Multivariate moment problems with applications to spectral estimation and physical layer security in wireless communications

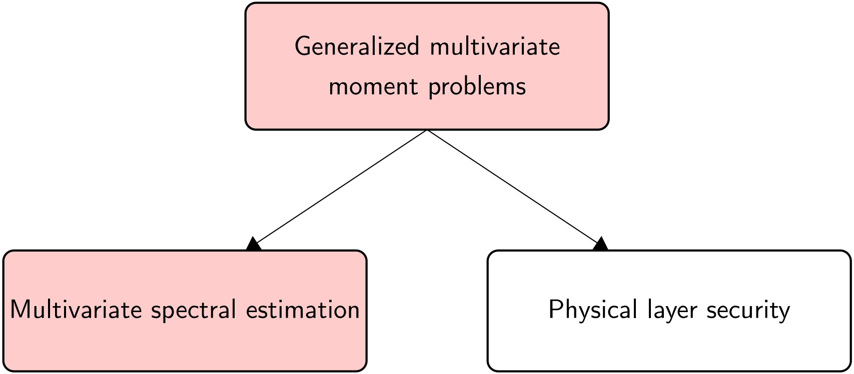
C. Masiero
Series XXVI
Advisor: Prof. Augusto Ferrante

Ph.D. School in Information Engineering,
Department of Information Engineering
University of Padova

April 11^{th}, 2014

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

Introduction



Multivariate spectral estimation

Framework

- Hypotheses: $y = \{y_k \,;\, k \in \mathbb{Z}\}$ is a zero mean, $\mathbb{R}^m-$valued, wide-sense stationary and purely non deterministic process
- Input: $\{y_k\}_{k=1}^N$ is an available finite data sequence
- Aim: Estimate the spectral density $\Phi(e^{j\vartheta})$ of y

- If Φ is rational, we can find a finitely-parametrized state-space model for the process

$$\Downarrow$$

smoothing, filtering, prediction...

- Thus, our aim is estimating rational spectral densities

Original contribution

Two novel approaches to multivariate spectral estimation:

1. Relative entropy rate estimation
2. Multivariate circulant rational covariance extension

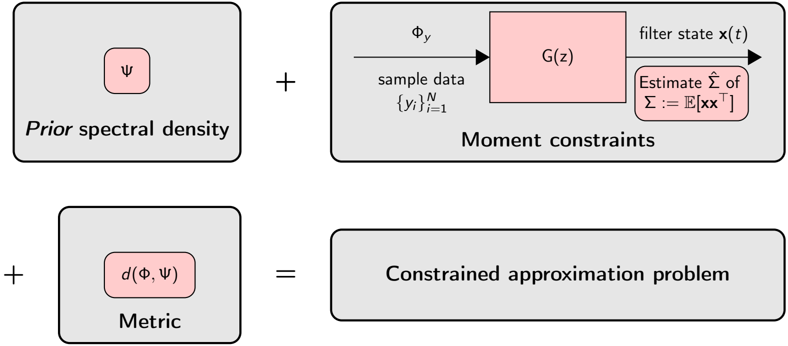
Spectral estimation as a generalized moment problem, that can be solved efficiently by means of convex optimization techniques

Multivariate spectral estimation

Relative entropy rate estimation

THREE-like spectral estimation

- We draw inspiration from THREE-like approaches[1]:



1 C. I. Byrnes, T. Georgiou, & A. Lindquist. "A new approach to spectral estimation: A tunable high-resolution spectral estimator". In: *IEEE Trans. Sig. Proc.* 49 (2000).

Spectrum approximation problem

Let $G(z)$ and $\Sigma = \Sigma^\top$ given. Compute

$$\hat{\Phi} := \quad \operatorname{argmin} d(\Phi, \Psi) \quad \text{such that} \quad \int G \Phi G^* = \Sigma$$

- Key point: choice of $d(\Phi, \Psi)$:
  1. Variational analysis should lead to a computable solution
  2. The solution should have low complexity

- Let y, z be Gaussian processes with densities Φ_y and Φ_z. Then, consider their relative entropy rate

$$d_{RER}(\Phi \| \Psi) = \frac{1}{2} \int_{-\pi}^{\pi} \log\det({\Phi_y}^{-1}\Phi_z) + \operatorname{Tr}\left[{\Phi_z}^{-1}(\Phi_y - \Phi_z)\right] \frac{d\vartheta}{2\pi}$$

- Set $d(\Phi, \Psi) = d_{RER}(\Phi \| \Psi)$. Spectral estimation is recast as a convex optimization problem

