SIAM J. COMPUT.
Vol. 47, No. 4, pp. 1547–1584

NP-HARDNESS OF REED–SOLOMON DECODING, AND THE PROUHET–TARRY–ESCOTT PROBLEM*

VENKATA GANDIKOTA†, BADIH GHAZI‡, AND ELENA GRIGORESCU†

Abstract. Establishing the complexity of *bounded distance decoding* for Reed–Solomon codes is a fundamental open problem in coding theory, explicitly asked by Guruswami and Vardy [IEEE *Trans. Inform. Theory*, 51 (2005), pp. 2249–2256]. The problem is motivated by the large current gap between the regime when it is NP-hard and the regime when it is efficiently solvable (i.e., the Johnson radius). We show the first NP-hardness results for asymptotically smaller decoding radii than the maximum likelihood decoding radius of Guruswami and Vardy. Specifically, for Reed–Solomon codes of length N and dimension $K = \Theta(N)$, we show that it is NP-hard to decode more than $N - K - c\frac{\log N}{\log\log N}$ errors (with $c > 0$ an absolute constant). Moreover, we show that the problem is NP-hard under quasi-polynomial-time reductions for an error amount $> N - K - c\log N$ (with $c > 0$ an absolute constant). An alternative natural reformulation of the bounded distance decoding problem for Reed–Solomon codes is as a *polynomial reconstruction* problem. In this view, our results show that it is NP-hard to decide whether there exists a degree K polynomial passing through $K + c\frac{\log N}{\log\log N}$ points from a given set of points $(a_1, b_1), (a_2, b_2) \ldots, (a_N, b_N)$. Furthermore, it is NP-hard under quasi-polynomial-time reductions to decide whether there is a degree K polynomial passing through $K + c\log N$ many points. These results follow from the NP-hardness of a generalization of the classical subset sum problem to higher moments, called *moments subset sum*, which has been a known open problem, and which may be of independent interest. We further reveal a strong connection with the well-studied Prouhet–Tarry–Escott problem in number theory, which turns out to capture a main barrier in extending our techniques. We believe the Prouhet–Tarry–Escott problem deserves further study in the theoretical computer science community.

Key words. Reed–Solomon decdoing, polynomial reconstruction, Prouhet–Tarry–Escott problem, bounded distance decoding

AMS subject classifications. 94B35, 94B05

DOI. 10.1137/16M110349X

1. Introduction.

Despite being a classical problem in the study of error-correcting codes, the computational complexity of decoding Reed–Solomon (RS) codes [RS60] in the presence of large amounts of error is not fully understood. In the bounded distance decoding (BDD) problem, the goal is to recover a message corrupted by a bounded amount of error. Motivated by the large gap between the current efficient decoding regime and the NP-hard regime for RS codes, we study the NP-hardness of BDD for asymptotically smaller error radii than previously known. In this process, we unravel a strong connection with the Prouhet–Tarry–Escott (PTE) problem, a famous problem from number theory that has been studied for more than two centuries.

*Received by the editors November 16, 2016; accepted for publication (in revised form) May 29, 2018; published electronically August 7, 2018. A preliminary version of this work appeared in the proceedings of ISIT'15 and FOCS'16.

http://www.siam.org/journals/sicomp/47-4/M110349.html

Funding: The first author was supported in part by a grant from the Purdue Research Foundation and by NSF CCF-1649515. The second author was supported in part by NSF STC award CCF 0939370 and NSF awards CCF-1217423, CCF-1420956, CCF-1420692, and CCF-1217423. The third author was supported in part by NSF CCF-1649515.

†Purdue University, West Lafayette, IN 47907 (vgandiko@purdue.edu, elena-g@purdue.edu).

‡Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139 (badih@mit.edu).

An RS code of length N, dimension K, defined over a finite field $\mathbb{F}$, is the set of vectors (called *codewords*) corresponding to evaluations of low-degree univariate polynomials on a given set of evaluation points $\mathcal{D} = \{\alpha_1, \alpha_2, \ldots, \alpha_N\} \subseteq \mathbb{F}$. Formally, $RS_{\mathcal{D},K} = \{\langle p(\alpha_1), \ldots, p(\alpha_N)\rangle \mid p \in \mathbb{F}[x]$ is a univariate polynomial of degree $< K\}$. The Hamming distance between $x, y \in \mathbb{F}^N$ is $\Delta(x, y) := |\{i \in [N] \mid \ x_i \neq y_i\}|$. In the *BDD problem*, given a target vector $y \in \mathbb{F}^N$ and a distance parameter λ, the goal is to output $c \in \mathcal{C}$ such that $\Delta(c, y) \leq \lambda$.

It is well-known that if the number of errors is $\lambda \leq (N - K)/2$, there is a unique codeword within distance λ from the message, which can be found efficiently [Pet60, BW86]. Further, Sudan [Sud97] and Guruswami and Sudan [GS99] show that efficient decoding of up to $\lambda = N - \sqrt{NK}$ errors (the "Johnson radius") is possible (in this setting, the algorithm may output a small list of possible candidate messages). At the other extreme, if the number of errors is at least $N - K$ (the covering radius), finding one close codeword becomes trivial, amounting to interpolating a degree $K - 1$ polynomial through $\leq K$ points. However, just below that radius, namely, at $N - K - 1$ errors, the problem becomes NP-hard, a celebrated result of Guruswami and Vardy [GV05]. The proof approach of [GV05] is only applicable to the maximum likelihood decoding setting of $N-K-1$ errors, prompting the fundamental problem of understanding the complexity of BDD in the wide remaining range between $N-\sqrt{NK}$ and $N - K - 1$: *"It is an extremely interesting problem to show hardness of bounded distance decoding of Reed-Solomon codes for smaller decoding radius"* [GV05].

The only other work addressing the hardness of decoding RS codes is due to Cheng and Wan [CW07, CW10], who show randomized reductions from the discrete log problem over finite fields, which is not believed to be NP-hard.

In this work, we study the complexity of the decision version of BDD, where the number of errors is parametrized by $d \geq 0$, as formalized next:

Problem *Bounded distance decoding of Reed–Solomon codes with parameter d (*RS-BDD(d)*)*
Input $\mathcal{D} = \{\alpha_1, \alpha_2, \ldots, \alpha_N\} \subseteq \mathbb{F}$, where $\alpha_i \neq \alpha_j$ for all $i \neq j$, target $y = (y_1, y_2, \ldots, y_N)$, and integer $K < N$
Goal Decide if there exists $p \in RS_{\mathcal{D},K}$ such that $\Delta(p, y) \leq N - K - d$

We emphasize that the BDD problem above is in fact the basic and natural polynomial reconstruction problem, where the input is a subset of points $\mathcal{D} = \{(\alpha_1, y_1), (\alpha_2, y_2), \ldots, (\alpha_N, y_N)\} \subseteq \mathbb{F} \times \mathbb{F}$, and the goal is to decide if there exists a polynomial p of degree $< K$ that passes through at least $K + d$ points in $\mathcal{D}$. We will next state our main result in both forms.

1.1. Contributions. Our main technical contribution is the first NP-hardness result for BDD of RS codes for a number of errors that is asymptotically smaller than $N - K$, and its alternative view in terms of polynomial reconstruction.

THEOREM 1.1. *There exists $c > 0$ such that for every $1 \leq d \leq c \cdot \frac{\log N}{\log \log N}$, the* RS-BDD($d$) *problem for RS codes of length N, dimension $K = N/2-d+1$ over finite fields of size $|\mathbb{F}| = 2^{\mathsf{poly}(N)}$, and characteristic larger than d is NP-hard. Furthermore, there exists $c > 0$ such that for every $1 \leq d \leq c \cdot \log N$,* RS-BDD($d$) *over finite fields of size $|\mathbb{F}| = 2^{N^{O(\log N)}}$, and characteristic larger than d does not have $N^{O(\log N)}$-time algorithms unless NP has quasi-polynomial-time algorithms.*

Equivalently, there exists $c > 0$ such that for every $1 \le d \le c \cdot \frac{\log N}{\log\log N}$, it is NP-hard to decide whether there exists a polynomial of degree $< K = N/2 - d + 1$ passing through $K + d$ many points from a given set $\mathcal{D} = \{(\alpha_1, y_1), (\alpha_2, y_2), \ldots, (\alpha_N, y_N)\} \subseteq \mathbb{F} \times \mathbb{F}$ with $|\mathbb{F}| = 2^{\mathsf{poly}(N)}$. Furthermore, there exists $c > 0$ such that for every $1 \le d \le c \cdot \log N$, the same interpolation problem over fields of size $|\mathbb{F}| = 2^{N^{O(\log N)}}$ and characteristic larger than d does not have $N^{O(\log N)}$-time algorithms unless NP has quasi-polynomial-time algorithms.

We note that, as in [GV05], we require the field size to be exponential in N in our Theorem 1.1. Our results significantly extend [GV05], which only show NP-hardness for $d = 1$.

The core of the proof of Theorem 1.1 is showing the NP-hardness of the following natural generalization of the classic subset sum problem to higher moments, and which may be of independent interest:

> **Problem** *Moments subset sum with parameter d, over a field $\mathbb{F}$ (*MSS(d)*)*
> **Input** Set $A \subseteq \mathbb{F}$ of size $|A| = N$, integer k, elements $m_1, m_2, \ldots, m_d \in \mathbb{F}$
> **Goal** Decide if there exists $S \subseteq A$ such that $\sum_{w \in S} w^\ell = m_\ell$ for all $\ell \in [d]$, and $|S| = k$.

We point out that the moments subset sum problem has natural analogues over continuous domains in the form of generalized moment problems and truncated moments problems, which arise frequently in economics, operations research, statistics, and probability [Las09].

We also note that the reduction from MSS(d) to RS-BDD(d) uses the equivalence between elementary symmetric polynomials and moments polynomials, which holds when the field is of characteristic larger than d (see Lemma 2.1 for the formal reduction).

In this work, we prove the NP-hardness of the moments subset sum problem for large degrees.

THEOREM 1.2. *There exists $c > 0$ such that for every $1 \le d \le c \cdot \frac{\log N}{\log\log N}$, the moments subset sum problem* MSS(d) *over prime fields of size $|\mathbb{F}| = 2^{\mathsf{poly}(N)}$ is NP-hard. Furthermore, there exists $c > 0$ such that for every $1 \le d \le c \cdot \log N$, the moments subset sum problem* MSS(d) *over fields of size $|\mathbb{F}| = 2^{N^{O(\log N)}}$ does not have $N^{O(\log N)}$-time algorithms unless NP has quasi-polynomial-time algorithms.*

Furthermore, we reveal a novel connection between moments subset sum (and hence RS decoding) and the well-studied PTE problem in diophantine analysis, which is the main barrier for extending Theorems 1.2 and 1.1 to $d = \omega(\log N)$, as we will explain shortly.

The PTE problem [Pro51, Dic13, Wri59] first appeared in letters between Euler and Goldbach in 1750–1751, and it is an important topic of study in classical number theory (see, e.g., the textbooks of Hardy and Wright [HW79] and Hua [Hua82]). It is also related to other classical problems in number theory, such as variants of the Waring problem and problems about minimizing the norm of cyclotomic polynomials, considered by Erdös and Szekeres [ES59, BI94]. The PTE system is sometimes also referred to as the Vinogradov system (see, e.g., [Woo92]).

In the PTE problem, we are given $k \ge 1$ and the goal is to find disjoint sets of integers $\{x_1, x_2, \ldots, x_s\}$ and $\{y_1, y_2, \ldots, y_s\}$ satisfying the system

$$\begin{aligned} x_1 + x_2 + \cdots + x_s &= y_1 + y_2 + \cdots + y_s, \\ x_1^2 + x_2^2 + \cdots + x_s^2 &= y_1^2 + y_2^2 + \cdots + y_s^2, \\ &\cdots \\ x_1^k + x_2^k + \cdots + x_s^k &= y_1^k + y_2^k + \cdots + y_s^k. \end{aligned}$$

We call s the *size* of the PTE solution. It turns out that the completeness proof of our reduction in Theorem 1.2 relies on *explicit* solutions to this system for degree $k = d$ and of size $s = 2^k$. As explained next, despite significant efforts that have been devoted to constructing PTE solutions during the last 100 years, no explicit solutions of size $s = 2^{o(k)}$ are known. This constitutes the main barrier to extending our Theorems 1.2 and 1.1 to $d = \omega(\log N)$.

The main open problem that has been tackled in the PTE literature is constructing solutions of small size s compared to the degree k. It is relatively easy to show that $s \geq k+1$, and straightforward (yet nonconstructive!) pigeonhole counting arguments show the existence of solutions with $s = O(k^2)$. If we further impose the constraint that the system is not satisfied for degree $k+1$ (which is a necessary constraint for our purposes), then solutions of size $s = O(k^2 \log k)$ are known to exist [Hua82]. However, these results are nonconstructive, and the only general explicit solutions have size $s = O(2^k)$ (e.g., [Wri59, BI94]). A special class of solutions studied in the literature is for $s = k+1$ (i.e., of minimum possible size). Currently there are known explicit parametric constructions of infinitely many minimum-size solutions for $k \leq 12$ (e.g., [BI94, BLP03]), and finding such solutions often involves numerical simulations and extensive computer-aided searches [BLP03].

From a computational point of view, an important open problem is to understand whether PTE solutions of size $O(k^2)$ (which are known to exist) can be *efficiently constructed*, i.e., in time $\mathsf{poly}(k)$.

We identify the following generalization of the PTE problem as a current barrier to extending our results.

PROBLEM 1.1. *Given a field $\mathbb{F}$, integer d, and $a, b \in \mathbb{F}$, efficiently construct two disjoint sets $\{x_1, \ldots, x_s\}, \{y_1, \ldots, y_s\} \subseteq \mathbb{F}$, with $s = o(2^d)$, satisfying*

$$\begin{aligned} x_1 + x_2 + \cdots + x_s &= y_1 + y_2 + \cdots + y_s, \\ a^i + \sum_{j=1}^{s} x_j^i &= b^i + \sum_{j=1}^{s} y_j^i \quad \forall i \in \{2, \ldots, d\}. \end{aligned}$$

We believe that this question is worth further study in the theoretical computer science community. In this work, we prove the following theorem, which is at the core of the completeness of our reduction.

THEOREM 1.3. *There is an explicit construction of solutions for Problem* 1.1 *with $s = O(2^d)$, which can be computed in time $\mathsf{poly}(s)$.*

In the next subsection, we outline the proof of Theorem 1.2, and in the process, we explain how PTE solutions of degree d naturally arise when studying the computational complexity of MSS(d).

1.2. Proof overview.

Reduction from 1*-in-*3*-SAT to Subset-Sum.* The proof of Theorem 1.1 will follow from Theorem 1.2 along with a reduction from MSS(d) to RS-BDD(d) (given in

section 2). To prove Theorem 1.2, we will give a polynomial-time reduction from the 1-in-3-SAT problem in which we are given a 3-SAT formula ϕ on n variables and m clauses and are asked to determine if there exists an assignment $z \in \{0,1\}^n$ satisfying exactly one literal in each clause. It is known that this problem is NP-hard even for $m = O(n)$ [Sch78]. We start by briefly recalling the reduction from 1-in-3-SAT to Subset-Sum which will be used in our reduction to MSS(d) (for more details on the standard reduction from 1-in-3-SAT to Subset-Sum, we refer the reader to section 3). In this reduction, we are given a 3-SAT formula which we use to construct a set of integers such that there is a subset whose sum equals a given target m_1' iff there is an assignment that satisfies exactly one literal of each clause of the 3-SAT formula. Specifically, each variable $(z_t, \overline{z_t})$ is mapped to two integers a_t' (corresponding to z_t) and b_t (corresponding to $\overline{z_t}$). The integers a_t' and b_t' and the target m_1' are defined in terms of their length-$(n+m)$ Σ-ary representation (for some sufficiently large constant, say, $\Sigma = 10$) as follows:

- The Σ-ary representations of a_t' and b_t' consist of two parts: a variable region consisting of the leftmost n digits and a clause region consisting of the (remaining) rightmost m digits.
- In the variable region, a_t' and b_t' have a 1 at the tth digit and 0's at the other digits.
- In the clause region, for every $j \in [m]$, a_t' (respectively, b_t') has a 1 at the jth location if z_t (respectively, $\overline{z_t}$) appears in clause j and a 0 otherwise.
- The target m_1' is set to the integer whose Σ-ary representation is the all 1's.

Those Σ-ary representations are illustrated later in Figure 1. In section 3 we sketch the completeness and soundness of the reduction.

Extending to higher moments via inhomogeneous PTE systems. Extending this reduction so that the second moment also equals the target m_2 (whenever the given 3-SAT formula has an assignment satisfying exactly one literal in each clause) raises immediate technical hurdles, since we have very little grasp on the second moment. As the number of moments increases, the problem becomes more complex, since in order to show completeness we need to simultaneously satisfy several polynomial equations of increasingly larger degrees.

We next describe the general idea behind our reduction from 1-in-3-SAT to MSS(d). In this reduction, the completeness step will rely on explicit solutions to "inhomogeneous PTE instances" and the soundness step will rely on a delicate balancing of the magnitudes of these explicit solutions.

Our starting point is the standard reduction from 1-in-3-SAT to Subset-Sum, which we build on as follows. For each 1-in-3-SAT variable, we create a collection of *explicit* auxiliary numbers which "stabilize" the contribution of this variable to all ith moment equations with $2 \le i \le d$ while having no net effect on the first moment equation. Concretely, if a and b are the numbers corresponding to the two literals of the given variable, then we need to find numbers $x_1, \ldots, x_s, y_1, \ldots, y_s$ satisfying

$$x_1 + x_2 + \cdots + x_s = y_1 + y_2 + \cdots + y_s,$$

$$(\dagger) \qquad a^i + \sum_{j=1}^{s} x_j^i = b^i + \sum_{j=1}^{s} y_j^i \quad \forall i \in \{2, \ldots, d\}.$$

Note that in order for the overall reduction to run in polynomial time, the above auxiliary variables should be *efficiently constructible*. Moreover, we observe that (†) is an inhomogeneous PTE instance: for $a = b$, it reduces to a PTE instance of degree d.

Of course, in our case a and b will not be equal, and (†) is a more general system (and is hence harder to solve) than PTE instances. Nevertheless, as we will see shortly, solving (†) can be essentially reduced to finding explicit PTE solutions of degrees $i \le d$.

In addition, we ensure that the added auxiliary rational numbers satisfy a "bimodality" property regarding their magnitudes, which will allow the recovery of a satisfying 1-in-3-SAT assignment from any solution to the MSS(d) instance.

