Electronic Colloquium on Computational Complexity, Report No. 50 (2021)

Linear Threshold Secret-Sharing with Binary Reconstruction

Marshall Ball[1], Alper Çakan[2], and Tal Malkin[3]

[1]University of Washington
[2]Bogazici University
[3]Columbia University

Abstract

Motivated in part by applications in lattice-based cryptography, we initiate the study of the size of linear threshold ('t-out-of-n') secret-sharing where the linear reconstruction function is restricted to coefficients in $\{0, 1\}$. We prove upper and lower bounds on the share size of such schemes. One ramification of our results is that a natural variant of Shamir's classic scheme [Comm. of ACM, 1979], where bit-decomposition is applied to each share, is optimal for when the underlying field has characteristic 2. Another ramification is that schemes obtained from some monotone formulae are optimal for certain threshold values when the field's characteristic is any constant. We prove our results by defining and investigating an equivalent variant of Karchmer and Wigderson's Monotone Span Programs [CCC, 1993].

We also study the complexity such schemes with the additional requirement that the joint distribution of the shares of any unauthorized set of parties is not only independent of the secret, but also uniformly distributed. This property is critical for security of certain applications in lattice-based cryptography. We show that any such scheme must use $\Omega(n \log n)$ field elements, regardless of the field. Moreover, this is tight up to constant factors for the special cases where any $t = n - 1$ parties can reconstruct, as well as for any threshold when the field characteristic is 2.

1 Introduction

Threshold secret sharing, introduced by Blakley [Bla79] and Shamir [Sha79], allows a dealer to distribute n *shares* of a secret value to n distinct parties, such that any t parties can reconstruct the secret from their shares, but any cohort of fewer than t parties can glean nothing about the secret value. While originally introduced in the context of secure data storage, secret sharing has since found a myriad of applications in cryptography and beyond (e.g., see references in [Bei11]).

A particularly useful and well-understood variant of secret-sharing is *linear* secret-sharing schemes: schemes where the secret is represented as a field element, the shares are comprised of collections of field elements, and any t parties can reconstruct the secret by applying a linear function to the field elements in their shares. A canonical example of a linear secret-sharing scheme is Shamir's scheme [Sha79].[1]

Shamir's scheme enjoys some desirable properties (in addition to linearity): each share is comprised of just a single field element (an optimal share size), and additionally the residual distribution of shares corresponding to any unauthorized set (any $\leq t - 1$ shares) is uniformly distributed. A major drawback of

[1]Recall that to share a secret s in Shamir's scheme, one chooses a random polynomial p of degree $t - 1$, such that $p(0) = s$. The ith share is then simply $p(\alpha_i)$ where $\{\alpha_1, \ldots, \alpha_n\}$ is a set of distinct non-zero values.

ISSN 1433-8092

Shamir's scheme is that it is *not* black-box in the underlying field; it requires the field is at least as large as n. In particular, the reconstruction coefficients may be *arbitrary elements* in this large field.

Another classical linear secret sharing scheme that *is* black-box in the underlying field is that of Benaloh and Leichter [BL88]. Their scheme is recursively defined with respect to any monotone formula computing the access structure (in our case, the t-out-of-n threshold function):

- **Initialization.** Assign the secret, s, to the output wire of the formula
- **Recursion.** Given a (sub)-formula with output labeled s':
  - If the top gate is OR, assign both input wires to that gate s' and recurse on both subformulas,
  - If the top gate is AND, assign left input wire to that gate uniformly random r and the right input wire $s' - r$, and recurse on both subformulas,
  - If the (sub)formula is an input variable, x_i, concatenate s' to the ith share.

This scheme clearly assumes nothing about the underlying field, and hence allows for reconstruction with *binary, or* $\{0, 1\}$*, coefficients*. Unfortunately, we can observe that it does not enjoy the advantages of Shamir's scheme: unauthorized shares are clearly not uniform in general, and moreover the size of shares is comparable to the size of the formula, which can be quite large. For the particular case of $n/2$-out-of-n thresholds, or majority, the smallest known formula is of size $n^{5.3}$ [Val84] (and in fact the smallest bound on *explicit* monotone formulas computing majority gives size approximately n^{5000} [AKS83, Pat90, HMP06]).

In this work, we ask whether it is possible to get the best of both worlds:

(Q1) Are there linear threshold secret sharing schemes that admit small shares *and* reconstruction via binary coefficients?

(Q2) Are there linear threshold secret sharing schemes that are black-box in the underlying field and admit small shares?

(Q3) Moreover, are there such schemes where, additionally, unauthorized shares are uniformly distributed?

With the most general question (Q1) in mind, we initiate the study of *linear threshold secret-sharing with binary reconstruction*, where the coefficients of all linear reconstruction functions are simply 0 and 1 (See Definition 4). That is, the secret can be reconstructed by a sum of some subset of the field elements making up (sufficiently many) shares. In particular, we are interested in the minimum size of the shares for such schemes, quantified in terms of the total number of field elements. We also investigate such schemes which are further required to be black-box in the underlying field, towards answering (Q2). Finally, we investigate the minimum share size of such schemes under the additional requirement from (Q3), that unauthorized sets of shares are uniformly distributed.

While we believe this topic to be natural and interesting in its own right, in Section 1.3 we highlight some surprising applications of such schemes from recent results in lattice-based cryptography.

1.1 Our Results

In this section we discuss our results, and those from folklore, on secret sharing with binary reconstruction.

Karchmer and Wigderson [KW93] observed a tight connection between monotone span programs and linear secret sharing. A *monotone span program* consists of a matrix, M, over some vector space where the rows are labeled by input variables, $x_1, \ldots, x_n$. A monotone span program accepts an input if and only if the rows corresponding to inputs $x_i = 1$ *span* the all ones vector.

Following in the footsteps of [KW93] and much subsequent work on linear secret sharing, we begin by defining restricted models of monotone span programs that are equivalent to the notions of secret sharing we are interested in.

On threshold secret sharing with binary reconstruction. A simple folklore construction of secret sharing with binary reconstruction involves a simple bit-decomposition of Shamir's scheme. In particular, if Shamir's scheme would deal a share $s \in \mathbb{F}_q$ then the share in the modified scheme is $s' = (s, s \cdot 2, s \cdot 2^2, \ldots, s \cdot 2^{\log q - 1})$. To see that such a scheme admits binary reconstruction, suppose Shamir's scheme would require multiplication by reconstruction coefficient α such that $\alpha = \alpha_0 + \alpha_1 \cdot 2 + \alpha_2 \cdot 2^2 + \cdots + \alpha_{\log q - 1} \cdot 2^{\log q - 1}$ (where $\alpha' = (\alpha_0, \alpha_1, \ldots, \alpha_{\log q - 1}) \in \{0,1\}^{\log q}$ is the binary representation of α as an integer), then observe that $\alpha \cdot s = \sum s \cdot \alpha_i \cdot 2^i = \langle \alpha', s' \rangle$.

This yields an upper bound of total share size $O(n \log n)$ for threshold secret sharing with binary reconstruction, but requires a field of size at least n. In contrast, we observe that any such scheme for $1 < t < n$ requires total share size at least $2n - 1$. Resolving the gap between these bounds remains an open problem.

However, for the specific case of secret sharing with binary reconstruction over finite fields with *characteristic 2*, we do arrive at tight bounds. In particular, we show that the optimal total share size of such a scheme is $n \lceil \log_2 n \rceil$. More generally, we observe a lower bound of $n \log_{\mathrm{char}(\mathbb{F})} n$. This indicates that the only hope achieving linear total share complexity must follow the folklore scheme and utilize large characteristic where $\mathrm{char}(\mathbb{F}) = \Omega(n)$.

We conclude by noting that the upper bound for characteristic two, due to Karchmer and Wigderson [KW93], may yield non-trivial results for access structures other than threshold as it makes use of a general connection to monotone-span programs.

On threshold secret sharing that is black-box in the underlying field. As noted above, any linear secret-sharing scheme which is black-box in the underlying field must utilize binary reconstruction (as these are the only two elements guaranteed to exist). Thus, we can deduce from our lower bound of $n \log(n)$ for binary reconstruction with respect to characteristic 2 that any black-box threshold secret-sharing scheme must have total share size at least $n \log n$. Given the existence of schemes at least this efficient for any field, any improvement on this bound must explicitly exploit the fact the black-box nature of the construction.

As mentioned previously for the special case of majority, Benaloh and Leichter's scheme [BL88] when implemented with Valiant's probabilistic construction of a monotone formula for majority [Val84] gives the existence of a black-box linear threshold secret-sharing scheme with total size $O(n^{5.3})$. For the general case, Bopanna [Bop85] gave a probabilistic construction of monotone formulas computing t-out-of-n Threshold functions that yields total share size $O((\min\{t, n-t\})^{4.3} n \log n)$. To our knowledge, no fully-explicit scheme of comparable size is known.

We observe that it may be possible to improve on these upper-bounds if one start from small *series-parallel undirected contact networks* (See Definition 5) for the threshold function, which are potentially smaller than corresponding monotone-formula. Explicit undirected contact networks without the series-parallel restriction are known to beat Bopanna's bound. Additionally, as is the case with [BL88], this connection applies for arbitrary access structures, beyond threshold.

On uniformly-distributed unauthorized shares in threshold secret sharing with binary reconstruction. Note that neither the folklore construction specified above nor that of Benaloh and Leichter yield schemes with uniformly distributed unauthorized shares. Do such schemes exist?

Yes, in fact, we prove that Karchmer and Wigderson's scheme for characteristic 2 [KW93] indeed yields uniformly distributed unauthorized shares (with total share size $O(n \log n)$). Recall that we showed this is tight for the case of characteristic 2.

More generally, we show general connections between share size of black-box secret sharing schemes with uniform unauthorized shares and the complexity of the access structure in restricted computation models (see Section 1.2). We observe that constructions in these models yield an upper bound on total share size for threshold secret sharing of $\min\{\binom{n}{t}t, \binom{n}{t-2}t(n-t)\log(n-t)\}$.

Using extremal set theory (and, alternately, graph theory) we show a general lower bound of $\Omega(n \log n)$ on total share size of threshold schemes with binary reconstruction and uniform unauthorized shares for *any underlying field*. Recall that if unauthorized shares may be arbitrarily distributed, we only know comparable bounds for fields with *constant* characteristic.

Unfortunately, there is an exponential gap between we these bounds for large t. We show that significantly improving *either* the upper bound *or* the lower bound will require different techniques.

To this end, we give an independent construction for the special cases of 2-out-of-n and $(n-1)$-out-of-n threshold secret sharing that is tight, i.e. optimal share size for these cases is $\Omega(n \log n)$.

Our results are summarized in the following table.

0,1 Recons	Unauth-uniform	Lower	Upper	Remarks
	✓	n [KW93]	n [KW93]	Upper bound requires $\lvert\mathbb{F}\rvert \geq n+1$ and $1 < t < n$
✓		$\max\{n \log_{char(\mathbb{F})}(n), 2n-1\}$	$O((\min\{t, n-t\})^{4.3} n \log(n))$ [HRS93]	$1 < t < n$
✓		$\Omega(n \log(n))$	$O(n \log(n))$ [KW93]	$char(\mathbb{F}) = 2$ and $1 < t < n$
✓	✓	$\Omega(n \log(n))$	$O(n \log(n))$	$char(\mathbb{F}) = 2$ and $2 < t < n$
✓		$\Omega(n \log(n))$	$O((\min\{t, n-t\})^{4.3} n \log(n))$ [HRS93]	$char(\mathbb{F}) = O(1)$ and $1 < t < n$
✓	✓	$\Omega(n \log(n))$	$\min\{O(\binom{n}{t-2}t(n-t)\log(n-t)), \binom{n}{t}t)\}$	$2 < t < n$
✓	✓	$\Omega(n \log(n))$	$O(n \log(n))$	$t = n-1$

1.2 Technical Overview

As discussed above, in this paper, we introduce two new models of linear secret sharing schemes with perfect privacy, motivated by applications in lattice based cryptography. In the first one, we are restricting the linear reconstruction functions to use coefficients only from a fixed, small set. While both for generality and for ease in some of the proofs, we define the model in a general way to allow for any set here, we will mostly be interested in the case where this set is $\{0, 1\}$. In the second model, we impose the additional the requirement that the joint distribution of the shares of any unauthorized set of parties be uniform. While we also prove some general results about these models, our main focus will be computing the threshold functions in these models. For both models, we are concerned with the total number shares (field elements) distributed to the parties. To show upper and lower bounds for this quantity, we use the following equivalence.

