Holographic Reduction: A Domain Changed Application and its Partial Converse Theorems

Mingji Xia

(State Key Laboratory of Computer Science, Institute of Software, the Chinese Academy of Sciences, Beijing 100190, China)

Abstract   Holographic reductions between some Holant problems and some $\#\mathrm{CSP}(H_d)$ problems are built, where H_d is some complex value binary function. By the complexity of these Holant problems, for each integer $d \geq 2$, $\#\mathrm{CSP}(H_d)$ is in P when each variable appears at most d times, while it is $\#$P-hard when each variables appears at most $d+1$ times. $\#\mathrm{CSP}(H_d)$ counts weighted summation of graph homomorphisms from input graph G to graph H_d, and the maximum occurrence of variables is the maximum degree of G.

We conjecture that the converse of holographic reduction holds for most of $\#$Bi-restriction Constraint Satisfaction Problems, which can be regarded as a generalization of a known result about counting graph homomorphisms. It is shown that the converse of holographic reduction holds for some classes of problems.

Key words: holographic reduction; graph homomorphism; holant problem; $\#$CSP; $\#$BCSP

1   Introduction

Class $\#$P is proposed by Valiant for which the permanent is $\#$P-hard[19]. An important kind of complexity results about counting problems in $\#$P is dichotomy theorem, which claims that all problems in a class is either polynomial computable or $\#$P-hard. There are dichotomy theorems for $\#\mathrm{CSP}$[2,3,10,12,14], counting graph homomorphisms[1,8,16], and Holant problems[10−11]. Most studied $\#$CSP problems and Holant problems have domain size 2. Except Ref. [15], most studied counting graph homomorphisms problems have arbitrary domain size, and they are $\#$CSP problem defined by one binary function, if we allow self-loop and multi-edge in input graphs. Holant problem is a restricted version of $\#$CSP, such that each variable occurs twice, but this restriction makes it a more general problem class than $\#$CSP.

In this paper, we construct a series of complex value binary symmetric functions H_d, $d = 2, 3, \ldots$. For each integer $d \geq 2$, if permitting a variable occurring $d+1$ times

instead of d times, a polynomial computable $\#\mathrm{CSP}(H_d)$ problem becomes $\#$P-hard. In the language of counting graph homomorphisms, for each integer $d > 2$, there exists a complex weighted undirected graph H_d, such that counting the summation of the weights of all homomorphisms from input graph G to H_d is $\#$P-hard, when the maximum degree of G is restricted to $d + 1$, but it has polynomial time algorithm, when the maximum degree is restricted to d. By the notation $\#\mathbf{F}|\mathbf{H}$ of $\#$Bi-restriction Constraint Satisfaction Problem, for each integer $d \geq 2$, $\#\{H_d\}|\{=_1, =_2, \ldots, =_d\}$ is polynomial time computable, while $\#\{H_d\}|\{=_1, =_2, \ldots, =_{d+1}\}$ is $\#$P-hard, where $=_k$ denotes the equivalence relation of arity k.

It is well known that $\#$SAT and $\#$2SAT are $\#$P-hard. There are many other $\#$P-hard results of maximum degree bounded counting problems in Ref. [18]. There are two general results about maximum degree and complexity for a class of problems. In Ref. [16], it is proved that if $\#\mathrm{CSP}(H)$ is hard, then there exist some constant C (maybe depends on H), such that it is still hard when the maximum degree of input graph G is restricted to C, where H is a 0-1 weighted undirected graph. That is, H is a binary function from $[n]^2$ to $\{0, 1\}$ or rational numbers, where n is the number of vertices in H. In our result, the range of H_d is the field of complex numbers, and we do not know whether it can be strengthened to $\{0, 1\}$. In Ref. [10], it is proved for complexity weighted Boolean $\#$CSP, if $\#\mathrm{CSP}(\mathbf{F})$ is hard, then it is also hard, when each variables appears at most 3 times ($\#\mathbf{F}|\{=_1, =_2, =_3\}$). In Boolean $\#$CSP, each variable takes value from Boolean domain $\{0, 1\}$, so our result does not hold for Boolean domain. In our result, the domain of H_d is very large, depending on the construction and d. Our result shows, in a large class of counting problems, the relationship of maximum degree and complexity is quite complicated.

This result is proved mainly by holographic reduction from some Boolean domain Holant problems. Holographic reduction is proposed by Valiant in his senior paper holographic algorithms[21]. There have been lots of studies of holographic reduction[4−7,22−24], including designing algorithms on planar graphs, and characterization of matchgates under holographic reduction, and proving $\#$P-hardness, etc. Here the holographic reduction is between two problems of different domains. There are not many this kind of applications. The first example is the holographic algorithm for PL-FO-2-COLOR problem[21]. Its role is not very clear, although there is characterization for matchgates case[5].

We also study the converse of holographic reduction. It is an algebra problem, asking whether the sufficient condition in holographic reduction is also a necessary condition. We conjecture it holds, since it is a generalization of a known result about graph homomorphisms[13,17], and we prove that it holds for some classes of Holant problems.

In section 2, we introduce definitions and holographic reduction. In section 3, we prove the result about maximum degree and complexity. In section 4, we prove the converse of holographic reduction holds for some classes of Holant problems.

