Expérimentation des méthodes itératives de Newton et Gauss-Seidel en variables discrètes

Ze Qu Jiang

THESE

présentée à

l' Université Scientifique et Médicale de Grenoble

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE

Mathématiques Appliquées

(Analyse numérique)

par

Ze Qu JIANG

EXPERIMENTATION DES METHODES ITERATIVES DE NEWTON ET GAUSS-SEIDEL EN VARIABLES DISCRETES

Thèse soutenue le 31 mars 1982 devant la Commission d'Examen :

Monsieur	N. GASTINEL	:	Président
Messieurs	C. BENZAKEN E. GOLES F. ROBERT M. SOUTIF		Examinateurs

Stagiaire chinois n'ayant au départ aucune expérience de la vie et du travail à l'etranger, je suis très reconnaissant à F. ROBERT de m'avoir chaleureusement acceuilli et proposé un sujet de recherche : itérations discrètes, qui m'intéresse beaucoup. D'ailleurs, au cours de mon travail, j'ai été constamment soutenu par ses conseils et suggestions qui m'étaient indispensables.

Je suis très heureux d'avoir appris que M. N. GASTINEL avait accepté d'être le président de mon jury, ainsi que M. M. SOUTIF, M. C. BENZAKEN, M. F. ROBERT et M. E. GOLES seraient membres de ce jury.

Je remercie vivement M. A. EBERHARD et M^{elle} C. DICRESCENZO de m'avoir donné beaucoup d'assistance au cours de mon apprentissage de l'utilisation de l' ordinateu

Je voudrais aussi remercier M^{me} Cl. MEYRIEUX d'avoir pris des soins pour la frapp et la réalisation de ce travail ainsi que pour les autres choses concernant mon stage à l'équipe d'analyse numérique.

Je voudrais encore remercier tous mes collègues qui m'ont aidé et qui m'ont expri la gentillesse et l'amitié.

Z. JIANG

TABLE DES MATIERES

page

CHAPITRE 2 : MÉTHODE DE GAUSS-SEIDEL

CHAPITRE 3 : COMPARAISONS DES MÉTHODES

INTRODUCTION

Le comportement d'itérations dans un cadre discrèt avec une notion de convergence stationnaire provenant d'un outil métrique a été étudié par F. Robert qui l'a rédigé dans son polycopié "Itérations discrètes" [1]. Il s'agit d'une transposition dans un contexte discrèt de résultats classiques d'analyse d'itérations dans le cadre continu.

Voilà la raison qui m'a attirée de me consacrer à ce sujet que j'entrepris en démarrant par la réalisation de la méthode de Newton dans $(Z/2)^n$ à la fois simplifiée et standard.

Ce travail se consiste principalement en deux parties : le procédé d'itération et la résolution d'un système d'équations ayant la variable X dans $(Z/2)^n$ et la fonctin F(x) donnée soit par une table , soit par des expressions polynomiales.

Ayant recours aux méthodes usuelles, j'ai obtenu un algorithme qui peut être utilisé pour n étant petit ainsi que pour n assez grand (par exemple, n = 20 , dans ce cas, pensons que le nombre des éléments dans $(Z/2)^n$ dépasse un million ! ($2^{20} = 1048576$)) et qui se trouve en annexe 1.

Pour qu'on puisse effectuer l'itération de Newton dans $(Z/p)^n$, (p premier) j'ai étendu l'application de mon algorithme qui enfin devient principalement utilisable pour p et n quelconques, et qui nous permet d'expérimenter beaucoup d'exemples et d'examiner des propriétés diverses en relation avec l'étude théorique de la méthode faite par Melle. SL EL BERNOUSSI [3].

Tous ce qui concerne la méthode de Newton se trouve dans le premier chapitre où on peut aussi trouver quelques préparations nécessaires, une méthode pour résoudre un système d'équations linéaires dans $(Z/p)^n$ et quelques idées sur le calcul de dérivée discrète dans $(Z/p)^n$.

Pour bien comparer, je transpose une méthode de Gauss-Seidel dans $(Z/p)^n$ et fournis quelques résultats obtenus qui se trouvent dans le deuxième chapitre où on peut aussi trouver quelques notions sur les éléments propres d'une matrice à éléments dans Z/2.

A la fin, les comparaisons de ces trois méthodes et la conclusion se trouvent dans le troisième chapitre.

Le principal but de mon travail consiste non seulement à présenter l'expérimentation de certaines méthodes d'itérations discrètes et l'analyse des résultats divers, mais à révéler les problèmes et les difficultés qui existent à la fois théoriquement et expérimentalement dans ces méthodes afin d'attirer l'attention pour les résoudre.

D'après un proverbe chinois qui dit :

" D'un petit flacon sortira une jarre de vin "

je serais très heureux si ce que j'ai fait est de valeur utile même si petite pour les grands succès d'autrui dans ce domaine.

A cause de la limitation de mes connaissances, ainsi que des difficultés de la langue, je prie d'excuser les problèmes et les fautes qui existent certainement dans le texte qui suit.

Z. JIANG

Effectivement, nous avons jugé bien préférable de conserver tout son arôme à la syntaxe utilisée par Monsieur JIANG !

P. ROBERT

CHAPITRE I

MÉTHODES DE NEWTON

Rappelons, dans le contexte d'itérations sur $\mathbb{R}^n$, la méthode itérative de Newton : $x^{r+1} = x^r - A_r^{-1} F(x^r)$ pour la recherche d'une racine a de l'application F donnée de $\mathbb{R}^n$ dans $\mathbb{R}^n$ ($F(a) = 0$).
Si l'on prend pour A_r une matrice constante non singulière, on obtient la méthode dite Newton-simplifiée ; si $A_r = F'(x^r)$, la méthode est appelée celle de Newton-standard qui est très usuelle et fondamentale, au point de vue à la fois expérimental et théorique (référence [2]). A partir de là une idée s'est produite : est ce possible de transposer ces méthodes dans le contexte de variables discrètes, par exemple dans $(Z/p)^n$ (au lieu de $\mathbb{R}^n$) ? A l'aide de la notion de dérivée discrète et des opération dans Z/p, cette transposition est devenue possible :

I.1. LE CONTEXTE ET LE MATERIEL NECESSAIRE

I.1.1. CONTEXTE ET OPERATIONS

$$\text{Soit } X = \left\{ x \;\middle|\; x = (x_1,\ldots,x_n)^T \right\} = (Z/p)^n$$

avec $x_i \in Z/p = \{0,1,\ldots,p-1\}$ $(i=1,\ldots,n$; p premier)
et F une application de $(Z/p)^n$ dans $(Z/p)^n$ (cf [6]) On notera f_i les composantes de F, de sorte que la relation $y = F(x)$ s'écrit

$$y_i = f_i(x_1,\ldots,x_n) \quad \text{avec } x_j \in Z/p,\ i=1,2,\ldots,n,\ y_i \in Z/p .$$

On rappelle que pour a et b dans Z/p on utilise les opérations suivantes :

addition $\oplus$ dans Z/p : $a \oplus b = \begin{cases} a+b & \text{si } a+b < p \\ a+b-p & \text{sinon} \end{cases}$

soustraction $\ominus$: $a \ominus b = \begin{cases} a-b & \text{si } a \geq b \\ p+a-b & \text{sinon} \end{cases}$

multiplication $\otimes$: $a \otimes b = r$, r vérifiant $ab = p.q+r$
avec $q \in \{0,1,\ldots\} = \mathbb{N}$
+ - . sont dans les sens habituels.

Avec $\oplus$, $\ominus$, $\otimes$ on peut aussi définir les opérations de matrice et de vecteurs dont les éléments ou les composantes sont dans Z/p.

I.1.2. VOISINAGE

Le voisinage immédiat d'un point $x \in (Z/2)^n$ est l'ensemble noté V_x , des points de la forme : $\bar{x}^j = x \oplus e_j$ (j = 1,2,... n) (où $e_j \equiv (0,\ldots\underset{j}{1},\ldots 0)^T$ $(Z/2)^n$) , X^j est le jème voisin de x .

DEFINITION
Dans $(Z/p)^n$, (p > 2) , l'ensemble des points $V_d = \{\bar{X}^j \mid \bar{X}^j = X \oplus e_j\}$ seront appelé le voisinage à droite de X .
De même $V_g = \{\hat{X}^j \mid \hat{X}^j = X \ominus e_j\}$ serait appelé le voisinage à gauche de X , $\forall X \in (Z/p)^n$, $j = 1,2,\cdots n$.

REMARQUE
Puisque dans $(Z/2)^n$, l'opération $\oplus$ est identique à $\ominus$,
On a $V_x \equiv V_d \equiv V_g$ pour tout $x \in (Z/2)^n$.

I.1.3. CONVERGENCE

DEFINITION
Une suite de points dans $(Z/p)^n$, $X^0, X^1, \cdots X^r \cdots$ sera dite convergente vers un point $\xi \in (Z/p)^n$, s'il existe un entier naturel m tel qu'à partir du point x^m , $x^m = \xi$ (convergence stationnaire en ξ).

REMARQUE

Si cette suite est engendrée par une itération $x^{r+1} = F(x^r)$ démarrant d'un point de départ x° quelconque dans $(Z/p)^n$, on dira que cette itération est convergente. Ce ξ bien entendu est alors un point fixe de F .

DEFINITION

On dira qu'une itération a une convergence globale, si elle atteint le même (unique) point fixe en démarrant de tout point de $(Z/p)^n$ pour point initial x° . Quant à la convergence locale on emprunte une définition de [1] :

DEFINITION

Soit $\xi = F(\xi)$ un point fixe de F , dans $(Z/p)^n$, sera dit attractif dans un voisinage V_ξ de ξ si les deux condition suivantes sont réalisées :

a) $F(V_\xi) \subset V_\xi$

b) pour tout x° pris dans V_ξ , l'itération $x^{n+1}=F(x^n)$, finit par stationner en ξ au bout d'au plus n pas.

Si $p > 2$, V_ξ peut être soit le voisinage à droite, soit celui à gauche de .

I.2. DERIVEE ET DERIVATION DE FONCTION DANS Z/p

I.2.1. DEFINITION DE DERIVEE

DEFINITION 1

$\frac{\partial f(x)}{\partial X_j}$ sera appelée dérivée partielle (en la variable x_j) d'une fonction $f(x) \equiv f(x_1,\ldots,x_j,\ldots,x_n) : (Z/p)^n \longrightarrow Z/p$, avec par définition si $\frac{\partial f(x)}{\partial X_j} = f(x \theta e_j) \theta f(x) \equiv f(x_1,\ldots,x_j \theta 1,\ldots,x_n)$ $\theta f(x_1,\ldots,x_j,\ldots,x_n)$, $(x_j \in Z/p$, $j=1,\ldots,n)$.

DEFINITION 2

Dans la définition précédente, si $p > 2$, on appellera pour cette dérivée partielle, la dérivée à droite, notée $\frac{\partial f(X)}{\partial X_j}\Big|_d \equiv A$, si l'on remplace dans la définition 1 $x \theta e_j$ par $x \Theta e_j$, ainsi que $x_j \theta 1$ par $x_j \theta 1$, on appellera la dérivée à gauche, notée $\frac{\partial f(X)}{\partial X_j}\Big|_g \equiv B = f(x)-f(x \theta e_j)$.

DEFINITION 3

Une matrice (n , n) dont les éléments appartiennent à Z/p sera dite la matrice de dérivée en x notée F'(x) d'une fonction vector vectorielle

$F(x) \equiv F(x_1,\ldots,x_j,\ldots,x_n) : (Z/p)^n \longrightarrow (Z/p)^n$, si son jème vecteur colonne $\Delta_j = F(x\theta e_j)\theta F(x)$, pour tout $j=1,\ldots,n$.

De la même façon que la définition 1 et 2 on a par analogie, la

DEFINITION 4

Pour $p > 2$, dans la définition, on appellera :

la matrice de dérivée à droite , si $\Delta_j = F(x\theta e_j)\theta F(x)$;

la matrice de dérivée à gauche , si $\Delta_j = F(x)\theta F(x\theta e_j)$.

REMARQUE

Nous présenterons ici deux formules utiles :
Soit a une racine de F(x) dans $(Z/p)^n$, (F(a) = 0) ;
$\bar{x}^o \in V_d(a)$; $x^\circ \in V_g(a)$ $(\bar{x}^o - a = e_j$; $a - x^\circ = e_j)$
Alors, on a selon la définition 4 :

$F(\bar{x}^o) = F'_d(a) \otimes (\bar{x}^o \theta a) = F'_d(a) \otimes e_j, \ldots, (\alpha)$;

$F(x^\circ) = F'_g(a) \otimes (a \Theta x^\circ) = F'_g(a) \otimes e_j$; (β)

En général $F(x^r \Theta e_j)\Theta F(x^r) = F'_d(x^r) \otimes e_j$; (α')

$F'(\bar{x}^r \Theta e_j)\Theta F(x^r) = F'_g(x^r) \otimes e_j$; (β')

I.2.2. EXEMPLES DE DERIVEES DIVERSES

1 $f(X)$ $(Z/2)^2 \longrightarrow Z/2$ donnée par une table

X			f(X)
a	0	0	0
b	0	1	0
c	1	0	1
d	1	1	1

$$\frac{\partial f(a)}{\partial X_1} = f(c) \theta f(a) = 1$$

$$\frac{\partial f(a)}{\partial X_2} = f(b) \theta f(a) = 0$$

2 $f(X) : (Z/3) \quad Z/3$, donnée par une table

X			f(X)
a	0	0	1
b	0	1	0
c	0	2	1
d	1	0	2
e	1	1	0
f	1	2	0
g	2	0	1
h	2	1	2
i	2	2	1

$$\left.\frac{\partial f(a)}{\partial X_1}\right|_d = f(d) \theta f(a) = 1$$

$$\left.\frac{\partial f(a)}{\partial X_1}\right|_g = f(g) \theta f(a) = 0$$

$$\left.\frac{\partial f(a)}{\partial X_2}\right|_d = f(b) \theta f(a) = 2$$

$$\left.\frac{\partial f(a)}{\partial X_2}\right|_g = f(c) \theta f(a) = 0$$

3 $F(X) : (Z/2)^2 \longrightarrow (Z/2)$; donnée par sa table

X		F(X)	
0	0	0	1
0	1	0	0
1	0	1	0
1	1	1	1

$$F'(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$F'(d) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

4 $F(X) : (Z/3)^n \longrightarrow (Z/3)^n$, donnée par sa table

X		F(X)	
a	0 0	1	2
b	0 1	0	0
c	0 2	1	0
d	1 0	2	1
e	1 1	0	2
f	1 2	0	1
g	2 0	1	0
h	2 1	2	1
i	2 2	1	1

$$F'_d(a) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad F'_g(a) = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

$$F'_d(d) = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}, \quad F'_g(d) = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

I.2.3. DERIVATION DE FONCTION DANS Z/p

L'obligation de suivre les définitions des dérivées pour les dérivation nous amène a se demander si la dérivation peut être effectuée selon des règles usuelles pour $f(x) : (Z/p)^n \longrightarrow (Z/p)$ donnée par un polynôme.

PROPRIETE 1 : Formules de dérivation dans Z/2

Etant donné $f(x) : (Z/2)^n \longrightarrow Z/2$, on a des règles de base :

a) $\frac{\partial f(X)}{\partial X_j} = 0$, pour tout $j=1,\ldots,n$, ssi $f(x) = C$ (constante $\in Z/2$)

b) $\frac{\partial f(X)}{\partial X_{ij}} = \prod_{\substack{\ell=1 \\ \ell \neq j}}^{k} x_{i_\ell}$, si $f(X) = \prod_{\ell=1}^{k} x_{i_\ell}$ $(1 \leq i_\ell \leq n \ , \ 1 \leq k \leq n \ , \ 1 \leq j \leq K)$

($\prod$ étant le produit dans Z/2)

Il est facile de les prouver.

En outre, on en a encore deux concernant deux fonctions (polynômes)

c) $$\frac{\partial (f_1(X) \oplus f_2(X))}{\partial X_j} = \frac{\partial f_1(X)}{\partial X_j} \oplus \frac{\partial f_2(X)}{\partial X_j}$$

d) $$\frac{\partial (f_1(X) \otimes f_2(X))}{\partial X_j} = \frac{\partial f_1(X)}{\partial X_j} \otimes f_2(X \oplus e_j) \oplus \frac{\partial f_2(X)}{\partial X_j} \otimes f_1(X)$$

$$= \frac{\partial f_2(X)}{\partial X_j} \otimes f_1(X \oplus e_j) \oplus \frac{\partial f_1(X)}{\partial X_j} \otimes f_2(X)$$

Pour prouver d). On a selon la définition :

$$\frac{\partial(f_1(x)\otimes f_2(x))}{\partial X_j} = f_1(x\oplus e_j)\otimes f_2(x\oplus e_j) \oplus f_1(x)\otimes f_2(x)$$

$$= \{[f_1(x\oplus e_j)\otimes f_2(x\oplus e_j)] \oplus [f_1(x)\otimes f_2(x\oplus e_j)]\} \oplus$$

$$\{[f_1(x)\otimes f_2(x\oplus e_j)] \oplus [f_1(x)\otimes f_2(x)]\}$$

$$= f_2(x\oplus e_j)\otimes \frac{\partial f_1(x)}{\partial X_j} \oplus f_1(x) \otimes \frac{\partial f_2(x)}{\partial X_j}.$$

Pour obtenir la 2ème égalité de d , il suffit qu'on change les positions de $f_1(x)$ et $f_2(x)$.

REMARQUE

Il n'est que d, qui diffère un peu de la dérivation usuelle. Soit $F(x) = (f_1(x),;..,f_n(x))^T$ dont $f_i(x) : (Z/2)^n \longrightarrow Z/2$ sont des polynômes, alors $F'(x)$ peut se donner d'après les dérivées partielles de $f_i(x)$ de la façon usuelle :

$$F'(x) = \left(\frac{\partial f_i(x)}{\partial X_j}\right) .$$

PROPRIETE 2

Formule de dérivation dans Z/p . (p > 2 , premier)

Etant donné $f(x) : (Z/p)^n \longrightarrow Z/p$, Notons que

$A = \frac{\partial f(x)}{\partial X_j}\Big|_d$, $B = \frac{\partial f(x)}{\partial X_j}\Big|_g$, alors on a les formules suivantes :

a') $A = B = 0$, pour tout $j=1,...,n$, ssi $f(x) = C$ (constante de Z/p)

b') $A = B = C \prod_{\substack{\ell=1 \\ \ell\neq j}}^{K} x_{i_\ell}$, si $f(x) = C \prod_{\ell=1}^{K} x_{i_\ell}$

$(1 \leq i_\ell \leq n , 1 \leq K \leq n , 1 \leq j \leq K)$

(la droite de l'égalité étant le produit dans Z/p)

c') $A = A_1 \oplus A_2$, $B = B_1 \oplus B_2$, si $f(x) = f_1(x)\oplus f_2(x)$

$$A_i = \frac{\partial f_i(x)}{\partial X_j}\Big|_d \quad , \quad B_i = \frac{\partial f_i(x)}{\partial X_j}\Big|_g \quad (i=1,2)$$

d') $A = A_1 \otimes f_2(x \oplus e_j) \oplus f_1(x) \otimes A_2 = A_2 \otimes f_1(x \oplus e_j) \oplus f_2(x) \otimes A_1$

$B = B_1 \otimes f_2(x \oplus e_j) \oplus f_1(x) \otimes B_2 = B_2 \otimes f_1(x \oplus e_j) \oplus f_2(x) \otimes B_1$

Si $f(x) = f_1(x) \otimes f_2(x)$.

Pour la dérivation de puissance : x_j^m , $2 \leq m \leq p-1$)

e) Si $f(x) = x_j^m$, alors $A = [x_j \oplus 1]^m \ominus X_j^m$;

$B = x_j^m \ominus [x_j \oplus 1]^m$.

Soit une fonction vectorielle dans $(Z/P)^n$,
$F(x) = (f_1(x), \ldots, f_n(x))^T$ dont $f_i(x) : (Z/P)^n \longrightarrow Z/p$ sont des polynômes, alors les matrices de dérivée : $F'_d(x)$, celle à droite ; $F'_g(x)$ celle à gauche peuvent se donner d'après les dérivées respectives de $f_i(x)$, ou bien

$$F'_d(x) = \left(\frac{\partial f_i(x)}{\partial X_j}\Big|_d\right) \quad , \quad F'_g(x) = \left(\frac{\partial f_i(x)}{\partial X_j}\Big|_g\right) .$$

Ce qui suit sont des exemples sur les matrices de dérivée d'une fonction $F(x)$ donnée par des polynômes dans $(Z/p)^n$.

I.2.4. EXEMPLES DE DERIVATIONS

(Ici, on remplace $\oplus$, $\ominus$, $\otimes$ par + , - , . pour simplifier les écritures).

1. $p=2$, $n=3$

$$F(x) = \begin{cases} f_1 = (1-x_1)(1-x_2) + x_2 x_3 \\ f_2 = (1-x_1)(1-x_2) + x_1(1-x_3) \\ f_3 = (1-x_2)(1-x_3) + x_1(1-x_2) \end{cases}$$

étant équivalente à une table.

x			F(x)		
0	0	0	1	1	1
0	0	1	1	1	0
0	1	0	0	0	0
0	1	1	1	0	0
1	0	0	0	1	0
1	0	1	0	0	1
1	1	0	0	1	0
1	1	1	1	0	0

Selon les règles précédentes, on obtient la matrice de dérivée notée

$$F_1'(x) = \begin{pmatrix} x_2-1 & x_1+x_3-1 & x_2 \\ x_2-x_3 & x_1-1 & -x_1 \\ 1-x_2 & x_3-x_1-1 & x_2-1 \end{pmatrix}$$

A l'autre aspect, on peut l'obtenir selon la table, notée $F_2'(x)$, Après un travail laborieux, on vérifie que :

$$F_1'(a) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = F_2'(a) \; ; \; F_1'(e) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} = F_2'(e), \ldots$$

$$\ldots, F_1'(h) = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = F_2'(h)$$

2. $p=3$, $n=2$

$$F(x) = \begin{cases} f_1 = x_1^2 + x_1 x_2 + 1 \\ f_2 = x_1 + x_2^2 - x_1 x_2 \end{cases}$$

	x		F(x)	
a	0	0	1	0
b	0	1	1	1
c	0	2	1	1
d	1	0	2	1
e	1	1	0	1
f	1	2	1	0
g	2	0	2	2
h	2	1	1	1
i	2	2	0	2

Selon les règles précédentes, on obtient les matrices de dérivées suivantes :

$$F_{d_1}'(x) = \begin{pmatrix} 2x_1+x_2+1 & x_1 \\ 1-x_2 & 2x_2-x_1+1 \end{pmatrix}$$

$$F_{g_1}'(x) = \begin{pmatrix} 2x_1+x_2-1 & x_1 \\ 1-x_2 & 2x_2-x_1-1 \end{pmatrix}$$

A l'autre aspect, on peut les obtenir, selon la table, notées $F'_{d_2}(x)$ et $F'_{g_2}(x)$, alors on a :

$$F'_{d_1}(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = F'_{d_2}(a) \quad ; \quad F'_{g_1}(a) = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} = F'_{g_2}(a)$$

$$F'_{d_1}(b) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = F'_{d_2}(a) \quad ; \quad F'_{g_1}(b) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = F'_{g_2}(a)$$

. . .

$$F_{d_1}(i) = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} = F'_{d_2}(i) \quad ; \quad F'_{g_1}(i) = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} = F'_{g_2}(i)$$

I.3. METHODES ITERATIVES DE NEWTON.

Soit F une application de $(Z/p)^n$ dans $(Z/p)^n$, pour laquelle on cherche une racine a dans $(Z/p)^n$: $F(a) = 0$.

On transposera la méthode générale de Newton (référence [2]) de la façon suivante : on se donne une suite de matrices A_r (n,n) a éléments dans Z/p , un vecteur initial x° dans $(Z/p)^n$ et l'on définit la suite $x^\circ, x^1, \ldots, x^r, \ldots$, de la façon suivante :
x^r état connu, on calcule $F(x^r)$ et A_r .
On résoud, si possible , le système linéaire

$$(1) \quad \begin{cases} A_r \theta z = F(x^r) & (1') \\ \text{et l'on pose } x^{r+1} = x^r \theta z & (1'') \end{cases}$$

Selon le choix de A_r , on obtiendra différentes méthodes dont voici les deux plus courantes :

I.3.1. METHODE DE NEWTON SIMPLIFIEE

Dans le système (1) , si A_r est à la fois constante et non singulière, on note $A_r = A$ indépendant à la fois de x et de γ , on appellera la méthode de Newton simplifiée, (1) peut devenir une seule formule suivante :

$$x^{r+1} = x^r \ominus A^{-1} \otimes F(x^r) \quad \ldots (2)$$

A^{-1} étant l'inverse de A ($A \otimes A^{-1} = A^{-1} \otimes A = I$)

REMARQUE 1

Evidemment pour que a soit une racine de la fonction F(x) dans $(Z/p)^n$, (F(a) = 0), il faut et il suffit que a soit un point fixe de l'itération (2).

REMARQUE 2

Si nous posons $N(x) = x \ominus A^{-1} \otimes F(x)$, l'itération de Newton simplifiée est la méthode d'approximations successives (itération parallèle), $x^{r+1} = N(x^r)$, (r=0,1,2,...).
Particulièrement, si on prend A = I , on obtiendra la forme la plus simple de (2) : $x^{r+1} = x^r \ominus F(x^r)$ itération destiné à résoudre l'équation F(x) = 0.
La réalisation de cette méthode est si simple qu'il n'en est rien à dire. Le comportement de l'itération sera décrit plus loin.

I.3.2. METHODE DE NEWTON STANDARD.

Dans le système (1) , si $A_r = F'(x^r)$, (1) deviendra

$$(3) \quad \begin{cases} F'(x^r) \otimes z = F(x^r) & (3') \\ x^{r+1} = x^r \ominus z & (3'') \end{cases}$$

On appelle (3) la méthode de Newton-Standard.

REMARQUE 3

Bien entendu $F'(x^r)$ peut être la dérivée à droite $F'_d(x^r)$ ou la dérivée à gauche $F_g(x^r)$. En raison de la similitude de ces deux dérivées j'ai effectué mes exemples toujours avec $F'_d(x^r)$.

REMARQUE 4

Si $F'(x^r)$ est régulière, le système (3) sera résoluble de façon unique ; dans ce cas, on pourrait écrire (3) sous la forme suivante :

$$x^{r+1} = x^r \theta [F'(x^r)]^{-1} \mathbb{Z} F(x^r)$$

Si $F'(x^r)$ est singulière, dans ce cas, l'existence de solution de (3) dépend de la cohérence de $R[F'(x^r)]$ et $R[\bar{F}'(x^r)]$ qui sont les rangs de $F'(x^r)$ et de $\bar{F}'(x^r)$ respectivement où $\bar{F}'(x^r)$ étant matrice (n,nx1) est constitué par $F'(x^r)$ en ajoutant $F(x^r)$ comme son dernier vecteur colonne.

REMARQUE 5

La réalisation de cette méthode est présentée dans mon algorithme qui se trouve à l'annexe 1. J'utilise souvent un procédé avec lequel lorsqu'un point fait sa parution de nouveau, l'itération doit reprendre un nouveau point de départ (pour éviter procéder infinitivement) ainsi de suite jusqu'à ce que l'itération totale dans $(Z/p)^n$ soit obtenue.

I.3.3. UNE METHODE POUR RESOUDRE LE SYSTEME LINEAIRE (3).

Dans le contexte de variable continues, la méthode de Gauss est très usuelle grâce à son économie et à sa stabilité. Nous allons adapter cette méthode au cas des variables discrètes (système linéaire dans $(Z/p)^n$) .

1. Introduction

Ce qui suit nous montre brièvement quelques exemples typiques

avec p=n=3.

$F'(x^r)$ $\quad F(x^r)$

1° $\left|\begin{matrix} 0 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 2 & 2 \end{matrix}\right| \xrightarrow{③ \ominus 2 \otimes ②} \left|\begin{matrix} 0 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 \end{matrix}\right| \xrightarrow{① \oplus ②} \left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 \end{matrix}\right| \xrightarrow{② \ominus ①}$

$\xrightarrow{③ \ominus 2 \otimes ①} \left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}\right| \xrightarrow{② \ominus 2 \otimes ③} \left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{matrix}\right|$ d'où $z = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}$

2° $\left|\begin{matrix} 0 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 1 & 2 \end{matrix}\right| \xrightarrow{③ \ominus 2 \otimes ②} \left|\begin{matrix} 0 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{matrix}\right| \xrightarrow{1 \oplus 2} \left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{matrix}\right| \xrightarrow[③ \ominus 2 \otimes ①]{② \ominus ①}$

$\left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{matrix}\right|$ la troisième équation est contradictoire alors, il n'y a pas de solution pour z .

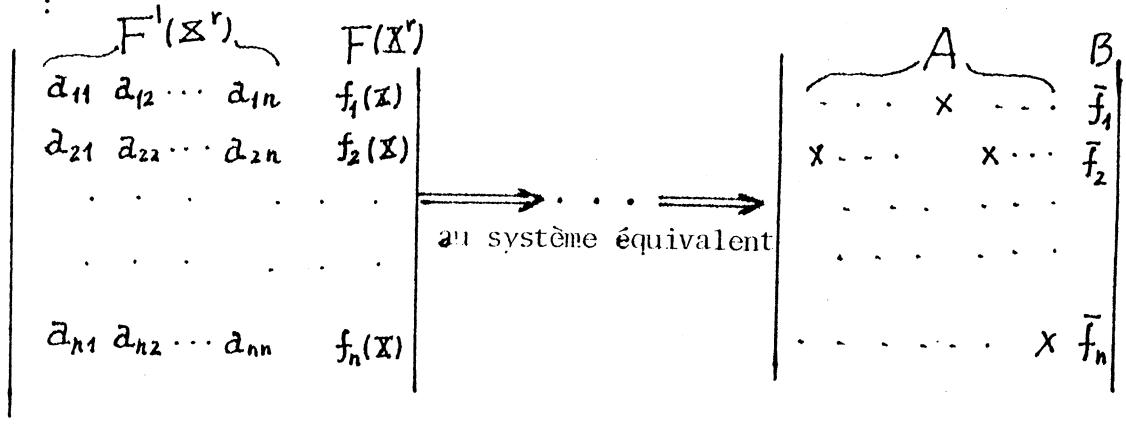
$\left|\begin{matrix} 0 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 1 & 1 \end{matrix}\right| \xrightarrow{③ \ominus 2 \otimes ②} \left|\begin{matrix} 0 & 2 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 0 & 1 \end{matrix}\right| \xrightarrow{① \div ②} \left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 0 & 1 \end{matrix}\right| \xrightarrow[③ \ominus 2 \otimes ①]{② \ominus ①}$

$\left|\begin{matrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{matrix}\right|$ Il est évident que la troisième composante des solutions du système peut être choisie arbitraire dans Z/3.

Dans ce cas, il y a trois solutions pour z ,

$z_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $z_2 = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}$, $z_3 = \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix}$.

Bien entendu, tous ces opérations utilisent la division $\oplus$, l'inverse de multiplication $\otimes$, qui existe effectivement lorsque p est un nombre premier, (Z/p est alors un corps) (on y voit $1 \oplus x$ se paraître sous la forme du nombre inverse de x).
En cas général, p premier, n entier positif, en faisant le même procédé (combinaisons linéaires de lignes) on passe du système donné :



Les X représentent les éléments non nuls, les autres sont nuls .
La matrice finale A est alors caractérisée de la façon suivante :
1) Chaque colonne a un élément non nul au plus.
2) En suite, on utilise un ensemble noté $T = \{ t_1, \ldots, t_\ell \}$ où $t_1, \ldots, t_\ell$ sont les numéros des lignes de A identiquement nulles ($0 \leq \ell \leq n$).

REMARQUE 6

Les positions des X, ou bien la forme du système final A dépend du choix des lignes participant aux combinaisons linéaires. Bien que cette forme de A puisse varier, les solutions du système original ne pourrait jamais être changées.

2. Solutions du système (3).

PROPOSITION 1

Lorsqu'il est soluble, le nombre m de solutions du système (3) va être donné par la formule suivante : $m = p^{\ell}$.
En effet, si $\ell = 0$, c'est-à-dire, si A n'a aucune ligne nulle il est clair alors que chaque ligne a un et seulement un élément non nul.
Dans ce cas, le système (3) a une solution unique : $m = p^{\circ} = 1$.
Si $1 \leq \ell < n$, il existe au moins une ligne numérotée t avec $t \notin T$. Dans cette ligne, on marque i le numéro de la colonne où le premier élément non nul est situé. On fait de même sur toutes les lignes dont les numéros n'appartienne pas à T . On obtient $\{i_1,\ldots,i_k\} = I$, évidemment $K = n - \ell$. Les numéros des autres colonnes sont $\{j_1,\ldots,j_\ell\} = J$,

i) Si $\bar{f}_t = 0$, $\forall\, t \in T$, cela signifie que le système (3) est soluble. Sans perdre de généralité, on peut supposer que les composantes $x_{j_1},\ldots,x_{j_\ell}$ des solutions soient indépendantes. Les autres composantes $x_{i_1},\ldots,x_{i_k}$ dépendent éventuellement de $x_{j_1},\ldots,x_{j_\ell}$.
N'importe quel membre de Z/p peut se donner à x_j , pour $\forall\, j \in J$, même pour $\ell = n$, toutes les composantes sont indépendantes. C'est-à-dire que toutes les possibilités de combinaisons de $x_{j_1},\ldots,x_{j_\ell}$ dans Z/p conviennent, d'où les p^{ℓ} solutions du système, selon une formule de combinaison (dans l'exemple précédent, $\ell = 1$, $p = 3$, alors $m = 3^1 = 3$).

ii) Si pour certain $t \in T$, on a $\bar{f}_t \neq 0$, il est clair que le système est impossible. En effet, pourqu'on puisse conclure que le système (3) n'a pas de solution, il faut et il suffit qu'il existe au moins un $t \in T$ vérifiant $\bar{f}_t$ non nul. Dans ce cas on obtient au moins une équation contractoire du système (3).

I.4. LE COMPORTEMENT ITERATIF DE NEWTON POUR F(x) DONNEE ARBITRAIREMENT.

Une fonction $F(x) : (Z/p)^n \longrightarrow (Z/p)^n$, peut être donnée de façon différente, généralement, soit par n polynômes de degré $\leq p-1$ à coefficients dans Z/p, soit par une table tirée au hasard. Dans ce paragraphe, on parlera surtout de cette dernière façon qu'on utilisera souvent pour expérimenter le comportement itératif de la méthode.

I.4.1. NEWTON SIMPLIFIE

i) Configuration du graphe itératif

Rappelons la méthode : $x^{r+1} = x^r \ominus [A^{-1} \otimes F(x^r)]$ (2)

PROPOSITION 1

Dans le graphe de Newton simplifié, un point quelconque dans $(Z/p)^n$, a un et seulement un successeur qui va poursuivre jusqu'à ce qu'un point fixe ou un cycle apparaisse.

