A Generalized Special-Soundness Notion and its Knowledge Extractors

Thomas Attema[1,2,3], Serge Fehr[1,2], and Nicolas Resch[4]

[1] CWI, Cryptology Group, Amsterdam, The Netherlands
serge.fehr@cwi.nl
[2] Leiden University, Mathematical Institute, Leiden, The Netherlands
[3] TNO, Cyber Security and Robustness, The Hague, The Netherlands
thomas.attema@tno.nl
[4] University of Amsterdam, Informatics Institute, Amsterdam, The Netherlands
n.a.resch@uva.nl

Abstract. A classic result in the theory of interactive proofs shows that a *special-sound* Σ-protocol is automatically a *proof of knowledge*. This result is very useful to have, since the latter property is typically tricky to prove from scratch, while the former is often easy to argue — *if* it is satisfied. While classic Σ-protocols often are special-sound, this is unfortunately not the case for many recently proposed, highly efficient interactive proofs, at least not in this strict sense. Motivated by this, the original result was recently generalized to k-special sound Σ-protocols (for arbitrary, polynomially bounded k), and to multi-round versions thereof. This generalization is sufficient to analyze (e.g.) Bulletproofs-like protocols, but is still insufficient for many other examples.

In this work, we push the relaxation of the special soundness property to the extreme, by allowing an *arbitrary* access structure Γ to specify for which subsets of challenges it is possible to compute a witness, when given correct answers to these challenges (for a fixed first message). Concretely, for any access structure Γ, we identify parameters t_Γ and κ_Γ, and we show that any Γ-special sound Σ-protocol is a proof of knowledge with knowledge error κ_Γ if t_Γ is polynomially bounded. Similarly for multi-round protocols.

We apply our general result to a couple of simple but important example protocols, where we obtain a tight knowledge error as an immediate corollary. Beyond these simple examples, we analyze the FRI protocol. Here, showing the general special soundness notion is non-trivial, but can be done (for a certain range of parameters) by recycling some of the techniques used to argue ordinary soundness of the protocol (as an IOP). Again as a corollary, we then derive that the FRI protocol, as an interactive proof by using a Merkle-tree commitment, is a proof of knowledge with almost optimal knowledge error.

Finally, building up on the technique for the parallel repetition of k-special sound Σ-protocols, we show the same strong parallel repetition result for Γ-special sound Σ-protocol and its multi-round variant.

1 Introduction

Background. A key feature of an interactive proof is *soundness*, which requires that the verifier will not accept a false statement, i.e., an instance x that is not in the considered language, except with bounded probability. In many situations however, a stronger notion of soundness is needed: *knowledge soundness*. Informally, knowledge soundness requires the prover to *know* a witness w that certifies that x is a true statement, in order for the verifier to accept (except with bounded probability). More formally, this is captured by the existence of an efficient *extractor*, which has (rewindable) oracle access to any, possibly dishonest, prover, and which outputs a witness w for the considered statement x with a probability that is tightly related to the probability of the prover making the verifier accept.

Since their introduction, interactive proofs that satisfy knowledge soundness, typically referred to *proofs of knowledge* then, have found a myriad of applications. However, showing that an interactive proof satisfies knowledge soundness is typically non-trivial — often significantly more involved than showing ordinary soundness. By default, it involves *designing* the extractor, and *proving* that it "does the job." We got spoiled in the past, where most of the considered interactive proofs were Σ-protocols, i.e., public-coin 3-round interactive proofs, and had the additional property of being *special-sound*. Indeed, this made life rather easy since special-soundness is a property that is usually quite easy to prove, and that implies ordinary and knowledge soundness via a general classical result. Thus, knowledge soundness was often obtained (almost) for free. However, this has changed in recent years, where the focus has shifted towards finding *highly efficient* interactive proofs (where efficiency is typically measured via the communication complexity, verification time, etc.); many of these highly efficient solutions are *not* special-sound, and thus require a knowledge-soundness proof from scratch.

Given this situation, it would be desirable to have stronger versions of the generic "*special-soundness* $\Rightarrow$ *knowledge soundness*" result that applies to a *weaker* notion of special-soundness, which then hopefully is satisfied by these new cutting-edge interactive proofs. One step in this direction was recently made in [1, 2], where the above implication was extended to k-special-sound interactive proofs, and, even more generally, to $(k_1, \ldots, k_\mu)$-special-sound *multi-round* public-coin interactive proofs, for arbitrary positive integer parameters, subject to being suitably bounded from above (e.g., $k \leq \text{poly}(|x|)$). Rather naturally, k-special-soundness means that from accepting responses to k pairwise distinct challenges for one fixed message, a witness can be efficiently computed (so that 2-special-soundness coincides with the classical special-soundness property); for the multi-round version, a suitable tree of transcripts is needed for computing the a witness. This weaker notion of special-soundness is in particular suffi-

cient to analyze Bulletproofs-like protocols, and so we directly obtain knowledge soundness for these protocols.[5]

However, this weaker notion still falls short of capturing many of the recent highly-efficient interactive proofs. For instance, a commonly used amortization technique, where the prover proves a *random linear combination* of n statements (instead of proving all the statements individually), requires correct responses for n *linearly independent* challenge vectors in order to compute a witness. Another example comes from the design principle to first construct a highly efficient probabilistically checkable proof (PCP) or interactive *oracle* proof (IOP), and then to compile it into a standard (public-coin) interactive proof in the natural way by means of a Merkle-tree commitment [15, 16, 17]. Also here, one does not obtain a special-sound protocol in the above generalized sense (or then only for a too large parameter); instead, one requires challenges that correspond to sets whose union covers all (or sufficiently many of) the leaves of the Merkle tree, in order to obtain a witness.

Our Technical Results. In this paper, we push the weakening of the special-soundness property to the extreme. For Σ-protocols, in the spirit of ordinary or k-special-soundness, the notion of special-soundness that we consider in this work requires that a witness can be efficiently computed from accepting responses to *sufficiently many* pairwise distinct challenges, but now "sufficiently many" is captured by an arbitrary monotone (access) structure Γ, i.e., an arbitrary monotone set of subsets of the challenge set. This gives rise to the notion of Γ-special-soundness, which coincides with k-special-soundness in the special case where Γ is the threshold access structure with threshold k. This naturally extends to multi-round public-coin interactive proofs, leading to the notion of $(\Gamma_1, \ldots, \Gamma_\mu)$-special-soundness. Similar notions were considered in [14, 13] in the setting of *commit-and-open* Σ-protocols, and in some more constrained form, where the monotone structures are replaced by matroids, in [18, 19].

We cannot expect for every Γ that a Γ-special-sound protocol is a proof of knowledge. Instead, we identify parameters t_Γ and κ_Γ, determined by the structure Γ, and for any Γ-special-sound Σ-protocol we prove existence of an extractor that has an knowledge error κ_Γ and an expected run time that scales with t_Γ. Thus, as long as $t_\Gamma \leq \mathrm{poly}(|x|)$, Γ-special-soundness implies knowledge soundness. Similarly for $(\Gamma_1, \ldots, \Gamma_\mu)$-special-sound multi-round protocols.

The construction of our extractor for Γ-special-sound protocols (and its multi-round generalization) is inspired by the extractor construction from [2]. As

[5] Certain Bulletproofs-like protocols are not exactly $(k_1, \ldots, k_\mu)$-special-sound, but, e.g., require the k_i different challenges also to be different modulo the sign. But this can easily be dealt with, either by increasing k_i by a factor 2, or by halving the challenge space (so that if c is a valid challenge then $-c$ is not). In [12], they also observe this issue and generalize the extraction procedure to allow for general equivalence relations; however, by the above, this is not really necessary: instead, one can just restrict the challenge space to consist of one representative of each equivalence class.

a nice consequence, we can recycle the line of reasoning from [2] to prove strong parallel repetition and extend it to our general notion of special-soundness, showing that also here the knowledge error of a parallel repetition decreases exponentially with the number of repetitions.

Applications. Our general technique gives immediate, tight results for simple but important example protocols. For example, applied to the above mentioned amortization technique of proving a random linear combination, we directly obtain knowledge extraction with a knowledge error that matches the trivial cheating probability. Similarly, applied to the natural interactive proof for a Merkle commitment, where the prover is challenged to open a random subset (of a certain size), we obtain a knowledge error that matches the probability of one faulty node not being opened.

In order to demonstrate the usefulness of our result beyond the above simple examples, we analyze the (interactive) FRI protocol [5] and prove that for a certain range of the parameters, when instantiated with a Merkle tree commitment using a collision resistant hash function (or with any non-interactive, computationally binding vector commitment scheme with local openings), the protocol is a proof of knowledge with almost optimal knowledge error.[6] In more detail, for any proximity parameter δ up to $\delta < \frac{1-\rho}{4}$, where ρ is the relative rate of the considered code, we show a knowledge error of $(1-\delta)^t + O(N/|\mathbb{F}|)$, where N is the length of the code; this is close to the trivial cheating probability of $\max\{(1-\delta)^t, 1/|\mathbb{F}|\}$. In contrast to the above simple examples, arguing that the FRI protocol is $(\Gamma_1, \ldots, \Gamma_\mu)$-special-soundness is not trivial; however, technical results from [5] can be recycled in order to show this, and knowledge soundness then follows immediately from our generic result.

A final example, which we would like to briefly discuss, is parallel repetition. This example shows that our generic technique does not always work. For simplicity, consider a k-special-sound Σ-protocol with $k > 2$ (but the discussion also applies to multi-round protocols, and to our generalized notion of special soundness). Then, its t-fold parallel repetition is *not* k-special sound anymore (unless $k = 2$). One can argue that it is $\big((k-1)^t + 1\big)$-special sound — but this parameter is exponential in t, and thus one cannot directly conclude knowledge soundness. On the other hand, equipped with our generalized notion, one can observe that the parallel repetition is Γ-special sound for Γ being the structure that accepts a list of challenge vectors, each vector of length t, if there is one position where the challenge vectors feature at least k different values. Unfortunately, also here, the crucial parameter t_Γ turns out to be exponential for this structure Γ, and so our generic result does not imply knowledge soundness. Fortunately, for this particular and important example, the parallel repetition result from [2] applies in case of k-special sound protocols (and its multi-round

[6] We point out that, when considering the FRI protocol for an actual hash function (rather than the random oracle), ordinary soundness is meaningless: the *existence* of an opening of a Merkle commitment with a certain (not too obscure) property holds trivially. Thus, it is crucial to argue knowledge soundness in this case.

generalization), and our extension of the parallel repetition applies in case of arbitrary $(\Gamma_1, \ldots, \Gamma_\mu)$-special-sound protocols. Thus, after all, we can still argue (optimal) knowledge soundness in this case.

In conclusion, we expect that with our generic result for $(\Gamma_1, \ldots, \Gamma_\mu)$-special-sound protocols (which requires control over certain parameters to be applicable), and with our general parallel repetition result, our work offers powerful tools for proving knowledge soundness of many sophisticated proofs of knowledge.

2 Preliminaries

We write $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ for the set of nonnegative integers. Further, for any $q \in \mathbb{Z}$, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ denotes the ring of integers modulo q.

2.1 Interactive Proofs

Let us now introduce some standard terminology and definitions with respect to interactive proofs. We follow standard conventions as presented in [3].

Let $R \subseteq \{0,1\}^* \times \{0,1\}^*$ be a binary relation, containing statement-witness pairs $(x; w)$. We assume all relations to be NP-relations, i.e., verifying that $(x; w) \in R$ takes time polynomial in $|x|$. An interactive proof for a relation R aims to allow a prover $\mathcal{P}$ to convince a verifier $\mathcal{V}$ that a public statement x admits a (secret) witness w, i.e., $(x; w) \in R$, or even that the knows a witness w for x.

Definition 1 (Interactive Proof). *An* interactive proof $\Pi = (\mathcal{P}, \mathcal{V})$ *for relation R is an interactive protocol between two probabilistic machines, a prover $\mathcal{P}$ and a polynomial time verifier $\mathcal{V}$. Both $\mathcal{P}$ and $\mathcal{V}$ take as public input a statement x and, additionally, $\mathcal{P}$ takes as private input a witness w such that $(x; w) \in R$. The verifier $\mathcal{V}$ either accepts or rejects. Accordingly, we say the corresponding transcript (i.e., the set of all messages exchanged in the protocol execution) is* accepting *or* rejecting*.*

An interactive proof with three communication rounds, where we may assume the prover to send the first and final message, is called a Σ-protocol. Further, an interactive proof is said to be *public-coin* if the verifier publishes all its random coins. In this case, we may assume all the verifier's messages to be sampled uniformly at random from finite (challenge) sets.

An interactive proof is said to be *complete* if for any statement witness pair $(x; w)$ an honest execution results in an accepting transcript (with high probability). It is *sound* if a dishonest prover cannot convince an honest verifier on public inputs x that do not admit a witness w, i.e., on false statements x. More precisely, $(\mathcal{P}, \mathcal{V})$ is sound if $\mathcal{V}$ rejects false statements x with high probability. The stronger notion of *knowledge soundness* requires that (potentially dishonest) provers that succeed in convincing the verifier with large enough probability must actually "know" a witness w. We will mainly be interested in analyzing the knowledge soundness of interactive proofs. For this reason, we formally define this property below.

Definition 2 (Knowledge Soundness). *An interactive proof $(\mathcal{P}, \mathcal{V})$ for relation R is* knowledge sound *with knowledge error $\kappa\colon \mathbb{N} \to [0,1]$ if there exists a positive polynomial q and an algorithm $\mathcal{E}$, called a* knowledge extractor*, with the following properties. Given input x and black-box oracle access to a (potentially dishonest) prover $\mathcal{P}^*$, the extractor $\mathcal{E}$ runs in an expected number of steps that is polynomial in $|x|$ (counting queries to $\mathcal{P}^*$ as a single step) and outputs a witness $w \in R(x)$ with probability*

$$\Pr\big((x; \mathcal{E}^{\mathcal{P}^*}(x)) \in R\big) \geq \frac{\epsilon(\mathcal{P}^*, x) - \kappa(|x|)}{q(|x|)},$$

where $\epsilon(\mathcal{P}^*, x) := \Pr\big((\mathcal{P}^*, \mathcal{V})(x) = \mathsf{accept}\big)$ is the success probability of $\mathcal{P}^*$ on public input x.

Remark 1 (Interactive Arguments). In some cases, soundness and knowledge soundness only hold with respect to computationally bounded provers, i.e., unbounded provers can falsely convince a verifier. Computationally (knowledge) sound protocols are referred to as interactive *arguments*. Proving soundness of interactive arguments can be significantly more complicated than proving soundness of interactive proofs. However, in the context of knowledge soundness, an interactive argument for relation R can oftentimes be cast as an interactive proof for a modified relation

$$R' = \{(x; w) : (x; w) \in R \text{ or } w \text{ solves some computational problem}\}.$$

Hence, in this case the knowledge extractor will either output a witness w with respect to the original relation w, or it will output the solution to some computational problem, e.g., a discrete logarithm relation. In fact, our analysis of the FRI protocol in Section 8 exemplifies this general principle. For this reason, knowledge soundness of interactive arguments can typically be analyzed via knowledge extractors that are originally defined for interactive proofs. Therefore, we will focus on the analyzes of interactive proofs.

Proving knowledge soundness of Σ-protocols directly is a nontrivial task, as it requires the construction of an efficient knowledge extractor. It is typically much easier to prove a related *threshold* special-soundness property, which states that a witness can be extracted from a sufficiently large set of colliding and accepting transcripts.

Definition 3 (k-out-of-N Special-Soundness). *Let $k, N \in \mathbb{N}$. A 3-round public-coin interactive proof $\Pi = (\mathcal{P}, \mathcal{V})$ for relation R, with challenge set of cardinality $N \geq k$, is k-out-of-N special-sound if there exists an algorithm that, on input a statement x and k accepting transcripts $(a, c_1, z_1), \ldots (a, c_k, z_k)$ with common first message a and pairwise distinct challenges $c_1, \ldots, c_k$, runs in time polynomial in $|x|$ and outputs a witness w such that $(x; w) \in R$. We also say Π is k-special-sound and, if $k = 2$, it is simply said to be special-sound.*

It is known that k-out-of-N special-soundness implies knowledge soundness with knowledge error $(k-1)/N$. Recently, the multi-round generalization $(k_1, \ldots, k_\mu)$-out-of-$(N_1, \ldots, N_\mu)$ special-soundness has become relevant. It is now known that also this generalization tightly implies knowledge soundness [1]. For a formal definition, we refer either to [1] or to Section 6 where we generalize this (multi-round) notion beyond the threshold setting.

