Corrigé du partiel de M.A.O. Calcul Formel

Vendredi 21 avril 2017
Master 1 M.F.A., Orsay

1. Il s'agit de l'algorithme d'Euclide étendu qui calcule $R_{\ell-1} = \text{pgcd}(A, B)$ et une relation de Bezout $AU_{\ell-1} + BV_{\ell-1} = R_{\ell-1}$. Le coût de ce calcul est $O(\deg A \cdot \deg B)$ opérations arithmétiques.

2. Comme $\deg A > \deg B > 0$, le coût en opérations arithmétiques de la division euclidienne de A par B est $O(\deg B \cdot (\deg A - \deg B))$, donc $O(\deg A \cdot \deg B)$.

3. ```
def euclide_etendu(A, B, K=QQ):
    P = PolynomialRing(K, 'X')
    A, B = P(A), P(B)
    R = [A, B]
    U = [P(1), P(0)]
    V = [P(0), P(1)]
    Q = []
    while R[-1]:
        Q.append(R[-2] // R[-1])
        R.append(R[-2] % R[-1])
        U.append(U[-2] - Q[-1] * U[-1])
        V.append(V[-2] - Q[-1] * V[-1])
        assert(U[-1].degree() == B.degree() - R[-2].degree())
        assert(V[-1].degree() == A.degree() - R[-2].degree())
        assert(R[-1] == A * U[-1] + B * V[-1])
    return R, U, V
```

```
sage: P.<X> = QQ[]
sage: A0 = X^8
sage: B0 = X^7 - X^5 + X^3 - X
```

```
sage: R, U, V = euclide_etendu(A0, B0)
sage: R, U, V
([X^8, X^7 - X^5 + X^3 - X, X^6 - X^4 + X^2, -X, 0],
 [1, 0, 1, -X, -X^6 + X^4 - X^2 + 1],
 [0, 1, -X, X^2 + 1, X^7])
```
```

```
sage: n = len(R)
sage: n
5
```

```
sage: for k in range(n):
....:     print " = A * () + B * ()".format(R[k], U[k], V[k])
....:
X^8 = A * (1) + B * (0)
X^7 - X^5 + X^3 - X = A * (0) + B * (1)
X^6 - X^4 + X^2 = A * (1) + B * (-X)
-X = A * (-X) + B * (X^2 + 1)
0 = A * (-X^6 + X^4 - X^2 + 1) + B * (X^7)
```

4. La matrice $M_j = \begin{bmatrix} 0 & 1 \\ 1 & -Q_j \end{bmatrix}$ convient.

5. Si $j \leq 1$ c'est évident ; sinon on a $\begin{bmatrix} U_{j-1} & V_{j-1} \\ U_j & V_j \end{bmatrix} = M_{j-2}M_{j-3}\dots M_0$ puisque $\begin{bmatrix} U_0 & V_0 \\ U_1 & V_1 \end{bmatrix} = I_2$. En prenant le déterminant on obtient $U_{j-1}V_j - V_{j-1}U_j = \pm 1$ donc U_j et V_j sont premiers entre eux.

6. (*a*) On a $\deg R_\ell = -\infty < \deg R_{\ell-1} < \dots < \deg R_0 = \deg A$ et $\deg R < \deg A$ (puisque $\deg V \geq 0$) donc il existe un entier $r \in \{1, \dots, \ell\}$, et un seul, tel que $\deg R_r \leq \deg R < \deg R_{r-1}$.

   (*b*) Tout d'abord on a
$$\deg(R_r V) = \deg R_r + \deg V \leq \deg R + \deg V < \deg A.$$
   Ensuite, si $r \geq 2$ alors l'expression de $\deg V_{j+2}$ rappelée au début du problème donne
$$\deg(RV_r) < \deg R_{r-1} + (\deg A - \deg R_{r-1}) = \deg A.$$
   Pour $r \in \{0, 1\}$, on a trivialement $\deg(RV_r) \leq \deg R < \deg A$. Finalement on obtient donc dans tous les cas $\deg(R_r V - RV_r) < \deg A$.

