Decoding a Thesis: Properties of Quasi-Cyclic Codes Under the Schur Product

Michael Rudow

A THESIS

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Master of Arts

2017

Supervisor of Thesis

Graduate Group Chairman

1 Acknowledgements

The author would like to acknowledge the invaluable advice he received from Professor Brett Hemenway and Professor Nadia Heninger. As the author's advisers for this thesis, they introduced him to the problem, directed him to background to reading for context, helped him with the plethora of questions that arose, and moreover guided him throughout the research process.

2 Abstract

For a subspace W of a vector space V of dimension n, the schur product space W^k for $k \in \mathbb{N}$ is defined to be the span of all vectors formed by the component-wise multiplication of k vectors in W. It is well known that repeated applications of the schur product to the subspace W creates subspaces $W, W^2, W^3, \ldots$ whose dimensions are monotonically non-decreasing [Ran15]. However, quantifying the structure and growth of such spaces remains an important open problem with applications to cryptography and coding theory. This paper focuses on quasi-cyclic error correcting codes, a subclass of linear spaces particularly relevant to cryptography. Specifically, it qualifies how increasing powers of quasi-cyclic codes grow under the schur product. The paper shows that given a generator of a quasi-cyclic code, it is possible in quadratic time to determine the maximum dimension the code will grow to, as well as the generators for any powers of the code that have achieved that dimension. It also qualifies when powers of the code and or dimension of the code is invariant under the schur product.

3 Introduction

This paper focused on properties of quasi-cyclic codes under the schur product (component-wise multiplication). Quasi-cyclic codes are a special subset of the commonly used linear codes, whose properties under the schur product have been a recent area of research. Due to their efficient descriptions, quasi-cyclic codes have also appeared in variants of the McEliece Cryptosystem [BCGO09]. Furthermore, quasi-cyclic codes, especially cyclic codes, are closely related to cyclic lattices, which have applications to cryptography.

Lattice-based cryptography, such as cryptography based on the shortest vector problem, is becoming increasingly popular due to its post-quantum nature. Replacing traditional lattices with cyclic lattices, which are structurally similar to cyclic codes, may offer a significant improvement in computation time by reducing storage space and matrix-vector product operations [MR08]. Moreover, Micciancio and Regev list as an open question whether using such cyclic lattices will greatly improve the public key length and efficiency of a LWE-based cryptosystem [MR08]. Through understanding properties of cyclic lattices, cryptographers will be more able to avoid incorporating possible structural weaknesses in cryptosystems that might arise from using cyclic lattices. It is a natural extension to explore whether this paper's results can be extended to cyclic lattices due to their similarities. Furthermore, Kositwattanarerk and Oggier show how to produce a lattice from a family of nested binary linear codes which are closed under the schur product [KO14]. Perhaps exploring the subclass of nested cyclic codes that are closed under the schur product will produce lattices with interesting properties. Kositwattanarerk and Oggier also mention that "[c]onnections between lattices and linear codes are classically studied (see e.g. [2]). Lattices constructed from codes often inherit certain properties from the underlying codes and have manageable encoding and decoding complexity"[KO14]. Thus there is reason to believe that some properties of quasi-cyclic codes may translate to the lattices they can construct.

The McEliece Cryptosystem is a well known cryptosystem based on the difficulty of the decoding problem for general linear codes [McE78], and it is believed to remain secure against quantum computing adversaries. While this property makes the McEliece Cryptosystem desirable, the length of the private key is significantly longer than other modern cryptosystems. Through modifying the McEliece Cryptosystem to use quasi-cyclic codes, one can substantially reduce the length of the private key. Unfortunately, certain properties of quasi-cyclic codes can cause such modifications to introduce vulnerabilities to the cryptosystem. For example, in an attempt to reduce the drawback of having a long private key in the McEliece Cryptosystem, Berger, Cayrel, Gaborit, and Otmani described a variant of the cryptosystem using quasi-cyclic codes [BCGO09]. Later, Otmani, Perret, and Tillich as well as Couvreur, Márquez-Corbella, and Pellikaan were able to produce an attacks against the quasi-cyclic code based McEliece system [FOPT10, UL09]. Through another avenue of attacks using properties of codes when squared under the schur product, Couvreur, Otmani, and Tillich were able to successfully break other variants of the McEliece Cryptosystem [COT17]. Specifically, random codes squared under the schur product grow in dimension faster than wild goppa codes, and this enables an attacker to distinguish between certain wild goppa and random codes; through doing so, an attacker can compute a filtration of the public code which can be used to efficiently recover the key [COT17]. Overall, the behaviour of quasi-cyclic codes under the schur product have important applications variants of the McEliece Cryptosystem.

This thesis will focus on properties of quasi-cyclic codes under the schur product. Namely, it will show how a generator for a quasi-cyclic code is sufficient to efficiently compute the following: (1) the dimension the code will grow to under the schur product, (2) the generators for powers of the code after reaching the equilibrium dimension, (3) the criteria under which the code or powers of the code is invariant under powers of the schur product. In doing so, it will supplement the existing framework for the design and analysis of related cryptosystems.

4 Preliminaries

This section will highlight key definitions which will be used throughout the paper. These definitions are closely related to key properties that the theorems will to prove as well as standard building blocks that the proofs will use to do so. It is necessary to learn them not only to follow the proofs, but to understand the motivations behind and consequences of the results.

Definition 4.1 (Schur Product of Vectors)**.** Let C be a code in $\mathbb{F}^n$ and let $c, d \in C$. The *schur product of vectors* c and d, denoted $c * d$, is the component wise product of the codes $(c_1 \cdot d_1, \cdots, c_n \cdot d_n)$.

Definition 4.2 (Ideal Codes)**.** Let $\mathbb{F}$ be a finite field, and $f(x) \in \mathbb{F}[x]$ a polynomial with $\deg(f) = n$. Then for any divisor $g(x)$ of $f(x)$, define the *ideal code*

$$C = \{\text{coeff}(g(x)h(x) \mod f(x)) \mid h(x) \in \mathbb{F}[x]/(f)\} \subset \mathbb{F}^n$$

Definition 4.3 (Linear Code)**.** A code C over $\mathbb{F}^n$ is *linear* if $\forall c_1, c_2 \in C, c_1 + c_2 \in C$ and $\forall a \in F, c \in C, a \cdot c \in C$.

Definition 4.4 (Quasi-Cyclic Codes)**.** Let $\mathbb{F}$ be a finite field, and C an ideal code over $\mathbb{F}$ with modulus $f(x)$.

- When $f(x) = x^n - a$, for some $a \in \mathbb{F}$, the ideal code is called a *quasi-cyclic code.* Quasi-cyclic codes are a subset of linear codes. Let ℓ denote the minimum natural number such that $a^\ell = 1$.

- When $f(x) = x^n - 1$, the ideal code is called a *cyclic code*.

- When $f(x) = x^n + 1$, the ideal code is called a *negacyclic code*.

Definition 4.5 (Support of a vector)**.** For a vector $c \in \mathbb{F}^n$, define

$$\operatorname{supp}(c) = \{i \mid c_i \neq 0\}$$

Definition 4.6 (Coefficients of a polynomial)**.** Let $f(x) = x^n - a$ and $p(x) \in \frac{\mathbb{F}[x]}{f(x)}$. Therefore, $p(x) = \sum_{i=0}^{n} c_i x^i$ where $c_0, \ldots, c_n \in \mathbb{F}$. Then define $\operatorname{coeff}(p(x)) = (c_0, \ldots, c_n)$.

Definition 4.7 (Hamming weight)**.** For a vector $c \in \mathbb{F}^n$, define

$$\operatorname{wt}(c) = |\operatorname{supp}(c)|$$

Definition 4.8 (Minimum distance, minimum weight)**.** Let C be a linear code over $\mathbb{F}^n$. Then the *minimum distance* of C is given by $\min_{c_1, c_2 \in C} \operatorname{wt}(c_1 - c_2)$. Since C is a linear code, $c_1 - c_2 = c_3 \in C$ is defined to be a vector of *minimum weight* in C.

Definition 4.9 (Generator Matrix (G))**.** Let $\mathbb{F}$ be a field and C be a quasi-cyclic code generated by polynomial $g(x)$ of degree $n - k$ which divides $x^n - a$. The *generator matrix* for C is defined as the $k \times n$ matrix where the ith row is equal to $\operatorname{coeff}(x^i \cdot g(x))$. Denote this matrix G. G is upper triangular because $\deg(g(x)) = n - k$.

Definition 4.10 (Standard Form Generator Matrix (G'))**.** Let $\mathbb{F}$ be a field and C be a quasi-cyclic code generated by polynomial $g(x)$ of degree $n - k$ which divides $x^n - a$.

The *standard form generator matrix* for C is defined as the reduced row echelon form of the Generator Matrix G. The reduced Generator Matrix is a $k \times n$ matrix whose leftmost $k \times k$ sub-matrix is I_k. Denote this matrix G'. Denote its ith row as g_i. Note that $g_k = \text{coeff}(x^k \cdot g(x))$ because G is upper triangular and Gaussian Elimination on an upper triangular matrix doesn't change the final row.

Definition 4.11 (Shift)**.** Let $\mathbb{F}$ be a finite field, and C a quasi-cyclic code over $\mathbb{F}$ generated by $g(x)$. Let $c = \text{coeff}(p(x) \cdot g(x)) \in C$ for some polynomial $p(x)$. Then $s^i c$ is defined to be $= \text{coeff}(x^i \cdot p(x) \cdot g(x))$. Moreover, for $c = (c_1, c_2, \cdots, c_{n-1}, c_n)$, it follows that $sc = (a \cdot c_n, c_1, c_2, \cdots, c_{n-1})$

Definition 4.12 (Castelnuovo-Mumford Regularity [Ran15])**.** The *Castelnuovo-Mumford regularity* of a nonzero linear code $C \subseteq \mathbb{F}^n$ is the smallest integer $r = r(C) \geq 0$ such that $\dim(C^r) = \dim(C^{r+i}), \forall i \geq 0$.

Definition 4.13 (Hilbert Sequence [Ran15])**.** Let $C \subseteq \mathbb{F}^n$ be a linear code. The sequence of integers $\dim(C^i), i \geq 0$ is called the dimension sequence, or the *Hilbert Sequence*, of C. The sequence of integers, $d_{\min}(C^i), i \geq 0$ is called the distance sequence of C.

Definition 4.14 (Resultant Polynomial)**.** Let $C \subset \mathbb{F}^n$ be an ideal code with modulus $f(x) = x^n - a$, generator $g(x)$ and dimension k. The Quasi-Cyclic Hilbert Sequence will eventually reach some $C^{z\ell+1}$ such that $|C^{z\ell+1}| = |C^{(z+r)\ell+1}|$ for any natural number r, and $z = r'(C)$. Let $C^{z\ell+1} = (q(x))$ for $n - \deg(q(x)) = |C^{z\ell+1}|$ and $q(0) = 1$. Then $q(x)$ is defined to be the *resultant polynomial* of $g(x)$.

