The Evelyn Nelson Lectures

2020-2021 Lecture

Friday, March 5, 2021
3:30 - 4:30 pm
Virtual

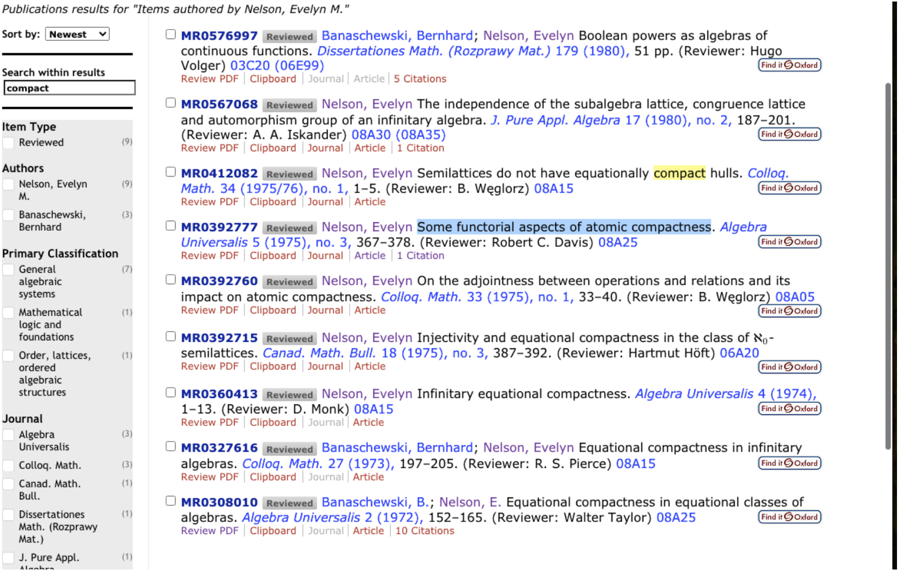
Ehud Hrushovski
University of Oxford

Title of Talk: ***On the logic of finite fields (with an additive character.)***

Evelyn M. Nelson

1943 - 1987

Dr. Evelyn Nelson was a member of the Department at the time of her death in 1987. In her memory and in recognition of her contributions to the University and the Mathematical Community, the Department, with the generous support of her many friends and colleagues, established the Evelyn Nelson Lecture Series. This lecture series has focused on matters relating to the Foundations of Mathematics.



Publications results for "Items authored by Nelson, Evelyn M."

Sort by: Newest

Search within results

compact

Item Type

□ Reviewed (9)

Authors

□ Nelson, Evelyn M. (9)

□ Banaschewski, Bernhard (3)

Primary Classification

□ General algebraic systems (7)

□ Mathematical logic and foundations (1)

□ Order, lattices, ordered algebraic structures (1)

Journal

□ Algebra Universalis (3)

□ Colloq. Math. (3)

□ Canad. Math. Bull. (1)

□ Dissertationes Math. (Rozprawy Mat.) (1)

□ J. Pure Appl. Algebra

□ **MR0576997** Reviewed Banaschewski, Bernhard; Nelson, Evelyn Boolean powers as algebras of continuous functions. *Dissertationes Math. (Rozprawy Mat.)* 179 (1980), 51 pp. (Reviewer: Hugo Volger) 03C20 (06E99)
Review PDF | Clipboard | Journal | Article | 5 Citations
Find it Oxford

□ **MR0567068** Reviewed Nelson, Evelyn The independence of the subalgebra lattice, congruence lattice and automorphism group of an infinitary algebra. *J. Pure Appl. Algebra* 17 (1980), no. 2, 187–201. (Reviewer: A. A. Iskander) 08A30 (08A35)
Review PDF | Clipboard | Journal | Article | 1 Citation
Find it Oxford

□ **MR0412082** Reviewed Nelson, Evelyn Semilattices do not have equationally compact hulls. *Colloq. Math.* 34 (1975/76), no. 1, 1–5. (Reviewer: B. Węglorz) 08A15
Review PDF | Clipboard | Journal | Article
Find it Oxford

□ **MR0392777** Reviewed Nelson, Evelyn Some functorial aspects of atomic compactness. *Algebra Universalis* 5 (1975), no. 3, 367–378. (Reviewer: Robert C. Davis) 08A25
Review PDF | Clipboard | Journal | Article | 1 Citation
Find it Oxford

