deux fois une variable de valeur un. En effet, quand le chemin de la variable x_i vers la variable x'_i est découvert on peut décrémenter toutes les variables visitées avant de commencer la recherche d'un chemin à partir de la variable y_k (E_1 étant la seule équation non équilibrée après la découverte du chemin de x_i jusqu'à x'_i). On obtient alors une nouvelle solution s' ($s' \neq 0$) en décrémentant de un les variables des chemins de x_i jusqu'à x'_i et de y_k jusqu'à y'_k (l'équation E_1 étant ainsi équilibrée).

$$\begin{array}{ccccc} x_i & + & x_j & = & y_k \\ \updownarrow{\scriptstyle -1} & & & & \updownarrow{\scriptstyle -1} \\ x'_i & & & & y'_k \end{array}$$

Cas 1.2 : $x_i \overset{+}{\frown} y_k$ ou $x_i + x_j \overset{=}{\frown} y_k$

Il suffit de décrémenter de un les variables du chemin de x_i vers y_r ou de x_j vers y_k pour obtenir une solution $s' \neq 0$ telle que $s' < s$.

$$x_i \overset{+}{\underset{-1}{\frown}} y_k \text{ ou } x_i + x_j \overset{=}{\underset{-1}{\frown}} y_k$$

Cas 1.3 : $x_i + x_j = y_k$

Dans ce cas, soit on peut trouver deux chemins de y_k vers des variables de multiplicité un, soit on se retrouve dans un cas que l'on peut traiter différemment (cas 1.2).

Cas 2 : L'équation E_1 peut être également de la forme :

$$x_i = y_j + y_k$$

Dans ce cas, les cas ci-dessous peuvent être traités de manière identique au cas 1.

Cas 2.1 : $x_i = y_j + y_k$, avec $x_i \to x'_i$ et $y_k \to y'_k$

Cas 2.2 : $x_i = y_j + y_k$ ou $x_i = y_j + y_k$

Cas 2.3 : $x_i = y_j + y_k$

Cas 3 : Enfin l'équation E_1 peut être de la forme :

$$x_i = y_k$$

Dans ce cas, les deux cas possibles sont simples à traiter.

Cas 3.1 : $x_i = y_k$, avec $x_i \to x'_i$ et $y_k \to y'_k$

Cas 3.2 : $x_i = y_k$

Le lemme 5 est donc prouvé pour tout système d'équations diophantiennes linéaires sous forme réduite tel que chaque variable soit au plus de

multiplicité deux, et tel que celui-ci ne contienne pas de couple d'équations de la forme :

$$x_a + x_b = x_c$$

$$x_a = x_b$$

□

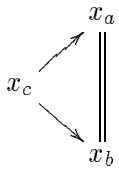
Nous allons maintenant étendre cette preuve au cas général.

Preuve du lemme 5 (version étendue) : Nous considérons maintenant également les équations du type :

$$x_a + x_b = x_c$$

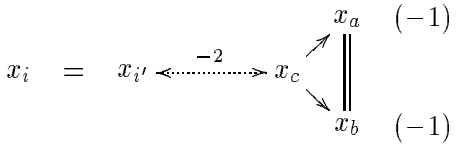
$$x_a = x_b$$

Le graphe de dépendance du système d'équations diophantiennes linéaires contient un nouveau type de nœud de la forme suivante :



La variable x_c doit alors être décrémentée de deux et pas de un comme dans les cas précédents. Nous avons trouvé dans le graphe de dépendance de S pour la solution s (supposée minimale) un chemin de la variable x_i jusqu'à la variable x_c. Il nous reste alors à analyser tous les cas possibles de manière fastidieuse afin de s'assurer que nous ne pouvons pas être dans un cas pouvant dégénérer, c'est-à-dire, un cas où la variable x_i doit être décrémentée d'une valeur supérieure (strictement) à deux.

Cas 1 : Chaque variable du chemin de x_i jusqu'à x_c est au moins de valeur deux dans la solution s (x_i y compris), dans ce cas, on peut décrémenter x_i de deux en équilibrant toutes les équations visitées.



Cas 2 : Il existe une variable x_r appartenant au chemin de x_i jusqu'à x_c telle que x_r soit une variable de valeur un dans la solution s. Supposons

que x_r soit la seule variable de valeur un entre x_r et x_c. Nous avons donc la situation suivante dans le graphe de dépendance :

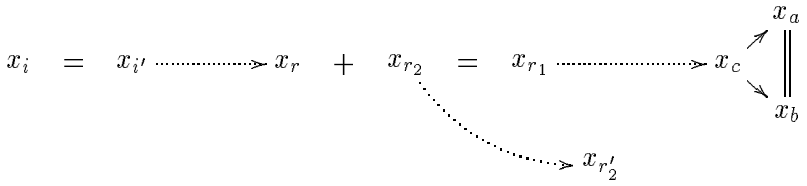
$$x_r \longrightarrow x_{r_1}$$

et l'équation E_r (équation à laquelle correspond cet arc du graphe) est de la forme :

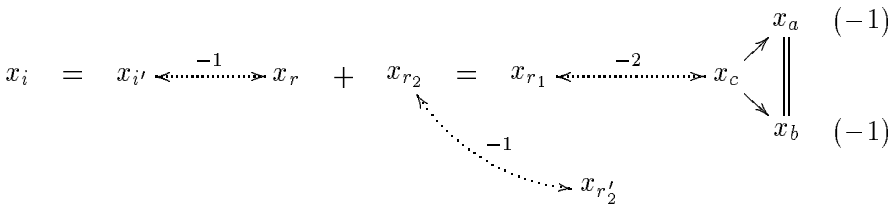
$$x_r + x_{r_2} = x_{r_1}$$

avec x_{r_1} de valeur supérieure ou égale à deux et x_r de valeur un. On doit alors décrémenter la variable x_{r_2} de un pour équilibrer l'équation E_r.

Cas 2.1 : Il existe un chemin de x_{r_2} jusqu'à une variable $x_{r'_2}$ de multiplicité un ne contenant aucune variable du chemin de x_i jusqu'à x_r, ni du chemin de x_r jusqu'à x_c.