1.2.1 Equivalence to a New Span Program Model

Following a track similar to the existing linear secret sharing schemes literature, we define new variations of the monotone span program model and prove that these are equivalent to the new secret sharing models. The first model we define requires that any *authorized* submatrix be able to span the fixed target only using a fixed set of span coefficients. However, note that the requirement that the *unauthorized* submatrices cannot span the target vector stay the same, that is, it has to hold for any span without restrictions to the coefficients. In the second model, we further add the *uniformity* requirement that any *unauthorized* submatrix have full row rank. We extend the well-known equivalence between linear secret sharing schemes with perfect privacy and monotone span programs to show that both the coefficients and the uniformity are preserved.

1.2.2 Upper Bounds

While our focus will be on lower bounds, we explore some upper bounds for the case of coefficient set $\{0, 1\}$, in order to show that some of our lower bounds are tight. We define two new contact network variations that lead to upper bounds for our monotone span programs, and hence for our secret sharing models. The first model requires that the graph underlying the contact network be a series-parallel graph. We observe that the contact network to span program construction of [KW93] leads to coefficients $\{0, 1\}$. The second contact network model we define further requires that the subgraph be acylic when the input is unauthorized. We show that the same construction from this model yields uniform restricted span programs. We further define a new *non-local* monotone formula model that forbids computing disjunction of small conjunctions. We show that, for the case of threshold function, converting this type of formula to a contact network using the known conversion gives us a network with the acyclicity property defined above. We show upper bounds for this formula model that utilizes an existing explicit formula construction for the special case of $t = 2$. We further show some lower bounds by using extremal combinatorics regarding intersections of fixed size subsets of a set and proving that such a model has to have distinct subtrees/subformulae computing almost all subsets of $[n]$. Our lower bounds show that the upper bounds we give are close to optimal.

We finally show that *decomposing* a program is the optimal method when we want to restrict the coefficients to a subset that is a subfield, even when we working with the stronger uniform model. This implies a tight lower bound for the case where the field characteristic does not grow with the number of parties and the threshold value is constant.

1.2.3 Lower Bounds

Our lower bounds are in two cases. For the general case, we first show a new canonical span program definition that conforms to our new span program models, and then show that the size preserving conversion into the canonical model also preserves the coefficient set. Then, we prove that there is a size-preserving conversion that lets us switch the coefficient set with the matrix entry set, at the cost of taking the *dual* of the computed function. Using these results, we show that the subfield decomposition method is optimal, as mentioned above. For the uniform case, we show a field independent $n \log_2(n)$ lower bound for computing any threshold function ($2 < t < n$) in the *uniform* span program model. We do this by showing that that if we can find a large family of authorized subsets of parties that have a fixed core subset and have large pairwise intersections, then the total share size must also be large or else we can find cancellations in span equations, which leads to a violation of the uniformity. We start with a primitive version of the argument that gives the lower bound for some cases and then make it more flexible in the next step. Then, we go on to show lower bounds for various threshold values. Finally, we show that a single, condensed and graph-theoretic argument can show the same lower bound for (almost) all threshold values. Finally, using Ahlswede-Khachatrian Complete Intersection Theorem [AK97] we also show that the proof technique we present cannot give a lower bound that is asymptotically better than the one shown here. More specifically for the case where the coefficient set is $\{0, 1\}$, the lower bound we give matches the upper bound we give above for any threshold value and a field of characteristic 2 or any field with threshold value $t = n - 1$. This shows that the bound we give is optimal for both threshold-independent and field-agnostic lower bounds.

1.3 Secret Sharing with Binary Reconstruction in Lattice-Based Cryptography

We describe two recent applications of linear threshold secret sharing in lattice-based cryptography that require such restrictions on reconstruction coefficients. The first highlights the utility of binary reconstruction coefficients, and the second highlights the additional utility of requiring unauthorized shares to be uniformly distributed. Understanding the share size of such schemes has immediate ramifications to the efficiency of such constructions. We additionally anticipate that schemes admitting such simple reconstruction will find applications beyond those presented here.

Threshold Cryptosystems. Threshold cryptography is taken to refer to a family of objects where a cryptographic secret is shared amongst n servers in such a manner that if any t servers come together they can accomplish a task, but security is preserved so long as less than t servers are corrupted. Boneh et al. [BGG$^+$18] construct Threshold Fully Homomorphic Encryption (TFHE), a primitive that was effectively complete for threshold cryptography in general. In TFHE, an encryption key is made public and n parties are given shares an associated decryption scheme. Given data encrypted under public key, each party can *independently* perform a computation on the encrypted data, homomorphically, before using their share of the decryption key to perform a "partial decryption." Any t partial decryptions can be combined to recover the result of computation in the clear and semantic security holds even if an adversary corrupts $t-1$ parties. An important property is compactness: the size of ciphertext is independent of the number of decryptors and does not grow with complexity of homomorphic computation. (Without compactness there are trivial solutions.)

Boneh et al. [BGG$^+$18] showed TFHE schemes could be constructed from the Learning with Errors assumption (LWE), and since publication numerous further applications have been found in situations requiring secure computation with limited interaction. The authors, in fact, gave two constructions of TFHE from LWE, both relying on linear secret sharing. At a high level, both schemes take advantage of the fact that decryption in LWE-based FHE schemes is effectively an inner product between the secret key and the ciphertext. As such, the natural thing to do is secret-share the secret key using a linear secret sharing scheme and perform the inner products locally with each share of the key and simply perform linear reconstruction on the resulting partial decryptions. The problem is that taking an inner product does not immediately decrypt, but instead yields the plaintext plus some small noise. Thus, if the linear reconstruction function has large coefficients, this noise will not remain small and hence the "reconstructed noise" may occlude the reconstructed plaintext.

Boneh et al. propose to get around this by using schemes that only use binary reconstruction coefficients. The authors conclude by observing that such a scheme exists for any access structure computable by monotone Boolean formulas (including threshold functions) – the Benaloh and Leichter [BL88] scheme we described above. Unfortunately, as also noted above, this results in a scheme where the share size scales polynomially with the circuit size. Consequently, this also leads to large keys in the TFHE scheme, and comparatively high noise growth. Hence, any improvement to linear threshold secret-sharing with binary reconstruction will immediately result in an improved TFHE scheme.

Boneh et al. additionally proposed a solution that uses Shamir's scheme as is and instead modified the noise distribution of a specific FHE scheme. Unfortunately, the resulting ciphertext is not immediately compact and thus requires further compilation with a non-threshold FHE scheme. As a result, new ideas are needed to yield a scheme with practical parameters.

Fuzzy Identity-Based Encryption and Attribute-Based Encryption. Attribute-Based Encryption (ABE) is a public-key encryption scheme with fine-grained access control. Unlike in a traditional public-key encryption, in ABE an authority can issue secret keys bound to predicates, sk_P, associated with some single public key, pk. Given a encryption of m (encrypted under pk), a party holding sk_P can recover m if and only if $P(m) = 1$. Fuzzy Identity-Based Encryption (Fuzzy IBE) refers to the specific case that the family of allowable predicates are restricted to threshold functions.

Prior to 2013 [Boy13, GVW13]), ABE schemes for NC^1 were known from pairing-based assumptions, but not lattice-based assumptions. As outlined in [ABV$^+$12, Appendix B], a tempting paradigm for achieving such an object involved viewing the predicate P as specifying an access structure for a linear secret sharing scheme and sampling LWE trapdoors with the shares baked in, which in turn allow decryption when the receiver is holding authorized shares for the message. We refer the reader to [ABV$^+$12, Appendix B] for details, but the reason this goes awry is for similar reasons to the above. Correctness is not achieved due to noise growth when the reconstruction coefficients are large. Thus, small reconstruction coefficients are needed. However, in this case the classic scheme of [BL88] does not yield a secure ABE via the recipe of [ABV$^+$12], because unauthorized sets of shares may contain correlations that damage the LWE security. If the secret sharing scheme has the additional property that unauthorized shares are uniformly distributed, the scheme is secure.

Agrawal et al. [ABV$^+$12] invoke this recipe with Shamir's scheme to construct Fuzzy IBE, however to deal with the large reconstruction coefficient in Shamirs scheme, they are required to modify the noise distribution (in a similar manner to the second TFHE construction of [BGG$^+$18]). The resulting scheme consequently requires a larger base field ($(\ell!)^2$ times larger, where ℓ is the length of an "identity"). Consequently, linear secret sharing with binary coefficients and uniformly distributed unauthorized shares immediately yields practical improvements to Fuzzy IBE from LWE.

2 Preliminaries

Notation. Unless otherwise specified, any column or row representation of a vector is according to the standard basis of $\mathbb{F}^d$ for the appropriate value of d. Similarly, any matrix $M_{k\times\ell}$ is a representation over the standard bases of $\mathbb{F}^k$ and $\mathbb{F}^\ell$. For a matrix $M_{k\times\ell}$ over a field $\mathbb{F}$, and a subset $A \subset \mathbb{F}$, $\mathrm{Rowspan}_A(M)$ denotes the set $\{vM | v \in A^{1\times k}\}$. When $\mathbb{F}$ is clear from the context and $A = \mathbb{F}$, we will drop the subscript.

By $\mathbf{1}$ ($\mathbf{0}$), we denote the unique row vector whose entries are all ones (zeroes) in the implicit basis of appropriate dimension, and its dimension will be clear from the context.

We will consider elements of $\{0,1\}^n$ and subsets of $[n]$ interchangeably in the natural way. Th_n^t denotes the t-out-of-n threshold function, i.e, the function $Th_n^t : \{0,1\}^n \to \{0,1\}$ where $Th_n^t(x) = 1$ if and only if $|x| \geq t$. For any set A, $x \in A^n$ and $i \in [n]$, x_i denotes the i^{th} component of x.

We show the degree of a field extension $\mathbb{F}$ over $\mathbb{L}$ as $|\mathbb{F} : \mathbb{L}|$.

The following generalizes the span program model of [KW93].

Definition 1. Fix a field $\mathbb{F}$ and two sets $A, B \subseteq \mathbb{F}$. A *restricted span program over* $(\mathbb{F}, A, B)$ is a labeled matrix $\hat{M}(M, \rho)$ where $M_{k\times\ell}$ is a matrix over $\mathbb{F}$ with entries only in A and $\rho : \mathrm{rows}(M) \to \{x_i^\epsilon | i \in [n], \epsilon \in \{0,1\}\}$. For any $v \in \{0,1\}^n$, M_v denotes the submatrix consisting of rows $r \in \mathrm{rows}(M)$ such that $\rho(r) = x_i^\epsilon$ with $\epsilon = v_i$ for some $i \in [n]$.