□ **MR0392760** Reviewed Nelson, Evelyn On the adjointness between operations and relations and its impact on atomic compactness. *Colloq. Math.* 33 (1975), no. 1, 33–40. (Reviewer: B. Węglorz) 08A05
Review PDF | Clipboard | Journal | Article
Find it Oxford

□ **MR0392715** Reviewed Nelson, Evelyn Injectivity and equational compactness in the class of $\aleph_0$-semilattices. *Canad. Math. Bull.* 18 (1975), no. 3, 387–392. (Reviewer: Hartmut Höft) 06A20
Review PDF | Clipboard | Journal | Article
Find it Oxford

□ **MR0360413** Reviewed Nelson, Evelyn Infinitary equational compactness. *Algebra Universalis* 4 (1974), 1–13. (Reviewer: D. Monk) 08A15
Review PDF | Clipboard | Journal | Article
Find it Oxford

□ **MR0327616** Reviewed Banaschewski, Bernhard; Nelson, Evelyn Equational compactness in infinitary algebras. *Colloq. Math.* 27 (1973), 197–205. (Reviewer: R. S. Pierce) 08A15
Review PDF | Clipboard | Journal | Article
Find it Oxford

□ **MR0308010** Reviewed Banaschewski, B.; Nelson, E. Equational compactness in equational classes of algebras. *Algebra Universalis* 2 (1972), 152–165. (Reviewer: Walter Taylor) 08A25
Review PDF | Clipboard | Journal | Article | 10 Citations
Find it Oxford

Interpretations preserving atomic compactness — positive logic. I will use today a very well-behaved special case, *continuous logic*.

General atomic compactness recently used critically for a general structure theorem on approximate subgroups, and approximate lattices in semi-simple Lie groups.

Model theory compactifies classes of structures, adding nonstandard elements with the same theory. This allows studying asymptotic or general properties of the original class by investigating single elements of the boundary.

Finite fields $\mathbb{F}_p$ pseudo-finite field F.

(F looks like $\mathbb{F}_p$ for large p).

Trouble is that *everything* changes. If we want to study an additive character

$$\Psi_p : \mathbb{F}_p \to \mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$$

$$\Psi : F \to \mathbb{T}^*$$

However, $\mathbb{T}$ is *atomic compact*: there exists a retraction

$$\mathbb{T}^* \to \mathbb{T}$$

In this case, canonically. This allows another limit operation, where $\mathbb{F}_p \rightsquigarrow F$ while $\mathbb{T}$ stays put: $\Psi : F \to \mathbb{T}$. This special case is *continuous logic*.

Foundations.

Mathematical assertions represented as formulas. Clear conditions for truth in a model, and for validity of arguments.

An exponential 'tree' of statements St. An exponential 'tree' of proofs. Prf. A map $Prf \to St$.

Gödel: This map is not surjective

Now the problem becomes to explain why anything *is* provable.

A priori, one would expect the image to be tiny (though this is hard to quantify.)

Mathematical experience is otherwise: people expect to be able to prove, or disprove, significant statements in their field. For the most part they (eventually) succeed.

Model theory attempts to account for the existence of 'normal science'; not globally for all of mathematics, but not at the level of a single theorem either; rather by subject, and by structural features cutting across subjects. This implies a process of permanent expansion.

Rich frameworks exist for e.g. real geometry; for p-adic geometry; for equational classes; for stable and simple theories.
I will discuss *finite fields*.
And, to the extent that time permits, expansion by an *additive character*.

1 Pseudo-finite fields.

Language allowing polynomials $(+, \cdot)$, equality $=$, logical connectives $\wedge, \vee, \neg$ and quantifiers $(\forall x), (\exists x)$.

A field F is *pseudo-finite* if any sentence true in F is true in some finite field.

Theorem (Ax 1967/8). *F is pseudo-finite iff $F \models PF$:*

(i) F is perfect;

(ii) F has a unique extension field F_n of order n; and

(iii) Every absolutely irreducible F- variety (or curve) has an F-point.
If $f(X,Y) \in F[X,Y]$ is irreducible in $F^{alg}[X,Y]$, then there exist infinitely many pairs $(a,b) \in F^2$ with $f(a,b) = 0$.

