Towards a parameterised version of Toda's theorem

Catherine McCartin

Massey University, New Zealand

c.m.mccartin@massey.ac.nz

August 25, 2017

$\#P$

Define the class $\#P$ to be the class of all functions

$$f_M : \{0,1\}^* \to \mathbb{N}$$

such that M is a non-deterministic Turing machine and $f_M(x)$ gives the number of accepting paths of M on input x.

$f \in \#P$ iff there is a set $A \in P$ and $k \geq 0$ such that $\forall x \in \{0,1\}^*$,

$$f(x) = |\{y \in \{0,1\}^{|x|^k} \mid x\#y \in A\}|$$

$\#P$

View $\#P$ as a class of functions that give the cardinality of a set of *witnesses* to an existential formula.

Denote the set of all witnesses for x wrt $p : \mathbb{N} \to \mathbb{N}$ and $A \subseteq \Sigma^*$ by

$$W(p, A, x) \stackrel{def}{=} \{y \in \{0,1\}^{p(|x|)} \mid x\#y \in A\}$$

Complexity classes defined by $|W(p, A, x)|$

$$L \in NP \overset{def}{\iff} \exists A \in P,\ \exists c \geq 0,\ \forall x\ \ x \in L \Leftrightarrow |W(n^c, A, x)| > 0$$

$$L \in \Sigma^p_{k+1} \overset{def}{\iff} \exists A \in \Pi^p_k,\ \exists c \geq 0,\ \forall x\ \ x \in L \Leftrightarrow |W(n^c, A, x)| > 0$$

$$L \in RP \overset{def}{\iff} \exists A \in P,\ \exists c \geq 0,\ \forall x$$

$$x \in L \Rightarrow |W(n^c, A, x)| > \frac{3}{4} \cdot 2^{|x|^c}$$
$$x \notin L \Rightarrow |W(n^c, A, x)| = 0$$

$$L \in BPP \overset{def}{\iff} \exists A \in P,\ \exists c \geq 0,\ \forall x$$

$$x \in L \Rightarrow |W(n^c, A, x)| > \frac{3}{4} \cdot 2^{|x|^c}$$
$$x \notin L \Rightarrow |W(n^c, A, x)| \leq \frac{1}{4} \cdot 2^{|x|^c}$$

Complexity classes defined by $|W(p, A, x)|$

$$L \in \oplus P \overset{def}{\iff} \exists A \in P,\ \exists c \geq 0,\ \forall x\ \ x \in L \Leftrightarrow |W(n^c, A, x)|\ \ odd$$

$$L \in PP \overset{def}{\iff} \exists A \in P,\ \exists c \geq 0,\ \forall x\ \ x \in L \Leftrightarrow |W(n^c, A, x)| \geq 2^{|x|^c - 1}$$

$$L \in \#P \overset{def}{\iff} \exists A \in P,\ \exists c \geq 0,\ \forall x\ \ L(x) = |W(n^c, A, x)|$$

Operators on complexity classes

Generalise to a set of operators $BP, R, \#, \Sigma^p, \Sigma^{log}, \Pi^p, \Pi^{log}$ on complexity classes.

$$
\begin{array}{ll}
R \cdot \mathcal{C} & R \cdot P = RP \\
BP \cdot \mathcal{C} & BP \cdot P = BPP \\
\oplus \cdot \mathcal{C} & \oplus \cdot P = \oplus P \\
\Sigma^p \cdot \mathcal{C} & \Sigma^p \cdot P = NP \\
\Pi^p \cdot \mathcal{C} & \Pi^p \cdot P = co - NP
\end{array}
$$

$$L \in BP \cdot \mathcal{C} \overset{def}{\iff} \exists A \in \mathcal{C},\ \exists k \geq 0,\ \forall x$$

$$x \in L \Rightarrow |W(n^k, A, x)| > \frac{3}{4} \cdot 2^{|x|^k}$$
$$x \notin L \Rightarrow |W(n^k, A, x)| \leq \frac{1}{4} \cdot 2^{|x|^k}$$

Toda's theorem

$P^{\#P}$ is the class of decision problems solvable in polynomial time with an oracle for some $f \in \#P$.