DEMONSTRATION

C'est assez évident, puisque A est inversible : x^{r+1} , est déterminé de façon unique. Par ailleurs, puisque $(Z/p)^n$ est un ensemble fini (a p^n éléments), la suite engendrée va certainement finir sur un point déjà itéré ; il se forme conséquemment un cycle (pour un cycle de longueur 1, on dit aussi un point fixe).

REMARQUE 1

La longueur du transitoire (c'est-à-dire le nombre de pas qu'il faut pour obtenir un point du cycle) est très variable selon les cas, parmi nombreux exemples. Quelque fois elle est bien supérieur à n, (cf. Fig. 1.1). Quelque fois il existe beaucoup de points de départ pour lesquels la longueur du transitoire est inférieure à n (cf. Fig 2.1). En général, il n'y a pas de liaison évidente, la longueur du transitoire et la dimension n..
On peut simplement dire que le transitoire croit lorsque n croît.

REMARQUE 2

Les longueurs des cycles qui se paraissent dans des différents exemples effectués en méthode de Newton simplifiée sont variables. Un cycle de longueur 2 avec p=2 , n=4, se trouve dans Fig. 3.5, celui de longueur 3 avec p=5, n=2 se trouve dans Fig. 5.1 ; celui de longueur 5 avec p=n=3 , se trouve dans Fig. 4.1.

REMARQUE 3

Le nombre de cycles n'est pas grand par rapport au nombre de points de $(Z/p)^n$ (p^n). Expérimentalement, la fréquence de ce nombre vibre à l'environ de **2** parmi nombreux exemples, (cf. Fig. 1.1 avec p=2, n=5 ; Fig. 2.2. avec p=2, n=5 ; Fig. 3.2 avec p=2 , n=4 ; Fig. 3.5 avec p=2 , n=4 ; Fig. 4.1 avec p=n=3 ; Fig. 5.1 avec p=5 , n=2 , etc...).

REMARQUE 4

Une fois que A est choisie, le changement de la position d'une racine de F , ou l'augmentation de la quantité de ses racines ne peut largement influer sur le graphe itératif de Newton simplifié. En effet, d'après (2), la modification de la valeur de $F(x^r)$ ne peut influer que sur x^{r+1} , (cf. de Fig. 2.1. à Fig. 2.2.).

REMARQUE 5

Le choix de A va beaucoup intervenir dans le comportement itératif. Après l'observation de deux graphes (cf. Fig. 3.1. et Fig. 3.2), on y trouve une grande différence (F(x) donnée par une même table), même pour une petite variation de A : là

$$A_1 \ \theta \ A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ pour } p=2 \ , \ n=4 \ ,$$

et qu'il y a quatre points qui ont changé leurs successeurs.

De plus, entre les deux autres graphes (cf. Fig. 3.4 et Fig. 3.5), six points (numéro 1, 2, 4, 6 12, 14) ont changés leurs successeurs pour

$$A_4 \,\theta\, A_5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{(pour } p=2 \text{ , } n=4\text{)}$$

et même table de F(x).
Malheureusement, on n'a pas encore trouvé dans notre contexte un bon moyen avec lequel un choix A pouvant favoriser la recherche de racine, pourrait être fourni .
Néanmoins, ce qui suit, sont des choix particuliers de A qui peuvent être des conditions nécessaires et suffisantes de certaines sortes de convergence locale.

ii) Convergence locale

PROPOSITION 3

Dans (2), pour que x^{r+1} soit une racine a de F(x) (si elle existe dans $(Z/p)^n$) pour $x^r \in V_d(a)$, ($V_g(a)$, resp.), il faut et il suffit qu'on mette $A = F'_d(a)$, ($F'_g(a)$ resp.) (non singulière).

DEMONSTRATION

Condition suffisante : selon I.2, remarque 3, on a
$F(x^r) = F'_d(a) \,\emptyset\, (x^r \theta a)$ et revient à (2)
$x^{r+1} = x^r \theta A^{-1} \emptyset F(x^r) = x^r \theta [F'_d(a)]^{-1} \emptyset F'_d(a) \emptyset (x^r \theta a) = x^r \theta x^r \theta a = a$

Condition nécessaire : $a = x^{r+1} = x^r \theta A^{-1} \emptyset F(x^r) = x^r \theta a = A^{-1} \emptyset F(x^r)$
On pose qu'ici $x^r \theta a = e_j$, (j=1,2,...,n) , alors on a :
$e_j = A^{-1} \emptyset F'_d(a) \emptyset e_j$. Cela illustre que $\Delta j = ej$, où Δj est le jème vecteur colonne de la matrice $A^{-1} \emptyset F'_d(a)$, c'est à-dire
$A^{-1} \emptyset F'_d(a) = I$, $A = F'_d(a)$.

COROLLAIRE

Dans (2) pour que x^{r+1} soit une racine a de F (si elle existe dans $(Z/p)^n$) pour $\forall\, x^r \quad V(a) = V_d(a) \quad V_g(a)$, il faut et il suffit que les deux conditions suivantes soient satisfaites :

1) $F'_d(a) = F'_g(a)$

2) on prend $A = F'_d(a) = F'_g(a)$.

Deux exemples se présentent dans la Fig. 4.3 avec p=n=3 , et la Fig. 5.3 (p=5,n=2).

REMARQUE 6

Dans $(Z/2)^n$, pour qu'une racine soit attactive dans son voisinage immédiat, une condition nécessaire et suffisante est la suivante :

1) La matrice $I \oplus [A^{-1} \otimes F'(a)]$ ait au plus un 1 par colonne

2) Cette matrice possède le rayon spectral booléen nul (c'est-à dire qu'il existe une matrice de permutation p telle que $p^t[I \oplus (A^{-1} \otimes F'(a))]P$ soit triangulaire inférieur stricte (cf. [1]).

On peut trouver une vérification dans la figure 3.1.

1.4.2. NEWTON STANDARD

i) Configuration de graphe itératif

Rappelons la méthode (3) $\begin{cases} F'(x^r) \otimes z = F(x^r) \\ x^{r+1} = x^r \ominus z \end{cases}$

PROPOSITION 4

Dans le graphe de Newton standard, le successeur d'un point quelconque dans $(Z/p)^n$ soit n'existe pas (système linéaire impossible), soit existe, dans ce dernier cas le nombre de successeurs peut être p^ℓ (ℓ entier, $0 \leq \ell \leq n$). L'itération d'un point initial quelconque de $(Z/p)^n$ va s'arrêter soit en cas de la présence d'un cycle soit en cas d'impossibilité.

DEMONSTRATION

En effet, le successeur d'un point est tout à fait dépendant de l'état des solutions de (3). D'après I.3 proposition 1, si la solution de (3) existe, son nombre sera p^{ℓ} (p premier, ℓ entier $0 \leq \ell \leq n$). Si (3) est un système incompatible, sa solution n'existe pas, alors le successeur n'existe non plus. On dit qu'on est tombé dans un puits.

REMARQUE 7

Expérimentalement, la longueur maximum ℓ , du transitoire (vers un cycle, point fixe ou vers un puits) est effectivement assez petite par rapport à celle de la méthode de Newton simplifiée. Parmi nombreux exemples, semble-t-il, qu'elle ne dépasse pas n, quelque soit n et p.

Dans la figure 1.2, $\ell = 4 < 5 = n$; dans la figure 2.3 , $\ell = 3 < 5 =$ dans la figure 4.2, $\ell = 3 = n$, dans la figure 5.2 , $\ell = 2 = n$

J'ai trouvé un exemple exceptionnel, (très rarement), dans la figure 4.4 : numéro 23 1 21 6 3 , $\ell = 4 > 3 = n$,
(mais 3 est un puits).

REMARQUE 8

Expérimentalement, le nombre de cycles obtenu dans Newton standard est toujours assez petit et ces cycles sont eux mêmes très courts (voir plus loin). Cette caractéristique est presque la même que pour la méthode de Newton simplifiée. Il semble que ce nombre ne croîsse pas lorsque n croît , et qu'il croîsse un peu lorsque p croît. Il faut dire que dans pas mal d'exemples, il n'existe pas de cycle (mis a part les points fixes) (cf. fig. 2-3, fig. 4-2) dans un graphe partiel avec n = 20 (cf. fig. 13-2).

REMARQUE 9

Puisque pour un point il existe éventuellement plusieurs successeurs on devrait classer des cycles en deux sortes : ceux qui n'ont aucune sortie de boucle, noté cycle C, ceux qui ont au moins une sortie de boucle, noté cycle $\bar{C}$.

Expérimentalement, la longueur des cycles C ne dépasse p (cf. fig. 5.2) ; et la longueur des cycles $\bar{C}$ ne dépasse p dans la plupart des exemples, (cf. Fig. 1-2, figu. 10-2, fig. 12-1,...), mais il existe parfois des contres exemples (cf. Fig. 6-2, longueur 5 contre p=3).

REMARQUE 10

Si l'on modifie la position d'une racine de F, cela ne changera que les successeurs du voisinage correspondant de cette racine. Eventuellement cela va accroître le nombre de points conduisant vers la racine beaucoup plus que la méthode de Newton simplifiée, surtout en cas de plusieurs racines (cf. Fig. 1-2, et Fig. 1.3, Fig. 4-4 et Fig. 4-2).

ii) Convergence locale

PROPOSITION 5

Dans (3), soit a une racine de F : $(Z/p)^n \longrightarrow (Z/p)^n$. Pour que $r^{x+1} = a$, $\forall\, x^r \in V_g(a)(V_d(a)$, resp.) il faut et il suffit qu'on choisisse $F'_d(x^r)$ ($F'_g(x^r)$, resp.) pour la dérivée $F'(x^r)$.

DEMONSTRATION

Condition suffisante : selon I.2 remarque 3, on a $F(x^r) \oplus e_j) \ominus F(x^r) = F'_d(x^r) \otimes e_j$ et puis : $F(x^r) = F(x^r \oplus e_j) \ominus F'_d(x^r) \otimes e_j$

on revient à (3) : $F'_d(x^r) \otimes z = F(x^r \oplus e_j) \ominus F'_d(x^r) \otimes e_j$

car $x^r \in V_g(a)$, sans perdre la généralité , on pose $x^r = a \oplus e_j$.

c'est-à-dire $F(x^r \oplus e_j) = F(a) = 0$, alors il reste le système suivant $F'_d(x^r) \otimes z = -F'_d(x^r) \otimes e_j$.

c'est-à-dire $z = -e_j$, étant une solution de (3)' on l'amène à (3)"

$$x^{r+1} = x^r \ominus (-e_j) = x^r \oplus e_j = a \ .$$

Condition nécessaire : posons $x^{r+1} = a$, $x^r = a \theta e_j$

On revient à (1): $A_r \otimes z = F(x^r) = F(x^r \theta e_j) \theta F'_d(x^r) \otimes e_j = -F'_d(x^r) \otimes e_j$

à d'autre aspect : $x^{r+1} = x^r \theta z \Rightarrow z = x^r \theta x^{r+1} = a \theta e_j \theta a = -e_j$

on revient au précédent : $A_r \otimes (-e_j) = -F'_d(x^r) \otimes e_j$

$$\left[A_r \theta F'_d(x^r) \right] \otimes e_j = 0$$

cela illustre que la jème colonne de la matrice $A_r \theta F'_d(x^r)$ soit nulle, alors pour tout j=1,...,n ce qui signifie $A_r \theta F'_d(x^r) = 0 \Rightarrow A_r = F'_d(x^r)$.

PROPOSITION 6

Dans (1), soit $A_r \neq 0$, matrice nulle, $p > 2$, alors qu'il n'existe pas d'autre choix de A_r pour que x^{r+1} soit la racine a de F(x) : $(Z/p)^n \longrightarrow (Z/p)^n$, pour $\forall\, x^r \in V(a) = V_g(a) \cup V_d(a)$.

En effet, s'il existe certaine $A_1 \neq 0$ dont les éléments appartiennent à Z/p , pour que la conclusion soit vraie. D'après les deux propositions précédentes et (1') , $z_1 = e_j$, $z_2 = -e_j$ sont les solutions de (1)". Ainsi, on obtient deux égalité suivantes $Z_r \otimes e_j = F(x^r)$, $-A_r \otimes e_j = F(x^r)$, on en réduit une seule $A_r \otimes e_j = -A_r \otimes e_j$.

En cas de $p > 2$, cette égalité n'est vraie que la jième colonne de A_r est nulle, pour $\forall$ j=1,...,n , c'est que $A_r = 0$, cela est contradictoire de la supposition.

Sur l'attraction d'une racine de F(x) dans $(Z/p)^n$, on peut trouver la référence dans [3].

Dans les exemples que j'ai fais en méthode de Newton standard, le voisinage à gauche d'une racine, converge vers cette racine dans un seul coup, car j'ai utilisé la dérivée à droite, (cf. fig. 4-2, fig. 4-3, fig. 5-2,...).

Bien que la convergence locale soit partiellement garantie en cette méthode, le problème de singularité existe encore, surtout pour p = 2. Il est donc naturel de s'engager à l'étude de singularité.

iii) Cas de sigularité.

Sur un point x^r de $(Z/p)^n$, le système (3) , avec la dérivée à droite peut s'écrire de la façon suivante :

$$\begin{cases} (\Delta_j) \oslash z = F(x^r) \\ x^{r+1} = x^r \theta z \end{cases}$$

d'où $\Delta_j = F(x^r \theta e_j) \theta F(x^r)$, $(j=1,2,\ldots,n)$,

jème vecteur colonne de $F'_d(x^r)$

* Soit $F'_d(x^r)$ singulière , $\Delta_{i_1},\ldots,\Delta_{i_\ell}$ étant les vecteurs indépendants $(0 \leq \ell \leq n-1)$, $\{i_1,\ldots,i_\ell\} \subset \{1,2,\ldots,n\}$, dans ce cas on a :

PROPOSITION 7

Pour que le système (3) soit soluble, il faut et il suffit que $F(x^r)$ soit une combinaison linéaire de $\Delta_{i_1},\ldots,\Delta_{i_\ell}$, où vecteur nul, c'est-à-dire que :

$$(e) \quad \begin{cases} F(x^r) = \sum_{k=1}^{\ell} \alpha_k \oslash \Delta_{i_k} \text{ , si } \ell \neq 0 \text{ } (\ell \text{ entier positif}) \\ F(x^r) = 0 \text{ (vecteur nul) si } \ell = 0 \end{cases}$$

d'où α_k entier : $0 \leq \alpha_k \leq p-1$, $(1 \leq k < \ell)$

La démonstration est presque la même que celle dans IR^n .

COROLLAIRE

Soit p=2 , pour que le système (3) ($F'_d(x^r)$ singulière) soit soluble il faut et il suffit que $F(x^r)$, satisfasse l'une de trois conditions suivantes :

a) existe ℓ' voisins de x^r , tels que $\sum_{k=1}^{\ell'} F(x^r \theta e_{j_k}) = 0$

(vecteur nul) d'où ℓ' impair , $1 \leq \ell' \leq n-1$.

b) existe ℓ' voisins de x^r, tels que $\sum_{k=1}^{\ell'} F(x^r \theta e_{j_k}) = F(x^r)$

d'où ℓ' pair,

$2 \leq \ell' \leq n-1$, $n \geq 3$,

c) $F(x^r) = 0$ (vecteur nul)

ici, $\{j_1, \ldots, j_{\ell'}\} \subset \{i_1, \ldots, i_\ell\}$. $\Delta i_1 \ldots \Delta i_\ell$, vecteurs indépendants. En effet, dans la proposition 7 , puisque α_k soit 0 , soit 1,(e) devient :

$$F(x^r) = \sum_{k=1}^{\ell} \alpha_k \theta \Delta_{i_k} = \sum_{k=1}^{\ell'} [F(x^r \theta e_{j_k}) \theta F(x^r)]$$

car p=2 , $F(x^r) \theta F(x^r) = 0$, alors on a :

$$\sum_{k=1}^{\ell'} F(x^r + e_{j_k}) = 0 \quad \text{si} \quad \ell' \text{ impair}$$

$$\sum_{k=1}^{\ell'} F(x^r \theta e_{j_k}) = F(x^r) \quad \text{si} \quad \ell' \text{ pair.}$$

* Soit $F(x^r)$ donnée tout à fait arbitrairement ainsi que pour $F'_d(x^r)$. Supposons qu'il y ait R_k formations pour $F'_d(x^r)$ singulière dont le rang appartient à l'ensemble $\{0,1,\ldots,n-1\}$, alors que $R_k.p^k$ formations correspondantes du système (3) seraient solubles.

En tout cas, il y a S1 formations solubles pour le système (3) avec $F'_d(x^r)$ singulière , d'où $S1 = \sum_{k=0}^{n-1} R_k.p^k$

A l'autre aspect, il y a S formations possibles pour former le système (3) avec $F'_d(x^r)$ singulière , d'où
$S = [p^{n^2} - (p^n-1)(p^n-p)\ldots(p^n-p^{n-1})].p^n$, selon l'annexe 2 de [1].
Alors, on obtient la

PROPOSITION 8

La proportion des formations solubles du système (3) sur un point x^r de $(Z/p)^n$ avec $F'_d(x^r)$ singulière, notée λ_n^p peut s'écrire de la façon suivante :

$$\lambda_n^p = \frac{S1}{S} = \frac{\sum_{k=0}^{n-1} R_k \cdot p^k}{[p^{n^2} - (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})] \cdot p^n}$$

* Dans l'annexe 2 de mon texte, une recherhce de R_k et un tableau de λ_n^p seront présentés.

Soit $F(x^r)$ donnée arbitrairement sauf vecteur nul, dans ce cas, on a :

COROLLAIRE

La proportion des formations solubles du système (3), sur un point x^r , de $(Z/p)^n$, avec $F(x^r)$ non nul et $F'_d(x^r)$ singulière, notée $\bar{\lambda}_n^p$, peut s'écrire de la façon suivante :

$$\bar{\lambda}_n^p = \frac{\bar{S}1}{\bar{S}} = \frac{\sum_{K=0}^{n-1} R_K \cdot (p^K - 1)}{[p^{n^2} - (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})] \cdot (p^n-1)}$$

* Supposons que dans $(Z/p)^n$. $F(x)$ possède ℓ racines, $a_i (F(a_i)=0)$ $(i=1,\ldots,\ell)$. Sur lesquelles la proportion du sytème soluble est égale à 1 respectivement, et sur les autres $(p^n -)$ points de $(Z/p)^n$, cette proposition est egale à $\bar{\lambda}_n^p$ respectivement.

Au point de vue globale, on note représentant la proportion moyenne des systèmes (3), solubles sur tous les points de $(Z/p)^n$ alors on a :

PROPOSITION 9

$$\lambda = \begin{cases} \bar{\lambda}_n^p & \ell = 0 \text{ (pas de racine)} \\ \bar{\lambda}_n^p + \dfrac{\ell \cdot (1-\bar{\lambda}_n^p)}{p^n} & 0 < \ell \leq p^n \end{cases}$$

En effet,

$$\lambda = \frac{\sum_{K=1}^{\ell} 1 + \sum_{K=1}^{p^n-\ell} \bar{\lambda}_n^p}{p^n} = \frac{\ell + (p^n-\ell)\bar{\lambda}_n^p}{p^n} = \bar{\lambda}_n^p - \frac{\ell(1-\bar{\lambda}_n^p)}{p^n}$$

Evidemment, si $\ell = 0$, $\lambda = \bar{\lambda}_n^p$.

REMARQUE 11

Cette formule nous montre que l'augmentation de la quantité de racines peut accroître sensiblement la proportion du système (3) soluble. Mais cette influence sera diminuée si p ou n croît.

iv) Une tendance d'accroîssement de $F'_d(x)$ régulière avec p
D'après les figures que j'ai faites, en méhtode de Newton standard, avec F(x) donnée au hasard, on peut en tirer un tableau suivant :

figure	p	n	taux de $F'_d(x)$ regulière	
			expérimental	théorique(cf Annexe2 de 1
1_2	2	5	0.218	0.298
1_3	2	5	0.281	0.298
2_3	2	5	0.344	0.298
4_2	3	3	0.592	0.570
4_4	3	3	0.592	0.570
5_2	5	2	0.760	0.768
5_4	5	2	0.800	0.768

* entre les taux expérimental et théorique, l'écart n'est pas grand.

* La tendance d'accroîssement de ce taux avec p est assez évidente.

I.5. LE COMPORTEMENT ITERATIF DE NEWTON POUR F(x) DONNE PAR DES EXPRESSIONS POLYNOMILAES.

I.5.1. F(x) LINEAIRE

i) Newton simplifié

Soit $F(x) = B \otimes x \oplus C$, $F(x) : (Z/p)^n \longrightarrow (Z/p)^n$;
soit matrice B constante et inversible à éléments de Z/p ,
C vecteur constant.
Alors, F admet $a = -B^{-1} \otimes C$ pour unique racine.
Si l'on prend A=B , pour $\forall\ x^\circ \in (Z/p)^n$, on aura $x^1 = a$.

En effet $x = x^{\circ}\theta A^{-1}\otimes F(x^{\circ}) = x^{\circ}\theta[B^{-1}\otimes B\otimes x^{\circ}\theta B^{-1}\otimes C] = -B^{-1}\otimes C = a$

ii) Newton standard

Pour $\forall\, x^r \in (Z/p)^n$, selon la dérivation de fonction de I.2.3, on a $F'_d(x^r)$ (ou $F'_g(x^r)$) B . Dans ce cas le système (3) devient

$B\otimes z = F(x^r)$, $B\otimes z = B\otimes x^r\theta C$ (soit B inversible)

$\Rightarrow z = x^r\theta B^{-1}\otimes C \Rightarrow x^{r+1} = x^r\theta x^r\theta B^{-1}\otimes c = -B^{-1}\otimes c = a$.

I.5.2. F(x) PRESQUE LINEAIRE

Soit $F(x) = B\otimes x\theta C\theta U(x)$, d'où $U(x)$, l'expression vectorielle non linéaire. Au cas où il existe beaucoup de points de $(Z/p)^n$ tels que $U(x) = 0$. On obtient toujours de bons résultats sur la convergence, en utilisant les méthodes de Newton.

Tels exemples se trouvent dans la figure 7.1 et 7.2.

I.5.3. F(x) quadratique homogène.

Pour simplifier les écritures, dans ce qui suit, on remplace $\otimes$, θ , θ par celles habituelles.

* Soit $F(x) = (f_1,\ldots,f_n)^t$, $f_i(x) = x_i(x_1+\ldots+x_i+\ldots+x_n)$ $(Z/p)^n \longrightarrow Z/p$, alors ; on a les propriétés suivantes :

(i) F(x) possède p^{n-1} racines (qui constituent un ensemble noté R)

(ii) $m = p^{n-1}$, m , le nombre des voisins différents à gauche de toutes les racines, (qui constituent un ensemble, noté S)

(iii) Un point $\bar{a}$ quelconque dans S possède p^{n-1} successeur qui ne sont pas d'autres que tous les points de R.

En utilisant Newton standard et $F'_d(x)$, selon la dérivation de I.2.3 on a

$$F'_d(x) = \begin{pmatrix} (x_1+\cdots+x_n)+x_1+1 & x_1 & \cdots & x_1 \\ x_2 & (x_1+\cdots+x_n)+x_2+1 & \cdots & x_2 \\ \cdots & \cdots & \cdots & \cdots \\ x_n & x_n & \cdots & (x_1+\cdots+x_n)+x_n+1 \end{pmatrix}$$

On peut trouver les illustrations de ces propriétés dans Fig. 8.1 8.2, 8.3, 8.4 avec p et n différents.

Soit F(x) donné en forme suivante : $(Z/3)^3 \longrightarrow (Z/3)^3$

$$F(x) = \begin{cases} f_1 = (x_{11} + x_{12})^2 \\ f_2 = (x_{21} + x_{22})^2 \\ f_3 = (x_{31} + x_{32})^2 \end{cases} \quad \text{ou} \quad F(x) = \begin{cases} f_1 = x_{11}^2 + x_{12}^2 \\ f_2 = x_{21}^2 + x_{22}^2 \\ f_3 = x_{31}^2 + x_{32}^2 \end{cases}$$

d'où $x_{i1} \neq x_{i2}$, $x_{ij} \in \{x_1, x_2, x_3\}$, (i=1,2,3 , j=1,2)

Alors, en utilisant Newton standard et $F'_d(x)$, on a les propriétés suivantes :

(i) F(x) possède une et seulement une racine a = (0,0,0)

(ii) F(x) possède (sauf a) un autre point fixe b = (1,1,1) (ou b = (2,2,2) resp.)

(iii) Dans le graphe itéraitf, il n'y a que le voisinage à gauche de a et celui à droite de b (lui même compris) convergent en un seul coup vers la racine a et les autres points de (Z/3) sont isolés. (cf. Fig. h et Fig. k).

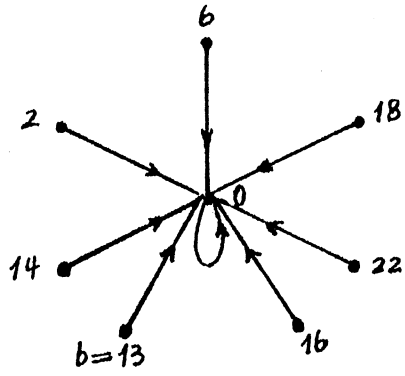


fig – h

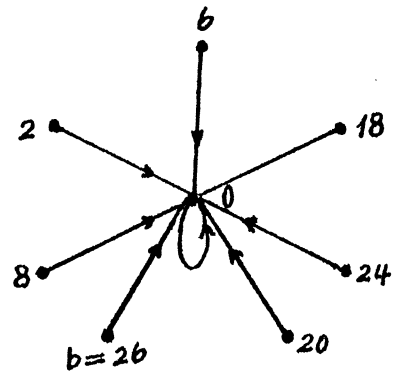


fig – K

* Soit F(x) donné en forme suivante : $(Z/3)^n \longrightarrow (Z/3)^n$

$$F(x) = \begin{cases} f_1 = x_{11}^2 + x_{12}x_{13} \\ f_2 = x_{21}^2 + x_{22}x_{23} \\ f_3 = x_{31}^2 + x_{32}x_{33} \end{cases}$$

d'où $x_{11} \neq x_{i2} \neq x_{i3}$

$x_{i1} \neq x_{i3}$

$x_{ij} \in \{x_1, x_2, x_3\}$ $\begin{pmatrix} i=1,2,3 \\ j=1,2,3 \end{pmatrix}$

Soit le point $y = (y_1, y_2, y_3)$ de $(Z/3)^3$ étant l'un des successeurs d'un point $x\ (x_1, x_2, x_3) \in (Z/3)^3$, en utilisatn la méthode de Newton standard et

$$F_d'(x) = \begin{pmatrix} 2x_1+1 & x_3 & x_2 \\ x_3 & 2x_2+1 & x_1 \\ x_2 & x_1 & 2x_3+1 \end{pmatrix}$$

Soit $\bar{y}$ obtenu en échangeant les positions de deux composantes de y (par exemple, on échange y_1 et y_2 alors $\bar{y} = (y_2, y_1, y_3)$).

Alors, $\bar{y}$ est sûrement l'un des successeurs d'un point $\bar{x}$ obtenu de la même façon qu'on a obtenu $\bar{y}$ de y .
(Par l'exemple ci-dessus, $\bar{x} = (x_2, x_1, x_3)$).

On peut vérifier cette propriété dans la fig. 6.1 sur laquelle certain genre de similitude s'exprime.

I.5.4. F(x) quadratique général.

Etant donnée une fonction quadratique dans $(Z/p)^n$ qui n'a pas de chose particulière, alors, sur laquelle, le graphe itératif de la méthode de Newton Standard se paraît plus général. Deux exemples se présentent dans les figures 9.1 et 9.2.

I.5.5. F(x) ayant des composantes identiques.

Soit $F(x) = (f_1, \ldots, f_j, \ldots, f_n)^t$, $f_i(x)$: $(Z/p)^n \longrightarrow Z/p$, $(i=1,2,..,n$
dont $f_k(x) \equiv f_j(x)$, $(\forall\ x \in (Z/p)^n$, $1 \leq k$, $j \leq n)$.

Dans ce cas, la matrice $F_d'(x)$ (ou $F_g'(x)$) est sûrement singulière. Néanmoins les systèmes (3) sur la plupart des points restent encore solubles.
Bien que chaque point ait plusieurs flèches et la configuration de l'itération soit un peu désordonnée, la situation de la convergence se paraît éventuellement bonne. La figure 10.2 nous donne un exemple :

$$F(x) = \begin{cases} f_1 = x_1^2 + x_2x_3 + x_3 \\ f_2 = x_2x_3 + p - 1 \\ f_3 = f_1 \end{cases} \qquad F_d'(x) = \begin{pmatrix} 2x_1+1 & x_3 & 1+x_2 \\ 0 & x_2 & 1+x_2 \\ 2x_1+1 & x_3 & 1+x_2 \end{pmatrix}$$

$(p=n=3)$

Dans le graphe, on s'apperçoit que

(i) seulement deux points isolés et trois puits (15, 24, 6, 11, 13

(ii) puisque le rang m de $F_d'(x)$ est toujours égale à 2, chaque point à ℓ flèches sorties ($\ell = p^{n-m} = 3^1 = 3$) sauf les points isolé et puits.

(iii) deux racines et deux cycles de longueur 2, non bloqués.

(iv) tous les points sauf ceux isolés et puits, conduisent au moins à une racine, et le pas transitoire ne dépasse pas la dimension n.

I.5.6. Symétries sur certaines sortes de fonctions.

(1) F(x) indépendant de certaines variables.

Soit $F(x) = (f_1,\ldots,f_n)^t$, $f_i(x_{j_1},x_{j_2},\ldots,x_{j_k}) : (Z/p)^n \longrightarrow Z/p$, i=1,2,

d'où $1 \leq j_\ell \leq n$, $(\ell = 1,\ldots,k)$, $k < n$, dans ce cas, la matrice $F_d'(x)$ (ou $F_g'(x)$) est aussi singulière, sur quelque soit $x \in (Z/p)^n$.

Cette fois-ci expérimentalement les systèmes (3) sur la plupart des points ne restent éventuellement plus solubles, et la fréquence des présences des points isolés (puits) croître énormément. Mais tous les points de $(Z/p)^n$ se paraissent dans le graphe itératif de Newton standard, tout à fait symétriquement (on l'appelle p-symétrie).

La figure 10.1 nous donne un exemple : $(p=n=3)$

$$F(x) = \begin{cases} f_1 = x_2^2 + x_2 + x_3 \\ f_2 = x_2x_3 + p - 1 \\ f_3 = x_2 + x_3^2 + p - 2 \end{cases} \qquad F_d'(x) = \begin{pmatrix} 0 & 2x_2+2 & 1 \\ 0 & x_3 & x_2 \\ 0 & 1 & 2x_3+1 \end{pmatrix}$$

Il est évident qu'il manque la variable x_1 dans les expressions de $f_i(x)$, (i=1,2,3). Dans le graphe, on peut constater la 3-symétrie Un autre exemple caractérisé de I.5.5. et de I.5.6.(1) se trouve dans la fig. 11.1.

(2) F(x) ne contenant des termes croisées de certaine variable (P=2)

Soit $\bar{N} = \{j_1,\ldots,j_k\}$, $N = \{1,2,\ldots,n\}$, $1 \leq j_1,\ldots,j_k \leq n$,

on pose $\bar{\bar{N}} = N - \bar{N}$

Soit $F(x) = (f_1,\ldots,f_{j_1},\ldots,f_{j_k},\ldots,f_n)^t$, $f_i(x) : (Z/2)^n \longrightarrow Z/2$ $(i=1,2,\ldots,n.)$

d'où $f_{\ell'}(x_1,\ldots,x_n) = f_{\ell'}(x_2,\ldots,x_n)$, $\ell' \in \bar{\bar{N}}$

$f_\ell(x_1,\ldots,x_n) = x_1 + \bar{f}_\ell(x_2,\ldots,x_n)$, $\ell \in N$.

Bien entendu x_1 peut être remplacée par d'autre variable.

Voici un exemple, n = 4 ; $\bar{N} = \{3\}$

$$F(x) = \begin{cases} f_1 = x_2 + 1 \\ f_2 = x_2x_3 + x_3x_4 + x_3 + 1 \\ f_3 = x_1 + x_2x_4 + x_3 \\ f_4 = x_2 + 1 \end{cases} \qquad F'(x) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & x_3 & x_2+x_4+1 & x_3 \\ 0 & x_4 & 1 & x_2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

REMARQUE

En cas général, la matrice F'(x) est indépendante de la variable x_1, alors il est évident que $F'(x_1+1,x_2,\ldots,x_n) = F'(x_1,x_2,\ldots,x_n)$ et que la première colonne de $F'(x) = (0,\ldots,\underset{j_1}{1},\ldots,\underset{j_k}{1},\ldots 0)^t$.

D'ailleurs, on a une

PROPOSITION

Soit un point $x = (x_1,\ldots,x_n)$ de $(Z/2)^n$, $\bar{x} = (x_1+1,x_2,\ldots,x_n)$, son premier voisin,.

Soit le point $y = (y_1,\ldots,y_n)$ l'un des successeurs de x , en méthode de Newton standard. Alors y est aussi l'un des successeurs de $\bar{x}$.

DEMONSTRATION

Puisque y est successeur de x , z = x-y est une solution du système (3), sur le point x, c'est-à-dire que F'(x)(x-y) = F(x) . Et puis, on a une vérification suivante :

$$F'(\bar{x})(\bar{x}-y) = F'(x)\begin{pmatrix} x_1+1-y_1 \\ x_2-y_2 \\ \vdots \\ x_n-y_n \end{pmatrix} = F'(x)\begin{pmatrix} x_1-y_1+1 \\ x_2-y_2+0 \\ \vdots \\ x_n-y_n+0 \end{pmatrix} = F'(x)(x-y) +$$

$$+F'(x)\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = F(x) + (0,\cdots \underset{j_1}{1} \cdots, \underset{j_k}{1}, \cdots 0)$$

$$= F(\bar{x})$$

Cela illustre que $\bar{x}$-y est une solution du système sur le point $\bar{x}$, et signifie y est un successeur de x .
Le graphe de l'exemple précédent se trouve dans la figure 11.2.

COROLLAIRE

Si $\bar{N} \equiv N$, ce sera le cas linéaire, tous les voisins d'un point quelconque dans $(Z/2)^n$, ont des mêmes successeurs. En outre, si cet état est avec F'(x) (constante à ce moment) régulière, alors la conséquence est tout à fait la même que dans I.5.2 ii).

I.5.7. UNE SERIE DE $F_n(x)$ AYANT LA STRUCTURE ANALOGUE.

Soit une série $F_n(x)$ ayant la structure analogue, en cas de dimensions diverses, que nous donne-t-ils, les graphes itératifs dans les différents espaces de $(Z/p)^n$ en utilisant Newton standard ? Expérimentalement, je m' aperçois que l'analogie des structures de $F_n(x)$ (n différents) pourrait s'être trouvée entre les graphes qui correspondent à $F_n(x)$. Avec laquelle, on pourrait en tirer les propriétés communes des itérations.

Voilà trois exemples qui se présentent dans les fig. 12.1, – 12.3, (n=6,8,20 resp.).

I.5.8. F(x) : $(Z/p)^n \longrightarrow (Z/p)^n$, avec n ou p assez grand).

