

# The First Ramseyian Theorem and its Application: The Hilbert Cube Lemma and the Hilbert's Irreducibility Theorem

Mark B. Villarino - Universidad de Costa Rica  
William Gasarch - University of MD  
Ken Regan - University of Buffalo

# Credit where Credit is Due

This talk is based on

Hilbert's Proof of his Irreducibility Theorem  
by Villarino, Gasarch, Regan  
American Mathematics Monthly  
Vol 125, No. 6, 2018, Pages 513–530  
<http://arxiv.org/abs/1611.06303>  
Or Just Google Gasarch Hilbert

This talk emphasizes the Ramsey Connection

# Brief History of Early Ramsey Theory I

- 1) 1894: Hilbert proves **Hilbert Cube Lemma (HCL)**

**App:** The Hilbert Irreducibility Theorem (HIT)

Hilbert viewed **HCL** as a means to an end so he  
did not launch what is now called Ramsey Theory :-)

- 2) 1926: Schur proves **Schur's Theorem (ST)**:

$\forall$  finite cols of  $\mathbb{N}$   $(\exists x, y, z)$  mono,  $x + y = z$ .

**App:**  $(\forall n)(\forall^\infty p)(\exists x, y, z \neq 0(p))[x^n + y^n \equiv z^n(p)]$ ,

Hence showed that FLT cannot be solved modularly.

Schur viewed **ST** as a means to an end so he  
did not launch what is now called Ramsey Theory :-)

# Brief History of Early Ramsey Theory II

- 3) 1927: Van der Waerden proves **Van der Waerden's theorem (VDW)** to resolve conjecture of Baudet and Schur.

**App** None.

Van der Waerden viewed **VDW** as an isolated problem so he **did not launch what is now called Ramsey Theory** :-)

## Brief History of Early Ramsey Theory III

4) 1930: Ramsey proves **Ramsey's theorem (RT)**.

**App:** Given a sentence about hypergraphs:

$$\phi = (\exists \vec{x})(\forall \vec{y})[\psi(\vec{x}, \vec{y})]$$

can determine all  $n$  such that there is a hypergraph on  $n$  vertices that satisfies  $\phi$ .

Ramsey died in 1930 so he

**did not launch what is now called Ramsey Theory :-)**

He likely viewed RT as a means to an end so I suspect he **would not have launched what is now called Ramsey Theory :-)**  
(Irony?)

## Brief History of Early Ramsey Theory IV

- 5) 1931: Rado proves **Rado's Theorem (RaT)** which gives a condition on a linear equation such that any finite coloring of  $\mathbb{N}$  yields a mono solution.

**App:** None, but a great result in and of itself.

Rado did see importance of **RaT** but still

did not launch what is now called Ramsey Theory :-)

**Note:** Later, with Erdos, Can Ram,  $R(k) \leq 2^{2^{4k}}$ ,  $\infty$ -Ram

- 6) 1935: Erdos-Szekeres rediscover **RT**.

**App:**  $(\forall n)(\exists KLEIN(n))$  such that  $\forall$  sets of  $KLEIN(n)$  points in the plane in general position  $\exists n$  points that form a convex  $n$ -gone.

Erdos viewed **RT** as important so he

did launch what is now called Ramsey Theory :-)

Yeah!

# We Fill a Gap in the Literature

The theorems and-or applications of Schur, Van der Waerden, Rado, Erdos-Szekeres are well known, well documented, and available in English in modern mathematical language.

The theorems and applications of Ramsey have not been written up in modern mathematical language but is in English and isn't that hard. (I may have a writeup of that for RATLOCC 2020!)

The theorems and application of Hilbert were (until now) only available in German and not written up in modern mathematical language.

**We rectify that!**

# Hilbert's Irreducibility Theorem (HIT)

**Notation:** Throughout this talk  $t$  ranges over  $\mathbb{N}$ .

**Theorem:** Let  $f(x, y) \in \mathbb{Z}[x, y] - \mathbb{Z}[x]$ . Assume

$$(\forall^\infty t)[f(x, t) \text{ is reducible in } \mathbb{Z}[x]].$$

Then  $f(x, y)$  is reducible in  $\mathbb{Q}[x, y]$ .

