

Novel Techniques for Signal Analysis and Processing

Stephen D. Casey

American University
Washington, DC USA
scasey@american.edu
2021 Annual EM Portfolio Review
AFOSR Grant Number FA9550-20-1-0030

January 6, 2021



- *Secure and Accurate Wireless Communication: Time-Frequency Analysis* – develops a new architecture for time-frequency analysis. This method, the Projection Method, gives a more computationally efficient way to sample, transmit, and then reconstruct adaptive frequency band (AFB) and ultra wideband (UWB) signals. (Two U.S. Patents, 9 papers.)



- *Secure and Accurate Wireless Communication: Time-Frequency Analysis* – develops a new architecture for time-frequency analysis. This method, the Projection Method, gives a more computationally efficient way to sample, transmit, and then reconstruct adaptive frequency band (AFB) and ultra wideband (UWB) signals. (Two U.S. Patents, 9 papers.)
- *Efficient Network Analysis: Network Tomography* – demonstrates a way to create a system that will efficiently monitor traffic in hyperbolic network, e.g., the internet, working simply on the geometry or structure of the network itself. Our analysis looks at weighted graphs and how the weights change due to an increase in traffic. (Four papers.)

- *Secure and Accurate Wireless Communication: Time-Frequency Analysis* – develops a new architecture for time-frequency analysis. This method, the Projection Method, gives a more computationally efficient way to sample, transmit, and then reconstruct adaptive frequency band (AFB) and ultra wideband (UWB) signals. (Two U.S. Patents, 9 papers.)
- *Efficient Network Analysis: Network Tomography* – demonstrates a way to create a system that will efficiently monitor traffic in hyperbolic network, e.g., the internet, working simply on the geometry or structure of the network itself. Our analysis looks at weighted graphs and how the weights change due to an increase in traffic. (Four papers.)
- *FHSS Signal Analysis: Analysis of Point Processes* – (12 papers, two U.S. Patent applications.) Focus of this talk.

- *Secure and Accurate Wireless Communication: Time-Frequency Analysis* – develops a new architecture for time-frequency analysis. This method, the Projection Method, gives a more computationally efficient way to sample, transmit, and then reconstruct adaptive frequency band (AFB) and ultra wideband (UWB) signals. (Two U.S. Patents, 9 papers.)
- *Efficient Network Analysis: Network Tomography* – demonstrates a way to create a system that will efficiently monitor traffic in hyperbolic network, e.g., the internet, working simply on the geometry or structure of the network itself. Our analysis looks at weighted graphs and how the weights change due to an increase in traffic. (Four papers.)
- *FHSS Signal Analysis: Analysis of Point Processes* – (12 papers, two U.S. Patent applications.) Focus of this talk.
- Appendix A – Zeta Function ; Appendix B – Equidistribution ; Appendix C – FHSS.



Periodic Point Processes

- Radar or Sonar.
- Bit synchronization in communications.
- Unreliable measurements in a fading communications channel.
- **FHSS** – Compute the “jump times” of a pseudorandomly occurring change in the carrier frequency of “frequency hopping” radios, where the change rate is governed by shift register outputs. In this case it is desired to find the underlying fundamental periods τ_k .
- Assumption – noisy signal data is set of **event times, namely “Time of Arrival” (TOA's)** $s(t) + \eta(t)$ with gaps in the data.
- Questions – $s(t)$ periodic? period $\tau = ?$ Are there multiple periods $\tau_k = ?$ If so, what are they? How do we deinterleave the signals?
- **Solutions – Two Algorithms –**
MEA – Extremely efficient and stable analysis of one-period data.
EQUIMEA – Extremely efficient and stable analysis of multi-period data, including extraction of the fundamental period of the generators and deinterleaving the processes.



The **MEA (Modified Euclidean Algorithm)** algorithm works on data from single period processes, computing an estimate of the underlying period. It is extremely computationally efficient and straightforward, consisting of a sequence of subtractions, sorts, and eliminations/replacements.

- Extremely computationally efficient and straightforward, consisting of a sequence of subtractions, sorts, and eliminations/replacements.
- It works on **all** single period processes, but in particular on sparse data sets where others break down.
- In particular, it is the only algorithm that is proven to extract the fundamental hop period from sparse and noisy FHSS data, e.g., 90% missing, 10% jitter noise.
- Its justification, however, rests on some deep mathematics, including a probabilistic interpretation of the Riemann zeta function.

The **EQUIMEA (Equidistributed Modified Euclidean Algorithm)** algorithm works on data from multiple period processes. It extracts the fundamental underlying periods of the data and then deinterleaves the processes. It uses the MEA as an engine, reinforcing the data from any one of the given generators by iteration.

- First, the MEA reinforces the data from any one of the given generators by iteration.
- It then uses spectral analysis to extract the periods and match filtering to deinterleave.
- It also works on **all** multiple period processes, but in particular on sparse data sets where others break down.
- In particular, it is the only algorithm that is proven to extract the fundamental hop periods from sparse and noisy FHSS data, e.g., 90% missing, 10% jitter noise.
- Its justification also rests on some deep mathematics, including the probabilistic interpretation of the Riemann zeta function, a measure theoretic Weyl's equidistribution theorem, and Wiener's periodogram.

Mathematical Underpinnings

Finite set of real numbers

$$S = \{s_j\}_{j=1}^n, \text{ with } s_j = k_j\tau + \varphi + \eta_j,$$

where

- τ (the period) is a fixed positive real number to be determined
- k_j 's are non-repeating positive integers (natural numbers)
- φ (the phase) is a real random variable uniformly distributed over the interval $[0, \tau)$
- η_j 's (the noise) are zero-mean independent identically distributed (iid) error terms. We assume that the η_j 's have a symmetric probability density function (pdf), and that

$$|\eta_j| \leq \eta_0 \leq \frac{\tau}{2} \text{ for all } j,$$

where η_0 is an *a priori* noise bound.



