Generalizations and Variations of Quillen-Suslin Theorem and their Applications

Hyungju Park
Korea Institute for Advanced Study
(KIAS)

Questions I hope to address

- What does the original Quillen–Suslin Theorem say?
- Quillen–Suslin and K_0 group of the polynomial ring?
- What is the K_1 analogue of Quillen–Suslin?
- Gubeladze's generalization of Quillen–Suslin? ➔ coordinate ring of a toric variety is hermite (a la T.Y. Lam)
- Why does Quillen–Suslin have anything to do with Digital Signal Processing??? Wavelets?
- Unimodular Completion for Linear Phase Filter Banks?
- Over D–modules? ➔ Stafford Theorem: Hildebrand–Schmale, Leykin, Quadrat, Gago–Vargas
- What is a parahermitian analogue of Quillen–Suslin?
- Why can we view the Lin–Bose Conjecture as a generalization of Quillen–Suslin? ➔ proofs by Pommaret, Pa, Srinivas

Basics on Quillen-Suslin:
Module theoretic and geometric

- Serre conjecture, 1955: Any (f.g. and proj.) module over a polynomial ring is free, or any vector bundle over an affine space is trivial. ➔ Quillen-Suslin Theorem, 1976
- $K_0[x\_1,\ldots,x\_n]=\mathbb{Z}$
- Algorithmic Form: Given a (f.g. and proj.) module over a polynomial ring, can we find its free basis? ➔ Fitchas-Galligo (1990), Logar-Sturmfels (1992), Pa-Woodburn (1995), Lombardi-Yengui (2005)

Basics on Quillen-Suslin: A motivating example

- $A=(1-xy,\ x^2,\ y^3)^t \in R^3$ where $R=\mathbb{C}[x,y]$.
- A is a unimodular vector over R

➔ By Nullstellensatz, we get an exact sequence

$$0 \to S \to R^3 \to R \to 0$$

$$(h_1,h_2,h_3) \mapsto h_1(1-xy)+h_2x^2+h_3y^3$$

- This sequence splits

➔ S is projective

➔ S is free of rank 2 (by Quillen-Suslin).

- A syzygy computation with GB gives

$S=\langle(0,-y^3,x^2),\ (-y^3,0,1-xy),\ (-x^2,1-xy,0)\rangle$.

➔ can NOT get a minimal set of generators for S!!!

Suslin's Stability

- An elementary matrix $E_{ij}(f)$: its diagonals are 1's, its (i,j) entry is f, and other entries are 0's.
- Given: $A \in SL_p(k[x_1,\ldots,x_m])$
- Problem: Write A as a product of elementary matrices. Or is it possible at all?
- Suslin's Stability Theorem (K_1–analogue of Quillen–Suslin Theorem, 1977): Such factorization exists if $p \geq 3$. Equivalently,

  $SL_p(k[x_1,\ldots,x_m]) = E_p(k[x_1,\ldots,x_m])$, $\forall p \geq 3$
- Algorithmic Proof: Pa and Woodburn (1995). Uses a successive localizations of a ring, and GB.
- A heuristic algorithm: Implemented but not published (by Pa).

- Example: Factor the following matrix into elementary matrices:

$$A = \begin{pmatrix} 1-xy & x^2 & 0 \\ -y^2 & 1+xy & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Suslin's Stability: the unfortunate case

- $A \in SL_2(k[x_1,\ldots,x_m])$
- Problem: Determine if A can be decomposed into elementary matrices, and if it can, find such a factorization.
- Counter-example:

  Cohn matrix

$$A = \begin{pmatrix} 1-xy & x^2 \\ -y^2 & 1+xy \end{pmatrix}$$

- Algorithm: Pa (1999). Uses a monomial order.

Gubeladgze's generalization

Toric analogue of Quillen-Suslin

- Anderson's Conjecture, 1978: Quillen-Suslin holds for affine normal subrings of polynomial rings generated by monomials
- Gubeladze'sTheorem, 1988: Q-S holds for monoid rings of seminormal monoids.
- For normal monoids, this says in geometric language that algebraic vector bundles over affine toric varieties are trivial.
- $I_{\mathcal{A}}$: a toric ideal in $k[x_1,\ldots,x_m]$. Then any (f.g. and proj.) modules over $k[x_1,\ldots,x_m]/I_{\mathcal{A}}$ are free. (c.f. Swan's Theorem for the case of a torus)
- Algorithm: Laubenbacher-Woodburn, 1997

1-D Discrete-time Signals

- A discrete-time signal is a sequence of real numbers, i.e.

