The Method of Types: a useful technical tool for forensic analysis

M.Barni and B.Tondi

Università degli Studi di Siena – Dipartimento di Ingegneria

Outline

- **Theoretical background**
  - Description of the Method of Types;
  - Universal Source Coding.
- **An application to Multimedia Forensics**
  - Adversary-aware source identification: the known source case.

Theoretical background

Description of the Method of Types

Introduction

- Csiszár, Körner (1981).
- **Powerful tool in Information Theory (IT)**:
    - all the most important results of IT can be proved by using the M.of T. : *Shannon theory*, *AEP (large deviation theory)*, *channel capacity*,....;
    - the **Universal Source Coding** wholly relies on the M. of T.
- Based on elements of *combinatorial calculus*.

The concept of 'type'

$X \rightarrow$ Source of symbols, DMS ($\mathcal{X} \rightarrow$ alphabet);
a_i, $i = 1, 2...|\mathcal{X}| \rightarrow$ symbols;
$X^n \rightarrow$ random sequence of length n;
$x^n \rightarrow$ realization of X^n, n-length vector drawn from the source;

The concept of 'type'

$X \rightarrow$ Source of symbols, DMS ($\mathcal{X} \rightarrow$ alphabet);
a_i, $i = 1, 2...|\mathcal{X}| \rightarrow$ symbols;
$X^n \rightarrow$ random sequence of length n;
$x^n \rightarrow$ realization of X^n, n-length vector drawn from the source;

Definition (Type)

The type of a sequence x^n is the empirical probability distribution (dpe), i.e. the probability distribution for the source X we are able to estimate from the available sequence,

$$P_{x^n} : \mathcal{X} \rightarrow [0, 1] \qquad P_{x^n}(a_i) = \frac{N(a_i/x^n)}{n} \qquad \forall a_i,\ i = 1, 2, ..., |\mathcal{X}|.$$

$P_{x^n} \rightarrow |\mathcal{X}|$-length vector

Some notation and basic concepts

- $\mathcal{P}_n$: the set of all types computed on n-length sequences: $\mathcal{P}_n = \{P_{x^n}\}$;
- $T(P_{x^n})$: the set of n-length sequences having type P_{x^n}: $\forall P \in \mathcal{P}_n,\ T(P) = \{x^n : P_{x^n} = P\}$; $T() \rightarrow$ type class;

$\Rightarrow$ P_{x^n}, $\mathcal{P}_n$ and $T(P_{x^n})$ are the 'actors' of the Method of Types.

Some notation and basic concepts

- $\mathcal{P}_n$: the set of all types computed on n-length sequences: $\mathcal{P}_n = \{P_{x^n}\}$;
- $T(P_{x^n})$: the set of n-length sequences having type P_{x^n}: $\forall P \in \mathcal{P}_n,\ T(P) = \{x^n : P_{x^n} = P\}$; $T() \rightarrow$ type class;

$\Rightarrow$ P_{x^n}, $\mathcal{P}_n$ and $T(P_{x^n})$ are the 'actors' of the Method of Types.

Quantity of IT involved: the K-L distance and Empirical entropy.

Remind

- Kullback-Leibler distance or divergence between two distributions (e.g. P and Q) on the same alphabet:

$$\mathcal{D}(P||Q) = \sum_{a \in \mathcal{X}} P(a) \log \frac{P(a)}{Q(a)};$$

- Empirical entropy: $H(P_{x^n}) = -\sum_{a \in \mathcal{X}} P_{x^n}(a) \log P_{x^n}(a)$.

The Method of Types

The Method of Types : provides useful bounds on the probability of a type class $Pr\{T(P)\} = Pr\{x^n \in T(P)\}$, for any $P \in \mathcal{P}_n$, and states its behavior for large n (*strong version of the LLN*).

The Method of Types

The Method of Types : provides useful bounds on the probability of a type class $Pr\{T(P)\} = Pr\{x^n \in T(P)\}$, for any $P \in \mathcal{P}_n$, and states its behavior for large n (*strong version of the LLN*).

