

# ON THE SATISFIABILITY PROBLEM FOR THE SYMMETRIC GROUP $S_4$ AND MODULAR CIRCUITS



Simon Grünbacher and Erhard Aichinger

Institute for Algebra

Austrian Science Fund FWF P33878



Der Wissenschaftsfonds.

# THE QUESTION



# The Question

Let  $S_4$  be the symmetric group on a four-element set.

A **polynomial** over  $S_4$  is a product of variables and constants.

**Example:**  $(1\ 2)xy(4\ 3)$  is a polynomial of **length** 4.

We are interested in the complexity of the decision problem  $\text{POLSAT}(S_4)$ :

**Given:** A polynomial  $p$  over  $S_4$ .

**Asked:** Is there an assignment  $x \in S_4^n$  such that  $p(x) = 1$ ?

If we instead ask whether  $p(x) = 1$  for **all** assignments, the problem is called  $\text{POLEQV}(S_4)$ .

# WHAT HAPPENED BEFORE



## Why $S_4$ ?

The following related questions already have an answer:

- Systems of equations over a fixed finite group  $G$ . [M. Goldmann, A.Russell 2002]
- $\text{POLSAT}(S_3)$  and  $\text{POLEQV}(S_3)$  are in P. [G. Horvath, C.Szabo 2006], [S. Burris, J.Lawrence 2004]
- $\text{POLSAT}(A_4)$  and  $\text{POLEQV}(A_4)$  are in P. [G.Horvath, C.Szabo 2012]
- In fact:  $S_4$  is the smallest group for which the problems are not known to be in P.
- $\text{POLSAT}(S_5)$  and  $\text{POLEQV}(S_5)$  are in NPC/coNPC. [M.Goldmann, A.Russel 2002]

# Representations of polynomials

**Question:** Does the choice of representation matter?

**Answer:** Yes! We have the following:

**Theorem [M. Kompatscher, 2019]**

Let  $G$  be a finite non-nilpotent group. Then there is a term  $t$  such that  $\text{POLSAT}(G, t)$  is NP-complete and  $\text{POLEQV}(G, t)$  is coNP-complete.

## Lower bounds

Conjecture [Exponential Time Hypothesis, R.Impagliazzo, R.Paturi 2001]

All deterministic algorithms solving 3-satisfiability take  $\exp(o(n))$  time.

Theorem [P. Idziak, P. Kawalek, J. Krzaczkowski, 2020]

If ETH holds, then  $\text{POLSAT}(S_4)$  and  $\text{POLEQV}(S_4)$  both require  $\exp(o(\log^2(n)))$  time.

**Proof idea:** Find a polynomial  $p$  of length  $\exp(O(\sqrt{n}))$  that expresses  $n$ -bit conjunction. Use this to do a very inefficient reduction.

# Modular Circuits

The complexity of solving equations is related to the strength of the following computational model:

## Definition

For integers  $m_1, \dots, m_h$ , a  $\text{CC}[m_1, \dots, m_h]$ -circuit is a boolean circuit with:

- depth  $h$
- arbitrary fan-in
- gates at depth  $i$  that return 1 iff  $m_i$  divides  $\sum_i x_i$ .

## Conjecture [Strong Exponential Size Hypothesis]

Let  $p_1, \dots, p_h$  be primes. Then  $\text{CC}[p_1, \dots, p_h]$ -circuits require  $\exp(o(n^{1/(h-1)}))$  gates to compute  $\text{AND}_n$ .

**Note:** Lower bound can be matched.



# Conjunction and satisfiability

## Lemma [Folklore]

Fix  $p_1, \dots, p_h$ . Let  $\gamma(n)$  be a lower bound on the size of  $\text{CC}[p_1, \dots, p_h]$ -circuits computing  $\text{AND}_n$ . Then we can decide  $\exists x \in \{0, 1\}^n : C(x) = 1$  for such a circuit in deterministic time  $\exp(O(\gamma^{-1}(|C|) \log(|C|)))$ .

**Proof:** Assume  $C(x) = 1$  is satisfiable.

Let  $a$  be a solution of minimal hamming weight  $k$ .