Lorsque n et p s'accroîssent les éléments de l'espace de $(Z/p)^n$ vont énormément accroître. Ce nombre est si grand qu'on ne peut obtenir le graphe itératif total, et qu'il nous empêche naturellement de chercher les racines de F(x).
Avec mon algorithme, on peut quand même effectuer l'itération et obtenir certains graphes partiels que l'on veut.
Une fois que les points initiaux sont bien choisis, les propriétés itératives pourraient quand même s'exprimer dans les graphes partiels, et les racines pourraient être trouvées. Surtout la réalisation de ce travail est utile pour savoir la configuration itérative dans les grands espaces.
Voilà deux exemples, qui se trouvent dans la Fig. 13.1 Fig. 13.2). Pour p=2 , n=20. Dans ce cas, le nombre des éléments de (Z/2) est égale à 1.048576.

CHAPITRE 2

MÉTHODE DE GAUSS-SEIDEL

Pour accélérer la convergence d'une itération d'approximations successives vers un point fixe dans le cadre continu, on utilise couramment la méthode de Gauss-Seidel (cf. [4]) qui a été transposée par F. Robert (cf. [1]) dans le cadre discrèt, précisément dans $X = \{0,1\}^n$, en utilisant un opérateur noté G , associé à une application $H(x)$, $(x \in X)$ de X dans lui-même :

Étant donnée une itération $x^{r+1} = H(x^r)$... (5) $r=0,1,2,...$ qui correspond au mode itération parallèle, on obtient la méthode de Gauss-Seidel sur H , qui correspond au mode purement série, et qui s'écrit ci-dessous :

$$(4) \quad \begin{cases} x_1^{r+1} = h_1(x_1^r, x_2^r, \cdots, x_n^r) \\ x_2^{r+1} = h_2(x_1^{r+1}, x_2^r, \cdots, x_n^r) \\ \quad \cdots \quad \cdots \\ x_n^{r+1} = h_n(x_1^{r+1}, \cdots, x_{n-1}^{r+1}, x_n^r) \end{cases}$$

Dans ce chapitre, on va essayer de la retransposer dans $(Z/2)^n$, ainsi que dans $(Z/p)^n$ (p, premier) afin qu'on puisse bien connaitre le comportement itératif de cette méthode dans notre contexte.

II.1. PREPARATION NECESSAIRE

On tient toujours à chercher les racines d'une application F de $(Z/p)^n$, qui sont les points fixes du mode parallèle :

$x^{r+1} = x^r \theta F(x^r)$ (5') (r=0,1,2,...)

d'où si on pose $H(x^r) = x^r \theta F(x^r)$ cela devient $x^{r+1} = H(x^r)$ (avec les opérations dans Z/p).

REMARQUE 1

Les points fixes du mode série (4) sont évidemment les mêmes que ceux de (5).

REMARQUE 2

Rappelons la méthode de Newton simplifiée :

$x^{r+1} = x^r \theta A^{-1} \theta F(x^r)$ (2)

dans laquelle, si l'on pose A=I , (2) sera devenu la forme (5') c'est-à-dire que le mode parallèle (5') est un cas particulier de la méthode de Newton simplifiée, sur lequel on va expérimenter la méthode de Gauss-Seidel.

Rappelons quelques notions standard dans le cadre d'itérations sur $X = \{0,1\}^n$, (cf. [1]).

1. Chaque matrice A (n,n) booléenne possède au moins une valeur propre (soit 0 , soit 1), dont la plus grande ($0 \prec 1$) est appelée son rayon spectral booléen $\rho(A)$ (cf. [1]).

2. $\rho(B(H)) = 0$ est une condition nécessaire et suffisante pour que l'opérateur H(x) soit contractant (où B(H) est la matrice d'incidence de l'opérateur H).

3. Cette condition est équivalente à $[B(H)]^p = 0$ (à droite, la matrice nulle ; à gauche : la puissance booléenne, avec p entier $\leq n$), et aussi à dire qu'il existe une matrice de permutation p , telle que $p^t[B(H)]P$ soit une matrice triangulaire inférieure stricte.

4. La contraction de l'opérateur H , ($\rho(B(H)) = 0$) est une condition suffisante, pour que premièrement il existe un seul point fixe $\xi \in X$ de H ; deuxièmement l'itération (5) stationne en ξ au bout de p pas au plus ($p \leq n$) , quelque soit le point de départ, ce qui revient à dire que le graphe d'itération de H est simple (un seul bassin, avec un point fixe).

5. Sous la condition de H(x) contractant dans $X = \{0,1\}^n$, l'opérateur série G, est aussi contractant et au moins autant que H(x). Donc le graphe de l'itération (4) est lui-aussi simple.

II.2. ELEMENTS PROPRES DANS $(Z/2)^n$

La seule différence entre l'addition 1+1=1 dans $\{0,1\}^n$, et l'addition 1⊕1=0 dans Z/2 entraine une grande différence quant à l'existence d'éléments propres de matrices à éléments dans $\{0,1\}$ ou dans Z/2 .
Avant d'effectuer l'itération dans $(Z/2)^n$, il est besoin de bien connaître les éléments propres dans Z/2, et leurs fonctions dans la convergence locale. Dans ce paragraphe on rappellera rapidement leurs définitions et quelques propriétés et conséquences principales.

Soit B(n,n) une matrice à éléments dans Z/2.

DEFINITION

Un vecteur u ($u \neq 0$) de $(Z/2)^n$ est dit vecteur propre de B, s'il existe $\lambda \in Z/2$ tel que :

$$B \otimes u = \lambda \otimes u \qquad \text{(opérations de } Z/2\text{)}$$

sera alors appelée valeur propre de B attachée au vecteur propre u .

DEFINITION

(B) désignera "la plus grande valeur propre" de B, si B en possède au moins une (0 ou 1), celle-ci sera appelé le rayon spectral de B.

PROPOSITION 1

Pour qu'une matrice B à éléments dans Z/2 admette 0 pour valeur propre, il faut et il suffit que B soit singulière.

PROPOSITION 2

Pour qu'une matrice B admette 1 pour valeur propre (i.e. $\bar{\rho}(B) = 1$) , il faut et il suffit que la matrice $B = I \oplus B$ soit singulière.

Bien entendu, B et $\bar{B}$ satisfont le système suivant

$$BX = \lambda X$$

$$BX = \bar{\lambda} X \qquad \text{où } \lambda \in Z/2 \text{ , } \bar{\lambda} = \lambda \oplus 1$$

COROLLAIRE 1

Pour qu'une matrice B admette uniquement 0 pour valeur propre (i.e. $\bar{\rho}(B) = 0$) il faut et il suffit que B soit singulière et $\bar{B}$ soit régulière.

COROLLAIRE 2

Pour qu'une matrice B n'ait aucune valeur propre, il faut et il suffit que B et $\bar{B}$ soient régulières.

Exemples

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ , alors } \bar{B} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ sont régulières .}$$

Ni B ni $\bar{B}$ n'admettent de valeurs propres.

- 39 -

Selon la définition, si B a une valeur propre soit 0, soit 1 alors B devrait satisfaire soit le système $B \boxtimes X = x$, soit le système $B \boxtimes X = 0$. Mais ni l'un ni l'autre ne peuvent être résolus dans $(Z/2)^n$.

REMARQUE

Si une matrice B(n,n) à éléments de Z/2 admet uniquement 0 pour valeur propre (i.e. $\bar{\rho}(B) = 0$), alors il existe un entier p tel que B^p (puissance dans Z/2) soit matrice nulle, soit B elle-même.

Exemples

i) $B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $B^2 = 0$; $B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ $B^4 = B$.

ii) $B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ $B^4 = 0$; $B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ $B^8 = B$.

Rappelons dans [1], la condition "il existe un entier $p \leq n$ tel que $B^p = 0$ (puissance booléenne)" est celle nécessaire et suffisante pour que $\rho(B) = 0$ (le rayon spectral booléen). La propriété correspondante dans $(Z/2)^n$ n'existe plus, en réalité on a la :

PROPOSITION 3

Soit B une matrice à éléments dans Z/2
s'il existe p un entier (≥ 1) tel que $B^p = 0$ (puissance dans Z/2) alors $\bar{\rho}(B) = 0$.

Pour certaines matrices, on a par exemple la :

PROPOSITION 4

Soit une matrice B(n,n) à éléments de Z/2 ayant au plus un seul 1 par colonne, si $\bar{\rho}(B) = 0$ (rayon spectral dans Z/2) alors, il existe un entier $p \leq n$ tel que la puissance dans Z/2 $B^p = 0$ (matrice nulle).

Bien qu'il y ait grande différence entre les éléments propres booléens et ceux dans Z/2, avec la proposition 3 et 4, on a quand même une condition nécessaire et suffisante qui correspond à celle dans [1].

PROPOSITION 5

Soit $\xi = H(\xi)$ un point fixe de H dans $(Z/2)^n$, pour que ξ soit attractif dans son voisinage immédiat, il faut et il suffit que

1) $H'(\xi)$ (dérivée dans $(Z/2)^n$) ait au plus un seul 1 par colonne
2) $\bar{\rho}(H'(\xi)) = 0$ (le rayon spectral dans Z/2).

Oui, car pour des matrices B à éléments dans $\{0,1\}$ ayant au plus un 1 par colonne, on a

$$\forall\ p \qquad \overset{\otimes}{B^p} = B^p$$

puissance dans Z/2 ; puissance booléenne

Donc

$$\bar{\rho}(B) = 0 \iff \rho(B) = 0 \quad .$$

dans Z/2 ; booléen

II.3. LE COMPORTEMENT ITERATIF DE GAUSS-SEIDEL POUR F(x) DONNEE ARBITRAIREMENT.

En effectuant la méthode de Gauss-Seidel sur des exemples pris au hasard, j'ai eu l'impression générale que les graphes de l'itération (4) (H(x) associé à F(x)) ressemblent à ceux de la méthode de Newton-simplifiée, mais en étant "plus contractants".

II.3.1. CONFIGURATION DU GRAPHE D'ITERATION

Rappelons la proposition 1 de I.4.1 ; parallèlement on a :

PROPOSITION 1

Dans le graphe de Gauss-Seidel, un point quelconque dans $(Z/p)^n$ a un et seulement un successeur qui va poursuivre jusqu'à ce qu'un point fixe ou un cycle se paraisse.

En effet, x^{r+1} est défini de manière unique à partir de x^r et on itère sur un ensemble fini.

REMARQUE 1

La longueur du transitoire est variable selon les cas. Quelque fois elle est supérieure à n (cf. fig. 16.4), quelque fois elle est inférieure à n (cf. Fig. 14.2, fig. 15.2). En tout cas, elle est sûrement inféiruere à celle du mode parallèle correspondant (comparaison fig. 14.1 et Fig. 14.2 ; Fig. 15.1 et Fig. 15.2 ; Fig. 15.3 et Fig. 15.4 ; Fig. 16.1 et Fig. 16.2 ; Fig. 16.3 et Fig. 16.4).

REMARQUE 2

Expérimentalement les longueurs des cycles en méthode de Gauss Seidel ne sont généralement pas grandes. La fréquence des cycles de longueur 2 parait plus souvent que les autres (cf. Fig. 15.2 , p=2 , n=5 ; Fig. 17.2 , p=2 , n=4 ; Fig. 17.3 , p=n=3 ; Fig. 18.1 , p=5 , n=2) .
Les cycles de grandes longueur sont rares, (cf. Fig. 14.2 , longueur 5 , avec p=2 , n=5). En cas particulier, cette longueur peut dépasser beaucoup plus que n (cf. Fig. 21.1, Fig. 21.4).
En tout cas, la longueur de cycle en méthode de Gauss-Seidel ne dépasse pas celle en mode parallèle correspondant associé à même table de F.

REMARQUE 3

Le nombre de cycles est effectivement faible (cf. Fig. 14 $\sim$ Fig. 17)

REMARQUE 4

Lorsqu'on change la table de la fonction F(x) à laquelle H(x) est associée, en imposant qu'un point choisi x devienne racine, cela change non seulement (pour Gauss-Seidel) le successeur de ce point (qui devient x lui-même), mais éventuellement cela peut

changer les successeurs de ses voisins immédiats (cf. Fig. 15.2 et Fig. 15.4 ; Fig; 16.2, Fig. 17.3, Fig. 17.4).

II.3.2. CONVERGENCE LOCALE.

PROPOSITION 2

Dans l'itération de Gauss-Seidel (4), pour que x^{r+1} soit une racine a de F, lorsque x^r étant le jième voisin à droite (ou à gauche) de a il faut et il suffit que la jième colonne de la matrice $F'_d(a)$ (ou $F'_g(a)$), notée Δ_j , vérifie la condition suivante :

$$\delta_1 = \cdots = \delta_{j-1} = 0 \ (\text{si } j>1) \text{ et } \delta_j = 1$$

où $\quad \Delta_j = (\delta_1, \cdots \delta_{j-1}, \delta_j, \cdots \delta_n)^t$

DEMONSTRATION

L'itération (4) peut s'écrire de la façon suivante :

$$(4)' \quad \begin{cases} x_1^{r+1} = x_1^r \ominus f_1(x_1^r, \cdots, x_n^r) \\ \cdots \\ x_{j-1}^{r+1} = x_{j-1}^r \ominus f_{j-1}(x_1^{r+1}, \cdots, x_{j-2}^{r+1}, x_{j-1}^r, \cdots x_n^r) \\ x_j^{r+1} = x_j^r \ominus f_j(x_1^{r+1}, \cdots, x_{j-1}^{r+1}, x_j^r, \cdots x_n^r) \\ x_{j+1}^{r+1} = x_{j+1}^r \ominus f_{j+1}(x_1^{r+1}, \cdots, x_j^{r+1}, x_{j+1}^r, \cdots x_n^r) \\ \cdots \\ x_n^{r+1} = x_n^r \ominus f_n(x_1^{r+1}, \cdots, x_{n-1}^{r+1}, x_n^r) \end{cases}$$

d'où $F(x) : (Z/p)^n \longrightarrow (Z/p)^n$, $F(x) = (f_1(x), \ldots, f_n(x))$

$f_i(x) : (Z/p)^n \longrightarrow Z/p$, $(i=1,2,\ldots,n)$.

Condition suffisante :

Selon I.2. remarque (3), on a $F(x^r) = F'_d(a) \otimes (x^r \ominus a)$

qui devient : $F(x^r) = F'_d(a) \otimes e_j = \Delta_j$, ou bien :

$$f_i(x^r) = \begin{cases} 0 & i \prec j \\ 1 & i=j \\ \delta_i & n \geq i > j \end{cases} \ldots (W) \text{ , d'ailleurs , on a } x_i^r = \begin{cases} a_i \ominus 1 \text{ si } i=j \\ a_i \text{ sinon} \end{cases} \quad (W')$$

Dans (4') selon (w) et (w') on a ($j > 1$)

$$x_1^{r+1} = x_1^r \theta f_1(x^r) = x_1^r \theta 0 = a_1 \quad ;$$

Pour $2 \leq i \leq j-1$,

$$x_i^{r+1} = x_i^r \ominus f_i(x_1^{r+1}, \cdots, x_{i-1}^{r+1}, x_i^r, \cdots, x_n^r) = x_i^r \ominus f_i(a_1, \cdots a_{i-1}, x_i^r, \cdots x_n^r)$$
$$= x_i^r \ominus f_i(x_1^r, \cdots, x_n^r) = x_i^r = a_i \quad ;$$

Ensuite ($j \geq 1$)

$$x_j^{r+1} = x_j^r \ominus f_j(x_1^{r+1}, \cdots x_{j-1}^{r+1}, x_j^r, \cdots, x_n^r) = x_j^r \ominus f_j(a_1, \cdots a_{j-1}, x_j^r, \cdots x_n^r)$$
$$= x_j^r \ominus f_j(x^r) = x_j^r \ominus 1 = a_j \quad ;$$

pour $n \geq i \geq j+1$,

$$x_i^{r+1} = x_i^r \ominus f_i(x_1^{r+1}, \cdots x_j^{r+1}, \cdots x_{i-1}^{r+1}, x_i^r, \cdots x_n^r)$$
$$= x_i^r \ominus f_i(a_1, \cdots a_j, \cdots a_n) = x_i^r \ominus f_i(a) = x_i^r = a_i \quad ;$$

Finalement, on en résulte que $x_i^{r+1} = a_i$, $(i=1,\ldots,n)$, soit $x^{r+1} = a$.

Condition nécessaire : Si l'on a (w)' et l'égalité suivante :

$$x_i^{r+1} = a_i \ , \ (i=1,\ldots,n)$$

On pourrait les ramener à (4)' :

$$f_1(x^r) = f_1(x_1^r, \cdots x_n^r) = x_1^r \ominus x_1^{r+1} = x_1^r \ominus a_1 = a_1 \ominus a_1 = 0 \quad (j>1)$$

Pour $2 \leq i \leq j-1$:

$$f_i(x^r) = f_i(a_1, \cdots a_{i-1}, x_i^r, \cdots x_n^r) = f_i(x_1^{r+1}, \cdots x_{i-1}^{r+1}, x_i^r, \cdots x_n^r)$$
$$= x_i^r \ominus x_i^{r+1} = x_i^r \ominus a_i = 0$$

Pour $i=j$ ($j \geq 1$) :

$$f_j(x^r) = f_j(a_1, \cdots a_{j-1}, x_j^r, \cdots x_n^r) = f_j(x_1^{r+1}, \cdots x_{j-1}^{r+1}, x_j^r, \cdots x_n^r)$$
$$= x_j^r \ominus x_j^{r+1} = x_j^r \ominus a_j = a_j \ominus 1 \ominus a_j = 1$$

Quant aux autres $f_i(x^r)$, $(n \geq i > j)$, ils peuvent être quelconque dans Z/p. Ainsi on a établi l'égalité (w) qui illustre que Δ_j , la jième colonne de $F_d'(x)$ (ou $F_g'(x)$), possdèe la propriété énoncée.

On peut trouver quelques vérifications dans Fig. 17.1 et Fig. 17.2. Il en résulte donc la :

PROPOSITION 3

Dans l'itération de Gauss-Seidel (4), pour que x^{r+1} soit une racine a de F, quelque soit x^r dans $V_d(a)$ (ou $V_g(a)$ resp.) il faut et il suffit que $F'_d(a)$ (ou $F'_g(a)$) soit une matrice triangulaire inférieure à une diagonale pleine de 1.
Quelques exemples se trouvent dans Fig. 16.4, Fig. 19.2, et Fig. 19.6.

REMARQUE 5

Rappelons qu'en utilisant le mode parallèle, selon I.4.1 ii), "$F'_d(a)$ (ou $F'_g(a)$) = I" est une condition nécessaire et suffisante pour que x^{r+1} soit une racine de F pour tout $x^r \in V_d(a)$ (ou $V_g(a)$).
Cette condition du point de vue de la convergence locale est beaucoup plus restrictive que celle de la proposition 3 ci-dessus en utilisant le mode-série (Gauss-Seidel) (cf. Fig. 16.3 et Fig. 16.4).

REMARQUE 6

Quant à l'attraction dans le voisinage immédiat d'une racine a de F dans $(Z/2)^n$, elle ne peut pas être garantie. La Fig. 14.3 et la Fig. 14.4 en donnent une illustration. Un exemple dans lequel une telle attraction a été vérifiée. Grâce à la structure de G'(x) se présente dans la Fig. 18.4 (comparer avec Fig. 18.3).

Dans l'itération de Gauss-Seidel 4 (ou (4)'), la détermination du successeur d'un point x^r quelconque appartenant à $(Z/p)^n$ dépend des valeurs respectives de F aux points suivants :

$$x^r = (x_1^r, \cdots x_n^r), \quad C^1 = (x_1^{r+1}, x_2^r, \cdots, x_n^r), \quad C^2 = (x_1^{r+1}, x_2^{r+1}, x_3^r, \cdots x_n^r),$$
$$\cdots \; C^{n-1} = (x_1^{r+1}, \cdots, x_{n-1}^{r+1}, x_n^r)$$

qui constituent un ensemble de points : $S = \{x^r, C, \ldots, C^{n-1}\}$ dans lequel les points ne sont pas forcément différents l'un à l'autre. Alors on a la :

PROPOSITION 4

Pour que x^{r+1} soit une racine a de F pour $x^r \in (Z/p)^n$, il suffit que cette racine a appartienne à S.

Il n'est pas difficile de la prouver, à l'aide de la démonstration de la condition suffisante de la proposition 2 dans ce paragraphe.

II.4. LE COMPORTEMENT ITERATIF DE GAUSS-SEIDEL POUR F(x) DONNE PAR DES EXPRESSIONS POLYNOMIALES.

Dans ce paragraphe, on va donner une impression générale, en examinant quelques exemples pour des applications F données par des expressions polynomiales.

II.4.1. LES COMPOSANTES DE F(x) AYANT LA FORME TRIANGULAIRE INFERIEURE PAR RAPPORT AUX VARIABLES.

Soit $F(x) = (f_1(x), \ldots, f_n(x)) \quad : \quad (Z/p)^n \longrightarrow (Z/P)^n$.

d'où $f_i(x) = f_i(x_1, x_2, \ldots, x_t) \quad : \quad (Z/p)^n \longrightarrow Z/P \quad , \quad (i=1,2,\ldots,n)$

$$\text{ou bien} \begin{cases} f_1(x) = f_1(x_1) \\ f_2(x) = f_2(x_1, x_2) \\ \cdots \\ f_n(x) = f_n(x_1, x_2, \ldots, x_{n-1}, x_n) \end{cases}$$

$$\text{par exemple} \begin{cases} f_1(x) = x_1 + 1 \\ f_2(x) = x_1 + x_1 x_2 \\ f_3(x) = x_1 x_3 + x_2 x_3 + X_3 + 2 \end{cases} \qquad (p=n=3)$$

Dans ce cas, expérimentalement l'itération de (4) (Gauss-Seidel) nous donne toujours de bons résultats au sens de convergence à la fois locale et globale.

Pour exprimer ce phénomène, il suffit de montrer que parmi des polynômes de ce genre, il est relativement facile d'en trouver certains qui satisfont les conditions suffisantes de la proposition 3 de II.3, surtout pour p assez petit.

Quelques exemples se présentent dans la Fig. 19, dans laquelle on peut aussi trouver les comparaisons avec le mode parallèle.

II.4.2. $\bar{F}(x)$ OBTENU PAR PERMUTATION DES COMPOSANTES DE $F(x)$

Notant $F(x) = (f_1(x),\ldots,f_i(x),\ldots,f_n(x)) : (Z/p)^n \longrightarrow (Z/p)^n$

$f_i(x) : (Z/p)^n \longrightarrow Z/p \quad , \quad (i=1,2,\ldots,n)$

Soit $\bar{F}(x) = (f_{i1}(x),\ldots,f_{ij}(x),\ldots,f_{in}(x)) : (Z/p)^n \longrightarrow (Z/p)^n$

$(i_1,\ldots,i_j,\ldots i_n)$ représente une permutation de $(1,2,\ldots,n)$

Résoudre $F(x) = 0$, c'est résoudre $F(x) = 0$, l'itération parallèle reste inchangée. Par contre on s'apercevrait qu'en méthode de Gauss-Seidel, les configurations d'itération obtenues pour F et pour $\bar{F}$ sont bien différentes.

Cela est en contraste frappant avec la méthode de Newton standard dans laquelle il 'ny a aucune différence entre les graphes obtenus pour F et pour $\bar{F}$ en considérant que le système $F'_d(x^r) \otimes z = F(x^r)$ et le système $\bar{F}'_d(x^r) \otimes z = \bar{F}(x^r)$ ont les mêmes solutions .

Cette remarque nous amène à rechercher un rangement relativement rationnel de composantes de $F(x)$, pour obtenir une meilleure $\bar{F}(x)$ sur laquelle on pourrait obtenir un meilleur graphe d'itération de Gauss-Seidel.

* Expérimentalement, si la matrice de $F'_d(a)$ (ou $F'_g(a)$) possède une diagonale pleine de 0 , cela entraine toujours de mauvais résultats, c'est-à-dire que la convergence vers cette racine a est toujours mauvaise. Dans ce cas, s'il n'y a pas d'autre racine,

de nombreux cycles ou des cycles de grande longueur paraissent éventuellement dans le graphe d'itération (cf. Fig. 20.4, Fig. 21.1).

Pour éviter le phénomène précédent, on pourrait faire certaines permutations de composantes de F(x), telles que la matrice de $F'_d(a)$ (ou $F'_g(a)$) soit une matrice dont les éléments distincts avec ceux correspondant de la matrice ayant la forme triangulaire inférieure et une diagonale pleine de 1, soient les moins nombreux possible.
On peut vérifier cette évolution de la Fig. 20.4 à la Fig. 20.1, de la Fig. 21.1 à la Fig. 21.3.

Bien entendu, réarranger les composantes de F(x), revient à choisir un mode série particulier sur F (cf. [1]).

II.4.3. $F(x) : (Z/p)^n \longrightarrow (Z/p)^n$ avec p assez grand.

Quelque exemples avec $p = 11$, $n = 3$, se présentent dans les fig. 23.1 ~ 23.3. On y voit les graphes partiels représentant des configurations globales d'itération.

CHAPITRE III

COMPARAISONS DE MÉTHODES

Dans les deux chapitres précédents, on a présenté trois méthodes d'itérations discrètes que l'on rappelle ci-dessous :

Newton simplifiée : (2) : $x^{r+1} = x^r \theta A^{-1} \otimes F(x^r)$

(A, matrice à éléments dans Z/p, non singulière)

dont le cas particulier (A=I) est appelé : le mode purement parallèle : (5) : $x^{r+1} = x^r \theta F(x^r)$

Newton standard :

$$(3) : \begin{cases} F(x^r) \otimes z = F(x^r) \\ x^{r+1} = x^r \theta z \end{cases}$$

Gauss-Seidel (mode purement série) :

$$(4) : \begin{cases} x_1^{r+1} = x_1^r \theta f_1(x_1^r, \ldots, x_n^r) \\ x_2^{r+1} = x_2^r \theta f_2(x_1^{r+1}, x_2^r, \ldots, x_n^r) \\ \ldots \\ x_n^{r+1} = x_n^r \theta f_n(x_1^{r+1}, \ldots, x_{n-1}^{r+1}, x_n^r) \end{cases}$$

(où $F(x) = (f_1(x), \ldots, f_n(x))$, $f_i(x) : (Z/p)^n \longrightarrow Z/p$, $(i=1,2,\ldots,n)$).

Dans ce chapitre on va faire des comparaisons sur la convergence, la configuration et le temps de calcul.

III.1. COMPARAISON DES CONFIGURATIONS.

* On voit bien que dans la méthode de Newton-simplifiée le successeur d'un point x^r quelconque dans $(Z/p)^n$ est uniquement dépendant de x^r et $F(x^r)$, lorsque la matrice A a été choisie.

Dans la méthode de Newton-standard, celui-ci est déterminé non seulement de x^r et $F(x^r)$, mais aussi des valeurs de F dans le voisinage (à droite ou à gauche) immédiat de x^r. En remplaçant ce voisinage par l'ensemble S associé à ce point (S défini dans la proposition de II.3), on pourrait dire la même chose pour la méthode de Gauss-Seidel.

* Il existe un et seulement un successeur de x^r dans Newton-simplifiée et dans Gauss-Seidel. Il en existe éventuellement plusieurs ou il peut n'en exister qucun (x^r est alors un puits) dans Newton-standard.

* Une fois la dimension n est fixée, le changement de p ne pourrait pas influer sur les caractéristiques de la configurations d'itération de Newton-simplifiéeou de Gauss-Seidel dans $(Z/p)^n$. Par contre, l'augmentation de p peut énormément faire décroitre la quantité de puits et les cas où il existe plusieurs successeurs pour un point : le taux de systèmes singuliers décroît fortement (cf. l'annexe 3).

Expérimentalement, dans le graphe d'itération de Gauss-Seidel ou de Newton-standard, il existe parfois certains points ayant plusieurs flèches entrant (cela signifie que ces points pourraient être appelés attractifs) dont le nombre, semble-il, est beaucoup plus grand que dans celui de Newton-simplifiée. Cela pourrait être une des explications pour le fait que les pas d'itération de Newton-simplifiée sont plus nombreux que ceux de Newton standard et de Gauss-Seidel.

Cette impression se reflète fortement quand F possède au moins une racine.

III.2. COMPARAISON DES CONVERGENCES

Soit F une application dans $(Z/p)^n$ dans lui-même, ayant au moins une racine : les itérations considérées ont au moins un point fixe ; on constate que le cadre de la convergence, surtout locale, parait différemment dans les graphes de ces trois méthodes.

Soit a une racine de F.

Inconditionnellement, les points du voisinage à gauche (ou à droite) correspondant à la dérivée à droite (ou à gauche) de a convergent sur a en un seul coup, si l'on effectue l'itération de Newton-standard.

Eventuellement, les points de l'ensemble S associé à a , ainsi que ceux de son voisinage convergent sur a en un seul coup, si l'on effectue l'itération de Gauss-Seidel ou de Newton-simplifiée.

Précisément, si F(x) possède un caractère tel que la jième colonne de la matrice de $F'_d(a)$ (ou $F'_g(a)$ resp.) ait la forme suivante : $(0\ldots0\ 1\ x\ x\ldots x)^T$ (x désigne n'importe quel élément de Z/p) , alors la ^{j}méthode^{n}Gauss-Seidel permet que le jième voisin à droite (ou à gauche) de a converge sur a en un seul coup ; si la jième colonne de $F'_d(a)$ (ou $F'_g(a)$) est identique à celle de A , alors méthode de Newton simplifiée permet que le jième voisin à droite (ou à gauche) converge sur a en un seul coup.

Evidemment, la restriction pour satisfaire la condition de convergence en méthode de Newton-simplifiée est plus forte que celle en méthode Gauss-Seidel.

* Quant à la convergence globale, sur le plan théorique elle ne peut pas être garantie par une condition suffisante dans mon texte. D'après ce que j'ai expérimenté, je pourrais présenter quelques intuitions suivantes :

a) L'accroîssement de quantité de racines de F dans $(Z/p)^n$, peut évidemment améliorer la situation de convergence globale, pour chacune de ces trois méthodes. Par ailleurs, ce qu'il faut souligner, est que cet effet est beaucoup plus évident sur la méthode de Newton-standard. De plus, dans ce cas, il

existe éventuellement quelques points pouvant conduire à plusieurs racines de F .

b) Le nombre de cycles peut beaucoup détériorer la convergence globale pour chacune de ces trois méthodes : c'est-à-dire que le mauvais état de la convergence globale parait souvent lorsqu'il y a relativement de nombreux cycles.

Expérimentalement, le nombre de cycles dans Newton-standard est moindre que dans Gauss-Seidel qui est lui-même moindre que dans Newton-simplifiée.

c) Bien entendu, le nombre de puits pour la méthode de Newton standard peut beaucoup intervenir sur la convergence globale.

d) Quand p et n sont assez petits, où les points ne sont pas nombreux, l'état de la convergence locale peut jouer un rôle remarquable dans la globale. Mais en cas de points nombreux de $(Z/p)^n$, cet effet va beaucoup diminuer.

Pour bien comparer, j'ai effectué beaucoup d'exemples qui permettent d'établir le tableau comparatif suivant.
(F_i signifie que F(x) possède i racines ;
F(x) obtenu au hasard).

	I : Méthode de Newton-standard II : Méthode de Gauss-Seidel III : Méthode de Newton-simplifiée	Exemples	nombre de points pouvant conduire à une racine			nombre de points ne conduisant sûrement pas à une racine			nombre de puits				nombre de cycles			longueur maximum des cycles			le pas maximum du transitoire aboutissant à un point fixe			le pas maximum du transitoire aboutissant à un cycle			le pas maximum aboutissant à un puits	nombre de points pouvant conduire à deux racines	temps de calcul x s. total		
			I	II	III	I	II	III	I	I	II	III	I	II	III	I	II	III	I	II	III	I	I	I	II	III
p=5 n=2 nombre de points dans $(Z/p)^n$ 25	F_1 (une racine)	1	6	1	1	19	24	24	5	1	2	1	2	4	9	3	0	0	7	7	5	0	/	0.337	0.281	0.375
		2	16	25	1	9	0	24	4	0	0	1	/	/	5	5	8	0	/	/	8	3	/	0.386	0.302	0.417
		3	7	25	3	18	0	22	3	1	0	1	5	/	9	4	8	1	5	/	5	3	/	0.340	0.279	0.377
		4	11	1	4	14	24	20	4	1	1	2	4	5	3	4	0	3	3	5	6	0	/	0.332	0.281	0.374
	F_2 (deux racines)	5	10	25	2	15	0	23	2	1	0	2	4	/	3	3	9	0	5	/	5	0	0	0.335	0.284	0.393
		6	23	25	5	2	0	20	2	0	0	2	/	/	5	7	7	2	/	/	3	0	0	0.368	0.311	0.382
		7	8	9	2	17	16	23	3	1	1	2	3	5	3	2	4	0	5	4	8	3	1	0.339	0.289	0.375
	F_3 (trois racines)	8	23	15	22	2	10	3	2	0	1	1	/	5	3	5	3	5	/	1	0	0	1	0.333	0.281	0.373
		9	19	25	4	6	0	21	3	0	0	3	/	/	5	4	4	1	/	/	4	2	1	0.331	0.281	0.373
		10	20	25	11	5	0	14	4	0	0	1	/	/	2	4	7	4	/	/	8	1	0	0.339	0.285	0.372
p=2 n=5 nombre de points dans $(Z/p)^n$ 32	F_1 (une racine)	11	10	32	13	22	0	9	14	1	0	2	2	/	2	3	5	8	0	/	8	4	/	0.692	0.401	0.539
		12	10	1	1	22	31	31	14	1	1	1	2	4	2	2	0	0	0	3	13	4	/	0.677	0.401	0.504
		13	7	2	29	25	30	3	16	1	1	1	2	2	2	2	1	11	0	4	1	4	/	0.635	0.386	0.503
		14	9	9	2	23	23	30	17	1	1	2	2	2	8	2	2	1	0	4	6	3	/	0.616	0.384	0.516
	F_2 (deux racines)	15	19	32	18	13	0	14	11	0	0	1	/	/	2	5	7	7	/	/	6	4	3	0.680	0.397	0.505
		16	14	8	10	18	24	22	13	0	1	1	/	3	2	3	2	4	/	4	11	2	4	0.683	0.391	0.506

III.3. INDICATIONS PRATIQUES.

Etant donnée une application F dans $(Z/p)^n$, nous allons donner quelques recommandations pour choisir l'une des trois méthodes étudiées dans le but de déterminer les racines de F.

Utiliser la méthode de Newton-standard pour F(x) linéaire ou fortement linéaire.

Dans le premier chapitre, on a prouvé à la fois théoriquement et expérimentalement que cette méthode entraine toujours de très bons résultats (cf. Fig. 7.2). Mais en utilisant la méthode de Gauss-Seidel, il n'est pas sûr qu'on puisse obtenir le résultat désiré (cf. Fig. 24.3).

Utiliser la méthode de Gauss-Seidel pour F(x) ayant la forme triangulaire inférieure par rapport aux variables.

