日本ソフトウェア科学会第 33 回大会 (2016 年度) 講演論文集

Church-Rosser Theorem and Compositional Z-Property

Ken-etsu Fujita and Koji Nakazawa

The Church-Rosser theorem is one of the most fundamental properties on rewriting systems. In order to prove the theorem for beta-equality, Church and Rosser extracted the key property called confluence or so-called Strip lemma. Then the theorem can be proved by induction on the number of peaks from the key property. Here, the key property can be verified by using well-known notions such as parallel reduction and residuals. Although confluence and the Church-Rosser property are equivalent to each other, the property of confluence is a special case of the theorem. First, we investigate *directly* the theorem from the viewpoint of Takahashi translation, which provides a new and constructive proof of the theorem. The proof method has recently been established by the first author. Next, we show that the method is available as well under a general framework of the *compositional Z* (Nakazawa-Fujita) that makes it possible to apply a divide-and-conquer method for proving the *Church-Rosser property*.

1 Introduction

The Church-Rosser theorem [3] is one of the most fundamental properties on rewriting systems, which guarantees uniqueness of computation and consistency of a formal system. For instance, for proof trees and formulae of logic the unique normal forms of the corresponding terms and types in a Pure Type System (PTS) can be chosen as their denotations [24] via the Curry-Howard isomorphism.

The Church-Rosser theorem for β-equality states that if $M =_\beta N$ then there exists P such that $M \twoheadrightarrow P$ and $N \twoheadrightarrow P$. Here, we write $M =_\beta N$ iff M is obtained from N by a finite series of reductions ($\twoheadrightarrow$) and reversed reductions ($\twoheadleftarrow$). As the Church-Rosser theorem for β-reduction (confluence) has been well studied, to the best of our knowledge the Church-Rosser theorem for β-equality is always *secondary* proved as a corollary from the theorem for β-reduction [3] [4] [2] [9].

In order to prove the theorem, Church and Rosser extracted the key property of confluence. The property states that if $M \twoheadrightarrow N_1$ and $M \twoheadrightarrow N_2$ then we have $N_1 \twoheadrightarrow P$ and $N_2 \twoheadrightarrow P$ for some P. Two proof techniques of the property are well known; tracing the residuals of redexes along a sequence of reductions [3] [2] [9], and working with parallel reduction [4] [2] [9] [22] known as the method of Tait and Martin-Löf. Moreover, a simpler proof of the theorem is established only with Takahashi's translation [22] (the Gross-Knuth reduction strategy [2]), but with no use of parallel reduction [14] [5].

One of our motivation is to analyze quantitative properties in general of reduction systems. For instance, measures for developments are investigated by Hindley [8] and de Vrijer [21]. Statman [19] proved that deciding the $\beta\eta$-equality of typable λ-terms is not elementary recursive. Schwichtenberg [17] analysed the complexity of normalization in

チャーチ・ロッサーの定理と合成的 Z-特性.

藤田 憲悦, 群馬大学大学院理工学府, Graduate School of Science and Technology, Gunma University.
中澤 巧爾, 名古屋大学大学院情報科学研究科, Graduate School of Information Science, Nagoya University.

the simply typed lambda-calculus, and showed that the number of reduction steps necessary to reach the normal form is bounded by a function at the fourth level of the Grzegorczyk hierarchy ε^4 [7], i.e., a non-elementary recursive function. Ketema and Simonsen [11] extensively studied valley sizes of confluence and the Church-Rosser property in term rewriting and λ-calculus as a function of given term sizes and reduction lengths. However, there are no known bounds for the Church-Rosser theorem for β-equality up to our knowledge.

In this study, we are also interested in quantitative analysis of the witness of the Church-Rosser theorem: how to find common contractums with the least size and with the least number of reduction steps. For the theorem for β-equality ($M =_\beta N$ implies $M \twoheadrightarrow^{l_3} P$ and $N \twoheadrightarrow^{l_4} P$ for some P), we study functions that set bounds on the least size of a common contractum P, and the least number of reduction steps l_3 and l_4 required to arrive at a common contractum, involving the term sizes of M and N, and the length of $=_\beta$. For the theorem for β-reduction ($M \twoheadrightarrow^{l_1} N_1$ and $M \twoheadrightarrow^{l_2} N_2$ implies $N_1 \twoheadrightarrow^{l_3} P$ and $N_2 \twoheadrightarrow^{l_4} P$ for some P), we study functions that set bounds on the least size of a common contractum P, and the least number of reduction steps l_3 and l_4 required to arrive at a common contractum, involving the term size of M and the lengths of l_1 and l_2.

In this paper, first we investigate *directly* the Church-Rosser theorem for β-equality *constructively* from the viewpoint of Takahashi translation [22]. Although the two statements are equivalent to each other, the theorem for β-reduction is a special case of that for β-equality. Our investigation shows that a common contractum of M and N such that $M =_\beta N$ is determined by (i) M and the number of occurrences of reduction ($\rightarrow$) appeared in $=_\beta$, and also by (ii) N and that of reversed reduction ($\leftarrow$). The main lemma plays a key role and reveals a new invariant involved in the equality $=_\beta$, independently of an exponential combination of reduction and reversed reduction. In terms of iteration of Takahashi translation, this characterization of the Church-Rosser theorem makes it possible to analyse how large common contractums are and how many reduction-steps are required to obtain them. From this, we obtain an upper bound function for the theorem in the fourth level of the Grzegorczyk hierarchy.

Next, we demonstrate that the proof method is available as well under a general framework of the *compositional Z* [15]. The compositional Z-property is an extension of the so-called Z-property [5], which makes it possible to apply a divide-and-conquer method for proving confluence. For this extension, the measure functions constructed for quantitative analysis of the Church-Rosser theorem are abstracted as fundamental modules of bound functions. The paper makes a contribution to quantitative analysis of abstract rewriting systems under the framework of the compositional Z.