2 Preliminary

Let $[n]$ denote the set $\{0, 1, \ldots, n-1\}$. $[f_0, f_1, \ldots, f_k]$ denotes a symmetric function F over $[2]^k$, such that f_i is the value of F on the inputs of Hamming weight i. The value table of a function F over $[n]^k$ can be written as a column vector $F = (F_{x_1 x_2 \cdots x_k})$

or a row vector $F' = (F_{x_1 x_2 \cdots x_k})'$ of length n^k, where $F_{x_1 x_2 \cdots x_k} = F(x_1, x_2, \ldots, x_k)$. We also look a row or column vector of length n^k as a function in the same way. A binary function $F(x, y)$ can also be written as a matrix $(T_{x,y})$, where $T_{x,y} = F(x, y)$, and this matrix is denoted by $\widehat{F}$.

Let $=_k$ denote the equivalence relation in k variables. For example, $=_1$ is $[1, 1]$, and $=_2$ is $[1, 0, 1]$, when variables are in domain $[2]$. Let $\mathbf{R}_{=}^{\mathbf{d}}$ denote the set $\{=_1, =_2, \ldots, =_d\}$, and $\mathbf{R}_{=}$ denote the set of all equivalence relations.

Define a general counting problem $\#\mathbf{F}|\mathbf{H}$, named #Bi-restriction Constraint Satisfaction Problem. $\mathbf{F}$ and $\mathbf{H}$ are two sets of functions in variables of domain $[n]$.

An instance (G, ϕ_l, ϕ_r) of this problem is a bipartite graph $G(U, V, E)$, and two mappings, $\phi_l : v \in U \rightarrow F_v \in \mathbf{F}$ and $\phi_r : v \in V \rightarrow F_v \in \mathbf{H}$ (using F_v to denote the value of ϕ_l or ϕ_r on v), satisfying the arity of F_v is d_v, the degree of v. The bipartite graph G is given as two one to one mappings, $\phi_1 : (v, i) \rightarrow e$ and $\phi_2 : (u, i) \rightarrow e$, where $v \in V$ and $u \in U$ respectively, $i \in [d_v]$ (or $[d_u]$), and $e \in E$ is one of the edges incident to v (or u). Let $e_{v,i} = \phi_s(v, i)$, $v \in U \cup V$, $s = 1, 2$.

In such an instance, edges are looked as variables with domain $[n]$. Vertex v is looked as function F_v (specified by ϕ_l or ϕ_r) in its edges, and $e_{v,i}$ specifies which edge of v is the ith input of F_v.

The value on this instance is defined as a summation over all $[n]$ valued assignments σ of edges,

$$\#\mathbf{F}|\mathbf{H}(G, \phi_l, \phi_r) = \sum_{\sigma : E \rightarrow [n]} \prod_{v \in U \cup V} F_v(\sigma(e_{v,1}), \sigma(e_{v,2}), \ldots, \sigma(e_{v,d_v})).$$

Suppose p is a nonzero constant. If $F \in \mathbf{F}$ is replaced by pF, then the value of $\#\mathbf{F}|\mathbf{H}$ is simply multiplied by a power of p. Since p does not affect the computational complexity of $\#\mathbf{F}|\mathbf{H}$, we usually ignore it. $\#\mathbf{F}|\{=_2\}$ is also called Holant($\mathbf{F}$) problem in Ref. [10]. $\#\mathbf{F}|\mathbf{R}_{=}$ is #CSP($\mathbf{F}$), equivalent to Holant($\mathbf{F} \cup \mathbf{R}_{=}$).

We say two problems $\#\mathbf{F}|\mathbf{H}$ and $\#\mathbf{P}|\mathbf{Q}$ are *result equivalent*, if there are two bijections $\sigma_l : \mathbf{F} \rightarrow \mathbf{P}$ and $\sigma_r : \mathbf{H} \rightarrow \mathbf{Q}$, such that for any instance (G, ϕ_l, ϕ_r),

$$\#\mathbf{F}|\mathbf{H}(G, \phi_l, \phi_r) = \#\mathbf{P}|\mathbf{Q}(G, \sigma_l \circ \phi_l, \sigma_r \circ \phi_r).$$

Use $\otimes$ to denote tensor product. Suppose A and B are two matrices, and $A = (a_{ij})$ has size $k \times m$.

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1m}B \\ a_{21}B & a_{22}B & \ldots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1}B & a_{k2}B & \ldots & a_{km}B \end{pmatrix}.$$

$A^{\otimes r}$ denotes the tensor product of r matrices, that is, $A^{\otimes 1} = A$ and $A^{\otimes(r+1)} = A^{\otimes r} \otimes A$. If $A = (A_1, \ldots, A_m)$, that is, the ith column of A is A_i, then the $i_1 i_2 \cdots i_r$ column of $A^{\otimes r}$ is $A_{i_1} \otimes \cdots \otimes A_{i_r}$ by definition.

Suppose F is a binary function, then $A^{\otimes 2}F$ and $A\widehat{F}A'$ are the column vector form and matrix form of the same function.

We say two problems $\#\mathbf{F}|\mathbf{H}$ and $\#\mathbf{P}|\mathbf{Q}$ are *algebra equivalent*, if there exist a nonsingular matrix M, and two bijections $\sigma_l : \mathbf{F} \to \mathbf{P}$ and $\sigma_r : \mathbf{H} \to \mathbf{Q}$, such that for any function $F \in \mathbf{F}$ and $H \in \mathbf{H}$,

$$\sigma_l(F)' = F' \, M^{\otimes R_F}, \quad \sigma_r(H) = (M^{-1})^{\otimes R_H} \, H,$$

where R_F (resp. R_H) denotes the arity of F (resp. H).

Both result equivalent and algebra equivalent are equivalence relations.

