The probabilistic method of Erdős in inverse Galois theory

Orges Leka

April 25, 2026

Abstract

We formulate a probabilistic strategy for inverse Galois theory based on relative resolvents. Let $G \leq S_n$ be a transitive subgroup of order n. A classical relative resolvent criterion says that, for an irreducible degree n polynomial $h \in \mathbb{Q}[x]$, a rational zero of an appropriate S_n/G-resolvent forces $\mathrm{Gal}(h/\mathbb{Q}) \leq G$ up to conjugacy. Since irreducibility gives transitivity and $|G| = n$, this inclusion then forces equality.

The idea developed here is to impose the rational-root condition for the resolvent as an explicit algebraic condition on the rational coefficients of h, and then choose the coefficients randomly on the resulting coefficient variety. The desired Erdos-type conclusion would be that the probability of irreducibility is positive on this constrained family. This would produce a polynomial over $\mathbb{Q}$ with Galois group G. We formulate a finite rational height box,define Bernoulli variables for resolvent success and irreducibility, compute their expectations, and state a counting conjecture under which an Erdős-type existence argument follows.

Contents

1 The basic setting

Let

$$G \leq S_n$$

be a transitive subgroup with

$$|G| = n.$$

Thus the action of G on $\{1, \ldots, n\}$ is regular.

We seek a monic polynomial

$$h(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$$

with

$$\mathrm{Gal}(h/\mathbb{Q}) \cong G.$$

If h is irreducible of degree n, then its Galois group acts transitively on its n roots. Since $|G| = n$, it is enough to force the actual Galois group into a conjugate of G. This is the role of an absolute S_n/G-resolvent.

2 The primitive invariant and the absolute resolvent

Let

$$z_1, \ldots, z_n$$

be formal root variables. The symmetric group S_n acts by

$$\tau \cdot z_i = z_{\tau(i)}.$$

Define

$$m = z_1^1 z_2^2 \cdots z_n^n$$

and the G-orbit sum

$$\Theta_G(z_1, \ldots, z_n) = \sum_{\sigma \in G} \sigma \cdot m = \sum_{\sigma \in G} z_{\sigma(1)}^1 z_{\sigma(2)}^2 \cdots z_{\sigma(n)}^n.$$

Equivalently,

$$\Theta_G = \sum_{\sigma \in G} \prod_{i=1}^{n} z_{\sigma(i)}^i.$$

Lemma 2.1 (Primitivity of the orbit sum)**.** *The invariant Θ_G has stabilizer exactly G:*

$$\mathrm{Stab}_{S_n}(\Theta_G) = G.$$

Proof. For $\tau \in G$, left multiplication gives

$$\tau \cdot \Theta_G = \sum_{\sigma \in G} \tau\sigma \cdot m = \sum_{\sigma \in G} \sigma \cdot m = \Theta_G.$$

Thus $G \leq \mathrm{Stab}_{S_n}(\Theta_G)$.

Conversely, suppose $\tau \in S_n$ fixes Θ_G. Then

$$\sum_{\sigma \in G} \tau\sigma \cdot m = \sum_{\sigma \in G} \sigma \cdot m.$$

The monomials $\rho \cdot m$, $\rho \in S_n$, are pairwise distinct because the exponents $1, 2, \ldots, n$ are pairwise distinct. Hence

$$\{\tau\sigma \cdot m : \sigma \in G\} = \{\sigma \cdot m : \sigma \in G\}.$$

Equivalently, $\tau G = G$, and therefore $\tau \in G$. Thus $\mathrm{Stab}_{S_n}(\Theta_G) = G$. □

The associated absolute S_n/G-resolvent is

$$R_G(Y) = \prod_{\tau G \in S_n/G} (Y - \Theta_\tau),$$

where

$$\Theta_\tau := \tau \cdot \Theta_G = \sum_{\sigma \in G} \prod_{i=1}^{n} z_{\tau\sigma(i)}^i.$$

Thus

$$R_G(Y) = \prod_{\tau G \in S_n/G} \left(Y - \sum_{\sigma \in G} \prod_{i=1}^{n} z_{\tau\sigma(i)}^i \right).$$