- The third axiom scheme, PAC, is a qualitative consequence of Weil's Riemann Hypothesis for curves over finite fields.

$$|X(\mathbb{F}_p)| = p + O(p^{1/2})$$

- To prove such a statement requires an understanding of *definable subsets* of F^n. Previous work (Robinson) clarified the phenomena of *quantifier elimination* (=every formula is equivalent to a quantifier-free one, e.g. RCF; amalgamation) and of *model completeness* (=every formula is equivalent to an existential one.) Ax had to recognize and work with an intermediate situation:

QE Definable sets are finite Boolean combinations of finite (étale) projections.

$f : U \to V$ a finite covering map; $f(U(F))$ viewed as a basic set.

Consequences.

- Decidability of PF.
- Definable dimension and measure theory. (Van den Dries, Chatzidakis-Macintyre-Van den Dries.)
- Nature of the dimension theory (simplicity).
- A conceptual home for the study of large finite fields. (e.g. Tao, expanding polynomials; H.-Pillay, definable groups).

Dimension theory: $\dim(X) \in \mathbb{N}$ for $X \subset F^n$ a definable set.
Three equivalent definitions:

1. $\dim(X) = \min\{\dim(Y) : X \subset Y, Y \text{ algebraic.}\}$
   algebraic boundedness, Van den Dries.

2. $\dim(X) = d$ iff for almost all p, $c_0 p^d \leq X(\mathbb{F}_p) \leq c_1 p^d$.

3. If (X_t) is a definable family of definable subsets of Y, $\dim(X_t) = d = \dim(Y)$, then $\dim(X_t \cap X_{t'}) < d$ for 'many' t.

Definable measure theory

(2): In fact $X(\mathbb{F}_p) = \mu(X)p^d + O(p^{d-1/2})$, with $0 < \mu(X) \in \mathbb{Q}$ definable and with the properties of a *measure*

Theorem (Chatzidakis-Van den Dries-Macintyre 1992)**.** *Let $\mathbb{F}$ be a pseudo-finite field. Then there exists a definable measure μ on definable subsets of $\mathbb{F}$ such that for a definable set V,*

$$p^{-\dim(V)}|V(\mathbb{F}_p)| \rightarrow_p \mu(V)$$

Analogue of classification of definable sets:

Theorem (H.-Pillay 1994)**.** *A Zariski dense definable subgroup of an algebaic group G is the image of $H(F)$ under a surjecdtive morphism of algebraic groups $H \to G$ with finite kernel.*

Strong approximation: A Zariski dense group of matrices in $SL_n(\mathbb{Z})$ reduces mod p to $SL_n(\mathbb{F}_p)$ for almost all p.
Weisfeiler (1984, modulo CFSG),
Gabber (in Katz 1988), Nori (1987), H.-Pillay (1995)

Proof. $H \leq SL_n(\mathbb{F}_p)$.
N generated by elements of order p. By Jordan (1877), H/N is commutative up to bounded index. (so in Zariski dense setting, $H = N$.)
N generate by definable groups $A_1, A_2, \cdots$. Let $B_n = A_1 A_2 \cdots A_n$.
B_n is definable:

$$B_3 = \{x : (\exists x_1 \in A_1)(\exists x_2 \in A_2)(\exists x_3 \in A_3)(x = x_1 x_2 x_3)\}$$

$\dim(B_n)$ is increasing, hence stabilizes at some n_0.
B_n stabilizes at $4n_0$. (?! - simplicity)
Hence N is definable. By previous theorem, image under a finite morphism of an algebraic group (now invoke simple connectedness of SL_n.)

□

2 Finite fields with an additive character

Standard additive character

$$\Psi_p : \mathbb{F}_p \to \mathbb{T}$$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to \mathbb{R}/p\mathbb{Z} \to \mathbb{T}$$

$$\Psi_p(n \mod p) := exp(2\pi i \frac{n}{p})$$

Exponential sums: given $f : X \to \mathbb{F}_p$,

$$\mathbb{E}_{x \in X} \Psi_p f(x)$$

Weyl's equidistribution criterion

Consider a sequence $f_n : X_n \to [0,1]$ (X_n a finite set)
Equidistribution:
for any $0 < \alpha < \beta < 1$,

$$\lim_n \frac{f^{-1}(\alpha,\beta)}{|X_n|} \to (\beta - \alpha)$$

Weyl: equidistribution holds iff for every $m \in \mathbb{Z}$, $m \neq 0$,

$$\lim_n \mathbb{E}_{x \in X_n} e^{2\pi i m f(x)} = 0$$

For $f : X_p \to \mathbb{F}_p$: iff for every nontrivial homomorphism $\chi : \mathbb{F}_p \to \mathbb{T}$, $(\chi = \Psi^m)$,

$$\lim_n \mathbb{E}_{x \in X_n} \chi(f(x)) = 0$$

The Weil bound on exponential sums.

