Bounds on the Threshold Gap in Secret Sharing over Small Fields

Ignacio Cascudo* Ronald Cramer† Chaoping Xing‡

June 5, 2012

Abstract

We consider the class of secret sharing schemes where there is no a priori bound on the number of players n but where each of the n share-spaces has fixed cardinality q. We show two fundamental lower bounds on the *threshold gap* of such schemes. The threshold gap g is defined as $r-t$, where r is minimal and t is maximal such that the following holds: for a secret with arbitrary a priori distribution, each r-subset of players can reconstruct this secret from their joint shares without error (r-reconstruction) and the information gain about the secret is nil for each t-subset of players jointly (t-privacy). Our first bound, which is completely general, implies that if $1 \leq t < r \leq n$, then $g \geq \frac{n-t+1}{q}$ independently of the cardinality of the secret-space. Our second bound pertains to $\mathbb{F}_q$-linear schemes with secret-space $\mathbb{F}_q^k$ ($k \geq 2$). It improves the first bound when k is large enough. Concretely, it implies that $g \geq \frac{n-t+1}{q} + f(q,k,t,n)$, for some function f that is strictly positive when k is large enough. Moreover, also in the $\mathbb{F}_q$-linear case, bounds on the threshold gap *independent* of t or r are obtained by additionally employing a dualization argument. As an application of our results, we answer an open question about the asymptotics of *arithmetic secret sharing schemes* and prove that the asymptotic optimal corruption tolerance rate is strictly smaller than 1.

Keywords: Secret sharing, threshold gap, error correcting codes, Norse bounds, Griesmer bound, arithmetic secret sharing

1 Introduction

We consider the class secret sharing schemes where there is no a priori bound on the number of players n but where each of the n share-spaces (i.e., a set in which a share takes its value) has fixed cardinality q. We show two fundamental lower bounds on the *threshold gap* of such schemes. The threshold gap g is defined as $r-t$, where r is minimal and t is maximal such that the following holds: for a secret with arbitrary a priori distribution, each r-subset of players can reconstruct this secret from their joint shares without error (r-reconstruction) and the information gain about the secret is nil for each t-subset of players jointly (t-privacy).

For a given scheme, let λ^* denote average share-length (in bits), i.e., the average Shannon-entropy of the n shares. Our first lower bound states that, if $1 \leq t < r \leq n$, then

$$g \geq \frac{n-t+1}{2^{\lambda^*}},$$

independently of the cardinality of the secret-space (i.e., the set in which the secret can be selected arbitrarily). It follows at once that, in particular,

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

We stress that this result is completely general and is not restricted to, say, linear, ideal, threshold or even perfect schemes. Our proof is based on a careful inductive collision-entropy argument, where

*CWI Amsterdam, The Netherlands. Email: i.cascudo@cwi.nl

†CWI Amsterdam & Mathematical Institute, Leiden University, The Netherlands. Homepage: www.cwi.nl/∼cramer, www.math.leidenuniv.nl/∼cramer

‡Division of Mathematical Sciences, Nanyang Technological University, Singapore. Homepage: www3.ntu.edu.sg/home/xingcp/

induction is enabled by *shortening*, i.e., the process of collapsing to a convenient sub scheme by conditioning on a certain event followed by removal of some players. The key element of our collision-entropy argument is a generalization of the proof idea behind the Norse Bound on covering radius from coding theory [14]. In the $\mathbb{F}_q$- linear case the dependency on t can be removed using a dualization technique. If $1 \leq t < r \leq n-1$, this leads to the lower bound

$$g \geq \frac{n+2}{2q-1}.$$

Hence, the threshold gap is $\Omega(n)$ if q is fixed.

Our second lower bound involves the cardinality of the secret-space. We first show that if there exists an r-reconstructing, t-private secret sharing scheme whose secret-space has cardinality M, then there exists an $[n-t, M, d]$ q-ary error correcting code where $d \geq n-r+1$. As an immediate consequence, restrictions on the parameters n, t, r, q, M are obtained from known bounds on (linear) error correcting codes, such as Singleton, Plotkin, Hamming, etc. However, a particularly nice result is obtained from a suitable application of the *Griesmer bound*. This leads to a simple bound that is easy to compare with our first bound. This bound is only valid for $\mathbb{F}_q$- linear schemes, however. Concretely, for $\mathbb{F}_q$-linear schemes with secret-space $\mathbb{F}_q^k$ $(k \geq 2)$, we show that

$$g \geq \frac{n-r+1}{q} + (k-1),$$

or, equivalently,

$$g \geq \frac{n-t+1}{q} + f(q,k,n,t)$$

where

$$f(q,k,n,t) := k - 1 - \frac{n-t+1}{q(q+1)}.$$

We note that the argumentation underlying our second bound does *not* give a non-trivial result for $k=1$ (in fact, it leads to the triviality $g \geq 1$). Thus, for $k=1$ only our first bound gives a non-trivial result. Again we can remove the dependency on r using a dualization technique, thereby obtaining

$$g \geq \frac{n+2}{2q-1} + h(q,k,n)$$

where

$$h(q,k,n) := \frac{2q}{2q+1}\left(k - 1 - \frac{1}{q} \cdot \frac{n+2}{2q-1}\right).$$

This improves our first bound when the size of the secret is large enough, i.e., when

$$k > 1 + \frac{n+2}{q(2q-1)}.$$

As an application of our first bound, we answer an open question about certain *arithmetic secret sharing schemes* (see Section 5 for the definition). An $(n, t, 2, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q$ over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear secret sharing scheme where the secret is selected from $\mathbb{F}_q$ and each of the n shares is an element of $\mathbb{F}_q$. Moreover, there is t-privacy and, if one considers the "component-wise" product of any two sharings, then the product of the two respective secrets is $(n-t)$-wise uniquely determined by it. Such schemes have become a fundamental primitive in cryptographic protocol theory. Quite surprisingly, especially those with good *asymptotic* properties have recently been shown to be of great importance in the design of two-party secure protocols (see the references in [6]). It is known by algebraic geometric arguments [7, 5, 6] that if q is fixed, then there are infinite families of such schemes with n unbounded and $t = t(n)$ (as well as important variations) such that the quantity $\frac{3t}{n-1}$ tends *asymptotically* to a *positive* constant, which is the salient property. It is a very interesting open problem whether there exists a proof for these facts that *avoids* the use of advanced results from algebraic geometry, in particular, the existence of certain good infinite towers of algebraic function fields. See the references for explicit lower bounds. On the other hand, in the *non-asymptotic case*, this rate can be equal to 1 by taking suitable instantiations of Shamir's scheme. It was stated as one of the open theoretical problems in [5] to decide whether asymptotically this

rate *has* to be strictly smaller than 1 (*as a further price to be paid for "good asymptotics"*, besides the apparent necessity of algebraic-geometric machinery). We settle this open problem in the affirmative. Namely, we show that, for q fixed, $\frac{3t}{n-1} < 1-\epsilon$ for some some $\epsilon = \epsilon(q) > 0$ and for *all large enough* n. More precisely, if we let $\widehat{\tau}(q)$ denote the best possible achievable asymptotic rate, then we show that

$$\widehat{\tau}(q) \leq 1 - \frac{3q-2}{3q^2-3q+1} < 1$$

for all finite fields $\mathbb{F}_q$. We prove this result by a combination of our first threshold gap bound for linear schemes, basic properties of arithmetic secret sharing (specifically, the relationship between privacy in the scheme and reconstruction in its "square" on the one hand, and reconstruction in the scheme on the other hand), and, once again, shortening. It is interesting to note that the upper- and lower bounds on $\widehat{\tau}(q)$ are quite far apart still.

1.1 Related work

After completing an earlier version of this paper, an unpublished result by Joe Kilian and Noam Nisan [12] about *threshold secret sharing* was brought to our attention [3]. In essence, they showed that, if $r = t+1$, $t \neq 0, n-1$ and if the secret-space has at least cardinality 2, at least one of the share-spaces has cardinality $n-t+1$ or larger (independently of whether the scheme is linear or not). As it turned out, this result is in fact mentioned, albeit without proof, in the literature, e.g. in Amos Beimel's PhD.-thesis [1] (as well as in at least one other paper including the same author, such as [2]).

Although their bound does not imply any lower bounds on the threshold gap (indeed, it assumes $g = 1$ to begin with), it is relevant to our results. Their bound follows as a special case of our first bound if one substitutes $g = 1$ and interprets it as an upper bound for the average entropy of the shares. As a consequence of their bound, if c is an arbitrary constant with $0 < c < 1$ then there is a constant $c' > 0$ such that for any threshold scheme with $t < cn$, it must hold that

$$\lambda^* \geq c' \log n,$$

i.e., the shares are at least of logarithmic size. We incorporate the bound of Kilian and Nisan (Theorem 3.2 below) and, for the first time, its (original) proof with their kind permission. This will at the same time serve as a conceptual introduction to our first lower bound on the threshold gap, whose proof idea turned out to bear some similarities to theirs (yet it has to deal with a much more general scenario).

1.2 Outline of the paper

The paper is organized as follows. In Section 2 we give general definitions about (not necessarily linear or ideal) secret sharing schemes, including the notion of threshold gap. In Section 3, we state our first lower bound on the threshold gap of an arbitrary secret sharing scheme. In order to do this we first include the result and proof by Kilian and Nisan about threshold secret sharing schemes, then we generalize this bound for schemes with an arbitrary threshold gap and finally, we state in subsection 3.2 our improved bound in the case of linear secret sharing schemes. In Section 4 we state our second lower bound, which incorporates the size of the secret and is better than the bound in Section 3 when the secret is large. Finally, in Section 5 we recall the concept of arithmetic secret sharing scheme, we apply our bounds on the threshold gap from the previous sections in order to bound the parameters of such schemes, and we prove the aforementioned upper bounds on $\widehat{\tau}(q)$.

2 Formal Definition of Secret Sharing

In this section we first introduce some notation that will be useful for our purposes and then we define the notion of secret sharing scheme, first introduced in [4] and [15].

2.1 Vectors of Random Variables

DEFINITION 2.1 (VECTOR OF RANDOM VARIABLES) *A* vector of random variables *is a vector* $\mathbf{X} = (X_j)_{j\in\mathcal{I}}$ *such that the* index-set $\mathcal{I} \subset \mathbb{Z}_{\geq 0}$ *is finite and non-empty and the* X_j*'s are random variables defined on the same* finite *probability space.*

Moreover, for each $j \in \mathcal{I}$, $\mathcal{X}_j$ *is the finite* alphabet *where* X_j *takes its values.* [1] *If* $\mathbf{X}$ *is a vector of random variables,* $\mathcal{I}(\mathbf{X})$ *denotes the index-set.*

Note that $\mathbf{X}$ can be seen as the random variable with alphabet $\times_{j\in\mathcal{I}}\mathcal{X}_j$ whose probability distribution is the joint distribution of $\{X_j\}_{j\in\mathcal{I}}$.

