An application of Shoenfield's absoluteness theorem to the theory of uniform distribution

Martin Goldstern

October 1992/January 1993

ABSTRACT. Theorem: If $\mathbf{C}$ is a Polish probability space, $W \subseteq \omega^\omega \times \mathbf{C}$ a Borel set whose sections W_x $(x \in \omega^\omega)$ have measure one and are decreasing $(x \leq x' \to W_x \supseteq W_{x'})$, then the set $\bigcap_x W_x$ has measure one.
We give two proofs of this theorem: one in the language of set theory, the other in the language of probability theory, and we apply the theorem to a question on completely uniformly distributed sequences.

Supported by DFG grant Ko 490/7-1

Introduction.

The law of large numbers implies that almost every infinite sequence in $\{0,1\}$ is uniformly distributed, i.e., for almost all $t \in {}^\omega 2$ we have $\lim_{n\to\infty} D(t,n) = 0$, where $2 = \{0,1\}$, $\omega = \{0,1,2,\ldots\}$, and the "discrepancy" D is defined by $D(t,n) = 2 \cdot \left|\frac{|\{i<n : t(i)=0\}|}{n} - \frac{1}{2}\right|$, and "almost all" refers to the product measure on ${}^\omega 2$ induced by the equidistributed measure on $\{0,1\}$, i.e., $\mu(\{0\}) = \mu(\{1\}) = \frac{1}{2}$.
A similar argument shows that for all k, almost all sequences are k-uniformly distributed, i.e., for all k, for almost all $t \in {}^\omega 2$ we have $\lim_{n\to\infty} D_k(t,n) = 0$, where

$$D_k(t,n) := 2^k \cdot \max_{w \in {}^k 2} \left| \frac{|\{i < n : (t(i), \ldots, t(i+k-1)) = w\}|}{n} - \frac{1}{2^k} \right|$$

Since the measure is countably additive, we can switch the quantifiers "for all k" and "for almost all t" and get:

for almost all $t \in {}^\omega 2$, for all k, t is k-uniformly distributed

If we replace the constant k by a function $s \in {}^\omega \omega$ we are led to the following concept: A sequence $t \in {}^\omega 2$ is called s-uniformly distributed, if $\lim_{n\to\infty} D_{s(n)}(t,n) = 0$.
Let R_s be the set of s-uniformly distributed sequences. It is easy to see that s must not grow faster than $\log n$ (in this paper, log always means the logarithm to the base 2) if the set R_s should be nonempty. Flajolet-Kirschenhofer-Tichy and Grill determined the exact bound for s below which still almost all sequences are s-uniformly distributed:

1. Theorem ([2], [4]): $\mu(R_s) = 1$ iff $\varphi_s \to \infty$, where $\varphi_s(n) = \lfloor \log n - \log\log n - s(n) \rfloor$.
See also [3] for a generalization of this result.

Now let

$$R = \bigcap_s R_s$$

where s ranges over all functions with $\varphi_s \to \infty$. Since R is an uncountable intersection of measure one sets, it is a priori not clear if R has measure one, or indeed if R can be nonempty.
We will show below that R must have measure 1. That is, as in the remark about k-uniformly distributed, we can again switch quantifiers and get

2. Theorem: For almost all $t \in {}^\omega 2$, for all s for which $\varphi_s \to \infty$ we have: t is s-uniformly distributed.

We will give two proofs of this theorem: One for logicians, using the technique of forcing and Shoenfield's absoluteness theorem for $\mathbf{\Sigma^1_2}$-sets, and the second for those mathematicians who are more familiar with the language of probability theory. Here we use von Neumann's theorem that Borel sets can be uniformized by measurable functions.

3. Notation: ω is the set of natural numbers. $2 = \{0,1\}$.

${}^\omega\omega$ is the Baire space (= all functions from ω to ω) with the usual metric and topology. The variable x always ranges over elements of ${}^\omega\omega$. This spaces is naturally ordered by $x_1 \le x_2 \Leftrightarrow \forall n\, x_1(n) \le x_2(n)$.
$\omega{\nearrow}\omega$ is the set of sequences which diverge to infinity, a subspace of ${}^\omega\omega$. The variable y always ranges over elements of $\omega{\nearrow}\omega$.
Let $\mathbf{C}$ be any perfect Polish space (i.e., complete metric separable) with a complete probability measure μ (i.e., μ is σ-additive, all Borel sets are measurable, and all subsets of measure zero sets are measurable). The reader may think of $\mathbf{C} = {}^\omega 2$, the set of all functions from ω to 2. The variable t always ranges over $\mathbf{C}$.
Analytic sets (also called $\boldsymbol{\Sigma}^1_1$ sets) are those subsets of $\mathbf{C}$ which can be obtained as projections of Borel sets in $\mathbf{C} \times {}^\omega\omega$ (or equivalently, are a continuous image of ω^ω). A subset of $\mathbf{C}$ is coanalytic or $\boldsymbol{\Pi}^1_1$ iff its complement is analytic. (All propositions below will remain true if "$\boldsymbol{\Sigma}^1_1$" and "$\boldsymbol{\Pi}^1_1$" are replaced by "Borel".) It is well known that all analytic sets are measurable. ([6], see also [7, 2H.8])
All facts from descriptive set theory that we use here can be found in Moschovakis book [7]. For facts and references about forcing consult [5].

