Polynomial Secret Sharing Schemes and Algebraic Matroids

Amos Beimel[1], Oriol Farràs[2], and Adriana Moya[2]

[1] Department of Computer Science, Ben Gurion University
[2] Universitat Rovira i Virgili, Tarragona, Spain
amos.beimel@gmail.com,{oriol.farras,adriana.moya}@urv.cat

Abstract. In a secret sharing scheme with polynomial sharing, the secret is an element of a finite field, and the shares are obtained by evaluating polynomials on the secret and some random field elements, i.e., for every party there is a set of polynomials that computes the share of the party. These schemes generalize the linear ones, adding more expressivity and giving room for more efficient schemes. To identify the access structures for which this efficiency gain is relevant, we need a systematic method to identify the access structure of polynomial schemes; i.e., to identify which sets can reconstruct the secret in the scheme. As a first step, we study ideal polynomial secret sharing schemes where there is a single polynomial for each party. Ideal schemes have optimal share size because the size of each share is the size of the secret.

Our goal is to generalize results of linear secret sharing schemes, i.e., schemes in which the shares are computed by applying linear mappings and the linear dependency of these mappings determines their access structures. To achieve this goal, we study the connection between the algebraic dependency of the sharing polynomials and the access structure of the polynomial scheme. Our first result shows that if the degree of the sharing polynomials is not too big compared to the size of the field, then the algebraic dependence of the sharing polynomials determines the access structure of the scheme. This contributes to the characterization of ideal polynomial schemes and establishes a new connection between families of ideal schemes and algebraic matroids.

Conversely, we ask the question: If we associate a polynomial with each party and the dealer, can we use these polynomials to realize the access structure determined by the algebraic dependency of the polynomials? Our second result shows that these access structures admit statistical schemes with small shares. Finally, we extend this result to the general case where each party may have more than one polynomial.

The first author is partially supported by ISF grant 391/21 and by ERC project NFITSC (101097959). The second and the third authors are supported by the grant 2021 SGR 00115 from the Government of Catalonia and by the project HERMES, funded by INCIBE and by the European Union NextGeneration EU/PRTR, and the project ACITHEC PID2021-124928NB-I00, funded by MCIN/AEI/10.13039/501100011033/FEDER, EU.

Table of Contents

1 Introduction

Secret sharing schemes are a cryptographic primitive designed to protect a secret value by distributing it into shares. In these schemes, the secret is held by the *dealer*, and each share is privately sent to a different party. A subset of parties is *authorized* if their shares determine the secret value. The *access structure* of a secret sharing scheme is the family of authorized subsets. A scheme is *perfect* if subsets of parties that are not authorized cannot obtain any information on the secret, in the information-theoretic sense. Secret sharing schemes were introduced by Blakley [20] and Shamir [61] in 1979, and are used to prevent the disclosure or the loss of the secret value in many different cryptographic applications (see [8], for example, for a list of applications). For these applications, there is a need for efficient schemes and, in particular, shares should be as short as possible. This leads to the problem of minimizing the share size (or the *information ratio*, which is the ratio between the size of the secret and the size of the largest share).

The most common secret sharing schemes are linear. However, most access structures require linear schemes with exponential share size [5,11,58]. This motivates the study of other families of schemes that can overcome this limitation. To address this goal, Paskin-Cherniavsky and Radune [57] defined secret sharing schemes with polynomial sharing; in such schemes, the secret is an element of a finite field and the shares are obtained by applying polynomials to the secret and some random field elements. These schemes were further studied in [15,12]. Polynomial secret sharing schemes generalize linear secret sharing schemes, adding more expressivity and giving room for more efficient schemes. Our goal in this work is to better understand polynomial secret sharing schemes and their relationship with the algebraic dependency of the sharing polynomials (trying to generalize similar concepts for linear secret sharing schemes).

1.1 Our Goals

In a linear secret sharing scheme, each party is associated with a set of vectors, i.e., the i-th party is associated with some vectors $v_{i,1} \ldots, v_{i,k_i} \in \mathbb{F}^{m+1}$ for some finite field $\mathbb{F}$ and $m > 0$. To share a secret $s \in \mathbb{F}$, the dealer picks uniformly random elements $r_1, \ldots, r_m \in \mathbb{F}$ and sends $v_{i,j} \cdot (s, r_1, \ldots, r_m)$ for $1 \leq j \leq k_i$ to the i-th party. Namely, each share contains k_i elements, and each element is a linear combination of the secret s and the random elements $r_1, \ldots, r_m$.

In a secret sharing scheme with polynomial sharing, or *polynomial secret sharing scheme*, the secret is an element of a finite field $\mathbb{F}$, and the shares are obtained by applying polynomials to the secret and some random field elements. That is, the i-th party is associated with some polynomials $P_{i,1}, \ldots, P_{i,k_i} \in \mathbb{F}[x_0, \ldots, x_m]$ for some $m, k_i > 0$, and the shares of a secret $s \in \mathbb{F}$ are generated by picking uniformly distributed randomness $r_1, \ldots, r_m \in \mathbb{F}$ and sending $P_{i,j}(s, r_1, \ldots, r_m)$ for $1 \leq j \leq k_i$ to the i-th party.

Linear schemes are perfect, and their access structure is determined by the vectors of the scheme: A subset of parties A is authorized if the vector $e =$

$(1, 0, \ldots, 0)$ is dependent on A's vectors. Hence, the search for a linear scheme for a given access structure can be translated into a linear algebra problem. These properties do not hold in the case of schemes with polynomial sharing. In general, they are not necessarily perfect, i.e., there might be sets of parties that can determine partial information on the secret. Given an access structure, we would like to know how to construct efficient polynomial schemes realizing it.

The first objective of this work is to provide a criterion to determine the access structure of perfect polynomial schemes. For that, we focus on the class of ideal schemes with polynomial sharing to take advantage of results on matroid theory and algebra.

In an *ideal* secret sharing scheme, the size of each share is equal to the size of the secret, and this is the best possible situation for a perfect scheme [46]. In this case, we say that its access structure is called *ideal* as well. Brickell and Davenport [22] proved that ideal access structures are determined by matroids. A matroid is a combinatorial structure generalizing linear spaces and cycles in undirected graphs. Namely, Brickell and Davenport proved that the minimal authorized subsets correspond to the circuits of a matroid containing the point $\{0\}$. In this case, we say that the access structure is a *port* of that matroid. Conversely, not all matroids determine ideal access structures [60]. The characterization of matroids that determine access structures with ideal schemes is an open problem. This connection between secret sharing schemes and matroids has been crucial in the search of positive and negative results about the existence of efficient secret sharing schemes, e.g., in lower bounds on the share size for general access structures [11,52], characterization of ideal multipartite and ideal weighted threshold access structures [17,35,37], and separation results for different secret sharing techniques [10,14,9]. For example, it is known that an access structure has an ideal linear secret sharing scheme if and only if the access structure is a port of a representable matroid [21]. We aim to extend this tight connection to the families of ideal polynomial schemes and matroids determined by polynomials.

The second objective of this work is to study the security of schemes with polynomial sharing. As mentioned above, polynomial secret sharing schemes are not perfect, in general. Some subsets of parties may have partial information about the secret (i.e., they are neither authorized nor forbidden), as shown in the following example.

Example 1.1. Consider the scheme with three parties in a finite field $\mathbb{F}_p$ with $p > 2$ where the share of the first party is $P_1(s, r) = r$, the share of the second party is $P_2(s, r) = s^2 + r$, and the share of the third party is $P_3(s, r) = s + r^2$. It does not have perfect correctness since the first and second party cannot fully recover the secret, i.e., they can determine s^2, so they have two options for the secret. Moreover, the third party has partial information about the secret: that is, there are $\frac{p+1}{2}$ possible values of the secret. However, note that the same polynomials over binary fields lead to a perfect secret sharing scheme, more concretely, the 2-threshold secret sharing scheme. △

We analyze the properties of these schemes and provide methods to transform them into schemes with strong security guarantees. We prove that the algebraic dependence of the polynomials is important in achieving the above goals. We say that a set of polynomials $\{P_1, \ldots, P_k\}$ with $P_i \in \mathbb{F}[x_0, \ldots, x_m]$ is algebraically dependent over $\mathbb{F}$ if there exists a non-zero polynomial $Q \in \mathbb{F}[y_1, \ldots, y_k]$ satisfying that $Q(P_1, \ldots, P_k) = 0$. This polynomial Q is called the annihilator of $P_1, \ldots, P_k$. We say that a polynomial P_0 depends on a set of polynomials $\{P_1, \ldots, P_k\}$ if there exists an annihilator of $\{P_0, \ldots, P_k\}$ that depends on the first coordinate.

Example 1.2. Consider the polynomials $P_0(x_1, x_2) = x_1$, $P_1(x_1, x_2) = x_1^2 + x_2$, $P_2(x_1, x_2) = x_1 + x_2^2$, and $P_3(x_1, x_2) = x_1 x_2$ over $\mathbb{F}_4[x_1, x_2]$. Observe that P_0, P_1, P_2 are algebraically dependent over $\mathbb{F}_4$ because $Q(y_1, y_2, y_3) = y_1^4 + y_1 + y_2^2 + y_3$ is the annihilator of P_0, P_1, P_2 since

$$Q(P_0, P_1, P_2) = x_1^4 + x_1 + (x_1^2 + x_2)^2 + x_1 + x_2^2 = 0.$$

The polynomials P_0, P_1, and P_3 are also algebraically dependent since the polynomial $R(y_1, y_2, y_3) = y_1^3 + y_1 y_2 + y_4$ is an annihilator for P_0, P_1 and P_3 as

$$R(P_0, P_1, P_3) = x_1^3 + x_1(x_1^2 + x_2) + x_1 x_2 = 0.$$

Consequently, P_0 is dependent on $\{P_1, P_2\}$ and on $\{P_1, P_3\}$. Analogously, it can be proved that P_0 is dependent on $\{P_2, P_3\}$. △

1.2 Our Results

Our work unveils algebraic properties of polynomial secret sharing schemes that are important for the characterization of their access structure and for the construction of schemes with strong security guarantees. In a scheme with polynomial sharing, we can define an access structure Γ by the algebraic dependence of the polynomials as follows: A subset is in Γ if the secret, i.e., the polynomial $P_0(s, r_1, \ldots, r_m) = s$ depends algebraically on the polynomials of these parties.

Example 1.3. Consider the polynomials P_0, P_1, P_2, P_3 of the Example 1.2 over $\mathbb{F}_4[x_1, x_2]$. The access structure defined by the algebraic dependence of the polynomials P_1, P_2, P_3 with respect to $P_0(x_1, x_2) = x_1$ is a 2-out-of-3 threshold access structure since the polynomial P_0 depends algebraically on every subset of two polynomials in $\{P_1, P_2, P_3\}$. △

We present our results below. First, we present a generalization of a result of ideal linear secret sharing schemes to the ideal polynomial case. Namely, we show that the access structure of ideal polynomial schemes is Γ under certain restrictions on the degree of the polynomials. Later, we give constructions of schemes with statistical security for the access structures defined by the algebraic dependence of some polynomials.

Characterization of the Access Structure of Ideal Polynomial Secret Sharing Schemes. Recall that ports of linearly representable matroids admit ideal secret sharing schemes, and the access structure of an ideal linear scheme is the port of the associated linear matroid [22,21]. This connection cannot be directly generalized to polynomial schemes, as there are ideal polynomial schemes whose access structures do not coincide with the access structure determined by the algebraic dependence of the sharing polynomials [53,18] (see Example 1.10 and Example 4.8). The main contribution of this work is that we circumvent these negative results. We show that if the field is large enough, then the access structure of an ideal polynomial scheme is determined by the algebraic dependence of the polynomials.

We prove two incomparable results in our work. Our first theorem considers schemes with polynomial sharing (as discussed above) and polynomial reconstruction, i.e., for every authorized set A holding shares $(\mathsf{sh}_i)_{i\in A}$ for the secret s, there is a polynomial Q_A such that $Q_A((\mathsf{sh}_i)_{i\in A}) = s$.

Theorem 1.4. *Let Σ be an ideal polynomial secret sharing scheme over a field $\mathbb{F}_q$. Let d_1 and d_2 be the degrees of the sharing and reconstruction polynomials, respectively. If $q > \max\{d_1^{n+1}, d_1 d_2\}$, then the access structure of Σ is determined by the algebraic dependence of the sharing polynomials.*

In the above theorem, there are no restrictions on the characteristic of the field (e.g., it applies to $\mathbb{F}_{2^\ell}$ for large enough ℓ). In this result, a restriction on the degree of the polynomials is needed. Even though the access structure of a polynomial scheme is perfect, there are cases where the access structure determined by the algebraic dependence and the polynomial mappings are different. This is discussed in Section 4, where we show that there exist schemes with $q = d_1^n$ where the statement does not hold. See also Example 1.10.

In the case that the field is prime, we are able to guarantee that the access structure is the one determined by the algebraic dependence of the sharing polynomials without any restriction on the degree of the reconstruction polynomials.

Theorem 1.5. *Let Σ be an ideal perfect secret sharing scheme with polynomial sharing in a field of prime order p. If the sharing polynomials are of degree at most d and $p = \Omega(nd^{8n})$, then the access structure of Σ is determined by the algebraic dependence of the sharing polynomials.*

We can restate the previous theorem in terms of the algebraic matroid defined by the sharing polynomials and the polynomial $P_0(s, r_1, \ldots, r_m) = s$, namely, a set A is dependent if and only if the polynomials $\{P_i\}_{i\in A}$ are algebraically dependent. This result generalizes the connection between ideal linear schemes and representable matroids to the algebraic context.

Corollary 1.6. *Let Σ be an ideal secret sharing scheme satisfying the conditions of Theorem 1.4 or Theorem 1.5, then the access structure of Σ is a port of the algebraic matroid represented algebraically by the sharing polynomials.*

We next study multi-linear schemes, which generalize the linear ones by considering secrets that are vectors of elements in a finite field. We show that every multi-linear scheme can be described as a polynomial scheme whose sharing polynomials are q-polynomials. These are polynomials over $\mathbb{F}_{q^r}$ where the monomials are powers of a single variable, and the exponent is a power of q. For example, $P_1(x_0, x_1, x_2) = x_0 + x_1 - x_2^q$ and the rest of polynomials in Example 4.8 are q-polynomials.

Constructing Statistical Secret Sharing Schemes from Polynomials. We next discuss the converse direction, considering the general case where each party may have more than one polynomial. We define the access structure Γ as the family of subsets A satisfying that P_0 is dependent on $\cup_{i\in A}\{P_{i,1}, \ldots, P_{i,k_i}\}$. Then the question is: Can Γ be realized by a secret sharing scheme with small shares?

We give positive answers to this question in a weaker security setting, presenting two constructions of schemes with statistical security. A statistical scheme with security parameter ℓ satisfies the following: Authorized subsets may fail to reconstruct the secret with negligible probability of error in ℓ, and unauthorized subsets may obtain some amount of information about the secret that is negligible in ℓ.

Theorem 1.7 (Informal). *Let n, d, t be positive integers and let p be a prime. Assume that each party $1 \leq i \leq n$ has k_i polynomials of degree at most d over $\mathbb{F}_p$, and let $k = \sum_{i=1}^{n} k_i$. Let Γ be the access structure on $\{1, \ldots, n\}$ determined by these polynomials as above.*

If $t > \sum_{i\in A} k_i$ for every $A \notin \Gamma$ and $p > d^{\Omega(t^2)}$, then there exists a statistical scheme Σ realizing Γ with total share size $k\ell \log p$ and secret size $\Theta(\ell \log p)$, where ℓ is the security parameter.

The previous result applies to polynomial schemes, where the sharing polynomials are defined over a field $\mathbb{F}_p$ for a prime p. Notice that the resulting share size is polynomial in the number of parties only when k is polynomial and d is small. As discussed in Section 5, these schemes are built in two stages. We first consider the scheme in which the shares are computed by evaluating the sharing polynomials directly. This scheme provides very weak privacy. In the second stage, we apply a black-box transformation that guarantees statistical security.

In our last result, we are able to overcome the limitation that the polynomials are defined over a prime field. For that, we explore a different construction that does not have any restriction on the finite field. In this case, we cannot bound the share size of the resulting scheme; however, we can bound the information ratio.

Theorem 1.8 (Informal). *Let n, k be positive integers and let $\mathbb{F}$ be a field. Assume that each party $1 \leq i \leq n$ has polynomials over $\mathbb{F}$, and there are k polynomials in total. Let Γ be the access structure determined by these polynomials as above. Then there exists a statistical scheme realizing Γ with total information ratio that tends to k when the security parameter increases.*

To prove this result, we first consider the case in which each party has only one polynomial. For this case, we show that this scheme exists by applying a result of matroid theory. Namely, we prove the following result and then extend it to the general case.

Theorem 1.9. *Let Γ be a port of an algebraic matroid over a finite field. The access structure Γ admits a statistical secret sharing schemes with information ratio tending to* 1 *when the security parameter increases.*

As a consequence of this result, we observe that the optimal information ratio of statistical schemes is not preserved by duality. The dual of an access structure Γ on a set E is $\Gamma^* = \{A \subseteq E : E \setminus A \notin \Gamma\}$. The question if the optimal information ratio for perfect schemes is preserved by duality is still open.

1.3 Our Techniques

We divide this section in three parts. First, we explain the techniques used in Theorem 1.4 and Theorem 1.5 for the characterization of the access structure of ideal polynomial schemes. Then, we present the techniques used in Theorem 1.7 and Theorem 1.8 to construct statistical schemes.

Characterization of the Access Structure of Ideal Polynomial Secret Sharing Schemes. In Theorem 1.4, we prove that under some conditions, the access structure of an ideal polynomial scheme with polynomial sharing and polynomial reconstruction is indeed the one defined by the algebraic dependence of the polynomials. To prove this theorem, we consider an ideal polynomial secret sharing scheme over $\mathbb{F}_q$ realizing an n-party access structure Γ. Let $P_0(s, r_1, \ldots, r_m) = s$ and let P_i be the polynomial that computes the share of the i-th party for $1 \leq i \leq n$. We want to prove that a set of parties A can reconstruct the secret if and only if the polynomial P_0 algebraically depends on the polynomials $\{P_i\}_{i \in A}$.

First, assume that a set of parties A can reconstruct the secret. Since the there is polynomial reconstruction, there exists a polynomial $Q_A(y_1, \ldots, y_{|A|})$ such that $Q_A(\{P_i(s, r_1, \ldots, r_m)\}_{i \in A}) = s$ for every $s, r_1, \ldots, r_m \in \mathbb{F}_q$.

Notice that over finite fields, this does not imply that $Q_A(\{P_i\}_{i \in A}) = P_0$, as there are non-zero polynomials that evaluate to zero on all the points (e.g., the polynomial $x^q - x$ over the field $\mathbb{F}_q$). Let R be the polynomial $R(s, r_1, \ldots, r_m) = Q_A(\{P_i(s, r_1, \ldots, r_m)\}_{i \in A}) - P_0(s, r_1, \ldots, r_m)$.

By the conditions of Theorem 1.4, the degree of the sharing polynomials is at most d_1 and the degree of the reconstruction polynomial is at most d_2; hence the degree of $R(s, r_1, \ldots, r_m)$ is at most $d_1 \cdot d_2 < q$. By the Schwartz–Zippel lemma (also called DeMillo–Lipton–Schwartz–Zippel lemma), any polynomial that is not identically zero and has degree less than q has at least one root. Thus, $R(s, r_1, \ldots, r_m)$ is identically zero, i.e., P_0 algebraically depends on $\{P_i\}_{i \in A}$.

Second, assume that P_0 depends algebraically on $\{P_i\}_{i\in A}$; without loss of generality, assume that A is a minimal set satisfying this property (in particular, $\{P_i\}_{i\in A}$ are independent). In other words, there exists a non-zero polynomial $F(y_0, y_1, \ldots, y_{|A|})$ such that $F(s, \{P_i\}_{i\in A}) = 0$; i.e., F is an annihilator polynomial. By Beecken, Mittman, and Saxena [7], there exists such an annihilator polynomial of degree at most d_1^n. We show that this implies that there is a secret s and shares $(\mathsf{sh}_i)_{i\in A}$ that have positive probability for the secret s and have probability 0 for the secret 0. Therefore, the parties in A have some partial information on the secret. Since each set of parties is either forbidden (i.e., has no information on the secret) or authorized (i.e., can reconstruct the secret), the set A must be authorized and the theorem follows.

In Theorem 1.5, we prove a similar result but without requiring polynomial reconstruction. However, the result requires that the scheme is defined over a large prime field. This is because we use results of Dvir, Gabizon, and Wigderson [32] about rank extractors for polynomial sources. Namely, we use the property that, for large enough prime fields, the output of algebraically independent polynomials is close to having the min-entropy of uniformly distributed random variables. This allows to connect the information theoretic property of the ideal scheme to an algebraic relation between the sharing polynomials.

It is worth noticing that, for fields of large enough characteristic, the algebraic rank of a set of polynomials can be efficiently computed by means of the Jacobian rank of the polynomials [7], which is computed from their partial derivations. Under the conditions of Theorem 1.4 and Theorem 1.5, the characteristic is large enough, and this property holds. This simplifies the search of authorized subsets given a set of polynomials.

The relations we establish in Theorem 1.4 and Theorem 1.5 between ideal polynomial schemes and the algebraic dependence of the sharing polynomials can be rephrased using matroids defined by polynomials, which is a special class of connection between ideal polynomial schemes and algebraic matroids. This extends the known connection of these two objects in the linear case.

