Electronic Colloquium on Computational Complexity, Report No. 107 (2026)

Testing Equivalence to the Hamiltonian Cycle Polynomial

Agrim Dewan
Indian Institute of Science
agrimdewan@iisc.ac.in

Abstract

The Hamiltonian Cycle polynomial, denoted as HC_n, is defined to be the sum of the weighted Hamiltonian Cycles in an n-vertex complete digraph, with vertices labeled 1 to n and edges weighted by formal variables $x_{i,j}$. The Permanent and HC, defined as the family $\{HC_n | \ n \geq 1\}$, were studied by Valiant (STOC 1979), with the former shown to be VNP-complete over all fields of characteristic other than 2, and the latter to be VNP-complete over *every* field. Since its introduction, HC has been studied from the perspective of circuit lower bounds by Jerrum-Snir (JACM 1982), determinantal complexity by Huttenhain-Ikenmeyer (LAA 2016), and its connection with the Permanent and the Determinant polynomials by Goulden-Jackson (EJC 1981) and Grochow (ToC 2017). It has been the most prominent choice for generalising results to all fields, such as in Malod (CCC 2007) and Grochow-Mulmuley-Qiao (ICALP 2016), owing to its VNP-completeness over every field. Hrubes (ToCT, 2016) showed the VNP-completeness of many graph-based polynomial families over every field by using HC.

In Kayal (STOC 2012), a randomised polynomial time algorithm was given for the following problem: Given an n^2-variate degree-n polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ as a black box, decide if there exists $A \in \mathrm{GL}_{n^2}(\mathbb{F})$ such that $f(\mathbf{x}) = Perm_n(A\mathbf{x})$. Here, the Permanent polynomial $Perm_n$ computes the permanent of the $n \times n$ symbolic matrix $(x_{i,j})$. This problem is known as testing equivalence to the Permanent, or alternatively, ET for Permanent.

In this work, we study ET for HC. While both families are VNP-complete, the efficient ET algorithm for Permanent does not imply the same for HC. Besides, there are crucial differences between the two polynomials that make studying the complexity of ET for HC interesting: The underlying decision problem corresponding to the Permanent is in P (detecting perfect matchings in a bipartite graph), but that for HC (detecting Hamiltonian cycles in a digraph) is NP-complete. The Permanent polynomial is known to be characterised by its symmetries as shown by Mulmuley-Sohoni (SIAM J. Computing, 2001). This property yields an *efficient* algorithm for the circuit-testing problem for the Permanent, a special case of ET for the Permanent, in which we check whether a given circuit computes the Permanent. In contrast, we show HC_n is *not* characterised by its symmetries.

In this work, we give a randomised polynomial time ET algorithm for HC with mild constraints on the underlying field. The algorithm is obtained by studying and completely characterising the Lie algebra and the symmetries of HC_n. We show that, like the Permanent polynomial, the symmetries of HC_n are generated by permutation and scaling matrices over large enough fields. However, we also show that, unlike the Permanent polynomial, HC_n is *not* characterised by its symmetries. Nevertheless, like the Permanent polynomial, HC_n is downward self-reducible, as shown in Zhang-Bai (TCS 2011), which implies HC_n is characterised by circuit identities and that we can efficiently test whether a given circuit C computes HC_n. We also get a Flip theorem for HC_n as a result of its circuit identities.

ISSN 1433-8092

Contents

1 Introduction

Two n-variate polynomials $f, g \in \mathbb{F}[\mathbf{y}]$ are *equivalent*, denoted by $f \sim g$, if $f(\mathbf{y}) = g(A\mathbf{y} + \mathbf{b})$ for some invertible $A \in \mathrm{GL}_n(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^n$. Clearly, the relation $f \sim g$ is an equivalence relation. The Polynomial Equivalence problem (PE) involves deciding for two given polynomials f and g, if $f \sim g$ holds or not. Here, the inputs are assumed to be given as lists of coefficients. On one hand, PE is known to be at least as hard as Graph Isomorphism [AS05, Kay11]. On the other hand, the known upper bound on its complexity depends on the underlying field. Over finite fields, PE is in NP $\cap$ co-AM and hence unlikely to be NP-complete, while over $\mathbb{Q}$ we do not even know if it is decidable [Sax06, Thi98]. Even when both inputs are restricted, limited results are known, see Appendix B.1 for a detailed discussion. Thus, understanding the complexity of PE remains a challenge. This has led to a natural variant of PE, called *equivalence testing*, being studied in the literature to make progress towards addressing this challenge.

Equivalence testing. PE asks to check the equivalence of two arbitrary polynomials. In contrast, for Equivalence Testing (ET), we first fix a polynomial family $\mathscr{F}$ or a circuit[1] class $\mathscr{C}$, the goal then is to decide for a given *single* polynomial f, whether $f \sim g$, for some g in $\mathscr{F}$ or in $\mathscr{C}$, respectively. The two versions are called ET for polynomial families and ET for circuit classes, respectively. The study of ET for polynomial families was initiated in [Kay11, Kay12], where efficient ET algorithms were given for the Power Symmetric and Elementary Symmetric polynomials, the Permanent and the Determinant. Since then, efficient ET algorithms have been given for various important polynomial families. The ET algorithms are efficient even if f is given as a black-box[2] or as a circuit. The study of ET for circuit classes is more recent, with the authors of [GST23] showing an efficient ET for read-once formulas (ROFs). The authors of [BDSS24] showed that ET for sparse polynomials (depth-2 circuits) is NP-hard. Later, ET for read-once oblivious algebraic branching programs (ROABPs) was also shown to be NP-hard [RS25, BDGT24]. See Appendix B.2 for more results on ET for polynomial families and circuit classes.

Among all the polynomial families for which ET has been studied so far, the Permanent (see Definition 1.1) is the most prominent VNP-complete family.[3] An efficient ET algorithm for a VNP-complete family does not imply the same for other VNP-complete families. Since ET has been shown to be NP-hard for some natural circuit classes, a natural question arises:

Is ET "hard" for some "natural" VNP-complete polynomial family?

The Hamiltonian Cycle polynomial family, defined below, is another natural VNP-complete family.

Definition 1.1 (Permanent and Hamiltonian Cycle polynomial families)**.** Let $n \geq 1$. The Permanent polynomial $Perm_n(X_n)$ and the Hamiltonian Cycle polynomial $HC_n(X_n)$ are homogeneous degree-n polynomials defined on the $n \times n$ matrix of variables $X_n = (x_{i,j})_{i,j\in[n]}$ as:

$$Perm_n(X_n) := \sum_{\sigma\in S_n} \prod_{i\in[n]} x_{i,\sigma(i)} \quad \text{and} \quad HC_n(X_n) := \sum_{\sigma\in C_n} \prod_{i\in[n]} x_{i,\sigma(i)}, \tag{1}$$

respectively, with HC_1 defined as the zero polynomial. Here, S_n and $C_n \subsetneq S_n$ are the set of all permutations on $\{1, 2 \ldots n\}$, and the set of all *cyclic* permutations on $\{1, 2 \ldots n\}$, respectively. We denote by $Perm$ the family $\{Perm_n | \ n \geq 1\}$ and by HC the family $\{HC_n | \ n \geq 1\}$.

[1] By a circuit we mean an *arithmetic circuit*, unless stated otherwise. An arithmetic circuit is like a Boolean circuit except it uses $+$ or $\times$ gates in place of AND, OR, and NOT gates, and the edges are labeled by $\mathbb{F}$-elements. The circuit computes a polynomial over $\mathbb{F}$.

[2] Black-box access to a polynomial f means we are given oracle access to f. Thus, we can query f at any point $\mathbf{a}$ of our choosing and obtain $f(\mathbf{a})$ in unit time.

[3] The classes VP and VNP are the algebraic analogues of P and NP, respectively, see [Val79, Bür00] for a rigorous definition. The authors of [GS19] studied ET for the Nisan-Wigderson polynomial (NW), which is in VNP but not known to be VNP-complete. The Pascal determinant, see [Gur04] and Chapter 8 in [Lan15], is a generalisation of the Determinant and is VNP-complete. The Pascal Determinant is characterised by its continuous symmetries [Lan15], due to which an ET algorithm for the Pascal Determinant follows almost similarly to that for the Determinant given in Corollary 4.6.4 of [Gro12].

Treating X_n as the adjacency matrix of a complete digraph G with edge weights as formal variables, $HC_n(X_n)$ is the sum of the weights of all the Hamiltonian cycles of G. The Permanent polynomial is the sum of all the weights of perfect matchings in a bipartite graph, whose biadjacency matrix is X_n. Observe that though HC_n is defined on n^2 many variables, it depends only on the off-diagonal $n^2 - n$ entries, which we denote as $\mathbf{x}$. We treat HC_n as an $(n^2 - n)$-variate polynomial in $\mathbf{x}$ variables, and the evaluation of HC_n at an $n \times n$ matrix A is denoted by $HC_n(A)$, where the diagonal entries of A will be ignored.

After the Permanent, HC seems to be the most prominent example of a VNP-complete family. In [Val79], HC was shown to be VNP-complete over *every* field, while the VNP-completeness of Permanent holds only over fields of characteristic other than 2. The proof of VNP-completeness of HC by [Val79] does *not* rely on the VNP-completeness of the Permanent. In fact, HC is VNP-complete even over rings [Mal03]. There have been various works where HC has been studied in multiple contexts, such as lower bounds [JS82, Juk15, AB87, HI16], and its connection to the Permanent and the Determinant [GJ81, Bür00, Gro17]. It has been the main choice as a VNP-complete family over all fields whenever such a family was sought to generalize results to all fields [Mal07, KPTT15, GMQ16, IM18, IS22, DRS24]. The author of [Hru16] used the completeness of HC over every field to show the existence of more VNP-complete families over every field. See Appendix B.3 for a detailed discussion on works involving HC. Thus, HC is a well-studied, natural, and fundamental VNP-complete family.

In this work, we study the Equivalence Testing problem for HC, defined as follows:

Problem 1.1 (ET for HC)**.** Given black box access to an $n^2 - n$-variate degree-n polynomial $f(\mathbf{x})$, decide if there exists $A \in \mathrm{GL}_{n^2-n}(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^{n^2-n}$ such that $f(\mathbf{x}) = HC_n(A\mathbf{x} + \mathbf{b})$ and return A and $\mathbf{b}$ if they exist.

ET for HC_n. While both the Permanent and HC are VNP-complete, the efficient ET algorithm for Permanent does not imply the same for HC.[4] It is a priori unclear why ET for HC could be "easy" because there are crucial differences between the Permanent and HC. First, the complexity of the *zero-testing problem* for the Permanent and HC is vastly different. The zero-testing problem for a polynomial family $\mathscr{F} = \{f_n\}$, where f_n is n-variate and has integer coefficients, is the task of checking for a *given* point $\mathbf{a} \in \{0,1\}^n$, whether $f(\mathbf{a})$ is 0 or not over $\mathbb{Z}$. Note that f is *not* given to us in any form, that is, we don't even have black-box access to f. Zero-testing for the Permanent lies in P because it is the task of detecting a perfect matching in a bipartite graph.[5] Zero-testing for HC is NP-complete because it amounts to detecting a Hamiltonian Cycle in a digraph.[6] In both cases, the graph is given as a 0/1 matrix. Second, the Permanent polynomial is known to be characterised by its symmetries [MS01], see Definition 2.5, and [Gro12] for a proof, but we show HC_n is *not* characterised by its symmetries in Theorem 3. This becomes important in the context of the *circuit testing problem* for a polynomial family $\mathscr{F}$ which asks to check if a given circuit C computes f_n for some n, i.e., is $\mathrm{C}(\mathbf{y}) = f(\mathbf{y})$? The circuit testing problem for a polynomial family $\mathscr{F}$ is a special case of ET for $\mathscr{F}$, with A as the identity matrix and $\mathbf{b} = \mathbf{0}$. Efficient circuit testing algorithms for the Permanent follow by the downward self-reducibility[7] of $Perm_n$ [KI04] and also due to characterisation by symmetries of $Perm_n$ [MS01], see Page 81 in [Gro12] for another proof. Since HC_n is not characterised by its symmetries, one cannot hope to perform circuit testing efficiently for it via symmetries. Given these crucial differences between the two polynomials, it is natural to ask:

Is ET "easy" for the Hamiltonian Cycle polynomial?

[4] The completeness of the Permanent and HC is with respect to p-projections [Val79], which means any polynomial $f(\mathbf{y})$ can be obtained from $Perm_m(X)$ (or HC_n) by replacing each x variable in $Perm_m$ by a $\mathbf{y}$ variable or a field constant. In contrast, $f \sim Perm_m$ happens via *invertible* linear transforms on the variables. Thus, $g \sim HC_n$ does *not* necessarily mean that $g \sim Perm_m$ for some m.

[5] In fact, it is in quasi-NC^2 [FGT21] and very recently it has been shown to be in NC [CGG+26].

[6] Similarly, the Permanent has an FPRAS [JSV04] while no FPRAS exists for HC unless NP=RP. An FPRAS for the Permanent is a randomised algorithm which takes as input a non-negative $n \times n$ matrix A and a parameter $0 < \epsilon < 1$, and with high probability outputs a value in the range $[(1-\epsilon)Perm_n(A), (1+\epsilon)Perm_n(A)]$. The running time is $(n\frac{1}{\epsilon})^{O(1)}$.

[7] For the Permanent, downward self-reducibility means that computing the Permanent of $n \times n$ matrix polytime Turing reduces to computing the Permanent of n many $(n-1) \times (n-1)$ matrices, which follows by the cofactor expansion of the Permanent. In general, a problem is said to be downward self-reducible if solving an instance I of size n Turing reduces to solving instances of smaller size.

In this work, we answer this question positively by showing a randomised polynomial time ET algorithm for HC (see Theorem 1). To our knowledge, an efficient ET for HC was *not* known before this work.

The author of [Kay12] developed the ET algorithm for the Permanent by using the knowledge of the symmetries and the Lie algebra of the Permanent, which have been well studied [MM62, Bot67]. We follow the approach of [Kay12] and study the Lie algebra and symmetries of HC_n to design an ET algorithm for it, though there are challenges to overcome in analysing the Lie algebra and designing the ET algorithm. The Permanent contains some "nice" monomials which are leveraged by [Kay12] in his algorithm, but these monomials are absent in HC_n. Thus, we deviate significantly from the implementation of the scaling matrix recovery step in [Kay12] and instead use ideas from [GS19]. The last step of the ET algorithm for $Perm_n$ uses circuit testing for a soundness check. Since HC_n is not characterised by its symmetries, we cannot hope to perform circuit testing for it via this route. To perform circuit testing for HC, we show it is characterised by circuit identities (Theorems 4 and 5) via its downward self-reducibility (Lemma 4 in [ZB11]). See Section 1.2 for a discussion on the proof ideas and Appendix A for a detailed comparison with [Kay12, GS19]. Table 1 summarises the results and compares the properties of HC_n with the Permanent polynomial.

1.1 Our Results

We first state our assumptions on the computational model. Over $\mathbb{Q}$ and finite fields $\mathbb{F}_q$, we assume the Turing machine model. Over fields like $\mathbb{R}$ and $\mathbb{C}$, we assume a model similar to the BSS model [BSS89], where one can perform an arithmetic operation in unit time. We also assume access to an efficient black-box univariate polynomial factorisation algorithm, an assumption which is justified over fields $\mathbb{F}_q$ [Ber71] and $\mathbb{Q}$ [LLL82]. We consider HC_n for $n \geq 3$. For $n = 2$, HC_n is a monomial, and an efficient ET algorithm follows for it by the factorisation algorithm of [KT90].

Theorem 1 (ET for HC)**.** *Let $\mathbb{F}$ be a field where $|\mathbb{F}| > 3n^5$ and $char(\mathbb{F}) = 0$ or $char(\mathbb{F}) > n$. There is a randomised $(n\beta)^{O(1)}$ time algorithm which, when given black-box access to an (n^2-n)-variate, homogeneous degree-n polynomial $f(\mathbf{x})$ with β as the bit complexity of the coefficients, decides correctly, with high probability, if there exists $A \in \mathrm{GL}_{n^2-n}(\mathbb{F})$ such that $f(\mathbf{x}) = HC_n(A\mathbf{x})$ and outputs A if it exists. Over finite fields, the running time is randomised $(n \log(|\mathbb{F}|))^{O(1)}$.*

Remarks.
1. The algorithm also works for the more general case where $f = HC_n(A\mathbf{y} + \mathbf{b})$, $A \in \mathbb{F}^{(n^2-n)\times m}$ is a full row rank matrix (hence $n^2 - n \leq m$) and $\mathbf{b} \in \mathbb{F}^{n^2-n}$ is a translation vector. See Theorem 28 in [Kay12] and Appendix B in [KNST19], which show how to appropriately modify the ET algorithm to handle the general case.
2. The constraint on the characteristic arises from computing derivatives of f and is imposed to ensure that these derivatives don't vanish. The constraint on the field size is due to the use of the Polynomial Identity Lemma [DL78, Lip89, Sch80, Zip79].

The ET algorithm uses the knowledge of the group of symmetries $\mathscr{G}_{HC_n}$ and the Lie Algebra $\mathfrak{g}_{HC_n}$ of HC_n, see Definitions 2.1 and 2.2. In Propositions 3.1 and 3.2, we completely characterise and give a basis for $\mathfrak{g}_{HC_n}$, while Theorem 2 gives the general structure of $\mathscr{G}_{HC_n}$.

Theorem 2 (Structure of $\mathscr{G}_{HC_n}$)**.** *Let $|\mathbb{F}| > \binom{n^2-n}{2}$. If A is a symmetry of HC_n, then $A = PS$ for some permutation matrix P and scaling matrix S.*

Remarks.
1. Propositions 3.4 and 3.6 describe the permutation and scaling symmetries of HC_n respectively. If we treat HC_n as a polynomial in all the variables of X_n, then any $A \in \mathscr{G}_{HC_n}$ acts on X_n as $A(X_n) = PLX_nRP^T$ or $A(X_n) = PLX_n^TRP^T$, where P is a permutation matrix, and L and R are diagonal matrices such that $Perm_n(RL) = 1$. In contrast, any $A \in \mathscr{G}_{Perm_n}$ acts as $A(X_n) = PLX_nRQ$ or $A(X_n) = PLX_n^TRQ$, where P and Q are permutation matrices and L, R are as before.

Unlike $Perm_n$, HC_n is *not* characterised by its symmetries, see Definition 2.5.

Property	HC_n ***(This work)***	***Permanent***
Efficient ET algorithm?	Yes	Yes
Explicit basis of Lie algebra known?	Yes	Yes
Characterisation by symmetries?	**No**, for $n \geq 5$	**Almost all fields**
Symmetries generated by PS matrices?	Yes	Yes
Characterisation by circuit identities?	Yes	Yes
Scaling symmetries continuous?	Almost all fields, except for $n = 4$ over $\mathbb{Q}, \mathbb{R}, \mathbb{C}$	Almost all fields
Flip Theorem known?	Yes	Yes
Complexity of Zero testing?	**NP-complete**	**P**

Table 1: A comparison between Permanent and HC_n

Theorem 3 (Non-characterisation by symmetries)**.** *Let $n \geq 5$ and $\mathbb{F}$ be such that $|\mathbb{F}| > \binom{n^2-n}{2}$. Then, HC_n is* not *characterised by its symmetries over $\mathbb{F}$.*

Remarks. 1. In Appendix C.17.3, we show that HC_n, for $n = 3$ and 4, is characterised by its symmetries over appropriate fields $\mathbb{F}$.

However, it turns out that HC_n is characterised by circuit identities (see Definition 2.4) over *any* field $\mathbb{F}$. This follows from the downward self-reducibility of HC_n as shown in Lemma 3.2, and Lemma 4 of [ZB11].

Theorem 4 (Circuit Identities)**.** *Over any field $\mathbb{F}$, HC_n is characterised by circuit identities.*

As a consequence of Theorem 4, we get Theorems 5 and 6. We use Theorem 5 to prove the soundness of the ET algorithm given by Theorem 1.

Theorem 5 (Circuit Testability)**.** *Let C be a circuit in $n^2 - n$ variables, of size s, and degree of output polynomial $d = s^{O(1)}$ over a field $\mathbb{F}$, where $|\mathbb{F}| > 2d$. There is a randomised $(ns)^{O(1)}$ time algorithm over $\mathbb{F}$ which, when given black box access to C, decides correctly with high probability whether $\mathsf{C}(\mathbf{x}) = HC_n(\mathbf{x})$ or not.*

A flip theorem essentially states that if some function is not computable by small-size circuits, then we can efficiently construct a short list of counterexamples such that any small-size circuit fails on some counterexample in the list. Flip theorem is known for the Permanent polynomial [Mul10, Mul11] and the Nisan-Wigderson polynomial [GS19].

Theorem 6 (Flip Theorem for HC)**.** *Let $|\mathbb{F}| > n^{O(1)}$. Suppose HC_n is not computable by $n^{O(1)}$ size circuits over $\mathbb{F}$. There is a randomised $n^{O(1)}$ time algorithm which on input 1^{n^2-n} outputs $n-1$ matrices $A_1, \ldots A_{n-1}$, where $A_i \in \mathbb{F}^{n \times n}$, such that, with high probability, for any polynomial size circuit C there is an $i \in [n-1]$, $\mathsf{C}(A_i) \neq HC_n(A_i)$. Further, derandomisation of black-box polynomial identity testing implies that the A_i's can be computed in deterministic $n^{O(1)}$ time.*

Remarks. 1. Note that Theorem 5 is *not* implied by Theorem 6 because HC_n is not known to be computable by $n^{O(1)}$ size circuit. Verifying $\mathsf{C}(A_i) \neq HC_n(A_i)$ for some i needs the evaluations $HC_n(A_i)$, which can not be done efficiently.

1.2 Proof Techniques

We follow the Lie algebraic approach of [Kay12], which was used to obtain an ET algorithm for the Permanent. We describe the ET algorithm for the HC at a high level. Suppose we are given black-box access to an $n^2 - n$-variate degree-n polynomial $f(\mathbf{x})$. The algorithm has four steps:

1. *Reduction to PS-equivalence testing.* Using the structure of the Lie algebra of HC_n, compute an invertible D such that $f(D\mathbf{x}) = HC_n(PS\mathbf{x})$ for some permutation P and scaling S, assuming $f \sim HC_n$. See Algorithm 2.

2. *Reduction to S-equivalence testing.* Let $f_1(\mathbf{x}) = f(D\mathbf{x})$. Using the knowledge of the permutation symmetries of HC_n, and the set of vanishing second-order partial derivatives of HC_n, recover P so that $f_1(P\mathbf{x}) = HC_n(S\mathbf{x})$, assuming $f \sim HC_n$. Thus, $f_1(P\mathbf{x})$ is S-equivalent to HC_n. See Algorithm 3.

3. *Recovering S.* Let $f_2(\mathbf{x}) = f_1(P\mathbf{x})$, assuming $f \sim HC_n$. Query f_2 at $k = O(n^2)$ many points to get constants $c_1, c_2, \ldots, c_k$, and solve a system of linear equations where the variables are the entries of S which we wish to recover. See Algorithm 4.

4. *Verification \ Soundness Test.* Let $B = DPS$. Use the downward self-reducibility, Lemma 3.2 or Lemma 4 of [ZB11], of HC_n to verify if $f(B\mathbf{x}) = HC_n(\mathbf{x})$. If so, output B^{-1}. See Algorithm 1.

Though the ET algorithm for HC is obtained via the Lie algebraic approach, like it was done for the Permanent in [Kay12], there are two major differences between the algorithms. First, the Lie algebra and the symmetries of the Permanent have been well-studied [Bot67, MM62], and are leveraged by [Kay12]. To our knowledge, the Lie algebra and symmetries of HC_n have not been studied before. Therefore, we first study and give a complete characterisation of the Lie algebra $\mathfrak{g}_{HC_n}$ of HC_n over all fields (see Propositions 3.1 and 3.2) by using ideas from [GS19] to construct a basis for $\mathfrak{g}_{HC_n}$; we also characterise the group of symmetries $\mathcal{G}_{HC_n}$ over large enough fields (Proposition 3.3). Second, we deviate from [Kay12] in the execution of Step 3. The deviation occurs because of an important difference in the monomials of HC_n and those of $Perm_n$. In $Perm_n$, there are enough pairs of monomials which differ in exactly 2 variables and are leveraged by [Kay12] to recover S by querying the scaled Permanent polynomial at these monomials. In contrast, *any* two monomials of HC_n differ in at least 3 variables (see Claim 3.1), which makes it unclear if they can be leveraged in the same way as for $Perm_n$ to recover S. Instead, we follow the approach in [GS19] to recover S. There are other key technical differences between our analysis and that in [Kay12, GS19], see Appendix A for a detailed comparison. Refer to Table 1 for a comparison of results between HC_n and the Permanent.

To prove Theorem 2, we leverage the structure of $\mathfrak{g}_{HC_n}$ and conjugacy of Lie algebras of equivalent polynomials (Lemma 2.2). We prove Theorem 3 by using the knowledge of the permutation (Proposition 3.6) and scaling symmetries (Proposition 3.4) of HC_n. Theorem 4 is proved by using the downward self-reducibility of HC_n and an adaptation of Lemma 7.13 from [Bür00]. Theorems 5 and 6 then follow by using the identities established in Theorem 4.

2 Preliminaries

2.1 Notations and Definitions

The set of natural numbers is $\mathbb{N} = \{1, 2 \ldots\}$, while $\mathbb{Z}$ denotes the integers. For $n \in \mathbb{N}$, We use $[n]$ to denote the set $\{1, \ldots, n\}$ and $[a, b]$ to denote $\{a, \ldots, b\}$. The set of $n \times n$ invertible matrices over $\mathbb{F}$ is denoted by $GL_n(\mathbb{F})$. The set of permutations on $[n]$ is denoted by S_n and the set of cyclic permutations on $[n]$ by C_n. A field is denoted by $\mathbb{F}$, while $\mathbb{F}^\times$ denotes $\mathbb{F}\backslash\{0\}$. We denote the integers mod m by $\mathbb{Z}_m$. The dimension of a vector space V over a field $\mathbb{F}$ is denoted by $\dim_{\mathbb{F}}(V)$. By $\in_r$ we denote uniform random selection from a set, and by "b.b.a to f" we mean black-box access to f.

We denote the set of variables on which HC_n depends as $\mathbf{x} := \{x_{i,j} |\ i, j \in [n], i \neq j\}$, with $|\mathbf{x}| = n^2 - n$ and $X_n = \{x_{i,j} |\ i, j \in [n]\}$ to denote the entire set of n^2 variables on which HC_n is defined. By scaling matrices, we mean diagonal matrices. We treat a scaling matrix $S \in \mathbb{F}^{m \times m}$ as a vector in $\mathbb{F}^m$ by identifying the diagonal as a vector in $\mathbb{F}^m$. Thus, the entries of $S \in \mathbb{F}^{n^2 \times n^2}$, will be referred to as $S_{i,j}$, where $i, j \in [n]$. For a matrix $M \in \mathbb{F}^{m \times m}$ and $S, T \subseteq [m]$, we denote by $M_{\bullet \times T}$ the matrix M restricted to columns in T, by $M_{S \times \bullet}$ the matrix M restricted to rows in S, and by $M_{S \times T}$ the matrix M restricted to the rows and columns in S and T respectively. By $n^{O(1)}$, we denote a polynomially bounded function of n.

2.2 Algebraic and algorithmic preliminaries

Lemma 2.1 (Computing Derivatives [KNST19]). Let $f \in \mathbb{F}[\mathbf{y}]$ be an n-variate degree-d polynomial with bit complexity β. Given black-box access to f, we can obtain in $(nd\beta)^{O(1)}$ time black-box access to a derivative $\frac{\partial f}{\partial y}$ for any $y \in \mathbf{y}$.

