数理解析研究所講究録 1268 巻 2002 年 105-109

The word problem for the braid inverse monoid

Isamu Inata, Naoki Kataumi and Takatoshi Tobita
(稲田 勇、片海 直樹、飛田 享俊)

Department of Information Science, Toho University, Funabashi 274-8510, Japan
(東邦大学理学部情報科学学科)

1 Monoid presentations

Let A be an alphabet and A^* the free monoid generated by A. The empty word is denoted by 1. A (*monoid*) *presentation* is an ordered pair (A, R) where $R \subseteq A^* \times A^*$. A monoid M is *defined* by (A, R) if $M \cong A^*/=_R$ where $=_R$ is the congruence on A^* generated by R. In this situation, we say that M is *generated* by A, A is a *generating* set of M, and R is a set of *defining relations* of M. If a monoid M is generated by an alphabet A, then there is a natural surjection $f : A^* \to M$. For any $w \in A^*$, the image of w under f is denoted by $[w]$.

If a monoid M has a presentation (A, R) such that both A and R are finite, then we say that M is *finitely presented.*

Let M be a monoid with a finite presentation (A, R). The *word problem* for M is to decide, given $u, v \in A^*$, whether $u =_R v$.

2 Automatic monoids

In this section, we give definitions and results for automatic monoids and groups. For more information, we refer to [2, 3].

Let M be a monoid with a finite generating set A and let $\pi : A^* \to M$ be the natural surjection. If there is a regular subset L of A^* such that the restriction $\pi|_L : L \to M$ is surjective, then the ordered pair (A, L) is called a *rational structure* for M.

Let M be a monoid with a rational structure (A, L) and \$ a new symbol such that $\$ \notin A$. Set $A(2,\$) = (A \cup \{\$\}) \times (A \cup \{\$\}) - (\$,\$)$. Define a mapping $\nu : A^* \times A^* \to A(2,\$)$ by $\nu(1,1) = 1$ and for $u = a_1a_2 \cdots a_m$ and $v = b_1b_2 \cdots b_n$,

$$\nu(u,v) = \begin{cases} (a_1,b_1)(a_2,b_2)\cdots(a_m,b_m)(\$,b_{m+1})\cdots(\$,b_n) & \text{if } m < n \\ (a_1,b_1)(a_2,b_2)\cdots(a_m,b_m) & \text{if } m = n \\ (a_1,b_1)(a_2,b_2)\cdots(a_n,b_n)(a_{n+1},\$)\cdots(a_m,\$). & \text{if } m > n \end{cases}$$

Set $L_= = \{\nu(u,v) \mid u, v \in L \text{ such that } [u] = [v] \text{ in } M\}$ and, for $a \in A$, $L_a = \{\nu(u,v) \mid u, v \in L \text{ such that } [ua] = [v] \text{ in } M\}$.

A monoid M is called *automatic* if there is a rational structure (A, L) such that $L_=$ and L_a for all $a \in A$ are regular subsets of $A(2,\$)$. In this situation, the rational structure (A, L) is called an *automatic structure* for M.

Result 2.1 (see [2, 3]) *Let M be an automatic monoid. Then the word problem for M is solvable in quadratic time. Moreover if M is a group, then M is finitely presented.*

Let M be a monoid with a rational structure (A, L). For any $w \in A^*$ and non-negative integer t, define a word $w(t) \in A^*$ by

$$w(t) = \begin{cases} \text{the prefix of } w \text{ of length } t & \text{if } t \le |w|, \\ w & \text{otherwise.} \end{cases}$$

For any $u, v \in A^*$, let $d(u, v) = \min\{|w| \mid w \in A^* \text{ such that } [uw] = [v] \text{ in } M\}$. We say that (A, L) satisfies the *fellow traveler property* if there is a constant k such that $d(u(t), v(t)) < k$ for all $t \ge 0$ whenever $u, v \in L$ and $[ua] = [v]$ in M for some $a \in A \cup \{1\}$.

