Matrix Constructions derived from Group Rings and Group Matrix Rings with Applications to Algebraic Coding Theory

Adrian Korban

University of Chester

July 6, 2021

Joint works

1. S.T. Dougherty, University of Scranton, USA
2. J. Gildea, University of Chester, UK
3. S. Sahinkaya, Tarsus University, Turkey
4. D. Ustun, Tarsus University, Turkey

Group Rings and the well Established Isomorphism

Let R be a ring and G be a finite group of order n. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in RG$ - **here, R can be any ring**. Define the matrix $\sigma(v) \in M_n(R)$ to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{1}$$

We note that the elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are the elements of the group G in some given order.
The above is a well known map which was introduced in [7].

Group Rings and the well Established Isomorphism

For example,

1. Let G be the cyclic group of order n. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in RG$, then the matrix $\sigma(v)$ has the following form:

$$\sigma(v) = circ(\alpha_{g_1}, \alpha_{g_2}, \alpha_{g_3}, \ldots, \alpha_{g_n}).$$

2. Let G be the dihedral group of order $2n$. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_{2n}} g_{2n} \in RG$, then the matrix $\sigma(v)$ can be of the following form:

$$\sigma(v) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix},$$

where $A = circ(\alpha_{g_1}, \alpha_{g_2}, \ldots, \alpha_{g_n})$, $B = circ(\alpha_{g_{n+1}}, \alpha_{g_{n+2}}, \ldots, \alpha_{g_{2n}})$.

Group Codes

From now on, we assume that R is a finite commutative Frobenius ring.

In [4], group codes over finite Frobenius rings are studied with the use of the well established isomorphism. Namely, define the following group code over a finite commutative Frobenius ring R:

$$\mathcal{C} = \langle \sigma(v) \rangle. \tag{2}$$

The code is formed by taking the row space of $\sigma(v)$ over the ring R.

Group Codes

In [4], it is shown that group codes constructed in this way:

1. Are left ideals in the group ring RG
2. **The automorphism group of $\mathcal{C}$ has a subgroup isomorphic to G**
3. The dual of a group code $\mathcal{C}$ is also a group code
4. Certain codes cannot be of this form, like the putative $[72, 36, 16]$ code

Group Codes

Suggestions for possible research:

1. Can one classify, for example, all extremal binary self-dual codes of a particular length for a specific group? For example, all extremal binary dihedral codes of length 68?
2. Can one investigate group codes over non-commutative rings?

Reversible Group Codes

In [1], the following is shown:
Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{\ell-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G, with $\beta^{-1} = \beta$. We list the elements of $G = \{g_1, g_2, \ldots, g_n\}$ as follows:

$$\{e, h_1, \ldots, h_{\ell-1}, \beta h_{\ell-1}, \beta h_{\ell-2}, \beta h_2, \beta h_1, \beta\}. \tag{3}$$

Theorem

Let R be a finite ring. Let G be a finite group of order $n = 2\ell$ and let $H = \{e, h_1, h_2, \ldots, h_{\ell-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G with $\beta^{-1} = \beta$. List the elements of G as in (3), then any linear G-code in R^n (a left ideal in RG) is a reversible code of index 1.

Reversible Group Codes

Reversibility is a desirable property for constructing DNA codes (please see [1] for details on DNA Codes), therefore, the possible research area is:

1. Can one construct some interesting DNA codes using the above theorem for different groups?

LCD Group Codes

Definition

A Linear Complementary Dual (LCD) Code, is a linear code that has a trivial intersection with its orthogonal.

Currently (work in progress), we are working on group LCD Codes using the well established isomorphism given in Equation (1). Namely, we were able to show the following:

Theorem

Let $v \in RG$. If $C(v)$ is a non-trivial LCD code then $v = v^T$.

We are now in the process of constructing group LCD codes using the well established isomorphism given in Equation (1).

LCD Group Codes

Possible research area?

It is well known that LCD codes have applications in crypto-systems. What we are able to do with the use of the well established isomorphism $\sigma(v)$, is that we can combine the reversibility property together with the condition $v = v^T$ so that one can construct LCD codes that are reversible at the same time.

Question: Would codes that are both: LCD and reversible, have applications in DNA computing?

Generator Matrices of the form $[I_n \mid \sigma(v)]$

In [6], the authors consider generator matrices of the form $[I_n \mid \sigma(v)]$, where $\sigma(v)$ is the well established isomorphism from Equation (1) to construct binary self-dual codes with. The authors only employ groups of orders 16 and 8 to construct binary self-dual codes of length 64 as images of codes of lengths 8 and 16 over the rings $\mathbb{F}_4 + u\mathbb{F}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ respectively. They then apply the well-known extension and neighbour constructions to find new extremal binary self-dual codes of length 68.

Generator Matrices of the form $[I_n \mid \sigma(v)]$

Possible research suggestions:

1. Can one consider groups of orders higher than 8 and 16 to construct interesting and hopefully new binary self-dual codes of different lengths using the generator matrix of the form $[I_n \mid \sigma(v)]$?
2. Can one classify up to equivalence, all binary self-dual codes generated from $[I_n \mid \sigma(v)]$ for different groups?
3. Can one employ the generator matrix of the form $[I_n \mid \sigma(v)]$ to construct interesting codes with, other than binary self-dual codes?