  $(a_n)_{n\in\mathbb{Z}} = (\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots)$

  where a_n is in $\mathbb{R}$ and there exists an integer N s.t. $a_n=0$ for all $n<N$.
- The set $\mathcal{S}$ of discrete-time signals forms an $\mathbb{R}$-vector space with the operations of superposition and scalar multiplication of sequences.

1-D Discrete-time Signals

- For given two signals (a_n) and (c_n), define their convolution $(b_n):=(a_n)*(c_n)$ by

$$b_n := \sum_{i+j=n} a_i c_j$$

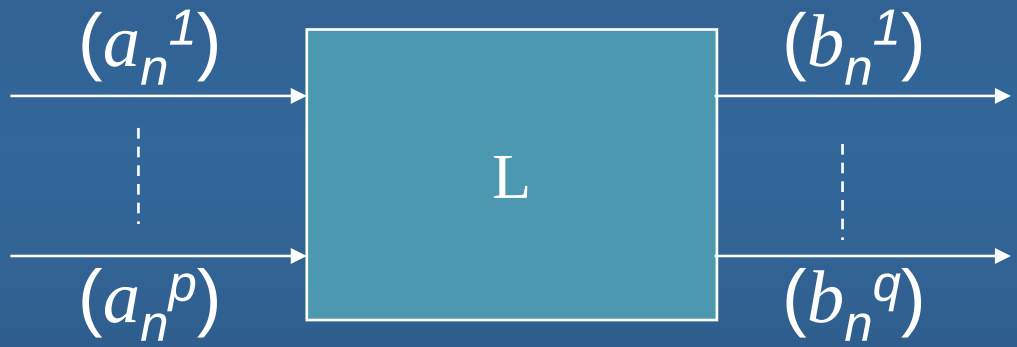
- The set S of discrete-time signals equipped with superposition and convolution forms a commutative ring with identity (e_n), where $e_n = \delta_{n,0}$. The identity element (e_n) is called the impulse.

Linear Time Invariant System

- Single-Input Single-Output (SISO) System

Linear Time Invariant System

- Multi-Input Multi-Output (MIMO) System



- A p-input q-output linear time-invariant system is an $\mathcal{S}$-module homomorphism from $\mathcal{S}^p$ to $\mathcal{S}^q$ defined by convolutions with various fixed signals.

Algebraic Formulation

- The ring $\mathcal{S}$ of discrete-time signals is isomorphic to the ring $\mathbb{R}[[z^{-1}]]_{z^{-1}}$ via the Z-transform

$$(a_n) \mapsto \sum_{n=-\infty}^{\infty} a_n z^{-n}$$

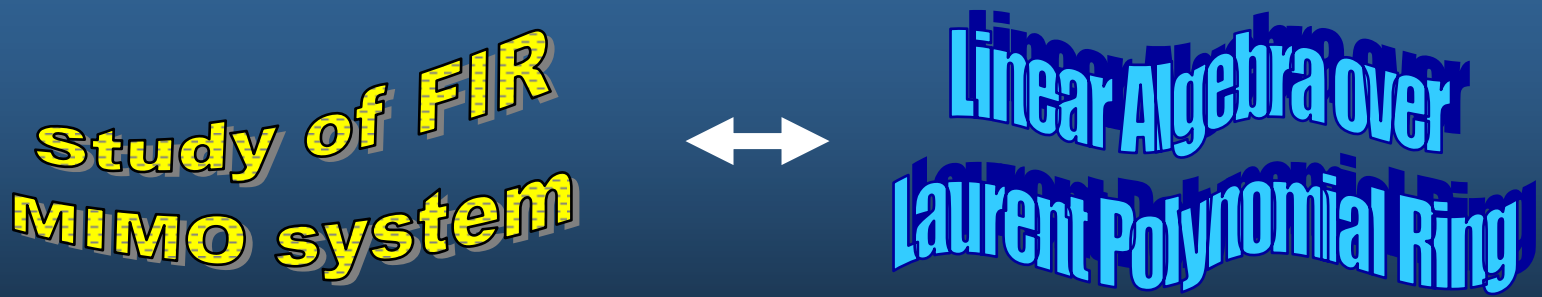
- Linear Time Invariant System → multiplication by f in $\mathbb{R}[[z^{-1}]]_{z^{-1}}$
- FIR system → multiplication by a Laurent polynomial in $\mathbb{R}[z,z^{-1}]$

