Theoretical Computer Science 411 (2010) 739–750

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

On blockwise symmetric signatures for matchgates ☆

Jin-Yi Cai [a], Pinyan Lu [b,*]

[a] Computer Sciences Department, University of Wisconsin, Madison, WI 53706, USA

[b] Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, PR China

ARTICLE INFO

Keywords:
Matchgates
Matchgate identities
Blockwise symmetric signatures
Holographic algorithm

ABSTRACT

We give a classification of blockwise symmetric signatures in the theory of matchgate computations. The main proof technique uses matchgate identities, also known as useful Grassmann–Plücker identities.

1. Introduction

The most fundamental question in computational complexity theory is that of what differentiates between polynomial time and exponential time problems. On the one hand, we have many completeness results and conjectured separations of complexity classes. On the other hand we have precious few unconditional separations. In fact, the most spectacular advances in the field in the past 20 years have been as regards *upper bounds*, i.e., surprising ways to do computation efficiently. Valiant's theory of matchgate and holographic algorithms [11,13] is one such methodology.

The basic idea in matchgate computations is to encode 0–1 bits of a computation in terms of *perfect matchings*. The complexity of graph matching is very interesting in its own right, having inspired the notion of P in the first place [5]. While a brute force attempt at graph matching seems to take exponential time, it turns out that the decision problem is in P. More relevant, counting perfect matchings is known to be in P for planar graphs, by the FKT method [7,8,10]. (Counting all, not necessarily perfect, matchings for planar graphs is #P-complete, as is counting perfect matchings for general graphs [6].) So one can say that graph matching is right at the border of polynomial time and (probably) exponential time. Valiant's theory of matchgate computations uses the FKT method as the starting point.

To give a flavor of this methodology, let's consider the problem $\#_7$Pl-Rtw-Mon-3CNF. Given a planar read-twice monotone 3CNF formula, this problem asks for the number of satisfying assignments modulo 7. Without the modulo 7, it is #P-complete even for such restricted formulae [14]. Furthermore, counting mod 2, denoted as $\#_2$Pl-Rtw-Mon-3CNF, is $\oplus$P-complete (and hence NP-hard). But, using matchgates, Valiant showed that $\#_7$Pl-Rtw-Mon-3CNF $\in$ P [14].

A matchgate is a weighted planar graph with some external nodes. For example, let π be a path of length 3: all three edges have weight 1, and the two end vertices are external nodes. If we remove exactly one of the two external nodes we have three vertices left and therefore there is no perfect matching. If we remove either both or none of the two external nodes we get a unique perfect matching with weight 1 (the product of weights of matching edges). We can record this information as $(1, 0, 0, 1)^{\mathrm{T}}$, indexed by 00, 01, 10, 11; this is called the (standard) *signature* of π. One can use this gadget to replace a Boolean variable x in a planar formula φ, and 00, 01, 10, 11 will naturally correspond to truth values of x to be fanned out to the two clauses of φ in which x appears (recall that it is read twice). Then the signature $(1, 0, 0, 1)^{\mathrm{T}}$ indicates consistency of this truth assignment on x.

☆ Supported by NSF CCR-0511679 and by the National Natural Science Foundation of China Grant 60553001 and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.

* Corresponding author.
E-mail addresses: jyc@cs.wisc.edu (J.-Y. Cai), lpy@mails.tsinghua.edu.cn (P. Lu).

0304-3975/$ – see front matter
doi:10.1016/j.tcs.2009.10.012

Now for each clause in φ we wish to find a matchgate with three external nodes having signature $(0, 1, 1, 1, 1, 1, 1, 1)^{\mathrm{T}}$, indexed by $000, 001, \ldots, 111$. This signature corresponds to a Boolean OR. One can replace each clause by such a gadget, and connect its three external nodes to the gadgets of its three variables. Then the total number of perfect matchings of the resulting planar graph is exactly the number of satisfying assignments of φ. This can be computed by the FKT method, which would imply $\mathrm{P}^{\#\mathrm{P}} = \mathrm{P}$.

It turns out that a matchgate with the *standard* signature $(0, 1, 1, 1, 1, 1, 1, 1)^{\mathrm{T}}$ does not exist. However, using a basis transformation a (non-standard) signature in the form $(0, 1, 1, 1, 1, 1, 1, 1)^{\mathrm{T}}$ *is realizable* over the field $\mathbf{Z}_7$ (but not $\mathbf{Q}$). This gives the result that $\#_7$Pl-Rtw-Mon-3CNF $\in$ P. (In this paper we will not be concerned with non-standard signatures.)

The signatures $(1, 0, 0, 1)^{\mathrm{T}}$ and $(0, 1, 1, 1, 1, 1, 1, 1)^{\mathrm{T}}$ are called symmetric signatures, since their values only depend on the Hamming weight of the index. Symmetric signatures have natural combinatorial meanings (such as two equal bits or the Boolean OR). Therefore the study of symmetric signatures is of foremost importance for understanding the power of these exotic algorithms. To this end, we have achieved a complete classification of bitwise symmetric signatures [3].

In Valiant's surprising algorithm for $\#_7$Pl-Rtw-Mon-3CNF he took another innovative step in the use of matchgates. In his algorithm, the matchgates have external nodes grouped in blocks of two each (called "2-rail" in [14]). This naturally raises the question of classification of blockwise symmetric signatures. This paper is concerned with this classification.

The classification theorem of blockwise symmetric signatures is more difficult compared to that of bitwise symmetric signatures. The main reason for this is that matchgate signatures are characterized by a set of parity requirements (due to the consideration of perfect matchings) and an exponential sized set of algebraic constraints called *Matchgate Identities* (MGI), a.k.a. the *useful Grassmann–Plücker identities* [1,2,9,12]. These MGI are non-linear, and are more subtle as compared to parity requirements. They come about due to an equivalence between the perfect matching polynomial PerfMatch and the *Pfaffian* [2,1]. For bitwise symmetric signatures, these MGI degenerate into something more readily treatable. This paper is the first time one is able to mount a successful and systematic attack on these MGI. We find proofs on MGI technically challenging, with almost every step a struggle (at least to the authors). The proof for the first main theorem for the decomposition theory for blockwise symmetric signatures still has a discernible central theme. In one direction the proof is done by a direct construction. In the more difficult direction the proof is an induction which utilizes matchgate identities at two different levels, an outer sum and an inner sum. The theorem has a technical condition that the initial entry $\Gamma^{00\cdots0} \neq 0$. We dispense with this technical condition in the theorem for signatures with block size 2. This proof is even more technically "relentless", in the words of a referee. It is basically a long sequence of lemmas, using the matchgate identities in all kinds of combinations. Unfortunately, we don't know of a more elegant and more conceptual proof in this part. Fortunately, the theorem statement itself is still elegant and succinct. Whether one can remove the technical condition $\Gamma^{00\cdots0} \neq 0$ for signatures with block size greater than 2 is an interesting open problem. Perhaps to obtain a proof of that one will need a better conceptual understanding of blockwise symmetric signatures.

At a higher level, the new theory of matchgate and holographic algorithms represents a *novel* algorithm design methodology given by Valiant, with its ultimate reach unknown. Will the new theory lead to a collapse of complexity classes? We don't know. Only a systematic study will (one hopes) tell. To get a classification theorem for blockwise symmetric signatures seems a useful step.

2. Background

Let $G = (V, E, W)$ be a weighted undirected planar graph. A *matchgate* Γ is a tuple (G, X) where $X \subseteq V$ is a set of external nodes, ordered counterclockwise on the external face. Γ is called an odd (resp. even) matchgate if it has an odd (resp. even) number of nodes.

Each matchgate Γ with n external nodes is assigned a (standard) *signature* $(\Gamma^{\alpha})_{\alpha\in\{0,1\}^n}$ with 2^n entries,

$$\Gamma^{i_1 i_2 \ldots i_n} = \mathrm{PerfMatch}(G - Z) = \sum_{M} \prod_{(i,j)\in M} w_{ij},$$

where the sum is over all perfect matchings M of $G - Z$, and $Z \subseteq X$ is the subset of external nodes having the characteristic sequence $\chi_Z = i_1 i_2 \ldots i_n$.