Result 2.2 (see [3]) *For a group G with a rational structure (A, L), (A, L) is an automatic structure for G if and only if (A, L) satisfies the fellow traveler property.*

Let M be a monoid with a rational structure (A, L). (A, L) satisfies the *strong* fellow traveler property if there is a constant k such that, for any $u = a_1 a_2 \cdots a_m$, $v = b_1 b_2 \cdots b_n \in L$ satisfying $[ua] = [v]$ for some $a \in A \cup \{1\}$, there are $w_1, w_2, \ldots, w_\ell \in A^*$ such that $|w_i| < k$ for all i, and $[a_1 w_1] = [b_1]$, $[a_2 w_2] = [w_1 b_2], \ldots, [a_\ell w_\ell] = [w_{\ell-1} b_\ell]$ where $\ell = \max\{m, n\}$.

Theorem 2.3 *For a monoid M with a rational structure (A, L), if (A, L) satisfies the strong fellow traveler property, then M is automatic and finitely presented.*

3 Finite complete presentations

In this section, we one result about monoids with finite complete presentations. For more information on such monoids, we refer to [1].

Let (A, R) be a presentation of a monoid M. We write $u \to v$ if $(u, v) \in R$. The relation $\to_R$ on A^* is defined as follows: for $x, y \in A^*$, $x \to_R y$ if $x = x_1 u x_2$ and $y = x_1 v x_2$ for some $x_1, x_2 \in A^*$ and $u \to v \in R$. The reflexive transitive closure of $\to_R$ is denote by $\to_R^*$. R is *noetherian* if there is no infinite sequence $x_1 \to_R x_2 \to_R \cdots \to_R x_n \to_R \cdots$. R is *confluent* if, for any $x, y, z \in A^*$ such that $z \to_R^* x$ and $z \to_R^* y$, there is $w \in A^*$ such that $x \to_R^* w$ and $y \to_R^* w$. Moreover R is *complete* if R is both noetherian and confluent. We set $\mathrm{Left}(R) = \{u \in A^* \mid u \to v \in R \text{ for some } v \in A^*\}$ and $\mathrm{Irr}(R) = A^* - A^* \cdot \mathrm{Left}(R) \cdot A^*$.

Result 3.1 (see [1]) *Let M be a monoid with a finite complete presentation (A, R). Then, the word problem for M is solvable and $(A, \mathrm{Irr}(R))$ is a rational structure for M.*

4 Braid groups and its word problem

In this section, we consider braid groups. For more information on braid groups and its word problem, we refer to [3, 4, 5].

A *braid* on n strings is defined as a system of n strings in $\mathbf{R}^2 \times [0, 1] \subset \mathbf{R}^3$. It consists of disjoint intertwining n strings which join n fixed points in the upper plane $\mathbf{R}^2 \times \{0\}$ and n fixed points in the lower plane $\mathbf{R}^2 \times \{1\}$, and intersecting each intermediate plane $\mathbf{R}^2 \times \{t\}$ in exactly n points. A string attached to the upper plane at the i-th position is called the *i-th string*.

By B_n, we denote the set of isotopy classes of braids on n strings. We identify a braid with its isotopy class, and we call an element in B_n simply a braid. B_n has a group structure as follows. The product of two braids β_1 and β_2, denoted by juxtaposition $\beta_1 \beta_2$, is defined as follows. First attach β_2 under β_1 identifying the upper plane of β_2 and the lower plane of β_1, and then remove the center plane. The *trivial braid* is the braid in which all strings go straight from the upper plane to the lower plane. And the *inverse* of a braid is defined as the mirror image of it with respect to the vertical direction.

