CODES OVER RINGS

STUDENTS / UNIVERSITIES
Şeyda Köse (METU)
Baran Zadeoğlu (Bilkent University)

SUPERVISOR(S)
Cem Güneri

Sabancı Üniversitesi

PURE PROGRAM FOR UNDERGRADUATE RESEARCH

ABSTRACT

In order to investigate linear codes, it is important to factorize polynomials of the type $x^m - \lambda$ over various chain rings into its basic irreducible factors and determine which of these factors are self-reciprocal. In this project we investigate this problem over more general rings when m is a odd prime number.

OBJECTIVES

The initial objective was to work on the following conjecture [1].

Conjecture 3.5 Assume that m is an odd prime and $\gcd(m, q) = 1$, where q is a prime power. Let $\alpha \mid (m-1)$ and $\mathrm{ord}_m(q) = \frac{m-1}{\alpha}$, we can cast the factorization of $x^m - \lambda$ into distinct basic irreducible polynomials over $R_k = \frac{\mathbb{F}_q[u]}{\langle u^k \rangle}$ as follows.

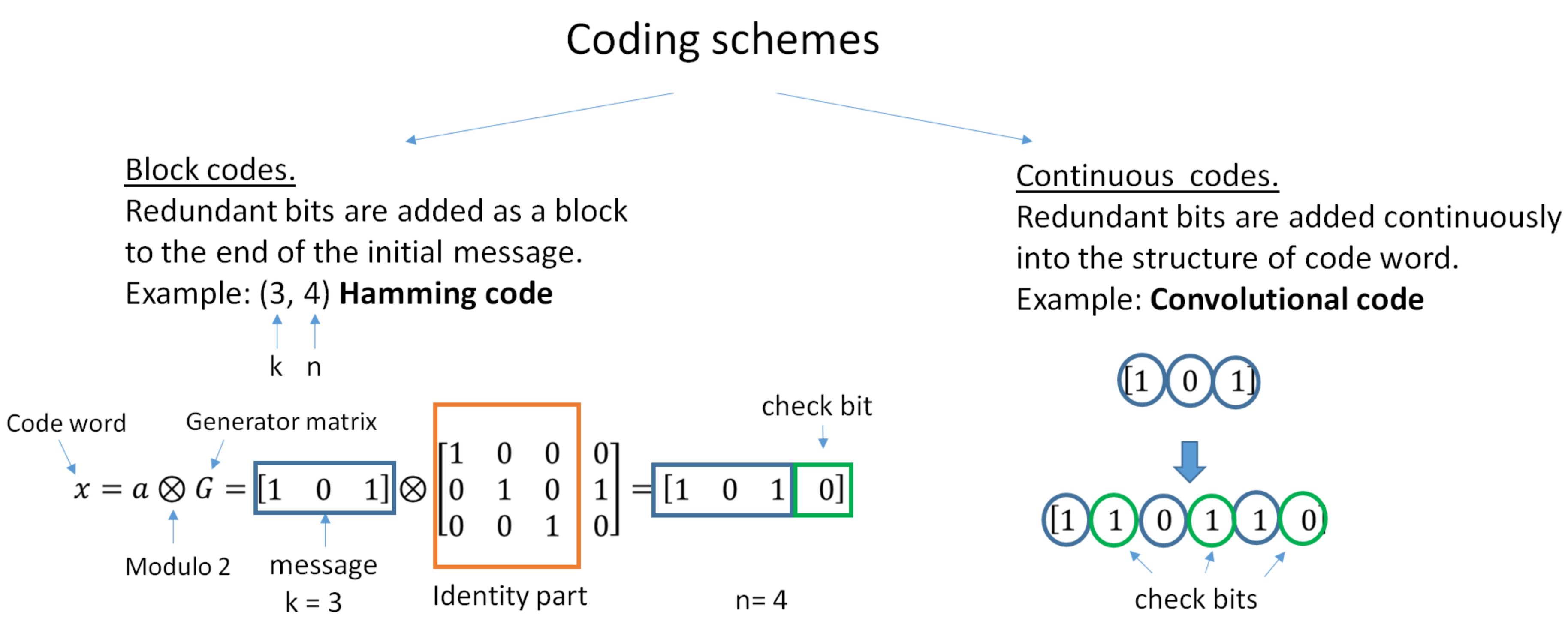
(1) If α is an odd integer, then we have $x^m - \lambda = A(x)\prod_{i=1}^{\alpha} g_i(x)$, where $g_i(x) = g_i^*(x)$, $\deg(g_i(x)) = \frac{m-1}{\alpha}$;

(2) If α is an even integer, then we have $x^m - \lambda = A(x)\prod_{j=1}^{\frac{\alpha}{2}} h_j(x)h_j^*(x)$, where $\deg(h_j(x)) = \deg(h_j^*(x)) = \frac{m-1}{\alpha}$; if

(i) $\lambda = 1$, $A(x) = x - 1$, or
(ii) $\lambda = -1$, $A(x) = x + 1$, or
(iii) $\lambda = 1 + \omega u^t$, q is a power of 2, $A(x) = x + 1 + \omega u^t$, where $t \geq \lceil \frac{k}{2} \rceil$, $\omega \in R_k^\times$.