Definition 4.15 (Pattern Polynomial)**.** Let $C \subset \mathbb{F}^n$ be an ideal code with modulus $f(x) = x^n - a$, generator $g(x)|f(x)$ with identity constant term and dimension k. Let $p(x)$ be the highest degree polynomial, with degree $n-v$, $v|n$, and $p(0) = 1$, such that $p(x)|g(x)$ and $\{x^i p(x), 0 \leq i < v\}$ have disjoint support. Then $p(x)$ is defined to be the *pattern polynomial* of $g(x)$. Note, that by transitivity, $p(x)|f(x)$. Furthermore, for non-trivial $g(x)$, since $p(x)|g(x)$, it is clear that $g(x) = p(x) \cdot q(x)$. Thus $deg(p(x)) + deg(q(x)) = n - v + deg(q(x)) = deg(g(x)) < n$, so $g(x) = \sum_{i=0}^{v-1} c_i x^i p(x)$.

5 Prior Work

There have been a number of recent results pertaining to properties of linear codes under the schur product. This section will highlight a few of the results of Randriambololona which are extremely relevant to this paper and will be referenced later.

Lemma 5.1 ([Ran15]). *For any linear code $C \subseteq \mathbb{F}^n$ and $z \geq 1$, $\dim(C^{z+1}) \geq \dim(C^z)$. $d_{min}(C^{z+1}) \leq d_{min}(C^z)$ where d_{min} denotes the minimum distance.*

Lemma 5.2 ([Ran15]). $\forall z \in \{1, \ldots, r(C) - 1\}, \dim(C^{z+1}) > \dim(C^z)$.

Lemma 5.3 ([Ran15]). *For any linear code $C \subseteq \mathbb{F}^n, z \geq 0, z \in \mathbb{Z}$. Then $z \geq r(C)$ if and only if $\dim(C^z) = \dim(C^z)$ which occurs if and only if C^z is generated by a basis of codewords with disjoint supports.*

6 Basic known results about quasi-cyclic codes

This section will introduce well known results about quasi-cyclic codes. In doing so, it will build the framework to support the novel results presented later in the paper. Furthermore, it will introduce the reader to straightforward examples of several proof styles involving quasi-cyclic codes under the schur product. Overall, the material in this section completes the necessary background to understand this paper's results.

Lemma 6.1. *Let $\mathbb{F}$ be a field, and $n \in \mathbb{Z}^+$. Then $\mathbb{F}^n$ is a commutative ring under the schur product with multiplicative identity $1 = 1^n$ and additive identity $0 = 0^n$.*

Proof. $\mathbb{F}$ is a field, so it is a commutative ring. Thus in each component of $\mathbb{F}^n$, the component is a commutative ring with additive identity 0 and multiplicative identity 1. Hence $\mathbb{F}^n$ is a commutative ring with additive identity 0^n and multiplicative identity 0^n under component-wise addition and multiplication.

□

Lemma 6.2 (Consecutive zeros of a quasi-cyclic code)**.** *Let $C \subset \mathbb{F}^n$ be a quasi-cyclic code of dimension k. Then $c \in C$ has k consecutive zeros if and only if $c = 0^n$.*

Proof. In the first direction, if $c = 0^n$ then clearly it contains n consecutive $0's$ hence k consecutive zeroes.

In the second direction, suppose c has k consecutive zeroes starting in position i when c is considered as a one-indexed array. Let $c' = s^{n-i+1}c$ and note that c' has the same number of nonzero indices as c and begins with k consecutive zeroes.

As a quasi-cyclic code of dimension k, C is generated by k linearly independent codewords $c_1, \ldots, c_k$. Let $d_1, \ldots, d_k$ be the result of applying Gaussian Elimination to the matrix whose jth row is c_j. Then $\text{Span}(\{d_1, \ldots, d_k\}) = \text{Span}(C)$. Thus $c' = \sum_{j=1}^{k} a_j d_j = \sum_{j=0} 0 \cdot d_j = 0^n$ because the first k positions of c' are zero, the first k positions of each the d_j's have disjoint support, so in order for $\sum_{j=1}^{k} a_j d_j$ to be zero in the first k positions, $a_j = 0\ \forall j \in \{1, \ldots, k\}$. Since c' and c each have the same number of nonzero positions, then c has n positions that are 0, so $c = 0^n$.

□

Lemma 6.3 (Basis of a quasi-cyclic code). *For any quasi-cyclic code C of dimension k over modulus $x^n - a$ and field $\mathbb{F}$, if C is generated by a polynomial of minimal degree $g(x)$ of degree $n - k$, then $g(x)|x^n - a$ and $\{\text{coeff}(x^i \cdot g(x)) \mid 0 \leq i < k\}$ forms a basis for C.*

Proof. While this is a well known result, a proof is included for completeness. Let $g(x)$ be the generator of C with minimal degree.

The following will prove that $g(x)|x^n - a$. Suppose towards contradiction that $g(x)$ doesn't divide $x^n - a$. Then $d(x) = \gcd(g(x), x^n - a)$ and $\deg(d(x)) < \deg(g(x))$, so $a(x)g(x) + b(x)(x^n - a) = d(x)$. Therefore, $d(x) \in (g(x))$ and $\deg(d(x)) < n - k$, so $\{x^i d(x), 0 \leq i \leq k\}$ are $k + 1$ linearly independent vectors contradicting that g is the generator. Thus $g(x)|x^n - a$ as desired.

The next proof will show that $\{\text{coeff}(x^i \cdot g(x)) \mid 0 \leq i < k\}$ forms a basis for C. Since $\deg(x^i \cdot g(x)) \neq \deg(x^j \cdot g(x)) \forall i \neq j \in \{0, \ldots, k-1\}$, $B = \{x^i \cdot g(x) \mid 0 \leq i < k\}$

is a linearly independent set of size k.

Furthermore, a proof by induction will show $x^i \cdot g(x) \in \text{Span}(B)$. In the base case $i = 0$ so $x^i \cdot g(x) = g(x) \in \text{Span}(B)$. Next, assume in the inductive hypothesis, for $0 \leq i < s$, that $x^i \cdot g(x) \in \text{Span}(B)$. For the inductive step, let $i = s$ then $x^i \cdot g(x) = x \cdot (x^{i-1} \cdot g(x)) = x \cdot \sum_{j=0}^{k-1} c_j x^j g(x)$ for some c_j's by the inductive hypothesis. Thus $x^i \cdot g(x) = \sum_{j=0}^{k-1} c_j x^{j+1} g(x)$. For $j + 1 < k$, $c_j x^{j+1} g(x) \in \text{Span}(B)$, so it suffices to show $x^k g(x) \in \text{Span}(B)$. Since B contains a polynomial of degree x^{n-k+j} for $0 \leq j < k$, $\exists c'(x) \in \text{Span}(B)$ such that $\deg(x^k g(x) - c'(x)) < n - k$. But then $\text{coeff}(x^k g(x) - c'(x))$ ends in at least k zeroes, so by Lemma 6.2, $\text{coeff}(x^k g(x) - c'(x)) = 0^n$. Therefore, $x^k g(x) \equiv c'(x) \in \text{Span}(B)$. This concludes the proof by induction that $x^i \cdot g(x) \in \text{Span}(B)$. Therefore, $(g(x)) = C = \text{Span}(B)$.

Since $C = \text{Span}(B)$ and B is a linearly independent set, it is a basis for C. □

Lemma 6.4 (Minimum weight of a quasi-cyclic code)**.** *Any quasi-cyclic code of length n and dimension k has minimum distance $\geq \frac{n}{k}$. Furthermore, if a code c has weight $\frac{n}{k}$ and its first position where it is nonzero is position p, then c is nonzero exactly in positions $p + z \cdot k$ for $0 \leq z < \frac{n}{k}$.*

Proof. By linearity of C, the code's minimum distance is the same as the minimum weight of a nonzero codeword. Suppose towards contradiction that $c \neq 0^n \in C$ and $\text{wt}(c) < \frac{n}{k}$, let i be the first nonzero index of c and $c' = s^{n+1-i}c$. Hence c' starts with a nonzero index. Let $i_1 < i_2 < \ldots < i_d$ denote the indices of the nonzero coordinates of c'. By assumption, $d < \frac{n}{k}$. The following will prove by induction that

$i_j \leq 1 + (j-1)k$. In the base case, $i_1 = 1$ so it holds. In the inductive hypothesis, assume $i_j \leq 1+(j-1)k$. In the inductive step, $i_{j+1} \leq k+i_j \leq k+1+(j-1)k \leq 1+jk$ by Lemma 6.2. Hence $i_{j+1} \leq 1 + jk$.

Then $i_d \leq 1 + (d-1)k < 1 + (\frac{n}{k} - 1)k = n + 1 - k$. Thus $i_d \leq n - k$ so c' is zero in its final k positions. This means $c' = 0^n$, so $c = 0^n$, which contradicts that $c \neq 0^n$. Hence the original assumption is false, no $c \neq 0^n \in C$ can have $\text{wt}(c) < \frac{n}{k}$.

In the case that $\text{wt}(c) = \frac{n}{k}$, let c' be defined similarly. Replace $d < \frac{n}{k}$ with $d = \frac{n}{k}$ then $i_d \leq 1+(d-1)k$ becomes $i_d \leq 1+(d-1)k = 1+(\frac{n}{k}-1)\cdot k = 1+n-k = n-k+1$. As before, if $i_d < n - k + 1$ there is a contradiction, thus $i_d = n - k + 1$ to avoid contradiction. But in order for this to happen, $i_d - i_1 - 1 = n - k + 1 - 1 = n - k$ and $i_d - i_1 = \sum_{j=1}^{d-1} i_{j+1} - i_j \leq \sum_{j=1}^{d-1} k = (d-1)k = (\frac{n}{k} - 1)k = n - k$ by Lemma 6.2. Equality requires $i_{j+1} - i_j = k$ uniformly. Thus c' is nonzero in and only in positions $1 + z \cdot k$ for $0 \leq z < d$ as desired. A simple shift back from c' to c completes the proof. □

Lemma 6.5 (Generator of a quasi-cyclic code)**.** *Let C be a quasi-cyclic code of length n, dimension k and generator $g(x)$ over modulus $x^n - a$ and field $\mathbb{F}$. Then $\exists q(x)|x^n - a$ such that $(g(x)) = (q(x)) = C$.*

Proof. Suppose no $q(x)$ exists that generates C and $q(x)|x^n - a$. Then $d(x) \cdot g(x) + s(x) \cdot (x^n - a) = q(x)$ for $q(x) = \gcd(g(x), x^n - a)$. Since $d(x) \cdot g(x) \equiv q(x) \mod x^n - a, (q(x)) \subseteq (g(x))$. Since $q(x)|g(x), (g(x)) \subseteq (q(x))$. Furthermore, $x \nmid q(x)$ since $q(x)|x^n - a$ and $x \nmid x^n - a$. Therefore $C = (q(x))$ for $q(x)|x^n - a$ contradicting the assumption.

