Probabilistic Infinite Secret Sharing*

László Csirmaz[1]

[1]Central European University, Budapest
csirmaz@renyi.hu

Abstract

The study of probabilistic secret sharing schemes using arbitrary probability spaces and possibly infinite number of participants lets us investigate abstract properties of such schemes. It highlights important properties, explains why certain definitions work better than others, connects this topic to other branches of mathematics, and might yield new design paradigms.

A *probabilistic secret sharing scheme* is a joint probability distribution of the shares and the secret together with a collection of *secret recovery functions* for qualified subsets. The scheme is measurable if the recovery functions are measurable. Depending on how much information an unqualified subset might have, we define four scheme types: *perfect*, *almost perfect*, *ramp*, and *almost ramp*. Our main results characterize the access structures which can be realized by schemes of these types.

We show that every access structure can be realized by a non-measurable perfect probabilistic scheme. The construction is based on a paradoxical pair of independent random variables which determine each other.

For measurable schemes we have the following complete characterization. An access structure can be realized by a (measurable) perfect, or almost perfect scheme if and only if the access structure, as a subset of the Sierpiński space $\{0,1\}^P$, is open, if and only if it can be realized by a span program. The access structure can be realized by a (measurable) ramp or almost ramp scheme if and only if the access structure is a G_δ set (intersection of countably many open sets) in the Sierpiński topology, if and only if it can be realized by a Hilbert-space program.

Keywords: secret sharing; probability space; Sierpiński topology; product measure; span program; Hilbert space program.
AMS classification numbers: 60B05, 94A62, 46C99, 54D10

1 Introduction

The topic of this paper is to study secret sharing schemes where the domain of the secret, the domain of the shares, or the set of players are not necessarily finite. This type of approach studying infinite objects instead of finitary ones is not novel even in the realm of cryptography, see, e.g., [3, 5, 12, 13, 14]. Further motivation and several examples can be found in the companion paper [7]. As can be expected, even finding the right definitions can be hard and far from trivial, we elaborate on this issue in Section 6.

Secret sharing has several faces. In particular, it can be investigated equally from either combinatorial or probabilistic point of view, see, for example, 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 secret sharing schemes as (joint) probability distributions of shares and the secret. Defining probability measures on arbitrary (product) spaces is not without problems, see [1, 8, 15] for a general description of the problems, especially how and when conditional distribution can be defined. Our definitions avoid referring to conditional distributions at the

*This research has been partially supported by the "Lendület" Program.

expense of a less transparent and less intuitive formulation of the concept. In Sections 2.3 and 2.4 we give all necessary definitions from Probability Theory we will use later on. Nevertheless, a good working knowledge of measure theory and probability spaces, as can be found, e.g., in [10], definitely helps.

A basic requirement in secret sharing is that qualified subsets should be able to recover the secret. The most straightforward way to ensure this property is via *recovery functions*: for each qualified subsets A there is a function h_A which, given the shares of members of A, gives the value of the secret. In the classical case, recovery functions only affect the efficiency of the system. Quite surprisingly, this is far from the truth in general. In Section 3 we present a scheme in which every share determines the secret, while every collection of the shares is *independent* of the secret, i.e. "gives no information on the secret." The usual way to avoid such "uninteresting" or "pathological" cases is requiring the relevant functions to be *measurable*. This is exactly what we do here: we focus on *measurable* schemes where recovery functions are measurable.

Depending on how much information an unqualified subset might have on the secret, we define four types. In *perfect* schemes 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 *almost perfect*, if for some constant $c \geq 1$ the ratio of the conditional and unconditional probabilities is always between $1/c$ and c. An almost perfect scheme with $c = 1$ is perfect. Almost perfect schemes were introduced in [5] where they were called "c-scheme."

We call a scheme *ramp* when the constant which bounds the ratio of conditional and unconditional probabilities should not be uniform but might depend on the unqualified set (but not on the value of the actual shares). Finally the scheme is *almost ramp* if the constant might depend on the value of the actual value of the shares. In the last case the condition can be rephrased as unqualified subsets cannot exclude any value of the secret with positive probability.

