4

Matchgates and Holographic Algorithms

Some counting problems are #P-hard on general instances, but are tractable over planar structures. In fact, one of the most remarkable algorithms for counting problems is Kasteleyn's algorithm (a.k.a. the FKT algorithm) to count the number of perfect matchings for any planar graph. Starting from this chapter, we will gradually build a theory that aims to show that this is not only a beautiful polynomial time counting algorithm, but also a *universal* strategy for a broad class of counting problems, in a very strong technical sense. This will be one of the highlights in Volume I of this book, and will be built on the theory of matchgates and holographic algorithms. We note that a corresponding theory on problems over general domains has not yet been developed, and will be a challenge for the future. To develop this topic fully we start with Pfaffian orientations on planar graphs.

4.1 Pfaffian Orientations and Kasteleyn's Algorithm

An $n \times n$ matrix A is called skew-symmetric if $A_{i,j} = -A_{j,i}$, for $1 \leq i, j \leq n$. We assume the entries of A are from a field of characteristic $\neq 2$. Then $A_{i,i} = 0$.

Every permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & 2k \\ i_1 & i_2 & \dots & i_{2k} \end{pmatrix}$ defines a partition of $[2k]$ into disjoint pairs $\tilde{\pi} = \{\{i_1, i_2\}, \{i_3, i_4\}, \dots, \{i_{2k-1}, i_{2k}\}\}$. The Pfaffian of an $n \times n$ skew-symmetric matrix A is defined as follows. Suppose $n = 2k \geq 2$ is even; then

$$\mathrm{Pf}(A) = \sum_{\pi} \epsilon_\pi A_{i_1,i_2} A_{i_3,i_4} \cdots A_{i_{2k-1},i_{2k}}, \tag{4.1}$$

where the sum is over all permutations $\pi = \begin{pmatrix} 1 & 2 & \dots & 2k \\ i_1 & i_2 & \dots & i_{2k} \end{pmatrix}$ such that

$$i_1 < i_2,\ i_3 < i_4,\ \dots,\ i_{2k-1} < i_{2k} \quad \text{and} \quad i_1 < i_3 < \cdots < i_{2k-1}. \tag{4.2}$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

The symbol ϵ_π in (4.1) denotes the sign of the permutation π; it is $+1$ or -1 depending on whether the parity of π is even or odd, respectively. We note that there is a natural 1-1 correspondence between permutations π satisfying the stipulation (4.2) and partitions of $[n]$ into disjoint pairs.

If n is odd, then we define $\mathrm{Pf}(A) = 0$. By convention if $n = 0$ we define $\mathrm{Pf}(A) = 1$.

For any permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & 2k \\ i_1 & i_2 & \dots & i_{2k} \end{pmatrix}$, not necessarily satisfying the stipulation (4.2), define

$$a_\pi = \epsilon_\pi A_{i_1,i_2} A_{i_3,i_4} \cdots A_{i_{2k-1},i_{2k}}.$$

We make a simple but important observation: If $\tilde{\pi} = \widetilde{\pi'}$, then $a_\pi = a_{\pi'}$, i.e., the expression a_π has the same value if we list the partition $\tilde{\pi} = \{\{i_1, i_2\}, \{i_3, i_4\}, \dots, \{i_{2k-1}, i_{2k}\}\}$ in any order of the pairs, as well as in any order of the two labels of each pair. This follows from the fact that A is skew-symmetric. This invariance will be used repeatedly.

We say two pairs of labels $i_{2j-1} < i_{2j}$ and $i_{2\ell-1} < i_{2\ell}$ form a crossover , or an overlapping pair, iff $i_{2j-1} < i_{2\ell-1} < i_{2j} < i_{2\ell}$ or $i_{2\ell-1} < i_{2j-1} < i_{2\ell} < i_{2j}$. Suppose π is a permutation satisfying the stipulation (4.2). Let $c(\pi)$ be the number of crossovers among the pairs in the partition $\tilde{\pi}$. Then the sign ϵ_π is also $(-1)^{c(\pi)}$. Hence it can be computed as the parity of the number of crossovers. To see this, consider the permutation π and consider a sequence of adjacent transpositions that moves the sequence $(1, 2, \dots, 2k-1, 2k)$ to $(i_1, i_2, \dots, i_{2k-1}, i_{2k})$. We have $i_1 = 1$ by (4.2). The number of transpositions that will bring i_2 to the position right after 1 is the number of labels strictly between $i_1 = 1$ and the number i_2, and has the same parity as the number of crossovers the pair $\{i_1, i_2\}$ forms with all other pairs of labels $\{\{i_3, i_4\}, \dots, \{i_{2k-1}, i_{2k}\}\}$ in $\tilde{\pi}$. After i_1, i_2 are placed in the first two positions, if $n > 2$, then i_3 is the minimum among all other labels by (4.2), and is currently located right after the first two elements. Then we move i_4 to the position right after i_3. The proof is completed by induction. We note that the definition of Pfaffian and this notion of crossovers apply to any totally ordered label set, in particular to any index set of a principal submatrix obtained from A by selecting a common subset of rows and columns.

The Pfaffian can be computed in polynomial time [Bar83, GM94]. A key relation to determinant is the following theorem due to Cayley [Hal66] (also see p. 352 of [Jac85a]).

Theorem 4.1. *For any $n \times n$ skew-symmetric matrix A,*

$$\det(A) = [\mathrm{Pf}(A)]^2.$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Note that for odd n, a skew-symmetric matrix A has $\det(A) = 0$. For even n, an algorithm similar to Gaussian elimination can be derived using the identity $\mathrm{Pf}(BAB^{\mathrm{T}}) = \det(B)\mathrm{Pf}(A)$, for any $n \times n$ matrix B. It can be even computed in NC [MSV04].

Let $G = (V, E)$ be a simple undirected graph without self-loops and parallel edges. Suppose the vertices of G are labeled by a totally ordered set, e.g., $V = \{1, 2, \ldots, n\}$. Assign an indeterminate x_e for every edge $e = \{u, v\} \in E$. Then we define the skew-symmetric adjacency matrix $A = A(G)$ of the graph G to be

$$A_{u,v} = \begin{cases} x_e & \text{if } e = \{u, v\} \in E \text{ and } u < v \\ -x_e & \text{if } e = \{u, v\} \in E \text{ and } u > v \\ 0 & \text{if } \{u, v\} \notin E \end{cases}. \tag{4.3}$$

Note that for any permutation π, the partition $\tilde{\pi}$ is a perfect matching iff all pairs are edges. Denote by $\mathcal{M}(G)$ the set of all perfect matchings of G. There is a 1-1 correspondence between nonzero terms in $\mathrm{Pf}(A)$ and $\mathcal{M}(G)$. For any $M \in \mathcal{M}(G)$ there are $2^k k!$ permutations of the form $\pi = \begin{pmatrix} 1 & 2 & \ldots & 2k \\ i_1 & i_2 & \ldots & i_{2k} \end{pmatrix}$ that can represent M, i.e., $\tilde{\pi} = M$, of which the unique permutation that satisfies the stipulation (4.2) is called a *canonical* expression. All other permutation expressions for M are obtained by permuting the order of the pairs $\{i_{2\ell-1}, i_{2\ell}\}$ and the order within each pair.

We define the weight of a perfect matching M in G to be the product of edge weights x_e for all $e \in M$, namely $\Gamma(M) = \Gamma_G(M) = \prod_{e \in M} x_e$. It follows that $a_\pi = \pm\Gamma(M)$, if $\tilde{\pi} = M$.

An orientation of a graph G assigns one direction to each edge of G. We denote by $u \to v$ if the edge $\{u, v\}$ is oriented from u to v. In this case u is its tail, and v is its head. For an oriented graph $\overrightarrow{G}$ we modify the skew-symmetric matrix A in (4.3) to be $B = B(\overrightarrow{G})$:

$$B_{u,v} = \begin{cases} x_e & \text{if } e = \{u, v\} \in E \text{ and } u \to v \\ -x_e & \text{if } e = \{u, v\} \in E \text{ and } v \to u \\ 0 & \text{if } \{u, v\} \notin E \end{cases}. \tag{4.4}$$

In other words, we change the sign at both entries $A_{u,v}$ and $A_{v,u}$ if $u < v$ and $\{u, v\}$ is oriented $v \to u$.

Given an orientation, we will consider the Pfaffian of B:

$$\mathrm{Pf}(B) = \sum_{\pi} \epsilon_\pi B_{i_1,i_2} B_{i_3,i_4} \cdots B_{i_{2k-1},i_{2k}}, \tag{4.5}$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

where the sum is over permutations π satisfying (4.2). For a perfect matching M in an oriented graph $\overrightarrow{G}$, suppose $M = \tilde{\pi}$, define the Pfaffian term

$$\mathrm{Pf}_{\overrightarrow{G}}(M) = \epsilon_\pi B_{i_1,i_2} B_{i_3,i_4} \cdots B_{i_{2k-1},i_{2k}}. \tag{4.6}$$

It is a term in $\mathrm{Pf}(B)$ when π is the canonical expression for M and it is equal to either the weight of the perfect matching $\Gamma_G(M)$ or its negation $-\Gamma_G(M)$. However, we can choose any permutation π representing M, and the value $\mathrm{Pf}_{\overrightarrow{G}}(M)$ is defined, which does not depend on the particular partition π corresponding to M, owing to the invariance observed earlier.

Definition 4.2. For any perfect matching M in an oriented graph $\overrightarrow{G}$, the *sign* of the perfect matching M with respect to this orientation is

$$\mathrm{sgn}_{\overrightarrow{G}}(M) = \frac{\mathrm{Pf}_{\overrightarrow{G}}(M)}{\Gamma_G(M)} \in \{-1, 1\}. \tag{4.7}$$

When $\overrightarrow{G}$ is clear from the context, we write $\mathrm{sgn}(M)$ instead.

We note that $\mathrm{sgn}(M)$ can be computed with any partition π corresponding to M, i.e., $\tilde{\pi} = M$, owing to the invariance of $\mathrm{Pf}_{\overrightarrow{G}}(M)$. In particular, $\mathrm{sgn}(M)$ can be computed simply as the sign ϵ_π of the permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & 2k \\ i_1 & i_2 & \dots & i_{2k} \end{pmatrix}$, where each matching edge $\{i_{2\ell-1}, i_{2\ell}\} \in M$ is listed by its orientation $i_{2\ell-1} \to i_{2\ell}$. This permutation π is in general not a canonical expression.

If M and M' are two perfect matchings, the symmetric difference $M \oplus M'$ consists of a set of cycles of even length that are alternating between edges from M and M'. For any orientation on a graph G, if C is a cycle of even length, then we say it is evenly oriented if there are an even number of edges oriented in one direction, and oddly oriented otherwise. Clearly this notion does not depend on the direction since C has an even length.

Lemma 4.3. *For any orientation on a graph G, and perfect matchings M and M', if k is the number of evenly oriented cycles in $M \oplus M'$ with respect to the orientation, then*

$$\mathrm{sgn}(M) \cdot \mathrm{sgn}(M') = (-1)^k.$$

Proof. We first show that if this equality holds for one orientation then it holds for all orientations. Let e be an edge in $\overrightarrow{G}$ and suppose we reverse its orientation. If $e \notin M \oplus M'$ then obviously the reversal has no effect on the equality. Suppose $e \in M \oplus M'$. Then k is changed by 1, and exactly one of $\mathrm{sgn}(M)$ and $\mathrm{sgn}(M')$ is changed. Hence we may choose any orientation convenient for M

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

and M' to prove our equality. So we choose one that gives a cyclic orientation on each cycle of $M \oplus M'$ (either direction of the cyclic orientation for each cycle is acceptable). We may orient all other edges arbitrarily. In this orientation, k is the number of cycles in $M \oplus M'$.

Next we will relabel the vertices of $\overrightarrow{G}$. If we apply a permutation σ on the vertices of $\overrightarrow{G}$, the Pfaffian term for a perfect matching M is changed as follows. Suppose M corresponds to the permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & 2k \\ i_1 & i_2 & \dots & i_{2k} \end{pmatrix}$, where each matching edge $\{i_{2\ell-1}, i_{2\ell}\} \in M$ is listed by its orientation $i_{2\ell-1} \to i_{2\ell}$. We write its corresponding Pfaffian term $b_\pi = \epsilon_\pi B_{i_1,i_2} B_{i_3,i_4} \cdots B_{i_{2k-1},i_{2k}}$. If $\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_{2k} \\ j_1 & j_2 & \dots & j_{2k} \end{pmatrix}$, then each matching edge is also oriented as $j_{2\ell-1} \to j_{2\ell}$ in the new labeling. The skew-symmetric matrix B' defined by the new labeling has $B'_{j_{2\ell-1},j_{2\ell}} = B_{i_{2\ell-1},i_{2\ell}}$, and thus the corresponding product is unchanged $B'_{j_1,j_2} B'_{j_3,j_4} \cdots B'_{j_{2k-1},j_{2k}} = B_{i_1,i_2} B_{i_3,i_4} \cdots B_{i_{2k-1},i_{2k}}$. But the sign ϵ_π becomes $\epsilon_{\sigma\pi} = \epsilon_\sigma \epsilon_\pi$. Hence the change to $\operatorname{sgn}(M)$ is to multiply it by ϵ_σ. The same is true for the change to $\operatorname{sgn}(M')$. Note that we wrote σ as $\begin{pmatrix} i_1 & i_2 & \dots & i_{2k} \\ j_1 & j_2 & \dots & j_{2k} \end{pmatrix}$ in reference to π that corresponds to M. However, the conclusion that we change $\operatorname{sgn}(M)$ by multiplying it with ϵ_σ is independent of how we express σ. In particular, for M', we can write σ in reference to π' corresponding to M', and the conclusion is the same. Hence the product $\operatorname{sgn}(M) \cdot \operatorname{sgn}(M')$ remains unchanged. Meanwhile the value k is clearly the same. So we may choose to label all vertices as follows. Pick any cycle of $M \oplus M'$ and start at any edge of this cycle in M. Label its tail as 1 and its head as 2. Label the rest of the cycle along the chosen orientation using the next unused integers. Thus if the cycle has length 2ℓ, then its vertices are labeled from 1 to 2ℓ consecutively along the orientation starting at the tail of one edge of M. Then starting with $2\ell + 1$ we label the next cycle of $M \oplus M'$, if there is any, in exactly the same way. After all cycles of $M \oplus M'$ are dealt with, we label all remaining vertices so that each edge in $M \cap M'$ is labeled consecutively with the next unused integers, and increasing from tail to head.

Now the Pfaffian term $\operatorname{Pf}_{\overrightarrow{G}}(M)$ for M is just the product of all edge weights $\Gamma_G(M)$. This is seen easily if we write b_π in the way where the permutation π is the identity, and we list all matched edges in the oriented order. For the Pfaffian term $b_{\pi'}$ corresponding to M', we still list the product part $B_{i_1,i_2} B_{i_3,i_4} \cdots B_{i_{2k-1},i_{2k}}$ in the oriented order for each matched edge. The sign $\epsilon_{\pi'}$ for the permutation is as follows. The part for the first cycle of length 2ℓ in $M \oplus M'$ has the form $\begin{pmatrix} 1 & 2 & \dots & 2\ell-1 & 2\ell \\ 2 & 3 & \dots & 2\ell & 1 \end{pmatrix}$, which is an even cycle as a permutation, and has

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

an odd parity. The permutation π' is simply a product of these even cycles in the permutation group, disjoint and one even cycle for each cycle in the graph $M \oplus M'$. Hence it has parity $\epsilon_{\pi'} = (-1)^k$. □

Definition 4.4. An orientation of a connected plane graph is called a *Pfaffian orientation* if along the boundary of every non-outer face, there are an odd number of clockwise-oriented edges.