D'après ce qu'on a raconté dans II.4.1, la méthode de Gauss-Seidel entraine toujours de bons résultats, car la forme de F(x) convient alors bien au caractère triangulaire de cette méthode (cf. Fig. 19.2). Mais sur le même F(x), l'effet des autres méthodes n'est pas aussi brillant que le précédent.

Eventuellement, le résultat de Newton standard reste encore bon, (cf. Fig. 24.1, Fig. 24.2).

Utiliser la méthode de Newton-standard, au cas où il existe des composantes de F(x) étant identiques.

Bien que le graphe d'itération soit un peu compliqué (plusieurs flèches sortant d'un point), car la Jacobienne a toujous au moins 2 lignes identiques, donc est singulière, le nombre de puits est relativement petit, d'ailleurs, il existe beaucoup de points pouvant conduire vers une ou plusieurs racines, autrement dit, si l'on démarre à partir d'un point initial quelconque, on pourrait prévoir la grande probabilité de trouver une ou même toutes les racines de F, en quelques coups d'itérations (cf. Fig. 10.2). Mais la méthode de Newton-simplifiée et de Gauss-Seidel restent toujours insensibles à ce caractère de F.

Utiliser la méthode de Newton-standard pour $F(x)$ ayant certains caractères symétriques.

Car, dans ce cas, en passant les résolutions du système (3), cette méthode peut reflèter ces caractères symétriques dans le graphe d'itération beaucoup mieux qu'en utilisant les deux autres méthodes, (cf. Fig. 11.1).

III.4. COMPARAISON DES TEMPS DE CALCUL

Dans la méthode de Newton-standard, en partant d'un point x^r dans $(Z/p)^n$, pour obtenir x^{r+1} , on doit résoudre un système linéaire. Généralement, cela va dépenser assez de temps de calcul. Dans la méthode de Newton simplifiée, il faudrait d'abord calculer l'inverse de la matrice A et puis au cours de l'itération, il s'agit toujours de multiplication de la matrice et le vecteur. Le temps de calcul ne peut pas être négligeable.

Dans la méthode de Gauss-Seidel, pour un point x^r de $(Z/p)^n$, il s'agit que de la modification de ses composantes avec laquelle on cherche le successeur de x^r .

Effectivement, toute fois que p et n sont choisis, pour obtenir le graphe d'itération global, la dépense de temps en méthode de Gauss-Seidel reste toujours la moindre par rapport à celles en méthode de Newton-simplifiée et de Newton-standard. Cet effet deviendrait plus frappant lorsque p^n croît. (Cf. le tableau de ce chapitre).

III.5. CONCLUSION

J'ai ainsi pu obtenir une connaissance empirique relativement globale sur chacune de ces trois méthodes itératives dans $(Z/p)^n$. Dans ce qui suit, je voudrais présenter quelques points de vue pour conclure ce travail.

a) Il vaut mieux abandonner la méthode de Newton simplifiée, car dans la pratique, on n'en voit pas les avantages, quelque soit le point de vue adopté .

b) En ce qui concerne la méthode de Newton-standard et celle de Gauss-Seidel : chacune a sa propre caractéristique au cours de l'itération. On ne peut pas distinguer simplement ce qui est relativement la meilleure des deux.

c) Expérimentalement, dans Newton-standard, il y a d'un tiers à la moitié des points de $(Z/p)^n$ pouvant conduire au moins vers une racine pour F(x) général. Dans Gauss-Seidel, on ne peut pas simplement donner une proportion de tels points, mais parmi de nombreux exemples pour F(x) toujours général, il y a à peu près la moitié des cas où les points conduisant vers une racine représentant une grande proportion des points de $(Z/p)^n$.

d) Expérimentalement, avant d'effectuer l'itération dans $(Z/p)^n$ sur une série de $F_n(x)$ avec n assez grand, il vaut mieux d'abord prendre des exemples avec n assez petit. Car en examinant les graphes de ces exemples (plus faciles, plus économes), on pourrait découvrir les caractéristiques essentielles du graphe d'itération sur cette série de $F_n(x)$.

e) Je n'arrive pas à trouver un moyen de savoir si toutes les racines de F(x) pourraient être trouvées en effectuant certaine itération partielle lors de p^n assez grand.

f) Je n'arrive pas à trouver un moyen de pouvoir sûrement améliorer une mauvaise concergence de l'itération.

g) Je ne sais pas s'il y a de la valeur pour chercher la racine de $F(x)$ dans $(Z/p)^n$, lorsqu'on utilise une méthode itérative combinant les caractéristiques à la fois de Newton-Standard et de Gauss-Seidel : on obtiendrait alors l'analogue des méthodes du type Quasi-Newton étudiées dans $\mathbb{R}^n$ (cf. [5] et [7]).

A la fin, je voudrais souligner que ce travail est fait par un Oriental en Occident, cela nous fait rappeler un proverbe chinois qui disait

" C'est le même soleil qui se lève à l'Orient
et se couche à l'Occident ".

ANNEXE 1 : ALGORITHMES ET PROGRAMMES

Algorithme.

1. Un programme principal pour réaliser l'itération sur $(Z/p)^n$ en méthode de Newton-standard, nommé itezp, va se présenter ci-dessous en langage 'fortran'

m (entier positive) - désigne le numéro du point présent
b(i) (tableau) - conservateur des points passés
nn(i) (tableau) - les traces de l'itération de points (d'où, 888, 999 sont deux signaux séparant les points sectionnés.
r(i,j) (tableau avec deux dimensions - conservateur des nouveaux points de départ provenus des solutions des systèmes $F'(x^r) \cdot z = F(x^r)$... (3')

(1) S'il ne reste plus de point initial, aller à (10) sinon faire entrer un point x^r dont le numéro est m

(2) Faire comparer m avec le contenu de b(i)
Si m est déjà dans b(i) aller à (3), sinon faire marquer m dans b(i) et dans nn(i) et puis aller à (5).

(3) Marquer m et 999 dans nn(i). Si m vient de (1) sans calcul retourner à (1)

(4) Si r(i,j) non vide, prendre un point dont le numéro est le nouveau m retourner à (2), sinon retourner à (1)

(5) En utilisant m former le vecteur x^r avec lequel procurer $F(x^r)$ soit par une table, soit par un tableau calculé en certaine formule, soit par appeler un autre sous-programme (surtout lors de p^n assez grand), si $F(x^r)$ est un vecteur nul, marger x^r, un point fixe, ou bien une racine trouvée de F(x)

(6) En utilisant x^r et $F(x^r)$, former la dérivée $F'(x^r)$ (pour obtenir les vecteurs des voisins des x^r , faire le même que $F(x^r)$)

(7) Appeler le sous-programme, nommé respn, pour résoudre le système $F'(x^r) \cdot z = F(x^r)$ (3')

(8) Si (3') n'a pas de solution, marquer 888 dans nn(i) aller à (4)

(9) Si (3') a de plusieurs solutions d'après (3"), on obtiendra plusieurs nouveaux points de départ. Conserver-les dans r(i,j), en prendre un dont le numéro est nouveau m, alors, aller à (2)
Sinon (solution unique), prendre ce nouveau point de départ dont le numéro est nouveau m,
aller à (2)

(10) La fin de l'itération totale.

2. Un des sous-programmes nommé respn pour résoudre (3').
En prenant une manière de creuser une matrice par colonne ,
On déroule le schémas de ce sous-programme.

i,j (entiers positifs) - désignent respectivement les numéros de lignes et colonnes

a(i,j) (tableau) - désigne une matrice (n x (n+1)) dont la dernière colonne est $F(x^r)$ ou bien $\bar{f}_i$

I.J. désignent deux ensembles de lignes et colonnes respectivement

Tout d'abord on donne 1 à j

(1) si j=n aller à (5)

(2) dans jème colonne , chercher un certain élément non nul qui est situé dans ième ligne
Si $i \notin b(j)$, et $a(i,j) \neq 0$, faire $j \Rightarrow I$, $i \Rightarrow b(j)$ aller à
sinon ($\forall\, i \notin b(j)$, $a(i,j) = 0$) faire $j \Rightarrow J$, $j \Leftarrow j+1$
retourner à (1)

(3) dans ième ligne faire la division ($\ominus$) telle que ,
$a(i,j) = 1$

(4) Faire l'élimination de ligne telle que $a(u,j) = 0$
($1 \leq u \leq n$, $u \neq i$) , $j \Leftarrow j+1$ aller à (1)

(5) Soit $J = \{j_1, j_2, \ldots, j_\ell\}$, $I = \{i_1, i_2, \ldots, i_k\}$, $(\ell+k = n)$
Si J est vide ou bien $k = n$
$z(i) = a(b(i),n+1)$ (solution) , $(i=1,\ldots,n)$
aller à (9)

(6) Si certain $i_t \notin b(j)$ tel que $\bar{f}_{i_t} \neq 0$
marquer solution z impossible, aller à (9)
Sinon supposer v = 1

(7) Prendre vème possibilité de combinaison de $x_{j_1},\ldots,x_{j_\ell}$ qui peuvent être n'importe quel nombre dans Z/p, comme composantes de solutions z_v .

(8) D'après le système évolué et $x_{j_1},\ldots,x_{j_\ell}$ déjà fixés, calculer les autres composantes $x_{i_1},\ldots,x_{i_k}$ de z_v
Si $v \neq p^\ell$, faire $v \Leftarrow v+1$,
aller à (7)

(9) La fin de ce sous-programme.

```
      integer q,w,u,s,b,a,r,d,y,p,fzp
       logical papop
       dimension d(2,3),lx(2),y(49,4),lz(2),r(12,2),nn(300),w(17),u(17),a(49,2),b
     \c(49),jj(49),q(2)
444     format(i4,3x,f5.3)
222    format(25i4)
111    format(1x,'vd :(',5(i3,','),')')
200    format((6x,2i3,3x,2i3))
1200    format((4(1x,i1)))
600    format(100i4)
333    format((5(1x,i3)))
       read(40,200)((y(i,j),j = 1,4),i = 1,49)
       i1 = 0
       kk = 0
       ik = 0
       n = 2
       p = 7
       do 23 mm = 1,p ** n
       m = mm - 1
       if(i1.eq.0) goto 63
42          do 41 i = 1,i1
              if(m.eq.b(i)) goto 20
41     continue
 63    i1 = i1 + 1
       b(i1) = m
       kk = kk + 1
        nn(kk) = m
       if(m.ne.mm-1) goto 31
       k =0
       w(k) = 0
       u(k) = 0
       do 3 i = 1,n
         lx(i) = y(mm,i)
  3    continue
31       ii = 0
       do 16 i = 1,n
         d(i,n+1) = y(n+1,n+1)
         if(d(i,n+1).ne.0) ii = ii + 1
 16    continue
       do 4 i = 1,n
       if(lx(i).eq.p-1) goto 5
       q(i) = m + p * * (n - i)
EOF
       goto 4
  5    q(i) = m - (p-1) * p * * (n-i)
  4    continue
      if(ii.ne.0) goto 30
!      write(6,333)lx
!      write(6,111) q
!      write(6,333)((y(q(i)+1,n+j),i = 1,5),j = 1,5)
 30      do 7 i = 1,n
        do 8 j = 1,n
          ii = y(q(i)+1,n+j) - y(n+1,n+j)
          d(j,i) = fzp(ii)
  8    continue
  7    continue
       call rezpn(d,lz,p,n,papop,n1,a,fzp)
       if(papop) goto 77
       if(n1.ne.0) goto 88
       ik = ik + 1
       go to 13
88        k = k + 1
       jj(k) = m
       w(k) = n1
       u(k) = 1
       s = 0
       if(k.eq.1) goto 54
       do 2 i = 1,k -1
             s = s + w(i)
  2    continue
 54    do 51 i = 1,n1
             do 52 j = 1,n
              ii = lx(j) - a(i,j)
              r(s+1,j) = fzp(ii)
 52           continue
 51    continue
 27    j = s + u(k)
       do 11 i = 1,n
             lx(i) = r(j,i)
 11    continue
       if(u(k).eq.1) goto 14
       kk = kk +1
       nn(kk) = jj(k)
       goto 14
 13    do 17 i = 1,n
         ii = lx(i) - lz(i)
         lx(i) = fzp(ii)
 17    continue
 14    m = 0
       do 15 i = 1,n
         m = m + lx(i) * p ** (n-i)
 15    continue
         if(.not.papop) goto 42
 77      papop = .false.
       kk = kk + 1
       nn(kk) = 888
       goto 43
 20            if(nn(kk).gt.125) goto 2
       kk = kk + 1
       nn(kk) = m
       kk = kk + 1
       nn(kk) = 999
 43    if(k.eq.0) goto 23
 29       if(u(k).eq.w(k)) goto 28
       u(k) = u(k) + 1
       goto 27
 28    if(k.eq.1) goto 23
       k = k - 1
       s = s - w(k)
       goto 29
 23    continue
             write(6,600) nn
EOF
        ss = p * * n
        write(6,444) ik ,ik/ss
       write(6,222) b
        stop
```

rezpn.fortran 03/15/82 1602.7 hfh Mon

```
      subroutine rezpn(a,x,ip,n,imp,ll,r,zpf)
      logical imp
      integer a,x,r,b,q,s1,zpf
     dimension a(2,3),x(2),r(49,2),b(2),k1(2),k2(2),iy(2)
      imp = .false.
      n1 = 0
      n2 = 0
      ll = 0
     do 11 k = 1,n
        do 12 i = 1,n
          if(a(i,k).eq.0) goto 12
          if(n1.eq.0) goto 17
          do 18 j = 1,n1
            if(i.eq.b(j)) goto 12
 18         continue
 17       ll = i
          n1 = n1 + 1
          k1(n1) = k
          b(n1) = ll
EOP
          goto 13
 12     continue
        n2 = n2 + 1
        k2(n2) = k
        if(k.eq.n) goto 15
        goto 11
 13     if(a(ll,k).eq.1) goto 19
        l2 = mzp(a(ll,k))
        do 22 j = k+1,n+1
          a(ll,j) = a(ll,j) * l2
          a(ll,j) = zpf(a(ll,j))
 22     continue
 19     do 23 i = 1,n
          if((i.eq.ll).or.(a(i,k).eq.0)) goto 23
          do 24 j = k+1,n+1
            if(a(ll,j).eq.0) goto 24
            a(i,j) = a(i,j) - a(i,k) * a(ll,j)
            a(i,j) = zpf(a(i,j))
 24       continue
 23     continue
 11     continue
 15     if(n2.ne.0) goto 25
        do 26 i = 1,n1
EOP
          x(i) = a(b(i),n+1)
 26     continue
        goto 35
 25     if(n1.ne.0) goto 27
        do 28 i = 1,n
          if(a(i,n+1).eq.0) goto 28
          goto 14
 28     continue
 27     do 29 i = 1,n
          do 30 j = 1,n1
            if(i.eq.b(j)) goto 29
 30       continue
          if(a(i,n+1).eq.0) goto 29
          goto 14
 29     continue
 16     ll = ip ** n2
        do 31 i = 1,ll
          do 32 j = 1,n2
            r(i,k2(n2-j+1)) = iy(n-j+1)
 32       continue
          if(n2.eq.n) goto 31
          do 33 j = 1,n1
            ll = 0
            do 34 k = 1,n2
              ll = ll + a(b(j),k2(k)) * r(i,k2(k)
 34         continue
            r(i,k1(j)) = a(b(j),n+1) - ll
 33       continue
 31     continue
        goto 35
 14     imp = .true.
 35     return
        end
```

fzp.fortran

```
      integer function fzp(i)
       ip = 7
       fzp = i - ip * (i/ip)
       if(i.lt.0) fzp = ip + fzp
       if(fzp.eq.ip) fzp = 0
       return
       end
```

chervp.fortran

```
      subroutine chervp(nn,ip,mm,ix)
      dimension ix(2)
      im = mm
      do 11 i  = 1,nn-1
        ii = ip * * (nn-i)
        do 12 j = 1,ip
          kk = j * ii
          if(im.gt.kk) goto 12
          if(im.lt.kk) goto 13
          ix(i) = j
          do 14 k = i+1,nn
            ix(k) = 0
 14       continue
          goto 15
 13       ix(i) = j - 1
          im = im - ix(i) * ii
          goto 11
 12     continue
 11   continue
EOP
      ix(nn) = im
 15   return
      end
```

ANNEXE 2 : QUELQUES TABLEAUX THEORIQUES ET EXPERIMENTAUX

Etant donné un système d'équations linéaire dans $(Z/p)^n$ dont la matrice de coefficients A, le vecteur de variables X , le vecteur de constantes B , sont ceux à éléments quelconques dans Z/p , peut s'écrire comme ci-dessous :

$$A \otimes X = B \qquad (6)$$

Une fois que p et n sont choisis, cela va fixer le nombre de toutes les formations possibles de former le système (6), noté S, dont l'une partie serait celui des systèmes solubles, noté S1, l'autre serait celui des systèmes impossibles.

On peut aussi diviser S1 en deux parties, celle avec A régulière notée S11 , celle avec A singulière , notée S12 où on note R pour le nombre de formations possibles de A singulière, R_r pour le nombre de formations possibles avec A possèdant le rang r ($r = 0,1,\ldots,n-1$). En brève, on a des relations suivantes :

$$S = p^{n^2} \cdot p^n$$

$$S1 = S11 + S12$$

$$S11 = p^n(p^n-1)(p^n-p) \ldots (p^n-p^{n-1})$$

$$R = \sum_{r=0}^{n-1} R_r = p^{n^2} - (p^{n-1}-1)(p^n-p) \ldots (p^n-p^{n-1})$$

$$S12 = \sum_{r=0}^{n-1} R^r \cdot p^r$$

Pour obtenir la proportion des systèmes solubles , λ_n^p $(= \frac{S1}{S})$, il faudrait procurer S12 qui dépend de la détermination de chaque R_r.

Dans ce but, je voudrais introduire un moyen d'écrire toutes les formations possibles de A à rang r avec les rangements des r vecteurs indépendants dans A dont le nombre est noté Tr, dans lequel il y a Lr répétitions de formations qui doivent être soustraits.

Voilà une série de formules pour calculer R_r :

$$R_r = T_r - L_r$$

$$T_r = p^{r(n-r)} \cdot C_n^r \cdot Q_r$$

$$Qr = (p^n-1)(p^n-p) \ldots (p^n-p^{r-1})$$

$$L_r = \sum_{j=1}^{S_r} \frac{C_n^r \cdot Q_r \cdot j \cdot m_j}{j+1}$$

$$S_r = \sum_{i=1}^{k} C_{n-r}^i \cdot C_r^{r-i} \quad , \quad (k = \min (r,n-r))$$

pour calculer L_r , j'obtiens un tableau des valeurs de m_j divers qui se présente ci-dessous. Ainsi , on pourrait obtenir un tableau de R_r et celui de λ_n^ρ .

λ_n^p : p \ n	1	2	3	4	5	6		∞
2	0.7500	0.6719	0.6394	0.6254	0.6173	0.6125		0.608
3	0.7778	0.7257	0.7100	0.7049	0.7031			0.702
5	0.8400	0.8141	0.8092	0.8081				0.808
7	0.8776	0.8625	0.8604	0.8601				0.860
11	0.9174	0.9105	0.9099					0.910
13	0.9290	0.9240						0.924
17	0.9446	0.9416						0.942
19	0.950	0.949						0.949
97	0.990							0.990
103	0.990							0.990

TABLEAU DE λ_n^p

* pour tout p , $\frac{p}{n}$ converge vers une limite quand n croît, le rythme s'accélère plus vite quand p croît .

* pour p assez grand, la proportion des systèmes solubles se rapproche rapidement de 1.

* En comparant avec l'annexe 2 de [1], on peut en trouver, lors de p assez petit, la différence évidente entre la proportion dessystèmes solubles et celle de leurs matrices de coefficients qui sont réguliers. Surtout quand p=2 , celle-ci parait beaucoup plus frappante.

R_r : n / p / r	2		3			4				5				
	0	1	0	1	2	0	1	2	3	0	1	2	3	4
2	1	9	1	49	294	1	225	7602	37800	1	961	144150	4036200	19373760
	R = 10		R = 344			R = 45628				R = 23555072				
3	1	32	1	338	8112	1	3200	811200	17971200					
	R = 33		R = 8451			R = 18785601								
5	1	144	1	3844	461280	1	97344	311825280	36211968000					
	R = 145		R = 465125			R = 36523890625								
7	1	384	1	19494	6549984									
	R = 385		R = 6569479											
11	1	1440												
	R = 1441													
13	1	2352												
	R = 2353													

TABLEAU DE R_r

n	2	3				4								5																															
m_j r	1	1		2		1			2					3			1				2							3									4							
s_r	1	2		2		3			5					3			4				9							9									4							
p j	1	1	2	1	2	1	2	3	1	2	3	4	5	1	2	3	1	2	3	4	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	1	2	3	4
2	1	2	1	2	1	3	3	1	4	4	2	5	0	3	3	1	4	6	4	1	6	9	8	15	6	7	12	0	0	6	9	8	15	6	7	12	0	0	4	6	4	1
3	2	4	4	4	4	6	12	8	8	16	8	40	8	6	12	8	8	24	32	16	12	36	40	120	72	112	192	144	0	12	36	40	120	72	112	240	96	0	8	24	32	16
5	4	8	16	8	16	12	48	64	16	64	32	320	192	12	48	64																												
7	6	12	36	12	36	18	108	216	24	144	72	1080	1080	18	108	216																												
11	10	20	100	20	100																																							
13	12																																											

Table de m_j

1 Le tableau suivant nous donne quelques valeurs de proportions des matrices A régulières des systèmes (6) , à la fois théoriques ·(TT) et expérimentales (TE).

2 Dans les lignes à * , représentent quelques valeurs de proportions des systèmes solubles, à la fois théoriques et expérimentales.

3 A B C D représentent les exemple dans lesquelles les proportions expérimentales ont été obtenues.

4 Ce tableau nous montre que les proportions expérimentales diffèrent un peu à celle théoriques et maintiennent les mêmes propriétés que celles théoriques possèdent.

p \ n	1		2		3		4		5	
	TT	TE	TT	TE	TT	TE	TT	TE	TT	TE
2	0.500	A0.500 B0.500 C 1.000	0.375	A0.500 B0.250 C 0.500	0.328	A0.375 B0.250 C 0.500	0.307 *0.625	A0.375 B0.313 A0.625 B0.688	0.298 *0.617	A0.281 B0.344 A0.625
3	0.666	A0.667 B0.333 C 0.667	0.592	A0.333 B0.556 0.667	0.570	A0.593 B0.444 C 0.444	0.563 *0.705	A0.588 B0.492 A0.725 B0.690	0.561 *0.703	A0.426 B0.551 A0.639 B0.726
5	0.800	A0.800 B1.000 C 0.600	0.768	A0.760 B0.800 C0.720 D0.840	0.761	A0.639 B0.589 C 0.753	0.760 *0.808	A0.763 B0.556 A0.784 B0.728	0.760 *0.808	A0.712 B0.582 A0.784 B0.801
7	0.857	A1.000 B0.857 C 0.857	0.839	A0.716 B0.816 C 0.796	0.837	A0.830 B0.856 C 0.790	0.836 *0.860	A0.842 B0.817 A0.858 B0.835	0.836 *0.860	A0.789 B0.810 A0.813 B0.845
11	0.909	A0.909 B1.000	0.901	A0.818 B0.909 C 0.893	0.900	A0.869 B0.890	0.900 *0.910	A0.866 B0.925 A0.870 B0.932	0.900 *0.910	A0.878 B0.917 A0.895 B0.928

ANNEXE 3 : COLLEXION DES FIGURES

Finalement, je voudrais dans ces dernières pages, collectionner quelques exemples que j'ai effectué avec lesquelles j'ai dessiné beaucoup de graphes d'itérations de ces trois méthodes, qui ont été choisis selon les raisons suivantes :

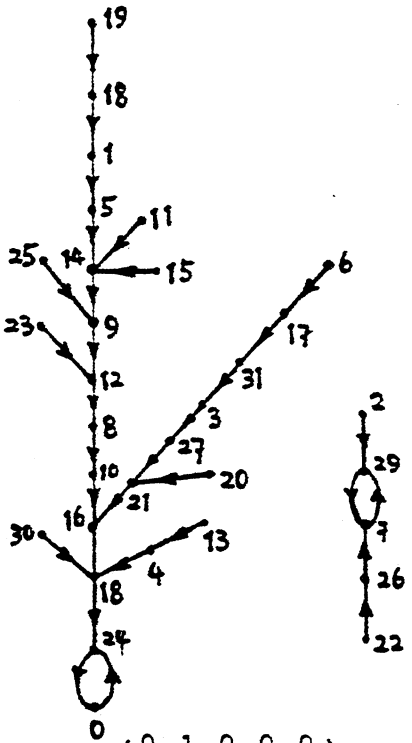
1) pouvant refléter les caractéristiques générales pour F(x) donnée par une table ou des polynômes généraux.

2) pouvant présenter quelques particularités pour certains types de F(x) bien caractérisée.

3) pouvant s'exprimer quelques évolutions d'itérations pour F(x) ou ce qui associé à l'itération, ayant certaines transformations de structure.

	x					F(x)				
0	0	0	0	0	0	1	1	0	0	0
1	0	0	0	0	1	0	0	1	0	0
2	0	0	0	1	0	1	1	1	1	1
3	0	0	0	1	1	1	1	0	0	0
4	0	0	1	0	0	0	1	1	0	1
5	0	0	1	0	1	1	0	0	1	1
6	0	0	1	1	0	0	1	1	1	1
7	0	0	1	1	1	1	1	0	0	1
8	0	1	0	0	0	0	0	0	0	1
9	0	1	0	0	1	0	0	1	1	0
0	0	1	0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0	1	1	0
2	0	1	1	0	0	0	0	1	0	0
3	0	1	1	0	1	1	0	0	1	0
4	0	1	1	1	0	0	0	1	1	1
5	0	1	1	1	1	0	0	0	1	0
6	1	0	0	0	0	0	0	0	0	1
7	1	0	0	0	1	1	0	1	0	1
8	1	0	0	1	0	1	0	0	0	1
9	1	0	0	1	1	1	0	1	1	1
0	1	0	1	0	0	0	0	0	1	0
1	1	6	1	0	1	0	0	1	1	0
2	1	0	1	1	0	1	0	1	0	0
3	1	0	1	1	1	1	1	0	1	1
4	1	1	0	0	0	1	1	0	0	0
5	1	1	0	0	1	0	1	0	0	0
6	1	1	0	1	0	1	1	1	1	0
7	1	1	0	1	1	1	0	1	0	1
8	1	1	1	0	0	1	1	1	1	0
9	1	1	1	0	1	1	1	0	0	1
0	1	1	1	1	0	1	0	1	0	0
1	1	1	1	1	1	1	1	1	0	0

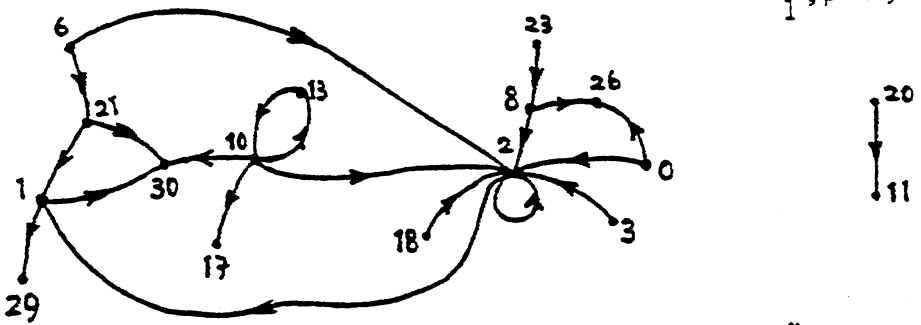
Newton simplifiée sur F_0



$$A=A^{-1}=\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Fig.1.1

Newton standard sur F_1, p=2, n=5



$V_x(2)=\{2,18,10,6,0,3\}$

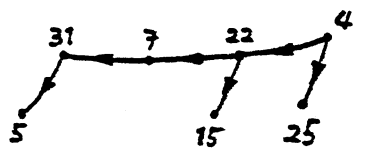
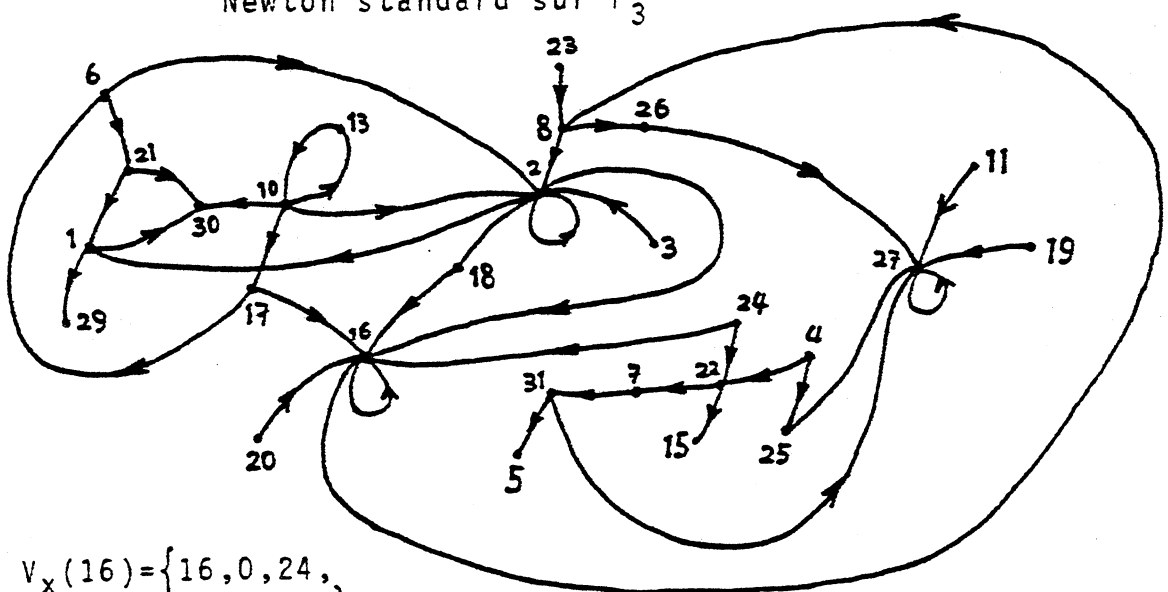


Fig.1.2

Newton standard sur F_3



$V_x(16)=\{16,0,24,20,18,17\}$

$V_x(27)=\{27,11,19,31,25,26\}$

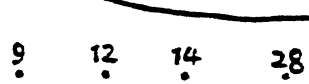


Fig.1.3

	x					F(x)				
0	0	0	0	0	0	1	1	1	1	1
1	0	0	0	0	1	1	0	1	0	0
2	0	0	0	1	0	1	1	1	0	1
3	0	0	0	1	1	1	1	1	1	0
4	0	0	1	0	0	1	1	0	1	1
5	0	0	1	0	1	1	1	1	1	0
6	0	0	1	1	0	1	1	0	0	1
7	0	0	1	1	1	1	1	0	0	0
8	0	1	0	0	0	1	0	1	1	1
9	0	1	0	0	1	1	0	1	0	0
10	0	1	0	1	0	1	0	1	0	1
11	0	1	0	1	1	0	0	0	1	0
12	0	1	1	0	0	1	0	0	1	1
13	0	1	1	0	1	1	0	0	0	1
14	0	1	1	1	0	1	0	0	0	1
15	0	1	1	1	1	0	0	0	1	0
16	1	0	0	0	0	0	1	1	1	1
17	1	0	0	0	1	0	0	1	1	1
18	1	0	0	1	0	0	1	1	0	1
19	1	0	0	1	1	0	0	1	0	0
20	1	0	1	0	0	0	1	0	1	1
21	1	0	1	0	1	1	1	0	0	1
22	1	0	1	1	0	0	1	0	0	1
23	1	0	1	1	1	0	0	0	0	1
24	1	1	0	0	0	0	0	1	1	1
25	1	1	0	0	1	0	1	1	1	1
26	1	1	0	1	0	0	0	1	0	1
27	1	1	0	1	1	0	1	1	0	1
28	1	1	1	0	0	0	0	0	1	1
29	1	1	1	0	1	0	1	0	1	0
30	1	1	1	1	0	0	0	0	0	1
31	1	1	1	1	1	1	1	0	0	0

Newton simplifiée sur F_2
p=2, n=5

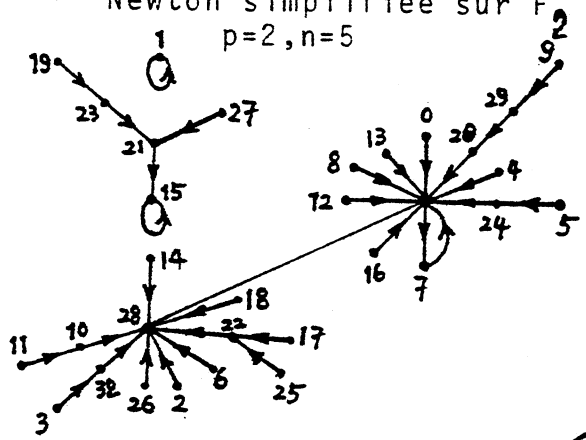


Fig.2.1

Newton simplifiée sur F_3
p=2, n=5

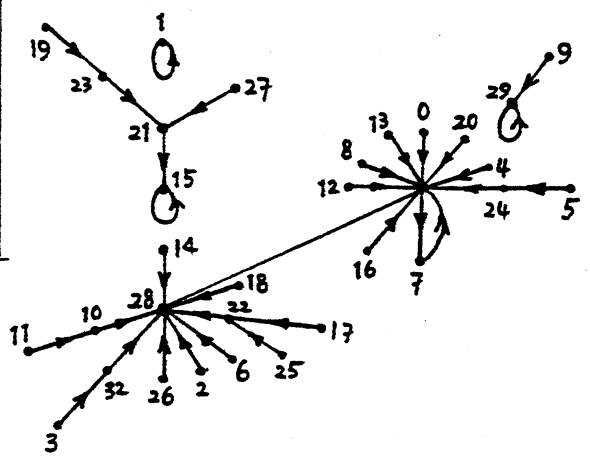


Fig.2.2

Newton standard sur F_2, p=2, n=5

$V_x(1)=\{1,0,3,5,9,17\}$

$V_x(15)=\{15,7,11,13,14,31\}$

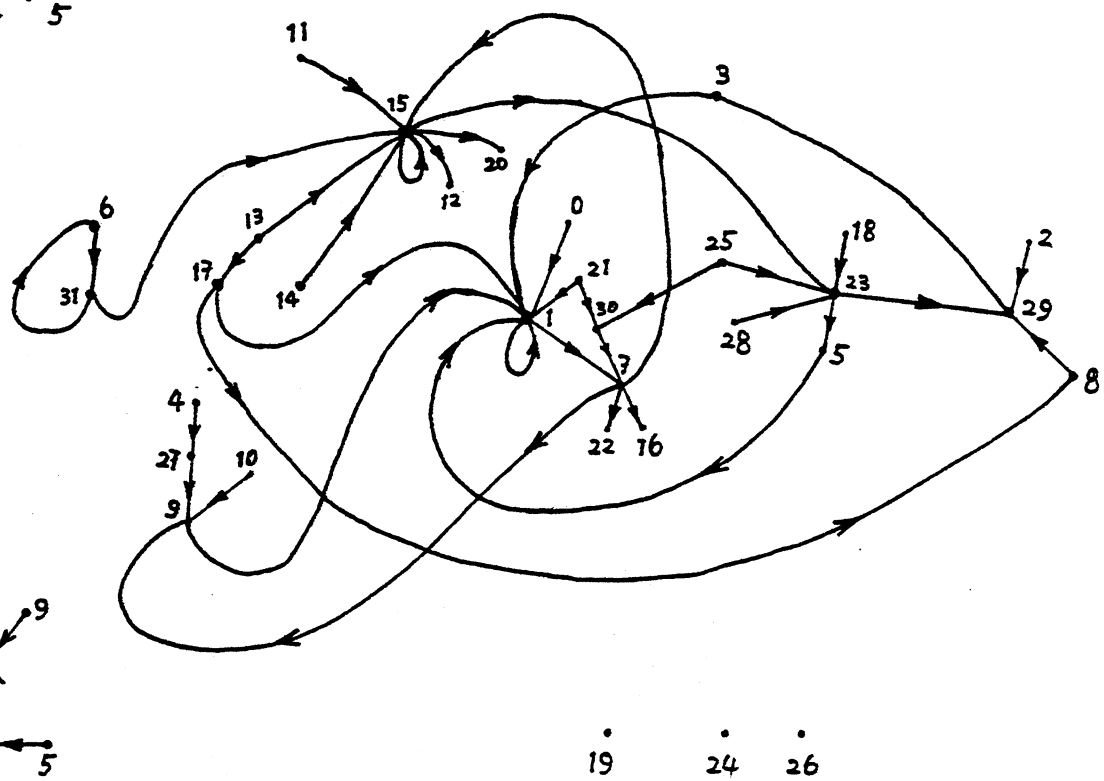


Fig.2.3

	x				F(x)			
0	0	0	0	0	1	0	1	0
1	0	0	0	1	1	0	0	0
2	0	0	1	0	0	0	0	1
3	0	0	1	1	0	0	0	0
4	0	1	0	0	1	0	0	0
5	0	1	0	1	0	1	1	0
6	0	1	1	0	1	0	1	0
7	0	1	1	1	1	0	1	1
8	1	0	0	0	1	0	0	1
9	1	0	0	1	1	1	1	1
0	1	0	1	0	1	0	1	1
1	1	0	1	1	1	1	1	1
2	1	1	0	0	1	0	1	0
3	1	1	0	1	0	1	0	0
4	1	1	1	0	1	0	0	0
5	1	1	1	1	1	0	1	1