□

Lemma 6.6 (Schur Product of a quasi-cyclic code)**.** *Let C be a quasi-cyclic code of length n, dimension k and generator $g(x)$ over modulus $x^n - a$ and field $\mathbb{F}$. Let ℓ denote the minimum natural number such that $a^\ell = 1$. Then for $z \in \mathbb{N}$ (where $0 \in \mathbb{N}$), $C^{z\cdot\ell+1}$ is a quasi-cyclic code of length n over modulus $x^n - a$ with generator $q(x)$.*

Proof. Proof by induction on z that $C^{z\cdot\ell+1}$ is a quasi-cyclic code of length n, dimension k over modulus $x^n - a$. In the base case, $z = 0$ so C is by assumption a quasi-cyclic code. In the inductive hypothesis, $C^{(z-1)\cdot\ell+1}$ is assumed to be quasi-cyclic for $z \geq 1$. In the inductive step, it suffices to show $C^{z\cdot\ell+1}$ is an ideal of $x^n - a$ since the domain is a PID and by Lemma 6.5 the generator of the ideal can without loss of generality be assumed to divide $x^n - a$. Note: $C^{z\cdot\ell+1}$ is a linear code.

The following will show that $C^{z\cdot\ell+1}$ is a subgroup under addition. By the inductive hypothesis, $C^{(z-1)\cdot\ell+1}$ is a quasi cyclic code. Take any $p_1(x), p_2(x) \in C^{z\cdot\ell+1}$, and then showing $p_1(x) - p_2(x) \in C^{z\cdot\ell+1}$ shows that the ideal is a subgroup under addition. This holds by virtue of the fact that it is a linear combination of elements of $C^{z\cdot\ell+1}$, which itself is a linear code.

Thus it suffices to show $C^{z\cdot\ell+1}$ is closed under multiplication. Take any $r(x), z(x) \in C^{z\cdot\ell+1}$. Let $r(x) = p(x) * \sum_{i=1}^{\ell} q_i(x)$ for some $p(x) \in C^{(z-1)\cdot\ell+1}$ and $q_i(x) \in C \forall i \in \{1, \ldots, \ell\}$. Let $z(x) = \sum_{i=0}^{n-1} d_i x^i$. Then $r(x) \cdot z(x) = \sum_{i=0}^{n-1} d_i x^i \cdot r(x)$. Since $C^{z\cdot\ell+1}$ is closed under linear combinations, it only remains to be shown that $x^i \cdot r(x) \in C^{z\cdot\ell+1}$

for $i \in \{0, \dots, n-1\}$.

It suffices to show $x^i \cdot r(x) = (x^i \cdot p(x)) * (\pi_{j=1}^{\ell} x^i \cdot q_j(x)) \in C^{z \cdot \ell + 1}$. To do so, it suffices to show $(x^i \cdot r(x))[m] = ((x^i \cdot p(x)) * (\pi_{j=1}^{\ell} x^i \cdot q_j(x)))[m]$. If $m - i \geq 0$ then $(x^i \cdot r(x))[m] = r(x)[m-i] = (x^i \cdot p(x)) * (\pi_{j=1}^{\ell} x^i \cdot q_j(x))[m-i]$ by definition. If $m - i < 0$ then $(x^i \cdot r(x))[m] = r(x)[n+m-i] \cdot a$ and $(x^i \cdot p(x)) * (\pi_{j=1}^{\ell} x^i \cdot q_j(x))[m] = (p(x)[n+m-i] \cdot a) * (\pi_{j=1}^{\ell} \cdot q_j(x)[n+m-i] \cdot a) = (p(x)[n+m-i]) * (\pi_{j=1}^{\ell} q_j(x)[n+m-i]) \cdot a^{\ell+1} = (p(x)[n+m-i] \cdot) * (\pi_{j=1}^{\ell} \cdot q_j(x)[n+m-i]) \cdot a$ as desired since $p(x), q_j(x)$ are all quasi cyclic over $x^n - a$.

$\square$

Example 6.7 (Schur Product of a quasi-cyclic code). There exists a quasi-cyclic code C such that C^d is not quasi-cyclic.

Consider $x^6 - 2 = (x^3+2)(x^3+4)$ over $F = \mathbb{Z} \mod 7$ then $2 \equiv 2 \mod 7, 2^2 \equiv 4 \mod 7, 2^3 \mod 7 \equiv 1$ so $\ell = 3$. Let $g(x) = x^3 + 4$ and $C = (g(x))$. Next, consider C^2, noting that $2 \neq z \cdot \ell + 1$. C is spanned by $(\{x^3+4, x^4+4x, x^5+4x^2\})$.

For any $v_1 \neq v_2 \in \{x^3+4, x^4+4x, x^5+4x^2\}$, $v_1 * v_2 = 0$ since they never both have a nonzero coefficient in the same power of x. Thus C^2 is spanned by $(\{(x^3+4) * (x^3+4), (x^4+4x) * (x^4+4x), (x^5+4x^2) * (x^5+4x^2)\}) = (\{x^3+2, x^4+2x, x^5+2x^2\})$. Suppose towards contradiction that this was a quasi-cyclic code over $x^6 - 2$, then it is generated by $q(x) = x^3 + 2$.

$(x^3+2) \cdot (-x^3) + (x^6 - 2) \equiv -2x^3 - 2 \equiv 5x^3 + 5$

$(x^3+2) \cdot (-5) + (5x^3 + 5) \equiv 2$

$(x^3+2)\cdot 4(-x^3-5)+(4)\cdot(x^6-2)\equiv(x^3+2)\cdot 4(6x^3+2)+(4)\cdot(x^6-2)\equiv(x^3+2)\cdot(3x^3+1)+(4x^6+6)\equiv(3x^6+6x^3+x^3+2)+(4x^6+6)\equiv 1$

If $C^2=(q(x))$ then $|C^2|=6$. Yet $C^{3+1}=((x^3+4)^4)=((x^3+1)*(x^3+4))=(x^3+4)=C$ so $|C^{3+1}|=3<6=|C^2|$. This is a contradiction by Lemma 5.1, so C^2 is not a quasi-cyclic code over x^6-2

As a result of Lemma 6.6 and Example 6.7, the following definitions are needed to reflect that only certain powers of quasi-cyclic codes are quasi-cyclic:

Definition 6.8 (Quasi-Cyclic Castelnuovo-Mumford Regularity)**.** Let C be a quasi cyclic code generated by some $g(x)$ dividing modulus $f(x)=x^n-a$ over $\mathbb{F}$ with $a^\ell=1$. Then the *quasi-cyclic Castelnuovo-Mumford regularity*, $r'(C)=z$ for the unique $z\in\mathbb{Z}$ such that $z\ell+1\geq r(C)>(z-1)\ell+1$.

Definition 6.9 (Quasi-Cyclic Hilbert Sequence)**.** Let $C\subseteq\mathbb{F}^n$ be a quasi-cyclic code generated by some $g(x)$ dividing modulus $f(x)=x^n-a$ over $\mathbb{F}$ with $a^\ell=1$. The *quasi-cyclic Hilbert sequence* of C is defined as $\dim(C^{i\ell+1}), i\geq 0$.

7 Results

This section will introduce the novel results of this paper. In particular, Theorem 7.1 and Theorem 7.2 will qualify the structure for of quasi-cyclic codes that leads to growth under the schur product. Furthermore, Theorem 7.3 will show that such a structure can be efficiently identified. Moreover, Theorem 7.13 and 7.15 will qualify when the code remains invariant under the schur product for powers $z\ell + 1$ for $z \geq r'(C)$ or for any $z\ell + 1$. Finally, Lemma 7.16 will show how the generators for the intermediate codes can be computed efficiently.

Theorem 7.1. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g_0(x)$ and dimension k. Let $q(x)$, with degree $n-k'$, be the resultant polynomial of $g_0(x)$ and $z = r'(C)$. Let $p_0(x)$ be the pattern polynomial of $g_0(x)$. Consider the start of the Quasi-Cyclic Hilbert Sequence $C, \ldots, C^{z\ell+1}$ where $g_i(x)$ is the generator of $C^{i\ell+1}$, and $p_i(x)$ is the pattern polynomial of $g_i(x)$. Then $p_i(x) = p_0(x)^{i\ell+1}$, and so since $g_z(x) = q(x) = \sum_{i=0}^{0} x^0 q(x)$, $p_0(x)^{z\ell+1} = p_z(x) = q(x)$.*

Proof. To show the existence of a pattern polynomial for $g(x)$, it suffices to show that at least one polynomial $p'(x)$ exists which satisfies all the properties of the pattern polynomial other than being of maximal degree, since the pattern polynomial is then taken to simply be the one of highest degree. For any generator $g(x)$, since $1|f(x)$, $\{x^i, 0 \leq i < n\}$ has disjoint support, and $g(x) = \sum_{i=0}^{n-1} c_i x^i \cdot 1$, the polynomial $p'(x) = 1$ satisfies all properties of the pattern polynomial other than perhaps being of maximal degree. Therefore, generator $g(x)$ will necessarily have some pattern polynomial $p(x)$

which may or may not equal 1.

Proof by Induction that $p_i(x) = p_0(x)^{i\ell+1}$. Let $g_0(x) = \sum_{\alpha=0}^{v-1} b_\alpha x^\alpha p_0(x)$. In the base case, it is clear that $p_0(x) = p_0(x)^1$ by definition. In the inductive hypothesis, assume that for $0 \leq i < \zeta$ that $p_i(x) = p_0(x)^{i\ell+1}$ and $g_i(x) = \sum_{j=0}^{v-1} e_j x^j p_i(x)$. In the inductive step, let $i = \zeta$, and it suffices to show $C^{i\ell+1} = (g_i(x))$ where $p_i(x) = p_0(x)^{i\ell+1}$.

By the IH, it is given that $C^{(i-1)\ell+1} = (g_{i-1}(x))$. Then $C^{i\ell+1} = (A)$ for $A = \{(x^j \cdot g_{i-1}(x)) * \Pi_{m=1}^{\ell} x^{h_m} \cdot g_0(x), 0 \leq j < n - \deg(g_{i-1}(x)), 0 \leq h_m < k\}$. Let $w = |C^{i\ell+1}|$. Take any $r(x) = (x^j \cdot g_{i-1}(x)) * \Pi_{m=1}^{\ell} x^{h_m} \cdot g_0(x) \in A$. The following will show that the pattern polynomial of $r(x)$ is given by $p_0(x)^{i\ell+1}$

Case 1: $r(x) = 0$. Then $r(x) = \sum_{j=0}^{w-1} b_j x^j p_0(x)^{i\ell+1}$ for $b_j = 0$ uniformly.