On peut alors décrémenter la variable x_i de un en équilibrant toutes les équations différentes de E_1. Les variables du chemin de x_i jusqu'à x_r et de x_{r_2} jusqu'à $x_{r'_2}$ sont décrémentées de un, ainsi que les variables x_a et x_b tandis que les variables du chemin de x_{r_1} jusqu'à x_c sont décrémentées de deux. Ce qui nous permet d'équilibrer toutes les équations visitées.



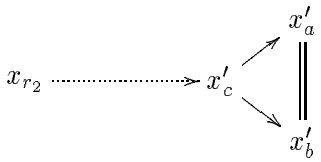
Remarque : Les méthodes de parcours du graphe de dépendance du système S pour la solution s implique que l'on ne parcours pas toutes le variables des équations visitées. De plus, si on visite deux fois une variable identique, nous devons d'abord visiter une nouvelle variable d'une équation déja visitée.

Exemple 10 *Supposons que nous ayons la situation suivante :*

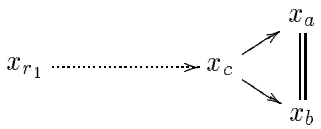
$$x_{p-1} = x_p \longrightarrow x_{p_1} = x_{p_1+1}$$

avec E_p une équation de la forme $x_p + x_{p_2} = x_{p_1}$. Cette équation est visitée mais pas la variable x_{p_2}. Lors de la recherche d'un nouveau chemin, si les variables x_p et x_{p_1} sont les premières variables rencontrées d'un chemin déjà parcouru alors nous avons visité la variable x_{p_2} auparavant (car sinon nous devons visiter les variables x_{p-1} ou x_{p_1+1} et dans ce cas, ni x_p, ni x_{p_1} ne sont les premières variables visitées).

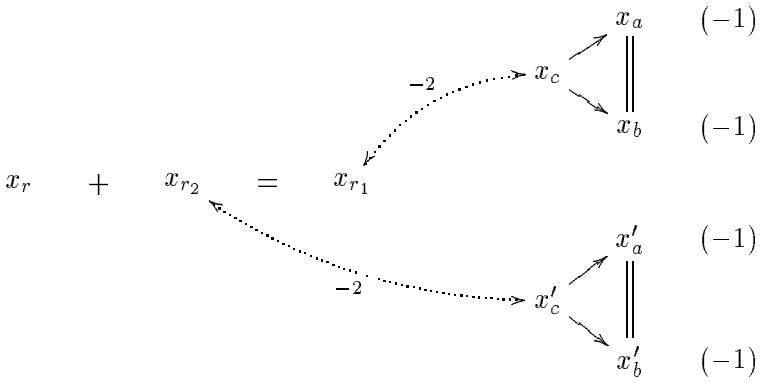
Cas 2.2 : En voulant décrémenter la variable x_{r_2} de un, nous aboutissons dans le graphe de dépendance à une équation de la forme $x'_c = x'_a + x'_b$ avec $x'_a = x'_b$. Nous avons donc un chemin de la forme suivante :



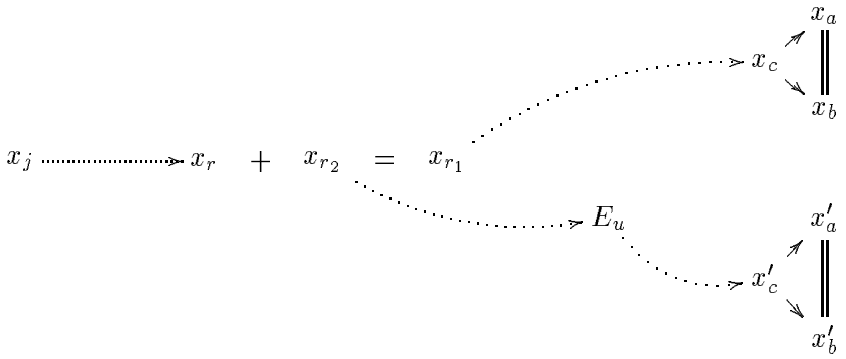
que nous supposons distinct du chemin :



Dans ce cas la solution s n'est pas minimale, car nous pouvons décrémenter les variables du chemin de x_{r_1} jusqu'a x_c et de x_{r_2} jusqu'à x'_c (ainsi que les variables x_a, x'_a, x_b et x'_b) et nous obtenons une solution $s' < s$ telle que $s' \neq 0$. Contradiction.

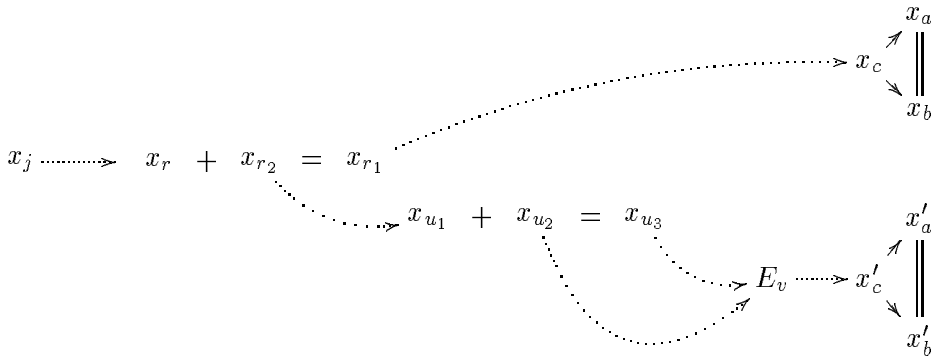


Cas 2.3 : En voulant décrémenter la variable x_{r_2} de un, nous aboutissons dans le graphe de dépendance à nouveau sur une équation de la forme $x'_c = x'_a + x'_b$ avec $x'_a = x'_b$. Mais, il existe une variable x_u sur le chemin de x_{r_2} jusqu'à x'_c de valeur un. Supposons que l'équation E_u où apparait x_u soit de la forme $x_{u_1} + x_{u_2} = x_{u_3}$, nous devons alors décrémenter x_{u_2} pour équilibrer l'équation E_u.