Theorem 2.1.[21]   If $\#\mathbf{F}|\mathbf{H}$ and $\#\mathbf{P}|\mathbf{Q}$ are algebra equivalent, then they are result equivalent under the same bijections σ_l and σ_r.

By this theorem, if $\#\mathbf{F}|\mathbf{H}$ and $\#\mathbf{P}|\mathbf{Q}$ are algebra equivalent, we can reduce one to the other. This kind of reduction is called holographic reduction. The matrix M in the algebra equivalent is called the base of holographic reduction. There is another form of this theorem, which is convenient for domain size changed applications.

Theorem 2.2.[21]   Suppose F is a function over $[m]^s$, and H is a function over $[n]^t$, and M is an $m \times n$ matrix. Problems $\#\{F'\}|\{M^{\otimes t}H\}$ and $\#\{F'M^{\otimes s}\}|\{H\}$ are result equivalent.

This theorem also holds for general function sets like Theorem 2.1.

3 An Application

Let $\{a_i\}$ be Fibonacci sequence, that is, $a_0 = 0$, $a_1 = 1$, $a_{i+2} = a_{i+1} + a_i$, and let d be an integer no less than 2. Let $F_i = [a_0, a_1, \ldots, a_i]$, $i = 1, 2, \ldots, d$, $F_{d+1} = [a_0, a_1, \ldots, a_d, -2a_d]$.

We need some complexity results for Holant problems. One is that $\#\{=_2\}|\{F_1, \ldots, F_d\}$ is polynomial time computable[9,10]. The other is the following hardness lemma, which is not a straightforward corollary of the dichotomy theorems for Holant^C and Holant* in Ref. [10].

Lemma 3.1.   For any integer $d \geq 2$, $\#\{=_2\}|\{F_1, \ldots, F_{d+1}\}$ is $\#$P-hard.

Proof: We will reduce the problems in the following list to the problem before it.

$$\#\{F_1, \ldots, F_{d+1}\}|\{=_2\}$$
$$\#\{F_1, P, F_3\}|\{=_2\}$$
$$\#\{F_1, F_3\}|\{P\}$$
$$\#\{=_1, =_3\}|\{Q\}$$
$$\#\{=_1, =_2, =_3\}|\{Q\}$$
$$\#\{=_1, =_2, =_3\}|\{Q, =_2\}$$
$$\#\mathbf{R}_=|\{Q\}$$

In the first reduction, the binary function $P = [a_{d-1}, a_d, -2a_d]$ is constructed directly by connecting $d-1$ functions $F_1 = [0, 1]$ to F_{d+1}.

The second reduction is simply because $\#\mathbf{F}|\mathbf{F}$ is a restricted version of $\#\mathbf{F}|\{=_2\}$.

The third reduction is holographic reduction by the base $M = \begin{pmatrix} 1 & -1 \\ \frac{1+\sqrt{5}}{2} & \frac{-1+\sqrt{5}}{2} \end{pmatrix}$.

$Q = \begin{pmatrix} 2a_d - a_{d-1} & 5a_d + a_{d-1} \\ 5a_d + a_{d-1} & 2a_d - a_{d-1} \end{pmatrix}$, ignoring a constant factor.

In the fourth reduction, $=_2$ is constructed by connecting unary function $\widehat{Q} =_1$ to $=_3$, where $\widehat{Q} =_1$ is constructed by connecting $=_1$ to Q.

In the fifth reduction, we can apply the interpolation reduction method in Ref.[16] to realize right side $=_2$, by using Q^s, $s = 1, 2, \ldots, \text{poly(n)}$, to interpolate on the eigenvalues.

In the last reduction, $r - 2$ functions $=_3$ are connected by right side $=_2$ to realize left side $=_r$.

All entries in $\widehat{Q}$ are nonzero, and $\widehat{Q}$ is nonsingular, by result in Ref. [1], $\#\mathbf{R}_=|\{Q\}$ is #P-hard. $\qquad\square$

Theorem 3.1. For any integer $d \geq 2$, there exists a complex valued symmetric binary function H_d, such that $\#\{H_d\}|\mathbf{R}_=^{\mathbf{d}}$ has polynomial time algorithm, but $\#\{H_d\}|\mathbf{R}_=^{\mathbf{d+1}}$ is #P-hard.

Proof: We construct a holographic reduction between $\#\{=_2\}|\{F_1, \ldots, F_{d+1}\}$ and $\#\{H_d\}|\{=_1, \ldots, =_{d+1}\}$. Let $k = d + 1$.

The first problem is in domain $[2]$, and the second problem is in domain $[m]$. The value of m will be determinated later in the construction.

We construct a matrix M of size $2 \times m$, such that for any $1 \leqslant i \leqslant k$,

$$M^{\otimes i}(=_i) = F_i. \tag{3.1}$$

Recall that $=_i$ and F_i denote the column vectors of length m^i and 2^i corresponding to the two functions.

Suppose there are c_j columns with the same value $\begin{pmatrix} b_j \\ b_j q_j \end{pmatrix}$ in M temporarily, $0 \leqslant j \leqslant k$. We have $M^{\otimes i}(=_i) = \sum_{j=0}^{k} c_j \begin{pmatrix} b_j \\ b_j q_j \end{pmatrix}^{\otimes i}$, because the $s_1 s_2 \cdots s_i$ columns of $M^{\otimes i}$ is $M_{s_1} \otimes \cdots \otimes M_{s_i}$ (M_s denotes the sth column of M), and the vector $=_i$ is nonzero only on entries $s_1 s_2 \cdots s_i$ satisfying $s_1 = s_2 = \cdots = s_i$.