Case 2: $r(x) \neq 0$. Therefore $x^j \cdot g_{i-1}(x) = x^j \sum_{t=0}^{v-1} e_t x^t p_{i-1}(x) = \sum_{m=0}^{v-1} e_t x^{t+j} p_0(x)^{(i-1)\ell+1}$. Since $j + \deg(g_{i-1}(x)) < n$ it means that $e_t = 0$ for any $t + j + \deg(p_0(x)) \geq n$. Thus if $e_t \neq 0$ then $t + j + (n - v) < n$ so $t + j < v$. Then $x^{h_m} \cdot g_0(x) = x^{h_m} \cdot \sum_{a=0}^{v-1} b_a x^a p_0(x) = \sum_{\alpha=0}^{v-1} b_\alpha x^{h_m+\alpha} p_0(x)$. Since $h_m + \deg(g_0(x)) < n$ it means that $b_\alpha = 0$ for any $h_m + \alpha + \deg(p_0(x)) \geq n$. Thus if $b_\alpha \neq 0$ then $h_m + \alpha + (n - v) < n$ so $h_m + \alpha < v$.

$r(x) = (\sum_{t=0}^{v-1} e_t x^{t+j} p_0(x)^{(i-1)\ell+1}) * (\Pi_{m=1}^{\ell} \sum_{\alpha=0}^{v-1} b_\alpha x^{h_m+\alpha} p_0(x))$.

$r(x) = \sum_{t=0}^{v-1} e_t x^{t+j} p_0(x)^{(i-1)\ell+1} * \Pi_{m=1}^{\ell} \sum_{\alpha=0}^{v-1} b_\alpha x^{h_m+\alpha} p_0(x)$.

$\Pi_{m=1}^{\ell} \sum_{\alpha=0}^{v-1} b_\alpha x^{h_m+\alpha} p_0(x) = \sum_{(\delta_1,\ldots,\delta_\ell)\in\Delta} \Pi_{m=1}^{\ell} b_{\delta_m} x^{h_m+\delta_m} p_0(x)$. For some appropriately defined set Δ which has the property that $\forall(\delta_1, \ldots, \delta_\ell) \in \Delta, 0 \leq \delta_m < v$ for $1 \leq m < \ell$ and $h_m + \delta_m < v$. This holds as it is simply a reordering of terms.

$r(x) = \sum_{t=0}^{v-1} e_t x^{t+j} p_0(x)^{(i-1)\ell+1} * (\sum_{(\delta_1,\ldots,\delta_\ell)\in\Delta} \Pi_{m=1}^{\ell} b_{\delta_m} x^{h_m+\delta_m} p_0(x))$.

$r(x) = \sum_{t=0}^{v-1} \sum_{(\delta_1,\ldots,\delta_\ell)\in\Delta} (e_t x^{t+j} p_0(x)^{(i-1)\ell+1}) * \Pi_{m=1}^{\ell} (b_{\delta_m} \cdot x^{h_m+\delta_m} \cdot p_0(x))$.

$r(x) = \sum_{t=0}^{v-1} \sum_{(\delta_1,\ldots,\delta_\ell)\in\Delta} \Pi_{m=1}^{\ell} (e_t \cdot b_{\delta_m})(x^{t+j} p_0(x)^{(i-1)\ell+1}) * (x^{h_m+\delta_m} \cdot p_0(x))$.

By definition $(x^\alpha p_0(x)) * (x^b p_0(x))$ if nonzero for $0 \le \alpha, b < v$ iff $\alpha = b$. Since $0 \le t+j < v, 0 \le h_m + \delta_m < v$ for $1 \le m \le \ell$, $e_t \cdot b_{\delta_m} \ne 0$ if and only if $t+j = h_m + \delta_m$ for $1 \le m \le \ell$. So all nonzero terms have are a constant multiplied by a power of x in $\{0, \ldots, v-1\}$ multiplied by $p_0(x)^{i\ell+1}$. Through eliminating terms which are zero and collecting similar terms, $r(x)$ can be rewritten as $r(x) = \sum_{t=0}^{v-1} f_t x^t p_0(x)^{i\ell+1}$ for appropriately defined f_t's. Since $r(x) \in A$ arbitrarily, $\forall r(x) \in A$, it holds that $r(x) = \sum_{t=0}^{v-1} f_t x^t p_0(x)^{i\ell+1}$ for appropriately defined f_t's.

For any $r(x) \in (A)$, by Lemma 7.4, $r(x)$ can be written as $r(x) = \sum_{t=0}^{v-1} f_t x^t p_0(x)^{i\ell+1}$. Since $g_i(x)$ is a linear combination of terms in (A) and $g_i(0) = 1$, $g_i(x) = \sum_{t=0}^{v-1} f_t x^t p_0(x)^{i\ell+1}$ where $f_0 = 1$

In order to show that $p_0(x)^{i\ell+1}$ is the pattern polynomial for $g_i(x)$, it therefore suffices to show that there is no higher degree polynomial $p'(x)$ which is the pattern polynomial of $g_i(x)$. This will be achieved in a proof by contradiction. Suppose not. Then $g_i(x) = \sum_{t=0}^{v'-1} f'_t x^{t'} p'(x)$ for $v' < v$, $f'_0 = 1$, and $p'(x) = \sum_{j=0}^{\frac{n}{v'}-1} (d')^j x^{v'j}$.

By Lemma 7.4, it is clear that for any $m(x) \in (g_i(x)) = C^{i\ell+1}$, $m(x) = \sum_{j=0}^{v'-1} \beta_j x^j p'(x) = \sum_{j=0}^{n-1} \gamma_j x^j$ which means that whenever $\gamma_j \ne 0$ that $\gamma_y \ne 0$ for $y \equiv j + v' \mod n$ and $y, j \in \{0, \ldots, n-1\}$. Because $p_0(x)$ is the pattern polynomial of $g_0(x)$, there is no pattern polynomial of $g_0(x)$ of degree $n - v' > n - v$ or equivalently $v' < v$. By

Lemma 7.5, $\exists m'(x) \in (g_0(x))$ s.t. $m'(x) = \sum_{j=0}^{n-1} \gamma'_j x^j$ and $\gamma'_j \neq 0$ but $\gamma'_y = 0$ for $y \equiv j \mod v'$. Then $m'(x)^{i\ell+1} \in (g_i(x))$ which is a contradiction. Thus the original assumption is false, no such $p'(x)$ exists. Thus $p_0(x)^{i\ell+1}$ is the pattern polynomial for $g_i(x)$. This concludes the proof of the inductive step and thus the proof by induction that the pattern polynomial of $g_i(x)$ is $p_0(x)^{i\ell+1}$.

□

Theorem 7.2. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$ and dimension k. Let $q(x)$, with degree $n - k'$, be the resultant polynomial of $g(x)$ and $p(x)$ its pattern polynomial. Then the generator $g_z(x)$ for $C^{z\ell+1}$ for $z \geq r'(C)$ is given by $p(x)^{z\ell+1}$.*

Proof. By Theorem 7.1, $q(x) = p(x)^{r'(C)\ell+1}$. Then for $z \geq r'(C)$ let $z' = z - r'(C)$. $C^{z\ell+1} = C^{r'(C)\ell+1} * C^{z'\ell}$. Since $C^{r'(C)\ell+1} = (p(x)^{r'(C)\ell+1})$, $C^{z\ell+1} = \text{Span}(\{p(x)^{r'(C)\ell+1} * \Pi_{i=1}^{z'\ell} x^{b_i} g(x)\})$ for $0 \leq b_i < k$. By definition of the resultant polynomial, $|C^{r'(C)\ell+1}| = |C^{z\ell+1}| = v$. Since coeff$(p(x)^{r'(C)\ell+1} * (x^{b_i} g(x)))$ starts with b_i zeroes and ends in $v-1$ zeroes, $b_i \neq 0 \to p(x)^{r'(C)\ell+1} * (x^{b_i} g(x)) = 0$ by Lemma 6.2. Thus the only nonzero term in the span is $p(x)^{r'(C)\ell+1} * g(x)^{r'(C)\ell+1}$ where $g(x) = p(x) + \sum_{j=1}^{v-1} x^j c_j p(x)$. By similar reasoning, $p(x)^{r'(C)\ell+1} * \sum_{j=1}^{v-1} x^j c_j p(x) = 0$, so the span is generated by $p(x)^{z\ell+1}$.

□

Theorem 7.3. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$, and dimension k. Let w be the length of the input. Clearly $w \geq$*

$\mathrm{wt}(g(x)) + log(n) + log(a)$ *to include a description of* $g(x), n,$ *and* a. *It is possible to compute the pattern polynomial* $p(x)$ *in* $O(w^2)$ *time. After doing so, it is possible to compute* $\{c_i\}$ *such that* $g(x) = \sum_{i=0}^{v-1} c_i x^i p(x)$ *in* $O(v)$ *time.*

Proof. $p(x) = \sum_{j=0}^{\frac{n}{v}-1} \alpha^i x^{vi}$. When $g(x) = \sum_{j=0}^{v-1} c_i x^i p(x)$, $g(x) = \sum_{i=0}^{n-1} b_i x^i$ and without loss of generality, $g(0) = p(0) = 1$. Either $p(x) = u$ for a unit u, or $p(x)$ has two nonzero terms who occur as coefficients for x^0 and x^v. Thus $v \in D \cup \{n\}$ where $D = \{b_i - b_0\} = \{b_i - 1\}$ for $0 \leq i < n$ chosen only from b_i listed in the input. Choose b_i's with increasing order of i to get $D \cup \{n\}$ in an array A that is sorted. Thus a set of set of candidates for v which includes v is acquired in $O(w)$ time.

Furthermore, since at most one element was added to A for each nonzero coefficient of $g(x)$, $|A| < w$. $p(x)$ has the smallest v and therefore largest $\deg(p(x)) = n - v$ for a pattern that fits the other requirements. Therefore, test the candidate v's in increasing order, and halt when v is found that passes the test.

To test a candidate $v \in A$: If $v = n$ it is trivial that $p(x) = 1$. So if that point in the check is reached, it can be computed in $O(1)$. Otherwise, see if $v|n$ and if not discard v. If $v|n$ keep track of d such that $v \cdot d = n$. Then since $c_0 = 1$ it is clear that if the candidate v is correct, then by definition $b_v = 1 \cdot \alpha^1 = \alpha$, as the second nonzero position of $p(x)$ is given by α^1. It is necessary to check $\alpha^{-\frac{n}{v}} = a$ and if not reject this candidate v. Let I be defined as the set of indexes of $g(x)$ that are nonzero and are therefore entered in the input.

Then this v is correct and $p(x)$ is certified by definition if and only if for every starting position $t \in \{0, \ldots, v-1\} \cap I$ it is the case that: $b_t = 0, b_j = 0$ for any $j \equiv t \mod v$ or $b_t \neq 0, b_{t+e\cdot v} = \alpha b_{t+(e-1)\cdot v}$ for every $e \in \{1, \ldots, \frac{n}{v} - 1\}$. After checking all case 1 and 2 possibilities, every single index in I of $g(x)$ has been checked (if an index unchecked, then discard v).