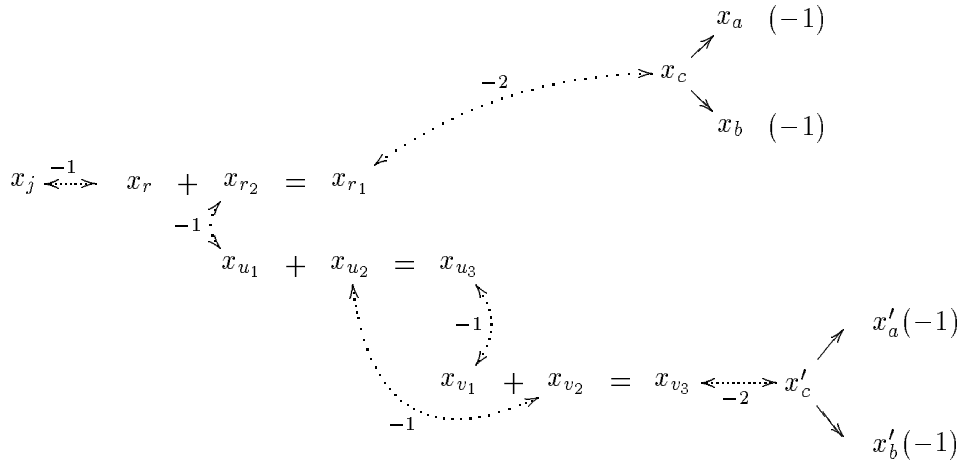


Cas 2.3.1 : Il existe un chemin de x_{u_2} vers une variable de multiplicité un ne contenant aucune variable déjà parcourue. Nous sommes alors dans un cas similaire au cas 2.2.

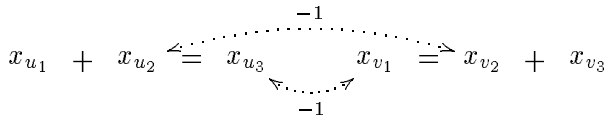
Cas 2.3.2 : En voulant décrémenter la variable x_{u_2} nous rencontrons une variable du chemin de x_{u_3} vers x'_c.



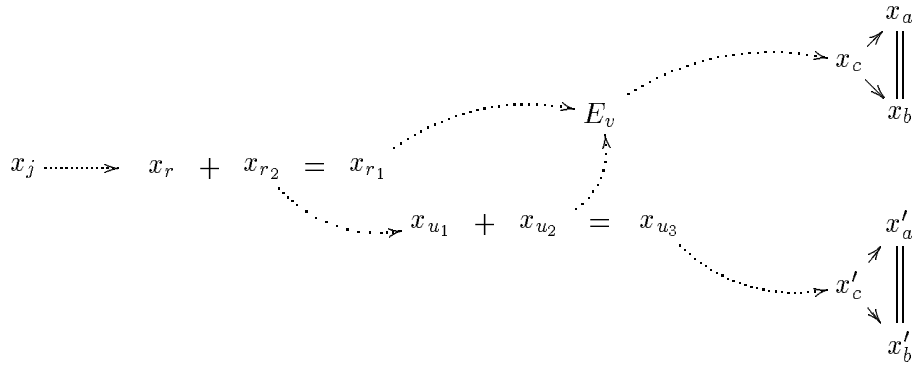
Si l'équation E_v est de la forme $x_{v_1} + x_{v_2} = x_{v_3}$. La variable x_j peut alors être décrémentée de un.



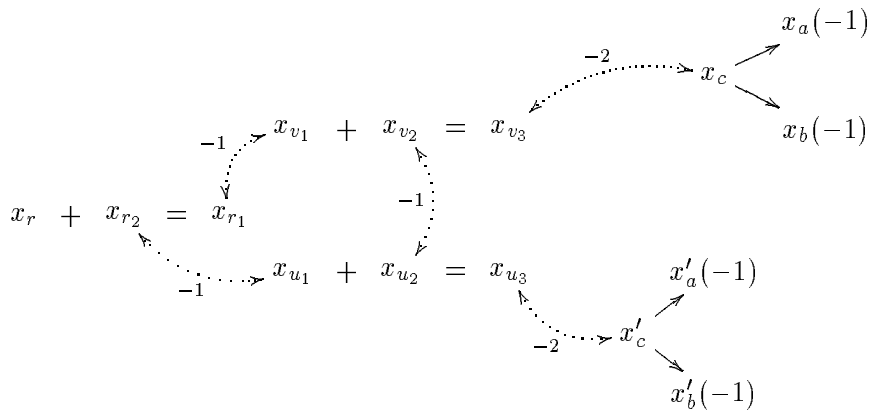
Sinon, l'équation E_v est de la forme $x_{v_1} = x_{v_2} + x_{v_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



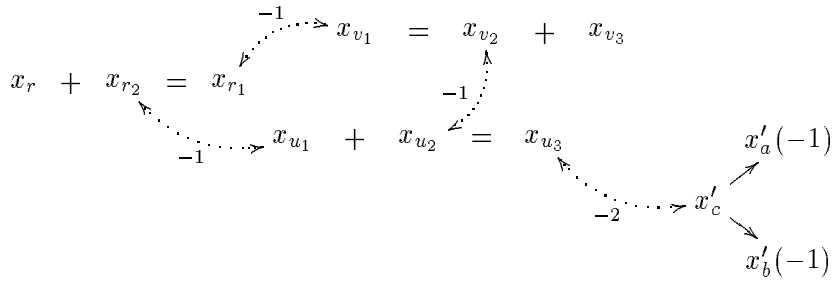
Cas 2.3.3 : En voulant décrémenter la variable x_{u_2} nous rencontrons une variable du chemin de x_{r_1} vers x_c.