We say that $\hat{M}$ computes $f : \{0,1\}^n \to \{0,1\}$ if for all $x \in \{0,1\}^n$,

$$\begin{cases} \mathbf{1} \in \mathrm{Rowspan}_B(M_x), & \text{if } f(x) = 1 \\ \mathbf{1} \notin \mathrm{Rowspan}_{\mathbb{F}}(M_x), & \text{if } f(x) = 0 \end{cases}$$

We define $\mathrm{size}(\hat{M})$ to be the number of rows in M, $\mathrm{rows}(\hat{M}, i)$ to be the rows of $i \in [n]$, that is, $\{r \in \mathrm{rows}(M) | \rho(r) = x_i^\epsilon \text{ for some } \epsilon \in \{0,1\}\}$, and $\mathrm{rowcount}(\hat{M}, i)$ to be $|\mathrm{rows}(\hat{M}, i)|$. More generally, for any $P \subset [n]$, we take $\mathrm{rows}(\hat{M}, P)$ and $\mathrm{rowcount}(\hat{M}, P)$ to denote $\bigcup_{i\in P} \mathrm{rows}(\hat{M}, i)$ and $\sum_{i\in P} \mathrm{rowcount}(\hat{M}, i)$, respectively.

For any $f : \{0,1\}^n \to \{0,1\}$, we denote the set of all restricted span programs over $(\mathbb{F}, A, B)$ computing f as $\mathrm{SP}_{A,B,\mathbb{F}}(f)$ and the smallest program size in this set as $\mathrm{size}(\mathrm{SP}_{A,B,\mathbb{F}}(f))$.

We will usually refer to the span program $\hat{M}$ and its underlying matrix M interchangeably, denoting both as M.

Definition 2. Let $\hat{M}(M, \rho)$ be a restricted span program computing $f : \{0,1\}^n \to \{0,1\}$ over $(\mathbb{F}, A, B)$. If M_x has full row rank as an $\mathbb{F}$-matrix for all $x \in \{0,1\}^n$ such that $f(x) = 0$, then we call $\hat{M}$ a *uniform* program.

Similar to the above, $\mathrm{SP}_{A,B,\mathbb{F}} - \mathrm{Uniform}(f)$ and $\mathrm{size}(\mathrm{SP}_{A,B,\mathbb{F}} - \mathrm{Uniform}(f))$ denote the set of uniform restricted span programs computing f and the size of the smallest program in this set, respectively.

For both models defined above and similar models that will be defined below, the qualifier *monotone* will mean that all labels are of the form x_i^1. The corresponding sets will be denoted as $\mathrm{MSP}_{A,B,\mathbb{F}}(f)$ and $\mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Uniform}(f)$.

Remark. In the context of span programs, we will refer to $\mathbf{1}$ as the target vector. For usual span programs, it is well known that any two definitions with different non-zero target vectors are equivalent, since a program can be converted to be a program for another target vector through a simple change of basis. However, we have to be more careful with the restricted span programs.

It's easy to see that the set of coefficients, B, is preserved when we change the basis. The entry set, however, requires a more detailed investigation, and we avoid it since we won't need it here. The uniformity is similar to the set of coefficients and is preserved.

2.1 Restricted, Information-Theoretically Secure Linear Secret Sharing Schemes

In this section, we define the new secret sharing models that motivate the definitions of the restricted span program models of the previous section. We will also extend the known equivalence between the linear secret sharing schemes with perfect privacy and monotone span programs to between their new counterparts.

Definition 3. [Bei11] Fix number of parties $n \in \mathbb{Z}^+$, and sets $R, S, S_1, \ldots, S_n$. A secret sharing with perfect privacy scheme realizing the access function $f : \{0,1\}^n \to \{0,1\}$ over the domain of secrets S and domains of shares $S_1, \ldots, S_n$ with random input domain R is a family of functions $(\text{share}, (\text{reconstruct}_P)_{P \subseteq [n]})$ where $\text{share} : S \times R \to S_1 \times \cdots \times S_n$ and $\text{reconstruct}_P : (\bigtimes_{i \in P} S_i) \to S$ satisfy the following for all $P \subseteq [n]$.

Correctness If $f(P) = 1$, then

$$\Pr_{r \sim R}[\text{reconstruct}_P(\text{share}(s, r)_P) = s] = 1$$

Perfect Privacy If $f(P) = 0$, then, for all $a, b \in S, v \in \bigtimes_{i \in P} S_i$,

$$\Pr_{r \sim R}[\text{share}(a, r)_P = v] = \Pr_{r \sim R}[\text{share}(b, r)_P = v]$$

Here, share_P refers to the joint share vector of subset P, that is, components indexed $i \in [n]$ of share_P with $i \in P$.

We call a scheme linear when the domain of secret and shares are all a field $\mathbb{F}$ and all the reconstruction functions are linear on the shares.

Definition 4. Fix a field $\mathbb{F}$ and a set $B \subseteq \mathbb{F}$. A restricted secret sharing scheme $S(\text{share}, \text{reconstruct})$ over $(B, \mathbb{F})$ is a linear secret sharing scheme over $\mathbb{F}$ with perfect privacy such that the reconstruction coefficients are only from B. If for a restricted secret sharing scheme, the joint distribution of the shares of any unauthorized set is uniform, then the scheme is called a uniform scheme.

To provide intuition, throughout the text, we sometimes use the secret sharing nomenclature for span programs, such as referring to the rows labeled x_i^ϵ as the rows of party i or referring to x with $f(x) = 0$ as an *unauthorized* input.

We extend the equivalence proof of [Bei96] to show that the set of coefficients and uniformity are preserved.

Lemma 1. *For any field $\mathbb{F}$, sets $A, B \subseteq \mathbb{F}$, function $f : \{0,1\}^n \to \{0,1\}$ and $M \in \mathrm{MSP}_{A,B,\mathbb{F}}(f)$, there is a restricted secret sharing scheme S realizing f over $(B, \mathbb{F})$ with $\text{size}(S) = \text{size}(M)$. Furthermore, if M is uniform, S is also uniform.*

Proof. Let $k \times \ell$ be the size of M. For each $s \in \mathbb{F}$, define $N_s = \{v \in \mathbb{F}^{\ell \times 1} | \mathbf{1}v = s\}$ and fix an arbitrary indexing $\gamma_s : [|N_s|] \to N_s$. Let $R = [|N_1|]$, also noting that $|N_s| = |N_1|$ for all $s \in \mathbb{F}$. We construct the scheme $(\text{share}, \text{reconstruct}, R)$ over $(B, \mathbb{F})$ as follows.

Define $\text{share}(s, r) = M\gamma_s(r)$ where in the resulting vector, an entry will be a share piece for party j if the corresponding row in M is labeled x_j^1.

Consider any P such that $f(P) = 1$. Then, there is u_P with entries in B such that $u_P M_P = \mathbf{1}$. Hence, $u_P(M_P\gamma_s(r)) = u_P M_P \gamma_s(r) = \mathbf{1}\gamma_s(r) = s$. Therefore, we define $\text{reconstruct}_P(q) = u_P q$ and we have correctness.

Now consider any P such that $f(P) = 0$. Pick $u \in \mathbb{F}^{\ell \times 1}$ such that $M_P u = \mathbf{0}$ and $\mathbf{1}u = 1$. Such u exists since $\mathbf{1} \notin \text{Rowspan}_{\mathbb{F}}(M_P)$. For any $s_1, s_2 \in \mathbb{F}$ and any $c \in \mathbb{F}$, we will show that $\phi(r) = \gamma_{s_2}^{-1}((s_2 - s_1)u + \gamma_{s_1}(r))$ is a bijection from $\{r \in R | M_P\gamma_{s_1}(r) = c\}$ to $\{r \in R | M_P\gamma_{s_2}(r) = c\}$. First of all, it's well defined: $\beta(x) = ((s_2 - s_1)u + x)$ is a bijection from N_{s_1} to N_{s_2} since $\mathbf{1}\beta(x) = s_2 - s_1 + \mathbf{1}x = s_2$. A similar argument shows that $\gamma_{s_1}^{-1}((s_1 - s_2)u + \gamma_{s_2}(r))$ is also well-defined and acts as the inverse of $\phi(r)$, hence proving our claim.

Lastly, we prove that uniformity is preserved. Assume that M is uniform, and we claim the scheme constructed above is uniform. Again consider any P such that $f(P) = 0$. Since we want to show that all share vectors of the appropriate dimension have non-zero and equal probability, observe that it's enough to show that for each $s \in \mathbb{F}$ and $c_1, c_2 \in \mathbb{F}^{\text{rowcount}(M,P) \times 1}$, there is a bijection between $\{r \in R | M_P\gamma_s(r) = c_1\}$ and $\{r \in R | M_P\gamma_s(r) = c_2\}$ and that both are non-empty sets. But there is indeed a bijection since $\{v \in \mathbb{F}^{\ell \times 1} | M_P v = c_1, \mathbf{1}v = s\}$ and $\{v \in \mathbb{F}^{\ell \times 1} | M_P v = c_2, \mathbf{1}v = s\}$ are both translations of $\{v \in \mathbb{F}^{\ell \times 1} | M_P v = 0, \mathbf{1}v = 0\}$ and since γ_s is also a bijection. Finally, observe that when we concatenate the row vector $\mathbf{1}$ to M_P it still has full row rank since M_P has full row rank and $\mathbf{1} \notin \text{Rowspan}(M_P)$. Hence, $\{v \in \mathbb{F}^{\ell \times 1} | M_P v = c_1, \mathbf{1}v = s\}$ is always non-empty. $\square$

Lemma 2. *For any field $\mathbb{F}$, set $B \subseteq \mathbb{F}$, function $f : \{0,1\}^n \to \{0,1\}$ and a restricted secret sharing scheme S realizing S over $(B, \mathbb{F})$, there is $M \in \text{MSP}_{\mathbb{F},B,\mathbb{F}}(f)$ with $\text{size}(M) = \text{size}(S)$. Furthermore, if S is uniform, M is also uniform.*

Proof. Let R be the domain of the random input of share and fix any ordering of R and S. We define the matrix $M_{\text{size}(S) \times (|R||\mathbb{F}|)}$ as follows. Index the columns of M by $(r, s) \in R \times \mathbb{F}$, ordering first by the index of s and then by the index of r. Set the column labeled (r, s) to $\text{share}(s, r)$. Index the rows by the party indices. That is, if the i^{th} entry of the joint share vector belongs to party j, label the i^{th} row of M with x_j^1. Finally, let the target vector w be the concatenation of $\begin{bmatrix} s_i & s_i & \dots & s_i \end{bmatrix}_{1 \times |R|}$ for $i = 1$ to $|\mathbb{F}|$ in that order.

Consider any fixed $r \in R$ and $s \in \mathbb{F}$. Take $P \subseteq [n]$ such that $f(P) = 1$. Let v be the joint share vector of P and let k be its dimension. Then, by the correctness of the secret sharing scheme, there is $c = \begin{bmatrix} c_1 & c_2 & \dots & c_k \end{bmatrix}_{1 \times |R|} \in B^k$ such that, $\text{reconstruct}_P(v) = \sum_{i=1}^k c_i v_i = s$. Then, we see that $cM_P = w$. The case when $f(P) = 0$ is proven similarly by contradiction.

Lastly, we show that uniformity is preserved. Take any P such that $f(P) = 0$. Consider M_P and let ℓ be its number of rows. By the uniformity of the secret sharing scheme, for any $i \in [\ell]$ and for all $s \in \mathbb{F}$, there is $r \in R$ such that the column labeled (r, s) is e_i, the vector with 1 in the i^{th} coordinate and 0 in all the others. Hence, $\text{rank}(M_P) = \ell$. $\square$

Remark. Observe that in the proof of Lemma 2, instead of requiring that the joint distribution of the shares of the unauthorized sets be uniform, we could show the same results with the weaker assumption that the support of those distributions are equal to their respective spaces or even just that those supports span their respective spaces. In fact, based on this observation, we can see that any such *weaker* scheme can be converted to a uniform scheme by first applying Lemma 2 and then Lemma 1 while preserving the total share size.

