**Applied Mathematics E-Notes, 11(2011), 244–248 ©** ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

# Approximate GCD A La Dedieu[*]

Jean-Claude Yakoubsohn, Mohamed Masmoudi, Guillaume Chèze[†],
and
Didier Auroux [‡]

Received 11 November 2010

**Abstract**

In this paper, we use results due to Dedieu et al. within the framework of the approximate gcd problem. We obtain explicit and simple formulas for certifying the convergence of Newton-Gauss' method.

## 1 Introduction

Approximate gcd is a difficult problem of symbolic-numeric computation. It has been widely studied in the recent years, leading to many theoretical results and algorithms. We refer the reader to [5, 1, 7, 9, 10, 2, 6, 8] for an example of such algorithms and references. The common idea of many algorithms is to guess an approximate solution of the problem, and then to improve the accuracy and precision of the solution. In this paper, we propose to study the second point. One way to improve the accuracy of an approximate solution is indeed to use the Newton-Gauss method initialized with this solution. The Newton-Gauss algorithm converges as soon as the first guess is close enough to an attractor. The point is then to bound the distance between the approximate and exact solutions, and to numerically measure it.

Smale's $\alpha$-theory answers these questions in the case of Newton's method. In our framework, the convergence for Newton-Gauss' method has been proved by Dedieu-Shub [3] and Dedieu-Kim [4].

In this paper, we use the main results of [3] and [4] within the framework of the approximate gcd problem. We obtain explicit and simple formulas for certifying the convergence of Newton-Gauss' method.

## 2 Newton-Gauss Operator and Dedieu's Theorem

In this section we recall the main results of [3] and [4].

[*] Mathematics Subject Classifications: 49M15, 33F10.

[†] Institut de Mathématiques de Toulouse,Université Paul Sabatier Toulouse 3, 31062 Toulouse cedex 9, France

[‡] Laboratoire J. A. Dieudonné, University of Nice Sophia Antipolis, Parc Valrose, 06108 Nice cedex 2, France

DEFINITION 1. Let $\mathbb{E}$ and $\mathbb{F}$ be two Hilbert spaces, and $\varphi : E \to \mathbb{F}$ an analytic map. We suppose that $Im(D\varphi(x))$ is closed in $\mathbb{F}$. We define the Newton-Gauss operator by

$$N_\varphi(x) = x - D\varphi(x)^\dagger \varphi(x)$$

where $D\varphi(x)^\dagger$ denotes the Moore-Penrose pseudo inverse of $D\varphi(x)$.

DEFINITION 2. Let $\varphi$ be an analytic map between two Hilbert spaces $\mathbb{E}$ and $\mathbb{F}$, such that the image of $D\varphi(x)$ is closed in $\mathbb{F}$. Let $x \in \mathbb{E}$, we set:

- $\beta(\varphi, x) = \|D\varphi(x)^\dagger\| \ \|\varphi(x)\|$,
- $\gamma(\varphi, x) = \sup_{k\geq 2} \Big( \|D\varphi(x)^\dagger\| \ \Big\|\dfrac{D^k\varphi(x)}{k!}\Big\| \Big)^{\frac{1}{k-1}}$,
- $\alpha(\varphi, x) = \beta(\varphi, x)\, \gamma(\varphi, x)$,
- $\psi(\lambda) = 1 - 4\lambda + 2\lambda^2$.

THEOREM 1. Let $x$ and $\zeta \in \mathbb{E}$ such that $D\varphi(\zeta)^\dagger \varphi(\zeta) = 0$, $D\varphi(\zeta)$ injective, and

$$v = \|x - \zeta\| \, \gamma(\varphi, \zeta) < 1 - \frac{\sqrt{2}}{2}.$$

If

$$\alpha(\varphi, \zeta) < \frac{1}{2\sqrt{2}},$$

then Newton-Gauss' sequence satisfies

$$\|x_k - \zeta\| \leq \lambda^k \|x - \zeta\|$$

where

$$\lambda = \frac{v + \sqrt{2}\,(2 - v)\, \alpha(\varphi, \zeta)}{\psi(v)} < 1.$$

This theorem certifies the convergence of Newton-Gauss' algorithm inside a disk of given radius. The following result gives a sufficient condition for convergence of Newton-Gauss' method.

