Décomposition de Jordan-Chevalley-Dunford et itérations de Newton-Halley-Householder

Jean-François Burnol, 8 avril 2017

1 Fractions chinoises

Soient $n_1, \ldots, n_k$ des entiers strictement positifs premiers entre eux deux à deux. La fraction rationnelle

$$f = \frac{\dfrac{a_1}{n_1} + \cdots + \dfrac{a_k}{n_k}}{\dfrac{1}{n_1} + \cdots + \dfrac{1}{n_k}}$$

résout le problème Chinois :

$$\begin{aligned} f &\equiv a_1 \pmod{n_1} \\ \cdots &\qquad \cdots\cdots \\ f &\equiv a_k \pmod{n_k} \end{aligned}$$

On y a donné un sens à $f \pmod{n_j}$ en observant qu'après avoir multiplié le numérateur et le dénominateur par $P = \prod_j n_j$, elle prend la forme $f = A/B$ avec B premier avec P, et donc on interprète $1/B$ comme un inverse modulaire modulo P. Le résultat est indépendant du choix du dénominateur entier premier avec P.

On obtient une véritable solution entière avec une identité de Bézout $UB + VP = 1$, alors $x = UA$ est solution entière des congruences chinoises ($x \mod P$ étant le sens que l'on a donné à $f \mod P$).

Plus généralement, supposons données des y_j inversibles modulo n_j alors le problème Chinois est également résolu par cette autre fraction rationnelle

$$f = \frac{\dfrac{a_1 y_1}{n_1} + \cdots + \dfrac{a_k y_k}{n_k}}{\dfrac{y_1}{n_1} + \cdots + \dfrac{y_k}{n_k}}$$

qui donnera au final bien sûr la même solution entière modulo P, cette solution étant unique.

http://jf.burnol.free.fr/agreg170406Chinois.pdf

2 Fractions rationnelles chinoises

Plaçons nous dorénavant sur un corps $\mathbf{K}$, et pour le moment nous travaillons dans une clôture algébrique $\overline{\mathbf{K}}$.

Soit $P = \prod_j (X - \lambda_j)^{e_j}$ un polynôme unitaire, avec ses racines λ_j de multiplicités e_j, $1 \leqslant j \leqslant k$, soient Y_j, $1 \leqslant j \leqslant k$ des polynômes vérifiant $Y_j(\lambda_j) \neq 0$, et soient A_j, $1 \leqslant j \leqslant k$ des polynômes quelconques. Alors la fraction rationnelle

$$F = \frac{\sum_j \frac{A_j Y_j}{(X-\lambda_j)^{e_j}}}{\sum_j \frac{Y_j}{(X-\lambda_j)^{e_j}}}$$

résout le problème Chinois

$$\forall j \qquad F \equiv A_j \pmod{(X - \lambda_j)^{e_j}}$$

au sens où $F - A_j$ possède en λ_j un zéro de multiplicité au moins e_j.

La vérification est immédiate. Alors là j'ai un problème de notations : je ne peux pas utiliser D comme lettre pour un *dénominateur*, car plus tard j'utilise la lettre D pour *Dunford* et on aura $D = F$. Je vais prendre la lettre U car c'est celle que j'ai utilisée dans une fiche dont je donnerai le lien plus bas, mais ça me gêne un peu à cause du fait que j'aime bien U et V pour Bézout. Bon tant pis. Bref, je reviens à la vérification, en multiplicant numérateur et dénominateur par P on écrit F sous la forme :

$$\begin{aligned} F &= \frac{V}{U} \\ V &= \sum_j A_j Y_j \prod_{i \neq j} (X - \lambda_i)^{e_i} \\ U &= \sum_j Y_j \prod_{i \neq j} (X - \lambda_i)^{e_i} \end{aligned}$$

On constate que $U(\lambda_j) \neq 0$ puisque par hypothèse $Y_j(\lambda_j) \neq 0$, et après avoir écrit $F - A_j = (V - A_j U)/U$, on voit que le polynôme $V - A_j U$ a un zéro d'ordre au moins e_j en λ_j.

