A.E. de Jonge

Bounds on the parameters of arithmetic codices

Bachelor thesis, June 12, 2013

Supervisor: Dr. I. Cascudo

Mathematical Institute, Leiden University

Contents

1 Introduction

This thesis is concerned with an object called 'arithmetic codex' which has been introduced recently in [6], and generalizes a number of notions which have been used both in cryptography (in the areas of secret sharing and multiparty computation) and algebraic complexity theory.
The field of secure multi-party computation is concerned with finding protocols that offer the possibility to compute a function in several variables by a number of parties. The extra requirement for these protocols is that all the players have an input for the function of which they do not want others to find out the value. A common example is that of two millionaires that want to determine who of them is the richest without having to reveal the value of their assets [14].
Secret sharing schemes were introduced by Shamir [12] and Blakley [4]. They later turned out to provide an important building block for many multiparty computation protocols, especially when we want to achieve information-theoretic security, i.e., security which holds regardless of the computational power of the adversary. The fundamental results in this area were given by Ben-Or, Goldwasser and Wigderson [3] and, independently, Chaum, Crépeau and Damgaard [8]. They both use Shamir's secret sharing scheme in which certain multiplicative properties are essential. Cramer Damgaard and Maurer [9] captured these algebraic properties in the notion of multiplicative and strongly multiplicative secret sharing schemes. Both notions are encompassed by the concept of arithmetic codex.
On the other hand, the codex also has use in the field of algebraic complexity theory, that analyses the amount of operations one needs to perform algebraic calculations. Namely, the notion of codex encompasses that of symmetric bilinear multiplication algorithm [5].
In this thesis, we first introduce the notion of codex and provide some basic theory. Then we study the conditions under which these objects exist by establishing several bounds on its parameters. We consider first a fruitful approach to finding bounds on some of the integer parameters, based on the relation of codices with coding theory. This approach however does not exploit the multiplicative nature of codices and so we turn to a strategy that depends on the algebra attached to a codex. We can compare the latter bounds with several results known in algebraic complexity. In particular, Fiduccia and Zalcstein and later Adler and Strassen established some results on the multiplicative complexity of algebras. These, in turn, imply as a special case bounds on certain codices. The results in this thesis allow to find alternative and comparatively simple proofs for the same codex bounds in some cases. Furthermore the arguments can be generalized to find bounds on codices which are not direct consequences of the results in [1] and [10].

2 Preliminary Theory

In this section we will provide some theory that is used throughout this thesis. The concept of a codex is what in this thesis revolves around, hence it shall be introduced first.

2.1 Definition of the (n, t, d, r)-codex

We start with the definition of an algebra and a short remark.

Remark. Throughout this thesis, $\mathbb{N}$ will be the set of natural numbers including the zero element 0. Also, any ring will be assumed to be unital and any ring homomorphism $R \to S$ must send 1_R to 1_S.

Definition 2.1 (Algebra)**.** Let R and S be rings and $\phi : R \longrightarrow S$ be a ring homomorphism such that the image of R is contained in the center $Z(S)$ (i.e. for any $r \in R$ and $s \in S$, $\phi(r)s = s\phi(r)$). Suppose moreover that R is commutative, then S is called an *algebra* over R.

We will only consider algebras over finite fields, which in addition are finite commutative rings. If not explicitly stated otherwise, any algebra in this writing will be assumed to be of this kind.
Notice that an algebra of this kind is also a vector space over a finite field, with multiplication in S as additional operation.

Definition 2.2 (Projections)**.** Let $\{R_i\}_{i=0}^n$ be $n+1$ algebras over a common ring. We define natural projections for any subset $A \subseteq \{0, \dots, n\}$:

$$\pi_A : \prod_{i=0}^{n} R_i \longrightarrow \prod_{i \in A} R_i \ , \qquad (r_i)_{i=0}^n \longmapsto (r_i)_{i \in A}.$$

where the product over elements $i \in A$ is taken ordered naturally.

Note that the empty product of objects in the category of rings with identity is its terminal object: The ring with one element. The empty projection is thus the unique ring morphism onto $\{e\}$.

Remark. Let R and S be two algebras over a common ring. Often we will look at $P := R \times S$ with coordinatewise operations. This turns P into an algebra over the same ring. This fact may be used implicitly.

The projections we have just defined are K-algebra morphisms. They preserve addition, multiplication and scalar multiplication.
An n-code, as to be defined below, can be thought of as a kind of 'pre-codex'.

Definition 2.3 (n-Code)**.** Let K be a finite field, S an algebra over K with finitely many elements, and $n \in \mathbb{N}$ a non-zero natural number. A K-linear subset $C \subset S \times K^n$ is called an *n-code* for S over K if:

1. $\mathrm{Im}(\pi_0|_C) = S$;
2. $\ker(\pi_{\{1,\dots,n\}}) \cap C \subseteq \ker(\pi_0)$.

For an n-code C for S over K we define the constant $k_C := \dim_K(S)$. If there is no risk of ambiguity, the subscript C may be left out.

The second property in Definition 2.3 is often referred to as n-reconstruction, which is defined in more rigour through the coming definitions. The property is equivalent to $\pi_{\{1,\dots,n\}}|_C$ being injective. However, there is no such short description for the other types of reconstruction that will follow shortly.
If we have an n-code C for S over K and an element $c = (s, x_1, \dots, x_n) \in C$, then we call s the secret of c, and the x_i its shares. The motivation for this nomenclature comes from the area of secret sharing. Secret sharing schemes were introduced by Shamir [12] and, independently, by Blakley [4]. Secret sharing schemes are used to split the knowledge of some information (a secret) into pieces (the shares) such that a certain minimal number of these pieces are needed to reconstruct the secret, while a small number of shares gives no information about it. Arithmetic codices can be turned into secret sharing schemes, as we will explain below, and the following definitions are inspired by this connection.

Definition 2.4 (A-Reconstruction)**.** Let $C \subseteq S \times K^n$ be an n-code for S over K, and let $A \subseteq \{1, \dots, n\}$ be a non-empty set of indices. We call C *A-reconstructing* if:

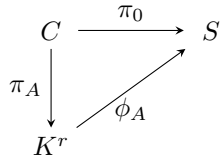
$$\ker(\pi_A) \cap C \subseteq \ker(\pi_0).$$

Note. The second axiom in the definition of an n-code is the requirement of $\{1, \dots, n\}$-reconstruction.

It might not be immediately obvious how this is connected to the intuition that one has about reconstruction. A lemma to light up the connection with secret sharing might be nice.

Lemma 2.5. *Let C be an n-code for S over K and let A be a non-empty subset of $\{1, \dots, n\}$, r its cardinality. Then the following three statements are equivalent:*

1. *C is A-reconstructing,*
2. *For all $s \in S \setminus \{0\}$ there exists no element $c = (s, c_1, \dots, c_n) \in C$ such that $\pi_A(c) = 0$.*
3. *There exists a linear function $\phi_A : K^r \to S$, such that for all $c \in C$, $\pi_0(c) = \phi_A \circ \pi_A(c)$. That is, the following diagram commutes.*



Proof. We will prove *1* $\Rightarrow$ *3*, *3* $\Rightarrow$ *2* and then *2* $\Rightarrow$ *1*.

1 $\Rightarrow$ *3*: By the property of A-reconstruction, we know that for any $c \in C$ such that $\pi_A(c) = 0_A$, its secret must be zero too $\pi_0(c) = 0_S$. Linearity of C and of the function π_A now imply that for any two $c, c' \in C$ that have the same A-coordinates, $\pi_A(c) = \pi_A(c')$, their secrets must be identical: $\pi_0(c) = \pi_0(c')$.

This means that we can define the function $\phi'_A : \mathrm{Im}(\pi_A|_C) \to S$, that maps $\bar{c} \in \mathrm{Im}(\pi_A|_C)$ to s_c. Where we take $s_c := \pi_0(c)$ for some $c \in C$ with $\pi_A(c) = \bar{c}$. Of course, we have $\pi_0 = \phi'_A \circ \pi_A$ by construction, and we can extend ϕ'_A linearly to a function of the desired type by choosing a complement $V \subset K^r$ of $\mathrm{Im}(\pi_A|_C)$ and a linear function $\psi_A : V \to S$ from V to S and setting $\phi_A := \phi'_A + \psi_A$.

3 $\Rightarrow$ *2*: Choose a function ϕ_A that suffices the conditions of *3*, and assume towards contradiction that we have $s \in S \setminus \{0\}$ and $c \in C$ such that $\pi_0(c) = s$ and $\pi_A(c) = 0$.

