On Symmetric Signatures in Holographic Algorithms

Jin-Yi Cai[a] *and Pinyan Lu[b]
[a] Computer Sciences Department, University of Wisconsin
Madison, WI 53706, USA
jyc@cs.wisc.edu
[b] Department of Computer Science and Technology, Tsinghua University
Beijing, 100080, P. R. China
lpy@mails.tsinghua.edu.cn

Abstract

The most intriguing aspect of the new theory of matchgate computations and holographic algorithms by Valiant [12] [14] is that its reach and ultimate capability are wide open. The methodology produces unexpected polynomial time algorithms solving problems which seem to require exponential time. To sustain our belief in P $\neq$ NP, we must begin to develop a theory which captures the limit of expressibility and power of this new methodology.

In holographic algorithms, *symmetric signatures* have been particularly useful. We give a complete characterization of these symmetric signatures over all bases of size 1. These improve previous results [4] where only symmetric signatures over the Hadamard basis (special basis of size 1) were obtained. This in particular confirms a conjecture by Valiant [18]. We also give a complete characterization of Boolean symmetric signatures over bases of size 1.

Finally, it is an open problem whether signatures over bases of higher dimensions are strictly more powerful. The recent result by Valiant [17] seems to suggest that bases of size 2 might be indeed more powerful than bases of size 1. This result is with regard to a restrictive counting version of #SAT called #Pl-Rtw-Mon-3CNF. It is known that the problem is #P-hard, and its mod 2 version is $\oplus$P-hard. Yet its mod 7 version is solvable in polynomial time by holographic algorithms. This was accomplished by a suitable symmetric signature over a basis of size 2 [17]. We show that the same unexpected holographic algorithm can be realized over a basis of size 1. Furthermore we prove that 7 is the only modulus for which such an "accidental algorithm" exists.

Subject: Computational and structural complexity.

1 Introduction

Valiant has recently developed the theory of matchgate computations and holographic algorithms [12, 14]. This is a novel methodology to design polynomial time algorithms. With this methodology, for some seemingly exponential time computations, one can design a custom made process to carry out exponentially many cancellations so that the computation can actually be done in polynomial time. Frequently the technical content of this design process amounts to finding a suitable *signature*.

These algorithms can appear quite unintuitive and exotic. So far, the main impact of this new theory is not so much as solving every day algorithmic problems, but rather pointing out the existence of some unexpected ways of doing computation. Thus, to us, the most intriguing aspect of the new theory is its

*Supported by NSF CCR-0208013 and CCR-0511679.

broader implication in complexity theory. A case in point is the following restrictive version of #SAT (the problem of counting satisfying assignments), called #Pl-Rtw-Mon-3CNF. Here we consider only planar Boolean formulae in Conjunctive Normal Form with 3 variables in each clause. Furthermore we assume each variable appears positively (Monotone) and in exactly two clauses (Read twice). (This problem can also be stated naturally as a Vertex Cover problem on 2-3-regular planar bipartite graphs.) #Pl-Rtw-Mon-3CNF has been studied before, including its approximate versions [6, 5, 1]. It is known to be #P-hard. Moreover counting the satisfying assignments modulo 2 for such formulae is $\oplus$P-hard. However, Valiant [17] showed that a surprising polynomial time (he called it an "accidental") algorithm exists for this counting problem mod 7, denoted $\#_7$Pl-Rtw-Mon-3CNF, using holographic algorithms. What makes this work is a particular *symmetric signature* exists over the field $\mathbf{Z}_7$. This is what Valiant called an "accidental or freak object" [17]. [1]

Suppose we all believe P $\neq$ NP. Unless and until a proof of P $\neq$ NP is found, one should regard this as an open problem. Then it is reasonable to ask where do we derive our confidence in this assertion. Certainly this is not due to any strong unconditional lower bound. We believe this confidence is based on the fact that all existing algorithmic approaches do not seem to tackle a myriad of NP-hard problems. Valiant's new theory of holographic algorithms challenges us to re-examine this belief critically. To put it bluntly, if you haven't seen these "exotic" or "accidental" algorithms, and haven't looked closely at how such algorithms behave, then how do you know such algorithms do not exist for one NP-hard problem? As Valiant pointed out [14], "any proof of P $\neq$ NP may need to explain, and not only to imply, the unsolvability" of NP-hard problems in this framework.

Valiant actually introduced two related theories, first, matchgate/matchcircuit [12], and second, holographic algorithms [14]. In the first theory, the basic notion is a matchgate and its *character*, defined by Pfaffians. He used this theory to simulate a fragment of quantum computations. In the second, a new ingredient was added, that of a linear vector basis through which computation is expressed. In this second theory, the matchgates are assumed to be planar, and each matchgate is associated with a *signature* defined by the Perfect Matching polynomial PerfMatch. Then the computation is ultimately done in terms of the Fisher-Kasteleyn-Temperley (FKT) method [7, 8, 11] via the *Holant Theorem* [14]. After the development from [3, 4], a certain unification of the two theories was achieved. Basically, using the algebraic properties of Pfaffians, we were able to achieve a complete characterization of *realizable* characters in [3]. In [4] an equivalence theorem was proved for matchgates/characters on the one hand and planar-matchgates/signatures on the other, thereby the characterization theorem also applies to planar matchgates and their *standard signatures*. In this paper, we will use these results.

Due to space limitations, we will omit most definitions, and refer the readers to [12, 14, 3, 4, 2]. A *planar matchgate* $\Gamma = (G, X, Y)$ is a weighted graph $G = (V, E, W)$ with a planar embedding, having external nodes, the input nodes X and the output nodes Y, placed on the outer face. Define $\text{PerfMatch}(G) = \sum_M \prod_{(i,j)\in M} w_{ij}$, where the sum is over all perfect matchings M. The *standard signature*, $u = u(\Gamma)$, is defined to be a $2^{|Y|} \times 2^{|X|}$ matrix whose entries are indexed by subsets $X' \subseteq X$ and $Y' \subseteq Y$, and the entry at (row Y', column X') is $u_Z = \text{PerfMatch}(G - Z)$, where $Z = X' \cup Y'$. Here $G - Z$ denotes the subgraph of G obtained by removing the subset of nodes in Z (and all their incident edges). Matchgates with only output nodes are called *generators*. Matchgates with only input nodes are called *recognizers*.

