Cuntz algebras, generalized Walsh bases and applications

Gabriel Picioroaga

November 9, 2013
INFAS

Basics

$H_{\langle\,,\,\rangle}$ separable Hilbert space, $(e_n)_{n\in\mathbb{N}}$ ONB in H:

$$\langle e_n\,,\,e_m\rangle = \delta_{n,m}$$

$$\overline{span}\{e_n\} = H$$

$$v = \sum_{k=1}^{\infty} \langle v\,,\,e_k\rangle\, e_k \iff \lim_{n\to\infty} ||v - \sum_{k=1}^{n} \langle v\,,\,e_k\rangle\, e_k|| = 0$$

Basics

$H_{\langle\,,\,\rangle}$ separable Hilbert space, $(e_n)_{n\in\mathbb{N}}$ ONB in H:

$$\langle e_n\,,\,e_m\rangle = \delta_{n,m}$$

$$\overline{span}\{e_n\} = H$$

$$v = \sum_{k=1}^{\infty} \langle v\,,\,e_k\rangle\, e_k \iff \lim_{n\to\infty} ||v - \sum_{k=1}^{n} \langle v\,,\,e_k\rangle\, e_k|| = 0$$

In applications:
$H = L^2$ space and v encodes a *signal, state, image, measurable function*.

"Good" Approximation: least mean square deviation

Example

- Fourier: $(\frac{1}{\sqrt{2\pi}} e^{inx})_{n \in \mathbb{Z}}$ ONB on $L^2[-\pi, \pi]$
- Wavelet : $\{2^{n/2}\psi(2^n t - k) \mid n, k \in \mathbb{Z}\}$ ONB in $L^2(\mathbb{R})$
- Walsh: discrete sine-cosine versions, ± 1 on dyadic intervals
- $(exp(\lambda \cdot 2\pi x)_{\lambda \in \Lambda}$ exponential bases on some L^2(fractals)

Main ideas and layout of the talk:

- *Cuntz relations generate a diversity of bases: Examples, Old and New (generalized Walsh)*
- *Zoom in on the new Walsh, study structure properties (How different from the old one is it ?)*
- *Possible applications of the generalized Walsh.*

Set Up

R- $d \times d$ expansive. $B \subset \mathbb{R}^d$, $N = |B|$. IFS:

$$\tau_b(x) = R^{-1}(x + b) \quad (x \in \mathbb{R}^d,\ b \in B)$$

Hutchinson: $\exists!$ attractor (X_B, μ_B) invariant for the IFS.
μ_B is invariant for $r : X_B \to X_B$

$$r(x) = \tau_b^{-1}(x),\ \text{if } x \in \tau_b(X_B)$$

Set Up

R- $d \times d$ expansive. $B \subset \mathbb{R}^d$, $N = |B|$. IFS:

$$\tau_b(x) = R^{-1}(x+b) \quad (x \in \mathbb{R}^d,\ b \in B)$$

Hutchinson: $\exists!$ attractor (X_B, μ_B) invariant for the IFS.
μ_B is invariant for $r : X_B \to X_B$

$$r(x) = \tau_b^{-1}(x),\ \textit{if } x \in \tau_b(X_B)$$

Example

IFS : $\tau_j(x) = \frac{x+j}{N}$, $j = 0, 1, ..., N-1$

Attractor: $X = [0,1]$, with λ the Lebesgue measure

$r(x) = Nx \bmod 1$

IFS : $\tau_j(x) = \frac{x+j}{N}$, $j = 0, 1, ..., N-1$

Cuntz Relations

Definition

$$\mathcal{O}_N : \qquad S_i^* S_j = \delta_{i,j} I, \qquad \sum_{i=0}^{N-1} S_i S_i^* = I$$

QMFs

QMF basis $\Longrightarrow$ *multiresolution for the wavelet representation associated to a filter* m_0.

Definition

A *QMF basis* is a set of N QMF's $m_0, m_1, \ldots, m_{N-1}$ such that

$$\frac{1}{N} \sum_{r(w)=z} m_i(w)\overline{m_j}(w) = \delta_{ij}, \quad (i, j \in \{0, \ldots, N-1\}, z \in X)$$

QMF bases and Cuntz algebra representations

Proposition

Let $(m_i)_{i=0}^{N-1}$ *be a QMF basis. The operators on* $L^2(X, \mu)$

$$S_i(f) = m_i f \circ r, \quad i = 0, \dots, N-1$$

are isometries and form a representation of the Cuntz algebra $\mathcal{O}_N$.

Main Result

Theorem

$\mathcal{H}$ Hilbert space, $(S_i)_{i=0}^{N-1}$ Cuntz representation of $\mathcal{O}_N$.
$\mathcal{E}$ orthonormal, X top.space, $f : X \to \mathcal{H}$ norm continuous function and:

Main Result

Theorem

$\mathcal{H}$ *Hilbert space,* $(S_i)_{i=0}^{N-1}$ *Cuntz representation of* $\mathcal{O}_N$.
$\mathcal{E}$ *orthonormal,* X *top.space,* $f : X \to \mathcal{H}$ *norm continuous function and:*

1. $\mathcal{E} = \cup_{i=0}^{N-1} S_i \mathcal{E}$.
2. $\overline{\text{span}}\{f(t) : t \in X\} = \mathcal{H}$ *and* $||f(t)|| = 1$, *for all* $t \in X$.

Main Result

Theorem

$\mathcal{H}$ *Hilbert space,* $(S_i)_{i=0}^{N-1}$ *Cuntz representation of* $\mathcal{O}_N$.
$\mathcal{E}$ *orthonormal,* X *top.space,* $f : X \to \mathcal{H}$ *norm continuous function and:*

1. $\mathcal{E} = \cup_{i=0}^{N-1} S_i \mathcal{E}$.
2. $\overline{\text{span}}\{f(t) : t \in X\} = \mathcal{H}$ *and* $||f(t)|| = 1$, *for all* $t \in X$.
3. *on the range of* f *the Cuntz isometries are like "multiplication-dilation" operators*
4. $\exists\ c_0 \in X$ *such that* $f(c_0) \in \overline{\text{span}}\mathcal{E}$.

Main Result

Theorem

$\mathcal{H}$ *Hilbert space*, $(S_i)_{i=0}^{N-1}$ *Cuntz representation of* $\mathcal{O}_N$.
$\mathcal{E}$ *orthonormal*, X *top.space*, $f : X \to \mathcal{H}$ *norm continuous function and:*

1. $\mathcal{E} = \cup_{i=0}^{N-1} S_i \mathcal{E}$.
2. $\overline{\text{span}}\{f(t) : t \in X\} = \mathcal{H}$ *and* $||f(t)|| = 1$, *for all* $t \in X$.
3. *on the range of* f *the Cuntz isometries are like "multiplication-dilation" operators*
4. $\exists\ c_0 \in X$ *such that* $f(c_0) \in \overline{\text{span}}\mathcal{E}$.
5. *If the Ruelle (transfer) operator admits as fixed point a function* h *constant on* $f^{-1}(\text{span}\mathcal{E})$ *then* h *is constant.*

Main Result

Theorem

$\mathcal{H}$ *Hilbert space,* $(S_i)_{i=0}^{N-1}$ *Cuntz representation of* $\mathcal{O}_N$.
$\mathcal{E}$ *orthonormal*, X *top.space,* $f : X \to \mathcal{H}$ *norm continuous function and:*

1. $\mathcal{E} = \cup_{i=0}^{N-1} S_i \mathcal{E}$.
2. $\overline{\text{span}}\{f(t) : t \in X\} = \mathcal{H}$ *and* $||f(t)|| = 1$, *for all* $t \in X$.
3. *on the range of* f *the Cuntz isometries are like "multiplication-dilation" operators*
4. $\exists\ c_0 \in X$ *such that* $f(c_0) \in \overline{\text{span}}\mathcal{E}$.
5. *If the Ruelle (transfer) operator admits as fixed point a function* h *constant on* $f^{-1}(span\mathcal{E})$ *then* h *is constant.*

Then $\mathcal{E}$ *is an orthonormal basis for* $\mathcal{H}$.

In applications:

- $f(t) = exp_t$ *on* $L^2(X_B, \mu_B)$

- $S_l(g) = e_l g \circ r$, (B, L) *Hadamard pair*
- $S_i(g) = m_i g \circ r$, $m_i = \sqrt{N} \sum_{j=0}^{N-1} a_{ij} \chi_{[j/N,(j+1)/N]}$

- $\mathcal{E} = \{S_{l_1} \circ S_{l_2} \circ \cdots \circ S_{l_n}(exp_{-c})\}$, *c extreme cycle point.*
- $\mathcal{E} = \{S_{i_1} \circ S_{i_2} \circ \cdots \circ S_{i_n}(\mathbf{1})\}$

Consequences

1-dimensional: $0 \in B \subset \mathbb{R}$, $R > 1$, $\frac{1}{R}B$ admits a set L as *spectrum*.

