MATHEMATICS OF COMPUTATION
Volume 67, Number 224, October 1998, Pages 1665–1678
S 0025-5718(98)00973-9

EUCLID'S ALGORITHM AND THE LANCZOS METHOD OVER FINITE FIELDS

JEREMY TEITELBAUM

ABSTRACT. This paper shows that there is a close relationship between the Euclidean algorithm for polynomials and the Lanczos method for solving sparse linear systems, especially when working over finite fields. It uses this relationship to account rigorously for the appearance of self-orthogonal vectors arising in the course of the Lanczos algorithm. It presents an improved Lanczos method which overcomes problems with self-orthogonality and compares this improved algorithm with the Euclidean algorithm.

INTRODUCTION

The Lanczos method is an iterative algorithm for solving linear systems of the form $Ax = b$, where A is a square symmetric matrix and b is a known vector. In its original formulation, A was a matrix with real entries. Recently, however, the algorithm has been applied to solve the large, but very sparse, linear systems over finite fields which arise in the final stages of sieve methods for factoring integers and solving discrete logarithm problems. In this situation, the algorithm often succeeds in producing a solution, but it is also possible that the method will fail, even when the matrix A is nonsingular and a solution does in fact exist. This failure occurs when the algorithm encounters a vector v which is self-orthogonal with respect to the inner product defined by A.

Several authors have devised methods for overcoming the failure of the Lanczos method. Over finite fields, and $\mathbf{F}_2$ in particular, Coppersmith ([C1]) and Montgomery ([M]) describe block versions of the Lanczos algorithm which work with subspaces rather than individual vectors; in addition to avoiding failures, these algorithms applied to blocks of size N achieve an N-fold speedup over the original method. Coppersmith, and to a lesser extent Montgomery as well, also employ "look-ahead" techniques to enable the algorithm to continue beyond problems caused by self-orthogonality.

Despite the great practical success of the Lanczos method, even over the field with two elements, the literature lacked a theoretical explanation of why the Lanczos method works over finite fields and how likely the various sorts of failures are. In this note, we reconsider the theory of the Lanczos algorithm over finite fields. We show a close relationship between the Lanczos algorithm and the Euclidean algorithm for polynomials.

Received by the editor February 8, 1996.
1991 *Mathematics Subject Classification.* Primary 11Y16, 65F10, 15A33.
The author is supported by the National Science Foundation.

Using our Euclidean interpretation of the Lanczos method, we are able to account rigorously for the occurrence of self-orthogonal vectors. We also consider an improved version of the Lanczos algorithm which begins exactly like the usual Lanczos but will always either produce a solution to $Ax = b$ or construct an element of the cyclic A-subspace generated by b which is orthogonal to this entire subspace. Our improved Lanczos algorithm is similar to a (nonblock) version of the "look-ahead" methods discussed by Coppersmith [C1], put into a convenient form for comparison with the Euclidean algorithm. We also remark that our improved Lanczos is related to methods for handling "non-normal" Pade approximations as discussed in ([B]).

The other standard method for solving linear systems over finite fields is known as Wiedemann's algorithm ([W]). Wiedemann's algorithm exploits the Berlekamp-Massey algorithm, also well known to be related to Euclid's algorithm ([D]). Thus one aspect of our results is to show that the Lanczos method and Wiedemann's method are members of the same family of algorithms.

In addition, Coppersmith has considered the behavior of a "block" Berlekamp-Massey algorithm in [C2]. Therefore, although our results directly explain the sources and likelihood of failure only for the nonblock Lanczos method, by connecting the method to the Euclidean algorithm we reduce the problem of understanding the block versions to understanding the Euclidean algorithm applied to polynomials with matrix coefficients—a problem very close to that considered by Coppersmith.

In Section 1 of the paper, we review the Lanczos method. Section 2 relates Lanczos to the Euclidean algorithm, Section 3 describes our improved version of the Lanczos method, and Section 4 relates the improved version to Euclid.

I would like to thank Dan Bernstein for teaching me the Berlekamp-Massey algorithm and at least five other "Euclidean" algorithms, an education which led to the ideas in this paper, and Don Coppersmith for his comments on the preprint.

1. The Lanczos method

We begin by describing the Lanczos method in its original formulation. Suppose that A is a symmetric $n \times n$ matrix with entries in a field $\mathbf{F}$, and suppose that b is a nonzero column vector with n entries. Let us write $[x, y]$ for the usual inner product and (x, y) for the inner product determined by A; in explicit terms, $[x, y] = x^t y$ and $(x, y) = x^t A y$. If $(b, b) = 0$, then the algorithm fails immediately; otherwise initialize $w_0 = b$ and

$$w_1 = Aw_0 - \frac{(Aw_0, w_0)}{(w_0, w_0)} w_0.$$

The main iterative step is repeated from $i = 1$ while (w_i, w_i) is nonzero:

$$w_{i+1} = Aw_i - \frac{(Aw_i, w_i)}{(w_i, w_i)} w_i - \frac{(Aw_i, w_{i-1})}{(w_{i-1}, w_{i-1})} w_{i-1}.$$

When a non-zero w_i is obtained with $(w_i, w_i) = 0$ the algorithm fails; if $w_i = 0$ the algorithm has succeeded and the solution x is recovered by the formula

$$x = \sum_{j=0}^{i-1} \frac{[b, w_j]}{(w_j, w_j)} w_j.$$

2. Lanczos and Euclid

We reformulate the Lanczos algorithm in order to better understand its operation. We view $V = \mathbf{F}^n$ as a module over the polynomial ring $\mathbf{F}[T]$, with T acting by A. The element b generates an $\mathbf{F}[T]$ submodule K of $\mathbf{F}^n$. We let R denote the quotient ring $\mathbf{F}[T]/\mathrm{Ann}(b)$ so that K is free of rank one over R. We let $P(T)$ be the monic generator of $\mathrm{Ann}(b)$, and we let m be the degree of P and the dimension of K.

