Invariant factors and Elementary Divisors

Problem definitions:

- Det: Given $A \in \mathbb{F}^{n \times n}$, compute determinant of A.
- Rank: Given $A \in \mathbb{F}^{n \times m}$, compute rank of A.
- LinSol: Given $A \in \mathbb{F}^{n \times m}, b \in \mathbb{F}^n$, find $x \in \mathbb{F}^m$ such that $Ax = b$.
- RNull: Given $A \in \mathbb{F}^{n \times m}$, find $x \in \mathbb{F}^m$ such that $Ax = 0$, a uniformly random sample of the right nullspace of A..
- Minp: Given $A \in \mathbb{F}^{n \times n}$, compute minimal polynomial of A.
- Charp: Given $A \in \mathbb{F}^{n \times n}$, compute characteristic polynomial of A.
- Frob: Given $A \in \mathbb{F}^{n \times n}$, compute the invariant factors of of A.
- s-Frob: Given $A \in \mathbb{F}^{n \times n}$, compute the first s invariant factors of of A.

A similarity class is characterized by a table of elementary divisors, $g_i^{e_{i,j}}$, where $g_1, \ldots g_k$ is an enumeration of the occurring irreducible factors and $e_{i,j}$ is the exponent of g_i in the j-th invariant factor, $f_j = \prod_i g_i^{e_{i,j}}$.

An *s invariant factor matrix* is a matrix that has at most s non constnt invariant factors. An *s,d-elementary divisor matrix* is a matrix in which f_s is square free with at most d irreducible factors occurring. The idea behind this definition is that we will have good algorithms for problem Frob when d and s are not too large.

For this discussion suppose that A is a sparse or structured matrix such that the cost of matrix vector product is soft-O(n). In other words $mv_A(x) = n^\alpha$, where $\alpha = 1 + o(1)$. For instance, A may be sparse with 7 nonzeroes per row or A may be Toeplitz with matrix vector cost $\mathrm{O}(n \log(n))$. Also let A be over **any** finite field. In other words we propose to conquer the small field problem without the painful-in-practice $\mathrm{O}(\log(n))$ cost of using an extension field.

An algorithm is Monte Carlo if it is randomized and a wrong result is possible. ϵ is an upper bound on the the probability of error. For instance if $\lg(1/\epsilon) = 20$, there is at most a one in 2^{20} (about 1 in a million) chance of error.

An algorith is *Las Vegas* if it is randomized but will never return a wrong result, but bad luck may lead to a longer run time. In this case the given run time is the expected run time.

Observations:

1. Wiedemann's algorithm solves Minp = 1-Frob at cost $\mathrm{O}(n^2 \log(1/\epsilon)$, Monte Carlo. (Las Vegas if minimum polynomial equals characteristic polynomial.)
2. Block wiedemann (to be presented next time) with blocksize $\mathrm{O}(s)$ solves s-Frob at cost $\mathrm{O}(n^2)$, if s is constant, Monte Carlo.

3. Frob implies Det, Rank, Minp, Charp in the same run time
4. For matrices A which are s invariant factor matrices, Block Wiedemann with blocksize $\mathrm{O}(s)$ solves Frob, Las Vegas. at cost $\mathrm{O}(n^2)$. (most matrices)
5. For matrices A which are $s, 1$-elementary divisor matrices, Block Wiedemann with blocksize $\mathrm{O}(s)$ solves Frob at cost $\mathrm{O}(n^2)$, Monte Carlo. (more matrices, particularly many of low rank)
6. For matrices A which are $s, 2$-elementary divisor matrices, Block Wiedemann with blocksize $\mathrm{O}(s)$ with a trace trick solves Frob at cost $\mathrm{O}(n^2)$, Monte Carlo. (a few more matrices)
7. For matrices A which are s, d-elementary divisor matrices, small d, Block Wiedemann with blocksize $\mathrm{O}(s)$ with a few more tricks (and more cost) solves Frob at cost $\mathrm{O}(n^2)$, Monte Carlo. (still more matrices)
8. For matrices A which are **not** s, d-elementary divisor matrices, small d, Block Wiedemann with blocksize $\mathrm{O}(s)$ with a discrete log trick (and more cost) solves **Charp**, Monte Carlo.
9. LinSol $\leftrightarrow$ RNull.
10. For matrices A such that $x^2 \not| f_1$, Wiedemann or Block Wiedemann solves LinSol and RNull at cost $\mathrm{O}(n^2)$.
11. For matrices A such that $x^2 \not| f_s$ and ..., Block Wiedemann with blocksize $\mathrm{O}(s)$ solves LinSol and RNull at cost $\mathrm{O}(n^2)$.

Proof sketches

5 $f_s = f_{s+1} = f_{s+2} = \ldots$ until the degrees add up to n.

6 We have $f_s = gh$, a product of two irreducibles. The characteristic polynomial is $g^k h^l \prod_{i=1..s} f_i$ for some nonnegative k, l. Two linear relations on k, l are easily obtained. One considers the degree; the second considers the trace.
degree: $n = k \deg(g) + l \deg(h) + \sum_{i=1..s} \deg(f_i)$.
trace: $\mathrm{tr}(A) = k\mathrm{tr}(g) + l\mathrm{tr}(h) + \sum_{i=1..s} \mathrm{tr}(f_i)$.
If these are independent they determine k and l. If the conditions are dependent there may still be a unique solution in which k, l are nonnegative integers.

7 Log/Det discussion...

8 Same as item above, but we don't have that the last known invariant factor is square free. We get the algebraic multiplicity of the irreducibles but not the geometric multiplicity.

9 LinSol $\leftrightarrow$ RNull.

RNull by way of LinSol: Let $r \in \mathbb{F}^m$ be random. Solve $Ax = Ar$. Return $x - r$. LinSol by way of RNull: Apply RNull to (A, b) obtaining vector $v \in \mathbb{F}^{n+1}$ and scalar $v_b \in \mathbb{F}$ such that $(A, b)(v, v_b)^T = 0$. If the system is consisitent the probability that $v_b = 0$ is $1/q$ for field size q. For $v_b \neq 0$ the solution is $A(-1/v_b)v = b$.

10 The minpoly has the form $f_1(x) = f(x)x$, where $f(0) \neq 0$. The image and kernel of A are complementary. Choose random vector r. Then $f(A)r$ is a random sample of the right nullspace of A.

11 The minpoly has the form $f_1(x) = f(x)x^{k_1}$, where $f(0) \neq 0$. The image and kernel of A **not** complementary. Reduce the problem to the nilpotent part. Consider that nilpotent part of A is similar to a block diagonal of the form $\oplus J(x, k_i)$, where there are not too many k_i and they are not too large. Push through the details.

$$
\left[\begin{array}{ccc|cc|cc|c|c|c|c}
0 & & & & & & & & & & \\
1 & 0 & & & & & & & & & \\
 & 1 & 0 & & & & & & & & \\
\hline
 & & & 0 & & & & & & & \\
 & & & 1 & 0 & & & & & & \\
\hline
 & & & & & 0 & & & & & \\
 & & & & & 1 & 0 & & & & \\
\hline
 & & & & & & & 0 & & & \\
\hline
 & & & & & & & & 0 & & \\
\hline
 & & & & & & & & & 0 & \\
\hline
 & & & & & & & & & & 0
\end{array}\right]
$$