Lemma 4.5. *Any Pfaffian orientation in a connected plane graph G satisfies the following property: For every cycle C, the number of clockwise-oriented edges of C is of the opposite parity to the number of vertices contained within C. (This number does not include the vertices on the cycle C).*

Proof. Let V and E be the number of vertices and edges contained within C, respectively, and let ℓ be the number of edges on C, which is also the number of vertices on C. The vertices contained within C are those in the interior of the region bounded by C; they do not include those on the cycle C. Similarly, the edges within C do not include those on C. An edge is a bridge edge iff it has the same face on both sides. Then in a traversal of the boundary of a face Δ, if there is a bridge edge e, it is traversed twice, once in each direction. In particular, in either orientation of e, it contributes one to the count of clockwise-oriented edges along the boundary of Δ. For a nonbridge edge e, depending on its orientation, it contributes one to the count of clockwise-oriented edges to exactly one face it borders on but not the other.

Suppose there are F faces bounded by C, and let c_i be the number of clockwise-oriented edges on the boundary of the ith face ($1 \le i \le \mathsf{F}$). Each c_i is odd by assumption; therefore $\mathsf{F} \equiv \sum_{i=1}^{\mathsf{F}} c_i \pmod 2$. By Euler's formula, counting the face formed by the exterior of C, we have $(\mathsf{V} + \ell) - (\mathsf{E} + \ell) + (\mathsf{F} + 1) = 2$. It follows that $\mathsf{E} = \mathsf{V} + \mathsf{F} - 1$.

If we add up all the clockwise-oriented edges among all boundary edges in F faces, each interior edge within C regardless orientation contributes one and each clockwise-oriented edge on C contributes one. Hence $\sum_{i=1}^{\mathsf{F}} c_i = \mathsf{E} + c$, where c is the number of clockwise-oriented edges on C.

It follows that

$$\mathsf{F} \equiv \sum_{i=1}^{\mathsf{F}} c_i = \mathsf{E} + c = \mathsf{V} + \mathsf{F} - 1 + c \pmod 2,$$

and hence $\mathsf{V} + c \equiv 1 \pmod 2$. □

If G has a Pfaffian orientation, then with respect to this orientation every two perfect matchings M and M' must have the same sign: $\operatorname{sgn}(M) = \operatorname{sgn}(M')$.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

In fact, since every cycle of $M \oplus M'$ contains a perfect matching (possibly empty) in its interior, the number of vertices within the cycle must be even. Each cycle of $M \oplus M'$ has an even length, consisting of edges from M and M' alternatingly. By Lemma 4.5 the cycle is oddly oriented. By Lemma 4.3, $\operatorname{sgn}(M) \cdot \operatorname{sgn}(M') = 1$.

Hence for a Pfaffian orientation, every Pfaffian term has the same sign.

Definition 4.6. The perfect matching polynomial, $\operatorname{PerfMatch}(G)$, is the following:

$$\operatorname{PerfMatch}(G) = \sum_{M \in \mathcal{M}(G)} \prod_{e \in M} x_e, \tag{4.8}$$

where $\mathcal{M}(G)$ is the set of all perfect matchings in G and x_e corresponds to the edge e in G.

We will usually assign a value $w(e)$ in a field to each x_e as the edge weight for e. The default choice of the field is $\mathbb{C}$; but one can replace $\mathbb{C}$ by any commutative ring. To discuss the computation of the perfect matching polynomial $\operatorname{PerfMatch}(G)$, we usually fix an assignment of weights $w(e) \in \mathbb{C}$ for x_e. The case $w(e) = 1$ for all edges e in G is called the unweighted case; in this case $\operatorname{PerfMatch}(G)$ is the number of perfect matchings in G. For a graph G with at least one vertex, if it has no perfect matchings, then $\operatorname{PerfMatch}(G) = 0$. By convention if G is the empty graph with no vertices, we define $\operatorname{PerfMatch}(G) = 1$. Pfaffian orientation can be used to compute $\operatorname{PerfMatch}(G)$ for any planar graph G.

Theorem 4.7 (Kasteleyn). *Every connected planar graph has a Pfaffian orientation. Such an orientation can be constructed in polynomial time, leading to a polynomial-time algorithm to compute* $\operatorname{PerfMatch}(G)$ *for any weighted planar graph G.*

Proof. A graph can tested for planarity, and if so a planar embedding of the graph can be computed in polynomial time [HT74]. Assume G is a connected planar graph, and given a planar embedding. If G is a tree, then any orientation is acceptable. If G is not a tree, then choose any edge on the boundary of the outer face that belongs to a cycle. (Such an edge exists by a simple induction: Take any edge e on the boundary of the outer face. If e is a bridge edge, then its removal disconnects G into two parts. Since G is not a tree, at least one part is not a tree. The traversal of the boundary of the outer face of G consists of the concatenation of two traversals of the boundaries of the outer faces of the two parts, in sequence. Then by induction, one edge of the traversal belongs to a cycle.) Let F be the non-outer face containing this edge e. By induction we can construct a Pfaffian orientation for $G - \{e\}$, the graph with the same vertex

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

set as G but with edge e removed. By definition, in this Pfaffian orientation every non-outer face of $G - \{e\}$ contains an odd number of clockwise oriented edges. Now add e back, and orient e appropriately we can guarantee that F also has an odd number of clockwise-oriented edges. This completes the proof by induction.

For a Pfaffian orientation, let $B = B(\overrightarrow{G})$ be the skew-symmetric matrix. Then either $\mathrm{Pf}(B) = \mathrm{PerfMatch}(G)$ or $\mathrm{Pf}(B) = -\mathrm{PerfMatch}(G)$. The equality is a polynomial equality: for the given Pfaffian orientation, either $+$ holds for all weight values, or $-$ holds for all weight values. Setting all weight values to 1, we can decide which sign is valid for the particular orientation (unless there is no perfect matching and G is nonempty, in which we can safely output $\mathrm{PerfMatch}(G) = 0$). Then we can compute $\mathrm{PerfMatch}(G)$ for the actual weight values. If G has connected components $G_1, G_2, \ldots, G_m$, then $\mathrm{PerfMatch}(G) = \prod_{i=1}^{m} \mathrm{PerfMatch}(G_i)$. □

Exercise: Show that $\mathrm{PerfMatch}(G)$ can be computed in polynomial time for weighted plannar (multi)graphs G with self-loops and multiple edges.

4.2 Matchgates

Valiant initially introduced *matchgates* as a way to show that a nontrivial, though restricted, fragment of quantum computation can be simulated in classical polynomial time [Val02b]. At the heart of this simulation technique is a way to encode certain quantum states by a classical computation of perfect matchings, and to simulate certain quantum gates by the so-called matchgates. Subsequently he introduced holographic algorithms using matchgates [Val08]. It is in this context that holographic transformations were introduced. This idea turns out to have a wider applicability as a general reduction method. We have already encountered its use for the dichotomy of Holant* problems in Chapter 2. In the context of holographic algorithms based on matchgates, this is essentially a reduction from a problem to the planar PERFECT MATCHING problem. Theorem 4.7 shows that there is a remarkable polynomial time algorithm – Kasteleyn's algorithm – to compute the weighted sum of perfect matchings for a planar graph. We introduce matchgates in this section.

Definition 4.8. A matchgate is an undirected weighted plane graph G with a subset of distinguished nodes on its outer face, called the external nodes, ordered in a clockwise order.

A plane graph is a planar graph given with a particular planar embedding. Without loss of generality, we assume all edge weights are nonzero; zero weighted edges can be deleted.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Let G be a matchgate with k external nodes. For each length-k bitstring α, G defines a subgraph G^α obtained from G by the following operation: For all $1 \le i \le k$, if the ith bit of α is 1, then we remove the ith external node and all its incident edges. Thus, $G^{00\ldots0} = G$, and $G^{11\ldots1}$ is obtained from G by removing *all* external nodes and their incident edges.

Definition 4.9. We define the signature of a matchgate G as the vector $\Gamma_G = (\Gamma_G^\alpha)$, indexed by $\alpha \in \{0,1\}^k$ in lexicographic order, as follows:

$$\Gamma_G^\alpha = \text{PerfMatch}(G^\alpha) = \sum_{M \in \mathcal{M}(G^\alpha)} \prod_{e \in M} w(e). \tag{4.9}$$

For a perfect matching $M \in \mathcal{M}(G^\alpha)$ we define $\Gamma_G^\alpha(M) = \prod_{e \in M} w(e)$ as the *perfect matching term*, equal to the product of the edge weights for the matching M. Where G is clear, we omit the subscript G, and write Γ for Γ_G, Γ^α for Γ_G^α, and $\Gamma^\alpha(M)$ for $\Gamma_G^\alpha(M)$.

We denote by $\mathscr{M}$ the set of all matchgate signatures .

Definition 4.10. A matchgate signature Γ is *symmetric* if, for all α and β of equal Hamming weight, $\Gamma^\alpha = \Gamma^\beta$.

In other words, the value of a symmetric signature entry is only a function of how many 1's there are in its index, not their particular pattern. These signatures are important because they have a clear combinatorial meaning.

Regarding symmetric signatures that are realizable as matchgate signatures, we will prove

Theorem 4.11. *A symmetric signature is the signature of a matchgate iff it has the following form, for some $a, b \in \mathbb{C}$ and integer k (we take the convention that $0^0 = 1$):*

1. $[a^k b^0, 0, a^{k-1}b, 0, a^{k-2}b^2, 0, \ldots, a^0 b^k]$ *(arity $2k \ge 2$)*
2. $[a^k b^0, 0, a^{k-1}b, 0, a^{k-2}b^2, 0, \ldots, a^0 b^k, 0]$ *(arity $2k+1 \ge 1$)*
3. $[0, a^k b^0, 0, a^{k-1}b, 0, a^{k-2}b^2, 0, \ldots, a^0 b^k]$ *(arity $2k+1 \ge 1$)*
4. $[0, a^k b^0, 0, a^{k-1}b, 0, a^{k-2}b^2, 0, \ldots, a^0 b^k, 0]$ *(arity $2k+2 \ge 2$).*

We will postpone the proof of this theorem until we have properly developed the theory of matchgates.

Some Problems

We list some problems that can be solved in polynomial time using holographic algorithms with matchgates. The first several problems are all from the initial paper by Valiant [Val08].

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

We start with a 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 of a graph such that certain local constraints are satisfied. Pauling [Pau35] initially proposed such a model for planar square lattices, where the constraint was that an orientation assigned exactly two incoming and two outgoing edges at every node. The question of determining how the number of such orientations grows for various planar repeating structures has been extensively studied [Lie67a, Lie67b, Lie67c, Lie67d, Bax82, Wel93].

#PL-3-NAE-ICE

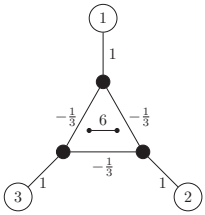
INPUT: A planar graph $G = (V, E)$ of maximum degree 3

OUTPUT: The number of orientations such that no node has all incident edges directed toward it or all incident edges directed away from it

Hence #PL-3-NAE-ICE counts the number of no-sink-no-source orientations. A node of degree 1 will preclude such an orientation. We assume every node has degree 2 or 3. To solve this problem by a holographic algorithm with matchgates, we design a signature grid based on G as follows. We attach to each node of degree 3 a signature $[0, 1, 1, 0]$ (as a contravariant tensor). This represents a NOT-ALL-EQUAL or NAE gate of arity 3. For any node of degree 2 we use a binary NAE signature, i.e., a binary DISEQUALITY signature $(\neq_2) = [0, 1, 0]$ (also a contravariant tensor). For each edge in E we use a binary DISEQUALITY signature $(\neq_2)$ (as a covariant tensor), which stands for an orientation from one node to the other. (To express such a problem, it is completely arbitrary to label one side as contravariant and the other side as covariant tensors; cf. Section 1.3.2 of Chapter 1. They are called generators and recognizers , respectively.) From the given planar graph G we obtain a signature grid Ω, where the underlying graph G' is the edge–vertex incidence graph of G. By definition, Holant_Ω is an exponential sum where each term is a product of appropriate entries of the signatures. Each term is indexed by a 0-1 assignment on all edges of G'; it has value 0 or 1, and it has value 1 iff it corresponds to an orientation of G such that at every vertex of G the local NAE constraint is satisfied. Therefore Holant_Ω is precisely the number of valid orientations required by #PL-3-NAE-ICE.

Note that the signature $[0, 1, 1, 0]$ is not the signature of any matchgate according to Theorem 4.11. A simple reason for this is that a matchgate signature, being defined in terms of perfect matchings, cannot have nonzero values for inputs of both odd and even Hamming weight.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press



(a) A matchgate with signature $[6, 0, -2, 0]$, and $H[6, 0, -2, 0] = [0, 1, 1, 0]$



(b) A matchgate with signature $[2, 0, -2]$, and $H[2, 0, -2] = [0, 1, 0]$. Replacing the weights from ± 2 to $\pm\frac{1}{2}$ gives $\frac{1}{2}[1, 0, -1]$, and $\frac{1}{2}[1, 0, -1]H^{-1} = [0, 1, 0]$.



(c) A matchgate with signature $\frac{1}{2}[1, 0, 1]$, and $\frac{1}{2}[1, 0, 1]H = [1, 0, 1]$.

Figure 4.1. Some matchgates used in #PL-3-NAE-ICE.

However, under a holographic transformation using $H = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ with $H^{-1} = 2H$,

$$(H^{-1})^{\otimes 3}[0, 1, 1, 0] = (H^{-1})^{\otimes 3}\left\{\begin{bmatrix}1\\1\end{bmatrix}^{\otimes 3} - \begin{bmatrix}1\\0\end{bmatrix}^{\otimes 3} - \begin{bmatrix}0\\1\end{bmatrix}^{\otimes 3}\right\} = [6, 0, -2, 0],$$

$$(H^{-1})^{\otimes 2}[0, 1, 0] = H^{\otimes 2}\left\{\begin{bmatrix}1\\1\end{bmatrix}^{\otimes 2} - \begin{bmatrix}1\\0\end{bmatrix}^{\otimes 2} - \begin{bmatrix}0\\1\end{bmatrix}^{\otimes 2}\right\} = [2, 0, -2],$$

and

$$[0, 1, 0]H^{\otimes 2} = \frac{1}{2}[1, 0, -1],$$

as the matrix form of this binary signature is $\frac{1}{4}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. These signatures are all realizable as matchgate signatures, by Theorem 4.11. More concretely, we can exhibit the requisite matchgates in Figures 4.1a and b.

Hence #PL-3-NAE-ICE is precisely the following Holant problem on planar graphs:

$$\text{Holant}([0, 1, 0] \mid [0, 1, 0], [0, 1, 1, 0]) \equiv_{\text{T}}$$
$$\text{Holant}\big(\tfrac{1}{2}[1, 0, -1] \mid [2, 0, -2], [6, 0, -2, 0]\big).$$

Now we may replace each signature $\frac{1}{2}[1, 0, -1]$, $[2, 0, -2]$, and $[6, 0, -2, 0]$ in Ω by its corresponding matchgate; then we can compute Holant_{Ω} in polynomial time by Kasteleyn's algorithm.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

An often useful perspective on holographic transformations is to think of a matrix $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in GL_2(\mathbb{C})$ as representing two generalized truth values of $\left[\mathbf{b}_0 = \begin{pmatrix} a \\ b \end{pmatrix}, \mathbf{b}_1 = \begin{pmatrix} c \\ d \end{pmatrix}\right]$.

We consider a covering problem next. A cycle is a sequence of edges through distinct nodes that starts and ends at the same vertex. A chain is a sequence of edges through distinct nodes that starts and ends at distinct vertices. A cycle-chain cover in $G = (V, E)$ is a set of cycles and chains that are vertex disjoint and the union of their vertex sets is all of V. For real values (x, y), the (x, y) cycle-chain sum of G is the sum of $x^i y^j$ over all cycle-chain covers C, where i and j are the numbers of cycles and chains in C respectively. Note that the $(1, 1)$ cycle-chain sum is the total number of cycle-chain covers G. Note also that the $(2, 0)$ cycle-chain sum is a weighted sum of cycle-chain covers C of G with only cycles, and the weight is 2^i if C has i cycles. In particular, $1/2$ of the $(2, 0)$ cycle-chain sum mod 2 is the parity of the number of Hamiltonian cycles of G. The number of Hamiltonian cycles is #P-hard [LOT03], and the proof can be adapted to show that if nodes of both degrees 2 and 3 are allowed, then the parity problem is $\oplus$P-complete [Val05], which is NP-hard under randomized reduction [VV86]. Similarly, the $(2, 4)$ cycle-chain sum is also $\oplus$P-hard.

