rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

On the Schur Product of Vector Spaces over Finite Fields

Bachelor Thesis Mathematics

July 2012

Student: Christiaan Koster

First Supervisor: Prof. dr. J. Top

Second Supervisor: Prof. dr. H. L. Trentelman

Abstract

In this thesis we consider the vector space of all n-tuples over finite fields. We will investigate the Schur product, also known as entry-wise multiplication, of its linear subspaces, which is equal to the span of the Schur product over all pairs of vectors of a subspace. The number of d-dimensional linear subspaces will be counted, certain properties of the Schur product will be shown and the Schur product of cyclic codes will also be investigated. The main goal is to find good bounds on the number of subspaces for which the Schur product is equal to the total space. This will then be compared to the total number of subspaces as either the dimension of the vector space or the number of elements of the base field tend to infinity.

Contents

1 Introduction

In this modern day and age we live in an information-driven society. Private information about people or companies is very valuable, while the people themselves do not wish this information to be known to others. One could think of PIN-codes or credit card numbers, but also the economic situation of a person and very sensitive data such as nuclear missile codes. While the information must not be known to certain others, it also has to be able to be used. The information in such cases can be regarded as a secret. The problem is to find out how a secret from a certain party can be used in combination with other secrets from other parties, without the secret being known to any of the other parties. An important tool used in solving this problem is known as secret-sharing.
In this thesis we consider vector spaces of n-tuples over finite fields and investigate the Schur product, also known as entry-wise multiplication, of linear subspaces of the vector spaces. The Schur product is a product that is used in secret sharing. The main goal of this thesis is to find the number of subspaces, or upper and lower bounds, for which the Schur product is equal to the whole vector space and compare this to the total number of linear subspaces. In order to do this we first count the exact number of linear subspaces. Next we investigate some basic properties of the Schur product and then we handle the main question by trying various methods. It will be done by a coding theoretic approach and we also consider how the Schur product acts on cyclic codes.

1.1 Preliminaries

Let K be a finite field, there is the following theorem on the classification of finite fields, found (in Dutch) in [3]:

Theorem 1.

1. *Let K be a finite field. Then there is a prime p and an integer $m \geq 1$ with $\#K = p^m$.*
2. *Conversely, for each prime p and integer $m \geq 1$ there is a finite field with p^m elements, and this field is uniquely determined up to isomorphisms.*

The field with $q = p^m$ elements will be denoted by $\mathbb{F}_q$. If p is a prime, then $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ and we write $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ where $a \in \mathbb{F}_p$ is identified with $a + p\mathbb{Z}$. For convenience we just write a instead of $a + p\mathbb{Z}$. In this thesis, the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$ will be considered, for any integer n, with standard vector addition and scalar multiplication. Define

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0) \\ e_2 &= (0, 1, \ldots, 0) \\ &\vdots \\ e_n &= (0, \ldots, 0, 1), \end{aligned}$$

then the set $\{e_1, \ldots, e_n\}$ forms the standard basis of $\mathbb{F}_q^n$.

Definition 1. *A set $V \subset \mathbb{F}_q^n$ is called a linear subspace of $\mathbb{F}_q^n$ if for all $v, w \in V$ and $\alpha \in \mathbb{F}_q$ it holds that:*

1. $v + w \in V$

2. $\alpha v \in V$.

Definition 2. *The collection of all d-dimensional linear subspaces of $\mathbb{F}_q^n$ is denoted by $G(d,n)(\mathbb{F}_q)$, $1 \leq d \leq n$.*

The set $G(d,n)$ is also known as the Grassmannian of $\mathbb{F}_q^n$. It has a lot of useful properties, but these will not be treated in this thesis. Here it will just be used as easy notation to pick a d-dimensional linear subspace of $\mathbb{F}_q^n$.

Definition 3. *The general linear group $GL(n, \mathbb{F}_q)$ is defined as the group of all $n \times n$ invertible matrices over $\mathbb{F}_q$.*

Definition 4. *For any $n \in \mathbb{N}$ let $S = \{1, 2, \ldots, n\}$. The symmetric group of S consisting of all bijections of S onto itself is denoted by S_n. An element $\sigma \in S_n$ is called a permutation.*

In this thesis a subspace $V \in G(d,n)(\mathbb{F}_q)$ will be often be written as the span of d basis vectors $v_1, \ldots, v_d$. Each v_i can be written as $v_i = a_{i,1}e_{\sigma(1)} + \cdots + a_{i,n}e_{\sigma(n)}$ for a permutation $\sigma \in S_n$ and where $a_{i,j} \in \mathbb{F}_q$ for $i = 1, \ldots, d$, $j = 1, \ldots, n$. Since $v_1 \neq 0$ we can assume that $a_{1,1} \neq 0$ by choosing σ appropriately and since $V = \text{Span}\{v_1, \ldots, v_d\}$ we can take $a_{i,i} = 1$. Then subtracting $a_{k,1}v_1$ from v_k for each $k = 2, \ldots, d$, a new basis for V is $\{v_1, w_2, \ldots, w_d\}$ where each w_j can be written as $w_j = b_{j,2}e_{\sigma(2)} + \cdots + b_{j,n}e_{\sigma(n)}$. Since v_1 and w_2 are linearly independent, we can assume $b_{j,2} \neq 0$ and even $b_{j,2} = 1$. Now subtract $b_{m,2}w_2$ from w_m for each $m = 3, \ldots, d$. This can be continued repeatedly until we find a basis for V of the form

$$\{u_i = e_{\eta(i)} + \tilde{a}_{i,i+1}e_{\eta(i+1)} + \cdots + \tilde{a}_{i,n}e_{\eta(n)} : \tilde{a}_{i,j} \in \mathbb{F}_q \text{ for } i = 1, \ldots d, j = i+1, \ldots, n\}$$

for a $\eta \in S_n$. For any $i > 1$ we can now subtract $\tilde{a}_{l,i}u_i$ from u_l for each $l = 1, \ldots, i-1$. Doing this for each $i > 1$ and replacing u_j with $u_j - \tilde{a}_{j,i}u_i$ whenever $j < i$ we find a basis for V of the form

$$\{e_{\tau(i)} + c_{i,d+1}e_{\tau(d+1)} + \cdots + c_{i,n}e_{\tau(n)} : c_{i,j} \in \mathbb{F}_q \text{ for } i = 1, \ldots d, j = d+1, \ldots, n\} \tag{1}$$

for a $\tau \in S_n$. For τ fixed, this basis is unique.

1.2 Coding Theory

In this thesis we will also look at linear subspaces of $\mathbb{F}_q^n$ from a coding theory perspective. All definitions and theorems in this part can be found (in Dutch) in [2]. Since we only consider linear subspaces of $\mathbb{F}_q^n$, the following definition of codes will be used.

Definition 5. *Let K be a field. A code of length n is a linear subspace C of K^n. An element $c \in C$ is called a word of the code.*

Definition 6. *A cyclic code is a code $C \subset \mathbb{F}_q^n$ such that if $c = (c_1, \ldots, c_n) \in C$ then $(c_n, c_1, \ldots, c_{n-1}) \in C$.*

Definition 7. *The dual $C^\perp$ of a code C is defined as*

$$C^\perp = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} a_i c_i = 0 \quad \forall (c_1, \ldots, c_n) \in C\}$$

Note that $C^\perp$ is always linear as well.

Proposition 1. *Let $C \subset \mathbb{F}_q^n$ be a code, then $Dim(C) + Dim(C^\perp) = n$.*

Example 1. *Let $C \subset \mathbb{F}_2^3$ be linear and cyclic. We can construct cyclic codes C of dimension $0, 1, 2$ and 3. If $e_i \in C$ for any $i \in \{1, 2, 3\}$, then, since C is cyclic, $e_i \in C$ for $i = 1, 2, 3$. Hence, in this case $Dim(C) = 3$ and $C = \mathbb{F}_2^3$. If $C = Span\{(1, 1, 1)\}$, then C is a cyclic code with $Dim(C) = 1$. Finally, let $C = \{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}$. Then C is a cyclic code with $Dim(C) = 2$. These codes, along with $C = \{(0, 0, 0)\}$, are the only cyclic codes in $\mathbb{F}_2^3$.*

Let $\mathbb{F}_q[X]$ denote the polynomial ring over $\mathbb{F}_q$, then for any $n \geq 1$ define

$$R := \mathbb{F}_q[X]/(X^n - 1) = \{a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \mod (X^n - 1) : a_0, \ldots, a_{n-1} \in \mathbb{F}_q\}$$

Next define a mapping $g : \mathbb{F}_q^n \to R$ as

$$g((b_0, \ldots, b_{n-1})) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \mod (X^n - 1)$$

for $(b_0, \ldots, b_{n-1}) \in \mathbb{F}_q^n$. Then g is an isomorphism between the vector spaces $\mathbb{F}_q^n$ and R, that is g is a linear bijective map. From now on, elements of R will be denoted by $\overline{f} \in R$ where $f \in \mathbb{F}_q[X]$. The point of the identification of $\mathbb{F}_q^n$ with R will become clear when cyclic codes are considered.
Let $C \subset \mathbb{F}_q^n$ be a cyclic code, then C gets mapped by g onto $\tilde{C} \subset R$. Now we will determine what properties $\tilde{C}$ has, caused by the fact that C is a cyclic code.
That C is linear implies the following:

1. $0 \in \tilde{C}$, since $(0, \ldots, 0) \in C$.
2. if $\overline{f}_1, \overline{f}_2 \in \tilde{C}$ and $a \in \mathbb{F}_q$, then $\overline{f}_i = g(c_i)$ for a $c_i \in C$. Since C is linear, also $c_1 - ac_2 \in C$ and hence $\overline{f_1 - af_2} = g(c_1 - ac_2) \in \tilde{C}$.

So $\tilde{C}$ is linear as well.
That C is cyclic means that if $(b_0, \ldots, b_{n-1}) \in C$, then $(b_{n-1}, b_0, \ldots, b_{n-2}) \in C$. In $\tilde{C}$ this means that if $\overline{f} = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \mod (x^n - 1) \in \tilde{C}$ then also $b_{n-1} + b_0X + \cdots + b_{n-2}X^{n-1} \mod (X^n - 1) \in \tilde{C}$. However in $\tilde{C}$ it holds that $1 \mod (X^n - 1) = X^n \mod (x^n - 1)$. So $b_{n-1} + b_0X + \cdots + b_{n-2}X^{n-1} \mod (X^n - 1) = b_0X + \cdots + b_{n-2}X^{n-1} + b_{n-1}X^n \mod (X^n - 1) = \overline{Xf}$. Hence $\tilde{C}$ being cyclic means that if $\overline{f} \in \tilde{C}$ then $\overline{Xf} \in \tilde{C}$ as well.
Combining this with the linearity of $\tilde{C}$ the third property becomes

3. for any $\overline{f} \in \tilde{C}$, $\overline{g} \in R$ it holds that $\overline{fg}, \overline{gf} \in \tilde{C}$.

All 3 properties together are exactly the properties that make $\tilde{C}$ an ideal in R. Hence, we can conclude that

Proposition 2. *$\tilde{C} \subset R$ is linear and cyclic $\Leftrightarrow$ $\tilde{C}$ is an ideal in R.*

So to find cyclic codes in $\mathbb{F}_q^n$ is equivalent to finding ideals in R. The following proposition states how to do that.

Proposition 3. *I is an ideal in $R \Leftrightarrow I = \overline{f}R$ with $f|(X^n - 1)$.*

For an ideal I generated by a polynomial $\overline{f}$, that is $I = \overline{f}R$, we will use the alternative notation $I = (\overline{f})$.

Example 2. *We will again look at $\mathbb{F}_2^3$ like in example 1. Now $R = \mathbb{F}_2[X]/(X^3 - 1)$ and $X^3 - 1 = (X + 1)(X^2 + X + 1)$. All cyclic codes can be found by looking at the ideals $(1), (X+1), (X^2+X+1), (X^3-1)$ (for convenience we won't denote the bar on each generator). Now $(1) = R$ and thus has dimension 3. Next, $(X+1) = \{0, X+1, X^2+X, 1+X^2\}$ which is a 2-dimensional cyclic code and it corresponds with $C = \{(0,0,0), (1,1,0), (0,1,1,), (1,0,1)\}$ like in example 1. Furthermore, $(X^2 + X + 1) = \{0, X^2 + X + 1\}$ and $(X^3 - 1) = \{0\}$.*

For a cyclic code $(f) \subset R$ with $f|(X^n - 1)$ we can also determine the dimension.

Proposition 4. *Let $f|(X^n - 1) \in \mathbb{F}_q[X]$, then the cyclic code $(\overline{f})$ has dimension $n - deg(f)$.*

Using proposition 4 there is an easy way of constructing a basis for a cyclic code $C = (\overline{f}) \subset R$ with $f|(X^n - 1)$. Let $k =$deg(f) and write $f = \sum_{i=0}^{k} a_i X^i$ where each $a_i \in \mathbb{F}_q$. Since C is cyclic, each of the elements $\overline{X^j f} \in C$. For $0 \leq j \leq n - k - 1$ these elements correspond with

$$(a_0, \ldots, a_k, 0, \ldots, 0), (0, a_0, \ldots, a_k, 0, \ldots, 0), \ldots, (0, \ldots, 0, a_0, \ldots, a_k) \in \mathbb{F}_q^n$$

These vectors are all linearly independent and there are $n-k$ of these vectors which is exactly the dimension of C, so they are a basis of C.

2 The Number of Subspaces of $\mathbb{F}_q^n$

In this section we will count the number of d-dimensional subspaces of $\mathbb{F}_q^n$. We start with the most simple case, namely $d = 1$.

Example 3. *To count all the* 1*-dimensional subspaces of* $\mathbb{F}_q^n$*, it is needed to count how many vectors there are that have a different span. So we have to count all the non-zero vectors up to scalar multiples. There are* $q^n - 1$ *non-zero vectors in* $\mathbb{F}_q^n$*, so the number of* 1*-dimensional subspaces is equal to* $(q^n - 1)/(q - 1) = \sum_{i=1}^{n-1} q^i$*.*

To count how many subspaces there are of arbitrary dimension, a counting argument using group theory will be used. Let $V_d \subset \mathbb{F}_q^n$ be the linear subspace of dimension d, $0 < d \leq n$, defined as $V_d = \mathrm{Span}\{e_1, \ldots, e_d\}$. Let V be another d-dimensional linear subspace of $\mathbb{F}_q^n$ with a chosen basis $\{f_1, \ldots, f_d\}$. We extend this basis to a basis of $\mathbb{F}_q^n$: $\{f_1, \ldots, f_d, f_{d+1}, \ldots, f_n\}$ is a basis of $\mathbb{F}_q^n$ for certain $f_{d+1}, \ldots, f_n \in \mathbb{F}_q^n$. Now define the matrix $A : \mathbb{F}_q^n \to \mathbb{F}_q^n$ by $e_i \mapsto f_i$ for $i = 1, \ldots, n$. Observe that $A \in \mathrm{GL}(n, \mathbb{F}_q)$ and that $AV_d = V$. But V is an arbitrary d-dimensional linear subspace of $\mathbb{F}_q^n$ and for each V we can find the matrix as defined above. So

$$\begin{aligned} G(d,n)(\mathbb{F}_q) :&= \{V \subset \mathbb{F}_q^n : V \text{ a linear subspace of } \mathbb{F}_q^n, \mathrm{Dim}(V) = d\} \\ &= \{AV_d : A \in \mathrm{GL}(n, \mathbb{F}_q)\}. \end{aligned}$$

Note that it is possible that $A_1V_d = A_2V_d$ for $A_1, A_2 \in \mathrm{GL}(n, \mathbb{F}_q)$, $A_1 \neq A_2$, so the same subspace could be obtained by different invertible matrices. For example, let $\{f_1, \ldots, f_d, f_{d+1}, \ldots, f_n\}$ and $\{f_1, \ldots, f_d, \tilde{f}_{d+1}, \ldots, \tilde{f}_n\}$ be two different bases of $\mathbb{F}_q^n$ and let $A_1 : e_i \mapsto f_i$, $i = 1, \ldots, n$ and $A_2 : e_j \mapsto f_j$, for $j = 1, \ldots d$ and $e_j \mapsto \tilde{f}_i$ for $j = d+1, \ldots, n$. Then $A_1V_d = A_2V_d$, but $A_1 \neq A_2$.
We now look at what happens when $AV_d = V_d$. We get the following lemma.

Lemma 1. *The set* $H := \{A \in GL(n, \mathbb{F}_q) : AV_d = V_d\}$ *is a subgroup of* $GL(n, \mathbb{F}_q)$*.*

Proof. For the identity matrix I we have $IV_d = V_d$, so $I \in H$. If $A, B \in H$, so $AV_d = V_d$ and $BV_d = V_d$, then $ABV_d = AV_d = V_d$ and hence $AB \in H$. Also, since $AV_d = V_d$ we get $V_d = A^{-1}V_d$, so $A^{-1} \in H$. Hence H is a subgroup of $\mathrm{GL}(n, \mathbb{F}_q)$. □

We use the following result from group theory found in [1].

Theorem 2. *[Lagrange's Theorem] If* H *is a subgroup of a finite group* G*, then* $\#H | \#G$*.*

The proof of this theorem shows that $\#G = [G : H] \cdot \#H$ and $G = \bigcup_{i=1}^{m} g_iH$ for certain $g_i's \in G$ where $m = [G : H]$ is the index of H in G and $g_iH \cap g_jH = \emptyset$ if $i \neq j$.
Using this result for the groups used in this section, we get

$$\mathrm{GL}(n, \mathbb{F}_q) = \bigcup_{i=1}^{[\mathrm{GL}(n,\mathbb{F}_q):H]} g_iH$$

for certain $g_i's \in \mathrm{GL}(n, \mathbb{F}_q)$ with $g_iH \cap g_jH = \emptyset$ if $i \neq j$. We get the following lemma.

Lemma 2. *Let $G1 = \{g_1, \dots . g_m\}$, where $m = [GL(n, \mathbb{F}_q) : H]$, such that $GL(n, \mathbb{F}_q) = \bigcup_{g \in G1} gH$ and $V_d = Span\{e_1, \dots, e_d\}$. Then*

$$G(d, n)(\mathbb{F}_q) = \{gV_d : g \in G1\}.$$

Furthermore $\#G(d, n)(\mathbb{F}_q) = [GL(n, \mathbb{F}_q) : H]$.