   (*c*) On a
$$R_r V - RV_r = (AU_r + BV_r)V - (AU + BV)V_r = A(U_r V - UV_r).$$
   Si $U_r V \neq UV_r$ alors $\deg(U_r V - UV_r) \geq 0$ d'où $\deg(R_r V - RV_r) \geq \deg A$ ce qui contredit le résultat de la question (*b*).

   (*d*) D'après (*c*), V_r divise $U_r V$. En outre V_r est premier avec U_r d'après la question 5. Donc V_r divise V : il existe $S \in \mathbb{K}[X]$ tel que $V = SV_r$. Comme $U_r V = UV_r$ et $V_r \neq 0$ (car $r \geq 1$) on en déduit $U = SU_r$. Il vient alors $R = AU + BV = SR_r$.

7. Comme $\deg R_t < \deg A$ on a $t \geq 1$. En outre on a $BV_t - R_t = -AU_t \equiv 0 \bmod A$, $\deg R_t < k$ et enfin $\deg V_t = \deg A - \deg R_{t-1} \leq \deg A - k$ par définition de t si $t \geq 2$; la majoration $\deg V_1 \leq \deg A - k$ est triviale puisque $V_1 = 1$.

8. On a $k = 4$, $t = 3$, et $(R_3, V_3) = (-X, X^2 + 1) \in \mathcal{E}(A_0, 4)$:

```
sage: R3, V3 = R[3], V[3]
sage: R3, V3
(-X, X^2 + 1)
```

9. (*a*) On a $\deg R_r \leq \deg R < k$ donc $r \geq t$.

   (*b*) La question 6(*d*) fournit $S \in \mathbb{K}[X]$ non nul tel que $U = SU_r$, $V = SV_r$ et $R = SR_r$. Supposons $r > t$. On a $\deg V_t < \deg V_r \leq \deg V$ donc $V - V_t \neq 0$. En outre on a $\deg R < \deg R_{r-1} \leq \deg R_t$ donc $\deg(R - R_t) = \deg R_t$. Enfin on a $\deg V \leq \deg A - k < \deg A - \deg R_t$ et $\deg V_t = \deg A - \deg R_{t-1} < \deg A - \deg R_t$ si $t \geq 2$; la majoration $\deg V_t < \deg A - \deg R_t$ est triviale pour $t = 1$. On peut donc également appliquer la question 6(*d*) à l'identité $R - R_t = A(U - U_t) + B(V - V_t)$, et l'entier de la question 6(*a*) est alors t. On obtient ainsi un polynôme $T \in \mathbb{K}[X]$ tel que $R - R_t = TR_t$, d'où $R = (T + 1)R_t = SR_r$, et de même $(T + 1)U_t = SU_r$ et $(T + 1)V_t = SV_r$. Si un polynôme irréductible $D \in \mathbb{K}[X]$ divise S mais pas $T + 1$, alors il divise U_t et V_t ce qui est impossible d'après la question 5. De même, aucun polynôme irréductible ne peut diviser $T + 1$ sans diviser S. Donc S et $T + 1$ sont associés dans $\mathbb{K}[X]$, et il existe $\alpha \in \mathbb{K}^*$ tel que $R_r = \alpha R_t$; c'est impossible car $\deg R_r < \deg R_t$. On a donc $r = t$.

   Autre solution : La question 6(*d*) fournit $S \in \mathbb{K}[X]$ non nul tel que $U = SU_r$, $V = SV_r$ et $R = SR_r$. On a $\deg V \geq \deg V_r$ (car $S \neq 0$) et $\deg V_r = \deg A - \deg R_{r-1}$ (si $r \geq 2$; si $r = 1$ alors $t = 1$ d'après (*a*) et il n'y a plus rien à démontrer). Comme $(R, V) \in \mathcal{E}(A, k)$ on en déduit $\deg R_{r-1} \geq \deg A - \deg V \geq k$ donc $t > r - 1$, ce qui donne $t = r$ grâce à la question (*a*).

10. Considérons $v_0, \ldots, v_m$ comme des inconnues. La relation (1), écrite pour i allant de 0 à $N - 1 - m$, est alors un système linéaire homogène de $N - m$ équations. Comme $m \geq N/2$, on a $m + 1 > N - m$ donc ce système admet une solution non triviale.

