Laszlo Csirmaz

Infinite probabilistic secret sharing

Kybernetika, Vol. 59 (2023), No. 2, 179–197

Persistent URL: http://dml.cz/dmlcz/151690

KYBERNETIKA — VOLUME *59* (2023), NUMBER 2, PAGES 179–197

INFINITE PROBABILISTIC SECRET SHARING

Laszlo Csirmaz

A probabilistic secret sharing scheme is a joint probability distribution of the shares and the secret together with a collection of secret recovery functions. The study of schemes using arbitrary probability spaces and unbounded number of participants allows us to investigate their abstract properties, to connect the topic to other branches of mathematics, and to discover new design paradigms. A scheme is perfect if unqualified subsets have no information on the secret, that is, their total share is independent of the secret. By relaxing this security requirement, three other scheme types are defined. Our first result is that every (infinite) access structure can be realized by a perfect scheme where the recovery functions are non-measurable. The construction is based on a paradoxical pair of independent random variables which determine each other. Restricting the recovery functions to be measurable ones, we give a complete characterization of access structures realizable by each type of the schemes. In addition, either a vector-space or a Hilbert-space based scheme is constructed realizing the access structure. While the former one uses the traditional uniform distributions, the latter one uses Gaussian distributions, leading to a new design paradigm.

Keywords: secret sharing, abstract probability space, Sierpiński topology, product measure, span program, Hilbert space program

Classification: 60B05, 94A62, 46C99, 54D10

1. INTRODUCTION

The topic of this paper is secret sharing schemes where the domain of the secret, the domain of the shares, or the set of players is not necessarily finite. This type of approach, namely studying infinite objects instead of finitary ones, is not novel even in the realm of cryptography, see, e. g., [3, 5, 14, 15, 16]. Further motivation and several examples can be found in [7]. As can be expected, even finding the right definition can be hard and far from trivial. We elaborate on this issue in Section 6.

Secret sharing has several faces; it can be investigated equally from either combinatorial or probabilistic point of view, see the survey paper [2]. The combinatorial view leads to *set theoretical generalizations* which are discussed in [6]. In this paper we take the probabilistic view and consider a secret sharing scheme as the (joint) probability distribution of the shares and the secret. Defining probability measures on arbitrary product spaces is not without problem, see [1, 10, 17] for a general description of the

DOI: 10.14736/kyb-2023-2-0179

problems, especially how and when the conditional distribution can be defined. Our definitions avoid referring to conditional distributions at the expense of a less transparent and less intuitive formulation. In Sections 2.3 and 2.4 we give all necessary definitions from probability theory that will be used later on. Nevertheless, a good working knowledge of measure theory and probability spaces, as can be found, e. g., in [12], definitely helps.

A basic requirement in secret sharing – usually called *correctness* – is that qualified subsets, joining their shares, should be able to recover the secret. The most straightforward way to ensure this property is via *recovery functions:* for each qualified subset A there is a function h_A which, given the shares of members of A, returns the value of the secret. In the classical case high complexity recovery functions can only make the scheme more efficient. Quite surprisingly, this is not true in general. In Section 3 we present a scheme in which every share determines the secret, while, at the same time, every collection of the shares is independent of the secret. This latter property is interpreted as that the shares give "no information" on the secret, and considered to be the strongest security requirement. Such a pathological situation can be avoided by requiring the recovery functions to be *measurable*. This is exactly what we do: we focus on *measurable* schemes where all recovery functions are measurable.

Depending on how much information an unqualified subset might have on the secret – the *security requirement* –, we define four scheme types. In a *perfect scheme* unqualified subsets should have no information at all, meaning that the conditional distribution of the secret, given the shares of the subset, is the same as the unconditional distribution. The scheme is *weakly perfect*, if, for some constant $c \geq 1$, the ratio of the conditional and unconditional probabilities is always between $1/c$ and c. A perfect scheme is a weakly perfect scheme with $c = 1$. Weakly perfect schemes were introduced in [5] where they were called "c-schemes."

The scheme is *ramp* when the constant which bounds the ratio of conditional and unconditional probabilities is not necessarily uniform but might depend on the unqualified set (but not on the value of the actual shares). Finally the scheme is *weakly ramp* if the constant c might depend on the actual values of the shares as well. The last case can be rephrased as unqualified subsets cannot exclude any secret value with positive probability.

In Sections 4 and 5 we characterize access structures which can be realized by schemes of these types. We have both topological and structural characterizations. Subsets of the set P of the participants can be considered as elements of the product $\{0,1\}^P$, therefore an access structure – the collection of qualified sets – is a subset of this space. Equipping $\{0,1\}^P$ with some topology we can speak about the topological properties of the access structure. The *Sierpiński topology* [19] is especially promising. If P is finite, a collection of subsets of P, as a subset of the topological space $\{0,1\}^P$ is open if and only if the collection is upward closed, which is a natural requirement for access structures. For definitions and examples for this topology, see Section 2.2. We prove that a scheme can be realized by a perfect or weakly perfect scheme if and only if it is an open set in this topology. Moreover, a scheme can be realized by a ramp or a weakly ramp scheme if and only if it is G_δ, that is, it is the intersection of countably many open sets.

The structural characterization uses *span programs* introduced in [13] and its general-

ization, *Hilbert-space programs*. In a span program we are given a vector space, a target vector, and every participant is assigned one or more vectors. A structure realized by the span program consists of those subsets of participants whose vectors span a linear space containing the target vector. In a Hilbert-space program the vector space is replaced by a Hilbert space, and a subset is qualified if the target vector is in the closure of the linear span of their vectors. We prove that exactly the open structures are realizable by span programs, and exactly the G_δ structures are realizable by Hilbert-space programs.

Finally Section 6 concludes the paper where we show that not every access structure is realizable by a measurable scheme, discuss additional scheme types, and list some open problems.

2. DEFINITIONS

This section defines access structures, then continues with Sierpiński topology and some basic properties of this topology. The definition of probability secret sharing scheme is followed by properties of probability measures on product spaces. Finally four scheme types are defined corresponding to different security requirements. Motivations and examples are omitted, they can be found, e. g., in [7].

2.1. Access structure

An access structure $\mathcal{A} \subset 2^P$ is a non-trivial upward closed (or monotone) family of subsets of the set P of participants. To avoid trivialities, an access structure does not contain singletons, and is not empty. Given the collection $\mathcal{A}_0 \subset 2^P$, the access structure *generated by* $\mathcal{A}_0$ is

$$\mathrm{gen}(\mathcal{A}_0) \stackrel{\mathrm{def}}{=} \{A \subseteq P : \ B \subseteq A \text{ for some } B \in \mathcal{A}_0\}.$$

By monotonicity, an access structure is determined uniquely by any of its generators. The access structure $\mathcal{A}$ is *finitely generated* if generated by a collection of finite subsets of P.

2.2. Sierpiński topology

The *Sierpiński space* is a topological space defined on the two element set $2 = \{0, 1\}$, where the open sets are the empty set, $\{1\}$, and $\{0, 1\}$. This topology is T_0, but not T_1, and is universal in the sense that every T_0 space can be embedded into a high enough power, see [19]. As only the Sierpiński topology is used, all topological notions in this paper refer to this topology. The elements of the product topological space $\{0, 1\}^P$ are the characteristic functions of subsets of P, so its points can be identified with the subsets of P. Consequently a collection $\mathcal{A}$ of subsets of P naturally corresponds to a subset of $\{0, 1\}^P$. The following claim is an easy consequence of the definition of the product topology.