Observation (Cardinality of $\mathcal{P}_n$)

$|\mathcal{P}_n| < (n+1)^{|\mathcal{X}|}$

Outline: any 'individual' symbol a_i has $(n+1)$ different occurrences possible.

The Method of Types

The Method of Types : provides useful bounds on the probability of a type class $Pr\{T(P)\} = Pr\{x^n \in T(P)\}$, for any $P \in \mathcal{P}_n$, and states its behavior for large n (*strong version of the LLN*).

Observation (Cardinality of $\mathcal{P}_n$)

$|\mathcal{P}_n| < (n+1)^{|\mathcal{X}|}$

Outline: any 'individual' symbol a_i has $(n+1)$ different occurrences possible.

Observation (Cardinality of $T(P)$)

The number of n-length sequences having type P has the following bounds:

$$\frac{2^{nH(P)}}{(n+1)^{|\mathcal{X}|}} \leq |T(P)| \leq n2^{nH(P)}. \quad (1)$$

$X \sim Q(x)$

Given a sequence x^n drawn from the source:

- $Pr\{x^n\}$?

OSS: $Pr\{x^n\}$ is the same for all the sequences x^n belonging to the same type class.

Theorem (Probability of a sequence)

The probability of a sequence x^n having type P_{x^n} is

$$Pr\{x^n\} = 2^{-n[H(P_{x^n}) + \mathcal{D}(P_{x^n}||Q)]}. \quad (2)$$

$X \sim Q(x)$

Given a sequence x^n drawn from the source:

- $Pr\{x^n\}$?

<u>OSS</u>: $Pr\{x^n\}$ is the same for all the sequences x^n belonging to the same type class.

Theorem (Probability of a sequence)

The probability of a sequence x^n having type P_{x^n} is

$$Pr\{x^n\} = 2^{-n[H(P_{x^n}) + \mathcal{D}(P_{x^n}||Q)]}. \tag{2}$$

Proof (1/2).

$$Pr\{x^n\} = \prod_{i=1}^{n} Q(x_i) = \prod_{a \in \mathcal{X}} Q(a)^{N(a/x^n)}$$

(2/2).

$$
\begin{aligned}
&= \prod_{a\in\mathcal{X}} Q(a)^{\frac{N(a/x^n)}{n}\cdot n} \\
&= \prod_{a\in\mathcal{X}} Q(a)^{P_{x^n}(a)\cdot n} \\
&= \prod_{a\in\mathcal{X}} 2^{nP_{x^n}(a)\log Q(a)} \\
&= \prod_{a\in\mathcal{X}} 2^{n[P_{x^n}(a)\log Q(a) - P_{x^n}(a)\log P_{x^n}(a) + P_{x^n}(a)\log P_{x^n}(a)]} \\
&= 2^{n\left(\sum_a [P_{x^n}(a)\log Q(a) - P_{x^n}(a)\log P_{x^n}(a) + P_{x^n}(a)\log P_{x^n}(a)]\right)} \\
&= 2^{-n[H(P_{x^n}) + \mathcal{D}(P_{x^n}||Q)]}. \qquad (3)
\end{aligned}
$$

□

Corollary

If $Q = P_{x^n}$, then

$$Pr\{x^n\} = 2^{-nH(P_{x^n})}. \qquad (4)$$

The corollary allows founding a stricter upper bound for $|T(P)|$, by simply noting that

$$Pr\{T(P_{x^n})\}_{Q=P_{x^n}} = |T(P_{x^n})| \cdot 2^{-nH(P_{x^n})} \leq 1$$

$$\rightarrow |T(P_{x^n})| \leq 2^{nH(P_{x^n})}.$$

Hence, $\forall P \in \mathcal{P}_n \qquad \frac{2^{nH(P)}}{(n+1)^{|\mathcal{X}|}} \leq |T(P_{x^n})| \leq 2^{nH(P)}.$

Given a type $P \in \mathcal{P}_n$:

- $Pr\{T(P)\}_Q$?

