Crossed Products and Coding Theory

Yuval Ginosar and Aviram R. Moreno
University of Haifa

Group graded rings

Recall that an (associative, with 1) ring A is graded by a group G if it admits is a decomposition

$$A = \bigoplus_{g \in G} A_g \tag{1}$$

as an abelian group such that

$$A_g A_h \subseteq A_{gh} \tag{2}$$

for every $g, h \in G$.

Group graded rings

Recall that an (associative, with 1) ring A is graded by a group G if it admits is a decomposition

$$A = \bigoplus_{g \in G} A_g \qquad (1)$$

as an abelian group such that

$$A_g A_h \subseteq A_{gh} \qquad (2)$$

for every $g, h \in G$.
The abelian group A_g is termed the g**-th homogeneous component** of A.

Group graded rings

Recall that an (associative, with 1) ring A is graded by a group G if it admits is a decomposition

$$A = \bigoplus_{g \in G} A_g \tag{1}$$

as an abelian group such that

$$A_g A_h \subseteq A_{gh} \tag{2}$$

for every $g, h \in G$.
The abelian group A_g is termed the **g-th homogeneous component** of A.
The multiplicative condition (2) yields that the e-component A_e is a ring, termed the **base ring** of A, and that (1) determines a decomposition of A as an A_e-bimodule.

Graded equivalence

There are few ways to define equivalence of graded rings in such a way that respects their grading.

Graded equivalence

There are few ways to define equivalence of graded rings in such a way that respects their grading.
A **graded-equivalence** between two graded rings

$$A = \bigoplus_{g \in G} A_g, \quad B = \bigoplus_{h \in H} B_h,$$

is a pair (ψ, ϕ), where $\psi : A \to B$ is a ring isomorphism and $\phi : G \to H$ is a group isomorphism such that $\psi(A_g) = B_{\phi(g)}$ for any $g \in G$.

Structure of crossed products

A G-graded ring $A = \bigoplus_{g \in G} A_g$ is a **crossed product** if there is an invertible homogeneous element $u_g \in A_g$ for every $g \in G$.

Structure of crossed products

A G-graded ring $A = \bigoplus_{g \in G} A_g$ is a **crossed product** if there is an invertible homogeneous element $u_g \in A_g$ for every $g \in G$.
In this case $A_g = A_e u_g = u_g A_e$, and hence $A = \bigoplus_{g \in G} A_e u_g$.

Structure of crossed products

A G-graded ring $A = \bigoplus_{g \in G} A_g$ is a **crossed product** if there is an invertible homogeneous element $u_g \in A_g$ for every $g \in G$.
In this case $A_g = A_e u_g = u_g A_e$, and hence $A = \bigoplus_{g \in G} A_e u_g$.
Let $R := A_e$, then we usually write

$$R * G = \bigoplus_{g \in G} R u_g .$$

Any element in $R * G$ is written as $\sum_{g \in G} \beta_g u_g$ with uniquely determined coefficients $\{\beta_g\}_{g \in G} \subset R$.

Structure of crossed products

Suppose that the base ring R of a crossed product is commutative.

Structure of crossed products

Suppose that the base ring R of a crossed product is commutative. Since the product in $R * G$ respects the G-grading, that is

$$Ru_g \cdot Ru_h = Ru_{gh}, \quad \forall g, h \in G, \tag{3}$$

then $R * G$ determines a G-action on the base ring R via the rule

$$\eta : \begin{array}{c} G \to \mathrm{Aut}(R) \\ g(r) := u_g r u_g^{-1} \end{array}, \quad g \in G, r \in R. \tag{4}$$

Structure of crossed products

Suppose that the base ring R of a crossed product is commutative. Since the product in $R*G$ respects the G-grading, that is

$$Ru_g \cdot Ru_h = Ru_{gh}, \quad \forall g,h \in G, \tag{3}$$

then $R*G$ determines a G-action on the base ring R via the rule

$$\eta : \begin{array}{c} G \to \mathrm{Aut}(R) \\ g(r) := u_g r u_g^{-1} \end{array}, \quad g \in G, r \in R. \tag{4}$$

Equation (3) gives rise to a two-place function

$$f : \begin{array}{ccc} G \times G & \to & R^* \\ (g,h) & \mapsto & u_g u_h u_{gh}^{-1} \end{array}, \tag{5}$$

where R^* denotes the multiplicative group of units of R.