In fact, using this connection we observe that the bound on the degree of the sharing and reconstruction polynomials in Theorem 1.4 is supported by the fact that there exist multi-linear matroids that are not algebraically representable [18]. If we consider the scheme determined by one of these multi-linear matroids $\mathcal{M}$, we get an ideal multi-linear scheme Σ whose access structure is a port of $\mathcal{M}$. Multi-linear schemes are actually schemes with polynomial sharing (see Remark 3.2). Therefore, the access structure of this polynomial scheme is not a port of an algebraic matroid. In particular, the matroid determined by the algebraic dependence on these polynomials is not $\mathcal{M}$.

Moreover, there are cases where the matroid is algebraic but the algebraic representation does not define the proper access structure of the scheme. Next, we see an example of a polynomial scheme, where the restriction on the degree is not satisfied and the access structure of the scheme is not the one determined by the algebraic dependence of the polynomials.

Example 1.10. Consider the polynomial scheme with two parties defined by the following polynomials over $\mathbb{F}_4$: $P_0(x_0, x_1, x_2) = x_0$, $P_1(x_0, x_1, x_2) = x_1 + x_2^2$, and $P_2(x_0, x_1, x_2) = x_0 + x_1^2 + x_2$. Each party does not have any information about the secret, and the two parties together can reconstruct the secret using the polynomial $Q(y_1, y_2) = y_1^2 + y_2$. Notice that for every $(s, r_1, r_2) \in \mathbb{F}_4^3$,

$$Q(P_1(s, r_1, r_2), P_2(s, r_1, r_2)) = (r_1 + r_2^2)^2 + s + r_1^2 + r_2 = s + r_2 + r_2^4,$$

and it is equal to r_0 because $r_2 + r_2^4 = 0$ for every $r_2 \in \mathbb{F}_4$. Hence, it is an ideal secret sharing scheme.

Nevertheless, if we analyze the access structure determined by the algebraic dependence of the polynomials, we get that the set of the two parties is unauthorized since the polynomial P_0 does not depend algebraically on the polynomials P_1 and P_2. To prove it we can apply the Jacobian criteria (see Example 4.8 and Section 5.2). Then, the access structure of the scheme and the one defined by the algebraic dependence do not coincide. In fact, the algebraic matroid defined by P_0, P_1, and P_2 is the uniform matroid with rank 3. △

In Example 4.8 we generalize the previous one by giving a scheme on n parties with sharing polynomials over $\mathbb{F}_{q^n}$ of degree $d_1 = q$ and reconstruction polynomials of degree q^{n-1}, that does not realize the access structure determined by the algebraic dependence. This justifies the bound on the degree of the sharing and reconstruction polynomials of Theorem 1.4.

Statistical Secret Sharing Schemes from Polynomial Schemes. As discussed above, in the second part of this work we are interested in constructing schemes with small shares for the access structure determined by the algebraic dependence of polynomials. Recall that this access structure Γ is defined as the family of subsets A satisfying that P_0 is dependent on $\cup_{i \in A}\{P_{i,1}, \ldots, P_{i,k_i}\}$. For that, we use different techniques that combine some classic results about polynomials over finite fields and more modern results about algebraic matroids.

First, we consider the straightforward option of evaluating the polynomials. That is, we consider the scheme where the i-th party receives $P_{i,1}(s, r_1, \ldots, r_m)$, $\ldots, P_{i,k_i}(s, r_1, \ldots, r_m)$ as shares for the secret s. Under the hypothesis of Theorem 1.7, we observe that the subsets in Γ can nearly determine the secret, in average; namely, we show that the entropy of the secret given the shares of subsets in Γ is very low. Conversely, the subsets not in Γ have almost no information about the secret, in average. The schemes, like the ones we get, where authorized subsets always have more information about the secret than those that are not authorized are called *partial* secret sharing schemes.

The information ratio of the resulting schemes is close to a constant, which is determined by the distribution of the outputs of the polynomial mappings. This constant depends on the number of possible outputs of the mappings; we bound this number by using Wooley's Theorem [63] and the Schwartz-Zippel Lemma [30].

We transform the partial secret sharing scheme into a scheme with statistical security by using a black-box transformation of Jafari and Khazaei [43] that is

based on wiretap channels techniques. In the resulting statistical scheme, the size of the shares and the secret increases linearly with the security parameter, while the information ratio of each party i remains bounded and close to k_i (the number of polynomials given to i-th party).

As a consequence of this result, we show that algebraic matroids represented with low degree polynomials over large enough prime fields admit statistical schemes with information ratio bounded by a constant. Again, since the results are for large prime fields, we can use the Jacobian criteria to compute the rank of the polynomials, and determine if a subset of parties is authorized or not by computing the rank of a matrix.

Partial secret sharing schemes do not provide the security required for many cryptographic applications, so we transform them into schemes with statistical security. However, we have found partial schemes with good properties. Namely, we have found ramp schemes whose trade-off between share size and the gap is almost optimal (see Example 5.13).

Statistical Secret Sharing Schemes from Algebraic Varieties. In Theorem 1.8, we show that we can improve Theorem 1.7 constructing statistical schemes for Γ with information ratio close to one even if the field is not prime. However, in this scheme we cannot provide bounds on the share size.

For this result, we introduce a new family of secret sharing schemes whose shares are determined by points on an algebraic variety. The study of these schemes is motivated by recent results of Matúš [54]. Next, we present these schemes as a generalization of the ideal linear schemes. In an ideal linear scheme, the i-th party is associated with a vector $v_i \in \mathbb{F}^m$. The shares of the i-th party are $v_i \cdot x$ for some $x \in \mathbb{F}^m$. If we consider the matrix whose columns are the vectors v_i, we get the generator matrix of a linear code C whose codewords are $(v_0 \cdot x, \ldots, v_n \cdot x)$, the shares of the scheme. Analogously, we can define the family of vectors of shares of the scheme by means of the dual code $C^\perp$. By definition of $C^\perp$, a vector $y = (y_0 \ldots, y_n) \in \mathbb{F}^{n+1}$ is a vector of shares of the scheme if and only if $\lambda \cdot y = 0$ for every $\lambda \in C^\perp$. To share a secret s, it is enough to pick uniformly at random one vector of this family with $y_0 = s$.

Our construction generalizes the previous one as follows. Recall that an annihilator of polynomials $P_1, \ldots, P_k \in \mathbb{F}[x_0, \ldots, x_m]$ is a polynomial $Q \in \mathbb{F}[y_1, \ldots, y_k]$ that satisfies $Q(P_1, \ldots, P_k) = 0$. Given a set of polynomials $P_0, \ldots, P_n$, we consider the family of their annihilators I, which plays the role of the dual code in the scheme presented above.

Then, we consider the family of points in $\mathbb{F}^{n+1}$ that are zeroes of all polynomials in I. That is, we consider the points $(y_0, \ldots, y_n) \in \mathbb{F}^{n+1}$ such that $Q(y_0, \ldots, y_n) = 0$ for every $Q \in I$. In the context of algebraic geometry, this family of points is called the algebraic variety determined by I and is denoted by $V(I)$. In our scheme, we pick a point in the algebraic variety uniformly at random. The resulting scheme is not a scheme with polynomial sharing, in general. In particular, it differs from the scheme whose sharing polynomials are $P_0, \ldots, P_n$. In terms of algebraic geometry, this difference is natural because the

number of points in $V(I)$ may be higher than the number of possible outputs of the polynomials in I.

In [54], Matúš defined sequences of algebraic varieties defined over extensions of $\mathbb{F}$. That is, the families of points in extensions $\mathbb{K}$ of $\mathbb{F}$ that are zeroes of all polynomials in I. Matús studied the random variables that are obtained by taking uniform distributions over these varieties, showing information-theory properties of algebraic matroids (see Section 6 for more details). The proof of these results uses the Lang-Weil bound [49] to bound the number of points in each of these algebraic varieties.

We adapt these results to show that, taking a large enough extension of the field, these random variables define partial secret sharing schemes for the access structure Γ determined by $P_0, \ldots, P_n$. Then, we extend this result to the case where each party has more than one polynomial.

Once we have these partial secret sharing schemes, we can use the black-box transformation mentioned above to convert them into statistical ones. Moreover, we use another construction to obtain schemes with a smaller information ratio. Jafari and Khazaei [43] showed that, given a sequence of partial schemes whose privacy and correctness are perfect in the limit and their information ratio converges to a constant, it is possible to create a statistical secret sharing scheme whose information ratio tends to that constant by increasing the security parameter.

As a side result, we observe that the optimal information ratio of statistical schemes is not preserved by duality (Theorem 7.1). This is done by applying the construction of statistical schemes for access structures defined by the algebraic dependence of polynomials (Proposition 5.2) and some previous results on duality properties of matroids [28,45].

1.4 Related Work

Ideal secret sharing schemes and matroids. Brickell and Davenport [22] proved that the access structure of an ideal secret sharing scheme determines a matroid, and that the access structure is indeed a port of this matroid. Conversely, only ports of certain matroids admit ideal schemes, and these matroids are called *entropic* [53,62]. Matroids that admit linear or multi-linear representations are entropic. Matúš showed that there exist algebraic matroids that are not entropic [53], and Ben-Efraim showed that there exist entropic matroids that are not algebraic [18], and the characterization of entropic matroids is still an open problem.

The connection between ideal schemes and matroids provides mathematical tools for the construction of ideal schemes and, among particular families of access structures, to characterize the ones that admit ideal schemes (e.g. [10,17,36,37]). Farràs proved that almost all matroid ports require linear schemes with share size exponential in the number of parties [33]. However, the best lower bounds on the information ratio for general schemes realizing matroid ports are just constant [6,42]. Martí-Farré and Padró showed that for

access structures that are not matroid ports, the information ratio of any secret sharing scheme is at least 3/2 [52].

Polynomial secret sharing schemes. Liu, Vaikuntanathan, and Wee [51] constructed two-server Conditional Disclosure of Secrets (CDS) protocols, where the sharing and reconstruction functions are quadratic polynomials. CDS protocols are basically equivalent to secret sharing schemes for the so-called forbidden access structures. Paskin-Cherniavsky and Radune [57] defined polynomial secret sharing schemes, studied the randomness complexity of these schemes, and gave an exponential upper bound on the randomness complexity. Beimel, Othman, and Peter [15] studied the family of schemes and conditional disclosure of secrets protocols with low degree polynomial reconstruction, finding lower bounds on the share size. They also show that, under plausible assumptions, secret sharing schemes with polynomial sharing are more efficient than secret sharing schemes with polynomial reconstruction. They provided constructions of secret sharing schemes with quadratic sharing and reconstruction, i.e., by polynomials of degree two, whose share size improve the best upper bound on the share size for linear schemes. This line of work was continued in [12], providing secret sharing schemes with polynomial reconstruction of degree d for general access structures, with share size decreasing with d.

Polynomial sources and rank extractors. Dvir, Gabizon, and Wigderson introduced polynomial sources [32], a class of distributions obtained by evaluating some low-degree polynomials on a uniform input. With polynomial sources, they constructed deterministic randomness extractors, generalizing previous extractors from affine sources. They proved that algebraic independence is related to the min-entropy of the polynomial sources. For that, they used a relation between the rank of the polynomials and the rank of the corresponding Jacobian matrix and Wooley's theorem to get a lower bound on the entropy of a polynomial source. Later, Dvir [31] extended this work by considering sources that are distributed uniformly on an algebraic variety. In a different context, Matúš also studied the entropy of these random variables [54]. Beecken, Mittman, and Sexena [7] gave a bound on the degree of the annihilator polynomial of some set of dependent polynomials, improving previous bounds in [32,47]. The well-known Schwartz-Zippel lemma bounds the number of zeroes of a polynomial in terms of its degree. This lemma was proved in [30] but it also appeared in [66] and [59]. We use results in [7,32,54] to approximate the entropy of polynomial sharings, and our generalization from linear to polynomial schemes is analogous to their generalization from affine to polynomial sources.

1.5 Discussion

Upper and lower bounds for polynomial schemes. For the class of linear secret sharing schemes, the best upper bound on the share size is $2^{0.7563n}$ [1,2,3,4,50], and the best lower bound is $2^{0.5n}$ [5]. For schemes with polynomial reconstruction, there are upper and lower bounds on the share size that depend on the

degree of polynomials [12,16]. The best upper bound for secret sharing schemes with quadratic sharing is $2^{0.705n}$ [16] and it is not known how to improve the share size taking higher degree polynomials. The best lower bound we have is $\Omega(n/\log n)$ [27], which holds for arbitrary secret sharing schemes. The fact that the randomness of polynomials can be arbitrarily large hinders the use of counting arguments to prove lower bounds on the share size.

Schemes from Algebraic Varieties. When proving Theorem 1.8, we worked with a class of secret sharing schemes that was not explicitly considered before, the ones whose shares are the points of an algebraic variety. These schemes generalize the linear ones, because the shares of linear schemes are points in an algebraic variety determined by polynomials of degree one. We have seen that, increasing the degree of these polynomials, we get more expressivity, being able to get statistical schemes with information ratio close to one for access structures that do not admit ideal linear schemes. Also, these schemes may be attractive for applications where non-linearity is a requirement, e.g., for robust secret sharing schemes and algebraic manipulation detection codes [26], which are used to check the integrity of the shares.

Construction of statistical schemes. The statistical secret sharing schemes in Theorem 1.7 and Theorem 1.8 are built with a generic transformation from partial secret sharing schemes to statistical schemes [43]. These statistical schemes could be improved by using specific properties of the polynomials. In the case of Theorem 1.8, we do not have bounds on the size of the share and the secret. Improving the Lang-Weil bound on the number of points of algebraic varieties [49] could provide better bounds on the size of the share and the secret.

Duality. Given a linear scheme for an access structure, it is possible to build a linear scheme with the same share size for the dual access structure [41,38,34]. It is not known if this property can be extended to secret sharing schemes with polynomial sharing or reconstruction, or to secret sharing schemes in general. It is not known if the class of algebraic matroids and the class of entropic matroids are closed by duality. The optimal information ratio of statistical secret sharing schemes is not closed by duality, in general (see Theorem 7.1). However, it is still not known if the optimal information ratio of perfect secret sharing schemes is closed by duality.

1.6 Organization

In Section 2, we present preliminaries on secret sharing schemes, matroids, and polynomials over finite fields. In Section 3, we prove the first results of this work, Theorems 1.4 and 1.5. In Section 4 we introduce the family of q-polynomials. Then, in Section 5, we prove Theorem 1.7. Finally, in Section 6, we prove Theorem 1.8 and Theorem 1.9. Supplementary material, including background definitions, proofs, technical details, and observations, is presented in the appendix.

2 Preliminaries

We present the preliminaries of this work in three subsections. The first one is dedicated to secret sharing schemes, the second one is dedicated to matroids, and the third one is dedicated to polynomials.

We denote the power set of a set E by 2^E. The statistical distance between random variables X and Y is defined as $\mathsf{SD}(X,Y) = \frac{1}{2}\sum_x |\mathsf{Pr}[X=x] - \mathsf{Pr}[Y=x]|$, and the Shannon entropy of a random variable X is defined as $H(X) = \sum_x \mathsf{Pr}[X=x] \log 1/\mathsf{Pr}[X=x]$, where the sum is taken over the support of X.

2.1 Secret Sharing Schemes

In this work, we need to deal with secret sharing schemes with different security notions. In this section, we present the definition of perfect secret sharing schemes (from [8]). Afterwards, we present the class of polynomial secret sharing schemes. Later in this work, in Section 5.1, we define another definition of security for the schemes, the statistically security (from [13]). Other notions needed for intermediate results, are provided in the Appendix A.1.

Definition 2.1. *For a set of n parties, a family Γ of subsets of $\{1,\ldots,n\}$ is called monotone if $A \in \Gamma$ and $A \subseteq B$ implies $B \in \Gamma$. An* access structure *is a monotone collection of subsets of $\{1,\ldots,n\}$. Sets in Γ are called* authorized *and sets not in Γ are called* forbidden.

Definition 2.2 (Secret Sharing Scheme). *Let K be a finite set of secrets, $|K| \geq 2$. A* secret sharing scheme *is a pair $\Sigma = \langle \Pi, \mu \rangle$, where μ is a probability distribution over some finite set R, and Π is a mapping from $K \times R$ to a set of n-tuples $K_0 \times K_1 \times \ldots \times K_n$, where K_i is called the share-domain of player i. A dealer distributes a secret $s \in K$ by first computing a vector of shares $\Pi(s,r) = (\mathsf{sh}_1, \ldots, \mathsf{sh}_n)$, and then giving sh_i to the party i. We say that the scheme $\Sigma = \langle \Pi, \mu \rangle$ is a secret sharing scheme realizing an access structure Γ if the following two requirements hold:*

Correctness: *For any authorized set $A \in \Gamma$, there exists a reconstruction function $\textsc{Recon}_A$ such that for every secret $s \in K$,*

$$\mathsf{Pr}[\textsc{Recon}_A(\Pi_A(s,r)) = s] = 1,$$

where $\Pi_A(s,r)$ is the restriction of $\Pi(s,r)$ to its A-entries.

Perfect privacy: *For any forbidden set $B \notin \Gamma$, for every two secrets $a, b \in S$, and for every possible vector of shares $\langle \mathsf{sh}_j \rangle_{j \in B}$,*

$$\mathsf{Pr}[\Pi_B(a,r) = \langle \mathsf{sh}_j \rangle_{j \in B}] = \mathsf{Pr}[\Pi_B(b,r) = \langle \mathsf{sh}_j \rangle_{j \in B}].$$

We define the the share size *of party j as $\log |K_j|$, the* share size *of the scheme as $\max_{1 \leq j \leq n}\{\log |K_j|\}$, and the* information ratio *of the scheme as*

$$\sigma(\Sigma) = \frac{\max_{1 \leq i \leq n} \log |K_i|}{\log |K_0|}.$$

Definition 2.3 (Ideal Secret Sharing Schemes and Ideal Access Structures). *We say that a secret sharing scheme Σ is* ideal *if $\sigma(\Sigma) = 1$, i.e., the size of the domain of shares of each party is the size of the domain of secrets. We say that an access structure is ideal if there is an ideal secret sharing scheme realizing it (with some finite domain of secrets).*

Next we define the family of schemes that are the subject of the study of this work, polynomial secret sharing schemes.

Definition 2.4 (Polynomial Secret Sharing Schemes). *Let $\mathbb{F}$ be a finite field. A secret sharing scheme with* polynomial sharing *$\Sigma = \langle \Pi, \mu \rangle$ is a secret sharing scheme where $S = \mathbb{F}$ is the domain of secrets, $R = \mathbb{F}^m$ is the randomness space for some $m > 0$, and μ is the uniform distribution. The i-th party's share is*

$$\Pi(s, r)_i = ((P_{i,1}(s, r), \ldots, P_{i,k_i}(s, r))$$

for some $k_i > 0$, where each $P_{i,j}(s, r)$ is a multivariate polynomial over $\mathbb{F}$. We say that a scheme has polynomial reconstruction *if for every authorized set A, the reconstruction function RECON_A is a polynomial that outputs s when evaluating on the shares $P_{i,j}(s, r)$ of $i \in A$.*

Other definitions of polynomial schemes [12] consider a set of secrets in $S \subseteq \mathbb{F}^k$ for some $k \geq 1$. In this work, we decided to set $S = \mathbb{F}$ because our work is focused on schemes with this property.

If $S = \mathbb{F}$ and the sharing polynomials are of degree 1 (or, equivalently, the reconstruction polynomials are of degree 1), then the scheme is *linear*. If $S = \mathbb{F}^k$ and the sharing polynomials are of degree 1, then the scheme is *k-linear*. We use the term *multi-linear* to refer to *k-linear* schemes, in general.

2.2 Matroids

In this section, we present the basic definition of matroids and the family of algebraic matroids, which is the one we are focused on. For an introduction to matroid theory, see [56]. We present the relation between matroids and ideal secret sharing schemes.

Definition 2.5 (Matroid). *Given a finite set E and a function $r \colon 2^E \to \mathbb{Z}$, the pair (E, r) is called a* matroid *if the following properties are satisfied for all $X, Y \subseteq E$.*

1. *$r(X) \leq |X|$.*
2. *$r(X) \leq r(Y)$ if $X \subseteq Y$.*
3. *$r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$.*

The set E and the function r are, respectively, the ground set *and the* rank function *of the matroid.*

Let $\mathcal{M} = (E, r)$ be a matroid. The *independent sets* of $\mathcal{M}$ are the sets $X \subseteq E$ with $r(X) = |X|$. Every subset of an independent set is independent and the maximal independent sets are called *bases*. We say that a non-independent set is dependent, and then, every set that contains a dependent set is also dependent. We call *circuits* of $\mathcal{M}$ the minimal dependent sets. All bases have the same number of elements, which equals $r(E)$, the *rank of the matroid*. In addition to the definition given in Definition 2.5, there are other equivalent sets of axioms characterizing matroids, which are stated in terms of the properties of the independent sets, the circuits, the bases, or the hyperplanes. See [56]. A matroid is *connected* if and only if for every two elements in E there is a circuit containing them.

Definition 2.6 (Ports of matroids). *Let $\mathcal{M} = (E, r)$ be a matroid and $a \in E$. The port of $\mathcal{M}$ at the point $a \in E$ is a collection of subsets of $E \setminus \{a\}$ defined as*

$$\Gamma = \{A \subseteq E \setminus \{a\} : r(A \cup \{a\}) = r(A)\},$$

i.e., $A \in \Gamma$ if and only if adding a to A does not increase its rank.