3 Upper Bounds

In this paper, our focus will be lower bounds. However, we do present upper bounds for reference.

Definition 5 ([HRS93])**.** An undirected contact network (UCN) (G, s, t, μ) is an undirected graph $G = (V, E)$ with edges labeled by variables or their negations, that is $\mu : E \to \{x_i^\epsilon | i \in [n], \epsilon \in \{0,1\}\}$, and two designated vertices, source $s \in V$ and terminal $t \in V$. For any $u \in \{0,1\}^n$, E_u is defined to be $\{e \in E : \mu(u) = x_i^\epsilon \text{ with } u_i = \epsilon\}$ and G_u is (V, E_u).

A UCN is said to compute a function $f(x_1, \dots, x_n) : \{0,1\}^n \to \{0,1\}$ if for all $x \in \{0,1\}^n$, $f(x) = 1$ if and only if there is a path from s to t in G_x. The size of a UCN is defined to be the number of edges its graph has, $|E|$.

An undirected monotone contact network (UMCN) is a UCN where all edges are labeled by (non-negated) variables, namely $\epsilon = 1$. A UCN is series-parallel if the underlying network graph is series-parallel.

Note that the same construction is named *symmetric branching programs* in [KW93] and we will use the terms interchangeably. Also, as in the case of span programs, we will refer to the contact network and its underlying graph interchangeably.

Now we present a lemma from [KW93] which allows us to obtain upper bounds for span programs using known contact network and formula sizes. Additionally, we observe that when the underlying graph of a contact network is series-parallel, the proof actually gives a program in $MSP_{\mathbb{F},\{0,1\},\mathbb{F}}(f)$.

Lemma 3. *[KW93] Fix a field $\mathbb{F}$. A UCN $G = (V, E)$ computing a function f can be converted into a span program of the same size computing f. Also, if the network is monotone, so is the resulting program. Finally, if the network is series-parallel, the resulting program is in* $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}(f)$.

Proof. See the original proof for the first two claims. We only show the final claim here.

Assume that the network is series-parallel. Pick any basis $B := \{v_1, v_2, \dots, v_\ell\}$ of $\mathbb{F}^V$ such that $v_1 - v_2 = \mathbf{1}$.[2] Let $b : V \to B$ be a bijection with $b(t) = v_1$ and $b(s) = v_2$. For every edge $e = (v, w) \in E$ of the branching program, create a row in the span program with the same label and set its value to $b(w) - b(v)$.

For any input x such that $f(x) = 1$, we will have a path from the source. Hence, summing the rows that correspond to the edges on that path, we get $b(t) - b(s)$. Note that we only summed (some of) the rows of the authorized set, so we only used the coefficients $0, 1$.

For any unauthorized set, we cannot reach the terminal from the source, and since the vectors attached to vertices make up a basis, we won't be able to span $b(s) - b(t)$.

$\square$

[2] One way of finding such a basis is as follows. Start with the standard basis $\{e_1, e_2, \dots, e_\ell\}$, and remember that $\mathbf{1} = \sum_{i=1}^{\ell} e_i$. Then, $\{\sum_{i=1}^{\ell} e_i + e_2, e_2, e_3, \dots, e_\ell\}$ is also a basis.

Using the monotone formula upper bounds stated in [Bop85], we get the following upper bounds.

Theorem 4. *[Bop85]* $\mathrm{size}(\mathrm{UMCN}(Th_n^t)) \leq O((\min\{t, n-t\})^{4.3} n \log(n))$

Corollary 5. $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}(Th_n^t)) \leq O((\min\{t, n-t\})^{4.3} n \log(n))$

3.1 Upper Bounds for $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(Th_n^t)$

While the monotone UCN model does not give $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}$ directly, requiring that the G_x be acyclic when $f(x) = 0$ is enough to get this property. Note that, in case of Th_n^t, this is equivalent to each cycle of the contact network having at least t distinct variables. We use the following restricted models to get $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}$ upper bounds.

Definition 6. Let $\hat{G}(G, s, t, \mu)$ be a UCN computing $f : \{0,1\}^n \to \{0,1\}$. If G_x is acyclic for all $x \in \{0,1\}^n$ such that $f(x) = 0$, then we call $\hat{G}$ a uniform network.

Lemma 6. *In Lemma 3, if the network is uniform, then so is the resulting program.*

Proof. Let G be a uniform UCN computing f and let M be the corresponding span program obtained using Lemma 3. For a contradiction, suppose there is x with $f(x) = 0$ such that M_x does not have full row rank. Then, there is a linear dependency $\sum_i c_i u_i = 0$ where $\{u_i\}_i$ is $\mathrm{rows}(M_x)$ and c_i are not all 0. Consider only those i such that $c_i \neq 0$. Consider any u_i and its corresponding edge in the network, (v, w). u_i is a difference of two basis vectors by construction. Therefore, for those basis vectors to be eliminated, there should be distinct j, k such that the edge of u_j touches v, the edge of u_k touches w and $c_j, c_k \neq 0$. Continuing like this, we get a connected subset of vertices of G_x such that each vertex of it has degree at least 2 in G_x, which implies G_x is cyclic. □

Definition 7. Restricted monotone formulae for threshold functions.
A restricted monotone formula for a threshold function is a monotone formula[3] F computing Th_n^t for some t, n such that OR gates cannot have as their input a literal; their inputs can only be outputs of other gates, and if an input of an OR gate is the output of a *pure* AND subtree [4], that subtree must be effectively computing $\bigwedge_{i \in S} x_i$ for some $S \subseteq [n]$ with $|S| \geq t-1$. We will interchangeably consider formulae as functions and as trees. We denote the set of restricted monotone formulae computing Th_n^t as $\mathrm{RestrictedFormula}(t, n)$.

Lemma 7. *For any restricted monotone formula* $F \in \mathrm{RestrictedFormula}(t, n)$ *and for any field* $\mathbb{F}$*, there is an* $\hat{M} \in \mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(Th_n^t)$ *with* $\mathrm{size}(\hat{M}) \leq \mathrm{size}(F)$*.*

Proof. We first convert the formula to a uniform UMCN by converting AND gates into series connections and OR gates into parallel connections. Therefore, the resulting network will be a series-parallel graph, and we will invoke Lemma 3 and 6 to complete the proof.

We start by creating a separate UMCN for each leaf x_i of the formula: draw a single edge between s and t and label it x_i. When two nodes of the formula are ORed, merge the corresponding UMCNs by a parallel composition by matching the source and the terminal vertices. Similarly, for an AND gate, merge the UMCNs by a series composition. It's easy to see that this recursive construction leads to an UMCN that computes the same function as the formula. We can also remove any multiple edges between any vertices v_1, v_2 by replacing a pair of multiple edges with vertices v_1', v_2' and edges (v_1, v_1'), (v_1', v_2), (v_1, v_2'), (v_2', v_2).

[3] We require fan-in = 2 and allow only AND, OR gates. Formula size is the number of gates.

[4] An AND gate which doesn't have any OR gates below

This can be generalized to any number of multiple edges between a fixed pair of vertices, and this increases the network size at most by a factor of two. However, note that multiple edges can occur only if $t = 2$.

We finally show that an optimal UMCN constructed from a formula this way is uniform. For a contradiction, assume G_x has a cycle for some x such that $Th_n^t(x) = 0$. Since there is a clear level order, any cycle will have a top vertex and a bottom vertex, with two branches creating the cycle. Since both branches will be either a pure AND or a mixture of ANDs and ORs, each will contain $t-1$ distinct literals. Unless these size $t-1$ sets of literals are exactly the same, their union will have size t at least, which is a contradiction. (t literals being 1 implies $Th_n^t(x) = 1$). The case where the sets are exactly same implies a redundancy; we can remove the one of the OR subbranches (or the whole branch, if it's a pure AND branch) since the other branch will still provide a path between the top and the bottom vertex. $\square$

Note that we are not claiming that this is the optimal way of constructing an $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}-$Uniform from a contact network or a formula, but these uniform network and restricted formula definitions are natural and readily give such programs.

Now, we show some upper bounds for $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}-\mathrm{Uniform}(\mathrm{Th}_n^t)$ that we obtain from contact networks and restricted formulae.

Theorem 8. $size(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(Th_n^t)) \leq \binom{n}{t}t$

Sketch. Use the sum of minterms form of f. $\square$

Some optimal monotone formula upper bounds such as the one in [Val84] are shown probabilistically. However, [Fri84, Section 1] gives a code-based explicit construction, which is still optimal for $t = \Theta(1)$ and $t = n - \Theta(1)$. In fact, below we will invoke his construction only for $t = 2$.

The following is an elementary construction using [Fri84], which nevertheless improves upon the naive upper bound by a factor of $\frac{n}{\log(n)}$ in some cases.

Theorem 9. $\mathrm{size}(\mathrm{RestrictedFormula}(t, n)) \leq O(\binom{n}{t-2}t(n-t)\log(n-t))$.

Proof. Observe that the threshold function Th_n^t for $t > 2$ can be written in terms of Th_{n-t+2}^2 as follows:

$$Th_n^t(x_1, x_2, \ldots, x_n) = \bigvee_{S=\{i_1,i_2,\ldots,i_{t-2}\}\subset[n]} x_{i_1}x_{i_2}\ldots x_{i_{t-2}}Th_{n-t+2}^2([n]-S)$$

Based on this, do the following for each $S = \{i_1, i_2, \ldots, i_{t-2}\} \subset [n]$ and OR the resulting formulae. Apply the construction of [Fri84] to get a formula for Th_{n-t+2}^2, and then replace each literal x_j (where $j \in [n] - S$) with $x_jx_{i_1}x_{i_2}\ldots x_{i_{t-2}}$. Note that this replacement only increases the size of each formula for Th_{n-t+2}^2 by a factor of $t-1$.

Since the formula for Th_{n-t+2}^2 is of size $O((n-t)\log(n-t))$, the formula we get for Th_n^t is of size $O(\binom{n}{t-2}t(n-t)\log(n-t))$. $\square$

We show below that the upper bounds obtained above are close to optimal for this model.

Theorem 10. $size(\mathrm{RestrictedFormula}(t, n)) \geq \Omega(\frac{\binom{n}{t-1}}{n-t})$

Proof. Consider any $S \subseteq [n]$ with $|S| = t$. We will show that there must be $S' \subseteq S$ with $|S'| = t-1$ such that there is a pure AND subtree of the formula computing $\bigwedge_{i \in S'} x_i$.

Assume this is true for now. Since we cannot re-use a computation result in a formula, we conclude that the minimum size of the formula is $t|\mathcal{F}^*|$ where $\mathcal{F}^*$ is the smallest collection of size $t-1$ subsets of $[n]$ that includes a size $t-1$ subset of each size t subset of $[n]$. Observe that, for each $K \subseteq [n]$, $|K| = t-1$, $\mathcal{F}^*$ has to include a subset $K' \subseteq [n]$, $|K'| = t-1$ with $|K \bigcap K'| \geq t-2$. Suppose otherwise. Then, let i be such that $i \notin K$ and consider $K \bigcup \{i\}$. This size t subset won't have any size $t-1$ subsets that's in $\mathcal{F}^*$ (i.e., $K \bigcup \{i\}$ won't be *covered*). Based on this, we conclude that $|\mathcal{F}^*| \geq \gamma(J(n, t-1))$ where $\gamma(J(n, t-1))$ is the domination number of the Johnson graph $J(n, t-1)$. It's an elementary result that $\gamma(G) \geq \frac{|V(G)|}{\Delta(G)+1}$ for any graph G, where $\Delta(G)$ is the maximum degree of G. Therefore, we get $|\mathcal{F}^*| \geq \Omega(\frac{\binom{n}{t-1}}{(n-t)(t)})$ since $J(n, t-1)$ is $(t-1)(n-t+1)$ regular.