Remark 2. Formally, the parameters k and N of a k-out-of-N special-sound interactive proof may depend on the size of the public input $|x|$. For notational convenience, we leave this dependency implicit.

2.2 Geometric Distribution

This work adapts the extractor of [2]. For this reason, we also need the following preliminaries on the geometric distribution from their work.

A random variable B with two possible outcomes, denoted 0 (failure) and 1 (success), is said to follow a Bernoulli distribution with parameter p if $p = \Pr(B = 1)$. Sampling from a Bernoulli distribution is also referred to as running a Bernoulli trial. The probability distribution of the number X of independent and identical Bernoulli trials needed to obtain a success is called the geometric distribution with parameter $p = \Pr(X = 1)$. In this case $\Pr(X = k) = (1-p)^{k-1}p$ for all $k \in \mathbb{N}$ and we write $X \sim \mathrm{Geo}(p)$. For two independent geometric distributions we have the following lemma.

Lemma 1. *Let $X \sim \mathrm{Geo}(p)$ and $Y \sim \mathrm{Geo}(q)$ be independently distributed. Then,*

$$\Pr(X \leq Y) = \frac{p}{p+q-pq} \geq \frac{p}{p+q}\,.$$

Proof. It holds that

$$\begin{aligned}\Pr(X \leq Y) &= \sum_{k=1}^{\infty} \Pr(X = k)\Pr(Y \geq k) = \sum_{k=1}^{\infty} (1-p)^{k-1}p \cdot (1-q)^{k-1} \\ &= \frac{p}{1-(1-p)(1-q)} = \frac{p}{p+q-pq} \geq \frac{p}{p+q}\,.\end{aligned}$$

□

3 A Generalized Notion of Special-Soundness for Σ-Protocols

In this section, we define a generalized notion of special-soundness. To this end, we first recall the definition of *monotone structures*.

Definition 4 (Monotone Structure). *Let $\mathcal{C}$ be a nonempty finite set and let $\Gamma \subseteq 2^{\mathcal{C}}$ be a family of subsets of $\mathcal{C}$. Then, Γ or $(\Gamma, \mathcal{C})$ is said to be a* monotone structure *if it is closed under taking supersets, i.e., $S \in \Gamma$ and $S \subseteq T \subseteq \mathcal{C}$ implies $T \in \Gamma$.*

In some textbooks monotone structures Γ do not contain the empty set $\emptyset$ by definition, which is equivalent to $\Gamma \neq 2^{\mathcal{C}}$, and they are required to be nonempty, which is equivalent to $\mathcal{C} \in \Gamma$. For convenience, we also consider $\Gamma = \emptyset$ and $\Gamma = 2^{\mathcal{C}}$ to be monotone structures. Then, for any $\mathcal{D} \subseteq \mathcal{C}$, the restriction

$$\Gamma|_{\mathcal{D}} = \{S \subseteq \mathcal{D} : S \in \Gamma\} \subseteq 2^{\mathcal{D}}$$

defines a monotone structure $(\Gamma|_{\mathcal{D}}, \mathcal{D})$.

Definition 5 (Minimal Set). *Let $(\Gamma, \mathcal{C})$ be a monotone structure. A set $S \in \Gamma$ is* minimal *if none of its proper subsets are in Γ, i.e., for all $T \subsetneq S$ it holds that $T \notin \Gamma$. Further, $M(\Gamma) \subseteq \Gamma$ denotes the set of minimal elements of Γ.*

Definition 6 (Distance to a Monotone Structure). *For a nonempty monotone structure $(\Gamma, \mathcal{C})$, we define the following distance function:*

$$d_\Gamma \colon 2^{\mathcal{C}} \to \mathbb{N}_0\,, \quad S \mapsto \min_{T \in \Gamma} |T \setminus S|\ .$$

Equivalently,

$$d_\Gamma \colon 2^{\mathcal{C}} \to \mathbb{N}_0\,, \quad S \mapsto \min_{T \subseteq \mathcal{C}} \{|T| : S \cup T \in \Gamma\}\,.$$

If $\Gamma = \emptyset$, we define d_Γ to be identically equal to ∞.

The value $d_\Gamma(S) \in \mathbb{N}_0$ equals the minimum number of elements that have to be added to the set S to obtain an element of Γ. In particular, $d_\Gamma(S) = 0$ if and only if $S \in \Gamma$. Hence, it shows how close S is to the monotone structure Γ.

The key observation is now that typical knowledge extractors for interactive proofs proceed by extracting some set of accepting transcripts from a dishonest prover attacking the interactive proof. Subsequently, the knowledge extractor computes a witness from this set of accepting transcripts. Clearly, the set of sets of accepting transcripts from which a witness can be computed is closed under taking supersets, i.e., it is a monotone structure. Therefore, the following special-soundness notion for 3-round Σ-protocols follows naturally.

Definition 7 (Γ-out-of-$\mathcal{C}$ Special-Soundness). *Let $(\Gamma, \mathcal{C})$ be a monotone structure. A 3-round public-coin interactive proof $(\mathcal{P}, \mathcal{V})$ for relation R, with challenge set $\mathcal{C}$, is* Γ-out-of-$\mathcal{C}$ special-sound *if there exists an algorithm that, on input a statement x and a set of accepting transcripts $(a, c_1, z_1), \ldots, (a, c_k, z_k)$ with common first message a and such that $\{c_1, \ldots, c_k\} \in \Gamma$, runs in time polynomial in $|x|$ and outputs a witness $w \in R(x)$. We also say $(\mathcal{P}, \mathcal{V})$ is Γ-special-sound.*

The above definition is a generalization of k-out-of-N special-soundness, where the extractability is guaranteed when given k colliding accepting transcripts with common first message a and pairwise distinct challenges c_i that are elements of a challenge set with cardinality N. Hence, when Γ contains all sets of cardinality at least k, i.e., it is a *threshold* monotone structure, Γ-out-of-$\mathcal{C}$ special-soundness reduces to k-out-of-N special-soundness, where $N = |\mathcal{C}|$.

Remark 3. Formally, the monotone structure $(\Gamma, \mathcal{C})$ of Definition 7 may depend on the size $|x|$ of the public input x, i.e., it should actually be replaced by an ensemble $(\Gamma_\lambda, \mathcal{C}_\lambda)$ of monotone structures indexed by the size $\lambda \in \mathbb{N}$ of the public input of $(\mathcal{P}, \mathcal{V})$. For simplicity, we will abuse notation by ignoring this dependency and simply writing $(\Gamma, \mathcal{C})$. See also Remark 2.

4 Knowledge Extraction for Γ-out-of-$\mathcal{C}$ Special-Sound Σ-Protocols

Our goal is to prove that, for certain monotone structures $(\Gamma, \mathcal{C})$, Γ-out-of-$\mathcal{C}$ special-soundness (tightly) implies knowledge soundness, and to determine the corresponding knowledge error. In order to prove this, we construct a knowledge extractor that, by querying a prover $\mathcal{P}^*$ attacking the interactive proof, obtains a set of accepting transcripts with common first message and for which the challenges form a set in Γ. Without loss of generality we may assume $\mathcal{P}^*$ to be deterministic,[7] i.e., $\mathcal{P}^*$ always outputs the same first message a. Hence, $\mathcal{P}^*$ can be viewed as a (deterministic) function

$$\mathcal{P}^* \colon \mathcal{C} \to \{0,1\}^* \quad c \mapsto y = (a, c, z)\,,$$

that on input a challenge $c \in \mathcal{C}$ outputs a protocol transcript $y = (a, c, z)$.

Let $A \subseteq \mathcal{C}$ be the set of challenges for which $\mathcal{P}^*$ succeeds, i.e., $A = \{c \in \mathcal{C} : V(\mathcal{P}^*(c)) = 1\}$. Then the goal of the extractor is to find a set $B \in \Gamma|_A$. The difficulty is that the extractor is only given oracle access to $\mathcal{P}^*$ and therefore does not know the set A. For this reason, extractors typically proceed recursively as follows: if at some point the extractor has found some $S \subseteq A$ with $S \notin \Gamma$, it will try new challenges $c \in \mathcal{C}$ until $\mathcal{P}^*$ succeeds. The hope is then that $S \cup \{c\} \subseteq A$ is "closer" to $\Gamma|_A$ than S. More precisely, the extractor tries to find a $c \in A \subseteq \mathcal{C}$ such that $d_{\Gamma|_A}(S \cup \{c\}) < d_{\Gamma|_A}(S)$. Note that not all challenges c shorten the distance to $\Gamma|_A$, e.g., $d_{\Gamma|_A}(S \cup \{c\}) = d_{\Gamma|_A}(S)$ for all $c \in S$. Since the extractor does not know the set A, it cannot evaluate this distance function.

However, for any S, the challenge set $\mathcal{C}$ can be partitioned into a partition of "useless" challenges and a partition of "potentially useful" challenges. The useless challenges are the $c \in \mathcal{C}$ such that $d_{\Gamma|_A}(S \cup \{c\}) = d_{\Gamma|_A}(S)$ for all $A \subseteq \mathcal{C}$ containing S, i.e., for all A useless challenges will not shorten the distance to $\Gamma|_A$. For instance, all $c \in S$ are useless challenges for any S and any Γ. However, in some settings the set of useless challenges is larger than S, and in general this observation is crucial for the extractor to be efficient. In fact, this is the case for all interactive proofs that warrant a generalization of the existing threshold special-soundness notion. All challenges $c \in \mathcal{C}$ that are not useless are potentially useful, i.e., for these challenges there exist an $A \subseteq \mathcal{C}$ containing S such that $d_{\Gamma|_A}(S \cup \{c\}) < d_{\Gamma|_A}(S)$. The set of useful challenges is denoted $U_\Gamma(S)$, where the function U_Γ is formally defined below.

[7] See [2] for a proof of this claim.

Definition 8 (Useful Elements). *For a monotone structure $(\Gamma, \mathcal{C})$, we define the following function:*

$$U_\Gamma \colon 2^{\mathcal{C}} \to 2^{\mathcal{C}}, \quad S \mapsto \left\{ c \in \mathcal{C} \setminus S : \exists A \in \Gamma \text{ s.t. } S \subset A \wedge A \setminus \{c\} \notin \Gamma \right\}.$$

Note that $\Gamma = \emptyset$ implies $U_\Gamma(S) = \emptyset$ for all $S \subseteq \mathcal{C}$. Moreover, if Γ is nonempty, $U_\Gamma(S) = \emptyset$ if and only if $S \in \Gamma$.

The following lemma shows that for any $c \in U_\Gamma(S)$, there exists an $A \in \Gamma$ containing $S \cup \{c\}$ such that

$$d_{\Gamma|_A}(S \cup \{c\}) < d_{\Gamma|_A}(S)\,,$$

i.e., the challenges $c \in U_\Gamma(S)$ are indeed potentially useful to the extractor. Even more so, it is essential that the extractor considers *all* challenges $c \in U_\Gamma(S)$. For every $c \in U_\Gamma(S)$, it might namely be the case that the $A \in \Gamma$ that "certifies" c, i.e., the A such that $S \subset A$ and $A \setminus \{c\} \notin \Gamma$, corresponds to the challenges for which the prover $\mathcal{P}^*$ succeeds. Since $A \setminus \{c\} \notin \Gamma$, the extractor can only succeed if it considers the challenge $c \in U_\Gamma(S)$ at some point.

The same lemma shows that challenges $c \notin U_\Gamma(S)$ will never decrease the distance, i.e., they are indeed useless to the extractor. More precisely, if $c \notin U_\Gamma(S)$, for every $A \in \Gamma$ containing $S \cup \{c\}$ it holds that

$$d_{\Gamma|_A}(S \cup \{c\}) = d_{\Gamma|_A}(S)\,.$$

Lemma 2. *Let $(\Gamma, \mathcal{C})$ be a monotone structure and $S \subset \mathcal{C}$. Then $c \in U_\Gamma(S)$ if and only if there exists an $A \in \Gamma$ containing $S \cup \{c\}$ such that*

$$d_{\Gamma|_A}(S \cup \{c\}) < d_{\Gamma|_A}(S)\,.$$

Proof. Let us first prove that $c \in U_\Gamma(S)$ implies the existence of an appropriate set $A \in \Gamma$. If $c \in U_\Gamma(S)$, then $c \notin S$ and there exists an A such that $S \subset A$ and $A \setminus \{c\} \notin \Gamma$. Now, let $T \in \Gamma|_A$ (i.e, $T \subseteq A$ and $T \in \Gamma$) be such that

$$d_{\Gamma|_A}(S) = |T \setminus S|\,.$$

Then, $T \setminus \{c\} \subseteq A \setminus \{c\} \notin \Gamma$, which implies that $c \in T \setminus S$. Hence,

$$d_{\Gamma|_A}(S \cup \{c\}) \leq |T \setminus (S \cup \{c\})| = |T \setminus S| - 1 = d_{\Gamma|_A}(S) - 1\,,$$

which proves the first implication of the lemma.

Let us now prove the other implication. To this end, let $A \in \Gamma$ containing $S \cup \{c\}$ be such that

$$d_{\Gamma|_A}(S \cup \{c\}) + 1 \leq d_{\Gamma|_A}(S)\,.$$

Further, let $T \in \Gamma|_A \subseteq 2^A$ be such that $d_{\Gamma|_A}(S \cup \{c\}) = |T \setminus (S \cup \{c\})|$. Without loss of generality we may assume that $S \subset T$. Then

$$d_{\Gamma|_A}(S) \leq |T \setminus S| \leq |T \setminus (S \cup \{c\})| + 1 = d_{\Gamma|_A}(S \cup \{c\}) + 1\,.$$

Hence,

$$d_{\Gamma|_A}(S) = |T \setminus S| = |T \setminus (S \cup \{c\})| + 1 = d_{\Gamma|_A}(S \cup \{c\}) + 1\,,$$

which implies that $c \in T \setminus S$ and $T \setminus \{c\} \notin \Gamma|_A$. It follows that $c \in U_\Gamma(S)$, which completes the proof of the lemma.

□

We also derive the following lemma, which shows that even if all useless challenges $c \in \mathcal{C} \setminus U_\Gamma(S)$ are added to the set $S \in 2^{\mathcal{C}} \setminus \Gamma$, the resulting subset is still not in Γ.

Lemma 3. *Let $(\Gamma, \mathcal{C})$ be a monotone structure and $S \in 2^{\mathcal{C}} \setminus \Gamma$. Then, $(\mathcal{C} \setminus U_\Gamma(S)) \cup S \notin \Gamma$.*

Proof. Suppose, to the contrary, that $(\mathcal{C} \setminus U_\Gamma(S)) \cup S \in \Gamma$. Further, let $A \subseteq \mathcal{C} \setminus (U_\Gamma(S) \cup S)$ be such that $A \cup S \in \Gamma$ and $A' \cup S \notin \Gamma$ for all $A' \subsetneq A$. Note that $A \neq \emptyset$, because $S \notin \Gamma$.

Now let $c \in A \subseteq \mathcal{C} \setminus (U_\Gamma(S) \cup S) \subseteq \mathcal{C} \setminus U_\Gamma(S)$, then $A \cup S \in \Gamma$ and $(A \cup S) \setminus \{c\} \notin \Gamma$. Hence, $c \in U_\Gamma(S)$, which contradicts the fact that $c \notin \mathcal{C} \setminus U_\Gamma(S)$. It follows that $(\mathcal{C} \setminus U_\Gamma(S)) \cup S \notin \Gamma$, which completes the proof. □

The knowledge extractor will be restricted to sampling challenges that are potentially useful. The value t_Γ defines the maximum number of accepting transcripts that the extractor has to find, before it succeeds and obtains the accepting transcripts for a set $S \in \Gamma$. The efficiency of our knowledge extractor will depend on t_Γ. A formal definition is given below. Further, in Section 5, we describe the monotone structure and corresponding k-values for three (classes of) interactive proofs and explain their relevance.

Definition 9 (t-value). *Let $(\Gamma, \mathcal{C})$ be a monotone structure and $S \subseteq \mathcal{C}$. Then*

$$t_\Gamma(S) := \max\left\{ t \in \mathbb{N}_0 : \begin{array}{c} \exists c_1, \ldots, c_t \in \mathcal{C} \text{ s.t.} \\ c_i \in U_\Gamma\big(S \cup \{c_1, \ldots, c_{i-1}\}\big)\ \forall i \end{array} \right\}.$$

Further,

$$t_\Gamma := t_\Gamma(\emptyset)\,.$$

It is easily seen that $t_\Gamma(S) = 0$ if and only if $S \in \Gamma$ or $\Gamma = \emptyset$. Further, the following lemma shows that adding an element $c \in U_\Gamma(S)$ to S decreases the corresponding k-value. This lemma plays a pivotal role in our recursive extraction algorithm.

