Holographic reduction: a domain changed application and its partial converse theorems

ICALP 2010

夏盟信
Mingji Xia

Institute of Software
Chinese Academy of Sciences

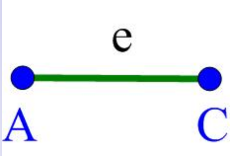
2010.7.6

Outline

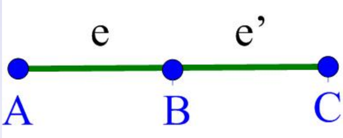
Matrix multiplication

- Product of vectors and matrices.

$AC = \sum_{e \in [n]} a_e c_e$
$A = (a_e), C = (c_e).$

- 

$ABC = \sum_{e,e' \in [n]} a_e b_{ee'} c_{e'}$
$A = (a_e), B = (b_{ee'}), C = (c_{e'}).$

- 

- Vector A (resp. C) is also a unary function

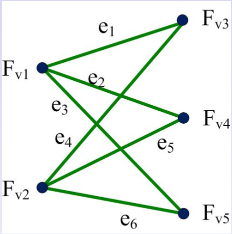
$$e \in [n] \to a_e$$

- Matrix B is also binary function

$$(e, e') \in [n]^2 \to b_{ee'}$$

#F|H

- The input of $\#\mathbf{F}|\mathbf{H}$ is a bipartite graph $G(U, V, E)$. Each vertex $v \in U \cup V$ has a function F_v.



- The value of this problem is

$$\sum_{e_1,\ldots,e_t \in [n]} \prod_{v \in U \cup V} F_v(e_{v,1}, \ldots, e_{v,d_v}),$$

where $e_{v,i}$ is the ith edge of v.

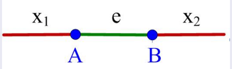
- If $v \in U$, $F_v \in \mathbf{F}$.
If $v \in V$, $F_v \in \mathbf{H}$.

Gadgets in #$\mathbf{F}|\mathbf{H}$

- Except defining the value (a function of arity 0) of an instance, we can also define the function of a gadget.

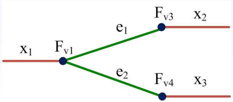
Example

$(AB)(x_1, x_2) = \sum_e a_{x_1,e} b_{e,x_2}$
$A = (a_{x_1,e}), B = (b_{e,x_2})$.

- 

- Given a gadget Γ, we can define its function F_Γ in its external edges $\{x_i\}$, by a summation over its internal edges $\{e_i\}$, where $e_{v,i}$ is the ith edge of v.

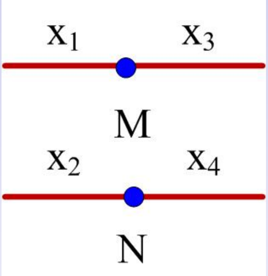
$$F_\Gamma(x_1, \ldots, x_s) = \sum_{e_1,\ldots,e_t \in [n]} \prod_{v \in U \cup V} F_v(e_{v,1}, \ldots, e_{v,d_v}).$$



More examples

$$M \otimes N$$

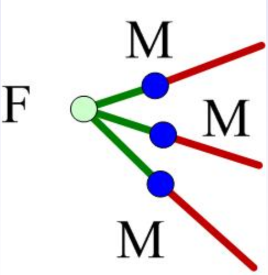
$$(M \otimes N)_{x_1 x_2, x_3 x_4} = M_{x_1, x_3} N_{x_2, x_4}$$



We also use a vector of length $[n]^k$ to denote a function of arity k.

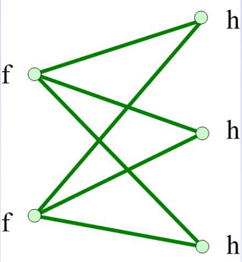
$$F(M \otimes M \otimes M)$$

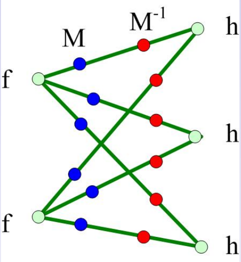
Also denoted as $F(M^{\otimes 3})$.

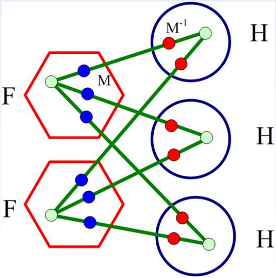


Holographic reduction

$AB = AEB = AMM^{-1}B = (AM)(M^{-1}B)$. ($E$ is identity matrix.)