For this c we know by means of the commutative diagram, and linearity of ϕ_A, that $s = \pi_0(c) = \phi_A \circ \pi_A(c) = \phi_A(0) = 0$. However, $s \neq 0$ by assumption. $\lightning$

2 $\Rightarrow$ *1*: Restating *1* in terms of elements, we get for all $c \in C$: $c \in \ker(\pi_A) \Rightarrow c \in \ker(\pi_0)$, which we need to prove. Assume we have a $c \in C$ such that $c \in \ker(\pi_A)$. Then we know that there cannot be a non-zero $s \in S$ such that $\pi_0(c) = s$ because that would contradict *2*, there would not exist such $c \in C$. Hence, there either exist no such c at all (which does not even happen as $0 \in C$), or all such c suffice $\pi_0(c) = 0$. Both cases imply *1*.

□

The third of these equivalent statements visualises the reconstruction that we spoke about earlier in the sense that, 'if you know the shares of A, you know the secret', through the reconstruction function ϕ_A.

Remark. A-reconstruction for an n-code C implies that for any subset $C' \subseteq C$ the 'reconstruction property', $\ker(\pi_A) \cap C' \subseteq \ker(\pi_0)$, holds. Hence, if C' is also an n-code, it has A-reconstruction. Also, if C is A-reconstructing, then for any subset $A' \subseteq \{1, \ldots, n\}$ that contains A, C is A'-reconstructing.

Definition 2.6 (r-Reconstruction)**.** Let $C \subseteq S \times K^n$ be an n-code for S over K, and let $r \in \mathbb{N}$ be a number such that $1 \leq r \leq n$. We say that C is *r-reconstructing*, or that C has the property of r-reconstruction, if for all subsets $A \subseteq \{1, \ldots, n\}$ of cardinality r, C is A-reconstructing.

Definition 2.7 (A-Privacy)**.** Let $C \subseteq S \times K^n$ be an n-code for S over K, and let $A \subseteq \{1, \ldots, n\}$ be a set of coordinates. We say that C is *A-private*, or that C has the property of A-privacy, if the projection function $\pi_{\{0\} \cup A} : C \longrightarrow S \times \pi_A(C)$ is surjective.

Note that for A-privacy it does not have to hold that the image of the projection is of dimension $t := \#A$.

Lemma 2.8. *Let C be an n-code for S over K and let A be a subset of $\{1, \ldots, n\}$. Then the following two statements are equivalent:*

1. *C has A-privacy,*
2. *For all $s \in S$ there exists an element $c = (s, c_1, \ldots, c_n) \in C$ such that $\pi_A(c) = 0$.*

Proof. The implication $1 \Rightarrow 2$ is trivial; As $\pi_A(C)$ is a linear subspace of $K^{\#A}$ it contains 0_A. By A-privacy, projection onto $S \times \pi_A(C)$ is surjective and the pre-images of $(s, 0_A)$ suffice.
For $2 \Rightarrow 1$ take an element $v = (s, v_A) \in S \times \pi_A(C)$, and a $c \in C$ such that $\pi_A(c) = v_A$. Write $c = (x, c_1, \ldots, c_n)$ for some $x \in S$ and pick by assumption existing elements $f, g \in C$ such that $\pi_0(f) = s$, $\pi_0(g) = x$ and they have zeroes in all coordinates of A, $\pi_A(f) = \pi_A(g) = 0_A$. Because of linearity, $c' := c + f - g$ is an element of C and it has s as its secret, $\pi_0(c') = x - x + s = s$.
Adding or subtracting f and g from c will not change the value of the projection onto the A coordinate because both f and g are zero on A, therefore $\pi_A(c') = \pi_A(c)$. Hence we have found an element mapping to $v \in S \times \pi_A(C)$, which concludes the proof. □

To see that A-privacy in some sense is the opposite of A-reconstruction, compare item 2 of Lemma 2.5 and Lemma 2.8.

Definition 2.9 (t-Privacy)**.** Let $C \subseteq S \times K^n$ be an n-code for S over K, and let $t \in \mathbb{N}$ be a number such that $0 \leq t \leq n$. We say that C is *t-private*, or that C has the property of t-privacy, if for all subsets $A \subseteq \{1, \ldots, n\}$ of cardinality t, C has A-privacy.

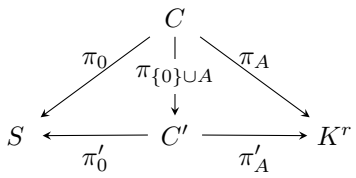
One can check that by this definition any n-code has 0-privacy. The property of $\emptyset$-privacy follows from property 1 in definition 2.3.
Note that if C has A-privacy, then for any subset $A' \subseteq A$, C has A'-privacy.

Lemma 2.10. *Let $C \subseteq S \times K^n$ be an n-code for S over K of length n that has r-reconstruction and t-privacy for some r and t in $\{0, \ldots, n\}$. Then the following statements hold:*

1. *For all $r' \in \{r, \ldots, n\}$, C has r'-reconstruction;*
2. *For all $t' \in \{0, \ldots, t\}$, C has t'-privacy;*
3. $0 \leq t < r \leq n$;
4. $\dim_K(S) \leq r$.

We will only prove the last statement, the first three should be easy to deduct from the theory above.

Proof. Suppose that $C \subseteq S \times K^n$ is an n-code for S over K, with r-reconstruction for some positive integer $r < \dim_K(S)$. We choose a set $A \subseteq \{1, \ldots, n\}$ of size r. Take the image of $\pi_{\{0\} \cup A}|_C$ and denote it as C'. The function $\pi_A : C \to K^r$ factors through $\pi'_A : C' \to K^r$, and we similarly get $\pi'_0 : C' \to S$. A summary is made compactly in the commutative diagram below.



By A-reconstruction of C, any $x \in \ker(\pi_A) \cap C$ must be in the kernel $\ker(\pi_0)$. We see that the kernel of π'_A is trivial and thus find that π'_A is injective.
On the other hand, we already had the surjection $\pi_0 : C \to S$, which also factors through $\pi'_0 : C' \to S$. As the diagram commutes, we have the identity $\pi_0 = \pi'_0 \circ \pi_{\{0\} \cup A}$, and since π_0 is surjective, π'_0 must be surjective too. All these sets are finite dimensional and all the functions K-linear, so we arrive at the contradiction:

$$r < \dim_K(S) \leq \dim_K(C') \leq \dim_K(K^r) = r \quad \lightning .$$

□

Definition 2.11. Let S be an algebra over a field K, $C \subseteq S$ any subset and $d \in \mathbb{N}$. We define a linear subset C^{*d} defined as:

$$C^{*d} := Span_K \left(\left\{ \prod_{i=1}^{d} x_i | x_i \in C \right\} \right).$$

Where $Span_K(X)$ denotes the smallest K-linear subspace of S containing X.

We will often call a product of d elements of an n-code C a *d-product* for short.

Definition 2.12 ((n, t, d, r)-Codex)**.** Let S be a finite algebra over a finite field K such that multiplication in S is commutative. Pick natural numbers $n, t, d, r \in \mathbb{N}$ such that n and d are positive and suppose that we have an n-code $C \subseteq S \times K^n$ for S over K. (So in particular, we have $0 \leq t < r \leq n$.) Then C is an (n, t, d, r)-*codex* for S over K if the following three properties hold:

1. C has t-privacy;
2. C^{*d} is an n-code;
3. C^{*d} has r-reconstruction.

For an (n, t, d, r)-codex C for S over K we still have defined the constant $k_C := \dim_K(S)$, as C is also an n-code for S over K. There is no distinction between k_C where C is viewed as a codex, and k_C where it is viewed as an n-code.

An (n, t, d, r)-codex is sometimes called an 'arithmetic codex' or even simply 'codex' if there is no need to specify the parameters explicitly. The notion has been introduced in slightly different form in [6], but the lemmas above should provide enough material to convince oneself of their equivalence.
The definition of (n, t, d, r)-codex encompasses several notions in cryptography and algebraic complexity theory. First an $(n, t, 1, r)$-codex C for S over K can be turned into a secret sharing scheme as follows. In order to share a secret $s \in S$, we can select uniformly at random an element $c \in C$ such that $\pi_0(c) = s$. The shares will then be the n coordinates $\pi_i(c)$. Then it is easy to see that, by t-privacy, the knowledge of only t shares gives no information about the secret. Furthermore the secret sharing scheme is linear. This means the following: Suppose that two secrets $s, s' \in S$ are shared using words $c = (s, c_1, \ldots, c_n)$ and $c' = (s', c'_1, \ldots, c'_n)$. Then by linearity of C given any $\lambda, \mu \in K$, we have $\lambda c + \mu c' \in C$. Therefore, if we apply the same fixed linear function to each share, the resulting vector consists of shares for 'the same' linear function applied to the secret (i.e. the linear function extended naturally to S).

