On Symmetric Signatures in Holographic Algorithms

Jin-Yi Cai
University of Wisconsin, Madison

Pinyan Lu
Tsinghua University, Beijing

NSF CCR-0208013 and CCR-0511679.

#P

Counting problems:

#SAT: How many satisfying assignments are there in a Boolean formula?

#PerfMatch: How many perfect matchings are there in a graph?

#P is at least as powerful as NP, and in fact subsumes the entire polynomial time hierarchy $\cup_i \Sigma_i^p$ [Toda].

#P-completeness: #SAT, #PerfMatch, Permanent, etc.

Some Surprises

Most #P-complete problems are counting versions of NP-complete decision problems.

But the following problems are solvable in P:

- Whether there exists a Perfect Matching in a general graph.
- Count the number of Perfect Matchings in a planar graph.

Note that the problem of counting the number of (not necessarily perfect) matchings in a planar graph is still #P-complete [Jerrum].

Holographic Algorithms by Valiant

Valiant recently introduced a beautiful theory called holographic algorithms.

Holographic algorithms are custom made for exponential cancellations.

Some seemingly exponential time computations can be done in polynomial time.

It produces an exponential number of solution fragments in a pattern of interference, analogous to quantum computing.

A Particular Counting Problem

$\#_7$Pl-Rtw-Mon-3CNF

Input: **A planar graph G_φ representing a Read-twice Monotone 3CNF Boolean formula φ.**

Output: **The number of satisfying assignments of φ, modulo 7.**

Here the vertices of G_φ represent variables x_i and clauses c_j. An edge exists between x_i and c_j iff x_i appears in c_j.

Nodes x_i have degree 2 and nodes c_j have degree 3.

#P-Hardness

Fact: **#Pl-Rtw-Mon-3CNF is #P-Complete.**

Fact: **$\#_2$Pl-Rtw-Mon-3CNF is $\oplus$P-Complete. Hence NP-hard by randomized reductions.**

An Accidental Algorithm

Valiant showed that there is a holographic algorithm solving $\#_7$Pl-Rtw-Mon-3CNF.

Hence $\#_7$Pl-Rtw-Mon-3CNF $\in$ P.

Using Matchgate Computations ...

A Matchgate Γ

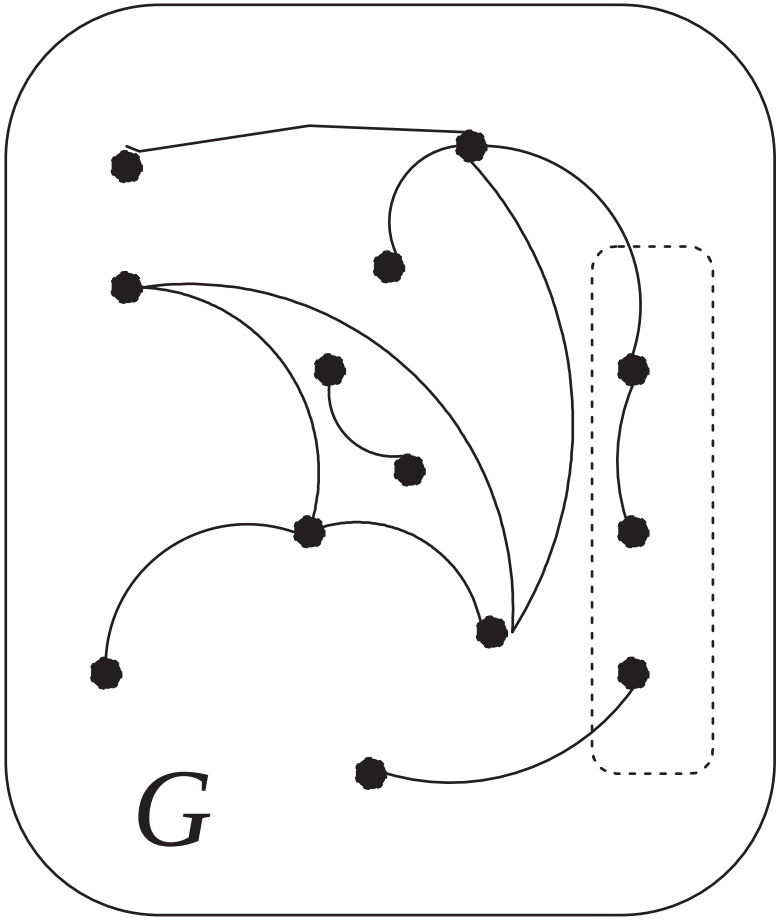


Figure 1: A matchgate Γ

Matchgate

A planar matchgate $\Gamma = (G, X)$ is a weighted graph $G = (V, E, W)$ with a planar embedding, having external nodes, placed on the outer face.