PROPERTY 1.2 (bimodality (informal)). *Every subset S of the auxiliary numbers is such that either $|\sum_{w\in S} w|$ is tiny or $|\sum_{w\in S} w|$ is huge.*

We note that the existence of explicit and efficiently constructible solutions of small size $s = O(d)$ to system (†) (and hence to a PTE system too) would at least ensure the completeness of a reduction with $d = O(N)$. If soundness can also be ensured for such solutions, then our techniques would extend to radii closer to the Johnson bound radius.

Overview of procedure for solving system (†). We build the auxiliary numbers recursively, by reducing the solution for degree i to a solution for degree $i-1$. Toward this goal, we design a subprocedure, which we refer to as AtomicSolver, that takes as inputs an integer $i \in \{2,3,\dots,d\}$, and a number R_i, and outputs 2^i rational[1] numbers $\{x_{i,j}, y_{i,j}\}_{j\in[2^{i-1}]}$ that satisfy a PTE system of degree $i-1$, along with a nonhomogeneous equation of degree i:

$$\sum_{\ell=1}^{2^{i-1}} (x_{i,\ell}^j - y_{i,\ell}^j) = 0 \quad \forall\ 2 \le j < i, \tag{1a}$$

$$\sum_{\ell=1}^{2^{i-1}} (x_{i,\ell}^i - y_{i,\ell}^i) = R_i. \tag{1b}$$

We can then run AtomicSolver sequentially on inputs $i \in \{2,\dots,d\}$ with the R_i input corresponding to a "residual" term that accounts for the contributions to the degree-i equation of the outputs of AtomicSolver(j,R_j) for all $2 \le j < i$, namely,

$$R_i = b^i - a^i + \sum_{2\le j<i} \sum_{\ell=1}^{2^{j-1}} (y_{j,\ell}^i - x_{j,\ell}^i). \tag{2}$$

Note that the aim of the AtomicSolver(i,R_i) procedure is to satisfy the degree-i equation (1b) without affecting the lower-degree equations (1a).

We then argue that the union $\cup_{2\le i\le d}\{x_{i,j}, y_{i,j}\}_{j\in[2^{i-1}]}$ of all output variables satisfies the polynomial constraints in (†) with $t = \exp(d)$.

Specifics of the AtomicSolver. We next illustrate the AtomicSolver procedure by describing its operation in the particular case where $i = d = 4$. In what follows, we drop "$i = 4$ subscripts" and denote $R = R_4$, $x_\ell = x_{4,\ell}$, and $y_\ell = y_{4,\ell}$ for all $1 \le \ell \le 8$. Then, (1b) above, which we need to satisfy, becomes

[1] In our case, we can afford having *rational* solutions to (1a) and (1b). Note that this system is still a generalization of the PTE problem since we can always scale the rational solutions by their least common denominator to get a PTE solution of degree $i-1$.

$$\sum_{\ell=1}^{8}(x_\ell^4 - y_\ell^4) = R. \tag{3}$$

First, we let α be a constant parameter (to be specified later on) and we set

$$x_1 - y_1 = \alpha, \tag{4a}$$

$$y_2 - x_2 = \alpha. \tag{4b}$$

Namely, in (4a) and (4b), we "couple" the ordered pairs (x_1, y_1) and (y_2, x_2) in the same way. Then, using (4a) and (4b), we substitute $y_1 = x_1 - \alpha$ and $x_2 = y_2 - \alpha$, and the sum of the $\ell = 1$ and $\ell = 2$ terms in (3) can be written as

$$(x_1^4 - y_1^4) - (y_2^4 - x_2^4) = p_\alpha(x_1) - p_\alpha(y_2), \tag{5}$$

where p_α is a *cubic* polynomial. If we set $x_1 - y_2 = \beta$, then (5) further simplifies to

$$p_\alpha(x_1) - p_\alpha(y_2) = q_{\alpha,\beta}(x_1), \tag{6}$$

where $q_{\alpha,\beta}$ is a *quadratic* polynomial.[2]

In the next step, we couple the ordered tuple (y_3, x_3, y_4, x_4) in the same way that we have so far coupled the tuple (x_1, y_1, x_2, y_2). The sum of the first four terms in the left-hand side (LHS) of (3) then becomes

$$\begin{aligned}\sum_{\ell=1}^{4}(x_\ell^4 - y_\ell^4) &= (x_1^4 - y_1^4 + x_2^4 - y_2^4) - (y_3^4 - x_3^4 + y_4^4 - x_4^4) \\ &= q_{\alpha,\beta}(x_1) - q_{\alpha,\beta}(y_3).\end{aligned} \tag{7}$$

As before, we set $x_1 - y_3 = \gamma$ and (7) further simplifies to

$$q_{\alpha,\beta}(x_1) - q_{\alpha,\beta}(y_3) = w_{\alpha,\beta,\gamma}(x_1), \tag{8}$$

where $w_{\alpha,\beta,\gamma}(x_1)$ is a *linear* polynomial in x_1. Finally, we couple the ordered tuple $(y_5, x_5, y_6, x_6, y_7, x_7, y_8, x_8)$ in the same way that we have so far coupled the tuple $(x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4)$, and we obtain that the following equation is equivalent to (3) above:

$$w_{\alpha,\beta,\gamma}(x_1) - w_{\alpha,\beta,\gamma}(y_5) = R. \tag{9}$$

Setting $x_1 - y_5 = \theta$, (9) further simplifies to

$$\theta \cdot h_{\alpha,\beta,\gamma} = R, \tag{10}$$

where $h_{\alpha,\beta,\gamma}$ is the coefficient of x_1 in the linear polynomial $w_{\alpha,\beta,\gamma}(x_1)$. We conclude that to satisfy (3), it suffices to choose α, β, γ such that $h_{\alpha,\beta,\gamma} \neq 0$ and to then set $\theta = R/h_{\alpha,\beta,\gamma}$.

It is easy to see that there exist α, β, γ such that $h_{\alpha,\beta,\gamma} \neq 0$ and that the above recursive coupling of the variables guarantees that (1a) is satisfied. The more difficult part will be to choose α, β, γ in a way that ensures the soundness of the reduction. This is briefly described next.

[2]Intuitively, we can think of the LHS of (6) (along with the setting $x_1 - y_2 = \beta$) as being a "derivative operator." This explains the fact that we are starting from a cubic polynomial $p_\alpha(\cdot)$ and getting a quadratic polynomial $q_{\alpha,\beta}(\cdot)$. This intuition was also used (twice) in (5) and will be again used in (8) and (9) in order to reduce the degree further.

Bimodality of solutions. In the above description of the particular case where $i = d = 4$, it can be seen that the produced solutions are $\{0, \pm 1\}$-linear combinations of $\{\alpha, \beta, \gamma, \theta\}$, which are required to satisfy (10). It turns out that in this case $h_{\alpha,\beta,\gamma} = 24 \cdot \alpha \cdot \beta \cdot \gamma$, and so (10) becomes

$$\theta \cdot \alpha \cdot \beta \cdot \gamma = \frac{R}{24}. \tag{11}$$

So assuming we can upper bound $|R|$,[3] we would be able to set θ to a sufficiently large power of 10 while letting α, β, and γ have tiny absolute values and satisfy (11). Using the fact that the auxiliary x_i and y_i variables are set to $\{0, \pm 1\}$-linear combinations of $\{\alpha, \beta, \gamma, \theta\}$, this implies that the bimodality property is satisfied. In section 3, we show that the bimodality property ensures that in any feasible solution to MSS(d), the auxiliary variables should have no net contribution to the degree-1 moment equation (Proposition 3.3), which then implies the soundness of the reduction.

General finite fields. We remark that as described above, our solution works over the rational numbers and, by scaling appropriately, over the integers. By taking the integer solution modulo a large prime p (i.e., $p = 2^{\mathsf{poly}(N)}$) the same arguments extend to $\mathbb{F}_p$. Moving to general finite fields $\mathbb{F} = \mathbb{F}_{p^\ell}$, we first observe that system (†) (and thus a PTE system too) has nonconstructive solutions of size $O(d)$, which follows from Deligne's generalization of the Weil bound (see section 6). Our reduction in the proof of Theorem 1.2 also extends to general fields $\mathbb{F} = \mathbb{F}_{p^\ell}$, where p is any prime larger than d and $\ell = \mathsf{poly}(N, d!)$. In this case, our reduction uses a representation of field elements in a polynomial basis $\{1, \gamma, \gamma^2, \ldots, \gamma^{\ell-1}\} \subseteq \mathbb{F}$, instead of decimal representations. For more details on this reduction, we refer the reader to section 7.

1.3. Related work. A number of fundamental works address the polynomial reconstruction problem in various settings. In particular, Goldreich, Rubinfeld, and Sudan [GRS00] show that that the polynomial reconstruction problem is NP-complete for univariate polynomials over large fields. Håstad's celebrated results [Hås01] imply NP-hardness for linear multivariate polynomials over finite fields. Gopalan, Khot, and Saket [GKS10] show NP-hardness for multivariate polynomials of larger degree over the field $\mathbb{F}_2$.

We note that in general, the polynomial reconstruction problem does not require the evaluation points to be all distinct (i.e., $x_i \neq x_j$ whenever $i \neq j$). This distinction is crucial to the previous results on polynomial reconstruction (e.g., [GRS00, GKS10]). It is this distinction that prevents those results from extending to the setting of RS codes and to their multivariate generalization, Reed–Muller codes.

On the algorithmic side, efficient algorithms for decoding of RS codes and their variants are well-studied. As previously mentioned, [Sud97, GS99] gave the first efficient algorithms in the list-decoding regime. Parvaresh and Vardy [PV05] and Guruswami and Rudra [GR08] construct capacity achieving codes based on variants of RS codes. Koetter and Vardy [KV03] propose soft decision decoders for RS codes. More recently, Rudra and Wootters [RW14] prove polynomial list-bounds for random RS codes.

A related line of work is the study of BDD and of maximum likelihood decoding for general codes, possibly under randomized reductions, and when an unlimited amount of preprocessing of the code is allowed. These problems have been extensively studied

[3] Which we will do by inductively upper bounding $|R_i|$.

under diverse settings, e.g., [Var97, ABSS97, DKRS03, DMS03, FM04, Reg04, GV05, Che08].

1.4. Organization of the rest of the paper. In section 2 we begin with a reduction from MSS(d) to RS-BDD(d). In section 3 we show our main reduction from 1-in-3-SAT to MSS(d) over the integers (and over primitive fields of large size) by showing how to build sets satisfying PTE equations; we prove the useful properties of these sets in sections 4 and 5 and Appendix A. In section 6 we show the existence of solutions to PTE equations over fields $\mathbb{F}_{p^\ell}$ of large characteristic, and in section 7 we show how to modify the reduction from section 3 to work over $\mathbb{F}_{p^\ell}$. We describe some final remarks in section 8.

2. Reduction from MSS(d) to RS-BDD(d). Throughout the paper, we use $[n]$ to denote the set $\{1, 2, \ldots, n\}$ for any positive integer n. In this section we show a formal reduction from MSS(d) to RS-BDD(d). Recall the MSS(d) problem.

DEFINITION 2.1 (moments subset sum: MSS(d)). *Given a set $A = \{a_1, \ldots, a_N\}$, $a_i \in \mathbb{F}$, integer k, and $m_1, \ldots, m_d \in \mathbb{F}$, decide if there exists a subset $S \subseteq A$ of size k, satisfying $M_i(S) = \sum_{a \in S} a^i = m_i$ for all $i \in [d]$. We call k the size of the* MSS(d) *instance.*

In Lemma 2.1 we show a reduction from MSS(d) to RS-BDD(d). We note that this connection has been previously made (e.g., [LW08]).

LEMMA 2.1. MSS(d) *is polynomial-time reducible to RS-BDD(d). Moreover, the reduction maps instances of* MSS(d) *on N numbers and of size k to RS codes of block length $N + 1$ and of dimension $k - d + 1$. The reduction holds over any finite field $\mathbb{F}$ of characteristic larger than d.*

The reduction in the proof of Lemma 2.1 uses the following symmetric subset sum problem, which is equivalent to MSS(d), over large fields.

DEFINITION 2.2 (symmetric subset sum: SSS(d)). *Given a subset $A = \{a_1, a_2, \ldots, a_N\}$ of N distinct elements of $\mathbb{F}$, an integer k, and elements $e_1, e_2, \ldots e_d \in \mathbb{F}$, decide if there exists a subset $S \subseteq A$ of size k such that for every $i \in [d]$, the elementary symmetric sums of the elements of $S = \{s_1, \ldots, s_k\}$ satisfy $E_i(S) = \sum_{1 \le j_1 < j_2 < \cdots < j_i \le k} s_{j_1} \cdots s_{j_i} = e_i$.*

We now describe the reduction from SSS(d) to RS-BDD(d).

LEMMA 2.2. SSS(d) *is polynomial-time reducible to* RS-BDD(d).

Proof. Given an instance $\langle A, k, e_1, e_2, \ldots, e_d \rangle$ of SSS(d), we construct an instance $\langle \mathcal{D}, y, K \rangle$ of RS-BDD(d) such that there exists an RS codeword $p \in RS_{\mathcal{D},K}$ with $\Delta(y, p) \le N - K - d$ iff there is a solution to the given instance of SSS(d). Here, $A = \{a_1, a_2, \ldots, a_N\}$ is a set of distinct nonzero elements of $\mathbb{F}$, $e_1, e_2, \ldots, e_d \in \mathbb{F}$ and $k \in \mathbb{Z}$.

Let $K := k - d + 1$. Define the degree d polynomial $f(x) := x^d - e_1 x^{d-1} + \cdots + (-1)^{d-1} e_{d-1} x$. For each element a_i of A, define an element $y_i \in \mathbb{F}$ as $y_i = -f(a_i)$. Define the target vector $y = (y_1, \ldots, y_N, (-1)^d e_d)$. The set $\mathcal{D}$ is then defined as $\mathcal{D} := \{a_1^{-1}, \ldots, a_N^{-1}, 0\}$. Note that $\langle \mathcal{D}, y, K \rangle$ is an instance of RS-BDD(d) which can be constructed in polynomial time given the instance $\langle A, k, e_1, \ldots, e_d \rangle$ of SSS(d). Let $D := \{(a_i^{-1}, y_i) \text{ for all } a_i \in A\} \cup \{(0, (-1)^d e_d)\}$. Note that an RS codeword $p \in RS_{\mathcal{D},K}$ at a distance at most $N - K - d$ from y corresponds to a univariate polynomial $p(x)$ of degree at most $K - 1$, which agrees with D in at least $K + d$ points.

Let S be a solution to SSS(d). We now show that there exists a polynomial of degree at most $k-d = K-1$ that agrees with D in at least $k+1 = K+d$ points. Define the following degree k polynomial:

$$g(x) := \prod_{a_i \in S} (x - a_i) = c_0 + c_1 x + \cdots + c_{k-1}x^{k-1} + x^k.$$

The coefficients of this polynomial are the symmetric sums of the roots of $g(x)$ (possibly negated), i.e., $c_{k-d} = (-1)^d e_d$, $\ldots$, $c_{k-2} = e_2$ and $c_{k-1} = -e_1$. We now define

$$\begin{aligned} p(x) &:= (x^k g(1/x) - x^d f(1/x))/x^d \\ &= c_0 x^{k-d} + c_1 x^{k-d-1} + \cdots + c_{k-d}. \end{aligned}$$

Note that the polynomial $p(x)$ has degree $k-d$. We point out that $g(1/x)$ refers to the rational function obtained by replacing x by $1/x$ in the polynomial $g(x)$. Also, the constant term of this polynomial is $c_{k-d} = (-1)^d e_d$. Hence, $p(0) = (-1)^d e_d$ and since $g(a_i) = 0$ for all $a_i \in S$, it follows that $p(a_i^{-1}) = -f(a_i) = y_i$ for all $a_i \in S$. Therefore, $p(x)$ agrees with at least $k+1$ points in D.

Conversely, we now show that if there is a polynomial $p(x)$ of degree at most $K-1 = k-d$ which agrees with (at least) $K+d = k+1$ points in D, then there is a solution to SSS(d). We first observe that if a degree $k-d$ polynomial passes through at least $k+1$ points of D, then it has to pass through the point $(0, (-1)^d e_d)$. To show this, assume $p(x)$ agrees with at least $k+1$ points of the form $(a_i^{-1}, y_i) \in D$. Let $g(x)$ be a degree k polynomial defined as

$$g(x) = x^{k-d}(p(1/x) + f(x)).$$

Therefore, if $p(x) = c_0 + c_1 x + \cdots + c_{k-d}x^{k-d}$, then $g(x)$ can be written as

$$g(x) = x^k + e_1 x^{k-1} + \cdots + (-1)^{d-1} e_{d-1} x^{k-d+1} + c_0 x^{k-d} + c_1 x^{k-d-1} + \cdots + c_{k-d}.$$

If $p(a_i^{-1}) = y_i = -f(a_i)$ for $k+1$ points, we have by definition that $g(a_i) = 0$ for these $k+1$ a_i points. This is a contradiction since $g(x)$ has degree at most k and it cannot have $k+1$ roots. Therefore, $p(0) = c_0 = (-1)^d e_d$. Also, $g(x)$ has k roots which have their first d symmetric sums equal to $e_1, e_2, \ldots, e_d$, respectively. Hence, there exists a solution to the given instance of SSS(d). ∎

To complete the proof of Lemma 2.1 we finally show a reduction from MSS(d) to SSS(d).

Claim 2.3. MSS(d) *is polynomial-time reducible to* SSS(d) *over finite fields of characteristic* $> d$.

Proof. By Newton's identities [Sta99] for set S and $j \in [|S|]$, it holds that

$$j \cdot e_j(S) = \sum_{k=1}^{j} (-1)^{k-1} e_{j-k}(S) \cdot M_k(S)$$

(where $e_0 = 1$). Applying them iteratively, we conclude that given an instance $\langle A, k, m_1, \ldots, m_d \rangle$ of MSS(d), one can construct an instance $\langle A, k, e_1, \ldots, e_d \rangle$ of SSS(d) using the transformation

$$e_j = \frac{1}{j!} \begin{vmatrix} m_1 & 1 & 0 & \cdots & \\ m_2 & m_1 & 2 & 0 & \cdots \\ \vdots & & \ddots & \ddots & \\ m_{j-1} & m_{j-2} & \cdots & m_1 & j-1 \\ m_j & m_{j-1} & \cdots & m_2 & m_1 \end{vmatrix} \quad \text{for every } j \in [d].$$

Note that we need that $(j!)^{-1} \in \mathbb{F}$, which holds if $\mathbb{F}$ has characteristic larger than d. Since we also have

$$m_j = (-1)^j \begin{vmatrix} e_1 & 1 & 0 & \cdots & \\ 2e_2 & e_1 & 1 & 0 & \cdots \\ \vdots & & \ddots & \ddots & \\ (j-1)e_{j-1} & e_{j-2} & \cdots & e_1 & 1 \\ je_j & e_{j-1} & \cdots & e_2 & e_1 \end{vmatrix} \quad \text{for every } j \in [d],$$

it follows that a set $S \subset A$ implies a "yes" instance for MSS(d) iff it also implies a "yes" instance for SSS(d). ∎

3. Reduction from 1-in-3-SAT to MSS(d). Recall the 1-in-3-SAT problem in which we are given a 3-SAT formula ϕ on n variables and m clauses and are asked to determine if there exists an assignment $z \in \{0,1\}^n$ satisfying exactly one literal in each clause. It is known that this problem is NP-hard even for $m = O(n)$ [Sch78].

