

令和1 年度 大阪教育大学 & AIMaP ワークショップ

ウェーブレット理論と工学への応用

OKU & AIMaP 2019 Workshop

Wavelet theory and its applications to engineering

主催：大阪教育大学, AIMaP

場所：大阪教育大学 天王寺キャンパス

日程：令和 1 年 12月 5 日(木) 13:20 – 18:00

令和 1 年 12月 6 日(金) 10:00 – 13:00

ウェーブレット理論と工学への応用

2019 年 12 月 5 日 – 12 月 6 日

大阪教育大学 天王寺キャンパス 西館 第 1 (A) 講義室

2019 年 12 月 5 日 (木) 13:20 – 18:00

13:20–13:30 開催の挨拶

13:30–14:30 座長：守本晃（大阪教育大学）

戸田浩，章忠（豊橋技術科学大学）

近似ガボールウェーブレットを用いた離散ウェーブレット変換の設計法に関する考察 1

ガボールウェーブレット（Gabor wavelet）は，時間周波数解析における優れた特性を持つウェーブレットとして知られているが，このウェーブレットは，もっぱら連続ウェーブレット変換に用いられており，これまで離散ウェーブレット変換に用いられることはなかった．そこで本研究では，オリジナルのガボールウェーブレットに最小限の補正を施した，近似ガボールウェーブレットを用いて，タイトウェーブレットフレームの設計を試みる．そして，さらに精度の高い近似ガボールウェーブレットを用いた，さまざまな条件における，双対ウェーブレットフレームの設計法を考察する．

15:00–16:00 座長：鈴木俊夫（流通経済大学）

井川信子（流通経済大学），守本晃，芦野隆一（大阪教育大学）

聴性定常反応とウェーブレット解析について 23

自作計測機器により SAM 音刺激を与えて得られた聴力正常成人の聴性誘発脳波データから聴性定常反応成分を抽出する際，その反応波形の特性に応じてどのようにウェーブレット解析を用いるかについて提案し，その工学的応用の有効性について議論する．

16:30–17:30 座長：橋本紘史（筑波大学）

新井康平（佐賀大学）

DWT ハイディングとトリプル DES による暗号通信 42

ステガノグラフィ離散ウェーブレット変換を使用したデータ隠蔽方法：DWT および暗号化トリプルデータ暗号化標準：DES を提案する．情報技術は，特に情報の処理と普及に関して，人間の生活から切り離せないものになっている．情報技術の進歩に伴い，情報を変更したり，損害を与えたりすることで，そのような情報を悪用することもある．そのような事態を回避するには，DWT メソッドを使用して，最初にデータを他のメディアに保護する必要がある．この方法を選択するのは，データ挿入の画像が元の画像にほとんど似ているためである．トリプル DES メソッドは，データをエンコードし，追加のセキュリティを提供して，隠されたデータを解決するのが難しいようにするためにも必要である．この方法を選択するのは，ブルートフォース，選択したプレーンテキストおよび既知のプレーンテキスト攻撃に対して耐性があるためである．テストに基づく，画像の挿入は，明るさとコントラストの画像操作に対して 100 % 耐性があるが，トリミング，サイズ変更，回転した画像操作にはそれほど耐性がない．他のテストとして写真データを例示する．

2019 年 12 月 6 日（金）10:00 – 13:00

10:00 – 11:00 座長：藤田景子（富山大学）

守本晃（大阪教育大学）

Mellin 変換を用いた、画像の拡大・縮小率を求める数値実験について 62

「2つの画像が拡大・縮小の関係にあるかどうか」、「拡大率はどの程度か」を調べることは、パターン認識などにおいて重要な前処理である。本講演では、スケール変換に対して不変な変換である Mellin 変換を用いて、画像の拡大率を求める数値実験について述べる。とくに、画像の平行移動の影響を無視できるフーリエ像の絶対値に対して、Mellin 変換を用いる場合の注意点・問題点などを議論したい。

11:30–12:30 座長：藤田景子（富山大学）

芦野隆一（大阪教育大学）

四元数線形正準変換

線形正準変換は光学や信号解析において重要な役割を果たしている。フーリエ変換、ラプラス変換、分数次フーリエ変換、フレネル変換などの変換は、線形正準変換の特別な場合として扱うことができる。したがって、四元数関数の線形正準変換を考えることは意味がある。本講演では、四元数線形正準変換を考える上で適切な合成積の定義を述べ、四元数線形正準変換の合成積定理について述べる。

大阪教育大学 天王寺キャンパス 西館 第 1 講義室

〒543-0054 大阪市天王寺区南河堀町 4-88 電話番号 (06)6775-6611

JR 天王寺駅，地下鉄天王寺駅，近鉄大阪阿部野橋駅下車，徒歩約 10 分。

JR 寺田町駅下車，徒歩 5 分。

注意：入校時に所属・氏名・用件を聞かれる場合があります。

<https://osaka-kyoiku.ac.jp/>

数学アドバンストイノベーションプラットフォーム

AIMaP : Advanced Innovation powered by Mathematics Platform

<https://aimap.imi.kyushu-u.ac.jp/wp/>

連絡先

守本晃，芦野隆一，森岡達史（大阪教育大学）

e-mail: morimoto@cc.osaka-kyoiku.ac.jp

tel: 072-978-3665

<https://www.osaka-kyoiku.ac.jp/~morimoto/TENWS/ws2019HP/>

戸田 浩, 章 忠

近似ガボールウェーブレットを用いた 離散ウェーブレット変換の設計法に 関する考察

戸田 浩, 章 忠
豊橋技術科学大学

1

Contents

1. Preliminaries.
2. We introduce our proposed Hilbert transform pairs of orthonormal bases of chromatic-scale wavelets.
3. Comparing between Gabor and our wavelets, we appeal why we want to use the Gabor wavelet in the discrete wavelet transform.
4. For this aim, we propose “Tight wavelet frame using complex wavelet designed in free shape of frequency domain”.
5. We construct the tight wavelet frame using an approximate Gabor wavelet.
6. The dual wavelet frame using an approximate Gabor wavelet.

The contents are like these.

2

Preliminaries

The inner product of the functions $f(t) \in L^2(\mathbf{R})$ and $g(t) \in L^2(\mathbf{R})$.

$$\langle f, g \rangle = \int_{-\infty}^{\infty} f(t) \overline{g(t)} dt$$

The norm of $f(t) \in L^2(\mathbf{R})$.

$$\|f\| = \sqrt{\langle f, f \rangle}$$

The Fourier transform of $f(t) \in L^1(\mathbf{R})$.

$$F(f)(\omega) = \hat{f}(\omega) = \int_{-\infty}^{\infty} f(t) e^{-i\omega t} dt$$

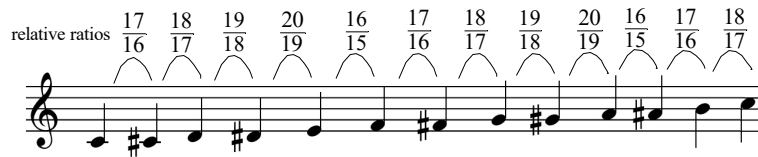
The inverse Fourier transform of $\hat{f}(\omega) \in L^1(\mathbf{R})$.

$$F^{-1}(f)(t) = f(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{f}(\omega) e^{i\omega t} d\omega$$

We use these formulas.

3

Our proposed “Hilbert transform pairs of orthonormal bases of chromatic-scale wavelets”



The original chromatic scale

All the local dilations $\frac{R_{j+1}}{R_j}$, $j \in \mathbf{Z}$ are represented as $\frac{n+1}{n}$, $n \in \mathbf{N}$.

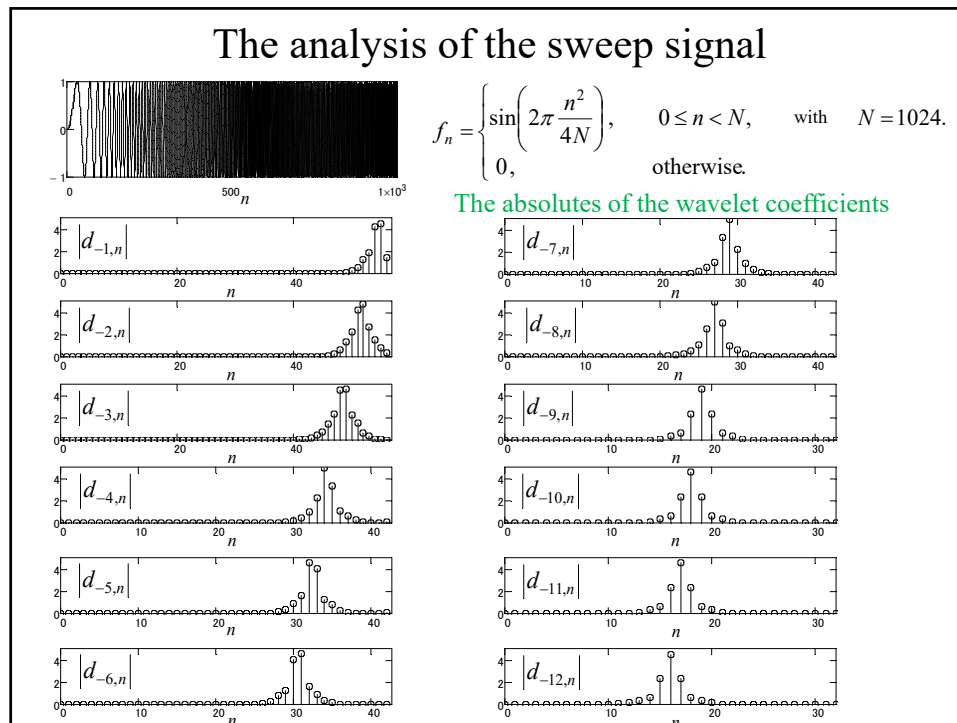
$$R_0 = 1, \quad \frac{R_1}{R_0} = \frac{17}{16}, \quad \frac{R_2}{R_1} = \frac{18}{17}, \quad \frac{R_3}{R_2} = \frac{19}{18}, \quad \frac{R_4}{R_3} = \frac{20}{19}, \quad \frac{R_5}{R_4} = \frac{16}{15},$$

$$\frac{R_6}{R_5} = \frac{17}{16}, \quad \frac{R_7}{R_6} = \frac{18}{17}, \quad \frac{R_8}{R_7} = \frac{19}{18}, \quad \frac{R_9}{R_8} = \frac{20}{19}, \quad \frac{R_{10}}{R_9} = \frac{16}{15}, \quad \frac{R_{11}}{R_{10}} = \frac{17}{16},$$

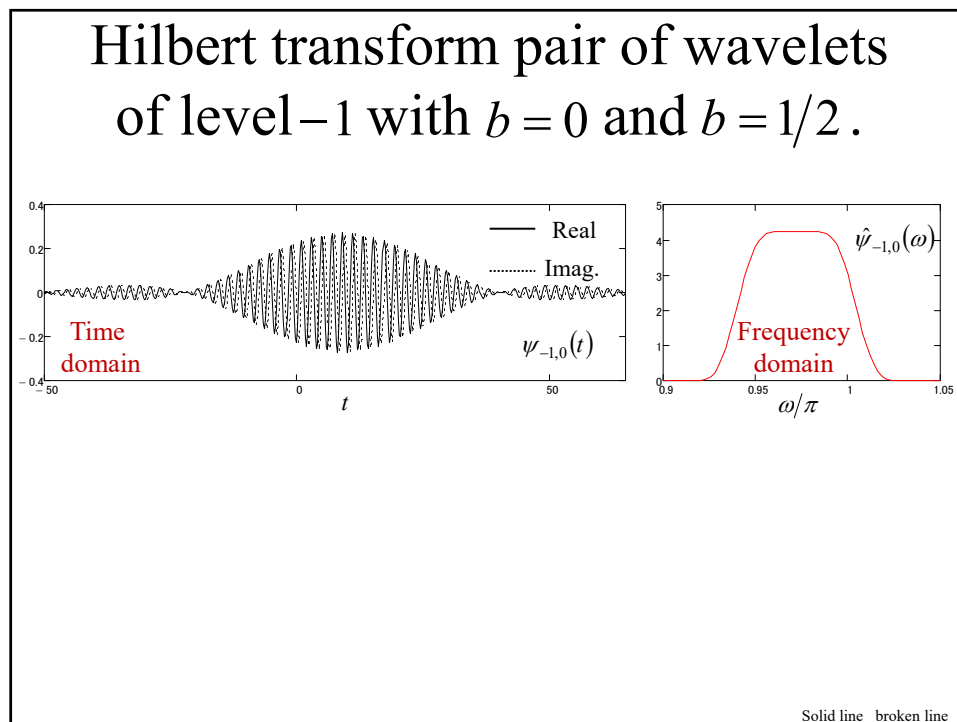
$$R_{12l+k} = 2^l R_k, \quad k = 0, 1, \dots, 11, \quad l \in \mathbf{Z}.$$

4

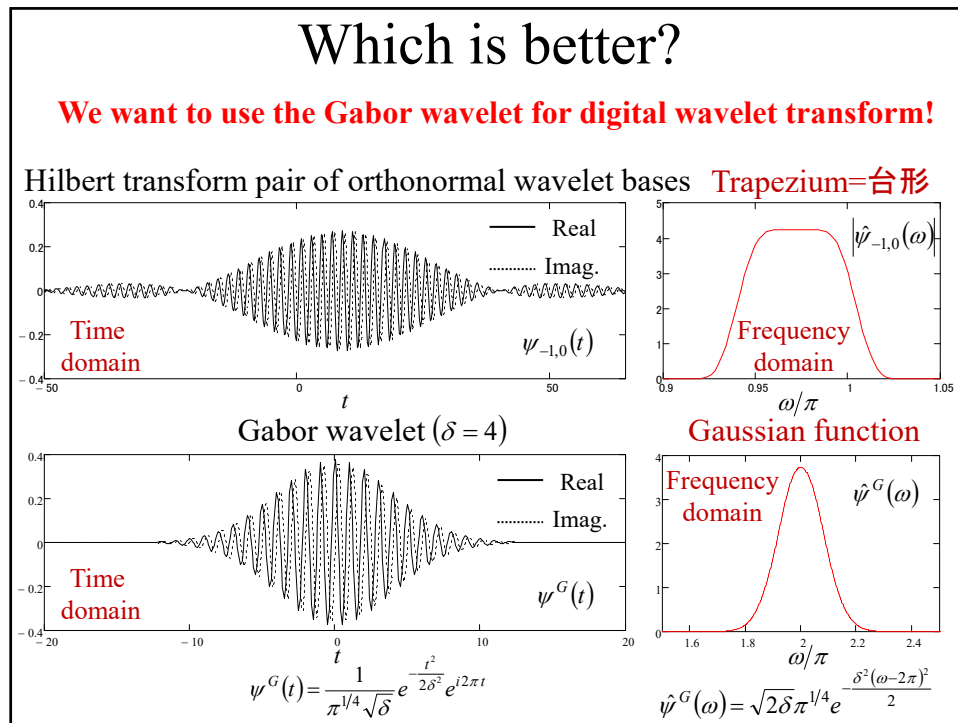
戸田浩, 章忠



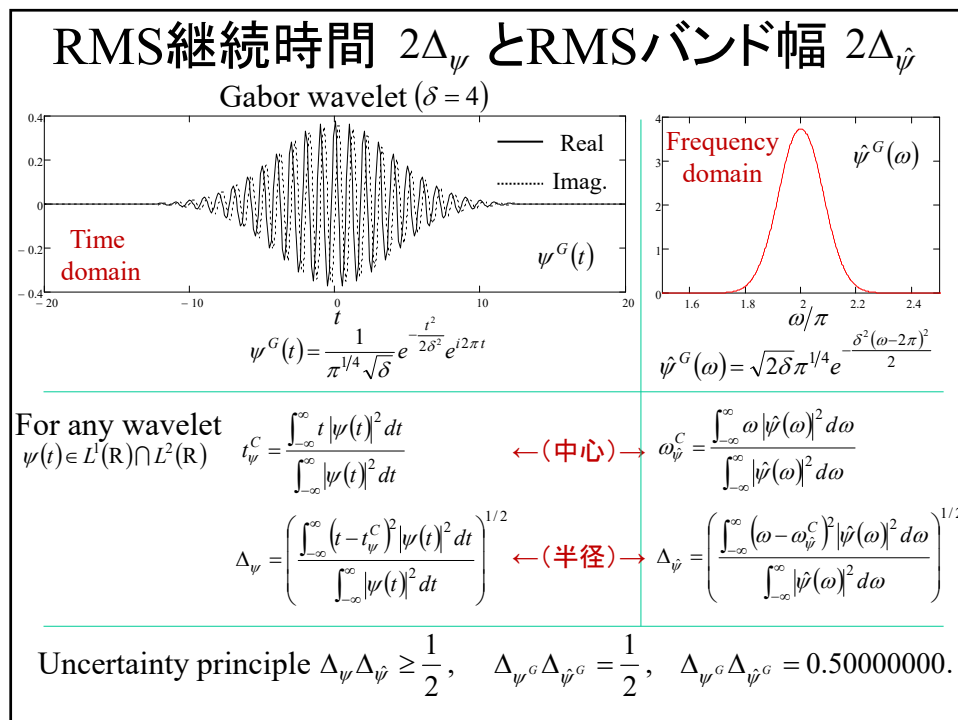
5



6

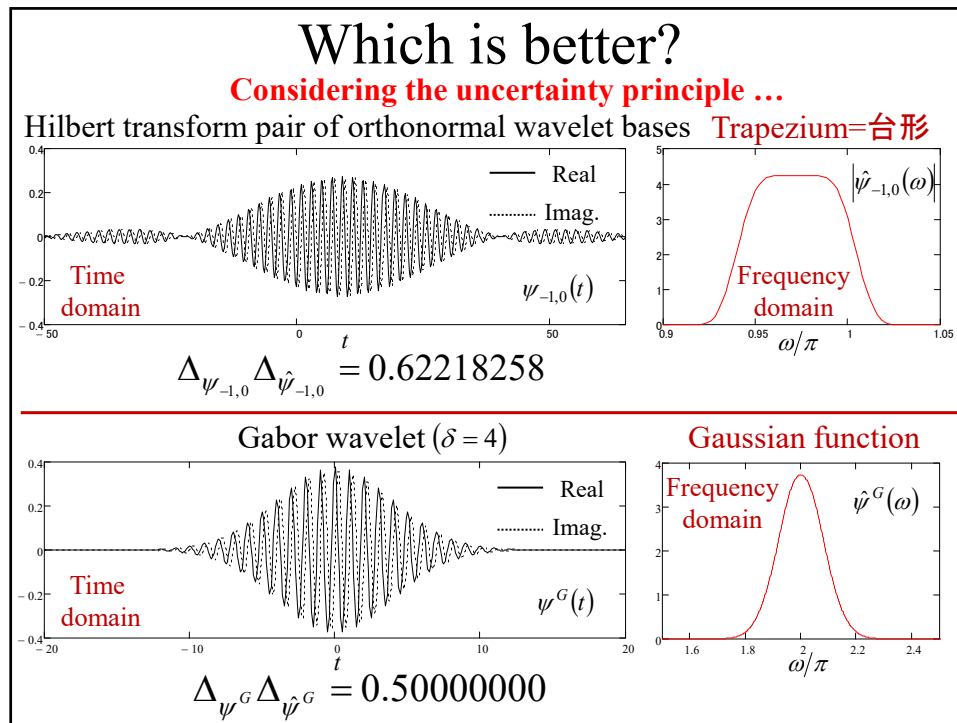


7

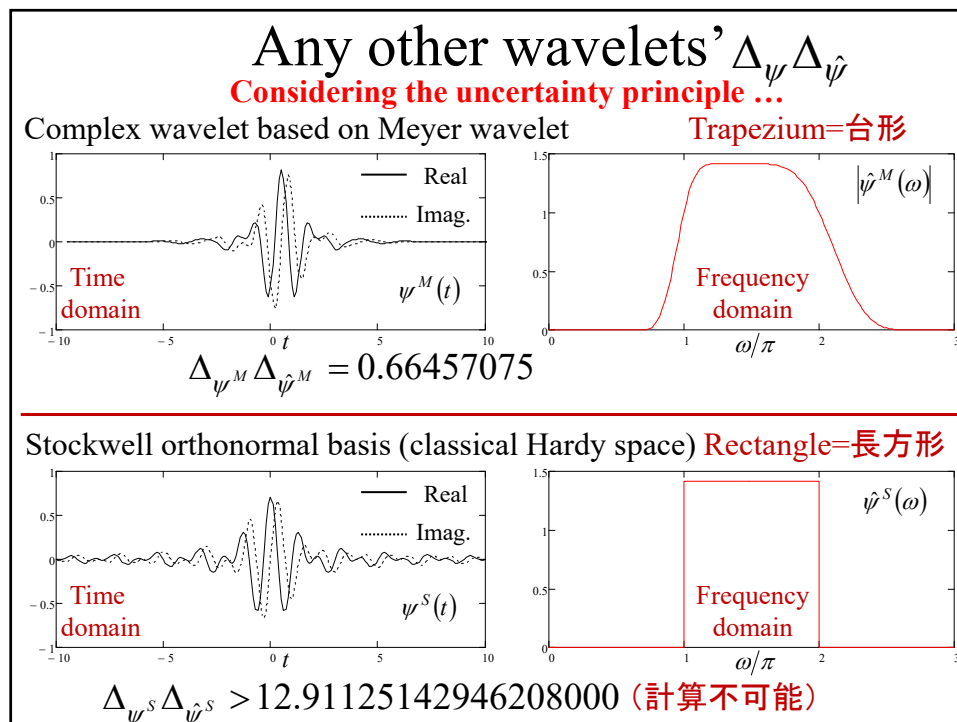


8

戸田浩, 章忠



9



10

We want to use the Gabor wavelet for digital transform!

For this aim, we propose the following method:

1. We design the original mother wavelet having free shape on the frequency domain.
2. Using the original mother wavelet, we construct an approximate tight wavelet frame.
3. Based on it, we construct a tight wavelet frame with minor modification.

11

The tight wavelet frame using an approximate Gabor wavelet

$$\begin{aligned}
 & f(t) \xrightarrow{\text{Transform}} \{d_{j,n}^P, d_{j,n}^N\} \xrightarrow{\text{Inv. transform}} \approx f(t) \\
 & d_{j,n}^P = \langle f, \psi_{j,n}^{\text{Orig}} \rangle, d_{j,n}^M = \langle f, \overline{\psi_{j,n}^{\text{Orig}}} \rangle \quad f(t) \approx \frac{1}{A^{\text{Orig}}} \left\{ \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} d_{j,n}^P \psi_{j,n}^{\text{Orig}}(t) + \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} d_{j,n}^N \overline{\psi_{j,n}^{\text{Orig}}}(t) \right\} \\
 & \quad \downarrow \quad \downarrow \\
 & \quad \boxed{\text{Remaking}} \\
 & \quad \psi^{\text{Rem}}(t) = \frac{\psi^{\text{Rem}'}(t)}{\|\psi^{\text{Rem}'}\|}, \\
 & \quad \hat{\psi}^{\text{Rem}'}(\omega) = \begin{cases} \sqrt{\frac{A^{\text{Orig}}}{\text{Orig}(\omega)}} \hat{\psi}^{\text{Orig}}(\omega), & \omega_0 < \omega < \omega_1, \\ 0 & \text{orhtewise.} \end{cases} \\
 & f(t) \xrightarrow{\text{Transform}} \{d_{j,n}^P, d_{j,n}^N\} \xrightarrow{\text{Inv. transform}} = f(t) \\
 & d_{j,n}^P = \langle f, \psi_{j,n}^{\text{Rem}} \rangle, d_{j,n}^N = \langle f, \overline{\psi_{j,n}^{\text{Rem}}} \rangle \quad f(t) = \frac{1}{A^{\text{Rem}}} \left\{ \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} d_{j,n}^P \psi_{j,n}^{\text{Rem}}(t) + \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} d_{j,n}^N \overline{\psi_{j,n}^{\text{Rem}}}(t) \right\} \\
 & \quad \downarrow \quad \downarrow \\
 & \boxed{f(t) = \frac{1}{A^{\text{Rem}}} \left\{ \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \psi_{j,n}^{\text{Rem}} \rangle \psi_{j,n}^{\text{Rem}}(t) + \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \overline{\psi_{j,n}^{\text{Rem}}} \rangle \overline{\psi_{j,n}^{\text{Rem}}}(t) \right\}, \quad A^{\text{Rem}} = \frac{A^{\text{Orig}}}{\|\psi^{\text{Rem}'}\|^2}.}
 \end{aligned}$$

12

戸田浩, 章忠

Theorem 1 for tight wavelet frames

The Fourier transform of $\psi(t) \in L^1(\mathbf{R}) \cap L^2(\mathbf{R})$

has a compact support of length Ω as follows:

$$0 < \sup_{\omega \in \mathbf{R}} |\hat{\psi}(\omega)| < \infty,$$

$$\text{supp } \hat{\psi}(\omega) \subseteq [\omega_0, \omega_1], \quad \omega_0 < \omega_1,$$

$$0 < \Omega = \omega_1 - \omega_0 < \infty.$$

$\{\psi_n(t) : n \in \mathbf{Z}\}$ is defined by

$$\{\psi_n(t) = \psi(t - pn) : n \in \mathbf{Z}\},$$

$$0 < p\Omega \leq 2\pi.$$

$p > 0$ is a constant real number.

