Private Information Retrieval: Share Conversions vs. Decoding Polynomials

Amos Beimel[2] and Or Lasri[2]
amos.beimel@gmail.com, orshlomo@post.bgu.ac.il

Faculty of Computer and Information Science, Ben Gurion University, Beer Sheva, Israel

Abstract. A private information retrieval (PIR) protocol enables a client to retrieve a bit from an N bit database replicated among k servers in such a way that each server learns no information about the retrieved bit. Modern PIR protocols with information-theoretic privacy (Efremenko, SICOMP, 2012; Dvir and Gopi, STOC, 2015; Ghasemi et al., STOC, 25) are based on matching vectors over a composite number m. To construct a PIR protocol from the matching vectors, these protocols use a decoding polynomial, a sparse polynomial that returns a non-zero value on 1 and returns zero on a certain set implied by the matching vectors.

Beimel et al. (CCC, 2012) abstracted the properties required by the transformation computed by the decoding polynomial, defining the notion of share conversion. In such a conversion, a set of parties is given shares of a secret in one secret-sharing scheme, and each party locally computes a new share (without any communication) such that the new shares are shares in a second secret-sharing scheme of a related secret. Beimel et al. showed that share conversion can replace the decoding polynomial in the PIR protocol of Efremenko and constructed a share conversion from the ring $\mathbb{Z}_6$ to the field $\mathbb{F}_{2^2}$. This share conversion cannot be computed by a decoding polynomial, as decoding polynomials convert shares from a ring $\mathbb{Z}_m$ to a finite field of characteristic p such that p does not divide m. Alon et al. (TCC, 2025) simplified and generalized the PIR protocols of Dvir and Gopi and Ghasemi et al., using share conversion; however, in this protocol, the share conversion is from a ring $\mathbb{Z}_m$ to a finite field of characteristic p such that p does not divide m.

In this paper, we study the power of share conversions. Our main result proves that if there is a k-party share conversion from a ring $\mathbb{Z}_m$ to a finite field of characteristic p such that p does not divide m, then there is a k sparse decoding polynomial from a ring $\mathbb{Z}_m$ to a finite field of characteristic p. This result implies that using share conversion in the protocol of Alon et al. can only improve the communication complexity by a constant factor. In addition, we show that if there is a k-party share conversion from a ring $\mathbb{Z}_m$ to a finite field, where m is a product of r distinct primes, then $k \geq r+1$, i.e., the number of servers in the resulting PIR protocols using the appropriate matching vectors is at least $r+1$. A similar result was recently proved by Ghasemi and Kopparty (ITCS 26); our lower bound also applies to the case in which the characteristic of the field divides m.

1 Introduction

Protecting the privacy of database queries from the database owner is important, as such queries can disclose, for example, political views, medical conditions, business intentions, personal interests, or research directions. Chor, Goldreich, Kushilevitz, and Sudan [10] presented a simple yet challenging version of this problem, called private information retrieval (PIR) protocols; in a PIR protocol, the database is modeled as an N-bit string $D = (D_1, D_2, \ldots, D_N)$, and a client wants to retrieve D_i without disclosing any information about i. Chor et al. showed that if a single database is used and the privacy is information theoretic (as considered in this paper), then N bits must be communicated; thus, they suggested that the client communicates with $k \geq 2$ servers, where each server holds a copy of the database and should learn no information about i. In the known PIR protocols, there is one message from the client to each server, called the query, and one message from each server to the client, called the answer. The communication complexity of k-server PIR protocols has been improved in the last three decades, resulting in the following protocols for 2 and 3 servers (these protocols can be generalized to more efficient protocols for $k > 3$ servers):

- A 3-server PIR protocol by Efremenko [13] with queries of length $2^{\tilde{O}\left(\sqrt{\log N}\right)}$ and answers of length $O(1)$; this protocol implies efficient locally decodable codes.
- A 2-server PIR protocol by Dvir and Gopi [12] with queries and answers of length $2^{\tilde{O}\left(\sqrt{\log N}\right)}$.
- A recent 3-server PIR protocol by Ghasemi, Kopparty, and Sudan [16] with queries and answers of length $2^{\tilde{O}\left(\sqrt[3]{\log N}\right)}$.

A simplified version of the PIR protocols of [12,16] was given in [1]. PIR protocols are closely related to information-theoretic secure multiparty computation protocols [18,4] and locally decodable codes [24].

The above PIR protocols of [13,12,16] use matching vectors over $\mathbb{Z}_m$,[1] where m is a composite number, and the communication complexity of the protocols is the length of the vectors. To use the matching vectors in PIR protocols, Efremenko [13] and follow-up works use decoding polynomials; specifically, Efremenko proved that if there is a k-sparse decoding polynomial, then there is a k-server PIR protocol that uses matching vectors over $\mathbb{Z}_m$, where m is a product of a small number of primes. Beimel, Ishai, Kushilevitz, and Orlov [6] generalized the notion of decoding polynomials by introducing share conversions from a ring to a field; they showed that a k-party share conversion implies a k-server PIR protocol. In the same work, they observed that decoding polynomials imply share conversions, and they presented several existential results on share conversions from $\mathbb{Z}_m$ to $\mathbb{F}_{p^\ell}$, e.g., a share conversion from $\mathbb{Z}_6$ to $\mathbb{F}_{2^2}$. Paskin-Cherniavsky and Schmerler [27] proved that for every $m = p_1 \cdot p_2$, where p_1, p_2

[1] The definitions of matching vectors and other notions mentioned in this paragraph appear in Section 1.1.

are distinct odd primes, there is a share conversion from $\mathbb{Z}_m$ to a finite field of characteristic p_1. As decoding polynomials define a share conversion from $\mathbb{Z}_m$ to a field of characteristic p, where p does not divide m, this shows that share conversion is a strict generalization of decoding polynomials. Alon, Beimel, and Lasri [1] generalized (and simplified) the scheme of [16], showing that it can be described using share conversion; however, in this case, the share conversion is from $\mathbb{Z}_m$ to a field of characteristic p, where p *does not* divide m. Alon et al. asked if this generalization can lead to improved PIR protocols. In this work, we address this question by studying the power of share conversions compared to decoding polynomials and providing lower bounds on the number of parties in share conversion. Our main result is that when p does not divide m, share conversion implies decoding polynomials; hence, the generalization of Alon et al. cannot improve the communication complexity of PIR protocols.

1.1 Technical Background

Before we present our results, we provide a few technical details and definitions, as our results are mostly technical. Cramer, Damgård, and Ishai [11] defined share conversion from a secret-sharing scheme with a domain of secrets S to a different secret-sharing scheme with the same domain S; this is a process in which each party applies a local transformation to its share in the first scheme (without any communication) so that the converted shares are shares in the second scheme for the same secret. They showed that the t-private CNF secret-sharing scheme[2] over a field can be locally converted to any *linear* t-private secret-sharing scheme. This motivated Beimel et al. [6] to use CNF secret-sharing schemes in PIR protocols (rather than a modification of Shamir's secret-sharing scheme as in [13]). We next describe the 1-private CNF secret-sharing scheme (which we will simply call CNF sharing).

Construction 1.1 (k-Party CNF Sharing over $\mathbb{Z}_m$ (for $m \in \mathbb{N}$)). To share a secret $s \in \mathbb{Z}_m$, the dealer chooses $r_1, \ldots, r_{k-1} \in \mathbb{Z}_m$ uniformly at random, computes $r_k = s - \sum_{j=1}^{k-1} r_j \bmod m$, and gives the i-th party all the random elements except for r_i; that is, the i-th share is $\mathsf{sh}_i = (r_j)_{j \neq i}$.

Beimel et al. [6] generalized the notion of share conversion to schemes with different domains of secrets, such that the secret in the first scheme and the secret in the second scheme satisfy some relation. The following share conversion from CNF sharing to additive sharing is the one used in PIR protocols.

Definition (k-Party S-Share Conversion from $\mathbb{Z}_m$ to a Field $\mathbb{F}$)**.** *For a set $S \subseteq \mathbb{Z}_m \setminus \{1\}$, a k-party S-share conversion is defined by k functions $C_1, \ldots, C_k : \mathbb{Z}_m^{k-1} \to \mathbb{F}$, such that for every secret $s \in \mathbb{Z}_m$ and for every CNF shares $(\mathsf{sh}_i)_{i=1}^k$ of the secret s:*

- *If $s \in S$, then $\sum_{i=1}^k C_i(\mathsf{sh}_i) = 0$,*

[2] A secret-sharing scheme is t-private if any t parties do not gain any information about the secret from their shares.

– *If* $s = 1$, *then* $\sum_{i=1}^{k} C_i(\mathsf{sh}_i) \neq 0$.[3]

There are no requirements for shares of a secret $s \notin S \cup \{1\}$.

Share conversion can be defined for a general 1-private linear secret-sharing scheme instead of CNF. Beimel et al. [6] (generalizing [11]) show that CNF sharing over commutative rings is complete for share conversion. That is, if there exists an S-share conversion from any 1-private linear secret-sharing scheme over $\mathbb{Z}_m$ to $\mathbb{F}$, then there is an S-share conversion from CNF sharing over $\mathbb{Z}_m$ to $\mathbb{F}$. Thus, to study S-share conversion, it suffices to study S-share conversion from CNF sharing.

Efremenko [13] introduced S-decoding polynomials to construct locally decodable codes and PIR protocols.

Definition (S-Decoding Polynomials)**.** *Let* $\mathbb{F}$ *be a finite field with characteristic* p *and* m *be an integer such that* $\mathbb{F}$ *contains an element* $\gamma \in \mathbb{F}$ *of order* m *(such a finite extension field of* $\mathbb{F}_p$ *exists if and only if* $p \nmid m$*). For a set* $S \subseteq \mathbb{Z}_m \setminus \{1\}$*, a* k*-sparse* S*-decoding polynomial is a polynomial* $P(X)$ *with at most* k *monomials such that*

– $P(\gamma^s) = 0$ *for every* $s \in S$,
– $P(\gamma) \neq 0$.

Efremenko observed that for every S there is a $|S| + 1$-sparse S-decoding polynomial $P(X) = \prod_{s \in S} (X - \gamma^s)$. Furthermore, for the specific set S of size 3 used in the 3-server PIR protocol (arising from the construction of matching vectors), Efremenko showed a 3-sparse decoding polynomial.

As mentioned, the main motivation for the study of share conversion and decoding polynomials is the construction of PIR protocols from matching vectors. For completeness, we define matching vectors.

Definition (S-Matching Vectors)**.** *For a set* $S \subseteq \mathbb{Z}_m \setminus \{1\}$*, an* S*-matching vectors family is a collection of vectors* $((\mathbf{u}_i, \mathbf{v}_i))_{i=1}^{N}$ *over* $\mathbb{Z}_m^h$ *such that:*

– $\langle \mathbf{u}_i, \mathbf{v}_i \rangle \bmod m = 1$ *for every* $i \in [N]$,
– $\langle \mathbf{u}_i, \mathbf{v}_j \rangle \bmod m \in S$ *for every* $i \neq j \in [N]$.

The best known PIR protocols [13,12,16,1] use S-matching vectors of Grolmusz [17] for the canonical set in $\mathbb{Z}_m$, where $m = p_1 \cdot \ldots \cdot p_r$ is a product of r distinct primes, defined as

$$S_{\mathrm{can},m} = \{x \in \mathbb{Z}_m : \forall i \in \{1, \ldots, r\} : x \bmod p_i \in \{0, 1\}\} \setminus \{1\}\,.$$

For example, $S_{\mathrm{can},6} = \{0, 3, 4\}$. The length of the matching vectors over $\mathbb{Z}_m$ of Grolmusz [17] is $2^{\tilde{O}(\sqrt[r]{\log N})}$, where m is a product of r distinct primes. Thus, the

[3] In [6], the requirement is that shares of $s = 0$ are converted to shares of a non-zero secret. Following the simplification of the PIR protocol in [1], we require it for $s = 1$. The same modification is applied to decoding polynomials. The results of the paper are not affected by this modification.

work in [13,21,22,9,6,27,26] towards constructing better S-decoding polynomials and share conversion was done for the set $S_{\text{can},m}$, where m is a product of r distinct primes.

A recent paper by Ghasemi and Kopparty [15] provided a new approach for better understanding decoding polynomials by studying the Fourier transform of functions $f : \prod_{i=1}^{r} \mathbb{Z}_{p_i} \to \mathbb{F}$ that satisfy constraints on the Boolean hypercube $\prod_{i=1}^{r} \{0,1\} \subseteq \prod_{i=1}^{r} \mathbb{Z}_{p_i}$, which they call delta functions.[4] In their work, they prove a lower bound of $r+1$ on the sparsity of $S_{\text{can},m}$-decoding polynomials, where m is a product of r distinct primes. Ghasemi and Kopparty [15] also prove a lower bound of 2^r on the sparsity of the $S^{+}_{\text{can},m}$-decoding polynomials, where $S^{+}_{\text{can},m} = \{x \in \mathbb{Z}_m : \forall i \in \{1,\ldots,r\} : x \bmod p_i \in \{0,1,2\}\}\backslash\{1\}$ is a natural generalization of $S_{\text{can},m}$. [5]

1.2 Our Results

Share Conversion vs. Decoding Polynomials. Our main result shows that when $p \nmid m$, an S-share conversion from $\mathbb{Z}_m$ to a field of characteristic p implies a k-sparse S-decoding polynomial; i.e., in this case, share conversion does not improve the communication complexity of PIR protocols compared to decoding polynomials.