In Sections 4 and 5 we characterize the access structures which can be realized by schemes of these types. We have both topological and structural characterizations. Subsets of P can be considered as points in the product space $\{0,1\}^P$, therefore access structures are subsets of this space. Equipping $\{0,1\}$ with some topology, we can speak about topological properties of access structures. The *Sierpiński topology* [17] is especially promising, as it has some intriguing properties used in logic. In our case, when P is finite, a structure in the Sierpiński topology is open if and only if it is upward closed. For definitions and examples for this topology, see Section 2.2. We prove that a scheme can be realized by a perfect, or by an almost perfect, scheme if and only if it is open. Similarly, a scheme can be realized by a ramp, or by an almost ramp, scheme if and only if the scheme is G_δ, that is, the intersection of countably many open sets.

The structural characterization uses *span programs* introduced in [11] and its generalization, *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 or participants whose vectors span the target vector. In a Hilbert-space program the vector space is replaced by a Hilbert space, and a subset is realized 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 a span program, 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, discuss further scheme types, and list some open problems.

2 Definitions

In this section we present the main definitions. We start with access structures, then continue with the Sierpiński topology, and show how this topology can be used. Then we give the definition of probability secret sharing scheme, and enlist some properties of probability on product spaces. Finally we define different types of schemes depending on how much information an unqualified subset might have. Due to the lack of space, motivations for some of the definitions can be found in the companion paper [7].

2.1 Access structure

An access structure is a non-trivial upward closed family of subsets of the set P of participants: $\mathcal{A} \subset 2^P$. To avoid certain trivialities, we assume that $\mathcal{A}$ dos not contain any singletons, and is not empty. Given $\mathcal{A}_0 \subset 2^P$, the structure *generated by* $\mathcal{A}_0$ is defined as

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

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

2.2 Sierpiński topology

The *Sierpiński space* SP is a topological space defined on the two element set $\{0,1\}$, where the open sets are the empty set, $\{1\}$, and $\{0,1\}$, see [17]. 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 of SP. Consider the product space SP^P; its elements are the characteristic functions of subsets of P, so these points can be identified with subsets of P. Thus a collection $\mathcal{A}$ of subsets of P naturally corresponds to a subset of the topological space SP^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 SP^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.

As in connection with access structures only the Sierpiński topology is used, we tacitly assume that all topological notions in this paper refer to this topology.

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*

$$A \in \mathcal{A} \quad \Leftrightarrow \quad A \in \mathrm{gen}(\mathcal{B}_i) \;\; \textit{for all } i,$$

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

Proof. As $\mathcal{B}_i$ has only finite elements, $\mathrm{gen}(\mathcal{B}_i)$ is open, and then $\bigcap_i \mathrm{gen}(\mathcal{B}_i)$ 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

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

As V_i is open, $V_i = \mathrm{gen}(\mathcal{B}_i)$, 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 what 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: 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 $A_i \in \mathcal{A} \subseteq \mathrm{gen}(\mathcal{B}_i)$, 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 $B \in \mathrm{gen}(\mathcal{B}_i)$, as $B_i \in \mathcal{B}_i$ is a subset of B, thus $B \in \bigcap_i \mathrm{gen}(\mathcal{B}_i)$. 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:

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

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

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

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, ..., 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 so that qualified subsets could recover the secret's value from their shares, while forbidden subset should have no, or only limited, information on the secret. 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 denoted by X_s, and the *domain of shares* for the participant $i \in P$ is denoted by 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 distributed.

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 shall put $X = \prod_{i \in I} X_i$, and for any subset $J \subseteq I$ we let $X^J = \prod_{i \in J} X_i$ to be the restriction of X into coordinates in J.

Informally, a *probabilistic secret sharing scheme* is a probability distribution on the set $X = \prod_{i \in I} X_i$ 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 $\mathcal{S} = \langle \mu, h \rangle$, where
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, for $i \in P$, X_i is the set of (possible) shares for participant i; and
h is the collection of *recovery functions*: for each qualified $A \subseteq P$ the function $h_A : X^A \to X_s$ tells the secret given the shares of members of A.