This paper is organized as follows. Section 1 is devoted to background, related work, and our contribution of this paper. Section 2 gives preliminaries including basic definitions and notions. Following [6], Section 3 provides the new proof of the Church-Rosser theorem for β-equality. Based on this, from the viewpoint of abstract rewriting systems, reduction length for the theorem is analyzed in Section 4. Section 5 recalls the compositional Z-property [15]. Section 6 demonstrates quantitative analysis of reduction systems under the framework of the compositional Z, and this part is a new result of the paper. Section 7 concludes with remarks, related work, and further work.

The paper is an extended abstract, and see [6] for the details of the new proof of the Church-Rosser theorem and quantitative analysis of the witness, and see also [15] for the details of the compositional

Z-property and its application.

2 Preliminaries

The set of λ-terms denoted by Λ is defined with a countable set of variables as follows.

Definition 2.1 (λ-terms).

$$M, N, P, Q \in \Lambda ::= x \mid (\lambda x.M) \mid (MN)$$

We write $M \equiv N$ for the syntactical identity under renaming of bound variables. We suppose that every bound variable is distinct from free variables. The set of free variables in M is denoted by $\mathrm{FV}(M)$.

If M is a subterm of N then we write $M \sqsubseteq N$ for this.

Definition 2.2 (β-reduction). One step β-reduction $\to$ is defined as follows, where $M[x := N]$ denotes a result of substituting N for every free occurrence of x in M.

1. $(\lambda x.M)N \to M[x := N]$
2. If $M \to N$ then $PM \to PN$, $MP \to MP$, and $\lambda x.M \to \lambda x.N$.

A term in the form of $(\lambda x.P)Q \sqsubseteq M$ is called a redex of M. A redex is denoted by R or S, and we write $R : M \to N$ if N is obtained from M by contracting the redex $R \sqsubseteq M$. We write $\twoheadrightarrow$ for the reflexive and transitive closure of $\to$. If $R_1 : M_0 \to M_1, \ldots, R_n : M_{n-1} \to M_n$ $(n \geq 0)$, then for this we write $R_0 \ldots R_n : M_0 \twoheadrightarrow^n M_n$, and the *reduction sequence* is denoted by the list $[M_0, M_1, \ldots, M_n]$. For operating on a list, we suppose fundamental list functions, `append`, `reverse`, `tail` (`cdr`), `map` and `max`.

Definition 2.3 (β-equality). A term M is β-equal to N with reduction sequence ls, denoted by $M =_\beta N$ with ls is defined as follows:

1. If $M \twoheadrightarrow N$ with reduction sequence ls, then $M =_\beta N$ with ls.
2. If $M =_\beta N$ with ls, then $N =_\beta M$ with `reverse`(ls).
3. If $M =_\beta P$ with ls_1 and $P =_\beta N$ with ls_2, then $M =_\beta N$ with `append`$(ls_1,$ `tail`$(ls_2))$.

Note that $M =_\beta N$ with reduction sequence ls iff there exist terms $M_0, \ldots, M_n (n \geq 0)$ in this order such that $ls = [M_0, \ldots, M_n]$, $M_0 \equiv M, M_n \equiv N$, and either $M_i \to M_{i+1}$ or $M_{i+1} \to M_i$ for each $0 \leq i \leq n-1$. In this case, we say that the *length* of $=_\beta$ is n, denoted by $=_\beta^n$. The arrow in $M_i \to M_{i+1}$ is called a *right arrow*, and the arrow in $M_{i+1} \to M_i$ is called a *left arrow*, denoted also by $M_i \leftarrow M_{i+1}$.

Definition 2.4 (Term size). Define a function $|\ | : \Lambda \to \mathbf{N}$ as follows.

1. $|x| = 1$
2. $|\lambda x.M| = 1 + |M|$
3. $|MN| = 1 + |M| + |N|$

Definition 2.5 (Takahashi's * and iteration). The notion of Takahashi translation M^* [22], that is, the Gross-Knuth reduction strategy [2] is defined as follows.

1. $x^* = x$
2. $((\lambda x.M)N)^* = M^*[x := N^*]$
3. $(MN)^* = M^*N^*$
4. $(\lambda x.M)^* = \lambda x.M^*$

The 3rd case above is available provided that M is not in the form of λ-abstraction. We write an iteration of the translation [23] as follows.

1. $M^{0*} = M$
2. $M^{n*} = (M^{(n-1)*})^*$

We write $\sharp(x \in M)$ for the free occurrence number of the variable x in M.

Lemma 2.6. $|M[x := N]| = |M| + \sharp(x \in M) \times (|N| - 1)$.

Proof. By straightforward induction on M. □

Definition 2.7 ($\mathsf{Redex}(M)$). A set of all redex occurrences in a term M is denoted by $\mathsf{Redex}(M)$. The cardinality of the set $\mathsf{Redex}(M)$ is denoted by $\sharp\mathsf{Redex}(M)$.

Lemma 2.8 ($\sharp\mathsf{Redex}(M)$). *We have* $\sharp\mathsf{Redex}(M) \leq \frac{1}{2}|M| - 1$ *for* $|M| \geq 4$.