Theorem (Probability of a type class)

The probability of the type class $T(P)$ is bounded as follows:

$$\frac{2^{-n\mathcal{D}(P||Q)}}{(n+1)^{|\mathcal{X}|}} \leq Pr\{T(P)\}_Q \leq 2^{-n\mathcal{D}(P||Q)}. \quad (5)$$

Proof (1/2).

$$Pr\{T(P)\}_Q = |T(P)| \cdot Pr\{x^n\} = |T(P)| \cdot 2^{-n[H(P)+\mathcal{D}(P||Q)]}. \quad (6)$$

(2/2).

We use the known bounds on $|T(P)|$:

1. $Pr\{T(P)\}_Q \leq 2^{nH(P)} \cdot 2^{n[H(P_{x^n}) + \mathcal{D}(P_{x^n}||Q)]} = 2^{-n\mathcal{D}(P||Q)}$;
2. $Pr\{T(P)\}_Q \geq \frac{2^{nH(P)}}{(n+1)^{|\mathcal{X}|}} \cdot 2^{n[H(P_{x^n}) + \mathcal{D}(P_{x^n}||Q)]} = \frac{2^{-n\mathcal{D}(P||Q)}}{(n+1)^{|\mathcal{X}|}}$.

□

According to the theorem, at the first order on the exponent we have

$$Pr\{T(P)\}_Q \simeq 2^{-n\mathcal{D}(P||Q)}.$$

(2/2).

We use the known bounds on $|T(P)|$:

1. $Pr\{T(P)\}_Q \leq 2^{nH(P)} \cdot 2^{n[H(P_{x^n})+\mathcal{D}(P_{x^n}||Q)]} = 2^{-n\mathcal{D}(P||Q)}$;
2. $Pr\{T(P)\}_Q \geq \frac{2^{nH(P)}}{(n+1)^{|\mathcal{X}|}} \cdot 2^{n[H(P_{x^n})+\mathcal{D}(P_{x^n}||Q)]} = \frac{2^{-n\mathcal{D}(P||Q)}}{(n+1)^{|\mathcal{X}|}}$.

□

According to the theorem, at the first order on the exponent we have

$$Pr\{T(P)\}_Q \simeq 2^{-n\mathcal{D}(P||Q)}.$$

- *For large n ?*

⇒ The *Law of Large Numbers (LLN)* comes out!

Hence, the unitary sum constraint yields: $Pr\{T(Q)\}_Q \to 1$.

[1] This is always possible if n is sufficiently large.

⇒ The *Law of Large Numbers (LLN)* comes out!

In order to see this interesting result, let us consider that

- If $Q \in \mathcal{P}_n$ [1] we can write

$$Pr\{T(Q)\}_Q \leq 1;$$

- As to the others $P \in \mathcal{P}_n$:

$$\begin{aligned} Pr\left\{\begin{matrix}\text{tutte le altre}\\ \text{type classes}\end{matrix}\right\} &\leq \sum_{P \in \mathcal{P}_n, P \neq Q} 2^{-n\mathcal{D}(P||Q)} \\ &\leq (n+1)^{|\mathcal{X}|} \max_{P \in \mathcal{P}_n, P \neq Q} 2^{-n\mathcal{D}(P||Q)} \\ &\leq (n+1)^{|\mathcal{X}|} 2^{-n \min_{P \in \mathcal{P}_n, Q \neq P} \mathcal{D}(P||Q)} \to 0. \end{aligned}$$

Hence, the unitary sum constraint yields: $Pr\{T(Q)\}_Q \to 1$.

[1] This is always possible if n is sufficiently large.

To sum up, from the previous theorem follows that

"As n tends to infinity, the probability of the right type class, i.e. $Pr\{T(Q)\}_Q$, tends to 1 , while the probability of any other type class or wrong type class, i.e. $Pr\{T(P)\}_Q$ (with $P \neq Q$), tends to 0"; that is, as $n \to \infty$

- $Pr\{T(Q)\}_Q \to 1$;
- $Pr\{T(P)\}_Q \to 0$.