We begin with a simple lemma which will be useful in our analysis.

Lemma 1. *Suppose that K and L are cyclic submodules of V, and that the annihilators of K and L are relatively prime. Then K and L are $(\cdot,\cdot)$-orthogonal.*

Proof. Let p and q be the respective annihilators of K and L. Write $xp + yq = 1$. Then

$$(k, l) = ((xp + yq)k, l) = (yqk, l) = (yk, ql) = 0.$$

□

Definition 2. The pair $\{A, b\}$ is *degenerate* if the restriction to K of the bilinear form $(\cdot,\cdot)$ determined by A is degenerate.

Unfortunately, it is possible for the matrix A to be invertible, and the pair $\{A, b\}$ degenerate. For example, suppose that F has characteristic 2, that A is the identity matrix, and that b is the vector $(1, 1)^t$. The inner product determined by A, restricted to the one-dimensional space generated by b, is identically zero.

One might hope that, for fixed A, at least some vector b has the property that $\{A, b\}$ is nondegenerate. As we see from the following proposition, this is true if the characteristic of $\mathbf{F}$ is not 2.

Proposition 3. *Suppose that the characteristic of $\mathbf{F}$ is not 2 and that A is invertible. Then there exist nondegenerate vectors.*

Proof. Let $Q(T)$ be the minimal polynomial of A acting on V. By Lemma 1, we reduce to the case $Q(T) = f(T)^r$ where f is an irreducible polynomial and r an integer. Let $V[i]$ be the subspace of V killed by $f^i(A)$. Notice that $f^{r-1}(A)V$ is orthogonal to $V[r-1]$. By nondegeneracy of the pairing on all of V, it follows that the induced pairing between $f^{r-1}(A)V$ and $V/V[r-1]$ is nondegenerate. However, since $V/V[r-1]$ is isomorphic to $f^{r-1}(A)V$, we view this pairing as a symmetric nondegenerate form $\langle,\rangle$ on $V/V[r-1]$; explicitly, this pairing is given by $\langle u, v\rangle = (u, f^{r-1}(A)v)$. Since the characteristic is different from two, we may find a vector w such that $\langle w, w\rangle = (w, f^{r-1}(A)w)$ is not zero. Now let M be the cyclic subspace generated by w. Any nonzero element x of M can be written $x = f^i(A)h(A)w$ where $h(T)$ is prime to $f(T)$ and $i < r$. Then we can find a polynomial $b(T)$ so that $f^i(T)h(T)b(T) = f^{r-1}(T) \pmod{(f^r(T))}$. Therefore

$$(x, b(A)w) = (w, f^{r-1}(A)w) \neq 0.$$

This shows that the pair $\{A, w\}$ is nondegenerate. □

The restriction to characteristic different from 2 in this proposition is essential. Suppose that $A \in M_4(\mathbf{F}_2)$ is the matrix

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

Then every cyclic subspace of $\mathbf{F}_2^4$ under the action of A is degenerate. To see this, notice first that $A^2 = 1$, so that A is invertible. If we choose any nonzero vector

$$v = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

then the cyclic subspace K generated by v is spanned by v and Av. If $v = Av$, then $v = (a, b, b, a)^t$ for some a and b, and so $(v, v) = 0$. If v and Av are independent, a direct calculation shows that the inner product determined by A, restricted to the span of v and Av, satisfies

$$(v, v) = (Av, v) = (Av, Av) = a^2 + b^2 + c^2 + d^2,$$

and so $(A + 1)v$ belongs to the kernel of $(\cdot, \cdot)$ on K. Thus K is always degenerate in this case.

To completely understand the behavior of the original Lanczos algorithm and the improved Lanczos we present below, we need to determine the probability that a randomly chosen pair of $\{A, b\}$ is nondegenerate. We have been unable to do this. However, the following proposition implies that $\{A, b\}$ is nondegenerate if the characteristic polynomial of A is square-free, which indicates that in some sense "general" pairs $\{A, b\}$ are nondegenerate.

Proposition 4. *Let $Q_A(T)$ be the characteristic polynomial of A. Suppose that that $P(T)$, the annihilator of b, is relatively prime to T and to $Q_A(T)/P(T)$. Then the pair $\{A, b\}$ is nondegenerate.*

Proof. By Lemma 1, cyclic factors of V belonging to relatively prime divisors of $Q_A(T)$ are orthogonal. This, together with our assumptions on $P(T)$, means that if $x \in K$ is $(,)$-orthogonal to all of K, it is $(,)$-orthogonal to all of V. If $(x, v) = 0$ for all $v \in V$, then $[x, Av] = [Ax, v] = 0$ for all $v \in V$. But the usual dot product is obviously nondegenerate on V, so $Ax = 0$. Since $P(T)$ is prime to T, A is invertible on K, so $x = 0$. □

Abusing notation somewhat, we let $(\cdot, \cdot)$ be the bilinear form on $\mathbf{F}[T]$ defined by $(u, v) = (ub, vb)$. We also observe that this bilinear form has the property $(pu, v) = (u, pv)$ for all $p \in \mathbf{F}[T]$.