Proof. We have already seen that for any $g \in \mathrm{GL}(n, \mathbb{F}_q)$ we get $gV_d \in G(d, n)(\mathbb{F}_q)$. So $\{gV_d : g \in G1\} \subseteq G(d, n)(\mathbb{F}_q)$. Let $V \in G(d, n)(\mathbb{F}_q)$, then we have seen there is a $g \in \mathrm{GL}(n, \mathbb{F}_q)$ such that $V = gV_d$. Since $\mathrm{GL}(n, \mathbb{F}_q) = \bigcup_{g_i \in G1} g_i H$, we get that $g = g_1 h$ for unique $g_1 \in G1$ and $h \in H$. Then $V = gV_d = g_1 h V_d = g_1 V_d$. So $V \in \{gV_d : g \in G1\}$. Hence $G(d, n)(\mathbb{F}_q) = \{gV_d : g \in G1\}$. Now the following holds for $g_i, g_j \in G1$: $g_i V_d = g_j V_d \Leftrightarrow g_j^{-1} g_i V_d = V_d \Leftrightarrow g_j^{-1} g_i \in H \Leftrightarrow g_j^{-1} g_i H = H \Leftrightarrow g_i H = g_j H \Leftrightarrow i = j$. So each $g_i \in G1$ gives a different $g_i V_d \in G(d, n)(\mathbb{F}_q))$. Hence $\#G(d, n)(\mathbb{F}_q) = \#\{gV_d : g \in G1\} = \#G1 = [\mathrm{GL}(n, \mathbb{F}_q) : H]$. □

Now we want to determine $[\mathrm{GL}(n, \mathbb{F}_q) : H] = \#\mathrm{GL}(n, \mathbb{F}_q)/\#H$.

Lemma 3. *The number of elements of $GL(n, \mathbb{F}_q)$ is equal to $\prod_{i=1}^{n}(q^n - q^{i-1})$.*

Proof. A matrix $A \in \mathrm{GL}(n, \mathbb{F}_q) \Leftrightarrow A$ has n linearly independent columns. Let $A = [v_1, \dots, v_n]$, with $v_i \in \mathbb{F}_q^n$, $i = 1, \dots, n$. Then v_1 needs to have at least one non-zero element for A to be invertible. So there are $q^n - 1$ possibilities. For v_2 we require that it is not a multiple of the first column, that is $v_2 \neq a_1 v_1$ with $a_1 \in \mathbb{F}_q$. So for v_2 there are $q^n - q$ possibilities. Continuing in this way, we find that v_i cannot be of the form $v_i = a_1 v_1 + \dots + a_{i-1} v_{i-1}$ with $a_j \in \mathbb{F}_q$, $j = 1, \dots, i-1$. So, for v_i there are $q^n - q^{i-1}$ possibilities. Then we get $\#\mathrm{GL}(n, \mathbb{F}_q) = \prod_{i=1}^{n}(q^n - q^{i-1})$. □

Now that $\#\mathrm{GL}(n, \mathbb{F}_q)$ is known, we need to know how many elements H has.

Lemma 4. *The number of elements of $H = \{A \in GL(n, \mathbb{F}_q) : AV_d = V_d\}$ is equal to*

$$\#H = \#GL(d, \mathbb{F}_q) \cdot \#GL(n-d, \mathbb{F}_q) \cdot q^{d(n-d)} = \prod_{i=1}^{d}(q^d - q^{i-1}) \cdot \prod_{i=1}^{n-d}(q^{n-d} - q^{i-1}) \cdot q^{d(n-d)}$$

Proof. To compute the number of elements of H, we first determine what the matrices of H look like as a block matrix. For $A \in H$ we have that $AV_d = V_d$, where $V_d = \mathrm{Span}\{e_1, \dots, e_d\}$. So A maps each e_i, $i = 1, \dots d$, to a linear combination of $e_1, \dots, e_d$. Taking into account that A has to be invertible, we get that A is of the form

$$A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix}$$

where $A_{11} \in \mathrm{GL}(d, \mathbb{F}_q)$, $A_{22} \in \mathrm{GL}(n-d, \mathbb{F}_q)$ and A_{12} a $d \times (n-d)$ matrix. Since each $a_{ij} \in \mathbb{F}_q$, there are $q^{d(n-d)}$ possibilities for A_{12}. So we get

$$\#H = \#\mathrm{GL}(d, \mathbb{F}_q) \cdot \#\mathrm{GL}(n-d, \mathbb{F}_q) \cdot q^{d(n-d)} = \prod_{i=1}^{d}(q^d - q^{i-1}) \cdot \prod_{i=1}^{n-d}(q^{n-d} - q^{i-1}) \cdot q^{d(n-d)}$$

□

Now we can count $\#G(d, n)(\mathbb{F}_q)$.

Corollary 1. *The number of elements of $G(d,n)(\mathbb{F}_q)$ is equal to*

$$\#G(d,n)(\mathbb{F}_q) = \frac{\prod_{i=1}^{n}(q^n - q^{i-1})}{q^{d(n-d)} \cdot \prod_{i=1}^{d}(q^d - q^{i-1}) \cdot \prod_{i=1}^{n-d}(q^{n-d} - q^{i-1})} \tag{2}$$

Proof. From lemma 2 we have $\#G(d,n)(\mathbb{F}_q) = [G : H] = \#\mathrm{GL}(n,\mathbb{F}_q)/\#H$. The result then follows from lemma 3 and 4. □

Observe that $\#G(d,n)(\mathbb{F}_q)$ is symmetric in the variable d around $n/2$, that is $\#G(d,n)(\mathbb{F}_q) = \#G(n-d,n)(\mathbb{F}_q)$. Another way to see this, is by using proposition 1. That is, if $V \in G(d,n)(\mathbb{F}_q)$, then $V^\perp \in G(n-d,n)(\mathbb{F}_q)$. So $\#G(d,n)(\mathbb{F}_q) \leq \#G(n-d,n)(\mathbb{F}_q)$. Interchanging d and $n-d$, it shows that $\#G(n-d,n)(\mathbb{F}_q) \leq \#G(d,n)(\mathbb{F}_q)$ and hence $\#G(d,n)(\mathbb{F}_q) = \#G(n-d,n)(\mathbb{F}_q)$.

2.1 Growth Pattern of $\#G(d,n)(\mathbb{F}_q)$

Now that we know the number of d-dimensional subspaces of $\mathbb{F}_q^n$, we wish to determine how that number grows as q increases. If q is large enough, then $q^n \gg q^{n-1}$ for any $n \in \mathbb{N}$, so approximately $\#\mathrm{GL}(n,\mathbb{F}_q) = \prod_{i=1}^{n}(q^n - q^{i-1}) \approx q^{n^2}$. To be exact, it holds that

$$\begin{aligned}\frac{\#GL(n,\mathbb{F}_q)}{q^{n^2}} &= \frac{\prod_{i=1}^{n}(q^n - q^{i-1})}{q^{n^2}} = \prod_{i=1}^{n}\frac{q^n - q^{i-1}}{q^n} \\ &= \prod_{i=1}^{n}(1 - q^{i-1-n}) = \prod_{i=1}^{n}(1 - q^{-i})\end{aligned} \tag{3}$$

Hence

$$\lim_{q\to\infty}\frac{\#GL(n,\mathbb{F}_q)}{q^{n^2}} = \lim_{q\to\infty}\prod_{i=1}^{n}(1 - q^{-i}) = 1$$

Using the same argument for $\#G(d,n)(\mathbb{F}_q)$, if q is large enough, we get approximately, using (2),

$$\#G(d,n)(\mathbb{F}_q) \approx \frac{q^{n^2}}{q^{d(n-d)} \cdot q^{d^2} \cdot q^{(n-d)^2}} = q^{n^2 - nd - n^2 + 2nd - d^2} = q^{d(n-d)}$$

So for fixed d and n this gives

$$\lim_{q\to\infty}\frac{\#G(d,n)(\mathbb{F}_q)}{q^{d(n-d)}} = 1 \tag{4}$$

Note that $\#G(d,n)(\mathbb{F}_q)$ has a maximum in the variable d when $d = \frac{n}{2}$ if n is even and when $d = \frac{n\pm1}{2}$ if n is odd. This allows us to determine the growth rate of the total number of subspaces. If n is even we write $n = 2m$ for $m \in \mathbb{N}$ and use (4) to obtain

$$\lim_{q\to\infty}\frac{\sum_{d=0}^{n}\#G(d,n)(\mathbb{F}_q)}{\#G(m,n,q)} = \lim_{q\to\infty}\frac{\sum_{d=0}^{2m}q^{d(2m-d)}}{q^{m^2}} = \lim_{q\to\infty}\sum_{d=0}^{2m}q^{-(m-d)^2} = 1$$

Hence, as $q \to \infty$ and n is even, it is enough to look at the number of subspaces of dimension $\frac{n}{2}$, instead of the total number of subspaces. This will be useful later on. If n is odd instead,

we write $n = 2m+1$. When $d = \frac{n\pm 1}{2}$ we know $\#G(d,n)(\mathbb{F}_q)$ has a maximum. Here that is when $d = m$ or $d = m+1$. Using (4) again we obtain

$$\lim_{q\to\infty} \frac{\sum_{d=0}^{n} \#G(d,n)(\mathbb{F}_q)}{2\#G(m,n,q)} = \lim_{q\to\infty} \frac{\sum_{d=0}^{2m+1} q^{d(2m+1-d)}}{2q^{m(m+1)}} = \frac{1}{2} \lim_{q\to\infty} \sum_{d=0}^{2m+1} q^{-(d-m)(d-m-1)} = 1$$

Thus for n odd and $q \to \infty$ only the subspaces of dimension $\frac{n\pm 1}{2}$ are important for counting the total number of subspaces.

Now that the growth patterns of $\#G(d,n)(\mathbb{F}_q)$ are known as $q \to \infty$, we are interested in the same growth pattern as n tends to infinity, both for fixed dimensions and the total number of subspaces. We start again with (3), that is what can be said about the convergence of

$$\lim_{n\to\infty} \prod_{i=1}^{n} (1 - q^{-i})$$

First, note that for any $i \in \mathbb{N}$ it holds that $1 - q^{-i} < 1$. Using this bound for each $i > 1$ it gives the upper bound

$$\lim_{n\to\infty} \prod_{i=1}^{n} (1 - q^{-i}) < 1 - \frac{1}{q}.$$

Second, for the convergence it is required that $\sum_{i=1}^{\infty} \log(1 - q^{-i})$ converges where log is the natural logarithm. Now, the logarithm satisfies $\log(1-x) \geq -2x$ for any $x \in [0, \frac{1}{2}]$. To show this, define $g : [0, \frac{1}{2}] \to \mathbb{R}$ by $g(x) = \log(1-x) + 2x$. Then $g(0) = 0$ and

$$g'(x) = \frac{-1}{1-x} + 2 = \frac{2x-1}{x-1} \geq 0 \text{ for } x \in [0, \frac{1}{2}].$$

The claim now follows. Since $0 < q^{-i} \leq \frac{1}{2}$ we find $\log(1 - q^{-i}) \geq -2q^{-i}$ and

$$-2\sum_{i=1}^{\infty} q^{-i} = -2(\frac{1}{1-\frac{1}{q}} - 1) = -2(\frac{q}{q-1} - 1) = \frac{-2}{q-1}$$

so $\sum_{i=1}^{\infty} \log(1 - q^{-i})$ converges by the comparison test and $\sum_{i=1}^{\infty} \log(1 - q^{-i}) \geq \frac{-2}{q-1}$.
Hence $\prod_{i=1}^{\infty}(1 - q^{-i})$ converges, so define ϕ as $\phi(q) := \prod_{i=1}^{\infty}(1 - q^{-i})$ and then

$$\phi(q) = \lim_{n\to\infty} \prod_{i=1}^{n} (1 - q^{-i}) = \exp(\lim_{n\to\infty} \log(1 - q^{-i})) \geq \exp(\frac{-2}{q-1})$$

See figure 1 for a plot of ϕ.
We can conclude that

$$\lim_{n\to\infty} \frac{\#GL(n,\mathbb{F}_q)}{\phi(q)q^{n^2}} = \frac{1}{\phi(q)} \lim_{n\to\infty} \frac{\#GL(n,\mathbb{F}_q)}{q^{n^2}} = \frac{1}{\phi(q)} \lim_{n\to\infty} \prod_{i=1}^{n} (1 - q^{-i}) = 1$$

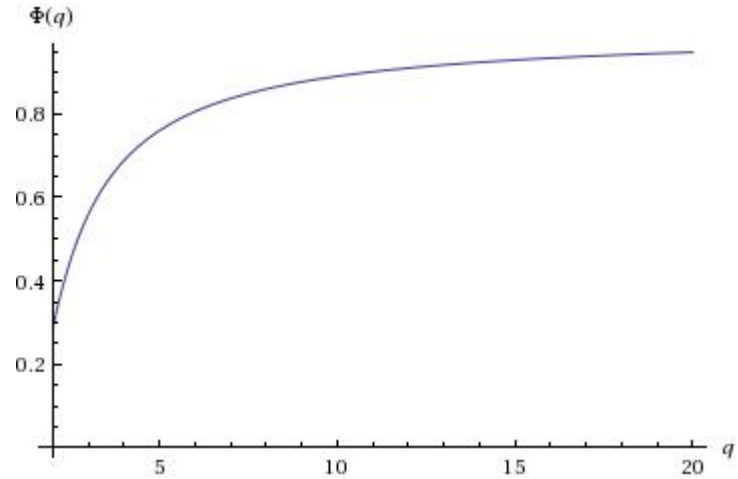

Figure 1: Plot of ϕ

For the growth rate $\#G(d,n)(\mathbb{F}_q)$ for d and q fixed while n tends to infinity we will find the growth rate of each term separately and then combine them. We have the following

$$\lim_{n\to\infty} \frac{\prod_{i=1}^{n}(1-q^{-i})}{\phi(q)q^{n^2}} = 1$$
$$\lim_{n\to\infty} \frac{q^{d(n-d)}\prod_{i=1}^{d}(q^d-q^{i-1})}{q^{d(n-d)}\prod_{i=1}^{d}(q^d-q^{i-1})} = 1$$
$$\lim_{n\to\infty} \frac{\phi(q)q^{(n-d)^2}}{\prod_{i=1}^{n-d}(q^{n-d}-q^{i-1})} = 1$$

Now

$$\lim_{n\to\infty} \#G(d,n)(\mathbb{F}_q)/\left(\frac{\phi(q)q^{n^2}}{q^{d(n-d)}\prod_{i=1}^{d}(q^d-q^{i-1})\phi(q)q^{(n-d)^2}}\right)$$
$$= \lim_{n\to\infty} \frac{\prod_{i=1}^{n}(1-q^{-i})}{\phi(q)q^{n^2}} \cdot \frac{q^{d(n-d)}\prod_{i=1}^{d}(q^d-q^{i-1})}{q^{d(n-d)}\prod_{i=1}^{d}(q^d-q^{i-1})} \cdot \frac{\phi(q)q^{(n-d)^2}}{\prod_{i=1}^{n-d}(q^{n-d}-q^{i-1})} = 1$$

Combining the powers of q in the first denominator gives

$$\frac{q^{n^2}}{q^{d(n-d)+(n-d)^2}} = \frac{q^{n^2}}{q^{nd-d^2+n^2-2nd+d^2}} = q^{nd}$$

Hence the growth rate of $\#G(d,n)(\mathbb{F}_q)$ for d and q fixed is

$$\lim_{n\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{nd}/\prod_{i=1}^{d}(q^d-q^{i-1})} = 1 \tag{5}$$

If now $d\to\infty$ as well, this gives us

$$\lim_{\substack{n\to\infty\\ d\to\infty}} \frac{\#G(d,n)(\mathbb{F}_q)}{\frac{q^{d(n-d)}}{\phi(q)}} = 1 \tag{6}$$

For the growth rate of the total number of subspaces as n tends to infinity, we again have to distinguish the cases n even and n odd. Since for n even only subspaces of dimension $\frac{n}{2}$ need to be considered, but for n odd the subspaces of dimensions $\frac{1}{2}(n \pm 1)$ are the ones that are important. We first take $n = 2m$ for $m \in \mathbb{N}$ and use both (5) and (6) and the symmetry of $G(d,n)(\mathbb{F}_q)$ to obtain

$$\begin{aligned}
\lim_{m\to\infty} \frac{\sum_{d=0}^{2m} \#G(d,2m)(\mathbb{F}_q)}{\#G(m,2m)(\mathbb{F}_q)} &= \lim_{m\to\infty} \frac{\phi(q)\sum_{d=0}^{2m} q^{2md}/\prod_{i=1}^{d}(q^d - q^{i-1})}{q^{m^2}} \\
&= \lim_{m\to\infty} \phi(q) \sum_{d=0}^{2m} \frac{q^{m(2d-m)}}{\prod_{i=1}^{d}(q^d - q^{i-1})} \\
&= \lim_{m\to\infty} \phi(q) \frac{q^{m^2}}{\prod_{i=1}^{m}(q^m - q^{i-1})} + \lim_{m\to\infty} 2\phi(q) \sum_{d=m+1}^{2m} \frac{q^{m(2d-m)}}{\prod_{i=1}^{d}(q^d - q^{i-1})} \\
&= 1 + 2\lim_{m\to\infty} \sum_{d=m+1}^{2m} q^{-(m-d)^2} = 1 + 2\lim_{m\to\infty} \sum_{d=1}^{m} q^{-d^2}
\end{aligned}$$

The series $\lim_{m\to\infty} \sum_{d=1}^{m} q^{-d^2} = \sum_{d=1}^{\infty} q^{-d^2}$ converges since $q^{-d^2} \leq q^{-d}$ for any $d \geq 1$ and $\sum_{d=1}^{\infty} q^{-d} = \frac{1}{q-1}$, so converges. Now define the function ϕ_{even} by $\phi_{even}(q) = 1 + 2\sum_{d=1}^{\infty} q^{-d^2}$, for a plot of ϕ_{even} see figure 2, then we find

$$\lim_{m\to\infty} \frac{\sum_{d=0}^{2m} \#G(d,2m)(\mathbb{F}_q)}{\dfrac{\phi_{even}(q)q^{m^2}}{\phi(q)}} = \frac{1}{\phi_{even}(q)} \lim_{m\to\infty} \frac{\phi(q)\sum_{d=0}^{2m} \#G(d,2m)(\mathbb{F}_q)}{q^{m^2}} = 1$$