If v passes this test, then $g(x) = \sum_{j=0}^{v-1} c_i x^i p(x)$ where $p(x) = \sum_{j=0}^{\frac{n}{v}-1} \alpha^i x^{vi}$ and $\alpha^{-\frac{n}{v}} = a$ so by Lemma 7.6, $p(x)|f(x)$. If v fails this test, then the pattern polynomial clearly cannot have degree $n - v$ so v should be discarded.

$p(x) = \sum_{j=0}^{n-1} \zeta_j x^j$ where $\zeta_i \neq 0$ if and only if $i \equiv 0 \mod v$. Hence $B = \{x^j p(x), 0 \leq j < v\}$ has disjoint support, since $(x^j p(x))[i] \neq 0$ iff $i \equiv j \mod v$.

$p(x) = \sum_{j=0}^{\frac{n}{v}-1} \alpha^j x^{vj}$ and $\alpha^{-\frac{n}{v}} = a$ so by Lemma 7.6, $p(x)|x^n - a$.

Thus $p(x)$ meets all the requirements to be the pattern polynomial for $g(x)$, so $p(x)$ is the pattern polynomial for $g(x)$.

At most one position was checked that didn't lie on the input $g(x)$ (because if such a position was checked, it would automatically eliminate v) so the total time to check v is $O(w)$ because it is necessary to check every position of $g(x)$ (lest $g(x) = (\sum_{i=0}^{v-1} \beta_i x^i p(x)) + Error$. So total time to check v is $O(w)$. Since $|A| \leq w$ it means there are at most $O(w)$ such v to check. Therefore, time to check all possible v (and thus acquire the correct one) is $O(w^2)$.

Given $p(x)$ with $p(0) = g(0) = 1$, it is clear that $c_i = b_i$. There are at most v such constants so it takes $O(v)$ time to compute them. Thus for $g(x) = \sum_{j=0}^{n-1} b_i x^i$ it the case that $g(x) = \sum_{j=0}^{v-1} b_i x^i p(x)$.

□

Lemma 7.4. *Let A be a set of polynomials such that $\forall r_b(x) \in A, r_b(x) = \sum_{t=0}^{v-1} f_{t,b}x^t p(x)$. Then $\forall r'_b(x) \in (A), r'_b(x) = \sum_{t=0}^{v-1} f'_{t,b}x^t p(x)$.*

Proof. It suffices to show that the property of A is closed under addition and multiplication. For addition Let $r(x) = \sum_{j=0}^{v-1} e_j x^j p(x) \in A, z(x) = \sum_{\alpha=0}^{n-1} c_\alpha x^\alpha p(x) \in A$ Then $r(x) + z(x) = \sum_{j=0}^{v-1}(e_j + c_j)x^j p(x)$ as desired.

It remains to show closure under multiplication. Take any $r(x) = \sum_{j=0}^{v-1} e_j x^j p(x) \in A, z(x) = \sum_{\alpha=0}^{n-1} c_\alpha x^\alpha$. Then $r(x) \cdot z(x) = \sum_{j=0}^{v-1} \sum_{\alpha=0}^{n-1}(e_j c_\alpha)p(x) \cdot x^{\alpha+j}$

$= \sum_{j=0}^{v-1}(\sum_{\alpha=0}^{n-1-j}(e_j c_\alpha)p(x) \cdot x^{\alpha+j} + \sum_{\alpha=n-1-j+1}^{n-1}(e_j c_\alpha)p(x) \cdot x^{\alpha+j-n})$

$= \sum_{j=0}^{v-1}(\sum_{\alpha=0}^{n-1-j}(e_j \cdot c_\alpha \cdot x^{\alpha+j})p(x)) + (\sum_{\alpha=n-j}^{n-1}(e_j \cdot c_\alpha \cdot a \cdot x^{\alpha+j-n})p(x))$. Since $\{x^j p(x), 0 \leq j < v\}$ spans $(p(x))$, it is clear that the above expression $= \sum_{j=0}^{v-1} \beta_j x^j p(x)$. Hence any $m(x) \in (A)$ is given by $m(x) = \sum_{j=0}^{v-1} \beta_j x^j p(x)$ as desired.

□

Lemma 7.5. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$ and dimension k with constant term $= 1$. If $g(x)$ has pattern polynomial $p(x)$ of degree v then for any $v' < v$ s.t. $v'|n$, $\exists m(x) = \sum_{j=0}^{n-1} \beta_j x^j p(x) \in (g(x))$ and $j \neq y \in \{0, \ldots, n-1\}$ s.t. $y \equiv j + v' \mod n$ and $\beta_j \neq 0, \beta_y = 0$*

Proof. Proof by contradiction. Assume not, then $\forall m(x) = \sum_{j=0}^{n-1} \beta_j x^j p(x) \in (g(x))$ and $j \neq y \in \{0, \ldots, n-1\}$ such that $y \equiv j + v' \mod n$, $\beta_j \neq 0$ iff $\beta_y \neq 0$. Then $g(x) = \sum_{j=0}^{v'-1} \alpha_j x^j p_j(x)$ where $p_j(x)$ are each polynomials of degree $n - v'$ which are have nonzero coefficients for all and only terms whose powers are congruent to 0 mod v'.

Furthermore, for any $l(x) = g(x) - d \cdot x^z g(x) \in (g(x)), l(x) = \sum_{j=0}^{v'-1} \gamma_j x^j p'_j(x)$ for some degree $n - v'$ polynomials $p'_j(x)$ who have nonzero coefficients for all and only terms whose powers are congruent to 0 mod v'. This is necessary to prevent having a nonzero constant multiplied by x^j in $l(x)$, but then having zero multiplied by x^y for $y \equiv j \mod v'$.

The following will show that the original $p_j(x)$'s are equal up to multiplication by a unit. Then for $d = -p_\eta(0)p_\theta(0)^{-1}$ it is clear that $p_\eta(x) - d \cdot p_\theta(x) = 0$. The reason is without loss of generality assume $\eta \geq \theta$ then $g(x) - d \cdot x^{\eta-\theta} g(x)$ is zero in position $\eta - \theta$, so it is zero in all positions $\equiv \eta - \theta \mod v'$. This means that it is zero in all positions corresponding to $p_\eta(x) - d \cdot p_\theta(x)$, so $p_\eta(x) - d \cdot p_\theta(x) = 0$. Thus $p_\eta = d \cdot p_\theta$.

So $g(x) = \sum_{j=0}^{v'-1} \gamma_j x^j p'(x)$ for some $p'(x) = p_\eta(x)$ of degree $n - v'$. WLOG, let $p'(x)$ have constant term $= 1$. $B = \{x^j p'(x), 0 \leq j < v'\}$ has disjoint support by definition.

$p'(x) = \sum_{i=0}^{\frac{n}{v'}-1} c_i x^{v'i}$. $\text{supp}(p'(x)) = \text{supp}(x^v p'(x)) = \{y, y \equiv 0 \mod v'\}$. Let d be the coefficient of the term of degree $n - v'$ of $p'(x)$. Then $x^{v'} p'(x) - d \cdot a \cdot p(0)^{-1} p(x) = 0$ since it is zero in the constant term and so it must be zero in every term congruent to $0 \mod v'$, and those were the only nonzero terms. Thus for $e = (d \cdot a \cdot p(0)^{-1})^{-1}$, $x^{v'} p'(x) = e^{-1} p'(x)$. Then $c_{i+1} = ec_i$ and $ae^{\frac{n}{v'}-1} = e^{-1}$, so $e^{-\frac{n}{v'}} \equiv a$. Without loss of generality, let $p'(0) = 1$. $p'(x) = \sum_{i=0}^{\frac{n}{v'}-1} e^i x^{v'i}$ with $e^{-\frac{n}{v'}} \equiv a$ so by Lemma 7.6,

$p'(x)|f(x)$. But also B has disjoint support and $g(x) = \sum_{j=0}^{v'-1} \gamma_j x^j p'(x)$ for $p'(x)$ of degree $n - v' > n - v$. By assumption, $v'|n$, so $p'(x)$ meets all the requirements to be the pattern polynomial of $g(x)$, except perhaps there is polynomial meeting all such requirements of even lower degree. This violates the assumption that $p(x)$ is the pattern polynomial of $g(x)$, thus no such $p'(x)$ exists.

Thus $\exists m(x) = \sum_{j=0}^{n-1} \beta_j x^j p(x) \in (g(x))$ and $j \neq y \in \{0, \ldots, n-1\}$ s.t. $y \equiv j + v' \mod n$ and $\beta_j \neq 0, \beta_y = 0$

□

Lemma 7.6. *Let $v|n$ and $p(x) = \sum_{j=0}^{\frac{n}{v}-1} d^j x^{v'j}$ with $d^{-\frac{n}{v}} = a$. Then $p(x)|x^n - a$.*

Proof. $p(x) \cdot (x^v \cdot a \cdot d - a) = (\sum_{j=0}^{\frac{n}{v}-1} d^{j+1} \cdot a \cdot x^{v(j+1)}) - (\sum_{j=0}^{\frac{n}{v}-1} d^j \cdot a \cdot x^{vj})$

$= (\sum_{j=1}^{\frac{n}{v}} d^j \cdot a \cdot x^{vj}) - (\sum_{j=0}^{\frac{n}{v}-1} d^j \cdot a \cdot x^{vj}) = d^{\frac{n}{v}} \cdot a \cdot x^{v \cdot \frac{n}{v}} + (\sum_{j=1}^{\frac{n}{v}-1} d^j \cdot a \cdot x^{vj}) - (\sum_{j=1}^{\frac{n}{v}-1} d^j \cdot a \cdot x^{vj}) - ax^0$

$= d^{\frac{n}{v}} \cdot a \cdot x^n - a = x^n - a = f(x)$

Thus $p(x) \cdot (x^v \cdot a \cdot d - a) = f(x)$ so $p(x)|x^n - a$. □

Lemma 7.7. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$ and dimension k. The Quasi-Cyclic Hilbert Sequence $C, C^{\ell+1}, C^{2\ell+1}, \ldots$ monotonically increases in dimension until $C^{z\ell+1} = (q(x))$ for some $q(x)|x^n - a$ at which point $|C^{z'\ell+1}| = |C^{z\ell+1}| = k'$ for any $z' \geq z$. Furthermore, $q(x) = \sum_{i=0}^{\frac{n}{k'}-1} d^i x^{i \cdot k'}$ where $d^{-\frac{n}{k}} = a$, $k'|n$, and the minimum weight vector in $(q(x))$ has weight $\frac{n}{k'}$.*

Proof. By Lemma 5.1, it is clear that $\dim(C^{(m+1)\ell+1}) \geq \dim(C^{(m+1)\ell}) \geq \ldots \geq \dim(C^{m\ell+1})$. By Lemma 5.2, it is clear $\dim(C^{(m+1)\ell+1}) > \dim(C^{m\ell+1})$ for $m < r(C)$.

By Lemma 5.3, it is clear that by the existance of $r(C)$, there exists z as desired. Moreover, $z = r'(C)$. At this point, $\dim(C^{z\ell+1}) = \dim(C^{z\ell+2})$ as a linear code by Lemma 5.3 suggest $C^{z\ell+1}$ is generated by $\dim(C^{z\ell+1})$ codewords of disjoint support, and let B be the set of the polynomial representations of such codewords.