We need that $\sum_{j=0}^{k} c_j \begin{pmatrix} b_j \\ b_j q_j \end{pmatrix}^{\otimes i} = F_i$. Notice that both sides of the equation are symmetric functions. We need $\sum_{j=0}^{k} c_j b_j^i [1, q_j, \ldots, q_j^i] = [a_0, a_1, \ldots, a_i]$ holds for $1 \leqslant i \leqslant k$. Let $b_j = 1$, we only need $\sum_{j=0}^{k} c_j q_j^i = a_i$. Let q_j are different integers. Then, this is a system of linear equations in c_j with nonsingular Vandermonde coefficient matrix in q_j. Because q_j and a_i are integers, the solution of c_j are rational.

We look at two simple cases firstly. If the solution of c_j are all nonnegative integers, it is done. If the solution of c_j are nonnegative rational numbers. Suppose p is a constant such that pc_j are nonnegative integers. Put pc_j columns $\begin{pmatrix} b_j \\ b_j q_j \end{pmatrix}$ in M. We get $M^{\otimes i}(=_i) = pF_i$. (The constant p does not change the complexity of the corresponding problem.)

In the general case, the solution of c_j may be negative rational. In fact we only need to show how to utilize b_j to realize a factor -1. Suppose we want some column $\begin{pmatrix} b \\ bq \end{pmatrix}$ in M contribute $-1 \begin{pmatrix} 1 \\ q \end{pmatrix}^{\otimes i}$ in $M^{\otimes i}(=_i) = \sum_{j=0}^{k} c_j \begin{pmatrix} b_j \\ b_j q_j \end{pmatrix}^{\otimes i}$ for

$1 \leqslant i \leqslant k$.

Let $r = e^{i2\pi/(k+1)}$. Replace this column $\begin{pmatrix} b \\ bq \end{pmatrix}$ by k columns $\begin{pmatrix} b_s \\ b_s q \end{pmatrix}$, $1 \leqslant s \leqslant k$, where $b_s = r^s$. Notice

$$\sum_{s=1}^{k} b_s^i = \sum_{s=1}^{s} r^{si} = \sum_{s=0}^{k} r^{si} - 1 = \frac{1 - r^{i(k+1)}}{1 - r^i} - 1 = -1,$$

for all $1 \leqslant i \leqslant k$. These k columns indeed contribute $-1 \begin{pmatrix} 1 \\ q \end{pmatrix}^{\otimes i}$.

Suppose we get the solution of c_j from the system of linear equations. Firstly, we only take the absolute values of this solution, and handle it as the second simple case to get a matrix M. Secondly, for each c_j which should take a negative value, we replace each of its pc_j columns in M by k new columns as above to get a new M satisfying equations 3.1.

By Theorem 2.2, let $H_d = (=_2)M^{\otimes 2}$, then $\#\{=_2\}|\{F_1,\ldots,F_{d+1}\}$ and $\#\{H_d\}|\mathbf{R}_{\underline{=}}^{\mathbf{d+1}}$ have the same value. Obviously, the same holographic reduction exists between $\#\{=_2\}|\{F_1,\ldots,F_d\}$ and $\#\{H_d\}|\mathbf{R}_{\underline{=}}^{\mathbf{d}}$.

By the results in Ref. [10], we know that $\#\{=_2\}|\{F_1,\ldots,F_d\}$ is in P, while $\#\{=_2\}|\{F_1,\ldots,F_{d+1}\}$ is #P-hard by lemma 3.1.

The conclusion follows from the complexity of $\#\{=_2\}|\{F_1,\ldots,F_d\}$ and $\#\{=_2\}|\{F_1,\ldots,F_{d+1}\}$.   □

4   Some Partial Converse of Holographic Reduction

Since result equivalent is enough to design reductions, and algebra equivalent is a sufficient condition of result equivalent, we wonder whether it is also a necessary condition. If it is not, maybe we can explore more sufficient conditions to design new reductions. This question itself is also an interesting mathematical problem.

The converse of Theorem 2.1 does not hold for some cases. For example $\#\{F_1 = F_2 = (1,0)\}|\{(4,1)'\}$ and $\#\{W_1 = (1,1), W_2 = (1,2)\}|\{(4,0)'\}$ always have the same value, but obviously there is no nonsingular M such that $F_1 = W_1 M$ and $F_2 = W_2 M$.

Unfortunately, the converse of Theorem 2.2 does not hold neither. Consider $\#\{F_1 = F_2 = (1,0), F_3 = (1,4)\}|\{(4,1)'\}$ and $\#\{W_1 = (1,1), W_2 = (1,2), W_3 = (2,0)\}|\{(4,0)'\}$. They always give the same value. Suppose the converse of Holant theorem holds, then it must be that $F_1 = W_1 M$ and $F_2 = W_2 M$, so the second column of M is a zero vector. Because $F_3 = W_3 M$, the second entry of F_3 should be zero. Contradiction.

It is still possible that the converse of the two theorems holds for most situation except for some special cases. In the following conjecture, we simply add a condition on the arity, but maybe this is far from the right condition.

Conjecture 4.1. $\#\mathbf{F}|\mathbf{H}$ and $\#\mathbf{P}|\mathbf{Q}$ are two counting problems, such that at least one of $\mathbf{F}$, $\mathbf{H}$, $\mathbf{P}$, $\mathbf{Q}$ contains some function of arity more than 1. If they are result equivalent, then they are algebra equivalent.

We compare this conjecture with the following result. (The result in Ref.[17] is more general.)

