Relations between pseudorandomness measures

Correlation dominates DFT, Ambiguity, Hamming AC

Gottlieb Isabel Pirsic and Arne Winterhof,
Johannes Kepler University, Linz and
RICAM, Linz

Setup (as usual):

We consider:

- Periodic sequences with period length T,
- over the finite alphabet $\mathbb{T}_m := \{\exp(2\pi ij/m) : j = 1, \dots, m\}$,
- and show results of the form: $A \ll B$, meaning

$$\exists C : A \leq C \cdot B.$$

PR measures: Correlation

- (Period.) Correlation Measure of order ℓ: $(e_i \in \mathbb{T}_m, i \geq 0)$

$$\Gamma_\ell(e_0, \ldots, e_{T-1}) = \max_{\phi, D} \left| \sum_{n=0}^{T-1} \varphi_1(e_{n+d_1})\varphi_2(e_{n+d_2}) \cdots \varphi_\ell(e_{n+d_\ell}) \right|,$$

  max over all ℓ-tuples of bijections and lags/shifts. ($\Gamma \to$ small)
- Motivation: modelling signal stream distortions, {reflect.s, Doppler effects} $\leftrightarrow$ {time shifts, phase dist.s }
- Very general! $\rightsquigarrow$ not easily tractable. Simplifications:
  - phase shifts (i.e., mult. of e_{n+d_i} with an m-th unit root)
  - conjugation
  - ℓ usually small, e.g., $\ell \in \{1, 2, 4\}$
- Example: Autocorrelation ($\ell = 2$, conjugation only)

$$C(E_T) = \max_{1 \leq t < T} \left| \sum_{n=0}^{T-1} e_n \overline{e_{n+t}} \right| \leq \Gamma_2$$

PR measures: DFT, Ambiguity

- Maximum discrete Fourier transform:

$$D(E_T) = \max_{0\le k<T}\left|\sum_{n=0}^{T-1} e_n \omega_T^{-kn}\right|$$

Note: usually $e_n \notin \mathbb{T}_T$. Otherwise: correlation term with $\ell = 1$ and phase shifts only

- Maximum ambiguity:

$$A(E_T) = \max_{1\le t,k<T}\left|\sum_{n=0}^{T-1} e_n \overline{e_{n+t}} \omega_T^{-kn}\right|.$$

Again: usually $e_n \notin \mathbb{T}_T$. Otherwise: correlation term with $\ell = 2$, phase shifts and conjugation only

- Motivations/Applications :
    - D : orthogonal frequency division multiplexing
    - A : relevant in radar systems signal processing

PR measures: Hamming AC

- Hamming Autocorrelation:

$$H(E_T) = \max_{1 \le t < T} \sum_{n=0}^{T-1} \delta(e_n, e_{n+t})$$
$$= \max_{1 \le t < T} \sum_{n=0}^{T-1} \frac{1}{m} \sum_{j=0}^{m-1} (e_n \overline{e_{n+t}})^j$$

- Measures the maximum congruity between the sequence and its shifts $\rightsquigarrow$ will be high, e.g., for subperiodic sequences

Relations: $\Gamma_2(E_T) \ll T^{1/2}\Gamma_4^{1/2}(E_T)$

- Binary, finite case previously by
  [Cassaigne, Mauduit, Sarközy: MR 1904866]
- (Our proof idea: Cauchy-Schwarz and resolving $|z|^2 = z\,\bar{z}$.)

For any $d_i, \varphi_i, (i = 1, 2)$ and positive integer J we have

$$J\left|\sum_{n=0}^{T-1}\varphi_1(e_{n+d_1})\varphi_2(e_{n+d_2})\right| \le \sum_{n=0}^{T-1}\left|\sum_{j=0}^{J-1}\varphi_1(e_{n+j+d_1})\varphi_2(e_{n+j+d_2})\right| =: W.$$

Cauchy-Schwarz implies

$$W^2 \quad \le \quad T\sum_{n=0}^{T-1}\left|\sum_{j=0}^{J-1}\varphi_1(e_{n+j+d_1})\varphi_2(e_{n+j+d_2})\right|^2$$

$$= \quad T\sum_{j,l=0}^{J-1}\sum_{n=0}^{T-1}\varphi_1(e_{n+j+d_1})\varphi_2(e_{n+j+d_2})\overline{\varphi_1}(e_{n+l+d_1})\overline{\varphi_2}(e_{n+l+d_2}).$$