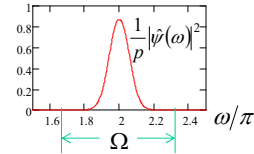
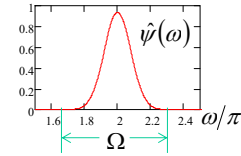
We define the following transform of $f(t) \in L^2(\mathbf{R})$.

$$(W^\psi f)(t) = \sum_{n \in \mathbf{Z}} \langle f, \psi_n \rangle \psi_n(t).$$

Then we have

$$W^\psi f \in L^2(\mathbf{R}),$$

$$F(W^\psi f)(\omega) = \frac{1}{p} |\hat{\psi}(\omega)|^2 \hat{f}(\omega).$$



13

The first step is the design of the original mother wavelet $\psi^{Orig}(t)$

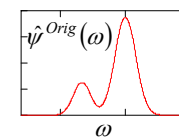
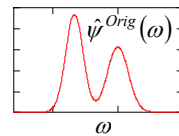
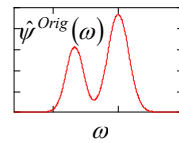
$$0 < \sup_{\omega \in \mathbf{R}} |\hat{\psi}^{Orig}(\omega)| < \infty$$

$$\|\psi^{Orig}\| = 1$$

$$|\hat{\psi}^{Orig}| \begin{cases} > 0, & \omega_0 < \omega < \omega_1, \\ = 0, & \text{otherwise,} \end{cases}$$

$$0 < \omega_0 < \omega_1 < \infty,$$

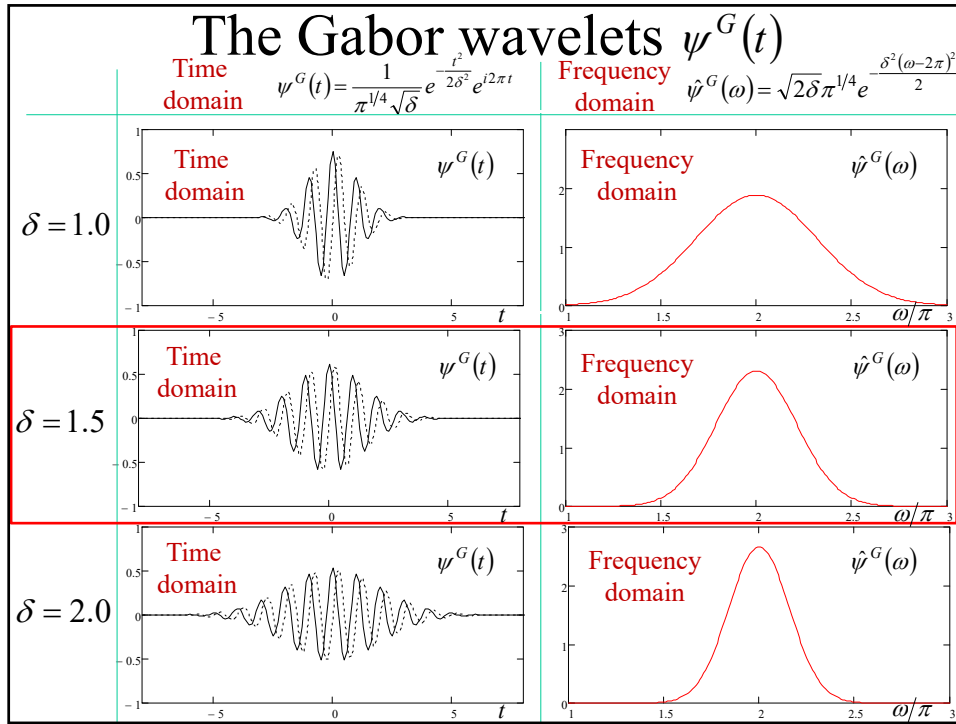
$$\Omega = \omega_1 - \omega_0 > 0.$$



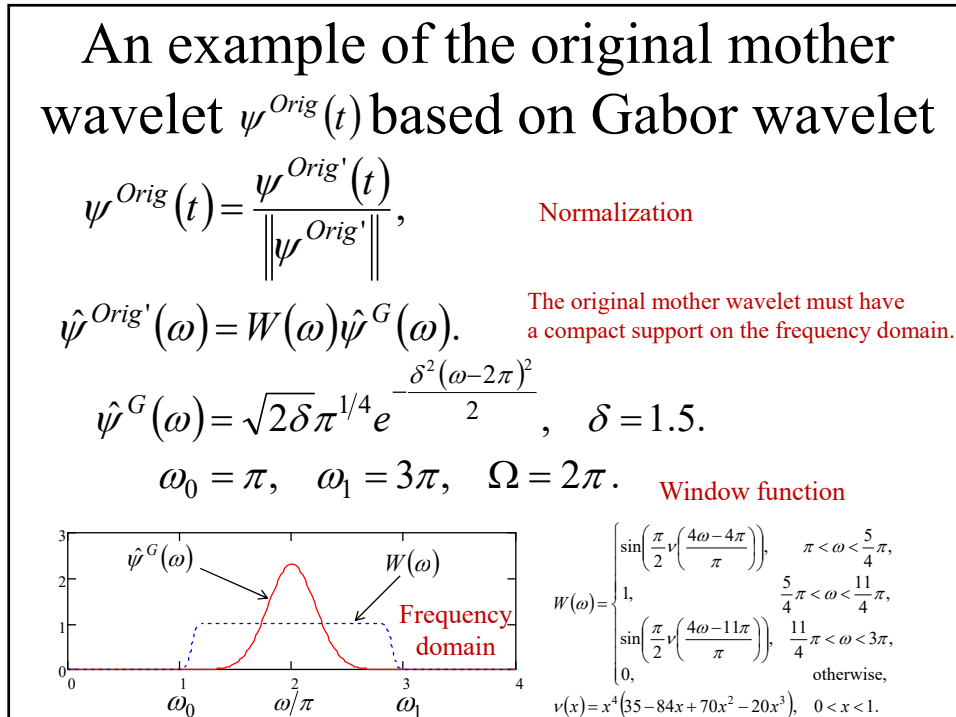
The original mother wavelet must be normalized and have a compact support on the frequency domain, but its shape is free!

We recommend the positive real function value, easy to treat

14



15



16

戸田浩, 章忠

The distance $p > 0$ between wavelets in level 0 and the dilation $a > 1$

$$0 < p\Omega \leq 2\pi,$$

$$1 < a \leq \frac{\omega_1}{\omega_0}.$$

Example of $p > 0$ and $a > 1$ based on Gabor wavelet can be set based on $\omega_0 = \pi$, $\omega_1 = 3\pi$, $\Omega = 2\pi$.

$$0 < p\Omega \leq 2\pi \quad \longrightarrow \quad p = 1,$$

$$1 < a \leq \frac{\omega_1}{\omega_0} \quad \longrightarrow \quad a = 2^{\frac{1}{4}}.$$

2 to the power of 1 quarter

17

The second step is the construction of an approximate tight wavelet frame

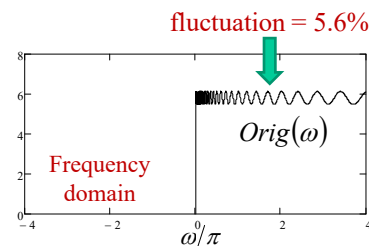
$$\psi_{j,n}^{Orig}(t) = \sqrt{a^j} \psi^{Orig}(a^j t - p n),$$

$$(W^{\psi^{Orig}} f)(t) = \sum_{j \in \mathbb{Z}} \sum_{n \in \mathbb{Z}} \langle f, \psi_{j,n}^{Orig} \rangle \psi_{j,n}^{Orig}(t).$$

Then we obtain

$$F(W^{\psi^{Orig}} f)(\omega) = \frac{1}{p} \sum_{j \in \mathbb{Z}} |\hat{\psi}^{Orig}(a^{-j} \omega)|^2 \hat{f}(\omega).$$

$$Orig(\omega) = \frac{1}{p} \sum_{j \in \mathbb{Z}} |\hat{\psi}^{Orig}(a^{-j} \omega)|^2.$$



18

The positive frequency domain is analyzed as

$$\psi_{j,n}^{Orig}(t) = \sqrt{a^j} \psi^{Orig}(a^j t - p n),$$

$$(W^{\psi^{Orig}} f)(t) = \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \psi_{j,n}^{Orig} \rangle \psi_{j,n}^{Orig}(t).$$

$$F(W^{\psi^{Orig}} f)(\omega) = Orig(\omega) \hat{f}(\omega).$$

In the same manner as above,
the negative frequency domain is analyzed as

$$(W^{\overline{\psi^{Orig}}} f)(t) = \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \overline{\psi_{j,n}^{Orig}} \rangle \overline{\psi_{j,n}^{Orig}}(t).$$

$$F(W^{\overline{\psi^{Orig}}} f)(\omega) = Orig(-\omega) \hat{f}(\omega).$$

Then we have

$$f(t) \approx \frac{1}{A^{Orig}} \left\{ \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \psi_{j,n}^{Orig} \rangle \psi_{j,n}^{Orig}(t) + \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \overline{\psi_{j,n}^{Orig}} \rangle \overline{\psi_{j,n}^{Orig}}(t) \right\},$$

$$A^{Orig} = \frac{1}{a\omega_0 - \omega_0} \int_{\omega_0}^{a\omega_0} Orig(\omega) d\omega.$$

The average of $Orig(\omega)$

19

The third step is the construction of a tight wavelet frame using a remaking mother wavelet

$$\psi^{Rem}(t) = \frac{\psi^{Rem'}(t)}{\|\psi^{Rem'}\|},$$

$$\hat{\psi}^{Rem'}(\omega) = \begin{cases} \sqrt{\frac{A^{Orig}}{Orig(\omega)}} \hat{\psi}^{Orig}(\omega), & \omega_0 < \omega < \omega_1, \\ 0 & \text{otherwise.} \end{cases}$$

$$Orig(\omega) = \frac{1}{p} \sum_{j \in \mathbf{Z}} |\hat{\psi}^{Orig}(a^{-j} \omega)|^2$$

fluctuation = 5.6%

$$Rem(\omega) = \frac{1}{p} \sum_{j \in \mathbf{Z}} |\hat{\psi}^{Rem}(a^{-j} \omega)|^2$$

fluctuation = 0%

20

戸田浩, 章忠

The third step is the construction of a tight wavelet frame using a remaking mother wavelet

$$\psi^{Rem}(t) = \frac{\psi^{Rem'}(t)}{\|\psi^{Rem'}\|},$$

$$\hat{\psi}^{Rem'}(\omega) = \begin{cases} \sqrt{\frac{A^{Orig}}{Orig(\omega)}} \hat{\psi}^{Orig}(\omega), & \omega_0 < \omega < \omega_1, \\ 0 & \text{otherwise.} \end{cases}$$

$$\psi_{j,n}^{Rem}(t) = \sqrt{a^j} \psi^{Rem}(a^j t - p n).$$

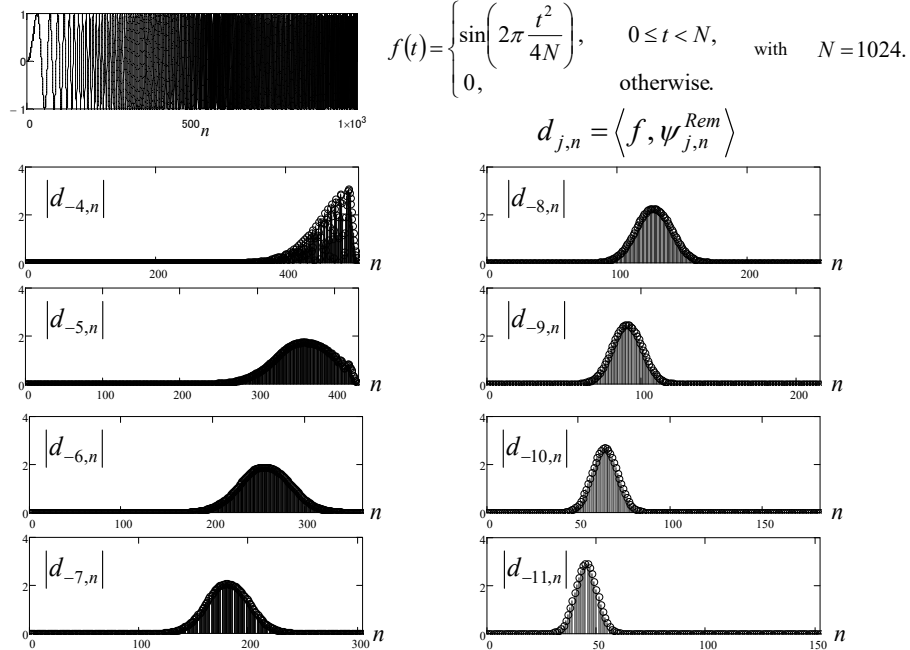
$\{\psi_{j,n}^{Rem}(t), \overline{\psi_{j,n}^{Rem}(t)} : j, n \in \mathbf{Z}\}$ constructs a tight wavelet frame as follows:

$$f(t) = \frac{1}{A^{Rem}} \left\{ \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \psi_{j,n}^{Rem} \rangle \psi_{j,n}^{Rem}(t) + \sum_{j \in \mathbf{Z}} \sum_{n \in \mathbf{Z}} \langle f, \overline{\psi_{j,n}^{Rem}} \rangle \overline{\psi_{j,n}^{Rem}(t)} \right\},$$

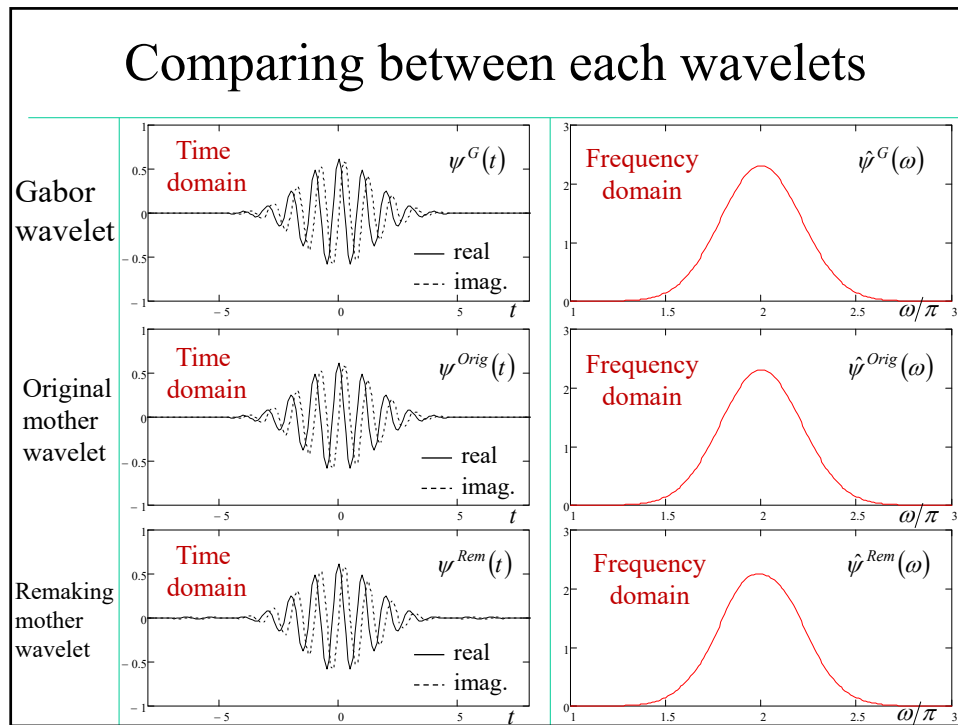
$$A^{Rem} = \frac{A^{Orig}}{\|\psi^{Rem'}\|^2}.$$

21

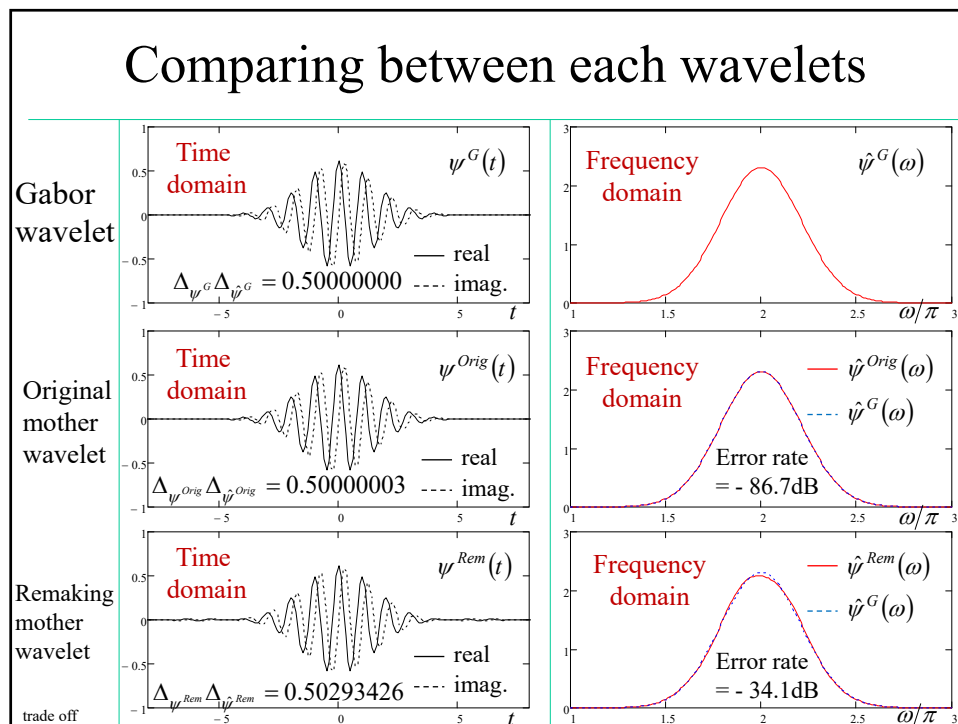
The analysis of the sweep signal



22

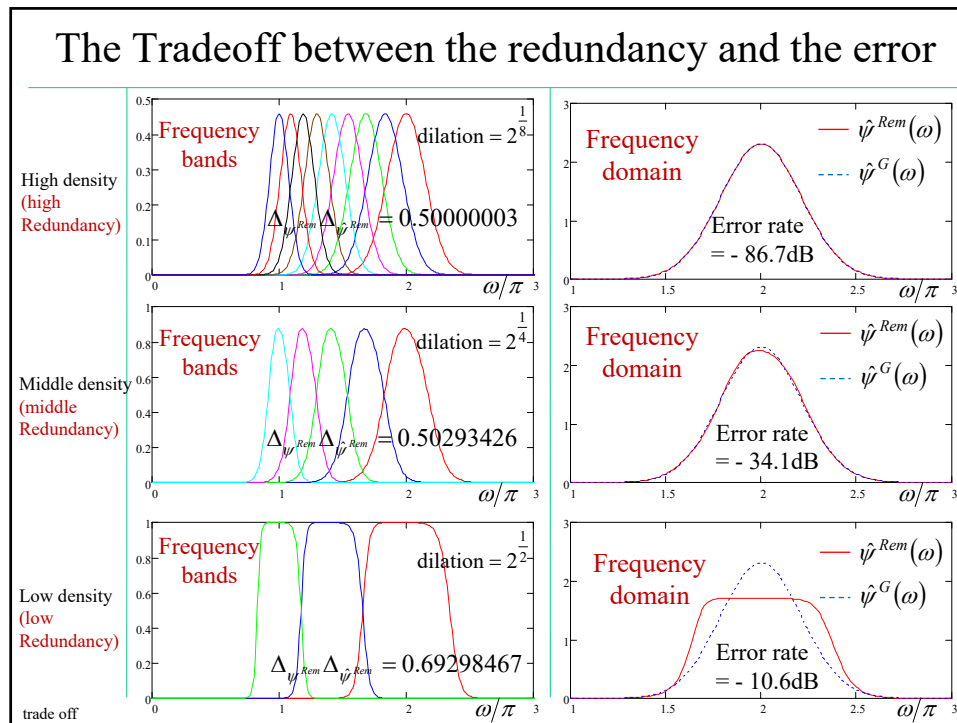


23

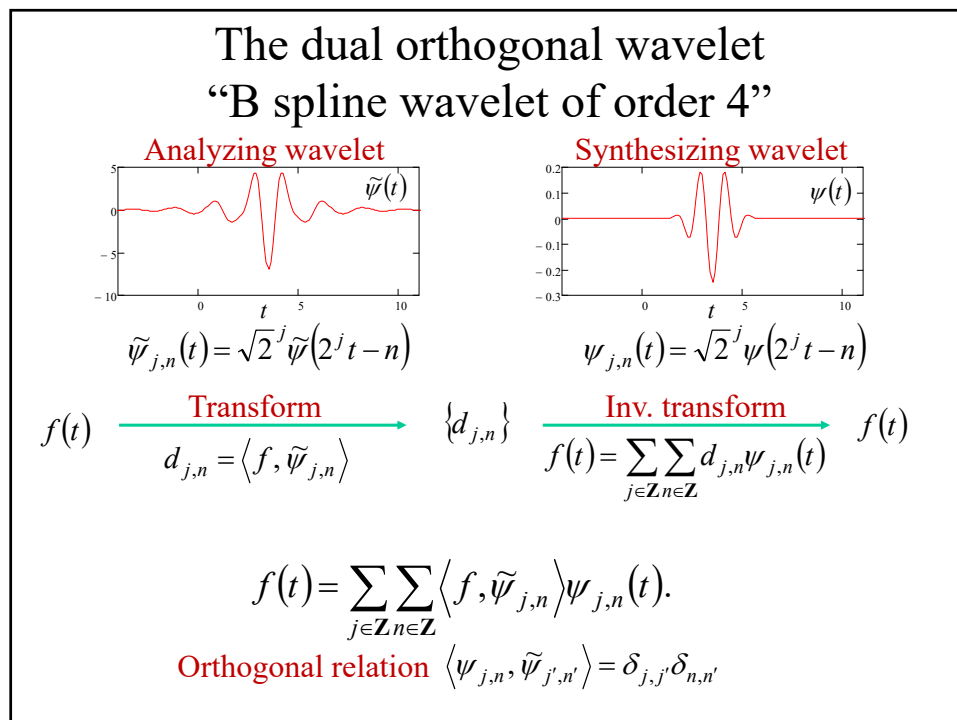


24

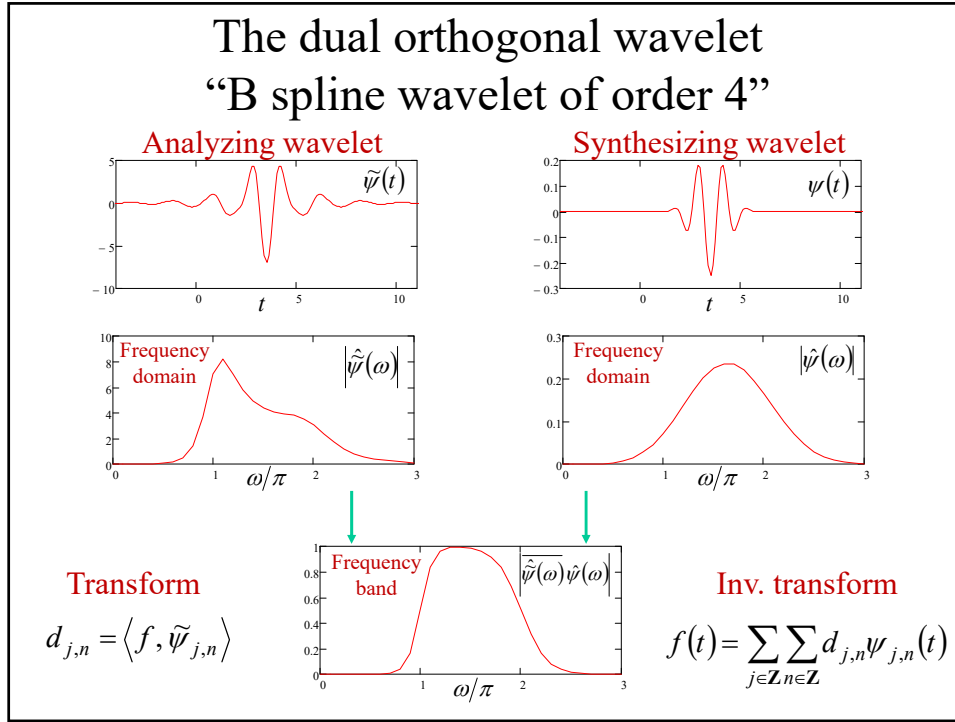
戸田浩, 章忠



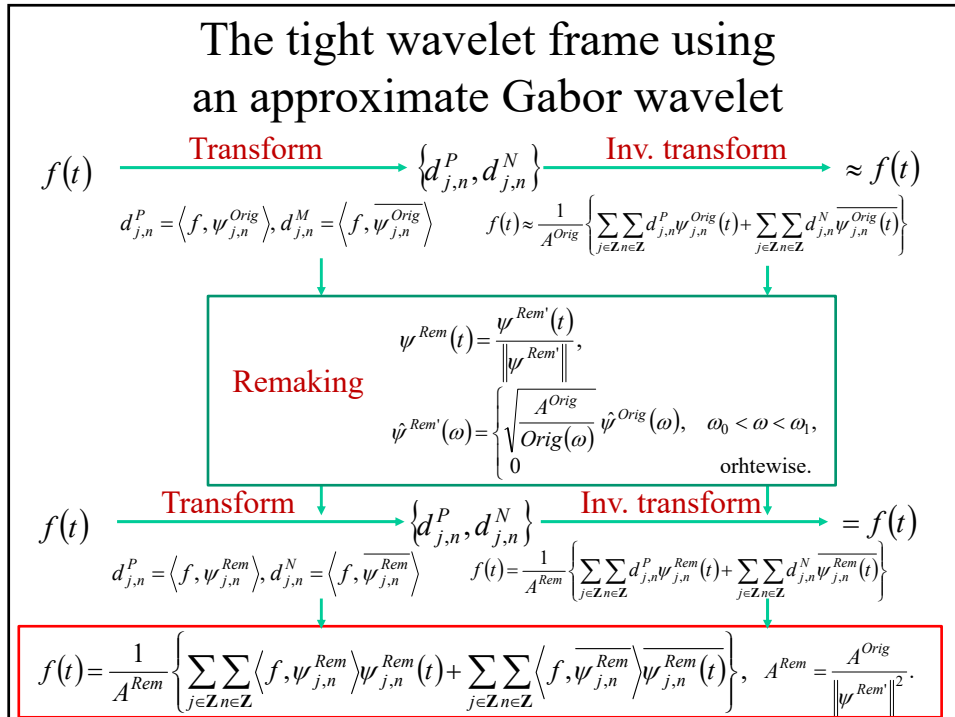
25



26

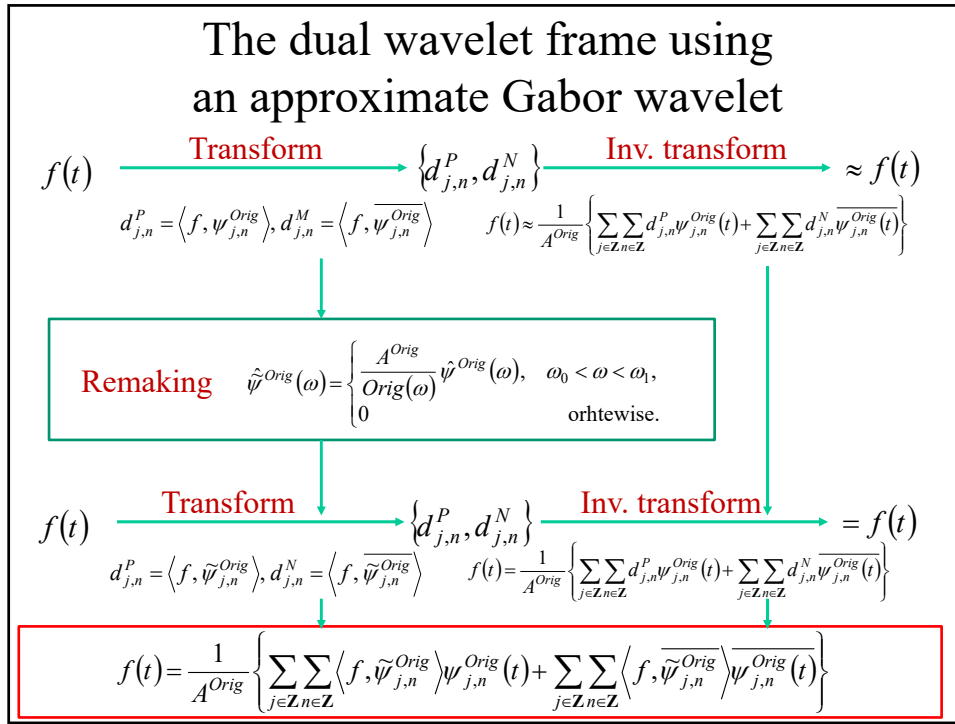


27



28

戸田浩, 章忠



29

Theorem 1 for tight wavelet frames

The Fourier transform of $\psi(t) \in L^1(\mathbf{R}) \cap L^2(\mathbf{R})$ has a compact support of length Ω as follows:

$$0 < \sup_{\omega \in \mathbf{R}} |\hat{\psi}(\omega)| < \infty,$$

$$\text{supp } \hat{\psi}(\omega) \subseteq [\omega_0, \omega_1], \quad \omega_0 < \omega_1,$$

$$0 < \Omega = \omega_1 - \omega_0 < \infty.$$

$\{\psi_n(t) : n \in \mathbf{Z}\}$ is defined by

$$\{\psi_n(t) = \psi(t - p n) : n \in \mathbf{Z}\},$$

$$0 < p \Omega \leq 2\pi.$$

$p > 0$ is a constant real number.

We define the following transform of $f(t) \in L^2(\mathbf{R})$.

$$(W^\psi f)(t) = \sum_{n \in \mathbf{Z}} \langle f, \psi_n \rangle \psi_n(t).$$

Then we have

$$W^\psi f = L^2(\mathbf{R}),$$

$$F(W^\psi f)(\omega) = \frac{1}{p} |\hat{\psi}(\omega)|^2 \hat{f}(\omega).$$

30

Theorem 2 for dual wavelet frames

The Fourier transform of $\tilde{\psi}(t) \in L^1(\mathbf{R}) \cap L^2(\mathbf{R})$ and $\psi(t) \in L^1(\mathbf{R}) \cap L^2(\mathbf{R})$ have a compact support of length Ω as follows:

$$\begin{aligned} 0 < \sup_{\omega \in \mathbf{R}} |\hat{\tilde{\psi}}(\omega)| < \infty, & \quad 0 < \sup_{\omega \in \mathbf{R}} |\hat{\psi}(\omega)| < \infty, \\ \text{supp } \hat{\tilde{\psi}}(\omega) \subseteq [\omega_0, \omega_1], & \quad \text{supp } \hat{\psi}(\omega) \subseteq [\omega_0, \omega_1], \quad \omega_0 < \omega_1, \\ 0 < \Omega = \omega_1 - \omega_0 < \infty. \end{aligned}$$

$$\begin{aligned} \{\tilde{\psi}_n(t) : n \in \mathbf{Z}\}, \quad \{\psi_n(t) : n \in \mathbf{Z}\} \text{ are defined by} \\ \{\tilde{\psi}_n(t) = \tilde{\psi}(t - pn) : n \in \mathbf{Z}\}, \quad \{\psi_n(t) = \psi(t - pn) : n \in \mathbf{Z}\}, \\ 0 < p\Omega \leq 2\pi. \end{aligned}$$

$p > 0$ is a constant real number.

We define the following transform of $f(t) \in L^2(\mathbf{R})$.

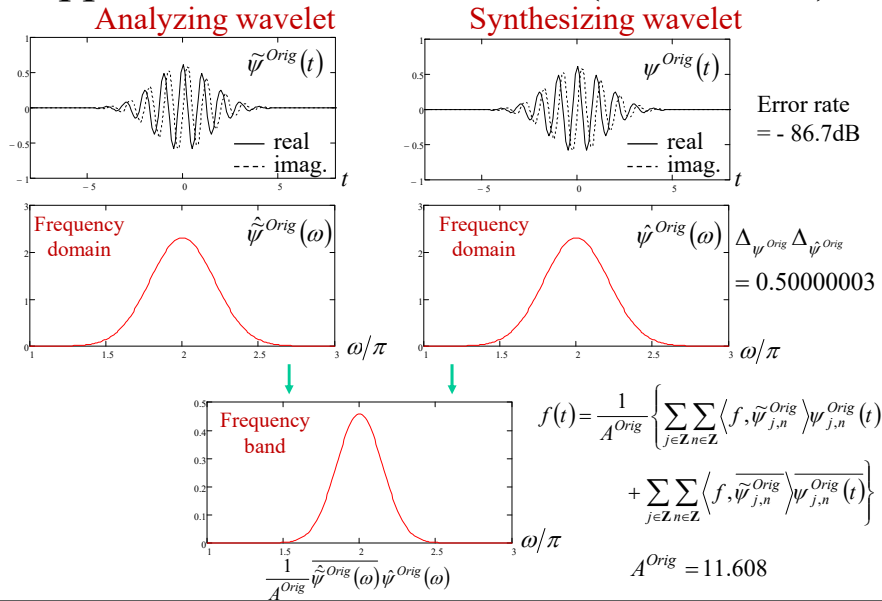
$$(W^{\tilde{\psi}, \psi} f)(t) = \sum_{n \in \mathbf{Z}} \langle f, \tilde{\psi}_n \rangle \psi_n(t).$$

Then we have

$$\begin{aligned} W^{\tilde{\psi}, \psi} f &= L^2(\mathbf{R}), \\ F(W^{\tilde{\psi}, \psi} f)(\omega) &= \frac{1}{p} \frac{\hat{\tilde{\psi}}(\omega)}{\hat{\psi}(\omega)} \hat{f}(\omega). \end{aligned}$$

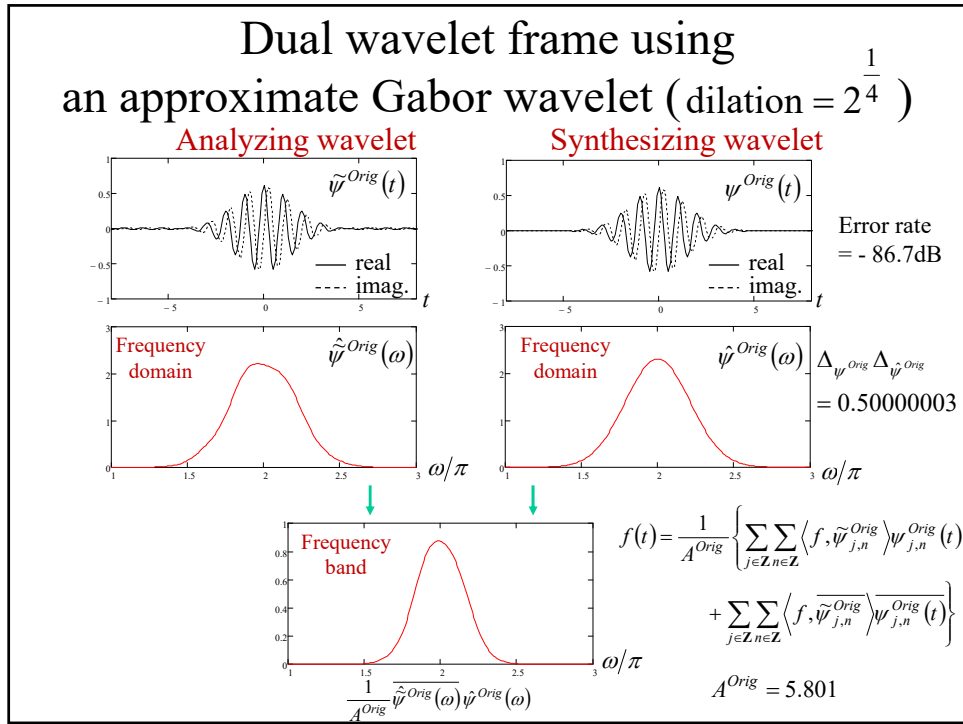
31

Dual wavelet frame using an approximate Gabor wavelet (dilation = $2^{\frac{1}{8}}$)