A port of a connected matroid Γ determines the matroid $\mathcal{M}$, i.e., if Γ is a port of a connected matroid at some point a, then there is a unique matroid satisfying this property. It is a consequence of [56, Prop. 4.1.2 and Th. 4.3.3].

Algebraic Dependency and Algebraic Matroids. We next briefly recall the notion of algebraic dependency. Let $\mathbb{F}$ be a field and $\mathbb{K}$ be a transcendental extension field of $\mathbb{F}$. An element $a \in \mathbb{K}$ is algebraically dependent on a set $\{a_1, \ldots, a_k\} \subseteq \mathbb{K}$ if and only if there exists a polynomial $F \in \mathbb{F}(y_0, y_1, \ldots, y_k)$ (i.e., with coefficients in $\mathbb{F}$) such that $F(a, a_1, \ldots, a_k) = 0$ and F contains at least one monomial with a non-zero coefficient and with a degree of y_0 greater than 0. F is the *annihilating polynomial* of $a, a_1, \ldots, a_k$. A set A in $\mathbb{K}$ is algebraically dependent over $\mathbb{F}$ if and only if there exists $a \in A$ such that a is algebraically dependent on $A \setminus \{a\}$. Conversely, a set B in $\mathbb{K}$ is algebraically independent over $\mathbb{F}$ if it is not dependent. The transcendence degree or algebraic rank of a set A in $\mathbb{K}$, denoted $\mathrm{trdeg}_{\mathbb{F}}(A)$, is the maximal size of a subset $B \subseteq A$ such that B is algebraically independent over $\mathbb{F}$. For every finite set $E \subseteq \mathbb{K}$, the pair $(E, \mathrm{trdeg}_{\mathbb{F}})$ is a matroid.

Definition 2.7 (Algebraic Matroids). *A matroid $\mathcal{M} = (E, r)$ is* algebraic *over a field $\mathbb{F}$ if there are elements $(a_i)_{i \in E}$ in a field extension $\mathbb{K}$ of $\mathbb{F}$ such that $r(A) = \mathrm{trdeg}_{\mathbb{F}}(A)$ for every set $A \subseteq E$. The elements $(a_i)_{i \in E}$ are called an* algebraic representation *of $\mathcal{M}$.*

See, e.g., [56] for more background on algebraic matroids. We will mainly consider the case where $\mathbb{K} = \mathbb{F}(x_1, \ldots, x_m)$, i.e., the field of rational functions (of m-variate polynomials) and we will consider representations with m-variant polynomials.

Remark 2.8. Recall that we mentioned that the authorized sets of the access structure Γ defined by a set of polynomials $P_0, \ldots, P_n$ are the subsets $A \subseteq \{1, \ldots, n\}$ such that the polynomial P_0 is algebraically dependent on the set of polynomials $\{P_i\}_{i \in A}$. Notice that, for the authorized sets A in Γ, the algebraic rank of $\{P_i\}_{i \in A}$ is the same as the algebraic rank of $\{P_i\}_{i \in A \cup \{0\}}$. Conversely, if the algebraic rank of $\{P_i\}_{i \in A}$ is not increased when adding P_0, then the polynomial P_0 is algebraically dependent on $\{P_i\}_{i \in A}$. Therefore, Γ is indeed the port of the algebraic matroid represented by the polynomials $P_0, \ldots, P_n$ at the point 0.

Example 2.9. Let $\mathcal{M} = (\{1, 2, 3\}, r)$ be the 2-uniform matroid with 3 elements, i.e., the matroid in which all sets of size at most 2 are independent. The elements $x_1^2, x_2^2, x_1 + x_2 \in \mathbb{F}_2(x_1, \ldots, x_m)$ are an algebraic representation of $\mathcal{M}$ in $\mathbb{F}_2$, i.e., every two polynomials are independent and the three polynomials are dependent – for $F(y_1, y_2, y_3) = y_1 + y_2 + y_3^2$ we obtain $F(x_1^2, x_2^2, x_1 + x_2) = x_1^2 + x_2^2 + (x_1 + x_2)^2 = 0$ (in $\mathbb{F}_2$). Indeed, the access structure defined by the polynomials $x_1^2, x_2^2, x_1 + x_2$ at any point is the 2-threshold access structure. △

Ideal Secret Sharing Schemes and Matroids. Brickell and Davenport [22] showed that every ideal access structures is a port of a matroid. Formally, given an ideal secret sharing scheme Σ with domain of secrets S, we define $n+1$ random variables $S_0, \ldots, S_n$, obtained by sampling a uniformly distributed secret s in S, choosing $r \in R$, and computing the shares $(\mathsf{sh}_1, \ldots, \mathsf{sh}_n) \leftarrow \Pi(s, r)$; S_0 is s and S_i is sh_i for $1 \leq i \leq n$.

Theorem 2.10 ([22]). *Given an ideal secret sharing scheme Σ realizing an access structure Γ, define*

$$r(A) = H(S_A)/H(S) = H(S_A)/\log|S|$$

for every $A \subseteq \{0, \ldots, n\}$. Then, $\mathcal{M} = (\{0, \ldots, n\}, r)$ is a matroid and Γ is the port of this matroid $\mathcal{M}$ at the point 0.

Conversely, not all ports of matroids admit ideal secret sharing schemes. This property is only satisfied by those that are entropic [53].

2.3 Polynomials over Finite Fields

We review some basic notions in relation to polynomials over finite fields. For a finite field $\mathbb{F}$ and a polynomial $P \in \mathbb{F}[x_0, \ldots, x_m]$, we denote by $\deg(P)$ the total degree of P. We write $P = 0$ if P is the zero polynomial. Note that there are polynomials over finite fields that are $P \neq 0$ even though $P(x) = 0$ for all $x \in \mathbb{F}$. For example, if $\mathbb{F}$ is a finite field of order prime p and $P(x) = x^p - x$.

Here we present a result which we will use afterwards that bounds the number of roots of a polynomial.

Lemma 2.11 (Schwartz-Zippel, [66,59]). *Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x_1, \ldots, x_t]$ be a non zero polynomial with degree d. Then, for any finite subset $S \subset \mathbb{F}$ we have*

$$|\{c \in S^t|, :\ f(c) = 0\}| \leq d \cdot |S|^{t-1}.$$

A bound of the degree of the annihilating polynomial of a algebraically dependent set of polynomials over finite fields is given in [7].

Theorem 2.12 ([44, Theorem 4.1.5] and [7, Corollary 5]). *Let $P_1, \ldots, P_n \in \mathbb{F}[x_0, \ldots, x_m]$ be polynomials of degree at most $d \geq 1$ and let $k = \mathrm{trdeg}_{\mathbb{F}}(P_1, \ldots, P_n)$. If $m > k$, then there exists an annihilating polynomial h of $P_1, \ldots, P_n$ with $\deg(h) \leq d^k$.*

Recall that the min-entropy of a random variable X is defined as $H_{\min}(X) = \log 1/p_{\max}$, where $p_{\max} = \max_{x \in \mathrm{supp}(X)} \mathsf{Pr}[X = x]$. The following result is a generalization of [32, Theorem 7.8]. See Remark 2.14 for more details.

Theorem 2.13 ([32, Theorem 7.8]). *Let k, m, and d be integers and $0 < \delta < 1$ be a real number. Let p be a prime such that $p > \max\{(2d)^{\frac{k}{\delta}}, 2^{\frac{10}{\delta}}, (2(2k+1)d^{2k})^{\frac{2}{\delta}}\}$. Let $P_1, \ldots, P_n$ be m-variate polynomials over $\mathbb{F}_p$ of degree at most d and let $k = \mathrm{trdeg}_{\mathbb{F}_p}(P_1, \ldots, P_n)$. Define the random variable X obtained by sampling $x_1, \ldots, x_m$ with uniform distribution from $\mathbb{F}_p^m$ and outputting $P_1(x_1, \ldots, x_m)$, $\ldots, P_n(x_1, \ldots, x_m)$. Then:*

1. *X has min entropy $\leq (k + \delta) \cdot \log(p)$.*
2. *X is ε-close to having min entropy at least $(k - \delta) \cdot \log(p)$ where $\varepsilon = \frac{2dk}{p}$.*

Remark 2.14. The original theorem in [32] uses n polynomials on n variables and we prove the generalization to an arbitrary number of variables m.

Suppose first that $m < n$, then take $n - m$ additional independent variables and define the polynomials $P'_1, \ldots, P'_n$, where $P'_i(x_1, \ldots, x_n) = P(x_1, \ldots, x_m)$. Since $\mathrm{trdeg}_{\mathbb{F}_p}(P_1, \ldots, P_n) = \mathrm{trdeg}_{\mathbb{F}_p}(P'_1, \ldots, P'_n)$, the theorem for $m < n$ follows from the theorem for $m = n$.

Now, suppose that $m > n$, and define $P_i(x_1, \ldots, x_m) = P_1(x_1, \ldots, x_m)$ for $n + 1 \leq i \leq m$, i.e., taking $m - n$ copies of the first polynomial, and let Y be the random variable obtained by sampling $x_1, \ldots, x_m$ with uniform distribution from $\mathbb{F}_p^m$ and outputting $P_1(x_1, \ldots, x_m), \ldots, P_m(x_1, \ldots, x_m)$. Observe that $\mathrm{trdeg}_{\mathbb{F}_p}(P_1, \ldots, P_n) = \mathrm{trdeg}_{\mathbb{F}_p}(P_1, \ldots, P_m)$, Furthermore, for every $(a_1, \ldots, a_n) \in \mathbb{F}^n$ we have

$$\mathsf{Pr}[X = (a_1, \ldots, a_n)] = \mathsf{Pr}[Y = (a_1, \ldots, a_n, a_1, \ldots, a_1)]$$

and for all $(a_1, \ldots, a_n, a_{n+1}, \ldots, a_m)$ such that $a_i \neq a_1$ for some $n + 1 \leq i \leq n$, $\mathsf{Pr}[Y = (a_1, \ldots, a_m)] = 0$. Hence, the result for $m > n$ follows from the original theorem.

3 Ideal Polynomial Secret Sharing Schemes Determine Algebraic Matroids

Let Γ be an access structure over the set of parties $\{1, \ldots, n\}$. Given an ideal secret sharing scheme realizing Γ with polynomial sharing, whose shares are determined by some polynomials $P_1, \ldots, P_n$, we can always consider the algebraic

matroid, whose ground set is $\{0, 1, \ldots, n\}$ and the algebraic representation is $P_0(s, r) = s$ and $P_1, \ldots, P_n$. In this case, the rank of the matroid is determined by the algebraic dependence of the polynomials. As Γ is ideal, it is a port of some matroid. A natural question to ask is if this matroid is the above algebraic matroid.

Question 3.1. Let Γ be an access structure that has a polynomial ideal secret sharing scheme. Is Γ the port of the algebraic matroid whose algebraic representation is the set of sharing polynomials?

Remark 3.2. In answering the above question, we need to be careful. Recall that every function $f : \mathbb{F}_q^k \to \mathbb{F}_q$ can be represented as a multivariate polynomial (whose degree in each variable is at most $q-1$). Based on the results of [22] (see Theorem 2.10), every ideal secret sharing scheme realizing an access structure Γ whose domain of secrets is S can be obtained as follows: Let Γ be the port of the matroid $\mathcal{M}$ and $B \cup \{0\} \subseteq \{0, \ldots, n\}$ be a basis of $\mathcal{M}$. By [22], the shares of B are uniformly distributed in S^B (independently of the secret) and the share of each $i \in \{1, \ldots, n\} \setminus B$ is determined by the secret and the shares of B; that is, there is a function $f : S \times (\times_{j \in B} S_j) \to S_i$ that computes the share of the i-th party. Thus, in every ideal secret sharing scheme whose size of the domain of secrets (and the size of the domain of shares of each party) is a prime power q, the shares can be computed by polynomials over $\mathbb{F}_q$.

As proved by Ben-Efraim [18], there is an ideal access structure whose associated matroid $\mathcal{M}$ is not algebraic. The ideal scheme for this access structure is multi-linear, and the sharings can be computed by multivariate polynomials $P_1, \ldots, P_n$ over some finite field $\mathbb{F}$. Thus, the algebraic matroid with representation $P_0(s, r) = s, P_1, \ldots, P_n$ is not $\mathcal{M}$.

We show that, under some restrictions, the answer to Question 3.1 is positive. We prove two incomparable results. In Theorem 3.3, we show that when the ideal secret sharing scheme has polynomial reconstruction (in addition to the polynomial sharing), the cardinality of the field is big enough, and the degree of the polynomials is small enough, then Γ is indeed a port of this matroid. In Theorem 3.5, we prove a similar result without requiring that the reconstruction is polynomial; however, in this case, we require that the cardinality of the field is prime (i.e., this result does not work for fields whose cardinality is a prime power p^k for $k > 1$). Corollary 1.6 is a direct consequence of Theorem 3.3 and Theorem 3.5.

3.1 Ideal Schemes with Polynomial Sharing and Polynomial Reconstruction

We next prove that the access structure of an ideal scheme with polynomial sharing and polynomial reconstruction is a port of an algebraic matroid, assuming that the field is big enough and the polynomials are of low degree.

Theorem 3.3 (Theorem 1.4 Restated). *Let Σ be an ideal polynomial secret sharing scheme realizing an n-party access structure Γ. Suppose that the domain of secrets in Σ is $\mathbb{F}_q$ for some prime power q and the sharing and reconstruction are polynomials over $\mathbb{F}_q$ of degree at most d_1 and d_2, respectively. If $q > \max\{d_1^{n+1}, d_1 d_2\}$, then Γ is a port of the algebraic matroid defined by the sharing polynomials of Σ.*

For the proof of this theorem, we need a technical lemma about matroid theory.

Lemma 3.4. *Let $\mathcal{M} = (E, r)$ be a matroid, $0 \in E$ and $A \subseteq E \setminus \{0\}$ be a set such that $r(A) = r(A \cup \{0\})$. Then there is a circuit $C \subseteq A \cup \{0\}$ such that $0 \in C$.*

Proof. Let $B \subseteq A$ be a maximal independent set that is contained in A, that is, an independent set $B \subseteq A$ such that $r(A) = r(B)$. By the monotonicity of the rank and the properties of A and B,

$$r(A \cup \{0\}) = r(A) = r(B) \leq r(B \cup \{0\}) \leq r(A \cup \{0\}).$$

Thus, $r(B) = r(B \cup \{0\})$ and B is an independent set such that $B \cup \{0\}$ is dependent. Thus, there is circuit $C \subseteq B \cup \{0\}$; since B is independent $0 \in C$. □

Proof of Theorem 3.3. Let $P_1, \ldots, P_n \in \mathbb{F}[s, r_1 \ldots, r_m]$ be the polynomials that determine the shares in Σ and $P_0(s, r_1, \ldots, r_m) = s$. Consider the matroid $\mathcal{M} = (E, r)$, with $E = \{0, \ldots, n\}$ and algebraic representation $\{P_0, \ldots, P_n\}$, i.e., for every subset $A \subseteq E$, $r(A) = \mathrm{trdeg}_{\mathbb{F}_q}((P_i)_{i \in A})$. We prove that Γ is the port of the algebraic matroid $\mathcal{M}$ at 0, i.e.,

$$A \text{ is a minimal authorized set in } \Gamma \text{ iff } A \cup \{0\} \text{ is a circuit in } \mathcal{M}. \tag{1}$$

To prove (1), we will prove two claims:

1. If A is a minimal authorized set of Γ, then 0 depends on the set A in $\mathcal{M}$.
2. If $A \cup \{0\}$ is a circuit in $\mathcal{M}$, then A is authorized in Γ.

In the end of the proof, we show that Items 1 and 2 imply (1).

Proving Item 1. Let A be a minimal authorized set in Γ; thus, there exists some polynomial $Q_A \in \mathbb{F}[y_1, \ldots, y_{|A|}]$ of degree at most d_2 that reconstructs the secret from the shares of the parties in A, i.e., for every secret $s \in \mathbb{F}_q$ and randomness $r_1, \ldots, r_m \in \mathbb{F}_q$,

$$Q_A((P_i(s, r_1, \ldots, r_m))_{i \in A}) = s = P_0(s, r_1, \ldots, r_m).$$

Consider the polynomial

$$R(s, r_1, \ldots, r_m) = Q_A(s, r_1, \ldots, r_m) - P_0(s, r_1, \ldots, r_m).$$

Observe that $R(s, r_1, \ldots, r_m) = 0$ for every assignment $s, r_1, \ldots, r_m$. By the hypothesis of the theorem, the degree of the polynomial $R(s, r_1, \ldots, r_m)$ is at most $d_1 \cdot d_2 < q$. By the Schwartz–Zippel Lemma, R is identically zero, i.e., the polynomial P_0 is algebraically dependent on $\{P_i\}_{i \in A}$ and $r(A \cup \{0\}) = \mathrm{trdeg}_{\mathbb{F}_q}((P_i)_{i \in A} \cup \{P_0\}) = \mathrm{trdeg}_{\mathbb{F}_q}((P_i)_{i \in A}) = r(A)$.

Proving Item 2. Let $A \cup \{0\}$ be a circuit of $\mathcal{M}$. We prove that A is authorized in Γ. By the perfect privacy of Σ, it suffices to prove that the parties in A get some information on the secret; in particular, we will prove that there exist some shares $(\mathsf{sh}_i)_{i\in A}$ such that have positive probability for a secret s and are not possible for the secret 0.

Since $P_0, \{P_i\}_{i\in A}$ are algebraically dependent, by Theorem 2.12, there exists an annihilating polynomial $F \in \mathbb{F}[y_0, y_1, \ldots, y_{|A|}]$ with $\deg(F) \leq d_1^{|A|}$, that is,

$$F(P_0, \{P_i\}_{i\in A}) = 0. \tag{2}$$

Now, consider the polynomial G with variables $s, r_1, \ldots, r_m$ defined as

$$G(s, r_1, \ldots, r_m) = F(0, (P_i(s, r_1, \ldots, r_m))_{i\in A}). \tag{3}$$

Since $\{P_i\}_{i\in A}$ are algebraically independent, the polynomial is not identically zero, i.e., $G(s, r_1, \ldots, r_m) \neq 0$. The degree of G is bounded by the product of degrees

$$\deg(G) \leq \deg(F) \cdot \max\{\deg(P_i)\} \leq (d_1)^{|A|} \cdot d_1 = d_1^{|A|+1} \leq d_1^{n+1} < q.$$

Since the degree of G is less than q, by Lemma 2.11, there exist some $s, r_1, \ldots, r_m$ for which $G(s, r_1, \ldots, r_m) \neq 0$. Consider the share $\mathsf{sh}_i = P_i(s, r)$ for every $i \in A$. By (2), for any randomness $r'_1, \ldots, r'_m$,

$$F(0, (P_i(0, r'_1, \ldots, r'_m))_{i\in A}) = 0 \quad \text{and} \quad F(0, (\mathsf{sh}_i)_{i\in A}) = G(s, (\mathsf{sh}_i)_{i\in A}) \neq 0.$$

Thus, for any randomness $r' = r'_1, \ldots, r'_m \in \mathbb{F}_q$,

$$(P_i(0, r'))_{i\in A} \neq (\mathsf{sh}_i)_{i\in A}.$$

So the shares $(\mathsf{sh}_i)_{i\in A}$ are impossible given the secret 0 and are possible given the secret s, implying that A is not forbidden, i.e., A is authorized.

We next explain why Items 1 and 2 imply (1). By Item 1, for every minimal authorized set A in Γ, the element 0 depends on the set A, i.e., $r(A) = r(A \cup \{0\})$. By simple properties of matroids (see Lemma 3.4), there is a circuit $C \subseteq A \cup \{0\}$ such that $0 \in C$; let $B = C \setminus \{0\}$. Thus, by Item 2, B is an authorized set. Since $B \subseteq A$ and A is a minimal authorized set, $A = B$ and $A \cup \{0\}$ is a circuit.

By Item 2, for every circuit $A \cup \{0\}$, the set A is an authorized set. If A is not a minimal authorized set, then there is a set $A' \subsetneq A$ such that A' is authorized then. By Item 1, $A' \cup \{0\} \subsetneq A \cup \{0\}$ is dependent, contradicting the fact that $A \cup \{0\}$ is a circuit.

We have proved that $A \cup \{0\}$ is a circuit of the algebraic matroid $\mathcal{M}$ if and only if A is a minimal authorized set of Γ, i.e., Γ is the port of the algebraic matroid. □

3.2 Ideal Schemes with Polynomial Sharing and Arbitrary Reconstruction

We next prove that the access structure of an ideal scheme with polynomial sharing and arbitrary reconstruction over a prime field is the port of an algebraic

matroid, assuming that the field is big enough and the sharing polynomials have low degree. The theorem is proved by using Theorem 2.13.

Theorem 3.5 (Theorem 1.5 Restated). *Let Σ be an ideal polynomial secret sharing scheme realizing an n-party access structure Γ. Suppose that the domain of secrets in Σ is $\mathbb{F}_p$ for some prime p and the sharing is by polynomials over $\mathbb{F}_p$ of degree at most d. If $p > \max\{16(2n+1)^4 d^{8n}, 2^{20}\}$, then Γ is a port of the algebraic matroid defined by the sharing polynomials of Σ.*

Proof. Let $P_1, \ldots, P_n \in \mathbb{F}[s, r_1 \ldots, r_m]$ be the polynomials of degree at most d that determine the shares in Σ and $P_0(s, r_1, \ldots, r_m) = s$. Now we consider the matroid $\mathcal{M} = (E, r)$, with $E = \{0, \ldots, n\}$ and the algebraic representation $\{P_0, \ldots, P_n\}$, i.e., for every subset $A \subseteq E$,

$$r(A) = \mathrm{trdeg}_{\mathbb{F}_q}((P_i)_{i \in A}).$$

Furthermore, consider the matroid $\mathcal{M}_\Sigma = (E, r_\Sigma)$ defined in Theorem 2.10, where $r_\Sigma(A) = H(S_A)/H(S) = H(S_A)/\log p$. We will prove that these matroids are equal, i.e., $r(A) = r_\Sigma(A)$ for every $A \subseteq \{0, \ldots, n\}$.