Lemma 4. *Let $(\Gamma, \mathcal{C})$ be a nonempty monotone structure and let $S \subseteq \mathcal{C}$ such that $S \notin \Gamma$. Then, for all $c \in U_\Gamma(S)$,*

$$t_\Gamma(S \cup \{c\}) < t_\Gamma(S)\,.$$

Proof. Let $c \in U_\Gamma(S)$ and $t := t_\Gamma(S \cup \{c\})$. Then, by definition, there exist $c_0 := c, c_1, \ldots, c_t \in \mathcal{C}$ such that $c_i \in U_\Gamma\big(S \cup \{c_0, \ldots, c_{i-1}\}\big)$ for all i. Hence,

$$t_\Gamma(S) \geq k + 1 = t_\Gamma(S \cup \{c\}) + 1 > t_\Gamma(S \cup \{c\}) \,,$$

which completes the proof. □

As in [2], we describe our technical results in a more abstract language. This will later allow us to easily derive composition results and handle more complicated scenarios, such as multi-round interactive proofs and parallel compositions. To this end, let us consider a finite set $\mathcal{C}$, a probabilistic algorithm $\mathcal{A}\colon \mathcal{C} \to \{0,1\}^*$ and a verification function $V\colon \mathcal{C} \times \{0,1\}^* \to \{0,1\}$. An output $y \leftarrow \mathcal{A}(c)$ of the algorithm $\mathcal{A}$ on input $c \in \mathcal{C}$ is said to be *accepting* or *correct* if $V(c,y) = 1$. The success probability of $\mathcal{A}$ is denoted as

$$\epsilon(\mathcal{A}) := \Pr\big(V\big(C, \mathcal{A}(C)\big) = 1\big) \,,$$

where C is uniformly random in $\mathcal{C}$. The obvious instantiation of $\mathcal{A}$ is given by a deterministic dishonest prover $\mathcal{P}^*$ attacking an interactive proof Π on input x. Note that even though it is sufficient to consider deterministic provers $\mathcal{P}^*$, we allow the algorithm $\mathcal{A}$ to be probabilistic. This generalization is essential when considering multiround interactive proofs and parallel repetitions [2].

Now let $\Gamma \subseteq 2^{\mathcal{C}}$ be a nonempty monotone structure. Then, for any $S \subset \mathcal{C}$ with $U_\Gamma(S) \neq \emptyset$, we define

$$\epsilon_\Gamma(\mathcal{A}, S) := \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \in U_\Gamma(S)\big) \,.$$

Typically, $U_\Gamma(\emptyset) = \mathcal{C}$ and thus $\epsilon(\mathcal{A}) = \epsilon_\Gamma(\mathcal{A}, \emptyset)$, i.e., all challenges $c \in \mathcal{C}$ are potentially useful. However, this is not necessarily the case.

Given oracle access to $\mathcal{A}$, the goal of the extractor is to find *correct* outputs $y_1, \ldots, y_k$ for challenges $c_1, \ldots, c_k \in \mathcal{C}$ such that $\{c_1, \ldots, c_k\} \in \Gamma$, i.e., such that $V(c_i, y_i) = 1$ for all i. If $\mathcal{A}$ corresponds to a dishonest prover attacking a Γ-out-of-$\mathcal{C}$ special-sound interactive proof on some input x, a witness w for statement x can be efficiently computed from the outputs $y_1, \ldots, y_k$.

Let us further define the following quality measure for the algorithm $\mathcal{A}$:

$$\delta_\Gamma(\mathcal{A}) := \min_{S \notin \Gamma} \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \notin S\big) \,.$$

The value $\delta_\Gamma(\mathcal{A})$ defines a "punctured" success probability of $\mathcal{A}$, i.e., it equals the success probability of $\mathcal{A}$ when the challenge c is sampled uniformly at random from some set $\mathcal{C} \setminus S \supseteq U_\Gamma(S)$ such that S is not in the monotone structure. We will show that the value $\delta_\Gamma(\mathcal{A})$ measures how well we can extract from the algorithm $\mathcal{A}$. The value $\delta_\Gamma(\mathcal{A})$ is a natural generalization of the measure

$$\delta_k(\mathcal{A}) := \min_{S \subseteq \mathcal{C} : |S| < k} \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \notin S\big) \,,$$

defined in [2]. More precisely, if Γ is equal to the collection of subsets of cardinality at least k, then $\delta_\Gamma(\mathcal{A}) = \delta_k(\mathcal{A})$.

For any set $T \in 2^{\mathcal{C}} \setminus \Gamma$, we also define

$$\delta_\Gamma(\mathcal{A}, T) := \min_{S : S \cup T \notin \Gamma} \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \notin S\big)\,.$$

Since $S \cup T \notin \Gamma$ implies $S \cup T' \notin \Gamma$ for all $T' \subseteq T$, it follows that

$$\delta_\Gamma(\mathcal{A}, T') \leq \delta_\Gamma(\mathcal{A}, T), \quad \forall\, T' \subseteq T\,. \tag{1}$$

Further, by Lemma 3, it follows that $\big(\mathcal{C} \setminus U_\Gamma(T)\big) \cup T \notin \Gamma$ for all $T \notin \Gamma$. Hence,

$$\begin{aligned} \delta_\Gamma(\mathcal{A}, T) &= \min_{S : S \cup T \notin \Gamma} \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \notin S\big) \\ &\leq \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \notin \mathcal{C} \setminus U_\Gamma(T)\big) \\ &= \Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \in U_\Gamma(T)\big) \\ &= \epsilon_\Gamma(\mathcal{A}, T)\,. \end{aligned} \tag{2}$$

We are now ready to define and analyze our extraction algorithm for Γ-out-of-$\mathcal{C}$ special-sound interactive Σ-protocols. The extractor is defined in Figure 1 and its properties are summarized in the following lemma.

Lemma 5 (Extraction Algorithm - Σ-protocols). *Let $(\Gamma, \mathcal{C})$ be a nonempty monotone structure and let $V\colon \mathcal{C} \times \{0,1\}^* \to \{0,1\}$. Then there exists an oracle algorithm $\mathcal{E}_\Gamma$ with the following properties: The algorithm $\mathcal{E}_\Gamma^{\mathcal{A}}$, given oracle access to a (probabilistic) algorithm $\mathcal{A}\colon \mathcal{C} \to \{0,1\}^*$, requires an expected number of at most $2t_\Gamma - 1$ queries to $\mathcal{A}$ and, with probability at least $\delta_\Gamma(\mathcal{A})/t_\Gamma$, it outputs pairs $(c_1, y_1), (c_2, y_2), \ldots, (c_\ell, y_\ell) \in \mathcal{C} \times \{0,1\}^*$ with $V(c_i, y_i) = 1$ for all i and $\{c_1, \ldots, c_k\} \in \Gamma$.*

Fig. 1. Recursive Expected Polynomial Time Extractor $\mathcal{E}_\Gamma^{\mathcal{A}}(S)$.

Parameters: a nonempty monotone structure $(\Gamma, \mathcal{C})$ and an $S \in 2^{\mathcal{C}} \setminus \Gamma$.
Oracle access to: Algorithm $\mathcal{A}\colon \mathcal{C} \to \{0,1\}^*$ and verification function $V\colon \mathcal{C} \times \{0,1\}^* \to \{0,1\}$.

- Sample $c_1 \in U_\Gamma(S)$ uniformly at random and evaluate $y_1 \leftarrow \mathcal{A}(c_1)$.
- If $V(c_1, y_1) = 0$, abort and output $\perp$.
- If $V(c_1, y_1) = 1$ and $\{c_1\} \cup S \in \Gamma$, output $(c_1, y_1) \in \mathcal{C} \times \{0,1\}^*$.
- Else, set $\textsc{coin} = 0$ and repeat
  - run $\mathcal{E}_\Gamma^{\mathcal{A}}(S \cup \{c_1\})$;
  - set $\textsc{coin} \leftarrow V\big(d, \mathcal{A}(d)\big)$ for $d \in U_\Gamma(S)$ sampled uniformly at random;

  until either $\mathcal{E}_\Gamma^{\mathcal{A}}(S \cup \{c_1\})$ outputs pairs $(c_2, y_2), \ldots, (c_k, y_k)$ (for some k) with $V(c_i, y_i) = 1$ for all i and $S \cup \{c_1, c_2, \ldots, c_k\} \in \Gamma$ or until $\textsc{coin} = 1$.

Output: In the former case, output pairs $(c_1, y_1), \ldots, (c_k, y_k) \in \mathcal{C} \times \{0,1\}^*$ with $V(c_i, y_i) = 1$ for all i and $\{c_1, \ldots, c_k\} \cup S \in \Gamma$. In the latter case, output $\perp$.

Proof. The extractor $\mathcal{E}_{\Gamma}^{\mathcal{A}}(S)$ is formally defined in Figure 1. It takes as input a subset $S \in 2^{\mathcal{C}} \setminus \Gamma$. The input S represents the set of accepting challenges that the extractor has already found, i.e., the goal of $\mathcal{E}_{\Gamma}^{\mathcal{A}}(S)$ is to find pairs (c_i, y_i) such that $V(c_i, y_i) = 1$ and $\{c_1, \ldots, c_k\} \cup S \in \Gamma$. Further, we define

$$\mathcal{E}_{\Gamma}^{\mathcal{A}} := \mathcal{E}_{\Gamma}^{\mathcal{A}}(\emptyset)\,.$$

Fist note that, since $\Gamma \neq \emptyset$ and thus $U_{\Gamma}(S) \neq \emptyset$ for all $S \notin \Gamma$, the extractor is well-defined. Let us now analyze the success probability and the expected number of $\mathcal{A}$-queries of the extractor.

Success Probability. By induction over $t_{\Gamma}(S)$, we will prove that $\mathcal{E}_{\Gamma}^{\mathcal{A}}(S)$ succeeds with probability at least

$$\frac{\delta_{\Gamma}(\mathcal{A}, S)}{t_{\Gamma}(S)}\,.$$

We first consider the base case. To this end, let $S \subseteq \mathcal{C}$ with $t_{\Gamma}(S) = 1$. Then, by Lemma 4, for all $c_1 \in U_{\Gamma}(S)$ $t_{\Gamma}(S \cup \{c_1\}) = 0$ and thus $S \cup \{c_1\} \in \Gamma$. Therefore, the extractor succeeds if and only if $V\big(c_1, \mathcal{A}(c_1)\big) = 1$ for the c_1 sampled from $U_{\Gamma}(S)$. Hence, the success probability of the extractor equals

$$\epsilon_{\Gamma}(\mathcal{A}, S) \geq \delta_{\Gamma}(\mathcal{A}, S)\,,$$

where the inequality follows from Equation 2. This proves the bound on the success probability for the base case $t_{\Gamma}(S) = 1$.

Let us now consider an arbitrary subset $S \subseteq \mathcal{C}$ with $t_{\Gamma}(S) > 1$ and assume that the claimed bound holds for all subsets $T \subseteq \mathcal{C}$ with $t_{\Gamma}(T) < t_{\Gamma}(S)$.

In the first step, the extractor succeeds with probability $\epsilon_{\Gamma}(\mathcal{A}, S)$ in finding a $c_1 \in U_{\Gamma}(S)$ and $y_1 \leftarrow \mathcal{A}(c_1)$ with $V(c_1, y_1) = 1$. If $\{c_1\} \cup S \in \Gamma$, the extractor has successfully completed its task. If not, the extractor starts running two geometric experiments until one of them finishes. In the first geometric experiment the extractor repeatedly runs $\mathcal{E}_{\Gamma}^{\mathcal{A}}(S \cup \{c_1\})$. By Lemma 4, it holds that $t_{\Gamma}(S \cup \{c_1\}) < t_{\Gamma}(S)$. Hence, by the induction hypothesis, $\mathcal{E}_{\Gamma}^{\mathcal{A}}(S \cup \{c_1\})$ succeeds with probability

$$p \geq \frac{\delta_{\Gamma}(\mathcal{A}, S \cup \{c_1\})}{t_{\Gamma}(S \cup \{c_1\})} \geq \frac{\delta_{\Gamma}(\mathcal{A}, S)}{t_{\Gamma}(S) - 1}\,,$$

where the second inequality follows from Equation 1 and Lemma 4. In the second geometric experiment, the extractor tosses a coin that returns heads with probability

$$q := \epsilon_{\Gamma}(\mathcal{A}, S)\,.$$

The second step of the extractor succeeds if the second geometric experiment does not finish before the first, and so by Lemma 1 this probability is lower

bounded as follows

$$\Pr\big(\mathrm{Geo}(p) \leq \mathrm{Geo}(q)\big) \geq \frac{p}{p+q} \geq \frac{\frac{\delta_\Gamma(\mathcal{A},S)}{t_\Gamma(S)-1}}{\frac{\delta_\Gamma(\mathcal{A},S)}{t_\Gamma(S)-1} + \epsilon_\Gamma(\mathcal{A},S)}$$
$$\geq \frac{\frac{\delta_\Gamma(\mathcal{A},S)}{t_\Gamma(S)-1}}{\frac{\epsilon_\Gamma(\mathcal{A},S)}{t_\Gamma(S)-1} + \epsilon_\Gamma(\mathcal{A},S)} = \frac{\delta_\Gamma(\mathcal{A},S)}{t_\Gamma(S)\cdot\epsilon_\Gamma(\mathcal{A},S)}\,,$$

where the second inequality follows from the monotonicity of the function $x \mapsto \frac{x}{x+q}$ and the third inequality follows from the fact that $\delta_\Gamma(\mathcal{A},S) \leq \epsilon_\Gamma(\mathcal{A},S)$ (Equation 2).

Since the first step of the extractor succeeds with probability $\epsilon_\Gamma(\mathcal{A},S)$, it follows that $\mathcal{E}_\Gamma^{\mathcal{A}}(S)$ succeeds with probability at least $\delta_\Gamma(\mathcal{A},S)/t_\Gamma(S)$ for all $S \in 2^{\mathcal{C}} \setminus \Gamma$, which proves the claimed bound. In particular, $\mathcal{E}_\Gamma^{\mathcal{A}}$ succeeds with probability at least $\delta_\Gamma(\mathcal{A})/t_\Gamma$.

Expected Number of $\mathcal{A}$-Queries. By induction over $t_\Gamma(S)$, we will prove that the expected number of $\mathcal{A}$-queries $Q_\Gamma(S)$ made by $\mathcal{E}_\Gamma^{\mathcal{A}}(S)$ is upper bounded as follows:

$$Q_\Gamma(S) \leq 2t_\Gamma(S) - 1\,.$$

We first consider the base case. To this end, let $S \subseteq \mathcal{C}$ with $t_\Gamma(S) = 1$. In this case, $\{c_1\} \cup S \in \Gamma$ for all $c_1 \in U_\Gamma(S)$. Hence, $\mathcal{E}_\Gamma^{\mathcal{A}}(S)$ either succeeds or fails after making exactly one $\mathcal{A}$-query, i.e., $Q_\Gamma(S) = 1 = 2t_\Gamma(S) - 1$, which proves the base case.

Let us now consider an arbitrary subset $S \subseteq \mathcal{C}$ with $t_\Gamma(S) > 1$ and assume that $Q_\Gamma(T) \leq 2t_\Gamma(T) - 1$ for all subsets $T \subseteq \mathcal{C}$ with $t_\Gamma(T) < t_\Gamma(S)$.

The extractor $\mathcal{E}_\Gamma^{\mathcal{A}}(S)$ first samples $c_1 \leftarrow_R U_\Gamma(S)$ uniformly at random and evaluates $y_1 \leftarrow \mathcal{A}(c_1)$. This requires exactly one $\mathcal{A}$-query. After this step the extractor aborts with probability $1 - \epsilon_\Gamma(\mathcal{A},S)$. Otherwise, and if $\{c_1\} \cup S \notin \Gamma$, it continues running the two geometric experiments until either one of them finishes. The second geometric experiment finishes in an expected number of $1/\epsilon_\Gamma(\mathcal{A},S)$ trials and requires exactly one $\mathcal{A}$-query per trial. Hence, the total expected number of trials for both experiments is at most $1/\epsilon_\Gamma(\mathcal{A},S)$. Further, since $t_\Gamma(S \cup \{c_1\}) < t_\Gamma(S)$ (Lemma 4) and by the induction hypotheses, the expected number of $\mathcal{A}$-queries of the first geometric experiment is at most

$$Q_\Gamma(S \cup \{c_1\}) \leq 2t_\Gamma(S \cup \{c_1\}) - 1 \leq 2t_\Gamma(S) - 3\,,$$

per iteration, where the second inequality follows again from Lemma 4. Hence, every iteration of the repeat loop requires an expected number of at most $2t_\Gamma(S) - 2$ $\mathcal{A}$-queries.

