

London Mathematical Society Lecture Note Series: 382

Forcing with Random Variables and Proof Complexity

JAN KRAJÍČEK
Charles University, Prague



CAMBRIDGE
UNIVERSITY PRESS

Contents

<i>Preface</i>	<i>page</i> xiii
<i>Acknowledgements</i>	xv
Introduction	1
Organization of the book	3
Remarks on the literature	5
Background	5
 PART I: BASICS	 7
1 The definition of the models	9
1.1 The ambient model of arithmetic	9
1.2 The Boolean algebras	10
1.3 The models $K(F)$	12
1.4 Valid sentences	13
1.5 Possible generalizations	14
2 Measure on \mathcal{B}	16
2.1 A metric on \mathcal{B}	16
2.2 From Boolean value to probability	17
3 Witnessing quantifiers	19
3.1 Propositional approximation of truth values	20
3.2 Witnessing in definable families	23
3.3 Definition by cases by open formulas	25
3.4 Compact families	29
3.5 Propositional computation of truth values	30
4 The truth in \mathbf{N} and the validity in $K(F)$	34

PART II: SECOND-ORDER STRUCTURES	37
5 Structures $K(F, G)$	39
5.1 Language L^2 and the hierarchy of bounded formulas	40
5.2 Cut \mathcal{M}_n , languages L_n and L_n^2	41
5.3 Definition of the structures	42
5.4 Equality of functions, extensionality and possible generalizations	44
5.5 Absoluteness of $\forall\Sigma_\infty^b$ -sentences of language L_n	45
PART III: AC^0 WORLD	47
6 Theories $I\Delta_0, I\Delta_0(R)$ and V_1^0	49
7 Shallow Boolean decision tree model	52
7.1 Family F_{rud}	52
7.2 Family G_{rud}	53
7.3 Properties of F_{rud} and G_{rud}	54
8 Open comprehension and open induction	55
8.1 The $\langle\langle \dots \rangle\rangle$ notation	55
8.2 Open comprehension in $K(F_{rud}, G_{rud})$	56
8.3 Open induction in $K(F_{rud}, G_{rud})$	57
8.4 Short open induction	58
9 Comprehension and induction via quantifier elimination: a general reduction	60
9.1 Bounded quantifier elimination	60
9.2 Skolem functions in $K(F, G)$ and quantifier elimination	61
9.3 Comprehension and induction for $\Sigma_0^{1,b}$ -formulas	61
10 Skolem functions, switching lemma and the tree model	63
10.1 Switching lemma	63
10.2 Tree model $K(F_{tree}, G_{tree})$	66
11 Quantifier elimination in $K(F_{tree}, G_{tree})$	70
11.1 Skolem functions	70
11.2 Comprehension and induction for $\Sigma_0^{1,b}$ -formulas	74
12 Witnessing, independence and definability in V_1^0	75
12.1 Witnessing $\forall X < x \exists Y < x \Sigma_0^{1,b}$ -formulas	76
12.2 Preservation of true $s\Pi_1^{1,b}$ -sentences	77
12.3 Circuit lower bound for parity	79

PART IV: $AC^0(2)$ WORLD	81
13 Theory $Q_2V_1^0$	83
13.1 Q_2 quantifier and theory $Q_2V_1^0$	83
13.2 Interpreting Q_2 in structures	84
14 Algebraic model	85
14.1 Family F_{alg}	85
14.2 Family G_{alg}	87
14.3 Open comprehension and open induction	88
15 Quantifier elimination and the interpretation of Q_2	89
15.1 Skolemization and the Razborov–Smolensky method	89
15.2 Interpretation of Q_2 in front of an open formula	92
15.3 Elimination of quantifiers and the interpretation of the Q_2 quantifier	94
15.4 Comprehension and induction for $Q_2\Sigma_0^{1,b}$ -formulas	95
16 Witnessing and independence in $Q_2V_1^0$	96
16.1 Witnessing $\forall X < x\exists Y < x\forall Z < x\Sigma_0^{1,b}$ -formulas	96
16.2 Preservation of true $s\Pi_1^{1,b}$ -sentences	98
PART V: TOWARDS PROOF COMPLEXITY	99
17 Propositional proof systems	101
17.1 Frege and Extended Frege systems	101
17.2 Language with connective \oplus and constant-depth Frege systems	103
18 An approach to lengths-of-proofs lower bounds	105
18.1 Formalization of the provability predicate	105
18.2 Reflection principles	107
18.3 Three conditions for a lower bound	108
19 PHP principle	110
19.1 First-order and propositional formulations of PHP	110
19.2 Three conditions for F_d and $F_d(\oplus)$ lower bounds for PHP	111
PART VI: PROOF COMPLEXITY OF F_d AND $F_d(\oplus)$	113
20 A shallow PHP model	115
20.1 Sample space Ω_{PHP}^0 and PHP-trees	115