Approaches to the Analysis

- The data can be thought of as a set of event times of a periodic process, which generates a zero-one time series or delta train with additive jitter noise $\eta(t)$ –

$$s(t) = \sum_{j=1}^n \delta(t - ((k_j\tau + \varphi) + \eta(t))).$$

- Another model – Let $f(t) = \sin(\frac{\pi}{\tau}(t - \varphi))$ and $S = \{\text{occurrence time of noisy zero-crossings of } f \text{ with missing observations}\}$.
- The k_j 's determine the best procedure for analyzing this data.
- Given a sequence of consecutive k_j 's, use least squares.
- Fourier analytic methods, e.g., Wiener's periodogram, work with some missing observations, but when the percentage of missing observations is too large ($> 50\%$), they break down.
- Number theoretic methods can work with very sparse data sets ($> 90\%$ missing observations). Trade-off – low noise – number theory vs. higher noise – combine Fourier with number theory.



The Modified Euclidean Algorithm (MEA)

$$S = \{s_j\}_{j=1}^n, \text{ with } s_j = k_j\tau + \varphi + \eta_j$$

Let $\hat{\tau}$ denote the value the algorithm gives for τ , and let “ \leftarrow ” denote *replacement*.

Initialize: Sort the elements of S in descending order. Set $\text{iter} = 0$.

- 1.) [Adjoin 0 after first iteration.] If $\text{iter} > 0$, then $S \leftarrow S \cup \{0\}$.
- 2.) [Form the new set with elements $(s_j - s_{j+1})$.] Set $s_j \leftarrow (s_j - s_{j+1})$.
- 3.) [Sort.] Sort the elements in descending order.
- 4.) [Eliminate zero(s).] If $s_j = 0$, then $S \leftarrow S \setminus \{s_j\}$.
- 5.) The algorithm terminates if S has only one element s_1 . Declare $\hat{\tau} = s_1$. If not, $\text{iter} \leftarrow (\text{iter} + 1)$. Go to 1.)



Assume $\tau = 1$.

- Estimates and their standard deviations are based on averaging over 100 Monte-Carlo runs
- n = number of data points, $iter$ = average number of iterations required for convergence, and $\%miss$ = average number of missing observations
- Estimates of τ are labeled $\hat{\tau}$, and $std(\hat{\tau})$ is the experimental standard deviation
- Threshold value of $\eta_0 = 0.35\tau = 0.35$ was used

Simulation Results, Cont'd

1.) *Noise-free estimation.*

Results from simulating noise-free estimation of τ .

n	M	%miss	iter	τ	2τ	3τ	$> 3\tau$
10	10^1	81.69	3.3	100%	0	0	0
10	10^2	97.92	10.5	100	0	0	0
10	10^3	99.80	46.5	100	0	0	0
10	10^4	99.98	316.2	100	0	0	0
10	10^5	99.998	2638.7	100	0	0	0
4	10^2	97.84	15.2	82%	12	4	2
6	10^2	97.82	14.2	97	3	0	0
8	10^2	97.80	10.2	98	1	1	0
10	10^2	97.78	10.2	99	1	0	0
12	10^2	97.76	8.6	100	0	0	0
14	10^2	97.75	7.4	100	0	0	0

2.) *Uniformly distributed noise.*

Results from estimation of τ from noisy measurements.

n	M	Δ	%miss	iter	$\hat{\tau}$	$std(\hat{\tau})$
10	10^1	10^{-3}	81.37	4.35	0.9987	0.0005
10	10^2	10^{-3}	97.88	9.67	0.9980	0.0010
50	10^3	10^{-3}	99.80	16.0	0.9969	0.0028
10	10^1	10^{-2}	80.85	4.38	0.9888	0.0046
10	10^1	10^{-2}	81.94	4.45	0.9883	0.0051
10	10^1	10^{-1}	81.05	4.33	0.8857	0.0432

The Structure of Randomness over \mathbb{Z}

Why does the MEA work, and work as well as it does?

Theorem

Given n ($n \geq 2$) “randomly chosen” positive integers $\{k_1, \dots, k_n\}$,

$$P\{\gcd(k_1, \dots, k_n) = 1\} \rightarrow 1^- \text{ quickly! as } n \rightarrow \infty.$$

Let $\text{card}\{\cdot\}$ denote cardinality of the set $\{\cdot\}$, and let $\{1, \dots, \ell\}^n$ denote the sublattice of positive integers in \mathbb{R}^n with coordinates c such that $1 \leq c \leq \ell$. Therefore,

$N_n(\ell) = \text{card}\{(k_1, \dots, k_n) \in \{1, \dots, \ell\}^n : \gcd(k_1, \dots, k_n) = 1\}$ is the number of relatively prime elements in $\{1, \dots, \ell\}^n$.

Theorem (MEA Theorem (C))

Let $N_n(\ell) = \text{card}\{(k_1, \dots, k_n) \in \{1, \dots, \ell\}^n : \gcd(k_1, \dots, k_n) = 1\}$. For $n \geq 2$, we have that

$$\lim_{\ell \rightarrow \infty} \frac{N_n(\ell)}{\ell^n} = [\zeta(n)]^{-1}.$$



The Structure of Randomness over \mathbb{Z} , Cont'd

Theorem (C)

Let $\omega \in (1, \infty)$. Then $\lim_{\omega \rightarrow \infty} [\zeta(\omega)]^{-1} = 1$, converging to 1 from below faster than $1/(1 - 2^{1-\omega})$.

Lemma

$$\gcd(k_1\tau, \dots, k_n\tau) = \tau \gcd(k_1, \dots, k_n).$$

What if “integers are noisy?” Remainder terms could be noise, and thus could be non-zero numbers arbitrarily close to zero. Subsequent steps in the procedure may involve dividing by such numbers, which would result in arbitrarily large numbers. The standard algorithm is unstable under perturbation by noise.