Newton simplifiée

p = 2 , n = 4

$$F'(3)=\begin{pmatrix}1&1&1&0\\1&0&0&0\\0&1&0&0\\1&1&0&1\end{pmatrix}$$

3 : racine de F(x)

$$A_2=\begin{pmatrix}1&1&1&0\\1&0&0&0\\1&1&0&0\\0&1&0&1\end{pmatrix}$$

$$A_2^{-1}=\begin{pmatrix}0&1&0&0\\0&1&1&0\\0&0&1&0\\1&1&1&1\end{pmatrix}$$

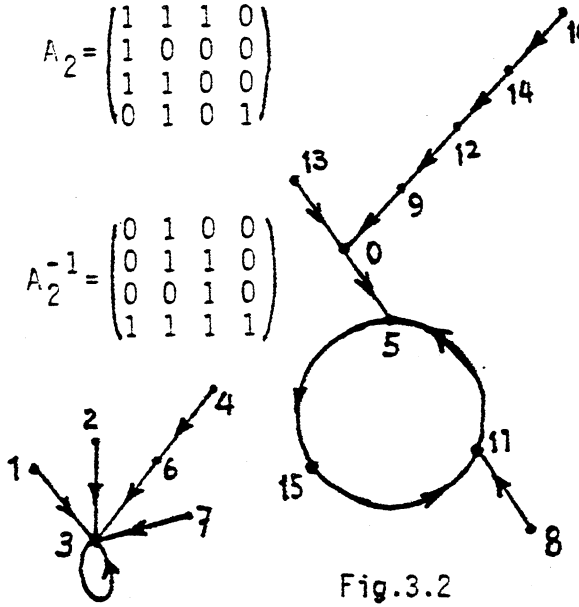


Fig.3.2

$A_3 = F'(3)$

$$A_3^{-1}=\begin{pmatrix}0&1&0&0\\0&0&1&0\\1&1&1&0\\0&1&1&1\end{pmatrix}$$

$V_z(3) = \{11, 7, 1, 2, 3\}$

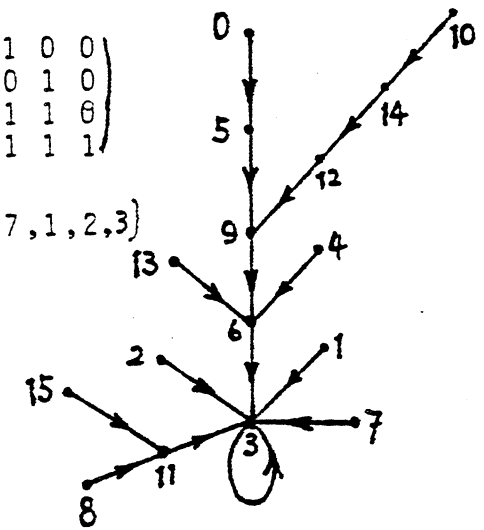


Fig.3.3

$$A_1=\begin{pmatrix}1&1&1&0\\0&0&0&0\\0&1&0&0\\0&1&0&1\end{pmatrix}$$

$$A_1^{-1}=\begin{pmatrix}0&1&0&0\\0&0&1&0\\1&1&1&0\\0&0&1&1\end{pmatrix}$$

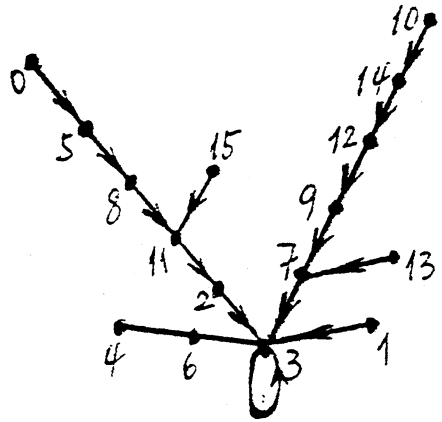


Fig.3.1

$$A_4=\begin{pmatrix}0&1&0&0\\1&0&1&1\\1&1&0&0\\0&1&0&1\end{pmatrix}$$

$$A_4^{-1}=\begin{pmatrix}1&0&1&0\\1&0&0&0\\0&1&1&1\\1&0&0&1\end{pmatrix}$$

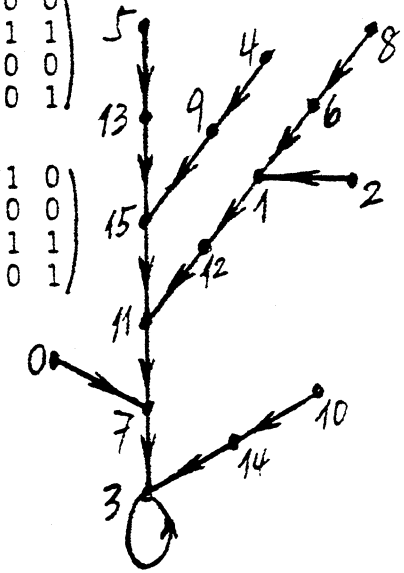


Fig.3.4

$$A_5=\begin{pmatrix}0&1&0&0\\1&0&1&0\\1&1&0&0\\0&1&0&1\end{pmatrix}$$

$$A_5^{-1}=\begin{pmatrix}1&0&1&0\\1&0&0&0\\1&1&1&0\\1&0&0&1\end{pmatrix}$$

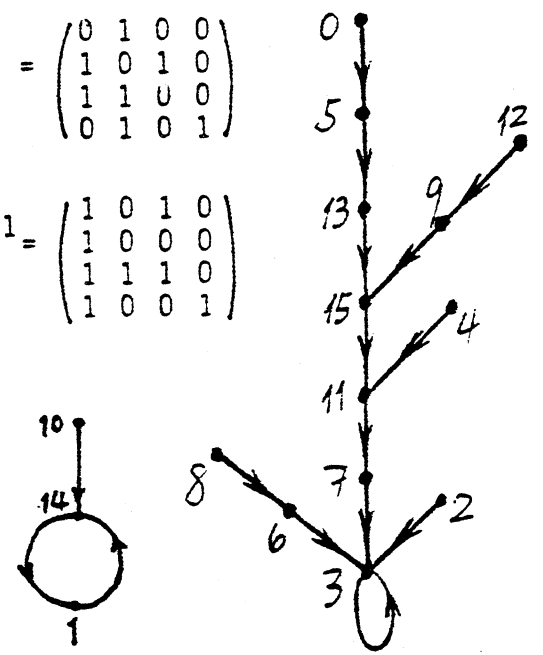


Fig.3.5

	x			F(x)		
0	0	0	0	2	1	1
1	0	0	1	1	0	2
2	0	0	2	1	2	1
3	0	1	0	1	1	0
4	0	1	1	1	0	1
5	0	1	2	1	0	2
6	0	2	0	1	2	2
7	0	2	1	1	2	0
8	0	2	2	1	0	1
9	1	0	0	0	2	1
10	1	0	1	2	1	1
11	1	0	2	1	2	0
12	1	1	0	1	2	0
13	1	1	1	0	0	2
14	1	1	2	1	0	1
15	1	2	0	2	0	1
16	1	2	1	1	1	1
17	1	2	2	0	0	0
18	2	0	0	1	2	2
19	2	0	1	2	2	2
20	2	0	2	1	1	0
21	2	1	0	0	1	2
22	2	1	1	0	0	1
23	2	1	2	0	1	1
24	2	2	0	2	0	2
25	2	2	1	0	2	1
26	2	2	2	1	1	2

Newton ismplifiée, p=n=3,sur F_1

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

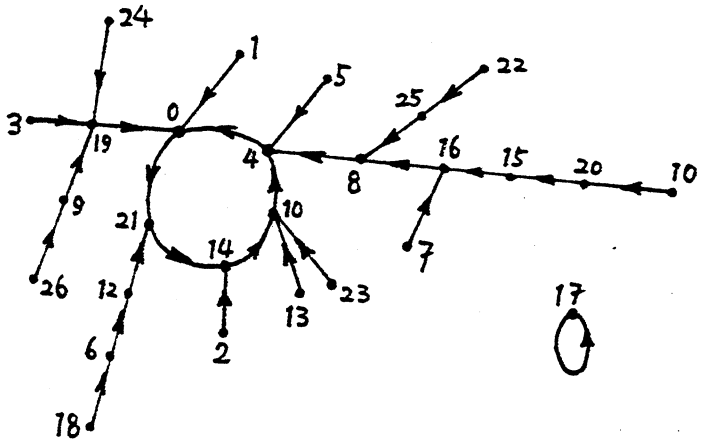


Fig.4.1

Newton standard sur F_2, p=n=3

Dans la table,F(6) remplacée par (0 0 0).

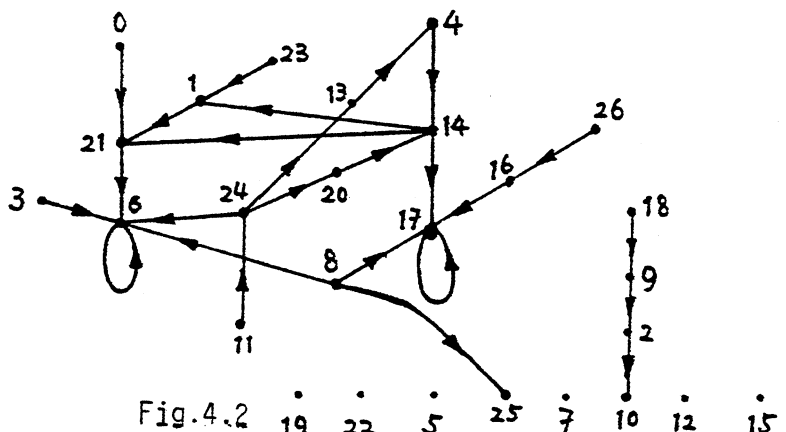


Fig.4.2

Newton simplifiée,p=n=3,sur F_3. Dans la table F(6),F(12),F(8),F(14),F(16),remplacées par (0 0 0),(0 0 0),(2 2 1),(2 1 0),(1 0 2),resp.

$$A = F_d'(17) = F_g'(17) = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

Alors, $V_d(17) \cup V_g(17) \longrightarrow 17$ (racine)

en un seul coup.

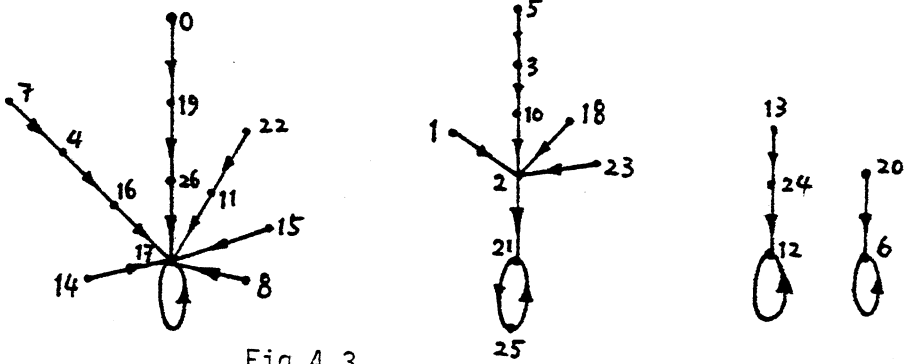


Fig.4.3

Newton standard sur F_1, p = n = 3

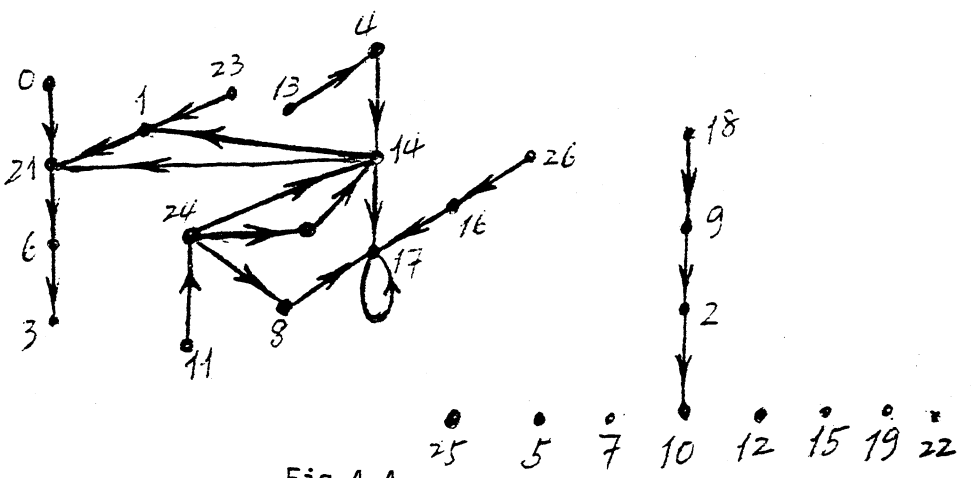


Fig.4.4

x		F(x)	
0	0	4	1
1	0	1	2
2	0	2	1
3	0	3	3
4	0	4	0
5	1	0	4
6	1	1	3
7	1	2	1
8	1	3	0
9	1	4	1
0	2	0	2
1	2	1	4
2	2	2	0
3	2	3	1
4	2	4	4
5	3	0	0
6	3	1	0
7	3	2	3
8	3	3	2
9	3	4	1
0	4	0	2
1	4	1	0
2	4	2	3
3	4	3	4
4	4	4	3

Newton simplifiée sur F_1

p=5, n=2, $A=\begin{pmatrix}3 & 1\\ 4 & 2\end{pmatrix}$

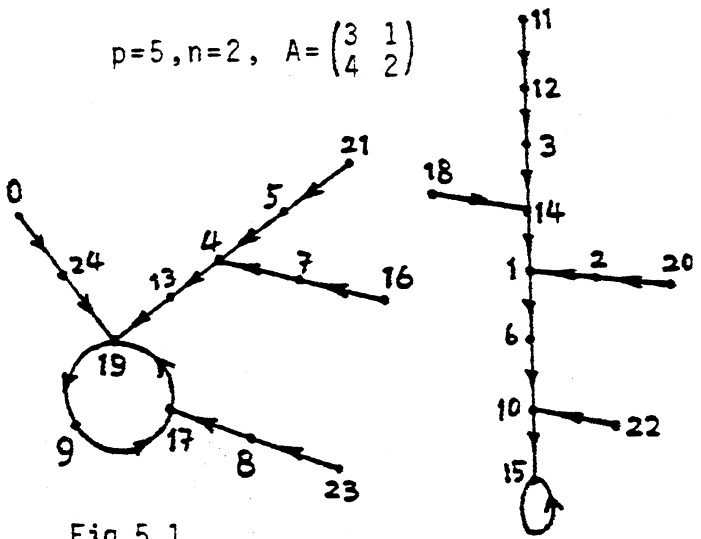


Fig.5.1

Newton standard sur F_1

p=5, n=2

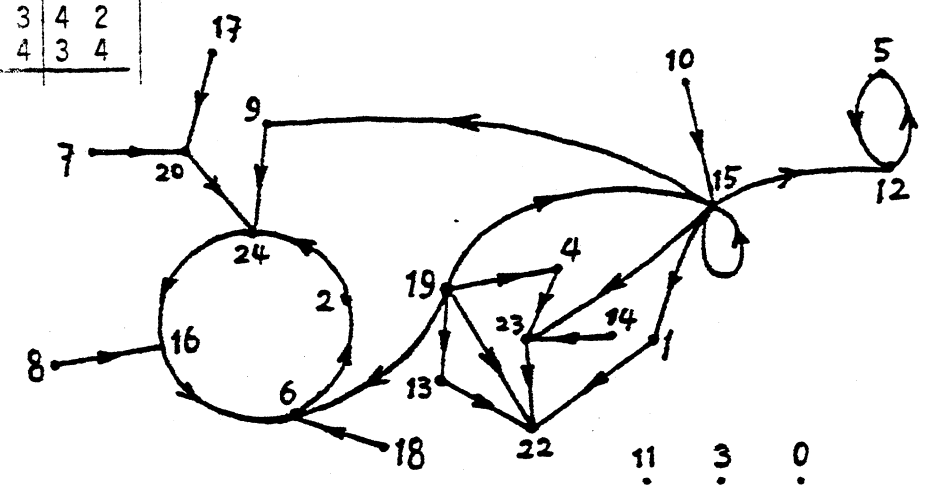


Fig.5.2

Newton simplifiée p=5, n=2

Dans la table on remplace F(8),F(15),F(22), F(7),F(13),F(9) par (0 0),(3 1),(3 1),(1 2) (2 0),(4 3) respectivement, on donc

$A=F_d'(8)=F_g'(8)=\begin{pmatrix}2 & 4\\ 0 & 3\end{pmatrix}$

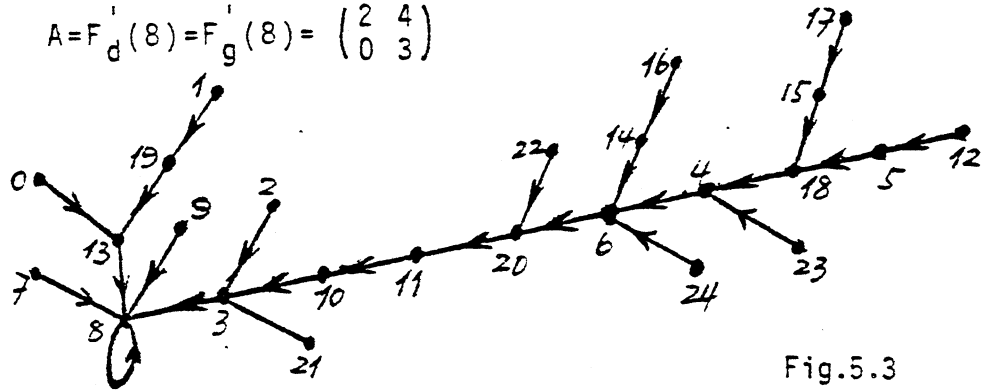


Fig.5.3

Newton standard p=5, n=2

même table que celle de fig 5-3

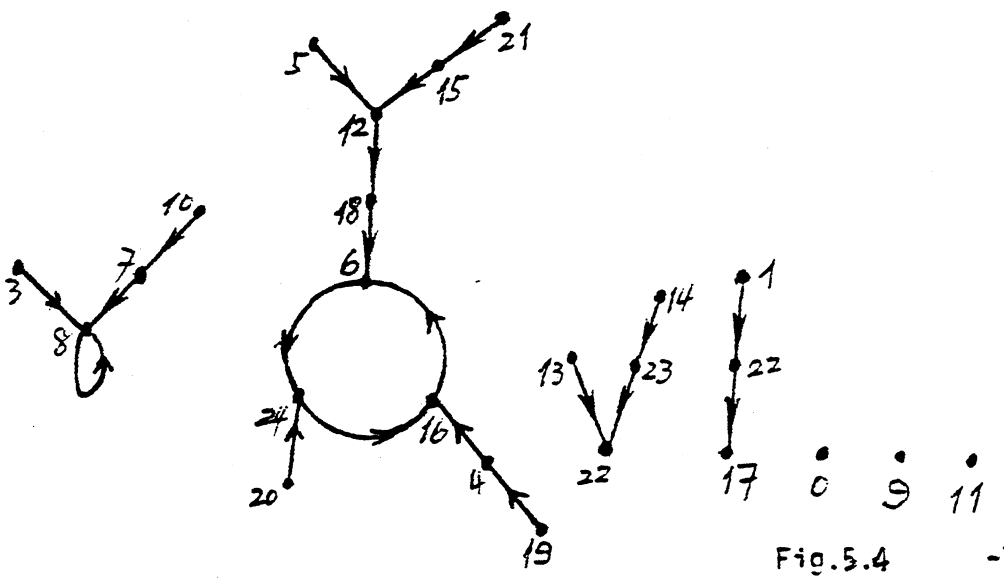


Fig.5.4

$$F(x) = \begin{cases} f_1 = x_1^2 + x_2x_3 \\ f_2 = x_2^2 + x_3x_1 \\ f_3 = x_3^2 + x_1x_2 \end{cases} \qquad F(x) : (Z/p)^n \longrightarrow (Z/p)^n$$

$p = n = 3$

Newton standard

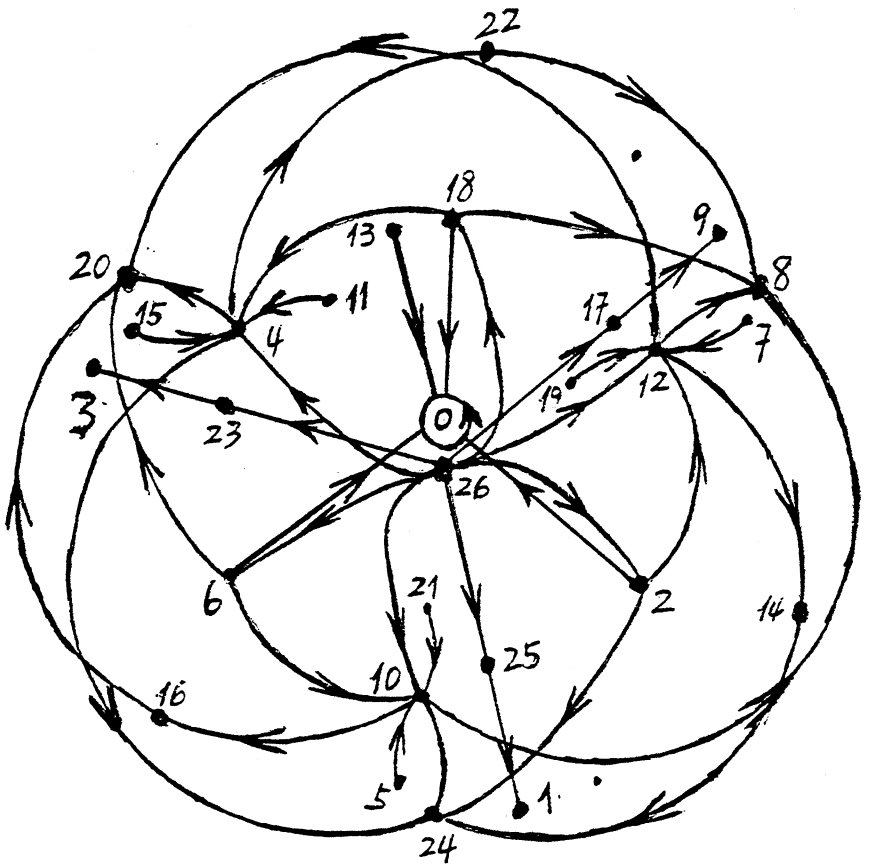


Fig.6.1

$$F(x) = \begin{cases} f_1 = x_1^2 + x_1x_2x_3 \\ f_2 = x_1x_2 + x_2^2 + x_2x_3 + 1 \\ f_3 = x_1x_3 + x_2x_3 + x_3^2 + x_3 \end{cases}$$

$F(x) : (Z/p)^n \longrightarrow (Z/p)^n \qquad p = n = 3$

Newton standard

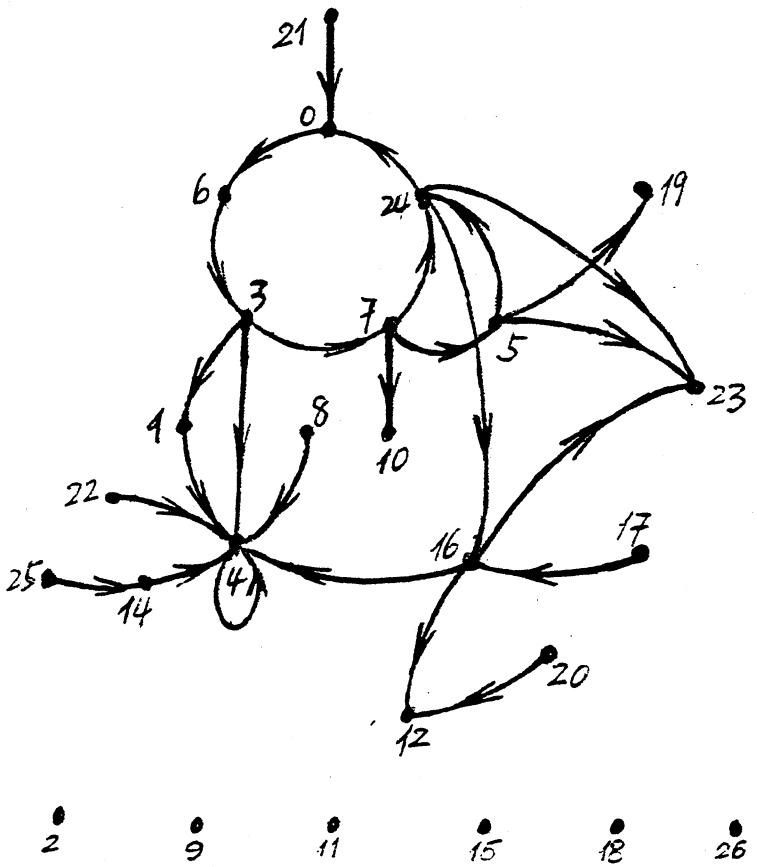


Fig.6.2

$$F(x) = \begin{cases} f_1 = 2x_1 + x_3 \\ f_2 = x_1 + x_2 + 2x_3 + x_1x_2 \\ f_3 = 2x_2 + 2x_3 + x_1x_2x_3 \end{cases}$$

$$A = B = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix} \qquad F(x) = Bx + C + U(x)$$

$$C = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad U(x) = \begin{pmatrix} 0 \\ x_1x_2 \\ x_1x_2x_3 \end{pmatrix} \qquad p = n = 3$$

Newton simplifiée

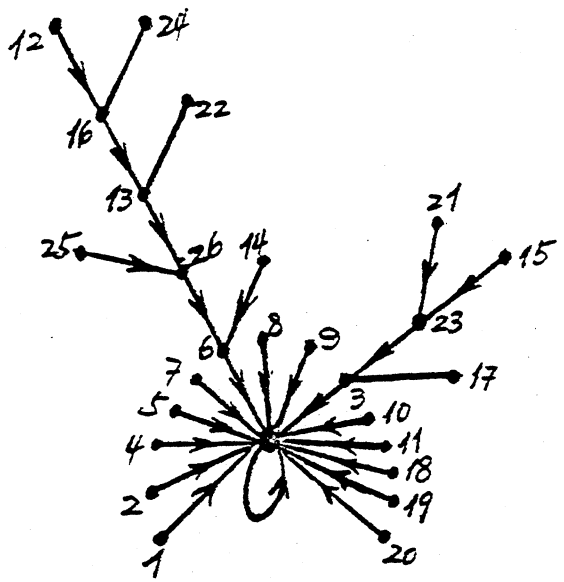


Fig.7.1

$$F(x) = \begin{cases} f_1 = x_2 + x_3 + x_4 + x_5 \\ f_2 = x_2 + x_3 + x_4 + x_5 + x_1x_2 \\ f_3 = x_3 + x_4 + x_5 + x_1x_2x_3 \\ f_4 = x_4 + x_5 + x_1x_2x_3x_4 + 1 \\ f_5 = x_5 + x_1x_2x_3x_4x_5 \end{cases} \qquad p = 2, n = 5$$

Newton standard

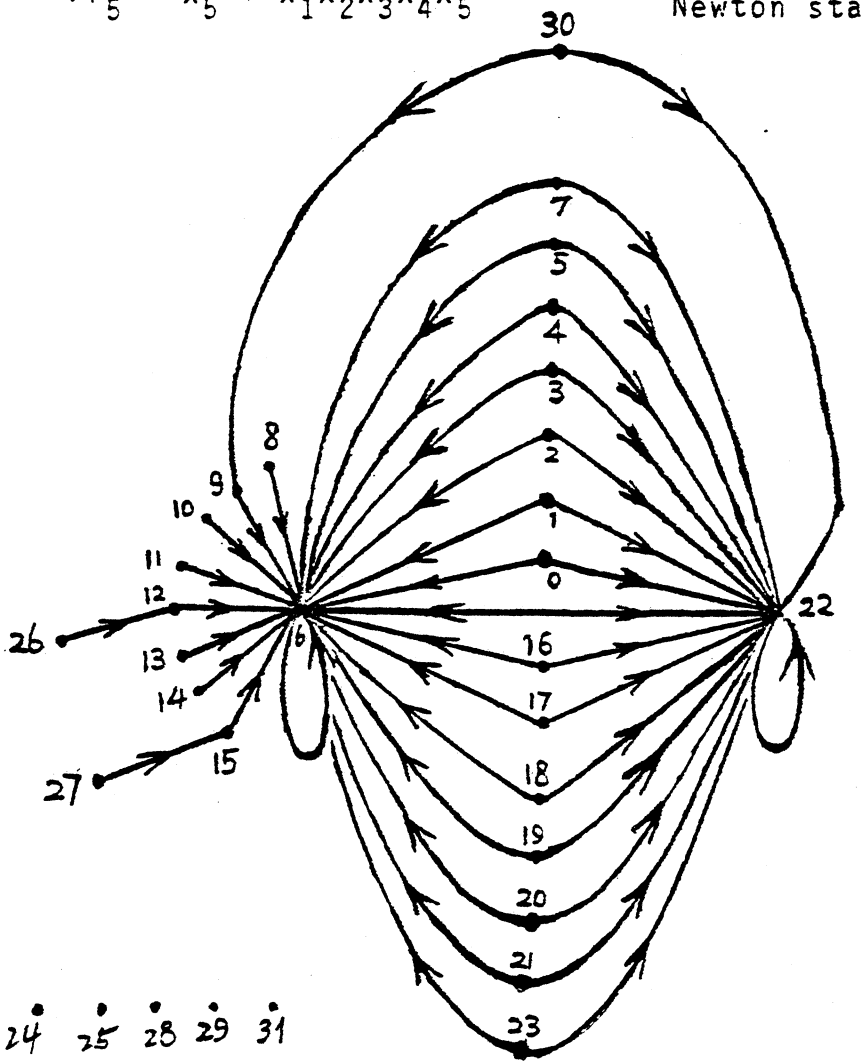


Fig.7.2

$$F(x)=\begin{cases} f_1=x_1(x_1+\cdots+x_n) \\ f_2=x_2(x_1+\cdots+x_n) \\ \quad\cdots \\ f_n=x_n(x_1+\cdots+x_n) \end{cases} \qquad F(x):(Z/p)^n \longrightarrow (Z/p)^n$$

