Estimation below the detection limit

Tamir Bendory

March 20, 2018

Abstract

Here comes the abstract

1 Introduction

In this paper, we consider the problem of estimating a set of signals $x_1, \ldots, x_K$ from their multiple occurrences in unknown, random, locations in a data sequence y. The data may also contain background information – independent of the signals – which is modeled as noise. For one-dimensional signals, the data can be thought of as a long time series and the signals as repetitive short events. For two-dimensional signals, y presents a big image, containing many smaller images. The problem is then to estimate the signals $x_1, \ldots x_K$ from y. This model appears, in different noise levels, in many applications, including spike sorting [22], passive radar [17] and system identification [27]. In Section 2 we provide a precise mathematical formulation of the model and the estimation problem.

If the noise level is negligible, estimating the signals is easy. In this scenario, standard detection and clustering algorithms can produce multiple copies of each signal that can be then averaged. Even in higher noise level regimes, clever methods based on template matching, such as those used in structural biology [20] and radar [17], may work. [Do we want to add another 1D example to demonstare the problem, similarly to Figure 1.1 in the bispectrum paper?] However, in the low signal–to–noise (SNR) regime, detection of individual signal occurrences is impossible as explained in Section 2. Figure 1 illustrates the problem in different noise levels and one underlying signal ($K = 1$). Figure 1b shows a 21×21 image, which is a downsampled version of a projection of TKTK, taken from ASPIRE package [1] [The image is taken from the example folder]. Figure 1a shows a excerpt of a big image (the data image) that contains many repetitions of the projection. In Figures 1c and 1e, the same excerpt is shown with the addition of i.i.d. Gaussian noise with standard deviations of $\sigma = 0.2$ and $\sigma = 1$, respectively. Figures 1d and 1f show estimates of the projection from noisy data with $\sigma = 1$. These examples demonstrate that our method can work even if the data may seem as a pure noise. In Section 4 we provide the details of this experiment and show more corroborating experiments.

In this work we focus on the low SNR regime. In order to estimate the signal, we use autocorrelation analysis of the data. In a nutshell, the method consists of two stages. First, we estimate a mix of the low–order autocorrelation functions of the signals from the data. These quantities can be estimated, to any desired accuracy, if the signals appear enough times in the measurement, without the need to detect individual occurrences. Then, the signals are

estimated from the mixed autocorrelations using a non-convex least-squares. In Section 3, we elaborate on the technique and prove some of its properties. Interestingly, expectation-maximization (EM) – a popular framework for similar estimation problems, such as Gaussian mixture models and multireference alignment – is intractable for this problem. Even if the number of signal occurrence M is known and $K = 1$, at each iteration EM needs to assign probabilities to each possible combination of M copies of the current signal estimation in the measurement.

This work is primely motivated by cryo-electron microscopy (cryo–EM), which is an innovative single particle reconstruction technology. The acquired data in a cryo-EM experiment is contaminated with high noise levels. Therefore, any molecule reconstruction algorithm must take the challenging SNR level into account. In the last part of this manuscript, we draw connections with the estimation problem under consideration and the cryo–EM problem.

2 Model

Let $x_1, \ldots, x_K \in \mathbb{R}^L$ be the sought signals and let $y \in \mathbb{R}^N$ be the data. For each x_i, we associate a binary signal $s_i \in \{0,1\}^N$, referred to as the *support signal* and let $s = \sum_{i=1}^K s_i$. The nonzero values of s_i indicates the locations of x_i in y. If $s_i[n] = 1$, then $y[n+j] = x_i[n+j] + \varepsilon[n+j]$ for $j = 0, \ldots, L-1$. We denote the cardinality of s_i by M_i and $M = \sum_{i=1}^K M_i$. Neither the M_i's nor M is assumed to be known.