Structure of crossed products

Suppose that the base ring R of a crossed product is commutative. Since the product in $R * G$ respects the G-grading, that is

$$Ru_g \cdot Ru_h = Ru_{gh}, \quad \forall g, h \in G, \tag{3}$$

then $R * G$ determines a G-action on the base ring R via the rule

$$\eta : \begin{array}{c} G \to \mathrm{Aut}(R) \\ g(r) := u_g r u_g^{-1} \end{array}, \quad g \in G, r \in R. \tag{4}$$

Equation (3) gives rise to a two-place function

$$f : \begin{array}{ccc} G \times G & \to & R^* \\ (g, h) & \mapsto & u_g u_h u_{gh}^{-1} \end{array}, \tag{5}$$

where R^* denotes the multiplicative group of units of R. Associativity of $R * G$ yields that (5) is a **2-cocycle.**

Structure of crossed products

Suppose that the base ring R of a crossed product is commutative. Since the product in $R*G$ respects the G-grading, that is

$$Ru_g \cdot Ru_h = Ru_{gh}, \quad \forall g,h \in G, \tag{3}$$

then $R*G$ determines a G-action on the base ring R via the rule

$$\eta : \begin{array}{c} G \to \mathrm{Aut}(R) \\ g(r) := u_g r u_g^{-1} \end{array}, \quad g \in G, r \in R. \tag{4}$$

Equation (3) gives rise to a two-place function

$$f : \begin{array}{ccc} G \times G & \to & R^* \\ (g,h) & \mapsto & u_g u_h u_{gh}^{-1} \end{array}, \tag{5}$$

where R^* denotes the multiplicative group of units of R.
Associativity of $R*G$ yields that (5) is a **2-cocycle.**
To keep the action (4) and the 2-cocycle $f \in Z^2_\eta(G, R^*)$ in mind, we denote the corresponding crossed product by $R^f_\eta * G$.

Families of crossed products

Certain crossed products draw special attention.

Families of crossed products

Certain crossed products draw special attention.
When the G-module structure on the base ring R is trivial, in other words, when R is central in $R^f_\eta * G$, then the crossed product $R^f_\eta * G$, or just $R^f * G$, is called a **twisted group ring.**

Families of crossed products

Certain crossed products draw special attention.
When the G-module structure on the base ring R is trivial, in other words, when R is central in $R^f_\eta * G$, then the crossed product $R^f_\eta * G$, or just $R^f * G$, is called a **twisted group ring.**
On the other hand, when the 2-cocycle $f \in Z^2_\eta(G, R^*)$ is identically 1, the corresponding crossed product $R^{\mathbf{1}}_\eta * G$ is called a **skew group ring**.

Families of crossed products

Certain crossed products draw special attention.

When the G-module structure on the base ring R is trivial, in other words, when R is central in $R^f_\eta * G$, then the crossed product $R^f_\eta * G$, or just $R^f * G$, is called a **twisted group ring.**

On the other hand, when the 2-cocycle $f \in Z^2_\eta(G, R^*)$ is identically 1, the corresponding crossed product $R^{\mathbf{1}}_\eta * G$ is called a **skew group ring**.

A skew group ring which is also a twisted group ring is just an (ordinary) group ring RG.

Families of crossed products

Certain crossed products draw special attention.

When the G-module structure on the base ring R is trivial, in other words, when R is central in $R^f_\eta * G$, then the crossed product $R^f_\eta * G$, or just $R^f * G$, is called a **twisted group ring.**

On the other hand, when the 2-cocycle $f \in Z^2_\eta(G, R^*)$ is identically 1, the corresponding crossed product $R^{\mathbf{1}}_\eta * G$ is called a **skew group ring**.

A skew group ring which is also a twisted group ring is just an (ordinary) group ring RG.

An important family of crossed products arises when R is a field and η is a Galois action admitting a fixed field $\mathbb{K}$. In this case $R^f_\eta * G$ is $\mathbb{K}$-central simple and is called a **classical crossed product**.