20.2	Structure $K(F_{\text{PHP}}^0, G_{\text{PHP}}^0)$ and open comprehension and open induction	118
20.3	The failure of PHP in $K(F_{\text{PHP}}^0, G_{\text{PHP}}^0)$	121
21	Model $K(F_{\text{PHP}}, G_{\text{PHP}})$ of V_1^0	123
21.1	The PHP switching lemma	123
21.2	Structure $K(F_{\text{PHP}}, G_{\text{PHP}})$	124
21.3	Open comprehension, open induction and failure of PHP	127
21.4	Bounded quantifier elimination	128
21.5	PHP lower bound for F_d : a summary	131
22	Algebraic PHP model?	132
22.1	Algebraic formulation of PHP and relevant rings	134
22.2	Nullstellensatz proof system NS and designs	135
22.3	A reduction of $F_d(\oplus)$ to NS with extension polynomials	136
22.4	A reduction of polynomial calculus PC to NS	138
22.5	The necessity of partially defined random variables	141
	PART VII: POLYNOMIAL-TIME AND HIGHER WORLDS	147
23	Relevant theories	149
23.1	Theories PV and $\text{Th}_V(L_{\text{PV}})$	149
23.2	Theories S_2^1 , T_2^1 and BT	150
23.3	Theories U_1^1 and V_1^1	151
24	Witnessing and conditional independence results	153
24.1	Independence for S_2^1	154
24.2	S_2^1 versus T_2^1	155
24.3	PV versus S_2^1	157
24.4	Transfer principles	160
25	Pseudorandom sets and a Löwenheim–Skolem phenomenon	163
26	Sampling with oracles	168
26.1	Structures $K(F_{\text{oracle}})$ and $K(F_{\text{oracle}}, G_{\text{oracle}})$	168
26.2	An interpretation of random oracle results	169
	PART VIII: PROOF COMPLEXITY OF EF AND BEYOND	171
27	Fundamental problems in proof complexity	173
28	Theories for EF and stronger proof systems	179
28.1	First-order context for EF: PV and S_2^1	179

28.2	Second-order context for EF: VPV and V_1^1	180
28.3	Stronger proof systems	181
29	Proof complexity generators: definitions and facts	183
29.1	τ -formulas and their hardness	184
29.2	The truth-table function	187
29.3	Iterability and the completeness of $\mathbf{tt}_{s,k}$	189
29.4	The Nisan–Wigderson generator	190
29.5	Gadget generators	192
29.6	Optimal automatizer for the τ -formulas	194
30	Proof complexity generators: conjectures	197
30.1	On provability of circuit lower bounds	197
30.2	Razborov’s conjecture on the NW generator and EF	201
30.3	A possibly hard gadget	204
30.4	Rudich’s demi-bit conjecture	205
31	The local witness model	207
31.1	The local witness model $K(F_b)$	207
31.2	Regions of undefinability	209
31.3	Properties of the local model $K(F_b)$	213
31.4	What does and what does not follow from $K(F_b)$	214
	<i>Appendix: Non-standard models and the ultrapower construction</i>	219
	<i>Standard notation, conventions and list of symbols</i>	230
	<i>References</i>	236
	<i>Name index</i>	243
	<i>Subject index</i>	245