DEFINITION 2.2 *The* support *of* $\mathbf{X}$, *denoted* $\mathrm{supp}(\mathbf{X})$, *is the set of all* $x \in \times_{j\in\mathcal{I}}\mathcal{X}_j$ *such that* $\mathrm{Prob}(\mathbf{X} = x) > 0$.

DEFINITION 2.3 *If* $A \subset \mathcal{I}$ *with* $A \neq \emptyset$, *then* $\mathbf{X}_A$ *denotes the vector of random variables* $(X_j)_{j\in A}$.

DEFINITION 2.4 (SHANNON AND COLLISION ENTROPIES) *Let* X *be a random variable which takes values in a finite alphabet* $\mathcal{X}$ *and for* $x \in \mathcal{X}$ *denote* $p(x) := Prob(X = x)$. *The* Shannon entropy *of* X *is*

$$H_1(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2(p(x)),$$

where $0\log_2 0 := 0$ *by convention. The* collision entropy *is*

$$H_2(X) = -\log_2(\sum_{x\in\mathcal{X}} p(x)^2).$$

REMARK 2.5 *By Jensen's inequality* $H_1(X) \geq H_2(X)$ *for any random variable* X *in the conditions above.*

DEFINITION 2.6 (ENCODING LENGTH) *The* average encoding length *of a vector of random variables* $\mathbf{X}$ *is defined as* $\lambda(\mathbf{X}) = \frac{1}{|\mathcal{I}|}\cdot\sum_{j\in\mathcal{I}} H_1(X_j)$, *where* H_1 *denotes the Shannon entropy.*

2.2 The Definition of Secret Sharing

DEFINITION 2.7 (SECRET SHARING) *A* secret sharing scheme Σ *is a pair* $(\mathbf{S}, i)$ *such that* $\mathbf{S}$ *is a vector of random variables with index-set* $\mathcal{I}$ *such that* $|\mathcal{I}| > 1$, $i \in \mathcal{I}$ *is the* designated index *and we have:*

- *(*Uniformity of the secret*) The* secret-space $\mathcal{S}_i$ *satisfies* $|\mathcal{S}_i| > 1$ *and*

$$H_1(S_i) = \log_2|\mathcal{S}_i|,$$

  i.e., there is a priori uncertainty about the secret S_i *and it has the uniform distribution on* $\mathcal{S}_i$.

- *(*Joint reconstruction*) Define* $\mathcal{I}^* = \mathcal{I}\setminus\{i\}$, *the* player set, *and* $\mathbf{S}^* = (S_j)_{j\in\mathcal{I}^*}$, *the* shares. *Then*

$$H_1(S_i|\mathbf{S}^*) = 0,$$

  i.e., the shares jointly determine the secret with probability 1.

We denote the cardinality of $\mathcal{I}^*$ *by* $n(\Sigma)$, *or* n *when* Σ *is clear from the context.*

DEFINITION 2.8 *The* average length of the shares *is* $\lambda^*(\Sigma) := \lambda(\mathbf{S}^*)$. *Whenever* Σ *is clear from the context we will use* λ^*.

Note that the definition allows the secret and individual shares to be in different sets, not even necessarily of the same cardinality.

[1] It is not assumed that for each $x \in \mathcal{X}_j$, $\mathrm{Prob}(X_j = x) > 0$.

DEFINITION 2.9 (RECONSTRUCTION AND PRIVACY SETS) *Let $\Sigma = (\mathbf{S}, i)$ be a secret sharing scheme with player set $\mathcal{I}^*$. Let $A \subset \mathcal{I}^*$ with $A \neq \emptyset$. Then A is a* reconstructing set *if*

$$H(S_i|\mathbf{S}_A^*) = 0, i.e.,$$

the shares of the set A jointly determine the secret with probability 1.

On the other hand, A is a privacy set *if*

$$H(S_i|\mathbf{S}_A^*) = H(S_i),$$

i.e., the a posteriori *uncertainty about the secret when given the shares for A, equals the* a priori *uncertainty about the secret (or equivalently, S_i and $\mathbf{S}_A^*$ are independent). By definition, $\emptyset$ is a privacy set.*

By information theory, $H(S_i|\mathbf{S}_A^*) = H(S_i)$ if and only if S_i, $\mathbf{S}_A^*$ are independent. Therefore, an equivalent definition of a non-empty privacy set A is that, for all $s \in \mathcal{S}_i$, the random variable $(\mathbf{S}_A^*)_{|S_i=s}$, i.e., $\mathbf{S}_A^*$ conditioned on the event $S_i = s$, has the same probability distribution as the random variable $\mathbf{S}_A^*$.

DEFINITION 2.10 (ACCESS STRUCTURE) *The* access structure $\Gamma(\Sigma)$ *consists of all reconstructing sets $A \subset \mathcal{I}^*$.*

DEFINITION 2.11 (r-RECONSTRUCTION) *Σ has r-*reconstruction *if each subset of $\mathcal{I}^*$ of cardinality at least r is an element of $\Gamma(\Sigma)$. The reconstruction threshold is the smallest r such that Σ has r-reconstruction, denoted by $r(\Sigma)$.*

Note that $\Gamma(\Sigma) \neq \emptyset$ since $\mathcal{I}^* \in \Gamma(\Sigma)$ by definition. In particular, $1 \leq r(\Sigma) \leq n(\Sigma)$. Furthermore, for all integers r with $r(\Sigma) \leq r \leq n(\Sigma)$ there is r-reconstruction.

DEFINITION 2.12 (ADVERSARY STRUCTURE) *The* adversary structure $\mathcal{A}(\Sigma)$ *consists of all privacy sets $A \subset \mathcal{I}^*$.*

DEFINITION 2.13 (t-PRIVACY) *Σ is said to have t-privacy if each subset of $\mathcal{I}^*$ of cardinality at most t is an element of $\mathcal{A}(\Sigma)$. The privacy threshold is the largest t such that Σ has t-privacy, denoted by $t(\Sigma)$.*

As before, 0-privacy means by convention that "the empty set gives no information about the secret." Since there certainly is a secret about which there is positive a priori uncertainty, this makes sense. Furthermore, $t(\Sigma) = 0$ does not necessarily mean that there are no privacy sets; it just means that there is an $i \in \mathcal{I}^*$ such that $\{i\}$ is *not* a privacy set. But the definition of secret sharing above certainly allows the "cryptographically non-interesting" case that there is no non-empty privacy set at all. However, it is useful, for technical reasons in proofs, to allow this case. Similarly, it is useful to allow $n = 1$. Note that for all integers t with $0 \leq t \leq t(\Sigma)$ there is t-privacy.

Suppose $A \neq \emptyset$ is a privacy set. Then, by definition, S_i and $\mathbf{S}_A^*$ are independent. Also by definition, the secret is uniformly randomly distributed on the secret-space $\mathcal{S}_i$, which satisfies $|\mathcal{S}_i| \geq 2$. Therefore, A is not a reconstructing set. Hence, there is the following lemma.

LEMMA 2.14 *$\mathcal{A}(\Sigma) \cap \Gamma(\Sigma) = \emptyset$. In particular, $0 \leq t(\Sigma) < r(\Sigma) \leq n$.*

One of the main parameters of interest in this work is the threshold gap.

DEFINITION 2.15 (THRESHOLD GAP) *The threshold gap of Σ is $g(\Sigma) := r(\Sigma) - t(\Sigma)$. Σ is a threshold secret sharing scheme if $g(\Sigma) = 1$.*

For the sake of notation, we will write g, r, t instead of $g(\Sigma)$, $r(\Sigma)$, $t(\Sigma)$ if Σ is clear from the context. The following straightforward lemma is often useful when proving privacy.

LEMMA 2.16 *Let $A \subset \mathcal{I}^*$ with $A \neq \emptyset$. If the distribution of $(S_i, \mathbf{S}_A^*)$ is the uniform distribution on $\mathcal{S}_i \times \mathrm{supp}(\mathbf{S}_A^*)$, then A is a privacy set.*

PROOF. Defining the uniform distribution on the Cartesian product of two given finite, non-empty sets V', V'' is the same as defining the uniform distribution on V' and, independently, the uniform distribution on V''. Indeed, for all $(v', v'') \in V' \times V''$, the following holds. First,

$$\text{Prob}(v', v'') = \frac{1}{|V'| \cdot |V''|}$$

by assumption. Second,

$$\text{Prob}(v') = \sum_{w'' \in V''} \text{Prob}(v', w'') = |V''| \cdot \frac{1}{|V'| \cdot |V''|} = \frac{1}{|V'|},$$

and

$$\text{Prob}(v'') = \sum_{w' \in V'} \text{Prob}(w', v'') = |V'| \cdot \frac{1}{|V'| \cdot |V''|} = \frac{1}{|V''|}.$$

Therefore,

$$\text{Prob}(v', v'') = \text{Prob}(v') \cdot \text{Prob}(v'').$$

Now take $V' = \text{supp}(S_i) = \mathcal{S}_i$ and $V'' = \text{supp}(\mathbf{S}_A^*)$. From the condition in the statement of the lemma it now follows that S_i, $\mathbf{S}_A^*$ are independent. △

3 A bound independent of the size of the secret

3.1 General bound

In this section we prove lower bounds for the threshold gap of a secret sharing scheme in terms of the number and average encoding length of the shares. In particular, our bound does *not* depend on the size of the *secret*. More precisely, we will prove the following theorem:

MAIN THEOREM 3.1 *Let Σ be a secret sharing scheme with $t(\Sigma) \geq 1$. Then*

$$g(\Sigma) \geq 2^{-\lambda^*(\Sigma)}(n(\Sigma) - t(\Sigma) + 1).$$

In particular, $g(\Sigma) \geq \frac{n(\Sigma)-t(\Sigma)+1}{\tilde{q}}$ where $\tilde{q}$ is the average cardinality of the share-spaces.

Before we prove this theorem, we state now (adapted to our language) the unpublished result and proof by Kilian and Nisan regarding the case $g = 1$, as mentioned in the introduction.