Fix a set A and let $k = r(A) = \mathrm{trdeg}_{\mathbb{F}_q}((P_i)_{i \in A})$ and $\delta = 1/2$. Note that the random variable S_A is obtained by sampling $s, r_1, \ldots, r_m$ with uniform distribution and computing the shares as $(P_i(s, r_1, \ldots, r_m)_{i \in A})$, i.e., as in Theorem 2.13. Furthermore,

$$p > \max\{16(2n+1)^4 d^{8n}, 2^{20}\} \geq \max\{(2d)^k, 2^{20}, (2(2k+1)d^{2k})^4\}.$$

Thus, S_A satisfies the hypothesis of Theorem 2.13 with $\delta = 1/2$.

By Theorem 2.13, the random variable S_A has min-entropy at most $(k + 1/2)\log p$ and is ε-close to a random variable Y having min-entropy at least $(k - 1/2)\log p$, with $\varepsilon = 2dk/p$. Furthermore, by Theorem 2.10, the random variable S_A is uniformly distributed over a domain of size $p^{r_\Sigma(A)}$. On one hand, $H(S_A) = H_{\min}(S_A)$ and

$$r_\Sigma(A) = \frac{H(S_A)}{\log(p)} = \frac{H_{\min}(S_A)}{\log(p)} \leq k + 0.5.$$

Since $r(A) = k$ and r_Σ are integers, we have that $r_\Sigma(A) \leq r(A)$. For the other direction, assume towards contradiction that $r_\Sigma(A) < r(A)$; as both ranks are integers, $r_\Sigma(A) \leq r(A) - 1$. Thus, S_A is uniformly distributed over a domain of size at most $p^{r(A)-1}$. Let $p_x = \mathsf{Pr}[S_A = x]$ and $p'_x = \mathsf{Pr}[Y = x]$. By our assumptions, $p_x \geq p^{-(r(A)-1)} > p^{-(r(A)-1/2)} \geq p'_x$. Thus,

$$2\mathsf{SD}(S_A, Y) = \sum |p_x - p'_x| \geq \sum p_x - \sum \frac{1}{p^{r(A)-1/2}} \geq 1 - \frac{p^{r(A)-1}}{p^{r(A)-1/2}} = 1 - p^{-1/2}.$$

Thus, since $\mathsf{SD}(S_A, Y) \leq 2dk/p \leq 1/2$,

$$p^{-1/2} \geq 1 - \frac{4dk}{p} \geq \frac{1}{2},$$

contradicting the fact that $p > 2^{20}$. Thus, from the above arguments $r_\Sigma(A) = r(A)$ for every A and the theorem follows. □

4 Secret Sharing Schemes with q-Polynomial Sharing

In this section we study a particular family of schemes with polynomial sharing. These are the schemes where the shares are given by the so-called q-polynomials. Next, we define this family of polynomials, and we show interesting properties of the associated schemes. Namely, we provide a connection between this family of polynomial schemes and multi-linear schemes, and we provide examples that illustrate the need for restrictions on the degree of polynomials in Theorem 3.3.

Definition 4.1. *Let q be a prime power and consider the finite field $\mathbb{F}_{q^r}$ for some $r > 0$. A polynomial of the form $P(x) = \sum_{i=0}^{r-1} a_i x^{q^i}$ where $a_i \in \mathbb{F}_{q^r}$ is a q-polynomial.*

Equipped with the operations of addition and composition of polynomials in $\mathbb{F}_{q^r}[x]$ modulo $x^{q^r} - x$, the set of q-polynomials forms a $\mathbb{F}_q$-algebra that is isomorphic to the algebra of $r \times r$ matrices over $\mathbb{F}_q$ (see [24]). These polynomials were firstly studied by Ore in [55] where they were given a structure of a skew field, i.e., a non commutative ring with field of fractions. Later, Carlitz [24] described an isomorphism between the $\mathbb{F}_q$-linearized polynomial mappings over $\mathbb{F}_{q^r}$ and the group of $r \times r$ matrices over $\mathbb{F}_{q^r}$. However, the mentioned papers only study univariate linearized polynomials, while our sharing polynomials are polynomials over more than one variable. We next see the construction of this isomorphism over multivariate linearized polynomials, detailed in Proposition 4.2.

First, notice that the field $\mathbb{F}_{q^r}$ can be seen as a vector space over $\mathbb{F}_q$. Let α be a primitive element of $\mathbb{F}_{q^r}$, then $\alpha^0, \ldots, \alpha^{r-1}$ constitutes a basis of $\mathbb{F}_q^r$ over $\mathbb{F}_q$. The q-polynomials in one variable are $\mathbb{F}_q$-linear functions from $\mathbb{F}_{q^r}$ to $\mathbb{F}_{q^r}$. Then, when using the transformation of $\mathbb{F}_{q^r}$ to $\mathbb{F}_q^r$, every q-polynomial P is a $\mathbb{F}_q$-linear map from $\mathbb{F}_q^r$ to $\mathbb{F}_q^r$ with an associated $r \times r$ matrix M_P over $\mathbb{F}_q$. Indeed, the isomorphism in [24] is based on this correspondence, and this implies that every $\mathbb{F}_q$-linear map from $\mathbb{F}_q^r$ to $\mathbb{F}_q^r$ can be written as a q-polynomial over $\mathbb{F}_{q^r}$.

Berson observed in [19] that every multivariate $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_{q^r}$ is linear in every coordinate. With this observation we can extend the previous isomorphism to the algebra of q-polynomials in m variables. For every q-polynomial on m variables we obtain a $\mathbb{F}_q$-linear map from $\mathbb{F}_q^{rm}$ to $\mathbb{F}_q^r$, i.e., a $rm \times r$ matrix over $\mathbb{F}_q$. Since the isomorphism is maintained, for every $\mathbb{F}_q$-linear map from $\mathbb{F}_q^{rm}$ to $\mathbb{F}_q^r$ there is a corresponding q-polynomial over $\mathbb{F}_{q^r}$ in m variables.

Next result summarizes the previous construction and a more detailed proof of it is in Appendix B.1.

Proposition 4.2. *Let q be a prime power and $\mathbb{F}_{q^r}$ a finite field. The algebra of q-polynomials on m variables over $\mathbb{F}_{q^r}$ is isomorphic with the algebra of $\mathbb{F}_q$-linear maps from $\mathbb{F}_q^{rm}$ to $\mathbb{F}_q^r$.*

With the use of the relation between q-polynomials and $\mathbb{F}_q$-linear maps, we obtain a correspondence between multi-linear secret sharing schemes and polynomial schemes with q-polynomial sharing.

Theorem 4.3. *Ideal secret sharing schemes over $\mathbb{F}_{q^r}$ with q-polynomial sharing are in correspondence with ideal r-linear secret sharing schemes.*

The properties that characterize ideal multi-linear secret sharing schemes can be translated to the q-polynomials that define the correspondence above. Then we obtain the following result.

Corollary 4.4. *A set of q-polynomials defines an ideal secret sharing scheme if and only if every sharing polynomial is a permutation polynomial in every variable of the support.*

4.1 Examples of q-Polynomial Schemes

In our work, we have seen several examples of ideal q-polynomial secret sharing schemes (Example 1.1, Example 1.10) and in Example 4.6 we see the construction of the matrix that represents a multi-linear scheme deduced from an ideal q-polynomial scheme.

However, schemes with q-polynomial sharing are not perfect, in general. In Example 4.7 we can observe the existence of a q-polynomial scheme that is not perfect and it deduces a non-ideal multi-linear scheme.

Remark 4.5. As we observed in Remark 3.2, every ideal secret sharing scheme whose domain of secrets is a finite field $\mathbb{F}_{q^r}$ has sharing functions that can be computed by polynomials. In general, the degree of these polynomials is at most $q^r - 1$. But in the case of ideal r-linear secret sharing, schemes over $\mathbb{F}_q$, we can bound the degree of the sharing polynomials by q^{r-1}.

Next we give an example of a scheme with q-polynomial sharing that does not realize the access structure determined by the algebraic dependence of the sharing polynomials but is a multi-linear scheme for another access structure. This example evidences the importance of the restriction on the degree of the sharing polynomials with respect to the size of the field.

Example 4.6. We consider the scheme of the Example 1.10 with sharing polynomials over $\mathbb{F}_4$ $P_0(x, y, z) = x$, $P_1(x, y, z) = y + z^2$, $P_2(x, y, z) = x + y^2 + z$. The scheme with secret P_0 and shares P_1, P_2 is 2-polynomial over $\mathbb{F}_4$ and it determines a 2-linear scheme over $\mathbb{F}_2$. Let α be a generator of $\mathbb{F}_4$ over $\mathbb{F}_2$ satisfying $\alpha^2 + \alpha + 1 = 0$. We consider the basis $\{1, \alpha\}$ of $\mathbb{F}_4$ as a $\mathbb{F}_2$-vector space. Then, the 2-linear representation of the scheme is defined by the $\mathbb{F}_2$-linear maps with matrices:

$$M_{P_0} = \begin{pmatrix} 1\,0 \\ 0\,1 \\ 0\,0 \\ 0\,0 \\ 0\,0 \\ 0\,0 \end{pmatrix} \quad M_{P_1} = \begin{pmatrix} 0\,0 \\ 0\,0 \\ 1\,0 \\ 0\,1 \\ 1\,0 \\ 1\,1 \end{pmatrix} \quad M_{P_2} = \begin{pmatrix} 1\,0 \\ 0\,1 \\ 1\,0 \\ 1\,1 \\ 1\,0 \\ 0\,1 \end{pmatrix}.$$

We can observe that the matrix $M_{P_0}|M_{P_1}|M_{P_2}$ defines an ideal 2-linear scheme, therefore, the polynomial scheme with secret P_0 and two parties with sharing

P_1 and P_2 is ideal. We can check that it is a multi-linear scheme for the port of the uniform matroid U_3^2.

Nevertheless, notice that the algebraic matroid defined by the polynomials is the uniform matroid U_3^3 since the algebraic rank of P_0, P_1 and P_2 is 3 and that they define an independent set of the matroid. Therefore, the polynomial scheme does not realize the access structure determined by the port of the algebraic matroid. △

Example 4.7. Consider now the scheme over $\mathbb{F}_4$ with secret P_0 and shares P_1 and P_2 where:

$$P_0(x,y) = x, \quad P_1(x,y) = x^2 + x + y, \quad P_2(x,y) = y.$$

This doesn't satisfy correctness since the parties P_1 and P_2 cannot fully recover the secret since they recover $x^2 + x$ that is not invertible over $\mathbb{F}_4$. In terms of the multi-linear scheme, we can observe that the linear mappings defined by the polynomials are:

$$M_{P_0} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \quad M_{P_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad M_{P_2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that M_{P_1} does not define an ideal multi-linear scheme since the submatrix of the first 2 rows is not 0 or full rank. Therefore, neither the polynomial scheme nor the multi-linear scheme is ideal. △

In previous examples (see Example 1.10) we saw that the access structure of a polynomial scheme may not be determined by the algebraic dependence of the sharing polynomials. This justifies the need for restrictions on the degree of polynomials in Theorem 3.3. We next see an example of an ideal q-polynomial scheme that shows the need for the bound on the degree of the sharing and reconstruction polynomials of Theorem 3.3 for an arbitrary number of parties.

Example 4.8. Let q be a prime power and n be the number of parties and q a prime power, we define a q-polynomial scheme over $\mathbb{F}_{q^n}$ with secret $P_0 = x_0$ and shares

$$\begin{aligned} P_1 &= x_0 + x_1 - x_2^q, \\ P_i &= x_i - x_{i+1}^q \text{ for } 1 < i < n, \text{ and} \\ P_n &= x_n - x_1^q. \end{aligned}$$

To prove that the scheme with these sharing is ideal we can construct the correspondent multi-linear representation and observe that it gives a representation for an ideal scheme.

Now, we show that the access structure does not correspond to the one determined by the algebraic dependence of P_i on P_0. Observe that the set of all parties is authorized since there is a reconstruction function

$$Q(y_1, \dots y_n) = y_1 + y_2^q + y_3^{q^2} + \dots + y_{n-1}^{q^{n-2}} + y_n^{q^{n-1}}$$

satisfying that for all $x_0, \ldots, x_n \in \mathbb{F}_{q^n}$,

$$Q(P_1(x_0, \ldots, x_n), \ldots, P_n(x_0, \ldots, x_n)) = x_0$$

since $x_1 - x_1^{q^n} = 0$ for all $x_1 \in \mathbb{F}_{q^n}$. But the set of polynomials $P_0, \ldots, P_n$ is algebraically independent, since the Jacobian matrix $J_{(x_0,\ldots,x_n)}(P_0, \ldots, P_n)$ has rank $n+1$:

$$J_{(x_0,\ldots,x_n)}(P_0, \ldots, P_n) = \begin{pmatrix} 1\,0\,0\ldots 0 \\ 1\,1\,0\ldots 0 \\ 0\,1\,1\ldots 0 \\ \vdots\,\vdots\,\vdots\,\ddots\,\vdots \\ 0\,0\,0\ldots 1 \end{pmatrix}$$

Here we use the implication of the Jacobian criterion that is true for arbitrary characteristic, see [7].

Notice that the maximum degree of the sharing polynomials is $d_1 = q$ and the reconstruction polynomial has degree $d_2 = q^{n-1}$. The subsets with less than n parties are all unauthorized, then there is only one reconstruction polynomial.

Therefore, we have found a scheme on $\mathbb{F}_{q^n}$ such that its access structure is not the port of the algebraic matroid defined by the sharing polynomials and the bound is $q^n = \max\{q^n, q \cdot q^{n-1}\}$. △

5 Secret Sharing Schemes from Polynomials

In previous sections we observed that, under some conditions, the access structures of ideal polynomial secret sharing schemes are determined by the algebraic rank of the sharing polynomials. It is natural to ask if the reciprocal is true, i.e., if considering a set of polynomials and the access structure Γ determined by their algebraic dependence, then the scheme defined by the evaluation of such polynomials has valuable properties. We show that the resulting schemes are not perfect, in general, but we can transform them into statistical schemes realizing Γ.

First, in Section 5.1, we present the family of statistical secret sharing schemes. In Section 5.2, we give some results on polynomials over finite fields that will be required later. In Section 5.3, we analyze the scheme that is obtained directly from the sharing polynomials. Analyzing the entropy of the resulting random variables, we show that this scheme is not perfect; however, when the cardinality of the field is prime and large enough, subsets in Γ can almost determine the secret, in average, whether those not in Γ have almost no information about the secret. After that, following ideas from Jafari and Khazaei [43], we construct statistical secret sharing schemes with bounded share and secret sizes.

5.1 Statistical Secret Sharing Schemes

In the definition of a secret sharing scheme realizing an access structure, the correctness and privacy are perfect. We can relax these requirements and ask

that the correctness holds with high probability and that the statistical distance between $\Pi_B(a,r)$ and $\Pi_B(b,r)$ is small. To quantify high probability and small statistical distance, the scheme gets as a security parameter ℓ (in unary) as an additional input.

Definition 5.1 (Statistical SSS). *Let ℓ be a security parameter. A statistical secret sharing $\Sigma = \langle \Pi, \mu \rangle$ is a pair that gets the security parameter as an additional input, where $\Pi(1^\ell, \cdot, \cdot)$ is a mapping from $[K_0(\ell)] \times [K_R(\ell)]$ to $[K_1(\ell)] \times \cdots \times [K_n(\ell)]$ for some functions $K_0, K_R, K_1, \ldots, K_n : \mathbb{N} \to \mathbb{N}$, and $\mu(1^\ell)$ is a distribution on some finite set. We say that Σ is a* statistical secret sharing scheme *for the access structure Γ (or Σ statistically realizes it) if:*

Polynomial secret length growth. *The secret length grows at most polynomially in ℓ,*

$$\log K_0(\ell) = O(\ell^c) \text{ for some } c \in \mathbb{N}.$$

Statistical-correctness. *There is some $\varepsilon(\ell) \in \ell^{-\omega(1)}$ (negligible function in ℓ) such that for every qualified set $A \in \Gamma$, there exists a reconstruction function $\textsc{Recon}_A$ such that for every secret s and every randomness r,*

$$\mathsf{Pr}[\textsc{Recon}_A(\Pi(1^\ell, s, r)_A) = s] \geq 1 - \varepsilon(\ell).$$

Statistical-privacy. *There is some $\varepsilon(\ell) \in \ell^{-\omega(1)}$ (negligible function in ℓ), such that for every unauthorized set $B \notin \Gamma$ and for every pair of secrets a, b and randomness r, the statistical distance*

$$\mathsf{SD}(\Pi(1^\ell, a, r)_B, \Pi(1^\ell, b, r)_B) \leq \varepsilon(\ell).$$

We define the optimal information ratio of statistical schemes *for an access structure Γ as the infimum of the information ratio of all sequences of statistical schemes realizing Γ.*

The following result guarantees the existence of statistical secret sharing schemes for an access structure from a family of random variables. This result is obtained by combining different results from [43]. We use this result as a black-box transformation for the construction of schemes. In the proof of Proposition 5.2, which can be found in Appendix C, we summarize the main steps of the construction presented in [43]. In Appendix A.1 and Appendix A.2 we give more details about this transformation, that uses wiretap channel techniques.

Proposition 5.2 ([43]). *Let $S_0, \ldots, S_n$ be jointly distributed random variables and let Γ be an access structure on $\{1, \ldots, n\}$. If*

$$C = \min_{B \notin \Gamma} H(S_0|S_B) - \max_{A \in \Gamma} H(S_0|S_A) > 0,$$

then there exists a sequence of random variables $(T_0^\ell, \ldots, T_n^\ell)_{\ell \in \mathbb{N}}$ with $|\mathrm{supp}(T_0^\ell)| = 2^{\ell R}$, where $R = C - \Theta(\ell^{-1/4})$, with the following properties: For every $s \in$

$\mathrm{supp}(T_0^\ell)$ *and for every subset* A *in* Γ *there exists a reconstruction function* $\textsc{Recon}_A$ *with*

$$\mathsf{Pr}[\textsc{Recon}_A(T_A^\ell) \neq T_0^\ell | T_0^\ell = s] < 2e^{-\sqrt{\ell}}. \tag{4}$$

And for every $s \in \mathrm{supp}(T_0^\ell)$ *and for every subset* B *not in* Γ*,*

$$\mathsf{SD}(p_{T_B^\ell | T_0^\ell = s}, p_{T_0^\ell}) \leq 3e^{-\sqrt{\ell}}. \tag{5}$$

Indeed, the schemes Σ *with* Π *defined as the outcome of the random variables* $(T_1^\ell, \ldots, T_n^\ell)_\ell$ *when* T_0^ℓ *is taken uniformly at random, is a statistical scheme for* Γ *with information ratio* $\max_{i \in P} H(S_i)/C$ *and security parameter* ℓ*. The share size of* i*-th share is* $\ell \log |S_i|$ *and secret size* ℓR*.*

5.2 Results on Polynomials over Finite Fields

We see now a criterion that yields a more efficient way to compute the transcendence degree of polynomials by using the partial derivative matrix, or Jacobian.

Definition 5.3. *For a set of polynomials* $P_1, \ldots, P_n \in \mathbb{F}[x_1, \ldots, x_m]$*, we define the* Jacobian *of* $P_1, \ldots, P_n$ *as*

$$J_x(P_1, \ldots, P_n) := (\partial_{x_j} P_i)_{i,j} = \begin{pmatrix} \partial_{x_1} P_1 & \ldots & \partial_{x_m} P_1 \\ \vdots & & \vdots \\ \partial_{x_1} P_n & \ldots & \partial_{x_m} P_n \end{pmatrix}$$

with $x = (x_1, \ldots, x_m)$ *and* $\partial_{x_j} P_i = \frac{\partial P_i}{\partial x_j}$*. We define the* Jacobian rank *of* $P_1, \ldots, P_n$ *as the rank of the matrix* $J_x(P_1, \ldots, P_n)$ *over* $\mathbb{F}[x_1, \ldots, x_m]$*, and we denote it by* $\mathrm{rank}_J(P_1, \ldots, P_n)$*.*

Lemma 5.4 (Jacobian criterion, Theorem 6 of [7]). *Let* $P_1, \ldots, P_n \in \mathbb{F}[x_1, \ldots, x_m]$ *be polynomials of degree at most* d *and transcendence degree* r*. If* $\mathrm{ch}(\mathbb{F}) = 0$ *or* $\mathrm{ch}(\mathbb{F}) > d^r$*, then* $\mathrm{rank}_J(P_1, \ldots, P_n) = \mathrm{trdeg}_{\mathbb{F}}\{P_1, \ldots, P_n\}$*.*

Next we present Theorem 5.5, which is an extended version of Wooley's theorem [63]. Theorem 5.5 will give us a connection between the algebraic independence and the entropy of some random variables. This extension is due to the fact that in [63] they consider congruences of d polynomials on d variables modulo prime powers. We restrict to the case of a prime finite field and extend to a higher number of variables.

