Perfect Space-Time-Block-Codes from certain bicyclic Crossed Product Algebras

Jens Diewald

Technical University Dortmund (Germany)

Noncommutative rings and their applications, IV
Lens 8-11 June 2015

Modeling Wireless communication

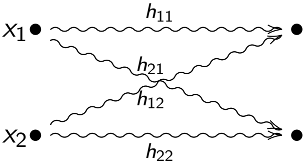
How to model the transmission of information over a wireless channel?

- Encode information in a complex number $x \in \mathbb{C}$.
- Send it over the wireless channel:

$$x\bullet \overset{h}{\rightsquigarrow} \bullet y = hx + v$$

- Receive the message $y = hx + v \in \mathbb{C}$.

Using two antennas on each side, the situation becomes:



$$y_1 = h_{11}x_1 + h_{12}x_2 + v_1$$

$$y_2 = h_{21}x_1 + h_{22}x_2 + v_2$$

This can be expressed as a matrix/vector equation.

$$\begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix} = \begin{pmatrix} h_{11} & \cdots & h_{1M} \\ \vdots & \ddots & \vdots \\ h_{N1} & \cdots & h_{NM} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_M \end{pmatrix} + \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix}.$$

Hereby

$$M \hat{=} \text{Number of transmit antennas}$$

and

$$N \hat{=} \text{Number of receive antennas.}$$

We can combine the elements sent over the channel in T consecutive timesteps into a matrix:

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1T} \\ \vdots & \ddots & \vdots \\ x_{M1} & \cdots & x_{MT} \end{pmatrix}.$$

This yields a matrix equation

$$Y = HX + V.$$

Definition

A Space-Time Block Code is a collection of such codewords X.

Design criteria

What influences the performance of a STBC?

- A lot of things.
- The difference of two codewords shall have a large determinant.

The latter condition suggests to use Division Algebras in order to construct good codes.

Background to this work

- Good STBC have been constructed from Division Algebras
- "Perfect" STBC have been constructed in any dimension from cyclic (Crossed Product) Algebras by Elia/Sethuraman/Kumar
- A "perfect" STBC has been constructed by Berhuy/Oggier from a bicyclic Crossed Product Algebra with respect to a Galois Group of type $C_2 \times C_2$.

Cyclic Algebras

Definition (incomplete)

Let $L|K$ be a cyclic Galois extension of degree n,
$\mathrm{Gal}(L|K) =< \sigma >$.
Then a Crossed Product Algebra over $L|K$ is of the form

$$A = \bigoplus_{i=0}^{n-1} e_\sigma^i L.$$

The multiplication is determined by a cocycle ξ_c of the form
$\xi_c(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i+j < n \\ c & \text{if } i+j \geq n \end{cases}$, for some $c \in K$.

Notation

Denote the cyclic Algebra over $L|K$ with respect to the cocycle ξ_c by $(L|K, \sigma, c)$.

Theorem

The Algebra $(L|K, \sigma, c)$ is a Division Algebra iff c^k is not a norm of $L|K$ for all proper divisors $k|[L:K]$.

Lemma

In $\mathbb{Q}(\zeta_{2^{d+2}})$ the prime number 5 is unramified and splits into two prime ideals $(1+2i)$ and $(1-2i)$ each of inertia degree 2^d.

Corollary

The element $\left(\frac{1+2i}{1-2i}\right)^k$ is not a norm of $\mathbb{Q}(\zeta_{2^{d+2}})|\mathbb{Q}(i)$ for any $k \mid 2^d = [\mathbb{Q}(\zeta_{2^{d+2}}) : \mathbb{Q}(i)]$.

Corollary

The cyclic algebra $\left(Q(\zeta_{2^{d+2}})|\mathbb{Q}(i), \sigma, \frac{1+2i}{1-2i}\right)$ *is a division algebra.*

Example (STBC with respect to C_4)

$K = \mathbb{Q}(i)$, $L = K(\zeta_{16})$, σ a generator of $\mathrm{Gal}(L|K)$ and $c := \frac{1+2i}{1-2i}$

$$M_x = \begin{pmatrix} x_{\mathrm{Id}} & c\sigma(x_\sigma^3) & c\sigma^2(x_{\sigma^2}) & c\sigma^3(x_\sigma) \\ x_\sigma & \sigma(x_{\mathrm{Id}}) & c\sigma^2(x_{\sigma^3}) & c\sigma^3(x_{\sigma^2}) \\ x_\sigma^2 & \sigma(x_\sigma) & \sigma^2(x_{\mathrm{Id}}) & c\sigma^3(x_{\sigma^3}) \\ x_{\sigma^3} & \sigma(x_\sigma^2) & \sigma^2(x_\sigma) & \sigma^3(x_{\mathrm{Id}}) \end{pmatrix}.$$