Definition 5. Define a formal differential form in $\mathbf{F}[[T]]dT/T$ by the formula

$$B(T)\frac{dT}{T} = \sum_{n=0}^{\infty} (1, T^n)\frac{dT}{T^{n+1}}.$$

The differential form $B(T)\frac{dT}{T}$ captures all of the information in the pairing $(\cdot, \cdot)$.

Definition 6. We denote by $\mathrm{ord}_{T=\infty}$ the valuation on $\mathbf{F}(T)$ defined by

$$\mathrm{ord}_{T=\infty}(P/Q) = \mathrm{degree}(Q) - \mathrm{degree}(P).$$

If $f(T)dT$ is a differential form over $\mathbf{F}(T)$, then we define

$$\mathrm{ord}_{T=\infty}(f(T)dT) = \mathrm{ord}_{T=\infty}(f) - 2.$$

Finally, we let $\mathrm{Res}_{T=\infty} f(T)dT$ be the coefficient of dT/T in the Laurent series expansion of $f(T)dT$ in powers of T and $1/T$. In each case we use the same notation for the natural extension of $\mathrm{ord}_{T=\infty}$ to the field of Laurent series in $1/T$ over $\mathbf{F}$.

Lemma 7. *Let p and q be elements of $\mathbf{F}[T]$. Then*

$$(p, q) = \mathrm{Res}_{T=\infty} pqB(T)\frac{dT}{T}.$$

Proof. Since $(T^m, T^n) = (1, T^{m+n})$, and the residue pairing is $\mathbf{F}$-linear, it suffices to verify this for the pairings $(1, T^m)$, where it is obvious. □

In particular, the differential form $B(T)dT/T$ has information on the minimal polynomial of A.

Lemma 8. *The differential form $B(T)dT/T$ is a rational differential form with denominator a divisor of $P(T)$; in other words, there is a polynomial $H(T)$ such that*

$$P(T)B(T)dT/T - H(T)dT = 0.$$

Proof. We have $(u, P(T)v) = 0$ for all u and v. Writing $P(T) = \sum_{k=0}^{m} a_k T^k$, with $a_m = 1$, we see that

$$P(T)B(T)\frac{dT}{T} = \sum_{k=-m}^{\infty} b_k \frac{dT}{T^{k+1}}$$

with $b_k = \sum_{j=0}^{m} a_j (1, T^{k+j})$, where we adopt the convention that $(1, T^r) = 0$ when $r < 0$. When $k \geq 0$, we see that $b_k = (1, P(T)T^k) = 0$, so only those terms with $k \leq -1$ survive; thus $P(T)B(T)dT/T$ is indeed a polynomial in T. □

Lemma 9. *Let $D(T)$ be the polynomial $P(T)/gcd(P(T), TH(T))$. Then $D(T)$ generates the radical of the bilinear form $(\cdot, \cdot)$.*

Proof. A polynomial $Q(T)$ belongs to the radical of $(\cdot, \cdot)$ if and only if $(Q(T), T^m)$ is zero for all $m \geq 0$. If $Q(T)$ has this property, then by the argument in the proof of Lemma 8, there is a polynomial $G(T)$ so that $Q(T)B(T)dT/T = G(T)dT$. Put another way, $B(T) = TG(T)/Q(T)$. But the fraction $B(T) = TH(T)/P(T)$ has denominator $D(T)$ in lowest terms, so $Q(T)$ is a multiple of $D(T)$. □

Let us now reconsider the Lanczos algorithm. We apply the Lanczos method to polynomials, using the inner product $(\cdot, \cdot)$, beginning with $w_0 = 1$ and $w_1 = T - (T, 1)/(1, 1)$. The iteration sets

$$w_{i+1} = (T - \alpha_i)w_i - \beta_i w_{i-1},$$

where α_i and β_i are the constants $(Tw_i, w_i)/(w_i, w_i)$ and $(Tw_i, w_{i-1})/(w_{i-1}, w_{i-1})$, respectively. Notice that w_i has degree i as a polynomial in T. Notice also that the vectors in V constructed by the Lanczos method beginning with b can be reconstructed as the sequence $w_i(A)b$.

Proposition 10. *Suppose that w_i is the i^{th} polynomial constructed by the Lanczos algorithm. Then there exists a unique polynomial $H_i(T)$ of degree $i-1$ so that*

$$\mathrm{ord}_{T=\infty}(w_i B(T)\frac{dT}{T} - H_i(T)dT) \geq i-1.$$

Furthermore, $(w_i, w_i) = 0$ if and only if the inequality is strict.

Proof. The construction of the polynomials is such that $w_0, \ldots, w_{i-1}$ span the space of polynomials in T of degree at most $i-1$, and w_i is orthogonal to w_j if $j < i$. Therefore $(w_i, T^j) = 0$ if $j < i$ and $(w_i, w_i) = (w_i, T^i)$. Write

$$w_i B(T)\frac{dT}{T} = (\sum_{k=-i}^{\infty} \frac{b_k}{T^k})\frac{dT}{T}.$$

Using the residue interpretation of the inner product, we see that

$$b_j = \mathrm{Res}_{T=\infty}(T^j w_i B(T)\frac{dT}{T}) = 0$$

if $0 \leq j < i$, and that $b_i = (w_i, w_i)$. This proves the proposition. □

We will now relate the Lanczos algorithm to Euclid's algorithm. Let us briefly recall well-known facts regarding approximating power series over $\mathbf{F}$ by rational functions. First, suppose that

$$S(T) = s_0/T + s_1/T^2 + s_2/T^3 + \cdots$$

is the Taylor expansion at infinity of a rational function $S(T) = H(T)/P(T)$ (in lowest terms) with coefficients in $\mathbf{F}$. Let $q_0 = 1$ and $p_0 = 0$. Then, given p_i and q_i with

$$\mathrm{ord}_{T=\infty}(q_i S(T) - p_i) < \infty,$$

let q_{i+1} be the monic polynomial of least degree such that there is a polynomial p_{i+1} with

$$\mathrm{ord}_{T=\infty}(q_{i+1}S(T) - p_{i+1}) > \mathrm{ord}_{T=\infty}(q_i S(T) - p_i) > 0.$$

Then p_i/q_i are the convergents to the continued fraction expansion of $S(T)$, the final q_i is $P(T)$, and

$$\mathrm{ord}_{T=\infty}(q_i S(T) - p_i) = \mathrm{degree}(q_{i+1}).$$

Recall that m is the dimension of K, the cyclic subspace generated by b.