C1. $\mathcal{E} = \{S_w(exp_{-c}) : c$ *extreme cycle point*$\}$ *is ONB in* $L^2(\mu_B)$ *made of piecewise exponential functions.*

$$S_{l_1}...S_{l_n}e_{-c}(x) = e_{l_1}(x)e_{l_2}(rx)...e_{l_n}(r^{n-1}x)e_c(r^nx)$$

C2. When $B \subset \mathbb{Z}$, $L \subset \mathbb{Z}$, *and* $R \in \mathbb{Z}$ *then* $\exists\Lambda$ *such that* $\{e_\lambda : \lambda \in \Lambda\}$ *is ONB for* $L^2(\mu_B)$.

Consequences

1-dimensional: $0 \in B \subset \mathbb{R}$, $R > 1$, $\frac{1}{R}B$ admits a set L as *spectrum*.

C1. $\mathcal{E} = \{S_w(exp_{-c}) : c$ *extreme cycle point*$\}$ *is ONB in* $L^2(\mu_B)$ *made of piecewise exponential functions.*

$$S_{l_1}...S_{l_n}e_{-c}(x) = e_{l_1}(x)e_{l_2}(rx)...e_{l_n}(r^{n-1}x)e_c(r^n x)$$

C2. When $B \subset \mathbb{Z}$, $L \subset \mathbb{Z}$, *and* $R \in \mathbb{Z}$ *then* $\exists \Lambda$ *such that* $\{e_\lambda : \lambda \in \Lambda\}$ *is ONB for* $L^2(\mu_B)$.

Example

Cantor's $(X_{1/4}, \mu_{1/4})$ admits exp ONB: $R = 4$, $B = \{0, 2\}$, spectrum $L = \{0, 1\}$

Example

$R = 3$, $B = \{0, 2\}$, $L = \{0, \frac{3}{4}\}$ spectrum of $\frac{1}{3}B$: Middle third Cantor set which is known not to admit exponential bases.

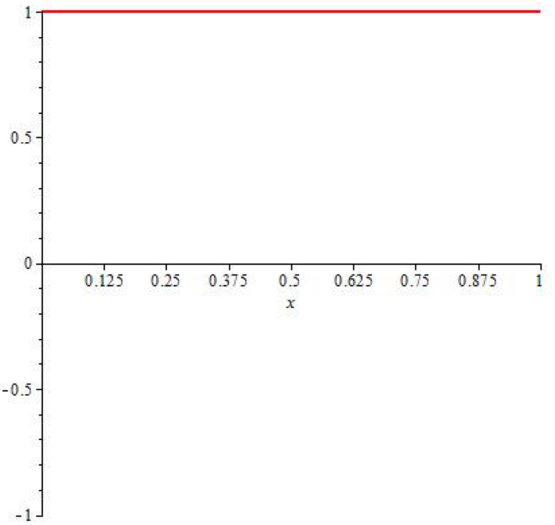
Consequences

C3. Walsh Bases: $[0,1]$ *is the attractor of the IFS:* $\tau_0 x = \frac{x}{2}$, $\tau_1 x = \frac{x+1}{2}$.
$rx = 2x mod 1$. $m_0 = 1$, $m_1 = \chi_{[0,1/2)} - \chi_{[1/2,1)}$ *form a QMF basis.*
$\mathcal{E} := \{S_w 1 : w \in \{0,1\}^*\}$ *is an ONB for* $L^2[0,1]$, *the Walsh basis.*

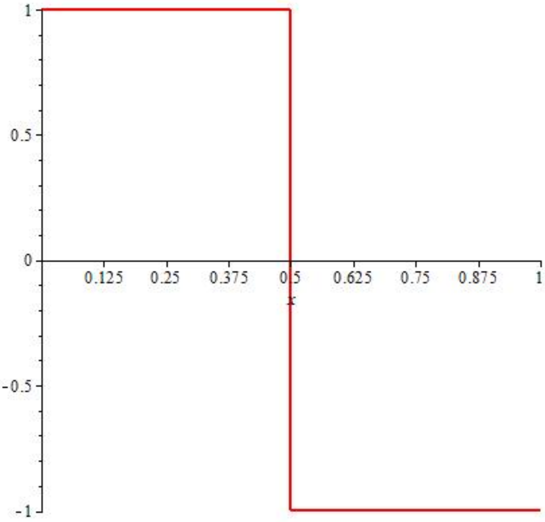
Description: For $n = \sum_{k=0}^{l} i_k 2^k$, the n'th Walsh function :

$$W_n(x) = m_{i_0}(x) \cdot m_{i_1}(rx) \cdots m_{i_l}(r^l x) = S_{i_0 i_1 \dots i_l} 1$$

