Heilbronn Institute Conference 2009

(incomplete) notes by James H. Davenport J.H.Davenport@bath.ac.uk

11-12 September 2009

1 The classical and *p*-adic Langlands programme — Buzzard

"p-adic modular forms seem to be becoming part of the p-adic Langlands conjecture."

The Langlands programme seeks to relate certain algebraic things (finite dimensional representations of Galois groups) with certain analytic things (e.g. Banach space representations of Lie groups).

Within this, there are two aspects: a local story and a global story. We will mostly look at the local story.

Let k be a finite field, e.g. $\mathbf{Z}/p\mathbf{Z}$, and $G = GL_2(k)$. What are the irreducible complex representations of G? If $\chi_1, \chi_2 : k^* \to \mathbf{C}^*$ are group homomorphisms, then (χ_1, χ_2) give us a 1-dimensional representation of $B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\} \subset G$. Then $\operatorname{Ind}_B^G(\chi_1, \chi_2) = \rho_{\chi_1, \chi_2}$ is a representation of G of dimension q+1 where q =

Then $\operatorname{Ind}_B(\chi_1, \chi_2) = p_{\chi_1, \chi_2}$ is a representation of G of dimension q+1 where q = |k|, which is almost always irreducible, but sometimes splits as 1-dimensional \oplus q-dimensional. There are also a few more "cuspidal" representations of dimension q-1 which can be obtained from certain one-dimensional representations of k'^* , where [k':k] = 2. This essentially deals with $GL_2(k)$.

What about $GL_2(\mathbf{R})$? There are many natural infinite-dimensional representations, e.g. Banach space ones, of $GL_2(\mathbf{R})$. Here the representations are almost always *topologically* irreducible. In fact these are all the representations.

Define a group $W = W_{\mathbf{R}}$ by

$$0 \to {\mathbf C}^* \to W_{\mathbf R} \to \pm 1 \to 0$$

where $j \mapsto -1$ and $jzj^{-1} = \overline{z}$ and $j^2 = -1 \in \mathbb{C}^*$. The 2-dimnesional semisimple (not necessarily irredicuble) representations of $W_{\mathbb{R}}$. Then there are two cases.

• $\rho(j)$ is diagonal. Then ρ factorsz through $W_{\mathbf{R}}^{\mathrm{ab}} \equiv \mathbf{R}^*$ and $z \mapsto z\overline{z}$ and χ_1, χ_2 are characters of $\mathbf{R} * *$.

• If ρ is irreducible, then $\rho = \operatorname{Ind}_{c^*}^{W_{\mathbf{R}}} \chi_1$. Then $z \mapsto z^n$ for $n \in \mathbf{Z}$, and $C^* \equiv \mathbf{R}_{\geq 0} \times S^1$.

So the two-dimensional representations are parameterized by (χ_1, χ_2) or by pairs (s, n).

In 1973, Langlands showed that if G is any connected reducive group over the reals, e.g. GL_n , SL_n , Sp_n , O(a, b), U(a, b) etc.) then there was a "canonical" map of irreducible Banach representations of $G(\mathbf{R})$ [hard problem] into semisimple representations of $W_{\mathbf{R}}$ into the L-group of G [easy problem], which is surjective with finite fibres. Example: the L-group of GL_n is $GL_n(\mathbf{C})$.

 \mathbf{Q} has a natural norm, but is not complete. One completion is \mathbf{R} , but there are other norms, with their own completions, e.g. *p*-adic (in which he defined $|p| = \epsilon$) norms and completions \mathbf{Q}_p . Note that these are not connected. Langlands conjectured that there should be an analogue of his theorem with \mathbf{R} replaced by \mathbf{Q}_p .

Theorem 1 (M. Harris, R. Taylor, 2000) There is a canonical bijection between the smooth irreducible representations of $GL_n(\mathbf{Q}_p)$ (on **C**-vector spaces) and semi-simple n-dimensional representations of WD_{Q_p} into $GL_n(\mathbf{C})$, where WD is the Weil-Deligne group.

Note that we still have some occurrences of **C** in this statement. What happens if we change these as well, into some extension E of \mathbf{Q}_{p} .

