

Relevant Theorems and misc:

Theorem 8.1 (Villard): Let A be a $N \times N$ matrix over K with minimal polynomial $\pi_A(\lambda)$, and let Y with $n \geq \phi$ columns chosen at random. If $K = GF(q)$ then $Prob\{dim\langle Y \rangle = \nu\} \geq \Phi(\pi_A, \phi)$.

Proposition 8.2 Let A be a $N \times N$ matrix over K with minimal polynomial $\pi_A(\lambda)$, and let X and Y be chosen at random with m rows and n columns. If $m \geq \min\{\phi, n\}$, then $D_Y(\lambda) = D_W(\lambda)$ with probability no less than $\Phi(\pi_A, \min\{\phi, n\})$.

Proposition 6.1: The minimal generating polynomial $D_{\bar{Y}}$ for the generic sequence $\{A^i \bar{Y}\}$ has determinantal degree ν .

2.6 of KaVi04: $rank(Hk_{e,d}) = deg(det(F_X^{A,Y}))$ for $d \geq deg(F_X^{A,Y})$ and $e \geq n$

2.7 of KaVi04: $\nu = \max\{rank(Hk_{e,d}(A, X, Y))\}$ over all possible e, d, X, Y . Moreover, ν is equal to the sum of the degrees of the first M invariant factors of $\lambda I - A$ (where M is the size of X, Y)

2.12 of KaVi04: Let s_i, \dots, s_ϕ be all the invariant factors of $\lambda I - A$. This i^{th} invariant factor of $F_X^{A,Y}$ divides s_i . Furthermore, there exist matrices W, Z st $\forall i, 1 \leq i \leq \min(M, \phi)$, the i^{th} invariant factor of $F_W^{A,Z}$ is equal to s_i (all other remaining ones are equal to 1).

Proposition 1: If we choose random matrices X, Y , then $deg(det(F_X^{A,Y})) = dim(\langle \bar{Y} \rangle)$ with high probability.

Proof: Directly follows from the theorems 8.1 and 8.2 and proposition 6.1

Proposition 2: For random choice of blocking matrices W, Z , the i^{th} invariant factor of $F_W^{A,Z}$ is equal to the i^{th} invariant factor of A for $1 \leq i \leq \min(M, \phi)$ (with all other remaining factors equal to 1) with high probability.

Proof: We choose \mathbb{X}, \mathbb{Y} as the specialization of \bar{X}, \bar{Y} given in (Villard, corollary 6.4). From the proof of theorem 2.12, we have that

$$deg(det(F_{\mathbb{X}}^{A,\mathbb{Y}})) = \max_{X,Y}(deg(det(F_X^{A,Y})))$$

Now, by proposition 1, for any random matrices W, Z , with high probability,

$$deg(det(F_W^{A,Z})) = deg(det(F_{\mathbb{X}}^{A,\mathbb{Y}}))$$

Assume $deg(det(F_W^{A,Z})) = \nu$ and let \bar{s}_i be the i^{th} invariant factor $F_W^{A,Z}$ then, by the first assertion of theorem 2.12, \bar{s}_i divides s_i . Since ν is the sum of the degrees of the invariant factors of $\lambda I - A$, this can only happen if $s_i = \bar{s}_i$ by the same reasoning as the end of theorem 2.12.