The polynomial time hierarchy is contained in $P^{\#P}$.

$$PH \subseteq P^{\#P}$$

Toda (FOCS 1989)

Toda's theorem

$$PH \subseteq BP \cdot \oplus P$$

This part of the proof can be broken down into inclusions that establish basic algebraic properties of operators on complexity classes.

Let $\mathcal{C}$ be a complexity class closed downward under $\leq_T^p$. Then

1. $\Sigma^p \cdot \mathcal{C} \subseteq R \cdot \Sigma^{log} \cdot \oplus \cdot \mathcal{C}$
2. $\Pi^{log} \cdot \oplus \cdot \mathcal{C} \subseteq \oplus \cdot \mathcal{C}$
3. $\oplus \cdot BP \cdot \mathcal{C} \subseteq BP \cdot \oplus \cdot \mathcal{C}$
4. $BP \cdot BP \cdot \mathcal{C} \subseteq BP \cdot \mathcal{C}$
5. $\oplus \cdot \oplus \cdot \mathcal{C} \subseteq \oplus \cdot \mathcal{C}$
6. $BP \cdot \mathcal{C}$ and $\oplus \cdot \mathcal{C}$ are closed downward under $\leq_T^p$

Toda's theorem

$$PH \subseteq BP \cdot \oplus P$$

Induction on levels of the polynomial-time hierarchy:

$\Sigma_0^p = P \subseteq BP \cdot \oplus P$

Suppose $\Sigma_k^p = P \subseteq BP \cdot \oplus P$
by 6, $BP \cdot \oplus P$ closed under complement, so $\Pi_k^p = P \subseteq BP \cdot \oplus P$

$$\begin{aligned}
\Sigma_{k+1}^p &= \Sigma^p \cdot \Pi_k^p \\
&\subseteq \Sigma^p \cdot BP \cdot \oplus P \\
&\subseteq R \cdot \Sigma^{log} \cdot \oplus \cdot BP \cdot \oplus P \\
&\subseteq R \cdot \oplus \cdot BP \cdot \oplus P \\
&\subseteq BP \cdot \oplus \cdot BP \cdot \oplus P \\
&\subseteq BP \cdot BP \cdot \oplus \cdot \oplus P \\
&\subseteq BP \cdot \oplus P
\end{aligned}$$

$PH = \bigcup_k \Sigma_k^p \subseteq BP \cdot \oplus P$

Toda's theorem

$$BP \cdot \oplus P \subseteq P^{\#P}$$

Let $L \in BPP \cdot \oplus P$. Then $\exists A \in \oplus P$ and $\exists k \geq 0$ such that $\forall x$

$$x \in L \Rightarrow |W(n^k, A, x)| > \frac{3}{4} \cdot 2^{|x|^k}$$

$$x \notin L \Rightarrow |W(n^k, A, x)| \leq \frac{1}{4} \cdot 2^{|x|^k}$$

$A \in \oplus P \quad \Rightarrow \exists$ polynomial time NDTM st $x\#w \in A$ iff $f(x\#w)$ is odd where $f(x\#w) =$ number of accepting paths of M on input $x\#w$.

Modify M to get N that on input $x\#w$ has $p(f(x\#w))$ accepting paths.