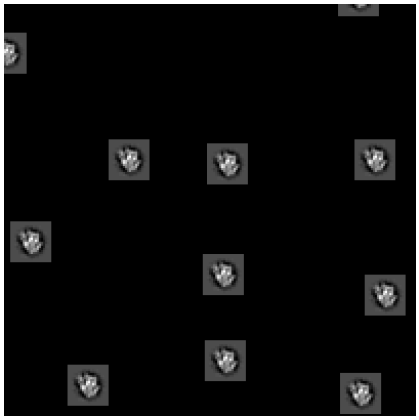
The support signals are generated by the following generative model. The signal s is initialized with zeros. First, an index i_1 is drawn uniformly from $\{1, \ldots, N\}$ and we set $s[i_1] = 1$. A second index i_2 is then drawn uniformly from $\{1, \ldots, N\}$. If $|i_2 - i_1| \geq L$, then we set $s[i_2] = 1$, otherwise we keep $s[i_2] = 0$ and draw a new index from uniform distribution. We then proceed adding nonzero entries to s, while keeping L entries separation until some halting criterion is obtained. We note that if the support is sparse enough, this generative model can be approximated by a simple Bernoulli process which takes the values of one and zero with probabilities M/N and $1 - M/N$, respectively. Once s is determined, each one of its nonzero entries is associated with one of the s_i's. In particular, for each $s[k] \neq 0$ we set $s_i[k] = 1$ and $s_j[k] = 0$ for $i \neq j$, where i is drawn form an unknown probability over $\{1, \ldots, K\}$.

The simplest way to present the forward model is a mix of blind deconvolution problems between the support signals and the target signals

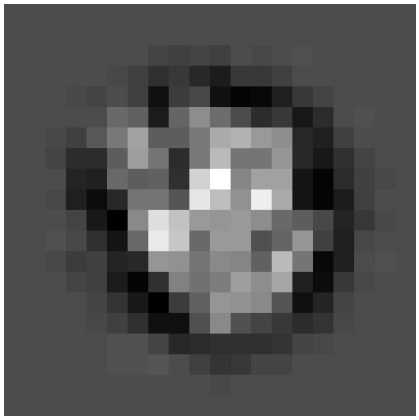
$$y = \sum_{i=1}^{K} x_i * s_i + \varepsilon, \quad \varepsilon \sim \mathcal{N}(0, \sigma^2 I). \tag{2.1}$$

We model the background information as i.i.d. Gaussian noise with zero mean and σ^2 variance. The goal is to estimate $x_1, \ldots, x_K$ from y.

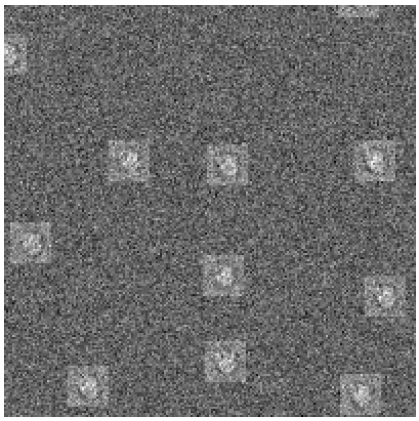
Blind deconvolution is a longstanding problem, arising in a variety of engineering and scientific applications, such as astronomy, communication, image deblurring, system identification and optics; see [21, 28, 5, 2], just to name a few. Clearly, the problem is ill-posed without additional information. In our case, the prior information is that s is a binary, sparse, signal. Other settings of blind deconvolution problems have been analyzed recently under different settings, see for instance [4, 24, 23, 25, 26, 14] where the focus is on high SNR regimes.



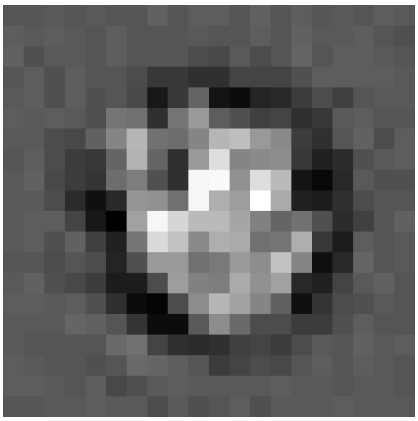
(a)