THEOREM 3.2 ([12]) *Let Σ be a threshold secret sharing scheme with n shares, privacy threshold $t(\Sigma) = t$ and where $\mathcal{S}_i = \{0, 1\}$ and $\mathcal{S}_j = \{0, 1\}^{m_j}$ for some integer $m_j > 0$ for all $j \in \mathcal{I}^*$. Then*

$$\sum_{j \in \mathcal{I}^*} m_j \geq n \log_2(n - t + 1).$$

PROOF. We begin by proving the case $t = 1$. We first claim that

$$\sum_{j \in \mathcal{I}^*} \frac{1}{2^{m_j}} \leq 1.$$

This will imply that at least $n \log_2 n$ bits must be dealt (which is tight for n a perfect power of 2). Since no single player is allowed to receive any information about a shared bit, the induced distributions on the conditioned variables $S_{j,0} = S_j | S_i = 0$ and $S_{j,1} = S_j|_{S_i=1}$ must be identical for all $j \in \mathcal{I}^*$. By a simple convexity argument,

$$Prob(S_{j,0} = S_{j,1}) \geq \frac{1}{2^{m_j}}.$$

Furthermore, for $j,k \in \mathcal{I}^*$, $j \neq k$, it is impossible for both $S_{j,0} = S_{j,1}$ and $S_{k,0} = S_{k,1}$. If this were the case, then in some circumstances it would be impossible to reconstruct the shared bit from the shares $\{j,k\}$. Thus,

$$\begin{aligned} Prob((\exists j) S_{j,0} = S_{j,1}) &= \sum_{j \in \mathcal{I}^*} Prob(S_{j,0} = S_{j,1}) \\ &\geq \sum_{j \in \mathcal{I}^*} \frac{1}{2^{m_j}}. \end{aligned}$$

Since any probability is at most 1, our claim is established.

Now consider the general case where $1 \leq t \leq n-1$. We can convert any such secret sharing scheme to a threshold scheme Σ' for $n-t+1$ players and with $t(\Sigma') = 1$. Let $A \subseteq \mathcal{I}^*$ be a set of $t-1$ indices and $B = \mathcal{I}^* \setminus A$. Let $\{s'_j\}_{j \in A}$ be a sequence of shares that could be dealt to A (since $t-1$ people know nothing, this sequence of shares must be valid for both 0 and 1.) To share a single bit b among B, use the scheme Σ to generate $\{s_{j,b}\}_{j \in \mathcal{I}^*}$, conditioned on $s_{j,b} = s'_j$ for $j \in A$. The shares of Σ' are $\{s_{j,b}\}_{j \in B}$. The values of $\{s'_j\}_{j \in A}$ are "hard-wired" into the secret sharing scheme, and thus do not need to be transmitted. We thus have,

$$\sum_{j \in B} \frac{1}{2^{m_j}} \leq 1.$$

By a simple convexity argument, we have that

$$\sum_{j \in B} m_j \geq (n-t+1) \log_2 (n-t+1).$$

By renumbering the players, we can ensure that if $j \in A$ and $k \in B$, then $m_j \geq m_k$. This gives us a final lower bound of $n \log_2(n-t+1)$ bits that must be shared among the n players.

△

We note that, even though this theorem is stated for the case where a bit is shared, it can be trivially extended to the case where the secret space is larger. The case $g = 1$ of our Main Theorem 3.1 could be read as

$$\sum_{j \in \mathcal{I}^*} H_1(S_j) \geq n \log_2 (n-t+1)$$

and hence is slightly more general than Theorem 3.2 in the sense that $H_1(S_j) \leq m_j$ for all j, but equality does not need to hold.

We now turn back to proving our Main Theorem 3.1. As it happened with Theorem 3.2, we will start by proving the case $t = 1$ and then we will prove the case of a general threshold scheme by constructing another scheme with $t = 1$ as above. First we need some definitions and simple observations.

DEFINITION 3.3 *Let $\Sigma := (\mathbf{S}, i)$ be a secret sharing scheme. Let $s \in \mathcal{S}_i$. Then $\mathbf{S}_{|S_i = s}$ is the vector of random variables $\mathbf{S}$ conditioned to the event $S_i = s$. Likewise we can consider $\mathbf{S}^*_{|S_i=s}$, $(\mathbf{S}_A)_{|S_i=s}$, $(S_j)_{|S_i=s}$. We define $C_{|s}(\Sigma) := supp\ (\mathbf{S}^*_{|S_i=s}) \subseteq \times_{j \in \mathcal{I}^*} \mathcal{S}_j$. We write $C_{|s}$ when Σ is clear from the context.*

Therefore, $C_{|s}$ is the set of "all possible sharings" of the secret s. We have already observed that

LEMMA 3.4 *If $A \in \mathcal{A}(\Sigma)$, then $(\mathbf{S}_A)_{|S_i=s}$ has the same distribution as $\mathbf{S}_A$ for all $s \in \mathcal{S}_i$.*

Now write $(C_{|s})_A$ the projection of $C_{|s}$ to the coordinates in A. We have the following.

LEMMA 3.5 *Let $s, s' \in \mathcal{S}_i$, $s \neq s'$. If $A \in \Gamma(\Sigma)$, then $(C_{|s})_A \cap (C_{|s'})_A = \emptyset$. In particular $C_{|s} \cap C_{|s'} = \emptyset$.*

PROOF. If $\mathbf{x} \in (C_{|s})_A \cap (C_{|s'})_A$, then it is clear that both $Prob(\mathbf{S}_A = \mathbf{x} | S_i = s) > 0$ and $Prob(\mathbf{S}_A = \mathbf{x} | S_i = s') > 0$ hold. This implies in turn that $Prob(S_i = s | \mathbf{S}_A = \mathbf{x}) > 0$ and $Prob(S_i = s' | \mathbf{S}_A = \mathbf{x}) > 0$. Therefore $\mathbf{S}_A$ does not determine S_i and $A \notin \Gamma(\Sigma)$. That proves the statement and in particular, since $\mathcal{I}^* \in \Gamma(\Sigma)$ by definition, we have $C_{|s} \cap C_{|s'} = \emptyset$. △

DEFINITION 3.6 *Given* $\mathbf{x} = (x_j)_{j\in\mathcal{I}^*}$, $\mathbf{x}' = (x'_j)_{j\in\mathcal{I}^*} \in \times_{j\in\mathcal{I}^*}\mathcal{S}_j$ *the Hamming distance between* $\mathbf{x}$ *and* $\mathbf{x}'$ *is*

$$d(\mathbf{x},\mathbf{x}') = |\{j \in \mathcal{I}^* : x_j \neq x'_j\}|.$$

Let $V, W \subseteq \times_{j\in\mathcal{I}^*}\mathcal{S}_j$. *The Hamming distance between* V *and* W *is*

$$d(V,W) := min_{(\mathbf{x},\mathbf{x}')\in V\times W} d(\mathbf{x},\mathbf{x}').$$

From Lemma 3.5 we have:

LEMMA 3.7 *Let* $s, s' \in \mathcal{S}_i$, $s \neq s'$. *Then*

$$d(C_{|s}, C_{|s'}) \geq n(\Sigma) - r(\Sigma) + 1.$$

PROOF. Suppose $d(C_{|s}, C_{|s'}) \leq n - r$. Then there exist two words $\mathbf{x} \in C_{|s}, \mathbf{x}' \in C_{|s'}$ which coincide in at least r coordinates. Call A the set of these coordinates. Then Lemma 3.5 tells us that $A \notin \Gamma(\Sigma)$. This contradicts the fact that $|A| \geq r$. △

We now prove our main combinatorial tool. If two vectors of random variables "look" locally the same (each coordinate has the same distribution) then we can upper bound the Hamming distance between their supports in terms of the encoding length of the variables.

LEMMA 3.8 *Let* $\mathbf{X}$, $\mathbf{Y}$ *be vectors of random variables with respective supports* $V, W \subseteq \times_{j\in\mathcal{I}^*}\mathcal{S}_j$ *and suppose that the marginal variables* X_j, Y_j *have the same probability distribution on* $\mathcal{S}_j$ *for all* $j \in \mathcal{I}^*$. *Furthermore assume* $V \cap W = \emptyset$. *Then*

$$0 < d(V,W) \leq |\mathcal{I}^*| \cdot \left(1 - 2^{-\lambda(\mathbf{X})}\right).$$

PROOF. For $j \in \mathcal{I}^*$, define the random variable D_j as follows: Sample $\mathbf{v} \in V$ according to $\mathbf{X}$ and, independently, $\mathbf{w} \in W$ according to $\mathbf{Y}$. Then $D_j = 0$ if $\mathbf{v}_j = \mathbf{w}_j$ and $D_j = 1$ if $\mathbf{v}_j \neq \mathbf{w}_j$. Also define $D = \sum_{j\in\mathcal{I}^*} D_j$. Note that the expectation $E(D_j)$ is the probability that $\mathbf{v}_j \neq \mathbf{w}_j$ and $E(D)$ is the "expected Hamming distance" between $\mathbf{v}$ and $\mathbf{w}$. Since X_j, Y_j have the same distribution, $E(D_j) = 1 - 2^{-H_2(X_j)}$, where H_2 denotes the collision entropy. By linearity of expectation, $E(D) = \sum_{j\in\mathcal{I}^*} E(D_j) = \sum_{j\in\mathcal{I}^*} \left(1 - 2^{-H_2(X_j)}\right)$. Hence, since in addition $V \cap W = \emptyset$, there is a pair $(\mathbf{v},\mathbf{w}) \in V \times W$ with $0 < d(\mathbf{v},\mathbf{w}) \leq \sum_{j\in\mathcal{I}^*} \left(1 - 2^{-H_2(X_j)}\right)$. In conclusion,

$$0 < d(V,W) \leq \sum_{j\in\mathcal{I}^*} \left(1 - 2^{-H_2(X_j)}\right) \leq$$

$$\sum_{j\in\mathcal{I}^*} \left(1 - 2^{-H_1(X_j)}\right) \leq |\mathcal{I}^*| \cdot \left(1 - 2^{-\lambda(\mathbf{X})}\right),$$

where the latter inequality follows from Jensen's inequality (note that 2^{-x} is a convex function). △

THEOREM 3.9 *Let* Σ *be a secret sharing scheme and suppose* $t(\Sigma) \geq 1$. *Then*

$$r(\Sigma) \geq 2^{-\lambda^*(\Sigma)} \cdot n(\Sigma) + 1.$$

In particular, $r(\Sigma) \geq \frac{n(\Sigma)}{\tilde{q}} + 1$, *where* $\tilde{q}$ *is the average cardinality of the share-spaces* $\mathcal{S}_j$.