Algebraic Formulation

- MIMO system → $f : (\mathbb{R}[z^{\pm}])^p \rightarrow (\mathbb{R}[z^{\pm}])^q$

  A multiplication by a matrix, i.e.

$$f \in \mathsf{M}_{qp}(\mathbb{R}[z^{\pm}])$$



Extensions to higher dimensions

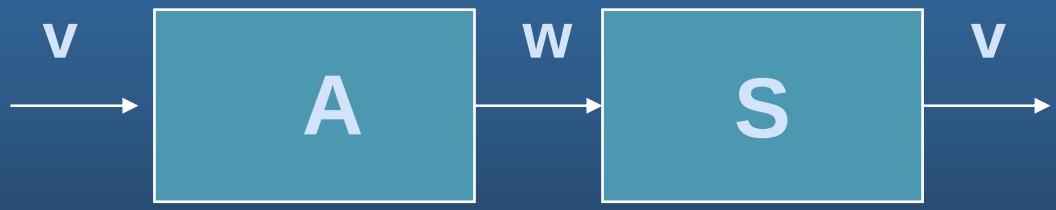
- An m-D discrete-time signal is a multiply-indexed sequence of real numbers, i.e. $(a_{i_1 \ldots i_m})_{(i_1,\ldots,i_m)\in\mathbb{Z}^m}$
- The ring of m-D discrete-time signals is naturally isomorphic to the ring

$$\mathbb{R}[[z_1^{-1},\ldots,z_m^{-1}]]_{z_1^{-1}\ldots z_m^{-1}}$$

via the Z-transform

Perfect Reconstruction of Signals

- An FIR system ⟷ A matrix with Laurent polynomial entries
- A Laurent polynomial matrix A is perfect reconstructing or unimodular if A has a left inverse, i.e. there exists S s.t. S A = I.



- **Problem**: For a given analysis system A, determine if A allows perfect reconstruction, and if it does, find all of its PR synthesis systems.

Perfect Reconstruction 1-D Example:

- Describe all the left inverses of the matrix

$$A := \begin{pmatrix} f_1(z) \\ f_2(z) \\ f_3(z) \end{pmatrix} = \begin{pmatrix} \frac{1}{z} + 1 + 2z \\ \frac{2}{z^2} + 1 \\ 1 - z \end{pmatrix}$$

- That is, describe the set L of all Laurent polynomial triples (g_1, g_2, g_3)'s s.t.

$$g_1(z)\, f_1(z) + g_2(z)\, f_2(z) + g_3(z)\, f_3(z) = 1.$$

- Hilbert Nullstellensatz: A is perfect reconstructing iff $f_1(z)$, $f_2(z)$, $f_3(z)$ have no common roots in $\mathbb{C}^*$.
- This problem can be easily solved by using Euclidean Division.