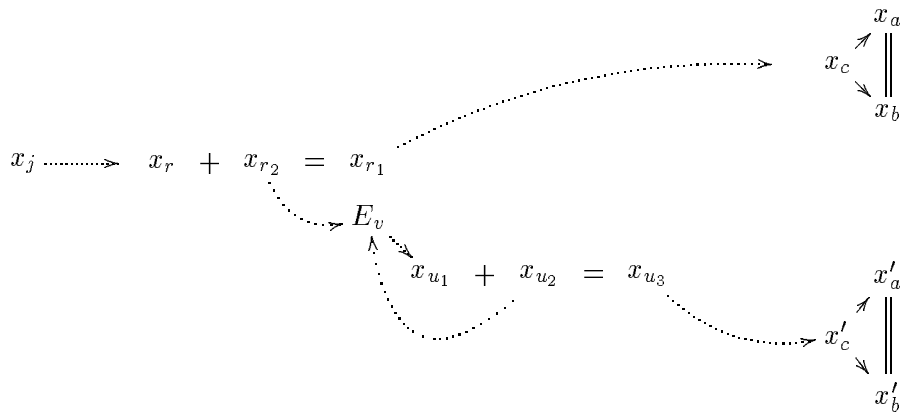
Si l'équation E_v est de la forme $x_{v_1} + x_{v_2} = x_{v_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



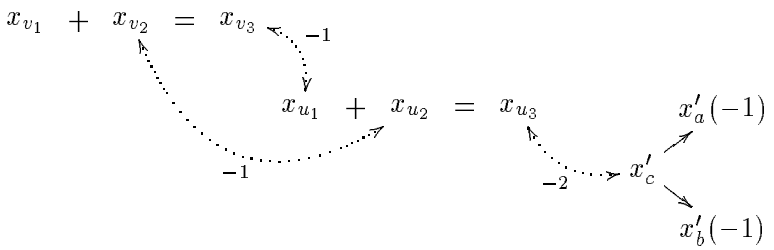
Sinon, l'équation E_v est de la forme $x_{v_1} = x_{v_2} + x_{v_3}$. Il existe également une solution $s' < s$ $(s' \neq 0)$:



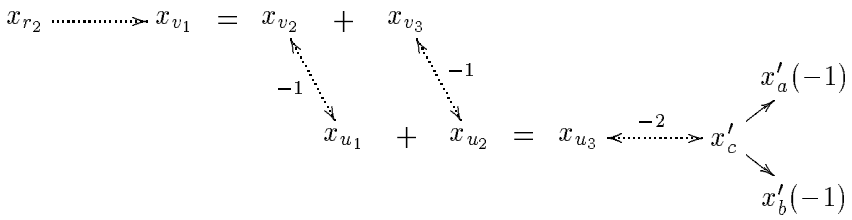
Cas 2.3.4 : En voulant décrémenter la variable x_{u_2} nous rencontrons une variable du chemin de x_{r_2} vers x_{u_1}.



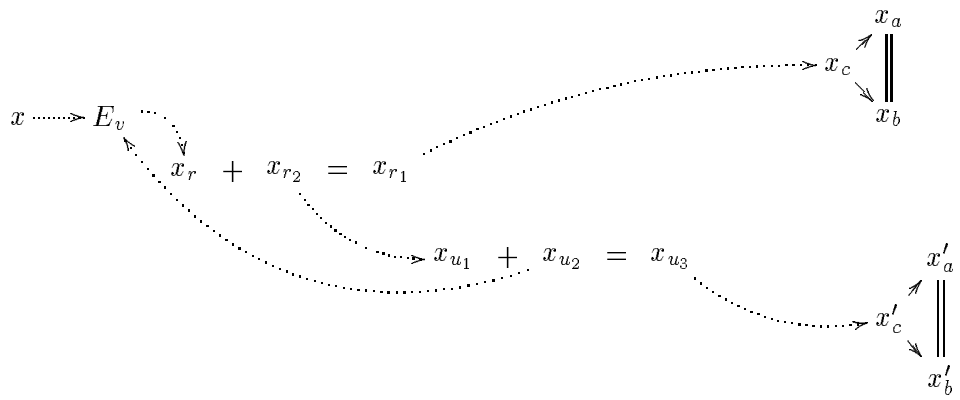
Si l'équation E_v est de la forme $x_{v_1} + x_{v_2} = x_{v_3}$. Il existe alors une solution $s' < s$ ($s' \neq 0$) :



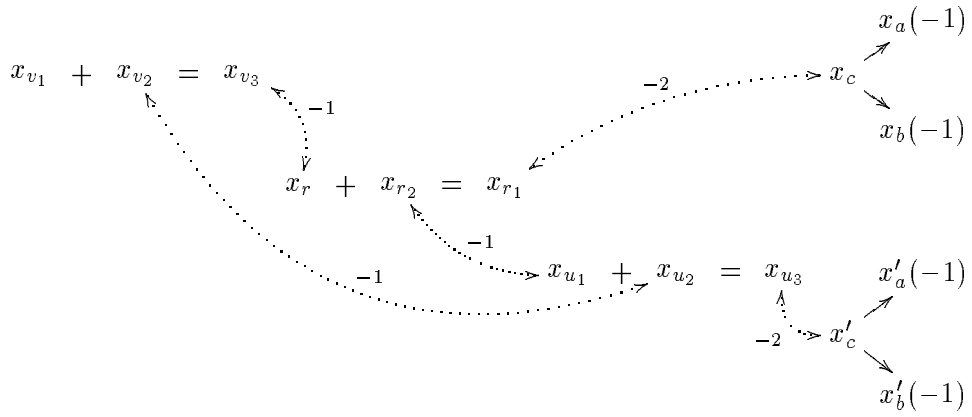
Sinon, l'équation E_v est de la forme $x_{v_1} = x_{v_2} + x_{v_3}$. Dans ce cas, nous devons décrémenter la variable x_{v_1} de deux. Nous sommes donc à nouveau dans un cas similaire au cas 2.2 ou 2.3, mais avec une variable x_{v_1} de profondeur strictement inférieure à la variable x_{u_1} (pour le cas 2.3) :



Cas 2.3.5 : En voulant décrémenter la variable x_{u_2} nous rencontrons une variable du chemin de x_j vers x_r.