Claim 2.1. The collection $\mathcal{A} \subseteq 2^P$ is open in $\{0, 1\}^P$ if and only if it is a finitely generated monotone structure.

In particular, if P is finite, then a non-trivial $\mathcal{A} \subset 2^P$ is an access structure if and only if it is open.

Definition 2.2. A set $\mathcal{A} \subseteq 2^P$ is G_δ if it is the intersection of countably many open sets.

Claim 2.3. $\mathcal{A} \subseteq 2^P$ is G_δ if and only if there are families $\mathcal{B}_1 \supseteq \mathcal{B}_2 \supseteq \cdots$ consisting of finite subsets of P such that

$$A \in \mathcal{A} \quad \Leftrightarrow \quad A \in \operatorname{gen}(\mathcal{B}_i) \ \text{ for all } i,$$

or, in other words, $\mathcal{A} = \bigcap_i \operatorname{gen}(\mathcal{B}_i)$.

P r o o f . As $\mathcal{B}_i$ has only finite elements, $\operatorname{gen}(\mathcal{B}_i)$ is open, and then $\bigcap_i \operatorname{gen}(\mathcal{B}_i)$ is G_δ.

In the other direction, assume $\mathcal{A} = \bigcap U_i$, where U_i is open. Define $V_i = \bigcap\{U_j : j \le i\}$, and put

$$\mathcal{B}_i \stackrel{\text{def}}{=} \{A \subseteq P : \ A \in V_i, \ \ A \text{ is finite}\}.$$

As V_i is open, $V_i = \operatorname{gen}(\mathcal{B}_i)$, and, of course, $\mathcal{A} = \bigcap_i V_i$ as well. Moreover $V_{i+1} \subseteq V_i$, thus V_i contains every finite set that V_{i+1} does. □

As an example, suppose P is infinite and let $\mathcal{A}$ be the family of all infinite subsets of P. Then $\mathcal{A}$ is not open, but it is G_δ as it is the intersection of the families generated by the n-element subsets of P – all of which are open.

For another example let $A_1, A_2, \ldots$ be disjoint infinite subsets of P and let $\mathcal{A}$ be the family generated by these subsets. Then $\mathcal{A}$ is upward closed, but it is not G_δ. To show this, suppose otherwise, and let $\mathcal{B}_1 \supseteq \mathcal{B}_2 \supseteq \cdots$ be the families as in Claim 2.3. As $A_i \in \mathcal{A} \subseteq \operatorname{gen}(\mathcal{B}_i)$, there is a (finite) $B_i \in \mathcal{B}_i$ with $B_i \subseteq A_i$. Consider the set $B = \bigcup_i B_i$. Clearly $B \in \operatorname{gen}(\mathcal{B}_i)$ as $B_i \in \mathcal{B}_i$ is a subset of B, thus $B \in \bigcap_i \operatorname{gen}(\mathcal{B}_i)$. On the other hand, $B \cap A_i = B_i$ is finite thus B does not extend any A_i, and therefore it is not an element of $\mathcal{A}$.

In the third example we have countably many *forbidden* subsets $F_1, F_2, \ldots$, and $\mathcal{A}$ consists of those subsets which are not covered by any of the forbidden sets:

$$\mathcal{A} = \{A \subseteq P : \ A \not\subseteq F_i, \ \ i = 1, 2, \ldots\}.$$

$\mathcal{A}$ is obviously upward closed, and it is also G_δ. To conclude so, it is enough to show that

$$\mathcal{A}_n = \{A \subseteq P : \ A \not\subseteq F_i, \ \ i = 1, 2, \ldots, n\}$$

is open, as clearly $\mathcal{A} = \bigcap_i \mathcal{A}_i$. But $A \in \mathcal{A}_n$ iff A has a point outside F_1, a point outside $F_2, \ldots$, a point outside F_n. That is, A has a subset with at most n elements which is also in $\mathcal{A}_n$. Therefore $\mathcal{A}_n$ is finitely generated, that is, it is open.

2.3. Probabilistic secret sharing scheme

A *secret sharing scheme* is a method to distribute some kind of information among the participants P so that qualified subsets could recover the secret's value from their shares – the scheme is *correct*, while forbidden subsets have no, or limited information on the secret – the *security* requirement. In probabilistic schemes the shares and the secret come from a (joint) probability distribution on the product space of the corresponding domains.

Definition 2.4. The *domain of secrets* is X_s, and the *domain of shares* of the participant $i \in P$ is X_i. We always assume that none of these sets is empty, and X_s has at least two elements, i. e. there is indeed a secret to be shared.

To make our notation simpler, we denote $P \cup \{s\}$ by I for the set of *indices*. If $A \subseteq P$ then As denotes the set $A \cup \{s\}$, in particular, $I = Ps$. We put $X = \prod_{i \in I} X_i$, and for a subset $J \subseteq I$ we let $X^J = \prod_{i \in J} X_i$ be the restriction of X into coordinates in J.

Informally, a probabilistic secret sharing scheme is a probability distribution on the set X together with a collection of recovery functions. Equivalently, it can be considered as a collection of random variables $\{\xi_i : i \in I\}$ with some joint distribution so that ξ_i takes values from X_i. The *share* of participant $i \in P$ is the value of ξ_i, and the *secret* is the value of ξ_s.

Definition 2.5. A *probabilistic secret sharing scheme* is a pair $\mathcal{S} = \langle \mu, h \rangle$, such that μ is a probability measure on the product space $X = \prod_{i \in I} X_i$, where $I = P \cup \{s\}$, X_s is the set of (possible) secrets, and X_i is the set of (possible) shares for participant $i \in P$; and h is the collection of *recovery functions*: for each $A \subseteq P$ the deterministic function $h_A : X^A \to X_s$ gives a secret value given the shares of members of A.

When the dealer uses the scheme $\mathcal{S} = \langle \mu, h \rangle$, she chooses an element $x \in X$ according to the given distribution μ, sets the secret to be $\xi_s = x(s)$, the s-coordinate of x, and send privately the participant $i \in P$ the share $\xi_i = x(i)$, the ith coordinate of x. When members of $A \subseteq P$ want to recover the secret, they use the recovery function h_A on their shares to pinpoint the secret value.

The scheme is *correct* if qualified subsets recover the secret value, at least with probability 1. To formalize this notion, we look at the distribution of shares of A and the secret value computed by the recovery function h_A. When $x \in X$ is a distribution of all shares, the *projection* $\pi_A(x)$ is its restriction to coordinates (indices) in A, and the recovery function gives the secret value $h_A(\pi_A(x)) \in X_s$. So the probability of those sequences x for which x_s equals this value must be 1.