Theorem (Valiant 2004)

$\#\{f\}|\{h\}$ and $\#\{F\}|\{H\}$ have the same value.

$$F = fM^{\otimes 3},$$

$$H = (M^{-1})^{\otimes 2}h.$$

An example: Fibonacci function

- A symmetric function F of arity k in Boolean variables is denoted as $[f_0, f_1, \ldots, f_k]$, where f_i is the value of F on inputs of weights i.
- $F_1 = [a_0, a_1] = [0, 1]$,
  $F_2 = [a_0, a_1, a_2] = [0, 1, 1]$,
  $F_3 = [a_0, a_1, a_2, a_3] = [0, 1, 1, 2]$, ...
  $F_k = [a_0, a_1, \ldots, a_k]$.
  ($\{a_i\}$ is Fibonacci sequence.)
- $=_k$ denotes the equivalent relation of arity k.
  $(=_k) = [1, 0, \ldots, 0, 1]$. $(=_k^{a,b}) = [a, 0, \ldots, 0, b]$.
- For any d, there is holographic reduction between $\#\{=_1^{1,-1}, \ldots, =_d^{1,-1}\}|\{=_2^{\varphi,\varphi-1}\}$ and $\#\{F_1, \ldots, F_d\}|\{=_2\}$.
  The base M is $\begin{pmatrix} 1 & \varphi \\ 1 & 1-\varphi \end{pmatrix}$, where $\varphi = \frac{\sqrt{5}-1}{2}$.

An example: Fibonacci function

- For any d, there is holographic reduction between $\#\{=_1^{1,-1},\ldots,=_d^{1,-1}\}|\{=_2^{\varphi,\varphi-1}\}$ and $\#\{F_1,\ldots,F_d\}|\{=_2\}$. The base M is $\begin{pmatrix} 1 & \varphi \\ 1 & 1-\varphi \end{pmatrix}$, where $\varphi=\frac{\sqrt{5}-1}{2}$.
- Because $\sqrt{5}\ a_k=\varphi^k-(1-\varphi)^k$, $\sqrt{5}\ F_k=(1,\varphi)^{\otimes k}-(1,1-\varphi)^{\otimes k}$.
- Because $(=_k^{1,-1})=(1,0)^{\otimes k}-(0,1)^{\otimes k}$,

$$(=_k^{1,-1})M^{\otimes k}=\sqrt{5}\ F_k.$$

- $$(M^{-1})^{\otimes 2}(=_2^{\varphi,\varphi-1})=(=_2)$$

A domain size changed application

$F_k = [a_0, a_1, \ldots, a_k]$, for any d, $\#\{F_1, F_2, \ldots, F_d\}|\{=_2\}$ is polynomial time computable.

A problem is #P-hard, if all problems in #P can be reduced to it.

Lemma

$P_{k+1} = [a_0, a_1, \ldots, a_k, -2a_k]$, for any $d \geq 2$, $\#\{F_1, F_2, \ldots, F_d, P_{d+1}\}|\{=_2\}$ is #P-hard.

Theorem

For any $d \geq 2$, there exists a complex binary function H_d such that $\#\{=_1, =_2, \ldots, =_{d+1}\}|\{H_d\}$ is #P-hard, but $\#\{=_1, =_2, \ldots, =_d\}|\{H_d\}$ is polynomial time computable.

- Only need to build a holographic reduction from $\#\{F_1, F_2, \ldots, F_d, P_{d+1}\}|\{=_2\}$ (domain is $[2]$) to $\#\{=_1, =_2, \ldots, =_{d+1}\}|\{H_d\}$ (domain is $[m]$). (This is also a holographic reduction from $\#\{F_1, F_2, \ldots, F_d\}|\{=_2\}$ to $\#\{=_1, =_2, \ldots, =_d\}|\{H_d\}$.)

Maximum degree and complexity

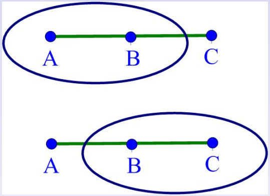
Many hardness results are strengthened to maximum degree bounded version.

- SAT $\rightarrow$ 3SAT (NP-hard)
- #SAT $\rightarrow$ #2SAT (#P-hard)
- Lots in [Vadhan 2001] ......
- #CSP($\mathbf{F}$)($\#\{=_1, =_2, \ldots\}|\mathbf{F}$) $\rightarrow$ $\#\{=_1, =_2, =_3\}|\mathbf{F}$ (each variables occurs at most 3 times), where $\mathbf{F}$ is composed of complex functions in Boolean variables. [Cai,Lu,Xia 2009]

  By this result, our theorem does not hold for Boolean domain.