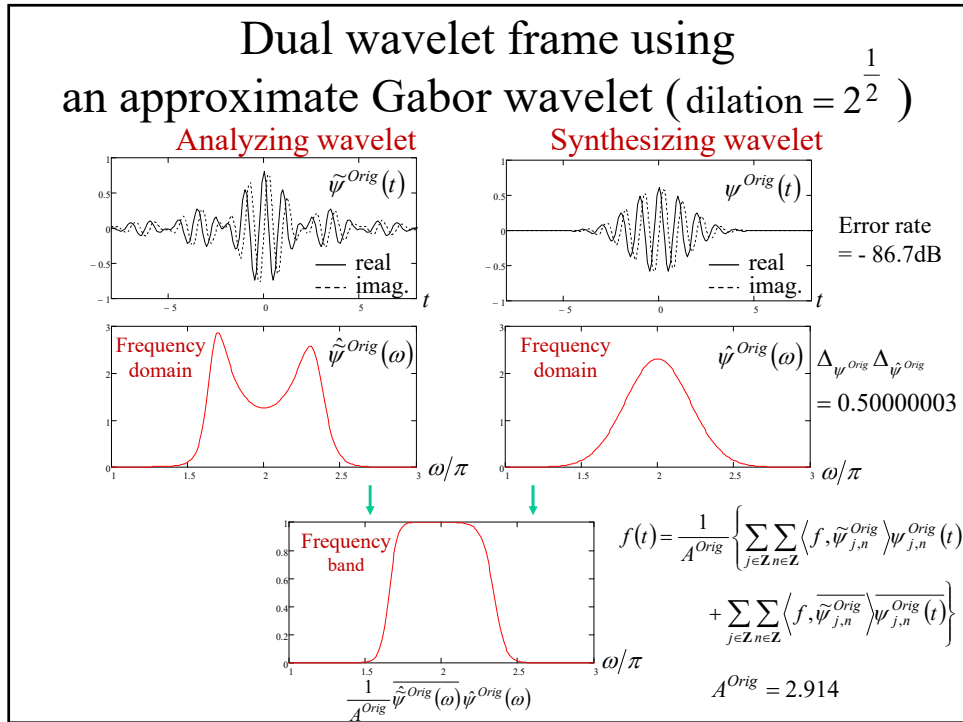


32

戸田浩, 章忠

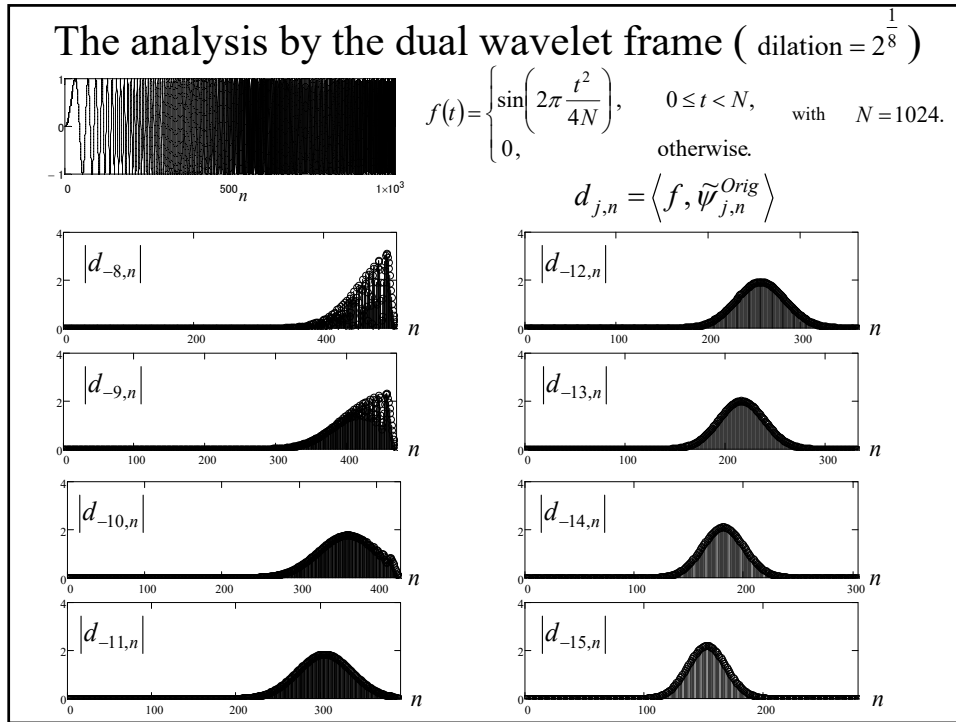


33

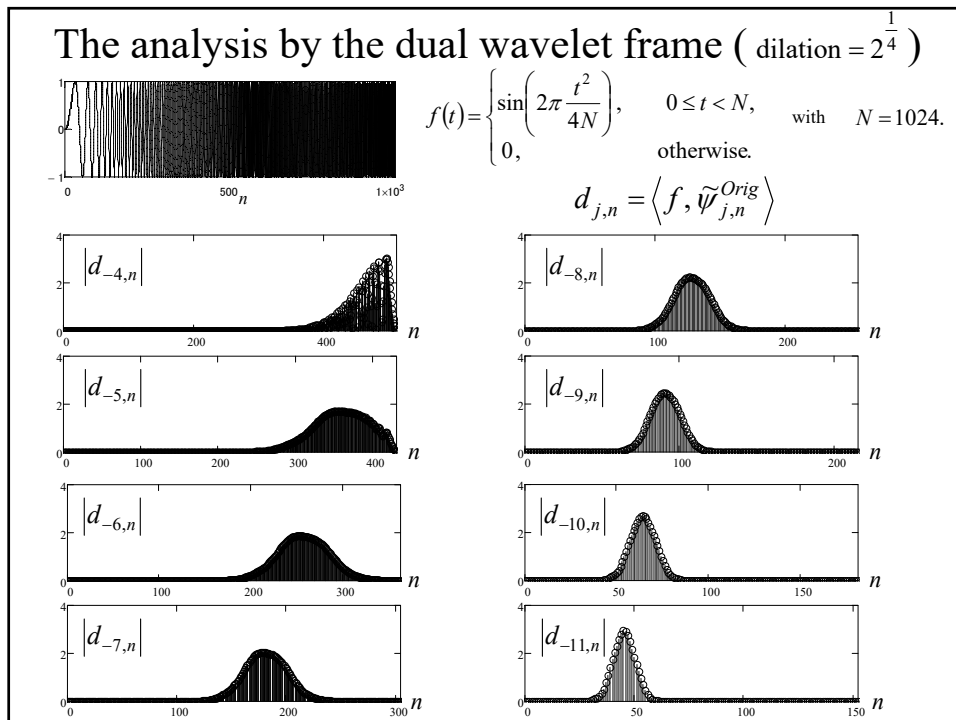


34

戸田浩, 章忠

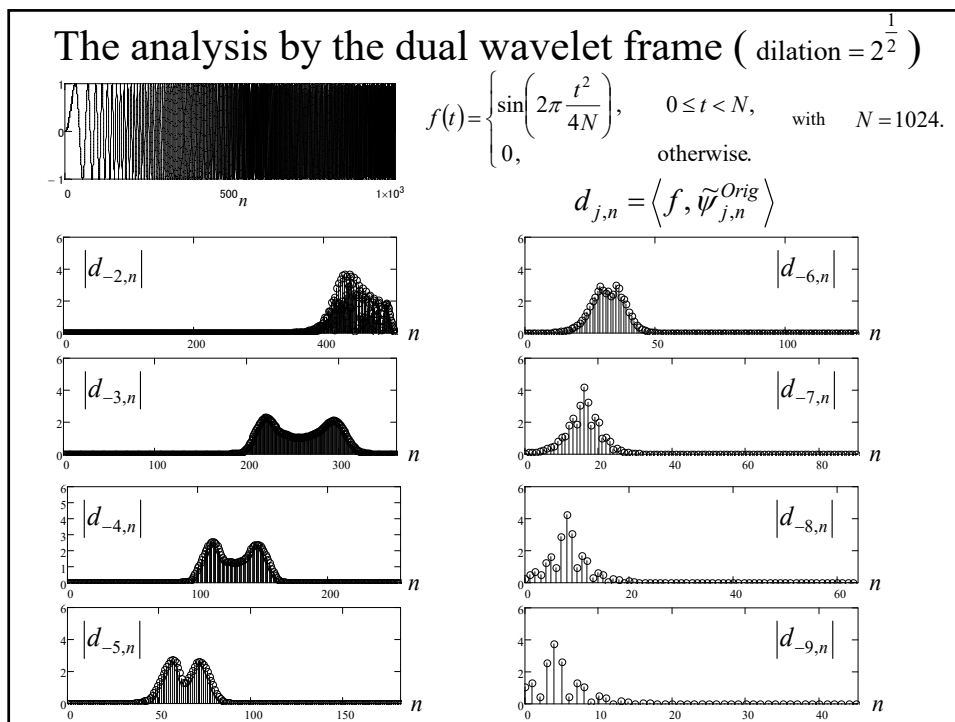


35

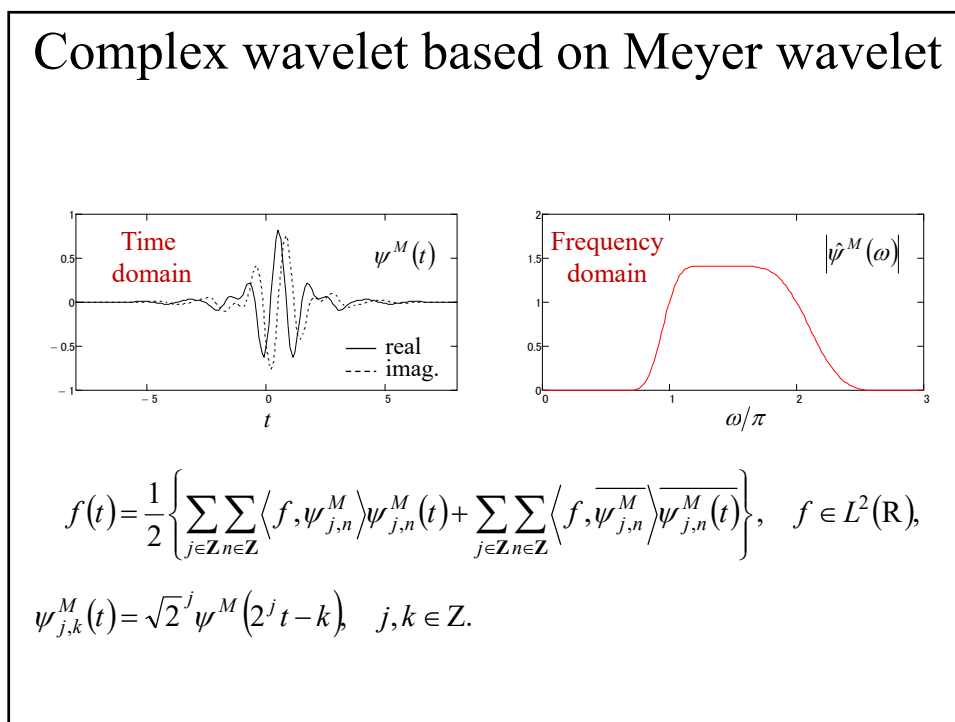


36

戸田浩, 章忠

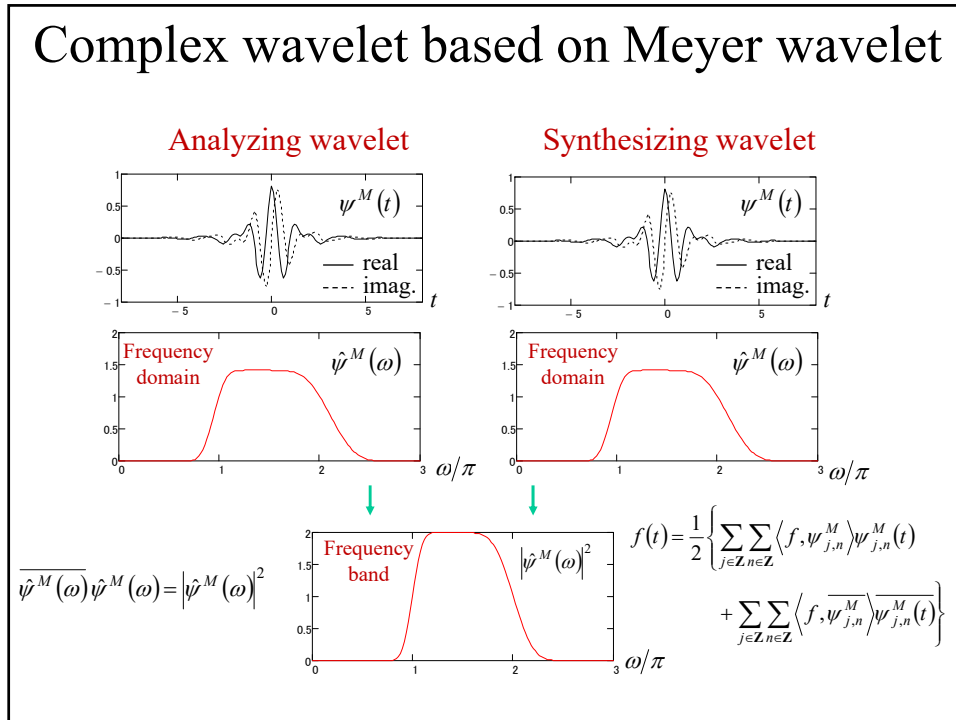


37

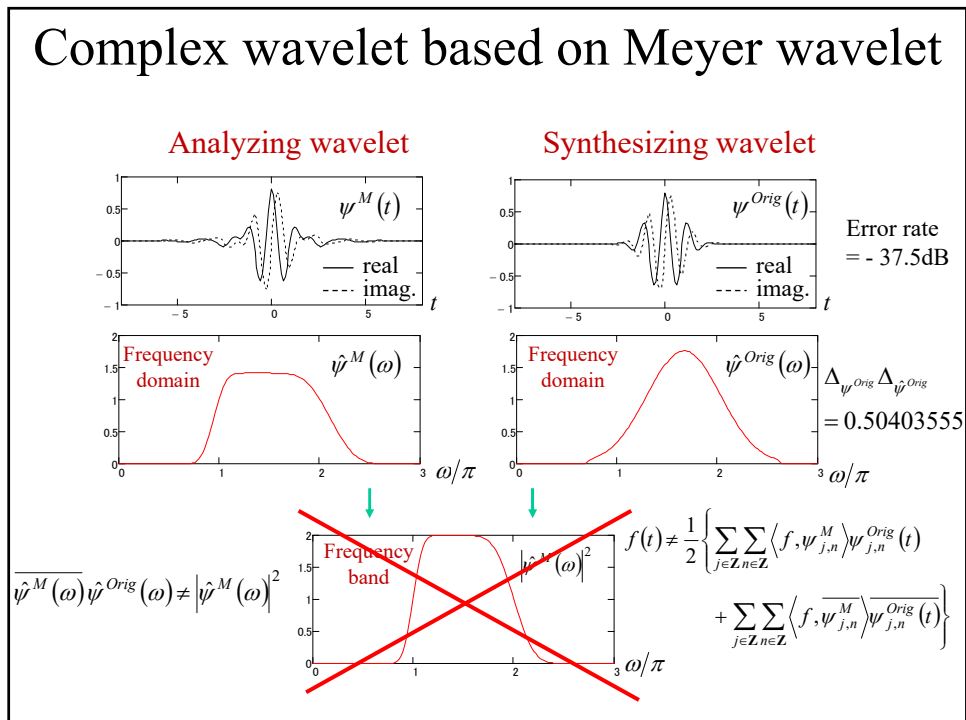


38

戸田浩, 章忠

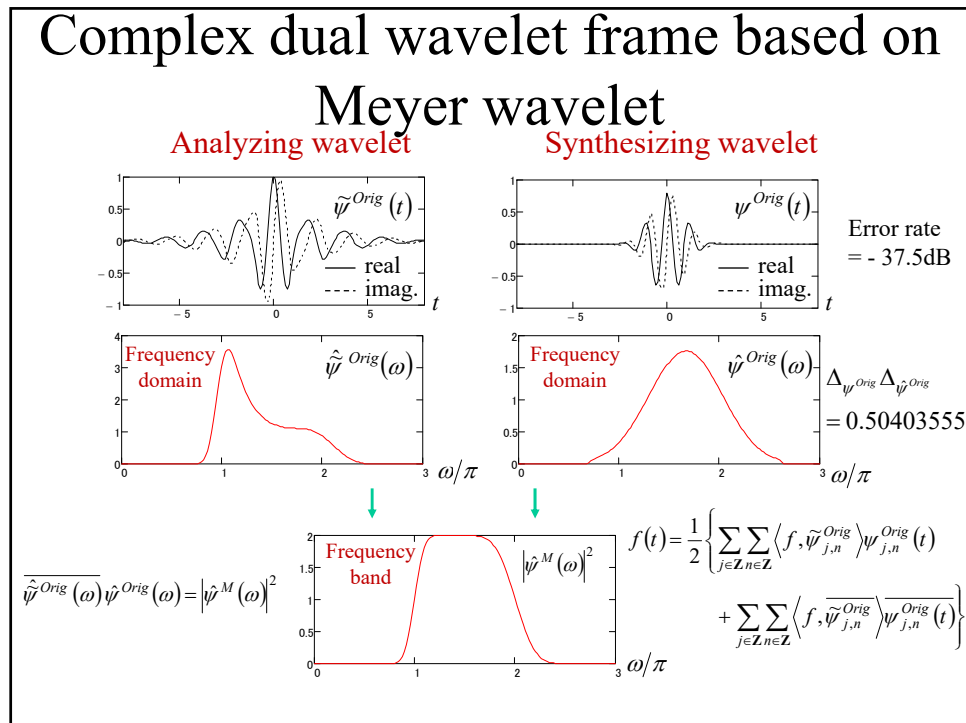


39

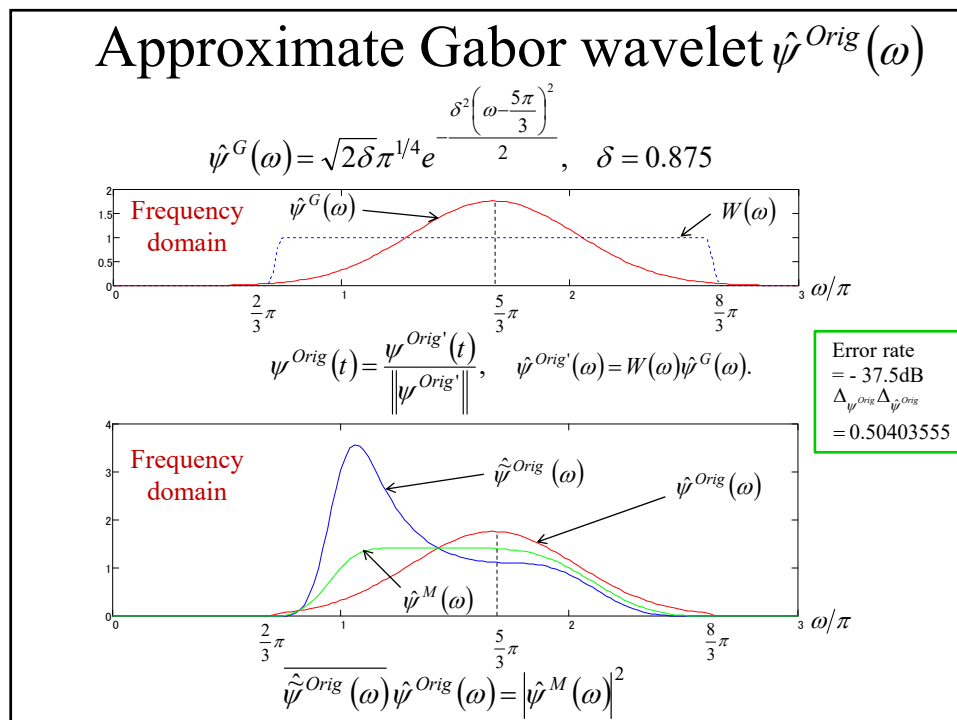


40

戸田浩, 章忠

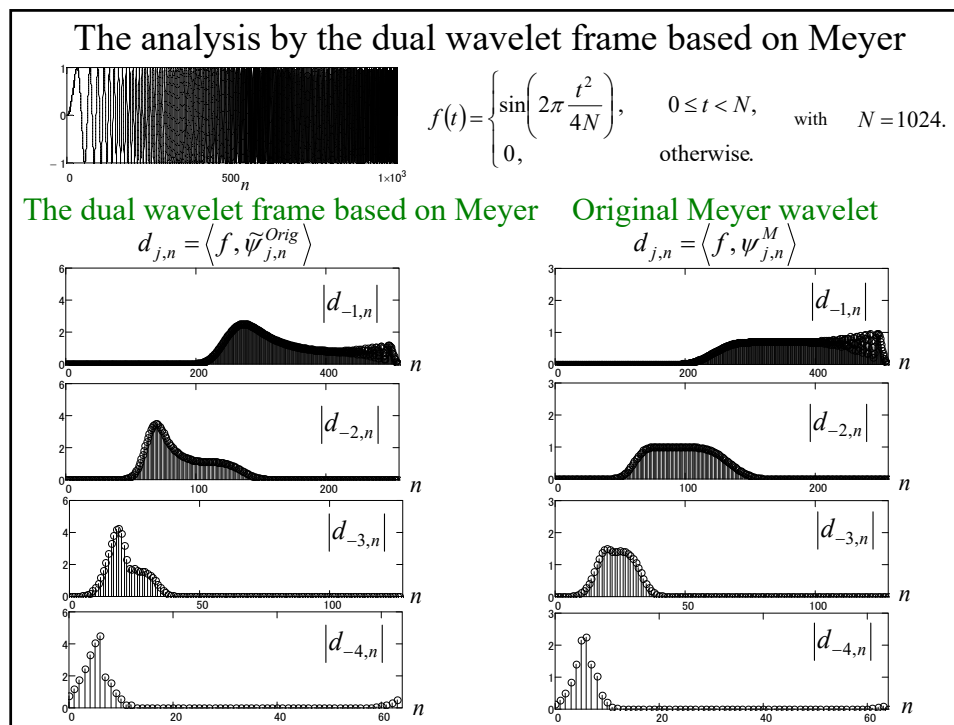


41



42

戸田浩, 章忠



43

Conclusion

1. We introduced our proposed Hilbert transform pairs of orthonormal bases of chromatic-scale wavelets.
2. We introduced the Gabor wavelets.
3. We introduced the tight wavelet frame using complex wavelet designed in free shape on frequency domain.
4. We constructed the tight wavelet frame using an approximate Gabor wavelet.
5. We constructed the dual wavelet frame using an approximate Gabor wavelet.

44

井川信子, 守本晃, 芦野隆一

聴性定常反応と ウェーブレット解析について

○井川 信子 (流通経済大学),
守本 晃 (大阪教育大学),
芦野 隆一 (大阪教育大学)

2019/12/5

AIMap2019大阪教育大学(N. Ikawa)

1

1

本発表の概要

自作計測機器により SAM 音刺激を与えて得られた聴力正常成人の聴性誘発脳波データから聴性定常反応成分を抽出する際, その反応波形の特性に応じてどのようにウェーブレット解析を用いるかについて提案し, その工学的応用の有効性について議論する.

2019/12/5

AIMap2019大阪教育大学(N. Ikawa)

2

2

本発表のアウトライン

➤ 他覚的聴力検査と聴性誘発脳波

聴性定常反応(Auditory Steady State Response : ASSR)について

➤ 波形にウェーブレット解析を実施:

- ・複素連続ウェーブレット解析(Complex Continuous Wavelet Analysis : CCWA)
- ・離散定常ウェーブレット解析(Discrete Stationary Wavelet Analysis : SWA)

2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

3

3

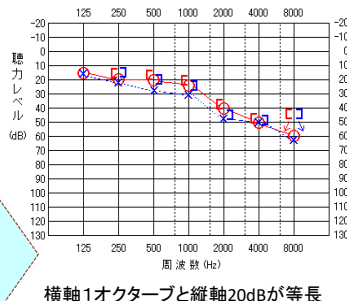
自覚的聴力検査 引: <http://www.shrc.or.jp/kensa/o.html>

純音聴力検査:

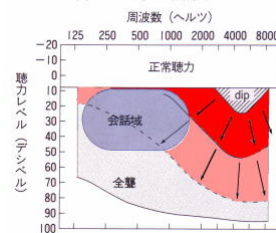
オーディオメータ(JIS T 1201)

被検者に、電氣的に発生した検査音を減衰器を通して与え、被検者自身の認知、応答によって聴覚機能を検査する装置→オーディオグラム(周波数の関数として聴力レベルを示したグラフ)を描く

老人性難聴の純音オーディオグラムの例



●騒音性難聴や老人性難聴は高音域(4,000ヘルツ)から始まる



2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

4

4

他覚的聴力検査

- 新生児, 乳幼児, 精神発達遅滞, 機能性難聴, 詐聴など純音聴力検査が施行できない症例において聴力レベルを推定するための検査法であり, 聴性誘発反応, 耳音響放射, アブミ骨筋反射などがある.
- 聴性誘発反応による臨床検査法は主に聴性脳幹反応(Auditory Brainstem Response : ABR)による. さらに, 各周波数の聴力レベルをより正確に推定できるとされることから
- **聴性定常反応 (auditory steady-state response : ASSR)** が用いられる.

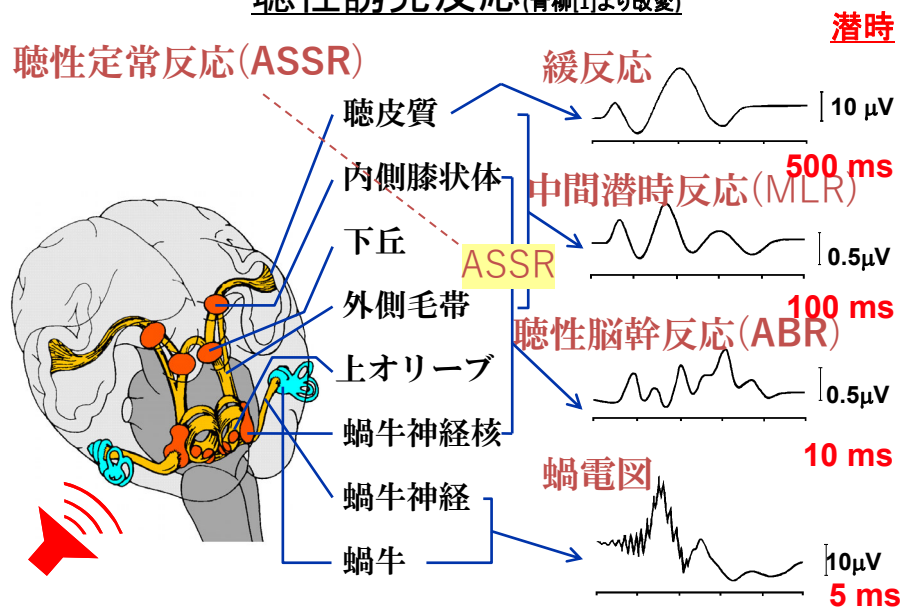
2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

5

5

聴性誘発反応(青柳[1]より改変)

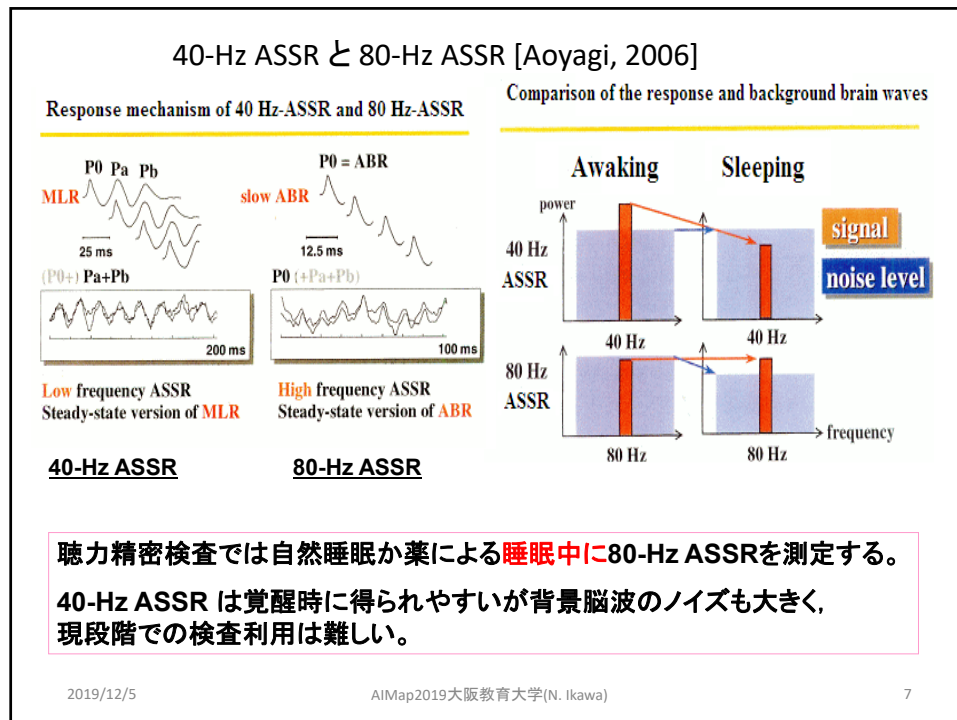


2019/12/5

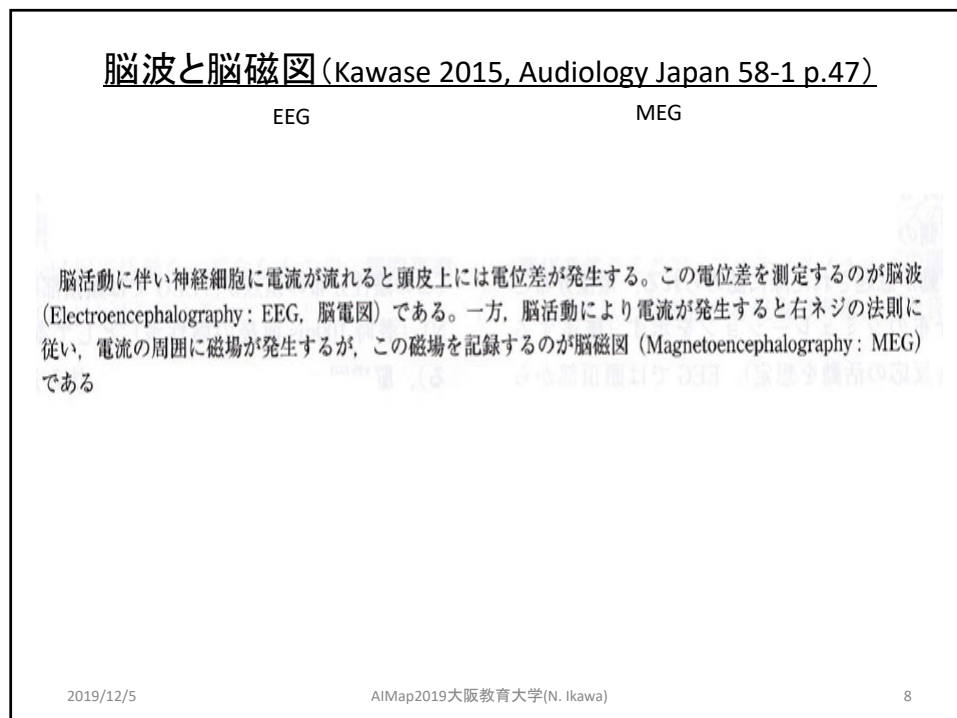
AIMaP2019大阪教育大学(N. Ikawa)

6

6



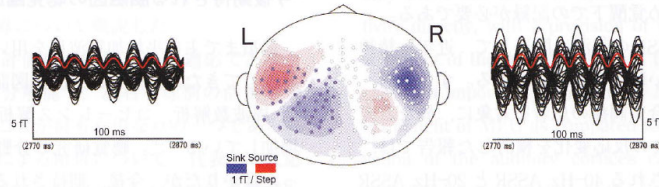
7



8

脳磁図による40-Hz ASSR (Kawase 2015, Audiology Japan 58-1 p.47)

A. 40-Hz ASSR (重ね合わせ波形と等磁場図)



B. 等価電流双極子の方向、大きさの変化 (40-Hz ASSR (1周期))

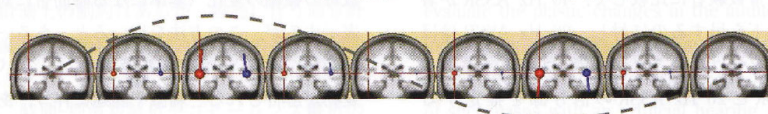


図5 脳磁図で記録される 40-Hz ASSR

右耳に 39-Hz AM 音 (搬送周波数 1000Hz) を 80dB SPL で提示した際に記録された脳磁図 40-Hz ASSR。A: ある時刻における等磁界図(中央), 並びに重ね合わせ波形(左: 左半球, 右: 右半球)。右半球でより振幅の大きな ASSR が記録されている。B: 等価電流双極子の方向, 大きさの変化 (1 周期分)。40-Hz ASSR は電流の向きが, 40-Hz の周期で変化する聴覚野の活動を記録しているものであることがわかる。

2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

9

9

聴覚スクリーニング検査と精密検査

- **自動ABR(Automated Auditory Brainstem Response : AABR)**は新生児聴カスクリーニングとして広く利用されている(装置):
 - ALGO 伝統的に利用されている
 - **MB11ベラフォン** 最近注目されている
- **スクリーニング**検査後,難聴等が疑われると,『**要精密検査**』(約1人/1,000人, 日本聴覚医学会)を実施する(ASSRを用いる装置):
 - **MASTER** 広く利用されてきた
 - **エクリプス** 最近注目されている

2019/12/5

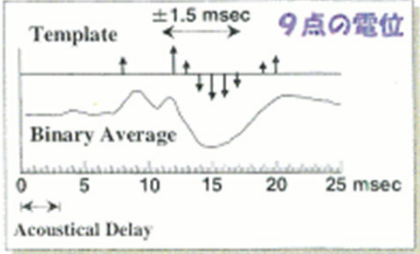
AIMaP2019大阪教育大学(N. Ikawa)

10

10

新生児聴覚スクリーニング

音圧 = 35 dB, 70 dB

自動ABR
Automated ABR (AABR)
(Natus ALGO®)

波形検出のアルゴリズム
Weighted-Binary Template
Matching Algorithm

(Herrmann BSの文献より)

出典: 青柳[1]
p.3No.3

2019/12/5AIMaP2019大阪教育大学(N. Ikawa)11

11

BA11ベラフォンによるスクリーニング検査

- 新生児聴覚スクリーニング検査のための機器は、より正確に、短時間に計測できるようになりだいたい進歩した。

例: MB11ベラフォンMB11 BERAphone®

<https://youtu.be/Kgx7A56dCjY?t=49>



2019/12/5AIMaP2019大阪教育大学(N. Ikawa)12

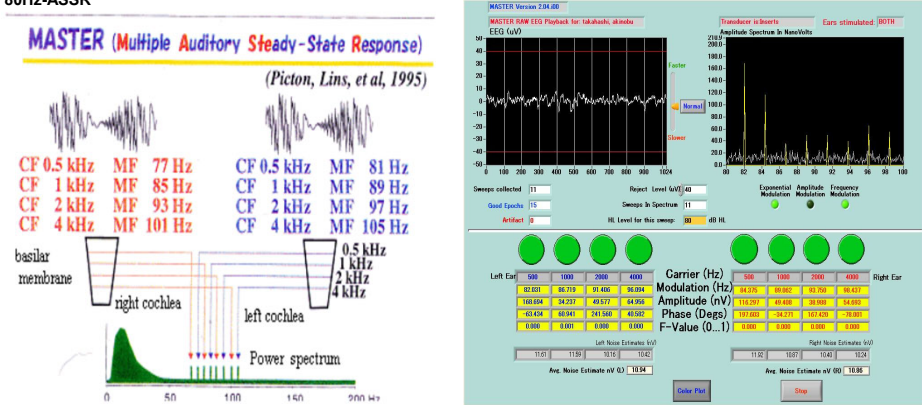
12

井川信子, 守本晃, 芦野隆一

MASTERによる測定

MASTER: Multiple Auditory STEady-State Response(Picton, Lins, et al, 1995) ,
<http://www.mastersystem.ca/> (Aoyagi[1]) An example of MASTER output window:

80Hz-ASSR



In the case of 80-Hz ASSR, MASTER system uses both relationship between the carrier frequency of input stimuli and the modulation frequency of cochlea responses.