An entry Γ^{α} is called an even (resp. odd) entry if the Hamming weight $\mathrm{wt}(\alpha)$ is even (resp. odd). It was proved in [1,2] that standard signatures are characterized by the following two sets of conditions. (1) The parity requirements: either all even entries are 0 or all odd entries are 0. This is due to perfect matchings. (2) A set of Matchgate Identities (MGI) defined as follows: A pattern α is an n-bit string, i.e., $\alpha \in \{0, 1\}^n$. A position vector $P = \{p_i\}$, $i \in [l]$, is a subsequence of $\{1, 2, \ldots, n\}$, i.e., $p_i \in [n]$ and $p_1 < p_2 < \cdots < p_l$. We also use p to denote the pattern, whose $(p_1, p_2, \ldots, p_l)$th bits are 1 while the others are 0. Let $e_i \in \{0, 1\}^n$ be the pattern with 1 in the ith bit and 0 elsewhere. Let $\alpha + \beta$ be the bitwise XOR of α and β. Then for any pattern $\alpha \in \{0, 1\}^n$ and any position vector $P = \{p_i\}$, $i \in [l]$,

$$\sum_{i=1}^{l} (-1)^i \Gamma^{\alpha+e_{p_i}} \Gamma^{\alpha+p+e_{p_i}} = 0. \tag{1}$$

The use of MGI will be central in this paper. These MGI come from the Grassmann–Plücker identities valid for Pfaffians. In fact initially Valiant introduced *two* theories of matchgate computation: The first is the matchcircuit theory with general

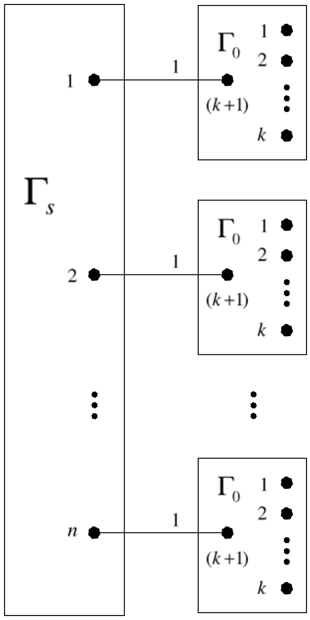

Fig. 1. Blockwise symmetric signature.

(non-planar) matchgates [11]. These matchgates have *characters* which are defined in terms of Pfaffians. The second is the theory of matchgrid/holographic algorithms [13]. These use planar matchgates with signatures defined by PerfMatch. In [2] it was proved that MGI characterize (general) matchgate characters. In [1] an equivalence theorem for characters and signatures was established, and thus MGI also characterize planar matchgate signatures. The dual forms of the theory have been useful in both ways: sometimes it is easier to reason and construct planar gadgets; at other times the algebraic Pfaffian setup seems essential. A case in point is that of symmetric signatures.

A signature Γ is (bitwise) symmetric if Γ^α only depends on $\mathrm{wt}(\alpha)$. A bitwise symmetric signature can be denoted as $[z_0, z_1, \ldots, z_n]$, where $\Gamma^\alpha = z_{\mathrm{wt}(\alpha)}$. It was proved in [2] that for even matchgates, a signature $[z_0, z_1, \ldots, z_n]$ is realizable iff for all odd i, $z_i = 0$, and there exist constants r_1, r_2 and λ such that $z_{2i} = \lambda \cdot (r_1)^{\lfloor n/2\rfloor - i} \cdot (r_2)^i$, for $0 \le i \le \lfloor \frac{n}{2} \rfloor$. Similar results hold for odd matchgates. These are proved via MGI and Pfaffians. It is interesting to note that the only construction for a planar matchgate realizing this signature is through a non-planar matchgate Γ and its character theory. There is no known direct construction.

A tensor (Γ^α) on index $\alpha = \alpha_1 \ldots \alpha_n$, where each $\alpha_i \in \{0, 1\}^k$, is *blockwise symmetric* if Γ^α only depends on the number of k-bit patterns of α_i, i.e., $\Gamma^{\cdots\alpha_i\cdots\alpha_j\cdots} = \Gamma^{\cdots\alpha_j\cdots\alpha_i\cdots}$, for all $1 \le i < j \le n$.

For an even (resp. odd) matchgate Γ with arity n, the *condensed signature* (g^α) of Γ is a tensor of arity $n-1$, and $g^\alpha = \Gamma^{\alpha b}$ (resp. $g^\alpha = \Gamma^{\alpha\bar{b}}$), where $\alpha \in \{0, 1\}^{n-1}$ and $b = p(\alpha)$ is the parity of $\mathrm{wt}(\alpha)$.

3. Decomposition theory for blockwise symmetric signatures

Theorem 1. *Let (Γ^α) be a blockwise symmetric tensor with block size k and arity nk. Assume that $n \ge 4$ and $\Gamma^{00\cdots0} \ne 0$. Then Γ is realizable by a matchgate iff there exist a matchgate Γ_0 with arity $k+1$ and condensed signature $(g^\alpha)_{\alpha\in\{0,1\}^k}$, and a symmetric matchgate Γ_s such that*

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \Gamma_s^{p(\alpha_1)p(\alpha_2)\cdots p(\alpha_n)} g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}. \quad (2)$$

Proof. We prove "⇐" by a direct construction. In Fig. 1, we extend every external node of Γ_s by a copy of the matchgate with condensed signature g, and view the remaining k external nodes of each copy as external. This gives us a new matchgate with nk external nodes, whose signature is given by (2). Therefore every signature which has form (2) is realizable.

Now we prove "⇒": Since $\Gamma^{00\cdots0} \ne 0$, by adding an extra isolated edge with weight $1/\Gamma^{00\cdots0}$ we can assume $\Gamma^{00\cdots0} = 1$. First we assume $r_1 = \Gamma^{e_1e_100\cdots0} \ne 0$ (where for convenience we consider $e_1 \in \{0, 1\}^k$), and prove the theorem under this assumption. We take Γ_s to be an even symmetric matchgate with signature $z_{2i} = (r_1)^{-i}$. By [2] this Γ_s exists. Since the given (Γ^α) is realizable, it can be realized by a matchgate Γ with nk external nodes. Viewing its first $k+1$ external nodes still as external nodes and the other nodes as internal, we have a matchgate with $k+1$ external nodes. This is our Γ_0. By definition its condensed signature is

$$g^\alpha = \begin{cases} \Gamma^{\alpha00\cdots0} & \text{when } \mathrm{wt}(\alpha) \text{ is even,} \\ \Gamma^{\alpha e_10\cdots0} & \text{when } \mathrm{wt}(\alpha) \text{ is odd.} \end{cases}$$

Note that $g^0 = 1$ and $g^{e_1} = r_1$. We prove (2) by induction on $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) \ge 0$ and $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n)$ is even.

If $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 0$, we have the only case that $\alpha_1\alpha_2\cdots\alpha_n = 00\cdots0$. In this case (2) is obvious.

If $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 2$, we have two cases depending on whether the two 1s are in the same block or not. If they are in the same block, we can assume it is in the first block since Γ is block symmetric; then $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \Gamma^{\alpha_1 00\cdots0} = g^{\alpha_1}$ and (2) is satisfied. If they are not in the same block, by symmetry, we may assume that $\alpha_1\alpha_2\cdots\alpha_n$ has the form $e_ie_j00\cdots0$. When 0 appears in the sup index of Γ, the sup index of g, a pattern or positions used by a MGI for Γ, it means a block of all zero. Using the pattern $0e_je_1e_100\cdots0$ and positions $e_ie_je_1e_100\cdots0$, from (1) we have the following matchgate identity (applying blockwise symmetry):

$$\Gamma^{e_ie_je_1e_10\cdots0}\Gamma^{00\cdots0} - \Gamma^{e_1e_10\cdots0}\Gamma^{e_ie_j0\cdots0} + \Gamma^{e_je_10\cdots0}\Gamma^{e_ie_10\cdots0} - \Gamma^{e_je_10\cdots0}\Gamma^{e_ie_10\cdots0} = 0.$$

The last two terms cancel out; we get

$$\Gamma^{e_ie_je_1e_100\cdots0} = \Gamma^{e_ie_j00\cdots0}\Gamma^{e_1e_100\cdots0}. \quad (3)$$

Next, using the pattern $0e_1e_je_100\cdots0$ and positions $e_ie_1e_je_100\cdots0$, we have the following matchgate identity:

$$\Gamma^{e_ie_je_1e_10\cdots0}\Gamma^{00\cdots0} - \Gamma^{e_je_10\cdots0}\Gamma^{e_ie_10\cdots0} + \Gamma^{e_1e_10\cdots0}\Gamma^{e_ie_j0\cdots0} - \Gamma^{e_je_10\cdots0}\Gamma^{e_ie_10\cdots0} = 0.$$

Combining with (3), we have $\Gamma^{e_ie_j00\cdots0}\Gamma^{e_1e_100\cdots0} = \Gamma^{e_ie_100\cdots0}\Gamma^{e_je_100\cdots0}$. Since $\Gamma^{e_1e_100\cdots0} = r_1 \neq 0$, we have $\Gamma^{e_ie_j00\cdots0} = \Gamma^{e_ie_100\cdots0}\Gamma^{e_je_100\cdots0}/r_1 = (r_1)^{-1}g^{e_i}g^{e_j}$. So (2) is satisfied.

