行政院國家科學委員會補助專題研究計畫成果報告

Hecke 算子的特徵值

計畫類別：☑個別型計畫　　□整合型計畫

計畫編號： NSC 89-2115-M-002-003

執行期間： 88 年 8 月 1 日至 89 年 7 月 31 日

計畫主持人：陳其誠教授

本成果報告包括以下應繳交之附件：

- □ 赴國外出差或研習心得報告一份
- □ 赴大陸地區出差或研習心得報告一份
- □ 出席國際學術會議心得報告及發表之論文各一份
- □ 國際合作研究計畫國外研究報告書一份

執行單位：國立台灣大學理學院數學系

中　華　民　國　90 年　5 月　30 日

行政院國家科學委員會專題研究計畫成果報告

Hecke 算子的特徵值

計畫編號：NSC 89-2115-M-002-003
執行期限：88 年 8 月 1 日至 89 年 7 月 31 日
主持人：陳其誠　　台大數學系

一、中文摘要

我們就以下三方面探討在多項式時間內完成 Hecke 算子的特徵值之演算的可能性，及因而引出的數論上的問題：
(A) 使用 Modular symbols
(B) 使用 Galois representations
(C) 使用 Quantum computations

關鍵詞：Hecke 算子、特徵值、Galois 表現、模符號、多項式時間演算法、類群、橢圓曲線、量子計算、代數數體。

Abstract

In the following three aspects, we discuss the problems related to obtaining polynomial time algorithm for computing the eigen-values of Hecke operators.
(A) Using Modular symbols
(B) Using Galois representations
(C) Using Quantum computation

Keywords: Hecke operator、eigen value、Galois representation、Modular symbol、polynomial time algorithm、class group、elliptic curve、quauntum computation、algebraic number field、Galois group.

二、緣由與目的

設 E 為定義在一有限體 Fq 上的橢圓曲線，Schoof 的演算法可以在 q 的多項式時間內算出 $|E(Fq)|$ 之值。現在假設 E 為一定義在 Q 上的橢圓曲線，使用 Schoof 的演算法，給它任一質數 P，我們則可在 P 的多項式時間內算出 $a_p = |\overline{E}_p(F_p)|$ 之值。這裡，我們用 $\overline{E}_p$ 表示 E 在 P 處的 reduction，根據 Shimura-Weil-Tanyama 定理，存在一個 weight 為 2 level 為 N(=E 的 conductor)的 modular form f 使得 a_p 恰為 Hecke 算子 T_p 作用之下 f 的 eigen-value。因而我們說，對於這個 f，存在一個演算法可以在 P 的多項式時間內完成計算出任一 T_p 作用下 f 的 eigen value。這即是我們討論下列問題的緣由，此即為本研究計畫之主題。

問題：給定正整數 N,k，及 character $\varepsilon:(Z/NZ)^* \to C^*$，設 f 為 type(N,k,ε)的 modular form，且為所有 Hecke 算子的 eigen-form，是否存在一演算法可以在 P 的多項式時間內完成算出 f 在 T_p 作用下的 eigen value a_p？

三、結果與討論

兩個議題必須先予以澄清，首先，當我們說「給定一個 modular form of level N，weight k」時，我們到底給定了關於 f 的什麼 data 使得這些 data 足以用來決定 f 呢？因為我們有興趣的是 Hecke eigen-form，故最「切題」的 data 應是 f 的一些 eigen-values，事實上，我們有下列粗淺，但不見於 literature 的 lemma。

Lemma：設 f,g 皆為 level N，weight k 的 modular form，w 為 $\Gamma(N)$ 在 i∞ 的 width。如果 $d=\prod_{\ell\text{質數}} \ell^{4c_\ell+1}(\ell+1)^2(\ell+1)$，$\ell^{c_\ell+1}\|N$

$q = e^{\frac{2\pi i z}{w}}$，

且 $f=\sum_{n=0}^{\infty}a_nq^n$ ， $g=\sum_{n=0}^{\infty}b_nq^n$

滿足 $a_n=b_n\ \forall\ n=0,1,\cdots, w\cdot\left[\frac{dk}{12}\right]+1,$

則 $f=g$.