For applications of the area of multiparty computation, it is important to consider secret sharing schemes which, in addition to linearity, enjoy other arithmetic properties that have to do with reconstruction of products of secrets given the products of the respective shares. More precisely, an $(n, t, 2, n)$-codex is a multiplicative secret sharing scheme and an $(n, t, 2, n-t)$-codex is a t-strongly multiplicative secret sharing scheme, as defined in [9].
On the other hand, the notion of $(n, 0, 2, n)$-codex is related to the bilinear complexity of an algebra S over K and has a longer history, for which we refer to [5].

2.2 Reduction lemmas

There are some lemmas that are used throughout this work. They provide a way of constructing a codex from another codex, with smaller integer parameters. As all the parameters n, t, d and r must be non-negative, it is only natural that we find bounds from these lemmas.

Lemma 2.13. *Let C be an (n, t, d, r)-codex for S over K with $d > 1$. Then C is also a codex for S over K with parameters $(n, t, d-1, r-t)$.*

Proof. First off, the set C is not changed in any way. It still is an n-code. The privacy is a property of the set C as well, so we don't need a proof for that either.
So we only nee to check if C^{*d-1} is an n-code and whether it has $(r-t)$-reconstruction.
The first axiom of n-codes is satisfied: $\pi_0(C)$ is surjective, hence, there is for any $s \in S$ an element $c_s = (s, x_1, \ldots, x_n)$ in C. In particular the element $c := c_1^{d-2} c_s \in C^{*d-1}$ has the property $\pi_0(c) = s$ because π_0 is a K-algebra morphism.
For the second axiom of n-codes we will prove that C^{*d-1} has $(r-t)$-reconstruction, as this implies it (Lemma 2.10).
Let $A \subset \{1, \ldots, n\}$ be a set of $r-t$ coordinates, and $x \in C^{*d-1}$ such that $x \in \ker(\pi_A)$. It suffices to show that $\pi_0(x) = 0$.
Take an index set $B \subseteq \{1, \ldots, n\}$ such that B has size t and the intersection of A and B is empty. This exists because $\#(\{1, \ldots, n\} \setminus A) \geq t$.
Since C has t-privacy, there exists an element $c \in C$ such that $\pi_0(c) = 1$ and $\pi_B(c) = 0_B$.
Consider the product $c \cdot x$. This is an element of C^{*d} (since $d \geq 2$), and of $\ker(\pi_{A \cup B})$ which implies $c \cdot x \in \ker(\pi_0)$ as $\#(A \cup B) = r$ and C^{*d} has r-reconstruction. Note that by the properties of coordinatewise multiplication we get the identity: $\pi_0(c \cdot x) = \pi_0(c) \cdot \pi_0(x) = 1 \cdot \pi_0(x)$ and we thus may conclude that $\pi_0(x) = 0$ which completes the proof. □

Corollary 2.14. *Iterating Lemma 2.13 we find that an (n, t, d, r)-codex C for S over K is also an $(n, t, 1, r-(d-1)t)$-codex for S over K.*

Corollary 2.15. *As for any (n, t, d, r)-codex for S over K the reconstruction parameter must be larger than $k := dim_K(S)$ by Lemma 2.10 (C^{*d} is an n-code). Hence, from 2.14 we also find:*

$$r \geq k + (d-1)t.$$

Lemma 2.16 (Shortening)**.** *Let C be an n-code for S over K with and r-reconstruction and t-privacy such that $t \geq 1$. Then the set*

$$C' := \pi_{\{0,\ldots,n-1\}}(C \cap \ker(\pi_n))$$

is an $(n-1)$-code with $(r-1)$-reconstruction and $(t-1)$-privacy. That is: If C is an $(n,t,1,r)$-codex for S over K with $t \geq 1$, then C' is an $(n-1,t-1,1,r-1)$-codex for S over K.

Proof. This is a proposition based on the concept known as shortening in coding theory. The idea is to eliminate one coordinate from the n-code by restricting the n-code to those elements with a zero in the last coordinate and then 'removing' this coordinate.
With this in mind consider the subset of C with the n-th coordinate zero, $C \cap \ker(\pi_n)$. Now cut out the n-th coordinate completely to get to the set of which we will soon see it is the desired $(n-1)$-code: $C' := \pi_{\{0,\ldots,n-1\}}(C \cap \ker(\pi_n))$.
Let's check this in detail:

> Axiom 1 of the definition of n-codes is not harmed by this. Let $s \in S$ be a secret, then since privacy is large enough, $t \geq 1$, there exists an element $c \in C$ such that $\pi_0(c) = s$ and $\pi_n(c) = 0$. Hence, $\pi_{\{0,\ldots,n-1\}}(c)$ is an element of C' that has s as zero-th coordinate.
>
> $(t-1)$-privacy: Let $A \subseteq \{1 \ldots, n-1\}$ be a set of size $t-1$ and pick a secret $s \in S$. I will show that there is an element $(s, 0_A)$ in the set $S \times \pi_A(C')$. Note that $A \cup \{n\}$ is a set of size t. By Lemma 2.8 there exists an element $c \in C$ that has the properties $\pi_0(c) = s$ and $\pi_{A\cup\{n\}}(c) = 0$. The image $c' := \pi_{\{0,\ldots,n-1\}}(c)$ is an element of C', and by the universal property of the product and since A is a subset of $\{1, \ldots, n-1\}$ we have: $s = \pi_{\{0\}}(c) = \pi_{\{0\}}(\pi_{\{0,\ldots,n-1\}}(c)) = \pi_{\{0\}}(c')$, and $0_A = \pi_A(c) = \pi_A(\pi_{\{1,\ldots,n-1\}}(c)) = \pi_A(c')$, and which is what was to be shown.
>
> $(r-1)$-reconstruction: This follows similarly, now by contradiction. Suppose $A \subseteq \{1, \ldots, n-1\}$ is a set of size $r-1$, and C' is not $(r-1)$-reconstructing. By lemma 2.5 this means there is s, an element of $S \setminus \{0\}$, and $c' \in C'$ such that $\pi_A(c) = 0$ while $\pi_0(c) = s$. By our construction there must exist an element $c \in C$ with the property that $\pi_n(c) = 0$ and $\pi_{\{0,\ldots,n-1\}}(c) = c'$. This element c has zeroes in the set $A \cup \{n\}$ of size r, hence $\pi_0(c) = 0$ holds by r-reconstruction of C. We must conclude that $\pi_0(c') = 0$, which contradicts the assumption and proves the claim. $\lightning$.

Note that $(r-1)$-reconstruction implies the second axiom of n-codes to finish the proof. □

Corollary 2.17 (Shortening)**.** *Let C be an (n,t,d,r)-codex for S over K where $t \geq 1$. Then we can construct another codex C' for S over K with parameters $(n-1, t-1, d, r-1)$.*

Proof. First of all note that both C and C^{*d} are n-codes. Define C' as in 2.16 and $(C^{*d})'$ similarly. The $(t-1)$-privacy for C' thus follows directly from the shortening lemma. The $(r-1)$-reconstruction of $(C')^{*d}$ follows from this lemma too, since $(C')^{*d} \subseteq (C^{*d})'$. (See note after definition of A-reconstruction.)

To justify the inclusion $(C')^{*d} \subseteq (C^{*d})'$ we argue: An element of $(C')^{*d}$ is the sum of a number of scaled d-products $\sum_{i=1}^{m} \lambda_i \pi(x_{i1}) \cdot \ldots \cdot \pi(x_{id})$, for which all of the x_{ij} lie in $C \cap \ker(\pi_n)$ and $\lambda_i \in K$, and where π is shorthand for $\pi_{\{1,\ldots,n\}}$. We can write this more compact because of the identity $\pi(ab) = \pi(a)\pi(b)$; $\sum_{i=1}^{m} \lambda_i \pi(x_{i1} \cdot \ldots \cdot x_{id})$.
On the other hand, the elements of $(C^{*d})'$ look exactly the same, but have the weaker condition that each d-product lies in the kernel: $x_{i1} \cdot \ldots \cdot x_{id} \in C \cap \ker(\pi_n)$. Of course, if for all j we have that the n-th coordinate is zero, $\pi_n(x_{ij}) = 0$, then the n-th coordinate of the product is zero too: $\pi_n(x_{i1} \cdot \ldots \cdot x_{id}) = 0$. Which shows that $(C')^{*d} \subseteq (C^{*d})'$. □

Corollary 2.18 (Shortening)**.** *Iterating the previous corollary we find from the (n, t, d, r)-codex C for S over K an $(n - t, 0, d, r - t)$ codex over the same field and algebra.*

Corollary 2.19. *By first applying Corollary 2.14 and then Corollary 2.18, we find that an (n, t, d, r)-codex for S over K gives rise to an $(n - t, 0, 1, r - dt)$-codex for the same algebra over the same field. Since the reconstruction parameter must be bigger than k by Lemma 2.10, we can improve the bound of Corollary 2.15 to:*

$$r \geq k + dt.$$

3 Examples

In this section some basic constructions are provided for the reader to get accommodated with the codex. The first example is a somewhat degenerate case, but a codex nonetheless.