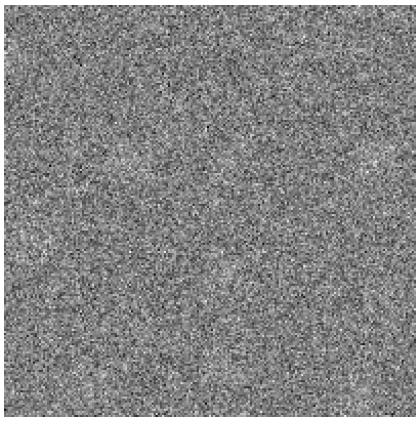
(b)



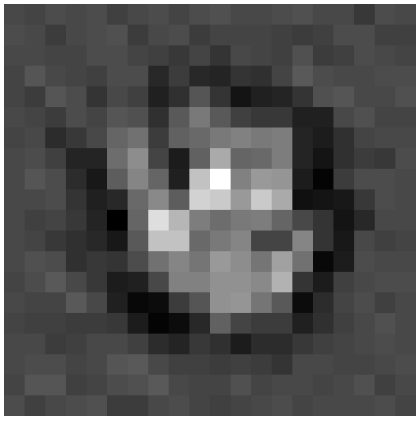
(c)



(d)



(e)



(f)

Figure 1: Figure (a) shows an excerpt of 2D data with multiple signal occurrences and no noise. Each small image is the 21×21 image shown in Figure (b). Figures (c) and (e) show the same data, now contaminated with i.i.d. Gaussian noise with $\sigma = 0.2$ and $\sigma = 1$, respectively. Figures (d) and (f) show estimates of the image (b) from data with noise level $\sigma = 1$ (as in Figure (e)). The signal appeared $M = 561 \times 10^6$ and $M = 110 \times 10^6$ times and the normalized recovery error is 0.078 and 0.135, respectively[3]

An important feature of the problem under consideration is that while both x_i's and s_i's are unknown, the goal is merely to estimate the x_i's. The s_i's are referred to as *nuisance variables*. Indeed, in many blind deconvolution applications the goal is merely to estimate one of the unknown signals. For instance, in image deblurring, both the blurring kernel and the high-resolution image are unknown, but the prime goal is only to sharpen the image. If x is known and $K = 1$, then s can be estimated by linear programming in the high SNR regime [15, 16, 11, 8, 12]. However, in the low SNR regime, estimating s is impossible. To see that, suppose that an oracle provides us M windows of length $W > L$, each contains one copy of x. Put it differently, we get a series of windows, each one contains a signal at unknown location. Estimating the first entry of the signal within each window is an easier problem than detecting the support of s. However, even this problem – called alignment or synchronization – is impossible in the low SNR regime. For instance, the variance of any estimator is, at best, proportional to σ^2 and independent of the number of windows, even if x is known [3]. Therefore, we conclude that that detecting the nonzero values of s is impossible in low SNR. In the next section we show that if M is large enough, then estimating the signals is possible, in any SNR level and to any accuracy, although we cannot detect their occurrences in y.

3 Autocorrelation analysis

Our method for estimating the signals relies on two pillars. First, we use the autocorrelation functions of the data to estimate a mix (i.e., linear combination) of the K signals autocorrelations. The mixed autocorrelation can be estimated to any accuracy, in any SNR level, if M is large enough and the separation condition on the support is held. Then, we use least-squares (LS) estimator to estimate the signals from their mixed autocorrelation. From pedagogical reasons, we start with the second stage of recovering signals from their autocorrelations. In this section we mainly discuss the uniqueness of the mapping from the autocorrelation to the signals. Concrete algorithms will be discussed in the next section.

For the purpose of this paper, we need the first three (aperiodic) autocorrelation functions of a signal $z \in \mathbb{R}^W$, defined as

$$\begin{aligned} a_z^1 &= \sum_{i=0}^{W-1} z[i], \\ a_z^2[\ell] &= \sum_{i=0}^{W-1-\ell} z[i]z[i+\ell], \\ a_z^3[\ell_1,\ell_2] &= \sum_{i=0}^{W-1-\max\{\ell_1,\ell_2\}} z[i]z[i+\ell_1]z[i+\ell_2]. \end{aligned} \tag{3.1}$$

Note that the autocorrelation functions are symmetric so that $a_z^2[\ell] = a_z^2[-\ell]$ and $a_z^3[\ell_1,\ell_2] = a_z^3[-\ell_1,-\ell_2]$.