Use a particular p such that :

$$z \;\; odd \quad \Rightarrow p(z) \equiv -1 \;\; (mod \;\; 2^{n^k+1})$$

$$z \;\; even \quad \Rightarrow p(z) = 0 \;\; (mod \;\; 2^{n^k+1})$$

Toda's theorem

$$BP \cdot \oplus P \subseteq P^{\#P}$$

Determine membership in L using $P^{\#P}$ computation:

Use machine K that on input x of length n

1. generates all strings $x\#w$ with $|w| = n^k$ by branching, one path per string
2. for each branch, runs N on $x\#w$

Number of accepting paths for K on input x:

$$\sum_{|w|=n^k} p(f(x\#w))$$

Modulo 2^{n^k+1}, this is

$$\sum_{\substack{|w|=n^k \\ f(x\#w)\ odd}} -1$$

Toda's theorem

$$\sum_{\substack{|w|=n^k \\ f(x\#w)\ odd}} -1$$

$$\begin{aligned}
&\equiv 2^{n^k+1} - |\{w \mid |w| = n^k \wedge f(x\#w)\ odd\}| \\
&\equiv 2^{n^k+1} - |\{w \mid |w| = n^k \wedge x\#w \in A\}| \\
&\equiv 2^{n^k+1} - |W(n^k, A, x)|
\end{aligned}$$

$$\begin{aligned}
x \in L &\Rightarrow \tfrac{3}{4} \cdot 2^{n^k} \leq |W(n^k, A, x)| \leq 2^{n^k} \\
&\Rightarrow 2^{n^k} \leq 2^{n^k+1} - |W(n^k, A, x)| \leq \tfrac{5}{4} \cdot 2^{n^k}
\end{aligned}$$

$$\begin{aligned}
x \notin L &\Rightarrow 0 \leq |W(n^k, A, x)| \leq \tfrac{1}{4} \cdot 2^{n^k} \\
&\Rightarrow \tfrac{7}{4} \cdot 2^{n^k} \leq 2^{n^k+1} - |W(n^k, A, x)| \leq 2^{n^k+1}
\end{aligned}$$

Valiant -Vazirani

RP computation with an oracle for *USAT* can determine general *SAT* with arbitrarily small one-sided error.

$$NP \subseteq RP^{USAT}$$

$\exists$ a polynomial time probabilistic TM M, with oracle *USAT* st:

$$\psi \ \ satisfiable \Rightarrow PR(M \ \ accepts \ \ \psi) \geq \frac{3}{4}$$

$$\psi \ \ unsatisfiable \Rightarrow PR(M \ \ accepts \ \ \psi) = 0$$

Alternatively, a determinisitic polynomial time TM N, with oracle *USAT* st for a string w of random bits, $|w| = p(|\psi|)$:

$$\psi \ \ satisfiable \Rightarrow PR_w(N \ \ accepts \ \ \psi\#w) \geq \frac{3}{4}$$

$$\psi \ \ unsatisfiable \Rightarrow PR_w(N \ \ accepts \ \ \psi\#w) = 0$$

Valiant -Vazirani

$NP \subseteq RP^{USAT}$

Construct a random tower of linear subspaces

$$\{0\} = E_0 \subset E_1 \subset \cdots \subset E_n = \mathbb{GF}_2^n$$

E_i has dimension i, all towers equally likely.

Choose a random basis $x_1, \ldots, x_n$ of $\mathbb{GF}_2^n$, $E_i = \{x_1, \ldots, x_{n-i}\}^\perp$
$A^\perp \stackrel{def}{=} \{y | \forall x \in A \ \ x \cdot y = 0\}$

Lemma: Let S be a non-empty subset of $\mathbb{GF}_2^n$.
Let $E_0 \subset \cdots \subset E_n$ be a random tower of subspaces of $\mathbb{GF}_2^n$ as above.
Then

$$Pr(\exists i \,|\, |S \cap E_i| = 1) \geq \frac{3}{4}$$

Valiant -Vazirani

$NP \subseteq RP^{USAT}$

Let n be the number of variables in ψ.

Machine N uses n^2 random bits (w) to construct random tower of linear subspaces $E_i \subseteq \mathbb{GF}_2^n$.

For each i, construct formula $\varphi_i =$ "$(x_1, \ldots, x_n) \in E_i$"

N queries the oracle on each $\psi \wedge \varphi_i$. If we get a "yes" then accept.