Hilbert proved this in 1894.

He proved and used **The Hilbert Cube Lemma (HCL)**

**HCL** is retrospectively the first Ramseyian Theorem

**HIT** is retrospectively the first app of a Ramseyian Theorem



# Applications of HIT

**Theorem 1:** Let  $f(x) \in \mathbb{Z}[x]$ . If  $(\exists^\infty t)[f(t) \in SQ]$  then there exists  $g(x) \in \mathbb{Z}[x]$  such that  $f(x) = g(x)^2$ .

**Theorem 2:** For all  $n \in \mathbb{N}$  there are an infinite number of  $f(x) \in \mathbb{Z}[x]$  that have Galois group  $S_n$  (and hence for  $n \geq 5$  are not solvable by radicals).

**Note:** Galois groups were Hilbert's motivation for HIT.

HIT is an app of HCL.

Theorem 1 is an app of HIT

By transitivity,

Theorem 1 an app of HCL

# Puiseux's Theorem

**Theorem:** Let  $f(x, y) \in \mathbb{C}[x, y]$ . Assume that  $x$  has degree  $d$ .

Then there exists  $r_1(y), \dots, r_d(y)$  such that:

- 1) For all  $t \in \mathbb{C}$  the roots of  $f(x, t)$  are  $r_1(t), \dots, r_d(t)$ .
- 2) There exists  $m, k$  such that the  $r_i(y)$ 's are all of the form:

$$A_m y^{m/k} + A_{m-1} y^{(m-1)/k} + \dots + A_1 y^{1/k} + A_0 + \frac{B_1}{y^{1/k}} + \frac{B_2}{y^{2/k}} + \dots$$

These are called **Puiseux Series (P-Series)**

**Note:** If the degree of  $x$  in  $f(x, y)$  is  $m_x$  and the degree of  $y$  in  $f(x, y)$  is  $m_y$  then  $m, k$  are bounded by

# Puiseux's Theorem

**Theorem:** Let  $f(x, y) \in \mathbb{C}[x, y]$ . Assume that  $x$  has degree  $d$ .

Then there exists  $r_1(y), \dots, r_d(y)$  such that:

- 1) For all  $t \in \mathbb{C}$  the roots of  $f(x, t)$  are  $r_1(t), \dots, r_d(t)$ .
- 2) There exists  $m, k$  such that the  $r_i(y)$ 's are all of the form:

$$A_m y^{m/k} + A_{m-1} y^{(m-1)/k} + \dots + A_1 y^{1/k} + A_0 + \frac{B_1}{y^{1/k}} + \frac{B_2}{y^{2/k}} + \dots$$

These are called **Puiseux Series (P-Series)**

**Note:** If the degree of  $x$  in  $f(x, y)$  is  $m_x$  and the degree of  $y$  in  $f(x, y)$  is  $m_y$  then  $m, k$  are bounded by

some function of  $m$  and  $k$ ? What function! I don't know! I can't find the answer on the web! I can't even find the question! If you know then please tell me!

# Hilbert Irreducibility Theorem

**Theorem:** Let  $f(x, y) \in \mathbb{Z}[x, y] - \mathbb{Z}[x]$ . Assume

$$(\forall^\infty t)[f(x, t) \text{ is reducible in } \mathbb{Z}[x]].$$

Then  $f(x, y)$  is reducible in  $\mathbb{Q}[x, y]$ .

**Proof:**

$r_1(y), \dots, r_d(y)$  are the P-series for  $f(x, y)$ .