Theorem 2 (Colmez, 2009) There is a canonical injection from semi-simple representations of $\operatorname{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ (into $GL_2(E)$) into irreducible unitary p-adic Banach spaces representations of $GL_2(\mathbf{Q}_p)$.

However, there is evidence that this is false for GL_3 . This raises the question — " do we have the right analogy of Langlands in this case"?

2 Codes on Graphs: Shannon's Challenge and Beyond — July L. Walker

Basic example is the Binary Symmetric Channel, with probability p of error (either $0 \rightarrow 1$ or *vice versa*). Repeated transmission (e.g. three times, or five or ...) will reduce the error rate, at the cost of reducing the data rate.

Theorem 3 (Shannon) Every channel has a capacity C such that for every R < C there is a code of rate R and error less than ϵ .

But the proof is probabilistic and non-constructive: Shannon's challenge is to find such codes.

A binary linear code of length n, dimension k and minimum distance d is a k-dimensional subspace C of \mathbf{F}_2^n such that any two distinct vectors differ in at least d positions.

Examples include Hamming codes (repetition is a special case), Reed–Solomon codes (as in CD players, DVDs, Blu-Ray etc.), cyclic codes, algebraic geometric codes.

In 1993, turbo codes were introduced. They come very close (*in simulations*) to achieving Shannon's bounds. Jin and McEliece (2002) studied the average performance of turbo codes under maximum likelihood decoding (because it can be done, not because it's the real question). Hiowever, turbo codes *have* led to a major change in coding theory.

Most codes can correct many more errors than the minimum distance, so let's shift to the average paradigm.

- **1960** Robert Gallagher's thesis introduced low density parity check (LDPC) codes. He was unable to simulate them effectively.
- **1990s** Rediscovered, and, this time, simulated. Actually beat turbo codes. MacKay–Neal, Sipser–Spielberg etc.

Let T be a (sparse, in practice) bipartite graph with vertices $X \cup F$. A configuraion is an assignment of 0,1 to the vertices in X such that each vertex in F is adjacent to an even number of 1s. These codes come equipped with an iterative message-passing decoding algorithm that is extrememly efficient and corrects, with high probability terms many more error patterns than are guaranteed by the minimum distance.

- 1. Which LDPC codes perform well?
- 2. How can we design other LDPC codes that perform well? There are heuristics like "large girth", but in practice 6 is enough (no-one knows why).

The decoding algorithm acts locally, so cannot distinguish betwene the original graph and any unramified cover of the graph.

Definition 1 A graph cover pseudocodeword for T is a vector p of integers p_i such that there is some cover \tilde{T} of T and a configuration on \tilde{T} that assigns p_i ones to vertex i in T.

Some theorems characterise these, e.g. iff the monomial $u_1^{p_1} \cdots u_k^{p_k}$ occurs with non-zero coefficient in a certain multivariate power series, normally of the edge zeta function of the normal graph of T.

There are some sequences of LDPC codes that, at the limit, provably perform at rates extremely close to Shannon capacity. *But* the evidence that individual LDPC codes are good comes from simulations. The study of pseudocodewords is based on an intuitive connection between the decoding algorithms and graph covers. The performance of algebraically constructed LDPC codes is still not entirely predictable.

The next challenge is Network Coding. The goal is to reliably transmit information from possibly several sources through a possibly unknown and unreliable network to possibly several sinks. Typical applications are the Internet, wireless neworks, satellite communications etc. The butterfly example shows that the network has to combine information within itself.

3 The local of the real, complex and Zilber exponentials — Macintyre

- 1. If $p(z) \in \mathbf{C}[z]$, how many solutions does $\exp(z) = p(z)$ have in **C**?
- 2. If $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n, c_1, \ldots, c_m, d_1, \ldots, d_n \in \mathbf{C}$, when does $\sum c_j \exp(\lambda_j z) = 0$, $\sum f_j \exp(\mu_j z) = 0$, have infoinitely many solutons in **C**?
- 1. Infinitely many unless p = 0, but if $p \in \mathbf{R}[z]$ only finitely many real solutions (Hardy).
- 2. Unknown, but there is a conjecture of H. Spariro (1958), saying that there must be a common factor of length at least 2. In the real case, again by Hardy, neither can have infinitely many real zeros, unless identically zero.