In order to prove Theorem 1.2, we start by describing the reduction from 1-in-3-SAT to MSS(d) and its properties. Henceforth, we denote by 1^ℓ the concatenation of ℓ ones and we let $(1^\ell)_{10}$ denote the positive integer whose decimal representation is 1^ℓ.

Reduction from 1-in-3-SAT to Subset-Sum. We start by recalling the standard reduction from 1-in-3-SAT to Subset-Sum (already discussed in the proof overview in subsection 1.2), which will be used in our reduction to MSS(d). In that reduction, each variable $(z_t, \overline{z_t})$ (with $t \in [n]$) is mapped to two integers a'_t (corresponding to z_t) and b'_t (corresponding to $\overline{z_t}$). The integers a'_t and b'_t and the target m'_1 have the following decimal representation of length $(n+m)$:

- The decimal representations of a'_t and b'_t consist of two parts: a variable region consisting of the leftmost n digits and a clause region consisting of the (remaining) rightmost m digits.
- In their variable regions, a'_t and b'_t have a 1 at the tth digit and 0's at the other digits. We denote the variable part of a'_t (respectively, b'_t) by ${a'_t}^v$ (respectively, ${b'_t}^v$).
- In the clause region, for every $j \in [m]$, a'_t (respectively, b'_t) has a 1 at the jth location if z_t (respectively, $\overline{z_t}$) appears in clause j and a 0 otherwise. We denote the clause part of a'_t (respectively, b'_t) by ${a'_t}^c$ (respectively, ${b'_t}^c$).
- We thus have that $a'_t = 10^m {a'_t}^v + {a'_t}^c$ (and similarly for b'_t).
- The target m'_1 is set to the integer whose decimal representation is the all 1's, i.e., we set $m'_1 = 10^m (1^n)_{10} + (1^m)_{10}$.

See Figure 1 for an illustration of the decimal representations. We now argue that this reduction from 1-in-3-SAT to Subset-Sum is complete and sound. Indeed, given a (1-in-3) satisfying assignment z to the 3-SAT formula ϕ, the subset $S = \{a'_t \mid t \in [n], z_t = 1\} \cup \{b'_t \mid t \in [n], z_t = 0\}$ satisfies

$$\sum_{w \in S} w = \sum_{\substack{t \in [n] \\ z_t = 1}} a'_t + \sum_{\substack{t \in [n] \\ z_t = 0}} b'_t = m'_1.$$

Conversely, a subset $S \subseteq \{a'_t, b'_t \mid t \in [n]\}$ such that $\sum_{w \in S} w = m'_1$ can be used to construct a (1-in-3) satisfying assignment z to ϕ by setting $z_t = 1$ if $a'_t \in S$ and 0 otherwise.

Our reduction from 1-in-3-SAT to MSS(d). Recall that an instance of MSS(d) consists of a tuple $\langle A, k, m_1, \ldots, m_d \rangle$. In our reduction, each variable $(z_t, \overline{z_t})$ is mapped

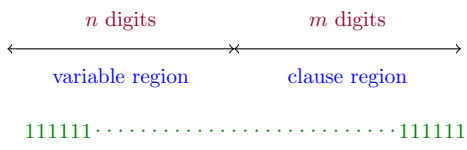

FIG. 1. *Decimal representations in the standard reduction from* 1*-in-*3*-SAT to Subset-Sum.*

to $2^{d+1}-2$ distinct rational numbers: $\{a_t\} \cup \{x_{t,i} \mid i \in [2^d-2]\}$ (corresponding to z_t) and $\{b_t\} \cup \{y_{t,i} \mid i \in [2^d-2]\}$ (corresponding to $\overline{z}_t$). Let $\{a'_t, b'_t \mid t \in [n]\}$ be the integers produced by the above standard reduction from 1-in-3-SAT to Subset-Sum. We denote by ${a'_t}^v$ (respectively, ${a'_t}^c$) the variable (respectively, clause) region of a'_t. Let ν be a natural number to be specified later on. Define

$$\begin{aligned} a_t &:= 10^\nu (10^m {a'_t}^v + {a'_t}^c), \\ b_t &:= 10^\nu (10^m {b'_t}^v + {b'_t}^c). \end{aligned} \tag{12}$$

For each $t \in [n]$, we will explicitly construct two sets of 2^d-2 *auxiliary rational numbers* $X_t = \{x_{t,i} \mid i \in [2^d-2]\}$ and $Y_t = \{y_{t,i} \mid i \in [2^d-2]\}$ which satisfy the following four properties:

Property (1):

$$\sum_{x \in X_t} x = \sum_{y \in Y_t} y = 0.$$

Property (2):

$$\sum_{x \in X_t} x^k - \sum_{y \in Y_t} y^k = b_t^k - a_t^k \text{ for every } k \in \{2, \ldots, d\}.$$

Property (3): For any subset $S \subseteq \bigcup_{t \in [n]} (X_t \cup Y_t)$, either $\left|\sum_{w \in S} w\right| > 10^{m+2n+\nu}$ or $\left|\sum_{w \in S} w\right| < 10^\nu$.

Property (4): Every rational number in the set $\bigcup_{t \in [n]} (X_t \cup Y_t)$ can be written as a fraction whose numerator and denominator are integers of magnitudes at most $10^{\mathsf{poly}(n,d!)}$. Moreover,

$$\left|\bigcup_{t \in [n]} (X_t \cup Y_t)\right| = n \cdot (2^{d+1}-4).$$

Properties (1) and (2) will be used to ensure completeness, Property (3) will be used to ensure soundness and Property (4) will guarantee the polynomial running-time. Constructing such auxiliary rational numbers is the crux of our reduction.

We now define the set $A := \bigcup_{t \in [n]} (\{a_t\} \cup \{b_t\} \cup X_t \cup Y_t)$. We will observe that $|A| = n(2^{d+1}-2)$ by showing that all the numbers $\{a_t\}, \{b_t\}$ and those in X_t and Y_t for $t \in [n]$ are distinct. Let $N := |A| = n(2^{d+1}-2)$ and $k = N/2$. The targets $m_1, \ldots, m_d$ are defined as

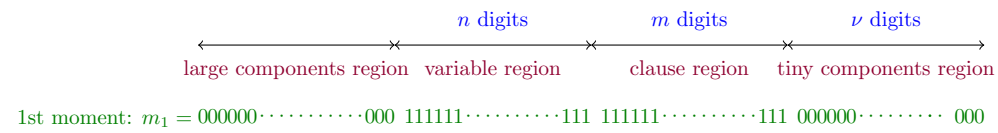

FIG. 2. *Decimal representations in the reduction from* 1-*in*-3-*SAT to* MSS(d). *The "large components region" only contains zeros in* $\{a_t, b_t \mid t \in [n]\}$ *but contains nonzeros in* $\{|x_{t,i}|, |y_{t,i}| \mid t \in [n], i \in [2^d - 2]\}$.

$$
\begin{aligned}
m_1 &:= 10^{\nu}(10^{m}(1^{n})_{10} + (1^{m})_{10}),\\
m_j &:= \sum_{t=1}^{n} a_t^j + \sum_{t=1}^{n} \sum_{x \in X_t} x^j \text{ for every } j \in \{2, \ldots, d\}.
\end{aligned} \tag{13}
$$

Note that a_t (respectively, b_t and m_1) defined above are obtained by inserting ν zeros to the right of the decimal representation of a'_t (respectively, b'_t and m'_1). Therefore, $a_t = 10^{\nu} \cdot a'_t$. Similarly, $b_t = 10^{\nu} \cdot b'_t$ and $m_1 = 10^{\nu} \cdot m'_1$ (see Figure 2 for a pictorial illustration).

The next fact is immediate.

FACT 3.1. *For any* $x \in \{a_t, b_t \mid t \in [n]\} \cup \{m_1\}$, *we have*

$$10^{\nu} < |x| < 10^{m+n+\nu+1}.$$

The next lemma is proved using Property (4) above (and its proof appears in section 4).

LEMMA 3.1. *For any positive integer* d, *the total size of the instance of* MSS(d) *constructed by our reduction is* $N = n \cdot (2^{d+1} - 2)$ *and every rational number has a* $\mathsf{poly}(n, d!)$*-digit representation in base* 10.

In section 3.1, we will show how to construct rational numbers satisfying Properties (1), (2), (3), and (4). The proof of Theorem 1.2 will follow from the next lemma along with Lemma 3.1 above. The proof of Theorem 1.1 will then follow from Theorem 1.2 and Lemma 2.1.

LEMMA 3.2 (main). *There exists a satisfying assignment to a* 1-*in*-3-*SAT instance* $\phi(z_1, \ldots, z_n)$ *iff there exists a subset* $S \subseteq A$ *of size* $|S| = n(2^d - 1)$ *such that for every* $k \in [d]$,

$$\sum_{w \in S} w^k = m_k.$$

We point out that the size requirement on $|S|$ in Lemma 3.2 is needed for the reduction from MSS(d) to RS-BDD(d) given in Lemma 2.1 to hold.

We now give the proof of Theorem 1.2.

Proof of Theorem 1.2. Consider our above reduction from 1-in-3-SAT to MSS(d). Recall that $N = n(2^{d+1} - 2)$ and thus $|S| = |A|/2 = N/2$. From Lemma 3.1 above, we know that every element constructed in the instance of MSS(d) has $\mathsf{poly}(n, d!)$-digit representation. Therefore, for any $d = O(\log n / \log \log n)$, the reduction runs in $\mathsf{poly}(n)$ time.

Let $c > 0$ be any sufficiently small absolute constant. The NP-hardness of MSS(d) for any $d < c \log N / \log \log N$ (under polynomial-time reductions) and for any $d < c \log N$ (under quasi-polynomial-time reductions) over the field of rationals

then follows from Lemma 3.2. By Lemma 3.1 above, we deduce the same hardness results for MSS(d) over prime fields of size $2^{\mathsf{poly}(N)}$. ∎

We now prove Lemma 3.2.

Proof of Lemma 3.2. We start by proving the completeness of our above reduction from 1-in-3-SAT to MSS(d). We show that given any satisfying assignment z to the 1-in-3-SAT instance ϕ, there exists a subset $S \subseteq A$ such that for every $k \in [d]$,

$$\sum_{w \in S} w^k = m_k.$$

Consider the following subset S of the set A:

$$S \triangleq \bigcup_{t \in [n]: z_t = 1} \{a_t\} \bigcup_{t \in [n]: z_t = 1} X_t \bigcup_{t \in [n]: z_t = 0} \{b_t\} \bigcup_{t \in [n]: z_t = 0} Y_t.$$

Note that $|S| = n(2^d - 1) = N/2$ since the number of auxiliary rational numbers included in S corresponding to each $t \in [n]$ is exactly equal to $2^d - 2$.

For every $k \in [d]$, we have that

$$\sum_{w \in S} w^k = \sum_{t \in [n]: z_t = 1} \left(a_t^k + \sum_{x \in X_t} x^k \right) + \sum_{t \in [n]: z_t = 0} \left(b_t^k + \sum_{y \in Y_t} y^k \right). \tag{14}$$

By Property (2) of the auxiliary rational numbers, we have that for any $t \in [n]$ and any $k \in \{2, 3, \ldots, d\}$,

$$\sum_{x \in X_t} x^k - \sum_{y \in Y_t} y^k = b_t^k - a_t^k.$$

Summing this equation over all $t \in [n]$ such that $z_t = 0$, we get that

$$\sum_{t \in [n]: z_t = 0} \left(b_t^k + \sum_{y \in Y_t} y^k \right) = \sum_{t \in [n]: z_t = 0} \left(a_t^k + \sum_{x \in X_t} x^k \right). \tag{15}$$

Combining (14) and (15) above, we conclude that for every $k \in \{2, 3, \ldots, d\}$,

$$\sum_{w \in S} w^k = \sum_{t=1}^{n} \left(a_t^k + \sum_{x \in X_t} x^k \right) = m_k.$$

For $k = 1$, Property (1) implies that for every $t \in [n]$, $\sum_{x \in X_t} x = 0$ and $\sum_{y \in Y_t} y = 0$. Therefore, (14) implies that

$$\sum_{w \in S} w = \sum_{t \in [n]: z_t = 1} a_t + \sum_{t \in [n]: z_t = 0} b_t. \tag{16}$$

Recall the integers a'_t, b'_t, and m'_1 produced by the standard reduction from 1-in-3-SAT to Subset-Sum (defined earlier in this section). Note that $\sum_{t \in [n]: z_t = 1} a'_t + \sum_{t \in [n]: z_t = 0} b'_t = m'_1$. Therefore, we can rewrite (16) as

$$\sum_{w\in S} w = 10^{\nu}\cdot\left(\sum_{t\in[n]:z_t=1} a'_t + \sum_{t\in[n]:z_t=0} b'_t\right) = 10^{\nu}\cdot m'_1 = m_1.$$

We now prove the soundness of our reduction. Let S be any solution to the MSS(d) instance. That is, $S \subseteq A$ is such that $\sum_{w\in S} w^k = m_k$ for every $k \in [d]$. Proposition 3.3 — which is stated below — shows that the auxiliary rational numbers in S should sum to 0. Therefore, there exists a subset $S' \subseteq \{a_t, b_t \mid t \in [n]\}$ such that $\sum_{w\in S'} w = m_1$. By definition of a_t, b_t, and m_1, it follows that there exists a subset of $\{a'_t, b'_t \mid t \in [n]\}$ which sums to m'_1. The soundness of our reduction then follows from the soundness of the standard reduction from 1-in-3-SAT to Subset-Sum. ∎

PROPOSITION 3.3. *Let $S \subseteq A$ be such that $\sum_{w\in S} w = m_1$. Let $D = \bigcup_{t\in[n]}(X_t \cup Y_t)$ be the set of all the auxiliary rational numbers. Then,*

$$\sum\nolimits_{y\in S\cap D} y = 0.$$

Proof. Since $\sum_{w\in S} w = m_1$, we have that

$$\sum_{y\in S\cap D} y + \sum_{w\in S\setminus D} w = m_1.$$

Note that $S \setminus D \subseteq \{a_t, b_t \mid t \in [n]\}$. Since the ν least significant digits of m_1 and those of each element of $S \setminus D$ are all equal to 0, either $|m_1 - \sum_{w\in S\setminus D} w| = 0$ or $|m_1 - \sum_{w\in S\setminus D} w| > 10^{\nu}$. If $|m_1 - \sum_{w\in S\setminus D} w| = 0$, then we are done. Henceforth, we assume that $|m_1 - \sum_{w\in S\setminus D} w| > 10^{\nu}$; we will derive a contradiction. By Fact 3.1, the elements of $S \setminus D$ as well as m_1 all have magnitudes at most $10^{m+n+\nu+1}$. Therefore, $|m_1 - \sum_{w\in S\setminus D} w| \le (2n+1)\cdot 10^{m+n+\nu+1} < 10^{m+2n+\nu}$. On the other hand, by Property (3) of the auxiliary rational numbers, we know that either $|\sum_{y\in S\cap D} y| > 10^{m+2n+\nu}$ or $|\sum_{y\in S\cap D} y| < 10^{\nu}$. Since $|\sum_{y\in S\cap D} y| = |m_1 - \sum_{w\in S\setminus D} w|$, we get a contradiction. Therefore, $\sum_{y\in S\cap D} y = 0$. ∎

3.1. Constructing the sets X_t and Y_t of auxiliary rational numbers. We now show how to construct the auxiliary rational numbers, starting from a_t, b_t described before, for every $t \in [n]$. We do so in Algorithm 1 below, which we call the AUXILIARYVARIABLEGENERATOR. Specifically, for every $t \in [n]$, we construct $2(2^d - 2)$ distinct auxiliary rational numbers which satisfy Properties (1), (2), (3), and (4) stated above. The AUXILIARYVARIABLEGENERATOR outputs the union of the rational numbers generated in Algorithm 2, which we call the ATOMICSOLVER, using the recursive coupling idea described in section 1.2. We use $\mathbf{1}^{\ell}$ (respectively, $\mathbf{0}^{\ell}$) to denote a column vector of ℓ ones (respectively, zeros). For any vector v, let v^T denote its transpose.

We now give the details of ATOMICSOLVER(t, i, $R_{t,i}$) for any $t \in [n]$ and $i \in \{2, 3, \ldots, d\}$. Let $\nu = n^2$. For every $t \in [n], i \in \{2, 3, \ldots, d\}$ and $r \in [i]$, we define the functions $f(t,i) := (i-1)! \cdot \nu_t$ and $g(t,i,r) := (t-1)d^2 + (i-1)i + r$, where ν_t is the tth prime integer greater than n^4. Using the prime number theorem [Sho09], it follows that the number of primes in the interval $[n^4, n^5]$ is larger than n, and thus $\nu_n < n^5$. Since the primes are of size at most n^5, they can be found in deterministic polynomial time using the sieve of Eratosthenes.

We will implement the recursive coupling idea of the ATOMICSOLVER described in section 1.2, in terms of matrix algebra. For example, recall that in the first step

Algorithm 1 AuxiliaryVariableGenerator

Input: $\bigcup_{t\in[n]} \{a_t, b_t\}$

Output: Sets of auxiliary rational numbers X_t, Y_t for every $t \in [n]$.

for $t \in [n]$ **do**
  $X_t = \emptyset$
  $Y_t = \emptyset$
  for $i \in \{2, \dots, d\}$ **do**
    $R_{t,i} = (b_t^i - a_t^i) + \sum_{y\in Y_t} y^i - \sum_{x\in X_t} x^i$
    Let $\{x_{t,i,j} \mid j \in [2^{i-1}]\} \bigcup \{y_{t,i,j} \mid j \in [2^{i-1}]\} =$ AtomicSolver$(t, i, R_{t,i})$
    Let $X_t = X_t \bigcup \{x_{t,i,j} \mid j \in [2^{i-1}]\}$ and $Y_t = Y_t \bigcup \{y_{t,i,j} \mid j \in [2^{i-1}]\}$
  end for
end for

of the variable coupling, we set $x_1 - y_1 = \beta$, $y_2 - x_2 = \beta$, and $x_1 - y_2 = \alpha$. We can then express x_1, x_2, y_1, y_2 as a linear combination of α, β, where we use the extra degree of freedom to choose $x_1 = -x_2$, as follows: $(x_1, x_2)^T = \frac{1}{2}\left[\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right] \cdot (\alpha, \beta)^T$, and $(y_1, y_2)^T = \frac{1}{2}\left[\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right] \cdot (\alpha, \beta)^T$. In general, the polynomial equations give rise to $2^i - 1$ linear constraints on 2^i unknowns $(x_1, \dots, x_{2^{i-1}}, y_1, \dots, y_{2^{i-1}})$. The extra degree of freedom allows us to preserve the symmetry of the solution, which enables us to describe the algorithm and its analysis in a clean form.

