Some algebraic views on chi

Jan Schoone

Radboud University

Thanksgiving 2019
Consider the quadratic map $\chi_n$:

$$\chi_n : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$$

$$(a_0, \ldots, a_{n-1}) \mapsto (b_0, \ldots, b_{n-1})$$

where $b_i = a_i + (a_{i+1} + 1)a_{i+2}$ (indices modulo $n$).

Using linear algebra, we can view $\chi_n$ as

$$\chi'_n : \mathbb{F}_{2n} \rightarrow \mathbb{F}_{2n}$$

$\alpha \mapsto ?$
Why is it possible?

Theorem 1

\[ F_2^n \cong F_2^n \text{ as vector spaces.} \]

**Reason:** Both are \( n \)-dimensional \( F_2 \)-vector spaces.

Given \( F_2^n = \left[ e_0, \ldots, e_{n-1} \right] \) and \( F_2^n = \left[ f_0, \ldots, f_{n-1} \right] \), then

\[ \phi : F_2^n \to F_2^n, \ v = \sum \lambda_i e_i \mapsto \lambda_i f_i \]

is a linear map.

\[ v \in \ker \phi \iff \phi(v) = 0 \]

\[ \iff \sum \lambda_i f_i = 0 \]

\[ \iff \lambda_i = 0 \forall i \]

\[ \iff v = 0 \]
What is $\mathbb{F}_{2^n}$?

**Definition 2**

$\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f)$ where $f$ is an irreducible polynomial of degree $n$.

E.g., $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$. So for $f \in \mathbb{F}_2[X]$ we consider $\overline{f} = f \mod X^3 + X + 1$.

Writing $\alpha = \overline{X}$ we get $\alpha^3 + \alpha + 1 = 0$, hence $\alpha^3 = \alpha + 1$.

$$\mathbb{F}_8 = \{ a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_2 \}.$$  

Clearly 3-dimensional.
The isomorphism

We have now found the basis for $\mathbb{F}_8$:

$$\mathbb{F}_8 = [1, \alpha, \alpha^2].$$

The isomorphism becomes

$$\phi: \mathbb{F}_2^3 \to \mathbb{F}_8, (a, b, c) \mapsto a + b\alpha + c\alpha^2.$$

$\chi_3': \mathbb{F}_8 \to \mathbb{F}_8$ is now given by

$$\chi_3' = \phi \circ \chi_3 \circ \phi^{-1}.$$
Given a function $f : K \rightarrow K$ and a set of pairs 
$$(x_0, f(x_0)), \ldots, (x_{m-1}, f(x_{m-1}))$$
we can approximate $f$ by a univariate polynomial in $K$.

$$\ell_j(t) = \prod_{\substack{i=0,\ldots,m-1 \atop i \neq j}} \frac{t - x_i}{x_j - x_i}$$

are the interpolation polynomials.

Then $\hat{f}(t) = \sum_{i=0}^{m-1} f(x_i) \cdot \ell_i(t)$.

Remark:
$$\ell_j(x_i) = \begin{cases} 
1 & \text{if } i = j; \\
0 & \text{if } i \neq j.
\end{cases}$$

So $\hat{f}(x_i) = f(x_i)$ for all $i \in \{0, \ldots, m - 1\}$. 
We apply Lagrange Interpolation on $\chi'_3$.

$$\widehat{\chi}'_3(t) = \alpha^3 t^6 + \alpha^3 t^5 + t^4 + \alpha^5 t^3 + \alpha^2 t$$

But taking the isomorphism to be

$$\phi: (a, b, c) \mapsto c + b\alpha + c\alpha^2$$

we get:

$$\widehat{\chi}'_3(t) = \alpha^3 t^6 + \alpha^3 t^5 + \alpha^4 t^4 + \alpha^5 t^3 + \alpha^5 t^2 + \alpha t.$$
Remarks on interpolation

1. Since we did the interpolation over all possible inputs, we have \( \hat{\chi}'_3 = \chi'_3 \).

2. For the same reason, we don’t need to compute any inverses for the interpolation polynomials.

\textbf{Reason:} We have

\[
\ell_j(t) = \prod_{i=0, \ldots, m-1 \atop i \neq j} \frac{t - x_i}{x_j - x_i} = \frac{\prod t - x_i}{\prod x_j - x_i}
\]

and

\[
\prod_{i=0, \ldots, m-1 \atop i \neq j} x_j - x_i = \prod_{\beta \in \mathbb{F}_{2^n}^*} \beta = 1 \cdot \gamma \cdot \gamma^2 \cdots \gamma^{2^n-2}
\]

\[
= \gamma \sum_{i=0}^{2^n-2} i = \gamma \frac{1}{2} (2^n - 2)(2^n - 1) = 1.
\]
Definition 3
Given a finite field $\mathbb{F}_{q^n}$, then $\varphi_{\mathbb{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto x^q$ is called the Frobenius automorphism.

Theorem 4
The only automorphisms of $\mathbb{F}_{q^n}$ are $\text{id}, \varphi_{\mathbb{F}}, \varphi_{\mathbb{F}}^2, \ldots, \varphi_{\mathbb{F}}^{n-1}$.

Definition 5
An element $\beta \in \mathbb{F}_{q^n}$ is called a normal element of $\mathbb{F}_{q^n}$ if the set

$$\mathcal{N}_\beta = \{\beta, \varphi_{\mathbb{F}}(\beta), \ldots, \varphi_{\mathbb{F}}^{n-1}(\beta)\}$$

is a linear independent set.
We then call $\mathcal{N}_\beta$ a normal basis for $\mathbb{F}_{q^n}$.
A normal basis for $\mathbb{F}_8$

$\alpha^3$ is a normal element of $\mathbb{F}_8$.

**Reason:**

\[
\begin{bmatrix}
\alpha^3 \\
\alpha^6 \\
\alpha^5 \\
\end{bmatrix}
= \begin{bmatrix}
\alpha + 1 \\
\alpha^2 + 1 \\
\alpha^2 + \alpha + 1 \\
\end{bmatrix}
= \begin{bmatrix}
\alpha + 1 \\
\alpha^2 + 1 \\
\alpha \\
\end{bmatrix}
= \begin{bmatrix}
1 \\
\alpha^2 \\
\alpha \\
\end{bmatrix}
\]

so $\{\alpha^3, \alpha^6, \alpha^5\}$ spans the entire $\mathbb{F}_8$.

An isomorphism can be found in

$$\mathbb{F}_2^3 \rightarrow \mathbb{F}_{2^3}, (a, b, c) \mapsto a\alpha^5 + b\alpha^6 + c\alpha^3$$

Used in cryptography, since squaring is now only a left-shift.
We apply Lagrange Interpolation again, to find:

$$\chi'_3(t) = t^6 + t^4 + t^2$$

It is now a polynomial in $\mathbb{F}_2[t]$!

Changing the isomorphism to

$$(a, b, c) \mapsto a\alpha^3 + b\alpha^6 + c\alpha^5$$

gives us:

$$\chi'_3(t) = t^6.$$
Find an argument as to why the coefficients are in $\mathbb{F}_{2^n}$ with any basis, yet with a normal basis they are in $\mathbb{F}_2$?

Examples show that varying the irreducible polynomial, or the normal element, may yield different results. Is the difference in the results predictable in a clear way?

What irreducible polynomial and normal element combination gives the polynomial representation of $\chi_n$ that has the lowest degree / is the most sparse?
\[ \chi_5(t) = t^{18} + t^{17} + t^{16} + t^{10} + t^9 + t^6 + t^4 + t^2 + t \]