Matchgates with only output nodes are called generators.

Matchgates with only input nodes are called recognizers.

Standard Signatures

Define $\mathrm{PerfMatch}(G) = \sum_M \prod_{(i,j)\in M} w_{ij}$**, where the sum is over all perfect matchings** M**.**

A matchgate Γ **is assigned a Standard Signature**

$$G = (G^S) \text{ and } R = (R_S),$$

for generators and recognizers respectively.

$$G^S = \mathrm{PerfMatch}(G - S).$$

$$R_S = \mathrm{PerfMatch}(G' - S).$$

Each entry is indexed by a subset S **of external nodes.**

Linear bases transformations

The first ingredient of the theory of holographic algorithms are the matchgates.

The second ingredient of the theory is a choice of linear basis, through which the computation is manipulated and interpreted.

So let $\boldsymbol{b}$ denote the standard basis for two dimensional space, $\boldsymbol{b} = [e_0, e_1] = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$.

Consider another basis $\boldsymbol{\beta} = [n, p] = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right]$.

Tensor framework

We assign to each generator Γ a contravariant tensor $\boldsymbol{G} = (G^{\alpha})$.

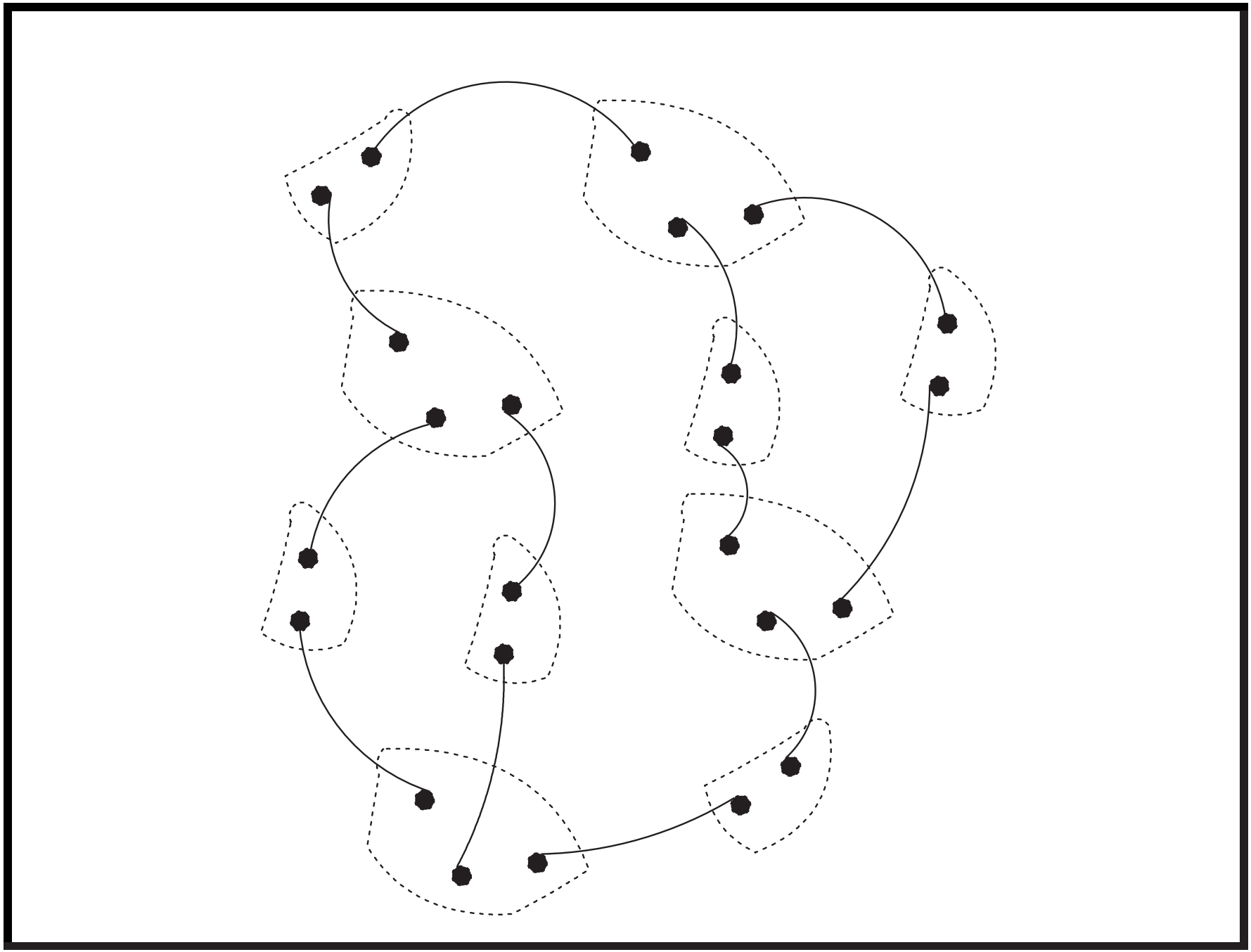
Under a basis transformation,

$$(G')^{i'_1 i'_2 \ldots i'_n} = \sum G^{i_1 i_2 \ldots i_n} \tilde{t}^{i'_1}_{i_1} \tilde{t}^{i'_2}_{i_2} \cdots \tilde{t}^{i'_n}_{i_n} \tag{1}$$

Correspondingly, each recognizer Γ gets a covariant tensor $\boldsymbol{R} = (R_{\alpha})$.

$$(R')_{i'_1 i'_2 \ldots i'_n} = \sum R_{i_1 i_2 \ldots i_n} t^{i_1}_{i'_1} t^{i_2}_{i'_2} \cdots t^{i_n}_{i'_n} \tag{2}$$

A Matchgrid Ω



Matchgrid and Holant

A matchgrid Ω is a weighted planar graph consisting of a number of generators and recognizers that are connected by connecting edges in a 1-1 fashion.

$$\text{Holant}(\Omega) = \sum_{x \in \boldsymbol{\beta}^{\otimes f}} \left\{ [\Pi_{1 \le i \le g} G(A_i, x|_{A_i})] \cdot [\Pi_{1 \le j \le r} R(B_j, x|_{B_j})] \right\}.$$

Holant Theorem

Theorem (Valiant)

$$\text{Holant}(\Omega) = \text{PerfMatch}(G).$$

A Wild Attempt at $\mathrm{P} = \mathrm{P}^{\#\mathrm{P}}$

We illustrate these concepts by the #P-complete problem #Pl-Rtw-Mon-3CNF (counting without mod).

Given φ as a planar graph G_φ.