Note that for any pair (t, i), the value of $\alpha_{t,i,r}$ for $1 \le r < i$ constructed by AtomicSolver is a power of 10 and hence an integer. However, $\alpha_{t,i,i}$ is a rational

Algorithm 2 AtomicSolver$(t, i, R_{t,i})$

Input: $t, i, R_{t,i}$

Output: Set of auxiliary rational numbers $\{x_{t,i,j} \mid j \in [2^{i-1}]\} \bigcup \{y_{t,i,j} \mid j \in [2^{i-1}]\}$

Let ν_t be the tth prime integer greater than n^4
Let $f(t, i) = (i-1)! \cdot \nu_t$
Let $g(t, i, r) = (t-1)d^2 + (i-1)i + r$ for all $1 < r < i$
Let $\alpha_{t,i,1} = 10^{f(t,i)}$
Let $\alpha_{t,i,r} = 10^{g(t,i,r)}$ for all $1 < r < i$
Let $\alpha_{t,i,i} = R_{t,i}/(i! \prod_{r\in[i-1]} \alpha_{t,i,r})$
Let $\alpha_{t,i} = [\alpha_{t,i,1}, \dots, \alpha_{t,i,i}]^T$
if $i = 2$ **then**
  $A_2 = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$ and $B_2 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$
else
  $A_i = \begin{bmatrix} A_{i-1} & \mathbf{1}^{2^{i-2}} \\ B_{i-1} & -\mathbf{1}^{2^{i-2}} \end{bmatrix}$ and $B_i = \begin{bmatrix} B_{i-1} & \mathbf{1}^{2^{i-2}} \\ A_{i-1} & -\mathbf{1}^{2^{i-2}} \end{bmatrix}$
end if
Let $[x_{t,i,1}, \dots, x_{t,i,2^{i-1}}]^T = \frac{1}{2} \cdot A_i \cdot \alpha_{t,i}$
Let $[y_{t,i,1}, \dots, y_{t,i,2^{i-1}}]^T = \frac{1}{2} \cdot B_i \cdot \alpha_{t,i}$
Return $\{x_{t,i,j} \mid j \in [2^{i-1}]\} \bigcup \{y_{t,i,j} \mid j \in [2^{i-1}]\}$

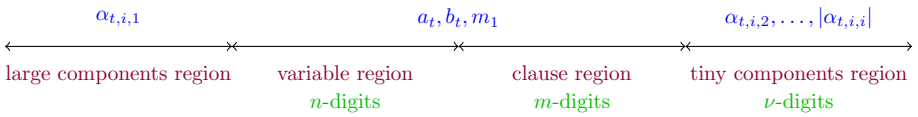

FIG. 3. *Values of $\alpha_{t,i,r}$ for any $i \in \{2, \ldots, d\}$ compared to those of a_t, b_t, and m_1.*

number and might be negative. In section 4 (Proposition 4.6), we will show more concrete bounds on the magnitudes of the $\alpha_{t,i,r}$. Figure 3 shows the magnitudes of $\alpha_{t,i,r}$ for any $i \in \{2, \ldots, d\}$ compared to the values of a_t, b_t, and m_1.

4. Verifying Properties (1), (2), (3), and (4). In this section, we prove that the rational numbers generated by the AUXILIARYVARIABLEGENERATOR (Algorithm 1) satisfy Properties (1), (2), (3), and (4) given in section 3. This is done in Lemmas 4.1, 4.2, and 3.1 (the last of which appeared in section 3 and is restated below).

LEMMA 4.1. *For every $t \in [n]$, the auxiliary rational numbers satisfy the following conditions:*

$$\sum_{x \in X_t} x = \sum_{y \in Y_t} y = 0,$$
$$\sum_{x \in X_t} x^k - \sum_{y \in Y_t} y^k = b_t^k - a_t^k \text{ for every } k \in \{2, \ldots, d\}.$$

LEMMA 4.2. *For any subset $S \subseteq \bigcup_{t \in [n]} (X_t \cup Y_t)$ of the auxiliary rational numbers, either*

$$\left| \sum_{w \in S} w \right| > 10^{m+2n+\nu} \quad \text{or} \quad \left| \sum_{w \in S} w \right| < 10^{\nu}.$$

LEMMA 3.1. *For any positive integer d, the total size of the instance of* MSS(d) *constructed by our reduction is $N = n \cdot (2^{d+1} - 2)$ and every rational number has a* poly$(n, d!)$*-digit representation in base* 10.

In order to prove Lemmas 4.1, 4.2, and 3.1, we first state some properties of the auxiliary rational numbers generated by the ATOMICSOLVER(t, i, $R_{t,i}$) and prove them in section 5.

PROPOSITION 4.4. *For any $t \in [n]$ and any $i \in \{2, \ldots, d\}$,* ATOMICSOLVER*(t, i, $R_{t,i}$), on input a rational $R_{t,i}$, returns two sets of auxiliary rational numbers $\{x_{t,i,j} \mid j \in [2^{i-1}]\}$ and $\{y_{t,i,j} \mid j \in [2^{i-1}]\}$ which satisfy*

$$\sum_{j=1}^{2^{i-1}} (x_{t,i,j}^i - y_{t,i,j}^i) = R_{t,i},$$
$$\sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k) = 0 \text{ for every } k \in \{1, \ldots, i-1\}.$$

PROPOSITION 4.5. *For any $t \in [n]$ and $i \in \{2, 3, \dots, d\}$,*

$$\sum_{j=1}^{2^{i-1}} x_{t,i,j} = \sum_{j=1}^{2^{i-1}} y_{t,i,j} = 0.$$

PROPOSITION 4.6. *For any $t \in [n]$ and any $i \in \{2, \dots, d\}$, we have that*

(a) $i! \cdot \prod_{r=1}^{i} \alpha_{t,i,r} = R_{t,i}$.
(b) $10^{n^4} < \alpha_{t,i,1} < 10^{d! \cdot n^5}$.
(c) $\alpha_{t,i,r} < 10^{n \cdot d^2}$ *for any* $1 < r < i - 1$.
(d) $|\alpha_{t,i,i}| < 2$.
(e) $\sum_{r=2}^{i} |\alpha_{t,i,r}| < 10^{\nu - nd}$.

PROPOSITION 4.7. *For any $t \in [n]$, $i \in \{2, \dots, d\}$ and $j \in [2^{i-1}]$, we have that*

$$10^{(i-1)! \cdot \nu_t} - 10^{\nu - nd} \le 2 \cdot |x_{t,i,j}| \le 10^{(i-1)! \cdot \nu_t} + 10^{\nu - nd}.$$

The same bounds also hold for $y_{t,i,j}$.

PROPOSITION 4.8. *The following statements hold:*

1. *For every $(t_1, i_1, j_1) \neq (t_2, i_2, j_2)$, we have that $x_{t_1,i_1,j_1} \neq x_{t_2,i_2,j_2}$.*
2. *For every $(t_1, i_1, j_1) \neq (t_2, i_2, j_2)$, we have that $y_{t_1,i_1,j_1} \neq y_{t_2,i_2,j_2}$.*
3. *For every $(t_1, i_1, j_1), (t_2, i_2, j_2)$, we have that $x_{t_1,i_1,j_1} \neq y_{t_2,i_2,j_2}$.*

4.1. Proof of Lemma 4.1. We now prove Lemma 4.1, which implies Properties (1) and (2) of the auxiliary rational numbers.

Proof of Lemma 4.1. From Proposition 4.5, we have that for any $t \in [n]$ and $i \in \{2, 3, \dots, d\}$, $\sum_{j=1}^{2^{i-1}} x_{t,i,j} = \sum_{j=1}^{2^{i-1}} y_{t,i,j} = 0$. Summing up this equation over all $i \in \{2, 3, \dots, d\}$, we get

$$\sum_{x \in X_t} x = \sum_{y \in Y_t} y = 0.$$

To prove the second part of Lemma 4.1, note that for any $k \in \{2, \dots, d\}$,

$$\begin{aligned}
\sum_{x \in X_t} x^k - \sum_{y \in Y_t} y^k &= \sum_{i=2}^{d} \sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k) \\
&= \sum_{i=2}^{k-1} \sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k) + \sum_{j=1}^{2^{k-1}} (x_{t,k,j}^k - y_{t,k,j}^k) \\
&\quad + \sum_{i=k+1}^{d} \sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k).
\end{aligned}$$

From the definition of the residual $R_{t,k}$, the first term satisfies

$$\sum_{i=2}^{k-1} \sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k) = b_t^k - a_t^k - R_{t,k}.$$

Also, Proposition 4.4 implies that $\sum_{j=1}^{2^{k-1}} (x_{t,k,j}^k - y_{t,k,j}^k) = R_{t,k}$ and $\sum_{i=k+1}^{d} \sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k) = 0$. Therefore, we conclude that

$$\sum_{x\in X_t} x^k - \sum_{y\in Y_t} y^k = b_t^k - a_t^k.$$

∎

4.2. Proof of Lemma 4.2. Before we prove Lemma 4.2, we note that the auxiliary rational numbers ($x_{t,i,j}$ and $y_{t,i,j}$) are ($\pm\frac{1}{2}$)-linear combinations of $\{\alpha_{t,i,r} \mid r \in [i]\}$ terms. From parts (b) and (c) of Proposition 4.6, we note that every $\alpha_{t,i,r}$ is either of small magnitude, i.e., $|\alpha_{t,i,r}| < 10^{nd^2}$, or of fairly large magnitude, i.e., $\alpha_{t,i,1} > 10^{n^4}$. Also, we note that for every pair $(t,i) \in [n] \times \{2,\ldots,d\}$ there is only one large magnitude term, i.e., $\alpha_{t,i,1}$. Therefore, an auxiliary rational number $x_{t,i,j}$(or $y_{t,i,j}$) is a ($\pm\frac{1}{2}$)-linear combination of one large magnitude term $\alpha_{t,i,1}$ and $i-1$ small magnitude terms.

Recall that D is the set of all the auxiliary rational numbers

$$D = \{x_{t,i,j}, y_{t,i,j} \mid t \in [n], i \in \{2,3,\ldots,d\}, j \in [2^{i-1}]\}.$$

For any auxiliary rational number $z \in D$, we can split z into terms of the form $\pm\frac{1}{2}\alpha_{t,i,r}$ with large magnitude and terms (of the same form) with small magnitudes, namely,

$$z = z_U + z_L,$$

where z_U is the term with large magnitude and z_L is the linear combinations of terms with small magnitudes. We now state and prove two properties of the small magnitude sum and the large magnitude sum which will imply the proof of Lemma 4.2.

CLAIM 4.1. *For any subset $S \subseteq D$, $\sum_{z\in S} z_L < 10^{\nu}$.*

Proof. By the triangle inequality, for any subset $S \subseteq D$,

$$\sum_{z\in S} z_L \le \frac{1}{2}\sum_{t=1}^{n}\sum_{i=2}^{d}\sum_{r=2}^{i}|\alpha_{t,i,r}|.$$

By Proposition 4.6(e), we have that for any $(t,i) \in [n] \times \{2,\ldots,d\}$, $\sum_{r=2}^{i}|\alpha_{t,i,r}| \le 10^{\nu-nd}$. Summing over all (t,i), we get that

$$\sum_{z\in S} z_L \le nd \cdot 10^{\nu-nd} < 10^{\nu}.$$

∎

CLAIM 4.2. *Let $S \subseteq D$ such that $\sum_{z\in S} z_U \neq 0$; then $\left|\sum_{z\in S} z_U\right| \ge \frac{1}{2}\cdot 10^{n^4}$.*

Proof. We show that for any subset of the auxiliary rational numbers, the contribution of the large magnitude terms is either 0 or larger than $\frac{1}{2}\cdot 10^{n^4}$. Note that all the large magnitude terms, i.e., $\alpha_{t,i,1}$ for any (t,i), are powers of 10 whose exponent is larger than n^4 and are therefore divisible by $\frac{1}{2}\cdot 10^{n^4}$. Thus, $\left|\sum_{z\in S} z_U\right|$ is divisible by $\frac{1}{2}\cdot 10^{n^4}$. If it is nonzero, then it is a nonzero multiple of $\frac{1}{2}\cdot 10^{n^4}$ and is hence larger than $\frac{1}{2}\cdot 10^{n^4}$. ∎

The proof of Lemma 4.2 now follows by combining Claims 4.1 and 4.2.

Proof of Lemma 4.2. For any subset $S \subseteq D$, we can split the sum of the rational numbers as

$$\sum_{z\in S} z = \sum_{z\in S} z_U + \sum_{z\in S} z_L.$$

If $\sum_{z\in S} z_U \neq 0$, then from Claims 4.1 and 4.2 we have

$$\left|\sum_{z\in S} z\right| \geq \left|\sum_{z\in S} z_U\right| - \left|\sum_{z\in S} z_L\right|$$
$$\geq \frac{1}{2}\cdot 10^{n^4} - 10^{\nu} = \Omega(10^{n^4}) > 10^{m+2n+\nu} \quad [\text{since } \nu = n^2 \text{ and } m = o(n^4)].$$

On the other hand, if $\sum_{z\in S} z_U = 0$, then from Claim 4.1,

$$\left|\sum_{z\in S} z\right| = \left|\sum_{z\in S} z_L\right| < 10^{\nu}.$$

∎

4.3. Proof of Lemma 3.1.

Proof of Lemma 3.1. In our construction of the instance of MSS(d), we create two integers, a_t and b_t, and $2^{d+1}-4$ auxiliary rational numbers, $X_t \cup Y_t$, corresponding to each of the n literals in the 1-in-3-SAT instance. From Claim 4.6 below, we know that all rational numbers in the set A are distinct. Therefore, the size of the set A in the instance of MSS(d) is $N = n(2^{d+1}-2)$. Now we show that every element constructed in the instance of MSS(d) has a $\mathsf{poly}(n, d!)$-digit representation.

From Fact 3.1, Proposition 4.7 and Claim 4.3 (which is given below), we know that the magnitudes of all the numbers generated by the reduction are bounded by $10^{\mathsf{poly}(n,d!)}$. Therefore, to complete the proof, it remains to show that the magnitudes of denominators of all the rational numbers in the instance of MSS(d) are also bounded by $10^{\mathsf{poly}(n,d!)}$.

We observe from the definitions of a_t and b_t (see (12)) that they are integers for every $t \in [n]$. Also, for any $t \in [n]$ and $i \in \{2,\dots,d\}$, each $\alpha_{t,i,r}$ with $1 \leq r \leq i-1$ and that is constructed by AtomicSolver(t, i, $R_{t,i}$) is a power of 10, and hence an integer, but $\alpha_{t,i,i}$ is a rational number. Each auxiliary rational number generated by AtomicSolver(t, i, $R_{t,i}$) is therefore a rational number due to the contribution from $\alpha_{t,i,i}$. From Claim 4.5 below, it follows that the denominator of every rational number in the instance of MSS(d) has magnitude at most $10^{\mathsf{poly}(n,d!)}$ and therefore has a $\mathsf{poly}(n, d!)$ digit representation. ∎

The following claims bound the magnitudes of various terms in the MSS(d) instance. See Appendix A.1 for their proofs.

Claim 4.3. *For every $k \in \{2,\dots,d\}$,*

$$|m_k| \leq 10^{k\cdot d!\cdot n^6}.$$

We now bound the magnitude of the denominators of $\alpha_{t,i,i}$ for every $(t,i) \in [n]\times\{2,\dots,d\}$. This bound will be used in Claim 4.5 to bound the magnitudes of denominators of all the rational numbers in the instance of MSS(d). Let $D(x)$ denote the magnitude of the irreducible denominator of a rational number x.

Claim 4.4. *For any $(t,i) \in [n]\times\{2,\dots,d\}$,*

$$D(\alpha_{t,i,i}) \leq 10^{(i!)^2\cdot n^6}.$$

Claim 4.5. *For any $x \in A \bigcup \{m_1,\dots,m_d\}$,*

$$D(x) < 10^{\mathsf{poly}(n,d!)}.$$

Claim 4.6. *All rational numbers in the set A are distinct.*

5. Proofs of the helper propositions, Propositions 4.4, 4.5, 4.6, 4.7, 4.8. In this section, we prove the helper propositions stated in the previous section.

We need the following claim in order to prove Proposition 4.4.

CLAIM 5.1. *For any $i \in \{2, \ldots, d\}$, let A_i and B_i be the matrices defined in the description of* ATOMICSOLVER *(Algorithm 2), and let $\{\alpha_r \mid r \in [i]\}$ be rational numbers. If*

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^{i-1}} \end{bmatrix} = \frac{1}{2} \cdot A_i \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_i \end{bmatrix}, \text{ and } \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{2^{i-1}} \end{bmatrix} = \frac{1}{2} \cdot B_i \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_i \end{bmatrix},$$

then $\{x_j \mid j \in [2^{i-1}]\}$ and $\{y_j \mid j \in [2^{i-1}]\}$ satisfy

$$\sum_{j=1}^{2^{i-1}} (x_j^k - y_j^k) = 0 \text{ for every } k \in \{1, \ldots, i-1\},$$
$$\sum_{j=1}^{2^{i-1}} (x_j^i - y_j^i) = i! \cdot \prod_{r=1}^{i} \alpha_r.$$

Proof of Proposition 4.4. We first show a structural property of the auxiliary rational numbers generated by any ATOMICSOLVER. The proof of Proposition 4.4 follows from it.

Note that Claim 5.1 is independent of t and the choice of the α terms. Recall the operation of ATOMICSOLVER$(t, i, R_{t,i})$ for any $(t, i) \in [n] \times \{2, \ldots, d\}$. It returns two sets of auxiliary rational numbers $\{x_{t,i,j} \mid j \in [2^{i-1}]\}$ and $\{y_{t,i,j} \mid j \in [2^{i-1}]\}$ which are constructed using matrices A_i and B_i. Using Claim 5.1, it then follows that these auxiliary rational numbers satisfy

$$\sum_{j=1}^{2^{i-1}} (x_{t,i,j}^i - y_{t,i,j}^i) = i! \cdot \prod_{r=1}^{i} \alpha_{t,i,r},$$
$$\sum_{j=1}^{2^{i-1}} (x_{t,i,j}^k - y_{t,i,j}^k) = 0 \text{ for every } k \in \{1, \ldots, i-1\}.$$

Using Proposition 4.6(a), we get that

$$\sum_{j=1}^{2^{i-1}} (x_{t,i,j}^i - y_{t,i,j}^i) = R_{t,i}.$$

This concludes the proof of Proposition 4.4. ∎

Now it remains to prove Claim 5.1.

