Depth-3 Arithmetic Circuits for $S_n^2(X)$ and Extensions of the Graham-Pollack Theorem

Jaikumar Radhakrishnan* Pranab Sen† Sundar Vishwanathan‡

Abstract

We consider the problem of computing the second elementary symmetric polynomial $S_n^2(X) \stackrel{\Delta}{=} \sum_{1 \le i < j \le n} X_i X_j$ using depth-three arithmetic circuits of the form $\sum_{i=1}^{r} \prod_{j=1}^{s_i} L_{ij}(X)$, where each L_{ij} is a linear form in $X_1, \ldots, X_n$. We consider this problem over several fields and determine *exactly* the number of multiplication gates required. The lower bounds are proved for inhomogeneous circuits where the L_{ij}'s are allowed to have constants; the upper bounds are proved in the homogeneous model. For reals and rationals, the number of multiplication gates required is exactly $n-1$; in most other cases, it is $\lceil \frac{n}{2} \rceil$.

This problem is related to the Graham-Pollack theorem in algebraic graph theory. In particular, our results answer the following question of Babai and Frankl: what is the minimum number of complete bipartite graphs required to cover each edge of a complete graph an odd number of times? We show that for infinitely many n, the answer is $\lceil \frac{n}{2} \rceil$.

1 Introduction

1.1 The Graham-Pollack theorem

Let K_n denote the complete graph on n vertices. By a *decomposition* of K_n, we mean a set $\{G_1, G_2, \ldots, G_r\}$ of subgraphs of K_n such that

1. Each G_i is a complete bipartite graph (on some subset of the vertex set of K_n); and
2. Each edge of K_n appears in precisely one of the G_i's.

*School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai 400005, India. Email: jaikumar@tcs.tifr.res.in.

†Laboratoire de Recherche en Informatique, Université de Paris-Sud, 91405 Orsay, France. Email: pranab@lri.fr. Most of this work was done while the author was a graduate student at the Tata Institute of Fundamental Research.

‡Department of Computer Science and Engineering, Indian Institute of Technology, Mumbai 400076, India. Email: sundar@cse.iitb.ernet.in.

It is easy to see that there is such a decomposition of the complete graph with $n-1$ complete bipartite graphs. Graham and Pollack [GP72] showed that this is tight.

Theorem *If $\{G_1, G_2, \ldots, G_r\}$ is a decomposition of K_n, then $r \geq n-1$.*

The original proof of this theorem, and other proofs discovered since then [dCH89, Pec84, Tve82], used algebraic reasoning in one form or another; no combinatorial proof of this fact is known.

One of the goals of this paper is to obtain extensions of this theorem. To better motivate the problems we study, we first present a proof of this theorem. This will also help us explain how algebraic reasoning enters the picture. Consider polynomials in variables $X = X_1, X_2, \ldots, X_n$ with rational coefficients. Let

$$\begin{aligned} S_n^2(X) &\triangleq \sum_{1 \leq i < j \leq n} X_i X_j; \\ T_n^2(X) &\triangleq \sum_{i=1}^{n} X_i^2. \end{aligned}$$

Then, we can reformulate the question as follows. What is the smallest r for which there exist sets $L_i, R_i \subseteq [n], L_i \cap R_i = \emptyset$, for $i = 1, 2, \ldots, r$, such that

$$S_n^2(X) = \sum_{i=1}^{r} (\sum_{j \in L_i} X_j) \times (\sum_{j \in R_i} X_j) \tag{1}$$

Notice that the two sums in the product on the right are homogeneous linear forms i.e. linear forms in $X_1, \ldots, X_n$ with constant term 0. One may generalise this question, and ask: What is the smallest r for which there exist homogeneous linear forms $L_i(X), R_i(X)$ for $i = 1, 2 \ldots, r$, such that

$$S_n^2(X) = \sum_{i=1}^{r} L_i(X) R_i(X) \tag{2}$$

Tverberg [Tve82] gave the following elegant argument to show that r must be at least $n-1$. Observe that $T_n^2(X) = (\sum_{i=1}^{n} X_i)^2 - 2S_n^2(X)$. Thus, (2) implies

$$T_n^2(X) = (\sum_{i=1}^{n} X_i)^2 - 2 \sum_{i=1}^{r} L_i(X)\, R_i(X) \tag{3}$$

Now if r is less than $n-1$, then there exists a non-zero $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Q}^n$ such that $L_i(\alpha) = 0$ for $i = 1, 2 \ldots, r$ and $\sum_{i=1}^{n} \alpha_i = 0$ (because at most $n-1$ homogeneous equations in n variables always have a non-zero solution). Under this assignment to the variables, the right hand side of (3) is zero but the left hand side is not.

With this introduction to the Graham-Pollack theorem and its proof, we are now ready to state the questions we consider in this paper. Observe that the lower bound for r in (2) depended crucially on the field being $\mathbb{Q}$, and there are two main difficulties in generalising

it to other fields. First, over fields of characteristic two, the relationship between $S_n^2(X)$ and $T_n^2(X)$ does not hold, for we cannot divide by 2. Second, even if we are not working over fields of characteristic two, $T_n^2(X)$ can vanish at some non-zero points. Equations similar to (2) have been studied in the past in at least two different contexts viz. covering a complete graph by complete bipartite graphs such that each edge is covered an odd number of times (the *odd cover problem*), and depth–3 arithmetic circuits for $S_n^2(X)$.

1.2 The odd cover problem

Suppose in the Graham-Pollack problem, we drop the condition that the bipartite graphs be edge-disjoint, but instead ask for each edge of the complete graph to be covered an odd number of times. We call this problem the *odd cover problem*. How many bipartite graphs are required in such a cover? This question was posed by Babai and Frankl [BF92], who also observed a lower bound of $\lfloor \frac{n}{2} \rfloor$. However, the upper bound was the trivial $n-1$. Note that this problem is equivalent to considering (1) over the field GF(2).

1.3 $\Sigma\Pi\Sigma$ arithmetic circuits

By a $\Sigma\Pi\Sigma$ arithmetic circuit over a field $\mathbb{F}$, we mean an expression of the form

$$\sum_{i=1}^{r} \prod_{j=1}^{s_i} L_{ij}(X) \tag{4}$$

where each $L_{ij}(X)$ is a (possibly inhomogeneous) linear form in variables $X_1, \ldots, X_n$. The above expression is to be treated as over the field $\mathbb{F}$. Such 'depth-three' circuits play an important role in the study of arithmetic complexity [NW96, GR00, SW99]. If each linear form $L_{ij}(X)$ is homogeneous (i.e. has constant term zero), the circuit is said to be homogeneous, or else, it is said to be inhomogeneous. Although depth-three circuits appear to be rather restrictive, these are the strongest model of circuits for which super polynomial lower bounds for computing explicit polynomials are known; no such lower bounds are known at present for depth-four circuits.

The k-th elementary symmetric polynomial on n variables is defined as follows.

$$S_n^k(X) \stackrel{\Delta}{=} \sum_{T \in \binom{[n]}{k}} \prod_{i \in T} X_i$$

Elementary symmetric polynomials are the most commonly studied candidates for showing lower bounds in arithmetic circuits. Nisan and Wigderson [NW96] showed that any homogeneous $\Sigma\Pi\Sigma$ circuit for computing $S_n^{2k}(X)$ has size $\Omega((n/4k)^k)$. In their paper, they explicitly stated the method of partial derivatives (but see also Alon [Alo86]). Although a super polynomial lower-bound was obtained in [NW96], the lower bound applied only to homogeneous circuits. Indeed, Ben-Or (see e.g. [NW96]) showed that any elementary symmetric polynomial can be computed by an inhomogeneous $\Sigma\Pi\Sigma$ formula of size

$O(n^2)$. Thus, inhomogeneous circuits are significantly more powerful than homogeneous circuits. Shpilka and Wigderson [SW99] (and later, Shpilka [Shp01]) addressed this shortcoming of the Nisan-Wigderson result and showed an $\Omega(n^2)$ lower bound on the size of inhomogeneous $\Sigma\Pi\Sigma$ formulae computing certain elementary symmetric polynomials, thus showing that Ben-Or's construction is optimal. To obtain their results, they augmented the method of partial derivatives by an analysis of (affine) subspaces where elementary symmetric polynomials vanish. Many of the lower bounds in this paper are inspired by the insights from [SW99] and [Shp01]. All the results cited above work over fields of characteristic zero. At present, no super-quadratic lower bounds are known for computing some explicitly defined polynomial in the inhomogeneous $\Sigma\Pi\Sigma$ model over infinite fields. Over finite fields the situation is better. Karpinski and Grigoriev [GK98] showed an exponential lower bound for computing the determinant polynomial using (inhomogeneous) $\Sigma\Pi\Sigma$ circuits over any finite field. Grigoriev and Razborov [GR00] showed an exponential lower bound for any (inhomogeneous) $\Sigma\Pi\Sigma$ circuit computing a *generalised majority* function over any finite field.

Though the elementary symmetric polynomials have been studied with reasonable success in the past in the $\Sigma\Pi\Sigma$ model of computation, the upper and lower bounds obtained till now agree at best to within constant multiplicative factors. In this paper, we study the simplest non-trivial elementary symmetric polynomial, viz. $S^2_n(X)$, in various flavours of the $\Sigma\Pi\Sigma$ model. This does not make the problem trivial; in fact, some of these flavours have implications to interesting combinatorial problems like, for example, the odd cover problem mentioned above. Instead of upper and lower bounds to within constant multiplicative factors, we shall be interested in the *exact* answer, in the spirit of Graham and Pollack. In all the cases we study, we obtain exact answers for infinitely many n, and in some cases, for all n. One of the implications of this work is an exact bound of $\lceil \frac{n}{2} \rceil$ for infinitely many even and odd n for the odd cover problem.

Organisation of this paper

In the next section, we give a summary of our results. In Section 3, we present formal proofs of our upper bound results. Section 4 contains formal proofs of our lower bound results. The appendix contains statements of our results and their proofs, for computing $S^2_n(X)$ using $\Sigma\Pi\Sigma$ arithmetic circuits over the fields $\mathrm{GF}(p^r)$, p an odd prime.

2 Our results

We study the computation of the elementary symmetric polynomial $S^2_n(X)$ using $\Sigma\Pi\Sigma$ arithmetic circuits over several fields, with the aim of obtaining exact bounds on the number of multiplication gates required. Many of the techniques developed earlier (in particular, the method of partial derivatives), in fact, give lower bounds on the number of multiplication gates. Also, counting the number of multiplication gates only, allows us to give bounds for the odd cover problem and the $1 \bmod p$ cover problem, p an odd prime

(generalisation of the Graham-Pollack problem where we now require that each edge be covered 1 mod p times).

As described in the introduction, computations of elementary symmetric polynomials have been considered for several flavours of $\Sigma\Pi\Sigma$ circuits. For the polynomial $S_n^2(X)$, we study three different flavours of the $\Sigma\Pi\Sigma$ model.

1. *The graph model:* This is the weakest model. Here, the linear forms $L_i(X)$ and $R_i(X)$ (see equation (2) above) must correspond to bipartite graphs; that is, all coefficients must be 1 (or 0), no variable can appear in both L_i and R_i (with coefficient 1), and no constant term is allowed in these linear forms. This is the setting for the Graham-Pollack theorem and its generalisations viz. the odd cover problem and the 1 mod p cover problem (p an odd prime).