Definition 2.6. The scheme $\mathcal{S} = \langle \mu, h \rangle$ is *correct* for the access structure $\mathcal{A} \subset 2^P$ if for all $A \in \mathcal{A}$,

$$\mu\big(\{x \in X : h_A(\pi_A(x)) = x_s\}\big) = 1.$$

In a correct scheme the recovery functions of qualified sets are determined almost uniquely. Indeed, let h_A and h_A^* be two correct recovery functions. The set of those points where h_A and h_A^* differ is a subset of

$$\{x \in X : h_A(\pi_A(x)) \neq x_s\} \cup \{x \in X : h_A^*(\pi_A(x)) \neq x_s\},$$

and both sets have measure zero. It follows that the recovery functions form a *coherent family* in the following sense: if A is qualified and $A \subseteq B$, then $h^*_B(y) = h_A(\pi_A(y))$ is also a correct recovery function, thus it must be equal to h_B almost everywhere.

A secret sharing scheme must also provide *security*, meaning that unqualified subsets should have no or limited information on the secret. As the precise definition requires some preparations from Probability Theory, we postpone it to Section 2.5.

2.4. Probability measure on product spaces

As usual in probability theory [12], the definition of a probability measure μ on the product space $X = \prod_i X_i$ requires a σ-algebra Σ on X. Let J be a subset of I, then $X^J = \prod_{i\in J} X_i$. A *cylinder* is a set of the form $C = U \times \prod_{i\notin J} X_i$ where $U \subseteq \prod_{i\in J} X_i$ is the *base* of the cylinder, and J is its *support*. Let moreover

$$\Sigma^J = \Big\{E \subseteq X^J : \Big(E \times \prod_{i\notin J} X_i\Big) \in \Sigma\Big\}.$$

It is easy to check that Σ^J is a σ-algebra on X^J if Σ is a σ-algebra on X. For each $J \subset I$ the *projection function* π_J maps the element $x \in X$ into X^J keeping those coordinates of x which are in J. With this notation a subset E of X_J is in Σ^J if and only if its inverse image under π_J is in Σ, namely, if $\pi_J^{-1}(E) \in \Sigma$. The σ-algebra on the product space X should be generated by its finite-support cylinders, i. e. all sets from Σ of the form

$$U \times \prod_{i\notin J} X_i, \quad \text{where } J \text{ is finite and } U \in \Sigma^J.$$

Let μ be a probability measure on $\langle X, \Sigma\rangle$. Elements of Σ are the *events*, and the probability of the event $E \in \Sigma$ is just $\mu(E)$. As usual, μ is *completed*, that is, not only elements of Σ have probability, but subsets of zero probability events are also measurable. This means that for each μ-measurable $U \subseteq X$ there is a $V \in \Sigma$ such that the symmetric difference of U and V is a μ-zero set (i. e., it is a subset of a set in Σ with μ-measure zero).

For a subset $J \subseteq I$ the *marginal probability* is provided by the probability measure μ^J defined on X^J as follows. $E \subseteq X^J$ is μ^J-measurable iff $\pi_J^{-1}(E)$ is μ-measurable, and

$$\mu^J(E) = \mu\big(\pi_J^{-1}(E)\big).$$

If J has a single element $J = \{j\}$ then we also write μ_j instead of $\mu^{\{j\}}$. In particular, μ_s is the marginal measure on the set of secrets. With this notation, if C is a cylinder with support J and base $U \in \Sigma^J$, then $\mu(C) = \mu^J(U)$.

As the probability measure μ determines the joint distribution of the random variables ξ_i for $i \in I$ (that is the σ-algebra Σ on the whole space X as well as the σ-algebras on each X^J) uniquely, we can, and will, use this measure μ only in probabilistic secret sharing schemes.

The following essential facts about probability measures will be used frequently and without further notice.

Claim 2.7. (a) For each $E \in \Sigma$ there is a countable set $J \subseteq I$ such that $E = \pi_J^{-1}\big(\pi_J(E)\big)$, that is, E is a cylinder with countable support.

(b) For any μ-measurable set $E \subseteq X$ and any $J \subseteq I$, $\mu^J\big(\pi_J(E)\big) \geq \mu(E)$.

(c) For any μ-measurable $E \subseteq X$ and $\varepsilon > 0$ there is a cylinder E' with finite support such that $\mu(E - E') = 0$, and $\mu(E' - E) < \varepsilon$.

(d) For any μ-measurable $E \subseteq X$ and $\varepsilon > 0$ there is a finite $J \subseteq I$ such that $\mu(E) \leq \mu^J(\pi_J(E)) < \mu(E) + \varepsilon$.

P r o o f .

(a) Cylinders with finite support have the stated property. Also, this property is preserved by taking complements and countable unions. Thus all elements in the smallest σ-algebra generated by finite support cylinders have the property claimed.

(b) The statement is immediate from the fact that $\pi_J^{-1}\big(\pi_J(E)\big) \supseteq E$.

(c) By part (a), any μ-measurable $E \subseteq X$ is, up to a set of measure zero, a cylinder C with countable support. Thus it is the intersection of the finite support cylinders $C_n = \pi_{J_n}^{-1}\big(\pi_{J_n}(C)\big)$ where J_n is the set of first n elements of the support of C. As $C_{n+1} \subseteq C_n$, $\lim_{n\to\infty} \mu(C_n) = \mu(C)$ decreasingly, and the claim follows.

(d) The first inequality comes from (b). By (c), there is a cylinder E' with finite support such that $E - E'$ is a zero set, while $\mu(E') < \mu(E) + \varepsilon/2$. As $\mu(E - E') = 0$, there is a zero set $Z \in \Sigma$ such that $Z \supseteq E - E'$. By (a) Z is a cylinder with countable support, thus there is a finite support cylinder $E'' \supseteq Z$ with $\mu(E'') < \varepsilon/2$. Let J be the (finite) support of $E' \cup E''$, then $\mu^J(\pi_J(E')) = \mu(E')$ and $\mu^J(\pi_J(E'')) = \mu(E'')$. As $E \subseteq E' \cup Z \subseteq E' \cup E''$,

$$\begin{aligned} \mu^J(\pi_J(E)) &\leq \mu^J(\pi_J(E' \cup E'')) \\ &\leq \mu^J(\pi_J(E')) + \mu^J(\pi_J(E'')) = \mu(E') + \mu(E'') \\ &< (\mu(E) + \varepsilon/2) + \varepsilon/2 = \mu(E) + \varepsilon, \end{aligned}$$

as was required.

□

Let $B \subseteq P$ be any subset of participants. The collective set of shares they receive falls into the (measurable) set $U \subseteq X^B$ with probability $\mu^B(U)$. Similarly, if $E \subseteq X_s$ is measurable, then the probability that the secret falls into E is $\mu_s(E)$. The *conditional probability distribution* of the secret, assuming that the shares of B come from the set U with $\mu^B(U) > 0$, is defined as

$$\mu_s(E|U) = \frac{\mu^{Bs}(U \times E)}{\mu^B(U)}.$$

Here we wrote Bs for $B \cup \{s\}$. Observe that $\mu^s(E|X^B) = \mu_s(E)$, and $\mu_s(\cdot|U)$ is a probability measure on X_s.

It would be tempting to define the conditional distribution given not a (measurable) subset of the shares, but the shares themselves. Unfortunately such conditional distributions do not always exist [4], nevertheless in statistics their existence is almost always assumed. Fortunately, at the expense of a slightly more complicated and less intuitive formulation, we can avoid those conditional distributions.

2.5. Security requirements

In a secret sharing scheme unqualified subsets are required to have no, or limited information on the secret. Depending on how strong the security guarantee is we distinguish four scheme types.