Pour obtenir une solution polynomiale aux congruences, il suffit donc de trouver une identité de Bézout (arrgh pour les notations..) $RU + SP = 1$, ce qui est possible puisque U ne s'annulant en aucune des racines de P est premier avec lui, et le polynôme RV (réduit éventuellement modulo P) donnera la solution cherchée.

3 La décomposition de Jordan-Chevalley-Dunford

Soit maintenant V un $\overline{\mathbf{K}}$-espace vectoriel de dimension finie et A un endomorphisme de polynôme caractéristique unitaire $P = \prod_j (X - \lambda_j)^{e_j}$. On note V_λ l'espace caractéristique pour la valeur propre λ.

Soient Y_j des polynômes vérifiant $\forall j \quad Y_j(\lambda_j) \neq 0$.

Considérons la fraction rationnelle

$$D = \frac{\sum_j \frac{\lambda_j Y_j}{(X-\lambda_j)^{e_j}}}{\sum_j \frac{Y_j}{(X-\lambda_j)^{e_j}}} = \frac{V}{U}$$

avec $U = \sum_j Y_j \prod_{i \neq j} (X - \lambda_i)^{e_i}$, $V = \sum_j \lambda_j Y_j \prod_{i \neq j} (X - \lambda_i)^{e_i}$. Le polynôme U est premier avec P donc il existe une identité de Bézout $RU + SP = 1$.

Ainsi $U(A)$ est inversible et nous pouvons définir $D(A) = U(A)^{-1} V(A) = R(A)V(A)$.

Il est clair que que $V(A) - \lambda_j U(A)$ est une somme de polynômes tous divisibles par $(X - \lambda_j)^{e_j}$ et $(A - \lambda_j)^{e_j}$ s'annule sur V_{λ_j} donc $V(A) - \lambda_j U(A)$ agit par l'endomorphisme nul sur V_{λ_j} (il y a beaucoup de V là-dedans, misère…). Et par conséquent $D(A)$ agit simplement par la multiplication par λ_j sur V_{λ_j}.

L'endomorphisme $A - D(A) = N$ est par conséquent nilpotent et l'écriture $A = D(A) + N$ réalise la décomposition de Dunford, ou de Jordan-Chevalley.

Notre objectif dorénavant est de trouver un algorithme pour calculer la fraction rationnelle D effectivement, et au passage montrer que si A est défini sur $\mathbf{K}$ alors on peut choisir D et donc finalement le polynôme d'endomorphisme $D(A)$ aussi comme étant définis sur $\mathbf{K}$.

4 Comment écrire le numérateur en fonction du dénominateur ?

C'est très simple :

$$\sum_j \frac{\lambda_j Y_j}{(X - \lambda_j)^{e_j}} = \sum_j \frac{(X - (X - \lambda_j))Y_j}{(X - \lambda_j)^{e_j}} = X \sum_j \frac{Y_j}{(X - \lambda_j)^{e_j}} - \sum_j \frac{Y_j}{(X - \lambda_j)^{e_j - 1}}$$

et donc

$$D = X - \frac{\sum_j \frac{Y_j}{(X-\lambda_j)^{e_j-1}}}{\sum_j \frac{Y_j}{(X-\lambda_j)^{e_j}}}$$

Mais le hic c'est que nous avons donc besoin de deux dénominateurs.

Au niveau des notations, j'utiliserai plutôt F dorénavant pour les fractions rationnelles.

5 Comment passer d'un dénominateur au suivant ?

On peut imaginer faire des dérivations, par exemple par rapport à λ_j. Mais on se récupère un e_j. Cela limite semble-t-il les possibilités pour une récurrence simple qui nous donnerait à la fois numérateur et dénominateur de la formule ci-dessus. Il semble qu'il nous faille prendre les e_j tous égaux.

Ceci nous amène donc au polynôme réduit $Q = \prod_j (X - \lambda_j)$. Dorénavant je vais aussi me limiter à la caractéristique nulle car dans ce cas on a simplement $Q = P/\mathrm{PGCD}(P, P')$ (ça marche aussi parfois en caractéristique positive, mais autant simplifier dès maintenant).