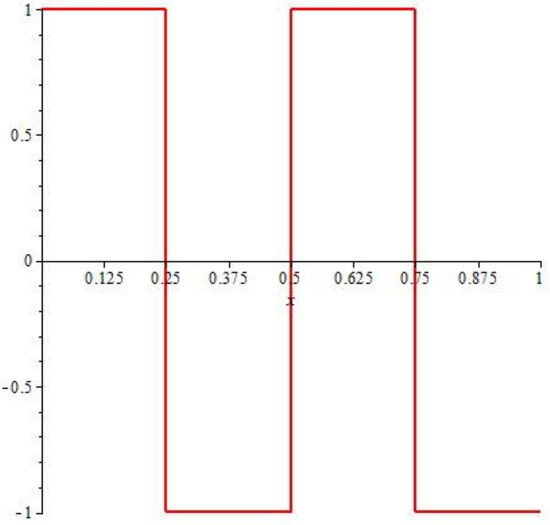
Walsh bases



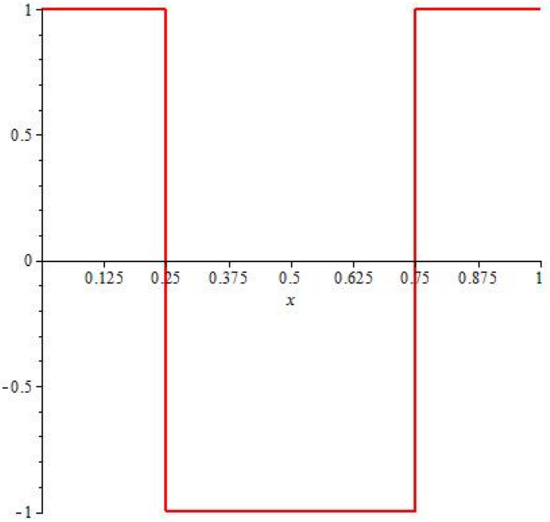
Walsh bases



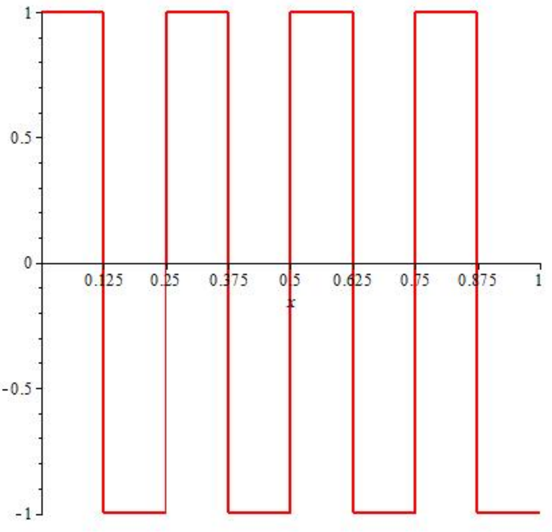
Walsh bases



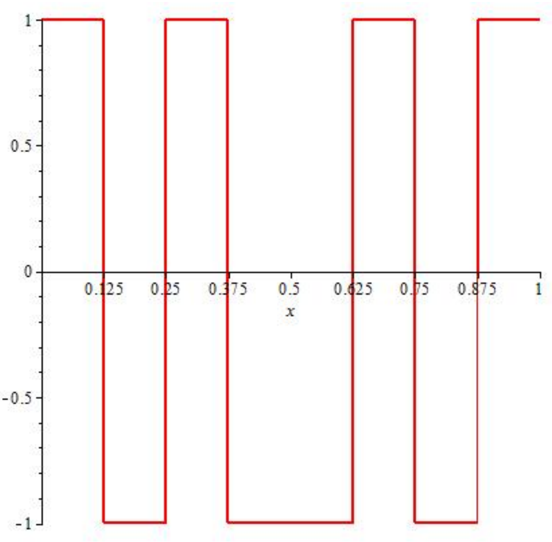
Walsh bases



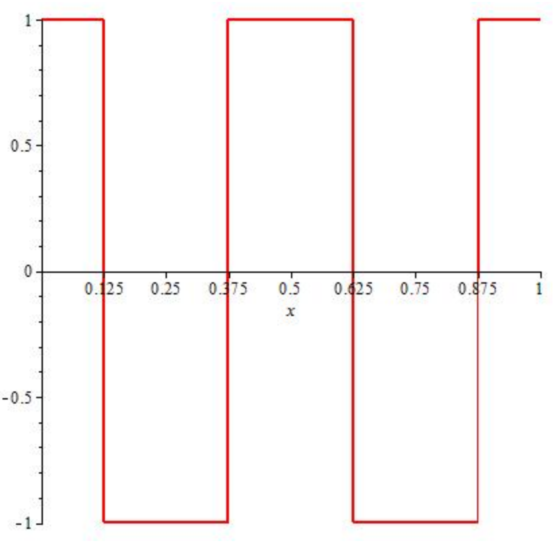
Walsh bases



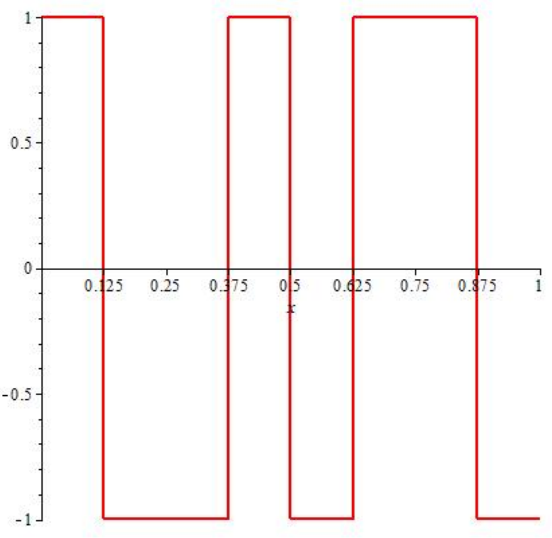
Walsh bases



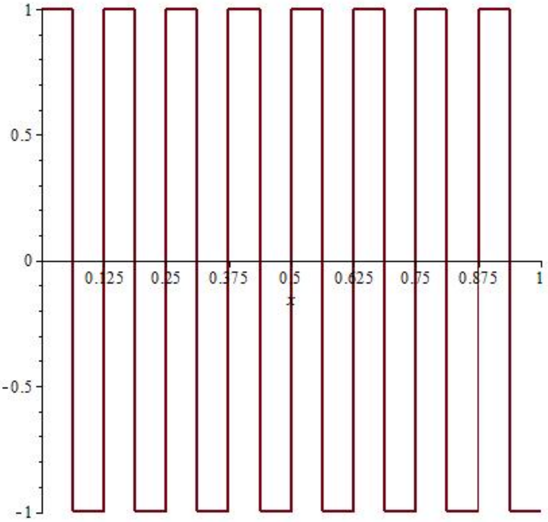
Walsh bases



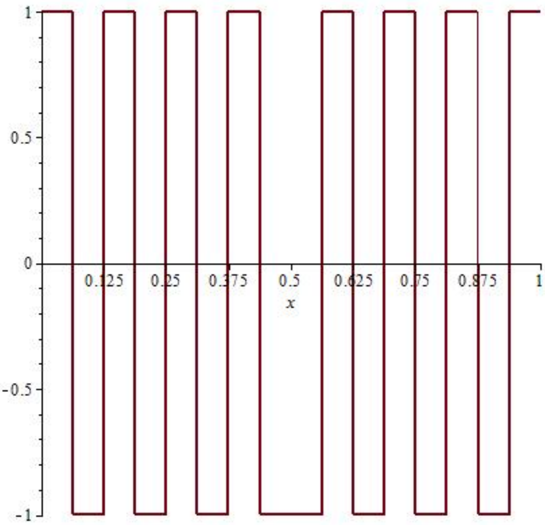
Walsh bases



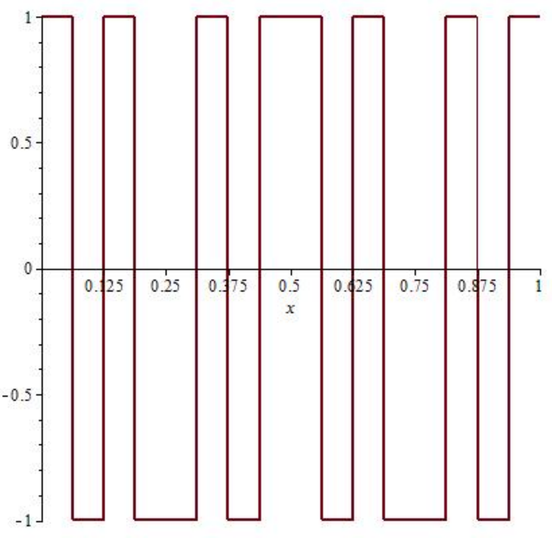
Walsh bases



Walsh bases



Walsh bases



Generalized Walsh bases

C4. *Let* $A = [a_{ij}]$ *a* $N \times N$ *unitary matrix,* $a_{1j} = \frac{1}{\sqrt{N}}$.

$$m_i(x) := \sqrt{N} \sum_{j=0}^{N-1} a_{ij} \chi_{[j/N,(j+1)/N]}(x)$$

$r(x) = Nx \bmod 1$, $n = \sum_{k=0}^{l} i_k N^k$ *with* $i_k \in \{0, 1, .., N-1\}$.

The n'th generalized Walsh function :

$$W_{n,A}(x) = m_{i_0}(x) \cdot m_{i_1}(rx) \cdots m_{i_l}(r^l x)$$

The set $(W_{n,A})_{n \in \mathbb{N}}$ *is ONB in* $L^2[0,1]$.

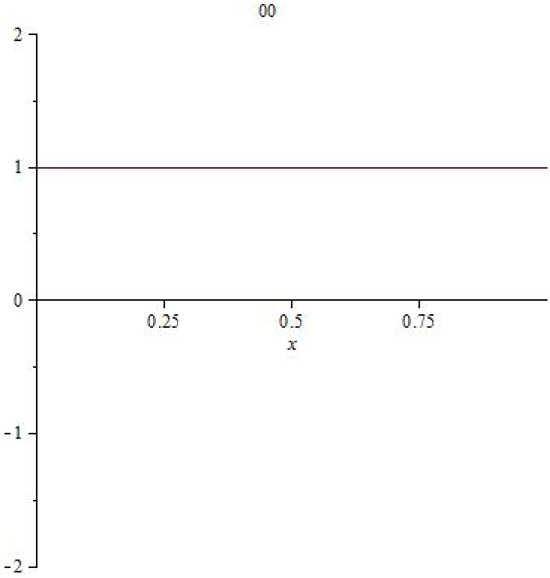
Generalized Walsh bases

Example

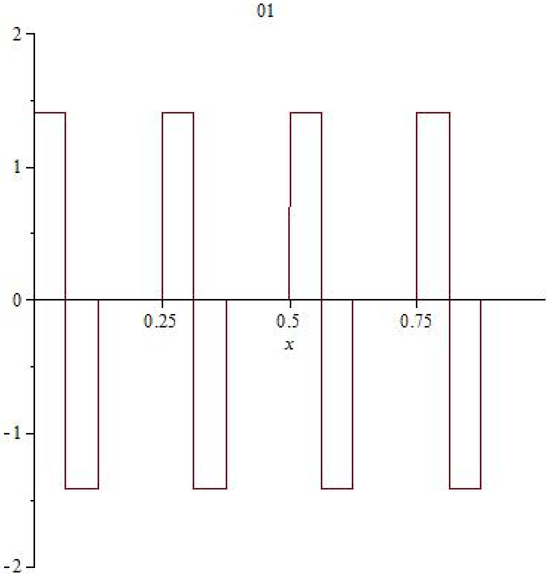
We will graph a few generalized Walsh functions that correspond to 4×4 matrix

$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 & 0 \\ 0 & 0 & \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