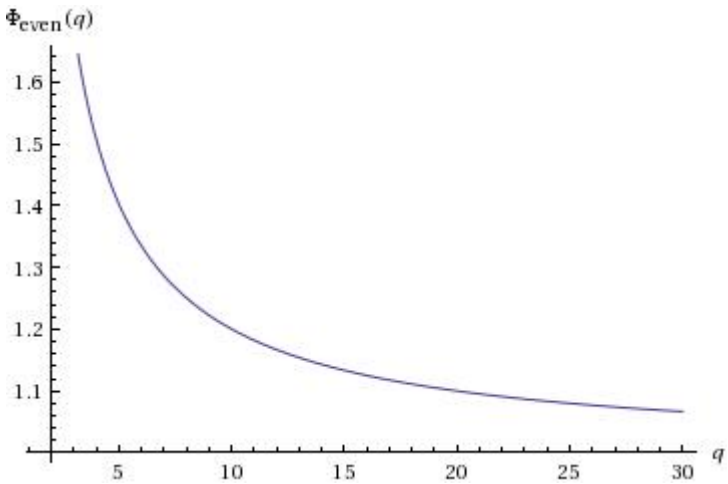

Figure 2: Plot of ϕ_{even}

Now we take $n = 2m + 1$, then the maximum number of subspaces occur at $d = m$ and $d = m + 1$. Since $G(d,n)(\mathbb{F}_q)$ is symmetric, we take $2\#G(m, 2m+1)(\mathbb{F}_q)$ in the limit. Using (5) and (6) again we obtain

$$\lim_{m\to\infty}\frac{\sum_{d=0}^{2m+1}\#G(d,2m+1)(\mathbb{F}_q)}{2\#G(m,2m+1)(\mathbb{F}_q)} = \lim_{m\to\infty}\frac{\phi(q)\sum_{d=0}^{2m+1}q^{(2m+1)d}/\prod_{i=1}^{d}(q^d-q^{i-1})}{2q^{m(m+1)}}$$
$$= \lim_{m\to\infty}\frac{1}{2}\phi(q)\sum_{d=0}^{2m+1}\frac{q^{(d-m)(m+1)+md}}{\prod_{i=1}^{d}(q^d-q^{i-1})}$$
$$= \lim_{m\to\infty}\phi(q)\frac{q^{(m+1)^2}}{\prod_{i=1}^{m+1}(q^m-q^{i-1})} + \lim_{m\to\infty}\phi(q)\sum_{d=m+2}^{2m+1}\frac{q^{(d-m)(m+1)+md}}{\prod_{i=1}^{d}(q^d-q^{i-1})}$$
$$= 1 + \lim_{m\to\infty}\sum_{d=m+2}^{2m+1}q^{-(d-m)(d-m-1)} = 1 + \lim_{m\to\infty}\sum_{d=1}^{m}q^{-d(d+1)}$$

The series $\lim_{m\to\infty}\sum_{d=1}^{m}q^{-d(d+1)} = \sum_{d=1}^{\infty}q^{-d(d+1)}$ converges as well since $q^{-d(d+1)} \leq q^{-d}$ for any $d \geq 1$. Now define the function ϕ_{odd} by $\phi_{odd}(q) = 1 + \sum_{d=1}^{\infty}q^{-d(d+1)}$, for a plot of ϕ_{odd} see figure 3, then we find

$$\lim_{m\to\infty}\frac{\sum_{d=0}^{2m+1}\#G(d,2m+1)(\mathbb{F}_q)}{\frac{2\phi_{odd}(q)q^{m(m+1)}}{\phi(q)}} = \frac{1}{\phi_{odd}(q)}\lim_{m\to\infty}\frac{\phi(q)\sum_{d=0}^{2m+1}\#G(d,2m+1)(\mathbb{F}_q)}{2q^{m(m+1)}} = 1$$

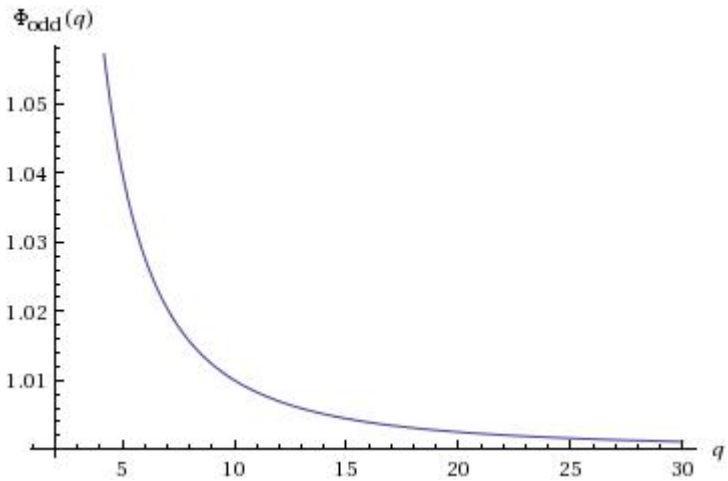

Figure 3: Plot of ϕ_{odd}

From figure 2 and figure 3 we can see that $\phi_{odd}(q) \to 1$ much faster than $\phi_{even}(q) \to 1$. This is not surprising, since for n even we took the subspaces of dimension $\frac{n}{2}$, but for n odd we took all the subspaces of dimensions $\frac{1}{2}(n \pm 1)$. We present the conclusions in the following proposition.

Proposition 5. *Define the functions ϕ and ϕ_2 as $\phi(q) = \lim_{n\to\infty} \prod_{i=1}^{n}(1-q^{-i})$, $\phi_{even}(q) = 1 + 2\sum_{d=1}^{\infty} q^{-d^2}$ and $\phi_{odd}(q) = 1 + \sum_{d=1}^{\infty} q^{-d(d+1)}$, then the following limits for the number of subspaces hold.*

$$\lim_{q\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{d(n-d)}} = 1$$

$$\lim_{q\to\infty} \frac{\sum_{d=0}^{2m} \#G(d,2m)(\mathbb{F}_q)}{q^{m^2}} = 1$$

$$\lim_{q\to\infty} \frac{\sum_{d=0}^{2m+1} \#G(d,2m+1)(\mathbb{F}_q)}{2q^{m(m+1)}} = 1$$

$$\lim_{n\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{nd}/\prod_{i=1}^{d}(q^d - q^{i-1})} = 1$$

$$\lim_{\substack{n\to\infty \\ d\to\infty}} \frac{\#G(d,n)(\mathbb{F}_q)}{\frac{q^{d(n-d)}}{\phi(q)}} = 1$$

$$\lim_{m\to\infty} \frac{\sum_{d=0}^{2m} \#G(d,2m)(\mathbb{F}_q)}{\frac{\phi_{even}(q)q^{m^2}}{\phi(q)}} = 1$$

$$\lim_{m\to\infty} \frac{\sum_{d=0}^{2m+1} \#G(d,2m+1)(\mathbb{F}_q)}{\frac{2\phi_{odd}(q)q^{m(m+1)}}{\phi(q)}} = 1$$

3 Schur Product

In this section the Schur product of vectors and subspaces of $\mathbb{F}_q^n$ will be defined and some basic properties will be shown. We start with the definition.

Definition 8. *Let $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$. The Schur product between v and w, denoted by $v * w$, is defined as*

$$v * w := (v_1 w_1, \ldots, v_n w_n)$$

For V, W linear subspaces of $\mathbb{F}_q^n$ the Schur product is defined as

$$V * W := Span\{v * w : v \in V, w \in W\}$$

In this thesis we only consider the Schur product $V * V$ for a $V \in G(d, n)(\mathbb{F}_q)$.

Lemma 5. *For any $u, v, w \in \mathbb{F}_q^n$ and $\alpha \in \mathbb{F}_q$ the following properties of the Schur product hold.*

1. $v * w = w * v$
2. $(\alpha v) * w = \alpha(v * w)$
3. $(u + v) * w = u * w + v * w$
4. $v * w = 0$ *if and only if for any* $i \in \{1, \ldots, n\}$ *it holds that* $v_i = 0$ *or* $w_i = 0$.
5. *For V, W subspaces of $\mathbb{F}_q^n$ with $W \subset V$, then $W * W \subset V * V$.*

Proof. 1. Since $v_i, w_i \in \mathbb{F}_q$, we have that $v_i w_i = w_i v_i$ for $i = 1, \ldots n$. So

$$v * w = (v_1 w_1, \ldots, v_n w_n) = (w_1 v_1, \ldots, w_n v_n) = w * v$$

2. $(\alpha v) * w = (\alpha v_1 w_1, \ldots, \alpha v_n w_n) = \alpha(v_1 w_1, \ldots, v_n w_n) = \alpha(v * w)$
3. $(u+v)*w = ((u_1+v_1)w_1, \ldots, (u_n+v_n)w_n) = (u_1 w_1+v_1 w_1, \ldots, u_n w_n+v_n w_n) = u*w+v*w$
4. $v * w = 0$ if and only if $v_i w_i = 0$ for $i = 1, \ldots, n$. Since $\mathbb{F}_q$ is a domain, $v_i w_i = 0$ if and only if $v_i = 0$ or $w_i = 0$.
5. Let $v, w \in W$, then $v, w \in V$. So $v * w \in V * V$. Hence $W * W \subset V * V$. □

If $V \subset \mathbb{F}_q^n$ is given as $V = \text{Span}\{v_1, \ldots, v_m\}$ with $v_i \in \mathbb{F}_q^n$, $i = 1, \ldots, m$, then any $u, w \in V$ can be written as $u = \sum_{j=1}^m a_j v_j$ and $w = \sum_{j=1}^m b_j v_j$ for certain $a_j, b_j \in \mathbb{F}_q$, $j = 1, \ldots, m$. Then

$$v * w = (\sum_{j=1}^m a_j v_j) * (\sum_{k=1}^m b_k v_k) = \sum_{j=1}^m \sum_{k=1}^m a_j b_k v_j * v_k$$

So $V * V$ is spanned by $\{v_j * v_k \quad : j = 1, \ldots, m, k = 1, \ldots, m\}$. Note, that if all vectors in $\{v_1, \ldots, v_m\}$ are linearly independent, it is in most cases not true that all vectors in $\{v_j * v_k \quad : j = 1, \ldots, m, k = 1, \ldots, m\}$ are linearly independent. As a consequence of this, we have the following result.

Corollary 2. *If $V \subset \mathbb{F}_q^n$ has dimension d, then $Dim(V * V) \leq \binom{d}{2} + d$.*

Proof. Let $\{v_1 \ldots, v_d\}$ be a basis of V. Then $V * V = \text{Span}\{v_j * v_k \quad : j = 1, \ldots, m, k = 1, \ldots, m\}$ and since the Schur product is symmetric the set $\{v_j * v_k \quad | j = 1, \ldots, m, k = 1, \ldots, m\}$ consists of at most $\binom{d}{2} + d$ elements. Hence $\text{Dim}(V * V) \leq \binom{d}{2} + d$. □

Some examples to show what the Schur product of subspaces can be will now be given.

Example 4. *1. Let $V \subset \mathbb{F}_q^3$ be given as $V = Span\{v_1 = (1,1,0), v_2 = (0,1,1)\}$. Then*

$$\begin{aligned} v_1 * v_1 &= (1,1,0) = v_1 \\ v_1 * v_2 &= (0,1,0) \\ v_2 * v_2 &= (0,1,1) = v_2 \end{aligned}$$

These are all linearly independent, and so $V * V = \mathbb{F}_q^3$.

2. Let $W \subset \mathbb{F}_q^3$ be given as $W = Span\{w_1 = (1,1,0), w_2 = (0,0,1)\}$. Then

$$\begin{aligned} w_1 * w_1 &= (1,1,0) = w_1 \\ w_1 * w_2 &= (0,0,0) \\ w_2 * w_2 &= (0,0,1) = w_2 \end{aligned}$$

We see that here $W * W = W$.

3. Let $U \subset \mathbb{F}_3^3$ be given as $U = Span\{u_1 = (1,0,0), u_2 = (0,2,1)\}$. Then

$$\begin{aligned} u_1 * u_1 &= (1,0,0) = u_1 \\ u_1 * u_2 &= (0,0,0) \\ u_2 * u_2 &= (0,1,1) \end{aligned}$$

From this we get $U * U = Span\{u_1, (0,1,1)\}$ and we notice that now $U * U \neq U$.

From these examples it is clear that the Schur product of subspaces can vary greatly. The Schur product of a subspace can be the whole space $\mathbb{F}_q^n$, the subspace itself, and it can be different from the subspace but with the same dimension. In particular, if $V \subset \mathbb{F}_q^n$, then it does not hold in general that $V \subset V * V$. However, over $\mathbb{F}_2$ we have that $v * v = v$ for any $v \in \mathbb{F}_2^n$. So then it is always true that $V \subset V * V$.
The Schur product of vectors was defined with respect to the standard basis of $\mathbb{F}_q^n$. The next example shows what can happen if a different basis is chosen.

Example 5. *Let (e_1, e_2, e_3) be the standard basis of $\mathbb{F}_3^3$ and take $v_1 = (2,1,0), v_2 = (0,1,2)$ with respect to this basis. If the subspace V is defined as $V = Span\{v_1, v_2\}$, we have*

$$\begin{aligned} v_1 * v_1 &= (1,1,0) \\ v_1 * v_2 &= (0,1,0) \\ v_2 * v_2 &= (0,1,1) \end{aligned}$$

and thus $V * V = \mathbb{F}_3^3$.

However, if we take $B = \{v_1, v_2, e_2\}$ as a basis of $\mathbb{F}_3^3$, then, with respect to the new basis, $v_1 = (1,0,0)_B, v_2 = (0,1,0)_B$. For the Schur product of V we now get

$$\begin{aligned} v_1 * v_1 &= (1,0,0)_B \\ v_1 * v_2 &= (0,0,0)_B \\ v_2 * v_2 &= (0,1,0)_B \end{aligned}$$

and so, with respect to the basis B, $V * V = V$.

From example 5 it is clear that the Schur product depends on the basis chosen for $\mathbb{F}_q^n$. This won't pose much of a problem though, since if B_1, B_2 are two different basis of $\mathbb{F}_q^n$ and $V, W \subset \mathbb{F}_q^n$ such that if $v = (v_1, \ldots, v_n)_{B_1} \in V$ then there is a $w \in W$ with $w = (v_1, \ldots, v_n)_{B_2}$ and vice versa. Let $(V * V)_{B_i}$ denote the Schur product of V with respect to the basis B_i. Then for any $u = (u_1, \ldots, u_n)_{B_1} \in (V * V)_{B_1})$ there is a $x \in (W * W)_{B_2}$ such that $x = (u_1, \ldots, u_n)_{B_2}$. So if for a $V \subset \mathbb{F}_q^n$ the Schur product $V * V$ has a certain property with respect to a basis B of $\mathbb{F}_q^n$, then there is a $W \subset \mathbb{F}_q^n$ such that $W * W$ has the same property with respect to the standard basis of $\mathbb{F}_q^n$.
In example 4 there were examples of subspaces for which the Schur product either increased in dimension or for which the dimension stayed the same. This leads us to wondering whether the Schur product can also decrease in dimension. The following lemma deals with this.

Lemma 6. *Let V be a d-dimensional subspace of $\mathbb{F}_q^n$, then $Dim(V * V) \geq d$.*

Proof. Let $V \in G(d,n)(\mathbb{F}_q)$, then from (1) there is a basis of V consisting of vectors of the form $v_i = e_{\sigma(i)} + \sum_{j=d+1}^{n} a_{i,j} e_{\sigma(j)}$ where $\sigma \in S_n$, $i = 1, \ldots, d$ and $a_{i,j} \in \mathbb{F}_q \quad \forall i, j$. Then $v_i * v_i = e_{\sigma(i)} + \sum_{j=d+1}^{n} a_{i,j}^2 e_{\sigma(j)}$. Since $e_{\sigma(i)} \notin \mathrm{Span}\{e_{\sigma(1)}, \ldots, e_{\sigma(i-1)}, e_{\sigma(i+1)}, \ldots, e_{\sigma(d)}\}$ for any $i \in \{1, \ldots, d\}$, it follows that $v_i * v_i \notin \mathrm{Span}\{v_1 * v_1, \ldots, v_{i-1} * v_{i-1}, v_{i+1} * v_{i+1}, \ldots, v_d * v_d\}$ for any $i \in \{1, \ldots, d\}$. Hence the vectors $v_1 * v_1, \ldots, v_d * v_d$ are all linearly independent and thus $\mathrm{Dim}(V * V) \geq d$. $\square$

4 Schur Product of Subspaces

Now that some of the basic properties of Schur products are known, we wish to answer the main question: How many linear subspaces of $\mathbb{F}_q^n$ are there for which the Schur product is not equal to $\mathbb{F}_q^n$. An exact answer might not be possible, but upper or lower bounds might be able to be found. In this section various methods will be used to try and find these upper or lower bounds.

Definition 9. *The set of all d-dimensional linear subspaces of $\mathbb{F}_q^n$ for which the Schur product is, respectively is not, equal to $\mathbb{F}_q^n$ is denoted by $\mathcal{W}(d,n,q)$, respectively $\mathcal{V}(d,n,q)$, i.e. $\mathcal{W}(d,n,q) = \{W \subset \mathbb{F}_q^n : Dim(W) = d, W * W = \mathbb{F}_q^n\}$ and $\mathcal{V}(d,n,q) = G(d,n)(\mathbb{F}_q) \backslash \mathcal{W}(d,n,q)$.*

A simple case is given by Corollary 2, since if $\binom{d}{2} + d < n$ it holds automatically that for a d-dimensional subspace the Schur product is not the whole space. Determining when

$$\binom{d}{2} + d - n = \frac{d(d+1)}{2} - n = 0$$

we find that $d = \frac{1}{2} \pm \frac{1}{2}\sqrt{1+8n}$. Since $d \geq 0$, the condition $\binom{d}{2} + d < n$ holds when $0 \leq d < -\frac{1}{2} + \frac{1}{2}\sqrt{1+8n}$. Since $\sqrt{1+8n} > \sqrt{8n} = 2\sqrt{2n}$, a more intuitive bound is $0 \leq d < -\frac{1}{2} + \sqrt{2n}$.

Lemma 7. *Let $V \in G(d,n)(\mathbb{F}_q)$ with $0 \leq d < -\frac{1}{2} + \frac{1}{2}\sqrt{1+8n}$ then $V \in \mathcal{V}(d,n,q)$.*

Next, from lemma 5 (5), if $W \subset V \subset \mathbb{F}_q^n$, then $W * W \subset V * V$. Hence, if $V * V \neq \mathbb{F}_q^n$, then $W * W \neq \mathbb{F}_q^n$ as well. Thus, if we can count $\#\mathcal{V}(n-1,n,q)$, then we can find a lower bound for all the lower dimensional subspaces for which the property holds. This can be done by counting how many different subspaces there are in all the $(n-1)$-dimensional subspaces for which the Schur product is not the whole space. However, counting this amount may be quite difficult as one needs to take into account all the subspaces which are counted multiple times. Using Magma Calculator to count the number of $(n-1)$-dimensional subspaces for which the Schur product is not the whole space for various n and q, the following results were obtained.

$n \setminus q$	2	3	4	5
1	1	1	1	1
2	3	4	5	6
3	6	9	12	15
4	10	16	22	28
5	15	25	35	45
6	21	49	51	-

From the table, there seems to be a pattern in each column. For $q = 2$ it seems to be $\#\mathcal{V}(n-1,n,2) = \sum_{k=1}^{n} k$. We will prove this is true to gain insight in the general case.

