Decompositions of Natural Numbers: From A Case Study in Mathematical Theory Exploration
Proofs of Properties in the Original Paper ⋆

Adrian Crăciun, Mădălina Hodorog ⋆⋆

Institute e-Austria
Bd. Vasile Pârvan No. 4
300223 Timişoara, Romania
{acraciun, mhodorog}@ieat.ro

Abstract. In this technical report we present the proofs of properties appearing when solving the problem of prime decomposition of natural numbers using a scheme-based systematic exploration model recently proposed by Bruno Buchberger. The proofs of these properties use definitions and propositions invented using knowledge schemes in the exploration process and proved using the Theorema system. The proofs in this paper are close to what the Theorema system will produce.

1 Introduction

In this technical reports we present the proofs of the properties appearing when solving the problem of prime decomposition of natural numbers using the scheme based systematic exploration model recently proposed by Bruno Buchberger [2, 4]. We start from the well-known axioms of natural numbers and develop the theory in exploration rounds, by introducing new notions (using definition schemes), exploring their properties (using proposition schemes), solving problems involving the notions (introduced by problem schemes, see [1, 3]). For more information on the development of the theory of natural number using the scheme-based exploration model, see [6, 7]. In the proofs we use definitions and propositions introduced when developing the theory of natural numbers, see the Appendix for their full form. For more information on the invention and the proof of these properties, see [6].

2 A Composed Object is not Irreducible

Assume, on a domain described by obj, with predicates $<$, P, $is\text{-}comp$, function $\bigotimes$, constant e (arbitrary but fixed constants), that:

⋆ Work supported by EU Marie Curie Project MERG-CT-2004-012718: SysteMaThEx.

⋆⋆ Corresponding author.

$$\textit{is-well-founded}[<, e, obj],$$
$$\textit{is-irreducible-property}[P, <, e, obj],$$
$$\textit{is-composition-property}[\textit{is-comp}, \bigotimes, <, e, obj].$$

Then,

$$\underset{\substack{obj[x] \\ e<x}}{\forall} (\textit{is-comp}[\bigotimes][x] \Rightarrow \neg P[x])$$

The proof of this property can be easily done by predicate logic.

Proof. Take arbitrary but fixed x_0 such that $obj[x_0]$ and $e < x_0$.
Assume $\textit{is-comp}[\bigotimes][x_0]$, (1)
Show $\neg P[x_0]$.
We prove by contradiction: Assume $P[x_0]$, i.e., $\underset{\substack{obj[y] \\ e<y}}{\forall} y \not< x$. (2)
From (1) and $\textit{is-composition-property}[\textit{is-comp}, \otimes, <, e, obj]$,

$$\underset{\substack{obj[y], obj[z] \\ e<y, e<z}}{\exists} x_0 = y \otimes z,$$

so we can take y_0, z_0 s.t. $obj[y_0], obj[z_0]$, $e < y_0, e < z_0$ and

$$x_0 = y_0 \otimes z_0 \ . \ (3)$$

From $\textit{is-composition-property}[\textit{is-comp}, \otimes, <, e, obj]$ we know

$$\textit{is-compatible-composition}[\otimes, <, e, obj], \text{ i.e.}$$

$$\underset{\substack{obj[x,y,z] \\ e<x, e<y, e<z}}{\forall} ((x = y \otimes z) \Rightarrow y < x \wedge z < x. \ (4)$$

From (3), (4), by modus ponens we get: $y_0 < x_0 \wedge z_0 < x$ which is in contradiction with (2).

3 Connection between divides (|) and multiplication (∗) function symbols.

We prove the following lemma, which expresses the connection between the divides (|) and the multiplication function symbols:

$$\texttt{Proposition}[\text{“connection divides and multiplication”},$$
$$\texttt{any}[\textit{is-nat}[y, z], \textit{is-greater-1}[y, z]],$$
$$y | y * z\,],$$

