KRONECKER MATRICES AND POLYNOMIAL GCDS

Daniel J. Bernstein

19960628 (draft 5)

Abstract. Kronecker matrices are a simple axiomatization of successive convergents to a rational function. This paper develops the basic theory of Kronecker matrices, including the best-approximation property, composition, division, Euclid's algorithm, Lehmer's lemma, the Brent-Gustavson-Yun algorithm, and the Berlekamp-Massey algorithm.

1. Introduction

This paper has two purposes. The first is to show how continued fraction theory for polynomials can be developed from the concept of a **Kronecker matrix**, which characterizes successive convergents to a rational function. The second is to serve as a reference for the Brent-Gustavson-Yun algorithm, which quickly computes any desired convergent, or even the entire continued fraction, for a rational function.

In section 2, I define Kronecker matrices and prove that they are essentially unique at each degree. I also prove a strong best-approximation property.

In section 3, I present a composition law for Kronecker matrices.

In section 4, I prove the existence of Kronecker matrices at every degree. The construction is Euclid's algorithm.

In section 5, I present Lehmer's trick and the Brent-Gustavson-Yun algorithm for constructing Kronecker matrices. Given fast polynomial arithmetic, the Brent-Gustavson-Yun algorithm is much faster than Euclid's algorithm.

In section 6, I explain two applications of Kronecker matrices.

Notation. This paper works with polynomials in one variable, z, over a field. The degree of 0 is $-\infty$. A **constant** means a polynomial of degree at most 0. If p is a polynomial and m is a nonnegative integer, there is a unique polynomial f such that $\deg(p - z^m f) < m$; this polynomial is denoted $\lfloor p/z^m \rfloor$. If $\deg p \geq m$ then $\deg \lfloor p/z^m \rfloor = \deg p - m$; if $\deg p < m$ then $\deg \lfloor p/z^m \rfloor = -\infty$.

2. Kronecker matrices and the best-approximation property

Let a, b be polynomials with $\deg a > \deg b$. For $n \geq 0$, a **Kronecker matrix for (a, b) at degree n** is a matrix $\begin{pmatrix} v & u \\ v' & u' \end{pmatrix}$ such that $vu' - v'u = 1$, $\deg u < \deg u' \leq n$, and $\deg(v'a + u'b) < \deg a - n$.

1991 *Mathematics Subject Classification.* Primary 11Y65. Secondary 11T55.

The author was supported by the National Science Foundation under grant DMS–9600083.

Typeset by $\mathcal{AMS}$-TEX

Theorem 2.2 states a fundamental best-approximation property of Kronecker matrices: $-v/u$ is the closest fraction to b/a with denominator of degree under $\deg u'$. The Kronecker matrix at degree n is essentially unique; see Theorem 2.3. The existence of Kronecker matrices is proven in section 4.

For brevity I will write $\begin{pmatrix} v & u \\ v' & u' \end{pmatrix}$ as $((v,u),(v',u'))$.

Theorem 2.1. *Let a, b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b) at degree n. Then $\deg u' + \deg(va+ub) = \deg a$.*

Thus $\deg(v'a+u'b) < \deg a - n \le \deg(va+ub) < \deg a - \deg u$.

Proof. First $u'(va+ub) - u(v'a+u'b) = (u'v-uv')a = a$. Second $\deg u < n$ and $\deg(v'a+u'b) < \deg a - n$ so $\deg u(v'a+u'b) < \deg a$. Thus $\deg u'(va+ub) = \deg a$. □

Theorem 2.2 (the best-approximation property). *Let a, b be polynomials with $\deg a > \deg b$. Define $D = \deg a$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b). Let f, g be polynomials with $\deg f < \deg u'$ and $\deg(ga+fb) < D - \deg u$. Then there is a polynomial d with $f = ud$ and $g = vd$.*

Proof. Define $c = vf - ug$ and $d = u'g - v'f$, so that $u'c + ud = f$ and $v'c + vd = g$. Define $x = va+ub$ and $x' = v'a+u'b$. Note that $\deg x' < D-n \le D - \deg u' = \deg x$ by Theorem 2.1.