11. Etant donné $(v_0, \ldots, v_m) \in \mathbb{K}^{m+1}$, posons $V(X) = \sum_{i=0}^{m} v_i X^i$; on a alors $\deg V \leq m = N - m$. La relation (1) signifie que pour tout $i \in \{0, \ldots, N - 1 - m\}$ le coefficient de degré $m + i$ du polynôme BV est nul, c'est-à-dire qu'on peut écrire BV sous la forme $R - X^N U$ avec $R, U \in \mathbb{K}[X]$ tels que $\deg R < m$. Cela montre que (1) est vérifiée si et seulement si il existe $R \in \mathbb{K}[X]$ tel que $(R, V) \in \mathcal{E}(X^N, m)$. La question 7 montre qu'il suffit d'appliquer l'algorithme d'Euclide étendu en s'arrêtant à l'étape t pour trouver un tel polynôme $V = V_t \neq 0$, donc une relation de récurrence non triviale. D'après la question 1, cet algorithme nécessite au maximum $O(N^2)$

opérations arithmétiques dans $\mathbb{K}$. En fait la première étape de l'algorithme d'Euclide étendu coûte déjà $O(N^2)$ opérations d'après la question 2, du moins dans le cas où $b_i = 0$ pour tout $i \geq 3N/4$ car on a alors $\deg A - \deg B \geq N/4$. Donc le coût du calcul de V_t n'est pas inférieur à $O(N^2)$ dans le pire des cas.

12. Les b_i sont les coefficients du polynme B_0 des questions 3 et 8. On obtient donc $V = X^2 + 1$ d'après la question 8, et la relation de récurrence est $b_{i+2} + b_{i+4} = 0$ pour tout $i \in \{0, \ldots, 3\}$.

13.
```
sage: B = [3, 1, 4, 1, 5, 9, 2, 6, 5, 3]
sage: len(B)
10

sage: B1 = P(B)
sage: B1
3*X^9 + 5*X^8 + 6*X^7 + 2*X^6 + 9*X^5 + 5*X^4 + X^3 + 4*X^2 + X + 3
sage: A = X^10
sage: A1 = X^10
sage: R, U, V = euclide_etendu(A1, B1)

sage: n = len(R)

sage: for k in range(n):
....:
....:     print "(degree ) = A * (degree ) + B * (degree
)".format(R[k].degree(), U[k].degree(), V[k].degree())
....:
(degree 10) = A * (degree 0) + B * (degree -1)
(degree 9) = A * (degree -1) + B * (degree 0)
(degree 8) = A * (degree 0) + B * (degree 1)
(degree 7) = A * (degree 1) + B * (degree 2)
(degree 6) = A * (degree 2) + B * (degree 3)
(degree 5) = A * (degree 3) + B * (degree 4)
(degree 4) = A * (degree 4) + B * (degree 5)
(degree 3) = A * (degree 5) + B * (degree 6)
(degree 2) = A * (degree 6) + B * (degree 7)
(degree 1) = A * (degree 7) + B * (degree 8)
(degree 0) = A * (degree 8) + B * (degree 9)
(degree -1) = A * (degree 9) + B * (degree 10)

sage: V[6]
-441/10965736*X^5 + 5905431/333095196736*X^4 - 3887415/333095196736*X^3 +
1692999/166547598368*X^2 - 4257855/333095196736*X + 3763053/166547598368
```

```
sage: for i in range(5):
....:     print sum(list(V[6])[5-k]*B[i+k] for k in range(6))
....:
0
0
0
0
0
```