由上述得知，如果 f 為 normalized Hecke eigen-form 且為 cuspidal，則其 eigen-values

$\left\{a_\ell \mid \ell\le w\left[\frac{dk}{12}\right]+1\right\}$

決定了 f。

另外，在實際演算上，我們常須對固定 N,k 先算出一些預備的 data（例如：決定一組 eigen-forms 的基底，並算出其 eigen-value a_ℓ 至足夠大的 ℓ），這些計算只做一次即可，在爾後的計算裡這些 data 可以重複使用，故當考慮大 p 之 a_p 值之計算所需的時間時，這一部份將視為常數，因此我們並不特別要求在這部份「節省時間」。事實上，這部份的計算通常仍以 modular symbols 的方法最為方便。

（A） Modular Symbols：

如果固定了 weight 與 level，cuspidal modular forms 可看成 Modular Symbols 所成之 $\boldsymbol{Z}$-module 上的 functionals，同時其 (dual)Hecke operator 也可定義在此 module 上，而所有 Hecke operators 所生成的 Hecke algebra 實為 finitely generated，故如上面 Lemma 所述，實由有限多個 T_ℓ 所決定。我們只須將這些 T_ℓ 對角化並在 Modular Symbols 上找到 eigenrectors 即可決定所有 cuspidal modular forms 中的全部 eigen-forms。於此，對於每一個 ℓ，其實包括了 $\ell+1$ 個小運算，每個小運算一以 $t_{\ell,k},\ k=1,..,\ell+1$, 表之一基本上為 Euclidean Algorithm — 皆為 ℓ 之 polynomial time 內可完成的運算。現在如果從事計算 T_p，P 很大，直接做即需 $P\cdot(\log p)^c$ 時間，非為 polgnomial time。一個值得再予思考辦證的想法是使用 Chinese Remainder 定理選用足夠多的小質數 ℓ，將 T_p modulo ℓ 求其 eigen values modulo 每個 ℓ 再給予復原成 eigen value over $\boldsymbol{Z}$。這個方法可否成功，似乎端賴於上述 $t_{\ell k}$ 之集體運算可否有 modulo ℓ 之 version 而可以不使用 Euclidean Algorithm，我們認為，對個別的 $t_{\ell k}$，這種 modulo ℓ 之運算並不存在，這就像，若要計算（A，B）modulo ℓ 仍需先算（A，B）一樣。

（B） Galois Representations：

如果 f 為 type(N,k,ε)，$k\ge 2$，且為 cuspidal，normalized，Hecke operators 的 common eigen-form，則 f 的所有的 eigen values 皆位於一個 number field K_f 中，而且，如果 $\boldsymbol{O}=\boldsymbol{O}_{K_f}$ 為 ring of integers 且 λ 為 sitting over prime number ℓ 的一個 prime ideal，則 Heck-Deligne-Langlands-Piateckii-Shapiro 的定理說：存在 representation φ_λ :Gal($\overline{\boldsymbol{Q}}/\boldsymbol{Q}$)→GL(2,$\boldsymbol{O}_\lambda$)，unramified outside $\ell\cdot N$ 使得 det $\varphi_\lambda(Fr_p)=\varepsilon(p)p^{k-1}$

$tr\varphi_\lambda(Fr_p)=a_p$., p∤ $N\ell$.

現將 φ_λ modulo λ，則得到

θ_λ : Gal($\overline{\boldsymbol{Q}}/\boldsymbol{Q}$)→GL(2, $\boldsymbol{F}_\lambda$)，其中 $\boldsymbol{F}_\lambda=\boldsymbol{Q}/\lambda$。我們只要從足夠多的 ℓ 與 λ 得知 $tr\bar{\varphi}_\lambda(Fr_p)$ 的值，即可回復 a_p 之值。以下是我們認為非常可行的程序。

(1) 當（N,k）固定時，K_λ 的可能性應只有有限個，故 up to isomorphism，$\bar{\varphi}_\lambda$ 的 image 也只有有限個可能性。

(2) 如果使用 discriminant 的計算，則應可決定一個有限多個 number field 所成的集合 S 使得 $\bar{\varphi}_\lambda$ 之 kernel 的 fixed field 必在集中。