Theorem 5.5. *Let* $\mathbb{F}_p$ *be a field of prime order* p*. Let* k*,* m*, and* d *be integers. Let* $\{P_1, \ldots, P_k\}$ *be some polynomials in* $\mathbb{F}_p[x_1, \ldots, x_m]$ *of degree at most* d *of rank* k*. For* $a \in \mathbb{F}_p^k$*, let*

$$N_a = |\{c \in \mathbb{F}_p^m \,:\, P_i(c) = a_i \text{ for every } 1 \leq i \leq k \text{ and } J_c(P_1, \ldots, P_k) \text{ has rank } k\}|$$

Then for every $a \in \mathbb{F}_p^k$*,* $N_a \leq d^k q^{m-k}$*.*

Proof. Wooley [63] proved that it is true for $m = k$. To prove that the result holds for $m > k$, we extend the set of polynomials in order to have m polynomials of rank m. This can be done by adding polynomials of the kind $P_i(x_i) = x_i$. Now, we can guarantee that when J has full rank then the new Jacobian has also full rank. With this extended set of polynomials, we can apply Wooley's theorem and get that for every $b \in \mathbb{F}^m$, N_b is at most the degree of the m polynomials, which is at most d^k. Now let $a \in \mathbb{F}^k$ and, by an abuse of notation, consider N_a as defined in the statement. We have that N_a is the sum of all N_b for $b \in \mathbb{F}^m$ whose first elements are a. Therefore, $N_a \leq d^k q^{m-k}$. □

5.3 Schemes from Polynomials

This section is dedicated to the proof of Theorem 1.7. This proof is divided into different intermediate steps. We start with Lemma 5.8, where we give bounds on the entropy of the jointly distributed random variables defined by the polynomials as $S_A = \{P_i(U_m)\}_{i \in A}$. Next, we are able to give bounds on $H(S_0|S_A)$ for every subset of parties A. The difference between the values of $H(S_0|S_A)$ for authorized and forbidden subsets is bounded in Proposition 5.9. With that, we can use the black-box transformation of Proposition 5.2 which uses the wiretap channel techniques to obtain statistical schemes for Γ.

Theorem 5.6 (Theorem 1.7 Restated). *Let n, m, k, t and d be positive integers and let p be a prime. For every $1 \leq i \leq n$, let $\{P_{i,j}\}_{1 \leq j \leq k_i}$ be some polynomials in $\mathbb{F}_p[x_0, \ldots, x_m]$ of degree smaller than d, and $P_0(x_0, \ldots, x_m) = x_0$. Let Γ be the n-party access structure determined by the polynomials $\{P_{i,j}\}$ and P_0.*

If $t > \sum_{i \in A} k_i$ for any maximal forbidden subset A not in Γ, and $\log p > (t^2 + 3t + 2) \log d$, then there exists a statistical scheme Σ realizing Γ with total share size $k\ell \log p$ and secret size $\ell(C - \Theta(\ell^{-1/4}))$, where $C = (1 - td^t/p) \log p - 3t^2 \log d$ and ℓ is the security parameter.

Remark 5.7. In the case that Γ is a t-threshold access structure, then the result can be slightly improved. It is enough to require $\log p > 6t \log d$ to get statistical schemes with secret size $\ell(C - \Theta(\ell^{-1/4}))$, where $C = (1 - td^t/p) \log p - 5t \log d$.

Another remark is that in this theorem we only considered the case that $P_0(x_0, \ldots, x_m) = x_0$. If we consider a scheme where the secret is determined by a polynomial of degree larger than one, it is possible to build a similar scheme with slightly smaller C.

In the following results, we just consider the case where each party has only one polynomial. That is, $k_i = 1$ for all $1 \leq i \leq n$. In the proof of Theorem 5.6, we show that it is enough to consider this case, and then the result can be extended to the general case.

Lemma 5.8. *Let $\{P_0, \ldots, P_n\}$ be some polynomials as in Theorem 5.6. Let $A \subseteq \{0, \ldots, n\}$ and $k = \operatorname{rank}(\{P_i\}_{i \in A})$. Consider the jointly distributed random variables $S_A = \{P_i(U_m)\}_{i \in A}$, where U_m is the uniform distribution over $\mathbb{F}_p^{m+1}$. Then,*

1. *If A is independent, $H(S_A) \geq k \log p - k \log 2d$.*
2. *If A is dependent, then $H(S_A) \leq k \log p + (|A| - k)(k \log d + \frac{d^k}{p} \log p)$.*

Proof. Observe that the rank of sets of an algebraic matroid coincide with the Jacobian rank of the polynomials in the representation because of the Jacobian criterion (Lemma 5.4) when the characteristic is $p > d^r$, where r is the rank of the matroid.

First, we prove the first statement. For that, we apply Theorem 5.5. Let E be the event such that J, the Jacobian matrix defined in Theorem 5.5, has (matrix) rank k. By Lemma 2.11, the probability that a minor of J of size k is zero is at most dk/p. Hence, $\mathsf{Pr}(E)$, the probability that J has full rank, is at least $1 - dk/p$.

Now we compute $\mathsf{Pr}(S_A = a \wedge E)$ for $a \in \mathbb{F}_p^k$. By Theorem 5.5, the set N_a is at most $p^{m-k}d^k$, and so $\mathsf{Pr}((S_A = a) \wedge E) \leq d^k/p^k$. Hence, we can bound $\mathsf{Pr}(S_A = a|E)$ as

$$\mathsf{Pr}(S_A = a|E) = \frac{\mathsf{Pr}((S_A = a) \wedge E)}{\mathsf{Pr}(E)} \leq \frac{d^k}{p^k(1 - dk/p)} \leq \left(\frac{2d}{p}\right)^k .$$

Therefore,

$$\begin{aligned} H(S_A) \geq H(S_A|E) &= \sum_{a \in \mathbb{F}_p^k} \mathsf{Pr}(S_A = a|E) \log(1/\mathsf{Pr}(S_A = a|E)) \\ &\geq \sum_{a \in \mathbb{F}_p^k} \mathsf{Pr}(S_A = a|E)(k \log p - k \log(2d)) \geq k \log p - k \log(2d). \end{aligned}$$

To prove the second statement, we first consider the case that A is a circuit with rank k. For that, we show the difference between the entropy of S_A and the entropy of every independent subset of A, $S_{A \setminus j}$, for $j \in A$, is bounded by $k \log d + \frac{d^k}{p} \log p$.

Let Q be the annihilator polynomial of A with degree d_Q. By Theorem 2.12, $d_Q \leq d^k$. This polynomial satisfies that for every $x \in \mathbb{F}^m$, $Q(\{P_i(x)\}_{i \in A}) = 0$. Fix $j \in A$ and let $I = A \setminus j$ be an independent set of rank k.

For $a \in \mathbb{F}^{k-1}$ such that $\mathsf{Pr}(S_I = a) > 0$, if $Q(x, a) = 0$ for every $x \in \mathbb{F}_p$, then S_j can take all values and $j|I$ is uniformly distributed over $\mathbb{F}_p$, therefore $H(S_j|S_I = a) = \log q$. For $a \in \mathbb{F}^{k-1}$ such that $Q(x, a) \neq 0$ for some x, then there are at most d_Q possible values of x such that $\mathsf{Pr}(S_j = x \wedge S_I = a) > 0$, since all values must satisfy that $Q(x, a) = 0$. Then, $H(S_j|S_I = a) \leq \log d_Q$.

Summing up,

$$\begin{aligned}
H(S_A) &= H(S_I) + H(S_j|S_I) \\
&= H(S_I) + \sum_{a\in\mathbb{F}^{k-1}} \mathsf{Pr}(S_I = a) H(S_j|S_I = a) \\
&= H(S_I) + \sum_{a\in\mathbb{F}^{k-1}, Q(\cdot,a)=0} \mathsf{Pr}(S_I = a) H(S_j|S_I = a) \\
&\quad + \sum_{a\in\mathbb{F}^{k-1}, Q(\cdot,a)\neq 0} \mathsf{Pr}(S_I = a) H(S_j|S_I = a) \\
&\leq H(S_I) + \mathsf{Pr}(Q(\cdot,a) = 0) \log q + \mathsf{Pr}(Q(\cdot,a) \neq 0) \log d_Q
\end{aligned}$$

By Lemma 2.11, the polynomial $Q(\cdot, a)$ is 0 with probability at most $\frac{d_Q}{p}$. Then,

$$\begin{aligned}
H(S_A) - H(S_I) &\leq \frac{d_Q}{p} \log p + \left(1 - \frac{d_Q}{p}\right) \log d_Q = \log d_Q + \frac{d_Q}{p}(\log p - \log d_Q) \\
&\leq k \log d + \frac{d^k}{p}(\log p - \log d_Q) \leq k \log d + \frac{d^k}{p} \log p.
\end{aligned}$$

Finally, we prove the second statement for every dependent subset. Let I be the maximal independent set contained in A. Let $j \in A \setminus I$ and let B_j be the unique circuit contained in $j \cup I$.

By the submodularity of the entropy function, for all $j \in A \setminus I$,

$$H(S_{B_j}) - H(S_{B_j \setminus j}) \geq H(S_A) - H(S_{A\setminus j}).$$

Therefore,

$$H(S_A) - H(S_I) \leq \sum_{j\in A\setminus I} (H(S_A) - H(S_{A\setminus j})) \leq \sum_{j\in A\setminus I} (H(S_{B_j}) - H(S_{B_j\setminus j})).$$

For every $j \in A \setminus I$, use the bound for the circuit B_j and the independent set $B_j \setminus j$ and the bound for $H(S_I)$, obtaining

$$H(S_A) \leq k \log p + (|A| - k) \left(k \log d + \frac{d^k}{p} \log p\right).$$

□

Proposition 5.9. *Let S_A be the random variables defined by the joint distribution $\{P_i(U_m)\}_{i\in A}$ where U_m is the uniform distribution over $\mathbb{F}_p^{m+1}$ and $\{P_0, \ldots, P_n\}$ are the polynomials of Theorem 5.6. Let Γ be the access structure corresponding to the polynomials. Then the random variables satisfy that*

$$C = \min_{B\notin\Gamma} H(S_0|S_B) - \max_{A\in\Gamma} H(S_0|S_A) \geq \left(1 - \frac{td^t}{p}\right) \log p - 5t \log d.$$

Proof. We work with authorized and forbidden subsets of Γ.

Claim 5.10. *If $A \in \Gamma$, then $H(S_0|S_A) \leq (d^t/p + 3t \log d/\log p)H(S_0)$.*

First, consider the case that A is minimal in Γ. In this case, A is independent and $A \cup \{0\}$ is a circuit. Suppose that $|A| = k$, and so $A \cup \{0\}$ has rank k. By Lemma 5.8,

$$\begin{aligned} H(S_0|S_A) &\leq k \log p + k \log d + \frac{d^k}{p} \log p - k \log p + k \log 2d \\ &\leq (d^k/p + 3k \log d/\log p)H(S_0). \end{aligned}$$

If $A \in \Gamma$ but it is not minimal, then there is $A' \subseteq A$ that is minimal in Γ and $H(S_0|S_A) \leq H(S_0|S_{A'})$. Now, since the size of maximal forbidden subsets is smaller than t, the size of minimal authorized subsets is at most t.

Claim 5.11. *If $A \notin \Gamma$, then*

$$H(S_0|S_A) \geq (1 - (t-1)d^{t-1}/p - (t^2+1)\log d/\log p)H(S_0).$$

Let A be a non authorized set of size $k < t$. The rank of $A \cup \{0\}$ is greater than the rank of A, which we denote k'. Therefore, $A \cup \{0\}$ contains an independent set I of size $k'+1$. Therefore,

$$\begin{aligned} H(S_0|S_A) &= H(S_{A\cup\{0\}}) - H(S_A) \geq H(S_I) - H(S_A) \\ &\geq (k'+1)\log p - (k'+1)\log 2d - k' \log p - (k-k')(k' \log d + \frac{d^{k'}}{p} \log p) \\ &\geq \log p - (2(k'+1) + (k-k')k') \log d - (k-k')\frac{d^{k'}}{p} \log p \\ &\geq \log p - (k^2 + 2k + 2) \log d - k\frac{d^k}{p} \log p \\ &\geq (1 - kd^k/p - (k^2+2k+2)\log d/\log p)H(S_0). \end{aligned}$$

The claim is obtained by taking $t = k+1$.

Therefore the advantage of the authorized sets over the forbidden ones is

$$C = \min_{B \notin \Gamma} H(S_0|S_B) - \max_{A \in \Gamma} H(S_0|S_A) \geq \left(1 - \frac{td^t}{p}\right) \log p - (t^2 + 3t + 1) \log d$$

which is positive for $p > d^{t^2+3t+2}$. □

Remark 5.12. If Γ is a t-threshold access structure, we can give a more accurate bound because we know that the maximal forbidden subsets are independent. Therefore, the advantage is

$$C \geq \left(1 - \frac{td^t}{p}\right) \log p - 5t \log d,$$

and we can guarantee that this value is positive for $p > d^{6t}$.

Proof of Theorem 5.6. First, we prove this result when every party has only one polynomial. In this case, we can call the polynomials simply as $P_0, \ldots, P_n$. The result for the case is obtained by combining Proposition 5.9 and Proposition 5.2 as follows.

Consider the jointly distributed random variables $S_A = \{P_i(U_m)\}_{i \in A}$ where U_m is the uniform distribution over $\mathbb{F}_p^{m+1}$. By Proposition 5.9, they have positive secret capacity C. By Proposition 5.2, there exists a statistical scheme Σ realizing Γ with shares T_i^ℓ and secret space T_0^ℓ of size $2^{\ell R}$, with $R = C - \Theta(\ell^{-1/4})$ and security parameter ℓ. The size of the secret of the resulting schemes is ℓR and the share size is $\ell \log p$.

Now we consider the case where each party may have more than one polynomial. Notice that in this case, we can consider a scheme in an extended set of parties $\{1, \ldots, k\}$ where each party has one polynomial. Now, the subsets that are forbidden in Γ are in correspondence with subsets of size less than t in this new setting. Applying the results we got above, we obtain a statistical secret sharing scheme with security parameter ℓ realizing Γ with total share size $k\ell \log p$ and same secret size. □

We note that the restriction on the degree of sharing polynomials with respect to the field size is needed. This is justified by Example 5.15, where we give a polynomial scheme not satisfying the restrictions and for which an unauthorized subset has more information about the secret than an authorized subset.

5.4 Polynomial Ramp Schemes

Despite that this work is focused on schemes with perfect or statistical security, we observe that we can also get interesting polynomial schemes in the *ramp* setting, i.e., schemes with two thresholds t_1 and t_2 where we can guarantee that subsets of size at least t_2 are authorized, and subsets of size at most t_1 are forbidden. Next, we present a ramp scheme with an almost optimal trade-off between the share size and the gap $t_2 - t_1$.

Example 5.13. Let $\mathbb{F}$ be a field of size p prime. The scheme is defined by the polynomials $P_{a,b}(x, y) = (x-a)(y-b)$ for $a, b \in \mathbb{F}$ for the shares and $P_0(x, y) = x$ for the secret. The access structure Γ defined by these polynomials is the 2-threshold access structure on $n = p^2$ parties and share size $\log p = \frac{1}{2} \log n$. Indeed, every pair of polynomials P_{a_1,b_1}, P_{a_2,b_2} is algebraically independent over $\mathbb{F}$ and every triple of polynomials is algebraically dependent.

Nevertheless, the scheme defined by these polynomials does not realize Γ perfectly. First, notice that there are parties with partial information about the secret. Let $s \in \mathbb{F}$ be a secret, the parties with polynomial share $P_{s,b}$ have share 0 but the parties with polynomial share $P_{s',b}$ with $s' \neq s$ have probability $1/p$ to have share 0;

$$1 = Pr(P_{s,r}(s, r) = 0) \neq Pr(P_{s',r}(s, r) = 0).$$

Then, the parties have probability $1/p$ to have more information. So the scheme is not 1-private.

Moreover, sets with two parties do not satisfy perfect correctness, since, in general, the reconstruction function is a degree-2 polynomial and there are cases where the parties do not have any information about the secret. Concretely, let $a_1, a_2, b_1, b_2 \in \mathbb{F}$ and two parties with $P_{a_1,b_1,}, P_{a_2,b_2}$ as polynomial shares. If $b_1 = b_2$ and $a_1 \neq a_2$, if $r = b_1$, the parties have the share 0 for any secret and they cannot reconstruct it. Moreover, there are subsets with more than two parties that still do not satisfy correctness for every secret and randomness. For example, the subset of p parties with polynomial share P_{a_i,b_i}, where the b_i's coincide, cannot reconstruct the secret when the randomness $r = b_i$ since all shares will be 0. The first size of subsets with perfect correctness is $p + 1$, since all subsets of size $p + 1$ will reconstruct the secret with probability 1. Let $s, r \in \mathbb{F}$, since there are $p + 1$ polynomials, there is at least a pair with same a but different b and then they can reconstruct a secret. This makes the scheme to have $(p + 1)$-reconstruction.

Schemes with such privacy and reconstruction thresholds require share size at least $\log((p^2 + 1)/(p + 1))$ [25]. In our case, the share size is $\log p$, which is very close to this bound.

Even tough the scheme does not have good security properties, from the results in Section 5, in particular Remark 5.12, it is deduced that, in average, every authorized subset has more information about the secret that any forbidden one. In partiuclar, let S_0 be the random variable associated to the secret, let S_i be the random variable associated to the share of party i, and let $S_{i,j}$ be the random variable associated to the share of the pair of parties i, j. Then,

$$\min_i H(S_0|S_i) - \max_{i,j} H(S_0|S_{i,j}) \geq \left(1 - \frac{8}{p}\right) \log p - 10,$$

which is very close to $\log p$ for large enough p. △

Notice that for this access structure, by relaxing the privacy and correctness requirements, we could overcome the share size limitations of perfect secret sharing schemes. In the case of 2-threshold access structures, Kilian and Nissan showed that the share size of any perfect scheme sharing for a one-bit secret is at least $\log n$ [48,25]. In our scheme, the number of parties is $n = p^2$, and the share size is $\log p = \frac{1}{2} \log n$. Looking precisely at the information each share has about the secret, we see that for every election of $(a, b) \in \mathbb{F}^2$, there is a subset of parties of size p that does not have information about the secret (those parties (a, b) with $b = y$).

Next, we provide a construction based on the Shamir scheme that has similar properties. Compared to the previous one, it reaches 1-privacy, but it requires public information. The share size of each user is the same, but the amount of public information is the same as the total share size. This variant reduces the known bound of the field for the Shamir scheme but loses perfectness.

Example 5.14. A variant of the Shamir scheme for a 2-access structure over a field of order $p = \sqrt{n}$ is by constructing p shares $s_1, \ldots, s_p$ using the Shamir scheme and then assign the shares randomly to the n parties. This assignment

is made public. The size of the public information is $n \log n = 0.5n \log n$ and the total share size is $0.5n \log n$. Notice that this scheme is not perfect since, with probability $1/p$, two-party subsets cannot reconstruct the secret. △

5.5 Remark on Theorem 5.6

Our construction of statistic secret sharing schemes from polynomials in Theorem 5.6 has a restriction on the degree of the polynomials and the size of the field. If t is the size of the maximal forbidden subset of Γ and d is the maximum degree of the sharing polynomials, then

$$\log p > (t^2 + 3t + 2) \log d.$$

Here we show some examples of schemes which sharing polynomials do not satisfy this restriction and then they lead to non valid schemes for their access structures.

Example 5.15. If $p = 2q+1$ is a safe prime, i.e., q is prime. Then the polynomial scheme in $\mathbb{F}_p$ with $P_1(s,r) = r$, $P_2(s,r) = s^q + r$ and $P_2(s,r) = r^q + s$ as polynomial sharings does not satisfy the hypothesis of Theorem 1.7 since the degree of the polynomials exceeds the bound needed, $\log p > 12 \log q$.

Note that the party P_3 has much more information about the secret for any $s, r \in \mathbb{F}_p$ since $r^q = \pm 1$. But the authorized set defined by parties P_1, P_2 has almost no information about the secret since they can recover s^q which takes only ± 1 values. Therefore, there is a forbidden set that has much more information about the secret than an authorized set. △

6 Secret Sharing Schemes from Algebraic Varieties

In previous constructions of secret sharing schemes for access structures determined by polynomials, we have considered polynomial sharing by evaluating the polynomials (as in Theorem 5.6). In this section, we consider the algebraic variety defined by the ideal of annihilator polynomials and give as shares a uniform distribution on the points of the variety.

Using a new result in matroid theory by Matúš [54], we construct sequences of secret sharing schemes with information ratio tending to one from algebraic matroids. Afterwards, using a transformation by Jafari and Khazaei [43] we obtain statistical schemes with information ratio tending to one in the security parameter. Next, we explain the ideas of this construction in more detail, which follow in three steps, and prove the following theorem. Most of the technical results and all proofs are in Appendix D.

Theorem 6.1 (Theorem 1.9 Restated). *The ports of algebraic matroids over a finite field admit statistical secret sharing schemes with information ratio tending to* 1.

Next, we introduce some definitions and results needed for the proof of the previous theorem. Given a set E, *polymatroid* is a pair (E, r) with rank function $r : 2^E \to \mathbb{R}$ satisfying $r(\emptyset) = 0$ and the conditions *2* and *3* of Definition 2.5.