Theorem 1.2 (Informal). *Let m be an integer and p be a prime such that $p \nmid m$. If there exists a k-party S-share conversion from $\mathbb{Z}_m$ to a finite field of characteristic p, then there is a k-sparse S-decoding polynomial from $\mathbb{Z}_m$ to a finite field of characteristic p.*

The condition that $p \nmid m$ is a necessary condition for the existence of a decoding polynomial from $\mathbb{Z}_m$ to a finite field of characteristic p (since the definition requires a field element γ of order m). Yet, it is not a necessary condition for general S-share conversion, as the share conversions found by Beimel et al. [6], Paskin-Cherniavsky and Schmerler [27], and Paskin-Cherniavsky and Nissenbaum [26] are from $\mathbb{Z}_m$ to a field $\mathbb{F}_{p^\ell}$ such that $p|m$. Nevertheless, Theorem 1.2 implies that one cannot gain much by using general share conversion, as given a k-party share conversion from $\mathbb{Z}_m$ to a field of characteristic p such that $p|m$, one can easily construct a k-party share conversion from $\mathbb{Z}_{m/p}$ to a field of characteristic p; thus, even in this case, one can gain only one prime by using $p|m$ (e.g., using the best known constructions of matching vectors [17], the complexity will change from $2^{\tilde{O}(\sqrt[r]{\log N})}$ to $2^{\tilde{O}(\sqrt[r-1]{\log N})}$).

A Lower Bound on the Number of Parties in a $S_{\text{can},m}$-Share Conversion. The best known $S_{\text{can},m}$-share conversion for an m that is a product of r distinct

[4] Ghasemi and Kopparty also give upper bounds for the sparsity of delta functions for other groups that are not applicable to PIR.

[5] Ghasemi and Kopparty state their result for the set in which $x \bmod p_i \in \{-1,0,1\}$; translating their result to the requirement that $P(\gamma) \neq 1$ results in the above defined set.

primes requires $c \cdot 2^r$ parties for some constant $c < 1$ [13,21,22,9,12,16]. It is not known if an exponential number of parties is required or if there are conversions with fewer parties. Ghasemi and Kopparty [15] have recently proved that the sparsity of every $S_{\text{can},m}$-decoding polynomial is at least $r+1$. We show that $S_{\text{can},m}$-share conversion requires at least $r+1$ parties, even if $p \mid m$.

Theorem 1.3 (Informal). *For every $r \geq 1$, if there exists a k-party $S_{\text{can},m}$-share conversion for m that is a product of r distinct primes, then $k \geq r+1$.*

We note that the result of [15] and our result do not solve the big open problem of the number of parties required for the $S_{\text{can},m}$-share conversion. In particular, for $r = 3$, at least 4 parties are required, and there are constructions with 6 parties [21,3]; it is not known if there are such share conversions with 4 or 5 parties.

We also prove that a k-party $S_{\text{can},m}$-share conversion, where m is a product of r primes, implies a $(k-1)$-party $S_{\text{can},m'}$-share conversion where m' is a product of $r-1$ primes.

Theorem 1.4. *If there exists a k-party $S_{\text{can},m}$-share conversion and $m = m' \cdot p$, then there exists a $(k-1)$-party $S_{\text{can},m'}$-share conversion.*

This result can be used as an induction step in an alternative proof for Theorem 1.3. Furthermore, if one can prove, for example, a lower bound of 5 on the number of parties in any $S_{\text{can},m}$-share conversion, for every m that is a product of 3 primes, Theorem 1.4 will imply a lower bound of $r+2$ on the number of parties in any $S_{\text{can},m}$-share conversion, for every m that is a product of r primes.

A Tight Lower Bound on the Number of Parties in $\mathbb{Z}_m \setminus \{1\}$-Share Conversion. Our next result is a lower bound on the number of parties in $\{2,\ldots,b\}$-share conversion for any $b \in \{2,\ldots,m\}$; we prove that, in such share conversion, the number of parties is at least b.

Theorem 1.5 (Informal). *Let $2 \leq b \leq m$ be integers. In any $\{2,\ldots,b\}$-share conversion from $\mathbb{Z}_m$ to any field, the number of parties is at least b.*

The above lower bound is tight, since by Efremenko [13], for every S, there is an $(|S|+1)$-party S-share conversion.

By our lower bound, in any $\mathbb{Z}_m \setminus \{1\}$-share conversion, the number of parties is at least m. Efremenko [13] constructed short $\mathbb{Z}_m \setminus \{1\}$-matching vectors and then showed how to use them to construct $S_{\text{can},m}$-matching vectors; our results show that the $\mathbb{Z}_m \setminus \{1\}$-matching vectors cannot be used directly to construct efficient PIR protocols.

An Exponential Lower Bound on the Number of Parties in $S_{\text{zero},m}$-Share Conversion. Our last result is a lower bound on the sparsity of decoding polynomials and the number of parties in share conversion for a set that extends the canonical set. For $m = p_1 \cdot \ldots \cdot p_r$, define

$$S_{\text{zero},m} = \left\{ x \in \mathbb{Z}_m : \bigvee_{i \in [r]} x \equiv 0 \pmod{p_i} \right\}.$$

For example, $S_{\text{zero},15} = \{0, 3, 6, 9, 12, 5, 10\}$ (while $S_{\text{can},15} = \{0, 6, 10\}$). Alon et al. [1] constructed a 2^r-sparse $S_{\text{zero},m}$-decoding polynomial; by [13] this implies $S_{\text{zero},m}$-share conversion with 2^r parties. One might hope that there exists a $S_{\text{zero},m}$-share conversion with fewer parties and shorter $S_{\text{zero},m}$-matching vectors; together, these facts could lead to more efficient PIR protocols. However, we prove that the $S_{\text{zero},m}$-decoding polynomial and share conversion of [1] are optimal.

Theorem 1.6 (Informal). *The sparsity of every $S_{\text{zero},m}$-decoding polynomial for m that is a product of r distinct primes is at least 2^r. In particular, in any $S_{\text{zero},m}$-share conversion over a finite field of characteristic p, if $p \not| m$, then the number of parties is at least 2^r, and if $p \mid m$, then the number of parties is at least 2^{r-1}.*

Note that the lower bound given by [15] for $S^{+}_{\text{can},m}$ is incomparable to our result, as neither set is contained within the other. Furthermore, the proofs of the two lower bounds are different.

1.3 Related Works

Chor et al. [10], in addition to introducing PIR protocols, presented non-trivial results; they constructed a 2-server PIR protocol with communication of $O(N^{1/2})$ and a k-server PIR protocol for $k > 2$ with communication of $O(N^{1/k})$. Since then, the communication complexity of information theoretic private information retrieval protocols has been studied and improved [2,20,5,7,28,13,21,22,9,12,16]. In particular, Efremenko [13] shows that for every $r \geq 2$ there is a 2^r-server PIR protocol with query complexity of $2^{\tilde{O}\left(\sqrt[r]{\log N}\right)}$ and answers of length $O(1)$, and a 3-server PIR protocol with query length of $2^{\tilde{O}\left(\sqrt{\log N}\right)}$, which is currently the best known 3-server PIR protocol with short answers.

Dvir and Gopi [12] broke the $N^{1/3}$ barrier for the communication complexity of 2-server PIR protocols, constructing a PIR protocol with a communication complexity of $2^{\tilde{O}\left(\sqrt{\log N}\right)}$; they also generalized their results to a 2^{r-1}-server PIR protocol for $r \geq 2$ with a communication complexity of $2^{\tilde{O}\left(\sqrt[r]{\log N}\right)}$. Recently, Ghasemi, Kopparty, and Sudan [16] improved the constructions for more than two servers; in particular, they constructed a 3-server PIR protocol with a communication complexity of $2^{\tilde{O}\left(\sqrt[3]{\log N (\log\log N)^2}\right)}$. Itoh and Suzuki [21,22], as well as Chee et al. [9], showed how to construct non-trivial $S_{\text{can},m}$-decoding polynomials, resulting in $3^{r/2}$-server PIR where $r \leq 102$ is even, $2 \cdot 3^{(r-1)/2}$-server PIR where $r \leq 103$ is odd, and $(3/4)^{51} \cdot 2^r$-server PIR for $r \geq 104$ with a communication complexity of $2^{\tilde{O}\left(\sqrt[r+1]{\log N}\right)}$.

PIR protocols with short answers are closely related to locally decodable codes (LDC), which encode a string x into a longer string y, such that even if a large portion of y is corrupted, each bit of x can still be decoded with high probability by probing a few bits of y. Katz and Trevisan [24] have shown that

any k-server PIR protocol with short answers can be transformed into a k-query locally decodable code whose alphabet has constant size and whose length m is exponential in the length of the PIR queries. There is an implication in the other direction as well – a construction of a k-query locally decodable code of length m implies a k-server PIR protocol with query length $\log m$ and answer length $O(1)$, as in [28,13,22,9].

2 Our Techniques

In this section, we demonstrate the ideas of our proofs by proving special cases of our main results.

2.1 Fourier Transform and Decoding Polynomials

Following [15], we use the representation of functions given by their Fourier transform over finite fields, i.e., the range of the functions is a finite field; in the more common usage of the Fourier transform, the range is $\mathbb{C}$. See, e.g., [8, Chapter 8.1] and Section 3.4 for more background on the Fourier transform over finite fields. The Fourier transform states that every function $f : \mathbb{Z}_m \to \mathbb{F}_{p^\ell}$ can be represented as a linear combination of the functions $\left\{\psi_\beta(x) = \gamma^{\beta x} : \beta \in \mathbb{Z}_m\right\}$, where γ is an element of order m in $\mathbb{F}_{p^\ell}$; formally,

$$f(x) = \sum_{\beta \in \mathbb{Z}_m} \hat{f}(\beta)\gamma^{\beta x},$$

where $\hat{f}(\beta) \in \mathbb{F}_{p^\ell}$ are called the Fourier coefficients.

As a warm-up, we explain the simple connection between a sparse decoding polynomial and a sparse Fourier representation of a related function. Given a k-sparse S-decoding polynomial $P(X) = a_1 X^{\alpha_1} + \cdots + a_k X^{\alpha_k}$, define the function $f : \mathbb{Z}_m \to \mathbb{F}_{p^k}$ as follows: $f(x) = P(\gamma^x) = a_1\gamma^{\alpha_1 x} + \cdots + a_k\gamma^{\alpha_k x}$; this is a function satisfying

$$f(1) \neq 0 \quad \text{and} \quad f(s) = 0 \text{ for every } s \in S. \tag{1}$$

Observe that the function f is actually described by its Fourier representation with k non-zero coefficients. Conversely, every function f that satisfies (1) and has a k-sparse Fourier representation implies a k-sparse S-decoding polynomial. Thus, as observed in [15], to study the existence of decoding polynomials, it suffices to study such functions f. In this paper, we show that studying Fourier representations of general share conversion functions is useful.

2.2 Decoding Polynomials from Modified Shamir Share Conversion

Efremenko [13] constructed k-server PIR protocols from decoding polynomials using a modified version of the 1-private Shamir secret-sharing scheme.

Construction 2.1 (k-Party Modified Shamir Sharing over $\mathbb{Z}_m$, for any (possibly composite) $m \in \mathbb{N}$). Let $\alpha_1, \ldots, \alpha_k$ be distinct k elements of $\mathbb{Z}_m$. To share a secret $s \in \mathbb{Z}_m$, the dealer chooses $r \in \mathbb{Z}_m$ uniformly at random, and gives the i-th party the share $\mathsf{sh}_i = r + \alpha_i s \bmod m$.

As Beimel et al. [6] noted, the S-decoding polynomial used in the PIR protocol of Efremenko [13] implies an S-share conversion from the modified Shamir scheme. In this section, we show that the converse also holds, i.e., that a k-party S-share conversion from the modified Shamir secret-sharing scheme implies a k-sparse S-decoding polynomial over the same field (in Section 4, we show the stronger results for CNF S-share conversion). A necessary condition for this to hold is for the share conversion to be from $\mathbb{Z}_m$ to a field $\mathbb{F}_{p^\ell}$ such that $p \nmid m$. In addition, we consider $\ell \geq 1$, such that $m | p^\ell - 1$ (since $p \nmid m$, such ℓ exists). Thus, there exists an element $\gamma \in \mathbb{F}^*_{p^\ell}$ of order m.