Definition 2.1 (Group of Symmetries [GS19]). Let $f \in \mathbb{F}[\mathbf{y}]$ be an n-variate polynomial. The group of symmetries of f over $\mathbb{F}$, denoted by $\mathscr{G}_f$, is the set of matrices $\{A \in \mathrm{GL}_n(\mathbb{F}) : f(A\mathbf{y}) = f(\mathbf{y})\}$ which also form a group under matrix multiplication.

Definition 2.2 (Lie Algebra of a polynomial). Let $f \in \mathbb{F}[\mathbf{y}]$, where $\mathbf{y} := \{y_1, y_2, \ldots, y_n\}$. The Lie Algebra associated with f, denoted by $\mathfrak{g}_f$, is the set $\{A \in \mathbb{F}^{n\times n} \mid \sum_{i,j\in[n]} A_{i,j} y_j \frac{\partial f}{\partial y_i} = 0\}$, which also forms a vector space over $\mathbb{F}$.

Lemma 2.2 (Conjugacy of Lie Algebras [Kay12]). Let $f \in \mathbb{F}[\mathbf{y}]$ be an n-variate polynomial. If $g(\mathbf{y}) = f(A\mathbf{y})$, where $A \in \mathrm{GL}_n(\mathbb{F})$, then $\mathfrak{g}_g = A^{-1} \cdot \mathfrak{g}_f \cdot A$.

Lemma 2.3 (Computing basis of Lie Algebra [Kay12]). Given black-box access to an n-variate degree d polynomial $f \in \mathbb{F}[\mathbf{y}]$, a basis of $\mathfrak{g}_f$ can be computed in randomised $(nd\beta)^{O(1)}$ time, where β is the bit complexity of the coefficients.

For $A \in \mathbb{C}^{n\times n}$, define $e^A := \sum_{i\in\mathbb{N}} \frac{A^i}{i!}$, the sum always converges. Over $\mathbb{C}$, $\mathfrak{g}_f$ is related to $\mathscr{G}_f$ as in Definition 2.3.

Definition 2.3 (Continuous and Discrete Symmetries). Let $f \in \mathbb{C}[\mathbf{y}]$. If $A \in \mathfrak{g}_f$, then $e^{tA} \in \mathscr{G}_f$ for all $t \in \mathbb{R}$; see [Hal15] for a proof. The continuous symmetries of f are the elements of the set $\{e^{tA} : A \in \mathscr{G}_f \text{ and } t \in \mathbb{R}\}$. All other symmetries in $\mathscr{G}_f$ are the discrete symmetries of f.

Definition 2.4 (Characterisation by circuit identities [Gro12]). An n-variate polynomial $f(\mathbf{y})$ is said to be characterised by circuit identities if there exist $m = n^{O(1)}$ many polynomials $g_1(\mathbf{z}), \ldots, g_m(\mathbf{z})$, with each g_i computable by a $n^{O(1)}$ size circuit over $\mathbb{Z}$ and $|\mathbf{z}| \leq k$, f is the only non-zero polynomial upto scaling that satisfies $g_i(f(\mathbf{y}_1), f(\mathbf{y}_2) \ldots f(\mathbf{y}_k)) = 0$, where $\mathbf{y}_i$ can be computed from $\mathbf{y}$ by a $n^{O(1)}$ size circuit.

Definition 2.5 (Characterisation by symmetries). A homogeneous degree-d polynomial $f \in \mathbb{F}[\mathbf{y}]$ is characterised by its symmetries if for every homogeneous degree-d polynomial $g \in \mathbb{F}[\mathbf{y}]$, $\mathscr{G}_f \subseteq \mathscr{G}_g$ implies $g = c \cdot f$, for somes $c \in \mathbb{F}^\times$.

3 Lie Algebra and the Symmetries of HC_n

In Section 3.1, we analyse $\mathfrak{g}_{HC_n}$, the Lie Algebra of HC_n, and show that it comprises diagonal matrices and that it is a $2n-2$ dimensional vector space over any field $\mathbb{F}$, for $n = 3$ and $n \geq 5$. We analyse $\mathfrak{g}_{HC_4}$ and the symmetries of HC_4 in Appendix C.17. In Section 3.2, we use $\mathfrak{g}_{HC_n}$ to show that over large enough fields the symmetries of HC_n are generated by permutation and scaling matrices (which proves Theorem 2) and analyse the permutation and scaling symmetries of HC_n. In Section 3.3, we show that HC_n is *not* characterised by its symmetries, proving Theorem 3. In Section 3.4, we show that HC_n is characterised by circuit identities over any field by using the downward self-reducibility of HC_n and prove Theorems 4, 5 and 6. All missing proofs can be found in Appendix C.

3.1 Lie Algebra

Proposition 3.1, proved in Appendix C.1, shows that $\mathfrak{g}_{HC_n}$ comprises diagonal matrices $A \in \mathbb{F}^{(n^2-n)\times(n^2-n)}$, where for all $\sigma \in C_n$ the sum of the diagonal entries in A corresponding to σ is 0. To prove Proposition 3.1, we use Observation 3.1, which follows from Claim 3.1. Claim 3.1 states that any two cyclic permutations, when interpreted as Hamiltonian cycles on the complete digraph, must have at least 3 different edges.

Proposition 3.1. Let $n \geq 3$. Then for $A \in \mathbb{F}^{(n^2-n)\times(n^2-n)}$,

$$A \in \mathfrak{g}_{HC_n} \iff A \text{ is diagonal and } \sum_{i=1}^{n} A_{(i,\sigma(i)),(i,\sigma(i))} = 0 \text{ for all } \sigma \in C_n.$$

Observation 3.1. Let $\sigma_1, \sigma_2 \in C_n$ with $\sigma_1 \neq \sigma_2$ and m_σ denote $\prod_{i\in[n]} x_{i,\sigma(i)}$ for $\sigma \in C_n$. Then,

$$x_{i_1,j_1}\frac{\partial m_{\sigma_1}}{\partial x_{i_2,j_2}} \neq x_{i_3,j_3}\frac{\partial m_{\sigma_2}}{\partial x_{i_4,j_4}},$$

where i_k's, j_k's $\in [n]$, $j_2 = \sigma_1(i_2)$, and $j_4 = \sigma_2(i_4)$ (to ensure non-zero derivatives).

Claim 3.1. Let $\sigma_1, \sigma_2 \in C_n$ with $\sigma_1 \neq \sigma_2$. There exists $S \subseteq [n]$, such that $|S| = 3$ and $\sigma_1(i) \neq \sigma_2(i)$ for all $i \in S$.

By Proposition 3.1, any $A \in \mathfrak{g}_{HC_n}$ can be identified with a vector in $\mathbb{F}^{n^2-n}$. Proposition 3.2 shows that for $n \neq 4$, $\mathfrak{g}_{HC_n}$ is a $(2n-2)$-dimensional over any $\mathbb{F}$. In Appendix C.17.1, we analyse $\mathfrak{g}_{HC_4}$ over all fields.

Proposition 3.2. Let $\mathbb{F}$ be any field and $n = 3$ or $n \geq 5$. Consider $A^{(k)}$, $B^{(\ell)}$ and $C \in \mathbb{F}^{n^2-n}$, where $k \in [2,n], \ell \in [2,n-1]$, defined as:

$$A^{(k)}_{(i,j)} = \begin{cases} 1 & i = 1, \\ -1 & i = k, \\ 0 & \text{otherwise} \end{cases}, \quad B^{(\ell)}_{(i,j)} = \begin{cases} 1 & j = 1, \\ -1 & j = l, \\ 0 & \text{otherwise} \end{cases}, \quad C_{(i,j)} = \begin{cases} -1 & i = 2, \\ 1 & j = 2, \\ 0 & \text{otherwise} \end{cases}$$

Then, $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_n}) = 2n-2$ with $\mathscr{B}_n = \{A^{(2)}, \ldots, A^{(n)}, B^{(2)}, \ldots, B^{(n-1)}, C\}$ as a basis.

Proposition 3.2 is proved in Appendix C.4. In the proof, we define a matrix $M^{HC_n} \in \mathbb{F}^{(n-1)!\times(n^2-n)}$ to represent the linear equations given by Proposition 3.1. Therefore, the nullspace of M^{HC_n} is $\mathfrak{g}_{HC_n}$. The rows of M^{HC_n} are indexed by $\sigma \in C_n$ and columns by variables $x_{i,j}$ in lex order. We then show that the set $\mathscr{B}_n$ in the proposition is linearly independent over *any* $\mathbb{F}$ and that $\mathscr{B}_n \subset \mathfrak{g}_{HC_n}$. Lastly, we construct in $n^{O(1)}$ time a $(n-1)(n-2) \times (n^2-n)$ submatrix $M^{(n)}$ of M^{HC_n} such that $M^{(n)}$ has full row rank over *any* $\mathbb{F}$ (see Proposition C.1). Thus, M^{HC_n} has rank at least $(n-1)(n-2)$, which along with the fact that $\mathscr{B}_n \subset \mathfrak{g}_{HC_n}$ proves Proposition 3.2.

Corollary 3.1 describes the structure of any $\mathbf{z} \in \mathfrak{g}_{HC_n}$ and follows by considering the matrix formed by the equations in (2), noting that the matrix is full row rank, and that the entries of the elements of $\mathscr{B}_n$ in Proposition 3.2 satisfy (2). Corollary 3.2 describes the entries of any continuous symmetry of HC_n, and follows from Corollary 3.1 and Definition 2.3. In Appendix C.6, we further analyse $M^{(n)}$, which proves useful in analysing the scaling symmetries of HC_n over all fields and to prove the correctness of Algorithm 4.

Corollary 3.1. Let $n = 3$ or $n \geq 5$ and $\mathbf{z} \in \mathbb{F}^{n^2-n}$. Then, $\mathbf{z} \in \mathfrak{g}_{HC_n}$ if and only if the entries $z_{i,j}$ satisfy (2).

$$\begin{aligned} z_{i,j} &= z_{i,1} + z_{1,j} + z_{2,3} - z_{1,3} - z_{2,1} \quad i \in [2,n-1],\ j \in [2,n]\ , i \neq j, (i,j) \neq (2,3), \\ z_{n,1} &= (n-2)(z_{1,3} + z_{2,1} - z_{2,3}) - \sum_{\ell=2}^{n} z_{1,\ell} - \sum_{\ell=2}^{n-1} z_{\ell,1}, \\ z_{n,j} &= z_{1,j} + (n-3)(z_{1,3} + z_{2,1} - z_{2,3}) - \sum_{\ell=2}^{n} z_{1,\ell} - \sum_{\ell=2}^{n-1} z_{\ell,1} \\ &= z_{n,1} + z_{1,j} + z_{2,3} - z_{1,3} - z_{2,1}, \quad j \in [2,n-1]. \end{aligned} \tag{2}$$

Corollary 3.2. Over $\mathbb{C}$, any continuous symmetry $S \in \mathscr{G}_{HC_n}$ is a diagonal matrix, with $S_{i,j}$'s satisfying (3).

$$\begin{aligned} S_{i,j} &= S_{i,1}S_{1,j}\frac{S_{2,3}}{S_{1,3}S_{2,1}} \quad i \in [2,n-1],\ j \in [2,n]\ , i \neq j, (i,j) \neq (2,3), \\ S_{n,1} &= \left(\frac{S_{1,3}S_{2,1}}{S_{2,3}}\right)^{n-2}\left(\prod_{\ell=2}^{n} S_{1,\ell}\prod_{\ell=2}^{n-1} S_{\ell,1}\right)^{-1}, \\ S_{n,j} &= S_{n,1}S_{1,j}\frac{S_{2,3}}{S_{1,3}S_{2,1}} \quad j \in [2,n-1]. \end{aligned} \tag{3}$$

3.2 The Symmetries of HC_n

Lemma 3.1 shows that over large enough fields, $\mathfrak{g}_{HC_n}$ contains an element with distinct eigenvalues. Proposition 3.3 then shows that over such fields, every symmetry of HC_n is generated by permutation and scaling symmetries, proving Theorem 2. The proof of Proposition 3.3 follows from Lemmas 2.2 and 3.1 (see Appendix C.8). We then analyse and characterise the permutation and scaling symmetries of HC_n.

Lemma 3.1. Suppose $|\mathbb{F}| > \binom{n^2-n}{2}$. There exists $A \in \mathfrak{g}_{HC_n}$ such that A has distinct eigenvalues.

Proposition 3.3 (Theorem 2 restated)**.** Suppose $|\mathbb{F}| > \binom{n^2-n}{2}$. If $A \in \mathscr{G}_{HC_n}$, then $A = PS$, where P is a permutation matrix and S is a scaling matrix.

Scaling symmetries. Proposition 3.4, proved in Appendix C.9, shows that any scaling symmetry S of HC_n satisfies (3) for $n \neq 4$ and follows from Lemma C.2. In Appendix C.17.2, we show that HC_4 has discrete scaling symmetries over $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and certain finite fields.

Proposition 3.4 (Scaling symmetries are continuous)**.** Let $\mathbb{F}$ be any field and $n = 3$ or $n \geq 5$. If $S \in \mathscr{G}_{HC_n}$ is a scaling symmetry, then the entries $S_{i,j}$ satisfy (3).

Permutation Symmetries. Proposition 3.5 shows that HC_n has non-trivial permutation symmetries. In terms of the matrix X_n, $P^{(\sigma)}$ acts as $X_n \mapsto QX_nQ^T$, where Q is the $n \times n$ matrix corresponding to $\sigma \in S_n$, and $P^{(T)}$ acts as $X_n \mapsto X_n^T$. Proposition 3.6, proved in Appendix C.11, shows that the permutation symmetries are generated by those described in Proposition 3.5. To prove Proposition 3.6, we use Observation 3.2, which tells us when the second-order derivatives of HC_n vanish.

Proposition 3.5. Let $\sigma \in S_n$. The matrices $P^{(\sigma)}$ and $P^{(T)}$, as below, are permutation symmetries of HC_n.

$$P^{(\sigma)}_{(i,j),(k,\ell)} := \begin{cases} 1 & k = \sigma(i), \ell = \sigma(j), \\ 0 & \text{otherwise} \end{cases}, \quad P^{(T)}_{(i,j),(k,\ell)} := \begin{cases} 1 & k = j, \ell = i, \\ 0 & \text{otherwise} \end{cases}.$$

Here $i, j, k, \ell \in [n]$, $i \neq j$ and $k \neq \ell$. Also, $P^{(\sigma)}$ and $P^{(T)}$ commute with one another.

Proposition 3.6. If $P \in \mathscr{G}_{HC_n}$ is a permutation symmetry, then $P = P^{(\sigma)}$ or $P = P^{(\sigma)}P^{(T)}$ for some $\sigma \in S_n$.

Observation 3.2. Let $i, j \in [n]$, $i \neq j$ and $R_{i,j}$ be the set of variables $x_{k,\ell}$, other than $x_{i,j}$, such that $\frac{\partial^2 HC_n}{\partial x_{i,j}\partial x_{k,\ell}} = 0$. Then,

$$x_{k,\ell} \in R_{i,j} \iff i = k, \text{ or } j = \ell, \text{ or } i = \ell \text{ and } j = k.$$

Further, we can partition $R_{i,j}$ as

$$R_{i,j} := Q_{i,j} \sqcup T_{i,j} \sqcup \{x_{j,i}\},\ Q_{i,j} := \{x_{k,j} \mid k \in [n]\backslash\{i,j\}\} \text{ and } T_{i,j} := \{x_{i,k} \mid k \in [n]\backslash\{i,j\}\}.$$

The partitions also satisfy:

1. $\frac{\partial^2 HC_n}{\partial x_{i_1,j_1}\partial x_{i_2,j_2}} \neq 0$ if $x_{i_1,j_1} = x_{j,i}$ and $x_{i_2,j_2} \in Q_{i,j} \sqcup T_{i,j}$, or $x_{i_1,j_1} \in T_{i,j}, x_{i_2,j_2} \in Q_{i,j}$.

2. $\frac{\partial^2 HC_n}{\partial x_{i_1,j_1}\partial x_{i_2,j_2}} = 0$ if $x_{i_1,j_1}, x_{i_2,j_2} \in Q_{i,j}$ or $x_{i_1,j_1}, x_{i_2,j_2} \in T_{i,j}$.

If $f = HC_n(P\mathbf{x})$, where P is a permutation matrix, then $\frac{\partial^2 f}{\partial x_{i,j}\partial x_{k,\ell}} = 0$ if and only if $P^{-1}(x_{i,j})$ and $P^{-1}(x_{k,\ell})$ are as specified in Observation 3.2. Thus, P creates a bijection on $R_{i,j}$ which also maps the partitions of $R_{i,j}$ in Observation 3.2 appropriately. If $P \in \mathcal{G}_{HC_n}$ is a permutation symmetry, then it creates, for each variable $x_{i,j}$, a bijection between the set $R_{i,j}$ and $R_{k,\ell}$, where $x_{k,\ell} = P(x_{i,j})$, such that the bijection also maps the partitions of $R_{i,j}$ as described in Observation 3.2 accordingly to those of $R_{k,\ell}$. analysing these bijections for variables $x_{1,j}$ and $x_{i,1}$, and noting that the image of $R_{1,j} \cap R_{i,1}$ is a singleton shows how P is generated by the permutation symmetries described in Proposition 3.5.

3.3 HC_n is not characterised by its symmetries

Proposition 3.7, proved in Appendix C.13, shows that for $n \geq 5$, HC_n is *not* characterised by its symmetries, unlike the Permanent polynomial, proving Theorem 3. The proof involves defining a polynomial $g(\mathbf{x})$ as the sum over the image of a monomial, m_σ, under all the permutation symmetries (Proposition 3.6) of HC_n. Here, $\sigma \in S_n \backslash C_n$ such that $\sigma(i) \neq i$ for all $i \in [n]$. It is easy to see that such a σ exists for $n \geq 5$, for example $\sigma = (1\,2)(3\,4\,\ldots\,n)$. Then, it is not hard to observe that every scaling symmetry of HC_n (Proposition 3.4) is also a scaling symmetry of g, but $g \neq c \cdot HC_n$ for any $c \in \mathbb{F}^\times$.

Proposition 3.7 (Non-characterisation by symmetries)**.** Let $n \geq 5$ and $\mathbb{F}$ be any field such that $|\mathbb{F}| > \binom{n^2-n}{2}$. There exists a non-zero polynomial f such that $\mathcal{G}_{HC_n} \subseteq \mathcal{G}_f$ but $f \neq c \cdot HC_n$ for any $c \in \mathbb{F}^\times$.

More generally, in Appendix C.14 we show how to obtain a scaling symmetry of the Permanent polynomial from that of HC_n. In contrast, for $n = 3$ and $n = 4$, we show HC_n is characterised by its symmetries over appropriate fields in Appendix C.17.3.

3.4 Circuit Identities, Circuit Testing and Flip Theorem

Though HC_n is not characterised by its symmetries, it is characterised by circuit identities (see Definition 2.4), which follows from HC_n being downward self-reducible, as shown in Lemma 4 of [ZB11]. We give a proof of downward self-reducibility in the proof of Lemma 3.3 for completeness (see Appendix C.16). The proof given here was discovered by the author independently before coming across [ZB11]. To prove the circuit identities, we use Lemma 3.2, an adaptation of Lemma 7.13 in [Bür00], which shows that HC_n can be expressed as HC_m for all $m > n \geq 2$. Lemma 3.3 then shows that HC_n is downward self-reducible over any field, and can be proved using induction on n. Note that we use the matrix X_n with $x_{i,i}$ replaced by 0's in the statement and proof of Lemmas 3.2 and 3.3 for ease of exposition.

Lemma 3.2. Let $n, m \in \mathbb{N}$ with $m > n \geq 2$. In $O(m^2)$ time, we can construct a $m \times m$ matrix $Y^{(m,n)}$ from X_n such that $HC_m(Y^{(m,n)}) = HC_n(\mathbf{x})$.

Lemma 3.3. Let $f \in \mathbb{F}[\mathbf{x}]$. Then, $f = HC_n$ if and only if f satisfies the identities

$$f(Y^{(n,k)}) = \sum_{i=2}^{k} x_{1,i} f(Y_i^{(n,k-1)}) \quad k \in [3,n], \text{ and } f(Y^{(n,2)}) = x_{1,2}x_{2,1},$$

where $Y^{(n,k)}$ is constructed from X_k as described in the proof of Lemma 3.2. The matrix $Y_i^{(n,k-1)}$ is obtained from X_k by first swapping row i with row 2 and column i with column 2 in X_k, removing the 1st row and 2nd column to obtain the $(k-1) \times (k-1)$ matrix $X_k^{(i)}$, and constructing $Y^{(n,k-1)}$ using $X_k^{(i)}$ by Lemma 3.2.

Proof of Theorem 4. Represent the $n-1$ identities in Lemma 3.3 as polynomials $g_1(\mathbf{x},\mathbf{z}),\ldots,g_{n-1}(\mathbf{x},\mathbf{z})$, where $|\mathbf{z}| = n-1$, g_i's are degree 2 polynomials over $\mathbb{Z}$ and have $n^{O(1)}$ size circuit over $\mathbb{Z}$. This establishes circuit identities for HC_n and proves Theorem 4.

Proof of Theorems 5 and 6. Algorithm 1, when given black-box access to a size-s circuit C in $\mathbf{x}$ variables and of degree $d = s^{O(1)}$, tests C on the $n-1$ identities in Lemma 3.3. The degree of each identity, when we use C in it, is at most d. If C computes HC_n, then Algorithm 1 will always return "Yes". If C does *not* compute HC_n, then some identity fails to hold for C. By the Polynomial Identity Lemma and the fact $|U| > 2d$, the probability that some identity fails to hold is at least $\frac{1}{2}$. By repeating Algorithm 1 $s^{O(1)}$ times, we can boost the success probability to $1-(\frac{1}{2})^{s^{O(1)}}$. This proves Theorem 5. Theorem 6 follows easily because the random matrices sampled by Algorithm 1 provide the list of counterexamples against polynomial-size circuits, assuming HC_n is not computable by polynomial-size circuits.

Algorithm 1 Circuit Testing for HC_n

Input: B.b.a to size-s circuit C in $\mathbf{x}$ variables and of degree $s^{O(1)}$.
Output: "Yes" if $\mathrm{C}(\mathbf{x}) = HC_n(\mathbf{x})$, else "No".

1. Let $U \subseteq \mathbb{F}$ with $|U| > 2d$. Choose $n-1$ matrices $M_2, M_3, \ldots, M_n$, where M_i are $i \times i$ matrices with entries chosen uniformly at random from U.
2. For $i \in [2,n]$, check if the i'th identity in Lemma 3.3 does not hold for C when evaluated at M_i. Return "No" if so.
3. Return "Yes".

4 Equivalence Testing for HC

In this section, we present the ET algorithm for HC_n, and argue its correctness and efficiency by using the structural results proven in Section 3. In Section 4.1, we show the reduction to PS-equivalence; the correctness of the reduction follows from Lemma 3.1. In Section 4.2, we show how to recover a permutation; the correctness follows from Observation 3.2. The problem then reduces to checking scaling equivalence with HC_n. In Section 4.3, we show how to recover a scaling matrix by using Proposition 3.4 and Lemma C.2. All missing proofs can be found in Appendix D. We present the analysis assuming $f = HC_n(A\mathbf{x})$ and that all steps which employ randomisation execute correctly. Every step where randomisation is used has a small probability of failing due to the assumption on the field size. We run Algorithm 1 at the end to verify the correctness of the recovered transform. If $f \neq HC_n(A\mathbf{x})$, Algorithm 1 will output "No" with high probability. If $f = HC_n(A\mathbf{x})$, Algorithm 1 always accepts.

4.1 Reduction to PS-equivalence

Algorithm 2 shows the reduction to PS-equivalence testing. If $f = HC_n(A\mathbf{x})$, then by Lemma 2.2, $\dim_{\mathbb{F}}(\mathfrak{g}_f)$ is $2n-2$.We then compute a random element of $\mathfrak{g}_f$ and diagonalise it. The algorithm outputs the diagonalising matrix if it exists. The correctness and complexity analysis of Algorithm 2 is given by Proposition 4.1.

Proposition 4.1. If $f = HC_n(A\mathbf{x})$ for some $A \in GL_{n^2-n}(\mathbb{F})$, with high probability Algorithm 2 computes in randomised $n^{O(1)}$ time a $D \in GL_{n^2-n}(\mathbb{F})$ such that $f(D\mathbf{x}) = HC_n(PS\mathbf{x})$.

Algorithm 2 Reduction to PS-equivalence Test

Input: B.b.a to $f(\mathbf{x})$.
Output: $D \in \mathrm{GL}_{n^2-n}(\mathbb{F})$ s.t. $f(D\mathbf{x}) = HC_n(PS\mathbf{x})$ if $f(\mathbf{x}) = HC_n(A\mathbf{x})$.

1. Compute a basis $\{B_1, B_2, \ldots, B_k\}$ of $\mathfrak{g}_f$ from b.b.a to f. If $k \neq 2n-2$, abort and output "f not equivalent to HC_n".
2. Let $U \subseteq \mathbb{F}$ be such that $|U| = 3n^5$. Let $a_1, a_2 \ldots a_k \in_r U$ and $C := \sum_{i\in[k]} a_i B_i$. Compute and output a matrix D such that $D^{-1}CD$ is a diagonal matrix. If such a D does not exist, abort output "f not equivalent to HC_n".

4.2 P-equivalence test

Let $f(\mathbf{x}) = HC_n(P\mathbf{x})$. Using the permutation symmetries and second-order partial derivatives of HC_n, Algorithm 3 recovers a permutation P' such that $f(\mathbf{x}) = HC_n(P'\mathbf{x})$, where P' is P up to a permutation symmetry. Claim 4.1 and Proposition 4.2 argue the correctness.

Claim 4.1. Without loss of generality, $P(x_{1,2}) = x_{1,2}$.

Proposition 4.2. If $f(\mathbf{x}) = HC_n(P\mathbf{x})$, then with high probability Algorithm 3 computes P' in randomised $n^{O(1)}$ time such that $P' = \tilde{P}P$, where $\tilde{P}$ is as described in Proposition 3.5.

Algorithm 3 P-equivalence Test

Input: B.b.a to $f(\mathbf{x})$.
Output: $P' \in \mathrm{GL}_{n^2-n}(\mathbb{F})$ s.t. $HC_n(P'\mathbf{x}) = f(\mathbf{x})$, if $f(\mathbf{x}) = HC_n(P\mathbf{x})$.