Now, we need to prove our initial claim. Consider any $S \subseteq [n]$ with $|S| = t$ and its evaluation by this formula. First of all, it's easy to see that the formula must contain at least 1 OR gate. Start at the root vertex of the formula. Since an AND gate means both subtrees evaluate to 1, we can descend down to an OR gate that must evaluate to 1. After this point, if we get to an OR gate, we recursively call the descend procedure for the child that evaluates to 1. We stop when we have reached an AND gate.

By the definition of RestrictedFormula, its easy to see that this descending procedure will terminate at an AND gate that has output 1 in this case and that's computing $\bigwedge_{i \in S'} x_i$ for some $S' \subseteq [n]$ with $|S'| \geq t-1$ in general. If $|S'| > t-1$, we must have $S = S'$, which means (by descending one more level) that a subset of S is computed by a pure AND subtree. If $|S'| = t-1$, this implies $S' \subset S$, which again proves our claim. $\square$

As discussed above, this model is not the only way we can obtain $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}$ upper bounds through contact networks or formulae. Below we use a more direct analysis to obtain a better upper bound for a specific case.

Definition 8. For a function $f : \{0,1\}^n \to \{0,1\}$, define its dual $f' : \{0,1\}^n \to \{0,1\}$ as $f'(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}$.

Observe that dual of a monotone formula is again a monotone formula of the same size. It's easy to see that dual of Th_n^t is Th_n^{n-t+1}.

Theorem 11. $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t)) \leq O(n \log(n))$ *for* $t = 2$ *and* $t = n-1$.

Proof. For $t = 2$, the requirement that each cycle contain at least t distinct variables is trivially satisfied. This shows that any formula upper bound for $t = 2$ transfers to our case. So we just use [Fri84] formula directly to get $O(n \log(n))$. We cannot hope for a better upper bound through formulae since it is known that there is a $\Omega(n \log(n))$ lower bound for monotone formulae for $t = 2$ [HRS93].

For $t = n-1$, take the dual of [Fri84] formula constructed for $t = 2$. Any parallel part in this construction corresponds to A_0^j and A_1^j of [Fri84, Section 1], and their union contains all the variables by the definition given there. Hence, any cycle contains all n variables. $\square$

3.2 Subfield Decomposition

The method of converting a program over $\mathbb{F}$ to a program over the subfield $\mathbb{L}$ is useful for us in the case when $char(\mathbb{F}) = 2$, since then $\{0,1\}$ is a subfield.

[KW93, Theorem 12] uses subfield decomposition method to show upper bounds for $\mathrm{MSP}_{\mathbb{F}_2,\mathbb{F}_2,\mathbb{F}_2}(\mathrm{Th}_n^t)$ through Shamir's secret sharing scheme over larger fields of characteristic 2. [CF02, Lemma 3] uses the same method for *integer span programs*. Here, we show that this method also preserves uniformity. We modify the decomposition slightly to be able to show the uniformity, so we first show in detail the correctness of the method in our context.

Theorem 12. *Let $\mathbb{L}$ be a subfield of $\mathbb{F}$. Then, $size(\mathrm{MSP}_{\mathbb{L},\mathbb{L},\mathbb{L}}(f)) \leq size(\mathrm{MSP}_{\mathbb{F},\mathbb{F},\mathbb{F}}(f)) \cdot |\mathbb{F} : \mathbb{L}|$ and $size(\mathrm{MSP}_{\mathbb{L},\mathbb{L},\mathbb{L}} - \mathrm{Uniform}(f)) \leq size(\mathrm{MSP}_{\mathbb{F},\mathbb{F},\mathbb{F}} - \mathrm{Uniform}(f)) \cdot |\mathbb{F} : \mathbb{L}|$*

Proof. Let $\{a_0, a_1, \ldots, a_{\ell-1}\}$ be an $\mathbb{L}$-basis of $\mathbb{F}$ where $\ell = |\mathbb{F} : \mathbb{L}|$ and $a_0 = 1$. For any $x \in \mathbb{F}$, let N_x denote the $\ell \times \ell$ matrix whose k^{th} row is the $\mathbb{L}$-coordinates of $a_k x$ as a row vector. We omit the proof here, but it's easy to show that $N_{xy} = N_x N_y$ and $N_{x+y} = N_x + N_y$ for all $x, y \in \mathbb{F}$ using the fact that multiplication is linear. Finally, for any matrix A with entries in $\mathbb{F}$, let $\hat{A}$ denote the matrix created by replacing each entry x of A with N_x.

Let $M_{s\times k} \in \mathrm{MSP}_{\mathbb{F},\mathbb{F},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t)$ with target vector $w_{1\times k} = [1, 0, \ldots, 0]$. We claim $\hat{M} \in \mathrm{MSP}_{\mathbb{L},\mathbb{L},\mathbb{L}}(\mathrm{Th}_n^t)$ with target vector $w_{1\times k\ell} = [1, 0, \ldots, 0]$. Note that it is fine to use these target vectors since we can change target vectors at the end to return to the original model.

First, the correctness. Let $A \subseteq [n]$ be such that $f(A) = 1$. Then, there is v such that $vM_A = w_{1\times k}$. Hence, $\hat{v}\hat{M}_A = (\widehat{w_{1\times k}})$. Considering the $\mathbb{L}$-coordinates of 0 and 1, it is easy to see that only keeping the first row gives us $(\hat{v})_1 \hat{M}_A = w_{1\times k\ell}$.

Then, the security. Let A be such that $f(A) = 0$. Then, $w_{1\times k} \notin \mathrm{Rowspan}(M_A)$ Then, $\tilde{M}_A v = ([0, \ldots, 0, 1]^T)_{(s_A+1)\times 1}$ has a solution, where $\tilde{L}$ is the matrix obtained by appending $[1, 0, \ldots, 0]^T$ at the bottom of L for any matrix L. Then, consider the multiplication $\widehat{(\tilde{M}_A)}\hat{v}$, and drop the last $(\ell - 1)$ rows of $\widehat{(\tilde{M}_A)}$ and all except the first column of $\hat{v}$. Denote these as P and u respectively. Observe that we have $Pu = ([0, \ldots, 0, 1]^T)_{(s_A\ell+1)\times 1}$ and $P = \widetilde{(\hat{M}_A)}$. Therefore, $w_{k\ell\times 1} \notin \mathrm{Rowspan}(\hat{M}_A)$.

Finally, the uniformity. Let A be such that $f(A) = 0$. Assume for a contradiction that $\hat{M}_A$ does not have full row rank. Then, there is a row vector $v \neq 0$ with entries in $\mathbb{L}$ such that $v\hat{M}_A = [0, \ldots, 0]_{1\times k\ell}$. Now, observe that there is (unique) $(v_c)_{1\times s_A}$ such that the first row of $\hat{v}_c$ is equal to v. Then, we can see that the first row of $\hat{v}_c \hat{M}_A$ is all zeroes. We claim this is a contradiction. Consider $v_c M_A$. Since v is not 0, v_c is not 0 either. By definition, we have that M_A has full row rank. Hence, $v_c M_A$ is not all zero. Therefore, the first row of $\hat{v}_c \hat{M}_A$ cannot be all zeroes. $\square$

Corollary 13. *$size(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(Th_n^t)) \leq O(n \log(n))$ for any $\mathbb{F}$ with $char(\mathbb{F}) = 2$.*

4 Lower Bounds

4.1 $\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}(\mathrm{Th}_n^t)$

Theorem 14. *For any field $\mathbb{F}$ of finite characteristic $char(\mathbb{F})$ and any t with $2 \leq t \leq n-1$,*

$$size(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}(Th_n^t)) \geq n \log_{char(\mathbb{F})}(n)$$

Since we have the upper bound $O(n \log_2(n))$ for any field $\mathbb{F}$ with $char(\mathbb{F}) = 2$, that is obtained through bit decomposition, we conclude that the lower bound is tight for such $\mathbb{F}$. Furthermore, using monotone contact networks, we get the same upper bound for any field $\mathbb{F}$ (of any characteristic including 0) and for threshold $t = \Theta(1)$ or $n - \Theta(1)$, we again conclude that the lower bound is tight for the case of $\Theta(1)$ characteristic and such threshold values.

We begin by outlining the proof of the theorem. First, we will show that conversion into a canonical form that preserves the program size and the coefficient set B. Then, we will prove that there is again a size preserving conversion between $\mathrm{MSP}_{A,B,\mathbb{F}}(f)$ and $\mathrm{MSP}_{B,A,\mathbb{F}}(f')$ where f' is the dual of f, inspired by [Gal98]. Lastly, we show $\mathrm{size}(\mathrm{MSP}_{\{0,1\},\mathbb{F},\mathbb{F}}(\mathrm{Th}_n^t)) \geq n \log_{char(\mathbb{F})}(n)$ using an adaptation of a theorem of [KW93].

4.1.1 Canonical Forms

We start with canonical forms. The following definition is from [KW93].

Definition 9. Let M be a span program computing f. We say that M is canonical if the columns of M are in one-to-one correspondence with $U = f^{-1}(0) \subset \{0,1\}^n$ and for every $u \in U$, the column corresponding to u in M_u is 0. We denote the class of canonical monotone span programs as $MSPCanon_{A,B,\mathbb{F}}$.

Observe that this condition automatically implies the security condition: since the column u of M_u will be $\mathbf{0}$, M_u cannot span $\mathbf{1}$. Therefore, we can think of this condition as replacing the security condition.

With a small modification, construction of [KW93, Theorem 6] preserves the set of coefficients. We observe this below and also the fact that in some cases the set of entries is also preserved. Full proof given for completeness.

Lemma 15. *For any $M \in \mathrm{MSP}_{A,B,\mathbb{F}}(f)$, there is $N \in \mathrm{MSP}_{\mathbb{F},B,\mathbb{F}} - \mathrm{Canonical}(f)$ with $\mathrm{size}(M) = \mathrm{size}(N)$. Furthermore, if A is a subfield of $\mathbb{F}$, then $N \in \mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Canonical}(f)$*

Proof. Define the canonical program matrix N as follows: row labels are the same as those of M, and columns are labeled by $u \in f^{-1}(0)$. Define column corresponding to u as $\frac{M(r(u))}{\mathbf{1}(r(u))}$ where $r(u)$ is some vector such that $M_u r(u) = 0$ and $\mathbf{1}r(u) \neq 0$. Such $r(u)$ has to exist since $f(u) = 0$ and hence $\mathbf{1}$ is not in the row span of M_u.

N computes f. Take $\sigma \in f^{-1}(1)$. There is $w(\sigma)$ with entries in B such that $w(\sigma)M_\sigma = \mathbf{1}$. Then, $w(\sigma)\frac{M_\sigma r(u)}{\mathbf{1}r(u)} = \frac{\mathbf{1}r(u)}{\mathbf{1}r(u)} = 1$ for all $u \in U$. So, $w(\sigma)N = \mathbf{1}$.

Now consider any $u \in U$. We have $M_u r(u) = 0$, so column u of N_u is all zeroes.

Observe that the reconstruction coefficients stay the same, so the set B is preserved. Furthermore, if A is a field, than r_u above can be chosen with entries in A. Since M has its entries in A, all of Mr_u, $\mathbf{1}r_u$ and $\frac{M(r(u))}{\mathbf{1}(r(u))}$ will have their entries in A. □

4.1.2 Switching the Sets A and B

The following is inspired by [Gal98, Theorem 3.4].