4. Acknowledgement: Thanks to Reinhard Winkler for interesting dicussions about random numbers.

The main lemma and its application

5. Main Lemma: Assume that for each $y \in \omega{\nearrow}\omega$ we have a set $U_y \subseteq \mathbf{C}$ such that
- (A) The set $\{(y,t) : y \in \omega{\nearrow}\omega, t \in U_y\}$ is a $\boldsymbol{\Pi}^1_1$ subset of $\subseteq \omega{\nearrow}\omega \times \mathbf{C}$.
- (B) For all $y \in \omega{\nearrow}\omega$, $\mu(U_y) = 1$
- (C) If $y \le y'$ (that means $\forall n\, y(n) \le y'(n)$), then $U_y \subseteq U_{y'}$

Then $\mu(\bigcap_{y\in\omega\nearrow\omega} U_y) = 1$.

We will actually not prove the lemma itself, but an equivalent version:

6. Lemma: Assume that for each $x \in {}^\omega\omega$ we have a set $W_x \subseteq \mathbf{C}$ such that
- (A') The set $\{(x,t) : x \in {}^\omega\omega, t \in W_x\}$ is a $\boldsymbol{\Pi}^1_1$ set $\subseteq {}^\omega\omega \times \mathbf{C}$.
- (B') For all $x \in {}^\omega\omega$, $\mu(W_x) = 1$
- (C') If $x \le x'$, then $W_x \supseteq W_{x'}$

Then $\mu(\bigcap_{x\in{}^\omega\omega} W_x) = 1$.

Proof that lemma 6 implies lemma 5: For every unbounded $x \in {}^\omega\omega$ we define its "inverse" function $x^* \in \omega{\nearrow}\omega$ by

$$x^*(n) = \min\{m : x(m) \ge n\}$$

Now given a family $(U_y : y \in \omega{\nearrow}\omega)$ let $W_x := U_{x^*}$ for all unbounded $x \in {}^\omega\omega$, and $W_x = \mathbf{C}$ otherwise.
We claim $\bigcap_y U_y = \bigcap_x W_x$. The inclusion "$\subseteq$" is clear. For the converse inclusion, it is enough to see

$$\forall y \in \omega{\nearrow}\omega\, \exists x \in {}^\omega\omega : x^* \le y$$

Given $y \in \omega\nearrow\omega$, we can find a sequence x which increases so fast that for all n, $x(y(n)) \geq n$, e.g., $x(m) := \max\{k : y(k) \leq m\}$. So $x^*(n) = \min\{i : x(i) \geq n\} \leq y(n)$.
Hence $\bigcap_x W_x = \bigcap_y U_y$ has measure 1.

7. Application: let $\mathbf{C} = {}^\omega 2$ with the usual product measure. Let s range over functions in ${}^\omega\omega$ satisfying $\varphi_s \geq 0$ and $\varphi_s \to \infty$, where $\varphi_s = \lfloor \log n - \log\log n - s(n) \rfloor$. Let R_s be the set of s-uniformly distributed sequences in 2^ω, and let $R := \bigcap_s R_s$. It is easy to check that $s \leq s'$ implies $R_{s'} \subseteq R_s$, and $\varphi_{\varphi_s} = s$.
For each function $y \in \omega\nearrow\omega$ let

$$U_y = \begin{cases} R_{\varphi_y} & \text{if } y \leq \log - \log\log \\ 2^\omega & \text{otherwise} \end{cases}$$

Now check that all the assumptions of the main lemma are satisfied. If $\varphi_s \to \infty$, then letting $y := \varphi_s$ we have $s = \varphi_y$, so $R_s \supseteq R_{\varphi_y} = U_y$. Hence $R = \bigcap_s R_s$ has measure 1.

8. Remark: Note that the inclusion in lemma 5(C) or lemma 6(C') cannot be replaced by an "almost" inclusion (modulo measure zero sets or even modulo finite sets): Let F be a Borel isomorphism between ${}^\omega\omega$ and $\mathbf{C}$ (see [7, 1G4]), and let $W_x = \mathbf{C} - \{F(x)\}$, then $\bigcap_x W_x = \emptyset$.