OSS: the *decreasing velocity* of each probability ($Pr\{T(P)\}_Q$, $P \neq Q$) is regulated by $\mathcal{D}(P||Q)$.

This result can be interpreted as follows:

- The number of the sequences, i.e. the "right" and "wrong" ones[2], grows much with n; that is

$$|T(P)| \simeq 2^{nH(P)};$$

  Some "wrong-type" sequences could be in number more than the "right-type" ones;
- the probability of a sequence decreases very rapidly as n increase, according to $Pr\{x^n \in T(P)\}_Q = 2^{-n(H(P)+\mathcal{D}(P||Q))}$.

Thus, for a given type class, "**the only way through which the increasing of the number of sequences could balance the reduction of the probability of any sequence is $\mathcal{D}(P||Q) = 0$, which can only be achieved if $P = Q$**".

[2] "right sequence" $= x^n \in \{T(Q)\}_Q$, "wrong sequence" $= x^n \in \{T(P)\}_Q$ where $P \neq Q$.

Universal Source Coding

Universal Source Coder (Weak)

The weak Universal Source Coder is a coder which, employing a bit rate R, succeeds in correctly coding any source $X \sim Q(X)$ having $H(X) \leq R$.

- Why Weak?

If the source has $H(X) < R$ the universal coder does not reach the entropy as code rate (Shannon Coding) $\rightarrow$ *it's possible to do better!*

Universal Source Coder (Weak)

The weak Universal Source Coder is a coder which, employing a bit rate R, succeeds in correctly coding any source $X \sim Q(X)$ having $H(X) \leq R$.

- Why Weak?

If the source has $H(X) < R$ the universal coder does not reach the entropy as code rate (Shannon Coding) $\rightarrow$ *it's possible to do better!*

Universal Source Coder (Strong)

The strong Universal Source Coder is a coder which, for any source $X \sim Q(X)$, succeeds in generating a code having rate $R = H(X)$.

- Why Strong?

$H(X)$ is the Shannon limit for the rate $\rightarrow$ *it's NOT possible to do better!*

- Such a coder (weak and strong) really exists?

Yes, the Method of Types allows to prove the existence.

Theorem (Existence of the Weak U.S.C.)

For any discrete memoryless source X a Universal Source Coding exists.

Outline of the Proof (1/2).

We are interested in *coding* the sources X with $H(X) \leq R$. Let us show it is possible by using rate R.

$$\text{Fix } n,\ \mathcal{P}_n \rightarrow \begin{cases} P : H(P) \leq R & (a) \\ P : H(P) > R & (b). \end{cases}$$

We consider only types P in (a) [3].

[3] It is reasonable according to the Method of Types.

(2/2).

- How many bit are necessary?
  - How many sequences there are in a **type-class**?

$$|T(P)| \leq 2^{nH(P)} \leq 2^{nR};$$

  - How many **type**?

$$N^{\circ}\{P \in (a)\} \leq |\mathcal{P}_n| < (n+1)^{|\mathcal{X}|}.$$

Number of sequences which must be indexed: $< (n+1)^{|\mathcal{X}|} 2^{nR}$.

Average number of *bit per symbol* required:

$< \frac{\log[(n+1)^{|\mathcal{X}|} 2^{nR}]}{n} = |\mathcal{X}| \frac{\log(n+1)}{n} + \frac{nR}{n} \longrightarrow R$ bit/symbol.

□

(2/2).

- How many bit are necessary?
  - How many sequences there are in a **type-class**?

$$|T(P)| \leq 2^{nH(P)} \leq 2^{nR};$$

  - How many **type**?

$$N^{\circ}\{P \in (a)\} \leq |\mathcal{P}_n| < (n+1)^{|\mathcal{X}|}.$$

Number of sequences which must be indexed: $< (n+1)^{|\mathcal{X}|} 2^{nR}$.