Simplifying assumptions for this talk:

- 1)  $f(x, y)$  is monic, and
- 2) P-series have  $k = 1$ . Hence the  $r_i(y)$ 's are of the form

$$A_m y^m + A_{m-1} y^{m-1} + \dots + A_1 y + A_0 + \frac{B_1}{y} + \frac{B_2}{y^2} + \dots$$

# Even More Simplifying Assumptions for This Talk

We assume:

1. Degree of  $x$  in  $f(x, y)$  is 7.
2.  $r_1, \dots, r_7$  each have poly-part degree  $\leq$  BLAH.
3. Note for later: Let  $S(z_1, z_2, z_3)$  be any of

$$S(z_1, z_2, z_3) = z_1 + z_2 + z_3$$

$$S(z_1, z_2, z_3) = z_1 z_2 + z_1 z_3 + z_2 z_3$$

$$S(z_1, z_2, z_3) = z_1 z_2 z_3$$

Then  $S(r_1(y), r_2(y), r_3(y))$  (or any other 3  $r_i$ 's) is a  $P$ -series with poly-part of degree  $\leq 3 \times$  BLAH which we call  $n$ .

## We Color Almost all $t$

Recall that  $\forall^\infty t$   $f(x, t)$  is reducible over  $\mathbb{Z}$ ; fix some such  $t$ .

$$f(x, t) = g_t(x)h_t(x) \text{ where } g_t(x), h_t(x) \in \mathbb{Z}[x]$$

$g_t(x)$  has roots  $r_1(t), r_3(t), r_4(t)$ .

Color  $t$  with one of  $(1, 3, 4)$  or  $(2, 5, 6, 7)$ .

## Symmetric Functions of the $r_i$ are in $\mathbb{Z}$

$f(x, t) = g_t(x)h_t(x)$  where  $g_t(x), h_t(x) \in \mathbb{Z}[x]$

$g_t(x)$  has roots  $r_1(t), r_3(t), r_4(t)$ .

Since  $g_t(x)$  has roots  $r_1(t), r_3(t), r_4(t)$  the coefficients of  $g_t(x)$  are symmetric functions in  $r_1(t), r_3(t), r_4(t)$ .

# Some Color Appears Infinitely Often!

Some color appears infinitely often.

**Simplifying Assumption For This Talk:** That color is  $(1, 3, 4)$

So  $\exists^\infty t$

1.  $f(x, t) = g_t(x)h_t(x)$ , and

2.  $g_t(x) = (x - r_1(t))(x - r_3(t))(x - r_4(t)) \in \mathbb{Z}[x]$

Let  $S_1, S_2, S_3$  be the elementary Symmetric Functions. Then

$$(x - r_1(y))(x - r_3(y))(x - r_4(y)) =$$

$$x^3 - S_1(r_1(y), r_3(y), r_4(y))x^2 + S_2(r_1(y), r_3(y), r_4(y))x$$

$$- S_3(r_1(y), r_3(y), r_4(y))$$

Hence for  $i = 1, 2, 3$ :

$$(\exists^\infty t)[S_i(r_1(t), r_3(t), r_4(t)) \in \mathbb{Z}]$$



## Symmetric Functions of the Roots

$$(x - r_1(y))(x - r_3(y))(x - r_4(y)) = \\ x^3 - S_1(r_1(y), r_3(y), r_4(y))x^2 + S_2(r_1(y), r_3(y), r_4(y))x \\ - S_3(r_1(y), r_3(y), r_4(y))$$

$$(\exists^\infty t)[S_i(r_1(t), r_3(t), r_4(t)) \in \mathbb{Z}]$$

**Key:**  $S_i(r_1(y), r_3(y), r_4(y))$  is a P-series of degree  $n$ .

**Want:** If  $S$  is a P-series and  $(\exists^\infty t)[S(t) \in \mathbb{Z}]$  then  $S$  is a polynomial.

**IF** for  $i = 0, 1, 2$ ,  $S_i(r_1(y), r_2(y), r_3(y)) \in \mathbb{C}[y]$

Assume for  $i = 0, 1, 2$   $S_i(r_1(y), r_2(y), r_3(y)) = T_i(y) \in \mathbb{C}[y]$ .