When the dealer uses the scheme $\mathcal{S} = \langle \mu, h \rangle$, she simply 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 gives the participant $i \in P$ the share $\xi_i = x(i)$, the i-coordinate of x.

When members of $A \subseteq P$ want to recover the secret, they simply use the recovery function h_A on their shares to pinpoint the secret value.

Of course, we want qualified subsets to recover the secret from their shares. A scheme *realizes* an access structure, if this is indeed the case, at least with probability 1. To formalize this notion, we look at all possible distribution of shares and the secret where the secret is computed according to the recovery function h_A. When $x \in X$ is such a distribution, then the *projection* $\pi_A(x)$ is its restriction to coordinates (indices) in A, thus the recovery function gives the secret value $h_A(\pi_A(x)) \in X_s$. So x_s should be equal to this value, and the probability of those sequences x for which this happens must be 1.

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

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

Recovery functions are determined almost uniquely by the distribution μ. Indeed, let h_A and h_A^* be two recovery functions. The set of those points where h_A and h_A^* and 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, by assumption, both sets have measure zero. Also, recovery functions are *coherent* in the following sense: if A is qualified and $A \subseteq B$, then $h^*_B(y) = h_A(\pi_A(y))$ is also a recovery function mapping shares of B into the proper secrets, thus it must be equal to h_B almost everywhere.

In a secret sharing scheme we also want unqualified subsets have no, or limited information on the secret. As the precise definitions require some preparations from Probability Theory, we postpone them to Section 2.5.

2.4 Probability measure on product spaces

As usual in probability theory [10], the definition of a probability measure μ on the 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

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

It is easy to check that Σ^J is a σ-algebra on X^J. For each $J \subset I$ the *projection function* π_J maps any element $x \in X$ into X^J keeping only 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 Σ 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 the $\langle X, \Sigma\rangle$ space. Elements of Σ are the *events*, and the probability of the event $E \in \Sigma$ is just $\mu(E)$. As usual, μ is completed, i.e., not only elements of Σ have probability, but subsets of zero probability sets 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., 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 denote $\mu^{\{j\}}$ as μ_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 when defining a probabilistic secret sharing scheme.

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

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 $J \subseteq I$, $\mu^J\big(\pi_J(E)\big) \ge \mu(E)$.

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 $\mu(E) \le \mu^J(\pi_J(E)) < \mu(E) + \varepsilon$.

Proof. 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 $C_n = \pi_{J_n}^{-1}(\pi_{J_n}(C))$ 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 will fall into the set $U \subseteq X^B$ with probability $\mu^B(U)$. Similarly, if $E \subseteq X_s$ 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 comes from the set U with $\mu^B(U) > 0$ is defined as

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

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 not always exist [4], nevertheless in statistics their existence is almost always assumed. Fortunately, at the expense of a bit more complicated and less intuitive formulation, we can avoid the usage if those conditional distributions.

2.5 Perfect schemes, ramp schemes, and everything in between

When using a secret sharing scheme, *unqualified* subsets of the participants are required to have no information, or at least limited information on the secret. Depending on what this requirement is exactly, we distinguish several different type of schemes.

Definition 2.8. Let $\mathcal{S} = \langle \mu, h \rangle$ be a secret sharing scheme on the set P of participants. We call the scheme *perfect*, *almost perfect*, *ramp*, or *almost ramp* scheme, if the collective shares of any unqualified subset $B \subseteq P$ satisfies the condition listed below:

- **perfect**: B gets no information on the secret. In other words, the collective shares of B and the secret are (statistically) independent. That is, for every measurable $U \subseteq X^B$ and $E \subseteq X_s$,
$$\mu^{Bs}(U \times E) = \mu^B(U) \cdot \mu_s(E).$$
This fact can be expressed as the conditional probability $\mu_s(\cdot|U)$ coincides with $\mu_s(\cdot)$ for all $U \subseteq X^B$ with $\mu^B(U) > 0$.