Theorem 6.2 ([40,39]). *Let $(S_x)_{x\in E}$ be some random variables and, for every $X \subseteq E$, define $S_X = (S_x)_{x\in X}$. Consider the mapping $h\colon 2^E \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(X) = H(S_X)$ if $\emptyset \neq X \subseteq E$. Then, h is the rank function of a polymatroid with ground set E.*

Polymatroids that can be defined from random variables as in Theorem 6.2 are called *entropic*. Matúš [54] proved that for every algebraic matroid $\mathcal{M} = (E, r)$ there exists a sequence of entropic polymatroids whose rank function tends to a multiple of the matroid rank r. It implies that algebraic matroids are *almost entropic*. In this construction, the polymatroids are determined by the algebraic variety defined by the annihilating polynomials of the algebraic representations of the matroid.

Let $\mathcal{M}$ be an algebraic matroid over a finite field $\mathbb{G}$. For a large enough extension $\mathbb{F}$ of $\mathbb{G}$, the variety defined by the annihilating polynomials of the algebraic representation of $\mathcal{M}$ is non empty, and we define the random variables $S_{\mathbb{F}}$ that take uniform distribution on the points of this variety. Define the jointly distributed random variables $S_{\mathbb{F},A}$ that take the projection of $S_{\mathbb{F}}$ over the coordinates in A, for every $A \subseteq E$. Define the polymatroid $\mathcal{S}_{\mathbb{F}} = (E, h_{\mathbb{F}})$ with rank function

$$h_{\mathbb{F}}(A) = \frac{H(S_{\mathbb{F},A})}{\log |\mathbb{F}|}.$$

The sequence of entropic polymatroids $\mathcal{S}_{\mathbb{F}}$ is obtained by considering an increasing sequence of algebraic varieties over field extensions of $\mathbb{F}$. Define

$$\sigma_{\mathbb{F}} = \frac{\max_{i\in P} h_{\mathbb{F}}(P_i)}{h_{\mathbb{F}}(P_0)},$$

where the maximum is taken for $i \in E \setminus \{0\}$.

The proof of Lemma 6.3, which is from [54], can be found in Appendix D.1.

Lemma 6.3. *Let $\mathbb{F}$ be a finite field of size q and $\mathcal{S}_{\mathbb{F}} = (E, h_{\mathbb{F}})$ be the polymatroid defined above. Then, for every $K \subseteq E$,*

$$|h_{\mathbb{F}}(K) - r(K)| \leq \frac{\mathfrak{n}}{\ln q}$$

for some constant $\mathfrak{n}$ that depends on the variety determined by the representation of $\mathcal{M}$, but it is independent of q.

Lemma 6.4. *Let Γ be the access structure determined by the matroid $\mathcal{M}$. The polymatroid $\mathcal{S} = (E, h_{\mathbb{F}})$, where $|\mathbb{F}| = q$, satisfies the following.*

- *If $A \in \Gamma$, then $h_{\mathbb{F}}(0 : A) \geq 1 - \frac{\mathfrak{n}}{\ln q}$.*
- *If $B \notin \Gamma$, then $h_{\mathbb{F}}(0 : B) \leq \frac{\mathfrak{n}}{\ln q}$.*

Proof. Recall that $h_{\mathbb{F}}(0:C) = h_{\mathbb{F}}(0) + h_{\mathbb{F}}(C) - h_{\mathbb{F}}(C \cup \{0\})$ for any $C \subseteq E \setminus \{0\}$. For an authorized subset $A \in \Gamma$,

$$\begin{aligned} h_{\mathbb{F}}(0:A) &= h_{\mathbb{F}}(0) + h_{\mathbb{F}}(A) - h_{\mathbb{F}}(A \cup \{0\}) \\ &\geq 1 - \frac{\mathfrak{n}}{\ln q} + r(A) - \frac{\mathfrak{n}}{\ln q} - \left(r(A \cup \{0\}) + \frac{\mathfrak{n}}{\ln q} \right) = 1 - \frac{\mathfrak{n}}{\ln q}. \end{aligned}$$

Let B be a non authorized subset, this is that $r(B \cup \{0\}) = 1 + r(B)$.

$$\begin{aligned} h_{\mathbb{F}}(0:B) &= h_{\mathbb{F}}(0) + h_{\mathbb{F}}(B) - h_{\mathbb{F}}(B \cup \{0\}) \\ &\leq 1 + r(B) - \left(r(B \cup \{0\}) - \frac{\mathfrak{n}}{\ln q} \right) = \frac{\mathfrak{n}}{\ln q} \end{aligned}$$

□

Combining this technical lemma with the construction detailed in Appendix D.1, we deduce the following result.

Proposition 6.5. *Let $\mathcal{M}$ be an algebraic matroid over a finite field $\mathbb{G}$, and let Γ be a port of $\mathcal{M}$. For a sufficiently large extension $\mathbb{F}$ of $\mathbb{G}$, the random variables $S_{\mathbb{F},A}$ satisfy that*

$$C = \min_{B \notin \Gamma} H(S_{\mathbb{F},0} | S_{\mathbb{F},B}) - \max_{A \in \Gamma} H(S_{\mathbb{F},0} | S_{\mathbb{F},A}) > 0.$$

Proof. Since $1 \geq h_{\mathbb{F}}(0) \geq 1 - \frac{\mathfrak{n}}{\ln q}$, by Lemma 6.4 we can see that the polymatroid $\mathcal{S}_{\mathbb{F}} = (E, h_{\mathbb{F}})$ satisfies that

$$\begin{aligned} \max_{A \in \Gamma} h_{\mathbb{F}}(A \cup \{0\}) - h_{\mathbb{F}}(A) &= \max_{A \in \Gamma} h_{\mathbb{F}}(0) - h_{\mathbb{F}}(0:A) \leq \frac{\mathfrak{n}}{\ln q}, \\ \min_{B \notin \Gamma} h_{\mathbb{F}}(B \cup \{0\}) - h_{\mathbb{F}}(B) &= \min_{B \notin \Gamma} h_{\mathbb{F}}(0) - h_{\mathbb{F}}(0:B) \geq 1 - \frac{2\mathfrak{n}}{\ln q}. \end{aligned}$$

Therefore,

$$\begin{aligned} C =& \log |\mathbb{F}| \left(\min_{B \notin \Gamma} (h_{\mathbb{F}}(B \cup \{0\}) - h_{\mathbb{F}}(B)) - \max_{A \in \Gamma} (h_{\mathbb{F}}(A \cup \{0\}) - h_{\mathbb{F}}(A)) \right) \\ \geq& 1 - O\left(\frac{1}{\ln q} \right). \end{aligned}$$

So if the field $\mathbb{F}$ is sufficiently large, $C > 0$. □

These random variables define a partial secret sharing scheme when $\mathbb{F}$ is large enough. Next, we use a black-box constructions from partial secret sharing schemes to statistical secret sharing schemes seen in Proposition 5.2 [43].

Proposition 6.6. *Let $\mathcal{M}$ be an algebraic matroid over a finite field $\mathbb{G}$, and let Γ be a port of $\mathcal{M}$. For a sufficiently large extension $\mathbb{F}$ of $\mathbb{G}$, there is a statistical secret sharing scheme realizing Γ whose information ratio tends to $\sigma_{\mathbb{F}}$ by increasing the security parameter.*

The proof of this proposition is by combining Proposition 5.2 and Proposition 6.5. Observe that $\sigma_{\mathbb{F}}$ tends to 1 when $|\mathbb{F}| \to \infty$ because

$$1 - O\left(\frac{1}{\ln q}\right) \leq \sigma_{\mathbb{F}} \leq 1 + O\left(\frac{1}{\ln q}\right).$$

Following the ideas in [43], we find a statistical secret sharing scheme with information ratio tending to 1 instead of $\sigma_{\mathbb{F}}$. To do that, we use [43, Lemma 6.3], detailed in Appendix D.2, and consider a field $\mathbb{F}$ for every security parameter ℓ, such that $\sigma_{\mathbb{F}}$ tends to 1 when ℓ increases. This completes the proof of Theorem 6.1.

In Theorem 1.8, we study the case where each party may have more than one polynomial. We consider the statistical scheme of Theorem 6.1 in an extended set of parties $\{1, \ldots, k\}$ where each party has one polynomial. We use this scheme on the set of n parties by giving each party i, the k_i shares of the scheme. Then, it has total information ratio tending to k when the security parameter increases.

7 Optimal Information Ratio of Statistical Secret Sharing Schemes

A classic and open question about secret sharing schemes is if duality preserves the optimal information ratio of an access structure or the optimal share size, even for the ideal case. Nevertheless, when the schemes are linear or multi-linear, the question is solved by the duality of representable matroids [56] and we have that the information ratio is preserved. Our work about statistical secret schemes for access structures determined by algebraic matroids, and the fact that here exist almost entropic matroids whose dual does not have this property implies the following result.

Theorem 7.1. *The optimal information ratio of statistical schemes for an access structure is not preserved by duality.*

Proof. Kaced [45] proved that the class of almost entropic matroids is not closed by duality, and an explicit counterexample was presented by Csirmaz [28].

If a matroid $\mathcal{M}$ is almost entropic, there exists a sequence of entropic polymatroids that tend to the matroid. If Γ is a port of $\mathcal{M}$ at 0, this sequence of polymatroids satisfies that the entropy of 0 conditioned to an authorized set is very low and the entropy of 0 conditioned to a forbidden set is almost the entropy of 0. Using the transformation in Proposition 5.2, we can transform these polymatroids to a family of statistical secret sharing schemes whose information ratio tends to 1.

Conversely, if we have statistical secret sharing schemes with information ratio tending to one, they define a sequence of polymatroids that tends to an entropic matroid. Then, the access structure of the scheme is a port of a matroid that is almost entropic.

Therefore, access structures that are ports of $\mathcal{M}$ have optimal information ratio 1, while ports of its dual have optimal information ratio strictly greater than 1. □

Since it is not true that all the access structures preserve optimal information ratio for statistical schemes by duality, a natural question is to characterize the family of matroids for which this property holds. By the results we obtained, for ports of algebraic matroids, the optimal information ratio for statistical schemes is 1. However, it is not known if algebraic representation is closed under duality, in general.

Acknowledgments

We thank Shahram Khazaei and Carles Padró for valuable comments and suggestions. This work was initiated due to the insights of František Matúš on the study of algebraic matroids in [54]. We acknowledge his influence and inspiration in shaping our research.

References

1. Bar Alon, Amos Beimel, and Or Lasri. Simplified PIR and CDS protocols and improved linear secret-sharing schemes. Technical Report 2024/1599, IACR Cryptology ePrint Archive, 2024.
2. Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In *EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 441–471, 2019.
3. Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In *52nd STOC*, pages 280–293, 2020.
4. Benny Applebaum and Oded Nir. Upslices, downslices, and secret-sharing with complexity of 1.5^n. In *CRYPTO 2021*, volume 12827 of *LNCS*, pages 627–655, 2021.
5. László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.
6. Michael Bamiloshin, Aner Ben-Efraim, Oriol Farràs, and Carles Padró. Common information, matroid representation, and secret sharing for matroid ports. *Des. Codes Cryptogr.*, 89(1):143–166, 2021.
7. Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Information and Computation*, 222:2–19, 2013. 38th International Colloquium on Automata, Languages and Programming (ICALP 2011).
8. Amos Beimel. Secret-sharing schemes: A survey. In *IWCC 2011*, volume 6639 of *LNCS*, pages 11–46, 2011.
9. Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. In *TCC 2014*, volume 8349 of *LNCS*, pages 394–418, 2014.
10. Amos Beimel and Benny Chor. Universally ideal secret-sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

11. Amos Beimel and Oriol Farràs. The share size of secret-sharing schemes for almost all access structures and graphs. In *TCC 2020*, volume 12552 of *LNCS*, pages 499–529, 2020.
12. Amos Beimel, Oriol Farràs, and Or Lasri. Improved polynomial secret-sharing schemes. In *TCC*, volume 14370 of *LNCS*, pages 374–405. Springer, 2023.
13. Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. In *Proc. of the 16th IEEE Conf. on Computational Complexity*, pages 188 – 202, 2001. Journal version: *SIAM J. of Discrete Mathematics*, 19(1):258–280, 2005.
14. Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. *SIAM J. on Discrete Mathematics*, 19(1):258–280, 2005.
15. Amos Beimel, Hussien Othman, and Naty Peter. Quadratic secret sharing and conditional disclosure of secrets. In *CRYPTO 2021*, volume 12827 of *LNCS*, pages 748–778, 2021.
16. Amos Beimel, Hussien Othman, and Naty Peter. Quadratic secret sharing and conditional disclosure of secrets. *IEEE Trans. Inf. Theory*, 69(11):7295–7316, 2023.
17. Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In J. Kilian, editor, *Proc. of the Second Theory of Cryptography Conference – TCC 2005*, volume 3378 of *LNCS*, pages 600–619. Springer-Verlag, 2005.
18. Aner Ben-Efraim. Secret-sharing matroids need not be algebraic. *Discrete Mathematics*, 339(8):2136–2145, 2016.
19. Joost Berson. Linearized polynomial maps over finite fields. *Journal of Algebra*, 399:389–406, 2014.
20. George Robert Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, volume 48, pages 313–317, 1979.
21. Ernest F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
22. Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.
23. Antonio Cafure and Guillermo Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields and Their Applications*, 12(2):155–185, 2006.
24. Leonard Carlitz. A note on the betti-mathieu group. *Portugaliae Mathematica*, 22:121–125, 1963.
25. Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Bounds on the threshold gap in secret sharing and its applications. *IEEE Trans. Inf. Theory*, 59(9):5600–5612, 2013.
26. Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, and Daniel Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In Nigel P. Smart, editor, *EUROCRYPT*, volume 4965 of *LNCS*, pages 471–488. Springer, 2008.
27. László Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptography*, 53(3):195–209, 2009.
28. László Csirmaz. Secret sharing and duality. *Journal of Mathematical Cryptology*, 15:157 – 173, 2019.
29. Imre Csiszár and János Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24:339–348, 1978.
30. Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978.
31. Zeev Dvir. Extractors for varieties. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 102–113, 2009.

32. Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. In *FOCS 2007*, pages 52–62, 2007.
33. Oriol Farràs. Secret sharing schemes for ports of matroids of rank 3. *Kybernetika*, 56(5):903–915, 2020.
34. Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, dec 2017.
35. Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. In M. Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 448–465. Springer-Verlag, 2007.
36. Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. *J. Cryptology*, 25(3):434–463, 2012.
37. Oriol Farràs and Carles Padró. Ideal hierarchical secret sharing schemes. *IEEE Transactions on Information Theory*, 58(5):3273–3286, 2012.
38. Serge Fehr. Efficient construction of the dual span program. Manuscript, 1999.
39. Satoru Fujishige. Entropy functions and and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan*, 61:14–18, 1978.
40. Satoru Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39:55–72, 1978.
41. Anna Gál. *Combinatorial Methods in Boolean Function Complexity*. PhD thesis, U. of Chicago, 1995.
42. Emirhan Gürpinar and Andrei Romashchenko. How to use undiscovered information inequalities: Direct applications of the copy lemma. In *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*, pages 1377–1381. IEEE, 2019.
43. Amir Jafari and Shahram Khazaei. Partial secret sharing schemes. *IEEE Transactions on Information Theory*, 69(8):5364–5385, 2023.
44. Johannes Mittmann. *Independence in Algebraic Complexity Theory*. PhD thesis, Rheinische Friedrich-Wilhelms-Universität Bonn, December 2013.
45. Tarik Kaced. Information inequalities are not closed under polymatroid duality. *IEEE Transactions on Information Theory*, 64(6):4379–4381, 2018.
46. Ehud D. Karnin, Jonathan W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.
47. Neeraj Kayal. The complexity of the annihilating polynomial. In *IEEE Conference on Computational Complexity*, pages 184–193, 2009.
48. Joe Kilian and Noam Nisan. Private communication, 1990.
49. Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math. 76*, pages 819–827, 1954.
50. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *50th STOC*, pages 699–708, 2018.
51. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *CRYPTO 2017*, volume 10401 of *LNCS*, pages 758–790, 2017.
52. Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. *J. Mathematical Cryptology*, 4(2):95–120, 2010.
53. František Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203:169–194, 1999.
54. František Matúš. Algebraic matroids are almost entropic. *Proc. Amer. Math. Soc.*, 152:1–6, 2024.
55. Oystein Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35:559–584, 1933.

56. James G. Oxley. *Matroid theory*. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, second edition, 2011.
57. Anat Paskin-Cherniavsky and Artiom Radune. On polynomial secret sharing schemes. In *ITC 2020*, volume 163 of *LIPIcs*, pages 12:1–12:21, 2020.
58. Lajos Rónyai, László Babai, and Murali K. Ganapathy. On the number of zero-patterns of a sequence of polynomials. *Journal of the AMS*, 14(3):717–735, 2001.
59. Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. of the ACM*, 27:701–717, 1980.
60. P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.
61. Adi Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
62. J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.
63. Trevor Wooley. A note on simultaneous congruences. *J. Number Theory*, 58:288–297, 1996.
64. Aaron D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, 1975.
65. Mohammad Yassaee, Mohammad Aref, and Amin Gohari. Achievability proof via output statistics of random binning. *Information Theory, IEEE Transactions on*, 60:1044–1048, 07 2012.
66. Richard E. Zippel. Probabilistic algorithms for sparse polynomials. In *Proc. of the International Symp. on Symbolic and Algebraic Manipulation (EUROSAM '79)*, volume 72 of *LNCS*, pages 216–226. Springer-Verlag, 1979.

A Appendix of Section 2

A.1 Partial Secret Sharing Schemes

For the proofs of Theorem 1.7 and Theorem 1.8 we construct schemes with relaxed security properties, called partial security. The security notion of these schemes is weaker than the one of perfect and statistical schemes, and only requires that the mutual information between the secret and a subset of parties is higher for subsets in the access structures than for subsets that are not [43]. Next, we introduce a more general definition of secret sharing schemes in terms of random variables that includes the non-perfect ones.

Definition A.1 (IT definition of SSS). *Let E be a finite set of* parties*, let $0 \in E$ be a distinguished party, which is called* dealer*. A* secret sharing scheme *Σ on the set E is a discrete random vector $(S_i)_{i\in E}$ such that $H(S_0) > 0$ and $H(S_0|S_{E\setminus\{0\}}) = 0$.*

In the previous definition, the random variable S_0 corresponds to the *secret value*, while the random variables $(S_i)_{i\in E\setminus\{0\}}$ correspond to the *shares* of the secret that are distributed among the parties. For a subset $A \subseteq E \setminus \{0\}$, we define S_A as the jointly distributed random variable that takes projection of $(S_i)_{i\in E\setminus\{0\}}$ over the coordinates in A.

Let $\Sigma = (S_i)_{i\in E}$ be a secret sharing scheme and Γ the access structure defined by Σ. If $A \in \Gamma$, then the correctness property of the scheme implies that the random variable S_0 is completely determined by the value of S_A and

$$H(S_0|S_A) = 0 \qquad (\text{or equivalently } I(S_0{:}S_A) = H(S_0))$$

which implies that the secret value is determined by the shares of the players in A. For a set $B \notin \Gamma$, the privacy property of the scheme implies that the random variables S_0 and S_B are independent and then,

$$H(S_0|S_B) = H(S_B) \qquad (\text{or } I(S_0{:}S_B) = 0)$$

that is, the shares of the players in B do not provide any information on the secret in this situation.

Equivalently, the statistical scheme with shares defined by the outcome of the random variables $(S_0, \ldots, S_n)$ with security parameter ℓ, satisfies that for every authorized set A,

$$\mathsf{Pr}[\textsc{Recon}_A(S_A) \neq s | S_0 = s]$$

is negligible in ℓ, and for every forbidden set B,

$$\mathsf{SD}(p_{S_B|S_0=s}, p_{S_B})$$

is negligible in ℓ.

From this new definition of secret sharing schemes we are able to talk about how an access structure can partially realize a secret sharing scheme. The idea of this weaker notion of security is that the amount of information gained about the secret by every authorized set is strictly larger than that of any forbidden one.

Definition A.2 (Partial SSS). *A secret sharing scheme $\Sigma = (S_i)_{i\in E}$ is a* partial scheme *for the access structure Γ (or* partially realizes *Γ) if*

$$C = \min_{B\notin\Gamma} H(S_0|S_B) - \max_{A\in\Gamma} H(S_0|S_A) > 0.$$

This parameter C is called secret capacity*. We say a scheme is* partially correct *if unqualified sets gain no information about the secret, $H(S_0|S_B) = H(S_0)$ for any B unqualified set in Γ. We say a scheme is* partially private *if qualified sets fully recover the secret, $H(S_0|S_A) = 0$ for any A qualified set in Γ.*

The *partial information ratio* of the scheme is defined as $H(S_0)/C$ times the standard information ratio of the scheme. And the partial information ratio of an access structure is the infimum of the partial information ratio of all secret sharing schemes that partially realize it.

A.2 Wiretap Channel

In this section, we give the definition of a the multi-receiver wiretap channel, which is a generalization of the wiretap channel introduced by Wyner [64]. We give the necessary notions and notations to quantify the reliability and the secrecy of this kind of wiretap channel model, following the work of Jafari and Khazaei [43].