Theorem 4.1.[13,17]   Suppose H_1 and H_2 are directed acyclic graphs. If for all directed acyclic graphs G, the number of homomorphisms from G to H_1 is equal to the number of homomorphisms from G to H_2, then H_1 and H_2 are isomorphic.

Theorem 4.1 can be regarded as a special case of the conjecture that $\mathbf{H} = \mathbf{Q} = \mathbf{R}_=$, and $\mathbf{F} = \{H_1\}$, $\mathbf{P} = \{H_2\}$, with stronger conclusion that the matrix M in algebra equivalent is a permutation matrix.

Now we prove that if there is a matrix M keeping $=_k$ unchanged for all airty k, then it must be permutation matrix.

Suppose $M = (M_{ij})$ is an $n \times n$ matrix. Let M_j denote the jth column of M, and e_j denote the standard column base vector. e_{ij} denotes the ith entry of e_j, that is, (e_{ij}) is identity matrix. We have condition $M^{\otimes k}(=_k) = (=_k)$, which means $\sum_{j=1}^n M_j^{\otimes k} = \sum_{j=1}^n e_j^{\otimes k}$, $1 \leqslant k \leqslant n$. Fix an i and focus on the $(ii \cdots i)$th entry of these vector equations. We get $\sum_{j=1}^n M_{ij}^k = \sum_{j=1}^n e_{ij}^k$, $1 \leqslant k \leqslant n$. This means $\{M_{ij} | 1 \leqslant j \leqslant n\}$ and $\{e_{ij} | 1 \leqslant j \leqslant n\}$ are the same multi-set, that is, each row of M is composed of 1 one and $n-1$ zeros. Suppose one column of M contains more than one 1. For example $M_{sj} = M_{tj} = 1$. Consider the $(ii \cdots ij)$th entry of these vector equations, we will get a contradiction. Hence, M is a permutation matrix.

In the rest of this paper, we prove that the conjecture holds for several classes of problems $\#\mathbf{F}|\{=_2\}$ (Holant problems). We denote this problem by $\#\mathbf{F}$ for simplicity. The range of all functions are real numbers.

Since we only consider $\#\mathbf{F}|\{=_2\}$ problems, the base M keep $=_2$ unchanged, that is, $M^{\otimes 2}(=_2) = (=_2)$. The matrix corresponds to $=_2$ is identity matrix I, so the matrix form of this equation is $MIM' = I$, which means M is orthogonal.

Theorem 4.2.   Suppose $\mathbf{F} = \{F_1, \ldots, F_t\}$ and $\mathbf{P} = \{P_1, \ldots, P_t\}$ are composed of unary functions over $[n]$. If $\#\mathbf{F}$ and $\#\mathbf{P}$ are result equivalent, then they are algebra equivalent.

Proof: This a straightforward linear algebra problem.

Let F (resp. P) denote the matrix whose ith column is F_i (resp. P_i). The condition is that $F'F = P'P$.

If $t = n$ and F is full rank, then P is also full rank. Let $M = HF^{-1}$. Obviously, $MF_i = H_i$. Because $F'F = H'H = F'M'MF$, M is orthogonal matrix.

For the general case, we can show F and P has the same maximum linear independent column subset (two subset have the same element index) and the other columns are generated by this set in the same way. We can turn them into nonsingular matrices. Details omitted.   □

Theorem 4.3.   Suppose F and H are two symmetric binary real functions over $[n]^2$. If $\#\{F\}$ and $\#\{H\}$ are result equivalent, then they are algebra equivalent.

Proof: Suppose KFK' and LHL' are diagonal matrices and K, L are orthogonal matrices.

$\#\{F\}$ and $\#\{KFK'\}$, $\#\{H\}$ and $\#\{LHL'\}$ are algebra equivalent. We only need to prove that $\#\{KFK'\}$ and $\#\{KHK'\}$ are algebra equivalent.

Consider a cycle of length i. Since $\#\{KFK'\}$ and $\#\{LHL'\}$ have the same value on it, $\mathrm{tr}((KFK')^i) = \mathrm{tr}((LHL')^i)$.

Take $i = 1, \ldots, n$, we get that the diagonal entries sets of KFK' and LHL' are the same. Hence, $\#\{KFK'\}$ and $\#\{LHL'\}$ are algebra equivalent under a permutation matrix.   □

Corollary 4.1.   Suppose F_1, F_2, H_1, H_2 are symmetric binary real functions over $[k]^2$, and all eigenvalues of F_1 are equal. If $\#\{F_1, F_2\}$ and $\#\{H_1, H_2\}$ are result equivalent, then they are algebra equivalent.

Proof: By Theorem 4.3, the eigenvalues of H_1 are also equal. If these eigenvalues are zero, then F_1 and H_1 are zero function. The conclusion holds by Theorem 4.3.

If these eigenvalues λ are not zero, $\#\{F_1, F_2\}$ (resp. $\#\{H_1, H_2\}$) is algebra equivalent to $\#\{\lambda I, P_2\}$ (resp. $\#\{\lambda I, Q_2\}$). By Theorem 4.3, $\#\{\lambda I, P_2\}$ and $\#\{\lambda I, Q_2\}$ are algebra equivalent.   □

We need the following lemma for the next theorem.

Lemma 4.1. $G = (U, V, E)$ is a bipartite graph with edge weight function $w : E \to \{1, -1\}$. If for every cycles $e_1, e_2, \ldots, e_{2k}$ of G, $w(e_1)w(e_2) \cdots w(e_{2k}) = 1$, we say G is consistent. If G is consistent, then we can extend weight function w to a complete bipartite graph $G' = (U, V, U \times V)$, such that G' is also consistent.