- **almost perfect**: for all unqualified B the conditional probabilities $\mu_s(\cdot|U)$ might deviate from $\mu_s(\cdot)$ by a constant factor only, i.e. for some positive constant $c \geq 1$ (independently of B, depending only on the scheme)
$$\frac{1}{c} \cdot \mu^B(U) \cdot \mu_s(E) \leq \mu^{Bs}(U \times E) \leq c \cdot \mu^B(U) \cdot \mu_s(E) \tag{1}$$
for all measurable $U \subseteq X^B$ and $E \subseteq X_s$.

- **ramp**: the constant $c = c_B$ in (1) might depend on the subset B (but, of course, should not depend on U and E).
- **almost ramp**: based on their collective shares, no subset of the secrets with positive measure can be excluded:
$$\mu^B(U) \cdot \mu_s(E) > 0 \text{ implies } \mu^{Bs}(U \times E) > 0$$
(observe that the inverse implication always holds).

These definitions extend the usual ones for classical secret sharing schemes. In perfect schemes the collection of shares of any unqualified set is statistically independent of the secret, which is the traditional requirement. *Almost perfect* schemes were introduced [5], where an almost perfect scheme with constant c was called a "c scheme." There is no universally accepted definition 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 last two definitions reflect this idea. However, see the discussion in Section 6.

When $\mathcal{S}$ is traditional, 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 almost perfect, ramp, and almost ramp schemes are equivalent, while there are (traditional) schemes which are almost perfect, but not perfect.

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

$$\textit{perfect} \Rightarrow \textit{almost perfect} \Rightarrow \textit{ramp} \Rightarrow \textit{almost ramp}.$$

None of the implications can be reversed.

Proof. It is not difficult to construct schemes witnessing the irreversibility of these implications, see [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 it is shown in Theorem 3.2. The proof uses the following paradoxical construction of two random variables, which shows that independence and determinacy are not necessarily mutually exclusive.

Theorem 3.1 (G. Tardos, [16])**.** *Let I denote the unit interval* $[0, 1]$. *There are two random variables ξ and η with at joint distribution on $I \times I$ such that*

a) both ξ and η are uniformly distributed on I,
b) ξ and η are independent,
c) both of them determine the others value uniquely.

Proof. The idea of the construction is to find a subset $H \subseteq I \times I$ with the following properties:

1) H is a graph of a bijection from I to I,
2) H has a point in every positive (Lebesgue) measurable subset of $I \times I$.

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

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

whenever U is a measurable subset of $I \times I$. 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 2) above 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) evidently holds. Now let $E \subseteq I$ be (Lebesgue) measurable. Then

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

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

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

which shows that ξ and η are independent, indeed.

Thus we only need to show how to find the subset $H \subset I \times I$. We shall use transfinite induction (thus the axiom of choice) to pick points of H. First note that every positive measurable set contains a positive closed set, and there are only continuum many such sets. Let $F \subseteq I \times I$ be closed and positive, then F contains a generalized continuum large grid. Namely, there are subsets U, $V \subseteq I$ such that both U and V have continuum many elements and $U \times V \subseteq F$. Using these properties we proceed as follows.

Enumerate all closed positive sets as F_α, and all real numbers in I as x_α where α runs over all ordinals less than $\mathbf{c} = 2^\omega$. At each stage we add at most three 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 1) and 2). Indeed, every real number in I will be 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 I. Finally H contains a point from each positive closed subset of $I \times I$, and thus from each positive measurable subset as well. □

We remark that the bijection H encodes is not measurable in the product space (which, incidentally, is the standard Lebesgue measure on $I \times I$).

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

Proof. Take the pair of random variables $\langle \xi, \eta \rangle$ from Theorem 3.1. Give everyone ξ as a share, and set η as the secret.

ξ determines η, therefore qualified subsets can recover the secret.

ξ and η are independent, therefore unqualified subsets have "no information on the secret."

Consequently this is a perfect probabilistic secret sharing scheme realizing $\mathcal{A}$. We remark, that it is not measurable, as the recovery function is not measurable. □

4 Structures realized by (almost) perfect schemes

From this point on all schemes are assumed to be measurable. In this section we give a complete characterization of access structures which can be realized by perfect and almost perfect schemes as defined in Definition 2.8. Recall that an access structure $\mathcal{A} \subset 2^P$ is open, if it is open in the Sierpiński topology.