#PL-3-CYCLE-CHAIN

INPUT: A planar 3-regular graph $G = (V, E)$

OUTPUT: The $(1, 1)$ cycle-chain sum of G

To solve this problem by a holographic algorithm with matchgates, we design a signature grid as follows. We represent each node of degree 3 in V by a generator with signature $[0, 1, 1, 0]$. For each edge in E we use a recognizer with a binary EQUALITY signature $(=_2) = [1, 0, 1]$, which enforces a 0-1 assignment of the edges, and is interpreted as either taking or not taking the edge in the cycle-chain cover. The signature $[0, 1, 1, 0]$ at each node of degree 3 enforces that the subgraph formed by the edges taken is a spanning subgraph (i.e., a subgraph containing all vertices) and has degree either 1 or 2 at every vertex, hence a cycle-chain cover.

By a holographic transformation using H, both $[6, 0, -2, 0] = (H^{-1})^{\otimes 3}[0, 1, 1, 0]$ and $\frac{1}{2}[1, 0, 1] = [1, 0, 1]H^{\otimes 2}$ are realizable as matchgate signatures (Figures 4.1a and c). Hence #PL-3-CYCLE-CHAIN is computable in polynomial time.

The next problem is a satisfiability problem.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

#PL-3-NAE-SAT

INPUT: A planar formula Φ consisting of a conjunction of NAE clauses each of size 3

OUTPUT: The number of satisfying assignments of Φ

This is a variant of 3SAT. Lichtenstein [Lic82] 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 its negation appears in that clause. The SAT problem is when the gate for each clause is the Boolean OR. When SAT is restricted to planar formulae it is still NP-complete, and its corresponding counting problem is #P-complete. Moreover, for many connectives other than NAE (e.g., EXACTLY-ONE) the unrestricted or the planar decision problems are still NP-complete, and the corresponding counting problems are #P-complete [IMRS98].

We design a signature grid as follows. To each NAE clause we assign a generator with signature $[0, 1, 1, 0]$. To each Boolean variable we assign a generator with signature $(=_k)$, where k is the number of clauses in which the variable appears, either negated or unnegated. Further, if a variable occurrence is negated we have a recognizer $[0, 1, 0]$ along the edge that joins the variable generator and the NAE generator, and if the variable occurrence is unnegated then we use a recognizer $[1, 0, 1]$ instead. Under a holographic transformation using H, $(=_k)$ is transformed to

$$(H^{-1})^{\otimes k}\left\{\begin{bmatrix}1\\0\end{bmatrix}^{\otimes k}+\begin{bmatrix}0\\1\end{bmatrix}^{\otimes k}\right\}=\begin{bmatrix}1\\1\end{bmatrix}^{\otimes k}+\begin{bmatrix}1\\-1\end{bmatrix}^{\otimes k}=2[1,0,1,0,\ldots].$$

Thus, by Theorem 4.11, all the signatures used can be realized by matchgates under a holographic transformation.

The next problem is related to a class of problems called node deletion problems.

Generally speaking, for a graph G and a graph property Φ, one is interested in subsets of vertices S of G such that $G \setminus S$ has the property Φ, where $G \setminus S$ is the graph obtained from G by the removal of S together with all incident edges of S. Often one can also investigate the problem in a subclass of graphs G, such as planar graphs or graphs with maximum degree at most Δ, for some Δ.

The optimization problem is to find a subset of minimum cardinality that can be removed. With an additional threshold parameter k as input together with G, one can define a decision problem on whether a subset of cardinality at most k exists that can be removed in order to satisfy the property. The problem of

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

finding a minimum cardinality subset can be reduced to the decision problem by a polynomial time Turing reduction (Cook reduction), since for the minimum parameter k the answer to the decision problem with $(G \setminus \{v\}, k-1)$ is Yes iff v belongs to some removal subset of minimum cardinality k. Hence we can find a solution subset S of minimum cardinality by using the oracle for decision problem by an iteration. Note that for any subset S' of cardinality $k-1$ such that $(G \setminus \{v\}) \setminus S'$ has property Φ, the subset $S = S' \cup \{v\}$ is a solution to G of minimum cardinality k.

Furthermore, among all removal subsets of minimum cardinality, one can define a counting problem, or a parity counting problem.

The following problem can be solved in polynomial time by holographic algorithms with matchgates.

PL-NODE-BIPARTITION

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

OUTPUT: The minimum cardinality of a subset $S \subset V$ such that $G \setminus S$ is a bipartite graph

Lewis and Yannakakis [LY80] discuss a general approach to such "node deletion" problems. See also [KD79, Yan81a, Yan81b]. If we consider edge deletion instead of node deletion, then this is just another way of defining the problem MAX-CUT, which is NP-hard (and even NP-hard to approximate [GW95, ALM+98, Hås01]). Hadlock proved that planar MAX-CUT is solvable in polynomial time [Had75]. Choi et al. [CNR89] showed that for maximum degree ≤ 3, the minimization problems for node deletion and for edge deletion are equivalent with respect to bipartiteness. Thus PL-NODE-BIPARTITION is also solvable in polynomial time. Choi et al. also proved that for planar graphs with maximum degree ≤ 4, or for general graphs with maximum degree ≤ 3, the decision problem is NP-complete. This improves an earlier result by Krishnamoorthy and Deo [KD79] that the problem is NP-complete for planar graphs with maximum degree ≤ 6.

We can solve the problem PL-NODE-BIPARTITION using a holographic algorithm with matchgates as follows. We may assume all vertices are of degree 2 or 3, as retaining any vertex of degree 1 does not violate bipartiteness. We will use generator signatures $[x, 1, x]$ and $[x, 1, 1, x]$ for a vertex of degree 2 and 3 respectively. These are realizable by matchgates under H. For each edge we use a recognizer signature $[0, 1, 0]$; this results in an orientation. The recognizer signature $[0, 1, 0]$ is also realizable by matchgates under H^{-1}. For any orientation, each source or sink node contributes a factor x, and the other nodes contribute a factor 1. The Holant sum is a polynomial in x, where the degree,

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

i.e., the largest i for which x^i has a nonzero 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.

The degree of this polynomial is 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.

Exercise: Show that, for any x, the signatures $[x, 1, x]$ and $[x, 1, 1, x]$ can be realized by matchgates under H.

Notice that once the minimum cardinality k is obtained to an instance G of PL-NODE-BIPARTITION, we can further compute the parity of the number of subsets S of cardinality k such that S is an independent set and $G \setminus S$ is a connected bipartite graph.

Let S be a subset of cardinality k such that $G \setminus S$ is bipartite. Since k is minimum, any vertex $v \in S$ must have edges connecting to both sides of the bipartite graph $G \setminus S$; otherwise one can keep v and $S - \{v\}$ is a solution to PL-NODE-BIPARTITION with cardinality $k - 1$, a contradiction. Let $G[S]$ be the induced subgraph of G on S, then $G[S]$ is a matching, i.e., every vertex in S has degree at most 1 in $G[S]$. Suppose $G[S]$ has m edges. Let κ be the number of connected components of $G \setminus S$. We claim that there are exactly $2^{m+\kappa}$ orientations counted in the coefficient of x^{n-k} of the Holant sum that correspond to S being a solution to PL-NODE-BIPARTITION. Clearly any orientation that corresponds to S being a solution is counted in the $2^{m+\kappa}$ distinct orientations that are obtained by independently flipping the orientations on the m matching edges, and for each connected component C of $G \setminus S$, flipping all edges $\{(u, v) \mid u \in C \text{ or } v \in C\}$. Note that these edges include any edge connecting a sink or a source node of C with a node in S. However, under an arbitrary flip, for any connected component C, the sink nodes and source nodes become source nodes and sink nodes respectively, and the nodes in S must remain nonsink nonsource nodes, because $|S|$ is minimum.

Clearly, S is an independent set iff $m = 0$ in $G[S]$, and $G \setminus S$ is connected iff $\kappa = 1$. Therefore every independent set S of $|S| = k$ such that $G \setminus S$ is connected and bipartite is counted exactly twice in the Holant sum in the coefficient of x^{n-k}, and all other S of $|S| = k$ contribute a number congruent to 0 mod 4. Hence if we divide this coefficient by 2 and then take the number mod 2, we get the parity of the number of independent sets $S \subset V$ such that $|S| = k$ and $G \setminus S$ is a connected bipartite graph. This solves the problem in polynomial time.

In [Val10], Valiant presents several interesting problems of this kind.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

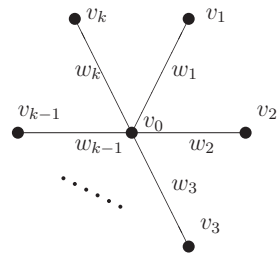


Figure 4.2. A matchgate with an underlying star graph

We now consider a matching problem. Jerrum [Jer87] showed that counting the number of (not necessarily perfect) matchings in a planar graph is #P-complete, and Vadhan [Vad01] subsequently proved that it remains #P-complete even for planar bipartite graphs of degree 6. For degree 2 the problem can be solved easily and one might have conjectured that all other nontrivial cases are #P-complete. However, the following problem [Val08] 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, and (ii) the quantity $-(w_1 + \cdots + w_k)$ for all the V_2 nodes that are not matched, where $w_1, \ldots, w_k$ 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 1, 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.

To solve this problem, we use a different matrix $M = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$. Consider the matchgate pictured in Figure 4.2. This star graph has a central vertex v_0 and k external nodes labeled $v_1, \ldots, v_k$, and the edge (v_0, v_i) has weight w_i $(1 \le i \le k)$. Its signature Γ has nonzero entries only at weight $k-1$, and the value $\Gamma^\alpha = w_i$, where $\alpha = 1^{i-1}01^{k-i}$ has a single 0 at bit position i. The covariant transformation is $\Gamma M^{\otimes k} = \sum_{i=1}^{k} w_i (1,0)^{\otimes(i-1)} \otimes (-1,1) \otimes (1,0)^{\otimes(k-i)}$. This signature has nonzero values $-(w_1 + \cdots + w_k)$ at 0^k, and w_i at $0^{i-1}10^{k-i}$. All other entries of $\Gamma M^{\otimes k}$ are 0.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

To each vertex in V_2 we attach the recognizer signature $\Gamma M^{\otimes k}$ above. To each vertex in V_1 we attach the At-Most-One signature $[1, 1, 0]$ as a generator. Under a contravariant transformation $(M^{-1})^{\otimes 2}[-1, 0, 1] = [1, 1, 0]$. We verify that $M^{\otimes 2}[1, 1, 0] = [-1, 0, 1]$ by its matrix form

$$\begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

and $[-1, 0, 1]$ can be realized by a matchgate consisting of a path of length 3, where the two end vertices are external nodes, and the weights of the three edges are respectively 1, 1 and -1 along the path.

This problem is motivated by its proximity to counting the number of (not necessarily perfect) matchings in a planar graph, which is #P-complete [Jer87]. Still, the quantity $-(w_1 + \cdots + w_k)$ seems a little artificial. If one were to be able to replace $-(w_1 + \cdots + w_k)$ by 1, then one would be able to count all (not necessarily perfect) matchings in such planar bipartite graphs. Later in this chapter, we will develop the theory of matchgates to address the problem of when a desired set of signatures can be realized by a holographic algorithm with matchgates. This theory will show that one cannot replace $-(w_1 + \cdots + w_k)$ by 1.

Now we consider a curious counting satisfiability problem.

#$_7$PL-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: 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 #PL-RTW-MON-3CNF. This problem is known to be #P-complete. Its graphic representation is simply a 2-3-regular graph, i.e., a bipartite graph where every vertex on the left has degree 2 representing a Boolean variable, and every vertex on the right has degree 3 representing an Or clause. For a given planar, read-twice, monotone 3CNF formula Φ, we design a signature grid by assigning the binary Equality signature $[1, 0, 1]$ as a generator for each variable, and the Boolean Or signature on three variables $[0, 1, 1, 1]$ as a recognizer on each clause. We will consider these signatures over the finite field $\mathbb{Z}_7$. Let $M = \begin{bmatrix} 4 & 1 \\ 5 & 1 \end{bmatrix}$, with inverse $M^{-1} = \begin{bmatrix} -1 & 1 \\ 5 & -4 \end{bmatrix}$. We verify that, over $\mathbb{Z}_7$,

$$\begin{aligned} [0, 1, 1, 1](M^{-1})^{\otimes 3} &= [(1, 1)^{\otimes 3} - (1, 0)^{\otimes 3}](M^{-1})^{\otimes 3} \\ &= (4, -3)^{\otimes 3} - (-1, 1)^{\otimes 3} = [2, 0, 2, 0]. \end{aligned}$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Meanwhile $M^{\otimes 2}[1, 0, 1]$ has its matrix form

$$MI_2M^{\mathrm{T}} = \begin{bmatrix} 4 & 1 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 5 \end{bmatrix} = [3, 0, 5].$$

Both $[2, 0, 2, 0]$ and $[3, 0, 5]$ can be realized as matchgate signatures, by Theorem 4.11.

We remark that $\#_2$PL-RTW-MON-3CNF, the parity version of the counting problem #PL-RTW-MON-3CNF, is $\oplus$P-complete [Val06], thus NP-hard under randomized reductions [VV86]. The polynomial time solvability for mod 7 is a surprise, especially in view of its hardness mod 2. In this chapter we will develop the theory to give an explanation of this mystery.

Finally we consider a geometric problem.

2-COLOR-COUNTING

INPUT: A set S of n points on a plane is given, where no three points are colinear. Also given is a set of line segments between some pairs of points in S. We assume no three line segments intersect at a point not in S, and every point of S is incident to either two or three line segments.

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

We use the NAE generator signatures $[0, 1, 0]$ or $[0, 1, 1, 0]$ for each point with either two or three incident line segments respectively. For each intersection of two line segments we use the generator signature $G = (H^{-1})^{\otimes 4}\Gamma$, where Γ is the signature of the matchgate given in Figure 4.3, and $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. G has exactly two nonzero values $G^{0101} = G^{1010} = 1$. This ensures that the coloring on the line segment is properly propagated past an intersection, and two intersecting line segments are colored differently. For each line segment between two consecutive points which are from S or are intersection points, we add a binary EQUALITY recognizer signature $(=_2)$. Under a holographic transformation by H (which is symmetric and, up to a scalar, orthogonal and thus its own inverse), $[0, 1, 0]$, $[0, 1, 1, 0]$ and $(=_2) = [1, 0, 1]$ are all realizable. It follows that the problem 2-COLOR-COUNTING can be solved in polynomial time.

The fact that the matchgate signature Γ is as stated can be directly verified. However, after Section 4.3.2 it will become clear why this construction works.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

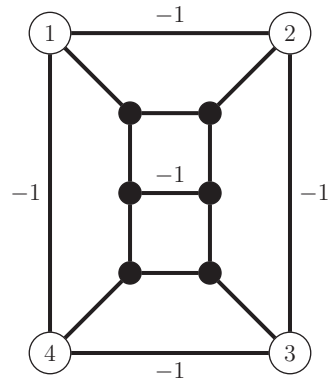


Figure 4.3. A matchgate with signature Γ indexed by $\{0,1\}^4$. Edges without explicitly labeled weight all have weight 1. Listed lexicographically $\Gamma = (1,0,0,-1,0,1,-1,0,0,-1,1,0,-1,0,0,1)^{\mathrm{T}}$. Also see Figure 4.5 in Section 4.3.2. Under the holographic transformation H this matchgate has signature $G = (H^{-1})^{\otimes 4}\Gamma$, up to a nonzero factor, $G^{0101} = G^{1010} = 1$ and $G^{\alpha} = 0$ for other $\alpha \in \{0,1\}^4$.