Since Θ_G has stabilizer exactly G, its distinct formal conjugates are indexed by the left cosets S_n/G. Therefore

$$\deg_Y R_G = [S_n : G] = \frac{n!}{n} = (n-1)!.$$

The values Θ_τ are permuted by S_n. Hence the coefficients of $R_G(Y)$ are symmetric polynomials in $z_1, \ldots, z_n$. If

$$h(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

has roots $z_1, \ldots, z_n$, then

$$e_k(z_1, \ldots, z_n) = (-1)^k a_{n-k}.$$

Consequently,

$$R_G(Y) \in \mathbb{Q}[a_0, \ldots, a_{n-1}][Y].$$

This is the key algebraic object used in the probabilistic construction.

3 The resolvent criterion

Let $h \in \mathbb{Q}[x]$ be separable of degree n, with roots $z_1, \ldots, z_n$. Let

$$H = \mathrm{Gal}(h/\mathbb{Q}) \leq S_n$$

be the Galois group through its action on the roots.

The standard resolvent principle says that rational roots of the absolute S_n/G-resolvent detect whether H fixes a coset of G. More precisely, away from the specialization locus where distinct formal resolvent values collide, one has

$$R_G(Y) \text{ has a rational root} \quad \Longrightarrow \quad H \leq \tau G \tau^{-1}$$

for some $\tau \in S_n$.

Proposition 3.1 (Resolvent criterion, regular case)**.** *Let $G \leq S_n$ be regular with $|G| = n$. Let $h \in \mathbb{Q}[x]$ be separable and irreducible of degree n, and suppose that the specialized resolvent*

$$R_G(Y; h)$$

has a rational simple root $Y_0 \in \mathbb{Q}$. Then

$$\mathrm{Gal}(h/\mathbb{Q}) \cong G$$

up to conjugacy in S_n.

Proof. Since Y_0 is a rational root, it is fixed by the actual Galois group $H = \mathrm{Gal}(h/\mathbb{Q})$. The simplicity assumption ensures that this root corresponds to a unique coset τG. Hence H fixes that coset, so

$$H \leq \tau G \tau^{-1}.$$

Since h is irreducible, H acts transitively on the n roots. Thus $n \mid |H|$. But

$$|H| \leq |\tau G \tau^{-1}| = |G| = n.$$

Therefore $|H| = n$, and the inclusion is equality. Hence $H = \tau G \tau^{-1}$. □

Remark 3.2. *If the specialized resolvent has multiple coincident roots, then a rational root may come from a collision of several cosets. In applications one either removes this exceptional non-collision locus or includes the condition*

$$R'_G(Y_0) \neq 0$$

in the good event.

4 The exact collapse value and the split base point

The exact uncollapsed construction explains why the special value $-a_{n-1}$ is natural, even though the randomized model below will use the more flexible condition that the resolvent have some rational root.

Let

$$h_0(x) = (x-1) \cdot (x-2) \cdots (x-n)$$

Hence

$$\mathrm{Gal}(h_0/\mathbb{Q}) = C_1 \leq G.$$

Consequently, the absolute S_n/G-resolvent of h_0 has a rational root. For the identity coset this root is precisely $-a_{n-1}^{(0)}$, where

$$h_0(x) = x^n + a_{n-1}^{(0)} x^{n-1} + \cdots + a_0^{(0)}.$$

5 Randomized coefficient interpolation

We now describe a randomized interpolation procedure between the split base polynomial h_0 and a polynomial expected to have large Galois group.

Let

$$h_1(x) = x^n + x + 1$$

be the Selmer-type polynomial. Write

$$h_1(x) = x^n + a_{n-1}^{(1)} x^{n-1} + \cdots + a_1^{(1)} x + a_0^{(1)}.$$

Also write

$$h_0(x) = x^n + a_{n-1}^{(0)} x^{n-1} + \cdots + a_1^{(0)} x + a_0^{(0)}$$

for the split base polynomial constructed above from $\alpha_i = i$ and $\beta_g = \prod_i \alpha_{g(i)}^i$.