Nous voyons en particulier que Q est défini sur $\mathbf{K}$ si P l'est (c'est faux en caractéristique positive : $Q = X - T^{1/p}$, $P = Q^p = X^p - T$, $\mathbf{K} = \mathbf{F}_p(T)$).

Mais bon, même en prenant les e_j tous égaux, cette histoire de dériver par rapport à λ_j semble un peu délicate. On peut par contre dériver par rapport à X. Et cette opération est définie sur $\mathbf{K}$.

Mais alors le problème va être avec les Y_j. Il semble qu'on soit contraint de les prendre constants : $Y_j = y_j \in \overline{\mathbf{K}}$. Bon, ben alors ça marche :

$$\frac{d}{dX} \sum_j \frac{y_j}{(X-\lambda_j)^e} = -e \sum_j \frac{y_j}{(X-\lambda_j)^{e+1}}$$

Tout est en place. Notre problème de la décomposition de Dunford sera résolu en prenant $e = \max(e_j)$ ou n'importe quel entier plus grand, autrement dit on devra prendre e de sorte que P divise Q^e.

6 La récurrence

Elle porte sur les

$$U_n = Q^n \frac{d^{n-1}}{dX^{n-1}} \sum_j \frac{y_j}{(X-\lambda_j)} = (-1)^{n-1}(n-1)!Q^n \sum_j \frac{y_j}{(X-\lambda_j)^n},$$

qui sont donc des polynômes :

$$U_n = (-1)^{n-1}(n-1)! \sum_j y_j \prod_{i\neq j} (X-\lambda_i)^n$$

et la récurrence est

$$U_{n+1}Q^{-n-1} = (U_nQ^{-n})' = U_n'Q^{-n} - nU_nQ^{-n-1}Q' \tag{1}$$

$$U_{n+1} = -nQ'U_n + QU_n' \tag{2}$$

Je mets le terme avec Q' en premier car il jouera le rôle d'un inversible, tandis que Q joue celui d'un nilpotent. On pourrait normaliser en divisant par U_n par $(-1)^{n-1}(n-1)!$. Je laisse comme cela.

Nous pouvons aussi exprimer les U_n sous la forme :

$$U_n = Q^n \frac{d^{n-1}}{dX^{n-1}}(U_1/Q)$$

Le polynôme U_1 est n'importe quel polynôme de degré strictement inférieur à celui de Q, et premier avec lui. S'il est défini sur $\mathbf{K}$ tous les U_n le seront.

D'une manière générale, nous n'avons semble-t-il pas beaucoup de choix :

1. On peut prendre $U_1 = 1$.
2. On peut prendre $U_1 = Q'$.
3. On peut prendre plus généralement $U_1 = (Q')^m \pmod{Q}$ pour un entier m.

Dans

http://jf.burnol.free.fr/agreg170406Dunford_NewAlgo.pdf

j'avais utilisé $U_1 = Q'$ car cela donne la fraction rationnelle la plus simple avec tous les $y_j = 1$. Mais le choix $U_1 = 1$ est aussi intéressant, et de plus les récurrences construisent alors des polynômes de plus petits degrés !

7 La formule générale pour la décomposition de Jordan-Chevalley-Dunford

Soit P le polynôme caractéristique unitaire de l'endomorphisme A sur un espace vectoriel de dimension finie sur un corps $\mathbf{K}$, de caractéristique nulle. Soit $Q = P/\mathrm{PGCD}(P, P')$ le polynôme réduit, qui est aussi dans $\mathbf{K}[X]$.

Soit maintenant U_1 n'importe quel polynôme de $\mathbf{K}[X]$ premier avec Q et de degré strictement inférieur à lui. Par exemple $U_1 = 1$ ou $U_1 = Q'$. [1]

Définissons, pour $n \geqslant 1$:

$$U_n = Q^n \frac{d^{n-1}}{dX^{n-1}}(U_1/Q)$$

de sorte que la récurrence

$$U_{n+1} = -nQ'U_n + QU_n'$$

est vérifiée.