THEOREM 2. Let $x \in \mathbb{E}$ such that $D\varphi(x)$ is injective. We set

$$\kappa = \|D\varphi(x)\| \ \|D\varphi(x)^\dagger\|,$$

$$\lambda = \frac{1}{8\kappa + 16},$$

$$\Lambda = 4\, \frac{1 - \lambda}{\psi(\lambda^2)} \Big( \frac{1}{16\kappa + 32} + \frac{\lambda^2}{1 - \lambda} + \kappa\lambda \Big).$$

We have $0 \leq \Lambda < 1$.
We suppose that

$$\alpha(\varphi, x) \leq \frac{1}{16\kappa + 32},$$

then

1. there exists a unique $\zeta \in \mathbb{E}$ such that $D\varphi(\zeta)^\dagger\varphi(\zeta) = 0$ and
$$\|\zeta - x\| < \frac{\lambda}{\gamma(\varphi, x)};$$
2. Newton-Gauss' sequence $x_k = N_\varphi^k(x)$ converges towards $\zeta$ and
$$\|x_k - \zeta\| \leq \Lambda^k \|x - \zeta\|.$$

# 3 Application to GCD Problem

Let $f$ and $g$ be two unitary polynomials in $\mathbb{C}[X]$. We assume that an algorithm for computing the approximate gcd returned $p$, $f_1$, $g_1$ such that
$$\varepsilon^2 := \|f - pf_1\|_2^2 + \|g - pg_1\|_2^2,$$
is small, and $\deg(p.f_1) \leq \deg(f)$ and $\deg(p.g_1) \leq \deg(g)$. We also assume that $p$ is of maximum degree, i.e. there does not exist any polynomials $P$, $F_1$, and $G_1$ such that $\deg P > \deg p$ and $\|f - PF_1\|_2^2 + \|g - PG_1\|_2^2 \leq \|f - pf_1\|_2^2 + \|g - pg_1\|_2^2$.

Usually, one first sets $f_1$ and $g_1$, and solves a linear least square problem in order to obtain a better solution for $p$. Then one sets $p$, and solves a linear least square problem in order to improve $f_1$ and $g_1$. This process is then iteratively repeated.

We now propose a way to improve simultaneously $p$, $f_1$ and $g_1$ with a Newton-Gauss method. We define the following function:
$$\varphi(p, f_1, g_1) = (f - p.f_1; g - p.g_1).$$
Our goal is to give a certified condition on $p$, $f_1$ and $g_1$ for Newton-Gauss' convergence. As we have
$$\begin{aligned}\varphi(p + \tilde{p}, f_1 + \tilde{f}_1, g_1 + \tilde{g}_1) &= (f - p.f_1 - p.\tilde{f}_1 - f_1.\tilde{p} - \tilde{p}.\tilde{f}_1,\\ &\quad g - p.g_1 - p.\tilde{g}_1 - g_1.\tilde{p} - \tilde{p}.\tilde{g}_1),\end{aligned}$$
then
$D\varphi(p, f_1, g_1)(\tilde{p}, \tilde{f}_1, \tilde{g}_1) = \big(-Sylv(p, f_1)(\tilde{p}, \tilde{f}_1), -Sylv(p, g_1)(\tilde{p}, \tilde{g}_1)\big)$, where $Sylv(p, f_1)$ is the Sylvester matrix associated to $p$ and $f_1$, see [11, Chapter 6]. We set
$$\mathcal{V} = \{(p, f_1, g_1) \mid \det Sylv(p, f_1) = 0 \text{ and } \det Sylv(p, g_1) = 0\}.$$
$\mathcal{V}$ is a closed Zariski set, thus a set with measure zero for the Lebesgue measure. Thus we can assume that in numerical experiments $(p, f_1, g_1)$ does not belong to this variety $\mathcal{V}$. Then we now assume $D\varphi(p, f_1, g_1)$ to be injective.

On the other side, $\frac{1}{2}D^2\varphi(p, f_1, g_1)(\tilde{p}, \tilde{f}_1, \tilde{g}_1) = (-\tilde{p}.\tilde{f}_1, -\tilde{p}.\tilde{g}_1)$. Moreover, we have the following result:

PROPOSITION 1. Let $C_{inf} = \sqrt{2^{-2\deg f} + 2^{-2\deg g}}$, and
$C_{sup} = \sqrt{(\deg f + 1)^3 + (\deg g + 1)^3}$. Then $C_{sup} \geq \frac{1}{2}\|D^2\varphi(p, f_1, g_1)\|_2 \geq C_{inf}$.

PROOF. We have the following bounds (corollary 6.33 in [11]):

$$\sqrt{\deg F + \deg G + 1}\|F.G\|_\infty \geq \|F.G\|_2 \geq 2^{-degF - \deg G}\|F\|_2\|G\|_2.$$

We apply this formulae with $F = \tilde{p}$ and $G = \tilde{f}_1$ (resp. $G = \tilde{g}_1$), assuming that $\|\tilde{p}\|_2 \leq 1$, $\|\tilde{f}_1\|_2 \leq 1$ and $\|\tilde{g}_1\|_2 \leq 1$.