For parameters

$$t_0, t_1, \ldots, t_{n-1}$$

define

$$b_i(t_i) = a_i^{(0)} t_i + (1 - t_i) a_i^{(1)} \qquad (0 \leq i \leq n-1).$$

Equivalently,

$$b_i(t_i) = a_i^{(1)} + t_i(a_i^{(0)} - a_i^{(1)}).$$

Then set

$$h(x; t_0, \dots, t_{n-1}) = x^n + \sum_{i=0}^{n-1} b_i(t_i) x^i.$$

For every rational choice of the parameters, this polynomial lies in $\mathbb{Q}[x]$.

5.1 The finite rational height box

There is no countably additive uniform probability measure on $\mathbb{Q} \cap [0,1]$. Therefore we work with a finite rational height box. For $B \geq 1$, define

$$\mathcal{T}_B = \left\{ \frac{u}{v} \in \mathbb{Q} \cap [0,1] : 0 \leq u \leq v, \gcd(u,v) = 1, 1 \leq v \leq B \right\}.$$

We choose

$$t_0, t_1, \dots, t_{n-1}$$

independently and uniformly from $\mathcal{T}_B$. Thus the probability space is

$$\Omega_B = \mathcal{T}_B^n.$$

Every point of Ω_B gives a rational polynomial

$$h(x; t_0, \dots, t_{n-1}) \in \mathbb{Q}[x].$$

5.2 The uniform mass on $\mathcal{T}_B$

For $v = 1$, the admissible fractions are

$$0 = \frac{0}{1}, \qquad 1 = \frac{1}{1}.$$

For $v \geq 2$, the reduced fractions with denominator v and lying in $[0,1]$ are precisely

$$\frac{u}{v}, \qquad 1 \leq u \leq v-1, \qquad \gcd(u,v) = 1.$$

There are $\varphi(v)$ such numerators. Hence

$$|\mathcal{T}_B| = 2 + \sum_{v=2}^{B} \varphi(v) = 1 + \sum_{v=1}^{B} \varphi(v).$$

Therefore each element of $\mathcal{T}_B$ has probability

$$p_B = \frac{1}{|\mathcal{T}_B|} = \frac{1}{1 + \sum_{v=1}^{B} \varphi(v)}.$$

Moreover,

$$\sum_{v=1}^{B} \varphi(v) \sim \frac{3}{\pi^2} B^2,$$

so

$$|\mathcal{T}_B| \sim \frac{3}{\pi^2} B^2, \qquad p_B \sim \frac{\pi^2}{3B^2}.$$

Since the n parameters are independent, every tuple in $\mathcal{T}_B^n$ has probability

$$\frac{1}{|\mathcal{T}_B|^n}.$$

6 The Bernoulli variables

Let

$$R_G(Y; b_0, \ldots, b_{n-1}) \in \mathbb{Q}[b_0, \ldots, b_{n-1}][Y]$$

be the absolute S_n/G-resolvent associated to the chosen primitive invariant. After substituting

$$b_i = b_i(t_i)$$

we obtain

$$R_G(Y; t_0, \ldots, t_{n-1}) := R_G(Y; b_0(t_0), \ldots, b_{n-1}(t_{n-1})) \in \mathbb{Q}[Y].$$

6.1 The resolvent Bernoulli variable

Define

$$X_B = \begin{cases} 1, & \text{if there exists } Y_0 \in \mathbb{Q} \text{ such that } R_G(Y_0; t_0, \ldots, t_{n-1}) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Thus X_B is a Bernoulli random variable on $\mathcal{T}_B^n$. The event $X_B = 1$ means that the randomly chosen polynomial has an S_n/G-resolvent with a rational root.

In a fully rigorous implementation one may refine this to a regular success event by also requiring that at least one rational root be simple:

$$R'_G(Y_0; t_0, \ldots, t_{n-1}) \neq 0.$$

This removes the exceptional collision locus of the resolvent.

6.2 The irreducibility Bernoulli variable

Define

$$Z_B = \begin{cases} 1, & \text{if } X_B = 1 \text{ and } h(x; t_0, \ldots, t_{n-1}) \text{ is irreducible over } \mathbb{Q}, \\ 0, & \text{otherwise.} \end{cases}$$

Optionally, one may include the non-collision condition for the rational resolvent root in the definition of $Z_B = 1$. Under this regularity condition, $Z_B = 1$ implies

$$\mathrm{Gal}(h/\mathbb{Q}) \cong G.$$

Indeed, the rational resolvent root forces the Galois group into a conjugate of G, and irreducibility makes it transitive. Since $|G| = n$, this containment must be equality.

