Group rings are simply the best ..

Ted Hurley

National University of Ireland Galway

The Dark Side

A Group Ring colleague asked: “When and why did you go over to the **Dark Side**?”.

The Dark Side

A Group Ring colleague asked: “When and why did you go over to the **Dark Side**?”.

Thoughts:

The Dark Side

A Group Ring colleague asked: “When and why did you go over to the **Dark Side**?”.

Thoughts:

- Fourier matrix diagonalises a circulant matrix. This is actually equivalent to the *convolution theorem* in signal processing. A circulant matrix $\equiv$ an element of a *cyclic group ring*.

The Dark Side

A Group Ring colleague asked: “When and why did you go over to the **Dark Side**?”.

Thoughts:

- Fourier matrix diagonalises a circulant matrix. This is actually equivalent to the *convolution theorem* in signal processing. A circulant matrix $\equiv$ an element of a *cyclic group ring*.
- Many codes and cryptographic schemes can be realised as schemes in groups or group rings.
- Discrete Logarithm problem: Given a power of an element in an algebraic system, find the element.
- Codes used came from zero divisors. Why are the units neglected?
- Computer Scientists and Engineers get all the credit when an algebraic system/idea becomes useful or even essential!

What's a linear block code?

$$GH^T = 0$$

where G is a generator matrix of size $r \times n$ and H is a check matrix of size $(n-r) \times n$.

Entries of the matrices are often in some finite field, but are not restricted to such.

This is an $[n, r]$ code: The *length* is n, the *dimension* r and the *rate* is $\frac{r}{n}$.
$[n, r, d]$: An $[n, r]$ code with (minimum) distance d. A $[n, r, d]$ code can correct $\lfloor \frac{d}{2} \rfloor$ errors. The biggest d can be is $(n - r + 1)$ and a code attaining its biggest possible distance is called a *maximum distance separable*, MDS, code.

Required properties

Possible requirements of a code:

(i) Have a specified large rate.
(ii) Be capable of correcting a specified number of errors; if possible be an MDS code.
(iii) Have efficient encoding and decoding algorithms.

Required properties

Possible requirements of a code:

(i) Have a specified large rate.
(ii) Be capable of correcting a specified number of errors; if possible be an MDS code.
(iii) Have efficient encoding and decoding algorithms.

(iv) Be over a field of characteristics p, ($p = 2$ is special of course),
(v) Be over a field of prime order; in a field of prime order the arithmetic is simply *modular arithmetic*.

Special **type** requirements

In addition special *types* of codes may be required.

- Require a code to contain its dual, $\mathcal{C}^{\perp} \cap \mathcal{C} = \mathcal{C}^{\perp}$. From a dual-containing code, a *Quantum Error Correcting Code*, (QECC), may be constructed – and everyone knows that any mention of *quantum* makes it far more important than anything else(!).

Special **type** requirements

In addition special *types* of codes may be required.

- Require a code to contain its dual, $\mathcal{C}^\perp \cap \mathcal{C} = \mathcal{C}^\perp$. From a dual-containing code, a *Quantum Error Correcting Code*, (QECC), may be constructed – and everyone knows that any mention of *quantum* makes it far more important than anything else(!).
- Require codes such that $\mathcal{C}^\perp \cap \mathcal{C} = 0$: Such a code is called a *Linear Complementary Dual*, LCD, code.
  "LCD codes have been studied amongst other things for improving the security of information on sensitive devices against *side-channel attacks* (SCA) and *fault non-invasive attacks*, and have found use in *data storage* and *communications' systems*."

Special **type** requirements

In addition special *types* of codes may be required.

- Require a code to contain its dual, $\mathcal{C}^\perp \cap \mathcal{C} = \mathcal{C}^\perp$. From a dual-containing code, a *Quantum Error Correcting Code*, (QECC), may be constructed – and everyone knows that any mention of *quantum* makes it far more important than anything else(!).
- Require codes such that $\mathcal{C}^\perp \cap \mathcal{C} = 0$: Such a code is called a *Linear Complementary Dual*, LCD, code.
  "LCD codes have been studied amongst other things for improving the security of information on sensitive devices against *side-channel attacks* (SCA) and *fault non-invasive attacks*, and have found use in *data storage* and *communications' systems*."

Type, elements

- Require that the check matrix of the code has a small number of non-zero elements (relative to its length). Such a code is called a *Low Density Parity Check*, LDPC, code. These codes have, for example, proved useful in medical devices.

Type, elements

- Require that the check matrix of the code has a small number of non-zero elements (relative to its length). Such a code is called a *Low Density Parity Check*, LDPC, code. These codes have, for example, proved useful in medical devices.