(Weil 1948) X an absolutely irreducible curve over $F = \mathbb{F}_q$, f a nonconstant regular function on C, $\chi : \mathbb{F}_p \to \mathbb{T}$ a nontrivial character. Then:

$$\frac{1}{q} \sum_{x \in C(F)} \chi(f(x)) \leq cq^{-1/2}$$

Where c depends only on the degrees. (E.g. on $\deg f, \deg g$ if $X = \{(x, y) : g(x, y) = 0\}$.)
In particular, the values of the "polynomial phase" $\Psi_p \circ f$ on C are equi-distributed; provided f is not constant on C.
A large thery extends this to higher-dimensional varieties (Deligne, Katz,$\cdots$).
This work inspire by Kowalski (2007) Exponential sums over definable subsets of finite fields. Obtains bounds on exponential sums over Ax-definable sets.

Theorem. *[Kowalski] Let $V \subset \mathbb{A}^n$ be a definable set over $\mathbb{F}_p$, whose intersection with linear hyperplanes is lower-dimensional; and assume f is not constant on any large set. Then*

$$\mathbb{E}_{x \in V(\mathbb{F}_p)} \Psi(f(x))| \leq O(p^{-1/2})$$

Can the additive character $\chi : \mathbb{F}_p \to \mathbb{T}$ be put *into* the logic?

Continuous logic (with a discrete universe).

Fundamental element of structure of standard Hilbert-style *structure*:
a *relation* $R \subset A^n$; *or*, equivalently:
a function $\chi : A^n \to \{0,1\}$; *or*
a function $\chi : A^n \to X$ with X a finite space; *or*
a function $\chi : A^n \to X$ with X a profinite space. (compact, Hausdorff, totally disconnected).

Generalization:
allow $\chi : A^n \to X$ with $X = X_\chi \subset \mathbb{R}$ (or $\mathbb{C}$) a compact Hausdorff space.
The new aspect is really possible *connectedness* of the image rather than continuity.
The analogue of knowing the truth value of finitely many formulas is knowing the value of a formula *to some given resolution.*
A thoroughgoing generalization of all basic notions of logic exists, beginning with *compactness* and *effectiveness*. (Chang and Keisler 1966 - topo-

logical approach. Ben-Yaacov, Berenstein, Henson, Usvyatsov -metric, $X_\chi \subset \mathbb{R}$.)
Ultraproducts: $\chi((a_n)_u) = \lim_u \chi(a_n)$.
Connectives: $+, \cdot, \cdot\alpha$; quantifiers: $\sup, \inf$.
When allowing $X_\chi \subset \mathbb{C}$, add complex conjugation to connectives, and $\cdot i$.

Definition. *T admits quantifier-elimination if for any formula $\psi(x)$ and any $\epsilon > 0$ there exists a quantifier-free formula $\phi(x)$ such that whenever $M \models T$ and $a \in M^k$, we have $|\psi(a) - \phi(a)| < \epsilon$.*

The usual criteria for QE go through from the discrete 1st-order logic case.

Lemma. *T admits quantifier-elimination if and only if a type is determined by a quantifier-free type; iff a partial isomorphism between saturated models extends.*

(Proof: the continuous map restricting complete types to qf types will under these circumstances be a bijection; as the two spaces are compact Hausdorff, it is a homeomorphism.)

Theorem.

- *The theory* PF_+ *of finite fields with additive characters* $\mathbb{F}_q^+$ *is decidable.*
- PF_+ *admits quantifier-elimination relative to algebraically bounded quantifiers:*

  $$\sum \{\Psi(x) : x^n + c_1 x^{n-1} + \cdots + c_n = 0\}$$

  is taken as basic.
- *The completions are determined by the 'absolute numbers', the isomorphism type of the subfield of points algebraic over the prime field, enriched with* Ψ*.*
- *The pseudo-finite measure is definable. (Generalizing Ch-vdD-Mac).*
- *The discrete definable sets are just those definable in Ax's theory of finite fields. (Hence Ax's theorem is included.)*
- PF_+ *is a simple theory: indeed a higher amalgamation principle holds.*

Analytically, the quantifier-elimination the following consequence: Consider the class of functions $\mathbb{F}_p^n \to \mathbb{C}$ obtained from characteristic functions of varieties along with the additive character $\Psi(n \mod p) = e^{2\pi i n/p}$, by pre- or post-composing with polynomials and applying min and sup operators. Then any element of this class can be uniformly approximated by a polynomial expression in values of Ψ at certain algebraic functions of the variables. Definability of the measure means that the same remains true if averaging operators are also allowed.