Let $C_1, \ldots, C_k : \mathbb{Z}_m \to \mathbb{F}_{p^\ell}$ be a share conversion from the modified Shamir scheme defined by some elements $0 \leq \alpha_1 < \ldots < \alpha_k < m$. Consider the representation by the Fourier transform

$$C_i(x) = \sum_{\beta \in \mathbb{Z}_m} \hat{C}_i(\beta) \cdot \gamma^{\beta \cdot x}.$$

Let $r, s \in \mathbb{Z}_m$,

$$\begin{aligned} & C_1(r + \alpha_1 s) + \cdots + C_k(r + \alpha_k s) \\ &= \sum_{\beta \in \mathbb{Z}_m} \left[\hat{C}_1(\beta) \cdot \gamma^{\beta(r+\alpha_1 s)} + \cdots + \hat{C}_k(\beta) \cdot \gamma^{\beta(r+\alpha_k s)} \right] \\ &= \sum_{\beta \in \mathbb{Z}_m} \gamma^{\beta \cdot r} \left[\hat{C}_1(\beta) \cdot (\gamma^s)^{\beta \alpha_1} + \cdots + \hat{C}_k(\beta) \cdot (\gamma^s)^{\beta \alpha_k} \right]. \end{aligned} \tag{2}$$

For every $\beta \in \mathbb{Z}_m$, define $P_\beta(X) = \sum_{i=1}^k \hat{C}_i(\beta) \cdot X^{\beta \alpha_i}$. By (2) and by the properties of share conversion, for every $r \in \mathbb{Z}_m$

$$C_1(r + \alpha_1 s) + \cdots + C_k(r + \alpha_k s) = \sum_{\beta \in \mathbb{Z}_m} \gamma^{\beta \cdot r} \cdot P_\beta(\gamma^s) = \begin{cases} \neq 0 & \text{if } s = 1, \\ 0 & \text{if } s \in S. \end{cases} \tag{3}$$

First, observe that by (3), there exists β^* such that $P_{\beta^*}(\gamma^1) \neq 0$. Fix $s \in S$ and define the polynomial $Q(Y) = \sum_{\beta \in \mathbb{Z}_m} Y^\beta \cdot P_\beta(\gamma^s)$. Note that $\deg(Q) < m$. From (3), we get that $Q(\gamma^r) = 0$ for every $r \in \mathbb{Z}_m$; i.e., Q has m roots. Thus, it must be that $Q \equiv 0$. Therefore, $P_\beta(\gamma^s) = 0$ for every $\beta \in \mathbb{Z}_m$. Therefore, P_{β^*} is an S-decoding polynomial with k-sparsity; i.e., its sparsity is the same as the number of parties in the share conversion.

2.3 Lower Bound for $S_{\mathrm{can},m}$-Share Conversion

We present a lower bound on the number of parties in an $S_{\mathrm{can},m}$-share conversion for the case where m is a product of two distinct primes. The general case where m is a product of r prime powers is proven in Section 5.1

Claim 2.2. *Let $m = p_1p_2$ where p_1, p_2 are two distinct primes. Every CNF $S_{\text{can},m}$-share conversion from $\mathbb{Z}_m$ must have at least three parties.*

Proof. Assume towards contradiction that there is a two-party $S_{\text{can},m}-$CNF share conversion $C_1, C_2 : \mathbb{Z}_m \to \mathbb{F}$. Denote $S_{\text{can},m} = \{0, s_1, s_2\}$, where for $i \in \{1,2\}$, $s_i \equiv 1 \pmod{p_i}$, and $s_i \equiv 0 \pmod{p_{3-i}}$. Observe that $s_1 + s_2 \equiv 1 \pmod{m}$. For every $s \in S_{\text{can},m} \cup \{1\}$, we will consider a two-party CNF sharing, i.e., $\mathsf{sh}_1, \mathsf{sh}_2 \in \mathbb{Z}_m$ such that $\mathsf{sh}_1 + \mathsf{sh}_2 \equiv s \pmod{m}$. We will show that a weighted sum of the share conversions is equal to zero, which is a contradiction since the share conversion for each $s \in S_{\text{can},m}$ sums to zero, but the share conversion on 1 is non-zero. Consider the following share conversions described in Table 1. By adding the share conversion of the first and fourth rows and

$s \in S_{\text{can},m} \cup \{1\}$	sh_1	sh_2	$C_1(\mathsf{sh}_1) + C_2(\mathsf{sh}_2)$
0	0	0	$C_1(0) + C_2(0) = 0$
s_1	s_1	0	$C_1(s_1) + C_2(0) = 0$
s_2	0	s_2	$C_1(0) + C_2(s_2) = 0$
1	s_1	s_2	$C_1(s_1) + C_2(s_2) \neq 0$

Table 1. Two-party CNF shares for $s \in S_{\text{can},m} \cup \{1\}$.

subtracting the second and third rows, we get zero. That is $C_1(s_1) + C_2(s_2) = (C_1(s_1)+C_2(0))+(C_1(0)+C_2(s_2))-(C_1(0)+C_2(0)) = 0$. This is a contradiction since the sum $C_1(\mathsf{sh}_1) + C_2(\mathsf{sh}_2)$ is non-zero (since $s_1 + s_2 \equiv 1 \pmod{m}$). □

The general case is derived similarly, where we view a weighted sum of the share conversion on all the elements in $S_{\text{can},m} \cup \{1\}$, such that all the elements in the sum are canceled out to zero, leading to a contradiction.

2.4 Lower Bound of $S_{\text{zero},m}$-Decoding Polynomials

In this paper, we present an exponential lower bound on the sparsity of $S_{\text{zero},m}$-decoding polynomial. In this section, we will show how to derive this lower bound for the special case where m is a product of two distinct primes. We will show that every $S_{\text{zero},m}$-decoding polynomial, where $m = p_1p_2$ has a sparsity of at least 4.

Claim 2.3. *Let $m = p_1p_2$ where p_1, p_2 are two distinct primes. Every $S_{\text{zero},m}$-decoding polynomial has sparsity of at least* 4.

Proof. Assume otherwise, i.e., that there exists an $S_{\text{zero},m}$-decoding polynomial $P(X)$ over a field $\mathbb{F}$ of sparsity at most 3. Let $\gamma \in \mathbb{F}$ be the element of order m that defines P. We consider the function $f : \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \to \mathbb{F}$ to be defined as $f(x_1, x_2) = P(\gamma^x)$, where $x \equiv x_1 \pmod{p_1}$ and $x \equiv x_2 \pmod{p_2}$. Note that f is

properly defined by the Chinese remainder theorem. We view the representation of f by its Fourier transform

$$f(x_1, x_2) = \sum_{\beta_1 \in \mathbb{Z}_{p_1},\, \beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1, \beta_2) \gamma_1^{\beta_1 x_1} \cdot \gamma_2^{\beta_2 x_2},$$

where γ_1, γ_2 are elements in $\mathbb{F}$ of order p_1, p_2, respectively, such that $\gamma^x \equiv \gamma_1^{x_1} \cdot \gamma_2^{x_2} \pmod{m}$. Thus, the non-zero coefficients of P are the non-zero Fourier coefficients of f; thus, the sparsity of P is the number of non-zero Fourier coefficients of f. Consider $f(x_1, 0)$, which is a function from $\mathbb{Z}_{p_1}$ to $\mathbb{F}$, such that

$$f(x_1, 0) = \sum_{\beta_1 \in \mathbb{Z}_{p_1},\, \beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1, \beta_2) \gamma_1^{\beta_1 x_1} \cdot \gamma_2^{\beta_2 \cdot 0} = \sum_{\beta_1 \in \mathbb{Z}_{p_1},\,} \left(\sum_{\beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1, \beta_2) \right) \gamma_1^{\beta_1 x_1}.$$

Therefore, the Fourier coefficients of $f(x_1, 0)$ are $\sum_{\beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1, \beta_2)$ for every $\beta_1 \in \mathbb{Z}_{p_1}$.

Let $x \equiv 0 \pmod{p_2}$, i.e., $x \in S_{\text{zero},m}$. Since P is an $S_{\text{zero},m}$-decoding polynomial, $f(x_1, 0) = P(\gamma^x) = 0$ for every $x_1 \in \mathbb{Z}_{p_1}$. Thus, $f(x_1, 0) \equiv 0$ and all its Fourier coefficients are zero, i.e, $\sum_{\beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1, \beta_2) = 0$ for every $\beta_1 \in \mathbb{Z}_{p_1}$. Symmetrically, by defining the function $f(0, x_2)$, we conclude that $\sum_{\beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1, \beta_2) = 0$ for every $\beta_2 \in \mathbb{Z}_{p_2}$.

Since P is a decoding polynomial, $P(\gamma) \neq 0$; therefore, $f \not\equiv 0$; thus, f has a non-zero Fourier coefficient $\hat{f}(\beta_1^*, \beta_2^*)$. If $f(\beta_1^*, \beta_2) = 0$ for every $\beta_2 \neq \beta_2^*$, then $\sum_{\beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1^*, \beta_2) = \hat{f}(\beta_1^*, \beta_2^*) \neq 0$. Thus, there exists $\beta_2' \neq \beta_2^*$ such that $\hat{f}(\beta_1^*, \beta_2') \neq 0$. Using the same argument, since $\sum_{\beta_1 \in \mathbb{Z}_{p_1}} \hat{f}(\beta_1, \beta_2') = 0$, there exists $\beta_1' \neq \beta_1^*$, such that $\hat{f}(\beta_1', \beta_2') \neq 0$. Since P and f have at most 3 non-zero coefficients, for every $\beta_2 \neq \beta_2'$, $\hat{f}(\beta_1', \beta_2) = 0$, and therefore $\sum_{\beta_2 \in \mathbb{Z}_{p_2}} \hat{f}(\beta_1', \beta_2) = \hat{f}(\beta_1', \beta_2') \neq 0$, which is a contradiction. □

3 Preliminaries

3.1 Notations

We start with some notation used in this paper. For vectors $\mathbf{x}, \mathbf{y} \in R^n$ over some set R, we denote the concatenated vector as $\mathbf{x}||\mathbf{y}$. We denote the empty vector by ε. For every set R and $n \in \mathbb{N}$, we denote $R^{\leq n} = \bigcup_{i=0}^{n} R^i$, where $R^0 = \{\varepsilon\}$. For every $m \in \mathbb{N}$, we define the equivalence relation over $\mathbb{Z} \times \mathbb{Z}$, where for every $a, b \in \mathbb{Z}$, we say that $a \equiv b \pmod{m}$ if m divides $a - b$. In contrast, $a \bmod m$ denotes the operator that outputs the remainder of the division of a by m. For a predicate P, we denote the indicator $\mathbb{1}[P]$ that equals 1 if P is true and 0 otherwise. Vectors are denoted by bold letters, e.g., $\mathbf{w}$.

We next present the Chinese remainder theorem (CRT), which is used frequently in this paper.

Theorem 3.1 (Chinese remainder theorem). *Let $m = m_1 \cdot \ldots \cdot m_r$ where $\gcd(m_i, m_j) = 1$ for every $i \neq j \in [r]$. For every $x_1 \in \mathbb{Z}_{m_1}, \ldots, x_r \in \mathbb{Z}_{m_r}$, there exists a unique $x \in \mathbb{Z}_m$ that satisfies the set of equalities*

$$x \equiv x_i \pmod{m_i}$$

for every $i \in [r]$. We denote that unique element as $\mathsf{CRT}(x_1, \ldots, x_r)$.

3.2 Secret-Sharing Schemes

A secret-sharing scheme defines a way to distribute shares to parties such that some sets can reconstruct the secret from the shares and some sets have no information on the shares. We focus on 1-private secret-sharing schemes in which no party can learn any information about the secret (in such a scheme, we will not require any correctness). The formal definition is given as follows.

Definition 3.2 (Secret-Sharing Schemes). *A secret-sharing scheme Π over a set of parties $P = \{p_1, \ldots, p_k\}$ with a domain of secrets S is a randomized mapping from S to a set of k-tuples $S_1 \times S_2 \times \cdots \times S_k$ (the set S_j is called the domain of shares of p_j). A dealer distributes a secret $s \in S$ according to Π by computing a vector of random shares $\Pi(s) = (\mathsf{sh}_1, \ldots, \mathsf{sh}_n)$ and privately communicating each share sh_j to party p_j. For every party $p_i \in P$, we denote $\Pi_i(s)$ as a restriction of $\Pi(s)$ to its i-th entry.*

A secret-sharing scheme Π is 1-private if every party $p_i \in P$ cannot learn any information about the secret from their share. Formally, for every two secrets $s, s' \in S$ and for every possible share $\mathsf{sh}_i \in S_i$:

$$\Pr[\Pi_i(s) = \mathsf{sh}_i] = \Pr[\Pi_i(s') = \mathsf{sh}_i].$$

Definition 3.3 (Linear Secret Sharing). *Let m be a positive integer. A* linear secret-sharing scheme *over the ring $\mathbb{Z}_m$ is defined by a pair $\langle M, \rho \rangle$, where M is a $tk \times b$ matrix over $\mathbb{Z}_m$, and $\rho : [tk] \to P$ is a mapping that labels each row of M by a party $p_i \in P$. For an index $i \in [k]$, we define M_i as the matrix obtained by restricting M to the rows labeled by p_i. To share a secret $s \in \mathbb{Z}_m$, the dealer acts as follows:*

- *Chooses $b-1$ ring elements $r_1, \ldots, r_{b-1}$ from $\mathbb{Z}_m$ uniformly at random and computes $r_b = s - \sum_{i=1}^{b-1} r_i \bmod m$, and defines $\mathbf{r} = (r_1, \ldots, r_b)$. The share of p_i is $\mathsf{sh}_i = M_i \cdot \mathbf{r}$.*[6]

Linear schemes are usually defined over fields and are also known as monotone span programs [23]. Fehr [14] defined linear secret-sharing schemes over rings and moduli and showed that a scheme is 1-private if, for every $i \in [k]$, there exists a vector $\mathbf{w}_i \in \mathbb{Z}_m^b$ such that $M_i \mathbf{w}_i = \mathbf{0}$ and $\mathbf{1}_b \cdot \mathbf{w}_i = 1$. Beimel et al. [6] showed the converse; we recite it in Claim 3.9. We recall the following linear 1-private secret-sharing schemes over $\mathbb{Z}_m$ that will be used in this paper.