Suppose that $c \ne 0$. Then $\deg u'c \ge \deg u' > \deg f = \deg(u'c+ud)$, so $\deg u'c = \deg ud$; thus $ud \ne 0$ since $u'c \ne 0$. Next $\deg c = \deg d + \deg u - \deg u' < \deg d$ so $\deg cx' < \deg d + \deg x' < \deg dx$. But $ga + fb = dx + cx'$ so $\deg(ga+fb) = \deg dx = \deg d + D - \deg u' = \deg c + D - \deg u \ge D - \deg u$. Contradiction.

Thus $c = 0$, and $(f,g) = (u,v)d$ as claimed. □

Theorem 2.3. *Let a, b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ and $((t,s),(t',s'))$ be Kronecker matrices for (a,b) at degree n. Then $((t,s),(\lambda t',\lambda s')) = ((\lambda v,\lambda u),(v',u'))$ for some invertible constant λ.*

Proof. Write $D = \deg a$.

By Theorem 2.1, $\deg(t'a+s'b) < D - n \le \deg(va+ub) < D - \deg u$. Suppose that $\deg s' < \deg u'$. By Theorem 2.2, there is a polynomial d with $s' = ud$ and $t' = vd$. Then $t'a + s'b = d(va+ub)$ so $\deg d = \deg(t'a+s'b) - \deg(va+ub) < 0$; thus $d = 0$, so $s' = t' = 0$, contradicting $ts' - t's = 1$.

Similarly $\deg u' < \deg s'$ is impossible. Thus $\deg u' = \deg s'$.

Next $\deg s < \deg s' = \deg u'$ and, by Theorem 2.1, $\deg(ta+sb) = D - \deg s' = D - \deg u' < D - \deg u$. By Theorem 2.2, there is a polynomial λ with $s = u\lambda$ and $t = v\lambda$.

Next $\lambda(vs'-t'u) = ts'-t's = 1$ so $a = \lambda(vs'-t'u)a = \lambda(s'(va+ub) - u(t'a+s'b))$ and $b = \lambda(vs'-t'u)b = \lambda(v(t'a+s'b) - t'(va+ub))$. Thus

$$\begin{aligned} v'a + u'b &= \lambda((v's'-u't')(va+ub) + (vu'-v'u)(t'a+s'b)) \\ &= \lambda(v's'-u't')(va+ub) + \lambda(t'a+s'b). \end{aligned}$$

But $\deg(v'a+u'b)$ and $\deg \lambda(t'a+s'b)$ are both under $D-n$, while $\deg(va+ub) \ge D-n$; thus $v's'-u't' = 0$. Finally $u' = \lambda(vs'-t'u)u' = \lambda(vs'u'-v's'u) = \lambda s'(vu'-v'u) = \lambda s'$ and $v' = \lambda(vs'-t'u)v' = \lambda(vu't'-t'v'u) = \lambda t'(vu'-v'u) = \lambda t'$. □

Notes. The proof of Theorem 2.2 is due in essence to Lagrange, who showed in [7] that each convergent to the continued fraction for a rational number β is an optimal approximation to β. Kronecker proved the same theorem for rational functions in [6]. Kronecker's proof relies on only a few properties of successive convergents; my definition of a Kronecker matrix is simply a statement of those properties.

Lagrange also showed that any good enough approximation to β must arise from the continued fraction for β. For polynomials, "good enough" means the same as "optimal," and Lagrange's technique implies Theorem 2.3. The observation that Theorem 2.3 can be proven directly, without continued fractions—in particular, without polynomial division—appears to be new.