Exercise: Show that we may compute the signature $G = (H^{-1})^{\otimes 4}\Gamma$ in problem 2-COLOR-COUNTING as follows. The 4×4 matrix form of G is the product $(H^{-1})^{\otimes 2} M(\Gamma)((H^{-1})^{\otimes 2})^{\mathrm{T}}$, where $M(\Gamma)$ is the 4×4 matrix form of Γ which has rows and columns indexed by $\{0,1\}^2$, in lexicographic order, and has entry Γ^{ijkl} in entry at row (ij) and column (kl). Conclude that the 4×4 matrix form of G is, up to a nonzero scalar,

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The two nonzero entries are indexed by 0101 and 1010 respectively. Written with the column listed in reverse order it is, up to a nonzero scalar,

$$\begin{bmatrix} G^{0000} & G^{0010} & G^{0001} & G^{0011} \\ G^{0100} & G^{0110} & G^{0101} & G^{0111} \\ G^{1000} & G^{1010} & G^{1001} & G^{1011} \\ G^{1100} & G^{1110} & G^{1101} & G^{1111} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

For most holographic algorithms that have been studied, the signatures needed are symmetric signatures. For this problem we used an asymmetric

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

signature G. Holographic algorithms that employ asymmetric signatures have not been extensively studied, and will be an interesting topic for the future. 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 signature grid that we obtain a planar graph.

4.3 The Theory of Matchgates

In this section we develop the theory of matchgates. The main result is that there is a set of identities, called matchgate identities, that characterize matchgate signatures.

4.3.1 Matchgate Identities

Without loss of generality we may assume the underlying graph of any matchgate is connected. If it is not connected and there are several connected components G_i, then consider a clockwise traversal of all the external nodes. We may consider the planar embedding is on the sphere with one fixed point in the outer face designated as ∞. We temporarily connect each external node to ∞ by nonintersecting paths. As we clockwise-traverse from one external node u to the next v, if they belong to different components G_i and G_j, we can connect u to v by a path of length 2: $u, e = \{u, w\}, w, e' = \{w, v\}, v$, adding a new node w, and one extra node w' with an edge $\{w, w'\}$. This gadget can be made disjoint from all the temporary paths to ∞, and also disjoint from each other. All new edges (there are three edges on each such gadget) have weight 1. In any perfect matching, w is matched to w' and therefore this gadget has no effect on the signature. Then we remove the temporary paths to ∞. Now the matchgate graph is (1) connected, and (2) its outer face uniquely well-defined for the given planar embedding, with a connected boundary.

By default we assume the edge weights are complex numbers in Definitions 4.8 and 4.9. Thus $\Gamma_G \in \mathbb{C}^{2^k}$, or equivalently we may consider it as a tensor in $(\mathbb{C}^2)^{\otimes k}$. But the theory can be developed in any commutative ring, in particular in a finite field. We will make occasional use of that.

Matchgate signatures satisfy a remarkable set of identities, called the *matchgate identities*. We will show that these identities are a necessary and sufficient condition for a vector of values to be the signature of a matchgate. We state the matchgate identities, or MGI.

Theorem 4.12. *Let Γ be the signature of a matchgate with k external nodes. For any length-k bitstrings $\alpha, \beta \in \{0, 1\}^k$, let $P = \{p_1, \ldots, p_l\}$, where*

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

$p_1 < \cdots < p_l$, be the subset of $[k]$ such that p_i is the ith bit where α and β differ. Then, the signature Γ satisfies

$$\sum_{i=1}^{l}(-1)^i \Gamma^{\alpha \oplus e_{p_i}} \Gamma^{\beta \oplus e_{p_i}} = 0, \tag{4.10}$$

where e_j denotes a length-k bitstring with a 1 in the jth index, and 0 elsewhere.

We will identify P with its characteristic sequence, which is $\alpha \oplus \beta \in \{0,1\}^k$, the bitwise XOR of α and β.

Exercise: Show that, for matchgates of arity at most 3, the parity condition is sufficient. For arity 4, there is a single MGI that is sufficient together with the parity condition.

A perfect matching has an even number of vertices. It follows that $\text{PerfMatch}(G^\alpha) = 0$, whenever G^α has an odd number of vertices. Thus, a matchgate signature satisfies the following:

> *Parity Condition*: For any matchgate signature Γ, either for all α of odd Hamming weight, or for all α of even Hamming weight, $\Gamma^\alpha = 0$.

The parity condition is a consequence of MGI.

Theorem 4.13. *If a vector Γ obeys the MGI, then it also obeys the parity condition.*

Proof. For a contradiction assume $\Gamma^\alpha \neq 0$ and $\Gamma^\beta \neq 0$, for some α and β of even and odd Hamming weight respectively. We define $\widetilde{\Gamma}$ by $\widetilde{\Gamma}^\gamma = \Gamma^{\gamma \oplus \alpha}$. Since $\gamma \oplus \gamma' = (\gamma \oplus \alpha) \oplus (\gamma' \oplus \alpha)$, if the vector Γ obeys the MGI then the vector $\widetilde{\Gamma}$ also obeys the MGI. Also $\widetilde{\Gamma}^{00\ldots0} = \Gamma^\alpha \neq 0$ and $\widetilde{\Gamma}^{\alpha \oplus \beta} = \Gamma^\beta \neq 0$. Note that $\alpha \oplus \beta$ has an odd Hamming weight.

Let $\beta' = \{p_1, \ldots, p_l\}$ be of minimum odd Hamming weight such that $\widetilde{\Gamma}^{\beta'} \neq 0$. Now invoke the MGI on the bitstrings $00\ldots0 \oplus e_{p_1}$ and $\beta' \oplus e_{p_1}$. That gives

$$0 = -\widetilde{\Gamma}^{00\ldots0}\widetilde{\Gamma}^{\beta'} + \sum_{i=2}^{l}(-1)^i \widetilde{\Gamma}^{00\ldots0 \oplus e_{p_1} \oplus e_{p_i}} \widetilde{\Gamma}^{\beta' \oplus e_{p_1} \oplus e_{p_i}}. \tag{4.11}$$

We have $\widetilde{\Gamma}^{00\ldots0}\widetilde{\Gamma}^{\beta'} \neq 0$. If $l = 1$ then the sum $\sum_{i=2}^{l}$ is vacuous, and we have a contradiction. So $l \geq 2$ and we consider each term in the sum $\sum_{i=2}^{l}$. Observe that for every $2 \leq i \leq l$, $\beta' \oplus e_{p_1} \oplus e_{p_i}$ has an odd Hamming weight *less* than that of β', hence $\widetilde{\Gamma}^{\beta' \oplus e_{p_1} \oplus e_{p_i}} = 0$. Thus the sum $\sum_{i=2}^{l}$ is 0 but $\widetilde{\Gamma}^{00\ldots0}\widetilde{\Gamma}^{\beta'} \neq 0$, a contradiction. □

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Nonetheless, because the parity condition is a set of linear equations, and the MGI are quadratic, in practice the parity condition is a good criterion to apply first.

Exercise: Show that, for matchgates of arity at most 3, the parity condition also implies MGI. For signatures of arity 4 satisfying the parity condition, there is a single MGI that is sufficient to imply all MGI.

MGI were first introduced by Valiant in [Val02a, Val02b] in the context of proving certain 2-input 2-output quantum gates cannot be realized by a matchgate. It was shown that 2-input 2-output matchgates must satisfy certain identities that are named the matchgate identities. These identities are actually concerned with *characters* of matchgates. These so-called characters are defined directly in terms of Pfaffians, and their underlying matchgates need not be planar by definition. In the case of 2-input 2-output matchgates, these character values constitute a 4×4 matrix, called a character matrix. Subsequently [CC06, CCL09, CG14] this theory is generalized to matchgates of an arbitrary number of external nodes. The ultimate result is that there is an equivalence of matchgate characters (of not necessarily planar matchgates) and matchgate signatures (of planar matchgates). Furthermore, matchgate identities characterize matchgate signatures. Theorem 4.12 states that MGI is a necessary condition. Theorem 4.18 states that MGI is also sufficient and will be proved in Section 4.3.2.

The matchgate identities are inspired by a set of identities called Pfaffian signature identities. These identities have the same form as MGI but apply to Pfaffian signatures. The original discovery and proof of MGI are based on the Pfaffian signature identities, but we will present with permission a short and elegant bijective proof of MGI due to Jerrum [Jer15].

If we fix any Pfaffian orientation for G, it defines a directed graph $\overrightarrow{G}$. Then $\overrightarrow{G}^{\alpha}$, which is obtained from $\overrightarrow{G}$ by removing some vertices and their incident edges according to α, is *also* Pfaffian oriented. This is because we remove zero or more vertices only on the outer face, and the removal of these vertices and their incident edges does not create any *non-outer face*. Thus a single fixed Pfaffian orientation for G induces a set of Pfaffian orientations, one for each G^{α}. We assume a Pfaffian orientation for G is fixed, and each G^{α} inherits the induced Pfaffian orientation.

As the orientation in $\overrightarrow{G}$ induces a Pfaffian orientation for all G^{α}, we can naturally refer to the oriented graph $\overrightarrow{G^{\alpha}} = \overrightarrow{G}^{\alpha}$. The skew-symmetric matrix $B(\overrightarrow{G^{\alpha}})$ is obtained from $B(\overrightarrow{G})$ (see (4.4)) by removing the appropriate rows and columns indicated by the 1's in α. We abbreviate $\mathrm{Pf}(B(\overrightarrow{G^{\alpha}}))$ as $\mathrm{Pf}^{\alpha}_{\overrightarrow{G}}$. Where $\overrightarrow{G}$ is clear, we just write Pf^{α}. With a given Pfaffian orientation on the plane graph

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

G, and a given labeling of its k external nodes in clockwise order, we define the Pfaffian signature of $\overrightarrow{G}$ as follows.

Definition 4.14. The Pfaffian signature of $\overrightarrow{G}$ is the vector (Pf^{α}) indexed by $\alpha \in \{0,1\}^k$.

Each Pfaffian signature entry Pf^{α} is a sum of Pfaffian terms (see (4.5) and (4.6)) for $\overrightarrow{G^{\alpha}}$. Each nonzero Pfaffian term $\mathrm{Pf}_{\overrightarrow{G^{\alpha}}}(M)$ corresponds to a perfect matching $M \in \mathcal{M}(G^{\alpha})$.

By the property of a Pfaffian orientation, $\mathrm{Pf}(B(\overrightarrow{G})) = \pm\mathrm{PerfMatch}(G)$ is a term by term equation. Thus, for every $\alpha \in \{0,1\}^k$, there exists $\epsilon(\alpha) \in \{-1,1\}$, such that for all $M \in \mathcal{M}(G^{\alpha})$,

$$\mathrm{Pf}_{\overrightarrow{G^{\alpha}}}(M) = \epsilon(\alpha)\Gamma_{G^{\alpha}}(M). \tag{4.12}$$

The sign $\epsilon(\alpha)$ is the same for every $M \in \mathcal{M}(G^{\alpha})$.

Theorem 4.15. *Let $\overrightarrow{G}$ be a plane graph with a Pfaffian orientation and k external nodes. For any length-k bitstrings $\alpha, \beta \in \{0,1\}^k$, let $P = \{p_1, \ldots, p_l\}$, where $p_1 < \cdots < p_l$, be the subset of $[k]$ whose characteristic sequence is $\alpha \oplus \beta$. Then,*

$$\sum_{i=1}^{l} (-1)^i \mathrm{Pf}^{\alpha \oplus e_{p_i}} \mathrm{Pf}^{\beta \oplus e_{p_i}} = 0. \tag{4.13}$$

Theorem 4.15 will follow from the Grassmann–Plücker identities over Pfaffian minors of a matrix. We state the following definition of the Grassmann–Plücker identities for a skew-symmetric matrix A. In writing $\mathrm{Pf}(i_1, i_2, \ldots, i_K)$ we mean the Pfaffian of the $K \times K$ matrix whose rows and columns are the $i_1, i_2, \ldots, i_K$th rows and columns of A, in that order. The order matters: $\mathrm{Pf}(i_1, i_2, \ldots) = -\mathrm{Pf}(i_2, i_1, \ldots)$, for instance. In particular, if there are two identical rows and columns, the Pfaffian is 0. When we write $\mathrm{Pf}(i_1, i_2, \ldots, \widehat{i_k}, \ldots, i_K)$, the $\widehat{i_k}$ means that i_k is explicitly excluded from that list.

Theorem 4.16. (The Grassmann–Plücker Identities). *Let $I = \{i_1, i_2, \ldots, i_K\}, J = \{j_1, j_2, \ldots, j_L\}$ be subsets of indices of a skew-symmetric A, where $i_1 < i_2 < \cdots < i_K$ and $j_1 < j_2 < \cdots < j_L$. Then*

$$\sum_{\ell=1}^{L} (-1)^{\ell-1} \mathrm{Pf}(j_\ell, i_1, \ldots, i_K) \mathrm{Pf}(j_1, \ldots, \widehat{j_\ell}, \ldots, j_L)$$

$$+ \sum_{k=1}^{K} (-1)^{k-1} \mathrm{Pf}(i_1, \ldots, \widehat{i_k}, \ldots, i_K) \mathrm{Pf}(i_k, j_1, \ldots, j_L) = 0. \tag{4.14}$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Theorem 4.16 has the following short proof [Val02b, Mur00] originally from [Oht92].

Proof of Theorem 4.16. From the definition of Pfaffian:

$$\mathrm{Pf}(j_\ell, i_1, \ldots, i_K) = \sum_{k=1}^{K} (-1)^{k-1} \mathrm{Pf}(j_\ell, i_k) \mathrm{Pf}(i_1, \ldots, \widehat{i_k}, \ldots, i_K)$$

$$\mathrm{Pf}(i_k, j_1, \ldots, j_L) = \sum_{\ell=1}^{L} (-1)^{\ell-1} \mathrm{Pf}(i_k, j_\ell) \mathrm{Pf}(j_1, \ldots, \widehat{j_\ell}, \ldots, j_L)$$

and also $\mathrm{Pf}(j_\ell, i_k) + \mathrm{Pf}(i_k, j_\ell) = 0$. The proof is completed by substituting these into (4.14). □

There is another form of these identities that is more closely related to the Pfaffian signature identities (4.13).

Theorem 4.17. *Let A, I, J be as in Theorem 4.16. For a subset S of indices of A, we write* $\mathrm{Pf}(S)$ *when S is listed in increasing order. Let $I \Delta J = \{k_1, \ldots, k_m\}$ (listed in increasing order) be the symmetric difference of I and J. Then*

$$\sum_{s=1}^{m} (-1)^{s-1} \mathrm{Pf}(I \Delta \{k_s\}) \mathrm{Pf}(J \Delta \{k_s\}) = 0. \tag{4.15}$$

Proof of Theorem 4.17. We prove Theorem 4.17 by Theorem 4.16.

Consider a term in (4.14), and let x be the element that is moved from the index set of one Pfaffian to another. If $x \in I \cap J$, clearly the term is 0. It follows that there is a one-to-one correspondence between the remaining terms in (4.14) and the terms in (4.15). All we need to show is that each such term in (4.14) has the same sign as its counterpart in (4.15).

Suppose $x \in J - I$. In that case, the term in (4.14) is

$$(-1)^z \mathrm{Pf}(x, i_1, \ldots, i_K) \mathrm{Pf}(j_1 \ldots, \hat{x}, \ldots, j_L),$$

where z is the number of elements in J less than x. We write $z = a + b$, where

$$\begin{aligned} a &= |\{y \mid y \in J - I, y < x\}| \\ b &= |\{y \mid y \in J \cap I, y < x\}|, \end{aligned}$$

and we also define

$$c = |\{y \mid y \in I - J, y < x\}|.$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

We can put the indices in $\mathrm{Pf}(x, i_1, \ldots, i_K)$ in increasing order by moving x along until it is in its proper place. To do this we move x exactly $b + c$ entries. Thus

$$\mathrm{Pf}(x, i_1, \ldots i_K) = (-1)^{b+c}\mathrm{Pf}(I \cup \{x\})$$

and so it follows that

$$(-1)^z\mathrm{Pf}(x, i_1, \ldots i_K) = (-1)^{a+c}\mathrm{Pf}(I \cup \{x\}).$$

It is clear that $a + c$ is precisely the number of those in $I \Delta J$ less than x, exactly the sign in front of the corresponding term in (4.15).

The argument for the case $x \in I - J$ is symmetric. □

Now we are ready to prove Theorem 4.15.