9. Other applications: Almost every metric result in which a $o(\ )$ appears can be strenghtened by using lemma 5. For example, Drmota-Winkler showed that

$$\text{If } s(N) = o(\sqrt{N/\log N}), \text{ then } \mu(T_s) = 1,$$

where T_s is the set of s-uniformly distributed sequences $x \in [0,1]^\omega$ (see [1] for definitions and references), and $s(N) = o(\sqrt{N/\log N})$ means that $\lim_N s(N) \Big/ \sqrt{N/\log N} = 0$.

Now for $y \in \omega\nearrow\omega$ let $s_y(N) = \left\lfloor \sqrt{N/\log N} \Big/ y(N) \right\rfloor$, and let $U_y = T_{s_y}$. Applying the lemma we immediately get that

$$\mu\Big(\bigcap_s T_s\Big) = 1$$

where the intersection is taken over all s satisfying $s(N) = o(\sqrt{N/\log N})$.

Proof of lemma 6 for logicians

The set $W := \{t : \forall x\, t \in W_x\}$ is a $\mathbf{\Pi^1_1}$ set, hence measurable. Assume that $\mu(W) < 1$. So there exists a Borel (G_δ) set A with $\mu(A) < 1$ such that $W \subseteq A$. Note that the statement

$$(*) \qquad\qquad \forall t : [\forall x\, t \in W_x \;\Rightarrow\; t \in A]$$

is a $\mathbf{\Pi^1_2}$-statement, hence absolute between any two transitive universe with the same ordinals ([9], see also [7, 8F10]).
Now let r be a random real over the universe V, $r \in \mathbf{C} - A$, and work in $V[r]$. Random forcing is ${}^\omega\omega$-bounding, i.e., we have

$$\forall x \in {}^\omega\omega\, \exists x' \in {}^\omega\omega \cap V : x \leq x'$$

Since the condition (C') is also absolute, this implies $\forall x \in {}^\omega\omega\, \exists x' \in {}^\omega\omega \cap V : W_x \supseteq W_{x'}$, and so

$$\bigcap_{x \in {}^\omega\omega} W_x = \bigcap_{x' \in {}^\omega\omega \cap V} W_{x'}$$

Moreover,

$$\forall x' \in {}^\omega\omega \cap V : r \in W_{x'}$$

(since r is a random real and each $W_{x'}$ contains a Borel set of full measure), so together we get

$$\forall x \in {}^\omega\omega : r \in W_x.$$

Since $(*)$ holds also in $V[r]$, we get $V[r] \models r \in A$, a contradiction.

Proof of lemma 6 for probabilists

Now we repeat our argument in the language of probability theory. Our main tool is von Neumann's selection theorem ([8], see also [7, 4E9]).
We let our probability space be $\mathbf{C}$.
We will consider random variables (= measurable functions) T from $\mathbf{C}$ into $\mathbf{C}$, and random variables X from $\mathbf{C}$ into ${}^\omega\omega$.

10. Definition: Let $B \subseteq \mathbf{C} \times {}^\omega\omega$. We say that f "uniformizes" B iff
(1) $f \subseteq B$
(2) f is a partial function.
(3) $dom(f) = \{t : \exists x\, (t, x) \in B\}$.
The von Neumann selection theorem says that every $\mathbf{\Sigma^1_1}$ set can be uniformized by a measurable function. (Note that the possibly better known $\mathbf{\Pi^1_1}$ uniformization theorem will in general not yield measurable functions [7, 5A7].)
Hence we get:

11. Lemma: Let $B \subseteq \mathbf{C} \times {}^\omega\omega$ be a $\mathbf{\Sigma^1_1}$ set. Assume that $\forall t \in \mathbf{C}\, \exists x \in {}^\omega\omega\, (t, x) \in B$. Then
(1) $\exists X \mu[(I, X) \in B] = 1$, where I is the identity function from $\mathbf{C}$ to $\mathbf{C}$, and X ranges over all random variables in ${}^\omega\omega$.
(2) Moreover, $\forall T\, \exists X \mu[(T, X) \in B] = 1$. Here, T and X range over random variables in $\mathbf{C}$ and ${}^\omega\omega$, respectively.

Proof: (1) — There is a measurable function $f \subseteq B$ with domain $\mathbf{C}$. So for all $t \in \mathbf{C}$, $(t, f(t)) \in B$. Let $X := f$.
(2) — Let f be the function from (1), and let $X = f \circ T$.

12. Remark: Those logicians who have not skipped this section will notice that (2) is again Shoenfield's theorem, since random variables naturally correspond to $\mathbb{B}$-names of reals (where $\mathbb{B}$ is the random algebra).