1. Compute b.b.a to $\frac{\partial^2 HC_n}{\partial x_{i,j}\partial x_{k,\ell}}$, where $i \neq j$ and $k \neq \ell$. Check if $\frac{\partial^2 HC_n}{\partial x_{i,j}\partial x_{k,\ell}}$ is identically zero or not, and store this information.
2. Compute the set $R'_{1,2} := \{x_{k,\ell} \mid \frac{\partial^2 HC_n}{\partial x_{1,2}\partial x_{k,\ell}} = 0 \text{ and } (k,\ell) \neq (1,2)\}$. Partition $R'_{1,2}$ as $\{x_{i,j}\} \sqcup Q'_{1,2} \sqcup T'_{1,2}$ such that items 1 and 2 in Observation 3.2 hold. If no such partition exists, abort and output "f not equivalent to HC_n".
3. Set $P'(x_{1,2}) := x_{1,2}$, $P'(x_{2,1}) := x_{i,j}$ and $P'(x_{1,t}) := x_{i_t,j_t}$, where $x_{i_t,j_t} \in T'_{1,2}$ and $t \in [3,n]$.
4. For all $x_{i_t,j_t} \in T'_{1,2}$, compute R'_{i_t,j_t} as in Step 2 and partition it. Let $\{x_{k_t,\ell_t}\}$ be the singleton set in the partitioning. Set $P'(x_{t,1}) := x_{k_t,\ell_t}$. Abort and output "$f$ not equivalent to HC_n" if the partition does not exist.
5. For $a, b \in [2,n]$, $a \neq b$, compute $R'_{k_a,\ell_a} \cap R'_{i_b,j_b}$, where $P'(x_{a,1}) = x_{k_a,\ell_a}$ and $P'(x_{1,b}) = x_{i_b,j_b}$, as computed in earlier steps. If $R'_{k_a,\ell_a} \cap R'_{i_b,j_b}$ is a singleton $\{x_{c,d}\}$, set $P'(x_{a,b}) := x_{c,d}$, else abort and output "f not equivalent to HC_n".
6. Output P'.

4.3 S-equivalence test

We assume $n \neq 4$. Suppose $f(\mathbf{x}) = HC_n(S\mathbf{x})$, where $S \in GL_{n^2-n}(\mathbb{F})$ is a scaling matrix. Algorithm 4 gives the scaling equivalence test over $\mathbb{F}_q$. The same algorithm, with some changes, will also work over other fields $\mathbb{F}$, see Appendix D.5.1 for details. The correctness of Step 1 follows from Claim 4.2, while that of the remaining steps follows from Proposition 4.3. In Appendix D.6, we show an S-equivalence test for HC_4 over $\mathbb{Q}$, $\mathbb{R}$, and finite fields.

Claim 4.2. Without loss of generality, $S'_{1,j} = 1$, $S'_{2,3} = 1$ and $S'_{i,1} = 1$, where $i \in [2,n-1], j \in [2,n]$.

Proposition 4.3. If $f(\mathbf{x}) = HC_n(S\mathbf{x})$, then in deterministic $(n \log q)^{O(1)}$ time Algorithm 4 outputs an S' such that $S'S$ is a scaling symmetry of HC_n.

Algorithm 4 S-equivalence test

Input: B.b.a to $f(\mathbf{x})$.
Output: $S' \in \mathrm{GL}_{n^2-n}(\mathbb{F}_q)$ s.t. $HC_n(S'\mathbf{x}) = f(\mathbf{x})$ and $S' = \tilde{S}S$, where $\tilde{S}$ is a scaling symmetry, if $f(\mathbf{x}) = HC_n(S\mathbf{x})$.

1. Set $S'_{1,j} = 1$, $S'_{2,3} = 1$ and $S'_{i,1} = 1$, where $i \in [2, n-1], j \in [2, n]$.
2. Query f to obtain the coefficients of monomials corresponding to the rows $\sigma_1, \ldots, \sigma_{(n-1)(n-2)}$ of the matrix $M^{(n)}$ constructed in Proposition C.1. Let c_k be the k'th coefficient. If $c_k = 0$ for some k, then abort and ouput "f not equivalent to HC_n".
3. Let $T := \{(i,j) |\ (i,j) \neq (1,k),\ k \in [2,n]$ and $(i,j) \neq (\ell, 1),\ \ell \in [2, n-1]$ and $(i,j) \neq (2,3)\}$. Consider the matrix $M := M^{(n)}_{\bullet \times T}$. Compute $\beta = (det(M))^{-1}$ in $\mathbb{Z}_{q-1}$.
4. For each row σ_k, $k \in [(n-1)(n-2)]$ and $(i,j) \in T$, compute the cofactor of M with respect to σ_k and (i,j), and denote it as $\alpha_{k,(i,j)}$. Set $S'_{i,j} = \prod_{k=1}^{(n-1)(n-2)} c_k^{\beta\alpha_{k,(i,j)} \bmod q-1}$.
5. Output S'.

5 Acknowledgements

The author thanks Chandan Saha for suggesting the problem and Abhiram Aravind for going through the proofs, which helped improve the presentation of the paper. The author also thanks the anonymous reviewers of MFCS 2026 for their constructive and informative feedback, particularly one reviewer for pointing to the Pascal Determinant polynomial family, which is VNP-complete and for which an ET algorithm can be designed using knowledge of its continuous symmetries.

References

[AB87] Noga Alon and Ravi B. Boppana. The monotone circuit complexity of boolean functions. *Comb.*, 7(1):1–22, 1987. 2, 21

[Ara11] Manuel Araújo. Classification of Quadratic forms. https://www.math.tecnico.ulisboa.pt/~ggranja/manuel.pdf, 2011. 19

[AS05] Manindra Agrawal and Nitin Saxena. Automorphisms of Finite Rings and Applications to Complexity of Problems. In Volker Diekert and Bruno Durand, editors, *STACS 2005, 22nd Annual Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, February 24-26, 2005, Proceedings*, volume 3404 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2005. 1, 19

[Bac90] Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990. 49

[BDGT24] Vishwas Bhargava, Pranjal Dutta, Sumanta Ghosh, and Anamay Tengse. The Complexity of Order-Finding for ROABPs. *CoRR*, abs/2411.18981, 2024. 1, 20

[BDJ26] Markus Bläser, Sagnik Dutta, and Gorav Jindal. Problems from Optimization and Computational Algebra Equivalent to Hilbert's Nullstellensatz. In Kasper Green Larsen and Barna Saha, editors, *Proceedings of the 2026 Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2026, Vancouver, BC, Canada, January 11-14, 2026*, pages 6308–6331. SIAM, 2026. 20

[BDS24] Omkar Baraskar, Agrim Dewan, and Chandan Saha. Testing Equivalence to Design Polynomials. In Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov, editors, *41st International Symposium on Theoretical Aspects of Computer Science, STACS 2024, Clermont-Ferrand, France, March 12-14, 2024*, volume 289 of *LIPIcs*, pages 9:1–9:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. 20

[BDSS24] Omkar Baraskar, Agrim Dewan, Chandan Saha, and Pulkit Sinha. NP-Hardness of Testing Equivalence to Sparse Polynomials and to Constant-Support Polynomials. In Karl Bringmann, Martin Grohe, Gabriele Puppis, and Ola Svensson, editors, *51st International Colloquium on Automata, Languages, and Programming, ICALP 2024, July 8-12, 2024, Tallinn, Estonia*, volume 297 of *LIPIcs*, pages 16:1–16:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. Full version available at ECCC. 1, 20

[Ber71] Elwyn R. Berlekamp. Factoring polynomials over large finite fields. In Stanley R. Petrick, Jean E. Sammet, Robert G. Tobey, and Joel Moses, editors, *Proceedings of the second ACM symposium on Symbolic and algebraic manipulation, SYMSAC 1971, Los Angeles, California, USA, March 23-25, 1971*, page 223. ACM, 1971. 3

[BM25] Jaroslaw Blasiok and Linus Meierhöfer. Hardness of Clique Approximation for Monotone Circuits. In Srikanth Srinivasan, editor, *40th Computational Complexity Conference, CCC 2025, Toronto, Canada, August 5-8, 2025*, LIPIcs, pages 4:1–4:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. 21

[Bot67] Peter Botta. Linear Transformations that Preserve the Permanent. *Proceedings of the American Mathematical Society*, 18(3):566–569, 1967. 3, 5

[Bre76] Richard P. Brent. Multiple-precision zero-finding methods and the complexity of elementary function evaluation. In J.F. Traub, editor, *Analytic Computational Complexity*, pages 151–176. Academic Press, 1976. 49

[BRS17] Markus Bläser, B. V. Raghavendra Rao, and Jayalal Sarma. Testing Polynomial Equivalence by Scaling Matrices. In Ralf Klasing and Marc Zeitoun, editors, *Fundamentals of Computation Theory - 21st International Symposium, FCT 2017, Bordeaux, France, September 11-13, 2017, Proceedings*, volume 10472 of *Lecture Notes in Computer Science*, pages 111–122. Springer, 2017. 19

[BSS89] Lenore Blum, Mike Shub, and Steve Smale. On a Theory of Computation and Complexity over the Real Numbers: NP-completeness, Recursive Functions and Universal Machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, 1989. 3

[Bür00] Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*, volume 7 of *Algorithms and computation in mathematics*. Springer, 2000. 1, 2, 5, 9, 18, 21, 22

[Bür24] Peter Bürgisser. Completeness classes in algebraic complexity theory. *CoRR*, abs/2406.06217, 2024. 22

[CGG+26] Abhranil Chatterjee, Sumanta Ghosh, Rohit Gurjar, Roshan Raj, and Thomas Thierauf. Bipartite matching is in NC. *Electron. Colloquium Comput. Complex.*, TR26, 2026. 2

[CGR+25] Bruno Cavalar, Mika Göös, Artur Riazanov, Anastasia Sofronova, and Dmitry Sokolov. Monotone Circuit Complexity of Matching. *CoRR*, abs/2507.16105, 2025. To appear in the proceedings of 58th Annual ACM Symposium on Theory of Computing (STOC 2026). 21

[CGS23] Suryajith Chillara, Coral Grichener, and Amir Shpilka. On Hardness of Testing Equivalence to Sparse Polynomials Under Shifts. In Petra Berenbrink, Patricia Bouyer, Anuj Dawar, and Mamadou Moustapha Kanté, editors, *40th International Symposium on Theoretical Aspects of Computer Science, STACS 2023, March 7-9, 2023, Hamburg, Germany*, volume 254 of *LIPIcs*, pages 22:1–22:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. 20

[CKR22] Bruno Pasqualotto Cavalar, Mrinal Kumar, and Benjamin Rossman. Monotone Circuit Lower Bounds from Robust Sunflowers. *Algorithmica*, 84(12):3655–3685, 2022. Conference version appeared in the proceedings of LATIN 2020. 21

[DL78] Richard A. DeMillo and Richard J. Lipton. A Probabilistic Remark on Algebraic Program Testing. *Inf. Process. Lett.*, 7(4):193–195, 1978. 3

[DOS14] Zeev Dvir, Rafael Oliveira, and Amir Shpilka. Testing Equivalence of Polynomials under Shifts. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 417–428. Springer, 2014. 19

[DRS24] Pranjal Dutta, Mahesh Sreekumar Rajasree, and Santanu Sarkar. Complexity of Monomial Prediction in Cryptography and Machine Learning. In *2024 26th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, pages 118–125, 2024. 2, 22

[FGT21] Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite Perfect Matching is in Quasi-NC. *SIAM J. Comput.*, 50(3), 2021. Conference version appeared in the proceedings of STOC 2016. 2

[GGKS19] Ankit Garg, Nikhil Gupta, Neeraj Kayal, and Chandan Saha. Determinant Equivalence Test over Finite Fields and over Q. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, Patras, Greece, July 9-12, 2019*, volume 132 of *LIPIcs*, pages 62:1–62:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. 20

[GJ81] Ian P. Goulden and David M. Jackson. The Enumeration of Directed Closed Euler Trails and Directed Hamiltonian Circuits by Lagrangian Methods. *Eur. J. Comb.*, 2(2):131–135, 1981. 2, 20

[GMQ16] Joshua A. Grochow, Ketan D. Mulmuley, and Youming Qiao. Boundaries of VP and VNP. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, Rome, Italy, July 11-15, 2016*, LIPIcs, pages 34:1–34:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. 2, 22

[GQ23] Joshua A. Grochow and Youming Qiao. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness. *SIAM J. Comput.*, 52(2):568–617, 2023. Conference version appeared in the proceedings of ITCS 2021. 19

[Gre11] Bruno Grenet. An Upper Bound for the Permanent versus Determinant Problem. Manuscript, 2011. 21

[Gri97] Dima Grigoriev. Testing Shift-Equivalence of Polynomials by Deterministic, Probabilistic and Quantum Machines. *Theor. Comput. Sci.*, 180(1-2):217–228, 1997. 19

[Gro12] Joshua A. Grochow. *Symmetry and equivalence relations in classical and geometric complexity theory*. PhD thesis, University of Chicago, Chicago, IL, 2012. 1, 2, 6, 18, 20, 45

[Gro17] Joshua A. Grochow. Monotone Projection Lower Bounds from Extended Formulation Lower Bounds. *Theory Comput.*, 13(1):1–15, 2017. 2, 21

[GS19] Nikhil Gupta and Chandan Saha. On the Symmetries of and Equivalence Test for Design Polynomials. In Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen, editors, *44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, Aachen, Germany, August 26-30, 2019*, volume 138 of *LIPIcs*, pages 53:1–53:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. 2, 1, 3, 4, 5, 6, 18, 19, 20

[GST23] Nikhil Gupta, Chandan Saha, and Bhargav Thankey. Equivalence Test for Read-Once Arithmetic Formulas. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 4205–4272. SIAM, 2023. 1, 19, 20

[Gur04] Leonid Gurvits. Classical complexity and quantum entanglement. *J. Comput. Syst. Sci.*, 69(3):448–484, 2004. 1

[Hal15] Brian C. Hall. *Lie Groups, Lie Algebras, and Representations*. Springer, 2015. 6

[HI16] Jesko Hüttenhain and Christian Ikenmeyer. Binary determinantal complexity. *Linear Algebra and its Applications*, 504:559–573, 2016. 2, 21

[HK71] Kenneth Hoffman and Ray Kunze. *Linear Algebra*. Pearson, second edition, 1971. 30

[Hru16] Pavel Hrubes. On Hardness of Multilinearization and VNP-Completeness in Characteristic 2. *ACM Trans. Comput. Theory*, 9(1):1:1–1:14, 2016. 2, 22

[IM18] Christian Ikenmeyer and Stefan Mengel. On the relative power of reduction notions in arithmetic circuit complexity. *Inf. Process. Lett.*, 130:7–10, 2018. 2, 22

[IS22] Christian Ikenmeyer and Abhiroop Sanyal. A note on VNP-completeness and border complexity. *Inf. Process. Lett.*, 176:106243, 2022. 2, 22

[JS82] Mark Jerrum and Marc Snir. Some Exact Complexity Results for Straight-Line Computations over Semirings. *J. ACM*, 29(3):874–897, 1982. 2, 21

[JSV04] Mark Jerrum, Alistair Sinclair, and Eric Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. *J. ACM*, 51(4):671–697, 2004. Conference version appeared in the proceedings of STOC 2001. 2

[Juk14] Stasys Jukna, 2014. https://cstheory.stackexchange.com/questions/27496/why-is-hamiltonian-cycle-so-different-from-permanent. 21

[Juk15] Stasys Jukna. Lower Bounds for Tropical Circuits and Dynamic Programs. *Theory Comput. Syst.*, 57(1):160–194, 2015. 2, 21

[Kay11] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In Dana Randall, editor, *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pages 1409–1421. SIAM, 2011. 1, 19, 20

[Kay12] Neeraj Kayal. Affine projections of polynomials: extended abstract. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 643–662, 2012. 2, 1, 3, 4, 5, 6, 18, 19, 20

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. *Comput. Complex.*, 13(1-2):1–46, 2004. Conference version appeared in the proceedings of STOC 2003. 2, 18

[KNS19] Neeraj Kayal, Vineet Nair, and Chandan Saha. Average-case linear matrix factorization and reconstruction of low width algebraic branching programs. *Comput. Complex.*, 28(4):749–828, 2019. 19

[KNST19] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of Full Rank Algebraic Branching Programs. *ACM Trans. Comput. Theory*, 11(1):2:1–2:56, 2019. Conference version appeared in the proceedings of CCC 2017. 3, 6, 19, 20

[KPTT15] Pascal Koiran, Natacha Portier, Sébastien Tavenas, and Stéphan Thomassé. A τ -conjecture for Newton Polygons. *Found. Comput. Math.*, 15(1):185–197, 2015. 2, 22

[KT90] Erich L. Kaltofen and Barry M. Trager. Computing with Polynomials given by Black Boxes for their Evaluations: Greatest Common Divisors, Factorization, Separation of Numerators and Denominators. *J. Symb. Comput.*, 9(3):301–320, 1990. Conference version appeared in the proceedings of FOCS 1988. 3

[Lam04] T. Y. Lam. *Introduction To Quadratic Forms Over Fields*. American Mathematical Society, 2004. 19

[Lan15] Joseph M Landsberg. Geometry and complexity theory. *NSF Award Number 1405348. Directorate for Mathematical and Physical Sciences*, 14(1405348):5348, 2015. 1

[Lip89] Richard J. Lipton. New directions in testing. In Joan Feigenbaum and Michael Merritt, editors, *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, pages 191–202. DIMACS/AMS, 1989. 3

[LLL82] Arjen K Lenstra, Hendrik W Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. 3

[Mal03] Guillaume Malod. *Polynômes et coefficients. (Polynomials and coefficients)*. PhD thesis, Claude Bernard University Lyon 1, France, 2003. 2, 21

[Mal07] Guillaume Malod. The complexity of polynomials and their coefficient functions. In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007), 13-16 June 2007, San Diego, California, USA*, pages 193–204. IEEE Computer Society, 2007. 2, 22

[Mer83] Russell Merris. Single-hook characters and hamiltonian circuits. *Linear and Multilinear Algebra*, 14(1):21–35, 1983. 18, 20

[MM62] Marvin Marcus and FC May. The Permanent Function. *Canadian Journal of Mathematics*, 14:177–189, 1962. 3, 5

[MNS20] Janaky Murthy, Vineet Nair, and Chandan Saha. Randomized Polynomial-Time Equivalence Between Determinant and Trace-IMM Equivalence Tests. In *45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020, August 24-28, 2020, Prague, Czech Republic*, volume 170 of *LIPIcs*, pages 72:1–72:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. 20

[MR04] Thierry Mignon and Nicolas Ressayre. A quadratic bound for the determinant and permanent problem. *International Mathematics Research Notices*, 2004(79):4241–4253, 01 2004. 21

[MS01] Ketan Mulmuley and Milind A. Sohoni. Geometric Complexity Theory I: An Approach to the P vs. NP and Related Problems. *SIAM J. Comput.*, 31(2):496–526, 2001. 2

[MS18] Meena Mahajan and Nitin Saurabh. Some Complete and Intermediate Polynomials in Algebraic Complexity Theory. *Theory Comput. Syst.*, 62(3):622–652, 2018. Conference version appeared in the proceedings of CSR 2016. 21

[MS21] Dori Medini and Amir Shpilka. Hitting Sets and Reconstruction for Dense Orbits in VP_e and $\Sigma\Pi\Sigma$ circuits. In Valentine Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, Toronto, Ontario, Canada (Virtual Conference), July 20-23, 2021*, LIPIcs, pages 19:1–19:27. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 20

[Mul10] Ketan Mulmuley. Explicit proofs and the flip. *arXiv preprint arXiv:1009.0246*, 2010. 4

[Mul11] Ketan Mulmuley. On P vs. NP and geometric complexity theory: Dedicated to Sri Ramakrishna. *J. ACM*, 58(2):5:1–5:26, 2011. 4

[Raz85] Alexander Razborov. Lower bounds on the monotone complexity of some boolean function. In *Soviet Math. Dokl.*, volume 31, pages 354–357, 1985. 21

[RR19] C. Ramya and B. V. Raghavendra Rao. Linear projections of the Vandermonde polynomial. *Theor. Comput. Sci.*, 795:165–182, 2019. 20

[RS25] C. Ramya and Pratik Shastri. On the Hardness of Order Finding and Equivalence Testing for ROABPs. In C. Aiswarya, Ruta Mehta, and Subhajit Roy, editors, *45th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2025, BITS Pilani, K K Birla Goa Campus, India, December 17-19, 2025*, LIPIcs, pages 49:1–49:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. 1, 20

[Sax06] Nitin Saxena. *Morphisms of rings and applications to complexity*. PhD thesis, Indian Institute of Technology, Kanpur, 2006. 1, 19

[Sch80] Jacob T. Schwartz. Fast Probabilistic Algorithms for Verification of Polynomial Identities. *J. ACM*, 27(4):701–717, 1980. 3

[SG25] Hamilton Sawczuk and Edinah Gnang. Two proofs of the hamiltonian cycle identity. *CoRR*, abs/2510.02473, 2025. 20

[Sha73] Daniel Shanks. Five number-theoretic algorithms. In *Proceedings of the Second Manitoba Conference on Numerical Mathematics (Winnipeg), 1973*, 1973. 49

[Thi98] Thomas Thierauf. The Isomorphism Problem for Read-Once Branching Programs and Arithmetic Circuits. *Chic. J. Theor. Comput. Sci.*, 1998, 1998. 1

[Ton91] Alberto Tonelli. Bemerkung über die auflösung quadratischer congruenzen. *Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen*, 1891:344–346, 1891. 49

[Val79] Leslie G. Valiant. Completeness classes in algebra. In Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho, editors, *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 249–261. ACM, 1979. 1, 2, 21

[Wal13] Lars Ambrosius Wallenborn. Computing the hilbert symbol, quadratic form equivalence and integer factoring. Diploma thesis, Rheinischen Friedrich-Wilhelms-Universität Bonn, 2013. 19

[Ye11] Ke Ye. The stabilizer of immanants. *Linear Algebra and its Applications*, 435(5):1085–1098, 2011. 18

[ZB11] Jinshan Zhang and Fengshan Bai. An improved fully polynomial randomized approximation scheme (FPRAS) for counting the number of hamiltonian cycles in dense digraphs. *Theor. Comput. Sci.*, 412(4-5):419–429, 2011. 3, 4, 5, 9

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979. 3

A Comparison with [Kay12] and [GS19]

Lie Algebra has been used to develop ET algorithms for many polynomial families; refer to Appendix B for an overview. As our techniques are based on [Kay12, GS19], we compare our techniques with theirs. Since HC_n is a linear combination of the Immanant polynomials [Mer83, Bür00], and the symmetries and Lie algebra of Immanants are known [Ye11], it is possible that the symmetries of HC_n can be studied via those of the Immanant polynomials. However, the definition of the Immanant polynomial is representation theoretic, and the proof technique of [Ye11] also involves some representation theory, while HC_n has a simpler and intuitive definition, and our proof technique does *not* need representation theory. Moreover, HC_n is a linear combination of the Immanant polynomials as long as the characteristic of the underlying field does *not* divide n, thus the analysis of HC_n via this linear combination may not hold over all fields. It is also unclear whether the proof of [Ye11] will directly yield an ET algorithm or hold for HC, because at certain points *non-cyclic* permutations are needed in their proof.

Comparison with [Kay12]. The author of [Kay12] uses the symmetries of the Permanent polynomial to describe an explicit basis for the Lie algebra of the Permanent polynomial. In contrast, the symmetries and the Lie Algebra of HC_n have not been studied before to our knowledge, so we analyse the Lie Algebra first and use it to argue about the symmetries. We use ideas from [GS19] to establish an explicit basis for the Lie algebra of HC_n, see Comparison with [GS19] for more details.

In Proposition 3.1, we give a basis for $\mathfrak{g}_{HC_n}$ over *any* field, except for $n = 4$. All but one of the elements of this basis are similar to those of the basis for $\mathfrak{g}_{Perm_n}$, the Lie algebra of the Permanent polynomial, given in Proposition 39 in [Kay12]. The single differing basis element for HC_n ensures the linear independence of the basis elements over *every* field. In contrast, the basis given for $\mathfrak{g}_{Perm_n}$ is a basis as long as the characteristic of the underlying field does *not* divide n, the degree of the Permanent polynomial. For HC_4, we give a basis over characteristic 2 fields separately from other fields. This exception arises because $\mathfrak{g}_{HC_4}$ is determined by the *nullspace* of 6 linear equations in 12 variables, each corresponding to a permutation in C_4, such that all the equations are linearly dependent over characteristic 2 fields. Five of the linear equations are linearly independent over any field, implying that the sixth equation is a linear combination of the five equations over characteristic 2 fields. This causes $\mathfrak{g}_{HC_4}$ to be 6 dimensional over fields of characteristic other than 2 and 7 dimensional over characteristic 2 fields. Using this, we show that HC_4 has discrete symmetries over $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and certain finite fields. See Appendix C.17 for details.

Our implementation of Step 2 differs from that for the Permanent polynomial because the set of vanishing second-order partial derivatives of HC_n differs from that for the Permanent polynomial. As mentioned earlier, our execution of Step 3 for HC_n completely differs from that for the Permanent. For the Permanent, there are sufficiently many pairs of monomials such that for each pair, the monomials differ in exactly two variables. For example, the monomials $x_{1,1}x_{2,2}x_{3,3}\dots x_{n,n}$ and $x_{1,2}x_{2,1}x_{3,3}\dots x_{n,n}$ share $n-2$ variables. Assuming that $x_{1,1}, x_{1,2}$ and $x_{2,1}$ are unscaled, which follows from the scaling symmetries of the Permanent, we query the scaled Permanent polynomial at these two monomials, which gives two scalars λ_1 and λ_2. Then, $\frac{\lambda_1}{\lambda_2}$ is the factor by which $x_{2,2}$ is scaled. In this way, S can be recovered from black-box access to a scaled Permanent polynomial. In contrast, any two monomials of HC_n differ in at least 3 variables (see Claim 3.1). It is then unclear whether Step 3 can be performed in a similar way to the Permanent polynomial. Instead, we implement Step 3 by solving a system of linear equations as was done in [GS19]. For the Permanent polynomial, Step 4 can be performed via downward self-reducibility [KI04], as was done in [Kay12], or by using circuit identities arising from the characterisation by symmetries of the Permanent, see Page 81, Proof of Theorem 3.2.1 in [Gro12]. The latter identities also yield a *more* efficient circuit testing algorithm. In contrast, though HC_n is not characterised by its symmetries, we use its downward self-reducibility to verify if the given input is equivalent to HC_n under the recovered transform.

Comparison with [GS19]. The authors of [GS19] studied the Lie Algebra and symmetries of the Nisan-Wigderson polynomial, denoted NW, and gave an ET algorithm for NW in a special case where A is a block-permuted permutation scaling matrix. The monomials of NW correspond to the evaluations of a

low-degree univariate polynomial over a finite field, while those of HC_n correspond to cyclic permutations. This leads to many structural differences between the symmetries and the Lie algebras of HC_n and NW.

The main idea we use from [GS19] is their argument for establishing a basis for $\mathfrak{g}_{NW}$, the Lie algebra of NW. They argue an upper bound on the nullity of a matrix M, where the rows of M are the linear equations that determine $\mathfrak{g}_{NW}$, and the nullspace of M is $\mathfrak{g}_{NW}$. To establish this upper bound, they lower bound the rank of M by constructing an appropriate full rank submatrix M' of M. Then, they show an explicit set of linearly independent vectors that lies in the nullspace of M and has the same size as the upper bound, thus getting a basis of $\mathfrak{g}_{NW}$. They describe M' explicitly and use it to describe all scaling symmetries of NW over $\mathbb{Q}$, $\mathbb{R}$, and certain finite fields, and give a scaling equivalence test for NW over $\mathbb{R}$ and certain finite fields.

While we follow the same idea at a high level, the crucial difference is that our argument for HC_n holds over *any* field, as shown in Proposition 3.2. This is in contrast to the case of NW, where the nullity upper bound argument holds as long as the characteristic of the field does not divide d, the degree of NW. While the authors of [GS19] describe M' explicitly, we construct M' efficiently via induction in our case, as shown in Proposition C.1. We also leverage M' to describe all scaling symmetries of HC_n and give a scaling equivalence test for it over *all* fields.