Definition 2.8. Let $\mathcal{S} = \langle \mu, h \rangle$ be a secret sharing scheme on the set P of participants. The scheme is *perfect*, *weakly perfect*, *ramp*, or *weakly ramp* if the collective set of shares of an unqualified subset $B \subseteq P$ satisfies the following condition:

perfect B gets no information on the secret, meaning that the set of shares and the secret are (statistically) independent. That is, for every measurable $U \subseteq X^B$ and $E \subseteq X_s$ we have

$$\mu^{Bs}(U \times E) = \mu^B(U) \cdot \mu_s(E).$$

This can also be expressed as the conditional probability $\mu_s(\cdot|U)$ coincides with the unconditional probability $\mu_s(\cdot)$ for all $U \subseteq X^B$ with $\mu^B(U) > 0$.

weakly perfect For $U \subseteq X^B$ the conditional probability $\mu_s(\cdot|U)$ deviates from $\mu_s(\cdot)$ by a constant factor only, i. e., for some positive constant $c \geq 1$ (independently of the unqualified set B), for all measurable $U \subseteq X^B$ and $E \subseteq X_s$,

$$\frac{1}{c} \cdot \mu^B(U) \cdot \mu_s(E) \leq \mu^{Bs}(U \times E) \leq c \cdot \mu^B(U) \cdot \mu_s(E). \tag{1}$$

ramp The constant $c = c_B$ in (1) might depend on the subset B (but not on U and E).

weakly ramp Based on their collective shares, B cannot exclude any subset of the secrets with positive measure:

$$\mu^B(U) \cdot \mu_s(E) > 0 \text{ implies } \mu^{Bs}(U \times E) > 0.$$

(Observe that the reverse implication always holds.)

These definitions reflect and extend the usual ones in classical secret sharing schemes. The traditional requirement for perfect schemes is the statistical independence as defined here. Weakly perfect schemes were introduced in [5], where such schemes with constant c are called "c-schemes." No universally accepted definition exists for ramp schemes. The best approach is that in a ramp scheme under no circumstances an unqualified subset should be able to recover the secret. Our definitions reflect this idea. However, see the discussion in Section 6.

When the scheme $\mathcal{S}$ is classical, namely the number of participants is finite and both the shares and the secret come from a finite domain (that is, X is finite), then the conditions for weakly perfect, ramp, and weakly ramp schemes are equivalent, while not equivalent to perfect schemes.

Claim 2.9. The types above are listed in decreasing strength, namely

$$\text{perfect} \;\Rightarrow\; \text{weakly perfect} \;\Rightarrow\; \text{ramp} \;\Rightarrow\; \text{weakly ramp}.$$

None of the implications can be reversed.

P r o o f . It is not difficult to construct schemes witnessing the irreversibility of these implications. For concrete examples consult [7]. □

3. NON-MEASURABLE SCHEMES REALIZE ALL

The probabilistic secret sharing scheme $\mathcal{S} = \langle \mu, h \rangle$ is *measurable* if all recovery functions h_A are measurable. Requesting measurability seems to be a technical issue. It is not, as is shown by Theorem 3.2. The proof uses a paradoxical construction of two random variables due to Gábor Tardos, and is included here with his permission.

Theorem 3.1. (G. Tardos) Let $\mathbb{I}$ denote the unit interval $[0, 1]$. There are two random variables ξ and η with at joint distribution on $\mathbb{I} \times \mathbb{I}$ such that

(a) both ξ and η are uniformly distributed on $\mathbb{I}$,
(b) ξ and η are independent,
(c) both of them determine the other's value.

P r o o f . The idea of the construction is to find a subset $H \subseteq \mathbb{I} \times \mathbb{I}$ with the following properties:

(i) H is a graph of a bijection from $\mathbb{I}$ to $\mathbb{I}$,

(ii) H has a point in every positive (Lebesgue) measurable subset of $\mathbb{I} \times \mathbb{I}$.

When we have such an H, then define the σ-algebra Σ on H as the trace of the (Lebesgue) measurable sets of $\mathbb{I} \times \mathbb{I}$, and define the probability measure μ on H as

$$\mu(U \cap H) = \lambda(U)$$

whenever U is a measurable subset of $\mathbb{I} \times \mathbb{I}$. This definition is sound as if $U_1 \cap H = U_2 \cap H$ for two measurable subsets U_1 and U_2, then property (ii) ensures $\lambda(U_1) = \lambda(U_2)$. Let (ξ, η) be a random element of H distributed according to the measure μ. As H is a graph of a bijective function, property (c) holds. Now let $E \subseteq \mathbb{I}$ be (Lebesgue) measurable. Then

$$\text{Prob}(\xi \in E) = \mu(H \cap (E \times \mathbb{I})) = \lambda(E \times \mathbb{I}) = \lambda(E),$$

thus ξ is indeed uniformly distributed on $\mathbb{I}$, and similarly for η. Finally, let E and F be measurable subsets of $\mathbb{I}$. Then

$$\begin{aligned}\mathrm{Prob}(\,\xi \in E \text{ and } \eta \in F) &= \mu(H \cap (E \times F)) \\ &= \lambda(E \times F) = \lambda(E) \cdot \lambda(F) \\ &= \mathrm{Prob}(\,\xi \in E) \cdot \mathrm{Prob}(\,\eta \in F),\end{aligned}$$

which shows that ξ and η are independent.

Thus we need to find a subset $H \subset \mathbb{I} \times \mathbb{I}$ satisfying (i) and (ii). We will use transfinite induction (thus the axiom of choice) to add points of H. First note that every positive measurable set contains a positive closed set, and there are only continuum many closed sets. Let $F \subseteq \mathbb{I} \times \mathbb{I}$ be closed and positive, then F contains a generalized continuum by continuum grid. Namely, there are subsets U, $V \subseteq \mathbb{I}$ such that both U and V have continuum many elements and $U \times V \subseteq F$ [8]. Using these properties we proceed as follows.

Enumerate all closed positive sets as F_α, and all real numbers in $\mathbb{I}$ as x_α where α runs over all ordinals less than continuum. At each stage we add at most three new points to H. Suppose we are at stage indexed by α. As there is a continuum by continuum grid in F_α and until so far we added less than continuum many points to H, there is a point in F_α such that neither its x nor its y-coordinate has been chosen as an x (or y respectively) coordinate of any previous point. Add this element of F_α to H. Then look at the real number x_α. If there is no point in H so far with an x-coordinate (or y-coordinate) equal to x_α, then add the point (x_α, z) (the point (z, x_α)) to H, where z is not among the y-coordinates (x-coordinates) of points in H so far.

The set H we constructed during this process satisfies properties (i) and (ii). Indeed, every real number in $\mathbb{I}$ is a first (second) coordinate of some element of H. During the construction we made sure that every horizontal (vertical) line intersects H in at most a single point. Thus H is indeed a graph of a bijection of $\mathbb{I}$. Finally H contains a point from each positive closed subset of $\mathbb{I} \times \mathbb{I}$, and thus from each positive measurable subset as well. □

Remark that the bijection encoded by H is not measurable in the product space (which, incidentally, is the standard Lebesgue measure on $\mathbb{I} \times \mathbb{I}$).