Bicyclic Algebras

Definition (incomplete)

Let $L|K$ be a bicyclic Galois extension of degree $n \cdot m$,
$\mathrm{Gal}(L|K) = < \sigma, \tau > \cong C_n \times C_m$.
Then a Crossed Product Algebra over $L|K$ is of the form

$$A = \bigoplus_{i=0}^{n-1} \bigoplus_{j=0}^{m-1} e_\sigma^i e_\tau^j L.$$

Definition

The multiplication is determined by a cocycle of the form

$$\xi_{u,b_\sigma,b_\tau}(\sigma^i\tau^j, \quad \sigma^k\tau^l) = \prod_{t=0}^{k-1}\prod_{s=0}^{j-1}\sigma^{-t}\tau^{-(s+l)}(u)$$
$$\cdot \begin{cases} 1 & , \text{ if } i+k<n \text{ and } j+l<m \\ \tau^{-(j+l)}(b_\sigma) & , \text{ if } i+k\geq n \text{ and } j+l<m \\ b_\tau & , \text{ if } i+k<n \text{ and } j+l\geq m \\ \tau^{-(j+l)}(b_\sigma)b_\tau & , \text{ if } i+k\geq n \text{ and } j+l\geq m. \end{cases}$$

Notation

Denote the Crossed Product Algebra over $L|K$ with respect to the cocycle ξ_{u,b_σ,b_τ} by $(L|K,(\sigma,\tau),(u,b_\sigma,b_\tau))$.

Theorem

Let $u, b_\sigma, b_\tau \in L$ satisfy the following conditions:

1) $N_{L|L^\sigma}(u) = \frac{\tau^{-1}(b_\sigma)}{b_\sigma}$
2) $N_{L|L^\tau}(u) = \frac{b_\tau}{\sigma^{-1}(b_\tau)}$

Then $A = (L|K,(\sigma,\tau),(u,b_\sigma,b_\tau))$ is a Crossed Product Algebra.

Theorem (Amitsur, Saltman (1978))

$A = (L|K, (\sigma, \tau), (u, b_\sigma, b_\tau))$ is a division algebra iff there is no proper divisor $k \mid nm$ such that the following relations hold:

(1) $b_\sigma^k = N_{L|L^\sigma}(a_\sigma)$ *for some* $a_\sigma \in L^\times$

(2) $b_\tau^k = N_{L|L^\tau}(a_\tau)$ *for some* $a_\tau \in L^\times$

(3) $u^k = \frac{\sigma^{-1}(a_\tau)}{a_\tau} \cdot \frac{a_\sigma}{\tau^{-1}(a_\sigma)}$.

This turns out not to be useful.

Instead we will make use of the following fact:

Theorem (Brauer, Hasse, Noether)

Every Crossed Product Algebra over a Numberfield is a cyclic Algebra.

Construction with respect to Galois groups $C_2 \times C_{2^d}$

Consider field extensions:

$$\begin{tikzcd}
& L \arrow[dl, dash, "2"'] \arrow[dr, dash, "2^d"] & \\
K(\zeta_{2^{d+2}}) \arrow[dr, dash, "2^d"'] & & K(b_\tau) \arrow[dl, dash, "2"] \\
& K = \mathbb{Q}(i) &
\end{tikzcd}$$

And choose:

$$\begin{aligned}
u &= \zeta_{2^{d+2}}^2, \\
b_\sigma &= \zeta_{2^{d+2}}, \\
b_\tau^2 &\in K, \\
\sigma &: \begin{cases} \zeta_{2^{d+2}} \mapsto \zeta_{2^{d+2}} \\ b_\tau \mapsto -b_\tau, \end{cases} \\
\tau^{-1} &: \begin{cases} \zeta_{2^{d+2}} \mapsto \zeta_{2^{d+2}}^{-4} \cdot \zeta_{2^{d+2}} \\ b_\tau \mapsto b_\tau. \end{cases}
\end{aligned}$$

Proposition

Then $(L|K, (\sigma, \tau), (u, b_\sigma, b_\tau))$ is a Crossed Product Algebra.

Proposition

$$(L|K, (\sigma, \tau), (u, b_\sigma, b_\tau)) = (K(e_\sigma)|K, \tau', b_\tau^2),$$

where $\tau' : K(e_\sigma) \to K(e_\sigma),\ x \mapsto e_\tau x e_\tau^{-1}$ *is a generator of the cyclic Galois Group of the field extension* $K(e_\sigma)|K$

Proof.

- We have $e_\sigma^2 = \zeta_{2^{d+2}}$, hence e_σ may be considered as a 2^{d+3}-th root of unity. Therefore $K(e_\sigma)|K$ is a cyclic Galois extension of degree 2^{n+2}.
- One can check that τ' is actually an automorphism of $K(e_\sigma)$, generating $\mathrm{Gal}(K(e_\sigma)|K$. This makes use of the fact that u was chosen from $K(b_\sigma) = L^\sigma$.