B Other related works

B.1 Results on PE

As stated in Section 1, the complexity of PE is not well understood. PE is known to be in PSPACE over $\mathbb{C}$, in EEXP over $\mathbb{R}$, in NP $\cap$ co-AM over finite fields, and over $\mathbb{Q}$ it is not even known to be decidable [Sax06]. Even when both the inputs are restricted, limited results are known. The variant in which both inputs are degree two polynomials is called Quadratic form equivalence (QFE). Due to well-known classification results for such polynomials [Lam04, Ara11], QFE has polynomial time algorithms over $\mathbb{R}$, $\mathbb{C}$, finite fields, and $\mathbb{Q}$ (assuming access to an integer factoring oracle) [Sax06, Wal13]. In contrast, Cubic form equivalence (CFE), where both inputs are degree three polynomials, is at least as hard as graph isomorphism [AS05, Kay11]. Further, CFE is polynomial time equivalent to isomorphism/equivalence problems like algebra isomorphism, trilinear form-equivalence, etc., as shown by [GQ23]. Recently, in [GST23], the authors studied PE for orbits of ROFs, a significant generalization of QFE, and gave a randomised polynomial time algorithm for PE for orbits of additive-constant-free ROFs, a mild restriction of general ROFs.

A variant of PE is the Shift Equivalence Test problem (SET), as referred to by [DOS14], where we have to decide for given $f, g \in \mathbb{F}[\mathbf{x}]$ whether $f(\mathbf{x}) = g(\mathbf{x} + \mathbf{b})$ for some $\mathbf{b} \in \mathbb{F}^{|\mathbf{x}|}$. The author of [Gri97] showed that when f and g are given verbosely as a list of coefficients of all $\binom{n+d}{d}$ monomials, there is a deterministic algorithm over characteristic 0 fields, a randomised algorithm over prime residue fields and a quantum algorithm for characteristic 2 fields, all with running time polynomial in $\binom{n+d}{d}$. Later, [DOS14] gave a randomised $(nds)^{O(1)}$ algorithm when f and g are given as black-boxes with degree bound d and circuit size bound s. The author of [Kay12] also gave a randomised polynomial-time algorithm for SET; see Theorem 28 in the paper, and Appendix B of [KNST19] for another proof.

In [BRS17], the authors studied the Scaling equivalence problem, yet another variant of PE, which involves checking for two given polynomials f and g whether there exists a scaling matrix $S \in \mathrm{GL}_{|\mathbf{x}|}(\mathbb{F})$ such that $f(\mathbf{x}) = g(S\mathbf{x})$. They gave a randomised polynomial-time algorithm for the scaling equivalence problem over $\mathbb{R}$ when the inputs are given as black boxes.

B.2 Results on ET

As mentioned in Section 1, the study of ET for polynomial families was initiated in [Kay11] where randomised polynomial time ET algorithms were given for the Power Symmetric and the Elementary Symmetric polynomials. Following this, efficient ET algorithms were given for several other important polynomial families and circuit classes, see Table 2. The authors of [KNS19] used ET for the determinant to give an

	Algorithmic results (randomised polynomial time)	
Family/Circuit class	***Technique***	***Reference***
Determinant	Lie Algebra	[Kay12, Gro12, GGKS19]
Permanent	Lie Algebra	[Kay12]
IMM	Lie Algebra	[KNST19]
Trace-IMM	Lie Algebra	[MNS20]
Sum-Product	Hessian,Lie Algebra, Vector Space Decomposition	[Kay11, GST23, BDS24, MS21]
Power Symmetric	Hessian	[Kay11]
Elementary Symmetric	Second-order partial derivative	[Kay11]
Vandermonde	Analysis of product of linear forms	[RR19]
Continuant	Interpolating sets, Directional derivatives analysis of product of linear forms	[MS21]
Design Polynomials	Lie Algebra, Vector Space Decomposition	[GS19, BDS24]
ROF	Hessian	[GST23]
Hamiltonian Cycle polynomial	Lie Algebra	**This work**
	Hardness results	
Sparse polynomials	NP-hardness	[BDSS24]
ROABP	NP-hardness	[BDGT24, RS25]

Table 2: A list of ET results

efficient average-case reconstruction algorithm for low-width Algebraic Branching Programs (ABPs). Thus, ET algorithms have been used to design efficient reconstruction algorithms.

It is clear from Table 2 that studying ET for polynomial families has led to efficient algorithms in every case so far. In contrast, read-once formulas (ROFs) and t-design polynomials for low t, a subclass of sparse polynomials (depth-2 circuits), are the only circuit classes for which we have efficient ET algorithms so far. Sparse polynomials form a natural circuit class for which ET was shown to be NP-hard [BDSS24]. Later, the authors of [BDGT24] showed the NP-hardness of testing permutation equivalence to read-once oblivious algebraic branching programs (ROABPs). The authors of [RS25] adapted the techniques of [BDSS24, BDGT24] to show ET for ROABPs is NP-hard.

Other hardness results. The author of [Kay12] showed that the more general problem of checking if a polynomial is an affine projection[8] of another polynomial is NP-hard via a reduction from Graph 3-Colorability. More recently, the authors of [BDJ26] improved upon the result in [Kay12] by showing a reduction from polynomial solvability over any field to checking affine equivalence of polynomials. They also showed that the SparseShift problem[9], a variant of the Shift Equivalence Testing problem, is at least as hard as polynomial solvability over any integral domain including fields. This result is an improvement over [CGS23], where the authors showed the same result but over integral domains which are *not* fields.

B.3 Related works involving HC

Connections and comparisons between Permanent and HC. The authors of [GJ81] showed an identity expressing HC_n as a sum of the product of the evaluation of the Permanent and the Determinant polynomials at various submatrices of X_n; see [SG25] for an accessible proof. The author of [Mer83] showed that HC_n can also be written as a linear combination of Immanant polynomials, which are a generalization of

[8] An n-variate polynomial $f(\mathbf{x})$ is an affine projection of m-variate $g(\mathbf{y})$ if there exist an $A \in \mathbb{F}^{m\times n}$ and a $\mathbf{b} \in \mathbb{F}^m$ such that $f(\mathbf{x}) = g(A\mathbf{x}+\mathbf{b})$.

[9] The problem involves checking if for a given $f(\mathbf{x})$ whether $f(\mathbf{x}+\mathbf{b})$ has strictly fewer monomials than f for some shift $\mathbf{b} \in \mathbb{F}^{|\mathbf{x}|}$.

Result	***Permanent***	HC_n
Monotone circuit lower bound	$n(2^{n-1}-1)$ [JS82]	$(n-1)((n-2)2^{n-3}+1)$ [JS82]
Tropical circuit lower bound	$2^{\Omega(n)}$ [Juk15]	$2^{\Omega(n)}$ [Juk15]
Monotone Boolean circuit lower bound	$2^{n^{1/3-o(1)}}$ [CGR+25]	$2^{\tilde{\Omega}(n^{1/4})}$ [BM25]
Determinantal complexity lower bound	$\frac{n^2}{2}$ [MR04]	**Unknown**
Binary determinantal complexity upper bound	2^n-1 [Gre11]	$(n-1)2^{n-2}+1$ [HI16]

Table 3: Some bounds for the Permanent and HC_n

the Permanent and the Determinant polynomials. In [Bür00], the author showed that HC_{n-2} can be written as a rational linear combination of p-projections of HC_n and the Determinant polynomial.[10]

The Permanent polynomial and HC_n have been studied with respect to lower bounds and upper bounds, with some results as presented in Table 3. The authors of [JS82] studied the computation of polynomials by circuits over semi-rings[11], which led to monotone arithmetic circuit lower bounds. They showed a $2^{\Omega(n)}$ monotone arithmetic circuit lower bound for HC_n and the Permanent over the semi-ring $(\mathbb{R}^{\geq 0}, +, \times, 0, 1)$. They also showed that for a polynomial f, monotone arithmetic circuit lower bounds over the Boolean semi-ring $\mathbb{B} = (\{0,1\}, \vee, \wedge, 0, 1)$ imply monotone arithmetic circuit lower bounds over $(\mathbb{R}^{\geq 0}, +, \times, 0, 1)$. Note, monotone Boolean circuit lower bounds for the Boolean function defined by f imply monotone arithmetic circuit lower bounds for f over $\mathbb{B}$.

A monotone Boolean circuit lower bound for the Hamiltonian Cycle function follows from the fact that the Clique function is a monotone Boolean projection[12] of HC_n, as observed by [AB87, Val79], and such lower bounds for the Clique function have been studied [AB87, CKR22, BM25], with the most recent lower bound being $2^{\tilde{\Omega}(n^{1/2})}$. Prior to the improved monotone Boolean circuit lower bound for the Permanent function by [CGR+25], the best known bound was $n^{\Omega(\log n)}$ by [Raz85], which also implied a $n^{\Omega(\log n)}$ monotone arithmetic circuit lower bound for the Permanent polynomial over $\mathbb{B}$. Before this improvement, [Juk14] posed the question whether HC is a monotone p-projection of the Permanent. If the answer were yes, then we would get a $2^{n^{\Omega(1)}}$ monotone arithmetic circuit lower bound for the Permanent polynomial over $\mathbb{B}$, because the Clique polynomial family is a monotone p-projection of HC [Val79]. However, the author of [Gro17] showed that HC is *not* a monotone p-projection of the Permanent over $\mathbb{B}$, $\mathbb{R}$ and other semi-rings, which also shows that the Permanent is *not* VNP-complete under monotone p-projections over $\mathbb{R}^{\geq 0}$ for polynomials with non-negative coefficients.[13] It is *unknown* whether HC is VNP-complete under monotone p-projections over $\mathbb{R}$ for such polynomials.

The lower bounds established by [JS82] for the Permanent polynomial and HC_n also hold over the tropical semi-rings $(\mathbb{R}, \min, +, +\infty, 0)$ and $(\mathbb{R}^{\geq 0}, \min, +, +\infty, 0)$. Circuits over tropical semi-rings are called tropical circuits. The author of [Juk15] studied tropical circuits, motivated by the observation that many dynamic programming algorithms correspond to tropical circuits over tropical semi-rings. He showed that the power of tropical circuits lies between that of monotone Boolean circuits and monotone arithmetic circuits, and also showed $2^{\Omega(n)}$ tropical circuit lower bounds for the Permanent and HC_n, among other polynomials, over the tropical semi-rings $(\mathbb{N}, \min, +, +\infty, 0)$ and $(\mathbb{N}, \max, +, 0, 0)$, where the former is a proper sub semi-ring of $(\mathbb{R}, \min, +, +\infty, 0)$.

In [Mal03], the classes VP^0 and VNP^0 were defined using constant-free circuits, where the only constants that appear as inputs are 1, 0 or -1. In the work, HC was shown to be VNP^0-complete, which also

[10] An n-variate polynomial $f(\mathbf{x})$ is a p-projection of m-variate $g(\mathbf{y})$ if $m = n^{O(1)}$ and there exists a mapping $\phi : \mathbf{y} \mapsto \mathbb{F} \sqcup \mathbf{x}$ such that $g(\phi(\mathbf{y})) = f(\mathbf{x})$. The projection is monotone if the scalars lie in $\mathbb{F}^{\geq 0}$, the set of non-negative elements of $\mathbb{F}$.

[11] A semi-ring $(S, +, \times, 0, 1)$ comprises a set S such that $(S, +, 0)$ and $(S, \times, 1)$ are commutative monoids, $\times$ distributes over $+$, and $a \times 0$ is 0 for all $a \in S$.

[12] An n-variate monotone Boolean function $f(\mathbf{x})$ is a monotone-projection of the m-variate monotone Boolean function $g(\mathbf{y})$ if there exists a mapping $\phi : \mathbf{y} \mapsto \{0,1\} \sqcup \mathbf{x}$ such that $g(\phi(\mathbf{y})) = f(\mathbf{x})$.

[13] Later, [MS18] showed that even the Clique polynomial is not a monotone affine projection of the Permanent polynomial.

implies HC is VNP-complete over *any* ring. The VP^0 vs VNP^0 question (equivalently, is HC in VP^0?) is connected to the τ-conjecture concerning the number of integer roots of univariate integer polynomials, see [Bür24] for an overview. With this context, showing VP $\neq$ VNP (Valiant's conjecture) implies a superpolynomial lower bound on the determinantal complexity of the Permanent polynomial, and $\mathrm{VP}^0 \neq \mathrm{VNP}^0$ will show a superpolynomial lower bound on the binary determinantal complexity of HC_n.[14] Table 3 shows that the Permanent polynomial has a quadratic determinantal complexity lower bound, while for HC_n *no* such lower bound is known.

Usefulness of HC as a VNP-complete family. In various works [Mal07, KPTT15, GMQ16, IM18, IS22], HC has been the primary choice of a VNP-complete family over all fields for generalizing results to all fields.[15] The author of [Hru16] noted the lack of VNP-complete families over characteristic 2 fields and showed VNP-completeness of multiple graph-based polynomial families over such fields. He used HC to show the completeness of Clique* polynomial family, a variant of the Clique polynomial family known to be VNP-complete over fields of characteristic other than 2 [Bür00], over characteristic 2 fields. He then showed that four other graph-based polynomial families are VNP-complete over all fields using the Clique* polynomial family. Thus, the VNP-completeness of all five polynomial families relies on that of HC.

In [DRS24], the authors used HC to show that a variant of the monomial prediction problem, where in this variant the input polynomial is a composition of "easy" functions, is $\oplus$P-complete over finite fields and NP-hard over $\mathbb{Z}$. The motivation for studying this variant comes from cryptography. They also adapt the proof to show the #P-completeness of a problem motivated by machine learning.

C Missing Proofs from Section 3

C.1 Proof of Proposition 3.1

We prove the forward direction first. If $A \in \mathfrak{g}_{HC_n}$, then, by definition, A satisfies

$$\sum_{\substack{i_1,j_1,i_2,j_2 \in [n],\\ i_1 \neq j_1, i_2 \neq j_2}} A_{(i_1,j_1),(i_2,j_2)} x_{i_2,j_2} \frac{\partial HC_n}{\partial x_{i_1,j_1}} = 0. \tag{4}$$

Let $m_\sigma := \prod_{i\in[n]} x_{i,\sigma(i)}$ for all $\sigma \in C_n$. By linearity of the derivative operator, it suffices to analyse the monomials generated from m_σ in (4). For any σ, we have that,

$$x_{i_1,j_1} \frac{\partial m_\sigma}{\partial x_{i_2,j_2}} = x_{i_3,j_3} \frac{\partial m_\sigma}{\partial x_{i_4,j_4}} \iff (i_1,j_1) = (i_2,j_2) \text{ and } (i_3,j_3) = (i_4,j_4). \tag{5}$$

assuming $(i_2,j_2) \neq (i_4,j_4)$ and the derivatives are non-zero. From Observation 3.1, we get that the coefficient of the monomial $x_{i_1,j_1}\frac{\partial m_\sigma}{\partial x_{i_2,j_2}}$, where $(i_1,j_1) \neq (i_2,j_2)$ and $j_2 = \sigma(i_2)$, in (4) is just $A_{(i_1,j_1),(i_2,j_2)}$. From (5) and Observation 3.1, the coefficient of m_σ is $\sum_{i\in[n]} A_{(i,\sigma(i)),(i,\sigma(i))}$. Thus, we get that all the off-diagonal entries $A_{(i_1,j_1),(i_2,j_2)}$ are 0 while the diagonal entries $A_{(i,j),(i,j)}$ satisfy

$$\sum_{i\in[n]} A_{(i,\sigma(i)),(i,\sigma(i))} = 0 \quad \forall \sigma \in C_n.$$

The reverse direction can be verified easily by using Observation 3.1 and the condition in (5).

[14] The determinantal complexity of a polynomial f, $\mathrm{dc}(f)$, is the smallest $m \in \mathbb{N}$ such that $f = det(M)$, where M is a $m \times m$ matrix with entries as affine forms. The binary determinantal complexity, $\mathrm{bdc}(f)$, is defined similarly, with M being a matrix with entries as 0, 1 or variables. Clearly, $\mathrm{bdc}(f) \geq \mathrm{dc}(f)$.

[15] In [GMQ16], the authors work over algebraically closed fields, and using HC, their result generalizes to all closed fields.

C.2 Proof of Observation 3.1

We assume throughout the proof that the derivatives we consider are non-zero. For $n = 3$, $|C_3| = 2$ with $\sigma_1 = (1\,2\,3)$ and $\sigma_2 = (1\,2\,3)$. Then, we have

$$x_{i_1,j_1}\frac{\partial x_{1,2}x_{2,3}x_{3,1}}{\partial x_{i_2,j_2}} = x_{i_3,j_3}\frac{\partial x_{1,3}x_{3,2}x_{2,1}}{\partial x_{i_3,j_3}}$$
$$\iff x_{i_1,j_1}x_{i_4,j_4}x_{1,2}x_{2,3}x_{3,1} = x_{i_2,j_2}x_{i_3,j_3}x_{1,3}x_{3,2}x_{2,1}.$$

It can be verified that the last equality cannot hold for any choice of $x_{i,j}$ variables, proving the observation statement for $n = 3$. Now assume $n > 3$. As $\sigma_1 \neq \sigma_2$, by Claim 3.1, there exists $S = \{k_1, k_2, k_3\} \subseteq [n]$ such that $\sigma_1(k_\ell) \neq \sigma_2(k_\ell)$ where $\ell \in [3]$. Consider the following cases:

1. $i_2 \in S$ and $i_4 \in S$: In this case, we have that

$$x_{i_1,j_1}\frac{\partial m_{\sigma_1}}{\partial x_{i_2,j_2}} = x_{i_1,j_1}\frac{\prod_{i\in S} x_{i,\sigma_1(i)}}{x_{i_2,j_2}}\prod_{i\notin S} x_{i,\sigma_1(i)}$$

   and

$$x_{i_3,j_3}\frac{\partial m_{\sigma_2}}{\partial x_{i_4,j_4}} = x_{i_3,j_3}\frac{\prod_{i\in S} x_{i,\sigma_2(i)}}{x_{i_4,j_4}}\prod_{i\notin S} x_{i,\sigma_2(i)}$$

2. $i_2 \in S$ and $i_4 \notin S$: In this case we have,

$$x_{i_1,j_1}\frac{\partial m_{\sigma_1}}{\partial x_{i_2,j_2}} = x_{i_1,j_1}\frac{\prod_{i\in S} x_{i,\sigma_1(i)}}{x_{i_2,j_2}}\prod_{i\notin S} x_{i,\sigma_1(i)}$$

   and

$$x_{i_3,j_3}\frac{\partial m_{\sigma_2}}{\partial x_{i_4,j_4}} = x_{i_3,j_3}\prod_{i\in S} x_{i,\sigma_2(i)}\frac{\prod_{i\notin S} x_{i,\sigma_2(i)}}{x_{i_4,j_4}}$$

   Note that the case $i_2 \notin S$ and $i_4 \in S$ is the same as this case with the appropriate changes in the resulting monomials.

3. $i_2 \notin S$ and $i_4 \notin S$

$$x_{i_1,j_1}\frac{\partial m_{\sigma_1}}{\partial x_{i_2,j_2}} = x_{i_1,j_1}\prod_{i\in S} x_{i,\sigma_1(i)}\frac{\prod_{i\notin S} x_{i,\sigma_1(i)}}{x_{i_2,j_2}}$$

   and

$$x_{i_3,j_3}\frac{\partial m_{\sigma_2}}{\partial x_{i_4,j_4}} = x_{i_3,j_3}\prod_{i\in S} x_{i,\sigma_2(i)}\frac{\prod_{i\notin S} x_{i,\sigma_2(i)}}{x_{i_4,j_4}}$$

   By the unique factorization theorem for multivariate polynomials, if the resulting monomials were equal, then their factors must be the same. However, as $|S| = 3$, it is not hard to observe in all of the above cases that regardless of the choice of x_{i_3,j_3}, there will always exist a $k \in S$, such that $x_{k,\sigma_1(k)}$ is not divisible by any $x_{\ell,\sigma_2(\ell)}$ for $\ell \in [n]$ or x_{i_3,j_3}. Similarly, regardless of any choice of x_{i_1,j_1}, there exists a $k' \in S$ such that $x_{k',\sigma_2(k')}$ is not divisible by any $x_{\ell,\sigma_1(\ell)}$ for $\ell \in [n]$ or x_{i_1,j_1}.

C.3 Proof of Claim 3.1

For $n = 3$, there are only two cyclic permutations $(1\ 2\ 3)$ and $(1\ 3\ 2)$. It is then easy to see that the claim holds for $n = 3$ with $S = \{1, 2, 3\}$. Hence, we assume $n \geq 4$. As $\sigma_1 \neq \sigma_2$ and both are n-cycles, we can write σ_1 and σ_2 as

$$\sigma_1 : (1\ m_1\ m_2\ \ldots\ m_i\ m_{i+1}\ \ldots\ m_n),$$
$$\sigma_2 : (1\ m_1\ m_2\ \ldots\ m_i\ m'_{i+1}\ \ldots\ m'_n),$$

where $i < n-1$ (otherwise $\sigma_1 = \sigma_2$), $m_j = \sigma_1^{j-1}(1)$ for $j \in [n]$, $m'_j = \sigma_2^{j-1}(1)$ for $j \in [i+1, n]$, with $m'_{i+1} \neq m_{i+1}$ while $m'_j = m_j$ for all $j \in [i]$. Thus, $\sigma_1(m_i) \neq \sigma_2(m_i)$.

As σ_2 is an n-cycle, there exists $k_2 \in [i+1, n-1]$ such that $\sigma_2(m'_{k_2}) = m_{i+1}$. As σ_1 is an n-cycle, there exists $k_1 \in [i+2, n]$ such that $m_{k_1} = m'_{k_2}$ and $\sigma_1(m_{k_1}) \neq m_{i+1}$. Thus, $\sigma_1(m_{k_1}) \neq \sigma_2(m_{k_1})$.

We now further leverage the fact that σ_1, σ_2 are n-cycles to find an m_j such that $\sigma_1(m_j) \neq \sigma_2(m_j)$. Consider the following cases:

1. $m'_{i+1} \neq m_{k_1+1}$: This implies $\sigma_1(m_{k_1}) \neq m'_{i+1}$. As σ_1 and σ_2 are permutations, there exists a $j_1 \in [i+1, n-1] \backslash \{k_1\}$ such that $\sigma_1(m_{j_1}) = m'_{i+1}$ and $\sigma_2(m_{j_1}) \neq m'_{i+1}$.
2. $m'_{i+1} = m_{k_1+1}$: In this case, we show that there exists a $j_1 \in [i+1, k_1-1]$ such that $\sigma_1(m_{j_1}) \neq \sigma_2(m_{j_1})$. Suppose to the contrary that there did not exist such a j_1, then $\sigma_1(m_j) = \sigma_2(m_j)$ for all $j \in [i+1, k_1-1]$. Since $m'_{k_2+1} = \sigma_2(m'_{k_2}) = m_{i+1}$, we also get from the previous assumption that $m_{i+j} = m'_{k_2+j}$ for $j \in [1, k_1 - i]$. Based on this, we have the following subcases, each of which leads to a contradiction. Thus, the claimed j_1 exists.
   (a) $k_1 - i > n - k_2$: Taking $j = n - k_2 + 1$, we get that $m_{i+n-k_2+1} = m'_{k_2+n-k_2+1} = 1$. This implies $\sigma_1^{i+n-k_2}(1) = 1$ and hence $i = k_2 \mod n$, a contradiction as $i < k_2 < n$.
   (b) $k_1 - i < n - k_2$: Taking $j = k_1 - i$, we get that $m'_{k_2+k_1-i} = m_{k_1}$. As $m_{k_1} = m'_{k_2}$, we get that, $m'_{k_2+k_1-i} = m'_{k_2}$. This implies $\sigma_2^{k_2+k_1-i-1}(1) = \sigma_2^{k_2-1}(1)$ and hence $i = k_1 \mod n$, a contradiction as $0 < k_1 - i < n$.
   (c) $k_1 - i = n - k_2$: Taking $j = k_1 - i$, we get that $m_{i+k_1-i} = m'_{k_2+k_1-i}$ implying $m_{k_1} = m'_{k_2+k_1-i} = m'_{k_2+n-k_2} = m'_n$. Thus, we get that $m'_n = m_{k_1} = m'_{k_2}$, a contradiction as $0 < k_2 < n$.

Take S to be $\{m_i, m_{k_1}, m_{j_1}\}$.

C.4 Proof of Proposition 3.2

Define the matrix $M^{HC_n} \in \mathbb{F}^{(n-1)! \times (n^2-n)}$, with rows indexed by $\sigma \in C_n$ and columns by (i, j) in lexicographic order of the variables $x_{i,j}$, as

$$M^{HC_n}_{(\sigma,(i,j))} = \begin{cases} 1 & \sigma(i) = j, \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

where $\sigma \in C_n$. The matrix M^{HC_n} represents the system of linear equations described by Proposition 3.1, and hence its nullspace is $\mathfrak{g}_{HC_n}$. We analyse M^{HC_n} for $n \neq 4$ here to show the set $\mathscr{B}_n$ as described in the proposition statement is a basis for $\mathfrak{g}_{HC_n}$. For $n = 3$, M^{HC_3} is as in (7).

$$\begin{array}{c} \\ (1,2,3) \\ (1,3,2) \end{array} \begin{array}{c} \begin{array}{cccccc} (1,2) & (1,3) & (2,1) & (2,3) & (3,1) & (3,2) \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array} \tag{7}$$

Clearly, M^{HC_3} is full row rank over any $\mathbb{F}$. Hence, $\dim(\mathfrak{g}_{HC_3}) = 4$ over any $\mathbb{F}$. The set $\mathscr{B}_3$ described in the proposition statement can be easily verified to lie in $\mathfrak{g}_{HC_3}$. Stacking the elements of $\mathscr{B}_3$ together, we get the following matrix

$$\begin{array}{c} \\ (1,2) \\ (1,3) \\ (2,1) \\ (2,3) \\ (3,1) \\ (3,2) \end{array} \begin{array}{c} \begin{array}{cccc} A^{(2)} & A^{(3)} & B^{(2)} & C \end{array} \\ \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & -1 \\ -1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \end{pmatrix} \end{array} \tag{8}$$

It can be easily verified that the matrix in (8) has rank 4 by noting that the submatrix indexed by the first four rows has determinant 1, proving the statement for $n = 3$. Now, we assume $n \geq 5$. Note that for any $\sigma \in C_n$, $k \in [2, n]$ and $\ell \in [2, n-1]$, we have

$$\sum_{i=1}^{n} A^{(k)}_{(i,\sigma(i))} = A^{(k)}_{(1,\sigma(1))} + A^{(k)}_{(k,\sigma(k))} = 1 - 1 = 0,$$

$$\sum_{i=1}^{n} B^{(\ell)}_{(i,\sigma(i))} = B^{(\ell)}_{(\sigma^{-1}(1),1)} + B^{(\ell)}_{(\sigma^{-1}(\ell),\ell)} = 1 - 1 = 0 \text{ and}$$

$$\sum_{i=1}^{n} C_{(i,\sigma(i))} = C_{(2,\sigma(2))} + C_{(\sigma^{-1}(2),2)} = -1 + 1 = 0.$$

Thus, $\mathscr{B}_n \subset \mathfrak{g}_{HC_n}$. We now show that $\mathscr{B}_n$ is $\mathbb{F}$-linearly independent, implying $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_n}) \geq 2n - 2$. Let $M \in \mathbb{F}^{(n^2-n)\times(2n-2)}$ be the matrix formed by stacking the elements of $\mathscr{B}_n$ as columns, and let R be the set

$$R = \{(1, j) \mid j \in [2, n-1]\} \sqcup \{(2, 3)\} \sqcup \{(i, 1) \mid i \in [2, n-1]\} \sqcup \{(1, n)\}.$$

Then, upto reordering of rows, the submatrix $M_{R\times\bullet}$ is as follows

$$\begin{array}{c} \\ (1,2) \\ (1,3) \\ \vdots \\ (1,n-1) \\ (2,3) \\ (2,1) \\ (3,1) \\ \vdots \\ (n-1,1) \\ (1,n) \end{array} \begin{array}{c} \begin{array}{ccccc|ccccc} A^{(2)} & A^{(3)} & \dots & A^{(n-1)} & A^{(n)} & B^{(2)} & B^{(3)} & \dots & B^{(n-1)} & C \end{array} \\ \left(\begin{array}{ccccc|ccccc} 1 & 1 & \dots & 1 & 1 & -1 & 0 & \dots & 0 & 1 \\ 1 & 1 & \dots & 1 & 1 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \dots & 1 & 1 & 0 & 0 & \dots & -1 & 0 \\ -1 & 0 & \dots & 0 & 0 & 0 & -1 & \dots & 0 & -1 \\ \hline -1 & 0 & \dots & 0 & 0 & 1 & 1 & \dots & 1 & -1 \\ 0 & -1 & \dots & 0 & 0 & 1 & 1 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & 0 & 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & \dots & 1 & 1 & 0 & 0 & \dots & 0 & 0 \end{array}\right) \end{array} \tag{9}$$

We show that $det(M_{R\times\bullet}) = \pm 1$. On $M_{R\times\bullet}$, apply the elementary row operations $R_i \mapsto R_i - R_{2n-2}$, where R_i refers to the i'th row, for all $i \in [1, n-2]$ and $R_{n-1} \mapsto R_{n-1} - R_n$ to get the following matrix:

$$
\begin{array}{c|c|ccccc|ccccc|}
 & A^{(2)} & A^{(3)} & \dots & A^{(n-1)} & A^{(n)} & B^{(2)} & B^{(3)} & \dots & B^{(n-1)} & C \\
(1,2) & 0 & 0 & \dots & 0 & 0 & -1 & 0 & \dots & 0 & 1 \\
(1,3) & 0 & 0 & \dots & 0 & 0 & 0 & -1 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(1,n-1) & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & -1 & 0 \\
(2,3) & 0 & 0 & \dots & 0 & 0 & -1 & -2 & \dots & -1 & 0 \\
\hline
(2,1) & -1 & 0 & \dots & 0 & 0 & 1 & 1 & \dots & 1 & -1 \\
(3,1) & 0 & -1 & \dots & 0 & 0 & 1 & 1 & \dots & 1 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(n-1,1) & 0 & 0 & \dots & -1 & 0 & 1 & 1 & \dots & 1 & 0 \\
(1,n) & 1 & 1 & \dots & 1 & 1 & 0 & 0 & \dots & 0 & 0
\end{array}
$$

As the resulting matrix is block triangular, $det(M_{R\times\bullet})$ is, up to a sign, the product of the determinants of the lower-left block matrix and the upper-right block matrix in the above matrix. It is easily verified that the lower-left block matrix has determinant $(-1)^{n-2}$, while the upper-right block matrix has determinant $(-1)^{n-1}$. Hence, $det(M_{R\times\bullet}) = \pm 1$ and $\mathscr{B}_n$ is $\mathbb{F}$-linearly independent.

