Factorization tests arising from counting modular forms and automorphic representations

Miao Gu[1] and Greg Martin

1: University of British Columbia / Duke University

Background

- Let k be a positive even integer.
- $A(k,N)$ is the number of non-isomorphic automorphic representations associated with the space of weight-k cusp forms on $\Gamma_0(N)$. Equivalently, it is the dimension of the space of weight-k newforms of level dividing N. (complicated)
- $G(k,N)$ is the function from Gekeler's Theorem. (simple)
- $B(k,N)$ is the dimension of the space of weight-k newforms on $\Gamma_0(N)$. (complicated)
- $H(k,N)$ is a modified version of $G(k,N)$. (simple)

Gekeler's Theorem (1995)

Using the Dirichlet characters χ_{-4} and χ_{-3}, define

$$G(k,N) = \frac{k-1}{12}N - \frac{1}{2} + c_2(k)\chi_{-4}(N) + c_3(k)\chi_{-3}(N).$$

(Note: $c_2(k)$, χ_{-4} have period 4, and $c_3(k)$, χ_{-3} have period 3.)

Theorem: If N is squarefree, then $A(k,N) = G(k,N)$.

Spaces of Modular Forms

Let $S(k,N)$ be the dimension of weight-k cusp forms on $\Gamma_0(N)$. By the Atkin–Lehner decomposition of spaces of cusp forms

$$S(k,N) = \sum_{d|N} A(k,d) \qquad A(k,N) = \sum_{d|N} B(k,d).$$

Dimension Formulas (Martin, 2005)

- $A(k,N) = \frac{k-1}{12}Ns_0^*(N) - \frac{1}{2}v_\infty^*(N) + c_2(k)v_2^*(N) + c_3(k)v_3^*(N)$
- $B(k,N) = \frac{k-1}{12}Ns_0^\#(N) - \frac{1}{2}v_\infty^\#(N) + c_2(k)v_2^\#(N) + c_3(k)v_3^\#(N)$

where s_0^*, v_∞^*, v_2^*, v_3^*, $s_0^\#$, $v_\infty^\#$, $v_2^\#$ and $v_3^\#$ are multiplicative functions which require the factorization of N to compute.