□

Corollary

If we choose b_τ *such that* $b_\tau^2 = \frac{1+2i}{1-2i}$ *holds, the algebra* $(L|K, (\sigma, \tau), (u, b_\sigma, b_\tau))$ *is a Division Algebra.*

A similar construction works in the cases $C_4 \times C_{2^d}$ and $C_3 \times C_{3^d}$:

Proposition

If we choose b_τ such that $b_\tau^4 = \frac{1+2i}{1-2i}$ holds, the algebra $(\mathbb{Q}(\zeta_{2^{d+2}})|\mathbb{Q}(i),(\sigma,\tau),(\zeta_{2^{d+2}},\zeta_{2^{d+2}},b_\tau))$ is a Division Algebra for all $d \in \mathbb{N}_0$.

Proposition

If we choose b_τ such that $b_\tau^3 = \frac{1+3\zeta_3}{1+3\zeta_3^2}$ holds, the algebra $(\mathbb{Q}(\zeta_{3^{d+1}})|\mathbb{Q}(\zeta_3),(\sigma,\tau),(\zeta_{3^{d+1}},\zeta_{3^{d+1}},b_\tau))$ is a Division Algebra for all $d \in \mathbb{N}_0$.

Example (STBC with respect to $C_2 \times C_0$)

$K = \mathbb{Q}(i)$ and $L = K\left(\sqrt{\frac{1+2i}{1-2i}}\right) = K(\sqrt{5})$. We obtain the cyclic algebra $A = (L|K, \sigma, i)$, which yields the well known Golden Code. The codewords are of the form

$$\begin{pmatrix} x_{\mathrm{Id}} & i\sigma(x_\sigma) \\ x_\sigma & \sigma(x_{\mathrm{Id}}) \end{pmatrix}.$$

Example (STBC with respect to $C_2 \times C_2$)

$K = \mathbb{Q}(i)$, $L = \mathbb{Q}(\zeta_8, b_\tau)$ and $A = \left(L|K, (\sigma,\tau), \left(i, \zeta_8, \sqrt{\frac{1+2i}{1-2i}}\right)\right)$,
where

$$\sigma : \begin{cases} \zeta_8 \mapsto \zeta_8 \\ b_\tau \mapsto -b_\tau, \end{cases} \quad \text{and } \tau : \begin{cases} \zeta_8 \mapsto -\zeta_8 \\ b_\tau \mapsto b_\tau. \end{cases}$$

Then, for a codeword we get

$$\begin{pmatrix} x_{\mathrm{Id}} & \zeta_8\sigma(x_\sigma) & b_\tau\tau(x_\tau) & i\zeta_8 b_\tau\sigma\tau(x_{\sigma\tau}) \\ x_\sigma & \sigma(x_{\mathrm{Id}}) & b_\tau\tau(x_{\sigma\tau}) & ib_\tau\sigma\tau(x_\tau) \\ x_\tau & -i\zeta_8\sigma(x_{\sigma\tau}) & \tau(x_{\mathrm{Id}}) & -\zeta_8\sigma\tau(x_\sigma) \\ x_{\sigma\tau} & i\sigma(x_\tau) & \tau(x_\sigma) & \sigma\tau(x_{\mathrm{Id}}) \end{pmatrix}.$$

Example ($C_2 \times C_4$)

$K = \mathbb{Q}(i)$ and $L = \mathbb{Q}(\zeta_{16}, b_\tau)$, $u = \zeta_{16}^2$, $b_\sigma = \zeta_{16}$, $b_\tau = \sqrt{\frac{1+2i}{1-2i}}$,

$$\sigma : \begin{cases} \zeta_{16} \mapsto \zeta_{16} \\ b_\tau \mapsto -b_\tau, \end{cases} \quad \text{and } \tau : \begin{cases} \zeta_{16} \mapsto i\zeta_{16} \\ b_\tau \mapsto b_\tau. \end{cases}$$

The codewords are of the form:

$$\begin{pmatrix}
x_{\mathrm{Id}} & \zeta_{16}\sigma(x_\sigma) & b_\tau\tau^3(x_{\tau^3}) & i\zeta_{16}^3 b_\tau\sigma\tau^3(x_{\sigma\tau^3}) & b_\tau\tau^2(x_{\tau^2}) & -i\zeta_{16} b_\tau\sigma\tau^2(x_{\sigma\tau^2}) & b_\tau\tau(x_\tau) & -\zeta_{16}^3 b_\tau\sigma\tau(x_{\sigma\tau}) \\
x_\sigma & \sigma(x_{\mathrm{Id}}) & b_\tau\tau^3(x_{\sigma\tau^3}) & i\zeta_{16}^2 b_\tau\sigma\tau^3(x_{\tau^3}) & b_\tau\tau^2(x_{\sigma\tau^2}) & -ib_\tau\sigma\tau^2(x_{\tau^2}) & b_\tau\tau(x_{\sigma\tau}) & -\zeta_{16}^2 b_\tau\sigma\tau(x_\tau) \\
x_\tau & -i\zeta_{16}^3\sigma(x_{\sigma\tau}) & \tau^3(x_{\mathrm{Id}}) & -i\zeta_{16}\sigma\tau^3(x_\sigma) & b_\tau\tau^2(x_{\tau^3}) & -\zeta_{16}^3 b_\tau\sigma\tau^2(x_{\sigma\tau^3}) & b_\tau\tau(x_{\tau^2}) & -\zeta_{16} b_\tau\sigma\tau(x_{\sigma\tau^2}) \\
x_{\sigma\tau} & \zeta_{16}^2\sigma(x_\tau) & \tau^3(x_\sigma) & \sigma\tau^3(x_{\mathrm{Id}}) & b_\tau\tau^2(x_{\sigma\tau^3}) & -i\zeta_{16}^2 b_\tau\sigma\tau^2(x_{\tau^3}) & b_\tau\tau(x_{\sigma\tau^2}) & -ib_\tau\sigma\tau(x_{\tau^2}) \\
x_{\tau^2} & i\zeta_{16}\sigma(x_{\sigma\tau^2}) & \tau^3(x_\tau) & \zeta_{16}^3\sigma\tau^3(x_{\sigma\tau}) & \tau^2(x_{\mathrm{Id}}) & -\zeta_{16}\sigma\tau^2(x_\sigma) & b_\tau\tau(x_{\tau^3}) & -i\zeta_{16}^3 b_\tau\sigma\tau(x_{\sigma\tau^3}) \\
x_{\sigma\tau^2} & -i\sigma(x_{\tau^2}) & \tau^3(x_{\sigma\tau}) & -\zeta_{16}^2\sigma\tau^3(x_\tau) & \tau^2(x_\sigma) & \sigma\tau^2(x_{\mathrm{Id}}) & b_\tau\tau(x_{\sigma\tau^3}) & i\zeta_{16}^2 b_\tau\sigma\tau(x_{\tau^3}) \\
x_{\tau^3} & \zeta_{16}^3\sigma(x_{\sigma\tau^3}) & \tau^3(x_{\tau^2}) & \zeta_{16}\sigma\tau^3(x_{\sigma\tau^2}) & \tau^2(x_\tau) & i\zeta_{16}^3\sigma\tau^2(x_{\sigma\tau}) & \tau(x_{\mathrm{Id}}) & i\zeta_{16}\sigma\tau(x_\sigma) \\
x_{\sigma\tau^3} & -i\zeta_{16}^2\sigma(x_{\tau^3}) & \tau^3(x_{\sigma\tau^2}) & -i\sigma\tau^3(x_{\tau^2}) & \tau^2(x_{\sigma\tau}) & \zeta_{16}^2\sigma\tau^2(x_\tau) & \tau(x_\sigma) & \sigma\tau(x_{\mathrm{Id}})
\end{pmatrix}.$$

Comparison of the minimal determinants

1) For $C_{2^{d+2}}$:

$$\frac{\sqrt{5}}{(2^{d+2}\cdot 5)^{2^{d+1}}} \leq \delta_{\min}(C) \leq \frac{1}{(2^{d+2})^{2^{d+1}}}.$$

2) For $C_2 \times C_{2^{d+1}}$:

$$\frac{\sqrt{5}}{(2^{d+1}\cdot 5)^{2^{d+1}}} \leq \delta_{\min}(C) \leq \frac{1}{(2^{d+1}\cdot \sqrt{5})^{2^{d+1}}}.$$

3) For $C_4 \times C_{2^d}$:

$$\frac{\sqrt{5}}{(2^{d+1}\cdot 5)^{2^{d+1}}} \leq \delta_{\min}(C) \leq \frac{1}{(2^{d+1}\cdot \sqrt{5}^3)^{2^{d+1}}}.$$

1) For $C_{3^{d+1}}$:

$$\frac{\sqrt{7}}{\left(\sqrt{7\cdot 3^{d+1}}\right)^{3^{d+1}}} \leq \delta_{\min}(C) \leq \frac{1}{\sqrt{3^{d+1}}^{3^{d+1}}}.$$

2) For $C_3 \times C_{3^d}$:

$$\frac{\sqrt{7}}{\left(\sqrt{7\cdot 3^{d}}\right)^{3^{d+1}}} \leq \delta_{\min}(C) \leq \frac{1}{7^{3^d}\sqrt{3^d}^{3^{d+1}}}.$$