Quillen-Suslin Setup

- $R=\mathbb{C}[z,z^{-1}]$
- $0 \to S \to R^3 \xrightarrow{\cdot A} R \to 0$

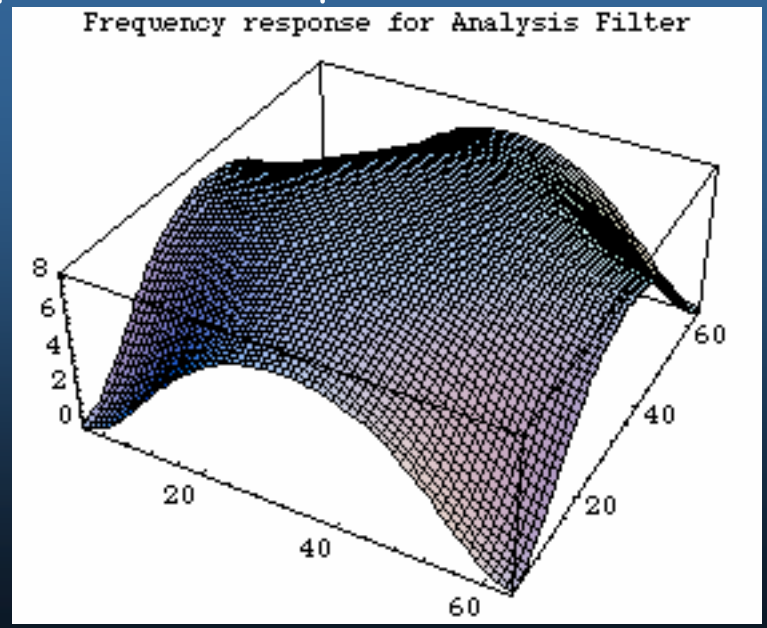
  $(h_1,h_2,h_3) \mapsto h_1f_1+h_2f_2+h_3f_3$
- This sequence splits ➔ S is projective
- By Quillen-Suslin over R, S is free of rank 2. ➔ ∃ a free basis $\{v_1, v_2\} \subset R^3$ for the module S of sygyzies.
- By GB, find a particular left inverse $v_p=(g_1,g_2,g_3)$ of $A=(f_1,f_2,f_3)^t$. Then the set of all the left inverse of A is $\{v_p+a_1v_1+a_2v_2 \mid a_1,a_2 \in R\}$.

Perfect Reconstruction: 2-D Example

- Consider the filter $G(z_1,z_2)$ with this impulse response, i.e. $G(z_1,z_2) = \Sigma g_{ij}\, z_1^{-i}\, z_2^{-j}$ where g_{ij} is given by this matrix.

$$\frac{1}{4096}\begin{pmatrix} 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 24 & -96 & 24 & 0 & 0 \\ 0 & 24 & -192 & 456 & -192 & 24 & 0 \\ 8 & -96 & 456 & 3200 & 456 & -96 & 840 \\ 0 & 24 & -192 & 456 & -192 & 24 & 0 \\ 0 & 0 & 24 & -96 & 24 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 \end{pmatrix}$$

- This filter has a diamond shaped low-pass frequency response.
- Does this filter have PR property? If it does, find a matching synthesis Filter.

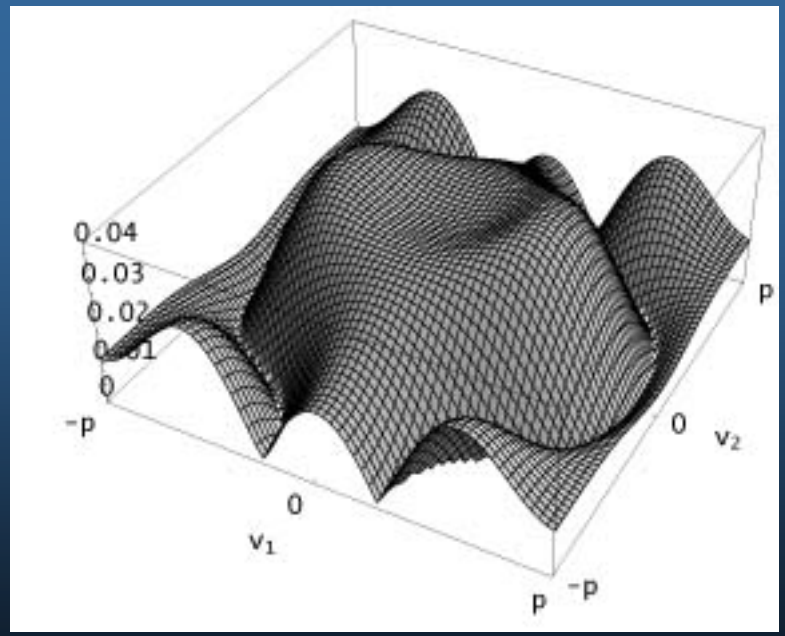


Perfect Reconstruction: 2-D Example

- Let $H(z_1,z_2)$ be the filter with this impulse response. Then $G(z_1,z_2)$ and $H(z_1,z_2)$ together make a 2-channel PR filter bank with quincunx sampling lattice.

$$\frac{1}{3585}\begin{pmatrix} 0 & 0 & 48 & 0 & 0 \\ 0 & 96 & 576 & 96 & 0 \\ 48 & 576 & 4288 & 576 & 48 \\ 0 & 96 & 576 & 96 & 0 \\ 0 & 0 & 48 & 0 & 0 \end{pmatrix}$$

- This particular synthesis filter was found by an algorithm based on Gröbner bases, and by performing a numerical optimization w.r.t. syzygy parameters.