A one-dimensional signal is determined uniquely by its third-order auto-correlation:

Proposition 3.1. *Suppose that $z[0]$ and $z[L-1]$ are non-zeros. Then, a signal $z \in \mathbb{R}^W$ is determined uniquely from a_z^2 and a_z^3.*

Proof. From the second-order autocorrelation, we ge

$$a_z^2[L-1] = z[0]z[L-1] \neq 0.$$

Then, from the third-order autocorrelation we can compute $z[k]$ for all $k = 0, \dots L-1$ by

$$a_z^3[k, L-1] = z[0]z[k]z[L-1]. \tag{3.2}$$

□

We note that the length of the signal can be easily derived from the second-order autocorrelation of the signal. Therefore, the assumption that $z[0]$ and $z[L-1]$ is met in practice. We also note that for one-dimensional signals, the second-order autocorrelation does not determined the signals uniquely [7, 9]. This is not the case for dimensions greater than one, in which almost all signals are determined uniquely from their aperiodic autocorrelations, up to sign (phase in the complex case) and reflection through the origin (with conjugation in the complex case) [18, 19, 9]. The sign ambiguity can be resolved by the mean of the signal if it is not zero. However, in order to determine the reflection symmetry (Z_2 symmetry), one needs to use the third moment.

The heterogeneous case $K > 1$ was explored for periodic autocorrelation functions. The aperiodic autocorrelations are the periodic autocorrelations of signals padded by zeros. Therefore, the following results hold for our setup as well [This part is wrong – Email correspondence with Alex]. In [6], it was shown that a mix of K third-order autocorrelations determine a finite list of K generic signals when

- $K = 2$ when $L > 1$,
- $K = 3$ when $L > 12$,
- $K = 4$ when $L > 18$,
- $5 \leq K \leq 15$ when $L \geq 6K - 5$.

The authors conjecture that for $K > 15$, $L \geq 6K - 5$ is enough. Recently, Joe told use that he has proven that there is unique mapping in the same regime. This also holds for arbitrary weights γ_i which are rational fractions.

[Where we should refer to Gianakis's paper?]

We are moving forward to discuss the second question of how to estimate the autocorrelation of the signals from the data. The analysis is conducted in the asymptomatic regime where $M_1, \dots, M_K, N \to \infty$. We define the ratios

$$\gamma_i = \frac{M_i L}{N}, \tag{3.3}$$

and $\gamma = \sum_{i=1}^K \gamma_i$. Under the separation condition, we have $\gamma \leq \frac{L}{2L-1} \approx 1/2$. The main insight is that if s satisfies the separation condition, then the first L entries of the data

autocorrelations converge to a γ scaled version of a mix of the signals autocorrelations:

$$\lim_{N\to\infty} a_y^1 = \sum_{i=1}^{K} \gamma_i a_{x_i}^1, \tag{3.4}$$

$$\lim_{N\to\infty} a_y^2[\ell] = \sum_{i=1}^{K} \gamma_i a_{x_i}^2[\ell] + \sigma^2\delta[\ell], \tag{3.5}$$

$$\lim_{N\to\infty} a_y^3[\ell_1,\ell_2] = \sum_{i=1}^{K} \gamma_i a_{x_i}^3[\ell_1,\ell_2] + \sigma^2\left(\sum_{i=1}^{K}\gamma_i a_{x_i}^1\right)(\delta[\ell_1,0]+\delta[0,\ell_2]+\delta[\ell_1,\ell_2]), \tag{3.6}$$

for $\ell,\ell_1,\ell_2 = 0,\dots L-1$. These relations are proved in Appendix A. The analysis is similar to [10, 13], yet a special caution should be taken with the noise dependencies. This means that given $M_1,\dots,M_K$ and σ^2 and K does not exceed the limit for uniqueness, the one can estimate the signals from the third-order autocorrelation of the data. In other words, the signals can be estimated in asymptotic estimation rate of σ^6/N.