Let $\mathcal{X}$ be the input alphabet and $(\mathcal{Y}_i)_{i\in\mathcal{R}}$, $(\mathcal{Z}_i)_{i\in\mathcal{E}}$ output alphabets. Let $P(((Y_i)_{i\in\mathcal{R}},(Z_j)_{j\in\mathcal{E}})|\mathcal{X})$ be a conditional probability distribution of the random variable $((Y_i)_{i\in\mathcal{R}},(Z_j)_{j\in\mathcal{E}})$ when conditioned on X, where X is a $\mathcal{X}-$valued random variable corresponding to the channel input. Y_i and Z_j are the random variables valued in $\mathcal{Y}_i$ and $\mathcal{Z}_j$ respectively, and correspond to channel output of the receivers and the eavesdroppers.

A wiretap channel models communication between a sender, a set of legitimate receivers with index set $\mathcal{R}$ and a set of eavesdroppers with index set $\mathcal{E}$. When the sender transmits a message given by the random variable X through the channel, according to the probability distribution p, each receiver $i \in \mathcal{R}$ obtains a message Y_i and each eavesdropper $j \in \mathcal{E}$ gets a message Z_j. The goal of the wiretap channel is to reliably transmit a message to the receivers by using m independent instances of the channel, while keeping it secret from the eavesdroppers. This can be obtained by using two algorithms:

1. A publicly-known probabilistic algorithm for encoding $\mathsf{Enc} : \mathcal{K} \longrightarrow \mathcal{X}^m$
2. Deterministic algorithms for decoding, $\mathsf{Dec}_i : \mathcal{Y}_i^m \longrightarrow \mathcal{K}$, one for every receiver $i \in \mathcal{R}$

where $\mathcal{K}$ is the set of messages. To transmit a message k in $\mathcal{K}$, the sender encodes it to obtain a tuple $x^m = (x_1,\ldots,x_m) \leftarrow \mathsf{Enc}(k)$. Each symbol x_k is independently distributed through the channel, let $y_i^m = (y_1,\ldots,y_m)$ and $z_j^m = (z_1,\ldots,z_m)$ be the tuples that the receivers and eavesdroppers i and j get respectively. Each receiver uses its own decoder Dec_i to compute a message $\widehat{k}_i$. We denote K the random variable for the message, in $\mathcal{K}$. Let X^m, Y_i^m, Z_j^m

be the encoders output, the receiver and eavesdropper input respectively. And denote $\widehat{K_i}$ the i-th decoder's output. The following definition is from [43].

Definition A.3. *A* rate $R \geq 0$ *is achievable if for every* m *there exist an encoder and decoders such that:*

1. *K is uniformly distributed on $\mathcal{K} = \{1, \ldots, e^{mR}\}$.*
2. ***Reliability.** For every receiver $i \in \mathcal{R}$, the average decoding error probability $\mathsf{Pr}[\mathsf{Dec}_i(Y_i^m) \neq K]$ is negligible in m.*
3. ***Privacy.** For every eavesdropper $j \in \mathcal{E}$, the average statistical distance $\mathsf{SD}(p_{Z_j^m K}, p_{Z_j^m} p_K)$ is negligible in m.*

In this case, we say that the set of pairs $(\mathsf{Enc}, \mathsf{Dec}_i)_m$ is a CK rate-R wiretap coding family *for the probability distribution $\Sigma = (X, (Y_i)_{i\in\mathcal{R}}, (Z_j)_{j\in\mathcal{E}})$.*

The secret capacity *of a wiretap channel associated to the distribution $\Sigma = (X, (Y_i)_{i\in\mathcal{R}}, (Z_j)_{j\in\mathcal{E}})$ is the maximum of the rates R of any CK rate-R wiretap coding family for this distribution.*

In general, the secret capacity of the wiretap channel is an open problem. However, it can be proved that if the value

$$C = \min_{i\in\mathcal{R}} I(X : Y_i) - \max_{j\in\mathcal{E}} I(X : Z_j) \tag{6}$$

satisfies $C > 0$, then it is a lower bound on the secret capacity of a wiretap channel associated to Σ (see [65], or see [29]).

Note that the conditions of reliability and privacy defined above require that the error probability is negligible on the average, but if we recall the definition of statistical security for secret sharing, we need to consider stronger requirements:

2'. **Strong reliability.** For every receiver $i \in \mathcal{R}$ and every message $k \in \mathcal{K}$, the decoding error probability $\mathsf{Pr}[\mathsf{Dec}_i(Y_i^m) \neq K | K = k]$ is negligible in m.

3'. **Strong privacy.** For every eavesdropper $j \in \mathcal{E}$ and every message $k \in \mathcal{K}$, the statistical distance $\mathsf{SD}(p_{Z_j^m|K=k}, p_{Z_j^m})$ is negligible in m.

Let $R > 0$ be a fixed achievable rate with respect to the weak requirements. It is known that it is also achievable by strong reliability and privacy requirements [43]. This is done by reducing the message size by a factor of at most $e^{-|\mathcal{R}|+|\mathcal{E}|}$.

Lemma A.4 ([43]). *The rate $R = C - \Theta(\frac{1}{m^{1/4}})$ is achievable with strong reliability and strong privacy requirements with the upper bound $2e^{-\sqrt{m}}$ and $3e^{-\sqrt{m}}$ for reliability and privacy errors respectively.*

B Appendix of Section 4

B.1 Isomorphism between q-Polynomials and $\mathbb{F}_q$-Linear Maps

We prove Proposition 4.2 by extending the isomorphism of [24] to the case of q-polynomials on m variables. For that, we first prove Claim B.1 and Claim B.2.

Claim B.1. *A q-polynomial over $\mathbb{F}_{q^r}$ defines a $\mathbb{F}_q$-linear map over the vector space $\mathbb{F}_q^r$.*

Proof. Observe first that q-polynomial mappings are $\mathbb{F}_q$-linear. That is, a q-polynomial P satisfies that if $a \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^r}$, then $P(a\alpha) = aP(\alpha)$ since $a^{q^k} = a$ for every $k \geq 0$. And that if $\beta \in \mathbb{F}_q$ then $P(\alpha+\beta) = P(\alpha) + P(\beta)$ since $\mathbb{F}_{q^r}$ has characteristic q and $(\alpha+\beta)^{q^k} = \alpha^{q^k} + \beta^{q^k}$.

The elements of $\mathbb{F}_{q^r}$ can be described as the $\mathbb{F}_q$-vector space of dimension r generated by the powers of α, where α is a primitive element of $\mathbb{F}_{q^r}$, i.e., a generator of the multiplicative group. Then, any q-polynomial $P \in \mathbb{F}_q[X]$ satisfies that

$$P(\sum_{i=0}^{r} a_i \alpha^i) = \sum_{i=0}^{r} a_i P(\alpha^i),$$

and so it is a $\mathbb{F}_q$-linear map and it is uniquely determined by the action of P over α^i, $1 \leq i \leq r-1$.

A multivariate q-polynomial is linear in every variable, therefore it still defines a $\mathbb{F}_q$-linear map over $\mathbb{F}_{q^r}$. □

Now we see that all linear maps are indeed q-polynomials.

Claim B.2. *All $\mathbb{F}_q$-linear maps from $(\mathbb{F}_q^r)^m$ to $\mathbb{F}_q^r$ are q-polynomials on m variables over $\mathbb{F}_{q^r}$.*

Proof. We first consider the case $m = 1$. Let $P \in \mathbb{F}_q^r \to \mathbb{F}_q^r$ be a $\mathbb{F}_q$-linear map. Identifying every element of $\mathbb{F}_q^r$ with an element of the finite field $\mathbb{F}_{q^r}$, it can be written as a polynomial in $\mathbb{F}_{q^r}[X]$. Let X^s be a monomial appearing in P. By linearity we have $P(X+Y) = P(X)+P(Y)$ and $P(aX) = aP(X)$ for all $a \in \mathbb{F}_q$. Comparing terms of equal degree yields $(X+Y)^s = X^s + Y^s$ and $(aX)^s = aX^s$.

Let p be the unique prime number such that q is a power of p. If s is not a power of p, say $s = dp^e$ with $d > 1$ and $e \geq 0$, then $(X+Y)^s = (X+Y)^{dp^e} = (X^{p^e} + Y^{p^e})^d$ contains the nonzero term $dX^{(d-1)p^e}Y^{p^e}$ which contradicts the fact that $(X+Y)^s = X^s + Y^s$.

Now, let a be the generator of the multiplicative group $\mathbb{F}_q^*$, then by linearity of f we have that $a^s = a$. So $\mathbb{F}_q \subseteq \mathbb{F}_s$ and then s is indeed a power of q. Therefore, a univariate linear map over $\mathbb{F}_q^r$ is a q-polynomial over $\mathbb{F}_{q^r}$.

Now consider the general case of m variables. We will reduce to the univariate case. Let $P \in (\mathbb{F}_q^r)^m \to \mathbb{F}_q^r$ a $\mathbb{F}_q$-linear map. As before, it can be written as a polynomial in $\mathbb{F}_{q^r}[X_1, \ldots, X_m]$. Let $X_1^{s_1} \cdots X_s^{s_m}$ be a monomial appearing in P. If we evaluate the polynomial in two vectors of variables $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_m)$ and compare terms of degree $s_1, \ldots, s_m$ we have

$$(X_1 + Y_1)^{s_1} \cdots (X_m + Y_m)^{s_m} = X_1^{s_1} \cdots X_m^{s_m} + Y_1^{s_1} \cdots Y_m^{s_m}.$$

The left-hand side contains the terms $X_1^{a_1}Y_1^{b_1} \cdots X_m^{a_m}Y_m^{b_m}$ with $a_i + b_i = s_i$ for all i. Suppose we have $i \neq j$ such that both $s_i > 0$ and $s_j > 0$. Substituting $X_i = Y_j = 0$ we get that

$$X_j^{s_j} Y_i^{s_i} \prod_{k \neq i,j} (X_k + Y_k)^{s_k} = 0$$

which is a contradiction. So, there are no terms in P with more than one variable. Then, we can write $P = P_1 + \ldots + P_m$ where $P_i \in \mathbb{F}_{q^r}[X_i]$ which we have seen before that are q-polynomials. □

Proof of Proposition 4.2. Note that the set of q-polynomials is a non-commutative ring with the product defined as the composition of polynomials. We denote it as $\mathbb{F}_{q^r}^{(q)}[X]$. Indeed, if P, Q are q-polynomials, then $P * Q(z) := P(Q(z))$ is also a q-polynomial. Consider the morphism of rings $\mathbb{F}_{q^r}^{(q)}[X] \to \mathbb{F}_q^{r\times r}$ consisting of the transformation of a q-polynomial P to the matrix M_P determined by the linear mapping induced in P in Claim B.1. This is well defined since if P, Q are q-polynomials, $M_{P+Q} = M_P + M_Q$, $M_{P*Q} = M_P \cdot M_Q$ and the identity q-polynomial goes to the identity $r \times r$ matrix Id_r.

The kernel of this morphism is the set of q-polynomials that is 0 when evaluated at every $x \in \mathbb{F}_{q^r}$. This is, the ideal generated by $X^{q^r} - X$. From B.2 we note that it is a surjective morphism. Therefore,

$$\mathbb{F}_{q^r}^{(q)}[X]/(X^{q^r} - X) \simeq \mathbb{F}_q^{r\times r}.$$

Then, the set of q-polynomials under the operation of composition modulo $X^{q^r} - X$ constitutes a group isomorphic to the $r \times r$ matrices over $\mathbb{F}_q$.

This isomorphism can be extended to q-polynomials on m variables and $mr \times r$ matrices:

$$\mathbb{F}_{q^r}^{(q)}[X_1, \ldots, X_m]/(X_1^{q^r} - X_1, \ldots, X_m^{q^r} - X_m) \simeq \mathbb{F}_q^{mr\times r}$$

deducing $\mathbb{F}_q$-linear maps from $\mathbb{F}_q^{rm}$ to $\mathbb{F}_q^r$. □

Now we revisit the proof of Theorem 3.3 but in the case of having q-polynomial sharing. We improve the bound on the degree of the polynomials.

Corollary B.3. *Let Σ be an ideal polynomial secret sharing scheme realizing an n-party access structure Γ. Suppose that the domain of secrets in Σ is $\mathbb{F}_{q^r}$ for some prime power q and the sharing and reconstruction are q-polynomials over $\mathbb{F}_{q^r}$ of degree at most d_1 and d_2 respectively. If $q^r > \max\{d_1^n, d_1 d_2\}$, then Γ is a port of the algebraic matroid defined by the sharing polynomials of Σ.*

Proof. The difference in this result is the item 2 of the proof, i.e., the case where $A \cup \{0\}$ is a circuit in the matroid $\mathcal{M}$. Let $P_0 = s$ and $\{P_i\}_{i\in A}$ be the polynomials of the sharing. By Theorem 2.12, there exists an annihilating polynomial $F \in \mathbb{F}[y_0, y_1, \ldots, y_{|A|}]$ with $\deg(F) \leq d_1^{|A|}$, i.e.

$$F(P_0, \{P_i\}_{i\in A}) = 0.$$

Moreover, this annihilating polynomial is again a q-polynomial, therefore a linear polynomial on every variable,

$$F = F_{P_0} + \sum_{i\in A} F_{P_i}.$$

Now, consider the polynomial G with variables $s, r_1, \ldots, r_m$ defined as

$$\begin{aligned} G(s, r_1, \ldots, r_m) &= F(0, (P_i(s, r_1, \ldots, r_m))_{i \in A}) = \\ &= \sum_{i \in A} F_{P_i}(s, r_1, \ldots, r_m) = -F_{P_0}(s, r_1, \ldots, r_m). \end{aligned}$$

The degree of G is bounded by the product of degrees

$$\deg(G) \leq \deg(F) \cdot \deg P_0 \leq (d_1)^{|A|} \leq d_1^n < q^r.$$

The rest of the proof follows as the original proof of the Theorem 3.3. □

C Appendix of Section 5

C.1 Statistical Schemes from Partial Schemes

In this section, we show the construction of a statistical secret sharing scheme from a partial secret sharing scheme given in [43].

Let $\Pi = (S_i)_{i \in E}$ be a partial scheme for the access structure Γ with partial information ratio σ. Then, the secret capacity of the scheme is

$$C = H(S_0)\delta = \min_{A \in \Gamma} I(S_0 : S_A) - \max_{B \notin \Gamma} I(S_0 : S_B) > 0.$$

We define a multi-receiver and multi-eavesdropper wiretap channel where each qualified set of the access structure Γ can be viewed as a receiver, and each unqualified set is an eavesdropper. See Appendix A.2 for the definition of a multi-receiver and multi-eavesdropper wiretap channel.

Let

$$\Sigma = (X, (Y_A)_{A \in \Gamma}, (Z_B)_{B \notin \Gamma}) = (S_{P_0}, (S_A)_{A \in \Gamma}, (S_B)_{B \notin \Gamma})$$

and consider the associated wiretap channel. Notice that the secret capacity coincides with the constant C associated to the wiretap channel Σ defined in (6). By Lemma A.4, the rate $R = C - \Theta(\frac{1}{m^{1/4}})$ is achievable.

The wiretap channel that gives this rate is defined as the sequence of random variables $(K_\ell, X^\ell, (S_A)^\ell_{A \in \Gamma}, (S_B)^\ell_{B \notin \Gamma}, (\widehat{K_A})^\ell_{A \in \Gamma})_{\ell \in \mathbb{N}}$ which idea is to transmit a message K_ℓ of the space $\{1, \ldots, e^{\ell R}\}$ to the receivers, which are authorized subsets of Γ. Notice that for convenience, the base of the logarithms of the entropy function is changed to e [43]. The variable X^ℓ is the output of the encoding

$$\mathsf{Enc} : \{1, \ldots, e^{\ell R}\} \to (\mathrm{supp} S_{P_0})^\ell.$$

Then, ℓ copies of the random variables $S_0, \ldots, S_n$ are made and every element of the vector X^ℓ is the value of every S_0. For each value of S_0, the rest of the variables $S_1, \ldots, S_n$ are defined, and for each $1 \leq i \leq n$, the vector $S_i^\ell = (S_i^j)_{1 \leq j \leq \ell}$ is defined coordinatewise with the ℓ values of S_i. S_A^ℓ and S_B^ℓ correspond to the receivers and eavesdroppers inputs of the wiretap channel. And finally $\widehat{K_A}^\ell$ is the output of the decoding algorithm of the variable S_A^ℓ defined by the maximum likelihood criterion.

Proposition C.1. *The achievable conditions of the wiretap channel give rise to the following properties on the random variables. Let $R = C - \Theta(\frac{1}{\ell^{1/4}})$, for every element $k \in \{1, \ldots, e^{\ell R}\}$ and A authorized subset in Γ,*

$$\mathsf{Pr}[\widehat{K_A}^{\ell} \neq K_\ell | K_\ell = k] < 2e^{-\sqrt{\ell}} \textit{(Strong reliability)}$$

and for every $k \in \{1, \ldots, e^{\ell R}\}$ and unauthorized subset B in Γ,

$$\mathsf{SD}(p_{S_B^\ell | K_\ell = k}, p_{S_B^\ell}) \leq 3e^{-\sqrt{\ell}} \textit{ (Strong privacy).}$$

The proof of this proposition is deduced from Lemma A.4.

Now, we use the random variables of the wiretap to define a secret sharing scheme that will statistically realize the access structure Γ with security parameter ℓ. Define the sequence of random variables $(T_0^\ell, \ldots T_n^\ell)_{\ell \in \mathbb{N}}$ as

$$\begin{aligned} T_0^\ell &= K_\ell, \\ T_i^\ell &= S_i^\ell, 1 \leq i \leq n. \end{aligned}$$

The T_0^ℓ will be the secret random variable and the T_i^ℓ will be the shares. Observe that for every set $A \in \Gamma$, there exists the sequence of random variables $(\widehat{K_A})_{\ell \in \mathbb{N}}$ which is the result of the maximum likelihood algorithm of the variables T_A^ℓ. Proposition 5.2 follows from the properties of the variables given in Proposition C.1.

Let Σ be the statistical scheme with share functions $(T_i^\ell)_{i \in E}$ with security parameter ℓ. Then, the information ratio σ of Σ is

$$\frac{\max_{i \in P} H(T_i^\ell)}{H(T_0^\ell)}.$$

Claim C.2. *Let σ be the partial information ratio of the scheme Π. Then, the information ratio of the scheme Σ tends to σ when ℓ increases.*

Proof. Let i be a qualified party in the access structure. Then,

$$\lim_{\ell \to \infty} \frac{H(T_i^\ell)}{H(T_0^\ell)} = \lim_{\ell \to \infty} \frac{H(S_i^\ell)}{H(K_\ell)} = \lim_{\ell \to \infty} \frac{H(S_i^\ell)}{\ell(C_\Pi - \Theta(\ell^{-1/4})) \log e} = \frac{H(S_i)}{C_\Pi \log e}.$$

Here we have used the relation $\lim_{\ell \to \infty} \frac{H(S_i^\ell)}{\ell} = H(S_i)$, which is known to hold for a wiretap channel [43]. For an unqualified party j, the result is similar. Then,

$$\lim_{\ell \to \infty} \frac{\max_{i \in P} H(T_i^\ell)}{H(T_0^\ell)} = \max_{i \in P} \frac{H(S_i)}{C_\Pi \log e} = \frac{1}{\delta} \frac{\max_{i \in P} H(S_i)}{H(S_{P_0})} = \sigma.$$

□

Summing up, we have found a statistical secret sharing scheme Σ for the access structure Γ with information ratio tending to σ when the security parameter increases.

C.2 Proof of Proposition 5.2

Proof of Proposition 5.2. The proof of this result is based on a construction done in [43], which starts with statistical secret sharing schemes from a set of random variables with positive secret capacity i.e., with $C = \min_{B \notin \Gamma} H(S_0|S_B) - \max_{A \in \Gamma} H(S_0|S_A) > 0$. [43, Theorem 6.1] proves that from this set of random variables with positive secret capacity $S_0, \ldots, S_n$, it can be defined a statistical family of secret sharing schemes $(T_0^\ell, \ldots, T_n^\ell)_\ell$ with secret space of size $2^{\ell R}$, satisfying Equation (4) and Equation (5). The main tool used to prove this is the wiretap channel, see [43] and Appendix A.1 for more details. Now, consider the secret sharing scheme Π with security parameter ℓ that takes as shares the outcome of the random variables $(T_1^\ell, \ldots, T_n^\ell)_\ell$ and T_0^ℓ as secret, with uniform randomness. It satisfies that for every authorized set A in Γ and every r, s,

$$\mathsf{Pr}[\textsc{Recon}_A(T_A^\ell) = T_0^\ell | T_0^\ell = s] = \mathsf{Pr}[\textsc{Recon}_A(\Pi_\ell(s,r)_A) = s] > 1 - 2e^{\sqrt{-\ell}}.$$

And for every unauthorized set B of Γ and secret s, $\mathsf{SD}(p_{T_B^\ell | T_0^\ell = s}, p_{T_0^\ell}) \leq 3e^{-\sqrt{\ell}}$. Then, by the triangle inequality, for every pair of secret s, s',

$$\mathsf{SD}(T_B^\ell | T_0^\ell = s, T_B^\ell | T_0^\ell = s') = \mathsf{SD}(\Pi_\ell(s,r)_A, \Pi_\ell(s',r)_A) \leq 6e^{-\sqrt{\ell}}.$$

□

D Appendix of Section 6

D.1 Algebraic Matroids are Almost Entropic

In this section, we first provide details of the proof of the following result by Matúš [54]. Then, using a construction in that proof, we are able to prove some technical results of Section 6.