Cyclic crossed products

When $G := C_n$ is a cyclic group of order n, a crossed product $R^f_\eta * C_n$ is isomorphic to

$$R[y;\eta]/\langle y^n - \beta\rangle,$$

where $R[y;\eta]$ is the **skew polynomial ring**, whose indeterminate y acts on R via the automorphism $\eta(\sigma)$ and $\beta \in R^*$ is η-invariant.

Linear codes, constacyclic codes

Let R be a commutative ring with 1.

Linear codes, constacyclic codes

Let R be a commutative ring with 1.
An R-**linear code of length** n is an R-sublattice of the free R-module $M := R^n$ (called the **ambient space**).

Linear codes, constacyclic codes

Let R be a commutative ring with 1.
An R-**linear code of length** n is an R-sublattice of the free R-module $M := R^n$ (called the **ambient space**).
A code W of length n is **cyclic** if

$$(x_1, x_2 \cdots, x_n) \in W \Rightarrow (x_n, x_1, \cdots, x_{n-1}) \in W.$$

Linear codes, constacyclic codes

Let R be a commutative ring with 1.
An R-**linear code of length** n is an R-sublattice of the free R-module $M := R^n$ (called the **ambient space**).
A code W of length n is **cyclic** if

$$(x_1, x_2 \cdots, x_n) \in W \Rightarrow (x_n, x_1, \cdots, x_{n-1}) \in W.$$

More generally, W is β-**constacyclic** for some $\beta \in R^*$ if

$$(x_1, x_2 \cdots, x_n) \in W \Rightarrow (\beta x_n, x_1, \cdots, x_{n-1}) \in W.$$

Linear codes, constacyclic codes

Let R be a commutative ring with 1.
An R-**linear code of length** n is an R-sublattice of the free R-module $M := R^n$ (called the **ambient space**).
A code W of length n is **cyclic** if

$$(x_1, x_2 \cdots, x_n) \in W \Rightarrow (x_n, x_1, \cdots, x_{n-1}) \in W.$$

More generally, W is β-**constacyclic** for some $\beta \in R^*$ if

$$(x_1, x_2 \cdots, x_n) \in W \Rightarrow (\beta x_n, x_1, \cdots, x_{n-1}) \in W.$$

As can easily be verified, constacyclic codes are ideals of the twisted cyclic group ring $R[y]/\langle y^n - \beta \rangle$.

Crossed product codes

More general families, namely group codes, skew constacyclic codes and classical crossed product codes have been well-studied and shown to yield good parameters.

Crossed product codes

More general families, namely group codes, skew constacyclic codes and classical crossed product codes have been well-studied and shown to yield good parameters.
Although not always explicitly presented in this way, all of those are ideals of certain crossed products $R * G$ which are lattices over R.

Crossed product codes

More general families, namely group codes, skew constacyclic codes and classical crossed product codes have been well-studied and shown to yield good parameters.

Although not always explicitly presented in this way, all of those are ideals of certain crossed products $R * G$ which are lattices over R. The length of such codes is the cardinality of G, and their rank as free R-modules is often denoted as their dimension.

Hamming isometry

Let $\mathcal{B}$ be an R-basis of an R-lattice M. We say that the pair $(M, \mathcal{B})$ is a **based R-lattice**.

Hamming isometry

Let $\mathcal{B}$ be an R-basis of an R-lattice M. We say that the pair $(M, \mathcal{B})$ is a **based R-lattice**.

Such a based R-lattice determines a **Hamming weight**

$$\mathcal{H}_{\mathcal{B}} : \begin{array}{ccc} M & \to & \mathbb{N} \\ \sum_{b \in \mathcal{B}} r_b b & \mapsto & \left| \{ b | \quad r_b \neq 0 \} \right|, \end{array}$$

which, in turn, furnishes M with a metric space structure.

Hamming isometry

Let $\mathcal{B}$ be an R-basis of an R-lattice M. We say that the pair $(M, \mathcal{B})$ is a **based R-lattice**.
Such a based R-lattice determines a **Hamming weight**

$$\mathcal{H}_{\mathcal{B}} : \begin{array}{ccc} M & \to & \mathbb{N} \\ \sum_{b \in \mathcal{B}} r_b b & \mapsto & \left| \{ b | \quad r_b \neq 0 \} \right|, \end{array}$$

which, in turn, furnishes M with a metric space structure.
Note that the unit sphere in the metric space $(M, \mathcal{B})$ is the set of nonzero "monomials" $\{rb\}_{r \in R, b \in \mathcal{B}}$.