Theorem 3.2. Given any access structure $\mathcal{A} \subset 2^P$, there is a perfect (non-measurable) secret sharing scheme realizing $\mathcal{A}$.

P r o o f . Take the pair of random variables $\langle \xi, \eta \rangle$ from Theorem 3.1. Give every participant ξ as a share, and set η as the secret. Now ξ determines η, therefore qualified subsets can recover the secret. Similarly, ξ and η are independent, therefore unqualified subsets have "no information on the secret." Consequently this is a perfect probabilistic secret sharing scheme realizing $\mathcal{A}$. Note that it is not measurable as the recovery function is not measurable. □

4. STRUCTURES REALIZED BY PERFECT AND WEAKLY PERFECT SCHEMES

From this point on only measurable schemes are considered. This section gives a complete characterization of access structures which can be realized by perfect or weakly perfect measurable schemes as defined in Definition 2.8. Recall that an access structure $\mathcal{A} \subset 2^P$ is *open* if the qualified sets form an open set in the Sierpiński topology.

Monotone span programs were introduced by Karchmer and Wigderson [13], and they are used to study linear schemes. To fit into our framework we extend it by allowing infinitely many participants and arbitrary vector spaces. Given a vector space V and a subset $H \subset V$, the *linear span* of H is the set of all (finite) linear combinations of elements of H. The linear span is a linear subspace of V.

Definition 4.1. Let P be the (possibly infinite) set of participants. A *span program* consists of a vector space V, a target vector $\mathbf{v} \in V$, and a function $\varphi : P \to 2^V$ which assigns a (not necessarily finite) collection of vectors to each participant. The structure $\mathcal{A} \subset 2^P$ is *realized* by the span program if

$$A \in \mathcal{A} \quad \Leftrightarrow \quad \mathbf{v} \in \text{linear span of } \bigcup\{\, \varphi(p) : p \in A\}.$$

It is clear that structures realized by span programs are monotone and finitely generated.

Theorem 4.2. The following statements are equivalent for any access structure $\mathcal{A} \subset 2^P$.

1 $\mathcal{A}$ is realized by a span program.

2 $\mathcal{A}$ is realized by a perfect measurable probabilistic scheme.

3 $\mathcal{A}$ is realized by a weakly perfect measurable probabilistic scheme.

4 $\mathcal{A}$ is open.

5 $\mathcal{A}$ is finitely generated.

P r o o f . The equivalence $4 \Leftrightarrow 5$ is the statement of Claim 2.1. The implication $2 \Rightarrow 3$ is trivial, thus we need to prove the implications $3 \Rightarrow 5$, $5 \Leftrightarrow 1$, and $5 \Rightarrow 2$.

$3 \Rightarrow 5$: We remark that $\mathcal{A}$ is finitely generated if and only if every qualified set contains a finite qualified set. Suppose that the weakly perfect measurable scheme $\mathcal{S} = \langle \mu, h \rangle$ realizes $\mathcal{A}$ and let $c \geq 1$ be the constant from Definition 2.8, equation (1).

Choose a subset $E_1 \subset X_s$ of the secrets so that both E_1 and its complement $E_2 = X_s - E_1$ is positive:

$$p_1 = \mu_s(E_1) > 0, \qquad p_2 = \mu_s(E_2) > 0,$$

and, of course, $p_1 + p_2 = 1$. Let $A \in \mathcal{A}$ be infinite, we must show that it has a finite qualified subset. The recovery function h_A is measurable, thus the sets $U_i = h_A^{-1}(E_i)$

are measurable, and $\mu^{As}(U_1 \times E_2) = \mu^{As}(U_2 \times E_1) = 0$ as h_A gives the right secret with probability 1. Consequently

$$\begin{aligned}\mu^A(U_1) &= \mu^{As}(U_1 \times X_s) = \mu^{As}(U_1 \times E_1) + \mu^{As}(U_1 \times E_2) \\ &= \mu^{As}(U_1 \times E_1) \\ &= \mu^{As}(U_1 \times E_1) + \mu^{As}(U_2 \times E_1) \\ &= \mu^{As}(X^A \times E_1) = \mu_s(E_1) = p_1.\end{aligned}$$

By item (d) of Claim 2.7, for every positive $\varepsilon > 0$ there is a finite subset $B \subset A$ such that setting $V_1 = \pi_B(U_1) \subseteq X^B$,

$$\mu^{Bs}(V_1 \times E_2) < \mu^{As}(U_1 \times E_2) + \varepsilon = \varepsilon,$$

and, by item (b) of the same Claim,

$$\mu^B(V_1) \geq \mu^A(U_1) = p_1.$$

Now we claim that if ε is small enough, then B is qualified. Indeed, $\mathcal{S}$ is weakly perfect with constant c, thus if B were unqualified then applying condition (1) for $V_1 \subseteq X^B$ and $E_2 \subseteq X_s$ we get

$$\frac{1}{c} \cdot p_1 \cdot p_2 \leq \frac{1}{c} \cdot \mu^B(V_1) \cdot \mu_s(E_2) \leq \mu^{Bs}(V_1 \times E_2) < \varepsilon.$$

But this inequality clearly does not hold when ε is small enough, proving the implication.

$5 \Rightarrow 1$: Suppose $\mathcal{A} \subset 2^P$ is finitely generated, say $\mathcal{A} = \mathrm{gen}(\mathcal{B})$, where every $B \in \mathcal{B}$ is finite. Let V be a large enough (infinite dimensional) vector space, and fix the target vector $\mathbf{v} \in V$. We want to assign vectors to participants so that $\mathbf{v}$ is in the linear span of the vectors assigned to members of $A \subseteq P$ if and only if A is qualified. This can be done as follows. For each $B \in \mathcal{B}$ (B is finite!) choose $|B| - 1$ vectors from V which are linearly independent from everything chosen so far (including the target vector), and set the $|B|$th vector so that the sum of these $|B|$ many vectors equals $\mathbf{v}$. Assign these vectors to the corresponding members of B. A participant $p \in P$ will receive all vectors assigned to him.

$1 \Rightarrow 5$: This is true as if $\mathbf{v}$ is in the linear span of $\bigcup\{\varphi(p) : p \in A\}$, then it is a finite linear combination, thus $\mathbf{v}$ is in the linear span of $\bigcup\{\varphi(p) : p \in A'\}$ for some finite $A' \subseteq A$.

$5 \Rightarrow 2$: The proof of the implication $5 \Rightarrow 1$ above gives the stronger result that if $\mathcal{A}$ is finitely generated, then it can be realized by a span program in which the vector space V is over some (in fact, any) finite field $\mathbb{F}$. This span program will be used to create the required probabilistic scheme.

Fix an arbitrary base H of the vector space V. For each $\mathbf{h} \in H$ from this base the dealer picks a random $r_{\mathbf{h}} \in \mathbb{F}$ independently and uniformly (this is where we need $\mathbb{F}$ to be finite). Every element $\mathbf{x}$ of the vector space V has a unique representation as a finite linear combination of base elements, say $\mathbf{x} = \sum_i \alpha_i \mathbf{h}_i$. Define $r(\mathbf{x})$ to be the field element $\sum_i \alpha_i r_{\mathbf{h}_i}$. Clearly, this r is a linear function, and $r(\mathbf{h}) = r_{\mathbf{h}}$ whenever $\mathbf{h} \in H$.