Proof. Note that $\sharp\mathsf{Redex}(M) = 0$ for $|M| < 4$. By straightforward induction on M for $|M| \geq 4$. □

Lemma 2.9 (Substitution). *If $M_1 \twoheadrightarrow^{l_1} N_1$ and $M_2 \twoheadrightarrow^{l_2} N_2$, then $M_1[x := M_2] \twoheadrightarrow^{l} N_1[x := N_2]$ where $l = l_1 + \sharp(x \in M_1) \times l_2$.*

Proof. By induction on the derivation of $M_1 \twoheadrightarrow^{l_1} N_1$. The case of $l_1 = 0$ requires induction on $M_1 \equiv N_1$. □

Proposition 2.10 (Term size after n-step reduction). *If $M \twoheadrightarrow^{n} N$ $(n \geq 1)$ then*

$$|N| < 8\left(\frac{|M|}{8}\right)^{2^n}.$$

Proof. By induction on n. □

Lemma 2.11 (Size of M^*). *We have $|M^*| \leq 2^{|M|-1}$.*

Proof. By straightforward induction on M. □

3 New proof of the Church-Rosser theorem for β-equality

Proposition 3.1 (Complete development). *We have $M \twoheadrightarrow^{l} M^*$ where $l \leq \frac{1}{2}|M| - 1$ for $|M| \geq 4$.*

Proof. By induction on the structure of M. Otherwise by the minimal complete development [9] with respect to $\mathsf{Redex}(M)$, where $l \leq \sharp\mathsf{Redex}(M) \leq \frac{1}{2}|M| - 1$ from Lemma 2.8. □

Definition 3.2 (Iteration of exponentials $\mathbf{2}^m_n$, $\mathsf{F}(m,n)$). Let m and n be natural numbers.

1. (1) $\mathbf{2}^m_0 = m$; (2) $\mathbf{2}^m_{n+1} = 2^{\mathbf{2}^m_n}$.
2. (1) $\mathsf{F}(m,0) = m$; (2) $\mathsf{F}(m,n+1) = 2^{\mathsf{F}(m,n)-1}$.

Proposition 3.3 (Length to M^{n*}). *If $M \twoheadrightarrow M^* \twoheadrightarrow \cdots \twoheadrightarrow M^{n*}$, then the reduction length l with $M \twoheadrightarrow^{l} M^{n*}$ is bounded by $\mathsf{Len}(|M|,n)$, such that*

$$\mathsf{Len}(|M|,n) = \begin{cases} 0, & \text{for } n = 0 \\ \frac{1}{2}\sum_{k=0}^{n-1}\mathsf{F}(|M|,k) - n, & \text{for } n \geq 1 \end{cases}$$

and then we have $\mathsf{Len}(|M|,n) < \mathbf{2}^{|M|}_{n-1}$ for $n \geq 1$.

Proof. From Lemma 2.11, we have $|M^*| \leq 2^{|M|-1}$, and hence $|M^{k*}| \leq \mathsf{F}(|M|,k) < \mathbf{2}^{|M|}_k$ for $k \geq 1$. Let $M \twoheadrightarrow^{l_1} M^* \twoheadrightarrow^{l_2} \cdots \twoheadrightarrow^{l_n} M^{n*}$. Then from Proposition 3.1, each l_k is bounded by $\mathsf{F}(|M|,k-1)$:

$$l_k \leq \frac{1}{2}|M^{(k-1)*}| - 1 \leq \frac{1}{2}\mathsf{F}(|M|,k-1) - 1$$

Therefore, l is bounded by $\mathsf{Len}(|M|,n)$ that is smaller than $\mathbf{2}^{|M|}_{n-1}$ for $n \geq 1$.

$$\begin{aligned} l &\leq \sum_{k=1}^{n} l_k \\ &\leq \frac{1}{2}\sum_{k=0}^{n-1}\mathsf{F}(|M|,k) - n \\ &= \mathsf{Len}(|M|,n) \\ &< \frac{1}{2}\sum_{k=0}^{n-1}\mathbf{2}^{|M|}_k - n \\ &< \mathbf{2}^{|M|}_{n-1} - n \end{aligned}$$

□

Lemma 3.4 (Cofinal property). *If $M \to N$ then $N \twoheadrightarrow^{l} M^*$ where $l \leq \frac{1}{2}|N| - 1$ for $|N| \geq 4$.*

Proof. By induction on the derivation of $M \to N$. □

Lemma 3.5. *$M^*[x := N^*] \twoheadrightarrow^{l} (M[x := N])^*$ with $l \leq |M^*| - 1$.*

Proof. By induction on the structure of M. □

Proposition 3.6 (Monotonicity).

1. *If $M \to N$ then $M^* \twoheadrightarrow^{l} N^*$ with $l \leq |M^*| - 1$.*
2. *If $M \twoheadrightarrow^{m} N$, then $M^* \twoheadrightarrow^{l} N^*$ where $l \leq 2^{|M|^{2^{(m-1)}}} - m$.*

Proof. 1. By induction on the derivation of $M \to N$.

2. From Proposition 2.10, Proposition 3.6 (1) and Lemma 2.11. □

Lemma 3.7 (Main lemma [6]). *Let $M =^k_\beta N$ with length $k = l + r$, where r is the number of occurrences of right arrow $\to$ in $=^k_\beta$, and l is that of left arrow $\leftarrow$ in $=^k_\beta$. Then we have both $M^{r*} \twoheadleftarrow N$ and*

$M \twoheadrightarrow N^{l*}$.

Proof. By induction on the length of $=^k_\beta$.

(1) Case of $k = 1$ is handled by Lemma 3.4.

(2-1) Case of $(k+1)$, where $M =^k_\beta M_k \to M_{k+1}$: From the induction hypothesis, we have $M_k \twoheadrightarrow M^{r*}$ and $M \twoheadrightarrow M_k^{l*}$ where $l + r = k$.
From $M_k \to M_{k+1}$, Lemma 3.4 gives $M_{k+1} \twoheadrightarrow M_k^*$, and then $M_k^* \twoheadrightarrow M^{(r+1)*}$ from the induction hypothesis $M_k \twoheadrightarrow M^{r*}$ and Proposition 3.6. Hence, we have $M_{k+1} \twoheadrightarrow M^{(r+1)*}$. On the other hand, we have $M_k^{l*} \twoheadrightarrow M_{k+1}^{l*}$ from $M_k \to M_{k+1}$ and the repeated application of Proposition 3.6. Then the induction hypothesis $M \twoheadrightarrow M_k^{l*}$ derives $M \twoheadrightarrow M_{k+1}^{l*}$, where $l + (r+1) = k+1$.

