

Holographic Algorithms

Jin-Yi Cai

ABSTRACT. Leslie Valiant recently proposed a theory of holographic algorithms. These novel algorithms achieve exponential speed-ups for certain computational problems compared to naive algorithms for the same problems. The methodology uses Pfaffians and (planar) perfect matchings as basic computational primitives, and attempts to create exponential cancellations in computation. In this article we survey this new theory of matchgate computations and holographic algorithms.

1. Some Historical Background

There have always been two major strands of mathematical thought since antiquity and across civilizations: *Structural Theory* and *Computation*, as exemplified by Euclid's *Elements* and Diophantus' *Arithmetica*. Structural Theory prizes the formulation and proof of structural theorems, while Computation seeks efficient algorithmic methods to solve problems. Of course, these strands of mathematical thought are not in opposition to each other, but rather they are highly intertwined and mutually complementary. For example, from Euclid's *Elements* we learn the Euclidean algorithm to find the greatest common divisor of two positive integers. This algorithm can serve as the first logical step in the structural derivation of elementary number theory. At the same time, the correctness and efficiency of this and similar algorithms demand proofs in a purely structural sense, and use quite a bit more structural results from number theory [4]. As another example, the computational difficulty of recognizing primes and the related (but separate) problem of integer factorization already fascinated Gauss, and are closely tied to the structural theory of the distribution of primes [21, 1, 2].

The precise formulation of the concept of computation can be traced to the work of Gödel, Turing, and other logicians in the 1930s, who

Supported in part by NSF CCR-0511679.

were particularly concerned with foundational questions in mathematics: What is true, what is a proof, and what is ultimately provable. Out of such foundational investigations, we arrive at the rigorous concept of computation and what is, and is not, ultimately computable. This is considered well established now and is encapsulated by the model of Turing machines, or by Gödel's general recursive functions [48].

An important harbinger which motivated much of this development is Hilbert's 10th problem, which asks for an algorithmic procedure to decide whether a general Diophantine equation (a polynomial in several variables with integer coefficients) has an integer solution. This problem was finally shown by Matiyasevich in 1970 to admit no algorithm which can always answer correctly in a finite number of steps [43, 44]. Thus, starting with the work by Gödel, Turing, and others, in answering Hilbert's Entscheidungsproblem, computability theory was born.

However, in computability theory, we focus on ultimate computability in a logical sense, regardless of how long the computation may last, as long as it is finite. Starting in the 1960s, a new focus was given for efficient computations [14, 16, 25]. To capture this notion, complexity classes were defined; the most prominent among them were the classes P and NP. Loosely speaking, P denotes the class of all problems which can be solved by an algorithm whose running time is bounded by a fixed polynomial in the size of the input. The class P is called deterministic polynomial time, and is identified with the notion of what is efficiently computable. The class NP denotes all problems which have the property that whenever the answer is Yes for an instance of the problem, there is a short proof which can be *efficiently* verified. Here being short means that the size of the proof is bounded by a polynomial, and being efficient means that this verification is computable in deterministic polynomial time.

For example, most computations one does in linear algebra are in P, such as computing the determinant of an integer matrix, or solving a linear system of equations with rational coefficients. An archetypical problem in NP is the Boolean Satisfiability Problem (SAT): Given a propositional formula Φ in Conjunctive Normal Form (CNF), *decide* whether Φ has a satisfying assignment. Here the formula Φ takes the form $\Phi = \bigwedge_j C_j$, where each C_j is a disjunction of literals $\widehat{x}_{j_1} \vee \dots \vee \widehat{x}_{j_d}$ (where a literal \widehat{x}_j is either the Boolean variable x_j or its negation \overline{x}_j), and a satisfying assignment is a mapping $\sigma : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$, which assigns a truth value to each variable x_i , such that every C_j evaluates to true.

Many problems from NP have been shown to be NP-complete. This is a notion borrowed from computability theory. We will not formally define it, but it means that every problem in NP can be reduced by a computation in P to any NP-complete problem. It implies that if

any NP-complete problem is solvable in P, then every problem in NP is solvable in P. Examples of NP-complete problems include the above mentioned SAT, Graph 3-Coloring (given a graph, is it 3-colorable), Hamiltonicity (given a graph, does it contain a Hamiltonian circuit), and thousands more [19]. Typically, to solve an NP-complete problem it seems to require the examination of exponentially many possibilities. Whether this is intrinsically the case, is a major open problem in Theoretical Computer Science and in Mathematics, and is known as the P vs. NP problem [13]. Cook [15] was the first to introduce NP-completeness and proved that the problem SAT is NP-complete. He also proved that some restricted versions of SAT, called 3SAT, where each clause C_j contains 3 literals, are also NP-complete. (Note, however, the 2SAT problem where each clause has 2 literals is in P.) Soon afterwards, Karp [29] proved a host of other problems to be NP-complete, making NP-completeness a ubiquitous tool to prove (relative) intractability. Levin [34] in the former Soviet Union independently discovered NP-completeness.

There are many other complexity classes, e.g., the polynomial time hierarchy PH (the 0th level and the first level of PH are P and NP respectively), PSPACE, which denotes all problems computable in polynomial bounded space complexity, and a class introduced by Valiant called #P. A function is in #P if it counts the number of solutions to an instance of a problem in NP. A typical function in #P is to count the number of satisfying assignments to a Boolean formula, or the number of Traveling Salesman tours under a certain threshold for a given graph, etc. It is known that the trivial containment $P \subseteq NP \subseteq PH \subseteq PSPACE$ holds. Also trivially #P can compute NP and can be computed in PSPACE. A well known theorem by Toda [50] says that the class #P is at least as hard as PH. Thus #P-completeness is harder than NP-completeness, assuming the standard complexity theory hypothesis that the polynomial time hierarchy does not collapse. From P to PSPACE none of the above containments is known to be proper, although they are all conjectured to be.

All these classes at or above NP seem to require exponential time computation. However, the apparent need to examine exponentially many possibilities could be misleading for certain problems. There are some problems which may appear to require this exponential blow-up, but in fact do not, i.e., there are ingenious and sometimes complicated algorithms, which provably solve a problem in polynomial time. An example is the Perfect Matching problem: Given any undirected graph, decide whether there is a perfect matching, i.e., a subset M of edges such that every vertex is incident to exactly one edge in M . Edmonds [16] proved that the Perfect Matching problem is solvable in P (and in fact this motivated the concept of P initially.)

Another surprisingly good algorithm is the Fisher-Kestelyan-Temperley method, which can count the number of perfect matchings in a planar graph in polynomial time [30, 31, 49]. For weighted graphs, this method can find the sum of all weights of perfect matchings M , where the weight of a perfect matching M is the product of all the weights of the matching edges in M . The counting version corresponds to the special case where all edge weights are one. Roughly speaking, this algorithm works as follows. First it assigns a suitable factor of ± 1 to each weighted edge of the planar graph, and then it computes the Pfaffian of (the skew-symmetric adjacency matrix of) the modified graph. As the computation of a Pfaffian is essentially of the same complexity as the determinant, this algorithm is in polynomial time. Valiant's new holographic algorithms will use this remarkable algorithm as a basic component in its operations.

In this article, we will survey the new algorithm design method called holographic algorithms. This method uses perfect matching as a basic coding technique to encode computations, and then the FKT-algorithm to carry out the final computation. A particularly innovative idea is to choose a set of linear basis vectors to express and interpret a desired computation. In effect, the algorithm is designed to manipulate sums of perfect matchings in superpositions, while the speed up is achieved by cancellations among such "holographic mixes". These holographic algorithms are quite unlike anything before, except perhaps quantum algorithms. At the heart of the computation is a process of introducing and then cancelling exponentially many computational fragments. But unlike quantum algorithms, these holographic algorithms produce classical polynomial time algorithms. So far this method has produced some exotic algorithms for problems which were not known to be in P previously, and minor variations of which are known to be NP-complete or NP-hard.

The most intriguing question is whether this new theory can lead to any collapse of complexity classes. We contend that our belief of $\text{NP} \neq \text{P}$ is based on the sense and experience that the usual algorithmic paradigms are insufficient for NP-hard problems (we don't have strong lower bounds for general models of computation). But does our erstwhile experience apply to these new exotic algorithms? If the answer is no, then it is conceivable that the new methodology may lead to a radically revised conception of P vs. NP. Of course it is quite possible that the theory of holographic algorithms does not in the end lead to any collapse of complexity classes. But even in this eventuality, as Valiant suggested in [54], "any proof of $\text{P} \neq \text{NP}$ may need to explain, and not only to imply, the unsolvability" of NP-hard problems using this approach.

In Section 2 we will start with some basic definitions on holographic algorithms. In Section 3 we describe some specific problems for which

there are holographic algorithms showing that the problems belong to P. In Section 4 we discuss symmetric signatures. In Section 5 we consider admissibility and realizability of signatures. In Section 6 we consider a class of general unsymmetric signatures.

2. Preliminaries

In this section we give some basic definitions. Terminologies from the theory of holographic algorithms have been mostly introduced by Valiant [52, 54, 53], but we also include some modifications from [7, 8].

Let $G = (V, E, W)$ be a weighted undirected graph, where V is the set of vertices represented by integers $k_1 < k_2 < \dots < k_n$, E is the set of edges, and W denotes the weights of the edges. We represent the graph by a skew-symmetric matrix M , called the (skew-symmetric adjacency) matrix of G , where $M(i, j) = w(k_i, k_j)$ if $i < j$, $M(i, j) = -w(k_j, k_i)$ if $i > j$, and $M(i, i) = 0$.

The Pfaffian of an $n \times n$ skew-symmetric matrix M is defined to be 0 if n is odd, 1 if n is 0, and if $n = 2k$ where $k > 0$ then it is defined as

$$\text{Pf}(M) = \sum_{\pi} \epsilon_{\pi} w(i_1, i_2) w(i_3, i_4) \dots w(i_{2k-1}, i_{2k}),$$

where

- $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ is a permutation,
- summation is over all permutations π where $i_1 < i_2, i_3 < i_4, \dots, i_{2k-1} < i_{2k}$ and $i_1 < i_3 < \dots < i_{2k-1}$, and
- $\epsilon_{\pi} \in \{-1, 1\}$ is the sign of the permutation π , i.e., +1 for even permutations and -1 for odd permutations. Another equivalent definition of ϵ_{π} is that it is the sign or parity of the number of *overlapping* pairs where a pair of edges $(i_{2r-1}, i_{2r}), (i_{2s-1}, i_{2s})$ is overlapping iff $i_{2r-1} < i_{2s-1} < i_{2r} < i_{2s}$ or $i_{2s-1} < i_{2r-1} < i_{2s} < i_{2r}$.

The Pfaffian is computable in polynomial time. In particular, $(\text{Pf}(M))^2 = \det(M)$.

In the notation for the Pfaffian $\text{Pf}(i_1, \dots, i_r)$ of a submatrix consisting of rows and columns i_1, \dots, i_r , we implicitly assume the indices are in increasing order $i_1 < \dots < i_r$. If i_1, \dots, i_r are not in increasing order, the sign will vary according to the parity of the permutation, e.g., $\text{Pf}(i_2, i_1, \dots, i_r) = -\text{Pf}(i_1, i_2, \dots, i_r)$ and so on.

A matching is a subset of edges such that no two edges share a common vertex. A perfect matching is a matching which matches all vertices.

There is a graph-theoretic interpretation of the Pfaffian. If M is the matrix of a graph G , then there is a one-to-one correspondence between monomials in the Pfaffian and perfect matchings in G . The monomial $w(i_1, i_2) \dots w(i_{2k-1}, i_{2k})$ in $\text{Pf}(M)$ corresponds to the perfect matching

$\{(i_1, i_2), \dots, (i_{2k-1}, i_{2k})\}$ in G . The condition on the permutation implies that every perfect matching corresponds to exactly one monomial. The coefficient ϵ_π of this monomial is the parity of the number of overlapping pairs of edges, in the sense defined earlier.

The following theorem states the Grassmann-Plücker identities.

THEOREM 2.1 ([46]). *For any $n \times n$ skew-symmetric matrix M , and for any $I = \{i_1, \dots, i_K\} \subseteq [n]$ and $J = \{j_1, \dots, j_L\} \subseteq [n]$, the following are called the Grassmann-Plücker identities,*

$$(1) \quad \sum_{l=1}^L (-1)^l \text{Pf}(j_l, i_1, \dots, i_K) \text{Pf}(j_1, \dots, \hat{j}_l, \dots, j_L) \\ + \sum_{k=1}^K (-1)^k \text{Pf}(i_1, \dots, \hat{i}_k, \dots, i_K) \text{Pf}(i_k, j_1, \dots, j_L) = 0$$

where the notation \hat{j} denotes that this entry j is deleted.

Now we will restrict to planar graphs. A (planar) *matchgate* is a planar graph with some external nodes labeled as *input* and/or *output* nodes. We will only define matchgates with only input or only output nodes. Let $G = (V, E, W)$, $G' = (V', E', W')$ be weighted undirected planar graphs. A *generator matchgate* Γ is a tuple (G, X) where $X \subset V$ is a set of external *output* nodes. A *recognizer matchgate* Γ' is a tuple (G', Y) where $Y \subset V'$ is a set of external *input* nodes. The external nodes are ordered counter-clock wise on the external face. Γ is called an odd (resp. even) matchgate if it has an odd (resp. even) number of nodes. As combinatorial objects, a generator matchgate and a recognizer matchgate have no difference. It is the way they are used and how their assigned *signature* tensors are transformed which distinguish them.