Inductively we assume that (2) has been proved for all $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) \leq 2(i-1)$, for some $i \geq 2$. Now $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 2i > 0$. By symmetry, we can assume that $\alpha_1 \neq 00\cdots0$. Let t be the position of the first 1 in α_1. Using the pattern $\alpha_1\alpha_2\cdots\alpha_n + e_t$ and positions $\alpha_1\alpha_2\cdots\alpha_n$ (we denote this as $P = \{p_j\}$ where $j = 1, 2, \ldots, 2i$), we have the following matchgate identity:

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \sum_{j=2}^{2i}(-1)^j\Gamma^{\alpha_1\alpha_2\cdots\alpha_n+e_t+e_{p_j}}\Gamma^{e_t+e_{p_j}}. \quad (4)$$

Since every Γ^β in the RHS has $\mathrm{wt}(\beta) \leq 2i-2$, we can apply (2) to them.

Now we do the summation of the RHS in (4) block by block; the sum of the rth block is denoted as S_r. Let $w_r = \mathrm{wt}(\alpha_r)$. Let $2q$ be the number of odd w_r, i.e., the number of blocks among $\alpha_1, \alpha_2, \ldots, \alpha_n$ with odd weight. Note that this number is even.

For the first block, if $w_1 = 1$, then $S_1 = 0$, being an empty sum. Assume $w_1 > 1$. In the notation below we consider $e_t, e_{p_j} \in \{0, 1\}^k$ for convenience.

$$S_1 = \sum_{j=2}^{w_1}(-1)^j\Gamma^{(\alpha_1+e_t+e_{p_j})\alpha_2\cdots\alpha_n}\Gamma^{(e_t+e_{p_j})00\cdots0} \quad (5)$$

$$= r_1^{-q}g^{\alpha_2}\cdots g^{\alpha_n}\sum_{j=2}^{w_1}(-1)^jg^{\alpha_1+e_t+e_{p_j}}g^{e_t+e_{p_j}}. \quad (6)$$

Note that the exponent q in r_1^{-q} comes from the fact that the number of blocks with odd weight among $\alpha_1+e_t+e_{p_j}, \alpha_2, \ldots, \alpha_n$ is $2q$.

If w_1 is odd, using the pattern $(\alpha_1 + e_t)1$ and positions α_11, we have the following matchgate identity for Γ_0:

$$-g^{\alpha_1} + \sum_{j=2}^{w_1}(-1)^jg^{\alpha_1+e_t+e_{p_j}}g^{e_t+e_{p_j}} + g^{\alpha_1+e_t}g^{e_t} = 0.$$

Substituting this in (6), we have

$$S_1 = r_1^{-q}g^{\alpha_2}\cdots g^{\alpha_n}(g^{\alpha_1} - g^{\alpha_1+e_t}g^{e_t}). \quad (7)$$

We note that this is also valid for $w_1 = 1$.

If w_1 is even, using the pattern $(\alpha_1 + e_t)0$ and positions α_10, we have the following matchgate identity for Γ_0:

$$-g^{\alpha_1} + \sum_{j=2}^{w_1}(-1)^jg^{\alpha_1+e_t+e_{p_j}}g^{e_t+e_{p_j}} = 0.$$

Substituting this in (6), we have

$$S_1 = r_1^{-q}g^{\alpha_1}g^{\alpha_2}\cdots g^{\alpha_n}. \quad (8)$$

If all S_r are empty blockwise sums for $r > 1$ (i.e., $w_r = 0$ for all $r > 1$), then w_1 must be even, and we are done. Now suppose there are non-empty blockwise sums S_r, for $r > 1$. For the rth block, let v_r be the number of 1s in the first $r-1$ blocks, and p^r_j ($j \in [w_r]$) be the position of the jth 1 in α_r. Then

$$S_r = (-1)^{v_r} \sum_{j=1}^{w_r} (-1)^j \Gamma^{(\alpha_1+e_t)\alpha_2\cdots(\alpha_r+e_{p^r_j})\cdots\alpha_n} \Gamma^{(e_t)00\cdots(e_{p^r_j})\cdots 0} \quad (9)$$

$$= (-1)^{v_r} r_1^{-q'} g^{e_t} g^{\alpha_1+e_t} g^{\alpha_2} \cdots \widehat{g^{\alpha_r}} \cdots g^{\alpha_n} \sum_{j=1}^{w_r} (-1)^j g^{\alpha_r+e_{p^r_j}} g^{e_{p^r_j}}, \quad (10)$$

where $\widehat{g^{\alpha_r}}$ denotes a missing factor, and $2q'$ is the total number of odd blocks in $\alpha_1+e_t, \alpha_2, \ldots, \alpha_r+e_{p^r_j}, \ldots, \alpha_n$ from the first factor Γ and in $(e_t)00\cdots(e_{p^r_j})\cdots 0$ from the second factor Γ. If w_r is even, using the pattern $\alpha_r 1$ and positions $\alpha_r 0$, we have the following matchgate identity for Γ_0:

$$\sum_{j=1}^{w_r} (-1)^j g^{\alpha_r+e_{p^r_j}} g^{e_{p^r_j}} = 0.$$

Substituting this in (10), we have $S_r = 0$.

Therefore, among block sums S_r, for $r > 1$, we need only consider blocks with odd w_r. Assuming that w_r is odd now, we have that $q' = q$ if w_1 is odd, and $q' = q+1$ if w_1 is even. Using the pattern $\alpha_r 0$ and positions $\alpha_r 1$, we have the following MGI for Γ_0:

$$\sum_{j=1}^{w_r} (-1)^j g^{\alpha_r+e_{p^r_j}} g^{e_{p^r_j}} + g^{\alpha_r} = 0.$$

Substituting this in (10), we have $S_r = -(-1)^{v_r} r_1^{-q'} g^{e_t} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_r} \cdots g^{\alpha_n}$.

To summarize, after the first block sum S_1, every even block will be zero, and every odd block will alternatingly contribute a $\pm r_1^{-q'} g^{e_t} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$. If S_1 is an even block sum, then this alternating sum has an even number of such terms, and they all cancel out. This leaves us with the desired result $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = S_1 = r_1^{-q} g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}$ from (8). If the first block is odd, then $q' = q$, and there are an odd number of alternating S_r for $r > 1$ and w_r odd, starting with the sign $-(-1)^{v_2} = +1$. These will cancel out pairwise except one $r_1^{-q} g^{e_t} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$ left, which cancels the $-r_1^{-q} g^{e_t} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$ in S_1 from (7). Finally in either cases, we have $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = r_1^{-q} g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}$. This is precisely (2).

Now we consider the case $\Gamma^{e_1e_100\cdots0} = 0$. If there exists any $i \in [k]$ such that $\Gamma^{e_ie_i00\cdots0} \neq 0$, the above proof can go through similarly. Therefore we assume for all $i \in [k]$, $\Gamma^{e_ie_i00\cdots0} = 0$.

Consider any $1 \le i, j, s, t \le k$ (not necessarily distinct). Using the pattern $0e_je_se_t00\cdots0$ and positions $e_ie_je_se_t00\cdots0$ we get (applying block symmetry)

$$\Gamma^{e_ie_je_se_t0\cdots0}\Gamma^{00\cdots0} - \Gamma^{e_se_t0\cdots0}\Gamma^{e_ie_j0\cdots0} + \Gamma^{e_ie_s0\cdots0}\Gamma^{e_je_t0\cdots0} - \Gamma^{e_je_s0\cdots0}\Gamma^{e_ie_t0\cdots0} = 0.$$

Also using the pattern $0e_se_je_t00\cdots0$ and positions $e_ie_se_je_t00\cdots0$ we get

$$\Gamma^{e_ie_se_je_t0\cdots0}\Gamma^{00\cdots0} - \Gamma^{e_je_t0\cdots0}\Gamma^{e_ie_s0\cdots0} + \Gamma^{e_se_t0\cdots0}\Gamma^{e_ie_j0\cdots0} - \Gamma^{e_se_j0\cdots0}\Gamma^{e_ie_t0\cdots0} = 0.$$

Adding the two, we get $\Gamma^{e_ie_se_je_t00\cdots0} = \Gamma^{e_se_j00\cdots0}\Gamma^{e_ie_t00\cdots0}$.