If the noise level σ^2 is known, then for $K=1$, one can estimate M from only the first two moments, namely, with estimation rate of σ^4/N.

Proposition 3.2. *Let $K=1$. Then,*

$$\frac{M}{N} = \frac{(a_y^1)^2}{\sum_{j=0}^{L-1} a_y^2[j] - \sigma^2}.$$

Proof. The relation is proved by plugging the definitions of the signal autocorrelations into the right-hand side of the equation (3.1). □

Proposition 3.3. *It is possible to estimate M and σ from the third moment.*

Proof. See Appendix B. □

If we assume that s is sparse, then by ignoring the separation condition, one can describe the generative process of s as a Bernoulli process with parameter M/N. Therefore, in low SNRone can estimate the parameter that control this statistical process, although cannot estimate individual entries.

Estimating σ and M?

4 Numerical experiments

4.1 One-dimensional experiments

4.2 Two-dimensional experiments

Solving RRR, and then 200 LS iteration on window of size W and 500 iterations on window of size L.

5 Conclusion

Here we conclude the paper: cryo – EM, structured background, without separation, heterogeneity In particular, in cryo–EM, multiple projections of a molecule (signal), taken from unknown viewing directions, are recorded on two-dimensional detector array. Current algorithms try to detect these projections in a low SNR regime and then use them for the reconstruction process. Since the Then, the reconstruction problem is to detect these projection, and then use them to estimat The data acquired in both technologies is composed of multiple projections of a molecule (the signal), taken from unknown viewing direction, and drawn in high noise level. The reconstitution problem is then to estimate the molecule from this data.

A word on the sample complexity

References

[1] `http://spr.math.princeton.edu`.

[2] Karim Abed-Meraim, Wanzhi Qiu, and Yingbo Hua. Blind system identification. *Proceedings of the IEEE*, 85(8):1310–1322, 1997.

[3] Cecilia Aguerrebere, Mauricio Delbracio, Alberto Bartesaghi, and Guillermo Sapiro. Fundamental limits in multi-image alignment. *IEEE Transactions on Signal Processing*, 64(21):5707–5722, 2016.

[4] Ali Ahmed, Benjamin Recht, and Justin Romberg. Blind deconvolution using convex programming. *IEEE Transactions on Information Theory*, 60(3):1711–1732, 2014.

[5] GR Ayers and J Christopher Dainty. Iterative blind deconvolution method and its applications. *Optics letters*, 13(7):547–549, 1988.

[6] Afonso S Bandeira, Ben Blum-Smith, Amelia Perry, Jonathan Weed, and Alexander S Wein. Estimation under group actions: recovering orbits from invariants. *arXiv preprint arXiv:1712.10163*, 2017.

[7] Robert Beinert and Gerlind Plonka. Ambiguities in one-dimensional discrete phase retrieval from fourier magnitudes. *Journal of Fourier Analysis and Applications*, 21(6):1169–1198, 2015.

[8] Tamir Bendory. Robust recovery of positive stream of pulses. *IEEE Transactions on Signal Processing*, 65(8):2114–2122, 2017.

[9] Tamir Bendory, Robert Beinert, and Yonina C Eldar. Fourier phase retrieval: Uniqueness and algorithms. In *Compressed Sensing and its Applications*, pages 55–91. Springer, 2017.

[10] Tamir Bendory, Nicolas Boumal, Chao Ma, Zhizhen Zhao, and Amit Singer. Bispectrum inversion with application to multireference alignment. *arXiv preprint arXiv:1705.00641*, 2017.

[11] Tamir Bendory, Shai Dekel, and Arie Feuer. Robust recovery of stream of pulses using convex optimization. *Journal of Mathematical Analysis and Applications*, 442(2):511–536, 2016.

[12] Brett Bernstein and Carlos Fernandez-Granda. Deconvolution of point sources: A sampling theorem and robustness guarantees. *arXiv preprint arXiv:1707.00808*, 2017.

[13] Nicolas Boumal, Tamir Bendory, Roy R Lederman, and Amit Singer. Heterogeneous multireference alignment: a single pass approach. *arXiv preprint arXiv:1710.02590*, 2017.