Example 6. *Let $V \in G(n-1,n)(\mathbb{F}_2)$, then $V \subset V * V$. Thus, $V \in \mathcal{V}(n-1,n,2)$ is equivalent to $V * V = V$ in this case. There is a basis of V of the form*

$$\{v_i = e_{\sigma(i)} + a_i e_{\sigma(n)} : a_i \in \mathbb{F}_2, i = 1, \ldots, n-1\}$$

for a certain permutation $\sigma \in S_n$. Then $v_i * v_j = a_i a_j e_{\sigma(n)}$ if $i \neq j$ and $v_i * v_i = v_i$. So, if $V * V = V$, this implies that $v_i * v_j = 0$ for all $i \neq j$. Hence, there is at most one $a_i \neq 0$.

There are two possibilities now: either $a_i = 0$ for all i, or there is exactly one $a_i \neq 0$. If all $a_i = 0$, then V is just the span of $n-1$ standard basis vectors. So there are $\binom{n}{n-1} = n$ different subspaces for which this is true. Now assume there is exactly one $a_i \neq 0$. Without loss of generality we can take $a_1 \neq 0$, so $a_1 = 1$. Then $V = Span\{e_{\sigma(1)} + e_{\sigma(n)}, e_{\sigma(2)}, \ldots, e_{\sigma(n-1)}\}$. If $\sigma(1)$ and $\sigma(n)$ are chosen, V is fixed. For $\sigma(1)$ and $\sigma(n)$ there are $\binom{n}{2}$ different choices. Hence

$$\#\mathcal{V}(n-1,n,2) = n + \binom{n}{2} = n + \frac{n(n-1)}{2} = \frac{n(n+1)}{2} = \sum_{k=1}^{n} k.$$

From the Magma Calculator data, the number of elements of $\mathcal{V}(n-1,n,q)$ seems to increase as follows: for $q = 3$ the data suggest $\#\mathcal{V}(n-1,n,3) = \sum_{k=1}^{n}(2k-1)$, for $q = 4$ it is $\#\mathcal{V}(n-1,n,4) = \sum_{k=1}^{n}(3k-2)$. In general this seems to be $\#\mathcal{V}(n-1,n,q) = \sum_{k=1}^{n}((q-1)k-(q-2)$. This can be rewritten as

$$\begin{aligned}
\sum_{k=1}^{n}((q-1)k-(q-2) &= (q-1)\frac{n(n+1)}{2} - n(q-2) \\
&= q(\frac{n(n+1)}{2} - n) - \frac{n(n+1)}{2} + 2n \\
&= q\binom{n}{2} - \binom{n}{2} + n \\
&= (q-1)\binom{n}{2} + n
\end{aligned}$$

We will prove this is true, using mostly the same arguments used in example 6 but adjusted where needed.

Lemma 8. *The number of elements of $\mathcal{V}(n-1,n,q)$ is equal to*

$$\#\mathcal{V}(n-1,n,q) = q\frac{n(n-1)}{2} - \frac{n(n-3)}{2}.$$

Proof. Let $V \in \mathcal{V}(n-1,n,q)$. We choose a basis of V of the form

$$\{v_i = e_{\sigma(i)} + a_i e_{\sigma(n)} : a_i \in \mathbb{F}_q, i = 1, \ldots, n-1\}$$

for a certain $\sigma \in S_n$. Then $v_i * v_i = e_{\sigma(i)} + a_i^2 e_{\sigma(n)}$ and $v_i * v_j = a_i a_j e_{\sigma(n)}$ when $i \neq j$. The vectors $v_1 * v_1, \ldots, v_{n-1} * v_{n-1}$ are linearly independent and $v_i * v_j \notin \mathrm{Span}\{v_1 * v_1, \ldots, v_{n-1} * v_{n-1}\}$. Since $V \in \mathcal{V}(n-1,n,q)$, this implies $v_i * v_j = 0$ for all $i \neq j$. Hence there is at most one $a_i \neq 0$. If all $a_i = 0$, then V is just the span of $n-1$ standard basis vectors. So there are $\binom{n}{n-1} = n$ different subspaces for which this is true. Now suppose there is exactly one $a_i \neq 0$. Without loss of generality we can take $a_1 \neq 0$. Then $V = \mathrm{Span}\{e_{\sigma(1)} + a_1 e_{\sigma(n)}, e_{\sigma(2)}, \ldots, e_{\sigma(n-1)}\}$. For a_1 there are $q-1$ possibilities. If $\sigma(1)$ and $\sigma(n)$ are chosen, V is fixed. For $\sigma(1)$ and $\sigma(n)$ there are $\binom{n}{2}$ different choices. Hence $\#\mathcal{V}(n-1,n,q) = (q-1)\binom{n}{2} + n$. □

From the proof it is seen that

$$\mathcal{V}(n-1,n,q) = \{V = \mathrm{Span}\{e_{\sigma(1)} + a_1 e_{\sigma(n)}, e_{\sigma(2)}, \ldots, e_{\sigma(n-1)}\} : \sigma \in S_n, a_1 \in \mathbb{F}_q\}$$

For $(n-1)$-dimensional subspaces we could determine $\#\mathcal{V}(n-1,n,q)$ exact. One could wonder if, using similar arguments, $\#\mathcal{V}(d,n,q)$ can be determined for arbitrary d. This might be possible for some specific d's, however the combinatorics involved quickly become complicated as d approaches $\frac{n}{2}$. For $d=n-2$ we will compute $\#\mathcal{V}(n-2,n,q)$ analytically, which will also make clear how the computations are more difficult from the $n-1$-dimensional case.
Any element V of $G(n-2,n)(\mathbb{F}_q)$ has a basis of the form

$$\{v_i = e_{\sigma(i)} + a_i e_{\sigma(n-1)} + b_i e_{\sigma(n)} : a_i, b_i \in \mathbb{F}_q, i = 1,\dots,n-2, \sigma \in S_n\}$$

If $V \in \mathcal{V}(n-2,n,q)$, then either $\mathrm{Dim}(V*V) = n-2$ or $\mathrm{Dim}(V*V) = n-1$. When $n=2$ or $n=3$ it is trivial to compute $\#\mathcal{V}(n-2,n,q)$, since then $\#\mathcal{V}(n-2,n,q) = \#G(n-2,n)(\mathbb{F}_q)$. So let $n \geq 4$, we will look at both cases separately. Let $\mathrm{Dim}(V*V) = n-2$. Since the vectors $v_1 * v_1, \dots, v_{n-2} * v_{n-2}$ are linearly independent, this means that $v_i * v_j = 0$ whenever $i \neq j$. Hence there are at most one $a_i \neq 0$ and one $b_i \neq 0$. If there is one $a_i \neq 0$, then we can choose i arbitrarily since permutations are used to count all the different possibilities. There are the following cases:

1. $a_i = b_i = 0$ for $i = 1,\dots,n-2$, so $V = \mathrm{Span}\{e_{\sigma(1)},\dots,e_{\sigma(n-2)}\}$ for which there are $\binom{n}{2}$ possibilities.

2. $a_{n-2} \neq 0$ and $b_j = 0$ for $j = 1,\dots,n-2$. So $V = \mathrm{Span}\{e_{\sigma(1)},\dots,e_{\sigma(n-3)}, e_{\sigma(n-2)} + a_{n-2}e_{\sigma(n-1)}\}$. There are $q-1$ choices for a_{n-2}, $\binom{n}{2}$ different choices for $\sigma(n-2)$ and $\sigma(n-1)$. There are then $n-2$ choices left for $\sigma(n)$, which each give rise to a different subspace. Hence there are $\binom{n}{2}(q-1)(n-2)$ different subspaces of this form.

3. There is exactly one $a_i \neq 0$ and $b_j \neq 0$ with $i \neq j$. Take $i = n-3$ and $j = n-2$, so

   $$V = \mathrm{Span}\{e_{\sigma(1)},\dots,e_{\sigma(n-4)}, e_{\sigma(n-3)} + a_{n-3}e_{\sigma(n-1)}, e_{\sigma(n-2)} + b_{n-2}e_{\sigma(n)}\}$$

   There are $(q-1)^2$ different choices for a_{n-3} and b_{n-2} together and $\binom{n}{4}$ different possibilities for $\sigma(n-3),\dots,\sigma(n)$. To determine how many different subspaces there are for $\sigma(n-3),\dots,\sigma(n)$ fixed, it is equal to counting how many different two 2cycles there are on S_4, which is 3. So in this case there are $3\binom{n}{4}(q-1)^2$ different possibilities.

4. $a_{n-2} \neq 0$ and $b_{n-2} \neq 0$ and $a_i = b_i = 0$ when $i \neq n-2$. Here $V = \mathrm{Span}\{e_{\sigma(1)},\dots,e_{\sigma(n-2)} + a_{n-2}e_{\sigma(n-1)} + b_{n-2}e_{\sigma(n)}\}$. For the a_{n-2} and b_{n-2} there are $(q-1)^2$ choices. Switching any of the $\sigma(n-2), \sigma(n-1)$ and $\sigma(n)$ doesn't give any new subspaces and when they are chosen the rest is fixed. Hence there are $\binom{n}{3}(q-1)^2$ different subspaces of this form.

These were all the cases of $\mathrm{Dim}(V*V) = n-2$. So now we let $\mathrm{Dim}(V*V) = n-1$. Since the vectors $v_1 * v_1, \dots, v_{n-2} * v_{n-2}$ are linearly independent, this means that there are k, l, $k \neq l$ such that $v_k * v_l \notin \mathrm{Span}\{v_1 * v_1, \dots, v_{n-1} * v_{n-1}\}$ and $v_i * v_j = \alpha v_k * v_l$ for all $i \neq j$ and $\alpha \in \mathbb{F}_q$. This happens in the following cases.

5. There are at least two $a_i \neq 0$ and $b_j = 0$ for all j. So V is of the form $V = \mathrm{Span}\{e_{\sigma(1)} + a_1 e_{\sigma(n-1)}, \dots, e_{\sigma(n-2)} + a_{n-2}e_{\sigma(n-1)}\}$. First note that each choice of $\sigma(n)$ gives rise to the same number of subspaces with all the choices for the a_i's and $\sigma(1),\dots,\sigma(n-1)$ and all these subspaces are different. Consider now the case with σ the identity, then the matrix of V with respect to the basis used here is:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & a_1 & 0 \\ 0 & 1 & \ddots & \vdots & a_2 & 0 \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-2} & 0 \end{pmatrix}$$

We want at least two $a_i \neq 0$, which means that all the vectors $(a_1, \ldots, a_{n-2})$ with at most one $a_i \neq 0$ are rejected, which there are $1 + (n-2)(q-1)$ of. Hence there are $q^{n-d} - (1 + (n-2)(q-1))$ possible vectors that satisfy the condition. Next we need to count how many different subspaces are formed when the first $n-1$ columns are permuted. Note that permuting any of the first $n-2$ columns does not give any new subspaces. So we only need to switch the column with the a_i's with each of the first $n-2$ ones. If it is switched with the first column, the matrix turns into

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 & 1 & 0 \\ a_2 & 1 & \ddots & \vdots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots \\ a_{n-2} & 0 & \cdots & 1 & 0 & 0 \end{pmatrix}$$

We can take linear combinations of the rows without changing the span of the subspace. Now, if $a_1 \neq 0$, then multiplying the first row with a_1^{-1} and adding specific scalar multiples of it to any of the other rows turns the matrix back into the same form as before the permutation. However, if $a_1 = 0$ this is no longer possible. Hence only the case with $a_1 = 0$ needs to be considered. For this there are now $q^{n-3} - (1 - (n-3)(q-1)$ possibilities. Next we swap the a_i's with the second column. If now either $a_1 \neq 0$ or $a_2 \neq 0$, we can again take scalar multiples of the first or second rows respectively and add them to the other ones to turn matrix back into either of the previous forms (after swapping the first and second row if necessary). Hence we can take $a_1 = 0$ and $a_2 = 0$, there are $q^{n-4} - (1 - (n-4)(q-1)$ possibilities here. We can continue in this way until there are no new possibilities. This happens when we can take $a_1 = 0, \ldots, a_{n-3} = 0$. So in total, for fixed $\sigma(n)$, there are $\sum_{k=2}^{n-2} \left(q^{n-k} - (1 + (n-k)(q-1)\right) = \sum_{k=2}^{n-2} \left(q^k - (1 + (k)(q-1)\right)$. This sum can be simplified as follows.

$$\begin{aligned} \sum_{k=2}^{n-2} \Big(q^k - (1 + (k)(q-1)\Big) &= \sum_{k=2}^{n-2} q^k - (q-1) \sum_{k=2}^{n-2} k - (n-3) \\ &= \frac{q^{n-1} - q^2}{q-1} - \frac{1}{2}(q-1)(n-3)n - (n-3) \\ &= \frac{q^{n-1} - q^2}{q-1} - (n-3)(\frac{1}{2}(q-1)n + 1) \end{aligned}$$

Letting $\sigma(n)$ vary, the total number of subspaces in this case is

$$n \sum_{k=2}^{n-2} \Big(q^k - (1 + (k)(q-1)\Big) = n \left(\frac{q^{n-1} - q^2}{q-1} - (n-3)(\frac{1}{2}(q-1)n + 1) \right)$$

Note that when σ is first taken to be the identity, we then swapped $\sigma(n-1)$ with each $\sigma(1), \ldots, \sigma(n-4)$ to get all the possibilities for fixed $\sigma(n)$. So changing $\sigma(n-2)$

and $\sigma(n-2)$ does not change the amount of possibilities. Also, the dual of V is here equal to $V^\perp = \text{Span}\{e_{\sigma(n)}, -a_1 e_{\sigma(1)} - \cdots - a_{n-2}e_{\sigma(n-2)} + e_{\sigma(n-1)}\}$. The total number of subspaces in this case could also be counted by counting the number of 2-dimensional subspaces of the form $V^\perp$ with at least two $a_i \neq 0$. This will be used in the next case.

6. There are at least two $a_i \neq 0$ and there is exactly one $b_j \neq 0$. Without loss of generality we take $b_n \neq 0$. So V is of the form $V = \text{Span}\{e_{\sigma(1)} + a_1 e_{\sigma(n-1)}, \ldots, e_{\sigma(n-3)} + a_{n-3}e_{\sigma(n-1)}, e_{\sigma(n-2)} + a_{n-2}e_{\sigma(n-1)} + b_{n-2}e_{\sigma(n)}\}$. The dual of V is given as

$$V^\perp = \text{Span}\{b_{n-2}e_{\sigma(n-2)} - e_{\sigma(n)}, -a_1 e_{\sigma(1)} - \cdots - a_{n-2}e_{\sigma(n-2)} + e_{\sigma(n-1)}\}$$

To count all the subspaces here, it is enough to count all the subspaces of the form of $V^\perp$. For the first basis vector there are $\binom{n}{2}(q-1)$ possibilities. For the second basis vector we look at the previous case. The difference in $V^\perp$ between the two cases is the term $b_{n-2}e_{\sigma(n-2)}$. However, from the previous case, taking $\sigma(n-2)$ fixed does not change the possibilities of the vectors $-a_1 e_{\sigma(1)} - \cdots - a_{n-2}e_{\sigma(n-2)} + e_{\sigma(n-1)}$. So the total number of subspaces here is equal to

$$\binom{n}{2}(q-1)\sum_{k=2}^{n-2}\Big(q^k - (1+(k)(q-1)\Big) = \binom{n}{2}(q-1)\left(\frac{q^{n-1}-q^2}{q-1} - (n-3)(\frac{1}{2}(q-1)n+1)\right)$$

7. There are at least two $a_i \neq 0$ and two $b_j \neq 0$ with the condition that

$$\text{Dim}(\text{Span}\{(a_i, b_i) * (a_j, b_j) : 1 \leq i < j \leq n-2\}) = 1 \tag{7}$$

This condition ensures that there is at least one i with $a_i \neq 0$ and $b_i \neq 0$. Suppose that there are $k, l, m \in \{1, \ldots, n-2\}$, all distinct, such that $(a_k, b_k) * (a_l, b_l \neq 0$, $(a_k, b_k) * (a_m, b_m) \neq 0$ and $(a_l, b_l), (a_m, b_m)$ linearly independent. If $a_k \neq 0$ and $b_k \neq 0$, then in matrices,

$$\begin{vmatrix} a_k a_l & b_k b_l \\ a_k a_m & b_k b_l \end{vmatrix} = a_k b_k \begin{vmatrix} a_l & b_l \\ a_m & b_m \end{vmatrix} \neq 0$$

Then the condition (7) is not satisfied. Next, suppose $b_k = 0$ (taking $a_k = 0$ then isn't required because of the permutation). Since (a_l, b_l) and (a_m, b_m) are linearly independent, having both $b_l = 0$ and $b_m = 0$ is not possible. If $b_l = 0$ there is a j, $j \neq m$, such that $b_j \neq 0$. If $a_j \neq 0$ as well condition (7) is automatically not satisfied and if $a_j = 0$ the previous situation applies with $(a_j, b_j), (a_k, b_k)$ and (a_m, b_m), thus (7) is then not satisfied as well. So assume $a_i \neq 0$, $b_i \neq 0$ for $i = l, m$. But then $(a_l, b_l) * (a_m, b_m)$ and $(a_k, b_k) * (a_l, b_l)$ are linearly independent, and again (7) is not satisfied. This shows that the only subspaces that can satisfy (7) with at least three $a_i \neq 0$ and two $b_j \neq 0$ are the subspaces with all the (a_i, b_i) linearly dependent.

Now let all the (a_i, b_i) linearly dependent. So there is a k such that for all i there is an α_i with $(a_i, b_i) = \alpha_i(a_k, b_k)$. If σ is the identity, this gives the following matrix.