Result 4.1 (see [3, 5]) *B_n has a finite complete presentation and is automatic. Hence, the word problem for B_n is solvable.*

5 Braid inverse monoids

A *partial braid* on n strings is defined as a subsystem of a braid on n strings, that is, it consists of disjoint intertwining m strings ($0 \leq m \leq n$) which join m points of the n fixed points in the upper plane $\mathbb{R}^2 \times \{0\}$ and m points of the n fixed points in the lower plane $\mathbb{R}^2 \times \{1\}$, and intersecting each intermediate plane $\mathbb{R}^2 \times \{t\}$ in exactly m points. Accordingly, a partial braid on n strings can be obtained from a braid on n strings by removing some (possibly all or no) strings. For example, in Fig.1, the right-hand side is a partial braid that is obtained from the braid at the left-hand side by removing the fourth string. By BI_n, we denote the set of isotopy classes of partial braids.

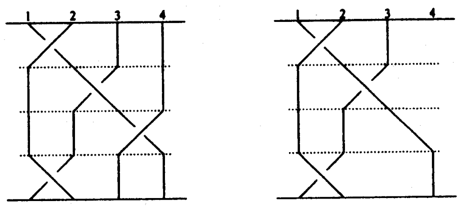

Fig.1 (a braid and a partial braid on 4 strings)

We define the product of two partial braids β_1 and β_2, denoted by juxtaposition $\beta_1\beta_2$, as follows. First attach β_2 under β_1 identifying the upper plane of β_2 and the lower plane of β_1. Then remove every string in β_1 (resp. β_2) that has no corresponding string in β_2 (resp. β_1). Lastly remove the center plane. For example, in Fig.2, we remove the second string in β_1, because it has no corresponding string in β_2. We also remove the fourth string in β_2 for the same reason.

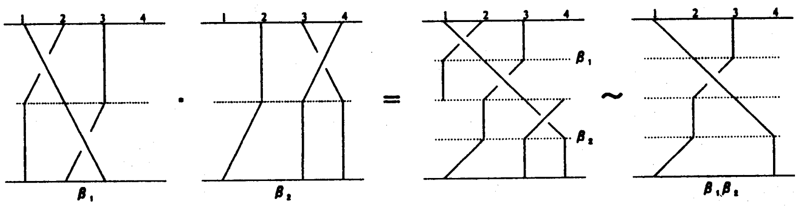

Fig.2 (the product of two partial braids β_1 and β_2 on 4 strings)

Then BI_n is a monoid with this operation and contains B_n as a subgroup.

Result 5.1 (see [6]) *BI_n is finitely presented.*

6 The word problem for BI_3

In this section, we give a finite complete presentation and an automatic structure for BI_3 using a finite complete presentation and an automatic structure for B_3.

Let x, y, $[xy]$, $[yx]$, δ and δ^{-1} be braids as in Fig.3. Let

$$\begin{aligned} A' &= \{x, y, [xy], [yx], \delta, \delta^{-1}\} \text{ and} \\ R' &= \{xy \to [xy],\ x[yx] \to \delta,\ yx \to [yx],\ y[xy] \to \delta,\ [xy]x \to \delta,\ [xy][xy] \to x\delta,\ [yx]y \to \delta, \\ &\quad [yx][yx] \to y\delta,\ \delta x \to y\delta,\ \delta y \to x\delta,\ \delta[xy] \to [yx]\delta,\ \delta[yx] \to [xy]\delta,\ \delta^{-1}x \to y\delta^{-1}, \\ &\quad \delta^{-1}y \to x\delta^{-1},\ \delta^{-1}[xy] \to [yx]\delta^{-1},\ \delta^{-1}[yx] \to [xy]\delta^{-1},\ \delta\delta^{-1} \to 1,\ \delta^{-1}\delta \to 1\}. \end{aligned}$$

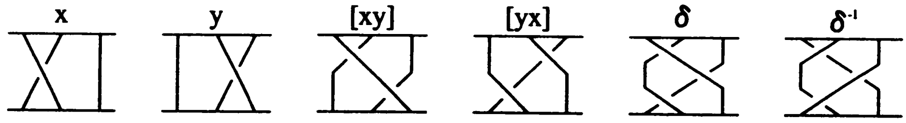

Fig.3

Result 6.1 (see [3, 5]) *(A', R') is a finite complete presentation of B_3 and $(A', \mathrm{Irr}(R'))$ is an automatic structure for B_3.*