RER Spectrum approximation problem

$$\hat{\Phi} := \operatorname{argmin} d_{RER}(\Phi \| \Psi) \quad \text{such that} \int G \Phi G^* = \Sigma$$

- The solution of the dual problem, $\hat{\Lambda}$, exists and it is unique.
- Then,

$$\hat{\Phi} = \left[\Psi^{-1} + G^* \hat{\Lambda} G\right]^{-1}, \quad \deg(\hat{\Phi}) \leq \deg \Psi + 2n$$

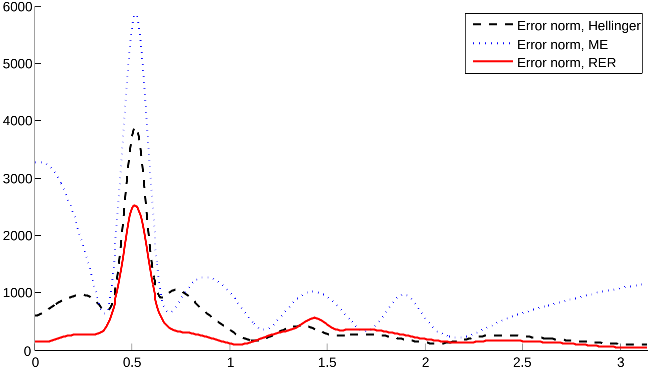
  while the best one so far available in the multivariate framework is $\deg \Psi + 4n$ [2]
- $\hat{\Lambda}$ can be computed via an efficient matricial Newton-like algorithm

---

2

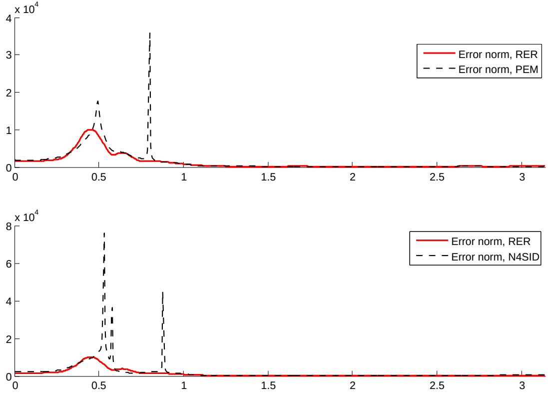
A. Ferrante, M. Pavon, & F. Ramponi. "Hellinger vs. Kullback-Leibler multivariable spectrum approximation". In: *IEEE Trans. Aut. Control* 53 (2008), pp. 954–967.

Simulation results



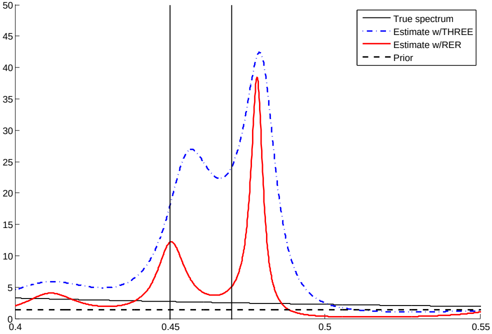
Comparison of THREE-like approaches (average estimation error).
Bivariate model; 40*th* order; $G(z)$ with 4 complex pairs of poles equispaced in $[0, \pi]$ with radius 0.7; Prior: PEM(3) model.
RER: estimate order = 11; Hellinger: estimate order = 19.

Simulation results (cont'd)



Comparison of RER, PEM and N4SID (average estimation error) for short data record ($N = 100$)

Simulation results (cont'd)



Comparison of THREE and RER in detecting spectral lines.
Poles of $G(z)$: $0.95 \pm j0.42$, $0.95 \pm j0.44$, $0.95 \pm j0.46$, $0.95 \pm j0.48$, $0.95 \pm j0.50$

Conclusions

RER (Relative Entropy Rate) estimator

- Spectral estimation as a convex spectrum approximation problem
- The upper bound on the complexity of the solution improves on the best one so far available in the multivariate framework
- The estimator is effective, especially in case of short data records
- The estimator exhibits high resolution features