Average number of *bit per symbol* required:

$< \frac{\log[(n+1)^{|\mathcal{X}|} 2^{nR}]}{n} = |\mathcal{X}| \frac{\log(n+1)}{n} + \frac{nR}{n} \longrightarrow R$ bit/symbol.

- Practical coders: *LZ77*, *LZ78*, *LZW*.

Source Coding vs Universal Source Coding

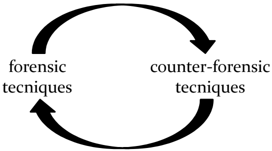
- Are both asymptotic codings!
- The differences lies on the *velocities*.

  If the source is known (Source Coding) the entropy value can be reached *by a lower n in practice*.

An application to Multimedia Forensics

Definition of the problem

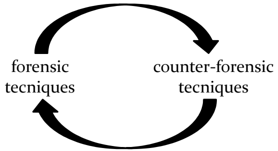
Limits of forensic analysis in presence of an adversary: "*Any attempt to improve the forensic analysis will be accompanied by a dual effort to device more powerful counter-forensic techniques that leave less and less evidence into the forged documents*"
$\rightarrow$ **virtuous loop**



Compelling goal: to investigate the ultimate limits of forensics and counter forensics analysis.

Definition of the problem

Limits of forensic analysis in presence of an adversary: "*Any attempt to improve the forensic analysis will be accompanied by a dual effort to device more powerful counter-forensic techniques that leave less and less evidence into the forged documents*"
→ **virtuous loop**



Compelling goal: to investigate the ultimate limits of forensics and counter forensics analysis.

- Our contribution: to provide a theoretical framework to the **source identification problem** in presence of an adversary.

Adversary-aware source identification: the known source case

The Source Identification Problem

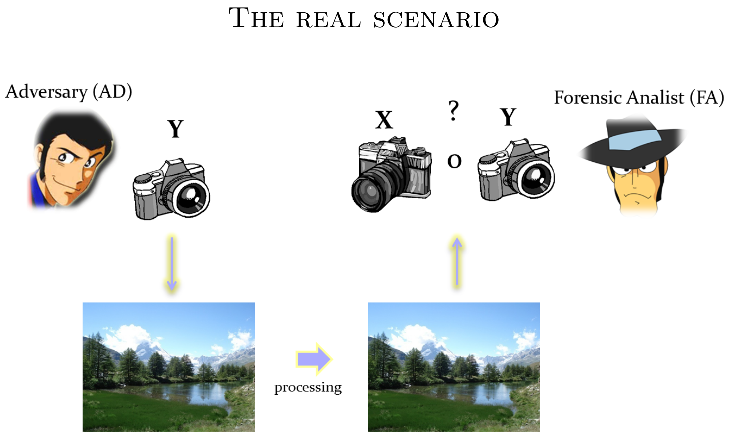


Figure : the image the AD want to modify might have *critical relevance* in many fields (e.g. judicial, medical,....).

Problem schematization

Sources: $X \sim P_X$, $Y \sim P_Y$.

The FA's aim: to distinguish sequences generated by X from those generated by Y.

$$x^n = x_1, x_2, \ldots, x_n \quad \rightarrow \ \in X \ \text{ or } \in Y?$$

The AD's aim: to trasform a sequence drawn from Y, e.g. y^n, into a new sequence z^n, as close as possible to y^n [a], in such a way that the FA believes that z^n has been generated by X.

$$y^n = y_1, y_2, \ldots, y_n \quad \rightarrow \quad z^n = z_1, z_2, \ldots, z_n.$$

[a] in real contexts the AD will want to preserve perceptual similarities between the images.

Theoretical foundations

- **Game Theory** $\rightarrow$ the source identification problem is formalized as a game (*zero-sum game*).

Players: the Forensic analyst (FA) and the Adversary (AD).