Lemma 16. *For any $M \in \mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Canonical}(f)$, there is $N \in \mathrm{MSP}_{B,A,\mathbb{F}} - \mathrm{Canonical}(f')$ with $\mathrm{size}(M) = \mathrm{size}(N)$.*

Proof. Define $U_f = f^{-1}(0) \subseteq \{0,1\}^n$ and $V_f = f^{-1}(1) \subseteq \{0,1\}^n$. Define the following row vector sets for all $i \in [n]$. $C_i = \{c_v^i\}_{v \in V_f}$ and $B_i = \{b_u^i\}_{u \in U_f}$. Here, c_v^i is the vector of span coefficients of rows of party i when the authorized input $v \in V$ is spanning $\mathbf{1}$. b_u^i is the column u of rows(M, i). We will consider $x \in \{0,1\}^n$ as both a subset of $[n]$ and as a binary vector.

By definition, $c_v^i \neq \mathbf{0}$ only if $v_i = 1$. Similarly, by the definition of canonical form, $b_u^i \neq \mathbf{0}$ only if $u_i = 0$. Also observe that c_v^i and b_u^i both have dimension rowcount(M, i).

We define N as follows. Index columns by the elements of $(f')^{-1}(0)$. It's easy to see that $U_{f'} = (f')^{-1}(0) = \{[n] \setminus v : v \in f^{-1}(1)\}$. Similarly, $V_{f'} = \{[n] \setminus u : u \in U_f\}$. i will have rowcount(M, i) many rows in N, and we define the column $[n] \setminus v$ of i to be c_v^i. Now we verify the correctness and the canonical form requirements. Due to the way we defined the vector sets, it's easy to see that $\sum_{i=1}^n (c_v^i)^T (b_u^i) = \sum_{i=1}^n (b_u^i)^T (c_v^i) = 1$ for all $v \in V_f$ and $u \in U_f$. Therefore, we conclude that, for each authorized input $([n] \setminus u)$ of f', using the coefficients $\{b_u^i\}_{i \in [n]}$ we get 1 in each column $([n] \setminus v)$ of N. Note that $b_u^i \neq \mathbf{0}$ only if $u_i = 0$ by definition, which means that during when spanning $\mathbf{1}$ for the authorized set $[n] \setminus u$, we use the rows of some i only if $([n] \setminus u)_i = 1$; that is, only if i is included. This shows that the correctness is satisfied. The canonical form is satisfied since the column $[n] \setminus v$ of the rows of party i will be $\mathbf{0}$ if $([n] \setminus v)_i = 1$, since $c_v^i = \mathbf{0}$ when $v_i = 0$.

Finally, we need to show $N \in \mathrm{MSP}_{B,A,\mathbb{F}} - \mathrm{Canonical}(f')$. Since $M \in \mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Canonical}(f)$, this is satisfied: entries of N come from c_v^i (which are span coefficients of M) and span coefficients of N come from b_u^i (which are entries of M). □

Corollary 17. $\mathrm{size}(\mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Canonical}(f)) = \mathrm{size}(\mathrm{MSP}_{B,A,\mathbb{F}} - \mathrm{Canonical}(f'))$

4.1.3 Proof of the Main Theorem

Definition 10. [KW93] An function $g : \{0,1\}^\ell \to \{0,1\}$ is called a *restriction* of a function $f : \{0,1\}^n \to \{0,1\}$ if g can be obtained by hardwiring (each to 0 or 1 independently) some of the inputs of f.

Lemma 18. *Let g be a restriction of $f : \{0,1\}^n \to \{0,1\}$. Then, for any $M \in \mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Canonical}(f)$, there is $N \in \mathrm{MSP}_{A,B,\mathbb{F}} - \mathrm{Canonical}(g)$ with size$(N) \leq$ size(M).*

Proof. See the proof of [KW93, Theorem 7]. It's easy to see that the construction there preserves A and B. □

Lemma 19. *If $A, B, \mathbb{F}$ are all fields such that $A \subseteq B \subseteq \mathbb{F}$,*

$$\mathrm{MSP}_{A,B,\mathbb{F}}(f) = \mathrm{MSP}_{A,A,A}(f)$$

Proof. Consider any $M \in \mathrm{MSP}_{A,B,\mathbb{F}}(f)$, we will show $M \in \mathrm{MSP}_{A,A,A}(f)$. Let d_i be rowcount(M, i) for $i \in [n]$. Consider any authorized input $v \in f^{-1}(1)$. Then, there is a row vector $r \in B^{(\sum_{i \in v} d_i)}$ such that $rM_v = \mathbf{1}$. Since $\mathbf{1}$ and M_v both have their entries in A, then there is $r' \in A^{(\sum_{i \in v} d_i)}$ such that $r'M_v = \mathbf{1}$, since a solution in an extension field implies a solution in the subfield (see [HK04], for example).

The security condition is trivial: for an unauthorized input $u \in f^{-1}(0)$, since M_u cannot $\mathbb{F}$-span $\mathbf{1}$, then it cannot A-span it either.

Now, take any $N \in \mathrm{MSP}_{A,A,A}(f)$, we will show $N \in \mathrm{MSP}_{A,B,\mathbb{F}}(f)$. Since $A \subset B$, the coefficient set condition is trivially satisfied. Finally, consider any unauthorized input $u \in f^{-1}(0)$. Assume for a contradiction there is $r \in \mathbb{F}^{(\sum_{i\in u} d_i)}$ such that $rN_v = \mathbf{1}$. As above, this would imply existence of $r' \in A^{(\sum_{i\in u} d_i)}$ such that $r'N_v = \mathbf{1}$, which is a contradiction. □

Finally, the proof of the main theorem. [KW93, Theorem 11] gives an algebraic variation of a lower bound proof for Th_n^2 formula size to show that $\text{size}(\text{MSP}_{\mathbb{F}_2,\mathbb{F}_2,\mathbb{F}_2}(\text{Th}_n^2)) \geq n\log_2(n)$. Here, we use the same counting argument in a more general setting along with the lemmas above to show results for the restricted model.

Proof. Let $\mathbb{L}$ be the prime subfield of $\mathbb{F}$. Observe that $size(MSP_{\mathbb{F},\{0,1\},\mathbb{F}}(Th_n^t)) \geq size(MSP_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^t))$ since $\{0,1\} \subseteq \mathbb{L}$. We will mainly work with $\mathbb{L}$ in the proof.

We will prove

$$size(MSP_{\mathbb{L},\mathbb{F},\mathbb{F}}(Th_n^2)) \geq n\log_{|\mathbb{L}|}(n)$$

Assume this is true for now. By Lemma 19, $size(MSP_{\mathbb{L},\mathbb{F},\mathbb{F}}(Th_n^2)) = size(MSP_{\mathbb{L},\mathbb{L},\mathbb{L}}(Th_n^2))$. Then, by Corollary 17, $size(MSP_{\mathbb{L},\mathbb{L},\mathbb{L}}(Th_n^2)) = size(MSP_{\mathbb{L},\mathbb{L},\mathbb{L}}(Th_n^{n-1}))$. Again by Lemma 19, $size(MSP_{\mathbb{L},\mathbb{L},\mathbb{L}}(Th_n^{n-1})) = size(MSP_{\mathbb{L},\mathbb{F},\mathbb{F}}(Th_n^{n-1}))$. Therefore, $size(MSP_{\mathbb{L},\mathbb{F},\mathbb{F}}(Th_n^{n-1})) \geq n\log_{|\mathbb{L}|}(n)$. Finally, again by using Corollary 17, we get

$$size(MSP_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^2)) \geq n\log_{|\mathbb{L}|}(n)$$
$$size(MSP_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^{n-1})) \geq n\log_{|\mathbb{L}|}(n)$$

For any $t \leq n-1$, when we hardwire $n-t-1$ inputs of Th_n^t to 0, we get Th_{t+1}^t. Hence, by Lemma 18, $size(MSPCanon_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^t)) \geq (t+1)\log_{char(\mathbb{F})}(t+1)$. Therefore, for any t with $\frac{n}{2} \leq t \leq n-1$, $size(MSPCanon_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^t)) \geq \Omega(n\log_{char(\mathbb{F})}(n))$. Lastly, note that by Lemma 15, $size(MSPCanon_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^t)) = size(MSP_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^t))$. This proves the main inequality for $\frac{n}{2} \leq t \leq n-1$.

Similar to above, for any $t \geq 2$, we can hardwire $t-2$ inputs of Th_n^t to 1 and get Th_{n-t+2}^2. Therefore, for t with $\frac{n}{2} \geq t \geq 2$, we get $size(MSP_{\mathbb{F},\mathbb{L},\mathbb{F}}(Th_n^t)) \geq \Omega(n\log_{char(\mathbb{F})}(n))$, hence proving the main inequality for all $2 \leq t \leq n-1$.

Now we prove $size(MSP_{\mathbb{L},\mathbb{F},\mathbb{F}}(Th_n^2)) \geq n\log_{|\mathbb{L}|}(n)$. Take any $M \in MSP_{\mathbb{L},\mathbb{F},\mathbb{F}}(Th_n^2)$. Let ℓ be the number of columns of M and d_i be the number of rows of i. For any $a \in \mathbb{L}\setminus\{0\}$, define the set of column vectors $R_a := \{r \in \mathbb{L}^t : \mathbf{1}r = a\}$. Also, for all $i \in [n]$, $R_{i,a} := \{r \in \mathbb{L}^t : M_i'r = w_{d_i,a}\}$ where M_i' is a matrix with d_i+1 rows with first d_i rows set to $M_{\{i\}}$ and the last row set to $\mathbf{1}$. $w_{d_i,a}$ is the column vector of size d_i+1 with first d_i rows equal to 0 and the last row equal to a. It's easy to see that $\bigcup_{i\in[n]} R_{i,a} \subseteq R_a$. Also, for any $i,j \in [n]$ with $i \neq j$, we have $R_{i,a} \bigcap R_{j,a} = \emptyset$. We prove the disjointness by contradiction as follows. Suppose there is $r \in R_{i,a} \bigcap R_{j,a}$. Let $\{b_m\}_{m\in[d_i]}$ and $\{c_k\}_{k\in[d_j]}$ be the rows of parties i and j respectively. Since $t=2$, there is $\{\beta_m\}_{m\in[d_i]}, \{\gamma_k\}_{k\in[d_j]} \subseteq \mathbb{L}$ such that $\sum_{m=1}^{d_i}\beta_m b_m + \sum_{k=1}^{d_j}\gamma_k c_k = \mathbf{1}$. Multiplying by r on both sides and considering the definitions of R_i, R_j, we get $0 = \mathbf{1}r$. This is a contradiction since $\mathbf{1}r = a \neq 0$ by definition.

Using disjointness, we get $\sum_{i=1}^n |R_{i,a}| \leq |R_a|$. Now, observe that R_a is defined by a single linear equation in $\mathbb{L}$. Hence, $|R_a| = |\mathbb{L}|^{t-1}$. Similarly, $|R_{i,a}| = |\mathbb{L}|^{t-rank_{\mathbb{L}}(M_i')}$. Note that here we used the fact that $\mathbf{1}$ is not in $\mathbb{L}$-span of M_i' (since $t > 1$), which shows the non-homogeneous equation system defining $R_{i,a}$ is not *inconsistent*. Using the fact $rank_{\mathbb{L}}(M_i') \leq d_i + 1$, we now have $\sum_{i=1}^n |\mathbb{L}|^{t-1-d_i} \leq |\mathbb{L}|^{t-1}$. Applying the arithmetic-geometric mean inequality (or Jensen's inequality directly), we get $\sum_{i=1}^n d_i \geq n\log_{|\mathbb{L}|}(n)$. □

Remark. To get a lower bound when the field characteristic grows with n, one approach that looks promising is to consider r with entries in $\{0,1\}$ and consider programs with entries in $\{0,1\}$, instead of in $\mathbb{L}$. In fact, one can use a linear recursion[5] or use combinatorial approaches directly to see that there are $\sum_{k=0}^{\lfloor \frac{\ell-1}{k} \rfloor} \binom{\ell}{char(\mathbb{F})k+1}$ solutions to $\mathbf{1}r = 1$ with r having entries in $\{0,1\}$. However, the other side is problematic: sets $R_{i,1}$ can have small sizes that is independent of d_i. For example, in the case $\ell = 2n$, $char(\mathbb{F}) = n^2+1$, it's possible that $|R_{i,a}| = 1$, no matter how large or small d_i is,[6] which renders this approach useless.