Monotone span programs were introduced by Karchmer and Wigderson in [11], and they are used to define *linear schemes.* To fit to our purposes, we extend the notion of span programs by allowing infinitely many participants and arbitrary vector spaces. If V is a vector space and $H \subset V$, then the *linear span* of H is the set of all (finite) linear combinations of elements of H.

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 participants. The structure $\mathcal{A} \subset 2^P$ *realized* by the span program is defined as

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

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 an almost perfect measurable probabilistic scheme;*
4. *$\mathcal{A}$ is open;*
5. *$\mathcal{A}$ is finitely generated.*

Proof. 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 $3 \Rightarrow 5$, $5 \Rightarrow 1$, and $1 \Rightarrow 2$.

$3 \Rightarrow 5$: We remark that $\mathcal{A}$ is finitely generated if and only if every qualified set contains a finite qualified set. Suppose that the almost perfect 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 almost 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 $\mathcal{A} = \text{gen}(\mathcal{B})$, 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 this $|B|$ many vectors be equal to $\mathbf{v}$. Assign these vectors to the members of B. A participant $p \in P$ will receive all vectors assigned to him.

1 $\Rightarrow$ 2: If $\mathcal{A} \subset 2^P$ is realized by any span program, then it is finitely generated. 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. Thus if $\mathcal{A}$ can be realized by any span program, then it can be realized by a span program over a finite field $\mathbb{F}$.

Fix a base H of the vector space V, and for each $\mathbf{h} \in H$ the dealer picks $r_{\mathbf{h}} \in \mathbb{F}$ uniformly and independently (this is where we need $\mathbb{F}$ to be finite). Write the goal vector in base H as the finite sum $\mathbf{v} = \sum_j \beta_j \mathbf{h}_j$ ($\mathbf{h}_j \in H$), and set the secret to be $s = \sum_j \beta_j r_{\mathbf{h}_j}$.

Next, suppose the participant p was assigned the vector $\mathbf{x}$. Write $\mathbf{x}$ as a (finite) linear combination of base elements: $\mathbf{x} = \sum_i \alpha_i \mathbf{h}_i$, and then the dealer gives p the share $\langle \mathbf{x}, \sum_i \alpha_i r_{\mathbf{h}_i} \rangle$. Thus p receives a share (an element of $\mathbb{F}$ labeled by the public vector $\mathbf{x}$) for each vector assigned to him.

It is clear that subsets of participants which have $\mathbf{v}$ in their linear span can compute the secret (as an appropriate linear combination of certain shares), and shares of an unqualified set is independent of the secret, as was required. □

5 Structures realized by (almost) ramp schemes

In this section we give a characterization of access structures which can be realized by measurable (almost) 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], which says 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 subsets of the Hilbert space to participants. The structure $\mathcal{A} \subset 2^P$ realized by the Hilbert-space program is defined as

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

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 an almost ramp measurable scheme;*
4. *$\mathcal{A}$ is G_δ.*

Proof. 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 an almost 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

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

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 almost 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 $v_n = \sum_{i=1}^n e_i/i$. 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 [9]. 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 an *almost 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.

However, it is easy to twist this scheme to be a ramp one. The only change is to set the secret to be the *fraction part* of ξ_v, see this trick in [7]. As the density function of the fractional part of a normal distribution is bounded (there is a $c \geq 1$ such that it is between $1/c$ and c) and the bound depends on the variation only, the conditional distribution of the secret, given the shares of an unqualified set, is 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 theorem 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 of this theorem 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, X_s, into countably many positive sets $X_s = \bigcup_i E_i$, where $\mu_s(E_i) > 0$. 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

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

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.*

Proof. 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. □

Quite 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 our scheme participants are indexed by the positive integers, and X_s 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}. Participant with index $i \le t$ 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 have the required properties.

6 Conclusion

In this paper we looked at the theoretical problems of probabilistic secret sharing schemes. It is quite natural to look at the classical secret sharing schemes from probabilistic point of view, and even the first few steps towards an "abstract" definition is quite 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, practically we cannot say anything.