Solution : Replace division with subtraction, and threshold/average/filter/transform to eliminate noise.



The Structure of Randomness over \mathbb{Z} , Cont'd

Lemma (The Key Lemma)

The MEA preserves the gcd, i.e.,

$$\gcd(k_1, \dots, k_n) = \gcd((k_1 - k_2), (k_2 - k_3), \dots, (k_{n-1} - k_n), k_n).$$

Combining the MEA Theorem with the Theorems and Lemmas above gives the theoretical underpinnings of the Modified Euclidean Algorithm. Moreover, the estimate

$$(1 - 2^{1-\omega})^{-1} \leq [\zeta(\omega)]^{-1} \leq 1$$

shows that the algorithm very likely produces this value in the noise-free case or with minimal noise with as few as 10 data elements.



Theorem

Let $\omega \in (1, \infty)$. Then $\lim_{\omega \rightarrow \infty} [\zeta(\omega)]^{-1} = 1$, converging to 1 from below faster than $1/(1 - 2^{1-\omega})$.

Proof : Since $\zeta(\omega) = \sum_{n=1}^{\infty} n^{-\omega}$ and $\omega > 1$,

$$\begin{aligned} 1 &\leq \zeta(\omega) = 1 + \frac{1}{2^\omega} + \frac{1}{3^\omega} + \frac{1}{4^\omega} + \frac{1}{5^\omega} + \cdots \\ &\leq 1 + \frac{1}{2^\omega} + \frac{1}{2^\omega} + \underbrace{\frac{1}{4^\omega} + \cdots + \frac{1}{4^\omega}}_{4\text{-times}} + \underbrace{\frac{1}{8^\omega} + \cdots + \frac{1}{8^\omega}}_{8\text{-times}} + \cdots \\ &= \sum_{k=0}^{\infty} \left(\frac{2}{2^\omega} \right)^k = \frac{1}{1 - \frac{2}{2^\omega}} = \frac{1}{1 - 2^{1-\omega}}. \end{aligned}$$

As $\omega \rightarrow \infty$, $(1 - 2^{1-\omega}) \rightarrow 1^+$. Thus, $[\zeta(\omega)]^{-1} \rightarrow 1^-$ as $\omega \rightarrow \infty$. \square

Additional details in Appendix A.

Mathematical Models – Multiple Periods

Our data model is the union of M copies of $S = \{s_{i,j}\}_{j=1}^{n_i}$ with $s_j = k_j\tau + \varphi + \eta_j$, each with different periods or “generators” $\Gamma = \{\tau_i\}$, k_{ij} ’s and phases. Let $\tau_M = \max_i\{\tau_i\}$ and $\tau_m = \min_i\{\tau_i\}$. Then our data is

$$\mathcal{S} = \bigcup_{i=1}^M \left\{ \varphi_i + k_{ij}\tau_i + \eta_{ij} \right\}_{j=1}^{n_i},$$

- where n_i is the number of elements from the i^{th} generator
- the different periods or “generators” are $\Gamma = \{\tau_i\}$
- $\{k_{ij}\}$ is a linearly increasing sequence of natural numbers with missing observations
- φ_i (the phases) are random variables uniformly distributed in $[0, \tau_i)$
- η_{ij} ’s are zero-mean iid Gaussian with standard deviation $3\sigma_{ij} < \tau/2$
- We think of the data as events from M periodic processes, and represent it, after reindexing, as $\mathcal{S} = \{\alpha_l\}_{l=1}^N$, where $N = \sum_i n_i$.



The Structure of Randomness over $[0, T)$

Theorem (Weyl's Equidistribution Theorem)

Let ϕ be an irrational number, $j \in \mathbb{N}$. Let

$$\langle j\phi \rangle = j\phi - \lfloor j\phi \rfloor.$$

Then given a, b , $0 \leq a < b < 1$,

$$\frac{1}{n} \text{card} \left\{ 1 \leq j \leq n : \langle j\phi \rangle \in [a, b] \right\} \longrightarrow (b - a)$$

as $n \longrightarrow \infty$.

The Structure of Randomness over $[0, T)$

Assuming only minimal knowledge of the range of $\{\tau_i\}$, namely bounds T_L, T_U such that $0 < T_L \leq \tau_i \leq T_U$, we phase wrap the data by the mapping

$$\Phi_\rho(\alpha_I) = \left\langle \frac{\alpha_I}{\rho} \right\rangle = \frac{\alpha_I}{\rho} - \left\lfloor \frac{\alpha_I}{\rho} \right\rfloor,$$

where $\rho \in [T_L, T_U]$, and $\lfloor \cdot \rfloor$ is the floor function. Thus $\langle \cdot \rangle$ is the fractional part, and so $\Phi_\rho(\alpha_I) \in [0, 1)$.

Definition

A sequence of real random variables $\{x_j\} \subset [0, 1)$ is essentially uniformly distributed in the sense of Weyl if given a, b , $0 \leq a < b < 1$,

$$\frac{1}{n} \text{card} \left\{ 1 \leq j \leq n : x_j \in [a, b] \right\} \longrightarrow (b - a)$$

as $n \longrightarrow \infty$ almost surely.

Applying Weyl's Theorem

We assume that for each i , $\{k_{ij}\}$ is a linearly increasing infinite sequence of natural numbers with missing observations such that

$$k_{ij} \longrightarrow \infty \text{ as } j \longrightarrow \infty.$$

Weyl's Theorem applies asymptotically.

Theorem (C)

For almost every choice of ρ (in the sense of Lebesgue measure) $\Phi_\rho(\alpha_I)$ is essentially uniformly distributed in the sense of Weyl.