From this it follows that

$$Q_\Gamma(S) \leq 1 + \epsilon_\Gamma(\mathcal{A},S)\frac{2t_\Gamma(S) - 2}{\epsilon_\Gamma(\mathcal{A},S)} = 2t_\Gamma(S) - 1\,,$$

for all $S \in 2^{\mathcal{C}} \setminus \Gamma$. In particular, $\mathcal{E}_\Gamma^{\mathcal{A}}$ requires an expected number of at most $2t_\Gamma - 1$ $\mathcal{A}$-queries, which completes the proof of the lemma. □

Remark 4 (Expected Polynomial Runtime). The (expected) runtime of the extractor is typically measured in the number of queries it makes to the adversary $\mathcal{P}^*$. To make a query, the extractor has to sample a challenge $c \in U_\Gamma(S)$ for some $S \notin \Gamma$ with $|S| < t_\Gamma$. Additionally, it must verify the transcript outputted by the adversary. Since the verification of a transcript takes polynomial time by definition, it follows that the extractor runs in expected polynomial time if it can efficiently sample $c \in U_\Gamma(S)$ for all $S \notin \Gamma$ with $|S| < t_\Gamma$.

By basic probability theory, for any $S \notin \Gamma$,

$$\begin{aligned}
\Pr\big(V(C, \mathcal{A}(C)) = 1 \mid C \notin S\big) &= \frac{\Pr\big(V(C, \mathcal{A}(C)) = 1 \wedge C \notin S\big)}{\Pr\big(C \notin S\big)} \\
&\geq \frac{\Pr\big(V(C, \mathcal{A}(C)) = 1) - \Pr\big(C \in S\big)}{\Pr\big(C \notin S\big)} \\
&= \frac{\epsilon(\mathcal{A}) - \Pr\big(C \in S\big)}{1 - \Pr\big(C \in S\big)} \\
&= \frac{\epsilon(\mathcal{A}) - |S| \,/\, |\mathcal{C}|}{1 - |S| \,/\, |\mathcal{C}|} \,.
\end{aligned}$$

Hence, taking the minimum over all $S \notin \Gamma$ shows that

$$\delta_\Gamma(\mathcal{A}) \geq \frac{\epsilon(\mathcal{A}) - \kappa_\Gamma}{1 - \kappa_\Gamma} \,, \tag{3}$$

where $\kappa_\Gamma = \max_{S \notin \Gamma} |S| \,/\, |\mathcal{C}|$. In Γ-out-of-$\mathcal{C}$ special-sound interactive proofs, a dishonest prover can potentially take any $S \notin \Gamma$ and choose the first message so that it will succeed if the verifier chooses a challenge $c \in S$. Hence, κ_Γ equals the trivial cheating strategy for Γ-out-of-$\mathcal{C}$ special-sound interactive proofs.

Since the extractor succeeds with probability at least $\delta_\Gamma(\mathcal{A})/t_\Gamma$, the following theorem follows.

Theorem 1. *Let $(\mathcal{P}, \mathcal{V})$ be a Γ-out-of-$\mathcal{C}$ special-sound Σ-protocol such that t_Γ is polynomial in the size $|x|$ of the the public input statement x of $(\mathcal{P}, \mathcal{V})$ and sampling from $U_\Gamma(S)$ takes polynomial time (in $|x|$) for all S with $|S| < t_\Gamma$. Then $(\mathcal{P}, \mathcal{V})$ is knowledge sound with knowledge error $\kappa_\Gamma = \max_{S \notin \Gamma} |S| \,/\, |\mathcal{C}|$.*

5 Examples

In this section, we describe three very simple interactive proofs and their special-soundness properties. The first example shows that for the special case of k-out-of-N special-soundness notion, we recover the known results. The second and third example present techniques that have found numerous applications, but cannot be analyzed via their threshold special-soundness properties, i.e., these interactive proofs require an alternative analysis. Our knowledge extractor offers the means to easily handle these interactive proof as well. Finally, the fourth

example shows that our generic techniques do not always suffice. In Section 8, we will consider a more complicated protocol and demonstrate how our techniques enable a knowledge soundness analysis of the multi-round protocol FRI [5].

Example 1 (Threshold Access Structures). Let $\mathcal{C}$ be a finite set with cardinality N, and let Γ be the monotone structure that contains all subsets of $\mathcal{C}$ of cardinality at least $k \leq N$. Then a Γ-out-of-$\mathcal{C}$ special-sound interactive proof is also k-out-of-N special-sound. Moreover, $U_\Gamma(A) = \mathcal{C} \setminus A$ for all $A \notin \Gamma$, $t_\Gamma = k$, and $\kappa_\Gamma = (k-1)/N$. Hence, in the case of k-out-of-N special-soundness, we recover the results from [2].

Example 2 (Standard Amortization Technique). Let $\mathbb{F}$ be a finite field and let Ψ be an $\mathbb{F}$-linear map. The following amortization technique, known from Σ-protocol theory, allows a prover to prove knowledge of n Ψ-preimages $x_1, \ldots, x_n$ of $P_1, \ldots, P_n$ for essentially the cost of one. The amortization technique is a 2-round protocol that proceeds as follows. First, the verifier samples a challenge vector $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}^n$ uniformly at random. Second, upon receiving the challenge vector $\mathbf{c}$, the prover responds with the element $z = \sum_{i=1}^n c_i x_i$. Finally, the verifier checks that $\Psi(z) = \sum_{i=1}^n c_i P_i$. Hence, instead of sending n preimages the prover only has to send one preimage.

The n preimages $x_1, \ldots, x_n$ of $P_1, \ldots, P_n$ can be extracted from accepting transcripts $(\mathbf{c}_1, z_1), \ldots, (\mathbf{c}_k, z_k)$ if the challenge vectors $\mathbf{c}_1, \ldots, \mathbf{c}_k$ span the vector space $\mathbb{F}^n$. Hence, the amortization protocol is Γ-out-of-$\mathbb{F}^n$ special-sound, where Γ is the monotone structure that contains all subsets spanning $\mathbb{F}^n$. Further, $t_\Gamma = n$, $U_\Gamma(A) = \mathbb{F}^n \setminus \operatorname{span}(A)$ for all $A \notin \Gamma$; and $\kappa_\Gamma = 1/|\mathbb{F}|$; thus, we obtain optimal knowledge soundness.

At the same time, the amortization protocol is $(|\mathbb{F}|^{n-1}+1)$-out-of-$|\mathbb{F}|^n$ special-sound, i.e., the threshold special-soundness parameter of this protocol is $|\mathbb{F}|^{n-1} + 1$, which is much larger than $t_\Gamma = n$. In fact, the parameter $|\mathbb{F}|^{n-1} + 1$ is typically not polynomially bounded, in which case knowledge soundness can not be derived from this threshold special-soundness property.

Example 3 (Merkle Tree Commitments). Let us now consider an interactive proof for proving knowledge of the opening of a Merkle tree commitment P, i.e., P is the root of a Merkle tree and the prover claims to know all n leafs. To verify this claim, the verifier selects a subset S of k (distinct) indices between 1 and n uniformly at random. The prover sends the corresponding leafs together with their validation paths, which are checked by the verifier.

An opening of the commitment P can be extracted from accepting transcripts $(S_1, z_1), \ldots, (S_\ell, z_\ell)$ if the subsets S_i cover $\{1, \ldots, n\}$. Hence, this interactive proof is Γ-out-of-$\mathcal{C}$, where

$$\mathcal{C} = \{S \subseteq \{1, \ldots, n\} : |S| = k\} \quad \text{and} \quad \Gamma = \left\{\mathcal{D} \subseteq \mathcal{C} : \bigcup_{S \in \mathcal{D}} S = \{1, \ldots, n\}\right\}.$$

Further, $t_\Gamma = n - k + 1$, $U_\Gamma(\mathcal{D}) = \{A \in \mathcal{C} : A \not\subseteq \bigcup_{S \in \mathcal{D}} S\}$ for all $\mathcal{D} \notin \Gamma$, and $\kappa_\Gamma = (n-k)/n$; thus, we obtain optimal knowledge soundness.

The threshold special-soundness parameter of this protocol is $\binom{n-1}{k} + 1$ which is typically much larger than $t_\Gamma = n - k + 1$. Hence, also in this case our generalization provides a much more efficient knowledge extractor.

This simple interactive proof is an essential component in many more complicated protocols based on probabilistically checkable proofs (PCPs), interactive oracle proofs (IOPs) or MPC-in-the-head.

Example 4 (Parallel Repetition). Finally, we consider an example where our generic technique does not work. To this end, let Π^t be the t-fold parallel composition of a k-out-of-N special-sound interactive proof Π with challenge set $\mathcal{C}$, i.e., Π^t has challenge set $\mathcal{C}^t$. Then, as discussed in the introduction, Π^t is $\big((k-1)^t + 1\big)$-out-of-N^t special-sound, i.e., its threshold special-soundness parameter $(k-1)^t + 1$ grows exponentially in t (if $k > 2$).

The parallel repetition Π^t is also Γ-out-of-$\mathcal{C}^t$ special-sound, where Γ contains all subsets of challenge vectors $\mathbf{c} \in \mathcal{C}^t$ such that there is one position $1 \leq i \leq t$ where the challenge vectors feature at least k different values. Then, $\kappa_\Gamma = (k-1)^t/N^t$. However, $t_\Gamma = (k-1)^t+1$, i.e., t_Γ equals the threshold special-soundness parameter and grows exponentially in t. Hence, in this particular example, the correct access structure does not yield an efficient extractor. Fortunately, here we can apply the parallel repetition result of [2].

6 Knowledge Extraction for Multi-Round Interactive Proofs

Let us now move to the analysis of multi-round interactive proofs $(\mathcal{P}, \mathcal{V})$. To this end, we first generalize the notion of Γ-out-of-$\mathcal{C}$ special-soundness to multi-round interactive proofs. A $2\mu+1$-round interactive proof is said to be $(\Gamma_1, \ldots, \Gamma_\mu)$-out-of-$(\mathcal{C}_1, \ldots, \mathcal{C}_\mu)$ if there exists an efficient algorithm that can extract a witness from appropriate trees of transcripts. Before we formally define trees of transcripts, we first define the related trees of challenges.

Definition 10 (Tree of Challenges). *Let $(\Gamma_i, \mathcal{C}_i)$ be monotone structures for $1 \leq i \leq \mu$. A set containing a single challenge vector $(c_1, \ldots, c_\mu) \in \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ is also referred to as a $(1, \ldots, 1)$-tree of challenges. Further, for $1 \leq t \leq \mu$, a $(1, \ldots, 1, \Gamma_t, \ldots, \Gamma_\mu)$-tree T_t of challenges is the union of several $(1, \ldots, 1, \Gamma_{t+1}, \ldots, \Gamma_\mu)$-trees, such that*

- *The first $t-1$ coordinates of all $\mathbf{c} \in T_t \subseteq \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ are equal;*
- *The t-th coordinates of the tree elements form an element in Γ_t, i.e.,*

$$\{c \in \mathcal{C}_t : \exists (c_1, \ldots, c_{t-1}, c, c_{t+1}, \ldots, c_\mu) \in T_t\} \in \Gamma_t \,.$$

Moreover, we define the following monotone structure:

$$\Gamma_{\text{TREE}}(\Gamma_1, \ldots, \Gamma_\mu) := \{S \subseteq \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu : S \text{ contains a } (\Gamma_1, \ldots, \Gamma_\mu)\text{-tree}\} \,.$$

Trivially, the verifier's messages in a transcript of a $2\mu+1$-round interactive proof with challenge sets $\mathcal{C}_1,\ldots,\mathcal{C}_\mu$ form a $(1,\ldots,1)$-tree of challenges. Hence, by adding the prover's messages we obtain a $(1,\ldots,1)$-tree of transcripts, and thus, in the obvious way, we obtain the notion of a tree of transcripts. The only additional requirement is that the prover's messages *collide*, i.e., they are uniquely determined by the challenges received before sending the message. In particular, the first message of every transcript is the same. Note that if the transcripts are generated by a deterministic prover, this property is guaranteed to hold.

Definition 11 (Tree of Transcripts). *Let $(\Gamma_i,\mathcal{C}_i)$ be monotone structures for $1\leq i\leq\mu$. Let $(\mathcal{P},\mathcal{V})$ be a $2\mu+1$-round public-coin interactive proof with challenge sets $\mathcal{C}_1,\ldots,\mathcal{C}_\mu$. A $(\Gamma_1,\ldots,\Gamma_\mu)$-tree of transcripts is a set of protocol transcripts, such that*

- *The corresponding set of challenge vectors, obtained by ignoring the prover's messages, is a $(\Gamma_1,\ldots,\Gamma_\mu)$-tree of challenges;*
- *The prover's messages* collide*, i.e., if two transcripts $(a_0,c_1,a_1,\ldots,c_\mu,a_\mu)$ and $(a'_0,c'_1,a'_1,\ldots,c'_\mu,a'_\mu)$ are both in the tree, and $c_i=c'_i$ for all $i\leq j$, then also $a_i=a'_i$ for all $i\leq j$.*

Prior works (e.g., [10, 11, 1]) considered $(k_1,\ldots,k_\mu)$-trees, where $k_i\in\mathbb{N}$ for all i. These are special cases of the above defined trees. More precisely, if $\Gamma_i=\{S\subseteq\mathcal{C}_i:|S|\geq k_i\}$, a $(k_1,\ldots,k_\mu)$-tree is the same as a $(\Gamma_1,\ldots,\Gamma_t)$-tree.

We are now ready to define a generalized multi-round special-soundness notion.

Definition 12 ($(\Gamma_1,\ldots,\Gamma_\mu)$-out-of-$(\mathcal{C}_1,\ldots,\mathcal{C}_\mu)$ Special-Soundness). *Let $(\Gamma_i,\mathcal{C}_i)$ be monotone structures for $1\leq i\leq\mu$. A $2\mu+1$-round public-coin interactive proof $(\mathcal{P},\mathcal{V})$ for relation R, with challenge sets $\mathcal{C}_1,\ldots,\mathcal{C}_\mu$, is* $(\Gamma_1,\ldots,\Gamma_\mu)$-out-of-$(\mathcal{C}_1,\ldots,\mathcal{C}_\mu)$ special-sound *if there exists a polynomial time algorithm that, on input a statement x and a $(\Gamma_1,\ldots,\Gamma_\mu)$-tree of accepting transcripts, outputs a witness $w\in R(x)$. We also say that $(\mathcal{P},\mathcal{V})$ is $(\Gamma_1,\ldots,\Gamma_\mu)$-special-sound.*

Our goal is now to prove that, for appropriate monotone structures, $(\Gamma_1,\ldots,\Gamma_\mu)$-out-of-$(\mathcal{C}_1,\ldots,\mathcal{C}_\mu)$ special-soundness (tightly) implies knowledge soundness. As before, again borrowing the notation from [2], we present our results in a more abstract language. To this end, let $\mathcal{A}\colon\mathcal{C}_1\times\cdots\times\mathcal{C}_\mu\to\{0,1\}^*$ be a probabilistic algorithm and

$$V\colon\mathcal{C}_1\times\cdots\times\mathcal{C}_\mu\times\{0,1\}^*\to\{0,1\}$$

a verification function. The success probability of $\mathcal{A}$ is denoted as

$$\epsilon(\mathcal{A}):=\Pr\big(V\big(C,\mathcal{A}(C)\big)=1\big)\,,$$

where C is distributed uniformly at random over $\mathcal{C}_1\times\cdots\times\mathcal{C}_\mu$. The obvious instantiation of $\mathcal{A}$ is again a deterministic prover $\mathcal{P}^*$ attacking a $(\Gamma_1,\ldots,\Gamma_\mu)$-out-of-$(\mathcal{C}_1,\ldots,\mathcal{C}_\mu)$ special-sound interactive proof.