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \alpha_1 a_1 & \alpha_1 b_1 \\ 0 & 1 & \ddots & \vdots & \alpha_2 a_2 & \alpha_2 b_2 \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & \alpha_{n-2}a_{n-2} & \alpha_{n-2}b_{n-2} \end{pmatrix}$$

Subtracting α_i times the k'th row from row i puts the matrix back into a form of case 6. So no new subspaces are formed in this situation. This leaves only one form left for the a_i and b_i, namely there are j, l, $j \neq l$ such that $a_i \neq 0$ and $b_i \neq 0$ for $i = j, l$, (a_j, b_j) and $(a_l, b_l$ are linearly independent and $a_i = b_i = 0$ for $i \neq j$ and $i \neq l$. Without loss of generality, let $j = n-3$ and $k = n-2$, then V is of the form $V = \text{Span}\{e_{\sigma(1)}, \ldots, e_{\sigma(n-4)}, e_{\sigma(n-3)} + a_{n-3}e_{\sigma(n-1)} + b_{n-3}e_{\sigma(n)}, e_{\sigma(n-2)} + a_{n-2}e_{\sigma(n-1)} + b_{n-2}e_{\sigma(n)}\}$. Since we want $a_i \neq 0$, $b_i \neq 0$, $i = n-2, n-3$, and $(a_{n-3}, b_{n-3}), (a_{n-2}, b_{n-2})$ linearly independent, there are $(q-1)^2((q-1)^2 - (q-1)) = (q-1)^3(q-2)$ possible choices for the a_i and b_i. Next, if $\sigma(n-3), \ldots, \sigma(n)$ are chosen, each of the choices for $\sigma(1), \ldots, \sigma(n-4)$ gives the same subspace. So there are at least $\binom{n}{4}$ possible choices for the permutations. Now it only needs to be determined if swapping any two of $\sigma(n-3), \ldots, \sigma(n)$ leads to a new subspace or not. It is clear that swapping $\sigma(n-3)$ and $\sigma(n-2)$ does not give any new subspaces, same with swapping $\sigma(n-1)$ and $\sigma(n)$. So if it can be shown that swapping $\sigma(n-3)$ and $\sigma(n-1)$ does not give any new subspaces, we are done. To this end we write $e_{\sigma(n-3)} + a_{n-3}e_{\sigma(n-1)} + b_{n-3}e_{\sigma(n)}$ and $e_{\sigma(n-2)} + a_{n-2}e_{\sigma(n-1)} + b_{n-2}e_{\sigma(n)}$ in matrix form for $n = 4$, since only these four columns matter, and σ the identity, to easily see what happens.

$$\begin{pmatrix} 1 & 0 & a_1 & b_1 \\ 0 & 1 & a_2 & b_2 \end{pmatrix}$$

Swapping the first and third column and multiplying the first row by a_1^{-1} gives

$$\begin{pmatrix} 1 & 0 & a_1^{-1} & a_1^{-1}b_1 \\ a_2 & 1 & 0 & b_2 \end{pmatrix}$$

Subtracting a_2 times the first row from the second row gives

$$\begin{pmatrix} 1 & 0 & a_1^{-1} & a_1^{-1}b_1 \\ 0 & 1 & -a_1^{-1}a_2 & b_2 - a_1^{-1}a_2b_1 \end{pmatrix}$$

Calculating the determinant of the last two columns gives

$$\begin{vmatrix} a_1^{-1} & a_1^{-1}b_1 \\ -a_1^{-1}a_2 & b_2 - a_1^{-1}a_2b_1 \end{vmatrix} = a_1^{-1}(b_2 - a_1^{-1}a_2b_1) + a_1^{-2}b_1a_2 = a_1^{-1}b_2 \neq 0$$

Hence swapping $\sigma(n-3)$ and $\sigma(n)$ does not give any new subspaces. So the total number of subspaces in this case is equal to $\binom{n}{4}(q-1)^3(q-2)$.

Adding the numbers in all cases now gives $\#\mathcal{V}(n-2, n, q)$, which is

$$\begin{aligned} \#\mathcal{V}(n-2,n,q) = &\binom{n}{2} + \binom{n}{2}(q-1)(n-2) + 3\binom{n}{4}(q-1)^2 + \binom{n}{3}(q-1)^2 \\ &+ n\left(\frac{q^{n-1}-q^2}{q-1} - \frac{1}{2}(n-3)((q-1)n+2)\right) \\ &+ \binom{n}{2}(q-1)\left(\frac{q^{n-1}-q^2}{q-1} - \frac{1}{2}(n-3)((q-1)n+2)\right) + \binom{n}{4}(q-1)^3(q-2) \end{aligned}$$

This can be simplified and we conclude this in the following lemma.

Lemma 9. *The number of elements of $\mathcal{V}(n-2,n,q)$ is equal to*

$$\#\mathcal{V}(n-2,n,q) = \binom{n}{2}(1+(q-1)(n+2)) + \left(\binom{n}{3} + 3\binom{n}{4}\right)(q-1)^2 + \binom{n}{4}(q-1)^3(q-2) + \left(n + \binom{n}{2}(q-1)\right)\left(\frac{q^{n-1}-q^2}{q-1} - \frac{1}{2}(n-3)((q-1)n+2)\right)$$

4.1 Bilinear Form

Another way of determining if a subspace $V \in \mathcal{V}(d,n,q)$ is by using proposition 1. If $V \in G(d,n)(\mathbb{F}_q)$, this means that $V * V \neq \mathbb{F}_q^n \iff \mathrm{Dim}((V*V)^\perp) > 0$. Hence, if $V * V \neq \mathbb{F}_q^n$ there is a $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that $\sum_{i=1}^n a_i v_i w_i = 0$ for all $(v_1, \ldots, v_n), (w_1, \ldots, w_n) \in V$. This can be written as a bilinear form.

Definition 10. *A bilinear form on $\mathbb{F}_q^n$ is a function $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ which is linear in each argument separately, that is for all $u, v, w \in \mathbb{F}_q^n$ and $\alpha \in \mathbb{F}_q$:*

1. $B(u+v,w) = B(u,w) + B(v,w)$
2. $B(u,v+w) = B(u,v) + B(u,w)$
3. $B(\alpha u, v) = B(u, \alpha v) = \alpha B(u,v)$

Any bilinear form on $\mathbb{F}_q^n$ can be expressed as $B(x,y) = x^T A y = \sum_{i,j=1}^n a_{ij} x_i y_j$ where A is a $n \times n$ matrix. So, if $V * V \neq \mathbb{F}_q^n$, then $B_a(v,w) = \sum_{i=1}^n a_i v_i w_i = 0$ for all $v, w \in \mathbb{F}_q^n$ for a bilinear form B_a (we write B_a to denote the dependency on the vector $a = (a_1, \ldots, a_n)$). Since the summation is over a single index only, the matrix that generates the bilinear form is symmetric. We can again use a counting argument using group theory to get a lower bound on $\#\mathcal{V}(d,n,q)$.

Lemma 10. *Define the set G as*

$$G = \{A \in GL(n,\mathbb{F}_q) : \forall a \in \mathbb{F}_q^n \backslash \{0\}, \exists b \in \mathbb{F}_q^n \backslash \{0\} \text{ such that } B_a(Av, Aw) = B_b(v,w) \forall v, w \in \mathbb{F}_q^n\}$$

Then G is a subgroup of $GL(n,\mathbb{F}_q)$.

If D_a is the matrix that generates B_a, then $B_a(Av, Aw) = v^T A^T D_a A w$. So the condition that $B_a(Av, Aw) = B_b(v,w)$ $\forall v, w \in \mathbb{F}_q^n$ is equivalent to $A^T D_a A = D_b$. Hence, G can be written as

$$G = \{A \in GL(n,\mathbb{F}_q) : \forall a \in \mathbb{F}_q^n \backslash \{0\}, \exists b \in \mathbb{F}_q^n \backslash \{0\} \text{ such that } A^T D_a A = D_b\}.$$

Proof. (Lemma 10) If $I \in GL(n,\mathbb{F}_q)$ is the identity matrix, then $I^T D_a I = D_a$, so $I \in G$.
If $A, C \in G$, then $\forall a \in \mathbb{F}_q^n \backslash \{0\}, \exists b, c \in \mathbb{F}_q^n \backslash \{0\}$ such that $A^T D_a A = D_b$ and $C^T D_a C = D_c$. Then, since $A \in G$, $(AC)^T D_a AC = C^T A^T D_a AC = C^T D_b C$ for a $b \in \mathbb{F}_q^n \backslash \{0\}$. And since $C \in G$, $C^T D_b C = D_c$ for a $c \in \mathbb{F}_q^n \backslash \{0\}$. Thus, $AC \in G$.
Finally, if $A \in G$, then $A^T D_a A = D_b$. And hence $(A^T)^{-1} A^T D_a A A^{-1} = (A^T)^{-1} D_b A^{-1} = (A^{-1})^T D_b A^{-1}$. Thus $A^{-1} \in G$. So G is a subgroup of $GL(n,\mathbb{F}_q)$. □

We write G_n instead of just G if the size of the matrices is important. Recall that if $V_d = \text{Span}\{e_1, \ldots, e_d\}$, then $H = \{A \in GL(n, \mathbb{F}_q) : AV_d = V_d\}$ is a group. Thus $H \cap G$ is a subgroup of G. Using theorem 2, $G = \bigcup_{i=1}^m g_i(H \cap G)$ for certain $g_i's \in G$, $m = [G : H \cap G]$ and $g_i(H \cap G) \cap g_j(H \cap G) = \emptyset$ if $i \neq j$. Then, from the proof of lemma 2, each of these g_i gives a different $g_iV_d \in G(d, n)(\mathbb{F}_q)$.

Lemma 11. *Let $G1 = \{g_1, \ldots .g_m\}$, where $m = [G : H \cap G]$, such that $G = \bigcup_{i=1}^m g_i(H \cap G)$, then the set $\{g_iV_d : g_i \in G_1\} \subset \mathcal{V}(d, n, q)$ and $\#\{g_iV_d : g_i \in G_1\} = [G : H \cap G]$.*

Proof. Let B_b be a bilinear form on $\mathbb{F}_q^n$ such that $B_b(v, w) = 0$ for all $v, w \in V_d$. Let $g \in G$, then there is a bilinear form B_a such that $B_a(gv, gw) = B_b(v, w) = 0$ for all $v, w \in V_d$. Hence $gV_d \in \mathcal{V}(d, n, q)$ and thus $\{g_iV_d : g_i \in G_1\} \subset \mathcal{V}(d, n, q)$. Since each $g_i \in \{g_iV_d : g_i \in G_1\}$ gives a different $g_iV_d \in G(d, n)(\mathbb{F}_q)$ by the proof of lemma 2, we have $\#\{g_iV_d : g_i \in G_1\} = \#G1 = [G : H \cap G]$. □

Next, we want to determine what elements of G look like to determine $\#G$ and $\#(H \cap G)$.

Lemma 12. *The group G consists of permutation matrices plus scalar multiplication of the columns, i.e. if $A \in G$ with $A = [v_1, \ldots, v_n]$ where each $v_i \in \mathbb{F}_q^n$, then $v_i = \beta_i e_{\sigma(i)}$ for $i = 1, \ldots, n$, $\beta_i \in \mathbb{F}_q^*$ and a permutation $\sigma \in S_n$.*

Proof. Let $A \in GL(n, \mathbb{F}_q)$ with

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

Define $v_j = (a_{1j}, \ldots, a_{nj})$ for $j = 1, \ldots, n$. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$, then, with matrix multiplication, $(A^T D_\alpha A)_{jk} = \sum_{i=1}^n \alpha_i a_{ij} a_{ik}$. Note that $A^T D_\alpha A$ is a symmetric matrix. Now

$$\begin{aligned} A \in G &\iff \sum_{i=1}^n \alpha_i a_{ij} a_{ik} = 0 \quad \forall \alpha \in \mathbb{F}_q^n \backslash \{0\}, 1 \leq j < k \leq n \\ &\iff a_{ij} a_{ik} = 0, \quad i = 1, \ldots, n, 1 \leq j < k \leq n \\ &\iff v_j * v_k = 0, 1 \leq j < k \leq n \\ &\iff v_j = \beta_j e_{\sigma(j)}, \quad j = 1, \ldots, n, \quad \beta_j \in \mathbb{F}_q^*, \quad \sigma \in S_n \end{aligned}$$

□

So G consists of matrices with in each row and column exactly one non-zero element. Each permutation $\sigma \in S_n$ and $\beta_j \in \mathbb{F}_q^*$, $j = 1, \ldots, n$, with $v_j = \beta_j e_{\sigma(j)}$ gives a different matrix $A = [v_1, \ldots, v_n] \in G$. Hence

$$\#G = (q-1)^n n! \tag{8}$$

Now, let $A \in (H \cap G)$. From lemma 4, $A \in H$ is of the form

$$A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix}$$

where $A_{11} \in \mathrm{GL}(d, \mathbb{F}_q)$, $A_{22} \in \mathrm{GL}(n-d, \mathbb{F}_q)$ and A_{12} a $d \times n-d$ matrix. Since $A \in G$ as well, A is a permutation plus scalar multiples. Hence $A_{11} \in G_d$, $A_{22} \in G_{n-d}$ and $A_{12} = 0$. From (8) it follows that

$$H \cap G = (q-1)^d d! \cdot (q-1)^{n-d}(n-d)! = (q-1)^n d!(n-d)!$$

Now we can compute $[G, H \cap G]$.

$$[G, H \cap G] = \frac{\#G}{\#(H \cap G)} = \frac{(q-1)^n n!}{(q-1)^n d!(n-d)!} = \binom{n}{d}$$

Thus $\#\mathcal{V}(d, n, q) \geq \binom{n}{d}$. However, this bound could have been acquired more easily. We started with V_d and multiplied it with a permutation matrix plus scalar multiples. But this just results in a permutation on the first d standard basis vectors. Thus, for $g \in G$, $gV_d = \mathrm{Span}\{e_{\sigma(1)}, \ldots, e_{\sigma(d)}\}$ for a permutation $\sigma \in S_n$. And there are exactly $\binom{n}{d}$ permutations of $\{1, \ldots, d\}$ in S_n.

4.2 Schur Product of Cyclic Codes

In this section we investigate what the Schur product of cyclic codes is and try to find bounds on the number of cyclic codes C for which $C * C = \mathbb{F}_q^n$. First there is the following lemma.

Lemma 13. *Let C be a cyclic code, then $C * C$ is also cyclic.*

Proof. We have $C * C = \mathrm{Span}\{b * c : b, c \in C\}$. Let $b = (b_1, \ldots, b_n), c = (c_1, \ldots, c_n) \in C$, then $b * c = (b_1c_1, \ldots, b_nc_n) \in C * C$. C is cyclic, so $(b_n, b_1, \ldots, b_{n-1}), (c_n, c_1, \ldots, c_{n-1}) \in C$. Thus $(b_nc_n, b_1, c_1, \ldots, b_{n-1}c_{n-1}) = (b_n, b_1, \ldots, b_{n-1}) * (c_n, c_1, \ldots, c_{n-1}) \in C * C$. So $C * C$ is cyclic as well. □

Recall that $\mathbb{F}_q^n$ as vector space can be identified with $R = \mathbb{F}_q[X]/(x^n - 1)$ and that a code C is linear and cyclic in R if and only if $C = (\overline{f})$ with $f|(X^n - 1)$. Also, let $k =$deg(f) and write $f = \sum_{i=0}^{k} a_i X^i$ where each $a_i \in \mathbb{F}_q$, then $\mathrm{Dim}(C) = n - k$ and the set $\{X^i f : i = 0, \ldots, n-k-1\}$ forms a basis for C. For the Schur product of C only the Schur product between all the basis vectors matter. Let $0 \leq j \leq n-k-1$, then

$$\begin{aligned} f * (X^j f) &= (a_0, \ldots, a_k, 0, \ldots, 0) * (0, \ldots, 0, a_0, \ldots, a_k, 0, \ldots, 0) \\ &= (0, \ldots, 0, a_0a_j, \ldots, a_ka_{k-j}, 0, \ldots, 0) \\ &= \sum_{i=j}^{k} a_i a_{i-j} X^i = \sum_{i=0}^{k-j} a_{i+j} a_i X^{i+j} \end{aligned}$$

Similarly for $0 \leq j \leq l \leq n-k-1$

$$(X^j f) * (X^l f) = \sum_{i=l-j}^{k} a_i a_{i-l+j} X^{i+j} = \sum_{i=0}^{k-l+j} a_{i+l-j} a_i X^{i+l}$$

If we want to know what the Schur product of basis vectors is, we only need to look at $f * (X^j f)$ for $0 \leq j \leq n-k-1$, since the coefficients that arise in $(X^j f) * (X^l f)$, $j \leq l$, also appear in $f * (X^{l-j} f)$. Since $C * C$ is cyclic, if there is a $0 \leq j \leq n-k-1$ such that $f * (X^j f) = \alpha X^l$ for an $\alpha \in \mathbb{F}_q^*$ and $1 \leq l \leq k+1$ then $X^i \in C * C$ for each $i = 1, \ldots, n$ and thus $C * C = \mathbb{F}_q^n$. We show this is possible if the dimension of C is large enough.

Lemma 14. *Let $C = (\overline{f})$ with $f|(X^n - 1)$. If Dim$(C) \geq \frac{1}{2}(n+1)$ then $C * C = \mathbb{F}_q^n$.*

Proof. Let $k =$deg(f) and write $f = \sum_{i=0}^{k} a_i X^i$ with $a_i \in \mathbb{F}_q$ and since $f|(X^n - 1)$ we have $a_0 \neq 0$ and $a_k = 1$. Since Dim$(C) \geq \frac{1}{2}(n+1)$ and Dim$(C) = n - k$ it holds that $k \leq \frac{1}{2}(n-1)$ and thus $k \leq n - k - 1$. So $X^k f = \sum_{i=0}^{k} a_i X^{k+i} \in C$. Now $f * (X^k f) = \sum_{i=0}^{0} a_{i+k} a_i X^{i+k} = a_0 a_k X^k$. Hence $X^i \in C * C$ for each $i = 1, \ldots, n$ and thus $C * C = \mathbb{F}_q^n$. □

Lemma 7 and lemma 14 together give a bound for which cyclic codes the Schur product is still undetermined. This is for

$$-\frac{1}{2}(1 - \sqrt{1 + 8n}) \leq \text{Dim}(C) \leq \frac{n}{2} \tag{9}$$

Note that for $n = 7$ it holds that $3 < -\frac{1}{2}(1 - \sqrt{1 + 8 \cdot 7})$ and $4 \geq \frac{1}{2}(7 + 1) = 4$, so there is no possible cyclic code that satisfies (9) here. Since both bounds are strictly increasing, it follows that for $n < 7$ there are no cyclic codes that satisfy (9) either. For $n = 8$ we have $-\frac{1}{2}(1 - \sqrt{1 + 8 \cdot 8}) \leq 4 \leq \frac{8}{2}$. Thus for $n \geq 8$ it is possible that there are cyclic codes that satisfy (9).

Next we determine when $C * C = C$.