Let  $C'$  be the circuit obtained from  $C$  by fixing  $x_i$  to 0 whenever  $a_i = 0$ .

Then  $C'$  computes  $\text{AND}_k$  by minimality of  $a$ .

Therefore  $|C| \geq |C'| \geq \gamma(k)$ , thus  $k \leq \gamma^{-1}(|C|)$ .

$\implies$  It suffices to check only those  $x$  with hamming weight at most  $\gamma^{-1}(|C|)$ .

**Note:** There is also a randomized  $\exp(O(\gamma^{-1}(|C|) + \log(|C|)))$  algorithm.

# Upper bounds

SESH also leads to algorithms for some equation satisfiability problems.

**Note:** A hardness assumption leads to an algorithm.

**Intuition:** Easier to reason about a computationally limited model.

## Theorem [M.Kompatscher, 2022]

Assume SESH and let  $A$  be a finite **nilpotent** algebra from a congruence modular variety. Then there is  $t(A) > 0$  and  $\exp(O(\log^{t(A)}(n)))$  algorithms solving  $\text{CSAT}(A)$  and  $\text{CEqv}(A)$ .

**Question:** Can we apply this idea also to  $S_4$ ?

## Upper bounds for $S_4$

According to [P.Idziak, P.Kawalek, J.Krzaczkowski and A.Weiß 2020]:

*The paper [2] contains all necessary pieces to provide a  $\exp(O(\log^{r(G)}(n)))$  upper bound for  $\text{POLSAT}(G)$  whenever  $G$  is solvable [under SESH].*

**Our contribution:** Work out the details for  $S_4$ .

# What we did

## Theorem [Erhard Aichinger, S.G. 2025]

The following problems are polytime-equivalent:

- $\text{POLSAT}(S_4)$
- the complement of  $\text{POLEQV}(S_4)$
- the satisfiability problem for  $\text{CC}[2, 3, 2]$ -circuits

Therefore, SESH implies a  $\exp(O(\log(n)^3))$  deterministic upper bound for both problems.

# THE PROOF



# The proof

We prove only the reduction from  $\text{POLSAT}(S_4)$  to circuit satisfiability.

The **holomorph** of a group  $G$  is  $\text{Hol}(G) := G \rtimes \text{Aut}(G)$ .

We have  $S_4 \cong \text{Hol}(\mathbb{Z}_2^2) \cong \mathbb{Z}_2^2 \rtimes \text{GL}_2(\mathbb{Z}_2) \cong \mathbb{Z}_2^2 \rtimes (\mathbb{Z}_3 \rtimes \mathbb{Z}_2)$ .

We first reduce  $\text{POLSAT}(S_4)$  to an intermediate problem involving the matrix ring  $\mathbb{Z}_2^{2 \times 2}$ .

# Restricted expressions

## Definition

A restricted monomial expression is a product of variables and elements from  $GL_2(\mathbb{Z}_2)$ . A **restricted polynomial expression**  $p$  is a sum of restricted monomial expressions. The **restricted equivalence problem**  $REQV(\mathbb{Z}_2^{2 \times 2})$  asks whether  $p(X) = 0$  for all **invertible**  $X$ .

**Example:**  $Z \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} XY + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

**Non-example:**  $XY \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

We will use the following **interpolation** result:

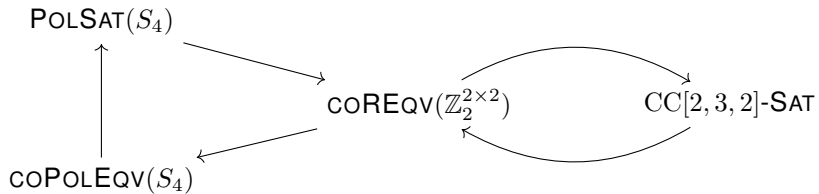
## Lemma

Let  $f : (\mathbb{Z}_2^{2 \times 2})^k \rightarrow \mathbb{Z}_2^{2 \times 2}$  be a function. Then there is a restricted polynomial expression computing  $f$ .