(2-2) Case of $(k+1)$, where $M =^k_\beta M_k \leftarrow M_{k+1}$: From the induction hypothesis, we have $M_k \twoheadrightarrow M^{r*}$ and $M \twoheadrightarrow M_k^{l*}$ where $l + r = k$, and hence $M_{k+1} \twoheadrightarrow M^{r*}$. From $M_{k+1} \to M_k$ and Lemma 3.4, we have $M_k \twoheadrightarrow M_{k+1}^*$, and then $M_k^{l*} \twoheadrightarrow M_{k+1}^{(l+1)*}$. Hence, $M \twoheadrightarrow M_{k+1}^{(l+1)*}$ from the induction hypothesis $M \twoheadrightarrow M_k^{l*}$, where $(l+1) + r = k+1$.

□

Given $M_0 =^k_\beta M_k$ with reduction sequence $[M_0, \ldots, M_k]$, then for natural numbers i and j with $0 \le i \le j \le k$, we write $\sharp r[i,j]$ for the number of occurrences of right arrow $\to$ appeared in $M_i =^{(j-i)}_\beta M_j$, and $\sharp l[i,j]$ for that of left arrow $\leftarrow$ in $M_i =^{(j-i)}_\beta M_j$. In particular, we have $\sharp l[0,k] + \sharp r[0,k] = k$.

Corollary 3.8 (Main lemma refined [6]). *Let $M_0 =^k_\beta M_k$ with reduction sequence $[M_0, M_1, \ldots, M_k]$. Let $r = \sharp r[0,k]$ and $l = \sharp l[0,k]$. Then we have $M_0 \twoheadrightarrow M_r^{m_l*}$ and $M_r^{m_l*} \twoheadleftarrow M_k$, where $m_l = \sharp l[0,r] \le \min\{l,r\}$.*

Proof. From the main lemma, we have two reduction paths such that $M_0 \twoheadrightarrow M_k^{l*}$ and $M_0^{r*} \twoheadleftarrow M_k$, where the paths have a crossed point that is the term M_r^{n*} for some $n \le k$ as follows: Let m_l be $\sharp l[0,r]$, then $\sharp l[r,k] = (l - m_l)$ and $\sharp r[r,k] = m_l$. Hence, from the main lemma, we have $M_0 \twoheadrightarrow M_r^{m_l*} \twoheadleftarrow M_k$ where $m_l \le \min\{l,r\}$. Moreover, we have $M_r \twoheadrightarrow M_k^{(l-m_l)*}$ by the main lemma again, and then $M_r^{m_l*} \twoheadrightarrow M_k^{((l-m_l)+m_l)*}$ from the repeated application of Proposition 3.6. Therefore, we indeed have $M_0 \twoheadrightarrow M_r^{m_l*} \twoheadrightarrow M_k^{l*}$. Similarly, we have $M_0^{r*} \twoheadleftarrow M_r^{m_l*} \twoheadleftarrow M_k$ as well. □

Observe that a crossed point $M_r^{m_l*}$ in Corollary 3.8 gives a "good" common contractum such that the number m_l, i.e., iteration of the translation $*$ is minimum. Consider two reduction paths: (i) a reduction path from $M_r^{m_l*}$ to M_0^{r*}, and (ii) a reduction path from $M_r^{m_l*}$ to M_k^{l*}, see the picture in the proof of Corollary 3.8. In general, the reduction paths (i) and (ii) form the boundary line between common contractums and non-common ones. Let B be a term in the boundary (i) or (ii). Then any term M such that $B \twoheadrightarrow M$ is a common contractum of M_0 and M_k. In this sense, the term $M_r^{m_l*}$ where $0 \le m_l \le \min\{l,r\}$ can be considered as an optimum common reduct of M_0 and M_k in terms of Takahashi translation. Moreover, the refined lemma gives a divide and conquer method such that $M_0 =^k_\beta M_k$ is divided into $M_0 =^r_\beta M_r$ and $M_r =^l_\beta M_k$, where the base case is a valley such that $M_0 \twoheadrightarrow M_r \twoheadleftarrow M_k$ with $m_l = 0$.

The results of Lemma 3.7 and Corollary 3.8 can be unified as follows. The main theorem shows that every term in the reduction sequence ls of $M_0 =^k_\beta M_k$ generates a common contractum: For every term M in ls, there exists a natural number $n \le \max\{l,r\}$ such that M^{n*} is a common contractum of M_0 and M_k. Moreover, there exist a term N in ls and a natural number $m \le \min\{l,r\}$ such that N^{m*} is a common contractum of all the terms in ls.

Theorem 3.9 (Main theorem for β-equality [6])**.** *Let $M_0 =^k_\beta M_k$ with reduction sequence $[M_0, \dots, M_k]$. Let $l = \sharp l[0,k]$ and $r = \sharp r[0,k]$. Then there exist the following common reducts:*

1. *We have $M_0 \twoheadrightarrow M_{r-i}^{\sharp r[r-i,k]*}$ and $M_{r-i}^{\sharp r[r-i,k]*} \twoheadleftarrow M_k$ for each $i = 0, \dots, r$. We also have $M_0 \twoheadrightarrow M_{r+j}^{\sharp l[0,r+j]*}$ and $M_{r+j}^{\sharp l[0,r+j]*} \twoheadleftarrow M_k$ for each $j = 0, \dots, l$.*
2. *For every term M in the reduction sequence, we have $M \twoheadrightarrow M_r^{m_l *}$ where $m_l = \sharp l[0,r]$.*

