A Multi-modular Echelon Form Algorithm over Cyclotomic Fields

Jennifer Balakrishnan and William Stein

May 2005

1 The Algorithm

Let K be the number field $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ is a primitive nth root of unity. Recall that the minimal polynomial of ζ_n is the nth cyclotomic polynomial Φ_n, and that the ring of integers $\mathcal{O}_K$ of K is $\mathcal{O}_K = \mathbb{Z}[\zeta_n] = \mathbb{Z}[x]/\Phi_n(x)$ [**?**]. We assume access to an algorithm for quickly computing reduced row echelon forms of matrices over small finite fields $\mathbb{F}_p$.

Let A be a matrix with entries in K. Define $H_v(A) = \max\{|a_{ij}|_v\}$ and $H(A) = \max H_v(A)$, where the v run through the archimedean absolute values of K. Whenever we write "echelon form" below, we mean "reduced row echelon form".

INPUT: A matrix A with entries in a cyclotomic field $K = \mathbb{Q}(\zeta_n)$.
OUTPUT: The reduced row echelon form of A.

1. Rescale the input matrix A so that none of the entries have denominators. This does not change the echelon form and makes reduction modulo many primes easier. Henceforth we assume all the entries of A are in $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

2. Let h be a guess for the height $H(E)$ of the echelon form E.

3. Consider primes p that split completely in $\mathbb{Z}[\zeta_n] = \mathbb{Z}[x]/(\Phi_n(x))$. Write $p = \wp_1\wp_2\cdots\wp_r$, where $r = \varphi(n)$. These are the primes $p \equiv 1 \pmod{n}$, and there are infinitely many such primes by Dirichlet's theorem on primes in arithmetic progression [[ref]]. List successive such primes $p_1, p_2, \ldots$ such that the product of the p_i is bigger than $c \cdot h \cdot H(A) + 1$, where c is the number of columns of A. (How? Go through the primes that are 1 mod n and use a primality test [ref].)

4. For each prime p_j do the following:

   (a) Via the Chinese Remainder Theorem, we have the isomorphism

$$\mathcal{O}_K/(p) \cong \bigoplus_{i=1}^{r} \mathcal{O}_K/\wp_i.$$

Each factor $\mathcal{O}_K/\wp_i$ is isomorphic to $\mathbb{F}_p$. We represent elements in $\mathbb{Z}[\zeta_n]$ as polynomials in ζ_n. We have $\wp_i = (p, \zeta_n - b_i)$, for some $b_i \in \mathbb{Z}$. Let $a_i \in \mathbb{F}_p$ be the reduction of b_i modulo p. We thus have a homomorphism $\mathcal{O}_K \to \bigoplus_{i=1}^{r} \mathcal{O}_K/\wp_i \cong \mathbb{F}_p^r$ given by

$$f(\zeta_n) \mapsto (f(a_1), f(a_2), \ldots, f(a_r)) \pmod{p}.$$

(b) Now consider $\mathcal{O}_K/(p)$ as the $\mathbb{F}_p$-vector space $\mathbb{F}_p[x]/(\Phi_n(x))$ with basis

$$\{1, \bar{\zeta}_n, \bar{\zeta}_n^2, \ldots, \bar{\zeta}_n^{r-1}\}.$$

Consider the linear transformation

$$T : \mathcal{O}_K/(p) \to \mathbb{F}_p^r$$

defined above. Compute the image of each basis vector under T:

$$\begin{aligned}
1 &\mapsto (1, 1, \ldots, 1)\\
\bar{\zeta}_n &\mapsto (a_1, a_2, \ldots, a_r)\\
\bar{\zeta}_n^2 &\mapsto (a_1^2, a_2^2, \ldots, a_r^2)\\
&\vdots\\
\bar{\zeta}_n^{r-1} &\mapsto (a_1^{r-1}, a_2^{r-1}, \ldots, a_r^{r-1}).
\end{aligned}$$

Hence T can be represented by the Vandermonde matrix F below:

$$\begin{pmatrix}
1 & a_1 & a_1^2 & \ldots & a_1^{r-1}\\
1 & a_2 & a_2^2 & \ldots & a_2^{r-1}\\
\vdots & \ldots & \ldots & \ldots & \vdots\\
1 & a_r & a_r^2 & \ldots & a_r^{r-1}
\end{pmatrix}$$

The a_i are distinct nth roots of unity in $\mathbb{F}_p^\times$, so the Vandermonde determinant is nonzero.

(c) Since we will be interested in computing T^{-1}, compute the inverse of F, e.g., by finding the echelon form of F.

(d) Compute the echelon form of $A \pmod{\wp_i}$ for $i = 1, \ldots, r$, using an algorithm for echelon forms over $\mathbb{F}_p$. (Note: If A is square and $A \pmod{\wp_i}$ is invertible, then A must be invertible, hence its echelon form is the identity matrix, and we terminate the algorithm.)