The dealer sets the secret to $r(\mathbf{v})$ where $\mathbf{v}$ is the goal vector. Participant p's share will be the collection $\langle \mathbf{x}, r(\mathbf{x})\rangle$ where $\mathbf{x}$ runs over the vectors in $\varphi(p)$. That is, p receives the share $r(\mathbf{x})$ (an element of $\mathbb{F}$) labeled by the public vector $\mathbf{x}$ for each vector $\mathbf{x}$ assigned to him. It is clear from the linearity of r that subsets of participants which have $\mathbf{v}$ in their linear span can compute the secret (as an appropriate linear combination of their shares), and shares of an unqualified set is independent of the secret, as was required. □

5. STRUCTURES REALIZED BY RAMP AND WEAKLY RAMP SCHEMES

This section characterizes access structures which can be realized by measurable (weakly) ramp schemes. The characterization uses the notion of Hilbert-space programs, which is similar to that of span programs, only the vector space is replaced by a Hilbert space, and the target vector should be in the *closure* of the linear span rather than in the linear span of the generating vectors.

We also prove a generalization of the main result of Chor and Kushilevitz [5] saying that if the scheme distributes infinitely many secrets, then the share domain of important participants should be large. Finally we give a ramp scheme which distributes infinitely many secrets, while every share domain is finite. Of course, in this scheme no participant can be important.

Definition 5.1. A *Hilbert-space program* consists of a Hilbert space H, a target vector $v \in H$, and a function $\varphi : P \to 2^H$ which assigns a subset of the Hilbert space to each participant. The structure $\mathcal{A} \subset 2^P$ realized by the Hilbert-space program is

$$A \in \mathcal{A} \quad \Leftrightarrow \quad v \in \text{closure of the linear span of } \bigcup\{\varphi(p) : p \in A\}.$$

Theorem 5.2. The following statements are equivalent for any access structure $\mathcal{A} \subseteq 2^P$.

1 $\mathcal{A}$ is realized by a Hilbert-space program;

2 $\mathcal{A}$ is realized by a ramp measurable probabilistic secret sharing scheme;

3 $\mathcal{A}$ is realized by a weakly ramp measurable scheme;

4 $\mathcal{A}$ is G_δ.

P r o o f . The implication $2 \Rightarrow 3$ is trivial; we will show $1 \Rightarrow 2$, $3 \Rightarrow 4$ and $4 \Rightarrow 1$. Also, we will use Claim 2.3 which gives an equivalent characterization of G_δ structures.

$3 \Rightarrow 4$: Let $\mathcal{S} = \langle \mu, h\rangle$ be a weakly ramp scheme which realizes $\mathcal{A} \subset 2^P$. As in the proof of Theorem 4.2, choose $E_1 \subset X_s$, $E_2 = X_s - E_1$ so that

$$p_1 = \mu_s(E_1) > 0, \qquad p_2 = \mu_s(E_2) > 0, \qquad p_1 + p_2 = 1.$$

As the set of all participants is always qualified, and h_P is measurable, the sets $U_i = h_P^{-1}(E_i) \subseteq X_P$ are measurable, $\mu^{Ps}(U_1 \times E_2) = \mu^{Ps}(U_2 \times E_1) = 0$, and

$$\mu^P(U_1) = \mu^{Ps}(U_1 \times E_1) = p_1.$$

Let us define the family $\mathcal{B}_n$ of finite subsets of P as follows:

$$B \in \mathcal{B}_n \quad \Leftrightarrow \quad B \text{ is finite, and } \mu^{Bs}(\pi_B(U_1) \times E_2) < \frac{1}{n}.$$

It is clear that $\mathcal{B}_{n+1} \subseteq \mathcal{B}_n$, thus $\mathcal{B} = \bigcap_n \operatorname{gen}(\mathcal{B}_n)$ is G_δ. We claim that a subset of participants is qualified if and only it is in $\mathcal{B}$. First, let $A \subseteq P$ be qualified. Then $g_A = h_P \circ \pi_A$ is a (measurable) recovery function for A, thus letting $V_1 = g_A^{-1}(E_1)$, $\mu^{As}(V_1 \times E_2) = 0$, and then for each n there is a finite $B_n \subseteq A$ such that

$$\mu^{B_n s}(\pi_{B_n}(V_1) \times E_2) < \frac{1}{n}.$$

Observing that $V_1 = \pi_A(U_1)$, we get that $A \in \operatorname{gen}(\mathcal{B}_n)$ for each n, as was required. In the other direction, let $B \subseteq P$ be not qualified, and let $V_1 = \pi_B(U_1) \subseteq X^B$. As $\mu^B(V_1) \geq \mu^P(U_1) = p_1 > 0$ and $\mu_s(E_2) = p_2 > 0$, the weakly ramp property gives

$$\mu^{Bs}(V_1 \times E_2) = \mu^{Bs}(\pi_B(U_1) \times E_2) > 0.$$

For any subset B' of B, $\mu^{B's}(\pi_{B'}(U_1) \times E_2) \geq \mu^{Bs}(V_1 \times E_2)$, consequently B is not in $\operatorname{gen} \mathcal{B}_n$ when $n \geq 1/\mu^{Bs}(V_1 \times E_2)$.

$4 \Rightarrow 1$: Let $\mathcal{B}_1 \supseteq \mathcal{B}_2 \supseteq \cdots$ be families of finite subsets of P such that $\mathcal{A} = \bigcap_n \operatorname{gen}(\mathcal{B}_n)$, as given by Claim 2.3. Then $A \in \mathcal{A}$ if and only if A is in $\operatorname{gen}(\mathcal{B}_n)$ for infinitely many n. Let H be a huge dimensional (not separable) Hilbert space, and fix an orthonormal base $e_1, e_2, \ldots$, (countably many elements) plus $\{\bar{e}_\alpha : \alpha \in I\}$ for some index set I. The target vector will be

$$v = e_1 + \frac{e_2}{2} + \frac{e_3}{3} + \cdots,$$

and let $v_n = \sum_{i=1}^n e_i/i$. (Actually, instead of $1/i$ one can take arbitrary non-zero coefficients a_i as long as $\sum_i a_i^2$ converges.) For each (finite) $B \in \mathcal{B}_n$, the first $|B| - 1$ members of B will be assigned new base elements from among $\bar{e}_\alpha$, and the last member will be assigned an element from H so that the sum of these $|B|$ elements be equal to v_n.

The target vector is in the closure of the linear span of Hilbert space elements assigned to members of $A \subseteq P$ if and only if v_n is in their linear span for infinitely many n. But this latter event happens if and only if A is in $\operatorname{gen}(\mathcal{B}_n)$, thus this Hilbert-space program realizes $\mathcal{A}$, as required.

$1 \Rightarrow 2$: Let H be the (real) Hilbert space over which the program is defined, and fix an orthonormal base $\{e_\alpha : \alpha \in I\}$ of H. For each element in this base assign a standard normal random variable ξ_α so that they are totally independent. An element $a \in H$ can be written as

$$a = \sum \lambda_\alpha e_\alpha, \quad \text{where } \sum \lambda_\alpha^2 < \infty.$$

Assign the (random) variable $\xi_a = \sum \lambda_\alpha \xi_\alpha$ to this element $a \in H$. More information about these *Gaussian spaces* can be found in [11]. We list here only some basic properties which will be needed for our construction.