Proposition 11. *The Lanczos algorithm succeeds (that is, it constructs $\{w_i\}_{i=0}^m$, with $w_0 = 1$, $w_m = 0$ and $(w_i, w_i) \neq 0$ for $i < m$) if and only if $\{A, b\}$ is nondegenerate and the continued fraction expansion of $B(T)/T$ has length m.*

Proof. We apply the isomorphism between K and $R = \mathbf{F}[T]/P(T)$ and consider the w_i as elements of the polynomial ring $\mathbf{F}[T]$, with $w_0 = 1$. If the Lanczos algorithm succeeds, R has an orthogonal basis, so $(\cdot, \cdot)$ is nondegenerate. By Lemma 9, $B(T) = TH(T)/P(T)$ is in lowest terms. In addition, by Proposition 10, we have constructed a sequence w_i of polynomials, where w_i is of degree i, which satisfies

$$\mathrm{ord}_{T=\infty}(w_i B(T)\frac{dT}{T} - H_i dT) = i-1$$

or alternatively

$$\mathrm{ord}_{T=\infty}(w_i B(T)/T - H_i) = i+1.$$

Since w_m is monic, $w_m \equiv 0 \bmod P(T)$ and w_m has degree m, we have $w_m = P(T)$. From this it follows that the w_i are the denominators of a sequence of best approximations, and therefore the continued fraction expansion of $B(T)/T$ has length m.

Conversely, suppose that the continued fraction expansion has length m. Let $q_0, \ldots, q_{m-1}, q_m$ be the denominators of the convergents, with $q_0 = 1$ and $q_m = P(T)$. Then we see that $B(T) = TH(T)/P(T)$ must be in lowest terms, and therefore by Lemma 9 that $\{A, b\}$ is nondegenerate. In addition, we must have q_i of degree i. Finally, the approximation property of the q_i tells us that there are polynomials p_i with

$$\mathrm{ord}_{T=\infty}(q_i B(T)\frac{dT}{T} - p_i dT) = i - 1.$$

In terms of the inner product, this means that q_i is orthogonal to all polynomials of degree less than i, but (q_i, q_i) is not zero. Now apply the Lanczos method starting with $q_0 = w_0 = 1$. Suppose that $w_i = q_i$ for $i < N$. Then (w_{N-1}, w_{N-1}) is not zero, so we construct w_N of degree N which is monic and orthogonal to all polynomials of degree less than N. Since the q_i, $0 \le i \le N$, are an orthogonal basis for these polynomials, and since q_N and w_N are both monic, we must have $w_N = q_N$. Consequently, the q_i are precisely the w_i, and Lanczos succeeds. □

We extract the following corollary from the proof.

Corollary 12. *Under the hypotheses of the proposition, the Lanczos polynomials are the denominators of the convergents to H/P.*

We see from the above discussion that there are two sources of failure for the Lanczos algorithm. What we might call a "serious" failure occurs if the pair $\{A, b\}$ is degenerate; a "mild failure" occurs if H/P has a short continued fraction expansion.

Corollary 13. *Suppose that $\mathbf{F}$ has q elements, that $\{A, b\}$ is nondegenerate, and that K has dimension m. Then the Lanczos algorithm will succeed with probability $(1 - 1/q)^m$.*

Proof. A failure occurs if, when applying Euclid's algorithm to $(TH(T), P(T))$, one obtains a quotient of degree bigger than one. At each stage of the algorithm the chance of this happening is $1/q$ and there are m independent trials. □

3. Improved Lanczos

The reformulation of Lanczos given above suggests the possibility of improving the Lanczos algorithm so that it is not vulnerable to the "mild" failure caused by the discovery of a self-orthogonal vector (that is, a w_i with $(w_i, w_i) = 0$). Such improvements are often called "look-ahead methods." They are relevant even over the real numbers, where a small value for (w_i, w_i) can introduce numerical instability. In this section, we will present our version of an improved Lanczos algorithm, and compare it to the Euclidean algorithm. Our improved algorithm has the same running time as basic Lanczos, but depending on how it is implemented may require more storage.

Recall that K is the cyclic subspace of $\mathbf{F}^n$ generated by b. We begin by adopting some rather artificial terminology whose significance will become clear in a moment.

Definition 14. Let v be any vector in K. We will call the subspace of K spanned by $v, \dots, A^r v$ a "block" (of degree r, based at v) provided that $(v, A^i v) = 0$ for $0 \leq i < r-1$ and $(v, A^r v) \neq 0$. By convention, we view the zero subspace as a block of degree -1 based at 0.

Notice that a vector v with $(v, v) \neq 0$ spans a block of degree zero.