[6] The standard definition is choosing $b-1$ ring elements $r_2, \ldots, r_b$ from $\mathbb{Z}_m$ uniformly at random and letting $r_1 = s$; these two definitions are equivalent by a linear manipulation of the columns of the matrix.

Construction 3.4 (Additive Secret Sharing). To share a secret $s \in \mathbb{Z}_m$ in a k-party additive sharing scheme over $\mathbb{Z}_m$ do the following:

- Choose $r_1, \ldots, r_{k-1} \in \mathbb{Z}_m$ uniformly at random.
  Compute $r_k = s - \sum_{i=1}^{k-1} r_i \bmod m$.
- The share of p_i is $\mathsf{sh}_i = r_i$.

CNF sharing is an extension of additive sharing, where each party receives all random elements except one.

Construction 3.5 (CNF Secret Sharing [19]). To share a secret $s \in \mathbb{Z}_m$, in a k-party CNF sharing scheme over $\mathbb{Z}_m$ do the following:

- Additively share s into k shares $r_1, \ldots, r_k$.
- The share of the i-th party is $\mathsf{sh}_i = (r_j)_{j \neq i}$.

In the CNF secret-sharing scheme, each party p_i does not hold r_i; thus, it has no information about s. This implies that the scheme is 1-private. Observe that in the two-party case, the CNF sharing and additive sharing are equivalent.

Next, we consider a modified version of the 1-private Shamir secret-sharing scheme. In the 1-private Shamir scheme, the shares are points on a line where the secret is the constant term and the slope is random. In the modified version, the constant term is random, and the slope is the secret.

Construction 3.6 (Modified Shamir's Secret Sharing). Let $0 \leq \alpha_1 < \alpha_1 < \ldots < \alpha_k < m$. To share a secret $s \in \mathbb{Z}_m$, do the following:

- Choose with uniform distribution $r \in \mathbb{Z}_m$.
- The share of the i-th party is $\mathsf{sh}_i = r + \alpha_i \cdot s$.

Since in the modified shamir's secret-sharing scheme r acts as a one-time pad, the scheme is 1-private.

3.3 Share Conversion

An S-share conversion, introduced by Beimel et al. [6], involves parties holding shares of a 1-private linear secret-sharing scheme over a ring and each party can locally converts its share to a new share, resulting in shares of an additive secret-sharing scheme for a new secret, where the new secret related to the original secret.

Definition 3.7 (S-Share Conversion [6]). *Let Π be a k-party sharing scheme over $\mathbb{Z}_m$, where the share of each party is in $\mathbb{Z}_m^t$, and let $S \subseteq \mathbb{Z}_m \setminus \{1\}$. The functions $C_1, \ldots, C_k : \mathbb{Z}_m^t \to \mathbb{F}$ are a k-party (Π, S)-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}$ if the following requirements hold.*

- *If $\mathsf{sh}_1, \ldots, \mathsf{sh}_k \leftarrow \Pi(1)$, then $C_1(\mathsf{sh}_1) + \cdots + C_k(\mathsf{sh}_k) \neq 0$.*
- *If $\mathsf{sh}_1, \ldots, \mathsf{sh}_k \leftarrow \Pi(s)$ and $s \in S$, then $C_1(\mathsf{sh}_1) + \cdots + C_k(\mathsf{sh}_k) = 0$.*

We say that there is an S-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}$ if there exists a 1-private linear secret-sharing scheme Π over $\mathbb{Z}_m^t$ for some $t \geq 1$ and an (Π, S)-share conversion share conversion $C_1, \ldots, C_k$ from $\mathbb{Z}_m$ to $\mathbb{F}$.

The definition we present here slightly differs from the original definition in [6], as in [6] they consider a set S that does not contain 0, instead of 1, and the sharing of 0 is converted to an additive sharing of a non-zero secret. The change was made to fit the simplified version of the PIR protocol in [1]. Alon et al. [1] showed that these definitions are equivalent. The next theorem asserts that a share conversion can always start from CNF sharing.

Theorem 3.8 ([6]). *If there is an S-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}$, then there is a CNF S-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}$.*

For the sake of completion we prove Theorem 3.8. As a first step towards proving the theorem, we prove the following claim, which, as mentioned, is the converse of a claim from [14].

Claim 3.9. *Let $\langle M, \rho \rangle$ be a 1-private linear secret-sharing over $\mathbb{Z}_m$. For every $i \in [k]$, there exists a column vector $\mathbf{w}_i \in \mathbb{Z}_m^b$ such that $M_i \mathbf{w}_i = \mathbf{0}_t$ (where t is the number of rows in M_i) while $\mathbf{1}_b \cdot \mathbf{w}_i = 1$.*

Proof. The vector $\mathbf{r} = \mathbf{0}_b$ (where b is the number of columns in M) is a possible random vector for the secret $s = 0$. Thus, the vector $\mathbf{0}_t = M_i \mathbf{0}_b$ is a valid share for p_i for the secret 0. By the 1-privacy, this vector is also valid for the secret 1; thus, there exists a vector of randomness, denoted by $\mathbf{w}_i$, that generates the vector $\mathbf{0}_t$ for the secret 1; that is, $M_i \mathbf{w}_i = \mathbf{0}_t$ and $\mathbf{1}_b \cdot \mathbf{w}_i = 1$. □

Define the matrix $W = (\mathbf{w}_1, \ldots, \mathbf{w}_k)$; that is, W contains k columns, where the i-th column is the vector $\mathbf{w}_i$, guaranteed by Claim 3.9. Consider the linear scheme $M' = MW$.

Proof (of Theorem 3.8). Let $C'_1, \ldots, C'_k : \mathbb{Z}_m^t \to \mathbb{F}$ be an S-share conversion with respect to M. Let $s \in \mathbb{Z}_m$, and let $\mathbf{r}' = (r'_1, \ldots, r'_k)$ such that $\sum_{i=1}^k r'_i = s$ be the vector used for generating CNF shares of the secret s, i.e., the share of p_i is $\mathsf{sh}_i = (r_j)_{j \neq i}$. Each party p_i will locally compute the M'-share $\mathsf{sh}'_i = M'_i \mathbf{r}'$ from sh_i. Since the i-th column of M'_i is $M'_i \mathbf{w}_i = 0$; thus p_i can compute $M'_i \mathbf{r}'$ without knowing r'_i. We will show that the following relation between sh_i and sh'_i holds.

- For every $s \in \mathbb{Z}_m$, if $(\mathsf{sh}_i)_{i=1}^k$ are CNF shares of s, then $(\mathsf{sh}'_i)_{i=1}^k$ are M shares of s.

That is, we will show that there exists a vector $\mathbf{r} = (r_1, \ldots, r_b)$ over $\mathbb{Z}_m$, such that $M_i \mathbf{r} = \mathsf{sh}'_i$ for every $i \in [k]$, and $\mathbf{1}_b \cdot \mathbf{r} = s$. Let $\mathbf{r} = W\mathbf{r}'$. On one hand,

$$M_i \mathbf{r} = M_i (W \mathbf{r}') = (M_i W) \mathbf{r}' = M'_i \mathbf{r}' = \mathsf{sh}'_i.$$

On the other hand,

$$\mathbf{1}_b \cdot \mathbf{r} = \mathbf{1}_b(W\mathbf{r}') = (\mathbf{1}_b W)\mathbf{r}' = \mathbf{1}_k \cdot \mathbf{r}' = s,$$

where $\mathbf{1}_b W = \mathbf{1}_k$ since $\mathbf{1}_b \cdot \mathbf{w}_i = 1$, for every $i \in [k]$.

For each $i \in [k]$, we define the following CNF S-share conversion:

$$C_i(\mathsf{sh}_i) = C'_i(\mathsf{sh}'_i).$$

We next prove that $C_1, \ldots, C_k$ are a (CNF, S)-share conversion.

- If $s \in S$, then,
$$\sum_{i=1}^{k} C_i(\mathsf{sh}_i) = \sum_{i=1}^{k} C'_i(\mathsf{sh}'_i) = 0.$$
- If $s = 1$, then,
$$\sum_{i=1}^{k} C_i(\mathsf{sh}_i) = \sum_{i=1}^{k} C'_i(\mathsf{sh}'_i) \neq 0.$$

□

As we previously described, Efremenko [13] presented a construction for k-server PIR protocol. Beimel et al. [6] defined share conversion and observed that Efremenko implicitly constructed share conversions via sparse decoding polynomials. We present a definition of decoding polynomials that slightly differs from the definition in [13], defining them by a subset $S \subseteq \mathbb{Z}_m \setminus \{1\}$ where the former definition was only defined by $S \subseteq \mathbb{Z}_m \setminus \{0\}$.

Definition 3.10 (S-Decoding polynomials). *Let $S \subseteq \mathbb{Z}_m \setminus \{1\}$ be a set, p be a prime and $\ell \geq 1$ be an integer such that $m \mid p^\ell - 1$. Let $\gamma \in \mathbb{F}_{p^\ell}$ be an element of order m (such γ always exists). A polynomial $P(X) \in \mathbb{F}_{p^\ell}[X]$ is called an S-decoding polynomial if:*

$$P(\gamma^s) = \begin{cases} \alpha \neq 0 & \text{if } s = 1 \\ 0 & \text{if } s \in S. \end{cases}$$

A polynomial is k-sparse if it has at most k non-zero coefficients.

Next, we specify the sets that are used in the constructions of PIR protocols from share conversions and from decoding polynomials. Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r$ are positive integers. In the best known PIR constructions [13,16], a variation of this set is used

$$\begin{aligned} S_{\mathrm{can},m} &= \{x \in \mathbb{Z}_m : \forall i \in [r], x \bmod p_i^{e_i} \in \{0,1\}\} \setminus \{1\} \\ &= \{s_B \in \mathbb{Z}_m : B \subsetneq [r], \forall i \in [r], s_B \equiv \mathbb{1}[i \in B] \pmod{p_i^{e_i}}\}. \end{aligned}$$

Another set that is used for share conversions and decoding polynomials in [1] is

$$S_{\mathrm{zero},m} = \mathbb{Z}_m \setminus \mathbb{Z}_m^* = \left\{ x \in \mathbb{Z}_m : \bigvee_{i \in [r]} x \equiv 0 \pmod{p_i^{e_i}} \right\}.$$

Note that $S_{\mathrm{can},m} \subseteq S_{\mathrm{zero},m}$; thus, every $S_{\mathrm{zero},m}$-share conversion (resp. decoding polynomial) is also an $S_{\mathrm{can},m}$-share conversion (resp. decoding polynomial).

3.4 Fourier Transform over Finite Fields

We now define the Fourier transform for functions from a modulo group $\mathbb{Z}_m^k$ to a finite field and state the Fourier inversion formula.[7]

Definition 3.11 (Discrete Fourier Transform over $\mathbb{Z}_m^k$). *Let $m > 0$ be an integer, p be a prime such that $p \nmid m$, and $\ell \geq 1$ such that $m \mid p^\ell - 1$. Let $\gamma \in \mathbb{F}_{p^\ell}^*$ be an element of order m. For a function $f : \mathbb{Z}_m^k \to \mathbb{F}_{p^\ell}$, the Fourier transform of f is a function $\hat{f} : \mathbb{Z}_m^k \to \mathbb{F}_{p^\ell}$, defined for every $\boldsymbol{\beta} \in \mathbb{Z}_m^k$,*

$$\hat{f}(\boldsymbol{\beta}) = \frac{1}{m} \sum_{\mathbf{x} \in \mathbb{Z}_m^k} f(\mathbf{x}) \cdot \gamma^{-\langle \boldsymbol{\beta}, \mathbf{x} \rangle},$$

where $m = \underbrace{1 + \cdots + 1}_{m \text{ times}}$.[8]

Theorem 3.12 (Fourier Inversion Formula). *Every function $f : \mathbb{Z}_m^k \to \mathbb{F}$ can be uniquely represented using its Fourier transform as follows:*

$$f(\mathbf{x}) = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^k} \hat{f}(\boldsymbol{\beta}) \cdot \gamma^{\langle \boldsymbol{\beta}, \mathbf{x} \rangle},$$

where each $\hat{f}(\beta)$ is called a Fourier coefficient.

We show a simple example of the Fourier transform of functions from $\mathbb{Z}_3$ to $\mathbb{F}_2$.

Example 3.13. Let $f : \mathbb{Z}_2 \to \mathbb{F}_3$. Then, $(-1) \in \mathbb{F}_3$ is an element of order $|\mathbb{Z}_2| = 2$. The Fourier transform of f is

$$f(x) = a_0 \cdot (-1)^{0 \cdot x} + a_1 \cdot (-1)^{1 \cdot x} = a_0 + a_1 \cdot (-1)^x,$$

where a_0, a_1 are the Fourier coefficients. Since 2^{-1} in $\mathbb{F}_3$ is 2,

$$a_0 = 2^{-1} \cdot \left(f(0) \cdot (-1)^{-0 \cdot 0} + f(1) \cdot (-1)^{-0 \cdot 1} \right) = 2f(0) + 2f(1),$$

and,

$$a_1 = 2^{-1} \cdot \left(f(0) \cdot (-1)^{-0 \cdot 1} + f(1) \cdot (-1)^{-1 \cdot 1} \right) = 2f(0) - 2f(1).$$

When $m = m_1 \cdot \ldots \cdot m_r$, where $\gcd(m_i, m_j) = 1$ for every $i \neq j$, the Fourier transform of a function $f : \prod_{i=1}^r \mathbb{Z}_{m_r} \to \mathbb{F}$ can be defined by the Fourier transform of the equivalent function $g : \mathbb{Z}_m \to \mathbb{F}$, where

$$g(x) = f(x \bmod m_1, \ldots, x \bmod m_r).$$

---

[7] The Fourier transform can be defined for other groups.