On note R representant l'ensemble de racines

p = 3
n = 2
R = {0,5,7}

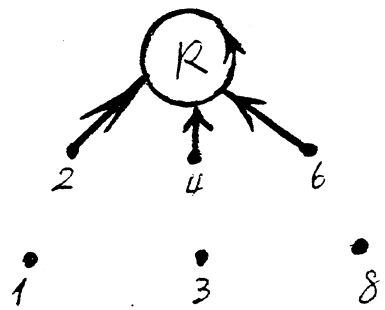


Fig.8.1

p = 7 , R = {0,13,19,25,31,37,43}
n = 2

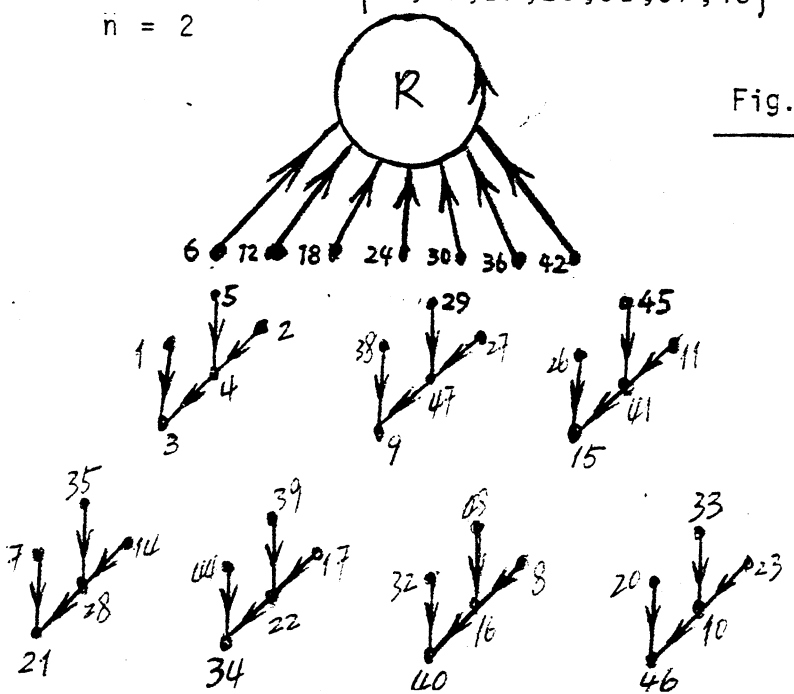


Fig.8.2

p = n = 3, R = {0,5,7,11,13,15,19,21,26}

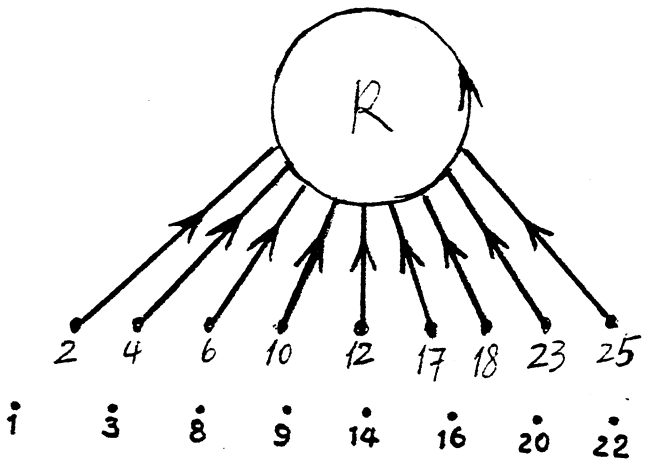


Fig.8.2

p = 11, n = 2, R = {0,21,31,41,51,61,71,81, 91,101,111}

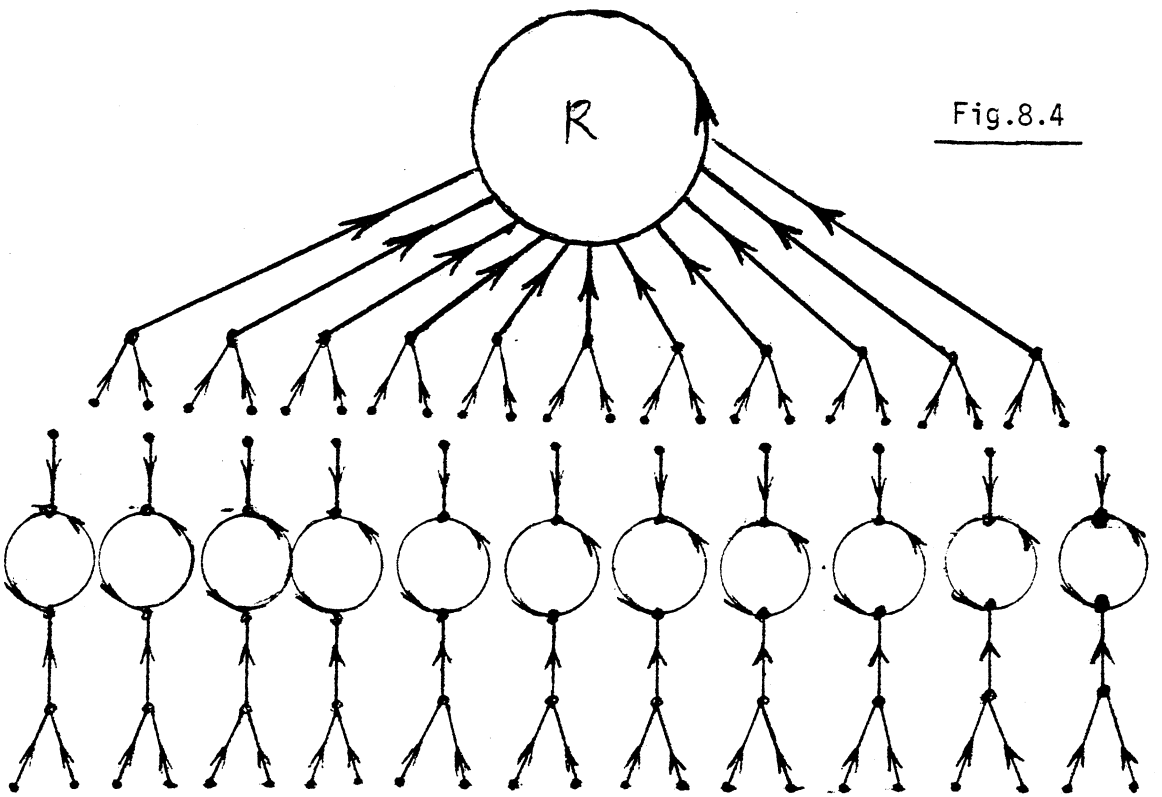


Fig.8.4

$$F(x) = \begin{cases} f_1 = x_2^2 + x_4x_3 + x_3 + p - 1 \\ f_2 = x_3^2 + x_1x_2 + x_3 + x_4 + p - 1 \\ f_3 = x_1^2 + x_4^2 + x_1x_3 + x_2x_3 + x_2 \\ f_4 = x_2^2 + x_1x_3 + x_4 + 1 \end{cases}$$

$F(x): (Z/p)^n \longrightarrow (Z/p)^n$, $p = 2$., $n = 4$

Newton standard

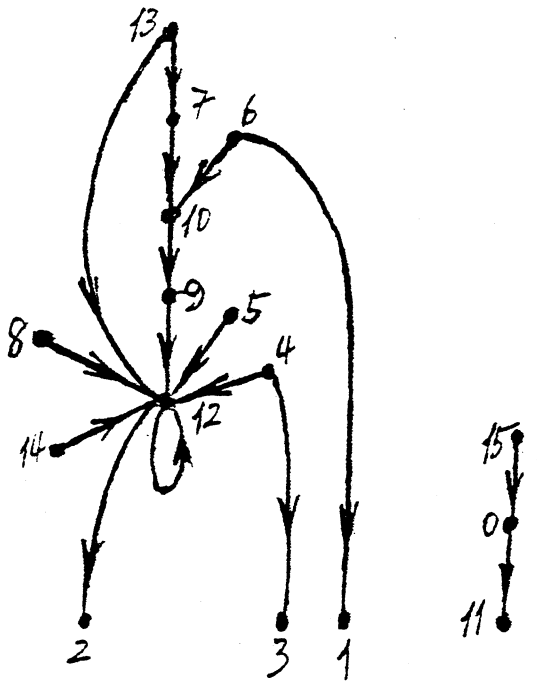


Fig.9.1

$$F(x) = \begin{cases} f_1 = x_1^2 + x_2^2 + x_3^2 + x_2 + p - 1 \\ f_2 = x_1x_2 + x_1x_3 + x_2x_3 + (p-2)x_1 + x_3 \\ f_3 = x_1^2 + x_1x_2 + x_2^2 + (p-1)x_3 + 1 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n$, $p = n = 3$, Newton standard

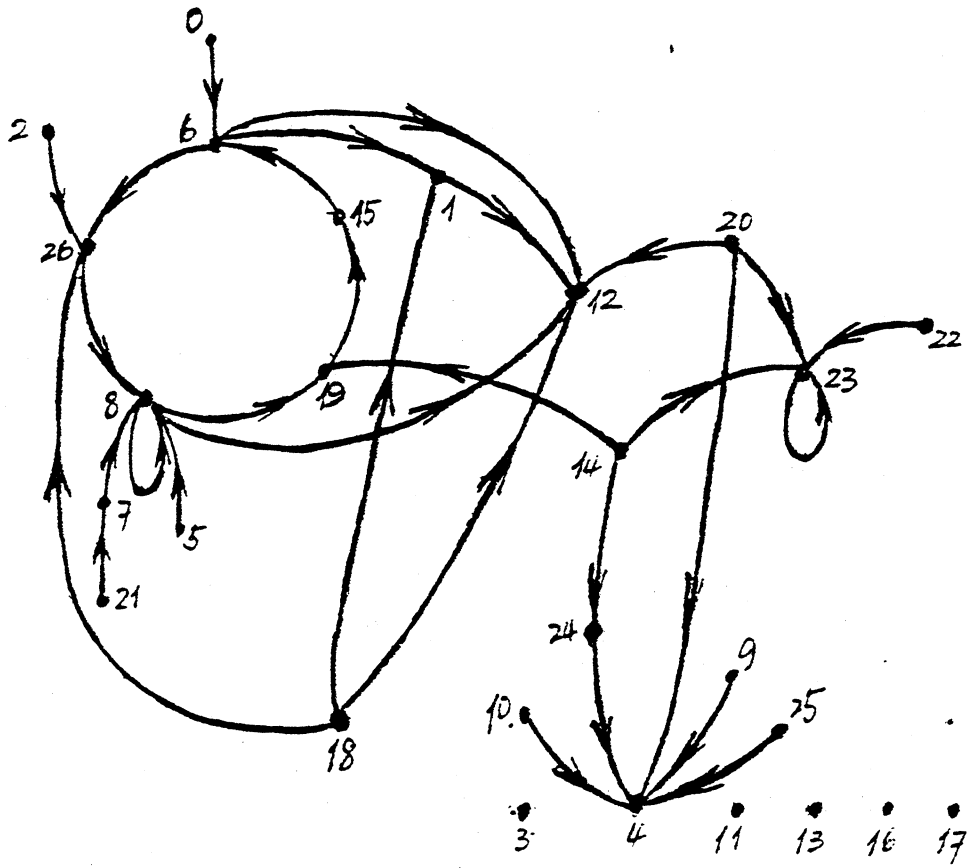
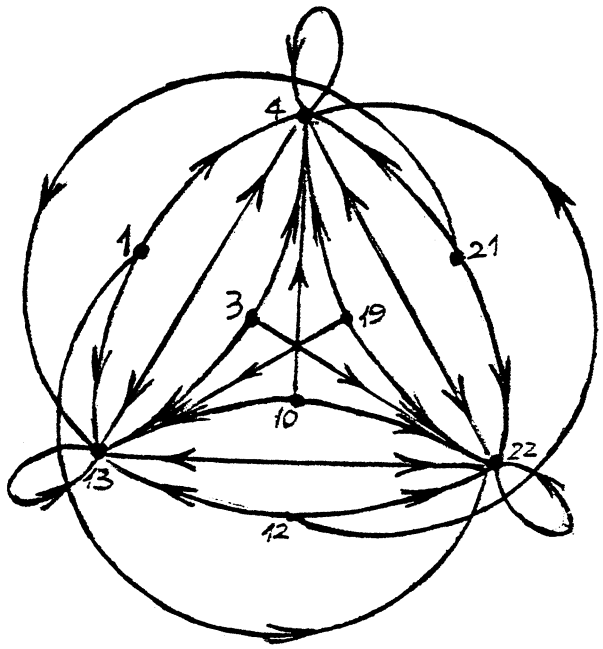


Fig.9.2

$$F(x) = \begin{cases} f_1 = x_2^2 + x_2 + x_3 \\ f_2 = x_2x_3 + p - 1 \\ f_3 = x_2 + x_3^2 + p - 2 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n$, $p = n = 3$

Newton standard



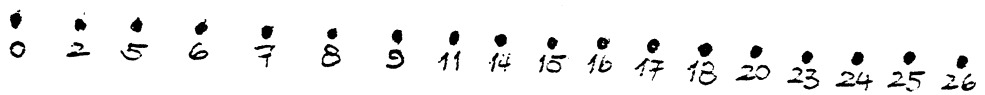


Fig.10.1

$$F(x) = \begin{cases} f_1 = x_1^2 + x_2x_3 + x_3 \\ f_2 = x_2x_3 + x_3 + p - 1 \\ f_3 = f_1 \end{cases}$$

$F(x) : (Z/p)^n \longrightarrow (Z/p)^n$, $p = n = 3$

Newton standard

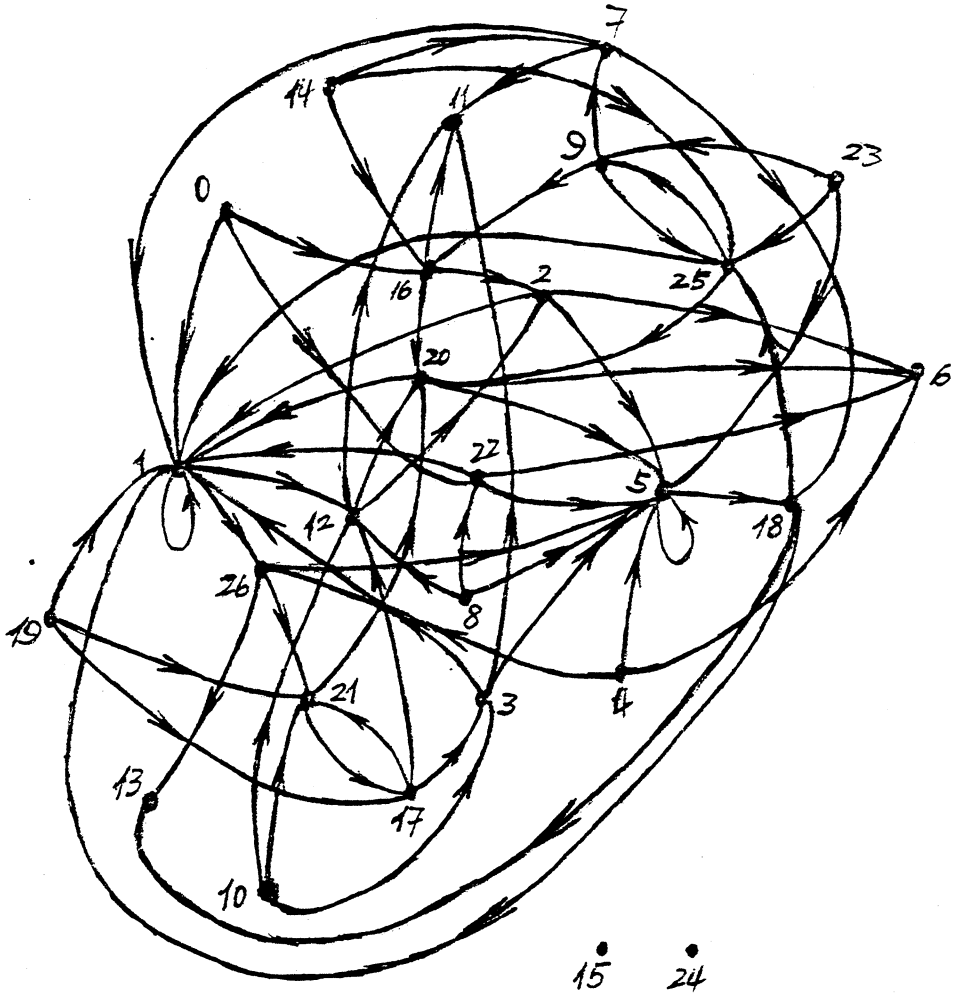


Fig.10.2

$$F(x) = \begin{cases} f_1 = x_2 + 1 \\ f_2 = x_2x_3 + x_3x_4 + x_3 + 1 \\ f_3 = f_2 \\ f_4 = f_1 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n, p = 2, n = 4$

Newton standard

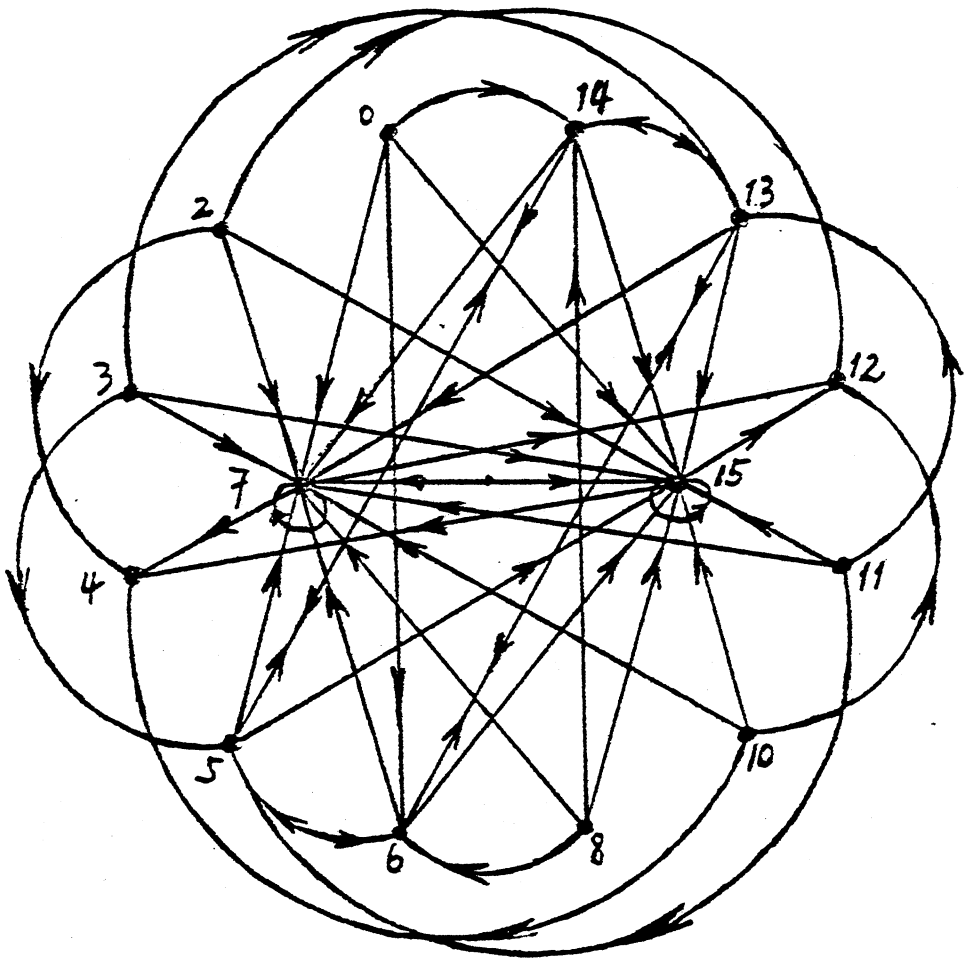


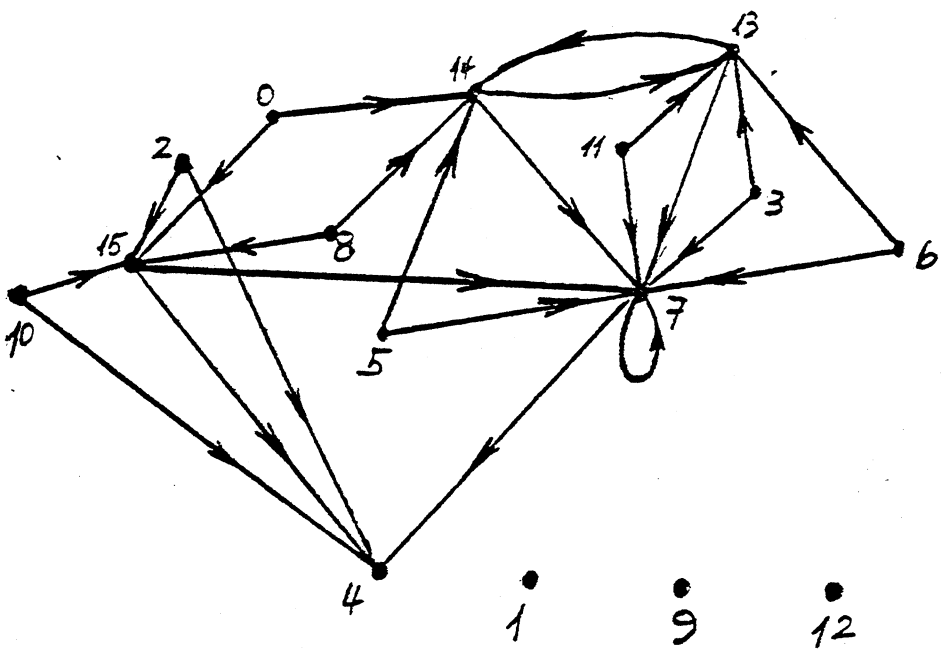
Fig.11.1

1 • • 9

$$F(x) = \begin{cases} f_1 = x_2 + 1 \\ f_2 = x_2x_3 + x_3x_4 + x_3 + 1 \\ f_3 = x_1 + x_2x_4 + x_3 \\ f_4 = f_1 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n, p = 2, n = 4$

Newton stantdard



1 9 12

Fig.11.2

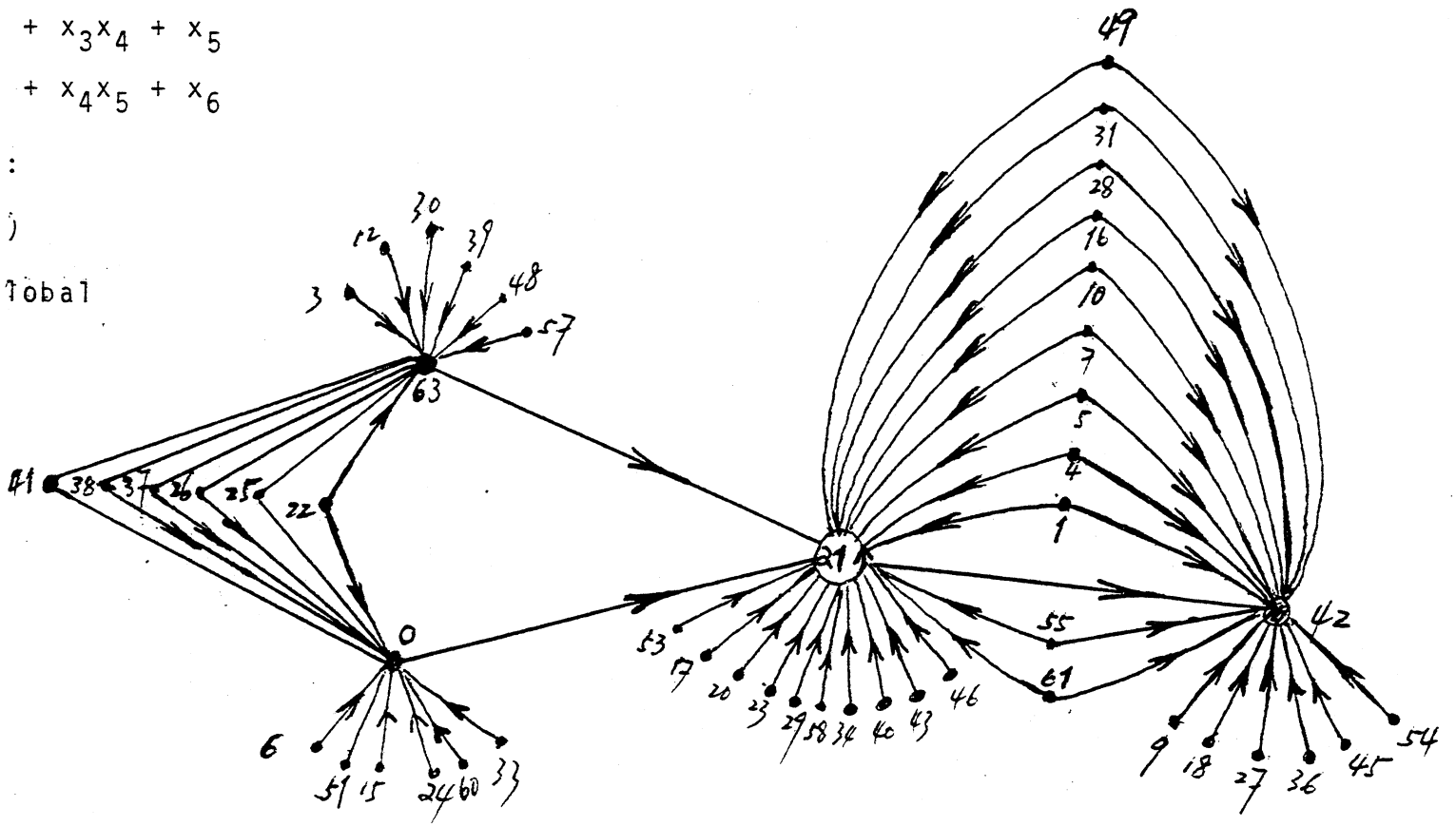
Newton stantdard p = 2, n = 6

$$F=\begin{cases} f_1=x_1x_2 + x_3x_4 + x_5x_6 + x_1 \\ f_2=x_2x_3 + x_4x_5 + x_6x_1 + x_2 \\ \quad . \quad . \quad . \\ f_5=x_5x_6 + x_1x_2 + x_3x_4 + x_5 \\ f_6=x_6x_1 + x_2x_3 + x_4x_5 + x_6 \end{cases}$$

une seule racine :

21 = (0 1 0 1 0 1)

dans le graphe global



2 8 11 13 14 19 32 35 44 47 50 52 56 59 62

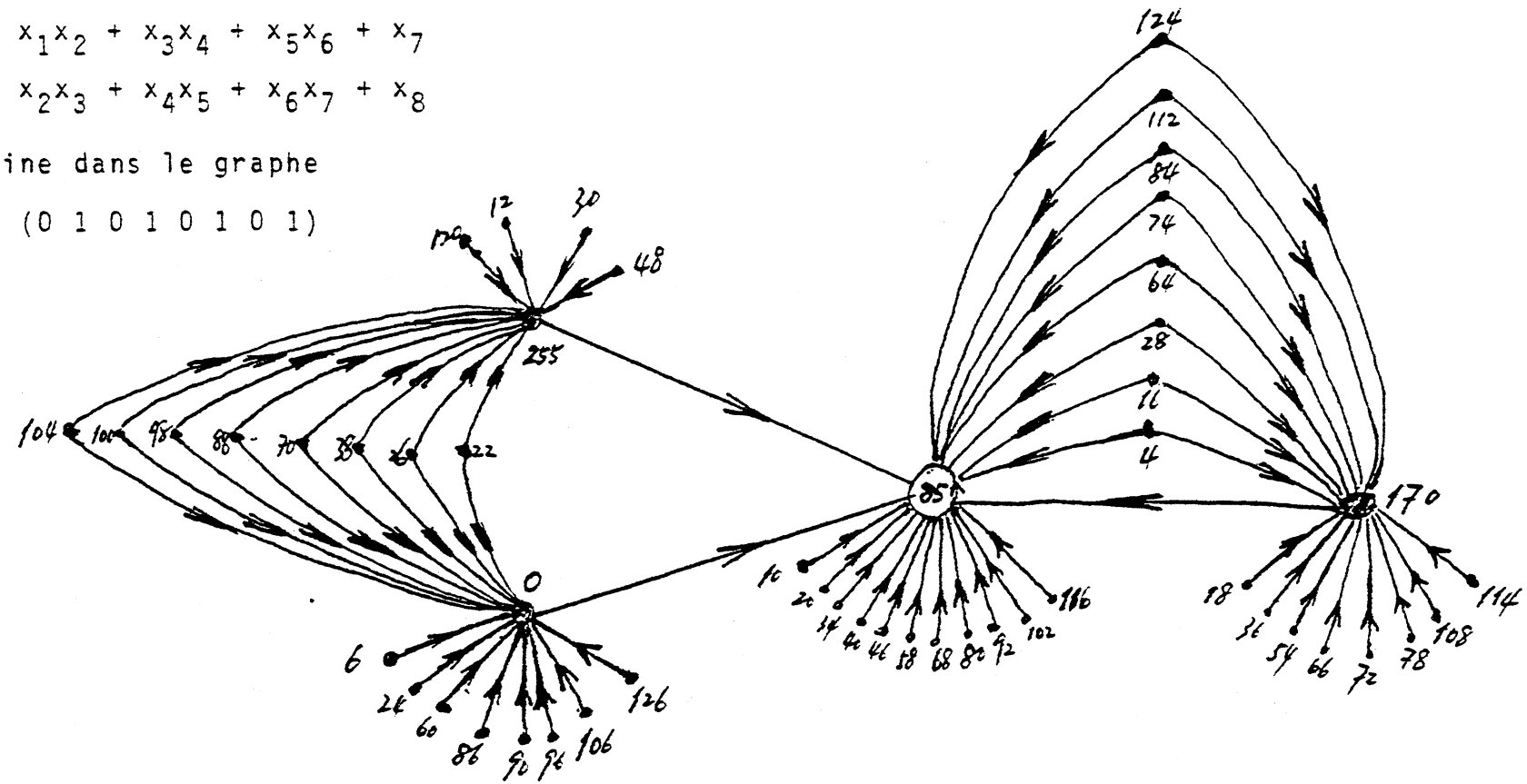
Fig.12.1

Newton standard p = 2, n = 8

$$F=\begin{cases} f_1=x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8 + x_1 \\ f_2=x_2x_3 + x_4x_5 + x_6x_7 + x_8x_1 + x_2 \\ \quad . \quad . \quad . \quad . \quad . \quad . \\ f_7=x_7x_8 + x_1x_2 + x_3x_4 + x_5x_6 + x_7 \\ f_8=x_8x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_8 \end{cases}$$

une seule racine dans le graphe

partiel 85 = (0 1 0 1 0 1 0 1)



2 8 14 32 42 44 50 52 56 62 76 82 94 110 118 122

Fig .12.2

Newton standard $\quad p = 2, \quad n = 20$

$$F = \begin{cases} f_1 = x_1x_2 + x_3x_4 + \cdots + x_{19}x_{20} + x_1 \\ f_2 = x_2x_3 + x_4x_5 + \cdots + x_{20}x_1 + x_2 + 1 \\ \quad \cdots \\ f_{19} = x_{19}x_{20} + x_1x_2 + \cdots + x_{17}x_{18} + x_{19} \\ f_{20} = x_{20}x_1 + x_2x_3 + \cdots + x_{18}x_{19} + x_{20} + 1 \end{cases}$$

une racine dans le graphe partiel

a = (0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1)

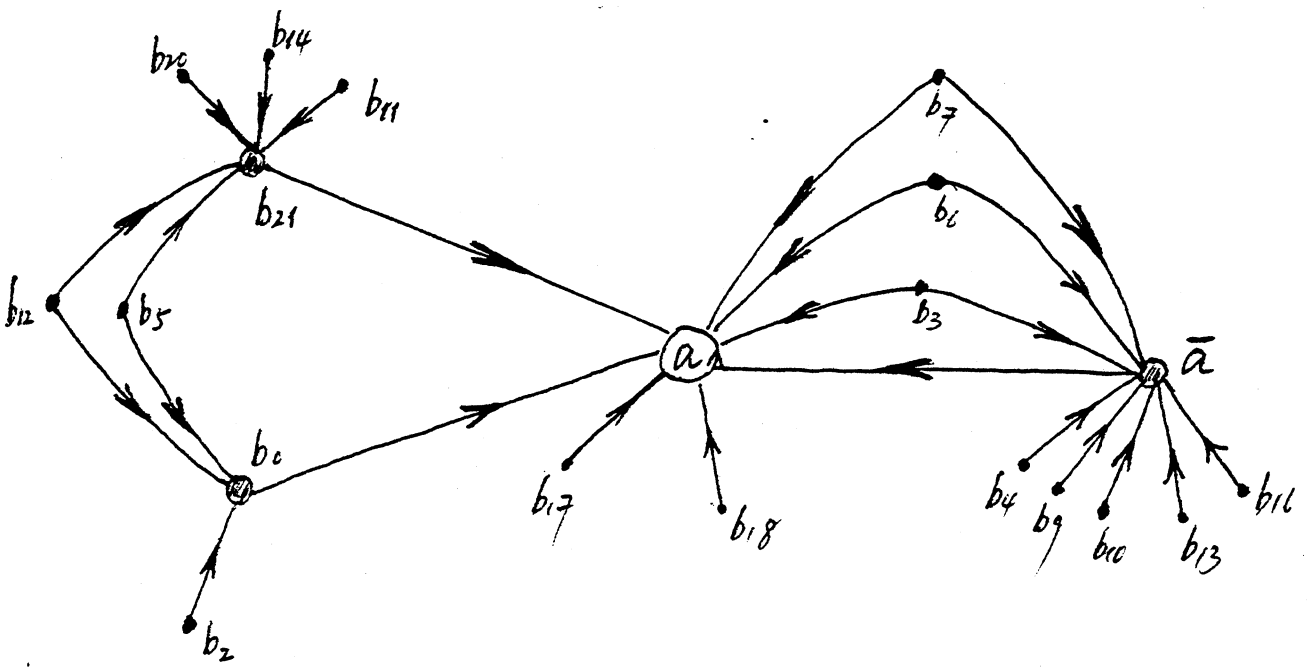


Fig.12.3

b_1 b_8 b_{15} b_{19}

Newton standard , p = 2, n = 20

$$\begin{cases} f_1 = x_1x_2 + \ldots + x_5x_6 + \ldots + x_{19}x_{20} + x_1 + 1 \\ f_2 = x_2x_3 + \ldots + x_6x_7 + \ldots + x_{20}x_1 + x_2 + 1 \\ f_3 = x_3x_4 + \ldots + x_7x_8 + \ldots + x_1x_2 + x_3 + 1 \\ \quad \ldots \\ f_{19} = x_{19}x_{20} + x_1x_2 + \ldots + x_{16}x_{17} + x_{18} + 1 \\ f_{20} = x_{20}x_1 + x_2x_3 + \ldots + x_{18}x_{19} + x_{20} + 1 \end{cases}$$

Dans le graphe partiel on a trouvé deux racines suivantes

$a_1 = (1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1)$

$a_2 = (0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1)$

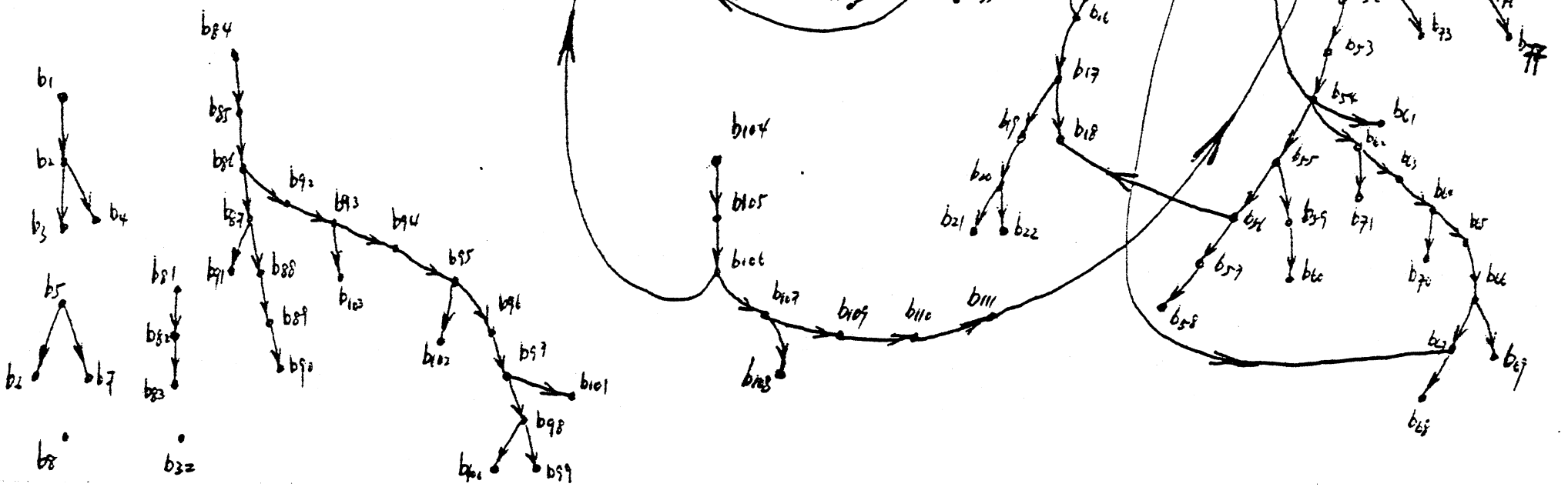


Fig.13.1

Newton standard $p = 2$, $n = 20$.