Proof. Both 1 and 2 are proved similarly from Lemma 3.7, Corollary 3.8, and monotonicity. We show the case 2 here. Let M_i be a term in the reduction sequence of $M_0 =^k_\beta M_k$ where $0 \leq i \leq r$. Take $a = \sharp r[0,i]$, then $M_a^{\sharp l[0,a]}$ is a crossed point of $M_0 \twoheadrightarrow M_i^{\sharp l[0,i]*}$ and $M_i \twoheadrightarrow M_0^{\sharp r[0,i]*}$. From $M_i \twoheadrightarrow M_r^{\sharp l[i,r]*}$ and monotonicity, we have $M_i^{\sharp l[0,i]*} \twoheadrightarrow M_r^{m_l *}$ where $m_l = \sharp l[0,i] + \sharp l[i,r]$. Hence, we have $M_i \twoheadrightarrow M_a^{\sharp l[0,a]*} \twoheadrightarrow M_i^{\sharp l[0,i]*} \twoheadrightarrow M_r^{m_l *}$. The case of $r \leq i \leq k$ is also verified similarly. □

Note that the case of $i = r$ and $j = l$ implies the main lemma, since $\sharp r[0,k] = r$ and $\sharp l[0, r+l] = \sharp l[0,k] = l$. Note also that the case of $i = 0 = j$ implies the refinement, since $\sharp l[0,r] = m_l = \sharp r[r,k]$.

Corollary 3.10 (Confluence)**.** *Let $P_n \leftarrow \cdots \leftarrow P_1 \leftarrow M \rightarrow Q_1 \rightarrow \cdots \rightarrow Q_m$ $(1 \leq n \leq m)$. Then we have $P_n \twoheadrightarrow Q_m^{n*}$ and $Q_m \twoheadrightarrow Q_m^{n*}$. We also have $P_n \twoheadrightarrow Q_{(m-n)}^{n*}$ and $Q_m \twoheadrightarrow Q_{(m-n)}^{n*}$.*

Proof. From the main lemma and the refinement where $Q_0 \equiv M$. □

4 Quantitative analysis of Church-Rosser theorem

Following the results and proof methods in the previous section, the size of common reducts and the number of reduction steps leading to a common reduct are investigated in detail in [6]. The method is a *general* principle and indeed can be extended to handle any system with the Z-property [5].

Let $(A, \rightarrow)$ be an abstract rewriting system where the reduction $\rightarrow$ is a binary relation on the set A. An element of A is also called a term, and suppose that the size of a term M is well defined, denoted by a natural number $|M|$.

Following Definitions 2.2 and 2.3, we define the reflexive transitive closure of $\rightarrow$ with a reduction sequence ls, denoted by $\twoheadrightarrow^n$ with length n of ls. We also define the reflexive transitive symmetric closure of $\rightarrow$ with a sequence ls, denoted by $=^n_A$ with length n of ls. From the definition, $M =_A N$ with sequence ls if and only if there exists a finite sequence of terms $M_0, \dots, M_n \in A$ $(n \geq 0)$ such that $ls = [M_0, \dots, M_n]$, $M_0 \equiv M$, $M_n \equiv N$ and either $M_i \rightarrow M_{i+1}$ or $M_i \leftarrow M_{i+1}$ for $0 \leq i \leq n-1$. For natural numbers i and j with $0 \leq i \leq j \leq n$, we write $\sharp r[i,j]$ for the number of occurrences of right arrow $\rightarrow$ appeared in $M_i =_A^{(j-i)} M_j$, and $\sharp l[i,j]$ for the number of occurrences of left arrow $\leftarrow$ appeared in $M_i =_A^{(j-i)} M_j$.

For quantitative analysis, we prepare important measure functions, $\mathsf{TermSize}$, Mon and Rev.

Definition 4.1 (TermSize)**.** By induction on the derivation, we define $\mathsf{TermSize}(M =_A N)$ as follows:

1. If $M \twoheadrightarrow^n N$ with reduction sequence (list) ls, then $\mathsf{TermSize}(M \twoheadrightarrow^n N)$ is defined by $\mathtt{max}(\mathtt{map}\ (\mathtt{fn}\ x \Rightarrow |x|)\ ls)$.
2. If $M =_A N$ is derived from $N =_A M$, then $\mathsf{TermSize}(M =_A N)$ is defined by $\mathsf{TermSize}(N =_A M)$.
3. If $M =_A N$ is derived from $M =_A P$ and $P =_A N$, then define $\mathsf{TermSize}(M =_A N)$ as $\max\{\mathsf{TermSize}(M =_A P), \mathsf{TermSize}(P =_A N)\}$.

Proposition 4.2 (TermSize)**.** *Let $M_0 =^k_A M_k$ with sequence ls. For each term M in ls, we have $|M| \leq \mathsf{TermSize}(M_0 =^k_A M_k)$.*

Proof. By induction on the derivation of $=_A$. □

We suppose an abstract rewriting system $(A, \to)$ having the following function f from A to A together with measure functions (bound functions) Mon and Rev to the set of natural numbers, such that (i) if $M \twoheadrightarrow^n N$ $(n \geq 1)$ then $f(M) \twoheadrightarrow^l f(N)$ where $l \leq \mathtt{Mon}(|M|, n)$, and (ii) if $M \to N$ then $N \twoheadrightarrow^l f(M)$ where $l \leq \mathtt{Rev}(|M|)$, provided that the measure functions are monotonic. We write $f^{n+1}(M) = f(f^n(M))$ and $f^0(M) = M$.

Then it is straightforward to reformulate Lemma 3.7 and Corollary 3.8 in terms of abstraction rewriting systems.