Let S be the truth assignments satisfying ψ.

$Pr(N \ \ accepts \ \ \psi\#w) = Pr(\exists i \ \ \psi \wedge \varphi_i \in USAT)$

$$\geq \frac{3}{4} \text{ if } \mathrm{S} \neq \emptyset, \ \ 0 \text{ if } \mathrm{S} = \emptyset$$

Parameterized counting classes

Definition (Parameterized witness function)

Let $w : \Sigma^* \times \mathcal{N} \to \mathcal{P}(\Gamma^*)$, and let $\langle \sigma, k \rangle \in \Sigma^* \times \mathcal{N}$.

The elements of $w(\langle \sigma, k \rangle)$ are *witnesses* for $\langle \sigma, k \rangle$.

Associate a parameterized language $L_w \subseteq \Sigma^* \times \mathcal{N}$ with w

$$L_w = \{ \langle \sigma, k \rangle \in \Sigma^* \times \mathcal{N} \mid w(\langle \sigma, k \rangle) \neq \emptyset \} .$$

L_w is the set of problem instances that have witnesses.

Parameterized counting classes

Definition (Parameterized counting problem)

Let $w : \Sigma^* \times \mathcal{N} \to \mathcal{P}(\Gamma^*)$ be a parameterized witness function.

The corresponding *parameterized counting problem* can be considered as a function $f_w : \Sigma^* \times \mathcal{N} \to \mathcal{N}$ that, on input $\langle \sigma, k \rangle$, outputs $|w(\langle \sigma, k \rangle)|$.

Parameterised counting classes

Definition (Parameterized counting reduction)

Consider two (witness functions for) parameterized counting problems.

$$w : \Sigma^* \times \mathcal{N} \to \mathcal{P}(\Gamma^*)$$
$$v : \Pi^* \times \mathcal{N} \to \mathcal{P}(\Delta^*)$$

A *parameterized counting reduction* from w to v consists of a parameterized transformation

$$\rho \ : \ \Sigma^* \times \mathcal{N} \to \Pi^* \times \mathcal{N}$$

and a function

$$\tau \ : \ \mathcal{N} \to \mathcal{N}$$

such that

$$|w(\langle \sigma, k \rangle)| = \tau(|v(\rho(\langle \sigma, k \rangle))|).$$

When such a reduction exists we say that *w reduces to v*.

Parameterized counting classes

#WEIGHTED WEFT t DEPTH h CIRCUIT SATISFIABILITY (WCS(t, h))

Input:	A weft t depth h decision circuit C.
Parameter:	A positive integer k.
Output:	The number of weight k satisfying assignments for C.

Let $w_{\mathcal{F}(t,h)} : \Sigma^* \times \mathcal{N} \to \mathcal{P}(\Gamma^*)$ be the standard parameterized witness function associated with this counting problem:

$$w_{\mathcal{F}(t,h)}(\langle C, k\rangle) = \{ \text{ weight } k \text{ satisfying assignments for } C \} .$$

Definition ($\#W[1]$)

Define a parameterized counting problem, f_v, to be in $\#W[1]$ iff there is a parameterized counting reduction from v, the parameterized witness function for f_v, to $w_{\mathcal{F}(1,h)}$.

Parameterized counting classes

#WEIGHTED t-NORMALIZED SATISFIABILITY

Input:	A t-normalized propositional formula X.
Parameter:	A positive integer k.
Output:	The number of weight k satisfying assignments for X.

For all $t \geq 1$, #WEIGHTED t-NORMALIZED SATISFIABILITY is complete for $\#W[t]$.

Definition ($\#W[t]$)

Define a parameterized counting problem, f_v, to be in $\#W[t]$ iff v reduces to standard parameterized witness function for #WEIGHTED t-NORMALIZED SATISFIABILITY.