Soit maintenant, pour $n \geqslant 2$ (et on posera $F_1 = X$), F_n les fractions rationnelles

$$F_n = X + (n-1)\frac{U_{n-1}}{U_n}Q = X + (n-1)\frac{(U_1/Q)^{(n-2)}}{(U_1/Q)^{(n-1)}}$$

Théorème. *La fraction rationnelle $Q(F_n)$ s'annule modulo (Q^n), au sens où elle possède en chaque λ_j un zéro de multiplicité au moins n.*

Preuve. Sur la clôture algébrique, nos calculs précédents ont établi

$$n \geqslant 2 \implies F_n = \frac{\sum_j \lambda_j y_j (X-\lambda_j)^{-n}}{\sum_j y_j (X-\lambda_j)^{-n}}$$

avec les coefficients y_j définis par

$$\frac{U_1}{Q} = \sum_j \frac{y_j}{X-\lambda_j}$$

On peut aussi écrire cela

$$F_n = \frac{V_n}{U_n}$$

1. La restriction sur le degré de U_1 peut être levée voir plus loin.

avec

$$U_n = (-1)^{n-1}(n-1)! \sum_j y_j \prod_{i \neq j} (X - \lambda_i)^n$$
$$V_n = (-1)^{n-1}(n-1)! \sum_j \lambda_j y_j \prod_{i \neq j} (X - \lambda_i)^n$$

donc $V_n - \lambda_j U_n$ s'annule en λ_j avec multiplicité au moins n.

Or $Q(F_n)U_n^{\deg Q} = \prod_j (V_n - \lambda_j U_n)$ et par conséquent ce polynôme s'annule en chaque λ_j avec multiplicité au moins n.

Et $U_n(\lambda_j) \neq 0$ pour tout j, car $y_j \neq 0$, puisque U_1 et Q sont premiers entre eux, et donc $U_1(\lambda_j) \neq 0$. □

Corollaire 1. *Soit W_n un inverse de U_n modulo Q^n. Alors le polynôme*

$$D_n = X + (n-1)W_n U_{n-1} Q$$

vérifie

$$Q(D_n) \equiv 0 \mod Q^n$$

Par conséquent le polynôme d'endomorphisme $D_n(A)$ est la partie semi-simple de l'endomorphisme A de polynôme caractéristique P (à condition que P divise Q^n.)

8 Les itérations de Newton-Halley-Householder

On a $U_2 = -Q'U_1 + QU_1'$ et $F_2 = X + \frac{U_1}{U_2}Q$, donc

$$F_2 = X - \frac{Q}{Q'} \frac{U_1}{U_1 - \frac{Q}{Q'}U_1'}$$

Le cas $U_1 = 1$ est particulièrement simple :

$$F_2 = X - \frac{Q}{Q'}$$

qui n'est autre que l'itération de Newton pour approcher numériquement une racine de l'équation $Q(x) = 0$.

Si l'on prend $U_1 = Q'$, c'est un peu plus compliqué :

$$F_2 = X - \frac{Q}{Q'} \frac{1}{1 - \frac{QQ''}{(Q')^2}}$$

mais modulo Q^2, les deux sont identiques, car elles résolvent le même problème Chinois, comme expliqué précédemment.

Regardons F_3 lorsque $U_1 = 1$, $U_2 = -Q'$, $U_3 = 2(Q')^2 - QQ''$, cela donne

$$F_3 = X - 2\frac{Q'}{2(Q')^2 - QQ''}Q$$

Et l'itération $x \leftarrow x - \frac{2ff'}{2(f')^2 - ff''}$ est connue dans la littérature (semble-t-il depuis 1694...) sous le nom de « méthode de HALLEY ».

Elle possède la propriété cubique : si l'on démarre suffisamment près d'un zéro simple de f, on triple grosso modo le nombre de chiffres corrects à chaque itération.