Example 3.1 (Diagonal embedding)**.** In most cases an object that in some sense is trivial can provide for useful intuition and counterexamples. One can take any finite field K and embed this into the n-fold cartesian product for some positive $n \in \mathbb{N}$.

$$\Delta := \{ (x, \ldots, x) \mid x \in K \} \subseteq K \times K^n$$

This set is an n-code with only 0-privacy as its dimension is 1. The set is closed under coordinatewise multiplication. Even stronger: For any $d \in \mathbb{N}$, with $d \geq 1$, we have $\Delta = \Delta^{*d}$. Since Δ has obvious 1-reconstruction, this construction provides an $(n, 0, d, r)$-codex for K over K for any choice of positive n, d and r with $r \leq n$.

For the next example we introduce the notation $K[X]_{\leq m}$, being the set of polynomials in one variable of degree at most m over a field K.

Theorem 3.1 (Lagrange interpolation)**.** *Let K be a field and $p_0, \ldots, p_m \in K$ a set of distinct points, then the evaluation map*

$$\phi : K[X]_{\leq m} \longrightarrow K^{m+1}, f \longmapsto (f(p_i))_{i=0}^{m}$$

is a K-linear isomorphism.

We will not prove the theorem here. It is left as an exercise in [13, par. 12]. The interested reader can find all ingredients for the proof in this dictate.

Example 3.2 (Lagrange interpolation codex)**.** Suppose that K is a finite field and $\overline{K}$ a fixed algebraic closure of K. Let $P = \{p_1, \ldots, p_n\} \subseteq \overline{K}$ be an indexed set of n distinct points. Then we define a set:

$$C_m(P) := \{(f(p_i))_{i=1}^{n} | f \in K[X]_{\leq m}\} \subseteq \prod_{i=1}^{n} K(p_i).$$

We will use that this set is the image of the natural projection:

$$ev_P : K[X]_{\leq m} \to \prod_{i=1}^{n} K[X]/(X - p_i),$$
$$f \mapsto (f \mod (X - p_1), \ldots, f \mod (X - p_n))$$

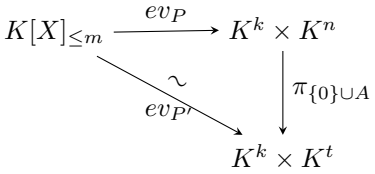
Where the subscript P is left out if it is clear from the context.

Theorem 3.2. *Let K be a finite field, $n, t, d, k \in \mathbb{N}$ natural numbers such that n, d, and k are positive, K has at least $k + n$ elements, and the inequality $d(t + k - 1) + 1 \leq n$ holds. Then there exists an $(n, t, d, d(t + k - 1) + 1)$-codex for K^k over K.*

Proof. Let n, t, d, k, K, be as in the theorem and define $r := d(t + k - 1) + 1$. We can choose $n + k$ distinct points in K, $P = \{p_{01}, \ldots, p_{0k}, p_1, \ldots, p_n\} \subseteq K$ and we will show that $C := C_{t+k-1}(P)$ is a codex with the desired properties. As usual we show that C has t-privacy, and that C^{*d} has the required r-reconstruction property. The reconstruction property needed for C to be an n-code will follow from this. Lastly, the first axiom of n-codes for C is a direct consequence of one of the diagrams below and will be noted at the appropriate spot.

t-Privacy: To prove that there is t privacy, choose a set t coordinates $A \subseteq \{1, \ldots, n\}$, and a secret $s \in K^k$. By lemma 2.8 we have to show that there is an element in $c \in C$ with $\pi_{\{0\}\cup A}(c) = (s, 0_A) \in K^k \times K^t$.

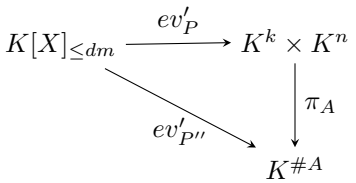
Define the set of points we need to evaluate at for the 'privacy map' $\pi_{\{0\}\cup A}|_C$, $P' := \{p_{01}, \ldots, p_{0k}\} \cup \{p_i | i \in A\}$ and write $m := k + t - 1$. Note that by the universal property of the product, the following diagram commutes:



Lagrange's theorem tells us that $ev_{P'}$ actually is an isomorphism. Therefore the polynomial $f := ev_{P'}^{-1}(s, 0_A)$ is well-defined, and its image under the evaluation in all points, $ev_P(f)$, is an element of our codex. It has the desired property because of the commutative diagram above.

The diagram also shows that the first axiom of n-codes for C holds ($\pi_0|_C$ is surjective), as we have $\pi_0|_C = \pi_0 \circ ev_P = \pi_0 \circ \pi_{\{0\}\cup A} \circ ev_P = \pi_0 \circ ev_{P'}$, and the last is a composition of two surjective functions.

r-Reconstruction: Note that the set C^{*d} is a subset of the image of the function $ev'_P : K[X]_{\leq dm} \to K^k \times K^n$ that maps a polynomial of degree less or equal to dm to its evaluation in the points of P. Pick a subset of coordinates $A \subseteq \{1, \ldots, n\}$ of at least $dm + 1$ elements and define $P'' := \{p_i | i \in A\}$. We will take a closer look at the set C^{*d} with respect to this A. As the following variation of the diagram above also commutes, any element $x \in C^{*d} \cap \ker(\pi_A)$ yields a unique $f \in {ev'_P}^{-1}(x)$ of degree $\leq dm$ for which $ev'_{P''}(f) = 0_A$ holds. (Note: By 3.2 evaluation in more than dm points must be injective and $n \geq dm + 1$ holds by assumption, so f is unique.)



Such a polynomial must have zeroes in all points of A because of the identity $ev'_{P'}(f) = ev'_P \circ \pi_A(f) = \pi_A(x) = 0_A$. The polynomial f must then be zero because a non-zero polynomial may have at most dm zeroes. Hence $x = ev'_P(f) =$

$0 \in K^k \times K^n$ for any $x \in C^{*d} \cap \ker(\pi_A)$ and so we find for any set A of size $d(k+t-1)+1$ that C^{*d} has A-reconstruction.

□

We conclude this section with some possibilities to generalize the last example. Suppose that instead of using a set of points in K, $P = \{p_{01} \ldots, p_{0k}, p_1, \ldots, p_n\} \subseteq K$, we would have chosen the points $p_{01}, \ldots, p_{0k}$ in $\overline{K}$, such that each two distinct p_{0i} p_{0j} that both not lie in K are not Galois conjugate and the last points $p_1, \ldots, p_n$ lie in K. Then if we properly generalize the Lagrange interpolation theorem, and increase the reconstruction parameter (to $dt + d[\sum_{i=1}^{k} \dim_K(K(p_{0i}))] + 1$) this again yields a codex along the same line of argument, this time for the algebra that is the product of the finite extension fields $K(p_{0i})$ over K. Moreover, all the points p_{0i} that do not lie in K, do not count for the restriction on the size of K. That is, we must only have $\#K \geq \#\{i | p_{0i} \in K\} + n$, instead of $\#K \geq k + n$.
Another way to circumvent the problem of having too few points that works for any of the Lagrange interpolation polynomial based codices, is to add a 'point at infinity'. Its evaluation map will be the defined as

$$ev_\infty : K[X]_{\leq m} \to K \qquad \sum_{i=0}^{m} a_i X^i \longmapsto a_m.$$

Lastly we cannot leave unnoticed that one can generalize the Lagrange interpolation codex to algebras other than fields like $S = K[X]/(f)$ for any $f \in K[X]$ that does not vanish at any of the evaluation points. To do so, we can use the exact same approach as in 3.2, but we will need a stronger version of Theorem 3.1 to assure that the isomorphisms $ev_{P'}$ exists. (The Chinese remainder theorem for commutative rings will be sufficient to cover at least the case of S.) Unfortunately, we cannot go into further detail.

4 Bounds based on the theory of linear Codes

By constructing a subspace of a finite vector space from a codex a vast amount of theorems of coding theory can be accessed in the context of codices. In this section we will establish this relationship.
First of all, there is need for a formal definition of linear codes. A more extensive introduction on this topic can be found in [11].