This last requirement here can be achieved by looking at units in group rings where one of the unit elements has *small support* compared to the size.

Type, elements

- Require that the check matrix of the code has a small number of non-zero elements (relative to its length). Such a code is called a *Low Density Parity Check*, LDPC, code. These codes have, for example, proved useful in medical devices.

This last requirement here can be achieved by looking at units in group rings where one of the unit elements has *small support* compared to the size.

For Coding Theory and Cryptography, it's the *elements* involved that are important. Algebraists are more interested in *structures*; "All you ever try to use me for is in a bad way - looking for a possible counterexample to a (stupid?) conjecture! I'm better than that! "

It's time to appreciate the beauty and usefulness of the *members* that make up the structures.

Simply the best

Best codes to any *of these requirements and types may be constructed using essentially methods and structures from group rings and their associated matrices.*

Not only that, the linear block codes constructed have *efficient encoding and decoding algorithms*. Complexity is $\max O(n \log n, t^2)$ for a code $[n, r, d]$ where $t = \lfloor \frac{d}{2} \rfloor$.

Here I'll give relatively small prototype examples as an illustration of the general methods.

Simply the best

Best codes to any *of these requirements and types may be constructed using essentially methods and structures from group rings and their associated matrices.*

Not only that, the linear block codes constructed have *efficient encoding and decoding algorithms*. Complexity is $\max O(n\log n, t^2)$ for a code $[n, r, d]$ where $t = \lfloor \frac{d}{2} \rfloor$.

Here I'll give relatively small prototype examples as an illustration of the general methods.

Note: Linear block codes only have been mentioned but convolutional codes, codes with *memory*, to requirements and types, can also be derived by similar methods.

How?

There are a number of structures from group rings and from structures inspired by group rings that enable the conditions and types required to be fulfilled.

How?

There are a number of structures from group rings and from structures inspired by group rings that enable the conditions and types required to be fulfilled.

Some of constructions use Vandermonde/Fourier matrices but not as we know them! Fourier matrices are special types of Vandermonde matrices and we'll restrict our attention to these here as examples.

With a little care on the selection of the rows, MDS (maximum distance separable) codes are obtained by selecting rows from Vandermonde/Fourier matrices. With a *little more care* in the selection, codes to required specifications and types may be constructed.

Dual-containing

Prototype Example: Construct a dual-containing code, preferably also MDS, with rate $\frac{3}{5}$ and which can correct 2 errors. Thus require a $[n, r, n-r+1]$ code with $\frac{r}{n} = \frac{3}{5}$ and $(n-r+1) \geq 5$. Then easily get $n \geq 10$. With $n = 10$ get $r = 6$.

Dual-containing

Prototype Example: Construct a dual-containing code, preferably also MDS, with rate $\frac{3}{5}$ and which can correct 2 errors. Thus require a $[n, r, n-r+1]$ code with $\frac{r}{n} = \frac{3}{5}$ and $(n-r+1) \geq 5$. Then easily get $n \geq 10$. With $n = 10$ get $r = 6$.

Let $\{e_0, e_1, \dots e_9\}$ be the rows of a Fourier 10×10 matrix. Let $\mathcal{C} = \langle e_0, e_1, e_2, e_3, e_4, e_5 \rangle$. Then $\mathcal{C}$ is an MDS $[10, 6, 5]$ code but also $\mathcal{C}^\perp = \langle e_1, e_2, e_3, e_4 \rangle$. Thus $\mathcal{C}$ is dual-containing as $\mathcal{C}^\perp \cap \mathcal{C} = \mathcal{C}^\perp$. (Play with the rows of a Fourier matrix!)

Dual-containing

Prototype Example: Construct a dual-containing code, preferably also MDS, with rate $\frac{3}{5}$ and which can correct 2 errors. Thus require a $[n, r, n - r + 1]$ code with $\frac{r}{n} = \frac{3}{5}$ and $(n - r + 1) \geq 5$. Then easily get $n \geq 10$. With $n = 10$ get $r = 6$.

Let $\{e_0, e_1, \dots e_9\}$ be the rows of a Fourier 10×10 matrix. Let $\mathcal{C} = \langle e_0, e_1, e_2, e_3, e_4, e_5 \rangle$. Then $\mathcal{C}$ is an MDS $[10, 6, 5]$ code but also $\mathcal{C}^\perp = \langle e_1, e_2, e_3, e_4 \rangle$. Thus $\mathcal{C}$ is dual-containing as $\mathcal{C}^\perp \cap \mathcal{C} = \mathcal{C}^\perp$. (Play with the rows of a Fourier matrix!)