Proof of Claim 5.1. We proceed by induction on i. For the base case, consider $i = 2$. From the definition of A_2 and B_2, we get that

$$x_1 = \frac{\alpha_1}{2} + \frac{\alpha_2}{2},$$
$$x_2 = -\frac{\alpha_1}{2} - \frac{\alpha_2}{2},$$

$$y_1 = \frac{\alpha_1}{2} - \frac{\alpha_2}{2},$$
$$y_2 = -\frac{\alpha_1}{2} + \frac{\alpha_2}{2}.$$

Therefore,

$$x_1 + x_2 - y_1 - y_2 = 0,$$
$$x_1^2 + x_2^2 - y_1^2 - y_2^2 = 2 \cdot \alpha_1 \cdot \alpha_2,$$

and the claim thus holds for $i = 2$. We now assume that the induction hypothesis holds for all $i < \ell \leq d$. For $i = \ell$, we have that

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^{\ell-1}} \end{bmatrix} = \frac{1}{2} \cdot A_\ell \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_\ell \end{bmatrix} \text{ and } \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{2^{\ell-1}} \end{bmatrix} = \frac{1}{2} \cdot B_\ell \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_\ell \end{bmatrix}.$$

From the recursive definitions of the matrices A_ℓ and B_ℓ in Algorithm 2, we can split the above equations as

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^{\ell-2}} \end{bmatrix} = \frac{1}{2} \cdot A_{\ell-1} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{\ell-1} \end{bmatrix} + \frac{1}{2} \cdot \begin{bmatrix} \alpha_\ell \\ \alpha_\ell \\ \vdots \\ \alpha_\ell \end{bmatrix},$$
$$\begin{bmatrix} x_{2^{\ell-2}+1} \\ x_{2^{\ell-2}+2} \\ \vdots \\ x_{2^{\ell-1}} \end{bmatrix} = \frac{1}{2} \cdot B_{\ell-1} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{\ell-1} \end{bmatrix} - \frac{1}{2} \cdot \begin{bmatrix} \alpha_\ell \\ \alpha_\ell \\ \vdots \\ \alpha_\ell \end{bmatrix},$$
$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{2^{\ell-2}} \end{bmatrix} = \frac{1}{2} \cdot B_{\ell-1} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{\ell-1} \end{bmatrix} + \frac{1}{2} \cdot \begin{bmatrix} \alpha_\ell \\ \alpha_\ell \\ \vdots \\ \alpha_\ell \end{bmatrix},$$
$$\begin{bmatrix} y_{2^{\ell-2}+1} \\ y_{2^{\ell-2}+2} \\ \vdots \\ y_{2^{\ell-1}} \end{bmatrix} = \frac{1}{2} \cdot A_{\ell-1} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{\ell-1} \end{bmatrix} - \frac{1}{2} \cdot \begin{bmatrix} \alpha_\ell \\ \alpha_\ell \\ \vdots \\ \alpha_\ell \end{bmatrix}.$$

Equivalently, they can be rewritten as

$$x_j = \begin{cases} x'_j + \frac{1}{2} \cdot \alpha_\ell \text{ if } j \leq 2^{\ell-2}, \\ y'_{j-2^{\ell-2}} - \frac{1}{2} \cdot \alpha_\ell \text{ if } j > 2^{\ell-2}. \end{cases} \tag{17}$$

Similarly,

$$y_j = \begin{cases} y'_j + \frac{1}{2} \cdot \alpha_\ell \text{ if } j \leq 2^{\ell-2}, \\ x'_{j-2^{\ell-2}} - \frac{1}{2} \cdot \alpha_\ell \text{ if } j > 2^{\ell-2}, \end{cases} \tag{18}$$

where by the induction hypothesis the elements of $\{x'_j, y'_j \mid j \in [2^{\ell-2}]\}$ satisfy

$$\sum_{j=1}^{2^{\ell-2}} (x'^{k}_{j} - y'^{k}_{j}) = 0 \text{ for every } k \in \{1, \ldots, \ell-2\},$$

$$\sum_{j=1}^{2^{\ell-2}} (x'^{\ell-1}_{j} - y'^{\ell-1}_{j}) = (\ell-1)! \cdot \prod_{r=1}^{\ell-1} \alpha_r.$$

We now use the recursive definitions of x_j, y_j from (17) and (18) and the induction hypothesis to show the following set of equalities:

$$\sum_{j=1}^{2^{\ell-1}} (x_j^k - y_j^k) = 0 \text{ for every } k \in \{1, \ldots, \ell-1\},$$

$$\sum_{j=1}^{2^{\ell-1}} (x_j^\ell - y_j^\ell) = \ell! \cdot \prod_{r=1}^{\ell} \alpha_r.$$

We first use the recursive definitions of x_j, y_j from (17) and (18) to get the equations in terms of x'_j, y'_j. On reordering and massaging the terms a bit, we get that for any $k \in \mathbb{N}$,

$$\begin{aligned}
&\sum_{j=1}^{2^{\ell-1}} (x_j^k - y_j^k) \\
&\quad = \sum_{j=1}^{2^{\ell-2}} \left(\left(x'_j + \frac{1}{2} \cdot \alpha_\ell \right)^k - \left(y'_j + \frac{1}{2} \cdot \alpha_\ell \right)^k \right) \\
&\qquad + \sum_{j=2^{\ell-2}+1}^{2^{\ell-1}} \left(\left(y'_{j-2^{\ell-2}} - \frac{1}{2} \cdot \alpha_\ell \right)^k - \left(x'_{j-2^{\ell-2}} - \frac{1}{2} \cdot \alpha_\ell \right)^k \right) \\
&\quad = \sum_{j=1}^{2^{\ell-2}} \left(\left(x'_j + \frac{1}{2} \cdot \alpha_\ell \right)^k - \left(x'_j - \frac{1}{2} \cdot \alpha_\ell \right)^k \right) \\
&\qquad - \sum_{j=1}^{2^{\ell-2}} \left(\left(y'_j + \frac{1}{2} \cdot \alpha_\ell \right)^k - \left(y'_j - \frac{1}{2} \cdot \alpha_\ell \right)^k \right) \quad \text{(reordering terms)} \\
&\quad = \sum_{j=1}^{2^{\ell-2}} \left(2 \sum_{\substack{r=0 \\ r \equiv 1 \bmod 2}}^{k} \frac{1}{2^r} \cdot \binom{k}{r} x'^{k-r}_{j} \alpha_\ell^r \right) \\
&\qquad - \sum_{j=1}^{2^{\ell-2}} \left(2 \sum_{\substack{r=0 \\ r \equiv 1 \bmod 2}}^{k} \frac{1}{2^r} \cdot \binom{k}{r} y'^{k-r}_{j} \alpha_\ell^r \right) \quad \text{(expanding the terms in the summation)} \\
&\quad = \sum_{j=1}^{2^{\ell-2}} \left(2 \sum_{\substack{r=0 \\ r \equiv 1 \bmod 2}}^{k} \frac{1}{2^r} \cdot \binom{k}{r} \left(x'^{k-r}_{j} - y'^{k-r}_{j} \right) \alpha_\ell^r \right) \\
&\quad = \sum_{\substack{r=0 \\ r \equiv 1 \bmod 2}}^{k} \frac{1}{2^{r-1}} \cdot \binom{k}{r} \left(\sum_{j=1}^{2^{\ell-2}} \left(x'^{k-r}_{j} - y'^{k-r}_{j} \right) \right) \alpha_\ell^r \quad \text{(switching summations)}.
\end{aligned}$$

First, let us consider the case $k \leq \ell - 1$. We will now show that the inner summation is 0 for all $k \leq \ell - 1$. Note that r is an odd integer ranging from 0 to ℓ, hence $r \geq 1$. Therefore, $k - r \leq \ell - 2$. Recall that from the induction hypothesis, we have $\sum_{j=1}^{2^{\ell-2}} (x'^k_j - y'^k_j) = 0$ for every $k \in \{1, \ldots, \ell - 2\}$. This implies that each summation is 0, i.e., $\sum_{j=1}^{2^{\ell-2}} (x'^{k-r}_j - y'^{k-r}_j) = 0$. Hence, it follows that

$$\sum_{j=1}^{2^{\ell-1}} (x_j^k - y_j^k) = 0 \qquad \text{for } k \in \{1, \ldots, \ell - 1\}.$$

Similarly, for $k = \ell$, we note the term corresponding to $r = 1$ is the only surviving term in the summation. The remaining terms corresponding to $r > 1$ in the summation are all 0 by the induction hypothesis.

$$\begin{aligned}
\sum_{j=1}^{2^{\ell-1}} (x_j^\ell - y_j^\ell) &= \sum_{\substack{r=0 \\ r \equiv 1 \bmod 2}}^{\ell} \frac{1}{2^{r-1}} \cdot \binom{\ell}{r} \left(\sum_{j=1}^{2^{\ell-2}} (x'^{\ell-r}_j - y'^{\ell-r}_j) \right) \alpha_\ell^r \\
&= \binom{\ell}{1} \cdot \alpha_\ell \sum_{j=1}^{2^{\ell-2}} (x'^{\ell-1}_j - y'^{\ell-1}_j) \\
&\quad + \sum_{\substack{r=2 \\ r \equiv 1 \bmod 2}}^{\ell} \frac{1}{2^{r-1}} \cdot \binom{\ell}{r} \left(\sum_{j=1}^{2^{\ell-2}} (x'^{\ell-r}_j - y'^{\ell-r}_j) \right) \alpha_\ell^r \\
&= \binom{\ell}{1} \cdot \alpha_\ell \sum_{j=1}^{2^{\ell-2}} (x'^{\ell-1}_j - y'^{\ell-1}_j) \qquad \text{(by induction hypothesis)} \\
&= \ell \cdot (\ell - 1)! \cdot \prod_{r=1}^{\ell-1} \alpha_r \cdot \alpha_\ell \qquad \text{(by induction hypothesis)} \\
&= \ell! \cdot \prod_{r=1}^{\ell} \alpha_r.
\end{aligned}$$

This concludes the proof of Claim 5.1. ∎

Proof of Proposition 4.5. The proof uses the recursive structure of the matrices A_i and B_i. Recall that $\mathbf{1}^\ell$ denotes a vector of ℓ ones and $\mathbf{0}^\ell$ denotes a vector of ℓ zeros. Also recall the definitions of $x_{t,i,j}$ and $y_{t,i,j}$ from Algorithm 2:

$$\begin{bmatrix} x_{t,i,1} & \ldots & x_{t,i,2^{i-1}} \end{bmatrix}^T = \frac{1}{2} \cdot A_i \cdot \begin{bmatrix} \alpha_{t,i,1} & \ldots & \alpha_{t,i,i} \end{bmatrix}^T \qquad \text{and}$$

$$\begin{bmatrix} y_{t,i,1} & \ldots & y_{t,i,2^{i-1}} \end{bmatrix}^T = \frac{1}{2} \cdot B_i \cdot \begin{bmatrix} \alpha_{t,i,1} & \ldots & \alpha_{t,i,i} \end{bmatrix}^T.$$

Therefore, for any $(t, i) \in [n] \times \{2, \ldots, d\}$,

$$\sum_{j=1}^{2^{i-1}} x_{t,i,j} = \frac{1}{2} \cdot (\mathbf{1}^{2^{i-1}})^T \cdot A_i \cdot \begin{bmatrix} \alpha_{t,i,1} & \ldots & \alpha_{t,i,i} \end{bmatrix}^T.$$

Similarly, the sum of all the $\{y_{t,i,j} \mid j \in [2^{i-1}]\}$ can be written as

$$\sum_{j=1}^{2^{i-1}} y_{t,i,j} = \frac{1}{2} \cdot (\mathbf{1}^{2^{i-1}})^T \cdot B_i \cdot \begin{bmatrix} \alpha_{t,i,1} & \ldots & \alpha_{t,i,i} \end{bmatrix}^T.$$

We show by induction on $i \geq 2$ that

$$(\mathbf{1}^{2^{i-1}})^T \cdot A_i = (\mathbf{0}^i)^T \text{ and } (\mathbf{1}^{2^{i-1}})^T \cdot B_i = (\mathbf{0}^i)^T.$$

For the base case $i = 2$, it can be verified that

$$\begin{bmatrix}1 & 1\end{bmatrix} \cdot A_2 = \begin{bmatrix}1 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 1\\ -1 & -1\end{bmatrix} = \begin{bmatrix}0 & 0\end{bmatrix} \text{ and}$$
$$\begin{bmatrix}1 & 1\end{bmatrix} \cdot B_2 = \begin{bmatrix}1 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\end{bmatrix}.$$

We now assume that the induction hypothesis holds for all $i < \ell \leq d$. For $i = \ell$, we observe that

$$\begin{aligned}(\mathbf{1}^{2^{\ell-1}})^T \cdot A_i &= \begin{bmatrix}(\mathbf{1}^{2^{\ell-2}})^T & (\mathbf{1}^{2^{\ell-2}})^T\end{bmatrix} \cdot \begin{bmatrix}A_{\ell-1} & \mathbf{1}^{2^{\ell-2}}\\ B_{i-1} & -\mathbf{1}^{2^{\ell-2}}\end{bmatrix}\\ &= \begin{bmatrix}(\mathbf{1}^{2^{\ell-2}})^T \cdot A_{\ell-1} + (\mathbf{1}^{2^{\ell-2}})^T \cdot B_{\ell-1} & 0\end{bmatrix}.\end{aligned}$$

By the induction hypothesis, we have that $(\mathbf{1}^{2^{\ell-2}})^T \cdot A_{\ell-1} + (\mathbf{1}^{2^{\ell-2}})^T \cdot B_{\ell-1} = (\mathbf{0}^{\ell-1})^T$. Therefore,

$$(\mathbf{1}^{2^{\ell-1}})^T \cdot A_\ell = \begin{bmatrix}\mathbf{0}^{\ell-1} & 0\end{bmatrix}.$$

Similarly,

$$(\mathbf{1}^{2^{\ell-1}})^T \cdot B_\ell = \begin{bmatrix}(\mathbf{1}^{2^{\ell-2}})^T \cdot B_{\ell-1} + (\mathbf{1}^{2^{\ell-2}})^T \cdot A_{\ell-1} & 0\end{bmatrix} = \begin{bmatrix}\mathbf{0}^{\ell-1} & 0\end{bmatrix}.$$

This concludes the proof of Proposition 4.5. ∎

We now show certain bounds on the magnitudes of $\alpha_{t,i,r}$ and hence on the magnitudes of the auxiliary rational numbers $x_{t,i,j}$ and $y_{t,i,j}$. In order to prove Proposition 4.6, we will need the following claim.

CLAIM 5.2. *For any $t \in [n]$, $i \in \{2, \ldots, d\}$ and $j \in [2^{i-1}]$,*

$$|x_{t,i,j} - y_{t,i,j}| = \alpha_{t,i,2}.$$

Proof. We use the recursive matrix definitions given in Algorithm 2 to show that for every $(t, i, j) \in [n] \times \{2, \ldots, d\} \times [2^{i-1}]$, it is the case that

$$|x_{t,i,j} - y_{t,i,j}| = \alpha_{t,i,2}.$$

From the definition of $\{x_{t,\ell,j}, y_{t,\ell,j} \mid j \in [2^{\ell-1}]\}$ given in Algorithm 2, we know that

$$\begin{bmatrix}x_{t,\ell,1}\\ x_{t,\ell,2}\\ \vdots\\ x_{t,\ell,2^{\ell-1}}\end{bmatrix} = \frac{1}{2} \cdot A_\ell \cdot \begin{bmatrix}\alpha_{t,\ell,1}\\ \alpha_{t,\ell,2}\\ \vdots\\ \alpha_{t,\ell,\ell}\end{bmatrix} \text{ and } \begin{bmatrix}y_{t,\ell,1}\\ y_{t,\ell,2}\\ \vdots\\ y_{t,\ell,2^{\ell-1}}\end{bmatrix} = \frac{1}{2} \cdot B_\ell \cdot \begin{bmatrix}\alpha_{t,\ell,1}\\ \alpha_{t,\ell,2}\\ \vdots\\ \alpha_{t,\ell,\ell}\end{bmatrix}.$$

Therefore,

$$\begin{bmatrix}x_{t,\ell,1} - y_{t,\ell,1}\\ x_{t,\ell,2} - y_{t,\ell,2}\\ \vdots\\ x_{t,\ell,2^{\ell-1}} - y_{t,\ell,2^{\ell-1}}\end{bmatrix} = \frac{1}{2} \cdot (A_\ell - B_\ell) \cdot \begin{bmatrix}\alpha_{t,\ell,1}\\ \alpha_{t,\ell,2}\\ \vdots\\ \alpha_{t,\ell,\ell}\end{bmatrix}.$$

From the recursive definition of the matrices $A_\ell = \begin{bmatrix} A_{\ell-1} & \mathbf{1}^{2^{\ell-2}} \\ B_{\ell-1} & -\mathbf{1}^{2^{\ell-2}} \end{bmatrix}$ and $B_\ell = \begin{bmatrix} B_{\ell-1} & \mathbf{1}^{2^{\ell-2}} \\ A_{\ell-1} & -\mathbf{1}^{2^{\ell-2}} \end{bmatrix}$, we get that $A_\ell - B_\ell = \begin{bmatrix} A_{\ell-1} - B_{\ell-1} & \mathbf{0}^{2^{\ell-2}} \\ B_{\ell-1} - A_{\ell-1} & \mathbf{0}^{2^{\ell-2}} \end{bmatrix}$. Therefore, we get the following closed form expression for $A_\ell - B_\ell$:

$$A_\ell - B_\ell = \begin{bmatrix} A_2 - B_2 & \mathbf{0}^2 & \cdots & \mathbf{0}^2 \\ B_2 - A_2 & \mathbf{0}^2 & \cdots & \mathbf{0}^2 \\ & & \vdots & \\ A_2 - B_2 & \mathbf{0}^2 & \cdots & \mathbf{0}^2 \\ B_2 - A_2 & \mathbf{0}^2 & \cdots & \mathbf{0}^2 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 & \cdots & 0 \\ 0 & -2 & 0 & \cdots & 0 \\ & & & \vdots & \\ 0 & 2 & 0 & \cdots & 0 \\ 0 & -2 & 0 & \cdots & 0 \end{bmatrix} \qquad \left(A_2 - B_2 = \begin{bmatrix} 0 & 2 \\ 0 & -2 \end{bmatrix}\right),$$

and therefore for every $j \in [2^{\ell-1}]$,

$$|x_{t,\ell,j} - y_{t,\ell,j}| = \alpha_{t,\ell,2}. \qquad \square$$

We are now ready to prove Proposition 4.6.