Theorem D.1 ([54]). *Algebraic matroids are almost entropic.*

The proof of Theorem D.1 is constructive. Given an algebraic matroid $\mathcal{M} = (E, r)$, and the access structure given by the matroid port Γ, a sequence of random variables $\{S_q\}_q$ is constructed such that, for q big enough, the polymatroids defined by the distributions of those random variables partially realize the access structure Γ.

First, consider the algebraic representation of $\mathcal{M}$. That is, $n = |E|$, $\mathbb{G}$ a finite field, and $\mathbb{H}$ a transcendental extension of $\mathbb{G}$ that contains the algebraic elements representing $\mathcal{M}$, $(e_i)_{i \in E} \subseteq \mathbb{H}$. Then,

$$r(A) = \deg_{tr/\mathbb{G}} \mathbb{G}((e_i)_{i \in A})$$

for every $A \subseteq E$. Now, consider the polynomials with coefficients in $\mathbb{G}$ that vanish after substituting e_i, $i \in E$ and the ideal generated by these polynomials, $I_{\mathbb{G}}$. This is a prime ideal since if a product of two polynomials belongs to $I_{\mathbb{G}}$, then

one of them vanishes after substituting e_i, $i \in E$. Consider the affine algebraic variety $V_{\mathbb{G}}$ in $\mathbb{G}^n$ defined by the ideal $I_{\mathbb{G}}$. If we replace $\mathbb{G}$ by $\overline{\mathbb{G}}$ we still get a prime ideal $I_{\overline{\mathbb{G}}}$ and the variety $V_{\overline{\mathbb{G}}}$ satisfies that $I(V_{\overline{\mathbb{G}}}) = I_{\overline{\mathbb{G}}}$ and therefore

$$\mathbb{G}[x_1, \ldots, x_n]/I_{\overline{\mathbb{G}}} \simeq \mathbb{G}[e_1, \ldots, e_n].$$

The dimension of the variety $V_{\overline{\mathbb{G}}}$ is the transcendence degree of its function field, which is the field of fractions of $\mathbb{G}[e_1, \ldots, e_n]/I_{\overline{\mathbb{G}}}$. Taking transcendence degree over $\mathbb{G}$, we get

$$\dim V_{\overline{\mathbb{G}}} = \deg_{tr/\mathbb{G}} \mathrm{Frac}(\mathbb{G}[e_1, \ldots, e_n]/I_{\overline{\mathbb{G}}}) = \deg_{tr/\mathbb{G}} \mathbb{G}((e_i)_{i \in Q}) = r(\mathcal{M}).$$

Let $\mathbb{G}_{V_{\overline{\mathbb{G}}}}$ be the smallest subfield of $\overline{\mathbb{G}}$ containing all the coefficients of the polynomials that define $V_{\overline{\mathbb{G}}}$. Then, if $\mathbb{F}$ is a finite field extending $\mathbb{G}_{V_{\overline{\mathbb{G}}}}$, the Lang-Weil bound [49] estimates the number of points of the variety $V_{\overline{\mathbb{G}}}$ with coordinates in the field $\mathbb{F}$, say $V_{\mathbb{F}}$. It is approximately $|\mathbb{F}|^{\dim V}$, i.e., $|\mathbb{F}|^{r(\mathcal{M})}$. This is, there exists a constant $\kappa > 0$ not depending on $\mathbb{F}$ such that

$$\left| \frac{|V_{\mathbb{F}}|}{|\mathbb{F}|^{r(\mathcal{M})}} - 1 \right| \leq \frac{\kappa}{\sqrt{|\mathbb{F}|}}. \tag{7}$$

Since $V_{\overline{\mathbb{G}}}$ is nonempty, at least the extension of $\mathbb{G}$ that contains the coordinates of a point in $V_{\overline{\mathbb{G}}}$ is non empty. Then, for a large enough $\mathbb{F}$, the inequality implies that $V_{\mathbb{F}}$ is nonempty.

From now on, assume $V_{\mathbb{F}}$ is non-empty. Define a random variable S associated to $V_{\mathbb{F}}$ taking a uniform distribution on the coordinates of the points in $V_{\mathbb{F}}$ and let $P_{\mathbb{F}}$ be the probability measure of S. Then, for every $x_i, y_i \in \mathbb{F}$, $1 \leq i \leq n$, if $(x_1, \ldots x_n), (y_1, \ldots, y_n) \in V_{\mathbb{F}}$, then

$$P_{\mathbb{F}}(S = (x_1, \ldots, x_n)) = P_{\mathbb{F}}(S = (y_1, \ldots, y_n)).$$

Else if $(x_1, \ldots, x_n) \notin V_{\mathbb{F}}$, then $P_{\mathbb{F}}(S = (x_1, \ldots, x_n)) = 0$. For every $I \subseteq \{1, \ldots, n\}$, let $\pi_I : \mathbb{F}^n \to \mathbb{F}^I$ be the coordinate projection. The marginal probability measure on $\mathbb{F}^I$ is denoted by $P^I_{\mathbb{F}}$, and the projections of S are denoted by $S^I = \pi^I(S)$ and are random variables having joint distribution $P_{\mathbb{F}}$. This is, if $x \in \mathbb{F}^I$,

$$P^I_{\mathbb{F}}(S^I = x) = P_{\mathbb{F}}(S \in \pi_I^{-1}(x))$$

Let $\pi^{-1}_{I,V_{\mathbb{F}}}(x_I)$ be the fibre consisting of the elements in $V_{\mathbb{F}}$ that project to x_I. Then, if $x \in \pi_I(V_{\mathbb{F}})$,

$$P^I_{\mathbb{F}}(S^I = x) = \frac{|\pi^{-1}_{I,V_{\mathbb{F}}}(x_I)|}{|V_{\mathbb{F}}|}.$$

And if $x \notin \pi_I(V_{\mathbb{F}})$, it holds $P^I_{\mathbb{F}}(S^I = x) = 0$. The entropy of the marginal $P^I_{\mathbb{F}}$ can be written as

$$H(P^A_{\mathbb{F}}) = - \sum_{y_A \in \pi_A(V_{\mathbb{F}})} \frac{|\pi^{-1}_{A,V_{\mathbb{F}}}(y_A)|}{|V_{\mathbb{F}}|} \ln \frac{|\pi^{-1}_{A,V_{\mathbb{F}}}(y_A)|}{|V_{\mathbb{F}}|}.$$

Consider the polymatroid $\mathcal{M}_{\mathbb{F}} = (Q, h_{\mathbb{F}})$ with

$$h_{\mathbb{F}}(A) = H(S_A)/\log(|\mathbb{F}|) \tag{8}$$

for any $A \subseteq Q$. With the following result we see that the polymatroid $\mathcal{M}_{\mathbb{F}}$ can be arbitrarily close to $\mathcal{M}$ when the cardinality of $\mathbb{F}$ is sufficiently large.

Lemma D.2 (Lemma 6.3 Restated). *Let $\mathcal{M} = (E, r)$ be an algebraic matroid. Let $(E, h_{\mathbb{F}})$ be the polymatroid defined above for a finite field $\mathbb{F}$ of size q. Then, for every $K \subseteq E$,*

$$|h_{\mathbb{F}}(K) - r(K)| \leq \frac{\mathfrak{n}}{\ln q}$$

for some constant $\mathfrak{n}$ that depends on the variety determined by the representation of $\mathcal{M}$, but it is independent of q.

Let $q = |\mathbb{F}|$, then consider the polymatroid $\mathcal{M}_{\mathbb{F}} = (E, h)$ where

$$h(A) = \frac{H(P_{\mathbb{F}}^A)}{\ln q}. \tag{9}$$

for any $A \subseteq E$.

Lemma D.2 claims that polymatroids $\mathcal{M}_{\mathbb{F}}$ have good convergence properties and the rank function h tends to r when increasing q.

Proof of Lemma D.2. First, we will show that for a circuit $C \subseteq E$ and a $j \in C$,

$$h(C) - h(C \setminus j) \leq \frac{\mathfrak{j}_V}{\ln q}$$

for some constant $\mathfrak{j}_V$ not depending on the field $\mathbb{F}$. Then, we will consider an arbitrary set $K \subseteq E$ and see that

$$|h(K) - r(K)| \leq \frac{\mathfrak{n}_V}{\ln q}.$$

Let C be a circuit, the elements e_i, $i \in C$ are dependent while the e_i, $i \in C \setminus j$ are independent for all $j \in C$. Therefore, there exists a polynomial P_C with coordinates in C and irreducible, since each subset of C is independent. For a $j \in C$, this polynomial can be seen as a polynomial in the indeterminate x_j with degree $d_{j,C}$ whose coefficients are polynomials in $J = C \setminus j$.

$$H(P_{\mathbb{F}}^C) = H(P_{\mathbb{F}}^J, P_{\mathbb{F}}^j) = H(P_{\mathbb{F}}^J) + H(P_{\mathbb{F}}^j | P_{\mathbb{F}}^J)$$

$$H(P_{\mathbb{F}}^j | P_{\mathbb{F}}^J) = - \sum_{y_C \in \pi_C(V_{\mathbb{F}})} P_{\mathbb{F}}^C(S^C = y_C) \ln \frac{P_{\mathbb{F}}^C(S^C = y_C)}{P_{\mathbb{F}}^J(S^J = \pi_J^C(y_C))}$$

where $\pi_J^C : \mathbb{F}^C \to \mathbb{F}^J$ is the coordinate projector and S^C is the random variable associated with the probability distribution $P_{\mathbb{F}}^C$.

$$\begin{aligned} H(P_{\mathbb{F}}^j|P_{\mathbb{F}}^J) &= -\sum_{y_C \in \pi_C(V_{\mathbb{F}})} \frac{|\pi_{C,V_{\mathbb{F}}}^{-1}(y_C)|}{|V_{\mathbb{F}}|} \ln \frac{\frac{|\pi_{C,V_{\mathbb{F}}}^{-1}(y_C)|}{|V_{\mathbb{F}}|}}{\frac{|\pi_{J,V_{\mathbb{F}}}^{-1}(\pi_J^C(y_C))|}{|V_{\mathbb{F}}|}} \\ &= -\sum_{y_C \in \pi_C(V_{\mathbb{F}})} \frac{|\pi_{C,V_{\mathbb{F}}}^{-1}(y_C)|}{|V_{\mathbb{F}}|} \ln \frac{|\pi_{C,V_{\mathbb{F}}}^{-1}(y_C)|}{|\pi_{J,V_{\mathbb{F}}}^{-1}(\pi_J^C(y_C))|} \\ &= -\sum_{y_J \in \pi_J(V_{\mathbb{F}})} \frac{|\pi_{J,V_{\mathbb{F}}}^{-1}(y_J)|}{|V_{\mathbb{F}}|} \left[\sum_{y_j \in \mathbb{F}} \frac{|\pi_{C,V_{\mathbb{F}}}^{-1}(y_j, y_J)|}{|\pi_{J,V_{\mathbb{F}}}^{-1}(y_J)|} \ln \frac{|\pi_{C,V_{\mathbb{F}}}^{-1}(y_j, y_J)|}{|\pi_{J,V_{\mathbb{F}}}^{-1}(y_J)|} \right] \end{aligned} \quad (10)$$

For some $y_J \in \pi_J(V_{\mathbb{F}})$, let $\nu_{j,C}$ be the number of $y_j \in \mathbb{F}$ such that $\pi_{J,V_{\mathbb{F}}}^C(y_j, y_J) = y_J$. This is the number of nonzero summands in the brackets of (10) and is at most the roots of the polynomial $P_C(y_J)(x_j)$. In the general case, the substitution of y_J to P_C results in a nonzero polynomial in x_j of degree $d_{j,C}$, then $1 \leq \nu_{j,C} \leq d_{j,C}$. Otherwise, when $P_C(y_J)(x_j) = 0$, there are at most q possible values of y_j, then $\nu_{j,C} \leq q$.

For each circuit C and $j \in C$, consider the subvariety $W_{j,C}$ of V of zeros of the coefficients of $P_C(x_j)$, which are polynomials with variables in $J = C \setminus j$. The $y_J \in \pi_J(V_{\mathbb{F}})$ such that $P_C(y_J)(x_j) = 0$ are the ones in $\pi_{J,V_{\mathbb{F}}}(W_{j,C} \cap \mathbb{F}^n)$. It follows that the sums in the brackets of (10) are dominated by

$$\sum_{y_J \in \pi_{J,V_{\mathbb{F}}}(W_{j,C} \cap \mathbb{F}^n)} \frac{|\pi_{J,V_{\mathbb{F}}}^{-1}(y_J)|}{|V_{\mathbb{F}}|} \ln q + \sum_{y_J \in \pi_{J,V_{\mathbb{F}}}((V \setminus W_{j,C}) \cap \mathbb{F}^n)} \frac{|\pi_{J,V_{\mathbb{F}}}^{-1}(y_J)|}{|V_{\mathbb{F}}|} \ln d_{j,C}$$

which is at most

$$\frac{|W_{j,C} \cap \mathbb{F}^n|}{|V_{\mathbb{F}}|} \ln q + \ln d_{j,C}.$$

Using again the Lang-Weil bound applied to the subvariety $W_{j,C}$ and V, we get

$$\frac{|W_{j,c} \cap \mathbb{F}^n|}{|V_{\mathbb{F}}|} \leq \frac{q^{\dim W_{j,C}}}{q^{r(\mathcal{M})}} \frac{c_{W_{j,C}} + \frac{\kappa_{W_{j,C}}}{\sqrt{q}}}{1 - \frac{\kappa_V}{\sqrt{q}}} \leq \frac{\mathfrak{k}_V}{q}$$

where the constant $\mathfrak{k}_V$ does not depend on the field $\mathbb{F}$. Also, take $\mathfrak{d}_V$ bigger than all $\ln d_{j,C}$ and from (10) we get

$$H(X^j|X^J) \leq \mathfrak{k}_V \frac{\ln q}{q} + \mathfrak{d}_V$$

so the non-generic part of the sum is smaller than $\mathfrak{k}_V$ and taking $\mathfrak{j}_V = \mathfrak{k}_V + \mathfrak{d}_V$ we get

$$H(P_{\mathbb{F}}^C) \leq H(P_{\mathbb{F}}^J) + \mathfrak{j}_V.$$

Taking quotient on $\ln q$,

$$h(C) - h(J) \leq \frac{\mathrm{j}_V}{\ln q}.$$

For a dependent set K, let J be the maximal independent set contained in K. Let $k \in K \setminus J$ and $\gamma(k, J)$ be the unique circuit contained in $k \cup J$. By the submodularity of the entropy,

$$h(\gamma(k, J)) + h(J) \geq h(J \cup k) + h(\gamma(k, J) \setminus k),$$

and iterating it,

$$h(K) - h(J) \leq \sum_{k \in K \setminus J} [h(J \cup k) - h(J)] \leq \sum_{k \in K \setminus J} [h(\gamma(k, J) - h(\gamma(k, J) \setminus k)].$$

For every $k \in K \setminus J$, use the bound in for the circuit $\gamma(k, J)$ and independent set $\gamma(k, J) \setminus k$,

$$h(K) - h(J) \leq |Q| \frac{\mathrm{j}_V}{\ln q}$$

then

$$h(K) - |E| \frac{\mathrm{j}_V}{\ln q} \leq h(J) \leq |J| = r(K). \tag{11}$$

To get the other bound, from the Lang-Weil inequality

$$h(E) \geq \frac{\ln |V_{\mathbb{F}}|}{\ln q} \geq r(\mathcal{M}) + \frac{\ln(1 - \kappa_V/\sqrt{q})}{\ln q}$$

Now use the bound (11) with $K = E$ and I a base (i.e. a maximal independent subset) and that $h(I) \leq h(J) + h(I \setminus J)$,

$$r(\mathcal{M}) + \frac{\ln(1 - \kappa_V/\sqrt{q})}{\ln q} \leq h(E) \leq h(I) + |E| \frac{\mathrm{j}_V}{\ln q} \leq h(J) + |I \setminus J| + |E| \frac{\mathrm{j}_V}{\ln q}$$

since $H(P_{\mathbb{F}}^{I \setminus J}) \leq \ln q^{|I \setminus J|} = |I \setminus J| \ln q$. Using that $r(I) = r(\mathcal{M})$ and that $r(\mathcal{M}) - |I \setminus J| \leq r(K)$, we obtain

$$r(K) + \frac{\ln(1 - \kappa_V/\sqrt{q})}{\ln q} - |E| \frac{\mathrm{j}_V}{\ln q} \leq h(J) \leq h(K). \tag{12}$$

Combining both bounds, (11) and (12), we get that for every K arbitrary subset of E,

$$\big|h(K) - r(K)\big| \leq \frac{\mathfrak{n}_V}{\ln q}$$

for some constant $\mathfrak{n}_V$ not depending on q. □

Remark D.3. There are several open questions related to this proof in order to define better secret sharing schemes from the polymatroids obtained.

First, the size of the field $\mathbb{F}$ such that the variety $V_{\mathbb{F}}$ is nonempty is unknown, and this size defines later the first field where the sequence of polymatroids

is defined. Moreover, the number of points of the variety is estimated by the Lang-Weil bound, but can be improved with more sophisticated bounds in [23]. This could lead to finding a better approximation of the rank function of the polymatroids $h_{\mathbb{F}}$, and improvements of this bound would lead to better privacy and correctness bounds.

A better knowledge of the polynomials that define the algebraic variety could also give better bounds and improve the convergence of the polymatroids to the original matroid. For example, a good improvement could be a bound for the field $\mathbb{G}_{V_{\overline{\mathbb{G}}}}$ where the coefficients live, or the degree of the polynomials that define the variety.

D.2 Statistical Schemes with Information Ratio Tending to 1

Suppose now that we have a sequence of partial schemes $\{\Pi_k\}_k$ with information ratios π_k and they satisfy $\lim_{k\to\infty} \pi_k = 1$. The following lemma is the principal tool to get a statistical scheme with information ratio tending to 1 instead of σ.

Lemma D.4 ([43]). *Let $\{\sigma_i\}_{i\in\mathbb{N}}$ be a sequence of real numbers with $\lim_{i\to\infty} \sigma_i = 1$ and $\{c_i\}_{i\in\mathbb{N}}$ another sequence of real numbers. If a sequence of real numbers $\{\sigma_{i,\ell}\}$ satisfies that $\lim_{\ell\to\infty} \sigma_{i,\ell} = \sigma_i$ and $\{\ell_{i,\ell}\}$ satisfies that $\ell_{i,\ell} \leq c_i\ell$, then there exists $\mu : \mathbb{N} \to \mathbb{N}$ such that*

$$\lim_{\ell\to\infty} \sigma_{\mu(\ell),\ell} = 1, \quad \text{and} \quad \ell_{\mu(\ell),\ell} < \ell^2.$$

Proof. For every i, since $\lim_{\ell\to\infty} \sigma_{i,\ell} = \sigma_i$, there exists some M_i for which $|\sigma_{i,\ell} - \sigma_i| \leq 1/i$ for every $\ell \geq M_i$. We want $\mu(\ell)$ to satisfy $\ell > M_{\mu(\ell)}$ and also, we want $\ell > C_{\mu(\ell)}$, so let

$$d_i = \max\{M_1, \ldots, M_i, C_1, \ldots, C_i\} + i.$$

Observe that d_i is an increasing sequence of non-negative real numbers and it goes to infinity as $i \to \infty$. Then, define $\mu(\ell)$ as follows:

$$\mu(\ell) = \begin{cases} 1 \text{ if } \ell < d_1, \\ i \text{ if } d_i < \ell \leq d_{i+1} \end{cases}$$

Note that $\ell > d_{\mu(\ell)} \geq M_{\mu(\ell)}$, so $|\sigma_{\mu(\ell),\ell} - \sigma_{\mu(\ell)}| \leq 1/i$. Since $\mu(\ell)$ is also a monotone increasing unbounded sequence, $\lim_{\ell\to\infty} \sigma_{\mu(\ell)} = 1$. Then, we have that

$$\lim_{\ell\to\infty} \sigma_{\mu(\ell),\ell} = 1.$$

Also note that since $\ell > d_{\mu(\ell)} \geq c_{\mu(\ell)}$, we have that $\ell_{\mu(\ell),\ell} \leq c_{\mu(\ell)}\ell < \ell^2$. □

Let Σ_k be the statistical scheme deduced from the partial secret sharing scheme Π_k. Let σ_k be the information ratio of every scheme, and note from Claim C.2 that σ_k tends to π_k, the information ratio of the partial scheme. Let C_{Π_k} be the secret capacity of the partial scheme Π_k, we also want that the secret

length of the final family grows polynomially in ℓ, so let $\ell_{k,\ell}$ be the secret length of the scheme Σ_k, note that it satisfies that

$$\ell_{k,\ell} \leq C_{\Pi_k} \ell.$$

For every ℓ, we want a value $\mu(\ell)$ for which the secret sharing scheme $\Sigma_{\mu(\ell)}$ will be selected, This value has to satisfy that $\lim_{\ell \to \infty} \sigma_{\mu(\ell)} = 1$ and $\ell_{\mu(\ell),\ell} = O(\ell^c)$ for some $c > 0$. With this value, for each ℓ we will consider the statistical sharing scheme $\Sigma_{\mu(\ell)}$ with security parameter ℓ.

Note that the statistical correctness and privacy still hold for the scheme $\Sigma_{\mu(\ell)}$ since the errors of the scheme Σ_k do not depend on k and then, the errors of the final scheme $\Sigma_{\mu(\ell)}$ are still negligible in ℓ. Finally, we obtained a statistical secret sharing scheme, for the access structure Γ with information ratio tending to 1 with the security parameter and with quadratic secret length grow. This completes the proof of the Theorem 1.9.