Proof. Take y_0 arbitrary but fixed such that $\textit{is-nat}[y_0], y_0 > 1$.
Show $\underset{\textit{is-nat}[z]}{\forall} y_0 | y_0 * z$. (1)
We proof formula (1) by complete induction on the $<$ predicate symbol.
Take z_0 arbitrary but fixed such that $\textit{is-nat}[z_0], z_0 > 1$.
Assume $\underset{\substack{\textit{is-nat}[z] \\ z<z_0}}{\forall} y_0 | y_0 * z$. ($\diamondsuit$)
Show $y_0 | y_0 * z_0$. (2)
By applying the definition of '|'in formula (2) we have to prove:
$y_0 | y_0 * z_0 - y_0$. (3)
By applying the distributivity of '$-$' towards '$*$' in formula (3), we have to prove:
$y_0 | y_0 * (z_0 - 1)$. (4)
By the hypothesis we have $z_0 > 1$. In the exploration process we have to prove the following property $\underset{\textit{is-nat}[z]}{\forall} z - 1 < z$.
Instantiating in this property $z \leftarrow z_0$ we obtain $z_0 - 1 < z_0$. (5)
We instantiate $z \leftarrow z_0 - 1$ in formula ($\diamondsuit$) based on formula (5), and we obtain:
$y_0 | y_0 * (z_0 - 1)$, so formula (4) holds.

4 Natural Numbers Form a Decomposition Domain

We prove that natural numbers form a decomposition domain:

$$\textit{is-decomposition-domain}[\textit{is-nat}, *, \textit{is-prime}, \lhd, 1] \Leftrightarrow \bigwedge \begin{cases} \textit{is-compatible-composition}[*, \lhd, 1, \textit{is-nat}] \ (1) \\ \textit{is-irreducible-property}[\textit{is-prime}, \lhd, 1, \textit{is-nat}] \ (2) \\ \underset{\textit{is-nat}[x]}{\forall} \ \underset{\substack{\textit{is-nat}[y,z] \\ 1 \lhd y, 1 \lhd z}}{\exists} x = y * z \ (3) \\ \neg \textit{is-prime}[x] \wedge 1 \lhd x \end{cases},$$

that is prove formulae (1),(2) and (3).

Proof (1). We prove $\textit{is-well-founded}[\lhd, 1, \textit{is-nat}]$ (1.1) and

$$\underset{\substack{\textit{is-nat}[x,y,z] \\ 1 \lhd x, 1 \lhd y, 1 \lhd z}}{\forall} ((x = y * z) \Rightarrow y \lhd x \wedge z \lhd x) \ (1.2)$$

Formula (1.1) is successfully proved in the exploration process.
We now prove formula (1.2).
Take x_0, y_0, z_0 arbitrary but fixed such that $\textit{is-nat}[x_0, y_0, z_0], 1 \lhd x_0, 1 \lhd y_0, 1 \lhd z_0$.
Assume $x_0 = y_0 * z_0$ (4).
Show $y_0 \lhd x_0 \wedge z_0 \lhd x_0$(5) .
We prove only $y_0 \lhd x_0$, as (5.2) is proved analogically.
From the definition of $\lhd$, we have to prove: $y_0 \neq x_0 \wedge y_0 | x_0$.
We prove $y_0 \neq x_0$ by contradiction. We assume $y_0 = x_0$, so (4) becomes

$x_0 = x_0 * z_0 \Rightarrow z_0 = 1$, which is in contradiction with $1 \lhd z_0$.
We prove $y_0|x_0$. By (4), we have to prove $y_0|y_0 * z_0$ (6).
In the exploration process we successfully proved the following lemma

$$\underset{is\text{-}nat[y,z]}{\forall} y|y * z.$$

Instantiatiating $y \leftarrow y_0, z \leftarrow z_0$ in this lemma we obtain the formula (6).

Proof (2). Formula (2) holds because the *is-irreducible-property*[*is-prime*, $\lhd$, 1, *is-nat*] generates the definition for the *is-prime* predicate symbol:

$$\underset{\substack{is\text{-}nat[x]\\ 1\lhd x}}{\forall} is\text{-}prime[x] \Leftrightarrow \underset{\substack{is\text{-}nat[y]\\ 1\lhd y}}{\forall} y \not\lhd x.$$

Proof (3). Take x_0 arbitrary but fixed such that $is\text{-}nat[x_0], \neg is\text{-}prime[x_0], 1 \lhd x_0$.
Show $\underset{\substack{is\text{-}nat[y,z]\\ 1\lhd y \wedge 1\lhd z}}{\exists} x_0 = y * z$ (7).
From the definition of *is-prime* predicate symbol, instantiating $x \leftarrow x_0$:

$$\neg is\text{-}prime[x_0] \Rightarrow \neg(\underset{\substack{is\text{-}nat[y]\\ 1\lhd y}}{\forall} y \not\lhd x_0),$$

which is equivalent with:

$$\neg is\text{-}prime[x_0] \Rightarrow \underset{\substack{is\text{-}nat[y]\\ 1\lhd y}}{\exists} y \lhd x_0 \ (8).$$