So consider commutative rings with unit R, with a function E such that E(x + y) = E(x)E(y) and E(0) = 1. We might (**C**) or might not (**R**) have periods. We can get wild groups of periods via model theory (but not interesting). E-rings form an equational class, so free E-rings on X exist, denoted $[X]^E$. Similarly $k[X]^E$ for any field k.

"If you assume Schanuel's conjecture you can prove anything" — Birch.

Let R have characteristic 0. Let $\lambda = {\lambda_1, \ldots, \lambda_n} : \lambda_i \in R$. Let

$$\lambda = \{\lambda_1, \dots, \lambda_n, E(\lambda_1), \dots, E(\lambda_n)\}.$$

Then tr. deg. $(\tilde{\lambda})$ =linear dimension λ .

Theorem 4 $[x]^E$ satisfies Schanuel's conjecture.

Let $k = \mathbf{R}$. Fix a system. Then the set \tilde{Z} for which an \overline{X} exists is the most general set you can define. Implicit in Wilkie (1991), but false for \mathbf{C} .

For any k satisfying SC, we get a dependence relation: α depends on \tilde{Z} if there is a system of equations for which α is the first coordinate of a solution.

A strong extension $K \rightarrow L$ is one where dimension does not drop. Assume **C** satisfies SC. Then **R** \rightarrow **C** is not strong since dim_{**R**}(π) = 1. but dim_{**C**}(π) = 0.

Zilber fields, and characteristic 0 E-fields which satisfy SC, have an infinite cyclic group of periods and the morphisms are strong embeddings. These uiversal domains are constructed by general nonsense (as could be done for algebraic closures). But to give intelligible axioms is not general nonsense. These axioms look like

If V is a variety over K and $v \subset K^n \times (K^*)^n$ and ... then V meets $\{(x, E(x)) : x \in K^n\}.$

If we ask for this meet to be generic, and that the closure of countable sets is countable, then (Zilber's "Steinitz") there is a unique one in each uncountable cardinal. Let¹ \mathcal{B} be Zilber's model of the categorical theory in cardinality 2^{\aleph_0} .

Conjecture 1 (Zilber) $\mathcal{B} \equiv C$

 $\mathbf{C} \models$ Hadamard (Analysis). $\mathcal{B} \models$ Hadamard (Algebra).

Theorem 5 (SN (Schanuel Nullstellensatz)) If $F \in K[x]^E$ has no zero in K, F = E(G) for $G \in K[x]^E$.

- 1. **C** and \mathcal{B} have solutions for the same elements of $[X]^E$ and the set of such elements is decidable.
- 2. Problem (Deligne) Is the set of 1-variable systems from $[X]^E$ solvable in **C** decidable?

Suppose F and G have a common divisor of the same form \ldots

- **Q.** Does π exist in \mathcal{B} .
- **A.** In \mathcal{B} there is an α which is a generator of the periods, and we can distinguish α from $-\alpha$. Whether that answers your question is an interesting question.

Q.—**JHD** Is \mathcal{B} essentially what an algebraist thinks might be **C**?

A. Essentially.

4 How and how not to compute the exponential of a matrix — Higham

Quoted Sengupta (Adv. Appl. Math 1998).

Theorem 6 (Cayley-Hamilton) If $A, B \in \mathbb{C}^{n \times n}$, AB = BA and $f(x, y) = \det(xA - yB)$ then f(A, B) = 0.

In general, we only quote consequences of this theorem.

1. $p(t) = \det(tI - A)$ implies p(A) = 0

2. . . .

- Waltz's method: $C_k = (I + 2^{-k}A)^{2^k}$ ill-conditioned. Diagonalization: $A = Z \operatorname{diag}(\lambda_i)Z^{-1}$, but this assumes diagonalizability. Scaling and Squaring:
 - 1. $B := A/2^s$ so $||B||_{\infty} = 1$
 - 2. $r_m(B) = [m/m]$ Padé approximant to e^B

¹ "We can't call it **Z**, and Boris is Zilber's first name!"

3. $X = r m(B)^{2^s} \approx e^A$

There are explicit formulae for the Padé approximant to e^B : $p_m(x)/p_m(-x)$ where $p_m(x) = \sum \ldots$ Can shiw that this produces the *exact* exponential of some $A + \Delta A$, where there is an explicit formula for ΔA . Moler & Van Loan (1978) chose m = 6 and $||2_{-s}A|| \leq \frac{1}{2}$. Higham (2005) uses symbolic computation, for various $m \leq 13$. Produces a complicated formula for efficient evaluation of a degree 13 matrix-valued polynomial.