Proof of Proposition 4.6.

(a) This follows from the definition of $\alpha_{t,i,i}$ in Algorithm 2.

(b) $\alpha_{t,i,1} = 10^{f(t,i)} = 10^{(i-1)!\nu_t}$, where ν_t is the tth prime greater than n^4. Since ν_t is increasing in t, and since for any fixed t, $\alpha_{t,i,1}$ is increasing in i, we have that $\max_{t,i}\{\alpha_{t,i,1}\} = \alpha_{n,d,1}$ and $\min_{t,i}\{\alpha_{t,i,1}\} = \alpha_{1,2,1}$. As we noted earlier, the prime number theorem implies that the nth prime greater than n^4 has value at most n^5. Therefore,

$$10^{n^4} < 10^{\nu_1} = \alpha_{1,2,1} \le \alpha_{t,i,1} \le \alpha_{n,d,1} = 10^{(d-1)!\cdot\nu_n} < 10^{d!\cdot n^5}.$$

(c) From the definitions given in Algorithm 2, for every $1 < r < i-1$, $\alpha_{t,i,r} = 10^{g(t,i,r)}$. Note that $\max_{t,i,r}\{g(t,i,r)\} = g(n,d,d-1) \le nd^2$ and therefore,

$$\alpha_{t,i,r} \le \alpha_{n,d,d-1} = 10^{g(n,d,d-1)} \le 10^{n\cdot d^2}.$$

(d) and (e) We fix an arbitrary $t \in [n]$. We prove by induction on $i \in \{2,\dots,d\}$ that

$$|\alpha_{t,i,i}| < 2 \text{ and } \sum_{r=2}^{i} |\alpha_{t,i,r}| \le 10^{\nu - nd}. \tag{19}$$

For the base case $i = 2$, we have that $\alpha_{t,2,2} = \frac{b_t^2 - a_t^2}{2\cdot\alpha_{t,2,1}}$. We recall from the definitions of a_t, b_t in (12) that the variable part of a_t is the same as that of b_t. Therefore,

$$|b_t - a_t| \le 10^{m+\nu}. \tag{20}$$

Also, from Fact 3.1, we know that $|a_t|$ and $|b_t|$ are at most $10^{m+\nu+n+1}$. For brevity, let $M := m + \nu + n + 1$. Note that since $m < O(n^3), M = O(n^3)$. So we get that

$$|b_t^2 - a_t^2| = |(b_t - a_t)(b_t + a_t)| \le 10^{m+\nu} \cdot 2 \cdot \max\{a_t, b_t\} < 10^{m+\nu} \cdot 2 \cdot 10^M.$$

Since $m + \nu < M$, we have that

$$|\alpha_{t,2,2}| < \frac{10^{m+\nu} \cdot 2 \cdot 10^M}{2 \cdot 10^{f(t,2)}} < 10^{2M - f(t,2)}.$$

By the definitions given in Algorithm 2, we have that $f(t,2) = \nu_t$ and that ν_t is a prime larger than n^4. Also, we have that $M = O(n^3)$ and $f(t,2) > 2M$. Therefore, it follows that $|\alpha_{t,2,2}| < 1 < 10^{\nu - nd}$ and the bounds in (19) hold for $i = 2$.

We now assume that the induction hypothesis holds for all $i < \ell \le d$, and we prove that it holds for $i = \ell$. We need to show that

$$|\alpha_{t,\ell,\ell}| < 2 \text{ and } \sum_{r=2}^{\ell} |\alpha_{t,\ell,r}| \le 10^{\nu - nd}.$$

We first bound the magnitude of $\alpha_{t,\ell,\ell}$ for any $t \in [n]$. From the definitions given in Algorithm 2, we have that

$$|\alpha_{t,\ell,\ell}| = \frac{|R_{t,\ell}|}{i! \cdot \prod_{r \in [\ell-1]} \alpha_{t,\ell,r}}, \text{ where } R_{t,\ell} = b_t^\ell - a_t^\ell + \sum_{u=2}^{\ell-1} \sum_{v=1}^{2^{u-1}} y_{t,u,v}^\ell - x_{t,u,v}^\ell.$$

We will bound each individual term in the definition of $\alpha_{t,\ell,\ell}$ separately. The term $|b_t^\ell - a_t^\ell|$ in $R_{t,\ell}$ can be factorized as $|b_t^\ell - a_t^\ell| = |(b_t - a_t)(\sum_{k=0}^{\ell-1} b_t^k a_t^{\ell-1-k})|$. As noted earlier in (20), $|b_t - a_t| < 10^{m+\nu} < 10^M$. Also, from Fact 3.1, we have that $\max\{a_t, b_t\} < 10^M$. Thus, we get that

$$\begin{aligned} |b_t^\ell - a_t^\ell| &= \left| (b_t - a_t) \left(\sum_{k=0}^{\ell-1} b_t^k a_t^{\ell-1-k} \right) \right| \\ &< 10^M \cdot \ell \cdot \max\{a_t^{\ell-1}, b_t^{\ell-1}\} \\ &\le 10^M \cdot \ell \cdot 10^{M(\ell-1)} = \ell \cdot 10^{M\ell}. \end{aligned} \tag{21}$$

Using the definitions of $\alpha_{t,\ell,r}$, the denominator in the expression for $\alpha_{t,\ell,\ell}$ can be written as

$$\begin{aligned} \ell! \cdot \prod_{r=1}^{\ell-1} \alpha_{t,\ell,r} &= \ell! \cdot 10^{f(t,\ell) + \sum_{r=2}^{\ell-1} g(t,\ell,r)} \\ &\ge \ell! \cdot 10^{f(t,\ell) + g(t,\ell,2)}. \end{aligned} \tag{22}$$

Now to bound the magnitude of $\left| \sum_{u=2}^{\ell-1} \sum_{v=1}^{2^{u-1}} y_{t,u,v}^\ell - x_{t,u,v}^\ell \right|$, we apply the triangle inequality to obtain

$$\begin{aligned} \left| \sum_{u=2}^{\ell-1} \sum_{v=1}^{2^{u-1}} y_{t,u,v}^\ell - x_{t,u,v}^\ell \right| &\le \sum_{u=2}^{\ell-1} \sum_{v=1}^{2^{u-1}} |y_{t,u,v}^\ell - x_{t,u,v}^\ell| \\ &= \sum_{u=2}^{\ell-1} \sum_{v=1}^{2^{u-1}} \left| (y_{t,u,v} - x_{t,u,v}) \left(\sum_{k=0}^{\ell-1} y_{t,u,v}^k x_{t,u,v}^{\ell-1-k} \right) \right| \\ &\le \sum_{u=2}^{\ell-1} \sum_{v=1}^{2^{u-1}} |(y_{t,u,v} - x_{t,u,v})| \cdot \ell \cdot \max\{|x_{t,u,v}|^{\ell-1}, |y_{t,u,v}|^{\ell-1}\}. \end{aligned}$$

The last inequality follows from the fact that $|x_{t,u,v}|$ and $|y_{t,u,v}|$ are much larger than 1 for all (t,u,v), which was shown in Proposition 4.7. Using Claim 5.2, we know that for any $(t,u,v) \in [n] \times \{2, \ldots, \ell-1\} \times [2^{u-1}]$,

$$|x_{t,u,v} - y_{t,u,v}| = \alpha_{t,u,2} = 10^{g(t,u,2)}.$$

Also, from the construction of the auxiliary rational numbers in Algorithm 2, it follows that for any $t \in [n]$ and $u \in \{2, \dots, d\}$, each $x_{t,u,v}$ and $y_{t,u,v}$ for $v \in [2^{u-1}]$, is a $(\pm\frac{1}{2})$-linear combination of $\{\alpha_{t,u,r} \mid r \in [u]\}$. Therefore,

$$\max\{|x_{t,u,v}|, |y_{t,u,v}|\} \le \frac{1}{2}\sum_{r=1}^{u}|\alpha_{t,u,r}|.$$

Since $u < \ell$, using the induction hypothesis, we know that $\sum_{r=2}^{u}|\alpha_{t,u,r}| < 10^{\nu - nd}$. So, we get that

$$\max\{|x_{t,u,v}|, |y_{t,u,v}|\} \le \frac{1}{2}|\alpha_{t,u,1}| + \frac{1}{2}\sum_{r=2}^{u}|\alpha_{t,u,r}| < \frac{1}{2}(10^{f(t,u)} + 10^{\nu - nd}) < 10^{f(t,u)}.$$

From these observations, we get that

$$\left|\sum_{u=2}^{\ell-1}\sum_{v=1}^{2^{u-1}} y^{\ell}_{t,u,v} - x^{\ell}_{t,u,v}\right| \le \sum_{u=2}^{\ell-1}\sum_{v=1}^{2^{u-1}} 10^{g(t,u,2)} \cdot \ell \cdot (10^{f(t,u)})^{\ell-1}.$$

Note that $\max_{u}\{g(t,u,2)\} = g(t,\ell-1,2)$ and for any fixed t, we have that $f(t,i)$ is increasing in i. Therefore, $f(t,u) \le f(t,\ell-1)$ for all $u \le \ell - 1$. Thus,

$$\left|\sum_{u=2}^{\ell-1}\sum_{v=1}^{2^{u-1}} y^{\ell}_{t,u,v} - x^{\ell}_{t,u,v}\right| \le \ell \cdot 2^{\ell} \cdot 10^{g(t,\ell-1,2)} \cdot 10^{(\ell-1)f(t,\ell-1)}. \tag{23}$$

Combining (21), (22), and (23), we get the following upper bound on the magnitude $\alpha_{t,\ell,\ell}$:

$$\begin{aligned}
|\alpha_{t,\ell,\ell}| &= \frac{|R_{t,\ell}|}{\ell! \cdot \prod_{r=1}^{\ell-1}\alpha_{t,\ell,r}} \\
&\le \frac{|b^{\ell}_t - a^{\ell}_t|}{\ell! \cdot \prod_{r=1}^{\ell-1}\alpha_{t,\ell,r}} + \frac{\left|\sum_{u=2}^{\ell-1}\sum_{v=1}^{2^{u-1}} y^{\ell}_{t,u,v} - x^{\ell}_{t,u,v}\right|}{\ell! \cdot \prod_{r=1}^{\ell-1}\alpha_{t,\ell,r}} \\
&\le \frac{\ell \cdot 10^{M\ell}}{\ell! \cdot 10^{f(t,\ell)+g(t,\ell,2)}} + \frac{\ell \cdot 2^{\ell} \cdot 10^{g(t,\ell-1,2)+(\ell-1)f(t,\ell-1)}}{\ell! \cdot 10^{f(t,\ell)+g(t,\ell,2)}}.
\end{aligned}$$

We now show that each of the two summands in the last equation is less than 1, and thus $|\alpha_{t,\ell,\ell}| < 2$.

The first term can be simplified by plugging in the definition of $f(t,\ell)$ and using the fact that $g(t,\ell,r) > 2$, which yields

$$\frac{\ell \cdot 10^{M\ell}}{\ell! \cdot 10^{f(t,\ell)+g(t,\ell,2)}} < \frac{1}{(\ell-1)!} \cdot 10^{M\cdot\ell - (\ell-1)!\cdot\nu_t - 2}.$$

Since $\ell \cdot M < (\ell-1)! \cdot \nu_t$, it follows that

$$\frac{\ell \cdot 10^{M\ell}}{\ell! \cdot 10^{f(t,\ell)+g(t,\ell,2)}} < 1.$$

For the second term, we note that

$$f(t,\ell) = (\ell-1)! \cdot \nu_t = (\ell-1)\cdot(\ell-2)! \cdot \nu_t = (\ell-1)\cdot f(t,\ell-1)$$

and for any $\ell \geq 2$,

$$g(t,\ell,2) - g(t,\ell-1,2) = 2\ell - 2 \geq 2.$$

Moreover, for any $\ell \geq 2$, we have $2^\ell/(\ell-1)! \leq 4$. Therefore,

$$\begin{aligned}\frac{\ell \cdot 2^\ell \cdot 10^{g(t,\ell-1,2)+(\ell-1)f(t,\ell-1)}}{\ell! \cdot 10^{f(t,\ell)+g(t,\ell,2)}} &= \frac{2^\ell}{(\ell-1)!} \cdot 10^{g(t,\ell-1,2)-g(t,\ell,2)} \cdot 10^{(\ell-1)f(t,\ell-1)-f(t,\ell)} \\ &\leq 4 \cdot 10^{-1} \\ &< 1.\end{aligned}$$

Now that we have established $|\alpha_{t,\ell,\ell}| < 2$, we show that $\sum_{r=2}^{\ell} |\alpha_{t,\ell,r}| < 10^{\nu-nd}$. We split this summation into two terms as follows:

$$\sum_{r=2}^{\ell} |\alpha_{t,\ell,r}| = \sum_{r=2}^{\ell-1} |\alpha_{t,\ell,r}| + |\alpha_{t,\ell,\ell}|.$$

From the definition of $\alpha_{t,\ell,r}$ for $1 < r < \ell$, we have that

$$\sum_{r=2}^{\ell-1} |\alpha_{t,\ell,r}| = \sum_{r=2}^{\ell-1} 10^{g(t,\ell,r)} < 10^{g(t,\ell,\ell-1)+1}.$$

Since $g(t,i,r)$ is increasing in each value of (t,i,r), we have that

$$g(t,\ell,\ell-1) + 1 \leq g(n,d,d-1) + 1 = n \cdot d^2.$$

Recall that $\nu = n^2$, and therefore, for any $d = o(\sqrt{n})$, we have that

$$10^{g(t,\ell,\ell-1)+1} \leq 10^{n\cdot d^2} \leq 10^{\nu-nd-1}.$$

Therefore, it follows that

$$\sum_{r=2}^{\ell} |\alpha_{t,\ell,r}| \leq \sum_{r=2}^{\ell-1} |\alpha_{t,\ell,r}| + |\alpha_{t,\ell,\ell}| < 10^{\nu-nd-1} + 2 < 10^{\nu-nd}.$$

This concludes the proof of Proposition 4.6. ∎

Proof of Proposition 4.7. From the definition of $\alpha_{t,i,r}$ in Algorithm 2, we know that each auxiliary rational number is a $(\pm\frac{1}{2})$-linear combination of $\{\alpha_{t,i,r} \mid r \in [i]\}$, i.e.,

$$x_{t,i,j} = \sum_{r=1}^{i} u_r \cdot \alpha_{t,i,r} \quad \text{with } u_r \in \left\{\pm\frac{1}{2}\right\}.$$

Therefore,

$$\frac{1}{2}\cdot|\alpha_{t,i,1}| - \frac{1}{2}\cdot\sum_{r=2}^{i}|\alpha_{t,i,r}| \leq \left|\sum_{r=1}^{i} u_r \cdot \alpha_{t,i,r}\right| \leq \frac{1}{2}\cdot|\alpha_{t,i,1}| + \frac{1}{2}\cdot\sum_{r=2}^{i}|\alpha_{t,i,r}|.$$

Using Proposition 4.6 (e), we know that $\sum_{r=2}^{i}|\alpha_{t,i,r}| \leq 10^{\nu-nd}$ and recall from definitions given in Algorithm 2 that $\alpha_{t,i,1} = 10^{(i-1)!\cdot\nu_t}$. Therefore,

$$\frac{1}{2}\cdot(10^{(i-1)!\cdot\nu_t} - 10^{\nu-nd}) \leq |x_{t,i,j}| \leq \frac{1}{2}\cdot(10^{(i-1)!\cdot\nu_t} + 10^{\nu-nd}).$$

This concludes the proof of Proposition 4.7. ∎

For any two integral tuples $(p_1, p_2, \ldots, p_d)$ and $(q_1, q_2, \ldots, q_d)$ of the same dimension, we say that $(p_1, p_2, \ldots, p_d) > (q_1, q_2, \ldots, q_d)$ if there is an $i \in [d]$ such that $p_i > q_i$ and $p_j = q_j$ for all $j < i$.

Proof of Proposition 4.8. Let $t_1, t_2 \in [n], i_1, i_2 \in \{2, \ldots, d\}, j_1 \in [2^{i_1} - 1]$, and $j_2 \in [2^{i_2} - 1]$. If $(t_1, i_1, j_1) = (t_2, i_2, j_2)$, then from Claim 5.2, we know that $|x_{t_1,i_1,j_1} - y_{t_1,i_1,j_1}| = \alpha_{t,i,2} \neq 0$ and it follows that $x_{t_1,i_1,j_1} \neq y_{t_1,i_1,j_1}$. We now show that if $(t_1, i_1, j_1) \neq (t_2, i_2, j_2)$, then $x_{t_1,i_1,j_1} \neq x_{t_2,i_2,j_2}$. The proof holds if either or both the $x_{t,i,j}$'s are replaced with $y_{t,i,j}$. Let

$$x_{t_1,i_1,j_1} = u_1 \cdot 10^{(i_1-1)!\cdot\nu_{t_1}} + \sum_{r=2}^{i_1} u_r \cdot \alpha_{t_1,i_1,r} \quad \text{for some } u_r \in \left\{\pm\frac{1}{2}\right\}$$

and

$$x_{t_2,i_2,j_2} = v_1 \cdot 10^{(i_2-1)!\cdot\nu_{t_2}} + \sum_{r=2}^{i_2} v_r \cdot \alpha_{t_2,i_2,r} \quad \text{for some } v_r \in \left\{\pm\frac{1}{2}\right\}.$$

If $x_{t_1,i_1,j_1} = x_{t_2,i_2,j_2}$, then on reordering the terms we get

$$\left|u_1 \cdot 10^{(i_1-1)!\cdot\nu_{t_1}} - v_1 \cdot 10^{(i_2-1)!\cdot\nu_{t_2}}\right| = \left|\sum_{r=2}^{i_2} v_r \cdot \alpha_{t_2,i_2,r} - \sum_{r=2}^{i_1} u_r \cdot \alpha_{t_1,i_1,r}\right|. \tag{24}$$

Note that if $|u_1 \cdot 10^{(i_1-1)!\cdot\nu_{t_1}} - v_1 \cdot 10^{(i_2-1)!\cdot\nu_{t_2}}|$ is nonzero, then using the fact that ν_{t_1} and ν_{t_2} are larger than n^4, we have that

$$\left|u_1 \cdot 10^{(i_1-1)!\cdot\nu_{t_1}} - v_1 \cdot 10^{(i_2-1)!\cdot\nu_{t_2}}\right| \geq 10^{n^4}.$$

But from part (e) of Proposition 4.6, we have that

$$\left|\sum_{r=2}^{i_2} v_r \cdot \alpha_{t_2,i_2,r} - \sum_{r=2}^{i_1} u_r \cdot \alpha_{t_1,i_1,r}\right| \leq \frac{1}{2}\sum_{r=2}^{i_2}|\alpha_{t_2,i_2,r}| + \frac{1}{2}\sum_{r=2}^{i_1}|\alpha_{t_1,i_1,r}| \leq 10^{\nu - nd},$$

which yields a contradiction since $\nu - nd < n^4$. Therefore, the LHS of (24) is 0. Since $u_1, v_1 \in \{\pm\frac{1}{2}\}$, it follows that $u_1 = v_1$. Also, since ν_{t_1} and ν_{t_2} are primes larger than n^4 and $i_1, i_2 \leq d < n$, $(i_1 - 1)!\nu_{t_1} = (i_2 - 1)!\nu_{t_2}$ holds only if $t_1 = t_2$ and $i_1 = i_2$.

