Putting "Reproducible Signal Processing" into practice:

A case study in Watermarking

M. BARNI, G. BARTOLI - (UNIVERSITY OF SIENA, ITALY)
F. PÉREZ-GONZALEZ, P. COMESAÑA - (UNIVERSITY OF VIGO, SPAIN)

Signal processing and scientific methodology

- Many signal processing papers lack rigorous **experimental validation**
  - Theoretical papers are often verified by a **single experiment** carried out on a single signal/image
  - Performance are only rarely compared with those of competing schemes
  - Improvements are often justified by comparing with only **one similar algorithm** performing worse

- Even worse: vaguely described **experimental conditions** → no reproducibility of results
- Often, readers must simply trust the authors !

Why is this so ?

- We all recognize the importance of good experiments but ...
  - Lack of time
  - Lack of research groups devoted to experimental signal processing or implementing someone else's algorithms
  - Non-rewarding work
  - Intellectual property issues
- Encourage good experimental research
- Define a rigorous format for experiment description

Our approach to RSP

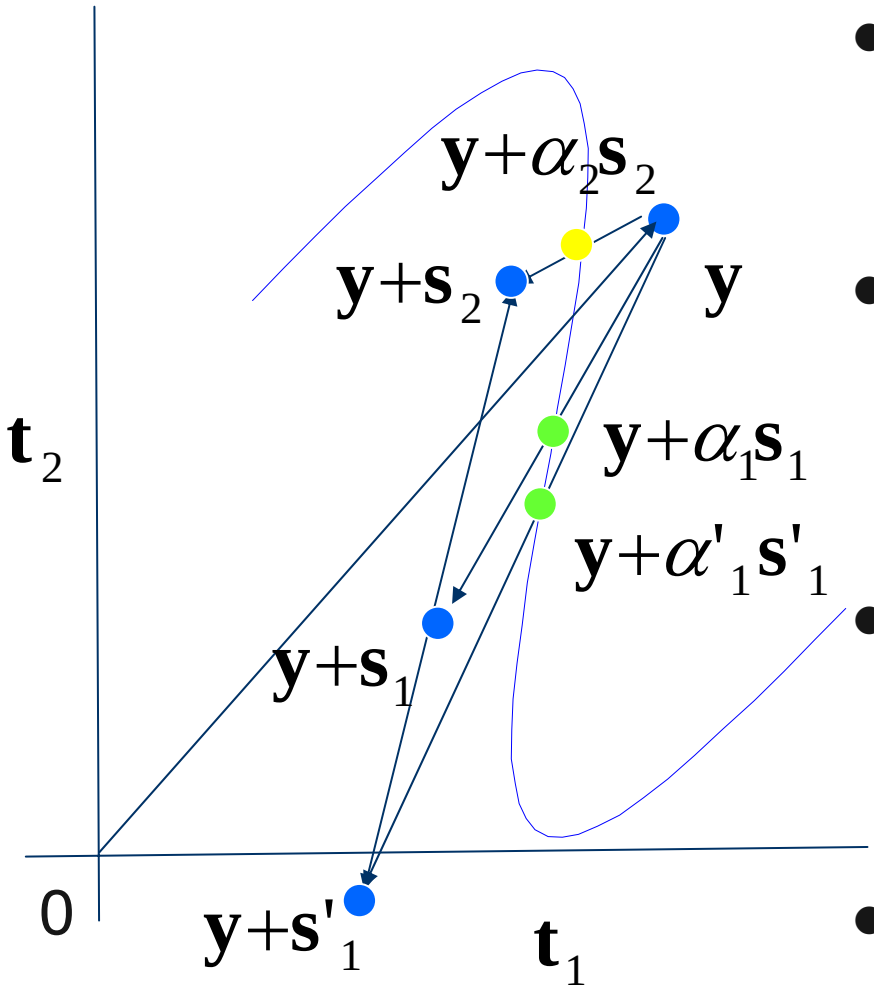
- A straightforward approach... **share** the software and the data set
- Problems:
  - **Portability**: which format should be used ?
  - **Readability**: are the authors correctly implementing the described algorithm ?
  - **Licensing problems**: open source or binary format ?
- Algorithms and experiments have always to be carefully described:
  - Description (a block diagram or a pseudo-code)
  - Parameters
  - Dataset

A case study (*in watermarking*)