Hamming isometry

Let $\mathcal{B}$ be an R-basis of an R-lattice M. We say that the pair $(M, \mathcal{B})$ is a **based R-lattice**.
Such a based R-lattice determines a **Hamming weight**

$$\mathcal{H}_{\mathcal{B}} : \begin{array}{ccc} M & \to & \mathbb{N} \\ \sum_{b \in \mathcal{B}} r_b b & \mapsto & \left| \{ b | \ \ r_b \neq 0 \} \right|, \end{array}$$

which, in turn, furnishes M with a metric space structure.
Note that the unit sphere in the metric space $(M, \mathcal{B})$ is the set of nonzero "monomials" $\{rb\}_{r \in R, b \in \mathcal{B}}$.
The quality of a code, given as a sublattice of the based R-lattice $(M, \mathcal{B})$, is measured by the minimal Hamming distance between its elements (as well as by its length and rank).

An **isometry** between two based R-lattices $(M, \mathcal{B})$ and $(M', \mathcal{B}')$ is defined to be an invertible R-module morphism $\rho : M \to M'$ that satisfies

$$\mathcal{H}_{\mathcal{B}'}(\rho(m)) = \mathcal{H}_{\mathcal{B}}(m) \tag{6}$$

for every $m \in M$.

An **isometry** between two based R-lattices $(M, \mathcal{B})$ and $(M', \mathcal{B}')$ is defined to be an invertible R-module morphism $\rho : M \to M'$ that satisfies

$$\mathcal{H}_{\mathcal{B}'}(\rho(m)) = \mathcal{H}_{\mathcal{B}}(m) \tag{6}$$

for every $m \in M$.
Based lattices are called isometric if such an isometry does exist.

An **isometry** between two based R-lattices $(M, \mathcal{B})$ and $(M', \mathcal{B}')$ is defined to be an invertible R-module morphism $\rho : M \to M'$ that satisfies

$$\mathcal{H}_{\mathcal{B}'}(\rho(m)) = \mathcal{H}_{\mathcal{B}}(m) \tag{6}$$

for every $m \in M$.

Based lattices are called isometric if such an isometry does exist.

A based lattice can be mapped isometrically to itself. We say that an R-module automorphism $\rho : M \to M$ is an isometry of $(M, \mathcal{B})$ if

$$\mathcal{H}_{\mathcal{B}}(\rho(m)) = \mathcal{H}_{\mathcal{B}}(m), \quad \forall m \in M. \tag{7}$$

An **isometry** between two based R-lattices $(M, \mathcal{B})$ and $(M', \mathcal{B}')$ is defined to be an invertible R-module morphism $\rho : M \to M'$ that satisfies

$$\mathcal{H}_{\mathcal{B}'}(\rho(m)) = \mathcal{H}_{\mathcal{B}}(m) \tag{6}$$

for every $m \in M$.
Based lattices are called isometric if such an isometry does exist. A based lattice can be mapped isometrically to itself. We say that an R-module automorphism $\rho : M \to M$ is an isometry of $(M, \mathcal{B})$ if

$$\mathcal{H}_{\mathcal{B}}(\rho(m)) = \mathcal{H}_{\mathcal{B}}(m), \quad \forall m \in M. \tag{7}$$

We stress that the base $\mathcal{B}$ determines the metric in both sides of (7). The isometries of a based R-lattice $(M, \mathcal{B})$ evidently form a group under composition of maps.

Any isometry $\rho : M \to M'$ between $(M, \mathcal{B})$ and $(M', \mathcal{B}')$ maps the unit sphere of one space onto the unit sphere of the other, hence yields a (unique) bijection $\rho' : \mathcal{B} \to \mathcal{B}'$ such that

$$\rho(b) = r_b \rho'(b), \quad \forall b \in \mathcal{B} \tag{8}$$

for some $r_b \in R^*$.

