Proof Mining in Topological Dynamics

Philipp Gerhardy
Department of Mathematics
University of Oslo

Logic Colloquium 2008, Bern, Switzerland, July 3-8.
van der Waerden’s Theorem and Topological Dynamics

Proof Mining

Proof Analysis

Conclusion
van der Waerden’s Theorem

Definition
An arithmetic progression of length $k$ is a sequence of the form $a, a + b, a + 2b, \ldots, a + (k - 1)b$ for integers $a, b > 0$.

van der Waerden’s Theorem
For any $q, k > 0$ there exists an $N = N(q, k) > 0$ such that for any $q$-colouring $C_1 \cup \ldots \cup C_q$ of $[-N, N] \subseteq \mathbb{Z}$, one of the colours contains an arithmetic progression of length $k$.

Question: Growth rate of function $N(q, k)$?
van der Waerden’s Theorem

Different proofs of van der Waerden’s Theorem:

- van der Waerden: combinatorial proof.
- Furstenberg and Weiss: topological dynamics.
- Shelah: different combinatorial proof.
- Gowers: (Fourier) analytic proof.

Question: What information do the proofs provide about $N(q, k)$?
Furstenberg and Weiss prove van der Waerden’s Theorem via the following result in topological dynamics:

**Multiple Birkhoff Recurrence (Furstenberg/Weiss, 1978)**

Let $(X, d)$ be a compact metric space and $T_1, \ldots, T_l$ commuting homeomorphisms of $X$. Then there exists a point $z \in X$ such that for every $\varepsilon > 0$ there is an $n > 0$ satisfying $d(T_i^n z, z) \leq \varepsilon$ simultaneously for $i = 1, \ldots, l$.

$q$-colouring of $\mathbb{N}$ translates into compact metric space $(X, d)$, $k$-term progression into point $z$ for $k$ homeomorphisms.
Analyzing Furstenberg and Weiss’ proof

Motivation for analyzing (a proof due to Girard of) the Multiple Birkhoff Recurrence Theorem:

- Bounds for Multiple Birkhoff Recurrence Theorem translate into bounds for van der Waerden’s Theorem.
- No explicit bounds in the Multiple Birkhoff Recurrence Theorem.
- Previous analysis by Girard (using cut elimination) only treats specialization of Multiple Birkhoff Recurrence Theorem to space and homeomorphisms arising from van der Waerden’s Theorem.

Remark: Proof by Girard eliminates an unnecessary appeal to compactness in proof by Furstenberg and Weiss.
Proof mining - an overview

Proof mining is the information of extracting additional information from proofs in mathematics. Additional information can be:

- Quantitative: a rate of convergence from a convergence proof.
- Qualitative: uniformity results, strengthening of theorems (same conclusion follows from weaker premises).

On the one hand, develop general methods to extract additional information from proofs. On the other hand, carry out case studies and analyze concrete proofs.
Proof interpretations

Proof interpretations: transform formal proofs into enriched proof from which desired additional information can be read off.

Examples:

- Cut elimination - applies to first-order proofs.
- No-counterexample interpretation - more general than cut elimination, but not fully modular.
- Functional interpretations - fully modular, requires functionals in all finite types.
Metatheorems

Using proof interpretations we may prove metatheorems that:

- classify theorems and proofs from which additional information may be extracted,
- describe general properties and conditions that allow to predict the kind of information that may be extracted,
- describe methods that allow to carry out the extraction from a sufficiently formal proof.

Metatheorems may cover Peano arithmetic and classical analysis in all finite types and extensions thereof with new types, constants and axioms to represent e.g. arbitrary metric spaces, hyperbolic spaces, normed linear spaces, etc.
Girard’s variant of Multiple Recurrence

Girard proved the following variant of the Multiple Birkhoff Recurrence Theorem:

**MBR, variant (Girard, 1987)**

Let \((X, d)\) be a compact metric space, let \(T_1, \ldots, T_l\) commuting homeomorphisms of \(X\) and let \(G\) be the commutative group generated by \(T_1, \ldots, T_l\). Then

\[
\forall \varepsilon > 0 \exists N \in \mathbb{N} \exists S_1, \ldots S_M \in G \forall z_0 \in X \exists n \leq N \exists i \leq M (d(T^n_1 S_i z_0, S_i z_0) < \varepsilon \land \ldots d(T^n_l S_i z_0, S_i z_0) < \varepsilon).
\]

To make this fully effective, we must provide the bound \(N\) and some description of the group elements \(S_i\).
Proofs of MBR by Furstenberg/Weiss and Girard

To analyze Girard’s variant of MBR for general compact metric spaces and arbitrary homeomorphisms, we must make explicit the following notions:

- \((X, d)\) is a compact metric space,
- \(T_i\) are continuous, commuting homeomorphisms of \(X\),
- \(G^T\) is the group of homeomorphisms generated by a finite set \(T = \{T_1, \ldots, T_l\}\).

We write \(G^T_M\) for the group elements of \(G^T\) that can be written as words of length \(< M\) when written as words over the generators \(T_1, \ldots, T_l\).
Making compactness explicit

$(X, d)$ compact metric space: $(X, d)$ metric space, totally bounded + complete; actually only total boundedness is needed.

Total boundedness: for any $\varepsilon > 0$ there is a number $k$ such that among any $k$ elements two elements are $\varepsilon$-close.

We require a modulus of total boundedness $\gamma$:

$$\forall \varepsilon > 0 \forall (x_n)_{n \in \mathbb{N}} \exists 1 \leq i < j \leq \gamma(\varepsilon)(d_X(x_i, x_j) \leq \varepsilon).$$
Proof of MBR - induction base

This enrichment is used e.g. in the following proof step:

**Lemma**

Let \((X, d)\) and \(T\) be given. Then for every \(\varepsilon > 0\) there exists a \(z \in X\) and an \(n > 0\) such that \(d(T^n z, z) < \varepsilon\).