2. *The homogeneous model:* Here the linear forms are required to be homogeneous, that is, no constant term is allowed in them. However, any element from the field is allowed as a coefficient in the linear forms. This model was studied by Nisan and Wigderson [NW96], using the method of partial derivatives.

3. *The inhomogeneous model:* This is the most general model; there is no restriction on the coefficients or the constant term.

We show our upper bounds in the graph and the homogeneous model; our lower bounds hold even in the stronger inhomogeneous model. We juxtapose our results against the previously known results and also briefly mention the proof technique used, highlighting our contribution. Note that the previous lower bounds were for the homogeneous circuit model only, and were proved using the method of partial derivatives [NW96] (but see also the rank arguments of Babai and Frankl [BF92] for the graph model). Below, the notation $\exists^\infty n$ means *'for infinitely many n'* and the notation $\forall n$ means *'for all n'*.

2.1 The odd cover problem and computing $S_n^2(X)$ over GF(2)

Bounds:

	Our Bounds			Previous Bounds	
	Upper Bounds		Lower Bounds	Upper Bounds	Lower Bounds
	Graph	Hom.	Inhom.	Graph	Hom.
$n \equiv 0 \bmod 4$	$\frac{n}{2}\exists^\infty n$	$\frac{n}{2}\exists^\infty n$	$\frac{n}{2}\forall n$	$n-1\forall n$	$\frac{n}{2}\forall n$
$n \equiv 2 \bmod 4$	$\frac{n}{2}\exists^\infty n$	$\frac{n}{2}\exists^\infty n$	$\frac{n}{2}\forall n$	$n-1\forall n$	$\frac{n}{2}\forall n$
$n \equiv 3 \bmod 4$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$	$\lceil\frac{n}{2}\rceil\ \forall n$	$n-1\forall n$	$\lfloor\frac{n}{2}\rfloor\ \forall n$
$n \equiv 1 \bmod 4$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$	$\lfloor\frac{n}{2}\rfloor\ \exists^\infty n$	$\lfloor\frac{n}{2}\rfloor\ \forall n$	$n-1\forall n$	$\lfloor\frac{n}{2}\rfloor\ \forall n$

Proof Methods. For the upper bound in the graph model, we restrict our attention to a class of schemes, which we call *pairs constructions*, for constructing odd covers of K_n . We relate the pairs construction to the existence of certain kinds of *good* matrices. We then give two different constructions of *good* matrices. The first construction is based on *conference matrices*, which are related to *Hadamard matrices*. The second construction is based on *symmetric designs*, and uses some elementary properties about quadratic residues. The first construction gives optimal odd covers for infinitely many n of the form 0 mod 4; the second gives optimal odd covers for infinitely many n of the form 2 mod 4. We get $\lceil \frac{n}{2} \rceil$ sized odd covers for infinitely many n of the forms $n = 1, 3 \bmod 4$ from odd covers of K_{n+1} of optimal size.

The $\lfloor \frac{n}{2} \rfloor$ upper bound in the homogeneous model for $n \equiv 1 \bmod 4$ is got by locally transforming a homogeneous circuit computing $S^2_{n-1}(X)$ using $\frac{n-1}{2}$ multiplication gates to a homogeneous circuit computing $S^2_n(X)$ using the same number of multiplication gates.

For the lower bound, we use the method of substitution used by Shpilka and Wigderson [SW99], and subsequently refined by Shpilka [Shp01]. However, the proof is not a straightforward application of earlier methods. Technical difficulties arise because we are working over GF(2) and not over fields of characteristic zero. Almost all the earlier lower bound proofs used partial derivatives in some way or the other. Over GF(2), most of these approaches fail to work. Thus, we have to exploit the method of substitution in ways which do not use partial derivatives.

In fact, we place the method of substitution in a general framework and recast it to obtain a family of equations. We then exploit the family of equations depending upon the field in question, to obtain different lower bounds for different fields.

2.2 1 mod p cover problem, p an odd prime

Bounds:

	Our Bounds	Previous Bounds	
	Upper Bounds Graph	Upper Bounds Graph	Lower Bounds Hom.
n even	$\frac{n}{2}\exists^\infty n$	$n-1 \forall n$	$\frac{n}{2}\forall n$
n odd	$\lceil \frac{n}{2} \rceil \exists^\infty n$	$n-1 \forall n$	$\lfloor \frac{n}{2} \rfloor \forall n$

Proof Methods. The upper bound follows by a *pairs construction* argument (refer Section 2.1). We reduce the problem of existence of a pairs construction to the existence of certain kinds of matrices *good for p*. By a modification of the *symmetric designs* construction (refer Section 2.1), we construct an infinite family of matrices *good for p*. This suffices to show the upper bounds for the 1 mod p cover problem. We use the same lower bounds as those known earlier for homogeneous circuits.

2.3 Computing $S_n^2(X)$ over $\mathbb{C}$

Bounds:

	Our Bounds		Previous Bounds	
	Upper Bounds Hom.	Lower Bounds Inhom.	Upper Bounds Hom.	Lower Bounds Hom.
$\forall n$	$\lceil \frac{n}{2} \rceil$	$\lceil \frac{n}{2} \rceil$	$\lceil \frac{n+1}{2} \rceil$	$\lceil \frac{n}{2} \rceil$

Proof Methods. For the upper bound, we reformulate the algebraic problem and arrive at a suitable bilinear form. Then, if the notion of "distance" between vectors is defined using this bilinear form, the problem reduces to finding suitably spaced vectors with complex coordinates. We then show the existence of such a suitably spaced family of vectors. The proof has a geometric flavour. For the lower bound, we now use the general framework mentioned in Section 2.1. This time however, the way we exploit the family of equations is very different; in particular, we view the constraints geometrically and arrive at a (different) bilinear form. Then, if the notion of "distance" between vectors is defined using this bilinear form, the problem reduces to placing a certain number of points on a sphere of a certain radius such that all the points are equidistant with a certain common distance. We then show that such a placement of points is impossible.

2.4 Computing $S_n^2(X)$ over $\mathbb{R}$ and $\mathbb{Q}$

Bounds:

	Our Bounds		Previous Bounds	
	Upper Bounds Graph	Lower Bounds Inhom.	Upper Bounds Graph	Lower Bounds Hom.
$\forall n$	$n-1$	$n-1$	$n-1$	$n-1$

Proof Methods. In this case, we show that the trivial upper bound of $n-1$ is tight even for inhomogeneous circuits. The proof of the Graham-Pollack theorem works only for homogeneous circuits. To extend the result to inhomogeneous circuits, we need to use the method of substitution. The result is relatively straightforward once the problem is placed in this framework. We state the result for completeness.

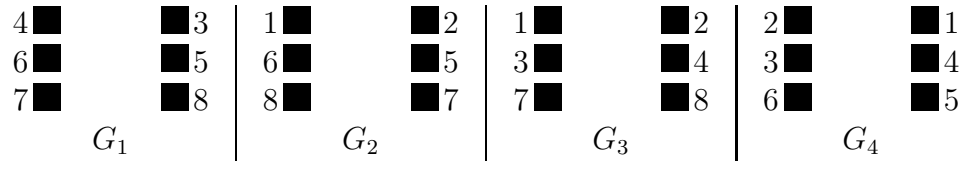
3 Upper bounds

3.1 The odd cover problem and computing $S_n^2(X)$ over GF(2)

In this section, we will show that there is an odd cover of K_{2n} by n complete bipartite graphs whenever there exists a $n \times n$ matrix satisfying certain properties. We describe a particular scheme for producing an odd cover of K_{2n}, which we call a *pairs construction*. We express the requirements for a pairs construction in the language of matrices, and then give sufficient conditions for a matrix to encode a pairs construction. We call a matrix satisfying these sufficient conditions a *good* matrix.

We want to cover the edges of K_{2n} with n complete bipartite graphs such that each edge is covered an odd number of times. A complete bipartite graph is fully described by specifying its two colour classes A and B. Partition the vertex set $[2n]$ (of K_{2n}) into ordered pairs $(1,2),(3,4),\ldots,(2n-1,2n)$. In a *pairs construction* of an odd cover of K_{2n}, if one element of a pair does not participate in a complete bipartite graph G in the odd cover decomposition, then the other element of the pair does not participate in G either, and also, both the elements of a pair do not appear in the same colour class in G. Hence, to describe a complete bipartite graph G in a pairs construction of an odd cover decomposition, it suffices to specify for each pair $(2i-1,2i)$, whether the pair participates in the bipartite graph, and when it does, whether $2i$ appears in colour class A or B. We specify the n complete bipartite graphs in the odd cover decomposition by a $n \times n$ matrix $\mathbf{M}$ with entries in $\{-1,0,1\}$. The rows of the matrix are indexed by pairs; the ith row is for the pair $(2i-1,2i)$. The columns are indexed by the complete bipartite graphs of the odd cover decomposition. If $\mathbf{M}_{ij}=0$, the pair $(2i-1,2i)$ does not participate in the jth bipartite graph G_j; if $\mathbf{M}_{ij}=1$, $2i$ appears in colour class B of G_j; if $\mathbf{M}_{ij}=-1$, $2i$ appears in colour class A of G_j.

$$\mathbf{M} = \begin{array}{c} \\ (1,2) \\ (3,4) \\ (5,6) \\ (7,8) \end{array} \begin{array}{c} \begin{array}{cccc} G_1 & G_2 & G_3 & G_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & -1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & 0 & -1 \\ 1 & -1 & 1 & 0 \end{bmatrix} \end{array}$$



The matrix $\mathbf{M}$ describes a pairs construction of an odd cover of K_8 by complete bipartite graphs G_1, G_2, G_3, G_4.

Figure 1: An example of a pairs construction.

We now identify properties of the matrix $\mathbf{M}$ which ensure that the complete bipartite

graphs arising from it form an odd cover of K_{2n}.

Definition 1 *A $n \times n$ matrix with entries from $\{-1, 0, 1\}$ is* good *if it satisfies the following conditions:*

1. *In every row, the number of non-zero entries is odd.*
2. *For every pair of distinct rows, the number of columns where they both have non-zero entries is congruent to* 2 mod 4*.*
3. *Any two distinct rows are orthogonal over the integers.*

Lemma 1 *If an $n \times n$ matrix is good, then the n complete bipartite graphs that arise from it form an odd cover of K_{2n}.*

Proof: Since the number of non-zero entries in a row is odd, the number of times the corresponding edge $\{2i-1, 2i\}$ is covered is odd. Next, consider edges whose vertices come from different pairs: say, the edge $\{1, 3\}$. We need to show that the number of bipartite graphs where 1 and 3 are placed on opposite sides is odd. Consider the rows of the matrix corresponding to pairs $(1, 2)$ and $(3, 4)$. Since these rows are orthogonal over the integers, the number of times 1 appears on the opposite side of 3 must be equal to the number of times 1 appears on the opposite side of 4. Since the number of columns where both rows have non-zero entries is congruent to 2 mod 4, the number of times 1 appears on the opposite side of 3 (as well as the number of times 1 appears on the opposite side of 4) must be odd. Thus, given a good matrix, we can construct n complete bipartite graphs covering each edge of K_{2n} an odd number of times. ■

Thus, to obtain odd covers, it is enough to construct good matrices. We now give two methods for constructing such matrices.