3. Composition of Kronecker matrices

Say $((v,u),(v',u'))$ is a Kronecker matrix for (a,b). Define $x = va + ub$ and $x' = v'a + u'b$. **Composition** says how to obtain further Kronecker matrices for (a,b) given Kronecker matrices for (x,x').

Theorem 3.1. *Let a,b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b). If $u \neq 0$ then $\deg v < \deg v'$.*

Proof. By assumption $\deg u \geq 0$ so $\deg u' \geq 1$. If $v \neq 0$ then $\deg vu' \geq 1 > 0 = \deg(vu' - v'u)$ so $\deg vu' = \deg v'u$ so $\deg v = \deg v' + \deg u - \deg u' < \deg v'$.

If $v = 0$ then $v' \neq 0$ so $\deg v = -\infty < \deg v'$. □

Theorem 3.2. *Let a,b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b) at degree n. Then $\deg v' \leq \deg u' + \deg b - \deg a$.*

Proof. If $v' = 0$ then $\deg v' = -\infty < \deg u' + \deg b - \deg a$.

If $v \neq 0$ then $\deg v'a \geq \deg a \geq \deg a - n > \deg(v'a + u'b)$ so $\deg v'a = \deg u'b$ so $\deg v' = \deg u' + \deg b - \deg a$. □

Theorem 3.3. *Let a,b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b). If $u = 0$ then $v' = 0$ and $\deg u' = \deg v = 0$.*

Proof. $vu' = 1$ so $\deg v = \deg u' = 0$. By Theorem 3.2, $\deg v' \leq \deg b - \deg a < 0$. □

Theorem 3.4. *Let a,b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b). Then $\deg v' < \deg u'$ and $\deg v \leq \deg u'$.*

Proof. If $u = 0$ then $\deg v' < 0 = \deg v = \deg u'$ by Theorem 3.3.

If $u \neq 0$ then $\deg v < \deg v'$ by Theorem 3.1; and $\deg v' \leq \deg u' + \deg b - \deg a < \deg u'$ by Theorem 3.2. □

Theorem 3.5 (composition). *Let a,b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b). Define $x = va + ub$ and $x' = v'a + u'b$. Let $((t,s),(t',s'))$ be a Kronecker matrix for (x,x') at degree m. Then the product $((t,s),(t',s'))((v,u),(v',u'))$ is a Kronecker matrix for (a,b) at degree $m + \deg a - \deg x$.*

Proof. (1) The original matrices have determinant 1, so their product does too.

(2) By Theorem 3.4, $\deg t \le \deg s'$. Thus $\deg tu \le \deg s'u < \deg s'u'$. Also $\deg su' < \deg s'u'$. Thus $\deg(tu + su') < \deg s'u' = \deg s' + \deg a - \deg x \le m + \deg a - \deg x$ by Theorem 2.1.

(3) $\deg(t'x + s'x') < \deg x - m = \deg a - (m + \deg a - \deg x)$. $\square$

4. Euclid's algorithm

There is a Kronecker matrix for (a, b) at every degree $n \ge 0$, by Theorem 4.3 below. The construction combines **division**, as expressed in Theorem 4.2, with composition.

Theorem 4.1. *Let a, b be polynomials with $\deg a > \deg b$. If $n < \deg a - \deg b$ then $((1, 0), (0, 1))$ is a Kronecker matrix for (a, b) at degree n.*

In particular, $((1, 0), (0, 1))$ is a Kronecker matrix for $(a, 0)$ at every degree.

Proof. $1 \cdot 0 - 0 \cdot 1 = 1$; $\deg 0 = -\infty < 0 = \deg 1 \le n$; $\deg b < \deg a - n$. $\square$

Theorem 4.2 (division). *Let a, b be polynomials with $\deg a > \deg b$. Let q, r be polynomials with $a = bq - r$ and $\deg r < \deg b$. Define $m = \deg a - \deg b$. Then $((0, 1), (-1, q))$ is a Kronecker matrix for (a, b) at degree m.*

Proof. $0 \cdot q - 1(-1) = 1$; $\deg 1 = 0 < m = \deg q$; $\deg r < \deg b = \deg a - m$. $\square$

Theorem 4.3. *Let a, b be polynomials with $\deg a > \deg b$. Then, for any $n \ge 0$, there is a Kronecker matrix for (a, b) at degree n.*

Proof. Define $m = \deg a - \deg b$.