[8] m is invertible in $\mathbb{F}_{p^\ell}$ since $p \nmid m$, thus $\frac{1}{m}$ is defined in the field.

Theorem 3.14. *Let $m = m_1 \cdot \ldots \cdot m_r$ be such that $\gcd(m_i, m_j) = 1$ holds for every $i \neq j$, and let $f : \prod_{i=1}^{r} \mathbb{Z}_{m_r} \to \mathbb{F}$ be a function. For every $\gamma \in \mathbb{F}$ of order m, there exists $\gamma_1, \ldots \gamma_r \in \mathbb{F}$ such that*

- *γ_i is an element of order m_i for every $1 \leq i \leq r$.*
- *For every $x_1 \in \mathbb{Z}_{m_1}, \ldots, x_r \in \mathbb{Z}_{m_r}$,*

$$\gamma^{\mathsf{CRT}(x_1,\ldots,x_r)} = \gamma_1^{x_1} \cdot \ldots \cdot \gamma_r^{x_r}$$

and

$$f(x_1, \ldots, x_r) = \sum_{(\beta_i)_{i=1}^{r} \in \prod_{i=1}^{r} \mathbb{Z}_{m_i}} \hat{f}(\beta_1 \ldots \beta_r) \prod_{i=1}^{r} \gamma_i^{\beta_i \cdot x_i},$$

where $\hat{f}(\beta_1, \ldots, \beta_r) = \hat{g}(\mathsf{CRT}\,(\beta_1, \ldots, \beta_r))$.

To prove Theorem 3.14, define for every $1 \leq i \leq r$ two elements $s_i \in \mathbb{Z}_m$ and $\gamma_i \in \mathbb{F}$, where $s_i \equiv 1 \pmod{m_i}$ and $s_i \equiv 0 \pmod{m_j}$ for $j \neq i$ and $\gamma_i = \gamma^{s_i}$. It can be checked that these $\gamma_1, \ldots \gamma_r$ satisfy all the requirements of the theorem.

3.5 Number of Roots in a Grid of a Multivariate Polynomial

We next provide a lemma that bounds the number of roots in the grid of a multivariate polynomial. This lemma will be used in the proof of Lemma 4.3, the lemma showing that a share conversion implies a decoding polynomial. For completeness, we provide its proof.

Lemma 3.15 ([25]). *Let Q be an n-variate polynomial over a field $\mathbb{F}$, such that the degree of each variable in the polynomial is less than d, and let $Z \subseteq \mathbb{F}$ be a set of size d. If $Q(\mathbf{x}) = 0$ for every $\mathbf{x} \in Z^n$, then $Q \equiv 0$, i.e., all its coefficients are zero.*

Proof. We will prove this lemma by induction on the number of variables n. For $n = 1$, the polynomial Q is a univariate polynomial of degree at most $d-1$; thus, if it has d roots then $Q \equiv 0$. Assume that the claim holds for $(n-1)$-variate polynomials. Let $Q(X_1, \ldots, X_n)$ be a non-zero n-variate polynomial. We consider Q as a polynomial in X_n, whose coefficients are polynomials in $X_1, \ldots, X_{n-1}$

$$Q(X_1, \ldots, X_n) = \sum_{i=0}^{d-1} Q_i(X_1, \ldots, X_{n-1}) \cdot X_n^i.$$

For every $\mathbf{x}' = (x_1, \ldots, x_{n-1}) \in Z^{n-1}$, define $R_{\mathbf{x}}(X_n) = Q(x_1, \ldots, x_{n-1}, X_n)$. Then, R is a univariate polynomial of degree at most $d-1$ such that $R_{\mathbf{x}'}(x_n) = 0$ for every $x_n \in Z$, therefore, $R_{\mathbf{x}'} \equiv 0$. Thus, for every $0 \leq i \leq d-1$ we get that $Q_i(\mathbf{x}') = 0$ for every $\mathbf{x}' \in Z^n$. From the induction hypothesis, $Q_i \equiv 0$ for every $0 \leq i \leq d-1$, therefore, $Q \equiv 0$. □

4 Decoding Polynomials from Share Conversion

In this section, we show that if there is a k-party S-share conversion from $\mathbb{Z}_m$ to a field $\mathbb{F}_{p^\ell}$ where $p \nmid m$, then there is a k-sparse S-decoding polynomial over $\mathbb{F}_{p^{\ell'}}$ for some $\ell' \geq \ell$.

Theorem 4.1. *Let $m > 0$, and let p be a prime such that $p \nmid m$. If there exists a k-party S-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_{p^{\ell'}}$ for some $\ell' > 0$, then there is a k-sparse S-decoding polynomial over $\mathbb{F}_{p^\ell}$, where $\ell < \ell' + m$.*

The main part of the proof of Theorem 4.1 is in Lemma 4.3, where we show that a k-party *CNF* S-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_{p^\ell}$ *such that* $m \mid p^\ell - 1$ implies a k-sparse S-decoding polynomial over $\mathbb{F}_{p^\ell}$. In the end of the section, we complete the proof of Theorem 4.1, removing the two restrictions in Lemma 4.3. Before we present and prove Lemma 4.3, we recall the share conversion from CNF sharing of an arbitrary secret $s \in \mathbb{Z}_m$ to modified Shamir sharing over $\mathbb{Z}_m$ of the same secret s. We show this conversion first, since the proof of Lemma 4.3 implicitly uses it.

Construction 4.2. Let $m \geq 1$ be an integer and let $s \in \mathbb{Z}_m$ be a secret. Let $r_1, \ldots, r_k \in \mathbb{Z}_m$ such that $\sum_{i=1}^{k} r_i = s$, and $\mathsf{sh}_i = (r_j)_{j \neq i}$, the CNF share of the i-th party of the secret s. Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_{k-1}) \in \mathbb{Z}_m^{k-1}$; the parties convert the k-party CNF sharing to k-party modified Shamir sharing with the parameters $\alpha_1 = -\beta_1, \ldots, \alpha_{k-1} = -\beta_{k-1}, \alpha_k = 0$; that is, the parties locally compute shares $\mathsf{sh}'_1, \ldots, \mathsf{sh}'_n$ such that $\mathsf{sh}'_i = r - \beta_i s$ for the same $r \in \mathbb{Z}_m$ (unknown to each party).

For every $1 \leq i \leq k$, we define a transformation $\phi_i : \mathbb{Z}_m^{k-1} \to \mathbb{Z}_m^{k-1}$

$$\begin{aligned}\phi_i(\beta_1, \ldots, \beta_{k-1}) &= (\beta_1 - \beta_i, \ldots, \beta_{i-1} - \beta_i, \beta_{i+1} - \beta_i, \ldots, \beta_{k-1} - \beta_i, \beta_k - \beta_i) \\ &= (\beta_j - \beta_i)_{j \in [k], j \neq i},\end{aligned}$$

where β_k is fixed to 0; thus, ϕ_k is the identity function. Every party i converts its share sh_i to a new share sh'_i as follows,

$$\begin{aligned}\mathsf{sh}'_i &= \langle \phi_i(\boldsymbol{\beta}), \mathsf{sh}_i \rangle \\ &= \sum_{\substack{j \in [k]: \\ j \neq i}} (\beta_j - \beta_i) r_j = \sum_{j=1}^{k} (\beta_j - \beta_i) r_j \\ &= \sum_{j=1}^{k} \beta_j r_j - \beta_i \sum_{j=1}^{k} r_j = \sum_{j=1}^{k-1} \beta_j r_j - \beta_i \sum_{j=1}^{k} r_j \\ &= \langle \boldsymbol{\beta}, \mathsf{sh}_k \rangle - \beta_i s.\end{aligned}$$

Thus, for every $1 \leq i \leq k$, the i-th share is $\mathsf{sh}'_i = r - \beta_i s$ for $r = \langle \boldsymbol{\beta}, \mathsf{sh}_k \rangle$.

Lemma 4.3. *Let $m > 0$ be an integer, p be a prime such that $p \nmid m$, and $\ell \geq 1$ be an integer such that $m \mid p^\ell - 1$. If there exists a k-party CNF S-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_{p^\ell}$, then there exists a k-sparse S-decoding polynomial $P(X) \in \mathbb{F}_{p^\ell}[X]$.*

Proof. Let $C_1, \ldots, C_k : \mathbb{Z}_m^{k-1} \to \mathbb{F}_{p^\ell}$ be a CNF S-share conversion and let $\gamma \in \mathbb{F}_{p^\ell}$ be an element of order m (since $m \mid p^\ell - 1$, such γ exists). For each function C_i, consider its Fourier transform

$$C_i(\mathbf{x}) = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \hat{C}_i(\boldsymbol{\beta}) \cdot \gamma^{\langle \boldsymbol{\beta}, \mathbf{x} \rangle}.$$

Let $r_1, \ldots, r_k, s \in \mathbb{Z}_m$ such that $\sum_{i=1}^k r_i = s$, and let $\mathsf{sh}_1, \ldots, \mathsf{sh}_k$ be the respective CNF shares, i.e., $\mathsf{sh}_i = (r_j)_{j \neq i}$. Then,

$$\sum_{i=1}^k C_i(\mathsf{sh}_i) = \sum_{i=1}^k \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \hat{C}_i(\boldsymbol{\beta}) \cdot \gamma^{\langle \boldsymbol{\beta}, \mathsf{sh}_i \rangle} = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \sum_{i=1}^k \hat{C}_i(\boldsymbol{\beta}) \cdot \gamma^{\langle \boldsymbol{\beta}, \mathsf{sh}_i \rangle}. \tag{4}$$

For every $1 \leq i \leq k$, let $\phi_i : \mathbb{Z}_m^{k-1} \to \mathbb{Z}_m^{k-1}$ be the transformation from Construction 4.2. Recall that for every $\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}$ it holds that $\langle \phi(\boldsymbol{\beta}), \mathsf{sh}_i \rangle = \langle \beta, \mathsf{sh}_k \rangle - \beta_i s$.

Also, observe that for every $1 \leq i \leq k$, the transformation ϕ_i is a permutation. Therefore, the sum in (4) is equal to

$$\begin{aligned} &\sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \left(\sum_{i=1}^k \hat{C}_i(\phi_i(\boldsymbol{\beta})) \cdot \gamma^{\langle \phi_i(\boldsymbol{\beta}), \mathsf{sh}_i \rangle} \right) \\ &\quad = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \left(\sum_{i=1}^k \hat{C}_i(\phi_i(\boldsymbol{\beta})) \cdot \gamma^{\langle \boldsymbol{\beta}, \mathsf{sh}_k \rangle - \beta_i s} \right) \\ &\quad = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \gamma^{\langle \boldsymbol{\beta}, \mathsf{sh}_k \rangle} \left(\sum_{i=1}^k \hat{C}_i(\phi_i(\boldsymbol{\beta})) \cdot (\gamma^s)^{m - \beta_i} \right), \end{aligned} \tag{5}$$

where β_k is fixed to 0. The reason we use the transformations ϕ_i is that it enables us to group elements together and define polynomials that do not depend on the shares.

define the polynomial $P_{\boldsymbol{\beta}}(X) = \sum_{i=1}^k \hat{C}_i(\phi_i(\boldsymbol{\beta})) \cdot X^{(m-\beta_i) \bmod m}$ for every $\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}$. By (4) and (5),

$$\sum_{i=1}^k C_i(\mathsf{sh}_i) = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \gamma^{\langle \boldsymbol{\beta}, \mathsf{sh}_k \rangle} \cdot P_{\boldsymbol{\beta}}(\gamma^s). \tag{6}$$

From the definition of share conversion for $s = 1$, there must exist $\boldsymbol{\beta}^*$ such that $P_{\boldsymbol{\beta}^*}(\gamma^1) \neq 0$. We will show that for every $\boldsymbol{\beta}$, it holds that $P_{\boldsymbol{\beta}}(\gamma^s) = 0$ for every $s \in S$. Therefore, we will get that $P_{\boldsymbol{\beta}^*}$ is an S-decoding polynomial with sparsity k.

For every $s \in S$, define a $(k-1)$-variate polynomial

$$Q_s(Y_1, \ldots, Y_{k-1}) = \sum_{\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}} \prod_{i=1}^{k-1} Y_i^{\beta_i} \cdot P_{\boldsymbol{\beta}}(\gamma^s).$$

We will show that $Q_s \equiv 0$, and therefore $P_{\boldsymbol{\beta}}(\gamma^s) = 0$ for every $\boldsymbol{\beta} \in \mathbb{Z}_m^{k-1}$ and every $s \in S$. Observe that the degree of each variable in Q_s is at most $m-1$. Let $Z = \{\gamma^r : r \in \mathbb{Z}_m\}$. We next show that all elements in Z^{k-1} are roots of Q_s. Consider $(\gamma^{r_1}, \ldots, \gamma^{r_{k-1}}) \in \mathbb{F}_{p^\ell}^{k-1}$, from the definition of share conversion and by (6)

$$\begin{aligned} Q_s(\gamma^{r_1}, \ldots, \gamma^{r_{k-1}}) &= \sum_{\boldsymbol{\beta} \in \mathbb{Z}_{\boldsymbol{m}}^{\boldsymbol{k-1}}} \prod_{i=1}^{k-1} (\gamma^{r_i})^{\beta_i} \cdot P_{\boldsymbol{\beta}}(\gamma^s) \\ &= \sum_{\boldsymbol{\beta} \in \mathbb{Z}_{\boldsymbol{m}}^{\boldsymbol{k-1}}} \gamma^{\sum_{i=1}^{k-1} \beta_i r_i} \cdot P_{\boldsymbol{\beta}}(\gamma^s) \\ &= \sum_{\boldsymbol{\beta} \in \mathbb{Z}_{\boldsymbol{m}}^{\boldsymbol{k-1}}} \gamma^{\langle \boldsymbol{\beta}, \mathsf{sh}_k \rangle} \cdot P_{\boldsymbol{\beta}}(\gamma^s) = \sum_{i=1}^{k} C_i(\mathsf{sh}_i) = 0, \end{aligned}$$

since $s \in S$. Therefore, Q_s has m^{k-1} roots in Z^{k-1}. Thus, by Lemma 3.15, $Q_s \equiv 0$. □

We now complete the technical details of proving Theorem 4.1.