Parameterized counting classes

#WEIGHTED CIRCUIT SATISFIABILITY

Input:	A decision circuit C.
Parameter:	A positive integer k.
Output:	The number of weight k satisfying assignments for C.

Definition ($\#W[P]$)

Define a parameterized counting problem, f_v, to be in $\#W[P]$ iff v reduces to standard parameterized witness function for #WEIGHTED CIRCUIT SATISFIABILITY.

Parameterized class operators

Definition (Parametric connection)

A parametric connection is a function $\alpha : (N \times N) \to (N \times N) : (n, k) \to (n', k')$, a polynomial q, and arbitrary functions $f, g : N \to N$ with $n' = f(k)q(n)$ and $k' = g(k)$.

$\exists \cdot C$ stands for the class of parameterized languages A such that for some $B \in C$ there are nice parametric connections (n, k, n', k', n'', k'') giving for all (x, k),

$$(x, k) \in A \Leftrightarrow (\exists y \in \Sigma^{n'}) \; [wt(y) = k' \wedge (x\#y, k'') \in B]$$

$(n = |x|, n' = |y|, \; n'' = n + n'$ and $wt(y)$ denotes the weight of y.)

Similarly, define "bounded weight" versions of $\forall$, $\oplus$, BPP

Parameterized analogues of PH

Definition ($G[t]$)

$G[t]$ (Uniform $G[t]$) is the class of parameterized languages $L \subseteq \Sigma^* \times \mathbb{N}$ for which there is a parameterized (uniform) family of weft t circuits $F = C_{n,k}$ such that for all x and k, with $n = |x|$, $\langle x, k\rangle \in L \Leftrightarrow C_{n,k}(x) = 1$

Uniform $G[t] = FPT$

Definition ($N[t]$)

$N[t] = \exists \cdot \mathit{Uniform}\ G[t]$

Definition ($H[t]$)

$$\Sigma_1[t] = W[t] = \langle \exists \cdot \mathit{Uniform}\ G[t] \rangle$$
$$\Pi_1[t] = \langle \forall \cdot \mathit{Uniform}\ G[t] \rangle$$

$$H[t] = \bigcup_{i=0}^{\infty} \Sigma_i[t] \cup \Pi_i[t]$$

Parameterized analogues of Toda's theroem

$$N[t] \subseteq BP \cdot \bigoplus \cdot G[t]\,?$$

(analogue of $NP \subseteq BP \cdot \oplus \cdot P$)

$$H[t] \subseteq BP \cdot \bigoplus \cdot G[t]\,?$$

$$\cup_{t \geq 1} W[t] \subseteq FPT^{\#W[1]}\,?$$

+ve results

A randomized (FPT, many-one) reduction from a parameterized language L to a parameterized language L' is a randomized procedure that transforms (x, k) into (x', k') subject to:

1. Running time is FPT.
2. There is a function f' and a constant c' such that, $\forall$ (x, k)

   $(x, k) \in L \Rightarrow Pr[(x', k') \in L'] \geq \frac{1}{f'(k)|x|^{c'}}$

   $(x, k) \notin L \Rightarrow Pr[(x', k') \in L'] = 0$

For all $t \geq 1$ there is an FPT many-one randomized reduction from $W[t]$ to UNIQUE $W[t]$.

(Downey, Fellows and Reagan 1996)

+ve results

UNIQUE k-INDEPENDENT SET is hard for $W[1]$ under randomized polynomial-time reductions.

k-INDEPENDENT SET WITH A UNIQUENESS PROMISE is hard for $W[1]$ under randomized polynomial-time reductions.

(Müller 2008)

+ve results

$\oplus$ MULTICOLOURED CLIQUES

Input:	A graph G and a colouring $c : V(G) \to [k]$.
Parameter:	A positive integer k.
Question:	Is there an odd number of multicoloured cliques? (cliques of size exactly k, each colour used once).