Modulo Q^3, on a

$$F_3 \equiv X - \frac{Q}{Q'}\left(1 + \frac{QQ''}{2(Q')^2}\right) = X - \frac{Q}{Q'} - \frac{Q^2Q''}{2(Q')^3} \pmod{Q^3}$$

L'itération $x \leftarrow x - \frac{f}{f'} - \frac{f^2f''}{2(f')^3}$ est appelée itération de HOUSEHOLDER. Elle possède aussi la propriété cubique.

Tous ces F_3 sont égaux modulos Q^3 à l'unique polynôme de degré $< 3 \deg Q$ résolvant le problème chinois correspondant à la partie semi-simple de la multiplication par X modulo Q^3.

Le problème de schémas itératifs généralisant celui de NEWTON ou de HALLEY est abordé par HOUSEHOLDER dans

A. S. HOUSEHOLDER, *The Numerical Treatment of a Single Nonlinear Equation*, McGraw-Hill, New York, (1970)

Dans le chapitre 4, section *Iterations of higher order*, Théorème 4.4.2 on trouve la formule

$$x + p\frac{(g/f)^{(p-1)}}{(g/f)^{(p)}}$$

comme « itération d'ordre $p+1$ », et une expression déterminantale est donnée mais il faut revenir au début du livre pour comprendre les notations.

Si je comprends bien le texte les formules avec $g = 1$ semblent remonter au moins à SCHRÖDER, 1870.

E. Schröder *Über unendliche viele Algorithmen zur Auflösung der Gleichungen*, Math. Ann., 2 :317-365. (1870)

Je ne suis pas allé voir l'article encore. Et Householder suggère d'utiliser $g = f'$ si f a une racine multiple.

Dans mon texte

http://jf.burnol.free.fr/agreg170406Dunford_NewAlgo.pdf

j'avais pris $U_1 = Q'$ car c'était la chose se présentant plus naturellement dans cette approche, mais ça fonctionne aussi avec $U_1 = 1$ comme dit précédemment, et correspond aux choix $y_j = 1/Q'(\lambda_j)$. Les polynômes sont alors de degrés un peu plus petits. Et le F_2 est exactement celui de la formule de Newton pour ce choix là.

Je peux donc clarifier la relation entre l'approche du document ci-dessus pour traiter le problème de la décomposition de Dunford et l'approche itérative de Chevalley dans *Théorie des groupes de Lie, Tome II*.

Chevalley utilise une forme de la méthode de Newton qui converge quadratiquement vers la solution.

Mon texte cité ci-dessus est lié à l'existence des méthodes itératives de Halley-Schröder-Householder qui sont d'ordres supérieurs : cubique, quartique, etc... Il n'y a pas, moralement, d'itération dans cette méthode car elle accomplit le résultat en une seule transformation ! Pour la transformation il existe des formules plus ou moins explicites [2] (à la Faa di Bruno, avec des déterminants, et je devrais regarder en particulier plus l'aspect approximants de Padé) mais peut-être que le plus simple au niveau calculatoire est encore de la mettre en place par les récurrences naïves que j'ai indiquées.

On peut aussi, si l'on veut, une fois atteint le niveau N et obtenu le F_N se mettre à itérer à la Chevalley et alors on aura une solution de $Q(F) \equiv 0$ modulo Q^{N^n} au bout de la n^e itération... Comme ces itérations semblent un peu dantesques si l'on reste avec des fractions rationnelles, a priori on travaillera avec des polynômes et pour cela il y a une inversion initiale de Q' à faire modulo Q^N. Même au niveau des polynômes les degrés explosent exponentiellement (plus vite que Q^{N^n}) et donc on travaille en fait modulo un idéal. Au pire, modulo l'idéal final P, mais *il suffit en fait de calculer modulo Q^{N^n} à la n^e étape.*

Dans la partie qui met sur pied la transformation par une récurrence initiale, on peut aussi travailler modulo Q^n à la n^e étape (celle qui donne U_n), mais c'est déjà le cas ! En effet les formules de récurrence fournissent déjà des polynômes de degrés inférieurs

2. Il y a un article de Thomas Simon où si je me souviens bien les dérivées de $1/f$ donnent lieu à divers développements, mais j'ai oublié les détails. Bien sûr la combinatoire liée à cela doit avoir une riche littérature. À commencer par le livre de Householder.