PROOF. Fix two different secrets $s, s' \in \mathcal{S}_i$. Now we will apply Lemma 3.8 to the variables $\mathbf{S}_{|S_i=s}$ and $\mathbf{S}_{|S_i=s'}$ with support in the sets $C_{|s}$ and $C_{|s'} \subseteq \times_{j\in\mathcal{I}^*}\mathcal{S}_j$ respectively. We can do this because, since $t \geq 1$, $\{j\} \in \mathcal{A}(\Sigma)$ for all $j \in \mathcal{I}^*$ and according to Lemma 3.4, the variables $(S_j)_{|S_i=s}$ and $(S_j)_{|S_i=s'}$ have both the same distribution (since they both have the same distribution as S_j). Furthermore, by Lemma 3.5, $C_{|s} \cap C_{|s'} = \emptyset$. Therefore, Lemma 3.8 implies

$$d(C_{|s}, C_{|s'}) \leq |\mathcal{I}^*| \cdot \left(1 - 2^{-\lambda^*}\right).$$

Finally by Lemma 3.7 (and since $|\mathcal{I}^*| = n$) we achieve

$$r \geq 2^{-\lambda^*} \cdot n + 1.$$

As for the second part of the theorem, we have

$$\lambda^* = \frac{\sum_{j\in\mathcal{I}^*} H_1(S_j)}{n} \leq \frac{\sum_{j\in\mathcal{I}^*} \log(|\mathcal{S}_j|)}{n}.$$

This together with Jensen's inequality implies $2^{\lambda^*} \leq \tilde{q}$ which leads to the result. △

Obviously, this is enough to prove Main Theorem 3.1 in the case $t = 1$. In order to attain the result in the general case $t \geq 1$, we reduce it to the case $t = 1$ using appropiate "shortening" of the secret sharing scheme. This notion is formalized next.

DEFINITION 3.10 *Let $\Sigma = (\mathbf{S}, i)$ be a secret sharing scheme and let $\emptyset \neq A \in \mathcal{A}(\Sigma)$ and $\mathbf{x} \in \times_{j\in A}\mathcal{S}_j$ with $P(\mathbf{S}_A = \mathbf{x}) > 0$. Write $B = \mathcal{I} \setminus A$ and $B^* = \mathcal{I}^* \setminus A$. Then we write $\Sigma_{|\mathbf{S}_A=\mathbf{x}} := (\mathbf{T}, i)$ where $\mathbf{T}$ is the vector of random variables $\mathbf{T} := \mathbf{S}_{B|\mathbf{S}_A=\mathbf{x}}$ defined on $\times_{j\in B}\mathcal{S}_j$.*

LEMMA 3.11 *With the definitions above, let $\Sigma' := \Sigma_{|\mathbf{S}_A=\mathbf{x}}$. Then $\Sigma' = (\mathbf{T}, i)$ is a secret sharing scheme with player set B (so $n(\Sigma') = n(\Sigma) - |A|$).*

In addition

$$\mathcal{A}(\Sigma') \supseteq \{D \subseteq B^* : D \cup A \in \mathcal{A}(\Sigma)\}$$

and

$$\Gamma(\Sigma') \supseteq \{D \subseteq B^* : D \cup A \in \Gamma(\Sigma)\}.$$

In particular $r(\Sigma') \leq r(\Sigma) - |A|$ and $t(\Sigma') \geq t(\Sigma) - |A|$.

Moreover, suppose in addition that $H_1(S_j) \geq H_1(S_\ell)$ for all $j \in A$, $\ell \in B^*$ and that

$$\sum_{j\in B^*} H(S_j|\mathbf{S}_A = \mathbf{x}) \leq \sum_{j\in B^*} H(S_j|\mathbf{S}_A = \mathbf{y})$$

for all $\mathbf{y} \in supp\ \mathbf{S}_A$. Then

$$\lambda^*(\Sigma) \geq \lambda^*(\Sigma').$$

PROOF. We first prove that Σ' is a secret sharing scheme, verifying the two conditions in Definition 2.7.

a) First, note that $T_i = S_{i|\mathbf{S}_A=\mathbf{x}}$. Since $A \in \mathcal{A}(\Sigma)$, S_i and $\mathbf{S}_A$ are independently distributed. Therefore $T_i = S_{i|\mathbf{S}_A=\mathbf{x}}$ has the same distribution as S_i which, since Σ is a secret sharing scheme, is the uniform distribution on $\mathcal{S}_i$.

b) Second, we need to prove that the value of $\mathbf{T}^*$ determines the value of T_i. For any $\mathbf{y} \in \times_{j\in B^*}\mathcal{S}_j$ with $P(\mathbf{T}^* = \mathbf{y}) > 0$ we have $P(\mathbf{S}_A = \mathbf{x}, \mathbf{S}_{B^*} = \mathbf{y}) > 0$. Since Σ is a secret sharing scheme, the value of $\mathbf{S}^*$ completely determines the value of S_i, so there exists a unique $z \in S_i$ with $P(S_i = z|\mathbf{S}_A = \mathbf{x}, \mathbf{S}_{B^*} = \mathbf{y}) = 1$. But this implies that $P(T_i = z|\mathbf{T}^* = \mathbf{y}) = 1$. We have proved that $\mathbf{T}^*$ determines T_i.

We can now generalize these two observations in order to prove the claims about $t(\Sigma')$ and $r(\Sigma')$. Let $D \subseteq B^*$ and suppose that $D \cup A \in \mathcal{A}(\Sigma)$ and consequently S_i and $\mathbf{S}_{D\cup A}$ are independently distributed. Then it is again straightforward that T_i is uniformly distributed from $\mathbf{T}_D$. Let D be a subset of B^* such that $D \cup A \in \Gamma(\Sigma)$. Then the value of $\mathbf{S}_{D\cup A}$ determines the value of S_i. By a similar argument as we used in part b) of the proof that Σ' is a secret sharing scheme this means $\mathbf{T}_D$ determines T_i.

Finally, we proved the claim about $\lambda^*(\Sigma)$ and $\lambda^*(\Sigma')$. Assume that $H_1(S_j) \geq H_1(S_\ell)$ for all $j \in A$, $\ell \in B^*$ and that $\sum_{j\in B^*} H(S_j|\mathbf{S}_A = \mathbf{x}) \leq \sum_{j\in B^*} H(S_j|\mathbf{S}_A = \mathbf{y})$ for all $\mathbf{y} \in \text{supp } \mathbf{S}_A$. Suppose this is the case. Then

$$\lambda^*(\Sigma) = \frac{\sum_{j\in\mathcal{I}^*} H(S_j)}{n(\Sigma)} \geq \frac{\sum_{j\in B^*} H(S_j)}{n(\Sigma) - (|A| - 1)} \geq$$

$$\frac{\sum_{j\in B^*} H(S_j|\mathbf{S}_A)}{n(\Sigma) - (|A| - 1)} =$$

$$\frac{\sum_{j\in B^*}\sum_{\mathbf{y}\in \text{supp } \mathbf{S}_A} P(\mathbf{S}_A=\mathbf{y})H(S_j|\mathbf{S}_A=\mathbf{y})}{n(\Sigma)-(|A|-1)} =$$

$$\sum_{\mathbf{y}\in \text{supp } \mathbf{S}_A} P(\mathbf{S}_A=\mathbf{y})\left(\frac{\sum_{j\in B^*} H(S_j|\mathbf{S}_A=\mathbf{y})}{n(\Sigma)-(|A|-1)}\right) \geq$$

$$\frac{\sum_{j\in B^*} H(S_j|\mathbf{S}_A=\mathbf{x})}{n(\Sigma)-(|A|-1)} = \frac{\sum_{j\in B^*} H(T_j)}{n(\Sigma')} = \lambda^*(\Sigma')$$

Here we have used in the first inequality that the average of the multi-set $\{H(S_j)\}_{j\in\mathcal{I}^*}$ is larger or equal than the average of the multi-set $\{H(S_j)\}_{j\in B}$ because all the elements that we remove from the first multi-set to obtain the second were larger than the elements that remain in it, by the first of the assumptions. On the other hand, in the third inequality, we use that the expectation of the random variable that samples $\mathbf{y}$ according to $\mathbf{S}_A$ and outputs $\sum_{j\in B^*} H(S_j|\mathbf{S}_A=\mathbf{y})$ is larger or equal than its minimum value, which is attained when $\mathbf{S}_A=\mathbf{x}$ by the second of the assumptions.

△

Now it is easy to prove Main Theorem 3.1 in the general case:

Proof (of Main Theorem 3.1) If $t(\Sigma)=1$, it is a direct consequence of Theorem 3.9. If $t(\Sigma)\geq 1$ then we choose $A\subseteq\mathcal{I}^*$ the set of $t(\Sigma)-1$ indices j such that $H(S_j)$ are largest, we denote $B^*=\mathcal{I}^*\setminus A$ and we choose $\mathbf{x}\in\text{supp } \mathbf{S}_A$ such that $\sum_{j\in B^*} H(S_j|\mathbf{S}_A=\mathbf{x})$ is smallest. We can construct the secret sharing scheme $\Sigma'=(\mathbf{T},i)$ as in Definition 3.10 (note $A\in\mathcal{A}(\Sigma)$). Note that, by Lemma 3.11, $t(\Sigma')\geq t(\Sigma)-|A|=1$ and consequently we can apply Theorem 3.9 to Σ'. This gives $r(\Sigma')\geq 2^{-\lambda^*(\Sigma')}\cdot n(\Sigma')+1$ and therefore

$$r(\Sigma)-t(\Sigma)\geq r(\Sigma')-1\geq 2^{-\lambda^*(\Sigma')}\cdot n(\Sigma')\geq$$
$$2^{-\lambda^*(\Sigma)}\cdot(n(\Sigma)-t(\Sigma)+1)$$

where in addition we have used in the first inequality that $r(\Sigma)-|A|\geq r(\Sigma')$ (Lemma 3.11), and in the third that $\lambda^*(\Sigma)\geq\lambda^*(\Sigma')$ because of the last part of Lemma 3.11 and our selection of A and $\mathbf{x}$.

△

As a consequence we can state the following.

Corollary 3.12 *Let $\{\Sigma_n\}_n$ be a family of* threshold *($g=1$) secret sharing schemes on n players, where n is unbounded, and suppose there is a constant $c<1$ such that $1\leq t(\Sigma_n)\leq cn$ for all n. Then the average size of the shares is at least logarithmic in n, i.e., $\lambda^*(\Sigma_n)=\Omega(\log n)$.*

3.2 Improvement for linear secret sharing schemes

In the main result of this section, Main Theorem 3.27, we prove a lower bound for the threshold gap of a *linear* secret sharing scheme which, as opposed to what happened with Main Theorem 3.1, does not depend on the privacy threshold.

We define now the concept of linear secret sharing scheme and some related notions and properties, including the definition of dual secret sharing scheme and the relationship between the thresholds of a scheme and those of its dual, which will play an important role in the proof of our main result.

Definition 3.13 *Let $\mathbb{F}_q$ be a finite field. A linear secret sharing scheme (LSSS) over $\mathbb{F}_q$ is a secret sharing scheme $\Sigma=(\mathbf{S},i)$ where the secret and share spaces $\mathcal{S}_j$ are $\mathbb{F}_q$-vector spaces and $\mathbf{S}$ has the uniform distribution on a $\mathbb{F}_q$-linear subspace $V\leq\times_{j\in\mathcal{I}}\mathcal{S}_j$.*

Without loss of generalization, we may consider that all spaces $\mathcal{S}_j$ are of the form $\mathbb{F}_q^{k_j}$ for some $k_j\geq 0$. For simplicity we will consider in most of this section the case where $\mathcal{S}_j=\mathbb{F}_q$ for all $j\neq i$, i.e., every share consists of one element of the finite field. The secret will consist of k elements of $\mathbb{F}_q$. Note that the random variable $\mathbf{S}$ has the uniform distribution over a linear code over $\mathbb{F}_q$ of length $|\mathcal{I}^*|+k$. This suggests the notion of n-code, which appeared in [6], and we detail below, after introducing some notation.