Introduces the concept of over-scalring, e.g. in $\begin{pmatrix} 1 & b0 & 1 \end{pmatrix}$ for very large (say 10^8) b. There is a formula

$$\exp(A_{11} \quad A_{12}0 \quad A_{22}) = (\exp A_{11} \quad \int \dots \quad 0 \quad \exp A_{22}) \tag{1}$$

where A_{12} occurs linearly in the off-diagonal element.

Lemma 1 If $k = pm_1 + qm_2$ with $p, q \in \mathbf{N}$ then

 $||A^k||^{1/k} \le \dots$

Hence we can use $||A^k||^{1/k}$ rather than ||A|| in some of our conditioning estimates, and this basically solves over-scaling. Bottom line: no slower than MatLab's expm, and sometimes more accurate. However, the stability of the scl;aing phase is still not well-understood.

Frechét derivative:

$$f(A + E) - f(A) - L(A, E) = o(||E||).$$

For exponentials, $L(A, E) = \int_0^1 e^{A(1-s)} E e^{As} ds$, which is essentially the same term in (4). Used to be $538n^3$ flops, with Al-Mohy & Higham (2009) can use symbolic differentiation of the algorithm to compute e^A and the derivative in $48n^3$ flops.

Other problems are structured matrices (Topelitz etc.), and also the ned for factorization-free methods for large sparse matrices, when we probably don't want $\exp(A)$, but the ability to compute $\exp(A)b$ for vectors b.

Q. What about tridiagonal, say?

- **A.** Well, $\exp(A)$ is full, but decays away from the diagonal, so maybe we should only compute the near-diagonal entries.
- **privately** This is true even if the matrix is not diagonal-dominant: if it is, then a binomial expansion will show this, but diagonal dominance is *not* necessary.

5 Packing, energy minimization and exceptional structures — Henry Cohn (Microsoft Cambridge)

Why are some packings and structures more beautiful than others?

n = 1 Trivial.

n=2 Hexagonal.

- $n=3\,$ Hales 1998: not e
that there are various solutions, such as FCC, hexagonal etc.
- n > 3 Bounds only, and every dimension seems to be different, e.g. 8 is very different. There has been a recent improvement on Keith Ball's bound, but in general the bounds differ massively. Cohn–Elkies have a slight improvement on the classic Rogers' bound. n = 24 and n = 8 the upper and lower bounds *seem* to be equal, but this has only been proved to 30 decimal places.

The thompson problem: a bunch of electrons on the surface of a sphere. Packing problems are a limiting case. As we vary the potential function, how do the optimal configurations change? Four points on S^2 always form a transdedron, so we have universal optimality. Look at Coulomb on S^2 . With 43 points, we have 21 parameters, but with 44 points, we have only one.

Let

$$E_f(\mathcal{C}) = \frac{1}{2} \sum_{x,y \in \mathcal{C}} f(|x-y|^2)$$

We say f is completely monotonic There are universal optima for n = 2, 3, 6, 4, 12 (but not for the cube or the dodecahedron) on S^2 . For 5 points, where are two possible configuration: poles and equilateral triangle on equator, and north pole plus square in southern hemisphere (this is a one-parameter family, based on the latitude of the square.

Conjecture 2 For any completely monotone potential, one or other of these is optimal.

In 8 dimensions, the E_8 root system (N = 240) is the optimal solution, and for 24, the Leech lattice (N = 196560). But there are no known configurations for $9 \le 9 \le 20$. There is also an infinite family in dimension $q(q^3 + 1)/(q + 1)$ with $(q + 1)(q^3 + 1)$ points $(q \ a \ prime \ power)$.

Culd a computer discover these? They can discover the 600-cell or the E_8 root system with no external guidance. We focus on the harmonic potential function: $r \mapsto 1/r^{n/2-1}$ in \mathbb{R}^n . We foud two configurations (actually already known): n = 10 has 40 points (Conway et al.) and n = 14 has 64 (doubly-shortened Nordstrom-Robinson code). Actually recognising the configurations is difficult, but careful reorganising of the points can show structure.