The random variable ξ_a is normal with expected value 0 and variance $\|a\|^2$, furthermore ξ_a and ξ_b are independent if and only if a and b are orthogonal. If v is in the

closure of the linear span of $E \subseteq H$, then ξ_v is determined (with probability 1) by the values of $\{\xi_a : a \in E\}$.

Let $L \subseteq H$ be a closed linear subspace. Any $v \in H$ has an orthogonal decomposition $v = v_1 + v_2$ such that $v_1 \perp L$ and $v_2 \in L$. If $v_1 \neq 0$ then ξ_v has a conditional distribution given the values of all ξ_a for $a \in L$, and this distribution is normal with variance $\|v_1\|^2$ (the expected value depends on the values of the variables ξ_a).

We define a secret sharing scheme $\mathcal{S}$ realizing $\mathcal{A}$ as follows. Every domain will be either the set of reals or some power of the reals. Let $v \in H$ be the target vector. The secret is the value of ξ_v. The share of participant $p \in P$ is the collection of the values of ξ_a for all elements $a \in H$ assigned to p.

If $A \subseteq P$ is qualified, then v is in the closure of the linear span, thus ξ_v is determined by the shares of A. If $B \subseteq P$ is unqualified, then the target vector is not in the closure of the linear span, let $v_1 \neq 0$ be its orthogonal component. The conditional distribution of the secret, *given all shares of* B, is normal with $\|v_1\|^2$ variance. As the density function of the normal distribution is nowhere zero, the probability that the secret is in the set $E \subseteq R$, both in the unconditional and in the conditional case, is zero if and only if E is a zero set. Consequently this $\mathcal{S}$ is a *weakly ramp scheme* realizing $\mathcal{A}$. It is easy to see that this scheme is never ramp as the ratio of the conditional and unconditional distribution function is never bounded.

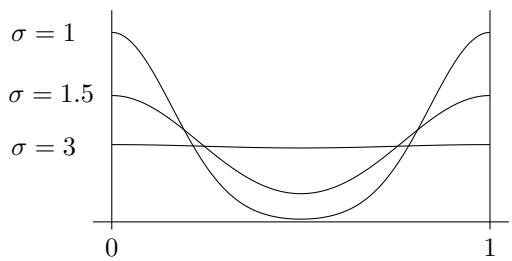

Fig. 1. Density function of the fractional part of a normal variable.

However, one can twist this scheme to be a ramp one. The only change is to set the secret to be the *fractional part* of ξ_v, see this trick in [7]. The density function of the fractional part of a normal random variable is depicted on Figure 1 for different variances. There is a $c > 1$, depending on the variance only, such that this density function is between $1/c$ and c. Consequently the conditional distribution of the secret given the shares of an unqualified set (which is the fractional part of another normal distribution) is also bounded, where the bound depends on the subset only and not on the actual values of the shares. Consequently this scheme is a ramp scheme realizing $\mathcal{A}$. □

Next we prove a generalization of the main result of Chor and Kushilevitz [5]. It follows from a slightly more general statement which we prove first.

Theorem 5.3. Suppose $\mathcal{S}$ is a measurable ramp scheme, A and B are disjoint unqualified sets such that $A \cup B$ is qualified. Suppose moreover that there are infinitely many secrets. Then μ^A is atomless.

An immediate consequence is that under the same conditions the set of shares of A, namely X^A, must have cardinality (at least) continuum.

Proof. Suppose by contradiction that X^A is atomic and $\mu^X(\{a\}) > 0$ for some $a \in X^A$. Partition the set of secrets into countably many positive sets as $X_s = \bigcup_i E_i$ where $\mu_s(E_i)$ is positive. Let $h : X^A \times X^B \mapsto X_s$ be the function which determines the secret given the shares of A and B. Let

$$V_i = \{y \in X^B : h(a, y) \in E_i\}.$$

As h is measurable, each V_i is measurable, moreover the sets $\{a\} \times V_i \times E_i$ and $\{a\} \times X^B \times E_i$ have the same measure. Using the boundedness property for A we get

$$\begin{aligned} \mu^{Bs}(V_i \times E_i) &\geq \mu^{ABs}(\{a\} \times V_i \times E_i) \\ &= \mu^{ABs}(\{a\} \times X^B \times E_i) \\ &= \mu^{As}(\{a\} \times E_i) \\ &\geq \frac{1}{c_A} \cdot \mu^A(\{a\}) \cdot \mu_s(E_i). \end{aligned}$$

Applying the boundedness twice for B we have

$$\begin{aligned} \mu^{Bs}(V_i \times E_1) &\geq \frac{1}{c_B} \cdot \mu^B(V_i) \cdot \mu_s(E_1) \\ &= \frac{\mu_s(E_1)}{c_B^2 \cdot \mu_s(E_i)} \cdot c_B \mu^B(V_i) \cdot \mu_s(E_i) \\ &\geq \frac{\mu_s(E_1)}{c_B^2 \cdot \mu_s(E_i)} \mu^{Bs}(V_i \times E_i) \\ &\geq \frac{1}{c_B^2 c_A} \cdot \mu_s(E_1) \cdot \mu^A(\{a\}), \end{aligned}$$

where we used $\mu(E_i) > 0$ and the previous estimate in the last step. As h is defined on $X^A \times X^B$ and $\bigcup_i E_i = X_s$, we have $\bigcup_i V_i = X^B$, furthermore the V_i's are pairwise disjoint. Thus

$$1 \geq \mu^{Bs}(X_B \times E_1) = \sum_i \mu^{Bs}(V_i \times E_1) \geq \sum_i \left(\frac{1}{c_B^2 c_A} \cdot \mu_s(E_1) \cdot \mu^A(\{a\})\right),$$

which can happen only when $\mu^A(\{a\}) = 0$, a contradiction. □

A participant $p \in P$ is *important* if there is an unqualified set $B \subseteq P$ such that $B \cup \{p\}$ is qualified.

Corollary 5.4. Suppose $\mathcal{S}$ is a measurable ramp scheme which distributes infinitely many secrets. Then the share domain of every important participant must have cardinality at least continuum.

P r o o f . By assumption, no singleton is qualified, thus we can apply Theorem 5.3 with $A = \{p\}$ and the unqualified B such that $A \cup B$ is qualified. As μ_p is atomless, X_p must have at least continuum many elements. □

Surprisingly there are interesting ramp schemes where no participant is important, thus this Corollary is not applicable. We sketch here a ramp scheme which distributes infinitely many secrets, while every participant has a finite share domain – consequently no participant can be important.

In the scheme participants are indexed by the positive integers, and X_s – the set of secrets – is also the set of positive integers. The dealer chooses the secret $s \in X_s$ with probability 2^{-s}. After choosing the secret, she picks a *threshold number* $t > s$ with probability 2^{-t+s}. The participant with index $i \leq t$ gets an integer from $[1, i]$ uniformly and independently distributed, participant with index $i > t$ gets s as the share.

The secret can be recovered by any infinite set of participants as the eventual value of their shares, while any finite set is unqualified. It is easy to see that this scheme is (measurable) ramp realizing all infinite subsets of the positive integers, and has the required properties.