From this we have

$$(\Gamma^{e_ie_j00\cdots0})^2 = \Gamma^{e_ie_je_ie_j00\cdots0} = \Gamma^{e_ie_je_je_i00\cdots0} = \Gamma^{e_ie_i00\cdots0}\Gamma^{e_je_j00\cdots0} = 0.$$

Therefore for all $i, j \in [k]$, we have $\Gamma^{e_ie_j00\cdots0} = 0$. Now we define $g^\alpha = \Gamma^{\alpha 00\cdots0}$ when $\mathrm{wt}(\alpha)$ is even, and $g^\alpha = 0$ when $\mathrm{wt}(\alpha)$ is odd, and inductively prove (2) similarly to before. (g^α) is the condensed signature of a realizable matchgate Γ_0 of arity $k+1$ obtained from Γ as follows: View its first k external nodes (in the first block) still as external and the rest as internal, add a new isolated edge with weight 1, and one end as the $(k+1)$st external node and the other end as an internal node. We will still arrive at (4). Now all block sums $S_r = 0$, for $r > 1$, since it involves a $\Gamma^{e_t+e_{p_j}}$, and e_t appears in the first block.

Consider the first block sum S_1. Suppose $q > 0$, i.e., there are some odd w_r. Then there are at least two odd blocks. Only the first block has a changed index in the sum, so some odd block among $\alpha_2, \ldots, \alpha_n$ remains in $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n+e_t+e_{p_j}}$. Thus, by induction it is 0, since the corresponding $g^{\alpha_i} = 0$. Now suppose $q = 0$, i.e., all blocks are even. By induction we get

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = g^{\alpha_2} \cdots g^{\alpha_n} \sum_{j=2}^{w_1} (-1)^j g^{\alpha_1+e_t+e_{p_j}} g^{e_t+e_{p_j}}.$$

Using the pattern $(\alpha_1+e_t)0$ and positions $\alpha_1 0$ on Γ_0, we have MGI,

$$-g^{\alpha_1} + \sum_{j=2}^{w_1} (-1)^j g^{\alpha_1+e_t+e_{p_j}} g^{e_t+e_{p_j}} = 0,$$

This gives $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}$ proving (2). □

In Theorem 1, we assumed $\Gamma^{00\cdots0} \neq 0$. So it must be an even matchgate. For odd matchgates, we have a similar theorem under the assumption $\Gamma^{e_1 00\cdots0} \neq 0$. This proof is slightly more complicated but along similar lines. Due to space limitations we present it in Appendix. These theorems give an elegant decomposition structure of blockwise symmetric signatures. There is an underlying bitwise symmetric signature Γ_s, whose structure is very clear to us. Therefore, the realizability condition is within each block.

4. Characterization of the blockwise symmetric signature with block size 2

In Theorem 1, we have two assumptions: $n \geq 4$ and $\Gamma^{00\ldots0} \neq 0$. $n \geq 4$ is necessary for some boundary reason. The assumption $\Gamma^{00\ldots0} \neq 0$ is more technical but we are not able to bypass it in general. However, in this section we show that this assumption is not necessary for block size $k = 2$.

Theorem 2. *If Γ is a blockwise symmetric signature for some matchgate whose block size is 2 and with arity 2n where $n \geq 4$, then there exist four numbers $g^{00}, g^{01}, g^{10}, g^{11}$ and a realizable bitwise symmetric signature Γ_s such that*

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \Gamma_s^{p(\alpha_1)p(\alpha_2)\cdots p(\alpha_n)} g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}. \quad (11)$$

We only prove it for even matchgates here; the proof is similar for odd matchgates. If $\Gamma^{00,00,\ldots,00} \neq 0$ or $\Gamma^{11,11,\ldots,11} \neq 0$ (we use "," to separate blocks), we are done by Theorem 1. Note that flipping all bits preserves block symmetry. Now we assume that Γ is an even matchgate, $n \geq 4$, and $\Gamma^{00,00,\ldots,00} = \Gamma^{11,11,\ldots,11} = 0$. This assumption is made for all the following claims.

Claim 1. *For any $\alpha \in \{00, 01, 10, 11\}^{n-4}$, we have*

$$\Gamma^{01,01,01,01,\alpha}\Gamma^{00,00,00,00,\alpha} = (\Gamma^{01,01,00,00,\alpha})^2.$$
$$\Gamma^{10,10,10,10,\alpha}\Gamma^{00,00,00,00,\alpha} = (\Gamma^{10,10,00,00,\alpha})^2.$$
$$\Gamma^{01,01,10,10,\alpha}\Gamma^{00,00,00,00,\alpha} = \Gamma^{01,01,00,00,\alpha}G^{10,10,00,00,\alpha} = (\Gamma^{01,10,00,00,\alpha})^2.$$

Proof. All three equations follow from MGI. The α part is not involved in the MGI. This means that the pattern for these bits is exactly α and the position vector bits for these bit locations are all 0. For convenience, we only list below the pattern and positions for the other bits, which are really involved in the MGI. We also use this simplified notation in the following claims.

This claim is quite direct from MGI. We only list the pattern and positions used, and omit the actual MGI. The first equation uses the pattern 00, 01, 01, 01 and positions 01, 01, 01, 01. The second equation uses the pattern 00, 10, 10, 10 and positions 10, 10, 10, 10. The last equation is from two MGI: one uses the pattern 00, 01, 10, 10 and positions 01, 01, 10, 10; the other uses the pattern 00, 10, 01, 10 and positions 01, 10, 01, 10. □

Claim 2.

$$\Gamma^{00,00,\{00,01,10\}^{n-2}} = 0.$$
$$\Gamma^{11,11,\{11,01,10\}^{n-2}} = 0.$$

Proof. We only prove $\Gamma^{00,00,\{00,01,10\}^{n-2}} = 0$; the second equation can be obtained for the first by flipping all the bits. For $\alpha \in \{00, 01, 10\}^{n-2}$, we prove it by induction on $\mathrm{wt}(\alpha) \geq 0$ and $\mathrm{wt}(\alpha)$ is even. The case $\mathrm{wt}(\alpha) = 0$ is by assumption. We use Claim 1 to go from weight i to weight $i + 2$. □

Claim 3. *For any $\alpha \in \{00, 01, 10, 11\}^{n-3}$,*

$$\Gamma^{00,00,00,\alpha} = 0.$$
$$\Gamma^{11,11,11,\alpha} = 0.$$

Proof. We also only need to prove $\Gamma^{00,00,00,\alpha} = 0$. For $\alpha \in \{00, 01, 10, 11\}^{n-3}$, we prove it by induction on the number of non-"00" blocks in α. (We denote this number by $N_0(\alpha)$.)

If every block in α is 00, then it is by assumption. Inductively we assume it has been proved for all $N_0(\alpha) < i$. Now $N_0(\alpha) = i$. If α does not have any block "11", it has been proved by Claim 2. Otherwise, we can assume $\alpha = 11, \alpha'$ by block symmetry. Since $N_0(00, \alpha') = i - 1$, we have $\Gamma^{00,00,00,00,\alpha'} = 0$.

Using the pattern 00, 00, 01, 11 and positions 00, 00, 11, 11, we have MGI (note that we omit the α' part, and also we omit the symbol Γ in the MGI):

$$\begin{aligned} 0 &= (00, 00, 11, 11)(00, 00, 00, 00) - (00, 00, 00, 11)(00, 00, 11, 00) \\ &\quad + (00, 00, 01, 01)(00, 00, 10, 10) - (00, 00, 01, 10)(00, 00, 10, 01). \end{aligned}$$

The first term is 0, and by Claim 1, the last two terms cancel out. It follows that $\Gamma^{00,00,00,11,\alpha'}\Gamma^{00,00,11,00,\alpha'} = 0$, which is exactly $\Gamma^{00,00,00,\alpha} = 0$. □

From Claims 1 and 3, we have:

Claim 4. *For any* $\alpha \in \{00, 01, 10, 11\}^{n-4}$,

$$\Gamma^{01,10,00,00,\alpha} = \Gamma^{01,01,00,00,\alpha} = \Gamma^{10,10,00,00,\alpha} = 0.$$

Claim 5. *For any* $\alpha \in \{00, 01, 10, 11\}^{n-2}$, *the following are all valid:*

$$\Gamma^{00,00,\alpha} = 0, \qquad \Gamma^{11,11,\alpha} = 0, \qquad \Gamma^{00,11,\alpha} = 0.$$