Proposition 4.3 (Lemma 3.7 revised). *Let $M =_A^k N$ with length $k = l + r$, where $r = \sharp r[0, k]$, $l = \sharp l[0, k]$ and $\mathsf{B} = \mathsf{TermSize}(M =_A^k N)$. Then we have $f^r(M) \twoheadleftarrow^a N$ such that $a \leq \mathsf{Main}(M =_A^k N)$, where the function* Main *is defined by induction on k, as follows:*

1. $\mathsf{Main}(M \leftarrow N) = 1$
2. $\mathsf{Main}(M \to N) = \mathsf{Rev}(|M|)$
3. $\mathsf{Main}(M =_A^n P \leftarrow Q) = \mathsf{Main}(M =_A^n P) + 1$
4. $\mathsf{Main}(M =_A^n P \to Q) = \mathsf{Mon}(\mathsf{B}, p) + \mathsf{Rev}(\mathsf{B})$, *where* $p = \mathsf{Main}(M =_A^n P)$.

Proof. From the proof of Lemma 3.7. Particularly in the last case where $f^{\sharp r[0,n]+1}(M) \twoheadleftarrow^a f(P) \twoheadleftarrow^b Q$, we have $a + b \leq \mathsf{Mon}(|P|, p) + \mathsf{Rev}(|P|) \leq \mathsf{Mon}(\mathsf{B}, p) + \mathsf{Rev}(\mathsf{B})$. □

Proposition 4.4 (Corollary 3.8 revised). *Let $M =_A^k N$ with reduction sequence $[M_0, M_1, \ldots, M_k]$, where $r = \sharp r[0, k]$, $l = \sharp l[0, k]$ and $m_l = \sharp l[0, r]$. Then we have $M \twoheadrightarrow^a f^{m_l}(M_r)$ and $f^{m_l}(M_r) \twoheadleftarrow^b N$, where $a \leq \mathsf{Main}(M_r =_A^r M)$ and $b \leq \mathsf{Main}(M_r =_A^l N)$.*

Proof. From Corollary 3.8 and Proposition 4.3. □

We remark that from Lemma 3.4 and Proposition 3.6, the measure function Main is a function in the fourth level of the Grzegorczyk hierarchy in the case of λ-calculus [6].

5 Compositional Z-property

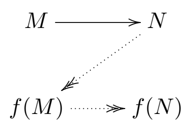
We begin with Dehornoy and van Oostrom's Z theorem, and then extend it for compositional functions, called the *compositional Z*. It gives a sufficient condition for that a compositional function satisfies the Z-property, by dividing a rewriting system into two parts.

Definition 5.1 ((Weak) Z-property [15]). Let $(A, \to)$ be an abstract rewriting system, and $\twoheadrightarrow$ be the reflexive transitive closure of $\to$. Let $\to_\times$ be another relation on A, and $\twoheadrightarrow_\times$ be its reflexive transitive closure.

1. A mapping f satisfies the *weak Z-property for* $\to$ *by* $\to_\times$ if $M \to N$ implies $N \twoheadrightarrow_\times f(M) \twoheadrightarrow_\times f(N)$ for any $M, N \in A$.
2. A mapping f satisfies the *Z-property for* $\to$ if it satisfies the weak Z-property by $\to$ itself.

When f satisfies the (weak) Z-property, we also say that f *is (weakly) Z*.

It becomes clear why we call it the Z-property when we draw the condition as the following diagram.



Theorem 5.2 (Z theorem [5]). *If there exists a mapping satisfying the Z-property for an abstract rewriting system, then it is confluent.*

This theorem has been applied to confluence proofs for some variants of λ-calculus in [5] [13] [1] [16]. In fact, we can often prove that the usual complete developments have the Z-property.

The compositional Z is the following, which is easily proved from Theorem 5.2 with the diagrams in Figure 1.

Theorem 5.3 (Compositional Z [15]). *Let $(A, \to)$ be an abstract rewriting system, and $\to$ be $\to_1 \cup \to_2$. If there exist mappings $f_1, f_2 : A \to A$ such*

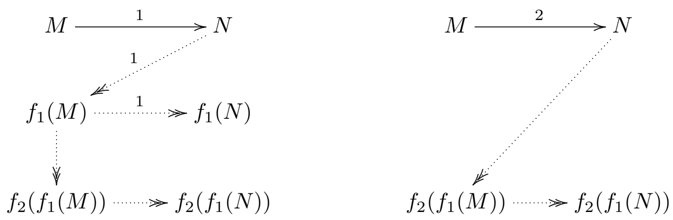


Figure 1 Proof of Theorem 5.3

that

(a) f_1 *is Z for* $\to_1$

(b) $M \to_1 N$ *implies* $f_2(M) \twoheadrightarrow f_2(N)$

(c) $M \twoheadrightarrow f_2(M)$ *holds for any* $M \in \mathrm{Im}(f_1)$

(d) $f_2 \circ f_1$ *is weakly Z for* $\to_2$ *by* $\to$ *,*

then $f_2 \circ f_1$ *is Z for* $(A, \to)$*, and hence* $(A, \to)$ *is confluent.*

One example of the compositional Z is a confluence proof for the $\beta\eta$-reduction on the untyped λ-calculus (although it can be directly proved by the Z theorem as in [13]). Let $\to_1 \,=\, \to_\eta$, $\to_2 \,=\, \to_\beta$, and f_1 and f_2 be the usual complete developments of η and β, respectively. Then, it is easy to see the conditions of the compositional Z hold. The point is that we can forget the other reduction in the definition of each complete development.

Furthermore, we have another sufficient condition for the Z-property of compositional functions as follows. It is a special case of the compositional Z where $f_1(M) = f_1(M)$ holds for any $M \to_1 N$. All of the examples (except for $\beta\eta$ above) of the application of compositional Z in [15] are in this case.