(e) Use F^{-1} to find a matrix B_j with entries in $\mathcal{O}_K$, such that $B \equiv B_{\wp_i} \pmod{\wp_i}$ for $i = 1, \ldots, r$. We hope that the reduction of B modulo p equals the reduction of the echelon form of A modulo p. (In fact equality holds for all but finitely many primes, as we will see.)

5. Discard any B_k whose pivot column list is not maximal among pivot lists of all B_j found.

6. Use the usual Chinese Remainder Theorem over $\mathbb{Z}$ to find a matrix B with entries in $\mathbb{Z}[\zeta_n]$ such that $B \equiv B_i \pmod{p_i}$ for all p_i. Note: one only needs to do a few CRT's, then do a linear combination of matrices. Also to use CRT on $f(\zeta_n)$ and $g(\zeta_n)$, just view both as the vector of integer coefficients, and apply CRT to those two vectors.

7. Use rational reconstruction on each entry of B to find a matrix C whose entries in $\mathbb{Q}(\zeta_n)$, viewed as polynomials in ζ_n, have coefficients that are rational numbers a/b such that $0 \leq |a|, b \leq \sqrt{M/2}$, where $M = \prod p_i$ and $C \equiv B_i \pmod{p_i}$ for each prime p_i. If rational reconstruction fails, compute a few more echelon forms modulo the next few primes (using the above steps) and attempt rational reconstruction again. Let E be the matrix over $\mathbb{Q}(\zeta_n)$ so obtained.

8. Compute the denominator d of E, i.e., the smallest positive integer such that dE has entries in $\mathbb{Z}[\zeta_n]$. If
$$H_v(dE)H_v(A)m \leq \prod p_i$$
for a fixed valuation v, then by Theorem **??**, E is the reduced row echelon form of A. If not, repeat the above steps with a few more primes. Note that $H_v(A) = \max\{|a_{ij}|_v\}$, and since each entry a_{ij} is of the form $b_0 + b_1\zeta_n + \cdots + b_t\zeta_n^t$, by the triangle inequality, we have that
$$|a_{ij}|_v = |b_0 + b_1\zeta_n + \cdots + b_t\zeta_{n^t}| \leq \sum |b_i||\zeta_n^i| = \sum |b_i|.$$
So to bound $H_v(A)$, use the upper bound given by the above inequalities.

Theorem 1.1. *Suppose A is a matrix with c columns and entries in $\mathcal{O}_K$. Let $E = ...$ If*
$$H_v(dE)H_v(A)c \leq \prod p_i$$
for a fixed valuation v, then E is the reduced row echelon form of A.

2 Examples

2.1 Example 1

Let $K = \mathbb{Q}(\zeta_3)$. We compute the echelon form of two matrices with entries in K using the above algorithm.

For our first example, let A be the matrix
$$A = \begin{pmatrix} 1+\zeta & 2+\zeta & \zeta \\ 1 & 1+\zeta & -2 \\ 1 & 5 & -1+\zeta \end{pmatrix}.$$

Step 1. None of the entries of A have denominators, so we proceed to Step 2.

Step 2. Let $h = 10$ be a guess for the height h.

Step 3. The ring of integers $\mathcal{O}_K$ of K is $\mathbb{Z}[\zeta_3]$, and the primes that split completely in $\mathcal{O}_K$ are congruent to 1 mod 3. Our list of primes starts with 7, 13, and 19. Notice, though, that since $c = 3$, $h = 10$, and $H(A) = 5$, taking the primes $p_1 = 13$ and $p_2 = 19$ results in $13 \cdot 19 > c \cdot h \cdot H(A) + 1 = 151$, and so it suffices to use 13 and 19.

Step 4a. The third cyclotomic polynomial $\Phi_3(x)$ is $\Phi_3(x) = x^2 + x + 1$, and taking the prime $p_1 = 13$, we see that 13 splits in $\mathbb{Z}[\zeta_3]$ as $\wp_1\wp_2$, where $\wp_1 = (13, \zeta_3 - 3)$ and $\wp_3 = (13, \zeta_3 - 9)$. Our homomorphism T thus takes

$$a + b\zeta_3 \mapsto (\overline{a + 3b}, \overline{a + 9b}).$$

Step 4b. We compute the matrix F corresponding to the linear map T above: $F = \begin{pmatrix} 1 & 3 \\ 1 & 9 \end{pmatrix}$.