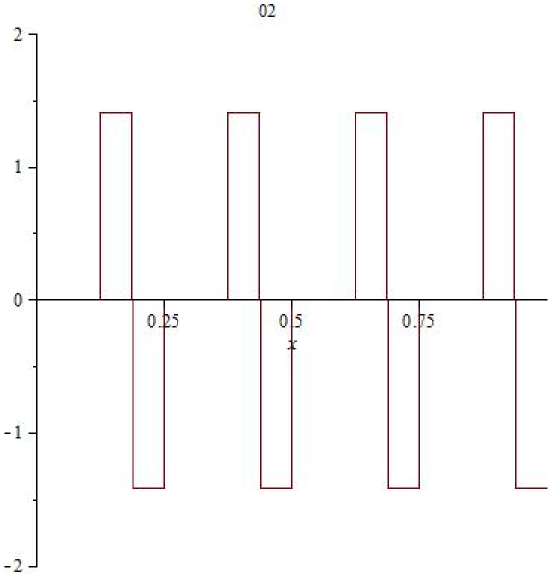
Generalized Walsh bases



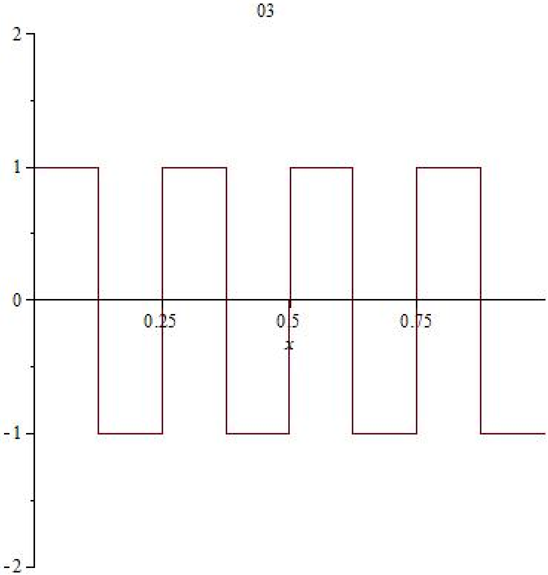
Generalized Walsh bases



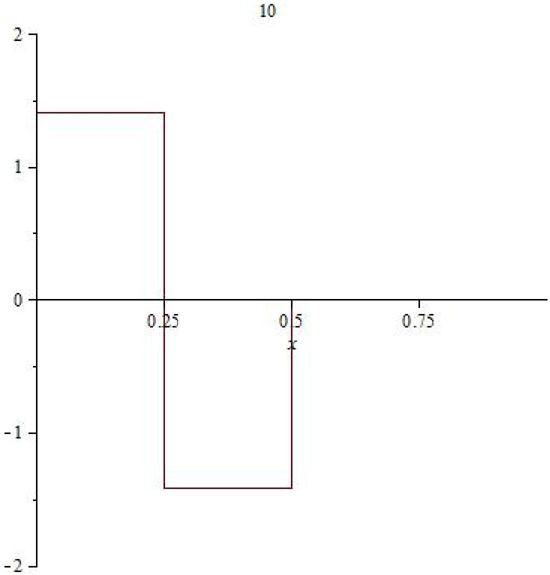
Generalized Walsh bases



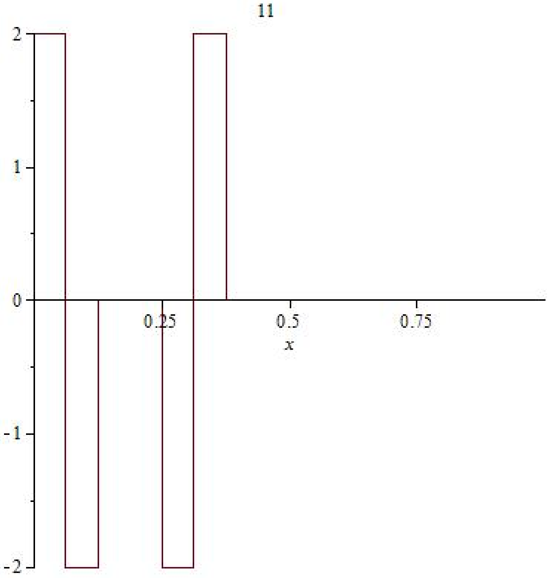
Generalized Walsh bases



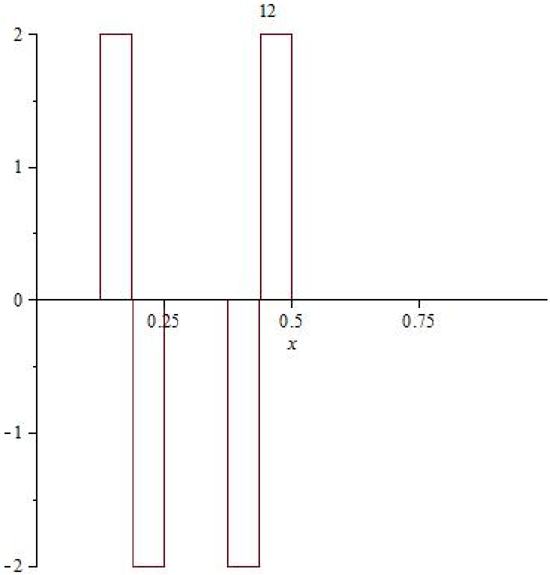
Generalized Walsh bases



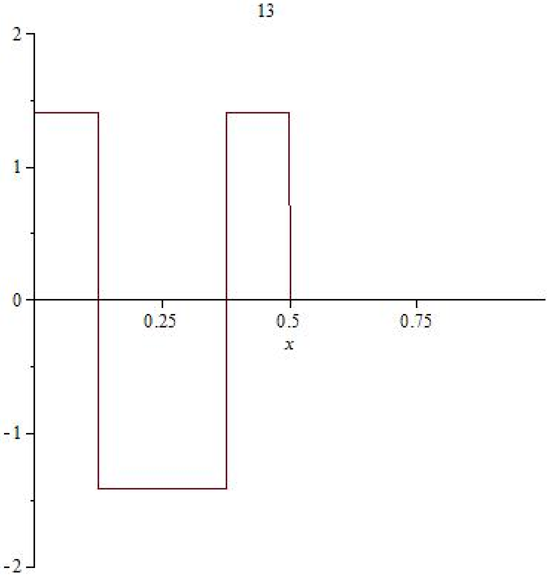
Generalized Walsh bases



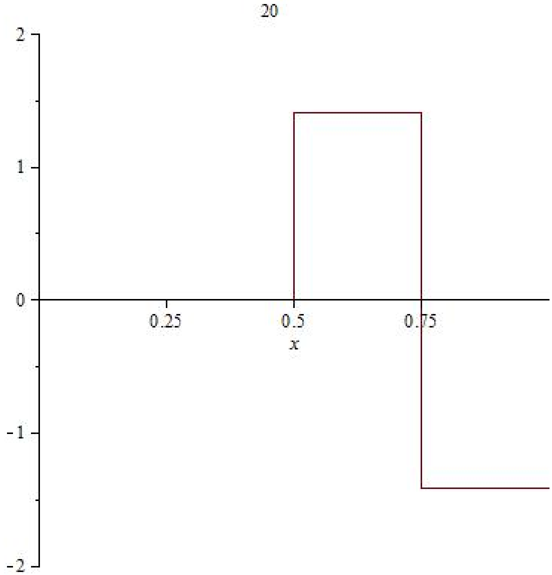
Generalized Walsh bases



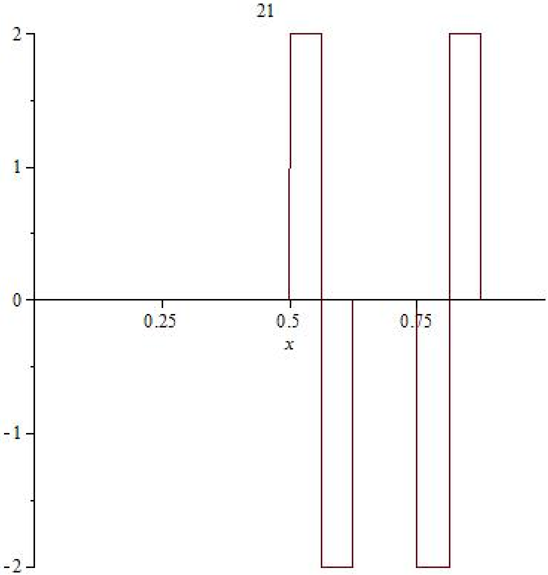
Generalized Walsh bases



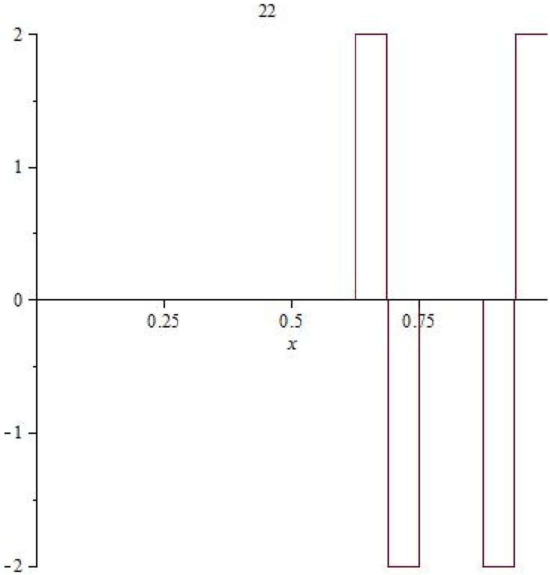
Generalized Walsh bases



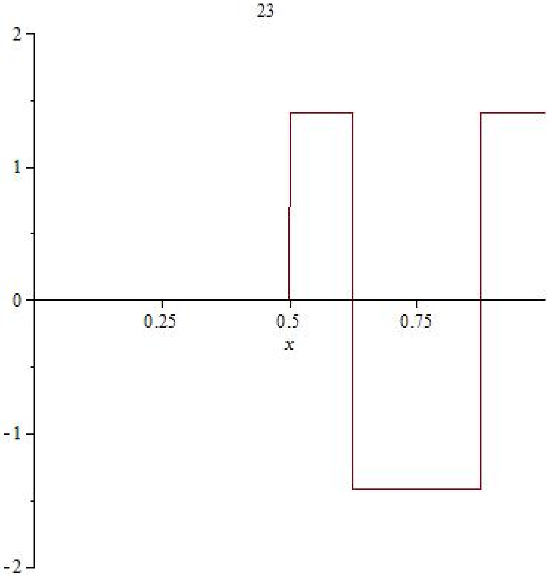