Applying Weyl's Theorem, Cont'd

- Moreover, the set of ρ 's for which this is not true are rational multiples of $\{\tau_i\}$. Additionally, since \mathbb{Q} is countable (and thus measure zero), these occur (in the sense of $\{\tau_i\}$) with probability zero. Therefore, except for those values, $\Phi_\rho(\alpha_{ij})$ is essentially uniformly distributed in $[T_L, T_U)$. The values at which $\Phi_\rho(\alpha_{ij}) = 0$ almost surely are $\rho \in \{\tau_i/n : n \in \mathbb{N}\}$. These values of ρ cluster at zero, but spread out for lower values of n .
- We phase wrap the data by computing modulus of the spectrum, i.e., compute

$$|S_{iter}(\tau)| = \left| \sum_{j=1}^N e^{(2\pi i s(j)/\tau)} \right|.$$

- The values of

$$|S_{iter}(\tau)|$$

will have peaks at the periods τ_j and their harmonics $(\tau_j)/k$.

Additional details in Appendix B.



The EQUIMEA Algorithm – Multiple Periods

The EQUIMEA Algorithm – Multiple Periods

Our data model is the union of M copies of $S = \{s_{i,j}\}_{j=1}^{n_i}$ with $s_j = k_j\tau + \varphi + \eta_j$, each with different periods or “generators” $\Gamma = \{\tau_i\}$, k_{ij} ’s and phases. Let $\tau_M = \max_i\{\tau_i\}$ and $\tau_m = \min_i\{\tau_i\}$. Then our data is

$$S = \bigcup_{i=1}^M \left\{ \varphi_i + k_{ij}\tau_i + \eta_{ij} \right\}_{j=1}^{n_i},$$

Let $\hat{\tau}$ denote the value the algorithm gives for τ , and let “ \leftarrow ” denote *replacement*.

After reindexing, $S = \{\alpha_l\}_{l=1}^N$, where $N = \sum_i n_i$.

Initialize: Sort the elements of S in descending order. Form the new set with elements $(s_l - s_{l+1})$. Set $s_l \leftarrow (s_l - s_{l+1})$. (Note, this eliminates the phase φ .) Set $\text{iter} = 1$, $i = 1$, and **Error**. Go to **1.**)

The EQUIMEA Algorithm – Multiple Periods

- 1.) [Adjoin 0 after first iteration.] $S_{iter} \leftarrow S \cup \{0\}$.
- 2.) [Sort.] Sort the elements of S_{iter} in descending order.
- 3.) [Compute all differences.] Set $S_{iter} = \bigcup (s_j - s_k)$ with $s_j > s_k$.
- 4.) [Eliminate zero(s).] If $s_j = 0$, then $S_{iter} \leftarrow S_{iter} \setminus \{s_j\}$.
- 5.) [Adjoin previous iteration.] Form $S_{iter} \leftarrow S_{iter} \cup S_{iter-1}$.
- 6.) [Compute spectrum.] Compute $|S_{iter}(\tau)| = \left| \sum_{j=1}^N e^{(2\pi i s(j)/\tau)} \right|$.
- 7.) [Threshold.] Choose the largest peak. Label it as τ_{iter} .
- 8.) If $|\tau_{iter} - \tau_{iter-1}| < \text{Error}$. Declare $\hat{\tau}_i = \tau_{iter}$. If not, $iter \leftarrow (iter + 1)$. Go to 1.).
- 9.) Given τ_i , frequency notch $|S_{iter}(\tau)|$ for $\hat{\tau}_i/m$, $m \in \mathbb{N}$. Let $i \leftarrow i + 1$.
- 10.) [Compute spectrum.] Compute $|S_{iter}(\tau)| = \left| \sum_{j=1}^N e^{(2\pi i s(j)/\tau)} \right|$.
- 11.) [Threshold.] Choose the largest peak. Label it as τ_{i+1} . Algorithm terminates when there are no peaks. Else, go to 9.).

The EQUIMEA Algorithm – Two Periods

- The data in Figure 1 had two underlying periods equaling 1 and $\phi = (1 + \sqrt{5})/2$, with 90% of the information randomly removed and 10% jitter noise.
- Figure 2 shows $|\text{Spec}_{iter}|$ after two iterations. By proceeding right to left, one can easily see the two underlying periods – $\phi = \frac{1+\sqrt{5}}{2}$ and 1.
- One can then deinterleave each separate periodic process from the original by convolving with the individual pulse trains $\sum_{k \in \mathbb{Z}} \delta(t - k\phi)$ and $\sum_{k \in \mathbb{Z}} \delta(t - k)$. Each will reinforce the data elements from the specific generator, allowing the elements to be extracted.
- Figure 3 shows the data deinterleaved, demarked by color – Red – period 1, Green – period ϕ .