Step 4c. The inverse of F is $F^{-1} = \begin{pmatrix} 8 & 6 \\ 2 & 11 \end{pmatrix}$

Step ??. We have that $A \pmod{\wp_1} = \begin{pmatrix} 4 & 5 & 3 \\ 1 & 4 & 11 \\ 1 & 5 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{F}_{13})$, and as $A \pmod{\wp_1}$ is invertible, the echelon form is just $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Since the echelon form of some reduction is the identity matrix, the echelon form of A is just the identity matrix, and we are done.

2.2 Example 2

For our second example, let A be the matrix

$$A = \begin{pmatrix} 1+\zeta & 2+\zeta & \zeta \\ 1 & 1+\zeta & -2 \end{pmatrix}.$$

Step 1. None of the entries of A have denominators, so we proceed to Step 2.

Step 2. Let $h = 10$ be a guess for the height h.

Step 3. The ring of integers $\mathcal{O}_K$ of K is $\mathbb{Z}[\zeta_3]$, and the primes that split completely in $\mathcal{O}_K$ are congruent to 1 mod 3. Note as above that it suffices to use $p_1 = 13$ and $p_2 = 19$.

Step 4a. Again, for the prime $p_1 = 13$, we see that 13 splits in $\mathbb{Z}[\zeta_3]$ as $\wp_1\wp_2$, where $\wp_1 = (13, \zeta_3 - 3)$ and $\wp_3 = (13, \zeta_3 - 9)$. Our homomorphism T thus takes

$$a + b\zeta_3 \mapsto (\overline{a + 3b}, \overline{a + 9b}).$$

Step 4b. We compute the matrix F corresponding to the linear map T above: $F = \begin{pmatrix} 1 & 3 \\ 1 & 9 \end{pmatrix}$.

Step 4c. The inverse of F is $F^{-1} = \begin{pmatrix} 8 & 6 \\ 2 & 11 \end{pmatrix}$.

Step 4d. We see that

$$A \pmod{\wp_1} = \begin{pmatrix} 4 & 5 & 3 \\ 1 & 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 12 \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{13})$$

and

$$A \pmod{\wp_2} = \begin{pmatrix} 10 & 11 & 9 \\ 1 & 10 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 9 \\ 0 & 1 & 8 \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{13}).$$

Step 4e. Applying F^{-1} to the entries of $\begin{pmatrix} (1,1) & (0,0) & (2,9) \\ (0,0) & (1,1) & (12,8) \end{pmatrix}$, we find that

$$B_1 = \begin{pmatrix} 1 & 0 & 5-\zeta \\ 0 & 1 & 1+8\zeta \end{pmatrix}.$$

We repeat Steps $4a$ through $4e$ for the prime $p_2 = 19$:

Step 4'a. For the prime $p_2 = 19$, we see that 19 splits in $\mathbb{Z}[\zeta_3]$ as $\wp_1\wp_2$, where $\wp_1 = (19, \zeta_3 - 7)$ and $\wp_3 = (19, \zeta_3 - 11)$. Our homomorphism T thus takes

$$a + b\zeta_3 \mapsto (\overline{a+7b}, \overline{a+11b}).$$

Step 4'b. We compute the matrix F corresponding to the linear map T above: $F = \begin{pmatrix} 1 & 7 \\ 1 & 11 \end{pmatrix}$.

Step 4'c. The inverse of F is $F^{-1} = \begin{pmatrix} 17 & 3 \\ 14 & 5 \end{pmatrix}$.

Step **??**$_2$. We see that

$$A \pmod{\wp_1} = \begin{pmatrix} 8 & 9 & 7 \\ 1 & 8 & 17 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{19}),$$

and

$$A \pmod{\wp_2} = \begin{pmatrix} 12 & 13 & 11 \\ 1 & 12 & 17 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 16 \\ 0 & 1 & 8 \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{19}).$$

Step 4'e. Applying F^{-1} to $\begin{pmatrix} (1,1) & (0,0) & (1,16) \\ (0,0) & (1,1) & (2,8) \end{pmatrix}$,

we find that

$$B_2 = \begin{pmatrix} 1 & 0 & 8-\zeta \\ 0 & 1 & 1+11\zeta \end{pmatrix}.$$

Step **??**. We get

$$B = \begin{pmatrix} 1 & 0 & 122-\zeta \\ 0 & 1 & 1+125\zeta \end{pmatrix}.$$

Step **??**. We find that

$$C = \begin{pmatrix} 1 & 0 & -\frac{3}{2} - \zeta \\ 0 & 1 & 1 + \frac{3}{2}\zeta \end{pmatrix}.$$

Here we computed, e.g., $-\frac{3}{2}$ by applying rational reconstruction to $122 \pmod{247}$ (see ...).

3 Comments

There's work one does for a given cyclotomic field and many primes $p \equiv 1 \pmod{n}$, which does not have to be repeated if we are computing echelon forms of many matrices. This is a space versus time tradeoff.