Let $q(x) \in B$ with lowest degree. Let $\dim(C^{z\ell+1}) = k'$. Then each of the codewords in B have weight at least $\frac{n}{k'}$ by Lemma 7.10. $\sum_{a(x)\in B} \text{wt}(a(x)) \geq k'\frac{n}{k'} = n$ for $|B| = k'$. In order for this to happen, $\text{wt}(a(x)) = \frac{n}{k'}$ for each $a(x) \in B$, so $k'|n$. Thus by Lemma 7.10, $a(x) = x^m \sum_{j=0}^{\frac{n}{k'}-1} c_{a,i}x^{k'j}$ for some $0 \leq m < k'$ for all $a(x) \in B$. Thus $\deg(q(x)) = n - k', q(x) = \sum_{j=0}^{\frac{n}{k'}-1} c_j x^{k'j}$ and $\{x^i \cdot q(x), 0 \leq i < k'\}$ are k' polynomials of different degrees, thus k' linearly independent polynomials which must span $C^{z\ell+1}$.

Now $\{x^i \cdot q(x), 0 \leq i < n - \deg(q(x))\}$ has disjoint support and generates $C^{z\ell+1}$, a quasi-cyclic code of dimension k' over $x^n - a$. By Lemma 7.11 $q(x) = \sum_{i=0}^{\frac{n}{k'}-1} d^i x^{i\cdot k'}$ where $d^{-\frac{n}{k}} = a$. By Lemma 7.10, $k'|n$ and the minimum weight vector has weight $\frac{n}{k'}$. □

Lemma 7.8. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$, pattern $p(x) = \sum_{j=0}^{\frac{n}{v}-1} d^j x^{vj}$, and dimension k. Let $z = r'(C)$. Then $\forall e \geq z \in \mathbb{N}, C^{e\ell+1} = (p(x))^{e\ell+1})$.*

Proof. Proof by induction that $C^{e\ell+1} = (p(x)^{e\ell+1})$ for $e \geq z$. In the base case, by Theorem 7.1, $C^{z\ell+1} = (q(x)) = (p(x)^{z\ell+1})$. In the inductive hypothesis, assume for some $(e-1) \geq z$ that $C^{(e-1)\ell+1)} = (p(x)^{(e-1)\ell+1})$. In the inductive step, $q(x)g(x)^{(e-z)\ell+1} = p(x)^{e\ell+1} \in C^{e\ell+1}$ is a polynomial of degree $n - v$. Thus $B = \{x^i p(x)^{e\ell+1}, 0 \leq i < v\}$ is a set of v linearly independent vectors in $C^{e\ell+1}$. Since $|C^{z\ell+1}| = n - \deg(p(x)) = v$, $|C^{e\ell+1}| = v$, B spans $C^{e\ell+1}$. Hence $(p(x)^{e\ell+1}) = C^{e\ell+1}$. This concluded the proof by induction.

□

Lemma 7.9. *Let $C \subset \mathbb{F}^n$ for $\mathbb{F}$ a finite field be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$ with pattern $p(x)$ and dimension k. Let $p(x) = \sum_{j=0}^{\frac{n}{v}-1} c_j x^{vj}$. Let $z = r'(C)$. Then $C^{z\ell+1}, C^{(z+1)\ell+1}, C^{(z+2)\ell+1}, \ldots$ forms a cycle of length at most max$(z \cdot |F|, |F|)$ that contains some code generated by $p(x)$*

Proof. By Lemma 7.8, $C^{z'\ell+1} = p(x)^{z'\ell+1}$ for any $z' \geq z$. Consider $m = \max(z \cdot |F|, |F|)$. Then $C^{m\ell+1} = (C^m)^\ell * C = ((p(x)^m)^\ell * p(x)) = ((\sum_{j=0}^{\frac{n}{v}-1} c_i^m x^{jv})^\ell * p(x)) = ((\sum_{j=0}^{\frac{n}{v}-1} x^{jv})^\ell * p(x)) = ((\sum_{j=0}^{\frac{n}{v}-1} x^{jv}) * p(x)) = (p(x))$. Then $C^{(e \cdot m)\ell+1} = (C^m)^{e \cdot \ell} * C = (p(x))$ by a similar argument. This sequence of codes forms a cycle, and the cycle's length is at most m.

□

Lemma 7.10. *Let C be a quasi-cyclic code of size n with generator polynomial, $g(x)$, and dimension k. Then then $B = \{x^i \cdot g(x) \mid 0 \leq i < k\}$ has disjoint support if and only if the minimum weight vector of C has weight $\frac{n}{k}$ and $g(x)$ has minimum weight. This occurs only when $k|n$. In this case, $G = G'$, and $g(x) = \sum_{i=0}^{\frac{n}{k}-1} c_i x^{k \cdot i}$.*

Proof. To begin, note that the minimum weight vector is always an integer. Thus if the minimum weight is $\frac{n}{k}$, then $k|n$ and $n = k \cdot w$. The following argument will use one-indexing.

Suppose c is the minimum weight vector of c and $\mathrm{wt}(c) = \frac{n}{k}$. Then $\exists c'$ s.t. $\mathrm{wt}(c') = \frac{n}{k}$ and $c'[1] = 1$. There are $\frac{n}{k} - 1$ remaining nonzero positions, and each one must occur within k positions of the previous one to avoid violating Lemma 6.2. Thus the final nonzero positions occurs at or before position $k(\frac{n}{k} - 1) + 1 = n - k + 1$. If it occurred before position $n - k + 1$ then the final k positions would be zero, forcing $c' = 0$. Thus the final nonzero position occurs at position $n - k + 1$. Thus there are $\frac{n}{k} - 1$ nonzero indexes each at most k positions apart, spanning a total of $(n - k + 1) - 1 = n - k$ positions. The only way for this to occur is if each nonzero position is exactly k positions apart from the previous one. Thus $c'(x) = \sum_{i=0}^{\frac{n}{k}-1} d_i x^{ki}$.

$(c' - g)[1] = 0$ since $c'[1] = g[1] = 1$. $(c' - g)[n - j] = 0$ for $0 \leq j < k$ since $c'[n - j] = g[n - j] = 0$. Thus k consecutive positions of $c' - g$ are zero, hence $c' - g = 0$ by Lemma 6.2, so $c' = g$. The vectors of B have disjoint support since $\{x^i c'(x), 0 \leq i < k\}$ has the property that $x^i c'(x)$ is nonzero in and only in positions $\equiv i + 1 \mod k$.

Suppose B has disjoint support. $\mathrm{wt}(\sum_{i=1}^{k} g_i) = \sum_{i=1}^{k} \mathrm{wt}(g_i) \leq n$. Furthermore, $\mathrm{wt}(g_i) \geq \frac{n}{k}$ for any g_i. $n \geq \sum_{i=1}^{k} \mathrm{wt}(g_i) \geq \sum_{i=1}^{k} \frac{n}{k} \geq n$ by Lemma 7.10 which requires $\mathrm{wt}(g_i) = \frac{n}{k}$ for every g_i. So $\frac{n}{k}$ is an integer. Since $\forall c \in C, \mathrm{wt}(c) \geq \frac{n}{k}$ by Lemma 7.10 and $\exists c = g \in C$ s.t. $\mathrm{wt}(c) = \frac{n}{k}$ it is clear that $c = g$ is the minimum weight vector.

$G = \{x^i g(x), 0 \leq i < k\}$, and $g(x) = \sum_{i=0}^{\frac{n}{k}-1} d_i x^{ki}$ where $d_0 = 1$ without loss of generality. G is upper triangular since $\deg(g(x)) = n - k$ and it is lower triangular since $g[j] = 0$ for any $j \in \{2, \ldots, k\}$. Thus G is in RREF and $G = G'$. □

Lemma 7.11. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator g and dimension k. Then $B = \{x^i \cdot g(x), 0 \leq i < k\}$ has disjoint support iff $g = u \cdot \sum_{i=0}^{\frac{n}{k}-1} d^i x^{k \cdot i}$ where u is a unit and $d^{-\frac{n}{k}} = a$*

Proof. Suppose $g = u \cdot \sum_{i=0}^{\frac{n}{k}-1} d^i x^{k \cdot i}$ where u is a unit and $d^{-\frac{n}{k}} = a$. Take $(x^i g(x)) * (x^j g(x)) \mid i \neq j \in \{0, \ldots, k-1\}$ Then $x^i g(x)$ is nonzero only in positions congruent to $i \mod k$ and $x^j g(x)$ is only nonzero in positions congruent to $j \mod k$. Since no position is congruent to i and $j \mod k$, no position can be nonzero. Thus $(x^i g(x)) * (x^j g(x)) \equiv 0$. Thus B has disjoint support.

Suppose B has disjoint support. By Lemma 7.10, $g(x) = \sum_{i=0}^{\frac{n}{k}-1} c_i x^{ki}$ and $x^k g = \sum_{i=0}^{k-1} e_i x^i g(x) = e_0 g(x)$ since $x^k g(x)[i] = 0$ for $i \in \{2, \ldots, k\}$. Thus $x^k g(x) = e_0 g(x)$. Hence $c_{i+1} \cdot e_0 = c_i$. So $c_{i+1} = d \cdot c_i$ for $d = e_0^{-1}$. Thus by starting without loss of generality with $c_0 = 1$, then $c_i = d^i$. Hence $g(x) = u \sum_{i=0}^{\frac{n}{k}-1} d^i x^{ki}$ for unit u which makes $c_0 = 1$. Furthermore, since $x^k g(x) \equiv e_0 g(x) \equiv d^{-1} g(x)$, $d^{\frac{n}{k}-1} \cdot a \equiv e_0 \cdot c_0 \equiv d^{-1}$ so $d^{-\frac{n}{k}} \equiv a$.

□

Lemma 7.12. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$ and pattern polynomial $p(x)$ of dimension v. If $C^{z\ell+1} = C^{(z+1)\ell+1}$, then every nonzero coefficient y of $p(x)$ satisfies $y^\ell = 1$.*

Proof. Clearly, by definition of the Quasi-Cyclic Castelnuovo-Mumford Regularity, $z \geq r'(C)$. Hence $C^{z\ell+1} = (q(x) * p(x)^{z'\ell})$ for some non negative integer z' by Theorem 7.1. But also by Theorem 7.1, $q(x) = p(x)^{r'(C)\ell+1}$, so $C^{z\ell+1} = (p(x)^{z\ell+1})$. so $|C^{z\ell+1}| =$

$n - \deg(p(x)^{z\ell+1}) = n - \deg(p(x)) = v$. Furthermore, $p(x)^{z\ell+1} = u \cdot p(x)^{z\ell+1} * p(x)^{\ell}$.