$$F(X)=\begin{cases} f_1 = x_1x_{11} + x_2x_{13} + \cdots + x_5x_{19} + x_{19} \\ f_2 = x_2x_{12} + x_3x_{14} + \cdots + x_6x_{20} + x_2 \\ \quad \cdots \\ f_{10} = x_{10}x_{20} + x_{11}x_{12} + \cdots + x_{14}x_8 + x_{10} \\ \quad \cdots \\ f_{19} = x_{19}x_9 + x_{20}x_{11} + \cdots + x_3x_{17} + x_1 \\ f_{20} = x_{20}x_{10} + x_1x_{12} + \cdots + x_4x_{18} + x_{20} \end{cases}$$

deux racines a_1 et a_2 dans le graphe partiel

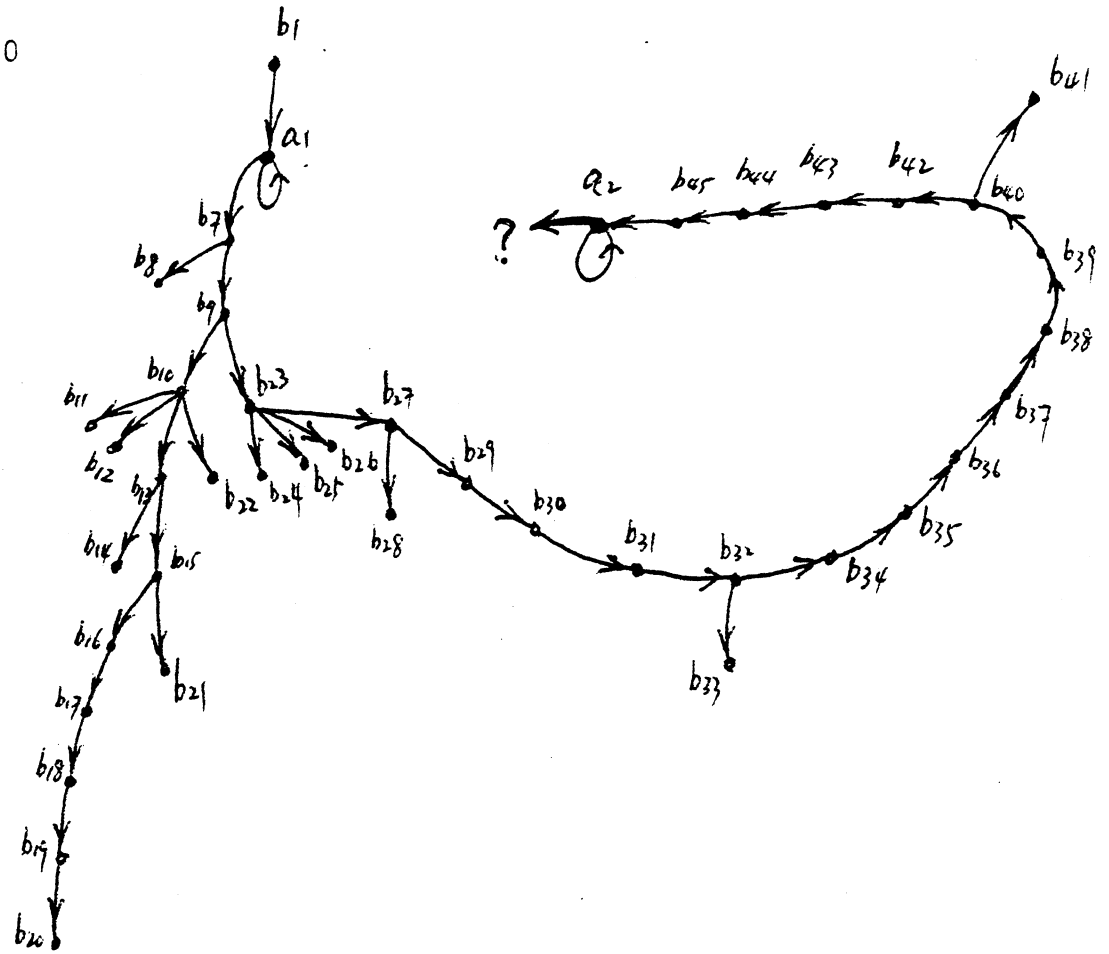


Fig.13.2

même table que celle
de fig 1
Le mode parallèle
p = 2, n = 5
($x^{r+1}=H(x)=x^r e\ F(x^r)$)
(Newton simplifié
avec A = I)
(pas de racine)

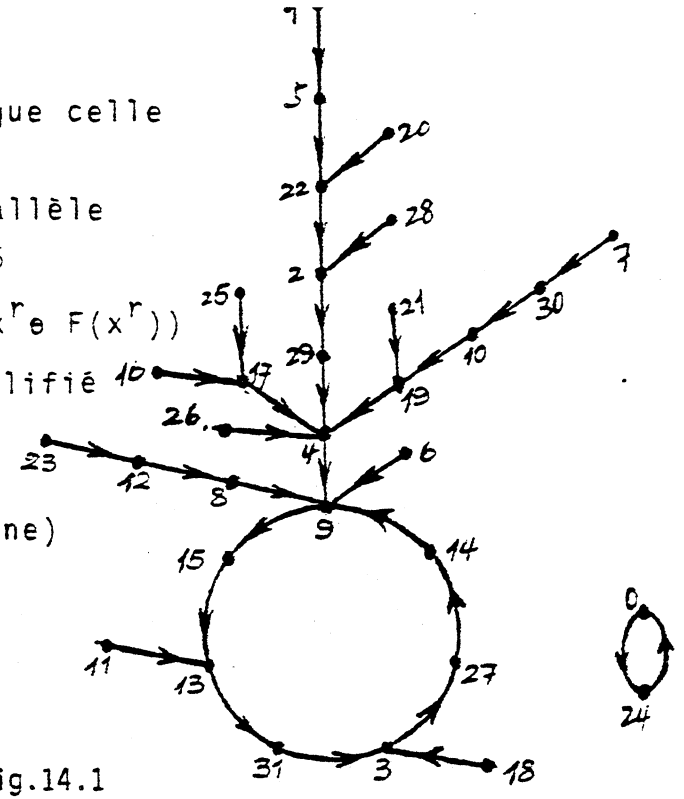


Fig.14.1

même indication pour F(x)
Gauss Seidel,p=2, n=5
(mode série) sur H
associé à F_0(pas de
racine)

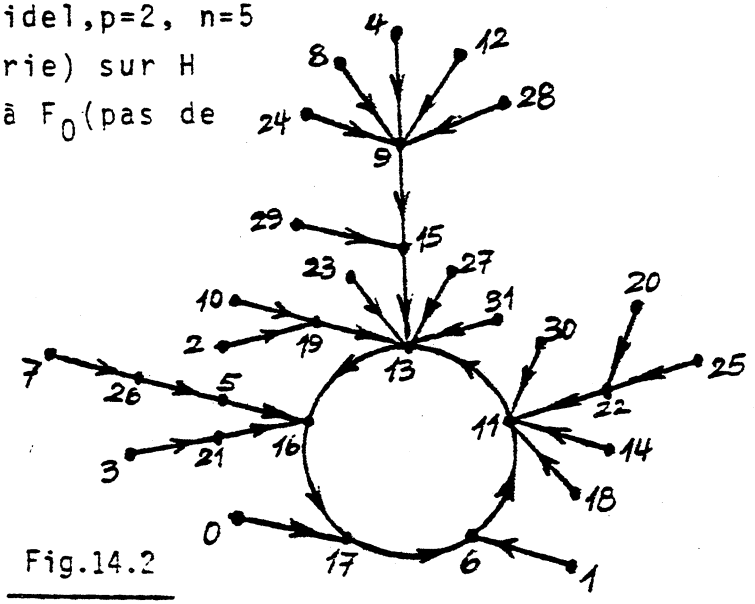


Fig.14.2

Dans la table de fig 1
F_1 a été àbtenu en imposant
la racine 2=(0 0 0 1 0)
F(18),F(10),F(6),F(0),F(3)
remplacées par (1 1 0 0 0),
(0 1 1 0 0),(0 0 1 0 1)
(1 0 0 1 0),(0 0 0 0 1),
alors,

$$H'(2)=\begin{pmatrix}0&0&0&1&0\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&0\\0&0&1&0&0\end{pmatrix}$$

2 est attractif dans son
voisinage immédiat
$V_x(2)=\{18,10,6,0,3,2\}$

Le mode parallèle,p=2,n=5

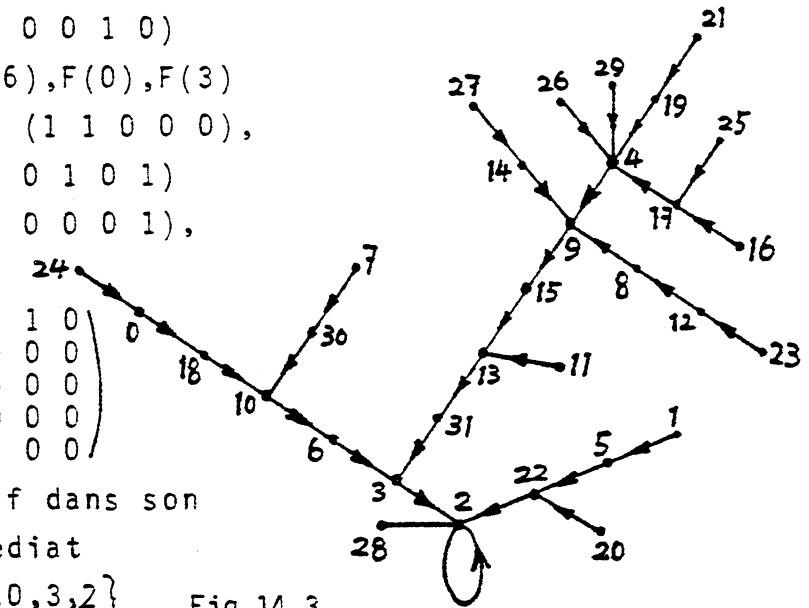


Fig.14.3

même indication que fig 14-3
Gauss Seidel sur H associé à
F_1,p = 2,n = 5

$$G'(2)=\begin{pmatrix}0&0&0&1&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&1&0\\0&0&0&1&0\end{pmatrix}$$

2 n'est pas attractif, mais
globalement le graphe est
encore plus contractant que
fig 14-3.

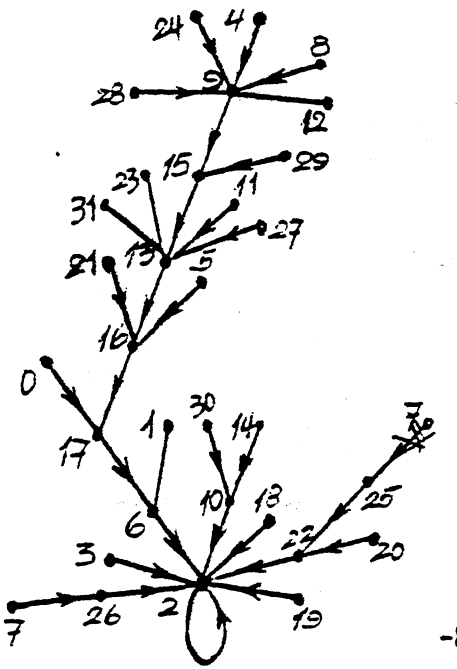


Fig.14.4

La table de F(x) se trouve dans fig 2

le mode parallèle sur H associé à F_0

p = 2, n = 5

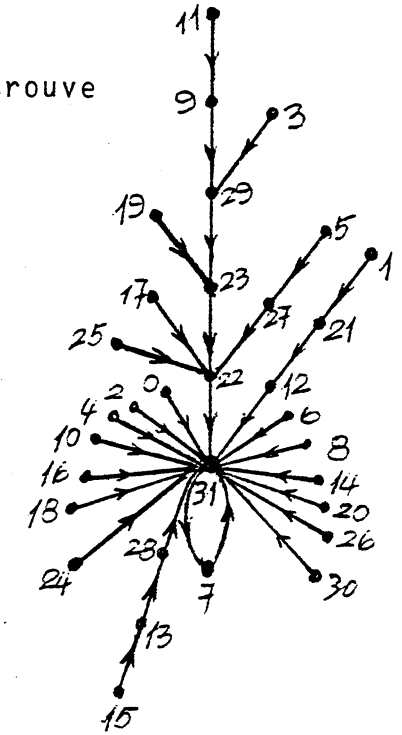


Fig.15.1

même indication que fig 15_1

Gauss Seidel sur H associé à F_0

p = 2, n = 5

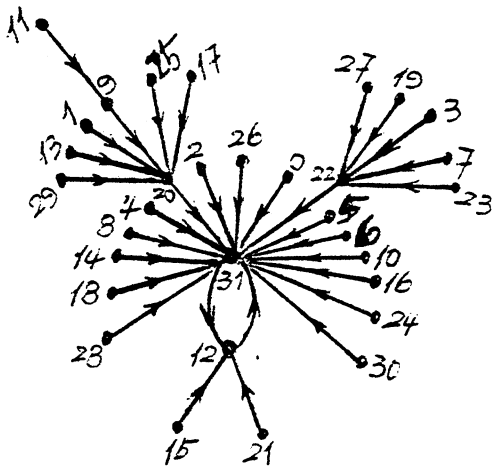


Fig.15.2

même table de F(x) que celle de fig 2

F_2 a été obtenu en imposant la racine 1 = (0 0 0 0 1) et la racine 15=(0 1 1 1 1)

le mode parallèle sur H associé à F_2

p = 2, n = 5

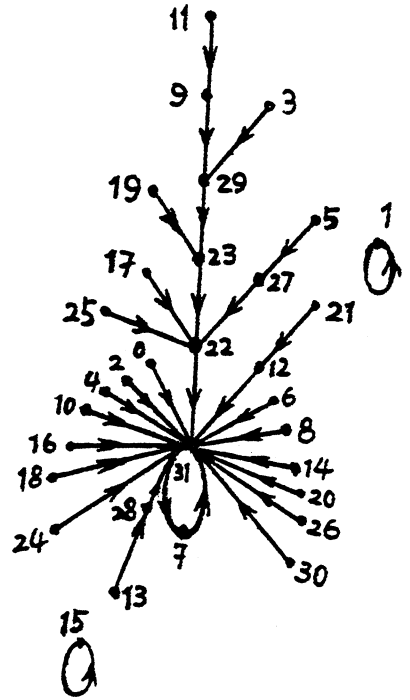


Fig.15.3

même indication que fig 15_3

Gauss Seidel sur H associé à F_2

p = 2, n = 5

(31 est le 1er voisin de la racine 15)

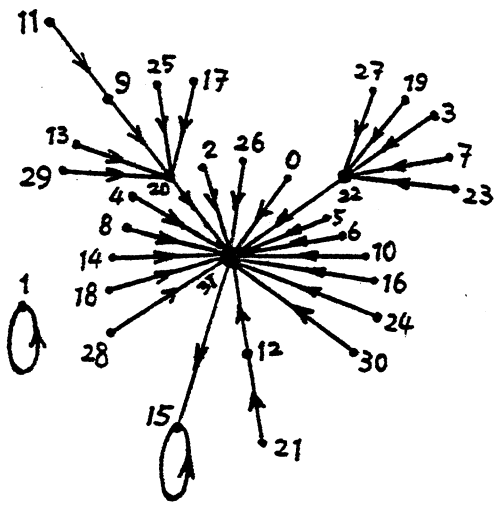


Fig.15.4

même table de F(x) que celle de fig 1; même indication pour F_3

Le mode parallèle, p=2, n=5 sur H associé à F_3

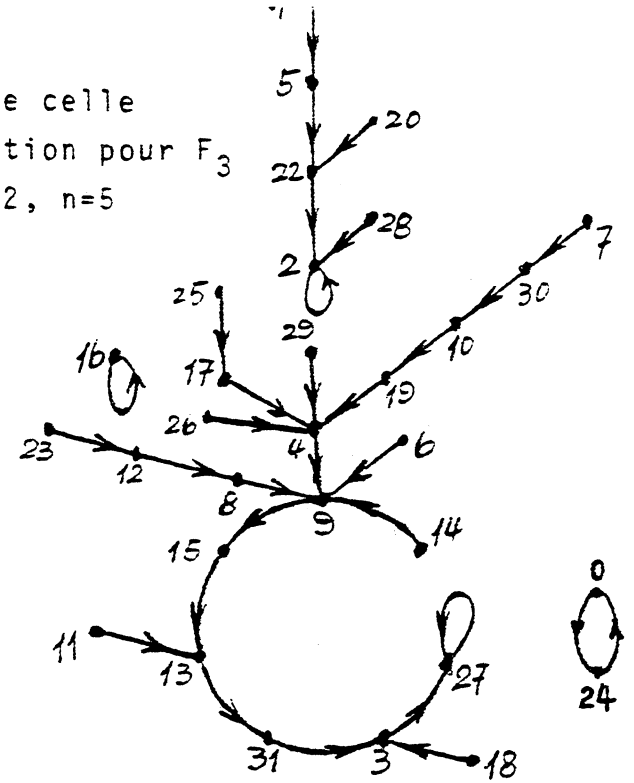


Fig.16.1

même indicatiion pour F_3

Gauss Seidel, p=2, n=5, sur H associé à F_3

18 est le 1er voisin de 2;

0 est le 1er voisin de 16

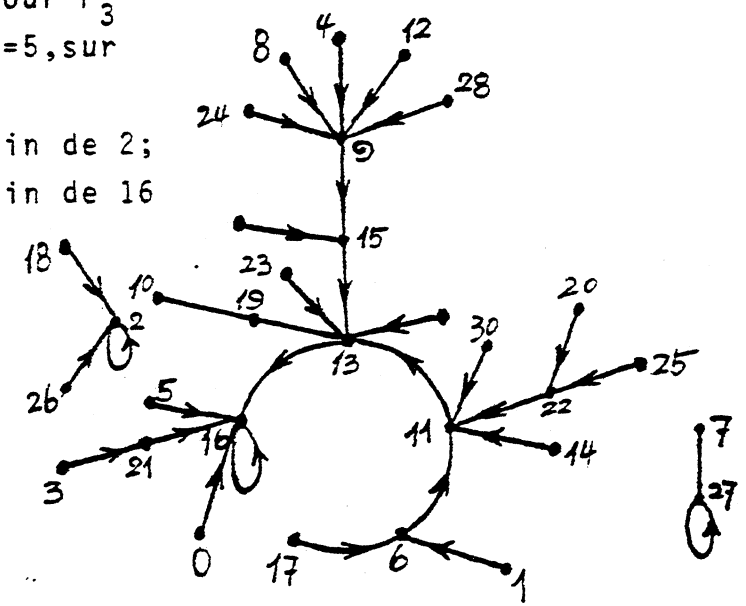


Fig.16.2

même indication que fig 16-1

Le mode parallèle, p=2, n=5 sur H associé à F_1

F_1 a été obtenu en imposant la racine 2(0 0 0 1 0)

F(18), F(10), F(6), F(0), F(3) remplacées par (1 0 0 0 0), (0 1 0 0 0), (0 0 1 0 0), (0 0 0 1 0), (0 0 0 0 1)

$F'(2) = I$

$V_x(2) = \{18, 10, 6, 0, 3, 2\}$

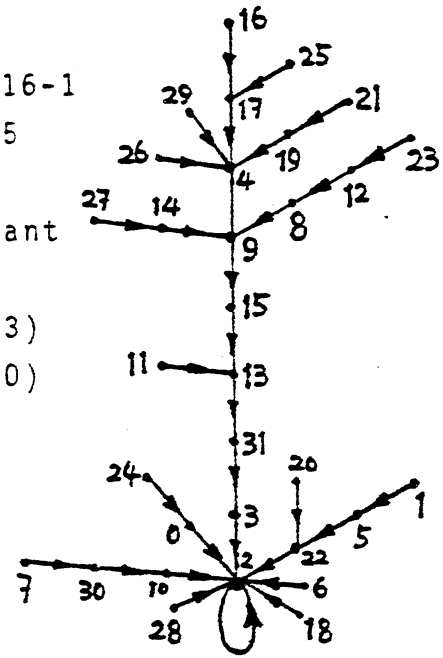


Fig.16.3

même indication que fig 16-3

Gauss Seidel, p=2, n=5

F(18), F(10), F(6), F(0), F(3) remplacées par (1 0 0 0 0), (* 1 0 0 0), (* * 1 0 0), (* * * 1 0), (* * * * 1)

* peut être n'importe quel élement de Z/2.

$$F'(2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ * & 1 & 0 & 0 & 0 \\ * & * & 1 & 0 & 0 \\ * & * & * & 1 & 0 \\ * & * & * & * & 1 \end{pmatrix}$$

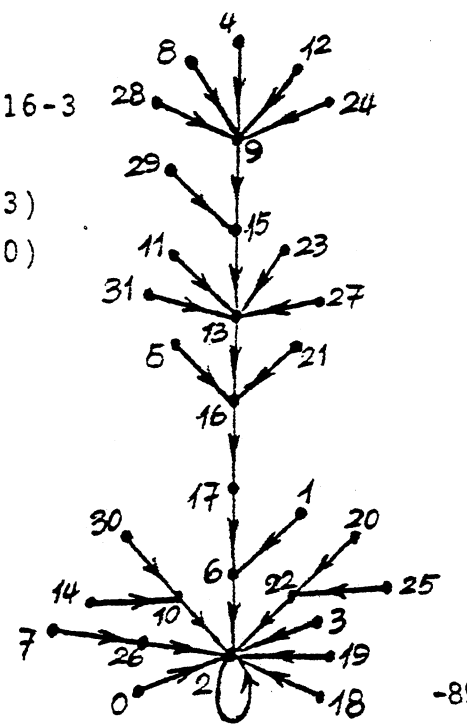


Fig.16.4

	x				F(x)			
0	0	0	0	0	1	1	1	1
1	0	0	0	1	0	1	1	1
2	0	0	1	0	0	1	0	1
3	0	0	1	1	0	0	0	0
4	0	1	0	0	0	1	1	0
5	0	1	0	1	1	0	0	1
6	0	1	1	0	1	0	1	1
7	0	1	1	1	0	1	0	0
8	1	0	0	0	0	1	0	1
9	1	0	0	1	1	0	1	0
10	1	0	1	0	0	1	0	1
11	1	0	1	1	1	0	1	1
12	1	1	0	0	0	1	1	0
13	1	1	0	1	1	1	1	0
14	1	1	1	0	0	1	0	0
15	1	1	1	1	1	0	0	0

$$F'(3)=\begin{pmatrix}1&0&0&0\\0&1&1&1\\1&0&1&0\\1&0&1&1\end{pmatrix}$$

Gauss Seidel, p=2, n=4
11 et 7 sont le 1er et 2ème voisins resp. de la racine 3

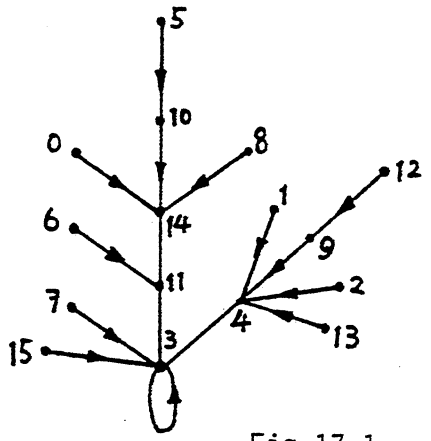


Fig.17.1

Vérifications de la proposition 2 de II 3

Gauss Seisel p=n=3
même table que celle de fig 4
26 est le 1er voisin de 17

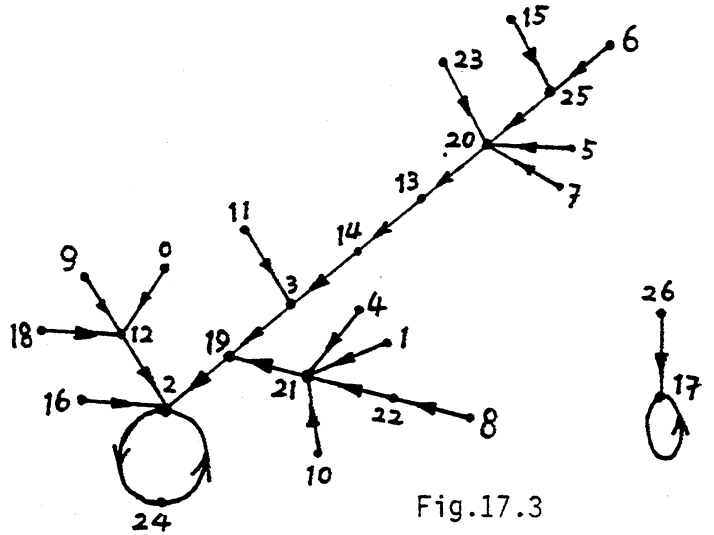


Fig.17.3

	x				F(x)			
0	0	0	0	0	1	0	1	0
1	0	0	0	1	1	0	0	0
2	0	0	1	0	0	0	0	1
3	0	0	1	1	0	0	0	0
4	0	1	0	0	1	0	0	0
5	0	1	0	1	0	1	1	0
6	0	1	1	0	1	0	1	0
7	0	1	1	1	1	0	1	1
8	1	0	0	0	1	0	0	1
9	1	0	0	1	1	1	1	1
10	1	0	1	0	1	0	1	1
11	1	0	1	1	1	1	0	1
12	1	1	0	0	1	0	1	0
13	1	1	0	1	0	1	0	0
14	1	1	1	0	1	0	0	0
15	1	1	1	1	1	0	1	1

$$F'(3)=\begin{pmatrix}1&1&1&0\\1&0&0&0\\0&1&0&0\\1&1&0&1\end{pmatrix}$$

Gauss Seidel, p=2, n=4
11 et 2 sont le 1er et le 2ème voisin de la racine 3

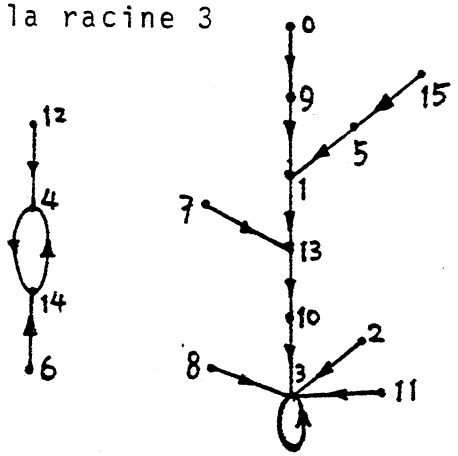


Fig.17.2

Dans la table de fig 4
F_2 a été obtenu en imposant la racine 6=(0 2 0)
Gauss Seidel, p=n=3
24 est le 1er voisin à gauch de la racine 6

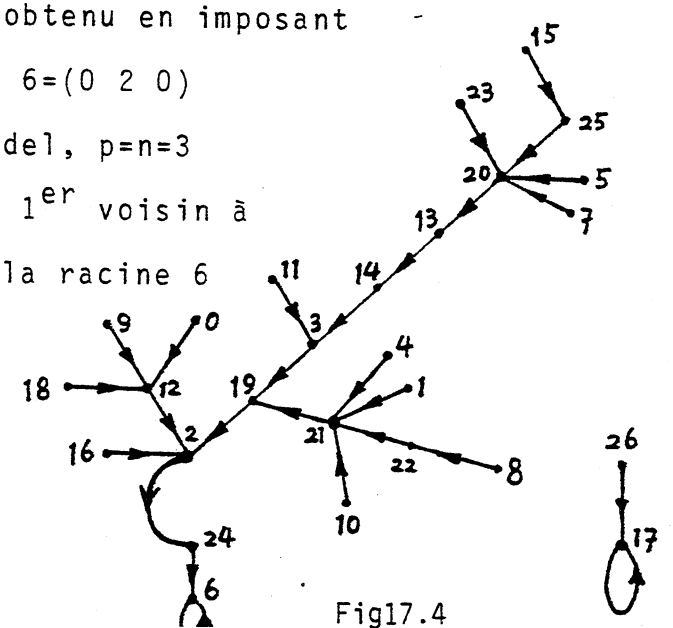


Fig17.4

même table que celle de fig 5

Gauss Seidel sur H associé à F_1

p = 5, n = 2

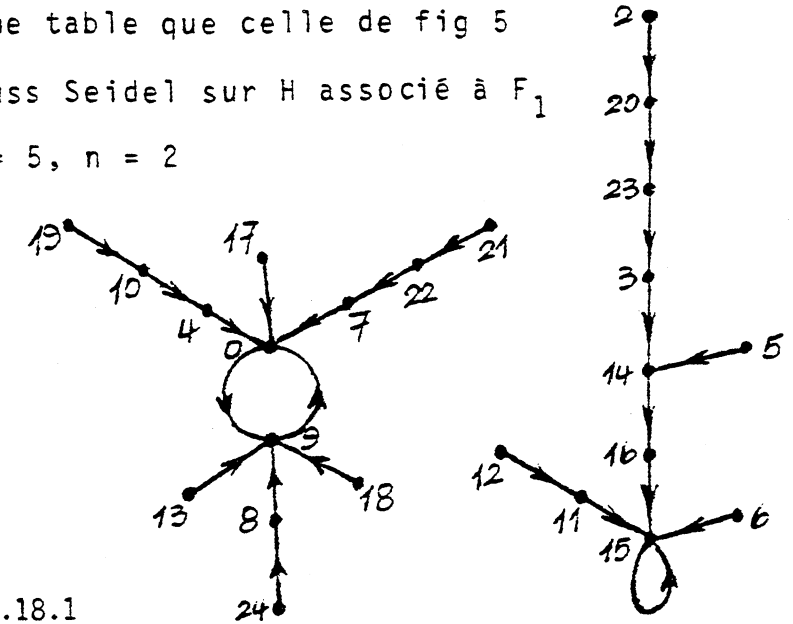


Fig.18.1

Dans la table de fig 5

F_2 a été obtenu en imposant

la racine 22=(4 2)

Gauss Seidel sur H associé

à F

p = 5,n = 2

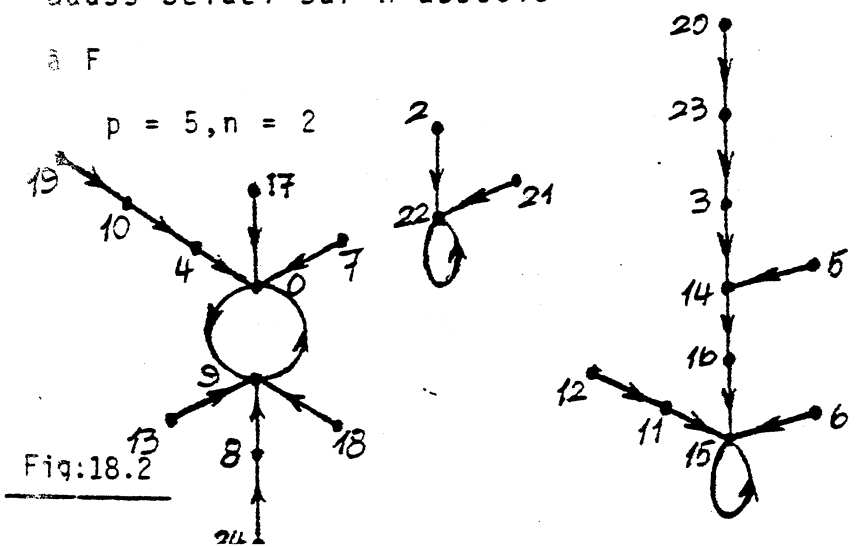


Fig:18.2

$$F(X)=\begin{cases} f_1=x_1 + x_2 + x_4 \\ f_2=x_1 + x_2 + x_3+x_4+ x_2x_3+ 1 \\ f_3=x_2 \\ f_4=x_1x_4 \end{cases}$$

le mode parallèle, p=2, n=4

$x^{r+1} = H(x) = x^r e F(x^r)$

la racine a=(0 0 1 0)=2

$$F'(a)= \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

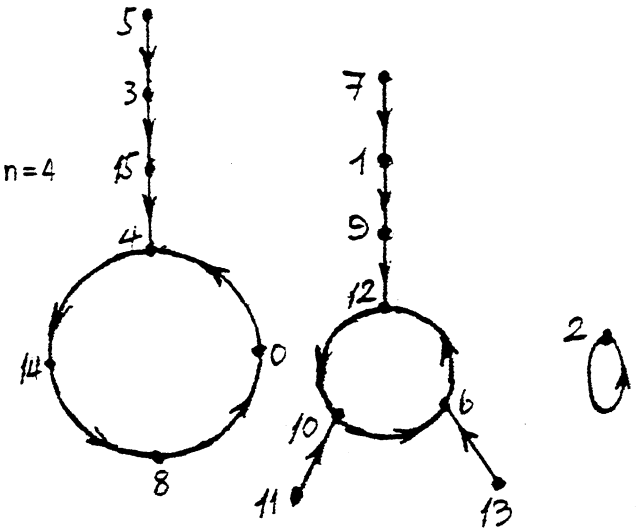


Fig.18.3

$$F(X)=\begin{cases} f_1=x_1+x_2+x_4 \\ f_2=x_1+x_2+x_3+x_4+x_2x_3+1 \\ f_3=x_2 \\ f_4=x_1x_4 \end{cases}$$

Gauss Se idel, p=2, n=4

La racine a=2 est attractive

dans son voisinage immédial

$V_x(a)= \{10, 6, 0, 3, 2\}$

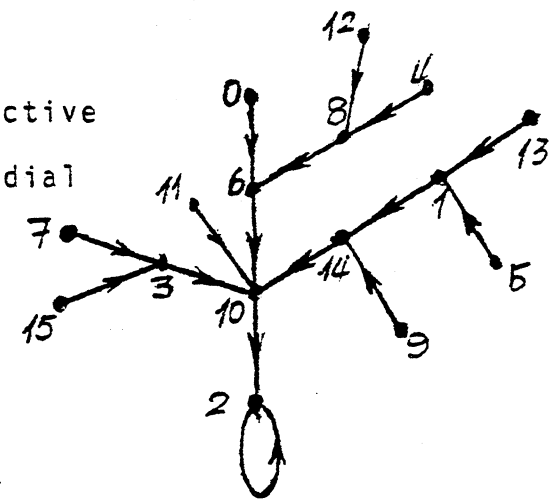


Fig.18.4

$$F(x) = \begin{cases} f_1 = x_1 + 1 \\ f_2 = x_1 + x_1 x_2 + 1 \\ f_3 = x_1 x_2 + x_3 \\ f_4 = x_1 x_3 + x_2 x_3 + x_4 \end{cases}$$

$$F'_d(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$G'_d(a) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$a = 8 = (1,0,0,0)$

$p = 2$, $n = 4$

racine de F.