Then for  $j = 0, 1, 2, 3$  there exists  $U_j(y) \in \mathbb{C}[y]$  such that:

$\exists^\infty t$

$$f(x, t) = (x^3 + T_2(t)x^2 + T_1(t)x + T_0(t)) \times$$

$$(x^4 + U_3(t)x^3 + U_2(t)x^2 + U_1(t)x + U_0(t))$$

AND

For  $i = 0, 1, 2$ , for  $j = 0, 1, 2, 3$ ,  $T_i(t) \in \mathbb{Z}$ ,  $U_j(t) \in \mathbb{Z}$

Number-of-Roots-argument and interpolation shows:

$$f(x, y) = (x^3 + T_2(y)x^2 + T_1(y)x + T_0(y)) \times$$

$$(x^4 + U_3(y)x^3 + U_2(y)x^2 + U_1(y)x + U_0(y))$$

where both factors are in  $\mathbb{Z}[x, y]$ .

# What we Want, What we Really Really Want

Want

**Theorem** Let  $S(y)$  be a P-series.

If  $(\exists^\infty t)[S(t) \in \mathbb{Z}]$  then  $S(y) \in \mathbb{C}[y]$ .

# What we Want, What we Really Really Want

Want

**Theorem** Let  $S(y)$  be a P-series.

If  $(\exists^\infty t)[S(t) \in \mathbb{Z}]$  then  $S(y) \in \mathbb{C}[y]$ .

Sounds Reasonable.

# What we Want, What we Really Really Want

Want

**Theorem** Let  $S(y)$  be a P-series.

If  $(\exists^\infty t)[S(t) \in \mathbb{Z}]$  then  $S(y) \in \mathbb{C}[y]$ .

Sounds Reasonable.

Prob not true. Neither Hilbert nor I could prove it.

# What we Want, What we Really Really Want

Want

**Theorem** Let  $S(y)$  be a P-series.

If  $(\exists^\infty t)[S(t) \in \mathbb{Z}]$  then  $S(y) \in \mathbb{C}[y]$ .

Sounds Reasonable.

Prob not true. Neither Hilbert nor I could prove it.

Go back to the coloring.

The condition  $(\exists^\infty t)[COL(t) = (1, 3, 4)]$  is not strong enough.

# Our Will is Strong, Our Premise is Weak

The premise:

$$(\exists^\infty t)[S(t) \in \mathbb{Z}]$$

is too weak. The  $t$  could be anything. No pattern. Need a more structured set of naturals where  $S(t) \in \mathbb{Z}$ .

## Definition of an $n$ -Cube

**Definition:** Let  $n \in \mathbb{N}$ . Let  $t, \mu_1, \dots, \mu_n \in \mathbb{N}$ .  $CUBE(t; \mu_1, \dots, \mu_n)$  is the set:

$$\{t + b_1\mu_1 + \dots + b_n\mu_n : b_1, \dots, b_n \in \{0, 1\}\}.$$

**Example:**  $CUBE(t; \mu_1, \mu_2, \mu_3)$  is

$$\begin{aligned} & \{t\} \cup \\ & \{t + \mu_1, t + \mu_2, t + \mu_3\} \cup \\ & \{t + \mu_1 + \mu_2, t + \mu_1 + \mu_3, t + \mu_2 + \mu_3\} \cup \\ & \{t + \mu_1 + \mu_2 + \mu_3\} \end{aligned}$$



# Hilbert Cube Lemma

**HCL:**  $n \in \mathbb{N}$ .  $COL$  a finite coloring of  $\mathbb{N}$ .

$$(\exists c)(\exists \mu_1, \dots, \mu_n \in \mathbb{N})$$

$$(\exists^\infty t')(\forall t \in CUBE(t'; \mu_1, \dots, \mu_{n+1}))[COL(t) = c].$$

1. Today can prove from VDW's theorem.
2. Hilbert proved from scratch.
3. Hilbert's proof is a typical Ramsey-Theoretic Argument (now).
4. How typical?

**Prove HCL without using VDW's Theorem**

was on take home final of my Graduate Ramsey Theory course. 20 out of 22 students got it right.

## Back to Our Coloring

We color almost all  $t$  as before.

Apply HCL with  $n + 1$  (one more than highest  $\deg(S_i)$ ) to get  
 $(\exists \mu_1, \dots, \mu_{n+1})(\forall i = 1, 2, 3)$

$$(\exists^\infty t)[T_i(t + b_1\mu_1 + \dots + b_{n+1}\mu_{n+1}) \in \mathbb{Z}]$$

$(b_i \in \{0, 1\})$

$T_i$  is coefficient of  $g_y(x)$ .  $T_i$  is a P-series.