Let $\mathbf{b} = [\mathbf{b}_0, \mathbf{b}_1] = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$ denote the standard basis of a vector space V . Define $\text{PerfMatch}(G) = \sum_M \prod_{(i,j) \in M} w_{ij}$ to be the sum over all perfect matchings M in G . Each matchgate is assigned a *signature* tensor. A generator Γ with m output nodes is assigned a contravariant tensor $\mathbf{G} \in V_0^m$ of type $\binom{m}{0}$. This tensor under the standard basis \mathbf{b} has the form

$$\sum G^{i_1 i_2 \dots i_m} \mathbf{b}_{i_1} \otimes \mathbf{b}_{i_2} \otimes \dots \otimes \mathbf{b}_{i_m},$$

where

$$G^{i_1 i_2 \dots i_m} = \text{PerfMatch}(G - Z),$$

and where Z is the subset of the output nodes having the characteristic sequence $\chi_Z = i_1 i_2 \dots i_m$. Similarly, a recognizer Γ' with m input nodes is assigned a covariant tensor $\mathbf{R} \in V_m^0$ of type $\binom{0}{m}$. This tensor under

the standard (dual) basis \mathbf{b}^* has the form

$$\sum R_{i_1 i_2 \dots i_m} \mathbf{b}^{i_1} \otimes \mathbf{b}^{i_2} \otimes \dots \otimes \mathbf{b}^{i_m},$$

where

$$R_{i_1 i_2 \dots i_m} = \text{PerfMatch}(G' - Z),$$

where Z is the subset of the input nodes having $\chi_Z = i_1 i_2 \dots i_m$.

In particular, \mathbf{G} transforms as a contravariant tensor under a basis transformation $\beta_j = \sum_i \mathbf{b}_i t_j^i$,

$$(G')^{i'_1 i'_2 \dots i'_m} = \sum G^{i_1 i_2 \dots i_m} \tilde{t}_{i'_1}^{i_1} \tilde{t}_{i'_2}^{i_2} \dots \tilde{t}_{i'_m}^{i_m},$$

where (\tilde{t}_j^i) is the inverse matrix of (t_j^i) . Similarly, \mathbf{R} transforms as a covariant tensor, namely

$$(R')_{i'_1 i'_2 \dots i'_m} = \sum R_{i_1 i_2 \dots i_m} t_{i'_1}^{i_1} t_{i'_2}^{i_2} \dots t_{i'_m}^{i_m}.$$

A signature is symmetric, if each entry only depends on the Hamming weight of the index. This notion is invariant under basis transformations. A symmetric signature is denoted by $[\sigma_0, \sigma_1, \dots, \sigma_m]$.

A *matchgrid* $\Omega = (A, B, C)$ is a weighted planar graph consisting of a disjoint union of: a set of g generators $A = (A_1, \dots, A_g)$, a set of r recognizers $B = (B_1, \dots, B_r)$, and a set of f connecting edges $C = (C_1, \dots, C_f)$, where each C_i edge has weight 1 and joins an output node of a generator with a input node of a recognizer, so that every input and output node in every constituent matchgate has exactly one such incident connecting edge.

Let $\mathbf{G} = \bigotimes_{i=1}^g \mathbf{G}(A_i)$ be the tensor product of all the generator signatures, and let $\mathbf{R} = \bigotimes_{j=1}^r \mathbf{R}(B_j)$ be the tensor product of all the recognizer signatures. Then $\text{Holant}(\Omega)$ is defined to be the contraction of the two product tensors, under some basis β , where the corresponding indices match up according to the f connecting edges C_k .

Valiant's Holant Theorem is

THEOREM 2.2 (Valiant). *For any matchgrid Ω over any basis β , let G be its underlying weighted graph; then*

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

The FKT algorithm can compute the perfect matching polynomial $\text{PerfMatch}(G)$ for a planar graph in polynomial time. The complexity of this algorithm is essentially the evaluation of a Pfaffian of a (modified) skew-symmetric matrix of the graph.

3. Some Holographic Algorithms

In this section, we list some problems which can be solved in polynomial time using holographic algorithms. The first several problems are all taken from the initial paper by Valiant [54].

We start with an “ice” problem motivated by statistical physics. An orientation of an undirected graph G is an assignment of a direction to each of its edges. An ice problem involves counting the number of orientations such that certain local constraints are satisfied. Pauling [47] initially proposed such a model for planar square lattices, where the constraint was that an orientation had to have incoming and outgoing degree two at every node. The question of determining how the number of such orientations grows for various planar repeating structures has been analyzed [38, 39, 40, 41, 5, 58]. However, more generally the range of natural counting problems for graph-theoretic problems for which there are polynomial time algorithms is very limited, including for “ice” problems.

#PL-3-NAE-ICE

INPUT: A planar graph $G = (V, E)$ of maximum degree 3.

OUTPUT: The number of orientations such that no node has all the edges directed towards it or all the edges directed away from it.

To solve this problem by a holographic algorithm, we design a matchgrid as follows: We represent each node of degree three in V by a recognizer matchgate with signature $(0, 1, 1, 1, 1, 1, 0)$. This represents a NOT-ALL-EQUAL or NAE gate. For any degree two node we use a recognizer matchgate with the binary NAE (i.e. NOT-EQUAL) gate signature $(0, 1, 1, 0)$. For each edge in E we use a generator matchgate with signature $(0, 1, 1, 0)$, which stands for an orientation from either of the two nodes to the other one (i.e., either $\beta_0 \otimes \beta_1$ or $\beta_1 \otimes \beta_0$, but not $\beta_0 \otimes \beta_0$ nor $\beta_1 \otimes \beta_1$). Then we connect the external nodes of these matchgates by an edge of weight 1, in a one-to-one fashion according to the given planar graph G . Now consider the exponential sum evaluated in the definition of the Holant under this basis β . Each term in the sum is a product of 0’s and 1’s which come from the appropriate entries of the signatures of the matchgates in the matchgrid. Each term is indexed by an assignment on every connecting edge between external nodes of these matchgates, which can be either β_0 or β_1 . Then it is not hard to see, when this exponential sum is evaluated over the basis β , each term is 0 or 1, and it is 1 iff it corresponds to an orientation of every edge such that at each vertex the local NOT-ALL-EQUAL constraint is satisfied. Thus, it follows that the Holant is precisely the number of valid orientations required by #PL-3-NAE-ICE. While we express the solution by the Holant under the basis β , algorithmically we evaluate the Holant by the FKT algorithm.

In the next section we will discuss the question of realizability of these signatures. We will see that these signatures are all realizable in the Hadamard basis $\left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right]$ (this is called **b2** in [54]).

The next problem is a Satisfiability problem.

#PL-3-NAE-SAT

INPUT: A planar formula Φ consisting of a conjunction of NOT-ALL-EQUAL clauses each of size 3.

OUTPUT: The number satisfying assignments of Φ .

This is a constrained satisfiability problem, where we are given a planar formula which is a Boolean conjunction of NOT-ALL-EQUAL clauses. Lichtenstein [37] defined the notion of planar formulae. A Boolean formula is planar if it can be represented by a planar graph where vertices represent variables and clauses, and there is an edge iff the variable or literal appears in that clause. The SAT problem is where the gate for each clause is the Boolean OR. When SAT is restricted to planar formulae it is still NP-complete. Moreover, for many connectives other than NOT-ALL-EQUAL (e.g., EXACTLY-ONE), the unrestricted or the planar decision problems are still NP-complete, and the corresponding counting problems are #P-complete [27].

To solve this problem by a holographic algorithm, we represent each NOT-ALL-EQUAL gate with the recognizer signature $(0, 1, 1, 1, 1, 1, 1, 0)$, and represent a Boolean variable having fan-out k with the generator signature for EQUALITY, namely $\beta_0 \otimes \beta_0 \otimes \cdots \otimes \beta_0 + \beta_1 \otimes \beta_1 \otimes \cdots \otimes \beta_1 = (1, 0, \dots, 0, 1)$ (there are $2^k - 2$ zeroes). Again we will see in the next section these signatures are realizable in the Hadamard basis.

The next problem is essentially a decision problem, rather than a counting problem.

PL-NODE-BIPARTITION

INPUT: A planar graph $G = (V, E)$ of maximum degree 3.

OUTPUT: The cardinality of a smallest subset $V' \subset V$ such that the deletion of V' and its incident edges results in a bipartite graph.

This problem is known to be NP-complete for maximum degree 6 [33]. See [35] for a general approach to such “node deletion” problems. Note that numerous other planar NP-complete problems, such as Hamiltonian cycles and minimum vertex covers, are NP-complete already for degree 3 (e.g., [20], and [19]).

For this problem, Valiant introduced another idea of applying the general machinery of the Holant. We will see that with an arbitrary real value x , the recognizer signature $(x, 1, 1, 1, 1, 1, 1, x)$ and $(x, 1, 1, x)$ are both realizable, and moreover it is simultaneously realizable with the generator signature $(0, 1, 1, 0)$, all over the Hadamard basis. The signature $(0, 1, 1, 0)$ can be used to effect an ORIENTATION gate. Now if we use the ORIENTATION gate for an edge, and the above recognizer

signatures for a node of degree 3 or 2 respectively, then a node that has its incident edges either all oriented away from it or all oriented toward it will contribute a factor x . In the other cases, namely when some edges are oriented away from it and some are oriented toward it, the node will contribute a factor 1. These terms are then summed up in the exponential sum in the Holant, which we evaluate over the Hadamard basis where the signatures are realized. Thus, in the final outcome, the Holant is a polynomial in x , where the largest i for which x^i has a non-zero coefficient is exactly the maximum number of nodes that a bipartite graph can have that is obtained by deleting nodes and incident edges from G .

Now this polynomial can have maximum possible degree at most $|V|$. Thus by evaluating the Holant at $|V| + 1$ distinct values of x , we can interpolate the polynomial and reconstruct it. Consequently, we can find its actual degree d , which gives $|V| - d$ as the answer to the instance of PL-NODE-BIPARTITION.

We also note that if instead of considering node deletion we consider edge deletion, this is just another way of defining the well known problem of MAX-CUT, which is NP-hard (and even NP-hard to approximate [22, 3, 26]). The holographic algorithm by Valiant above is the first polynomial time algorithm for PL-NODE-BIPARTITION [54]. On the other hand, planar MAX-CUT is known to be in P [24]. In [6] a joint generalization was shown to be also solvable in polynomial time by holographic algorithms.

PL-NODE-EDGE-BIPARTITION

INPUT: A planar graph $G = (V, E)$ of maximum degree 3. A non-negative integer $k \leq |V|$.

OUTPUT: The minimal l such that deletion of at most k nodes (including all of their incident edges) and l more edges results in a bipartite graph.

The holographic algorithm for this problem is slightly more complicated, but follows generally the same methodology as Valiant's algorithm for PL-NODE-BIPARTITION. The interpolation method is again crucial.

We now consider a matching problem. We note that Jerrum [28] showed that counting the number of (not necessarily perfect) matchings in a planar graph is #P-complete, and Vadhan [51] subsequently proved that it remains #P-complete even for planar bipartite graphs of degree six. For degree two the problem can be solved easily, and one might have conjectured that all other nontrivial cases are #P-complete. However, Valiant showed that the following problem can be solved in polynomial time.

#X-MATCHINGS

INPUT: A planar weighted bipartite graph $G = (V, E, W)$ where V has bipartition V_1, V_2 and the nodes in V_1 have degree 2.

OUTPUT: The sum of the masses of all matchings of all sizes where the mass of a matching is the product of (i) the weights of all the edges present in the matching, as well as of the quantity, (ii) “ $-(w_1 + \dots + w_k)$ ” for all the V_2 nodes that are not matched, where w_1, \dots, w_k are the weights of the edges incident to that (unmatched) node.

Note that if every V_2 node has degree 4 and every edge has weight one, then computing #X-MATCHINGS gives the number of matchings, but each weighted by $(-4)^k$, where k is the number of unmatched V_2 nodes. Computing this mod 5 gives the number of matchings mod 5.

At this point we may want to pause and reflect a bit. While the factor $-(w_1 + \dots + w_k)$ may appear contrived, there is nothing contrived about mod 5. In fact, one will be hard pressed to think of any other polynomial time algorithm computing this problem mod 5. One may have conjectured that it is complete for Mod_5P , a complexity class which is hard for NP under randomized reductions.

To solve this problem, we use a different basis $\beta = \left[\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]$.

Valiant showed that suitable signatures can be realized under this basis with appropriate matchgates [54].

This problem is motivated by its proximity to counting the number of (not necessarily perfect) matchings in a planar graph, which is #P-complete [28]. Still, the quantity $-(w_1 + \dots + w_k)$ seems a little artificial. If one were to be able to replace $-(w_1 + \dots + w_k)$ by 1, then one would be able to count all (not necessarily perfect) matchings in such planar bipartite graphs. In [6] we proved that a direct adaptation with suitable signatures by dropping the $-(w_1 + \dots + w_k)$ factor *cannot* be done by a holographic algorithm. In that paper we defined a restricted class of holographic algorithms called holographic templates. Without going into the formal definitions of holographic templates, we quote

THEOREM 3.1. *There is no holographic template using any basis of two linearly independent vectors to solve the counting problem for all (not necessarily perfect) matchings for these graphs, which is the same as the above problem with $-(w_1 + \dots + w_k)$ replaced by 1.*

Now we consider a curious Satisfiability counting problem.