Let us now write $\mathbf{\Gamma} = (\Gamma_1, \Gamma_2, \ldots, \Gamma_\mu)$ and $\boldsymbol{\mathcal{C}} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$. Then the punctured success probability, defined in Section 4, has the following natural generalization for multi-round interactive proofs:

$$\delta^V_{\mathbf{\Gamma}}(\mathcal{A}) := \min_{S \notin \Gamma_{\text{TREE}}(\mathbf{\Gamma})} \Pr\big(V(C, \mathcal{A}(C)) = 1 \,\big|\, C \notin S\big)\,. \tag{4}$$

Remark 5. The value $\delta^V_{\mathbf{\Gamma}}(\mathcal{A})$ matches the value $\delta^V_{\Gamma}(\mathcal{A})$ of Section 4, but with an adjusted monotone structure

$$(\Gamma, \mathcal{C}) = \big(\Gamma_{\text{TREE}}(\mathbf{\Gamma}), \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu\big)\,,$$

for $\delta^V_{\Gamma}(\mathcal{A})$. Therefore, in principle, one could immediately apply the results from Section 4. However, this would lead to a suboptimal result and typically an inefficient extractor. More precisely, the value $t_{\Gamma_{\text{TREE}}(\mathbf{\Gamma})}$ grows linearly in the product of the sizes of the challenge sets $\mathcal{C}_1, \ldots, \mathcal{C}_{\mu-1}$. Therefore, in the following, we do a more elaborate analysis that exploits the additional tree structure of $\Gamma_{\text{TREE}}(\mathbf{\Gamma})$.

Oftentimes, the verification function V is clear from context, in which case we simply write $\delta_{\mathbf{\Gamma}}(\mathcal{A})$ instead of $\delta^V_{\mathbf{\Gamma}}(\mathcal{A})$. The minimum in Equation 4 is over all subset $S \subseteq \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ that do not contain a $\mathbf{\Gamma}$-tree. Hence, again we puncture the success probability by removing some set S from which we cannot extract. Since we take the minimum over all such subsets S, $\delta^V_{\mathbf{\Gamma}}(\mathcal{A}) > 0$ implies the existence of a $\mathbf{\Gamma}$-tree of challenges T such that $\mathcal{A}$ succeeds with positive probability on all challenges in T. Further, if $\delta^V_{\mathbf{\Gamma}}(\mathcal{A}) = 0$, this extractability property cannot be guaranteed. Hence, at least in principle, extraction is possible if $\delta_{\mathbf{\Gamma}}(\mathcal{A}) > 0$. However, it is far less obvious that extraction can also be done efficiently. The following lemma shows that, for appropriate monotone structures $(\Gamma_i, \mathcal{C}_i)$, an efficient extraction algorithm indeed exists. This is a generalization of [2, Lemma 4]. Using the notation we introduced here, their proof almost immediately carries over to this more generic setting. For completeness, we present the proof below.

Lemma 6 (Multi-Round Extraction Algorithm). *Let $\mathbf{\Gamma} = (\Gamma_1, \ldots, \Gamma_\mu)$ and $\boldsymbol{\mathcal{C}} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ be such that $(\Gamma_i, \mathcal{C}_i)$ are nonempty monotone structures for all i. Further, let $T := \prod_{i=1}^{\mu} t_{\Gamma_i}$ and $V \colon \boldsymbol{\mathcal{C}} \times \{0,1\}^* \to \{0,1\}$. Then, there exists an algorithm $\mathcal{E}^{\mathcal{A}}$ so that, given oracle access to any (probabilistic) algorithm $\mathcal{A} \colon \boldsymbol{\mathcal{C}} \to \{0,1\}^*$, $\mathcal{E}^{\mathcal{A}}$ requires an expected number of at most $2^\mu \cdot T$ queries to $\mathcal{A}$ and, with probability at least $\delta_\Gamma(\mathcal{A})/T$, outputs pairs $(\mathbf{c}_i, y_i) \in \boldsymbol{\mathcal{C}} \times \{0,1\}^*$ such that $\{\mathbf{c}_i\}_i$ is a $\mathbf{\Gamma}$-tree with $V(\mathbf{c}_i, y_i) = 1$ for all i.*

Proof. The proof goes by induction on μ. For the base case $\mu = 1$, the lemma directly follows from Lemma 5. So let us assume the lemma holds for $\mu' := \mu - 1$. Further, let $\boldsymbol{\mathcal{C}}' := \mathcal{C}_2 \times \cdots \times \mathcal{C}_\mu$, $\mathbf{\Gamma}' := (\Gamma_2, \ldots, \Gamma_\mu)$ and $T' := \prod_{i=2}^{\mu} t_{\Gamma_i}$.

Then, for any $c \in \mathcal{C}_1$, let $\mathcal{A}_c$ be the algorithm that takes as input a vector $\mathbf{c}' = (c_2, \ldots, c_\mu) \in \boldsymbol{\mathcal{C}}'$ and runs $\mathcal{A}(c, \mathbf{c}')$. The function V_c is defined accordingly, i.e.,

$$V_c \colon \boldsymbol{\mathcal{C}}' \times \{0,1\}^* \to \{0,1\}, \quad (\mathbf{c}', y) \mapsto V(c, \mathbf{c}', y)\,.$$

By the induction hypothesis there exists an algorithm $\mathcal{E}_{\mu-1}^{\mathcal{A}_c}$ that outputs a set $\mathcal{Y} = \{(\mathbf{c}'_i, y_i)\}_i \subseteq \boldsymbol{\mathcal{C}}' \times \{0,1\}^*$ with

$$V_c(\mathbf{c}'_i, y_i) = V(c, \mathbf{c}'_i, y_i) = 1 \ \forall i \quad \text{and} \quad \{\mathbf{c}'_i\}_i \in \Gamma_{\text{TREE}}(\Gamma_2, \ldots, \Gamma_\mu)\,.$$

Moreover, $\mathcal{E}_{\mu-1}^{\mathcal{A}_c}$ requires an expected number of at most $2^{\mu-1} \cdot T'$ queries to $\mathcal{A}_c$ (and thus to $\mathcal{A}$) and succeeds with probability at least $\delta_{\Gamma'}^{V_c}(\mathcal{A}_c)/T'$. We define $W\colon \mathcal{C}_1 \times \{0,1\}^* \to \{0,1\}$, by setting $W(c, \mathcal{Y}) = 1$ if and only if $\mathcal{Y}$ is a set satisfying the above properties.

Now let $\mathcal{B}^{\mathcal{A}}\colon \mathcal{C}_1 \to \{0,1\}^*$ be the algorithm that, with oracle access to $\mathcal{A}$, takes as input an element $c \in \mathcal{C}_1$ and runs $\mathcal{E}_{\mu-1}^{\mathcal{A}_c}$. By Lemma 5, there exists an expected polynomial time algorithm $\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$, with oracle access to $\mathcal{B}^{\mathcal{A}}$, that aims to output pairs $(c_j, \mathcal{Y}_j) \in \mathcal{C}_1 \times \{0,1\}^*$ with $W(c_j, \mathcal{Y}_j) = 1$ for all j and $\{c_j\}_j \in \Gamma_1$.

Rearranging the output $\{(c_j, \mathcal{Y}_j)\}_j \in \mathcal{C}_1 \times \{0,1\}^*$ of a successful $\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$-invocation is easily seen to give a set of pairs $(\mathbf{c}_i, y_i) \in \boldsymbol{\mathcal{C}} \times \{0,1\}^*$ such that $\{\mathbf{c}_i\}_i$ is a Γ-tree with $V(\mathbf{c}_i, y_i) = 1$ for all i. For this reason, the extractor $\mathcal{E}^{\mathcal{A}}$ simply runs $\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$. Note that, by the associativity of the composition of oracle algorithms, $\mathcal{E}^{\mathcal{A}} = \mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}} = (\mathcal{E}_1^{\mathcal{B}})^{\mathcal{A}}$ is indeed an algorithm with oracle access to $\mathcal{A}$.

Let us now analyze the success probability and the expected number of $\mathcal{A}$-queries of the algorithm $\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$ and therefore of $\mathcal{E}^{\mathcal{A}}$.

Success Probability. Let us write $t_i := t_{\Gamma_i}$ for all i. Again by Lemma 5, it follows that $\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$ succeeds with probability at least

$$\begin{aligned}
\frac{\delta_{\Gamma_1}^{W}(\mathcal{B}^{\mathcal{A}})}{t_1} &= \min_{S_1 \notin \Gamma_1} \frac{\Pr\big(W(C_1, \mathcal{B}^{\mathcal{A}}(C_1)) = 1 \mid C_1 \notin S_1\big)}{t_1} \\
&= \min_{S_1 \notin \Gamma_1} \frac{\Pr\big(W(C_1, \mathcal{B}^{\mathcal{A}}(C_1)) = 1 \wedge C_1 \notin S_1\big)}{t_1 \cdot \Pr(C_1 \notin S_1)} \\
&= \min_{S_1 \notin \Gamma_1} \frac{\sum_{c \notin S_1} \Pr(C_1 = c) \cdot \Pr\big(W(c, \mathcal{B}^{\mathcal{A}}(c)) = 1\big)}{t_1 \cdot \Pr(C_1 \notin S_1)} \\
&= \min_{S_1 \notin \Gamma_1} \frac{\sum_{c \notin S_1} \Pr(C_1 = c) \cdot \Pr\big(W(c, \mathcal{E}_{\mu-1}^{\mathcal{A}_c}) = 1\big)}{t_1 \cdot \Pr(C_1 \notin S_1)} \\
&\geq \min_{S_1 \notin \Gamma_1} \frac{\sum_{c \notin S_1} \Pr(C_1 = c) \cdot \delta_{\boldsymbol{\Gamma}'}^{V_c}(\mathcal{A}_c)}{t_1 \cdot T' \cdot \Pr(C_1 \notin S_1)} \\
&= \min_{S_1 \notin \Gamma_1} \frac{\sum_{c \notin S_1} \Pr(C_1 = c) \cdot \delta_{\boldsymbol{\Gamma}'}^{V_c}(\mathcal{A}_c)}{T \cdot \Pr(C_1 \notin S_1)}\,, \qquad (5)
\end{aligned}$$

where C_1 is distributed uniformly at random over $\mathcal{C}_1$. Now note that

$$\delta_{\boldsymbol{\Gamma}'}^{V_c}(\mathcal{A}_c) = \min_{S' \notin \Gamma_{\text{TREE}}(\boldsymbol{\Gamma}')} \Pr\big(\Lambda : C_1 = c \wedge (C_2, \ldots, C_\mu) \notin S'\big)\,,$$

where Λ denotes the event $V(C, \mathcal{A}(C)) = 1$ and $C = (C_1, \ldots, C_\mu)$ is distributed uniformly at random over $\mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$.

Hence,

$$\begin{aligned}\sum_{c\notin S_1}\frac{\Pr(C_1=c)\delta^{V_c}_{\mathbf{\Gamma}'}(\mathcal{A}_c)}{\Pr(C_1\notin S_1)} &= \min_{S'\notin \Gamma_{\text{TREE}}(\mathbf{\Gamma}')}\frac{\Pr\big(C_1\notin S_1\wedge \Lambda:(C_2,\ldots,C_\mu)\notin S'\big)}{\Pr(C_1\notin S_1)}\\ &= \min_{S'\notin \Gamma_{\text{TREE}}(\mathbf{\Gamma}')}\Pr\big(\Lambda: C_1\notin S_1\wedge (C_2,\ldots,C_\mu)\notin S'\big)\\ &= \min_{S'\notin \Gamma_{\text{TREE}}(\mathbf{\Gamma}')}\Pr\big(\Lambda: C\notin S\big)\,,\end{aligned}$$

where

$$S := \{(c_1,\mathbf{c}')\in\mathcal{C}_1\times\boldsymbol{\mathcal{C}}' : c_1\in S_1\vee\mathbf{c}'\in S'\}\subseteq\boldsymbol{\mathcal{C}}\,.$$

Since $S_1\notin\Gamma_1$ and $S'\notin\Gamma_{\text{TREE}}(\mathbf{\Gamma}')$, it follows that $S\notin\Gamma_{\text{TREE}}(\mathbf{\Gamma})$. Hence,

$$\sum_{c\notin S_1}\frac{\Pr(C_1=c)\delta^{V_c}_{\mathbf{\Gamma}'}(\mathcal{A}_c)}{\Pr(C_1\notin S_1)}\geq\min_{S\notin\Gamma_{\text{TREE}}(\mathbf{\Gamma})}\Pr\big(\Lambda:C\notin S\big)=\delta^V_\Gamma(\mathcal{A})\,.$$

Plugging this equality into Equation 5 shows that

$$\frac{\delta^W_{\Gamma_1}(\mathcal{B}^{\mathcal{A}})}{t_1}\geq\frac{\delta^V_\Gamma(\mathcal{A})}{T}\,,$$

which shows that $\mathcal{E}_1^{B^{\mathcal{A}}}$ (and thus $\mathcal{E}^{\mathcal{A}}$) has the desired success probability.

Expected Number of $\mathcal{A}$-Queries. By Lemma 5, it follows that $\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$ requires an expected number of at most $2t_1-1<2t_1$ queries to $\mathcal{B}^{\mathcal{A}}$. By the induction hypothesis it follows that $\mathcal{B}^{\mathcal{A}}(c)$ requires an expected number of at most $2^{\mu-1}\cdot T'$ queries to $\mathcal{A}$ for every $c\in\mathcal{C}_1$. Hence, $\mathcal{E}^{\mathcal{A}}=\mathcal{E}_1^{\mathcal{B}^{\mathcal{A}}}$ requires an expected number of at most $2^\mu\cdot T$ queries to $\mathcal{A}$, which completes the proof of the lemma. □

By basic probability theory, for any $S\subseteq\mathcal{C}_1\times\cdots\times\mathcal{C}_\mu$, it follows that

$$\begin{aligned}\Pr\big(V(C,\mathcal{A}(C))=1\mid C\notin S\big)&=\frac{\Pr\big(V(C,\mathcal{A}(C))=1\ \wedge\ C\notin S\big)}{\Pr\big(C\notin S\big)}\\ &\geq\frac{\Pr\big(V(C,\mathcal{A}(C))=1\big)-\Pr\big(C\in S\big)}{\Pr\big(C\notin S\big)}\\ &=\frac{\epsilon_\Gamma(\mathcal{A})-\Pr\big(C\in S\big)}{1-\Pr\big(C\in S\big)}\\ &=\frac{\epsilon_\Gamma(\mathcal{A})-|S|/|\mathcal{C}|}{1-|S|/|\mathcal{C}|}\,.\end{aligned}$$

Hence,

$$\begin{aligned}\delta_\Gamma(\mathcal{A})&\geq\min_{S\notin\Gamma_{\text{TREE}}(\mathbf{\Gamma})}\frac{\epsilon_\Gamma(\mathcal{A})-|S|/|\mathcal{C}|}{1-|S|/|\mathcal{C}|}\\ &=\frac{\epsilon_{\mathbf{\Gamma}}(\mathcal{A})-\kappa_{\mathbf{\Gamma}}}{1-\kappa_{\mathbf{\Gamma}}}\,,\end{aligned}$$

where

$$\kappa_{\mathbf{\Gamma}} = \max_{S \notin \mathit{\Gamma}_{\text{TREE}}(\mathbf{\Gamma})} \frac{|S|}{|\mathcal{C}|} = 1 - \prod_{i=1}^{\mu} \left(1 - \max_{S_i \notin \mathit{\Gamma}_i} \frac{|S_i|}{|\mathcal{C}_i|}\right) = 1 - \prod_{i=1}^{\mu} (1 - \kappa_{\mathit{\Gamma}_i}) \,.$$

These observations complete the proof of the following theorem.