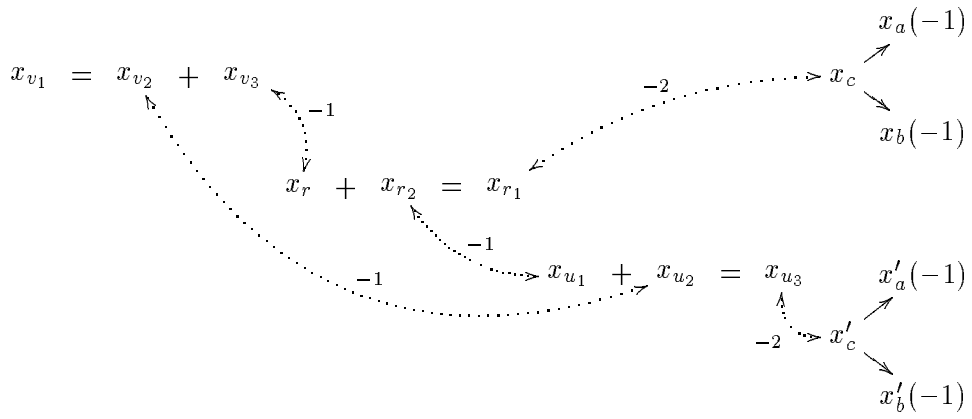


Si l'équation E_v est de la forme $x_{v_1} + x_{v_2} = x_{v_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



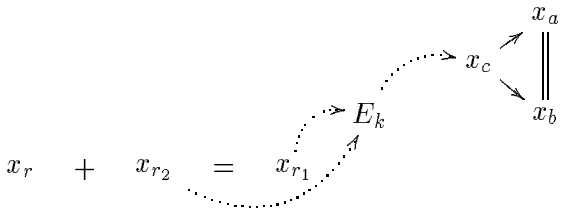
Sinon, l'équation E_v est de la forme $x_{v_1} = x_{v_2} + x_{v_3}$. Dans ce cas, nous devons décrémenter la variable x_{u_1} de deux. Nous sommes donc à nouveau dans un cas similaire au cas 2 mais, avec une variable x_{v_1} de profondeur

strictement inférieure à la variable x_c :

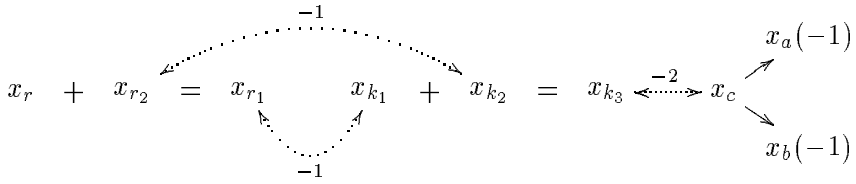


Cas 2.3.6 : En voulant décrémenter la variable x_{u_2} nous rencontrons une variable x_{c_1} telle qu'il existe une équation de la forme $x_{c_1} = x_{a_1} + x_{b_1}$ avec $x_{a_1} = x_{b_1}$. Nous itérons alors sur le cas 2.2 ou 2.3 (le nombre d'itérations étant nécessairement fini car le nombre de variables est fini).

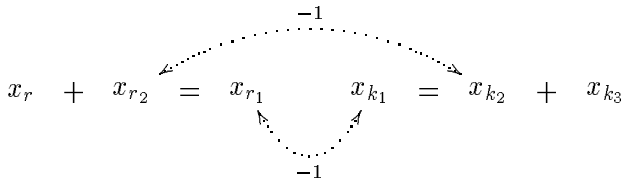
Cas 2.4 : En voulant décrémenter la variable x_{r_2} nous rencontrons une équation E_k déjà visitée lors de la recherche du chemin de x_{r_1} jusqu'à x_c.



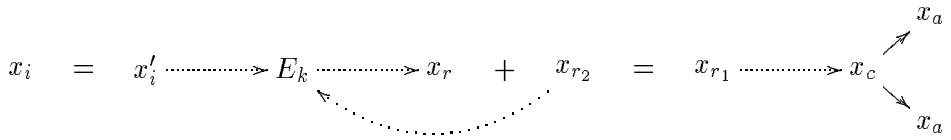
Si l'équation E_k est de la forme $x_{k_1} + x_{k_2} = x_{k_3}$. La solution s n'est pas minimale, et on peut construire une nouvelle solution $s' < s$ telle que $s' \neq 0$ de la façon suivante :



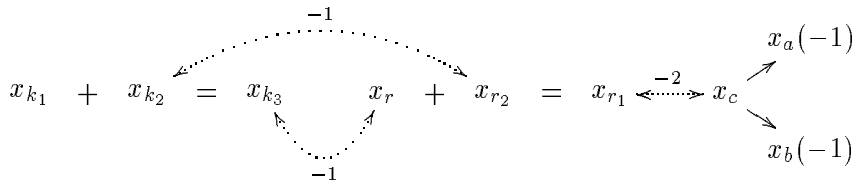
Sinon, l'équation E_k est de la forme $x_{k_1} = x_{k_2} + x_{k_3}$. Alors, la solution s n'est alors pas minimale, et on peut construire une nouvelle solution $s' < s$ telle que $s' \neq 0$ de la façon suivante :



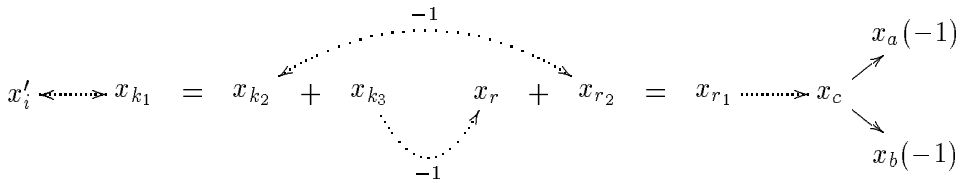
Cas 2.5 : En voulant décrémenter la variable x_{r_2} nous rencontrons une équation E_k déjà visitée lors de la recherche du chemin de x_i jusqu'à x_r.