**Proof:** Take any \(x \in X\), consider the sequence \(\{T^i x\}\). By compactness two elements of the sequence are \(\varepsilon\)-close.

**Question:** Which elements? Answer lies in total boundedness!
Proof of MBR - induction base

Notation

Let $G^T$ be a group generated by $T_1, \ldots, T_l$, then $G^T_M \subseteq G^T$ (for $M > 0$) is the subset of group elements which can be written as a word of length $< M$ over the generators.

Lemma

Let $(X, d)$ and $T$ be given and let $G$ be the group generated by $T$ and let $\gamma$ be a modulus of total boundedness for $(X, d)$. Let $\varepsilon > 0$ be given and let $N = M = \gamma(\varepsilon/2)$. Then for each $x \in X$ there exists $n \leq N$ and $g \in G_M$ s.t. $d(T^ngx, gx) < \varepsilon$.

NB: Bounds on $N, M$ are uniform in point $x \in X$. 

Multiple Birkhoff Recurrence Theorem - effective version

Continuing the enrichment and transformation of the proof, one obtains the following:

**Multiple Birkhoff Recurrence Theorem (effective version)**

*Let* \((X, d)\) *be a metric space with modulus of total boundedness* \(\gamma\), *let* \(T_1, \ldots, T_l\) *be commuting homeomorphisms of* \(X\) *with common modulus of uniform continuity* \(\omega_T\) *and let* \(G\) *be the group generated by* \(T_1, \ldots, T_l\). *Then for every* \(\varepsilon > 0\) *there exist* \(N, M > 0\) *(to be defined below) such that for every* \(x \in X\) *simultaneously* \(\min_{0 < n \leq N} \min_{g \in G_M} d(T_i^n g x, g x) < \varepsilon\) *for* \(i = 1, \ldots, l\).
Multiple Birkhoff Recurrence Theorem - effective version

Define:

- $N^1(\varepsilon, \gamma, \omega) = M^1(\varepsilon, \gamma, \omega) = \gamma(\varepsilon/2)$.
- $\varphi^k(i) = N^k(\varepsilon_{i}^{k+1}, \gamma, \omega^2)$,
- $\varphi^k(i) = 2M^k(\varepsilon_{i}^{k+1}, \gamma, \omega^2) + N^k(\varepsilon_{i}^{k+1}, \gamma, \omega^2)$.
- $\varepsilon^k_1 = \varepsilon/4$ and $\varepsilon^k_{i+1} = \omega \varphi^k_N(i) + i \cdot \varphi^k_M(i)(\varepsilon_i/2)$.
- $N^{k+1}(\varepsilon, \gamma, \omega) = \varphi^k_N(\gamma(\varepsilon/2)) \cdot \gamma(\varepsilon/2)$
- $M^{k+1}(\varepsilon, \gamma, \omega) = \varphi^k_M(\gamma(\varepsilon/2)) \cdot \gamma(\varepsilon/2)$.

Then $N = N^l(\varepsilon, \gamma, \omega)$ and $M = M^l(\varepsilon, \gamma, \omega)$. 
Comments on effective version of MBR

- Straightforward 'interpretation' of the proof, once moduli for continuity and total boundedness are introduced.
- Interpret lemmas, combine realizers to interpret theorem; structure of proof is preserved.
- Already topological proof of MBR has Ackermann realizers (iterations of $\omega, \gamma$).
Conclusions

Extracted bounds are the same, because combinatorial proof (by van der Waerden) and topological proof (by Girard) are the same (only formulated in different contexts).

**Results:** General bounds for MBR. Insights into connections between combinatorics and topological dynamics. Example of how to analyse general proofs in topological dynamics.

MBR and van der Waerden’s Theorem

Let a $q$-colouring of $\mathbb{Z}$ be given and construct $(X, d)$ and $T_1, \ldots, T_l$ as before.

$\gamma(k) = q^{2k+1}$ is a modulus of total boundedness for $X$.

$\omega_T(k) = k + l$ is a common modulus of continuity for the $T_i$.

Applying the above bounds to these $\gamma, \omega_T$ again yields van der Waerden’s bounds (modulo some constants).
Analogies between Combinatorics and Topological Dynamics (vdW and MBR)

<table>
<thead>
<tr>
<th>Combinatorics</th>
<th>Topological Dynamics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finite set</td>
<td>Compact space</td>
</tr>
<tr>
<td>Number of colours</td>
<td>Number of $\varepsilon$-neighbourhoods</td>
</tr>
<tr>
<td>Colouring of $\mathbb{Z}$</td>
<td>Point</td>
</tr>
<tr>
<td>Colouring of finite block</td>
<td>$\varepsilon$-neighbourhood</td>
</tr>
<tr>
<td>Length of progression</td>
<td>Number of homeomorphisms</td>
</tr>
<tr>
<td>Blocks within blocks</td>
<td>Continuity</td>
</tr>
</tbody>
</table>

Philipp Gerhardy
Proof Mining in Topological Dynamics
Analogies between Combinatorial and Topological Proof

**Induction Base:** Exhaust colours vs. exhaust $\varepsilon$ neighbourhoods.

**Induction Step:** Long progressions, few colours $\Rightarrow$ shorter progressions, more colours vs. Many homeomorphisms, large $\varepsilon$ $\Rightarrow$ fewer homeomorphisms, smaller $\varepsilon$.

Number of colours grows by colouring blocks, length of blocks from induction hypothesis vs. shrinking of $\varepsilon$ by applying continuity, amount of continuity by induction hypothesis.