In the design of holographic algorithms so far, the most useful signatures have been the so-called *symmetric signatures*. A symmetric signature is one where u_Z only depends on the cardinality of Z; we denote this by $\sigma_{|Z|}$. Thus, a symmetric signature of a generator or a recognizer with k external nodes

[1] From Valiant [17]: "... the situation with the P = NP question is not dissimilar to that of other unresolved enumerative conjectures in mathematics. The possibility that accidental or freak objects in the enumeration exist cannot be discounted, if the objects in the enumeration have not been systematically studied previously."

can be identified with a vector of $k+1$ entries $\sigma = [\sigma_0, \sigma_1, \ldots, \sigma_k]$. The ingenious idea of holographic algorithms is that one can transform the standard signatures under a linear transformation of the basis vectors. Under this transformation, the symmetric signature will remain a symmetric signature, but will have a clear combinatorial meaning. E.g., $\sigma = [0, 1, 1, 1]$ will mean a Boolean OR. These combinatorial interpretations, when applied with the Holant Theorem [14], lead to polynomial time algorithms. The symmetric signatures are responsible for a majority of the interesting polynomial time algorithms in the new theory.

To understand the limit of holographic algorithms, and to develop a substantial theory for this new methodolgy, we must come to grips with what can or cannot be done by signatures of matchgates, under *all possible* basis transformations. This is still a rather remote goal. For now we can only say something intelligent on symmetric signatures, and over bases of size 1.

In this paper, we give a complete characterization of symmetric signatures over bases of size 1. Our characterization is valid for all fields with sufficiently large characteristic p (including the complex numbers $\mathbf{C}$, with characteristic ∞). These improve previous results [4] where only symmetric signatures over the Hadamard basis, which is a special basis of size 1, were obtained. In [4], those results were proved using properties of Krawtchouk polynomials. Here we are able to prove a much stronger results without the use of these special polynomials. This in particular confirms a conjecture by Valiant [18]. We also give a complete characterization of Boolean symmetric signatures over bases of size 1.

It is an open problem whether signatures over bases of higher dimensions are strictly more powerful. The recent result by Valiant [17] seems to suggest that this might be the case. He considered a restrictive version of #SAT, called #Pl-Rtw-Mon-3CNF: To count the number of satisfying assignments for a planar monotone read-twice 3CNF formula. The problem is #P-hard for counting [5, 1] and $\oplus$P-hard for counting mod 2. But Valiant showed that it is solvable by an exotic holographic algorithm for counting mod 7. In order to do that, he used a suitable signature, with a basis of size 2. We show that the same holographic algorithm for $\#_7$Pl-Rtw-Mon-3CNF can be realized over a basis of size 1. Furthermore we prove that 7 is the only modulus for which such an "accidental algorithm" exists.

2 Holographic Algorithms for $\#_7$Pl-Rtw-Mon-3CNF

We briefly review some background information on holographic algorithms.

We use the tensor theoretic treatment for matchgates (see [2]). Let $\mathbf{b}$ denote the standard basis for two dimensional space (or size 1), $\mathbf{b} = [e_0, e_1] = \left[\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right]$. Consider another basis $\boldsymbol{\beta} = [n, p] = \left[\begin{pmatrix}n_0\\n_1\end{pmatrix}, \begin{pmatrix}p_0\\p_1\end{pmatrix}\right]$. Let T be the transformation matrix from $\mathbf{b}$ to $\boldsymbol{\beta}$, where $T = \begin{bmatrix}n_0 & p_0\\ n_1 & p_1\end{bmatrix}$, and $\boldsymbol{\beta} = \mathbf{b}T$. For convenience, denote $T = (t^i_j)$ and $T^{-1} = (\tilde{t}^i_j)$. (Upper index is for row and lower index is for column.)

Each generator (with n output nodes) is associated with a contravariant tensor $\mathbf{G}$. Each recognizer (with n input nodes) is associated with a covariant tensor $\mathbf{R}$. The standard signature of a matchgate is the expression of its matchgate tensor under the standard basis for the tensor product space. Under a basis transformation $\boldsymbol{\beta} = \mathbf{b}T$, these tensors take different forms, and transform either *contravariantly* or *covariantly*.

More concretely, the contravariant tensor $\mathbf{G}$ of a generator transforms under the basis transformation $\boldsymbol{\beta} = \mathbf{b}T$ as

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

Here the entry of the standard signature $G^{i_1 i_2 \ldots i_n} = \text{PerfMatch}(G - Z)$, and the bit string $i_1 i_2 \ldots i_n$

denotes subset Z. Correspondingly, the covariant tensor $\mathbf{R}$ of a recognizer transforms as

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

(where the sum is with all matching upper and lower indices.)

Let's consider #Pl-Rtw-Mon-3CNF. We are given a planar formula in 3CNF form, where each variable appears positively, and appearing in exactly 2 clauses. By being a planar formula [9] our formula can be drawn as a planar bipartite graph (L, R, E), where each variable x is represented by a node in L, and each clause C is represented by a node in R, such that they are connected iff x appears in C. Because it is a Read-twice 3CNF, each node in L has degree 2, and each node in R has degree 3.

Now we replace each node in L by a generator with 2 outputs, and replace each node in R by a recognizer with 3 inputs, and connect each generator output and recognizer input in the natural way. This means that, suppose x appears in C, and $G[x]$ and $R[C]$ are the generator and recognizer for x and C respectively, then there is an edge (with assigned weight 1) connecting one output of $G[x]$ and one input of $R[C]$.

This is called a matchgrid Ω. If Ω has g generators $G[i]$ and r recognizers $R[j]$, and $w(= 2g = 3r)$ connecting wires, the beautiful *Holant Theorem* of Valiant [14] states that under *any basis* $\boldsymbol{\beta}$,

$$\text{Holant}(\Omega) = \text{PerfMatch}(G), \tag{3}$$

where

$$\text{Holant}(\Omega) = \sum_{x \in \boldsymbol{\beta}^{\otimes f}} \{[\Pi_{1 \le i \le g} G[i]^x] \cdot [\Pi_{1 \le j \le r} R[j]_x]\}. \tag{4}$$

(In tensor language, this is called a contraction.)