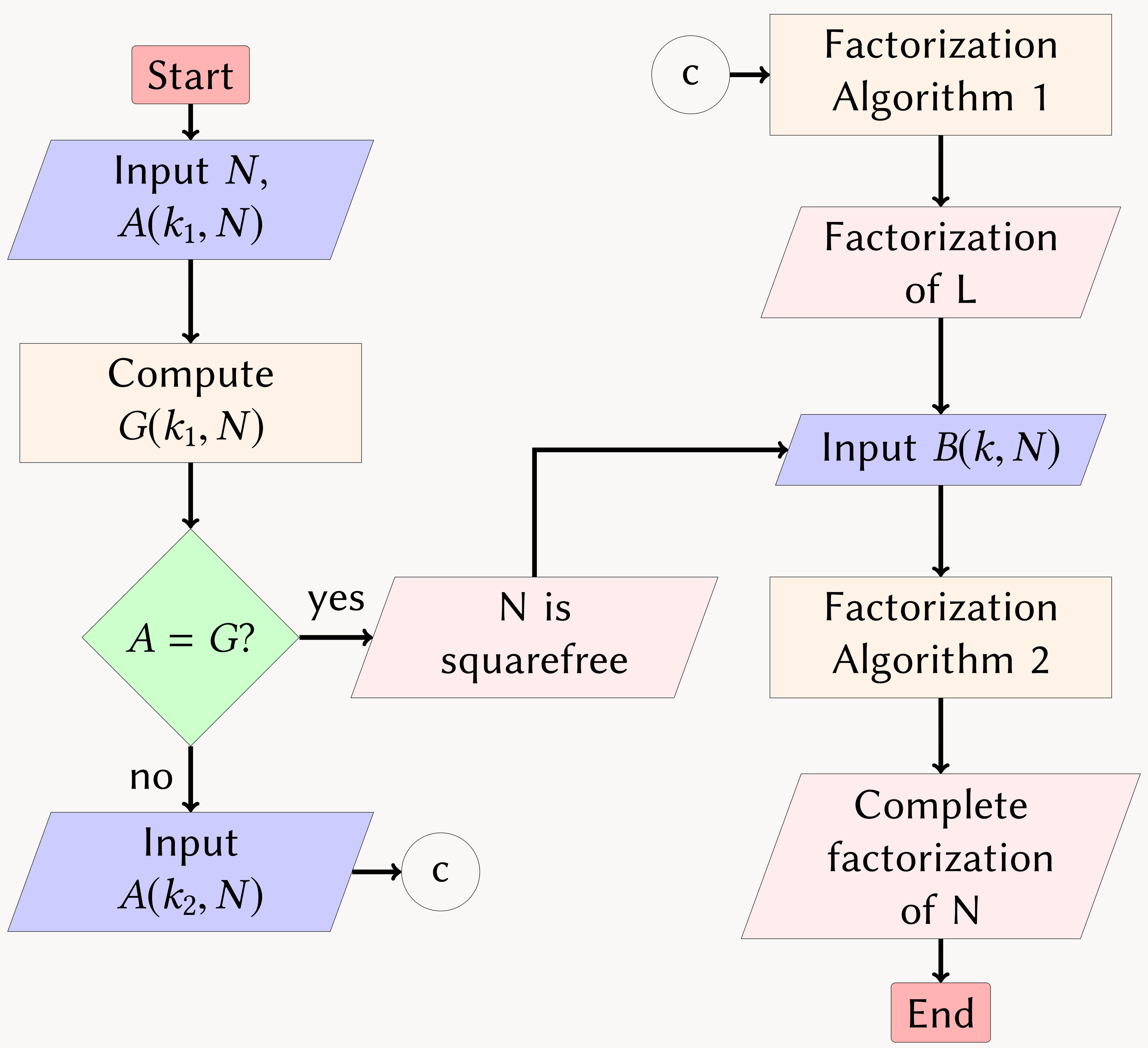
(Note: extra term needed when $k = 2$)