Any isometry $\rho : M \to M'$ between $(M, \mathcal{B})$ and $(M', \mathcal{B}')$ maps the unit sphere of one space onto the unit sphere of the other, hence yields a (unique) bijection $\rho' : \mathcal{B} \to \mathcal{B}'$ such that

$$\rho(b) = r_b \rho'(b), \quad \forall b \in \mathcal{B} \tag{8}$$

for some $r_b \in R^*$.
In fact, given a bijection $\rho' : \mathcal{B} \to \mathcal{B}'$ and invertible coefficients $r_b \in R^*$, condition (8) is also sufficient for a based R-module morphism $\rho : (M, \mathcal{B}) \to (M', \mathcal{B}')$ to be an isometry.

Clearly, isometric lattices M and M' are of the same rank, say n.

Clearly, isometric lattices M and M' are of the same rank, say n. Denote the bases elements $\mathcal{B} = \{b_i\}_{i=1}^n$, and $\mathcal{B}' = \{b'_i\}_{i=1}^n$.

Clearly, isometric lattices M and M' are of the same rank, say n. Denote the bases elements $\mathcal{B} = \{b_i\}_{i=1}^n$, and $\mathcal{B}' = \{b_i'\}_{i=1}^n$. Then the bijection ρ' determines a permutation in the symmetric group Σ_n on n elements.

Clearly, isometric lattices M and M' are of the same rank, say n. Denote the bases elements $\mathcal{B} = \{b_i\}_{i=1}^n$, and $\mathcal{B}' = \{b_i'\}_{i=1}^n$. Then the bijection ρ' determines a permutation in the symmetric group Σ_n on n elements.
By (8), the group $\Gamma_n(R)$ of isometries of a based R-lattice $(M, \mathcal{B})$ of rank n is generated by two subgroups, namely the above symmetry group Σ_n, and the group of invertible diagonal isometries given by n-tuples $(r_{b_1}, \ldots, r_{b_n}) \in (R^*)^n$ as in (8) (with the identity permutation).

Clearly, isometric lattices M and M' are of the same rank, say n. Denote the bases elements $\mathcal{B} = \{b_i\}_{i=1}^n$, and $\mathcal{B}' = \{b'_i\}_{i=1}^n$.
Then the bijection ρ' determines a permutation in the symmetric group Σ_n on n elements.
By (8), the group $\Gamma_n(R)$ of isometries of a based R-lattice $(M, \mathcal{B})$ of rank n is generated by two subgroups, namely the above symmetry group Σ_n, and the group of invertible diagonal isometries given by n-tuples $(r_{b_1}, \ldots, r_{b_n}) \in (R^*)^n$ as in (8) (with the identity permutation).
More precisely, $\Gamma_n(R)$ is the wreath product

$$\Gamma_n(R) = R^* \wr \Sigma_n = (R^*)^n \rtimes \Sigma_n, \tag{9}$$

where Σ_n acts on n-tuples of R^* by permutations.

Clearly, isometric lattices M and M' are of the same rank, say n.
Denote the bases elements $\mathcal{B} = \{b_i\}_{i=1}^n$, and $\mathcal{B}' = \{b'_i\}_{i=1}^n$.
Then the bijection ρ' determines a permutation in the symmetric group Σ_n on n elements.
By (8), the group $\Gamma_n(R)$ of isometries of a based R-lattice $(M, \mathcal{B})$ of rank n is generated by two subgroups, namely the above symmetry group Σ_n, and the group of invertible diagonal isometries given by n-tuples $(r_{b_1}, \ldots, r_{b_n}) \in (R^*)^n$ as in (8) (with the identity permutation).
More precisely, $\Gamma_n(R)$ is the wreath product

$$\Gamma_n(R) = R^* \wr \Sigma_n = (R^*)^n \rtimes \Sigma_n, \qquad (9)$$

where Σ_n acts on n-tuples of R^* by permutations.
The group $\Gamma_n(R)$ is called the **monomial** group of the lattice R^n.

As shown above for constacyclic codes, an R-lattice M can be equipped with an additional ring structure (admitting R as a subring).

As shown above for constacyclic codes, an R-lattice M can be equipped with an additional ring structure (admitting R as a subring).
In this case, a code in the ambient space M is usually considered as an ideal of M which is also an R-sublattice.