Proof: Given $G = (U, V, E)$, we take a spanning tree of each of its connected components. We get a forest and denote it by $G_1 = (U, V, E_1)$. Edges in E_1 take the same weight as in G. Extend G_1 to a spanning tree $G_2 = (U, V, E_2)$, that is, $E_1 \subseteq E_2$, such that the weights of edges in $E_2 - E$ are either 1 or -1 arbitrarily. At last, we extend G_2 to complete graph G'. For each edge $(u, v) \notin E_2$, there is a unique path $P_{u,v}$ in G_2 connecting u and v. We set the weight of (u, v) to the product of weights of edges in $P_{u,v}$.

Firstly, we prove that G' is consistent. Take an arbitrary cycle C' of G'. For each edge e in C', there is a unique path P_e corresponding to it in the spanning tree G_2. We replace each edge e in C by its path P_e to get a cycle C_2 of G_2. By the definition of weights of G', the two cycles have the same product of edge weights. Each edge appears in C_2 for even many times. (Otherwise, if C_2 contains some edge e for odd many times, the cycle will start from one of the two components of the graph $(U, V, E_2 - \{e\})$ and stay in the other component.) Hence the products of edge weights are 1 for both cycles C and C'.

Secondly, we prove that G' and G give the same weight to edges in E. We prove it for all edges in each connected component of G. To reuse the notations above, we can assume that G is connected. By definition, G' and G give the same weight to edges in E_1. Because both G' and G are consistent, and the weight of $e = (u, v) \notin E_1$ is decided by the weights on the path $P_{u,v} \subseteq E_1$, they give the same weight to e.   □

Theorem 4.4.   Suppose F_1, F_2, H_1, H_2 are symmetric binary real functions over $[k]^2$, and all eigenvalues of F_1 are different and all eigenvalues of F_2 are different. If $\#\{F_1, F_2\}$ and $\#\{H_1, H_2\}$ are result equivalent, then they are algebra equivalent.

Proof: By Theorem 4.3, there exist orthogonal matrices K_1, L_1 and diagonal matrix Λ_1 such that $F_1 = K_1' \Lambda_1 K_1$, $H_1 = L_1' \Lambda_1 L_1$. Because $\#\{F_1, F_2\}$ and $\#\{\Lambda_1, K_1 F_2 K_1'\}$, $\#\{H_1, H_2\}$ and $\#\{\Lambda_1, L_1 H_2 L_1'\}$, are algebra equivalent, $\#\{\Lambda_1, K_1 F_2 K_1'\}$ and $\#\{\Lambda_1, L_1 H_2 L_1'\}$ are result equivalent.

To prove the conclusion, we only need to prove $\#\{\Lambda_1, K_1 F_2 K_1'\}$ and $\#\{\Lambda_1, L_1 H_2 L_1'\}$ are algebra equivalent. We use F (resp. H) to denote $K_1 F_2 K_1'$ (resp. $L_1 H_2 L_1'$).

Applying Theorem 4.3 to $\#\{F\}$ and $\#\{H\}$, there exist orthogonal matrices K, L and diagonal matrix Λ such that $F = K \Lambda K'$, $H = L \Lambda L'$. The diagonal entries of Λ are different eigenvalues.

Let σ_i denote the binary relation $\{(i,i)\}$, $i \in [n]$. Consider a circle of $r + s$ with r functions Λ_1 and s functions F. The value of $\#\{\Lambda_1, F\}$ on this instance is $tr(\Lambda_1^r F^s) = tr(\Lambda_1^r K \Lambda^s K')$. This equation holds for any r and s. Suppose the ith diagonal entry of Λ_1 is λ_i. $tr(\Lambda_1^r K \Lambda^s K') = \Sigma_i \lambda_i^r tr(\sigma_i K \Lambda^s K')$. Fix s and take n different values of r. We get a nonsingular system of linear equations in $tr(\sigma_i K \Lambda^s K')$, with Vandermonde coefficient matrix in λ_i.

Similar analysis also holds for $tr(\Lambda_1^r L \Lambda^s L')$. By the conditions $tr(\Lambda_1^r F^s) = tr(\Lambda_1^r H^s)$. Two systems of linear equations are the same, so if $\lambda_i \neq 0$, $tr(\sigma_i K \Lambda^s K') = tr(\sigma_i L \Lambda^s L')$. If there is some unique $\lambda_{i_0} = 0$, notice $tr((\Sigma_{i \in [n]} \sigma_i) K \Lambda^s K') = tr(=_2 K \Lambda^s K') = tr(L \Lambda^s L') = tr((\Sigma_{i \in [n]} \sigma_i) L \Lambda^s L')$, we also have $tr(\sigma_{i_0} K \Lambda^s K') = tr(\sigma_{i_0} L \Lambda^s L')$.

Similar analysis holds for Λ part. Hence, for any i, j, $tr(\sigma_i K \sigma_j K') = tr(\sigma_i L \sigma_j L')$, which means $(K(i,j))^2 = (L(i,j))^2$.

Define a weighted undirected bipartite graph $G = (U, V, E)$, such that $(i,j) \in E$ iff $L(i,j) \neq 0$. The weight of (i,j) is $w((i,j)) = K(i,j)/L(i,j) \in \{1, -1\}$.