For the upper bound, $\|\tilde{p}.\tilde{f}_1\|_\infty = \max_k \left|\sum_{i+j=k} \tilde{p}_i \tilde{f}_{1,j}\right| \leq \deg(\tilde{p}.\tilde{f}_1) + 1 \leq \deg f + 1$, as $|\tilde{p}_i| \leq 1$ and $|\tilde{f}_{1,j}| \leq 1$ for all $i, j$.

Then, we take the supremum over all $\tilde{p}$ and $\tilde{f}_1$ of norm smaller than 1, and the lower bound becomes $2^{-\deg \tilde{p} - \deg \tilde{f}_1} \geq 2^{-\deg f}$.

We denote by $\mathcal{D}$ Dedieu's constant:

$$\mathcal{D} := \left\| \left(Sylv(p, f_1); Sylv(p, g_1)\right)^\dagger \right\|.$$

We have then the following bounds for the gcd:

THEOREM 3. With the previous notations we have:

$$\beta(p, f_1, g_1) = \mathcal{D}\,\varepsilon\,;$$

$$C_{sup}\,\mathcal{D} \geq \gamma(p, f_1, g_1) \geq C_{inf}\,\mathcal{D}\,;$$

$$\alpha(p, f_1, g_1) \leq C_{sup}\,\mathcal{D}^2\,\varepsilon,.$$

In conclusion, we get an easy test to check the convergence of Newton-Gauss' method for the approximate gcd problem.

# 4 Numerical Example

In this section, we compute the corresponding bounds on a toy example. We set

$$f = (x-1)(x-2)(x-3) = x^3 - 6x^2 + 11 - 6,$$

$$g = (x - 1.00001)(x+3)(x+2) = x^3 + 3.99999x^2 + 0.99995x - 6.00006.$$

An approximate gcd is given by

$$p = x - 1.000005,$$

$$f_1 = (x-2)(x-3) + 10^{-6} = x^2 - 5x + 6.000001,$$

$$g_1 = (x+3)(x+2) + 10^{-6} = x^2 + 5x + 6.000001.$$

Then $\mathcal{D} = 1.298105$, $\varepsilon = 5.660389 \times 10^{-5}$, $C_{sup} = 11.31371$. Theorem 3 gives the following bound on $\alpha(p, f_1, g_1)$:

$$C_{sup}\,\mathcal{D}^2\,\varepsilon = 1.079122 \times 10^{-3}.$$

The bound given in theorem 2 is

$$\frac{1}{16\kappa + 32} = 3.779289 \times 10^{-3}.$$

Then, as the bound of Theorem 3 is smaller than the bound of Theorem 2, we can certify the convergence of Newton-Gauss' method in this case.

**Acknowledgment.** The authors were partially supported by the French ANR DISCO.

## References

[1] B. Beckermann and G. Labahn, When are two numerical polynomials relatively prime? J. Symbolic Comput., 26(6)(1998), 677–689.

[2] D. A. Bini and P. Boito, Structured matrix-based methods for polynomial $\epsilon$-gcd: analysis and comparisons, In ISSAC 2007, 9–16, ACM, New York, 2007.

[3] J.-P. Dedieu and M. Shub, Newton's method for overdetermined systems of equations, Math. Comp., 69(231)(2000), 1099–1115.

[4] J.-P. Dedieu and M.-H. Kim, Newton's method for analytic systems of equations with constant rank derivatives, J. Complexity, 18(1)(2002), 187–209.

[5] I. Z. Emiris, A. Galligo and H. Lombardi, Certified approximate univariate GCDs, J. Pure & Applied Algebra, Special Issue on Algorithms for Algebra, 117 & 118(1997), 229–251.

[6] E. Kaltofen, Z. Yang and L. Zhi, Structured low rank approximation of a Sylvester matrix, Symbolic-numeric computation, Trends Math., 69–83, Birkhäuser, Basel, 2007.

[7] N. K. Karmarkar and Y. N. Lakshman, On approximate GCDs of univariate polynomials, J. Symbolic Comput., 26(6)(1998), 653–666.

[8] J. Nie, J. Demmel and M. Gu, Global minimization of rational functions and the nearest GCDs, J. Global Optim., 40(4)(2008), 697–718.

[9] M.-T. Noda and T. Sasaki, Approximate GCD and its application to ill-conditioned algebraic equations, In Proceedings of the International Symposium on Computational Mathematics, 38(1991), 335–351.

[10] V. Y. Pan, Computation of approximate polynomial GCDs and an extension, Inform. and Comput., 167(2)(2001), 71–85.

[11] J. von zur Gathen and J. Gerhard, Modern Computer Algebra, $2^{nd}$ ed., CUP, Cambridge, UK, 2003.