- 70 dB : 512 epochs -> 32 sweeps
 - 60 dB : 474 epochs -> 29 sweeps
 - 80 dB : 184 epochs -> 11 sweeps
 (1 sweep = 16 epochs)

2019/12/5 AIMaP2019大阪教育大学(N. Ikawa) 13

13

さらに進んで Eclipse エクリプス(インターアコースティクス社(デンマーク)製)

Diatec HPより <https://www.diatec-diagnostics.jp/solutions/products/abr/interacoustics-eclipse-complete-solution#>

PCベース型で精密検査や臨床研究用の聴性誘発反応検査装置。ABR, ASSR, OAE, VEMP, 自動ABR検査モジュールを搭載可能。
 刺激音にCE-Chirp®刺激音も利用できる。

- CE-Chirp®刺激音: 従来よりもより大きな反応振幅が得られる。
- ASSRでは8周波数、両側同時測定により検査時間の大幅な短縮を実現。(=>30分未満)
- 各反応時のノイズを比較し、加算平均の際にノイズの少ない反応により比重を置く計算方式であるベイズ推定により、最終平均値に含まれるノイズを減らし、より安定した波形を得ることができ、検査中に被検者が覚醒した場合の波形の乱れを防ぐ。(=>基本は睡眠中)



2019/12/5 AIMaP2019大阪教育大学(N. Ikawa) 14

14

さらに進んで Eclipse エクリプス(インターアコースティクス社(デンマーク)製)

Diatec HPより <https://www.diatec-diagnostics.jp/solutions/products/abr/interacoustics-eclipse-complete-solution#>

ABR技術と検査基準

残留ノイズ検査の停止基準

聴性誘発反応検査において唯一ともいえる最も重要な課題は、ノイズの軽減です。残留ノイズは加算平均の停止基準となり、多くの場合は検査時間を短縮し、反応の確実性を判断する指標となります。

CE-Chirp®音 - 反応振幅の増大

閾値検査用の刺激音、CE-Chirp®音はクラウス・エルバリング氏により開発されました。各周波数における蝸牛内の伝播速度を補償することで、従来のクリック音やトーンバーストに比べておよそ2倍の反応振幅が得られます。

従来のCE-Chirp®音は、中入力の音圧で最大の反応振幅が得られるように設計されています。CE-Chirp® LS音では、高入力の音圧でも明確な反応波形を得ることができます。CE-Chirp® LS音は音圧別に設計されており、従来のCE-Chirp®音を全面的に改良した刺激音です。

狭帯域の刺激音、NB CE-Chirp® LS音は音圧別に潜時を調整した刺激音です。クリック音やCE-Chirp® LS音と近似した潜時に行えるように改善されました。潜時以外は、従来のNB CE-Chirp®音と変わりません。

これらのCE-Chirp®音は、EP25およびASSRの検査モジュールに標準搭載されており、EP15にもオプションで搭載が可能です。

ベイズ推定 - 検査時間の節約

ABR検査でベイズ推定を使用することで、被検査者の体動が生じた場合でも安定した波形を得ることができます。測定中の生理的なノイズによる影響は最小限に抑えられ、低いノイズ量を維持したまま加算平均が継続されます。結果的に、貴重な検査時間も短縮されます。

Fmp - 反応精度の向上

反応の有無を判定する際、反応波形の確実性を判断する客観的な指標となるのが、Fmpです。Fmpグラフには統計データに基づいた測定中の反応の質がFmp値として表示されます。Fmp値を参考にすることで反応の判定がより容易になり、検査時間の短縮にも繋がります。



測定中に算出された反応の確実性がFmp値として表示されます。上図では、上限8000回の加算回数に対して僅か1500回の加算で99%の反応確実性が得られています。



停止基準は、特定の加算回数ではなく、残留ノイズにすることを推奨します。

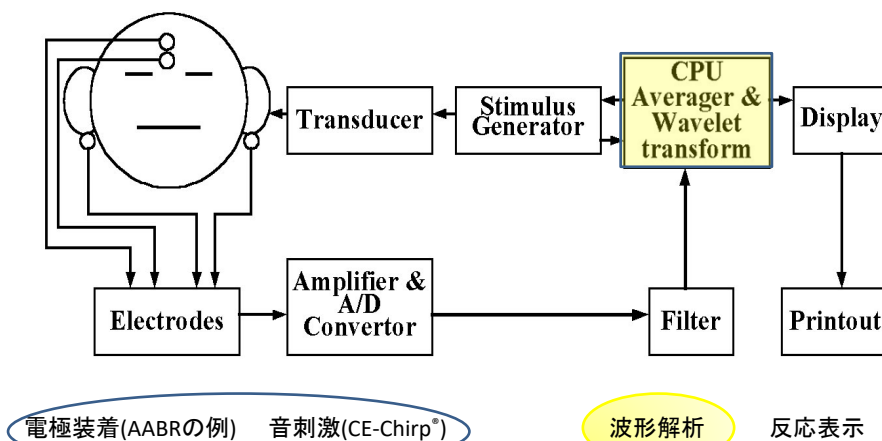
2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

15

15

出発点: ABR・ASSR の導出装置の改良(効率化)



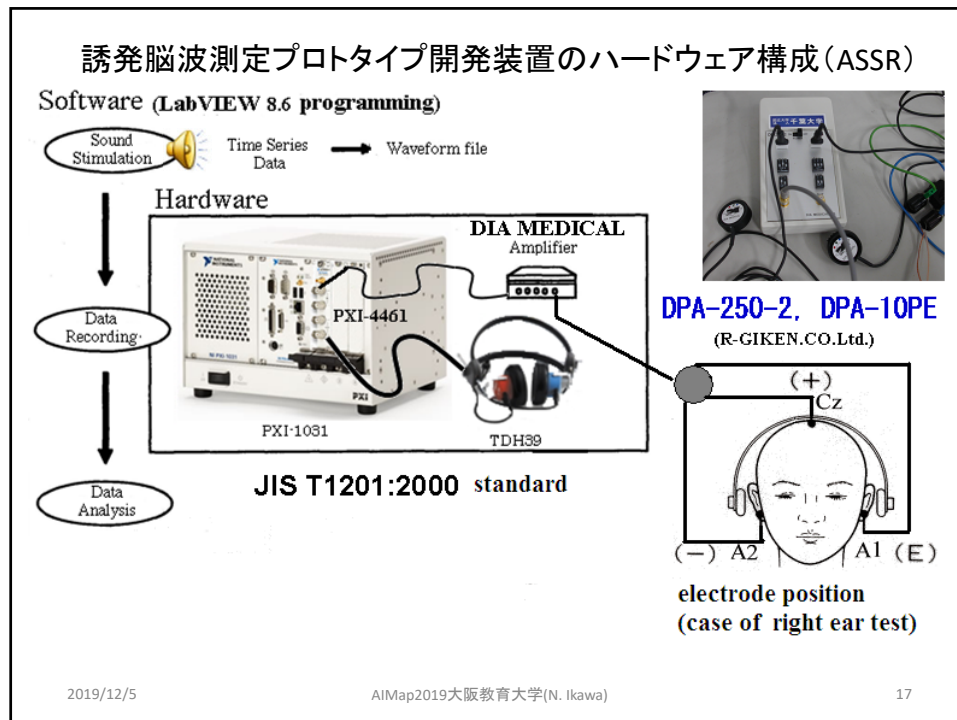
2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

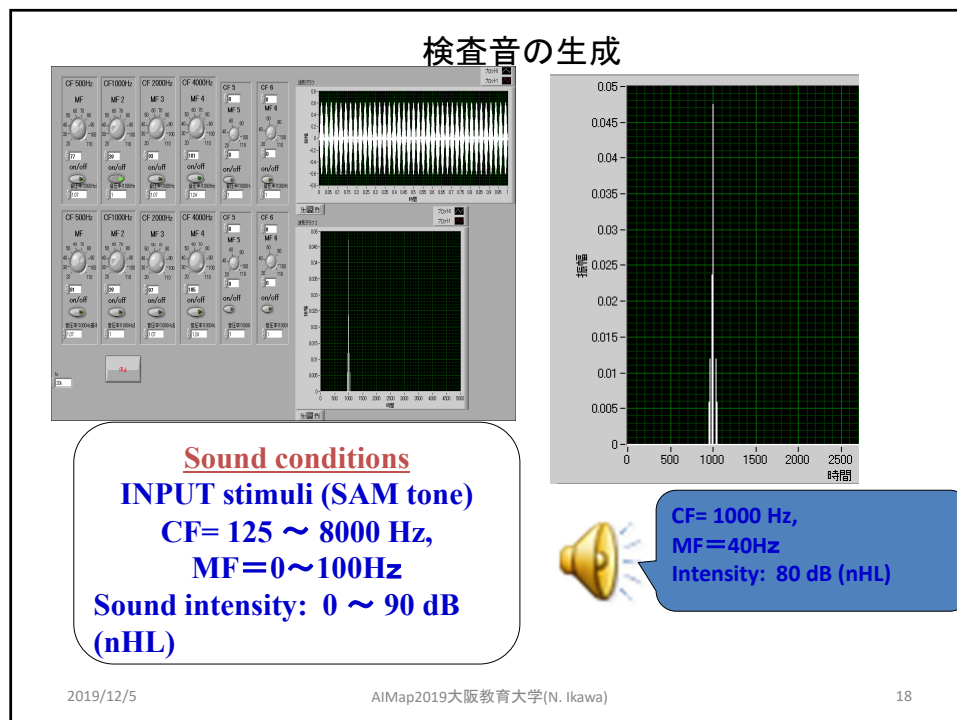
16

16

井川信子, 守本晃, 芦野隆一



17



18

音刺激に同期して脳波データを集録する:
Dynamic input and output using NI-PXI(PXI-4461)

図略

2019/12/5

AIMap2019大阪教育大学(N. Ikawa)

19

19

ASSR臨床検査装置も
MASTERからエクリップスへと改善されつつあるが

- ・検査時間は30分をちょっときるくらい.
- ・被験者を眠らせなければならない.
- 臨床面では精密検査なのでこれで十分と思う医師も少なくない.
- しかし、より速くかつ正確な
誘発脳波波形から反応の抽出は必要である.
- ウェーブレット解析を用いて観察する.

2019/12/5

AIMap2019大阪教育大学(N. Ikawa)

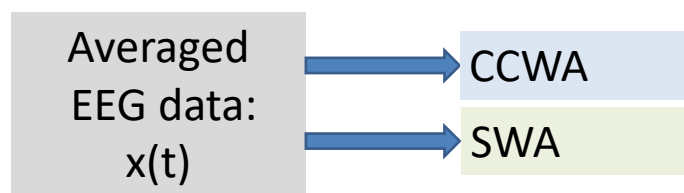
20

20

40-Hz ASSRを対象にCCWA とSWAを適用

40-Hz ASSR検出用にデータ集録した誘発脳波に

- ・複素連続ウェーブレット解析(Complex Continuous Wavelet Analysis: **CCWA**)
- ・離散定常ウェーブレット解析(Discrete Stationary Wavelet Analysis : **SWA**)



2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

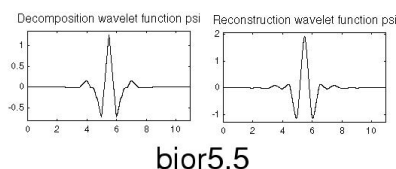
21

21

SWA分解レベルと構成周波数

分解レベル	構成周波数
D 1	256 — 512 Hz
D 2	128 — 256 Hz
D 3	64 — 128 Hz
D 4	32 — 64 Hz
D 5	16 — 32 Hz
D 6	8 — 16 Hz
D 7	4 — 8 Hz
A 7	0 — 4 Hz

サンプリング周波数 1024 Hz



2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

22

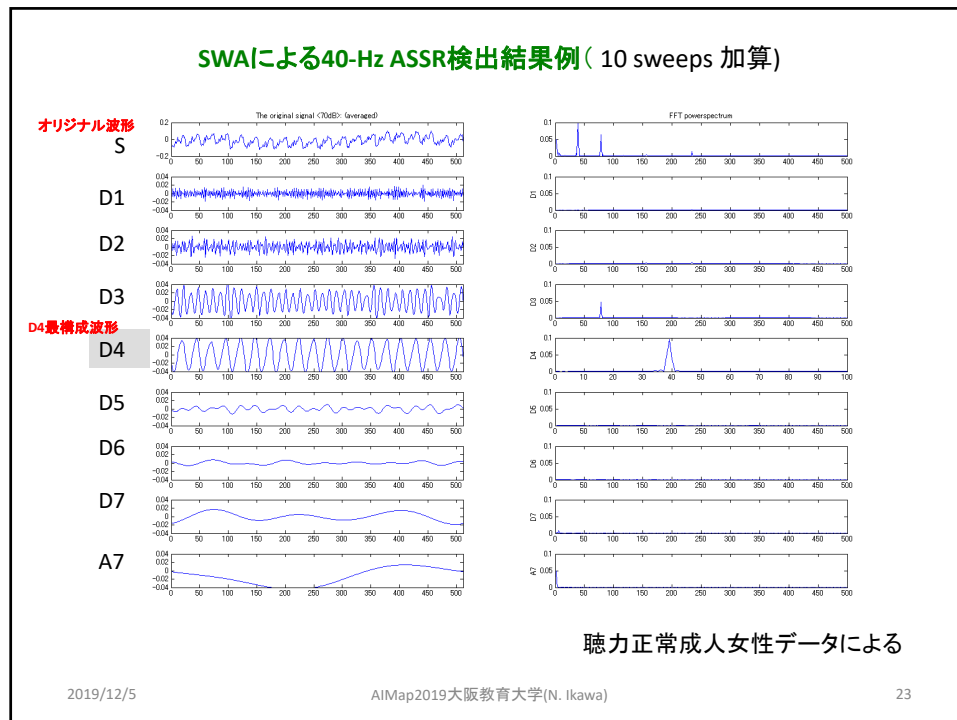
22

ヒトの脳波は周波数帯域ごとに以下のように名前が付けられ、それぞれ異なった生理学的な意義を有す:

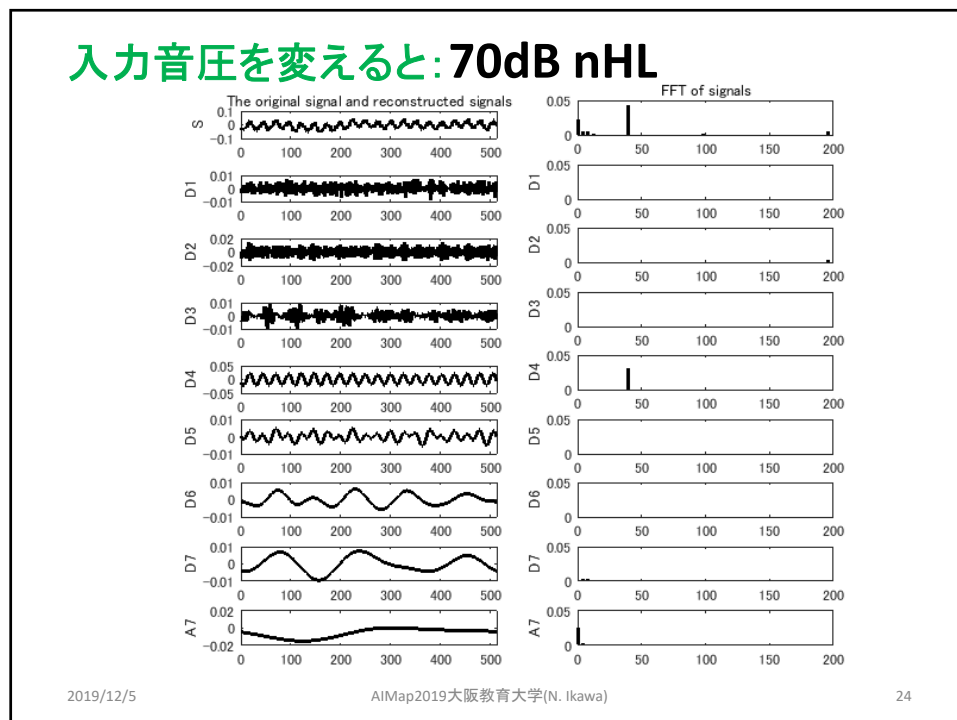
- ・**デルタ波** δ (デルタ): 1~3Hz
- ・**シータ波** θ (シータ): 4~7Hz
- ・**アルファ波** α (アルファ): 8~13Hz
- ・**ベータ波** β (ベータ): 14~30Hz
- ・**ガンマ波** γ (ガンマ): 30~64Hz

注) β と γ 帯域の境界の周波数は28Hzとするものなど諸説ある。

一般に健常者では、安静・閉眼・覚醒状態では後頭部を中心に α 波が多く出現する。また睡眠の深さ(睡眠段階)は脳波の周波数などに基いて分類されている。



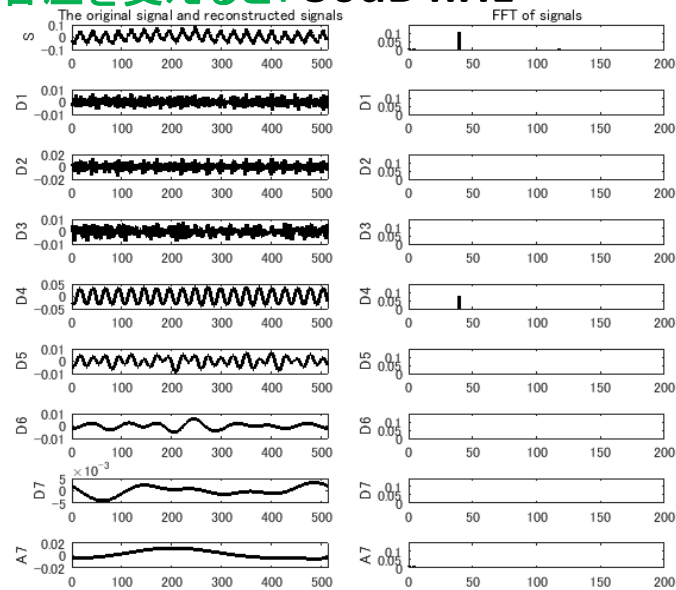
23



24

井川信子, 守本晃, 芦野隆一

入力音圧を変えると: 50dB nHL

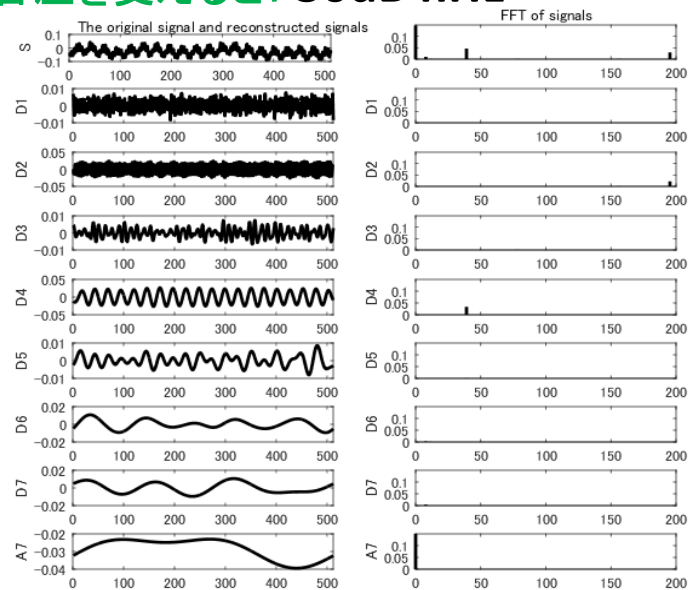


2019/12/5

25

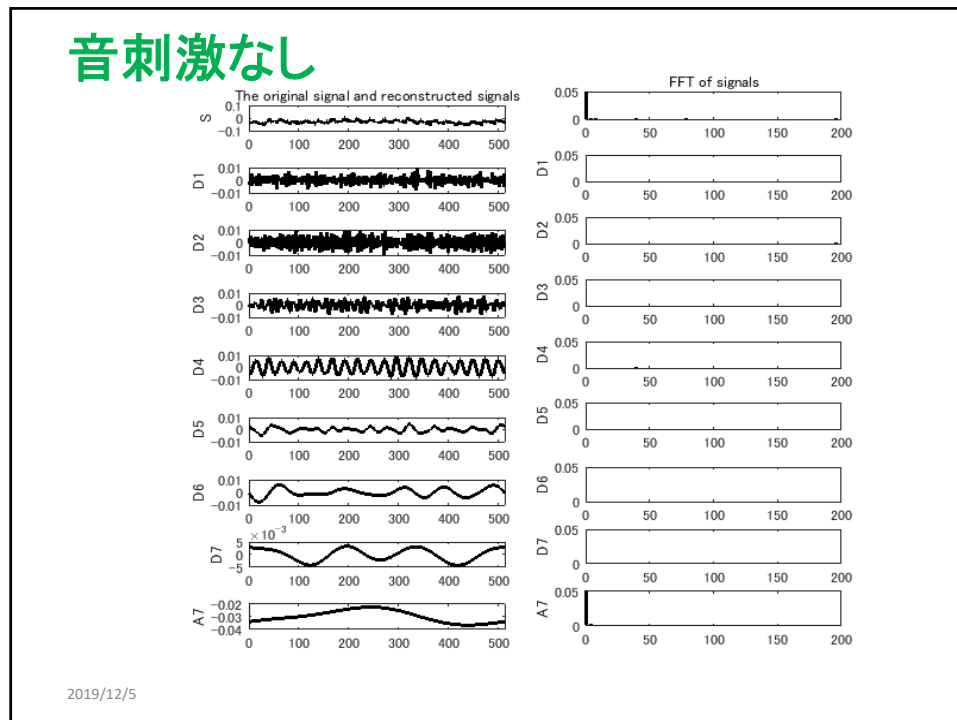
25

入力音圧を変えると: 30dB nHL

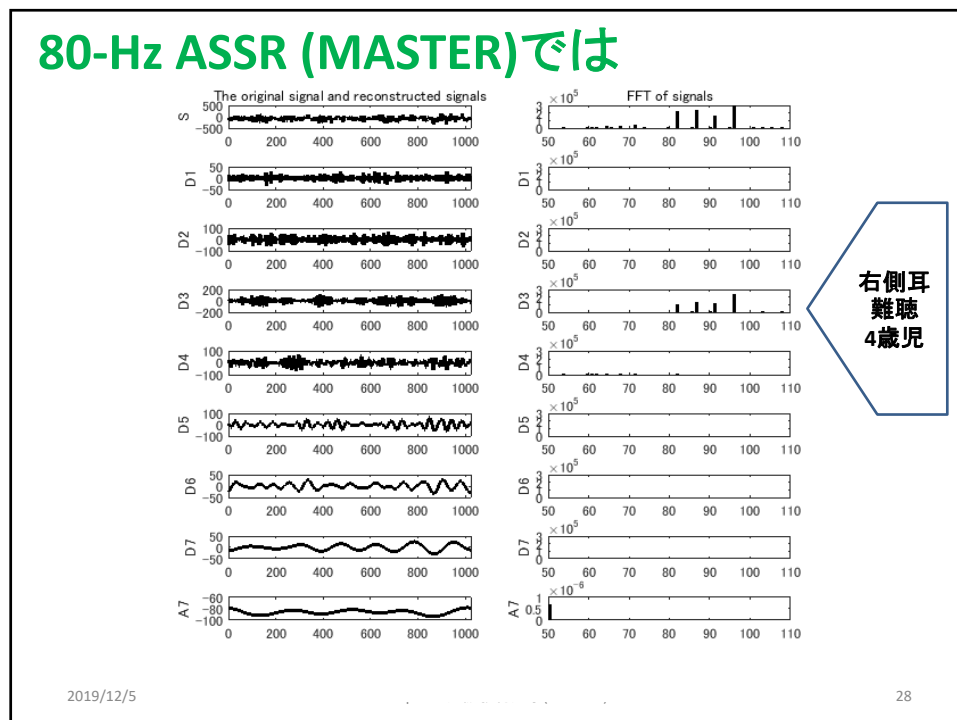


2019/12/5

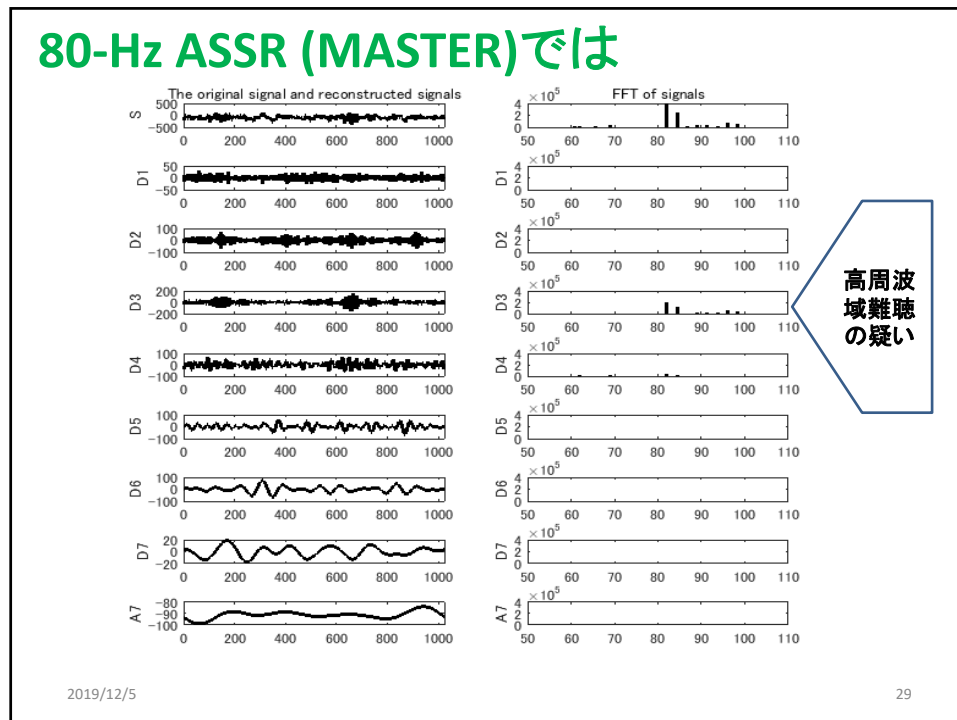
26



27



28



29

CCWA

Wavelet Function:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right), \quad a(\neq 0), \quad b \in \mathbb{R}$$

$$W_\psi[x(t)] = C(a, b) = \int_{-\infty}^{\infty} x(t) \psi_{a,b}^*(t) dt$$

Complex Morlet Function:

$$\psi(t) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{t^2}{2\sigma^2}} e^{i\omega_0 t}$$

$$W_\psi[x(t)] = C(a, b) = \int_{-\infty}^{\infty} x(t) \frac{1}{\sqrt{2\pi\sigma^2 a}} e^{-\frac{(\frac{t-b}{a})^2}{2\sigma^2}} e^{-i\omega_0(\frac{t-b}{a})} dt$$

2019/12/5 AIMaP2019大阪教育大学(N. Ikawa) 30

30

CCWA

Complex Morlet Function:

$$\psi(t) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{t^2}{2\sigma^2}} e^{i\omega_0 t}$$

$$W_\psi[x(t)] = C(a, b) = \int_{-\infty}^{\infty} x(t) \frac{1}{\sqrt{2\pi\sigma^2 a}} e^{-\frac{(t-b)^2}{2\sigma^2}} e^{-i\omega_0(\frac{t-b}{a})} dt$$

Here, we put $\sigma = \frac{\sqrt{3}}{2}$, $\omega_0 = 2\pi$,

Using MATLAB function **cmorwvf(Lb, Ub, U, N, fb, fc)**,
where

N = 1000; Lb = -5; Ub = 5; fb = 1.5; fc = 1;

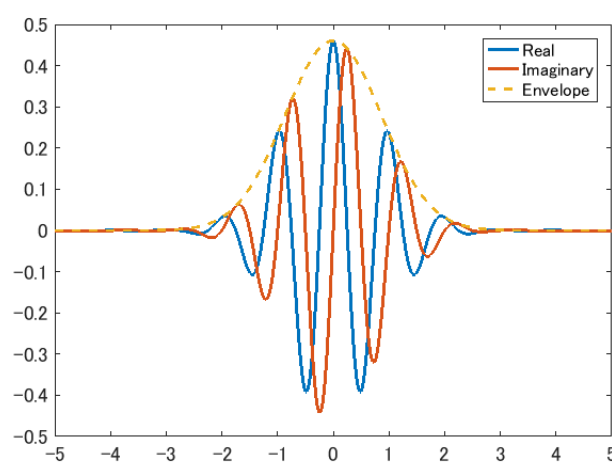
2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