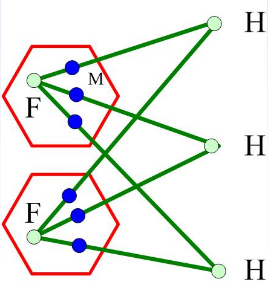
  By our theorem, we can not get this kind of strong degree bounded #P hardness results for general counting problem classes.
- If #CSP($\{G\}$) is hard, there exists some d (depends on G) such that $\#\{=_1, \ldots, =_d\}|\{G\}$ is hard, where G is a 0-1 weighted undirected graph. [Dyer,Greenhill 2000]

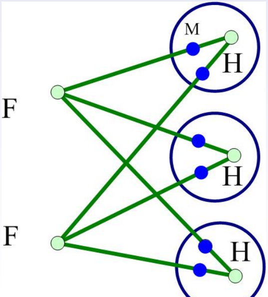
Matrix multiplication satisfies associative law.
$(AB)C = A(BC)$.



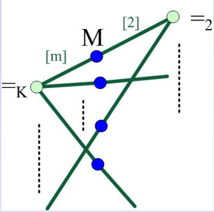
Theorem (Valiant 2004)

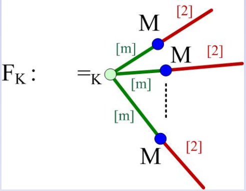
$\#\{FM^{\otimes 3}\}|\{H\}$ and $\#\{F\}|\{M^{\otimes 2}H\}$ *have the same value.*





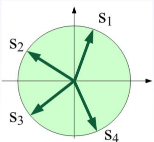
From $\#\{F_1, F_2, \ldots, F_d\}|\{=_2\}$ to $\#\{=_1, =_2, \ldots, =_d\}|\{H_d\}$





- Find M such that $F_k = (=_k)M^{\otimes k}$. Recall,
  Theorem: there exists $H_d (= M'M)$, ...
- Two small tricks for constructing such a M.
  1. $[a_0, a_1, a_2 \ldots, a_k] = \sum_{i=0}^{k} \frac{c_i}{c}[1, r_i, r_i^2, \ldots, r_i^k]$.
     If r_i are different integers, there is an integer solution for c_i and c.
     $|c_i|[1, r_i, r_i^2, \ldots, r_i^k]$ can be realized in $(=_k)M^{\otimes k}$ by setting $|c_i|$ rows of $(1, r_i)$ in M.

If c_i is negative, we utilize $\sum_{s=1}^{k} r_s^i = -1$ for $i = 1, 2, \ldots, k$, where $r_s = e^{\frac{2\pi s}{k+1}}$.



2.

Remark

- In this application, just some problems examples are constructed. There is no requirement on domain size m and function H_d.
- Under these weak requirements, we realize a strong transformation on one side by holographic reduction.
- Open problem:
  Assume FP$\neq$#P. Is there some class of problems, such that predicating the complexity of these problems is uncomputable?
  In some papers about dichotomy theorems, it is considered whether their dichotomy theorems are computable, and some of them are open.

Converse of holographic reduction

Conjecture

Under some conditions, the converse of holographic reduction holds.

For example,
$\#\{f\}|\{h\}$ and $\#\{F\}|\{H\}$ have the same value, where f and F are ternary functions, and h and H are binary functions. Then, there exists nonsingular matrix M such that,

$$F = fM^{\otimes 3},$$

$$H = (M^{-1})^{\otimes 2}h.$$

It does not holds for some special cases. For example, $\#\{(1,0),(1,0)\}|\{(4,1)\}$ and $\#\{(1,1),(1,2)\}|\{(4,0)\}$.

Converse of some cases

Theorem (Lovász 1967, Dyer,Goldberg,Paterson 2006)

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.

- If there is a holographic reduction between $\#\mathbf{R}_=|\{H_1\}$ and $\#\mathbf{R}_=|\{H_2\}$, it can be proved that the base M is a permutation matrix.

  $\mathbf{R}_=$ denotes $\{=_1, =_2, \ldots =_k, \ldots\}$.

Converse of some cases

In the following, we only consider $\#\mathbf{F}|\{=_2\}$. Range is real number.

- Domain is arbitrary $[d]$.
  - $\mathbf{F}$ is composed of unary functions.
  - $\mathbf{F}$ is composed of one symmetric binary function.
  - $\mathbf{F}$ is composed of two symmetric binary functions F_1 and F_2. All eigenvalues of F_1 are equal.
  - $\mathbf{F}$ is composed of two symmetric binary functions F_1 and F_2. All eigenvalues of F_1 are different, so is F_2.
- Domain is $[2]$.
  - $\mathbf{F}$ is composed of two symmetric binary functions.
  - $\mathbf{F}$ is composed of one unary function and one symmetric binary function.
  - $\mathbf{F}$ is composed of one symmetric ternary function.