Generalized Walsh bases



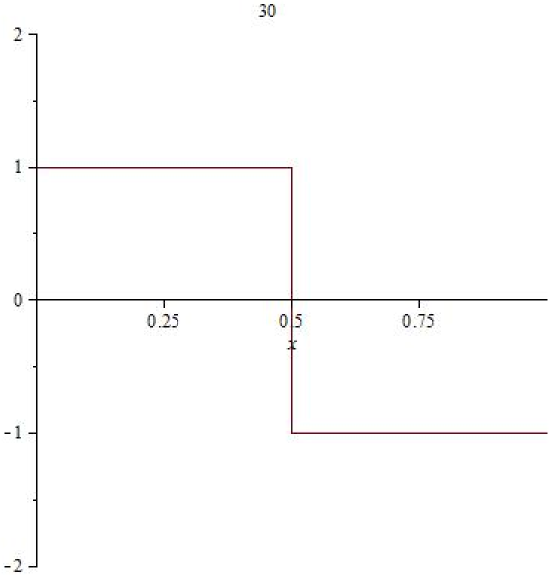
Generalized Walsh bases



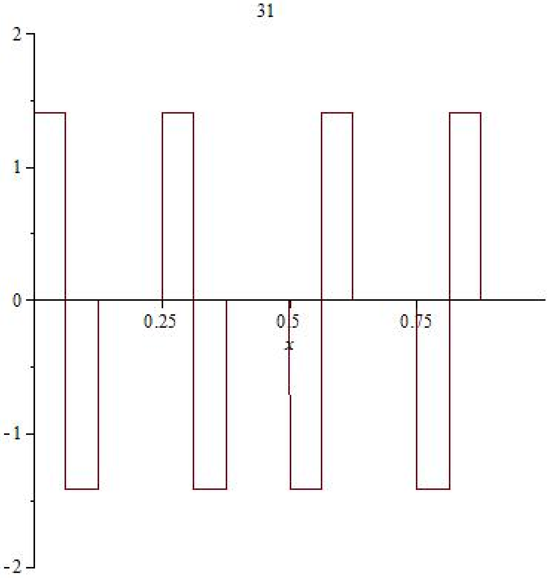
Generalized Walsh bases



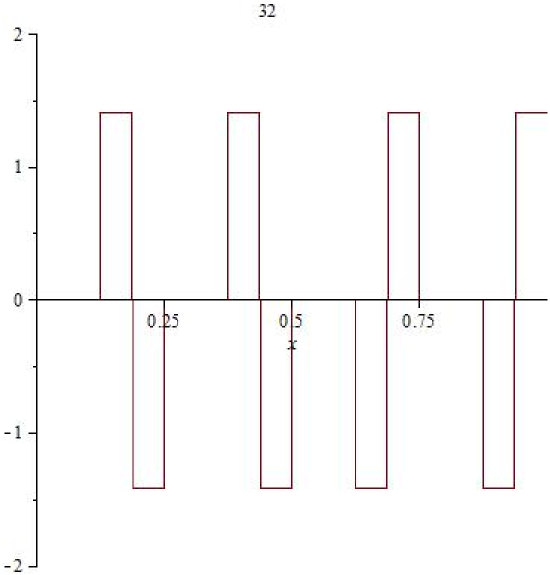
Generalized Walsh bases



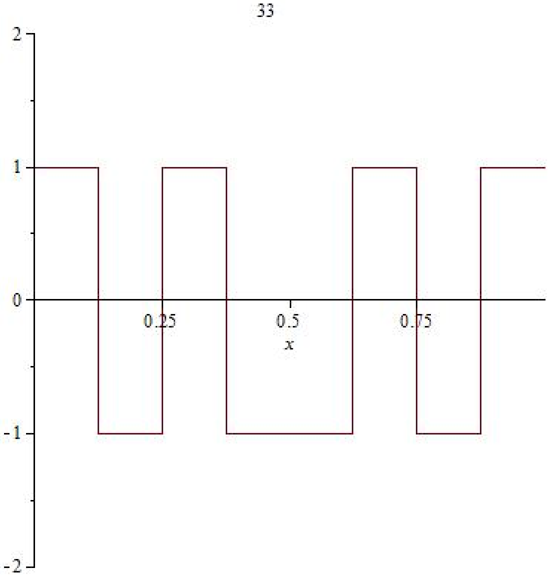
Generalized Walsh bases



Generalized Walsh bases



Generalized Walsh bases

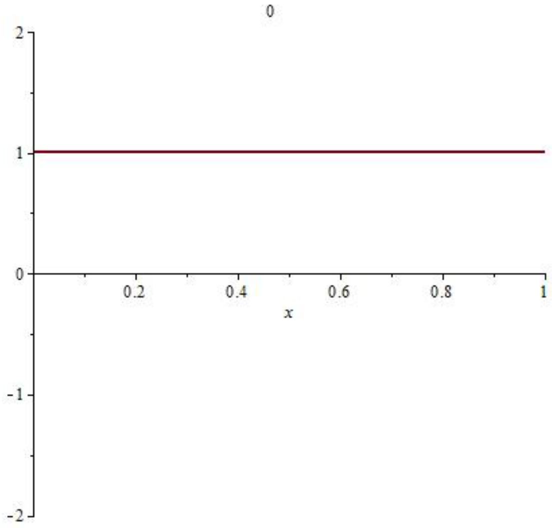


Example

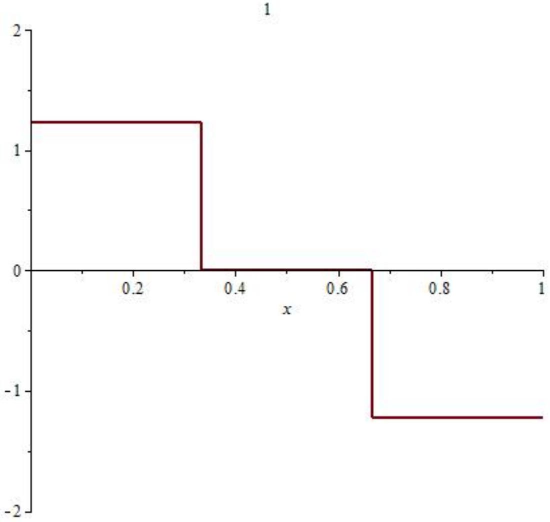
We will graph a few generalized Walsh functions that correspond to 3×3 matrix

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ -\frac{\sqrt{6}}{6} & \frac{\sqrt{6}}{3} & -\frac{\sqrt{6}}{6} \end{pmatrix}$$