As shown above for constacyclic codes, an R-lattice M can be equipped with an additional ring structure (admitting R as a subring).
In this case, a code in the ambient space M is usually considered as an ideal of M which is also an R-sublattice.
An isometry of based R-lattice rings is defined to be a based R-lattices isometry which is also a morphism of rings.

Hamming metric on crossed products

Crossed products ambient spaces are regarded as based R-lattices with a G-graded R-basis of units $\mathcal{B} := \{u_g\}_{g\in G}$.

Hamming metric on crossed products

Crossed products ambient spaces are regarded as based R-lattices with a G-graded R-basis of units $\mathcal{B} := \{u_g\}_{g\in G}$.
The corresponding Hamming weight on $R^f_\eta * G$ is

$$\mathcal{H}_{\mathcal{B}} : \begin{array}{ccc} R^f_\eta * G & \to & \mathbb{N} \\ \sum_{g\in G} \beta_g u_g & \mapsto & \left|\{g| \ \ \beta_g \neq 0\}\right|, \end{array}$$

Hamming metric on crossed products

Crossed products ambient spaces are regarded as based R-lattices with a G-graded R-basis of units $\mathcal{B} := \{u_g\}_{g\in G}$.
The corresponding Hamming weight on $R^f_\eta * G$ is

$$\mathcal{H}_{\mathcal{B}} : \begin{array}{ccc} R^f_\eta * G & \to & \mathbb{N} \\ \sum_{g\in G} \beta_g u_g & \mapsto & \left|\{g| \ \ \beta_g \neq 0\}\right|, \end{array}$$

It is not hard to verify that an isometry between two crossed products of G over R is nothing but G-graded equivalence as defined above.

Distinct choices of an algebra structure and a basis, without which one cannot have a Hamming distance, may essentially yield the same codes.

Distinct choices of an algebra structure and a basis, without which one cannot have a Hamming distance, may essentially yield the same codes.
For example, H.Q. Dinh (2008) gave an example of an algebraic isometry between two "based lattices", one of which determines certain negacyclic codes (constacyclic with $\beta = -1$) while the other one determines certain cyclic ones.

Distinct choices of an algebra structure and a basis, without which one cannot have a Hamming distance, may essentially yield the same codes.

For example, H.Q. Dinh (2008) gave an example of an algebraic isometry between two "based lattices", one of which determines certain negacyclic codes (constacyclic with $\beta = -1$) while the other one determines certain cyclic ones.

It is therefore natural to mod out ambient code spaces by the isometry equivalence relation.

Distinct choices of an algebra structure and a basis, without which one cannot have a Hamming distance, may essentially yield the same codes.
For example, H.Q. Dinh (2008) gave an example of an algebraic isometry between two "based lattices", one of which determines certain negacyclic codes (constacyclic with $\beta = -1$) while the other one determines certain cyclic ones.
It is therefore natural to mod out ambient code spaces by the isometry equivalence relation.

Problem

Let G be a group, R a commutative ring and $\eta : G \to Aut(R)$. Determine the Hamming isometric classes $R_\eta^f * G$ over the 2-cocycles $f \in Z_\eta^2(G, R^*)$.

Hamming isometry classification

The set

$$\mathrm{Aut}_{\eta}(G) := \{\psi \in \mathrm{Aut}(G) | \eta \circ \psi = \eta\}$$

is a subgroup of the automorphism group $\mathrm{Aut}(G)$, which admits a natural action on the corresponding cohomology group $H^2_{\eta}(G, R^*)$. We have

Hamming isometry classification

The set

$$\mathrm{Aut}_\eta(G) := \{\psi \in \mathrm{Aut}(G) | \eta \circ \psi = \eta\}$$

is a subgroup of the automorphism group $\mathrm{Aut}(G)$, which admits a natural action on the corresponding cohomology group $H^2_\eta(G, R^*)$. We have

Theorem

Two crossed products $R^f_\eta * G$ and $R^{f'}_\eta * G$ are isometric if and only if $[f]$ and $[f']$ belong to the same orbit under the $Aut_\eta(G)$-action on $H^2_\eta(G, R^*)$. In other words, fixing an action η, the Hamming isometry classes of crossed products $R^f_\eta * G$ are in one-to-one correspondence with the quotient set $H^2_\eta(G, R^*)/Aut_\eta(G)$.