Thus it is enough to prove

$$\mathbb{P}(Z_B = 1) > 0$$

for some height bound B. More ambitiously, one would like to prove

$$\liminf_{B \to \infty} \mathbb{P}(Z_B = 1) > 0.$$

6.3 Expectation of X_B

Since X_B is Bernoulli,

$$\mathbb{E}[X_B] = \mathbb{P}(X_B = 1).$$

Let

$$N_B = \#\left\{(t_0, \ldots, t_{n-1}) \in \mathcal{T}_B^n : \exists Y_0 \in \mathbb{Q} \text{ with } R_G(Y_0; t_0, \ldots, t_{n-1}) = 0\right\}.$$

Then

$$\mathbb{E}[X_B] = \mathbb{P}(X_B = 1) = \frac{N_B}{|\mathcal{T}_B|^n}.$$

Using

$$|\mathcal{T}_B| = 1 + \sum_{v=1}^{B} \varphi(v),$$

we obtain the exact formula

$$\mathbb{E}[X_B] = \frac{N_B}{\left(1 + \sum_{v=1}^{B} \varphi(v)\right)^n}.$$

For $B \gg 0$, since

$$|\mathcal{T}_B| \sim \frac{3}{\pi^2} B^2,$$

we get

$$\mathbb{E}[X_B] \sim \frac{N_B}{\left(\frac{3}{\pi^2} B^2\right)^n} = N_B \left(\frac{\pi^2}{3B^2}\right)^n.$$

6.4 A positive lower bound for $\mathbb{E}[X_B]$

The expectation of X_B is positive because the split base polynomial lies in the search space. Indeed, if

$$t_0 = t_1 = \cdots = t_{n-1} = 1,$$

then

$$b_i(1) = a_i^{(0)}$$

for all i, and hence

$$h(x; 1, \ldots, 1) = h_0(x).$$

But h_0 is completely split over $\mathbb{Q}$, so

$$\mathrm{Gal}(h_0/\mathbb{Q}) = C_1 \leq G.$$

Therefore the absolute S_n/G-resolvent of h_0 has a rational root, and so

$$X_B(1, \ldots, 1) = 1.$$

Since $1 \in \mathcal{T}_B$ for every $B \geq 1$, this gives

$$N_B \geq 1.$$

Consequently,

$$\mathbb{E}[X_B] = \frac{N_B}{|\mathcal{T}_B|^n} \geq \frac{1}{|\mathcal{T}_B|^n} > 0.$$

Equivalently,

$$\mathbb{E}[X_B] \geq \left(\frac{1}{1 + \sum_{v=1}^{B} \varphi(v)}\right)^n.$$

For $B \gg 0$, this lower bound is approximately

$$\mathbb{E}[X_B] \gtrsim \left(\frac{\pi^2}{3B^2}\right)^n.$$

This proves positivity for the resolvent Bernoulli variable. It does not prove positivity for Z_B, because the point $(1, \ldots, 1)$ gives the completely split polynomial h_0, which is reducible.

6.5 Conditional expectation of Z_B

We now condition on the resolvent-success event

$$X_B = 1.$$

Since $Z_B = 1$ implies $X_B = 1$, one has

$$Z_B \le X_B.$$

Conditional on $X_B = 1$, the random variable Z_B is again Bernoulli. Its expectation is

$$\mathbb{E}[Z_B \mid X_B = 1] = \mathbb{P}(Z_B = 1 \mid X_B = 1).$$

Let

$$M_B = \#\left\{(t_0, \dots, t_{n-1}) \in \mathcal{T}_B^n : X_B = 1 \text{ and } h(x; t_0, \dots, t_{n-1}) \text{ is irreducible over } \mathbb{Q}\right\}.$$

Then

$$\mathbb{P}(X_B = 1) = \frac{N_B}{|\mathcal{T}_B|^n}, \qquad \mathbb{P}(Z_B = 1) = \frac{M_B}{|\mathcal{T}_B|^n}.$$

Therefore

$$\mathbb{E}[Z_B \mid X_B = 1] = \frac{\mathbb{P}(Z_B = 1)}{\mathbb{P}(X_B = 1)} = \frac{M_B}{N_B}.$$

Thus the conditional expectation is exactly the proportion of resolvent-successful choices that produce an irreducible polynomial.