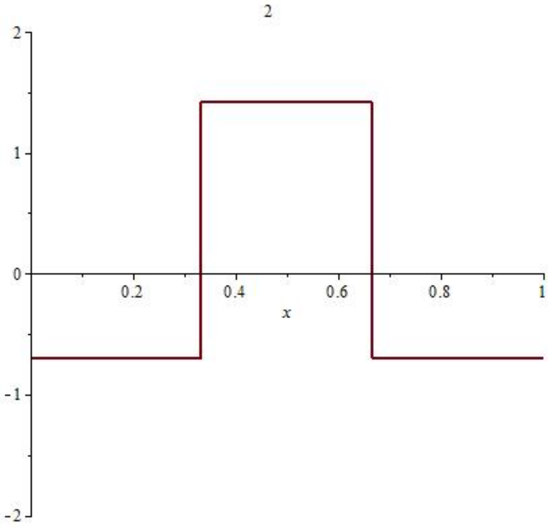
Generalized Walsh bases



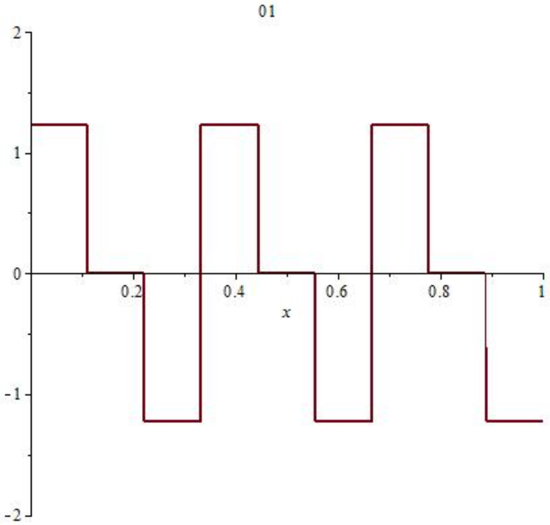
Generalized Walsh bases



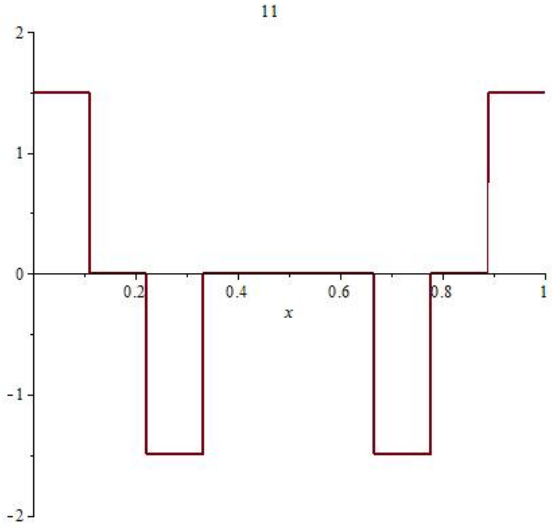
Generalized Walsh bases



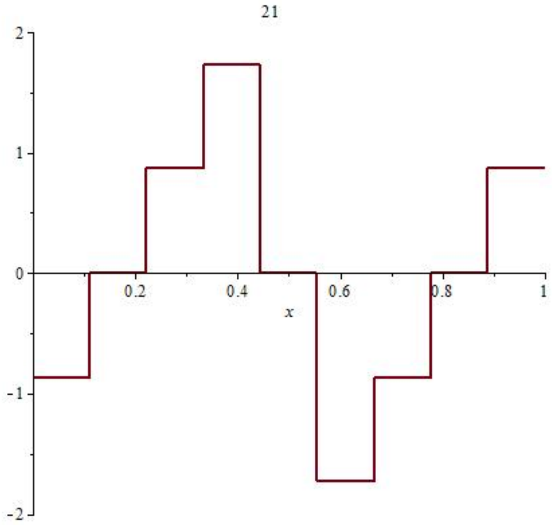
Generalized Walsh bases



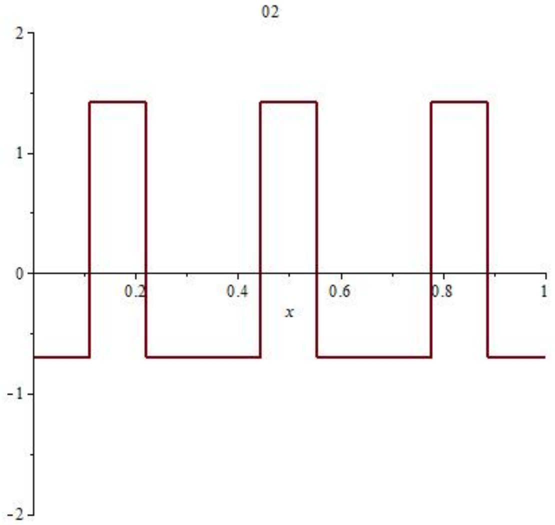
Generalized Walsh bases



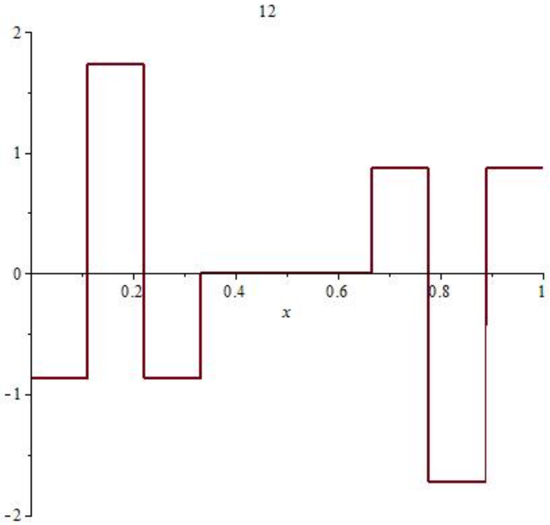
Generalized Walsh bases



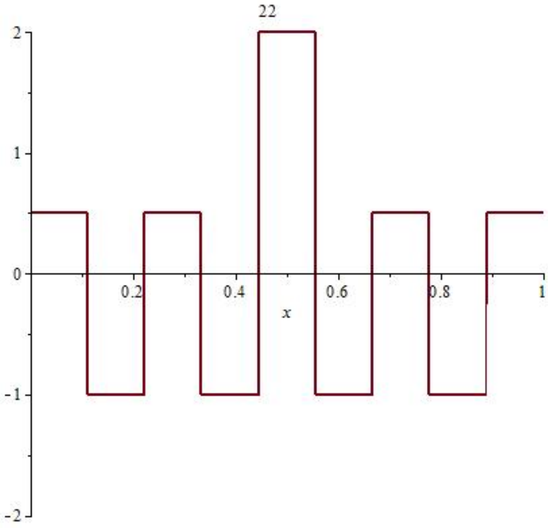
Generalized Walsh bases



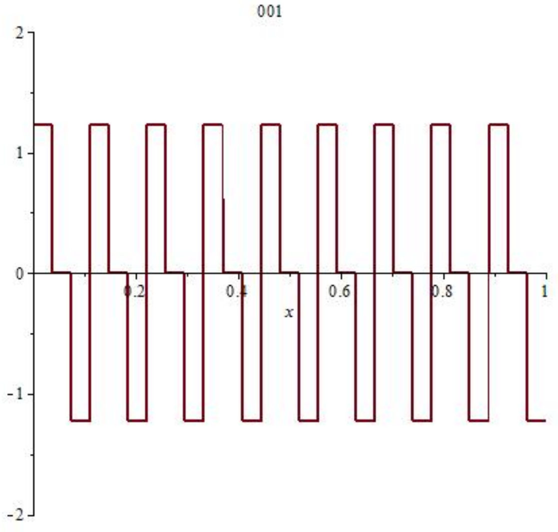
Generalized Walsh bases



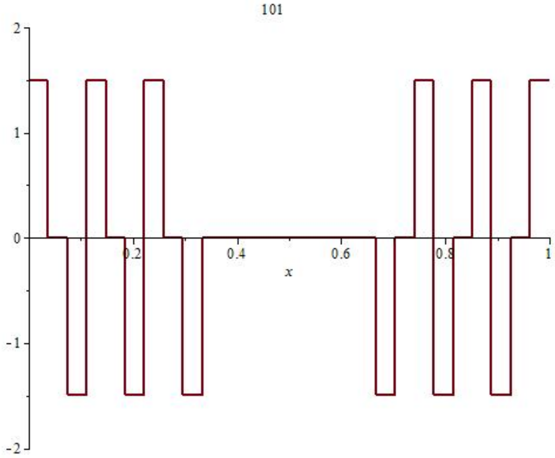
Generalized Walsh bases



Generalized Walsh bases



Generalized Walsh bases



Some differences

The classic Walsh functions form a group :

$$W_n(x) \cdot W_m(x) = W_{n \oplus m}(x)$$

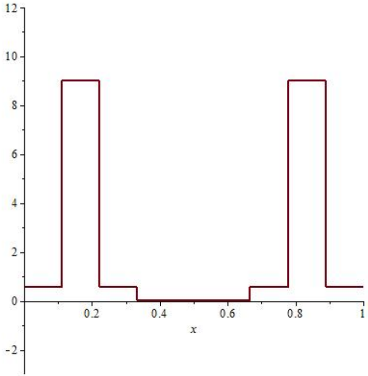


Figure: Graph of $W^4_{7,A} \Rightarrow (W_{n,A})_n$ does not form a group

Convergence properties

Theorem

For $f \in L^1[0,1]$ *the sequence*

$$S_{N^q}(x) = \sum_{n=0}^{N^q-1} \langle f\,,\, W_{n,A} \rangle\, W_{n,A}(x)$$

converges a.e. to $f(x)$*.*

Corollary

If $f \in L^1[0,1]$ *is continuous in a neighborhood of* $x = a$ *then* $S_{N^q} \to f$ *uniformly inside an interval centered at* a*.*