Theorem 2. *Let $(\mathcal{P}, \mathcal{V})$ be a $(\mathit{\Gamma}_1, \ldots, \mathit{\Gamma}_\mu)$-out-of-$(\mathcal{C}_1, \ldots, \mathcal{C}_\mu)$ special-sound interactive proof such that $T_{\mathbf{\Gamma}} = \prod_{i=1}^{\mu} t_{\mathit{\Gamma}_i}$ is polynomial in the size $|x|$ of the public input statement x of $(\mathcal{P}, \mathcal{V})$ and sampling from $U_{\mathit{\Gamma}_i}(S_i)$ takes polynomial time (in $|x|$) for all $1 \leq i \leq \mu$ and $S_i \subset \mathcal{C}_i$ with $|S_i| < t_{\mathit{\Gamma}_i}$. Then $(\mathcal{P}, \mathcal{V})$ is knowledge sound with knowledge error*

$$\kappa_{\mathbf{\Gamma}} = 1 - \prod_{i=1}^{\mu} \left(1 - \max_{S_i \notin \mathit{\Gamma}_i} \frac{|S_i|}{|\mathcal{C}_i|}\right) .$$

7 Parallel Repetition

Sometimes the knowledge error of an interactive proof is too large. A natural approach for reducing the knowledge error is parallel repetition. In the t-fold parallel repetition $(\mathcal{P}^t, \mathcal{V}^t)$ of an interactive proof $(\mathcal{P}, \mathcal{V})$ both the prover and the verifier run t instances of $(\mathcal{P}, \mathcal{V})$ in parallel. Further, $\mathcal{V}^t$ accepts if and only if all t invocations of $(\mathcal{P}, \mathcal{V})$ are accepted by $\mathcal{V}$. Ideally parallel repetition reduces the knowledge error at an exponential rate, i.e., from κ down to κ^t. However, there exist protocols for which parallel repetition does not reduce the knowledge error at all [4].

Recently, it was shown that, for $(k_1, \ldots, k_\mu)$-special-sound interactive proofs with $k_i \in \mathbb{N}$ for all i, t-fold parallel repetition decreases the knowledge error at an optimal rate from κ down to κ^t [2]. Here, we show that this result immediately generalizes to $(\mathit{\Gamma}_1, \ldots, \mathit{\Gamma}_\mu)$-out-of-$(\mathcal{C}_1, \ldots, \mathcal{C}_\mu)$ special-sound interactive proofs.

The first observation of [2] is that any algorithm $\mathcal{A}$ attacking the t-fold parallel repetition $(\mathcal{P}^t, \mathcal{V}^t)$ of a $(2\mu+1)$-round interactive proof $(\mathcal{P}, \mathcal{V})$ naturally induces t algorithms $\mathcal{A}_1, \ldots, \mathcal{A}_t$, all attacking a single invocation of $(\mathcal{P}, \mathcal{V})$. Namely, for $1 \leq j \leq t$, the probabilistic algorithm $\mathcal{A}_j \colon \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu \to \{0,1\}^*$ is defined as follows. It samples $\mathbf{c}[j'] \in \boldsymbol{\mathcal{C}} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ (for $j' \neq j$) uniformly at random and outputs $\mathcal{A}_j(\mathbf{c}) = \mathcal{A}(\mathbf{c}[1], \ldots, \mathbf{c}[j-1], \mathbf{c}, \mathbf{c}[j+1], \ldots, \mathbf{c}[t])$ together with the sampled challenge vectors $\mathbf{c}[j']$. The verification function V used to verify the output of $\mathcal{A}$ can also be used to verify the output of $\mathcal{A}_j$. In particular, it is easily seen that $\mathcal{A}_j$ and $\mathcal{A}$ have the same success probability, i.e.,

$$\epsilon^V(\mathcal{A}_j) = \epsilon^V(\mathcal{A}) \;\forall j \,.$$

However, the same does not need to hold for the punctured success probabilities $\delta^V(\mathcal{A}_j)$.

Given a knowledge extractor $\mathcal{E}$ for $(\mathcal{P}, \mathcal{V})$ another knowledge extractor $\mathcal{E}_t$ for $(\mathcal{P}^t, \mathcal{V}^t)$ can be defined as follows. When given oracle access to an algorithm $\mathcal{A}$

attacking $(\mathcal{P}^t, \mathcal{V}^t)$, the extractor $\mathcal{E}_t^{\mathcal{A}}$ simply runs t-extractors $\mathcal{E}^{\mathcal{A}_1}, \ldots, \mathcal{E}^{\mathcal{A}_t}$ in parallel. The extractor $\mathcal{E}_t^{\mathcal{A}}$ succeeds if at least one of the extractors $\mathcal{E}^{\mathcal{A}_j}$ succeeds. In [2, Lemma 5], it was shown that for $(k_1, \ldots, k_\mu)$-special-sound interactive proofs this happens with large enough probability, implying knowledge soundness of the t-fold parallel repetition.

The following lemma is a generalization of [2, Lemma 5], showing that also for $(\Gamma_1, \ldots, \Gamma_\mu)$-out-of-$(\mathcal{C}_1, \ldots, \mathcal{C}_\mu)$ special-sound interactive proofs at least one of the extractors $\mathcal{E}^{\mathcal{A}_j}$ succeeds with large enough probability.

Lemma 7. *Let $\mathbf{\Gamma} = (\Gamma_1, \ldots, \Gamma_\mu)$ and $\boldsymbol{\mathcal{C}} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ be such that $(\Gamma_i, \mathcal{C}_i)$ are nonempty monotone structures for all $1 \le i \le \mu$. Further, let $\mathcal{A}$ be a (probabilistic) algorithm that takes as input a row $(\mathbf{c}[1], \ldots, \mathbf{c}[t]) \in \boldsymbol{\mathcal{C}}^t$ of columns $\mathbf{c}[j] = (c_1[j], \ldots, c_\mu[j]) \in \boldsymbol{\mathcal{C}}$ and outputs a string $y \in \{0,1\}^*$, and let $V \colon \boldsymbol{\mathcal{C}}^t \times \{0,1\}^* \to \{0,1\}$ be a verification algorithm.*

Then

$$\sum_{j=1}^{t} \delta_{\mathbf{\Gamma}}(\mathcal{A}_j) \ge \epsilon_{\mathbf{\Gamma}}(\mathcal{A}) - \kappa_{\mathbf{\Gamma}}^t \,,$$

where

$$\kappa_{\mathbf{\Gamma}} = 1 - \prod_{i=1}^{\mu} \left(1 - \max_{S_i \notin \Gamma_i} \frac{|S_i|}{|\mathcal{C}_i|}\right).$$

Proof. Let $C = (C[1], \ldots, C[t])$ denote the random variable distributed uniformly over $\boldsymbol{\mathcal{C}}^t$, i.e., $C[j]$ is distributed uniformly over $\boldsymbol{\mathcal{C}} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_\mu$ for all $1 \le j \le t$. Further, let Λ denote the event $V(C, \mathcal{A}(C)) = 1$ and, for $1 \le j \le t$, let $S[j] \notin \Gamma_{\text{TREE}}(\mathbf{\Gamma})$ be such that it minimizes

$$\delta_{\mathbf{\Gamma}}^V(\mathcal{A}_j) := \min_{S \notin \Gamma_{\text{TREE}}(\mathbf{\Gamma})} \Pr\big(V(C, \mathcal{A}(C)) = 1 \,\big|\, C \notin S\big)\,. \tag{6}$$

Since $S[j] \notin \Gamma_{\text{TREE}}(\mathbf{\Gamma})$, it follows that

$$|S[j]| \le |\boldsymbol{\mathcal{C}}| - \prod_{i=1}^{\mu} \left(|\mathcal{C}_i| - \max_{S_i \notin \Gamma_i} |S_i|\right).$$

Hence,

$$\Pr\big(C[j] \in S[j]\big) \le \kappa_{\mathbf{\Gamma}}\,.$$

Therefore, using elementary probability theory,

$$\begin{aligned}
\sum_{j=1}^{t} \delta_{\mathbf{\Gamma}}^V(\mathcal{A}_j) &= \sum_{j=1}^{t} \Pr\big(\Lambda \mid C[j] \notin S[j]\big) \ge \sum_{j=1}^{t} \Pr\big(\Lambda \wedge C[j] \notin S[j]\big) \\
&\ge \Pr\big(\Lambda \wedge \exists\, j : C[j] \notin S[j]\big) \ge \Pr\big(\Lambda\big) - \Pr\big(C[j] \in S[j]\ \forall i\big) \\
&= \epsilon^V(\mathcal{A}) - \prod_{j=1}^{t} \Pr\big(C[j] \in S[j]\big) \ge \epsilon^V(\mathcal{A}) - \kappa_{\mathbf{\Gamma}}^t\,,
\end{aligned}$$

which completes the proof. □

Remark 6. For the special case of threshold structures $\Gamma_i := \{S \subseteq \mathcal{C}_i : |S| \geq k_i\}$, i.e., when considering $(k_1, \ldots, k_\mu)$-special-sound interactive proofs, Lemma 5 of [2] actually shows the slightly stronger upper-bound

$$\sum_{j=1}^{t} \delta_{\mathbf{\Gamma}}(\mathcal{A}_j) \geq \frac{\epsilon_{\mathbf{\Gamma}}(\mathcal{A}) - \kappa_{\mathbf{\Gamma}}^t}{1 - \kappa_{\mathbf{\Gamma}}} \,.$$

In our generalization, we cannot guarantee that the sets $S[j]$ minimizing Equation 6 are of maximum cardinality. For this reason, we derive a slightly smaller lower-bound, which is still sufficient for deriving a tight bound on the knowledge error of parallel repetitions.

Hence, at least one of the extractors $\mathcal{E}^{\mathcal{A}_j}$ invoked by $\mathcal{E}_t^{\mathcal{A}}$ succeeds with probability at least

$$\frac{1}{t}\sum_{j=1}^{t} \frac{\delta_{\mathbf{\Gamma}}(\mathcal{A}_j)}{T_{\mathbf{\Gamma}}} \geq \frac{\epsilon^V(\mathcal{A}) - \kappa_{\mathbf{\Gamma}}^t}{tT_{\mathbf{\Gamma}}} \,,$$

where $T_{\mathbf{\Gamma}} = \prod_{i=1}^{\mu} t_{\Gamma_i}$. In [2, Equation 3], it is shown how to refine this bound to

$$\frac{1}{t}\sum_{j=1}^{t} \frac{\delta_{\mathbf{\Gamma}}(\mathcal{A}_j)}{T_{\mathbf{\Gamma}}} \geq \frac{\epsilon^V(\mathcal{A}) - \kappa_{\mathbf{\Gamma}}^t}{2T_{\mathbf{\Gamma}}} \,.$$

Both bounds imply the following parallel repetition theorem.

Theorem 3 (Parallel Repetition). *Let $(\mathcal{P}, \mathcal{V})$ be a $(\Gamma_1, \ldots, \Gamma_\mu)$-out-of-$(\mathcal{C}_1, \ldots, \mathcal{C}_\mu)$ special-sound interactive proof such that $T_{\mathbf{\Gamma}} = \prod_{i=1}^{\mu} t_{\Gamma_i}$ is polynomial in the size $|x|$ of the public input statement x of $(\mathcal{P}, \mathcal{V})$ and sampling from $U_{\Gamma_i}(S_i)$ takes polynomial time (in $|x|$) for all $1 \leq i \leq \mu$ and $S_i \subset \mathcal{C}_i$ with $|S_i| < t_{\Gamma_i}$. Then the t-fold parallel repetition $(\mathcal{P}^t, \mathcal{V}^t)$ of $(\mathcal{P}, \mathcal{V})$ is knowledge sound with knowledge error $\kappa_{\mathbf{\Gamma}}^t$, where*

$$\kappa_{\mathbf{\Gamma}} = 1 - \prod_{i=1}^{\mu}\left(1 - \max_{S_i \notin \Gamma_i} \frac{|S_i|}{|\mathcal{C}_i|}\right),$$

is the knowledge error of $(\mathcal{P}, \mathcal{V})$ and $\mathbf{\Gamma} = (\Gamma_1, \ldots, \Gamma_\mu)$.

8 Analysis of the FRI-protocol

In this section we show how to use our generalized notion of special-soundness to prove essentially tight knowledge soundness of the Fast Reed-Solomon Interactive Oracle Proof of Proximity due to Ben-Sasson et al. [5], assuming it has been compiled into an interactive proof the natural way (i.e., the oracles are replaced by compact commitments to the vectors with a local opening functionality). We first provide the necessary background on the protocol before providing our analysis. We remark that we use ideas that were implicit in prior works; our main aim in this section is to demonstrate the power of our generalized special-soundness notion and the accompanying knowledge extractor.

8.1 Preliminaries on Reed-Solomon Codes

Let $\mathbb{F}$ be a finite field of cardinality q and $S \subseteq \mathbb{F}$. Given a polynomial $f(X) \in \mathbb{F}[X]$ we let $f(S) = (f(s))_{s \in S}$ denote the vector of evaluations of f over the domain S (given in some arbitrary, but fixed, order).

For any $0 \leq \rho \leq 1$, the Reed-Solomon code $\mathrm{RS}[\mathbb{F}, S, \rho] \subseteq \mathbb{F}^{|S|}$ consists of all evaluations over the domain S of polynomials $F(X) \in \mathbb{F}[X]$ of degree less than $\rho|S|$. In notation,

$$\mathrm{RS}[\mathbb{F}, S, \rho] := \{F(S) : F(X) \in \mathbb{F}[X] \wedge \deg(F) < \rho|S|\} \ .$$

We set $\rho = 2^{-r}$ for an integer $r < \log_2(|S|)$, which implies $\rho|S| \in \mathbb{N}$ and that the dimension of $\mathrm{RS}[\mathbb{F}, S, \rho]$ is precisely $\rho|S|$.

In the sequel we will assume S is a multiplicative subgroup of $\mathbb{F}^*$ of order a power of 2, with the understanding that our analysis should generalize readily to other "smooth" evaluation domains for FRI protocols. Letting $N = |S|$, we therefore have $S = \langle \omega \rangle = \{1, \omega, \omega^2, \ldots, \omega^{N-2}\}$ where ω is a primitive N-th root of unity. Note then that $S^2 = \langle \omega^2 \rangle = \{1, \omega^2, \omega^4, \ldots, \omega^{N-1}\}$ is a multiplicative subgroup of $\mathbb{F}^*$ of order $N/2$. More generally, for any $j = 1, 2, \ldots, \log_2(N)$, $S^{2^j} = \langle \omega^{2^j} \rangle$ is multiplicative subgroup of $\mathbb{F}^*$ of order $N/2^j$.

Given two polynomials $f(X), g(X) \in \mathbb{F}[X]$ we let $d_S(f, g) := |\{s \in S : f(s) \neq g(s)\}|$ denote the number of points $s \in S$ on which f and g differ. Equivalently, it denotes the (unnormalized) Hamming distance between the vectors $f(S)$ and $g(S)$.

Given a polynomial $f \in \mathbb{F}[X]$, we let

$$\delta_S(f) := \frac{\min_F \{d_S(f, F) : F \in \mathbb{F}[X], \deg(F) < \rho|S|\}}{|S|} \ .$$

In other words, $\delta_S(f)$ denotes the relative Hamming distance of $f(S)$ to a closest codeword in $\mathrm{RS}[\mathbb{F}, S, \rho]$.

8.2 FRI-Protocol

Let $\mathcal{O}^f$ be an oracle implementing some function $f \colon S \to \mathbb{F}$, which of course uniquely corresponds to a polynomial of degree less than $N = |S|$. We are interested in the situation where a prover claims that $f(X)$ is in fact a polynomial of degree $< \rho N$, i.e., that $f(S) \in \mathrm{RS}[\mathbb{F}, S, \rho]$. In order to verify this, the verifier may make queries to $\mathcal{O}^f$, but it is easy to see that in order to catch a lying prover the verifier must query each $s \in S$ (or at least $\Omega(|S|)$ such points in order to catch the prover with good probability).

Thus, for soundness, we will be satisfied with rejecting oracles implementing functions that are *far* from low degree, i.e., such that $\delta_S(f) \geq \delta$.[8] However, here as well we cannot hope to catch cheating verifiers without making $\Omega(N)$ queries.[9]

[8] If the oracle is implementing a function f for which $\delta_S(f)$ is small, the verifier can typically apply self-correction techniques to the oracle in order to be able to proceed as if f were indeed of low degree.

[9] Assuming $\delta, \rho = \Omega(1)$, as is standard.

It turns out to be possible to make significantly less (i.e., just logarithmically many) oracle queries if we allow the verifier to *interact with* the prover.

The resulting protocols are referred to as *interactive oracle proofs of proximity* (IOPPs). In order to demonstrate the utility of our general special soundness notion, we will show how to analyze a Fast Reed-Solomon Interactive Oracle Proof of Proximity (FRI-protocol) [5].