DEFINITION 3.14 *The $\mathbb{F}_q$-vector space morphism $\pi_0 : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^k$ is defined by the projection*

$$(s_1, \ldots, s_k, c_1, \ldots, c_n) \mapsto (s_1, \ldots, s_k).$$

For each $i \in \{1, \ldots, n\}$, the $\mathbb{F}_q$-vector space morphism $\pi_i : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q$ is defined by the projection

$$(s_1, \ldots, s_k, c_1, \ldots, c_n) \mapsto c_i.$$

For $\emptyset \neq A \subset \{1, \ldots, n\}$, the $\mathbb{F}_q$-vector space morphism $\pi_A : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^{|A|}$ is defined by the projection

$$(s_1, \ldots, s_k, c_1, \ldots, c_n) \mapsto (c_i)_{i \in A}.$$

For $\mathbf{v} \in \mathbb{F}_q^k \times \mathbb{F}_q^n$, it is sometimes convenient to denote $\pi_0(\mathbf{v}) \in \mathbb{F}_q^k$ by $\mathbf{v}_0$ and $\pi_A(\mathbf{v}) \in \mathbb{F}_q^{|A|}$ by $\mathbf{v}_A$. We write $\mathcal{I}^* = \{1, \ldots, n\}$. It is also sometimes convenient to refer to $\mathbf{v}_0$ as the secret-component *of $\mathbf{v}$ and to $\mathbf{v}_{\mathcal{I}^*}$ as its* shares-component.

DEFINITION 3.15 *An n-code for $\mathbb{F}_q^k$ (over $\mathbb{F}_q$) is an $\mathbb{F}_q$-vector space $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ such that*

(i) $\pi_0(C) = \mathbb{F}_q^k$ *and*

(ii) $(\text{Ker } \pi_{\mathcal{I}^*}) \cap C \subset (\text{Ker } \pi_0) \cap C$.

For $\mathbf{c} \in C$, $\mathbf{c}_0 \in \mathbb{F}_q^k$ is the secret *and $\mathbf{c}_{\mathcal{I}^*} \in \mathbb{F}_q^n$ the* shares.

PROPOSITION 3.16 *Given an n-code C for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, let $\mathbf{S}$ be the random variable with uniform distribution over C. Then $(\mathbf{S}, 0)$ is a LSSS with n shares, secret space $\mathbb{F}_q^k$ and share spaces $\mathbb{F}_q$. We will denote this LSSS as $\Sigma(C)$.*

PROOF. The condition (i) means that, in C, the secret can take any value in $\mathbb{F}_q^k$. More precisely, for a uniformly random vector $\mathbf{c} \in C$, the secret $\mathbf{c}_0$ is uniformly random in $\mathbb{F}_q^k$. So the only nontrivial requirement to be checked is that there is joint reconstruction of the secret. Suppose, on the contrary, that $\mathbf{S}^*$ did not determine $\mathbf{S}_0$. This would imply that there are two words $\mathbf{c}, \mathbf{c}' \in C$ with $\mathbf{c}_{\mathcal{I}^*} = \mathbf{c}'_{\mathcal{I}^*}$ and $\mathbf{c}_0 \neq \mathbf{c}'_0$. But then $\mathbf{c} - \mathbf{c}' \in (\text{Ker } \pi_{\mathcal{I}^*}) \cap C$ and $\mathbf{c} - \mathbf{c}' \notin \text{Ker } \pi_0$, which contradicts the assumption (ii) above. △

We will now state some facts about the access and adversary structures of LSSS. These are straightforward generalizations of known results.

DEFINITION 3.17 *Let*

$$\Gamma_C := \{A \subset \mathcal{I}^* : A \neq \emptyset, (\text{Ker } \pi_A) \cap C \subset (\text{Ker } \pi_0) \cap C\}.$$

PROPOSITION 3.18 *Γ_C is the access structure of the scheme $\Sigma(C)$, i.e., $\Gamma_C = \Gamma(\Sigma(C))$*

PROOF. $\Gamma_C \subseteq \Gamma(\Sigma(C))$ is a generalization of the proof of Proposition 3.16. On the other hand, if $A \in \Gamma(\Sigma(C))$, then $A \neq \emptyset$ and for every two words $\mathbf{c}, \mathbf{c}' \in C$ such that $\mathbf{c}_A = \mathbf{c}'_A$, we must have $\mathbf{c}_0 = \mathbf{c}'_0$. But in particular if $\mathbf{c}'$ is the zero word, we have that for any $\mathbf{c} \in C$ with $\mathbf{c}_A = \mathbf{0}$, we must have $c_i = 0$, which is exactly the condition $A \in \Gamma_C$ △

DEFINITION 3.19 *We say $A \subseteq \mathcal{I}^*$ is* disconnected from 0 *if the map $\pi_{0,A} : C \longrightarrow \mathbb{F}_q^k \times \pi_A(C)$ given by $\mathbf{c} \mapsto (\mathbf{c}_0, \mathbf{c}_A)$ is surjective.*
We define the set

$$\mathcal{A}_C := \{A \in \mathcal{I}^* : A = \emptyset \text{ or } A \text{ is disconnected from } 0\}.$$

PROPOSITION 3.20 *$\mathcal{A}_C$ is the adversary structure of the scheme $\Sigma(C)$, i.e., $\mathcal{A}_C = \mathcal{A}(\Sigma(C))$.*

PROOF. Since $\mathbf{S}$ is uniformly distributed in C, for any non-empty set $A \subset \mathcal{I}^*$, the distribution of $(S_0, \mathbf{S}_A)$ is uniform on the set Im $\pi_{0,A}$, and $\mathbf{S}_A$ is uniform on the set Im π_A. So A being disconnected implies that the distribution of $(S_0, \mathbf{S}_A)$ is uniform on supp $S_0 \times$ supp $\mathbf{S}_A$ and by Lemma 2.16, $A \in \mathcal{A}(\Sigma(C))$. On the other hand if $A \in \mathcal{A}(\Sigma(C))$ is non-empty, then every element in supp $S_0 \times$ supp $\mathbf{S}_A$ is in supp $\mathbf{S}_{\{0\} \cup A} = \pi_{0,A}(C)$ (otherwise S_0 and $\mathbf{S}_A$ cannot be independent) which means $\pi_{0,A}(C) = \mathbb{F}_q^k \times \pi_A(C)$ (because supp $S_0 = \mathbb{F}_q^k$). △

PROPOSITION 3.21

$$\mathcal{A}_C = \{A \subseteq \mathcal{I}^* : A = \emptyset \text{ or } \pi_0(\text{Ker } \pi_A \cap C) = \mathbb{F}_q^k\}.$$

PROOF. Let A be disconnected from 0. Since $\mathbf{0} \in C$, we have $\mathbf{0}_A \in \pi_A(C)$. Therefore for any $\mathbf{x} \in \mathbb{F}_q^k$, there exists a word $\mathbf{c} \in C$ such that $\pi_{0,A}(\mathbf{c}) = (\mathbf{x}, \mathbf{0}_A)$. But then $\mathbf{c} \in \text{Ker } \pi_A \cap C$, so $\mathbf{x} \in \pi_0(\text{Ker } \pi_A \cap C)$.

In order to prove the other direction, let $A \in \mathcal{I}^*$ be such that

$$\pi_0(\text{Ker } \pi_A \cap C) = \mathbb{F}_q^k.$$

For every $\mathbf{x} \in \mathbb{F}_q^k$, let $\mathbf{c}^{\mathbf{x}}$ be a word in Ker $\pi_A \cap C$ with $\pi_0(\mathbf{c}^{\mathbf{x}}) = \mathbf{x}$. On the other hand for every $\mathbf{y} \in \pi_A(C)$, let $\mathbf{w}^{\mathbf{y}} \in C$ be a word with $\pi_A(\mathbf{w}^{\mathbf{y}}) = \mathbf{y}$. Now, given any pair $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^k \times \pi_A(C)$, write $\mathbf{z} = \pi_0(\mathbf{w}^{\mathbf{y}})$ and define $\mathbf{d} = \mathbf{c}^{\mathbf{x}-\mathbf{z}} + \mathbf{w}^{\mathbf{y}} \in C$. It is easy to see that $\pi_{0,A}(\mathbf{d}) = (\mathbf{x}, \mathbf{y})$. Therefore Im $(\pi_{0,A}) = \mathbb{F}_q^k \times \pi_A(C)$. △

This means that a non-empty set A is a privacy set if and only if for all $\mathbf{x} \in \mathbb{F}_q^k$, there is a word $\mathbf{c} \in C$ with $\mathbf{c}_0 = \mathbf{x}$ and $\mathbf{c}_A = \mathbf{0}$. And in particular:

COROLLARY 3.22 *If $k = 1$, then*

$$\Gamma_C = \{A \subseteq \mathcal{I}^* : A \neq \emptyset \text{ and } \nexists \mathbf{c} \in C \text{ with } \mathbf{c}_0 = 1, \mathbf{c}_A = \mathbf{0}\}$$

and

$$\mathcal{A}_C = \{A \subseteq \mathcal{I}^* : A = \emptyset \text{ or } \exists \mathbf{c} \in C \text{ with } \mathbf{c}_0 = 1, \mathbf{c}_A = \mathbf{0}\}.$$

Therefore $\Sigma(C)$ is perfect, i.e., for any $A \subseteq \mathcal{I}^*$ either $A \in \Gamma(\Sigma(C))$ or $A \in \mathcal{A}(\Sigma(C))$.

DEFINITION 3.23 *Let C be an n-code. We define $r(C) := r(\Sigma(C))$ and $t(C) := t(\Sigma(C))$*

We need to introduce now the concept of the dual n-code of a given n-code.

DEFINITION 3.24 *Let $< \cdot, \cdot >$ denote the dot product in $\mathbb{F}_q^k \times \mathbb{F}_q^n$, i.e., if $\mathbf{c} := (x_1, \ldots x_k, y_1, \ldots, y_n)$ and $\mathbf{c}' := (x'_1, \ldots x'_k, y'_1, \ldots, y'_n) \in \mathbb{F}_q^k \times \mathbb{F}_q^n$, then*

$$< \mathbf{c}, \mathbf{c}' > := \sum_{i=1}^{k} x_i x'_i + \sum_{j=1}^{n} y_j y'_j.$$

Given an n-code C for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, we define its dual $C^\perp \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ as the set

$$C^\perp := \{\mathbf{c}^* \in \mathbb{F}_q^k \times \mathbb{F}_q^n :< \mathbf{c}^*, \mathbf{c} >= 0 \ \forall \mathbf{c} \in C\}.$$

It is easy to see that if C is an n-code for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ then so is $C^\perp$. Furthermore, we can give a relation between the access and adversary structure of an n-code and its dual.