- UNIVigo provided an RSP description of a paper
- UNISI tries to reproduce UNIVigo's results

- Goals of an **oracle attacker**:
  - Try to remove the watermark from a host signal/image
- Features:
  - **No knowledge** about the watermarking algorithm
  - Suitable for attacking **general detection functions**
  - Based only on the **binary output** of the detector

Algorithm steps



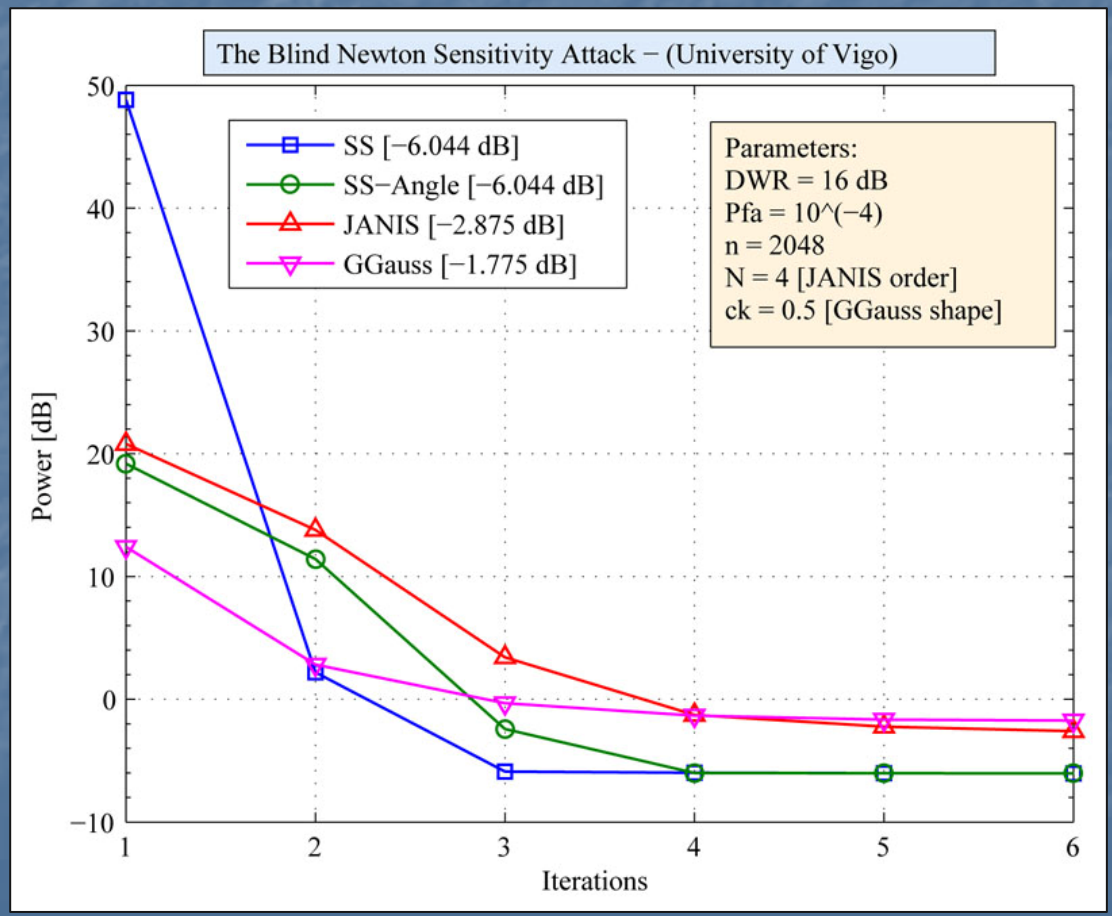
- Step1: Get perturbartion and find α such that $\mathbf{y}+\alpha\mathbf{s}$ is on the boundary.
- Step 2: Numerically evaluate gradient of $d_{\mathbf{y}}(h_{\mathbf{y}}(\mathbf{s}))$ and possibly Hessian on the boundary.
- Step 3: Update

$$\mathbf{s}_{k+1} = \mathbf{s}_k - \xi_k \cdot \left[\nabla^2 (d_{\mathbf{y}} \circ h_{\mathbf{y}})(\mathbf{s}_k)\right]^{-1} \cdot \nabla (d_{\mathbf{y}} \circ h_{\mathbf{y}})(\mathbf{s}_k)$$

- Step 4: Go back to 1.