Construction 1: Skew symmetric conference matrices

A *Hadamard matrix* $\mathbf{H}_n$ is an $n \times n$ matrix with entries in $\{-1, 1\}$ such that $\mathbf{H}_n \mathbf{H}_n^T = n\mathbf{I}_n$, where $\mathbf{I}_n$ is the $n \times n$ identity matrix. A *conference matrix* $\mathbf{C}_n$ is an $n \times n$ matrix, with 0's on the diagonal and $-1, +1$ elsewhere, such that $\mathbf{C}_n \mathbf{C}_n^T = (n-1)\mathbf{I}_n$. The following fact can be verified easily.

Lemma 2 *$n \times n$ conference matrices, where $n \equiv 0 \bmod 4$, are good matrices.*

Skew symmetric conference matrices can be obtained from *skew Hadamard matrices*. A skew Hadamard matrix is defined as a Hadamard matrix that one gets by adding the identity matrix to a skew symmetric conference matrix. Several constructions of skew Hadamard matrices can be found in [Hal86, p. 247]. In particular, the following theorem is proved there.

Theorem 1 *There is a skew Hadamard matrix of order n if $n = 2^t k_1 \cdots k_s$, where $n \equiv 0 \bmod 4$, each $k_i \equiv 0 \bmod 4$ and each k_i is of the form $p^r + 1$, p an odd prime.*

Corollary 1 *There is a good matrix of order n if n satisfies the conditions in the above theorem. Note that the conditions hold for infinitely many n.*

As an illustrative example, we show the existence of skew Hadamard matrices $\mathbf{F}_n$ when n is a power of 2. To do this, we modify the well-known recursive construction for Hadamard matrices. For $n = 2$, set $(\mathbf{F}_2)_{21} = -1$ and the rest of the entries 1. Suppose now that we have constructed $\mathbf{F}_n$. To construct $\mathbf{F}_{2n}$, place a copy of $\mathbf{F}_n$ in the top left corner, a copy of $-\mathbf{F}_n$ in the bottom left corner, and copies of $\mathbf{F}_n^T$ in the top right and bottom right corners. It is easy to check that $\mathbf{F}_{2n}$ so constructed is skew Hadamard. In fact, the matrix $\mathbf{M}$ in Figure 1 is nothing but $\mathbf{F}_4 - \mathbf{I}_4$.

Construction 2: Symmetric designs

The matrices $\mathbf{M}$ that we now construct are based on a well-known construction for symmetric designs. These matrices are not conference matrices; in fact, they have more than one zero in every row.

Let q be a prime power congruent to 3 mod 4. Let $\mathbb{F} = \mathrm{GF}(q)$ be the finite field of q elements. Index the rows of $\mathbf{M}$ with lines and the columns with points of the projective 2-space over $\mathbb{F}$. That is, the projective points and lines are the one dimensional and two dimensional subspaces respectively, of $\mathbb{F}^3$. A projective point is represented by a vector in $\mathbb{F}^3$ (out of $q-1$ possible representatives) in the one dimensional subspace corresponding to it. A projective line is also represented by a vector in $\mathbb{F}^3$ (out of $q-1$ possible representatives). The representative for a projective line can be thought of as a 'normal vector' to the two dimensional subspace corresponding to it. We associate with each projective line L a linear form on the vector space $\mathbb{F}^3$, given by $L(w) = v^T w$, where $w \in \mathbb{F}^3$ and v is the chosen representative for L. For a projective line L and a projective point Q, let $L(Q) \stackrel{\Delta}{=} L(w)$, where w is the chosen representative for Q. Now the matrix $\mathbf{M}$ is defined as follows. If $L(Q) = 0$ (i.e. projective point Q lies on projective line L), we set $\mathbf{M}_{L,Q} = 0$; if $L(Q)$ is a (non-zero) square in $\mathbb{F}$, set $\mathbf{M}_{L,Q} = 1$; otherwise, set $\mathbf{M}_{L,Q} = -1$.

We now check that $\mathbf{M}$ is a good matrix. M is a $n \times n$ matrix, where $n = q^2+q+1$, q a prime power congruent to 3 mod 4. The number of non-zero entries per row is $q^2+q+1-(q+1) = q^2$, which is odd. The number of columns where two distinct rows have non-zero entries is $q^2+q+1-2(q+1)+1 = q^2-q$. This number is 2 mod 4 since $q \equiv 3 \bmod 4$. Recall that in the projective 2-space over $\mathrm{GF}(q)$, each line contains $q+1$ points, and two distinct lines intersect in a single point. Now we only need to check that any two distinct rows (corresponding to distinct projective lines L, L') are orthogonal over the integers. We first observe that the following equality holds over the integers.

$$\sum_P \eta(L(P))\eta(L'(P)) = \frac{1}{q-1} \sum_{v \neq (0,0,0)} \eta(L(v))\eta(L'(v)) \tag{5}$$

where,

$$\eta(x) \;=\; \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \text{ is a (non-zero) square} \\ -1 & \text{if } x \text{ is not a square} \end{cases}.$$

[The first sum is over all points P of the projective 2-space. The second is over all non-zero triples v in $\mathbb{F}^3$.] The equality holds because if we take two non-zero triples u and $w = \alpha u$ ($\alpha \neq 0$) corresponding to the same projective point, then

$$\begin{aligned}\eta(L(w))\eta(L'(w)) &= \eta(L(\alpha u))\eta(L'(\alpha u)) \\ &= \eta(\alpha L(u))\eta(\alpha L'(u)) \\ &= \eta(\alpha)\eta(L(u))\eta(\alpha)\eta(L'(u)) \\ &= \eta(L(u))\eta(L'(u))\end{aligned}$$

Now consider the sum on the right hand side of (5). We have

$$\sum_{v\neq(0,0,0)} \eta(L(v))\eta(L'(v)) = \sum_{a,b\in\mathbb{F};a,b\neq 0} \sum_{\substack{v:L(v)=a,L'(v)=b \\ v\neq(0,0,0)}} \eta(a)\eta(b)$$

The linear forms corresponding to two distinct projective lines are linearly independent; i.e., L and L' are linearly independent. Hence, for every pair (a, b) in the sum above, there are exactly q triples v such that $L(v) = a$ and $L'(v) = b$. Thus,

$$\begin{aligned}\sum_{v\neq(0,0,0)} \eta(L(v))\eta(L'(v)) &= q \cdot \sum_{a,b\in\mathbb{F};\ a,b\neq 0} \eta(a)\eta(b) \\ &= q \cdot \sum_{a,b\in\mathbb{F};\ a,b\neq 0} \eta(ab) \\ &= q(q-1) \cdot \sum_{c\in\mathbb{F};\ c\neq 0} \eta(c) \\ &= 0\end{aligned}$$

The last equality holds because there are exactly $(q-1)/2$ squares and the same number of non–squares in $\mathbb{F} - \{0\}$. We conclude that the left hand side of (5) is 0; hence, the rows corresponding to distinct projective lines are orthogonal over the integers.

We have thus proved the following lemma.

Lemma 3 *If $q \equiv 3 \bmod 4$ is a prime power then there is a good matrix of order q^2+q+1. Note that infinitely many such q exist.*

We can now easily prove the following theorem and its corollary.

Theorem 2 *For infinitely many $n \equiv 0, 2 \bmod 4$ we have an odd cover of K_n using $\frac{n}{2}$ complete bipartite graphs.*

Proof: We use $\frac{n}{2} \times \frac{n}{2}$ *good* matrices to construct an odd cover of K_n using $\frac{n}{2}$ complete bipartite graphs(see Lemma 1). For infinitely many $n \equiv 0 \bmod 4$, we can use the *good* matrices of Corollary 1. For infinitely many $n \equiv 2 \bmod 4$, we can use the *good* matrices of Lemma 3. ■

Corollary 2 *For infinitely many $n \equiv 1, 3 \bmod 4$ we have an odd cover of K_n using $\lceil \frac{n}{2} \rceil$ complete bipartite graphs.*

Proof: For odd n, any odd cover of K_{n+1} using $\frac{n+1}{2}$ complete bipartite graphs gives us an odd cover for K_n too. The corollary now follows from the above theorem. ∎

We also prove the following lemma, which allows us to construct homogeneous $\Sigma\Pi\Sigma$ circuits for $S_n^2(X)$ with $\lfloor \frac{n}{2} \rfloor$ multiplication gates, for infinitely many $n \equiv 1 \bmod 4$.

Lemma 4 *If $S_n^2(X), n \equiv 0 \bmod 4$, can be computed over GF(2) by a homogeneous $\Sigma\Pi\Sigma$ circuit using $\frac{n}{2}$ multiplication gates, then $S_{n+1}^2(X)$ can be computed over GF(2) by a homogeneous $\Sigma\Pi\Sigma$ circuit using $\frac{n}{2}$ multiplication gates.*

Proof: Consider a homogeneous circuit over GF(2)

$$\sum_{i=1}^{r} L_i(X_1, \ldots, X_n) R_i(X_1, \ldots, X_n) \tag{6}$$

for $S_n^2(X_1, \ldots, X_n)$, $n \equiv 0 \bmod 4$, where $r = \frac{n}{2}$. Define for $1 \leq i \leq r$, homogeneous linear forms $L_i'(X_1, \ldots, X_{n+1})$, $R_i'(X_1, \ldots, X_{n+1})$ over GF(2) as follows.

$$\begin{array}{rcll} L_i'(X_1, \ldots, X_{n+1}) & \stackrel{\Delta}{=} & L_i(X_1, \ldots, X_n) + X_{n+1} & \text{if } L_i \text{ has an odd number of terms} \\ & \stackrel{\Delta}{=} & L_i(X_1, \ldots, X_n) & \text{otherwise} \\ R_i'(X_1, \ldots, X_{n+1}) & \stackrel{\Delta}{=} & R_i(X_1, \ldots, X_n) + X_{n+1} & \text{if } R_i \text{ has an odd number of terms} \\ & \stackrel{\Delta}{=} & R_i(X_1, \ldots, X_n) & \text{otherwise} \end{array}$$

We have the following equality over GF(2).

Claim

$$S_{n+1}^2(X_1, \ldots, X_{n+1}) = \sum_{i=1}^{r} L_i'(X_1, \ldots, X_{n+1}) R_i'(X_1, \ldots, X_{n+1})$$

Proof: Define homogeneous linear forms over $\mathbb{Z}$, $L_i''(X_1, \ldots, X_{n+1})$, $R_i''(X_1, \ldots, X_{n+1})$, for $1 \leq i \leq r$, as follows.

$$\begin{array}{rcl} L_i''(X_1, \ldots, X_{n+1}) & \stackrel{\Delta}{=} & L_i(X_1, \ldots, X_n) + a_i X_{n+1} \\ R_i''(X_1, \ldots, X_{n+1}) & \stackrel{\Delta}{=} & R_i(X_1, \ldots, X_n) + b_i X_{n+1} \end{array}$$

where a_i, b_i denote the number of (non-zero) terms in L_i, R_i respectively. Consider the following formula over $\mathbb{Z}$.

$$\sum_{i=1}^{r} L_i''(X_1, \ldots, X_{n+1}) R_i''(X_1, \ldots, X_{n+1}) \tag{7}$$

Let $c_{jk}, 1 \leq j \leq k \leq n$ denote the coefficient of $X_j X_k$ in (6), treating (6) as a formula over $\mathbb{Z}$ instead of over GF(2). Since formula (6) computes $S_n^2(X)$ over GF(2), $c_{jk}, 1 \leq$

$j < k \leq n$ are odd, and $c_{jj}, 1 \leq j \leq n$ are even. Let $c''_{jk}, 1 \leq j \leq k \leq n+1$ denote the coefficient of X_jX_k in (7) (note that c''_{jk} is an integer). For $1 \leq j \leq k \leq n$, $c''_{jk} = c_{jk}$. We will now show that $c''_{j,n+1}, 1 \leq j \leq n$ are odd, and $c''_{n+1,n+1}$ is even. This suffices to prove the claim, since $L''_i \equiv L'_i \bmod 2$ and $R''_i \equiv R'_i \bmod 2$.