Definition 4.1 (Linear Code)**.** Let $p \in \mathbb{N}$ be a prime number, m a positive integer. Take q to be equal to p^m and $K = \mathbb{F}_q$ the field of p^m elements. The we call $C \subseteq K^n$ a *linear code of length n over K* if it is a K-linear subspace of the vectorspace K^n for an $n \in \mathbb{N}$.

The theory of linear codes makes extensive use of a distance measure called the 'Hamming distance'. We'll have to use this concept to get our bounds.

Definition 4.2 (Hamming weight)**.** Let $V = \mathbb{F}_q^n$ be a finite vectorspace. For an element $x \in V$ we define the *Hamming weight* (often just weight if not ambiguous) as:

$$w(x) := \#\{i | x_i \neq 0\}.$$

Definition 4.3. For two elements x and y of the vectorspace $V = \mathbb{F}_q^n$, the *distance* of the two elements as:

$$d(x, y) := w(x - y).$$

It is easily checked that this indeed is a metric on V. Note that V becomes a discrete topological space with regards to this metric, as the image of d is discrete. There are however other aspects of the metric just defined that are interesting. Such as:

Definition 4.4. Let $C \subseteq \mathbb{F}_q^n$ be a linear code. We define the *diameter of C* as:

$$d(C) := \min\{d(x, y) | x, y \in C \text{ with } x \neq y\}.$$

Note that this is equivalent to:

$$d(C) = \min\{w(c) | c \in C \setminus \{0\}\},$$

since C is linear.
Now let's state some theorems from coding theory that we will be able to harvest soon. All of these can be found in [11].

Theorem 4.5 (Singleton bound)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Then we have the following bound:*

$$n \geq k + d(C) - 1.$$

Theorem 4.6 (Griesmer bound)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Then we have the following bound:*

$$n \geq \sum_{i=1}^{k-1} \left\lceil \frac{d(C)}{q^i} \right\rceil.$$

Theorem 4.7 (Plotkin bound)**.** *Let $C \subseteq \mathbb{F}_q^n$ be a linear code of dimension k, such that $d(C) > n(q-1)/q$. Then we have the following bound:*

$$q^k \leq \frac{d(C)}{d(C) - \frac{q-1}{q}n}.$$

The theorem that translates a codex into a linear code is as follows:

Theorem 4.8. *Let C be an $(n, t, 1, r)$-codex for S over $K := \mathbb{F}_q$. Then there exists a linear code C' of length n over K of dimension $\dim(S)$ such that $d(C') \geq n - r + 1$.*

Proof. Let $B = \{s_i\}_{i=1}^k$ be a basis for S over K. Because of the property $\pi_0(C) = S$, we can choose a C-representative for each s_i: $c_i = (s_i, x_i) \in C$.
The set $\{x_i\}_{i=1}^k$ must be linearly independent. Indeed, suppose that we have a non-trivial relation $\sum_{i=1}^k \lambda_i \cdot x_i = 0$ then we get a relation $\sum_{i=1}^k \lambda_i \cdot (s_i, x_i) = (s, 0_{K^n})$ and as a linear combination of elements of C, $(s, 0_{K^n})$ again lies in C. Then, by the n-reconstruction of C, $s = 0$ must hold. This means that we have the non-trivial combination $\sum_{i=1}^k \lambda_i s_i = 0_S$, which contradicts the assumption that the s_i form a basis for S over K. ↯
We have now found a linear subspace space of K^n, namely $\text{span}_K\{x_1, \cdots, x_k\}$, it has dimension k and length n. Name this linear code C' and note that we can view this as the image of the K-vectorspace isomorphism f defined by $f(s_i) = x_i$ that sends a secret to a uniquely chosen representation in K^n.
It remains to show that the diameter of C' is at least $n-r+1$. Suppose towards contradiction that $d(C') \leq n-r$. Then there exists a non-zero $x \in C' \setminus \{0\}$ such that x has weight less than or equal to $n - r$. This means that there is a set $A \subseteq \{1, \ldots, n\}$ of size r such that x has only zeroes in this set of coordinates: $\pi_A(x) = (0, \ldots, 0)$.
Now let c be an element of the original codex C such that $\pi_{\{1,\ldots,n\}}(c) = x$. This element must exist by our construction. The r-reconstruction property of C implies that $\pi_0(c) = 0$. Recall that each element in C' is a representation of only one element $s \in S$, and that since this representation system is chosen linearly, the unique element corresponding to 0_S is the zero vector. Thus we conclude that $x = 0_{K^n}$, a contradiction as x was non-zero. ↯ □

With diligence we can now translate the bounds from linear coding theory into the following theorems for codices. (Note that an (n, t, d, r)-codex is also an $(n, t, 1, r)$-codex by Lemma 2.13.)

Theorem 4.9 (Singleton bound, codex version)**.** *Let $C \subseteq S \times \mathbb{F}_q^n$ be an (n, t, d, r)-codex for S over $\mathbb{F}_q$. Then we have the following bound:*

$$r \geq \dim(S).$$

Note that we already found this bound in Lemma 2.10, through a completely different proof.

Theorem 4.10 (Griesmer bound, codex version)**.** *Let $C \subseteq S \times \mathbb{F}_q^n$ be an (n, t, d, r)-codex for S over $\mathbb{F}_q$. Then we have the following bound:*

$$n \geq \sum_{i=1}^{\dim(S)-1} \left\lceil \frac{n-r+1}{q^i} \right\rceil.$$

The Plotkin bound can be translated most easily with a little bit of analysis.

Theorem 4.11 (Plotkin bound (codex version))**.** *Let $C \subseteq S \times \mathbb{F}_q^n$ be an (n, t, d, r)-codex for S over $\mathbb{F}_q$, such that $n > q(r-1)$. Then we have the following bound:*

$$q^{k-1} \leq \frac{n-r+1}{n-q(r-1)},$$

where $k = k_C$ is the dimension of S over $\mathbb{F}_q$.

Proof. From the codex we distil a linear code $C' \subseteq \mathbb{F}_{q^k}^n$ of dimension k with diameter $d(C') \geq n-r+1$. From $n > q(r-1)$ we expand to $n-r+1 > n(q-1)/q$ to find that the inequality $d(C') > n(q-1)/q$ holds. Hence, we obtain the Plotkin bound for the linear code C':

$$q^k \leq \frac{d(C')}{d(C') - \frac{q-1}{q}n}.$$

We only need to justify that we can replace $d(C')$ with its lower bound $n-r+1$. To do so, compare the upper bound on q^k with the continuous (with respect to the usual topology) function:

$$f_a : \mathbb{R}_{>a} \to \mathbb{R}_{>0}, \qquad x \mapsto \frac{x}{x-a}$$

In which we choose a a positive real number. The derivative of f_a is negative on all of $\mathbb{R}_{>a}$, so f_a is a decreasing function. Thus we derive for all positive $a \in \mathbb{R}$ and all numbers $x, y \in \mathbb{R}_{>a}$:

$$x > y \Rightarrow \frac{x}{x-a} < \frac{y}{y-a}.$$

The conclusion now follows immediately, after tidying up the inequality. □

The theorems that we have obtained now are not the strongest possible, since we haven't used the parameters t and d of an (n, t, d, r)-codex yet. Certainly Corollary 2.19 can improve the bounds a bit. We show what this does for the Griesmer bound. Also, note that these bounds make no use of the multiplicative structure of S. We'll arrive at those in the next section.

Theorem 4.12 (Griesmer bound, codex version, enhanced)**.** *Let $C \subseteq S \times \mathbb{F}_q^n$ be an (n, t, d, r)-codex for S over $\mathbb{F}_q$. Then we have the following bound:*

$$n \geq \sum_{i=1}^{\dim(S)-1} \left\lceil \frac{n-r+dt+1}{q^i} \right\rceil.$$

Note that the only information on the algebra S that the results in this section use is its dimension k. In the next section we will see some results that have a stronger dependence on the structure of the algebra. Finally, note that if $\dim(S) = 1$, the results of this section become trivial. However, in [7], the following restriction was proved, using also arguments from code theory in a slightly different way.

Theorem 4.13. *Let $C \subseteq S \times \mathbb{F}_q^n$ be an (n, t, d, r)-codex for S over $\mathbb{F}_q$. Then we have the following bound:*

$$r - t \geq \frac{n - t + 1}{q}.$$

5 Algebra dependent bounds

In this section we arrive at the main result that were proved in the course of the project. There was a bound known for finite fields. In particular, the following theorem was known (albeit unpublished).