Our RSP objective

- To **reproduce** the results obtained by the authors of the paper (*University of Vigo*)



The experience we made

- Originale paper (common problems)
  - Focus on the algorithm core
  - Missing informations on initialization and/or stop condition details
- **Vigo** supplied material:
  - pseudo-code description
  - initialization procedure
  - Data set: synthetic random sequences (algorithm provided)
- **Siena** implemented the BNSA algorithm
  - The implementation of BNSA did not raise any particular problem
  - Nevertheless, several ambiguities were still present...

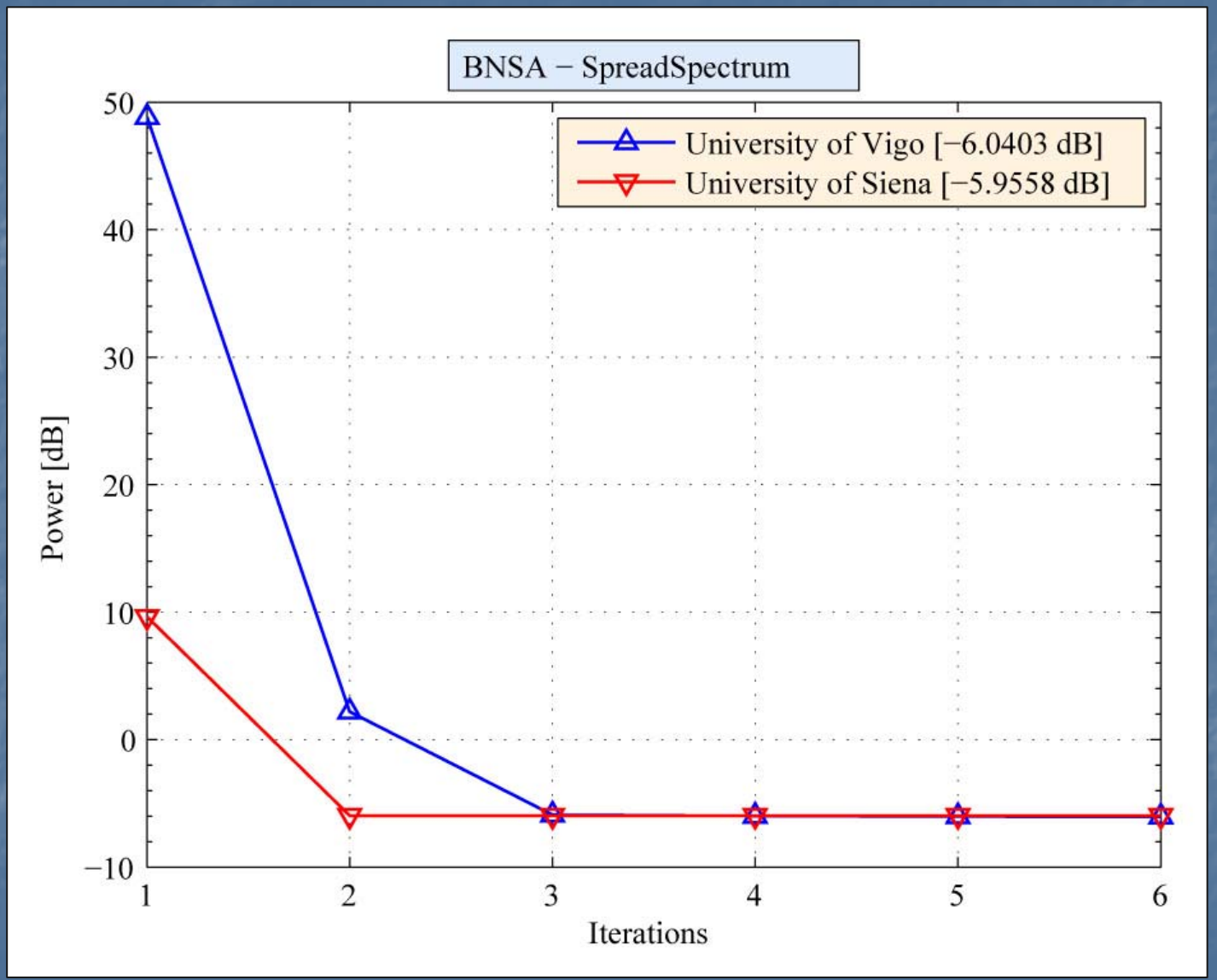
Insights we've got

- How to interpret graphs with no tables ? How were the results on the 100-trials sequences averaged
  - UniVIGO itself had difficulties in reproducing results.
- A few ambiguities about the **initialization** like 0/0 singularities or infinite loops
  - This was explained with direct communication between the two universities
- UNIVigo used an **approximation** of the gradient instead of the true Hessian (different plots in the paper used different set-ups)
  - Siena obtained comparable results also with the approximated version (scientific insight)