If $n < m$ then $((1, 0), (0, 1))$ works by Theorem 4.1.

If $n \ge m$ then $b \ne 0$ so there are polynomials q, r with $a = bq - r$ and $\deg r < \deg b$. By Theorem 4.2, $((0, 1), (-1, q))$ is a Kronecker matrix for (a, b) at degree m. By induction there is a Kronecker matrix for (b, r) at degree $n - m < n$. Thus, by Theorem 3.5, there is a Kronecker matrix for (a, b) at degree $n - m + \deg a - \deg b = n$. $\square$

Notes. The construction in Theorem 4.3 is Euclid's algorithm: divide a by b, divide b by the remainder, and so on; from the quotients q build the matrices $((0, 1), (-1, q))$; multiply to obtain the desired Kronecker matrix. Simon Stevin observed in 1585 that Euclid's algorithm can be applied to polynomials over a field.

5. Lehmer's lemma

This section describes a different way to construct a Kronecker matrix for (a, b) at degree n. For $n < \deg a - \deg b$, the identity matrix works by Theorem 4.1. For $n \ge \deg a - \deg b$, there are two possibilities, stated in Theorem 5.3 and Theorem 5.6. The construction uses **Lehmer's lemma**, as expressed in Theorem 5.2, together with division and composition.

Theorem 5.1. *Let a, b be polynomials with $\deg a > \deg b$. Let n be an integer with $0 \le n \le \deg a$. Define $i = \deg a - n$. Define $f = \lfloor a/z^i \rfloor$ and $g = \lfloor b/z^i \rfloor$. Then $\deg f = n > \deg g$.*

Proof. By assumption $\deg a \ge i$ so $\deg f = \deg a - i = n$; and $\deg g \le \deg b - i < \deg a - i$. $\square$

Theorem 5.2 (Lehmer's lemma). *In the situation of Theorem 5.1, let m be an integer with $0 \le m \le n/2$, and let $((v,u),(v',u'))$ be a Kronecker matrix for (f,g) at degree m. Then $((v,u),(v',u'))$ is a Kronecker matrix for (a,b) at degree m.*

Thus the Kronecker matrix for (a,b) at degree m is determined by the first $2m+1$ coefficients of a and the corresponding coefficients of b. In practice m is always selected as $\lfloor n/2 \rfloor$.

Proof. Write $D = \deg a$. By assumption $2m \le n = D - i$ so $m + i \le D - m$. Now $v'a+u'b = v'(z^i f+a-z^i f)+u'(z^i g+b-z^i g) = z^i(v'f+u'g)+v'(a-z^i f)+u'(b-z^i g)$. It suffices to show that $z^i(v'f+u'g)$, $v'(a-z^i f)$, and $u'(b-z^i g)$ all have degree smaller than $D-m$: (1) $\deg(v'f+u'g) < n-m = D-i-m$ so $\deg z^i(v'f+u'g) < D-m$. (2) $\deg u' \le m$ so $\deg u'(b-z^i g) < m+i \le D-m$. (3) $\deg v' < \deg u' \le m$ by Theorem 3.4 so $\deg v'(a-z^i f) < m+i \le D-m$. $\square$

Theorem 5.3. *In the situation of Theorem 5.2, define $x' = v'a+u'b$, and assume that $\deg x' < i$. Then $((v,u),(v',u'))$ is a Kronecker matrix for (a,b) at degree n.*