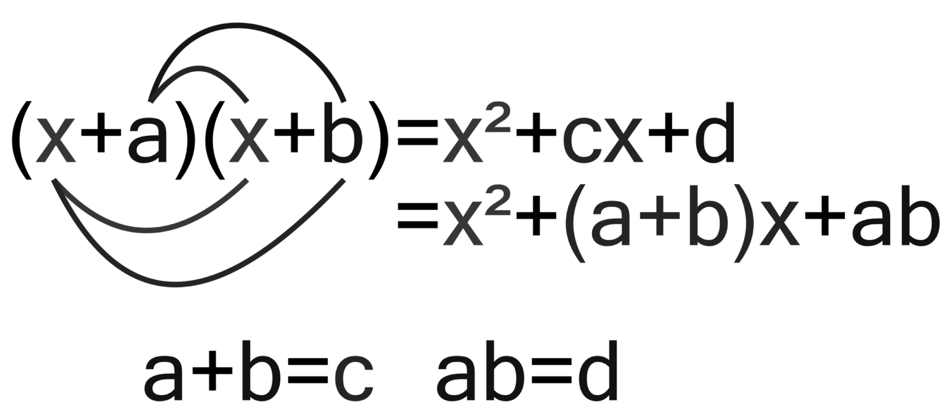
PROJECT DETAILS

- A list of messages can be modelled as vector subspaces over "finite fields" and such subspaces are called "code".
- Modelling a code as a vector space allows us to do linear algebra to it and this makes predicting and analyzing the structure of the codes more convenient.
- We can also use certain algebraic tools and methods of linear algebra to construct a basis for a linear code.



[4]

- Traditional codes are vector subspaces with coefficients from a finite field $\mathbb{F}_q$, such as $\mathbb{Z}_p$ for a prime p.
- One of the benefits of using such algebraic structures is the unique factorization property.



[3]

- Cyclic linear codes can be seen as ideals in $\mathbb{F}_q[X] / <x^m-1>$. Every ideal is principle and generators of these ideals are exactly the factors of x^m-1 over this ring.
- We want to factorize $x^m - \lambda$ over $\mathbb{F}_q[u] / <u^k>$.
- Let $x^m - \lambda = f_1(x)f_2(x)\ldots f_k(x)$ over $\mathbb{F}_q[u] / <u^k>$ where each $f_i(x)$ is irreducible . Then there are 2^k cyclic codes of that length m.
- By the Chinese Reminder Theorem;

$$\frac{R[X]}{<x^m - \lambda>} \cong \frac{R[X]}{<f_1>} \oplus \ldots \oplus \frac{R[X]}{<f_k>}$$

where $R = \mathbb{F}_q[u] / <u^k>$ and $R[X]/<f_i>$ is a field for all i.

- This corresponds to the decomposition of linear codes over $R[X]/<x^m - \lambda>$;

$$C \cong C_1 \oplus C_2 \oplus \ldots \oplus C_k$$

- As a method to factorize a polynomial $f(x)$ over $\mathbb{F}_q[u] / <u^k>$ we can quotient through the ideal $<u>$, use the unique factorization in $\mathbb{F}_q$ and lift the factorization to $\mathbb{F}_q[u] / <u^k>$ via Hensel's lemma [2].
- In fact, we can generalize this factorization to any finite local commutative ring.

CONCLUSION

Over a finite local commutative ring R with the residue field K, let π be the natural quotient map and $char(K) = p$. Define $\ell = \mathrm{ord}_m(q)$, $\alpha = (m-1)/\ell$. Let f be a polynomial in $R[X]$ with $\pi(f) = x^m \pm 1$ in $K[X]$.

We conclude that the conjecture is wrong when both α and ℓ are even. We also proved the following cases;

- When α is odd;
  f splits into a linear component $A(x)$ with $\pi(A(x)) = x \pm 1$ and α many self-reciprocal basic irreducible polynomials of degree ℓ.
- When α is even and ℓ is odd;
  f splits into a linear component $A(x)$ with $\pi(A(x)) = x \pm 1$ and $\alpha/2$ many pair of reciprocal basic irreducible polynomials of degree ℓ.

REFERENCES

[1]Qian, Liqin et al. "On self-dual and LCD quasi-twisted codes of index two over a special chain ring." *Cryptography and Communications* (2018)

[2] McDonald, Bernard R. (1974). *Finite rings with identity*. New York : M. Dekker

[3] By Silver Spoon - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=14994424

[4] By Kirlf - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=76380289