Proposition C.1 shows a rank lower bound of $(n-1)(n-2)$ for M^{HC_n} implying, by the Rank-Nullity Theorem, that $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_n}) \leq 2n-2$, proving $\mathscr{B}_n$ is a basis and hence Proposition 3.2. Note that Proposition C.1 also shows how to efficiently construct a row basis $M^{(n)}$ of M^{HC_n}, which we leverage in Algorithm 4. For $n = 3$, we have $M^{(3)} = M^{HC_3}$.

Proposition C.1. Let $n \geq 5$. We can construct in time $n^{O(1)}$ a submatrix $M^{(n)} \in \mathbb{F}^{(n-1)(n-2)\times(n^2-n)}$ of M^{HC_n} such that $M^{(n)}$ contains a $(n-1)(n-2)\times(n-1)(n-2)$ submatrix with determinant ± 1.

Proof. This will be a proof by induction on n.

Base case. For $n = 5$, let R be the following set of 5-cycles

$$R = \{(1\,2\,3\,4\,5), (1\,3\,2\,4\,5), (1\,4\,2\,3\,5), (1\,5\,2\,3\,4), (1\,3\,4\,5\,2), (1\,2\,4\,3\,5),$$

$$(1\,2\,5\,3\,4), (1\,2\,4\,5\,3), (1\,3\,4\,2\,5), (1\,2\,3\,5\,4), (1\,3\,2\,5\,4), (1\,3\,5\,2\,4).\}$$

Then, we set $M^{(5)} = M^{HC_5}_{R\times\bullet}$, where each row is indexed by a permutation $\sigma \in R$ and column by (i,j), corresponding to the variable $x_{i,j}$, ordered lexicographically.

$$
\begin{array}{c|cccc|cccc|cccc|cccc|cccc|}
(1\,2\,3\,4\,5) & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
(1\,3\,2\,4\,5) & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
(1\,4\,2\,3\,5) & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
(1\,5\,2\,3\,4) & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
(1\,3\,4\,5\,2) & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
(1\,2\,4\,3\,5) & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
(1\,2\,5\,3\,4) & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
(1\,2\,4\,5\,3) & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
\hline
(1\,3\,4\,2\,5) & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
(1\,2\,3\,5\,4) & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
(1\,3\,2\,5\,4) & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
(1\,3\,5\,2\,4) & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0
\end{array}
\tag{10}
$$

By Gaussian elimination, it can be verified that $M^{(5)}$ has full row rank (see (11)). Moreover, the pivot entries are ± 1, hence $M^{(5)}$ has a submatrix with determinant ± 1.

$$
\begin{array}{c}
(1\,2\,3\,4\,5) \\
(1\,3\,2\,4\,5) \\
(1\,4\,2\,3\,5) \\
(1\,5\,2\,3\,4) \\
(1\,3\,4\,5\,2) \\
(1\,2\,4\,3\,5) \\
(1\,2\,5\,3\,4) \\
(1\,2\,4\,5\,3) \\
(1\,3\,4\,2\,5) \\
(1\,2\,3\,5\,4) \\
(1\,3\,2\,5\,4) \\
(1\,3\,5\,2\,4)
\end{array}
\left(\begin{array}{cccc|cccc|cccc|cccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & -1 & 1 & 1 & -2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & -1 & 1 & 1 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 3 & -2 & 1 & 1 & -2 & 1 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & -1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 & 1 & -1 & 0 & 1 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 1 & 0 & -1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0
\end{array}\right) \tag{11}
$$

Inductive hypothesis. Suppose that we can construct $M^{(n-1)}$ in $O((n-1)^5)$ time, where $n > 5$. By Claim C.1, which we prove later, we can extend $M^{(n-1)}$ to a submatrix of M^{HC_n}. Thus, we treat $M^{(n-1)}$ as a $(n-2)(n-3) \times (n^2-n)$ submatrix of M^{HC_n}.

Claim C.1. Let $n \geq 3$ and $R' = \{\sigma \in C_n |\ \sigma(1) = 2\}$ and $T = \{(i,j) |\ i \neq 1, j \neq 2 \text{ and } (i,j) \neq (2,1)\}$. Then $M^{HC_n}_{R' \times T} = M^{HC_{n-1}}$. In particular, $M^{(n-1)}$ can be extended to a submatrix M' of M^{HC_n} in $O(n^4)$ time such that M' has a $(n-2)(n-3) \times (n-2)(n-3)$ submatrix with determinant ± 1.

Now, let $R_1 = \{\tau_3, \tau_4, \ldots, \tau_{n-1}, \tau_n\} \subseteq C_n$ such that for $i \in [3,n]$, $\tau_i(1) = i$, $\tau_i(2) \neq 1$ and $\tau_i(n) = 2$. Let $R_2 = \{\sigma_3, \sigma_4, \ldots, \sigma_{n-1}, \sigma_n\} \subseteq C_n$ such that for $i \in [3, n-2]$, $\sigma_i(1) = i$, $\sigma_i(i+1) = 2$ and $\sigma_i(2) = 1$, $\sigma_{n-1}(1) = n-1$, $\sigma_{n-1}(2) = 1$, $\sigma_{n-1}(3) = 2$, and $\sigma_n(1) = n$, $\sigma_n(2) \neq 1$, $\sigma_n(3) = 2$. Note that $|R_1| = |R_2| = n-2$ and $n > 5$ ensures R_1 and R_2 exist. An explicit choice of R_1 and R_2, which can be constructed in $O(n^2)$ time, is as follows

$$
\begin{aligned}
R_1 = \{&(1\,3\,n\,2\,n-1\,n-2\,\ldots\,7\,6\,5\,4), \\
&(1\,4\,n\,2\,n-1\,n-2\,\ldots\,7\,6\,5\,3), \\
&(1\,5\,n\,2\,n-1\,n-2\,\ldots\,7\,6\,4\,3), \\
&(1\,6\,n\,2\,n-1\,n-2\,\ldots\,7\,5\,4\,3), \\
&\vdots \\
&(1\,n-3\,n\,2\,n-1\,n-2\,\ldots\,6\,5\,4\,3), \\
&(1\,n-2\,n\,2\,n-1\,n-3\,\ldots\,6\,5\,4\,3), \\
&(1\,n-1\,n\,2\,n-2\,n-3\,\ldots\,6\,5\,4\,3), \\
&(1\,n\,2\,n-1\,n-2\,n-3\,\ldots\,6\,5\,4\,3)\}
\end{aligned} \tag{12}
$$

$$
\begin{aligned}
R_2 = \{&(1\,3\,n\,n-1\,n-2\,\ldots\,7\,6\,5\,4\,2),\\
&(1\,4\,n\,n-1\,n-2\,\ldots\,7\,6\,3\,5\,2),\\
&(1\,5\,n\,n-1\,n-2\,\ldots\,7\,4\,3\,6\,2),\\
&(1\,6\,n\,n-1\,n-2\,\ldots\,5\,4\,3\,7\,2),\\
&\vdots\\
&(1\,n-3\,n\,n-1\,n-4\,\ldots\,5\,4\,3\,n-2\,2),\\
&(1\,n-2\,n\,n-3\,n-4\,\ldots\,5\,4\,3\,n-1\,2),\\
&(1\,n-1\,n\,n-2\,n-3\,\ldots\,6\,5\,4\,3\,2),\\
&(1\,n\,3\,2\,n-1\,n-2\,\ldots\,7\,6\,5\,4)\}
\end{aligned}
\tag{13}
$$

Consider the matrix $M^{(n)} = M^{HC_n}_{\tilde{R}\times\tilde{T}}$, where $\tilde{R} = R \sqcup R_1 \sqcup R_2$ with R as the set of permutations in C_n corresponding to the rows of $M^{(n-1)}$, R_1 as in (12) and R_2 as in (13), and $\tilde{T} = T \sqcup T_1 \sqcup T_2$ with T as per Claim C.1, $T_1 = \{(1,j) \mid j \in [3,n]\}$ and $T_2 = \{(2,1)\} \sqcup \{(i,2) \mid i \in [3,n]\}$. The matrix $M^{(n)}$ is as:

$$
M^{(n)} = \begin{array}{c} \\ R \\ R_1 \sqcup R_2 \end{array}
\begin{array}{c} \begin{array}{cc} T & T_1 \sqcup T_2 \end{array} \\
\left(\begin{array}{c|c} M^{(n-1)} & 0_{(n-2)(n-3)\times(2n-3)} \\ \hline B & C \end{array}\right) \end{array}
\tag{14}
$$

where $C \in \mathbb{F}^{(2n-4)\times(2n-3)}$ is a $0/1$ matrix. Claim C.1 ensures that $M^{(n-1)}$ has only zero entries corresponding to the columns indexed by $T_1 \sqcup T_2$. By the inductive hypothesis, there exists a $(n-2)(n-3) \times (n-2)(n-3)$ submatrix N of $M^{(n-1)}$ such that $det(N) = \pm 1$. Let $T' \subset T$ be the set of $(n-2)(n-3)$ columns, such that $N = M^{(n-1)}_{\bullet\times T'}$. Let $C' = C_{\bullet\times T_1 \sqcup (T_2\setminus\{(n,2)\})}$. Note that C' is a $(2n-4) \times (2n-4)$ matrix. Since $M^{(n)}$ is block-diagonal, we get that

$$
det(M^{(n)}_{\bullet\times T'\sqcup T_1\sqcup(T_2\setminus\{(n,2)\})}) = det(N) \cdot det(C').
$$

The matrix C', up to a reordering of rows and columns, is as in (15), where the columns are ordered lexicographically with respect to the elements of $T_1 \sqcup (T_2\setminus\{(n,2)\})$.

$$
C = \begin{array}{c}
\\
\tau_3 \\ \tau_4 \\ \vdots \\ \tau_{n-2} \\ \tau_{n-1} \\ \tau_n \\
\sigma_3 \\ \sigma_4 \\ \vdots \\ \sigma_{n-2} \\ \sigma_{n-1} \\ \sigma_n
\end{array}
\begin{array}{c}
\begin{array}{ccccccc|ccccccc}
(1,3) & & \ldots & & & (1,n) & (2,1) & (3,2) & (4,2) & & \ldots & & (n-1,2)
\end{array} \\
\left(\begin{array}{ccccccc|ccccccc}
1 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\
0 & 0 & \ldots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\
0 & 0 & \ldots & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\ \hline
1 & 0 & \ldots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & 1 & 0 & 0 & 0 & \ldots & 0 & 1 \\
0 & 0 & \ldots & 0 & 1 & 0 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 0 & \ldots & 0 & 0 & 1 & 0 & 1 & 0 & 0 & \ldots & 0 & 0
\end{array}\right)
\end{array}
\tag{15}
$$

It is then not hard to see that $det(C) = \pm 1$. Since $det(N) = \pm 1$, this completes the inductive step.

The entire argument can be converted to a recursive algorithm to compute $M^{(n)}$ in $O(n^5)$ time. The matrix $M^{(5)}$ in (10) is the matrix for $n = 5$, the base case. By using Claim C.1 we can map an already

constructed $M^{(n-1)}$ to an $(n-2)(n-3) \times (n^2-n)$ matrix in $O(n^4)$ time. The rows corresponding to the sets in (12) and (13) can then be added to the resulting matrix in $O(n^4)$ time to get $M^{(n)}$. Since the recursion runs for $O(n)$ many steps and each step needs $O(n^4)$ time, $M^{(n)}$ can be consturcted in $O(n^5)$ time. □

Proof of Claim C.1. We first show an injective map $\phi_2 : C_{n-1} \to C_n$ which maps $\pi \in C_{n-1}$ to a $\sigma \in C_n$ such that $\sigma(1) = 2$. Let $\pi \in C_{n-1}$ where $\pi = (1\ j_1\ j_2\ \dots\ j_{n-2})$ with $j_i = \pi^i(1)$, $i \in [n-2]$. Then ϕ_2 acts as follows:

$$\phi_2 : (1\ j_1\ j_2\ \dots\ j_{n-2}) \mapsto (1\ 2\ j_1+1\ j_2+1\ \dots\ j_{n-2}+1).$$

Formally, $\sigma = \phi_2(\pi)$ is defined as

$$\sigma(1) = 2,\ \sigma(i+1) = \pi(i)+1 \text{ and } \sigma(k+1) = 1.$$

where $i, k \in [n-1]$ and $\pi(k) = 1$. Clearly, σ is an n-cycle. We show ϕ_2 is injective.

Suppose $\pi_1, \pi_2 \in C_{n-1}$ such that their respective images σ_1 and σ_2 under ϕ_2 satisfy $\sigma_1 = \sigma_2$. Thus, $\sigma_1(i) = \sigma_2(i)$ for all $i \in [n]$. Let $\pi_1(k) = 1$ with $k \in [2, n-1]$, then from the definition of ϕ_2, and $\sigma_2 = \sigma_1$, we get that $\sigma_2(k+1) = \sigma_1(k+1) = 1$. This implies $\pi_2(k) = 1$, for otherwise $\sigma_2(k+1) = \pi_2(k)+1 \neq 1$ a contradiction. We also have that for all $i \in [n-1]\backslash\{k\}$, $\sigma_2(i+1) = \sigma_1(i+1) = \pi_1(i)+1$. Since $\sigma_2(i+1) = \pi_2(i)+1$, we get that $\pi_1(i)+1 = \pi_2(i)+1$ or $\pi_1(i) = \pi_2(i)$ for all $i \in [n-1]\backslash\{k\}$. Thus, $\pi_1 = \pi_2$.

Hence, ϕ_2 is injective into C_n. Since ϕ_2 is injective, it is a bijection from $C_{n-1} \to R'$, where R', as in the claim statement, is the subset of C_n comprising n-cycles σ such that $\sigma(1) = 2$. Thus, the matrix $M^{HC_n}_{R' \times T}$ must be the same as $M^{HC_{n-1}}$. It is easy to see that we can compute $\phi_2(\pi)$ in $O(n)$ time for any $\pi \in C_{n-1}$ if we treat π as a list of length n. Thus, we can extend $M^{(n-1)}$ to a matrix with n^2-n columns in $O(n^4)$ time by using ϕ_2 to map each row of $M^{(n-1)}$ to a row of M^{HC_n}. Note that the rank of the extended matrix is at least $(n-2)(n-3)$. This is because under the action of ϕ_2 all the columns (i,j) and $(i,1)$ of $M^{(n-1)}$, where $i, j \in [n-1]$ with $j \neq 1$, map to $(i+1, j+1)$ and $(i+1, 1)$ respectively in the extended matrix. Thus, the structure of $M^{(n-1)}$ is preserved in the extended matrix, hence the rank is also at least $(n-2)(n-3)$. □

C.5 Proof of Corollary 3.1

Let T be the set

$$T = \{(i,j) |\ i, j \in [2,n],\ i \neq j, (i,j) \neq (2,3)\} \sqcup \{(n,1)\}.$$

Let T^c denote the complement of T. Note that $|T| = (n-1)(n-2)$.

From the equations in (2) form the matrix $N \in \mathbb{F}^{(n-1)(n-2)\times(n^2-n)}$ such that $N\mathbf{z} = 0$, with each row expressing $z_{i,j}$, where $(i,j) \in T$, in terms of $z_{k,\ell}$, where $(k,\ell) \in T^c$. The rows of N are indexed by $z_{i,j}$, while the columns are indexed by all $\mathbf{z}$ variables. Let the elements of T and T^c be ordered by lexicographic ordering. After reordering the rows of N in lexicographic order, N can be written as

$$\begin{array}{cc} T & T^c \\ (I_{(n-1)(n-2)} & \mid\ M), \end{array}$$

where $I_{(n-1)(n-2)}$ is the $(n-1)(n-2) \times (n-1)(n-2)$ identity matrix and row (i,j) of M corresponds to the linear form for $z_{i,j}$ in (2). Clearly, N has full row rank, and thus the dimension of the null space of N is $2n-2$. It is easily verifiable that the elements of $\mathscr{B}_n$ described in Proposition 3.2 satisfy the equations in (2), proving the corollary.

C.6 Further analysis of $M^{(n)}$

Lemma C.1 shows that a subset T of the columns of $M^{(n)}$ is such that $|T| = (n-1)(n-2)$ and $M^{(n)}_{\bullet \times T}$ has determinant ± 1. Lemma C.2, proved using Lemma C.1, is used to analyse the structure of the scaling

symmetries of HC_n over all fields. Lemma C.3, proved using Lemma C.2, shows that solving the system of linear equations represented by M^{HC_n} over an Abelian group reduces to solving the system of linear equations represented by $M^{(n)}$. Lemma C.3 is used to prove the correctness of Algorithm 4 over all fields.

Note that for Lemmas C.2 and C.3 we work over an Abelian group G, where we treat $+$ as the group operation, 0 as the group identity. For $g \in G$ and $k \in \mathbb{Z}^+$, kg means g added to itself k times, $(-k)g$ means $-g$, the inverse of g, added to itself k times, and $0g$ gives the group identity 0.

Lemma C.1. Let $\mathbb{F}$ be any field, $M^{(n)}$ be the matrix as constructed in the proof of Proposition 3.2 (See Proposition C.1). Then, $det(M^{(n)}_{\bullet \times T}) = \pm 1$, where T is as

$$T = \{(k,\ell) \mid (k,\ell) \neq (1,j),\ j \in [2,n] \text{ and } (k,\ell) \neq (i,1),\ i \in [2,n-1] \text{ and } (k,\ell) \neq (2,3)\}.$$

Proof. Consider the matrix N as constructed in Appendix C.5 and the matrix $M^{(n)}$ as constructed in Proposition C.1. Both $M^{(n)}$ and N are $(n-1)(n-2) \times (n^2-n)$ matrices. From the argument in Appendix C.5, it follows that both matrices also have the *same* nullspace over *any* $\mathbb{F}$. It then follows from a standard Linear Algebra result, see Section 2.5 in [HK71], that their row spaces must be the same. Thus, there exists $B \in \mathrm{GL}_{(n-1)(n-2)}(\mathbb{F})$ such that

$$BM^{(n)} = N$$

implying

$$BM^{(n)}_{\bullet \times T} = N_{\bullet \times T} = I_{(n-1)(n-2)}$$

where the last equality follows from the construction of N. Thus,

$$det(B)det(M^{(n)}_{\bullet \times T}) = 1$$

Now, M being a $0/1$ matrix implies $det(M^{(n)}_{\bullet \times T})$ is an integer. Since the above matrix product above holds over *any* $\mathbb{F}$, we get that $det(M^{(n)}_{\bullet \times T}) = \pm 1$ and $det(B) = \pm 1$. Further, if $M_1 = M^{(n)}_{\bullet \times T}$, then $B = M_1^{-1}$. Thus,

$$BM^{(n)} = N$$

can be written as

$$M_1^{-1} \,.\, (M_1 \mid M_2) = (I_{(n-1)(n-2)} \mid M)$$

In particular, we get that $-M_1^{-1}M_2$ produces the linear combination of $z_{i,j}$'s corresponding to the RHS of the equations in (2).

□

Lemma C.2. Let G be an Abelian group (equivalently a $\mathbb{Z}$-module) and $g_{i,j} \in G$, with $i,j \in [n]$ and $i \neq j$, such that $\sum_{i=1}^{n} g_{i,\sigma(i)} = 0$ holds for all $\sigma \in C_n$. Then, the $g_{i,j}$'s satisfy (2).

Proof. The system of linear equations in the statement can be written as $M^{HC_n}.\mathbf{g} = \mathbf{0}$ because the rows of M^{HC_n} correspond to such a system of linear equations. Now,

$$M^{HC_n}\mathbf{g} = \mathbf{0} \implies M^{(n)}\mathbf{g} = \mathbf{0}$$

because $M^{(n)}$, as constructed in Proposition C.1, contains a subset of the rows of M^{HC_n}. Note, now the number of equations is $(n-1)(n-2)$. We can write the system $M^{(n)}\mathbf{g} = \mathbf{0}$ as

$$(M_1 \mid M_2) \,.\, \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \end{pmatrix} = \mathbf{0},$$

where $M_1 = M^{(n)}_{\bullet \times T}$, where T is as in Lemma C.1, $M_2 = M^{(n)}_{\bullet \times T^c}$, where T^c is the complement of T, $\mathbf{g}_1$ are the entries $g_{i,j}$ with $(i,j) \in T$, and $\mathbf{g}_2$ are the remaining entries. We then get that

$$M_1 \mathbf{g}_1 + M_2 \mathbf{g}_2 = \mathbf{0}$$

Since M_1 is a $0/1$ matrix with $det(M_1) = \pm 1$, then M_1^{-1} is also an integer matrix. Thus, multiplying on the left by M_1^{-1} on both sides of the above equation is an invertible operation, which gives

$$\mathbf{g}_1 + M_1^{-1} M_2 \mathbf{g}_2 = \mathbf{0} \implies \mathbf{g}_1 = -M_1^{-1} M_2 \mathbf{g}_2.$$

From the proof of Lemma C.1, it follows that the matrix product $-M_1^{-1} M_2$ produces a linear combination of $\mathbf{g}_2$ entries which is exactly the same as the linear forms in the RHS of the equations in (2). Thus, we get that the $g_{i,j}$'s satisfy (2). □

Lemma C.3. Let G be an Abelian group such that

$$\sum_{i=1}^{n} x_{i,\sigma(i)} = h_\sigma \; \sigma \in C_n, \tag{16}$$

where $h_\sigma \in G$, has a solution. Then, any solution to

$$\sum_{i=1}^{n} x_{i,\sigma(i)} = h_\sigma \; \sigma \in R, \tag{17}$$

where R is the set permutations corresponding to rows of $M^{(n)}$, is also a solution to (16).

Proof. Let $\mathbf{u}$ be a solution to (16), which exists by assumption. Then $\mathbf{u}$ is also a solution to (17), since these equations are a subset of those of (16). Let $\mathbf{v}$ be a solution to (17). Then for $\sigma \in R$, we have that,

$$\sum_{i=1}^{n} (u_{i,\sigma(i)} - v_{i,\sigma(i)}) = \sum_{i=1}^{n} u_{i,\sigma(i)} - \sum_{i=1}^{n} v_{i,\sigma(i)} = h_\sigma - h_\sigma = 0.$$

where all equalities follow from the fact that G is Abelian. Thus, $\mathbf{u} - \mathbf{v}$ is a solution to $M^{(n)}.\mathbf{x} = \mathbf{0}$ which implies $\mathbf{u} - \mathbf{v}$ is also a solution to $M^{HC_n}.\mathbf{x} = \mathbf{0}$ by the proof of Lemma C.2. Now, note that

$$M^{HC_n}.\mathbf{v} = M^{HC_n}.(\mathbf{v} - \mathbf{u} + \mathbf{u}) =$$

$$M^{HC_n}.(\mathbf{v} - \mathbf{u}) + M^{HC_n}.\mathbf{u} = \mathbf{h}.$$

Here, $\mathbf{h}$ is the vector with entries as h_σ. The equalities follow from G being Abelian, the linearity of matrix operations, and the aforementioned observation about $\mathbf{u} - \mathbf{v}$. □

C.7 Proof of Lemma 3.1

Consider the matrix M as

$$M = \sum_{k=2}^{n} w_k A^{(k)} + \sum_{\ell=2}^{n-1} y_k B^{(\ell)} + zC$$

where w_k's, y_ℓ's and z are formal variables. Assuming $i \neq j$, the entries of M are as

$$M_{i,j} = \begin{cases} \sum_{k=2}^{n} w_k - y_2 + z & i = 1, j = 2 \\ \sum_{k=2}^{n} w_k - y_j & i = 1, j \in [3, n-1] \\ \sum_{k=2}^{n} w_k & i = 1, j = n \\ \sum_{\ell=2}^{n-1} y_\ell - w_2 - z & i = 2, j = 1 \\ -w_2 - y_j - z & i = 2, j \in [3, n-1] \\ -w_2 - z & i = 2, j = n \\ \sum_{\ell=2}^{n-1} y_\ell - w_i & i \in [3, n], j = 1 \\ -w_i - y_2 + z & i \in [3, n], j = 2 \\ -w_i - y_j & i \in [3, n], j \in [3, n-1], i \neq j \\ -w_i & i \in [3, n-1], j = n \end{cases}$$

It can be seen that all the entries of M are distinct linear polynomials, hence the difference of any two entries of M is a non-zero linear polynomial. Let $S \subseteq \mathbb{F}$, with $|S| > \binom{n^2-n}{2}$. Then, by the Polynomial Identity Lemma, for a random choice of the w_k's, y_ℓ's and z variables, two entries of M are the same with probability at most $\frac{1}{|S|}$. Applying union bound on all $\binom{n^2-n}{2}$ pairs of entries, we get that there exists a pair of equal entries in M with probability at most $\frac{\binom{n^2-n}{2}}{|S|} < 1$. Thus, with probability at least $1 - \frac{\binom{n^2-n}{2}}{|S|} > 0$, M has distinct diagonal entries. Hence, there exists an $M \in \mathfrak{g}_{HC_n}$ with distinct eigenvalues.