**Proof idea:** It is known that  $f$  is computed by a general polynomial  $p$ .

**Fact:** You can replace every noninvertible constant  $a$  by a sum of two invertible constants. Expand the result.

## A picture





# From groups to matrices

**Initial problem:**  $\exists x \in S_4^m : p(x) = 1$

Representation:  $S_4 \cong \mathbb{Z}_2^2 \times \text{GL}_2(\mathbb{Z}_2)$

Multiplication:  $\begin{pmatrix} v \\ A \end{pmatrix} \cdot \begin{pmatrix} w \\ B \end{pmatrix} := \begin{pmatrix} v + Aw \\ AB \end{pmatrix}.$

Representation for  $S_4$ -polynomials:  $\prod_{i=1}^n \begin{pmatrix} v_i \\ A_i \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m p_j y_j \\ q \end{pmatrix}$  where  $p_1, \dots, p_m, q$  are restricted polynomial expressions.

**New problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m, y \in (\mathbb{Z}_2^2)^m : \sum_i p_i(X) y_i = 0 \wedge q(X) = 1$

# Getting rid of vectors

**Current problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m, y \in (\mathbb{Z}_2^2)^m : \sum_i p_i(X)y_i = 0 \wedge q(X) = 1$

**Observation:** If  $\sum_{i=1}^N g_i = 0$  over  $(\mathbb{Z}_2^2, +)$  then there exists  $S \subseteq [N]$  with  $|S| \leq 4$  and  $\sum_{s \in S} g_s = 0$ .

$\implies$  The equation  $\sum_i p_i y_i = 0$  has a solution iff it has a solution with at most 4 nonzero  $y_i$ .

$\implies$  Sufficient to check a smaller set  $S$  of  $O(n^4)$  choices of  $y$ .

**Interpolation:** For all  $v \in \mathbb{Z}_2^2$  there is a constant restricted polynomial expression  $M(v)$  with  $M(v) = (v \ 0)$ .

**New problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m : \exists y \in S : \sum_i p_i(X)M(y_i) = 0 \wedge q(X) - 1 = 0$ .

# Getting rid of AND

**Current problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m : \exists y \in S \sum_i p_i(X)M(y_i) = 0 \wedge q(X) - 1 = 0$ .

We wish to express  $a = b = 0$  by a single inequality.

If  $\mathbb{Z}_2^{2 \times 2}$  was a field, we would use  $(1 - a^{q-1})(1 - b^{q-1}) \neq 0 \iff a = b = 0$ .

**Interpolation:** Choose a binary restricted polynomial expression  $r$  with

$$r(x, y) \neq 0 \iff x = y = 0.$$

For  $y \in S$  let  $h_y(X) = r(\sum_i p_i(X)M(y_i), q(X) - 1)$ .

**New problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m : \exists y \in S : h_y(X) \neq 0$ .

# Getting rid of OR

**Current problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m : \exists y \in S : h_y(X) \neq 0$ .

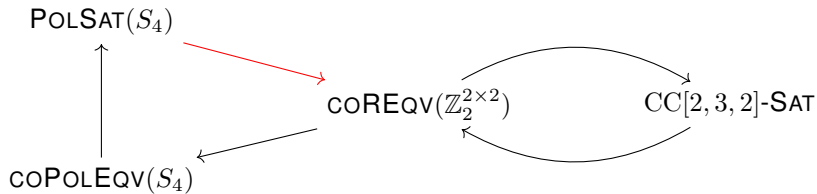
**Goal:** Eliminate disjunction over  $S$ .

**Fact:** Every  $A \in \mathbb{Z}_2^{2 \times 2}$  is a sum of some  $B, C \in \text{GL}_2(\mathbb{Z}_2)$ .

**New problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^m Z, W \in \text{GL}_2(\mathbb{Z}_2)^S : \sum_{s \in S} (Z_s + W_s) h_s(X) \neq 0$ .

We will write  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^N : g(X) \neq 0$  for brevity.

# Status update



# Inequalities to equalities

**Current problem:**  $\exists X \in \mathrm{GL}_2(\mathbb{Z}_2)^N : g(X) \neq 0$

**Interpolation:** Choose a restricted polynomial expression  $t$  with  $t(x) = 0 \iff x \neq 0$ .

**New problem:**  $\exists X \in \mathrm{GL}_2(\mathbb{Z}_2)^N : t(g(X)) = 0$ .

We will write  $\exists X \in \mathrm{GL}_2(\mathbb{Z}_2)^N : f(X) = 0$  for brevity.