$\mathcal{C}$ is a $[10, 6, 5]$ code and so by a special, what is called a CSS, construction, an (MDS) $[[10, 2, 5]]$ quantum code is obtained.

Dual-containing

Prototype Example: Construct a dual-containing code, preferably also MDS, with rate $\frac{3}{5}$ and which can correct 2 errors. Thus require a $[n, r, n-r+1]$ code with $\frac{r}{n} = \frac{3}{5}$ and $(n-r+1) \geq 5$. Then easily get $n \geq 10$. With $n = 10$ get $r = 6$.

Let $\{e_0, e_1, \ldots e_9\}$ be the rows of a Fourier 10×10 matrix. Let $\mathcal{C} = \langle e_0, e_1, e_2, e_3, e_4, e_5 \rangle$. Then $\mathcal{C}$ is an MDS $[10, 6, 5]$ code but also $\mathcal{C}^\perp = \langle e_1, e_2, e_3, e_4 \rangle$. Thus $\mathcal{C}$ is dual-containing as $\mathcal{C}^\perp \cap \mathcal{C} = \mathcal{C}^\perp$. (Play with the rows of a Fourier matrix!)

$\mathcal{C}$ is a $[10, 6, 5]$ code and so by a special, what is called a CSS, construction, an (MDS) $[[10, 2, 5]]$ quantum code is obtained.

Over what fields can the Fourier 10×10 matrix exist? The characteristic must not divide 10 but otherwise a finite field of any other characteristic is available. For example in GF(11), the order of $2 \mod 11$ is 10 so this nice prime order field may be used.

What does a generator matrix look like?

A generator matrix for the (MDS) dual-containing code over $GF(11)$ in the last slide is as follows:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}$$

The entries are taken $\mod 11$. Nice.

What does a generator matrix look like?

A generator matrix for the (MDS) dual-containing code over $GF(11)$ in the last slide is as follows:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\
1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\
1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\
1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\
1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10
\end{pmatrix}$$

The entries are taken $\mod 11$. Nice.

Essentially any rate may be specified and a required number of errors to be corrected can be specified.

Linear complementary dual, LCD, codes

An LCD code is a code $\mathcal{C}$ such that $\mathcal{C} \cap \mathcal{C}^{\perp} = 0$.

Prototype example: Form a 11×11 Fourier matrix. Denote its rows by $\{e_0, e_1, \ldots, e_{10}\}$. Let $\mathcal{C} = \langle e_0, e_1, e_2, e_3, e_8, e_9, e_{10} \rangle$. Then an $[11, 7, 5]$ MDS code (with efficient decoding algorithm) is derived. But also $\mathcal{C}^{\perp} = \langle e_4, e_5, e_6, e_7 \rangle$ so that $\mathcal{C} \cap \mathcal{C}^{\perp} = 0$. Thus an MDS, LCD $[11, 7, 5]$ code is obtained. The rate is $\frac{7}{11}$ and it can correct 2 errors.

Linear complementary dual, LCD, codes

An LCD code is a code $\mathcal{C}$ such that $\mathcal{C} \cap \mathcal{C}^{\perp} = 0$.

Prototype example: Form a 11×11 Fourier matrix. Denote its rows by $\{e_0, e_1, \ldots, e_{10}\}$. Let $\mathcal{C} = \langle e_0, e_1, e_2, e_3, e_8, e_9, e_{10} \rangle$. Then an $[11, 7, 5]$ MDS code (with efficient decoding algorithm) is derived. But also $\mathcal{C}^{\perp} = \langle e_4, e_5, e_6, e_7 \rangle$ so that $\mathcal{C} \cap \mathcal{C}^{\perp} = 0$. Thus an MDS, LCD $[11, 7, 5]$ code is obtained. The rate is $\frac{7}{11}$ and it can correct 2 errors.

If characteristic 2 is required then the smallest suitable field is $GF(2^{10})$. The prime field $GF(23)$ however has elements of order 11. Here then we can work in $GF(23)$ which means the work uses *modular arithmetic*.

A comparison, larger prototypes

In $GF(2^8)$ there exists an element of order $2^8 - 1 = 255$ from which a Fourier 255×255 matrix may be constructed. Thus MDS $[255, r, 255 - r + 1]$ codes may be constructed. By suitable choices, codes $[255, r, 255 - r + 1]$ which are Dual-Containing or which are Linear Complementary Dual may be obtained. High rates and high error-correcting capability are obtainable.