Si l'équation E_k est de la forme $x_{k_1} + x_{k_2} = x_{k_3}$. Alors, la solution s n'est alors pas minimale, et on peut construire une nouvelle solution $s' < s$ telle que $s' \neq 0$ de la façon suivante :

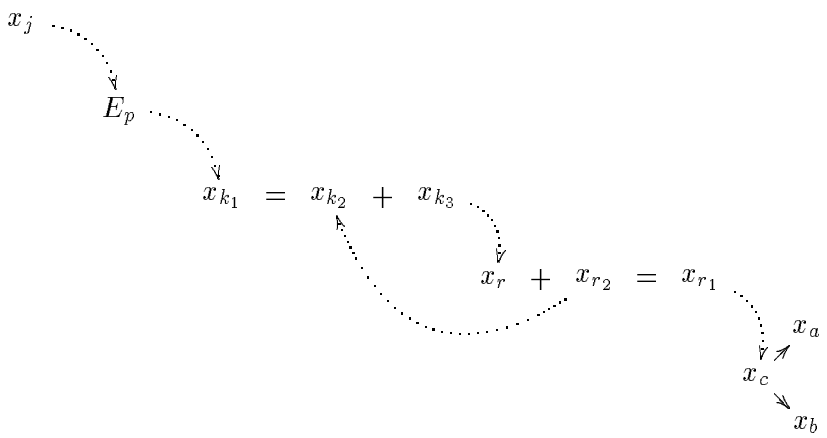


Si l'équation E_k est de la forme $x_{k_1} = x_{k_2} + x_{k_3}$. Nous sommes alors dans la situation suivante :



La variable x_{k_1} doit alors être décrémetée de deux.

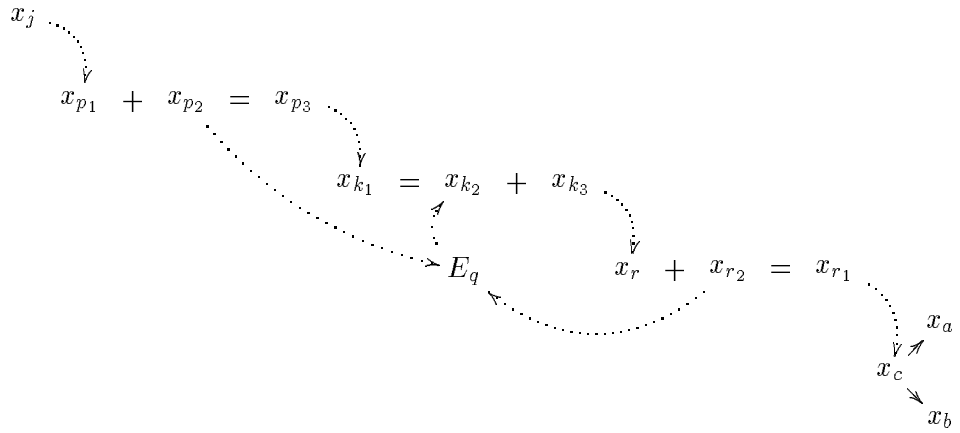
Nous allons voir ce cas en détail. Supposons qu'il existe une variable x_{p_1} sur le chemin de x_j jusqu'à une variable x_{k_1} de valeur un. Supposons que l'équation E_p où apparait x_{p_1} soit de la forme $x_{p_1} + x_{p_2} = x_{p_3}$, nous devons alors décrémenter la variable x_{p_2} de un pour équilibrer l'équation E_p.



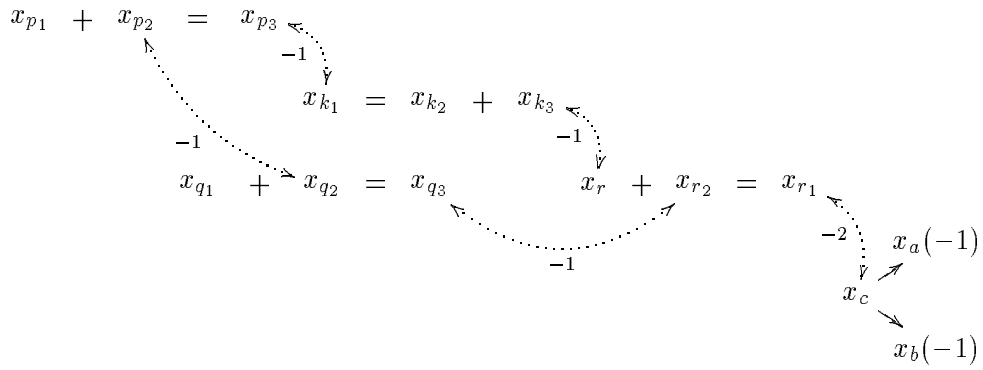
Cas 2.5.1 : Il existe un chemin de la variable x_{p_2} vers une variable de multiplicité un ne contenant aucune variable déjà parcourue. Nous sommes alors dans un cas équivalent au cas 2.1.

Cas 2.5.2 : En voulant décrémenter la variable x_{p_2} nous rencontrons une équation de la forme $x_{c_2} = x_{a_2} + x_{b_2}$ telle que $x_{a_2} = x_{b_2}$. Nous sommes alors dans le cas 2.2 ou 2.3.

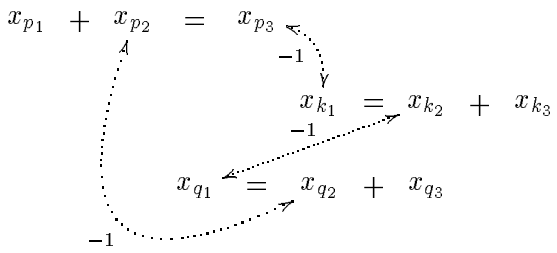
Cas 2.5.3 : En voulant décrémenter la variable x_{p_2}, nous rencontrons une variable x_{q_2} (d'une équation E_q) du chemin de x_{r_2} vers x_{k_2}.