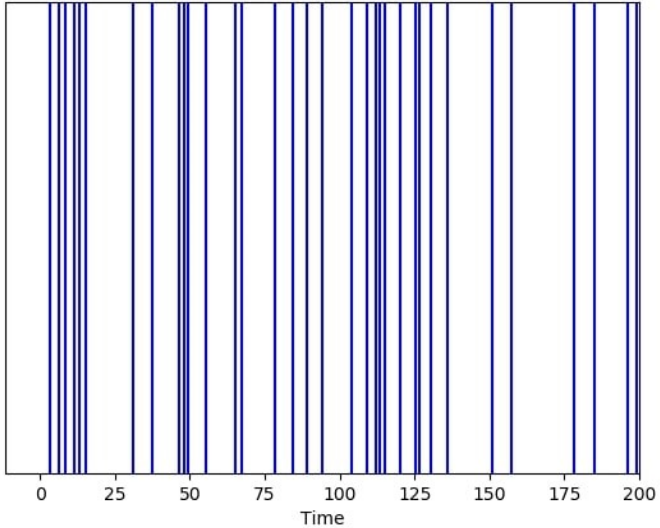


Figure: Two Periods Original Data

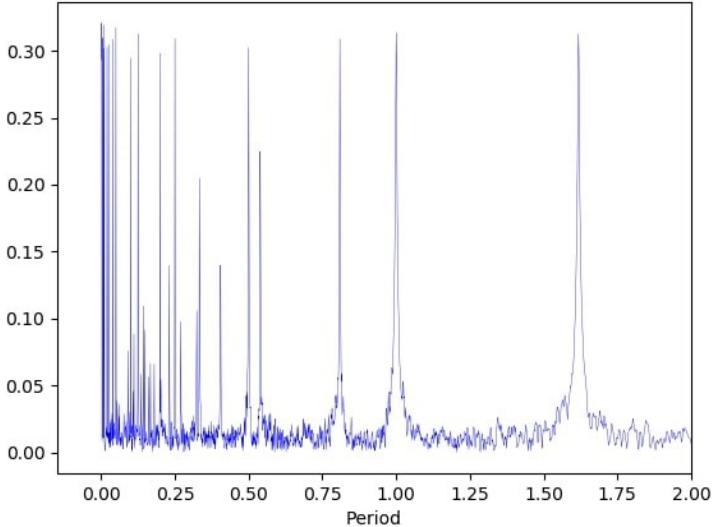


Figure: Two Periods EQUlter2 Spectrum

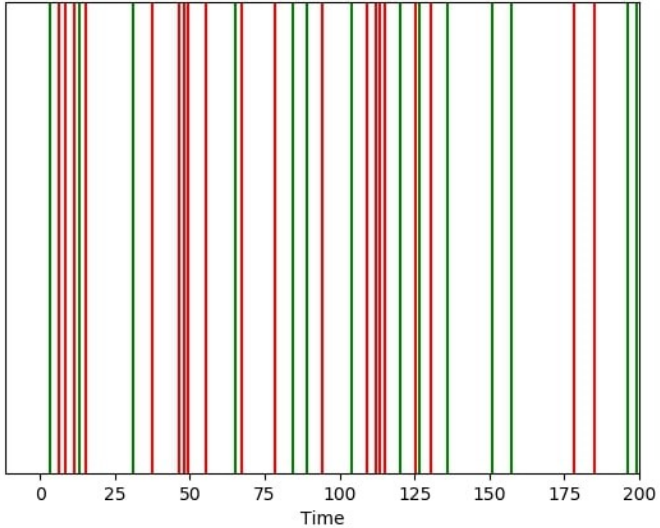


Figure: Two Periods Deinterleaved

- The data in Figure 4 had three underlying periods equaling $1, \phi = (1 + \sqrt{5})/2, \sqrt{7}$, with 90% of the information randomly removed, and 10% jitter noise.
- Figure 5 shows $|\text{Spec}_{iter}|$ after two iterations. By proceeding right to left, one can easily see the three underlying periods – $\sqrt{7}$, $\phi = \frac{1+\sqrt{5}}{2}$, and 1. (“Frequency notching” eliminates the first harmonic peak of $\sqrt{7}$, located at $\sqrt{7}/2$, and so the peak at ϕ stands out.)
- One can then deinterleave each separate periodic process from the original by convolving with the individual pulse trains $\sum_{k \in \mathbb{Z}} \delta(t - k\sqrt{7})$, $\sum_{k \in \mathbb{Z}} \delta(t - k\phi)$, and $\sum_{k \in \mathbb{Z}} \delta(t - k)$. Each will reinforce the data elements from the specific generator, allowing the elements to be extracted.
- Figure 6 shows the data deinterleaved, demarked by color – Red – period 1, Green – period ϕ , Cyan – period $\sqrt{7}$.