Lemma 15. *Let $C = (\overline{f})$ with $f = \left(\sum_{i=0}^{k} a_i X^i\right) | (X^n - 1)$ where $k =$ deg(f) and $a_k = 1$, then $C * C = C$ if and only if $a_i = 0$ or $a_i = 1$ for $i = 1, \ldots, k$ and $f * (X^j f) = 0$ for each $1 \leq j \leq n - k - 1$.*

Proof. Define $v_m := X^{m-1} f$ for $m = 1, \ldots, n - k$, then $\{v_1, \ldots, v_{n-k}\}$ forms a basis for C. The matrix of C with respect to this basis is:

$$\begin{pmatrix} a_0 & \cdots & a_k & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_k & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_0 & \cdots & a_k \end{pmatrix}$$

Now $v_m * v_m = \sum_{j=0}^{k} a_j^2 X^{j+m-1}$ and from the matrix it is clear that the vectors $v_1 * v_1, \ldots, v_{n-k} * v_{n-k}$ are all linearly independent. Suppose that $a_i = 0$ or $a_i = 1$ for each i, then $v_m * v_m = v_m$. For $1 \leq j < l \leq n - k$, $v_j * v_l = \sum_{i=l-j}^{k} a_i a_{i-l+j} X^{i+j}$, however the same coefficients arise in $v_1 * v_{l-j}$. so if $v_1 * v_j = 0$ for $j \neq 1$, then $v_j * v_l = 0$ as well. So $C * C = \text{Span}\{v_1 * v_1, \ldots, v_{n-k} * v_{n-k}\} = \text{Span}\{v_1, \ldots, v_{n-k}\} = C$.
Now suppose $C * C = C$. Observe that $v_1 * v_1 \notin \text{Span}\{v_2, \ldots, v_{n-k}\}$, thus $v_1 * v_1 = \alpha v_1$ for an $\alpha \in \mathbb{F}_q^*$. This means $\sum_{j=0}^{k} a_j^2 X^j = \sum_{j=0}^{k} \alpha a_j X^j$, hence $a_j^2 = \alpha a_j$ for $j = 1, \ldots, k$. So if $a_j \neq 0$, then $a_j = \alpha$. We had $a_k = 1$ and thus $a_i = 0$ or $a_i = 1$ for each a_i. For $1 \leq j \leq n - k - 1$ we have $v * v_j = \sum_{i=0}^{k-j} a_{i+j} a_i X^{i+j} = \sum_{m=1}^{n-k} \beta_m v_m$ for certain $\beta_m \in \mathbb{F}_q$. The degree of $f * (X^j f)$ is at most k, then looking at the matrix of C and keeping in mind that $a_k = 1$, one can see that $\beta_m = 0$ for each $m > 1$. However, the lowest power of $f * (X^p f)$ is at least j, and thus $\beta_1 = 0$ as well. Hence $f * (X^p f) = 0$ which completes the proof. □

Over $\mathbb{F}_2$ we know that $C \subset C * C$ for $C \in G(d, n)(\mathbb{F}_2)$. If C is cyclic as well, then $C * C$ is cyclic too. So if $C = (\overline{f})$, then $C * C = (\overline{g})$ for a $g \in \mathbb{F}_2[X]$ with $g|f|(X^n - 1)$.

Lemma 16. *If $C = (\overline{f})$ with $f \in \mathbb{F}_2[X]$ irreducible and $f|(X^n - 1)$, then either $C * C = C$ or $C * C = \mathbb{F}_2^n$. If in addition $f * (X^j f) = 0$ for $1 \leq j \leq n - k - 1$ then $C * C = C$.*

Proof. Since $C * C = (\overline{g})$ with $g|f|(X^n - 1)$ and f is irreducible it follows that either $g = 1$ or $g = f$. Hence it holds that either $C * C = C$ or $C * C = \mathbb{F}_2^n$. If we write $f = \sum_{i=0}^{k} a_i X^i$, then either $a_i = 0$ or $a_i = 1$ for any a_i and so the second claim follows from lemma 15. □

Since all cyclic codes can easily be found by finding the factorization of $X^n - 1$, a numerical method is possible to try and find results. The program that we used is the online version of Magma and the code can be found in Appendix A.2. Magma was used for $q = 2, 5, 17$ and various n to find the number of cyclic codes that there are and how many are in $\mathcal{W}(d, n, q)$, the number of cyclic codes that satisfy (9) and how many of those are in $\mathcal{W}(d, n, q)$. The following notation is used:

$$\begin{aligned}
\mathcal{C} &= \#\{C \in G(d,n)(\mathbb{F}_q) : C \text{ cyclic}\} \\
\mathcal{C}_1 &= \#\{C \in G(d,n)(\mathbb{F}_q) : C \text{ cyclic and } C \in \mathcal{W}(d,n,q)\} \\
\mathcal{D} &= \#\{C \in G(d,n)(\mathbb{F}_q) : C \text{ cyclic and } C \text{ satisfies (9)}\} \\
\mathcal{D}_1 &= \#\{C \in G(d,n)(\mathbb{F}_q) : C \text{ cyclic, } C \text{ satisfies (9) and } C \in \mathcal{W}(d,n,q)\}
\end{aligned}$$

The following results were obtained.

$q = 2$											
n	30	31	32	33	34	35	36	37	38	39	40
$\mathcal{C}$	243	128	33	32	27	64	125	4	9	32	81
$\mathcal{C}_1$	164	94	16	22	16	40	71	2	4	24	46
$\mathcal{D}$	101	50	9	12	12	20	47	0	2	12	27
$\mathcal{D}_1$	46	30	0	6	4	8	11	0	0	8	7

$q = 5$											
n	30	31	32	33	34	35	36	37	38	39	40
$\mathcal{C}$	1296	2048	1024	64	16	36	2096	4	64	2048	46656
$\mathcal{C}_1$	763	1654	553	40	6	21	2528	2	30	1821	32919
$\mathcal{D}$	580	912	430	22	6	10	1974	0	34	948	23715
$\mathcal{D}_1$	161	630	72	8	0	3	616	0	4	797	11100

$q = 17$											
n	30	31	32	33	34	35	36	37	38	39	40
$\mathcal{C}$	1024	4	2^{24}	32	324	32	2^{20}	4	64	256	65536
$\mathcal{C}_1$	700	2	-	22	153	24	-	2	30	210	45886
$\mathcal{D}$	476	0	-	12	135	10	-	0	34	106	33686
$\mathcal{D}_1$	228	0	-	6	0	8	-	0	4	82	15624

For $q = 17$, $n = 32$ and $n = 36$, Magma was only able to calculate $\mathcal{C}$, since the number of cyclic codes is too high there. The results seem to vary a lot, which was expected since the factorization of $X^n - 1$ varies a lot with n and q, however it makes it difficult to draw any conclusions from the data. One possible pattern that can be seen is that whenever $\mathcal{D} \neq 0$ then $\mathcal{D}_1 < \mathcal{D}$. However this is not always true. Taking $q = 3$ and $n = 37$ it holds that $f_1 \cdot f_2 \cdot f_3$

where

$$
\begin{aligned}
f_1 &= x + 2 \\
f_2 &= x^{18} + 2x^{16} + 2x^{14} + 2x^{13} + x^{11} + x^7 + 2x^5 + 2x^4 + 2x^2 + 1 \\
f_3 &= x^{18} + x^{17} + 2x^{16} + 2x^{15} + x^{14} + 2x^{13} + 2x^{12} + 2x^{10} + 2x^9 \\
&\quad + 2x^8 + 2x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + x + 1
\end{aligned}
$$

is the factorization of $X^{37} - 1$. The only cyclic codes here that satisfy (9) are $C_1 = (\overline{f_1 f_2})$ and $C_2 = (\overline{f_1 f_3})$ and it is true that $C_1 * C_1 = \mathbb{F}_q^n$ and $C_2 * C_2 = \mathbb{F}_q^n$.

One interesting case is if $q = p^k$ and $n = p^m$ for $k, m > 0$, since then $X^n - 1 = (X - 1)^n$. We have the following data from Magma.

$q = 2$				
n	8	16	32	64
$\mathcal{C}$	9	17	33	65
$\mathcal{C}_1$	4	8	16	32
$\mathcal{D}$	1	3	9	22
$\mathcal{D}_1$	0	0	0	0

$q = 3$				
n	9	27	81	243
$\mathcal{C}$	10	28	82	244
$\mathcal{C}_1$	5	14	41	122
$\mathcal{D}$	1	7	28	100
$\mathcal{D}_1$	0	0	0	0

$q = 5$				
n	25	125		
$\mathcal{C}$	26	126		
$\mathcal{C}_1$	13	63		
$\mathcal{D}$	6	47		
$\mathcal{D}_1$	0	0		

From the data it seems that there are no cyclic codes C that satisfy (9) and for which $C * C = \mathbb{F}_q^n$. This is probably due to the fact that all cyclic codes are generated by $(X - 1)^k$ for $0 \leq k \leq n$ and the structure these polynomials have. However, we do not have a proof for it.

One could also wonder whether the Schur product can be cyclic if the code it self is not cyclic and if the Schur product is not equal to $\mathbb{F}_q^n$. Or if the Schur product can be equal to the dual of a code. Let $C = \text{Span}\{(1, 1, 0, 0), (0, 0, 1, 1)\} \subset \mathbb{F}_2^4$, then $C^\perp = C = C * C$, so we have an example for the second question. One could investigate for which subspaces this holds, but these questions will not be answered in this thesis.

4.3 Lower Bounds on $\#\mathcal{W}(d, n, q)$

So far we have only tried to determine when a subspace $V \in \mathcal{V}(d, n, q)$ in a few specific cases. In this section we look at when a subspace $W \in \mathcal{W}(d, n, q)$, that is $W * W = \mathbb{F}_q^n$, and try to

find a good lower bound for $\#\mathcal{W}(d,n,q)$. If it is possible to find a lower bound $\Theta(n,q)$ on $\sum_{i=0}^{n} \#\mathcal{W}(d,n,q)$ such that

$$\lim_{n\to\infty} \frac{\Theta(m,q)}{\sum_{i=0}^{n} \#G(d,n)(\mathbb{F}_q)} > 0$$

or

$$\lim_{q\to\infty} \frac{\Theta(m,q)}{\sum_{i=0}^{n} \#G(d,n)(\mathbb{F}_q)} > 0,$$

then we know that the same limits hold for $\sum_{i=0}^{n} \#\mathcal{W}(d,n,q)$ instead of $\Theta(m,q)$. We start with d-dimensional subspaces of the following form:

$$W = \mathrm{Span}\{e_1 + a_{1,d+1}e_{d+1} + \cdots + a_{1,n}e_n, \ldots, e_d + a_{d,d+1}e_{d+1} + \cdots + a_{d,n}e_n\}$$

where $a_{i,j} \in \mathbb{F}_q$ for $i = 1,\ldots,d$ and $j = d+1,\ldots,n$. Let $w_i = e_i + a_{i,d+1}e_{d+1} + \cdots + a_{i,n}e_n$ for $i = 1,\ldots,d$, then $V = \mathrm{Span}\{w_1,\ldots,w_d\}$. If each w_i is written as a row of a matrix, the following matrix is acquired.

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & a_{1,d+1} & \cdots & a_{1,n} \\ 0 & 1 & \ddots & \vdots & a_{2,d+1} & \cdots & a_{2,n} \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & a_{d,d+1} & \cdots & a_{d,n} \end{pmatrix}$$

The set of vectors $\{w_i * w_i : i = 1,\ldots,d\}$ are all linearly independent, so if $W \in \mathcal{W}(d,n,q)$, then it is required that

$$\mathrm{Dim}(\mathrm{Span}\{w_i * w_j : 1 \le i < j \le d\}) = n - d. \tag{10}$$

Let $\tilde{e}_j \in \mathbb{F}_q^{n-d}$, $j = 1,\ldots n-d$ be the standard eigenvectors of $\mathbb{F}_q^{n-d}$ and define $\tilde{w}_i = a_{i,d+1}\tilde{e}_i + \cdots + a_{i,n}\tilde{e}_{n-d}$, for $i = 1,\ldots,d$. Then (10) is equivalent to

$$\mathrm{Span}\{\tilde{w}_i * \tilde{w}_j : 1 \le i < j \le d\} = \mathbb{F}_q^{n-d} \tag{11}$$

Two methods will be used to find bounds on when (11) holds.

4.3.1 First Bound

Define $k := \min\{m \in \mathbb{N} : \binom{m}{2} \ge n-d\}$. Let $\sigma \in S_d$, then if

$$\mathrm{Span}\{\tilde{w}_{\sigma(i)} * \tilde{w}_{\sigma(j)} : 1 \le i < j \le k\} = \mathbb{F}_q^{n-d}$$

it holds that $W * W = \mathbb{F}_q^n$ regardless of what each of the $\tilde{w}_{\sigma(j)}$ are for $k < j \le d$. For convenience we let σ be the identity permutation. Let $\tilde{W} := \mathrm{Span}\{\tilde{w}_1,\ldots,\tilde{w}_k\}$. The matrix of $\tilde{W}$ is

$$\begin{pmatrix} a_{1,d+1} & \cdots & a_{1,n} \\ a_{2,d+1} & \cdots & a_{2,n} \\ \vdots & \ddots & \vdots \\ a_{k,d+1} & \cdots & a_{k,n} \end{pmatrix}$$

Let $u_i = (a_{1,d+i}, \dots, a_{k,d+i}) \in \mathbb{F}_q^k$ for $i = 1, \dots, n-d$, then the u_i's are the columns of the matrix of $\tilde{W}$. We want that

$$\mathrm{Span}\{\tilde{w}_i * \tilde{w}_j : 1 \leq i < j \leq k\} = \mathbb{F}_q^{n-d}$$

This holds at least if for every $k = 1, \dots, n-d$ there are $i, j \in \{1, \dots, k\}, i \neq j$ such that $\tilde{e}_k = \tilde{w}_i * \tilde{w}_j$. Let $u_i = e_{i_1}^k + e_{i_2}^k$, where $i_1, i_2 \in \{1, \dots, d\}$ and $i_1 \neq i_2$ for $i = 1, \dots, n-d$ such that $u_i \neq u_j$ whenever $i \neq j$. Then it holds that for every $k = 1, \dots, n-d$, $e_k^{n-d} = \tilde{w}_i * \tilde{w}_j$ for certain i, j with $i \neq j$. To see this, suppose that $\tilde{w}_i * \tilde{w}_j = e_{\sigma(1)}^{n-d} + \dots + e_{\sigma(m)}^{n-d}$ for a permutation $\sigma \in S_{n-d}$ and $1 < m \leq n-d$. But then $u_{\sigma(1)} = u_{\sigma(2)}$, which is not possible by the construction of the u_i's.
Now to count all the different possibilities for the u_i. For u_1 there are $\binom{k}{2}$ possible ways to choose u_1. Since we want $u_2 \neq u_1$, there are $\binom{k}{2} - 1$ possible ways to choose u_2. Continuing this way we find there are $\prod_{k=0}^{n-d-1}(\binom{k}{2} - k)$ different possibilities to choose all the u_i. The same arguments still hold if instead we take $u_i = b_i e_{i_1}^k + c_i e_{i_2}^k$, where $b_i, c_i \in \mathbb{F}_q^*$, $i_1, i_2 \in \{1, \dots, d\}$ and $i_1 \neq i_2$ for $i = 1, \dots, n-d$ such that $e_{i_1}^k + e_{i_2}^k \neq e_{j_1}^k + e_{j_2}^k$ whenever $i \neq j$. Since each $b_i, c_i \in \mathbb{F}_q^*$, there are $(q-1)^{2(n-d)}$ possible ways of choosing all the b_i, c_i. We have only put constrains on the $\tilde{w}_i$ for $1 \leq i \leq k$. For $k < j \leq d$ the $\tilde{w}_j$ can be arbitrarily chosen. Combining this all, we find that

$$\#\mathcal{W}(d,n,q) \geq \psi(d,n,q) := \left(\prod_{j=0}^{n-d-1} \left(\binom{k}{2} - j \right) \right) (q-1)^{2(n-d)} q^{(d-k)(n-d)}$$

This estimate can be improved by observing that if in one fixed u_i the rest of the $k-2$ elements are arbitrarily chosen, it still holds that $W * W = \mathbb{F}_q^n$. To count the extra possibilities created in this way it is more complicated than just multiplying ψ by q^{k-2}, since then certain would be counted multiple times. We assume that $k > 2$. There are $n-d$ columns u_i to choose one from which will have more than two non-zero elements and each of these columns gives different subspaces. Pick u_1 as the column that has more than two non-zero elements. Let $j \in \{3, \dots, k\}$ arbitrarily and suppose that u_1 has j non-zero locations. There are $\binom{k}{j}$ different ways to choose the location of the j non-zero elements and each way gives different subspaces. Now to determine how many possibilities there are for all the other u_i, $i > 1$, such that they still have the same form as before, that is the location of the two non-zero elements are different in each pair u_i, u_j, $i, j > 1$, $i \neq j$. However, not all of those possible choices are allowed, since u_1 has to be taken into account such that (11) still holds. There are $\binom{j}{2}$ different ways of picking two of the j non-zero elements. With the u_i's chosen in this way, (11) at least holds, if there is at least one $v \in \mathbb{F}_q^k$ of the $\binom{j}{2}$ columns with exactly two of the j non-zero elements such that there is no u_j, $j > 1$, with the two non-zero elements at the same location as v. In other words, not all of the u_i, $i > 1$, can have the non-zero elements in locations that u_1 also has non-zero elements. So for a fixed choice of j non-zero locations, the number of possibilities for the u_i, $i > 1$, is equal to the total number of choices that satisfy the criteria minus the possibilities that all of the $u_i, i > 1$ have non-zero elements in the same locations that u_1 also has non-zero elements. This is equal to:

$$(q-1)^{2(n-d-1)+j} \left[\prod_{k=0}^{n-d-2} \left(\binom{k}{2} - i \right) - \left(\prod_{i=1}^{\binom{j}{2}} (n-d-i) \right) \left(\prod_{i=0}^{n-d-2-\binom{j}{2}} \left(\binom{k}{2} - \binom{j}{2} - i \right) \right) \right]$$

Summing over all possible j and all the possible columns the new estimate is:

$$\psi_2(d,n,q) := \psi(d,n,q) + (n-d)q^{(d-k)(n-d)}(q-1)^{2(n-d-1)+j}$$
$$\cdot \left[\prod_{k=0}^{n-d-2} \left(\binom{k}{2} - i \right) - \left(\prod_{i=1}^{\binom{j}{2}} (n-d-i) \right) \left(\prod_{i=0}^{n-d-2-\binom{j}{2}} \left(\binom{k}{2} - \binom{j}{2} - i \right) \right) \right] \quad (12)$$

We use this estimation (12) on some examples of $(n-1)$- and $(n-2)$-dimensional subspaces to see how good it is. The results are in the following table.