Game analysis: the main theoretical tools are

- **Hypothesis test** : used to formalize the classification problem faced by the FA:

  $$Hp\ 0 = \text{"}x^n \text{ belongs to } X\text{"};$$
  $$Hp\ 1 = \text{"}x^n \text{ belongs to } Y\text{"};$$

- **Information theory**: is the branch to which the main quantities involved in our analysis belong.

The Source Identification Game (known source case)

→ *The FA and the AD know the source X.*
The source Y is known to the AD and not necessarily to the FA.

SI_{ks} game $\doteq (\mathcal{S}_{FA}, \mathcal{S}_{AD}, u)$
$\mathcal{S}_{FA}, \mathcal{S}_{AD} \rightarrow$ *sets of strategies,* $\quad u \rightarrow$ *payoff.*

$$\mathcal{S}_{FA} = \{\Lambda_0 : P_X(x^n \notin \Lambda_0) \leq P^*_{fp}\},$$
$$\mathcal{S}_{AD} = \{f(y^n) : d(y^n, f(y^n)) \leq nD\},$$
$$u = -P_{fn} = -P_Y(f(y^n) \in \Lambda_0) = -\sum_{y^n : f(y^n) \in \Lambda_0} P_Y(y^n).$$

The Source Identification Game (known source case)

→ *The FA and the AD know the source X.*
The source Y is known to the AD and not necessarily to the FA.

SI_{ks} game $\doteq (\mathcal{S}_{FA}, \mathcal{S}_{AD}, u)$
$\mathcal{S}_{FA}, \mathcal{S}_{AD} \rightarrow$ *sets of strategies,* $\quad u \rightarrow$ *payoff.*

$$\mathcal{S}_{FA} = \{\Lambda_0 : P_X(x^n \notin \Lambda_0) \leq P^*_{fp}\},$$
$$\mathcal{S}_{AD} = \{f(y^n) : d(y^n, f(y^n)) \leq nD\},$$
$$u = -P_{fn} = -P_Y(f(y^n) \in \Lambda_0) = -\sum_{y^n : f(y^n) \in \Lambda_0} P_Y(y^n).$$

⇒ Limitations to the model for mathematical tractability:

hp) Asymptotic version of the game and limited resources for the FA: SI^{lr}_{ks}.

SI_{ks}^{lr} game: resolution procedure

1. Optimum strategies: $\mathcal{S}_{FA}^{*}$, $\mathcal{S}_{AD}^{*}$;
2. The profile $(\mathcal{S}_{FA}^{*}, \mathcal{S}_{AD}^{*})$ is a *Nash equilibrium*;
3. Payoff at the equilibrium: u^{*} $(= u(\mathcal{S}_{FA}^{*}, \mathcal{S}_{AD}^{*}))$.

$\rightarrow$ Step 1.
The determination of the optimum strategies passes through the search for the optimum acceptance region Λ_0 *and* f *function*:
$(\mathcal{S}_{FA}^{*}, \mathcal{S}_{AD}^{*}) \leftrightarrow (\Lambda_0^{*}, f^{*})$.

SI_{ks}^{lr} game: resolution procedure

1. Optimum strategies: $\mathcal{S}_{FA}^*$, $\mathcal{S}_{AD}^*$;
2. The profile ($\mathcal{S}_{FA}^*$,$\mathcal{S}_{AD}^*$) is a *Nash equilibrium*;
3. Payoff at the equilibrium: u^* $(= u(\mathcal{S}_{FA}^*, \mathcal{S}_{AD}^*))$.

$\rightarrow$ Step 1.

The determination of the optimum strategies passes through the search for the optimum acceptance region Λ_0 *and* f *function*: $(\mathcal{S}_{FA}^*, \mathcal{S}_{AD}^*) \leftrightarrow (\Lambda_0^*, f^*)$.

• Consequence of the limited resources assumption (**lr**):

the acceptance region Λ_0 is a union of type classes!!