Multivariate spectral estimation

Multivariate circulant rational covariance extension

Rational covariance extension

Given the sequence $C_k := \mathbb{E}[y(t+k)y^*(t)]$, for $k = 0, \dots, n$ find $C_{n+1}, C_{n+2}, \dots$ up to infinity such that

$$\sum_{k=-\infty}^{+\infty} C_k e^{-jk\vartheta}, \quad C_{-k} = C_k^*$$

converges for all $\vartheta \in \mathbb{T}$ to a positive definite spectral density $\Phi(e^{j\vartheta})$ that has the rational form

$$\Phi(e^{j\vartheta}) = P(e^{j\vartheta})Q^{-1}(e^{j\vartheta}).$$

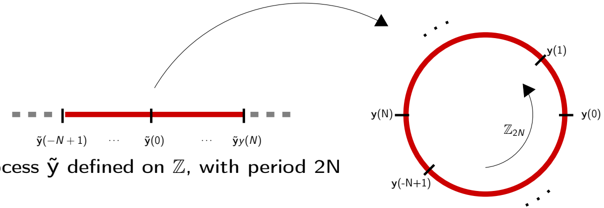
Our contribution

Circulant Rational Covariance Extension

- A convex optimization-based approach which provides multivariate rational covariance extension for periodic processes
- Efficient approximating procedure for regular multivariate rational covariance extension

Circulant rational covariance extension

- Periodic processes as processes indexed on $\mathbb{Z}_{2N}$:



Process $\tilde{\mathbf{y}}$ defined on $\mathbb{Z}$, with period 2N

Process $\mathbf{y}$ defined on $[-N+1, N]$ with mod $2N$ arithmetics

$$\mathbf{y} := \begin{bmatrix} \mathbf{y}(-N+1) \\ \vdots \\ \mathbf{y}(0) \\ \vdots \\ \mathbf{y}(N) \end{bmatrix}$$

- $\mathbf{y}$ is the restriction on $[-N+1, N]$ of $\tilde{\mathbf{y}}$ if and only if its covariance matrix $\Sigma := \mathbb{E}[\mathbf{y}\mathbf{y}^*]$ is block-circulant

$$\Sigma = \underbrace{\begin{bmatrix} C_0 & C_1^* & \cdots & C_1 \\ C_1 & C_0 & \cdots & C_2 \\ \vdots & \vdots & \ddots & \vdots \\ C_1^* & C_2^* & \cdots & C_0 \end{bmatrix}}_{\mathrm{Circ}\{C_\mathbf{0}, C_\mathbf{1}, \dots, C_\mathbf{N}, C^*_{\mathbf{N-1}}, \dots, C^*_\mathbf{1}\}}$$

Multivariate circulant rational covariance extension - 1

Problem statement

Given the sequence C_k's with values in $\mathbb{C}^{m\times m}$, for $k=0,\dots,n$, for $n<N$, find a rational spectral density $\Phi = PQ^{-1}$ such that

$$\int_{\pi}^{\pi} e^{jk\vartheta}\Phi(e^{j\vartheta})d\nu(\vartheta) = \frac{1}{2N}\sum_{h=-N+1}^{N} {\zeta_h}^k\Phi(\zeta_h) = C_k, \quad k=0,1,\dots,n.$$

Main results:

1. Parametrization of all the solutions in terms of $P(\zeta)$
2. Simultaneous estimation of P and Q based on the available data

- Assumption: $P(\zeta) = p(\zeta)I$

Multivariate circulant rational covariance extension - 2

Main Theorem

- Assume $P(\zeta) = p(\zeta)I$ is given. There exists a unique $\hat{Q}(\zeta)$ such that $\hat{\Phi}(\zeta) := P(\zeta)\hat{Q}(\zeta)^{-1}$ maximizes the generalized entropy

$$\mathbb{I}_P(\Phi) = \int_{-\pi}^{\pi} P(e^{j\vartheta}) \log\det \Phi(e^{j\vartheta}) d\nu(\vartheta)$$

  and solves the circulant covariance extension problem.
- $\hat{Q}(\zeta)$ is the unique minimizer of

$$\mathbb{J}_P(Q) := \langle C, Q \rangle - \int_{-\pi}^{\pi} P(e^{j\vartheta}) \log\det Q(e^{j\vartheta}) d\nu(\vartheta)$$

- $\hat{P}(\zeta)$ and $\hat{Q}(\zeta)$ can be estimated simultaneously by taking into account logarithmic moments, too.

Regular covariance extension by means of circulant rational covariance extension

1. It can be proved that, for $N \to \infty$, the solution of circulant rational covariance extension tends to the solution of regular covariance extension.