Now imagine we were able to find a generator matchgate G, a recognizer matchgate R, and a basis $\boldsymbol{\beta}$ over the field of complex numbers $\mathbf{C}$, such that G has a signature $[1, 0, 1]$ and R has a signature $[0, 1, 1, 1]$. Note that the signature $[1, 0, 1] = 1n \otimes n + 0(n \otimes p + p \otimes n) + 1p \otimes p$ has the clear combinatorial meaning of two equal signals nn or pp, and $[0, 1, 1, 1]$ has the Boolean meaning of OR. Thus the exponential sum represented by Holant(Ω) in (4) counts exactly the number of satisfying assignments of the original Boolean formula, since each such assignment contributes exactly one to the sum defining Holant(Ω).

However, Holant(Ω) is not computed by its defining expression (4), but rather as PerfMatch(G) in (3) by the Holant Theorem. Notice how fragments of actual Boolean assignments to the 3CNF formula, represented by the signature entries, get all "mixed up holographically" by the transformation in (1) and (2), so that each fragment is split into exponentially many "shares" which then get summed up in (3). The latter can be computed in polynomial time by the FKT method. Now if we were able to find such matchgates and a basis over $\mathbf{C}$ such that the (symmetric) signatures have the desired form, it would have collapsed #P to P.

However, Valiant showed that one *can* find such matchgates and a basis over $\mathbf{Z}_7$, but a larger basis of size 2 is used (we will not formally define this notion for space limitations). The resulting Holant counts the number of satisfying assignments modulo 7. This is surprising, especially because it is known that the problem modulo 2 is $\oplus$P-hard.

In the rest of this section we prove that the problem can be solved using a basis of size 1. Moreover, modulo 7 is the only modulus for which this is possible.

Theorem 2.1. *For* $\mathbf{Z}_7$ *and for basis* $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right] = \left[\binom{1}{6}, \binom{3}{5}\right]$, *there is a generator for* $[1, 0, 1]$ *and a recognizer for* $[0, 1, 1, 1]$.

Remark: We recall that the notation is for symmetric signatures. Thus for a generator, $[1,0,1]$ denotes $(1,0,0,1)^{\mathrm{T}}$ in dimension 4, and for a recognizer, $[0,1,1,1]$ denotes $(0,1,1,1,1,1,1,1,1)$ in dimension 8.
Proof: It is a simple fact that the standard signature $(3,0,0,5)^{\mathrm{T}}$ is realizable by a generator matchgate with 2 outputs. This can be shown directly by a direct construction [14] or it follows from the general theory of standard signature realizability theorem in terms of matchgate identities [14, 3, 4]. Similarly the standard signatures $[0,3,0,5]$ is realizable by a recognizer, with 3 inputs.

A simple calculation shows that $n \otimes n + p \otimes p = (3,0,0,5)^{\mathrm{T}}$ for the chosen basis $\boldsymbol{\beta}$ over $\mathbf{Z}_7$. Thus the generator has signature $[1,0,1]$ under the basis $\boldsymbol{\beta}$.

As a recognizer, its signature $u_{\boldsymbol{\beta}}$ w.r.t. the basis $\boldsymbol{\beta}$ and its standard signature u are related by the equation

$$u_{\boldsymbol{\beta}} = uT^{\otimes 3}, \qquad \text{where} \qquad T = \begin{bmatrix} n_0 & p_0 \\ n_1 & p_1 \end{bmatrix}.$$

We can calculate its signature w.r.t. $\boldsymbol{\beta}$, and we find the symmetric signature $[r_0, r_1, r_2, r_3]$, where
$r_0 = 3 \times 3n_0^2 n_1 + 5n_1^3 = 0$,
$r_1 = 3(n_0^2 p_1 + 2n_0 n_1 p_0) + 5n_1^2 p_1 = 1$,
$r_2 = 3(p_0^2 n_1 + 2p_0 p_1 n_0) + 5p_1^2 n_1 = 1$,
$r_3 = 3 \times 3p_0^2 p_1 + 5p_1^3 = 1$.
Therefore this matchgate recognizes $[0,1,1,1]$. □

Corollary 2.1. *There is a polynomial time algorithm for $\#_7$Pl-Rtw-Mon-CNF.*

For bases of size 1, we can further prove that a similar technique can not be applied to any other $\#_k$Pl-Rtw-Mon-3CNF problem unless $k = 7$. This result may highlight the true "accidental" nature of the polynomial time algorithm for $\#_7$Pl-Rtw-Mon-3CNF.

Theorem 2.2. *Characteristic 7 is the unique characteristic of a field for which there is a common basis of size 1 for generating $[1,0,1]$ and recognizing $[0,1,1,1]$.*

The proof is omitted here, and is given in the appendix.

3 Symmetric Signatures

In this section we give a closed form solution to characterize all symmtric signatures of generators and recognizers, under any basis of size 1. Our closed form applies to complex numbers $\mathbf{C}$ and to all fields with characteristic p greater than the arity n of the matchgate. Since we can calculate (t_j^i) and $(\tilde{t}_j^i)$ from $[n,p]$, we need only consider recognizers. The situation for generators is similar.

In tensor analysis we have the following proposition, which is straightfarward from (1)(2).

Proposition 3.1. *If a tensor $\mathbf{T}$ is symmetric in one basis, it is still symmetric after transforming to other basis.*

Since we focus on the case of two dimensional space $\mathbf{V}$ spanned by $\{e_0, e_1\}$, all the symmetric tensors in $\mathbf{V}^{\otimes n}$ form a $n+1$ dimensional space, which can be denoted by $\sigma = [\sigma_0, \sigma_1, \ldots, \sigma_n]$. The symmetric signature transforms as follows under a basis transformation:

$$\sigma'_{k'} = \sum_k \sigma_k a_{k'}^k, \tag{5}$$

where

$$a_{k'}^k = \sum_{s=0}^{k} \binom{k'}{s} \binom{n-k'}{k-s} (t_1^1)^s (t_1^0)^{k'-s} (t_0^1)^{k-s} (t_0^0)^{n-k-k'+s}. \tag{6}$$

We can rewrite (6) as

$$a^k_{k'} = (t^0_1)^{k'}(t^0_0)^{n-k'} \sum_{s=0}^{k} \binom{k'}{s}\binom{n-k'}{k-s}\left(\frac{t^1_1 t^0_0}{t^0_1 t^1_0}\right)^s \left(\frac{t^1_0}{t^0_0}\right)^k. \tag{7}$$

A matchgate is called an even or an odd matchgate, precisely when it has an even or an odd number of nodes. The parity consideration is crucial in signatures of matchgates, as they are defined in terms of perfect matchings. More subtle, but just as important, are the *matchgate identities* [14, 3]. From the work of [3, 4] we know the following precise information regarding symmetric standard signatures.