14. Posons $N = 200$ et notons $B = 3 + X + 4X^2 + \dots$ le polynôme de degré 199 dont les coefficients sont les 200 premières décimales de $\pi = 3.14\dots$. Supposons qu'il existe une relation de récurrence linéaire non triviale vérifiée par cette suite. Comme à la question 11 on en déduit un polynôme V de degré ≤ 80 pour lequel il existe $R, U \in \mathbb{K}[X]$ tels que $BV = R - X^{200}U$ avec $\deg R < 80$. Pour tout entier k tel que $80 \leq k \leq 120$ on a alors $(R, V) \in \mathcal{E}(X^{200}, k)$; on choisit $k = 80$. D'après la question 9(b) il existe $S \in \mathbb{K}[X]$ tel que $R = SR_t$ et $V = SV_t$. Or le calcul de V_t montre que $\deg V_t > 80$: c'est impossible car $\deg V \leq 80$ et $V \neq 0$.

```
sage: s = str(pi.n(digits=202)).replace('.', '')[:200]
sage: s
'31415926535897932384626433832795028841971693993751058209749445923078
164062862089986280348253421170679821480865132823066470938446095505
822317253594081284811174502841027019385211055596446229489549303819'


sage: B2 = P([ZZ(c) for c in s])
sage: B2
9*X^199 + X^198 + 8*X^197 + 3*X^196 + 3*X^194 + 9*X^193 + 4*X^192 + 5*X^191
+ 9*X^190 + 8*X^189 + 4*X^188 + 9*X^187 + 2*X^186 + 2*X^185 + 6*X^184 +
4*X^183 + 4*X^182 + 6*X^181 + 9*X^180 + 5*X^179 + 5*X^178 + 5*X^177 + X^175
+ X^174 + 2*X^173 + 5*X^172 + 8*X^171 + 3*X^170 + 9*X^169 + X^168 + 7*X^166
+ 2*X^165 + X^163 + 4*X^162 + 8*X^161 + 2*X^160 + 5*X^158 + 4*X^157 +
7*X^156 + X^155 + X^154 + X^153 + 8*X^152 + 4*X^151 + 8*X^150 + 2*X^149 +
X^148 + 8*X^147 + 4*X^145 + 9*X^144 + 5*X^143 + 3*X^142 + 5*X^141 + 2*X^140
+ 7*X^139 + X^138 + 3*X^137 + 2*X^136 + 2*X^135 + 8*X^134 + 5*X^133 +
5*X^131 + 5*X^130 + 9*X^129 + 6*X^127 + 4*X^126 + 4*X^125 + 8*X^124 +
3*X^123 + 9*X^122 + 7*X^120 + 4*X^119 + 6*X^118 + 6*X^117 + 3*X^115 +
2*X^114 + 8*X^113 + 2*X^112 + 3*X^111 + X^110 + 5*X^109 + 6*X^108 + 8*X^107
+ 8*X^105 + 4*X^104 + X^103 + 2*X^102 + 8*X^101 + 9*X^100 + 7*X^99 + 6*X^98
+ 7*X^96 + X^95 + X^94 + 2*X^93 + 4*X^92 + 3*X^91 + 5*X^90 + 2*X^89 +
8*X^88 + 4*X^87 + 3*X^86 + 8*X^84 + 2*X^83 + 6*X^82 + 8*X^81 + 9*X^80 +
9*X^79 + 8*X^78 + 2*X^76 + 6*X^75 + 8*X^74 + 2*X^73 + 6*X^72 + 4*X^70 +
```

```
6*X^69 + X^68 + 8*X^67 + 7*X^66 + 3*X^64 + 2*X^63 + 9*X^62 + 5*X^61 +
4*X^60 + 4*X^59 + 9*X^58 + 4*X^57 + 7*X^56 + 9*X^55 + 2*X^53 + 8*X^52 +
5*X^51 + X^49 + 5*X^48 + 7*X^47 + 3*X^46 + 9*X^45 + 9*X^44 + 3*X^43 +
9*X^42 + 6*X^41 + X^40 + 7*X^39 + 9*X^38 + X^37 + 4*X^36 + 8*X^35 + 8*X^34
+ 2*X^33 + 5*X^31 + 9*X^30 + 7*X^29 + 2*X^28 + 3*X^27 + 8*X^26 + 3*X^25 +
3*X^24 + 4*X^23 + 6*X^22 + 2*X^21 + 6*X^20 + 4*X^19 + 8*X^18 + 3*X^17 +
2*X^16 + 3*X^15 + 9*X^14 + 7*X^13 + 9*X^12 + 8*X^11 + 5*X^10 + 3*X^9 +
5*X^8 + 6*X^7 + 2*X^6 + 9*X^5 + 5*X^4 + X^3 + 4*X^2 + X + 3

sage: A2 = X^200
sage: A2
X^200

sage: R, U, V = euclide_etendu(A2, B2)
```