For any $1 \leq j \leq n$, it can be easily checked that

$$\begin{aligned} c''_{j,n+1} &= \sum_{\substack{k:1\leq k\leq n \\ k\neq j}} c_{jk} + 2c_{jj} \\ &\equiv \sum_{\substack{k:1\leq k\leq n \\ k\neq j}} 1 + 0 \pmod 2 \\ &\equiv 1 \pmod 2 \end{aligned}$$

The last equivalence follows from the fact that, for any fixed j, the number of monomials $X_jX_k, 1 \leq k \leq n, k \neq j$ is odd, since n is even.

$$\begin{aligned} c''_{n+1,n+1} &= \sum_{1\leq j\leq k\leq n} c_{jk} \\ &= \sum_{1\leq j<k\leq n} c_{jk} + \sum_{1\leq j\leq n} c_{jj} \\ &\equiv \left(\sum_{1\leq j<k\leq n} 1 + \sum_{1\leq j\leq n} 0 \right) \pmod 2 \\ &\equiv 0 \pmod 2 \end{aligned}$$

The last equivalence follows from the fact that the number of monomials $X_jX_k, 1 \leq j < k \leq n$ is even, since $n \equiv 0 \bmod 4$.

Hence the claim is proved. ■

The lemma now follows from the above claim. ■

We can now prove the following theorem.

Theorem 3 *For infinitely many $n \equiv 0, 2, 3 \bmod 4$ we have homogeneous $\Sigma\Pi\Sigma$ circuits computing $S^2_n(X)$ over GF(2) using $\lceil \frac{n}{2} \rceil$ multiplication gates. For infinitely many $n \equiv 1 \bmod 4$ we can compute $S^2_n(X)$ over GF(2) using homogeneous $\Sigma\Pi\Sigma$ circuits having $\lfloor \frac{n}{2} \rfloor$ multiplication gates.*

Proof: The first part of the theorem follows from Theorem 2 and Corollary 2. To prove the second part, consider a homogeneous circuit for $S^2_{n-1}(X_1, \ldots, X_{n-1})$, $n \equiv 1 \bmod 4$, using $r = \frac{n-1}{2}$ multiplication gates. Such circuits exist for infinitely many $n \equiv 1 \bmod 4$ by the first part of the theorem. We now invoke Lemma 4 to complete the proof. ■

3.2 $1 \bmod p$ cover problem, p an odd prime

In this subsection we will in fact show, for any odd number p (not necessarily prime), that there is a $1 \bmod p$ cover of K_{2n} by n complete bipartite graphs whenever there exists an

$n \times n$ matrix *good for* p (defined below). Also, from a $1 \bmod p$ cover of K_{2n+2} by $n+1$ bipartite graphs, we get a $1 \bmod p$ cover of K_{2n+1} by $n+1$ bipartite graphs. We note that the skew Hadamard matrix construction of Section 3.1 does not generalise to give us matrices *good for* p, when p is odd.

Definition 2 *Let p be an odd number. A matrix with entries from $\{-1, 0, 1\}$ is called a* good matrix for p *if it satisfies the following conditions:*

1. *In every row, the number of non-zero entries is* $1 \bmod p$.
2. *For every pair of distinct rows, the number of columns where they both have non-zero entries is congruent to* $2 \bmod 2p$.
3. *Any two distinct rows are orthogonal over the integers.*

Lemma 5 *Let p be an odd number. If an $n \times n$ matrix is good for p, then the n complete bipartite graphs that arise from it form a $1 \bmod p$ cover of K_{2n}. If $n = q^2 + q + 1$ where q is a prime power and $q \equiv -1 \bmod 2p$, then an $n \times n$ good matrix for p exists. Note that infinitely many such q exist, by a result of Dirichlet.*

Proof: The proof of the fact that an $n \times n$ good matrix for p gives us a $1 \bmod p$ cover of K_{2n} by n complete bipartite graphs, is similar to the proof of Lemma 1. The construction of an $n \times n$ good matrix for p when n is of the given form is similar to the symmetric designs construction of Section 3.1. ■

From the lemma, we can now prove the following theorem.

Theorem 4 *Given an odd number p, for infinitely many odd and even n, we have a $1 \bmod p$ cover of K_n using $\left\lceil \frac{n}{2} \right\rceil$ bipartite graphs.*

3.3 Fields of characteristic different from 2

Now we give the proofs for the upper bounds in the homogeneous circuit model for computing $S^2_n(X)$ over various fields of characteristic different from 2. We start by proving two lemmas.

Lemma 6 *$S^2_{2k+1}(X_1, \ldots, X_{2k+1})$ can be computed by a homogeneous $\Sigma\Pi\Sigma$ circuit using $k+1$ multiplication gates over any field of characteristic not equal to 2 which has square roots of -1.*

Proof: This result has been observed implicitly by Shpilka [Shp01]. We give a proof here for completeness. Let i denote a square root of -1.

$$\begin{aligned} & S^2_{2k+1}(X_1, \ldots, X_{2k+1}) \\ = \; & \frac{1}{2}((\sum_{j=1}^{2k+1} X_j)^2 - \sum_{j=1}^{2k+1} X_j^2) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}(((\sum_{j=1}^{2k+1} X_j)^2 - X_1^2) - \sum_{j=2}^{2k+1} X_j^2) \\
&= \frac{1}{2}((\sum_{j=2}^{2k+1} X_j)(2X_1 + \sum_{j=2}^{2k+1} X_j) - \sum_{j=1}^{k}(X_{2j}^2 + X_{2j+1}^2)) \\
&= \frac{1}{2}((\sum_{j=2}^{2k+1} X_j)(2X_1 + \sum_{j=2}^{2k+1} X_j) - \sum_{j=1}^{k}(X_{2j} + iX_{2j+1})(X_{2j} - iX_{2j+1}))
\end{aligned}
$$

This shows that $S^2_{2k+1}(X_1, \ldots, X_{2k+1})$ can be done with $k+1$ multiplication gates. ■

Lemma 7 *$S^2_{2k}(X_1, \ldots, X_{2k})$ can be computed by a homogeneous $\Sigma\Pi\Sigma$ circuit using k multiplication gates over any field $\mathbb{F}$ of characteristic not equal to 2 which has square roots of -1, 2 and $2k-1$.*

Proof: Let $a_m(X_1, \ldots, X_{2k})$ and $b_m(X_1, \ldots, X_{2k})$ denote the two homogeneous linear forms feeding into the mth multiplication gate, $1 \leq m \leq k$. Let

$$
\left.
\begin{array}{rcl}
a_m(X_1, \ldots, X_{2k}) & \stackrel{\Delta}{=} & \sum_{n=1}^{2k} a_{mn} X_{mn} \\
b_m(X_1, \ldots, X_{2k}) & \stackrel{\Delta}{=} & \sum_{n=1}^{2k} b_{mn} X_{mn}
\end{array}
\right\} \qquad 1 \leq m \leq k
$$

Since the circuit computes $S^2_{2k}(X_1, \ldots, X_{2k})$, equating the coefficients of $X_j^2, 1 \leq j \leq 2k$ we get

$$
\sum_{m=1}^{k} a_{mj} b_{mj} = 0 \qquad 1 \leq j \leq 2k
$$

Since the characteristic is not equal to 2, we can get an equivalent equation by multiplying both sides by 2.

$$
\sum_{m=1}^{k} (a_{mj} b_{mj} + a_{mj} b_{mj}) = 0 \qquad 1 \leq j \leq 2k \tag{8}
$$

Equating the coefficients of $X_j X_l, 1 \leq j < l \leq 2k$ we get

$$
\sum_{m=1}^{k} (a_{mj} b_{ml} + a_{ml} b_{mj}) = 1 \qquad 1 \leq j < l \leq 2k \tag{9}
$$

Let us define vectors $y_j \in \mathbb{F}^{2k}, 1 \leq j \leq 2k$ as follows

$$
y_j^T \stackrel{\Delta}{=} (a_{1j}, b_{1j}, a_{2j}, b_{2j}, \ldots, a_{kj}, b_{kj})
$$

We can write (8), (9) in a succinct matrix form as

$$
\left.
\begin{array}{rcll}
y_j^T \mathbf{A} y_j & = & 0 & 1 \leq j \leq 2k \\
y_j^T \mathbf{A} y_l & = & 1 & 1 \leq j < l \leq 2k
\end{array}
\right\} \tag{10}
$$

where the $2k \times 2k$ matrix $\mathbf{A}$ consists of k blocks of the 2×2 matrix

$$M \triangleq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

arranged along the diagonal. M has two eigenvalues 1 and -1, with corresponding eigenvectors $u_1^T = (1,1)$ and $u_{-1}^T = (1,-1)$ (note that $1 \neq -1$ in $\mathbb{F}$). It will be convenient to scale these vectors to obtain alternate eigenvectors $v_1^T = \frac{1}{\sqrt{2}}(1,1)$ and $v_{-1}^T = \frac{1}{\sqrt{2}}(i,-i)$, where i denotes a square root of -1 in $\mathbb{F}$ (note that $2 \neq 0$ in $\mathbb{F}$ and 2 and -1 have square roots in $\mathbb{F}$). Now,

$$v_1^T M v_1 = v_{-1}^T M v_{-1} = 1$$
$$v_1^T M v_{-1} = 0$$

The 2×2 matrix

$$N \triangleq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

is the change of basis matrix for going from the basis $\{v_1, v_{-1}\}$ of $\mathbb{F}^2$ to the standard basis $\{(1,0)^T, (0,1)^T\}$ of $\mathbb{F}^2$. We define another $2k \times 2k$ matrix $\mathbf{B}$, which consists of k blocks of the 2×2 matrix N arranged along the diagonal. $\mathbf{B}$ is a change of basis matrix from a basis of $\mathbb{F}^{2k}$ consisting of eigenvectors of $\mathbf{A}$, to the standard basis of $\mathbb{F}^{2k}$. If $z_j, 1 \leq j \leq 2k$ are the representations of the vectors $y_j, 1 \leq j \leq 2k$ in the eigenbasis of $\mathbf{A}$, then

$$y_j = \mathbf{B} z_j \qquad 1 \leq j \leq 2k$$

Since

$$\mathbf{B}^T \mathbf{A} \mathbf{B} = \mathbf{I}_{2k}$$

where $\mathbf{I}_{2k}$ is the $2k \times 2k$ identity matrix, (10) now becomes

$$\begin{aligned} z_j^T z_j &= 0 \qquad 1 \leq j \leq 2k \\ z_j^T z_l &= 1 \qquad 1 \leq j < l \leq 2k \end{aligned}$$