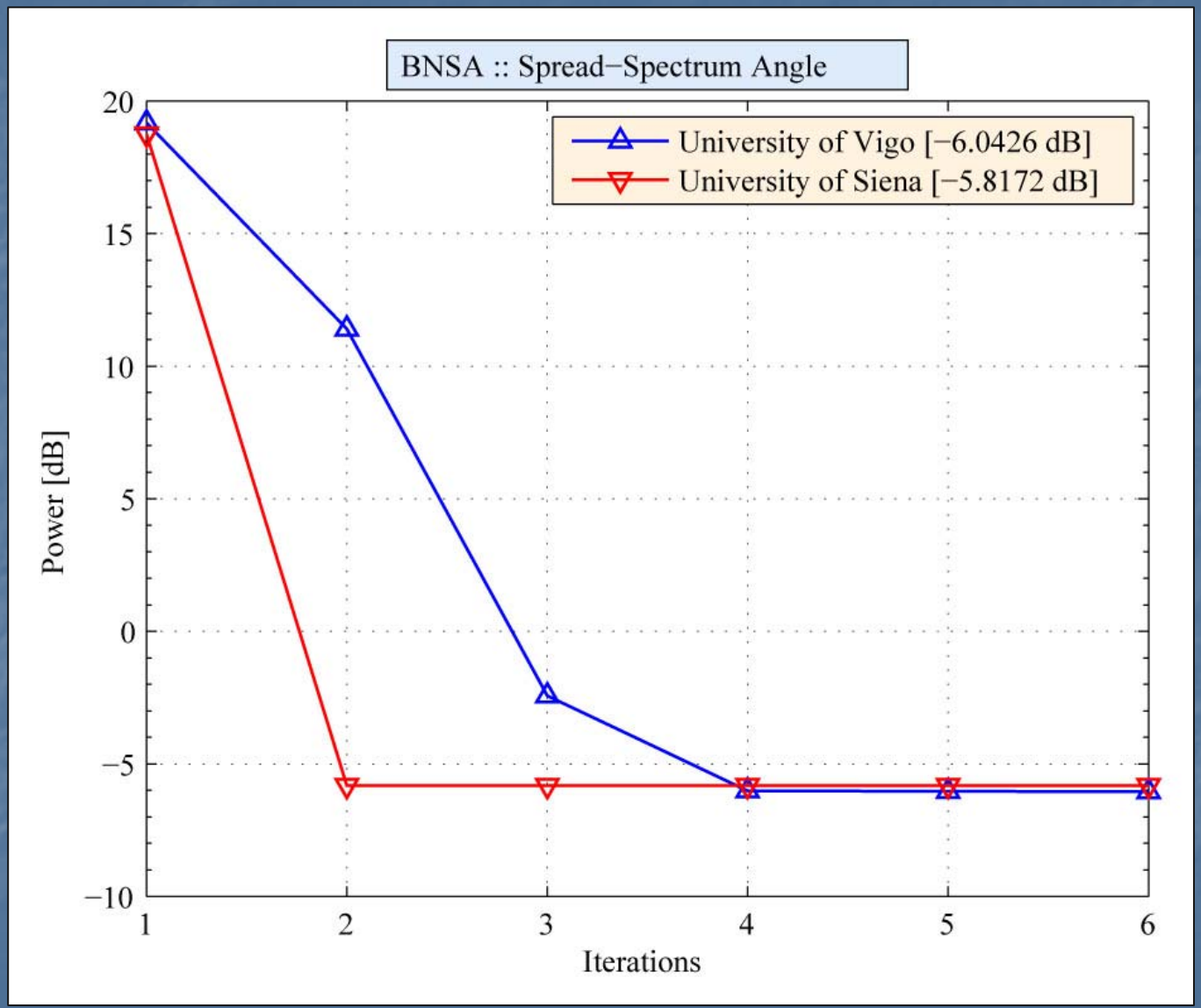
Insights we've got

- **MAIN PROBLEM**
- The re-implementation of **watermarking methods** (SS, SS-Angle, JANIS, GG) raised several interpretation problems
  - Communication between UNIVigo and UNISI was necessary
- **Estimation of false detection** probability was crucial for reproducibility, however, the way it was estimated was not clear
  - Different assumptions (no widely accepted solution) for the estimation
  - How often were the statistical parameters refreshed ?