Cancellations occur for $l=j$, $l=j+d_2-d_1$, and $l=j+d_1-d_2$ $\rightsquigarrow$ estimate sum for those (l,j) by T, rest by $\Gamma_4(E_T)$, we get:

$$W^2 \le T(3JT + J^2\Gamma_4(E_T)).$$

Choosing J such as to balance the two terms,

$$J = \left\lceil \frac{T}{\Gamma_4(E_T)} \right\rceil$$

we obtain

$$\left|\sum_{n=0}^{T-1}\varphi_1(e_{n+d_1})\varphi_2(e_{n+d_2})\right| \le 2T^{1/2}\Gamma_4(E_T)^{1/2}.$$

Main Results (More Relations)

- $$\boxed{D(E_T) \ll T^{1/2} C(E_T)^{1/2} \ll T^{1/2}\Gamma_2(E_T)^{1/2} \ll T^{3/4}\Gamma_4(E_T)^{1/4}}$$
- Use basically the same proof strategy.
- $\boxed{A(E_T) \ll T^{1/2}\Gamma_4(E_T)^{1/2}}$
- Again same strategy ...
- $$\begin{aligned} H(E_T) &\leq \frac{T}{m} + \frac{m-1}{m} \max_{1 \leq j \leq m} C(E_T^j) \\ &\ll \frac{T}{m} + \frac{m-1}{m} \max_{1 \leq j \leq m} \Gamma_2(E_T) \ll \frac{T}{m} + T^{1/2}\Gamma_4(E_T)^{1/2} \end{aligned}$$
- Proof idea: m prime $\rightsquigarrow$ power maps are permutations
- $m = 4$: special knowledge about square power map, representation as linear combination of permutations (specific to $m = 4$)

An Example (Some Honesty)

- Let $e_n = \chi(\bar{n}), n \in \mathbb{N}_0, \chi : (\mathbb{Z}/(p))^* \to \mathbb{T}_m, \chi(\bar{0}) := 1$ be a character sequence ($\rightsquigarrow$ period $T = p$). Then, with power maps as perm.s the corr. term becomes at best $\ll p^{1/2}$ where estimate obtained by the Weil bound cannot be improved.
- With the (hybrid) Weil bound (and another relation), we can however give better direct estimates:

$$
\begin{aligned}
C(E_p) &\leq 3 & &< p^{3/4} \\
D(E_p) &\ll p^{1/2} & &< p^{7/8} \\
A(E_p) &\ll p^{1/2} & &< p^{3/4} \\
H(E_p) &\leq \frac{p}{m} + 3 & &< \frac{p}{m} + p^{3/4}
\end{aligned}
$$

- Note 1: Here, C, D, A can also be bounded by $\Gamma_2, \Gamma_1, \Gamma_2$.
- Note 2: D, A also considered with arbitrary ω_R in place of ω_T $\rightsquigarrow$ Weil bound not applicable !

Two-prime gen.: high Γ_4, low $C/D/A/H$

- Let $e_n = \chi(\bar{n})\psi(\tilde{n}),\ n \in \mathbb{N}_0, \chi, \psi$ characters mod p and q of order m, i.e., multiplicative group homomorphisms $\chi : (\mathbb{Z}/(p))^* \to \mathbb{T}_m, \psi : (\mathbb{Z}/(q))^* \to \mathbb{T}_m;\ \bar{0}, \tilde{0} \mapsto 1$.
  We get $T = pq$.
- With the specific lags and permutations

$$0, p, q, p+q \quad \text{and} \quad id, conj, conj, id$$

  we get many cancellations in the corr. term and the worst possible $\Gamma_4 = pq$.
- We can however show

$$C \ll p \wedge q, \qquad D \ll p^{1/2} q^{1/2},$$

$$A \ll p^{1/2} \wedge q^{1/2}, \qquad H \ll \frac{pq}{m} + p \vee q.$$

- Hence, Γ_4 is a more exact figure to detect
  'pseudo-non-randomness'!

Developments

- Investigate the aperiodic and finite case (length N):
  need to restrict the lags further, similar techniques applicable

$$\Gamma_2(E_N) \ll N^{1/2}\Gamma_4^{1/2}, \text{ if } \Gamma_4 \gg N^{1/3}$$

- Hamming AC: treat composite cases, interesting question — but perhaps not very relevant ...
- Find more cases of high/low Γ_4 vs. high/low $C/D/A/H$

Developments

- Investigate the aperiodic and finite case (length N):
  need to restrict the lags further, similar techniques applicable

$$\Gamma_2(E_N) \ll N^{1/2}\Gamma_4^{1/2}, \text{ if } \Gamma_4 \gg N^{1/3}$$

- Hamming AC: treat composite cases, interesting question — but perhaps not very relevant ...
- Find more cases of high/low Γ_4 vs. high/low $C/D/A/H$

Thank you for your Patience/Attention !