[14] Yuejie Chi. Guaranteed blind sparse spikes deconvolution via lifting and convex optimization. *IEEE Journal of Selected Topics in Signal Processing*, 10(4):782–794, 2016.

[15] Yohann De Castro and Fabrice Gamboa. Exact reconstruction using beurling minimal extrapolation. *Journal of Mathematical Analysis and applications*, 395(1):336–354, 2012.

[16] Vincent Duval and Gabriel Peyré. Exact support recovery for sparse spikes deconvolution. *Foundations of Computational Mathematics*, 15(5):1315–1355, 2015.

[17] Sandeep Gogineni, Pawan Setlur, Muralidhar Rangaswamy, and Raj Rao Nadakuditi. Passive radar detection with noisy reference channel using principal subspace similarity. *IEEE Transactions on Aerospace and Electronic Systems*, 2017.

[18] MHMH Hayes. The reconstruction of a multidimensional sequence from the phase or magnitude of its fourier transform. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 30(2):140–154, 1982.

[19] Monson H Hayes and James H McClellan. Reducible polynomials in more than one variable. *Proceedings of the IEEE*, 70(2):197–198, 1982.

[20] Ayelet Heimowitz, Amit Singer, et al. Apple picker: Automatic particle picking, a low-effort cryo-em framework. *arXiv preprint arXiv:1802.00469*, 2018.

[21] Stuart M Jefferies and Julian C Christou. Restoration of astronomical images by iterative blind deconvolution. *The Astrophysical Journal*, 415:862, 1993.

[22] Michael S Lewicki. A review of methods for spike sorting: the detection and classification of neural action potentials. *Network: Computation in Neural Systems*, 9(4):R53–R78, 1998.

[23] Xiaodong Li, Shuyang Ling, Thomas Strohmer, and Ke Wei. Rapid, robust, and reliable blind deconvolution via nonconvex optimization. *arXiv preprint arXiv:1606.04933*, 2016.

[24] Yanjun Li, Kiryung Lee, and Yoram Bresler. Identifiability in blind deconvolution with subspace or sparsity constraints. *IEEE Transactions on Information Theory*, 62(7):4266–4275, 2016.

[25] Shuyang Ling and Thomas Strohmer. Self-calibration and biconvex compressive sensing. *Inverse Problems*, 31(11):115002, 2015.

[26] Shuyang Ling and Thomas Strohmer. Blind deconvolution meets blind demixing: Algorithms and performance bounds. *IEEE Transactions on Information Theory*, 2017.

[27] Lennart Ljung. System identification. In *Signal analysis and prediction*, pages 163–173. Springer, 1998.

[28] Ofir Shalvi and Ehud Weinstein. New criteria for blind deconvolution of nonminimum phase systems (channels). *IEEE Transactions on information theory*, 36(2):312–321, 1990.

A Autocorrelation estimations

To analyze the asymptotic behavior of the data autocorrelation functions, we consider one signal $K = 1$. The extension to $K > 1$ is straightforward by averaging the contributions of all signal with the appropriates weights, see [13].

Let us define

$$\gamma = \lim_{N\to\infty} \frac{M_N L}{N} < 1. \tag{A.1}$$

By assuming $M_N = \Omega(N)$, we also have $\gamma > 0$. We start by considering the first autocorrelation of the data

$$a_y^1 = \sum_{i=0}^{N-1} y[i] = \frac{1}{N/L} \sum_{j=0}^{M_N-1} \frac{1}{L} \sum_{i=0}^{L-1} x[i] + \underbrace{\frac{1}{N} \sum_{i=0}^{N-1} \varepsilon[i]}_{\text{noise term}} \xrightarrow{a.s.} \gamma a_x^1, \tag{A.2}$$

where the noise term converges to zero almost surely (a.s.) by the law of large numbers.