Let a, b, c, d, a^{-1}, b^{-1}, c^{-1}, d^{-1} and 0 be partial braids as in Fig.4. Let

$$A = A' \cup \{a,\ b,\ c,\ d,\ a^{-1},\ b^{-1},\ c^{-1},\ d^{-1},\ z,\ z^{-1},\ 0\}$$

and

$R = R' \cup \{xz \to z^2$, $xz^{-1} \to zz^{-1}$, $xa \to a^{-1}a$, $xb \to b$, $xc \to d$, $xd \to c$, $xa^{-1} \to aa^{-1}$, $xb^{-1} \to ab^{-1}$, $xc^{-1} \to zc^{-1}$, $xd^{-1} \to zd^{-1}$, $yz \to cz$, $yz^{-1} \to cz^{-1}$, $ya \to b$, $yb \to a$, $yc \to zz^{-1}$, $yd \to dz$, $ya^{-1} \to a^{-1}$, $yb^{-1} \to b^{-1}$, $yc^{-1} \to cc^{-1}$, $yd^{-1} \to cd^{-1}$, $[xy]z \to dz$, $[xy]z^{-1} \to dz^{-1}$, $[xy]a \to b$, $[xy]b \to a^{-1}a$, $[xy]c \to z$, $[xy]d \to cz$, $[xy]a^{-1} \to aa^{-1}$, $[xy]b^{-1} \to ab^{-1}$, $[xy]c^{-1} \to dc^{-1}$, $[xy]d^{-1} \to dd^{-1}$, $[yx]z \to cz^2$, $[yx]z^{-1} \to c$, $[yx]a \to a^{-1}a$, $[yx]b \to a$, $[yx]c \to dz$, $[yx]d \to zz^{-1}$, $[yx]a^{-1} \to ba^{-1}$, $[yx]b^{-1} \to bb^{-1}$, $[yx]c^{-1} \to czc^{-1}$, $[yx]d^{-1} \to czd^{-1}$, $\delta z \to dz^2$, $\delta z^{-1} \to d$, $\delta a \to a$, $\delta b \to a^{-1}a$, $\delta c \to cz$, $\delta d \to z$, $\delta a^{-1} \to ba^{-1}$, $\delta b^{-1} \to bb^{-1}$, $\delta c^{-1} \to dzc^{-1}$, $\delta d^{-1} \to dzd^{-1}$, $\delta^{-1}z \to d$, $\delta^{-1}z^{-1} \to dz^{-2}$, $\delta^{-1}a \to a$, $\delta^{-1}b \to a^{-1}a$, $\delta^{-1}c \to cz^{-1}$, $\delta^{-1}d \to z^{-1}$, $\delta^{-1}a^{-1} \to ba^{-1}$, $\delta^{-1}b^{-1} \to bb^{-1}$, $\delta^{-1}c^{-1} \to dz^{-1}c^{-1}$, $\delta^{-1}d^{-1} \to dz^{-1}d^{-1}$, $zx \to z^2$, $zy \to zc^{-1}$, $z[xy] \to z^2c^{-1}$, $z[yx] \to zd^{-1}$, $z\delta \to z^2d^{-1}$, $z\delta^{-1} \to d^{-1}$, $za \to a^{-1}a$, $zb \to 0$, $zc \to a$, $zd \to a^{-1}a$, $za^{-1} \to aa^{-1}$, $zb^{-1} \to ab^{-1}$, $z^{-1}x \to zz^{-1}$, $z^{-1}y \to z^{-1}c^{-1}$, $z^{-1}[xy] \to c^{-1}$, $z^{-1}[yx] \to z^{-1}d^{-1}$, $z^{-1}\delta \to d^{-1}$, $z^{-1}\delta^{-1} \to z^{-2}d^{-1}$, $z^{-1}z \to zz^{-1}$, $z^{-1}a \to a^{-1}a$, $z^{-1}b \to 0$, $z^{-1}c \to a$, $z^{-1}d \to a^{-1}a$, $z^{-1}a^{-1} \to aa^{-1}$, $z^{-1}b^{-1} \to ab^{-1}$, $ax \to aa^{-1}$, $ay \to a$, $a[xy] \to ab^{-1}$, $a[yx] \to aa^{-1}$, $a\delta \to ab^{-1}$, $a\delta^{-1} \to ab^{-1}$, $az \to aa^{-1}$, $az^{-1} \to aa^{-1}$, $a^2 \to 0$, $ab \to 0$, $ac \to a$, $ad \to 0$, $ac^{-1} \to a$, $ad^{-1} \to aa^{-1}$, $bx \to ba^{-1}$, $by \to b$, $b[xy] \to bb^{-1}$, $b[yx] \to