Lemma 3.1. *Suppose Γ is an even matchgate, with symmetric standard signature $\sigma = [\sigma_0, \sigma_1, \ldots, \sigma_n]$. Then for all odd i, $\sigma_i = 0$, and there exist constants r_1, r_2 and λ, such that $\sigma_{2i} = \lambda \cdot (r_1)^{[n/2]-i} \cdot (r_2)^i$.*

Lemma 3.2. *Suppose Γ is an odd matchgate, with symmetric standard signature $\sigma = [\sigma_0, \sigma_1, \ldots, \sigma_n]$. Then for all even i, $\sigma_i = 0$, and there exist constants r_1, r_2 and λ, such that $\sigma_{2i+1} = \lambda \cdot (r_1)^{[(n-1)/2]-i} \cdot (r_2)^i$.*

Let's substitute $r_1 = b^2$ and $r_2 = c^2$ (if necessary in an extension field). Since $b = 0$ and $c = 0$ is trivial, we assume at least one of them is non-zero.

Case 1: even n and even matchgate

In this case, we have $\sigma_k = \lambda b^{n-k} c^k$, $\forall k$ even, and $\sigma_k = 0$, $\forall k$ odd. From (5) and (7) we get:

$$\begin{aligned}
\sigma'_{k'} &= \sum_{k=0}^{n} \sigma_k a^k_{k'} \\
&= \lambda \sum_{k\ even} b^{n-k} c^k a^k_{k'} \\
&= \lambda (t^0_1)^{k'}(t^0_0)^{n-k'} \sum_{k\ even} b^{n-k} c^k \left[\sum_{s=0}^{k} \binom{k'}{s}\binom{n-k'}{k-s}\left(\frac{t^1_1 t^0_0}{t^0_1 t^1_0}\right)^s \left(\frac{t^1_0}{t^0_0}\right)^k\right] \\
&= \lambda (t^0_1)^{k'}(t^0_0)^{n-k'} \sum_{s=0}^{n} \binom{k'}{s}\left(\frac{ct^1_1}{t^0_1}\right)^s b^{k'-s} \left[\sum_{k\ even,\ k\geq s} \binom{n-k'}{k-s} b^{n-k'-k+s}\left(\frac{ct^1_0}{t^0_0}\right)^{k-s}\right].
\end{aligned}$$

Now the second sum within the brackets is

$$\sum_{k\ even,\ k\geq s} \binom{n-k'}{k-s} b^{n-k'-k+s}\left(\frac{ct^1_0}{t^0_0}\right)^{k-s} = \frac{1}{2}\left[\left(b + \frac{ct^1_0}{t^0_0}\right)^{n-k'} \pm \left(b - \frac{ct^1_0}{t^0_0}\right)^{n-k'}\right],$$

Choose $+$ if s is even and $-$ if s is odd.

Therefore, we have

$$\begin{aligned}
\sigma'_{k'} &= \frac{1}{2}\lambda (t^0_1)^{k'}(t^0_0)^{n-k'} \left[\left(b + \frac{ct^1_0}{t^0_0}\right)^{n-k'} + \left(b - \frac{ct^1_0}{t^0_0}\right)^{n-k'}\right] \left[\sum_{s\ even}^{n} \binom{k'}{s}\left(\frac{ct^1_1}{t^0_1}\right)^s b^{k'-s}\right] \\
&\quad + \frac{1}{2}\lambda (t^0_1)^{k'}(t^0_0)^{n-k'} \left[\left(b + \frac{ct^1_0}{t^0_0}\right)^{n-k'} - \left(b - \frac{ct^1_0}{t^0_0}\right)^{n-k'}\right] \left[\sum_{s\ odd}^{n} \binom{k'}{s}\left(\frac{ct^1_1}{t^0_1}\right)^s b^{k'-s}\right] \\
&= \frac{1}{2}\lambda (t^0_1)^{k'}[(bt^0_0 + ct^1_0)^{n-k'} + (bt^0_0 - ct^1_0)^{n-k'}] \cdot \frac{1}{2}\left[\left(b + \frac{ct^1_1}{t^0_1}\right)^{k'} + \left(b - \frac{ct^1_1}{t^0_1}\right)^{k'}\right] \\
&\quad + \frac{1}{2}\lambda (t^0_1)^{k'}[(bt^0_0 + ct^1_0)^{n-k'} - (bt^0_0 - ct^1_0)^{n-k'}] \cdot \frac{1}{2}\left[\left(b + \frac{ct^1_1}{t^0_1}\right)^{k'} - \left(b - \frac{ct^1_1}{t^0_1}\right)^{k'}\right]
\end{aligned}$$

$$= \frac{1}{2}\lambda[(bt_0^0 + ct_0^1)^{n-k'}(bt_1^0 + ct_1^1)^{k'} + (bt_0^0 - ct_0^1)^{n-k'}(bt_1^0 - ct_1^1)^{k'}].$$

The proof of other cases are omitted here, and can be found in the Appendix.

To sum up, we get the following theorem:

Theorem 3.1. *A symmetric signature $[x_0, x_1, \ldots, x_n]$ for a recognizer is realizable under the basis $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$* iff *it takes one of the following forms:*

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

$$x_i = \lambda[(sn_0 + tn_1)^{n-i}(sp_0 + tp_1)^i + \epsilon(sn_0 - tn_1)^{n-i}(sp_0 - tp_1)^i]. \tag{8}$$

- *Form 2: there exist (arbitrary) constants λ,such that for all $i, 0 \le i \le n$,*

$$x_i = \lambda[(n-i)n_0(p_1)^i(n_1)^{n-1-i} + ip_0(p_1)^{i-1}(n_1)^{n-i}]. \tag{9}$$

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

$$x_i = \lambda[(n-i)n_1(p_0)^i(n_0)^{n-1-i} + ip_1(p_0)^{i-1}(n_0)^{n-i}]. \tag{10}$$