Suppose that W is a block of degree r based at v. Define another sequence of vectors w_i, for $i = 0, \dots, r$, by setting $w_0 = v$ and inductively constructing

$$w_i = Aw_{i-1} - \frac{(Aw_{i-1}, A^r w_0)}{(w_0, A^r w_0)} w_0.$$

We will refer to the sequence of vectors $w_0, \dots, w_r$ as the dual vectors for W.

Lemma 15. *Let w_i be the vectors constructed as above for the block W of degree r based at v. Then, if $j \leq r$,*

$$(w_i, A^j v) = \begin{cases} 0 & \text{if } i + j \neq r, \\ (w_0, A^r v) & \text{if } i + j = r. \end{cases}$$

Furthermore, the w_i span W.

Proof. The defining properties of a block show that, for $0 \leq j \leq r$, $(v, A^j v) \neq 0$ if and only if $j = r$. We proceed by induction on i. Suppose that $i > 0$, and consider $(w_i, A^j v)$. We see that

$$(w_i, A^j v) = (w_{i-1}, A^{j+1} v) - \frac{(Aw_{i-1}, A^r v)}{(w_0, A^r v)} (w_0, A^j v).$$

Suppose that $i + j = r$. Then $j \leq r - 1$, and so

$$(w_i, A^j v) = (w_{i-1}, A^{j+1} v) = (w_0, A^r v)$$

by induction. If $i + j \neq r$ and $j \leq r - 1$, then $(w_{i-1}, A^{j+1} v) = 0$ and $(w_0, A^j v) = 0$ by induction. Finally, if $j = r$, then we obtain $(w_i, A^j v) = 0$ by construction. Since we have proved that the w_i are a dual basis to $A^j v$ relative to $(\cdot, \cdot)$, we see that they also span W. □

When the pair $\{A, b\}$ is nondegenerate, we can use a decomposition of the cyclic subspace K into blocks to construct a solution to the equation $Ax = b$.

Lemma 16. *Suppose that $\{A, b\}$ is nondegenerate. Then the restriction of the inner product $[\cdot, \cdot]$ to K is nondegenerate.*

Proof. Recall that $[x, Ay] = (x, y)$. If $\{A, b\}$ is nondegenerate, then A is invertible on K. Suppose $[x, u] = 0$ for all $u \in K$. Write $x = Av$ so that $[Av, u] = [v, Au] = (v, u) = 0$ for all $u \in K$. Therefore $v = 0$ and $x = 0$. □

Lemma 17. *Suppose that we write K as a $(\cdot, \cdot)$-orthogonal direct sum*

$$K = W_0 \oplus W_1 \oplus \cdots \oplus W_k,$$

where each W_i is a block based at v_i of degree r_i. Set

$$x = \sum_{i=0}^{k} \sum_{j=0}^{r_i} \frac{[w_{i,j}, b]}{(w_{i,0}, A^{r_i} v_i)} A^{r_i - j} v_i, \tag{1}$$

where $w_{i,0}, \dots, w_{i,r_i}$ are the dual vectors constructed as above starting with $w_{i,0} = v_i$. Then $Ax - b = 0$.

Proof. Since $(\cdot,\cdot)$ is nondegenerate on every block, it is nondegenerate on K. It follows that $[\cdot,\cdot]$ is nondegenerate on K as well. Therefore we need only verify that $[u, Ax-b]=0$ for all $u \in K$. Since the $w_{i,j}$ for fixed i span W_i, the $w_{i,j}$ together span K, and it suffices to check that $[w_{i,j}, Ax-b]=0$ for all pairs of $0 \le i \le k$ and $0 \le j \le r_i$. However, using the properties of the $w_{i,j}$ we see by calculation that

$$[w_{i,j}, Ax] = (w_{i,j}, x) = [w_{i,j}, b],$$

which is the desired result. □

Our improved Lanczos algorithm will construct an orthogonal decomposition of K of this form. Before presenting it, we lay some groundwork. Suppose that we have constructed a sequence of blocks $W_i \subset K$, $i=0,\dots,k$, of degree r_i, based at v_i, with the properties:

1. $v_0 = b$.
2. W_i and W_j are orthogonal with respect to $(\cdot,\cdot)$ if $i \neq j$.
3. $v_{i+1} = A^{r_i+1}v_i \pmod{\oplus_{j=0}^{i} W_j}$ for $0 \le i \le k-1$.

Let $w_{i,j}$, for $0 \le j \le r_i$, be the dual vectors for the block W_i. Set

$$v_{k+1} = A^{r_k+1}v_k - \sum_{j=0}^{r_k} \frac{(w_{k,j}, A^{r_k+1}v_k)}{(w_{k,0}, A^{r_k}v_k)} A^{r_k-j}v_k - \frac{(w_{k,0}, A^{r_k}v_k)}{(w_{k-1,0}, A^{r_{k-1}}v_{k-1})} v_{k-1} \tag{2}$$

where, in order to make the recurrence sensible for $k=0$, we adopt the convention that $v_{-1}=0$ and $(w_{-1}, A^{r_{-1}}v_{-1}) = 1$.

Let

$$M_k = W_0 \oplus W_1 \oplus \cdots \oplus W_k.$$

Lemma 18. *The vector v_{k+1} constructed in this way is orthogonal to all W_i for $i \le k$.*

Proof. We show first that v_{k+1} is orthogonal to W_j for $j \le k-2$. Notice that AW_j is spanned by $Av_j, A^2v_j, \dots, A^{r_j+1}v_j$. By the third property of our blocks,

$$AW_j \subset M_j + \langle v_{j+1} \rangle.$$

Suppose that $j \le k-2$. Observe that $A^{r_k}v_k$ belongs to W_k, and AW_j belongs to M_{j+1}. Since $j+1 \le k-1$, we see that M_{j+1} and W_k are orthogonal. On the other hand, $(v_{k+1}, W_j) = (A^{r_k}v_k, AW_j) = 0$, and so we conclude that v_{k+1} is orthogonal to W_j.