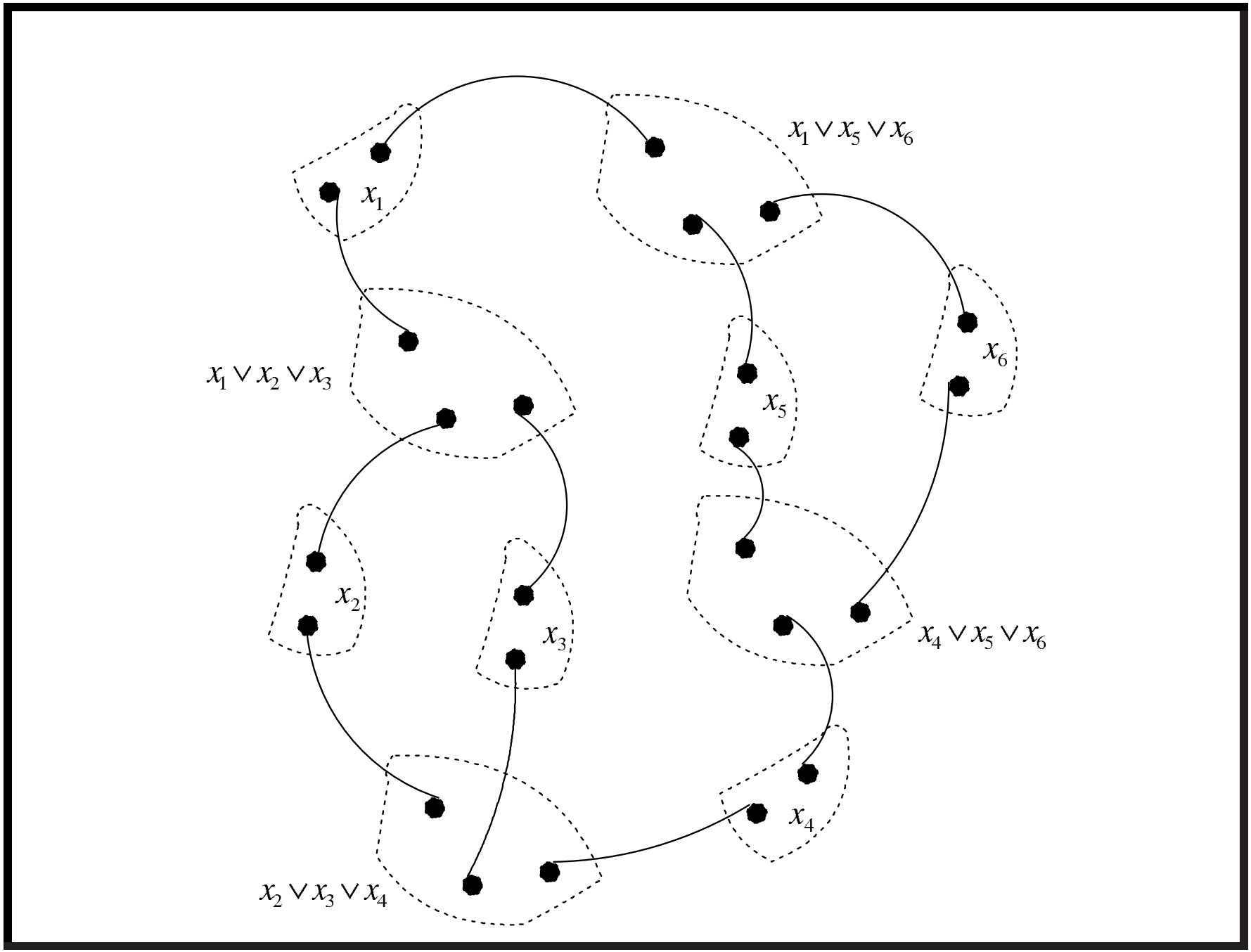
Variables and clauses are nodes.

Edge (x, C): x appears in C.

For each variable x we want a generator G with signature $G^{00} = 1, G^{01} = 0, G^{10} = 0, G^{11} = 1$, or $(1, 0, 0, 1)^{\mathtt{T}}$ for short.

This is indeed realizable as the standard signature by a path of length 3.

A Matchgrid for #Pl-Rtw-Mon-3CNF?


$x_1 \vee x_5 \vee x_6$
x_1
$x_1 \vee x_2 \vee x_3$
x_5
x_6
x_2
x_3
$x_4 \vee x_5 \vee x_6$
x_4
$x_2 \vee x_3 \vee x_4$

#Pl-Rtw-Mon-3CNF, Continued ...

Replace the vertex for x, which is read-twice, by this generator G.

This signature $(1, 0, 0, 1)^{\mathsf{T}}$ corresponds to a truth assignment: its outputs will be a consistent assignment of either 0 or 1.

We also wish to find a recognizer R with 3 inputs having signature $(0, 1, 1, 1, 1, 1, 1, 1)^{\mathsf{T}}$. This signature corresponds to a Boolean OR.

#Pl-Rtw-Mon-3CNF, Continued ...

The matchgrid is formed by connecting the generators to the recognizers as given in G_φ.

If this recognizer $(0,1,1,1,1,1,1,1)^{\mathtt{T}}$ exists, we would have shown #Pl-Rtw-Mon-3CNF $\in$ P, and therefore $\mathrm{P}^{\#\mathrm{P}} = \mathrm{P}$.

But the *standard* signature $(0,1,1,1,1,1,1,1)^{\mathtt{T}}$ does not exist.

However *over the field* $\mathbf{Z}_7$ (but not Q) They are realizable as non-standard signatures.

This gives $\#_7$Pl-Rtw-Mon-3CNF $\in$ P.