We finish this section with a lower bound that works for all fields, albeit it's an asymptotically insignificant result. Nevertheless, the approach will be useful in the next section for proving lower bounds for the uniform model.

Theorem 20. $\text{size}(\text{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}(\text{Th}_n^t)) \geq 2n-1$ *for all* t *such that* $1 < t < n$.

Proof. Consider any $M \in \text{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}}(\text{Th}_n^t)$. We will show that there can be at most one $i \in [n]$ such that $\text{rowcount}(M,i) = 1$. For a contradiction, without loss of generality, assume that $\text{rowcount}(M,i) = \text{rowcount}(M,t+1) = 1$.

Consider the following authorized sets A_1, A_2, A_3 and the unauthorized set U_1.

$$\begin{aligned}
A_1 &= \{1,2,\ldots,t-1,t\} \\
A_2 &= \{1,2,\ldots,t-1,t+1\} \\
A_3 &= \{2,3,\ldots,t-1,t,t+1\} \\
U_1 &= \{2,3,\ldots,t-1,t\}
\end{aligned}$$

Observe that, for any $i \in [n]$, when A is a minterm, $\text{rowcount}(M,i) = 1$ and $i \in A$, the coefficient of the single row of i must be nonzero.

Since rows of A_1 and A_2 can span $\mathbf{1}$, there is a $0-1$ combination of rows of these sets that are equal to each other. Canceling out the row of party 1, we see that rows of parties $\{2,\ldots,t-1,t\}$ can $\mathbb{F}$-span the only row of party $t+1$.

A_3 is also authorized, so it can span $\mathbf{1}$. But we can get rid of the row of party $t+1$ in this span equation by replacing it with what we obtained above. Thus, U_1 can $\mathbb{F}$-span the target, which violates the security condition. ☐

4.2 Lower Bounds via Extremal Sets

In this section, we prove a $\Omega(n\log(n))$ lower bound for computing thresholds functions with *uniform* restricted span programs with $\{0,1\}$ coefficients. Recall such a restricted span program, $\hat{M}(M,\rho)$, computing f is said to be uniform, if for all x such that $\text{Th}_n^t(x) = 0$ M_x has full row rank. Roughly, we show that if we can find a large family of authorized subsets that have a fixed core subset and have large pairwise intersections, then the total share size must also be large.

[5] This leads to a block diagonal matrix with block size $char(\mathbb{F})$ and each block being circulant, which can be solved with standard techniques.

[6] Consider the case when there is a row of full of 1s expect the last column. Since $\ell < char(\mathbb{F})$, this forces all of the first $\ell-1$ coordinates of r to be 0. Then, the last entry is forced to be 1 by the last row of the linear system. Hence, there is only 1 solution.

We start with a primitive version of the argument and then make it more flexible in the next step. Then, we go on to show lower bounds for various threshold values.

Finally, we show that a single, condensed version can show the same lower bound for (almost) all threshold values and then show that this is the optimal lower bound that can be shown with the technique we give here.

Theorem 21. *Suppose* $t + (2^c - 1)^{(t-1)} < n$ *for some* $2 < t < n$ *and* $c \in \mathbb{N}^+$*. Then, there cannot be* $M \in \mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t)$ *where* $\mathrm{rowcount}(M, i) = c$ *for all* $i \in [n]$*.*

Proof. Suppose otherwise. Let $v_{i,j}$ denote the j^{th} row of party i for $i = 1, \ldots, n$ and $j = 1, \ldots, c$.

Consider the subset of parties A=$\{1, 2, \ldots, (t-1)\}$. If we add any one more party to this set, it will be able to 0,1 span w. Note that no matter which party we add, we will have that, for each $i = 1, 2, \ldots, t-1$, the coefficient of $v_{i,j}$ is non-zero for at least one value of $j = 1, \ldots, c$. (Assume otherwise for some party i. Then its rows are contributing 0 to the span, so we can just drop party i and get a party set of (t-1) parties that can span w, which is a contradiction).

Therefore, there are $(2^c - 1)^{(t-1)}$ possible coefficient combinations for the rows of parties $1, 2, \ldots, t-1$ in any case where we add another party to them to span $\mathbf{1}$.

So, consider the parties $t, t+1, \ldots, t + (2^c - 1)^{(t-1)}$ (this is where we use the inequality assumption with c, t, n). If we add party t to the set A=$\{1, 2, \ldots, (t-1)\}$, they will be able to span $\mathbf{1}$. If we instead add party $t+1$, again they will be able to span $\mathbf{1}$ (since that makes t many parties). It continues like this for all values $t, t+1, \ldots, (2^c - 1)^{(t-1)}$

Now, we have $(2^c - 1)^{(t-1)} + 1$ span equations giving $\mathbf{1}$, where, in each of them we have t parties (first t-1 parties and one another party). Furthermore, in each of them, not all coefficients of the rows of a given party is 0 (due to reasoning above: we can go down to t-1 parties otherwise). By the pigeonhole principle, there must be two equations (without loss of generality, say they are the ones with party t and party t+1 respectively) where all the row coefficients of the parties $1, 2, \ldots, t-1$ are the same. Remembering that both equations are equal to $\mathbf{1}$, we can equate them and cancel everything related to rows of parties $1, 2, \ldots, t-1$.

Now, we have an equation of the following form: $b_1 v_{t,1} + b_2 v_{t,2} + \cdots + b_c v_{t,c} = d_1 v_{t+1,1} + d_2 v_{t+1,2} + \cdots + d_c v_{t+1,c}$. That is, some linear combination of rows of party t is equal to some (not necessarily the same coefficients) linear combination of rows of party $t+1$.

Finally, consider the unauthorized set of two parties: party t and party $t+1$ (since $t > 2$). By above, the submatrix of these two parties does not have full row rank, which is a contradiction.

□

We generalize the proof method shown above by making the number of parties that we try to cancel a parameter, along with the number of span equations we use. We will call these parameters x and ℓ respectively, and the proof method *x-fixed-ℓ-minterms* proof.

Proof. *x-fixed-ℓ-minterms* proof. Suppose in the proof above, instead of considering $(2^c-1)^{(t-1)}+1$ equations, we consider ℓ different equations for some parameter ℓ, corresponding to ℓ many distinct minimal (that is, of size t) authorized sets. We also require that all the minimal sets contain the first x parties, for some parameter x. Finally, we require that the union P of parties involved in pair of minimal sets, satisfy $|P - [x]| < t$. If there is a way of choosing a family of minimal sets satisfying these, we will call it a minimal set choosing strategy $Y_{x,\ell,t}$. It's easy to see that we also need $1 < x < t$.

Fix some x, ℓ, c such that there is a strategy $Y_{x,\ell,t}$ and $\ell > (2^c - 1)^x$. Then, there cannot be an MSP01-Uniform program where all n of the parties get c rows each. We prove by contradiction as follows.

Suppose otherwise. Then, we can invoke strategy $Y_{x,\ell,t}$ to get ℓ different span equations. Since $\ell > (2^c - 1)^x$; by the pigeonhole principle, there has to be two equations where the first x parties have exactly the same coefficients for each of their rows. Call the parties involved in those two equations P_1 and P_2. By cancellation, we get a linear dependence between rows of $(P_1 \cup P_2) - [x]$. By the definition of a strategy, we have $|(P_1 \cup P_2) - [x]| < t$. Hence, the fact that the submatrix of $(P_1 \cup P_2) - [x]$ is not of full row rank is a contradiction.

We can remove the requirement that all parties get the same number of rows as follows. Observe that the pigeonhole principle would still work if we assume that c is the largest number of rows that a party among the first x parties has. However, we are not required to invoke this proof with the *actual* first x parties. Instead, re-label parties so that parties $2, 3, \ldots, x$ are the parties with smallest number of rows. Then, invoke the proof by re-labeling the first party to be any party except one of those $x-1$ parties with smallest number of rows. Now, if we have the lower bound c^* under the assumption that all parties get the same number of rows, then in the general case, we get $\text{rowcount}(M, i) \geq c^*$ for all $i \in [n]$ expect $x - 1$ many of them. Hence, the total number of rows is lower bounded by $(n - x + 1)c^* + (x - 1)$.

Finally, it's easy to see that the impossibility result for $\ell > (2^c - 1)^x$ corresponds to the lower bound $c > \frac{\log_2(\ell)}{x}$. Hence, we get the following theorem. □

Theorem 22. *If there is a strategy $Y_{x,\ell,t}$, then we have* $\text{size}(\text{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \text{Uniform}(\text{Th}_n^t)) > (n - x + 1)\frac{\log_2(\ell)}{x} + (x - 1)$.

We now show some strategies for various cases and the corresponding lower bounds.

Lemma 23. *If $t + \ell - 1 \leq n$ and $x \geq 2$, then there is a strategy $Y_{x,\ell,t}$.*

Proof. On top of the first x parties, for each minimal set, add parties $\{x+1, x+2, \ldots, t-1, t+i-1\}$ for $i = 1, \ldots, \ell$. This gives us ℓ minimal sets, and we never run out of parties since $t + \ell - 1 \leq n$. Finally, the union of any two minimal sets contains $t - 1 - (x + 1) + 1 + 2$ parties, which is $\leq t - 1$ since $x \geq 2$. □

Corollary 24. $\text{size}(\text{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \text{Uniform}(\text{Th}_n^t)) \geq \Omega(n \log(n - t))$ *for $t \geq 3$.*

Proof. Invoke the *x-fixed-ℓ-minterms* proof using the strategy $Y_{x,\ell,t}$ for $x = 2$ and $\ell = n - t + 1$. □

Corollary 25. $\text{size}(\text{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \text{Uniform}(\text{Th}_n^t)) \geq \Omega(n \log(n))$ *for the majority function ($t = \lceil \frac{n}{2} \rceil$).*

Lemma 26. *If $\ell \leq \binom{n-x}{t-x}$ and $x \geq \min\{n - t + 1, \frac{t+1}{2}\}$, then there is a strategy $Y_{x,\ell,t}$.*

Proof. Simply pick all possible subsets of size $(t - x)$ of the set $\{x + 1, x + 2, \ldots, n\}$. $\ell \leq \binom{n-x}{t-x}$ guarantees that we can produce ℓ minimal sets without running out of possible subsets, and $x \geq \min\{n - t + 1, \frac{t+1}{2}\}$ guarantees the pairwise union size requirement (We don't prove it here, but it can be obtained using the elementary inequalities $|A \cup B| \leq |A| + |B|$ and $|U - A| \cup |U - B| \leq |U - A| + |U - B|$ where U contains both A, B.) □

Corollary 27. size($\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t)) \geq \Omega((n-x)^{\frac{\log(\binom{n-x}{t-x})}{x}})$ *for* $t \geq 3$ *where* $x = \min\{n-t+1, \frac{t+1}{2}\}$

Proof. Use the strategy shown above with $\ell = \binom{n-x}{t-x}$ and $x = \min\{n-t+1, \frac{t+1}{2}\}$. Again, this is the best lower bound we can get from this family of strategies. □

Corollary 28. *For any* $t = n-\Theta(1)$ *and* $t = \Theta(1)$*, except for* $t = 0, 1, 2, n$*, we have* $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t)) \geq \Omega(n \log(n))$.