Let us assume that $t_1 = t_2 = t$, $i_1 = i_2 = i$, and $j_1 > j_2$. If $x_{t,i,j_1} = x_{t,i,j_2}$, then (24) implies that

$$\sum_{r=2}^{i} (v_r - u_r) \cdot \alpha_{t,i,r} = 0.$$

Since $(v_r - u_r) \in \{0, \pm 1\}$, there exists a $\{0, \pm 1\}$-linear combination of $\alpha_{t,i,r}$ equal to 0. If $u_r = v_r$ for every $r \in \{2, \ldots, i\}$, then $j_1 = j_2$ since each auxiliary rational number is a distinct linear combination of the $\alpha_{t,i,r}$'s. So, there exists at least one $r \in \{2, \ldots, i\}$ such that $u_r \neq v_r$. Let r^* be the largest such r. We know that

$$\begin{aligned}
0 &= \left|\sum_{r=2}^{i} (v_r - u_r) \cdot \alpha_{t,i,r}\right| \\
&= \left|(v_{r^*} - u_{r^*}) \cdot \alpha_{t,i,r^*} + \sum_{r=2}^{r^*-1} (v_r - u_r) \cdot \alpha_{t,i,r}\right| \qquad \text{since } (v_r - u_r = 0 \text{ for } r > r^*) \\
&\geq \left||\alpha_{t,i,r^*}| - |\sum_{r=2}^{r^*-1} (v_r - u_r) \cdot \alpha_{t,i,r}|\right| \qquad \text{since } (|a+b| \geq |\,|a| - |b|\,|).
\end{aligned}$$

Recall that each $\alpha_{t,i,r} = 10^{g(t,i,r)}$ for $r \in \{2, \ldots, i-1\}$ is a distinct power of 10 and $|\alpha_{t,i,i}| < 2$. Since $r^* - 1 < i$, the term $\sum_{r=2}^{r^*-1}(v_r - u_r) \cdot \alpha_{t,i,r}$ is a $\{0, \pm 1\}$ linear combination of different powers of 10. So,

$$2 \leq \left| \sum_{r=2}^{r^*-1} (v_r - u_r) \cdot \alpha_{t,i,r} \right| \leq 2 \cdot 10^{g(t,i,r^*-1)}.$$

Now either $r^* = i$, in which case $|\alpha_{t,i,i}| < 2$, or $r^* < i$, and $|\alpha_{t,i,i}| = 10^{g(t,i,r^*)} \geq 2 \cdot 10^{g(t,i,r^*-1)}$. From these observations, it follows that, $|\alpha_{t,i,r^*}| - \left| \sum_{r=2}^{r^*-1}(v_r - u_r) \cdot \alpha_{t,i,r} \right| \neq 0$, which is a contradiction. Therefore, $j_1 = j_2$. ∎

6. Existence of (inhomogeneous) PTE solutions over general finite fields. Consider a general inhomogenenous PTE system of degree d:

$$\begin{aligned} x_1 + x_2 + \cdots + x_s &= y_1 + y_2 + \cdots + y_s + r_1, \\ x_1^2 + x_2^2 + \cdots + x_s^2 &= y_1^2 + y_2^2 + \cdots + y_s^2 + r_2, \\ &\cdots \\ x_1^d + x_2^d + \cdots + x_s^d &= y_1^d + y_2^d + \cdots + y_s^d + r_d, \end{aligned}$$

where $r_1, r_2, \ldots, r_d$ are arbitrary given field elements, $x_1, \ldots, x_s, y_1, \ldots, y_s$ are the variables, and s is the size of the inhomogeneous PTE solution. Note that this system generalizes the one (†) that plays a key role in our NP-hardness proof for RS decoding. We next show that this system always has a solution (for any field $\mathbb{F} = \mathbb{F}_{p^\ell}$, any $d < |\mathbb{F}|^{1/2-\delta}$, and any $\delta > 0$).

THEOREM 6.1. *Let $\mathbb{F}$ be a finite field, $r_1, r_2, \ldots, r_d \in \mathbb{F}$, and d be a positive integer such that $d \leq |\mathbb{F}|^{1/2-\delta}$. Then, there exists a solution in $\mathbb{F}$ to the system $\{\sum_{i=1}^s x_i^j - \sum_{i=1}^s y_i^j = r_j \ : \ j \in [d]\}$ of size $s = 3d/\delta$.*

In order to prove Theorem 6.1, we start with some definitions that will be useful to us. Let G be an arbitrary finite abelian group and $\mathbb{C}$ be the complex field. An additive character of G is a function $\chi : G \to \mathbb{C}$ such that $\chi(x+y) = \chi(x)\chi(y)$ for all $x, y \in G$. We will now define characters of groups of the form $\mathbb{F}^n$ where $\mathbb{F} = \mathbb{F}_{p^\ell}$ is a finite field with p being a prime integer.

Let $\omega = e^{2\pi i/p}$ be a primitive pth root of unity and let $Tr : \mathbb{F}_{p^\ell} \to \mathbb{F}_p$ be the trace operator which is defined as $Tr(x) = \sum_{i=0}^{\ell-1} x^{p^i}$ for all $x \in \mathbb{F}_{p^\ell}$. Then, an additive character of $\mathbb{F}^n = (\mathbb{F}_{p^\ell})^n$ is $\chi_a(x) = \omega^{Tr(a \cdot x)}$, where $a, x \in \mathbb{F}^n$ and $a \cdot x$ denotes the inner product over $\mathbb{F}^n$. In the particular case where $n = 1$, we denote the character of the field $\mathbb{F}$ corresponding to $a = 1$ by $\chi_1(\cdot)$. For more background on traces and characters, we refer the reader to [LN94].

Let μ be a distribution over vectors in $\mathbb{F}^n$. We denote by $\mu^{(s)}$ the distribution of the sum $x_1 + x_2 + \cdots + x_s$, where the x_i's are sampled independently from μ. We will use the following theorem of Kopparty and Saraf.

THEOREM 6.2 (see [KS13, appendix B]). *Let $\mathbb{F}$ be a finite field and n be a positive integer. Assume that there exists a positive real number β such that every nontrivial character χ of $\mathbb{F}^n$ satisfies*

$$|\mathbb{E}_{x \sim \mu} \chi(x)| \leq \beta.$$

Then,

$$\sum_{x \in \mathbb{F}^n} \left| \mu^{(s)}(x) - \frac{1}{|\mathbb{F}|^n} \right| \leq \beta^s \cdot |\mathbb{F}|^n,$$

and thus, $\mu^{(s)}$ is $(\frac{\beta^s \cdot |\mathbb{F}|^n}{2})$-close to the uniform distribution on $\mathbb{F}^n$ in total variation distance.

We will also use the following result of Deligne, which is a multivariate analogue of the Weil bound [Wei48].

THEOREM 6.3 (Deligne [Del78]). *Let $f(x_1, x_2, \ldots, x_t)$ be a t-variate polynomial over $\mathbb{F}$ of degree at most $|\mathbb{F}|^{1/2-\delta}$ for some $\delta > 0$. Then, either $\chi(f(x_1, x_2, \ldots, x_t))$ is constant or χ satisfies $|\mathbb{E}_{x_1,x_2,\ldots,x_t \in \mathbb{F}} [\chi(f(x_1, x_2, \ldots, x_t))]| \leq |\mathbb{F}|^{-\delta}$.*

Moreover, we will need the following basic lemma.

LEMMA 6.4. *Let $\mathbb{F}$ be any finite field. For every nonzero $a \in \mathbb{F}$ and every $i < \sqrt{|\mathbb{F}|}$, the function $Tr(ax^i)$ is nonconstant (as a function of $x \in \mathbb{F}$).*

Proof. Let $\mathbb{F} = \mathbb{F}_{p^\ell}$, where p is a prime and ℓ is a positive integer. By the definition of the trace function, we have that

$$Tr(ax^i) = ax^i + a^p x^{pi} + a^{p^2} x^{p^2 i} + \cdots + a^{p^{\ell-1}} x^{p^{\ell-1} i}. \tag{25}$$

Since a is a nonzero element of the field $\mathbb{F}$, we have that a^{p^j} is nonzero for each $j \in \{0, \ldots, \ell - 1\}$. Note also that for every $x \in \mathbb{F}_{p^\ell}$ we have that $x^{p^\ell} = x$. Therefore, we can evaluate the right-hand side in (25) by performing the following two steps:

1. For each $j \in \{0, \ldots, \ell-1\}$, the monomial $a^{p^j} x^{p^j i}$ is replaced by the monomial $a^{p^j} x^{e_j}$, where $e_j \in \{0, \ldots, p^\ell - 2\}$ is congruent to $p^j i$ modulo $p^\ell - 1$.
2. While there are two monomials of the form $a_j x^{e_j}$ and $a_{j'} x^{e_{j'}}$ with $e_j = e_{j'}$, we replace them by the monomial $(a_j + a_{j'}) x^{e_j}$.

It is now enough to argue that after step 1, there are more than $\ell/2$ values that are taken by the exponents $e_0, e_1, \ldots, e_{p^\ell - 2}$. This would imply that at least one monomial never gets merged with another monomial in step 2, which would ensure that the final polynomial is not identically equal to zero. We now claim that since $i < p^{\ell/2}$, the exponents $e_0, e_1, \ldots, e_{\ell/2}$ are pairwise distinct. Indeed, $p^j \cdot i \equiv p^k \cdot i \mod p^\ell - 1$ for some $0 \leq j < k \leq \ell/2$ iff $i \cdot p^j \cdot (p^{k-j} - 1) \equiv 0 \mod p^\ell - 1$. Since $i \cdot (p^{k-j} - 1) < p^\ell - 1$, the claim follows, and this concludes the proof of the lemma. ∎

We are now ready to prove Theorem 6.1.

Proof of Theorem 6.1. For $x, y \in \mathbb{F}$, we define $v_{x,y} := (x - y, x^2 - y^2, \ldots, x^d - y^d) \in \mathbb{F}^d$. Let μ be the distribution of $v_{x,y}$ when x, y are distributed independently and uniformly in $\mathbb{F}$. Note that for any nontrivial character χ_a (with $a \in \mathbb{F}^d$ being nonzero), we have

$$\mathbb{E}_{v_{x,y} \sim \mu} [\chi_a(v_{x,y})] = \mathbb{E}[\omega^{Tr(a \cdot v_{x,y})}] = \mathbb{E}_{x,y}[\omega^{Tr(g(x,y))}] = \mathbb{E}_{x,y}[\chi_1(g(x,y))],$$

where $g(x, y) := \sum_{i=1}^d a_i (x^i - y^i)$ is a polynomial of degree $d \leq |\mathbb{F}|^{1/2-\delta}$. By Deligne's Theorem 6.3, we have that either

$$|\mathbb{E}_{v_{x,y} \sim \mu} [\chi_a(v_{x,y})]| = |\mathbb{E}[\chi_1(g(x,y))]| \leq |\mathbb{F}|^{-\delta} \tag{26}$$

or $\chi_1(g(x, y))$ is constant. We now show that for every nonzero $a \in \mathbb{F}^d$, the resulting $\chi_1(g(x, y))$ is nonconstant and hence should satisfy (26). Since a is a nonzero element of $\mathbb{F}^d$, there exists $i^* \in [d]$ such that $a_{i^*} \neq 0$. For every $i \in [d]$ such that $i \neq i^*$, we set $x_i = y_i$. We also set $y_{i^*} = 0$. Under these settings, we get that $Tr(g(x, y)) = Tr(a_{i^*} x^{i^*})$. Applying Lemma 6.4 with $i = i^*$ and $a = a_{i^*}$ now implies that $Tr(g(x, y))$ is nonconstant (i.e., it takes more than one value in $\mathbb{F}_p$). Using the fact that the

map $x \mapsto \omega^x$ is a bijection, we deduce that $\chi_1(g(x,y))$ is nonconstant, and hence it satisfies (26).

Let $\mu^{(s)}$ be the distribution of the sum $\sum_{i=1}^{s} v_{x_i,y_i}$ when we sample s vectors $v_{x_1,y_1}, v_{x_2,y_2}, \ldots, v_{x_s,y_s} \in \mathbb{F}^d$ independently from the distribution μ. Note that $\mu^{(s)}$ is precisely the distribution of the vector

$$\left(\sum_{i=1}^{s} x_i - \sum_{i=1}^{s} y_i, \sum_{i=1}^{s} x_i^2 - \sum_{i=1}^{s} y_i^2, \ldots, \sum_{i=1}^{s} x_i^d - \sum_{i=1}^{s} y_i^d\right)$$

when we sample the x_i's and y_i's independently and uniformly in $\mathbb{F}$.

By Theorem 6.2 and (26), it follows that

$$\sum_{v \in \mathbb{F}^d} \left|\mu^{(s)}(v) - \frac{1}{|\mathbb{F}|^d}\right| \le (|\mathbb{F}|^{-\delta})^s \cdot |\mathbb{F}|^d = |\mathbb{F}|^{-\delta s + d}.$$

Setting $s = 3d/\delta$, we get that $\mu^{(s)}((r_1, r_2, \ldots, r_d)) \ge |\mathbb{F}|^{-d} - |\mathbb{F}|^{-2d} > 0$. We conclude that there exists a solution in $\mathbb{F}$ to the system $\{\sum_{i=1}^{s} x_i^j - \sum_{i=1}^{s} y_i^j = r_j \ : \ j \in [d]\}$ of size $s = 3d/\delta$. ∎

7. Reduction from 1-in-3-SAT to MSS(d) over $\mathbb{F}_{p^\ell}$. For the sake of this reduction, we let p be any prime number larger than d and let $\ell = \mathsf{poly}(n)$. Recall that to construct the field $\mathbb{F}_q = \mathbb{F}_{p^\ell}$, we consider an irreducible polynomial over $\mathbb{F}_p$ of degree ℓ. Let γ be a root of this polynomial in the algebraic closure of $\mathbb{F}_p$. Every element of $\mathbb{F}_q$ is then a linear combination of $1, \gamma, \ldots, \gamma^{\ell-2}, \gamma^{\ell-1}$ over $\mathbb{F}_p$ (we refer to [LN97] for a general treatment of finite fields.). Then, for $v = \sum_{i=0}^{\ell-1} v_i \gamma^i \in \mathbb{F}_q$, we will abuse notation and view v as the vector $(v_1, v_2, \ldots, v_{\ell-1})$. We now define an analogue of the notion of "magnitude" for elements in $\mathbb{F}_q$. Namely, for $v \in \mathbb{F}_q$, we define $|v|$ to be the largest nonzero index $i \in [\ell]$ in the vector representation of v. Note that this definition of magnitude satisfies the property that $|u+v| \le \max(|u|, |v|)$ for every $u, v \in \mathbb{F}_q$ and thus also satisfies the triangle inequality.

We now sketch a proof of the reduction from 1-in-3-SAT to MSS(d) over $\mathbb{F}_{p^\ell}$, which follows analogously to the proof over the field of rationals given in sections 3, 4, and 5 with some small modifications.

An instance of MSS(d) consists of a tuple $\langle A, k, m_1, \ldots, m_d \rangle$. Similar to the reduction over the field of rationals, each variable $(z_t, \overline{z_t})$ is mapped to $2^{d+1}-2$ distinct elements $\{a_t\} \cup \{x_{t,i} \mid i \in [2^d - 2]\}$ (corresponding to z_t) and $\{b_t\} \cup \{y_{t,i} \mid i \in [2^d - 2]\}$ (corresponding to $\overline{z}_t$) which satisfy the following properties:

Property (1):

$$\sum_{x \in X_t} x = \sum_{y \in Y_t} y = 0.$$

Property (2):

$$\sum_{x \in X_t} x^k - \sum_{y \in Y_t} y^k = b_t^k - a_t^k \text{ for every } k \in \{2, \ldots, d\}.$$

Property (3): The set of auxiliary field elements satisfies the "bimodal property." Namely, for any subset $S \subseteq \bigcup_{t \in [n]} (X_t \cup Y_t)$, there exists an L' such that either

$$\left|\sum_{w \in S} w\right| > n^4 + L' \quad \text{or} \quad \left|\sum_{w \in S} w\right| < \nu + L',$$

Now we show how to construct the instance $\langle A, k, m_1, \ldots, m_d \rangle$ of MSS(d) over $\mathbb{F}_q$. Let $\langle \tilde{A}, \tilde{k}, \tilde{m_1}, \ldots, \tilde{m_d} \rangle$ be the instance of MSS(d) obtained from the reduction over the rationals described in section 3. Let us scale the instance by multiplying all the rational numbers in the instance by the LCM L of their denominators. This makes all the elements of the instance an integer. Consider the map $\psi : \mathbb{Z} \to \mathbb{F}_q$ defined as follows: for any $x = \sum_{i \in [\ell]} 10^i x_i \in \mathbb{Z}$, let $\psi(x) = \sum_{i \in [\ell]} \gamma^i x_i = (x_1, \ldots, x_\ell) \in \mathbb{F}_q$. The instance of MSS($d$) over $\mathbb{F}_q$ is then obtained as follows:

- For any $\tilde{w} \in \tilde{A}$, let $w = \psi(L\tilde{w}) \in A \subset \mathbb{F}_q$.
- Let $k = \tilde{k}$.
- $m_k = \psi(L^k \tilde{m_k})$ for every $k \in [d]$.

We note that Properties (1), (2), and (3) of the auxiliary rational numbers described in section 3 can be preserved if we chose p and ℓ to be large enough. Therefore, the auxiliary field elements in the scaled and mapped instance over $\mathbb{F}_q$ now satisfy Properties (1), (2), and (3). The L' in Property (3) refers to the magnitude of $\psi(L)$.

We can then state the analogous statement of Lemma 3.2, which implies the NP-hardness of MSS(d) over $\mathbb{F}_q$.