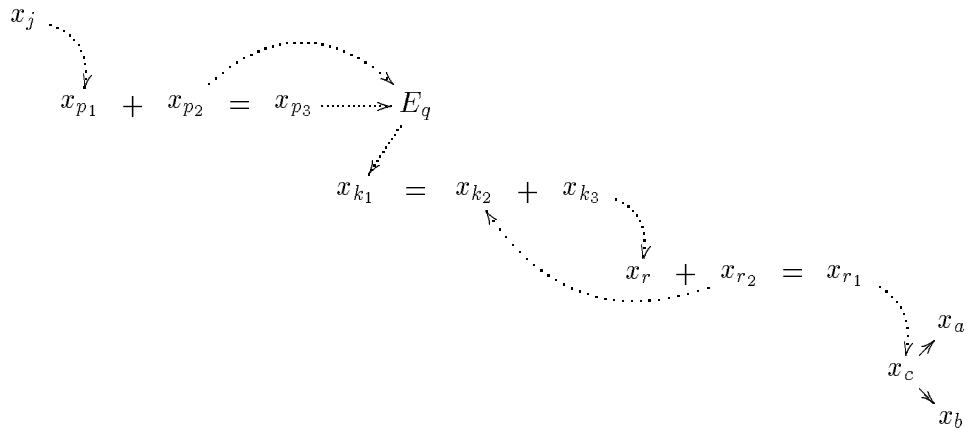
Si l'équation E_q est de la forme $x_{q_1} + x_{q_2} = x_{q_3}$. Il existe alors une solution $s' < s$ ($s' \neq 0$) :



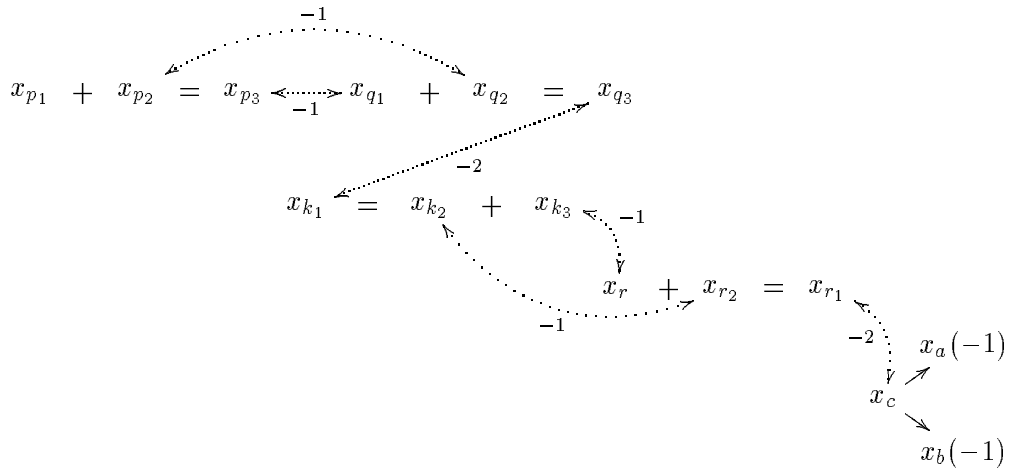
Sinon, l'équation E_q est de la forme $x_{q_1} = x_{q_2} + x_{q_3}$. Il existe alors une solution $s' < s$ ($s' \neq 0$) :



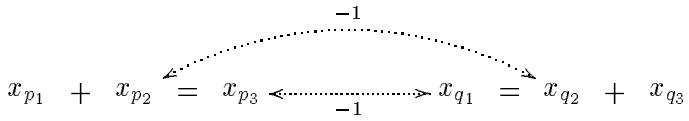
Cas 2.5.4 : En voulant décrémenter la variable x_{p_2}, nous rencontrons une variable x_{q_2} (d'une équation E_q) du chemin de x_{p_3} vers x_{k_1}.



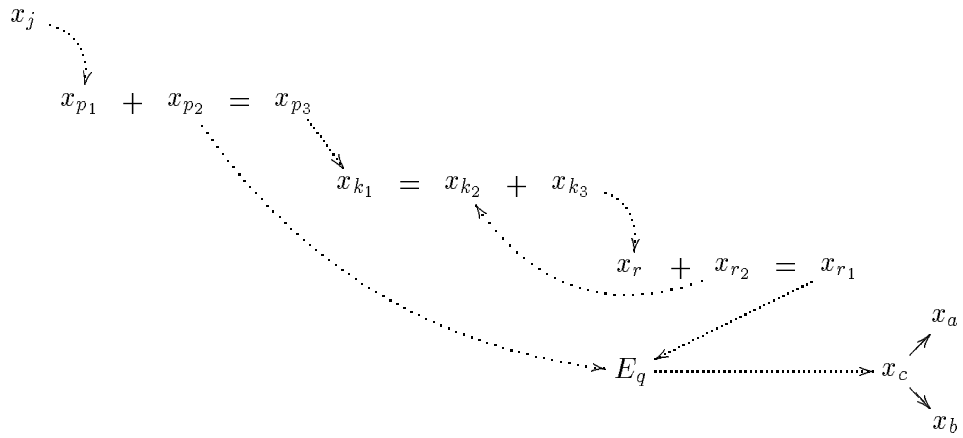
Si l'équation E_q est de la forme $x_{q_1} + x_{q_2} = x_{q_3}$. Il existe alors une solution $s' < s$ ($s' \neq 0$) :



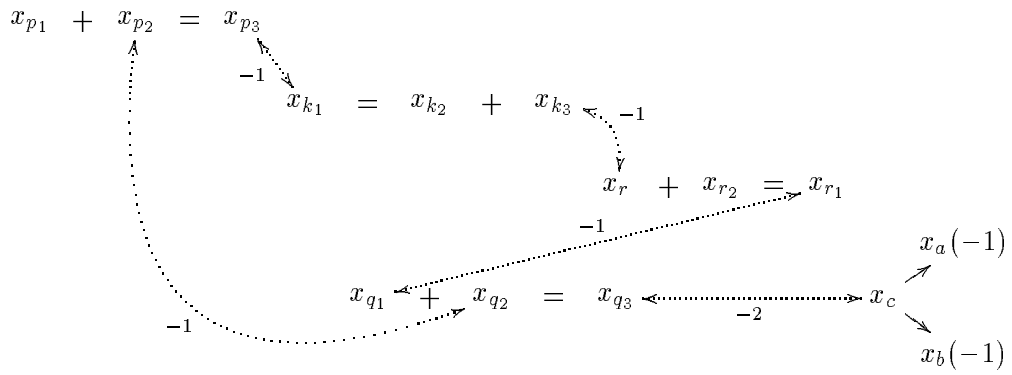
Sinon, l'équation E_q est de la forme $x_{q_1} = x_{q_2} + x_{q_3}$. Il existe alors une solution $s' < s$ ($s' \neq 0$) :