THEOREM 3.25 *We have*

$$\Gamma_{C^\perp} = \{A \subseteq \mathcal{I}^* : \mathcal{I}^* \setminus A \in \mathcal{A}_C\}.$$

Consequently $r(C^\perp) = n - t(C)$, $t(C^\perp) = n - r(C)$ and therefore $g(C) = g(C^\perp)$.

PROOF.

Let $A \subseteq \mathcal{I}^*$ be such that $B := \mathcal{I}^* \setminus A \in \mathcal{A}_C$. If $B = \emptyset$ then $A = \mathcal{I}^* \in \Gamma_{C^\perp}$. Otherwise, by Proposition 3.21, for each $\mathbf{x} \in \mathbb{F}_q^k$, there exists $\mathbf{c}^{\mathbf{x}} \in C$ with $\pi_0(\mathbf{c}^{\mathbf{x}}) = \mathbf{x}$ and $\pi_B(\mathbf{c}^{\mathbf{x}}) = \mathbf{0}$. Now let $\mathbf{w} \in C^\perp \cap Ker\ \pi_A$. Note $< \mathbf{w}, \mathbf{c}^{\mathbf{x}} >= 0$ for all $\mathbf{x} \in \mathbb{F}_q^k$. On the other hand, since for all $j \in \mathcal{I}^*$ either $j \in A$ or $j \in B$ and therefore at least one of $\mathbf{w}_i$, $(\mathbf{c}^{\mathbf{x}})_i$ is zero, we have $0 =< \mathbf{w}, \mathbf{c}^{\mathbf{x}} >=< \pi_0(\mathbf{w}), \mathbf{x} >$ for all $\mathbf{x} \in \mathbb{F}_q^k$. Therefore, $\pi_0(\mathbf{w}) = \mathbf{0}$ and $\mathbf{w} \in$ Ker π_0. We have proved $A \in \Gamma_C^\perp$.

On the other hand let $A \subseteq \mathcal{I}^*$ with $B := \mathcal{I}^* \setminus A \notin \mathcal{A}_C$ and let us prove $A \notin \Gamma_{C^\perp}$. By Proposition 3.21, there exists an $\mathbf{x} \in \mathbb{F}_q^k$ such that there is no word $\mathbf{c}$ in C with $\pi_0(\mathbf{c}) = \mathbf{x}$, $\pi_B(\mathbf{c}) = \mathbf{0}$. In

other words the vector $\mathbf{w} := (\mathbf{x}, \mathbf{0}) \in \mathbb{F}_q^{k+|B|}$, is not in the vector space $\pi_{0,B}(C)$. Therefore there is a vector $\mathbf{y} \in \mathbb{F}_q^{k+|B|}$ which is orthogonal to $\pi_{0,B}(C)$ but not to $\mathbf{w}$,i.e,

$$< \mathbf{y}, \mathbf{z} >= 0, \ \forall \mathbf{z} \in \pi_{0,B}(C) \tag{1}$$

$$< \mathbf{y}, \mathbf{w} >\neq 0 \tag{2}$$

Equation 2 tells us not only that $\mathbf{y}$ is nonzero, but since $\mathbf{w}_B = \mathbf{0}$, the only possibility is that $\mathbf{y}_0 \neq \mathbf{0}$. We now construct the vector $\mathbf{c}^* \in \mathbb{F}_q^{k+n}$ by $\pi_{0,B}(\mathbf{c}^*) = \mathbf{y}$ and $\mathbf{c}^*_A = \mathbf{0}$. Now for every $\mathbf{c} \in C$, we can split $< \mathbf{c}, \mathbf{c}^* >$ into the sum of $< \pi_{0,B}(\mathbf{c}^*), \pi_{0,B}(\mathbf{c}) >$ and $< \mathbf{c}^*_A, \mathbf{c}_A >$. But the first term equals $< \mathbf{y}, \pi_{0,B}(\mathbf{c}) >$ which is zero by Equation 1, while the second one is also zero because $\mathbf{c}^*_A = \mathbf{0}$. Therefore $\mathbf{c}^*$ is a word in $C^\perp$ and it also satisfies that $\mathbf{c}^* \in \text{Ker } \pi_A$, but $\mathbf{c}^* \notin \text{Ker } \pi_0$ (because $\mathbf{c}^*_0 = \mathbf{y}_0 \neq \mathbf{0}$). By definition, $A \notin \Gamma_{C^\perp}$.

Finally, since $(C^\perp)^\perp = C$, we also have

$$\Gamma_C = \{A \subseteq \mathcal{I}^* : \mathcal{I}^* \setminus A \in \mathcal{A}_{C^\perp}\},$$

and the statements about the reconstruction and privacy thresholds can be deduced from here. $\triangle$

We can state now a lower bound for the threshold gap of linear secret sharing schemes which does not depend, as it happened with the general bound in Main Theorem 3.1, on the value of the privacy threshold. The idea is to apply Main Theorem 3.1 to both the LSSS $\Sigma(C)$ and the dual LSSS $\Sigma(C^\perp)$. We remark that the bound in Main Theorem 3.27 does not depend at all on the size of the secret. Here we only assume that all shares are single elements of $\mathbb{F}_q$.

THEOREM 3.26 *Let Σ be a linear secret sharing scheme over $\mathbb{F}_q$ with all shares in $\mathbb{F}_q$, $t(\Sigma) \geq 1$ and $r(\Sigma) \leq n(\Sigma) - 1$. Then*

$$g(\Sigma) \geq \max\{\frac{n(\Sigma) - t(\Sigma) + 1}{q}, \frac{r(\Sigma) + 1}{q}\}.$$

PROOF. Let $\Sigma = \Sigma(C)$ for a linear code C over $\mathbb{F}_q$ of length $n(\Sigma) + k$. We will apply Main Theorem 3.1 to both Σ and $\Sigma^\perp := \Sigma(C^\perp)$ (note that by Theorem 3.25 and the assumption on $r(\Sigma)$, we have $t(\Sigma^\perp) \geq 1$, so we can indeed apply the theorem to $\Sigma^\perp$). Since every share is in $\mathbb{F}_q$, this gives us

$$g(\Sigma) \geq \frac{n(\Sigma) - t(\Sigma) + 1}{q}$$

and

$$g(\Sigma^\perp) \geq \frac{n(\Sigma^\perp) - t(\Sigma^\perp) + 1}{q}.$$

Now using Theorem 3.25 we can state this last inequality as $g(\Sigma) \geq \frac{r(\Sigma)+1}{q}$ which gives the result. $\triangle$

MAIN THEOREM 3.27 *Let Σ be a linear secret sharing scheme over $\mathbb{F}_q$ with all shares in $\mathbb{F}_q$, $t(\Sigma) \geq 1$ and $r(\Sigma) \leq n(\Sigma) - 1$. Then*

$$g(\Sigma) \geq \frac{n(\Sigma) + 2}{2q - 1}.$$

PROOF. We sum inequalities

$$g(\Sigma) \geq \frac{n(\Sigma) - t(\Sigma) + 1}{q}$$

and

$$g(\Sigma) \geq \frac{r(\Sigma) + 1}{q}$$

from Theorem 3.26 and use that $g(\Sigma) = r(\Sigma) - t(\Sigma)$. $\triangle$

COROLLARY 3.28 *If $\{\Sigma_n\}$ is an infinite family of ideal linear secret sharing schemes over the same finite field $\mathbb{F}_q$, where Σ_n has n players, $t(\Sigma_n) \geq 1$ and $r(\Sigma_n) \leq n - 1$ and n is unbounded then $g(\Sigma_n) = \Omega(n)$.*

REMARK 3.29 *We have introduced the assumption $r(\Sigma) \leq n(\Sigma) - 1$, which is crucial. For all $n > 0$ and every finite field $\mathbb{F}_q$, we can define the n-code C_n for $\mathbb{F}_q$ over $\mathbb{F}_q$ consisting of all vectors $\mathbf{c} \in \mathbb{F}_q \times \mathbb{F}_q^n$ such that $c_0 = \sum_{i=1}^n c_i$, and define $\Sigma_n := \Sigma(C_n, 0)$. This is indeed a LSSS (the additive LSSS over $\mathbb{F}_q$ for n players) such that $t(\Sigma_n) = n - 1$ and $r(\Sigma_n) = n$, so $g(\Sigma_n) = 1$.*

We state now, without proving it, the generalization of the Main Theorem 3.27 to the case where players may hold more than one element of the field as share.

THEOREM 3.30 *Let Σ be a linear secret sharing scheme over $\mathbb{F}_q$ where for each $j \in \mathcal{I}^*$ the j-th share is in $\mathbb{F}_q^{k_j}$ for some $k_j \geq 1$. Let $t(\Sigma) \geq 1$ and $r(\Sigma) \leq n(\Sigma) - 1$. Let $\overline{k} = \frac{1}{n} \sum_{j \in \mathcal{I}^*} k_j$. Then*

$$g(\Sigma) \geq \frac{n(\Sigma) + 2}{2q^{\overline{k}} - 1}.$$

In [11], Karchmer and Wigderson proved, in the equivalent language of monotone span programs, that the total number $\overline{k}n$ of field elements given as shares in a binary linear secret sharing scheme (which they call dimension of the span program) with a *threshold* access structure where $1 \leq t \leq n-2$ must be $\Omega(n \log n)$. See also [9]. In [5, Theorem 13], this was generalized to linear secret sharing schemes with threshold gap $o(\log n)$. Theorem 3.30 above improves the latter result, and therefore further generalizes the previous facts. More precisely it implies that $\overline{k}n = \Omega(n \log n)$ if $g = o(n)$.

4 Bounds Involving the Secret-Space

If the cardinality of the secret-space is "large," then there is the following connection with the theory of error correcting codes.