## Field work

**Current problem:**  $\exists X \in \text{GL}_2(\mathbb{Z}_2)^N : f(X) = 0$

We can view  $\mathbb{Z}_2^{2 \times 2}$  as a two-dimensional vector space over the four element field  $F_4 \subseteq \mathbb{Z}_2^{2 \times 2}$  generated by  $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ .

**Fact:** The elements 1 and  $\sigma := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  form a basis.

**Fact:** Every  $X \in \text{GL}_2(\mathbb{Z}_2)$  is of the form  $\phi(s, t) := (\alpha^{s+t} + \alpha^{2+t}) + \sigma(\alpha^{s+t} + \alpha^{1+t})$  for some  $s \in \{-1, 1\}, t \in \mathbb{Z}_3$ .

**Multiplication rule:**  $\phi(r, u)\phi(s, v) = \phi(rs, su + v)$

**Note:** Using the structure of  $\text{GL}_2(\mathbb{Z}_2) \cong \text{Hol}(\mathbb{Z}_3)$  here.

Multiplication can be expanded to yield sparse polynomials over  $\mathbb{Z}_3$ .

**New problem:**  $\exists s \in \mathbb{Z}_3^N, t \in \{-1, 1\}^N : \sum_i \alpha^{q_{1i}(s,t)} + \alpha^{q_{2i}(s,t)} + \sigma(\alpha^{q_{3i}(s,t)} + \alpha^{q_{4i}(s,t)}) = 0$

**Shorter version:**  $\exists s \in \mathbb{Z}_3^N, t \in \{-1, 1\}^N : \sum_i \alpha^{u_i(s,t)} = 0 \wedge \sum_i \alpha^{v_i(s,t)} = 0$

# Cleaning up

**Current problem:**  $\exists s \in \mathbb{Z}_3^N, t \in \{-1, 1\}^N : \sum_i \alpha^{u_i(s,t)} = 0 \wedge \sum_i \alpha^{v_i(s,t)} = 0$

We combine the two equations via  $a = b = 0 \iff 1 - ((1 - a^3)(1 - b^3))^3 = 0$ .

We represent  $s_i$  as a sum of two variables in  $\{-1, 1\}$  so all variables have the same domain.

**New problem:**  $\exists x \in \{-1, 1\}^{N'} : \sum_i \alpha^{p_i(x)} = 0$

Here, the  $p_i \in \mathbb{Z}_3[x_1, \dots, x_n]$  are in sparse representation.



# Towards circuits

**Current problem:**  $\exists x \in \{-1, 1\}^N : \sum_i \alpha^{p_i(x)} = 0$

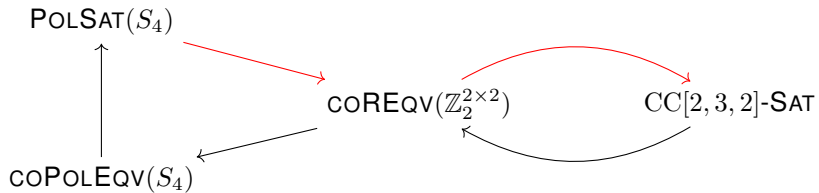
To evaluate such a expression, you need to:

- Take a product of  $\pm 1$ -valued variables (i.e. compute in  $\mathbb{Z}_2$ )
- Take a product of powers of  $\alpha$  (i.e. compute in  $\mathbb{Z}_3$ )
- Take a sum in  $F_4$  (i.e. compute in  $\mathbb{Z}_2^2$ )

Remaining translation steps tedious, but not difficult.

**Final problem:**  $\exists x : C(x) = 0$  for a  $\text{CC}[2, 3, 2]$ -circuit  $C$ .

## Towards circuits



# Open problems

**Task 1:** Prove superlinear lower bounds on  $CC[2, 3, 2]$ -circuits computing conjunction.

**Task 2:** Relate  $POLSAT(G)$  to specific modular circuit problems for other solvable groups  $G$ .