Implementation of bit-vector variables in a constraint solver with an application to the generation of cryptographic S-boxes

Kellen Dye

Constraint programming

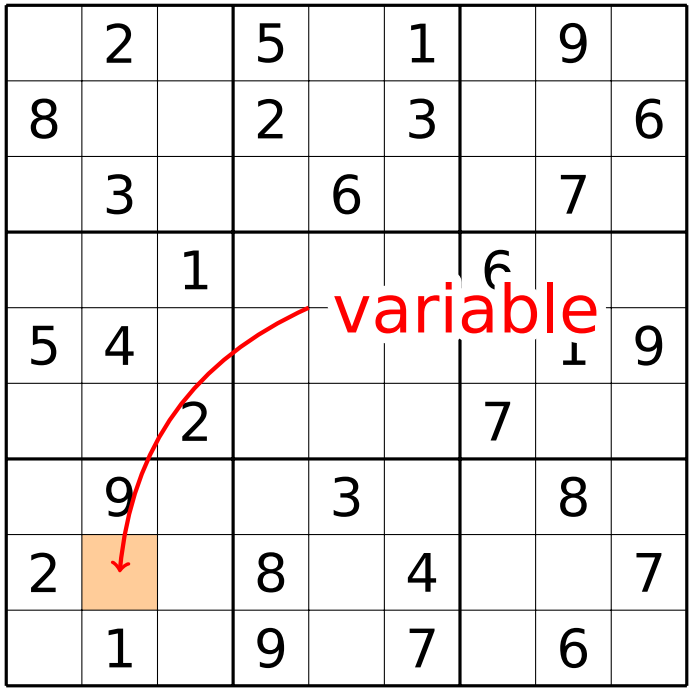
Constraint programming

Variables
Domains
Constraints

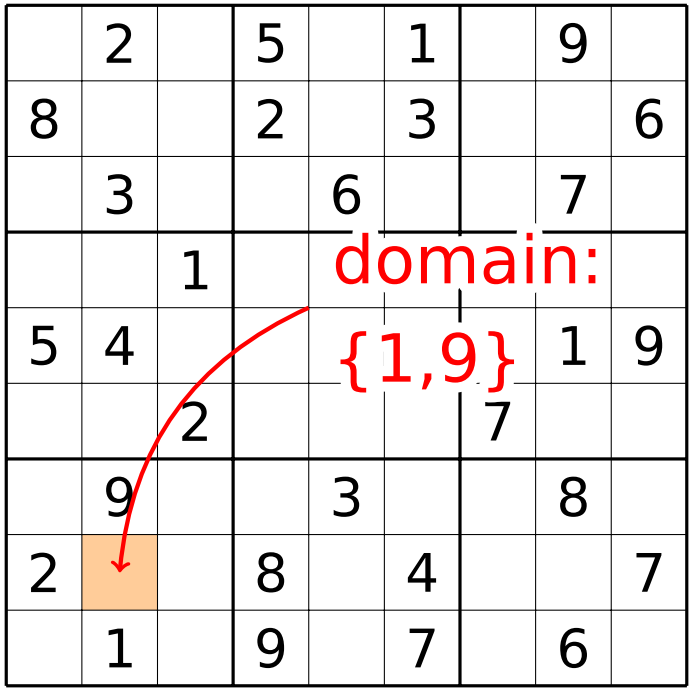
Sudoku

	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

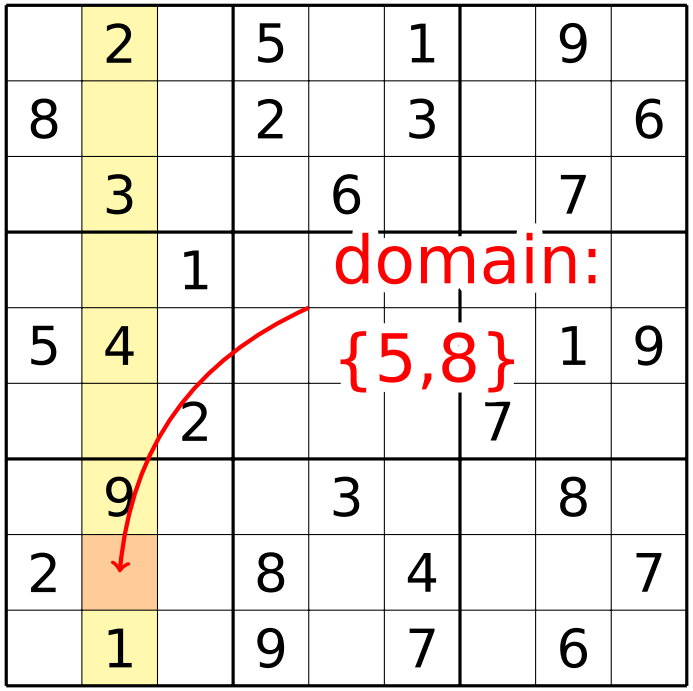
Sudoku: variables



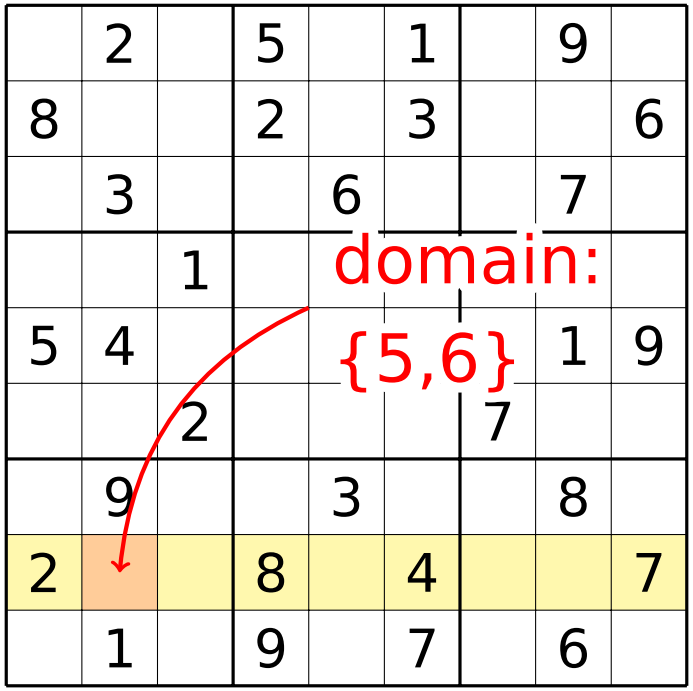
Sudoku: domains



Sudoku: constraints: columns



Sudoku: constraints: rows



Sudoku: constraints: blocks