There is a randomized FPT reduction from MULTICOLOURED CLIQUES to $\oplus$ MULTICOLOURED CLIQUES with one-sided error at most $\frac{1}{2}$; errors may only occur on yes-instances.

(Björklund, Dell, Husfeldt 2016)

$\oplus$ MULTICOLOURED CLIQUES

Let $\mathbb{F}$ denote a family of sets, $\mathbb{F} \subseteq 2^U$.

A *restriction* is a function $\rho : U \to \{0, 1, *\}$.

The restricted family $\mathbb{F}|_\rho$ consists of all sets $F \in \mathbb{F}$ that satisfy
$\rho(i) = 1 \Rightarrow i \in F$, $\rho(i) = 0 \Rightarrow i \notin F$

A random restriction is a distribution over restrictions ρ where $\rho(i)$ is randomly sampled for each i independently, subject to
$Pr_\rho(\rho(i) = 0) = p_0$ and $Pr_\rho(\rho(i) = 1) = p_1$. Define $p_* = 1 - (p_0 + p_1)$.

We are interested in the event $\mathbb{F}|_\rho$ is odd, $\oplus\mathbb{F}|_\rho$.

Let each set $F \in \mathbb{F}$ have size at most k.

Claim: If $p_0 = p_* = \frac{1}{2}$ and $p_1 = 0$, then $Pr_\rho(\oplus\mathbb{F}|_\rho) = 2^{-k}$

⊕ MULTICOLOURED CLIQUES

Let (G, kc) be an instance of multicoloured cliques.

Let $\mathbb{F} = \{S \subseteq V(G) \ : \ S \text{ is a multicoloured clique } \}$

For each vertex independently, flip a coin and remove it.

If the input doesn't contain a multicoloured clique, the output doesn't either.

If the input does contain a multicoloured clique, then, with probability $\geq 2^{-k}$ the output contains an odd number of them.

Repeat the reduction $t = O(2^k)$ times to get $G_1, \ldots, G_t$.

OR-composition for $\oplus$ MULTICOLOURED CLIQUES

Let $G_1, \dots, G_t$ and k be given as input, let $k' = tk$, with all k' colours distinct.

Add a fresh disjoint multicoloured clique of size k to each G_i to obtain $G_1^{+1}, \dots, G_t^{+1}$

Compute the "clique sum" H of the t graphs by adding all edges between vertices from distinct graphs.

Output $G' = H^{+1}$, that is H with fresh disjoint multicoloured clique of size k' added.

N_i = number of multicoloured cliques in G_i.

N_G = number of multicoloured cliques in $G' = 1 + \Pi_{i=1}^{k}(N_i + 1)$

N_G is odd $\Leftrightarrow$ at least one N_i is odd.

MULTICOLOURED CLIQUES

Reduction takes time 2^k $poly(n)$, parameter of the output is $t \cdot k = f(k)$.

If G doesn't have a multicoloured clique, then, with probability 1, the output G' has an even number of multicoloured cliques.

If G has a multicoloured clique, then, with probability at most $(1 - 2^{-k})^t \leq \frac{1}{2}$, the output G' has an even number of multicoloured cliques.

The main problem

Every known proof of Toda's theorem uses randomization in an essential way, and then amplification.

If we want to employ the usual parameterized restrictions on nondeterminism as restrictions on randomness, we are limited to $f(k) \cdot log\ n$ many random bits.

(Downey, Fellows and Reagan) uses $kn \cdot log\ n$ random bits

(Bj̈orklund, Dell, Husfeldt) uses $2^k \cdot n$ random bits

+ve result

$(Q, k) \in W[P] - BPFPT \iff$ there is a probabilistic FPT-time bounded Turing machine A such that, for every run of A on x, A tosses at most $f(k) \cdot log\ |x|$ coins and decides Q with two-sided error E.

If $E \leq \frac{1}{2} - |x|^{-c}$ then, via expander graphs, E can be improved to $|x|^{-g(k)}$.

(Müller 2008)