Proof of Theorem 4.1. The theorem assumes that there is a share conversion from some linear secret-sharing scheme over $\mathbb{Z}_m$ to sharing over $\mathbb{F}_{p^{\ell'}}$. First, by Theorem 3.8, there exists a k-party S-share conversion $C_1, \ldots, C_k : \mathbb{Z}_m^{k-1} \to \mathbb{F}_{p^{\ell'}}$ from CNF sharing over Z_m to sharing over $\mathbb{F}_{p^{\ell'}}$.

Next, we prove that we can take $\ell < \ell' + m$ such that $m \mid p^\ell - 1$ and the conversion is to sharing over $\mathbb{F}_{p^\ell}$. Observe that $\gcd(m, p) = 1$ since $p \nmid m$ and p is a prime. Thus, by Euler's theorem, $p^{\varphi(m)} \equiv 1 \pmod{m}$, where $\varphi(m) < m$ is Euler's totient function. Let $0 < \ell_0 < m$ be the minimal integer such that $m \mid p^{\ell_0} - 1$. Thus, for every $\alpha \geq 1$

$$m \mid p^{\alpha \cdot \ell_0} - 1 = (p^{\ell_0} - 1) \left(\sum_{j=0}^{\alpha-1} p^{j\ell_0} \right).$$

Let $\ell = \lceil \ell'/\ell_0 \rceil \cdot \ell_0$; hence, $\ell' \leq \ell < \ell' + m$. We define the functions $C'_1, \ldots, C'_k : \mathbb{Z}_m^k \to \mathbb{F}_{p^\ell}$ such that for every $i \in [k]$ and every $\mathbf{x} \in \mathbb{Z}_m^k$, the conversion $C'_i(\mathbf{x})$ is $C_i(\mathbf{x})$ padded with $\ell - \ell'$ zeros of $\mathbb{F}_p$, where every field element in $\mathbb{F}_{p^\ell}$ (resp., $\mathbb{F}_{p^{\ell'}}$) is represented as a vector in $\mathbb{Z}_p^\ell$ (resp., $\mathbb{Z}_p^{\ell'}$). The functions $C'_1, \ldots, C'_k$ are an S-share conversion (since $\sum_{i=1}^k C'_i(\mathsf{sh}_i) = \sum_{i=1}^k C_i(\mathsf{sh}_i) || 0^{\ell - \ell'}$).

Finally, we conclude from Lemma 4.3 that there exists a k-sparse S-decoding polynomial over $\mathbb{F}_{p^\ell}$. □

5 Lower Bounds for Share Conversions

In this section, we prove lower bounds on the number of parties in S-share conversions for three sets, $S_{\text{can},m}, S_{\text{zero},m}$, and $\{2, \ldots, b\}$ for every $2 \leq b \leq m$.

5.1 Lower Bound for $S_{\text{can},m}$-Share Conversion

We next present lower bounds on the number of parties in $S_{\text{can},m}$-share conversion. This lower bound yields a lower bound on the sparsity of $S_{\text{can},m}$-decoding polynomials over $\mathbb{F}_{p^\ell}$, reproving the recent lower bound given in [15]. Our lower bound also applies when $p|m$, generalizing [15].

In Section 2, we showed this lower bound for the case where $r = 2$. Next, we present the proof of the lower bound for general r, i.e., for a CNF $S_{\text{can},m}$-share conversion where m is a product of distinct r primes

Theorem 5.1. *Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $p_1, \ldots, p_r$ are r distinct primes and $e_1, \ldots, e_r \geq 1$ are integers for $r \geq 2$, and let p be a prime and ℓ be an integer. If there is an $S_{\text{can},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_{p^\ell}$, then $k \geq r + 1$.*

Proof. By Theorem 3.8, we can assume w.l.o.g. that the share conversion is from CNF. Assume, towards contradiction, that $k = r$. This is sufficient since if there is a share conversion for $k < r$, then there is a share conversion for $k = r$. [9]

Let $C_1, \ldots, C_k : \mathbb{Z}_m^{k-1} \to \mathbb{F}_{p^\ell}$ be the share conversion. For every $B \subseteq [r]$, we define a CNF sharing of a secret in $S_{\text{can},m} \cup \{1\}$. For every $B \subseteq [r]$ and $1 \leq i \leq r$, we define $r_{B,i}$ as follows: if $i \notin B$, then $r_{B,i} = 0$; otherwise, we define $r_{B,i}$ as the unique element in $\mathbb{Z}_m$ satisfying $r_{B,i} \equiv 1 \pmod{p_i^{e_i}}$ and $r_{B,i} \equiv 0 \pmod{p_j^{e_j}}$ for every $j \neq i$. We further define $\mathsf{sh}_{B,i} = (r_{B,j})_{j \neq i}$; as $\sum_{j=1}^{r} r_{B,j} \bmod p_i \in \{0, 1\}$. Every $B \subsetneq [r]$ defines a CNF sharing of a secret in $S_{\text{can},m}$, and $B = [r]$ defines a CNF sharing of 1. By the properties of share conversion, for every $B \subsetneq [r]$,

$$\sum_{i=1}^{r} C_i(\mathsf{sh}_{B,i}) = 0 \quad \text{and} \quad \sum_{i=1}^{r} C_i(\mathsf{sh}_{[r],i}) \neq 0. \tag{7}$$

Next, we will consider a linear combination of the share conversions corresponding to these CNF sharings. By the properties of share conversion, this sum equals the share conversion of the CNF sharing of $s = 1$, which is non-zero. On the other hand, we will show that this sum must be zero, yielding a contradiction. First, observe that $r_{B,j} = r_{B \cup \{i\},j}$ for every $B \subseteq [r] \setminus \{i\}$, and for every $j \neq i$, therefore, $\mathsf{sh}_{B,i} = \mathsf{sh}_{B',i}$. Consider the following linear combination,

$$\sum_{B \subseteq [r]} (-1)^{|B|} \cdot \sum_{i=1}^{r} C_i(\mathsf{sh}_{B,i}).$$

By the properties of the share conversion, i.e., by (7),

$$\sum_{B \subseteq [r]} (-1)^{|B|} \cdot \sum_{i=1}^{r} C_i(\mathsf{sh}_{B,i}) = (-1)^r \cdot \sum_{i=1}^{r} C_i(\mathsf{sh}_{[r],i}) \neq 0.$$

[9] This is derived by defining the share conversion functions for the additional parties to be constant zeros.

On the other hand,

$$\begin{aligned}
&\sum_{B\subseteq[r]} (-1)^{|B|} \cdot \sum_{i=1}^{r} C_i(\mathsf{sh}_{B,i}) \\
&= \sum_{i=1}^{r} \sum_{B\subseteq[r]} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) \\
&= \sum_{i=1}^{r} \left(\sum_{B\subseteq[r]\setminus\{i\}} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) + \sum_{\substack{B\subseteq[r]:\\ i\in B}} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) \right) \\
&= \sum_{i=1}^{r} \left(\sum_{B\subseteq[r]\setminus\{i\}} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) + \sum_{B\subseteq[r]\setminus\{i\}} (-1)^{|B|+1} C_i(\mathsf{sh}_{B\cup\{i\},i}) \right) \\
&= \sum_{i=1}^{r} \sum_{B\subseteq[r]\setminus\{i\}} (-1)^{|B|} \cdot \left(C_i(\mathsf{sh}_{B,i}) - C_i(\mathsf{sh}_{B\cup\{i\},i}) \right) \\
&= 0
\end{aligned}$$

which is a contradiction. □

5.2 Reducing One Party in $S_{\mathrm{can},m}$-Share Conversion

Next, we present a claim showing that the existence of a share conversion with k parties for $S_{\mathrm{can},m}$, where m is the product of r prime powers, implies the existence of a share conversion with $k-1$ parties for $S_{\mathrm{can},m'}$, where m' is the product of $r-1$ primes. This claim can be used as the induction step in an alternative proof of the lower bound in Theorem 5.1. In particular, the claim shows a connection between an $S_{\mathrm{can},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}_{p^\ell}$, where $m = p \cdot m'$, and an $S_{\mathrm{can},m'}$-share conversion from $\mathbb{Z}_{m'}$ to $\mathbb{F}_{p^\ell}$. By Theorem 4.1, the latter implies the existence of an $S_{\mathrm{can},m'}$-decoding polynomial over $\mathbb{F}_{p^{\ell'}}$ for any $\ell' \geq \ell$.

Theorem 5.2. *Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \geq 1$, and let $\mathbb{F}$ be a finite field. If there exists a k-party $S_{\mathrm{can},m}$-share conversion to $\mathbb{F}$, then there is a $(k-1)$-party S_{can,m_1}-share conversion to $\mathbb{F}$ where $m_1 = p_1^{e_1} \cdot \ldots \cdot p_{r-1}^{e_{r-1}}$.*

Proof. Let $C_1, \ldots, C_k : \mathbb{Z}_m^{k-1} \to \mathbb{F}$ be a k-party $S_{\mathrm{can},m}$-share conversion. By Theorem 3.8 we can assume w.l.o.g. that it is a CNF $S_{\mathrm{can},m}$-share conversion. We construct a $(k-1)$-party CNF S_{can,m_1}-share conversion $C'_1 \ldots, C'_{k-1} : \mathbb{Z}_{m_1}^{k-2} \to \mathbb{F}$ as follows. Given k-party CNF shares of a secret $s_1 \in \mathbb{Z}_{m_1}$, we will show that the parties compute (without knowing s_1) shares of a k-party CNF sharing of the secrets $s, s' \in \mathbb{Z}_m$ respectively, such that

$$s \equiv s' \equiv s_1 \pmod{m_1} \quad \text{while} \quad s \equiv 1 \pmod{p_r} \quad \text{and} \quad s' \equiv 1 \pmod{p_r}.$$

Then, each party computes $C_i(\mathsf{sh}_i) - C_i(\mathsf{sh}'_i)$. We will show that this is an S_{can,m_1}-share conversion. Furthermore, we will show that the shares of s and s' of the k-th party are identical; thus, the difference of C_k applied to the two shares is zero, which makes the k-th party redundant.

Let $s_1 \in \mathbb{Z}_{m_1}$, and let $r_{1,1}, \ldots, r_{1,k-1} \in \mathbb{Z}_{m_1}$ such that $s_1 \equiv \sum_{i=1}^{k-1} r_{1,i} \pmod{m_1}$. For every $i \in [k-1]$, let $\mathsf{sh}_{1,i} \in \mathbb{Z}_{m_1}^{k-2}$ be the CNF sharing of s_1 with $r_{1,1}, \ldots, r_{1,k-1}$, i.e., $\mathsf{sh}_{1,i} = (r_{1,j})_{j \neq i}$. We define $r_1, \ldots, r_k, r'_1, \ldots, r'_k \in \mathbb{Z}_m$ as follows. For every $1 \leq i \leq k-1$, define $r_i \in \mathbb{Z}_m$, and $r'_i \in \mathbb{Z}_m$ as elements in $\mathbb{Z}_m$ satisfying

$$r_i \equiv r'_i \equiv r_{1,i} \pmod{m_1} \text{ and } r_i \equiv r'_i \equiv 0 \pmod{p_r^{e_r}}.$$

In addition

$$r_k \equiv 0 \pmod{m_1}, r_k \equiv 1 \pmod{p_r^{e_r}} \quad \text{and} \quad r'_k = 0.$$

These elements exist by the CRT. Consider $s = \sum_{i=1}^{k} r_i \bmod m$ and $s' = \sum_{i=1}^{k} r'_i \bmod m$. Observe that

$$s \equiv s' \equiv s_1 \pmod{m_1},$$

and $s \equiv 1 \pmod{p_r^{e_r}}, s' \equiv 0 \pmod{p_r^{e_r}}$. We also define for every $1 \leq i \leq k$, $\mathsf{sh}_i = (r_j)_{j \neq i}$ and $\mathsf{sh}'_i = (r'_j)_{j \neq i}$, which are the CNF shares of the secrets s, s' respectively. Finally, for every $1 \leq i \leq k-1$, we define

$$C'_i(\mathsf{sh}_{1,i}) = C_i(\mathsf{sh}_i) - C_i(\mathsf{sh}'_i).$$

Note that the i-th party can locally compute sh_i and sh'_i given $\mathsf{sh}_{1,i}$; i.e., it can compute r_j, r'_j for every $j \neq i$, as r_j, r'_j can be computed from $r_{1,j}$; in addition, every party can compute r_k, r'_k as well (as they are independent of the original shares). Observe that $\mathsf{sh}_k = \mathsf{sh}'_k$ since $r_i = r'_i$ for $1 \leq i \leq k-1$. Thus, $C_k(\mathsf{sh}_k) - C_k(\mathsf{sh}'_k) = 0$. Therefore,

$$\sum_{i=1}^{k-1} C'_i(\mathsf{sh}_{1,i}) = \sum_{i=1}^{k-1} \left(C_i(\mathsf{sh}_i) - C_i(\mathsf{sh}'_i)\right) = \sum_{i=1}^{k} \left(C_i(\mathsf{sh}_i) - C_i(\mathsf{sh}'_i)\right).$$

We next prove that $C'_1, \ldots, C'_{k-1}$ are an S_{can,m_1}-share conversion.