Proofs of universal optimality use linear programming bounds for potential energy developed by Yudin. Potential energy depends only on the pair correlation function. We have a natural constraint of non-negatibity, and Torquato– Stillinger conjecture that for disordered packings in high dimension, these are the only constraints on the pair correlation function. The dual linear programming problem can say what the linear combination of the constraints is, which is how Cohn & Kumar proved universal optimality.

6 Topological complexity of definable sets — Vorobjov

We can define a semi-algebraic set (standard definition), and ask what upper bounds are known on the total Betti number (sum of Betti numbers) of such a set. Studied by Petrovskii/ Oleinik c. 1950, Milner–Thom in the 1960s. If X is algebraic, of degree < d in n-space, then

$$b(X) \le d(2d-1)^{n-1}$$

and for a semi-algebraic set with s inequalities

$$b(X) \le (csd)^n$$

These singly-exponential bounds, which are asymptotically tight, cannot be proved by triangularization methods, since that will give us doubly-exponential results.

Monotone Boolean combinations of only $\geq or$ only > again give $b(X) \leq (csd)^n$ (Basu). V. Arnold *Russ. Math. Surveys* **57**(2002) p. 833 describes the connections to Hilbert's 13th and 16th. problems. We might also be interested in upper computational complexity bounds. Upper bounds on Betti numbers lead to lower complexity bounds for algebraic computation trees [Ben-Or, Björner etc.].

Two ways to generalize.

- 1. Use other functions (e.g. exponential polynomials, as Macintyre), or other descriptions of complexity than the degree, e.g. # monomials. Here Pfaffian functions are the key concept: see Khovanskii (1980), and fewnomials (Khovanskii, Bihan–Sottile 2006), and sparse polynomials (Grigoriev, Risler, 1980s) in terms of additive complexity. For each of thee classes there is an analogy of Bézout's theorem, which gives an upper bound on the number of isolated solutions in terms of the descriptive complexity.
- 2. To sets defined more generally, e.g. with negation, or by quantifier elimination = projections. So suppose we have arbitrary Boolean formulae with s distinct polynomials. Then (Gabrielov–Vorobjov)

$$b_k(X) \leq (c\nu sd)^n$$

where $\nu = \min(k+1, n-k, s)$.

An o-minimal structure over the reals is a collection S_n such that

- (a) All algebraic subsets of \mathbf{R}^n are in S_n
- (b) For every n, S_n is closed under Boolean operations, Cartesian products and projects on subspaces.
- (c) The elements of S_1 are the finishint unions of points and intervals.

Elements of S_n are called definable subsets of \mathbb{R}^n . This generalizes semialgebraic, sub-analytic etc.

Let S be a union of an o-minimal family of closed sets $S_{\delta} : \delta > 0$, such that $S_{\delta'} \subset S_{\delta}$ for $\delta' > \delta$. Let further each S_{δ} be an intersection of closed sets $S_{\delta,\epsilon}$. where

Definition 2 (Telescope) For $0 < m \in \mathbb{Z}$ and $0 < \epsilon_0 \ll \delta_0 \ll \cdots \ll \epsilon_m \ll \delta_m \ll 1$ let $T(S) = S_{\delta_0,\epsilon_0} \cup S_{\delta_1,\epsilon_1} \cup \cdots$. In 2-D, m = 2 covers the whole plane. \ll signifies "is sufficiently smaller than".

Let S be a bounded set defined by a Boolean combinations of h(x) = 0and h(x) > 0, such that S is the union of its disjoint sign sets. Get S_{δ} by replacing h(x) by $h \ge \delta$ and each h < 0 by $h \le -\delta$. Furthermore, $S_{\delta,\epsilon}$ is obtained by replacing h = 0 by $-\epsilon < h < \epsilon$ as well. Then

$$\phi_k: \pi_k(T(S)) \to \pi_k(S); \ldots$$

and isomorphisms, and rank $H_k(S) = \operatorname{rank} H_k(T(S))$ and if $m \ge \dim(S)$, then $T(S) \simeq S$, and this proves the Gabrielov–Vorobjov result above.