We can write a set of equations equivalent to the above as follows (since $2 \neq 0$ in $\mathbb{F}$)

$$\left.\begin{aligned} z_j^T z_j &= 0 \qquad 1 \leq j \leq 2k \\ (z_j - z_l)^T (z_j - z_l) &= -2 \qquad 1 \leq j < l \leq 2k \end{aligned}\right\} \tag{11}$$

The second equation above can be thought as finding vectors $z_j \in \mathbb{F}^{2k}, 1 \leq j \leq 2k$ such that the "distance" between any two of them is $\sqrt{-2}$. The following set of vectors meets this requirement

$$z'_j = i e_j \qquad 1 \leq j \leq 2k$$

where $e_j, 1 \leq j \leq 2k$ are the standard basis vectors in $\mathbb{F}^{2k}$. We now have to ensure that the "length" of each vector is 0. For this shift the origin to a point $p \triangleq (w, w, \ldots, w)$, where w

will be determined later. Note that this operation does not change the "distance" between any pair of vectors. To determine w we have to solve the following equation

$$(i-w)^2 + (2k-1)w^2 = 0$$

which can be solved whenever $2k-1$ has a square root in the field. We now define

$$z_j \stackrel{\Delta}{=} z'_j - p \qquad 1 \leq j \leq 2k$$

The vectors $z_j, 1 \leq j \leq 2k$ are a solution to (11) which in turn implies a solution to (10) which proves the existence of a homogeneous circuit for the polynomial $S^2_{2k}(X_1, \ldots, X_{2k})$ using k multiplication gates. ∎

Using Lemmas 6 and 7, we can now prove our upper bound result for complex numbers. The proofs of our upper bounds for GF(p^r), p an odd prime can be found in the appendix.

Theorem 5 *$S^2_n(X_1, \ldots, X_n)$ can be computed by a homogeneous $\Sigma\Pi\Sigma$ circuit using $\lceil \frac{n}{2} \rceil$ multiplication gates over the field of complex numbers.*

Proof: Follows directly from Lemmas 6 and 7. ∎

4 Lower bounds

4.1 Preliminaries

In this subsection, we develop a framework for proving lower bounds for computing $S^2_n(X)$ in the inhomogeneous $\Sigma\Pi\Sigma$ model, based on the method of substitution [SW99, Shp01]. Suppose that over a field $\mathbb{F}$

$$S^2_n(X) = \sum_{i=1}^{r} \prod_{j=1}^{s_i} L_{ij}(X) \tag{12}$$

where each $L_{ij}(X)$ is a linear form over $X_1, \ldots, X_n$, not necessarily homogeneous. We wish to show that r must be large. Following the proof of the Graham-Pollack theorem that was sketched in the introduction, we could try to force some of the L_{ij}'s to zero by setting the variables to appropriate field elements. There are two difficulties with this plan. First, since the L_{ij}'s are not necessarily homogeneous, we may not be able to set all of them to zero; we can do so if the linear forms have linearly independent homogeneous parts. The second difficulty arises from the nature of the underlying field: as remarked in the introduction, $S^2_n(X)$ might vanish on non-trivial subspaces of $\mathbb{F}^n$.

In this subsection, our goal is to first show that if r is small, then $S^2_n(X)$ must be zero over a linear subspace of $\mathbb{F}^n$ of large dimension. Similar observations have been used by Shpilka and Wigderson [SW99, Lemma 3.3] and Shpilka [Shp01, Claim 4.6]. Our second goal is to examine linear subspaces of $\mathbb{F}^n$ over which $S^2_n(X)$ is forced to be zero. We derive conditions on such subspaces, and relate them to the existence of a certain family of vectors. Later on, we will exploit these equations based on the field in question, and derive our lower bounds for r.

Goal 1: Obtaining the subspace.

Lemma 8 *If $S_n^2(X)$ can be written in the form of (12) over a field $\mathbb{F}$, then there exist homogeneous linear forms $\ell_1, \ell_2, \ldots, \ell_r$ in variables $X_1, X_2, \ldots, X_{n-r}$ such that*

$$S_n^2(X_1, X_2, \ldots, X_{n-r}, \ell_1, \ell_2, \ldots, \ell_r) = 0 \tag{13}$$

Proof: We implement the idea discussed at the beginning of Section 4.1. Given an expression of the form (12), we collect a maximal consistent set of equations of the form $L_{ij}(X) = 0$, with at most one equation for each i. We write these equations in the form

$$\mathbf{A}X = b \tag{14}$$

where $\mathbf{A}$ is an $r' \times n$ matrix and $b \in \mathbb{F}^{r'}$ for some $r' \leq r$. Since (14) has a solution, and the rank of $\mathbf{A}$ is at most r, there is an affine subspace of solutions Γ of dimension $n - r$ in $\mathbb{F}^n$. (If the actual solution set is an affine subspace of dimension greater than $n-r$, then we let Γ be an affine subspace of the solution space of dimension exactly $n-r$.) We can view this set of solutions as follows (see e.g. [Art91, Chapter 1]): there are $n-r$ 'free variables,' and the values of the remaining r variables are given by (possibly inhomogeneous) linear forms in these $n - r$ variables. Since $S_n^2(X)$ is symmetric, we may assume that the $n - r$ 'free variables' are $X_1, X_2, \ldots, X_{n-r}$; for $i = 1, 2, \ldots, r$, let $\tilde{\ell}_i$ be the (possibly inhomogeneous) linear form in $X_1, X_2, \ldots, X_{n-r}$ that determines the value of X_{n-r+i} once the values for $X_1, X_2, \ldots, X_{n-r}$ are fixed.

Observe that $S_n^2(X)$ is constant over Γ. To see this, consider the right hand side of (12). If for some i an L_{ij} participates in (14), then that product contributes zero to the sum. Otherwise, since the chosen set of equations is maximal, for this i, the homogeneous part of each L_{ij} is in the row span of the matrix $\mathbf{A}$. That is, once $\mathbf{A}X$ has been fixed to b, the homogeneous part, and hence the entire linear form, is fixed. We conclude that

$$S_n^2(X_1, X_2, \ldots, X_{n-r}, \tilde{\ell}_1, \tilde{\ell}_2, \ldots, \tilde{\ell}_r) = \textit{constant}$$

Now comparing the coefficients of monomials of degree two on both sides of the above equation, we see that

$$S_n^2(X_1, X_2, \ldots, X_{n-r}, \ell_1, \ell_2, \ldots, \ell_r) = 0$$

where ℓ_i is the homogeneous part of $\tilde{\ell}_i$. ∎

Goal 2: The nature of the subspace. Our goal now is to understand the algebraic structure of the coefficients that appear in the linear forms $\ell_1, \ell_2, \ldots, \ell_r$ promised by Lemma 8. Let $\ell_i = \sum_{j=1}^{n-r} \ell_{ij} X_j, \ell_{ij} \in \mathbb{F}$, and let $\mathbf{L}$ be the $r \times (n-r)$ matrix (ℓ_{ij}). Let $y_1, y_2, \ldots, y_{n-r} \in \mathbb{F}^r$ be the $n - r$ columns of $\mathbf{L}$. We will obtain conditions on the columns by computing the coefficients of monomials X_j^2 for $1 \leq j \leq n-r$, and $X_i X_j$ for $1 \leq i < j \leq n - r$, in equation (13). For X_j^2 $(1 \leq j \leq n-r)$, we obtain the following equation over $\mathbb{F}$.

$$\sum_{k=1}^{r} \ell_{kj} + \sum_{1 \leq k < k' \leq r} \ell_{kj} \ell_{k'j} = 0 \quad 1 \leq j \leq r \tag{15}$$

For monomials of the form X_iX_j $(1 \leq i < j \leq n-r)$, we obtain the following equation over $\mathbb{F}$.

$$1 + \sum_{k=1}^{r} \ell_{ki} + \sum_{k=1}^{r} \ell_{kj} + \sum_{1 \leq k < k' \leq r} (\ell_{ki}\ell_{k'j} + \ell_{k'i}\ell_{kj}) = 0 \quad 1 \leq i < j \leq n-r \tag{16}$$

For a positive integer m, let $\mathbf{1}_m$ be the all 1's column vector and $\mathbf{0}_m$ be the all 0's column vector of dimension m. Let $\mathbf{U}_m$ be the $m \times m$ matrix with 1's above the diagonal and zero elsewhere. Let $\mathbf{J}_m$ be the $m \times m$ matrix with all 1's, and let $\mathbf{I}_m$ be the $m \times m$ identity matrix. Using this notation, we can rewrite (15) and (16) as follows.

$$\mathbf{1}_r^T y_j + y_j^T \mathbf{U}_r y_j = 0 \quad 1 \leq j \leq n-r \tag{17}$$

$$1 + \mathbf{1}_r^T y_i + \mathbf{1}_r^T y_j + y_i^T (\mathbf{J}_r - \mathbf{I}_r) y_j = 0 \quad 1 \leq i < j \leq n-r \tag{18}$$

If the characteristic of $\mathbb{F}$ is not two, we may rewrite (17) as

$$2\mathbf{1}_r^T y_j + y_j^T (\mathbf{J}_r - \mathbf{I}_r) y_j = 0 \quad 1 \leq j \leq n-r \tag{19}$$

With this, we are now ready to prove lower bounds. We will exploit (17), (18) and (19) (if the characteristic is not 2) to derive lower bounds for various fields.

4.2 Lower bounds for GF(2)

Let $\mathbb{Z}$ stand for the integers. For $y \in \mathbb{Z}^r$, let $|y|$ denote the number of odd components in y. For $y, y' \in \mathbb{Z}^r$, let $y \cdot y' \stackrel{\Delta}{=} \sum_{m=1}^{r} y_m y'_m$ be the dot product of y and y' over $\mathbb{Z}$.

Lemma 9 *Suppose $\ell_1, \ldots, \ell_r$ are homogeneous linear forms in the variables $X_1, \ldots, X_{n-r}$ such that $S_n^2(X_1, \ldots, X_{n-r}, \ell_1, \ldots, \ell_r) = 0$ over GF(2). Then $r \geq \lfloor \frac{n}{2} \rfloor$. If $n \equiv 3 \bmod 4$, then $r \geq \lceil \frac{n}{2} \rceil$.*

Proof: We use the arguments of Section 4.1. If there exist homogeneous linear forms $\ell_1, \ldots, \ell_r$ over variables $X_1, \ldots, X_{n-r}$ so that $S_n^2(X_1, \ldots, X_{n-r}, \ell_1, \ldots, \ell_r) = 0$ over GF(2), we have, from (17) and (18), vectors $y_j \in \mathrm{GF}(2)^r, 1 \leq j \leq n-r$ such that the following equations hold over $GF(2)$ (recall that J_r denotes the $r \times r$ all 1's matrix, and I_r denotes the $r \times r$ identity matrix).

$$\mathbf{1}_r^T y_j + y_j^T \mathbf{U}_r y_j = 0 \quad 1 \leq j \leq n-r \tag{20}$$

$$1 + \mathbf{1}_r^T y_i + \mathbf{1}_r^T y_j + y_i^T (\mathbf{J}_r - \mathbf{I}_r) y_j = 0 \quad 1 \leq i < j \leq n-r \tag{21}$$

Instead of thinking of the above equations as holding over $GF(2)$, it will help for this proof to treat the vectors y_j as elements of $\mathbb{Z}^r$ and the equations (20) and (21) as equivalences over the integers mod2.