The group of isometries of a crossed product $R_\eta^f * G$ is a subgroup of the monomial group (that is, the isometries only as based R-lattices) $\Gamma_{|G|}(R) = (R^*)^{|G|} \rtimes \Sigma_{|G|}$, generated by $(R^*)^{|G|}$ and by a subgroup of $\Sigma_{|G|}$ (see equation (9)) as follows.

The group of isometries of a crossed product $R_\eta^f * G$ is a subgroup of the monomial group (that is, the isometries only as based R-lattices) $\Gamma_{|G|}(R) = (R^*)^{|G|} \rtimes \Sigma_{|G|}$, generated by $(R^*)^{|G|}$ and by a subgroup of $\Sigma_{|G|}$ (see equation (9)) as follows.

The group of diagonal isometries $(R^*)^{|G|}$ does not change the cohomology class, i.e. yields crossed products $R_\eta^{f'} * G$ such that the cocycles $f' \in Z_\eta^2(G, R^*)$ are cohomologous to f.

The group of isometries of a crossed product $R_\eta^f * G$ is a subgroup of the monomial group (that is, the isometries only as based R-lattices) $\Gamma_{|G|}(R) = (R^*)^{|G|} \rtimes \Sigma_{|G|}$, generated by $(R^*)^{|G|}$ and by a subgroup of $\Sigma_{|G|}$ (see equation (9)) as follows.
The group of diagonal isometries $(R^*)^{|G|}$ does not change the cohomology class, i.e. yields crossed products $R_\eta^{f'} * G$ such that the cocycles $f' \in Z_\eta^2(G, R^*)$ are cohomologous to f.
The permutations in $\Sigma_{|G|}$ which take care of the multiplicative property of the isometries which correspond to the compatible automorphisms $\mathrm{Aut}_\eta(G)$.

The group of isometries of a crossed product $R_\eta^f * G$ is a subgroup of the monomial group (that is, the isometries only as based R-lattices) $\Gamma_{|G|}(R) = (R^*)^{|G|} \rtimes \Sigma_{|G|}$, generated by $(R^*)^{|G|}$ and by a subgroup of $\Sigma_{|G|}$ (see equation (9)) as follows.
The group of diagonal isometries $(R^*)^{|G|}$ does not change the cohomology class, i.e. yields crossed products $R_\eta^{f'} * G$ such that the cocycles $f' \in Z_\eta^2(G, R^*)$ are cohomologous to f.
The permutations in $\Sigma_{|G|}$ which take care of the multiplicative property of the isometries which correspond to the compatible automorphisms $\mathrm{Aut}_\eta(G)$.

Corollary

The isometry group of a crossed product $R_\eta^f * G$ is

$$(R^*)^{|G|} \rtimes Aut_\eta(G),$$

where $Aut_\eta(G)$ acts on $(R^*)^{|G|}$ as a subgroup of $\Sigma_{|G|}$.

Cyclic crossed products over finite fields

Cyclic crossed products over finite fields

The ingredients in the cyclic case are a cyclic group $C_n = \langle \sigma \rangle$, a finite field $\mathbb{F}_{q^r}$, where q is any prime number, and an action

$$\eta : \begin{array}{ccc} C_n & \to & \mathrm{Aut}(\mathbb{F}_{q^r}) \\ \sigma & \mapsto & \varphi^k, \end{array}$$

where

$$\varphi : x \mapsto x^q, \quad x \in \mathbb{F}_{q^r}$$

is the Frobenius automorphism, which generates the cyclic group $\mathrm{Aut}(\mathbb{F}_{q^r}) \cong C_r$.