By definition, $p(x) = u' \cdot \sum_{i=0}^{\frac{n}{k}-1} d^i x^{k \cdot i}$ where u' is a unit. But without loss of generality, let $p(0) = 1$. Then $p(0)^{(z+1)\ell+1} = p(0)^{z\ell+1} = 1$. Therefore, $p(0)^{z\ell+1} - p(0)^{(z+1)\ell+1} = 0$ and $\deg(p(x)^{z\ell+1} - p(x)^{(z+1)\ell+1}) = \deg(p(x)) = n - v$. Hence $p(x)^{z\ell+1} - p(x)^{(z+1)\ell+1}$ contains v consecutive zeroes, so by Lemma 6.2, $p(x)^{z\ell+1} - p(x)^{(z+1)\ell+1} = 0$. Thus $p(x)^{z\ell+1} = p(x)^{z\ell+1} * p(x)^{\ell}$ so $p(x)^{\ell}$ is 1 in every nonzero position. Therefore the nonzero coefficients y of $p(x)$ are all such that $y^{\ell} = 1$.

□

Theorem 7.13. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator g, dimension k, pattern polynomial $p(x)$ of degree $n - v$, and resultant polynomial $q(x)$. Then $C^{z \cdot \ell+1} = C^{(z+1) \cdot \ell+1}$ if and only if $z \geq r'(C)$ and $p(x) = u \cdot \sum_{i=0}^{\frac{n}{v}-1} d^i x^{v \cdot i}$ where u is a unit and $d^{\ell} = 1$ (note since that format has disjoint support, $d^{-\frac{n}{v}} = a$)*

Proof. First suppose $C^{z\ell+1} = C^{(z+1)\ell+1}$. Clearly, by definition of the Quasi-Cyclic Castelnuovo-Mumford Regularity, $z \geq r'(C)$. Hence $C^{z\ell+1} = q(x) * p(x)^{z'\ell}$ for some non negative integer z' by Corollary 7.20. But also by Theorem 7.1, $q(x) = p(x)^{r'(C)\ell+1}$, so $C^{z\ell+1} = p(x)^{z\ell+1}$. Thus $p(x)^{z\ell+1} = u \cdot p(x)^{z\ell+1} * p(x)^{\ell}$.

By definition and an application of Lemma 7.11, $p(x) = u' \cdot \sum_{i=0}^{\frac{n}{v}-1} d^i x^{v \cdot i}$ where u' is a unit and $d^{-\frac{n}{v}}$. By Lemma 7.12, every nonzero coefficient y of $p(x)$ satisfies $y^{\ell} = y$. Therefore, either $p(x) = 1$ and $1^{\ell} = 1$ or $d^1 = d$ is a nonzero coefficient of $p(x)$ and $d^{\ell} = 1$.

Suppose $p(x) = u \cdot \sum_{i=0}^{\frac{n}{v}-1} d^i x^{v \cdot i}$ where u is a unit, $d^\ell = 1$, and $z \geq r'(C)$. By Theorem 7.1, $g(x)^{z\ell+1} = q(x) \cdot p(x)^{z'\ell}$ for some non negative integer z'. Therefore, $C^{z\ell+1} = (p(x)^{z\ell+1})$ and $C^{(z+1)\ell+1} = (p(x)^{(z+1)\ell+1})$. $p(x)^{(z+1)\ell+1} = p(x)^{z\ell} * p(x)^{z\ell+1} = p(x)^{z\ell+1}$ because every nonzero coefficient of $p(x)^{z\ell+1}$ is multiplied by some $y^\ell = 1$ from the corresponding coefficient of $p(x)^\ell$. So $C^{z\ell+1} = (p(x)^{z\ell+1}) = (p(x)^{(z+1)\ell+1}) = C^{(z+1)\ell+1}$.

□

Corollary 7.14. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator g, dimension k, pattern polynomial $p(x)$ of dimension v. Then $C^{1+\ell} = C$ if and only $k|n$ and $g = u \cdot \sum_{i=0}^{\frac{n}{k}-1} d^i x^{k \cdot i}$ where u is a unit and $d^\ell = 1$ (note since that format has disjoint support, $d^{-\frac{n}{k}} = a$)*

Proof. First suppose $C = C^{\ell+1}$. Clearly, $r'(C) = 0$ so $C^{z\ell+1} = C^1$ for $z = 0$ has $z \geq r'(C)$. Then $g(x)$ is its own resultant polynomial, so $g(x) = p(x)^1 = p(x)$ and $k = v$. By Theorem 7.13, $p(x) = u \cdot \sum_{i=0}^{\frac{n}{v}-1} d^i x^{v \cdot i} = g(x)$ for $d^\ell = 1$.

Suppose $g(x) = u \cdot \sum_{i=0}^{\frac{n}{k}-1} d^i x^{k \cdot i}$ where u is a unit and $d^\ell = 1$. By definition, $g(x) = p(x)$ then by Theorem 7.13, $C^{(z+1)\ell+1} = C^{z\ell+1}$ for $z = 0$. Hence $C^{\ell+1} = C$. □

Theorem 7.15. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$, dimension k and pattern polynomial $p(x)$. Then $|C^{1+z \cdot \ell}| = |C| = k$ if and only if $g(x) = p(x)$ (Thus $C^{1+z \cdot \ell} = (g(x)^{1+z \cdot \ell})$)*

Proof. In the first direction, let $|C^{1+z \cdot \ell}| = |C|$. C is generated by $B = \{x^i g(x), 0 \leq i < k\}$. B has disjoint support otherwise without loss of generality $\exists i < j \in \{0, \ldots, k-1\}$

and $(x^i g(x))^{z\cdot\ell} * (x^j g(x)) \neq 0$. But $x^i g(x)$ ends in $k-i-1$ zeroes, and by $x^j g(x)$ it begins with j zeroes, so $(x^i g(x))^{z\cdot\ell}(x^j g(x))$ has $k+(j-i)-1 \geq k$ consecutive zeroes. Therefore, by Lemma 6.2, it is zero, which is a contradiction. Thus B has disjoint support. Then by Lemma 7.11, $g(x) = u \cdot \sum_{i=0}^{\frac{n}{k}-1} d^i x^{k\cdot i}$ where u is a unit, $k|n$ and $d^{-\frac{n}{k}} = a$, so $p(x) = g(x)$. Then by Theorem 7.1, $C^{1+z\cdot\ell} = (p(x)^{1+z\cdot\ell}) = (g(x)^{1+z\cdot\ell})$

In the reverse direction, if $g(x) = p(x)$ then C is generated by codewords of pairwise disjoint support, so by Lemma 5.3, $1 \geq r(C)$ so $r'(C) = 0$. Therefore, $|C| = |C^{1+z\cdot\ell}|$. Then by Theorem 7.1, since $g(x)$ is its own resultant polynomial, $C^{1+z\cdot\ell} = (p(x)^{1+z\cdot\ell}) = (g(x)^{1+z\cdot\ell})$

□

Lemma 7.16. *Given any quasi-cyclic code C where $|C| = k$ and given at least k linearly independent code words $c_1, \ldots, c_j$ for $j \geq k$, it is possible to determine g s.t. $(g) = C$ in $O(k^2 n)$ operations. Furthermore, given $C = (g(x))$ it is possible to determine q s.t. $(q) = C^{1+z\cdot\ell}$ given a basis for C in $O(n^4 log(z\cdot\ell))$ operations. Given $C = (g(x))$ it is possible to acquire the resultant polynomial $q(x)$ in $O(n^4 log(n))$ operations. Given $C = (g(x))$ it is possible to determine q s.t. $(q) = C^{1+z\cdot\ell}$ given a basis for C in $O(n^4 log(n) + n log(z\cdot\ell))$ operations. Note, while it is possible to encode $g(x)$ in roughly* $\mathrm{wt}(\mathrm{coeff}(g(x)))$ *input length, when working with vectors of length n, it is not unreasonable to want poly(n) time solution algorithms.*

Proof. Form G' by taking $c_1, \ldots, c_k$ and applying gaussian elimination. The kth row of G', g_k will be the final nonzero row and will be the representation of $s^{k-1}g$. It is represented by $(0^{k-1}, 1, \ldots)$. Thus by taking $s^{-(k-1)}g_k$, the possibility of multiplying the shifted positions by a^{-1} is irrelevant since all such positions are zero. Then the representation of g is $s^{-(k-1)}g_k$ and given the vector representation of g, $g(x)$ is easily determined.

There are k steps to the gaussian elimination for k rows. In each step, the pivot position moves to the right one. It takes $O(k)$ operations to find the row from the remaining rows that is nonzero in the pivot position. If none exist, then this extra computation is wasted. But it only occurs at most $O(n)$ times and $O(k \cdot n)$ doesn't effect the asymtotic runtime. If at least one row exists, it takes $O(n)$ time to swap the first remaining row and that row, and $O(n)$ operations to multiply the new first row by the appropriate value to have it begin with a leading 1. Then to reduce the remaining rows, it takes $O(n)$ time (one multiplication, and one subtraction) per row for k rows, so $O(k \cdot n)$ time. There are $O(k)$ leading ones in G', so this $O(k \cdot n)$ penalty is paid at most $O(k)$ times for a total cost of $O(k^2 \cdot n)$.

Given a basis of C, it is possible to determine a basis of $C^{1+z\cdot\ell}$ through use the method of repeated squaring to determine the basis for $C, C^2, C^4, \ldots$ until acquiring C^b for $b \leq 1 + z \cdot \ell < 2b$. Then create a product tree of the $b = log(1 + z \cdot \ell)$ at most $n \times n$ matrix representations of the basis, including the C^e's for e such that the eth bit of $1 + z \cdot \ell$ is 1. This tree involves at most b products. For each product, taking $E * F$ for $n \times n$ matrices E, F will create a $n^2 \times n$ matrix. This takes $O(n^3)$ time because there are $O(n^2)$ combination of rows, and the schur product of two rows involves n multiplications. Then gaussian elimination is applied by focusing on $O(n)$ pivot positions, taking $O(n^2)$ operations to find a row with nonzero first position, swap it to the first position, and multiply it by a value to make its first position 1. Or if none exists, there are no further operations on that pivot. Afterwords, it takes $O(n)$ operations (via a subtraction) to reduce each of the remaining $O(n^2)$ rows accordingly. Thus each pivot costs $O(n^3)$ operations, and there are $O(n)$ pivots. After the final pivot is acquired, the final $n^2 - n$ rows are removed to leave an $n \times n$ matrix. Since, at any intermediate step, there can be at most n linearly independent thus nonzero rows, this simplification is legitimate. Thus total number of operations is $O(n^4)$. This computation is completed $O(log(1 + z \cdot \ell))$ times, so total operational cost is $O(n^4 log(1 + z \cdot \ell))$.

Note that even though many intermediary powers of C are not congruent to 1 mod ℓ, performing the Gaussian Elimination is justified. Linear codes are closed under the schur product, so intermediary powers of C, as linear codes, are closed under Gaussian Elimination. Furthermore, in each intermediate step, the rows kept form a basis for the intermediate code, so any removed rows were superfluous.