Similarly we can prove

Theorem 3.2. *A symmetric signature $[x_0, x_1, \ldots, x_n]$ for a generator is realizable under the basis $\boldsymbol{\beta} = [n, p] = \left[\binom{n_0}{n_1}, \binom{p_0}{p_1}\right]$* iff *it takes one of the following forms:*

- *Form 1: there exist (arbitrary) constance λ, s, t and ϵ where $\epsilon = \pm 1$, such that for all $i, 0 \le i \le n$,*

$$x_i = \lambda[(sp_1 - tp_0)^{n-i}(-sn_1 + tn_0)^i + \epsilon(sp_1 + tp_0)^{n-i}(-sn_1 - tn_0)^i]. \tag{11}$$

- *Form 2: there exist (arbitrary) constants λ,such that for all $i, 0 \le i \le n$,*

$$x_i = \lambda[(n-i)p_1(n_0)^i(-p_0)^{n-1-i} - in_1(n_0)^{i-1}(-p_0)^{n-i}]. \tag{12}$$

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

$$x_i = \lambda[-(n-i)p_0(-n_1)^i(p_1)^{n-1-i} + in_0(-n_1)^{i-1}(p_1)^{n-i}]. \tag{13}$$

We wish to obtain another characterization of realizable symmetric signatures. First, we deal with some degenerate cases. The following three cases are called degenerate:

- In Form 1, $sn_0 + tn_1 = 0$ or $sn_0 - tn_1 = 0$.
- In Form 2, $n_1 = 0$.
- In Form 3, $n_0 = 0$.

In Form 1, if $sn_0 + tn_1 = 0$ and $sn_0 - tn_1 = 0$, then all the realizable signatures take the following form (λ is arbitrary):

$$[0, 0, \cdots, 0, \lambda]. \tag{14}$$

In Form 1, if $sn_0 + tn_1 = 0$ and $sn_0 - tn_1 \neq 0$, or $sn_0 + tn_1 \neq 0$ and $sn_0 - tn_1 = 0$, then all the realizable signatures take the following form (a, q, λ are arbitrary):

$$[a, aq, aq^2, \cdots, aq^{n-1}, \lambda]. \tag{15}$$

Notice that (14) is a special case of (15), we will not consider (14) later.

In Form 2, if $n_1 = 0$, then all the realizable signatures take the following form (λ_1, λ_2 is arbitrary):

$$[0, 0, \cdots, 0, \lambda_1, \lambda_2]. \tag{16}$$

In form 3, if $n_0 = 0$, then all the realizable signatures take the following form (λ_1, λ_2 is arbitrary):

$$[0, 0, \cdots, 0, \lambda_1, \lambda_2].$$

This is the same as (16).

Besides these degenerate cases, we can rewrite the sequence defined in Form 1 as $x_i = A\alpha^i + B\beta^i$, and the sequence defined Form 2 or Form 3 as $x_i = \alpha^i(Ai + B)$. Both are solutions to **second-order homogeneous linear recurrences** ($x_i = ax_{i-1} + bx_{i-2}$). To sum up in a more symmetric way, we have the following theorem:

Theorem 3.3. *A symmetric signature $[x_0, x_1, \cdots, x_n]$ is realizable on some basis of size 1 iff there exists three constants a, b, c(not all zero), such that $\forall k, 0 \leq k \leq n-2$,*

$$ax_k + bx_{k+1} + cx_{k+2} = 0. \tag{17}$$

Proof:

"$\Rightarrow$":

Since $[x_0, x_1, \cdots, x_n]$ is realizable, from Theorem 3.1 (3.2), x_i takes one of the forms in Theorem 3.1 (3.2). If it is degenerate as (15), we can let $a = -q, b = 1, c = 0$. If it is degenerate as (16), we can let $a = 1, b = 0, c = 0$. Otherwise it is a second-order homogeneous linear recurring sequence $x_i = a_0x_{i-1} + b_0x_{i-2}$, we can let $a = b_0, b = a_0, c = -1$. Therefore if $[x_0, x_1, \cdots, x_n]$ is realizable on some basis of size 1 , there exists three constants a, b, c (not all zero), such that $\forall k, 0 \leq k \leq n-2$, $ax_k + bx_{k+1} + cx_{k+2} = 0$.

"$\Leftarrow$":

If $c = 0$ and $b = 0$, then $a \neq 0$. From (17), we know $x_k = 0,\ \forall k, 0 \leq k \leq n-2$. So $\{x_i\}$ takes the form (16), which is realizable.

If $c = 0$ and $b \neq 0$, form (17) we have $ax_k + bx_{k+1} = 0,\ \forall k, 0 \leq k \leq n-2$. Let $q = -a/b$, we have $x_{k+1} = x_kq,\ \forall k, 0 \leq k \leq n-2$. Therefore $\{x_i\}$ takes the form (15), which is realizable.

Otherwise $c \neq 0$, substituting $a_0 = -b/c, b_0 = -a/c$, we have $x_{k+2} = a_0x_{k+1} + b_0x_k,\ \forall k, 0 \leq k \leq n-2$. The characteristic equation is $x^2 - a_0x - b_0 = 0$. Let α, β be the two roots of the characteristic equation. If $\alpha \neq \beta$, we can calculate A, B such that $x_i = A\alpha^i + B\beta^i,\ \forall i, 0 \leq i \leq n$. If $A = B = 0$, then $x_i = 0,\ \forall i, 0 \leq i \leq n$, which trivially realizable. If $A = 0$ and $B \neq 0$ (the case $B = 0$ and $A \neq 0$ is similar), then $x_i = B\beta^i$. Let $\lambda = \epsilon = s = t = 1, p_0 = p_1 = \sqrt[n]{B}\alpha/2, n_0 = n_1 = \sqrt[n]{B}/2$ (notice that this basis is not linearly independent) in (8), we know it is realizable. Otherwise $AB \neq 0$, let $\lambda = \epsilon = s = t = 1$ in (8), we have the following equations:

$$n_0 + n_1 = \sqrt[n]{A} \tag{18}$$

$$n_0 - n_1 = \sqrt[n]{B} \tag{19}$$

$$p_0 + p_1 = \alpha \sqrt[n]{A} \tag{20}$$

$$p_0 - p_1 = \beta \sqrt[n]{B} \tag{21}$$

From the above equations, we can get the value of n_0, n_1, p_0, p_1 and we conclude that $x_i = A\alpha^i + B\beta^i$ is realizable.
If $\alpha = \beta$ we can calculate A, B such that $x_i = \alpha^i(Ai + B),\ \forall i, 0 \leq i \leq n$. If $\alpha = 0$ or $A = 0$, the above argument shows it is realizable. Otherwise let $\lambda = n_1 = 1, p_1 = \alpha, n_0 = \frac{B}{n}, p_0 = A\alpha + \frac{B\alpha}{n}$ in form (9), we conclude that $x_i = \alpha^i(Ai + B)$ is realizable.