Next, we show that w_{k+1} is orthogonal to W_{k-1}. Write $v_{k+1} = A^{r_k+1}v_k + x + y$ where $x \in W_k$ and $y \in W_{k-1}$. Suppose that $h \in W_{k-1}$. Then, since W_k and W_{k-1} are orthogonal,

$$(v_{k+1}, h) = (A^{r_k}v_k, Ah) + (y, h).$$

Using Lemma 15, we may write

$$h = \sum_{i=0}^{r_{k-1}} \frac{(w_{k-1,i}, h)}{(w_{k-1,0}, A^{r_{k-1}}v_{k-1})} A^{r_{k-1}-i}v_{k-1}.$$

Since

$$A^{r_{k-1}+1}v_{k-1} \equiv v_k \pmod{(W_0 \oplus \cdots \oplus W_{k-1})}$$

and $A^{r_k}v_k \in W_k$, which is perpendicular to the earlier W_i, we see that

$$(A^{r_k}v_k, Ah) = \frac{(w_{k-1,0}, h)}{(w_{k-1,0}, A^{r_{k-1}}v_{k-1})}(A^{r_k}v_k, A^{r_{k-1}+1}v_{k-1})$$
$$= \frac{(w_{k-1,0}, h)}{(w_{k-1,0}, A^{r_k-1}v_{k-1})}(A^{r_{k-1}}v_k, v_k).$$

On the other hand, by Formula (2),

$$y = -\frac{(w_{k,0}, A^{r_k}v_k)}{(w_{k-1,0}, A^{r_{k-1}}v_{k-1})}v_{k-1},$$

so

$$(y, h) = -\frac{(w_{k,0}, A^{r_k}v_k)}{(w_{k-1,0}, A^{r_{k-1}}v_{k-1})}(v_{k-1}, h).$$

Since $v_{k-1} = w_{k-1,0}$ by definition, we conclude that v_{k+1} is orthogonal to W_{k-1}.

Finally, we point out that the formula for v_{k+1} and the duality properties show immediately that v_{k+1} is orthogonal to W_k, and this proves our lemma. □

Lemma 19. *Suppose that $v_{k+1} = 0$. Then $K = M_k$.*

Proof. If $v_{k+1} = 0$, then $AM_k \subset M_k$. Since $b \in M_k$, we conclude $K \subset M_k$, so $K = M_k$. □

Lemma 20. *Suppose that $v_{k+1} \neq 0$ and $(v_{k+1}, A^j v_{k+1}) = 0$ for $j = 0, \ldots, i-1$. Then $A^i v_{k+1}$ is orthogonal to M_k.*

Proof. We proceed by induction. We know the result for $i = 0$. We know that $AM_k \subset \langle v_{k+1}\rangle + M_k$. It follows that $(A^i v_{k+1}, M_k) = (A^{i-1}v_{k+1}, AM_k) = 0$. □

Lemma 21. *Let $d_k = \sum_{i=0}^{k}(r_i + 1)$. Suppose that $(v_{k+1}, A^j v_{k+1}) = 0$ for $j = 0, \ldots, n - d_k$. Then v_{k+1} belongs to the kernel of $(\cdot,\cdot)$ restricted to K.*

Proof. The number d_k is the dimension of M_k. The inner product $(\cdot,\cdot)$ is nondegenerate on M_k. Therefore, the orthogonal complement to M_k has dimension at most $n - d_k$. Under our hypotheses, and using the previous lemma, the $n - d_k + 1$ vectors $A^j v_{k+1}$ belong to this complement, and are consequently linearly dependent. From this it follows that K is spanned by M_k and $\{A^j v_{k+1}\}_{j=0}^{n-d_k}$, and therefore v_{k+1} is orthogonal to all of K. □

Our improved Lanczos algorithm works as follows.

Algorithm (Improved Lanczos).

Initialization. *Set $v_{-1} := 0$, $\alpha_{-1} := 1$, $v_0 := b$, $k := 0$, $r_{-1} := -1$, and $x := 0$.*

Stage I. (Block Building): *Given a nonzero vector v_k, find the smallest integer r_k such that*

$$0 \leq r_k < n - \sum_{j=0}^{k-1}(r_j + 1),$$

and $\alpha_k := (v_k, A^{r_k}v_k)$ is nonzero. If no such r_k exists, then we are in the situation of Lemma 21. This means that $\{A, b\}$ is degenerate, and we stop.

Stage II. (Projection): *Compute the dual vectors* $w_{k,i}$ *by setting* $w_{k,0} = v_k$ *and*

$$w_{k,i+1} = Aw_{k,i} - \frac{(Aw_{k,i}, A^{r_k}w_{k,0})}{\alpha_k} w_{k,0}.$$

Compute the new vector v_{k+1} *by formula* (2), *which in our terms reads*

$$v_{k+1} = A^{r_k+1}v_k - \sum_{j=0}^{r_k} \frac{(w_{k,j}, A^{r_k+1}v_k)}{\alpha_k} A^{r_k-j}v_k - \frac{\alpha_k}{\alpha_{k-1}} v_{k-1}.$$

Extend the computation of the solution x *by formula* (1) *setting*

$$x := x + \sum_{j=0}^{r_k} \frac{[w_{k,j}, b]}{\alpha_k} A^{r_k-j}v_k.$$

If $v_{k+1} = 0$, *we are in the situation of Lemma* 19, *so, by Lemma* 17, $Ax - b = 0$. *Otherwise, set* $k := k + 1$ *and return to Stage* I.