7 Bounding reducibility by degree partitions

Let

$$\Omega_B^X = \{(t_0, \dots, t_{n-1}) \in \mathcal{T}_B^n : X_B = 1\}$$

be the resolvent-successful sample space. Then

$$|\Omega_B^X| = N_B.$$

For $\omega \in \Omega_B^X$, write

$$h_\omega(x) = h(x; t_0, \dots, t_{n-1}).$$

If h_ω is reducible over $\mathbb{Q}$, then it has a factorization

$$h_\omega(x) = f_1(x) \cdots f_r(x)$$

into monic irreducible factors over $\mathbb{Q}$, with

$$\deg f_1 + \cdots + \deg f_r = n, \qquad 1 \le \deg f_j < n.$$

Thus every reducible polynomial determines a nontrivial partition of n,

$$\lambda = (d_1, \dots, d_r), \qquad d_1 + \cdots + d_r = n, \qquad r \ge 2.$$

Let $p(n)$ denote the partition function. The trivial partition (n) corresponds to the irreducible case. Hence the number of possible reducible degree patterns is $p(n) - 1$.

For each nontrivial partition $\lambda \vdash n$, define

$$\Omega_{B,\lambda}^X = \{\omega \in \Omega_B^X : h_\omega(x) \text{ has irreducible factor degrees given by } \lambda\}.$$

Then

$$\Omega^X_{B,\mathrm{red}} = \bigcup_{\substack{\lambda \vdash n \\ \lambda \neq (n)}} \Omega^X_{B,\lambda}.$$

By the union bound,

$$|\Omega^X_{B,\mathrm{red}}| \leq \sum_{\substack{\lambda \vdash n \\ \lambda \neq (n)}} |\Omega^X_{B,\lambda}|.$$

In particular,

$$|\Omega^X_{B,\mathrm{red}}| \leq (p(n)-1) \max_{\substack{\lambda \vdash n \\ \lambda \neq (n)}} |\Omega^X_{B,\lambda}|.$$

Dividing by N_B, we get

$$\mathbb{P}(h_\omega \text{ reducible over } \mathbb{Q} \mid X_B = 1) \leq (p(n)-1) \max_{\substack{\lambda \vdash n \\ \lambda \neq (n)}} \frac{|\Omega^X_{B,\lambda}|}{N_B}.$$

Since

$$\mathbb{E}[Z_B \mid X_B = 1] = 1 - \mathbb{P}(h_\omega \text{ reducible over } \mathbb{Q} \mid X_B = 1),$$

we obtain

$$\mathbb{E}[Z_B \mid X_B = 1] \geq 1 - (p(n)-1) \max_{\substack{\lambda \vdash n \\ \lambda \neq (n)}} \frac{|\Omega^X_{B,\lambda}|}{N_B}.$$

Thus, if for all nontrivial λ

$$\frac{|\Omega^X_{B,\lambda}|}{N_B} \leq \varepsilon_B,$$

then

$$\mathbb{E}[Z_B \mid X_B = 1] \geq 1 - (p(n)-1)\varepsilon_B.$$

In particular, if

$$(p(n)-1)\varepsilon_B < 1,$$

then

$$\mathbb{E}[Z_B \mid X_B = 1] > 0.$$

8 The Hardy–Ramanujan scale and the choice of $B(n)$

The partition function satisfies the Hardy–Ramanujan asymptotic formula

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

Thus, for large n,

$$p(n) - 1 \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

Put

$$Q_B := |\mathcal{T}_B|.$$

Then

$$Q_B \sim \frac{3}{\pi^2} B^2.$$

Suppose that, for some effective dimension κ and codimension saving $\delta > 0$, there are estimates