By counting the number of odd components (i.e. 1's) on the left and right hand side of (20), we obtain

$$|y_j| + \binom{|y_j|}{2} \equiv 0 \pmod 2 \quad 1 \leq j \leq n-r$$

From this it follows that

$$|y_j| \equiv 0 \text{ or } 3 \pmod 4 \quad 1 \le j \le n-r \tag{22}$$

Since $y_i^T(\mathbf{J}_r - \mathbf{I}_r)y_j = |y_i|\,|y_j| - y_i \cdot y_j$ over $\mathbb{Z}$, by counting the number of odd components (i.e. 1's) on both sides of (21), we get

$$|y_i| + |y_j| + |y_i|\,|y_j| + y_i \cdot y_j \equiv 1 \pmod 2 \quad 1 \le i < j \le n-r$$

In other words,

$$y_i \cdot y_j \equiv (1 + |y_i|)(1 + |y_j|) \pmod 2 \quad 1 \le i < j \le n-r \tag{23}$$

Let $w_1, \ldots, w_s$ be the vectors among $y_1, \ldots, y_{n-r}$ with $|y_j|$ odd, and let $e_1, \ldots, e_t$ be the remaining $t = n - r - s$ vectors, with $|y_j|$ even.

Claim If $y_1, y_2, \ldots, y_{n-r}$ are not linearly independent over GF(2), then the only dependency over GF(2) among them is $\sum_{k=1}^{t} e_k = \mathbf{0}_r$. Also, in that case, t is odd.

Proof: Let

$$\sum_{i=1}^{s} \alpha_i w_i + \sum_{k=1}^{t} \beta_k e_k \equiv \mathbf{0}_r \pmod 2$$

In the above equation, we think of w_i, e_k as vectors in $\mathbb{Z}^r$, α_i, β_k as integers, and the equality as an equivalence over the integers mod2. We take dot products of the two sides above with w_i and conclude, using (23), that $\alpha_i \equiv 0 \bmod 2$, for $1 \le i \le s$. Similarly, taking dot products with e_k, we obtain the system of equations $(\mathbf{J}_t - \mathbf{I}_t)\beta \equiv \mathbf{0}_t \bmod 2$, where $\beta \in \mathbb{Z}^t$ and the kth component of β is β_k. If t is even, $(\mathbf{J}_t - \mathbf{I}_t)$ is full-rank over GF(2), so $\beta \equiv \mathbf{0}_t \bmod 2$. So the y_j's are linearly independent over GF(2), which is a contradiction.

Now, if the y_j's are not linearly independent, then t must be odd, and the only dependency among them corresponds to β such that $(\mathbf{J}_t - \mathbf{I}_t)\beta \equiv \mathbf{0}_t \bmod 2$. The only non–trivial solution mod2 for this equation is $\beta \equiv \mathbf{1}_t \bmod 2$. ∎

By the claim above, we see that there are at least $n-r-1$ linearly independent vectors over GF(2) among the y_j's. Since the y_j's are r-dimensional vectors, we get $r \ge n - r - 1$ i.e. $r \ge \lfloor \frac{n}{2} \rfloor$. This proves the first part of the lemma.

To obtain a better bound for r when $n \equiv 3 \bmod 4$, we make better use of our equations, especially (22), which we have neglected so far. So suppose $n = 2r + 1$ and $n \equiv 3 \bmod 4$. We shall derive a contradiction.

If $n = 2r + 1$, then $n - r > r$, and since the y_j are r-dimensional vectors, y_j are not linearly independent over GF(2). Then by the claim above, t is odd, $\sum_{k=1}^{t} e_k \equiv \mathbf{0}_r \bmod 2$, and $w_1, \ldots, w_s, e_1, \ldots, e_{t-1}$ are linearly independent over GF(2). Since $s+t-1 = n-r-1 = r$, these vectors form a basis (over GF(2)) of the vector space $\mathrm{GF}(2)^r$; in particular $\mathbf{1}_r$ is in their span, that is

$$\sum_{i=1}^{s} \alpha_i w_i + \sum_{k=1}^{t-1} \beta_k e_k \equiv \mathbf{1}_r \pmod 2$$

for some $\alpha_i, \beta_k \in \mathbb{Z}$. Taking dot products with w_i and e_k, we conclude (using (23)) that $\alpha_i \equiv 1 \bmod 2$ for $1 \leq i \leq s$, and $(\mathbf{J}_{t-1} - \mathbf{I}_{t-1})\beta \equiv \mathbf{0}_{t-1} \bmod 2$, where $\beta \in \mathbb{Z}^{t-1}$ and the kth component of β is β_k. Since t is odd, $\mathbf{J}_{t-1} - \mathbf{I}_{t-1}$ is full rank over GF(2), and $\beta \equiv \mathbf{0}_{t-1} \bmod 2$. Thus

$$\sum_{i=1}^{s} w_i \equiv \mathbf{1}_r \pmod 2 \tag{24}$$

It is easy to verify that for all integer vectors y

$$|y| \equiv y \cdot y \pmod 4 \tag{25}$$

Using (24) and (25), $(\sum_{i=1}^{s} w_i) \cdot (\sum_{i=1}^{s} w_i) \equiv |\sum_{i=1}^{s} w_i| \equiv r \bmod 4$, that is

$$\sum_{i=1}^{s} w_i \cdot w_i + 2 \sum_{1 \leq i < j \leq s} w_i \cdot w_j \equiv r \pmod 4$$

By (22) and (25), $w_i \cdot w_i \equiv |w_i| \equiv 3 \bmod 4$, and by (23), $w_i \cdot w_j \equiv 0 \bmod 2$ for $i \neq j$. Thus

$$\sum_{i=1}^{s} 3 + \sum_{1 \leq i < j \leq s} 0 \equiv r \pmod 4$$

$$\Rightarrow 3s \equiv r \pmod 4 \tag{26}$$

Similarly, by starting with $\sum_{k=1}^{t} e_k \equiv \mathbf{0}_r \bmod 2$ and using (25) we get that, $(\sum_{k=1}^{t} e_k) \cdot (\sum_{k=1}^{t} e_k) \equiv |\sum_{k=1}^{t} e_k| \equiv 0 \bmod 4$, that is

$$\sum_{i=1}^{t} e_i \cdot e_i + 2 \sum_{1 \leq i < j \leq t} e_i \cdot e_j \equiv 0 \pmod 4$$

By (22) and (25), $e_i \cdot e_i \equiv 0 \bmod 4$, and by (23), $e_i \cdot e_j \equiv 1 \bmod 2$ for $i \neq j$. Thus

$$\sum_{i=1}^{t} 0 + \sum_{1 \leq i < j \leq t} 2 \equiv 0 \pmod 4$$

$$\Rightarrow \frac{t(t-1)}{2}\, 2 \equiv 0 \bmod 4$$

Since t is odd, we conclude that $t \equiv 1 \bmod 4$. But then, using (26),

$$n \equiv r + s + t \equiv 3s + s + 1 \equiv 1 \pmod 4$$

which is a contradiction.

Since $r \geq \lfloor \frac{n}{2} \rfloor$ holds for all n, we have shown that if $n \equiv 3 \bmod 4$, then $r \geq \lceil \frac{n}{2} \rceil$. ∎

Using Lemmas 8 and 9, we can now prove the following theorem.

Theorem 6 *Any (not necessarily homogeneous) ΣΠΣ circuit computing $S_n^2(X_1, \ldots, X_n)$ over GF(2) requires at least $\lceil \frac{n}{2} \rceil$ multiplication gates if $n \equiv 0, 2, 3 \bmod 4$, and at least $\lfloor \frac{n}{2} \rfloor$ multiplication gates if $n \equiv 1 \bmod 4$.*

4.3 Fields of characteristic different from 2

In this subsection, we give the proofs of our lower bounds for computing $S^2_n(X)$ using (not necessarily homogeneous) $\Sigma\Pi\Sigma$ arithmetic circuits over various fields of characteristic different from 2. Lemma 10 proves an upper bound on the dimension of a subspace over which $S^2_{2k}(X_1, \ldots, X_{2k})$ vanishes. The proof uses Nisan and Wigderson's method of partial derivatives.

Lemma 10 *If $k \neq 0$ in the field $\mathbb{F}$ then $S^2_{2k}(X_1, \ldots, X_{k+1}, \ell_1, \ldots, \ell_{k-1}) \neq 0$ for any $k-1$ homogeneous linear forms $\ell_1, \ldots, \ell_{k-1}$ in the variables $X_1, \ldots, X_{k+1}$ over $\mathbb{F}$.*

Proof: This lemma is in fact a special case of a more general result due to Shpilka [Shp01]. We give a short proof of it here, which is essentially Shpilka's proof restricted to our special case. We have the identity

$$\begin{aligned} S^2_{2k}(X_1, \ldots, X_{k+1}, \ell_1, \ldots, \ell_{k-1}) &= S^2_{k+1}(X_1, \ldots, X_{k+1}) + \\ & (X_1 + \cdots + X_{k+1})(\ell_1 + \cdots + \ell_{k-1}) + \\ & S^2_{k-1}(\ell_1, \ldots, \ell_{k-1}) \end{aligned}$$

Assuming for the sake of contradiction that the left hand side of the above equation is zero, we get

$$\begin{aligned} & S^2_{k+1}(X_1, \ldots, X_{k+1}) \\ &= -(X_1 + \cdots + X_{k+1})(\ell_1 + \cdots + \ell_{k-1}) - S^2_{k-1}(\ell_1, \ldots, \ell_{k-1}) \end{aligned}$$

We take the first order partial derivatives with respect to $X_1, \ldots, X_{k+1}$ of both the sides of the above equation. Since $k \neq 0$ in $\mathbb{F}$, the vector space spanned by the set of first-order partial derivatives of $S^2_{k+1}(X_1, \ldots, X_{k+1})$ is of dimension $k+1$. This follows from the fact that the matrix $\mathbf{J}_{k+1} - \mathbf{I}_{k+1}$ is of full rank if $k \neq 0$ in $\mathbb{F}$, where $\mathbf{J}_{k+1}$ is the $(k+1) \times (k+1)$ all 1's matrix and $\mathbf{I}_{k+1}$ is the $(k+1) \times (k+1)$ identity matrix. The vector space spanned by the first order partial derivatives of the right hand side of the above equation lies in the span of the linear forms $(X_1 + \cdots + X_{k+1})$ and $\ell_1, \ldots, \ell_{k-1}$. Hence its dimension is at most k, which results in a contradiction. This proves the lemma. ∎

Lemma 11 also proves upper bounds on the dimension of a subspace over which $S^2_{2k}(X_1, \ldots, X_{2k})$ vanishes, but the proof does not use partial derivatives.