We proceed with the second moment for fixed $\ell \in [0, \dots, L-1]$. Then, we can compute,

$$\begin{aligned} a_y^2[\ell] = \frac{1}{N} \sum_{i=0}^{N-1-\ell} & y[i]y[i+\ell] \\ & \underbrace{\frac{1}{N} \sum_{j=1}^{M_N} \sum_{i=0}^{L-\ell-1} x[i]x[i+\ell]}_{\text{signal term}} + \underbrace{\frac{1}{N} \sum_{i=0}^{N-1} \varepsilon[i]\varepsilon[i+\ell]}_{\text{noise term}}, \end{aligned} \tag{A.3}$$

where the cross terms between the signal and the noise almost surely vanish in the limit.

We treat the signal and noise terms separately. We first break the signal term into M_N different sums, each contains one copy of the signal, and get

$$\frac{1}{N} \sum_{j=1}^{M_N} \sum_{i=0}^{L-\ell-1} x[i]x[i+\ell] = \frac{M_N L}{N} \frac{1}{L} \sum_{i=0}^{L-\ell-1} x[i]x[i+\ell] = \gamma a_x^2[\ell]. \tag{A.4}$$

Similarly, for $\ell \neq 0$, we can break the noise term into a sum of independent terms

$$\frac{1}{N} \sum_{i=0}^{N-1-\ell} \varepsilon[i]\varepsilon[i+\ell] = \frac{1}{\ell} \sum_{i=0}^{\ell-1} \frac{1}{N/\ell} \sum_{j=0}^{N/\ell-1} \varepsilon[j\ell+i]\varepsilon[(j+1)\ell+i]. \tag{A.5}$$

Each term of $\frac{1}{N/\ell}\sum_{j=0}^{N/\ell-1}\varepsilon[j\ell+i]\varepsilon[(j+1)\ell+i]$ is an average of N/ℓ independent terms with expectation zero, and therefore converge to zero almost surely as $N\to\infty$. If $\ell=0$,

$$\frac{1}{N}\sum_{i=0}^{N-1}\varepsilon[i]^2 \xrightarrow{a.s.} \sigma^2. \tag{A.6}$$

We are now moving to the third-order autocorrelation. Let us fix $\ell_1\geq\ell_2$ and recall that

$$a_y^3[\ell_1,\ell_2]=\sum_{i=0}^{N-1-\ell_1} y[i]y[i+\ell_1]y[i+\ell_2].$$

Writing explicitly in terms of signal and noise, this sum can be broken into eight partial sums. The first contains only signal terms and converges to γa_x^3 from the same reasons as (A.4). Three other partial sums contain the product of two signal entries and one noise term. Since the noise is independent of the signal, then these terms go to zero almost surely.

We next analyze the contribution of triple product of noise terms. For $\ell_1\neq 0$, this sum can be formulate as follows:

$$\sum_{i=0}^{N-1-\ell_1}\varepsilon[i]\varepsilon[i+\ell_1]\varepsilon[i+\ell_2]=\frac{1}{\ell_1}\sum_{i=0}^{\ell_1-1}\frac{1}{N/\ell_1}\sum_{j=0}^{N/\ell_1-1}\varepsilon[j\ell_1+i]\varepsilon[(j+1)\ell_1+i]\varepsilon[j\ell_1+i+\ell_2].$$

For each fixed i, we sum of over N/ℓ_1 independent variables that goes to zero almost surely. For $\ell_1=\ell_2=0$, we get a some of N independent variables, each is a triple product of Gaussian variables with zero mean. Therefore, it is also converges to zero.

To complete the analysis, we consider the three terms composed of the product of two noise terms and one signal entry. Most of these terms converges to zero almost surely because of interdependency between the noise entries. For $\ell_1=0,\ell_2=0$ and $\ell_1=\ell_2$, a simple computation shows that the sum converges to $\gamma\sigma^2 a_x^1$.

B Proof of Proposition 3.3

We aim to prove that one can estimate both σ and M from the observed third moment. We will construct two independent quadratic equations of M which do not depend on σ. This will let us estimate M. Given M, we will estimate σ.