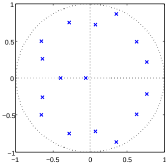
2. Circulant rational extension can be implemented efficiently (FFT)

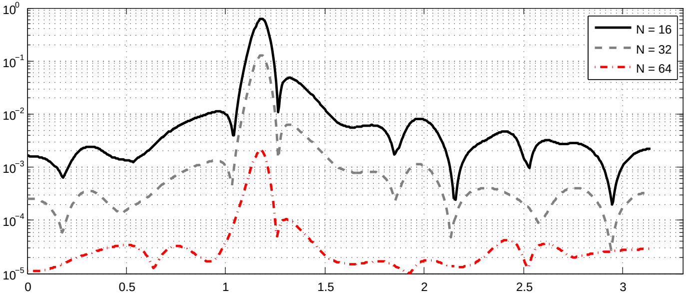
$$\Downarrow$$

Circulant rational extension provides a fast approximating procedure for solving regular rational covariance extension problem

Numerical examples: multivariate AR case

MVAR model of order 8



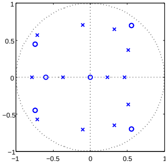


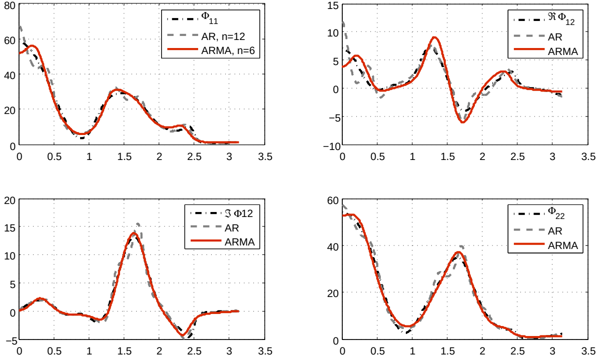
Estimation error

- The approximation gets more accurate as $N \to \infty$.

Numerical examples: multivariate ARMA case

Zero poles map





Comparison between AR (N=64, n=12) and ARMA (N=32,n=6)

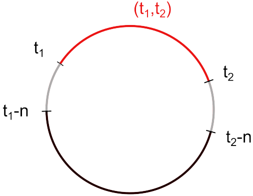
- Determining P from logarithmic moments yields better results.

Bilateral ARMA models

- After solving the circulant rational covariance extension problem we end up with a bilateral ARMA model:

$$\sum_{k=-n}^{n} Q_k y(t-k) = \sum_{k=-n}^{n} P_k e(t-k), \quad t \in \mathbb{Z}_{2N}$$

- Open problem: do bilateral ARMA models generalize standard models for reciprocal processes[3]?



Reciprocal process of order n

$$\sum_{k=-n}^{n} Q_k y(t-k) = e(t), \quad t \in \mathbb{Z}_{2N}$$

[3] A.J. Krener et al, B.C. Levy et al, A. Chiuso et al, F.P. Carli et al.

Conclusion

Circulant Rational Covariance Extension

- A first step towards rational covariance extension for multivariate periodic processes
- Fast approximation of regular multivariate rational covariance extension

Future Work

Relative Entropy Rate Estimation

- Application to graphical models

Multivariate Circulant Rational Covariance Extension

- Extension to rational models with general $P(\zeta)$
- Connection with reciprocal models

Thank you for your attention

A. Lindquist, C. Masiero, & G. Picci. "On the Multivariate Circulant Rational Covariance Extension Problem". In: *Proc. of 52nd IEEE CDC*. 2013.

A. Ferrante, C. Masiero, & M. Pavon. "Time and spectral domain relative entropy: A new approach to multivariate spectral estimation". In: *IEEE Trans. Aut. Contr* 57 (2012).

A. Ferrante, C. Masiero, & M. Pavon. "A New Metric for Multivariate Spectral Estimation Leading to Lowest Complexity Spectra". In: *Proc. of the 50th IEEE CDC - ECC*. 2011.

Determining P from logarithmic moments

- Aim: estimate P based on data only
- Idea: look for the spectral density Φ which maximizes the entropy gain

$$\int_{-\pi}^{\pi} \log\det \Phi(e^{j\vartheta})\ d\nu(\vartheta)$$

while satisfying the moment constraints which stem from the available covariance lags and the logarithmic moments

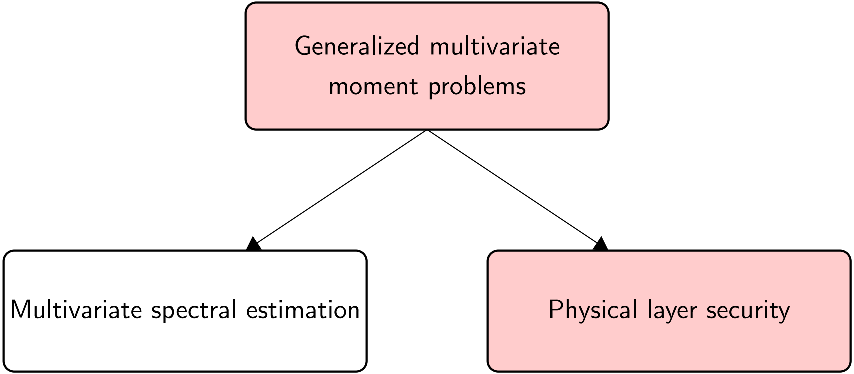
$$\gamma_k = \int_{-\pi}^{\pi} e^{jk\vartheta} \log\det \Phi(e^{j\vartheta}) d\nu(\vartheta), k = 1, 2, \dots, n$$