Corollary 5.4 ([15])**.** *Let* $(A, \to)$ *be an abstract rewriting system, and* $\to$ *be* $\to_1 \cup \to_2$ *. Suppose that there exist mappings* $f_1, f_2 : A \to A$ *such that*

(a) $M \to_1 N$ *implies* $f_1(M) = f_1(N)$

(b) $M \twoheadrightarrow_1 f_1(M)$ *for any* M

(c) $M \twoheadrightarrow f_2(M)$ *holds for any* $M \in \mathrm{Im}(f_1)$

(d) $f_2 \circ f_1$ *is weakly Z for* $\to_2$ *by* $\to$ *.*

Then, $f_2 \circ f_1$ *is Z for* $(A, \to)$*, and hence* $(A, \to)$ *is confluent.*

Proof. It is easily proved from Theorem 5.3. The condition (a) in Theorem 5.3 comes from the new conditions (a) and (b), and (b) in Theorem 5.3 is not necessary since we have $f_2(f_1(M)) = f_2(f_1(N))$ for any $M \to_1 N$. □

Corollary 5.4 can be seen as generalization of the *Z-property modulo*, proposed by Accattoli and Kesner [1]. For an abstract rewriting system $(A, \to)$ and an equivalence relation $\sim$ on A, the reduction modulo $\sim$, denoted $M \to_\sim N$, is defined as $M \sim P \to Q \sim N$ for some P and Q. The Z-property modulo says that it is a sufficient condition for the confluence of $\to_\sim$ that there exists a mapping which is well-defined on $\sim$ and weakly Z for $\to$ by $\to_\sim$. If we consider $\sim$ as the first reduction relation $\to_1$, and define $f_1(M)$ as a fixed representative of the equivalence class including M, then the conditions of the Z-property modulo implies the conditions of the compositional Z, since the reflexive transitive closure of $\to \cup \sim$ is $\twoheadrightarrow_\sim$.

6 Quantitative analysis under compositional Z-property

The two approaches in Sections 4 and 5 are naturally unified into a single framework. For this, we introduce the compositional Z-property together with measure functions Mon, Rev and Eval as modules of bound functions.

Proposition 6.1. *Let* $(A, \to)$ *be an abstract rewriting system, and* $\to$ *be* $\to_1 \cup \to_2$ *. Suppose that there exist functions* $f_1, f_2 : A \to A$ *and mono-*

tonic measure functions Rev_1*,* Rev_2*,* Eval_2 *and* Mon *such that all of the following conditions hold.*

1. f_1 *is Z for* $\to_1$ *:*
   If $M \to_1 N$ *then* $N \twoheadrightarrow_1^a f_1(M) \twoheadrightarrow_1 f_1(N)$*,*
   where $a \le \mathsf{Rev}_1(|M|)$*.*
2. *If* $M \to_1 N$ *then* $f_2(M) \twoheadrightarrow f_2(N)$*.*
3. $M \twoheadrightarrow^a f_2(M)$ *holds for any* $M \in \mathrm{Im}(f_1)$*,* *where* $a \le \mathsf{Eval}_2(|M|)$*.*
4. $f_2 \circ f_1$ *is weakly Z for* $\to_2$ *by* $\to$ *:*
   If $M \to_2 N$ *then* $N \twoheadrightarrow^a f_2(f_1(M)) \twoheadrightarrow f_2(f_1(N))$*,*
   where $a \le \mathsf{Rev}_2(|M|)$*.*
5. *If* $M \twoheadrightarrow^a N$ *then* $f_2(f_1(M)) \twoheadrightarrow^b f_2(f_1(N))$*,* *where* $b \le \mathsf{Mon}(|M|, a)$*.*

Let $f = f_2 \circ f_1$*. If* $M =_A^k N$ *with length* $k = l + r$ *where* $r = \sharp r[0,k]$*,* $l = \sharp l[0,k]$ *and* $\mathsf{B} = \mathsf{TermSize}(M =_A^k N)$*, then we have* $f^r(M) \twoheadleftarrow^a N$ *such that* $a \le \mathsf{Main}_Z(M =_A^k N)$*, where* Main_Z *is defined by induction on* k*, as follows:*

1. $\mathsf{Main}_Z(M \leftarrow N) = 1$
2. $\mathsf{Main}_Z(M \to_1 N) = \mathsf{Rev}_1(|M|) + \mathsf{Eval}_2(|f_1(M)|)$
3. $\mathsf{Main}_Z(M \to_2 N) = \mathsf{Rev}_2(|M|)$
4. $\mathsf{Main}_Z(M =_A^n P \leftarrow Q) =$
   $\mathsf{Main}_Z(M =_A^n P) + 1$
5. $\mathsf{Main}_Z(M =_A^n P \to_1 Q) =$
   $\mathsf{Mon}(\mathsf{B}, p) + \mathsf{Eval}_2(\mathsf{B}) + \mathsf{Rev}_1(\mathsf{B})$*,*
   where $p = \mathsf{Main}_Z(M =_A^n P)$
6. $\mathsf{Main}_Z(M =_A^n P \to_2 Q) = \mathsf{Mon}(\mathsf{B}, p) + \mathsf{Rev}_2(\mathsf{B})$*, where* $p = \mathsf{Main}_Z(M =_A^n P)$*.*

Proof. From the proof of Lemma 3.7 and the fact that $f = f_2 \circ f_1$ is Z for $(A, \to)$. □

Now we have the Church-Rosser theorem under the assumption of Proposition 6.1.