The set of strategies for the FA becomes:
$\mathcal{S}_{FA} = \{\Lambda_0 \in 2^{\mathcal{P}_n} : P_{fp} \leq 2^{-\lambda n}\}$.

Optimum strategy for the FA

- Λ_0^*?

The **Method of Types** allows to prove the following lemma:

Lemma (Optimum acceptance region)

Let Λ_1^* $(= \Lambda_0^{*,c})$ *be:*

$$\Lambda_1^* = \{P \in \mathcal{P}_n : \mathcal{D}(P||P_X) \geq \lambda - |\mathcal{X}|\frac{log(n+1)}{n}\}. \tag{7}$$

Then, we have

- $P_{fp} \leq 2^{-n(\lambda-\delta_n)}$, *with* $\delta_n \to 0$ *for* $n \to \infty$,
- *for every* $\Lambda_0 \in \mathcal{S}_{FA}$ *we have* $\Lambda_1 \subseteq \Lambda_1^*$.

Proof (1/2).

- *Part 1*

Λ_0^* and Λ_1^* are unions of type classes

$$P_{fp}(\Lambda_0^*) = P_X(x^n \in \Lambda_1^*) = \sum_{P \in \Lambda_1^*} P_X(T(P)). \quad (8)$$

By using the bound on the total number of types $|\mathcal{P}_n|$ and on the probability of a type class $Pr\{T(P)\}$, we have

$$\begin{aligned} P_{fp}(\Lambda_0^*) &\leq (n+1)^{|\mathcal{X}|} \max_{P \in \Lambda_1^*} P_X(T(P)) \\ &\leq (n+1)^{|\mathcal{X}|} 2^{-n \min_{P \in \Lambda_1^*} \mathcal{D}(P||P_X)} \\ &\leq (n+1)^{|\mathcal{X}|} 2^{-n\left(\lambda - |\mathcal{X}| \frac{\log(n+1)}{n}\right)} \\ &= 2^{-n\left(\lambda - 2|\mathcal{X}| \frac{\log(n+1)}{n}\right)}, \end{aligned} \quad (9)$$

(2/2).

proving the first part of the lemma with $\delta_n = 2|\mathcal{X}|\frac{\log(n+1)}{n}$.

- *Part 2*

Take an arbitrarily region $\Lambda_0 \in \mathcal{S}_{FA}$ and let P be a type in Λ_1:

$$\begin{aligned} 2^{-\lambda n} &\geq P_X(\Lambda_1) \\ &\geq P_X(T(P)) \\ &\geq \frac{1}{(n+1)^{|\mathcal{X}|}} 2^{-n\mathcal{D}(P||P_X)}. \end{aligned} \tag{10}$$

Hence, by taking the log of both sides:

$$\mathcal{D}(P||P_X) \geq \lambda - |\mathcal{X}|\frac{log(n+1)}{n}, \tag{11}$$

proving that $P \in \Lambda_1^*$. □

Interesting consequence of the *Lemma*:

The FA optimum strategy does not depend on:

- the strategy chosen by the AD;
- P_Y.

The optimum strategy is universally optimal across all the probability density function.

Interesting consequence of the *Lemma*:

The FA optimum strategy does not depend on:

- the strategy chosen by the AD;
- P_Y.

The optimum strategy is universally optimal across all the probability density function.

- *To sum up* :

The Method of Types has given a valuable contribution to our analysis by providing the **optimum strategy for the FA** (*first step of the Game Analysis*).

Future steps

The Method of Types turns out to be a useful tool even for

- determining the *value* and the *behavior* of the payoff at the equilibrium, $u(\Lambda_0^*, f^*)$ (*third step of the Game Analysis*);
- retracing the same steps and solving the **Source Identification Game with Training Data**.

References I

M.Barni and B.Tondi.
Lecture notes on information theory.
Notes for the course of Information Theory.