Approximation issues

Example

$$f(x) = \begin{cases} 0, & x \in [0, 1/16) \cup [1/8, 3/16) \cup [1/4, 1/2) \\ 1, & x \in [1/16, 1/8) \cup [3/16, 1/4) \cup [1/2, 1] \end{cases}$$

With generalized Walsh ONB to the unitary matrix

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ -\frac{\sqrt{6}}{6} & \frac{\sqrt{6}}{3} & -\frac{\sqrt{6}}{6} \end{pmatrix}$$

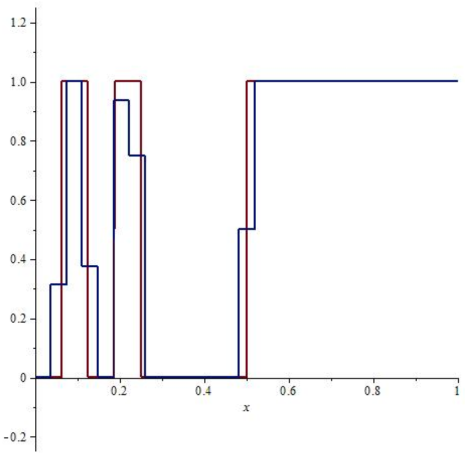


Figure: Graph of f and $S_{27}(f)$

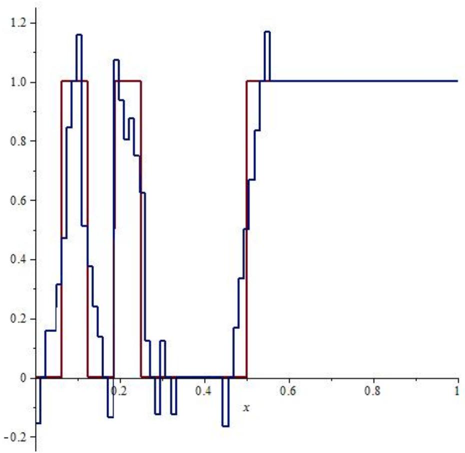


Figure: Graph of f and $S_{36}(f)$

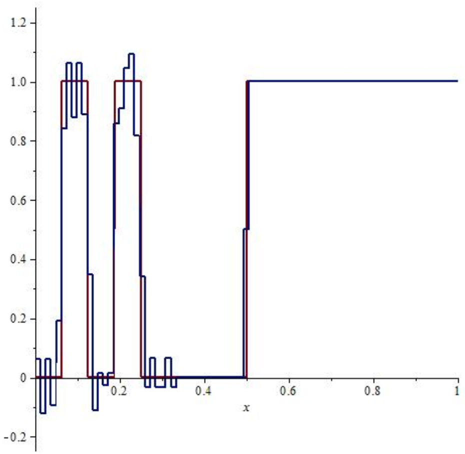


Figure: Graph of f and $S_{60}(f)$

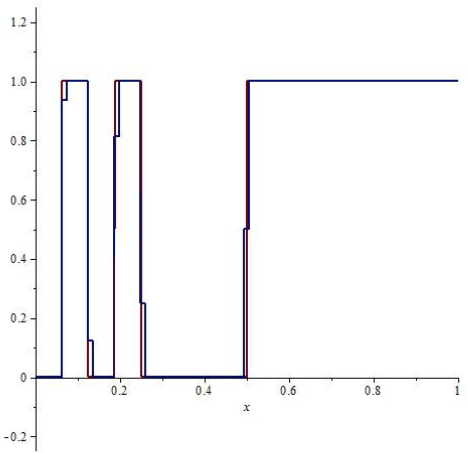


Figure: Graph of f and $S_{81}(f)$

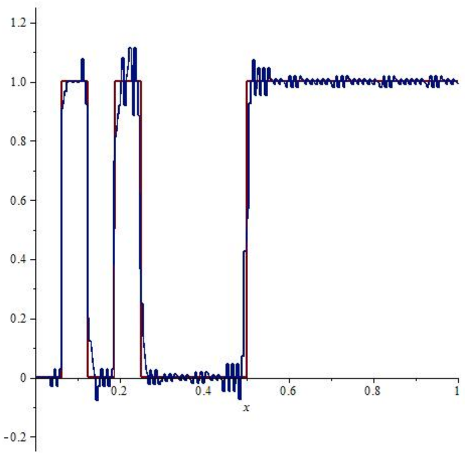


Figure: Graph of f and $S_{100}(f)$

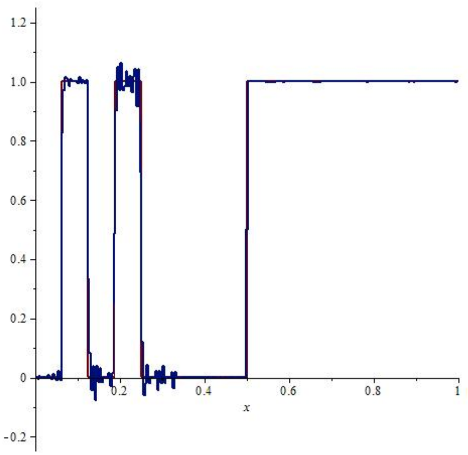


Figure: Graph of f and $S_{200}(f)$

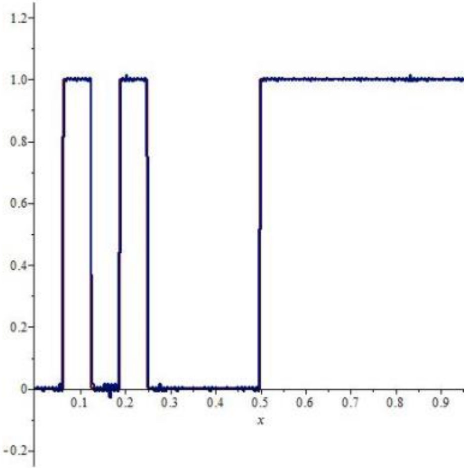


Figure: Graph of f and $S_{241}(f)$

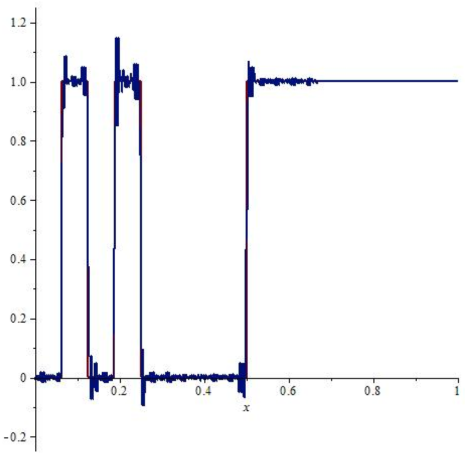


Figure: Graph of f and $S_{300}(f)$

Symmetric encryption

Corollary

If $f : [0,1] \to \mathbb{C}$ *is constant on the interval* $I_j := [j/N^q, (j+1)/N^q)$ *for some* $j \in \{0, 1, .., N^q - 1\}$, *then for all* $x \in I_j$ *:*

$$f(x) = \sum_{n=0}^{N^q-1} \langle f \, , \, W_{n,A} \rangle \, W_{n,A}(x)$$

$f(x) = v_j$, $x \in I_j$, $j = 0, \ldots, N^q - 1$.

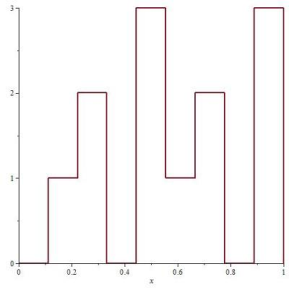
The sequence $\langle f \, , \, W_{n,A} \rangle$ *encrypts* f *with respect to a secret matrix* A.

Example

$f =$ "abcadbcad" is encoded as

$a_n = [1.333333333, -.2024226815, .1819316687, -.4048453629, .5672104250, .3354086404, .3638633377, .7203088198, 0.9945624111e-1]$

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0.25301205 & * & * \\ * & * & * \end{pmatrix}$$



Example

Given the previous sequence a_n and slightly "perturbed" matrix

$$\tilde{A} = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0.2 & * & * \\ * & * & * \end{pmatrix}$$

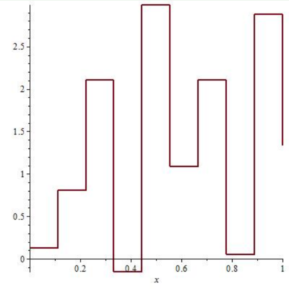


Figure: Graph of $\sum a_n W_{n,\tilde{A}}$

Continuity w.r.t. matrix entries

For a fixed sequence $(a_n)_{n=0}^{N^q-1}$ *the map*

$$\mathbb{R}^{N^2} \ni A \to \sum_{n=0}^{N^q-1} a_n W_{n,A} \text{ is continuous}$$

To strengthen the "encryption" : $f \to \langle f\,,\, W_{n,A}\rangle + $ *extra, e.g.* $(-1)^n M \sin(1/a^2)$

Previous example, now with entry $a = 0.25301204$

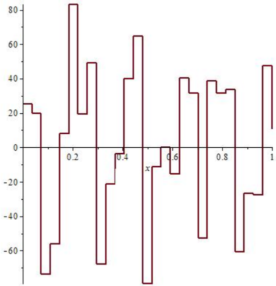


Figure: Graph of $\sum a_n W_{n,\tilde{A}}$

Encryption/Compression with Cuntz

- QMF *basis* $m_i(x) := \sqrt{N}\sum_{j=0}^{N-1} a_{ij}\chi_{[j/N,(j+1)/N]}(x)$
- $S_i(f) = m_i f \circ r$
- $S_i^*(f) = \frac{1}{N}\sum_{k=0}^{N-1} m_i(\frac{x+k}{N}) \cdot f(\frac{x+k}{N})$

signal $f \Rightarrow [S_i^*(f)]_{i=0,N-1}$ *(i.e.* f *encrypted).*

Compress $[S_i^*(f)]_{i=0,N-1}$.