We now consider the running time and storage requirements for this algorithm. We begin by making a number of remarks regarding implementation.

Remark I. In the event that all r_k are 1, this algorithm reduces to (plain) Lanczos.

Remark II. We will prove in Section 4 that the block sizes r_i are small. Consequently, in the block building stage, we may store the $A^i v_k$ as we consider them. As a result, we assume that we enter the projection stage knowing $v_k, \ldots, A^{r_k}v_k$.

Remark III. Using our knowledge of $v_k, \ldots, A^{r_k}v_k$, we carry out the computation of the $w_{k,i}$, the new vector v_{k+1}, and the extended solution x in a single loop. In addition, we do not store all of the $w_{k,j}$; only the one we need at the moment.

Stage II (Projection, Refined):

$v_{k+1} := A(A^{r_k}v_k) - (\alpha_k/\alpha_{k-1})v_{k-1}$;
$w := v_k$;
For i from 1 to r_k do
  $\beta := (w, v_{k+1})$;
  $x := x + ([w, b]/\alpha_k)A^{r_k-i+1}v_k$;
  $w := Aw - (\beta/\alpha_k)v_k$;
  $v_{k+1} := v_{k+1} - (\beta/\alpha_k)A^{r_k-i+1}v_k$;
done ;
$x := x + ([w, b]/\alpha_k)v_k$;
$v_{k+1} := v_{k+1} - ((w, v_{k+1})/\alpha_k)v_k$;

Proposition 22. *This refined version of the projection stage computes* x *and* v_{k+1} *according to formulae* (1) *and* (2).

Proof. Let v_{k+1}^i, w^i, and β^i be the values of v_{k+1}, w, and β, respectively, after i passes through the loop. It is clear that $w^0 = w_{k,0}$ and

$$v_{k+1}^0 = A^{r_k+1}v_k \pmod{W_{k-1}}.$$

It is also evident that when $i \geq 1$, then

$$v_{k+1}^i = A^{r_k+1}v_k \pmod{W_{k-1} + \langle A^{r_k}v_k, \ldots, A^{r_k-i+1}v_k\rangle}. \tag{3}$$

If we assume inductively that $w^i = w_{k,i}$, then

$$\beta^{i+1} := (w^i, v_{k+1}^i) = (w_{k,i}, v_{k+1}^i) = (w_{k,i}, A^{r_k+1}v_k)$$

using the duality properties of $w_{k,i}$ and equation 3. We see from this that

$$v_{k+1}^i := v_{k+1}^{i-1} - \frac{(w_{k,i}, A^{r_k+1}v_k)}{\alpha_k} A^{r_k-i+1}v_k$$

and

$$w^{i+1} := Aw_i - \frac{(w_{k,i}, A^{r_k+1}v_k)}{\alpha_k} v_k.$$

We conclude by induction that $w^i = w_{k,i}$ for all i; and taking into account the final steps of this refined projection stage we see that we correctly compute x and v_{k+1}. □

Remark IV. Once v_{k+1} has been computed, the only data we must keep in order to continue with the algorithm are v_{k+1} and the values of v_k and α_k.

Remark V. In the event that the improved Lanczos fails (so that $\{A, b\}$ is degenerate) it is probably worthwhile trying again with b replaced by $b + Au$ for some random vector u. Presumably the odds are good that $b + Au$ is nondegenerate for A. (I am grateful to Dan Bernstein for pointing this out to me.)

Running Time. Suppose that the matrix A has D nonzero entries. Then the time to compute Av is proportional to D, the time to compute $(\cdot, \cdot)$ is proportional to $D + n$, and the time to compute a scalar multiple av of v or a dot product $[\cdot, \cdot]$ is proportional to n.

It is easy to see from the description of the improved Lanczos algorithm that building a block of degree r requires $r+1$ computations of $(\cdot, \cdot)$, so the time for this stage is proportional to $(r + 1)(D + n)$.

In the projection stage, referring to the refined projection described in Remark III above, we must compute the dot product $(\cdot, \cdot)$ $r + 1$ times, to build the $w_{k,j}$ and v_{k+1}, and the dot product $[\cdot, \cdot]$ $r + 1$ times to construct the solution x. All together, including constructing the solution, we need three dot products to move ahead one step in the algorithm. In addition, each passage through the loop requires a fixed number U of scalar-vector multiplications, and a fixed number of matrix-vector multiplications.. Thus the time spent in the projection stage is proportional to $(r + 1)(D + n) + (r + 1)n + (r + 1)Un$. All together, this stage requires time proportional to $(r + 1)(D + n)$. Since the sum of the block dimensions is at most n, we have the following result.

Theorem 23. *The running time for the improved Lanczos is proportional to* $nD + n^2$.

4. Improved Lanczos and Euclid

Let us now consider the improved Lanczos algorithm in the same terms as we considered the original Lanczos method. Returning to the notation of Section 2 of this paper, we map $\mathbf{F}[T] \to \mathbf{F}^n$ via the map $T \mapsto Ab$. We then obtain an isomorphism of $R = \mathbf{F}[T]/P(T)$ with the cyclic submodule K of $\mathbf{F}^n$. We also have a symmetric bilinear form on $\mathbf{F}[T]$ defined by $(f, g) = (f(A)b, g(A)b)$ for polynomials f and g in $\mathbf{F}[T]$; assuming the pair $\{A, b\}$ is nondegenerate, this form yields a nondegenerate pairing on $R = \mathbf{F}[T]/P(T)$.