THEOREM 4.1 *Let $\Sigma = (\mathbf{S}, i)$ be a secret sharing scheme with $|\mathcal{S}_i| = M$ and $|\mathcal{S}_j| = q$ for all $j \in \mathcal{I}^*$. Then for each set $A \in \mathcal{A}(\Sigma)$, there exists a q-ary code D with length $n(\Sigma) - |A|$, minimum distance $d(D) \geq n(\Sigma) - r(\Sigma) + 1$ and size $|D| = M$. In particular, there exists a $q-ary$ code D' with length $n(\Sigma) - t(\Sigma)$, minimum distance $d(D') \geq n(\Sigma) - r(\Sigma) + 1$ and size $|D'| = M$. Moreover, in the case that $\Sigma = (\mathbf{S}, i)$ is an $\mathbb{F}_q$-linear secret sharing scheme with $\mathcal{S}_i = \mathbb{F}_q^k$ and $\mathcal{S}_j = \mathbb{F}_q$ for all $j \in \mathcal{I}^*$, there exists an $\mathbb{F}_q$-linear code D' with length $n(\Sigma) - t(\Sigma)$, minimum distance $d(D') \geq n(\Sigma) - r(\Sigma) + 1$ and dimension k.*

PROOF. Let $A \in \mathcal{A}(\Sigma)$ and assume it is non-empty. Let $\mathbf{x} \in \times_{j \in A} \mathcal{S}_j$ with $P(\mathbf{S}_A = \mathbf{x}) > 0$. Write $B = \mathcal{I} \setminus A$ and $B^* = \mathcal{I}^* \setminus A$. We consider the shortened secret sharing scheme $\Sigma' = \Sigma_{|\mathbf{S}_A = \mathbf{x}}$, as defined in Definition 3.10. By Lemma 3.11 we have that $r(\Sigma') \leq r(\Sigma) - |A|$. For each element $e \in \mathcal{S}_i$, select one word $\mathbf{w}_e \in C_{|e}(\Sigma')$. The words form a code D over $\mathcal{A}$ with length $n(\Sigma') = n(\Sigma) - |A|$. Note that no two words can be the same, since by Lemma 3.7 the distance between words in different sets $C_{|s}(\Sigma')$, $C_{|s'}(\Sigma')$ is at least 1. Hence $|D| = M$. Moreover, Lemma 3.7 also implies that the distance between any two different words of D is at least $n(\Sigma') - r(\Sigma') + 1$ which in turn is at least $n(\Sigma) - r(\Sigma) + 1$, therefore proving the claim about the minimal distance. We can also proof the result if A is the empty set. In this case we do not shorten but we construct D directly from Σ instead of Σ'.

In the case of a linear scheme, we proceed the same way except that when constructing D, in order to guarantee that it is a linear code, we first fix some basis of $\mathbb{F}_q^k$, and for each element $e \in \mathbb{F}_q^k$ in that basis, select one word $\mathbf{w}_e \in C_{|e}(\Sigma')$. The k selected words span a linear code D over $\mathbb{F}_q$, and from this point on the proof continues in exactly the same way.

△

As an immediate consequence, restrictions on the parameters n, t, r, q, M are obtained from known bounds on error correcting codes. For example, by combining Theorem 4.1 and the Singleton bound (see e.g.[14]), we would get the well known bound $g(\Sigma) \geq k$. However, a much stronger result is obtained from a suitable application of the *Griesmer bound*. This leads to a simple bound that is easy to compare with our first bound. The drawback, however, is that the Griesmer bound only applies to linear codes and consequently we will be restricted to linear secret sharing schemes.

Let $\lceil a \rceil$ denote the smallest integer that is larger than or equal to the real number a. The Griesmer bound [10] (see also [14, Chapter 2.7]) is as follows.

THEOREM 4.2 (GRIESMER BOUND) *Let C be an $\mathbb{F}_q$-linear code with length n, dimension $k \geq 1$, and minimum distance d. Then*

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil.$$

If we apply directly the Griesmer bound to the linear code in our Theorem 4.1, we get:

COROLLARY 4.3 *Let $\Sigma = (\mathbf{S}, i)$ be a linear secret sharing scheme with secrets in $\mathbb{F}_q^k$ and shares in $\mathbb{F}_q$. Then*

$$n(\Sigma) - t(\Sigma) \geq \sum_{i=0}^{k-1} \lceil \frac{n(\Sigma) - r(\Sigma) + 1}{q^i} \rceil.$$

Moreover, we also have

$$r(\Sigma) \geq \sum_{i=0}^{k-1} \lceil \frac{t(\Sigma) + 1}{q^i} \rceil.$$

The second expression is obtained by using the same dualization techniques as in Theorem 3.26. One may argue at first sight that it is difficult to compare this bound with the general bounds in Section 3. In order to facilitate comparison, we proceed as follows. Note that the right hand sides of both expressions are sums of the form $\sum_{i=0}^{k-1} \lceil a_i \rceil$, for some real numbers $a_i > 0$. We will use the bound $\lceil a_i \rceil \geq a_i$ for the two first terms of the sums (we will assume $k \geq 2$) and $\lceil a_i \rceil \geq 1$ for the remaining terms, if any. After rearranging terms we obtain.

COROLLARY 4.4 *Let $\Sigma = (\mathbf{S}, i)$ be a linear secret sharing scheme with secrets in $\mathbb{F}_q^k$ and shares in $\mathbb{F}_q$. Suppose $k \geq 2$. Then*

$$r(\Sigma) - t(\Sigma) \geq \frac{n(\Sigma) - r(\Sigma) + 1}{q} + (k-1).$$

Moreover, we also have

$$r(\Sigma) - t(\Sigma) \geq \frac{t(\Sigma) + 1}{q} + (k-1).$$

REMARK 4.5 *After an adequate rearrangement of terms the first inequality in Corollary 4.4 can also be written as*

$$g(\Sigma) \geq \frac{n - t(\Sigma) + 1}{q} + f(q, k, n(\Sigma), t(\Sigma))$$

where

$$f(q, k, n, t) := k - 1 - \frac{n - t + 1}{q(q+1)}$$

which allows for a better comparison with Main Theorem 3.1. It is clear that the bound in Corollary 4.4 is stronger if and only if $f(q, k, n(\Sigma), t(\Sigma)) > 0$, i.e., if and only if

$$k > 1 + \frac{n(\Sigma) - t(\Sigma) + 1}{q(q+1)}$$

(although we remark that Corollary 4.4 is only valid for linear *schemes while Main Theorem 3.1 holds in the general case).*

Summing both inequalities in Corollary 4.4 we get

MAIN THEOREM 4.6 *Let $\Sigma = (\mathbf{S}, i)$ be a linear secret sharing scheme with secrets in $\mathbb{F}_q^k$ and shares in $\mathbb{F}_q$. Suppose $k \geq 2$. Then*

$$g(\Sigma) \geq \frac{n(\Sigma) + 2}{2q+1} + \frac{2q}{2q+1} k - \frac{2q}{2q+1}$$

REMARK 4.7 *The bound above can also be written as:*

$$g(\Sigma) \geq \frac{n(\Sigma)+2}{2q-1} + h(q,k,n(\Sigma))$$

where

$$h(q,k,n) := \frac{2q}{2q+1}\left(k - 1 - \frac{1}{q}\cdot\frac{n+2}{2q-1}\right).$$

Therefore the bound in Theorem 4.6 above is strictly stronger than the bound in Main Theorem 3.27 if

$$k > 1 + \frac{n(\Sigma)+2}{q(2q-1)}.$$

However, for $k = 1$, only our first bound gives a non-trivial result.

5 Arithmetic secret sharing

In [6], the notion of arithmetic secret sharing was introduced. This generalizes previous notions, such as the strongly multiplicative secret sharing schemes defined in [8].

DEFINITION 5.1 (POWERS OF AN n-CODE) *Let $m \in \mathbb{Z}_{>0}$. For $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^m$, their* product *$\mathbf{x} * \mathbf{x}' \in \mathbb{F}_q^m$ is defined as $(x_1x'_1, \ldots, x_mx'_m)$. Let d be a positive integer.*
If C is an n-code for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, then $C^{*d} \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ is the $\mathbb{F}_q$-linear subspace generated by all terms of the form $\mathbf{c}^{(1)} * \ldots * \mathbf{c}^{(d)}$ with $\mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(d)} \in C$. For $d = 2$, we use the abbreviation $\widehat{C} := C^{*2}$.

REMARK 5.2 (POWERING NEED NOT PRESERVE n-CODE) *Suppose $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ is an n-code for $\mathbb{F}_q^k$. It follows immediately that the secret-component in C^{*d} takes any value in $\mathbb{F}_q^k$.* However, *the shares-component in C^{*d}* need not *determine the secret-component uniquely. Thus, C^{*d}* need not be an n-code for $\mathbb{F}_q^k$.

DEFINITION 5.3 (ARITHMETIC SSS [6]) *Let n, t, d, r, k, be integers with $n, d, k > 0$, $1 \leq t < r \leq n$. An* (n,t,d,r)-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ (over $\mathbb{F}_q$) *is an n-code C for $\mathbb{F}_q^k$ such that*

(i) $t \geq 1$, $d \geq 2$,

(ii) $t(C) \geq t$,

(iii) C^{*d} *is in fact an n-code for $\mathbb{F}_q^k$ and*

(iv) $r(C^{*d}) \leq r$.

An $(n,t,1,r)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ is simply a LSSS over $\mathbb{F}_q$ with secret in $\mathbb{F}_q^k$, shares in $\mathbb{F}_q$ and which has t-privacy and r-reconstruction. When we consider an (n,t,d,r)-arithmetic secret sharing scheme with $d > 1$ as a LSSS, we can state a stronger reconstruction threshold for it.

THEOREM 5.4 *Let C be an (n,t,d,r)-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Then as an n-code for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, C has t-privacy and $(r-(d-1)t)$-reconstruction (i.e. it is also a $(n,t,1,r-(d-1)t)$-arithmetic secret sharing scheme).*

PROOF. We need to prove that $r(C) \leq (r-(d-1)t)$. Let $A \subseteq \mathcal{I}^*$ with $|A| = r-(d-1)t$. We will prove that $(\text{Ker } \pi_A) \cap C \subset (\text{Ker } \pi_0) \cap C$. Let $\mathbf{c} \in (\text{Ker } \pi_A) \cap C$.

Let $B_1, \ldots, B_{d-1}$ disjoint subsets of $\mathcal{I}^*$ of size t such that their are also disjoint with A. Also let $\mathbf{1}_k \in \mathbb{F}_q^k$ the all-one vector of length k. Since $t(C) \geq t$, for all $m = 1, \ldots, d-1$ there is $\mathbf{y}^{(m)} \in C$ with $(\mathbf{y}^{(m)})_{B_m} = \mathbf{0}$ and $(\mathbf{y}^{(m)})_0 = \mathbf{1}_k$, by Proposition 3.21.

Consider now the vector $\mathbf{w} = \mathbf{c} * \mathbf{y}^{(1)} * \cdots * \mathbf{y}^{(d-1)}$ which is in C^{*d} because it is the product of d words in C. If we write $D := A \cup B_1 \cup \cdots \cup B_{d-1}$ then it is clear that $\mathbf{w}_D = \mathbf{0}$, so $\mathbf{w} \in \text{Ker } \pi_D \cap C^{*d}$. But since $|D| = |A| + (d-1)t = r$ and $r(C^{*d}) \leq r$, then $D \in \Gamma_{C^{*d}}$. Therefore $\mathbf{w} \in \text{Ker } \pi_0 \cap C^{*d}$. But by construction $\mathbf{w}_0 = \mathbf{c}_0$ so $\mathbf{c} \in \text{Ker } \pi_0 \cap C$. △

REMARK 5.5 *Note that, since* $r(C) - t(C) \geq k$ *we have the bound* $r \geq dt + k$. *Particularly, if* $k = 1$, $d = 2$, $r = n - t$, *then* $3t \leq n - 1$.