#₇PI-Rtw-Mon-3CNF

INPUT: A planar 3CNF Boolean formula where each variable appears positively and in exactly two clauses (Planar, Read-Twice, Monotone, 3CNF.)

OUTPUT: Count the number of satisfying assignments modulo 7.

Let us first consider simply the counting problem for this restricted class of Boolean formulae, which is denoted as $\#PI\text{-}Rtw\text{-}Mon\text{-}3CNF$. This problem is known to be $\#P$ -complete. For a given planar, read-twice, monotone formula Φ , we can express its number of satisfying assignments as an exponential sum in the form of a Holant as follows: For each clause C in Φ with 3 variables we would like the signature $R_C = (0, 1, 1, 1, 1, 1, 1, 1)$, where the entries are indexed by 3 bits $b_1b_2b_3 \in \{0, 1\}^3$. Here $b_1b_2b_3$ corresponds to a truth assignment to the 3 variables. Therefore, R_C corresponds to a Boolean OR gate. Suppose in the formula Φ a Boolean variable x appears in two clauses C and C' . Then we would like to have the signature $G_x = (1, 0, 0, 1)^T$, indexed by $b_1b_2 \in \{0, 1\}^2$, to indicate that the fan-out value from x to C and C' must be consistent, i.e., they must be either 00 or 11. Then we form the tensor products as in the construction of a Holant, $\mathbf{R} = \bigotimes_C R_C$ and $\mathbf{G} = \bigotimes_x G_x$. Suppose in the planar formula Φ there are exactly e edges connecting various x 's to various C 's; then both \mathbf{R} and \mathbf{G} have e indices, each taking values in $\{0, 1\}$, and both tensors have 2^e entries. The indices of $\mathbf{R} = (R_{i_1i_2\dots i_e})$ and $\mathbf{G} = (G^{i_1i_2\dots i_e})$ match up one-to-one according to which x appears in which C . Then the exponential sum $\langle \mathbf{R}, \mathbf{G} \rangle = \sum_{i_1, i_2, \dots, i_e \in \{0, 1\}} R_{i_1i_2\dots i_e} G^{i_1i_2\dots i_e}$ counts exactly the number of satisfying assignments to Φ . This is because each tuple $(i_1, i_2, \dots, i_e) \in \{0, 1\}^e$ assigns a value 0 or 1 to each connecting edge, and the product $R_{i_1i_2\dots i_e} G^{i_1i_2\dots i_e}$ is 1 when this is a consistent assignment of truth values to each variable and the truth assignment satisfies each clause; the product value is 0 otherwise.

Now the question is whether one can find all the needed signatures. (If one could, then $P = NP = \#P$.) It turns out that these signatures are not realizable over the field \mathbf{C} of characteristic 0, but they are realizable over a field of characteristic 7. This gives the polynomial time algorithm for the problem $\#_7PI\text{-}Rtw\text{-}Mon\text{-}3CNF$.

We note that in addition to the $\#P$ -completeness of the counting problem itself, it is also known that counting mod 2, i.e., $\#_2PI\text{-}Rtw\text{-}Mon\text{-}3CNF$ is NP-hard by a randomized reduction. Put in this context, this success with counting mod 7 is rather extraordinary. One might not have guessed that solving the problem modulo 7 is any easier than solving it mod 2 (*or is it?*). Finding the signatures and matchgates in the mod 7 case comes about by algebraic means, and is not intuitively obvious. Likewise, to show that suitable signatures exist only in characteristic 7 is also obtained algebraically, and not combinatorially obvious.

This brings us to the central interest of this subject, at least to this author. Our generally accepted conjecture of $NP \neq P$ is just a conjecture. We think it has been supported by our experience with the usual algorithmic paradigms which seem not to be applicable to NP-hard problems. But we don't have strong provable lower bounds for general models of computation. In the meanwhile, holographic algorithms produce exotic algorithms for which we have little experience. Our current conception of what a polynomial time algorithm can do may be inadequate. It is even conceivable that they lead to a collapse of complexity classes. So the attraction is from a complexity theoretic perspective. It is not so much about the particular problems that can be solved by this approach, but what it says to us about the limitations and unfamiliar ways of doing polynomial time computation, and our inadequate understanding of the ultimate reach of all polynomial time algorithms. For $NP \neq P$ and other standard conjectures in complexity theory to remain credible, we feel that they should all be re-examined against this new algorithm design paradigm.

We think the first step to develop the theory of holographic algorithms is to develop a coherent theory of realizable signatures. The search for a holographic algorithm for a particular combinatorial problem typically boils down to the existence of suitable signatures in a suitable tensor space. In general, realizability is specified by a family of algebraic equations called Matchgate Identities (MGI). This will be discussed in Section 5. These families of equations are non-linear, exponential in size, and difficult to handle. But whenever we find a suitable solution, we get an exotic polynomial time algorithm. Searching for these signatures is what Valiant called the “enumerative” form in [57]. Quoting Valiant [57]: “The objects enumerated are sets of polynomial systems such that the solvability of any one member would give a polynomial time algorithm for a specific problem ... the situation with the $P = NP$ question is not dissimilar to that of other unresolved enumerative conjectures in mathematics. The possibility that accidental or freak objects in the enumeration exist cannot be discounted, if the objects in the enumeration have not been systematically studied previously.”

We now return to the problem $\#_7\text{Pl-Rtw-Mon-3CNF}$. There is another aspect that is remarkable about Valiant's solution of this problem [57]. In holographic algorithms, since the underlying computation is ultimately reduced to perfect matchings, the linear basis vectors which express the computation are necessarily of dimension 2^k , for some integer k . This k is called the size of the basis. Most holographic algorithms so far [54, 7, 6, 57] use bases of size 1. (In this survey we have restricted the discussion to bases of size 1.) Surprisingly, Valiant's algorithm for $\#_7\text{Pl-Rtw-Mon-3CNF}$ used a basis of size 2. Utilizing bases of a higher dimension has always been a theoretical possibility, which may further

extend the reach of holographic algorithms. Valiant’s algorithm makes it realistic, and this freedom would have given us an infinite set of possibilities in which an exotic or “freak” object may materialize, leading to the collapse of complexity classes.

However, it has been shown that a universal bases collapse theorem [12] holds for holographic algorithms: Any holographic algorithm using two basis vectors of arbitrary size k can be simulated by a holographic algorithm using another basis of size 1. This cuts off a potentially infinite family of possible ways to achieve a collapse of complexity classes. However, holographic algorithms may use more than two bases vectors as well as in higher dimensions. In that case, whether there is a universal bases collapse is still open. Interested readers are referred to [11, 12] for more details.

Finally, we consider a geometric problem.

2-COLOR-COUNTING

INPUT: Given a set S of n points on a plane, where no three points are colinear. Also given a set of straight line segments between some pairs of points in S . We assume no 3 line segments intersect at a point ($\notin S$). Every point of S is incident to either 2 or 3 line segments.

OUTPUT: The number of 2-colorings for the line segments which satisfy the following conditions: (1) for every point in S , the incident line segments are not monochromatic; (2) when two line segments cross over each other, they have different colors.

For most holographic algorithms, the signatures needed are typically symmetric signatures which will be discussed in more detail in Section 4. For this problem 2-COLOR-COUNTING we will use unsymmetric signatures in our holographic algorithm. The theory of unsymmetric signatures have not been fully developed. The existence of the unsymmetric signatures for 2-COLOR-COUNTING follows from a difficult classification theorem in Section 6.

Another notable feature about 2-COLOR-COUNTING is that the problem is not *a priori* stated for a planar graph. It is in the process of forming the matchgrid that we obtain a planar graph.

There are several more problems that have been solved using holographic algorithms [54, 57, 7, 6, 10]. Interested readers are referred to these papers for more details.

4. Symmetric Signatures

As seen from the examples, the general outline of the design of a holographic algorithm consists of two parts as follows: (1) some suitable linear basis vectors and (2) some suitable matchgates. Typically a linear basis consists of two linearly independent vectors $\beta = [\beta_0, \beta_1]$. The

matchgates are used in two dual roles, as generators and recognizers. Before the basis transformation there is no real difference between generators and recognizers; they both define standard signatures $G^{i_1 i_2 \dots i_m} = \text{PerfMatch}(G - Z)$ (and similarly $R_{i_1 i_2 \dots i_m}$), where Z is the subset of the output nodes having the characteristic sequence $\chi_Z = i_1 i_2 \dots i_m$. However, the idea is to transform these standard signatures under the basis transformation $\beta_j = \sum_i \mathbf{b}_i t_j^i$, where $\mathbf{b} = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$ is the standard basis, to produce the *signatures*

$$\begin{aligned} (G')^{i'_1 i'_2 \dots i'_m} &= \sum G^{i_1 i_2 \dots i_m} \tilde{t}_{i'_1}^{i_1} \tilde{t}_{i'_2}^{i_2} \dots \tilde{t}_{i'_m}^{i_m}, \text{ and } (R')^{i'_1 i'_2 \dots i'_m} \\ &= \sum R_{i_1 i_2 \dots i_m} t_{i'_1}^{i_1} t_{i'_2}^{i_2} \dots t_{i'_m}^{i_m}, \end{aligned}$$

which are the entities that have some intended meanings.

For example, to express the meaning of Boolean OR of three bits, we want a recognizer signature which has dimension 8, and indexed by three bits $b_1 b_2 b_3 \in \{0, 1\}^3$, namely $(0, 1, 1, 1, 1, 1, 1, 1)$. This indicates that for the input bit pattern 000, this signature assigns the multiplier 0 and thus does not “recognize” it, but for all other “satisfiable” input bit patterns this signature assigns the multiplier 1, and thus “accepts” them. Clearly this signature is suitable for the problem of 3SAT for Boolean Satisfiability on the clause side. Note that this 8-dimensional tensor is not realizable by a matchgate as a standard signature. In this case we can give a simple reason for it. Standard signatures must satisfy the parity constraint, namely either all entries indexed by bit patterns with odd Hamming weights are zero or all entries indexed by bit patterns with even Hamming weights are zero. This parity constraint is a simple consequence of being a perfect matching. Later we will discuss more subtle constraints, called Matchgate Identities.

However, while $(0, 1, 1, 1, 1, 1, 1, 1)$ cannot be realized as a standard signature, under a suitable basis transformation, it *can* be realized as a signature. More concretely, if we take the basis

$$\left[\begin{pmatrix} 1 + \omega \\ 1 - \omega \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right],$$

where $\omega^3 = 1$ is a primitive third root of unity, then there in fact exists a matchgate with three external nodes with the standard signature

$$(R_{i_1 i_2 i_3}) = (0, 1, 1, 1, 1, 1, 1, 1) \left(\begin{pmatrix} 1 + \omega & 1 \\ 1 - \omega & 1 \end{pmatrix}^{-1} \right)^{\otimes 3}.$$

Indeed, we can calculate, up to a scalar multiple of $1/8$, $\left(\begin{pmatrix} 1+\omega & 1 \\ 1-\omega & 1 \end{pmatrix}^{-1}\right)^{\otimes 3}$ is

$$\begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ -1+\omega & 1+\omega & 1-\omega & -1-\omega & 1-\omega & -1-\omega & -1+\omega & 1+\omega \\ -1+\omega & 1-\omega & 1+\omega & -1-\omega & 1-\omega & -1+\omega & -1-\omega & 1+\omega \\ -3\omega & -2-\omega & -2-\omega & \omega & 3\omega & 2+\omega & 2+\omega & -\omega \\ -1+\omega & 1-\omega & 1-\omega & -1+\omega & 1+\omega & -1-\omega & -1-\omega & 1+\omega \\ -3\omega & -2-\omega & 3\omega & 2+\omega & -2-\omega & \omega & 2+\omega & -\omega \\ -3\omega & 3\omega & -2-\omega & 2+\omega & -2-\omega & 2+\omega & \omega & -\omega \\ 3+6\omega & 3 & 3 & -1-2\omega & 3 & -1-2\omega & -1-2\omega & -1 \end{pmatrix}$$

and by adding the last 7 rows we get

$$(R_{i_1 i_2 i_3}) = \frac{1}{4}(0, 1, 1, 0, 1, 0, 0, 1).$$

This is realizable as the standard signature of a planar matchgate with three external nodes; for example, we can take a disjoint union of an edge with weight $1/4$, together with a triangle. The 3 edges of the triangle all have weight 1 and the 3 vertices are the external nodes.

The signature $(0, 1, 1, 1, 1, 1, 1, 1)$ is a symmetric signature, i.e., the value of each entry only depends on the Hamming weight of the index. This notion is invariant under a basis transformation. A symmetric signature of arity m is denoted by a more compact notation with $m+1$ entries (instead of 2^m entries), $[z_0, z_1, \dots, z_m]$, where z_i denotes the signature value at an entry of index of weight i . Thus the Boolean OR signature above on 3 bits is denoted as $[0, 1, 1, 1]$.

Symmetric signatures are often convenient for the design of holographic algorithms, as they have easily interpretable combinatorial meanings. For symmetric signatures Cai and Lu [9] have achieved a complete characterization of their realizability. These tell us exactly what signatures can be realized over *some* bases.