Proof of Theorem 4.15. We prove Theorem 4.15 by Theorem 4.17. For a matchgate G, let α and β be two bitstrings of length k, where k is the number of external nodes in G. The ith bit of α, denoted as α_i, corresponds to the ith external node in G in clockwise order.

Let U be the set of all internal (i.e., not external) nodes in G. We define $I = \{v_i \mid \alpha_i = 0\} \cup U$, where v_i is the label of the ith external node in G. Similarly let $J = \{v_i \mid \beta_i = 0\} \cup U$. Observe that $I \Delta J = \{v_i \mid \alpha_i \neq \beta_i\}$. It follows that there is a term-for-term correspondence between (4.15) of Theorem 4.17 and (4.13) of Theorem 4.15. □

Now we present a bijective proof of MGI , Theorem 4.12. This proof is due to Jerrum [Jer15].

We first note that MGI trivially hold if l is odd. In this case, α and β have opposite parity, and so does $\alpha \oplus e_{p_i}$ and $\beta \oplus e_{p_i}$ for every p_i, and thus one of $G^{\alpha \oplus e_{p_i}}$ and $G^{\beta \oplus e_{p_i}}$ has an odd number of nodes, and hence MGI trivially holds by the parity condition. So we may assume l is even.

As before, we denote by $\mathcal{M}(G)$ the set of all perfect matchings of the graph G. We will establish a weight-preserving bijection

$$\bigcup_{i \text{ odd}} \left[\mathcal{M}(G^{\alpha \oplus e_{p_i}}) \times \mathcal{M}(G^{\beta \oplus e_{p_i}})\right] \longleftrightarrow \bigcup_{j \text{ even}} \left[\mathcal{M}(G^{\alpha \oplus e_{p_j}}) \times \mathcal{M}(G^{\beta \oplus e_{p_j}})\right].$$

More precisely, note that the MGI can be stated as

$$\sum_{1 \le i \le l,\ i \text{ odd}} \Gamma^{\alpha \oplus e_{p_i}} \Gamma^{\beta \oplus e_{p_i}} = \sum_{1 \le j \le l,\ j \text{ even}} \Gamma^{\alpha \oplus e_{p_j}} \Gamma^{\beta \oplus e_{p_j}}. \tag{4.16}$$

The product $\Gamma^{\alpha \oplus e_{p_i}} \Gamma^{\beta \oplus e_{p_i}}$ is a sum over all pairs $(M, M') \in \mathcal{M}(G^{\alpha \oplus e_{p_i}}) \times \mathcal{M}(G^{\beta \oplus e_{p_i}})$ of the product of their weight $w(M)w(M')$.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Take any $(M, M') \in \mathcal{M}(G^{\alpha \oplus e_{p_i}}) \times \mathcal{M}(G^{\beta \oplus e_{p_i}})$, consider their XOR $M \oplus M'$. Since M and M' are matchings in G, $M \oplus M'$ consists of a set of alternating paths and alternating cycles of even length. Since $\alpha_{p_i} \neq \beta_{p_i}$, there is an alternating path starting at p_i in $M \oplus M'$. This alternating path must end in some external node p_j. By planarity of G, there must be an even number of external nodes between i and j in cyclic order, among $\{p_1, p_2, \ldots, p_l\} - \{p_i, p_j\}$. This is because each external node in this list is the initial node of an alternating path in $M \oplus M'$, and must end at a node on this list. Alternating paths in $M \oplus M'$ do not cross paths in a plane graph G. An alternating path starting at any p_s where s is between i and j in cyclic order, either $i < s < j$ or $j < s < i$, must end in a node p_t with $i < t < j$ or $j < t < i$ respectively.

If we flip the edges of M and M' along the alternating path from p_i to p_j we obtain another pair $(\widetilde{M}, \widetilde{M'}) \in \mathcal{M}(G^{\alpha \oplus e_{p_j}}) \times \mathcal{M}(G^{\beta \oplus e_{p_j}})$. It is clearly an *involution*, i.e., this mapping is its own inverse. This sets up a bijective map between $\bigcup_{i \text{ odd}} [\mathcal{M}(G^{\alpha \oplus e_{p_i}}) \times \mathcal{M}(G^{\beta \oplus e_{p_i}})]$ and $\bigcup_{j \text{ even}} [\mathcal{M}(G^{\alpha \oplus e_{p_j}}) \times \mathcal{M}(G^{\beta \oplus e_{p_j}})]$.

It is clear that the product of weight $w(M)w(M')$, which is just a product of all edge weights of the alternating paths and cycles of $M \oplus M'$ (together with $w(e)^2$ from length 2 "cycles" for every edge $e \in M \cap M'$), is identical to $w(\widetilde{M})w(\widetilde{M'})$. The bijective map preserves the weight in the two sides of (4.16). This proves Theorem 4.12.

4.3.2 MGI Imply Matchgate-Realizable

Theorem 4.12 showed that the signature of any matchgate must satisfy the MGIs. In this subsection, we show that any $\Gamma \in (\mathbb{C}^2)^{\otimes k} = \mathbb{C}^{2^k}$ satisfying the MGIs can be realized as the signature of a matchgate with k external nodes. Thus MGIs are not only necessary but also sufficient conditions for matchgate signatures.

Consider a length 2^k vector Γ indexed by $\{0, 1\}^k$ satisfying MGI. If it is the all-zeros vector then it is trivially realizable. So assume there is at least one nonzero value.

Preprocessing Assume $\Gamma^{\beta} \neq 0$, for some $\beta \in \{0, 1\}^k$. Define $\Gamma'^{\alpha} = \Gamma^{\alpha \oplus \overline{\beta}} / \Gamma^{\beta}$, where $\overline{\beta} = \beta \oplus 11 \ldots 1$. Thus, $\Gamma'^{11\ldots1} = 1$, and Γ' also satisfies MGI. In this section we will create a matchgate G' with signature Γ'. Given such a G', we can create a matchgate G with signature Γ as follows. First we add two new nonexternal nodes u, v to G' and an edge $\{u, v\}$ of weight Γ^{β}. Those two nodes are not connected to any other nodes – in effect they contribute exactly a factor Γ^{β} to each perfect matching term. Then, if the ith bit of β is 0, we add a new edge $\{v_i, v_i'\}$ of weight one to the ith external node v_i,

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

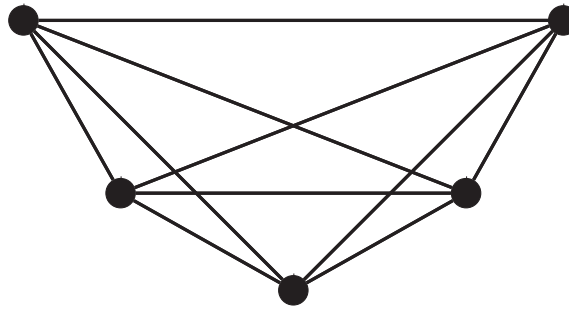


Figure 4.4. The embedding for K_5.

and making v_i' the new ith external node. It follows that the signature of G is exactly Γ.

Construction We now show that we can realize Γ satisfying MGI and $\Gamma^{11\ldots1} = 1$. Let K_k denote the complete graph on k vertices. The labels of K_k are ordered $1 < 2 < \cdots < k$, and correspond to the bit positions in the index for Γ. We place the nodes of K_k on a convex curve, as illustrated in Figure 4.4. The nodes are arranged in clockwise order by their index, and two edges cross each other geometrically in the drawing of the graph iff their labels form an overlapping pair as defined before algebraically. (We assume the k nodes are placed in general position, so that any pair of crossing edges intersect at a unique point. There are exactly $\binom{k}{4}$ such intersection points.) For each α of Hamming weight $k-2$, note that K_k^α has exactly one edge left. For each such α, set the weight of the unique edge in K_k^α to be Γ^α. This defines a weight for every edge of K_k.

Equality with Pfaffian Clearly our embedding of K_k is not planar for a general $k \geq 4$. We first prove the following equality. Let $\mathrm{Pf}(K_k^\alpha)$ be the Pfaffian value of the skew-symmetric matrix representing K_k^α, where the nodes of K_k^α have the induced order $1 < 2 < \cdots < k$. Then for all $\alpha \in \{0, 1\}^k$:

$$\mathrm{Pf}\big(K_k^\alpha\big) = \Gamma^\alpha. \tag{4.17}$$

It follows that the $\binom{k}{2}$ edge weights of K_k determine the 2^k values of any Γ satisfying MGI.

Equation (4.17) holds trivially for any α of Hamming weight $k-l$, for any odd l. The left-hand side is a Pfaffian of a matrix with an odd number of rows and columns, hence 0, and the right-hand side is 0 by the parity condition and Theorem 4.13. Now we consider the case when l is even.

Clearly (4.17) holds for any α of Hamming weight greater than or equal to $k-2$. By assumption Γ satisfies the MGIs (4.10). Inductively, consider α

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

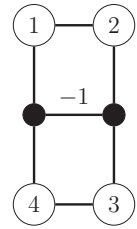


Figure 4.5. The crossover gadget. The external nodes are those labeled, and all edge weights are 1, except the edge labeled -1.

with Hamming weight $k - l$ for some even $l > 2$. Let $\{p_1, \ldots, p_l\}$ be the set of indices listed in increasing order $p_1 < \cdots < p_l$, where α has the bit 0. These are the bit positions where α differs from 1^k. Consider the MGI on $\alpha \oplus e_{p_1}$ and $1^k \oplus e_{p_1}$:

$$\Gamma^{\alpha}\Gamma^{11\ldots1} = \sum_{i=2}^{l}(-1)^i \Gamma^{\alpha \oplus e_{p_1} \oplus e_{p_i}} \Gamma^{1^k \oplus e_{p_1} \oplus e_{p_i}}. \tag{4.18}$$

As $\Gamma^{11\ldots1} = 1$, we see that Γ^{α} is defined by higher Hamming weight terms.

Thus all lower Hamming weight terms of Γ are determined by those of weight $k - 2$, or equivalently the $\binom{k}{2}$ edge weights of K_k. However, by Theorem 4.17, the Pfaffian values also satisfy exactly the same identities as MGI. By induction, it follows that $\mathrm{Pf}(K_k^{\alpha}) = \Gamma^{\alpha}$ for all α. We have proved (4.18).

Planarizing K_k We want to show next that there exists a *planar* matchgate G with signature $\Gamma_G = \Gamma$. We construct such a G from K_k. Consider the convex embedding of K_k. For $k \geq 4$ it has some edge crossings, as shown in Figure 4.4. The planar graph G is created by replacing each edge crossing with a *crossover gadget* from Figure 4.5. The crossover gadget is itself a matchgate X with the following signature:

$$X^{0000} = 1, \quad X^{0101} = 1, \quad X^{1010} = 1, \quad X^{1111} = -1$$

and for all other $\beta \in \{0, 1\}^4$, $X^{\beta} = 0$. We note that even though geometrically this gadget is only symmetric under a rotation of π (but not $\pi/2$), its signature is invariant under a cyclic permutation, and thus functionally it is symmetric under a rotation of $\pi/2$. Now we replace every crossing of a pair of edges in the embedded K_k by a copy of X. For example, this replacement by the crossover gadget changes Figure 4.4 to Figure 4.6. If an edge $\{i, j\}$ in K_k crosses some other edges (this happens for every nonadjacent i and j in the cyclic sense), then this replacement breaks the edge $\{i, j\}$ into several parts. If $\{i, j\}$ crosses $t \geq 0$ other edges, then it is replaced by t copies of the crossover gadget, connected by

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

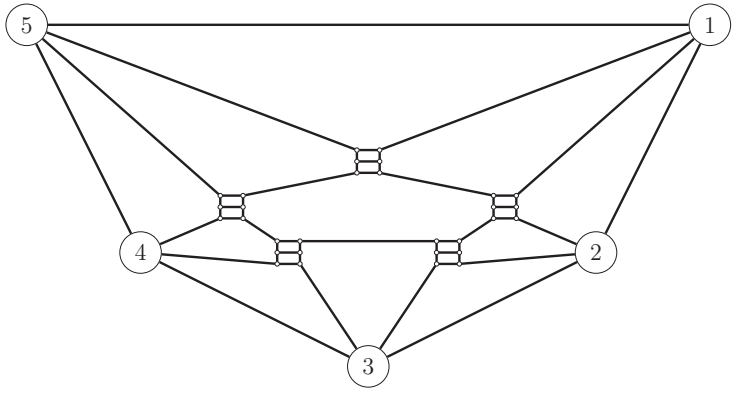


Figure 4.6. The graph from Figure 4.4 with the crossovers replaced by crossover gadgets from Figure 4.5.

$t + 1$ edges outside of crossover gadgets. Of course one copy of the crossover gadget is used for both edges of a pair of crossing edges in this replacement (see Figure 4.7). Define I to be the set of all edges in G that are *not* part of a crossover gadget. Then each edge $\{i, j\}$ in K_k defines a unique subset of edges in I, which we call the *i-j passage*. It is clear that I is a disjoint union of these i-j passages, over all $\binom{k}{2}$ pairs $1 \leq i < j \leq k$. Finally, we choose one edge in each i-j passage to have the weight $\Gamma^{[k]-\{i,j\}}$, namely the edge weight of $\{i, j\}$

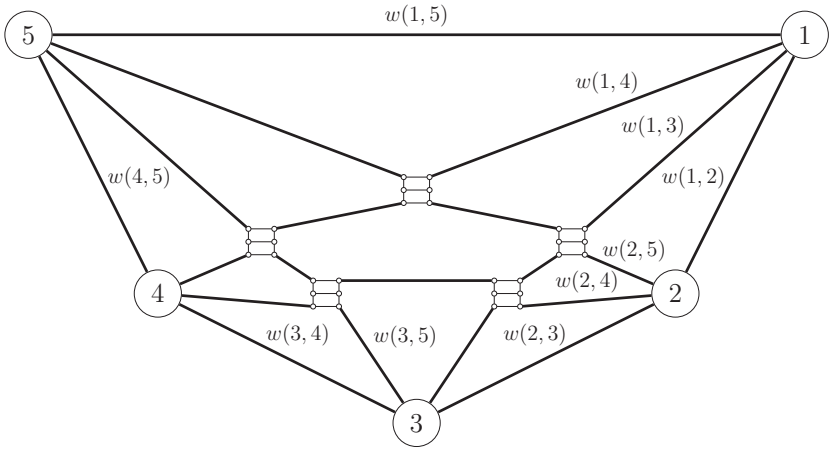


Figure 4.7. The "planarized" K_5 with edge weights. The unlabeled edges have weight 1. For notational simplicity, in the figure we use the notation $w(i, j)$ for $w(\{i, j\})$.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

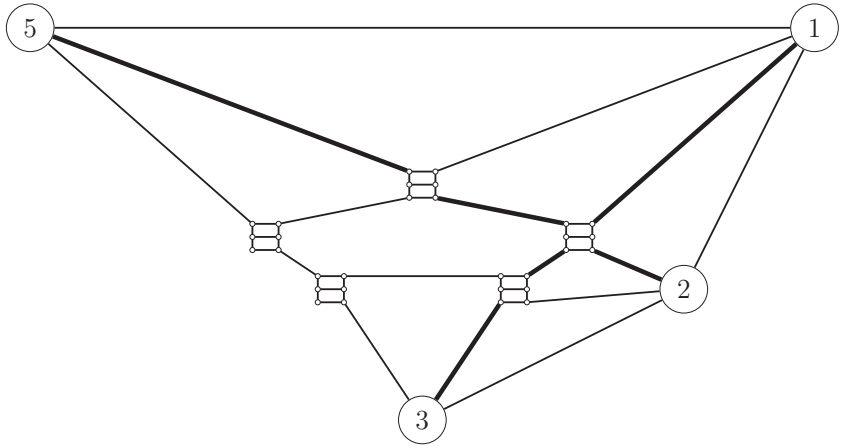


Figure 4.8. The thick edges comprise $S(M)$ for G^{00010}, where $M = \{\{1, 3\}, \{2, 5\}\}$.

in K_k. To be specific, we will choose this edge to be the one adjacent to i, the lower indexed external node of $\{i, j\}$. All other edges of I are assigned weight 1 (see Figure 4.7). This defines our planar matchgate G with external nodes $1 < 2 < \cdots < k$.