31

31

Complex Morlet Wavelet



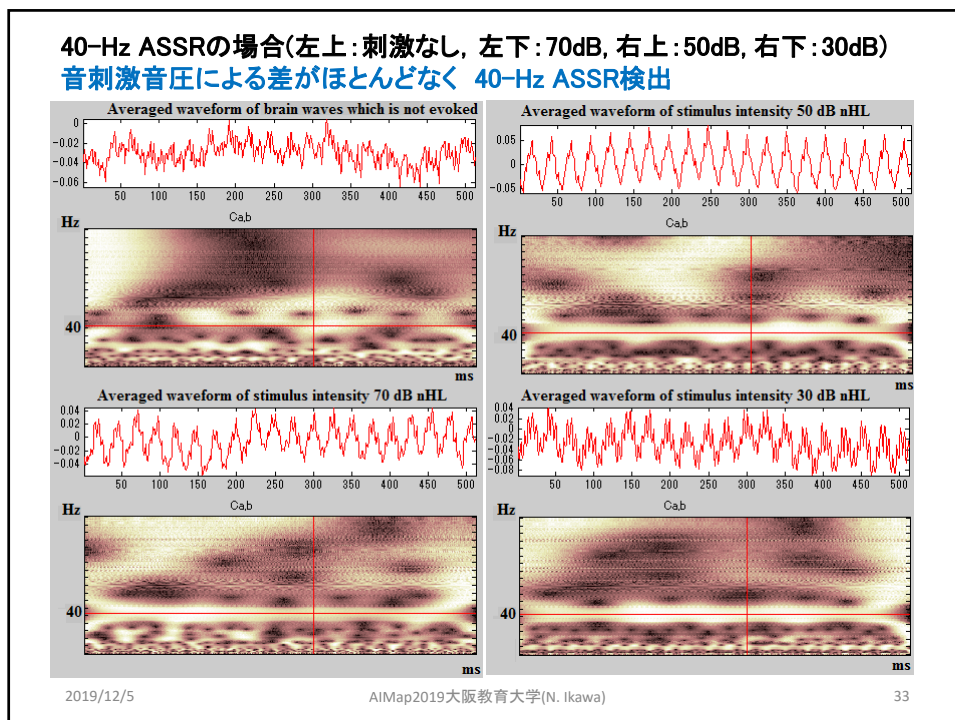
2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

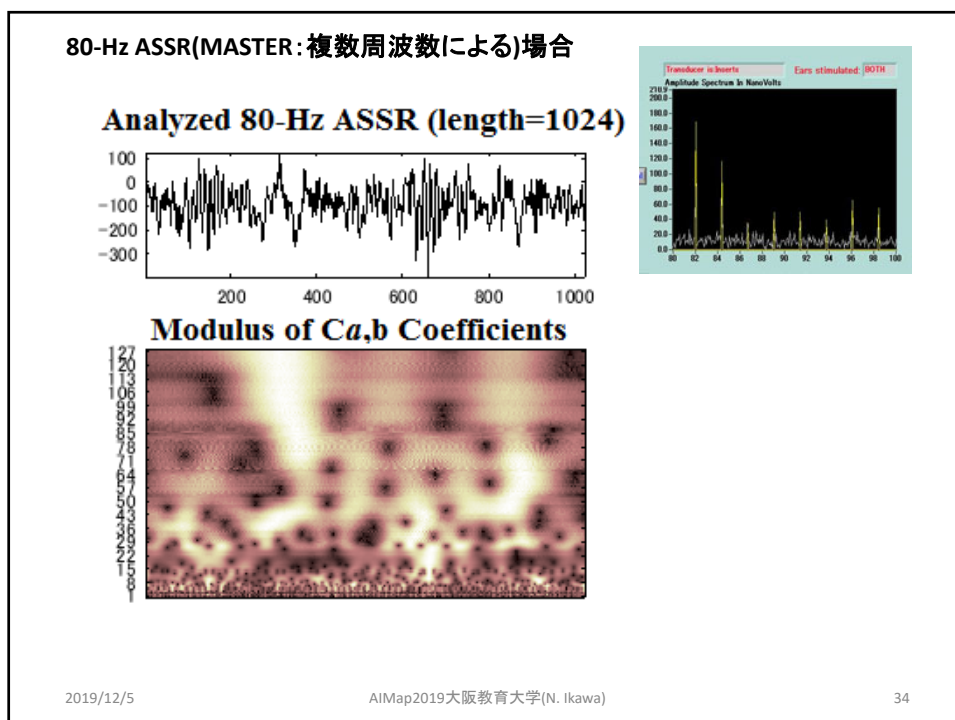
32

32

井川信子, 守本晃, 芦野隆一



33



34

SWAとCCWAの結果比較		
	SWA	CCWA
単一周波数	○	○
複数周波数	○	×
低い刺激音圧	△	○
測定時間	○	○
判定のしやすさ	△	○

2019/12/5 AIMaP2019大阪教育大学(N. Ikawa) 35

35

まとめ
SWAとCCWAを40-Hz ASSRを得る誘発脳波データに適用して比較した. ・単一周波数刺激で両者は有効である. 特にCCWAにおいて明確に検出ができた. ・複数周波数刺激の場合はSWAが有効であるが, 聴力閾値付近になると反応の判定が難しくなる.

2019/12/5 AIMaP2019大阪教育大学(N. Ikawa) 36

36

井川信子, 守本晃, 芦野隆一

文献一覧

- [1] 青柳優, 聴性定常反応, その解析法・臨床応用と起源, 2004, リオン株式会社.
- [2] N. Ikawa, T. Yahagi and H. Jiang, "Waveform analysis based on latency-frequency characteristics of auditory brainstem response using wavelet transform," Journal of Signal Processing, Vol. 9, No.6, pp. 505-518, 2005.11.
- [3] M. S. John, et al., MASTER: aWindow program for recording multiple auditory steadystate responses, Comput. Methods Programs Biomed., 61, 125-150, 1998.
- [4] 井川他, 聴性定常反応による聴力検査装置の試作—PXI-4461 による計測精度の向上—, 千葉大学CFME, 2009.
- [5] 井川, 守本, 芦野, “40Hz 聴性定常反応の加算法と離散定常ウェーブレット解析”, JSIAM年会, 47-48, 2011
- [6] 井川 信子, 守本 晃, 芦野 隆一, “離散定常ウェーブレット解析による高速聴性脳幹反応ピーク潜時検出”, 日本応用数理学会論文誌, Vol.27 No.2, pp.216-238, 2017.6.25.
- [7] 井川 信子, 守本 晃, 芦野 隆一, “他覚的聴力検査に用いる聴性誘発脳波の信号解析の改善について”, <http://www.osaka-kyoiku.ac.jp/~morimoto/WSPRO/wavelet2013proceedings.pdf>, 平成25年度数学・数理科学と諸科学・産業との連携研究ワークショップ「ウェーブレット理論と工学への応用」, 2013.11.23.
- [8] 井川 信子, 守本 晃, 芦野 隆一, “ウェーブレット解析による聴性定常反応波形高速加算法の検証”, JSIAM年会, 2501_2018-08-05-20-08-00-97313.pdf, 2018.9..

2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

37

37

ご清聴ありがとうございました.

謝辞

本発表は, 部分的に AIMaP と大阪教育大学のサポートを受けています.

2019/12/5

AIMaP2019大阪教育大学(N. Ikawa)

38

38

DWTハイディングとトリプルDESによる暗号通信

新井康平

佐賀大学 名誉教授、客員研究員

アリゾナ大学 客員教授

西九州大学、久留米工業大学 非常勤講師

国際学術会議 宇宙空間研究委員会 顕彰委員

日本学術会議 連携会員

ウェーブレットに係る著書

- 新井康平、ウェーブレット解析の基礎理論、森北出版(平成12年11月)
- 新井康平、Javaによる地球観測衛星画像処理法、森北出版(平成13年6月)
- 新井康平、Leland Jameson、ウェーブレット解析による地球観測衛星データの利用方法、森北出版(平成13年7月)
- 新井康平、独習ウェーブレット解析、近代科学社出版（平成18年6月）

研究概要

- ステガノグラフィ離散ウェーブレット変換を使用したデータ隠蔽方法：DWTおよび暗号化(トリプルデータ暗号化標準)：DES (Data Encryption Standard) を提案
- また、DWTを使用して、最初にデータを他のメディアに保護
- トリプルDESは、データをエンコードし、追加のセキュリティを提供して、隠されたデータの検出を困難にする
- これにより、ブルートフォース、選択したプレーンテキストおよび既知のプレーンテキスト攻撃に対して耐性を付ける
- テストの結果、DWTによる画像の挿入は、明るさとコントラストの画像操作に対して100%耐性があるが、トリミング、サイズ変更、回転した画像操作にはそれほど耐性がない

ステガノグラフィ

- 一般的に暗号データは暗号化されていることはわかって、解読できないというのが特徴
- ステガノグラフィの場合はそもそもデータ・メッセージが隠蔽されていること自体に気付かれないのが特徴
- ステガノグラフィは主に以下のような目的に利用
 - 電子透かしとして、著作権情報等を埋め込む
 - 改ざん防止
 - 諜報活動における情報の提供、隠蔽

DESとAES

- 従来、アメリカでは DES と呼ばれる暗号化方式が主流でした。しかし時代の変化に伴いDESは古い暗号方式となった為、アメリカ政府はより強力な暗号化方式を公募しました。その結果、選ばれた方式が共通鍵暗号方式（AES）です。
- AES（Advanced Encryption Standard）の規格には「AES-128」「AES-192」「AES-256」の3種類があります。鍵長が長くなれば安全性が増すがその分、計算量が増えるのでどの方式を使うかはケースバイケース

AES

- 共通鍵暗号方式（AES）は暗号化と復号で使う鍵が同じなのが特徴です。そのため第三者に鍵が知られてしまうと簡単に解読される危険性がある為、鍵を秘密にしておく必要があります。
- 共通鍵暗号方式（AES）は暗号化や復号化の処理が比較的簡単な為、処理時間が早いというメリットがあります。しかし処理が簡単な分、解読されやすいというデメリットもあります。また共通鍵暗号方式（AES）を使う相手の数に応じて鍵を作る必要があるため、鍵の数が多数必要となります。

RSA

- 公開鍵暗号方式（RSA）とは共通鍵暗号方式（AES）とは違い、暗号化と復号は別の鍵を使用する暗号方式です。
- 公開鍵暗号方式（RSA）を使用する場合には、まず暗号化の鍵を公開します。暗号化の鍵を公開することにより自分宛の暗号化には、公開した鍵を使用してもらいます。そのため鍵の受け渡しが容易であり秘密に管理する必要があるのは、自分の復号鍵だけとなります。

RSA VS AES

- 公開鍵暗号方式（RSA）では相手の数に応じて鍵を作る必要がありますが、共通鍵暗号方式（AES）では相手の数に関係なく公開鍵は1つでよいので鍵の管理が容易です。
- 公開鍵暗号方式（RSA）のメリットは安全性の高いという点ですが、処理時間が遅いというデメリットもあります。

公開鍵暗号方式と共通鍵暗号方式を使ったSSL

- 「公開鍵暗号方式」で、通信内容を暗号化するための「共通鍵」を、クライアント/サーバー間で共有します。
- 「クライアント」から、「SSL通信をしたいです」と、「サーバー」へ要求する
- 「サーバー」は、「了解」と言って、SSL（サーバー）証明書と公開鍵を、「クライアント」へ送信する
- 「クライアント」は、受け取った公開鍵を用いて、（クライアント側で生成した）「共通鍵」を暗号化して、「サーバー」へ送る
- 「サーバー」は、受け取った暗号データを、秘密鍵を用いて復号化し、「共通鍵」を取得する

- 共有した共通鍵を用いた「共通鍵暗号方式」で、実際の通信データ（個人情報やログイン情報）を暗号化して通信します。
- 「クライアント」が、通信データを「共通鍵」で暗号化し「サーバー」へ送信する
- 「サーバー」は、受け取った暗号データを「共通鍵」で復号化し、データを取得する
- 「サーバー」から「クライアント」への通信も、同じ流れになります。

SSL証明書

- 通信を暗号化する目的は、仮に第三者から通信データを傍受されても、暗号化されているので情報を特定されるリスクがないことです。
- Webサイトでは、特にネットショップなどで「個人情報」や「クレジットカード情報」を登録するページで、暗号化がされています。理由は明白で、第三者に傍受されると非常に危険な情報を扱うからです。
- ネットショップなどでは、必ず「SSL証明書」という、「公的な第三者機関（認証局）」が発行する証明書を取得して、安全性・信頼性を担保しています。
- 以前は、年に2～3万円はする「SSL証明書」でしたが、昨今では、3000円程度のモノもあり、個人でも導入が容易になっています

WordPressは、オープンソースのブログソフトウェア(PHPで開発)

- 個人でも、ブログやWebサイトを運営している方は、サイトの「管理ページ」や「管理ページにアクセスする際のログインページ」なども、暗号化をしておいた方が良いでしょう。
- もしログイン情報を第三者に傍受されていた場合、暗号化していなければ、第三者からその情報で不正ログインされてしまうリスクがあるからです。
- WordPressを利用している場合は、簡単に「ログインページ」と「管理ページ」を暗号化させることができます。

https://techacademy.jp/briefing-lp-wordpress-s?utm_source=yahoo&utm_medium=cpc&utm_campaign=03_briefing_wordpress&yclid=YSS.1000002331.EAlaIqObChMikeD5076d5glVQ7aWCh1vbQuaEAAYASAAEgltfPD_BwE

提案方法

- ステガノグラフィにはDWTに基づくものがある。DWTには、他のステガノグラフィ手法よりも優れた利点がある。**メッセージは、暗号化技術を使用して理解できない別の形式に事前にエンコードして、セキュリティを強化**
- 暗号化の主な目的は、許可されていない人々からデータを保護
- 暗号化のうちの1つはトリプルDES方法(処理時間が短い)
- 1が64ビットブロックで動作し、3つのキーを使用：各キーはサイズが56ビットであり、これらのキーはトリプルDESの長所
- この方法は、処理時間が適度に速く、**ブルートフォース、選択されたプレーンテキスト、既知のプレーンテキストなどの攻撃に対する耐性**がある

目的

- DESの処理速度の速い暗号化によってセキュリティを高め、
→**3重化DES**
- なおかつ、**秘匿情報を原情報に埋め込む**ことによって、→離散ウェーブレットに基づくステガノグラフィ
- **原情報の著作権**を守る
- **トリプルDESのキーを秘匿化することも可能**

- DESは、代表的な共通鍵暗号アルゴリズムで、米国では政府標準の暗号化手法の1つ
- DESは、データを64ビット長のブロックに分割し、各ブロックを56ビット長の鍵で暗号化する共通暗号鍵アルゴリズム
- トリプルDESは、DESを3重に繰り返すことで、暗号強度を高めている。DESは仕様が公開
- UNIXシステムにおけるログイン時のパスワードによるユーザー認証でDESが使われているのは有名
- UNIXのパスワードはDESの鍵として機能しており、ある固定したデータを、ユーザーが打ち込んだパスワードを鍵として暗号化
- その出力された暗号文を、/etc/passwdに記録されたユーザーの暗号文データと一致するかどうかをチェックすることによって、ユーザー認証を行っている。
- UNIXのパスワードが8文字までしか有効ではないのは、DESの鍵が56ビットであることと関連している。トリプルDESが採用されていれば、16文字あるいは24文字まで有効である。

トリプルDES暗号化

- トリプルDES 暗号化は、3つの8バイトのDES鍵からなる3倍長のDATA鍵を使用して、以下の方法により8バイトのデータを暗号化
- 最初の鍵を使用してデータを暗号化
- 2番目の鍵を使用して結果を復号
- 3番目の鍵を使用して2番目の結果を暗号化
- トリプルDES 暗号化が行われたデータを復号する場合は、以下のように手順は逆
- 3番目の鍵を使用してデータを復号
- 2番目の鍵を使用して結果を暗号化
- 最初の鍵を使用して2番目の結果を復号

DWTと挿入プロセス

挿入プロセスでは、カバー画像、ドキュメント (.docx、.xlsx、.pdf、または.txt)、およびキー (K1、K2、およびK3) が必要

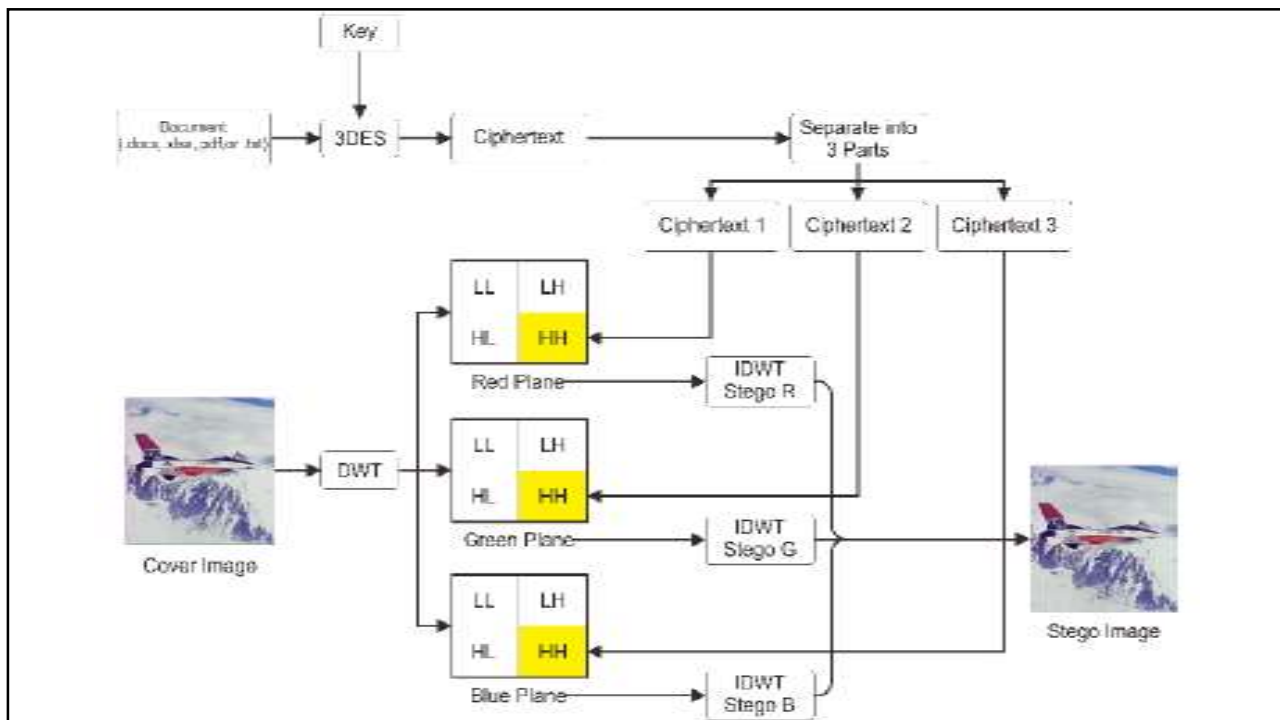
$$DWT\{f\{t\}\} = W_\phi(j_0, k) + W_\psi(j, k)$$

where,.

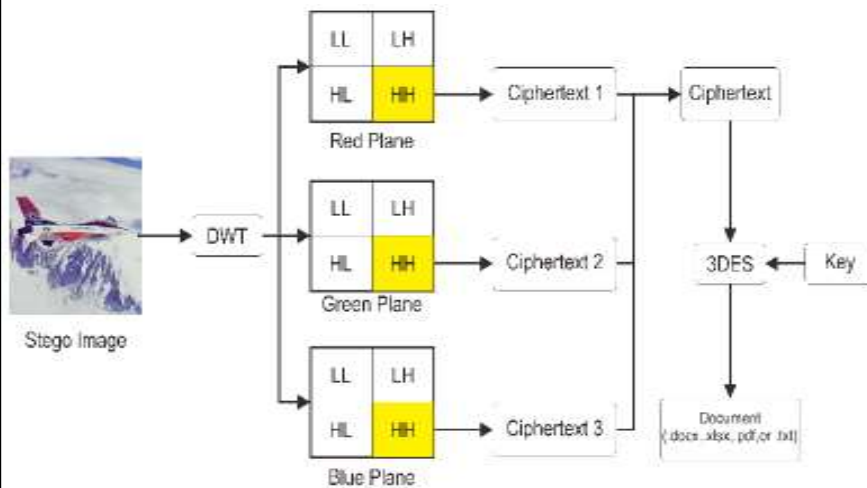
$$W_\phi(j_0, k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] \phi_{j_0, k}[n]$$

$$W_\psi(j, k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] \psi_{j, k}[n], \quad j \geq j_0$$

- 1) トリプルDESを使用してキーでドキュメントを暗号化し、暗号文を取得
- 2) 暗号文を、暗号文1、暗号文2、および暗号文3に分ける
- 3) DWTを使用してカバー画像を変換し、R、G、Bレイヤーの4つのサブバンドを取得
- 4) 各暗号文を各レイヤーR、G、BのHHサブバンドに挿入
- 5) 画像再構成はIDWTを使用して、ステゴ画像を生成



抽出方法



- 1) DWTを使用してステゴ画像を変換し、R、G、Bレイヤーの4つのサブバンドを取得
- 2) 各シートのHHサブバンドの情報を抽出
- 3) 抽出された情報を組み合わせて、完全な暗号文を取得
- 4) 3DESを使用して暗号文を復号化し、ドキュメントを取得するためのキーを使用

実験

52 OKU & AIMaP 2019 Workshop on Wavelet theory and its applications to engineering

カバー画像

- (a) Airplane.png
- (b) Arctichare.png
- (c) Baboon.png
- (d) Boat.png
- (e) Boy.bmp
- (f) Cat.png
- (g) Fruits.png
- (h) Frymire.png
- (i) Lena.png
- (j) Peppers.png



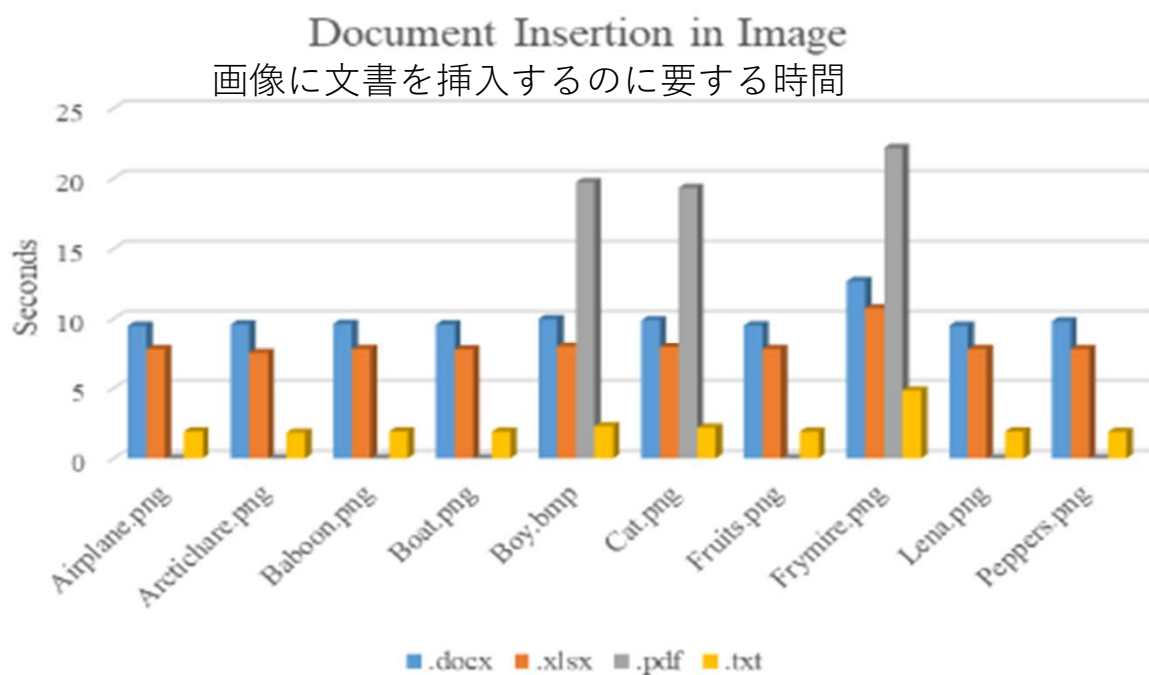
TYPES OF SUPPORTED DOCUMENTS

No	Dokumen	Cover Image
1	Docx	Png
2	Xlsx	Bmp
3	Pdf	Jpeg
4	Txt	Tiff

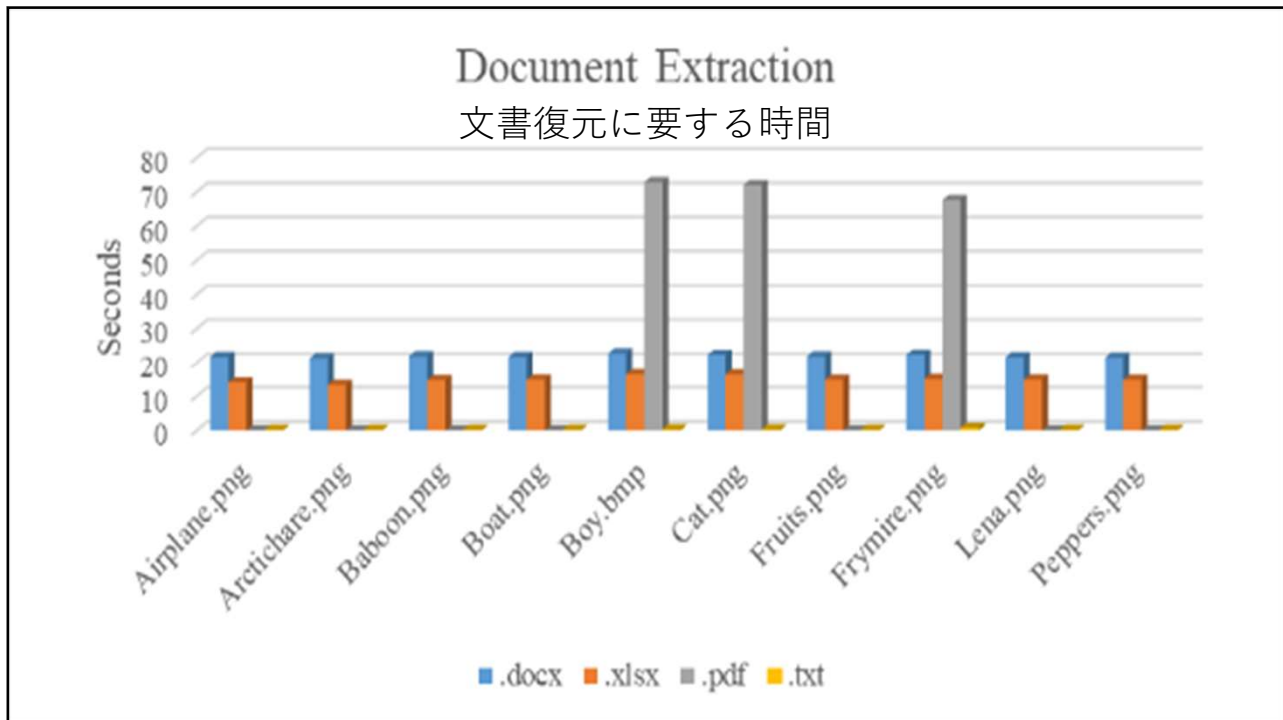
- ドキュメントの挿入
- さまざまな拡張子を持つドキュメントを各画像に挿入して、各画像に各素材を挿入する時間を比較
- このテストで使った文書の種類は、12 KB docx、サイズ9.67 KBのxlsx、22.3 KBの容量のpdf、および161バイトの容量のtxt