ba^{-1}$, $b\delta \to bb^{-1}$, $b\delta^{-1} \to bb^{-1}$, $bz \to ba^{-1}$, $bz^{-1} \to ba^{-1}$, $ba \to 0$, $b^2 \to 0$, $bc \to b$, $bd \to 0$, $bc^{-1} \to b$, $bd^{-1} \to ba^{-1}$, $cx \to cz$, $cy \to cc^{-1}$, $c[xy] \to czc^{-1}$, $c[yx] \to cd^{-1}$, $c\delta \to czd^{-1}$, $c\delta^{-1} \to cz^{-1}d^{-1}$, $ca \to b$, $cb \to 0$, $c^2 \to a^{-1}a$, $cd \to b$, $ca^{-1} \to a^{-1}$, $cb^{-1} \to b^{-1}$, $dx \to dz$, $dy \to dc^{-1}$, $d[xy] \to dzc^{-1}$, $d[yx] \to dd^{-1}$, $d\delta \to dzd^{-1}$, $d\delta^{-1} \to dz^{-1}d^{-1}$, $da \to b$, $db \to 0$, $dc \to a$, $d^2 \to b$, $da^{-1} \to aa^{-1}$, $db^{-1} \to ab^{-1}$, $a^{-1}x \to a^{-1}a$, $a^{-1}y \to b^{-1}$, $a^{-1}[xy] \to a^{-1}a$, $a^{-1}[yx] \to b^{-1}$, $a^{-1}\delta \to a^{-1}$, $a^{-1}\delta^{-1} \to a^{-1}$, $a^{-1}z \to a^{-1}a$, $a^{-1}z^{-1} \to a^{-1}a$, $a^{-1}b \to 0$, $a^{-1}c \to 0$, $a^{-1}d \to a^{-1}a$, $a^{-2} \to 0$, $a^{-1}b^{-1} \to 0$, $a^{-1}c^{-1} \to b^{-1}$, $a^{-1}d^{-1} \to b^{-1}$, $b^{-1}x \to b^{-1}$, $b^{-1}y \to a^{-1}$, $b^{-1}[xy] \to a^{-1}$, $b^{-1}[yx] \to a^{-1}a$, $b^{-1}\delta \to a^{-1}a$, $b^{-1}\delta^{-1} \to a^{-1}a$, $b^{-1}z \to 0$, $b^{-1}z^{-1} \to 0$, $b^{-1}a \to 0$, $b^{-1}b \to a^{-1}a$, $b^{-1}c \to a^{-1}$, $b^{-1}d \to a^{-1}$, $b^{-1}a^{-1} \to 0$, $b^{-2} \to 0$, $b^{-1}c^{-1} \to 0$, $b^{-1}d^{-1} \to 0$, $c^{-1}x \to d^{-1}$, $c^{-1}y \to zz^{-1}$, $c^{-1}[xy] \to zd^{-1}$, $c^{-1}[yx] \to z$, $c^{-1}\delta \to zc^{-1}$, $c^{-1}\delta^{-1} \to z^{-1}c^{-1}$, $c^{-1}z \to a^{-1}$, $c^{-1}z^{-1} \to a^{-1}$, $c^{-1}a \to 0$, $c^{-1}b \to a$, $c^{-1}c \to zz^{-1}$, $c^{-1}d \to aa^{-1}$, $c^{-1}a^{-1} \to a^{-1}$, $c^{-1}b^{-1} \to b^{-1}$, $c^{-2} \to a^{-1}a$, $c^{-1}d^{-1} \to a^{-1}$, $d^{-1}x \to c^{-1}$, $d^{-1}y \to zd^{-1}$, $d^{-1}[xy] \to zz^{-1}$, $d^{-1}[yx] \to zc^{-1}$, $d^{-1}\delta \to z$, $d^{-1}\delta^{-1} \to z^{-1}$, $d^{-1}z \to a^{-1}a$, $d^{-1}z^{-1} \to a^{-1}a$, $d^{-1}a \to a^{-1}a$, $d^{-1}b \to a$, $d^{-1}c \to aa^{-1}$, $d^{-1}d \to zz^{-1}$, $d^{-1}a^{-1} \to 0$, $d^{-1}b^{-1} \to 0$, $d^{-1}c^{-1} \to b^{-1}$, $d^{-2} \to b^{-1}$, $aa^{-1}a \to a$, $a^{-1}aa^{-1} \to a^{-1}$, $ba^{-1}a \to b$, $a^{-1}ab^{-1} \to b^{-1}$, $czz^{-1} \to c$, $zz^{-1}c^{-1} \to c^{-1}$, $dzz^{-1} \to d$, $zz^{-1}d^{-1} \to d^{-1}$, $z^2z^{-1} \to z$, $zz^{-2} \to z^{-1}\} \cup$ $\{\alpha 0 \to 0,\ 0\alpha \to 0 \mid \alpha \in A\}$.