We claim that $\Gamma_G = \Gamma$.

Fix any $\alpha \in \{0, 1\}^k$. For any $S \subseteq I$, define $\mathcal{M}_S(G^\alpha)$ to be the subset of all perfect matchings $M' \in \mathcal{M}(G^\alpha)$ such that $M' \cap I = S$. Every perfect matching $M \in \mathcal{M}(K_k^\alpha)$ defines a collection of i-j passages, one for each $\{i, j\} \in M$. Let $S(M)$ be the union of these i-j passages. Clearly the perfect matching $M \in \mathcal{M}(K_k^\alpha)$ can be recovered from $S(M)$, and is unique for the given $S(M)$. There is a 1-1 correspondence between M and $S(M)$. As an example, we consider $M = \{\{1, 3\}, \{2, 5\}\} \in \mathcal{M}(K_5^{00010})$. The set $S(M)$ for G^{00010} are the thick edges in Figure 4.8.

We will show that, for the purpose of computing the signature entry Γ_G^α, we need to consider only those perfect matchings $M' \in \mathcal{M}(G^\alpha)$ that satisfy the following property:

Property: There exists an $M \in \mathcal{M}(K_k^\alpha)$, such that

$$M' \cap I = S(M). \tag{4.19}$$

This is a consequence of the properties of the crossover gadget. If i is an external node in G^α, then any $M' \in \mathcal{M}(G^\alpha)$ must contain a unique edge e' incident to i. There is a unique j, which is another external node in G, such that e' belongs to the i-j passage. Then by the properties of the crossover gadgets along

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

this i-j passage, we may assume M' contains all edges of this i-j passage, saturating j. In particular, j belongs to G^α. All other M' collectively contribute 0, since the evaluation of the crossover gadget X will be 0. More formally, in the computation of $\Gamma_G^\alpha = \sum_{M' \in \mathcal{M}(G^\alpha)} \prod_{e' \in M'} w(e')$, we classify all $M' \in \mathcal{M}(G^\alpha)$ according to $M' \cap I$. If $S \neq S(M)$ for any $M \in \mathcal{M}(K_k^\alpha)$, then

$$\sum_{M' \in \mathcal{M}(G^\alpha):\ M' \cap I = S} \prod_{e' \in M'} w(e') = 0. \tag{4.20}$$

In fact, for any $M' \in \mathcal{M}(G^\alpha)$ such that $M' \cap I = S$ that is not $S(M)$ for any $M \in \mathcal{M}(K_k^\alpha)$, it must be the case that at some crossover gadget X, S induces an external removal pattern $\beta \notin \{0000, 0101, 1010, 1111\}$. Then $X^\beta = 0$, and (4.20) follows.

Thus we restrict to those perfect matchings $M' \in \mathcal{M}(G^\alpha)$ that satisfy the property (4.19). For any $M \in \mathcal{M}(K_k^\alpha)$, it is clear that

$$\sum_{M' \in \mathcal{M}_{S(M)}(G^\alpha)} \prod_{e' \in M'} w(e') = (-1)^{c(M)} \prod_{e \in M} w(e), \tag{4.21}$$

where $c(M)$ counts the number of copies of X where the external removal pattern is $\beta = 1111$. Thus $c(M)$ is exactly the number of overlapping pairs in M. It follows that

$$\begin{aligned}
\Gamma_G^\alpha &= \sum_{M' \in \mathcal{M}(G^\alpha)} \prod_{e' \in M'} w(e') \\
&= \sum_{S \subseteq I} \sum_{M' \in \mathcal{M}_S(G^\alpha)} \prod_{e' \in M'} w(e') \\
&= \sum_{M \in \mathcal{M}(K_k^\alpha)} \sum_{M' \in \mathcal{M}_{S(M)}(G^\alpha)} \prod_{e' \in M'} w(e') \\
&= \mathrm{Pf}\big(K_k^\alpha\big).
\end{aligned}$$

The last equality is because each Pfaffian term in $\mathrm{Pf}(K_k^\alpha)$ has exactly the same sign as in (4.21). Hence $\Gamma_G = \Gamma$ follows from this and (4.17).

Theorem 4.18. *Any $\Gamma \in (\mathbb{C}^2)^{\otimes k}$ satisfying the MGI is the signature of a matchgate with k external nodes. The matchgate has $O(k^4)$ nodes. If $\Gamma^{11\ldots1} = 1$, which is achievable by a normalization for every nonzero Γ, there exists a skew-symmetric matrix $M \in \mathbb{C}^{k \times k}$ such that $\Gamma^\alpha = \mathrm{Pf}(M^\alpha)$, where M^α is the matrix obtained from M by deleting all rows and columns belonging to the subset denoted by α.*

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Thus, after a normalization of $\Gamma^{11\ldots1} = 1$, a matchgate signature of arity k has a general parametrized form as the sub-Pfaffians of a $k \times k$ skew-symmetric matrix.

For example, consider the matchgate in Figure 4.3 for the problem 2-COLOR-COUNTING in Section 4.2. Its signature is $\Gamma = (1, 0, 0, -1, 0, 1, -1, 0, 0, -1, 1, 0, -1, 0, 0, 1)^{\mathrm{T}} \in \{0, 1\}^4$. The signature is given by the sub-Pfaffians of

$$\begin{bmatrix} 0 & -1 & +1 & -1 \\ +1 & 0 & -1 & +1 \\ -1 & +1 & 0 & -1 \\ +1 & -1 & +1 & 0 \end{bmatrix}.$$

After assigning appropriate edge weights to K_4 according to this matrix, we obtain the matchgate by replacing the single crossover of edges $\{1, 3\}$ and $\{2, 4\}$ by the crossover gadget in Figure 4.5. This results in the matchgate depicted in Figure 4.3.

4.3.3 Symmetric Signatures by Matchgates

We say a matchgate signature is *even* if it is the signature of an even matchgate, i.e., a matchgate with an even number of nodes. An even signature has nonzero values only for indices of even Hamming weight. We define an *odd* signature similarly. Recall that a symmetric arity-k signature can be denoted as $[z_0, z_1, \ldots, z_k]$, where z_i is the value of the signature for an index of Hamming weight i. The symmetric signatures that obey the MGI have a very concise description, which we prove next.

Theorem 4.19. *If $[z_0, \ldots, z_k]$ is an even symmetric matchgate signature, then $z_i = 0$ for all odd i, and there exist r_1 and r_2 not both zero such that for all even $i \geq 2$:*

$$r_1 z_{i-2} = r_2 z_i.$$

Conversely, every sequence of values satisfying these conditions is an even symmetric matchgate signature. The statement for odd symmetric signatures is analogous.

Stated equivalently, a sequence is a symmetric matchgate signature iff it takes the following form: Alternate entries of $[z_0, \ldots, z_k]$ are zero and the entries at the other alternate positions form a geometric progression.

Proof. By the parity condition, all odd parity entries of the signature of an even matchgate are 0. Consider any *even* i and j, where $0 \leq i < j \leq k$. We invoke the

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

MGI for $\alpha = 1^i 10^{k-i-1}$, $\beta = 1^i 01^{j-i-1} 0^{k-j}$, so that $\alpha \oplus \beta = 0^i 1^{j-i} 0^{k-j}$. We use the exponentiation notation here to denote repetition. The bitstring α has an odd Hamming weight $i+1$ and β has an odd Hamming weight $j-1$. Note that i and j being both even implies that $j - i - 1 \geq 1$. Using the fact that Γ is symmetric, the MGI under α, β can be simplified:

$$\sum_{s=1}^{j-i} (-1)^s \Gamma^{\alpha \oplus e_{i+s}} \Gamma^{\beta \oplus e_{i+s}} = -z_i z_j + \sum_{s=2}^{j-i} (-1)^s z_{i+2} z_{j-2} = 0. \tag{4.22}$$

There are an odd number of terms in the sum $\sum_{s=2}^{j-i} (-1)^s z_{i+2} z_{j-2}$ and the terms alternate their signs and begin with a $+$, so we conclude that

$$z_i z_j = z_{i+2} z_{j-2}.$$

In particular, if i is even and $0 \leq i \leq k-4$, then

$$z_i z_{i+4} = z_{i+2}^2.$$

If $z_{i+2} \neq 0$, then both $z_i \neq 0$ and $z_{i+4} \neq 0$. This means that if any even indexed entry that is not the first or the last even indexed entry (call it a nonexternal entry) is nonzero, then all even indexed entries are nonzero. In this case, the geometric progression is established, with common ratio $z_{i+2}/z_i = z_{i+4}/z_{i+2}$, for even $0 \leq i \leq k-4$.

Suppose all nonexternal even indexed entries are 0. If $k \leq 3$ then the theorem is self-evident. Suppose $k \geq 4$. Let $k^* \leq k$ be the maximum even index. Then $k^* \geq 4$ and we have

$$z_0 z_{k^*} = z_2 z_{k^*-2}.$$

Thus $z_2 = 0$. It follows that $z_0 z_{k^*} = 0$ and therefore at most one extremal even indexed entry can be nonzero. It is also easy to verify that a sequence satisfying the conditions of this theorem satisfies MGI, and hence is a matchgate signature. (We will give a direct construction shortly.) This completes the proof for even signatures. The proof for odd signatures is similar. The theorem follows. □

The explicit list of symmetric signatures in Theorem 4.11 follows from Theorem 4.19.

We have already demonstrated how to build a planar matchgate realizing any MGI-satisfying signature, through a planarizing procedure. It is instructive, however, to give a direct construction for the symmetric case. For the symmetric signature EXACT-ONE-1 $= [0, 1, 0, \ldots, 0]$ of arity n that represents a perfect matching, and its reversal EXACT-ONE-0 $= [0, \ldots, 0, 1, 0]$, we can design a matchgate based on a star graph. For EXACT-ONE-0 we take a star graph with

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

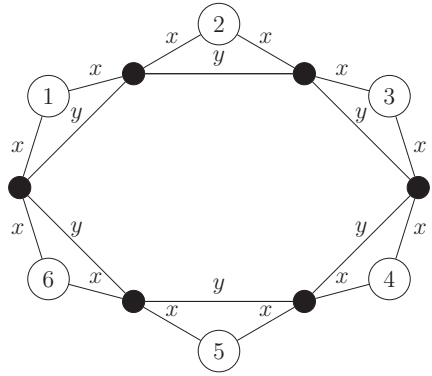


Figure 4.9. A matchgate for an even, symmetric, arity-6 signature.

a single internal vertex and n dangling edges. For EXACT-ONE-1 we can flip the 0's and 1's by extending each dangling edge to be a path of length 2. For weighted versions $[0, \lambda, 0, \ldots, 0]$ and $[0, \ldots, 0, \lambda, 0]$ we can assign the weight λ to all the edges incident to the single internal vertex.

These two cases correspond to some special cases in the list in Theorem 4.11 with $a = 0$ or $b = 0$ ($a = 0$ in item 2, $b = 0$ in item 3, and a or $b = 0$ in item 4.) Now consider a symmetric signature in Theorem 4.11 other than the two cases above. For such a signature, it is difficult to imagine a construction that is planar and also geometrically symmetric for all pairs of external nodes $1 \leq i < j \leq k$, if $k \geq 4$. In the following construction, the matchgates are not geometrically symmetric for all pairs of external nodes, but functionally they are, in terms of the signatures.

We present two closely related matchgate constructions, one for even symmetric signatures, and the other for odd. The constructions for both these cases work regardless if the signature has odd or even arity.

To construct a symmetric even matchgate G of arity k, we first take k triangles with vertices $\{a_i, b_i, c_i\}$ $(1 \leq i \leq k)$. The edges $\{a_i, b_i\}$ and $\{a_i, c_i\}$ have weight x, and $\{b_i, c_i\}$ has weight y. We link them in a cycle, identifying c_i with b_{i+1}, where the index is counted modulo k. The matchgate G has k external nodes $\{a_1, \ldots, a_k\}$, and a total of $2k$ nodes. In Figure 4.9 we have an example of a planar matchgate for an even, arity-6 signature. For a symmetric odd signature of arity k, we delete one external node in a matchgate for a symmetric even signature of arity $k + 1$. This is illustrated in Figure 4.10 for arity $k = 5$.

For an even matchgate of $2k$ nodes, we need to consider its values only at entries of even Hamming weight. Consider any $\alpha \in \{0, 1\}^k$ of even Hamming weight. $\alpha_i = 0$ iff a_i remains in G^α. If $\alpha = 1^k$, then G^α is a cycle of length k.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

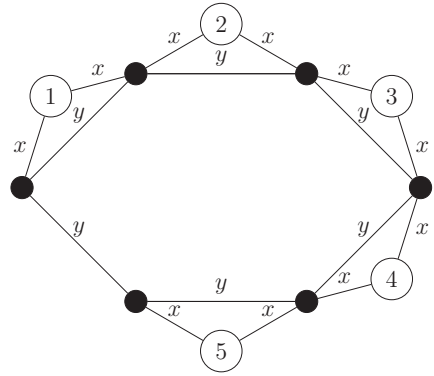


Figure 4.10. A matchgate for an odd, symmetric, arity-5 signature.

Since α also has even Hamming weight, k must be even, and there are exactly two perfect matchings of a cycle of even length, each having weight $y^{k/2}$.

Now assume $\alpha \neq 1^k$. Then α cyclically alternates between consecutive 0's (called a *0-run*) and consecutive 1's (called a *1-run*). Each a_i that remains in G^α must be matched to either b_i (we call it *left-match*) or $c_i = b_{i+1}$ (we call it *right-match*), both with weight x. Consider any 0-run. It is clear that either all a_i within this 0-run left-match or all right-match. Next consider a 1-run of m 1's; it is between two (not necessarily distinct) 0-runs, since $\alpha \neq 1^k$. If m is even, then the path of m edges all with weight y forces the two neighboring 0-runs to take either both left-match or both right-match. Moreover, both possibilities are realizable, and in each case the 1-run contributes a weight $y^{m/2}$. If m is odd, then the path of m edges forces the two neighboring 0-runs to take opposite types of left-match and right-match. Again both possibilities are realizable; in one case the 1-run contributes a weight $y^{(m-1)/2}$, and in another case it contributes a weight $y^{(m+1)/2}$. Furthermore, for two 1-runs 1^m and $1^{m'}$ both of odd length and are consecutive in the sense that the only 1-runs in between are of even length, they contribute a combined weight $y^{(m+m')/2}$. Since α has an even Hamming weight $|\alpha|$, there is an even number of 1-runs of odd length. Hence together the 1-runs contribute a weight $y^{|\alpha|/2}$. There are exactly two perfect matchings in G^α, each uniquely determined by the left-match or right-match choice of any particular a_i in G^α. It follows that the signature value is $\Gamma^\alpha = 2x^{k-|\alpha|}y^{|\alpha|/2}$. Clearly by choosing x and y suitably, we can realize an arbitrary even symmetric signature other than weighted Exact-One-1 and Exact-One-0.

The construction for odd symmetric signatures is to remove one external node in the matchgate for an even symmetric signature of arity one higher. If the even symmetric signature of arity $k+1$ has the form $[z_0, z_1, \ldots, z_{k+1}]$,

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

then the construction gives the signature $[z_1, \ldots, z_{k+1}]$ of arity k. The proof is complete.

4.3.4 Symmetric Signatures Transformable to Matchgates

In Section 4.2 we have seen a number of natural problems that can be solved by holographic reductions to matchgates. For an individual problem, specified by suitable local constraint functions expressed as generator and recognizer signatures, the task is to find suitable matchgates and a holographic transformation such that both the generator and recognizer signatures can be transformed to matchgate signatures. This is called the simultaneous realizability problem. This task for any individual problem is specified by families of algebraic equations. These families of equations are typically exponential in size. Searching for their solutions is what Valiant called "the enumeration" of "freak objects" in his Accidental Algorithms paper [Val06]. Dealing with such algebraic equations can be difficult.