Proof. For any $\alpha' \in \{00, 01, 10, 11\}^{n-4}$, using the pattern $10, 10, 10, 11, \alpha'$ and positions 10, 10, 01, 01, we have MGI:

$$\begin{aligned} 0 &= (00,10,10,11)(10,00,11,10) - (10,00,10,11)(00,10,11,10) \\ &\quad + (10,10,11,11)(00,00,10,10) - (10,10,10,10)(00,00,11,11). \end{aligned}$$

Since the first two terms cancel and from Claim 4 the third term is 0, we have

$$(10,10,10,10)(00,00,11,11) = 0. \tag{12}$$

Using the pattern $10, 10, 10, 11, \alpha'$ and positions 10, 01, 10, 01, we have MGI (here in all displayed entries of signature Γ in MGI we omit Γ and α' and display only the first eight bits):

$$\begin{aligned} 0 &= (00,10,10,11)(10,11,00,10) - (10,11,10,11)(00,10,00,10) \\ &\quad + (10,10,00,11)(00,11,10,10) - (10,10,10,10)(00,11,00,11). \end{aligned}$$

From Claim 4 we know that the second term is 0 and from (12) we know that the last term is 0, and since the first and the third terms are the same, we have

$$(00,10,10,11) = 0. \tag{13}$$

Similarly, we have

$$(00,01,01,11) = 0. \tag{14}$$

Using the pattern $10, 10, 01, 11, \alpha'$ and positions 10, 10, 10, 10, we have MGI:

$$\begin{aligned} 0 &= (00,10,01,11)(10,00,11,01) - (10,00,01,11)(00,10,11,01) \\ &\quad + (10,10,11,11)(00,00,01,01) - (10,10,01,01)(00,00,11,11). \end{aligned}$$

Since the first two terms cancel and the third term is 0 by Claim 4, we have

$$(10,10,01,01)(00,00,11,11) = 0. \tag{15}$$

Using the pattern $10, 01, 10, 11, \alpha'$ and positions 10, 10, 10, 10, we have MGI:

$$\begin{aligned} 0 &= (00,01,10,11)(10,11,00,01) - (10,11,10,11)(00,01,00,01) \\ &\quad + (10,01,00,11)(00,11,10,01) - (10,01,10,01)(00,11,00,11). \end{aligned}$$

From Claim 4 we know that the second term is 0 and from (15) we know that the last term is 0; since the first and the third terms are the same, we have

$$(10,01,00,11) = 0. \tag{16}$$

Using the pattern $00, 01, 00, 11, \alpha'$ and positions 11, 11, 00, 00, we have MGI:

$$\begin{aligned} 0 &= (10,01,00,11)(01,10,00,11) - (01,01,00,11)(10,10,00,11) \\ &\quad + (00,11,00,11)(11,00,00,11) - (00,00,00,11)(11,11,00,11). \end{aligned}$$

From Claim 3 we know that the last term is 0 and from (16) and (13) we know that the first two terms are 0. So we have

$$(11,00,00,11) = 0. \tag{17}$$

Now finally we are ready to prove Claim 5. We first prove $G^{00,00,\alpha} = 0$.
If α has any block 00, from Claim 3, we have $G^{00,00,\alpha} = 0$.
If α has any block of weight 1, then there must be at least two blocks of weight 1. So from Claim 4, we have $G^{00,00,\alpha} = 0$.
Otherwise every block of α is 11. Then from (17), we know $G^{00,00,\alpha} = 0$.
$G^{11,11,\alpha} = 0$ can be proved similarly.
Now we prove $G^{00,11,\alpha} = 0$. If α contains any block of 00 or 11, it has been proved. Otherwise, every block of α is 01 or 10. Then from (13), (14) and (16) we have $G^{00,11,\alpha} = 0$. □

Claim 5 says that every non-zero entry Γ^{α} can have at most one even block. This is an important step in the proof. The proof is by repeated applications of MGI (*death by a thousand cuts*, an ancient Chinese disgrace; unfortunately we cannot find a *coup de grâce*).

Claim 6. *For any* $\alpha \in \{00, 01, 10, 11\}^{n-2}$, *we have*

$$\Gamma^{01,01,\alpha}\Gamma^{10,10,\alpha} = (\Gamma^{01,10,\alpha})^2.$$

Proof. Using the pattern 00, 01 and positions 11, 11 (omitting α), we have MGI:

$$0 = (10, 01)(01, 10) - (01, 01)(10, 10) + (00, 11)(11, 00) - (00, 00)(11, 11).$$

From Claim 5, we know the last two terms are both 0. So we have

$$\Gamma^{01,01,\alpha}\Gamma^{10,10,\alpha} = (\Gamma^{01,10,\alpha})^2. \quad \square$$

Claim 7. *For* $n \geq 4$, $k = 2$, *if* n *is even and* $\Gamma^{00,00,\ldots,00} = \Gamma^{11,11,\ldots,11} = 0$, *Theorem 2 holds.*

Proof. Suppose $\Gamma^{\alpha_1,\alpha_2,\ldots,\alpha_n} \neq 0$; we show that each $\alpha_i \in \{01, 10\}$. Since n is even and we have an even matchgate, the number of odd blocks must be even, so if it has any even block it has at least two even blocks. Then by Claim 5 it is 0.

If $\Gamma^{01,01,\ldots,01} \neq 0$, w.l.o.g., we assume $\Gamma^{01,01,\ldots,01} = 1$. Let Γ_s be the matchgate having symmetric signature $[0, 0, \ldots, 0, 1]$ (in the notation for bitwise symmetric signatures); let $g^{01} = 1$ and $g^{10} = \Gamma^{10,01,01,\ldots,01}/\Gamma^{01,01,\ldots,01} = \Gamma^{10,01,01,\ldots,01}$. From Claim 6, we can verify that (11) is satisfied. This is seen as follows: Claim 6 allows one to "exchange" one block of 10 for one block of 01, incurring a factor of g^{10}. This works as long as $g^{10} \neq 0$. If $g^{10} = 0$, we can instead use Claim 6 to show that $\Gamma^{01,10,\alpha} = 0$, for all $\alpha \in \{01, 10\}^{n-2}$. Moreover we want to show that $\Gamma^{10,10,\ldots,10} = 0$ as well. For this purpose, we use MGI with the pattern 00, 10, 10, ..., 10 and all positions, and get

$$0 = (10, 10, 10, \ldots, 10)(01, 01, 01, \ldots, 01) - (01, 10, 10, \ldots, 10)(10, 01, 01, \ldots, 01) + \cdots.$$

The remaining terms (omitted) all have a 00 block in the first factor, and so they are all 0. The second term is also 0 as $g^{10} = 0$. Yet $(01, 01, 01, \ldots, 01) = 1$, so $(10, 10, 10, \ldots, 10) = 0$. This proves the claim when $\Gamma^{01,01,\ldots,01} \neq 0$.

If $\Gamma^{01,01,\ldots,01} = 0$, again from the "exchange" argument by Claim 6, the only possible non-zero entry of Γ is $\Gamma^{10,10,\ldots,10}$. Let $g^{00} = g^{11} = g^{01} = 0$ and $g^{10} = \sqrt[n]{\Gamma^{10,10,\ldots,10}}$. Then (11) is satisfied. (This may require us to go to an algebraic extension field.) $\square$

Claim 8. *For* $n \geq 4$, $k = 2$, n *is odd and* $\Gamma^{00,00,\ldots,00} = \Gamma^{11,11,\ldots,11} = 0$, *Theorem 2 holds.*

Proof. Since n is odd and Γ is an even matchgate, from Claim 5, we know that if $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} \neq 0$, then there is exactly one $\alpha_i \in \{00, 11\}$ and all other $\alpha_j \in \{01, 10\}$. By block symmetry, we assume $\alpha_1 \in \{00, 11\}$ and $\alpha_i \in \{01, 10\}$ (where $i = 2, 3, \ldots, n$).