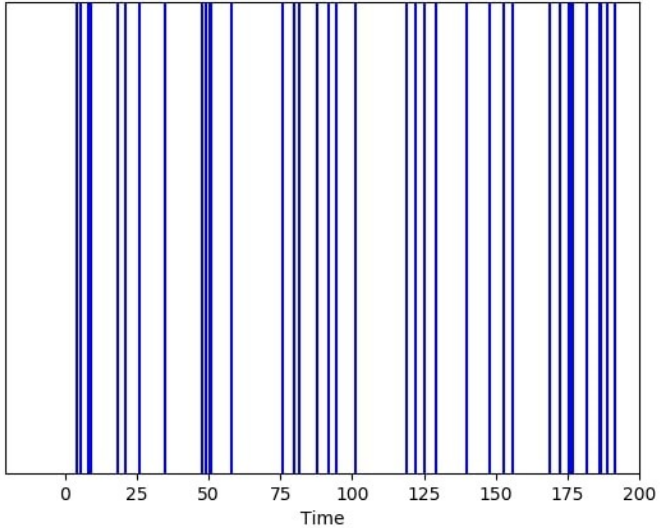


Figure: Three Periods Original Data

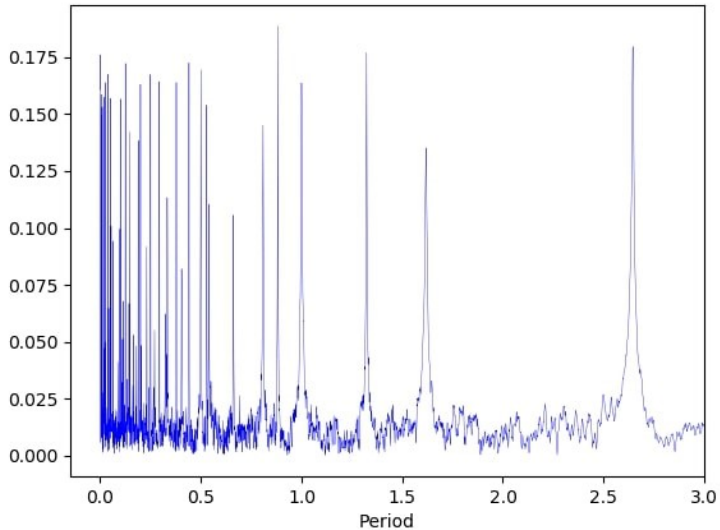


Figure: Three Periods EQUlter2 Spectrum

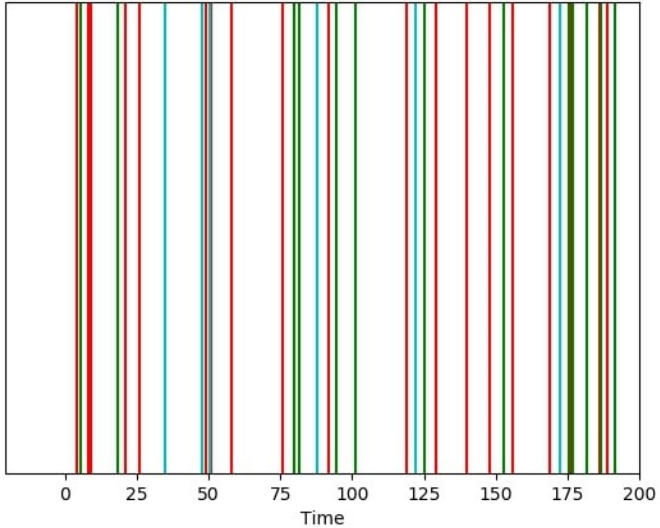


Figure: Three Periods Deinterleaved

- Complete analysis of one dimensional periodic point processes. $s(t) + \eta(t)$ with gaps in the data.
- Questions – $s(t)$ periodic? period $\tau = ?$ Are there multiple periods $\tau_k = ?$ If so, what are they? How do we deinterleave the signals?
- **Solutions – Two Algorithms –**
MEA – Extremely efficient and stable analysis of one-period data.
EQUIMEA – Extremely efficient and stable analysis of multi-period data, including extraction of the fundamental period of the generators and deinterleaving the processes.
- Future research – Extend the analysis to spatial periodic point processes. **Idea** : Create an “eigen-tuning” algorithm using the (EQUI)MEA machinery to reveal periodic structures in sparse noisy spatial periodic point processes.

References



S.D. Casey, "The analysis of periodic point processes," *Journal of Fourier Analysis and Applications (JFAF)*, 33 pp., submitted (2020).



S.D. Casey, "Periodic point processes : theory and application," *Applied Stochastic Models in Business and Industry (Special Issue Honoring B. Kedem)*, 21 pp., to appear (2020).



S.D. Casey and B.M. Sadler, "Pi, the primes, periodicities and probability," *The American Mathematical Monthly*, Vol. 120, No. 7, pp. 594–608 (2013).



S.D. Casey, "Sampling issues in Fourier analytic vs. number theoretic methods in parameter estimation," *31st Annual Asilomar Conference on Signals, Systems and Computers*, Vol. 1, pp. 453–457 (1998) (invited).



S.D. Casey and B.M. Sadler, "Modifications of the Euclidean algorithm for isolating periodicities from a sparse set of noisy measurements," *IEEE Transactions on Signal Processing*, Vol. 44, No. 9, pp. 2260–2272 (1996) .



D.E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms (Second Edition)*, Addison-Wesley, Reading, Massachusetts (1981).



K. Nishiguchi and M. Kobayashi, "Improved algorithm for estimating pulse repetition intervals," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 36, No. 2, pp. 407–421 (2000).



B.M. Sadler and S.D. Casey, "PRI analysis from sparse data via a modified Euclidean algorithm," *29th Annual Asilomar Conf. on Sig., Syst., and Computers* (invited) (1995).



B.M. Sadler and S.D. Casey, "On pulse interval analysis with outliers and missing observations," *IEEE Transactions on Signal Processing*, Vol. 46, No. 11, pp. 2990–3003 (1998).



B.M. Sadler and S.D. Casey, "Sinusoidal frequency estimation via sparse zero crossings," *Jour. Franklin Inst.*, Vol. 337, pp. 131–145 (2000).



Appendix A: π , the Primes, and Probability

Theorem

Given n ($n \geq 2$) “randomly chosen” positive integers $\{k_1, \dots, k_n\}$,

$$P\{\gcd(k_1, \dots, k_n) = 1\} = [\zeta(n)]^{-1}.$$

- Heuristic argument for this “theorem.” Given randomly distributed positive integers, by the Law of Large Numbers, about $1/2$ of them are even, $1/3$ of them are multiples of three, and $1/p$ are a multiple of some prime p . Thus, given n independently chosen positive integers,

$$\begin{aligned}P\{p|k_1, p|k_2, \dots, \text{and } p|k_n\} &= \\&\quad (\text{Independence}) \\P\{p|k_1\} \cdot P\{p|k_2\} \cdot \dots \cdot P\{p|k_n\} &= \\1/(p) \cdot 1/(p) \cdot \dots \cdot 1/(p) &= \\1/(p)^n.\end{aligned}$$

Therefore,

$$P\{p \nmid k_1, p \nmid k_2, \dots, \text{and } p \nmid k_n\} = 1 - 1/(p)^n.$$

- By the Fundamental Theorem of Arithmetic, every integer has a unique representation as a product of primes. Combining that theorem with the definition of gcd, we get

$$P\{\gcd(k_1, \dots, k_n) = 1\} = \prod_{j=1}^{\infty} 1 - 1/(p_j)^n,$$

where p_j is the j^{th} prime.

- But, by Euler's formula,

$$\zeta(z) = \prod_{j=1}^{\infty} \frac{1}{1 - (p_j)^{-z}}, \quad \Re(z) > 1.$$

Therefore,

$$P\{\gcd(k_1, \dots, k_n) = 1\} = 1/(\zeta(n)).$$

π , the Primes, and Probability, Cont'd

This argument breaks down on the first line. Any uniform distribution on the positive integers would have to be identically zero. The merit in the argument lies in the fact that it gives an indication of how the zeta function plays a role in the problem.