While finding exotic solutions such as the signature for $\#_7$PL-RTW-MON-3CNF can be artistically satisfying, the situation with ever more complicated algebraic constraints on such signatures for any given problem can quickly overwhelm such an artistic approach as well as a computer search. Furthermore, failure to find such solutions to a particular algebraic system yields no proof that such solutions do not exist, and it generally does not give us any insight as to why. The theory of matchgates provides a more systematic understanding. This theory is quite complete for symmetric signatures. We will show that the simultaneous realizability problem can be solved in polynomial time. Using this theory we can see why the modulus 7 is *the* modulus that works for counting PL-RTW-MON-3CNF. Underlying this success is the fact that 7 is $2^3 - 1$, and for any odd prime p, the number 2 is a quadratic residue in $\mathbb{Z}_q$ for any prime factor q of the Mersenne number $2^p - 1$. Generalizing this, we will show that $\#_{2^k-1}$PL-RTW-MON-kCNF is in P for all $k \geq 3$ (the problem is trivial for $k \leq 2$). Furthermore, no suitable signatures exist for any modulus other than factors of $2^k - 1$ for counting PL-RTW-MON-kCNF.

We start with an equivalent set of normal forms from Theorem 4.11 that is more suitable for holographic transformations. If a and b are both nonzero, then all four forms in Theorem 4.11 can be expressed as a sum of two tensor products of the following form: There exist nonzero α and $\beta \in \mathbb{C}$ such that

$$f = [f_0, f_1, \ldots, f_n] = \begin{bmatrix} \alpha, & \beta \end{bmatrix}^{\otimes n} \pm \begin{bmatrix} \alpha, & -\beta \end{bmatrix}^{\otimes n}. \tag{4.23}$$

Clearly any signature of the form in (4.23) takes one of the four forms in Theorem 4.11. Conversely, for form 1 (arity $n = 2k$) and form 2 (arity $n = 2k + 1$)

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

in Theorem 4.11 we can take + for the ± sign in (4.23) and

$$\alpha = \frac{a^{k/n}}{2^{1/n}} \quad \text{and} \quad \beta = \alpha\sqrt{\frac{b}{a}}.$$

We can verify that all entries at odd Hamming weight are 0, and the entry at Hamming weight $2i$ is $2\alpha^{n-2i}\beta^{2i} = a^{k-i}b^i$, for $0 \le i \le k$. For form 3 (arity $n = 2k+1$) and form 4 (arity $n = 2k+2$) in Theorem 4.11 we can take − for the ± sign and

$$\alpha = \frac{a^{(k+\frac{1}{2})/n}}{2^{1/n}b^{1/(2n)}} \quad \text{and} \quad \beta = \alpha\sqrt{\frac{b}{a}}.$$

We can verify that all entries at even Hamming weight are 0, and the entry at Hamming weight $2i+1$ is $2\alpha^{n-2i-1}\beta^{2i+1} = a^{k-i}b^i$, for $0 \le i \le k$.

However, if a or b is 0, but not both 0, there are some additional signatures in Theorem 4.11 that cannot be expressed as (4.23). These cases are as follows:

$$f = [0, \lambda, 0, \ldots, 0] \quad \text{or its reversal} \quad f' = [0, \ldots, 0, \lambda, 0] \tag{4.24}$$

for some $\lambda \neq 0$. These can be expressed as

$$f = \lambda \sum_{k=1}^{n} \left\{ \begin{bmatrix} 1 & 0 \end{bmatrix}^{\otimes(k-1)} \otimes \begin{bmatrix} 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \end{bmatrix}^{\otimes(n-k)} \right\} \tag{4.25}$$

and

$$f' = \lambda \sum_{k=1}^{n} \left\{ \begin{bmatrix} 0 & 1 \end{bmatrix}^{\otimes(k-1)} \otimes \begin{bmatrix} 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \end{bmatrix}^{\otimes(n-k)} \right\}. \tag{4.26}$$

Of course the case $a = b = 0$ in Theorem 4.11 is the identically 0 signature and corresponds to taking $\alpha = \beta = 0$ in (4.23) and $\lambda = 0$ in (4.25) and (4.26).

Now we can give a closed form expression for symmetric signatures that are transformable to matchgate signatures. We state this for recognizer signatures.

Theorem 4.20. *A symmetric signature $f = [f_0, f_1, \ldots, f_n]$ is transformable to a matchgate signature as a recognizer, i.e., $f = \Gamma M^{\otimes n}$ for some $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in GL_2(\mathbb{C})$ and a matchgate signature Γ iff it takes one of the following forms:*

1. $\exists \lambda, \alpha, \beta \in \mathbb{C}$ and $\epsilon = \pm 1$, such that

$$f = \lambda \left[\left(\begin{bmatrix} \alpha & \beta \end{bmatrix} M \right)^{\otimes n} + \epsilon \left(\begin{bmatrix} \alpha & -\beta \end{bmatrix} M \right)^{\otimes n} \right].$$

Thus, for $0 \le k \le n$, the entry of f at weight k is

$$f_k = \lambda \left[(a\alpha + b\beta)^{n-k}(c\alpha + d\beta)^k + \epsilon(a\alpha - b\beta)^{n-k}(c\alpha - d\beta)^k \right].$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

2. $\exists \lambda \in \mathbb{C}$, *such that*

$$f = \lambda \sum_{k=1}^{n} \left\{ \begin{bmatrix} a, & c \end{bmatrix}^{\otimes(k-1)} \otimes \begin{bmatrix} b, & d \end{bmatrix} \otimes \begin{bmatrix} a, & c \end{bmatrix}^{\otimes(n-k)} \right\}.$$

Thus, for $0 \leq k \leq n$, *the entry of* f *at weight* k *is*

$$f_k = \lambda \left[(n-k) a^{n-k-1} b c^k + k a^{n-k} c^{k-1} d \right].$$

3. $\exists \lambda \in \mathbb{C}$, *such that*

$$f = \lambda \sum_{k=1}^{n} \left\{ \begin{bmatrix} b, & d \end{bmatrix}^{\otimes(k-1)} \otimes \begin{bmatrix} a, & c \end{bmatrix} \otimes \begin{bmatrix} b, & d \end{bmatrix}^{\otimes(n-k)} \right\}.$$

Thus, for $0 \leq k \leq n$, *the entry of* f *at weight* k *is*

$$f_k = \lambda \left[(n-k) b^{n-k-1} a d^k + k b^{n-k} d^{k-1} c \right].$$

(We take the convention that $x^0 = 1$ *and* $0x^{0-1} = 0$, *even if* $x = 0$.*)*

We have a corresponding statement for a symmetric signature transformable to a matchgate signature as a generator: $g = (M^{-1})^{\otimes n} \Gamma'$ for some $M \in GL_2(\mathbb{C})$ and a matchgate signature Γ'. These formulae can be obtained from those in Theorem 4.20 by substituting $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ for $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$.

From now on, a signature that is transformable to the signature of a matchgate is also called a matchgate signature (or realizable as a matchgate signature). This conforms to the modern concept of tensors, which are given coordinate-free, and not chained to a particular basis. However, to avoid ambiguity, for a signature that is realizable directly as the signature of a matchgate without a transformation, we will call it a *standard* (matchgate) signature.

By the relationship between second order linear recurrences and the expressions obtained here, we have

Theorem 4.21. *A symmetric signature* $[x_0, x_1, \ldots, x_n]$ *is transformable to a matchgate signature under some holographic transformation iff* $\exists (a, b, c) \neq 0$ *such that*

$$a x_k + b x_{k+1} + c x_{k+2} = 0$$

for $0 \leq k \leq n-2$.

The expression of a matchgate realizable signature as the solution to a second-order linear recurrence relation has a uniqueness that we state explicitly below.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Lemma 4.22. *Suppose a sequence* $(x_0, x_1, \ldots, x_n)$*, where* $n \geq 3$*, has the following form:* $x_i = \lambda\alpha^i + \mu\beta^i$*,* $(\lambda\mu \neq 0, \alpha \neq \beta)$*, then the representation is unique. That is, if* $x_i = \lambda'(\alpha')^i + \mu'(\beta')^i$*,* $(0 \leq i \leq n,\ n \geq 3)$*, then* $\lambda' = \lambda$*,* $\mu' = \mu, \alpha' = \alpha, \beta' = \beta$ *or* $\lambda' = \mu, \mu' = \lambda, \alpha' = \beta, \beta' = \alpha$*.*

Lemma 4.23. *Suppose a sequence* $(x_0, x_1, \ldots, x_n)$*, where* $n \geq 3$*, has the following form:* $x_i = \lambda i\alpha^{i-1} + \mu\alpha^i$*,* $(\lambda \neq 0)$*, then the representation is unique. That is, if* $x_i = \lambda' i(\alpha')^{i-1} + \mu'(\alpha')^i$*,* $(0 \leq i \leq n,\ n \geq 3)$*, then* $\lambda' = \lambda, \mu' = \mu, \alpha' = \alpha$*.*

Also, the two cases in Lemma 4.22 and 4.23 are mutually exclusive, depending on whether the eigenvalues of the linear recurrence are distinct or not.

The following observation is due to Valiant [Val08].

Proposition 4.24. *If a generator or recognizer signature is realizable by a matchgate under a holographic transformation* M*, then it is also realizable by a matchgate under* M'*, where* $M' = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} M$*, for any nonzero* $x, y \in \mathbb{C}$*, or* $M' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} M$*.*

Let G be a recognizer signature of arity n realizable under a holographic transformation M by a matchgate with the standard signature Γ, then $G = \Gamma M^{\otimes n}$. If Γ is any standard signature, then so are $\Gamma \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}^{\otimes n}$ and $\Gamma \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\otimes n}$. For example, a matchgate with signature $\Gamma \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{\otimes n}$ is obtained from the given matchgate for Γ by appending an edge of weight 1 to each external node, which effectively flips the truth values 0 and 1. Proposition 4.24 can also be proved easily using MGI. The proof for generators is similar.

Proposition 4.24 implies that there is an equivalence relation $\sim$ among the holographic transformations, where one can multiply each row by a nonzero constant, or exchange the two rows of the transformation matrix M. Under this equivalence relation, $\mathrm{GL}_2(\mathbb{C})/\sim$ is a two-dimensional manifold. We call this the *basis manifold* $\mathcal{B}$. From now on we identify a basis transformation with its equivalence class containing it. When it is permissible, we use the dehomogenized coordinates $\begin{bmatrix} 1 & \xi \\ 1 & \eta \end{bmatrix}$ to represent a point (i.e., a basis class) in $\mathcal{B}$.

Theorem 4.20 gives a complete characterization of all the symmetric realizable matchgate signatures. These tell us exactly what signatures can be realized over *some* bases. However, to construct a holographic algorithm, one needs to realize some generators and recognizers simultaneously. In terms of $\mathcal{B}$, a given

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

generator (recognizer) defines a (possibly empty) subvariety that consists of all the bases over which it is realizable. The simultaneous realizability is equivalent to a nonempty intersection of these subvarieties. Thus we have to go beyond Theorem 4.20. For every signature that is realizable according to Theorem 4.20, we need to determine the subvariety where it is realizable.

Definition 4.25. Let f be a symmetric recognizer or generator signature of arity n. Then $B_{rec}(f)$ (respectively $B_{gen}(f)$) is the set of all bases in $\mathcal{B}$ for which the symmetric signature f for a recognizer (respectively a generator) is realizable. Formally,

$$B_{rec}(f) = \{M \in \mathcal{B} \mid f = \Gamma M^{\otimes n} \text{ for some matchgate signature } \Gamma\},$$

$$B_{gen}(f) = \{M \in \mathcal{B} \mid f = (M^{-1})^{\otimes n}\Gamma' \text{ for some matchgate signature } \Gamma'\}.$$

Since the identically 0 signature is realizable in every basis, we will assume the signature is not identically 0 in the following discussion.

Lemmas 4.26 to 4.30 give a complete and mutually exclusive list of symmetric matchgate realizable signatures for recognizers that are not identically 0. The corresponding set of results for symmetric matchgate realizable generators can be obtained by substituting $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ for $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$.

Recall that a symmetric signature $[x_0, x_1, \ldots, x_n]$ is nondegenerate iff $\operatorname{rank}\begin{bmatrix} x_0 & \cdots & x_{n-1} \\ x_1 & \cdots & x_n \end{bmatrix} = 2$. The signature is identically 0 iff $\operatorname{rank}\begin{bmatrix} x_0 & \cdots & x_{n-1} \\ x_1 & \cdots & x_n \end{bmatrix} = 0$. It has rank 1 iff it can be expressed as $[a^n, a^{n-1}b, \ldots, b^n]$, for $a, b \in \mathbb{C}$ and not both 0. Lemma 4.26 deals with degenerate signatures.

Lemma 4.26. *For $a, b \in \mathbb{C}$ and not both 0,*

$$B_{rec}([a^n, a^{n-1}b, \ldots, b^n]) = \left\{ \begin{bmatrix} a & b \\ x & y \end{bmatrix} \in \mathcal{B} \,\middle|\, x, y \in \mathbb{C} \right\}.$$

Remark: Every nonzero unary signature is of this form.

In the following we assume the signature is nondegenerate. For the case of arity $n = 2$, we have

Lemma 4.27.

$$B_{rec}([x, y, z]) = \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathcal{B} \,\middle|\, \begin{array}{c} xd^2 - 2ybd + zb^2 = 0, xc^2 - 2yac + za^2 = 0 \\ \text{or} \quad xcd - y(ad + bc) + zab = 0 \end{array} \right\}.$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

We can prove this lemma by noting that, for arity 2, the only requirement to be a standard signature of a matchgate is the parity constraint. The MGI is satisfied under the parity condition in this case.

In the following we assume the signature has arity $n \geq 3$, and nondegenerate. In this case, we note that the constants a, b, c in Theorem 4.21 are unique up to a scalar factor. In fact, if there are two linearly independent triples (a, b, c), then the following matrix

$$\begin{bmatrix} x_0 & x_1 & \dots & x_{n-2} \\ x_1 & x_2 & \dots & x_{n-1} \\ x_2 & x_3 & \dots & x_n \end{bmatrix}$$

has rank ≤ 1. The first row and the last row are not both 0, otherwise the signature is identically 0 (by $n \geq 3$). It follows that the matrix

$$\begin{bmatrix} x_0 & x_1 & \dots & x_{n-1} \\ x_1 & x_2 & \dots & x_n \end{bmatrix}$$

also has rank 1; hence the signature is degenerate.

The next lemma corresponds to nondegenerate signatures in Theorem 4.21, where $ac = 0$ and $b = 0$. For $b = c = 0$ (and $a \neq 0$) we have $[0, \dots, 0, \lambda, \mu]$, where $\lambda \neq 0$ by nondegeneracy. Its reversal $[\mu, \lambda, 0, \dots, 0]$ corresponds to $a = b = 0$ (and $c \neq 0$).

Lemma 4.28. *Let $\lambda \neq 0$. Then,*

$$B_{rec}([0, \dots, 0, \lambda, \mu]) = \left\{ \begin{bmatrix} 0 & 1 \\ n\lambda & \mu \end{bmatrix} \right\}.$$

Similarly for its reversal,

$$B_{rec}([\mu, \lambda, 0, \dots, 0]) = \left\{ \begin{bmatrix} 1 & 0 \\ \mu & n\lambda \end{bmatrix} \right\}.$$

The reversal signature $[\mu, \lambda, 0, \dots, 0]$ can also be viewed as a special case in Lemma 4.31 *if* we were to allow $\alpha = 0$ there, where for $\alpha = 0$ and $i = 0$, we take the convention that $i\alpha^{i-1} = 0$, and also $\alpha^i = 1$. However, for the listing to be mutually exclusive we disallow $\alpha = 0$ in Lemma 4.31.

Next we consider the case of nondegenerate signatures in Theorem 4.21 where $ac = 0$ and $b \neq 0$.