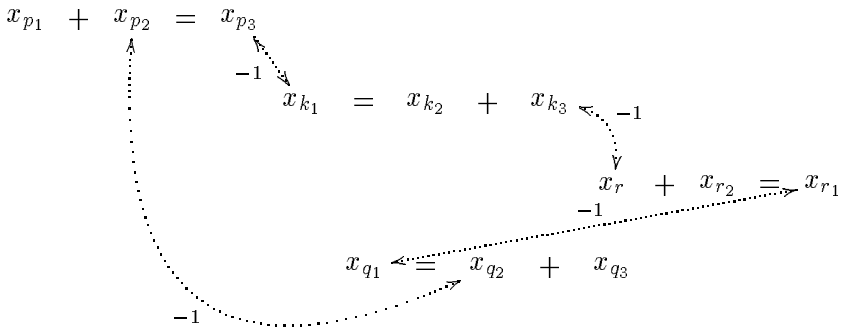
Cas 2.5.5 : En voulant décrémenter la variable x_{p_2}, nous rencontrons une variable x_{q_2} (d'une équation E_q) du chemin de x_{r_1} vers x_c.



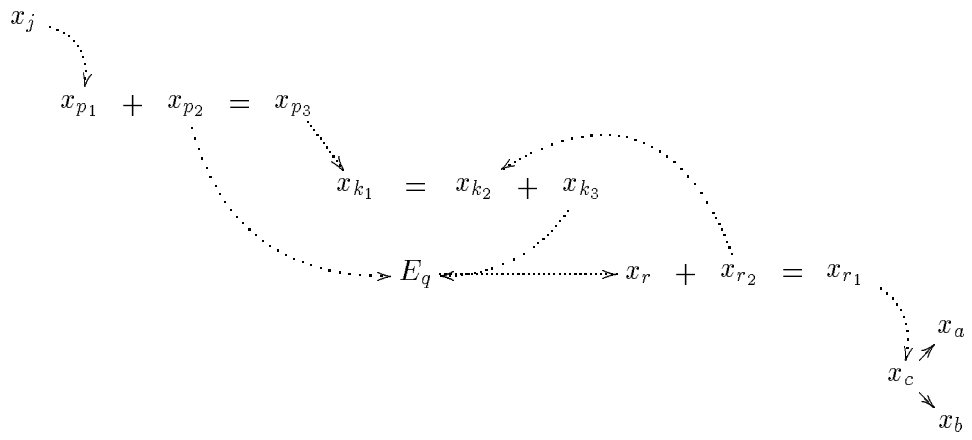
Si l'équation E_q est de la forme $E_q : x_{q_1} + x_{q_2} = x_{q_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



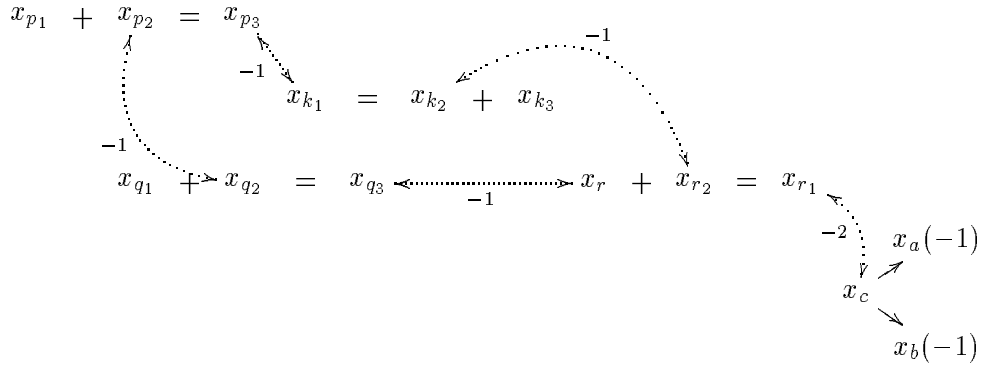
Sinon, l'équation E_q est de la forme $E_q : x_{q_1} = x_{q_2} + x_{q_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



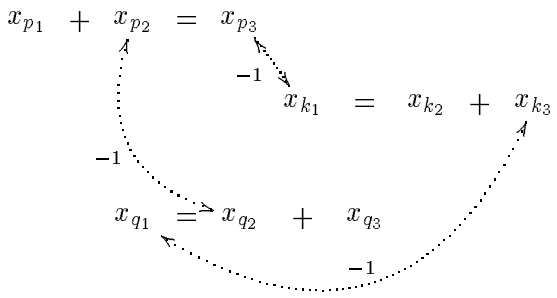
Cas 2.5.6 : En voulant décrémenter la variable x_{p_2}, nous rencontrons une variable x_{q_2} (d'une équation E_q) du chemin de x_{k_3} vers x_r.



Si l'équation E_q est de la forme $E_q : x_{q_1} + x_{q_2} = x_{q_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



Sinon, l'équation E_q est de la forme $E_q : x_{q_1} = x_{q_2} + x_{q_3}$. Il existe alors une solution $s' < s$ $(s' \neq 0)$:



Tous les cas traités précédemment sont tels que lorsque nous sommes à la recherche d'un nouveau chemin, nous voulons toujours décrémenter une variable de un. Donc, si une variable de l'équation E_1 est atteinte, alors nous pouvons montrer que la solution s n'est pas minimale exactement de la même manière que dans la preuve du lemme 5 dans sa version simplifiée. Les modifications interviennent pour les cas 1.1, 2.1 et 3.1 de la version simplifiée de la preuve. Mais, les variables pouvant toujours être décrémentées de un ou de deux, la preuve que s n'est pas une solution minimale dans ces cas reste pratiquement identique.

Donc, pour tout système d'équations diophantiennes linéaires tel que chaque variable soit au plus de multiplicité deux, chaque solution minimale (non nulle) de ce système est telle que chaque variable soit au plus de valeur deux. □

References

[CLR90] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to algorithms.* McGraw-Hill Book Company, 1990.

[HV94] L. A.. Hemaspaandra and H. Vollmer. The satanic notations : Counting classes beyond $\#p$ and other definitional adventures. *Sigact News*, 26(1):2–13, 1994.

[Koz92] D. Kozen. *The design and analysis of algorithms.* Springer Verlag, New York, 1992.

[Val79] L.G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.