Cyclic crossed products over finite fields

The ingredients in the cyclic case are a cyclic group $C_n = \langle \sigma \rangle$, a finite field $\mathbb{F}_{q^r}$, where q is any prime number, and an action

$$\eta : \begin{array}{ccc} C_n & \to & \mathrm{Aut}(\mathbb{F}_{q^r}) \\ \sigma & \mapsto & \varphi^k, \end{array}$$

where

$$\varphi : x \mapsto x^q, \quad x \in \mathbb{F}_{q^r}$$

is the Frobenius automorphism, which generates the cyclic group $\mathrm{Aut}(\mathbb{F}_{q^r}) \cong C_r$.
We may assume that

$$k \in \mathrm{div}(r).$$

Firstly,

$$m := \gcd\left(q^k - 1, \frac{nk}{r}\right) = \left|H^2_\eta(C_n, \mathbb{F}^*_{q^r})\right|.$$

Firstly,

$$m := \gcd\left(q^k - 1, \frac{nk}{r}\right) = \left|H^2_\eta(C_n, \mathbb{F}^*_{q^r})\right|.$$

Next, define an equivalence relation $\sim_\eta$ on the set

$$A_\eta := \{1, \cdots, m\}.$$

Firstly,

$$m := \gcd\left(q^k - 1, \frac{nk}{r}\right) = \left|H^2_\eta(C_n, \mathbb{F}^*_{q^r})\right|.$$

Next, define an equivalence relation $\sim_\eta$ on the set

$$A_\eta := \{1, \cdots, m\}.$$

Two elements $a, b \in A_\eta$ are $\sim_\eta$-equivalent if $aj \equiv b (\text{mod } m)$ for some integer j such that

$$\gcd(j, n) = 1, \text{ and } j \equiv 1 \left(\text{mod } \frac{r}{k}\right).$$

Firstly,

$$m := \gcd\left(q^k - 1, \frac{nk}{r}\right) = \left|H^2_\eta(C_n, \mathbb{F}^*_{q^r})\right|.$$

Next, define an equivalence relation $\sim_\eta$ on the set

$$A_\eta := \{1, \cdots, m\}.$$

Two elements $a, b \in A_\eta$ are $\sim_\eta$-equivalent if $aj \equiv b (\text{mod } m)$ for some integer j such that

$$\gcd(j, n) = 1, \text{ and } j \equiv 1 \left(\text{mod } \frac{r}{k}\right).$$

Theorem

Let $\eta : \sigma \mapsto \varphi^k$ be an action of a cyclic group C_n on a finite field $\mathbb{F}_{q^r}$. Then there is a one-to-one correspondence between the Hamming isometry classes of the crossed products $(\mathbb{F}_{q^r})^f_\eta * C_n$, and the quotient set $A_\eta / \sim_\eta$ as above.

Isometry of constacyclic ambient spaces

A consequence of the above theorem for trivial η re-establishes a result of B. Chen, Y. Fan, L. Lin and H. Liu (2012) for constacyclic codes.

Isometry of constacyclic ambient spaces

A consequence of the above theorem for trivial η re-establishes a result of B. Chen, Y. Fan, L. Lin and H. Liu (2012) for constacyclic codes.

Corollary

The Hamming isometry classes of ambient spaces of $\mathbb{F}_{q^r}$-constacyclic codes of length n, namely the twisted group algebras $(\mathbb{F}_{q^r})^f * C_n$, are in one-to-one correspondence with the set of divisors

$$div(gcd(q^r - 1, n)).$$

As another consequence we can determine when negacyclic codes of length n over the field $\mathbb{F}_{q^r}$ are essentially cyclic.

As another consequence we can determine when negacyclic codes of length n over the field $\mathbb{F}_{q^r}$ are essentially cyclic.
In order to formulate the answer in arithmetic terms we decompose the integers n and $q^r - 1 = |\mathbb{F}_{q^r}|$ to their 2-part and odd-part, that is

$$q^r - 1 = 2^{l_1} m_1, \quad n = 2^{l_2} m_2,$$

where m_1 and m_2 are odd.

As another consequence we can determine when negacyclic codes of length n over the field $\mathbb{F}_{q^r}$ are essentially cyclic.
In order to formulate the answer in arithmetic terms we decompose the integers n and $q^r - 1 = |\mathbb{F}_{q^r}|$ to their 2-part and odd-part, that is

$$q^r - 1 = 2^{l_1} m_1, \quad n = 2^{l_2} m_2,$$

where m_1 and m_2 are odd.
We have

Theorem

Negacyclic codes of length n over the field $\mathbb{F}_{q^r}$ are essentially cyclic if and only if either

1. $q = 2$, *or*
2. $q > 2$ *and* $l_1 > l_2$.