Dimension of the Basis

The basis of dimension 4 used by Valiant (FOCS06) is $n = (1, 1, 2, 1)^{\mathtt{T}}, p = (2, 3, 6, 2)^{\mathtt{T}}$**.**

The signature stands for $1n \otimes n + 0n \otimes p + 0p \otimes n + 1p \otimes p$ **(which we called** $(1, 0, 0, 1)^{\mathtt{T}}$ **for short) has dimension** $4^2 = 16$**.**

The one for $(0, 1, 1, 1, 1, 1, 1, 1)^{\mathtt{T}}$ **has dimension** $4^3 = 64$**.**

Basis of Dimension Two

In this paper we found another basis of minimal dimension 2, to show $\#_7$Pl-Rtw-Mon-3CNF $\in$ P.

Theorem

For $\mathbf{Z}_7$ and for basis

$$\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] = \left[\binom{1}{6}, \binom{3}{5} \right],$$

there is a generator for $(1,0,0,1)^{\mathtt{T}}$ and a recognizer for $(0,1,1,1,1,1,1,1)^{\mathtt{T}}$.

Symmetric Signatures

The main result in this paper is a complete classification of all Symmetric Signatures realizable by matchgates.

The algorithm for $\#_7$Pl-Rtw-Mon-3CNF follows as a consequence.

Characteristic 7 is Unique

Theorem

Characteristic 7 is the unique characteristic of a field for which there is a common basis of size 1 for generating $(1,0,0,1)^{\mathsf{T}}$ and recognizing $(0,1,1,1,1,1,1,1)^{\mathsf{T}}$.

Deeper connections with Mersenne numbers $2^p - 1$.

A Classification

Theorem

A symmetric signature $[x_0, x_1, \ldots, x_n]$ for a recognizer is realizable under the basis $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right]$ *iff* it takes one of the following forms:

- **Form 1: there exist constants λ, s, t and ϵ where $\epsilon = \pm 1$, such that for all $i, 0 \leq i \leq n$,**

  $$x_i = \lambda[(sn_0 + tn_1)^{n-i}(sp_0 + tp_1)^i + \epsilon(sn_0 - tn_1)^{n-i}(sp_0 - tp_1)^i].$$

- **Form 2: there exist constants λ,such that for all $i, 0 \leq i \leq n$,**

  $$x_i = \lambda[(n-i)n_0(p_1)^i(n_1)^{n-1-i} + ip_0(p_1)^{i-1}(n_1)^{n-i}].$$

- **Form 3: there exist constants λ,such that for all $i, 0 \leq i \leq n$,**

  $$x_i = \lambda[(n-i)n_1(p_0)^i(n_0)^{n-1-i} + ip_1(p_0)^{i-1}(n_0)^{n-i}].$$

A Classification

A similar theorem holds for generators.

Also a classification theorem for all realizable Boolean signatures.

The proofs use exponential sums and Matchgate Identities.

Another Classification

Theorem

A symmetric signature $[x_0, x_1, \cdots, x_n]$ is realizable on some basis of dimension 2 iff there exists three constants a, b, c (not all zero), such that $\forall k, 0 \leq k \leq n-2$,

$$ax_k + bx_{k+1} + cx_{k+2} = 0.$$

A Corollary

Corollary

Over the complex numbers C as well as all fields F of characteristic $p > 3$, every signature $[x_0, x_1, x_2, x_3]$ is realizable on some basis of dimension two.

This confirms a conjecture by Valiant.

Outlook

The most intriguing question is whether this new theory leads to any collapse of complexity classes.

The kinds of algorithms that are obtained by this theory are quite unlike anything before and almost exotic.

The uncertainty of its ultimate prospect makes it exciting.

Further Development

In this work we gave a complete classification of symmetric signatures realizable over bases of dimension 2.

The alternative solution to Valiant's $\#_7$Pl-Rtw-Mon-3CNF $\in$ P comes as a consequence.

Since this paper, we have been able to prove a Universal Bases Collapse Theorem, which says that no matter what dimension the Holographic Algorithm uses, it can always be replaced by bases of dimension two.

References

- **Cai and V. Choudhary.**
  On the Theory of Matchgate Computations.
  ECCC TR06-018.
- **Cai and V. Choudhary.**
  Some Results on Matchgates and Holographic Algorithms.
  ECCC TR06-048.
- **Jin-Yi Cai and Pinyan Lu.**
  Holographic Algorithms: The Power of Dimensionality Resolved.
- **Jin-Yi Cai and Pinyan Lu.**
  Holographic Algorithms: From Art to Science.