THEOREM 4.1. *A symmetric signature $[x_0, x_1, \dots, x_m]$ for a recognizer is realizable under the basis $\beta = [n, p] = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$ iff it takes one of the following forms:*

- *Form 1: there exist (arbitrary) constants λ, s, t and ϵ where $\epsilon = \pm 1$, such that for all $i, 0 \leq i \leq m$,*
- (2) $x_i = \lambda[(sn_0 + tn_1)^{m-i}(sp_0 + tp_1)^i + \epsilon(sn_0 - tn_1)^{m-i}(sp_0 - tp_1)^i].$
- *Form 2: there exist (arbitrary) constants λ , such that for all $i, 0 \leq i \leq m$,*
- (3) $x_i = \lambda[(m-i)n_0(p_1)^i(n_1)^{m-1-i} + ip_0(p_1)^{i-1}(n_1)^{m-i}].$

- *Form 3: there exist (arbitrary) constants λ , such that for all $i, 0 \leq i \leq m$,*

$$(4) \quad x_i = \lambda[(m-i)n_1(p_0)^i(n_0)^{m-1-i} + ip_1(p_0)^{i-1}(n_0)^{m-i}].$$

A similar theorem holds for generators. These theorems are proved by applying the Matchgate Identities. See Section 5.

There is another characterization theorem, assuming the characteristic of the field $p \neq 2$ and $p \nmid m$.

THEOREM 4.2. *A symmetric signature $[x_0, x_1, \dots, x_m]$ is realizable on some basis of size 1 iff there exist three constants a, b, c (not all zero), such that $\forall k, 0 \leq k \leq m-2$,*

$$(5) \quad ax_k + bx_{k+1} + cx_{k+2} = 0.$$

These characterization theorems are very informative, but they do not tell the whole story. To construct a holographic algorithm, one needs to realize some generators and recognizers simultaneously.

To discuss this simultaneous realizability, we first need the following simple lemma:

LEMMA 4.1 (Valiant, [54]). *If there is a generator (recognizer) with a certain signature for size one basis $\left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$ then there is a generator (recognizer) with the same signature for size one basis $\left[\begin{pmatrix} xn_0 \\ yn_1 \end{pmatrix}, \begin{pmatrix} xp_0 \\ yp_1 \end{pmatrix}\right]$ or $\left[\begin{pmatrix} xn_1 \\ yn_0 \end{pmatrix}, \begin{pmatrix} xp_1 \\ yp_0 \end{pmatrix}\right]$ for any $x, y \in \mathbf{F}$ and $xy \neq 0$.*

This leads to the following definition of an equivalence relation:

DEFINITION 4.1. Two bases $\beta = [n, p] = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$ and $\beta' = [n', p'] = \left[\begin{pmatrix} n'_0 \\ n'_1 \end{pmatrix}, \begin{pmatrix} p'_0 \\ p'_1 \end{pmatrix}\right]$ are equivalent, denoted by $\beta \sim \beta'$, iff there exist $x, y \in \mathbf{F}^*$ such that

$$n'_0 = xn_0, p'_0 = xp_0, n'_1 = yn_1, p'_1 = yp_1,$$

or

$$n'_0 = xn_1, p'_0 = xp_1, n'_1 = yn_0, p'_1 = yp_0.$$

LEMMA 4.2. $\text{GL}_2(\mathbf{F})/\sim$ is a two dimensional manifold (for $\mathbf{F} = \mathbf{C}$ or \mathbf{R}). For $\mathbf{F} = \mathbf{R}$, \mathcal{M} is topologically a Möbius strip.

We call this the *basis manifold* \mathcal{M} . From now on we identify a basis β with its equivalence class containing it. When it is permissible, we use the dehomogenized coordinates $\begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}$ to represent a point (i.e., a basis class) in \mathcal{M} . We will assume $\text{char.}\mathbf{F} \neq 2$.

In terms of \mathcal{M} , a given generator (recognizer) defines a (possibly empty) subvariety which consists of all the bases over which it is realizable. The simultaneous realizability is equivalent to a non-empty intersection of these subvarieties. Thus, we have to go beyond Theorem 4.1 and Theorem 4.2. For every signature which is realizable according to these theorems, we need to determine the subvariety where it is realizable.

DEFINITION 4.2.

Let $B_{rec}([x_0, x_1, \dots, x_n])$ (resp. $B_{gen}([x_0, x_1, \dots, x_n])$) be the set of all possible bases in \mathcal{M} for which a symmetric signature $[x_0, x_1, \dots, x_n]$ for a recognizer (resp. a generator) is realizable. We also use $B_{rec}(R)$ and $B_{gen}(G)$ for possibly unsymmetric signatures.

We will state the results for the recognizers. The results for the generators are similar. Since the identical zero signature is realizable in every basis, we will assume the signature is non-zero in the following discussion.

The following lemmas give a complete and mutually exclusive list of realizable symmetric signatures for recognizers.

LEMMA 4.3.

$$B_{rec}([a^m, a^{m-1}b, \dots, b^m]) = \left\{ \left[\binom{a}{n_1}, \binom{b}{p_1} \right] \in \mathcal{M} \mid n_1, p_1 \in \mathbf{F} \right\}.$$

Remark: Every signature with arity $m = 1$ is trivially of this form.

LEMMA 4.4.

$$B_{rec}([x_0, x_1, x_2]) = \left\{ \left[\binom{n_0}{n_1}, \binom{p_0}{p_1} \right] \in \mathcal{M} \mid \begin{array}{l} x_0 p_1^2 - 2x_1 p_1 n_1 + x_2 n_1^2 = 0, x_0 p_0^2 - 2x_1 p_0 n_0 + x_2 n_0^2 = 0 \\ \text{or } x_0 p_0 p_1 - x_1(n_0 p_1 + n_1 p_0) + x_2 n_0 n_1 = 0 \end{array} \right\}.$$

In the following the matchgate arity m is ≥ 3 .

LEMMA 4.5. Let $\lambda_1 \neq 0$. Suppose $p = \text{char} \mathbf{F} \nmid m$,

$$B_{rec}([0, 0, \dots, 0, \lambda_1, \lambda_2]) = \left\{ \left[\binom{0}{m\lambda_1}, \binom{1}{\lambda_2} \right] \right\}.$$

For $p \mid m$ and $\lambda_2 = 0$,

$$B_{rec}([0, 0, \dots, 0, \lambda_1, 0]) = \left\{ \left[\binom{0}{n_1}, \binom{1}{p_1} \right] \in \mathcal{M} \mid n_1, p_1 \in \mathbf{F} \right\}.$$

For $p \mid m$ and $\lambda_2 \neq 0$, then $[0, 0, \dots, 0, \lambda_1, \lambda_2]$ is not realizable.

LEMMA 4.6. For $AB \neq 0$,

$$B_{rec}([A, A\alpha, A\alpha^2, \dots, A\alpha^m + B]) = \left\{ \left[\binom{1}{1}, \binom{\alpha + \omega}{\alpha - \omega} \right] \mid \omega^m = \pm \frac{B}{A} \right\}.$$

For example, the EQUALITY gate $(1, 0, \dots, 0, 1)$ (there are $2^m - 2$ zeroes) that was used for $\#PL\text{-}3\text{-}NAE\text{-}SAT$ can be obtained by choosing $A = B = 1$ and $\alpha = 0$.

In terms of the formulation from Theorem 4.2, the other cases of Theorem 4.2 have the property that the a, b and c (in the theorem statement) are unique up to a scaling factor and $c \neq 0$. So we have a unique characteristic equation $cx^2 + bx + a = 0$, which has two roots α and β . If $\alpha \neq \beta$, we have the following lemma:

LEMMA 4.7. *For $AB \neq 0$ and $\alpha \neq \beta$,*

$$\begin{aligned} B_{rec}([A\alpha^i + B\beta^i | i = 0, 1, \dots, m]) \\ = \left\{ \left[\begin{pmatrix} 1 + \omega \\ 1 - \omega \end{pmatrix}, \begin{pmatrix} \alpha + \beta\omega \\ \alpha - \beta\omega \end{pmatrix} \right] \middle| \omega^m = \pm \frac{B}{A} \right\}. \end{aligned}$$

Remark: We denote $0^0 = 1$.

For example, the NOT-ALL-EQUAL gates of arity 3 can be obtained by choosing $A = 1, B = -1$, and choosing α, β to be the two roots of $x^2 - x + 1 = 0$. Then we have

$$B_{rec}([0, 1, 1, 0]) = \left\{ \left[\begin{pmatrix} 1 + \omega \\ 1 - \omega \end{pmatrix}, \begin{pmatrix} \alpha + \beta\omega \\ \alpha - \beta\omega \end{pmatrix} \right] \middle| \omega^3 = \pm 1 \right\}.$$

Notice that $\alpha^3 = -1$ and $\alpha\beta = 1$, let $\omega = \alpha$, we have (using \sim on \mathcal{M})

$$\left[\begin{pmatrix} 1 + \omega \\ 1 - \omega \end{pmatrix}, \begin{pmatrix} \alpha + \beta\omega \\ \alpha - \beta\omega \end{pmatrix} \right] = \left[\begin{pmatrix} 1 + \alpha \\ 1 - \alpha \end{pmatrix}, \begin{pmatrix} \alpha + 1 \\ \alpha - 1 \end{pmatrix} \right] = \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right],$$

arriving at the Hadamard basis.

However, we can only realize the symmetric NAE signatures $[0, 1, 0]$ and $[0, 1, 1, 0]$ of arity 2 and 3. For $m > 3$ the symmetric signature $[0, 1, 1, \dots, 1, 0]$ (there are $m - 1$ 1's) is not realizable. (This was first proved in [6] by a complicated proof; but it follows from these characterization theorems as an easy consequence.) This explains why for many problems solved by holographic algorithms there is a restriction of “maximum degree 3”.

If $\alpha = \beta$, we have the following lemma:

LEMMA 4.8. *Let $p = \text{char.}\mathbf{F}$ and let $A \neq 0$.*

Case 1: $p = 0$ or $p \nmid m$.

$$B_{rec}([A\alpha^{i-1} + B\alpha^i | i = 0, 1, \dots, m]) = \left\{ \left[\begin{pmatrix} 1 \\ B \end{pmatrix}, \begin{pmatrix} \alpha \\ mA + B\alpha \end{pmatrix} \right] \right\}.$$

Case 2: $p|m$ and $x_0 = 0$; in this case, the signature is of the form $Ai\alpha^{i-1}$.

$$B_{rec}([A\alpha^{i-1} | i = 0, 1, \dots, m]) = \left\{ \left[\begin{pmatrix} 1 \\ n_1 \end{pmatrix}, \begin{pmatrix} \alpha \\ p_1 \end{pmatrix} \right] \in \mathcal{M} \middle| n_1, p_1 \in \mathbf{F} \right\}.$$

Case 3: $p|m$ and $x_0 \neq 0$. Then it's not realizable.

Remark: If $\alpha = 0$, and $i = 0$, we still denote $i\alpha^{i-1} = 0$, and also $\alpha^i = 1$.

DEFINITION 4.3. The Simultaneous Realizability Problem (SRP):

Input: A set of symmetric signatures for generators and/or recognizers.

Output: A common basis of these signatures if any basis exists; “NO” if they are not simultaneously realizable.

Algorithm:

For every signature $[x_0, x_1, \dots, x_m]$, check if it satisfies Theorem 4.2. If not, output “NO” and halt.

Otherwise find $B_{gen}([x_0, x_1, \dots, x_m])$ or $B_{rec}([x_0, x_1, \dots, x_m])$ according to one of the Lemmas.

Check if these subvarieties have a non-empty intersection.

THEOREM 4.3. *This is a polynomial time algorithm for SRP.*

With the help of these characterization theorems, we can have a better understanding of, for example, why mod 7 is the only modulus that works for $\#_7\text{Pl-Rtw-Mon-3CNF}$. Moreover, we can obtain non-trivial generalizations to all Mersenne numbers of the form $2^k - 1$.

$\#_{2^k-1}\text{Pl-Rtw-Mon-}k\text{CNF}$

INPUT: A planar $k\text{CNF}$ Boolean formula which is monotone and read-twice.

OUTPUT: Count the number of satisfying assignments modulo $2^k - 1$.

We can also find some other exotic holographic algorithms.

$\#_{k+1}2/k\text{-X-MATCHINGS}$

INPUT: A planar bipartite graph $G = (V_1, V_2, E)$. Nodes in V_1 and V_2 have degrees 2 and k respectively.

OUTPUT: The number mod $(k+1)$ of all (not necessarily perfect) matchings.

5. Admissibility and Realizability

The theory of symmetric signatures has been satisfactorily developed. Symmetric signatures are particularly useful because they have clear combinatorial meanings. However, general (i.e., unsymmetric) signatures can also be useful. To understand completely the power of holographic algorithms, we must also study unsymmetric signatures as well. (In the following, we discuss generators only; the situation for recognizers is similar.)

We will denote the contravariant tensor for a generator in the form implicitly under a basis, $G = (G^S)$ where $S \subset [m]$, and $G^S = G^{\chi_S(1)\chi_S(2)\dots\chi_S(m)}$. A generator signature G is realizable on a basis β

iff the standard signature $\underline{G} = \beta^{\otimes m} G$ can be realized by some planar matchgate.

There are two conditions for a standard signature to be realizable:

Parity Constraint: Either $\underline{G}^S = 0$ for all $|S|$ even, or $\underline{G}^S = 0$ for all $|S|$ odd.

Matchgate Identities: \underline{G} satisfies all the *useful Grassmann-Plücker identities*.

The Parity Constraint is a consequence of the properties of being a perfect matching. Namely, if a matchgate realizing the signature has an even number of nodes (these are called even matchgates), then $\underline{G}^S = 0$ for all $|S|$ odd; similarly for matchgates with an odd number of nodes (odd matchgates), $\underline{G}^S = 0$ for all $|S|$ even.