LEMMA 7.1. *There exists a satisfying assignment to a 3-SAT instance* $\phi(z_1, \ldots, z_n)$ *iff there exists a subset* $S \subseteq A$ *such that for every* $k \in [d]$,

$$\sum_{w \in S} w^k = m_k.$$

The proof of Lemma 7.1 follows from the properties of the auxiliary elements stated above and all the steps of the proof over the field of rationals can be carried over here if we chose p and ℓ large enough, in order to ensure that there is no wrapping around when we add terms with large magnitudes.

8. Conclusion. The main open question that comes up from this work is to explicitly and efficiently construct degree-d PTE solutions of size subexponential in d (Problem 1.1). It would also be very interesting to prove analogous NP-hadness results for BDD of RS codes in the case where preprocessing is allowed. Finally, our NP-hardness results for RS codes apply to the case where the field size is exponential in the block length N; it would be very interesting to prove analogous NP-hardness results for smaller fields.

It would also be interesting to obtain improved hardness results for either MSS(d) or RS-BDD(d) based on the strong exponential time hypothesis, which has been extensively studied in recent work.

Appendix A.

A.1. Missing proofs from section 4.3.

CLAIM 4.3. *For every* $k \in \{2, \ldots, d\}$,

$$|m_k| \leq 10^{k \cdot d! \cdot n^6}.$$

Proof. Recall the definition of m_k from (13):

$$m_k = \sum_{t=1}^{n} a_t^k + \sum_{t=1}^{n} \sum_{x \in X_t} x^k \text{ for every } k \in \{2, \ldots, d\}.$$

Using the bounds on the magnitudes of a_t and $x \in X_t$ given in Fact 3.1 and Proposition 4.7, we get that

$$|m_k| \le n \cdot (10^{k\cdot(m+n+\nu+1)}) + n \cdot 2^d((10^{(d-1)!\cdot\nu_n} + 10^{\nu-nd})^k)$$
$$\le 10^{k\cdot(d!)\cdot n^6}. \qquad \square$$

Recall that $D(x)$ denotes the magnitude of the irreducible denominator of a rational number x.

CLAIM 4.4. *For any* $(t,i) \in [n] \times \{2,\dots,d\}$,

$$D(\alpha_{t,i,i}) \le 10^{(i!)^2\cdot n^6}.$$

Proof. The proof proceeds by first obtaining a recursive expression for $D(\alpha_{t,i,i})$, and then using induction on i to show the desired bound. We recall the definition of $\alpha_{t,i,i}$ from Algorithm 2:

$$\alpha_{t,i,i} = \frac{R_{t,i}}{i! \cdot \prod\limits_{r\in[i-1]} \alpha_{t,i,r}},$$

where $R_{t,i}$ is defined as

$$R_{t,i} = b_t^i - a_t^i + \sum_{u=2}^{i-1}\sum_{v=1}^{2^{u-1}} (y_{t,u,v}^i - x_{t,u,v}^i).$$

Therefore, it follows that the denominator of $\alpha_{t,i,i}$ is upper-bounded by the product of the denominator of $R_{t,i}$ and $i! \cdot \prod_{r=1}^{i-1} \alpha_{t,i,r}$. i.e.,

$$D(\alpha_{t,i,i}) \le D(R_{t,i}) \cdot \left(i! \cdot \prod_{r=1}^{i-1} \alpha_{t,i,r} \right)$$
$$= D(R_{t,i}) \cdot (i! \cdot 10^{(i-1)!\cdot\nu_t + \sum_{r=2}^{i-1} g(t,i,r)})$$
$$\le D(R_{t,i}) \cdot (i! \cdot 10^{(i-1)!\cdot n^5 + n\cdot d^3}).$$

The last inequality follows from the fact that $\sum_{r=2}^{i-1} g(t,i,r) = \sum_{r=2}^{i-1}(t-1)d^2 + (i-1)i + r \le td^3$ for all $2 \le i \le d$ and $\nu_t < n^5$ for any $t \in [n]$. We now obtain an expression for $D(R_{t,i})$. Since b_t and a_t are both integers, note that $D(R_{t,i}) = D\left(\sum_{u=2}^{i-1}\sum_{v=1}^{2^{u-1}}(y_{t,u,v}^i - x_{t,u,v}^i)\right)$. Also, recall that all the auxiliary rational numbers obtained from a given ATOMICSOLVER$(t,\ u,\ R_{t,u})$ (Algorithm 2) are $\pm\frac{1}{2}$ linear combinations of $\{\alpha_{t,u,1}\cdots,\alpha_{t,u,u}\}$. Since $\alpha_{t,u,u}$ is the only rational number among them, each auxiliary rational number obtained from ATOMICSOLVER$(t,\ u,\ R_{t,u})$ will have the same denominator as $D(\alpha_{t,u,u}/2)$, i.e., $D(x_{t,u,v}) = D(y_{t,u,v}) = D(\alpha_{t,u,u}/2) \le 2 \cdot D(\alpha_{t,u,u})$, for all $v \in [2^{u-1}]$. Therefore, $D(y_{t,u,v}^i - x_{t,u,v}^i) \le 2^i \cdot D(\alpha_{t,u,u}^i)$. Thus, it follows that $D(\sum_{v=1}^{2^{u-1}} y_{t,u,v}^i - x_{t,u,v}^i) \le 2^i \cdot D(\alpha_{t,u,u}^i)$, and we get the following expression for $D(R_{t,i})$:

$$D(R_{t,i}) \le LCM(\{2^i \cdot D(\alpha_{t,u,u}^i) \mid u \in \{2,\dots,i-1\}\}) \le 2^i \cdot \prod_{u=2}^{i-1} D(\alpha_{t,u,u}^i).$$

Substituting the above expression for $D(R_{t,i})$ back in to the expression obtained for $D(\alpha_{t,i,i})$, we get

$$D(\alpha_{t,i,i}) \le \left(\prod_{u=2}^{i-1} D(\alpha_{t,u,u}^i)\right) \cdot (2^i \cdot i! \cdot 10^{(i-1)!\cdot n^5 + n\cdot d^3}). \tag{27}$$

We now use induction on i to show that $D(\alpha_{t,i,i}) \le 10^{(i!)^2 \cdot n^6}$ for every $i \in \{2, \dots, d\}$. For the base case $i = 2$, from definition of $\alpha_{t,2,2}$ given in Algorithm 2, we know that

$$D(\alpha_{t,2,2}) = 2 \cdot 10^{\nu_t} < 10^{n^6}.$$

We now assume that the induction hypothesis holds that for all $i < \ell \le d$, i.e., that

$$D(\alpha_{t,i,i}) \le 10^{(i!)^2 \cdot n^6}.$$

From (27), we know that

$$\begin{aligned} D(\alpha_{t,\ell,\ell}) &\le \left(\prod_{u=2}^{\ell-1} D(\alpha_{t,u,u}^{\ell}) \right) \cdot (2^{\ell} \cdot \ell! \cdot 10^{(\ell-1)! \cdot n^5 + n \cdot d^3}) \\ &\le \left(\prod_{u=2}^{\ell-1} (10^{(u!)^2 \cdot n^6})^{\ell} \right) \cdot (10^{(\ell-1)! \cdot n^5 + n \cdot d^3 + \ell^2}) \\ &\le 10^{\ell \sum_{u=2}^{\ell-1} ((u!)^2 \cdot n^6) + (\ell)! n^5 + n d^3 + \ell^2} \\ &\le 10^{\ell \cdot (\ell-1) \cdot (\ell-1)!^2 \cdot n^6 + (\ell)! \cdot n^5 + n \cdot d^3 + \ell^2} \\ &\le 10^{(\ell!)^2 \cdot n^6}, \end{aligned}$$

where the last inequality follows from the fact that $\ell \cdot (\ell-1)!^2 \cdot n^6 > (\ell!) \cdot n^5 + n \cdot d^3 + \ell^2$ for any $\ell \le d$. ∎

CLAIM 4.5. *For any* $x \in A \bigcup \{m_1, \dots, m_d\}$,

$$D(x) < 10^{\mathsf{poly}(n, d!)}.$$

Proof. We first observe that the elements $\{a_t, b_t \mid t \in [n]\}$ obtained from the standard reduction from 1-in-3-SAT to Subset-Sum are all integers. So $D(a_t) = D(b_t) = 1$ for all $t \in [n]$. Next, we show that the magnitudes of denominators of the auxiliary rational numbers are all bounded by $2 \cdot 10^{(d!)^2 \cdot n^6}$. Consider the set of auxiliary rational numbers generated by AtomicSolver$(t,\ i,\ R_{t,i})$ for some $t \in [n]$ and $i \in \{2, 3, \dots, d\}$. Each $x_{t,i,j}$ (or $y_{t,i,j}$) is a $(\pm\frac{1}{2})$-linear combination of the $\{\alpha_{t,i,r} \mid r \in [i]\}$ terms. From the definitions given in Algorithm 2, we note that all $\alpha_{t,i,r}$ terms constructed by the AtomicSolver are integers except for $\alpha_{t,i,i}$. Therefore, each $x_{t,i,j}$ and $y_{t,i,j}$ have the same denominator as $\alpha_{t,i,i}/2$. Using Claim 4.4, we get that for every (t, i), $D(\alpha_{t,i,i,}) \le 10^{(i!)^2 \cdot n^6}$. Therefore, for any $j \in [2^{i-1}]$, $D(x_{t,i,j}) < 2 \cdot 10^{(i!)^2 \cdot n^6}$. A similar argument applies to $y_{t,i,j}$.

We now bound the magnitudes of the denominators of the targets $m_1, \dots, m_d$ defined in the MSS(d) instance. Recall from Definition 13 that m_1 is an integer. Therefore, $D(m_1) = 1$. All other targets are rational numbers defined as

$$m_k = \sum_{t=1}^{n} a_t^k + \sum_{t=1}^{n} \sum_{x \in X_t} x^k \text{ for every } k \in \{2, \dots, d\}.$$

The denominator of m_k is defined by the denominator of the sum $\sum_{t=1}^{n} \sum_{x \in X_t} x^k$. This sum can be expanded as $\sum_{t=1}^{n} \sum_{i=2}^{d} \sum_{j=1}^{2^{i-1}} x_{i,i,j}^k$. From the fact that $D(\sum_{j=1}^{2^{i-1}} x_{t,i,j}^k) \le 2^k D(\alpha_{t,i,i}^k)$ and Claim 4.4, we get

$$\begin{aligned} D(m_k) &\le \prod_{\substack{t\in[n]\\ i\in\{2\ldots,d\}}} 2^k D(\alpha_{t,i,i}^k) \\ &\le \prod_{\substack{t\in[n]\\ i\in\{2\ldots,d\}}} 10^{k(i!)^2\cdot n^6+k} \\ &\le (10^{k(d!)^2\cdot n^6+k})^{nd} \\ &= 10^{\mathsf{poly}(n,d!)}. \end{aligned}$$

Therefore, we conclude that every element of the instance of MSS(d) constructed by our reduction has a denominator of magnitude at most $10^{\mathsf{poly}(n,d!)}$. ∎

CLAIM 4.6. *All rational numbers in the set A are distinct.*

Proof. From Proposition 4.8, we know that all auxiliary rational numbers are distinct. Also, the distinctness of the integers $\{a_t, b_t \mid t \in [n]\}$ follows from the fact that the integers $\{a'_t, b'_t \mid t \in [n]\}$ constructed in standard reduction from 1-in-3-SAT to Subset-Sum are distinct. What remains to be shown is that all the auxiliary rational numbers are different from $\{a_t, b_t \mid t \in [n]\}$.

We show this fact by comparing the magnitudes of the two sets of numbers. From Fact 3.1, we know that $|v| < 10^{m+n+\nu+1}$ for every $v \in \{a_t, b_t \mid t \in [n]\}$, and from Proposition 4.7, we know that the magnitudes of all the auxiliary rational numbers are larger than $10^{\nu_1} - 10^{\nu-nd} > 10^{m+n+\nu+1}$. Therefore, the two sets of numbers are disjoint. ∎

Acknowledgments. We would like to thank Madhu Sudan for very helpful discussions that led to the proof of existence of inhomogeneous PTE solutions over finite fields. We would also like to thank Venkatesan Guruswami, Swastik Kopparty, Sean Prendiville, and Saugata Basu for helpful comments and conversations. We would like to thank Andrew Sutherland and Colin Ingalls for helpful correspondence.

REFERENCES

[ABSS97] S. ARORA, L. BABAI, J. STERN, AND Z. SWEEDYK, *The hardness of approximate optima in lattices, codes, and systems of linear equations*, J. Comput. System Sci., 54 (1997), pp. 317–331.

[BI94] P. BORWEIN AND C. INGALLS, *The Prouhet-Tarry-Escott problem revisited*, Enseign. Math., 40 (1994), pp. 3–27.

[BLP03] P. BORWEIN, P. LISONEK, AND C. PERCIVAL, *Computational investigations of the Prouhet-Tarry-Escott problem*, Math. Comput., 72 (2003), pp. 2063–2070.

[BW86] E. R. BERLEKAMP AND L. R. WELCH, *Error Correction for Algebraic Block Codes*, U.S. Patent 4,633,470, 1986.

[Che08] Q. CHENG, *Hard problems of algebraic geometry codes*, IEEE Trans. Inform. Theory, 54 (2008), pp. 402–406.

[CW07] Q. CHENG AND D. WAN, *On the list and bounded distance decodability of Reed-Solomon codes*, SIAM J. Comput., 37 (2007), pp. 195–209.

[CW10] Q. CHENG AND D. WAN, *Complexity of decoding positive-rate primitive Reed-Solomon codes*, IEEE Trans. Inform. Theory, 56 (2010), pp. 5217–5222.

[Del78] P. DELIGNE, *Aplications de la formule des traces aux sommes trigonometriques, SGA* $4\frac{1}{2}$, Lecture Notes in Math. 569, Springer, New York, 1978.

[Dic13] L. E. DICKSON, *History of the Theory of Numbers, Volume* II: *Diophantine Analysis*, Courier Corporation, North Chelmsford, MA, 2013.

[DKRS03] I. DINUR, G. KINDLER, R. RAZ, AND S. SAFRA, *Approximating CVP to within almost-polynomial factors is NP-hard*, Combinatorica, 23 (2003), pp. 205–243.

[DMS03] I. DUMER, D. MICCIANCIO, AND M. SUDAN, *Hardness of approximating the minimum distance of a linear code*, IEEE Trans. Inform. Theory, 49 (2003), pp. 22–37.

[ES59] P. Erdos and G. Szekeres, *On the product* $\prod_{k=1}^{n}(1-z^{ak})$*, Acad.* Serbe Sci. Publ. Inst. Math, 13 (1959), pp. 29–34.

[FM04] U. Feige and D. Micciancio, *The inapproximability of lattice and coding problems with preprocessing*, J. Comput. System Sci., 69 (2004), pp. 45–67.

[GKS10] P. Gopalan, S. Khot, and R. Saket, *Hardness of reconstructing multivariate polynomials over finite fields*, SIAM J. Comput., 39 (2010), pp. 2598–2621.

[GR08] V. Guruswami and A. Rudra, *Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy*, IEEE Trans. Inform. Theory, 54 (2008), pp. 135–150.

[GRS00] O, Goldreich, R, Rubinfeld, and M, Sudan, *Learning polynomials with queries: The highly noisy case*, SIAM J. Discrete Math., 13 (2000), pp. 535–570.

[GS99] V. Guruswami and M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometry codes*, IEEE Trans. Inform. Theory, 45 (1999), pp. 1757–1767.

[GV05] V. Guruswami and A. Vardy, *Maximum-likelihood decoding of Reed-Solomon codes is NP-hard*, IEEE Trans. Inform. Theory, 51 (2005), pp. 2249–2256.

[Hås01] J. Håstad, *Some optimal inapproximability results*, J. ACM, 48 (2001), pp. 798–859.

[Hua82] L. K. Hua, *Introduction to Number Theory*, Springer, New York, 1982.

[HW79] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, UK, 1979.

[KS13] S. Kopparty and S. Saraf, *Local list-decoding and testing of random linear codes from high error*, SIAM J. Comput., 42 (2013), pp. 1302–1326.

[KV03] R. Koetter and A. Vardy, *Algebraic soft-decision decoding of Reed-Solomon codes*, IEEE Trans. Inform. Theory, 49 (2003), pp. 2809–2825.

[Las09] J. B. Lasserre, *Moments, Positive Polynomials and Their Applications*, Vol. 1, World Scientific, River Edge, NJ, 2009.

[LN94] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, UK, 1994.

[LN97] R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20, Cambridge University Press, Cambridge, UK, 1997.

[LW08] J. Li and D. Wan, *On the subset sum problem over finite fields*, Finite Fields Appl., 14 (2008), pp. 911–929.

[Pet60] W. W. Peterson, *Encoding and error-correction procedures for the Bose-Chaudhuri codes*, IRE Trans. Inform. Theory, 6 (1960), pp. 459–470.

[Pro51] E. Prouhet, *Mémoire sur quelques relations entre les puissances des nombres*, C. R. Acad. Sci. Paris, 33 (1851).

[PV05] F. Parvaresh and A. Vardy, *Correcting errors beyond the Guruswami-Sudan radius in polynomial time*, in Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, Pittsburgh, PA, 2005, pp. 285–294.

[Reg04] O. Regev, *Improved inapproximability of lattice and coding problems with preprocessing*, IEEE Trans. Inform. Theory, 50 (2004), pp. 2031–2037.

[RS60] I. S. Reed and G. Solomon, *Polynomial codes over certain finite fields*, J. SIAM, 8 (1960), pp. 300–304.

[RW14] A. Rudra and M. Wootters, *Every list-decodable code for high noise has abundant near-optimal rate puncturings*, in Proceedings of the Symposium on Theory of Computing, New York, 2014, pp. 764–773.

[Sch78] T. J. Schaefer, *The complexity of satisfiability problems*, in Proceedings of STOC, ACM, 1978, pp. 216–226.

[Sho09] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, UK, 2009.

[Sta99] R P Stanley, *Enumerative Combinatorics*, Vol. 2., Cambridge University Press, Cambridge, UK, 1999.

[Sud97] M. Sudan, *Decoding of Reed Solomon codes beyond the error-correction bound*, J. Complexity, 13 (1997), pp. 180–193.

[Var97] A, Vardy, *Algorithmic complexity in coding theory and the minimum distance problem*, in Proceedings of the 29th Annual ACM Symposium on the Theory of Computing, El Paso, TX, 1997, pp. 92–109.

[Wei48] A. Weil, *Sur les courbes algebriques et les varietes qui s'en deduisent*, Actualities Sci. Ind., 1041, (1948).

[Woo92] T. D. Wooley, *On Vinogradov's mean value theorem*, Mathematika, 39 (1992), pp. 379–399.

[Wri59] E. M. Wright, *Prouhet's* 1851 *solution of the Tarry-Escott problem of* 1910, Amer. Math. Monthly, 66 (1959), pp. 199–201.