$$N_B \geq c_n Q_B^\kappa$$

and, for every nontrivial partition $\lambda \neq (n)$,

$$|\Omega^X_{B,\lambda}| \leq C_n Q_B^{\kappa-\delta}.$$

Then

$$\frac{|\Omega^X_{B,\lambda}|}{N_B} \leq \frac{C_n}{c_n} Q_B^{-\delta}.$$

Consequently,

$$\mathbb{E}[Z_B \mid X_B = 1] \geq 1 - (p(n)-1)\frac{C_n}{c_n} Q_B^{-\delta}.$$

It is enough to choose $B = B(n)$ so that

$$(p(n)-1)\frac{C_n}{c_n} Q_B^{-\delta} < 1.$$

Using $Q_B \sim (3/\pi^2)B^2$, this condition is approximately

$$(p(n)-1)\frac{C_n}{c_n}\left(\frac{3}{\pi^2}B^2\right)^{-\delta} < 1.$$

Equivalently, a sufficient scale is

$$B(n) \gg \left((p(n)-1)\frac{C_n}{c_n}\right)^{1/(2\delta)}.$$

By Hardy–Ramanujan, this suggests

$$B(n) \gg \left(\frac{C_n}{c_n}\frac{1}{4n\sqrt{3}}\exp\left(\pi\sqrt{\frac{2n}{3}}\right)\right)^{1/(2\delta)}.$$

If C_n/c_n grows moderately and $\delta = 1$, the natural scale becomes

$$B(n) \gg \frac{1}{2\cdot 3^{1/4}\sqrt{n}}\exp\left(\frac{\pi}{2}\sqrt{\frac{2n}{3}}\right).$$

9 A counting conjecture for the resolvent-successful locus

We formulate the counting input needed for the Erdős-type argument.

Conjecture 9.1 (Resolvent-success counting and factorization saving)**.** *Let $G \leq S_n$ be a regular subgroup of order n, and let Ω^X_B be the resolvent-successful sample space associated to the coefficient interpolation construction above. Put*

$$N_B := |\Omega^X_B|.$$

Then there exist constants

$$\kappa = \kappa(G) > 0, \qquad \delta = \delta(G) > 0,$$

and positive constants

$$c_G, C_G > 0$$

such that, for all sufficiently large B,

$$N_B \geq c_G |\mathcal{T}_B|^{\kappa}.$$

Moreover, for every nontrivial partition

$$\lambda \vdash n, \qquad \lambda \neq (n),$$

the number $R_{B,\lambda} = |\Omega^X_{B,\lambda}|$ *of resolvent-successful choices whose polynomial has factorization type* λ *satisfies*

$$R_{B,\lambda} \leq C_G |\mathcal{T}_B|^{\kappa-\delta}.$$

Equivalently, each nontrivial factorization stratum has a uniform power saving inside the resolvent-successful locus.

Under this conjecture, the reducible locus is negligible after choosing $B = B(n)$ sufficiently large compared with the partition count $p(n)$. Consequently, the conditional expectation

$$\mathbb{E}[Z_B \mid X_B = 1]$$

is positive for a suitable height bound B, and hence the probabilistic method produces a rational polynomial with Galois group G.

10 Algorithmic form for small experiments

For small values of n, the finite experiment can be implemented directly. The steps are:

1. Fix a regular subgroup $G \leq S_n$.
2. Build the split base polynomial by setting $\alpha_i = i$ and
$$\beta_g = \prod_{i=1}^{n} \alpha_{g(i)}^i, \qquad h_0(x) = \prod_{g \in G} (x - \beta_g).$$
3. Set $h_1(x) = x^n + x + 1$.
4. Interpolate coefficients by
$$b_i(t_i) = a_i^{(0)} t_i + (1 - t_i) a_i^{(1)}.$$
5. For each tuple $(t_0, \ldots, t_{n-1}) \in \mathcal{T}_B^n$, compute
$$h(x; t_0, \ldots, t_{n-1})$$
and its absolute S_n/G-resolvent
$$R_G(Y; t_0, \ldots, t_{n-1}).$$
6. Set $X_B = 1$ if the resolvent has a rational root.
7. Set $Z_B = 1$ if additionally the polynomial is irreducible over $\mathbb{Q}$ and, if required, the rational resolvent root is simple.

The split tuple $(1, \ldots, 1)$ always contributes to $X_B = 1$. The core experimental and theoretical question is whether, after conditioning on $X_B = 1$, the irreducible choices have positive density or at least occur for some finite height bound B.