The Matchgate Identities are derived from the Grassmann-Plücker identities (1), and can be stated as follows:

A pattern α is an m -bit string, i.e., $\alpha \in \{0, 1\}^m$. A position vector $P = \{p_i\}, i \in [l]$, is a subsequence of $\{1, 2, \dots, m\}$, i.e., $p_i \in [m]$ and $p_1 < p_2 < \dots < p_l$. We also use p to denote the m -bit string, whose (p_1, p_2, \dots, p_l) -th bits are 1 and others are 0. Let $e_i \in \{0, 1\}^m$ be the pattern with 1 in the i -th bit and 0 elsewhere. Let $\alpha + \beta$ be the pattern obtained from bitwise XOR the patterns α and β . Then for any pattern $\alpha \in \{0, 1\}^m$ and any position vector $P = \{p_i\}, i \in [l]$, we have the following identity:

$$(6) \quad \sum_{i=1}^l (-1)^i \underline{G}^{\alpha+e_{p_i}} \underline{G}^{\alpha+p+e_{p_i}} = 0.$$

THEOREM 5.1 ([6, 8]). *A tensor $\mathbf{G} = (G^{i_1, \dots, i_m})$ is realizable as the standard signature of some planar matchgate iff it satisfies all the Parity Constraint and (6) for all α and P .*

Prior to introducing holographic algorithms, Valiant had written a highly influential paper [52] in which he introduced (not necessarily planar) matchgates, and the theory of matchcircuits and characters associated with these (general, non-planar) matchgates. Valiant showed that a non-trivial fragment of quantum circuit computation can be simulated by these matchcircuits in polynomial time. In this matchcircuit theory, each matchgate Γ is assigned a character $\chi(\Gamma)$, somewhat similar to a signature. They are defined in terms of Pfaffians, together with a carefully defined factor called the “modifier”, which is designed to produce the right sign factors when a composition theorem for the matchcircuit is proved. We do not intend to discuss this theory in much detail in this survey, but the proof of Theorem 5.1 is ultimately connected to this Pfaffian based character theory. It is achieved in two steps. We first achieve a complete algebraic characterization of realizable character tensors: A necessary and sufficient condition for a tensor to be the

character tensor of some (general, not necessarily planar) matchgate. This characterization is in terms of a set of *useful* Grassmann-Plücker identities [8].

The second step is to prove a unification between the match-circuit/character theory and the matchgrid/signature theory [6, 8]. Roughly speaking, this unification is proved as follows. Given a planar matchgate with a standard signature \underline{G} , defined by the perfect matching polynomial PerfMatch , one can use the FKT algorithm to show that each entry of \underline{G} is equal to the Pfaffian of a submatrix of a *single* skew-symmetric matrix with a corresponding set of appropriate rows and columns deleted. This becomes an entry of the character of a matchgate. The FKT algorithm is applied simultaneously to the exponentially many induced subgraphs of the original planar matchgate with various external nodes removed. Due to a property of the FKT algorithm, it gives a single consistent orientation to produce the modified weighted graph, which is good for all entries of the signature to character identification. The reverse direction is more interesting. We take a general (not necessarily planar) matchgate Γ with a character $\chi(\Gamma)$, and realize it as the signature of a planar matchgate. This is done by an embedding of all the vertices of Γ on a convex curve *in the given order as in* Γ , and then replacing each physical crossing of a pair of edges by a planar crossover gadget. This produces a planar matchgate Γ' . One then argues that the PerfMatch value for each signature entry of Γ' is the same as the corresponding Pfaffian value of the character $\chi(\Gamma)$.

It follows that the set of *useful* Grassmann-Plücker identities also applies to signatures of planar matchgates, as necessary and sufficient conditions. Theorem 5.1 follows from that.

If we apply this to the class of symmetric signatures, we have

LEMMA 5.1. *Suppose Γ is an even matchgate with symmetric standard signature $[z_0, \dots, z_m]$. Then for all odd i , $z_i = 0$, and there exist r_1 and r_2 not both zero, such that for every even $2 \leq k \leq m$,*

$$r_1 z_{k-2} = r_2 z_k.$$

A similar statement holds for odd matchgates.

For $m \leq 3$ the condition $r_1 z_{k-2} = r_2 z_k$ is always satisfiable for some r_1 and r_2 not both zero.

Let $m \geq 4$, we use matchgate identities (6). Consider the pattern 1000α where α has Hamming weight $2i$, and $0 \leq 2i \leq m-4$. Let the position vector be $11110\dots 0$. Then (6) gives

$$\underline{G}^{0000\alpha} \underline{G}^{1111\alpha} - \underline{G}^{1100\alpha} \underline{G}^{0011\alpha} + \underline{G}^{1010\alpha} \underline{G}^{0101\alpha} - \underline{G}^{1001\alpha} \underline{G}^{0110\alpha} = 0.$$

It follows from symmetry that the last two terms cancel, and we get $z_{2i} z_{2i+4} = (z_{2i+2})^2$.

Also, if m is even, then consider the pattern 1000α and the position vector 1111β , where $\alpha = 0^{m-4}$ and $\beta = 1^{m-4}$. Then we have

$$\underline{G}^{0000\alpha}\underline{G}^{1111\beta} - \underline{G}^{1100\alpha}\underline{G}^{0011\beta} + \underline{G}^{1010\alpha}\underline{G}^{0101\beta} - \underline{G}^{1001\alpha}\underline{G}^{0110\beta} \pm \dots = 0.$$

The terms cancel except the first two, from which we get $z_0 z_m = z_2 z_{m-2}$. Similarly, if m is odd, we consider the pattern $1000 \dots 0$ and the position vector $1111 \dots 10$ and we can get $z_0 z_{m-1} = z_2 z_{m-3}$.

The lemma follows from this.

Combining even and odd matchgates we have

THEOREM 5.2. *A symmetric signature $[z_0, \dots, z_m]$ is realizable as the standard signature of a planar matchgate with even cardinality iff for all odd i , $z_i = 0$, and there exist constants r_1 , r_2 and λ , such that $z_{2i} = \lambda \cdot (r_1)^{\lfloor m/2 \rfloor - i} \cdot (r_2)^i$, for $0 \leq i \leq \lfloor \frac{m}{2} \rfloor$.*

A symmetric signature $[z_0, \dots, z_m]$ is realizable as the standard signature of a planar matchgate with odd cardinality iff for all even i , $z_i = 0$, and there exist constants r_1 , r_2 and λ , such that $z_{2i-1} = \lambda \cdot (r_1)^{\lceil m/2 \rceil - i} \cdot (r_2)^{i-1}$, for $1 \leq i \leq \lceil \frac{m}{2} \rceil$.

Theorem 5.2 is the first step in the proof of the characterization theorems of Section 4.

To isolate the requirements for signature tensors, we introduce a new concept called *admissibility*.

DEFINITION 5.1. A tensor G of arity n is *admissible* as a generator on a basis β iff $\underline{G} = \beta^{\otimes n} G$ satisfies the *Parity Constraint*. Let $B_{gen}^p(G)$ denote the subset of \mathcal{M} for which G is admissible as a generator.

By definition we have $B_{gen}(G) \subseteq B_{gen}^p(G)$ for all G .

DEFINITION 5.2. A generator G is called d -realizable (resp. d -admissible) for an integer $d \geq 0$ iff $B_{gen}(G) \subset \mathcal{M}$ (resp. $B_{gen}^p(G) \subset \mathcal{M}$) is a (non-empty) algebraic subset of dimension at least d .

By definition, if a generator G is d -realizable, then it is d -admissible.

Remark: Since \mathcal{M} has dimension two, 2-realizability is universal realizability, which means that G is realizable on any basis. This is because the conditions defining realizability are polynomial equations (with coefficients from (G^S) , and variables on \mathcal{M}). If there is at least one polynomial which is not identically 0, the algebraic set has dimension ≤ 1 . Using any 2-realizable signature is a freebie in the design of holographic algorithms; it places no restriction on the rest of the design. Therefore, they are particularly desirable.

The following theorem is a complete characterization of 2-admissibility over fields of characteristic 0. It uses rank estimates related to the *Kneser Graph* $KG_{2k+1,k}$ [32, 42, 45, 17, 18, 23, 36].

THEOREM 5.3. *Let G be a tensor of arity n . G is 2-admissible iff*

- (1) $n = 2k$ is even;
 - (2) all $G^S = 0$ except for $|S| = k$; and
 - (3) for all $T \subset [n]$ with $|T| = k + 1$,
- $$(7) \quad \sum_{S \subset T, |S|=k} G^S = 0.$$

The solution space is a linear subspace of dimension the Catalan number $\frac{1}{k+1} \binom{2k}{k}$.

Consider all subsets of $[n]$ of a certain cardinality. Let $0 \leq k \leq \ell \leq n$, and let $A_{k,\ell,n}$ denote the $\binom{n}{k} \times \binom{n}{\ell}$ Boolean matrix indexed by (A, B) , where $A, B \subset [n]$ and $|A| = k, |B| = \ell$, and the entry at (A, B) is $\chi_{[A \subset B]}$. It is known that over the rationals \mathbf{Q} , the rank $\text{rk}(A_{k,\ell,n}) = \min\{\binom{n}{k}, \binom{n}{\ell}\}$ [17, 18, 23, 36]. The situation with finite characteristic p is interesting and is more involved. For example, Linial and Rothschild [36] prove exact rank formula for characteristic 2 and 3. The rank “defect” compared to the characteristic 0 case provides more admissible signatures. For the rest of this article, we will focus on characteristic 0.

We restate the definition of d -admissibility in more detail.

DEFINITION 5.3. $G = (G^S)_{S \subset [n]}$ is called d -admissible if the following algebraic variety V has dimension at least d , where $V = V_0 \cup V_1 \subset \mathcal{M}$, and V_0 (resp. V_1) is defined by the set of all parity requirements for the generator signature of an odd (resp. even) matchgate.

More precisely, consider V_0 . We take a point (in dehomogenized coordinates) $\begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix} \in \mathcal{M}$. We also denote $x_0 = x, x_1 = y$. Let $T \subset [n]$ with $|T|$ even. Then we require

$$\left\langle \bigotimes_{\sigma=1}^n [1, x_{[\sigma \in T]}], G \right\rangle = 0.$$

Similarly we define V_1 , where we require that all $|T|$ be odd.

We note that

$$(8) \quad \left\langle \bigotimes_{\sigma=1}^n [1, x_{[\sigma \in T]}], G \right\rangle = \sum_{\substack{0 \leq i \leq n-|T| \\ 0 \leq j \leq |T|}} x^i y^j \sum_{\substack{A \subset T^c, |A|=i \\ B \subset T, |B|=j}} G^{A \cup B}.$$

If $\dim(V) = 2$, then either $\dim(V_0) = 2$ or $\dim(V_1) = 2$. For $\dim(V_0) = 2$, we have the following: For all $T \subset [n]$ with $|T|$ even, and for all $0 \leq i \leq n - |T|$ and $0 \leq j \leq |T|$,

$$(9) \quad \sum_{A \subset T^c, B \subset T, |A|=i, |B|=j} G^{A \cup B} = 0.$$

(If there is one equation not satisfied, then there is at least one non-trivial polynomial among the parity requirements, which implies $\dim(V_0) \leq 1$.) For $\dim(V_1) = 2$, the above holds for all $|T|$ odd. Continuing with $\dim(V_0) = 2$, by taking $i = 0$, we get for all $T \subset [n]$ with $|T|$ even, and $j \leq |T|$,

$$(10) \quad \sum_{S \subset T, |S|=j} G^S = 0.$$

Also by taking $j = 0$, we get for all $i \leq n - |T|$,

$$\sum_{S \subset T^c, |S|=i} G^S = 0.$$

If $S \subset [n]$ with $|S|$ even, then we may take $T = S$ and $j = |T|$, and it follows that

$$G^S = 0.$$

If n is odd, then T is even and T^c is odd, and together they range over all possible subsets of $[n]$. It follows that

$$G^S = 0,$$

for all $S \subset [n]$. That is, G is trivial.

An identical argument also shows that for $\dim(V_1) = 2$ and n odd, the trivial $G \equiv 0$ is the only possibility.

Now we assume $n = 2k$ is even, and continue with $\dim(V_0) = 2$. Both T and T^c are even. Pick any T even and $i = n - |T|$, and we get

$$\sum_{A \subset T^c, B \subset T, |A|=i, |B|=j} G^{A \cup B} = \sum_{S \supset T^c, |S|=i+j} G^S = 0,$$

i.e., for all even $T' \subset [n]$ and all $i \geq |T'|$,

$$(11) \quad \sum_{S \supset T', |S|=i} G^S = 0.$$

If $|S| = i < k$, we form the following system of equations from (10),

$$\sum_{S \subset T, |S|=i} G^S = 0,$$

where T ranges over all subsets of $[n]$ with $|T| = t$, and $t = i$ or $i + 1$, whichever is even. This linear system has rank $\binom{n}{i}$. It follows that $G^S = 0$ for all $|S| < k$.

Similarly, if $|S| = i > k$, we can use (11) with $|T| = i$ or $i - 1$, whichever is even, and sum over all subsets S containing T . This linear system also has rank $\binom{n}{i}$. It follows that $G^S = 0$ for all $|S| > k$.