If $\Gamma^{00,01,01,\ldots,01} \neq 0$, w.l.o.g., we assume $\Gamma^{00,01,01,\ldots,01} = 1$. Let $g^{00} = g^{01} = 1$. Using the pattern 10, 01, 01, ..., 01 and the first four bits as positions, we have

$$(00, 01)(11, 10) - (11, 01)(00, 10) + (10, 11)(01, 00) - (10, 00)(01, 11) = 0.$$

By block symmetry, the first and the last two terms are equal. So we have

$$\Gamma^{00,01,01,\ldots,01}\Gamma^{11,10,01,\ldots,01} - \Gamma^{11,01,01,\ldots,01}\Gamma^{00,10,01,\ldots,01} = 0. \tag{18}$$

Since $\Gamma^{00,01,01,\ldots,01} = 1$, letting $g^{11} = \Gamma^{11,01,01,\ldots,01}$ and $g^{10} = \Gamma^{00,10,01,\ldots,01}$, we have $\Gamma^{11,10,01,\ldots,01} = g^{11}g^{10}$. And we let Γ_s be the matchgate with symmetric signature $[0, 0, \ldots, 1, 0]$. The proof is similar to that for Claim 7. Degenerate cases happen when $g^{10} = 0$, or $g^{11} = 0$, or both. In particular, when $g^{10} = 0$, we need to prove $\Gamma^{00,10,10\ldots10} = 0$, which goes beyond Claim 6. This is shown by the MGI using the pattern 00, 00, 10, ..., 10 and positions 00, 11, 11, ..., 11 (all the bits except the first two). We also need to prove $\Gamma^{11,10,10,\ldots,10} = 0$ when $g^{10} = 0$ or $g^{11} = 0$ or both. This can be shown by the MGI using the pattern 10, 01, 01, ..., 01 and all positions.

If $\Gamma^{11,01,01,\ldots,01} \neq 0$, we have a similar proof.

Finally assume $\Gamma^{00,01,01,\ldots,01} = \Gamma^{11,01,01,\ldots,01} = 0$. From Claim 6 and the "exchange" argument, the only two possible non-zero entries of Γ are $\Gamma^{00,10,10,\ldots,10}$ and $\Gamma^{11,10,10,\ldots,10}$. If they are both 0, then Γ is trivial. Otherwise w.l.o.g. we assume $\Gamma^{00,10,10,\ldots,10} = 1$. Let $g^{01} = 0$, $g^{00} = g^{10} = 1$ and $g^{11} = \Gamma^{11,10,10,\ldots,10}$. And let Γ_s be the matchgate with symmetric signature $[0, 0, \ldots, 1, 0]$, we can verify that (11) is satisfied. $\square$

Combining with Claims 7 and 8, we have a complete proof for Theorem 2.

This paper presents an elegant decomposition theorem on the structure of blockwise symmetric signatures for matchgates. The main tool is matchgate identities. However the statement of Theorem 2 for $k > 2$ without any non-zero conditions is open. It would also be interesting to simplify the proofs.

Acknowledgments

We sincerely thank the referee and editors for their valuable comments. It was correctly pointed out by the referee and editors that the proofs are difficult and "relentlessly technical", especially in the proof for signatures with block size 2. We tried to give some explanations, but we have not been very successful in that. This could be due to our lack of understanding at a higher level or an inherent technical difficulty dealing with matchgate identities. A better and more conceptual proof would be very desirable and lead to a better understanding of realizable signatures.

Appendix. Decomposition theory for odd matchgates

Theorem 3. *Let (Γ^{α}) be a blockwise symmetric tensor with block size k and arity nk. Assume $n \geq 4$ and $\Gamma^{e_1 0\cdots 0} \neq 0$. Then Γ is realizable by a matchgate iff there exist a matchgate Γ_0 with arity $k+1$ and condensed signature $(g^{\alpha})_{\alpha\in\{0,1\}^k}$, and a symmetric matchgate Γ_s such that*

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \Gamma_s^{p(\alpha_1)p(\alpha_2)\cdots p(\alpha_n)} g^{\alpha_1} g^{\alpha_2}\cdots g^{\alpha_n}. \tag{19}$$

Proof. "$\Leftarrow$" can be proved in the same way as in Theorem 1.

Now we prove "$\Rightarrow$": Since $\Gamma^{100\cdots 0} \neq 0$, w.l.o.g., we can assume $\Gamma^{100\cdots 0} = 1$.

Let $r_1 = \Gamma^{e_1e_1e_100\cdots 0} \neq 0$. We take Γ_s to be an odd symmetric matchgate with signature $z_{2i+1} = (r_1)^i$. By [2] this Γ_s exists. Since the given (Γ^{α}) is realizable, it can be realized by a matchgate Γ with nk external nodes. View its first $k+1$ external nodes still as external nodes and other nodes as internal, we have a matchgate with $k+1$ external nodes. This is our Γ_0. By definition its condensed signature is

$$g^{\alpha} = \begin{cases} \Gamma^{\alpha 00\cdots 0} & \text{when } \mathrm{wt}(\alpha) \text{ is odd,} \\ \Gamma^{\alpha e_1 0\cdots 0} & \text{when } \mathrm{wt}(\alpha) \text{ is even.} \end{cases}$$

Note that in this definition $g^{\alpha} = 1$ for both $\alpha = 0^k$ and $\alpha = e_1 \in \{0,1\}^k$.

We prove (19) by induction on $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) \geq 0$ and $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n)$ is odd.

The base case $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 1$ is obvious. However before we deal with the case $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 3$, we first establish some identities.

Using the pattern and positions both as $e_ie_je_1e_100\cdots 0$ (for arbitrary $i, j \in [k]$), we have MGI:

$$\Gamma^{e_je_1e_10\cdots 0}\Gamma^{e_i0\cdots 0} - \Gamma^{e_ie_1e_10\cdots 0}\Gamma^{e_j0\cdots 0} + \Gamma^{e_ie_je_10\cdots 0}\Gamma^{e_10\cdots 0} - \Gamma^{e_ie_je_10\cdots 0}\Gamma^{e_10\cdots 0} = 0.$$

The last two terms cancel out, and we get

$$\Gamma^{e_je_1e_100\cdots 0}\Gamma^{e_i00\cdots 0} = \Gamma^{e_ie_1e_100\cdots 0}\Gamma^{e_j00\cdots 0}. \tag{20}$$

Next, using the pattern and position both as $e_ie_1e_je_100\cdots 0$, we have the following matchgate identity:

$$\Gamma^{e_je_1e_10\cdots 0}\Gamma^{e_i0\cdots 0} - \Gamma^{e_ie_1e_j0\cdots 0}\Gamma^{e_10\cdots 0} + \Gamma^{e_ie_1e_10\cdots 0}\Gamma^{e_j0\cdots 0} - \Gamma^{e_ie_1e_j0\cdots 0}\Gamma^{e_10\cdots 0} = 0.$$

Combining with (20), we have

$$\Gamma^{e_ie_je_100\cdots 0}\Gamma^{e_100\cdots 0} = \Gamma^{e_1e_1e_j00\cdots 0}\Gamma^{e_i00\cdots 0} = \Gamma^{e_1e_1e_i00\cdots 0}\Gamma^{e_j00\cdots 0}. \tag{21}$$

Let $j = 1$ in the above equation and note that $\Gamma^{e_100\cdots 0} = 1$ and $\Gamma^{e_1e_1e_1\cdots 0} = r_1$; we have

$$\Gamma^{e_ie_1e_100\cdots 0} = \Gamma^{e_1e_1e_100\cdots 0}\Gamma^{e_i00\cdots 0} = r_1 g^{e_i}.$$

Substituting this in (21), we have

$$\Gamma^{e_ie_je_100\cdots 0} = r_1 g^{e_i} g^{e_j}. \tag{22}$$

Now we come back to (part of the inductive base case) where $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 3$. We have three cases: the three 1s are in one block, two blocks or three blocks.

The case where they are in the same block is obvious by definition.

Next we consider the other two cases. If three 1s are in two blocks, then the form is $\Gamma^{e_i(e_j+e_l)00\cdots 0}$ $(j \neq l)$. Using the pattern and positions both as $e_1e_i(e_j+e_l)00\cdots 0$, we have MGI:

$$\Gamma^{e_i(e_j+e_l)0\cdots 0}\Gamma^{e_10\cdots 0} - \Gamma^{e_1(e_j+e_l)0\cdots 0}\Gamma^{e_i0\cdots 0} + \Gamma^{e_1e_ie_l0\cdots 0}\Gamma^{e_j0\cdots 0} - \Gamma^{e_1e_ie_j0\cdots 0}\Gamma^{e_l0\cdots 0} = 0.$$

Substituting (22) in the above equation, we find that the last two terms cancel out. And by definition, $\Gamma^{e_1(e_j+e_l)00\cdots 0} = g^{(e_j+e_l)}$. Therefore, we have

$$\Gamma^{e_i(e_j+e_l)00\cdots 0} = g^{e_i} g^{(e_j+e_l)}.$$

This satisfies (19).