□

Corollary 3.1. *Over the complex numbers* $\mathbf{C}$ *as well as all fields* $\mathbf{F}$ *of characteristic* $p > 3$*, every signature* $[x_0, x_1, x_2, x_3]$ *is realizable on some basis of size 1.*

Proof: View $r_1 = (x_0, x_1, x_2), r_2 = (x_1, x_2, x_3)$ as two vectors in 3-dimension Euclid space. Geometrically, there exists a non-zero vector $r_0 = (a, b, c)$ such that $r_0 \perp r_1$ and $r_0 \perp r_2$. That is $ax_0 + bx_1 + cx_2 = 0$ and $ax_1 + bx_2 + cx_3 = 0$. From Theorem 3.3, we know that $[x_0, x_1, x_2, x_3]$ is realizable. □

This confirms a conjecture by Valiant [18].

4 Boolean Symmetric Signatures

In this section, we consider the realizability of a special family of symmetric signatures, which we call boolean symmetric signatures (BSS).

Definition 4.1. *A signature of a generator or a recognizer is called a Boolean Symmetric Signature (BSS) iff it is symmetric* $[x_0, x_1, \ldots, x_n]$ *and* $\forall i \in [n], x_i \in \{0, 1\}$.

From Corollary 3.1 and Theorem 3.3 , we can conclude that:

Theorem 4.1. *When* $n \leq 3$*, all BSS are realizable.*

When $n \geq 4$, the set of realizable BSS is rather sparse. More precisely we have the following theorem:

Theorem 4.2. *When* $n \geq 4$*, a BSS* $[x_0, x_1, \ldots, x_n]$ *is realizable on some basis of size 1 iff it has one of the following forms* ($\lambda, \lambda_1, \lambda_2 \in \{0, 1\}$ *is arbitrary):*

$$[\lambda_1, 0, 0, \cdots, 0, \lambda_2] \tag{22}$$

$$[1, 1, \cdots, 1, \lambda] \tag{23}$$

$$[\lambda, 1, 1, \cdots, 1] \tag{24}$$

$$[0, 0, \cdots, 0, \lambda_1, \lambda_2] \tag{25}$$

$$[\lambda_1, \lambda_2, 0, 0, \cdots, 0] \tag{26}$$

$$[1, 0, 1, 0, \cdots, 0(1)] \tag{27}$$

$$[0, 1, 0, 1, \cdots, 0(1)] \tag{28}$$

Proof: From Theorem 3.3, we can check that form 22–28 are all realizable.
Now we prove that form 22–28 are the only possible cases. Since BSS $[x_0, x_1, \ldots, x_n]$ is realizable on some basis of size 1, we know that there exists three constants a, b, c(not all zero), such that $\forall k, 0 \leq k \leq n-2$, $ax_k + bx_{k+1} + cx_{k+2} = 0$.
If $c = 0$ and $b = 0$, then $a \neq 0$. From (17), we know $x_k = 0,\ \forall k, 0 \leq k \leq n-2$. So $\{x_i\}$ takes the form (25).
If $c = 0$ and $b \neq 0$, we know $\{x_i\}$ takes the form of (15). Since we further request it to be a BSS, the only possible form is (22),(23).
Otherwise $c \neq 0$, we can rewrite (17) as

$$x_{k+2} = a_0 x_{k+1} + b_0 x_k. \tag{29}$$

We prove the result by checking all the possible values of x_0, x_1, x_2, x_3.

- $[0, 0, *, *]$: from (29) we know $x_i = 0, \forall i$. This takes the form (26). (Here if * is not 0, the signature is not realizable)
- $[0, 1, 0, 0]$:from (29) we know $a_0 = b_0 = 0$ and therefore $x_i = 0, \forall i \geq 2$. This takes the form (26).
- $[0, 1, 0, 1]$:from (29) we know $a_0 = 0, b_0 = 1$. Therefore $\{x_i\}$ takes the form (28).
- $[0, 1, 1, 0]$:from (29) we know $a_0 = 1, b_0 = -1$. But $x_4 = x_3 - x_2 = -1$, so this is not a BSS. (Here we assume the characteristic of the field is not 2).
- $[0, 1, 1, 1]$:from (29) we know $a_0 = 1, b_0 = 0$. Therefore $\{x_i\}$ takes the form (24).
- $[1, 0, 0, *]$: from (29) we know $x_i = 0, \forall i \geq 1$. This takes the form (26). (Here if * is not 0, the signature is not realizable)
- $[1, 0, 1, 0]$: from (29) we know $a_0 = 0, b_0 = 1$. Therefore $\{x_i\}$ takes the form (27).
- $[1, 0, 1, 1]$: from (29) we know $a_0 = 1, b_0 = 1$.But $x_4 = x_3 + x_2 = 2$, so this is not a BSS. (Here we assume the characteristic of the field is not 2).
- $[1, 1, 0, 0]$: from (29) we know $x_i = 0, \forall i \geq 2$. This takes the form (26).
- $[1, 1, 0, 1]$: from (29) we know $a_0 = -1, b_0 = 1$.But $x_4 = -x_3 + x_2 = -1$, so this is not a BSS. (Here we assume the characteristic of the field is not 2).
- $[1, 1, 1, *]$: from (29) we know $x_i = 1, \forall i$. This takes the form (24). (Here if * is not 1, the signature is not realizable)

□

Acknowledgments

We would like to thank Leslie Valiant for many comments and questions, particularly for pointing out a mistake in an earlier draft. We also thank Andrew Yao, and his group of students in Tsinghua University, while the first author visited Tsinghua and gave lectures.

References

[1] R. Bubley, and M. Dyer, Graph orientations with no sink and an approximation for a hard case of #SAT, ACM SODA , (1997) 248-257.