If $s_1 = 1$, then $s = 1$ and $s' \in S_{\mathrm{can},m}$; therefore

$$\sum_{i=1}^{k-1} C'_i(\mathsf{sh}_{1,i}) = \sum_{i=1}^{k} C_i(\mathsf{sh}_i) - \sum_{i=1}^{k} C_i(\mathsf{sh}'_i) = \sum_{i=1}^{k} C_i(\mathsf{sh}_i) \neq 0.$$

If $s_1 \in S_{\mathrm{can},m_1}$, then both $s, s' \in S_{\mathrm{can},m}$; therefore

$$\sum_{i=1}^{k-1} C'_i(\mathsf{sh}_{1,i}) = \sum_{i=1}^{k} C_i(\mathsf{sh}_i) - \sum_{i=1}^{k} C_i(\mathsf{sh}'_i) = 0.$$

□

Observe that by the same proof, we can show that same result for $S_{\text{zero},m}$-share conversion, i.e., that by reducing one prime from m, we get an $S_{\text{zero},m'}$-share conversion with one less party.

Theorem 5.3. *Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \geq 1$, and let $\mathbb{F}$ be a finite field. If there exists a k-party $S_{\text{zero},m}$-share conversion to $\mathbb{F}$, then there is a $(k-1)$-party S_{zero,m_1}-share conversion to $\mathbb{F}$ where $m_1 = p_1^{e_1} \cdot \ldots \cdot p_{r-1}^{e_{r-1}}$.*

As stated before, combining Claim 2.2 and Theorem 5.2 can yield an alternative proof for Theorem 5.1 by induction, where Claim 2.2 is used as the basis and Theorem 5.2 is used in the induction step.

The alternative proof of Theorem 5.1 shows that if, for example, we can prove that 5 parties are necessary for $S_{\text{can},m}$-share conversion, where m is a product of 3 prime powers, then $r+2$ parties are necessary for $S_{\text{can},m}$-share conversion, where m is a product of r prime powers. Since we can use the case for $r = 3$ as a basis for the induction. More generally, we get the following corollary.

Corollary 5.4. *If there exists an r^* such that for every m that is a product of distinct r^* prime powers, every $S_{\text{can},m}$-share conversion has a least $r^* + d$ servers, then for every $r \geq r^*$ and for every m that is a product of distinct r prime powers, every $S_{\text{can},m}$-share conversion has at least $r + d$ servers.*

Now, we will present a similar result for decoding polynomials, i.e., we will show that if there exists a k-sparse $S_{\text{can},m}$-decoding polynomial where $m = m' \cdot p$, then there exists a $(k-1)$-sparse $S_{\text{can},m'}$-decoding polynomial. While the following result is implied by Theorem 5.2 combined with Theorem 4.1, its proof provides insight regarding the derived decoding polynomial.

Claim 5.5. *Let $m = p_1^{e_r} \cdot \ldots \cdot p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \geq 1$ are integers, and let $\mathbb{F}$ be a finite field. If there exists a k-sparse $S_{\text{can},m}$-decoding polynomial over $\mathbb{F}$, then there is a $(k-1)$-sparse S_{can,m_1}-decoding polynomial over $\mathbb{F}$ where $m_1 = p_1 \cdot \ldots \cdot p_{r-1}$.*

Proof. Let $\gamma \in \mathbb{F}^*$ be an element of order m, and let $P(X) = \sum_{i=1}^{k} a_i X^{\alpha_i}$ be a k-sparse $S_{\text{can},m}$-decoding polynomial. For every $B \subseteq [r]$, we denote $s_B \in \mathbb{Z}_m$ to be the unique element in $\mathbb{Z}_m$ such that $s_B \equiv 1 \bmod p_i$ if $i \in B$ and $s_B \equiv 0 \bmod p_i$ if $i \notin B$. For singletons $B = \{i\}$, we denote $s_i = s_{\{i\}}$. Let $\gamma_{m_1} = \gamma^{s_{[r-1]}}$ and $\gamma_r = \gamma^{s_r}$. First, observe that the order of γ_{m_1} is m_1, since m_1 is the smallest integer such that $m_1 \cdot s_{[r-1]} \equiv 0 \pmod m$; similarly, the order of γ_r is p_r, since p_r is the smallest integer such that $p_r \cdot s_r \equiv 0 \pmod m$. In addition, observe that

$$\gamma_{m_1} \cdot \gamma_r = \gamma^{s_{[r-1]} + s_r} = \gamma, \tag{8}$$

since $s_{[r-1]} + s_r \equiv 1 \pmod m$. We define the following polynomial

$$Q(X) = P(\gamma_r \cdot X) - \gamma_r^{\alpha_k} \cdot P(X).$$

We will show that Q is a $(k-1)$-sparse S_{can,m_1}-decoding polynomial. We start by showing the sparsity of Q.

$$\begin{aligned} Q(X) &= P(\gamma_r \cdot X) - \gamma_r^{\alpha_k} \cdot P(X) \\ &= \sum_{i=1}^{k} a_i \cdot \gamma_r^{\alpha_i} X^{\alpha_i} - \sum_{i=1}^{k} a_i \cdot \gamma_r^{\alpha_k} X^{\alpha_i} \\ &= \sum_{i=1}^{k} a_i \cdot (\gamma_r^{\alpha_i} - \gamma_r^{\alpha_k})\, X^{\alpha_i} \\ &= \sum_{i=1}^{k-1} a_i \cdot (\gamma_r^{\alpha_i} - \gamma_r^{\alpha_k})\, X^{\alpha_i}. \end{aligned}$$

The coefficient of X^{α_k} is zero; thus, Q is $(k-1)$-sparse.

Next, we show that Q is an S_{can,m_1}-decoding polynomial. For every $B \subseteq [r-1]$, we denote $s_B^1 \in \mathbb{Z}_{m_1}$ such that $s_B^1 \equiv 1 \pmod{p_i}$ if $i \in B$ and $s_B^1 \equiv 0 \pmod{p_i}$ if $i \neq B$, for every $i \in [r-1]$. The secret $s_B^1 \bmod p_r$ is not necessarily 0; thus, s_B^1 might be different from s_B. Yet, we know that for every $i \in [r-1]$

$$s_B^1 \cdot s_{[r-1]} \equiv s_B \pmod{p_i},$$

also, since $B \subseteq [r-1]$

$$s_B^1 \cdot s_{[r-1]} \equiv s_B^1 \cdot 0 \equiv s_B \pmod{p_r}.$$

Thus, $s_B^1 \cdot s_{[r-1]} \equiv s_B \pmod{m}$ Let $s_B^1 \in S_{\mathrm{can},m_1} \cup \{1\}$. Since $s_r + s_B \equiv s_{B\cup\{r\}} \pmod{m}$

$$\begin{aligned} Q(\gamma_{m_1}^{s_B^1}) &= Q(\gamma^{s_B^1 \cdot s_{[r-1]}}) = Q(\gamma^{s_B}) \\ &= P(\gamma_r \cdot \gamma^{s_B}) - \gamma_r^{\alpha_k} \cdot P(\gamma^{s_B}) \\ &= P(\gamma^{s_r} \cdot \gamma^{s_B}) - \gamma_r^{\alpha_k} \cdot P(\gamma^{s_B}) \\ &= P(\gamma^{s_{B\cup\{r\}}}) - \gamma_r^{\alpha_k} \cdot P(\gamma^{s_B}). \end{aligned} \tag{9}$$

If $s_B^1 \in S_{\mathrm{can},m_1}$, i.e., $B \subsetneq [r-1]$, then both $B, B\cup\{r\} \neq [r]$; thus, $s_B, s_{B\cup\{r\}} \in S_{\mathrm{can},m}$. Therefore, by (9)

$$Q(\gamma_{m_1}^{s_B^1}) = 0.$$

If $s_B^1 = 1$, i.e., $B = [r-1]$, then by

$$Q(\gamma_{m_1}^{s_{[r-1]}^1}) = P(\gamma^{s_{[r]}}) - \gamma_r^{\alpha_k} \cdot P(\gamma^{s_{[r-1]}}) = P(\gamma) - \gamma^{\alpha_k} \cdot 0 \neq 0.$$

□

5.3 Lower Bound for $\mathbb{Z}_m \setminus \{1\}$-Share Conversions

In this section, we present a lower bound on the number of parties for S-share conversion where $S = \mathbb{Z}_m \setminus \{1\}$, or more generally for $S = \{2, \ldots, b\}$ for every

$2 \leq b \leq m$. The proof of the lower bound is similar to the proof of Theorem 5.1 (i.e., the lower bound for $S_{\text{can},m}$); i.e., we consider conversions of shares of secrets in S, which sum to zero, and prove that a linear combination of these sharings is a conversion of shares if the secret 1, which should sum to a non-zero value, a contradiction.

Theorem 5.6. *Let m, $2 \leq b \leq m$, and $\mathbb{F}$ be a finite field. In any k-party $\{2,\ldots,b\}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}$, the number of parties k is at least b.*

Proof. Let $C_1,\ldots,C_k : \mathbb{Z}_m^{k-1} \to \mathbb{F}$ be a $\{2,\ldots,b\}$-share conversion, w.l.o.g., by Theorem 3.8, a CNF share conversion. Assume towards contradiction that $k < b$. For every $B \subseteq [k]$, we consider CNF shares for the secret $s = |B| + 1$. Define $\mathbf{r}_B = (r_{B,1},\ldots,r_{B,k})$ as follows

$$r_{B,1} = 2 \quad \text{if} \quad 1 \in B \quad \text{and} \quad r_{B,1} = 1 \quad \text{if} \quad 1 \notin B,$$

and for $2 \leq j \leq k$,

$$r_{B,j} = 1 \quad \text{if} \quad j \in B \quad \text{and} \quad r_{B,j} = 0 \quad \text{if} \quad j \notin B.$$

For every $1 \leq i \leq k$, let $\mathsf{sh}_{B,i} = (r_j)_{j \neq i}$.There is a unique sharing of the secret 1, defined by $B = \emptyset$, and every $\emptyset \neq B \subseteq [k]$ defines a sharing of s such that $2 \leq s \leq k+1$; since $k < b$, we get that $s \in \{2,\ldots,b\}$. Therefore,

$$\sum_{i=1}^{k} C_i(\mathsf{sh}_{\emptyset,i}) \neq 0 \quad \text{and} \quad \sum_{i=1}^{k} C_i(\mathsf{sh}_{B,i}) = 0 \quad \text{for every} \quad \emptyset \neq B \subseteq [k]. \tag{10}$$

Next, we consider a linear combination of the share conversions corresponding to these CNF sharings; this combination is the share conversion of the sharing of $s = 1$, which, by the properties of the share conversion, is non-zero. On the other hand, we will show that this sum must cancel out to zero, yielding a contradiction. First , observe that for every $B \subseteq [k]\backslash\{i\}$, $r_{B,j} = r_{B\cup\{i\},j}$ for every $j \neq i$; therefore, $\mathsf{sh}_{B,i} = \mathsf{sh}_{B\cup\{i\},i}$. Consider the following linear combination,

$$\sum_{B\subseteq[k]} (-1)^{|B|} \sum_{i=1}^{k} C_i(\mathsf{sh}_{B,i}).$$

By (10),

$$\begin{aligned}\sum_{B\subseteq[k]} (-1)^{|B|} \sum_{i=1}^{k} C_i(\mathsf{sh}_{B,i}) &= \sum_{B\subseteq[k],B\neq\emptyset} (-1)^{|B|} \sum_{i=1}^{k} C_i(\mathsf{sh}_{B,i}) + (-1)^0 \sum_{i=1}^{k} C_i(\mathsf{sh}_{\emptyset,i}) \\ &= (-1)^0 \sum_{i=1}^{k} C_i(\mathsf{sh}_{\emptyset,i}) \neq 0.\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{B\subseteq[k]} (-1)^{|B|} \cdot \sum_{i=1}^{k} C_i(\mathsf{sh}_{B,i}) \\
&= \sum_{i=1}^{k} \sum_{B\subseteq[k]} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) \\
&= \sum_{i=1}^{k} \left(\sum_{B\subseteq[k]\setminus\{i\}} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) + \sum_{\substack{B\subseteq[k]: \\ i\in B}} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) \right) \\
&= \sum_{i=1}^{k} \left(\sum_{B\subseteq[k]\setminus\{i\}} (-1)^{|B|} C_i(\mathsf{sh}_{B,i}) + \sum_{B\subseteq[k]\setminus\{i\}} (-1)^{|B|+1} C_i(\mathsf{sh}_{B\cup\{i\},i}) \right) \\
&= \sum_{i=1}^{k} \sum_{B\subseteq[k]\setminus\{i\}} (-1)^{|B|} \cdot \left(C_i(\mathsf{sh}_{B,i}) - C_i(\mathsf{sh}_{B\cup\{i\},i}) \right) \\
&= 0
\end{aligned}$$

which is a contradiction. □

5.4 Lower Bound for $S_{\mathbf{zero},m}$-Share Conversion

We next prove a lower bound on the number of parties in $S_{\mathrm{zero},m}$-share conversions and $S_{\mathrm{zero},m}$-decoding polynomials from $\mathbb{Z}_m$ to a field of characteristic p, where $p \nmid m$. Recall that $S_{\mathrm{zero},m} = \mathbb{Z}_m \setminus \mathbb{Z}_m^* = \{a \in \mathbb{Z}_m : \gcd(a,m) \neq 1\}$.