I. Csiszar.
The method of types.
IEEE Transactions on Information Theory, 44(6):2505–2523, October 1998.

T. M. Cover and J. A. Thomas.
Elements of Information Theory.
Wiley Interscience, New York, 1991.

M. Barni.
A game theoretic approach to source identification with known statistics.
In *ICASSP 2012, IEEE International Conference on Acoustics, Speech and Signal Processing*, Kyoto, Japan, 25-30 March 2012.

J. Nash.
Equilibrium points in n-person games.
Proceedings of the National Academy of Sciences, 36(1):48–49, 1950.

References II

M. J. Osborne and A. Rubinstein.
A Course in Game Theory.
MIT Press, 1994.

M.Chen, J. Fridrich, M. Goljan, and J. Lukas.
Determining image origin and integrity using sensor noise.
IEEE Transactions on Information Forensics and Security, 3(1):74–90, March 2008.

P. Comesana, N. Merhav, and M. Barni.
Asymptotically optimum universal watermark embedding and detection in the high snr regime.
IEEE Transactions on Information Theory, 56(6):2804–2815, June 2010 2010.

I. Csiszár and J. Körner.
Information Theory: Coding Theorems for Discrete Memoryless Systems. 2nd edition.
Cambridge University Press, 2011.

References III

H. Farid.
Exposing digital forgeries from JPEG ghosts.
IEEE Transactions on Information Forensics and Security, 4(1):154–160, March 2009.

M. Gutman.
Asymptotically optimal classification for multiple tests with empirically observed statistics.
IEEE Transactions on Information Theory, 35(2):401–408, March 1989.

Y-F. Hsu and S-F. Chang.
Camera response functions for image forensics: An automatic algorithm for splicing detection.
IEEE Transactions on Information Forensics and Security, 5(4):816–825, December 2010.

S. M. Kay.
Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory.
Prentice Hall, 1998.

References IV

M. Kendall and S. Stuart.
The Advanced Theory of Statistics, vol. 2, 4th edition.
MacMillan, New York, 1979.

M. Kirchner and R. Bohme.
Hiding traces of resampling in digital images.
IEEE Transactions on Information Forensics and Security, 3(4):582–292, December 2008.

M. Goljan, J. Fridrich, and M. Chen.
Sensor noise camera identification: countering counter forensics.
In *SPIE Conference on Media Forensics and Security, San Jose, CA*, 2010.

T. Gloe, M. Kirchner, A. Winkler, and R. Bohme.
Can we trust digital image forensics ?
In *ACM Multimedia 2007, Augsburg, Germany*, pages 78–86, September 2007.

W. Hoeffding.
Asymptotically optimal tests for multinomial distributions.
The Annals of Mathematical Statistics, 36(2):369–401, April 1965.

References V

S. Lyu and H. Farid.
How realistic is photorealistic ?
IEEE Transactions on Signal Processing, 53(2):845–850, February 2005.

B. Mahdian and S. Saic.
Using noise inconsistencies for blind image forensics.
Image and Vision Computing, pages 1497–1503, 2009.

N. Merhav and M. J. Weinberger.
On universal simulation of information sources using training data.
IEEE Transactions on Information Theory, 50(1):5–20, January 2004.

N. Merhav and E. Sabbag.
Optimal watermark embedding and detection strategies under limited detection resources.
IEEE Transactions on Information Theory, 54(1):255–274, January 2008.

X. Pan, X. Zhang, and S. Lyu.
Exposing image forgery with blind noise estimation.
In *ACM Multimedia and Security Workshop 2011, Buffalo, New York, USA*, pages 15–20, September 2011.

References VI

A. C. Popescu and H. Farid.
Exposing digital forgeries by detecting traces of resampling.
IEEE Transactions on Signal Processing, 53(2):758–767, February 2005.

E. Delp, N. Memon, and M. Wu.
Special issue on digital forensics.
IEEE Signal Processing Magazine, 26(2), March 2009.

L. Ziv.
On classification with empirically observed statistics and universal data compression.
IEEE Transactions on Information Theory, 34(2):278–286, March 1988.