Proof. $\deg(v'a+u'b) = \deg x' < i = \deg a - n$ by assumption. $\square$

Theorem 5.4. *In the situation of Theorem 5.2, define $x' = v'a+u'b$, and assume that $\deg x' \ge i$. Define $x = va+ub$. Let q and r be polynomials such that $x = x'q-r$ and $\deg r < \deg x'$. Then the product $((0,1),(-1,q))((v,u),(v',u'))$ is a Kronecker matrix for (a,b) at degree $\deg a - \deg x'$.*

Proof. By Theorem 2.1, $\deg x > \deg x'$. By Theorem 4.2, $((0,1),(-1,q))$ is a Kronecker matrix for (x,x') at degree $\deg x - \deg x'$. Thus, by Theorem 3.5, $((0,1),(-1,q))((v,u),(v',u'))$ is a Kronecker matrix for (a,b) at degree $\deg x - \deg x' + \deg a - \deg x' = \deg a - \deg x'$. $\square$

Theorem 5.5. *In the situation of Theorem 5.4, define $k = \max\{0, 2i - \deg x'\}$. Then $0 \le k \le \deg x'$.*

Proof. $\deg x' \ge i$ by assumption so $\deg x' \ge 2i - \deg x'$. $\square$

Theorem 5.6. *In the situation of Theorem 5.5, define $F = \lfloor x'/z^k \rfloor$, $G = \lfloor r/z^k \rfloor$, and $j = \deg x' - i$. Then $\deg F > \deg G$. Furthermore, let $((t,s),(t',s'))$ be a Kronecker matrix for (F,G) at degree j. Then the product*

$$\begin{pmatrix} t & s \\ t' & s' \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & q \end{pmatrix} \begin{pmatrix} v & u \\ v' & u' \end{pmatrix}$$

is a Kronecker matrix for (a,b) at degree n.

Proof. I will show that $((t,s),(t',s'))$ is a Kronecker matrix for (x',r) at degree j. Then, by Theorem 3.5, $((t,s),(t',s'))((0,1),(-1,q))((v,u),(v',u'))$ is a Kronecker matrix for (a,b) at degree $j + \deg a - \deg x' = \deg a - i = n$ as claimed.

Easy case: $k = 0$. Then $(F,G) = (x',r)$ so there is nothing to prove.

Hard case: $k = 2i - \deg x'$. In Theorem 5.1 and Theorem 5.2, substitute $x', r, F, G, k, j, t, s, t', s', \deg x' - k$ for $a, b, f, g, i, m, v, u, v', u', n$ respectively. Then, by Theorem 5.1, $\deg F = \deg x' - k > \deg G$. Note that $2j = 2\deg x' - 2i = \deg x' - k = \deg F$. Thus, by Theorem 5.2, $((t,s),(t',s'))$ is a Kronecker matrix for (x',r) at degree j. $\square$

Notes. The construction in Theorem 5.6 has a long and checkered history.

Lehmer observed in [8] that the first few iterations of Euclid's algorithm are determined by the first few digits of the inputs. With fast polynomial multiplication and division, and with optimal parameter choices, Lehmer's algorithm produces $\gcd\{a, b\}$ in essentially linear time.

Unfortunately, Lehmer did not know about fast multiplication. Schönhage, in [11], was the first to point out that $\gcd\{a, b\}$ can be computed quickly. Schönhage also observed that the entire continued fraction for b/a can be computed at about the same speed. (Every matrix is built up as a product of matrices $((0,1),(-1,q))$. The q's are the quotients in the continued fraction.)

Both Lehmer and Schönhage focused on integers. In [9], Moenck translated Schönhage's algorithm from integers to polynomials, eliminating many boundary cases that do not show up for polynomials. Moenck also claimed, incorrectly, that his algorithm would work for integers.

Moenck's algorithm was then repeated and oversimplified by Aho, Hopcroft, and Ullman in [2]. According to [3], the algorithm stated in [2] does not always successfully compute Kronecker matrices.