In order to implement the oracle $\mathcal{O}^f$ cryptographically, one makes use of a compact commitment scheme, typically via a Merkle tree [7].[10] In the following we denote the commitment to the vector $F(S) = (F(s))_{s\in S}$ with public parameters pp by $P \leftarrow \textsc{Com}_{\mathsf{pp}}(F(S))$ and the local opening information for $s \in S$ as γ_s. For example, in the case of a Merkle tree the public parameters pp would be a description of the hash function used, while γ_s would give hash values for the co-path of the leaf corresponding to s. We also assume access to a procedure $\textsc{Loc}_{\mathsf{pp}}$ which takes as input a commitment P, a domain element s, a value $y_s \in \mathbb{F}$ and the opening information γ_s and outputs 1 iff γ_s indeed certifies that P opens to y_s on the element s.

We can therefore view the (cryptographically compiled version of the) FRI-protocol as an interactive proof for the pair of relations $(\mathfrak{R}_0, \mathfrak{R}_\delta \cup \mathfrak{R}_{\mathsf{coll}})$, where for a parameter $\beta \in [0, 1)$ we define

$$\mathfrak{R}_\beta := \big\{(P, \mathsf{pp}; F, A, (\gamma_s)_{s\in A}) : \deg(F) < \rho N \ \wedge\ |A| \geq (1-\beta)N \\ \wedge\ \forall s \in A,\ \textsc{Loc}_{\mathsf{pp}}(P, s, F(s), \gamma_s) = 1\big\},$$

while

$$\mathfrak{R}_{\mathsf{coll}} := \big\{(\mathsf{pp}; s, y, y', \gamma, \gamma') : y \neq y' \ \wedge\ \textsc{Loc}_{\mathsf{pp}}(P, s, y, \gamma) = 1 \\ \wedge\ \textsc{Loc}_{\mathsf{pp}}(P, s, y', \gamma') = 1\big\}.$$

This means that completeness holds with respect to relation $\mathfrak{R}_0$ and soundness holds with respect to $\mathfrak{R}_\delta \cup \mathfrak{R}_{\mathsf{coll}}$, where the latter refers to the "or-relation" which accepts a witness for one or the other instance. On the one hand, this says that a prover that committed to a low-degree polynomial will indeed convince the verifier of this fact. On the other hand, if a prover succeeds in convincing the verifier then we can either extract a commitment to many coordinates that agree with a low-degree polynomial, or we can extract two distinct local openings from the same commitment (invalidating the binding property of the commitment).[11]

Folding. An important ingredient in the FRI-protocol is a folding operation. For our specific choice of S, it is defined as follows: for $f(X) \in \mathbb{F}[X]$ and $c \in \mathbb{F}$, we define

$$\mathrm{Fold}\big(f(X), c\big) = g(X) \in \mathbb{F}[X]$$

[10] More generally, any commitment scheme with local openings would suffice, although the communication costs do of course scale with the size of the commitments.

[11] Observe that this is a concrete instantiation of the idea alluded to in Remark 1: we can either extract a witness to the desired relation, or a solution to a computationally hard problem.

such that

$$g(X^2) = \frac{f(X) + f(-X)}{2} + c\frac{f(X) - f(-X)}{2X} .$$

Intuitively, this folding operation considers the even-power monomials of $f(X)$ and the odd-power monomials separately, obtains from these terms two polynomials of degree $\deg(f)/2$, and takes a random linear combination of these polynomials. Importantly, the polynomial $g(X)$ can then naturally be viewed as having degree roughly $\deg(f)/2$ (i.e., the degree is halved) and its domain is naturally viewed as $S^2 = \langle \omega^2 \rangle$, which has order $N/2$. That is, the folded polynomial has its degree and domain halved.

A one round version of the FRI-protocol thus proceeds as follows. First, the prover commits to $F(S)$, where it promises that $F(S) \in \mathrm{RS}[\mathbb{F}, S, \rho]$. The verifier picks a random challenge $c \in \mathbb{F}$, sends it to the prover, and the prover responds with the folding of F around c. The verifier first checks that $\deg(G) < \rho N/2$. If yes, the verifier then chooses t points $s_1, \ldots, s_t \in S$ such that the sets $\{\pm s_i\}$ are pairwise disjoint, and asks for the evaluations of F on all these points. It then checks that these evaluations are consistent with G, i.e., that $G(s_i^2) = \frac{f(s_i)+f(-s_i)}{2} + c\frac{f(s_i)-f(-s_i)}{2s_i}$ for all $1 \leq i \leq t$, and of course that these are indeed the values the prover committed to initially. This is summarized in Figure 1.

8.3 Analyzing the FRI-Protocol

In order to analyze the FRI-protocol, we must create an extractor that takes as input folding challenges and then openings for various points $s \in S$ that are consistent with the folded polynomials (which are assumed to be low-degree). From two distinct folding challenges $c, c' \in \mathbb{F}$, if $G(X)$ and $G'(X)$ are the folding around c and c' respectively of the function the prover committed to, then we can create the following polynomial:

$$F(X) = X\frac{G(X^2) - G'(X^2)}{c - c'} + \frac{cG'(X^2) - c'G(X^2)}{c - c'} .$$

Note that if G and G' have degree less than $\rho N/2$, then indeed F would have degree less than ρN.

The extractor may also rewind the second phase of the protocol to obtain sets A and A' covering at least $(1 - \delta)$ fraction of S. We can then conclude that we have consistent openings on their intersection $A \cap A'$ (assuming that we do not violate the binding property of the commitment, i.e., that we do not extract a witness for the relation $\mathfrak{R}_{\mathsf{coll}}$). The intersection $A \cap A'$ covers a $(1 - 2\delta)$ fraction of S, so we have found a low-degree polynomial agreeing with the commitment on a $(1 - 2\delta)$ fraction of the points of S.

At this point, we could iterate this argument. However, iterating this argument over μ folding rounds would cause us to only prove that the prover committed to a function that agrees with a low-degree polynomial on a $(1 - 2^\mu\delta)$-fraction of the coordinates (assuming that we did not extract a collision in the commitment). This is quite unsatisfactory, as we would like to have μ logarithmic in N

Protocol 1 FRI-protocol (one folding iteration)

PARAMETERS:	finite field $\mathbb{F}$ with $\lvert\mathbb{F}\rvert = q \in \mathbb{N}$, $r, t \in \mathbb{N}$, $\rho = 2^{-r} \in (0,1]$, primitive 2^r-root of unity $\omega \in \mathbb{F}$, $S := \langle\omega\rangle = \{1, \omega, \ldots, \omega^{2^r-1}\} \subseteq \mathbb{F}$ and $S^2 = \langle\omega^2\rangle$, vector commitment scheme $\textsc{Com}\colon \mathbb{F}^n \to \{0,1\}^*$ with local openings
PUBLIC INPUT:	$P \in \{0,1\}^*$, public parameters pp
PROVER'S PRIVATE INPUT:	$F\colon S \to \mathbb{F}$
PROVER'S CLAIM:	$\textsc{Com}_{\mathsf{pp}}\big(F(S)\big) = P \wedge F(S) \in \mathrm{RS}[\mathbb{F}, S, \rho]$

Prover $\mathcal{P}$		Verifier $\mathcal{V}$
		$c \leftarrow_R \mathbb{F}$
	$\xleftarrow{c}$	
$G(X) \leftarrow \mathrm{Fold}(F, c)$	$\xrightarrow{G(X)}$	
		For $1 \le i \le t$: $s_i \leftarrow_R S \setminus \{\pm s_1, \ldots, \pm s_{i-1}\}$
	$\xleftarrow{s_1, \ldots, s_t}$	
$F_i^+ = F(s_i)$, $F_i^- = F(-s_i)$ with local opening info γ_i^+, γ_i^-		
	$\xrightarrow{F_1^+, F_1^-, \ldots, F_t^+, F_t^-}$	
		For $1 \le i \le t$: $G(s_i^2) \stackrel{?}{=} \frac{F_i^+ + F_i^-}{2} + c\frac{F_i^+ - F_i^-}{2s_i}$
		$\textsc{Loc}_{\mathsf{pp}}(P, s_i, F_i^+, \gamma_i^+) \stackrel{?}{=} 1$ $\textsc{Loc}_{\mathsf{pp}}(P, -s_i, F_i^-, \gamma_i^-) \stackrel{?}{=} 1$
		Check that $\deg(G) < \rho N/2$

and $\delta \in (0,1)$ a constant. Fortunately, by relying on ideas from prior works (specifically, [5]) we can show that we can indeed extract a low-degree polynomial agreeing with the commitment on a $(1-\delta)$ fraction of coordinates (or, of course, a violation to the binding property of the commitment).

In order to analyze the soundness of the FRI-protocol more effectively, we will need the following *coset-distance* from f to $\mathrm{RS}[\mathbb{F}, S, \rho]$:

$$\Delta_S(f) := \min_{F \in \mathbb{F}[X],\ \deg(F) < \rho N} \frac{\lvert\{s \in S : f(s) \neq F(s) \vee f(-s) \neq F(-s)\}\rvert}{N} .$$

This distance notion has been used in prior works [5]. Observe that $\Delta_S(f) \ge \delta_S(f)$. Intuitively, this measure is useful because it allows for a careful accounting of how the Hamming metric behaves under the folding operation than the above

naïve analysis. For this reason, our extractor will succeed assuming a bound on $\Delta_S(f)$ rather than just $\delta_S(f)$.

The following lemma quantifies this intuition, by characterizing the set of challenges c that could cause the Hamming metric to decrease when a function f is folded around c. These ideas are implicit in [5, Lemma 4.4]; we restate and prove them in a language that is convenient for us.

Lemma 8. *Let $f(X) \in \mathbb{F}[X]$ be such that $\Delta_S(f) < (1-\rho)/2$. The number of choices for $c \in \mathbb{F}$ such that $\delta_{S^2}\big(\mathrm{Fold}(f,c)\big) < \Delta_S(f)$ is at most N.*

In particular, if there exist pairwise distinct $c_0, \ldots, c_N \in \mathbb{F}$ such that $\delta_{S^2}\big(\mathrm{Fold}(f,c)\big) \le \delta$ for all $i \in \{0,1,\ldots,N\}$, then $\Delta_S(f) \le \delta$.

Proof. Let $F(X) \in \mathbb{F}[X]$ be a polynomial of degree $< \rho N$ such that $\delta_S(f) = d_S(f(S), F(S))/|S|$, i.e., $F(S)$ denotes the unique closest codeword to $f(S)$ (where the uniqueness is due to the assumption $\Delta_S(f) < (1-\rho)/2$). Let $c \in \mathbb{F}$, set $g(X) := \mathrm{Fold}(f(X), c)$, and let $G(X) \in \mathbb{F}[X]$ be a polynomial of degree $< \rho N/2$ such that $G(S^2)$ is a codeword in $\mathrm{RS}[\mathbb{F}, S^2, \rho]$ closest to g. Since $\delta_S(f) \le \Delta_S(f) < (1-\rho)/2$,

$$G = \mathrm{Fold}(F, c)\,,$$

i.e., in this case folding and taking the closest codeword commute. Hence, $\delta_{S^2}(g) = d\big(g(S^2), G(S^2)\big)/\left|S^2\right|$.

Let

$$A := \{s \in S^2 : g(s) \neq G(s)\}$$

and

$$B := \{s \in S : f(s) \neq F(s) \vee f(-s) \neq F(-s)\}\,.$$

Then, $A \subseteq \{s^2 : s \in B \subseteq S\}$. Hence, using that $s \in B$ if and only if $-s \in B$, $|A| \le |B|/2$.

As $\delta_{S^2}(g) < \Delta_S(f)$, we have $|A| < \frac{|B|}{2}$. Hence there exists an $s \in B$ with $s^2 \notin A$. By the definition of A and B, it follows that:

(1) $f(s) \neq F(s)$ or $f(-s) \neq F(-s)$;
(2) $g(s^2) = G(s^2)$.

The second equation can be rewritten as follows:

$$\frac{f(s)+f(-s)}{2} + c\frac{f(s)-f(-s)}{2s} = \frac{F(s)+F(-s)}{2} + c\frac{F(s)-F(-s)}{2s}$$
$$\iff$$
$$s\big(f(s)+f(-s)-F(s)-F(-s)\big) = c\big(F(s)-F(-s)-f(s)+f(-s)\big)\,.$$

This is a linear equation in c. By item (1) it is nontrivial and thus has at most one solution.

We conclude that

$$c \in \left\{s\frac{F(s)+F(-s)-f(s)-f(-s)}{f(s)-f(-s)-F(s)+F(-s)} : s \in S\right\} \setminus \{\infty\}\,,$$

and as this set has size at most $|S| = N$ the claim follows. □

We now precisely define the notion of special-soundness that we will prove the FRI-protocol with one folding iteration (i.e., the protocol from Figure 1) satisfies. Informally, for the folding round the previous lemma tells us we need $N+1$ challenges to extract, while for the second round we need enough local openings of the commitment to reveal a $(1-\delta)$-fraction of the values that the prover committed to. We now make this formal.

Let

$$\mathcal{C} := \left\{ \{\pm s_1, \pm s_2, \ldots, \pm s_t\} : s_i^2 \in S^2 \ \forall i,\ s_i^2 \neq s_j^2 \ \forall i \neq j \right\} .$$

Let $(\Gamma_{N+1}, \mathbb{F})$ be the monotone structure that contains all subsets of $\mathbb{F}$ of cardinality at least $N+1$, and let $(\Gamma, \mathcal{C})$ be the monotone structure that contains all subsets of $\mathcal{C}$ that cover at least a $(1-\delta)$-fraction of S, i.e.,

$$A \in \Gamma \subset 2^{\mathcal{C}} \quad \iff \quad \left| \bigcup_{B \in A} B \right| \geq (1-\delta)N .$$

Theorem 4 (FRI-protocol (one folding iteration)). *Let $\rho = 2^{-r}$ for some $r \in \{0, 1, \ldots, m\}$ and let $\delta \in (0,1)$ be such that $\delta < \frac{1-\rho}{4}$. Protocol 1 is perfectly complete with respect to relation $\mathfrak{R}_0$ and (Γ_{N+1}, Γ)-out-of-$(\mathbb{F}, \mathcal{C})$ special-sound with respect to relation $\mathfrak{R}_\delta \cup \mathfrak{R}_{\mathsf{coll}}$.*

Proof. **Completeness:** This is immediate from prior work (e.g., [5]). To make our proof self-contained, we note that this follows immediately from the following facts concerning a polynomial $F(X) \in \mathbb{F}[X]$:

- if F has degree $< \rho N$ then $\mathrm{Fold}(F, c)$ has degree $< \rho N/2$ for any $c \in \mathbb{F}$; and
- for any $s \in S$ and $c \in \mathbb{F}$, $\mathrm{Fold}(F, c)(s^2) = \frac{F(s)+F(-s)}{2} + c\frac{F(s)-F(-s)}{2s}$.

Soundness: We must extract a witness for either the relation $\mathfrak{R}_\delta$ or the relation $\mathfrak{R}_{\mathsf{coll}}$ given a (Γ_{N+1}, Γ)-tree of accepting transcripts. Such a tree of transcripts consists of the following:

- folding challenges $c_0, \ldots, c_N \in \mathbb{F}$,
- polynomials $G_0, \ldots, G_N \in \mathbb{F}[X]$ of degree less than $\rho\frac{N}{2}$,
- subsets $A_0, \ldots, A_N \subseteq S$, each of size at least $(1-\delta)N$, which are closed under negation (i.e., $s \in A_j \iff -s \in A_j$), and
- for each $0 \leq j \leq N$, for each $s \in A_j$, opening information γ_{sj} for the element s. Let $y_{sj} \in \mathbb{F}$ be the element for which $\mathrm{Loc}_{\mathsf{pp}}(P, s, y_{sj}, \gamma_{sj}) = 1$.

Suppose there exists $j \neq j'$ such that, for some $s \in A_j \cap Aj'$, $y_{sj} \neq y_{sj'}$. Then, we may output the following witness for the relation $\mathfrak{R}_{\mathsf{coll}}$: $(s, y_{sj}, y_{sj'}, \gamma_{sj}, \gamma'_{sj})$.

We may now assume that the above does not occur. In other words, for each $s \in \bar{A} := A_0 \cup \ldots \cup A_N$ the set $\{y_{sj} : s \in A_j\}$ is in fact a singleton set; denote its unique element by y_s. We also let $\gamma_s := \gamma_{sj}$ where j is the smallest element in $\{0, 1, \ldots, N\}$ such that $s \in A_j$ (this is just an arbitrary tie-breaking rule).