Therefore the only non-zero entries of G are among G^S with half weight $|S| = k$. Also with $\dim(V_0) = 2$, we may assume k is odd. Otherwise, we already know $G^S = 0$ for all $|S|$ even.

A similar argument for V_1 shows that, in order for $\dim(V_1) = 2$, we must have $n = 2k$ even, all $G^S = 0$ except for $|S| = k$ and k is even.

Summarizing, we have

LEMMA 5.2. *If G is 2-admissible, then $n = 2k$ is even, all $G^S = 0$ except for $|S| = k$. If k is odd (resp. even) then the only possibility is $\dim(V_0) = 2$ (resp. $\dim(V_1) = 2$). Moreover, for all $T \subset [n]$ with $|T| = k + 1$,*

$$(12) \quad \sum_{S \subset T, |S|=k} G^S = 0.$$

Next we prove that the conditions in Lemma 5.2 are also sufficient for G being 2-admissible, i.e., we prove (9), and thus all the polynomials in (8) are identically zero.

Suppose k odd. We prove $\dim(V_0) = 2$. A similar argument does for k even and $\dim(V_1) = 2$. We only need to verify (9) for all $i + j = k$, namely for all $T \subset [n]$ with $|T|$ even, and for all $0 \leq i \leq n - |T|$, and $0 \leq j = k - i \leq |T|$,

$$(13) \quad \sum_{A \subset T^c, B \subset T, |A|=i, |B|=k-i} G^{A \cup B} = 0.$$

Denote by $t = |T|$ and $s = n - |T|$. By symmetry of T and T^c (both being even subsets of $[n]$) we may assume $s \leq t$. Since k is odd, we have the strict $s < t$, for otherwise $s = t = k$ would be odd.

We prove (13) by induction on $i \geq 0$. For the base case $i = 0$, $j = k$, we consider all $U \subset T$ with $|U| = k + 1$. Note that as $t \geq k + 1$, this is not vacuous. By (12) we have

$$\sum_{S \subset U, |S|=k} G^S = 0.$$

Summing over all such U , and considering how many times each $S \subset [n]$ with $|S| = k$ appears in the sum, we get

$$(14) \quad \sum_{\substack{A \subset T^c, |A|=0 \\ B \subset T, |B|=k}} G^{A \cup B} = \sum_{S \subset T, |S|=k} G^S = \frac{1}{\binom{t-k}{1}} \sum_{\substack{U \subset T \\ |U|=k+1}} \sum_{S \subset U, |S|=k} G^S = 0.$$

Inductively we assume (13) has been proved for $i - 1$, for some $i \geq 1$. Consider i and $j = k - i$. We may assume $i \leq s$; otherwise we are done. Also $k - i + 1 \leq t$. Consider all subsets $U = U_1 \cup U_2 \subset [n]$, where $U_1 \subset T^c$, $U_2 \subset T$, with $|U_1| = i$ and $|U_2| = k - i + 1$. Note that $|U| = k + 1$. We have

$$0 = \sum_{S \subset U, |S|=k} G^S = \sum_{A \subset U_1, |A|=i-1} G^{A \cup U_2} + \sum_{B \subset U_2, |B|=k-i} G^{U_1 \cup B},$$

as all sets $S \subset U$ with $|S| = k$ are classified into two classes according to whether $|S \cap U_1| = i - 1$ or i . Then summing over all such U ,

$$\begin{aligned} 0 = \sum_U \sum_{S \subset U, |S|=k} G^S &= \binom{s - (i - 1)}{1} \sum_{\substack{A \subset T^c, |A| = i - 1 \\ B \subset T, |B| = k - i + 1}} G^{A \cup B} \\ &+ \binom{t - (k - i)}{1} \sum_{\substack{A \subset T^c, |A| = i \\ B \subset T, |B| = k - i}} G^{A \cup B}, \end{aligned}$$

by considering how many times each S of the two classes appears in the sum $\sum_U \sum_S$. Since the first sum is 0 by inductive hypothesis, and $t - k + i \geq 1$, the second sum is also zero. Thus

$$\sum_{A \subset T^c, B \subset T, |A|=i, |B|=k-i} G^{A \cup B} = 0.$$

This proves Theorem 5.3.

The next theorem shows that any basis transformation on a 2-admissible G is just a scaling.

THEOREM 5.4.

If G is 2-admissible with arity $2k$, then $\forall \beta = \begin{pmatrix} n_0 & p_0 \\ n_1 & p_1 \end{pmatrix} \in \mathcal{M}$,
 $\beta^{\otimes 2k} G = (n_0 p_1 - n_1 p_0)^k G$.

COROLLARY 5.1. If G is 2-admissible and realizable on some basis (e.g., on the standard basis), then it is 2-realizable.

6. A Class of General Signatures

The basis $\mathbf{b2} = \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right]$ is probably the most successful basis in the design of holographical algorithms.

Consider the following extension of $\mathbf{b2}$

$$\mathbf{B2} = \left\{ \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \right] \in \mathbf{GL}_2(\mathbf{C}) \mid n_0 p_1 + n_1 p_0 = 0 \right\}.$$

Note that $\mathbf{b2} \in \mathbf{B2}$.

We will use dehomogenized coordinates $\begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix}$ for notational simplicity.

We will discuss a complete characterization theorem of all the signatures of arity n which are realizable on $\mathbf{B2}$. The plan is to first give a characterization of all the signatures which are admissible on $\mathbf{B2}$. Then we apply the set of all MGIs to them to get the characterization theorem.

For the parity constraint, we assume they are admissible as odd matchgate signatures (the case of even matchgates is similar). Consider

an arbitrary $\begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix} \in \text{B2}$, where non-singularity implies that $x \neq 0$.

Under a basis transformation $\underline{G} = \begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix}^{\otimes n} G$, the entry

(15)

$$\underline{G}^T = \left\langle \bigotimes_{\sigma=1}^n [1, (-1)^{\chi_{[\sigma \in T]} x}], G \right\rangle = \sum_{\substack{0 \leq i \leq n-|T| \\ 0 \leq j \leq |T|}} x^i (-x)^j \sum_{\substack{A \subset T^c, |A|=i \\ B \subset T, |B|=j}} G^{A \cup B}.$$

The polynomials should be identically zero when $|T|$ is even. This is the necessary and sufficient condition for G to be admissible on B2. Thus, for any T with $|T|$ even, the coefficient of x^i in the polynomial of (15) is

$$(16) \quad \sum_{|S|=i} (-1)^{|S \cap T|} G^S = 0.$$

When T ranges over all even subsets, we have a linear system for G^S . Thus we get $n+1$ linear equation systems according to the weight of S ; the i -th linear system, $0 \leq i \leq n$, is over the set of variables G^S with $|S| = i$, where the equations are indexed by subsets T with even cardinality. We define the coefficient matrix of the system as M , which is indexed by T and S . Then we have the following calculation of $M^T M$:

$$(17) \quad (M^T M)_{S_1, S_2} = \sum_{|T| \text{ is even}} (-1)^{|S_1 \cap T|} (-1)^{|S_2 \cap T|} = \sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|}.$$

There are three cases: If $S_1 \oplus S_2 = \emptyset$, or if $S_1 \oplus S_2 = [n]$, we have $\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 2^{n-1}$.

The third case is $S_1 \oplus S_2 \neq \emptyset$ and $S_1 \oplus S_2 \neq [n]$. We can take two elements a and b such that $a \in S_1 \oplus S_2$ and $b \notin S_1 \oplus S_2$. Then we can give a perfect matching of all the even subsets T by matching T and $T \oplus \{a, b\}$ together. For each pair of T and $T \oplus \{a, b\}$, one contributes a $+1$ and the other contributes a -1 in (17). They cancel out by each other, so overall we have $\sum_{|T| \text{ is even}} (-1)^{|(S_1 \oplus S_2) \cap T|} = 0$.

Now for the i -th system, for $i = |S| \neq n/2$, the case $S_1 \oplus S_2 = [n]$ does not occur. So the matrix $M^T M$ is $2^{n-1} I$, which means that $G^S = 0$, for all $|S| \neq n/2$. (In particular, only trivial $G \equiv 0$ exists for n odd.)

If $|S| = n/2$, the $n/2$ -th linear system gives $G^S = -G^{S^c}$. For the even matchgate case ($|T|$ is odd), it gives $G^S = G^{S^c}$. This is also sufficient. So we have the following theorem, which completely solves the problem of admissibility for B2:

THEOREM 6.1. *For a signature G with arity n , G is admissible on B2 iff there exists $\epsilon = \pm 1$ such that $G^S = 0$ for all $|S| \neq n/2$ and $G^S = \epsilon G^{S^c}$ for all $|S| = n/2$.*

Now we move on to the more difficult question of realizability. Realizability is more difficult than admissibility because it is controlled by the set of Matchgate Identities (MGI). These MGI are not only exponential in size, but also non-linear. We will apply all the MGIs to the signatures in the above theorem to get our characterization theorem over B2.

For a $\beta = \begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix} \in \text{B2}$, let $\underline{G} = \beta^{\otimes n} G$. The problem is to characterize when \underline{G} is realizable by an even matchgate as a standard signature. (The case for odd matchgate is similar.) From Theorem 6.1, we know that $G^S = 0$ for all $|S| \neq n/2$, and $G^S = G^{S^c}$ for all $|S| = n/2$. (For odd matchgates it would be $G^S = -G^{S^c}$; we omit it here.) By the basis transformation $\underline{G} = \beta^{\otimes n} G$, we have (T is even):

$$\underline{G}^T = x^{n/2} \sum_{|S|=n/2} (-1)^{|T \cap S|} G^S.$$

In the above equation, when substituted in any MGI, $x^{n/2}$ is just a global scaling factor. So we can just let $x = 1$, without changing its realizability.

We consider an arbitrary MGI of \underline{G} : for a pattern set A ($|A|$ is odd), position set P ($|P|$ is even), we have

$$\begin{aligned} 0 &= \sum_{i=1}^{|P|} (-1)^i \underline{G}^{A \oplus \{p_i\}} \underline{G}^{A \oplus P \oplus \{p_i\}} \\ &= \sum_{i=1}^{|P|} (-1)^i \sum_{|S_1|=n/2} (-1)^{|(A \oplus \{p_i\}) \cap S_1|} G^{S_1} \sum_{|S_2|=n/2} (-1)^{|(A \oplus P \oplus \{p_i\}) \cap S_2|} G^{S_2} \\ &= \sum_{|S_1|=|S_2|=n/2} G^{S_1} G^{S_2} \sum_{i=1}^{|P|} (-1)^i (-1)^{|(A \oplus \{p_i\}) \cap S_1|} (-1)^{|(A \oplus P \oplus \{p_i\}) \cap S_2|}. \end{aligned}$$

Over all odd A and even P these are also sufficient conditions. Note that for even matchgates, both A and $A \oplus P$ must be odd (so that the single bit flips $A \oplus \{p_i\}$ and $A \oplus P \oplus \{p_i\}$ are even).

Because the sets $A \oplus \{p_i\}$ and $A \oplus P \oplus \{p_i\}$ are both even, the coefficients of the four terms $G^{S_1} G^{S_2}$, $G^{S_1} G^{S_2^c}$, $G^{S_1^c} G^{S_2}$ and $G^{S_1^c} G^{S_2^c}$ are all equal. Therefore we can combine these four terms (and divide by 4)

and have

$$\begin{aligned}
0 &= \sum_{|S_1|=|S_2|=n/2, 1 \in S_1 \cap S_2} G^{S_1} G^{S_2} \\
&\quad \cdot \sum_{i=1}^{|P|} (-1)^i (-1)^{|(A \oplus \{p_i\}) \cap S_1|} (-1)^{|(A \oplus P \oplus \{p_i\}) \cap S_2|} \\
&= \sum_{|S_1|=|S_2|=n/2, 1 \in S_1 \cap S_2} G^{S_1} G^{S_2} (-1)^{|A \cap (S_1 \oplus S_2)|} (-1)^{|P \cap S_2|} \\
&\quad \cdot \sum_{i=1}^{|P|} (-1)^i (-1)^{| \{p_i\} \cap (S_1 \oplus S_2) |}.
\end{aligned}$$

Here we identify a set $X \subset [n]$ with its characteristic vector in our notations. We call an X a *single run* iff it is \emptyset , or $[n]$, or it consists of a contiguous segment of 0's and then 1's, in a circular fashion. We have the following theorem.

THEOREM 6.2. *For a signature G with arity n , G is realizable on $B2$ iff there exists $\epsilon = \pm 1$ such that*

- (1) $G^S = 0$ for all $|S| \neq n/2$;
- (2) $G^S = \epsilon G^{S^c}$ for all $|S| = n/2$; and
- (3) for any pair (S_1, S_2) , if $G^{S_1} G^{S_2} \neq 0$, then $S_1 \oplus S_2$ is a single run.