Example

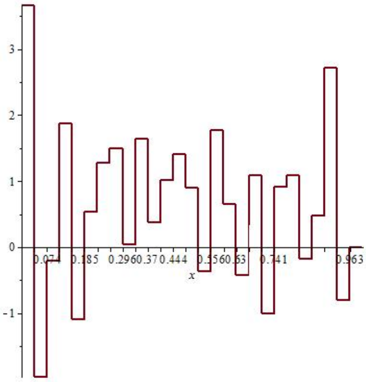


Figure: Signal f, piece wise constant on tri-adic intervals

Example

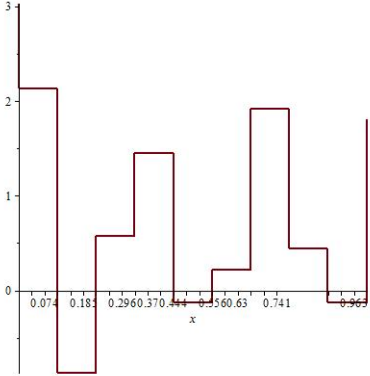


Figure: First frequency band, signal $S_0^* f$

Example

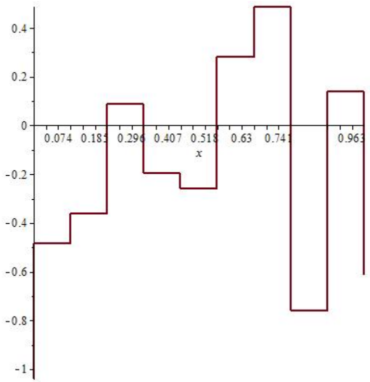


Figure: 2nd frequency band, signal $S_1^* f$

Example

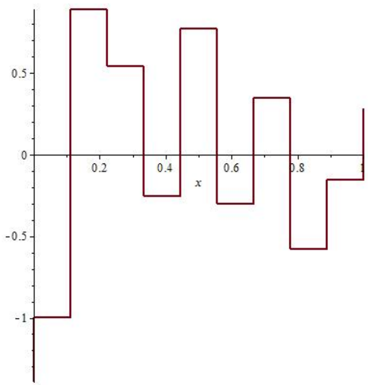


Figure: 3rd frequency band, signal $S_2^* f$

A cryptographic protocol

- *H_1 space of messages, H_2 the space of encrypted messages*
- *Assume plenty of operators $A : H_1 \to H_2$ and $B : H_1 \to H_2$ such that*

$$B^{-1} \circ A \circ B^{-1} \circ A = I_{H_1}$$

"Ping-pong" messaging (also Eve is eavesdropping):

1) Alice to Bob: $w_1 = A(v) \in H_2$
2) Bob to Alice: $w_2 = B^{-1}A(v) \in H_1$
3) Alice to Bob: $w_3 = AB^{-1}A(v) \in H_2$
4) Bob applies B^{-1} to w_3.

Bad choices

• $A(f)(x) = f(x+a)$, $B(f) = f(x+b)$
f can be detected from its translations

• $A(f)(x) = f(x^a)$, $B(f)(x) = f(x^b)$
dilation/compression, some of f could be guessed, issues with the domain

• *More generally* $f \in G$, G *Abelian group:* $Ax = ax$, $Bx = bx$.
Previous ping-pong:

$w_1 = af$,
$w_2 = b^{-1}w_1 \Rightarrow$ *Eve can figure out* $b = w_2^{-1}w_1$
$w_3 = a^{-1}w_2 = b^{-1}f \Rightarrow$ *Eve multiplies by b and reveals f*

Transforms commutation

A, B unitary $N \times N$ matrices having constant $1/\sqrt{N}$ first row.

$$\mathcal{W}_A : L^2[0,1] \to l^2(\mathbb{N}),\ \mathcal{W}_A(f) = \langle f\ ,\ W_{n,A} \rangle_{n \geq 0}$$

The inverse tranform (only needed for finite sequences) :

$$\mathcal{W}_A^{-1}((a_n)_n) = \sum_n a_n W_{n,A}$$

Question: Given f under what conditions for A and B does the "ping-pong" protocol work?

$$\mathcal{W}_B^{-1} \circ \mathcal{W}_A \circ \mathcal{W}_B^{-1} \circ \mathcal{W}_A(f) = f$$

Theorem

If $\langle row_{\,l,B}\,,\ row_{\,k,A}\rangle = \langle row_{\,l,A}\,,\ row_{\,k,B}\rangle$ *for all* k, l *in* $\{1, 2, 3, ..., N\}$

then $\forall f$ *piecewise constant on consecutive* N*-adic intervals :*

$$\mathcal{W}_B^{-1} \circ \mathcal{W}_A \circ \mathcal{W}_B^{-1} \circ \mathcal{W}_A(f) = f$$

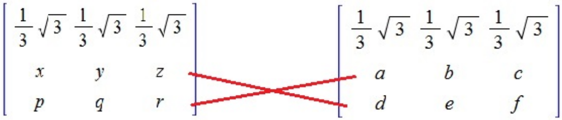
Theorem

If $\langle row_{\ l,B}\ ,\ row_{\ k,A}\rangle = \langle row_{\ l,A}\ ,\ row_{\ k,B}\rangle$ *for all* k, l *in* $\{1, 2, 3, ..., N\}$

then $\forall f$ *piecewise constant on consecutive* N*-adic intervals :*

$$\mathcal{W}_B^{-1} \circ \mathcal{W}_A \circ \mathcal{W}_B^{-1} \circ \mathcal{W}_A(f) = f$$

$N = 3$ one equation is relevant:



Protocol set up

- Alice has $A = [a_{i,j}]_{i=1,N}^{j=1,N}$ with real number entries.
- Bob receives from Alice:

$$\sum_{j=1}^{N} a_{kj} x_{lj} = \sum_{j=1}^{N} a_{lj} x_{kj}, \quad \forall 1 < l < k \leq N \qquad | \cdot \textit{masking coefficients}$$

Protocol set up

- Alice has $A = [a_{i,j}]_{i=1,N}^{j=1,N}$ with real number entries.
- Bob receives from Alice:

$$\sum_{j=1}^{N} a_{kj} x_{lj} = \sum_{j=1}^{N} a_{lj} x_{kj}, \quad \forall 1 < l < k \leq N \qquad | \cdot \textit{masking coefficients}$$

- $B = [x_{i,j}]_{i=1,N}^{j=1,N}$ must be unitary:

$$x_{1,j} = 1/\sqrt{N}, \quad \forall j = 1, ..., N$$
$$\sum_{j=1}^{N} |x_{i,j}|^2 = 1, \quad \forall i = 2, ..., N$$
$$\sum_{j=1}^{N} x_{i,j} = 0, \quad \forall i = 2, ..., N$$
$$\sum_{k=1}^{N} x_{i,k} \cdot x_{j,k} = 0, \quad \forall 1 < i < j \leq N$$

System of $N^2 - N$ quadratics with $N^2 - N$ unknowns.

Question

Are there infinitely many A for which the previous system has infinitely many solutions?
Study their Grobner bases.

Question

Are there infinitely many A for which the previous system has infinitely many solutions?
Study their Grobner bases.

Example

There are infintely many B transform "commuting" with

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ -\frac{\sqrt{6}}{6} & \frac{\sqrt{6}}{3} & -\frac{\sqrt{6}}{6} \end{pmatrix}$$

Thank you!

Bibliography:

1) D.Dutkay, G.Picioroaga, M.S. Song
"Orthonormal bases generated by Cuntz algebras"
to appear in JMAA

2) D.Dutkay, G.Picioroaga
"Generalized Walsh bases and applications",
to appear in ACAP

3) S.Harding, G.Picioroaga
"Continuity properties of a generalized Walsh system and applications to cryptography"-undergraduate research project