Le mode parallèle

$$x^{r+1} = H = x^r \theta F(x^r)$$

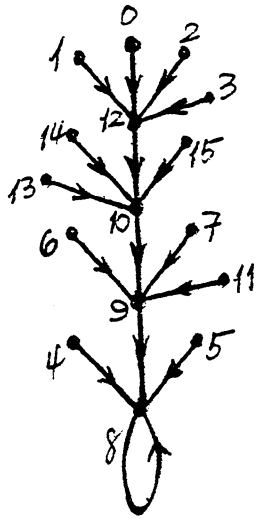


Fig. 19.1

Gauss-Seidel

sur H associé à F

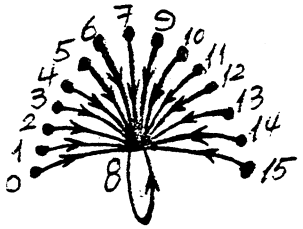


Fig.19.2

$$F(x) = \begin{cases} f_1 = x_1 + 1 \\ f_2 = 2x_1 + x_2 + 2x_3 + x_3^2 \\ f_3 = x_1 x_2 + x_3 + 2 \end{cases}$$

$p = n = 3$

$$F'_d(a) = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 2 & 1 \end{pmatrix}$$

$$G'_d(a) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$a = 24 = (2,2,0)$

racine de F

Le mode parallèle

$$x^{r+1} = H(x^r) = X^r \theta F(x^r)$$

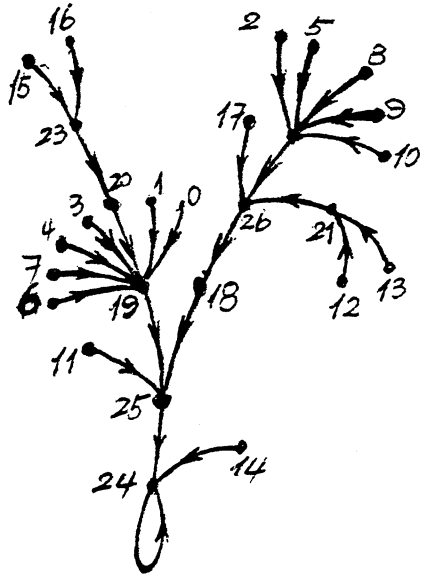


Fig.19.3

Gauss-Seidel

sur H associé à F

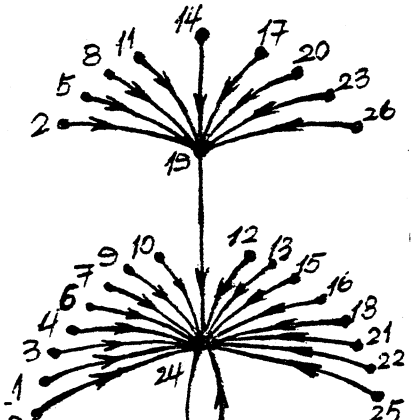


Fig. 19.4

$$F(x) = \begin{cases} f_1 = x_1 + 2 \\ f_2 = x_1 x_2 + x_1 + 2 \\ f_3 = x_1 x_2 + x_3 \end{cases}$$

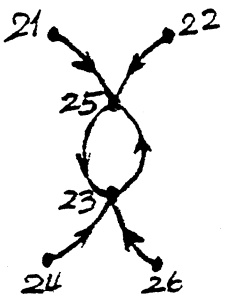
$p=n=3$

$$F'_d(a) = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} ; \quad F'_d(a) = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

$$G'_d(a) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} ; \quad G'_d(a) = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 2 & 2 & 0 \end{pmatrix}$$

$a = 14 = (1,1,2)$

$a = 18 = (2,0,0)$



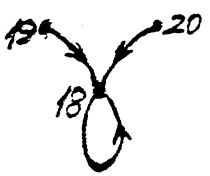
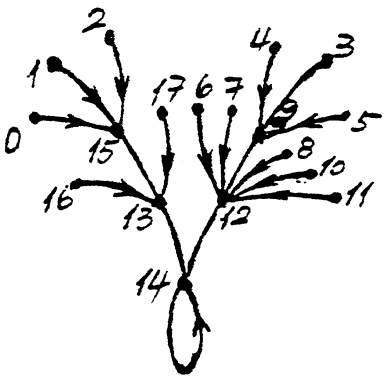
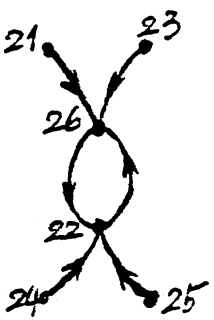


Fig.19.5

Le mode parallèle

$x^{r+1} = H = x^r \theta F(x^r)$





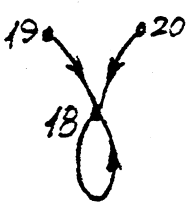
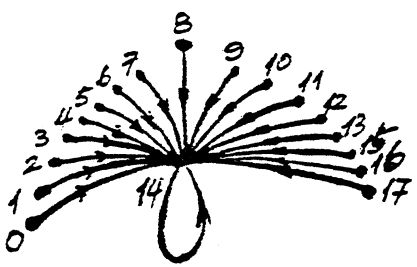


Fig.19.6



Gauss-Seidel

sur H associé à F

$$F(x)=\begin{cases} f_1 = x_1^2+x_2x_3 \\ f_2 = x_2^2+x_1x_3 \\ f_3 = x_3^2+x_1x_2 \end{cases}$$

$$F_d'(x)=\begin{pmatrix} 2x_1+1 & x_3 & x_2 \\ x_3 & 2x_2+1 & x_1 \\ x & x & 2x+1 \end{pmatrix}$$

$$F_d'(0)=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Gauss Seidel, p=n=3

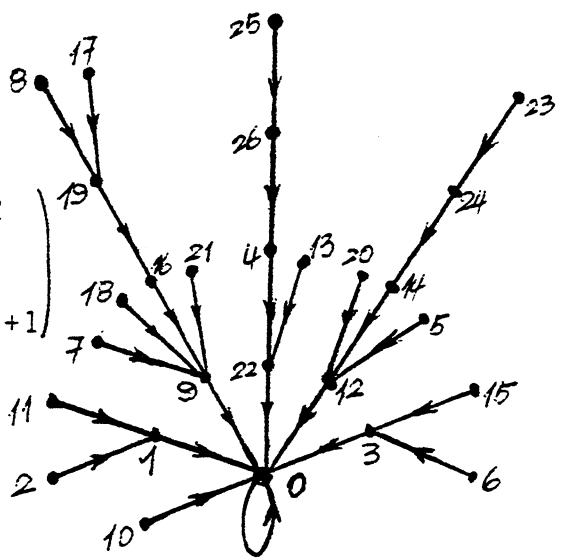


Fig.20.1

Au dessus,en effectuant les permutations de composantes de F(x),on obtient les figures ci- dessous (fig20-2～fig20-4)

$$F(x)=\begin{cases} f_1 = x_1^2+x_2x_3 \\ f_2 = x_3^2+x_1x_2 \\ f_3 = x_2^2+x_1x_3 \end{cases}$$

$$F_d'(0)=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Gauss Seidel,p=n=3

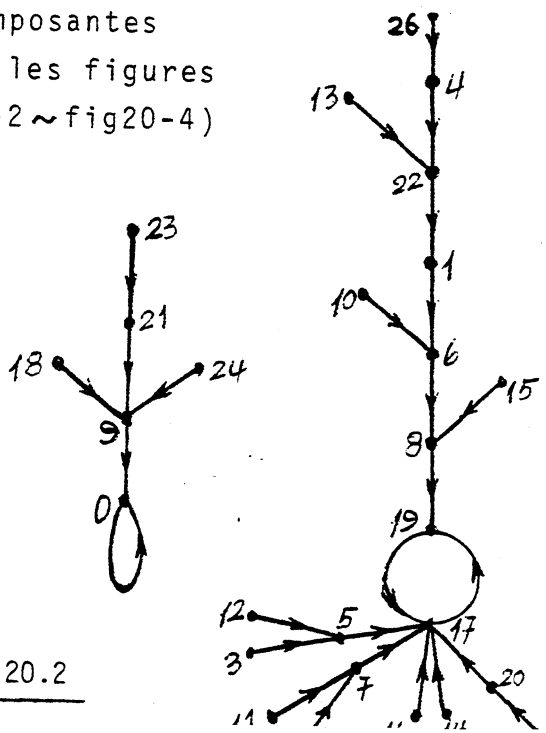


Fig.20.2

$$F(x)=\begin{cases} f_1 = x_3^2+x_1x_2 \\ f_2 = x_2^2+x_1x_3 \\ f_3 = x_1^2+x_2x_3 \end{cases}$$

$$F_d'(0)=\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Gauss Seidel, p=n=3

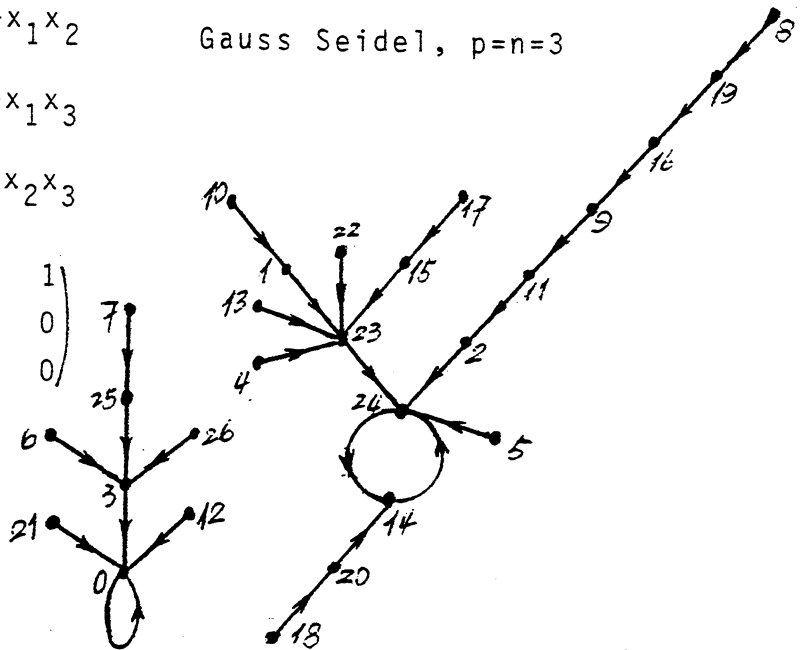


Fig.20.3

$$F(x)=\begin{cases} f_1 = x_3^2+x_1x_2 \\ f_2 = x_1^2+x_2x_3 \\ f_3 = x_2^2+x_1x_3 \end{cases}$$

$$F_d'(0)=\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Gauss Seidel, p=n=3

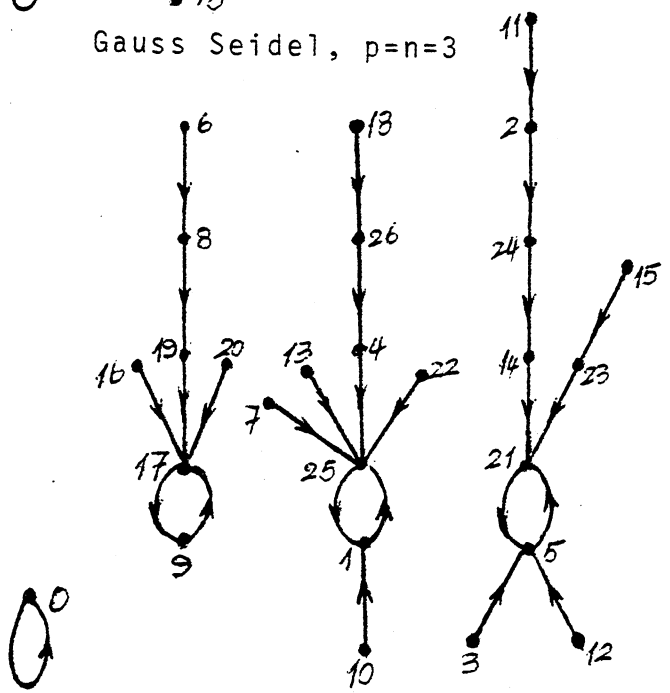


Fig.20.4

$$F(x) = \begin{cases} f_1=(x_2+x_3)^2 \\ f_2=(x_1+x_3)^2 \\ f_3=(x_1+x_2)^2 \end{cases}$$

p=n=3

$$F'(x) = \begin{pmatrix} 0 & 2(x_2+x_3)+1 & 2(x_2+x_3)+1 \\ 2(x_1+x_3)+1 & 0 & 2(x_1+x_3)+1 \\ 2(x_1+x_2)+1 & 2(x_1+x_2)+1 & 0 \end{pmatrix}$$

$$F'_d(a)=F'_d(0)= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Gauss-Seidel sur H associé à F

a=0=(0,0,0), racine de F

$V_d(0) = \{9,3,1\}$

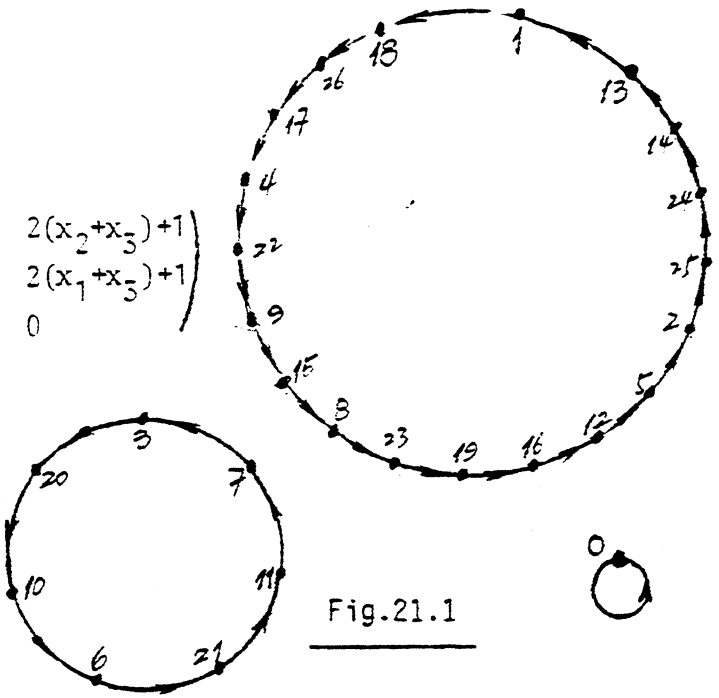


Fig.21.1

$$F(x) = \begin{cases} f_1=x_2^2+x_3^2 \\ f_2=x_1^2+x_3^2 \\ f_3=x_1^2+x_2^2 \end{cases}$$

p=n=3

$$F'_d(x) = \begin{pmatrix} 0 & 2x_2+1 & 2x_3+1 \\ 2x_1+1 & 0 & 2x_3+1 \\ 3x_1+1 & 2x_2+1 & 0 \end{pmatrix}$$

a=0=(0,0,0)

racine de F

$$F'_d(a)=F'_d(0)= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

(même matrice que celle de Fig.21.1)

$V_d(0)=\{9,3,1\}$; même graphe que Fig. 21.1.

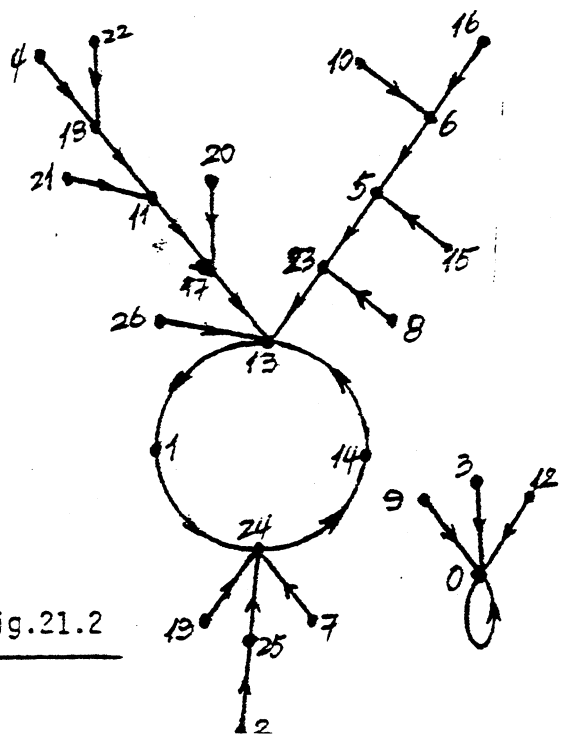


Fig.21.2

$$F(x) = \begin{cases} f_1=(x_1+x_3)^2 \\ f_2=(x_1+x_2)^2 \\ f_3=(x_2+x_3)^2 \end{cases}$$

$$F'_d(0) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Gauss-Seidel

sur H associé à F

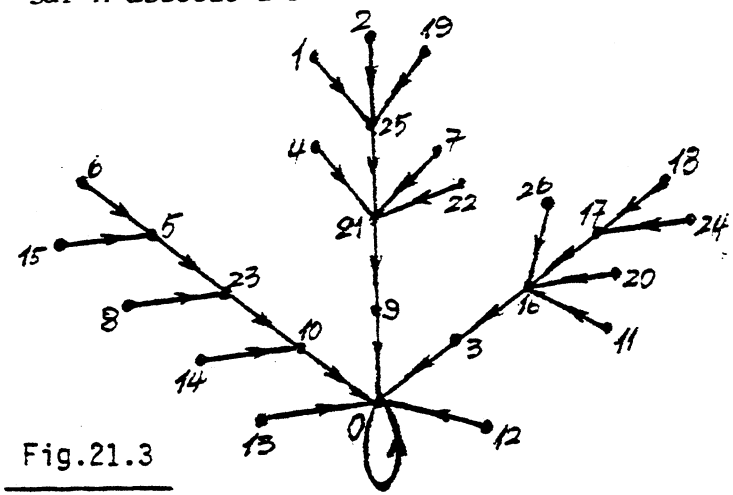


Fig.21.3

Au-dessus, en effectuant les permutations de composantes de F(x), on obtient les figures ci-dessous (Fig. 21.2 fig. 21.3)

$$F(x) = \begin{cases} f_1=(x_1+x_3)^2 \\ f_2=(x_2+x_3)^2 \\ f_3=(x_1+x_2)^2 \end{cases}$$

$$F'_d(0) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Gauss-Seidel sur H associé à F.

$p=2$, $F(x)=(f_1(x)\dots f_2(x)\dots f_n(x))$

$(Z/2)^n \xrightarrow{\quad} (Z/2)^n$

$$f_i(x) = \sum_{j=i}^{n} x_j + \sum_{j=1}^{i} x_i x_j + C_i \; : \; (Z/2)^n \longrightarrow (Z/2)$$

d'où $C_i = \begin{cases} 1 & \text{si } i \text{ impair} \\ 0 & \text{sinon} \end{cases}$

Gauss-Seidel sur H associé à F

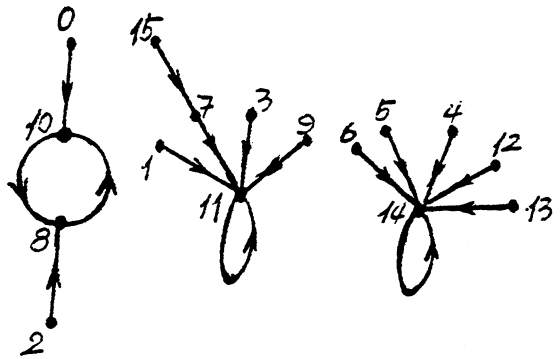


Fig.22.1

$n=5$

$a_{\quad}=23=(1,0,1,1,1)$, $a_{\quad}=29=(1,1,1,0,1)$; racines de F

$$F'(a_{\quad}) = \begin{pmatrix} 1&1&0&0&0 \\ 0&1&0&0&0 \\ 1&1&1&1&1 \\ 1&1&1&0&1 \\ 1&1&1&1&1 \end{pmatrix} \quad , \quad F'(a_{\quad}) = \begin{pmatrix} 1&0&0&1&0 \\ 1&0&0&1&0 \\ 1&1&1&1&0 \\ 0&0&0&1&0 \\ 1&1&1&1&1 \end{pmatrix}$$

$V(a_{\quad})=\{7,31,19,21,22\}$; $V(a_{\quad})=\{13,21,25,31,28\}$

$n=6$

$a_1=47=(1,0,1,1,1,1,1)$

$a_2=59=(1,1,1,0,1,1)$

$a_3=62=(1,1,1,1,1,0)$

$V(a_1)=\{15,63,39,43,45,46\}$

$V(a_2)=\{27,43,51,63,57,58\}$

$V(a_3)=\{30,46,54,58,60,63\}$

racines de F

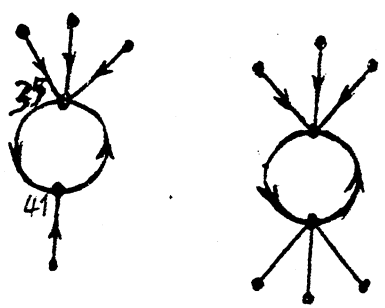


Fig.22.3

$n=4$

$$F'_d(x) = \begin{pmatrix} 1+x_2x_3x_4 & x_1x_3x_4 & x_1x_2x_4 & x_1x_2x_3 \\ x_2 & 1+x_1+x_3x_4 & x_2x_4 & x_2x_3 \\ x_3 & x_3 & 1+x_1+x_2+x_4 & x_3 \\ x_4 & x_4 & x_4 & x_1+x_2+x_3 \end{pmatrix}$$

$$F'(a_1) = \begin{pmatrix} 1&1&0&0 \\ 0&1&0&0 \\ 1&1&1&1 \\ 1&1&1&0 \end{pmatrix} \; ; \; F'(a_2) = \begin{pmatrix} 1&0&0&1 \\ 1&0&0&1 \\ 1&1&1&1 \\ 0&0&0&1 \end{pmatrix}$$

$a_1=11=(1,0,1,1)$, $a_2=14=(1,1,1,0)$; racines de F.

$V(11)=\{3,15,9,10\}$, $V(14)=\{6,10,12,15\}$

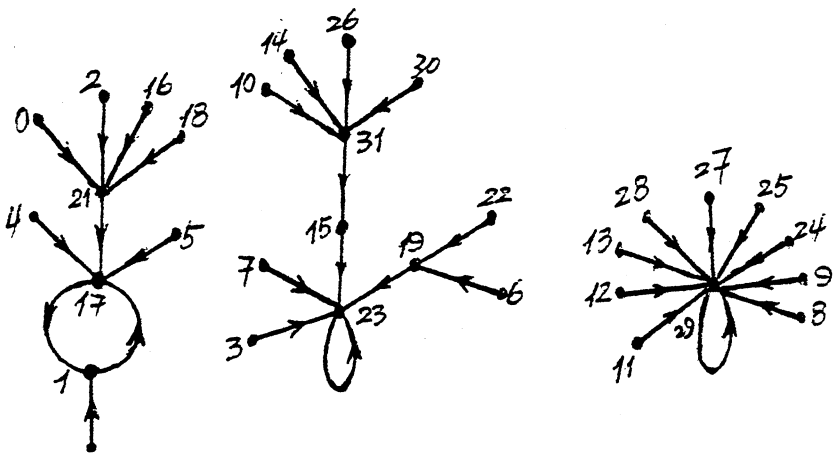
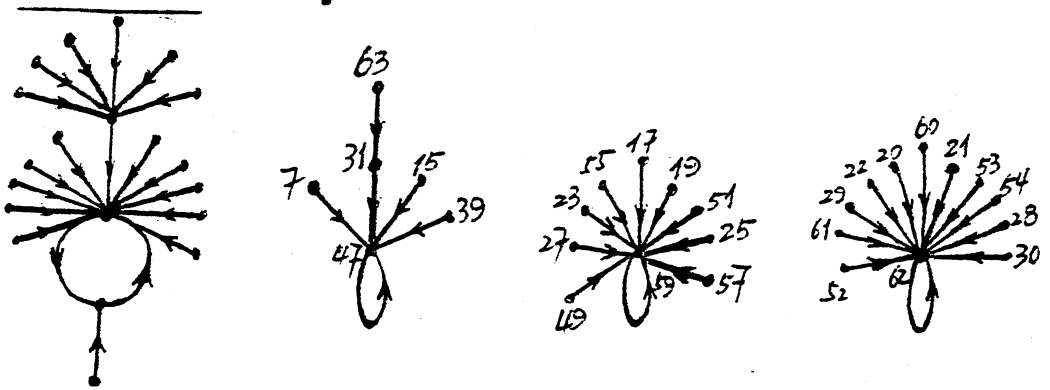


Fig.22.2



$$F(x) = \begin{cases} f_1 = x_1 + 1 \\ f_2 = 2x_1 + x_1x_2 + 2x_3 + x_3^2 \\ f_3 = x_1x_2 + x_3 + 2 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n$, $p = 11$, $n = 3$

Gauss Seidel, sur H, associé à F

graph partiel

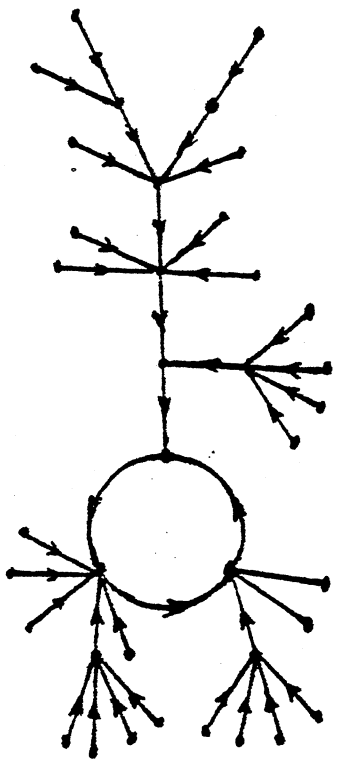


Fig.23.1

$$F(x) = \begin{cases} f_1 = x_1 + 1 \\ f_2 = 2x_1 + x_1x_2 + 3x_3 + x_1x_3 \\ f_3 = x_1x_2 + x_3 + 2 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n$, $p = 11$, $n = 3$

Gauss Seidel, sur H, associé à F

graph partiel

a: une racine de F(x)

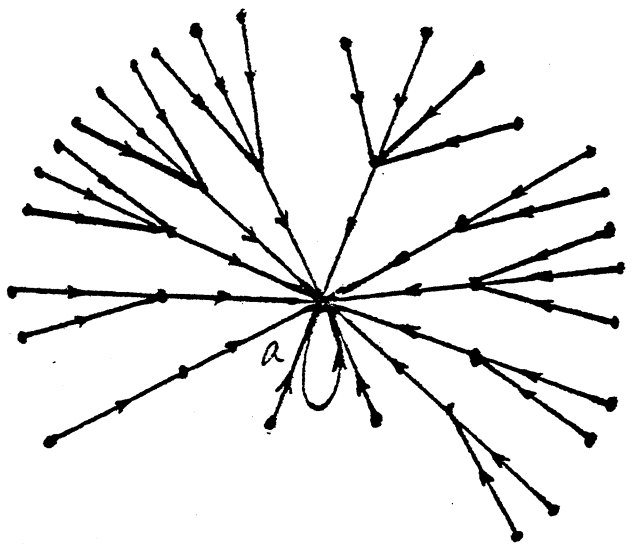


Fig.23.2

$$F(x) = \begin{cases} f_1 = x_1 + 1 \\ f_2 = 2x_1 + x_2 + 2x_3 + x_3^2 \\ f_3 = x_1x_2 + x_3 + 2 \end{cases}$$

$F(x):(Z/p)^n \longrightarrow (Z/p)^n$, $p = 11$, $n = 3$

Gauss Seidel, sur H, asscié à F

graph prtiel

(mêmes polynômes que fig19-3)

a_1, a_2: deux racines de F(x)

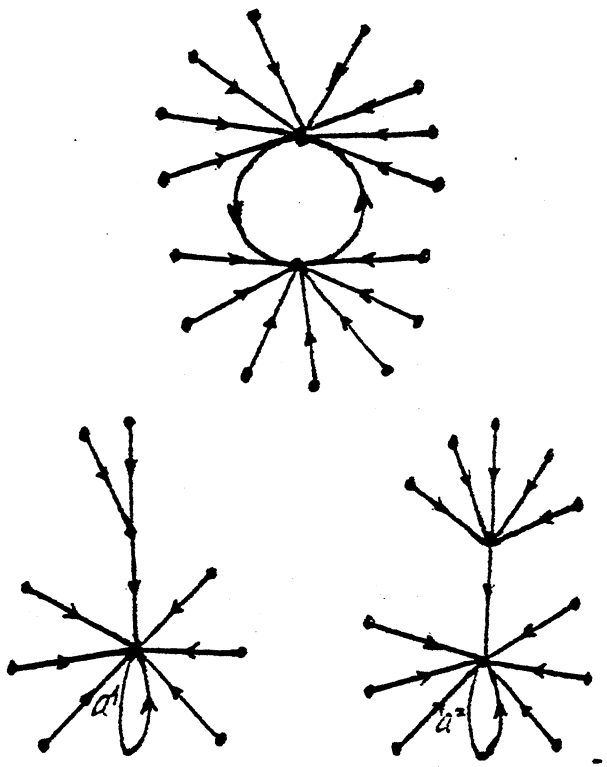


Fig.23.3

Newton standard sur F_1

p = 2, n = 4

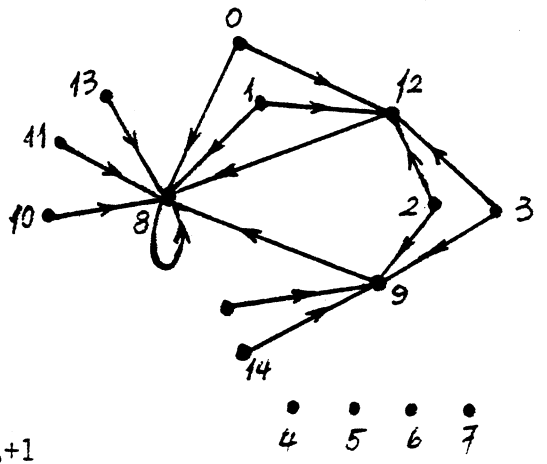


Fig.24.1

$$F(x)=\begin{cases} f_1=x_1+1 \\ f_2=x_1+x_1x_2+1 \\ f_3=x_1x_2+x_3 \\ f_4=x_1x_3+x_2x_3+x_4 \end{cases}$$

Newton simplifié, p=2,n=4

$$A=\begin{pmatrix} 1&0&1&0 \\ 0&1&0&0 \\ 0&0&1&1 \\ 0&1&0&1 \end{pmatrix}$$

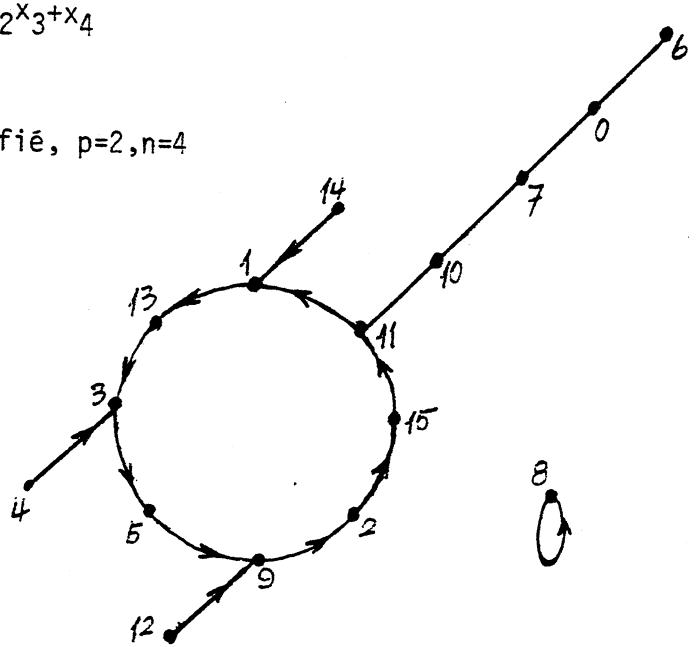


Fig.24.2

Gauss Seidel,p=2,n=3

$$F(x)=\begin{cases} f_1=x_3+1 \\ f_2=x_1+x_2+x_3 \\ f_3=x_2+x_3 \end{cases}$$

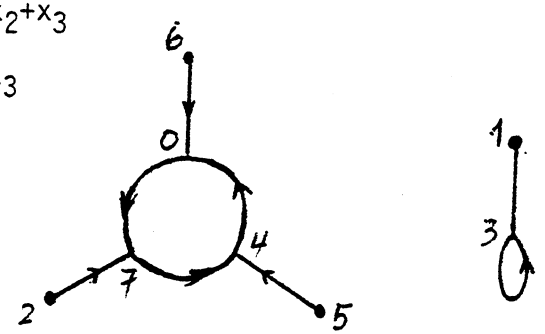


Fig.24.3

Gauss Seidel,p=2,n=4

$$F(x)=\begin{cases} f_1=x_2+x_4+1 \\ f_2=x_3+x_5 \\ f_3=x_1+x_2+1 \\ f_4=x_1+x_2+x_3 \end{cases}$$

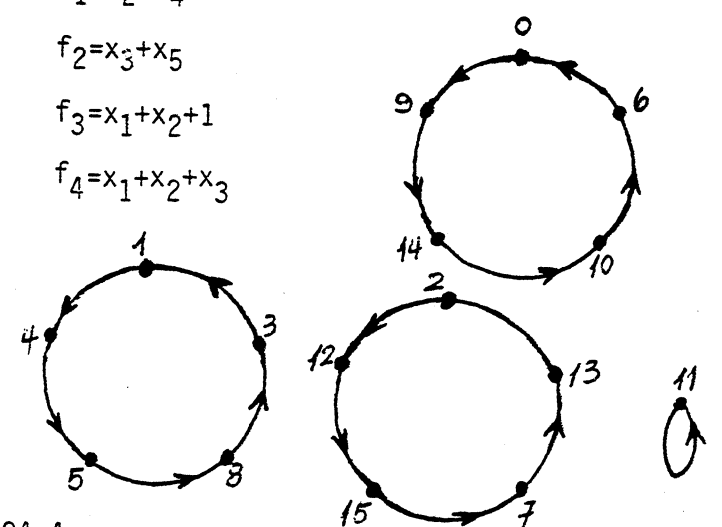


Fig.24.4

REFERENCES

[1] F. ROBERT : "Itérations discrètes". Polycopié de l'U.S.M.G. et l'I.N.P.G. (1981).

[2] B. DEMIDOVITCH et I. MARON : "Eléments de calcul numérique". traduit du russe par Valentin Polonski traduction française Edition Mir. (1973).

[3] S.EL BERNOUSSI:"Analyse et comparaison d'itérations discrètes; La méthode de Newton dans $(Z/p)^n$ " thèse I.M.A.G (1982)

[4] N. GASTINEL : "Analyse numérique linéaire". Hermann, Paris (1966).

[5] M. COSNARD : "Sur quelques méthodes Newton Like de résolution de systèmes d'équations non linéaires". Séminaire d'Analyse Numérique, I.M.A.G. n° 239 (1975).

[6] HAROLD STONE : "Discrete mathematical structures and their applications".
(c 1973), Science Research Associates. Inc. Printed in U.S.A.

[7] M. COSNARD : "Numerical Solution of Nonlinear Equations". ACM Transaction on Mathematical Software. Vol. 5. N° 1, March 1979, page 84-85.

Dernière page d'une thèse

VU

Grenoble, le 8 mars

Le Président de la thèse

M. GASTINEL

H. ZEQU JIANG

Vu, et permis d'imprimer,

Grenoble, le 9 mars 1982

Le Président de l'Université Scientifique et Médicale

UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE

Pour le Président,
M. TANCHE
Vice-Président Assesseur