[2] Jin-Yi Cai, Vinay Choudhary. Valiant's Holant Theorem and Matchgate Tensors. In Proceedings of TAMC 2006. Lecture Notes in Computer Science vol. 3959. pp 248-261. Also available as ECCC TR05-118.

[3] Jin-Yi Cai, V. Choudhary. On the Theory of Matchgate Computations. *Submitted*. Also available as ECCC TR06-018.

[4] Jin-Yi Cai, V. Choudhary. Some Results on Matchgates and Holographic Algorithms. In Proceedings of ICALP 2006, Part I. Lecture Notes in Computer Science vol. 4051. pp 703-714. Springer.

[5] H.B. Hunt, M.V. Marathe, V. Radhakrishnan and R.E. Stearns. The complexity of planar counting problems. SIAM J. Comput. 27:4 (1998) 1142-1167.

[6] H. B. Hunt III and R. E. Stearns. The complexity of very simple Boolean formulas with applications. SIAM J. Comput., 19:1 (1990) 44-70.

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

[8] P. W. Kasteleyn. Graph Theory and Crystal Physics. In *Graph Theory and Theoretical Physics*, (F. Harary, ed.), Academic Press, London, 43-110 (1967).

[9] D. Lichtenstein, Planar formulae and their uses. SIAM J. on Computing 11 (1982) 329-343.

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

[11] H. N. V. Temperley and M. E. Fisher. Dimer problem in statistical mechanics – an exact result. *Philosophical Magazine* 6: 1061– 1063 (1961).

[12] L. G. Valiant. Quantum circuits that can be simulated classically in polynomial time. *SIAM Journal on Computing*, 31(4): 1229-1254 (2002).

[13] L. G. Valiant. Expressiveness of Matchgates. *Theoretical Computer Science*, 281(1): 457-471 (2002). See also 299: 795 (2003).

[14] L. G. Valiant. Holographic Algorithms (Extended Abstract). In *Proc. 45th IEEE Symposium on Foundations of Computer Science*, 2004, 306–315. A more detailed version appeared in Electronic Colloquium on Computational Complexity Report TR05-099.

[15] L. G. Valiant. Holographic circuits. In *Proc. 32nd International Colloquium on Automata, Languages and Programming*, 1–15, 2005.

[16] L. G. Valiant. Completeness for parity problems. In *Proc. 11th International Computing and Combinatorics Conference*, 2005.

[17] L. G. Valiant. Accidental Algorthims. To appear in FOCS 2006.

[18] L. G. Valiant. Private communication.

Proof of Theorem 2.2

Proof: Let $\boldsymbol{\beta} = [n, p] = \left[\begin{pmatrix} n_0 \\ n_1 \end{pmatrix}, \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}\right]$ be a linearly independent basis, for which a generator and a recognizer as stated in the theorem exist. The standard signature of the generator is $n \otimes n + p \otimes p = (n_0^2 + p_0^2, n_0 n_1 + p_1 p_0, n_0 n_1 + p_1 p_0, n_1^2 + p_1^2)$. Being defined by Perfect Matchings, there is the parity constraint. Either all the even entries of the standard signature are 0 or all the odd entries are 0.

$$n_0^2 + p_0^2 = 0, \tag{30}$$

$$n_1^2 + p_1^2 = 0; \tag{31}$$

or

$$n_0 n_1 + p_1 p_0 = 0. \tag{32}$$

Let M be the matrix $\begin{bmatrix} n_0 & p_0 \\ n_1 & p_1 \end{bmatrix}^{-1}$, by Proposition 4.3 from [14] we may assume the determinant of M is 1. Then $M = \begin{bmatrix} p_1 & -p_0 \\ -n_1 & n_0 \end{bmatrix}$. Denote by $a = p_1, b = -n_1, c = -p_0$ and $d = n_0$, we can write M simply as $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$. Equation (30), (31) and (32) translate to

$$c^2 + d^2 = 0, \tag{33}$$

$$a^2 + b^2 = 0; \tag{34}$$

or

$$ac + bd = 0. \tag{35}$$

We also have

$$ad - bc = 1. \tag{36}$$

The signature of the recognizer w.r.t. $\boldsymbol{\beta} = [n, p]$ is $u_{\boldsymbol{\beta}} = [0, 1, 1, 1]$, in symmetric form. So the standard signature u can be written as $u = u_{\boldsymbol{\beta}} M^{\otimes 3}$. It can be shown that the standard signature takes the symmetric form $u = [\sigma_0, \sigma_1, \sigma_2, \sigma_3]$, where

$$\sigma_i = (a + b)^{3-i}(c + d)^i - a^{3-i} c^i \tag{37}$$

for $0 \leq i \leq 3$. The parity conditions require that

$$\sigma_0 = \sigma_2 = 0, \tag{38}$$

or

$$\sigma_1 = \sigma_3 = 0. \tag{39}$$

Notice that after changing the positions of a with c, and b with d, (38) and (39) translate to each other, (33) and (34) translate to each other, (35) remains unchanged. Wolog. we need only consider case (38). We expand (38) as

$$(a + b)^3 - a^3 = 0, \tag{40}$$

$$(a + b)(c + d)^2 - ac^2 = 0. \tag{41}$$

First we assume $b = 0$. From (36), we get $ad = 1 \neq 0$. (41) translates to

$$2c + d = 0. \tag{42}$$

Back to the generator contraints, if (33) and (34) hold, from (34) we have $a = 0$, a contradiction. If (35) holds, we get $ac = 0$. Since $a \neq 0$, we get $c = 0$, and from (42) we get $d = 0$. This is also a contradiction.

So we get $b \neq 0$, and from (40) we know $a \neq 0$ and (40) is translated to

$$(a + b)^2 + a(a + b) + a^2 = 0. \tag{43}$$

Case (33)(34): From (34) (43) we get

$$2a + 3b = 0. \tag{44}$$

From (33) (41) we get

$$c(2ad + 2bd - ac) = 0. \tag{45}$$

Suppose $c = 0$, from (33) we get $d = 0$, a contradiction. So

$$2ad + 2bd - ac = 0. \tag{46}$$

From (44) (46) we get

$$ac + bd = 0. \tag{47}$$

Then the standard signature of the generator is $(0, 0, 0, 0)^{\mathrm{T}}$, a contradiction.