We will also need the following easy fact about random variables $X : \mathbf{C} \to {}^\omega\omega$ (which corresponds to the fact that random forcing is ${}^\omega\omega$-bounding):

13. Fact: Let $X : \mathbf{C} \to {}^\omega\omega$ be a random variable. Then there is a family $(x_n : n \in \omega)$ of functions in ${}^\omega\omega$ such that

$$\mu[\exists n\, X \leq x_n] = 1$$

Proof: Call a Borel set $A \subseteq \mathbf{C}$ of positive measure "good" if there is a function $x_A \in {}^\omega\omega$ such that $A \subseteq [X \leq x_A]$. If there are finitely many good sets covering $\mathbf{C}$ (up to a measure zero set) then we are done. Otherwise, let $(A_n : n \in \omega)$ be a maximal antichain of good sets, i.e., a maximal family of sets which are

(1) good
(2) pairwise disjoint

Such a sequence can be found using Zorn's lemma. Again, if $\bigcup_n A_n$ covers $\mathbf{C}$ up to a measure zero set then we are done. So assume that $A := \mathbf{C} - \bigcup_n A_n$ has positive measure ε. Define a sequence $(k_n : n \in \omega)$ of natural numbers such that for each n the set $[X(n) > k_n]$ has measure $< \varepsilon/2^{n+3}$. Thus, the set $[\forall n\, X(n) \leq k_n] \cap A$ has measure $\geq \varepsilon - \varepsilon/4 > 0$, contradicting the maximality of the family $(A_n : n \in \omega)$.

14. Second proof of lemma 6: Let $I : \mathbf{C} \to \mathbf{C}$ be the identity function. Clearly, for any $x \in {}^\omega\omega$ we have $\mu[I \in W_x] = \mu(W_x) = 1$.
We now claim that the same is still true if we replace x by a random variable X. Indeed, let X be a random variable, $X : \mathbf{C} \to {}^\omega\omega$. Then we can find a family of functions $(x_n : n \in \omega)$ such that

$$\mu[\exists n\, X \leq x_n] = 1$$

Using the anti-monotonicity of the family $(W_x : x \in {}^\omega\omega)$ we get

$$\mu[\exists n\, W_X \supseteq W_{x_n}] = 1$$

and so: $\mu[W_X \supseteq \bigcap_n W_{x_n}] = 1$. Hence

$$(*) \qquad \mu[I \in W_X] \geq \mu[I \in \bigcap_n W_{x_n}] = \mu(\bigcap_n W_{x_n}) = 1$$

for all random variables X. So for all X $\mu[I \notin W_X] = 0$, hence by the contrapositive of lemma 11 it is impossible that $\forall t\, \exists x\; t \notin W_x$. Therefore

$$\exists t\, \forall x\; t \in W_x$$

So the set $\bigcap_x W_x$ is nonempty. Relativizing the above argument to any positive Borel set A we can show that the set $A \cap \bigcap_x W_x$ is nonempty. Hence W has outer measure 1. As remarked above, W must be measurable, so indeed $\mu(W) = 1$.

References.

[1] M. Drmota and R. Winkler, $s(N)$-uniform distribution modulo 1.

[2] P. Flajolet, P. Kirschenhofer and R.F. Tichy, Deviations from uniformity in random strings, Probab. Th. Rel. Fields 80 (1988), 139–150.

[3] P. Grabner, Block Distribution in Random Strings, Annales de l'Institut Fourier.

[4] K. Grill, A note on Randomness, Stat. and Probab. Letters.

[5] T. Jech, Multiple forcing, Cambridge Tracts in Mathematics 88, Cambridge 1986.

[6] N. Lusin, Sur la classification de M. Baire, Comptes Rendus Acad. Sci. Paris 164 (1917) 91–94.

[7] Y.N. Moschovakis, Descriptive Set Theory, Studies in Logic and the foundation of Mathematics, vol 100, North-Holland 1980.

[8] J. von Neumann, On rings of operators. Reduction theory. Ann. Math. 50 (1949) 448–451.

[9] J.R. Shoenfield, The problem of predicativity, Essay on the foundation of Mathematics, Magnes Press, Hebrew Univ. Jerusalem (1961) 132–139.

[10] R.F. Tichy, Zur Analyse und Anwendung von Zufallszahlen, Jahrbuch d. Kurt Goedel Ges. 109–116 (1990

[11] R. Winkler, Some remarks on Pseudorandom Sequences.

Martin Goldstern
2. Mathematisches Institut
FU Berlin
Arnimallee 3
1000 Berlin 33

`goldstrn@math.fu-berlin.de`