実験に用いたPC: Let's Note CF-R9

- CPU: Intel Core i7 (1.07GHz)
- RAM: 4GB
- 32 bit OS
- X64 Base Processor



54 OKU & AIMaP 2019 Workshop on Wavelet theory and its applications to engineering



画質評価

- 文書挿入した画像の画質評価結果
- 画像のHHに文書を挿入（この時、原画像および文書は1-255の値を持つが、256レベルすべてを挿入した：この挿入レベルをInsertion Valueと呼ぶ）
- 復元画像と原画像のMSEとPSNRを評価

Images	Image Assessment	Document Types			
		docx	xlsx	pdf	txt
Airplane 512x512	MSE	18	15	-	2
	PSNR	23	25	-	43
Arctichare 512x512	MSE	18	14	-	2
	PSNR	23	25	-	44
Baboon 512x512	MSE	18	16	-	2
	PSNR	23	24	-	42
Boat 512x512	MSE	18	15	-	2
	PSNR	23	25	-	43
Boy 768x512	MSE	14	11	22	1
	PSNR	26	27	21	46
Cat 490x733	MSE	14	12	23	2
	PSNR	25	27	21	45
Fruits 512x512	MSE	17	15	-	2
	PSNR	24	25	-	43
Frymire 1118x1106	MSE	5	5	7	1
	PSNR	34	35	31	52
Lena 512x512	MSE	17	15	-	2
	PSNR	23	25	-	43
Peppers 512x512	MSE	17	15	-	2
	PSNR	23	25	-	43

Insertion valueとPSNRとの関係

Original Image	Insertion Frequency	Insertion Value	Encryption Result	Decryption Result	PSNR
Airplane.png	HH	10	airplane.encripsi.nilai.10.png	Error	52 dB
Airplane.png	HH	20	airplane.encripsi.nilai.20.png	Error	49 dB
Airplane.png	HH	30	airplane.encripsi.nilai.30.png	Error	47 dB
Airplane.png	HH	40	airplane.encripsi.nilai.40.png	Error	45 dB
Airplane.png	HH	50	airplane.encripsi.nilai.50.png	Original Document	43 dB
Airplane.png	HH	60	airplane.encripsi.nilai.60.png	Original Document	41 dB
Airplane.png	HH	70	airplane.encripsi.nilai.70.png	Original Document	40 dB
Airplane.png	HH	80	airplane.encripsi.nilai.80.png	Original Document	39 dB
Airplane.png	HH	90	airplane.encripsi.nilai.90.png	Original Document	38 dB
Airplane.png	HH	100	airplane.encripsi.nilai.100.png	Original Document	37 dB
Airplane.png	HH	150	airplane.encripsi.nilai.150.png	Original Document	34 dB
Airplane.png	HH	200	airplane.encripsi.nilai.200.png	Original Document	32 dB
Airplane.png	HH	255	airplane.encripsi.nilai.255.png	Original Document	31 dB

画像処理攻撃に対する 耐性

Original Image	Manipulation	Degree / Area	Encryption Result	Decryption Result
Airplane.txt.png	Brightness	10%	Brightness.10%.png	Original Document
Airplane.txt.png	Brightness	20%	Brightness.20%.png	Original Document
Airplane.txt.png	Brightness	30%	Brightness.30%.png	Original Document
Airplane.txt.png	Brightness	50%	Brightness.50%.png	Original Document
Airplane.txt.png	Brightness	100%	Brightness.100%.png	Original Document
Airplane.txt.png	Brightness	150%	Brightness.150%.png	Original Document
Airplane.txt.png	Brightness	-150%	Brightness.minus150%.png	Original Document
Airplane.txt.png	Contrast	100%	Contrast.100%.png	Original Document
Airplane.txt.png	Contrast	-50%	Contrast.minus50%.png	Original Document
Airplane.txt.png	Crop	Up	Crop.atas.png	Original Document
Airplane.txt.png	Crop	Down	Crop.bawah.png	Blank Document
Airplane.txt.png	Crop	Right	Crop.kanan.png	"Can't be Extracted"
Airplane.txt.png	Crop	Left	Crop.kiri.png	"The Key That You Entered Is Incorrect"
Airplane.txt.png	Resize	400x400	Resize.400x400.png	"Can't be Extracted"
Airplane.txt.png	Resize	500x500	Resize.500x500.png	"Can't be Extracted"
Airplane.txt.png	Resize	510x510	Resize.510x510.png	"Can't be Extracted"
Airplane.txt.png	Resize	514x514	Resize.514x514.png	"Can't be Extracted"
Airplane.txt.png	Rotate	90° CW	Rotate.kanan.png	Blank Document
Airplane.txt.png	Rotate	90° CCW	Rotate.kiri.png	"Can't be Extracted"
Airplane.txt.png	Rotate	180°	Rotate.penuh.png	"Can't be Extracted"

ステガノグラフィー + 暗号化

Insertion@LL, Decryption Result: Blank Document, MSE=11%, PSNR=27dB

Original



Encryption Result



Insertion@LH, Decryption Result: Original Document, MSE=2%, PSNR=42dB

Original



Encryption Result



Insertion@HL, Decryption Result: Original Document, MSE=2%, PSNR=43dB

Original



Encryption Result



Insertion@HH, Decryption Result: Original Document, MSE=2%, PSNR=43dB

Original



Encryption Result



まとめ

- PDFドキュメントを使用した暗号化および復号化プロセスは、ファイルサイズが大きいため、他の種類のドキュメントを使用するよりも時間がかかる
- 抽出ドキュメントは、元のコンテンツと正確に一致: ドキュメント画像が大きいほど、またはドキュメントファイルサイズが小さいほど、品質が高い
- HLおよびHHにドキュメントを挿入すると、MSEおよびPSNRの値が大きくなるため、他よりも高品質の画像が生成
- 最小のMSEと大きなPSNR及びドキュメントを完全抽出でき観点から、**最適なInsertion Valueは50**
- ステゴ画像は、明るさとコントラスト操作の攻撃に対して耐性がある
- ステゴ画像は、**サイズ変更および回転攻撃に耐性がない**

References

- Kohei Arai, Kaname Seto, Data Hiding Based on Wavelet Multi-resolution Analysis, Journal of Visualization Society of Japan, Vol.22, Suppl.No.1, 229-232, 2002.
- Kohei Arai, Kaname Seto, Data Hiding Based on Multi-resolution Analysis Utilizing Information Content Concentrations by Means of Eigen Value decomposition, Journal of Visualization Society of Japan, Vol.23, No.8, pp.72-79,2003.
- Kohei Arai, Kaname Seto, Information Hiding Method Based on Coordinate Conversion, Journal of Visualization Society of Japan, 25, Suppl.No.1, 55-58,(2005)

- Kohei Arai, Kaname Seto, Data hiding based on Multi-Resolution Analysis taking into account scanning of the embedded image for improvement of invisibility, Journal of Visualization Society of Japan, 29, Suppl.1, 167-170, 2009.
- Kohei Arai and Yuji Yamada, Improvement of secret image invisibility in circulation image with Dyadic wavelet based data hiding with run-length coding, International Journal of Advanced Computer Science and Applications, 2, 7, 33-40, 2011
- Kohei Arai, Method for data hiding based on Legal 5/2 (Cohen-Daubechies-Feauveau: CDF 5/3) wavelet with data compression and random scanning of secret imagery data, International Journal of Wavelets Multi Solution and Information Processing, 11, 4, 1-18, B60006 World Scientific Publishing Company, DOI: 101142/SO219691313600060, 1360006-1, 2013.

- Kohei Arai, Data Hiding Method Replacing LSB of Hidden Portion for Secrete Image with Run-Length Coded Image, International Journal of Advanced Research on Artificial Intelligence, 5, 12, 8-16, 2016.
- Cahya Rahmed Kohei Arai, Arief Prasetyo, Noriza Arigki, Noble Method for Data Hiding using Steganography Discrete Wavelet Transformation and Cryptography Triple Data Encryption Standard: DES, International Journal of Advanced Computer Science and Applications: IJACSA, 9, 11, 261-266, 2018.

Mellin 変換を用いた，画像の拡大・縮小率を求める数値実験について

守本晃（大阪教育大学）

2019 年 12 月 5 日

1 Mellin 変換

$\mathbb{R}_+ := \{t \in \mathbb{R} \mid t \geq 0\}$ で定義された（急減少）関数 $f(t)$ の Mellin 変換を，

$$\mathcal{M}f(\omega) = \int_0^\infty f(t) t^\omega dt \quad (1)$$

で定義する．ただし， $\omega \in \mathbb{R}_+$ とする．

ω を非負の整数 n に取れば，Mellin 変換は， n 次モーメントを求めていることになる．全ての次数のモーメントが分かれば，元の関数が構成できるとかいう「モーメント母関数」があるので母関数について説明する．

逆変換は，複素領域で， $\mathcal{M}f(\omega)$ の極を全て囲む単純閉曲線 C で，線積分

$$f(t) = \frac{1}{2\pi i} \int_C \mathcal{M}f(\omega) t^{-\omega} d\omega$$

を計算することで得られる．逆ラプラス変換と似たような感じ．

1.1 Mellin 変換についての注意

Mellin 変換の定義式 (1) は，フランス人 Roger Godement の書いた Springer の教科書 “Analysis III” [1] での定義を採用した．工学系の多くの応用では，この定義を使っている．

Wolfram MathWorld [2] や Wikipedia [3] では，Mellin 変換の定義として，

$$\begin{aligned} \mathcal{M}f(s) &= \varphi(s) = \int_0^\infty f(t) t^{s-1} dt, \\ \mathcal{M}^{-1}\varphi(t) &= f(t) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \varphi(s) t^{-s} ds \end{aligned}$$

を採用している．逆変換は，複素平面上実部が c の直線で区切られた左半平面に $\varphi(s)$ の極が全て入るようにし， $\varphi(s)$ の極での $\varphi(s)t^{-s}$ の留数を全て足し合わせろということ．

我々の採用した Mellin 変換は，両側ラプラス変換

$$\mathcal{B}[f(t)](s) = \int_{-\infty}^{\infty} f(t) e^{-st} dt$$

において， $\eta = e^{-t}$ と変数変換すると，

$$\begin{aligned} \mathcal{B}[f(e^{-t})](s) &= \int_{-\infty}^{\infty} f(e^{-t}) e^{-st} dt \\ &= \int_{\infty}^0 f(\eta) (e^{-t})^s \left(-\frac{1}{e^{-t}} d\eta\right) \\ &= \int_0^{\infty} f(\eta) \eta^{s-1} d\eta \\ &= \mathcal{M}[f](s-1) \end{aligned}$$

になる．ただし， $\eta = e^{-t}$ と変数変換すると， $t : -\infty \rightarrow \infty$ は $\eta : \infty \rightarrow 0$ で， $d\eta = -e^{-t} dt$ であることを使った．

一方，Wolfram の定義では， $\mathcal{B}[f(e^{-t})](s) = \mathcal{M}[f](s)$ である． $\mathcal{M}[e^{-t}](s)$ がガンマ関数になる．

2 母関数

数列 $\{a_n\}$ に対して，関数列 $\{e_n(t)\}$ の重み付き和

$$f(t) = \sum_n a_n e_n(t)$$

を母関数とよぶ．母関数 (generating function) とは，数列から生成される関数という意味であり，テーラー展開，三角級数展開， z -変換 (ローラン展開) なども母関数である．

2.1 テーラー展開

数列 $\{a_n\}_{n=0,1,\dots}$ に対して，関数列として n 次単項式 t^n で和を取ると，母関数

$$f(t) = \sum_{n=0}^{\infty} a_n t^n \quad (2)$$

を得る．このとき，両辺を n 階微分して， $t = 0$ を代入することにより，

$$a_n = \frac{f^{(n)}(0)}{n!} \quad (3)$$

である．

逆に無限階連続微分できる関数 $f(t)$ に対して，係数を式 (3) で与え和 (2) を考えたとき，条件が良ければ元の関数に戻ることが分かっている（テーラーの定理）．

2.2 三角級数展開

関数列として， $\{e^{2\pi i n t}\}_{n \in \mathbb{Z}}$ を考えた場合が三角級数展開に相当する．数列 $\{a_n\}_{n \in \mathbb{Z}}$ に対して，和

$$f(t) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n t} \quad (4)$$

を考えると母関数になる． $f(t)$ は周期 1 の周期関数になる．区間 $[0, 1)$ で関数列 $\{e^{2\pi i n t}\}_{n \in \mathbb{Z}}$ が正規直交するので，数列 a_n は，

$$a_n = \int_0^1 f(t) \overline{e^{2\pi i n t}} dt = \int_0^1 f(t) e^{-2\pi i n t} dt \quad (5)$$

で計算できる．三角級数展開は，Fourier が 1807 年に熱伝導方程式を解くときに使った方法である．周期 1 の周期関数 $f(t)$ に対して，係数を式 (5) で定め，母関数 (4) を考えたときに，元に戻るかは，重要な問題であり，盛んに研究されている．1904 年にルベグ積分が発表されて， $L^2([0, 1))$ に入る関数なら元に戻ることが分かった．ちなみに，1845 年のリーマン積分を提案した論文のタイトルも，“Über die Darstellbarkeit einer Function durch eine trigonometrische Reihe”（三角級数による関数の表現可能性に関して）であった．

2.3 モーメント母関数

モーメント母関数（積率母関数）については， $f(t)$ のラプラス変換

$$\mathcal{L}[f](s) = \int_0^{\infty} f(t) e^{-st} dt$$

の e^{-st} に 0 の周りのテーラー展開

$$e^{-st} = \sum_{n=0}^{\infty} \frac{1}{n!} (-st)^n = \sum_{n=0}^{\infty} \frac{(-s)^n}{n!} (t)^n$$

を代入して、和と積分の順序を変えると、

$$\int_0^\infty f(t) e^{-st} dt = \int_0^\infty f(t) \left[\sum_{n=0}^\infty \frac{(-s)^n}{n!} (t)^n \right] dt = \sum_{n=0}^\infty \left[\int_0^\infty f(t) t^n dt \right] \frac{(-s)^n}{n!}$$

になり、 n 次モーメントを $\frac{(-s)^n}{n!}$ で足し合わせる母関数である。この母関数を逆ラプラス変換すれば、 $f(t)$ が再構成される。

3 スケール変換と Mellin 変換

スケール変換 $f_\alpha(t) = f(\alpha t)$ の Mellin 変換は、

$$\begin{aligned} \mathcal{M}f_\alpha(\omega) &= \int_0^\infty f(\alpha t) t^\omega dt \\ &= \int_0^\infty f(y) \left(\frac{y}{\alpha}\right)^\omega \frac{dy}{\alpha} \\ &= \alpha^{-(\omega+1)} \mathcal{M}f(\omega) \end{aligned}$$

である。これらの式から α を計算するには、

$$\alpha^{\omega+1} = \frac{\mathcal{M}f(\omega)}{\mathcal{M}f_\alpha(\omega)} \quad \Rightarrow \quad \alpha = \left(\frac{\mathcal{M}f(\omega)}{\mathcal{M}f_\alpha(\omega)} \right)^{1/(\omega+1)}.$$

図 1 では、一周期の $\sin(t)$ と $\sin(\alpha t)$, $\alpha = 0.7$. 時間幅 0.2 でサンプリングして、Mellin 変換を計算し、 α を横軸 ω で描いた推定した。

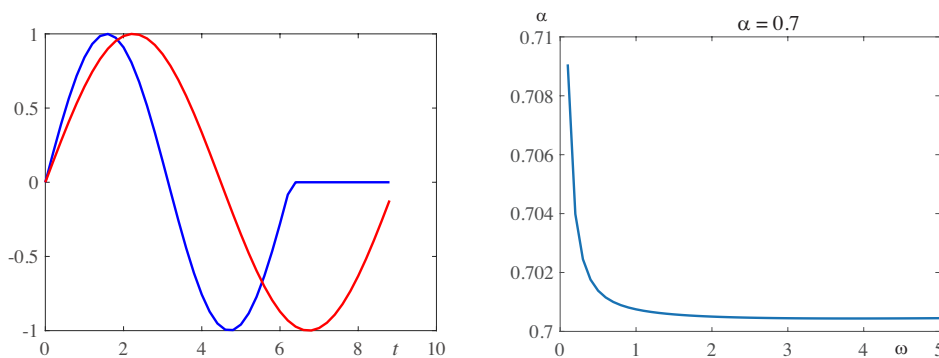


図 1: 青 : $\sin(t)$ 一周期, 赤 : $\sin(\alpha t)$, $\alpha = 0.7$ 一周期. 時間幅 0.2. 右 : α の推定.

原点の位置 $t = 0$ が非常に重要で、ここがずれると全く歯が立たない。図 2 参照。

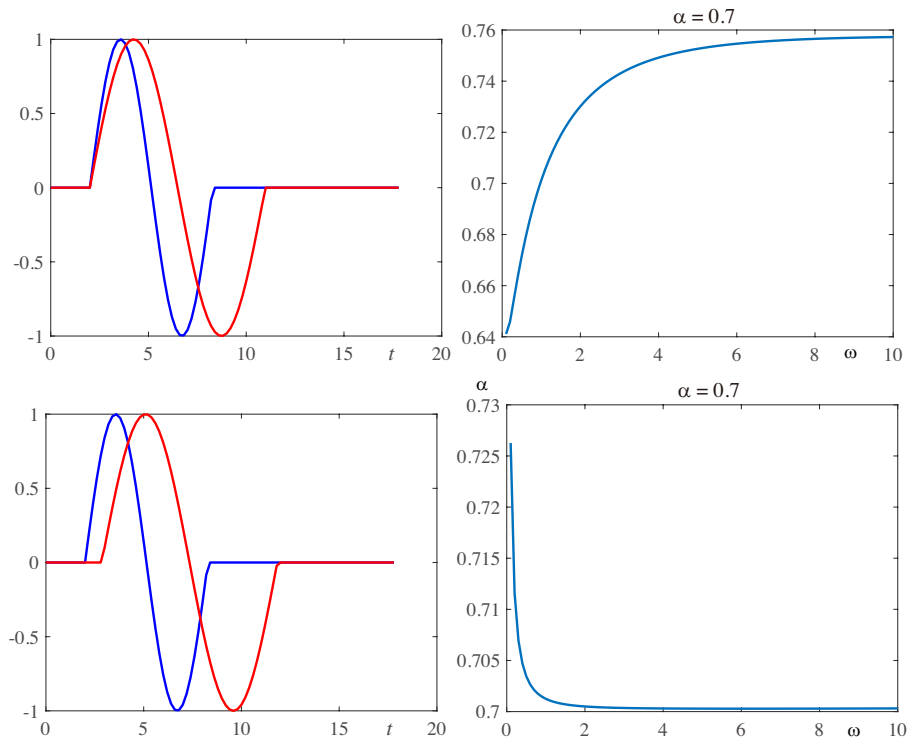


図 2: 上 : $\alpha = 0.7$ で原点がずれているとき. 下 : 原点が一致しているとき.

4 フーリエ空間で Mellin 作用素

実空間での平行移動は，フーリエ変換すると，変調に変わる．フーリエ変換の絶対値を取ると，変調部分は大きさ 1 なので考える必要がなくなる．そこで，フーリエ像の絶対値にたいして，Mellin 変換を考えると，実空間での平行移動の効果を打ち消せる． $f(t)$ と $f_\alpha(t) = f(\alpha t)$ のフーリエ変換は，それぞれ

$$\begin{aligned}\widehat{f}(\xi) &= \int_{\mathbb{R}} f(t) e^{-i\xi t} dt \\ \widehat{f}_\alpha(\xi) &= \int_{\mathbb{R}} f(\alpha t) e^{-i\xi t} dt = \int_{\mathbb{R}} f(s) e^{-i\xi s/\alpha} \frac{dt}{\alpha} = \frac{1}{\alpha} \widehat{f}\left(\frac{\xi}{\alpha}\right)\end{aligned}$$

である．フーリエ像の絶対値の Mellin 変換を考えよう．ただし，パラメータ $p > 0$ を追加するので，Mellin 作用素である．

$$\begin{aligned}\mathcal{M}|\widehat{f}|(p, \omega) &= \int_0^\infty |\widehat{f}(\xi)|^p \xi^\omega d\xi \\ \mathcal{M}|\widehat{f}_\alpha|(p, \omega) &= \int_0^\infty \left| \frac{1}{\alpha} \widehat{f}\left(\frac{\xi}{\alpha}\right) \right|^p \xi^\omega d\xi \\ &= \frac{1}{\alpha^p} \int_0^\infty |\widehat{f}(\eta)|^p (\alpha\eta)^\omega \alpha d\eta \\ &= \alpha^{\omega+1-p} \mathcal{M}|\widehat{f}|(p, \omega)\end{aligned}$$

よって， α を求めると，

$$\alpha^{\omega+1-p} = \frac{\mathcal{M}|\widehat{f}_\alpha|(p, \omega)}{\mathcal{M}|\widehat{f}|(p, \omega)} \implies \alpha = \left(\frac{\mathcal{M}|\widehat{f}_\alpha|(p, \omega)}{\mathcal{M}|\widehat{f}|(p, \omega)} \right)^{\frac{1}{\omega+1-p}}.$$

4.1 α の推定例と数値計算上の注意

4.1.1 信号とそのフーリエ変換

・ 信号については，図 3 左の 2 周期分の正弦波を考える．青が元の信号で，区間 $[0, 2\pi]$ 内に $\sin(2\pi t)$ 2 周期分を少しずらしてはめ込んで， $\Delta_1 = 0.01$ 間隔でサンプリングした信号である．一方，赤信号は $\alpha = 1.3$ とした $\sin(2\pi\alpha t)$ 2 周期分を少しずらして区間 $[0, 3\pi]$ にはめ込んで， $\Delta_2 = 0.007$ 間隔でサンプリングした信号である．fft を使ってフーリエ変換するときに，奇数長と偶数長で目盛りの扱いが異なるから，奇数長データは最後に 0 の要素を加えて各データ列は偶数長になるようにする．

・ フーリエ変換を計算するには，データの fft にサンプリング間隔をかければ，中点則を用いた数値積分になる．ただし，Matlab なら fftshift で直流成分を真ん中にする必要がある．このとき，青信号の角周波数軸は，

- 最低角周波数： $-\pi/\Delta_1$
- 角周波数刻み： $2\pi/\Delta_1$ /青信号のデータ長
- 最高角周波数： $\pi/\Delta_1 - \text{周波数刻み}$
- 角周波数軸：最低角周波数から最高角周波数までを角周波数刻みで

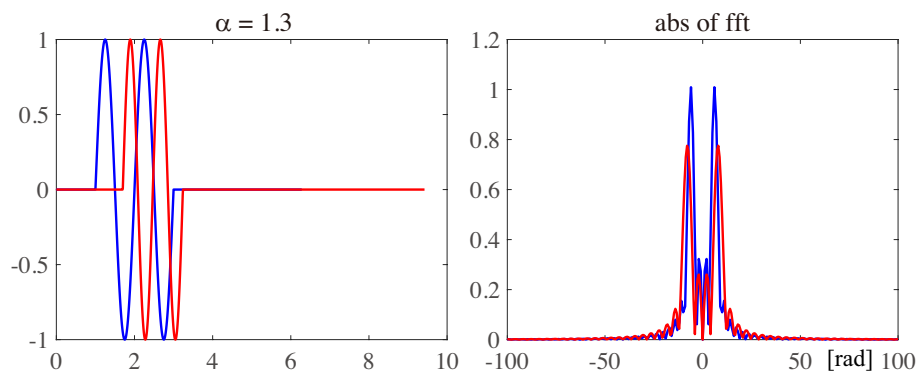


図 3: 左：青元信号，赤： $\alpha = 1.3$ で原点がずれている信号．右：それぞれのフーリエ変換の絶対値（ただし周波数軸を $[-100, 100]$ [rad] で切った）．