à $n \deg Q$.

Ici il y aura une inversion de U_n à faire modulo l'idéal final (alors que dans le schéma itératif de Chevalley on a une inversion à faire au tout début modulo Q).

Il y a peut-être des choses supplémentaires à dire sur les inverses modulaires des U_n. J'écris ces lignes sans avoir regardé encore de plus près.

9 Comportement des récurrences modulo les puissances de Q

Faisons quelques remarques sur la récurrence

$$U_{n+1} = -nQ'U_n + QU_n'$$

Supposons que $n \leqslant N$ et qu'au final nous réduisons modulo Q^N.

- Considérons $f_n(T) = -nQ'T + QT'$. Si $T_1 \equiv T_2 \pmod{Q}$, alors évidemment $f_n(T_1) \equiv f_n(T_2) \pmod{Q}$. Donc par récurrence nous avons clairement $U_n \equiv (-1)^{n-1}(n-1)!(Q')^{n-1}U_1 \pmod{Q}$. Autrement dit U_n est de la forme $(-1)^{n-1}(n-1)!(Q')^{n-1}$ plus un nilpotent.
- Plus précisément si $T_1 \equiv T_2 \pmod{Q^k}$ alors $f_n(T_1) \equiv f_n(T_2) \pmod{Q^k}$. On peut donc dire que les transformations ont une forme triangulaire par rapport à la filtration $(1) \supset (Q) \supset (Q^2) \supset \ldots$.
- L'idéal (P) est envoyé par lui-même par $T \mapsto QT'$ car P, même s'il n'est pas une puissance de Q, divise QP', si Q en est le polynôme réduit. Donc les transformations f_n sont d'une manière plus générale compatibles avec toutes les inclusions $(Q) \supset (P_1) \supset (P_2) \supset (Q^N)$.
- Mais il y a mieux. Supposons que nous changeons U_n en $T_n = U_n + Q^n X_n$. Alors U_{n+1} sera modifié en $T_{n+1} = -nQ'T_n + QT_n' = U_{n+1} - nQ'Q^nX_n + Q(nQ^{n-1}Q'X_n + Q^nX_n') = U_{n+1} + Q^{n+1}X_n'$. Donc l'erreur se propage d'une manière totalement contrôlée et au final, notre nouvel U_N, disons T_N est exactement égal à $U_N + Q^N X_n^{(N-n)}$. La fraction $F_N = X + (N-1)QU_{N-1}/U_N$ n'a pas changé modulo Q^N car U_{N-1} et U_N n'ont pas changé modulo Q^{N-1}.
- En particulier supposons que U_1 est changé en $T_1 = U_1 + QX_1$. Alors les formules de récurrence nous donneront les mêmes numérateurs V_N et U_N modulo Q^N pour la fraction rationnelle F_N et donc elle sera aussi une fraction rationnelle résolvant le problème chinois modulo Q^N.

Ces deux dernières remarques se font d'ailleurs immédiatement sur les formules

$$U_n = Q^n \frac{d^{n-1}}{dX^{n-1}}(U_1/Q) \qquad U_{n+m} = Q^{n+m}\frac{d^m}{dX^m}(U_n/Q^n)$$

On s'intéresse maintenant aux $U_m \pmod{Q^n}$ pour $m \geqslant n$. Soit Z_n la solution de degré $< n \deg Q$ au problème chinois (on note $k = \deg Q$) :

$$\forall 1 \leqslant j \leqslant k \quad Z_n \equiv \prod_{i\neq j}(X-\lambda_i) \pmod{(X-\lambda_j)^n}$$

En particulier $Z_1 = Q'$ et en général $Z_n - Q'$ est nilpotent.