Main Theorems

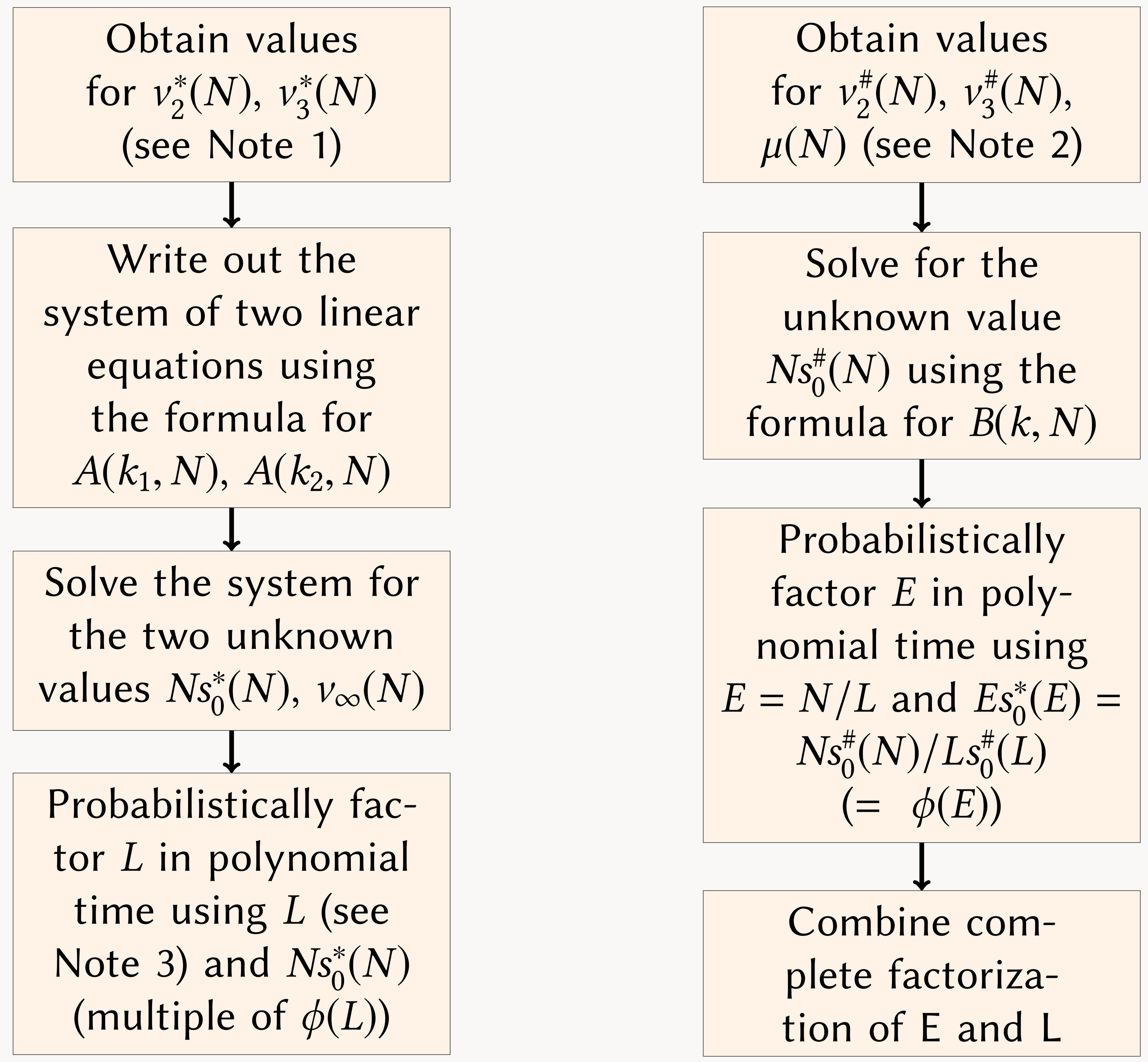
- The converse of Gekeler's Theorem is true with one small exception ($k = 2, N = 9$).
- If we have an oracle that quickly computes $A(k,N)$, even for a single k (or a positive linear combination of several $A(k,N)$, or even a sufficiently tight upper bound for $A(k,N)$), we have a polynomial-time test for squarefreeness.
- Similarly, we have a polynomial-time test for primality if we can compute $B(k,N)$ quickly.
- We can probabilistically obtain the complete factorization of the squarefull part of N if we have fast access to $A(k,N)$ for two distinct weights k_1 and k_2.
- If in addition we have fast access to $B(k,N)$ for a single weight k, we can probabilistically obtain complete factorization of N.

Main Algorithm (k_1, k_2 are distinct weights)

Write $N = EL$ where E is squarefree, L is squarefull and $(E,L) = 1$.



Factorization Algorithm 1 & 2



- Note 1: by definition, $v_2^*(N), v_3^*(N) \in \{-1,0,1\}$, and we can figure out which from $A(k,N)$.
- Note 2: the only possible values for $v_2^\#(N)$, $v_3^\#(N)$, and $\mu(N)$ are 0 or $\pm 2^m$ for $m \le \omega(N)$. Trying all these (polynomially many) values, we can verify the right factorization.
- Note 3: the denominator of $s_0^\#(N)$ is a nontrivial divisor of L; the value of L can be found by iterating this algorithm.

Calculating Dimensions/Further Research

- Calculating $S(k,N)$:
  - classical (Riemann-Roch)
  - trace formula (Ross, 1992)
- Calculating $A(k,N)$ and $B(k,N)$:
  - recursively, starting with values of $S(k,N)$ (traditional)
  - $A(k,N) = \mu(N) * S(k,N)$, $B(k,N) = \mu(N) * \mu(N) * S(k,N)$ (Martin, 2005)
- Further Research: finding ways to quickly obtain $A(k,N)$ and $B(k,N)$ without using the factorization of N

arXiv: 1709.02411 Email: miao.gu@duke.edu