Theorem 5.1. *Let $C \subseteq F \times K^n$ be an (n, t, d, r)-codex for F over K, where F is a finite field extension of K. Then we have the following inequality:*

$$n \geq dk - d + 1.$$

5.1 Local rings

The theorem we will prove here has the same conclusion under the weaker condition that F need just be a local ring that is an algebra over K. A bound for a non-local rings has also been found with the same proof, although the bound in this case is not very tight and above all hard to compute. The last section will show this by yet a stronger generalisation which holds for any codex over any algebra. To get to this point, we start off with some lemmas.

Lemma 5.2. *Let $C \subseteq S \times K^n$ be an (n, t, d, r)-codex for S over K. Then there exists a K-linear injective function $\sigma : S \to K^n$ such that for any $s \in S$ we have $(s, \sigma(s)) \in C$.*

Proof. Choose a basis $s_1, \ldots, s_k$ for S over K and pick elements $c_i = (s_i, x_i) \in C$ for some $x_i \in K^n$. These must exist because $\pi_0(C) = S$ by definition. Define the function $\sigma : S \to K^n$ by K-linearly extending $s_i \mapsto x_i$. We write s on the chosen basis $s = \lambda_1 s_1 + \ldots + \lambda_k s_k$ for some $\lambda_i \in K$ and we see that by linearity: $\sigma(s) = \lambda_1 x_1 + \ldots + \lambda_k x_k$. This way we found the first needed property, $(s, \sigma(s)) = (\lambda_1 s_1 + \ldots + \lambda_k s_k, \lambda_1 x_1 + \ldots + \lambda_k x_k) = \lambda_1 c_1 + \ldots + \lambda_k c_k \in C$, for any $s \in S$, by linearity of C.
To see that σ is injective, suppose that we have some $s \in \ker(\sigma)$. Then, we have $(s, \sigma(s)) \in C$ and by n-reconstruction of C, it follows that $(s, \sigma(s)) \in \ker(\pi_0)$. Indeed, the kernel of σ is trivial. □

Definition 5.3. A function $\sigma : S \to K^n$ such as in Lemma 5.2 will be called a *generator* for C.

Lemma 5.4. *Let S be a K-algebra over a field K, and $\sigma : S \to K^n$ be an injective K-linear function. Then there exists a basis $b_1, \ldots, b_k$ for S such that all $\sigma(b_i)$ have weight $\leq n - k + 1$.*

Proof. The image of σ has dimension k, equal to $\dim(S)$. Take any basis for $\sigma(S)$ and use Gaussian elimination to construct a basis $\{b_i'\}$ that is in normal (row echelon) form. Clearly, these vectors each have weight $\leq n - k + 1$. Their inverses under σ form a basis for S that meets the restriction we claimed. □

The next proposition is isolated from the proof of the theorem to improve its natural flow. It has a rather technical and long proof although it seems only reasonable to expect such a statement to be true a priori.

Proposition 5.5. *Suppose that $C \subseteq S \times K^n$ is an (n, t, d, r)-codex for S over K, and that $\sigma : S \to K^n$ is a generator for C. Take $x_1, \ldots, x_{d-1} \in S$, and define*

$$R := \{\sigma(x_1) \ldots \sigma(x_{d-1})\sigma(y) | y \in S\}.$$

Then there exists an injective linear function $f : x_1 \ldots x_{d-1}S \to R$.

Proof. First note that it is enough to prove that there exists a surjective linear function $g : R \to S$ whose image contains $x_1 \ldots x_{d-1}S$. One can extract a function as above from this easily.
Since σ is a generator, all the vectors $(s, \sigma(s))$ lie in C. In the set R we can thus only find products of d elements of $\pi_{\{1\ldots,n\}}(C)$. This gives the inclusion $R \subseteq \pi_{\{1,\ldots,n\}}(C^{*d})$. We'll define the function

$$i : R \longrightarrow C^{*d}, \qquad u \longmapsto (s_u, u)$$

that sends an element in $u \in R$ to the unique element $i(u) \in C^{*d}$ that has the property: $(\pi_{\{1\ldots,n\}} \circ i)(u) = u$.
Firstly, such an element exists for every $u = \sigma(x_1) \ldots \sigma(x_{d-1})\sigma(y) \in R$, namely $(x_1 \ldots x_{d-1}y, r)$. And secondly, this is well defined because of the reconstruction property for C^{*d}: We know that there cannot be two elements in $a, b \in C^{*d}$ such that $\pi_{\{1,\ldots,n\}}(a) = \pi_{\{1,\ldots,n\}}(b)$ and $\pi_0(a) \neq \pi_0(b)$. If this was the case, we would have $a - b \in C^{*d}$ with $\pi_0(a - b) \neq 0$ and $\pi_{\{1,\ldots,n\}} = 0$, which contradicts Lemma 2.5 as C^{*d} has n-reconstruction.
The function i must be linear because its right-inverse function $(\pi_{\{1,\ldots,n\}})$ is a linear function. So if we compose i with $\pi_0 : C^{*d} \to S$, we still have a linear function.
The image of $\pi_0 \circ i$ indeed contains $x_1 \ldots x_{d-1}S$. Any element $x_1 \ldots x_{d-1}s \in x_1 \ldots x_{d-1}S$, is mapped onto by $\sigma(x_1) \ldots \sigma(x_{d-1})\sigma(s)$. Hence, with $g := \pi_0 \circ i : R \to S$ we can construct the function we seek. □

The last ingredient of the theorems proof is a rephrasing of the concept of a local ring.

Lemma 5.6. *Let S be a finite algebra over a finite field K. Then the following statements are equivalent:*

1. *S is a local ring. That is, there exists a unique maximal ideal $\mathfrak{m} \subseteq S$.*
2. *The ideal generated by the set of non-units $S \setminus S^\times$, I, is not equal to S.*

Proof. We break the proof into the usual parts:

(1) ⇒ (2) We show that $\mathfrak{m} = I$. Firstly, $\mathfrak{m} \subseteq I$ holds because $\mathfrak{m} \neq S$ and thus cannot contain a unit. For the inclusion $I \subseteq \mathfrak{m}$, suppose that we have an element $x \in I$ such that $x \notin \mathfrak{m}$. Then, x is contained in some maximal ideal $\mathfrak{m}_x$, because x is not a unit. Obviously these two cannot be the same, $\mathfrak{m} \neq \mathfrak{m}_x$. However, this contradicts the fact that S only has one maximal ideal. So indeed, $I \subseteq \mathfrak{m}$. If we would not have elements in $I \setminus \mathfrak{m}$ then of course every element $x \in I$ is an element of $\mathfrak{m}$ and we are done immediately. Now the inclusion hold both ways, hence $I = \mathfrak{m}$.

(1) $\Leftarrow$ (2) The ideal I must be maximal as every ideal strictly containing it must contain a unit. Also, every ideal not equal to S consists of only non-units, and hence is a subset of I. Clearly this implies that I is the unique maximal ideal of S.

□

With all our instruments at the ready, we can now start with the first generalisation of Theorem 5.1.

Theorem 5.7. *Let $C \subseteq S \times K^n$ be an (n, t, d, r)-codex for S over K, then there exist elements $x_1, \ldots, x_{d-1} \in S \setminus \{0\}$, together with $x_0 := 1 \in S$ such that the following inequality holds:*

$$n \geq 1 - d + \sum_{i=0}^{d-1} \dim(x_0 \ldots x_i S)$$

Moreover, if S is local when considered as a ring, the x_i can be chosen unitary. We get the bound

$$n \geq dk - d + 1$$

for these algebras.