Lemma 4.29. *For $\lambda\mu \neq 0$,*

$$B_{rec}([\lambda, \lambda\alpha, \dots, \lambda\alpha^{n-1}, \lambda\alpha^n + \mu]) = \left\{ \begin{bmatrix} 1 & \alpha + \omega \\ 1 & \alpha - \omega \end{bmatrix} \middle| \, \omega^n = \pm\frac{\mu}{\lambda} \right\}.$$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Similarly for its reversal,

$$B_{rec}([\lambda\alpha^n + \mu, \lambda\alpha^{n-1}, \ldots, \lambda\alpha, \lambda]) = \left\{ \begin{bmatrix} \alpha + \omega & 1 \\ \alpha - \omega & 1 \end{bmatrix} \middle| \, \omega^n = \pm\frac{\mu}{\lambda} \right\}.$$

Here $\alpha = 0$ is Gen-Eq, and corresponds to the case $a = c = 0$ and $b \neq 0$. For $\alpha \neq 0$, the reversal signature $[\lambda\alpha^n + \mu, \ldots, \lambda\alpha^2, \lambda\alpha, \lambda]$ can also be written as $\lambda'[1, \alpha', \ldots, \alpha'^n] + [\mu, 0, \ldots, 0]$, where $\lambda' = \lambda\alpha^n$ and $\alpha' = 1/\alpha$, and then can be viewed as a special case in Lemma 4.30 *if* we were to allow $\beta = 0$ there; although for mutual exclusion we disallow $\beta = 0$ in Lemma 4.30.

Now we consider $ac \neq 0$ in Theorem 4.21. We use the fact that the triple (a, b, c) in the statement of Theorem 4.21 is unique up to a scalar factor. We have a unique characteristic equation $cX^2 + bX + a = 0$, which has two roots α and β. In particular the forms 1, 2 and 3 from Theorem 4.20 are mutually exclusive. Suppose $b^2 \neq 4ac$, i.e., $\alpha \neq \beta$, we have the following lemma.

Lemma 4.30. *For $\lambda\mu \neq 0$, $\alpha\beta \neq 0$, and $\alpha \neq \beta$,*

$$B_{rec}([\lambda\alpha^i + \mu\beta^i] | i = 0, 1, \ldots, n]) = \left\{ \begin{bmatrix} 1 + \omega & \alpha + \beta\omega \\ 1 - \omega & \alpha - \beta\omega \end{bmatrix} \middle| \, \omega^n = \pm\frac{\mu}{\lambda} \right\}.$$

If $b^2 = 4ac \neq 0$, i.e., the characteristic roots coincide $\alpha = \beta \neq 0$, we have the following lemma.

Lemma 4.31. *For $\lambda \neq 0$, and $\alpha \neq 0$,*

$$B_{rec}([\lambda i\alpha^{i-1} + \mu\alpha^i] | i = 0, 1, \ldots, n]) = \left\{ \begin{bmatrix} 1 & \alpha \\ \mu & n\lambda + \mu\alpha \end{bmatrix} \right\}.$$

Definition 4.32. Simultaneous Realizability Problem (SRP):

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

Output: A common basis of holographic transformation to matchgate signatures if any exists; "NO" if they are not simultaneously realizable as matchgate signatures by holographic transformations

SRP Algorithm: For every signature $[x_0, x_1, \ldots x_n]$, check if it satisfies Theorem 4.20.

If not, output "NO" and halt.

Otherwise find $B_{gen}([x_0, x_1, \ldots x_n])$ or $B_{rec}([x_0, x_1, \ldots x_n])$ according to one of the lemmas.

Check if these subvarieties have a nonempty intersection.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Theorem 4.33. *The SRP algorithm solves SRP in polynomial time.*

Proof. Checking whether every input signature satisfies Theorem 4.20 can obviously be done in polynomial time. Finding the right form and then the right lemma for a signature that satisfies Theorem 4.21 can also be done in polynomial time, as they are mutually exclusive.

Every subvariety of bases from Lemma 4.26 to 4.31 for recognizers, and similarly for generators, is of one of three kinds: a finite set of points (of linear size), a line, or a quadratic curve. More precisely, expressing things in terms of the manifold $\mathcal{B}$ shows the following. For Lemma 4.26 we get a line with $\xi =$ constant (in the dehomogenized coordinates notation defining $\mathcal{B}$). For Lemma 4.27 we get a union of two sets. The first is finite, where both the dehomogenized coordinates ξ and η satisfy a quadratic polynomial (and by projective closure). The second set is defined by an equation of the form $A\xi\eta + B(\xi + \eta) + C = 0$ (and by projective closure), where A, B, C are known constants. The other cases are all similar. For example, for Lemma 4.29, we get at most n points from the equation $\omega^n =$ constant. To sum up, the SRP algorithm is a polynomial time algorithm for SRP. □

4.3.5 #$_7$PL-RTW-MON-3CNF Redux

In Section 4.2 we had encountered the problem #$_7$PL-RTW-MON-3CNF. Valiant [Val06] also introduced another problem #$_7$Pl-3/2BIP-VC, which counts the number of vertex covers for a planar $(3, 2)$-regular bipartite graph, modulo 7. They were solved in polynomial time by holographic algorithms based on matchgates. He called these *accidental algorithms*. In this subsection, we apply the theory developed in Section 4.3 to find such algorithms almost *mechanically*. This theory provides more insight and understanding as to what can or cannot be accomplished. With this machinery we are able to generalize to the problems Pl-RTW-MON-kCNF (the same problem for kCNF formulae for a general k) and Pl-k/2BIP-VC (the same problem for planar $(k, 2)$-regular bipartite graphs). We show that there is a unique modulus $2^k - 1$ for which we can design such a holographic algorithm based on matchgates, which counts the number of solutions modulo $2^k - 1$. In the case of $k = 3$, this shows why 7 is special.

#$_{2^k-1}$PL-RTW-MON-kCNF

INPUT: A planar kCNF Boolean formula where each variable appears positively and in exactly two clauses (planar, read-twice, monotone, kCNF)

OUTPUT: The number of satisfying assignments modulo $2^k - 1$

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

When $k = 3$ this is $\#_7$PL-RTW-MON-3CNF from Section 4.2. As noted earlier, the counting problem #PL-RTW-MON-3CNF is #P-complete already for $k = 3$.

To solve the problem by a holographic algorithm, we wish to replace each variable by a generator with the signature $[1, 0, 1]$, and each clause by a recognizer with the signature $[0, 1, 1, \ldots, 1]$ (with k 1's). The symmetric signature $[1, 0, 1]$ is the binary EQUALITY function $=_2$ and corresponds to a consistent truth assignment on two edges leading to clauses, and $[0, 1, 1, \ldots, 1]$ (with k 1's) is the Boolean OR function of arity k corresponding to a clause. If we connect the generators and recognizers in a natural way, by Theorems 1.5 and 4.7, this would solve #PL-RTW-MON-kCNF in polynomial time, *if* the signatures are simultaneously realizable by matchgates under a holographic transformation.

Then the question boils down to whether there is a basis in $\mathcal{B}$ where $[1, 0, 1]$ for a generator and $[0, 1, 1, \ldots, 1]$ (with k 1's) for a recognizer can be simultaneously realized. For this, we use our machinery.

From Lemma 4.29, taking $\lambda = 1$, $\mu = -1$ and $\alpha = 1$ for $[\lambda\alpha^k + \mu, \lambda\alpha^{k-1}, \ldots, \lambda\alpha, \lambda]$, we have

$$B_{rec}([0, 1, 1, \ldots, 1]) = \left\{ \begin{bmatrix} 1+\omega & 1 \\ 1-\omega & 1 \end{bmatrix} \middle| \, \omega^k = \pm 1 \right\}.$$

We look for some $\omega^k = \pm 1$, such that $\begin{bmatrix} 1+\omega & 1 \\ 1-\omega & 1 \end{bmatrix} \in B_{gen}([1, 0, 1])$, which is obtained from Lemma 4.27 by substituting $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ for $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$. Explicitly,

$$B_{gen}([x, y, z]) = \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathcal{B} \;\middle|\; \begin{array}{c} xa^2 + 2yac + zc^2 = 0, xb^2 + 2ybd + zd^2 = 0 \\ \text{or} \quad xab + y(ad + bc) + zcd = 0 \end{array} \right\}. \tag{4.27}$$

Thus, we want $(1 + \omega)^2 + 1 = (1 - \omega)^2 + 1 = 0$ or $(1 + \omega)(1 - \omega) + 1 = 0$. The first case is impossible, and in the second case we require $\omega^2 = 2$. Together with the condition $\omega^k = \pm 1$, we have $2^k - 1 = 0$. From this we can already see that for every prime $p|2^k - 1$, $\#_p$PL-RTW-MON-kCNF is computable in polynomial time. In particular, this is true for every Mersenne prime $2^q - 1$. (Note that $\omega^2 = 2$ means that 2 is a quadratic residue.) If we develop the theory over a finite field $\mathbb{Z}_p$, we can obtain corresponding versions of Lemmas 4.27 and 4.29, and conclude that in order to have these signatures be simultaneously realizable over $\mathbb{Z}_p$, we must have $p|2^k - 1$.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

More generally we have:

Theorem 4.34. *There is a polynomial time algorithm for $\#_{2^k-1}$PL-RTW-MON-kCNF. Furthermore, any modulus m for which the appropriate signatures exist must be a divisor of $2^k - 1$.*

Proof. Our discussion above already shows that the modulus $2^k - 1$ is the best we can do. (Formally speaking we should present a generalization such as Theorem 1.5 over a ring such as $\mathbb{Z}_{2^k-1}$, which we will omit here.) We now give the polynomial algorithms in two cases:

Case 1: k is even.
Over the complex numbers $\mathbb{C}$, from (4.27), the generator form of Lemma 4.27, and Lemma 4.29, we can see that a generator for $[1, 0, 1]$ and a recognizer for $[1 + \epsilon 2^{k/2}, 1, 1, \ldots, 1]$ (where there are k 1's, and $\epsilon = \pm 1$) are simultaneously realizable in the basis $\begin{bmatrix} 1+\sqrt{2} & 1 \\ 1-\sqrt{2} & 1 \end{bmatrix}$.

Setting $\epsilon = 1$ and replacing each variable by a generator and each clause by a recognizer with the corresponding signatures, we obtain a matchgrid Ω. If we replace the generators and recognizers by their corresponding matchgates, we get a weighted planar graph G. Then Theorem 1.5 gives

$$\text{Holant}_\Omega = \text{PerfMatch}(G). \tag{4.28}$$

We will denote this value by X.

From the left-hand side of (4.28) we know that X is an integer because every entry in the signatures of generators $[1, 0, 1]$ and recognizers $[1 + 2^{k/2}, 1, 1, \ldots, 1]$ is an integer. Furthermore we have

$$X \equiv \#\text{PL-RTW-MON-}k\text{CNF} \pmod{1 + 2^{k/2}}.$$

From the right-hand side of (4.28) we know that X can be computed in polynomial time using the FKT algorithm for perfect matchings of a planar graph. The planar graph has weights from the subfield $\mathbb{Q}(\sqrt{2}) \subset \mathbb{C}$, which poses no problem to the Pfaffian evaluation of FKT in polynomial time in bit complexity.

Therefore $\#_{2^{k/2}+1}$PL-RTW-MON-kCNF can be computed in polynomial time. Similarly, setting $\epsilon = -1$, we can compute $\#_{2^{k/2}-1}$PL-RTW-MON-kCNF in polynomial time.

Since $\gcd(2^{k/2} + 1, 2^{k/2} - 1) = 1$ and $2^k - 1 = (2^{k/2} + 1)(2^{k/2} - 1)$, we can apply Chinese remaindering to get a polynomial time algorithm for $\#_{2^k-1}$PL-RTW-MON-kCNF.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

Case 2: k is odd.
Consider the ring $\mathbb{Z}_{2^k-1}$. (Formally we can develop the theory over such a ring, and consider invertible elements and matrices for the basis manifold, which we will omit.) Let $r = 2^{(k+1)/2} \in \mathbb{Z}_{2^k-1}$. Then r satisfies $r^2 = 2$ in $\mathbb{Z}_{2^k-1}$. We observe that $r^k - 1 = (2^k)^{(k+1)/2} - 1 = 0$ in $\mathbb{Z}_{2^k-1}$.

Therefore over this ring $\mathbb{Z}_{2^k-1}$ and with the basis $\begin{bmatrix} 1+r & 1 \\ 1-r & 1 \end{bmatrix}$, the generator $[1, 0, 1]$ and the recognizer $[0, 1, 1, \ldots, 1]$ (with k 1's) are simultaneously realizable by matchgates according to (4.27) and Lemma 4.29. As a result, we have a polynomial time algorithm for $\#_{2^k-1}$PL-RTW-MON-kCNF. □

Now we consider another problem.

$\#_{2^k-1}$PL-k/2BIP-VC

INPUT: A planar regular bipartite graph $G = (U, V, E)$, where every $u \in U$ has degree k and every $v \in V$ has degree 2 (planar $(k, 2)$-regular bipartite graph)

OUTPUT: The number of vertex covers mod $2^k - 1$

Consider an arbitrary subset $S \subseteq V$ of vertices from the right. Every vertex $u \in U$ on the left *either* has all its k adjacent vertices in S, in which case there are exactly two choices to extend S at u to a vertex cover, *or* has some of its k adjacent vertices not in S, in which case there is exactly one choice to extend S at u to a vertex cover. Thus, following the general recipe for holographic algorithms, we want a generator with signature $[1, 0, 1]$ and a recognizer with signature $[1, 1, \ldots, 1, 2]$ (with k 1's), to be simultaneously realized over some basis.

From Lemma 4.29, taking $\lambda = \mu = \alpha = 1$ for $[\lambda, \lambda\alpha, \ldots, \lambda\alpha^{n-1}, \lambda\alpha^n + \mu]$, we have

$$B_{rec}([1, 1, \ldots, 1, 2]) = \left\{ \begin{bmatrix} 1 & 1+\omega \\ 1 & 1-\omega \end{bmatrix} \middle| \, \omega^k = \pm 1 \right\}.$$

Then the same derivation for $\#_{2^k-1}$PL-RTW-MON-kCNF gives a polynomial time algorithm for $\#_{2^k-1}$PL-k/2BIP-VC.

Theorem 4.35. *There is a polynomial time algorithm for $\#_{2^k-1}$PL-k/2BIP-VC. Furthermore, any modulus m for which the appropriate signatures exist must be a divisor of $2^k - 1$.*

There is a 1-1 correspondence between vertex covers and independent sets, by taking complement. Thus we also have a polynomial time algorithm for $\#_{2^k-1}$PL-k/2BIP-IS, which is to count the number of independent sets mod

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press

$2^k - 1$ for planar $(k, 2)$-regular bipartite graph. More directly, we can proceed as before: For any planar $(k, 2)$-regular bipartite graph $G = (U, V, E)$, for any $S \subseteq V$, to extend it to an independent set, every $u \in U$ has either two choices if all k neighbors of u are not in S, or one choice (not to be included) otherwise. It follows that we should simultaneously realize a generator with signature $[1, 0, 1]$ and a recognizer with signature $[2, 1, \ldots, 1, 1]$ (with k 1's), and the rest are the same.

Our general machinery not only can find the required signatures when they exist, but also can prove certain desired signatures cannot be simultaneously realized. As an example, one may wish to extend the previous two problems to allow more than Read-twice as in #Pl-R_ℓ-Mon-kCNF, where $\ell > 2$. This calls for a simultaneous realizability of the Equality function of arity ℓ, $(=_\ell) = [1, 0, \ldots, 0, 1]$ (where there are $(\ell - 1)$ 0's), and the Boolean Or function on k inputs, $[0, 1, 1, \ldots, 1]$ (where there are k 1's). This can be shown to result in an empty intersection on $\mathcal{B}$.

In this book we focus on the exact complexity of counting problems. There is an active research area to study the approximate complexity of counting problems, and to the extent possible to reach classification theorems [JS93, GJP03, LLY12, SST12, MWW09, DFJ02, Wei06, Sly10, GGv+11, DGJ10, DGJR12, SS12, LLZ14, LL15, CGG+16, GGY16, GGJ16, GG16, GL16]. It appears that for approximate counting, there are more than just two levels of complexity, those that are solvable by a polynomial time approximation algorithm and those that are NP-hard to approximate. In particular, the problem to approximately count the number of independent sets for bipartite graphs (#BIS) appears to be a representative problem for a distinct class of intermediate complexity. This is in contrast to $\#_{2^k-1}$PL-k/2BIP-IS, which is solvable in polynomial time exactly.

https://doi.org/10.1017/9781107477063.005 Published online by Cambridge University Press