Lemma 11 *Suppose $k \neq -1$ in the field $\mathbb{F}$ and $\mathbb{F}$ is not of characteristic 2. Then $S^2_{2k}(X_1, \ldots, X_{k+1}, \ell_1, \ldots, \ell_{k-1}) \neq 0$ for any $k-1$ homogeneous linear forms $\ell_1, \ldots, \ell_{k-1}$ in the variables $X_1, \ldots, X_{k+1}$ over $\mathbb{F}$.*

Proof: Using the arguments of Section 4.1 (in particular (18) and (19)), we assume (using the notation of that section) for the sake of contradiction that there exist vectors $y_j \in \mathbb{F}^{k-1}, 1 \leq j \leq k+1$, such that the following equations hold (note that the characteristic of $\mathbb{F}$ is not 2).

$$\left.\begin{array}{rcll} \langle y_j, y_j \rangle + 2\mathbf{1}^T_{k-1} y_j & = & 0 & 1 \leq j \leq k+1 \\ \langle y_j, y_l \rangle + \mathbf{1}^T_{k-1} y_j + \mathbf{1}^T_{k-1} y_l & = & -1 & 1 \leq j < l \leq k+1 \end{array}\right\} \quad (27)$$

where $\langle v, w \rangle \stackrel{\Delta}{=} v^T(\mathbf{J}_{k-1} - \mathbf{I}_{k-1})w$ is a symmetric bilinear form on vectors in $\mathbb{F}^{k-1}$.

From the above equation, we get

$$\langle y_j - y_l, y_j - y_l \rangle = 2 \qquad 1 \leq j < l \leq k+1 \tag{28}$$

We can think of equation (28) as placing $k+1$ points with pairwise "distance" $\sqrt{2}$ in $\mathbb{F}^{k-1}$. We now show that if $k \neq -1$ in $\mathbb{F}$, this is impossible.

We have, for $1 < j < l \leq k+1$

$$\begin{aligned} 2 &= \langle y_j - y_l, y_j - y_l \rangle \qquad \ldots \text{u}sing\ (28) \\ &= \langle (y_j - y_1) - (y_l - y_1), (y_j - y_1) - (y_l - y_1) \rangle \\ &= \langle y_j - y_1, y_j - y_1 \rangle - 2\langle y_j - y_1, y_l - y_1 \rangle + \langle y_l - y_1, y_l - y_1 \rangle \\ &= 2 + 2 - 2\langle y_j - y_1, y_l - y_1 \rangle \qquad \ldots \text{u}sing\ (28) \end{aligned}$$

Hence, since $2 \neq 0$ in $\mathbb{F}$,

$$\langle y_j - y_1, y_l - y_1 \rangle = 1 \qquad 1 < j < l \leq k+1 \tag{29}$$

Now define a $k \times k$ matrix $\mathbf{A}$ where

$$a_{jl} \stackrel{\Delta}{=} \langle y_{j+1} - y_1, y_{l+1} - y_1 \rangle \qquad 1 \leq j, l \leq k$$

Using (28) and (29), we see that the matrix $\mathbf{A}$ has 2's on the main diagonal and 1's in other places. Since $k \neq -1$ in $\mathbb{F}$, $\mathbf{A}$ is of full rank. This implies that the vectors $y_2 - y_1, y_3 - y_1, \ldots, y_{k+1} - y_1$ are linearly independent. In fact we have shown that the vectors $y_1, \ldots, y_{k+1}$ are affinely independent. Since these vectors lie in $\mathbb{F}^{k-1}$, we have arrived at a contradiction. Hence the lemma is proved. ■

We can now prove the following lemma. This lemma allows us to prove lower bounds for computing $S_n^2(X)$ using (not necessarily homogeneous) $\Sigma\Pi\Sigma$ arithmetic circuits over $\mathbb{F}$ when $\mathbb{F}$ is not of characteristic 2 and n is even.

Lemma 12 *$S_{2k}^2(X_1, \ldots, X_{k+1}, \ell_1, \ldots, \ell_{k-1}) \neq 0$ for any $k-1$ homogeneous linear forms $\ell_1, \ldots, \ell_{k-1}$ in the variables $X_1, \ldots, X_{k+1}$ over a field $\mathbb{F}$, if $\mathbb{F}$ is not of characteristic 2.*

Proof: Follows from Lemmas 10 and 11. ■

We also prove the following lemma. This lemma allows us to prove lower bounds for computing $S_n^2(X)$ using (not necessarily homogeneous) $\Sigma\Pi\Sigma$ arithmetic circuits over $\mathbb{F}$ when $\mathbb{F}$ is not of characteristic 2 and n is odd.

Lemma 13 *Suppose $k \neq 0, \pm 1$ in the field $\mathbb{F}$ and $\mathbb{F}$ is not of characteristic 2. Then $S_{2k+1}^2(X_1, \ldots, X_{k+1}, \ell_1, \ldots, \ell_k) \neq 0$ for any k homogeneous linear forms $\ell_1, \ldots, \ell_k$ in the variables $X_1, \ldots, X_{k+1}$ over $\mathbb{F}$.*

Proof: Using the arguments of Section 4.1 (in particular (18) and (19)), we assume (using the notation of that section) for the sake of contradiction that there exist vectors $y_j \in$

$\mathbb{F}^k, 1 \leq j \leq k+1$, such that the following equations hold (note that the characteristic of $\mathbb{F}$ is not 2).

$$\left.\begin{array}{rcll} \langle y_j, y_j \rangle + 2\mathbf{1}_k^T y_j & = & 0 & 1 \leq j \leq k+1 \\ \langle y_j, y_l \rangle + \mathbf{1}_k^T y_j + \mathbf{1}_k^T y_l & = & -1 & 1 \leq j < l \leq k+1 \end{array}\right\} \tag{30}$$

where $\langle v, w \rangle \stackrel{\Delta}{=} v^T(\mathbf{J}_k - \mathbf{I}_k)w$ is a symmetric bilinear form on vectors in $\mathbb{F}^k$.

We can similarly show, as in the proof of Lemma 11, that the vectors $y_2 - y_1, y_3 - y_1, \ldots, y_{k+1} - y_1$ are linearly independent (since $k \neq -1$ and $2 \neq 0$ in $\mathbb{F}$). Also

$$\langle y_j - y_l, y_j - y_l \rangle = 2 \qquad 1 \leq j < l \leq k+1 \tag{31}$$

Since $k \neq 1$ in $\mathbb{F}$, let us define a vector $c \in \mathbb{F}^k$, $c \stackrel{\Delta}{=} \frac{-1}{k-1}\mathbf{1}_k$. Now $(\mathbf{J}_k - \mathbf{I}_k)c = -\mathbf{1}_k$ and $c^T(\mathbf{J}_k - \mathbf{I}_k)c = \frac{k}{k-1}$. Hence we have, for $1 \leq j \leq k+1$

$$\begin{aligned} \langle y_j - c, y_j - c \rangle &= \langle y_j, y_j \rangle - 2\langle y_j, c \rangle + \langle c, c \rangle \\ &= \langle y_j, y_j \rangle + 2\mathbf{1}_k^T y_j + \frac{k}{k-1} \end{aligned}$$

Using the first equation in (30) and above equation, we get the following equation

$$\langle y_j - c, y_j - c \rangle = \frac{k}{k-1} \qquad 1 \leq j \leq k+1 \tag{32}$$

Shifting the origin to the vector c and using (31) and (32) we have (using the same letters $y_j, 1 \leq j \leq k+1$ to denote the new vectors)

$$\left.\begin{array}{rcll} \langle y_j, y_j \rangle & = & \frac{k}{k-1} & 1 \leq j \leq k+1 \\ \langle y_j - y_l, y_j - y_l \rangle & = & 2 & 1 \leq j < l \leq k+1 \end{array}\right\} \tag{33}$$

We can think of equations (33) as placing $k+1$ points of pairwise "distance" $\sqrt{2}$ on the surface of a sphere of "radius" $\sqrt{\frac{k}{k-1}}$ in $\mathbb{F}^k$. We now show that if $k \neq 0, \pm 1$ in $\mathbb{F}$, this is impossible.

Using (33) we get, for $1 \leq j < l \leq k+1$

$$\begin{aligned} 2 &= \langle y_j - y_l, y_j - y_l \rangle \\ &= \langle y_j, y_j \rangle - 2\langle y_j, y_l \rangle + \langle y_l, y_l \rangle \\ &= \frac{2k}{k-1} - 2\langle y_j, y_l \rangle \end{aligned}$$

Since $2 \neq 0$ in $\mathbb{F}$, we get

$$\langle y_j, y_l \rangle = \frac{1}{k-1} \qquad 1 \leq j < l \leq k+1 \tag{34}$$

Using (33) and (34) we have, for $1 < j \leq k+1$

$$\begin{aligned}\langle \sum_{i=1}^{k+1} y_i, y_j - y_1 \rangle &= \langle \sum_{i=1}^{k+1} y_i, y_j \rangle - \langle \sum_{i=1}^{k+1} y_i, y_1 \rangle \\ &= 0\end{aligned}$$

Since $y_2 - y_1, y_3 - y_1, \ldots, y_{k+1} - y_1$ are k linearly independent vectors in $\mathbb{F}^k$, we conclude that

$$\sum_{i=1}^{k+1} y_i = 0 \tag{35}$$

as only the zero vector is orthogonal to all vectors in $\mathbb{F}^k$ under the bilinear map induced by the full rank matrix $\mathbf{J}_k - \mathbf{I}_k$ (since $k \neq 1$ in $\mathbb{F}$, $\mathbf{J}_k - \mathbf{I}_k$ is of full rank). Using (33), (34) and (35) and the fact that $2 \neq 0$ in $\mathbb{F}$, we get

$$\begin{aligned}0 &= \langle \sum_{j=1}^{k+1} y_j, \sum_{j=1}^{k+1} y_j \rangle \\ &= \sum_{j=1}^{k+1} \langle y_j, y_j \rangle + 2 \sum_{1 \leq j < l \leq k+1} \langle y_j, y_l \rangle \\ &= (k+1)\frac{k}{k-1} + 2\frac{(k+1)k}{2}\frac{1}{k-1} \\ &= \frac{2k(k+1)}{k-1}\end{aligned}$$

We have thus come to a contradiction since $k \neq 0, \pm 1$ and $2 \neq 0$ in $\mathbb{F}$. Hence the lemma is proved. ∎

We can now prove our lower bound result for complex numbers. The proofs of our lower bounds for GF(p^r), p an odd prime can be found in the appendix.

Theorem 7 *Any (not necessarily homogeneous) ΣΠΣ circuit computing $S_n^2(X_1, \ldots, X_n)$ over the field of complex numbers requires at least $\lceil \frac{n}{2} \rceil$ multiplication gates.*

Proof: Since $S_3^2(X_1, X_2, X_3)$ is an irreducible polynomial, any ΣΠΣ circuit computing it should have at least 2 multiplication gates. For larger values of n, we invoke Lemmas 8, 12 and 13 to complete the proof. ∎

Finally, we show that the $n-1$ lower bound of Graham and Pollack also extends to inhomogeneous ΣΠΣ circuits over rational and real numbers.