We just consider $\Lambda_1^r F^s$ in the above analysis. If consider $\Lambda_1^{r_1} F^{r_2} \Lambda_1^{r_3} F^{r_4}$, we can get for any $i, j, k, l \in [n]$, $tr(\sigma_i K \sigma_j K' \sigma_k K \sigma_l K') = tr(\sigma_i L \sigma_j L' \sigma_k L \sigma_l L')$, which means $K(i,j)K(k,j)K(k,l)K(i,l) = L(i,j)L(k,j)L(k,l)L(i,l)$. If none of them is zero, $((i,j),(k,j),(k,l),(i,l))$ is a cycle in G, and the equation says G is consistent on this cycle (the product of edge weights in the cycle is 1). If we consider arbitrary alternations between Λ and F, we get arbitrary cycles, so G is consistent. By lemma 4.1, we can get a consistent complete bipartite graph G'. Suppose the weight function of G' is $W(i,j)$, which is also a matrix.

For any 2×2 submatrix $W(\{i,k\}, \{j,l\})$ of W, its two rows are identical or linear dependent by a factor -1 (consider the circle $((i,j),(k,j),(k,l),(i,l))$ in G'). Hence the rank of W is 1.

Suppose W is the product of two ± 1 valued vectors $\delta_1 \delta_2'$. Let $\text{diag}(\delta_i)$ denote the diagonal matrix whose diagonal is δ_i. Since $W(i,j)L(i,j) = K(i,j)$ for all entries, $\text{diag}(\delta_1) \, L \, \text{diag}(\delta_2) = K$. Notice $\text{diag}(\delta_1) \, \Lambda_1 \, \text{diag}(\delta_1) = \Lambda_1$ and $\text{diag}(\delta_2) \, \Lambda \, \text{diag}(\delta_2) = \Lambda$. $\#\{\Lambda_1, F\}$ and $\#\{\Lambda_1, H\}$ are algebra equivalent by matrix $\text{diag}(\delta_1)$. $\square$

Corollary 4.2.   Suppose F_1, F_2, H_1, H_2 are symmetric binary real functions over $[2]^2$. If $\#\{F_1, F_2\}$ and $\#\{H_1, H_2\}$ are result equivalent, then they are algebra equivalent.

Proof: Since the size of domain is 2, either one of F_1 and F_2 have the same eigenvalues, or neither of them has.

The first case is by corollary 4.1, the second case is by Theorem 4.4. $\square$

Corollary 4.3.   Suppose F_1, H_1 are unary real functions over $[2]$, and F_2, H_2 are symmetric binary real functions over $[2]^2$. If $\#\{F_1, F_2\}$ and $\#\{H_1, H_2\}$ are result equivalent, then they are algebra equivalent.

Proof: Let binary functions $F_3 = F_1^{\otimes 2}$, $H_3 = H_1^{\otimes 2}$. Apply corollary 4.2 to $\#\{F_3, F_2\}$ and $\#\{H_3, H_2\}$.

There exists orthogonal matrix M, such that $M^{\otimes 2} F_3 = H_3$, $M^{\otimes 2} F_2 = H_2$

Because $M^{\otimes 2} F_3 = H_3$, which means $(MF_1)^{\otimes 2} = H_1^{\otimes 2}$, either $MF_1 = H_1$ or $MF_1 = -H_1$. If $MF_1 = H_1$, the conclusion holds by base M. If $MF_1 = -H_1$, the conclusion holds by base $-M$. $\square$

Theorem 4.5. Suppose F_3, H_3 are symmetric ternary real functions over $[2]^3$, If $\#\{F_3\}$ and $\#\{H_3\}$ are result equivalent, then they are algebra equivalent.

Proof: Suppose $H_3 = [h_0, h_1, h_2, h_3]$. F_1 (resp. H_1) denote the unary function by connecting two inputs of F_3 (resp. H_3) using $=_2$, that is, $H_1 = [h_0 + h_2, h_1 + h_3]$.

Let F_2 (resp. H_2) denote the binary function which is one F_3 (resp. H_3) function connected by one F_1 (resp. H_1).

Obviously, $\#\{F_1, F_2\}$ and $\#\{H_1, H_2\}$ are result equivalent. Apply corollary 4.3 to $\#\{F_1, F_2\}$ and $\#\{H_1, H_2\}$. There exists orthogonal matrix M such that $MF_1 = H_1$ and $M^{\otimes 2}F_2 = H_2$.

Let $M^{\otimes 3}F_3 = [f_0, f_1, f_2, f_3]$, $\Delta_j = h_j - f_j$, $j = 0, 1, 2, 3$. Because $MF_1 = [f_0 + f_2, f_1 + f_3]$ and $MF_1 = H_1$, $\Delta_0 + \Delta_2 = 0$ and $\Delta_1 + \Delta_3 = 0$.

Let $H_1 = [h_0 + h_2, h_1 + h_3] = MF_1 = [a, b]$, then $H_2 = [ah_0 + bh_1, ah_1 + bh_2, ah_2 + bh_3]$ and $M^{\otimes 2}F_2 = [af_0 + bf_1, af_1 + bf_2, af_2 + bf_3]$. ($F_2$ is composed of F_3 and F_1. Because M is orthogonal, $M^{\otimes 2}F_2$ can be realized by composing $M^{\otimes 3}F_3$ and MF_1.) Because $M^{\otimes 2}F_2 = H_2$, $a\Delta_0 + b\Delta_1 = 0$, $a\Delta_1 + b\Delta_2 = 0$, $a\Delta_2 + b\Delta_3 = 0$.

Now we get five linear equations about Δ_j. Notice a and b are real numbers, since F_3 and H_3 are real functions. Calculation shows that, there is only zero solution iff $a^2 + b^2 \neq 0$. Hence, if $a \neq 0$ or $b \neq 0$, we have proved $M^{\otimes 3}F_3 = H_3$.