Theorem 6.2 (Church-Rosser theorem)**.** *Let* $M =_A^k N$ *with reduction sequence* $[M_0, M_1, \ldots, M_k]$ *where* $r = \sharp r[0,k]$*,* $l = \sharp l[0,k]$ *and* $m_l = \sharp l[0,r]$*. Then we have* $M \twoheadrightarrow^a f^{m_l}(M_r)$ *and* $f^{m_l}(M_r) \twoheadleftarrow^b N$*, where* $a \le \mathsf{Main}_Z(M_r =_A^r M)$ *and* $b \le \mathsf{Main}_Z(M_r =_A^l N)$ *and* $f = f_2 \circ f_1$*.*

Proof. From Proposition 6.1. □

7 Concluding remarks

In this paper, first we investigated *directly* the Church-Rosser theorem for β-equality *constructively* from the viewpoint of Takahashi translation [22]. Our investigation shows that a common contractum of M and N such that $M =_\beta N$ is determined by (i) M and the number of occurrences of reduction ($\to$) appeared in $=_\beta$, and also by (ii) N and that of reversed reduction ($\leftarrow$). In terms of iteration of Takahashi translation, this characterization of the Church-Rosser theorem makes it possible to analyse how large common contractums are and how many reduction-steps are required to obtain them. From this, we obtained an upper bound function for the theorem in the fourth level of the Grzegorczyk hierarchy.

Next, we demonstrated that the proof method is available as well under a general framework of the compositional Z [15]. For this extension, the measure functions constructed for quantitative analysis of the Church-Rosser theorem are naturally abstracted as fundamental modules of bound functions. This approach makes it possible to analyze quantitative properties of abstract rewriting systems under the framework of the compositional Z.

Corollary 5.4 can be seen as generalization of the *Z-property modulo*, proposed by [1]. Moreover, it would be interesting to extend the compositional Z-property to cooperate with *confluent modulo equivalence* such as in [10] for applications to practical problems.

References

[1] B. Accattoli and D. Kesner: *The Permutative λ-calculus*, International Conference on Logic Programming and Automated Reasoning (LPAR 2012), Proceedings, no. 7180 in LNCS, pp. 15–22, 2012.

[2] H. P. Barendregt: *The lambda Calculus. Its Syn-*

tax and Semantics, North-Holland, revised edition, 1984.

[3] A. Church and J. B. Rosser: *Some properties of conversion*, Transactions of the American Mathematical Society 39 (3), pp. 472–482, 1936.

[4] H. B. Curry, R. Feys, and W. Craig: *Combinatory Logic*, Volume1, North-Holland, Third Printing, 1974.

[5] P. Dehornoy and V. van Oostrom: *Z, proving confluence by monotonic single-step upper bound functions*, Logical Models of Reasoning and Computation, 2008.

[6] K. Fujita: *On upper bounds on the Church-Rosser theorem*, Electronic Proceedings in Theoretical Computer Science, 3rd Workshop on Rewriting Techniques for Program Transformation and Evaluation, June 23, 2016.

[7] A. Grzegorczyk: *Some classes of recursive functions*, ROZPRAWY MATEMATYCZNE IV, pp. 1–48, 1953.

[8] J. R. Hindley: *Reductions of residuals are finite*, Transactions of the American Mathematical Society 240, pp. 345–361, 1978.

[9] J. R. Hindley and J. P. Seldin: *Lambda-calculus and Combinators, An Introduction*, Cambridge University Press, Cambridge, 2008.

[10] G. Huet: *Confluence Reductions: Abstract Properties and Applications to Term Rewriting Systems*, Journal of the Association for Computing Machinery 27-4, pp. 797–821, 1980.

[11] J. Ketema and J. G. Simonsen: *Least Upper Bounds on the Size of Confluence and Church-Rosser Diagrams in Term Rewriting and λ-Calculus*, ACM Transactions on Computational Logic 14 (4), 31:1–28, 2013.

[12] Z. Khasidashvili: *β-reductions and β-developments with the least number of steps*, Lecture Notes in Computer Science 417, pp. 105–111, 1988.

[13] Y. Komori, N. Matsuda, and F. Yamakawa: *A Simplified Proof of the Church-Rosser Theorem*, Studia Logica 102, pp. 175–183, 2014.

[14] R. Loader: *Notes on Simply Typed Lambda Calculus*, Tech. Rep. ECS-LFCS-98-381, Edinburgh, 1998.

[15] K. Nakazawa and K. Fujita: *Compositional Z: Confluence proofs for permutative conversion*, Studia Logica *published online*: May 2016.

[16] K. Nakazawa and T. Nagai: *Reduction System for Extensional Lambda-mu Calculus*, 25th International Conference on Rewriting Techniques and Applications joint with the 12th International Conference on Typed Lambda Calculi and Applications (RTA-TLCA 2014), Proceedings, no. 8560 in LNCS, pp. 349–363, 2014.

[17] H. Schwichtenberg: *Complexity of normalization in the pure lambda-calculus*, In A. S. Troelstra and D. van Dalen editors, *THE L.E.J.BROUWER CENTENARY SYMPOSIUM*, pp. 453–457, 1982.

[18] M. H. Sørensen: *A note on shortest developments*, Log. Meth. in Comput. Science 3 (4:2), pp. 1–8, 2007.

[19] R. Statman: *The typed λ-calculus is not elementary recursive*, Theoret. Comput. Sci. 9, pp. 73–81, 1979.

[20] V. van Oostrom: *Reduce to the max*, UU-CWI, July 1999.

[21] R. de Vrijer: *A direct proof of the finite developments theorem*, J. Symb. Log. 50-2, pp. 339–343, 1985.

[22] M. Takahashi: *Parallel reductions in λ-calculus*, J. Symb. Comput. 7, pp. 113–123, 1989.

[23] M. Takahashi: *Theory of Computation: Computability and Lambda Calculus*, Kindai Kagaku Sya, 1991.

[24] H. Tonino and K. Fujita: *On the adequacy of representing higher order intuitionistic logic as a pure type system*, Ann. Pure Appl. Logic 57, pp. 251–276, 1992.