Proof. Choose a linear function $\sigma : S \to K^n$ that sends a secret $s \in S$ to a representation $\sigma(s)$, i.e. $(s, \sigma(s)) \in C$ must hold for all $s \in S$ (Lemma 5.2).
Claim: If $m \leq d - 1$ there exist elements $x_1, \ldots, x_m \in S$ such that for all $i \in \{1, \ldots, m\}$:

$$\delta_i \leq n + i - \sum_{j=0}^{i-1} \dim(x_0 \ldots x_j S)$$

Where we define $x_0 = 1 \in S$, and $\delta_i := w(\sigma(x_0) * \ldots * \sigma(x_i))$.
If $m = 0$, this statement is trivial.
Induction hypothesis: Suppose that the claim is true for some non-negative $m = M \leq d - 2$. That is to say: We have elements $x_1, \ldots, x_M \in S \setminus \{0\}$ for which the inequalities above hold.
We consider the K-linear subspace $R_{M+1} := \{\sigma(x_1) * \ldots * \sigma(x_M) * \sigma(y) | y \in S\} \subseteq K^n$. By Lemma 2.13 and Lemma 2.10, C is also an $(n, t, M + 1, r)$-codex, of which we know that there must exist a linear injection $\sigma_{M+1} : x_1 \ldots x_M S \to R_{M+1}$ (Lemma 5.5).
The injection $\sigma_{M+1} : x_1 \ldots x_M S \to R_{M+1}$ finds us the inequality:

$$\dim(R_{M+1}) \geq \dim(x_0 \ldots x_M S).$$

On the other side, we can project R_{M+1} linearly and injectively into K^{δ_M} because for all $y \in S$, the support of a product $\sigma(x_1) * \ldots * \sigma(x_M) * \sigma(y)$ is contained in the support of $\sigma(x_1) * \ldots * \sigma(x_M)$.
We are now in the position to invoke Lemma 5.4, from which we get an element $r \in R_{M+1}$, that looks like $r := \sigma(x_1) * \ldots * \sigma(x_{M+1})$ for some $x_{M+1} \in S \setminus \{0\}$. By Theorem 4.9 it satisfies the relation:

$$w(r) =: \delta_{M+1} \leq \delta_M - \dim(x_0 \ldots x_M S) + 1,$$

since $\dim(R_{M+1}) \geq \dim(x_0 \dots x_M S)$. By induction hypothesis, this can be made explicit:

$$\begin{aligned}
\delta_{M+1} &\leq \delta_M - \dim(x_0 \dots x_M S) + 1 \\
&\overset{i.h.}{\leq} n + M - \sum_{j=0}^{M-1} [\dim(x_0 \dots x_j S)] - \dim(x_0 \dots x_M S) + 1 \\
&= n + (M+1) - \sum_{j=0}^{M} \dim(x_0 \dots x_j S)
\end{aligned}$$

This concludes the induction and the proof of the claim. But note that we can squeeze out one last lower bound for δ_{d-1}. Because, $\sigma_d : x_1 \dots x_{d-1} S \to R_d$ must still be injective along the same argument as before. We find:

$$\dim(x_0 \dots x_{d-1} S) \leq \delta_{d-1} \leq n + (d-1) - \sum_{j=0}^{d-2} \dim(x_0 \dots x_j S)$$

or equivalently:

$$n \geq 1 - d + \sum_{i=0}^{d-1} \dim(x_0 \dots x_i S).$$

Lastly, for the case S being local. We strengthen the induction hypothesis by adding: $x_0 \dots x_i S = S$ for any $i \leq m$, and note in the induction step that we can choose $x_{M+1} \in S$ a unit. Indeed, the injection σ_{M+1} is by induction hypothesis simply an injective linear function $S \to K^{\delta_{M+1}}$, such that by Lemma 5.4 we have a complete basis for S from which we can choose x_{M+1}. All of these base vectors b_i have an image under σ such that the product $\sigma(x_0) \dots \sigma(x_M)\sigma(b_i)$ has a weight that is smaller than $\delta_M - \dim(x_0 \dots x_M S) + 1$. By noting that any basis for S must contain a unit (because of Lemma 5.6) we can conclude that $x_0 \dots x_{M+1} S = S$. The rest of the proof follows verbatim. The conclusion follows by harvesting the extra constriction in the induction hypothesis:

$$\sum_{j=0}^{d-1} \dim(x_0 \dots x_j S) = d \cdot \dim(S).$$

□

5.2 The general case

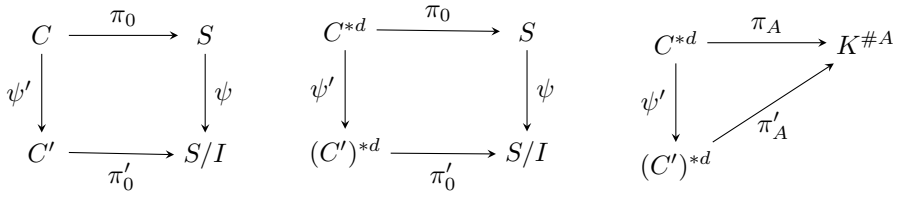
In the same way that we can reduce the integer parameters of a codex under some condition, we will show how to 'reduce' the algebra S. This enables us to retrieve bounds for general algebras from bounds for codices with an algebra of specific type.

Lemma 5.8. *Let $C \subset S \times K^n$ be an (n, t, d, r)-codex for S over K, and I an ideal of S strictly contained in S. Then the image of C under the natural projection $\psi' : S \times K^n \to (S/I) \times K^n$ is an (n, t, d, r)-codex for S/I over K.*

Proof. The proof is very similar to that of Lemma 2.16.
Define C' as the image $\psi'(C)$, abbreviate $\psi'(C^{*d})$ by $(C^{*d})'$ and then note that $(C')^{*d} = (C^{*d})'$. To see this, take $\psi'(\sum_{i=1}^{m} \lambda_i x_{i1} \dots x_{id}) \in (C^{*d})'$ and find that it is in fact an element of $(C')^{*d}$, by using the elementary properties of ψ':

$$\psi'(\sum_{i=1}^{m} \lambda_i x_{i1} \dots x_{id}) = \sum_{i=1}^{m} \lambda_i \psi'(x_{i1}) \dots \psi'(x_{id}).$$

This works both ways of course, so the equality must hold.
note that we have a commutative diagrams:



where we denote the natural morphism $S \to S/I$ by ψ and distinguish between the projection of $S \times K^n$ and that of $(S/I) \times K^n$ onto the first coordinate by denoting them $\pi_0 : C \to S$ and $\overline{\pi_0} : C' \to S/I$ respectively.
First we will prove that both the first axiom of n-codes hold for C' and $(C')^{*d}$. To do so, we need to prove that $\pi'_0|_{C'}$ and $\pi'_0|_{(C')^{*d}}$ are surjective. Let us take an $\overline{s} \in S/I$ with representative $s \mod I$ for some $s \in S$. Since C is an n-code, we have $c \in C$ such that $\pi_0(c) = s$, hence of course, $\psi \circ \pi_0(c) = \overline{s}$. $\pi'_0|_{C'}$ must then be surjective, since the first diagram tells us that:

$$\psi \circ \pi_0(c) = \pi'_0 \psi'(c) = \overline{s}$$

and the element $\psi'(c)$ lies in C'. The function $\pi'_0|_{(C')^{*d}}$ then is surjective because for every $s \in S$ we had found $c \in C'$ with $\pi'_0(c) = s$, so we have an element $w \in C'$ with $\pi'_0(w) = 1$ and $cw^{d-1} \in (C')^{*d}$ has the desired property: $\pi'_0(cw^{d-1}) = s$.
We now have to perform the same kind of reasoning to find the privacy and reconstruction properties:
t-privacy: Let $\overline{s} \in S/I$ be represented by $s \mod I$ for some $s \in S$, and suppose that $A \subseteq \{1, \dots, n\}$ is a set of size t. We need to show that there is an element $c' \in C'$ such that $\pi'_0(c') = \overline{s}$ and $\pi_A(c') = 0_A$ (Lemma 2.8). Since C is t-private, there is an element $c \in C$ such that $\pi_0(c) = s$ and $\pi_A(c) = 0_A$. Because of the first commutative diagram, we immediately find that $c' := \psi'(c)$ has the desired properties.
r-reconstruction: Suppose that $A \subseteq \{1, \dots, n\}$ is a set of size r and that we have an element $\overline{x} \in \ker(\pi'_A) \cap (C')^{*d}$ with a representative $x \mod (I \times \{0\}^n)$ for some $x \in C^{*d}$. We need to show that $\overline{x} \in \ker(\pi'_0)$. Since we have the third diagram, we know that $\pi_A(x) = 0$ must hold for the representative of $\overline{x}$. From the r-reconstruction of C^{*d} now follows that $x \in \ker(\pi_0)$ and so $x \in \ker(\psi \circ \pi_0)$. Again going back to diagram two, we know now that $x \in \ker(\pi'_0 \circ \psi')$ and thus indeed $\overline{x} = \psi'(x) \in \ker \pi'_0$ follows. Which was what was to be shown. r-Reconstruction for C' itself can be found with the help of the reduction lemma 2.13, from which the second axiom of n-codes for C' follows immediately. □

Theorem 5.9. *Let $C \subseteq S \times K^n$ be an (n, t, d, r)-codex for S over K and define the constant*

$$M := \max\{\dim_K(S/I) \mid I \subseteq S \text{ an ideal such that } I \neq S \text{ and } S/I \text{ is local }\}.$$

Then we have the inequality:

$$n \geq dM - d + 1.$$

Proof. By Lemma 5.8 we have for any ideal $I \subseteq S$ an (n, t, d, r)-codex for S/I over K. Hence, for any ideal such that S/I is local we get the bound from Theorem 5.7:

$$n \geq d \dim_K(S/I) - d + 1.$$

The statement follows immediately from this result. □

There is a nice classification result for Artinian commutative rings [2, Thm 8.7] which paraphrases to finite rings as:

Theorem 5.10. *Let R be a finite commutative ring. Then R is isomorphic to the direct sum of a number of finite local commutative rings $R_1, \ldots, R_n$.*

$$R \cong \bigoplus_{i=1}^{n} R_i.$$

Corollary 5.11. *Let $C \subseteq S \times K^n$ be an (n, t, d, r)-codex for S over K, m the number of maximal ideals of S and k the dimension of S over K. Then the following inequality holds:*

$$n \geq d\frac{k}{m} - d + 1$$

Proof. By 5.10 we have a decomposition of S into local subrings $S_1 \oplus \ldots \oplus S_m$, where m is the number of maximal ideals of S. (Indeed, the maximal ideals are precisely the sets $m_i := S_1 \oplus \ldots \oplus \mathfrak{m}_i \oplus \ldots \oplus S_m$, where $\mathfrak{m}_i$ is the maximal ideal of S_i.) For each $i \in \{1, \ldots, m\}$ we have the ideal $I_i := \ker(\pi_{\{i\}})$ of elements that are zero in S_i and for all of these we have $S/I_i = S_i$ is local. Now note that the an ideal I for which S/I is local must be one of the of the form $S_1 \oplus \ldots \oplus S_{i-1} \oplus J_i \oplus S_{i+1} \oplus \ldots \oplus S_m$, where J_i is an ideal of S_i, because a local ring cannot be decomposed non-trivially as a direct sum of rings. (Such a ring would not have a unique maximal ideal.) Because for two ideals $A, B \subseteq S$ for which $A \subseteq B$ we have the inequality $\dim_K(S/A) \geq \dim_K(S/B)$, we conclude that $\max\{\dim_K(S/I)\}$ with S/I local must be an element of of $\{\dim_K(S/I_i)\}$. Since the maximum of a set of integers is bigger than or equal to the average of that set, the claim follows. □

Yet again, we have not exploited all parameters at once in this theorem. This time especially r and t could still be used more efficiently. Using the (not proved) fact that we can just project an (n, t, d, r)-codex $C \subseteq S \times K^n$ for S over K onto its first coordinates to get an (r, t, d, r)-codex $\pi_{\{0,\ldots,r\}}(C) \subseteq S \times K^r$ for S over K, and the reduction lemma 2.18 we create an enhancement:

Theorem 5.12. *Let $C \subseteq S \times K^n$ be an (n, t, d, r)-codex for S over K and define the constant*

$$M := \max\{\dim_K(S/I) \mid I \subseteq S \text{ an ideal such that } S/I \text{ is local}\}.$$

Then we have the inequality:

$$r - t \geq dM - d + 1.$$

5.3 Tightness of the bounds

It is important to know when we cannot improve the bounds any further. The Lagrange polynomial interpolation based codex can under some conditions match the bounds that we have stated. In particular, if we have a field K that is large enough to accommodate $k + n$ elements, where $n = d(k + t - 1) + 1$ for some chosen $d, k, t \in \mathbb{N}$ with $d, k \leq 1$, then Theorem 3.2 states that there exists an (n, t, d, n)-codex for K^k over K and in the discussion at the end of the section, we even see that we can construct similar codices over a product of extensions of K. For these codices the bound of Corollary 5.11 becomes:

$$d(t + k - 1) + 1 \geq d\frac{k}{m} - d + 1,$$

which is tight if $t = 0$ and $m = 1$. Those two restrictions are readily met when we pick the set $P = \{p_0, \ldots, p_n\}$, that was introduced in the proof of 3.2, such that $p_1, \ldots, p_n \in K$, p_0 in any algebraic extension of K and take $n = d(\dim_K(K(p_0)) - 1) + 1$. But note that K must still suffice some conditions on its size. The construction of Lagrange interpolation based codices for rings other than fields noted at the end of Section 3 can be used to find tight bounds with the same parameters. For example with the ring $K[X]/(X^k)$.

6 Prospects

The structure theorem on finite rings noted in section 5 showed some new possibilities that can be exploited. Here I would like to sketch one of these prospects. One of the problems we have been looking at near the end of the project was:

Problem. Suppose that $C \subseteq A \times B \times K^n$ is an (n, t, d, r)-codex for $A \times B$ over K and for the K-algebras A and B we know that any (n_A, t_A, d, r_A)-codex for A and any (n_B, t_B, d, r_B)-codex for B over K there are inequalities:

$$n_A \geq l_A, \qquad n_B \geq l_B$$

hold for some values $l_A, l_B \in \mathbb{N}$ (possibly depending on A and B respectively). Then under the assumption that A is a local ring, it holds that:

$$n \geq l_A + l_B.$$

If this problem can be proved, then we can generalize Theorem 5.7 in such a way that we actually retrieve a lower bound similar to the lower bound on the complexity of an algebra that is proved in [1].

Corollary 6.1 (Under the assumption above)**.** *Suppose $C \subset S \times K^n$ is an (n, t, d, r)-codex for S over K, and the problem stated is proven. Then if we define m as the number of maximal ideals of S, we find:*

$$n \geq dk - m(d-1).$$

Proof. There are $S_1, \ldots, S_m$ such that $S \cong \bigoplus_{i=1}^{n} S_i$ by the classification theorem. All these S_i are local finite algebras over K, and so for all i we know that the inequality $n_i \geq dk_i - d + 1$ holds for any (n_i, t_i, d_i, r_i)-codex for S_i over K. Hence, by iterating the statement in the problem we find:

$$n \geq dk - m(d-1).$$

Lastly one sees quickly that in a finite direct sum of m local algebras, there are precisely m maximal ideals. They are exactly the sets $S_1 \oplus \ldots \oplus \mathfrak{m}_i \oplus \ldots \oplus S_m$, where $\mathfrak{m}_i$ is the maximal ideal of S_i. □

Remark. Note that the statement of Corollary 6.1 for the case $m = 1$ is true by Theorem 5.7.

To place these results into their correct context, we would like to note that the bound:

$$n \geq 2k - 1$$

for $(n, t, 2, r)$-codices for F over K where F is an extension field of K of degree k has been know since 1977, as a result of C. Fiduccia and Y. Zalcstein [10]. A generalisation for general algebras is implied by a result by A. Adler and V. Strassen on the bilinear complexity of algebras in [1]. Their results imply:

$$n \geq 2k - m$$

where m is the number of maximal ideals of the algebra. An affirmative answer to the problem we posed above would also prove the same result and generalize it for $d \geq 2$, as we have seen in Corollary 6.1.

References

[1] A. Adler and V. Strassen. *On the algorithmic complexity of associative algebras*, volume 15. North-Holland Publishing Company, 1981.

[2] M. Atiyah and I. MacDonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Company, 1969.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proc. of STOC 1988*, pages 1–10. ACM Press, 1988.

[4] G.R. Blakley. Safeguarding cryptographic keys. In *AFIPS Conference Proceedings*, volume 48, pages 313–317, 1979.

[5] P. Bürgisser, M. Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory.* Springer, 1997.

[6] I. Cascudo, R. Cramer, and C. Xing. The arithmetic codex. In *Cryptology ePrint Archive, Report 2012/388*, 2012. `http://eprint.iacr.org/`.

[7] I. Cascudo, R. Cramer, and C. Xing. Bounds on the threshold gap in secret sharing and its applications. To appear in IEEE transactions on information theory. Preliminary version at `http://eprint.iacr.org/2012/319.` In *Cryptology ePrint Archive, Report 2012/319*, 2012.

[8] D. Chaum, C. Crépeau, and I. Damgaard. Multi-party unconditionally secure protocols. In *Proc. of STOC 1988*, pages 11–19. ACM Press, 1988.

[9] R. Cramer, I. Damgaard, and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. In *Proc. of 19th Annual IACR EUROCRYPT, Brugge, Belgium*, volume 1807, pages 316–334. Springer Verlag, 2000.

[10] C. Fiduccia and Y. Zalcstein. Algebras having linear multiplicative complexities. In *Journal of the ACM (JACM)*, volume 24 issue 2, pages 311–331, 1977.

[11] W. Cary Huffman and V. Pless. *Fundamentals of errorcorrecting codes.* Cambridge University Press, 2003.

[12] A. Shamir. How to share a secret. In *Comm. ACM*, volume 22 issue 11, pages 612–613. ACM Press, 1979.

[13] P. Stevenhagen. Algebra 2, 2010. Dictaat Universiteit Leiden.

[14] A. Yao. Protocols for secure computations. In *Proceedings of Twenty-third IEEE Symposium on Foundations of Computer Science (FOCS1982)*, pages 160–164, 1982.