6. CONCLUSION

In this paper we looked at the theoretical problems of infinite probabilistic secret sharing schemes. It is quite natural to look at the classical secret sharing schemes from a probabilistic point of view. While the first few steps towards an abstract definition are easy, interesting and unexpected phenomena appear quite early. The non-measurable scheme in Section 3 was our first surprise. Without such a "technical" restriction as the measurability of the recovery function, nothing can be said.

Some interesting infinite schemes in [7] do not seem to fit into the security types defined in Section 2.5. Also, there are access structures which cannot be realized by any measurable scheme which could be considered to be secure in any sense shown by the following example.

> Let P be the lattice points in the positive quadrant; minimal qualified sets are the "horizontal" lines.

Suppose there are only two secrets (this can always be assumed). As the first row is qualified, there are finitely many participants in the first row who can determine the secret up to probability at least 0.9. Similarly, finitely many participants from the second row know the secret up to probability 0.99; finitely many from the third row with probability 0.999, etc. The union of these finite sets will know the secret with probability 1, thus this set will be qualified, while it intersects each row in finitely many elements. (We actually showed that this structure is not G_δ at the end of Section 2.2.)

The nice, and surprisingly natural, characterization of ramp and weakly ramp schemes in Section 5 hints that our definition is "the" right one. As remarked earlier, no universally accepted definition exists for weakly perfect, or ramp schemes. One flavor of definition uses entropies. If A is qualified, then the conditional entropy of the secret, given the shares of A, is zero. If the shares of B are independent of the secret, then the conditional entropy equals the entropy of the secret. A scheme is *ramp*, if for unqualified

subsets, this conditional entropy is never zero. While this definition is widely applied in getting lower bounds on the size of the shares in ramp schemes, it does not fit our definition. The correct translation would be requiring the *min-entropy* to be positive: a classical scheme $\mathcal{S}$ is *ramp* if for each value the secret can take with positive probability, the conditional probability of the same value for secret, given the value of the shares, is still positive. In other words: in a ramp scheme unqualified subsets cannot exclude any possible secret value (while the posterior probability that the secret takes that value might be much smaller than the a priori probability).

There are other interesting probabilistic schemes in [7] which have weaker security guarantees than weakly ramp schemes. In those schemes unqualified subsets can exclude large subsets of the secret space, while still some uncertainty remains. A typical example is where participant $i \in \mathbb{N}^+$ has a uniform random real number from $[0, 2^{-i}]$ as a share, and the secret is the sum of all shares. If participant i is missing, the rest can determine the secret up to an interval of length 2^{-i}, and within that interval the secret is uniformly distributed. Is there any structure which can be realized by such a scheme, but not by any ramp scheme? How can these scheme types be captured by a definition similar to those in Definition 2.8?

Finally we pose a question in another direction. Given an access structure $\mathcal{A}$, is there an easy way to recognize whether it is G_δ? Given any collection of qualified and unqualified subsets, decide if there is a G_δ structure separating them. As a concrete example: suppose there is a collection of unqualified subsets of P so that the union of any two of them is qualified. Under what conditions is there a ramp scheme realizing such a structure?

ACKNOWLEDGEMENT

The author would like to thank the support and the uncountably many discussions while developing the ideas in this paper of the members of the Cryptography group at the Rényi Institute. Their input was indispensable in forming and correcting the ideas presented here. Special thanks go to Gábor Tardos who asked about measurability and constructed the paradoxical example cited in this paper. Discussions with Balázs Gyenis about Hilbert spaces clarified the characterization of ramp schemes.

The research reported in this paper was partially supported by GACR project number 19-04579S, and by the Lendület program of the Hungarian Academy of Sciences.

(Received October 24, 2022)

REFERENCES

[1] J. Azema, M. Yor, F. Meyer, and R. de la Rue: Espaces de Lebesgue. In: Séminaire de Probabilités XXVII, volume 1557 of Lecture Notes in Mathematics, pages Springer Berlin – Heidelberg 1993, pp. 15–21. DOI:10.1007/BFb0087958

[2] A. Beimel: Secret-sharing schemes: A survey. In: IWCC (Y.-M. Chee, Z. Guo, S. Ling, F. Shao, Y. Tang, H. Wang, and Ch. Xing, eds.), volume 6639 of Lecture Notes in Computer Science, Springer 2011, pp 11–46.

[3] G. R. Blakley and L. Swanson: Infinite structures in information theory. In: CRYPTO 1982, pp. 39–50. DOI:10.1080/15244118208548018

[4] J. T. Chang and D. D. Pollard: Conditioning as disintegration. Statistica Neerlandica *51* (1997), 3, 287–317. DOI:10.1111/1467-9574.00056

[5] B. Chor and E. Kushilevitz: Secret sharing over infinite domain. J. Cryptology *6* (1993), 2, 97–86. DOI:10.1007/BF02620137

[6] A. Dibert: Generalized Secret Sharing. Master's Thesis, Central European University, Budapest 2011.

[7] A. Dibert and I. Csirmaz: Infinite secret sharing – Exmples. J. Math. Cryptology *8* (2014), 2, 141–168. DOI:10.1515/jmc-2013-0005

[8] H. G. Eggleston: Two measure properties of cartesian product sets. Quater. J. Math. Oxford *5* (1954), 108–115. DOI:10.1093/qmath/5.1.108

[9] D. H. Fremlin: Measure Theory, Volume 2. Torres Fremlin, Colchester 2003.

[10] J. Haezendonck: Abstract Lebesgue–Rokhlin spaces. Bull. Soc. Math. Belgique *25* (1973), 243–258.

[11] S. Janson: Gaussian Hilbert Spaces. Cambridge Tracts in Mathematics. Cambridge University Press, 1997.

[12] O. Kallenberg: Foundations of Modern Probability. Probability and Its Applications Series. Springer, 2010.

[13] M. Karchmer and A. Wigderson: On span programs. In: Structure in Complexity Theory Conference 1993, pp. 102–111.

[14] B. H. Makar: Transfinite cryptography. Cryptologia *4* (1980), 4, 230–237. DOI:10.1080/0161-118091855176

[15] J. Patarin: Transfinite cryptography. IJUC *8* (2012), 11–72.

[16] R. Phan and S. Vaudenay: On the impossibility of strong encryption over $\aleph_0$. In: Coding and Cryptology (Y. Chee, Ch. Li, S. Ling, H. Wang, and Ch. Xing, eds.), volume 5557 of Lecture Notes in Computer Science, Springer, Berlin–Heidelberg 2009, pp. 202–218. DOI:10.1007/978-3-642-01877-0_17

[17] V. A. Rokhlin: On the fundamental ideas of measure theory. Trans. Amer. Math. Soc. *10* (1962), 1–54.

[18] T. Tao: An introduction to measure theory. Amer. Math. Soc., Graduate Studies Math. *126* (2011), 206 pp. DOI:10.1090/gsm/126

[19] S. Watson: Power of the Sierpiński space. Topology Appl. *35* (1990), 2–3, 299–302. DOI:10.1016/0166-8641(90)90114-H

Laszlo Csirmaz, Alfred Renyi Institute of Mathematics, Budapest Hungary and Institute of Information Theory and Automation, The Czech Academy of Sciences, Pod Vodárenskou věží 4, 182 08 Praha 8. Czech Republic.

e-mail: csirmaz@renyi.hu