	$n=5, d=3, k=3$				$n=6, d=5, k=2$	
q	$\#\mathcal{W}(3,5,q)$	$\psi(3,5,q)$		q	$\#\mathcal{W}(5,6,q)$	$\psi(5,6,q)$
2	15	12		2	42	8
3	400	288		3	328	108
4	2997	1944		4	1314	576

In the table it can be seen that the estimated values are not really close to the real values, but also that it is at least not possible to improve the estimation my multiplying it by an $a > 1$. Furthermore, the ratio $\psi(d,n,q)/\#\mathcal{W}(d,n,q)$ for $n=5, d=3$ decreased from $q=2$ to $q=3$, and from $q=3$ to $q=4$, but for $n=6, d=5$ it increased. We can look at these cases in general.
Fix n and let $d = n-1$. Then $k=2$ and $\psi_2(n-1,n,q) = \psi(n-1,n,q) = (q-1)^2 q^(n-3)$. Using (4), that is

$$\lim_{q\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{d(n-d)}} = 1$$

it follows that

$$\lim_{q\to\infty} \frac{\psi_2(n-1,n,q)}{\#G(n-1,n)(\mathbb{F}_q)} = \lim_{q\to\infty} \frac{(q-1)^2 q^{n-3}}{q^{n-1}} = 1$$

If now $d = n-2$ is taken instead, then $k=3$ and $\psi_2(n-2,n,q) = 6((q-1)^4 - (q-1)^5)q^{2(n-5)+1}$. And so

$$\lim_{q\to\infty} \frac{\psi(n-1,n,q)}{\#G(n-2,n)(\mathbb{F}_q)} = \lim_{q\to\infty} \frac{6((q-1)^4 - (q-1)^5)q^{2(n-5)+1}}{q^{2(n-2)}}$$
$$= \lim_{q\to\infty} \frac{6((q-1)^3 + (q-1)^4)}{q^5} = 0$$

4.3.2 Second Bound

For the second bound on (11) we try a different method. Suppose that for a $d \in \{1,\dots,n-1\}$ we have vectors $v_i = (b_{i,1},\dots,b_{i,n})$ for $i = 1,\dots,d$ where $b_{i,j} \in \mathbb{F}_q$ for all i,j and let $b_{1,j} \neq 0$ for all j. Putting the vectors $v_2,\dots,v_d$ in a matrix it gives

$$A = \begin{pmatrix} b_{2,1} & \cdots & b_{2,n} \\ \vdots & \ddots & \vdots \\ b_{d,1} & \cdots & b_{d,n} \end{pmatrix}$$

Next, we take the Schur product of v_1 with $v_2,\dots,v_d$ respectively and the matrix of this is

$$\tilde{A} = \begin{pmatrix} b_{1,1}b_{2,1} & \cdots & b_{1,n}b_{2,n} \\ \vdots & \ddots & \vdots \\ b_{1,1}b_{d,1} & \cdots & b_{1,n}b_{d,n} \end{pmatrix}$$

Now the matrix $\tilde{A}$ is obtained from A by multiplying each column j by the constant $b_{1,j}$. Since each $b_{1,j} \neq 0$, it now follows that Rank($\tilde{A}$) =Rank(A). This will be used to give a bound for (11).

We have $W \in G(d,n)(\mathbb{F}_q)$, so take $\tilde{w}_1 = a_{1,d+1}\tilde{e}_i + \cdots + a_{1,n}\tilde{e}_{n-d}$ such that $a_{1,j} \neq 0$ for $j = d+1, \ldots, n$ and let $\mathrm{Dim}(\mathrm{Span}\{\tilde{w}_2, \ldots, \tilde{w}_d\}) = n-d$. Then, from what was just shown, (11) holds. This is possible if $d-1 \geq n-d$ or equivalently if $d \geq \frac{1}{2}(n+1)$. Now to count the number of possibilities for this. First, let $\tilde{w}_2, \ldots, \tilde{w}_{n-d+1}$ be the required linear independent vectors, then there are $(q-1)^{n-d}$ different choices for $\tilde{w}_1$, $\prod_{i=1}^{n-d}(q^{n-d} - q^{i-1})$ possibilities for the vectors $\tilde{w}_2, \ldots, \tilde{w}_{n-d+1}$ and $q^{(n-d)(d-(n-d-1))}$ different ways of choosing the vectors $\tilde{w}_{n-d+2}, \ldots, \tilde{w}_n$. In total we have

$$\mathcal{W}(d,n,q) \geq \varphi_1(d,n,q) := (q-1)^{n-d} q^{(n-d)(d-(n-d+1))} \prod_{i=1}^{n-d}(q^{n-d} - q^{i-1}) \tag{13}$$

possibilities for this. Let us check how good it is for $q \to \infty$ and d and n fixed. Using

$$\lim_{q\to\infty} \frac{\prod_{i=1}^{n-d}(q^{n-d} - q^{i-1})}{q^{(n-d)^2}} = 1$$

we find that

$$\begin{aligned} \lim_{q\to\infty} \frac{\varphi_1(d,n,q)}{q^{d(n-d)}} &= \lim_{q\to\infty} \frac{(q-1)^{n-d} q^{(n-d)(d-(n-d+1))} q^{(n-d)^2}}{q^{d(n-d)}} \\ &= \lim_{q\to\infty} \left(\frac{q-1}{q}\right)^{n-d} q^{(n-d)(2d-n)-(n-d)^2-d(n-d)} \\ &= \lim_{q\to\infty} \left(\frac{q-1}{q}\right)^{n-d} = 1 \end{aligned}$$

Now using (4), that is

$$\lim_{q\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{d(n-d)}} = 1$$

it follows that

$$\lim_{q\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{\varphi_1(d,n,q)} = 1.$$

Hence φ_1 is a good estimate as q tends to infinity and d and n are fixed. Now to check how it is if $n \to \infty$. Here we use

$$\lim_{n\to\infty} \frac{\prod_{i=1}^{n-d}(q^{n-d} - q^{i-1})}{\phi(q) q^{(n-d)^2}} = 1.$$

Since φ_1 works for $d > \frac{n}{2}$ and we let $n \to \infty$, so $d \to \infty$ as well, so

$$\lim_{n\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{dn}/\prod_{i=1}^{d}(q^d - q^{i-1})} = \lim_{n\to\infty} \frac{\#G(d,n)(\mathbb{F}_q)}{q^{d(n-d)}/\phi(q)} = 1.$$

Now

$$\lim_{n\to\infty} \frac{\varphi_1(d,n,q)}{q^{d(n-d)}/\phi(q)} = \lim_{n\to\infty} \frac{(q-1)^{n-d} q^{(n-d)(d-(n-d+1))} q^{(n-d)^2} \phi(q)^2}{q^{d(n-d)}}$$
$$= \phi(q)^2 \lim_{n\to\infty} \left(\frac{q-1}{q}\right)^{n-d} q^{(n-d)(2d-n)-(n-d)^2-d(n-d)}$$
$$= \phi(q)^2 \lim_{n\to\infty} \left(\frac{q-1}{q}\right)^{n-d} = 0$$

Thus φ_1 is not a good estimate for $\mathcal{W}(d,n,q)$ as n tends to infinity and q is fixed. The estimate can be improved by setting certain $\tilde{w}_i$ equal to 0 and by permuting the columns. However, this bound holds for $d > \frac{n}{2}$, so it is not usable for $d = \frac{n}{2}$, if n is even, which is where the highest number of subspaces are. If n is odd this bound does work for $d = \frac{1}{2}(n+1)$, but not for $d = \frac{1}{2}(n-1)$. We will first adapt the result for $d = \frac{n}{2}$ and $d = \frac{1}{2}(n-1)$ and then try to improve the result for $d = \frac{n}{2}$ first. If a good enough improvement can be found, the method could then be used to improve the results for $d = \frac{1}{2}(n+1)$ and $d = \frac{1}{2}(n-1)$ when n is odd.

Let $n = 2m$ with $m \in \mathbb{N}$ and take $d = m$. Recall that we chose subspaces W with matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & a_{1,1} & \cdots & a_{1,m} \\ 0 & 1 & \ddots & \vdots & a_{2,1} & \cdots & a_{2,m} \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & a_{m,m} & \cdots & a_{m,m} \end{pmatrix}$$

and we defined $\tilde{w}_i = (a_{i,1}, \ldots, a_{i,m}) \in \mathbb{F}_q^m$ for $i = 1, \ldots, m$. Again choose $a_{1,j} \neq 0$ for $j = 1, \ldots, m$. We will choose $\tilde{w}_2$ and $\tilde{w}_3$ such that $\tilde{w}_1 * \tilde{w}_2, \tilde{w}_1 * \tilde{w}_3, \tilde{w}_2 * \tilde{w}_3$ are linearly independent. If it is then possible to find $\tilde{w}_4, \ldots, \tilde{w}_d$ such that $\tilde{w}_2 * \tilde{w}_3, \tilde{w}_1 * \tilde{w}_2, \ldots, \tilde{w}_1 * \tilde{w}_d$ are all linearly independent we know that (11) holds. Let us solve the latter problem first. We will use the following:

Lemma 17. *Let $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ be such that $u_i \neq 0$ for $i = 1, \ldots, n$, then the mapping $f_u : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined as $f_u(v) = u * v$ is an isomorphism of vector spaces.*

Proof. The linearity of f_u follows from the properties of the Schur product. We show f_u is bijective. Let $v = (v_1, \ldots, v_n) \in Ker(f)$, then $u * v = 0$. So for each i either $u_i = 0$ or $v_i = 0$. But $u_i \neq 0$ for any i, it follows that $v = 0$. Thus $\mathrm{Ker}(f_u) = \{0\}$ and so f_u is injective. Next, let $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ and for each j write $w_j = \alpha_j u_j$. Define $\alpha = (\alpha_1, \ldots, \alpha_n)$, then $w = \alpha * u = f_u(\alpha)$, so f_u is onto. Thus f_u is an isomorphism. □

So if we have $\tilde{w}_2$ and $\tilde{w}_3$ such that $\tilde{w}_1 * \tilde{w}_2, \tilde{w}_1 * \tilde{w}_3, \tilde{w}_2 * \tilde{w}_3$ are linearly independent, we can find vectors $u_4, \ldots, u_m \in \mathbb{F}_q^m$ such that $\tilde{w}_1 * \tilde{w}_2, \tilde{w}_1 * \tilde{w}_3, \tilde{w}_2 * \tilde{w}_3, u_4, \ldots, u_m$ are linearly independent. Define $f_{\tilde{w}_1}$ as in lemma 17 and let $\tilde{w}_j = f_{\tilde{w}_1}^{-1}(u_j)$ for $j = 4, \ldots, d$, then $\tilde{w}_2 * \tilde{w}_3, \tilde{w}_1 * \tilde{w}_2, \ldots, \tilde{w}_1 * \tilde{w}_m$ are all linearly independent. It follows that if $\tilde{w}_2$ and $\tilde{w}_3$ are chosen in this way, it is only required to find all the possible ways of expanding the vectors $\tilde{w}_1 * \tilde{w}_2, \tilde{w}_1 * \tilde{w}_3, \tilde{w}_2 * \tilde{w}_3$ to a basis for $\mathbb{F}_q^m$. From the counting of $\#GL(n, \mathbb{F}_q)$ it follows that there are $\prod_{i=4}^{m}(q^m - q^{i-1})$ possibilities for this.

Now to solve when $\tilde{w}_1 * \tilde{w}_2, \tilde{w}_1 * \tilde{w}_3$ and $\tilde{w}_2 * \tilde{w}_3$ are linearly independent. For this it is enough to take $m = 3$. Let us consider $\tilde{w}_i = (1, a_{i,1}, a_{i,2})$ for $i = 1, 2, 3$ where $a_{1,1} \neq 0$ and $a_{1,2} \neq 0$. The matrix of the three Schur products is given as

$$A = \begin{pmatrix} 1 & a_{1,1}a_{2,1} & a_{1,2}a_{2,2} \\ 1 & a_{1,1}a_{3,1} & a_{1,2}a_{3,2} \\ 1 & a_{2,1}a_{3,1} & a_{2,2}a_{3,2} \end{pmatrix}$$

and we require $\mathrm{Det}(A) \neq 0$. If any $\tilde{w}_i$ is multiplied by a non-zero scalar α, two of the rows of A get multiplied by α and thus the determinant of the resulting matrix is still non-zero. Computing $\mathrm{Det}(A)$ gives

$$\begin{aligned} Det(A) = {} & a_{1,1}a_{3,1}a_{2,2}a_{3,2} - a_{2,1}a_{3,1}a_{1,2}a_{3,2} - a_{1,1}a_{2,1}a_{2,2}a_{3,2} \\ & + a_{2,1}a_{3,1}a_{1,2}a_{2,2} + a_{1,1}a_{2,1}a_{1,2}a_{3,2} - a_{1,1}a_{3,1}a_{1,2}a_{2,2} \end{aligned}$$

Solving $\mathrm{Det}(A) = 0$ for $a_{3,1}$ gives

$$a_{3,1} = \frac{a_{1,1}a_{1,2}a_{2,1}a_{3,2} - a_{1,1}a_{2,1}a_{2,2}a_{3,2}}{a_{1,1}a_{1,2}a_{2,2} - a_{1,2}a_{2,1}a_{2,2} + a_{1,2}a_{2,1}a_{3,2} - a_{1,1}a_{2,2}a_{3,2}}$$

Solving when the denominator is zero for $a_{3,2}$ gives

$$a_{3,2} = \frac{-a_{1,1}a_{1,2}a_{2,2} + a_{1,2}a_{2,1}a_{2,2}}{a_{1,2}a_{2,1} - a_{1,1}a_{2,2}}$$

Now this denominator is zero if

$$a_{2,1} = \frac{a_{1,1}a_{2,2}}{a_{1,2}}.$$

This is always well defined since we chose $a_{1,2} \neq 0$. Now for each $a_{3,1}, a_{3,2}, a_{2,1}$ there is one value which it may not be equal to, all other values are allowed. For $a_{2,2}$ there are no constraints, so free choice there. This gives us $(q-1)^8 q$ possibilities. For arbitrary n we then find $(q-1)^{m+5} q^{2m-5}$ possibilities for $\tilde{w}_1, \tilde{w}_2, \tilde{w}_3$ with all elements of $\tilde{w}_1$ non-zero. Combining this with the result for $\tilde{w}_4, \ldots, \tilde{w}_d$ we find as estimate

$$\mathcal{W}(m, 2m, q) \geq \vartheta(q, m) := (q-1)^{m+5} q^{2m-5} \prod_{i=4}^{m} (q^m - q^{i-1}) \tag{14}$$

We show the same limits hold here as in (13) by using

$$\lim_{q \to \infty} \frac{\prod_{i=4}^{m} (q^m - q^{i-1})}{q^{m(m-3)}} = 1.$$

Then

$$\lim_{q \to \infty} \frac{\vartheta(q, m)}{q^{m^2}} = \lim_{q \to \infty} \frac{(q-1)^{m+5} q^{2m-5} q^{m(m-3)}}{q^{m^2}} = \lim_{q \to \infty} \left(\frac{q-1}{q} \right)^{m+5} = 1$$

For the limit as m tends to infinity we use

$$\lim_{m \to \infty} \frac{\prod_{i=1}^{3} (q^m - q^{i-1}) \prod_{i=4}^{m} (q^m - q^{i-1})}{\phi(q) q^{m^2}} = \lim_{m \to \infty} \frac{\prod_{i=1}^{m} (q^m - q^{i-1})}{\phi(q) q^{m^2}} = 1$$

Hence, if q is fixed,

$$\begin{aligned}
\lim_{m\to\infty} \frac{\vartheta(q,m)}{q^{m^2}/\phi(q)} &= \lim_{m\to\infty} \frac{\phi(q)(q-1)^{m+5}q^{2m-5}\prod_{i=4}^{m}(q^m-q^{i-1})}{q^{m^2}} \\
&= \lim_{m\to\infty} \frac{\phi(q)^2(q-1)^{m+5}q^{2m-5}q^{m^2}}{\prod_{i=1}^{3}(q^m-q^{i-1})q^{m^2}} \\
&= \lim_{m\to\infty} \phi(q)^2\left(\frac{q-1}{q}\right)^{m+5}\cdot\frac{1}{\prod_{i=1}^{3}(1-q^{i-m-1})} \\
&= \lim_{m\to\infty} \phi(q)^2\left(\frac{q-1}{q}\right)^{m+5} = 0
\end{aligned}$$

Now let $n = 2m+1$. We will adapt the estimate for $d = \frac{1}{2}(n-1) = m$. In this case if $\tilde{w}_2, \ldots, \tilde{w}_m$ are linearly independent and $\tilde{w}_1$ has each coordinate non-zero, there are $m-1$ Schur products $\tilde{w}_1 * \tilde{w}_2, \ldots, \tilde{w}_1 * \tilde{w}_m$ which are linearly independent. So two vectors are required for a basis of $\mathbb{F}_q^n$. The same method as for n even will be used, only now we can take $m = 5$ and $\tilde{w}_i = (1, a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4})$ for $i = 1, \ldots, 4$. We now make sure that $\tilde{w}_1 * \tilde{w}_2, \tilde{w}_1 * \tilde{w}_3, \tilde{w}_1 * \tilde{w}_4, \tilde{w}_2 * \tilde{w}_3, \tilde{w}_2 * \tilde{w}_4$ are linearly independent. The matrix now here is equal to

$$B = \begin{pmatrix} 1 & a_{1,1}a_{2,1} & a_{1,2}a_{2,2} & a_{1,3}a_{2,3} & a_{1,4}a_{2,4} \\ 1 & a_{1,1}a_{3,1} & a_{1,2}a_{3,2} & a_{1,3}a_{3,3} & a_{1,4}a_{3,4} \\ 1 & a_{1,1}a_{4,1} & a_{1,2}a_{4,2} & a_{1,3}a_{4,3} & a_{1,4}a_{4,4} \\ 1 & a_{2,1}a_{3,1} & a_{2,2}a_{3,2} & a_{2,3}a_{3,3} & a_{2,4}a_{3,4} \\ 1 & a_{2,1}a_{4,1} & a_{2,2}a_{4,2} & a_{2,3}a_{4,3} & a_{2,4}a_{4,4} \end{pmatrix}$$

Solving when $\mathrm{Det}(B) = 0$ and each following denominator for $a_{2,1}, a_{3,1}, a_{2,2}, a_{2,3}$ and $a_{4,2}$ respectively we again find a single value which each of may not assume. For the second to last denominator we also require $a_{3,4} \neq a_{4,4}$. So we fine 9 elements which are also non-zero in addition to the first row. Hence there are $(q-1)^{5+9}q^{3\cdot 5-9}$ possibilities here and thus in general we find

$$\mathcal{W}(m, 2m+1, q) \geq (q-1)^{(m+1)+9}q^{3(m+1)-9}\prod_{i=6}^{m+1}(q^{m+1}-q^{i-1})$$

One can check that for this bound similar limits as earlier hold, but then for n odd. We will attempt to improve the bound for $n = 2m$ and $d = m$, that is (14), and check if it gives a different limit as n tends to infinity. Two different methods will be used.
The first method involves permutations on the columns of the matrix. The matrix is again equal to

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 & a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & a_{m,m} & \cdots & a_{m,m} \end{pmatrix}$$