Take y_0 such that $is\text{-}nat[y_0], 1 \lhd y_0$. By (8), $y_0 \lhd x_0$.
In the exploration process, we prove the proposition:

$$\underset{\substack{is\text{-}nat[x,y]\\ y\neq 0}}{\forall} y|x \Rightarrow r[x,y] = 0, \text{which implies } \underset{\substack{is\text{-}nat[x,y]\\ 1\lhd x \wedge 1\lhd y\\ x\neq y}}{\forall} y \lhd x \Rightarrow r[x,y] = 0.$$

Using this formula, the *quotient-remainder* theorem becomes:

$$\underset{\substack{is\text{-}nat[x,y]\\ 1\lhd x \wedge 1\lhd y\\ x\neq y}}{\forall} x = y * q[x,y] (9).$$

Instantiating $x \leftarrow x_0, y \leftarrow y_0$ in this formula we obtain:

$$x_0 = y_0 * q[x_0, y_0], \text{with } 1 \lhd y_0.$$

We still have to show $1 \lhd q[x_0, y_0]$, that is $1 \neq q[x_0, y_0] \wedge 1|q[x_0, y_0]$.
We show $1 \neq q[x_0, y_0]$ by contradiction. We assume $1 = q[x_0, y_0]$. By (9) this formula implies $x_0 = y_0 * 1 \Rightarrow x_0 = y_0$, which is in contradiction with $y_0 \lhd x_0$.

5 Conclusion

This technical report contains only the proofs of the properties that appear when solving the prime decomposition problem of natural numbers. They follow the rules of predicate logic and need no extra information about the prime decomposition problem or algorithm. The proofs are also similar with the result the THEOREMA system will produce. For more information on the prime decomposition problem, the reader can consult directly the paper, [5].

References

1. Buchberger, B.: Algorithm Invention and Verification by Lazy Thinking. In D. Petcu, V. Negru, D. Zaharie, and T. Jebelean, editors, *Proceedings of SYNASC 2003, 5th International Workshop on Symbolic and Numeric Algorithms for Scientific Computing Timisoara*, pages 2-26, Timisoara, Romania, 1-4 October 2003. Copyright: Mirton Publisher.
2. Buchberger, B.: Algorithm–Supported Mathematical Theory Exploration: A Personal View and Strategy. Lecture Notes in Artificial Intelligence, Springer, 7th Conference on Artificial Intelligence and Symbolic Computation(Research Institute for Symbolic Computation, Hagenberg, Austria) (Proceedings of AISC 2004):16, September.
3. Buchberger, B., Crăciun, A.: Algorithm Synthesis by Lazy Thinking: Examples and Implementation in Theorema. In F. Kamareddine, editor, *Electronic Notes in Theoretical Computer Science*, volume **93**, pages 24-59, 18 February 2004. Proc. of the Mathematical Knowledge Management Workshop, Edinburgh, Nov. 25, 2003.
4. Buchberger, B., Crăciun A., Jebelean T., Kovacs L., Kutsia T., Nakagawa K., Piroi F., Popov N., Robu J., Rosenkranz M., Windsteiger W.: Theorema: Towards Computer-Aided Mathematical Theory Exploration. Journal of Applied Logic, pages 470-504, 2006.
5. Crăciun, A., Hodorog, M.: Decompositions of Natural Numbers: From A Case Study in Mathematical Theory Exploration. To appear.
6. Hodorog, M.: Scheme–based Systematic Exploration of Mathematical Theories. Case study: The Natural Numbers. Technical Report no.07-06, I-Eat, 2006.
7. Hodorog, M., Crăciun, A.: Scheme-Based Systematic Exploration of Natural Numbers. *Proceedings of SYNASC 2006, 8th International Workshop on Symbolic and Numeric Algorithms for Scientific Computing Timisoara, Romania (2006)*, pages 23-34, Timisoara, Romania, September 26-29 2006. IEEE Computer Society Press.

Notions Used in the Proofs

Knowledge Schemes

$$\underset{p,r}{\forall}(\mathit{is\text{-}strict\text{-}partial\text{-}ordering}[p,r] \Leftrightarrow \underset{p[x,y,z]}{\forall} \bigwedge \begin{cases} \neg(r[x,x]) \\ (r[x,y] \wedge r[y,z]) \Rightarrow r[x,z]\ ) \\ r[x,y] \Rightarrow \neg(r[y,x]) \end{cases},$$

$$\underset{e,<,obj}{\forall} \mathit{is\text{-}minimal\text{-}element}[e,<,obj] \Leftrightarrow (obj[e] \bigwedge \underset{obj[x],x\neq e}{\forall} e < x)\ .$$