C.8 Proof of Proposition 3.3

Let $A \in \mathscr{G}_{HC_n}$, thus $HC_n(A\mathbf{x}) = HC_n(\mathbf{x})$ implying $\mathfrak{g}_{HC_n(A\mathbf{x})} = \mathfrak{g}_{HC_n}$. By the conjugacy of Lie Algebras of equivalent polynomials, Lemma 2.2, we also get that for every $B \in \mathfrak{g}_{HC_n(\mathbf{x})}$, there is a $C \in \mathfrak{g}_{HC_n}$ such that $B = A^{-1}CA$. Thus, $AB = CA$, with both B and C being diagonal matrices. Choose B to be a matrix where all the entries are distinct, which exists by Lemma 3.1. Consider the (i,j)'th row of A. As A is invertible, $A_{(i,j),(k,\ell)} \neq 0$ for some $k, \ell \in [n]$, $k \neq \ell$. Now, $AB = CA$ implies $(AB)_{((i,j),(k,\ell))} = (CA)_{((i,j),(k,\ell))}$. Thus,

$$A_{(i,j),(k,\ell)} B_{(k,\ell),(k,\ell)} = A_{(i,j),(k,\ell)} C_{(i,j),(i,j)}.$$

As $A_{(i,j),(k,\ell)} \neq 0$ we get $B_{(k,\ell),(k,\ell)} = C_{(i,j),(i,j)}$. Suppose $A_{(i,j),(k_1,\ell_1)} \neq 0$ for some $(k_1, \ell_1) \neq (k, \ell)$. Then, we also get that

$$A_{(i,j),(k_1,\ell_1)} B_{(k_1,\ell_1),(k_1,\ell_1)} = A_{(i,j),(k_1,\ell_1)} C_{(i,j),(i,j)},$$

implying

$$B_{(k,\ell_1),(k,\ell_1)} = C_{(i,j),(i,j)} = B_{(k,\ell),(k,\ell)},$$

a contradiction as all entries of B are distinct. Thus, every row of A has exactly one non-zero entry. Since A is invertible, it must be that $A = PS$ for some permutation P and scaling S.

C.9 Proof of Proposition 3.4

Let S be a scaling symmetry of HC_n. Then, we have that

$$\prod_{i=1}^{n} S_{i,\sigma(i)} = 1 \quad \forall \sigma \in C_n$$

This is a system of linear equations over the Abelian Group $\mathbb{F}^\times$, where we treat group multiplication as addition and 1 (multiplicative identity of $\mathbb{F}^\times$) as 0. Thus, we get that the above system of equations corresponds to

$$M^{HC_n}\mathbf{s} = \mathbf{0},$$

where the entries of $\mathbf{s}$ are the entries of S. By Lemma C.2, we get that the entries of S must satisfy the equations in (3), which are the multiplicative version of (2). Hence, S is a continuous scaling symmetry.

C.10 Proof of Proposition 3.5

Let $\pi \in C_n$. We can write π as $(1\ m_1\ m_2 \dots\ m_n)$. The monomial corresponding to π in HC_n is $\prod_{i\in[n]} x_{i,\pi(i)} = x_{1,m_1}x_{m_1,m_2}\dots x_{m_{n-1},m_n}x_{m_n,1}$. Under the action of $P^{(\sigma)}$, we have that

$$\prod_{i\in[n]} x_{i,\pi(i)} \mapsto \prod_{i\in[n]} x_{\sigma(i),\sigma(\pi(i))}.$$

Note

$$\prod_{i\in[n]} x_{\sigma(i),\sigma(\pi(i))} = x_{\sigma(1),\sigma(m_1)}x_{\sigma(m_1),\sigma(m_2)}\dots x_{\sigma(m_{n-1}),\sigma(m_n)}x_{\sigma(m_n),\sigma(1)}.$$

As $\sigma \in S_n$, the cycle π maps uniquely to $\tau = (\sigma(1)\ \sigma(m_1)\ \sigma(m_2)\dots\ \sigma(m_n))$. Hence $P^{(\sigma)}$ is a permutation symmetry of HC_n. Now we consider $P^{(T)}$. Under the action of $P^{(T)}$, we have

$$\prod_{i\in[n]} x_{i,\pi(i)} \mapsto \prod_{i\in[n]} x_{\pi(i),i}.$$

Thus, the cycle $\pi = (1\ m_1\ m_2\dots\ m_n)$ maps, under $P^{(T)}$, to the n-cycle $(1\ m_n\ m_{n-1}\dots m_2\ m_1)$, which is π^{-1}. Since the inverse of a permutation is unique, $P^{(T)}$ maps each monomial to a unique monomial and hence is also a permutation symmetry of HC_n. To see that $P^{(\sigma)}$ and $P^{(T)}$ commute, note

$$(P^{(\sigma)}P^{(T)})_{(i,j),(k,\ell)} = \sum_{(a,b),a\neq b} P^{(\sigma)}_{(i,j),(a,b)}P^{(T)}_{(a,b),(k,\ell)}.$$

From the definitions of $P^{(\sigma)}$ and $P^{(T)}$, we get that $P^{(\sigma)}_{(i,j),(a,b)}P^{(T)}_{(a,b),(k,\ell)} = 1$ if and only if $(a,b) = (\sigma(i),\sigma(j))$ and $(a,b) = (\ell,k)$. Equivalently, $P^{(\sigma)}_{(i,j),(a,b)}P^{(T)}_{(a,b),(k,\ell)} = 1$ if and only if $k = \sigma(j)$ and $\ell = \sigma(i)$. Thus, $(P^{(\sigma)}P^{(T)})_{(i,j),(k,\ell)} = 1$ if $k = \sigma(j)$ and $\ell = \sigma(i)$, otherwise it is zero. Similarly, $(P^{(T)}P^{(\sigma)})_{(i,j),(k,\ell)} = 1$ if $k = \sigma(j)$ and $\ell = \sigma(i)$, otherwise it is zero. Hence, we get $P^{(\sigma)}P^{(T)} = P^{(T)}P^{(\sigma)}$.

C.11 Proof of Proposition 3.6

Let P be a permutation symmetry, thus $HC_n(P\mathbf{x}) = HC_n(\mathbf{x})$. Suppose $P(x_{1,2}) = x_{i,j}$. By Observation 3.2, $R_{i,j}$ is as

$$R_{i,j} := Q_{i,j} \sqcup T_{i,j} \sqcup \{x_{j,i}\}.$$

From Observation 3.2 and P being a symmetry, we get that P induces a bijection Φ from $R_{1,2}$ to $R_{i,j}$ such that,

$$\Phi : Q_{1,2} \mapsto Q_{i,j},\ T_{1,2} \mapsto T_{i,j},\ \{x_{2,1}\} \mapsto \{x_{j,i}\} \tag{18}$$

or

$$\Phi : Q_{1,2} \mapsto T_{i,j},\ T_{1,2} \mapsto Q_{i,j},\ \{x_{2,1}\} \mapsto \{x_{j,i}\} \tag{19}$$

We get that $P(x_{2,1}) = x_{j,i}$. Suppose (18) holds. Since $T_{1,2} \mapsto T_{i,j}$ under Φ, there exists a bijection $\pi : [3,n] \to [n]\backslash\{i,j\}$, such that $\Phi(x_{1,t}) = x_{i,\pi(t)}$ with $t \in [3,n]$. Thus, $P(x_{1,t}) = x_{i,\pi(t)}$. Hence, P also induces a bijection similar to Φ from $R_{1,t}$ to $R_{i,\pi(t)}$. Since $\{x_{t,1}\} \subset R_{1,t}$, we get that $P(x_{t,1}) = x_{\pi(t),i}$. Thus, $R_{t,1}$ maps bijectively to $R_{\pi(t),i}$ under P as well. Extend π to a permutation on $[n]$ by defining $\pi(1) = i$ and $\pi(2) = j$. Now, for any x_{i_1,j_1}, with $i_1, j_1 \in [2,n]$ and $i_1 \neq j_1$, it is easy to see that $x_{i_1,j_1} \in T_{i_1,1}$ and $x_{i_1,j_1} \in Q_{1,j_1}$. Thus,

$P(x_{i_1,j_1}) \in T_{\pi(i_1),i}$ and $P(x_{i_1,j_1}) \in Q_{i,\pi(j_1)}$ which implies $P(x_{i_1,j_1}) = x_{\pi(i_1),\pi(j_1)}$. Hence, for all $i, j \in [n]$, $i \neq j$, we have that $P(x_{i,j}) = x_{\pi(i),\pi(j)} = P^{(\pi)}(x_{i,j})$. Thus, $P = P^{(\pi)}$.

Now, suppose (19) holds. Since $T_{1,2} \mapsto Q_{i,j}$ under Φ, there is a bijection $\pi : [3,n] \to [n]\backslash\{i,j\}$, such that $\Phi(x_{1,t}) = x_{\pi(t),j}$. An argument similar as above shows that $P(x_{1,t}) = x_{\pi(t),j}$ for all $t \in [3,n]$ and further $P(x_{t,1}) = x_{j,\pi(t)}$. Extend π to a permutation on $[n]$ by defining $\pi(1) = j$, $\pi(2) = i$. Like before, for any x_{i_1,j_1}, with $i_1, j_1 \in [2,n]$ and $i_1 \neq j_1$, $x_{i_1,j_1} \in T_{i_1,1}$ and $x_{i_1,j_1} \in Q_{1,j_1}$. Thus, $P(x_{i_1,j_1}) \in Q_{j,\pi(i_1)}$ and $P(x_{i_1,j_1}) \in T_{i,\pi(j_1)}$ which implies $P(x_{i_1,j_1}) = x_{\pi(j_1),\pi(i_1)}$. Hence, for all $i, j \in [n]$, $i \neq j$, we have that $P(x_{i,j}) = x_{\pi(j),\pi(i)} = P^{(T)}P^{(\pi)}(x_{i,j})$. Thus, $P = P^{(T)}P^{(\pi)}$.

C.12 Proof of Observation 3.2

The reverse implication easily follows from the fact that the monomials of HC_n correspond to n-cycles. We prove the forward direction. So, suppose $x_{k,\ell} \in R_{i,j}$, that is, $\frac{\partial^2 HC_n}{\partial x_{i,j}\partial x_{k,\ell}} = 0$. If $i = k$ or $j = \ell$, then we are done by the reverse direction. Hence, assume $i \neq k$ and $j \neq \ell$. Note we also have that $i \neq j$ and $k \neq \ell$. Then, we have the following possibilities:

1. $i \neq \ell$ and $k \neq j$: For $n = 3$, this case is not possible as i, j, k, ℓ are all distinct. For $n \geq 4$, it is easy to see that there exists $\pi \in C_n$, such that $\pi(i) = j$, $\pi(k) = \ell$. Hence,

$$\frac{\partial^2 HC_n}{\partial x_{i,j}\partial x_{k,\ell}} = \sum_{\substack{\pi\in C_n,\\ \pi(i)=j,\\ \pi(k)=\ell}} \prod_{i_1\in[n]\backslash\{i,k\}} x_{i_1,\pi(i_1)} \neq 0,$$

   a contradiction.

2. $i = \ell$ and $k \neq j$: There exists $\pi \in C_n$, such that $\pi(i) = j$, $\pi(k) = i = \ell$. Hence,

$$\frac{\partial^2 HC_n}{\partial x_{i,j}\partial x_{k,\ell}} = \sum_{\substack{\pi\in C_n,\\ \pi(i)=j,\\ \pi(k)=i}} \prod_{i_1\in[n]\backslash\{i,k\}} x_{i_1,\pi(i_1)} \neq 0,$$

   a contradiction. Note that the case $i \neq \ell$ and $k = j$ gives a contradiction in the same way.

3. $i = \ell$ and $k = j$: This is the assumption in the reverse direction.

Hence, only the last case is possible, proving the forward direction. The partition of $R_{i,j}$ as described in the Observation statement follows easily by using the conditions proved for the vanishing of the second-order derivatives of HC_n.

C.13 Proof of Proposition 3.7

Let $\pi \in S_n\backslash C_n$ such that $\pi(i) \neq i$ for all $i \in [n]$. For $n \geq 5$, it can be seen that such π's exist, a concrete example is $\pi = (1\,2)(3\,4\,\ldots\,n)$. Let $m_\pi := \prod_{i\in[n]} x_{i,\pi(i)}$. Consider the polynomial

$$g(\mathbf{x}) = \sum_{P\in\mathcal{G}_{HC_n}} m_\pi(P\mathbf{x}),$$

where P goes over all permutation symmetries of HC_n. Clearly, then $g(P\mathbf{x}) = g(\mathbf{x})$ for all permutation matrices $P \in \mathcal{G}_{HC_n}$. Now, let $S \in \mathcal{G}_{HC_n}$. By Proposition 3.4, we have that the entries of S are as described in (3). Any monomial in $g(\mathbf{x})$ corresponds to some $\sigma \in S_n\backslash C_n$ such that $\sigma(i) \neq i$ for all $i \in [n]$. This is because the permutation symmetries of HC_n preserve the cyclic decomposition of any permutation, which

can be observed from the proof of Proposition 3.5 (see Section C.10). We now show for any $\sigma \in S_n \backslash C_n$, where $\sigma(i) \neq i$ for all $i \in [n]$, that $m_\sigma(S\mathbf{x}) = m_\sigma(\mathbf{x})$ by showing that $\prod_{i=1}^n S_{i,\sigma(i)} = 1$ for such σ's. Thus, any monomial of g is preserved under S, implying $S \in \mathcal{G}_g$. Thus, $\mathcal{G}_{HC_n} \subseteq \mathcal{G}_g$ but $g \neq c \cdot HC_n$ for any $c \in \mathbb{F}^\times$.

If $\sigma(n) = 1$, then

$$\begin{aligned}
\prod_{i=1}^n S_{i,\sigma(i)} &= S_{1,\sigma(1)} S_{n,1} \prod_{i=2}^{n-1} S_{i,\sigma(i)} = S_{1,\sigma(1)} S_{n,1} \prod_{i=2}^{n-1} \left(S_{i,1} S_{1,\sigma(i)} \cdot \frac{S_{2,3}}{S_{1,3} S_{2,1}} \right) \\
&= \left(\frac{S_{2,3}}{S_{1,3} S_{2,1}} \right)^{n-2} S_{1,\sigma(1)} S_{n,1} \prod_{i=2}^{n-1} S_{i,1} S_{1,\sigma(i)} \\
&= \left(\frac{S_{2,3}}{S_{1,3} S_{2,1}} \right)^{n-2} S_{1,\sigma(1)} \left(\frac{S_{1,3} S_{2,1}}{S_{2,3}} \right)^{n-2} \left(\prod_{i=2}^{n} S_{1,i} \prod_{i=2}^{n-1} S_{i,1} \right)^{-1} \prod_{i=2}^{n-1} S_{i,1} S_{1,\sigma(i)} \\
&= \frac{\prod_{i=1}^{n-1} S_{1,\sigma(i)} \cdot \prod_{i=2}^{n-1} S_{i,1}}{\prod_{i=2}^{n} S_{1,i} \cdot \prod_{i=2}^{n-1} S_{i,1}} = 1
\end{aligned}$$

The last equality holds because $\sigma(n) = 1$ implies σ is a bijection from $[n-1]$ to $[2, n]$.

If $\sigma(n) = k$, where $k \in [2, n-1]$, then $\sigma(j) = 1$ for some $j \in [2, n-1]$. We then get that

$$\begin{aligned}
\prod_{i=1}^n S_{i,\sigma(i)} &= S_{1,\sigma(1)} S_{n,k} \prod_{i=2}^{n-1} S_{i,\sigma(i)} = S_{1,\sigma(1)} S_{n,k} S_{j,1} \prod_{i \neq 1,j,n} \left(S_{i,1} S_{1,\sigma(i)} \frac{S_{2,3}}{S_{1,3} S_{2,1}} \right) \\
&= S_{1,\sigma(1)} S_{n,1} S_{1,k} \frac{S_{2,3}}{S_{1,3} S_{2,1}} S_{j,1} \prod_{i \neq 1,j,n} \left(S_{i,1} S_{1,\sigma(i)} \frac{S_{2,3}}{S_{1,3} S_{2,1}} \right) \\
&= S_{1,\sigma(1)} \left(\frac{S_{1,3} S_{2,1}}{S_{2,3}} \right)^{n-2} \left(\prod_{i=2}^{n} S_{1,i} \prod_{i=2}^{n-1} S_{i,1} \right)^{-1} \left(\frac{S_{2,3}}{S_{1,3} S_{2,1}} \right)^{n-2} S_{1,k} S_{j,1} \prod_{i \neq 1,j,n} S_{i,1} S_{1,\sigma(i)} \\
&= \frac{(S_{1,\sigma(1)} S_{1,k} \prod_{i \neq 1,j,n} S_{1,\sigma(i)}) \cdot (S_{j,1} \prod_{i \neq j} S_{i,1})}{\prod_{i=2}^{n} S_{1,i} \cdot \prod_{i=2}^{n-1} S_{i,1}} = 1.
\end{aligned}$$

The last equality holds because $\sigma(j) = 1$ implies σ is a bijection from $[n] \backslash \{j\}$ to $[2, n]$.

C.14 Scaling symmetries of $Perm_n$ and HC_n

It is easy to observe that any scaling symmetry of $Perm_n$ also gives a scaling symmetry for HC_n because the monomials of HC_n are a subset of those of $Perm_n$. We record this as an observation.

Observation C.1. If $S \in \mathcal{G}_{Perm_n}$ is a scaling symmetry of Perm_n, then a matrix $S' \in \mathrm{GL}_{n^2-n}(\mathbb{F})$ can be constructed from S such that S' is a scaling symmetry of HC_n.

We now show the converse, that is, any scaling symmetry $S \in \mathcal{G}_{HC_n}$ can be used to derive a scaling symmetry S' of $Perm_n$, where $n \neq 4$. In Appendix C.17.3, we show for HC_4 an S over appropriate fields such that $S \in \mathcal{G}_{HC_4}$ but S cannot be extended to a scaling symmetry of the Permanent.

Proposition C.2. Let $S \in \mathcal{G}_{HC_n}$ be a scaling symmetry. Consider the diagonal matrix $S' \in \mathbb{F}^{n^2 \times n^2}$ defined as:

$$\begin{aligned}
&S'_{1,j} = S_{1,j} \quad j \in [2, n], \quad S'_{i,1} = S_{i,1} \quad i \in [2, n-1], \\
&S'_{1,1} = \frac{S_{1,3} S_{2,1}}{S_{2,3}}, \quad S'_{n,1} = \frac{S'^{n-2}_{1,1}}{\prod_{i=2}^{n} S'_{1,i} \cdot \prod_{i=2}^{n-1} S'_{i,1}} \\
&S'_{i,j} = \frac{S'_{1,j} S'_{i,1}}{S'_{1,1}} \quad i, j \in [2, n].
\end{aligned} \tag{20}$$

Then $S' \in \mathcal{G}_{Perm_n}$.

Proof. Let $\pi \in S_n$. Then there exists $j \in [n]$ such that $\pi(j) = 1$. Now,

$$\prod_{i=1}^{n} S'_{i,\pi(i)} = \frac{\prod_{i=1}^{n} S'_{i,1} S'_{1,\pi(i)}}{S'^{n}_{1,1}} = \frac{\prod_{i=1}^{n} S'_{i,1} \prod_{i=1}^{n} S'_{1,\pi(i)}}{S'^{n}_{1,1}}$$

$$= \frac{S'^{2}_{1,1} S'_{n,1} \prod_{i=2}^{n-1} S'_{i,1} \prod_{i=1, i\neq j}^{n} S'_{1,\pi(i)}}{S'^{n}_{1,1}} = 1$$

by using the definition of $S'_{n,1}$, proving the statement. □

C.15 Proof of Lemma 3.2

Let X_n denote the matrix of $n \times n$ many variables. We show first how any $\pi \in C_n$ can be extended to a $\sigma \in C_m$, where $m > n$. Using this extension, we define a $m \times m$ matrix $Y^{(m,n)}$ such that $HC_m(Y^{(m,n)}) = HC_n(\mathbf{x})$. Let $j \in [n]\backslash\{1\}$ such that $\pi(j) = 1$. The mapping $\Phi : C_n \to C_m$ maps π to σ as

$$\sigma(i) = \pi(i) \quad i \in [n]\backslash\{j\}, \quad \sigma(j) = n+1,$$

$$\sigma(k) = k+1 \quad k \in [n+1, m-1], \text{ and } \sigma(m) = 1.$$

It is not hard to see that Φ is an injective map from C_n to C_m. The entries of $Y^{(m,n)}$ are defined as follows

$$Y^{(m,n)}_{i,j} = \begin{cases} x_{i,j} & i \neq j,\ i \in [1,n],\ j \in [2,n] \\ x_{i,1} & i \in [2,n],\ j = n+1 \\ 1 & i \in [n+1, m-1], j = i+1 \text{ or } i = m, j = 1 \\ 0 & \text{otherwise,} \end{cases}$$

Then, $Y^{(m,n)}$ is as follows

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \vdots \\ n-1 \\ n \\ \hline n+1 \\ n+2 \\ \vdots \\ m-1 \\ m \end{array} \begin{array}{c} \begin{array}{cccccc|cccccc} 1 & 2 & 3 & \dots & n-1 & n & n+1 & n+2 & n+3 & \dots & m-1 & m \end{array} \\ \left(\begin{array}{cccccc|cccccc} 0 & x_{1,2} & x_{1,3} & \dots & x_{1,n-1} & x_{1,n} & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & x_{2,3} & \dots & x_{2,n-1} & x_{2,n} & x_{2,1} & 0 & 0 & \dots & 0 & 0 \\ 0 & x_{3,2} & 0 & \dots & x_{1,n-1} & x_{3,n} & x_{3,1} & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & x_{n-1,2} & x_{n-1,3} & \dots & 0 & x_{n-1,n} & x_{n-1,1} & 0 & 0 & \dots & 0 & 0 \\ 0 & x_{n,2} & x_{n,3} & \dots & x_{n,n-1} & 0 & x_{n,1} & 0 & 0 & \dots & 0 & 0 \\ \hline 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{array}\right) \end{array} \tag{21}$$

Now, let $\sigma \in C_n$. In $HC_m(Y^{(m,n)})$, the term corresponding to σ is $\prod_{i=1}^{m} Y^{(m,n)}_{i,\sigma(i)}$. It follows from the definition of $Y^{(m,n)}$ that for the term to be non-zero, it must be that $\sigma(m) = 1$, $\sigma(i) = i+1$ for $i \in [n+1, m-1]$, and $\sigma(1) \neq n+1$. Thus, σ is $(1\ k_1\ k_2\ \dots\ k_n\ n+1\ n+2\ \dots\ m-1\ m)$ where $k_i \in [2,n]$ which implies,

$$\prod_{i=1}^{m} Y^{(m,n)}_{i,\sigma(i)} = \prod_{i=1}^{n} Y^{(m,n)}_{i,\sigma(i)} \prod_{i=n+1}^{m} Y^{(m,n)}_{i,\sigma(i)} = \prod_{i=1}^{n} Y^{(m,n)}_{i,\sigma(i)}.$$

For the remaining $i \in [n] \backslash \{k_n\}$, $\sigma(i) \in [2, n]$. This further gives

$$\prod_{i=1}^{n} Y_{i,\sigma(i)}^{(m,n)} = Y_{k_n,n+1}^{(m,n)} \prod_{i=1, i\neq k_n}^{n} Y_{i,\sigma(i)}^{(m,n)} = x_{k_n,1} \prod_{i=1, i\neq k_n}^{n} x_{i,\sigma(i)}.$$

The n-cycle $\pi \in C_n$, defined as $\pi = (1\ k_1\ k_2\ \ldots\ k_n)$ clearly satisfies $\Phi(\pi) = \sigma$. Since ϕ is injective, π is the unique pre-image of σ under Φ. Hence, we can write

$$x_{k_n,1} \prod_{i=1, i\neq k_n}^{n} x_{i,\sigma(i)} = \prod_{i=1}^{n} x_{i,\pi(i)}.$$

Hence, every non-zero term in $HC_m(Y^{(m,n)})$ is a monomial of $HC_n(\mathbf{x})$. Conversely, it is easy to see from the map Φ that every $\pi \in C_n$ maps to a unique $\sigma \in C_n$ and that $\prod_{i=1}^{m} Y_{i,\sigma(i)}^{(m,n)} = \prod_{i=1}^{n} x_{i,\pi(i)}$. Thus, $HC_m(Y^{(m,n)}) = HC_n(\mathbf{x})$. It is easy to see that $Y^{(m,n)}$ can be constructed in $O(m^2)$ time.