The last case is that where three 1s are in three blocks. Then the form is $\Gamma^{e_i e_j e_l 00\cdots 0}$. Using the pattern and positions both as $e_1 e_i e_j e_l 00\cdots 0$, we have MGI:

$$\Gamma^{e_i e_j e_l 0\cdots 0}\Gamma^{e_1 0\cdots 0} - \Gamma^{e_1 e_j e_l 0\cdots 0}\Gamma^{e_i 0\cdots 0} + \Gamma^{e_1 e_i e_l 0\cdots 0}\Gamma^{e_j 0\cdots 0} - \Gamma^{e_1 e_i e_j 0\cdots 0}\Gamma^{e_l 0\cdots 0} = 0.$$

Substituting (22) in it, we find the last two terms cancel out and

$$\Gamma^{e_i e_j e_l 00\cdots 0} = r_1 g^{e_i} g^{e_j} g^{e_l}.$$

This also satisfies (19).

Inductively we assume that (19) has been proved for all $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) \le 2(i-1)+1$, for some $i \ge 2$. Now $\mathrm{wt}(\alpha_1\alpha_2\cdots\alpha_n) = 2i+1 \ge 5$.

By symmetry, we can assume $\alpha_1 \ne 0^k$. Consider the first bit of α_1; there are two cases: it is 1 or 0.

First we assume that the first bit of α_1 is 1. Using positions $(\alpha_1+e_1)\alpha_2\cdots\alpha_n$ and the pattern $\alpha_1\alpha_2\cdots\alpha_n + e_t$, where t is the position of the first 1 in the pattern $(\alpha_1+e_1)\alpha_2\cdots\alpha_n$, we have MGI:

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \sum_{j=2}^{2i}(-1)^j \Gamma^{\alpha_1\alpha_2\cdots\alpha_n+e_t+e_{p_j}}\Gamma^{e_1+e_t+e_{p_j}}. \quad (23)$$

Note that every Γ^β in the RHS has weight $\mathrm{wt}(\beta) \le 2i-1$, so we can apply (19) to them. Again we do the summation block by block; the sum of the rth block is denoted as S_r. Let $2q+1$ be the number of blocks with odd weight in the pattern $\alpha_1\alpha_2\cdots\alpha_n$. Note that this number is odd.

Now we must divide the proof into two cases, depending on whether t is in the first block (α_1+e_1) or not. If it is not, then $\alpha_1 = e_1$. In this case the first block is not involved in the MGI at all. Exactly the same proof as in Theorem 1 works here.

So we assume that t is in the first block (α_1+e_1). For the first block, let $w_1 = \mathrm{wt}(\alpha_1+e_1) = \mathrm{wt}(\alpha_1)-1$. If $w_1 = 1$, then $S_1 = 0$, being an empty sum. Assume that $w_1 > 1$. In the notation below we consider $e_t, e_{p_j} \in \{0,1\}^k$ for convenience.

$$S_1 = \sum_{j=2}^{w_1}(-1)^j \Gamma^{(\alpha_1+e_t+e_{p_j})\alpha_2\cdots\alpha_n}\Gamma^{(e_1+e_t+e_{p_j})00\cdots 0} \quad (24)$$

$$= r_1^q g^{\alpha_2}\cdots g^{\alpha_n}\sum_{j=2}^{w_1}(-1)^j g^{\alpha_1+e_t+e_{p_j}} g^{e_1+e_t+e_{p_j}}. \quad (25)$$

Note that the exponent q in r_1^q comes from the fact that the number of blocks with odd weight among $\alpha_1+e_t+e_{p_j}, \alpha_2, \ldots, \alpha_n$ is $2q+1$.

If w_1 is odd, using the pattern $(\alpha_1+e_t)1$ and positions $(\alpha_1+e_1)1$, we have the following MGI for Γ_0:

$$-g^{\alpha_1} + \sum_{j=2}^{w_1}(-1)^j g^{\alpha_1+e_t+e_{p_j}} g^{e_1+e_t+e_{p_j}} + g^{\alpha_1+e_t} g^{e_t+e_1} = 0.$$

Substituting this in (25), we have

$$S_1 = r_1^q g^{\alpha_2}\cdots g^{\alpha_n}(g^{\alpha_1} - g^{\alpha_1+e_t} g^{e_t+e_1}).$$

We note that this is also valid for $w_1 = 1$.

If w_1 is even, using the pattern $(\alpha_1+e_t)0$ and positions $(\alpha_1+e_1)0$, we have the following matchgate identity for Γ_0:

$$-g^{\alpha_1} + \sum_{j=2}^{w_1}(-1)^j g^{\alpha_1+e_t+e_{p_j}} g^{e_1+e_t+e_{p_j}} = 0.$$

Substituting this in (25), we have

$$S_1 = r_1^q g^{\alpha_1} g^{\alpha_2}\cdots g^{\alpha_n}.$$

If all S_r are empty blockwise sums for $r > 1$ (i.e., $w_r = 0$ for all $r > 1$), then w_1 must be even (this means that $\mathrm{wt}(\alpha_1)$ is odd), and we are done. Now suppose there are non-empty blockwise sums S_r, for $r > 1$. For the rth block, let $w_r = \mathrm{wt}(\alpha_r)$ and v_r be the number of 1s in the first $r-1$ blocks of the pattern $(\alpha_1+e_1)\alpha_2\cdots\alpha_n$, and p_j^r (where $j \in [w_r]$) be the position of the jth 1 in α_r. We have

$$S_r = (-1)^{v_r}\sum_{j=1}^{w_r}(-1)^j \Gamma^{(\alpha_1+e_t)\alpha_2\cdots(\alpha_r+e_{p_j^r})\cdots\alpha_n}\Gamma^{(e_1+e_t)00\cdots(e_{p_j^r})\cdots 0} \quad (26)$$

$$= (-1)^{v_r} r_1^{q'} g^{e_1+e_t} g^{\alpha_1+e_t} g^{\alpha_2}\cdots\widehat{g^{\alpha_r}}\cdots g^{\alpha_n}\sum_{j=1}^{w_r}(-1)^j g^{\alpha_r+e_{p_j^r}} g^{e_{p_j^r}}, \quad (27)$$

where $\widehat{g^{\alpha_r}}$ denotes a missing factor, and $2q'+1$ is the total number of odd blocks in $\alpha_1+e_t, \alpha_2, \ldots, \alpha_r+e_{p_j^r}, \ldots, \alpha_n$.

If w_r is even, using the pattern and positions both as $\alpha_r 0$, we have the following MGI for Γ_0:

$$\sum_{j=1}^{w_r}(-1)^j g^{\alpha_r+e_{p_j^r}} g^{e_{p_j^r}} = 0.$$

Substituting this in (26) and (27), we have $S_r = 0$.

Therefore, among block sums S_r, for $r > 1$, we need only consider blocks with odd w_r. Assume that w_r is odd now; we have $q' = q$ if w_1 is odd, and $q' = q - 1$ if w_1 is even. Using the pattern and positions both as $\alpha_r 1$, we have the following MGI for Γ_0:

$$\sum_{j=1}^{w_r}(-1)^j g^{\alpha_r+e_{p_j^r}} g^{e_{p_j^r}} + g^{\alpha_r} = 0.$$

Substituting this in (26) and (27), we have

$$S_r = -(-1)^{v_r} r_1^{q'} g^{e_t+e_1} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_r} \cdots g^{\alpha_n}.$$

To sum up, after the first block sum S_1, every even block will be zero, and every odd block will alternatingly contribute a $\pm r_1^{q'} g^{e_t+e_1} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$. If S_1 is an even block sum (this means that $\mathrm{wt}(\alpha_1 + e_1)$ is even, but $\mathrm{wt}(\alpha_1)$ is odd), then this alternating sum has an even number of such terms, and they all cancel out. This leaves us with the desired result $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = S_1 = r_1^q g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}$.

If S_1 is an odd block sum (this means that $\mathrm{wt}(\alpha_1 + e_1)$ is odd, but $\mathrm{wt}(\alpha_1)$ is even), then $q' = q$, and there are an odd number of alternating terms from S_r for $r > 1$, starting with the sign $-(-1)^{v_2} = +1$. (Note that $v_2 = w_1 = \mathrm{wt}(\alpha_1 + e_1)$ is odd.) These will cancel out pairwise except one $r_1^q g^{e_t+e_1} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$ left, which cancels the $-r_1^q g^{e_t+e_1} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$ in S_1. In either case, we have

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = r_1^q g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}.$$

Now we come back to the other case where the first bit of α_1 is 0.

Using the pattern and positions both as $(\alpha_1 + e_1)\alpha_2 \cdots \alpha_n$, we have MGI:

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = \sum_{j=2}^{2i}(-1)^j \Gamma^{(\alpha_1+e_1)\alpha_2\cdots\alpha_n+e_{p_j}} \Gamma^{e_{p_j}}. \tag{28}$$

Note that $\mathrm{wt}((\alpha_1 + e_1)\alpha_2 \cdots \alpha_n + e_{p_j}) = \mathrm{wt}(\alpha_1\alpha_2 \cdots \alpha_n) = 2i + 1$ in the RHS, but the first bit of $(\alpha_1 + e_1)\alpha_2 \cdots \alpha_n + e_{p_j}$ is 1. For these indices, we have already proved that (19) is satisfied.