Characterizations of structures realizable by perfect schemes in Section 4 was more or less straightforward. As can be seen in the companion paper [7], there are several exciting schemes which limit how much information unqualified subsets might have which do not fit into any common frame. Also, the following structure cannot be realized by any scheme which can be considered to be "ramp" in any weak sense:

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

Suppose there are only two secrets (this can be done without loss of generality, use the same trick as in the proof of Theorem 4.2). As the first row is qualified, there are finitely many elements in the first row who can determine the secret up to probability at least 0.9. Similarly, there are finitely many elements in the second row who know the secret up to probability 0.99; finitely many from the third row who know the secret with probability 0.999, etc. The union of these finite sets will know the secret with probability 1, thus it will be qualified, while it intersects each row in finitely many elements. (We showed that this structure is not G_δ at the end of Section 2.2.)

The nice, and quite natural, characterization of ramp and almost ramp schemes in Section 5 hints that our definition of ramp schemes is "the" correct one. As remarked earlier, no universally accepted definition exists for 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: the 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 a posterior probability that the secret takes that value might be much smaller than the a priori probability).

There are interesting probabilistic schemes in [7] which are weaker than the almost ramp schemes defined in Definition 2.8. In those schemes unqualified subsets can exclude large subsets of the secret space, while still remains some uncertainty. A typical example is when 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 a ramp scheme? How can these type of schemes be captured by a definition similar to that of ramp schemes?

Finally a question in other direction. Given an access structure $\mathcal{A}$, is there an easy way to recognize that it is G_δ? Given any collection of qualified and unqualified subsets, decide if there is a G_δ structure in between. As a concrete example: given a collection of subsets of P, I want any of them to be unqualified, but the union of any two of them to be qualified. Under what conditions is there such a ramp scheme realizing this structure?

Acknowledgments

I would like to thank the support and the uncountably many discussions while developing the ideas in this paper of,fdirst of all, members of the Cryptography group at the Renyi Institute. Their input were indispensable in forming and correcting my definitions and examples. Special thanks should 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 support of the "Lendület" program of the Hungarian Academy of Sciences is also acknowledged.

References

[1] Jacques Azma, Marc Yor, Paul Meyer, and Thierry de la Rue. Espaces de Lebesgue. In *Sminaire de Probabilits XXVII*, volume 1557 of *Lecture Notes in Mathematics*, pages 15–21. Springer Berlin / Heidelberg, 1993. 10.1007/BFb0087958.

[2] Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *IWCC*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer, 2011.

[3] G. R. Blakley and Laif Swanson. Infinite structures in information theory. In *CRYPTO*, pages 39–50, 1982.

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

[5] B. Chor and E. Kushilevitz. Secret sharing over infinite domain. *Journal of Cryptology*, 6(2):97–86, 1993.

[6] Alexander Dibert. Generalized secret sharing. Master's thesis, Central European University, Budapest, Hungary, 2011.

[7] Alexander Dibert and Laszlo Csirmaz. Infinite secret sharing – exmples. 2012. manuscript.

[8] J Haezendonck. Abstract Lebesgue–Rokhlin spaces. *Bulletin de la Societe Mathematique de Belgique*, 25:243–258, 1973.

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

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

[11] Mauricio Karchmer and Avi Wigderson. On span programs. In *Structure in Complexity Theory Conference*, pages 102–111, 1993.

[12] Boshra H. Makar. Transfinite cryptography. *Cryptologia*, 4(4):230–237, October 1980.

[13] Jacques Patarin. Transfinite cryptography. *IJUC*, 8(1):61–72, 2012. also avaiable as `http://eprint.iacr.org/2010/001`.

[14] Raphael Phan and Serge Vaudenay. On the impossibility of strong encryption over $\aleph_0$. In Yeow Chee, Chao Li, San Ling, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 5557 of *Lecture Notes in Computer Science*, pages 202–218. Springer Berlin / Heidelberg, 2009.

[15] Vladimir A. Rokhlin. On the fundamental ideas of measure theory. *Translations (American Mathematical Society)*, 10:154, 1962.

[16] Gabor Tardos. Personal communication.

[17] Stephen Watson. Power of the Sierpiński space. *Topology and its Applications*, 35(23):299 – 302, 1990.