For each $j \in \{0, 1, \ldots, N\}$, the polynomial G_j and the elements y_s for $s \in A_j$ satisfy the following relation:

$$G_j(s^2) = \frac{y_s + y_{-s}}{2} + c_j \frac{y_s - y_{-s}}{2s} \ .$$

Let $f(X) \in \mathbb{F}[X]$ be a polynomial consistent with the y_s's, i.e., for all $s \in A$ we have $f(s) = y_s$. Furthermore, for reasons to be clear later, we let f be different to the polynomial F_0 defined below outside of $\bar{A}$, i.e. $f(s) \neq F_0(s)$ for all $s \notin \bar{A}$. Then, for each $j \in \{0, 1, \ldots, N\}$ and all s^2 such that $\{\pm s\} \subseteq A_j$, we have

$$G_j(s^2) = \mathrm{Fold}\left(f, c_j\right)(s^2) \ .$$

We conclude that $\mathrm{Fold}\left(f, c_j\right)$ and G_j agree on at least $(1-\delta)\frac{N}{2}$ elements of S^2. As $\deg(G_j) < \rho\frac{N}{2}$ it follows that

$$\delta_{S^2}\left(\mathrm{Fold}\left(f, c_j\right)\right) \leq \delta \, .$$

By Lemma 8, if we establish that $\Delta_S(f) < \frac{1-\rho}{2}$, it in fact then follows that $\Delta_S(f) \leq \delta$, which in turn implies $\delta_S(f) \leq \delta$. As $2\delta < \frac{1-\rho}{2}$ by assumption, it suffices for us to show $\Delta_S(f) \leq 2\delta$. We focus on proving this now.

Consider the polynomial

$$F_0(X) := X\frac{G_0(X^2) - G_1(X^2)}{c_0 - c_1} + \frac{c_0 G_1(X^2) - c_1 G_0(X^2)}{c_0 - c_1} \ .$$

Since the degrees of G_0 and G_1 are smaller than $\rho\frac{N}{2}$, it follows that $\deg(F_0) < \rho N$. Furthermore, we note that for all $s \in A_0 \cap A_1$ we have $f(s) = F_0(s)$. Indeed,

$$\begin{aligned}
F_0(s) &= s \cdot \frac{G_0(s^2) - G_1(s^2)}{c_0 - c_1} + \frac{c_0 G_1(s^2) - c_1 G_0(s^2)}{c_0 - c_1} \\
&= \frac{s}{c_0 - c_1}\left[\frac{f(s) + f(-s)}{2} + c_0\frac{f(s) - f(-s)}{2s}\right. \\
&\qquad \left. - \left(\frac{f(s) + f(-s)}{2} + c_1\frac{f(s) - f(-s)}{2s}\right)\right] \\
&\quad + \frac{1}{c_0 - c_1}\left[c_0 \cdot \left(\frac{f(s) - f(-s)}{2} + c_1\frac{f(s) - f(-s)}{2s}\right)\right. \\
&\qquad \left. - c_1 \cdot \left(\frac{f(s) + f(-s)}{2} + c_0\frac{f(s) - f(-s)}{2s}\right)\right] \\
&= \frac{s}{c_0 - c_1} \cdot (c_0 - c_1)\frac{f(s) - f(-s)}{2s} + \frac{1}{c_0 - c_1} \cdot (c_0 - c_1)\frac{f(s) + f(-s)}{2} \\
&= \frac{f(s) - f(-s)}{2} + \frac{f(s) + f(-s)}{2} = f(s) \ .
\end{aligned}$$

From this, we can conclude that f and F_0 agree on at least $(1 - 2\delta)N/2$ pairs $\{\pm s\}$: here, we use the fact that as A_0 and A_1 are closed under negation, so is

$A_0 \cap A_1$. Thus, the number of $s \in S$ for which $f(s) \neq F_0(s)$ or $f(-s) \neq F_0(-s)$ is at most $2\delta N$. Recalling $\deg(F_0) < \rho N$, we conclude $\Delta_S(f) \leq 2\delta$, as desired.

Thus, we have found that $\Delta_S(f) \leq \delta$, which in particular means $\delta_S(f) \leq \delta$, as desired. Let $F(X)$ denote the (necessarily unique) polynomial of degree $< \rho N$ such that $d_S(F(S), f(S)) \leq \delta N$. As $d_S(F_0(S), f(S)) \leq 2\delta N$ it also follows that $d_S(F_0(S), F(S)) \leq 3\delta N < 1 - \rho$. As $F_0(S), F(S) \in \mathrm{RS}[\mathbb{F}, S, \rho]$ and this code has minimum distance $1 - \rho$, it must be that $F_0(S) = F(S)$, which further implies $F_0(X) = F(X)$ (as polynomials).

We can therefore extract a polynomial of degree $< \rho N$ that agrees with the function $f(X)$ on a $(1 - \delta)$ fraction of coordinates: namely, the polynomial $F_0(X)$. Furthermore, since f differs from F_0 outside of $\bar{A} = A_0 \cup \ldots \cup A_N$ (by the choice of f), we can find a subset $A \subseteq \bar{A}$ of size at least $(1 - \delta)N$ for which $f(s) = F_0(s)$ for all $s \in A$. We may therefore output the following witness for $\mathfrak{R}_\delta$: $(F_0(X), A, (\gamma_s)_{s \in A})$.

□

We are now in position to apply the machinery developed in Section 6 to conclude the following bound on the knowledge error.

Corollary 1 (Knowledge Error of FRI-protocol (one folding iteration)). *Let $\rho = 2^{-r}$ for some $r \in \{0, 1, \ldots, m\}$ and let $\delta \in (0, 1)$ be such that $\delta < \frac{1-\rho}{4}$. Protocol 1 is knowledge sound with respect to relation $\mathfrak{R}_\delta \cup \mathfrak{R}_{\mathsf{coll}}$ with knowledge error*

$$\begin{aligned}
\kappa &:= 1 - \left(1 - \frac{N}{|\mathbb{F}|}\right)\left(1 - \frac{\binom{\lceil (1-\delta)\frac{N}{2} \rceil - 1}{t}}{\binom{\frac{N}{2}}{t}}\right) \\
&\leq 1 - \left(1 - \frac{N}{|\mathbb{F}|}\right)\left(1 - (1-\delta)^t\right) \\
&\leq \frac{N}{|\mathbb{F}|} + (1-\delta)^t \ .
\end{aligned}$$

Proof. By Theorem 2, as Theorem 4 shows that Protocol 1 is (Γ_{N+1}, Γ)-out-of-$(\mathbb{F}, \mathcal{C})$ special-sound, it suffices to note that $\max_{S \notin \Gamma_{N+1}} \frac{|S|}{|\mathbb{F}|} = \frac{N}{|\mathbb{F}|}$ while

$$\max_{A \notin \Gamma} \frac{|A|}{|\mathcal{C}|} = \frac{\binom{\lceil (1-\delta)\frac{N}{2} \rceil - 1}{t}}{\binom{\frac{N}{2}}{t}} \leq (1-\delta)^t \ .$$

To see the equality, note that if $A \notin \Gamma$ then $\bigcup_{B \in A} B$ has cardinality less than $(1-\delta)N$, so A (which consists of pairs $\{\pm s\}$) has cardinality less than $(1-\delta)N/2$, and thus at most $\lceil (1-\delta)\frac{N}{2} \rceil - 1$. Similarly, one can observe that $\mathcal{C}$ is in bijection with subsets of S^2 of size t, of which there are $\binom{N/2}{t}$. □

8.4 Additional Folding Iterations

The above analysis can naturally be extended to handle more folding iterations. Let $F_0 := F$ be the low degree polynomial the prover commits to in the first

round. We have folding rounds $i = 1, \ldots, \mu$, and in round i the verifier sends a challenge $c_{i-1} \in \mathbb{F}$ and the prover provides a commitment to $F_i(S^{2^i})$ where $F_i(X) = \mathrm{Fold}(F_{i-1}, c_{i-1})(X)$. After these folding iterations, the verifier picks t pairs of points $\{\pm s_1, \ldots, \pm s_t\} \subseteq S$ such that $s_j^2 \neq s_{j'}^2$ for all $j \neq j'$ and then checks that for all $i = 1, \ldots, \mu$ and $j = 1, \ldots, t$, we have

$$F_i\big(s_j^{2^i}\big) = \frac{F_{i-1}\big(s_j^{2^{i-1}}\big) + F_{i-1}\big(-s_j^{2^{i-1}}\big)}{2} + c_{i-1}\frac{F_{i-1}\big(s_j^{2^{i-1}}\big) - F_{i-1}\big(-s_j^{2^{i-1}}\big)}{2s_j} \ .$$

The recursive structure of the extractor implies that after μ folding iterations we obtain a protocol with the following generalized special-soundness guarantee.

Theorem 5 (FRI-protocol (μ folding iterations).). *Let $\rho = 2^{-r}$ for some $r \in \{0, 1, \ldots, m\}$ and let $\delta \in (0, 1)$ be such that $\delta < \frac{1-\rho}{4}$. Let $\mu \in \mathbb{N}$ be such that $\mu \leq \log_2 N$, and for $i = 1, 2, \ldots, \mu$ let $N_i := N/2^{i-1}$. The FRI-protocol with μ folding iterations is perfectly complete with respect to relation $\mathfrak{R}_0$ and $(\Gamma_{N_1+1}, \Gamma_{N_2+1}, \ldots, \Gamma_{N_\mu+1}, \Gamma)$-out-of-$(\mathbb{F}, \mathbb{F}, \ldots, \mathbb{F}, \mathcal{C})$ special-sound with respect to relation $\mathfrak{R}_\delta \cup \mathfrak{R}_{\mathsf{coll}}$.*

This yields the following corollary regarding the knowledge error.

Corollary 2 (Knowledge Error of FRI-protocol (μ folding iterations)). *Let $\rho = 2^{-r}$ for some $r \in \{0, 1, \ldots, m\}$ and let $\delta \in (0, 1)$ be such that $\delta < \frac{1-\rho}{4}$. Let $\mu \in \mathbb{N}$ be such that $\mu \leq \log_2 N$, and for $i = 1, 2, \ldots, \mu$ let $N_i := N/2^{i-1}$. The FRI-protocol with μ foloding iterations is knowledge sound with respect to relation $\mathfrak{R}_\delta \cup \mathfrak{R}_{\mathsf{coll}}$ with knowledge error*

$$\begin{aligned}
\kappa &:= 1 - \left(\prod_{i=1}^{\mu}\left(1 - \frac{N_i}{|\mathbb{F}|}\right)\right) \cdot \left(1 - \frac{\binom{\lceil (1-\delta)\frac{N}{2} \rceil - 1}{t}}{\binom{\frac{N}{2}}{t}}\right) \\
&\leq 1 - \left(\prod_{i=1}^{\mu}\left(1 - \frac{N_i}{|\mathbb{F}|}\right)\right)\left(1 - (1-\delta)^t\right) \\
&\leq \sum_{i=1}^{\mu}\frac{N_i}{|\mathbb{F}|} + (1-\delta)^t \leq \frac{2N}{|\mathbb{F}|} + (1-\delta)^t \ .
\end{aligned}$$

8.5 Open Directions

Our argument, which implies knowledge soundness, is only for certain ranges of proximity parameter δ and relative rate ρ: we require $\delta < \frac{1-\rho}{4}$. However, one can hope for knowledge soundness for larger values of δ, perhaps even for δ as large as $1 - \rho$, the minimum distance of a Reed-Solomon code of rate ρ. A sequence of works [9, 8, 6] has now successfully proved (normal) soudness for the FRI-protocol for δ as large as $1 - \sqrt{\rho}$ (which is a well-known as the Johnson bound in the coding-theoretic literature). A natural direction which we leave open for future work is to improve our analysis in order to obtain knowledge soundness for larger values of δ.

Acknowledgments

The first author has been supported by TNO's Early Research Program - Next Generation Cryptography.

References

1. Attema, T., Cramer, R., Kohl, L.: A compressed Σ-protocol theory for lattices. In: Malkin, T., Peikert, C. (eds.) CRYPTO. Lecture Notes in Computer Science, vol. 12826, pp. 549–579. Springer (2021), https://doi.org/10.1007/978-3-030-84245-1_19
2. Attema, T., Fehr, S.: Parallel repetition of $(k_1, \ldots, k_\mu)$-special-sound multi-round interactive proofs. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO. Lecture Notes in Computer Science, vol. 13507, pp. 415–443. Springer (2022), https://doi.org/10.1007/978-3-031-15802-5_15
3. Attema, T., Fehr, S., Klooß, M.: Fiat-shamir transformation of multi-round interactive proofs. In: Kiltz, E., Vaikuntanathan, V. (eds.) Theory of Cryptography Conference (TCC). Lecture Notes in Computer Science, vol. 13747, pp. 113–142. Springer (2022), https://doi.org/10.1007/978-3-031-22318-1_5
4. Bellare, M., Impagliazzo, R., Naor, M.: Does parallel repetition lower the error in computationally sound protocols? In: IEEE Symposium on Foundations of Computer Science (FOCS). pp. 374–383. IEEE Computer Society (1997), https://doi.org/10.1109/SFCS.1997.646126
5. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Fast reed-solomon interactive oracle proofs of proximity. In: Chatzigiannakis, I., Kaklamanis, C., Marx, D., Sannella, D. (eds.) 45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic. LIPIcs, vol. 107, pp. 14:1–14:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2018), https://doi.org/10.4230/LIPIcs.ICALP.2018.14
6. Ben-Sasson, E., Carmon, D., Ishai, Y., Kopparty, S., Saraf, S.: Proximity gaps for reed-solomon codes. In: Irani, S. (ed.) 61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020. pp. 900–909. IEEE (2020), https://doi.org/10.1109/FOCS46700.2020.00088
7. Ben-Sasson, E., Chiesa, A., Spooner, N.: Interactive oracle proofs. In: Hirt, M., Smith, A.D. (eds.) Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9986, pp. 31–60 (2016), https://doi.org/10.1007/978-3-662-53644-5_2
8. Ben-Sasson, E., Goldberg, L., Kopparty, S., Saraf, S.: DEEP-FRI: sampling outside the box improves soundness. In: Vidick, T. (ed.) 11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA. LIPIcs, vol. 151, pp. 5:1–5:32. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2020), https://doi.org/10.4230/LIPIcs.ITCS.2020.5
9. Ben-Sasson, E., Kopparty, S., Saraf, S.: Worst-case to average case reductions for the distance to a code. In: Servedio, R.A. (ed.) 33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA. LIPIcs, vol. 102, pp. 24:1–24:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2018), https://doi.org/10.4230/LIPIcs.CCC.2018.24

10. Bootle, J., Cerulli, A., Chaidos, P., Groth, J., Petit, C.: Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In: Fischlin, M., Coron, J. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 9666, pp. 327–357. Springer (2016), https://doi.org/10.1007/978-3-662-49896-5_12
11. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: Short proofs for confidential transactions and more. In: IEEE Symposium on Security and Privacy (S&P). pp. 315–334. IEEE Computer Society (2018), https://doi.org/10.1109/SP.2018.00020
12. Dao, Q., Grubbs, P.: Spartan and bulletproofs are simulation-extractable (for free!). In: Hazay, C., Stam, M. (eds.) Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part II. Lecture Notes in Computer Science, vol. 14005, pp. 531–562. Springer (2023), https://doi.org/10.1007/978-3-031-30617-4_18
13. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Efficient nizks and signatures from commit-and-open protocols in the QROM. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13508, pp. 729–757. Springer (2022), https://doi.org/10.1007/978-3-031-15979-4_25
14. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Online-extractability in the quantum random-oracle model. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13277, pp. 677–706. Springer (2022), https://doi.org/10.1007/978-3-031-07082-2_24
15. Kilian, J.: A note on efficient zero-knowledge proofs and arguments (extended abstract). In: Kosaraju, S.R., Fellows, M., Wigderson, A., Ellis, J.A. (eds.) ACM Symposium on Theory of Computing (STOC). pp. 723–732. ACM (1992), https://doi.org/10.1145/129712.129782
16. Micali, S.: CS proofs (extended abstracts). In: 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994. pp. 436–453. IEEE Computer Society (1994), https://doi.org/10.1109/SFCS.1994.365746
17. Micali, S.: Computationally sound proofs. SIAM J. Comput. 30(4), 1253–1298 (2000), https://doi.org/10.1137/S0097539795284959
18. Wikström, D.: Special soundness revisited. IACR Cryptology ePrint Archive (2018), https://eprint.iacr.org/2018/1157
19. Wikström, D.: Special soundness in the random oracle model. IACR Cryptology ePrint Archive (2021), https://eprint.iacr.org/2021/1265