Theorem 8 *Any (not necessarily homogeneous) ΣΠΣ circuit computing $S_n^2(X_1, \ldots, X_n)$ over reals / rationals requires at least $n-1$ multiplication gates.*

Proof: As observed in the introduction of this paper

$$T_n^2(X_1, \ldots, X_n) = (\sum_{j=1}^{n} X_j)^2 - 2S_n^2(X_1, \ldots, X_n)$$

Hence, any $\Sigma\Pi\Sigma$ circuit computing $S_n^2(X_1, \ldots, X_n)$ with less than $n-1$ multiplication gates gives us a $\Sigma\Pi\Sigma$ circuit computing $T_n^2(X_1, \ldots, X_n)$ with less than n multiplication gates. This implies, from the ideas of Section 4.1, that there are $n-1$ homogeneous linear forms $\ell_1, \ldots, \ell_{n-1}$ in the variable X_1 such that $T_n^2(X_1, \ell_1, \ldots, \ell_{n-1}) = 0$. This is clearly impossible over rationals / reals, since the coefficient of X_1^2 will not vanish. ■

5 Conclusion and open problems

In this paper, we have studied the problem of computing the degree two elementary symmetric polynomial in n variables, $S_n^2(X)$, in the $\Sigma\Pi\Sigma$ arithmetic circuit model over various fields. For $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$, we obtain exact bounds for all n, and for GF(2) and GF(p^r), p an odd prime, we obtain exact bounds for infinitely many n. One of the implications of this work is an exact bound of $\lceil \frac{n}{2} \rceil$ for infinitely many n for the 1 mod p cover problem, p prime, generalising a result of Graham and Pollack.

Our work, however, leaves some important questions open. The most immediate one is to resolve the remaining gaps between upper and lower bounds for computing $S_n^2(X)$. This would be especially interesting for the odd cover problem, since we know examples of n where one requires more than $\lceil \frac{n}{2} \rceil$ complete bipartite graphs to odd-cover the edges of K_n. Another open problem is to prove exact bounds for $\Sigma\Pi\Sigma$ arithmetic circuits computing the degree k elementary symmetric polynomial in n variables, $S_n^k(X)$, when $k > 2$. And finally, probably the most important open problem in the field of arithmetic circuits today is to prove super polynomial lower bounds for inhomogeneous $\Sigma\Pi\Sigma$ arithmetic circuits computing an explicit polynomial (e.g. permanent, determinant) over fields of characteristic zero.

Acknowledgements

We thank Amir Shpilka for sending us a preliminary version of [Shp01] and generously sharing his insights with us.

References

[Alo86] N. Alon. Decomposition of the complete r-graph into complete r-partite r-graphs. *Graphs and Combinatorics*, 2:95–100, 1986.

[Art91] M. Artin. *Algebra*. Prentice-Hall India Private Limited, 1991.

[BF92] L. Babai and P. Frankl. *Linear Algebra Methods in Combinatorics (with applications to Geometry and Computer Science)*. Preliminary Version 2, Department of Computer Science, The University of Chicago, September 1992.

[dCH89] D. de Caen and D.G. Hoffman. Impossibility of decomposing the complete graph on n points into $n-1$ isomorphic complete bipartite graphs. *SIAM Journal of Discrete Mathematics*, 2:48–50, 1989.

[GK98] D. Grigoriev and M. Karpinski. An exponential lower bound for depth-3 arithmetic circuits. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 577–582, 1998.

[GP72] R. Graham and H. Pollack. On embedding graphs in squashed cubes. In *Graph Theory and Applications*, Lecture Notes in Mathematics, volume 303, pages 99–110. Springer-Verlag, 1972.

[GR00] D. Grigoriev and A. Razborov. Exponential lower bounds for depth-3 arithmetic circuits in algebras of functions over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 10(6):465–487, 2000.

[Hal86] M. Hall Jr. *Combinatorial Theory*. Wiley Interscience series in Discrete Mathematics, 1986.

[NW96] N. Nisan and A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6:217–234, 1996.

[NZM91] I. Niven, H. Zuckerman, and H. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., 1991. Fifth edition.

[Pec84] G. Peck. A new proof of a theorem of Graham and Pollack. *Discrete Mathematics*, 49:327–328, 1984.

[Shp01] A. Shpilka. Affine projections of symmetric polynomials. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity*, pages 160–171, 2001.

[SW99] A. Shpilka and A. Wigderson. Depth-3 arithmetic formulae over fields of characteristic zero. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pages 87–96, 1999.

[Tve82] H. Tverberg. On the decomposition of K_n into complete bipartite graphs. *Journal of Graph Theory*, 6:493–494, 1982.

Appendix

A Finite fields of odd characteristic

A.1 Bounds

Field		Our Bounds		Previous Bounds	
		Upper Bnds. Hom.	Lower Bnds. Inhom.	Upper Bnds. Hom.	Lower Bnds. Hom.
$\mathrm{GF}(p^r)$ r even $p > 3$	n even	$\frac{n}{2}\forall n$	$\frac{n}{2}\forall n$	$\frac{n}{2}+1\forall n$	$\frac{n}{2}\forall n$
	n odd	$\lceil\frac{n}{2}\rceil\ \forall n$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$ $\lfloor\frac{n}{2}\rfloor\ \forall n$	$\lceil\frac{n}{2}\rceil\ \forall n$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$ $\lfloor\frac{n}{2}\rfloor\ \forall n$
$\mathrm{GF}(3^r)$ r even	n even	$\frac{n}{2}\forall n$	$\frac{n}{2}\forall n$	$\frac{n}{2}+1\forall n$	$\frac{n}{2}\forall n$
	n odd	$\lceil\frac{n}{2}\rceil\ \forall n$	$\lfloor\frac{n}{2}\rfloor\ \forall n$	$\lceil\frac{n}{2}\rceil\ \forall n$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$ $\lfloor\frac{n}{2}\rfloor\ \forall n$
$\mathrm{GF}(p^r)$ r odd $p \equiv 1 \bmod 4$	n even	$\frac{n}{2}\exists^\infty n$	$\frac{n}{2}\forall n$	$\frac{n}{2}+1\forall n$	$\frac{n}{2}\forall n$
	n odd	$\lceil\frac{n}{2}\rceil\ \forall n$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$ $\lfloor\frac{n}{2}\rfloor\ \forall n$	$\lceil\frac{n}{2}\rceil\ \forall n$	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$ $\lfloor\frac{n}{2}\rfloor\ \forall n$
$\mathrm{GF}(p^r)$ r odd $p \equiv 3 \bmod 4$	n even	$\frac{n}{2}\exists^\infty n$	$\frac{n}{2}\forall n$	$n-1\forall n$	$\frac{n}{2}\forall n$
	n odd	$\lceil\frac{n}{2}\rceil\ \exists^\infty n$	$\lfloor\frac{n}{2}\rfloor\ \forall n$	$n-1\forall n$	$\lfloor\frac{n}{2}\rfloor\ \forall n$

A.2 Proofs of the upper bounds

For $\mathrm{GF}(p^r)$, r even and $\mathrm{GF}(p^r), p \equiv 1 \bmod 4$, r odd, the proof of the upper bound is very similar to our upper bound proof for complex numbers. The technical reason behind this is that these fields have square roots of -1. Since the fields $\mathrm{GF}(p^r), p \equiv 3 \bmod 4$, r odd do not have square roots of -1, we cannot mimic the upper bound arguments for complex numbers for these fields. To prove upper bounds for these fields, we use the upper bounds for the 1 mod p cover problem. Because of this, the upper bound of $\lceil\frac{n}{2}\rceil$ for infinitely many odd n actually holds only for infinitely many odd n congruent to 1 mod p. For these fields,

the lower bound of $\lceil \frac{n}{2} \rceil$ for odd n in the homogeneous model only holds if $n \not\equiv 1 \bmod p$. Thus, for these fields, there is a gap of an additive term of 1 between the upper and the lower bounds for infinitely many odd n.

GF(p^r), r even, p odd and GF(p^r), r odd, $p \equiv 1 \bmod 4$

Theorem 9 *Let p be an odd prime. $S_n^2(X)$ can be computed by a homogeneous $\Sigma\Pi\Sigma$ circuit using $\lceil \frac{n}{2} \rceil$ multiplication gates over GF(p^r), r even. Over GF(p^r), r odd, $p \equiv 1 \bmod 4$, $S_n^2(X)$ can be computed using $\lceil \frac{n}{2} \rceil$ multiplication gates if n is odd, $\frac{n}{2}$ multiplication gates for infinitely many even n, and $\frac{n}{2} + 1$ multiplication gates for all even n.*

Proof: If $p \equiv 1 \bmod 4$ then -1 and 2 have square roots in GF(p) (see e.g. [NZM91, Chapter 3]). Hence using Lemmas 6 and 7, over GF(p^r), r odd, $p \equiv 1 \bmod 4$ $S_n^2(X)$ can be computed using $\lceil \frac{n}{2} \rceil$ multiplication gates if n is odd, and using $\frac{n}{2}$ multiplication gates for even n such that $n-1$ has a square root in GF(p^r), which holds for infinitely many even n. For all even n, $S_n^2(X)$ can be computed using $\frac{n}{2} + 1$ multiplication gates by taking a circuit with that many gates for $S_{n+1}^2(X_1, \ldots, X_{n+1})$, and setting X_{n+1} to 0. Over GF(p^r), r even every element of GF(p) has a square root (see e.g. [Art91, Chapter 13]). Hence, using Lemmas 6 and 7 again, $S_n^2(X)$ can be computed using $\lceil \frac{n}{2} \rceil$ multiplication gates for all n. ∎

GF(p^r), r odd, $p \equiv 3 \bmod 4$

Theorem 10 *Let $p \equiv 3 \bmod 4$ be a prime. For infinitely many even and odd n, $S_n^2(X)$ can be computed by a homogeneous $\Sigma\Pi\Sigma$ circuit using $\lceil \frac{n}{2} \rceil$ multiplication gates over GF(p^r), r odd.*

Proof: Such fields do not have a square root of -1. Hence we cannot use either of the Lemmas 6 and 7. To get upper bounds of $\lceil \frac{n}{2} \rceil$ for infinitely many even and odd n, we have to make use of the fact that upper bounds for the 1 mod p cover problem (Theorem 4) give us upper bounds for computing $S_n^2(X)$ in the homogeneous circuit model. ∎

A.3 Proofs of the lower bounds

The proof of the lower bound is similar to the lower bound proof for complex numbers, though, because of technical difficulties, the results are not as tight for some values of n, as they were in the case of complex numbers.

Theorem 11 *Any (not necessarily homogeneous) $\Sigma\Pi\Sigma$ circuit computing $S_n^2(X_1, \ldots, X_n)$ over GF(p^r) where p is an odd prime, requires at least*

1. $\lceil \frac{n}{2} \rceil$ *multiplication gates if n is even*
2. $\lceil \frac{n}{2} \rceil$ *multiplication gates if n is odd and $n \not\equiv \pm 1, 3 \bmod p$*
3. $\lfloor \frac{n}{2} \rfloor$ *multiplication gates if n is odd and $n \equiv \pm 1, 3 \bmod p$*

Thus, as long as p is an odd prime, we have a lower bound of $\lfloor \frac{n}{2} \rfloor$ for all n. If $p > 3$, we have a $\lceil \frac{n}{2} \rceil$ lower bound for all even and infinitely many odd n.

Proof: The lower bounds in parts 1 and 2 follow from Lemmas 8, 12 and 13. Suppose n is odd. Since a $\Sigma\Pi\Sigma$ circuit computing $S_n^2(X_1, \ldots, X_n)$ also gives us a $\Sigma\Pi\Sigma$ circuit computing $S_{n-1}^2(X_1, \ldots, X_{n-1})$ for which we have a lower bound of $\frac{n-1}{2}$, we get the lower bound in part 3. ■