C.16 Proof of Lemma 3.3

We first prove the forward direction. It suffices to show that for all $n \geq 3$ it holds that

$$HC_n(\mathbf{x}) = \sum_{i=2}^{n} x_{1,i} HC_{n-1}(X_{n-1}^{(i)}),$$

where the matrix $X_{n-1}^{(i)}$ is obtained from X_n by first swapping row i with row 2 and column i with column 2, and then removing row 1 and column 2 from the resulting matrix. By Lemma 3.2, for all $k < n$, we can express $HC_k(X_k)$ as $HC_n(Y^{(n,k)})$ and $HC_{k-1}(X_{k-1}^{(i)})$ as $HC_n(Y_i^{(n,k-1)})$, completing the proof of the forward direction.[16] For $n = 3$ and $n = 4$, it can be easily verified that the above equality holds. Thus, we assume $n \geq 5$. We denote $X_{n-1}^{(i)}$ by $Z^{(i)}$ from now on for ease of exposition. Based on the above description, $Z^{(i)}$ looks as

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \vdots \\ i-2 \\ i-1 \\ i \\ \vdots \\ n-2 \\ n-1 \end{array} \begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & \ldots & i-2 & i-1 & i & \ldots & n-1 \end{array} \\ \begin{pmatrix} x_{i,1} & x_{i,3} & x_{i,4} & \ldots & x_{i,i-1} & x_{i,2} & x_{i,i+1} & \ldots & x_{i,n} \\ x_{3,1} & 0 & x_{3,4} & \ldots & x_{3,i-1} & x_{3,2} & x_{3,i+1} & \ldots & x_{3,n} \\ x_{4,1} & x_{4,3} & 0 & \ldots & x_{4,i-1} & x_{4,2} & x_{4,i+1} & \ldots & x_{4,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{i-1,1} & x_{i-1,3} & x_{i-1,4} & \ldots & 0 & x_{i-1,2} & x_{i-1,i+1} & \ldots & x_{i-1,n} \\ x_{2,1} & x_{2,3} & x_{2,4} & \ldots & x_{2,i-1} & 0 & x_{2,i+1} & \ldots & x_{2,n} \\ x_{i+1,1} & x_{i+1,3} & x_{i+1,4} & \ldots & x_{i+1,i-1} & x_{i+1,2} & 0 & \ldots & x_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n-1,1} & x_{n-1,3} & x_{n-1,4} & \ldots & x_{n-1,i-1} & x_{n-1,2} & x_{n-1,i+1} & \ldots & x_{n-1,n} \\ x_{n,1} & x_{n,3} & x_{n,4} & \ldots & x_{n,i-1} & x_{n,2} & x_{n,i+1} & \ldots & 0 \end{pmatrix} \end{array} \tag{22}$$

[16] We assume the diagonal entries of X_n are replaced by 0's

Formally, the entries of $Z^{(i)}$ are defined as follows

$$Z^{(i)}_{k,\ell} = \begin{cases} x_{k+1,\ell+1} & k,\ell \in [n-1]\backslash\{1,i-1\}, \\ x_{k+1,1} & k \in [n-1]\backslash\{1,i-1\}, \ell = 1 \\ x_{k+1,2} & k \in [n-1]\backslash\{1,i-1\}, \ell = i-1, \\ x_{i,\ell+1} & k = 1, \ell \in [n-1]\backslash\{1,i-1\}, \\ x_{i,2} & k = 1, \ell = i-1, \\ x_{2,\ell+1} & k = i-1, \ell \in [n-1]\backslash\{1,i-1\}, \\ x_{2,1} & k = i-1, \ell = 1, \\ x_{i,1} & k = 1, \ell = 1 \\ 0 & \text{otherwise,} \end{cases}$$

Note that we can replace $x_{i,1}$ by 0 in $X^{(i)}_{n-1}$ as HC_{n-1} does not depend on the diagonal entries. We show that

$$HC_{n-1}(Z^{(i)}) = \sum_{\substack{\sigma \in C_n, \\ \sigma(1)=i}} \prod_{j=2}^{n} x_{j,\sigma(j)},$$

Showing the above equality for a single i suffices as the proof is similar for all i. Let $\pi \in C_{n-1}$. Then in $HC_{n-1}(Z^{(i)})$, the term corresponding to π is

$$\prod_{j=1}^{n-1} Z^{(i)}_{j,\pi(j)}.$$

Based on the values of $\pi(1)$ and $\pi(i-1)$, we have the following cases:

1. $\pi(1) = i-1$. Then $\pi(i-1) = k$ and $\pi(\ell) = 1$, where $k,\ell \in [n-1]\backslash\{1,i-1\}$ and $k \neq \ell$ as $n \geq 5$. In this case

$$\prod_{j=1}^{n-1} Z^{(i)}_{j,\pi(j)} = Z^{(i)}_{1,i-1} Z^{(i)}_{i-1,k} Z^{(i)}_{\ell,1} \prod_{j\neq 1,i-1,\ell} Z^{(i)}_{j,\pi(j)} = x_{i,2} x_{2,k+1} x_{\ell+1,1} \prod_{j\neq 1,i-1,\ell} x_{j+1,\pi(j)+1}$$

2. $\pi(1) \neq i-1$ and $\pi(i-1) = 1$. Then $\pi(1) = k$ and $\pi(\ell) = i-1$, where $k,\ell \in [n-1]\backslash\{1,i-1\}$ and $k \neq \ell$ as $n \geq 5$. In this case

$$\prod_{j=1}^{n-1} Z^{(i)}_{j,\pi(j)} = Z^{(i)}_{1,k} Z^{(i)}_{i-1,1} Z^{(i)}_{\ell,i-1} \prod_{j\neq 1,i-1,\ell} Z^{(i)}_{j,\pi(j)} = x_{i,k+1} x_{2,1} x_{\ell+1,2} \prod_{j\neq 1,i-1,\ell} x_{j+1,\pi(j)+1}$$

3. $\pi(1) \neq i-1$ and $\pi(i-1) \neq 1$. Let $\pi(1) = j_1, \pi(i-1) = j_2$, $\pi(\ell) = i-1$ and $\pi(k) = 1$, with $j_1, j_2, \ell, k \in [n-1]$. In this case

$$\begin{aligned} \prod_{j=1}^{n-1} Z^{(i)}_{j,\pi(j)} &= Z^{(i)}_{1,j_1} Z^{(i)}_{i-1,j_2} Z^{(i)}_{\ell,i-1} Z^{(i)}_{k,1} \prod_{j\neq 1,i-1,\ell,k} Z^{(i)}_{j,\pi(j)} \\ &= x_{i,j_1+1} x_{2,j_2+1} x_{\ell+1,2} x_{k+1,1} \prod_{j\neq 1,i-1,\ell,k} x_{j+1,\pi(j)+1} \end{aligned}$$

In all of the above cases, π maps to a unique $\sigma \in C_n$ such that $\sigma(1) = i$ and $\prod_{j=1}^{n} x_{j,\sigma(j)} = x_{1,i} \prod_{j=1}^{n-1} Z^{(i)}_{j,\pi(j)}$. Thus, $x_{1,i} HC_{n-1}(X^{(i)}_{n-1})$ is the sum of all Hamiltonian cycles which visit the edge $(1,i)$. Hence,

$$HC_n(\mathbf{x}) = \sum_{i=2}^{n} x_{1,i} \Big(\sum_{\substack{\sigma \in C_n, \\ \sigma(1)=i}} \prod_{j=2}^{n} x_{j,\sigma(j)} \Big) = \sum_{i=2}^{n} x_{1,i} HC_{n-1}(X^{(i)}_{n-1}),$$

completing the proof of the forward direction. For the reverse direction, we use induction on n.

Base case $n = 2$. We have by assumption that $f(Y^{(2,2)}) = f(X_2) = x_{1,2}x_{2,1} = HC_2(X_2)$.

Inductive hypothesis. Suppose the reverse direction holds for all $k \in [2, n-1]$. Let f be such that it satisfies all $n-1$ identities, where $n > 2$. Then, we have that $f(Y^{(n,k)}) = HC_k(X_k)$ for $k \in [2, n-1]$. Thus, $HC_{n-1}(X_{n-1}^{(i)}) = HC_n(Y_i^{(n,n-1)}) = f(Y_i^{(n,n-1)})$. Hence,

$$f(\mathbf{x}) = f(Y^{(n,n)}) = \sum_{i=2}^{n} x_{1,i} f(Y_i^{(n,n-1)}) = \sum_{i=2}^{n} x_{1,i} HC_{n-1}(X_{n-1}^{(i)}) = HC_n(\mathbf{x}).$$

This proves the hypothesis for n.

C.17 Analysis for HC_4

We first analyse $\mathfrak{g}_{HC_4}$ in Section C.17.1 over all fields. We then determine the scaling symmetries of HC_4 over finite fields, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ in Section C.17.2. In Section C.17.3, we show that HC_4 and HC_3 are characterised by its symmetries over appropriate fields.

C.17.1 Lie Algebra

Proposition C.3 shows that over characteristic 2 fields, $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_4})$ is 7, while over other fields $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_4})$ is 6.

Proposition C.3. Let $\mathbb{F}$ be any field. If $\mathrm{char}(\mathbb{F}) \neq 2$, then $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_4}) = 6$ and the set $\mathscr{B}_n$ as described in Proposition 3.1 is a basis of $\mathfrak{g}_{HC_4}$ over $\mathbb{F}$. If $\mathrm{char}(\mathbb{F})$ is 2, then $\dim_{\mathbb{F}}(\mathfrak{g}_{HC_4}) = 7$ and a basis of $\mathfrak{g}_{HC_4}$ over $\mathbb{F}$ is the set of vectors $\mathscr{B}_n \sqcup \{D\}$, represented as the following matrix

$$\begin{array}{c} \\ (1,2) \\ (1,3) \\ (1,4) \\ (2,1) \\ (2,3) \\ (2,4) \\ (3,1) \\ (3,2) \\ (3,4) \\ (4,1) \\ (4,2) \\ (4,3) \end{array} \begin{array}{c} \begin{array}{ccccccc} A^{(2)} & A^{(3)} & A^{(4)} & B^{(2)} & B^{(3)} & C & D \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array} \tag{23}$$

Proof. Note that Proposition 3.1 already describes the structure of any $M \in \mathfrak{g}_{HC_4}$ as a diagonal matrix, the entries of which are the nullspace of the matrix M^{HC_4}. We analyse the nullspace of M^{HC_4} over all fields.

$$M^{HC_4} = \begin{array}{c} \\ (1,2,3,4) \\ (1,2,4,3) \\ (1,3,2,4) \\ (1,3,4,2) \\ (1,4,2,3) \\ (1,4,3,2) \end{array} \begin{array}{c} \begin{array}{ccc|ccc|ccc|ccc} & & & & & & & & & & & \end{array} \\ \left(\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \end{array} \tag{24}$$

Fields of characteristic other than 2. By applying Gaussian Elimination on M^{HC_4}, we get the following row reduced matrix. Note that each step of Gaussian Elimination uses only additions or subtractions of the rows.

$$\begin{array}{c} (1,2,3,4) \\ (1,2,4,3) \\ (1,3,2,4) \\ (1,3,4,2) \\ (1,4,2,3) \\ (1,4,3,2) \end{array} \left(\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 1 & 0 & -1 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & -1 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 2 & 0 & 2 & -2 & 0 \end{array}\right)$$

As the characteristic is not equal to 2, M^{HC_4} has row rank 6 and therefore the dimension of $\mathfrak{g}_{HC_4}$ is 6 over such fields. The set $\mathscr{B}_n$ described in Proposition 3.2 is easily verified to be a basis for $\mathfrak{g}_{HC_4}$. The linear independence of $\mathscr{B}_n$ over any field has already been argued in Section C.4.

Characteristic 2 fields. As before, after Gaussian Elimination the row reduced form of M^{HC_4} is as follows

$$\begin{array}{c} (1,2,3,4) \\ (1,2,4,3) \\ (1,3,2,4) \\ (1,3,4,2) \\ (1,4,2,3) \\ (1,4,3,2) \end{array} \left(\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Thus, the first five rows are linearly independent while the last row is a linear combination of the first five rows over characteristic 2 fields. Hence, the dimension of $\mathfrak{g}_{HC_4}$ is 7 over such fields. We now show that the columns of the matrix M in (23) form a basis for $\mathfrak{g}_{HC_4}$.

The first six columns of M are precisely the basis elements in the non-characteristic 2 case. It can be easily checked that the last column lies in $\mathfrak{g}_{HC_4}$. The submatrix indexed by the first 7 rows of M is

$$\begin{array}{c} \\ (1,2) \\ (1,3) \\ (1,4) \\ (2,1) \\ (2,3) \\ (2,4) \\ (3,1) \end{array} \begin{array}{c} \begin{array}{ccccccc} A^{(2)} & A^{(3)} & A^{(4)} & B^{(2)} & B^{(3)} & C & D \end{array} \\ \left(\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{array}\right) \end{array}.$$

By Gaussian Elimination, it can be verified that the determinant of this submatrix is 1. Hence, all the columns are linearly independent and thus form a basis for $\mathfrak{g}_{HC_4}$ over characteristic 2 fields. □

Proposition C.4 describes how the entries of any $\mathbf{z} \in \mathfrak{g}_{HC_4}$ are related and can be proved similarly to Corollary 3.1. Lemma C.4 is used in analysing the scaling symmetries of HC_4 and can be proved similarly as Lemma C.2.

Proposition C.4. Over characteristic 2 fields, $\mathbf{z} \in \mathfrak{g}_{HC_4}$ if and only if the entries of $\mathbf{z}$ satisfy

$$\begin{aligned} z_{3,2} &= z_{3,1} + z_{1,2} + z_{2,4} + z_{1,4} + z_{2,1}, \\ z_{3,4} &= z_{3,1} + z_{1,4} + z_{2,3} + z_{1,3} + z_{2,1}, \\ z_{4,1} &= z_{1,2} + z_{1,3} + z_{1,4} + z_{2,1} + z_{3,1}, \\ z_{4,2} &= z_{1,4} + z_{2,3} + z_{3,1} \\ &= z_{4,1} + z_{1,2} + z_{2,3} + z_{1,3} + z_{2,1}, \\ z_{4,3} &= z_{1,2} + z_{2,4} + z_{3,1} \\ &= z_{4,1} + z_{1,3} + z_{2,4} + z_{1,4} + z_{2,1}. \end{aligned} \tag{25}$$

Lemma C.4. Let R be a commutative ring with identity such that 2 is invertible in R. Consider the system of linear equations given by $M^{(HC_4)}\mathbf{x} = 0$ over R. Then, the entries of any solution $\mathbf{u}$ to this system of equations satisfy (2).

Proof. Let $\mathbf{u}$ be a solution. We can then write

$$(M_1 \mid M_2) \cdot \begin{pmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{pmatrix} = \mathbf{0},$$

where M_1 is the 6×6 matrix indexed by the set of columns $\{(2,4),(3,2),(3,4),(4,1),(4,2),(4,3)\}$, M_2 is the matrix indexed by the remaining columns, $\mathbf{u}_1$ and $\mathbf{u}_2$ are entries of $\mathbf{u}$ corresponding to the set of columns of M_1 and M_2 respectively. Thus, M_1 and M_2 are as follows

$$M_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

It can be verified by Gaussian Elimination that $det(M_1)$ is -2. Since 2 is invertible over R, then so is -2, implying that the adjoint of M_1 is well defined over R. Multiplying on the left by the adjoint of M_1 gives

$$\left(\begin{array}{cccccc|cccccc} -2 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 2 & 0 & 2 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 2 & -2 & 0 & -2 & 2 & 2 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 & -2 & 2 & -2 & 2 & 2 \\ 0 & 0 & 0 & -2 & 0 & 0 & -2 & 2 & -2 & 2 & -4 & -2 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & -2 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 & 0 & -2 & -2 & 2 & -2 & 0 & -2 & -2 \end{array}\right) \cdot \begin{pmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{pmatrix} = \mathbf{0}.$$

This then implies

$$-2 \cdot \begin{pmatrix} u_{2,4} + u_{1,3} - u_{1,4} - u_{2,3} \\ u_{3,2} - u_{1,2} + u_{1,3} + u_{2,1} - u_{2,3} - u_{3,1} \\ u_{3,4} + u_{1,3} - u_{1,4} + u_{2,1} - u_{2,3} - u_{3,1} \\ u_{4,1} + u_{1,2} - u_{1,3} + u_{1,4} - u_{2,1} + 2u_{2,3} + u_{3,1} \\ u_{4,2} + u_{1,4} + u_{2,3} + u_{3,1} \\ u_{4,3} + u_{1,2} - u_{1,3} + u_{1,4} + u_{2,3} + u_{3,1} \end{pmatrix} = \mathbf{0}$$

Since 2 is invertible in the ring, we can cancel out -2 which gives

$$\cdot \begin{pmatrix} u_{2,4}+u_{1,3}-u_{1,4}-u_{2,3} \\ u_{3,2}-u_{1,2}+u_{1,3}+u_{2,1}-u_{2,3}-u_{3,1} \\ u_{3,4}+u_{1,3}-u_{1,4}+u_{2,1}-u_{2,3}-u_{3,1} \\ u_{4,1}+u_{1,2}-u_{1,3}+u_{1,4}-u_{2,1}+2u_{2,3}+u_{3,1} \\ u_{4,2}+u_{1,4}+u_{2,3}+u_{3,1} \\ u_{4,3}+u_{1,2}-u_{1,3}+u_{1,4}+u_{2,3}+u_{3,1} \end{pmatrix} = \mathbf{0}$$

which essentially means that the entries of $\mathbf{u}$ satisfy the linear equations in (2), proving the lemma statement. □

C.17.2 Symmetries

Lemma 3.1 and Proposition 3.3 can be proved for HC_4 similarly to the general case. Thus, over fields $\mathbb{F}$ such that $|\mathbb{F}| > \binom{12}{2}$, the symmetries of HC_4 are generated by permutation and scaling matrices.

The permutation symmetries of HC_4 are the same as those described in Proposition 3.6. Observation C.2 shows that HC_4, over fields of characteristic other than 2 has a scaling symmetry D which is discrete, that is, D does not satisfy (3). The observation can be verified easily using (3). In particular, over $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and over $\mathbb{F}_q$, such that $2 \mid q-1$, HC_4 has a discrete symmetry.[17] Over characteristic 2 fields, the symmetry D becomes the identity matrix. Lemma C.5 describes the scaling symmetries of HC_4 over $\mathbb{Q}$, $\mathbb{R}$ and finite fields $\mathbb{F}_q$, where $2 \nmid q-1$, that is, $q = 2^k$ for some $k > 1$. Lemma C.6 describes the symmetries over finite fields $\mathbb{F}_q$ where $2 \mid q-1$, and its proof can be adapted for $\mathbb{C}$ and general fields $\mathbb{F}$.

Observation C.2. Let $\mathbb{F}$ be such that $\mathrm{char}(\mathbb{F}) \neq 2$. Then,

1. The diagonal matrix D with $D_{1,2} = D_{2,3} = D_{3,1} = -1$ and the rest of the entries as 1 is a discrete scaling symmetry of HC_4.
2. The diagonal matrix S, with entries satisfying

$$\begin{aligned} S_{1,2} &= \frac{S_{4,2}}{S_{2,4}S_{3,2}S_{4,1}S_{4,3}}, \quad S_{1,3} = \frac{1}{S_{2,4}S_{3,2}S_{4,1}}, \quad S_{1,4} = \frac{S_{3,4}S_{4,2}}{S_{2,4}S_{3,2}^2S_{4,1}S_{4,3}}, \\ S_{2,1} &= \frac{S_{2,4}S_{3,2}S_{4,1}}{S_{3,4}S_{4,2}}, \quad S_{2,3} = \frac{S_{2,4}S_{3,2}S_{4,3}}{S_{3,4}S_{4,2}}, \quad S_{3,1} = \frac{S_{3,2}S_{4,1}}{S_{4,2}}, \end{aligned} \tag{26}$$

   is a continuous scaling symmetry of HC_4.

When $\mathrm{char}(\mathbb{F}) = 2$, then D is the identity matrix.

Lemma C.5. Over $\mathbb{F}_q$ such that $2 \nmid q-1$, every scaling symmetry S of HC_4 is continuous, that is, the $S_{i,j}$'s satisfy the equations in (3). Over $\mathbb{R}$ and $\mathbb{Q}$, the entries $S_{i,j}$ are of the form $(-1)^{z_{i,j}} \cdot r_{i,j}$ with $z_{i,j} \in \mathbb{F}_2$ and $r_{i,j} > 0$ such that the $r_{i,j}$'s satisfy the equations in (3) and $z_{i,j}$'s satisfy (25). The symmetries over $\mathbb{Q}$ and $\mathbb{R}$ given by $S'_{i,j} = (-1)^{z_{i,j}}$ are discrete symmetries if and only if $z_{2,4} \neq z_{1,4} + z_{2,3} + z_{1,3}$.

Proof. Let S be a scaling symmetry of HC_4. Then we have

$$\prod_{i=1}^{4} S_{i,\sigma(i)} = 1 \quad \sigma \in C_4.$$

[17] $2 \mid q-1$ implies q is the power of an odd prime. Hence, $\mathrm{char}(\mathbb{F}_q) \neq 2$ in this case.

Over $\mathbb{F}_q$. Note that $2 \nmid q-1$ implies $q = 2^k$. Let γ be a generator of $\mathbb{F}_q^\times$. Then, we can write $S_{i,j}$ as $\gamma^{z_{i,j}}$. Thus, we can rewrite the above equations as

$$\sum_{i=1}^{4} z_{i,\sigma(i)} = 0 \quad \text{over } \mathbb{Z}_{q-1},$$

Since $2 \nmid q-1$, therefore 2 is invertible in $\mathbb{Z}_{q-1}$. Thus, by Lemma C.4, we get that the $z_{i,j}$'s are as described in (2). Consequently, the entries $S_{i,j}$ satisfy (3).
Over $\mathbb{R}$. We can write $S_{i,j}$ as $(-1)^{z_{i,j}} \cdot 2^{w_{i,j}}$, where $2^{w_{i,j}} = r_{i,j}$. Thus, we can rewrite the above equations as

$$\sum_{i=1}^{4} z_{i,\sigma(i)} = 0 \quad \text{over } \mathbb{F}_2, \text{ and } \sum_{i=1}^{4} w_{i,\sigma(i)} = 0 \quad \text{over } \mathbb{R}.$$

Note that over $\mathbb{F}_2$ and $\mathbb{R}$, we get, from the analysis in Section C.17.1, that the solutions to both these systems of equations must be described by the $\mathfrak{g}_{HC_4}$ basis elements over $\mathbb{F}_2$ and $\mathbb{R}$, respectively. Hence, the $z_{i,j}$'s satisfy (25) while the $r_{i,j}$'s satisfy (3). Since $\mathbb{Q}$ is a subfield of $\mathbb{R}$, every scaling symmetry over $\mathbb{Q}$ must satisfy the same conditions. The claim regarding $S'_{i,j}$ follows by noting that $z_{2,4} \neq z_{1,4} + z_{2,3} + z_{1,3}$ implies $z_{2,4} = 1 + z_{1,4} + z_{2,3} + z_{1,3}$ and then showing $S'_{i,j}$ does *not* satisfy (3). If $z_{2,4} = z_{1,4} + z_{2,3} + z_{1,3}$, then it is easily verified that $S'_{i,j}$ satisfy (3). □

Lemma C.6. Let $\mathbb{F}_q$ be such that $2 \mid q-1$. If $S' \in \mathcal{G}_{HC_4}$ is a scaling symmetry over such fields $\mathbb{F}$, then S' is D, S, or DS, where D and S are as in items 1 and 2 of Observation C.2.

Proof. Suppose S' is a scaling symmetry of HC_4. Then we get

$$\prod_{i=1}^{4} S'_{i,\sigma(i)} = 1 \quad \sigma \in C_4.$$

Let γ be a generator of $F_q^\times$ and $S'_{i,j} = \gamma^{z_{i,j}}$. Then we can rewrite the above system as

$$\sum_{i=1}^{4} z_{i,\sigma(i)} = 0 \quad \text{over } \mathbb{Z}_{q-1},$$

We can express this system as

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&1&0&0&0&1&1&0&0\\ 1&0&0&0&0&1&1&0&0&0&0&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&1&0&1&0&0&0&0&1&0&1&0\\ 0&0&1&0&1&0&1&0&0&0&1&0\\ 0&0&1&1&0&0&0&1&0&0&0&1 \end{array}\right) \cdot \mathbf{z} = \mathbf{0}. \tag{27}$$

Let R_i denote the i'th row of the above matrix. Applying the elementary row operations, $R_2 \to R_2 - R_1$, $R_4 \to R_4 - R_3$, $R_6 \to R_6 - R_5 - R_4 - R_2$ gives us (28). Note that all these operations are invertible, hence the solution set is the same.

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&1&0&0&0&1&1&0&0\\ 0&0&0&0&-1&1&1&0&-1&-1&0&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&0&0&1&0&-1&0&-1&1&-1&1&0\\ 0&0&1&0&1&0&1&0&0&0&1&0\\ 0&0&0&0&0&0&-2&2&0&2&-2&0 \end{array}\right) \cdot \mathbf{z} = \mathbf{0}. \tag{28}$$

It is not hard to see that $\mathbf{z}$ is a solution to (28) if and only if $\mathbf{z}$ is a solution to (29) or is in the nullspace (over $\mathbb{Z}_{q-1}$) of the matrix in (29). This follows because $\frac{q-1}{2}$ is the only element of order 2 under addition in $\mathbb{Z}_{q-1}$.

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&1&0&0&0&1&1&0&0\\ 0&0&0&0&-1&1&1&0&-1&-1&0&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&0&0&1&0&-1&0&-1&1&-1&1&0\\ 0&0&1&0&1&0&1&0&0&0&1&0\\ 0&0&0&0&0&0&-1&1&0&1&-1&0 \end{array}\right)\cdot\mathbf{z}=\begin{pmatrix}0\\0\\0\\0\\0\\\frac{q-1}{2}\end{pmatrix} \tag{29}$$

Applying the elementary row operations, $R_5 \to R_5+R_2$, $R_1 \to R_1+R_2$, $R_5 \to R_5+2R_6$, $R_2 \to R_2+R_6$ and $R_1 \to R_1+R_6$ gives us (30). These operations are invertible, hence the solution set remains unchanged.

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&0&1&0&1&0&1&-1&1\\ 0&0&0&0&-1&1&0&1&-1&0&-1&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&0&0&1&0&-1&0&-1&1&-1&1&0\\ 0&0&1&0&0&1&0&2&-1&1&-1&1\\ 0&0&0&0&0&0&-1&1&0&1&-1&0 \end{array}\right)\cdot\mathbf{z}=\begin{pmatrix}\frac{q-1}{2}\\\frac{q-1}{2}\\0\\0\\0\\\frac{q-1}{2}\end{pmatrix} \tag{30}$$

Thus, from (30), we get that any solution $\mathbf{z}$ to the system of equations in (28) is of the form

$$\begin{aligned} z_{1,2} &= \frac{q-1}{2} - z_{2,4} - z_{3,2} - z_{4,1} + z_{4,2} - z_{4,3}\\ z_{1,3} &= -z_{2,4} - z_{3,2} - z_{4,1}\\ z_{1,4} &= -z_{2,4} - 2z_{3,2} + z_{3,4} - z_{4,1} + z_{4,2} - z_{4,3}\\ z_{2,1} &= z_{2,4} + z_{3,2} - z_{3,4} + z_{4,1} - z_{4,2}\\ z_{2,3} &= \frac{q-1}{2} + z_{2,4} + z_{3,2} - z_{3,4} - z_{4,2} + z_{4,3},\\ z_{3,1} &= \frac{q-1}{2} + z_{3,2} + z_{4,1} - z_{4,2}. \end{aligned} \tag{31}$$

or is of form

$$\begin{aligned} z_{1,2} &= -z_{2,4} - z_{3,2} - z_{4,1} + z_{4,2} - z_{4,3}\\ z_{1,3} &= -z_{2,4} - z_{3,2} - z_{4,1}\\ z_{1,4} &= -z_{2,4} - 2z_{3,2} + z_{3,4} - z_{4,1} + z_{4,2} - z_{4,3}\\ z_{2,1} &= z_{2,4} + z_{3,2} - z_{3,4} + z_{4,1} - z_{4,2}\\ z_{2,3} &= z_{2,4} + z_{3,2} - z_{3,4} - z_{4,2} + z_{4,3},\\ z_{3,1} &= z_{3,2} + z_{4,1} - z_{4,2}. \end{aligned} \tag{32}$$

Thus, we get that $S'_{i,j} = \gamma^{z_{i,j}}$ are either as

$$\begin{aligned} S'_{1,2} &= -\frac{S'_{4,2}}{S'_{2,4}S'_{3,2}S'_{4,1}S'_{4,3}}, \quad S'_{1,3} = \frac{1}{S'_{2,4}S'_{3,2}S'_{4,1}}, \quad S'_{1,4} = \frac{S'_{3,4}S'_{4,2}}{S'_{2,4}S'^{2}_{3,2}S'_{4,1}S'_{4,3}},\\ S'_{2,1} &= \frac{S'_{2,4}S'_{3,2}S'_{4,1}}{S'_{3,4}S'_{4,2}}, \quad S'_{2,3} = -\frac{S'_{2,4}S'_{3,2}S'_{4,3}}{S'_{3,4}S'_{4,2}}, \quad S'_{3,1} = -\frac{S'_{3,2}S'_{4,1}}{S'_{4,2}}, \end{aligned} \tag{33}$$

or as

$$S'_{1,2} = -\frac{S'_{4,2}}{S'_{2,4}S'_{3,2}S'_{4,1}S'_{4,3}}, \quad S'_{1,3} = \frac{1}{S'_{2,4}S'_{3,2}S'_{4,1}}, \quad S'_{1,4} = \frac{S'_{3,4}S'_{4,2}}{S'_{2,4}S'^2_{3,2}S'_{4,1}S'_{4,3}},$$
$$S'_{2,1} = \frac{S'_{2,4}S'_{3,2}S'_{4,1}}{S'_{3,4}S'_{4,2}}, \quad S'_{2,3} = -\frac{S'_{2,4}S'_{3,2}S'_{4,3}}{S'_{3,4}S'_{4,2}}, \quad S'_{3,1} = -\frac{S'_{3,2}S'_{4,1}}{S'_{4,2}}. \tag{34}$$

Hence, any scaling symmetry S' is of the form D, S, or DS, where D and S are as per items 1 and 2 of Observation C.2 respectively. □

Over $\mathbb{C}$ and general fields $\mathbb{F}$. The proof of Lemma C.6 can be adapted to work over $\mathbb{C}$, and general fields $\mathbb{F}$ where $\text{char}(\mathbb{F}) \neq 2$, by treating the system of equations given by $\prod_{i=1}^{4} S'_{i,\sigma(i)} = 1$ over $\mathbb{C}$ (resp. $\mathbb{F}$) as a system of linear equations over $\mathbb{C}^\times$ (resp. $\mathbb{F}^\times$) where $+$ corresponds to multiplication and 0 is the multiplicative identity 1. Thus, we can represent this system just like (27), where the entries of $\mathbf{z}$ are the $S'_{i,j}$'s and $\mathbf{0}$ is replaced by the all ones vector $\mathbf{1}$. Applying Gaussian Elimination gives (28). Then, S' is a solution to (28) if and only if S' is a solution to (29), with $(q-1)/2$ replaced by -1 since $x^2 = 1$ has 1 and -1 as the only solutions over $\mathbb{F}$, or S' is in the nullspace (over $\mathbb{F}^\times$) of the matrix in (29). Then, we further perform elementary row operations to obtain (30), which then shows that $S'_{i,j}$'s satisfy (33) or (34). Thus, S' must be of form D,S, or DS.