## New Goal

Let  $T_0(y)$  be a P-series of degree  $n$ . Assume there exist  $\mu_1, \dots, \mu_{n+1}$  such that

$$(\exists^\infty t)[T_0(t + b_1\mu_1 + \dots + b_{n+1}\mu_{n+1}) \in \mathbb{Z}]$$

$$(b_i \in \{0, 1\})$$

then  $T_0 \in \mathbb{C}[y]$ .

## You're an Integer! And You're An Integer!

$$T_0(y) = A_n y^n + A_{n-1} y^{n-1} + \cdots + A_1 y + A_0 + \frac{B_1}{y} + \frac{B_2}{y^2} + \cdots$$

Assume, BWOC that  $(\exists i)[B_i \neq 0]$ . For this talk  $B_1 \neq 0$ .

$$(\exists^\infty t)[T_0(t) \in \mathbb{Z} \wedge T_0(t + \mu_1) \in \mathbb{Z}]$$

$$T_1(y) = T_0(y + \mu_1) - T_0(y)$$

$$(\exists^\infty t)[T_1(t) \in \mathbb{Z}]$$

$$T_2(y) = T_1(y) - T_1(y + \mu_2)$$

$$(\exists^\infty t)[T_2(t) \in \mathbb{Z}]$$

Etc down to  $T_n$ .

What happens to the poly part? The non-poly part?

## The Poly Part

$$T_0(y) = A_n y^n + A_{n-1} y^{n-1} + \cdots + A_1 y + A_0 + \frac{B_1}{y} + \frac{B_2}{y^2} + \cdots$$

$$T_0(y) = L_0(y) + \frac{B_1}{y} + \frac{B_2}{y^2} + \cdots \quad \deg(L_0) = n$$

$$T_1(y) = T_0(y + \mu_1) - T_0(y) = L_1(y) + \text{non poly stuff}, \quad \deg(L_1) = n - 1$$

$$T_2(y) = T_1(y + \mu_2) - T_1(y) = L_2(y) + \text{non poly stuff}, \quad \deg(L_2) = n - 2$$

etc.

$$T_n(y) = T_{n-1}(y + \mu_n) - T_{n-1}(y) = L_n(y) + \text{non poly stuff}, \quad \deg(L_n) = 0$$

Continued on next page

# The Poly Part

$$T_n(y) = T_{n-1}(y + \mu_n) - T_{n-1}(y) = L_n(y) + \text{non poly stuff}, \deg(L_n) = 0$$

So  $L_n(y)$  is a constant which we call  $c$ .

$$T_{n+1}(y) = T_n(y + \mu_{n+1}) - T_n(y) = \text{non poly stuff},$$

**Upshot:**  $T_{n+1}$  only has non-poly stuff.

**Recall:**  $(\exists^\infty t)[T_{n+1}(t) \in \mathbb{Z}]$

(We use later.)

## The Non-Poly Part

$$T_0(y) = A_n y^n + A_{n-1} y^{n-1} + \dots + A_1 y + A_0 + \frac{B_1}{y} + \frac{B_2}{y^2} + \dots$$

$$T_0(y) = L_0(y) + \frac{B_1}{y} + O\left(\frac{1}{y^2}\right)$$

For now ignore terms of order  $<$  the first term of nonpoly part.

$$T_1(y) = T_0(y + \mu_1) - T_0(y) = L_1(y) + M_1(y)$$

$$M_1(y) = B_1 \left( \frac{1}{y + \mu_1} - \frac{1}{y} \right) = B_1 \mu_1 \frac{1}{y(y + \mu_1)}$$