Prime Factorization: module theoretic formulation

- V: a vector space of dim p over a field k.

➔ Any subspace of V can be generated by p vectors.

- $R:=k[x_1,\ldots,x_m]$, $K:=k(x_1,\ldots,x_m)$
- M: submodule of R^p with $\dim_K(M \otimes K) = p$ generated by $v_1,\ldots,v_q$, $q \geq p$
- Problem: When can M be generated by p vectors?
- Answer (Pommaret, Pa, Srinivas): Iff the ideal generated by maximal minors of the $p \times q$ matrix $A:=(v_1,\ldots,v_q)$ is principal.

Prime Factorization:

determinant extraction problem

- A: a pxq polynomial matrix, q≥p, of normal full rank.
- $a_1,\ldots,a_l$: maximal minors of A
- $d=\gcd(a_1,\ldots,a_l)$
- **Prob**: When does A allow a prime factorization, i.e. when can A be factored as follows?

$$A = \underset{p}{\left(\begin{array}{ccc} v_1 & \cdots & v_q \end{array}\right)}_{q} = \underset{p}{\left(\begin{array}{ccc} w_1 & \cdots & w_q \end{array}\right)}_{p} \underset{p}{\left(\begin{array}{c} \\ \end{array}\right)}_{q}$$

where det of W:=$\left(\begin{array}{ccc} w_1 & \cdots & w_q \end{array}\right)$ is d.

Prime Factorization: system theoretic formulation

- $b_1,\ldots,b_l$: reduced maximal minors of A, i.e. $a_i = d\ b_i$
- **Theorem** (Pommaret, P, Srinivas).

A allows (unimodular) prime factorization iff $b_1,\ldots,b_l$ have no common roots in k_{alg}.

- This result can be viewed as a module theoretic extension of Hilbert Nullstellensatz, and is trivial in 1-D case.
- This result has been known in 2-D case since early 80's (Youla, Gnavi, Guiver, Bose...)
- In m-D, Lin-Bose formulated this conjecture, and proved the equivalence of this conjecture to various statements of interest.
- This theorem can be re-stated as a matrix extension problem ➔ an extension of Q-S.

Hermitian analogue of Quillen–Suslin

- Raghunathan's Theorem: Any inner product space over a polynomial ring (with respect to the polynomial involution) is isometric to a trivial inner product space, i.e. a free module with an inner product represented by a diagonal matrix.

Parahermitian analogue of Quillen-Suslin

- R: a commutative ring with an involution σ
- $G=\{X_1^{n_1}X_2^{n_2}\cdots X_m^{n_m} \mid n_1,n_2,\ldots, n_m\in \mathbb{Z}\}$, the free abelian group with m generators $X_1, X_2,\ldots,X_m$.
- $R[X_1,X_1^{-1},\ldots,X_m,X_m^{-1}]$, the Laurent polynomial ring over R, can be viewed as the group ring R[G]
- R[G] has a natural involution σ_p that is compatible with σ, i.e.

  for $f=\sum a_{i_1\cdots i_m}X^{i_1}\cdots X^{i_m}$ with $a_{i_1\cdots i_m}\in R$,

  $\sigma_p(f)=\sum \sigma(a_{i_1\cdots i_m})X^{-i_1}\cdots X^{-i_m}$.

  ➔ parahermitian involution
- $\mathcal{M}$, a f.g. projective module over $R[X_1,X_1^{-1},\ldots,X_m,X_m^{-1}]$, and $<\ ,\ >$ be a hermitian sesquilinear form on $\mathcal{M}$ w.r.t. the involution σ_p.
- A pair $(\mathcal{M},<\ ,\ >)$ is called a parahermitian space over R[G], if $<\ ,\ >$ is nonsingular, i.e. if its adjoint $h: \mathcal{M}\to \mathcal{M}^*$ defined by $h(v)=<v,\ \cdot\ >$ for $v\in \mathcal{M}$ is an isomorphism.

Parahermitian analogue of Quillen–Suslin

- Definition: parahermitian matrix, paraunitary matrix (group), parahermitian conjugate, etc.
- Parahermitian analogue of Serre conjecture: Is every parahermitian space isometric to a trivial one?