An Extension of the well Established Isomorphism

In [3], the map $\sigma(v)$ is extended to map $\Omega(v)$ so that one can obtain $n \times n$ matrices, fully defined by the elements appearing in the first row, over any ring R, that cannot be obtained from the well-established isomorphism ($\sigma(v)$).

$$\Omega(v) = \begin{pmatrix} \alpha_{g_{1_1}^{-1} g_1} & \alpha_{g_{1_2}^{-1} g_2} & \alpha_{g_{1_3}^{-1} g_3} & \dots & \alpha_{g_{1_n}^{-1} g_n} \\ \alpha_{g_{2_1}^{-1} g_1} & \alpha_{g_{2_2}^{-1} g_2} & \alpha_{g_{2_3}^{-1} g_3} & \dots & \alpha_{g_{2_n}^{-1} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n_1}^{-1} g_1} & \alpha_{g_{n_2}^{-1} g_2} & \alpha_{g_{n_3}^{-1} g_3} & \dots & \alpha_{g_{n_n}^{-1} g_n} \end{pmatrix}, \tag{4}$$

where $g_{j_i}^{-1}$ are simply the group elements.

Such matrices are called **composite matrices**. In [2], these matrices are used to define **composite group codes** with. It is shown that such codes are a family of group codes (left ideals in the group ring), but one can obtain more interesting codes due to the complexity of the matrix structure.

An Extension of the well Established Isomorphism

Advantages of the extended isomorphism:

1. One can obtain interesting codes, for example, self-dual codes that cannot be derived from the map $\sigma(v)$.
2. Certain codes cannot be obtained from this construction, for example, the binary self-dual code with parameters $[72, 36, 16]$.

Suggestions for research:

1. Can one explore other family of linear codes using the composite matrices? For example, LCD codes?
2. Can one classify binary self-dual codes of specific lengths with particular composite matrices?
3. Can one study composite group codes over different alphabets?

Generator Matrices of the form $[I_n \mid \Omega(v)]$

We have considered many generator matrices of the form $[I_n \mid \Omega(v)]$ to construct extremal binary self-dual codes with. We have constructed many such codes with the following parameters:

- Singly-even $[68, 34, 12]$ codes
- Singly-even $[72, 36, 12]$ codes
- Singly-even $[80, 20, 14]$ codes
- Singly-even $[84, 42, 14]$ codes
- Singly-even and Doubly-even $[96, 48, 16]$ codes

Possible research area?

There are still many possible cases to consider for the composite matrix $\Omega(v)$ that can be considered to search for extremal binary self-dual codes of different lengths with.

Group Matrix Rings and the well Established Isomorphism

Let $v = A_{g_1}g_1 + A_{g_2}g_2 + \cdots + A_{g_n}g_n \in M_k(R)G$, that is, each A_{g_i} is a $k \times k$ matrix with entries from the ring R. Define the block matrix $\sigma_k(v) \in M_n(M_k(R))$ to be

$$\sigma_k(v) = \begin{pmatrix} A_{g_1^{-1}g_1} & A_{g_1^{-1}g_2} & A_{g_1^{-1}g_3} & \dots & A_{g_1^{-1}g_n} \\ A_{g_2^{-1}g_1} & A_{g_2^{-1}g_2} & A_{g_2^{-1}g_3} & \dots & A_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{g_n^{-1}g_1} & A_{g_n^{-1}g_2} & A_{g_n^{-1}g_3} & \dots & A_{g_n^{-1}g_n} \end{pmatrix}. \tag{5}$$

Group Matrix Rings and the well Established Isomorphism

Construction 1 For a given element $v \in M_k(R)G$, we define the following code over the matrix ring $M_k(R)$:

$$C_k(v) = \langle \sigma_k(v) \rangle. \tag{6}$$

Here the code is generated by taking the all left linear combinations of the rows of the matrix with coefficients in $M_k(R)$.

Construction 2 For a given element $v \in M_k(R)G$, we define the following code over the ring R. Construct the matrix $\tau_k(v)$ by viewing each element in a k by k matrix as an element in the larger matrix.

$$B_k(v) = \langle \tau_k(v) \rangle. \tag{7}$$

Here the code $B_k(v)$ is formed by taking all linear combinations of the rows of the matrix with coefficients in R. In this case the ring over which the code is defined is commutative so it is both a left linear and right linear code.

Thank you

Please contact me:
email: adrian3@windowslive.com


Y. Cengellemis, A. Dertli, S.T. Dougherty, A. Korban, S. Sahinkaya, "Reversible G-Codes over the ring $\mathcal{F}_{j,k}$ with Applications to DNA Codes", **in submission**.


S.T. Dougherty, J. Gildea, A. Kaya, A. Korban, "Composite Matrices from Group Rings, Composite G- Codes and Constructions of Self-Dual Codes", Des., Codes and Cryptog., doi: https://doi.org/10.1007/s10623-021-00882-8.


S.T. Dougherty, J. Gildea and A. Korban, "Extending an Established Isomorphism between Group Rings and a Subring of the $n \times n$ Matrices", International Journal of Algebra and Computation, https://doi.org/10.1142/S0218196721500223.


S.T. Dougherty, J. Gildea, R. Taylor and A. Tylshchak, "Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes", Des., Codes and Cryptog., vol. 86, no. 9, pp. 2115-2138, 2018.


S.T. Dougherty, A. Korban, S. Sahinkaya, D. Ustun, "Group Matrix Ring Codes and Constructions of Self-Dual Codes", Applicable

Algebra in Engineering, Communication and Computing, doi: https://doi.org/10.1007/s00200-021-00504-9.

J. Gildea, A. Kaya, R. Taylor and B. Yildiz, "Constructions for Self-dual Codes Induced from Group Rings", Finite Fields Appl., vol. 51, pp. 71–92, 2018.

T. Hurley, "Group Rings and Rings of Matrices", Int. Jour. Pure and Appl. Math, Vol. 31, no. 3, pp. 319-335, 2006.