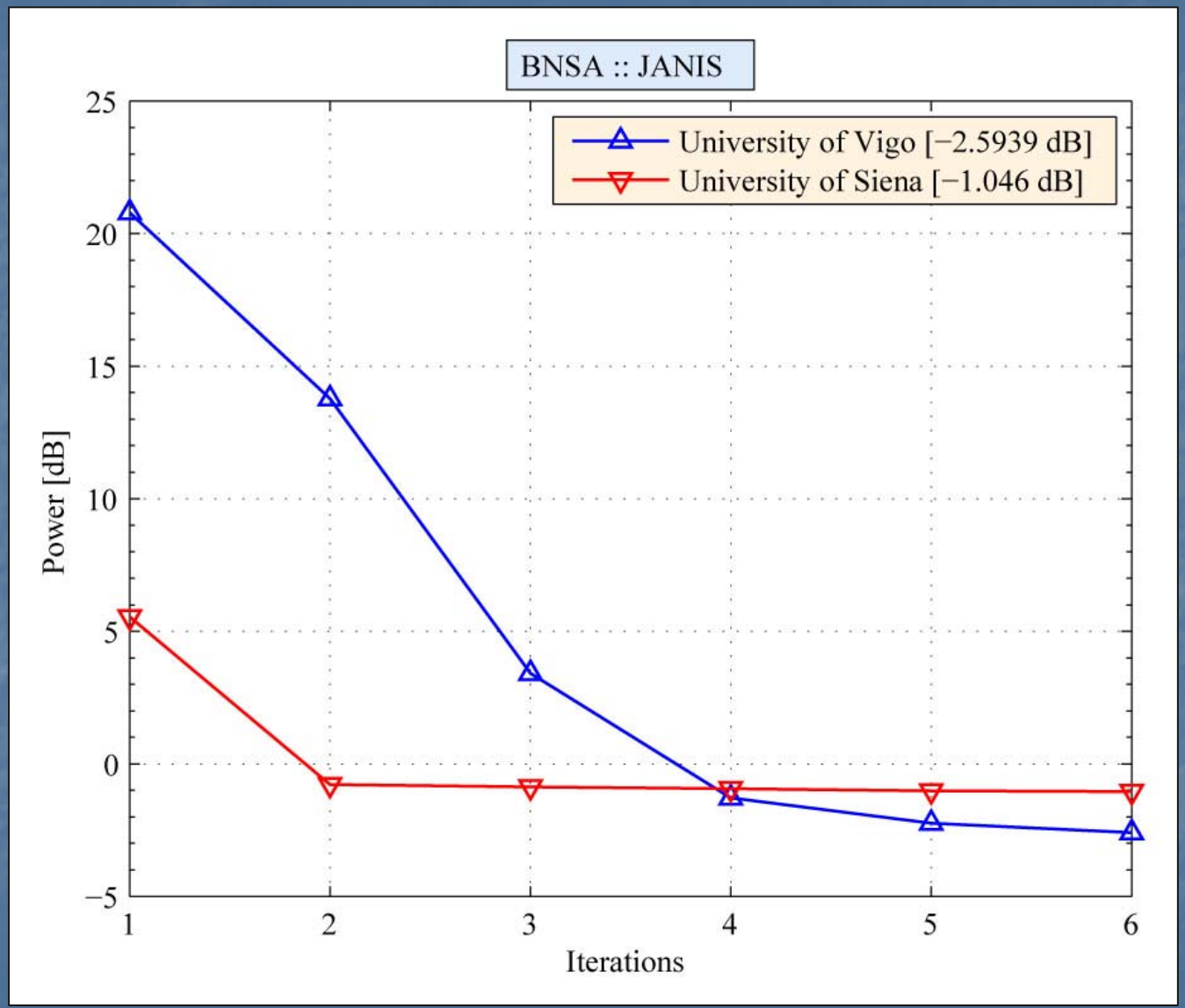
Reproduced results (1)



