Coq/SSReflect の extraction の改善

坂口和彦　亀山幸義　(筑波大学)

SSReflect は広く使われている Coq のライブラリである。これは元々数学の問題の形式化のために作られたものだが、その中には有限集合型などプログラミングに有用な道具も含まれている。しかし、有限集合型に関する定義の多くはそのまま program extraction して計算に使うには不向きである。本研究では SSReflect の有限集合型をより計算に向いた形で再定義し、実行時間がどの程度変化するかを調べる。

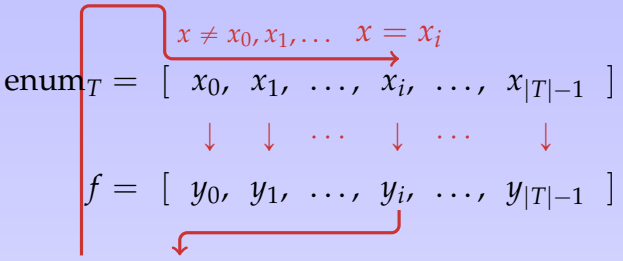
変更前

T は有限集合型 (T : finType)

↳ T の要素を重複無く列挙できる:

$\mathrm{enum}_T : \mathrm{seq}(T), \qquad \forall x : T.\, |\mathrm{enum}_T|_x = 1$

f は有限集合からの関数 ($f : \{\mathrm{ffun}\, T \to A\}$)



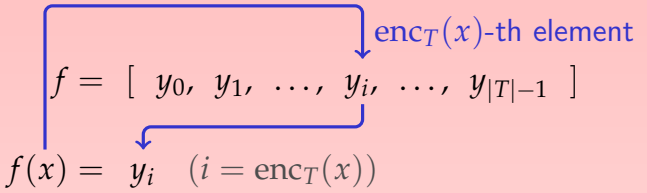
変更後 [3]

T は有限集合型 (T : finType)

↳ T と $\{0, \ldots, |T|-1\}$ の間に全単射が存在する:

$\mathrm{enc}_T : T \to {}'I_{|T|}, \qquad \mathrm{dec}_T : {}'I_{|T|} \to T$

f は有限集合からの関数 ($f : \{\mathrm{ffun}\, T \to A\}$)



その他の工夫:

finfun の定義に使われている tuple を配列型として extract し、リストから配列、またはその逆の変換をなるべく使わないようにいくつかの関数を再定義した。

実験

プレスバーガー算術に関する各種判定問題を有限オートマトンの問題に帰着して解く決定手続き [1, 2, 4] を例に取り、変更の前後でどの程度速度に差が出るかを調べた。Extract 先の言語としては OCaml を用いた。

実験結果 (satisfiability)

論理式	状態数	計算結果	実行時間 (×10)[s]	
			変更前	変更後
$2 \leqslant 2x + y \wedge 3x \leqslant 2y \wedge 3y \leqslant 2x + 3$	252	UNSAT	0.052	0.040
$2 \leqslant x + y \wedge x \leqslant 2 \wedge y \leqslant 2 \wedge x + y = 1 + 4z$	640	UNSAT	0.216	0.184
$2 \leqslant 2x + y \wedge 5x \leqslant 4y \wedge 5y \leqslant 4x + 5$	660	UNSAT	0.124	0.100
$1 \leqslant x + y \wedge x + y \leqslant 6 \wedge 3x \leqslant 5y \wedge 5y \leqslant 4x$	3240	SAT	0.156	0.120
$2 \leqslant x + y \wedge 3x \leqslant 6 + y \wedge 3y \leqslant 6 + x \wedge x + y = 1 + 4z$	4000	UNSAT	0.888	0.760
$3 \leqslant x + y \wedge x + y \leqslant 5 \wedge 5x \leqslant 7 + 2y \wedge 3 + 3y \leqslant 5x$	5616	SAT	0.164	0.128

参考文献

[1] Alexandre Boudet and Hubert Comon. "Diophantine equations, Presburger arithmetic and finite automata". In: *Trees in Algebra and Programming — CAAP '96*. Springer, 1996, pp. 30–43.

[2] Javier Esparza. *Automata Theory: An Algorithmic Approach*. 2012. URL: https://www7.in.tum.de/~esparza/automatanotes.html.

[3] Kazuhiko Sakaguchi. *Modified-fintype Branch on Mathematical Components Repository*. URL: https://github.com/pi8027/math-comp/tree/modified-fintype.

[4] 坂口和彦. *Coq による定理証明 - 2015.12*. Tsukuba Coq Users' Group, 2015.

Coq による定理証明 2015 12
坂口和彦
Tsukuba Coq Users' Group