である．それぞれのフーリエ変換の絶対値を描くと図 3 右になる．

フーリエ変換の絶対値を p 乗し， α を推定すると，図 4 および図 5 になる． $p = 3$ 以上にとると， $\alpha = 1.3$ と推定できる．ただし， $\omega = p - 1$ のところで，ゼロ割になり計算できない．

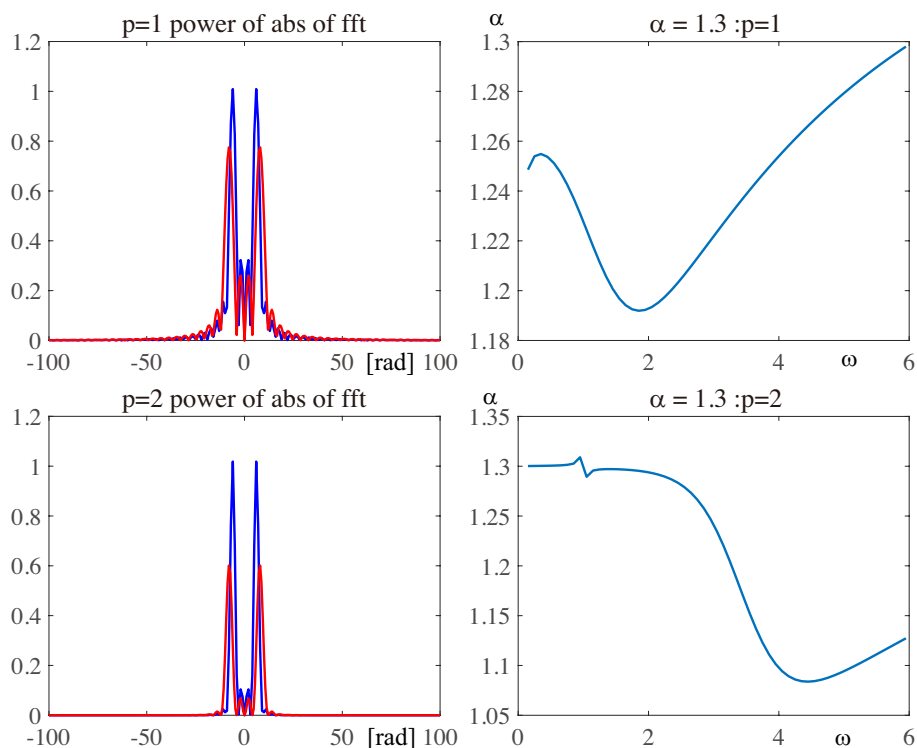


図 4: 左：フーリエ変換の絶対値の $p = 1, 2$ 乗．右： $\alpha = 1.3$ の推定（横軸 ω ）．

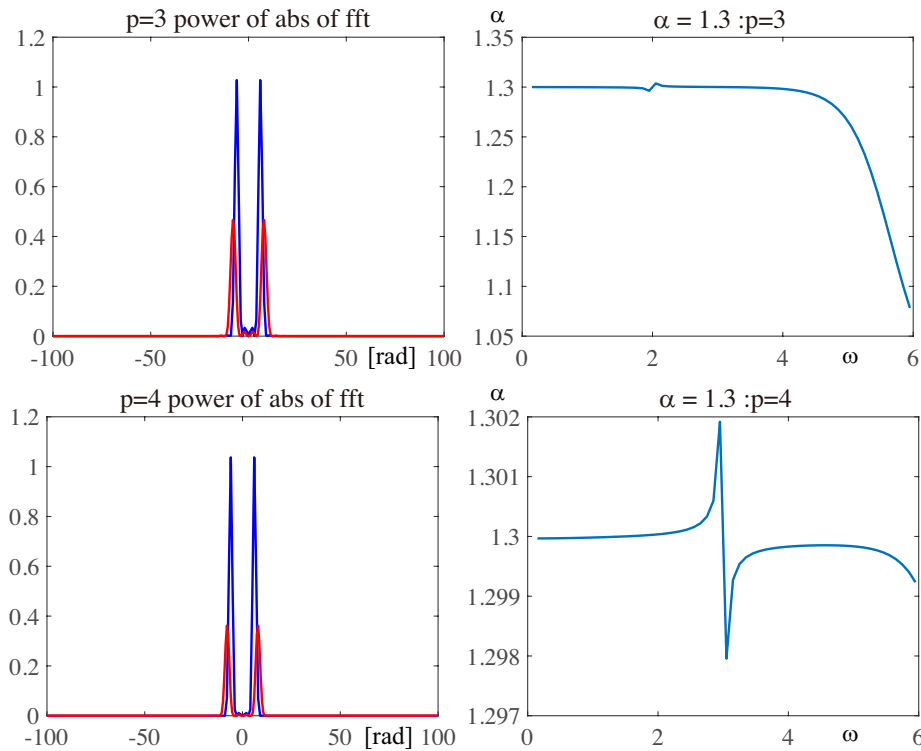


図 5: 左 : フーリエ変換の絶対値の $p = 3, 4$ 乗. 右 : $\alpha = 1.3$ の推定 (横軸 ω).

5 2次元関数に対する Mellin 変換・作用素

Mellin 変換は, 1 次元の区間 $[0, \infty)$ で定義された関数に対する変換であるから, 2 次元の関数・画像に対しては, (r, θ) で極座標表示し, 各 θ ごとに動径 r 方向に Mellin 変換を行う.

ここでは, Mellin 変換を原点からの距離 t の ω 乗に関数値 $f(t)$ をかけた積分と考えて, そのまま 2 次元に拡張した Mellin 作用素も定義する.

5.1 画像の極座標表示を用いた Mellin 変換

画像の左上を原点として, 図 6 左のように極座標 (r, θ) を入れる. θ の範囲は $0 \leq \theta \leq 90$ 度である.

図 7 左のバーバラさんの一部とそれを $\alpha = 0.73$ 倍に縮小した中図で θ を 0 度から 90 度まで, 0.5 度刻みで, ω を 1 から 10 まで 0.1 刻みで動かして α の値を計算すると図 8 左を得る. 縦方向が θ で上側が 0 度, 下側が 90 度である. 横方向が ω で左端が $\omega = 1$, 右端が $\omega = 10$ である. カラーバーから α の値は, 0.71 から 0.74 の間であることが分かる. 図 8 右には, 左図の α の値の分布状態をヒストグラムとして表示した.

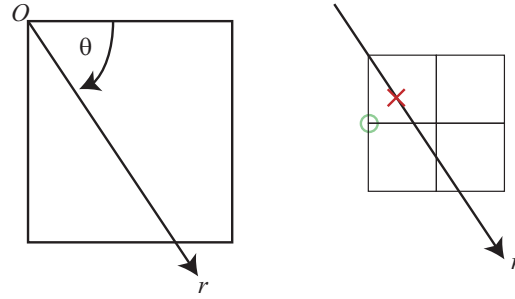


図 6: 左：画像の極座標表示．右：極座標表示された (r, θ) の位置 $\times$ に一番近い画素 $\circ$ の輝度を関数値とする．

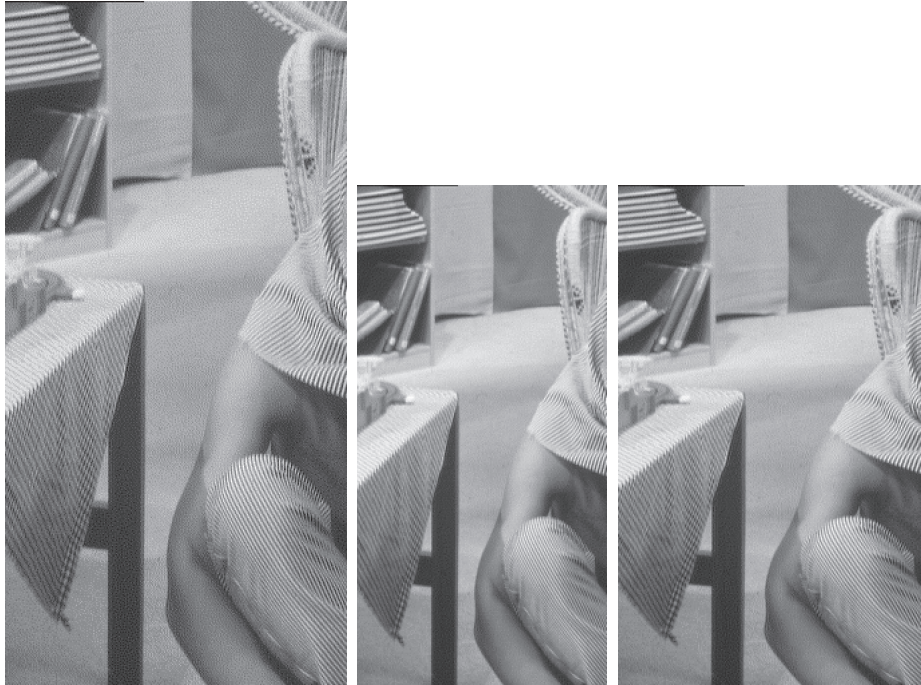


図 7: 左：バーバラさんの一部．中：その 0.73 倍．右：縦方向 0.73 倍，横方向 0.91 倍．

つぎに，図 7 右図のバーバラさんの一部を縦方向に $\alpha_1 = 0.73$ 倍，横方向に $\alpha_2 = 0.91$ 倍した画像に対して， α を計算する．計算結果を図 9 に示す．

5.2 2 次元 Mellin 作用素 その 1

$\mathbb{R}^2$ で定義された関数 $f(x_1, x_2)$ に対して，Mellin 作用素を

$$\mathcal{M}f(\omega) = \int_{\mathbb{R}^2} f(x_1, x_2) (x_1^2 + x_2^2)^{\omega/2} dx_1 dx_2$$

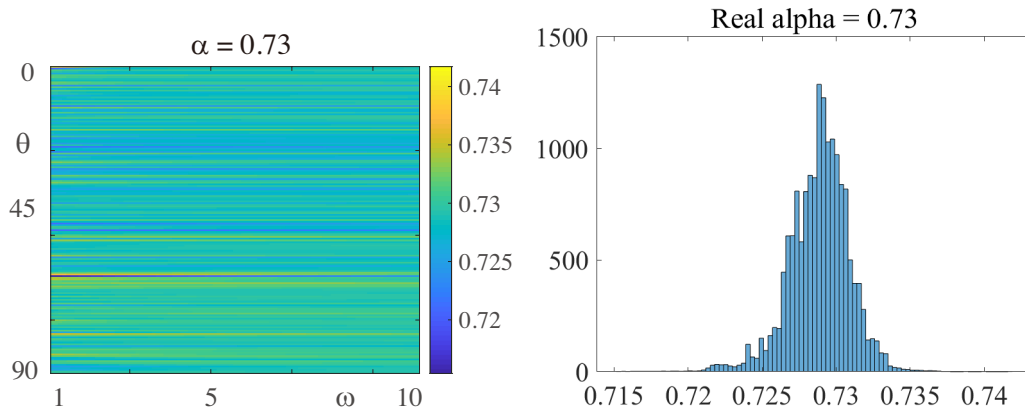


図 8: バーバラさんの一部とその 0.73 倍を Mellin 変換する．左： α を角度 θ ， ω に対して計算した図．右：左図の α の分布状態．

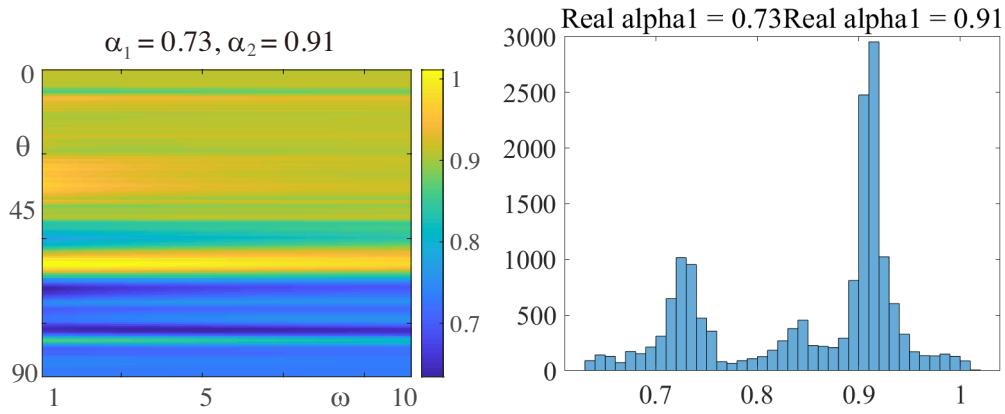


図 9: バーバラさんの一部とその縦 0.73 倍，横 0.91 倍を Mellin 変換する．左： α を角度 θ ， ω に対して計算した図．右：左図の α の分布状態．縦方向の $\alpha_1 = 0.73$ 倍と横方向の $\alpha_2 = 0.91$ 倍が現れる．

で定義すると，スケール変換 $f_\alpha(x_1, x_2) = f(\alpha x_1, \alpha x_2)$ に対しては，

$$\begin{aligned} \mathcal{M}f_\alpha(\omega) &= \int_{\mathbb{R}^2} f(\alpha x_1, \alpha x_2) (x_1^2 + x_2^2)^{\omega/2} dx_1 dx_2 \\ &= \int_{\mathbb{R}^2} f(y_1, y_2) \left(\frac{y_1^2 + y_2^2}{\alpha^2} \right)^{\omega/2} \frac{dy_1}{\alpha} \frac{dy_2}{\alpha} \\ &= \alpha^{-(\omega+2)} \mathcal{M}f(\omega) \end{aligned}$$

の関係が成立する。したがって、 α を求めると、

$$\alpha^{\omega+2} = \frac{\mathcal{M}f(\omega)}{\mathcal{M}f_\alpha(\omega)} \quad \Rightarrow \quad \alpha = \left(\frac{\mathcal{M}f(\omega)}{\mathcal{M}f_\alpha(\omega)} \right)^{\frac{1}{\omega+2}}$$

である。この方法で、図 7 左と中のバーバラさんの一部とその 0.73 倍に対して、 α を推定すると、図 10 であり、1 から 15 までの ω に対して、 $\alpha = 0.73$ で一定なことが分かる。

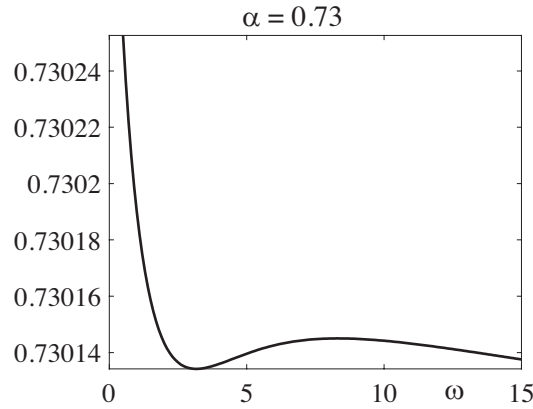


図 10: バーバラさん的一部分とその 0.73 倍を Mellin 作用素を用いて α を計算する。横軸 ω に対して、ほぼ $\alpha = 0.73$ で一定であることが分かる。

5.3 2 次元 Mellin 作用素 その 2

$\mathbb{R}^2$ で定義された関数 $f(x_1, x_2)$ に対して、Mellin 作用素を

$$\mathcal{M}_2 f(\omega_1, \omega_2) = \int_{\mathbb{R}^2} f(x_1, x_2) |x_1|^{\omega_1} |x_2|^{\omega_2} dx_1 dx_2$$

で定義する。スケール $\alpha = (\alpha_1, \alpha_2) \in \mathbb{R}_+$ をとり、スケール変換 $f_\alpha(x_1, x_2) = f(\alpha_1 x_1, \alpha_2 x_2)$ に対しては、

$$\begin{aligned} \mathcal{M}_2 f_\alpha(\omega_1, \omega_2) &= \int_{\mathbb{R}^2} f(\alpha_1 x_1, \alpha_2 x_2) |x_1|^{\omega_1} |x_2|^{\omega_2} dx_1 dx_2 \\ &= \int_{\mathbb{R}^2} f(y_1, y_2) \left| \frac{y_1}{\alpha_1} \right|^{\omega_1} \left| \frac{y_2}{\alpha_2} \right|^{\omega_2} \frac{dy_1}{\alpha_1} \frac{dy_2}{\alpha_2} \\ &= \alpha_1^{-(\omega_1+1)} \alpha_2^{-(\omega_2+1)} \mathcal{M}_2 f(\omega_1, \omega_2) \end{aligned}$$

の関係が成立する。したがって、比を

$$\mathcal{R}_\alpha(\omega_1, \omega_2) = \frac{\mathcal{M}_2 f(\omega_1, \omega_2)}{\mathcal{M}_2 f_\alpha(\omega_1, \omega_2)} = \alpha_1^{(\omega_1+1)} \alpha_2^{(\omega_2+1)}$$

とする．両辺の対数を取ると

$$\log(\mathcal{R}_\alpha(\omega_1, \omega_2)) = (\omega_1 + 1) \log(\alpha_1) + (\omega_2 + 1) \log(\alpha_2) \quad (6)$$

と ω_1, ω_2 の平面の方程式である．図 7 右のバーバラさんの一部を縦方向 0.73 倍，横方向 0.91 倍した画像なので， $\alpha_1 = 1/0.73 = 1.37$, $\log(\alpha_1) = 0.315$, $\alpha_2 = 1/0.91 = 1.10$, $\log(\alpha_2) = 0.0943$ である．このとき， $\log(\mathcal{R}_\alpha(\omega_1, \omega_2))$ を描くと，図 11 であり，平面になることがわかる．

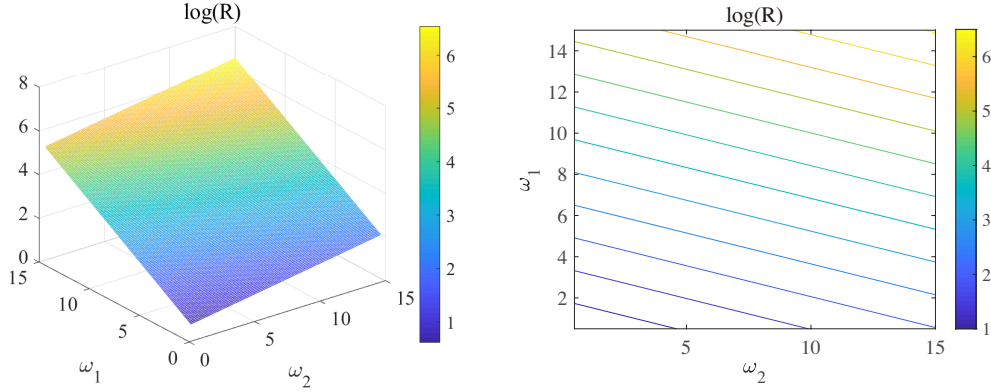


図 11: $\log(\mathcal{R}_\alpha(\omega_1, \omega_2))$ の 3D プロットと等高線．どちらも平面であることを示している．

さて，式 (6) のパラメータ $\beta_1 = \log(\alpha_1)$, $\beta_2 = \log(\alpha_2)$ を最小二乗法で推定しよう． n 番目のデータ $\omega^n = (\omega_1^n, \omega_2^n)$ に対して，二乗誤差の総和

$$E(\beta_1, \beta_2) = \sum_n [\beta_1(\omega_1^n + 1) + \beta_2(\omega_2^n + 1) - \log(\mathcal{R}_\alpha(\omega_1^n, \omega_2^n))]^2 \quad (7)$$

に対して，停留点 (β_1 偏微分と β_2 偏微分が同時に 0 になる点) を求める．すなわち，

$$\begin{cases} \frac{\partial E}{\partial \beta_1} = 2 \sum_n (\omega_1^n + 1) [\beta_1(\omega_1^n + 1) + \beta_2(\omega_2^n + 1) - \log(\mathcal{R}_\alpha(\omega_1^n, \omega_2^n))] = 0, \\ \frac{\partial E}{\partial \beta_2} = 2 \sum_n (\omega_2^n + 1) [\beta_1(\omega_1^n + 1) + \beta_2(\omega_2^n + 1) - \log(\mathcal{R}_\alpha(\omega_1^n, \omega_2^n))] = 0 \end{cases}$$

という， β_1, β_2 変数の連立一次方程式を解けば良い．整頓すると，

$$\begin{cases} \left[\sum_n (\omega_1^n + 1)^2 \right] \beta_1 + \left[\sum_n (\omega_1^n + 1)(\omega_2^n + 1) \right] \beta_2 = \sum_n (\omega_1^n + 1) \log(\mathcal{R}_\alpha(\omega_1^n, \omega_2^n)), \\ \left[\sum_n (\omega_1^n + 1)(\omega_2^n + 1) \right] \beta_1 + \left[\sum_n (\omega_2^n + 1)^2 \right] \beta_2 = \sum_n (\omega_2^n + 1) \log(\mathcal{R}_\alpha(\omega_1^n, \omega_2^n)). \end{cases}$$

これを解くと,

$$\beta = \begin{pmatrix} 0.3041 \\ 0.1027 \end{pmatrix} \Rightarrow \alpha = e^\beta = \begin{pmatrix} 1.36 \\ 1.11 \end{pmatrix} \Rightarrow 1./\alpha = \begin{pmatrix} 0.738 \\ 0.902 \end{pmatrix}$$

と実際の拡大・縮小比に近い値が出る.

6 2次元フーリエスペクトルの Mellin 作用素

2変数関数 $f(x_1, x_2)$ のフーリエ変換を

$$\widehat{f}(\xi_1, \xi_2) = \int_{\mathbb{R}^2} f(x_1, x_2) e^{-i(x_1\xi_1 + x_2\xi_2)} dx_1 dx_2$$

で定義すると, スケール変換 $f_\alpha(x_1, x_2) = f(\alpha x_1, \alpha x_2)$ のフーリエ変換は, $y_1 = \alpha x_1$, $y_2 = \alpha x_2$ と変数変換すると, $dy_1 dy_2 = \alpha^2 dx_1 dx_2$ なので,

$$\begin{aligned} \widehat{f}_\alpha(\xi_1, \xi_2) &= \int_{\mathbb{R}^2} f(\alpha x_1, \alpha x_2) e^{-i(x_1\xi_1 + x_2\xi_2)} dx_1 dx_2 \\ &= \int_{\mathbb{R}^2} f(y_1, y_2) e^{-i(y_1\xi_1 + y_2\xi_2)/\alpha} \frac{dy_1 dy_2}{\alpha^2} \\ &= \frac{1}{\alpha^2} \widehat{f}\left(\frac{\xi_1}{\alpha}, \frac{\xi_2}{\alpha}\right) \end{aligned}$$

である. 絶対値を取って, $|\widehat{f}(\xi_1, \xi_2)|$ と $|\widehat{f}_\alpha(\xi_1, \xi_2)|$ の $p > 0$ 乗の Mellin 作用素を考えると,

$$\begin{aligned} \mathcal{M}|\widehat{f}|(p, \omega) &= \int_{\mathbb{R}^2} |\widehat{f}(\xi_1, \xi_2)|^p (\xi_1^2 + \xi_2^2)^{\omega/2} d\xi_1 d\xi_2 \\ \mathcal{M}|\widehat{f}_\alpha|(p, \omega) &= \int_{\mathbb{R}^2} |\widehat{f}_\alpha(\xi_1, \xi_2)|^p (\xi_1^2 + \xi_2^2)^{\omega/2} d\xi_1 d\xi_2 \\ &= \int_{\mathbb{R}^2} \left| \frac{1}{\alpha^2} \widehat{f}\left(\frac{\xi_1}{\alpha}, \frac{\xi_2}{\alpha}\right) \right|^p (\xi_1^2 + \xi_2^2)^{\omega/2} d\xi_1 d\xi_2 \\ &= \int_{\mathbb{R}^2} \frac{1}{\alpha^{2p}} |\widehat{f}(\eta_1, \eta_2)|^p (\alpha^2 \eta_1^2 + \alpha^2 \eta_2^2)^{\omega/2} \alpha^2 d\eta_1 d\eta_2 \\ &= \alpha^{\omega+2-2p} \mathcal{M}|\widehat{f}|(p, \omega) \end{aligned}$$

ただし, $\eta_1 = \xi_1/\alpha$, $\eta_2 = \xi_2/\alpha$, $d\eta_1 d\eta_2 = d\xi_1 d\xi_2/\alpha^2$ とおき変えた. 従って, α を求めるためには, $\mathcal{M}|\widehat{f}|(p, \omega)$ と $\mathcal{M}|\widehat{f}_\alpha|(p, \omega)$ の商を取って,

$$\alpha^{\omega+2-2p} = \frac{\mathcal{M}|\widehat{f}_\alpha|(p, \omega)}{\mathcal{M}|\widehat{f}|(p, \omega)} \Rightarrow \alpha = \left(\frac{\mathcal{M}|\widehat{f}_\alpha|(p, \omega)}{\mathcal{M}|\widehat{f}|(p, \omega)} \right)^{\frac{1}{\omega+2-2p}}$$

で求まる.

謝辞

本研究は, 大阪教育大学と AIMaP と科研費 (C) 17K05363 の補助を受けている.

参考文献

- [1] R. Godement, Analysis III, Analytic and Differential Functions, Manifolds and Riemann Surfaces, Springer, 2015.
- [2] Wolfram MathWorld の Mellin Transform のページ <http://mathworld.wolfram.com/MellinTransform.html> : 2019 年 12 月 5 日.
- [3] Wikipedia の Mellin transform のページ https://en.wikipedia.org/wiki/Mellin_transform : 2019 年 12 月 5 日.