Let $\rho : \mathbf{R}^{n+r} \to \mathbf{R}^n$ and $Y = \rho(X)$ wher X is such a bounded semialgebraic set defined by s polynomials. Then effective quantifier elimination produces such a Boolean combination for Y, and implies

$$b_k(Y) \le (sd)^{cn^2r} :$$

which is much worse than we had before, and does not generalise to Pfaffians.

Gabrielov–Vorobjov–Zell lets us construct bounds without projection, and, for f closed, subjective and o-minimal, we have $b_k(Y) \leq \sum_{p+q=k} b_q(W_p)$ where W_p is the (k + 1)-fold fibred product of X.

If we represent X by X_{δ} and $X_{\delta,\epsilon}$, then $\rho(X_{\delta})$ and $\rho(X_{\delta,\epsilon})$ represent $\rho(X)$. $b_k(Y) \leq ((k+1)sd)^{c(k+nr)}$, a much better result.

We can iterate this procedure over t blocks of alternating quantifiers, the *i*th with r_i variables,

$$b_k(X) \le \left(2^{t^2} dsnr_1 \dots r_t\right)^{O(2^t nr_1 \dots r_t)}$$

Note that $(\exists x P(x)) \lor (\exists x Q(x))$ is $\exists x P(x) \lor Q(x)$, but not for \land , where we have to introduce new variables. But the bounds on Betti numbers (replacing \lor by \cup etc.) are in fact the same for \cap and \cup .

7 Renormalization of Interacting Diffusions den Hollander

Suppose we have a lattice of interacting diffusions, e.g. in statistical physics. Renormalization consists of regarding a group of interacting diffusions as if they were a composite diffusion. Our success story consists of converting this vague idea into real mathematics.

Systems of heierarchically interacting diffusions allow for a rigorous renormalization analysis.

Use stochastic analysis and functional analysis.

$$dX_i(t) = \sum_{j \in \Omega_N} a_n(i,j) [X_j(t) - X_i(t)] dt + \sqrt{g(X_i(t))} dW_i(t)$$

where $S \subset \mathbf{R}^d$ is the single-component state spoace, Ω_N is the hierarchical lattice of degree $N \in \mathbf{N}$; A_n is the random walk transition kernel on Ω_N ; g is the single-component diffusion function and W_i are independent Brownian motions.

Let S = [0, 1], and $g \in \mathcal{H}$ satisfying

- 1. h Lispschitz on [0, 1]
- 2. g(x) > 0 for $x \in (0, 1)$
- 3. g(0) = g(1) = 0.

Then

$$(Fg)(y) = \int_{[0,1]} g(x)\nu_y^g(dx)$$

where ν_{y}^{g} is the equilibrium distribution of

...

Then $F(\mathcal{H}) \subset \mathcal{H}$, the solution to the eigenvalue probulem $Fg = \lambda g$ is the one-parameter family $g = cg^*$ and $\lambda = \frac{1}{1+c}$ (c > 0) where $g^*(x) = x(1-x)$.

Theorem 7 (Wright–Fisher diffusion) $\lim_{k\to\infty} f^k(g) = g^*$.

On the half-line, where we assume $\lim_{x\to\infty} g(x)/x^2 = 0$, again the stochastic part has been completed.

Theorem 8 (Feller's diffusion) If $\lim_{x\to\infty 0} x^{-1}g(x) = c$, then $\lim_{k\to\infty} f^k(g) = cg^*$, where $g^*(x) = x$.

7.1 What about higher dimensions?

Two main complications.

1. Only for special cases of g can we show that there is a unique weak solution. The stochastic part of the renormalization programme has been carried through only for these special cases. 2. The analytic part of the renormalization programme suffers from the fact that, in general, there is no explicit formula for the equilibrium distribution, and hence not one for the renormalization transform.

Special case: $S \subset [0,1]^d \ (d \geq 2)$ closed convex. Assume

- 1. h Lispschitz on S
- 2. g(x) > 0 for $x \in interior(S)$
- 3. g(x) = 0 on the boundary.

Although the stochastic part is largely open, there is some progress on the analytic part. Similarly for $[0, \infty)^2$.

The scaling behaviour of large space-time blocks depends on the asymptotic behaviour of the single-component diffusion function near the boundary of the state space. We see that several classical diffusions appear as local or global attractors in this contexts.