## The Non-Poly Part

$$T_2(y) = T_1(y + \mu_2) - T_1(y) = L_2(y) + M_2(y)$$

$$\begin{aligned} M_2(y) &= B_1 \mu_1 \left( \frac{1}{(y + \mu_2)(y + \mu_1 + \mu_2)} - \frac{1}{y(y + \mu_1)} \right) \\ &= B_1 \mu_1 \mu_2 \left( \frac{2y + \mu_1 + \mu_2}{(y + \mu_2)(y + \mu_1 + \mu_2)(y(y + \mu_1))} \right) \end{aligned}$$

...

$$M_{n+1}(y) = B_1 \mu_1 \cdots \mu_{n+1} \frac{p(y)}{q(y)}, \quad \deg(q(y)) > \deg(p(y))$$

Since  $T_{n+1}(y)$  only has non-poly part,  $T_{n+1}(y) = M_{n+1}(y)$ , so

$$(\exists^\infty t) [B_1 \mu_1 \cdots \mu_{n+1} \frac{p(t)}{q(t)} \in \mathbb{Z}]$$

$B_1$  must be 0. Contradiction!



## Recap

- 1) Color almost all  $t \in \mathbb{N}$  with the factorization of  $f(x, t)$ .
- 2) By HCL get cubes of  $t$  with same factorization of  $f(x, t)$ .
- 3) For  $t$  in a cube,  $f(x, t) = g_t(x)h_t(x)$  with  $g_t, h_t \in \mathbb{Z}[x]$ .
- 4) Coefficients are symm functions of roots.
- 5) Coeffs of  $g_y(x)$  are  $S(y)$ , symm function of roots, so P-series.
- 6) For  $t$  in a cube,  $S(t) \in \mathbb{Z}$ .
- 7) ( $S$  a P-series,  $t$  in a cube set  $\implies S(t) \in \mathbb{Z}$ )  $\implies S(y) \in \mathbb{C}[y]$ .
- 8) Number-of-roots, interpolation:  $f(x, y) = g_y(x)h_y(x)$ .

# HIT 1890's

## HIT: Hilbert's Version

**Intuition:** If there are LOTS of  $t$  with  $f(x, t)$  reducible then  $f(x, y)$  is reducible. LOTS means Infinite.

**Theorem:** Let  $f(x, y) \in \mathbb{Z}[x, y] - \mathbb{Z}[x]$ . Assume

$$(\forall^\infty t)[f(x, t) \text{ is reducible in } \mathbb{Z}[x]].$$

Then  $f(x, y)$  is reducible in  $\mathbb{Q}[x, y]$ .

# HIT 1990's

## HIT: Modern Quantitative Version

**Intuition:** If there are LOTS of  $t$  with  $f(x, t)$  reducible then  $f(x, y)$  is reducible. LOTS means a large subset of  $\{-N, \dots, N\}$ .

**Definition:**  $|f|$  is the max abs val of coefficient.

**Theorem:**  $\exists$  function  $c(d)$  such that if  $f(x, y) \in \mathbb{Z}[x, y] - \mathbb{Z}[x]$  has degree  $d$ ,  $N \gg |f|^{c(d)}$ , and

$$|\{t : t \in \{-N, \dots, N\}, f(x, t) \text{ is reducible}\}| \geq |f|^{c(d)} \sqrt{N} \log N$$

then  $f(x, y)$  is reducible in  $\mathbb{Q}[x, y]$ .

**Note:** Sharper versions depend on the Galois Group of  $f$ .

# That was Then, This is Now: HCL

**Definition**  $H(n, c)$  is the least  $H$  such that for any  $c$ -coloring of  $[H]$  there is a mono  $n$ -cube.

Bounds on  $H(n, c)$  then and now:

**Hilbert's Bound:**

$$H(n, c) \leq \text{TOW}_{O(c)}(O(n))$$

**Gunderson and Rodl:**

$$c^{\Omega(2^n/n)} \leq H(n, c) \leq (2c)^{2^{n-1}}$$

**Application:** Graham-Rothchild-Spencer presentation of Szemerédi density for  $k = 3$  uses Gunderson-Rodl bounds on  $H(n, c)$ .

# Coda

Too bad Hilbert didn't pursue Theorems about coloring.

# Coda

Too bad Hilbert didn't pursue Theorems about coloring.

He could have been famous!