Proof. Just use the elementary inequality $\binom{n}{k} \geq (\frac{n}{k})^k$ with Corollary 27. The other side $\binom{n}{k} \leq (\frac{en}{k})^k$ shows that this is the best lower bound we can get for these thresholds using this family of strategies. □

It turns out that we can show all of these bounds, or in fact more, by a single graph theoretic argument: one that uses the properties of Johnson graphs. This reduction is only applicable when $x = 2$, but later we show that the lower bound (which applies to almost all threshold values) we get from this is the best lower bound we can get for any value of x.

Theorem 29. *For any* $3 \leq t \leq n-1$*, we have* $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t)) \geq \Omega(n \log(n))$.

Proof. Let $x = 2$. Then, let P_1, P_2 be any pair of subsets provided by a fixed strategy. It's easy to show that $|(P_1 \cup P_2) - [x]| \leq t-1$ implies $|(P_1 - [x]) \cap (P_2 - [x])| \geq t-3$. Since $P_1 \neq P_2$ and $|P_1 - [x]| = |P_2 - [x]| = t-2$, we get $|(P_1 \cup P_2) - [x]| = t-3$. This shows that $P_1 - [x], P_2 - [x]$ must be adjacent in the Johnson graph $J := J_{n-2,t-2}$. This was for any pair P_1, P_2, which means that we are looking for the largest clique in J. Its size is the clique number of the graph and is denoted $\omega(J)$.

[GM15, Section 16.6] states that $\chi(J_{n,k}) \leq n$, where $\chi(G)$ denotes the chromatic number of graph G. Since $\chi(G) \geq \omega(G)$ for any G, we conclude that $\omega(J) \leq n$.

In fact, for $t \leq \frac{n}{2}$, the largest clique that gives us this lower bound is the elementary sliding window family we used in Corollary 24. Furthermore, the same family/clique is one of the two simple cliques demonstrated in [GM15, Section 6.1]. Taking into account the other clique they show, get $\omega(J) \geq \max\{n-t+1, t-1\} \geq \frac{n}{2}$. Hence, we get a $n\log(n)$ lower bound for all $3 \leq t \leq n-1$, thus proving Theorem 29.

□

Lastly, we give the following result. It might indicate that *x-fixed-ℓ-minterms* method might not be using the full power of the 0,1 restriction, and results specific for binary matrices (and their ranks) might lead to better lower bounds for $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t))$.

Corollary 30. *Let* $B \subseteq \mathbb{F}$ *and* $0 \in B$*. Any x-fixed-ℓ-minterms based lower bound we get for* $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},\{0,1\},\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t))$ *also works for* $\mathrm{size}(\mathrm{MSP}_{\mathbb{F},B,\mathbb{F}} - \mathrm{Uniform}(\mathrm{Th}_n^t))$ *when we change the base of the logarithm from 2 to* $|B|$*. In particular, for constant* $|B|$*, the lower bound stays the same asymptotically.*

Proof. Just change the base 2 to $|B|$ in the pigeonhole principle argument of *x-fixed-ℓ-minterms* proof. □

4.3 Limitations

While the fact that various values of x provided $\Omega(n\log(n))$ lower bound for various threshold values was promising that better lower bounds could be obtained by setting $x > 2$, it turns out that just using $x = 2$ is sufficient.

Lemma 31. *The best lower bound we can obtain using the x-fixed-ℓ-minterms method is $\Omega(n\log(n))$.*

Proof. By Ahlswede-Khachatrian Complete Intersection Theorem [AK97][7], which provides bounds for strategies (or families of subsets in their terminology) for all possible values, we conclude the following.

If there is an integer r such that $0 \le r \le x-1$ and $x(2+\frac{t-2x}{r+1}) < n-x < x(2+\frac{t-2x}{r})$, then the largest family a strategy $Y_{x,\ell,t}$ can provide is $F_r = \{A \subset \{x+1, x+2, \ldots, n\} : |A| = (t-x), |A \cap \{x+1, x+2, \ldots, t-x+1+2r\}| \ge t-2x+1+r\}$. Then, under the assumption that such r exists, it's easy to see that

$$\begin{aligned}
\ell = |F_r| &\le \sum_{j=t-2x+1+r}^{t-2x+1+2r} \binom{t-2x+1+2r}{j}\binom{n-t+2x-1-2r}{t-x-j} \\
&\le \sum_{j=t-2x+1+r}^{t-2x+1+2r} \binom{t-2x+1+2r}{j} \sum_{j=t-2x+1+r}^{t-2x+1+2r} \binom{n-t+2x-1-2r}{t-x-j}
\end{aligned}$$

Then,

$$\begin{aligned}
\log(\ell) \le &\log(\sum_{j=t-2x+1+r}^{t-2x+1+2r} \binom{t-2x+1+2r}{j}) + \log(\sum_{j=t-2x+1+r}^{t-2x+1+2r} \binom{n-t+2x-1-2r}{t-x-j}) \\
\le &\log(\sum_{j=0}^{r} \binom{t-2x+1+2r}{j}) + \log(\sum_{j=x-1-2r}^{x-1-r} \binom{n-t+2x-1-2r}{j}) \\
\le &\log((r+1)\binom{t+1+2r}{j}) + \log((r+1)\binom{n-t+2x-1-2r}{j})
\end{aligned}$$

In the last part, we used the fact that $r \le \frac{t-2x+1+2r}{2} \le \frac{t-2x+1+2r}{2}$ and $x-1-r \le \frac{n-t+2x-1-2r}{2}$ and that the binomial coefficients are larger towards the middle.

Continuing by using $r+1 \le x$, $t+1+2r \le 4n$, $x-1-r \le x$, $n-t+2x-1-2r \le n+2x \le 4n$ and $x \le \frac{4n}{2}$,

$$\begin{aligned}
\log(\ell) \le &\log(x\binom{4n}{r}) + \log(x\binom{4n}{x}) \\
\le &2\log(x\binom{4n}{x}) \\
\le &2\log(x) + 2x\log(4en) \le 4x\log(4en)
\end{aligned}$$

The last part is by $\binom{n}{k} \le (\frac{en}{k})^k$.

[7] See [Kat17] if you are only interested in the theorem statement.

Hence, $\frac{\log(\ell)}{x} \leq O(\log(n))$.

Finally, the case where there is no such integer r. First of all, observe that if $t \leq 2x$, we get

$$\begin{aligned}\frac{\log(\ell)}{x} &\leq \frac{\log(\binom{n-x}{t-x})}{x} \leq \frac{t-x}{x}\log(\frac{e(n-x)}{t-x}) \\ &\leq \frac{t-x}{x}\log(n) \leq \log(n)\end{aligned}$$

Similarly, $n \leq 3x$ implies $\frac{\log(\ell)}{x} \leq \frac{\log(2^n)}{x} = \frac{n}{x} \leq 3$.

Therefore, we can assume $t > 2x$ and $n > 3x$. Under this, the inequality condition provided for r above becomes

$$x\frac{t-2x}{n-3x} - 1 < r < x\frac{t-2x}{n-3x}$$

It's easy to see that if $\frac{t-2x}{n-3x} \leq 1$, we can pick an integer r that both satisfies this and is in the range $0 \leq r \leq x-1$. Hence, we only need to focus on the case $t-2x > n-3x$, or $x > n-t$ equivalently.

In that case,

$$\begin{aligned}\frac{\log(\ell)}{x} &\leq \frac{\log(\binom{n-x}{t-x})}{x} = \frac{\log(\binom{n-x}{n-t})}{x} \\ &\leq \frac{n-t}{x}\log(\frac{e(n-x)}{n-t}) \leq \frac{n-t}{x}\log(en) \leq O(\log(n))\end{aligned}$$

□

The fact that we have $O(n\log(n))$ upper bound for fields of characteristic 2 shows that field-agnostic approaches like the one here cannot yield lower bounds better than $\Omega(n\log(n))$. With this lemma, we also showed that subset-counting approaches like the one presented is not likely to yield better lower bounds even if they were specifically for fields with characteristic different than 2.

Acknowledgments. We are grateful to Hoeteck Wee who proposed the problem to us, and provided many useful comments and suggestions towards solving it.

References

[ABV$^+$12] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck Wee. Functional encryption for threshold functions (or fuzzy IBE) from lattices. In *Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 280–297. Springer, 2012.

[AK97] Rudolf Ahlswede and Levon H. Khachatrian. The complete intersection theorem for systems of finite sets. *European Journal of Combinatorics*, 18(2):125 – 136, 1997.

[AKS83] Miklós Ajtai, János Komlós, and Endre Szemerédi. Sorting in c log n parallel sets. *Comb.*, 3(1):1–19, 1983.

[Bei96] Amos. Beimel. Secure schemes for secret sharing and key distribution, 1996.

[Bei11] Amos Beimel. Secret-sharing schemes: A survey. In *IWCC*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer, 2011.

[BGG+18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. Threshold cryptosystems from threshold fully homomorphic encryption. In *CRYPTO (1)*, volume 10991 of *Lecture Notes in Computer Science*, pages 565–596. Springer, 2018.

[BL88] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988.

[Bla79] George Robert Blakley. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318. IEEE, 1979.

[Bop85] Ravi B. Boppana. Amplification of probabilistic boolean formulas. In *FOCS*, pages 20–29. IEEE Computer Society, 1985.

[Boy13] Xavier Boyen. Attribute-based functional encryption on lattices. In *TCC*, volume 7785 of *Lecture Notes in Computer Science*, pages 122–142. Springer, 2013.

[CF02] Ronald Cramer and Serge Fehr. Optimal black-box secret sharing over arbitrary abelian groups. In *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '02, page 272–287, Berlin, Heidelberg, 2002. Springer-Verlag.

[Fri84] J. Friedman. Constructing o(n log n) size monotone formulae for the k-th elementary symmetric polynomial of n boolean variables. In *25th Annual Symposium onFoundations of Computer Science, 1984.*, pages 506–515, 1984.

[Gal98] Anna Gal. A characterization of span program size and improved lower bounds for monotone span programs. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 429–437, New York, NY, USA, 1998. Association for Computing Machinery.

[GM15] Christopher Godsil and Karen Meagher. *Erdős–Ko–Rado Theorems: Algebraic Approaches*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2015.

[GVW13] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In *STOC*, pages 545–554. ACM, 2013.

[HK04] Kenneth Hoffman and Ray A. Kunze. *Linear Algebra*. PHI Learning, second edition, 2004.

[HMP06] Shlomo Hoory, Avner Magen, and Toniann Pitassi. Monotone circuits for the majority function. In *APPROX-RANDOM*, volume 4110 of *Lecture Notes in Computer Science*, pages 410–425. Springer, 2006.

[HRS93] M. M. Halldorsson, J. Radhakrishnan, and K. V. Subrahmanyam. Directed vs. undirected monotone contact networks for threshold functions. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 604–613, 1993.

[Kat17] Gyula O.H. Katona. Around the complete intersection theorem. *Discrete Applied Mathematics*, 216:618 – 621, 2017. Levon Khachatrian's Legacy in Extremal Combinatorics.

[KW93] M. Karchmer and A. Wigderson. On span programs. In *[1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111, 1993.

[Pat90] Mike Paterson. Improved sorting networks with o(log N) depth. *Algorithmica*, 5(1):65–92, 1990.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[Val84] Leslie G. Valiant. Short monotone formulae for the majority function. *J. Algorithms*, 5(3):363–366, 1984.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il