Alon et al. [1] showed that for every $m = p_1 \cdot \ldots \cdot p_r$, there is an $S_{\mathrm{zero},m}$-decoding polynomial with sparsity 2^r. In this section, we show that the sparsity of 2^r for $S_{\mathrm{zero},m}$-decoding polynomials is tight; i.e., we prove a lower bound of 2^r for the sparsity of $S_{\mathrm{zero},m}$-decoding polynomials.

We start by providing a claim showing how lower bounds for S_1-share conversion and S_2-share conversion implies a stronger lower bound for an "OR" of the sets. In particular this claim used in the proof of the lower bound of $S_{\mathrm{zero},m}$-decoding polynomial as an induction step.

Claim 5.7. *Let $m = m_1 \cdot m_2$, where m_1, m_2 are integers such that $\gcd(m_1, m_2) = 1$. Let $S_1 \subseteq \mathbb{Z}_{m_1} \setminus \{1\}$ and $S_2 \subseteq \mathbb{Z}_{m_2} \setminus \{1\}$ be sets, and let*

$$S_{\mathrm{OR}} = \{x \in \mathbb{Z}_m : x \bmod m_1 \in S_1 \vee x \bmod m_2 \in S_2\}.$$

If for $i \in \{1,2\}$ every S_i-decoding polynomial over $\mathbb{F}$ has at least k_i sparsity, then,every S_{OR}-decoding polynomial over $\mathbb{F}$ has at least $k_1 \cdot k_2$ sparsity.

We say that a decoding polynomial has a sparsity of at least k, if it has at least k non-zero coefficients.

Proof. Let $\gamma_1, \gamma_2 \in \mathbb{F}$ be elements of order m_1, m_2 respectively such that $\gamma = \gamma_1 \cdot \gamma_2$ is an element of order m. Let $P(X)$ be an S_{OR}-decoding polynomial over $\mathbb{F}$. Consider the function $f : \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \to \mathbb{F}$, such that for every $x_1 \in \mathbb{Z}_{m_1}, x_2 \in \mathbb{Z}_{m_2}$,

$$f(x_1, x_2) = P(\gamma^{\mathsf{CRT}(x_1,x_2)}).$$

Consider the representation of f using its Fourier transform:

$$f(x_1, x_2) = \sum_{\beta_1 \in \mathbb{Z}_{m_1}} \sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_1^{x_1 \beta_1} \cdot \gamma_2^{x_2 \beta_2}.$$

Observe that by Theorem 3.14 the sparsity of P is the number of non-zero Fourier coefficients of f. Thus, we need to show that there are at least $k_1 k_2$ non-zero Fourier coefficients. We will show that the Fourier coefficients $\hat{f}(\beta_1, \beta_2)$ define at least k_2 distinct S_1-decoding polynomials, i.e., every coefficient appears in at most one polynomial, and since each polynomial has at least k_1 monomials, there are at least $k_1 k_2$ non-zero coefficients. Consider the function $f(x_1, 1)$, which is a function from $\mathbb{Z}_{m_1}$ to $\mathbb{F}$. Then,

$$f(x_1, 1) = \sum_{\beta_1 \in \mathbb{Z}_{m_1}} \left(\sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_2^{\beta_2} \right) \gamma_1^{x_1 \beta_1}.$$

Since P is an S_{OR}-decoding polynomial, for every $s_1 \in S_1$, $f(s_1, 1) = 0$, and $f(1, 1) \neq 0$. Thus, the polynomial

$$R(X) = \sum_{\beta_1 \in \mathbb{Z}_{m_1}} \left(\sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_2^{\beta_2} \right) X^{\beta_1}$$

is an S_1-decoding polynomial; therefore, there are at least k_1 different $\beta_1 \in \mathbb{Z}_{m_1}$, such that $\sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_2^{\beta_2} \neq 0$. Denote the set of such β_1 as $D \subseteq \mathbb{Z}_{m_1}$. For each $\beta_1 \in D$, define the polynomial

$$Q_{\beta_1}(Y) = \sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) Y^{\beta_2}.$$

By the definition of D, for every $\beta_1 \in D$,

$$Q_{\beta_1}(\gamma_2) = \sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_2^{\beta_2} \neq 0.$$

Let $s_2 \in S_2$, then,

$$f(x_1, s_2) = \sum_{\beta_1 \in \mathbb{Z}_{m_1}} \left(\sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_2^{s_2 \beta_2} \right) \gamma_1^{x_1 \beta_1}$$

Observe that $f(x_1, s_2)$ is a function from $\mathbb{Z}_{m_1}$ to $\mathbb{F}$, where for every $\beta_1 \in \mathbb{Z}_{m_1}$, its Fourier coefficient corresponding to β_1 is $\sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2) \gamma_2^{s_2 \beta_2}$. Since P

is an S_{OR}-decoding polynomial, for every $x_1 \in \mathbb{Z}_{m_1}$, $f(x_1, s_2) = 0$. Therefore, $f(x_1, s_2) \equiv 0$, and all its Fourier coefficients are zero; i.e., for every $\beta_1 \in \mathbb{Z}_{m_1}$, $\sum_{\beta_2 \in \mathbb{Z}_{m_2}} \hat{f}(\beta_1, \beta_2)\gamma_2^{s_2\beta_2} = 0$. In particular, for every $\beta_1 \in D$, $Q_{\beta_1}(\gamma_2^{s_2}) = 0$ for every $s_2 \in S_2$. In addition, $Q_{\beta_2}(\gamma_2) \neq 0$; thus, Q_{β_2} is an S_2-decoding polynomial. Therefore, for every $\beta_1 \in D$, there are at least k_2 different $\beta_2 \in \mathbb{Z}_{m_2}$ such that $\hat{f}(\beta_1, \beta_2) \neq 0$. Thus, in total, there are at least $k_1 k_2$ different pairs $\beta_1 \in \mathbb{Z}_{m_1}, \beta_2 \in \mathbb{Z}_{m_2}$ such that $\hat{f}(\beta_1, \beta_2) \neq 0$. □

Theorem 5.8. *Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \geq 1$. and $\mathbb{F}$ be a field of characteristic p. In every $S_{\mathrm{zero},m}$-share conversion from $\mathbb{Z}_m$ to $\mathbb{F}$, the number of parties is at least 2^r if $p \nmid m$ and is at least 2^{r-1} if $p \nmid m$.*

Proof. By Theorem 5.3 it suffice to consider the case where $p \nmid m$, since otherwise we can reduce the p factor from m. By Theorem 5.1 it suffices to prove the lower bound for the sparsity of $S_{\mathrm{can},m}$-decoding polynomials over $\mathbb{F}$.

We will prove the claim by induction on r. The basis of the induction is for $r = 1$. In this case $S_{\mathrm{zero},m} = \{0\}$. There is not a 1-sparse $S_{\mathrm{can},m}$-polynomial. Otherwise, if $P(X) = a \cdot X^\alpha$ is an $S_{\mathrm{zero},m}$-decoding polynomial, then $P(\gamma^0) = a = 0$, but $P(\gamma) = a\gamma^\alpha \neq 0$, which is a contradiction.

Assume that for every m, a product of $r-1$ prime powers, every $S_{\mathrm{can},m}$-decoding polynomial has at least 2^{r-1} sparsity. Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ and $m_1 = p_1^{e_1} \cdot \ldots \cdot p_{r-1}^{e_{r-1}}$. Observe that

$$\begin{aligned} S_{\mathrm{zero},m} &= \left\{ x \in \mathbb{Z}_m : \bigvee_{i=1}^{r} x \equiv 0 \pmod{p_r^{e_r}} \right\} \\ &= \left\{ x \in \mathbb{Z}_m : x \in S_{\mathrm{zero},m_1} \vee x \in S_{\mathrm{zero},p_r^{e_r}} \right\}. \end{aligned}$$

By the induction assumption, every S_{can,m_1}-decoding polynomial has at least 2^{r-1} sparsity. Since every $S_{\mathrm{zero},p_r^{e_r}}$-decoding polynomial has a sparsity of at least 2; thus, by Claim 5.7, every $S_{\mathrm{zero},m}$-decoding polynomial has at least $2^{r-1} \cdot 2 = 2^r$ sparsity. □

Acknowledgments

We thank Bar Alon for a simplification of the proof of Theorem 5.1.

The authors are partially supported by ISF grant 1614/25. The first author is also supported by ERC project NFITSC (101097959).

References

1. Bar Alon, Amos Beimel, and Or Lasri. Simplified PIR and CDS protocols and improved linear secret-sharing schemes. In *TCC 2025*, volume 16269 of *LNCS*, pages 365–398. Springer, 2025.

2. A. Ambainis. Upper bound on the communication complexity of private information retrieval. In P. Degano, R. Gorrieri, and A. Marchetti-Spaccamela, editors, *ICALP 97*, volume 1256 of *LNCS*, pages 401–407, 1997.
3. Hadar Amran. Constructing multi-servers private information retrieval protocols. Master's thesis, Ben-Gurion University, 2016.
4. Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 317–342. Springer, 2014.
5. Amos Beimel, Yuval Ishai, and Eyal Kushilevitz. General constructions for information-theoretic private information retrieval. *J. of Computer and System Sciences*, 71(2):213–247, 2005.
6. Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Ilan Orlov. Share conversion and private information retrieval. In *2012 IEEE 27th CCC*, pages 258–268, 2012.
7. Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and J. F. Raymond. Breaking the $O(n^{\frac{1}{2k-1}})$ barrier for information-theoretic private information retrieval. In *Proc. of the 43rd IEEE FOCS*, pages 261–270, 2002.
8. R. E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley publishing company, 1983.
9. Y. M. Chee, T. Feng, S. Ling, H. Wang, and L. F. Zhang. Query-efficient locally decodable codes of subexponential length. *Computational Complexity*, 22(1):159–189, 2013.
10. Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Proc. of the 36th IEEE FOCS*, pages 41–51, 1995. Journal version: *J. of the ACM*, 45:965–981, 1998.
11. R. Cramer, I. Damgård, and Yuval Ishai. Share conversion, pseudorandom secret-sharing and applications to secure distributed computing. In *TCC 2005*, volume 3378 of *LNCS*, pages 342–362. Springer, 2005.
12. Zeev Dvir and Sivakanth Gopi. 2-server PIR with sub-polynomial communication. In *47th STOC*, pages 577–584, 2015.
13. Klim Efremenko. 3-query locally decodable codes of subexponential length. *SIAM J. Comput.*, 41(6):1694–1703, 2012.
14. Serge Fehr. Span programs over rings and how to share a secret from a module. Master's thesis, ETH Zurich, 1998.
15. Fatemeh Ghasemi and Swastik Kopparty. Fourier sparsity of delta functions and matching vector pirs. In *ITCS*, pages 68:1–68:22, 2026.
16. Fatemeh Ghasemi, Swastik Kopparty, and Madhu Sudan. Improved PIR schemes using matching vectors and derivatives. In Michal Koucký and Nikhil Bansal, editors, *STOC25*, pages 1648–1656. ACM, 2025.
17. V. Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20:71–86, 2000.
18. Yuval Ishai and Eyal Kushilevitz. On the hardness of information-theoretic multiparty computation. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 439 – 455. Springer, 2004.
19. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing schemes realizing general access structure. In *Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1), 15-20, 1993.
20. Toshiya Itoh. Efficient private information retrieval. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, E82-A(1):11–20, 1999.
21. Toshiya Itoh and Yasuhiro Suzuki. New constructions for query-efficient locally decodable codes of subexponential length. *CoRR*, abs/0810.4576, 2008.

22. Toshiya Itoh and Yasuhiro Suzuki. Improved constructions for query-efficient locally decodable codes of subexponential length. *IEICE Transactions on Information and Systems*, E93-D(2):263–270, 2010.
23. Mauricio Karchmer and Avi Wigderson. On span programs. In *8th Structure in Complexity Theory*, pages 102–111, 1993.
24. J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *Proc. of the 32nd ACM Symp. on the Theory of Computing*, pages 80–86, 2000.
25. N.Alon and M.Tarsi. Colorings and orientations of graphs. *Combinatorica*, 12(2):125–134, June 1992.
26. Anat Paskin-Cherniavsky and Olga Nissenbaum. New bounds and a generalization for share conversion for 3-server PIR. *Entropy*, 24(4):497, 2022.
27. Anat Paskin-Cherniavsky and Leora Schmerler. On share conversions for private information retrieval. *Entropy*, 21(9), 2019.
28. S. Yekhanin. Towards 3-query locally decodable codes of subexponential length. In *STOC 2007*, pages 266–274, 2007.