Proof sketch–Unary functions

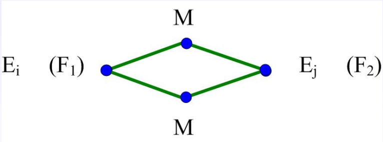
Domain is arbitrary $[d]$. $\mathbf{F}$ is composed of unary functions. $\#\{F_1, \ldots, F_k\}|\{=_2\}$ and $\#\{H_1, \ldots, H_k\}|\{=_2\}$ have the same value. That is,

$$F'F = H'H,$$

where matrices $F = (F_1, F_2, \ldots, F_k)$ and $H = (H_1, H_2, \ldots, H_k)$. The base of holographic reduction is simply HF^{-1}. Because $F'F = H'H$, $M'M = E$. M change $=_2$ into $=_2$.

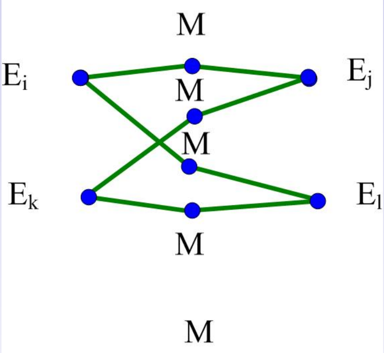
Proof sketch–Two symmetric binary functions

Domain is arbitrary $[d]$. $\mathbf{F}$ is composed of two symmetric binary functions F_1 and F_2. All eigenvalues of F_1 are different, so is F_2. $\#\{F_1, F_2\}|\{=_2\}$ and $\#\{H_1, H_2\}|\{=_2\}$.

- By the result for one symmetric function, we only need to prove for $\#\{F_1, MF_2M'\}|\{=_2\}$ and $\#\{F_1, TF_2T'\}|\{=_2\}$, where F_1 and F_2 are diagonal matrix with different diagonal entries, and M, T are orthogonal matrices.
- Using polynomial interpolation method, we can realize E_i by F_1 and F_2.
  $E_i(x, y)$ is always zero, except $E_i(i, i) = 1$.
- 

Because $\mathrm{tr}(E_i M E_j M') = \mathrm{tr}(E_i T E_j T')$, $M_{ij}^2 = T_{ij}^2$.

Proof sketch–Two symmetric binary functions

- $\left(\frac{M_{ij}}{T_{ij}}\right)^2 = \pm 1$, assume T_{ij} is not zero.
- 

  Because $\operatorname{tr}(E_i M E_j M' E_k M E_l M') = \operatorname{tr}(E_i T E_j T' E_k T E_l T')$, $\frac{M_{ij}}{T_{ij}} \frac{M_{il}}{T_{il}} \frac{M_{kj}}{T_{kj}} \frac{M_{kl}}{T_{kl}} = 1$.

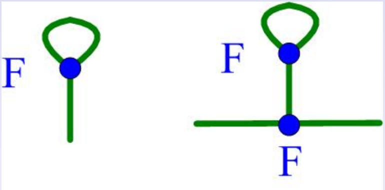
  Consider matrix $R = (\frac{M_{ij}}{T_{ij}})$. This means, the 2×2 submatrix $R_{ik,jl}$ has rank 1.
- We can prove R has rank 1. (If there are zero T_{ij}, the proof is quite a few more complicated.)

Proof sketch–Two symmetric binary functions

- $R = uv'$, then $UTV = M$.
  u, v are column vector composed of 1 and -1.
  U (resp. u) is the diagonal matrix whose diagonal is u (resp. v).
- Compose U with F_1. $UF_1U' = F_1$. $VF_2V' = F_2$.

Proof sketch–One symmetric ternary functions

Domain is [2]. $\#\{F\}|\{=_2\}$ and $\#\{H\}|\{=_2\}$.
We construct some gadgets to prove this case.



This does not work for $F = [x, y, -x, -y]$. The value of $\#\{F\}|\{=_2\}$ is always zero on non-bipartite graphs.
There is a direct proof for $[x, y, -x, -y]$ case.

Open problems

- Whether the converse of holographic reduction holds?
- If it does not hold, the condition is not a necessary condition.
  Can we find some other sufficient conditions and reductions?
- If it does hold, can we utilize it to prove complexity results?

Thank you !