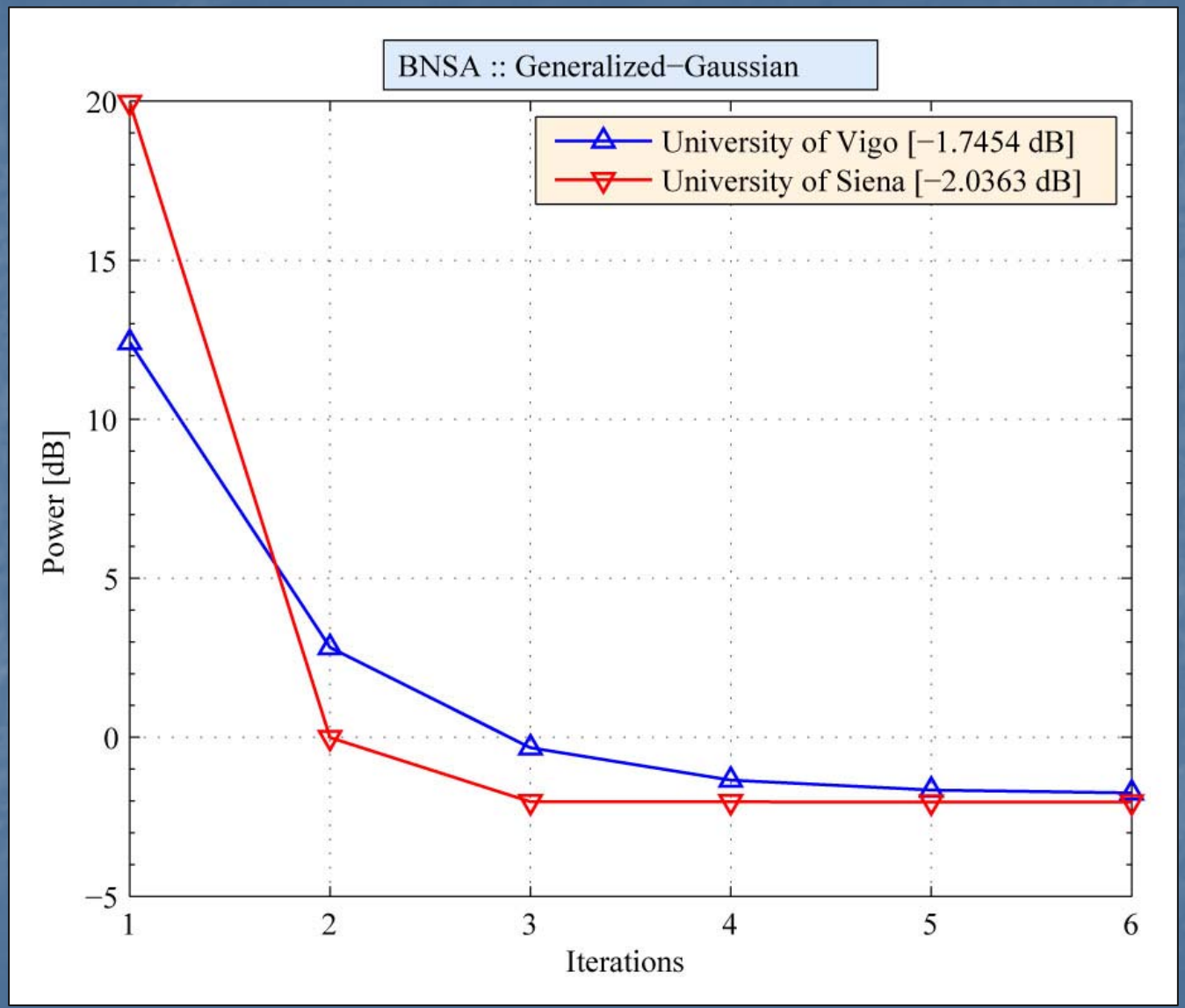
Reproduced results (2)



Reproduced results (3)



Reproduced results (4)



Conclusions

- RSP is extremely **insightful**:
  - We **both** gained a greater deal of knowledge about BNSA than an occasional reader
- RSP relies on **previous RSP**:
  - Ambiguities of involved papers are carried over future uses → more general consistence is needed
- RSP is **tough**:
  - The whole experience was harder than expected → experimental-research groups should be encouraged