To ease notation, let $\beta=M/N$. Recall that $a_y^1=\beta(\mathbf{1}^T x)$ and and $a_y^2[0]=\beta(\|x\|^2+\sigma^2)$, where $\mathbf{1}\in\mathbb{R}^L$ stands for vector of ones. Taking the product:

$$\begin{aligned} E_1 &:= (\beta(\mathbf{1}^T x))(\beta(\|x\|^2+\sigma^2)) \\ &= \sigma^2 a_y^1+\beta^2\tau, \end{aligned} \tag{B.1}$$

where $\tau := L\left(\sum_{j=1}^{L-1}(a_x^3[j,0]+a_x^3[0,j])+\sum_{j=0}^{L-1}a_x^3[0,0]\right)$. Next, we can estimate from a_y^3

$$E_2 := \beta\tau+3L\sigma^2 a_y^1. \tag{B.2}$$

Therefore, from (B.1) and (B.2) we get

$$E_2\beta-3L\sigma^2 a_y^1 = E_1-\sigma^2 a_y^1. \tag{B.3}$$

Now, recalling from Proposition 3.2

$$\sigma^2 = a_y^2 - (a_y^1)^2/\beta, \tag{B.4}$$

where we use $a_y^2 := \sum_{j=0}^{L-1} a_y^2[j]$. Rearranging the equations, we then get the quadratic equation

$$\mathcal{A}\beta^2 + \mathcal{B}\beta + \mathcal{C} = 0, \tag{B.5}$$

where

$$\begin{aligned}
\mathcal{A} &= E_2, \\
\mathcal{B} &= -(E_1 + (3L-1)a_y^1 a_y^2), \\
\mathcal{C} &= (3L-1)(a_y^1)^3.
\end{aligned}$$

We are now proceeding to derive the second quadratic equation. We notice that

$$E_3 = (a_y^1)^3 = \beta^3 \upsilon, \tag{B.6}$$

where [to check]

$$\upsilon = a_x^3[0,0] + 3\sum_{i=1}^{L-1} a_x^3[i,i] + 3\sum_{i=1}^{L-1}(a_x^3[i,0] + a_x^3[0,i]) + 6\sum_{1\le i\le j\le L-1} a_x^3[i,j].$$

On the other hand, from a_y^3 we can directly estimate

$$E_4 = \beta\upsilon + 9L\sigma^2 a_x^1. \tag{B.7}$$

Now, by multiplying both sides by β^2 and using (B.6), we get

$$\beta^2 E_4 = E_3 + 9L\sigma^2 a_x^1. \tag{B.8}$$

Plugging (B.4) and rearranging the equation, we get a second quadratic equation independent of σ:

$$\mathcal{D}\beta^2 + \mathcal{E}\beta + \mathcal{F} = 0, \tag{B.9}$$

where

$$\begin{aligned}
\mathcal{D} &= E_4 - 9La_x^1 a_y^2, \\
\mathcal{E} &= 9La_x^1 (a_y^1)^2, \\
\mathcal{F} &= -(a_y^1)^3.
\end{aligned}$$

To complete the proof, we need to show that the two quadratic equations (B.5) and (B.9) are independent. To this end, it is enough to show that the ratio between the coefficients is not the same. using (B.1), we have

$$\frac{\mathcal{B}}{\mathcal{C}} = \frac{-(E_1 + (3L-1)a_y^1 a_y^2)}{(3L-1)(a_y^1)^3} = -\frac{a_y^2[0]}{(3L-1)(a_y^1)^2} - \frac{a_y^2}{(a_y^1)^2}.$$

In addition,

$$\frac{\mathcal{E}}{\mathcal{F}} = -\frac{9La_x^1}{a_y^1}.$$

Now, suppose that the quadratics are dependent. Then, $\frac{\mathcal{B}}{\mathcal{C}} = \frac{\mathcal{E}}{\mathcal{F}}$, or,

$$\frac{a_y^2[0]}{(3L-1)(a_y^1)^2} + \frac{a_y^2}{(a_y^1)^2} = \frac{9La_x^1}{a_y^1}.$$

Rearranging the equation, we get

$$a_y^2[0] + (3L-1)(a_y^1)^2 - 9La_x^1 a_y^1 = 0.$$

For generic x, this polynomial equation is not satisfied. Therefore, the equations are independent.