Since $r'(C) \leq n$ it suffices to find $r'(C)$ in $O(n^4 log(n))$ time, then one can obtain $q(x)$, the generator of $C^{r'(C)\ell+1}$ in $O(n^4 log(n))$ time as above. Using the method of repeated squaring, $C, C^2, C^4, \ldots$ will encounter C^n in at most $log(n) + 1$ steps. Continue and at each step compute the generating matrix until either the dimension is n or the dimension doesn't grow. Let b be the power such that either $|C^b| = n$ or

$|C^b| = |C^{2b}|$. Then $\frac{b}{2} \leq r(C) \leq b$ and with the precomputed chain above, one can do binary search to find the largest index i such that $|C^i| = |C^b|$ on the interval $[\frac{b}{2}, b]$ and check any particular index with one multiplication and Gaussian Elimination using the already computed powers of C. $b - \frac{b}{2} = O(n)$, so it takes $O(log(n))$ such guesses to obtain $i = r(C)$ and for each guess takes $O(n^4)$ time. Given $r(C)$ it is simple to compute $r'(C)$. Thus in $O(n^4 log(n))$ time, one can obtain $r'(C)$ as desired. Then one can use this in $O(n^4 log(n))$ time to obtain $q(x)$.

It is possible determine the generating polynomial $g(x)$ for C in $O(n^3)$ time regardless of the input format (use Gaussian Elimination). If $1 + z \cdot \ell \leq n$, then it is possible to determine $C^{1+z\cdot\ell}$ in $O(n^4 log(n))$ operations. Otherwise $1 + z \cdot \ell > r'(C)$ so compute $p(x)$, the pattern polynomial of in $O(n^3 + n^2) = O(n^3 log(n))$ operations. Then the generator for $C^{1+z\cdot\ell} = \{p(x)^{1+z\cdot\ell}\}$. Use repeated squaring of the at most n nonzero positions of $p(x)$, taking $O(log(z \cdot \ell))$ operations on each such position, to compute $p(x)^{1+z\cdot\ell}$. Thus it takes $O(nlog(z \cdot \ell))$ additional operations. So total number of operations if $O(n^4 log(n) + nlog(z \cdot \ell))$

□

Lemma 7.17. *Let $C \subset \mathbb{F}^n$ be an quasi-cyclic code with modulus $f(x) = x^n - a$, generator $g(x)$, dimension k. If $k > n/2$ then $|C^{\ell+1}| = |C|$ or $|C^{\ell+1}| = n$*

Proof. If $|C^{\ell+1}| = |C| > n/2$, then the Lemma holds. Otherwise, $|C^{\ell+1}| > |C|$. Consider G' where $g_1 = (b_1, \ldots, b_n), b_1 = 1, b_j = 0 \forall j \in \{2, \ldots, k\}$, and $k > \frac{n}{2}$. Let $g = \text{coeff}(g(x)) = (c_1, \ldots, c_n)$ where $c_1 = 1, c_j = 0 \forall j \in \{n - (k-2), n\}$ since

$\deg(g(x)) = n-k$. Furthermore, $k > n/2$, thus $2k > n$, so $2k-1 = 2(k-1)+1 \geq n$. Hence $1+|\{2,\ldots,k\}|+|\{n-(k-2),\ldots,n\}| = 1+2(k-1) \geq n$, so $\{1\}\cup\{2,\ldots,k\}\cup\{n-(k-2),\ldots,n\} = \{1,\ldots,n\}$. Then $g_1^\ell * g = (b_1c_1,\ldots,b_nc_n) = (1,0^{n-1})$ because $b_1\cdot c_1 = 1\cdot 1 = 1$ and $\forall j \in \{2,\ldots,n\}, j \in \{2,\ldots,k\}\cup\{n-(k-2),\ldots,n\}$. Thus $(1,0^{n-1}) \in C^{\ell+1}$, so $|C^{\ell+1}| = n$.

□

Lemma 7.18. *It is possible for* $|C^2| - |C| = 1$.

Proof. The following will be a proof by example. Let $\mathbb{F} = GF(3)$ and $f(x) = x^6 - 1$ (so $\ell = 1$). Let $C = (g(x)), g(x) = x^4 + 2x^3 + x + 2$, so $|C| = k = 2$. $C = (\{(2,1,0,2,1,0),(0,2,1,0,2,1)\})$. Then $C^2 = (\{(2,1,0,2,1,0)*(2,1,0,2,1,0),(2,1,0,2,1,0)*(0,2,1,0,2,1)\}) = (\{(1,1,0,1,1,0),(0,2,0,0,2,0)\}) = (\{(1,1,0,1,1,0),(0,1,0,0,1,0)\}) = (\{(1,0,0,1,0,0),(0,1,0,0,1,0)\}) = (\{(1,0,0,1,0,0)\}) = (1+x^3)$. Thus $|C^2| = 6-3 = 3$. So $|C^2|-|C| = 3-2 = 1$.

□

Lemma 7.19. *In the cyclic case for* $1^n \notin C$, $\sum_{i=0}^{n-1} sg = 0^n$

Proof. Suppose towards contradiction that $\sum_{i=0}^{n-1} sg = (b,b,\ldots,b)$ for some $b \neq 0$. Then $b^{-1}\cdot(b,b,\ldots,b) = 1^n$, which is a contradiction. □

Corollary 7.20. *Aside from the trivial subspace* $C = \{0^n\}$ *generated by* $g(x) = 0$, *there is a bijection between subspaces* $C \subset \mathbb{F}^n$ *where* $C^2 = C$ *and factors of* n *where for each factor* k *the corresponding* C *has dimension* k. *This corollary applies only* *to when working over $f(x) = x^n - 1$ (cyclic case). Note: Corollary 7.20 does not say that if* $\dim(C) = k$ *and* $k \mid n$ *then* $C^2 = C$.

Proof. Let $m(k) = \sum_{i=0}^{\frac{n}{k}-1} x^{k \cdot i}$ for $k|n$.

For any factor k of n, let $g(x) = m(k) = \sum_{i=0}^{\frac{n}{k}-1} x^{k \cdot i}$. $(x^k - 1)g(x) = x^n - 1$ by Lemma 7.6 and $\dim((g(x)) = k$. Then $g(x)$ is its own pattern polynomial, so by Corollary 7.14, $C^2 = C$. Thus m maps factors of n to nontrivial generators of C's of the form $C^2 = C$. In doing so, m is injective because $\deg(m(k)) \neq \deg(m(k'))$ for $k' \neq k$.

Since $\ell = 1$ so $p(x)$ must satisfy its nonzero coefficients y has $y^\ell = y = 1$. In this case, by Corollary 7.14, the only relevant $g(x)$ are such that $g(x) = p(x)$. So for any such $g(x)$ that $C^2 = C$, it is clear that $g(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{k \cdot i}$ to be a pattern polynomial of that desired form. But then $g(x) = m(k)$. So m is surjective.

Thus m is bijective as desired.

□

Example 7.21. It is possible $C \not\subseteq C^{\ell+1}$. This is important since it is often the case that $C \subseteq C^{\ell+1}$. In particular, for a cyclic code C such that $1^n \in C$, then for any $c \in C, c * (1^n) = c \in C^2$ so $C \subseteq C^2$.

Consider over $\mathbb{F} = GF(5)$ and the polynomial $r(x) = x^4 - 1$. Since $(1)^1 = 1, \ell = 1$. Then $r(x) = (x+1)(x+2)(x+3)(x+4)$. Consider $g(x) = (x+1)(x+2)(x+4) = x^3 + 2x^2 + 4x + 3$. $\deg(g(x)) = 3$ and $\deg(r(x)) = 4$ so $\text{rank}(C) = 4 - 3 = 1$. Therefore, the basis is generated by $\text{Span}([3, 4, 2, 1])$. Hence the basis of C^2 is generated by

$\mathrm{Span}([3,4,2,1] * [3,4,2,1]) = \mathrm{Span}([3 \cdot 3, 4 \cdot 4, 2 \cdot 2, 1 \cdot 1]) = \mathrm{Span}([4,1,4,1])$.

Also, $[1,4,1,4] \cdot 4 = [4,1,4,1]$, so it is closed under shifts. $[4,1,4,1]$ is generated by $(x+2)(x+3)(x+4) = 4 + x + 4x^2 + x^3$, where $x+1 | g(x), x+1 \not| 4 + x + 4x^2 + x^3$. Note $[3,4,2,1] \notin \mathrm{Span}([4,1,4,1])$ since $2 \cdot [4,1,4,1] = [3,2,3,2]$ which is necessary to match first position, but then the rest of the positions are off. So $C \not\subseteq C^2$.

8 Conclusion and Future Directions

Overall, it is clear that quasi-cyclic codes have structured growth under the schur product. One can efficiently identify the dimension the code will grow to, the generators of the powers of the code past $r'(C)$, and when the code and or powers of the code are invariant under the schur product. This inherent structure is important to consider when developing and or performing cryptanalysis of cryptosystems involving quasi-cyclic or related codes to avoid inducing or to exploit vulnerabilities related to such properties.

The future directions of this work are twofold: improving the results proven in this paper and extending the results to other areas. In the first category, can the complexity bound for acquiring the pattern polynomial be improved from $O(w^2)$? Can $r'(C)$ be computed in time faster then $O(n^3 log(n))$? Can the time used to acquire generators of powers of C be written in terms of the input length rather than n, perhaps by using sparse matrix operations? Can the chain of generators for $C, C^{\ell+1}, C^{2\ell+1}, \cdots, C^{r'(C)\ell+1}$ be obtained more efficiently through using properties of the pattern polynomial? In the second category, can any of these results be extended to the context of cyclic lattices? Can the techniques used in this paper be modified to apply to similar yet different results in cyclic lattices? Micciancio and Regev [MR08] wondered if one could safely use cyclic lattices in LWE-based cryptosystems to improve efficiency. Can such extensions be used to justify or preclude doing so? Can properties of quasi-cyclic codes under the schur product be used to design and or break future cryptosystems which use quasi-cyclic codes?

References

[BCGO09] Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani. *Reducing Key Length of the McEliece Cryptosystem*, pages 77–97. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[COT17] A. Couvreur, A. Otmani, and J. P. Tillich. Polynomial time attack on wild mceliece over quadratic extensions. *IEEE Transactions on Information Theory*, 63(1):404–427, Jan 2017.

[FOPT10] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys*, pages 279–298. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[KO14] Wittawat Kositwattanarerk and Frédérique Oggier. Connections between construction d and related constructions of lattices. *Designs, Codes and Cryptography*, 73(2):441–455, 2014.

[McE78] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 1978.

[MR08] Daniele Micciancio and Oded Regev. Lattice-based cryptography, 2008.

[Ran15] Hugues Randriambololona. On products and powers of linear codes under componentwise multiplication. *Contemporary Mathematics*, 637, 2015.

[UL09] Valerie Gauthier Umana and Gregor Leander. Practical key recovery attacks on two mceliece variants. Cryptology ePrint Archive, Report 2009/509, 2009.