Example of such an expression: weak Gowers norm (taken somewhat out of context from Green-Tao 2007 (*).)

$$\|f\|_{u^{d+1}} := \sup_{Q \in \mathcal{P}_d(\mathbb{F}_p^n)} |\mathbb{E}_{x \in F^n} f(x) \Psi_p(-Q(x))|,$$

Remark (Thin ice)**.** *The first-order theory of the* $(\mathbb{F}_p, \Psi_p)$ *is undecidable. Likewise the continuous-logic theory of finite fields enriched with* $\Lambda(k) = k/p$*,* $k = \{0, 1, \cdots, p-1\}$*, is undecidable (*$\Sigma^0_2$*-complete.)*

Axioms for PF_+

Say that a hyperplane $Y \subset \mathbb{A}^n$ has *height* $\leq m$ if it can be defined by a linear equation $\sum A_i X_i = b$ with $A_i \in \mathbb{Z}$, $|A_i| \leq m$.

1. F is a field, $\mathbb{Q} \subset F$; $\Psi(x+y) = \Psi(x)\Psi(y)$; $|\Psi(x)| = 1$.
2. F has a unique Galois extension of order n for each n; $\Psi|\mathbb{Q}$ factors through $\mathbb{Q}/\mathbb{Z}$.
3. $h \in \mathbb{Q}[z_1, z_1^{-1}, \ldots, z_n, z_n^{-1}]$ be a Laurent polynomial with degrees $\leq m$, and no constant term.

   For any absolutely irreducible curve $C \subset \mathbb{A}^n$, not contained in any hyperplane of height at most m, and any $\epsilon > 0$, there exists $x \in C$ with $h(\chi(x)) < \epsilon$.

Compare:

1. $\Psi^{(n)}(C) = \mathbb{T}^n$ provided C is contained in no proper hyperplane
2. If C is contained in no proper hyperplane, check if it is rational (!); if it is, reduce to lower dimension.

Proposition. *Let $D \subset F^n$ be a PF-definable set. Then the image $\Psi^{(n)}(D)$ is a finite unions of cosets of subtori of U_1^n.*
The pushforward measure $\Psi_*^{(n)}\mu_D$ is a finite linear combination of Haar measures on such cosets.

However, when D varies, the image torus can jump; the dimension of the torus is *not* a definable function.

PF = pseudo-finite:
To show: a sentence consistent with PF is realized in a finite field $\mathbb{F}_p$:
Every sentence is equivalent to a quantifier-free étale sentence σ.
σ looks only at the roots $\alpha_1, \ldots, \alpha_n$ of a polynomial $f \in \mathbb{Q}[X]$, to specify (up to conjugacy) which ones lie in the field. For instance, it may say $\sqrt[n]{1} \subset F$. This holds when $p = 1 \mod n$; by Dirichlet such primes exist. The general case is Chebotarev's density theorem.

Analogue for PF_+; Duke-Friedlander-Iwaniec.

The additive character, within finite dimensional difference varieties

On PF_+, the additive character seems to have no effect on the Galois theory.

But viewed as a part of FA_{fin}, the character $(k,+) \to U_1$ induces new Galois characters.

Let f be a regular function on a curve C. We can also view C as a transformal curve The transformal curve D defined by $\sigma(y) - y = f(x)$ is a transformally étale cover of C (smooth and zero-dimensional). Define D_Ψ as the quotient of $D \times U_1$ by the identification of (d,t) with $(d+a, t+\Psi(a))$; we obtain an archimedean analogue of an l-adic local system over C, that plays an essential role in the Grothendieck-Deligne theory. The structural automorphism σ lifts, given an element a of $C(k)$, to translation by $\Psi(f(a))$ on D_Ψ.

Could this hint of a possible directly archimedean approach to point-counting questions over finite fields?

Question. *Let (F, μ_1) be an ultraproduct of finite fields with the $p^{-1/2}$-normalized counting measure. Is $Th(F, \mu_1)$ is simple as a continuous logic structure? Is every definable subset of F^n, definable over the pseudo-finite field F alone?*