PROOF. First we denote $X = S_1 \oplus S_2$ and use S instead of S_2 in the above MGI (we note that X is an even set and $1 \notin X$):

$$\begin{aligned}
(18) \quad &\sum_{|X| \text{ is even, } 1 \notin X} (-1)^{|A \cap X|} \\
&\cdot \sum_{|S|=|S \oplus X|=n/2, 1 \in S} G^S G^{S \oplus X} (-1)^{|P \cap S|} \sum_{i=1}^{|P|} (-1)^i (-1)^{| \{p_i\} \cap X |} = 0.
\end{aligned}$$

The above equation is valid for all odd sets A and even sets P . We define a set of valuables $Y(X, P)$ as

$$Y(X, P) = \sum_{|S|=|S \oplus X|=n/2, 1 \in S} G^S G^{S \oplus X} (-1)^{|P \cap S|} \sum_{i=1}^{|P|} (-1)^i (-1)^{| \{p_i\} \cap X |}.$$

We fix an arbitrary even P . Then letting A go through all the odd sets, we have a linear system for the valuables $Y(X, P)$ from (18), where the variables are indexed by even X not containing 1, and the equations are indexed by odd A . The coefficient matrix of this system is $((-1)^{|A \cap X|})$. This matrix has full rank, which can be proved similarly as in the two out of three cases for (17). Note that for two X_1 and X_2 , we have $X_1 \oplus X_2 \neq [n]$, because $1 \notin X_1 \oplus X_2$.

Therefore, we have for any even P and any even X with $1 \notin X$,

$$(19) \quad \sum_{|S|=|S \oplus X|=n/2, 1 \in S} G^S G^{S \oplus X} (-1)^{|P \cap S|} \sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} = 0.$$

Now we will fix an even X with $1 \notin X$, and view (19) as a linear system on the variables $G^S G^{S \oplus X}$, where the equations are indexed by all even P .

First we show that if X is a single run, then (19) always holds. If $P \cap X$ is even, since X is a single run and is even, and P is even, it follows that there are an even number of elements in both $P \cap X$ and $P \cap X^c$. A moment reflection shows that $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} = 0$.

If $P \cap X$ is odd, then by symmetry of S to $S \oplus X$, the combined coefficient of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$ is $(-1)^{|P \cap S|} + (-1)^{|P \cap (S \oplus X)|} = (-1)^{|P \cap S|} [1 + (-1)^{|P \cap X|}]$. When $P \cap X$ is odd, this is 0. So we proved the “if” part of this theorem.

Now we prove that the conditions in Theorem 6.2 are also necessary. We will show that in order to satisfy all the MGI, for any even X with $1 \notin X$, if X is not a single run, then for all S , $G^S G^{S \oplus X} = 0$. This is more difficult. The crux of the proof is to show that a certain exponential sized matrix has mutually orthogonal columns, a matrix which we don’t even give an explicit formula for its dimension.

Fix an even X with $1 \notin X$. We assume X is not a single run. Then we can pick a particular P with 4 elements, such that $p_1 < p_2 < p_3 < p_4$, and $p_2, p_4 \in X$ and $p_1, p_3 \notin X$. This can be done greedily, e.g., pick $p_1 = 1$ (we know that $1 \notin X$). Then run from 1, 2, 3, ... till the first $i \in X$. That is our p_2 . Since X is not a single run, by our definition $X \neq \emptyset$ in particular. So p_2 exists. Then the first one after that which is not in X is p_3 . Being not a single run, such a p_3 must exist. Then there must be another one after p_3 , which belongs to X , again by X being not a single run. This is our $p_4 \in X$. Now for this particular P , we can see that $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} \neq 0$.

For a fixed even X with $1 \notin X$, and X is not a single run, consider the linear equation system:

For all even P such that $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} \neq 0$, and $P \cap X$ is also even,

$$(20) \quad \sum_{|S|=|S \oplus X|=n/2, 1 \in S} (-1)^{|P \cap S|} G^S G^{S \oplus X} = 0.$$

Here the variables are all “ $G^S G^{S \oplus X}$ ”, where $|S| = |S \oplus X| = n/2$, $1 \in S$. Note that, as shown above, if $P \cap X$ is odd, then the combined coefficients of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$ are zero in (19). (That proof does not depend on X being a single run or not.) For $P \cap X$ is even, the coefficients of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$ are the same, which can be combined. Consequently in (20) we combine the coefficients of $G^S G^{S \oplus X} = G^{S \oplus X} G^S$,

but only consider for $P \cap X$ even. After this identification, the equation system in (20) (for a fixed X satisfying the conditions) has equations indexed by the P 's satisfying its stated conditions, and has variables $G^S G^{S \oplus X}$ after the identification S with $S \oplus X$. They range over unordered pairs $\{S, S \oplus X\}$ obtained by taking 1, and exactly half the elements of X and exactly $\frac{n}{2} - \frac{|X|}{2} - 1$ elements of $[n] - \{1\} - X$. We will not give a closed-form formula for the number of equations indexed by the P 's; nevertheless, we will show that columns of the matrix of the linear system (20) are mutually orthogonal!

In the following, when we say, consider two “distinct” S and S' in this equation system, we have the following property: $S \oplus S'$ is not any of the four sets: $\emptyset, [n], X, X^c$. (Not equal to \emptyset because they are distinct; not equal to $[n]$ because both contain 1; not equal to X because of the above identification; and finally not equal to X^c because $1 \notin S \oplus S'$ and yet $1 \in X^c$.)

Our goal is to show, for the linear equation system (20), the columns of “distinct” S and S' are orthogonal. First some comments. We will not use explicitly below the fact that X is not a single run to show orthogonality. Not being a single run was used to show that the column coefficient vectors in (19) are non-zero (for these vectors the entries are indexed by P as P runs through all the appropriate sets, the set of vectors is indexed by various S). In going from (19) to (20), we have already taken that into account.

We had proved earlier that for X not a single run, there exists some position vector P which makes the sum $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} \neq 0$. For a fixed X , in the linear equation system (19) the above quantity $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|}$ does not depend on variables $G^S G^{S \oplus X}$ indexed by S . We can collect those equations (a non-empty subset of equations indexed by P) in (19) where the above quantity is non-zero, and factor out this sum from each such equation. This gives us (20). Of course in (19) those equations (indexed by P) where the above sum is zero are trivially satisfied. This means that the orthogonality of the coefficient vectors in (20) implies that all $G^S G^{S \oplus X} = 0$ in (20) and therefore in (19).

(For notational simplicity, we may consider the equality $G^S G^{S \oplus X} = 0$ above really for all S , and not worry about S being half weight or $S \oplus X$ being half weight. As otherwise they are obvious.)

Now we wish to prove any two “distinct” column vectors for S and S' are orthogonal. Let's consider the condition $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} \neq 0$ more carefully. Lay out the elements $1, 2, 3, \dots, n$, and lay out the elements of X in that order from left to right. It breaks $[n]$ into runs. Say $1, 2, \dots, a \notin X$, $a+1, a+2, \dots, b \in X$, $b+1, b+2, \dots, c \notin X$, etc. We call $[1, 2, \dots, a]$ an “out” segment for X , $[a+1, a+2, \dots, b]$ an “in” segment for X , etc. Now consider going through elements of P , also

from 1 to n . Put down $-$ and $+$ alternately under each such element of P , from p_1 to the last P -element. These record the factor $(-1)^i$ in the sum. In each “in” and “out” segment of X , P will have either an even or an odd number of elements. Since $|P|$ is even, there must be an even number of segments (“in” or “out”) which have an odd number of P -elements. A moment’s reflection will convince us that whenever we have a segment which contains an even number of P -elements, we can ignore that segment. It does not affect the subsequent \pm labelling. And for either an “in” segment or an “out” segment of X , the contribution of these even number of P -elements to the sum $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|}$ is 0. So we can imagine a sequence of “even-segment removal” operations as follows: Whenever we see an “even segment” (either an “in” or an “out” segment of X which contains an even number of elements of P), we can remove it, and then merge the neighboring segments. This keeps the segments to be alternately “in” and “out” for X , and P is still even and therefore there remains an even number of segments with an odd number of P -elements. We can continue this process until no more “even segment” is left. When this process ends, we have an even number of “odd segments” left. They will still be alternately “in” and “out” for X . Now the key observation is this: There is nothing left (that even number = 0) iff that original sum $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} = 0$. This is because every “odd segment” that is left at the end contributes exactly the same ± 1 to the sum. If the even number of “odd segments” left starts with an “in” segment for X , then each segment contributes a $+1$; if it starts with an “out” segment for X , then each segment contributes a -1 .

Now consider two “distinct” S and S' , and consider the inner product of their column vectors. Denote by $D = S \oplus S'$. Then $D \neq \emptyset, [n], X, X^c$. The inner product is

$$\sum_P (-1)^{|P \cap S|} (-1)^{|P \cap S'|} = \sum_P (-1)^{|P \cap D|},$$

where P runs over all even subsets of $[n]$ with $|P \cap X|$ even, and satisfying $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} \neq 0$.

Now we design an involution (order 2 permutation) with no fixed point on the set of all such P ’s: Since $D \neq \emptyset, [n], X, X^c$, as we examine all elements from 1 to n , there must be two elements next to each other, both in X or both out of X , and one is in D and the other one is out of D . (This is because: as $D \neq \emptyset, [n]$, there must be “changes” in membership of D as we go from 1 to n . And if all such changes coincide with boundaries of “segments” (these are the change boundaries) of X , then either $D = X$ or $D = X^c$, but both are ruled out.) Thus there are i and $i+1$ which are in the same segment of X (either “in” segment or

“out” segment) such that $|D \cap \{i, i+1\}| = 1$. We use this $\{i, i+1\}$ to define our involution on the set of P 's: $P \mapsto P' = P \oplus \{i, i+1\}$.

Note that P is even iff P' is even, and also, $P \cap X$ is even iff $P' \cap X$ is even. Moreover, in the “eliminating the even segment” process described above, both P and P' will yield the same answer as to 0 or non-zero. Thus the involution is an involution on the set of even P , with $P \cap X$ even, and such that $\sum_{i=1}^{|P|} (-1)^i (-1)^{|\{p_i\} \cap X|} \neq 0$.

Finally, in the sum $\sum_P (-1)^{|P \cap D|}$, the term $(-1)^{|P \cap D|}$ and $(-1)^{|P' \cap D|}$ cancel, since

$$(-1)^{|P' \cap D|} = (-1)^{|P \cap D|} (-1)^{|\{i, i+1\} \cap D|} = -(-1)^{|P \cap D|}.$$

This completes the proof. \square

This theorem is quite powerful, and we believe that the full extent of its usefulness has not been explored.

When $n = 4$, there is a special case.

THEOREM 6.3. *For any $a, b \in \mathbf{C}$, the following generator*

$$(21) \quad G^\alpha = \begin{cases} a, & \alpha \in \{0101, 1010\}, \\ b, & \alpha \in \{0011, 1100\}, \\ 0, & \text{otherwise.} \end{cases}$$

is realizable on bases $\begin{pmatrix} 1 & x \\ 1 & -x \end{pmatrix}$ for all $x \neq 0$.

This family of signatures is used in the design of the holographic algorithm for the problem 2-COLOR-COUNTING in Section 3. In fact, for that particular problem we only need the case of $a = 1$ and $b = 0$ in Theorem 6.3. But other cases of a and b have also been used.

Acknowledgement. The author thanks Les Valiant for his comments on this article.

References

- [1] L. Adleman and M.-D. Huang, *Recognizing primes in random polynomial time*, in ‘Proc. 19th ACM Symposium on Theory of Computing’, 1987, 462–469.
- [2] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Annals of Mathematics **160** 781–793 (2004).
- [3] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, *Proof verification and hardness of approximation problems*, in ‘Proc. 33rd FOCS’, 14–23, 1992.
- [4] E. Bach and J. Shallit, *Algorithmic Number Theory*, Volume I: Efficient Algorithms, MIT Press, 1996.
- [5] R.J. Baxter, *Exactly Solved Models in Statistical Physics*, Academic Press, London, 1982.
- [6] J-Y. Cai and V. Choudhary, *Some Results on Matchgates and Holographic Algorithms*, in ‘Proceedings of ICALP 2006’, Part I, Lecture Notes in Computer Science, **4051**, 703–714; also available at Electronic Colloquium on Computational Complexity TR06-048, 2006.