Let $\text{card}\{\cdot\}$ denote cardinality of the set $\{\cdot\}$, and let $\{1, \dots, \ell\}^n$ denote the sublattice of positive integers in \mathbb{R}^n with coordinates c such that $1 \leq c \leq \ell$. Therefore,

$N_n(\ell) = \text{card}\{(k_1, \dots, k_n) \in \{1, \dots, \ell\}^n : \gcd(k_1, \dots, k_n) = 1\}$ is the number of relatively prime elements in $\{1, \dots, \ell\}^n$.

Theorem (C)

Let $N_n(\ell) = \text{card}\{(k_1, \dots, k_n) \in \{1, \dots, \ell\}^n : \gcd(k_1, \dots, k_n) = 1\}$. For $n \geq 2$, we have that

$$\lim_{\ell \rightarrow \infty} \frac{N_n(\ell)}{\ell^n} = [\zeta(n)]^{-1}.$$

Brief Discussion of Proof : Let $\lfloor x \rfloor$ denote the floor function of x , namely

$$\lfloor x \rfloor = \max_{k \leq x} \{k : k \in \mathbb{Z}\}.$$

$$N_n(\ell) = \ell^n - \sum_{p_i} \left(\left\lfloor \frac{\ell}{p_i} \right\rfloor \right)^n + \sum_{p_i < p_j} \left(\left\lfloor \frac{\ell}{p_i \cdot p_j} \right\rfloor \right)^n - \sum_{p_i < p_j < p_k} \left(\left\lfloor \frac{\ell}{p_i \cdot p_j \cdot p_k} \right\rfloor \right)^n + \dots$$

Convergence is demonstrated by a sequence of careful estimates, use of Möbius Inversion, and more careful estimates.

π , the Primes, and Probability, Cont'd

The counting formula is seen as follows. Choose a prime number p_i . The number of integers in $\{1, \dots, \ell\}$ such that p_i divides an element of that set is $\left\lfloor \frac{\ell}{p_i} \right\rfloor$. (Note that it is possible to have $p_i > \ell$, because $\left\lfloor \frac{\ell}{p_i} \right\rfloor = 0$.)

Therefore, the number of n -tuples (k_1, \dots, k_n) contained in the lattice $\{1, \dots, \ell\}^n$ such that p_i divides every integer in the n -tuple is

$$\left(\left\lfloor \frac{\ell}{p_i} \right\rfloor \right)^n.$$

Next, if $p_i \cdot p_j$ divides an integer k , then $p_i | k$ and $p_j | k$. Therefore, the number of n -tuples (k_1, \dots, k_n) contained in the lattice $\{1, \dots, \ell\}^n$ such that p_i or p_j or their product divide every integer in the n -tuple is

$$\left(\left\lfloor \frac{\ell}{p_i} \right\rfloor \right)^n + \left(\left\lfloor \frac{\ell}{p_j} \right\rfloor \right)^n - \left(\left\lfloor \frac{\ell}{p_i \cdot p_j} \right\rfloor \right)^n,$$

where the last term is subtracted so that we do not count the same numbers twice (in a simple application of the inclusion-exclusion principle).



Each term is convergent –

$$\begin{aligned} & \frac{1}{\ell^n} \sum_{p_i < \dots < p_k} \left(\left\lfloor \frac{\ell}{p_i \cdots p_k} \right\rfloor \right)^n \leq \frac{1}{\ell^n} \sum_{p_i < \dots < p_k \leq \ell} \left(\frac{\ell}{p_i \cdot p_j \cdot \dots \cdot p_k} \right)^n \\ &= \sum_{p_i < \dots < p_k \leq \ell} \left(\frac{1}{p_i \cdots p_k} \right)^n = \left(\sum_{p \leq \ell} \frac{1}{p^n} \right)^k \\ &\leq \left(\sum_{p \text{ prime}} \frac{1}{p^n} \right)^k \leq \left(\sum_{j=2}^{\infty} \frac{1}{j^n} \right)^k. \end{aligned}$$

Since $n \geq 2$, this series is convergent.

π , the Primes, and Probability, Cont'd

Now, let

$$M_k = \left(\sum_{j=2}^{\infty} \frac{1}{j^n} \right)^k, \text{ for } k = 2, 3, \dots$$

By noting that since $n \geq 2$ and the sum is over $j \in \mathbb{N} \setminus \{1\}$, we get

$$0 < \sum_j \frac{1}{j^n} \leq \left(\frac{\pi^2}{6} - 1 \right) < 1.$$

Since the k^{th} term in the expansion of $N_n(\ell)/\ell^n$ is dominated by M_k and since

$$\sum_{k=0}^{\infty} M_k \leq \sum_{k=0}^{\infty} \left(\frac{\pi^2}{6} - 1 \right)^k = \frac{6}{(12 - \pi^2)}$$

is convergent, the series converges absolutely.



Euler showed that

$$\begin{aligned} & 1 - \sum_{p_i} \frac{1}{p_i^n} + \sum_{p_i < p_j} \frac{1}{(p_i \cdot p_j)^n} - \sum_{p_i < p_j < p_k} \frac{1}{(p_i \cdot p_j \cdot p_k)^n} + \cdots \\ &= \sum_m \frac{\mu(m)}{m^n} = [\zeta(n)]^{-1}. \end{aligned}$$

where the last sum is over $m \in \mathbb{N}$. For $n \geq 2$, this series is absolutely convergent. □

Appendix B: Extending Weyl to Measures

Theorem (Weyl)

Given a fixed irrational number γ , then for every a, b such that $0 \leq a < b < 1$,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \text{card}\{1 \leq k \leq n : a \leq \langle k\gamma \rangle \leq b\} = (b - a). \quad (1)$$

Definition

A sequence of real random variables $\{x_j\} \subset [0, 1)$ is essentially uniformly distributed in the sense of Weyl if given a, b , $0 \leq a < b < 1$, $\frac{1}{n} \text{card}\{1 \leq j \leq n : x_j \in [a, b]\} \rightarrow (b - a)$ as $n \rightarrow \infty$ almost surely.