- The problem can be solved by minimizing

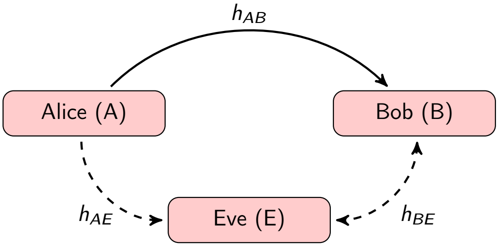
$$\mathbb{J}(P, Q) := \langle C, Q\rangle - \int_{-\pi}^{\pi} P(e^{j\vartheta}) \log\det Q(e^{j\vartheta}) d\nu(\vartheta) - \langle \Gamma, P\rangle + \int_{-\pi}^{\pi} P(e^{j\vartheta}) \log\det P(e^{j\vartheta}) d\nu(\vartheta)$$

Physical layer security in wireless communication

Introduction



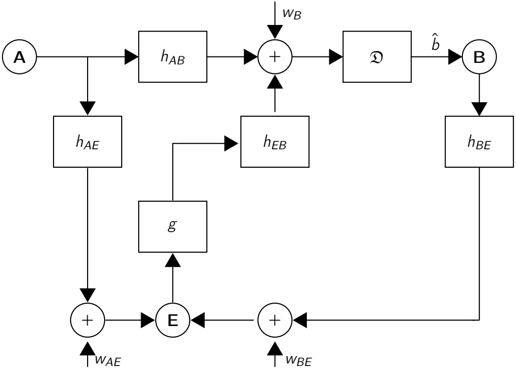
Framework



Task

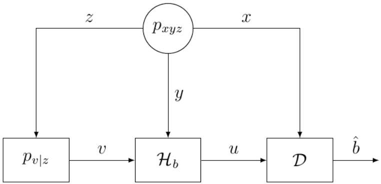
Authenticate the source of a messagge in a wireless communication scenario

Why physical layer authentication?



- Its performances are not undermined in case the attacker has high computational capabilities.
- It provides theoretical bounds which are not affected by the particular forgery strategy employed by the attacker.

Channel security: a hypothesis testing problem



- $\mathcal{H}_0$: legitimate packet;
  $\mathcal{H}_1$: forged packet
- α := false alarm probability;
  β := miss detection probability;

Aim

Compute theoretical bounds on the region of achievable type I and type II error probabilities.

Tightest bound on the error region

- We can prove that worst case performance of the security mechanism can be evaluated by computing

$$\inf_{p_{\mathbf{xv}} \in \mathcal{Q}} \mathcal{D}(p_{xv} \| p_{xy})$$

- The optimal attacking strategy corresponds to a Gaussian p.d.f. p_{xvz} with zero mean and covariance matrix

$$K_{\left[\begin{smallmatrix}\mathbf{x}\\ \mathbf{v}\\ \mathbf{z}\end{smallmatrix}\right]}(Z, C) = \begin{bmatrix} K_{\mathbf{xx}} & K_{\mathbf{xz}} K_{\mathbf{zz}}^{-1} Z^* & K_{\mathbf{xz}} \\ Z K_{\mathbf{zz}}^{-1} K_{\mathbf{xz}}^* & Z K_{\mathbf{zz}}^{-1} Z^* + C C^* & Z \\ K_{\mathbf{xz}}^* & Z^* & K_{\mathbf{zz}} \end{bmatrix}$$

- An iterative fixed point algorithm was designed, aiming at solving

$$\begin{cases} C^*(k+1) = C^*(k)(Z(k)K_{\mathbf{zz}}^{-1} B K_{\mathbf{zz}}^{-1} Z^*(k) + C(k)C^*(k))^{-1} A \\ Z^*(k+1) = K_{\mathbf{zx}} K_{\mathbf{xx}}^{-1} K_{\mathbf{xy}} + B K_{\mathbf{zz}}^{-1} Z^*(k)(Z(k)K_{\mathbf{zz}}^{-1} B K_{\mathbf{zz}}^{-1} Z(k)^* + C(k)C^*(k))^{-1} A \end{cases}$$

- Extensive simulations suggest that the algorithm always finds a minimum point for the cost function.