In [3], Brent, Gustavson, and Yun pointed out a generalization and two speedups of Moenck's algorithm. See below for a discussion of the generalization. The first speedup was to apply Lehmer's lemma to the second recursive Kronecker call—the construction of $((t, s),(t', s'))$ in Theorem 5.6—as well as the first. (To see the algorithm without this speedup, replace k by 0 in Theorem 5.6.) The second speedup is based on the observation that, after computing a Kronecker matrix $((v, u),(v', u'))$ for (a, b), one almost always calculates $va + ub$ and $v'a + u'b$. It is worth integrating this calculation into each of the Kronecker matrix constructions to take advantage of common subexpressions. (For Euclid's algorithm, this speedup was already standard practice. See [5, page 325].)

To explain how Moenck's algorithm was generalized, I'll introduce a bit of terminology: a **middle** Kronecker matrix for (a, b) means one at degree $\lfloor(\deg a)/2\rfloor$, and a **final** Kronecker matrix for (a, b) means one at degree $\deg a$. Notice that, for middle computations, both of the recursive Kronecker calls are also middle: m is always taken as $\lfloor(\deg f)/2\rfloor$ in Theorem 5.2, and $k = 2i - \deg x'$ so $j = (\deg F)/2$ in Theorem 5.6. On the other hand, for final computations, the first recursive call is middle while the second is final: $i = 0$ so $k = 0$ and $j = \deg x' = \deg F$.

Moenck was interested in computing a final Kronecker matrix so as to compute $\gcd\{a, b\}$; see Theorem 6.1 below. He stated an algorithm for middle Kronecker matrices, which called itself twice, and an algorithm for final Kronecker matrices, which called the middle algorithm and then called itself.

The Brent-Gustavson-Yun algorithm can compute any desired Kronecker matrix, not just middle and final matrices. The generalized algorithm was neither stated nor proven in [3]. According to the rough outline in [3], there is a "pre-middle" piece and a "post-middle" piece. In my description I have unified these two pieces. My version should be slightly faster than the original Brent-Gustavson-Yun algorithm in the "post-middle" range.

In [10], much later than but independently of [3], Montgomery stated and proved a similar generalization of Moenck's algorithm, including a "pre-middle" algorithm with the second Brent-Gustavson-Yun speedup. It is interesting to observe that

Montgomery's theorem makes no reference to continued fractions; Montgomery showed that the result is (in my language) a Kronecker matrix.

6. Applications of Kronecker matrices

In this section I survey the most common applications of Kronecker matrices: computing greatest common divisors and finding linear recurrences.

Theorem 6.1. *Let a, b be polynomials with $\deg a > \deg b$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (a,b) at degree n. If $n \ge \deg a$ then $va+ub$ is a greatest common divisor of $\{a,b\}$.*

Proof. By assumption $\deg(v'a+u'b) < \deg a - n \le 0$ so $v'a+u'b = 0$. Thus $a = u'(va+ub)$ and $b = v'(va+ub)$. $\square$

Theorem 6.2. *Let b be a polynomial with $\deg b < 2n$. Let f be a polynomial with $0 \le \deg f \le n$ such that coefficient k of fb is 0 for $\deg f \le k < 2n$. Let $((v,u),(v',u'))$ be a Kronecker matrix for (z^{2n}, b) at degree n. Then $\deg u' \le \deg f$, and coefficient k of $u'b$ is 0 for $\deg u' \le k < 2n$.*

In other words, if there is any recurrence of degree at most n for the lowest $2n$ coefficients of b, then u' is a recurrence of minimal degree.

Proof. By assumption $fb \equiv h \pmod{z^{2n}}$ for some polynomial h with $\deg h < \deg f$. Say $h = gz^{2n} + fb$.

Define $x = vz^{2n} + ub$ and $x' = v'z^{2n} + u'b$. By Theorem 2.1, $\deg x' < n \le \deg x$.