But we can also apply our Main Theorems 3.27 and 4.6 in combination with Theorem 5.4 after which we obtain

COROLLARY 5.6 *Let* C *be an* (n, t, d, r)*-arithmetic secret sharing scheme for* $\mathbb{F}_q^k$ *over* $\mathbb{F}_q$. *Then*

$$r \geq dt + \frac{n+2}{2q-1} + h(q,k,n)_+$$

where

$$h(q,k,n)_+ := \max\left\{0, \frac{2q}{2q+1}\left(k - 1 - \frac{1}{q}\cdot\frac{n+2}{2q-1}\right)\right\}.$$

PROOF. In order to apply Main Theorem 3.27 we only need to be careful that $t(C) \geq 1$ and $r(C) \leq n - 1$. But note $t(C) \geq t \geq 1$ (by definition of arithmetic secret sharing scheme) and $r(C) \leq r - (d-1)t \leq n - 1$. In the case $k = 1$, we cannot use Main Theorem 4.6, however the corollary is still true because $h(q, 1, n)_+ = 0$ and then the statement is guaranteed by Main Theorem 3.27 alone. △

For the rest of the chapter we will consider the case where $d = 2$, $r = n - t$, known as strongly multiplicative secret sharing scheme. In addition we will restrict to the case $k = 1$, for which a notion that measures the largest possible value of t with respect to n asymptotically was defined in [5], where it was named asymptotical optimal corruption tolerance. We recall its definition next.

DEFINITION 5.7 *Let* C *be an* n*-code for* $\mathbb{F}_q$ *over* $\mathbb{F}_q$. *We define* $\widehat{t}(C)$ *to be the maximum value of* t *for which* C *is an* $(n, t, 2, n-t)$*-arithmetic secret sharing scheme for* $\mathbb{F}_q$.
Moreover we define $\widehat{\tau}(C) := \frac{3\widehat{t}(C)}{n(C)-1}$.
In addition, let

$$T_q(n) := sup\{\widehat{\tau}(C) : C \text{ is an } n - \text{code for } \mathbb{F}_q \text{ over } \mathbb{F}_q\}.$$

And we define

$$\widehat{\tau}(q) := \limsup_{n\to\infty} T_q(n),$$

the asymptotical optimal corruption tolerance *over* $\mathbb{F}_q$.

REMARK 5.8 *We have* $0 \leq \widehat{\tau}(q) \leq 1$. *In [5], it was proved that* $\widehat{\tau}(q) > 0$ *for every finite field* $\mathbb{F}_q$. *Previously, in [7], it had been proved that* $\widehat{\tau}(q) \geq 1 - \frac{4}{(\sqrt{q}-1)} > 0$ *for any* q *square,* $q \geq 49$.

Now Corollary 5.6 implies:

MAIN THEOREM 5.9 $\widehat{\tau}(q) < 1 - \frac{1}{2q-1} < 1$ *for all finite fields* $\mathbb{F}_q$. *Therefore* $0 < \widehat{\tau}(q) < 1$ *for all finite fields* $\mathbb{F}_q$.

In the remaining of this section we will provide better bounds for $\widehat{\tau}(q)$. We will use two different ideas: on the one hand applying the gap bounds in Main Theorem 3.27 to *both* C and $\widehat{C}$. On the other hand we will actually apply the bounds after *shortening* these codes.

LEMMA 5.10 *Let* $\Sigma = \Sigma(C)$ *be an arithmetic secret sharing scheme. Let* $\widehat{\Sigma} := \Sigma(\widehat{C})$. *There is an ideal* $\mathbb{F}_q$*-linear secret sharing scheme* Σ' *such that* $n(\Sigma') = n(\Sigma) - r(\Sigma) + 1$, $r(\Sigma') \leq r(\widehat{\Sigma}) - r(\Sigma) + 1$ *and* $t(\Sigma') \geq t(\Sigma)$.

PROOF.
We take A the largest set in $\mathcal{A}(\Sigma)$. Because Σ is perfect, $|A| = r(\Sigma) - 1$. Since $A \in \mathcal{A}(\widehat{\Sigma})$ as well, we can shorten $\widehat{\Sigma}$ by fixing the shares of A to be zero. We obtain another *linear* scheme Σ' which has as player set $\mathcal{J}^* = \mathcal{I}^* \setminus A$, and by Lemma 3.11, satisfies $r(\Sigma') \leq r(\widehat{\Sigma}) - r(\Sigma) + 1$. We prove now that $t(\Sigma') \geq t(\Sigma)$. Let $B \subseteq \mathcal{J}^*$ with $|B| = t(\Sigma)$. Let $\mathbf{x} \in \mathbb{F}_q^k$. Since $A \in \mathcal{A}(\Sigma)$, by Proposition 3.21, there is a word $\mathbf{c} \in C$ with $\mathbf{c}_0 = \mathbf{x}$ and $\mathbf{c}_A = \mathbf{0}$. On the other hand, since $B \in \mathcal{A}(\Sigma)$, there is a word $\mathbf{c}' \in C$ with $\mathbf{c}'_0 = \mathbf{1}$ and $\mathbf{c}'_A = \mathbf{0}$. Let $\mathbf{w} = \mathbf{c} * \mathbf{c}' \in \widehat{C}$. Note $\mathbf{w}_A = \mathbf{0}$, so the vector $\mathbf{w}_{J^*}$ is a share vector for $\mathbf{x}$ in the shortened scheme Σ'. Moreover $\mathbf{w}_B = \mathbf{0}$. Since we can repeat this argument for any $\mathbf{x} \in \mathbb{F}_q^k$, Proposition 3.21 implies $B \in \mathcal{A}(\Sigma')$. △

THEOREM 5.11 *We have*

$$\widehat{t}(C) \leq \frac{(q-1)^2}{3q^2-3q+1} n(C) + c(q)$$

for some constant $c(q)$ which depends on q but not on $n(C)$.

PROOF. Let $\widehat{t}(C) = \widehat{t}$. Then C is an $(n, \widehat{t}, 2, n-\widehat{t})$-arithmetic secret sharing scheme for $\mathbb{F}_q$. Let $\Sigma := \Sigma(C)$ and $\widehat{\Sigma} := \Sigma(\widehat{C})$. We then have that $t(\Sigma) \geq \widehat{t}$ and $r(\widehat{\Sigma}) \leq n - \widehat{t}$. We now consider the scheme Σ' promised by Lemma 5.10. By Main Theorem 3.1 applied to Σ' we have

$$r(\Sigma') - t(\Sigma') = g(\Sigma') \geq \frac{n(\Sigma') - t(\Sigma') + 1}{q}.$$

By combining this with the inequalities in Lemma 5.10 and the facts that $t(\Sigma) \geq \widehat{t}$ and $r(\widehat{\Sigma}) \leq n - \widehat{t}$ we get

$$(q-1)\, n(\Sigma) - (q-1)\, r(\Sigma) \geq (2q-1)\, \widehat{t} - 1.$$

We now apply Main Theorem 3.1 again, this time to Σ and again using $t(\Sigma) \geq \widehat{t}$ we get

$$\widehat{t} \leq \frac{(q-1)^2}{3q^2-3q+1} n(\Sigma) + \frac{1}{3q^2-3q+1}.$$

△

Now it is straightforward that

MAIN THEOREM 5.12 *For any finite field $\mathbb{F}_q$,*

$$\widehat{\tau}(q) \leq 1 - \frac{3q-2}{3q^2-3q+1}.$$

PROOF. Given an integer n, for any n-code C, the following holds. By Theorem 5.11, $3\widehat{t}(C) \leq \frac{3(q-1)^2}{3q^2-3q+1} n + O(1)$, so

$$\widehat{\tau}(C) \leq \frac{3(q-1)^2 n}{(3q^2-3q+1)(n-1)} + O(n^{-1}).$$

Hence $T_q(n) \leq \frac{3(q-1)^2 n}{(3q^2-3q+1)(n-1)} + O(n^{-1})$ and consequently

$$\widehat{\tau}(q) \leq \frac{3(q-1)^2}{3q^2-3q+1} = 1 - \frac{3q-2}{3q^2-3q+1}.$$

△

6 Acknowledgements

We would like to thank Joe Kilian and Noam Nisan for their kind permission to include their unpublished result and, for the first time, its (original) proof. We also thank them and Amos Beimel for their helpful clarifications about the history of that result [3].

References

[1] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution.* PhD. Thesis, Department of Computer Science, Technion, 1996.

[2] A. Beimel and M. Franklin. Weakly-private secret sharing schemes. *Proceedings of the 4th Conference on Theory of Cryptography, TCC 2007*, Springer Verlag LNCS, vol. 4392, pp. 253-272, 2007.

[3] A. Beimel, J. Kilian and N. Nisan. Personal communications, 2012.

[4] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, 48 (1979), pp. 313–317.

[5] I. Cascudo, H. Chen, R. Cramer, C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Finite Field. *Proceedings of 29th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5677, pp. 466-486, August 2009.

[6] I. Cascudo, R. Cramer, C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. *Advances in Cryptology - CRYPTO 2011*, Springer Verlag LNCS, Vol. 6841, pp. 685-705, August 2011.

[7] H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Proceedings of 26th Annual IACR CRYPTO*, Springer Verlag LNCS, vol. 4117, pp. 516-531, Santa Barbara, Ca., USA, August 2006.

[8] R. Cramer, I. Damgaard, and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. *Proceedings of 19th Annual IACR EUROCRYPT*, Brugge, Belgium, Springer Verlag LNCS, vol. 1807, pp. 316-334, May 2000.

[9] R. Cramer, S. Fehr. Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups. *Advances in Cryptology - CRYPTO 2002*, Springer Verlag LNCS, Vol. 2442, pp. 272-287, August 2002.

[10] J.H. Griesmer. A bound for error-correcting codes. *IBM J. Research Develop.*, vol. 4, pp. 532-542, 1960.

[11] M. Karchmer and A. Wigderson. On span programs. *Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pp. 102–111, IEEE, 1993.

[12] J. Kilian and N. Nisan. Unpublished result, 1990. Explained by Joe Kilian in an email dated Jan. 4, 1991 and addressed to Eyal Kushilevitz.

[13] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*(11th impression), North Holland, 2003.

[14] V. Pless and W. C. Huffman. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.

[15] A. Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612-613, 1979.