Extending Weyl to Measures, Cont'd

We assume that for each i , $\{k_{ij}\}$ is a linearly increasing infinite sequence of natural numbers with missing observations such that $k_{ij} \rightarrow \infty$ as $j \rightarrow \infty$. We must make this assumption because the result is only approximately true for a finite length sequence.

Theorem (C)

For almost every choice of ρ (in the sense of Lebesgue measure) $\Phi_\rho(s_I)$ is essentially uniformly distributed in the sense of Weyl.

Sketch of Proof. Let $\rho \in [T_L, T_U]$, $\lfloor \cdot \rfloor$ be the floor function, and $\langle \cdot \rangle$ be the fractional part. The mapping

$$\Phi_\rho(s_I) = \left\langle \frac{s_I}{\rho} \right\rangle = \frac{s_I}{\rho} - \left\lfloor \frac{s_I}{\rho} \right\rfloor,$$

is a measurable and measure-preserving mapping into $[0, 1)$.



Extending Weyl to Measures, Cont'd

Claim . For a.e. choice of ρ , Φ_ρ is ergodic.

Proof of Claim. Normalize $[T_L, T_U)$ to $[0, 1)$. Let X be a square integrable random variable. Thus, we can expand X in a Fourier series

$$X(t) = \sum_{n \in \mathbb{Z}} \hat{X}[n] \exp(i\pi n t).$$

Then

$$X(\Phi_\rho(t)) = \sum_{n \in \mathbb{Z}} \hat{X}[n] \exp(i\pi n t / \rho).$$

For X to be invariant,

$$c_n(1 - \exp(i\pi n t / \rho)) = 0 \text{ for all } n.$$

This implies either

$$c_n = 0 \text{ or } \exp(i\pi n t / \rho) = 1.$$

But since ρ is irrational a.e., the latter is false on a set of full measure.



Extending Weyl to Measures, Cont'd

To finish the proof, note that the set of ρ 's for which this is not true are rational multiples of $\{\tau_i\}$. These are a set of measure zero. Therefore, except for those values, $\Phi_\rho(\alpha_{ij})$ is essentially uniformly distributed in $[0, 1)$. The values at which $\Phi_\rho(s_l) = 0$ almost surely are $\rho \in \{\tau_i/n : n \in \mathbb{N}\}$, which is a set of measure zero. □



Appendix C: Application to FHSS Systems

The algorithms are extremely effective tools for analyzing a very specific set of signals – hop times of frequency-hopping radios. Frequency-hopping spread-spectrum (FHSS) radio technology is a wireless technology that spreads signals over rapidly changing frequencies. Each available frequency band is divided into subfrequencies. Signals rapidly change, or “hop,” among these subfrequency bands in a pre-determined order. The actual messages are broken into segments. These segments are sent in these frequency hops, and then re-assembled by the receiver.

- **Three scales : Signal Environment, FHSS Signal, Transmitted Message**



Application to FHSS Systems, Cont'd

FHSS has advantages over a fixed-frequency transmission:

- FHSS signals are highly resistant to narrowband interference because the signal hops to a different frequency band.
- Signals are difficult to intercept **if the frequency-hopping pattern is not known.**
- FHSS transmissions can share a frequency band with many types of conventional transmissions with minimal mutual interference. FHSS signals add minimal interference to narrowband communications, and vice versa.
- Spread-spectrum signals are highly resistant to deliberate jamming, **unless the adversary has knowledge of the frequency-hopping pattern.**

Application to FHSS Systems, Cont'd

- **Task** – estimating the underlying hop timing of the FHSS signal from **covertly** extracted Fourier data gathered from the signal environment in which FHSS radios were transmitting.
- **Solutions** – The algorithms. This allowed the **identification of the clock cycle of the frequency-hopping pattern, which then lead to the analysis and classification of the this pattern.** Moreover, this in turn allowed for the analysis of the shift-register generated hop sequences, thus providing additional useful information of FHSS data.



The Covert System –

- Extremely fast acousto-optic (Bragg cell) systems computed a windowed discrete Fourier transform of the signal environment.
- From this, a data set could be extracted which contained the measurements of the FHSS carrier frequencies. The sequence of hop times were realized as (extremely noisy and sparse) changes of location in frequency space.
- Buried in all of this information was the signature – the fundamental clock cycle – that would allow the carrier frequencies to be tracked, which in turn made it possible to listen to the message. **The first and most fundamental problem in analyzing information from the hopping radios was to extract this fundamental clock cycle.**

Determining the underlying hop timing answers two important questions about a given FHSS signal.

- **First, it helps identify the radios.** Radios from different manufacturers generally have different underlying clock cycles. Put simply, it answers the question “Friend or foe?”
- The second is that it gives a **predictor for when the radio will hop.**

Application to FHSS Systems, Cont'd

Part of the acousto-optic system mentioned above was a **signal splitter, with one channel going into a signal delay**. This allowed, among other things, a set of markers at the clock cycles of the jumps to be placed. If a frequency change occurred near or at a marker, then it was flagged as a jump. These markers were incorporated into the delayed signal.

This then allowed the system to retune and capture the transmitted message from the delayed signal environment.

Moreover, if a signal got lost for a short while, and a jump occurred at a marker, it was recaptured. (Once several frequency hops were detected matching the given time signatures, a given signal was then reacquired.) Frequency hops were matched in the delayed signal, and the transmitted FHSS message was recorded.