On a, puisque $U_m = (-1)^{m-1}(m-1)!\sum_j y_j \prod_{i\neq j}(X-\lambda_i)^m$,

$$m \geqslant n \implies \forall 1 \leqslant j \leqslant k \quad \frac{U_m}{(-1)^{m-1}(m-1)!} \equiv Z_n^{m-n}\frac{U_n}{(-1)^{n-1}(n-1)!} \pmod{(X-\lambda_j)^n}$$

de sorte que tout simplement

$$m \geqslant n \implies \frac{U_m}{(-1)^{m-1}(m-1)!} \equiv Z_n^{m-n}\frac{U_n}{(-1)^{n-1}(n-1)!} \pmod{Q^n}$$

et donc on constate que

$$m > n \implies F_m = X + (m-1)\frac{U_{m-1}}{U_m}Q \equiv X - \frac{Q}{Z_n} \pmod{Q^n}$$

Notons à ce sujet que Z_n est inversible modulo Q^n, puisque $Z_n(\lambda_j) \neq 0$.

Mais par ailleurs nous savons que F_m résout un problème chinois modulo Q^m qui se réduit à celui dont F_n est aussi solution modulo Q^n.

On peut donc écrire

$$F_n \equiv X - Z_n^{-1}Q \equiv X - Z_{n-1}^{-1}Q \pmod{Q^n}$$

En effet on n'a besoin que de Z_n^{-1} modulo Q^{n-1}, et comme $Z_n \equiv Z_{n-1} \pmod{Q^{n-1}}$, on peut utiliser ce dernier et son inverse modulo Q^{n-1}.

Comme Z_{n-1} diffère de Q' par un nilpotent modulo Q^{n-1}, il est possible de faire une expansion en puissance de $(Z_{n-1} - Q')/Q'$. Il y a peut-être des choses plus intelligentes à faire (fractions continues ? si seulement j'avais lu Householder…).

On a déjà vu

$$F_1 = X$$
$$F_2 = X - \frac{Q}{Q'} \pmod{Q^2}$$
$$F_3 = X - \frac{Q}{Q'} - \frac{Q''Q^2}{2(Q')^3} \pmod{Q^3}$$

et celui d'après est

$$F_4 = X - \frac{Q}{Q'} - \frac{Q''Q^2}{2(Q')^3} - \frac{(3(Q'')^2 - Q'Q''')Q^3}{6(Q')^5} \pmod{Q^4}$$

Lorsque l'on veut faire une itération à la Newton-Halley-Schröder quartique comme celle-ci :

$$x \leftarrow x - \frac{f}{f'} - \frac{f''f^2}{2(f')^3} - \frac{(3(f'')^2 - f'f''')f^3}{6(f')^5}$$

il faut disposer de formules utilisables pour les dérivées successives ! Bon, c'est le cas pour les fonctions du type $x^a - u$ en tout cas. Par exemple pour calculer $\sqrt{2}$....

Addendum (9 avril) :

Il est avantageux pour la formule ci-dessus d'y utiliser à la place de $x^2 - 2$ par exemple, $f = x^{-2} - \frac{1}{2}$. Car alors l'itération est polynomiale, et évite d'avoir à faire des divisions en haute précision. cf Gourdon-Sebah :

http://numbers.computation.free.fr/Constants/Sqrt2/sqrt2.html

http://numbers.computation.free.fr/Constants/Algorithms/newton.html

Comme les pages ci-dessus ont (en tout cas avec le navigateur sur mon ordi) des problèmes d'affichage de symboles, je conseille de cliquer sur le lien qu'on y trouve pour leur version en fichier ps (et de le convertir en pdf par ps2pdf par exemple).

On peut envisager de faire les calculs avec des entiers et uniquement des puissances de 2 dans le dénominateur, en débutant à 3/2 par exemple. Ce qui est bien adapté à la représentation en binaire. En ne conservant à chaque étape qu'un nombre approprié (quadruplant à chaque étape, à peu près, pour une itération quartique) de chiffres dominants du numérateur (en binaire). Pas réfléchi aux détails. Je ne sais pas si Gourdon-Sebah utilisaient à l'époque (dans les calculs résumés sur leur page) de l'arithmétique flottante haute précision ou de l'arithmétique entière dans le style de ce que je viens d'esquisser.