As we have seen in Section 1, plain Lanczos applied to R finds the denominators in the continued fraction expansion of the power series $B(T)/T$ constructed from

the pairing $(\cdot,\cdot)$ provided that the degrees of these denominators go up by one at each stage. The improved Lanczos finds these denominators regardless of their degrees.

Theorem 24. *Apply the improved Lanczos to the ring $R = \mathbf{F}[T]/P(T)$ using the dot product $(\cdot,\cdot)$. Let W_i, for $i = 0\ldots,k$, be the blocks of degree r_i based at f_i constructed by this algorithm, starting with $f_0 = 1$. Suppose that the algorithm terminates with $f_{k+1} = 0$. Then the polynomials f_i are the denominators of the convergents to $B(T)/T$.*

Proof. We will show that the f_i are the denominators of a sequence of best approximations to $B(T)/T$. Let $d_k = \sum_{j=0}^{k}(r_j + 1)$. The polynomial f_i has degree d_{i-1} and is orthogonal to all of the W_j for $j < i$ and to the $T^j f_i$ for $j = 0,\ldots,r_i - 1$. Thus f_i is orthogonal to all polynomials of degree less than or equal to $d_i - 2$, but $(f_i, T^{r_i} f_i)$ is not zero. It follows that there exists a polynomial H_i of degree $d_{i-1} - 1$ such that

$$\operatorname{ord}_{T=\infty}(f_i B(T)\frac{dT}{T} + H_i dT) = d_i - 2. \tag{4}$$

Suppose that g is a polynomial of degree k where the integer k satisfies $d_{i-2} \le k < d_{i-1}$. Write

$$g \equiv (a_s x^s + \cdots + a_0) f_{i-1} \pmod{W_0 \oplus \cdots \oplus W_{i-2}},$$

with a_s nonzero. It follows that $(w_{i-1,r_{i-1}-s}, g) = a_s \neq 0$, where $w_{i-1,r_{i-1}-s}$ is the appropriate dual polynomial from W_{i-1}. Since $w_{i-1,r_{i-1}-s}$ has degree $d_{i-2}+r_{i-1}-s$, there is a polynomial p such that

$$\operatorname{ord}_{T=\infty}(gB(T)\frac{dT}{T} - p(T)dT) \le d_{i-2} + r_{i-1} - 1 - s = d_{i-1} - 2 - s.$$

Since $d_{i-1} - 2 - s \le d_{i-1} - 2 < d_i - 2$, we see that f_{i-1} and f_i are successive best approximations. From this it follows that f_i is the polynomial of least degree which achieves the approximation in equation (4), and therefore that f_i is the denominator of a convergent. By induction, the f_i are precisely the denominators of the convergents. □

We can now show that block sizes are typically small.

Corollary 25. *Over a finite field with q elements, if $\{A, b\}$ is nondegenerate, then a block of degree r occurs with probability $(1/q)^{r+1}$.*

Proof. The probability in question is the probability of obtaining a partial quotient of degree r in the course of applying the Euclidean algorithm to a pair of polynomials over $\mathbf{F}_q$. □

Conclusion

We have shown that the Lanczos method and the improved version of it we describe here are closely related to the Euclidean algorithm. They share this trait with Wiedemann's method, which employs another version of Euclid's algorithm, the Berlekamp-Massey algorithm, to the problem of solving linear equations over finite fields. It seems quite reasonable that the third common iterative method, the Conjugate Gradient method, is probably also based on Euclid, although we have not looked at it in detail.

As we mentioned in the introduction, when working with practical problems over fields of small characteristic, Coppersmith, Montgomery, and others have demonstrated the usefulness of working with block methods. If we apply the point of view of this note to the analysis of these block methods, we are led to consider the application of the Euclidean algorithm to polynomials with entries in a ring of matrices. This problem has been considered by Coppersmith in the context of the Berlekamp–Massey algorithm ([C2]), but more work is clearly needed to clarify the significance of that for a complete understanding of the behavior of block Lanczos methods.

References

[B] A. Bultheel, *Recursive algorithms for non-normal Pade tables,*, SIAM Journal on Applied Mathematics, **39,** (1980), 1:106–118. MR **82e:**65018

[C1] D. Coppersmith, *Solving linear equations over $GF(2)$; block Lanczos algorithm.*, Linear Algebra and its Applications **192** (1993), 33–60. MR **94i:**65044

[C2] D. Coppersmith, *Solving homogeneous linear equations over $GF(2)$ via block Wiedemann algorithm*, Mathematics of Computation **62** (1994), 205:333–350. MR **94c:**11124

[D] J. L. Dornstetter, *On the equivalence between Berlekamp's and Euclid's algorithms*, IEEE Transactions on Information Theory **33** (1987), 3:428–431. MR **88j:**94018

[K] E. Kaltofen, *Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems*, Mathematics of Computation **64** (1995), 210:777-806. MR **95f:**65094

[M] P. Montgomery, *A block Lanczos algorithm for finding dependencies over $GF(2)$*, Advances in cryptology—EUROCRYPT '95 (Saint-Malo, 1995), Lecture Notes in Computer Science 921, Springer, Berlin, 1995. MR **97c:**11115

[W] D.H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Transactions on Information Theory **32** (1988), 1:54–62. MR **87g:**11166

Jeremy Teitelbaum, Department of Mathematics, Statistics, and Computer Science (M/C 249), University of Illinois at Chicago, 851 S. Morgan St., Chicago, IL 60607, USA

E-mail address: jeremy@uic.edu