Let $\tilde{e}_i \in \mathbb{F}_q^m$ be the i'th standard basis vector and define $\tilde{v}_i = (a_{1,i}, \ldots, a_{m,i}) \in \mathbb{F}_q^m$ and $\tilde{w}_i = (a_{i,1}, \ldots, a_{i,m})$ for each $i = 1, \ldots, m$. Then the $\tilde{e}_i$'s and $\tilde{v}_i$'s make up the columns of the matrix. Permuting any two columns with each other can only give a new subspace if a $\tilde{e}_i$ is swapped with a $\tilde{v}_j$. All the permutations will be considered with a systematic approach. However, counting how many new subspaces are obtained when permuting an

arbitrary number of columns will be very difficult, since all possibilities of permuting columns need to be considered. So we do not expect this method to be feasible, we will check to see what happens when one or two columns are permuted. Swapping any $\tilde{e}_i$ with a $\tilde{v}_j$ will be denoted by $\tilde{e}_i \leftrightarrow \tilde{v}_j$. We change which rows are used to find the bound ϑ to make the approach used easier to understand. Instead of the first three rows with non-zero elements, we take the last three rows. So now $a_{m,j} \neq 0$ for $j = 1, \ldots, m$ and $\tilde{w}_{m-1}$ and $\tilde{w}_{m-2}$ have at least two and three non-zero coordinates, respectively, with two in the same column. Also, no permutations will be taken which require altering the values of the coordinates of $\tilde{w}_{m-2}, \tilde{w}_{m-1}, \tilde{w}_m$.
Let us start with $\tilde{e}_1 \leftrightarrow \tilde{v}_1$. Then we require $a_{1,1} = 0$, since otherwise linear combinations of the rows can be taken to get the matrix A back again, and thus no new subspace would be obtained. We require $\tilde{w}_1$ to be linearly independent with the three Schur products of the pairs of the last three rows. However, it does make the counting more difficult for arbitrary permutations, because the number of fixed zero coordinates determine if this is always the case or not. So we will ignore this requirement for now for the rows where the number of always zero coordinates can be greater than two. If the improved bound is still not good enough, there is no reason to include this requirement. We find there are

$$(q-1)^{m+5} q^{2m-5} (q^{m-1} - 1) \prod_{i=5}^{m} (q^m - q^{i-1})$$

different subspaces of this form which are obtained with the same method as ϑ. Next, we let $\tilde{e}_1 \leftrightarrow \tilde{v}_2$. If now $a_{1,2} \neq 0$ we can take linear combinations of the rows to again get the matrix A and if $a_{1,1} \neq 0$ the same can be done, just now we get the matrix of the previous permutation. So to obtain new subspaces, it is required that $a_{1,1} = a_{1,2} = 0$. In general, if $\tilde{e}_1 \leftrightarrow \tilde{v}_j$, the same arguments show that $a_{1,1} = \cdots = a_{1,j} = 0$. Since $\tilde{w}_1$ can not be the zero vector, this can be done for $1 \leq j \leq m-1$. The other coordinates of $\tilde{w}_1$ can again be freely chosen, hence we find

$$(q-1)^{m+5} q^{2m-5} (q^{m-j} - q^3) \prod_{i=5}^{m} (q^m - q^{i-1})$$

different subspaces here.
Now the second column gets permuted, we start again with $\tilde{e}_2 \leftrightarrow \tilde{v}_1$. Then, it is required that $a_{1,1} = 0$ and $a_{2,1} = 0$. If $\tilde{e}_2 \leftrightarrow \tilde{v}_j$, we still require $a_{1,1} = 0$ and now $a_{2,1} = \cdots = a_{2,j} = 0$ as well. Continuing these arguments we find that if $\tilde{e}_k \leftrightarrow \tilde{v}_1$ it is required that $a_{1,1} = \cdots = a_{k,1} = 0$. Since we don't alter the last three rows, this can be done for $1 \leq k \leq n-3$. In general, if $\tilde{e}_k \leftrightarrow \tilde{v}_j$ it is required that $a_{1,1} = \cdots = a_{k,1} = \cdots = a_{k,j} = 0$. Each of the vectors $\tilde{w}_1, \ldots, \tilde{w}_{k-1}$ has one fixed zero coordinate, so they do need to be linearly independent with the other vectors. Summing over all possible k and j we find

$$f_1(m,q) := \sum_{k=1}^{m-3} \sum_{j=1}^{m-1} (q-1)^{m+5} q^{2m-5} (q^{m-j} - 1) \prod_{i=5}^{k+3} (q^{m-1} - q^{i-1}) \prod_{i=k+4}^{m} (q^m - q^{i-1})$$

different subspaces for permuting only one column. To find the limit in this case we note that

each term in the sum can be bounded above by increasing certain powers of q. Hence

$$\begin{aligned}\lim_{m\to\infty}\frac{f(m,q)}{q^{m^2}/\phi(q)} &< \phi(q)\lim_{m\to\infty}(q-1)^{m+5}q^{2m-5}(q^m-1)\frac{\sum_{k=1}^{m-3}\sum_{j=1}^{m-1}\prod_{i=5}^{m}(q^m-q^{i-1})}{q^{m^2}}\\ &< \phi(q)\lim_{m\to\infty}(m-1)(m-3)(q-1)^{m+5}q^{3m-5}\frac{\prod_{i=5}^{m}(q^m-q^{i-1})}{q^{m^2}}\\ &= \phi(q)^2\lim_{m\to\infty}(m-1)(m-3)\left(\frac{q-1}{q}\right)^{m+5}=0\end{aligned}$$

We see it has the same limit as well. When permuting two columns the same approach can be used to find a general formula for $\tilde{e}_p \leftrightarrow \tilde{v}_l$ and $\tilde{e}_k \leftrightarrow \tilde{v}_j$, with $1 \le l < j \le n-1$ and $1 \le p < k \le m-3$. The method works by starting with $\tilde{e}_1 \leftrightarrow \tilde{v}_1$ and $\tilde{e}_2 \leftrightarrow \tilde{v}_2$ and then systematically increasing an index to find formulas for each general case, e.g. $\tilde{e}_1 \leftrightarrow \tilde{v}_1$ and $\tilde{e}_2 \leftrightarrow \tilde{v}_j$, $\tilde{e}_1 \leftrightarrow \tilde{v}_l$ and $\tilde{e}_2 \leftrightarrow \tilde{v}_j$ and so on. We again ignore the condition that the two rows where more than two coordinates at times need to be fixed to zero, which happens in $\tilde{w}_j$ and $\tilde{w}_l$, also have to be linearly independent to the Schur products on the last three rows. The total number of subspaces found is then equal to

$$\begin{aligned}f_2(m,q) :=&(q-1)^{m+5}q^{2m-5}\sum_{p=1}^{m-4}\sum_{k=p+1}^{m-3}\sum_{l=1}^{m-2}\sum_{j=l+1}^{m-1}(q^{m-j}-1)(q^{m-(k+1)}-q)\\ &\cdot\prod_{i=6}^{p+4}(q^{m-2}-q^{i-1})\prod_{i=p+5}^{l+3}(q^{m-1}-q^{i-1})\prod_{i=l+4}^{m}(q^m-q^{i-1})\end{aligned}$$

Here we can again bound each term in the sums by increasing the powers of q and leaving out certain negative terms. This gives

$$\begin{aligned}\lim_{m\to\infty}\frac{f_2(m,q)}{q^{m^2}/\phi(q)} &< \phi(q)\lim_{m\to\infty}(q-1)^{m+5}q^{4m-5}\frac{\sum_{p=1}^{m-4}\sum_{k=p+1}^{m-3}\sum_{l=1}^{m-2}\sum_{j=l+1}^{m-1}\prod_{i=6}^{m}(q^m-q^{i-1})}{q^{m^2}}\\ &= \phi(q)^2\lim_{m\to\infty}(m-1)(m-2)(m-3)(m-3)\left(\frac{q-1}{q}\right)^{m+5}=0\end{aligned}$$

And again the limit is the same. The only way this improvement could possibly be good enough, is if an arbitrary number of columns are permuted. However, this quickly becomes quite difficult to count, since the number of sums keeps increasing. Though we have a systematic way of counting, it becomes too much work as the number of permutations increases. Also, we have ignored the linear independence condition on certain rows, so the actual amount of new subspaces is even less than what was found. So we abandon this method of improving our bound.

The second method used involves which $\tilde{w}_i$ to choose with all non-zero coordinates. The bound ϑ which we found had this for $\tilde{w}_1$, and $\tilde{w}_2$ and $\tilde{w}_3$ had some fixed non-zero elements. So let us take $\tilde{w}_2, \tilde{w}_3, \tilde{w}_4$ now instead. To get new subspaces we then require at least one $a_{1,i} = 0$. Suppose we fix j coordinates to zero, then the rest has to be non-zero. If the linear independence condition is ignored here as well, this then gives $(q-1)^j\binom{n}{n-j}$ different ways of

choosing the first row. Summing over all possible j we find

$$g_2(m,q) := (q-1)^{m+5}q^{2m-5}\prod_{i=5}^{m}(q^m - q^{i-1})\sum_{j=1}^{m}(q-1)^j\binom{m}{m-j}$$

different subspaces. Since $\sum_{j=1}^{m}(q-1)^j\binom{m}{m-j} < q^m$, we find

$$\lim_{m\to\infty}\frac{g_2(m,q)}{q^{m^2}/\phi(q)} < \phi(q)\lim_{m\to\infty}\frac{(q-1)^{m+5}q^{3m-5}\prod_{i=5}^{m}(q^m-q^{i-1})}{q^{m^2}} = 0$$

If now $\tilde{w}_3, \tilde{w}_4, \tilde{w}_5$ are taken instead, we require zero-elements in both the first and the second row and they need to be linear independent with each other. This gives

$$\sum_{j=1}^{m-1}\left(\binom{m}{j}(q-1)^j\left(((q-1)^j-(q-1)) + \left(\binom{m}{j}-1\right)(q-1)^j + \sum_{\substack{k=1\\k\neq j}}^{m-1}(q-1)^k\binom{m}{k}\right)\right)$$

different ways of choosing the first two rows (again ignoring the linear independence condition). The total number of subspaces of this form has again the same limit as n tends to infinity by the same reason as the previous limit: less than all possibilities can be chosen for the first two rows. This can be done for each next three rows and an upper bound can be found in the same way each time. In fact, we can give an upper bound for each row, namely q^m. This will be done for each row, except the row all non-zero elements. We obtain the following. Let g_j denote the number of new subspaces if $\tilde{w}_j, \tilde{w}_{j+1}, \tilde{w}_{j+2}$ are taken as the three rows with the non-zero elements conditions. Then $g_j < (q-1)^m q^{m(m-1)}$ and hence

$$\lim_{m\to\infty}\frac{\sum_{j=1}^{m} g_j}{q^{m^2}} < \lim_{m\to\infty}\frac{\sum_{j=1}^{m}(q-1)^m q^{m(m-1)}}{q^{m^2}} = \lim_{m\to\infty} m\left(\frac{q-1}{q}\right)^m = 0$$

Hence, this method cannot possibly give us a good enough bound. Thus both methods of improving the bound ϑ do not lead to a change in the limit as n tends to infinity. There is no other method to improve the bound, while still using the same technique as in finding ϑ. We conclude that the methods used to find lower bounds $\#\mathcal{W}(d,n,q)$ in this section cannot give a bound $\Theta(m,q)$ such that $\lim_{m\to\infty}\frac{\Theta(m,q)}{q^{m^2}} > 0$. The results in this section then show that

$$\lim_{q\to\infty}\frac{\sum_{i=0}^{n}\mathcal{W}(d,n,q)}{\sum_{i=0}^{n}\#G(d,n)(\mathbb{F}_q)} = 1$$

while

$$\lim_{n\to\infty}\frac{\sum_{i=0}^{n}\mathcal{W}(d,n,q)}{\sum_{i=0}^{n}\#G(d,n)(\mathbb{F}_q)} \tag{15}$$

is still unknown. However, we do expect (15) to be at least strictly positive and perhaps even equal to 1. The reason for this is as follows: for (15) we only need to consider the subspaces with dimension $\frac{n}{2}$. If $\frac{n}{2}$ linearly independent vectors are arbitrarily chosen, there are $\frac{n}{2}(\frac{n}{2}+1)$ Schur products that can be created from these vectors. As n tends to infinity, we have $\frac{n}{2}(\frac{n}{2}+1) \gg n$ and hence it seems plausible that most of the time there are n linearly independent vectors among all those Schur products. To show that this is in fact true, a different counting technique then using combinatorics will probably have to be used.

5 Conclusion

In this thesis we considered the vector space $\mathbb{F}_q^n$ over a finite field with q elements and its linear subspaces. The number of d-dimensional subspaces was counted, and an explicit formula was proven. We found the growth pattern as either $q \to \infty$ or $n \to \infty$ for both the number of d-dimensional subspaces and the total number of linear subspaces. What we showed is that for the total number of subspaces it is enough to consider the subspaces with dimension $\frac{n}{2}$ as either q or n tend to infinity. This makes computations involving either of the limiting cases considerably easier.

The Schur product, denoted by $*$, of vectors was defined as their entry-wise multiplication and the Schur product of subspaces as the span of the Schur product over all pairs of vectors of the subspace. The Schur product of cyclic codes was investigated. We found that it is always cyclic as well and if the dimension of the code is larger than $\frac{n}{2}$, then the Schur product of it is equal to $\mathbb{F}_q^n$. In addition, computer code has been written which can be used in Magma to count all cyclic codes and their Schur products.

The goal was to find for how many subspaces the Schur product is equal to $\mathbb{F}_q^n$. We were able to count this exactly for $(n-1)$- and $(n-2)$-dimensional subspaces. However, for lower dimensional subspaces it becomes very complicated. An exact formula for arbitrary dimension might exist, but it would probably require a smart method of counting. We then tried to find estimates instead and found a lower bound on the number of subspaces V for which $V * V = \mathbb{F}_q^n$ using combinatorics, which in the limit as q tends to infinity has the same growth rate as the total number of subspaces. This implies that if q tends to infinity and one would pick an arbitrary subspace U, the chance that $U * U = \mathbb{F}_q^n$ is equal to 1. However, the limit of the ratio of this lower bound and the total number of subspaces is 0 as n tends to infinity. We do not expect this to be the case for the total number of subspaces V for which $V * V = \mathbb{F}_q^n$. To show that this is true, a different counting technique then using combinatorics will probably have to be used.

A Magma Code

In this section are the codes that are used in this thesis. The program used to execute the code is the online version of Magma, which can be found at http://magma.maths.usyd.edu.au/calc/.

A.1 Code for Schur Product on Subspaces

The following code is used to obtain $G(d,n)(\mathbb{F}_q)$ for given q, d, n. It then computes the Schur product of each element of $G(d,n)(\mathbb{F}_q)$ and calculates for how many the Schur product is equal to $\mathbb{F}_q^n$. The requires manual changes when the dimension of the subspaces is changed. Also, the code can only handle small n and q, since $\#GL(n,\mathbb{F}_q)$ quickly becomes too high for Magma to iterate over.

```
q:=2;
n:=5;
d:=3;
elts:=#GL(n,q)/(#GL(d,q)*#GL(n-d,q)*q^(d*(n-d)));

F:=GF(q);
G:=GL(n,q);
V:=VectorSpace(F,n);

H:={ sub< V | Basis(V)[1],Basis(V)[2],Basis(V)[3]> };
for g in G do
H:= H join { sub<V| Basis(V)[1]*g,Basis(V)[2]*g,Basis(V)[3]*g> };
if #H eq elts then
break;
end if;
end for;

T:=0;
for V1 in H do

L:= { h1*h2 : h1 in Basis(V1),  h2 in Basis(V1) };
Schur:= sub<V | L>;
if Dimension(Schur) eq Dimension(V) then
T:=T+1;
end if;
end for;

elts;
T;
```

A.2 Code for Schur Product on Cyclic Codes

This code is used to calculate the Schur product of all cyclic codes for given n and q. It computes the total number of cyclic codes, for how many the Schur product is equal to $\mathbb{F}_q^n$, the number of cyclic codes that satisfy the bounds (9) and for how many of these codes the Schur product is equal to $\mathbb{F}_q^n$. It also gives two vectors with the number of cyclic codes of a given dimension and for how many cyclic codes of a given dimension the Schur product is equal to $\mathbb{F}_q^n$.

```
q:=5;
n:=40;

F:=GF(q);
V:=VectorSpace(F,n);
R<x>:=PolynomialRing(GF(q));
H:=Factorization(x^n-1);
H;

A:=VectorSpace(RationalField(),n-1) ! 0;
B:=VectorSpace(RationalField(),n-1) ! 0;

Schurall:=0;
CycBound:=0;
CycBoundSchur:=0;
S:=1;
i:=0;

for V1 in H do
i:=i+1;
f:=V1[1];
l:=V1[2];
S:=S*(l+1);
if i eq 1 then
T1:={ R | f^i : i in {1 .. l}} join {R | 1};
else
T1:=car<T1,{ R | f^i : i in {1 .. l}} join {R | 1}>;
end if;
end for;

if i eq 1 then
T:=T1;
else
T:=Flat(T1);
end if;

for f in T do
if i eq 1 then
g:=f;
```

```
else
g:=1;
for j:= 1 to #H do
g:=g*f[j];
end for;
end if;
C:=CyclicCode(n,g mod (x^n-1));
k:=Dimension(C);

if Dimension(C) ne n and Dimension(C) ne 0 then

L:= { h1*h2 : h1 in Basis(C),  h2 in Basis(C) };
Schur:= sub<V | L>;

A[k]:=A[k]+1;
if k ge (-1/2*(1 -Sqrt(1+8*n))) and k le 1/2*(n) then
CycBound:=CycBound+1;
if Dimension(Schur) eq Dimension(V) then
Schurall:=Schurall+1;
CycBoundSchur:=CycBoundSchur+1;
B[k]:=B[k]+1;
end if;
else
if Dimension(Schur) eq Dimension(V) then
Schurall:=Schurall+1;
B[k]:=B[k]+1;

end if;
end if;
else
end if;

end for;

S;
Schurall+1;
CycBound;
CycBoundSchur;
A;
B;
```

References

[1] Jaap Top, *Groepentheorie*, Rijksuniversiteit Groningen, http://www.math.rug.nl/∼top/alg1.pdf

[2] Jaap Top, *Coderingstheorie*, Rijksuniversiteit Groningen, http://www.math.rug.nl/∼top/code.pdf

[3] B. van Geemen, H.W. Lenstra, F. Oort, J. Top, *Algebraische Structuren*, Rijksuniversiteit Groningen, 2012, http://www.math.rug.nl/∼ top/dic.pdf

[4] Ronald Cramer, Ivan Damgård, Jesper Buus Nielson, *Secure Multiparty Computation*, Book Draft, May 2011