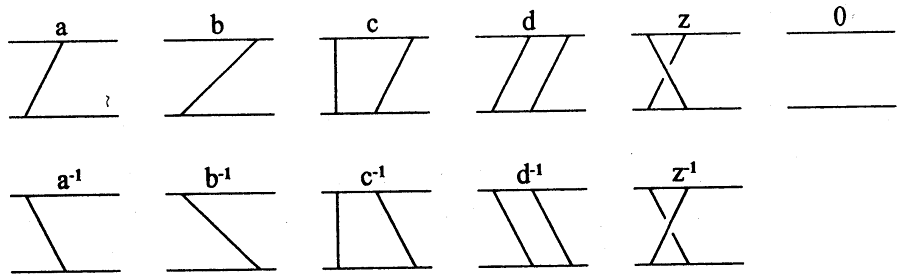

Fig.4

Theorem 6.2 (A, R) *is a finite complete presentation of* BI_3.

By the previous theorem and Result 3.1, $(A, \mathrm{Irr}(R))$ is a rational structure for BI_3. Moreover we have

Theorem 6.3 $(A, \mathrm{Irr}(R))$ *satisfies the strong fellow traveler property. Thus by Theorem 2.3, it is an automatic structure for* BI_3.

Hence, we have

Corollary 6.4 *The word problem for* BI_3 *is solvable.*

References

[1] R. V. Book and F. Otto, *String-Rewriting Systems*, Springer-Verlag, New York, 1993.

[2] C. M. Campbell, E. F. Robertson, N. Ruškuc and R. M. Thomas, *Automatic semigroups*, Theoretical Computer Science, **250** 2001, 365-391.

[3] J. W. Cannon, D. B. A. Epstein, D. F. Holt, S. V. F. Levy, M. S. Paterson and W. P. Thurston, *Word Processing in Groups*, Jones and Bartlett Publishers 1992.

[4] V. L. Hansen, *Braids and Coverings: selected topics*, London Math. Soc. Student Texts 18, Cambridge Univ. Press, 1989.

[5] S. M. Hermiller and J. Meier, *Artin groups, rewriting systems and three-manifolds*, Journal of Pure and Applied Algebra, **136** 1999, 141-156.

[6] I. Inata and Y. Kobayashi, *Monoids with subgroups of finite index and the braid inverse monoid*, SCMJ Special Issue on Computer Science, 2001 JAMS Annual Meeting, to appear. .