Over fields $\mathbb{F}$ where $\text{char}(\mathbb{F}) = 2$, the matrix D in the proof becomes the identity matrix. Hence, we get that all the scaling symmetries of HC_4 are continuous over such $\mathbb{F}$.

C.17.3 Characterisation by symmetries

The existence of the symmetry D as described in item 1 of Observation C.2 helps show that HC_4 is characterised by its symmetries over large enough fields $\mathbb{F}$ with $\text{char}(\mathbb{F}) \neq 2$ as we show in Proposition C.5. We use the approach in the proof of Proposition 3.4.5 in [Gro12], where it is shown that the Permanent is characterised by its symmetries. When $\text{char}(\mathbb{F}) = 2$, then Proposition C.6 shows that HC_4 is *not* characterised by its symmetries. Proposition C.7 shows HC_3 is characterised by its symmetries when $|\mathbb{F}| > \binom{6}{2}$.

Proposition C.5. Over any field $\mathbb{F}$ such that $|\mathbb{F}| > \binom{12}{2}$ and $\text{char}(\mathbb{F}) \neq 2$, HC_4 is characterised by its symmetries.

Proof. The assumption on the field size ensures that $\mathscr{G}_{HC_4}$ is generated by permutation and scaling matrices. Suppose $f(\mathbf{x})$ is a 12-variate homogeneous[18] degree-4 polynomial such that $\mathscr{G}_{HC_4} \subseteq \mathscr{G}_f$. Let m be a monomial in $f(\mathbf{x})$ and $x_{i,j}$ be a variable in m, with $i \neq j$. Let $c \in \mathbb{F}^\times$, $k \in [4]$ and $k \neq i$. Apply the mapping $x_{k,\ell} \mapsto c \cdot x_{k,\ell}$ for all $\ell \in [4]\backslash\{k\}$, and $x_{\ell,j} \mapsto c^{-1} \cdot x_{\ell,j}$ for all $\ell \neq j$. It is easily verified that for all $k \neq i$, the aforementioned mapping is a scaling symmetry of HC_4 satisfying item 2 of Observation C.2, and therefore is also a scaling symmetry of f. This implies m must contain for all $k \neq i$ some variable $x_{k,\ell}$ because $x_{i,j}$ is scaled down by c and if all variables in m are of form $x_{i,\ell}$ then the above mapping is not a scaling symmetry of f, a contradiction. Thus, m contains, for all $k \in [4]$, some $x_{k,\ell}$. Since f is homogeneous, m must contain exactly one $x_{k,\ell}$ for all $k \in [4]$.

The above argument can be adapted to further show that m must correspond to a permutation $\pi \in S_4$ with $\pi(i) \neq i$ for all $i \in [4]$, since $\mathbf{x}$ does *not* contain $x_{i,i}$ variables. Further, consider $f(D\mathbf{x})$, where D is as described in item 1 of Observation C.2. If m corresponded to one of the non-cyclic permutations $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, or $(1\,4)(2\,3)$, then it is not hard to see that under D, m gets mapped to $-m$, a contradiction. Thus, m corresponds to a cyclic permutation in C_4. Finally, applying all the permutation symmetries of HC_4 on f shows that for every $\sigma \in C_4$, there must be a monomial corresponding to it present in f. Hence $f = \alpha.HC_4$ for some $\alpha \in \mathbb{F}^\times$. □

[18] A polynomial f is homogeneous if all the monomials in f have the same degree.

Proposition C.6. Over any field $\mathbb{F}$ such that $|\mathbb{F}| > \binom{12}{2}$ and $\mathrm{char}(\mathbb{F}) = 2$, HC_4 is *not* characterised by its symmetries.

Proof. The condition $|\mathbb{F}| > \binom{12}{2}$ ensures $\mathscr{G}_{HC_4}$ is generated by permutation and scaling symmetries. Since $\mathrm{char}(\mathbb{F}) = 2$, all scaling symmetries of HC_4 are continuous by the modifications to the proof of Lemma C.6 as suggested in the paragraph Over $\mathbb{C}$ and general fields $\mathbb{F}$ in Appendix C.17.2. Over such fields, HC_4 is *not* characterised by its symmetries because for the polynomial

$$f(\mathbf{x}) = x_{1,2}x_{2,1}x_{3,4}x_{4,3} + x_{1,3}x_{3,1}x_{2,4}x_{4,2} + x_{1,4}x_{4,1}x_{3,2}x_{2,3},$$

it can be easily verified that $\mathscr{G}_{HC_4} \subseteq \mathscr{G}_f$ but $f \neq cHC_4$ for any $c \in \mathbb{F}^\times$. □

Proposition C.7. Over any field $\mathbb{F}$ such that $|\mathbb{F}| > \binom{6}{2}$, HC_3 is characterised by its symmetries.

Proof. The assumption on the field size ensures that $\mathscr{G}_{HC_3}$ is generated by permutation and scaling matrices. Suppose $f(\mathbf{x})$ is a 6-variate homogeneous degree-3 polynomial such that $\mathscr{G}_{HC_3} \subseteq \mathscr{G}_f$. Applying the same scaling map as in the proof of Proposition C.5, it can be shown that if m is a monomial of f, then m corresponds to a permutation $\sigma \in S_3 \backslash C_3$, such that $\sigma(i) \neq i$ for all $i \in [3]$. This immediately implies that $\sigma \in C_3$. Thus, m corresponds to a cyclic permutation. Finally, applying all the permutation symmetries of HC_3 on m shows that for every $\sigma \in C_3$, there must be a monomial corresponding to it present in f. Hence $f = \alpha.HC_3$ for some $\alpha \in \mathbb{F}^\times$. □

D Missing Proofs from Section 4

D.1 Proof of Proposition 4.1

If $f = HC_n(A\mathbf{x})$, then $\mathfrak{g}_f$ is $2n-2$ dimensional by Lemma 2.2 and Proposition 3.2. As $C = \sum_{i=1}^{2n-2} a_i B_i$, then $B' = ACA^{-1} = \sum_{i=1}^{2n-2} a_i AB_iA^{-1}$. By Lemma 2.2, B' lies in $\mathfrak{g}_{HC_n}$ and is a diagonal matrix with its entries being an $\mathbb{F}$-linear combination of a_i's. The matrices AB_iA^{-1} are a basis for $\mathfrak{g}_{HC_n}$. Since $|\mathbb{F}| > \binom{n^2-n}{2}$, by Lemma 3.1, there is a matrix in $\mathfrak{g}_{HC_n}$ with distinct eigenvalues. Thus, there exists a choice of a_i's such that B' has distinct eigenvalues. By the Polynomial Identity Lemma, B', over a random choice of a_i's from U, has distinct eigenvalues with probability $\geq 1 - \frac{\binom{n^2-n}{2}}{|U|} > 1 - \frac{1}{3n}$. Thus, C has distinct eigenvalues with high probability because C and B' are similar matrices. Hence, they also have the same characteristic polynomial which factorises over $\mathbb{F}$.

Therefore, there exists $D \in \mathrm{GL}_{n^2-n}(\mathbb{F})$ such that $C' = D^{-1}CD$ is diagonal. We can compute D by computing the characteristic polynomial of C, factorising the polynomial to get the eigenvalues $\lambda_1, \ldots, \lambda_{n^2-n}$, which are all distinct, and then finding the basis vector of the nullspace of $C - \lambda_i I_{(n^2-n)\times(n^2-n)}$ for all $i \in [n^2-n]$. The matrix D is formed from all these basis vectors.

Note that D also diagonalises the B_i's. Hence, the polynomial $g = f(D\mathbf{x}) = HC_n(AD\mathbf{x})$ is such that $\mathfrak{g}_g$ is diagonal. By Lemma 2.2, we get that

$$C' = D^{-1}CD = (AD)^{-1} \cdot B' \cdot AD,$$

with C' and B' being diagonal matrices with distinct entries. Then, following the same argument as in the proof of Proposition 3.3 (see Appendix C.8), we get that $AD = PS$ for some permutation matrix P and scaling matrix S.

Complexity analysis. Step 1 can be performed via Lemma 2.3 in $n^{O(1)}$ time. For Step 2, we need access to an efficient univariate polynomial factorisation algorithm to compute D. The running time is randomised $n^{O(1)}$.

D.2 Proof of Claim 4.1

Let $P(x_{i,j}) = x_{1,2}$. Let $\sigma \in S_n$ such that $\sigma(1) = i$ and $\sigma(2) = j$. Then $P^{(\sigma)}$, defined as per Proposition 3.5, is a permutation symmetry of HC_n. Thus, $HC_n(P^{(\sigma)}\mathbf{x}) = HC_n(\mathbf{x})$ implies $HC_n(P^{(\sigma)}P\mathbf{x}) = HC_n(P\mathbf{x})$. It then follows that $P^{(\sigma)}P(x_{1,2}) = x_{1,2}$ because

$$(P^{(\sigma)}P)_{(1,2),(1,2)} = \sum_{a,b\in[n],a\neq b} P^{(\sigma)}_{(1,2),(a,b)} P_{(a,b),(1,2)}$$

$$= P^{(\sigma)}_{(1,2),(i,j)} P_{(i,j),(1,2)} = P^{(\sigma)}_{(1,2),(\sigma(1),\sigma(2))} P_{(i,j),(1,2)} = 1.$$

The third last equality holds because $P_{(i,j)(1,2)} = 1$ by assumption, and the definition of σ ensures that the second last equality holds.

D.3 Proof of Proposition 4.2

Step 1 of Algorithm 3 errs with probability at most $\frac{n^5}{|U|}$, where $U \subset \mathbb{F}$, by the Polynomial Identity Lemma and union bound. For $|U| \geq 3n^5$, the error is upper bounded by $\frac{1}{3}$. Repeating the algorithm will boost the success probability.

The correctness of Steps 2 and 3 follows from Claim 4.1 and Observation 3.2. By Observation 3.2 we have that $P'(x_{2,1})$ must be $x_{i,j}$, proving the correctness of Step 4. Now, the set $T'_{1,2}$ is either the image of $T_{1,2}$ or that of $Q_{1,2}$ under P.

In the first case, the elements of $T'_{1,2}$ are of form $P(x_{1,t})$, $t \in [3,n]$. By mapping $x_{1,t}$'s to some permutation π of the elements of $T'_{1,2}$, we get that $P'P(x_{1,t}) = x_{1,\pi(t)}$. Step 5 then sets $P'(x_{t,1})$ such that $P'P(x_{t,1}) = x_{\pi(t),1}$. Extend π to a permutation on $[n]$ by defining $\pi(1) = 1, \pi(2) = 2$. For the remaining $x_{a,b}$ with $a, b \in [2,n]$, we set $P'(x_{a,b})$ consistently in Step 6 so that we get $P'P(x_{a,b}) = x_{\pi(a),\pi(b)}$. Thus, we get that $P'P = P^{(\pi)}$.

In the second case, the elements of $T'_{1,2}$ are of form $P(x_{t,2})$, $t \in [3,n]$. By mapping $x_{1,t}$'s to some permutation π of the elements of $T'_{1,2}$, we get that $P'P(x_{1,t}) = x_{\pi(t),2}$. Step 5 then sets $P'(x_{t,1})$ such that $P'P(x_{t,1}) = x_{2,\pi(t)}$. Extend π to a permutation on $[n]$ by defining $\pi(1) = 1, \pi(2) = 2$. For the remaining $x_{a,b}$ with $a, b \in [2,n]$, we set $P'(x_{a,b})$ consistently in Step 6 so that again we get $P'P(x_{a,b}) = x_{\pi(b),\pi(a)}$. Thus, we get that $P'P = P^{(\pi)}P^{(T)}$.

Complexity analysis. Step 1 of Algorithm 3 uses Lemma 2.1 to compute black-box access to second-order partial derivatives and uses the Polynomial Identity Lemma to check if the derivatives are identically zero, and can be performed in randomised $n^{O(1)}$ time. The remaining steps can be performed in $O(n^4)$ time. Hence, Algorithm 3 has running time randomised $n^{O(1)}$.

D.4 Proof of Claim 4.2

As $f(\mathbf{x}) = HC_n(S\mathbf{x})$, we define another scaling matrix D by setting $D_{1,j} := S^{-1}_{1,j}$ for $j \in [2,n]$, $D_{2,3} = S^{-1}_{2,3}$ and $D_{i,1} = S^{-1}_{i,1}$, where $i \in [2, n-1]$. Set the rest of the $D_{i,j}$'s as described in (3). Then, $D \in \mathscr{G}_{HC_n}$ by construction, hence $HC_n(D\mathbf{x}) = HC_n(\mathbf{x})$ implies $f = HC_n(S\mathbf{x}) = HC_n(DS\mathbf{x})$. Set $S' := DS$ and note that S' satisfies the observation statement.

D.5 Proof of Proposition 4.3

Suppose γ is a generator of $\mathbb{F}_q^\times$. Then we can write $S'_{i,j}$ as $\gamma^{y_{i,j}}$ and c_k as γ^{e_k}. This gives the following system of equations over $\mathbb{Z}_{q-1}$

$$\sum_{i=1}^{n} y_{i,\sigma_k(i)} = e_k \bmod q-1.$$

In terms of the matrix $M^{(n)}$, the above system can be written as

$$M^{(n)}.\mathbf{y} = \mathbf{e}$$

where the entries of $\mathbf{e}$ are the exponents e_k. As $\mathbb{Z}_{q-1}$ is a commutative ring, by Lemma C.3 any solution to the above system of linear equations will give a scaling matrix. Note that $y_{i,j} = 0$ for all $(i,j) \notin T$ by assumption, with T as described in Step 3 of Algorithm 4. Thus, we get a system of $(n-1)(n-2)$ many linear equations in $(n-1)(n-2)$ many $\mathbf{y}$ variables over $\mathbb{Z}_{q-1}$ which can be written as

$$M.\mathbf{y} = \mathbf{e}$$

with $M = M^{(n)}_{\bullet \times T}$ and $det(M) = \beta = \pm 1$ by Lemma C.1. From Cramer's rule, we get that

$$y_{i,j} = \beta \cdot \sum_{k=1}^{(n-1)(n-2)} e_k \alpha_{k,(i,j)} \bmod q-1.$$

Then,

$$S'_{i,j} = \gamma^{y_{i,j}} = \gamma^{\beta \cdot \sum_{k=1}^{(n-1)(n-2)} e_k \alpha_{k,(i,j)} \bmod q-1}.$$

As $c_k = \gamma^{e_k}$, therefore

$$S'_{i,j} = \prod_{k=1}^{(n-1)(n-2)} c_k^{\beta \cdot \alpha_{k,(i,j)} \bmod q-1}.$$

Clearly, $HC_n(S'\mathbf{x}) = HC_n(S\mathbf{x})$ which implies $S'S^{-1}$ is a scaling symmetry of HC_n. Note that Algorithm 4 does *not* need to compute the discrete logarithm of any element. The algorithm computes β and $\alpha_{k,(i,j)}$'s over $\mathbb{Z}_{q-1}$ and raises the coefficients c_k to powers as described above to compute $S'_{i,j}$.

Complexity analysis. Step 2 can be executed in $n^{O(1)}$ time as shown in the proof of Proposition C.1. Step 3 and 4 can be performed in $(n \log q)^{O(1)}$ time as M is a 0/1 matrix of dimension $(n-1)(n-2) \times (n-1)(n-2)$, implying the magnitude $|\alpha_{k,(i,j)}|$ of any cofactor is at most $((n-1)(n-2))!$ and has bit complexity $O(n^2 \log n \log q)$. Since $\beta = \pm 1$ by Lemma C.1. Thus, we can compute the cofactors in $(n \log q)^{O(1)}$ time over $\mathbb{Z}_{q-1}$, and the powers of the coefficients c_k by repeated squaring. Thus, the running time is deterministic $(n \log q)^{O(1)}$.

D.5.1 Correctness and Complexity over $\mathbb{Q}$ and other fields

To make Algorithm 4 work over other fields, the main changes are in Steps 3 and 4, where all computations involving the matrix M are over $\mathbb{Z}$ now. The argument given above for finite fields can be adapted to argue the correctness over all fields $\mathbb{F}$ by noting that the system we want to solve is

$$\prod_{i=1}^{n} S'_{i,\sigma_k(i)} = c_k$$

which is a system of linear equations over the group $\mathbb{F}^\times$, where we interpret multiplication as addition and 1 as 0. This system of linear equations can be written as

$$M^{(n)}.\mathbf{s} = \mathbf{c},$$

where the entries of $\mathbf{s}$ are $S'_{i,j}$ and $\mathbf{c}$ are the coefficients c_k. Lemma C.3 shows that solving the above system of equations will produce an S' such that $HC_n(S'\mathbf{x}) = f(\mathbf{x})$. By Claim 4.2, we reduce to solving

$$M.\mathbf{s}_1 = \mathbf{c},$$

where $M = M^{(n)}_{\cdot \times T}$ and the entries of $\mathbf{s}_1$ are $S'_{i,j}$ with $(i,j) \in T$. Since M is a 0/1 matrix, and by Lemma C.1 $det(M)$ is ± 1, we get that M^{-1} is an integer matrix. We can thus multiply by M^{-1} on the left to get

$$\mathbf{s}_1 = M^{-1}\mathbf{c}.$$

Note, since we treat $+$ as the multiplication operation, $M^{-1}\mathbf{c}$ is computed by raising c_k's or their inverses to integral powers as determined by the rows of M^{-1}. Thus, each $S'_{i,j}$ is obtained by multiplying integral powers of the c_k's.

Complexity analysis. For the complexity analysis, we can perform Steps 3 and 4 in $n^{O(1)}$ time using repeated squaring required for each $S_{i,j}$. Over $\mathbb{Q}$, the running time is $(nc)^{O(1)}$, where c is the bit complexity of f. Over $\mathbb{R}$, $\mathbb{C}$, and general fields $\mathbb{F}$, assuming that we can perform exact arithmetic, we get $n^{O(1)}$ running time.

D.6 S-equivalence test for HC_4

In this section, we show how to perform S-equivalence test for HC_4 over $\mathbb{Q}$, $\mathbb{R}$, and finite fields $\mathbb{F}_q$.

Over $\mathbb{F}_q$ when $2 \nmid q-1$. If $2 \nmid q-1$, then Algorithm 4 continues to work for HC_4, because 2 is invertible in the ring $\mathbb{Z}_{q-1}$ and Lemma C.4 continues to hold.

Over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{F}_q$ where $2 \mid q-1$. We will present the test over $\mathbb{Q}$ and the same will also hold over $\mathbb{R}$ and $\mathbb{F}_q$. Over $\mathbb{Q}$, we assume that rational numbers are given in the form $\frac{a}{b}$, where $a, b \in \mathbb{Z}$, $b \neq 0$. Over $\mathbb{R}$, we assume that the model of computation is able to compute positive square roots [Bre76]. Over $\mathbb{F}_q$, where $\text{char}(\mathbb{F}_q) > 2$ because $2 \mid q-1$, square root computation can be done in randomised $\log^{O(1)}(q)$ time [Ton91, Sha73] and in deterministic $\log^{O(1)}(q)$ time assuming the Generalised Reimann Hypothesis [Bac90].

The main idea is to solve the system of linear equations arising from the coefficients of each monomial. Suppose $f = HC_4(S\mathbf{x})$. Treat the permutations $\sigma \in C_4$ as 4-tuples of the form $(1, i_2, i_3, i_4)$ and order them lexicographically. Then, we have that

$$\prod_{i=1}^{4} S_{i,\sigma_j(i)} = c_j \quad j \in [6].$$

with $c_j \in \mathbb{Q}^\times$ as the coefficient corresponding to σ_j, which can be obtained from $f(\mathbf{x})$ by querying it at the respective monomial. Each c_j is of form $c_j = (-1)^{e_j} r_j$, where $r_j > 0$. We create a new diagonal matrix S', with $S'_{i,k} = (-1)^{z_{i,k}} w_{i,k}$, with $z_{i,k}$ and $w_{i,k}$ as variables over $\mathbb{F}_2$ and $\mathbb{Q}^{>0}$ (the multiplicative group of positive rationals) respectively. We thus have to solve the following systems

$$\sum_{i=1}^{4} z_{i,\sigma_j(i)} = e_j \text{ over } \mathbb{F}_2, \text{ and } \prod_{i=1}^{4} w_{i,\sigma_j(i)} = r_j \text{ over } \mathbb{Q}^{>0}.$$

Like in the case for general n, we can assume that $z_{1,2}, z_{1,3}, z_{1,4}, z_{2,1}, z_{2,3}, z_{2,4}$ and $z_{3,1}$ are 0 by Proposition C.4 and we can solve the system over $\mathbb{F}_2$ separately by adapting Algorithm 4. We now solve the system in $w_{i,k}$ variables, which we can express as follows

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&1&0&0&0&1&1&0&0\\ 1&0&0&0&0&1&1&0&0&0&0&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&1&0&1&0&0&0&0&1&0&1&0\\ 0&0&1&0&1&0&1&0&0&0&1&0\\ 0&0&1&1&0&0&0&1&0&0&0&1 \end{array}\right) \cdot \mathbf{w} = \begin{pmatrix} r_1\\ r_2\\ r_3\\ r_4\\ r_5\\ r_6 \end{pmatrix} \tag{35}$$

where $\mathbf{w}$ is a vector of variables over $(\mathbb{Q}^>)^6$, addition and subtraction correspond to multiplication and division in $\mathbb{Q}^>$, scaling by positive integer to raising to integral powers, scaling by -1 to taking the inverse of an element in $\mathbb{Q}^>$ and scaling by 0 means replacing the element by 1. Then, as in the proof of Lemma C.6, Gaussian elimination gives

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&1&0&0&0&1&1&0&0\\ 0&0&0&0&-1&1&1&0&-1&-1&0&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&0&0&1&0&-1&0&-1&1&-1&1&0\\ 0&0&1&0&1&0&1&0&0&0&1&0\\ 0&0&0&0&0&0&-2&2&0&2&-2&0 \end{array}\right) \cdot \mathbf{w} = \begin{pmatrix} r_1\\ \frac{r_2}{r_1}\\ r_3\\ \frac{r_4}{r_3}\\ r_5\\ \frac{r_6 r_3 r_1}{r_5 r_4 r_2} \end{pmatrix} \tag{36}$$

It is verifiable that $\frac{r_6 r_3 r_1}{r_5 r_4 r_2}$ is a square using $r_j = \prod_{i=1}^{4} S_{i,\sigma_j(i)}$.

A solution to (37) is also a solution to (36). As r_i's are assumed to be given in the form $\frac{a_i}{b_i}$, we can compute the positive square root of $\frac{r_6 r_3 r_1}{r_5 r_4 r_2}$ by computing its numerator and denominator, and then using binary search to compute the positive square root of the numerator and the denominator.

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&1&0&0&0&1&1&0&0\\ 0&0&0&0&-1&1&1&0&-1&-1&0&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&0&0&1&0&-1&0&-1&1&-1&1&0\\ 0&0&1&0&1&0&1&0&0&0&1&0\\ 0&0&0&0&0&0&-1&1&0&1&-1&0 \end{array}\right) \cdot \mathbf{w} = \begin{pmatrix} r_1\\ \frac{r_2}{r_1}\\ r_3\\ \frac{r_4}{r_3}\\ r_5\\ \sqrt{\frac{r_6 r_3 r_1}{r_5 r_4 r_2}} \end{pmatrix} \tag{37}$$

We can proceed further with Gaussian elimination to get

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1&0&0&0&0&1&0&1&0&1&-1&1\\ 0&0&0&0&-1&1&0&1&-1&0&-1&1\\ 0&1&0&0&0&1&0&1&0&1&0&0\\ 0&0&0&1&0&-1&0&-1&1&-1&1&0\\ 0&0&1&0&0&1&0&2&-1&1&-1&1\\ 0&0&0&0&0&0&-1&1&0&1&-1&0 \end{array}\right) \cdot \mathbf{w} = \begin{pmatrix} r'_1\\ r'_2\\ r_3\\ r'_4\\ r'_5\\ r'_6 \end{pmatrix} \tag{38}$$

where $r'_1 = \sqrt{\frac{r_6 r_3 r_1 r_2}{r_5 r_4}}$, $r'_2 = \sqrt{\frac{r_6 r_3 r_2}{r_5 r_4 r_1}}$, $r'_4 = \frac{r_4}{r_3}$, $r'_5 = \frac{r_6 r_3}{r_4}$, and $r'_6 = \sqrt{\frac{r_6 r_3 r_1}{r_5 r_4 r_2}}$. It can again be verified that $\frac{r_6 r_3 r_1 r_2}{r_5 r_4}$

and $\frac{r_6 r_3 r_2}{r_5 r_4 r_1}$ are both squares, and hence we can compute their positive square roots. We can then set $w_{i,j}$'s as

$$\begin{aligned} w_{1,2} &= \sqrt{\frac{r_6 r_3 r_1 r_2}{r_5 r_4}} \quad w_{2,1} = \frac{r_4}{r_3} \\ w_{1,3} &= r_3 \quad w_{2,3} = \sqrt{\frac{r_5 r_4 r_1}{r_6 r_3 r_2}} \\ w_{1,4} &= r_6 \frac{r_3}{r_4} \quad w_{3,1} = \sqrt{\frac{r_5 r_4 r_2}{r_6 r_3 r_1}} \end{aligned} \tag{39}$$

and the remaining $w_{i,j}$'s to 1. Thus, we get $S'_{i,j} = (-1)^{z_{i,j}} w_{i,j} \in \mathbb{Q}^\times$. It is then easily verifiable that $HC_4(S'\mathbf{x}) = f(\mathbf{x})$. Over $\mathbb{R}$, we can set $S'_{i,j}$'s in the same way, assuming the model of computation allows us to compute square roots exactly. Over $\mathbb{F}_q$, we do not need to consider signs separately and can represent the equations $\prod_{i=1}^{4} S_{i,\sigma_j(i)} = c_j$ as the system of equations in (36) and solve this system of equations as before using square root computations wherever necessary.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il