$$\underset{<,e,obj}{\forall} \mathit{is\text{-}well\text{-}founded}[<,e,obj] \Leftrightarrow \bigwedge \begin{cases} \mathit{is\text{-}strict\text{-}partial\text{-}ordering}[<,obj] \\ \mathit{is\text{-}minimal\text{-}element}[e,<,obj] \end{cases},$$

$$\underset{P,<,e,obj}{\forall} \mathit{is\text{-}irreducible\text{-}property}[P,<,e,obj] \Leftrightarrow \bigwedge \begin{cases} \mathit{is\text{-}well\text{-}founded}[<,e,obj] \\ \underset{\substack{obj[x] \\ e<x}}{\forall} P[x] \Leftrightarrow \underset{\substack{obj[y] \\ e<y}}{\forall} y \not< x \end{cases}.$$

$$\underset{\bigotimes,<,e,obj}{\forall} \mathit{is\text{-}compatible\text{-}composition}[\bigotimes,<,e,obj] \Leftrightarrow \bigwedge \begin{cases} \mathit{is\text{-}well\text{-}founded}[<,e,obj] \\ \underset{\substack{obj[x,y,z] \\ e<x,e<y,e<z}}{\forall} ((x = y \bigotimes z) \Rightarrow y < x \wedge z < x) \end{cases}.$$

$$\underset{is\text{-}red,<,e,\bigotimes,obj}{\forall} \mathit{is\text{-}composition\text{-}property}[\mathit{is\text{-}comp},\bigotimes,<,e,obj] \Leftrightarrow \bigwedge \begin{cases} \mathit{is\text{-}compatible\text{-}composition}[\bigotimes,<,e,obj] \\ \underset{\substack{obj[x] \\ e<x}}{\forall} \mathit{is\text{-}comp}[\bigotimes][x] \Leftrightarrow \underset{\substack{obj[y],obj[z] \\ e<y,e<z}}{\exists} x = y \bigotimes z \end{cases}.$$

$$\underset{\otimes,<,e,obj}{\forall} \mathit{is\text{-}decomposition\text{-}domain}[obj,\otimes,P,<,e] \Leftrightarrow \bigwedge \begin{cases} \mathit{is\text{-}compatible\text{-}composition}[\otimes,<,e,obj] \\ \mathit{is\text{-}irreducible\text{-}property}[P,<,e,obj] \\ \underset{\substack{obj[x] \\ \neg P[x] \wedge e<x}}{\forall} \underset{\substack{obj[y,z] \\ e<y \\ e<z}}{\exists} x = y \otimes z \end{cases}.$$

Definitions

$$\texttt{Definition}[\text{“divides relation symbol”}, \texttt{any}[\mathit{is\text{-}nat}[x],\mathit{is\text{-}nat}[y]], x|y = \begin{cases} \texttt{True} & \Leftarrow y = 0 \\ \texttt{False} & \Leftarrow x > y \\ x|(y-x) & \Leftarrow \mathit{otherwise} \end{cases}],$$

$$\texttt{Definition}[\text{“proper divides predicate symbol”},\ \texttt{any}[\textit{is-nat}[x],\ \textit{is-nat}[y]],\ ((x \lhd y) \Leftrightarrow ((x|y) \wedge (x = y)))\,].$$

$$\texttt{Definition}[\text{“is-positive predicate symbol”},\ \texttt{any}[\textit{is-nat}[x]],\ \textit{is-positive}[x] \Leftrightarrow x \neq 0.],$$

$$\texttt{Definition}[\text{“quotient”},\ \texttt{any}[\textit{is-nat}[x], \textit{is-nat}[y]],\ \mathrm{quot}[x,y] = \begin{cases} 0 & \Leftarrow x < y \\ \mathrm{quot}[x-y,y]+1 & \Leftarrow \text{otherwise} \end{cases}],$$

$$\texttt{Definition}[\text{“remainder”},\ \texttt{any}[\textit{is-nat}[x], \textit{is-nat}[y]],\ \mathrm{rem}[x,y] = \begin{cases} x & \Leftarrow x < y \\ \mathrm{rem}[x-y,y] & \Leftarrow \text{otherwise} \end{cases}].$$

Properties

$$\texttt{Proposition}[\text{“quotient-remainder theorem”},\ \texttt{any}[\textit{is-nat}[x], \textit{is-positive}[y]],\ x = y * \mathrm{quot}[x,y] + \mathrm{rem}[x,y] \wedge \mathrm{rem}[x,y] < y],$$