If $a = b = 0$, $H_1 = MF_1 = [0, 0]$, so $F_1 = [0, 0]$. let $F_3 = [x, y, -x, -y]$. There exist $s = (x - iy)/2$ and $t = (x + iy)/2$ such that $F_3 = s \begin{pmatrix} 1 \\ i \end{pmatrix}^{\otimes 3} + t \begin{pmatrix} 1 \\ -i \end{pmatrix}^{\otimes 3}$.

Because x and y are real number, $s \neq 0$, $t \neq 0$. Under base $\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$, $\#\{F_3\}|\{F_3\}$ is holographic reduced to $\#\{[s, 0, 0, t]\}|\{[8t, 0, 0, 8s]\}$. Similarly, H_3 also has form $H_3 = c \begin{pmatrix} 1 \\ i \end{pmatrix}^{\otimes 3} + d \begin{pmatrix} 1 \\ -i \end{pmatrix}^{\otimes 3}$, and under the same base, $\#\{H_3\}|\{H_3\}$ is holographic reduced to $\#\{[c, 0, 0, d]\}|\{[8d, 0, 0, 8c]\}$.

Because $\#\{F_3\}|\{F_3\}$ is special case of $\#\{F_3\}$, $\#\{[s, 0, 0, t]\}|\{[8t, 0, 0, 8s]\}$ and $\#\{[c, 0, 0, d]\}|\{[8d, 0, 0, 8c]\}$ are result equivalent. Hence, $st = cd$.

Notice $\begin{pmatrix} (\frac{c}{s})^{\frac{1}{3}} & 0 \\ 0 & (\frac{d}{t})^{\frac{1}{3}} \end{pmatrix}$ can turn $[s, 0, 0, t]$ into $[c, 0, 0, d]$. Let

$$M = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \begin{pmatrix} (\frac{c}{s})^{\frac{1}{3}} & 0 \\ 0 & (\frac{d}{t})^{\frac{1}{3}} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}^{-1}.$$

Then, $M^{\otimes 3}F_3 = H_3$ and $M'M = I$ (the second equation is right because of the condition $st = cd$). $\qquad\square$

References

[1] Bulatov A, Grohe M. The complexity of partition functions. Theor. Comput. Sci., 2005, 348 (2-3): 148–186.

[2] Bulatov A. The complexity of the counting constraint satisfaction problem. ICALP, 2008, (1): 646–661.

[3] Bulatov A, Dyer M, Goldberg L, Jalsenius M, Richerby D. The complexity of weighted Boolean #CSP with mixed signs. Theor. Comput. Sci., 2009, 410(38-40): 3949–3961.

[4]   Cai JY, Choudhary V. Valiant's holant theorem and matchgate tensors. Theor. Comput. Sci., 2007, 384(1): 22–32.

[5]   Cai JY, Lu P. Holographic algorithms: The power of dimensionality resolved. Theor. Comput. Sci., 2009, 410(18): 1618–1628.

[6]   Cai JY, Lu P. On blockwise symmetric signatures for matchgates. Theor. Comput. Sci., 2010, 411(4-5): 739–750.

[7]   Cai JY, Lu P. Holographic algorithms: from art to science. STOC. 2007. 401–410.

[8]   Cai JY, Chen X, Lu P. Graph homomorphisms with complex values: a dichotomy theorem. CoRR abs/0903.2009. 4728.

[9]   Cai JY, Lu P, Xia M. Holographic algorithms by Fibonacci gates and holographic reductions for hardness. FOCS 2008. 644–653.

[10] Cai JY, Lu P, Xia M. Holant problems and counting CSP. STOC, 2009. 715–724.

[11] Cai JY, Lu P, Xia M. A computational proof of complexity of some restricted counting problems. TAMC 2009. 138–149.

[12] Creignou N, Hermann M. Complexity of generalized satisfiability counting problems. Inf. Comput., 1996, 125(1): 1–12.

[13] Dyer M, Goldberg L, Paterson M. On counting homomorphisms to directed acyclic graphs. J. ACM, 2007, 54(6).

[14] Dyer M, Goldberg L, Jerrum M. The complexity of weighted Boolean CSP. SIAM J. Comput., 2009, 38(5): 1970–1986.

[15] Dyer M, Goldberg L, Jerrum M. A complexity dichotomy for hypergraph partition functions. CoRR abs/0811.0037. 2008.

[16] Dyer M, Greenhill C. The complexity of counting graph homomorphisms. Random Struct. Algorithms, 2000, 17(3-4): 260–289.

[17] Lovász L. Operations with structures. Acta. Math. Acad. Sci. Hung., 1967, (18): 321–328.

[18] Vadhan S. The complexity of counting in sparse, regular, and planar graphs. SIAM J. Comput., 2001, 31(2): 398–427.

[19] Valiant L. The complexity of computing the permanent. Theor. Comput. Sci., 1979, 8: 189–201.

[20] Valiant L. The complexity of enumeration and reliability problems. SIAM J. Comput., 1979, 8(3): 410–421.

[21] Valiant L. Holographic algorithms. SIAM J. Comput., 2008, 37(5): 1565–1594.

[22] Valiant L. Holographic circuits. ICALP. 2005. 1–15.

[23] Valiant L. Accidental algorthims. FOCS. 2006. 509–517.

[24] Xia M, Zhang P, Zhao W. Computational complexity of counting problems on 3-regular planar graphs. Theor. Comput. Sci., 2007, 384(1): 111–125.