A comparison, larger prototypes

In $GF(2^8)$ there exists an element of order $2^8 - 1 = 255$ from which a Fourier 255×255 matrix may be constructed. Thus MDS $[255, r, 255 - r + 1]$ codes may be constructed. By suitable choices, codes $[255, r, 255 - r + 1]$ which are Dual-Containing or which are Linear Complementary Dual may be obtained. High rates and high error-correcting capability are obtainable.

Compare: $[255, 239, 17], [255, 233, 23]$ may be familiar as the well-known and oft-used *Reed-Solomon codes*. "Reed-Solomon codes of these types are used in data storage systems, hard disk drives and optical communications. The Reed-Solomon $[255, 223, 33]$ is or was the NASA standard for deep space and satellite communications."

Things can only get better..

Over the *prime* field $GF(257)$, (MDS) codes of the form $[256, r, 256 - r + 1]$ may be constructed with efficient decoding algorithms and these can be made dual-containing or Linear Complementary Dual as required. For example $[256, 224, 33]$ has rate $\frac{7}{8}$ and can correct 16 errors.

The arithmetic is modular arithmetic in $GF(257)$. An efficient decoding algorithm is available.

Infinite

Theorems? Yes, many theorems result and the constructions give new light on existing work.

Infinite

Theorems? Yes, many theorems result and the constructions give new light on existing work.

Infinite series of codes to requirements and types may be constructed by the methods.

Infinite series in which the rate approaches a given R, $(0 < R < 1)$, and in which the relative distance $= \frac{distance}{length}$ approaches $(1 - R)$, can be described.

Infinite

Theorems? Yes, many theorems result and the constructions give new light on existing work.

Infinite series of codes to requirements and types may be constructed by the methods.

Infinite series in which the rate approaches a given R, $(0 < R < 1)$, and in which the relative distance $= \frac{distance}{length}$ approaches $(1 - R)$, can be described.

Theorem: "For any communicating channel, there exists error-correcting codes that enables transmissions to approach the Shannon limit." Shannon's proof did not explain how to construct such a code or how to decode it. It depended on 'random' codes, and decoding was a search through all words.

Infinite

Theorems? Yes, many theorems result and the constructions give new light on existing work.

Infinite series of codes to requirements and types may be constructed by the methods.

Infinite series in which the rate approaches a given R, $(0 < R < 1)$, and in which the relative distance $= \frac{distance}{length}$ approaches $(1 - R)$, can be described.

Theorem: "For any communicating channel, there exists error-correcting codes that enables transmissions to approach the Shannon limit." Shannon's proof did not explain how to construct such a code or how to decode it. It depended on 'random' codes, and decoding was a search through all words.

The constructions may be used to give constructive proofs of Shannon's theorem.

Who said it?

“A large part of mathematics which becomes useful, developed with absolutely no desire to be useful, and in a situation where nobody could possibly know in what area it would become useful; and there were no general indications that it ever would be so.”

Who said this?

Who said it?

“A large part of mathematics which becomes useful, developed with absolutely no desire to be useful, and in a situation where nobody could possibly know in what area it would become useful; and there were no general indications that it ever would be so.”

Who said this?

He continued:

“By and large it is uniformly true in mathematics that there is a time lapse between a mathematical discovery and the moment when it is useful; and that this lapse of time can be anything from 30 to 100 years, in some cases even more; and that the whole system seems to function without any direction, without any reference to usefulness, and without any desire to do things which are useful.”

Bridge that GAP

Field Theory comes to mind as taking hundreds of years for the applications to arrive.

Bridge that GAP

Field Theory comes to mind as taking hundreds of years for the applications to arrive.

New Coding Theory and new Cryptography have shortened the gaps considerably.

Bridge that GAP

Field Theory comes to mind as taking hundreds of years for the applications to arrive.

New Coding Theory and new Cryptography have shortened the gaps considerably.

However the tremendous contributions that Group Rings and their associated matrices can and do make to securing best codes and types of required codes have yet to be appreciated. The practitioners continue to grapple with older methods and with newer inefficient methods. The Coding Theorists/Computer Scientists and the Algebraists continue to grapple with one another.

Bridge that GAP

Field Theory comes to mind as taking hundreds of years for the applications to arrive.

New Coding Theory and new Cryptography have shortened the gaps considerably.

However the tremendous contributions that Group Rings and their associated matrices can and do make to securing best codes and types of required codes have yet to be appreciated. The practitioners continue to grapple with older methods and with newer inefficient methods. The Coding Theorists/Computer Scientists and the Algebraists continue to grapple with one another.

That's it!

Ted

Addendum

- “Make it stick” (Number of authors)
- “Make it clear”, “How to speak”: Patrick Winston.