Therefore we can apply (19) in the RHS of (28) and do the summation block by block. For the first block, let $w_1 = \mathrm{wt}(\alpha_1 + e_1)$ $(= \mathrm{wt}(\alpha_1) + 1)$. Note that $w_1 > 1$ since we assumed $\alpha_1 \neq 0^k$.

$$S_1 = \sum_{j=2}^{w_1}(-1)^j \Gamma^{(\alpha_1+e_1+e_{p_j})\alpha_2\cdots\alpha_n} \Gamma^{e_{p_j}0\cdots0} = r_1^q g^{\alpha_2} \cdots g^{\alpha_n} \sum_{j=2}^{w_1}(-1)^j g^{\alpha_1+e_1+e_{p_j}} g^{e_{p_j}}. \tag{29}$$

Note that the exponent q in r_1^q comes from the fact that the number of blocks with odd weight among $\alpha_1+e_1+e_{p_j}, \alpha_2, \ldots, \alpha_n$ is $2q + 1$.

If w_1 is odd, using the pattern and positions both as $(\alpha_1 + e_1)1$, we have the following MGI for Γ_0:

$$-g^{\alpha_1} + \sum_{j=2}^{w_1}(-1)^j g^{\alpha_1+e_1+e_{p_j}} g^{e_{p_j}} + g^{\alpha_1+e_1} = 0.$$

Here we used $g^{e_1} = g^{0^k} = 1$. Substituting this in (29), we have

$$S_1 = r_1^q g^{\alpha_2} \cdots g^{\alpha_n}(g^{\alpha_1} - g^{\alpha_1+e_1}).$$

If w_1 is even, using the pattern and positions both as $(\alpha_1 + e_1)0$, we have the following MGI for Γ_0:

$$-g^{\alpha_1} + \sum_{j=2}^{w_1}(-1)^j g^{\alpha_1+e_1+e_{p_j}} g^{e_{p_j}} = 0.$$

Substituting this in (29), we have

$$S_1 = r_1^q g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}.$$

If all S_r are empty blockwise sums for $r > 1$ (i.e., $w_r = 0$ for all $r > 1$), then w_1 must be even, and we are done. Now suppose there are non-empty blockwise sums S_r, for $r > 1$. For the rth block, let $w_r = \mathrm{wt}(\alpha_r)$ and v_r be the number of 1s in the first $r-1$ blocks of the pattern $(\alpha_1 + e_1)\alpha_2 \cdots \alpha_n$, and p_j^r (where $j \in [w_r]$) be the position of the jth 1 in α_r. We have

$$S_r = (-1)^{v_r} \sum_{j=1}^{w_r} (-1)^j \Gamma^{(\alpha_1+e_1)\alpha_2\cdots(\alpha_r+e_{p_j^r})\cdots\alpha_n} \Gamma^{000\cdots(e_{p_j^r})\cdots 0} \tag{30}$$

$$= (-1)^{v_r} r_1^{q'} g^{\alpha_1+e_1} g^{\alpha_2} \cdots \widehat{g^{\alpha_r}} \cdots g^{\alpha_n} \sum_{j=1}^{w_r} (-1)^j g^{\alpha_r+e_{p_j^r}} g^{e_{p_j^r}}, \tag{31}$$

where $\widehat{g^{\alpha_r}}$ denotes a missing factor, and $2q'+1$ is the total number of odd blocks in $\alpha_1+e_1, \alpha_2, \ldots, \alpha_r+e_{p_j^r}, \ldots, \alpha_n$. We also used $g^{0^k} = 1$.

If w_r is even, using the pattern and positions both as $\alpha_r 0$, we have the following MGI for Γ_0:

$$\sum_{j=1}^{w_r} (-1)^j g^{\alpha_r+e_{p_j^r}} g^{e_{p_j^r}} = 0.$$

Substituting this in (30) and (31), we have $S_r = 0$.

Therefore, among block sums S_r, for $r > 1$, we need only consider blocks with odd w_r. Assume w_r is odd now; we have $q' = q$ if w_1 is odd, and $q' = q - 1$ if w_1 is even. Using the pattern and positions both as $\alpha_r 1$, we have the following MGI for Γ_0:

$$\sum_{j=1}^{w_r} (-1)^j g^{\alpha_r+e_{p_j^r}} g^{e_{p_j^r}} + g^{\alpha_r} = 0.$$

Substituting this in (30) and (31), we have

$$S_r = -(-1)^{v_r} r_1^{q'} g^{\alpha_1+e_1} g^{\alpha_2} \cdots g^{\alpha_r} \cdots g^{\alpha_n}.$$

To sum up, after the first block sum S_1, every even block will be zero, and every odd block will alternatingly contribute a $\pm r_1^{q'} g^{\alpha_1+e_t} g^{\alpha_2} \cdots g^{\alpha_n}$. If S_1 is an even block sum (this means that $\mathrm{wt}(\alpha_1+e_1)$ is even), then this alternating sum has an even number of such terms, and they all cancel out. This leaves us with the desired result $\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = S_1 = r_1^q g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}$.

If S_1 is an odd block sum (this means that $\mathrm{wt}(\alpha_1+e_1)$ is odd), then $q' = q$, and there are an odd number of alternating terms from S_r for $r > 1$, starting with the sign $-(-1)^{v_2} = +1$. These will cancel out pairwise except one $r_1^q g^{\alpha_1+e_1} g^{\alpha_2} \cdots g^{\alpha_n}$ left, which cancels the $-r_1^q g^{\alpha_1+e_1} g^{\alpha_2} \cdots g^{\alpha_n}$ in S_1. In either case, we have finally

$$\Gamma^{\alpha_1\alpha_2\cdots\alpha_n} = r_1^q g^{\alpha_1} g^{\alpha_2} \cdots g^{\alpha_n}. \quad \square$$

References

[1] J.-Y. Cai, Vinay Choudhary, Some results on matchgates and holographic algorithms, in: Proceedings of ICALP 2006, Part I, in: Lecture Notes in Computer Science, vol. 4051, 2006, pp. 703–714. Also available at: ECCC TR06-048.

[2] J.-Y. Cai, Vinay Choudhary, Pinyan Lu, On the Theory of Matchgate Computations, in: The Proceedings of IEEE Conference on Computational Complexity 2007, pp. 305–318.

[3] J.-Y. Cai, Pinyan Lu, On symmetric signatures in holographic algorithms, in: The Proceedings of STACS 2007, in: LNCS, vol. 4393, 2007, pp. 429–440. Also available at: Electronic Colloquium on Computational Complexity Report TR06-135.

[4] J.-Y. Cai, Pinyan Lu, Holographic algorithms: From art to science, in: The Proceedings of STOC 2007, pp. 401–410.

[5] J. Edmonds, Minimum partition of a matroid into independent subsets, Journal of Research of the National Bureau of Standards, Section B 69 (1965) 67–72.

[6] M. Jerrum, Two-dimensional monomer–dimer systems are computationally intractable, Journal of Statistical Physics 48 (1987) 121–134. Journal of Statistical Physics 59 (1990) 1087–1088 (erratum).

[7] P.W. Kasteleyn, The statistics of dimers on a lattice, Physica 27 (1961) 1209–1225.

[8] P.W. Kasteleyn, Graph theory and crystal physics, in: F. Harary (Ed.), Graph Theory and Theoretical Physics, Academic Press, London, 1967, pp. 43–110.

[9] K. Murota, Matrices and Matroids for Systems Analysis, Springer, Berlin, 2000.

[10] H.N.V. Temperley, M.E. Fisher, Dimer problem in statistical mechanics — An exact result, Philosophical Magazine 6 (1961) 1061–1063.

[11] L.G. Valiant, Quantum circuits that can be simulated classically in polynomial time, SIAM Journal of Computing 31 (4) (2002) 1229–1254.

[12] L.G. Valiant, Expressiveness of matchgates, Theoretical Computer Science 281 (1) (2002) 457–471.

[13] L.G. Valiant, Holographic algorithms (extended abstract), in: Proc. 45th IEEE Symposium on Foundations of Computer Science, 2004, pp. 306–315. A more detailed version appeared in ECCC Report TR05-099.

[14] L.G. Valiant, Accidental algorithms, in: Proc. 47th Annual IEEE Symposium on Foundations of Computer Science, 2006, pp. 509–517.