- [7] J-Y. Cai and V. Choudhary, *Valiant's Holant Theorem and Matchgate Tensors* (Extended Abstract), in 'Proceedings of TAMC 2006', Lecture Notes in Computer Science, **3959**, 248–261; also available at Electronic Colloquium on Computational Complexity Report TR05-118.
- [8] J-Y. Cai, V. Choudhary, and P. Lu, *On the Theory of Matchgate Computations*, in 'IEEE Conference on Computational Complexity 2007', 305–318.
- [9] J-Y. Cai and P. Lu, *On Symmetric Signatures in Holographic Algorithms*, in 'Proceedings of STACS 2007', LNCS, **4393**, 429–440; also available at Electronic Colloquium on Computational Complexity Report TR06-135.
- [10] J-Y. Cai and P. Lu, *Holographic Algorithms: From Art to Science*, to appear in 'STOC 2007'; also available at Electronic Colloquium on Computational Complexity Report TR06-145.
- [11] J-Y. Cai and P. Lu, *Bases Collapse in Holographic Algorithms*, to appear in 'CCC 2007'; also available at Electronic Colloquium on Computational Complexity Report TR07-003.
- [12] J-Y. Cai and P. Lu, *Holographic Algorithms: The Power of Dimensionality Resolved*, to appear in 'ICALP 2007'; also available at Electronic Colloquium on Computational Complexity Report TR07-020.
- [13] *The Millennium Problems*, The Clay Institute, <http://www.claymath.org/millennium/P-vs-NP/>
- [14] A. Cobham, *The intrinsic computational difficulty of functions*, in 'Proc. Logic, Methodology, and Philosophy of Science II', North Holland, 1965.
- [15] S. Cook *The Complexity of Theorem Proving Procedures*, in 'Proceedings of the third annual ACM symposium on Theory of computing', 151–158, 1971.
- [16] J. Edmonds, *Maximum matching and a polyhedron with $(0, 1)$ vertices*, J. Res. Nat. Bur. Standards Sect B **69B** (1965) 125–130.
- [17] W. Foody and A. Hedayat, *On theory and applications of BIB designs with repeated blocks*, Annals Statist. **5** (1977) 932–945.
- [18] W. Foody and A. Hedayat, *Note: Correction to "On Theory and Application of BIB Designs with Repeated Blocks"*, Annals of Statistics **7**(4) (Jul. 1979) 925.
- [19] M. Garey and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, 1979.
- [20] M. Garey, D. Johnson, and L. Stockmeyer. *Some simplified NP-complete graph problems*, Theoretical Computer Science **1** 237-267 (1976).
- [21] C.F. Gauss, *Disquisitiones Arithmeticae*, Transl. by A.A. Clarke, Yale University Press, 1966.
- [22] M.X. Goemans and D.P. Williamson, *.879-approximation algorithms for MAX CUT and MAX 2SAT*, Proceedings of the twenty-sixth annual ACM symposium on Theory of computing, 422–431, 1994.
- [23] R.L. Graham, S.-Y.R. Li, and W.-C.W. Li, *On the Structure of t -Designs*, SIAM J. on Algebraic and Discrete Methods **1** 8 (1980).
- [24] F. Hadlock. *Finding a Maximum Cut of a Planar Graph in Polynomial Time*, SIAM Journal on Computing **4** (1975) 221–225.
- [25] J. Hartmanis and R.E. Stearns, *On the computational complexity of algorithms*, Trans. Amer. Math. Soc. **117** (1965) 285–306.
- [26] J. Håstad. *Some optimal inapproximability results*, Journal of the ACM **48**(4) July 2001.
- [27] H.B. Hunt, M.V. Marathe, V. Radhakrishnan, and R.E. Stearns, *The complexity of planar counting problems*, SIAM J. Comput. **27**(4) 1142–1167 (1998).
- [28] M. Jerrum. *Two-dimensional monomer-dimer systems are computationally intractable*, J. Stat. Phys. **48** (1987) 121-134; erratum, **59** (1990) 1087–1088.

- [29] R.M. Karp, *Reducibility Among Combinatorial Problems*. in ‘Complexity of Computer Computations’ (R.E. Miller and J.W. Thatcher, editors), New York, Plenum, 85–103, 1972.
- [30] P.W. Kasteleyn, *The statistics of dimers on a lattice*, Physica **27** 1209–1225 (1961).
- [31] P.W. Kasteleyn, *Graph Theory and Crystal Physics*, in ‘Graph Theory and Theoretical Physics’ (F. Harary, ed.), Academic Press, London, 43–110 (1967).
- [32] M. Kneser, *Aufgabe 360*, Jahresbericht der Deutschen Mathematiker-Vereinigung, **2**, Abteilung **58** 27 (1955).
- [33] M.S. Krishnamoorthy and N. Deo, *Node-deletion NP-complete problems*, Siam J. Comput. **8**(4) 619–625 (1977).
- [34] L. Levin, *Universal’nye perebornye zadachi*, Problemy Peredachi Informatsii **9**(3) 265–266 (1973); English translation, *Universal Search Problems*, in B.A. Trakhtenbrot *A Survey of Russian Approaches to Perebor (Brute-Force Searches) Algorithms*, Annals of the History of Computing **6**(4) 384–400 (1984).
- [35] J.M. Lewis and M. Yannakakis, *The node deletion problem for hereditary properties is NP-complete*, J. Comp. and Syst. Sciences **20** 219–230 (1980).
- [36] N. Linial and B. Rothschild, *Incidence Matrices of Subsets—A Rank Formula*, SIAM J. on Algebraic and Discrete Methods **2** 333 (1981).
- [37] D. Lichtenstein, *Planar formulae and their uses*, SIAM J. Comput. **11**(2) 329–343.
- [38] E.H. Lieb, *Exact solution of the problem of the entropy of two-dimensional ice*, Phys. Rev. Lett. **18** 692–694 (1967).
- [39] E.H. Lieb, *Residual entropy of square ice*, Phys. Rev. **162** 162–172 (1967).
- [40] E.H. Lieb, *Exact solution of the F model of an antiferroelectric*, Phys. Rev. Lett. **18** 1046–1048 (1967).
- [41] E.H. Lieb, *Exact solution of the two-dimensional Slater KDP model of a ferroelectric*, Phys. Rev. Lett. **19** 108–110 (1967).
- [42] L. Lovász, *Kneser’s conjecture, chromatic number, and homotopy*, Journal of Combinatorial Theory, Series A **25** 319–324 (1978).
- [43] Ju.V. Matijasevich, *The Diophantineness of Enumerable Sets*, Dokl. Akad. Nauk SSSR **191** 279–282 (1970); English translation: Soviet Math. Dokl. **11** 354–358 (1970).
- [44] Yu.V. Matijasevich, *Hilbert’s Tenth Problem*, Cambridge, MA, MIT Press, 1993.
- [45] J. Matoušek, *A combinatorial proof of Kneser’s conjecture*, Combinatorica **24**(1) 163–170 (2004).
- [46] K. Murota, *Matrices and Matroids for Systems Analysis*, Springer, Berlin, 2000.
- [47] L. Pauling, *The Structure and Entropy of Ice and of Other Crystals with Some Randomness of Atomic Arrangement*, J. Am. Chem. Soc. **57**(12) 2680–2684 (1935).
- [48] R. Soare, *Recursively enumerable sets and degrees*, Perspectives in Mathematical Logic, Springer-Verlag, 1987.
- [49] H.N.V. Temperley and M.E. Fisher, *Dimer problem in statistical mechanics – an exact result*, Philosophical Magazine **6** 1061–1063 (1961).
- [50] S. Toda, *PP is as Hard as the Polynomial-Time Hierarchy*, SIAM J. Comput. **20**(5) 865–877 (1991).
- [51] S.P. Vadhan, *The Complexity of Counting in Sparse, Regular and Planar Graphs*, SIAM Journal on Computing **8**(1) 398–427 (2001).
- [52] L.G. Valiant, *Quantum circuits that can be simulated classically in polynomial time*, SIAM Journal of Computing **31**(4) 1229–1254 (2002).
- [53] L.G. Valiant, *Expressiveness of Matchgates*, Theoretical Computer Science **281**(1) 457–471 (2002).

- [54] L.G. Valiant. *Holographic Algorithms* (Extended Abstract), in ‘Proc. 45th IEEE Symposium on Foundations of Computer Science’, 2004, 306–315; A more detailed version appeared in Electronic Colloquium on Computational Complexity Report TR05-099.
- [55] L.G. Valiant, *Holographic circuits*, in ‘Proc. 32nd International Colloquium on Automata, Languages and Programming’, 2005, 1–15.
- [56] L.G. Valiant, *Completeness for parity problems*, in ‘Proc. 11th International Computing and Combinatorics Conference’, 2005, 1–8.
- [57] L.G. Valiant, *Accidental Algorithms*, in ‘Proc. 47th Annual IEEE Symposium on Foundations of Computer Science’ 2006, 509–517.
- [58] D.J.A. Welsh, *Complexity: Knots, Colourings and Counting*, Cambridge University Press, 1993.

COMPUTER SCIENCES DEPARTMENT, UNIVERSITY OF WISCONSIN, MADISON,
WI 53706

E-mail address: `jyc@cs.wisc.edu`

Figures

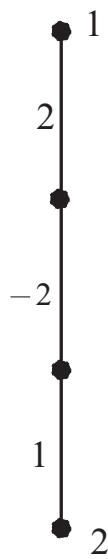


FIGURE 1. Under the basis **b2**, this generator matchgate has the signature $(0, 1, 1, 0)^T$.

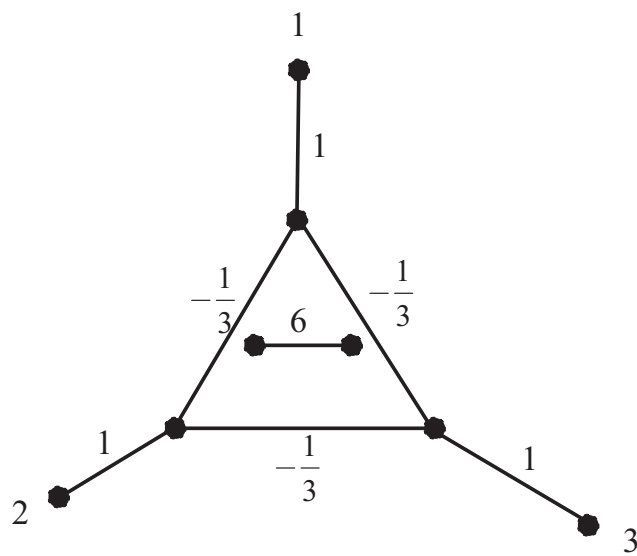


FIGURE 2. Under basis **b2**, this generator matchgate has the signature $(0, 1, 1, 1, 1, 1, 0)^T$.

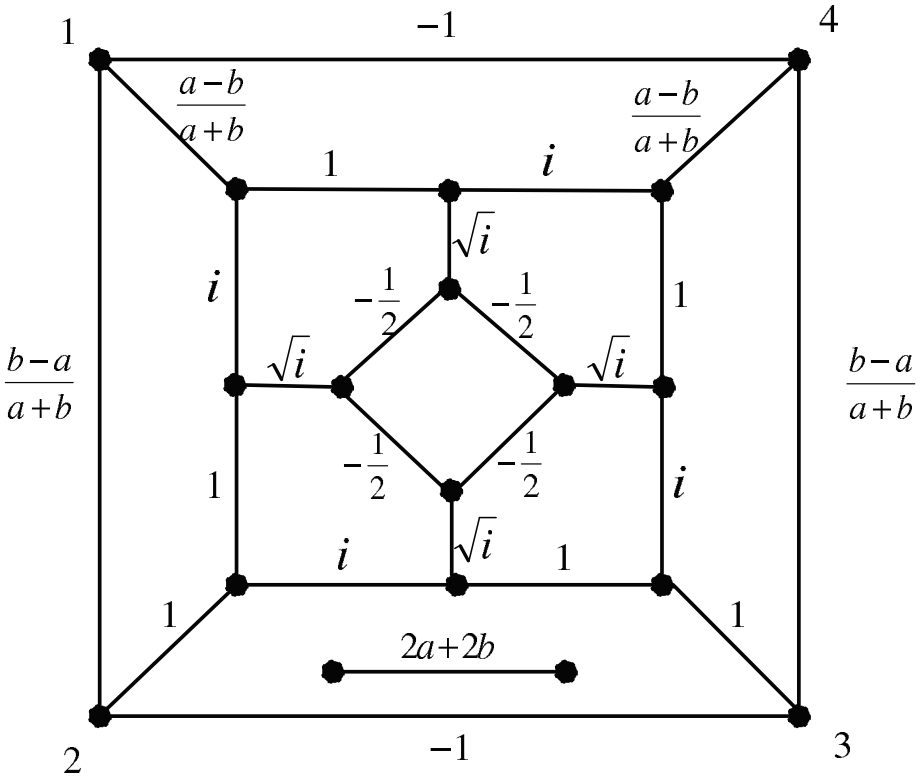


FIGURE 3. This planar matchgate has standard signature $(2a+2b, 0, 0, -2a+2b, 0, 2a-2b, -2a-2b, 0, 0, -2a-2b, 2a-2b, 0, -2a+2b, 0, 0, 2a+2b)^T$. Here $i = \sqrt{-1}$, and we assume $2a + 2b \neq 0$. (In case $2a + 2b = 0$, a similar matchgate will work.) This is an explicit construction for the matchgate promised in Theorem 6.3, which follows from the general Theorem 6.2.

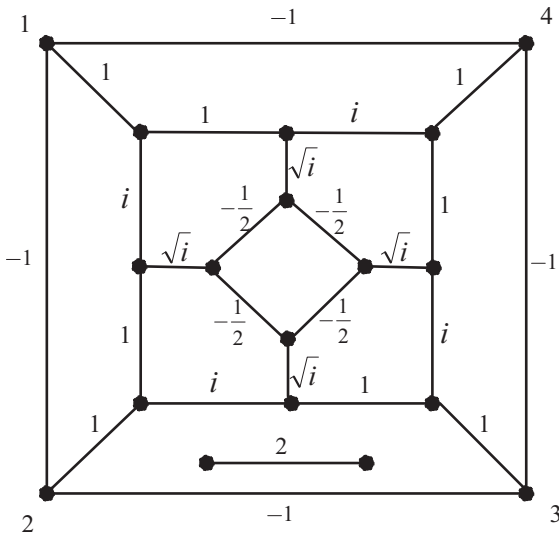


FIGURE 4. This is a special case of Figure 3. Under the basis **b2**, this generator matchgate has the signature G , where $G^{0101} = G^{1010} = 1$ and $G^\alpha = 0$ for other α . This matchgate together with Figure 1, 2 and 5 are used for the problem 2-COLOR-COUNTING.

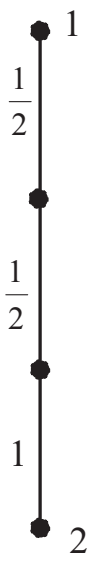


FIGURE 5. Under the basis **b2**, this recognizer matchgate has the signature $(1, 0, 0, 1)$.