Case (35): $b \times (35) + a \times (36)$ we get

$$(a^2 + b^2)d = a. \tag{48}$$

Since $a \neq 0$, by (48) we have

$$a^2 + b^2 \neq 0. \tag{49}$$

and

$$d = \frac{a}{a^2 + b^2}, \tag{50}$$

$$c = \frac{-b}{a^2 + b^2}. \tag{51}$$

Substituting (50)(51) in (41), we get

$$(a + b)(a - b)^2 - ab^2 = 0. \tag{52}$$

We now assume, after scaling appropriately using Proposition 4.3 form [14], that $b = 1$. Substituting this to (43) (52) we get

$$3a^2 + 3a + 1 = 0, \tag{53}$$

$$a^3 - a^2 - 2a + 1 = 0. \tag{54}$$

$3 \times (54) + (53)$

$$3a^3 - 3a + 4 = 0. \tag{55}$$

$3 \times (54) + a \times (53)$

$$6a^3 - 5a + 3 = 0. \tag{56}$$

$(56) - 2 \times (55)$

$$a - 5 = 0. \tag{57}$$

We get $a = 5$, and substituting it in (53) we get $91 = 0$. Therefore the field $\mathbf{F}$ must have characteristic either 7 or 13. From (49) we get $a^2 + b^2 = 26 \neq 0$, so the characteristic is not 13. Now with the result of Theorem 2.1 we complete the proof.

□

Proof details of Theorem 3.1

Case 2: odd n and even matchgate
In this case, we have $\sigma_k = \lambda b^{n-1-k}c^k$, $\forall k$ even, and $\sigma_k = 0$,$\forall k$ odd. From (5) and (7) we get:

$$\sigma'_{k'} = \sum_{k=0}^{n} \sigma_k a_{k'}^k = \lambda \sum_{k\ even} b^{n-1-k}c^k a_{k'}^k. \tag{58}$$

If $b \neq 0$, let $\lambda' = \lambda/b$, we can have the similar calculation as Case 1 and get the following form:

$$\sigma'_{k'} = \frac{1}{2}\lambda'[(bt_0^0 + ct_0^1)^{n-k'}(bt_1^0 + ct_1^1)^{k'} + (bt_0^0 - ct_0^1)^{n-k'}(bt_1^0 - ct_1^1)^{k'}]. \tag{59}$$

Otherwise $b = 0$, then $\sigma_{n-1} = \lambda c^{n-1}$, and $\sigma_k = 0$, $\forall k \neq n-1$. In this subcase, let $\lambda' = \lambda c^{n-1} = \sigma_{n-1}$. The only non-zero term in (5) is when $k = n-1$ and further more the only non-zero terms in (6) are when $s = k'$ and $s = k'-1$:

$$\begin{aligned}
\sigma'_{k'} &= \sum_{k=0}^{n} \sigma_k a_{k'}^k \\
&= \sigma_{n-1} a_{k'}^{n-1} \\
&= \lambda'((n-k')(t_1^1)^{k'}(t_0^1)^{n-1-k'}t_0^0 + k'(t_1^1)^{k'-1}t_1^0(t_0^1)^{n-k'}).
\end{aligned}$$

Case 3: odd n and odd matchgate
In this case, we have $\sigma_k = \lambda b^{n-k}c^{k-1}$, $\forall k$ odd, and $\sigma_k = 0$, $\forall k$ even. From (5) and (7) we get:

$$\sigma'_{k'} = \sum_{k=0}^{n} \sigma_k a_{k'}^k = \lambda \sum_{k\ odd} b^{n-k}c^{k-1} a_{k'}^k. \tag{60}$$

If $c \neq 0$, let $\lambda' = \lambda/c$, we can have the similar calculation as in Case 1 and get the following form:

$$\sigma'_{k'} = \frac{1}{2}\lambda'[(bt_0^0 + ct_0^1)^{n-k'}(bt_1^0 + ct_1^1)^{k'} - (bt_0^0 - ct_0^1)^{n-k'}(bt_1^0 - ct_1^1)^{k'}]. \tag{61}$$

Otherwise $c = 0$, then $\sigma_1 = \lambda b^{n-1}$, and $\sigma_k = 0$, $\forall k \neq 1$. In this subcase, let $\lambda' = \lambda b^{n-1} = \sigma_1$. The only non-zero term in (5) is when $k = 1$ and further more the only non-zero terms in (6) are when $s = 0$ and $s = 1$:

$$\begin{aligned}
\sigma'_{k'} &= \sum_{k=0}^{n} \sigma_k a_{k'}^k \\
&= \sigma_1 a_{k'}^1 \\
&= \lambda'((n-k')(t_1^0)^{k'}t_0^1(t_0^0)^{n-1-k'} + k't_1^1(t_1^0)^{k'-1}(t_0^0)^{n-k'})
\end{aligned}$$

Case 4: even n and odd matchgate
In this case, we have $\sigma_k = \lambda b^{n-k-1}c^{k-1}$, $\forall k$ odd, and $\sigma_k = 0$, $\forall k$ even. From (5) and (7) we get:

$$\sigma'_{k'} = \sum_{k=0}^{n} \sigma_k a_{k'}^k = \lambda \sum_{k\ odd} b^{n-k-1}c^{k-1} a_{k'}^k. \tag{62}$$

If $bc \neq 0$, let $\lambda' = \lambda/(bc)$, we can have the similar calculation as Case 1 and get the following form:

$$\sigma'_{k'} = \frac{1}{2}\lambda'[(bt_0^0 + ct_0^1)^{n-k'}(bt_1^0 + ct_1^1)^{k'} - (bt_0^0 - ct_0^1)^{n-k'}(bt_1^0 - ct_1^1)^{k'}]. \tag{63}$$

Otherwise if $b = 0$, similar with Case 2, we have

$$\sigma'_{k'} = \lambda'((n-k')(t_1^1)^{k'}(t_0^1)^{n-1-k'}t_0^0 + k'(t_1^1)^{k'-1}t_1^0(t_0^1)^{n-k'}). \tag{64}$$

If $c = 0$, similar with Case 3,we have

$$\sigma'_{k'} = \lambda'((n-k')(t_1^0)^{k'}t_0^1(t_0^0)^{n-1-k'} + k't_1^1(t_1^0)^{k'-1}(t_0^0)^{n-k'}). \tag{65}$$