Note that $\deg h < n < 2n - \deg u$. Suppose that $\deg f < \deg u'$. By Theorem 2.2, there is a polynomial d with $(f,h) = (u,x)d$. But f is nonzero, so d is nonzero, so $\deg h \ge \deg x \ge n$; contradiction. Thus $\deg f \ge \deg u'$.

Suppose that $\deg x' \ge \deg u'$. Find polynomials q, r with $x = qx' - r$, $\deg r < \deg x'$. By Theorem 4.2, $((0,1),(-1,q))$ is a Kronecker matrix for (x,x') at degree $\deg x - \deg x'$. Define $t' = qv' - v$ and $s' = qu' - u$. Then $((v',u'),(t',s')) = ((0,1),(-1,q))((v,u),(v',u'))$. By Theorem 3.5, $((v',u'),(t',s'))$ is a Kronecker matrix for (z^{2n}, b) at degree $2n - \deg x'$. By Theorem 2.1, $\deg s' = 2n - \deg(v'z^{2n} + u'b) = 2n - \deg x' > n \ge \deg f$. Furthermore $\deg(gz^{2n} + fb) = \deg h < \deg f \le n \le 2n - \deg u'$. By Theorem 2.2, there is a polynomial d with $(f,h) = (u',x')d$. But then $\deg x' - \deg u' = \deg h - \deg f < 0$. Contradiction.

Thus $\deg x' < \deg u'$. For $k < 2n$, coefficient k of $u'b$ is the same as coefficient k of x', which is 0 for $k \ge \deg u'$. $\square$

Notes. Euclid's algorithm for the construction in Theorem 6.2, with the standard algorithm for polynomial division, and with all polynomials reversed from left to right, is generally known as the "Berlekamp-Massey algorithm." See [4] for some background and [12] for a crucial application.

One can carry out the construction in Theorem 6.2 without knowing whether there is a small recurrence for the coefficients of b. If u' is a recurrence—i.e., if $\deg x' < \deg u'$—then, by Theorem 6.2, it is the minimal recurrence. Otherwise, by Theorem 6.2 again, every recurrence must have degree larger than n. In the latter case, one can find the minimal recurrence by doing one more division step, as in the proof of Theorem 6.2.

References

1. Alfred V. Aho (chairman), *Conference Record of the Fifth Annual ACM Symposium on the Theory of Computing*, Association for Computing Machinery, New York, 1973.
2. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, Reading, Massachusetts, 1974.
3. Richard P. Brent, Fred G. Gustavson, David Y. Y. Yun, *Fast solution of Toeplitz systems of equations and computation of Padé approximants*, Journal of Algorithms **1** (1980), 259–295.
4. Jean-Louis Dornstetter, *On the equivalence between Berlekamp's and Euclid's algorithms*, IEEE Transactions on Information Theory **33** (1987), 428–431.
5. Donald E. Knuth, *The Art of Computer Programming, volume 2: Seminumerical Algorithms*, 2nd edition, Addison-Wesley, Reading, Massachusetts, 1981.
6. Leopold Kronecker, *Monatsberichte Königl. Preuß. Akad. Wiss.*, 1881, pp. 535–600.
7. Joseph L. Lagrange (1798).
8. Derrick H. Lehmer, American Mathematical Monthly **45** (1938), 227–233.
9. Robert T. Moenck, *Fast computation of GCDs*, in [1], 142–151.
10. Peter L. Montgomery, *An FFT extension of the elliptic curve method of factorization*, Ph.D. thesis, University of California at Los Angeles, 1992.
11. Arnold Schönhage, *Schnelle Berechnung von Kettenbruchentwicklugen*, Acta Informatica **1** (1971), 139–144.
12. Douglas H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Transactions on Information Theory **32** (1986), 54–62.

Department of Mathematics, Statistics, and Computer Science, The University of Illinois at Chicago, Chicago, IL 60607–7045

E-mail address: djb@math.uic.edu